ITUPublications
Recomendaciones

Unión Internacional de Telecomunicaciones
Sector de la Normalización

Recomendación

UIT-T Y.4500.3 (01/2023)

SERIE Y: Infraestructura mundial de la información, aspectos del protocolo internet, redes de próxima generación, internet de las cosas y ciudades inteligentes

Internet de las cosas y ciudades y comunidades inteligentes – Marcos, arquitecturas y protocolos

---

Sistema oneM2M – Soluciones de seguridad

RECOMENDACIONES UIT-T DE LA SERIE Y

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN, ASPECTOS DEL PROTOCOLO INTERNET, REDES DE PRÓXIMA GENERACIÓN, INTERNET DE LAS COSAS Y CIUDADES INTELIGENTES

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN	
Generalidades	Y.100–Y.199
Servicios, aplicaciones y programas intermedios	Y.200–Y.299
Aspectos de red	Y.300–Y.399
Interfaces y protocolos	Y.400–Y.499
Numeración, direccionamiento y denominación	Y.500–Y.599
Operaciones, administración y mantenimiento	Y.600–Y.699
Seguridad	Y.700–Y.799
Características	Y.800–Y.899
ASPECTOS DEL PROTOCOLO INTERNET	
Generalidades	Y.1000–Y.1099
Servicios y aplicaciones	Y.1100–Y.1199
Arquitectura, acceso, capacidades de red y gestión de recursos	Y.1200–Y.1299
Transporte	Y.1300–Y.1399
Interfuncionamiento	Y.1400–Y.1499
Calidad de servicio y características de red	Y.1500–Y.1599
Señalización	Y.1600–Y.1699
Operaciones, administración y mantenimiento	Y.1700–Y.1799
Tasación	Y.1800–Y.1899
Televisión IP sobre redes de próxima generación	Y.1900–Y.1999
REDES DE LA PRÓXIMA GENERACIÓN	
Marcos y modelos arquitecturales funcionales	Y.2000–Y.2099
Calidad de servicio y calidad de funcionamiento	Y.2100–Y.2199
Aspectos relativos a los servicios: capacidades y arquitectura de servicios	Y.2200–Y.2249
Aspectos relativos a los servicios: interoperabilidad de servicios y redes en las redes de la próxima generación	Y.2250–Y.2299
Mejoras de las NGN	Y.2300–Y.2399
Gestión de red	Y.2400–Y.2499
Arquitecturas y protocolos de control de red	Y.2500–Y.2599
Redes basadas en paquetes	Y.2600–Y.2699
Seguridad	Y.2700–Y.2799
Movilidad generalizada	Y.2800–Y.2899
Entorno abierto con calidad de operador	Y.2900–Y.2999
REDES FUTURAS	Y.3000–Y.3499
COMPUTACIÓN EN LA NUBE	Y.3500–Y.3999
INTERNET DE LAS COSAS Y CIUDADES Y COMUNIDADES INTELIGENTES	
General	Y.4000–Y.4049
Definiciones y terminologías	Y.4050–Y.4099
Requisitos y casos de utilización	Y.4100–Y.4249
Infraestructura, conectividad y redes	Y.4250–Y.4399
Marcos, arquitecturas y protocolos	**Y.4400–Y.4549**
Servicios, aplicaciones, computación y proceso de datos	Y.4550–Y.4699
Gestión, control y calidad de funcionamiento	Y.4700–Y.4799
Identificación y seguridad	Y.4800–Y.4899
Evaluación y valoración	Y.4900–Y.4999

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T Y.4500.3

Sistema oneM2M – Soluciones de seguridad

Resumen

La Recomendación UIT-T Y.4500.3 proporciona especificaciones para la protección de la seguridad y la privacidad del sistema máquina a máquina (M2M).

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T Y.4500.3	2023-01-30	20	11.1002/1000/15076

Palabras clave

Autentificación, autorización, encriptación, integridad, seguridad, oneM2M, privacidad.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no se pronuncia en lo que respecta a la existencia, validez o aplicabilidad de los derechos de propiedad intelectual reclamados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patentes/derechos de autor de *software*, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar las correspondientes bases de datos del UIT-T disponibles en el sitio web del UIT-T en http://www.itu.int/ITU-T/ipr/.

© UIT 2023

Reservados todos los derechos. Ninguna parte de esta publicación puede reproducirse por ningún procedimiento sin previa autorización escrita por parte de la UIT.

ÍNDICE

Página

1 Alcance 1
2 Referencias 1
3 Definiciones 4
3.1 Términos definidos en otros documentos 4
3.2 Términos definidos en la presente Recomendación 5
3.3 Siglas y acrónimos 10
3.4 Símbolos 14
4 Convenios 14
5 Arquitectura de seguridad 15
5.1 Presentación general 15
5.2 Capas de seguridad 18
5.3 Integración en la arquitectura general de oneM2M 18
6 Servicios e interacciones de seguridad 19
6.1 Integración de la seguridad en el flujo de eventos de oneM2M 19
6.2 Capa de funciones de seguridad 23
6.3 Entorno seguro y abstracción del entorno seguro 28
7 Autorización 29
7.1 Mecanismo de control de acceso 29
7.2 Prevención de suplantación AE 40
7.3 Autorización dinámica 42
7.4 Control de acceso basado en funciones 54
8 Marcos de seguridad 58
8.1 Introducción general a los marcos de seguridad 58
8.2 Marcos de establecimiento de asociaciones de seguridad 65
8.3 Marcos de provisión de seguridad a distancia 76
8.4 Seguridad de extremo a extremo de las primitivas (ESPrim) 133
8.5 Seguridad de extremo a extremo de los datos (ESData) 146
8.6 Marcos de seguridad a distancia para la seguridad de extremo a extremo 158
8.7 Establecimiento de claves de extremo a extremo basadas en certificados (ESCertKE) 166
8.8 Detalles de un marco de seguridad con MAF 169
9 Procedimientos y parámetros de los marcos de seguridad 184
9.0 Introducción 184
9.1 Procedimientos y parámetros del marco de establecimiento de asociaciones de seguridad 184
9.2 Procedimientos y parámetros del marco de provisión de seguridad a distancia 188

Página

10 Detalles de los protocolos y los algoritmos 195
10.1 Detalles de un marco de seguridad basado en certificados 195
10.2 Detalles sobre el TLS y el DTLS 199
10.3 Detalles sobre la exportación y derivación de claves 200
10.4 Detalles sobre el credential-ID 204
10.5 KpsaID 204
10.6 Formato del KmID 205
10.7 Expiración de la inscripción 205
11 Arquitectura de protección de la privacidad mediante un gestor de la política de privacidad (PPM) 205
11.1 Introducción 205
11.2 Relación entre los componentes del PPM y del sistema oneM2M 205
11.3 Gestión de la política de privacidad en la arquitectura del sistema oneM2M 206
11.4 Modelos de implementación del gestor de la política de privacidad 211
12 Definiciones de los tipos de datos oneM2M específicos de seguridad 214
12.1 Introducción 214
12.2 Tipos de datos oneM2M específicos de seguridad simples 214
12.3 Tipos de datos oneM2M específicos de seguridad enumerados 215
12.4 Tipos de datos oneM2M específicos de seguridad complejos 219
Anexo A – Anexo en blanco 223
Anexo B – Anexo en blanco 224
Anexo C – Protocolos de seguridad asociados a tecnologías SE específicas 225
C.0 Introducción 225
C.1 UICC 225
C.2 Otro elemento seguro y elemento seguro incorporado compatible con la interfaz basada en ISO 7816 225
C.3 Entorno de ejecución confiable 225
C.4 Vinculación entre el SE y la CSE 225
Anexo D – Marco de seguridad UICC para dar soporte a los servicios oneM2M 226
D.0 Introducción 226
D.1 Marco de servicios oneM2M basado en UICC de la red de acceso 227
D.2 Aplicación del módulo de servicios oneM2M (1M2MSM) para credenciales simétricas en la UICC 235
Anexo E – Anexo en blanco 239
Anexo F – Adquisición de información de ubicación para el control de acceso basado en la ubicación 240
F.0 Introducción 240
F.1 Descripción de la región 240
F.2 Adquisición de la información de ubicación 241

Página

Anexo G – Anexo en blanco 244
Anexo H – Anexo en blanco 245
Anexo I – Anexo en blanco 246
Anexo J – Lista de atributos de privacidad 247
Apéndice I – Correspondencia de la terminología 3GPP GBA 263
Apéndice II – Mecanismo general de autentificación mutua 264
II.0 Introducción 264
II.1 Autentificación de grupos 264
Apéndice III – Apéndice en blanco 266
Apéndice IV – Apéndice en blanco 267
Apéndice V – Precisiones para que el marco UICC soporte los servicios M2M 268
V.0 Introducción 268
V.1 Contenido sugerido de los EF en la etapa previa a la personalización 268
V.2 Cambios en los EF mediante descarga de datos o aplicaciones CAT 268
V.3 Lista de los valores SFI a nivel del ADF_{M2MSM} o el DFM2M 269
V.4 Etiquetas UICC definidas en el Anexo J 269
Apéndice VI – Solicitud de decisión de control de acceso 270
Apéndice VII – Orientaciones de aplicación e índice de soluciones 271
Apéndice VIII – Apéndice en blanco 272
Apéndice IX – Apéndice en blanco 273
Apéndice X – Reglas de aplicación del lenguaje de marcaje de los términos y condiciones 274
Apéndice XI – Ejemplo de aplicación del SCEP 276
XI.1 Introducción 276
XI.2 Procedimiento de provisión de certificados utilizando el SCEP 276
Bibliografía 281

Recomendación UIT-T Y.4500.3

Sistema oneM2M – Soluciones de seguridad

1 Alcance

La presente Recomendación define las soluciones de seguridad aplicables al sistema máquina a máquina (M2M).

En la Recomendación se exponen la especificaciones de la versión 2 del Sistema oneM2M – Sistema oneM2M – Soluciones de seguridad V2.4.1 y es equivalente a las normas de los socios oneM2M, en particular ARIB, ATIS [b-ATIS.oneM2M.TS0003], CCSA, ETSI [b-ETSI TS 118 103], TIA, TSDSI [b-TSDSI STD T1.oneM2M TS-0003-2.4.1 V1.0.0], TTA [b-TTAT.MM-TS.0003 v2.4.1] y TTC [b-TTC TS-M2M-0003v2.4.1].

NOTA de redacción – La estructura de esta Recomendación, en particular las cláusulas 3, 4 y 5, es ligeramente distinta de la estructura habitual de las Recomendaciones del UIT-T, ya que el objetivo es su armonización con las normas equivalentes mencionadas en esta cláusula. Asimismo, varios anexos, apéndices y cláusulas se han dejado deliberadamente en blanco para mantener esta armonización.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

[UIT-T X.509]	Recomendación UIT-T X.509 (2019), *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos.*
[UIT-T Y.4500.1]	Recomendación UIT-T Y.4500.1 (2018), Sistema oneM2M – Arquitectura funcional.
[UIT-T Y.4500.4]	Recomendación UIT-T Y.4500.4 (2018), *Sistema oneM2M – Especificación del protocolo básico de la capa de servicio*.
[UITT Y.4500.11]	Recomendación UIT-T Y.4500.11 (2018), Sistema *oneM2M– Terminología común.*
[UIT-T Y.4500.22]	Recomendación UIT-T Y.4500.22 (2018), *Sistema oneM2M – Configuración de dispositivos sobre el terreno.*
[UIT-T Y.4500.32]	Recomendación UIT-T Y.4500.32 (2018), *Sistema oneM2M – Especificación de las interfaces MAF y MEF*.
[ARIB STD-T64-C. S0078-0]	ARIB STD-T64-C.S0078-0 v1.0 (2006), *Secured packet structure for CDMA Card Application Toolkit (CCAT) applications.*
[ARIB STD-T64 C.S0079-0]	ARIB STD-T64-C.S0079-0 v1.0 (2006), *Remote APDU Structure for CDMA Card Application Toolkit (CCAT) applications*.

[ETSI TS 101 220] ETSI TS 101 220 V16.0.0 (2021), *Smart Cards; ETSI numbering system for telecommunication application providers (Release 16)*.

[ETSI TS 102 221] ETSI TS 102 221 V16.2.0 (2020), *Smart Cards; UICC-Terminal interface; Physical and logical characteristics (Release 16)*.

[ETSI TS 102 225] ETSI TS 102 225 V11.0.0 (2012), *Smart Cards; Secured packet structure for UICC based applications (Release 11)*.

[ETSI TS 102 226] ETSI TS 102 226 V11.0.0 (2012), *Smart Cards; Remote APDU structure for UICC based applications (Release 11)*.

[ETSI TS 102 484] ETSI TS 102 484 V11.2.0 (2019), *Smart Cards; Secure channel between a UICC and an end-point terminal (Release 11)*.

[ETSI TS 102 671] ETSI TS 102 671 V11.0.0 (2018), *Smart Cards; Machine to Machine UICC; Physical and logical characteristics (Release 11)*.

[ETSI TS 131 115] ETSI TS 131 115 V10.1.1 (2013), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Secured packet structure for (U)SIM Toolkit applications (3GPP TS 31.115 version 10.1.1 Release 10)*.

[ETSI TS 131 116] ETSI TS 131 116 V10.3.0 (2012), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System(UMTS); LTE Remote APDU Structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications (3GPP TS 31.116 version 10.3.0 Release 10)*.

[ETSI TS 133 220] ETSI TS 133 220 V12.3.0 (2014), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System(UMTS); LTE; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) (3GPP TS 33.220 version 12.3.0 Release 12)*.

[IETF RFC 2104] IETF RFC 2104 (1997), *HMAC: Keyed-Hashing for Message Authentication*.

[IETF RFC 3548] IETF RFC 3548 (2003), The Base16, Base32, *and Base64 Data Encodings*.

[IETF RFC 3629] IETF RFC 3629 (2003), *UTF-8, a transformation format of ISO 10646*.

[IETF RFC 4279] IETF RFC 4279 (2005), *Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)*.

[IETF RFC 4492] IETF RFC 4492 (2006), Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS).

[IETF RFC 5246] IETF RFC 5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2*.

[IETF RFC 5280] IETF RFC 5280 (2008), *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

[IETF RFC 5289] IETF RFC 5289 (2009), *TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)*.

[IETF RFC 5480] IETF RFC 5480 (2009), *Elliptic Curve Cryptography Subject Public Key Information*.

[IETF RFC 5487] IETF RFC 5487 (2009), *Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode*.

[IETF RFC 5705] IETF RFC 5705 (2010), *Keying Material Exporters for Transport Layer Security (TLS)*.

[IETF RFC 5869] IETF RFC 5869 (2010), *HMAC-based Extract-and-Expand Key Derivation Function (HKDF)*.

[IETF RFC 6066] IETF RFC 6066 (2011), *Transport Layer Security (TLS) Extensions: Extension Definitions*.

[IETF RFC 6347] IETF RFC 6347 (2012), *Datagram Transport Layer Security Version 1.2*.

[IETF RFC 6655] IETF RFC 6655 (2012), *AES-CCM Cipher Suites for Transport Layer Security (TLS)*.

[IETF RFC 6920] IETF RFC 6920 (2013), *Naming Things with Hashes.*

[IETF RFC 6960] IETF RFC 6960 (2013), *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*.

[IETF RFC 6961] IETF RFC 6961 (2013), *The Transport Layer Security (TLS) Multiple Certificate Status Request Extension*.

[IETF RFC 7030] IETF RFC 7030 (2013), *Enrollment over Secure Transport.*

[IETF RFC 7250] IETF RFC 7250 (2014), *Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*.

[IETF RFC 7251] IETF RFC 7251 (2014), *AES-CCM Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)*.

[IETF RFC 7515] IETF RFC 7515 (2015), *JSON Web Signature (JWS).*

[IETF RFC 7516] IETF RFC 7516 (2015), *JSON Web Encryption (JWE)*.

[IETF RFC 7518] IETF RFC 7518 (2015), *JSON Web Algorithms (JWA)*.

[IETF RFC 7519] IETF RFC 7519 (2015), *JSON Web Token (JWT)*.

[IETF RFC 8824] IETF RFC 8824 (2020), *Simple Certificate Enrolment Protocol*.

[ISO/IEC 7816-4] ISO/IEC 7816-4:2020, *Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange*.

[NIST EC] National Institute of Standards and Technology (July 1999), *Recommended Elliptic Curves for Federal Government user*. http://csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf

[OIDF CC] OpenID Foundation (2014), *OpenID Connect Core 1.0 incorporating errata set 1*.

[TIA-1098-A] TIA-1098-A (2008), *Generic Bootstrapping Architecture (GBA) Framework, (3GPP2 S.S0109-A)*.

[Unicode] Unicode 5.1.0 (2008), Unicode Standard Annex #15; *Unicode Normalization Forms.* http://www.unicode.org.

[W3C XMLSIG] W3C Recommendation (2013), *XML Signature Syntax and Processing v1.1*. http://www.w3.org/TR/xmlsig-core1/.

[W3C XMLENC] W3C Recommendation (2013), *XML Encryption Syntax and Processing v1.1*. http://www.w3.org/TR/xmlenc-core1/.

3 Definiciones

3.1 Términos definidos en otros documentos

A los efectos de esta Recomendación, se aplicarán los términos y definiciones que figuran en la Recomendación [UIT Y.4500.11].

3.1.1 datos autentificados adicionales [TIA-1098-A]: Se refiere a los datos que están autentificados, pero que no han sido encriptados por un algoritmo de encriptación autentificado con datos asociados.

3.1.2 encriptación autentificada con datos asociados [TIA-1098-A]: Algoritmo que proporciona confidencialidad al texto sin formato y que sirve para comprobar su integridad y autenticidad, permitiendo a la vez comprobar la integridad y autenticidad de algunos datos autentificados adicionales. En este contexto, el texto sin formato se refiere a los datos autentificados y encriptados.

3.1.3 función de servidor de inicialización (BSF)[ETSI TS 133 220]: La BSF está alojada en un elemento de red bajo el control de un operador de red móvil. La BSF, el sistema de abonado de origen (HSS) y el equipo de usuario (UE) forman parte de la arquitectura de inicialización genérica (GBA) en la que se establece un secreto compartido entre la red y un UE mediante la ejecución del procedimiento de inicialización

NOTA – El secreto compartido puede ser utilizado entre las NAF y los UE, por ejemplo, para fines de autentificación

3.1.4 identificador de la transacción de inicialización (B-TID) [ETSI TS 133 220]: El identificador de la transacción de inicialización (B-TID) se utiliza para vincular la identidad del abonado con el material relativo a la clave en los puntos de referencia Ua, Ub y Zn de la GBA.

3.1.5 certificado CA [b-Menezes]: Certificado emitido por una autoridad de certificación (CA) que certifica la clave pública de otra CA.

3.1.6 firma digital [b-UIT-T X.510]: Resultado de una transformación criptográfica de datos que, si se realiza correctamente, ofrece un mecanismo que permite la autentificación del origen, la integridad de los datos y el no repudio del firmante.

NOTA – El resumen se obtiene mediante una función resumen (hash) unidireccional, mientras que el encriptado se realiza mediante la clave privada del firmante.

3.1.7 información de identificación personal [ETSI TS 133 220]: Toda información que sobre una persona mantiene una agencia, incluida la que pueda ser utilizada para distinguir o rastrear la identidad de una persona, como el nombre, el número de seguridad social, la fecha y el lugar de nacimiento, el nombre de soltera de la madre o el registro de datos biométricos, así como los demás datos relacionados con una persona, como la información médica, educativa, financiera y laboral.

3.1.8 punto de decisión de política [b-OASIS XACML]: Entidad de sistema que evalúa la política aplicable y emite una decisión de autorización.

3.1.9 punto de aplicación de política [b-OASIS XACML]: Entidad de sistema que realiza el control de acceso, emitiendo solicitudes de decisión y aplicando las decisiones de autorización.

3.1.10 punto de información de política [b-OASIS XACML]: Entidad de sistema que actúa como fuente de valores de atributo.

3.2 Términos definidos en la presente Recomendación

En esta Recomendación se definen los siguientes términos:

3.2.1 certificado AE-ID: Certificado con una cadena de certificados que llega hasta el certificado ancla de confianza, que incluye un identificador de entidad de aplicación (AE-ID) en la extensión *subjectAltName*.

NOTA – El certificado AE-ID puede utilizarse para verificar si a una entidad se le ha asignado el AE-ID del certificado.

3.2.2 configuración de la asociación: Fase de un marco de establecimiento de asociaciones de seguridad en la que la entidad que establece la asociación de seguridad (y el servidor del centro de distribución de claves, en el caso de los marcos de seguridad centralizados) recibe las identidades (y demás credenciales pertinentes) que permiten asegurar que se ha establecido la asociación de seguridad entre las entidades previstas.

3.2.3 toma de contacto de seguridad de la asociación: Fase de un marco de establecimiento de asociaciones de seguridad en la que los extremos de la asociación de seguridad efectúan la autentificación mutua.

3.2.4 credencial de inicialización: Credencial preaprovisionada que permite la autentificación mutua del inscrito y de la función de inscripción M2M.

3.2.5 configuración de la credencial de inicialización – Fase de un marco de provisión de seguridad a distancia en la que las credenciales de inicialización se aprovisionan previamente al inscrito y la función de inscripción M2M.

3.2.6 toma de contacto para inscripción de inicialización: Fase de un marco de provisión de seguridad a distancia en la que el inscrito y la función de inscripción M2M efectúan una autentificación mutua.

3.2.7 configuración de la instrucción de inicialización: Fase de un marco de provisión de seguridad a distancia en la que el inscrito y la función de inscripción M2M reciben identidades (y cualquier otra credencial pertinente) que permiten que la función de inscripción M2M establezca una credencial maestra entre el inscrito previsto y la función de autentificación M2M.

3.2.8 certificado: Véase certificado de clave pública.

3.2.9 autoridad de certificación: Autoridad que emite el certificado.

3.2.10 cadena de certificados: Secuencia de uno o más certificados CA en la que se valida la clave de verificación pública de cada certificado CA en el certificado de CA anterior, y la clave pública del primer certificado CA se considera a priori fiable.

NOTA – La confianza en la clave pública de cada certificado CA se fundamenta en la confianza en el certificado CA anterior.

3.2.11 nombre del certificado: Identificador único en el campo de nombre de un certificado (por ejemplo, en el atributo *subject* o *subjectAltName* de la Recomendación UIT-T X.509).

3.2.12 procedimiento para el aprovisionamiento de certificados: Procedimiento realizado por una entidad de seguridad y una MEF para aprovisionar a la entidad de seguridad con un certificado suministrado por la MEF y uno o varios certificados de la autoridad de certificación de la MEF.

NOTA – Pueden aprovisionarse certificados adicionales de la autoridad de certificación también por otros medios, como el preaprovisionamiento o [UIT-T Y.4500.22].

3.2.13 procedimiento de reaprovisionamiento de certificado: Procedimiento de aprovisionamiento de certificados realizado cuando la entidad de seguridad puede autentificarse con un certificado de inscripción válido.

3.2.14 solicitud de firma de certificado: Mensaje utilizado para solicitar un certificado de clave pública.

3.2.15 verificación de certificados: Proceso necesario para poder confiar en el certificado de una entidad.

3.2.16 autoridad de certificación [b-Menezes]: Autoridad encargada de establecer y garantizar la autenticidad de las claves públicas.

NOTA – [Esto] incluye la vinculación de las claves públicas a nombres distinguidos mediante certificados firmados, la gestión de los números de serie de los certificados y la revocación de certificados.

3.2.17 clave de encriptación de contenido: Clave simétrica utilizada para encriptar el texto sin formato con el fin de producir el texto cifrado y generar una verificación de integridad del mensaje (MIC).

NOTA – En la encriptación autentificada con datos asociados (AEAD) se utiliza directamente la clave de encriptación de contenido, mientras que en otros algoritmos la clave de encriptación de contenido se utiliza para generar claves distintas para el algoritmo de encriptación y el algoritmo de protección de la integridad.

3.2.18 configuración de credenciales: Fase de un marco de establecimiento de asociaciones de seguridad en la que se configuran las credenciales necesarias para el marco de establecimiento de asociaciones de seguridad para las entidades y funciones pertinentes.

3.2.19 credential-ID type-ID: Parte del ID de una credencial que indica el tipo de credencial que se identifica.

3.2.20 Certificado CSE-ID: Certificado con una cadena de certificados que llega hasta una raíz de confianza y que contiene un identificador de entidad de servicio común (CSE-ID) en la extensión *subjectAltName*.

NOTA – El certificado CSE-ID puede utilizarse para verificar si a una entidad se le ha asignado el CSE-ID del certificado.

3.2.21 certificado de dispositivo: Certificado con una cadena de certificados que llega hasta una raíz de confianza y que incluye en la extensión *subjectAltName* por lo menos un identificador de instancia de hardware globalmente único

NOTA – El certificado de dispositivo puede utilizarse para verificar si una entidad se ejecuta en la instancia de hardware identificada.

3.2.22 extremo de inicio del ESCertKE: Punto extremo ESCertKE que inicia el procedimiento ESCertKE.

3.2.23 mensajes ESCertKE: Mensajes intercambiados entre el extremo de inicio del ESCertKE y el extremo de terminación del ESCertKE como parte del establecimiento de claves mediante certificado de extremo a extremo.

3.2.24 procedimiento ESCertKE: Secuencia de mensajes ESCertKE intercambiados y procesamiento basado en esos mensajes ESCertKE, a efectos del establecimiento de claves de extremo a extremo mediante certificado.

3.2.25 extremo de terminación del ESCertKE: extremo de terminación del ESCertKE con el que el extremo de inicio del ESCertKE se propone realizar el procedimiento ESCertKE.

3.2.26 establecimiento de claves de extremo a extremo mediante certificados: Marco interoperable que permite a dos extremos utilizar certificados para establecer las claves simétricas

secretas de extremo a extremo para utilizarlas en otros marcos de seguridad de extremo a extremo, como la seguridad de datos de extremo a extremo (ESData) o la seguridad de primitivas de extremo a extremo (ESPrim).

3.2.27 seguridad de los datos de extremo a extremo: Marco interoperable para la protección de los datos que son transportados a través de los puntos de referencia del sistema oneM2M que tiene por objeto conseguir que las entidades de servicio común (CSE) que han transitado no tengan que asegurar esos datos.

3.2.28 seguridad de las primitivas de extremo a extremo: Marco interoperable para la seguridad del intercambio de primitivas del sistema oneM2M que tiene por objeto conseguir que las CSE no tengan que asegurar la confidencialidad y la integridad de las primitivas.

3.2.29 inscrito: Entidad de aplicación (AE) o CSE que requiere el aprovisionamiento a distancia de una clave simétrica que compartirá con un destinatario de la inscripción.

3.2.30 clave de inscripción: Clave simétrica que se establece entre un inscrito y la función de inscripción M2M tras una autentificación mutua exitosa.

NOTA – La clave simétrica que compartirán el inscrito y el destinatario de la inscripción puede obtenerse (en el inscrito y la función de inscripción M2M) de la clave de inscripción actualmente vigente; posteriormente la función de inscripción M2M suministra de forma segura la clave simétrica al destinatario de la inscripción.

3.2.31 generación de la clave de inscripción: Fase de un marco de provisión de seguridad a distancia en la que el inscrito y la función de inscripción M2M establecen una clave de inscripción y un identificador de clave de inscripción.

3.2.32 fase de inscripción: Etapa en el ciclo de vida de un equipo M2M en el que se le aprovisiona para su funcionamiento con un proveedor de servicios M2M específico.

3.2.33 destinatario de la inscripción: Función de autentificación M2M, CSE, o AE con el que un inscrito desea establecer una clave simétrica (credencial maestra o clave de conexión segura preaprovisionada) mediante la provisión de seguridad a distancia.

3.2.34 identificador de entidad: CSE-ID (o AE-ID respectivamente) de una CSE (o AE respectivamente).

3.2.35 envolvente ESData: Objeto de datos que contiene el resultado de la protección de una carga útil de seguridad de datos (ESData) de extremo a extremo utilizando los procedimientos de ESData.

3.2.36 carga útil de ESData: Datos que deben protegerse mediante la seguridad de datos de extremo a extremo (ESData).

3.2.37 certificado FQDN: Certificado con una cadena de certificados que llega hasta una raíz de confianza y que contiene un nombre de dominio totalmente cualificado (FQDN).

3.2.38 arquitectura de inicialización genérica: Conjunto de especificaciones de 3GPP y 3GPP2 que ofrecen características de seguridad y un mecanismo de inicialización de la autentificación y el acuerdo de claves para la seguridad de las aplicaciones sobre la base de los mecanismos de autentificación de red subyacentes de 3GPP y 3GPP2.

3.2.39 procedimiento de aprovisionamiento de certificado inicial: Procedimiento de aprovisionamiento de certificados que se realiza cuando la entidad de seguridad no puede autentificarse con un certificado de inscripción válido.

3.2.40 primitiva de solicitud interna: Primitiva de solicitud que debe ser protegida por la seguridad de primitivas de extremo a extremo (ESPrim).

3.2.41 primitiva de respuesta interna: Primitiva de respuesta que debe ser protegida por la seguridad de primitivas de extremo a extremo (ESPrim).

3.2.42 código de integridad del mensaje: Etiqueta calculada a partir de un mensaje y una clave simétrica, y adjuntada a un mensaje.

NOTA 1 – La finalidad del código de integridad del mensaje es facilitar, sin tener que recurrir a ningún mecanismo adicional, garantías en relación con el origen de un mensaje y su integridad.

NOTA 2 – El código de integridad del mensaje se denomina a veces código de autentificación del mensaje. Se utiliza aquí código de integridad del mensaje ya que la abreviatura del código de autentificación del mensaje, MAC, podría confundirse con el control de acceso a los medios. La definición se basa en el texto de [b-Menezes] (pág. 323).

3.2.43 clave de conexión segura M2M: Clave simétrica establecida por una función de autentificación M2M entre dos entidades (CSE o AE), con el fin de obtener una comunicación segura entre esas dos entidades.

NOTA – Esta clave de conexión segura M2M es el resultado de un procedimiento exitoso de establecimiento de una asociación de seguridad M2M.

3.2.44 habilitador de confianza M2M: Parte interesada a la que se le confía la habilitación de la autentificación de una o varias CSE o AE respecto de otras CSE o AE.

3.2.45 cliente MAF: CSE o AE configurada para utilizar los servicios de una función de autentificación M2M (MAF).

3.2.46 procedimiento de configuración de credenciales MAF: Procedimiento del marco de seguridad de la función de autenticación M2M (MAF) utilizado para la fase de inscripción de un extremo mediante el establecimiento de credenciales para la autentificación mutua entre un extremo y una MAF.

3.2.47 procedimiento de toma de contacto MAF: Procedimiento del marco de seguridad de la función de autenticación M2M (MAF)en el que una entidad y la MAF efectúan una autentificación mutua y generan una clave simétrica que puede ser utilizada en la toma de contacto de seguridad de la asociación para la autentificación mutua entre esa entidad y otras entidades.

3.2.48 procedimiento de registro de claves MAF: Procedimiento del marco de seguridad de la función de autenticación M2M (MAF) según el cual un extremo de origen y la MAF generan una clave simétrica que luego puede utilizarse para la autentificación mutua entre el extremo de origen y uno o más puntos extremos de destino.

3.2.49 procedimiento de recuperación de claves MAF: Procedimiento del marco de seguridad de la función de autenticación M2M (MAF) en el que un extremo de destino recupera la clave simétrica generada previamente por la MAF y un extremo de origen, con el fin de posibilitar la autentificación mutua entre el extremo de origen y el extremo de destino.

3.2.50 credenciales maestras: Credenciales utilizadas para la autentificación mutua entre una ASN/MN-CSE y la función de autenticación M2M (MAF). Esto tiene por objeto garantizar un acceso seguro a la infraestructura de un proveedor de servicios M2M.

NOTA – Las credenciales maestras se aprovisionan previamente o a distancia (sin que se dependa de esas credenciales).

3.2.51 autoridad de certificación MEF: Función de una autoridad de certificación que emite certificados aprovisionados por una función de inscripción M2M (MEF) para entidades de seguridad a través de la MEF.

NOTA – El término se refiere a una MEF, por lo que una autoridad de certificación MEF relativa a una MEF es distinta de una autoridad de certificación MEF relativa a otra MEF.

3.2.52 cliente MEF: funcionalidad para realizar procedimientos de la función de inscripción M2M (MEF) en nombre de una CSE o AE asociada, o en nombre de una o varias CSE o AE presentes en un nodo asociado o una función de autenticación M2M (MAF) asociada.

3.2.53 certificado aprovisionado por MEF: Certificado emitido por una autoridad de certificación, a través de una MEF, para autentificar a la entidad de seguridad.

NOTA – El término se refiere a una MEF, por lo que un certificado aprovisionado por MEF relativo a una MEF es distinto de un certificado aprovisionado por MEF relativo a otra MEF.

3.2.54 entidad de seguridad (oneM2M): CSE, AE, Nodo o Dispositivo M2M que puede ser autentificado.

NOTA – Cuando la entidad de seguridad es un nodo o dispositivo M2M, el nodo o dispositivo M2M actúa en nombre de la CSE y/o AE que se ejecuta en el nodo o dispositivo M2M.

3.2.55 Protocolo de estado de certificado en línea: Protocolo para solicitar un informe sobre el estado de uno o más certificados UIT-T X.509 [IETF RFC 6960].

3.2.56 fase operativa: Periodo del ciclo de vida de un equipo M2M durante el cual se utiliza para prestar servicios M2M.

3.2.57 primitiva de solicitud externa: Primitiva de solicitud utilizada para transportar el objeto de datos que contiene una primitiva de solicitud interna a la que se ha aplicado la seguridad de primitivas de extremo a extremo (ESPrim).

3.2.58 primitiva de respuesta externa: Primitiva de respuesta utilizada para transportar el objeto de datos que contiene una primitiva de respuesta interna a la que se ha aplicado la seguridad de primitivas de extremo a extremo (ESPrim).

3.2.59 punto de recuperación de política: Entidad del sistema que recupera la política o el conjunto de políticas aplicables.

3.2.60 clave de conexión segura preaprovisionada: Clave simétrica preaprovisionada para dos entidades (que pueden ser AE o CSE) y que se utiliza para la autentificación mutua de dichas entidades al establecerse la asociación de seguridad.

3.2.61 identificador de clave de conexión segura preaprovisionada: Identificador de una clave de conexión segura aprovisionada previamente.

3.2.62 clave simétrica de inscrito preaprovisionada: Clave simétrica que se preaprovisiona para el inscrito y la función de inscripción M2M.

3.2.63 identificador de la clave simétrica de inscrito preaprovisionada: Identificador de una clave simétrica del inscrito aprovisionada previamente.

3.2.64 clave privada de firma: Clave secreta que permite generar firmas que pueden ser verificadas utilizando la clave de verificación pública correspondiente.

3.2.65 certificado de clave pública: Documento electrónico que utiliza una firma digital para vincular una clave pública con una identidad.

NOTA – [b-Menezes] El *certificado de clave pública* es una estructura de datos que consta de una parte para datos y una parte para la firma. La parte para datos contiene datos en texto sin cifrar que incluyen, como mínimo, una clave pública [de verificación] y una cadena que identifica a la parte (entidad sujeto) que se asocia a ella. La parte para la firma consiste en la firma digital de una autoridad de certificación sobre la parte para datos, vinculando así la identidad de la entidad sujeto a la clave pública especificada.

3.2.66 tipo de certificado de clave pública: Nombre que describe el uso de un certificado de clave pública en el ámbito del sistema oneM2M.

3.2.67 infraestructura de clave pública: Conjunto de equipos, software, personas, políticas y procedimientos necesarios para crear, gestionar, distribuir, utilizar, almacenar y revocar certificados de clave pública. Para más detalles, véase [b-Menezes].

3.2.68 clave pública de verificación: Credencial que permite verificar las firmas digitales generadas por la clave privada de firma correspondiente, pero que no puede utilizarse para generar firmas digitales.

3.2.69 certificado de la clave pública bruta: Certificado que comprende únicamente la estructura *SubjectPublicKeyInfo* de un certificado UIT-T X.509 que lleva los parámetros necesarios para describir la clave pública [IETF RFC 7250].

3.2.70 autoridad de registro: Entidad funcional encargada de verificar las solicitudes de firma de certificados y de autorizar que una autoridad de certificación emita el certificado correspondiente.

3.2.71 identificador de la clave de inscripción relativo: Parte del identificador de la clave de inscripción que es única en el contexto de una función de inscripción M2M.

3.2.72 establecimiento de una asociación de seguridad: Procesamiento secuencial de la configuración de credenciales, la configuración de la asociación y toma de contacto de seguridad de la asociación entre dos entidades.

3.2.73 marco de establecimiento de asociaciones de seguridad: Marco de seguridad para el establecimiento de asociaciones de seguridad.

3.2.74 marco de inicialización de seguridad o marco de provisión de seguridad a distancia: Mecanismo que permite el aprovisionamiento a distancia de una credencial maestra y un identificador de credencial maestra a un inscrito y una función de autentificación M2M.

3.2.75 entorno seguro: Entidad lógica que protege los datos sensibles y las funciones sensibles de cualquier manipulación, vigilancia o ejecución no autorizadas y que proporciona acceso a esos datos y funciones sensibles a las entidades del sistema oneM2M autorizadas.

3.2.76 marco de seguridad: Conjunto de procedimientos que aseguran el establecimiento de una asociación de seguridad o la provisión de seguridad a distancia.

3.2.77 identificador de uso de seguridad: Identifica una característica de seguridad (por ejemplo, el marco de establecimiento de asociaciones de seguridad, la seguridad de primitivas de extremo a extremo o la seguridad de los datos de extremo a extremo), un protocolo utilizado para esa característica de seguridad y, en su caso, una opción dentro de un mismo protocolo.

NOTA – El identificador de uso de seguridad se utiliza para limitar las modalidades de utilización de una credencial.

3.2.78 función sensible: Función procesada dentro del entorno seguro que necesita protegerse contra cualquier vigilancia, manipulación o ejecución no autorizadas y que opera con datos sensibles, por ejemplo, la obtención de claves a partir de claves de capa de servicio a largo plazo M2M y algoritmos criptográficos.

3.2.79 certificado autofirmado: Certificado de clave pública firmado por la misma entidad cuya identidad certifica.

3.2.80 extremo de origen ESData: Entidad que produce un envolvente de datos de seguridad de extremo a extremo (ESData) a partir de una carga útil ESData.

3.2.81 clave simétrica: Clave secreta que se comparte entre dos entidades.

3.2.82 extremo ESData de destino: Entidad que produce la carga útil de seguridad de los datos de extremo a extremo (ESData) verificada a partir de un envolvente ESData.

3.2.83 certificado ancla de confianza: Certificado al que se otorga confianza a priori.

3.3 Siglas y acrónimos

En la presente Recomendación se utilizan las siguientes siglas y acrónimos:

(D)TLS-PSK (D) Conjuntos de cifrado de claves previamente compartidas en la TLS *((D) (TLS Pre-Shared Key (ciphersuites*))

AAA Autentificación, autorización y contabilidad (*Authentication, Authorization and Accounting)*

ABAC Control de acceso por atributos (*Attribute Based Access Control)*

ACP	Instancia de política de control de acceso (*AccessControlPolicy Instance*)
AE	Entidad de aplicación (*Application Entity*)
AEAD	Encriptación autentificada con datos asociados (*Authenticated Encryption with Associated Data*)
AE-ID	Identificador de la entidad de aplicación (*Application Entity Identifier*)
API	Interfaz de programación de aplicaciones (*Application Programming Interface*)
App-ID	Identificador de aplicación (*Application Identifier*)
ASN-CSE	CSE que reside en el nodo de servicio de aplicación (*CSE which resides in the Application Service Node*)
BSF	Función del servidor de inicialización (*Bootstrapping Server Function*)
B-TID	Identificador de la transacción de inicialización (*Bootstrapping Transaction Identifier*)
CA	Autoridad de certificación (*Certification Authority or Certificate Authority*)
CIDR	Encaminamiento entre dominios sin clase (*Classless Inter-Domain Routing*)
CoAP	Protocolo de aplicación limitada (*Constrained Application Protocol*)
CSE	Entidad de servicio común (*Common Service Entity*)
CSE-ID	Identificador de entidad de servicio común (*Common Service Entity Identifier*)
CSR	Solicitud de firma de certificado (*Certificate Signing Request*)
DAS	Sistema de autorización dinámico (*Dynamic Authorization System*)
DTLS	Protocolo de seguridad de la capa de transporte de datagramas (*Datagram Transport Layer Security (Protocol))*
EKU	Utilización de clave ampliada (*Extended Key Usage*)
Enrolee-ID	Identidad del inscrito (*Enrolee Identity*)
ESCertKE	Establecimiento de clave mediante certificado de extremo a extremo (*End-to-End Certificate-based Key Establishment*)
ESData	Seguridad de los datos de extremo a extremo (*End-to-End Security of Data*)
ESF	Función de seguridad de extremo a extremo (*End-to-End Security Function*)
ESPrim	Seguridad de las primitivas de extremo a extremo (*End-to-end Security of Primitives*)
EST	Inscripción en transporte seguro (*Enrolment over Secure Transport*)
FQDN	Nombre de dominio totalmente cualificado (*Fully Qualified Domain Name*)
GBA_ME	GBA basada en ME (*ME-based GBA*)
GBA_U	GBA con mejoras basadas en las UICC (*GBA with UICC-based enhancements*)
GUSS	Configuración de seguridad del usuario en la GBA (*GBA User Security Settings*)
HLR	Registro de posiciones propio (*Home Location Register*)
HSS	Sistema de abonado residencial (*Home Subscriber System*)
HTTP	Protocolo de transferencia de hipertexto (*HyperText Transfer Protocol*)
ID	Identificador (*Identifier*)
IdA	Identificador de la entidad A (*Identifier for entity A*)

IdB Identificador de la entidad B (*Identifier for entity B*)

IN Nodo de infraestructura (*Infrastructure Node*)

IN-CSE CSE que reside en el nodo de infraestructura (*CSE which resides in the Infrastructure Node*)

IPv4 Versión 4 del protocolo internet (*Internet Protocol version 4*)

IPv6 Versión 6 del protocolo internet (*Internet Protocol version 6*)

IV Vector de inicialización (*Initialization Vector)*

JWE Encriptación web JSON (*JSON Web Encryption*)

JWS Firma web JSON (*JSON web signature*)

JWT Testigo web JSON (*JSON Web Token*)

Kc Clave de conexión segura M2M *(M2M Secure ConnectionKey)*

KcID Identificador de clave de conexión segura M2M (*M2M Secure Connection Key Identifier*)

Ke Clave de inscripción (*Enrolment Key*)

KeID Identificador de clave de inscripción (*Enrolment Key Identifier*)

Ker Clave de renovación de la autentificación de la inscripción (*Enrolment Re-Authentication Key)*

Km Credencial maestra (*Master Credential*)

KmID Identificador de credencial maestra (*Master Credential Identifier*)

Kpm Credencial preaprovisionada para el suministro de la credencial maestra (*pre-provisioned credential for Master Credential provisioning*)

KpmID Identificador de credencial preaprovisionada para el suministro de la credencial maestra (*pre-provisioned credential for Master Credential provisioning Identifier*)

Kpsa Credencial aprovisionada para el establecimiento de una asociación de seguridad M2M (*provisioned credential for M2M Security Association Establishment)*

KpsaID Identificador de credencial aprovisionada para el establecimiento de una asociación de seguridad M2M (*provisioned credential for M2M Security Association Establishment Identifier*)

Ks Claves temporales a que se refiere la GBA (*temporary Key material referred to in GBA*)

Ks. NAF Abreviatura de Ks_(int/ext)_NAF (*Abbreviation of Ks_(int/ext)_NAF*)

Ks_(ext/int) _NAF Clave obtenida en la GBA_ME o clave obtenida en la GBA_U que se mantiene en la UICC (*Derived key in GBA_ME or Derived key in GBA_U which remains on UICC*)

Ks_ext_NAF Clave obtenida en la GBA_U que se envía al ME (*Derived key in GBA_U sent to the ME*)

Ks_int_NAF Clave obtenida en la GBA_U que se mantiene en la UICC (*Derived key in GBA_U which remains on UICC*)

Ks_NAF Clave obtenida en el ME (*Derived key in the ME*)

M2M Máquina a máquina (*Machine to Machine*)

M2M-SP Proveedor de servicios M2M (*M2M Service Provider*)

MAF	Función de autentificación M2M (*M2M Authentication Function)*
MAF-ID	Identificador de función de autentificación M2M (*M2M Authentication Function Identifier)*
Mca	Punto de referencia para comunicaciones M2M con la AE (*Reference Point for M2M Communication with AE*)
Mcc	Punto de referencia para comunicaciones M2M con la CSE (*Reference Point for M2M Communication with CSE*)
Mcc'	Punto de referencia para comunicaciones M2M con la CSE de diferentes proveedores de servicios M2M *(Reference Point for M2M Communication with CSE of different M2M Service Provider*)
Mcn	Punto de referencia para las comunicaciones M2M con el NSE (*Reference Point for M2M Communication with NSE)*
MEF	Función de inscripción M2M (*M2M Enrolment Function*)
MIC	Código de integridad del mensaje (*Message Integrity Code*)
MN-CSE	CSE que reside en el nodo central (*CSE which resides in the Middle Node*)
MTE	Habilitador de confianza M2M (*M2M Trust Enabler*)
NAF	Función de aplicación de red (*Network Application Function*)
OCSP	Protocolo de estado de certificación en línea (*Online Certificate Status Protocol*)
OTA	Radioeléctrico (*Over The Air*)
PDP	Punto de decisión de política (*Policy Decision Point*)
PEP	Punto de imposición de política **(***Policy Enforcement Point*)
PII	Información de identificación personal (*Personally Identifiable Information*)
PIP	Punto de información de política (*Policy Information Point*)
PKI	Infraestructura de clave pública (*Public Key Infrastructure*)
PRP	Punto de recuperación de política (*Policy Retrieval Point*)
RA	Autoridad de registro (*Registration Authority*)
RSPF	Marco de provisión de seguridad a distancia (*Remote Security Provisioning Framework*)
SAEF	Marco de establecimiento de asociaciones de seguridad (*Security Association Establishment Framework*)
SCEP	Protocolo simple de inscripción de certificados (*Simple Certificate Enrolment Protocol*)
SE	Entorno seguro (*Secure Environment*)
SUID	Identificadores de uso de seguridad (*Security Usage Identifier*)
TEE	Entorno de ejecución confiable (*Trusted Execution Environment*)
TEF	Función habilitadora de confianza (*Trust Enabling Function*)
TLS	Protocolo de seguridad de la capa de transporte (*Transport Layer Security (Protocol)*)
UE	Equipo de usuario (3GPP) *((3GPP) User Equipment*)
UICC	Tarjeta de circuito integrado universal (*Universal Integrated Circuit Card*)

UNSP Proveedor de servicio de red subyacente (*Underlying Network Service Provider*)

URI Identificador uniforme de recursos (*Uniform Resource Identifier*)

USS Configuración de la seguridad del usuario (*User Security Settings*)

XACML Lenguaje de marcaje de control de acceso extensible (*extensible Access Control Markup Language*)

3.4 Símbolos

A los efectos de la presente Recomendación se aplica el siguiente símbolo:

|| Concatenación

4 Convenios

En esta Recomendación los términos deberá, no deberá, debe, no debe, puede y puede no se interpretarán como se indica a continuación:

Deberá/no deberá:

Requisitos

1) Efecto en la norma: la norma ha de describir la característica requerida (es decir, especificar una solución técnica para el requisito).
2) Efecto en los productos: todas las implementaciones (solución M2M conforme a esta Recomendación) deben soportarla; y
3) Efecto en la implantación: todas las implantaciones (servicio M2M basado en esta Recomendación) deben utilizar la característica normalizada, siempre que sea posible; en caso contrario, pueden surgir problemas de interoperabilidad con otros servicios, entre otras cosas.

Debe/no debe:

Recomendación

1) Efecto en la norma: la norma ha de describir una solución que permita la presencia y la ausencia de la característica.
2) Efecto en los productos: las implementaciones pueden o no soportarla, aunque se recomienda el soporte.
3) Efecto en la implantación: la implantación puede o no utilizar la característica, pero se recomienda su utilización.

Puede/puede no:

Permiso/opción

1) Efecto en la norma: la norma ha de describir una solución que permita la presencia y la ausencia de la característica requerida.
2) Efecto en los productos: las implementaciones pueden o no soportarla.
3) Efecto en la implantación: una implantación puede o no utilizar la característica.

5 Arquitectura de seguridad

5.1 Presentación general

5.1.0 Introducción

La Figura 5.1.0-1 ofrece una visión general de la arquitectura de seguridad.

La arquitectura consta de las siguientes capas:

Capa de funciones de seguridad

Esta capa contiene un conjunto de funciones de seguridad que se exponen en el punto de referencia Mca y Mcc. Estas funciones de seguridad pueden clasificarse en seis categorías: identificación, autentificación, autorización, asociación de seguridad, tratamiento de datos sensibles y administración de seguridad.

Capa de entorno seguro

Esta capa implementa diversas capacidades de seguridad, como la derivación de claves, el cifrado/descifrado de datos, la generación/verificación de firmas, la lectura/escritura de credenciales de seguridad desde/hacia los entornos seguros, etc. Las funciones de seguridad de la capa de funciones de seguridad recurren a estas funciones para proteger las operaciones en los entornos seguros. Además, esta capa también proporciona acceso físico a los entornos seguros. Su implementación queda fuera del ámbito de la presente Recomendación. Esta capa no se especifica en la presente versión, pero cabe esperar que se tendrá en cuenta en futuras versiones.

Capa de abstracción de entorno seguro

Esta capa contiene uno o varios entornos seguros que ofrecen varios servicios de seguridad que proporcionan una protección adecuada para el almacenamiento de datos sensibles y la ejecución de funciones sensibles. Los datos sensibles incluyen las capacidades del entorno seguro (SE), las claves de seguridad, como las claves simétricas a largo plazo y las claves privadas asimétricas, las credenciales locales, las políticas de seguridad, la información sobre la identidad, la información sobre el abono, entre otras. Las funciones sensibles incluyen la encriptación de datos, la desencriptación de datos, etc. Aunque la implementación de entornos seguros está fuera del ámbito de la presente Recomendación, en el Anexo D se proporciona un marco de referencia para interconectar las entidades M2M con las tarjetas de circuito integrado universal (UICC).

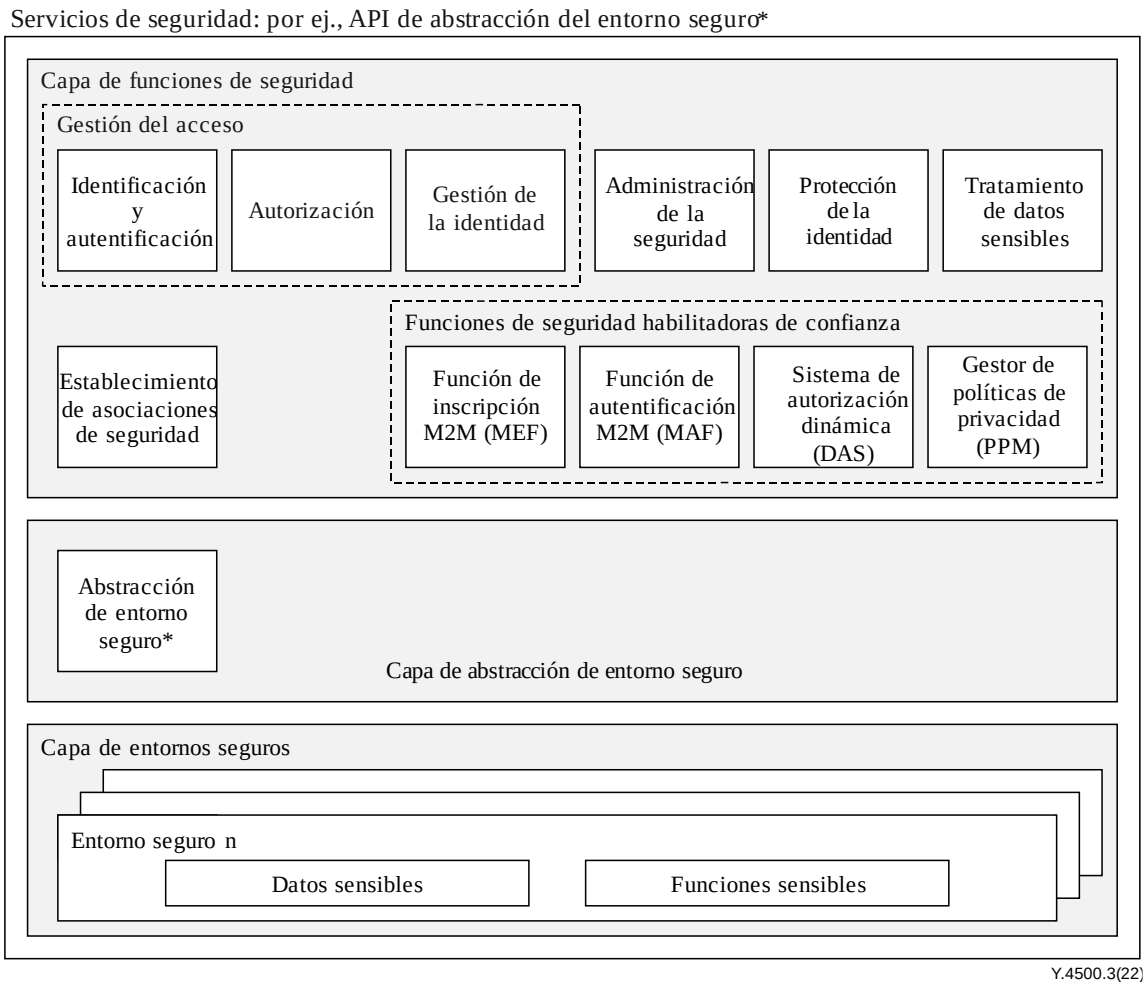


Figura 5.1.0-1 – Visión general de la arquitectura de seguridad

Principios de diseño

Los servicios de seguridad son modulares y configurables en función de las necesidades de la entidad de servicio común (CSE) anfitriona, sus puntos de referencia soportados y su finalidad.

La arquitectura se divide en varios componentes y subcomponentes que ofrecen un diseño modular. Este diseño hace posible la correspondencia de la arquitectura con diferentes nodos y entidades.

En función de los requisitos de cada entidad, la seguridad consta de componentes pertinentes que cumplen los requisitos del respectivo nodo o entidad y el caso de uso previsto.

La arquitectura debe adaptarse para que sea adecuada para su implementación en diferentes entidades. Por ejemplo, la arquitectura puede corresponderse con diferentes clases de dispositivos

El componente de administración de la seguridad debe permitir la administración de todos los recursos sensibles (datos y funciones) y también la configuración y ampliación de los propios servicios de seguridad.

Se accede al entorno seguro dentro de la CSE a través de la capa de abstracción del entorno seguro y está previsto que proporcione un nivel adecuado de protección a la información sensible enumerada en la cláusula 6.2.3.2.

Gestión del acceso

Los siguientes tres componentes forman parte de la capa de gestión del acceso. Se ofrecen más detalles en la cláusula 6.2.

5.1.1 Identificación y autentificación

La función de identificación y autentificación se encarga de la identificación y autentificación mutua de las CSE y las entidades de aplicación (AE).

La identificación es un proceso que permite comprobar si la identidad proporcionada para la autentificación es válida. La forma de realizar un proceso de identificación dependerá del propósito de la autentificación. Por ejemplo, en el caso del acceso a recursos, la función de autentificación puede requerir la identificación para comprobar si la AE o la CSE se ha registrado en la CSE local; en el caso del registro de una AE o CSE, la función de autentificación puede requerir la identificación para comprobar si la identidad proporcionada por una AE o CSE coincide con un certificado. Una vez superado este proceso de comprobación, la AE o CSE es identificada, y la identidad identificada será suministrada al proceso de autentificación.

La autentificación es el proceso que permite determinar si la identidad suministrada en la etapa de identificación está asociada a una credencial de confianza. La forma de realizar un proceso de autentificación dependerá del mecanismo de autentificación mutua que se utilice. Por ejemplo, en el caso de que se utilice un mecanismo de autentificación basado en un certificado, la función de autentificación puede requerir que la autentificación se realice mediante la verificación de una firma digital; si se utiliza un mecanismo de autentificación basado en una clave simétrica, la función de autentificación puede requerir que la autentificación verifique un código de integridad del mensaje (MIC). Una vez que se ha completado este proceso de validación, la AE o la CSE estarán autentificadas.

5.1.2 Autorización

La función de autorización se encarga de autorizar el acceso a los servicios y los datos a las entidades autentificadas de acuerdo con las políticas de control de acceso (ACP) y las funciones asignadas.

La política de control de acceso se define como un conjunto de condiciones que determinan si las entidades pueden tener acceso a un recurso protegido. La función de autorización puede soportar diferentes mecanismos de autorización, como la lista de control de acceso (ACL), el control de acceso basado en funciones (RBAC), etc. La función de autorización podría tener que evaluar múltiples políticas de control de acceso en un proceso de autorización para obtener una decisión final de control de acceso. Este proceso se describe con más detalle en la cláusula 7 Autorización

El proceso de evaluación de la autorización se basa en el recurso de suscripción al servicio, que especifica a qué servicios M2M y funciones de servicio M2M se ha suscrito la entidad autentificada y las políticas de control de acceso asociadas al recurso protegido. El proceso de evaluación de la autorización también puede considerar atributos contextuales como la hora o la ubicación geográfica.

Antes de la autorización, se puede realizar la autentificación mutua entre la CSE o la AE originadora y la CSE anfitriona, tal y como se especifica en la cláusula 8. La cláusula 6.1.2.2.1 describe las condiciones bajo las cuales la autentificación mutua es obligatoria. Una regla de control de acceso también puede incluir un indicador de que la regla de control de acceso se aplica solo cuando la autentificación mutua se ha realizado con éxito y el resultado de la autentificación mutua sigue siendo vigente; véase la cláusula 7.1.3 para más detalles

5.1.3 Gestión de identidades

La función de gestión de identidades proporciona identidades/identificadores oneM2M a la entidad solicitante en caso de que dichas identidades estén almacenadas en el entorno seguro. Los identificadores oneM2M, tal y como se definen en la Arquitectura oneM2M ([UIT-T Y.4500.1]), también pueden tratarse como datos sensibles a los que pueden acceder las AE o las CSE y utilizarse independientemente de las funciones de autentificación

5.2 Capas de seguridad

5.2.1 Capa de funciones de seguridad

Esta capa proporciona los siguientes servicios:

- Gestión del acceso
  - Identificación y autorización.
  - Autentificación.
  - Control de acceso.
- Tratamiento de datos sensibles:
  - Protección de funciones sensibles.
  - Almacenamiento seguro.
    - Funciones de seguridad habilitadoras de confianza:

MEF (función de inscripción M2M).

MAF (función de autentificación M2M).

DAS (sistema de autorización dinámica).

PPM (gestor de políticas de privacidad).

- Establecimiento de una asociación de seguridad

Conexión segura mediante el establecimiento de una sesión segura.

Conexión segura a través de la seguridad de los objetos.

- Administración de la seguridad (incluida la provisión de seguridad a distancia).
- Protección de la identidad.

Cada uno de estos servicios proporciona funciones y recursos en la interfaz de programación de aplicaciones (API) del Servicio de Seguridad y Administración.

5.2.2 Capa de abstracción del entorno seguro

La capa de abstracción del entorno seguro (que no se define en esta Recomendación) proporciona acceso al entorno seguro a través de una API de transporte de seguridad general. Un módulo asociado con el tipo de entorno seguro proporciona la conectividad física/lógica al entorno seguro. La capa de abstracción del entorno seguro también tiene que ser accesible en la capa de servicio

5.3 Integración en la arquitectura general de oneM2M

Los servicios de seguridad están previstos en los siguientes componentes arquitectónicos e interactúan en los diferentes puntos de referencia como se describe en la Recomendación UIT-T Y.4500.1. La Figura 5.3-1 muestra la arquitectura funcional de oneM2M.

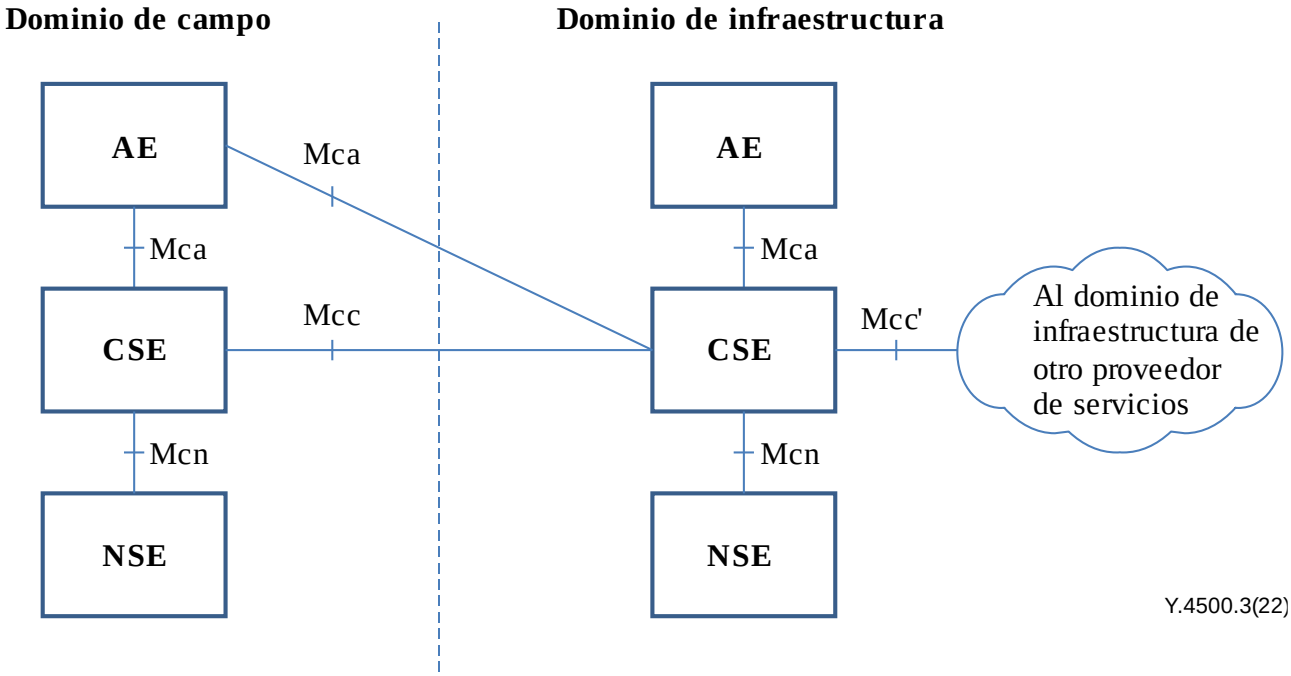


Figura 5.3-1 – Arquitectura funcional de oneM2M

6 Servicios e interacciones de seguridad

6.1 Integración de la seguridad en el flujo de eventos de oneM2M

6.1.1 Interacciones entre capas

Antes de que pueda tener lugar cualquier procedimiento de la capa de servicio común M2M, es preciso establecer la conectividad en la capa de servicio de red subyacente, lo que puede requerir procedimientos independientes de aprovisionamiento y registro de servicios especificados por la red subyacente.

El aprovisionamiento de seguridad de la capa de servicios (preaprovisionamiento de seguridad o inicialización de seguridad) y los procedimientos de establecimiento de asociaciones de seguridad definidos en esta Recomendación pueden tener lugar independientemente (y por lo general, inmediatamente después) de los procedimientos de establecimiento de conectividad de la capa de servicio de red.

Por último, es preciso tener en cuenta los requisitos de provisión de seguridad y de establecimiento de asociaciones de seguridad que imponen los proveedores de servicios de aplicaciones M2M. A nivel de la capa de servicio, el establecimiento de la asociación de seguridad da lugar a una sesión de seguridad de la capa de transporte (TLS) o de seguridad de la capa de transporte de datagramas (DTLS) que protege los mensajes que se intercambian entre la AE/CSE adyacente, es decir, salto a salto. Las AE que necesitan proteger la privacidad de su intercambio de información frente a asociaciones intermedias que no son de confianza, permiten encriptar el contenido de los recursos intercambiados entre las AE a través de la capa de servicio. En algunos supuestos (véase la cláusula 8.2.1), el establecimiento de una asociación de seguridad entre la AE/CSE adyacentes requiere sesiones TLS o DTLS separadas para cada dirección de transmisión, es decir, se puede aprovisionar un par de nodos de asociaciones de seguridad para soportar una asociación de seguridad directa entre ellas. Las interacciones de asociación de seguridad directa entre capas se detallan en la cláusula 8.5.

6.1.2 Visión general de la secuencia de eventos

6.1.2.1 Fase de inscripción

Los equipos M2M suelen requerir fases de aprovisionamiento y configuración antes de su puesta en funcionamiento real. Esto puede realizarse mediante un preaprovisionamiento que puede integrarse en la fase de fabricación o de despliegue del producto, o mediante un procedimiento de inicialización de la seguridad (es decir, una provisión de seguridad a distancia) que tiene lugar antes de que el equipo entre en funcionamiento real.

A nivel de la capa de servicio, este aprovisionamiento y configuración requiere la selección de la parte interesada que prestará servicios a través del equipo, especialmente el proveedor de servicios M2M. Esta fase de inscripción requiere acuerdos entre las partes interesadas.

La fase de inscripción puede producirse varias veces durante el ciclo de vida de un equipo M2M, pero solo se repite cuando un cambio en el proveedor de servicios afecta al aprovisionamiento o la configuración del equipo.

La fase de provisión de seguridad para las diferentes capas puede combinarse utilizando un método común de preaprovisionamiento de seguridad.

Los marcos de provisión de seguridad a distancia (RSPF) prevén el aprovisionamiento posterior de la información esencial para establecer una asociación de seguridad entre una entidad de dominio de campo y la función de autentificación M2M de un determinado proveedor de servicios M2M. La información de seguridad esencial incluye las credenciales e identificadores de seguridad. Los procedimientos de provisión de seguridad a distancia se basan en una función de inscripción M2M que puede ser externa al proveedor de servicios M2M para establecer las credenciales adecuadas.

Marco de provisión de seguridad a distancia con clave simétrica preaprovisionada: Se aprovisiona previamente una clave simétrica al inscrito y a la función de inscripción M2M para la autentificación mutua de estas entidades. Para más detalles, véase la cláusula 8.3.2.1.

Marco de provisión de seguridad a distancia mediante certificados: El inscrito y la función de inscripción M2M se autentifican mutuamente y se emiten claves de firma privadas y certificados que contienen la correspondiente clave de verificación pública. Para más detalles, véase la cláusula 8.3.2.2.

Marco de provisión de seguridad a distancia basado en GBA: Este método de provisión a distancia solo es aplicable a los dispositivos del proyecto de asociación de tercera generación (3GPP).

En este caso, la función de inscripción M2M incluye la funcionalidad de una función de servidor de inicialización GBA. Este marco utiliza claves simétricas 3GPP o del proyecto de asociación de tercera generación 2 (3GPP2) para autentificar al inscrito y la función de inscripción M2M (que también es un GBA BSF). Los detalles se especifican en 3GPP TS 33.220 [ETSI TS 133 220] y 3GPP2 S.S0109-A [TIA-1098-A]. Para más detalles, véase la cláusula 8.3.2.3.

NOTA 1 – El uso de GBA está previsto únicamente en la fase de inscripción. Obtiene una serie de credenciales simétricas que pueden utilizarse para cualquier propósito en la capa de aplicación, no necesariamente para la autentificación. Las especificaciones oneM2M las utilizan después para obtener una serie de credenciales simétricas como insumo Las especificaciones oneM2M las utilizan para obtener una serie de credenciales simétricas como insumo para los protocolos de seguridad para la autenticación y protección de la confidencialidad y la integridad de clave precompartida (PSK), concretamente (D)TLS-PSK y SAEF, ESPrim y ESData basados en PSK, tal como se describe en la cláusula 8.3.2.3.

NOTA 2 – La especificación no soporta la norma TS 33.221 Soporte de certificados de abonado (SSC), ya que, desde la publicación de la norma TS33.221, han aparecido muchas otras formas reconocidas a nivel mundial de implementar certificados en los dispositivos. El sistema oneM2M soporta el protocolo simple de inscripción de certificados (SCEP) en la cláusula 8.3.6.3, procedimientos de suministro de certificados mediante SCEP, y la inscripción en transporte seguro (EST) en la cláusula 8.3.6.2, procedimientos de suministro de certificados mediante EST. Para más detalles, véase la cláusula 8.3.2.3.

La Figura 6.1.2.1-1 ilustra los diferentes marcos de provisión de seguridad a distancia. Nótese que no hay comunicación entre las entidades M2M A y B en el procedimiento de provisión de seguridad a distancia. Una vez completado con éxito el procedimiento de provisión de seguridad a distancia, se aplica un procedimiento de establecimiento de asociación de seguridad.

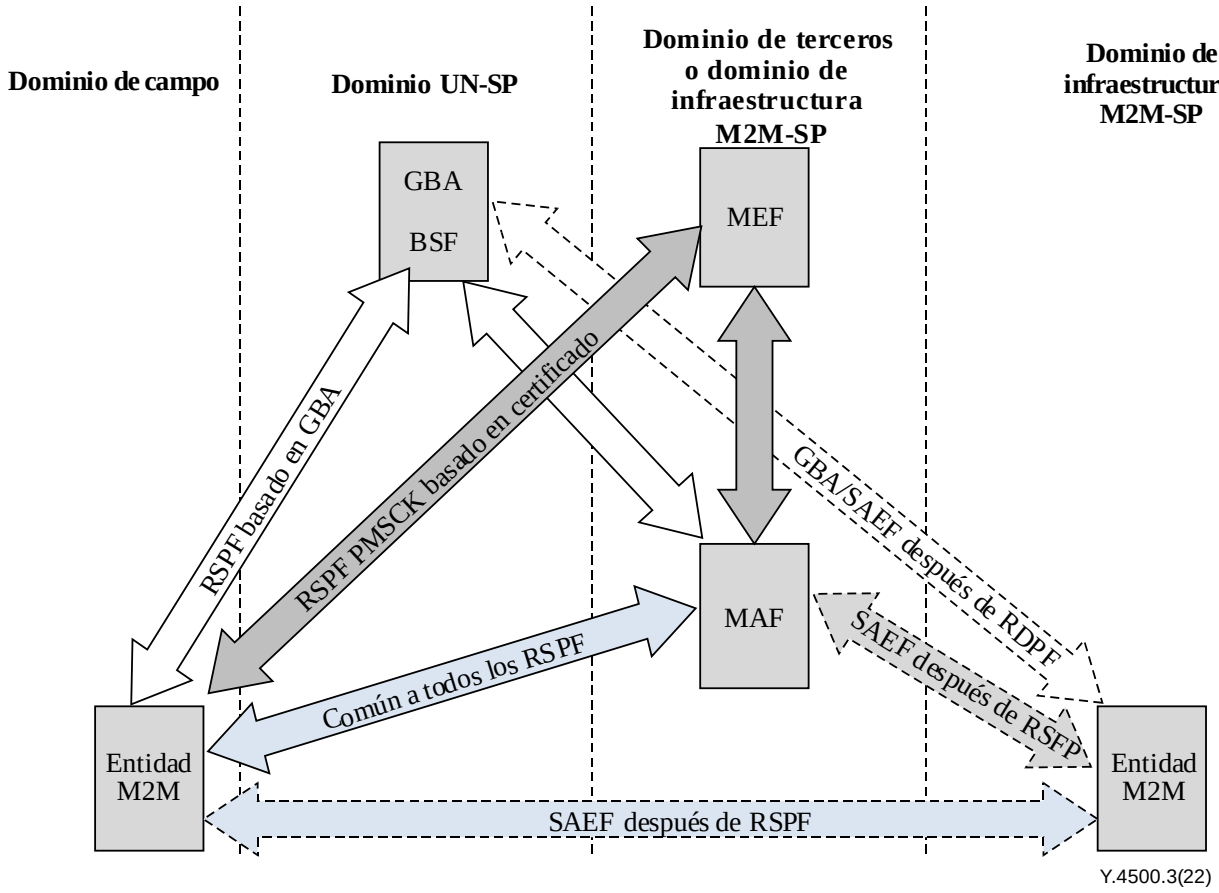


Figura 6.1.2.1-1 – Entidades implicadas en la provisión de seguridad a distancia

6.1.2.2 Fase operativa

6.1.2.2.1 Acceso al servicio M2M

Las CSE ofrecen servicios M2M a las AE y/o a otras CSE. Para poder utilizar los servicios M2M que ofrece una CSE, las AE y/o CSE deben identificarse y autentificarse mutuamente ante esa CSE, con el fin de proporcionar protección contra el acceso no autorizado y los ataques de denegación de servicio (DoS). Esta autentificación mutua permite suministrar una protección adicional de encriptación e integridad para el intercambio de mensajes a través de un único punto de referencia Mca, Mcc o Mcc. Además, se puede aprovisionar a las AE comunicantes que requieren una protección similar para sus propios intercambios de información para que puedan aplicar el mismo método de seguridad a sus comunicaciones.

Este es el objetivo del procedimiento de establecimiento de la asociación de seguridad, que debe ejecutarse antes de los procedimientos relacionados con el servicio especificados en la Recomendación UIT-T Y.4500.1 para el punto de referencia correspondiente.

En los puntos de referencia Mca y Mcc, es obligatorio establecer una asociación de seguridad entre una AE o CSE de dominio de campo, respectivamente, y un IN-CSE.

En el punto de referencia Mcc, es obligatorio establecer una asociación de seguridad entre un IN-CSE y un IN-CSE.

En el punto de referencia Mca, se recomienda firmemente establecer una asociación de seguridad entre la AE y la CSE en el dominio de campo.

NOTA 1 – El establecimiento de la asociación de seguridad en la interfaz Mca en un dominio local es opcional, dependiendo de la evaluación de riesgos, por ejemplo, en los supuestos en los que el acceso no autorizado puede evitarse mediante otras medidas de seguridad no incluidas en el ámbito de esta especificación. Esto incluye los siguientes casos de uso:

La AE y la CSE (es decir, los extremos de la Mca) se integran de forma segura en el mismo dispositivo físico (es decir, un ASN).

La seguridad de la comunicación está garantizada por la red subyacente (por ejemplo, WLAN o VPN).

La comunicación Mca tiene lugar en un cable (por ejemplo, Ethernet) en un entorno físico seguro.

La fase de establecimiento de la asociación de seguridad de la capa de servicio M2M y de la capa de aplicación M2M son generalmente independientes de los procedimientos similares que pueda requerir la capa de red, aunque podrían basarse en los servicios de seguridad proporcionados por la capa de red.

El sistema oneM2M admite los siguientes mecanismos de autentificación para el establecimiento de asociaciones de seguridad, que se describen con más detalle en la cláusula 8.2.1 Presentación de los marcos de establecimiento de asociaciones de seguridad:

Marco de establecimiento de asociaciones de seguridad de clave simétrica aprovisionada: Una clave simétrica se aprovisiona previamente a los extremos de la asociación de seguridad. Para más detalles, véase la cláusula 8.2.2.1.

Marco de establecimiento de asociaciones de seguridad mediante certificado: los extremos de la asociación de seguridad se autentifican a sí mismos utilizando claves de firma privadas y certificados que contienen la correspondiente clave de verificación pública. Para más detalles, véase la cláusula 8.2.2.2

Marco de establecimiento de asociaciones de seguridad basado en la función de autentificación M2M (MAF): Para el SAEF basado en MAF, el servidor de distribución de claves centralizado es una MAF alojada bien por un proveedor de servicios de terceros que tiene una relación de servicio con el proveedor de servicios M2M (M2M-SP), o bien alojada por el propio M2M-SP. La MAF autentifica una entidad de dominio de campo en nombre de un IN-CSE utilizando una clave simétrica. Para más detalles, véase la cláusula 8.2.2.3.

NOTA 2 – El uso de la GBA está previsto únicamente en la fase de inscripción. Obtiene una serie de credenciales simétricas que pueden ser utilizadas para cualquier propósito en la capa de aplicación, no necesariamente para la autentificación. Las especificaciones oneM2M las utilizan para luego obtener una serie de credenciales simétricas como insumo para los protocolos de seguridad para la autentificación y protección de la confidencialidad y la integridad de clave precompartida (PSK), en concreto (D)TLS-PSK y SAEF, ESPrim y ESData basados en PSK, como se establece en la cláusula 8.3.2.3.

La Figura 6.1.2.2.1-1 ilustra los diferentes casos de uso y las entidades implicadas en los distintos marcos de establecimiento de asociaciones de seguridad (SAEF) contemplados en esta Recomendación.

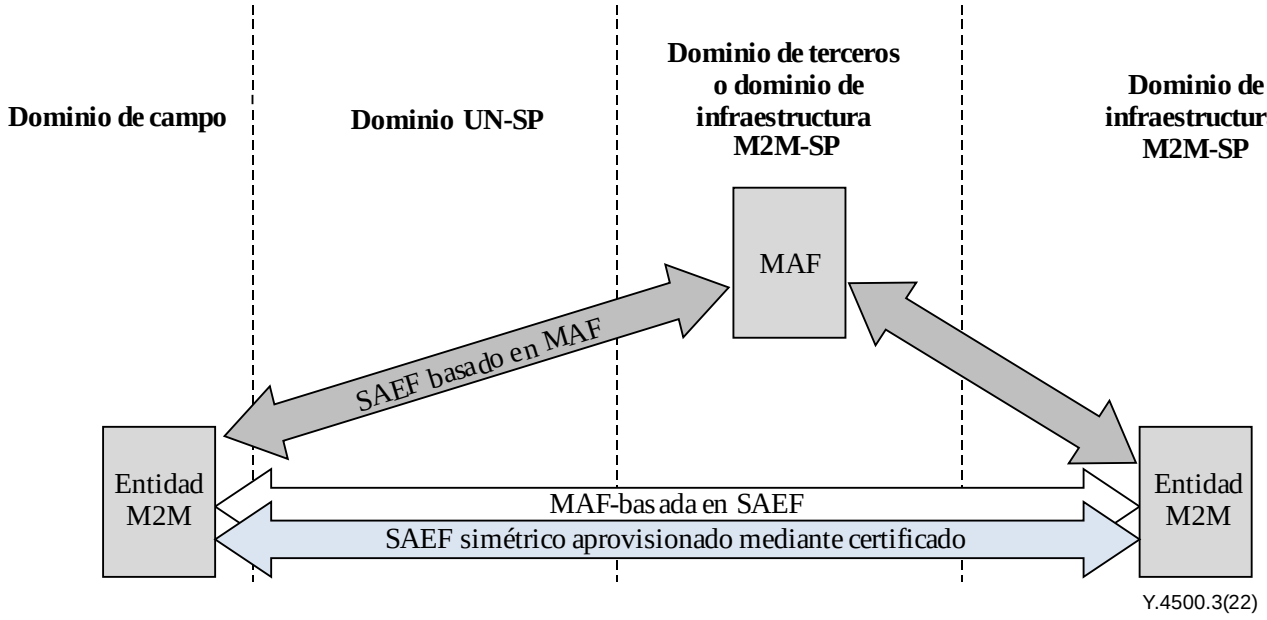


Figura 6.1.2.2.1-1 – Entidades implicadas en el establecimiento de asociaciones de seguridad

6.1.2.2.2 Autorización de acceso a los recursos M2M

Una vez que se ha concedido a una AE o a una CSE el acceso a los servicios M2M, se ejecuta el procedimiento de decisión de control de acceso especificado en la cláusula 7.1.5 de esta Recomendación antes de acceder a un recurso M2M, tal como se especifica en la Recomendación UIT-T Y.4500.1.

6.2 Capa de funciones de seguridad

6.2.1 Gestión del acceso

Este componente proporciona servicios de autentificación a la capa de aplicación. En el Anexo B se ofrece una descripción general de los mecanismos de autentificación. Los esquemas de autentificación mutua oneM2M permiten a las entidades oneM2M demostrar que conocen credenciales afines, como las credenciales maestras, sin tener que intercambiar el valor de dichas credenciales, y datos sensibles como las identidades de seguridad y los identificadores de seguridad. Para evitar la lectura y la copia de credenciales, un entorno seguro dentro del CSF de seguridad proporciona protección contra cualquier manipulación de dichas credenciales y de la información procesada conexa

6.2.1.1 Consideraciones para el almacenamiento de claves a largo plazo

Las claves de conexión segura aprovisionadas a largo plazo pueden suponer un riesgo para la seguridad si no se protegen adecuadamente, y por esta razón se recomienda que las claves de conexión segura aprovisionadas a largo plazo se almacenen en entornos seguros.

Las claves simétricas de conexión aprovisionadas a largo plazo pueden suponer un riesgo para la seguridad si no se protegen adecuadamente, y por esta razón se recomienda que las claves simétricas de conexión aprovisionadas a largo plazo se almacenen en entornos seguros.

Dado que, por definición, habrá una amplia gama de dispositivos que no se basan en el protocolo 3GPP con muchas implementaciones diferentes. Como es poco probable que se normalicen, esto no entra en el ámbito de oneM2M o de 3GPP. Sin embargo, se pueden consultar las guías de mejores prácticas de seguridad en [b-ETSI TS 103 645], [b-IoTSF SD-BP] y [b-GSMA IoT-SGA].

6.2.2 Autorización

La Figura 6.2.2-1 proporciona una visión general de alto nivel de una función de autorización genérica. Esta arquitectura comprende cuatro subcomponentes que se describen a continuación:

Punto de imposición de políticas (PEP):

El PEP intercepta las solicitudes de acceso a los recursos, realiza las solicitudes de decisión de control de acceso y aplica las decisiones de control de acceso. El PEP coexiste con la entidad que necesita servicios de autorización.

Punto de decisión de políticas (PDP):

El PDP interactúa con el punto de recuperación de políticas (PRP) y el punto de información de políticas (PIP) para obtener las políticas de autorización aplicables y los atributos necesarios para evaluar las políticas de autorización, respectivamente, y luego evalúa la solicitud de acceso utilizando las políticas de autorización para tomar una decisión de control de acceso. El PIP se encuentra en el servicio de autorización.

Punto de recuperación de políticas (PRP):

El PRP obtiene las políticas de autorización aplicables según una solicitud de decisión de control de acceso. Estas políticas aplicables deben combinarse para obtener una decisión final de control de acceso. El PRP se encuentra en el servicio de autorización.

Punto de información de políticas (PIP):

El PIP proporciona los atributos necesarios para evaluar las políticas de autorización, por ejemplo, la dirección IP del solicitante, la hora de creación del recurso, la hora actual o la información sobre la ubicación del solicitante. El PIP se encuentra en el servicio de autorización.

El servicio de autorización puede incluir cualquiera de los subcomponentes: PDP, PRP y/o PIP. Esto significa que los subcomponentes PEP, PRP, PDP y PIP pueden estar distribuidos en diferentes nodos. Por ejemplo, el PEP se encuentra en un ASN/MN y el PDP en el IN.

La presente versión no soporta la separación de PRP y PIP en diferentes CSE de PDP. El procedimiento genérico que se describe a continuación se proporciona a título informativo y para soportar futuras extensiones, mientras que la cláusula 7 proporciona los detalles de los mecanismos de autorización en la versión actual.

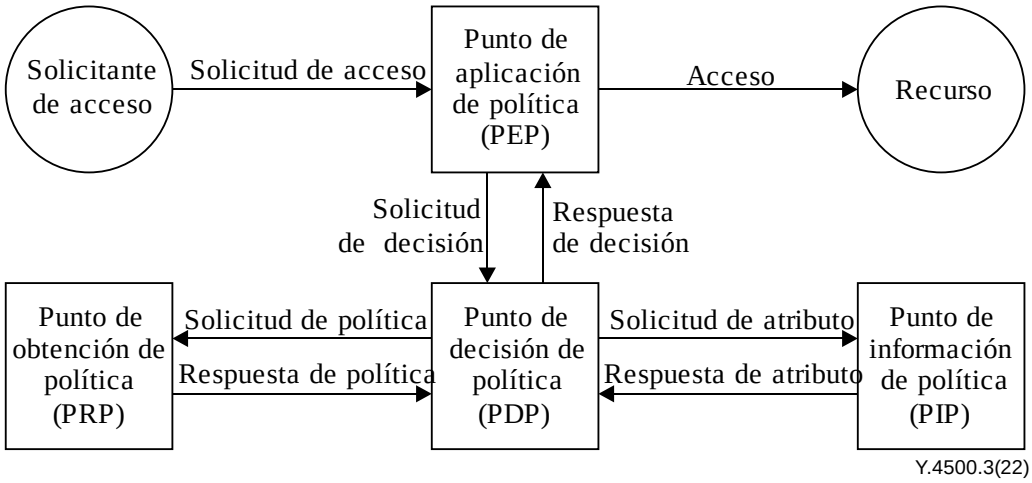


Figura 6.2.2-1 – Visión general de la función de autorización

El procedimiento genérico de autorización se muestra en la Figura 6.2.2-2.

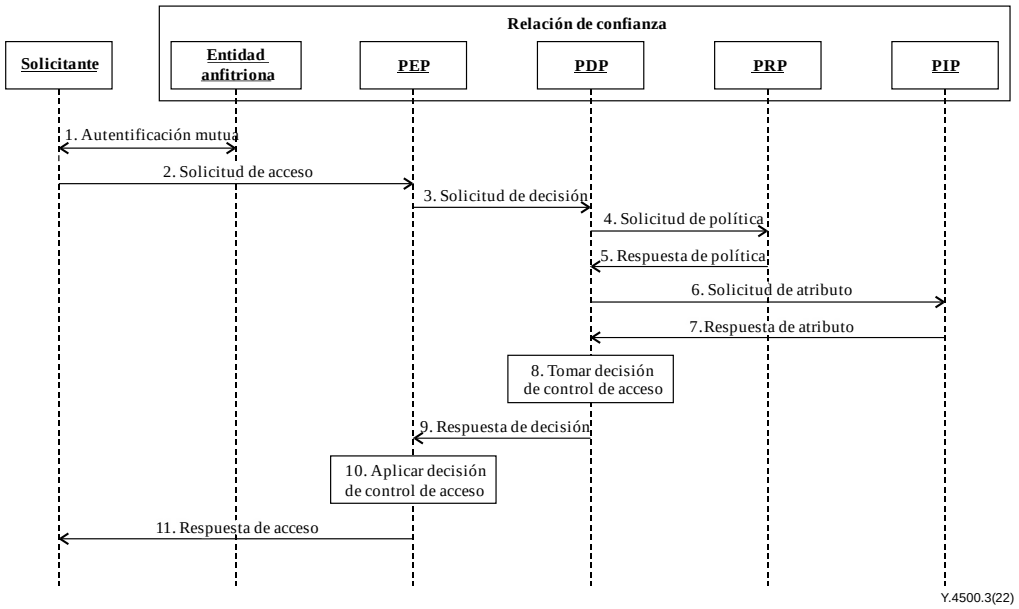


Figura 6.2.2-2 – Procedimiento de autorización

Etapa 001: Autentificación mutua (prerrequisito).

Etapa 002: El solicitante de acceso envía una solicitud de acceso al PEP.

Etapa 003: El PEP realiza una solicitud de decisión de control de acceso de acuerdo con la solicitud de acceso del solicitante, y envía la solicitud de decisión de control de acceso al PDP.`mj

Etapa 004: El PDP envía una solicitud de política de control de acceso que se genera en base a la solicitud de decisión de control de acceso al PRP.

Etapa 005: El PRP encuentra todas las políticas de control de acceso aplicables a la solicitud de acceso y las devuelve al PDP. Cuando intervienen varias políticas de control de acceso, el PRP también proporciona un algoritmo de combinación de políticas que permite combinar los resultados de las diferentes evaluaciones en un resultado final

Etapa 006 El PDP envía una solicitud de atributos al PIP si se requieren atributos para evaluar estas políticas de control de acceso.

Etapa 007: El PIP obtiene los atributos requeridos y los devuelve al PDP.

Etapa 008: El PDP evalúa la solicitud de acceso utilizando las políticas de control de acceso. Cuando se aplican varias políticas de control de acceso, el PEP debe calcular una decisión final de control de acceso utilizando el algoritmo de combinación de políticas.

Etapa 009: El PDP devuelve la decisión de control de acceso al PEP.

Etapa 010: El PEP ejecuta la decisión de control de acceso, es decir, reenvía la solicitud de acceso al recurso o deniega dicho acceso.

Etapa 011: El PEP devuelve el resultado del acceso al solicitante.

6.2.3 Administración de la seguridad

6.2.3.0 Introducción

El servicio de administración de seguridad ofrece capacidad para gestionar las funciones, recursos y atributos de seguridad. Esto incluye la gestión de los recursos proporcionados a través del entorno seguro. Además, puede ofrecer funciones para gestionar datos sensibles con sus identificadores asociados y abonos en nombre de otras entidades. La administración de la seguridad depende, por tanto, del tipo de entorno seguro que se utilice (módulo de hardware independiente, entorno de ejecución de confianza integrado o protección de software). Dependiendo del tipo de entorno seguro, se pueden utilizar distintas normas existentes para la administración a distancia de esos entornos seguros.

6.2.3.1 Preaprovisionamiento de seguridad del entorno seguro

Varios datos sensibles y objetos asociados son a menudo configurados mediante el preaprovisionamiento de un entorno seguro (ver cláusula 6.3.1 Entorno seguro) antes de desplegar el dispositivo M2M al que está relacionado.

Las UICC especificadas en [ETSI TS 102 671] y [ETSI TS 102 221] se suelen utilizar con este fin porque son necesarias para acceder a algunas redes subyacentes, proporcionan un alto nivel de seguridad y ofrecen una interfaz de transporte interoperable especificada en [ETSI TS 102 221]. El preaprovisionamiento oneM2M basado en UICC deberá seguir el marco especificado en el anexo D para garantizar la interoperabilidad

6.2.3.2 Administración de seguridad a distancia del entorno seguro

Los datos y funciones sensibles para la seguridad que están protegidos y aislados dentro del entorno seguro (SE) pueden permanecer accesibles a distancia para los administradores de seguridad legítimos después del despliegue. A diferencia de la gestión ordinaria de los dispositivos, la administración de seguridad a distancia presupone el establecimiento de un canal seguro entre el servidor de administración y el entorno seguro del nodo M2M (es decir, que el secreto utilizado para asegurar la conexión no está disponible en el nodo M2M fuera del entorno seguro). Los protocolos de administración de seguridad a distancia aplicables dependen del nivel de riesgo de cada aplicación M2M y no solo de las tecnologías de red subyacentes. Las tecnologías de uso generalizado que posibilitan la administración de seguridad a distancia para los diferentes niveles de seguridad distinguidos en oneM2M TR 0008 [b-oneM2M TR0008] se examinan en el Anexo C.

Dado que la administración de seguridad a distancia requiere que la información sensible de destino pueda modificarse a distancia, la protección de dicha información sensible frente a la piratería informática a distancia del dispositivo es especialmente importante. Si el entorno seguro se basa únicamente en la protección por software, la administración de seguridad a distancia de los siguientes datos debe permitirse únicamente cuando pueda mitigarse el acceso a distancia por posibles atacantes:

Clave privada e identificadores asociados.

Clave simétrica compartida a largo plazo (frente a la vida útil prevista del nodo M2M) e identificadores asociados.

Cualquier proceso y sus parámetros que manipule la información anterior, es decir, las funciones de seguridad.

6.2.4 Protección de la identidad

La protección de la identidad presta servicios a la capa de aplicación, como los seudónimos y la protección del anonimato de las transacciones.

6.2.5 Tratamiento de datos sensibles

6.2.5.0 Introducción

El servicio de tratamiento de datos sensibles ofrece ciertas funciones sensibles a la capa de aplicación. Entre las funciones sensibles destacan las siguientes:

Almacenamiento seguro.

Operaciones criptográficas.

Métodos para la inicialización de secretos (por ejemplo, GBA).

6.2.5.1 Funciones sensibles

Este servicio proporciona a las AE y CSE acceso a las funciones sensibles del entorno seguro

6.2.5.2 Almacenamiento seguro

Este servicio proporciona a las AE y CSE acceso a la capacidad de almacenamiento seguro del SE. Los datos almacenados de forma segura por la AE o CSE están previstos para ser accesibles solo a través de la API de seguridad y por entidades autorizadas. El almacenamiento seguro debe ser gestionado por el entorno seguro. Se prevé que los datos almacenados de forma segura permanezcan bajo el control de la parte interesada propietaria de los datos, es decir, la entidad que solicitó que los datos se guardaran en el almacenamiento seguro, independientemente de otras partes interesadas.

6.2.6 Funciones de seguridad habilitadoras de confianza

La arquitectura habilitadora de confianza oneM2M puede requerir la existencia de funcionalidades de seguridad dentro del dominio de la infraestructura: una función de autentificación M2M (MAF) y una función de inscripción M2M (MEF), ambas consideradas como funciones habilitadoras de confianza (TEF) y que sirven para la autentificación y la seguridad de extremo a extremo, así como un sistema de autorización dinámica (DAS) o autoridades de función con fines de autorización. La función de autentificación M2M y las funciones de inscripción M2M incorporarán la capacidad de proporcionar el registro y el aprovisionamiento de credenciales de extremo a extremo. Además, se puede implementar una funcionalidad de gestor de políticas de privacidad (PPM) para proteger la privacidad del usuario. Todas estas funciones pueden estar bajo el control del proveedor de servicios M2M o delegarse en un habilitador de confianza M2M (es decir, una parte en la que confíen todas las partes interesadas del ecosistema M2M).

Función de inscripción M2M (MEF):

La MEF se utiliza durante la fase de inscripción y apoya el procedimiento de inicialización de la seguridad que permite aprovisionar las credenciales maestras que se utilizarán para autentificar mutuamente a las entidades que acceden a la infraestructura de un proveedor de servicios M2M. La MEF se basa en una credencial inicial preaprovisionada en el nodo M2M (por ejemplo, durante la fabricación).

Las credenciales aprovisionadas por una MEF pueden utilizarse para la autentificación con una función de autentificación M2M en el marco de establecimiento de una asociación de seguridad (SAEF) basada en MAF, la seguridad de las primitivas de extremo a extremo (ESPrim) o la seguridad de los datos de extremo a extremo (ESData). Alternativamente, las credenciales suministradas pueden utilizarse directamente en el SAEF, ESPrim o ESData.

La función de autentificación M2M (MAF), utilizada durante la fase operativa de los servicios M2M:

Las credenciales maestras utilizadas para autentificar mutuamente a las CSE/AE durante la fase operativa se almacenan de forma segura en una funcionalidad específica de la infraestructura denominada función de autentificación M2M (MAF).

La MAF contiene de forma segura el conjunto de credenciales maestras que se utilizan para autentificar a las CSE/AE que se han inscrito a través del SP M2M o del habilitador de confianza M2M. La MAF almacena las credenciales maestras y posiblemente los identificadores de la CSE/AE asociada.

Una única MAF puede soportar todos los servicios de seguridad de las comunicaciones (SAEF, ESPrim y ESData) o solo algunos de ellos. Una MAF que proporciona SAEF basado en MAF es operada por el SP M2M, o por un habilitador de confianza M2M en nombre del SP M2M. Otras MAF pueden ser operadas por el habilitador de confianza M2M o por el SP M2M, y en esos casos no se presupone la existencia de una relación de confianza entre el habilitador de confianza M2M y el SP M2M en esos casos.

La MAF también se encarga de todas las operaciones de seguridad que implican el uso de las credenciales maestras.

Servidor del sistema dinámico de autorización (DAS) y autoridades de función: Estas funcionalidades gestionan los privilegios de autorización de acceso a los recursos que pueden ser asignados durante la operación y se describen en las cláusulas 7.3 y 7.4, respectivamente.

Gestor de políticas de privacidad (PPM). Esta funcionalidad ayuda a la gestión de las preferencias de privacidad expresadas por el sujeto de los datos con respecto a los requisitos del servicio y la normativa aplicable, y se describe en la cláusula 11.

6.3 Entorno seguro y abstracción del entorno seguro

6.3.1 Entorno seguro

El entorno seguro es una entidad lógica que proporciona funciones sensibles que operan con datos sensibles, almacenamiento seguro y otros recursos/funciones.

Se prevé la protección de los datos sensibles de seguridad y las funciones de seguridad contenidas en los nodos del dominio de campo M2M de cualquier acceso no autorizado o alteración, según lo determinado por el análisis de riesgo. Los datos y funciones sensibles incluyen las credenciales de seguridad y los algoritmos que los gestionan. El propósito de un entorno seguro es proporcionar el nivel de protección requerido (véase el Cuadro 6.3.1-1) a los datos sensibles durante su almacenamiento y uso, incluido, en particular cualquier secreto criptográfico simétrico o asimétrico a largo plazo utilizado durante la operación. Además, el aislamiento de los datos sensibles para la seguridad y las funciones controladas por diferentes partes interesadas dentro de un nodo M2M puede garantizarse mediante entornos seguros distintos. Esto es especialmente fundamental para los nodos M2M a los que los posibles atacantes pueden acceder a distancia o físicamente.

La elección de un entorno seguro se basa en un análisis de riesgos que tiene en cuenta todas las capas de una aplicación M2M, aunque debería aprovechar, en la medida de lo posible, las capacidades proporcionadas por la capa de servicio M2M o la red subyacente, por ejemplo, la tarjeta de circuito integrado universal (UICC) en las redes 3GPP y 3GPP2, o los requisitos del entorno de ejecución de confianza.

No se presupone ninguna implementación particular del entorno seguro. Un entorno seguro puede implementarse como elemento de seguridad independiente de hardware o como una función de software integrada. Cada entorno seguro puede relacionarse con un determinado nivel de seguridad dependiendo de la implementación particular del entorno seguro. Diferentes entornos seguros proporcionan diferentes niveles de seguridad y de protección como se indica en el Cuadro 6.3.1-1.

Cuadro 6.3.1-1 – Clasificación de los niveles de protección

Nivel de protección	Descripción
0	Sin protección. Los datos están expuestos incluso sin ataques activos.
1	Protección baja: los datos están protegidos de los observadores pasivos, aunque podrían quedar expuestos a ataques activos, ya sean locales o a distancia. Por ejemplo, hay soluciones de software que se basan en hardware de equipos auxiliares de procesamiento de uso general.
2	Protección media que asegura la protección de los datos frente a los ataques a distancia, pero siguen siendo posibles los ataques locales, especialmente los físicos; es decir, la protección media prevé contramedidas únicamente frente a los ataques de software Por ejemplo, las soluciones de software para proteger los datos y las funciones sensibles se basan en un procesamiento específico que ofrece un aislamiento reforzado y permite mantener el código y los datos sensibles alejados de un entorno operativo, un software y una memoria desprotegidos. El código que se ejecuta en el entorno protegido se verifica criptográficamente para garantizar la integridad.
3	Nivel elevado de protección que permite hacer frente a los ataques a distancia y locales para acceder a los datos, incluidos los ataques que implican un acceso físico. Esto incluye sólidas contramedidas frente a los ataques de software y hardware, como la detección de condiciones de funcionamiento anormales y la aleatorización, además del enmascaramiento por hardware de la memoria y el análisis de los canales paralelos de las operaciones que contienen datos sensibles.

El objetivo es que haya al menos un entorno seguro en cada nodo M2M que ofrezca un almacenamiento seguro a las CSE y AE locales, aunque podría haber varios.

6.3.2 Módulo del entorno seguro

El módulo del entorno seguro permite el acceso físico al entorno seguro (SE) correspondiente. Dependiendo del tipo de entorno seguro, el módulo del SE puede implementarse de forma diferente según el entorno seguro de que se trate.

NOTA – La especificación del módulo SE no está incluida en el ámbito de aplicación de esta Recomendación.

6.3.3 Abstracción del entorno seguro

No se define en la presente Recomendación.

7 Autorización

7.1 Mecanismo de control de acceso

7.1.1 Descripción general

El procedimiento de autorización M2M controla el acceso a los recursos y servicios alojados por las CSE y AE. El procedimiento de autorización exige que el originador del mensaje de solicitud de acceso a un recurso se haya identificado ante la función de autentificación, y que el originador y el receptor se hayan autentificado mutuamente.

El recurso al que se dirige un mensaje de solicitud tiene un atributo a*ccessControlPolicyIDs* asociado (incluido explícitamente como atributo del recurso al que se dirige el mensaje de solicitud, implícito desde el progenitor del recurso, o fijado por el sistema, véase la cláusula 9.6.1 de la Recomendación UIT-T Y.4500.1. El atributo *accessControlPolicyIDs* contiene una lista de identificadores de recursos <*accessControlPolicy*> aplicables al recurso al que se dirige el mensaje de solicitud.

La estructura general de los recursos <*accessControlPolicy*> se describe en la cláusula 9.6.2 Tipo de recurso accessControlPolicy de la Recomendación UIT-T Y.4500.1.

Cada uno de estos recursos <*accessControlPolicy*> incluye los atributos *privileges* y *selfPrivileges*, que incluyen la información, que en la presente Recomendación se denominan reglas de control de acceso, que se evalúa en función de los parámetros asociados con el mensaje de solicitud a fin de obtener la decisión de acceso.

La Figura 7.1.1-1 ilustra la relación entre las instancias de recursos <a*ccessControlPolicy*> (ACP) y las instancias de los recursos protegidos, denominados Resource_1 to Resource_N.

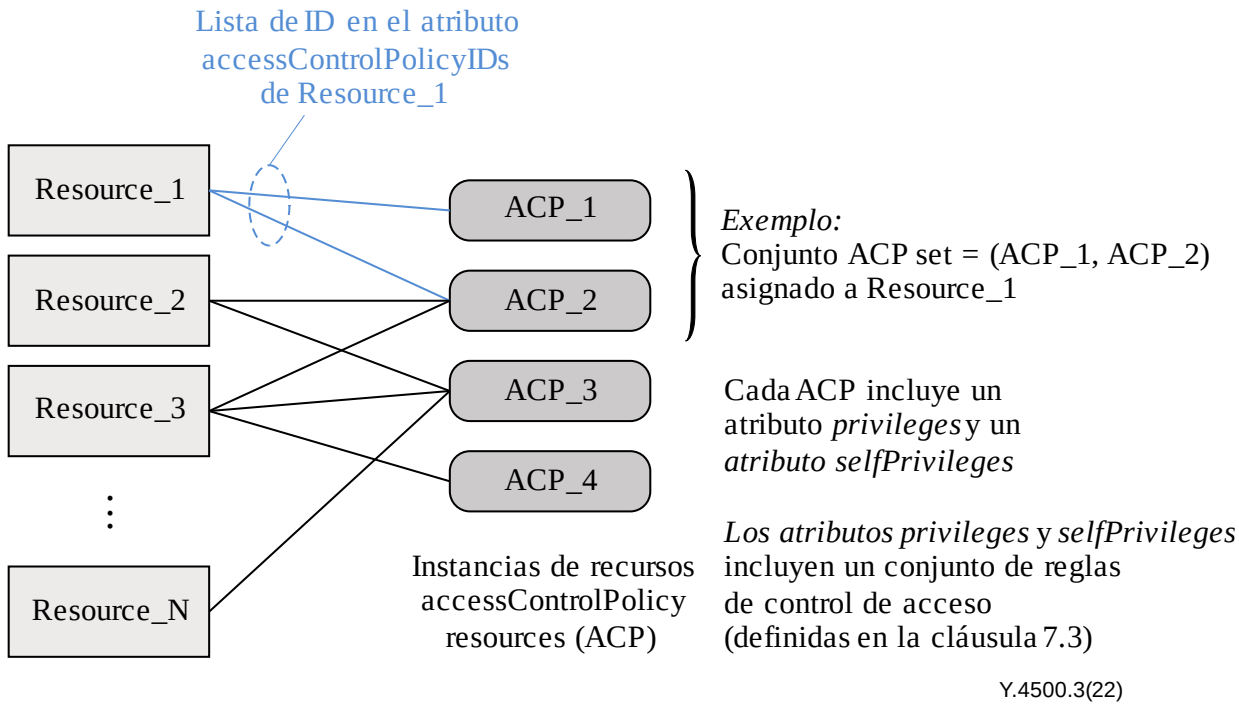


Figura 7.1.1-1 – Relación entre instancias de recursos y políticas de control de acceso

Las solicitudes de acceso a la propia ACP se evalúan en función del atributo *selfPrivileges* de esa ACP. Las solicitudes de acceso a instancias de todos los demás tipos de recursos se evalúan en función de los atributos *privileges* del conjunto de ACP asociado con el recurso de destino.

Si se trata de solicitudes relativas al tipo de recurso <*accessControlPolicy*>, la autorización se concede si la solicitud se evalúa hasta Permit(permiso) para al menos un atributo *selfPrivileges*. En cuanto a los otros tipos de recursos, la autorización se concede si la solicitud se evalúa hasta Permit para al menos un atributo de *privileges*.

Los *privileges* y *selfPrivilege*s definidos en el recurso a*ccessControlPolicy* determinan *a qué originador de la solicitud* se le permite el acceso al recurso que contiene este atributo, *para qué operación específica* (es decir, crear, recuperar, actualizar, eliminar, etc.) y *para qué restricciones de contexto específicas* (es decir, restricciones relativas al tiempo de acceso, la dirección IP del originador y su ubicación).

El método de control de acceso que se define aquí se ajusta al concepto de control de acceso por atributos (ABAC) descrito en [b-NIST 800-162].

Las políticas definidas en los recursos <*accessControlPolicy*> son ejecutadas por un mecanismo de control de acceso que emplea la arquitectura lógica de autorización descrita en la cláusula 6.2.2.

El mecanismo de control de acceso reúne la información necesaria para tomar la decisión de acceso que consiste en:

– Información incluida en el mensaje de solicitud de acceso al recurso, tal como se define en la cláusula 7.1.2 (Cuadro 7.1.2 1).
– La información contextual definida en la cláusula 7.1.2 (Cuadro 7.1.2-2).
– Los testigos (si los hay) asociados con la solicitud de acceso al recurso.
– Las políticas que rigen el acceso, definidas en la cláusula 7.1.3.

7.1.2 Parámetros del mensaje de solicitud

Esta cláusula determina los parámetros de un mensaje de solicitud que son evaluados por el mecanismo de control de acceso.

Los tipos de datos aplicables a estos parámetros se definen en la cláusula 6.4 de la Recomendación UIT-T Y.4500.4.

Los parámetros se enumeran en el Cuadro 7.1.2-1.

Cuadro 7.1.2-1 – Parámetros indicados en el mensaje de solicitud

Parámetro	Descripción	Obligatorio/ opcional	Utilización en el mecanismo de control de acceso
A	URI del recurso de destino	Obligatorio	Selección de *accessControlPolicy* asociada al recurso de destino
De	Identificador que representa al originador de la solicitud	Obligatorio (Nota 1)	Evaluado en función de accessControlOriginators en los atributos *privileges* y *selfPrivileges*
ID de función	Identificadores de función (Role IDs) del originador	Opcional	Evaluado en función de accessControlOriginators en los atributos *privileges* y *selfPrivileges*
Operación	Operación solicitada	Obligatorio	Evaluado en función de accessControlOriginators en los atributos *privileges* y *selfPrivileges*
Tipo de recurso	Tipo de recurso de destino	Opcional (Nota 2)	Evaluado en función de accessControlObjectDetails en los atributos *privileges*. Solo se aplica a las operaciones Create (crear).
Criterios de filtrado	Etiqueta de condición ***filterUsage*** en los criterios de filtrado	Opcional	Diferenciación entre las operaciones Retrieve (recuperar) y Discovery (descubrimiento)
Testigos	Testigos protegidos por ESData	Opcional	Contiene información de autorización (por ejemplo, identificadores de función) que se utilizará en la decisión relativa a la solicitud
ID de testigos	Identificadores de testigo (Token IDs) o Identificadores de testigo locales (Local-Token-ID)	Opcional	Identifica a los testigos que contienen información de autorización (por ejemplo, identificadores de función (role-ID)) que se utilizarán en la decisión relativa a la solicitud
NOTA 1: El parámetro de la primitiva ***From*** es obligatorio en todas las solicitudes, excepto en el procedimiento de registro de AE, en el que es opcional, como se especifica en la Recomendación UIT-T Y. 4500.1. NOTA 2: El parámetro de la primitiva ***resource Type*** de recurso está presente solo en las primitivas de solicitud Create.			

El Cuadro 7.1.2-2 enumera los parámetros de contexto asociados con un mensaje de solicitud que son evaluados por el mecanismo de control de acceso. Estos parámetros no se incluyen explícitamente en un mensaje de solicitud, pero pueden obtenerse en el receptor y validarse en función de los parámetros de la política de contexto, como se indica en el Cuadro 7.1.2-2.

Cuadro 7.1.2-2 – Parámetros de contexto asociados con un mensaje de solicitud

Parámetro	Descripción	Utilización en el mecanismo de control de acceso
rq_time	Sello de hora en que se recibió el mensaje de solicitud en la CSE anfitriona. Obtenida por el reloj del sistema de la CSE anfitriona.	Se valida en función del parámetro accessControlTimeWindow de una regla de control de acceso, véase la cláusula 7.1.3
rq_loc	Información sobre la ubicación del originador de la solicitud. Obtenida a través del punto de referencia Mcn.	Se valida con respecto al parámetro accessControlLocationRegion de una regla de control de acceso, véase la cláusula 7.1.3
rq_ip	Dirección IP de origen asociada a los paquetes IP que llevan el mensaje de solicitud. Obtenida a través del punto de referencia Mcn.	Se valida con respecto al parámetro accessControlIpAddress en una regla de control de acceso, véase la cláusula 7.1.3

Los testigos, definidos en la cláusula 7.3.3.1 Estructura de los testigos, pueden estar asociados con un mensaje de solicitud. Un testigo puede asociarse con una solicitud al estar incluido en el parámetro primitivo ***Tokens*** del mensaje de solicitud o al estar identificado en el parámetro primitivo ***Token IDs*** del mensaje de solicitud. Si la CSE anfitriona ha obtenido un testigo del servidor del sistema de autorización dinámica (DAS) utilizando la autorización dinámica directa, este testigo se asociará a una solicitud si el parámetro del titular del testigo coincide con el AE-ID o CSE-ID absoluto del originador de la solicitud. La autorización dinámica se especifica en la cláusula 7.3.

Cuadro 7.1.2-3 – Parámetros de contexto de seguridad asociados con un mensaje de solicitud

Parámetro	Descripción	Obligatorio/ opcional	Uso en el mecanismo de control de acceso
rq_authn	Valor booleano, TRUE/FALSE (VERDADERO/FALSO), que determina si se considera que el originador ha sido autentificado por la CSE anfitriona, y el parámetro ***From c***oincide con la identidad autentificada del originador.	Obligatorio	Validado con respecto al parámetro accessControlAuthenticationFlag en una regla de control de acceso, véase la cláusula 7.1.3

Se aplicarán los siguientes criterios para determinar si se considera que un originador ha sido autentificado por la CSE anfitriona.

Si el originador es una AE registrada ante la CSE anfitriona, los criterios para decidir si el originador se considera autentificado dependen del despliegue y/o de la implementación y de la confianza garantizada por la materialización física y lógica del dispositivo sobre el terreno que lleva la AE y la CSE anfitriona (por ejemplo, una inicialización segura y una resistencia a la manipulación). En muchos casos, es conveniente esperar que se utilice un canal seguro que implique una autentificación (por ejemplo, una sesión TLS o DTLS) para proteger las primitivas en la interfaz Mca, en cuyo caso la autentificación se considerará válida mientras dure la sesión TLS. Cuando este no sea el caso, por

ejemplo, porque el diseño físico y lógico es de confianza, la autentificación será considerada permanentemente válida a menos que se detecte que el dispositivo está en peligro.
Si el originador es una CSE registrada ante la CSE anfitriona, el originador se considerará autentificado mientras dure una sesión (D)TLS, ya que el Mcc siempre estará protegido por TLS o DTLS conforme a un marco de establecimiento de asociaciones de seguridad (SAEF), como se explica en la cláusula 8.2. La otra CSE puede ser el registrador o el registrado con respecto a la CSE anfitriona.

Si el originador es una AE o una CSE registrada ante una CSE distinta de la CSE anfitriona, el originador se considerará autentificado por la CSE anfitriona siempre y cuando la primitiva de solicitud esté protegida mediante la seguridad de primitivas de extremo a extremo (ESPrim), tal como se describe en la cláusula 8.4.

7.1.3 Formato de los atributos *privileges* y s*elfPrivileges*

Los atributos *privileges* y s*elfPrivilege*s presentan el mismo formato de tipo de datos que se indica a continuación.

Cada atributo *privileges* o s*elfPrivileges* comprende un conjunto de reglas de control de acceso. A continuación, el conjunto de reglas de control de acceso se denomina *acrs* y una regla de control de acceso individual de este conjunto se denomina a*cr*. Las reglas de control de acceso en *acrs* se indexan con la letra *k.* El número de reglas de control de acceso en el conjunto se indica con la letra K:

acrs = { *acr*(1), *acr*(2), ..., *acr*(*k*), ..., *acr*(K) }

Cada regla de control de acceso *acr(k*) está formada por tres tipos de componentes, denominados accessControlOriginators, accessControlOperations y accessControlContexts. El componente accessControlContext es un parámetro opcional.

Así, una regla de control de acceso *acr(k)* se representa como un par:

*acr(k) = {acr(k)*_accessControlOriginators, *acr(k)*_accessControlOperations}

o como tupla de 3:

*acr(k) = {acr(k)*_accessControlOriginators, *acr(k)*_accessControlOperations, acr(k)_accessControlContexts}

El término genérico access-control-rule-tuple se utiliza para referirse a una regla *acr*(*k*).

Un conjunto de reglas de control de acceso *acrs* puede constar de una mezcla de pares y de tuplas triples. En el caso de los pares, se admite cualquier parámetro de contexto asociado a un mensaje de solicitud.

Los tres parámetros que componen una access-control-rule-tuple admitidos en esta Recomendación se muestran en el Cuadro 7.1.3-1.

Cuadro 7.1.3-1 – Parámetros de una access-control-rule-tuple

Parámetro	Descripción de uso	Obligatorio /opcional	Formato
accessControlOriginators	Conjunto de originadores que pueden ser autorizados	Obligatorio	Lista de CSE-ID y/o AE ID, o palabra clave all para conceder acceso a todos los originadores
accessControlOperations	Conjunto de operaciones que pueden ser autorizadas	Obligatorio	Lista de operaciones Create (crear), Retrieve (recuperar), Update (actualizar), Delete

Cuadro 7.1.3-1 – Parámetros de una access-control-rule-tuple

Parámetro	Descripción de uso	Obligatorio /opcional	Formato
			(suprimir), Discover (descurbrir), Notify (notificar)
accessControlContexts	Véase Cuadro 7.1.3-3	Opcional	Véase Cuadro 7.1.3-3
accessControlObjectDetails	Véase Cuadro 7.1.3-4	Opcional	Véase Cuadro 7.1.3-4
accessControlAuthenticationFlag	Indica si la regla se aplica solo a los originadores que se consideran autentificados por la CSE anfitriona	Opcional	Booleano

El parámetro accessControlOriginators comprende una lista de nombres de dominio del proveedor de servicios (SP), CSE-ID, AE-ID, ID de recurso (resource-ID) de recursos <group> y/o ID de función (role-ID) de cualquier formato definido en la Recomendación UIT-T Y.4500.1. Si se va a permitir el acceso a todos los originadores, se puede incluir la palabra clave reservada all en el espacio de valores de accessControlOriginators.

El uso de un nombre de dominio SP en accessControlOriginators significa que todos los AE-ID y CSE-ID que coincidan con el nombre de dominio dado pueden ser autorizados.

Además, se permite utilizar el carácter comodín * en las representaciones de CSE-ID y AE-ID. El alcance de un * se termina con el siguiente carácter /. En el Cuadro 7.1.3-2 se muestran ejemplos de uso de caracteres comodín en los CSE-ID y AE-ID.

Los caracteres comodín no se aplican a los nombres de dominio del SP, a los resource-ID de los recursos <group> y a los identificadores de función (role-ID).

Cuadro 7.1.3-2 – Ejemplos de uso de caracteres comodín en CSE-ID y AE-ID de accessControlOriginators

	Forma de ID	Ejemplos	Significado
CSE-ID	Absoluto	//m2msp.org/myCSEID //*/myCSEID //*/myCSE*	Toda CSE cuyo identificador (ID) coincida con los comodines
	Relativo al SP	/myCSEID /myCSE*	Toda CSE coincidente del SP que aloja el recurso de destino
AE-ID	Absoluto	//m2msp.org/S988 //*/myCSEID/C9886 //*/myCSE*/C9886	Toda AE cuyo ID coincida con los comodines
	Relativo al SP	/myCSEID/C9886 /myCSEID/C98* /myCSE*/C98* /SmyAE*	Toda AE coincidente del SP que aloja el recurso de destino

El tipo de datos que se aplica a accessControlOriginators se define en la Recomendación UIT-T Y.4500.4.

El parámetro accessControlOperations comprende una lista de operaciones admisibles que puede ser cualquier subconjunto de los siguientes elementos: crear, recuperar, actualizar, eliminar, descubrir y notificar. Si bien las operaciones de creación, recuperación, actualización, eliminación y notificación se indican explícitamente en el parámetro *op* de un mensaje de solicitud, la operación de descubrimiento se indica mediante ***op*** = *Retrieve* en combinación con el suministro de los parámetros ***fc*** *y Disrestype* en el mensaje de solicitud.

El tipo de datos aplicable a accessControlOperations se define en [UIT-T Y.4500.4].

Los parámetros accessControlContexts se enumeran en el Cuadro 7.1.3-3.

Cuadro 7.1.3-3 – Parámetros de accessControlContexts

Parámetro	Descripción de uso	Obligatorio/opcional	Formatos
accessControlTimeWindow	Conjunto de intervalos de tiempo que pueden autorizarse	Opcional	Lista de intervalos de tiempo a los que se puede conceder acceso en formato crontab ampliado
accessControlLocationRegion	Conjunto de regiones de localización que pueden ser autorizadas	Opcional	1) Coordenadas de latitud/longitud, y un radio que define una región circular alrededor de las coordenadas 2) Código de país
accessControlIpAddress	Conjunto de direcciones IPv4 e IPv6 que pueden ser autorizadas	Opcional	Notación decimal en puntos con sufijo CIDR IPv6: grupos de dígitos hexadecimales separados por dos puntos con sufijo CIDR

El parámetro accessControlTimeWindow representa una lista de elementos que se ajustan a la sintaxis crontab ampliada definida en la cláusula 7.3.8 de la Recomendación UIT-T Y.4500.4. Permite definir intervalos de tiempo periódicamente recurrentes en los que se puede conceder el acceso, cuando el parámetro ***rq_time*** asociado al mensaje de solicitud de acceso entra en dicho intervalo.

Para los elementos de accessControlLocationRegion hay dos opciones de representación. Pueden representarse mediante un código de país de 2 letras o un círculo de radio *R* centrado en un punto definido mediante parámetros de longitud y latitud. Consulte el Anexo F para obtener información detallada. Cada elemento de accessControlLocationRegion define una región de localización admisible, que se compara con el parámetro ***rq_loc*** asociado al mensaje de solicitud de acceso.

Los tipos de datos aplicables a accessControlLocationRegion y ***rq_loc*** se definen en la Recomendación UIT-T Y.4500.4.

El parámetro accessControlIpAddress representa una lista de direcciones IPv4 e IPv6 en notación decimal en puntos con sufijo CIDR o grupos de dígitos hexadecimales separados por dos puntos con sufijo CIDR, respectivamente. Si el parámetro ***rq_loc*** asociado al mensaje de solicitud de acceso coincide con una de estas direcciones, se podrá conceder el acceso teniendo en cuenta este criterio.

Los tipos de datos aplicables a accessControlIpAddress y ***rq_ip*** se definen en la Recomendación UIT-T Y.4500.4.

El parámetro accessControlAuthenticationFlag es un valor booleano. Si el parámetro accessControlAuthenticationFlag no está presente, se asume que el valor es FALSE. Si el parámetro accessControlAuthenticationFlag es TRUE, esto indica que la regla de control de acceso se aplica

solo a los originadores que se consideran autentificados por la CSE anfitriona. La cláusula 7.1.2 precisa los criterios utilizados para decidir si se considera que el originador ha sido autentificado por la CSE anfitriona o no.

Los parámetros accessControlObjectDetails se enumeran en el Cuadro 7.1.3-4.

Cuadro 7.1.3-4 – Parámetros de accessControlObjectDetails

Parámetro	Descripción de uso	Obligatorio/opcional	Formatos
resourceType	Tipo de recurso al que se aplica la regla de control de acceso	Opcional	Identificador del tipo de recurso
specializationID	Identificador de mgmtDefinition o containerDefinition	Opcional	SmgmtDefinition o containerDefinition representados como una cadena.
childResourceType	Conjunto de identificadores de tipo de recurso que pueden crearse bajo el recurso progenitor	Opcional	Lista de tipos de recursos.

El atributo *accessControlObjectDetails* define un subconjunto de tipos de recursos vástagos del recurso de destino al que se aplica la regla de control de acceso. Si una regla de control de acceso incluye a*ccessControlObjectDetails*, se especificará el *childResourceType.* Las reglas de control de acceso que no incluyen ningún parámetro a*ccessControlObjectDetails* se aplican a todos los tipos de recursos vástagos del recurso de destino. El parámetro a*ccessControlObjectDetails* se describe en el Cuadro 9.6.2.4-1 de [UIT-T Y.4500.1]. Los tipos de recursos vástagos enumerados en el componente c*hildResourceTyp*e están sujetos al control de acceso solo para la operación Create. Una vez que se crea un recurso hijo, se aplican las políticas de control de acceso asignadas directamente a él. Los elementos r*esourceType* y s*pecializationID* son opcionales. Si el elemento *resourceType* o *specializationID* está presente en *accessControlObjectDetails*, la CSE compara el tipo de recurso o la especialización del recurso de destino con el valor indicado en el elemento *resourceType* o specializationID. Solo se realiza una comprobación posterior de *childResourceType* si se produce la coincidencia de *resourceType* o s*pecializationID*. Sin embargo, si no se proporcionan los elementos *resourceType* y *specializationID*, solo se realizará la comprobación de *childResourceType*.

7.1.4 Decisión de control de acceso

La decisión de acceso se obtiene comparando los parámetros asociados con un mensaje de solicitud de acceso a un recurso, tal como se describe en la cláusula 7.1.2, con las reglas de control de acceso incluidas en los atributos *privilegees* o s*elfPrivileges* de todos los conjuntos ACP asignados al recurso protegido por medio de los *accessControlPolicyID*, véase la Figura 7.1.1-1.

El resultado del algoritmo de decisión de acceso, es decir, la decisión de acceso es el resultado de la evaluación del conjunto de reglas de control de acceso aplicables, acrs, con respecto a los parámetros asociados al mensaje de solicitud de acceso. Esta decisión de acceso puede representarse mediante un valor de tipo de datos binario. El resultado global del algoritmo de decisión de acceso se indica aquí con el nombre de variable *res_acrs*:

$$res_acrs = \begin{cases} \text{TRUE or 1} & \text{if the request matches the access control rules} \\ \text{FALSE or 0} & \text{else} \end{cases}$$

El algoritmo de decisión de acceso de referencia se describe en la cláusula 7.1.5. Para un determinado conjunto de insumos, la implementación del procesamiento de la decisión de acceso arrojará el mismo resultado que el que arrojaría el algoritmo de decisión de acceso de referencia para esos insumos.

Si el algoritmo de decisión de acceso arroja el resultado *res_acrs* = TRUE, la decisión de acceso para el recurso solicitado será Permit (permiso).

Si el algoritmo de decisión de acceso arroja el resultado *res_acrs* = FALSE, o el algoritmo de decisión de acceso no es capaz de obtener un resultado final (por ejemplo, si los parámetros son indeterminados), la decisión de acceso para el recurso solicitado será Deny (denegar).

7.1.5 Descripción del algoritmo de decisión de acceso

El algoritmo de decisión de acceso de referencia definido en esta cláusula combina los resultados parciales de control de acceso obtenidos para cada una de las reglas de control de acceso individuales contenidas en un atributo *privileges* o a*utoprivilegios*. Además, si se asignan múltiples instancias de ACP al recurso protegido, el algoritmo de decisión de acceso de referencia combinará los resultados parciales de control de acceso obtenidos para los ACP individuales de un conjunto de ACP.

El algoritmo descrito en esta cláusula adopta un algoritmo de combinación Permit-overrides (permiso prioritario) con respecto a las reglas de control de acceso y los ACP, tal como se define en XACML [b-OASIS XACML]. Este algoritmo adopta el siguiente comportamiento:

Si la decisión es Permit para una sola regla de control de acceso incluida en el atributo *privileges* (o s*elfPrivilege*s) de un solo ACP, el resultado es permitir (Permitir).

En caso contrario, el resultado es denegar (Deny).

La lógica para evaluar una solicitud con respecto a un privilegio puede describirse matemáticamente de la siguiente manera. Un atributo *privileges* o s*elfPrivileges* incluido en un recurso <*accessControlPolicy*> representa un conjunto de reglas de control de acceso, *acrs*, que se conforma como en la Figura 7.1.5-1.

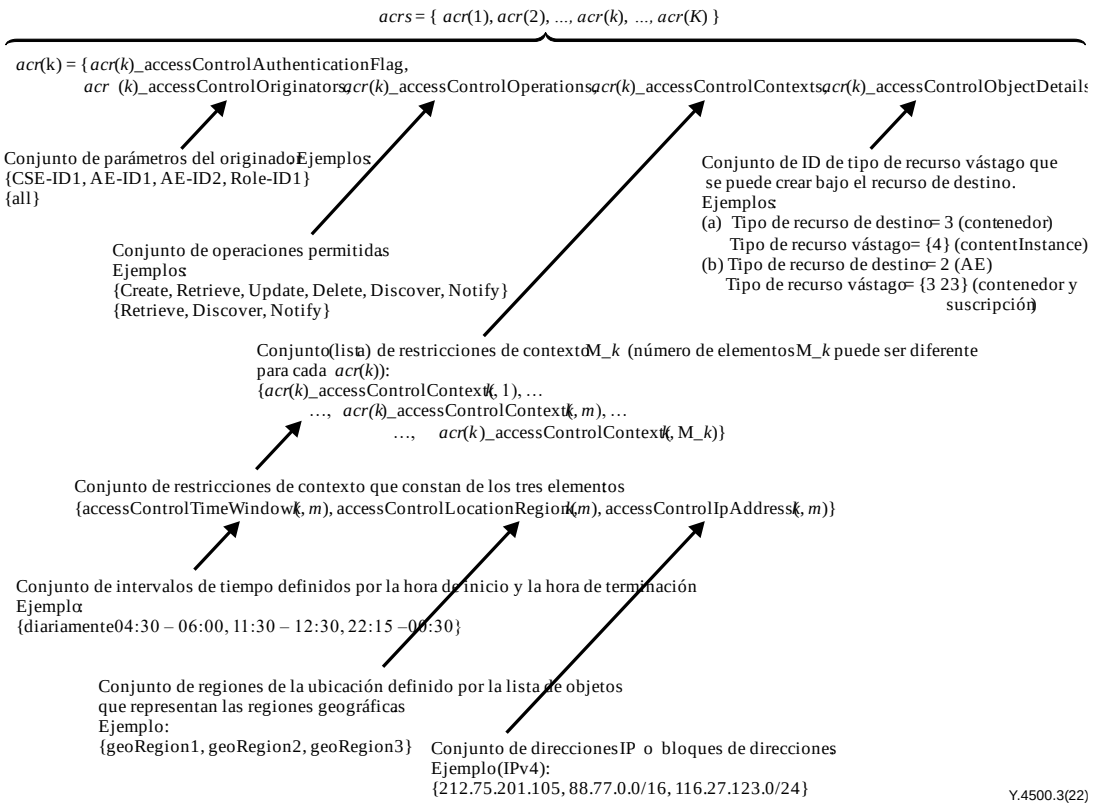


Figura 7.1.5-1 – Lógica para evaluar privilegios en el algoritmo de decisión de acceso de referencia

Los parámetros asociados con una solicitud que se evalúan con respecto a los parámetros contenidos en las reglas de control de acceso, se definen en la cláusula 7.1.3.

La decisión de acceso *res_acrs* definida en la cláusula 7.1.4 se obtiene determinando si los parámetros asociados con el mensaje de solicitud enumerados en los Cuadros 7.1.2-1 y 7.1.2-2 coinciden o no con alguna de las reglas de control de acceso contenidas en el conjunto de reglas de control de acceso definido en la cláusula 7.1.3 de la siguiente manera:

res_acrs = res_acr(1) OR res_acr(2) ... OR res_acr(k) ... OR res_acr(K),

donde *res_acr(k)* representa el resultado de la evaluación lógica (es decir, TRUE/FALSE o 1/0) de los parámetros de la solicitud con respecto a la k^a regla de control de acceso del conjunto *acrs*, que puede expresarse como sigue:

res_acr(k) = res_authn(k) AND res_origs(k) AND res_ops(k) AND res_ctxts(k) AND res_objd(k), k = 1…K.

La primera variable de resultado lógico parcial *res_authn(k)* del lado derecho de la ecuación anterior se evaluará con arreglo al Cuadro 7.1.5-1:

Cuadro 7.1.5-1 – Evaluación de *res_authn(k)*

***acr(k)*_accessControlAuthenticationFlag**	***rq_authn***	***res_authn***
TRUE	TRUE	TRUE
TRUE	FALSE	FALSE
FALSE	TRUE	TRUE
FALSE	FALSE	TRUE

Las cuatro variables de resultado lógico parcial restantes en el lado derecho de la ecuación anterior pueden definirse utilizando la siguiente función de conjunto:

$$\text{ismember}(x, \text{setX}) = \begin{cases} \text{TRUE or 1} & \text{if } x \in \text{setX} \\ \text{FALSE or 0} & \text{else} \end{cases}$$

Con la siguiente definición:

*res_origs(k) = ismember(**Originator**, acr(k)_accessControlOriginators)*

*res_ops(k) = ismember(**Operation**, acr(k)_ accessControlOperations)*

En la ecuación anterior, la variable ***Originator*** se refiere a la identidad autentificada del originador de la primitiva de solicitud que coincide con el parámetro ***From.***

El tercer resultado lógico parcial *res_ctxts(k*) se obtiene como sigue:

res_ctxts(k) = res_context(k, 1) ... OR res_context(k, m) ... OR res_context(k, M_k),

donde:

res_context(k, m) = res_time(k, m) AND res_ip(k, m) AND res_loc (k, m), k = 1…K, m = 1…M_k

y

*res_time(k, m) = ismember(**rq_time**, acr(k)_accessControlTimeWindow(m))*

*res_ip(k, m) = ismember(**rq_ip**, acr(k)_accessControlIpAddress(m))*

*res_loc (k, m) = ismember(**rq_loc**, acr(k)_accessControlLocationRegion(m))*

El cuarto resultado lógico parcial *res_objd(k)* se aplica únicamente a las primitivas de solicitud Create y se obtiene como

res_ objd(k) = res_ objdetails(k, 1) ... OR res_ objdetails(k, m) ... OR res_ objdetails(k, M_k),

donde:

res_ objdetails(k, m) = res_resourceType(k, m) AND res_specializationID(k, m) AND res_childResource(k,m),

para *m* = 1…M_*k***.** Los tres argumentos lógicos se definen a continuación.

Para cada elemento *acr(k)*_accessControlObjectDetails*(m)* en una regla de control de acceso, determinar si el parámetro opcional r*esourceTyp*e está presente

resourceType = acr(k)_accessControlObjectDetails(m)/resourceType

Dependiendo de la presencia de *resourceType*, *res_resourceType(k, m)* se obtiene como

$$res_resourceType(k,m) = \begin{cases} \text{TRUE or 1,} & \text{if not present in } acr(k)\text{_accessControlObjec tDetails}(m) \\ \text{TRUE or 1,} & \text{if present and } resourceType = targetResourceTypeID \\ \text{FALSE or 0,} & \text{if present and } resourceType \neq targetResourceTypeID \end{cases}$$

donde *targetResourceTypeID* es el identificador del tipo de recurso asociado con el recurso al que se refiere el parámetro ***To*** de la primitiva de solicitud Create.

Si el valor del elemento *resourceType* es 13 (<mgmtObject> specialization) o 28 (<flexContainer> specialization>), el elemento opcional specializationID se incluirá también en accessControlObjectDetails:

specializationID = acr(k)_accessControlObjectDetails(m)/specializationID

Si *specializationID* está presente, se comparará con los atributos *mgmtDefinition o containerDefinition* indicados en el parámetro ***Content*** (contenido) de la primitiva de la solicitud Create.

$$res_specializationID(k.m) = \begin{cases} \text{TRUE or 1,} & \text{if } specializationID \text{ not present in } acr(k)\text{_accessControlObjec tDetails}(m) \\ \text{TRUE or 1,} & specializationID = mgmtDefinition\,(resourceType = 13) \\ \text{TRUE or 1,} & specializationID = containerDefinition\,(resourceType = 28) \\ \text{FALSE or 0,} & specializationID \neq mgmtDefinition\,(resourceType = 13) \\ \text{FALSE or 0,} & specializationID \neq containerDefinition\,(resourceType = 28) \end{cases}$$

El elemento *childResourceType* es obligatorio en cualquier elemento accessControlObjectDetails de una regla de control de acceso. Incluye una lista de identificadores de tipo de recurso vástago *j = 1*...J a los que se aplica la regla. El elemento de la lista *j*[a] se indica como sigue:

childResourceType(k, m. j) = acr(k)_accessControlObjectDetails(m)/childResourceType(j), j = 1…J

La variable lógica *res_childResource(k, m)* se obtiene como

*res_ childResource (k, m) = ismember(**Resource Type**, childResourceType(k, m, j))*

*donde **Resource Type*** se refiere al valor del parámetro de la primitiva de solicitud Create en cuestión.

Si *resourceType* and *specializationID* no están presentes en *acr*(*k*)_accessControlObjectDetails(*m*), *res_ objdetails*(*k, m*) = *res_resourceType*(*k, m*) AND *res_specializationID*(*k, m*) AND *res_childResource*(*k,m*) = *res_childResource*(*k,m*)

Gracias al método de combinación Permit-overrides, si la decisión de control de acceso para una regla de control de acceso da como resultado *res_acr* = TRUE, el algoritmo de decisión de acceso de referencia puede detenerse sin necesidad de evaluar ninguna otra regla de control de acceso aplicable del ACP actual o de cualquier otro ACP del conjunto de ACP, y la decisión de acceso final es Permit.

7.2 Prevención de suplantación AE

7.2.1 Verificación del registrador del AE-ID

Dado que varias AE pueden comportarse de forma maliciosa y hacerse pasar por otra AE modificando su ID, la CSE anfitriona necesita contar con un mecanismo que le permita impedir la suplantación de AE. Este mecanismo funciona en el nivel de la CSE registradora, ya que la CSE registradora es un punto de entrada del sistema M2M.

Cuando la CSE registradora recibe una solicitud, deberá realizar el procedimiento que se muestra en la Figura 7.2.1-1 a continuación:

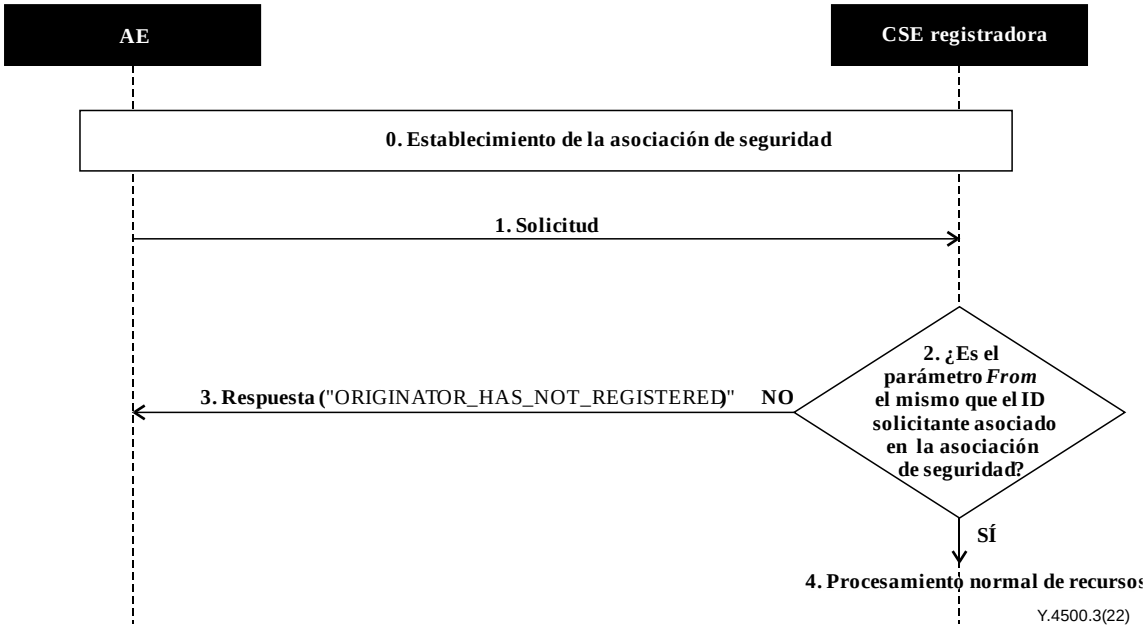


Figura 7.2.1-1 – Procedimiento de comprobación de la suplantación de AE

0 Puede establecerse una asociación de seguridad. La cláusula 6.1.2.2.1 describe los escenarios en los que es obligatorio el establecimiento de una asociación de seguridad entre una AE y una CSE, y describe los escenarios en los que se recomienda el establecimiento de una asociación de seguridad entre una AE y una CSE. Los procedimientos siguientes se llevarán a cabo si se ha establecido una asociación de seguridad.

1 La AE envía una solicitud a la CSE anfitriona a través de su CSE registradora como se especifica en la Recomendación UIT-T Y.4500.1 (la CSE anfitriona no está representada en esta figura y puede ser la CSE registradora u otra CSE).

2 La CSE registradora comprueba si el valor del parámetro ***From*** es el mismo que el ID asociado en la asociación de seguridad.

3 Si los valores no son idénticos, la CSE registradora enviará una respuesta con el código de estado de respuesta '4106' (ORIGINATOR_HAS_NOT_REGISTERED).

4 Si los valores son idénticos, la CSE registradora realizará los procedimientos descritos en la cláusula 8.2 de la Recomendación UIT-T Y.4500.1. Dependiendo del número de CSE de tránsito, la CSE registradora procesará la solicitud o la reenviará a la CSE anfitriona o a otra CSE de tránsito.

NOTA – Este procedimiento de verificación de suplantación no se aplica a las CSE. Esto se debe a que cuando una CSE de tránsito reenvía una solicitud a otra CSE, el parámetro ***From*** de la solicitud es el identificador del originador, que es diferente del identificador de la CSE de tránsito.

7.2.2 Verificación mediante la seguridad de las primitivas de extremo a extremo (ESPrim)

La seguridad de las primitivas de extremo a extremo (ESPrim) descrita en la cláusula 8.4 permite a un destinatario (una CSE o AE anfitriona) autentificar al originador *r* de una primitiva de solicitud que es gestionada por otras CSE. ESPrim también proporciona confidencialidad y protección de la integridad de estas primitivas de solicitud y respuesta. Las primitivas que son protegidas se denominan primitivas internas. La encriptación ESPrim se aplica a las primitivas internas para formar objetos ESPrim. Las primitivas externas se utilizan para transportar los objetos ESPrim entre el originador y la CSE o AE de destino. El registrador del originador no puede ver la primitiva interna encriptada ni verificar si el parámetro ***From*** de la primitiva interna es correcto. En cambio, se espera que el destinatario verifique que el parámetro ***From*** de la primitiva interna coincida con la identidad autentificada del originador.

Cuando el destinatario recibe una solicitud protegida por la ESPrim, debe realizar el procedimiento que se muestra en la Figura 7.2.2-1.

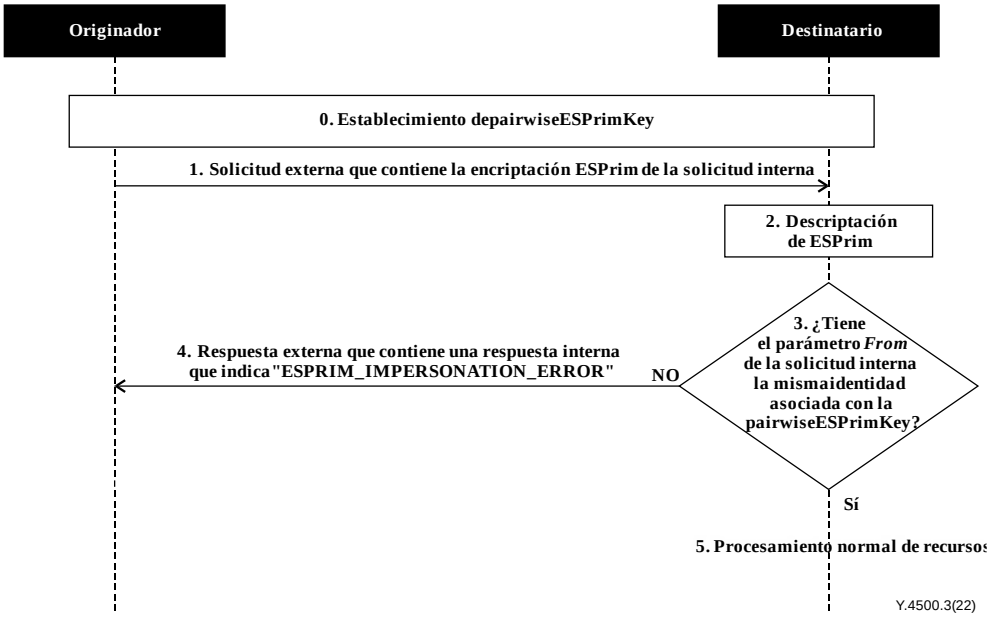


Figura 7.2.2-1 – Procedimiento de comprobación de la suplantación de AE

0 El destinatario y el originador han establecido previamente una clave simétrica ESPrimKey por pares. El destinatario asocia una identidad a la clave ESPrim simétrica por pares.

1 El originador compone la primitiva de solicitud interna, la encripta utilizando ESPrim para formar un objeto ESPrim, y lo envía al destinatario como se describe en la cláusula 8.4.

NOTA – Independientemente de que se aplique ESPrim, cada salto de Mcc está siempre protegido mediante un SAEF, y cada salto de Mca está opcionalmente protegido mediante un SAEF; véase la cláusula 6.1.2.2.1.

2 El destinatario aplica los procedimientos de la cláusula 8.4 para desencriptar el objeto ESPrim y obtener la primitiva de solicitud interna.

3 El destinatario comprueba si el valor del parámetro ***From*** es el mismo que el ID asociado con la pairwiseESPrimKey:

4 Si los valores no son idénticos, el destinatario enviará una respuesta con el código de estado de respuesta '4116' (ESPRIM_IMPERSONATION_ERROR).

5 Si los valores son idénticos, el destinatario registrará que el originador ha sido autentificado y realizará los procedimientos indicados en la cláusula 8.2 de la Recomendación UIT-T Y.4500.1.

7.3 Autorización dinámica

7.3.1 Objetivo de la autorización dinámica

La autorización dinámica ofrece un marco interoperable que permite otorgar dinámicamente a un originador permisos temporales que le proporcionan acceso a uno o más recursos en una o más CSE.

Los casos de uso, requisitos y propuestas aplicables se examinan en oneM2M TR-0019 [b-oneM2M TR0019].

En esta Recomendación se describen los parámetros de autorización dinámicos intercambiados y el procesamiento asociado en el originador y la CSE anfitriona. El transporte de los parámetros de autorización dinámica se especifica en [UIT-T Y.4500.1] y [UIT-T Y.4500.4].

7.3.2 Descripción detallada de la etapa 2 de la autorización dinámica

7.3.2.1 Modelo de autorización dinámica de referencia

El modelo de autorización dinámica de referencia se muestra en la Figura 7.3.2.1-1.

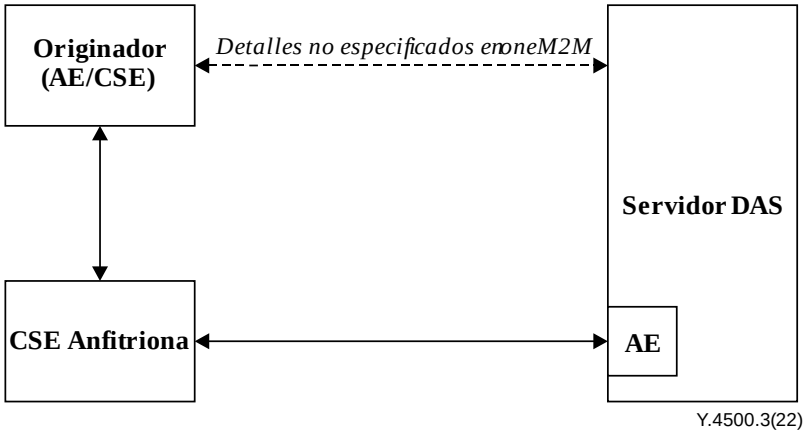


Figura 7.3.2.1-1 – Modelo de autorización dinámica de referencia

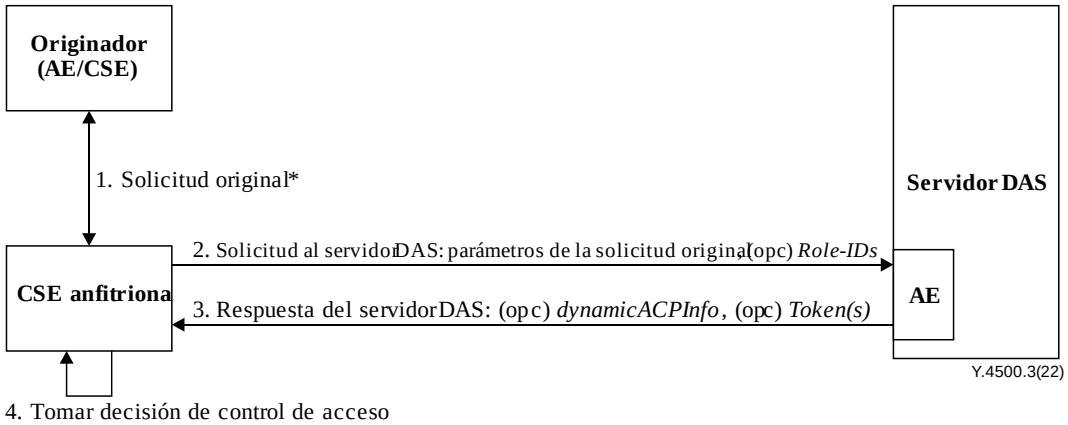
El modelo de autorización dinámica de referencia presenta los siguientes sistemas y entidades:

– Sistema de autorización dinámica (DAS): Sistema que soporta la autorización dinámica en nombre de los propietarios de los recursos. En la presente Recomendación no se describe el procesamiento ni el intercambio de mensajes dentro del sistema de autorización dinámica. Este sistema puede residir dentro o fuera de la red del proveedor de servicios.

– Servidor del sistema de autorización dinámica (DAS): Servidor configurado con políticas de autorización dinámica y provisto de credenciales para la emisión de.testigos. El servidor DAS puede incluir una AE para la interacción con el sistema oneM2M

A continuación se detallan los procedimientos de autorización dinámica:

La autorización dinámica directa se resume en la Figura 7.3.2.1-2. En este procedimiento, la CSE anfitriona interactúa con el servidor DAS para obtener la autorización dinámica.



** La solicitud original puede incluir Token(s) o Token IDs. Los detalles pertinentes se exponen en otras figura*

Figura 7.3.2.1-2 – Autorización dinámica directa

La **autorización dinámica indirecta** se resume en la Figura 7.3.2.1-3:

– Etapas 1-2: La CSE anfitriona puede proporcionar al originador ***Token Request Information*** (información sobre la solicitud de testigo) en la respuesta infructuosa.

– Etapa 3: El originador interactúa con el servidor DAS con la intención de que el servidor DAS emita testigos (*Tokens*) que autoricen al originador, y el originador recibe el testigo o un ID de testigo (*Token-ID)*. La interacción no se describe en esta Recomendación

– Etapas 4-7: El originador proporciona a la CSE anfitriona un *Token* o un *Token-ID* para indicar que el testigo debe tenerse en cuenta en la decisión de acceso. En el caso de un token-ID, la CSE anfitriona recupera el testigo correspondiente a través de una AE del servidor DAS. A continuación, se utiliza en la decisión de acceso. La CSE anfitriona puede proporcionar al originador un ID de testigo local (*Local-Token-ID)* que puede utilizarse para identificar el testigo.

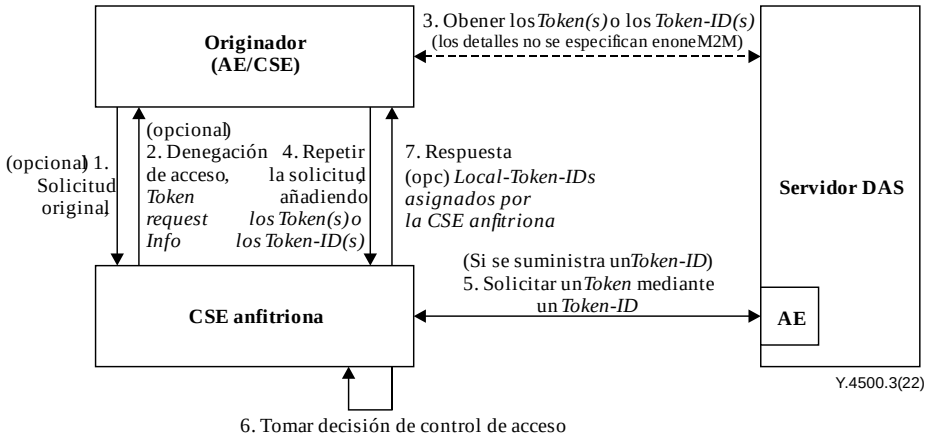


Figura 7.3.2.1-3 – Autorización dinámica indirecta

7.3.2.2 Autorización dinámica directa

En esta Recomendación se describen los parámetros intercambiados y el procesamiento asociado en la CSE anfitriona. El transporte de los parámetros se define en la cláusula 11.5.2, de [UIT-T Y.4500.1].

El flujo de mensajes para la autorización dinámica directa se muestra en la Figura 7.3.2.2-1 y se describe en el texto siguiente.

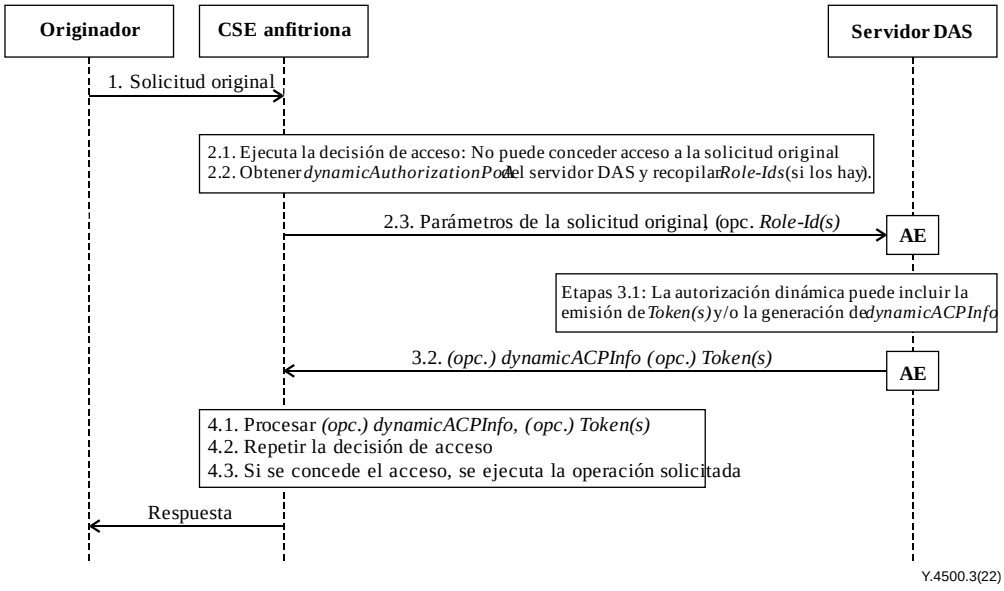


Figura 7.3.2.2-1 – Flujo de mensajes para la autorización dinámica indirecta

1 El originador envía una solicitud (denominada solicitud del originador en este flujo de mensajes) a la CSE anfitriona. Esta solicitud puede incluir *Tokens o TokenID*; véase la cláusula 7.3.2.3 Autorización dinámica indirecta.

2 Procesamiento inicial de la CSE anfitriona:

2.1 Si la solicitud del originador incluye ***Tokens*** o ***Token-IDs***, estos se procesan como se describe en la cláusula 7.3.2.3 Autorización dinámica indirecta. La CSE anfitriona evalúa el algoritmo de decisión de acceso, pero no puede conceder el acceso a la solicitud del originador basándose en las políticas de control de acceso configuradas

2.2 La CSE anfitriona determina el conjunto de servidores DAS con los que se puede realizar la autorización dinámica directa:

2.2.1 La CSE anfitriona examina todas las reglas a*ccessControlRules* con arreglo a las cuales la solicitud satisface las a*ccessControlOperation*s y los *accessControlContext*s en los recursos <*accessControlPolicy*> vinculados al recurso solicitado. La CSE anfitriona recopila todos los ID de función (*Role-ID)* en los a*ccessControlOperators* de estas *accessControlRules*. Estos *Role-ID* se agrupan según el AE-ID del servidor DAS identificado por el *Role-ID.*

NOTA 1 – En relación con el parámetro ID de función (Role-ID) – El originador podrá acceder si se emite uno o varios testigos que asocien al originador con uno o más de los Role-ID. Al proporcionar esta lista al servidor DAS, éste puede seleccionar un conjunto adecuado de uno o más Role-ID para asociarlo con el originador en el testigo, autorizando así al originador a acceder a los recursos solicitados. Las políticas configuradas en el servidor DAS dictarían qué Role-ID (si los hay) se incluyen en los testigos expedidos al originador.

2.2.2 La CSE anfitriona también recopilará el conjunto de recursos <*dynamicAuthorizationConsultation*> vinculados al recurso solicitado, y los agrupará según el atributo d*ynamicAuthorizationPoA* del servidor DAS del recurso <*dynamicAuthorizationConsultation*>.

2.3 La CSE anfitriona selecciona un servidor DAS (del conjunto descrito en la etapa 2.2) y envía un mensaje de solicitud oneM2M que contiene la información descrita en el Cuadro 7.3.2.2-1. El transporte de los parámetros se describe en la etapa 2.3, cláusula 11.5.2, de [UIT-T Y.4500.1].

Cuadro 7.3.2.2-1 – Información enviada desde la CSE anfitriona al servidor DAS durante la autorización dinámica directa

Parámetro	Descripción	Obligatorio/ opcional
Originador	Identificador del originador de la solicitud recibida por el receptor	Obligatorio
Tipo de recurso del originador	Tipo de recurso al que se dirige la solicitud originada recibida por el receptor	Obligatorio
Operación	Tipo de operación definida en la solicitud originada recibida por el receptor	Obligatorio
Dirección IP del originador	Dirección IP del originador de la solicitud recibida por el receptor	Opcional
Ubicación del originador	Ubicación del originador de la solicitud recibida por el receptor	Opcional
Identificadores de función del originador	Identificadores de función (role ID) del originador de una solicitud recibida por el receptor	Opcional
Fecha y hora de la solicitud	Fecha y hora en que la solicitud originada fue recibida por el receptor	Opcional

Cuadro 7.3.2.2-1 – Información enviada desde la CSE anfitriona al servidor DAS durante la autorización dinámica directa

Parámetro	Descripción	Obligatorio/ opcional
Identificador de recurso de destino	Identificador de recurso (resource ID) de destino de la solicitud originada recibida por el receptor	Opcional
Duración propuesta de un privilegio	Duración propuesta de privilegios de autorización solicitados por el receptor	Opcional
Identificadores de función de los ACP	El conjunto de funciones de acceso dinámico en los parámetros a*ccessControlDynAuthRole* asociados con el AE-ID del servidor DAS.	Opcional
Identificadores de testigo	Conjunto de identificadores de testigo (Token IDs) asociados con el originador	Opcional

3 Procesamiento del servidor DAS:

3.1 El servidor DAS procesa los parámetros recibidos. El servidor DAS puede decidir proporcionar los *Token(s)* y/o *dynamicACPInfo* que serán utilizados por la CSE anfitriona para crear un recurso dinámico <*accessControlPolicy*>. El servidor DAS aplica las políticas con las que está configurado para decidir las acciones apropiadas.

NOTA 2 – Los detalles de esta decisión dependen del sistema de autorización dinámica que se emplee; estos detalles no son visibles para el sistema oneM2M y no se abordan en esta Recomendación.

Los testigos (si los hay) se deberán conformar a la cláusula 7.3.3.1 Estructura de los testigos, con el siguiente perfil:

– anfitriona y podrá contener otros CSE-ID y AE-IDS.

– El parámetro audience contendrá únicamente el CSE-ID de la CSE anfitriona.

El servidor DAS aplicará la opción de protección ESData a los tokens individuales con los requisitos siguientes:

– El servidor DAS podrá encriptar el testigo de manera que la CSE anfitriona pueda desencriptarlo.

– La CSE anfitriona deberá ser capaz de verificar que el servidor DAS emitió el token.

El procesamiento de ESData da lugar a un envolvente de ESData que se denomina *ESData-protected Token* a los efectos de este flujo de mensajes.

Si el servidor DAS decide autorizar a la CSE anfitriona a crear un recurso dinámico <*accessControlPolicy*>, el servidor DAS creará un parámetro *dynamicACPInfo* que contendrá la siguiente información, tal como se indica en el Cuadro 7.3.2.2-2.

Cuadro 7.3.2.2-2 – Información incluida en el parámetro dynamicACPInfo

Parámetro	Descripción	Obligatorio/Opcional
Privilegios concedidos	Lista de privilegios concedidos	Opcional
Duración de los privilegios	Duración de los privilegios concedidos	Opcional
Testigos	Lista de testigos emitidos	Opcional

3.2 El servidor DAS enviará el (los) *Token*(s) protegido(s) por ESData (si lo hay) y el parámetro (opcional) *dynamicACPInfo* a través de la AE del servidor DAS a la CSE anfitriona. El transporte de los parámetros se especifica en la etapa 2.3, cláusula 11.5.2, de la Recomendación [UIT-T Y.4500.1].

4 Procesamiento de la CSE anfitriona:

4.1 La CSE anfitriona procesa los *Token(s*) protegidos por ESData (si están presentes) y el parámetro *dynamicACPInfo* (si está presente):

4.1.1 La CSE anfitriona deberá realizar las siguientes comprobaciones para cada *Token* protegido por ESData:

4.1.1.1 La CSE anfitriona deberá aplicar el procesamiento de ESData al *Token* protegido por ESData para extraer el testigo autentificado.

4.1.1.2 La CSE anfitriona realizará las siguientes verificaciones:

4.1.1.2.1 El parámetro issuer en el testigo deberá coincidir exactamente con la identidad del servidor DAS.

4.1.1.2.2 El CSE-ID de la CSE anfitriona deberá coincidir con el CSE-ID del parámetro audience del testigo.

4.1.1.2.3 El parámetro holder en el testigo deberá coincidir exactamente con el CSE-ID o AE-ID absoluto del originador del que se recibió la solicitud.

4.1.1.2.4 La CSE anfitriona comprobará que el testigo no ha caducado, comparando la hora actual con el parámetro notAfter del testigo.

4.1.1.3 La CSE anfitriona almacenará en caché el testigo verificado y podrá eliminarlo posteriormente cuando expire (como se define en la etapa 4.1.2.4).

4.1.2 Si el Servidor DAS proporciona el *dynamicACPInfo*, la CSE anfitriona creará un recurso dinámico <*accessControlPolicy*> que coincida con el d*ynamicACPInfo*.

4.2 La CSE anfitriona repite el mecanismo de decisión de acceso que se describe en la cláusula 7.1.4 Decisión de control de acceso.

4.3 Si se concede el acceso, la CSE anfitriona realiza la operación solicitada en la solicitud del originador, lo cual da lugar a que la CSE anfitriona envíe una solicitud al originador.

7.3.2.3 Autorización dinámica indirecta

Esta Recomendación especifica los parámetros intercambiados y el procesamiento conexo en el originador y la CSE anfitriona. El transporte de los parámetros se define en la cláusula 11.5.3 de la Recomendación UIT-T Y.4500.1.

El flujo de mensajes para la autorización dinámica indirecta se muestra en la Figura 7.3.2.3-1, y se describe en el texto siguiente.

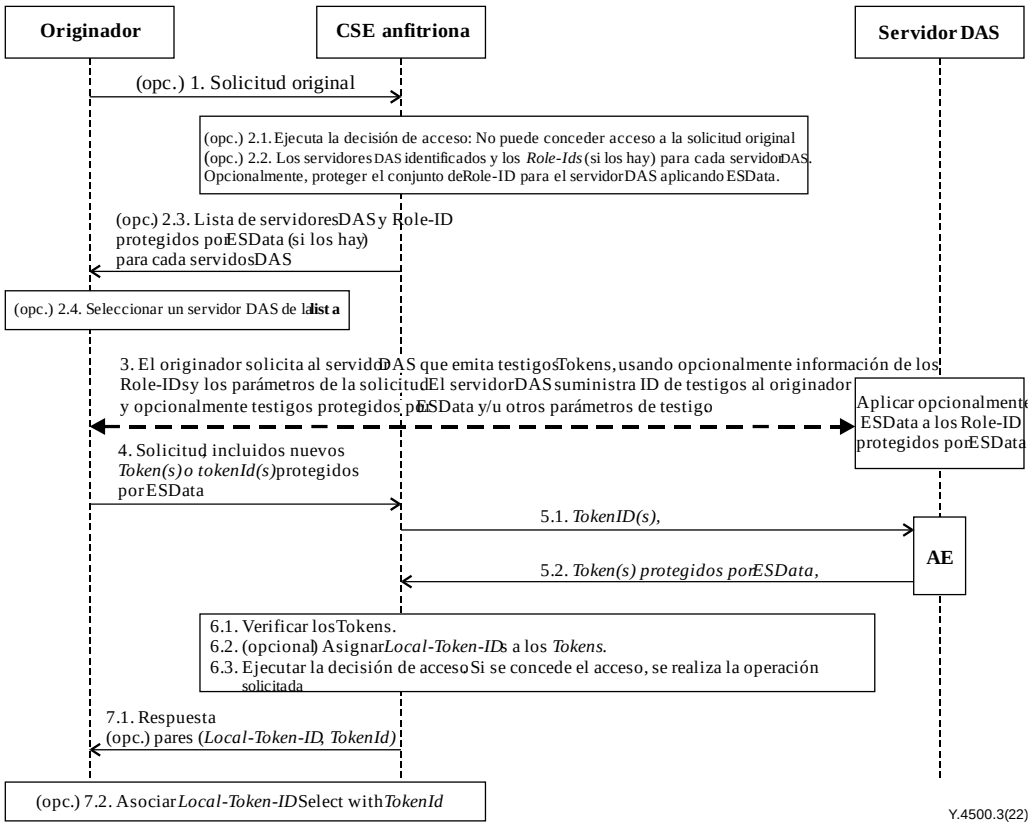


Figure 7.3.2.3-1 – Message flow for indirect dynamic authorization

1 (Opcional) El originador envía la solicitud a la CSE anfitriona. El originador incluye una indicación de que está listo para solicitar testigos a los servidores DAS para esta solicitud. Esta solicitud puede incluir una combinación de *tokens, tokenIDs, Local-Token-IDs*, pero este flujo de mensajes supone que estos no ofrecen suficientes permisos para acceder al recurso solicitado.

2 (Opcional) Procesamiento inicial de la CSE anfitriona:

2.1 La CSE anfitriona ejecuta la decisión de acceso para la solicitud del originador. Este flujo de llamadas supone que la solicitud del originador se deniega como consecuencia de la decisión de acceso. La CSE anfitriona tiene en cuenta la indicación de que el originador está preparado para solicitar testigos a los servidores DAS para esta solicitud.

2.2 La CSE anfitriona elabora una lista de servidores DAS y los identificadores de función (Role-ID) asociados (si los hay), tal como se describe en la etapa 2.2.1 de la autorización dinámica directa en la cláusula 7.3.2.3 Autorización dinámica directa.

Para cada servidor DAS, la CSE anfitriona podrá aplicar ESData al conjunto de identificadores de función para ser desencriptados por el servidor DAS. Por ejemplo, ESData puede encriptar el conjunto de Role-ID para que no sean visibles para el originador.

2.3 La CSE anfitriona enviará una respuesta infructuosa al originador, incluida la lista de servidores DAS y el conjunto asociado de de Role-ID opcionalmente protegidos por ESData.

2.4 El originador selecciona un servidor DAS identificado en la respuesta.

3 El originador deberá interactuar con el servidor DAS para solicitar la emisión de un *Token*. El originador puede proporcionar al servidor DAS el conjunto de identificadores de función, opcionalmente protegido por ESData y los parámetros de la solicitud original de acceso a los recursos. Si el conjunto de identificadores de función está protegido mediante ESData, el servidor DAS aplica ESData para extraer el conjunto de identificadores de función. El servidor DAS emite uno o más testigos y proporciona los identificadores de testigo y, opcionalmente, los testigos protegidos por

ESData al originador. El servidor DAS también puede proporcionar al originador otros parámetros del testigo; por ejemplo, el periodo de tiempo en el que el testigo es válido. Esta interacción depende de la tecnología del sistema de autorización dinámica que se utilice.

4 En el caso de las solicitudes que el originador desee que se autoricen utilizando un testigo emitido, el originador añadirá el testigo protegido por ESData proporcionado por el servidor DAS o *token-Id* (si no se ha proporcionado ningún testigo protegido por ESData) si el servidor DAS no ha proporcionado los correspondientes testigos protegidos por ESData. En particular, si la solicitud en la etapa 1 no tuvo éxito en la etapa 2.3, el creador puede repetir la solicitud con nuevos *Token(s)* y/o *token-ID*. Un mismo testigo puede utilizarse en varias solicitudes.

El originador enviará la solicitud a la CSE anfitriona.

5 (Opcional) Si la solicitud incluye *tokenID(s*), para cada *tokenID* la CSE anfitriona identifica la AE del servidor DAS a la que solicitar el correspondiente testigo:

5.1 La CSE anfitriona envía el(los) identificador(es) de testigo al servidor DAS a través de una AE del servidor DAS.

5.2 El servidor DAS devolverá el/los testigo(s) válido(s) protegido(s) por ESData a la CSE anfitriona a través de la AE del servidor DAS.

6 Procesamiento de la CSE anfitriona:

6.1 Procesamiento de testigos:

– El CSE-ID de la CSE anfitriona deberá coincidir con uno de los CSE-ID absolutos (que puede incluir comodines) en el parámetro audience del testigo.

– El parámetro holder del testigo deberá coincidir exactamente con el CSE-ID absoluto o el AE-ID del originador del que se ha recibido la solicitud.

– La CSE anfitriona verificará que el testigo es válido y no ha expirado, comparando la hora actual con los parámetros notBefore y notAfter del testigo. Si un testigo almacenado en caché ha expirado, podrá ser eliminado de la caché.

6.1.1 La CSE anfitriona aplicará ESData a los testigos protegidos por ESData, proporcionados en la solicitud o recuperados del servidor DAS, para extraer los testigos autentificados.

6.1.2 Si se ha proporcionado un Local-Token-ID en la solicitud, la CSE anfitriona intentará recuperar el testigo en caché.

6.1.3 La CSE anfitriona deberá realizar las siguientes comprobaciones para cada testigo autentificado y almacenado en caché asociado a la solicitud:

– El CSE-ID de la CSE anfitriona deberá coincidir con uno de los CSE-ID absolutos (que puede incluir comodines) en el parámetro audience del testigo.

– El parámetro holder del testigo deberá coincidir exactamente con el CSE-ID absoluto o el AE-ID del originador del que se ha recibido la solicitud.

– La CSE anfitriona verificará si el testigo es válido y no ha expirado, comparando la hora actual con los parámetros notBefore y notAfter del testigo. Si un testigo almacenado en la caché ha caducado, podrá ser eliminado de la caché.

6.1.4 Si no se ha podido recuperar ningún token identificado en las etapas 5 o 6.1.2, o si algún Token-ID protegido por ESData no ha superado la verificación en la etapa 6.1.1, o si ningún token ha superado la verificación en la etapa 6.1.3, la CSE anfitriona deberá responder con un error.

6.1.5 La CSE anfitriona puede almacenar en caché cualquier nuevo testigo.

6.2 La CSE anfitriona puede asignar *Local-Token-ID*(s) a los testigos almacenados en caché.

6.3 La CSE anfitriona tomará la decisión de acceso descrita en la cláusula 7.1.4, incluida la información de los testigos identificados en la solicitud. Si se concede el acceso, se realizará la operación solicitada.

7 Respuesta:

7.1 La CSE anfitriona envía una respuesta al originador. Para cada nuevo *Local-Token-ID* que se haya asignado, la CSE anfitriona proporciona el *Local-Token-ID* y el correspondiente *tokenID* en los parámetros de respuesta.

7.2 El originador asocia el *Local-Token-ID* con el *tokenID*. En posteriores solicitudes, el originador puede utilizar el *Local-Token-ID* en lugar del *Token* o del *tokenID*.

7.3.2.4 Estructura del testigo

Un testigo se utiliza para transportar información de autorización que puede ser funciones asignadas al titular del testigo o políticas de control de acceso aplicables al titular del testigo. La estructura del testigo se muestra en la Figura 7.3.2.4-1, y contiene los siguientes campos de datos:

version (versión): versión del testigo.

tokenID (ID del testigo): ID único del testigo.

holder (titular): ID del titular del testigo.

issuer (emisor): ID del emisor del testigo.

notBefore (no antes): testigo válido a partir de este momento.

notAfter (no después): el testigo caduca a partir de este momento.

tokenName (nombre del testigo): opcional, nombre legible del testigo.

audience (destinatarios): opcional, lista de CSE_ID de las CSE que se prevé que acepten el testigo.

permissions (permisos): permisos asociados al testigo. Su formato se especifica en la cláusula 9.6.39 de la Recomendación [UIT-T Y.4500.1].

extension (extensión): se utiliza para almacenar otra información, por ejemplo, información específica de la aplicación.

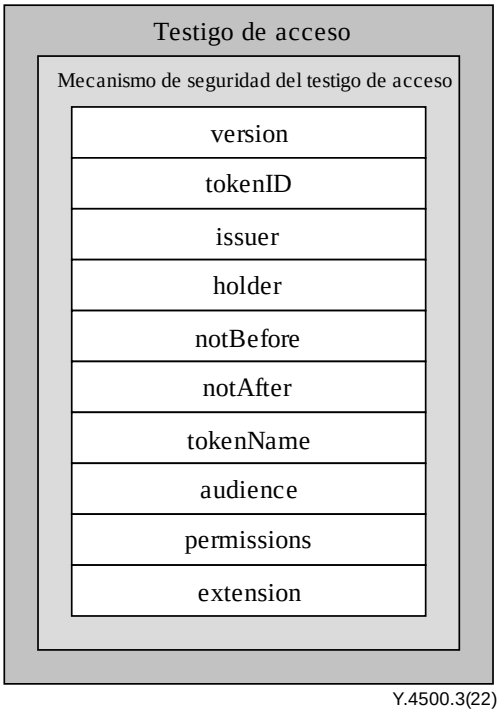


Figura 7.3.2.4-1 – Estructura de un testigo

Un testigo debe estar protegido por el mecanismo de seguridad de ESData. Los testigos deben estar firmados, encriptados o firmados y encriptados.

7.3.2.5 Evaluación de testigos

El proceso genérico de evaluación de un testigo puede describirse de la siguiente manera:

Validación de la seguridad del testigo: Dependiendo del mecanismo de seguridad utilizado por un testigo, la validación puede ser:

Verificar el testigo firmado;

Desencriptación del testigo encriptado; o

Desencriptar y verificar el testigo firmado y encriptado.

Una vez superada la validación de seguridad del testigo, se puede utilizar el texto sin formato del mismo para su posterior validación.

Validación del contenido del testigo: Dependiendo del contenido del testigo, la validación podrá comprobar:

Si la identidad del originador es idéntica a la del titular del testigo especificado en el campo de datos *holder*.

Si el emisor del testigo especificado en el campo de datos *issuer* es válido.

Si este testigo no ha caducado según los campos de datos *notBefore y notAfter*.

Si el identificador de la CSE anfitriona está en la lista de CSE-ID especificada en el campo de datos *audience* (en caso de que el campo de datos *audience* no esté vacío).

Una vez superada la validación del contenido del testigo, se utilizarán los permisos asociados a este testigo para el control de acceso.

Evaluación de los permisos del testigo: Comprobación del elemento de permiso en la lista de permisos uno por uno hasta que la solicitud de acceso esté autorizada por uno de los permisos o el final de la lista. Para cada permiso de la lista de permisos la evaluación se hará como sigue:

Comprobación del elemento *resourceID*. Si está presente, la información de autorización descrita en los elementos *privileges* y/o *roleID* se aplicará únicamente a los recursos especificados por este elemento. Si el elemento *privileges* está presente, entonces este elemento estará presente.

Si el elemento *privileges* está presente, las reglas de control de acceso contenidas en este elemento se utilizarán como política de control de acceso aplicable en el proceso en curso de toma de decisiones de control de acceso.

Si el elemento *roleID* está presente, los Role-ID contenidos en este elemento se utilizarán como funciones válidas en el proceso en curso de toma de decisiones de control de acceso.

7.3.2.6 Testigos web JSON (JWT) de oneM2M

7.3.2.6.1 Introducción a oneM2M JWT

El sistema oneM2M especifica una representación de testigos web JSON (JWT) [IETF RFC 7519] para los testigos utilizados en oneM2M. Un JWT que cumple con la presente cláusula se denomina*oneM2M JWT*.

Antecedentes: Un JWT utiliza la representación compacta de la firma web JSON (JWS), o la representación compacta del encriptado web JSON (JWE), especificadas en [IETF RFC 7515] y [IETF RFC 7519]. La especificación JWT [IETF RFC 7519] también se refiere a un JWT inseguro que es un JWS que utiliza el valor del parámetro de cabecera alg none y con la cadena vacía para su valor de firma JWS.

La especificación JWT define un elemento JSON que es la estructura de la carga útil del JWS o JWE cuando se utiliza como JWT. Esta carga útil comprende un conjunto de afirmaciones JWT, con [IETF RFC 7519] que estandariza un conjunto inicial de nombres de afirmaciones JWT. IANA mantiene un registro de nombres de afirmaciones JWT [b-IANA JWT].

7.3.2.6.2 Perfil oneM2M JWT

Afirmaciones oneM2M JWT: En el Cuadro 7.3.2.6.2-1 se puede apreciar la correspondencia de los nombres de afirmaciones JWT, en un oneM2M JWT con los elementos del tipo de datos complejo m2m:tokenClaimSet descrito en [UIT-T Y.4500.4]. Cuando están disponibles, se han utilizado los nombres de afirmaciones JWT registrados en IANA [b-IANA JWT]. En [UIT-T Y.4500.4] se especifica qué elementos son obligatorios y qué elementos son opcionales.

Cuadro 7.3.2.6.2-1 – Conjunto de afirmaciones JWT de oneM2M y correspondencia con los elementos de m2m:tokenClaimSet

Trayecto del elemento objeto de Token Claimset	Nombre abreviado del elemento objeto de Token Claimset	Nombre de afirmación de JWT de oneM2M	¿Dónde está definido este nombre de afirmación JWT?	Detalles adicionales para la correspondencia de los valores objeto de Token Claimset a los valores de afirmación JWT
version	***tkvr***	tkvr	[ITU-T Y.4500.4] nombres abreviados	Los valores deberán ser idénticos
tokenID	***tkid***	jti	[IETF RFC 7519]	Los valores deberán ser idénticos
issuer	***tkis***	iss	[IETF RFC 7519]	Los valores deberán ser idénticos
holder	***tkhd***	azp	OpenID Connect Core 1.0 [OIDF CC]	Los valores deberán ser idénticos
notBefore	***tknb***	nbf	[IETF RFC 7519]	El elemento notBefore de Token Claimset Object está en Basic Format de ISO8601, véase la Recomendación [UIT-T Y.4500.4]. Este elemento se corresponderá con la afirmación JWT nbf, que utiliza el formato NumericDate [RFC7519].
notAfter	***tkna***	exp	[IETF RFC 7519]	El elemento notAfter del Token Claimset Object está en el Basic Format de ISO8601, véase la Recomendación [UIT-T Y.4500.4]. Este elemento se corresponderá con la afirmación JWT exp, que utiliza el formato NumericDate [RFC7519].
tokenName	***tknm***	tknm	[ITU-T Y.4500.4] nombres abreviados	Los valores deberán ser idénticos
audience	***tkau***	aud	[IETF RFC 7519]	El elemento audience del Token Claimset Object es una lista de m2m:ID. Esta lista debe corresponder con la afirmación JWT aud que comprende una matriz de cadenas que distinguen mayúsculas y minúsculas, cada una de las cuales contiene un valor StringOrURI [RFC7519].
permissions	***tkps***	tkps	[ITU-T Y.4500.4] nombres abreviados	Los valores deberán ser idénticos
extension	***tkex***	tkex	[ITU-T Y.4500.4] nombres abreviados	Los valores deberán ser idénticos

perfil de seguridad oneM2M JWT. Tanto la representación compacta JWS como la representación compacta JWE son soportadas por ESData (véase la cláusula 8.5.3). Un oneM2M JWT puede utilizar cualquier clase de seguridad de ESData: Solo encriptación, solo firma o Nested-Sign-then-encrypt. Un oneM2M JWT puede utilizar cualquier algoritmo soportado por ESData para la representación compacta JWS y la representación compacta JWE.

Un oneM2M JWT puede ser un JWT no seguro, en cuyo caso se considera que oneM2M JWT utiliza la clase de seguridad ESData no segura.

La norma [IETF RFC 7519] examina las consideraciones de seguridad de los JWT, por lo que los operadores de los emisores de testigos (servidores de autorización dinámicos y Autoridades de Autorización) deberían consultar ese texto a la hora de decidir la clase de seguridad ESData y los algoritmos.

Parámetros de cabecera JOSE de los oneM2M JWT. Cuando se utiliza la clase de seguridad ESData de solo encriptación, entonces:

la cabecera JOSE del JWE incluirá los parámetros typ configurados como JWT.

La cabecera JOSE del JWE no incluirá el parámetro cty.

Si se utiliza la clase de seguridad ESData de solo firma, entonces:

la cabecera JOSE del JWS incluirá los parámetros typ configurados como JWT.

La cabecera JOSE del JWS no incluirá el parámetro cty.

7.3.2.6.3 Procedimientos oneM2M JWT

Configurar las CSE para la verificación de los testigos de un emisor de testigos. Para que una CSE pueda verificar los oneM2M JWT emitidos por un emisor de testigo concreto, la CSE deberá recibir la siguiente información de forma segura:

Las combinaciones de clases de seguridad y algoritmos ESData permitidas por el emisor del testigo.

Las credenciales para verificar los testigos que se conforman con esas clases de seguridad y algoritmos ESData, señalando que no se necesitan credenciales para verificar los testigos que utilizan la clase de seguridad ESData no segura.

En la presente especificación no se definen los mecanismos para proporcionar esta información a la CSE. Tampoco se definen las estructuras de datos para almacenar esta información en la CSE. El nivel de seguridad que debe aplicarse en cada CSE concreta debe obtenerse de la evaluación de riesgos específica de la aplicación.

Creación de un oneM2M JWT: Cuando un emisor de testigos es activado para crear un testigo, deberá realizar los siguientes pasos

El emisor de testigos formará un token claimset object que cumpla con el tipo de datos m2m:tokenClaimSet, con el elemento permission mediante la serialización JSON.

El emisor del testigo deberá crear el correspondiente conjunto de afirmaciones oneM2M JWT utilizando las correspondencias del Cuadro 7.3.2.6.2-1.

El emisor del testigo seleccionará una clase de seguridad, algoritmos y credenciales ESData correspondientes. Esta etapa también puede realizarse antes de la etapa 1) o entre las etapas 1) y 2).

El emisor del testigo creará el oneM2M JWT utilizando las afirmaciones del oneM2M JW, la clase de seguridad, algoritmos y las credenciales ESData correspondientes. Esta etapa también puede realizarse antes de la etapa 1) o entre las etapas 1) y 2).

El emisor del testigo creará el oneM2M JWT utilizando las afirmaciones oneM2M JWT, la clase de seguridad, algoritmos y las credenciales ESData correspondientes. Esta etapa utiliza el proceso descrito para los JWT en [IETF RFC 7519].

El oneM2M JWTresultante tiene el tipo de datos m2m:dynAuthJWT.

Validación de un oneM2M JWT: Cuando una CSE recibe un oneM2M JWT para utilizarlo en una decisión de acceso, la CSE deberá realizar las siguientes acciones:

La CSE validará la conformidad del oneM2M JWT con el tipo de datos m2m:dynAuthJWT.

La CSE validará la seguridad del oneM2M JWT como se describe en la cláusula 7.3.2.5, utilizando los detalles específicos del JWT en [IETF RFC 7519] y las credenciales configuradas (si es necesario). Una CSE descartará los oneM2M JWT que utilicen una clase de seguridad o algoritmo ESData no permitidos por el emisor del testigo.

La CSE creará un token claimset object a partir del conjunto de afirmaciones oneM2M JWT invirtiendo la correspondencia del Cuadro 7.3.2.6.2-1.

La CSE validará el token claimset object como se describe en la cláusula 7.3.2.5.

El elemento permissions del token claimset object puede ahora ser procesado como se describe en la cláusula 7.3.2.5.

7.4 Control de acceso basado en funciones

7.4.1 Arquitectura de control de acceso basada en funciones

La Figura 7.4.1-1 ofrece una visión general de la arquitectura de control de acceso basado en funciones en el sistema oneM2M. Las entidades relacionadas con la emisión de funciones y el control de acceso basado en funciones se describen a continuación:

Autoridad de autorización: Se encarga de asignar funciones a los originadores mediante la creación de recursos <role> y/o <token> en los repositorios de funciones y/o testigos.

Repositorio de funciones: Se trata de una CSE que se encarga de almacenar los recursos <role>.

Repositorio de testigos: Se trata de una CSE que se encarga de almacenar los recursos <token>.

NOTA 1 – Las flechas que aparecen en la Figura 7.4.1-1 representan las relaciones lógicas entre las entidades y no las relaciones de registro que forman los trayectos de datos reales.

NOTA 2 – Las funciones de PDP y PIP se combinan en la CSE anfitriona para la presente versión de oneM2M.

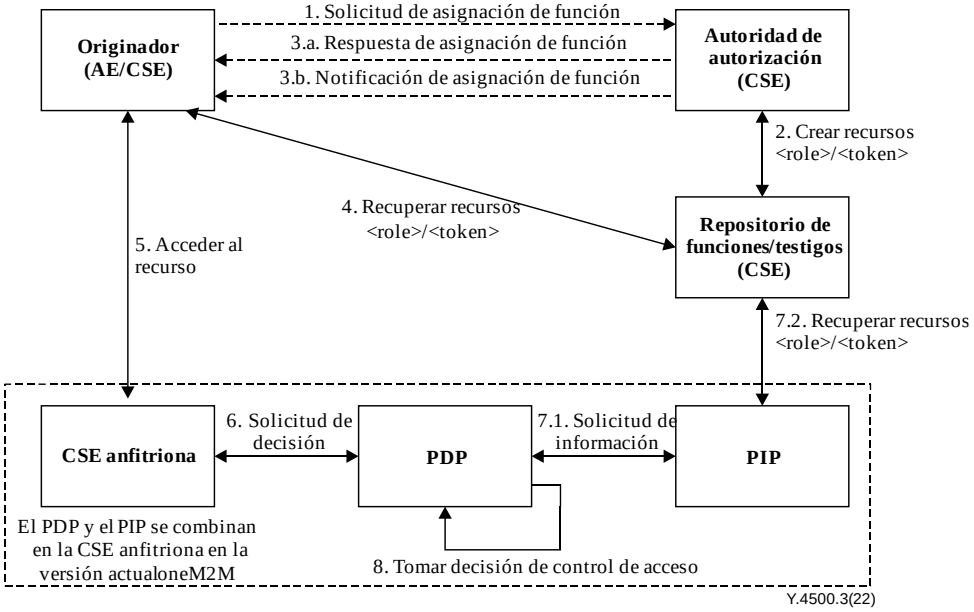


Figura 7.4.1-1 – Arquitectura de control de acceso basada en funciones

El procedimiento general de esta arquitectura se describe como sigue:

Etapa 001: Un originador puede solicitar una función a una Autoridad de autorización. Esta etapa puede no existir en algunas situaciones, por ejemplo, la Autoridad de autorización asigna directamente una función a un originador.

Esta etapa no se precisa en la presente Recomendación.

Etapa 002: La Autoridad de autorización comprobará si el privilegio aplicado puede asignarse al originador. Si está permitido, la Autoridad de autorización deberá crear un recurso <*role*> que especifique la asignación de la función en un repositorio de funciones, o emitir un testigo que contenga la función asignada al originador. El testigo emitido puede almacenarse en un recurso <*token*> en un repositorio de testigos.

Etapa 003: La Autoridad de autorización informa al originador sobre el resultado de la asignación de una función. La información devuelta puede contener un role-ID, un token-ID, un testigo o la información sobre los recursos <role> o <token> creados. Cabe considerar dos casos:

a) Si el originador envía una solicitud de asignación de función a la Autoridad de autorización, esta devuelve el resultado de la asignación de función mediante una respuesta de asignación de función.

b) Si la Autoridad de autorización asigna directamente una función a un originador, esta informa del resultado de la asignación de la función mediante una notificación de asignación de función.

Esta etapa no se precisa en la presente Recomendación.

Etapa 004: El originador puede recuperar las funciones y/o testigos asignados de un Repositorio de funciones y/o testigos utilizando la información proporcionada por una Autoridad de autorización con el fin de obtener información detallada sobre las funciones y/o testigos asignados.

Etapa 005: El originador envía una solicitud de acceso al recurso de destino en la CSE anfitriona. La solicitud puede contener la información de función que pueden ser los role-ID, los testigos o los token-ID.

Etapa 006: La CSE anfitriona puede enviar una solicitud de decisión de control de acceso a un PDP.

Etapa 007: El PDP puede tener que recuperar la información de asignación de función del originador de acuerdo con los role-ID y/o token-ID de los repositorios de función y/o de testigo.

Etapa 008: El PDP verifica las funciones y/o testigos del originador y, a continuación, toma una decisión de control de acceso de acuerdo con las políticas de control de acceso y las funciones.

7.4.2 Procedimiento de emisión de funciones

7.4.2.1 Introducción

Existen dos formas de asignar funciones a un originador.

Una forma es crear un recurso <*role*> que describa la función asignada al originador. Los recursos <*role*> se almacenan en repositorios de funciones desde los que las AE y CSE pueden recuperar los recursos <*role*> para obtener la información de asignación de funciones de un originador.

Otra forma es emitir un testigo que describa la función asignada al titular del testigo (es decir, el originador). El testigo emitido también puede almacenarse en un recurso <t*oken*> en un repositorio de testigos desde el que se puede recuperar el testigo emitido.

Un recurso <*role*> también puede apuntar a un recurso <*token*> en el que se almacena el testigo que contiene la función asignada a través del atributo *tokenLink.*

7.4.2.2 Procedimiento de asignación de funciones

El procedimiento general de asignación de una función a un originador se muestra en la Figura 7.4.2.2-1 y se describe a continuación:

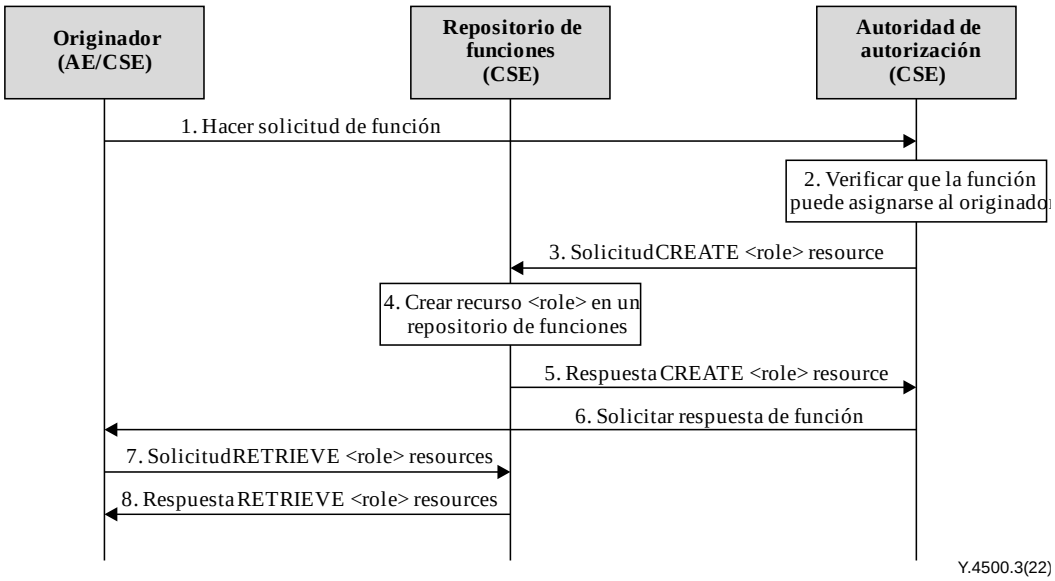


Figura 7.4.2.2-1 – Procedimiento de asignación de funciones

El procedimiento de asignación de funciones es el siguiente:

1 El originador puede enviar una solicitud de asignación de funciones a la autoridad de autorización. Sin embargo, la descripción de esta etapa está fuera del ámbito de aplicación de esta Recomendación.

2 La autoridad de autorización comprobará si la función solicitada puede ser asignada al originador. Una vez realizada la comprobación de autorización de privilegios, la autoridad de autorización asignará la función al originador.

3 La autoridad de autorización enviará una solicitud de creación de recursos <role> al repositorio de funciones.

4 El repositorio de funciones creará un recurso <role> de acuerdo con la solicitud de creación.

5 El repositorio de funciones devolverá el resultado de la creación del recurso <role> a la autoridad de autorización.

6 La autoridad de autorización devolverá el resultado de la asignación de la función al originador. Sin embargo, la descripción de esta etapa queda fuera del ámbito de esta Recomendación.

7 El originador puede enviar una solicitud de recuperación del recurso <role> al repositorio de funciones para obtener la información sobre la asignación de funciones.

8 El repositorio de funciones devolverá al originador el contenido recuperado de los recursos <role>.

7.4.2.3 Emisión de un testigo asociado con una función

El procedimiento general de emisión de un testigo de función (un testigo asociado a una función asignada) a un originador se muestra en la Figura 7.4.2.3-1 y se describe como sigue:

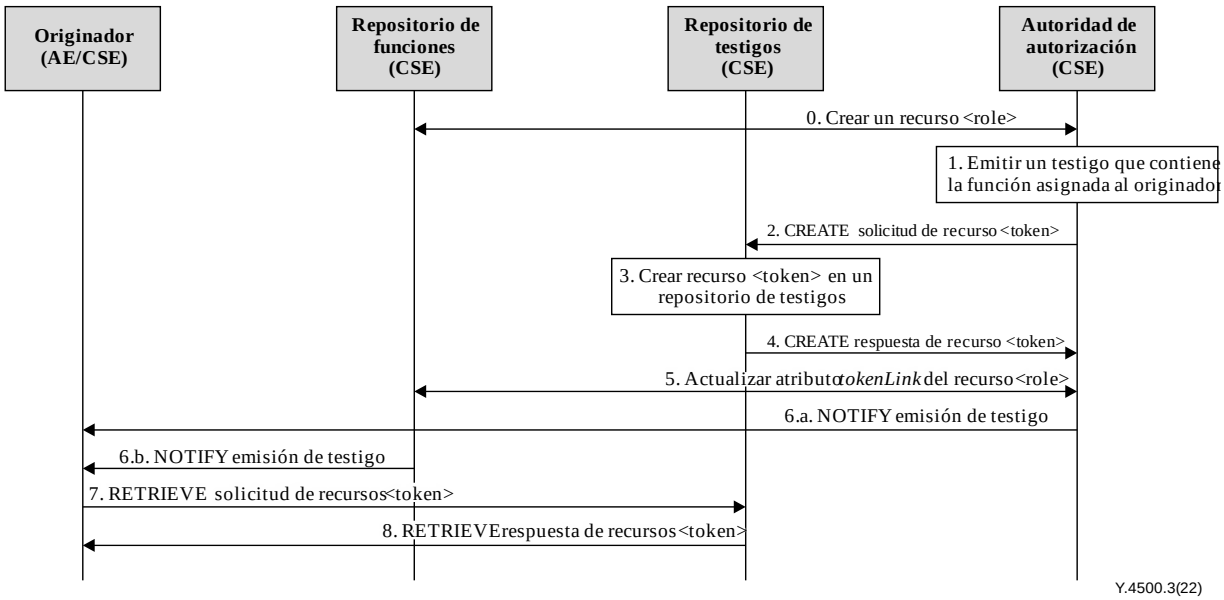


Figura 7.4.2.3-1 – Procedimiento de emisión de testigos de función

El procedimiento de emisión de función es el siguiente:

0 La autoridad de autorización crea un recurso <role> en un repositorio de funciones para una asignación de función.

1 La autoridad de autorización emite un testigo que contiene la función asignada al originador.

2 La autoridad de autorización enviará una solicitud de creación de recursos <token> a un repositorio de testigos.

3 El repositorio de testigos creará un recurso <token> de acuerdo con la solicitud de creación.

4 El repositorio de testigos devolverá el resultado de la creación del recurso <token> a la autoridad de autorización.

5 La autoridad de autorización actualizará el atributo *tokenLink* del recurso <*role*> con la dirección del recurso <*token*>.

6 La información sobre la emisión de testigos se transmitirá al originador. Hay dos maneras de tratar la notificación:

a) La autoridad de autorización utiliza la operación NOTIFY para informar al originador.

b) El repositorio de testigos procede a NOTIFY (notificar) al originador de acuerdo con la suscripción realizada por el originador al recurso <role>.

7 El originador puede enviar una solicitud de recuperación del recurso <*token*> al repositorio de testigos con el fin de obtener la información sobre la emisión de testigos.

8 El repositorio de testigos devolverá al originador el contenido recuperado del recurso <*token*>.

7.4.3 Procedimiento de control de acceso basado en funciones

El procedimiento general para utilizar una función en un proceso de autorización se muestra en la Figura 7.4.3-1 y se describe de la siguiente manera:

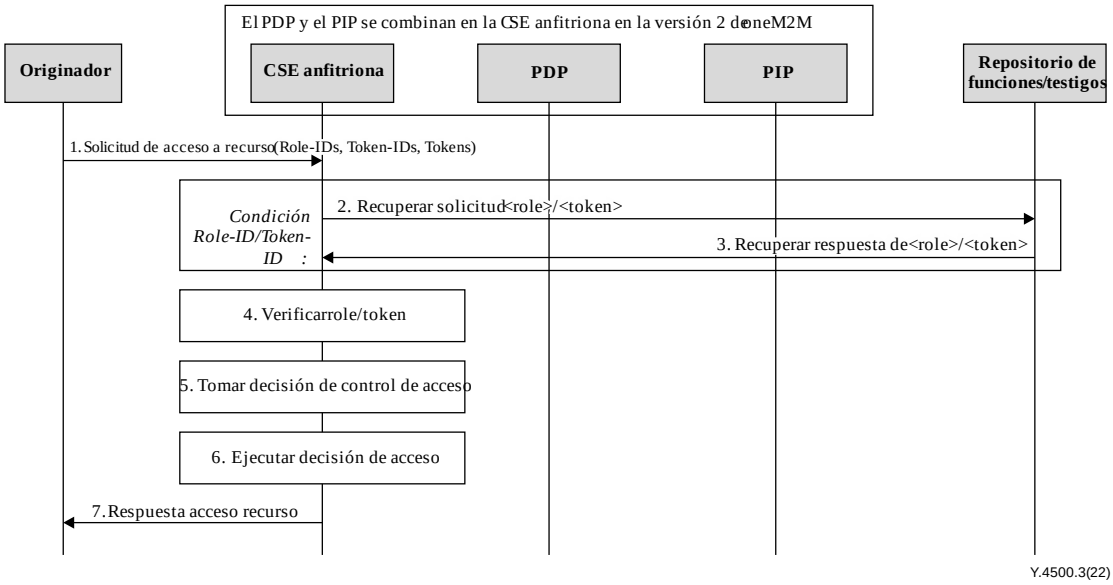


Figura 7.4.3-1 – Procedimiento de control de acceso basado en funciones

1 El originador incluirá los Role-IDs, Token-IDs o testigos pertinentes en la solicitud enviada a la CSE anfitriona.

2 En el caso de los Role-IDs o Token-IDs, la CSE anfitriona (cumpliendo la función de PIP) enviará una solicitud de recuperación de recursos <role> o <token> al repositorio de funciones o testigos.

3 El repositorio de funciones o el repositorio de testigos devolverá los atributos del recurso <role> o <token> a la CSE anfitriona.

4 La CSE anfitriona (cumpliendo la función de PDP) verificará las funciones y/o testigos recibidos; la verificación incluirá: si una función/un testigo es emitido por una autoridad de autorización válida, si el titular de la función/el testigo es el mismo que el originador, y si la función/el testigo sigue siendo válido. Solo se utilizarán funciones/testigos válidos para el control de acceso.

5 La CSE anfitriona (cumpliendo la función de PDP) evaluará la solicitud de acceso del originador utilizando políticas de control de acceso y/o Role-ID para tomar una decisión de control de acceso, como se describe en la cláusula 7.1.

6 La CSE anfitriona ejecutará la decisión de control de acceso, es decir, ejecutará el acceso al recurso en nombre del originador o denegará el acceso al recurso.

7 La CSE anfitriona devolverá al originador el resultado del acceso al recurso.

8 Marcos de seguridad

8.1 Introducción general a los marcos de seguridad

8.1.0 Aspectos generales

Para dar cabida a los diferentes casos de despliegue que se pueden presentar en el marco de las aplicaciones M2M, la presente especificación soporta varios métodos que permiten la provisión y el establecimiento de la seguridad en los sistemas M2M.

8.1.1 Introducción general a los marcos de seguridad de clave simétrica

En los marcos de seguridad de clave simétrica, se aprovisiona a cada par de entidades que necesitan autenticarse mutuamente con su propia clave simétrica compartida. Esto se lleva a cabo mediante el

preaprovisionamiento, por ejemplo, durante la fabricación o el despliegue del dispositivo, o mediante un marco de provisión de seguridad a distancia.

8.1.2 Introducción general a los marcos de seguridad basados en certificados

8.1.2.0 Introducción

Esta cláusula describe la configuración de credenciales y la verificación de certificados utilizada en el marco de establecimiento de asociaciones de seguridad mediante certificados y en el marco de provisión de seguridad a distancia mediante certificados.

8.1.2.1 Tipos de certificados de clave pública

En esta Recomendación se definen los procedimientos que utilizan los siguientes tipos de certificados de clave pública:

Certificados de clave pública bruta:

Descripción: Un certificado de clave pública bruta ([IETF RFC 7250]) contiene solo la clave pública bruta, sin ningún otro tipo de información que normalmente se proporciona en un certificado. El certificado de clave pública bruta se intercambia en la toma de contacto TLS en lugar de un certificado tradicional (véase [IETF RFC 7250]).

Utilización: Un certificado de clave pública bruta puede utilizarse para autentificar una CSE o una AE durante la fase de toma de contacto de seguridad de la asociación del establecimiento de la asociación de seguridad basada en certificados o durante la fase de toma de contacto de inscripción de inicialización del marco de provisión de seguridad a distancia basado en certificados.

Certificados de dispositivo:

Descripción: Estos certificados tienen una cadena de certificados hasta un ancla de confianza e incluyen uno o más identificadores de instancia de hardware globalmente únicos (como los identificadores de dispositivos M2M basados en identificadores de objetos que se tratan en el Anexo H Identificador de dispositivos M2M basado en identificadores de objetos [UIT-T Y.4500.1]) en la extensión subjectAltName del certificado. Se puede utilizar un certificado de dispositivo para verificar la identidad de la instancia de hardware en la que se está ejecutando la entidad.

Utilización: Los certificados de dispositivo pueden utilizarse para autentificar una CSE o AE que se ejecuta en un dispositivo M2M específico. Si el dispositivo M2M es un ASN o MN (que soporta una CSE), entonces el certificado de dispositivo se asocia implícitamente con la CSE que se ejecuta en el dispositivo. Si el dispositivo es un ADN (que no soporta una CSE), entonces el certificado de dispositivo no estará asociado implícitamente a una AE específica que se ejecute en el hardware. Un certificado de dispositivo puede utilizarse para autentificar una CSE de dominio de campo durante la fase de toma de contacto de seguridad de la asociación en el marco de establecimiento de la asociación de seguridad basada en certificados o durante la fase de inicialización del marco de provisión de seguridad a distancia basada en certificados.

Certificados de Node-ID:

Descripción: Estos certificados tienen una cadena de certificados hasta un ancla de confianza e incluyen el identificador de nodo (Node-ID) (véase la Recomendación UIT-T Y.4500.1) en la extensión subjectAltName del certificado. Se puede utilizar un certificado Node-ID para verificar la identidad de un nodo.

Utilización: Se puede utilizar un certificado Node-ID para autentificar una entidad de seguridad en un nodo que actúe en nombre de la CSE y/o de la(s) AE.

Certificados CSE-ID:

Descripción: Estos certificados tienen una cadena de certificados hasta un ancla de confianza e incluyen la representación del nombre de dominio público de un CSE-ID (véase la Recomendación UIT-T Y.4500.1) en la extensión subjectAltName del certificado. Un certificado CSE-ID verifica que la entidad que presenta el certificado tiene asignado un CSE-ID concreto.

Utilización: Un certificado CSE-ID solo puede utilizarse para autentificar una CSE.

Certificados AE-ID:

Descripción: Estos certificados tienen una cadena de certificados hasta un ancla de confianza e incluyen la representación URI completa de un AE-ID en la extensión subjectAltName del certificado. Un certificado AE-ID verifica que la entidad que presenta el certificado tiene asignado un AE-ID concreto.

Utilización: Un certificado AE-ID solo puede utilizarse para autentificar una AE.

Certificados FQDN:

Descripción: Estos certificados tienen una cadena de certificados hasta un ancla de confianza e incluyen el FQDN de una función de inscripción M2M en la extensión subjectAltName del certificado. Un certificado FQDN verifica que la entidad que presenta el certificado tiene asignado un FQDN concreto.

Utilización: Un certificado FQDN se utiliza para autentificar una función de inscripción M2M a un inscrito durante una fase de toma de contacto de inscripción de la inicialización en un marco de provisión de seguridad a distancia mediante certificado

NOTA – Los tipos y los detalles específicos de estos tipos se definen de tal forma que soporten diversos modelos de despliegue, garantizando al mismo tiempo que las entidades oneM2M dispongan de procedimientos claros para autentificar a otras entidades oneM2M que utilizan certificados.

Los perfiles de estos certificados figuran en la cláusula 10.1.1 Perfiles de certificados.

8.1.2.2 Validación del trayecto de certificación y verificación del estado del certificado

Si una entidad tiene que autentificar a otra entidad utilizando un certificado de dispositivo, un certificado CSE-ID, un certificado AE-ID o un certificado FQDN, la entidad deberá realizar una validación básica del trayecto de certificación (sección 6.1 de la norma IETF RFC 5280) como parte de la verificación del certificado de la otra entidad (véase la cláusula 8.1.2.4 Información necesaria para la autentificación de otra entidad mediante certificado).

Los certificados de la CA incluirán las extensiones de restricción de nombres (cláusula 4.2.1.10 Restricciones de nombres de la norma [IETF RFC 5280]) y restringirán los nombres (identificadores de dispositivos M2M basados en identificadores de objetos del Anexo H Identificadores de dispositivos M2M basados en identificadores de objetos [UIT-T Y.4500.1], la representación del nombre de dominio público del CSE-ID, el AE-ID absoluto o los FQDN) que pueden figurar en el certificado posterior utilizado para autentificar a la entidad (certificado de dispositivo, certificado CSE-ID, certificado AE-ID o certificado FQDN, respectivamente).

La cláusula 4.2.1.10 Restricciones de nombre en la norma [IETF RFC 5280] describe la manera en que se utiliza la extensión de restricción de nombre para restringir los URI y los FQDN.

La cláusula 10.4.1.4.2 Perfil para certificados de autoridad de certificación para certificados de dispositivo describe la manera en que se utiliza la extensión de restricción de nombres para restringir los identificadores de dispositivos M2M basados en identificadores de objeto.

La información de anclaje de confianza (cláusula 6.1.1 de la norma [IETF RFC 5280]) se proporciona a la entidad durante la configuración de credenciales, la configuración de asociaciones, la configuración de credenciales de inicialización o la configuración de instrucciones de inicialización.

NOTA 1 – La cláusula 6.1.1 de la norma [IETF RFC 5280] establece que la información de ancla de confianza es confiable porque fue proporcionada al procedimiento de procesamiento del trayecto por algún procedimiento fuera de banda digno de confianza. La configuración de credenciales, la configuración de asociaciones, la configuración de credenciales de inicialización y la configuración de instrucciones de inicialización satisfacen los requisitos de ser procedimientos fuera de banda dignos de confianza.

Verificación del estado de los certificados: En el caso de que una entidad del dominio de la infraestructura reciba un certificado MEF, la entidad verificará el estado del certificado utilizando una lista de revocación de certificados según lo descrito en la norma [IETF RFC 5280]. Se puede establecer una correspondencia entre el Protocolo de Estado de Certificados en Línea (OCSP) y HTTP, como se describe en el Apéndice A de [IETF RFC 6960], aunque actualmente no se ha definido una correspondencia entre OCSP y el protocolo de aplicación restringida (CoAP). Es posible además que el OCSP no sea de fácil aplicación en todos los entornos. Una alternativa puede ser el uso de la extensión de solicitud de estado de certificado TLS (sección 8 de [IETF RFC 6066]; también conocida como grapado OCSP o, de preferencia, la extensión de estado de certificado múltiple ([IETF RFC 6961]), si estuviera disponible.

NOTA 2 – La mayor parte del párrafo anterior se basa en el texto casi idéntico de la especificación CoAP [b-IETF RFC 7252], un protocolo con consideraciones similares (si no idénticas) a los de los despliegues de oneM2M.

8.1.2.3 Configuración de credenciales para marcos de seguridad basados en certificados

Si una entidad debe autentificarse utilizando un marco de seguridad mediante certificados, deberá contar con la siguiente información:

La clave de firma privada de la entidad.

NOTA – Una entidad se autentifica ante otras entidades demostrando que conoce la clave de firma privada que corresponde a una determinada clave de verificación pública.

El certificado de la entidad (y, si procede, la cadena de certificados), tal como se describe en la cláusula 10.1.1 Perfiles de certificados.

En el caso de un certificado CSE-ID, la entidad deberá estar configurada con el CSE-ID de la entidad.

En el caso de un certificado AE-ID, la entidad se configurará con el AE-ID de la entidad.

8.1.2.4 Información necesaria para la autentificación de otra entidad mediante certificado

La entidad A deberá estar configurada para poder confiar en la información que se expone a continuación con el fin de autentificar a la entidad B utilizando el SAEF basado en un certificado:

Una indicación del tipo de certificado de clave pública de otros certificados de la entidad B (es decir, certificado de clave pública bruta, certificado de dispositivo, certificado CSE-ID o certificado FQDN).

Si el certificado de la entidad B es un certificado de clave pública bruta:

Un identificador de clave pública para la clave pública bruta del certificado (véase la cláusula 10.1.2 Identificadores de clave pública).

Si el otro certificado de la entidad B es un certificado de dispositivo, un certificado CSE-ID o un certificado FQDN:

Un identificador globalmente único: El identificador globalmente único para la entidad que también está presente en la extensión subjectAltName del certificado de la otra entidad:

Certificado de dispositivo: Un identificador de instancia de hardware globalmente único (como el identificador de dispositivo M2M basado en identificadores de objeto del Anexo H Identificadores de dispositivos M2M basados en identificadores de objeto [UIT-T Y.4500.1]) que figura en el certificado de dispositivo.

Certificado CSE-ID: La representación del nombre de dominio público del CSE-ID según se define en la Recomendación [UIT-T Y.4500.1].

Información de ancla de confianza: Por lo que se refiere a los certificados de ancla de confianza de la cadena de certificados de la entidad B, véase la cláusula 8.1.2.2 Validación del trayecto y verificación del estado del certificado.

La entidad B se configurará para confiar en la información que se indica a continuación a fin de autenticar a la entidad A mediante el SAEF basado en certificados:

Una indicación del tipo de certificado de clave pública del certificado de la entidad A (es decir, certificado de clave pública bruta, certificado de dispositivo, certificado CSE-ID o certificado AE-ID).

Si el certificado de la entidad A es un certificado de clave pública bruta:

Un identificador de clave pública para la clave pública bruta del certificado (véase la cláusula 10.1.2 Identificadores de clave pública).

Si el certificado de la entidad A es un certificado de dispositivo, un certificado CSE-ID o un certificado AE-ID:

Información de ancla de confianza: para el certificado de ancla de confianza de la cadena de certificados de la entidad A (véase la cláusula 8.1.2.2 Validación del trayecto y verificación del estado del certificado).

Para autenticar la función de inscripción M2M utilizando el RSPF basado en certificados, se configurará un inscrito para que pueda confiar en la información de ancla de confianza de la cadena de certificados de la función de inscripción M2M.

Se configurará una función de inscripción M2M para que pueda confiar en la información que se indica a continuación con el fin de autentificar a un inscrito mediante el RSPF basado en certificados:

Una indicación del tipo de certificado de clave pública del certificado de la entidad B (es decir, certificado de clave pública bruta o certificado de dispositivo).

Si el certificado del inscrito es un certificado de clave pública bruta:

Un identificador de clave pública para la clave pública bruta del certificado (véase la cláusula 10.1.2 Identificadores de clave pública).

Si el certificado del inscrito es un certificado de dispositivo, un certificado CSE-ID o un certificado AE-ID:

Identificador globalmente único: El identificador globalmente único que también está presente en la extensión subjectAltName del certificado del inscrito:

Certificado de dispositivo: Un identificador de instancia de hardware globalmente único (como el identificador de dispositivos M2M basado en identificadores de objeto en el Anexo H Identificadores de dispositivos M2M basados en identificadores de objetos [UIT-T Y.4500.1]) que está presente en el certificado del dispositivo.

Certificado CSE-ID: La representación del nombre de dominio público del CSE-ID según se define en [UIT-T Y.4500.1]

Certificado AE-ID: El AE-ID absoluto asignado a la AE.

Información del ancla de confianza: La certificación del ancla de confianza para la cadena de certificados del inscrito (véase la cláusula 8.1.2.2 Validación del trayecto y verificación del estado del certificado)

8.1.2.5 Verificación de certificados

Esta cláusula describe la manera en que una entidad autentifica a otra entidad en la toma de contacto de seguridad de un marco de seguridad basado en certificados.

El certificado de la otra entidad se recibe durante la toma de contacto de seguridad.

El certificado de la otra entidad se verifica de la siguiente manera:

Si la información del certificado configurada durante la configuración de la asociación o la configuración de la instrucción de inicialización indica que el certificado de la otra entidad es un certificado de clave pública bruta, la entidad verificará que el identificador de clave pública (recibido durante la configuración de la asociación o la configuración de la instrucción de inicialización) corresponde al certificado de clave pública bruta (recibido durante la toma de contacto de seguridad) mediante el proceso descrito en la cláusula 10.1.2 Identificadores de clave pública.

Si la información del certificado configurada durante la configuración de la asociación o la configuración de la instrucción de inicialización indica que el certificado de la otra entidad es un certificado de dispositivo, un certificado CSE-ID, un certificado AE ID o un certificado FQDN, la entidad realizará las siguientes comprobaciones:

La entidad buscará una coincidencia entre el identificador globalmente único descrito en la cláusula 8.1.2.4 Información necesaria para la autentificación de otra entidad mediante certificado (recibido durante la configuración de la asociación o la configuración de la instrucción de inicialización) y los valores de la extensión subjectAltName del certificado de la otra entidad (recibidos durante la toma de contacto de seguridad). Si no hay una coincidencia exacta, la entidad abortará la toma de contacto (D)TLS.

Si se trata de un certificado de dispositivo, el identificador globalmente único es un identificador de instancia de hardware globalmente único (como el identificador de dispositivo M2M basado en identificadores de objeto en el Anexo H Identificadores de dispositivos M2M basados en identificadores de objetos [UIT-T Y.4500.1]). En este caso, la noción de coincidencia depende de la manera en que el identificador de instancia de hardware globalmente único pueda representarse en la extensión subjectAltName.

Si se trata de un certificado CSE-ID, el identificador globalmente único es la representación del nombre de dominio público del CSE-ID tal como se define en la Recomendación UIT-T Y.4500.1, y una coincidencia es un FQDN en la extensión subjectAltName del certificado de la otra entidad que coincide exactamente con la representación del nombre de dominio público del CSE-ID.

Si se trata de un certificado AE-ID, el identificador único global es el AE-ID, y la coincidencia es un URI en la extensión subjectAltName del certificado de la otra entidad que coincide exactamente con el AE-ID absoluto.

En el caso de un certificado FQDN, el identificador único global es el FDQN de la función de autentificación M2M o de la función de inscripción M2M, y una coincidencia es un URI, FQDN o dNSName en la extensión subjectAltName del certificado de la otra entidad que coincida exactamente con el FDQN de la función de autentificación M2M o de la función de inscripción M2M.

La entidad realizará la validación del trayecto y la verificación del estado del certificado utilizando el certificado ancla de confianza como se describe en la cláusula 8.1.2.2 Validación del trayecto y verificación del estado del certificado. Si esta verificación falla, la entidad deberá abortar la toma de contacto (D)TLS.

NOTA – Tras una exitosa toma de contacto de seguridad en la que la otra entidad proporciona una cadena de certificados, la identidad de la otra entidad (recibida durante la configuración de la asociación o la configuración de la instrucción de inicialización) puede asociarse con la información adicional extraída de la cadena de certificados de la otra entidad (por ejemplo, el fabricante de la otra entidad, el propietario de la otra entidad o los criterios de conformidad). Estos detalles no se incluyen en la presente Recomendación

8.1.3 Introducción general al marco gba (arquitectura de inicialización genérica)

La arquitectura de inicialización genérica (GBA) es un marco que podría utilizarse para la provisión de seguridad a distancia. En la Figura 8.1.3-1 se expone el marco GBA.

En el supuesto de que el proveedor de servicios M2M y el operador de la red subyacente hayan acordado utilizar las credenciales de la red subyacente como base para la seguridad entre un servicio de aplicación M2M/nodo intermedio y un nodo de infraestructura (incluido el caso en que el proveedor de servicios M2M y el operador de una red subyacente sean en realidad la misma entidad), se podría utilizar el procedimiento GBA.

Es importante que esta función se utilice únicamente en el marco de un acuerdo adecuado entre el proveedor de servicios M2M y el operador de la red subyacente. El texto normativo para el marco de establecimiento de asociaciones de seguridad basado en GBA (cláusula 8.2.2.2) y el marco de inicialización de seguridad basado en GBA (cláusula 8.3.2.2) asume implícitamente que dicho acuerdo ya existe. Dado que esta Recomendación es una especificación técnica, no se abordan aquí los detalles de dicho acuerdo.

En oneM2M TR-0008 [b-oneM2M TR0008] se incluye una introducción general a la GBA.

Después de una exitosa inicialización de GBA, el servicio de aplicación M2M/nodo intermedio y el BSF comparten una asociación de seguridad que consiste en un identificador de transacción de inicialización (B-TID) y material clave (claves de inicialización de GBA).

Esta asociación de seguridad puede ser utilizada por el servicio de aplicación M2M/nodo intermedio para obtener claves NAF (Ks_(ext/int)_NAF) compartidas entre un servicio de aplicación M2M/nodo intermedio y un nodo de infraestructura M2M o una función de autentificación M2M.

Existen dos modalidades de GBA: GBA basado en ME (GBA_ME) y GBA basado en UICC (GBA_U). En el caso de GBA_ME, se obtiene una clave específica de NAF: la clave Ks_NAF. En el caso de GBA_U, se obtienen dos claves específicas del NAF: Ks_ext_NAF (disponible en el ME) y Ks_int_NAF (que permanece dentro de la UICC).

La GBA_U solo puede realizarse cuando la UICC tiene conocimiento de la GBA.

El BSF determina el modo en el que debe ejecutarse en función de la capacidad de la UICC indicada en la configuración de seguridad del usuario GBA (GUSS).

Se recomienda el uso de GBA_U ya que proporciona un mayor nivel de seguridad que GBA_ME. La implicación de esta recomendación es que la entidad, AE o CSE, que utiliza las claves NAF basadas en GBA_U debe ser residente en la UICC.

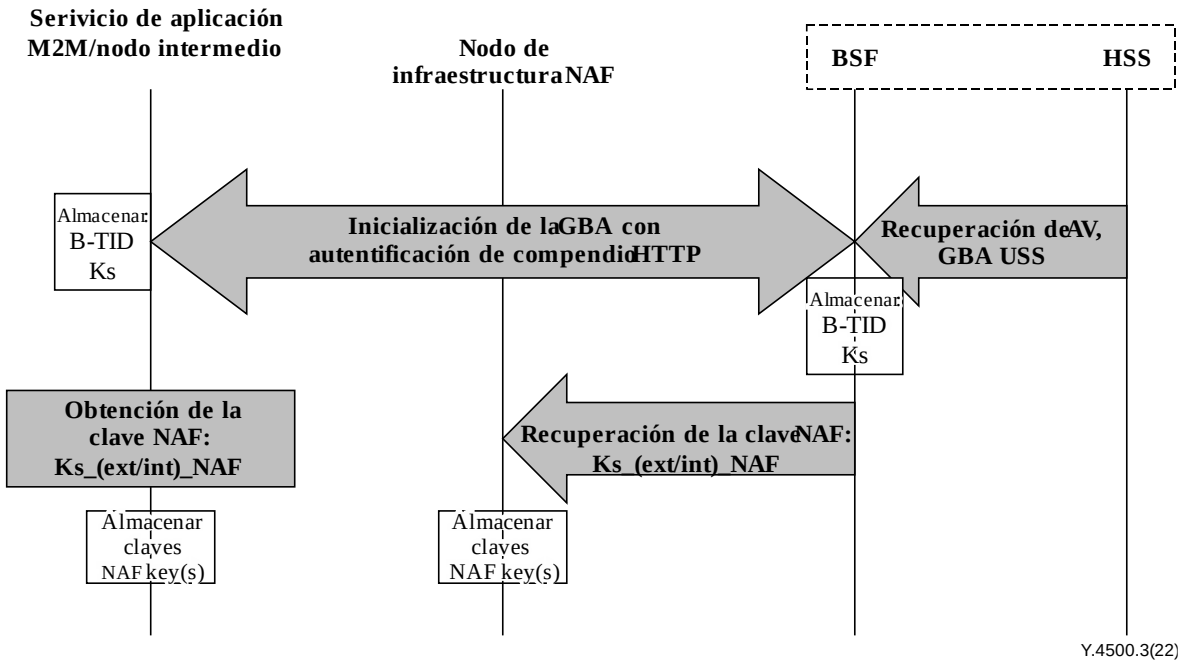


Figura 8.1.3-1 – Marco de la GBA

Nótese que la función de aplicación de red (NAF) puede ser un nodo de infraestructura o una función de autentificación M2M

8.2 Marcos de establecimiento de asociaciones de seguridad

8.2.1 Presentación de los marcos de establecimiento de asociaciones de seguridad

Los marcos de establecimiento de asociaciones de seguridad (SAEF) descritos en esta Recomendación se aplican a las conexiones directas en los puntos de referencia Mcc, Mcc' o Mca.

Los extremos del marco de establecimiento de la asociación de seguridad se indican como:

– La entidad A, que puede ser una AE o una CSE. Esta entidad siempre actúa como Cliente de la asociación de seguridad (sesión TLS/DTLS).

– La entidad B, que deberá ser una CSE. Esta entidad siempre actúa como servidor de la asociación de seguridad (sesión TLS/DTLS).

El sistema oneM2M soporta los siguientes marcos de establecimiento de asociaciones de seguridad:

Marcos de establecimiento de asociaciones de seguridad:

Establecimiento de asociación de seguridad de clave simétrica aprovisionada: Se aprovisiona a las entidades con una clave simétrica: esta se denomina clave simétrica M2M aprovisionada y se conoce como Kpsa. Las entidades se autentifican mutuamente mediante la verificación de los códigos de integridad de los mensajes (MIC) en la toma de contacto de seguridad que se generaron utilizando la clave simétrica. Para más detalles, véase la cláusula 8.2.2.1.

Establecimiento de una asociación de seguridad mediante certificado: Cada entidad recibe:

– una clave de firma privada que solo esa entidad conoce;

– un certificado que contiene la correspondiente clave pública de verificación; y

– una cadena de certificados desde el certificado de la entidad hasta un certificado raíz.

Cada entidad valida el certificado de la otra antes de conceder confianza a las claves públicas de verificación del certificado. En la toma de contacto de seguridad, la entidad A crea una firma digital de los parámetros de la sesión utilizando su clave de firma privada y la entidad B verifica la firma digital utilizando la clave de verificación pública de la entidad A. A continuación, se invierten los

papeles: la entidad B crea una firma digital y la entidad A la verifica. Para más detalles, véase la cláusula 8.2.2.2.

Establecimiento de la asociación de seguridad basada en la función de autenticación M2M (MAF): Este marco de establecimiento de asociaciones de seguridad utiliza la autenticación mutua de la entidad A y la función de autenticación M2M (MAF), y obtiene una clave de conexión segura M2M (Kc) que la MAF proporciona a la entidad B (a través de una comunicación separada mutuamente autenticada). Luego, las entidades se autentican mutuamente utilizando la clave de conexión segura M2M (Kc). Cada una de las entidades A y B puede utilizar credenciales de clave simétrica o certificados para la autenticación mutua con la MAF.

Para obtener una descripción más detallada de los anteriores marcos de establecimiento de asociaciones de seguridad, conviene comparar los siguientes aspectos de los marcos de establecimiento de asociaciones de seguridad.

Configuración de credenciales: Para el marco de establecimiento de asociaciones de seguridad de clave simétrica aprovisionada, la entidad A y la entidad B reciben la clave simétrica M2M aprovisionada que las entidades utilizan posteriormente para autentificarse mutuamente utilizando el preaprovisionamiento o el aprovisionamiento a distancia.

Para los marcos de establecimiento de asociaciones de seguridad basados en certificados, la entidad A y la entidad B son preaprovisionadas con la credencial que la entidad utiliza posteriormente para autenticarse ante la otra entidad utilizando el preaprovisionamiento o el aprovisionamiento a distancia.

Por lo que respecta al marco de establecimiento de asociaciones de seguridad basado en MAF, el procedimiento de configuración de credenciales MAF (cláusula 8.8.3.1) se realiza dos veces: una para aprovisionar credenciales para la autentificación mutua de la entidad A con MAF, y otra para aprovisionar credenciales para la autentificación mutua de la entidad B con MAF.

Configuración de la identidad: La configuración de la identidad puede tener lugar como parte de la configuración de las credenciales, o en un momento posterior.

En relación con el marco de establecimiento de asociaciones de seguridad basado en MAF, la MAF se configura con información sobre las identidades de la entidad B y, opcionalmente, de la entidad A. La cláusula 8.2.2.3 ofrece detalles adicionales.

NOTA 1 – Las especificaciones actuales no indican cómo se configura esta información en la MAF.

El conocimiento por la entidad A de su identidad (IdA) no tiene ningún efecto en el establecimiento de la asociación de seguridad.

La entidad B se configurará con su CSE-ID (IdB) antes de la configuración de la asociación.

Configuración de la asociación: La entidad A recibirá el IdB, el CSE-ID de la entidad B.

NOTA 2 – La presente especificación no describe la manera en que la entidad A recibe el IdB. Entre los ejemplos de mecanismos cabe citar la configuración a través de la gestión a distancia y los mecanismos de descubrimiento soportados por la red o redes subyacentes.

En el caso del marco de autenticación basado en certificados: cada entidad (entidad A y entidad B) se configura adicionalmente con la información del certificado que la entidad utiliza posteriormente para verificar a la otra entidad. La información de certificado necesaria depende del tipo de certificados, cuyos detalles se indican en la cláusula 8.1.2.4 Información necesaria para la autentificación de otra entidad mediante certificado.

En el caso del marco de establecimiento de asociaciones de seguridad basado en la MAF:

La MAF recibe la identidad de la entidad B para la que está autorizada a facilitar el establecimiento de una asociación de seguridad con la entidad A.

La entidad A y la MAF interactúan, utilizando el procedimiento de registro de claves MAF (cláusula 8.8.2.7) para establecer la clave de conexión segura M2M (Kc) y el identificador de clave de conexión segura M2M (KcID) y autorizar a la entidad A a establecer una asociación de seguridad con la entidad B. Esta etapa incluye la autentificación mutua mediante el procedimiento de toma de contacto MAF (cláusula 8.8.2.2). En esta etapa, la entidad A proporciona el IdB a la MAF. Véase la nota 2 más arriba.

Toma de contacto de seguridad de la asociación: Identificación, autentificación y establecimiento del contexto de seguridad entre las entidades:

En el caso del marco de establecimiento de asociación de seguridad basado en la MAF:

La entidad A proporciona el identificador de clave de conexión segura M2M (KcID) a la entidad B.

La entidad B y la MAF interactúan utilizando el procedimiento de recuperación de la clave MAF (cláusula 8.8.2.8). Esta etapa incluye la autentificación mutua mediante el procedimiento de toma de contacto MAF (cláusula 8.8.2.2). La entidad B envía el KcID a la MAF y, si la entidad B está autorizada, la MAF devuelve la clave de conexión segura M2M (Kc) y el IdA o un identificador globalmente único para la credencial utilizada por la MAF para autentificar a la entidad A durante la configuración de la asociación.

La clave de conexión segura M2M (Kc) se utiliza entonces en la toma de contacto de seguridad para la autentificación mutua entre la entidad A y la entidad B.

La entidad A asocia el contexto de seguridad resultante con el IdB: el AE-ID o CSE-ID de la entidad B establecido durante la configuración de la asociación.

La entidad B asocia el contexto de seguridad con uno de los elementos siguientes:

Un único CSE-ID absoluto y la indicación de que la entidad A es una CSE;

Un único AE-ID absoluto y la indicación de que la entidad A es una AE; o

Una lista de valores AE-ID absolutos permitidos y la indicación de que la entidad A es una AE. Este caso se aplica únicamente cuando la entidad A presenta un certificado de dispositivo.

En esta Recomendación se exponen los métodos que permiten a la entidad B determinar el CSE-ID o AE-ID aplicable antes del registro. Estos son:

Si la entidad A se autentifica utilizando un certificado CSE-ID (o un certificado AE-ID), la entidad B extraerá el CSE-ID (o AE-ID, respectivamente) del certificado y asociará el contexto de seguridad con este CSE-ID (o AE-ID, respectivamente), como se describe en la cláusula 10.1.1 Perfiles de certificados.

En todos los demás casos, la entidad B crea un ID de credencial (Credential-ID) globalmente único (véase la cláusula 10.4 Descripción detallada del identificador de credenciales) que identifica la credencial utilizada por la entidad A en el mecanismo de establecimiento de la asociación de seguridad. El identificador de credenciales (Credential-ID) identifica una de las Kpsa (en el caso de un SAEF PSK), un certificado (en el caso de un SAEF basado en un certificado) o la Km (en el caso de un SAEF basado en MAF). Posteriormente, la entidad B determina el CSE-ID o el AE-ID que son aplicables para este Credential-ID.

Si la entidad B asignó el o los AE-ID correspondientes a este Credential-ID, entonces la entidad B se encarga de determinar el o los AE-ID correspondientes a este Credential-ID.

De lo contrario, el CSE-ID o el o los AE-ID puede ponerse a disposición de la entidad B mediante uno de los siguientes métodos. Se prevé que el SP M2M garantice que uno de estos métodos proporcionará con éxito el CSE-ID o el o los AE-ID de la entidad A.

– Si el procedimiento de establecimiento de la asociación de seguridad es facilitado por una función de autenticación M2M, entonces la función de autenticación M2M puede recibir el CSE-ID o AE-ID y la función de autenticación M2M puede proporcionarlo a la entidad B al mismo tiempo que la Kc. La función de autenticación M2M podría haber recibido el CSE-ID o AE-ID durante el aprovisionamiento, incluso en el caso de que la función de autenticación M2M reciba el CSE-ID o AE-ID durante el aprovisionamiento a distancia por una función de inscripción M2M (que es similar al caso descrito en el siguiente punto).
– Si el procedimiento de establecimiento de la asociación de seguridad utiliza una clave simétrica aprovisionada a distancia a la entidad A y a la entidad B, la función de inscripción M2M podrá proporcionar a la entidad B el CSE-ID o el AE-ID durante el procedimiento de provisión de seguridad a distancia.
– Si el proveedor de servicios M2M asigna el(los) identificador(es) de entidad de la entidad A, entonces el CSE-ID o el o los AE-ID pueden ser configurados de forma segura por el proveedor de servicios M2M a la entidad B antes de la toma de contacto de seguridad de la asociación. Por ejemplo, el CSE-ID o el o los AE-ID puede ser configurado como parte de la configuración de credenciales o la configuración de la asociación. Esta especificación permite el uso de otros mecanismos, siempre y cuando dichos mecanismos proporcionen autenticación, protección de la integridad y, opcionalmente, confidencialidad.

EJEMPLO 1: Si el proveedor de servicios M2M puede configurar la entidad B antes del despliegue, podría configurar el CSE-ID o el o los AE-ID a la entidad B en ese momento.

EJEMPLO 2: Podría utilizarse un protocolo de gestión a distancia seguro para configurar la entidad B con los CSE-ID o el o los AE-ID. Sin embargo, esta característica no es actualmente interoperable ya que no existe un objeto de gestión estandarizado que facilite esta gestión.

– Si la entidad A es una AE y la entidad B es una CSE, los AE-ID aplicables pueden obtenerse recuperando los recursos <*serviceSubscribedAppRule*> aplicables a los que está vinculado por el atributo *ruleLinks* del <*serviceSubscribedNode*> de la entidad B en el IN-CSE, como se describe en la cláusula 10.1.1.2.2 Procedimiento de registro de la entidad de aplicación en [UIT-T Y.4500.1].

La Figura 8.2.1-1 resume los tres marcos de establecimiento de asociaciones de seguridad definidos anteriormente.

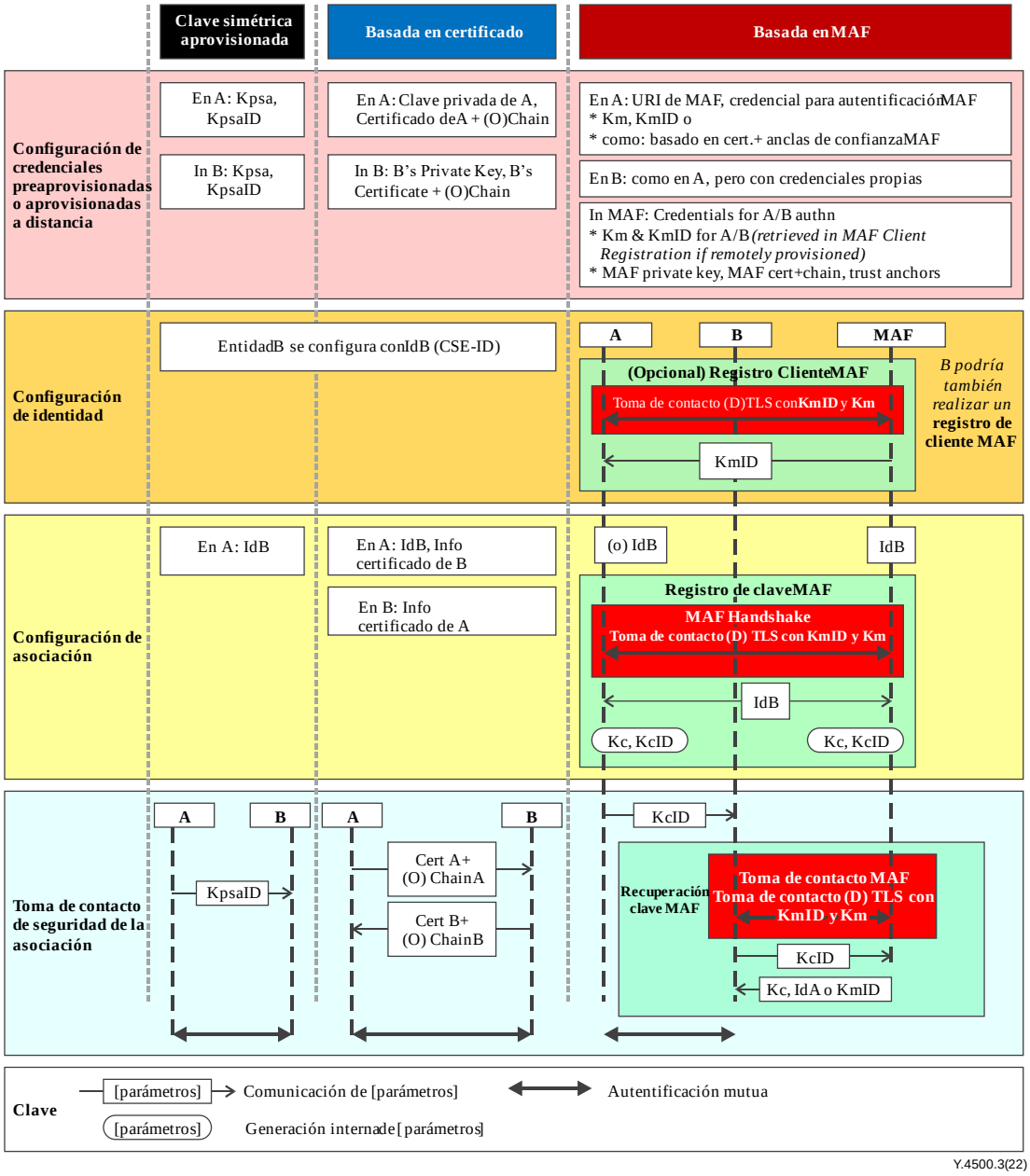


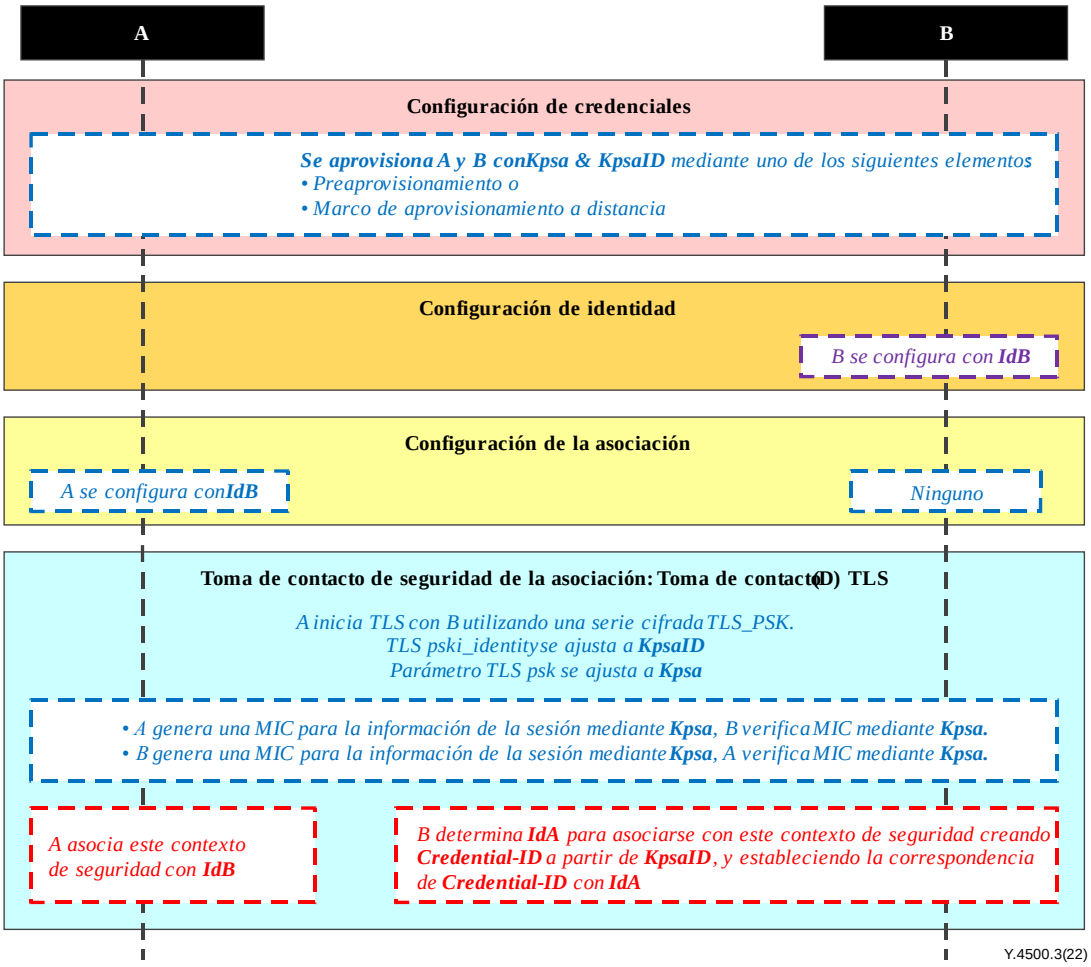
Figura 8.2.1-1 – Presentación de los marcos de establecimiento de asociaciones de seguridad

8.2.2 Descripción detallada de los marcos de establecimiento de asociaciones de seguridad

8.2.2.1 Marcos de establecimiento de asociaciones de seguridad con clave simétrica aprovisionada

Esta cláusula describe el marco de establecimiento de asociaciones de seguridad de clave simétrica aprovisionada. Este marco permite la autentificación mutua de dos entidades que corresponden a dos CSE o a una CSE y una AE. La credencial para este marco es una clave simétrica a largo plazo que se ha aprovisionado a las entidades que se van a autentificar. Esta clave se denomina clave de conexión segura aprovisionada y se conoce como Kpsa. El aprovisionamiento de Kpsa podría ser un preaprovisionamiento o un aprovisionamiento a distancia gracias a los marcos de provisión de seguridad a distancia, como se indica en la cláusula 8.3. Las entidades se autentifican mutuamente verificando los códigos de autentificación de los mensajes en la toma de contacto de seguridad de la asociación que se generaron mediante la clave de conexión segura aprovisionada.

La Figura 8.2.2.1-1 ilustra la secuencia de eventos cuando se utiliza el marco de establecimiento de asociaciones de seguridad de clave simétrica aprovisionada. En esta descripción, la entidad A y la entidad B corresponden a dos CSE o a una CSE y una AE o a una AE y una CSE (respectivamente).



NOTA: Se utilizan los colores de letra siguientes para diferenciar el tema general al que se refiere el texto:

El texto azul en cursiva resalta los detalles específicos de este marco de establecimiento de asociaciones de seguridad en particular.

El texto en cursiva de color morado destaca las acciones técnicas que pueden incluir etapas no especificadas por oneM2M.

El texto rojo en cursiva señala las propiedades relacionadas con la seguridad.

Figura 8.2.2.1-1 – Secuencia de eventos cuando se utiliza el marco de establecimiento de asociaciones de seguridad con clave simétrica aprovisionada

Configuración de credenciales: La clave de conexión segura aprovisionada (Kpsa) y el correspondiente identificador de clave de conexión segura aprovisionada, denominado KpsaID, se aprovisionan a ambas entidades mediante el preaprovisionamiento o el aprovisionamiento a distancia. El formato del KpsaID se define en la cláusula 10.5 Formato del KpsaID. Si la entidad A es una CSE, esa entidad también deberá estar configurada con su CSE-ID (no se muestra en la figura).

Configuración de la identidad: Véase la cláusula 8.2.1

Configuración de la asociación: La entidad A se configurará con la identidad de la entidad B (IdB) antes de realizar la toma de contacto de seguridad de la asociación. La entidad A utilizará esta identidad para la autentificación de la entidad B sobre la base de los argumentos anteriores. Esta identidad también se utiliza para encaminar el intercambio (D)TLS. La entidad A asociará la identidad de la entidad B con los mensajes protegidos dentro de los contextos de seguridad establecidos utilizando la clave de conexión segura aprovisionada Kpsa asociada con el identificador de clave de conexión segura aprovisionada KpsaID.

Si la entidad A es una CSE, la entidad B deberá estar configurada con el CSE-ID de la entidad A antes de realizar la toma de contacto de seguridad de la asociación. Si la entidad A es una AE, entonces la entidad B podrá configurarse con la identidad de la entidad A (IdA) antes de realizar la toma de contacto de seguridad de la asociación, o podrá determinar el IdA durante el registro (creación del recurso <AE>). La entidad B utilizará esta identidad para la autentificación de la entidad A sobre la base de los argumentos anteriores. La entidad B asociará la identidad configurada de la entidad A con los mensajes protegidos dentro de los contextos de seguridad establecidos utilizando la clave de conexión segura aprovisionada Kpsa asociada con el identificador de clave de conexión segura aprovisionada KpsaID.

Toma de contacto de seguridad de la asociación: Las entidades realizarán una toma de contacto (D)TLS-PSK [IETF RFC 4279] con el fin de establecer una sesión segura.

El parámetro psk_identity [IETF RFC 4279] se ajustará al valor del identificador de la clave de conexión segura aprovisionada KpsaID.

Las entidades ajustan el parámetro psk [IETF RFC 4279] al valor de la clave de conexión segura aprovisionada Kpsa.

El perfil de la serie cifrada (D)TLS para el marco de establecimiento de la asociación de seguridad de la clave de conexión segura aprovisionada será conforme a lo establecido en la cláusula 10.2.2.

Tras la exitosa autentificación de la entidad B, la entidad A asociará el contexto de seguridad con el Id B (identificador de entidad de la entidad B) configurado para la entidad A durante la configuración de la asociación.

Tras la exitosa autentificación de la entidad A, la entidad B asociará el contexto de seguridad con un CSE-ID o AE-ID:

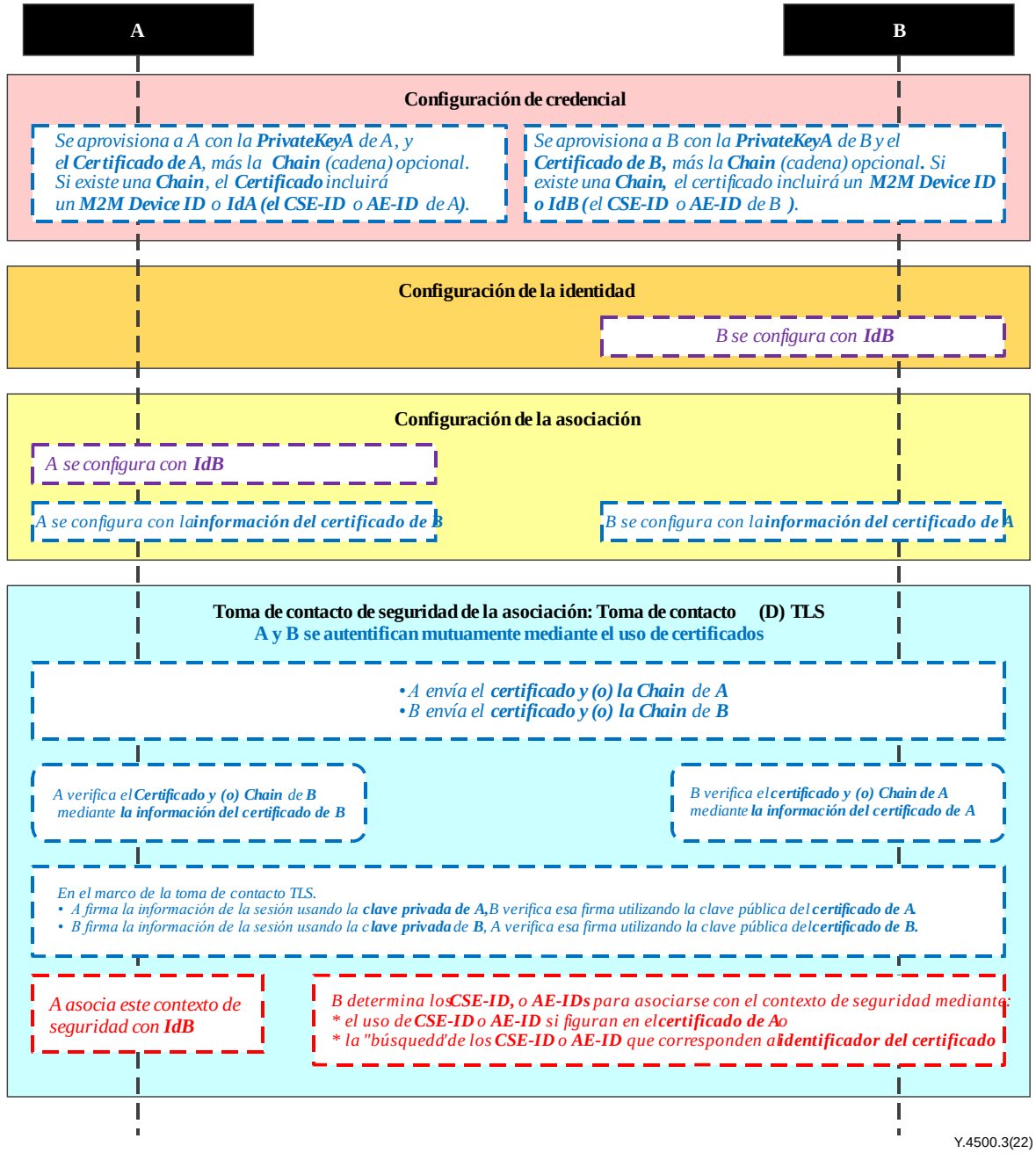
– Si la entidad B ya ha recibido el CSE-ID o el AE-ID correspondiente al KpsaID, la entidad B asociará el contexto de seguridad con ese CSE-ID o AE-ID.

En caso contrario, la entidad B asociará el contexto de seguridad con el Credential-ID creado a partir del KpsaID, tal como se explica en la cláusula 10.4, Descripción detallada del identificador de credenciales. La entidad B determinará entonces el CSE-ID o el AE-ID a partir del ID de credencial, tal como se describe en la cláusula 8.2.1, Presentación de los marcos de establecimiento de asociaciones de seguridad.

8.2.2.2 Marcos de establecimiento de asociaciones de seguridad mediante certificados

Esta cláusula describe el marco de establecimiento de asociaciones de seguridad mediante certificados.

La Figura 8.2.2.2-1 ilustra la secuencia de eventos relativos a la utilización del marco de establecimiento de asociaciones de seguridad basadas en certificados. En esta descripción, la entidad A y la entidad B representan dos CSE o a una CSE y una AE.



NOTA: Se utilizan los colores de letra siguientes para diferenciar el tema general al que se refiere el texto:

El texto azul en cursiva resalta los detalles específicos de este marco de establecimiento de asociaciones de seguridad en particular

El texto en cursiva de color morado destaca las acciones técnicas que pueden incluir etapas no especificadas por oneM2M.

El texto rojo en cursiva señala las propiedades relacionadas con la seguridad.

Figura 8.2.2.2-1 – Secuencia de eventos relativos a la utilización del marco de establecimiento de asociaciones de seguridad basadas en certificados

Configuración de credenciales: Las claves privadas y los certificados de cada entidad se preaprovisionarán como se indica en la cláusula 8.1.2.3 Configuración de credenciales para marcos de seguridad basados en certificados. Si la entidad A es una CSE, la entidad A también se configurará con su CSE-ID (no se muestra en la figura).

Configuración de la identidad: Véase la cláusula 8.2.1.

Configuración de la asociación: La entidad A y la entidad B se configurarán con la información necesaria para la autentificación y la identificación (durante la toma de contacto de seguridad de la asociación) de la entidad B y la entidad A, respectivamente:

La información configurada para la entidad A incluirá los siguientes argumentos:

– Información del certificado de la entidad B: según se describe en la cláusula 8.1.2.4, "Información necesaria para la autentificación de otra entidad mediante certificado".

– Identidad de la entidad B (IdB). La entidad A utilizará esta identidad para la autentificación de la entidad B utilizando los argumentos mencionados. Se utiliza para encaminar el intercambio (D)TLS**.**

NOTA – La entidad A asociará la identidad de la entidad B con los mensajes protegidos dentro de los contextos de seguridad establecidos de acuerdo con la información configurada del certificado de la entidad B.

La información configurada para la entidad B incluirá el siguiente argumento:

Información del certificado de la entidad A: tal como se describe en la cláusula 8.1.2.4 Información necesaria para la autentificación de otra entidad mediante certificado.

Toma de contacto de seguridad de la asociación

Cada entidad verificará el certificado de la otra entidad como se explica en la cláusula 8.1.2.2 Validación del trayecto de certificación y verificación del estado del certificado.

Las entidades se autenticarán mutuamente utilizando los certificados validados, según se especifica en TLS 1.2 [IETF RFC 5246] y DTLS 1.2 [IETF RFC 6347].

El perfil de la serie cifrada (D)TLS para el marco de establecimiento de la asociación de seguridad basada en certificados se conformará con lo dispuesto en la cláusula 10.2.3.

Tras la exitosa autentificación de la entidad B, la entidad A asociará el contexto de seguridad con el IdB (identificador de entidad de la entidad B) configurado para la entidad A durante la configuración de la asociación.

Tras la exitosa autentificación de la entidad A, la entidad B asociará el contexto de seguridad con un CSE-ID, un AE-ID o una lista de AE-ID permitidos:

– Si la entidad A establece un contexto de seguridad presentando un certificado CSE-ID, la entidad B asociará el contexto de seguridad con el CSE-ID del certificado.

– Si la entidad A establece un contexto de seguridad presentando un certificado de AE-ID, la entidad B asociará el contexto de seguridad con el AE-ID absoluto del certificado.

– Si la entidad A establece un contexto de seguridad presentando un certificado de dispositivo, la entidad B asociará el contexto de seguridad con el Credential-ID creado a partir del identificador de instancia de hardware globalmente único que figura en el certificado, tal como se describe en la cláusula 10.4, Descripción detallada del identificador de credenciales. A continuación, la entidad B utilizará el Credential-ID para determinar el CSE-ID, el AE-ID o la lista de AE-ID permitidos, tal como se describe en la cláusula 8.2.1 Presentación de los marcos de establecimiento de asociaciones de seguridad.

– Si la entidad A establece un contexto de seguridad presentando un certificado de clave pública bruta, la entidad B asociará el contexto de seguridad con el Credential-ID creado a partir del correspondiente identificador de clave pública descrito en la cláusula 10.1.2 Identificadores de clave pública. Después, la entidad B utilizará el Credential-ID para determinar el CSE-ID o el AE-ID, tal como se describe en la cláusula 8.2.1 Presentación de los marcos de establecimiento de asociaciones de seguridad.

8.2.2.3 Marcos de establecimiento de asociaciones de seguridad de clave simétrica basados en MAF

Esta cláusula describe el marco de establecimiento de asociaciones de seguridad basado en MAF.

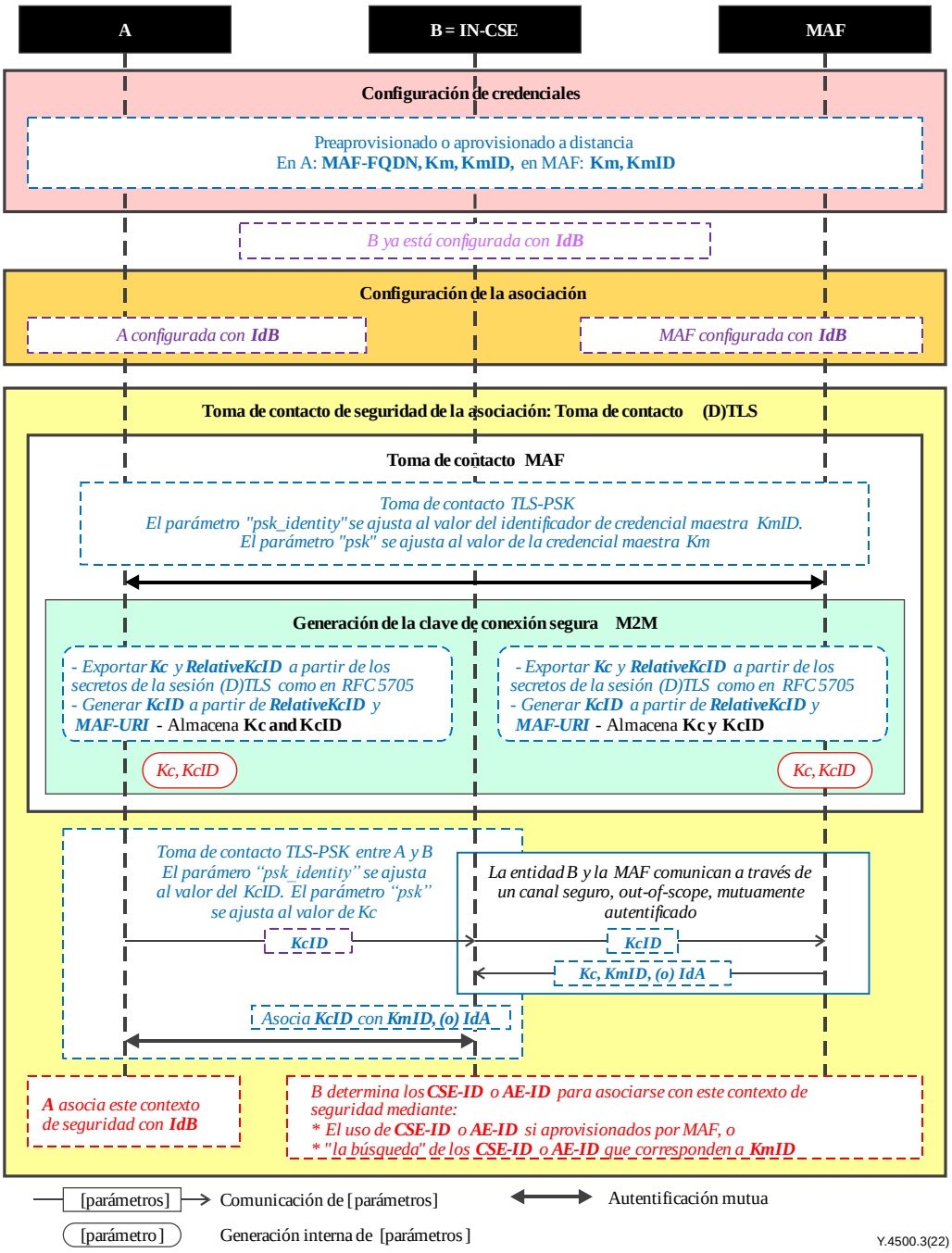
Este marco utiliza los procedimientos del marco de seguridad MAF de la cláusula 8.8, con la siguiente correspondencia de funciones:

– La entidad A desempeña la función de extremo de origen.

– La entidad B desempeña la función de extremo de destino.

La presente cláusula se refiere a las entidades mediante la expresión entidad A y entidad B.

La Figura 8.2.2.3-1 muestra la secuencia de eventos relativos a la utilización del marco de establecimiento de asociaciones de seguridad basado en MAF.



NOTA 1: Se utilizan los colores de letra siguientes para diferenciar el tema general al que se refiere el texto:

El texto azul en cursiva resalta los detalles específicos de este marco de establecimiento de asociaciones de seguridad en particular.

El texto en cursiva de color morado destaca las acciones técnicas que pueden incluir etapas no especificadas por oneM2M.

El texto rojo en cursiva señala las propiedades relacionadas con la seguridad.

Figura 8.2.2.3-1 – Secuencia de eventos relativos a la utilización del marco de establecimiento de asociaciones de seguridad basado en MAF

Configuración de credenciales: La entidad A (y la entidad B, respectivamente) se aprovisionarán individualmente con credenciales para la autentificación mutua con la MAF, como se describe en la cláusula relativa a la configuración de credenciales de la MAF (cláusula 8.8.3.1). Puede aplicarse el preaprovisionamiento o el aprovisionamiento a distancia. En el caso del aprovisionamiento a distancia de claves simétricas, la MAF recupera las claves simétricas de la MEF durante el procedimiento de registro del cliente MAF en la configuración de la identidad.

Configuración de la identidad: Se prevé que la MAF tenga autorización para prestar servicio a la entidad A y a la entidad B.

NOTA 1 – En las especificaciones actuales del sistema oneM2M no se indica cómo se proporciona esta autorización a la MAF.

La MAF se configura con información sobre las identidades de la entidad B y, opcionalmente, de la entidad A:

Si la entidad A es una CSE, se espera que la MAF esté configurada con el CSE-ID de la entidad A (denominado IdA).

Si la entidad A es una AE, se espera que la MAF esté configurada con el AE-ID de la entidad A (denominado IdA).

Se espera que la MAF esté configurada con el CSE-ID asignado a la entidad B por el proveedor de servicios M2M (denominado IdB).

NOTA 2 – Las especificaciones actuales del sistema oneM2M no indican cómo se configura esta información para la MAF.

Si la entidad A (o la entidad B, respectivamente) se aprovisiona a distancia con una clave simétrica para utilizarla con la MAF, la entidad A (o la entidad B, respectivamente) deberá realizar individualmente el procedimiento de registro del cliente MAF (cláusula 8.8.2.3) con la MAF. Este procedimiento se utiliza para que la MAF a) recupere la Km de la MEF, y b) proporcione al extremo el KmID que se utilizará para la posterior autentificación con la MAF en la etapa 5.

Configuración de la asociación: La entidad A y la MAF se configurarán con la información necesaria para la autentificación e identificación durante la toma de contacto MAF y la toma de contacto de seguridad de la asociación:

Autorización del SAEF: La entidad A deberá recibir el IdB, el CSE-ID de la entidad B.

Se espera que la MAF esté configurada con la identidad de la entidad B (IdB) para la que está autorizada a proporcionar una Kc para un SAEF con la entidad A.

La entidad A y la MAF establecerán un canal seguro mutuamente autentificado para la comunicación utilizando el procedimiento de toma de contacto MAF (cláusula 8.8.2.2), utilizando las credenciales aprovisionadas durante la configuración de credenciales.

La entidad A iniciará el procedimiento de registro de claves MAF (cláusula 8.8.2.7) con la MAF. El registro de la clave MAF incluirá el identificador de uso de seguridad (SUID) asociado con el SAEF basado en MAF y el IdB. Como consecuencia de este procedimiento:

La entidad A y la MAF establecen una clave de conexión segura M2M (Kc) y un identificador de clave de conexión segura M2M asociado (KcID), correspondientes a la clave simétrica de salida y al identificador de clave establecidos por el procedimiento de registro de claves MAF.

La MAF proporciona el periodo de validez de la clave de conexión segura M2M (Kc).

El identificador de uso de seguridad (SUID) limita el ámbito en el que se autoriza el uso de Kc. En este caso, el SUID se utiliza para garantizar que la entidad A utilizará Kc únicamente con el SAEF basado en MAF.

Toma de contacto de seguridad de la asociación: La entidad A iniciará una toma de contacto (D)TLS-PSK con la entidad B, con arreglo a la cláusula 10.2.2.

La entidad A enviará el KcID a la entidad B (nodo de infraestructura) como parámetro psk_identity en una toma de contacto (D)TLS-PSK.

La entidad B reconoce la parte MAF-FQDN del KcID en el parámetro psk_identity, y determina que la correspondiente clave de conexión segura M2M (Kc) se recuperará de la MAF correspondiente. La entidad B ajustará el RelativeKeyID para que sea la parte relativa del KcID.

La entidad B y la MAF llevarán a cabo el procedimiento de recuperación de la clave MAF descrito en la cláusula 8.8.2.8.

NOTA 1 – El procedimiento de recuperación de claves MAF incluye el establecimiento de un canal seguro mutuamente autentificado para la comunicación mediante el procedimiento de toma de contacto MAF (descrito en la cláusula 8.8.2.2), utilizando las credenciales aprovisionadas durante la configuración de credenciales.

La entidad B proporcionará el RelativeKeyID a la MAF. La MAF devuelve a la entidad B el valor de la clave simétrica de salida, el plazo de expiración (expirationTime), el identificador de uso de seguridad (SUID) y la identidad de la entidad A. El valor de Kc se ajustará al valor de la clave simétrica de salida. El periodo de validez de la Kc se ajustará al expirationTime. El SUID limita el ámbito en el que se utilizará Kc. En este caso, el SUID se utiliza para garantizar que la entidad B utilizará Kc únicamente con el SAEF basado en MAF.

NOTA 2 – La asignación del periodo de validez de Kc corresponde a la MAF.

La entidad A y la entidad B completarán la toma de contacto (D)TLS-PSK con el parámetro psk ajustado al valor de la clave de conexión segura M2M (Kc).

Tras la autentificación exitosa de la entidad B, la entidad A asociará el contexto de seguridad con el IdB (identificador de entidad de la entidad B) configurado para la entidad A durante la configuración de la asociación.

Tras la autentificación exitosa de la entidad A, la entidad B asociará el contexto de seguridad con un CSE-ID o AE-ID:

Si la MAF proporcionó a la entidad B un CSE-ID o AE-ID, la entidad B asociará el contexto de seguridad con ese CSE-ID o AE-ID.

En caso contrario, la entidad B asociará el contexto de seguridad con el Credential-ID creado a partir del KmID (proporcionado por la MAF) como se describe en la cláusula 10.4 Descripción detallada del identificador de credenciales. Luego, la entidad B determinará el CSE-ID o el AE-ID a partir del Credential-ID, tal como se describe en la cláusula 8.2.1 Presentación de los marcos de establecimiento de asociaciones de seguridad.

La entidad A y la entidad B pueden establecer una nueva toma de contacto (D)TLS-PSK utilizando Kc en cualquier momento dentro del periodo de validez de Kc. Una vez que expire este periodo, la entidad B suspenderá la toma de contacto (D)TLS-PSK, lo que indicará a la entidad B que es necesario realizar una nueva toma de contacto MAF.

8.3 Marcos de provisión de seguridad a distancia

8.3.1 Visión general de los marcos de provisión de seguridad a distancia

8.3.1.1 Objetivo de los marcos de provisión de seguridad a distancia

Los marcos de provisión de seguridad a distancia (RSPF) proporcionan credenciales a una parte inscrita, que es una entidad principal de seguridad en un nodo, una CSE o una AE, como parte de la inscripción de dicha parte en un SP M2M o habilitador de confianza M2M. La MEF tiene lugar en nombre de las *partes interesadas administradoras*, en particular SP M2M o habilitadores de confianza M2M de terceros (MTE). Una parte interesada administradora autoriza al proveedor de

servicio MEF a prestar servicios a los clientes de la MEF y supervisa la autorización de la gestión de credenciales.

Las credenciales son:
Una clave simétrica compartida por la parte inscrita y un objetivo de inscripción, que puede ser una MAF, un nodo, una CSE o una AE.

Si el objetivo de la inscripción es una MAF, la credencial puede utilizarse para opciones de protección SAEF basada en MAF, ESPrim basada en MAF y ESData basada en MAF, con la clave simétrica proporcionada utilizada para la autentificación mutua de la parte inscrita y la MAF.

Si el objetivo de la inscripción es un nodo, una CSE o una AE, la credencial sólo puede utilizarse para una de las opciones de protección SAEF basada en PSK, ESPrim basada en PSK o ESData basada en PSK. La clave simétrica proporcionada se utiliza para la autentificación mutua de la parte inscrita y el otro nodo, CSE o AE.

NOTA 1 – Este caso únicamente es aplicable si cabe esperar que la parte inscrita requiera una clave simétrica con un número relativamente reducido de CSE o AE.

Con respecto a los certificados para los que la parte inscrita conoce la clave privada correspondiente, y un conjunto de puntos de anclaje de confianza para autentificar la MAF del M2M SP o el MTE u otras entidades inscritas con el M2M SP o el MTE, esas credenciales pueden utilizarse para:

Garantizar la comunicación directa con otros nodos o CSE o AE mediante un SAEF basado en certificados, un establecimiento directo de claves con funcionalidad de extremo a extremo mediante certificados (ESCertKE), y opciones de protección ESData mediante certificado. Cabe esperar que los otros nodos, CSE o AE se autentifiquen a sí mismos mediante sus propios certificados, vinculados a un certificado CA de punto de anclaje de confianza proporcionado, en esos marcos de seguridad.

Formular opciones de protección SAEF basada en MAF, ESPrim basada en MAF y ESData basada en MAF, con el certificado utilizado para la autentificación de la parte inscrita en la MAF. Cabe esperar que ésta se autentifique mediante su propio certificado vinculado a un certificado CA de punto de anclaje de confianza proporcionado.

Las especificaciones oneM2M también admiten la provisión de credenciales por medio de los mecanismos de configuración de dispositivos especificados en [UIT-T Y.4500.22], incluida la provisión previa, es decir, mediante medios que no sean un marco de provisión de seguridad a distancia. El método de provisión previa puede venir dado por el despliegue de que se trate. En el Anexo D se describe un marco de provisión previa interoperable basado en UICC.

NOTA 2 – Los RSPF se especifican para proporcionar una interfaz interoperable, con objeto de que las entidades del dominio de campo interactúen con una MEF. Se recomienda el uso de los RSPF especificados para las entidades del dominio de campo por haber sido objeto de revisión por expertos en seguridad oneM2M. Los RSPF también pueden ser utilizados por entidades del dominio de infraestructura (nodos, AE, CSE y MAF) para interactuar con una MEF. Cabe esperar que la MEF pueda incluir interfaces "auxiliares" adicionales, no especificadas por oneM2M, a los efectos de coordinación de la información con las partes interesadas administradoras y los proveedores de servicios MAF.

8.3.1.2 Flujo de alto nivel

Una entidad principal de seguridad en un nodo, una AE o una CSE que requiere provisión a distancia se denomina *parte inscrita* o *cliente MEF de origen.* Al proveerse una clave, los nodos, las AE o las CSE, o la función de autentificación M2M con la que la parte interesada va a establecer la clave simétrica se denomina *parte inscrita objetivo o cliente MEF objetivo*.

El sistema oneM2M admite los siguientes métodos de autentificación para marcos de provisión de seguridad a distancia:

Marco de provisión de seguridad a distancia con clave simétrica provista previamente a la parte inscrita: Se provee previamente una clave simétrica a la parte inscrita y la función de inscripción

M2M para autentificación mutua de esas entidades. En la cláusula 8.3.2.1 se proporciona información adicional al respecto.

NOTA 1 – La presente versión de esta especificación sólo admite claves simétricas provistas previamente Las versiones futuras tienen por objeto admitir asimismo la autentificación mediante claves simétricas proporcionadas por otra MEF mediante un RSPF, u otros mecanismos.

Marco de provisión de seguridad a distancia mediante certificados: las funciones de parte interesada y M2M se basan respectivamente en:

– una clave de firma privada que sólo conoce esa entidad;
– un certificado que contenga la correspondiente clave pública de verificación; y
– (en el caso de un certificado de dispositivo, certificado CSE-ID o certificado AE-ID) una cadena de certificados que comprenda el certificado de entidad y un certificado de punto de anclaje de confianza.

El certificado puede proveerse previamente o proveerse en un RSPF mediante los procedimientos de provisión de certificados que figuran en la cláusula 8.3.6. Si una MEF provisiona un cliente de MEF, éste se autentificará con respecto a la MEF utilizando el último certificado provisto por la MEF.

La parte inscrita y la función de inscripción M2M validarán recíprocamente sus certificados antes de aceptar las claves públicas de verificación del certificado. Por medio del intercambio de seguridad, la función de inscripción M2M crea una firma digital de los parámetros de la sesión utilizando su clave de firma privada y la parte inscrita verifica la firma digital mediante la clave de verificación pública de la función de inscripción M2M. Posteriormente, los papeles se invierten, es decir, la parte inscrita crea una firma digital y la función de inscripción M2M la verifica.

En la cláusula 8.3.2.2 se amplía información al respecto.

Marco de provisión de seguridad a distancia basado en GBA: En este caso, la función de inscripción M2M se lleva mediante un servidor de inicialización GBA. Este marco utiliza claves simétricas 3GPP o 3GPP2 para autentificar la parte inscrita y la función de inscripción M2M (que también es una BSF GBA). Los detalles se especifican en 3GPP TS 33.220 [ETSI TS 133 220] y 3GPP2 S.S0109-A [TIA-1098-A]. En la cláusula 8.3.2.3 se amplía información al respecto.

Los marcos de provisión de seguridad a distancia abarcan las siguientes fases:

Configuración de las credenciales de cliente MEF: El cliente MEF y la función de inscripción M2M se proveen con la credencial de inicialización que la entidad utilizará para autentificarse con respecto a la otra entidad. Esta fase también se denomina configuración de credenciales de inicialización.

Frecuencia: Si la credencial es una clave simétrica, eso se dará en una ocasión por asociación entre el cliente MEF y la MEF. Si la credencial es un certificado, se produce en una ocasión por cada cliente MEF.

Configuración de servicio del cliente MEF: El cliente MEF está configurado con el URI de la función de inscripción M2M (con el fin de encaminar los mensajes (D)TLS a la función de inscripción M2M).

Por otro lado, en el caso del marco de provisión de seguridad a distancia basado en certificados:

El cliente MEF está configurado con los certificados CA de los puntos de anclaje de confianza de la función de inscripción M2M que el cliente MEF utilizará para verificar la función de inscripción M2M.

La función de inscripción M2M está configurada con la información del certificado del cliente MEF que la función de inscripción M2M utilizará para verificar el certificado del cliente MEF. La información necesaria del certificado depende de las características del certificado del cliente MEF,

habida cuenta de la información que figura en la cláusula 8.1.2.4 "Información necesaria para la autentificación de certificados de otra entidad".

Frecuencia: ello tiene lugar en una ocasión, por asociación entre el cliente MEF y la MEF.

NOTA 2 – En los casos de RSPF PPSK y RSPF basado en GBA, la configuración de las credenciales del cliente MEF y la asignación del mismo suelen producirse simultáneamente. En el caso de RSPF basado en certificados, la asignación de clientes MEF puede ser independiente de la configuración de credenciales de clientes MEF.

Coordinación de la parte interesada administradora con la MEF (en esta especificación no se proporciona información pormenorizada al respecto). Una parte interesada administradora autoriza a la MEF a prestar servicio a clientes MEF y supervisa la autorización de la distribución de claves simétricas y la gestión de MO en materia de seguridad con respecto a clientes MEF. Esto suele ocurrir antes del procedimiento de toma de contacto de la MEF.

Frecuencia: ello tiene lugar con arreglo a lo solicitado por la parte interesada administradora.

Instrucciones del procedimiento de provisión: El cliente MEF determina implícitamente que debe realizar procedimientos de provisión específicos, o recibe instrucciones explícitas al respecto. A raíz de ello, el cliente MEF inicia el procedimiento de toma de contacto de la MEF y los procedimientos de provisión en el intercambio de inscripciones.

Frecuencia: ello tiene lugar cada vez que el cliente MEF debe iniciar un conjunto de procedimientos de provisión.

Las fases de configuración de servicio del cliente MEF, coordinación de las partes interesadas administradoras con la MEF y establecimiento de instrucciones del procedimiento de provisión constituyen la configuración de las instrucciones de inicialización.

Procedimiento de toma de contacto de la MEF: Identificación, autentificación y establecimiento del entorno de seguridad entre el cliente MEF y la función de inscripción M2M.

Frecuencia: El procedimiento de toma de contacto de la MEF se produce siempre que el cliente MEF es activado mediante las instrucciones del procedimiento de provisión.

Esta fase también se denomina "procedimiento de toma de contacto para la inscripción de inicialización".

Intercambio de inscripciones: Después de que tenga lugar de forma satisfactoria un procedimiento de toma de contacto de la MEF en el RSPF basado en GBA, el cliente MEF y la MEF establecen una clave simétrica que permite generar claves utilizarlas con otras AE, CSE o MAF. No prosigue la interacción entre el cliente MEF y la MEF hasta que vence el periodo de validez de la clave simétrica establecida y tiene lugar inmediatamente un nuevo procedimiento de toma de contacto.

Tras el procedimiento de toma de contacto de la MEF en RSPF basados en PPSK y en certificados, el cliente MEF y la MEF establecen un canal seguro que se utiliza para proteger el intercambio de inscripciones utilizado para proveer credenciales. Dicho intercambio se describe con más detalle en la cláusula 8.3.4. El intercambio de inscripciones puede incluir los siguientes tipos de procedimientos: inscripción de clientes MEF, provisión de claves simétricas, provisión de certificados y configuración de dispositivos. La secuencia de procedimientos de intercambio de inscripciones puede ser controlada mediante el procedimiento de gestión de cliente MEF que se describe en la cláusula 8.3.4 y se especifica pormenorizadamente en la cláusula 8.3.9.

Frecuencia: ello tiene lugar siempre que se inicie mediante las instrucciones del procedimiento de provisión.

Utilización de las credenciales provistas: Dichas credenciales pueden utilizarse en los siguientes tipos de marcos de seguridad:

SAEF basado en certificados, ESPrim y ESData: Los certificados y los puntos de anclaje de confianza configurados se utilizan directamente en marcos de seguridad basados en certificados con los demás nodos, AE o CSE. Los puntos de anclaje de confianza también pueden configurarse de forma independiente, por ejemplo, con arreglo a lo establecido en [UIT-T Y.4500.22].

SAEF basado en PSK, ESPrim y ESData: El cliente MEF de origen y la MEF establecen una clave simétrica de uso restringido, el correspondiente identificador de clave y una lista de clientes MEF de destino autorizados. El cliente MEF de origen proporciona el identificador de clave al cliente MEF de destino en el protocolo de seguridad. Los clientes MEF de destino establecen una conexión segura con la MEF y llevan a cabo el procedimiento de recuperación de clave de la MEF (cláusula 8.3.5.2.8), con objeto de obtener la clave simétrica sujeta a autorización en la MEF.

SAEF basado en MAF, ESPrim y ESData: Si se utilizan certificados para la autentificación con respecto a la MAF, el certificado y los puntos de anclaje de confianza proporcionados durante la inscripción del certificado se utilizan para la autentificación recíproca del cliente MEF y la MAF. Si se utiliza una clave simétrica para dicha autentificación recíproca, el cliente MEF y la MEF establecen una clave simétrica y el correspondiente identificador de clave, con la restricción de su uso con una MAF específica. El cliente MEF (que ahora actúa como cliente MAF) lleva cabo el procedimiento de inscripción de cliente MAF, durante el cual el cliente MEF/MAF proporciona el identificador de clave a la MAF. Ésta establece una conexión segura con la MEF y realiza el procedimiento de recuperación de la clave de la MEF (cláusula 8.3.5.2.8) para obtener la clave simétrica sujeta a autorización en la MAF. Ésta proporciona un KmID para que el cliente MEF/MAF lo utilice en los procedimientos de toma de contacto de la MAF posteriores.

NOTA 3 – Si el objetivo de la inscripción alberga un recurso <ServiceSubscribedAppRule>, las credenciales obtenidas de la función de inscripción M2M o de la función de autentificación M2M deben almacenarse después de que el objetivo de inscripcióin establezca una conexión segura con la parte inscrita. Se genera un valor de ID de credencial en el formato mencionado en la sección 10.4 mediante la credencial utilizada para el establecimiento de una conexión segura y se añade al atributo applicableCredIDs del recurso <ServiceSubscribedAppRule>.

NOTA 4 – Si el identificador de la parte inscrita se obtiene mediante la función de inscripción M2M o la función de autentificación M2M, se almacena en el atributo allowedAEs del recurso <ServiceSubscribedAppRule>.

En la Figura 8.3.1.2-1 se representan las etapas de los marcos de provisión de seguridad a distancia.

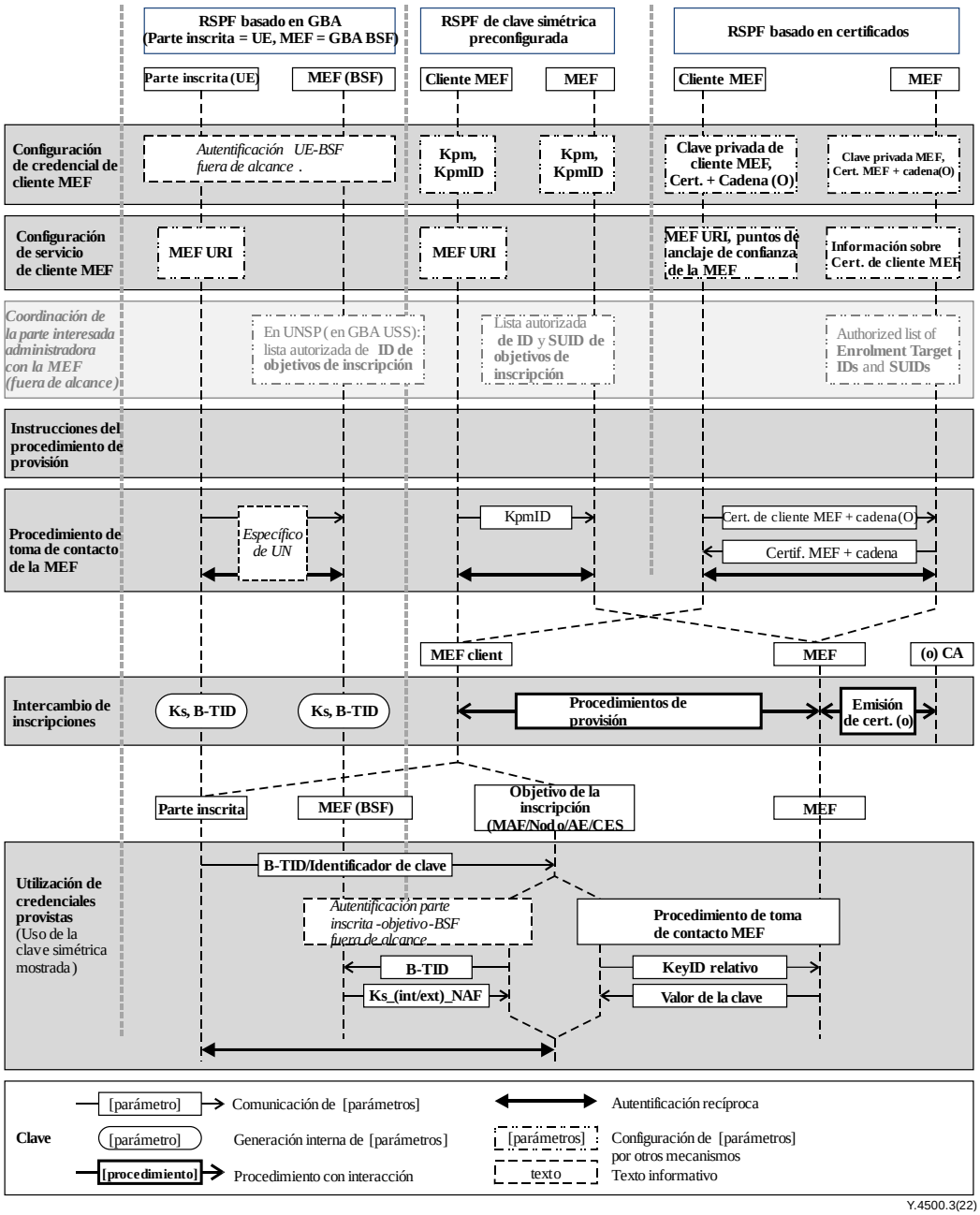


Figura 8.3.1.2-1 – Visión general de los marcos de provisión de seguridad compatibles con oneM2M

8.3.2 Marco de provisión de seguridad a distancia pormenorizado

8.3.2.1 Marco de provisión de seguridad a distancia de clave simétrica preconfigurada

En la presente cláusula se describe el marco de provisión de seguridad a distancia de clave simétrica preconfigurada. La credencial de inicialización para dicho marco es una clave simétrica a largo plazo configurada previamente en la función de inscripción de la parte inscrita y M2M; esa clave se denomina clave simétrica preconfigurada de la parte inscrita y se representa mediante las iniciales Kpm.

En la Figura 8.3.2.1-1 se representa la secuencia de eventos al utilizar el marco de provisión de seguridad a distancia de clave simétrica preconfigurada de la parte inscrita.

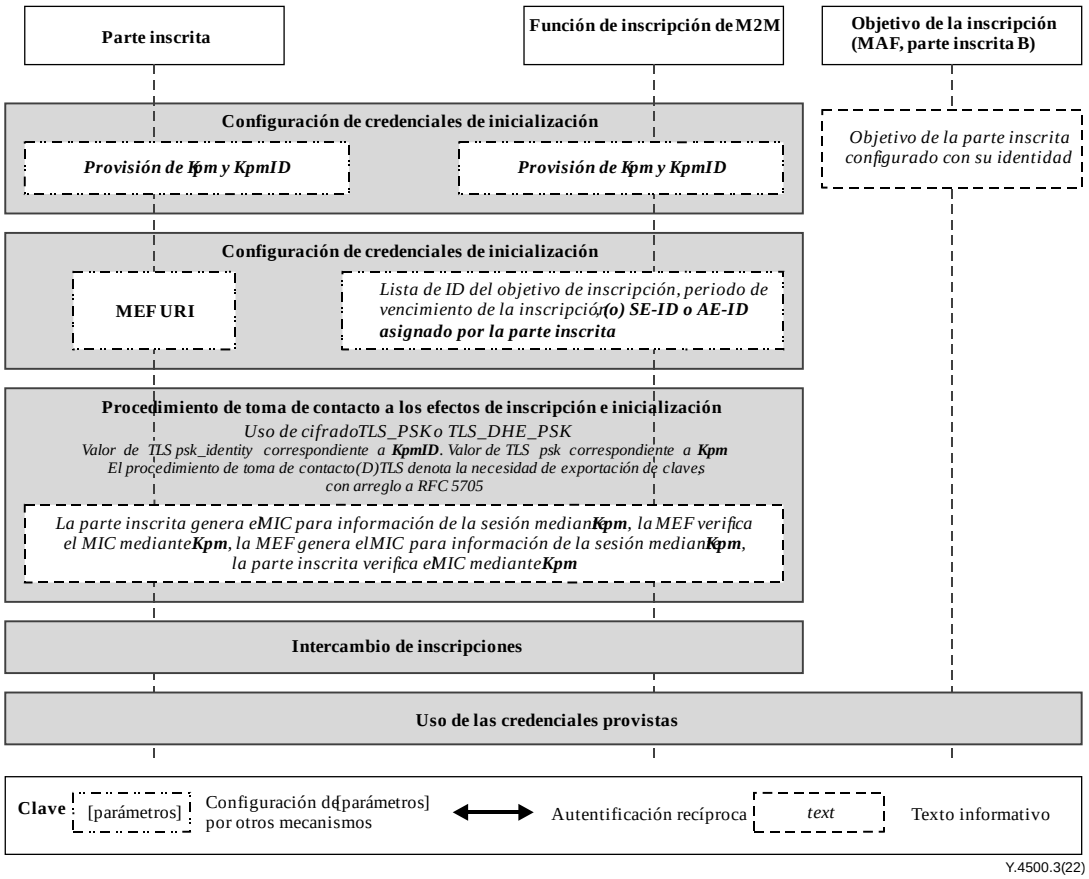


Figura 8.3.2.1-1 – Secuencia de eventos al utilizar el marco de provisión de seguridad a distancia de clave simétrica preconfigurada

Configuración de las credenciales de inicialización: La clave simétrica preconfigurada de la parte inscrita (Kpm) y el correspondiente identificador de clave simétrica preconfigurada de la parte inscrita (KpmID) se configuran previamente para ambas entidades. A la parte inscrita también se proporciona previamente el URI de la función de inscripción M2M (URI MEF), con objeto de encaminar el intercambio (D)TLS.

NOTA 1 – Esta preconfiguración se basa (por definición) en mecanismos no especificados en oneM2M.

Configuración de las instrucciones de inicialización: Las funciones de inscripción de la parte inscrita y M2M se configuran con la información necesaria para aprobar la provisión a distancia:

La parte inscrita se configura con los argumentos siguientes (o los obtiene), a fin de iniciar la provisión a distancia:

Identidad del objetivo de inscripción: identificación del objetivo de inscripción respecto del cual se realiza la provisión para la parte inscrita.

La parte inscrita asocia esos argumentos a la función de inscripción M2M. Dicha función puede identificarse con respecto a la parte inscrita mediante el identificador de clave simétrica de la parte inscrita (KpmID) o el URI de la función de inscripción M2M.

Vencimiento de la inscripción: Periodo de validez aplicable a la clave generada, es decir, el valor Ke que figura en la cláusula 10.7.

La función de inscripción M2M se configura con los argumentos siguientes, a fin de autorizar a dicha función de inscripción M2M a realizar la provisión a distancia a la parte inscrita para un objetivo de inscripción:

Identidad del objetivo de inscripción: identificación del objetivo de inscripción respecto del cual se realiza la provisión para la parte inscrita.

CSE-ID o AE-ID (ID de la parte inscrita) asignado a la parte inscrita. La función de inscripción M2M consiste en proveer esa identidad de entidad para la parte inscrita con el parámetro Km o Kpsa con arreglo al objetivo de inscripción, a tenor de la solicitud del mismo.

La función de inscripción M2M asocia esos argumentos a una parte inscrita. Dicha parte inscrita puede identificarse con respecto a la función de inscripción M2M mediante el identificador de clave simétrica preconfigurada de la parte inscrita (KpmID).

Vencimiento de la inscripción: periodo de validez aplicable a las claves generadas, es decir, el valor Ke. La función de inscripción M2M puede proporcionar ese periodo, así como el valor de Km o Kpsa, al objetivo de inscripción.

Procedimiento de toma de contacto sobre seguridad de inicialización: La parte inscrita y la función de inscripción M2M deben llevar a cabo un procedimiento de toma de contacto (D)TLS-PSK [IETF RFC 4279] a fin de establecer una sesión segura.

El valor del parámetro "psk_identity" [IETF RFC 4279] se fija con arreglo al del identificador de la clave simétrica preconfigurada de la parte inscrita (KpmID).

El valor del parámetro "psk" [IETF RFC 4279] se fija con arreglo al de la clave simétrica preconfigurada de la parte inscrita (Kpm).

El perfil de cifrado (D)TLS se especifica en la cláusula 10.2.2 "Cifrado TLS y DTLS para marcos de seguridad basados en TLS-PSK".

Generación de claves de inscripción: La clave de inscripción (Ke), el parámetro RelativeKeID y la clave de renovación de la autentificación de inscripción (Ker) los generan, mediante una sesión cifrada (D)TLS, la parte inscrita y la función de inscripción M2M por medio de la exportación de claves TLS ([IETF RFC 5705]), tal y como se describe en la cláusula 10.3.1 "Detalles de la exportación de claves TLS".

El identificador de la clave de inscripción (KeID) lo generan, mediante los parámetros RelativeKeID y el FQDN de la función de inscripción M2M, la parte inscrita y la función de inscripción M2M, como se describe en la cláusula 10.3.4 "Generación del KeID".

La parte inscrita y la función de inscripción M2M almacenan la clave de inscripción (Ke) y el identificador de la clave de inscripción (KeID), así como la clave de renovación de la autentificación de la inscripción (Ker).

NOTA 2 – La generación de la clave de inscripción para el marco de provisión de seguridad a distancia de clave simétrica preconfigurada es idéntica a la generación de la clave de inscripción para el marco de provisión de seguridad a distancia basada en certificados.

Intercambio de inscripciones: La parte inscrita debe realizar una petición con arreglo a una cabida útil que incluya los parámetros y valores indicados en el Cuadro 8.3.2.1-1. Dichos parámetros pueden serializarse mediante los formatos XML o JSON, por ejemplo.

Cuadro 8.3.2.1-1 – Petición inicial de la parte inscrita a la MEF

Nombre del parámetro	Valor del parámetro
Indicación de inscripción del certificado	<Verdadero/falso>
Indicación de inscripción de la MAF	<Verdadero/falso>
Indicación de gestión a distancia	<Verdadero/falso>

Estas indicaciones ponen de manifiesto si la parte inscrita está preparada para ejecutar esos procedimientos, bajo petición de la MEF. La parte inscrita enviará la petición al URI de intercambio de inscripciones de la MEF.

La MEF procesará la petición en función de las preferencias de esa parte interesada (véanse las condiciones previas) para determinar el tipo de provisión a la parte inscrita.

NOTA 3 – En la presente especificación no se define ese procesamiento.

Si la parte inscrita no debe ser objeto de provisión a distancia a los efectos de autentificación basada en certificados con objetivos de la parte interesada, la MEF llevará a cabo la etapa 10. Con objeto de aprovisionar a distancia la parte inscrita a los citados efectos de autentificación basada en certificados con objetivos de la parte interesada, la MEF deberá componer una respuesta con arreglo a una cabida útil que incluya los parámetros y valores indicados en el Cuadro 8.3.2.1-3. Dichos parámetros pueden serializarse mediante los formatos XML o JSON, por ejemplo.

Cuadro 8.3.2.1-2 – Respuesta de la MEF a la parte inscrita que activa la inscripción del certificado

Nombre del parámetro	Valor del parámetro
Tipo de instrucción	<Indicación de inscripción de la parte inscrita>
URI	<URI de inscripción del certificado de base>

La MEF enviará la respuesta a la parte inscrita.

Si la MEF encarga a la parte inscrita que realice la inscripción del certificado, dicha parte inscrita deberá llevar a cabo el procedimiento de inscripción de la manera descrita en la cláusula 8.3.3.1.

Tras realizar la inscripción del certificado, la parte inscrita enviará una petición a la MEF para confirmarlo.

Si la parte inscrita no necesita inscribirse a distancia mediante una función de autentificación M2M (MAF), la MEF pasará a la etapa 13. Con objeto de llevar a cabo la inscripción a distancia de la parte inscrita con una MAF, la MEF deberá componer una respuesta con una cabida útil que incluya los parámetros y valores indicados en el Cuadro 8.3.2.1-3. Dichos parámetros pueden serializarse mediante los formatos XML o JSON, por ejemplo.

Cuadro 8.3.2.1-3 – Respuesta de la MEF a la parte inscrita que activa la inscripción a distancia con una MAF

Nombre del parámetro	Valor del parámetro
Tipo de instrucción	Indicación de la inscripción de la MAF
Tipo de credencial	<Indicación de uso de certificados o de clave simétrica a los efectos de autentificación con respecto a la MAF>
URI de inscripción de clave MAF	<URI a través del cual se realiza la inscripción de la clave MAF>
URI de recuperación de clave MAF	URI a través del cual se realiza la recuperación de la clave MAF
URI de inscripción del cliente MAF (Opcional)	URI utilizado para recuperar el KmID asignado por la MAF.
Puntos de anclaje de confianza (Opcional)	Certificados CA de puntos de anclaje de confianza para el certificado MAF
Periodo de validez (Opcional)	Periodo de validez de la clave simétrica compartida con la MAF

La MEF enviará la respuesta a la parte inscrita.

Al recibir ese mensaje, la parte inscrita realizará el procedimiento de inscripción de cliente MAF descrito en la cláusula 8.8.2.4. Dicho procedimiento abarca el "uso de credenciales provistas a distancia".

Una vez finalizado el procedimiento de inscripción de clientes MAF, la parte inscrita enviará un mensaje a la MEF para confirmarlo. Ésta puede retomar la etapa 10 con objeto de llevar a cabo la provisión a la parte inscrita en relación con otra MAF.

Si la parte inscrita no necesita ser aprovisionada a distancia para que el servidor de gestión a distancia establezca contacto con miras a realizar nuevas configuraciones, la MEF pasará a la etapa 15. Con objeto de aprovisionar a distancia a la parte inscrita con respecto al servidor de gestión a distancia, la MEF deberá componer una respuesta con arreglo a una cabida útil que incluya los parámetros y valores indicados en el Cuadro 8.3.2.1-4. Dichos parámetros pueden serializarse mediante los formatos XML o JSON, por ejemplo.

Cuadro 8.3.2.1-4 – Respuesta de la MEF a la parte inscrita para llevar a cabo la provisión de la misma con respecto a un servidor de gestión a distancia

Nombre del parámetro	Valor del parámetro
Tipo de instrucción	<Indicación del servidor de gestión a distancia>
URI	<URI de base del servidor de gestión a distancia>

La MEF enviará la respuesta a la parte inscrita.

La parte inscrita enviará un mensaje a la MEF para acusar recibo de la instrucción. La parte inscrita iniciará el contacto con el servidor de gestión a distancia una vez que concluya la sesión TLS/DTLS con la MEF.

La MEF enviará una respuesta para indicar el final del intercambio de inscripciones.

La MEF concluirá la sesión TLS/DTLS.

Utilización de credenciales provistas a distancia: Si el objetivo de la inscripción es una MAF, se indicará a la parte inscrita que entable contacto con una MAF específica para llevar a cabo la inscripción.

Si se provee a la parte inscrita a distancia con un certificado y puntos de anclaje de confianza durante el intercambio de inscripciones, la parte inscrita puede utilizarlos en protocolos de seguridad con respecto al objetivo de la inscripción. En otros casos, la parte inscrita utilizará el KeID en protocolos de seguridad con respecto al objetivo de la inscripción, como se describe en las demás etapas.

La parte inscrita proporcionará el KeID como identificador de clave simétrica en el protocolo de seguridad.

El objetivo de la inscripción comprobará si posee las credenciales asociadas al KeID y, en el caso de no tenerlas, procederá a obtenerlas de la MEF.

El objetivo de la inscripción está preconfigurado con el FQDN/URL de la MEF y, para establecer una conexión segura utiliza las credenciales PSK o el certificado que también ha sido preconfigurado entre el objetivo de la inscripción y la MEF. Para una parte inscrita B, puede utilizarse a los efectos de autentificación una clave de renovación de autentificación de inscripción (Ker) establecida con la MEF, o a los efectos de autentificación, puede usarse un certificado proporcionado por la MEF.

Si el objetivo de la inscripción desea obtener información de credenciales de la MEF, se formará una petición de recuperación a la MEF con el valor del URI de destino *fetchCredentials*/< KeID>/< *security-usage-identifier* >, siendo < *security-usage-identifier* > el SUID aplicable específicamente a la clave simétrica. El campo *Originator* de la petición de recuperación (por ejemplo, el encabezamiento X-M2M-Origin al utilizarse HTTPS) contiene el ID (AE-ID/CSE-ID/MAF-ID) del objetivo de la inscripción/MAF.

Al recibir la petición de recuperación, la MEF llevará a cabo las acciones siguientes:

La MEF obtiene el KeID del URI de destino. Posteriormente recuperará la clave de inscripción (Ke) para el KeID correspondiente, según el proceso de generación de clave de inscripción definido en la cláusula 8.3.1.2. Si la MEF no puede obtener esta información, se enviará una respuesta de error acorde con lo establecido en la etapa "f)vii".

El ID del objetivo de inscripción se obtiene a través del campo originador incluido en la petición de obtención, y el identificador de uso de seguridad (SUID) se obtiene del URI de destino. La MEF deberá validar si el objetivo de inscripción específico cuenta con la autorización necesaria para obtener credenciales para la parte inscrita con arreglo al identificador de uso de seguridad de que se trate.

Si la validación no se lleva a cabo satisfactoriamente, se enviará una respuesta según lo establecido en la etapa "f)vii". Si la validación se lleva a cabo satisfactoriamente, la clave se generará mediante la clave de inscripción (Ke) obtenida en la etapa f)i', como se menciona en la cláusula 10.3.7.

La MEF determina el ID de la parte inscrita correspondiente al KeID.

El parámetro del periodo de validez de la parte inscrita para el KeID lo establece la MEF. Se trata de un valor preconfigurado que indica el periodo de validez de las credenciales que se proporcionan al objetivo de la inscripción/MAF.

Se compondrá una respuesta con arreglo a una cabida útil que incluya los parámetros y valores indicados en el Cuadro 8.3.2.1-5. Dichos parámetros pueden serializarse mediante los formatos XML o JSON, por ejemplo.

Cuadro 8.3.2.1-5 – Respuesta satisfactoria de la MEF al objetivo de inscripción

Nombre del parámetro	Valor del parámetro
Estado	Verdadero
Credencial	<Clave>
EnroleeID	<Valor del ID de la parte inscrita>
Periodo de validez	<Periodo de validez de la clave generada>

Si se produjera algún error a lo largo de las etapas anteriores, la MEF compondrá una respuesta con los parámetros indicados en el Cuadro 8.3.2.1-6.

Cuadro 8.3.2.1-6 – Respuesta insatisfactoria de la MEF al objetivo de inscripción

Nombre del parámetro	Valor del parámetro
Estado	Falso
ErrorString	<Motivo del fallo>

El objetivo de la inscripción, al recibir las credenciales, las utilizará en el protocolo de seguridad con la parte inscrita.

8.3.2.2 Marco de provisión de seguridad a distancia basado en certificados

En la presente cláusula se describe el marco de provisión de seguridad a distancia basado en certificados. Las credenciales de inicialización para dicho marco son certificados basados en pares de claves asimétricas.

NOTA 1 – Las claves privadas asimétricas de larga duración pueden plantear un riesgo de seguridad si no se protegen adecuadamente, de ahí que convenga almacenarlas en entornos seguros.

La Figura 8.3.2.2-1 muestra la secuencia de eventos relativa a la utilización del citado marco de provisión de seguridad a distancia basado en certificados.

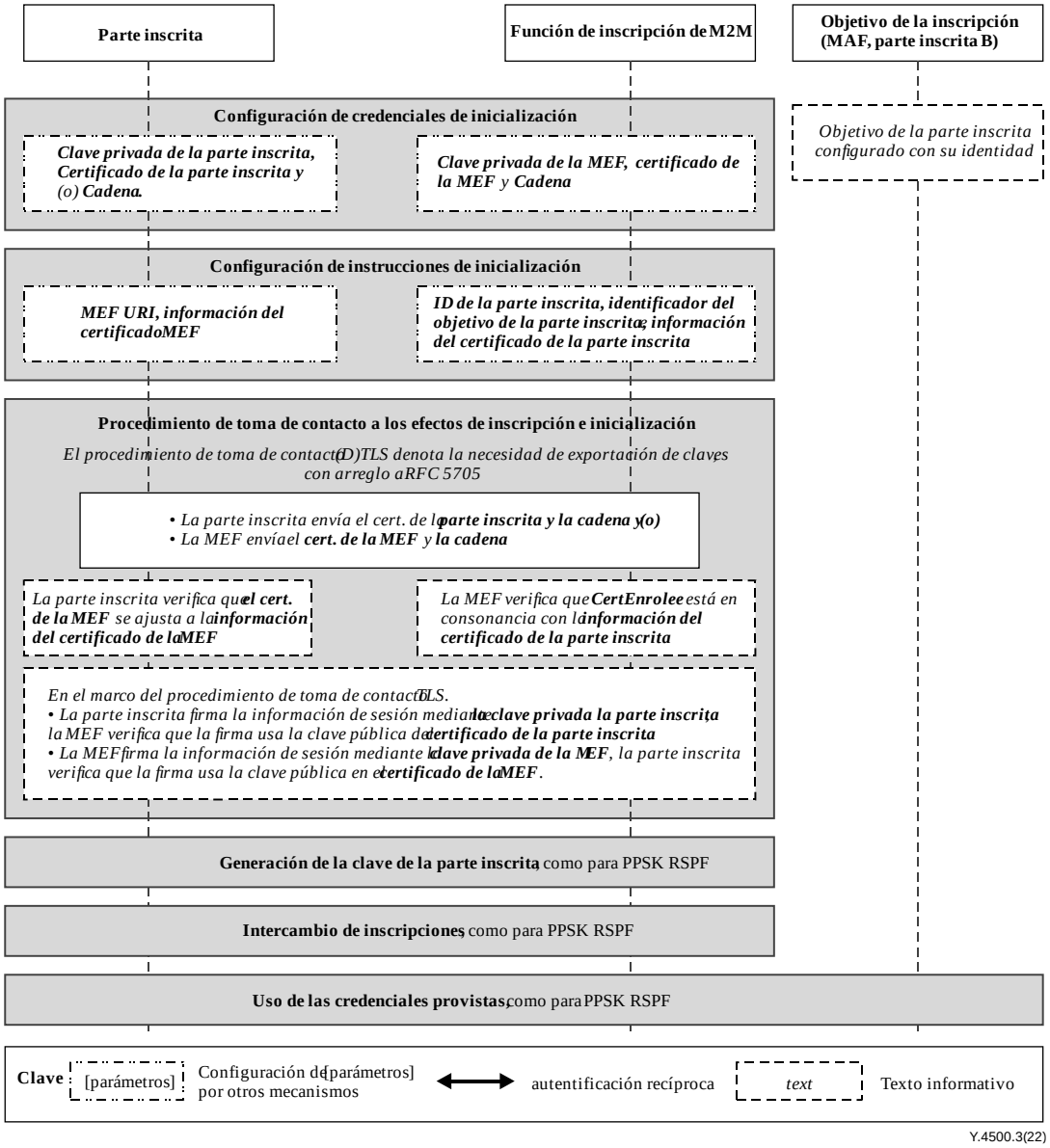


Figura 8.3.2.2-1 – Secuencia de eventos relativa a la utilización de un marco de provisión de seguridad a distancia basado en certificados

Configuración de credenciales de inicialización: Para este marco de provisión de seguridad a distancia, la parte inscrita y la función de inscripción M2M se autentifican de forma recíproca mediante un certificado de clave pública. Las credenciales de inicialización para la parte inscrita y la función de inscripción M2M están preconfiguradas, como se describe en la cláusula 8.1.2.3 "Configuración de credenciales para marcos de seguridad basados en certificados".

NOTA 2 – Cabe realizar la hipótesis de que las identidades de la función de inscripción M2M y del objetivo de inscripción se han configurado antes de esta etapa.

Configuración de la instrucción de inicialización: Además de la información que figura en la cláusula 8.3.1.2, la parte inscrita y la función de enrolamiento M2M se configuran con la información necesaria para autorizar la provisión a distancia:

La parte inscrita se configura con los argumentos siguientes (o los obtiene), a fin de iniciar la provisión a distancia:

Información necesaria para la autentificación del certificado de la función de inscripción M2M mediante un certificado MEF, tal como se describe en la cláusula 8.1.2.4 "Información necesaria para la autentificación del certificado de otra entidad".

La función de inscripción M2M se configura con los siguientes argumentos, que describen la parte inscrita autorizada a llevar a cabo el procedimiento de toma de contacto de seguridad con la función de inscripción M2M:

Información necesaria para la autentificación del certificado de la parte inscrita, tal como se describe en la cláusula 8.1.2.4 "Información necesaria para la autentificación del certificado de otra entidad".

Procedimiento de toma de contacto de seguridad de inicialización: La parte inscrita y la función de inscripción M2M llevan a cabo un procedimiento de toma de contacto (D)TLS, según se detalla en las especificaciones TLS v1.2 [IETF RFC 5246] y DTLS 1.2 [IETF RFC 6347], a fin de establecer una sesión segura.

Cada entidad (parte inscrita y función de inscripción M2M) verifica el certificado de la otra entidad, tal y como se describe en la cláusula 8.1.2.5 "Verificación de certificados".

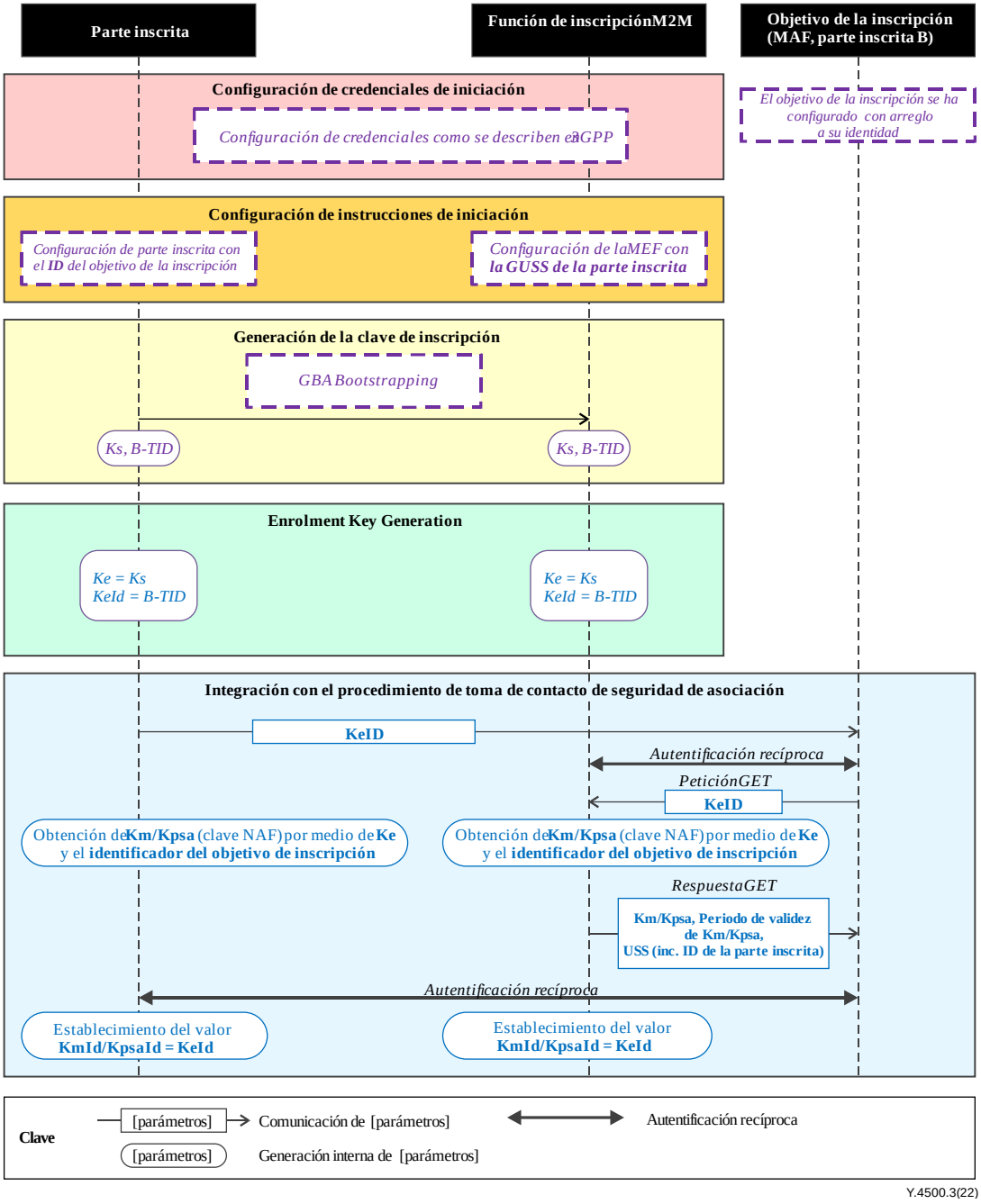
La parte inscrita y la función de inscripción M2M se autentifican recíprocamente mediante los certificados validados, según se detalla en las especificaciones TLS 1.2 [IETF RFC 5246] y DTLS 1.2 [IETF RFC 6347].

El perfil de cifrado (D)TLS se especifica en la cláusula 10.2.3 "Cifrado TLS y DTLS para marcos de seguridad basados en certificados".

Generación de claves de inscripción, intercambio de inscripciones y **utilización de credenciales provistas**: Las etapas son idénticas a las especificadas en "Generación de claves de inscripción", "Intercambio de inscripciones" y la "Utilización de credenciales previstas" en la cláusula 8.3.2.1 "Marco de provisión de seguridad a distancia de clave simétrica preconfigurada".

8.3.2.3 Marco de provisión de seguridad a distancia basado en GBA

Con objeto de compartir una credencial maestra (Km) o una clave de conexión segura configurada (Kpsa) de larga duración entre un servicio de aplicación o un nodo intermedio y un objetivo de inscripción, el servicio de aplicación M2M o nodo intermedio deberá realizar una inicialización GBA satisfactoria y obtener una clave NAF (Ks_(ext/int)_NAF). Dicha clave NAF será la credencial maestra (Km) o la clave de conexión segura configurada (Kpsa).



NOTA: Los siguientes colores de texto destacan el tema general al que se refiere el texto de que se trate: El texto de color negro contiene información pormenorizada independiente del marco de provisión de seguridad a distancia. *El texto de color azul en cursiva destaca los detalles específicos de este marco específico de provisión de seguridad a distancia. El texto de color púrpura en cursiva destaca las medidas de índole técnica que pueden comprender etapas no especificadas por oneM2M.*

Figura 8.3.2.3-1 – Secuencia de eventos relativa a la aplicación del marco de provisión de seguridad a distancia basado en GBA

Configuración de credenciales de inicialización: La configuración de credenciales para la parte inscrita y la función de inscripción M2M (MEF) se describe en la especificación 3GPP TS 33.220 [ETSI TS 133 220]. La MEF desempeña el papel de la BSF. Las credenciales utilizadas para realizar la autentificación recíproca entre la parte inscrita y la MEF guardan relación específica con el UNSP.

Configuración de la instrucción de inicialización: La parte inscrita, la MEF y el objetivo de la parte inscrita deben configurarse con la información necesaria para autorizar la provisión a distancia:

La parte inscrita se configurará con la identidad del objetivo de la inscripción, a saber, mediante la identificación del objetivo de inscripción con respecto al cual debe provisionarse la parte inscrita.

La MEF se configurará con el identificador de la parte inscrita y la identidad del objetivo de la inscripción:

Identidad del objetivo de inscripción: identificación del objetivo de inscripción con respecto al cual debe provisionarse la parte inscrita (autentificada mediante GBA).

CSE-ID o AE-ID (ID de la parte inscrita) asignado a la parte inscrita: la función de inscripción M2M debe proporcionar a esta identidad de entidad relativa a la parte inscrita el Km o Kpsa para el objetivo de la inscripción, cuando éste lo solicite.

La configuración de seguridad del usuario en la GBA (GUSS) permite indicar si la parte inscrita está autorizada a establecer una clave específica de la NAF con el objetivo de inscripción o si la BSF puede distribuir una clave específica de la NAF al objetivo de inscripción.

Procedimiento de toma de contacto para la inscripción de inicialización: El procedimiento de toma de contacto para la inscripción de inicialización permite el establecimiento de una clave de inicialización GBA (Ks) compartida entre la parte inscrita y la MEF con el correspondiente identificador de transacción de inicialización (B-TID) y el periodo de validez de la clave, mediante la etapa de inicialización GBA descrita en 3GPP TS 33.220 [ETSI TS 133 220].

Si una clave de inicialización Ks ya es compartida entre la parte inscrita y la MEF y sigue siendo válida, la etapa de toma de contacto para la inscripción de inicialización no es necesaria. La etapa de generación de la clave de inscripción puede tener lugar con la clave de inicialización Ks existente para la GBA.

Etapa de generación de la clave de inscripción: La clave de inscripción (Ke) será la clave de inicialización referente a la GBA (Ks) establecida durante el procedimiento de toma de contacto relativo a la inscripción de inicialización.

El identificador de clave de inscripción (Ke-ID) será el identificador de transacción de inicialización (B-TID) generado durante el procedimiento de toma de contacto relativo a la inscripción de inicialización.

Integración en el procedimiento de toma de contacto sobre asociación de seguridad: La parte inscrita y el objetivo de la inscripción establecerán la credencial maestra (Km) o la clave de conexión segura configurada (Kpsa) mediante los procedimientos descritos en 3GPP TS 33.220 [ETSI TS 133 220] sobre la base de la clave de inscripción (Ke) como Ks de la clave de inicialización GBA y el identificador de la clave de inscripción (Ke-ID) como B-TID. El objetivo de la inscripción desempeña la función de la NAF.

Configuración [ETSI TS 133 220] de seguridad del usuario de la parte inscrita (USS) de la MEF/BSF:

El FQDN de la NAF, utilizado como parámetro de entrada para generar Ks_(int/ext)_NAF, se configurará de la siguiente manera:

– Si el objetivo de la inscripción es una función de autentificación M2M, el FQDN de la NAF corresponderá al FQDN de la función de autentificación M2M.

– Si el objetivo de inscripción es una CSE, el FQDN de la NAF corresponderá a la representación del nombre de dominio público del CSE-ID, como se define en [UIT-T Y.4500.1].

Para GBA_ME, la clave específica de la NAF será Ks_NAF.

Para GBA_U, las claves específicas de la NAF serán Ks_int_NAF y Ks_ext_NAF.

La credencial maestra (Km) o la clave de conexión segura configurada (Kpsa) será la clave específica de la NAF:

Para GBA_ME, Km/Kpsa = Ks_NAF.

Para GBA_U, Km/Kpsa = Ks_int_NAF si la aplicación HTTP Client reside en la UICC. En caso contrario, Km/Kpsa = Ks_ext_NAF.

La parte inscrita y el objetivo de la inscripción establecerán el identificador de credencial maestra (KmID) o el identificador de clave de conexión segura (KpsaID) con respecto al valor del KeID.

La parte inscrita y el objetivo de la inscripción deberán llevar a cabo el procedimiento de toma de contacto (D)TLS-PSK ([IETF RFC 4279) con la credencial maestra (Km) o la clave de conexión segura configurada (Kpsa) como clave compartida previamente, de conformidad con la cláusula 10.2.2 "Cifrado TLS y DTLS para marcos de seguridad basados en TLS-PSK". Si la UICC se utiliza como entorno seguro compatible con la provisión de seguridad a distancia, se utilizará GBA-U con Km/Kpsa = Ks_int_NAF para la autentificación y el intercambio de claves.

8.3.3 Cláusula dejada en blanco intencionadamente

8.3.4 Intercambio de inscripciones

8.3.4.1 Procedimientos de intercambio de inscripciones

En el marco de un intercambio de inscripciones pueden tener lugar los siguientes procedimientos:

– Procedimientos de inscripción de clientes MEF;

– Procedimientos de provisión de claves simétricas;

– Procedimientos de provisión de certificados;

– Cabe aplicar los procedimientos de configuración de dispositivos que figuran en [UIT-T Y.4500.22], previa interacción de la MEF con un servidor DM e interacción del cliente MEF con el cliente DM en la entidad gestionada;

– Cabe aplicar asimismo procedimientos de control del cliente de la MEF (procedimientos CRUD dirigidos a un recurso < *mefClientCmd*>), que permiten a la MEF controlar la secuencia de los procedimientos de intercambio de inscripciones.

Las cláusulas siguientes describen los mecanismos de activación específicos para cada conjunto de procedimientos. Por otro lado, pueden utilizarse otros mecanismos no especificados por oneM2M, a fin de activar cualquier procedimiento de intercambio de inscripciones, siempre y cuando esos mecanismos proporcionen un grado de seguridad satisfactorio. Cabe destacar al respecto como ejemplos de mecanismos la configuración previa y la configuración manual.

8.3.4.2 Inscripción de clientes respecto de la MEF

Los procedimientos de inscripción de clientes respecto de la MEF se especifican en las cláusulas 8.3.5.2.3, 8.3.5.2.4, 8.3.5.2.5 y 8.3.5.2.6.

Dichos procedimientos de inscripción de clientes sólo pueden realizarse en el marco de un intercambio de inscripciones.

Los procedimientos de inscripción de clientes respecto de la MEF pueden activarse mediante los siguientes mecanismos específicos para oneM2M:

Procedimientos activados mediante la configuración de dispositivos: La configuración de dispositivos que figura en [UIT-T Y.4500.22] puede activar los procedimientos de inscripción de la MEF:

La adición de un MO [*MEFClientRegCfg]* conlleva que el cliente MEF lleve a cabo el procedimiento de inscripción de clientes MEF que figura en la cláusula 8.3.5.2.3.

La supresión de un MO [*MEFClientRegCfg]* conlleva que el cliente MEF interrumpa la correspondiente inscripción de clientes MEF, suprima toda credencial asociada a esa inscripción de clientes MEF y finalice la correspondiente inscripción de clientes MEF en la MEF. Ésta lleva a cabo

la última etapa al aplicar el procedimiento de interrupción de inscripción de clientes MEF que figura en la cláusula 8.3.5.2.6.

8.3.4.3 Provisión de claves simétricas

Los procedimientos de provisión de claves simétricas se especifican en las cláusulas 8.3.5.2.7, 8.3.5.2.8, 8.3.5.2.9 y 8.3.5.2.10.

Dichos procedimientos únicamente pueden aplicarse en el marco de un intercambio de inscripciones.

Estos procedimientos pueden activarse mediante los siguientes mecanismos específicos para oneM2M:

Procedimientos activados mediante control de clientes MEF "MO_Node": La provisión de dispositivos ([UIT-T Y.4500.22]) puede utilizarse para configurar el cliente MEF mediante un MO [*authenticationProfile]* que posea un nodo MO [*MEFClientRegCfg*] de nivel jerárquico inferior para indicar al cliente MEF que se proveerá una clave simétrica para las credenciales aplicadas a dicho MO [*authenticationProfile*]. Si un cliente MEF está sujeto a un control de cliente MEF "MO_NODE" que corresponda a la ruta de dicho MO [*authenticationProfile],* ello puede activar un procedimiento de provisión de claves simétricas acorde con los elementos de información incluidos en el comando de clientes MEF y los valores en curso de los parámetros relativos a estos nodos MO.

NOTA – La aplicación de la configuración de dispositivos para actualizar o suprimir el nodo MO [authenticationProfile] y/o su nodo MO de nivel jerárquico inferior [MEFClientRegCfg] no pone en marcha implícitamente un procedimiento de provisión de claves simétricas. El proceso de actualización o supresión no tendrá efecto hasta que otro mecanismo active algún procedimiento de provisión de claves simétricas.

Procedimientos activados a raíz del vencimiento del periodo de validez de una inscripción de clave de la MEF: Si el cliente MEF ejecuta previamente (de forma satisfactoria) un procedimiento de inscripción de claves MEF bajo el control de un MO [*authenticationProfile]* en el cliente MEF, y el valor temporal en curso es posterior al del parámetro *expirationTime del* recurso [*authenticationProfile],* corresponde aproximadamente al parámetro *expirationTime de la inscripción de* claves MEF más reciente, o rebasa su valor, ello puede conllevar que el cliente MEF realice la inscripción de claves MEF. El criterio para determinar si el valor temporal en curso corresponde aproximadamente al valor de "*expirationTime*" lo determina el cliente MEF.

Procedimientos activados al recibir, en el marco de un protocolo de seguridad oneM2M, un identificador de claves simétricas cuyo FQDN corresponde al FQDN de la MEF. Si un cliente MEF de destino recibe, en el marco de un protocolo de seguridad oneM2M, un identificador de claves simétricas cuyo FQDN corresponde al FQDN de la MEF, ello puede conllevar que el cliente MEF de destino ejecute el procedimiento de recuperación de claves MEF especificado en la cláusula 8.3.5.2.8. Véanse las etapas 6 y 7 que figuran en la cláusula 8.3.5.1.

8.3.4.4 Provisión de certificados

Los procedimientos de provisión de certificados se especifican en la cláusula 8.3.6.

Dichos procedimientos únicamente pueden aplicarse en el marco de un intercambio de inscripciones.

Estos procedimientos pueden activarse mediante los siguientes mecanismos específicos para oneM2M:

Activación de procedimientos mediante el procedimiento de control de clientes MEF: Si el cliente MEF recibe una instrucción de control de cliente MEF que identifica un procedimiento de provisión de certificados, ello conlleva que el cliente MEF ejecute el procedimiento de provisión de certificados mediante los elementos de información incluidos en dicha instrucción de control.

8.3.4.5 Configuración de dispositivos

La configuración de dispositivos se especifica en [UIT-T Y.4500.22].

La configuración de dispositivos puede realizarse en el marco de un intercambio de inscripciones con una MEF, o de una sesión DM con otros servidores DM (de forma independiente al intercambio de inscripciones). En la cláusula 8.3.8 se especifica la configuración de dispositivos en el marco de un intercambio de inscripciones con una MEF.

La configuración de dispositivos puede iniciarse mediante los siguientes mecanismos especificados para oneM2M:

Procedimientos activados mediante un procedimiento de instrucciones de control de clientes MEF: Si el cliente MEF recibe una instrucción de control de cliente MEF que identifica un procedimiento de configuración de dispositivos, ello conlleva que el cliente MEF inicie una sesión de configuración de dispositivos mediante los elementos de información incluidos en dicha instrucción de control.

8.3.4.6 Comando de cliente MEF

Los procedimientos de instrucciones de control de clientes MEF se especifican en la cláusula 8.3.9.

Los procedimientos de instrucciones de control de clientes MEF únicamente pueden aplicarse en el marco de un intercambio de inscripciones.

Los procedimientos de instrucciones de control de clientes MEF pueden activarse mediante los siguientes mecanismos específicos para oneM2M:

Procedimientos activados tras el procedimiento de inscripción de clientes MEF: La obtención de una instrucción de control de clientes MEF se llevará a cabo después de un procedimiento de inscripción de clientes MEF (que no consista en la supresión de un cliente MEF).

Procedimientos activados con arreglo al parámetro *retryDuration*: Si la MEF emite una instrucción de control de clientes MEF NO_MORE_COMMANDS, el parámetro *cmdArgs* incluye a su vez el parámetro *retryDuration,* que proporciona el periodo de tiempo tras el que el cliente MEF intenta obtener la instrucción de control de clientes MEF. El parámetro *retryDuration* se anula siempre que el cliente MEF interactúe satisfactoriamente con la MEF antes de ese periodo de tiempo. En la cláusula.8.3.9.6 se proporciona información adicional.

Procedimientos activados a raíz de un intento de ejecutar una instrucción de control de clientes MEF emitida previamente: Si el cliente MEF ha intentado ejecutar una instrucción de control de clientes MEF emitida previamente, dicho cliente MEF deberá realizar el procedimiento de actualización de la instrucción de control de clientes MEF con objeto de notificar el estado de dicha ejecución. La MEF puede emitir una instrucción de control de clientes ME en su respuesta.

En la Figura 8.3.4.6-1 se representa un ejemplo de procedimiento de instrucción de control de clientes MEF.

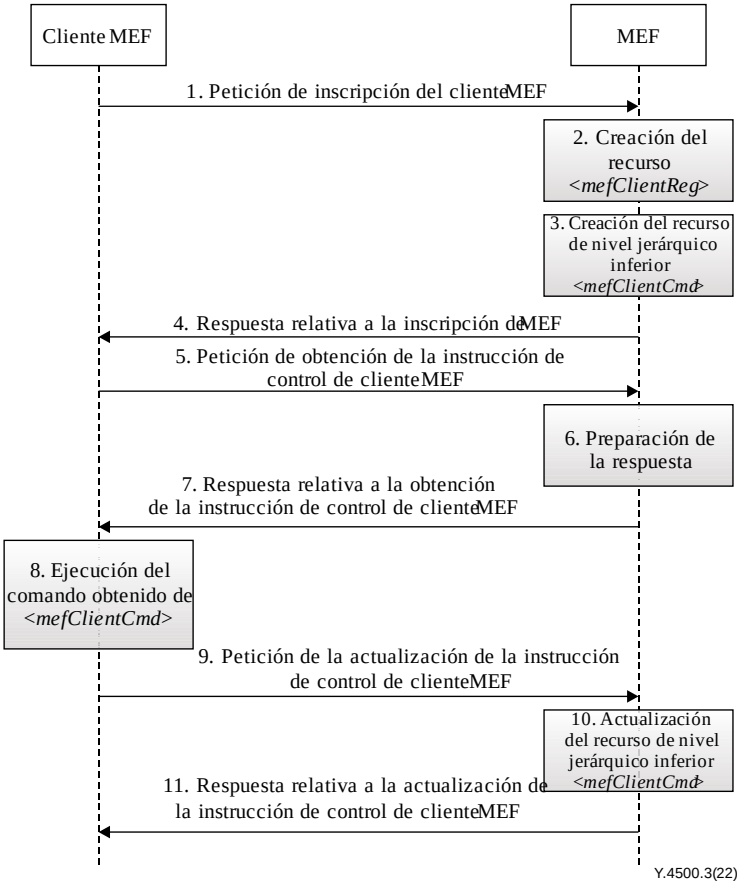


Figura 8.3.4.6-1 – Ejemplo de procedimiento de instrucción de control de clientes MEF

El cliente MEF envía una solicitud de inscripción de clientes MEF.
La MEF crea un recurso < *mefClientReg*>.

Si la MEF desea emitir una instrucción de control de clientes MEF, crea un recurso < *mefClientCmd*> de nivel jerárquico inferior al del recurso < mefClientReg>.

La MEF envía la respuesta de inscripción de clientes MEF que incluye una representación del recurso < *mefClientReg*>, incluida la referencia *childResource*, cuyo valor representa el ID de recurso de un recurso < *mefClientCmd*>.

La presencia de la referencia *childResource* hace que el cliente MEF obtenga el recurso < *mefClientCmd*>. El cliente MEF envía una petición de obtención de la instrucción de control de clientes MEF a la MEF.

La MEF integra la respuesta.

La MEF devuelve una respuesta relativa a la obtención de la instrucción de control de clientes ME que incluye el recurso < *mefClientCmd*>.

El cliente MEF analiza la respuesta recibida y ejecuta la instrucción de control que contiene.

Tras la ejecución de dicha instrucción, el cliente MEF notifica el resultado a la MEF mediante una petición de actualización de la instrucción de control de clientes MEF.

La MEF actualiza el parámetro < *mefClientCmd*>. Si la MEF tiene una nueva instrucción de control para el cliente MEF indicará un activador en la representación del recurso < *mefClientCmd*>.

La MEF envía la respuesta relativa a la actualización de la instrucción de control de clientes MEF. Si la respuesta recibida incluye otra instrucción de control de clientes MEF, se repiten las etapas 8 a 11.

8.3.5 Información pormenorizada sobre la provisión de claves simétricas

8.3.5.1 Introducción

En la cláusula 8.3.5 se describen los detalles y procedimientos comunes con objeto de utilizar un RSPF para proveer claves simétricas.

Esos marcos utilizan una MEF para proveer autentificación y distribución de claves simétricas para su uso por un punto extremo de origen que inicia el establecimiento de la clave simétrica, y uno o más puntos extremos de destino. Véase el Cuadro 8.3.5.1-1 "Asignación de funciones de marco MEF genérico a funciones de marco específico basado en MEF". Los clientes MEF pueden recuperar la clave simétrica de salida de la MEF. Ésta presta sus servicios en nombre de las partes interesadas administradoras, en particular los SP M2M o habilitadores de confianza M2M de terceros (MTE). Una parte interesada administradora autoriza a la MEF a prestar servicios a clientes MEF y supervisa la autorización de la distribución de claves simétricas. En el Cuadro 8.3.5.1-1 se describe la asignación de clientes MEF de origen y clientes MEF de destino a funciones en los marcos específicos basados en MEF, y el número autorizado de clientes MEF de destino.

Cuadro 8.3.5.1-1 – Asignación a marcos de seguridad específicos

Marco de seguridad basado en MEF	Cliente MEF de origen	Cliente MEF de destino	Número de clientes MEF de destino	Clave simétrica de salida
Marcos de seguridad MAF	Cliente MAF	MAF	1	Clave maestra M2M (Km)
Marco para el establecimiento de asociaciones de seguridad (SAEF)	Entidad A	Entidad B	1	Clave de conexión segura M2M (Kc)
Seguridad de extremo a extremo de primitivas (ESPrim)	Originador	Receptor	1	pairwiseESPrimKey
Seguridad de datos de extremo a extremo (ESData)	Extremo ESData de origen	Extremo ESData de destino	1..n	Clave ESData

En la cláusula 8.3.5 se especifican *los procedimientos MEF* entre los clientes MEF y los correspondientes mensajes. El funcionamiento y la gestión de la MEF, más allá de los detalles proporcionados para los procedimientos de la MEF, no se especifican en esta Recomendación.

La secuencia general para utilizar los procedimientos MEF se muestra en la Figura 8.3.5.1-1 y se describe a continuación:

– Cada cliente MEF deberá establecer de forma independiente las credenciales para la autentificación recíproca con la MEF, tal y como se describe en la **configuración de credenciales del cliente MEF** (cláusula 8.3.7.1).

– Cada cliente MEF se configurará de forma independiente para inscribirse en la MEF con una parte interesada administradora específica. La **configuración de inscripción de cliente MEF** (cláusula 8.3.7.2) proporciona los parámetros necesarios.

– Cada cliente MEF deberá realizar un **procedimiento de inscripción de cliente MEF** con la MEF. Ello facilita la confirmación de que el cliente MEF está preparado para utilizar los servicios de la MEF, bajo la autorización de la parte interesada administradora. El cliente MEF deberá inscribirse de forma independiente con respecto a cada parte interesada administradora, aun cuando lo haga a través de una único MEF. Si el cliente MEF se provisiona a distancia a los efectos de autentificación recíproca con la MEF, ésta proporcionará al cliente MEF el KmID que se utilizará para la autentificación posterior con respecto a la MEF.

Ulteriormente, con independencia de esa secuencia de eventos, el **procedimiento de actualización de inscripción del cliente MEF** puede aplicarse para confirmar que el cliente MEF está preparado para utilizar los servicios de la MEF, o establecer una nueva Km y KmID, y el **procedimiento de anulación de inscripción del cliente MEF** puede aplicarse para señalar que dicho cliente MEF deja de utilizar los servicios de la MEF.

El cliente MEF de origen deberá estar configurado para establecer una comunicación segura mediante una función de seguridad (SAEF, ESPrim o ESData) con claves simétricas establecidas a través de la MEF. Los detalles de esta configuración son específicos para la función de seguridad invocada, si bien deberán incluir la **configuración de inscripción de claves MEF** (cláusula 8.4.4.3).

El cliente MEF de origen deberá aplicar un **procedimiento de inscripción de claves MEF** para establecer una clave simétrica y el correspondiente identificador. El cliente MEF de origen también proporcionará el identificador de uso de seguridad (SUID), que limita el alcance de la credencial mediante la identificación de la función de seguridad (SAEF, ESPrim o ESData). Este procedimiento incluirá el **procedimiento de toma de contacto de la MEF** para la autentificación recíproca del cliente MEF de origen y la MEF.

Ulteriormente, con independencia de esa secuencia de eventos, el **procedimiento de actualización de inscripción de la clave MEF** puede aplicarse para actualizar el periodo de validez de la clave inscrita o la lista de clientes MEF de destino, y el **procedimiento de anulación de inscripción de la clave MEF** puede realizarse para suprimir la inscripción de la clave MEF.

El cliente MEF de origen proporcionará a los clientes MEF de destino el identificador de clave simétrica establecido en el procedimiento de inscripción de claves MEF. Los detalles de esta etapa dependen de la función de seguridad identificada por el SUID.

El cliente MEF de destino deberá realizar el **procedimiento de recuperación de la clave MEF** para obtener la clave simétrica y la información correspondiente. Este procedimiento incluirá el **procedimiento de toma de contacto de la MEF** para la autentificación recíproca del cliente MEF de destino y la MEF.

La clave simétrica se utilizará en el protocolo de seguridad entre el cliente MEF de origen y el cliente MEF de destino. Si el protocolo de seguridad requiere una única clave simétrica, se utilizará la primera mitad de la clave simétrica distribuida. Si el protocolo de seguridad requiere dos claves simétricas (por ejemplo, una clave de cifrado y una clave de integridad independiente), se utilizarán ambas mitades de la clave simétrica distribuida como las dos claves simétricas del protocolo de seguridad. Los detalles de esta etapa vendrán dados por la función de seguridad.

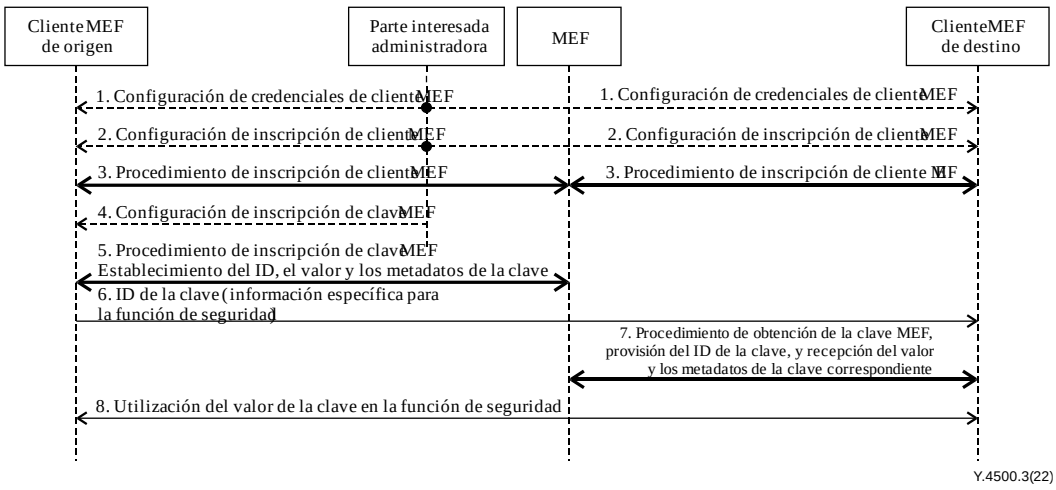


Figura 8.3.5.1-1 – Secuencia de eventos al aplicar el marco de seguridad MEF como parte de una función de seguridad

En la cláusula 8.3.5.2 se describen los flujos de procesamiento e información de los procedimientos MEF. En la cláusula 8.3.7 se describe la información relativa a la configuración de credenciales del cliente MEF, la configuración de inscripción del cliente MEF y la configuración de inscripción de la clave MEF.

8.3.5.2 Marco de seguridad de la MEF: flujos de procesamiento e información

8.3.5.2.1 Introducción

La cláusula 8.3.5.2 especifica los flujos de procesamiento e información de los procedimientos de la MEF.

8.3.5.2.2 Procedimiento de toma de contacto de la MEF

Finalidad: Un procedimiento de toma de contacto de la MEF establece una sesión TLS o DTLS autentificada recíprocamente para garantizar la comunicación entre un cliente MEF y la MEF. En el caso del procedimiento de inscripción de claves MEF, la sesión TLS o DTLS puede ser utilizada por el cliente MEF de origen y la MEF para denar el valor de la clave.

Condiciones previas: Debe cumplirse una de las siguientes condiciones:
Se han proporcionado al cliente MEF y a la MEF los certificados pertinentes, según se describe pormenorizadamente para la configuración de credenciales de cliente MEF en la cláusula 8.8.3.1, previa configuración con certificados de CA para validar los certificados pertinentes, según se describe en la configuración de inscripción del cliente MEF en la cláusula 8.8.3.2.

El cliente MEF y la MEF han establecido una credencial maestra simétrica (Kpm) con el correspondiente identificador de credencial maestra (KpmID). El Kpm y el KpmID pueden preconfigurarse, o el Kpm puede establecerse mediante el marco de provisión de seguridad a distancia con el KpmID establecido mediante el procedimiento de inscripción de cliente MEF.

NOTA – En el caso de establecer el Kpm mediante provisión a distancia, el procedimiento de toma de contacto de la MEF no puede aplicarse durante la inscripción del cliente MEF porque (a) la MEF no conoce el Kpm antes de dicha inscripción del cliente MEF y (b) el KpmID no se ha asignado antes de la inscripción del cliente MEF.

Descripción del procedimiento: Si el cliente MEF y la MEF han establecido una credencial maestra simétrica (Kpm) con el correspondiente identificador de credencial maestra (KpmID), el cliente MEF y la MEF establecerán la sesión TLS o DTLS mediante el procedimiento de toma de contacto TLS-PSK, de conformidad con la cláusula 10.2.2, con los siguientes detalles:

El parámetro "psk_identity" [IETF RFC 4279] se establecerá con arreglo al valor del identificador de credencial maestra (KpmID).

El parámetro "psk" [IETF RFC 4279] se establecerá con arreglo al valor de la credencial maestra (Kpm).

Si el cliente MEF y la MEF deben autentificarse mediante certificados, el cliente MEF y la MEF deberán establecer la sesión TLS o DTLS mediante el protocolo de toma de contacto TLS basado en certificados de acuerdo con la cláusula 10.2.2, sobre la base de la información siguiente:

El certificado del servidor TLS deberá ser el certificado de la MEF. El cliente MEF verificará el certificado de la MEF con respecto al conjunto de puntos de anclaje de confianza del certificado de la MEF, tal y como se describe en la cláusula 8.1.2.5.

El certificado del cliente TLS deberá ser el "certificado del cliente MEF". La MEF verificará el certificado del cliente MEF con respecto a la información del certificado del cliente MEF, tal y como se describe en la cláusula 8.1.2.5.

8.3.5.2.3 Procedimiento de inscripción del cliente MEF

Finalidad: El cliente MEF se inscribe en la MEF para confirmar que está preparado para utilizar los servicios de la MEF, bajo la autorización de la parte interesada administradora.

NOTA – El procedimiento de inscripción del cliente MEF es equivalente a la inscripción de CSE o AE, pero en este caso el cliente MEF se "inscribe" en la MEF, no en el CSE encargado de la inscripción.

Condiciones previas: El cliente MEF, la MEF y (si procede) la MEF cuentan con los parámetros descritos en la cláusula 8.3.7.

Descripción del procedimiento: El cliente MEF deberá establecer una conexión TLS (o DTLS) con la MEF mediante el procedimiento de toma de contacto de la MEF (cláusula 8.3.5.2.2). Esto proporciona a la MEF una identidad autentificada para el cliente MEF.

El cliente MEF deberá enviar una petición de inscripción de cliente MEF que incluya la información indicada en el Cuadro 8.3.5.2.3-1.

Cuadro 8.3.5.2.3-1 – Información del mensaje de petición de inscripción de cliente MEF

Parámetro	Descripción	Multiplicidad
MEF-FQDN	FQDN de la MEF, respecto de la configuración de las instrucciones de la MEF	1. 1
expirationTime	Periodo de validez de la inscripción propuesto.	2. 1
labels	Etiquetas para facilitar la detección del registro de inscripción del cliente MEF.	3. 0..1
adminFQDN	FQDN de la parte interesada administradora, proporcionado en la configuración de inscripción del cliente MEF	4. 1

Tras recibir dicha petición, la MEF la procesará. Si se producen errores, la MEF enviará una respuesta de error. La MEF podrá asignar diferentes valores a los parámetros recibidos del cliente MEF, según las instrucciones de la parte interesada administradora. Si la petición se procesa satisfactoriamente, la MEF elaborará una solicitud de respuesta de inscripción de cliente MEF que incluirá la información que figura en el Cuadro 8.3.5.2.3-2.

Cuadro 8.3.5.2.3-2 – Información del mensaje de respuesta sobre inscripción del cliente MEF

Parámetro	Descripción	Multiplicidad
MEFClientRegID	Identificador del nuevo registro de inscripción del cliente MEF.	1
labels	Etiquetas para facilitar la detección del registro de inscripción del cliente MEF	0..1
expirationTime	Periodo de validez del registro de inscripción del cliente MEF.	1
ID del cliente MEF	Identificador del cliente MEF	1
adminFQDN	FQDN de la parte interesada administradora	1

La MEF enviará la respuesta al cliente MEF.

El cliente MEF y la MEF almacenarán los parámetros.

8.3.5.2.4 Procedimiento de obtención de la configuración del cliente MEF

Finalidad: Este procedimiento permite a un cliente MEF obtener las configuraciones de cliente MEF proporcionadas por la parte interesada administradora a la MEF.

Condiciones previas:

El cliente MEF ha aplicado previamente el procedimiento de inscripción del cliente MEF para crear el registro de inscripción de dicho cliente MEF.

El periodo de validez del registro de inscripción del cliente de MEF no ha concluido.

Descripción del procedimiento. El procedimiento comprende las etapas siguientes:

El cliente MEF debe establecer una conexión TLS (o DTLS) con la MEF, con arreglo a lo descrito en la etapa 1 de la cláusula 8.3.5.2.3.

El cliente MEF enviará una petición de obtención de la configuración del cliente MEF que incluya la información indicada en el Cuadro 8.3.5.2.4-1.

Cuadro 8.3.5.2.4-1 – Información del mensaje de petición de obtención de la configuración del cliente MEF

Parámetro	Descripción	Multiplicidad
MEF-FQDN	FQDN de la MEF, basado en la configuración de las instrucciones de la MEF	1
MEFClientRegID	Identificador del registro de inscripción del cliente MEF en curso de actualización	1

Tras recibir la petición, la MEF la procesará. Si se producen errores, en particular si no existe ninguna configuración de cliente MEF asociada al registro de inscripción del cliente MEF identificado, la MEF enviará una respuesta de error. Si la petición se procesa adecuadamente, la MEF intentará obtener la configuración del cliente MEF que se asocie al registro de inscripción del cliente MEF identificado.

La MEF deberá formular una respuesta de obtención de la configuración del cliente MEF que contenga los siguientes parámetros.

Cuadro 8.3.5.2.4-2 – Información del mensaje de respuesta relativo a la obtención de la configuración del cliente MEF

Parámetro	Descripción	Multiplicidad
MEFClientCfg	Configuración del cliente MEF que se asocie al registro de inscripción del cliente MEF identificado	1

La MEF enviará la respuesta al cliente MEF.

El cliente MEF aplicará la configuración del cliente MEF.

8.3.5.2.5 Procedimiento de actualización de la inscripción del cliente MEF

Finalidad: Este procedimiento permite a un cliente MEF actualizar la inscripción del cliente MEF mediante toda combinación que incluya la ampliación del parámetro *expirationTime* del registro de inscripción del cliente MEF o la actualización del parámetro *labels*.

Condiciones previas: El cliente MEF ha aplicado previamente el procedimiento de inscripción del cliente MEF para crear el registro de inscripción de dicho cliente MEF.

La validez del registro de inscripción del cliente de MEF no ha vencido.

Descripción del procedimiento: El procedimiento comprende las etapas siguientes:

El cliente MEF deberá establecer una conexión TLS (o DTLS) con la MEF, con arreglo a lo descrito en la etapa 1 de la cláusula 8.3.5.2.3.

El cliente MEF enviará una petición de actualización de la inscripción del cliente MEF que incluya la información indicada en el Cuadro 8.3.5.2.5-1.

Cuadro 8.3.5.2.5-1 – Información del mensaje de petición de actualización de la inscripción del cliente MEF

Parámetro	Descripción	Multiplicidad
MEF-FQDN	FQDN de la MEF, basado en la configuración de las instrucciones de la MEF	1
MEFClientRegID	Identificador de la inscripción del cliente MEF en curso de actualización	1
expirationTime	Periodo de validez propuesto del registro de inscripción del cliente MEF.	0..1
labels	Etiquetas para facilitar la detección del registro de inscripción del cliente MEF	0..1
NOTA – Deberán incluirse al menos un parámetro expirationTime y un parámetro labels.		

Tras recibir la solicitud, la MEF la procesará. Si se producen errores, la MEF enviará una respuesta de error. Si la petición se procesa adecuadamente, la MEF actualizará el registro de inscripción del cliente MEF con los valores propuestos si lo autoriza la parte interesada administradora. La MEF podrá asignar valores diferentes a los parámetros recibidos del cliente MEF, según las instrucciones de la parte interesada administradora.

La MEF deberá formular una respuesta de actualización de la inscripción del cliente MEF que contenga los parámetros enumerados en el Cuadro 8.3.5.2.5-2.

Cuadro 8.3.5.2.5-2 – Información del mensaje de respuesta de actualización de la inscripción del cliente MEF

Parámetro	Descripción	Multiplicidad
expirationTime	Valor temporal actualizado relativo al periodo de validez del registro de inscripción del cliente MEF.	0..1
labels	Etiquetas actualizadas para facilitar la detección del registro de inscripción del cliente MEF	0..1
NOTA – La respuesta sólo incluye el parámetro expirationTime y/o labels si esos parámetros vienen incluidos en la correspondiente petición.		

La MEF enviará la respuesta al cliente MEF.

El cliente MEF y la MEF almacenarán los parámetros.

8.3.5.2.6 Procedimiento de anulación de la inscripción del cliente MEF

Finalidad: Este procedimiento permite a un cliente MEF concluir su inscripción en la MEF.

Condiciones previas: El cliente MEF ha aplicado previamente el procedimiento de inscripción del cliente MEF para crear el registro de inscripción de dicho cliente MEF.
La validez del registro de inscripción del cliente de MEF no ha vencido.

Descripción del procedimiento: El procedimiento comprende las etapas siguientes:

El cliente MEF deberá establecer una conexión TLS (o DTLS) con la MEF, con arreglo a lo descrito en la etapa 1 de la cláusula 8.3.5.2.3.

El cliente MEF enviará una petición de anulación de la inscripción del cliente MEF que incluya la información indicada en el Cuadro 8.3.5.2.6-1.

Cuadro 8.3.5.2.6-1 – Información del mensaje de solicitud de anulación de la inscripción del cliente MEF

Parámetro	Descripción	Multiplicidad
MEF-FQDN	FQDN de la MEF, basado en la configuración de la instrucción de la MEF	1
MEFClientRegID	Identificador del registro de inscripción del cliente MEF que va a anularse	1

Tras recibir la solicitud, la MEF la procesará. Si se producen errores, la MEF enviará una respuesta de error. Si la solicitud se procesa adecuadamente, la MEF suprimirá la información asociada al registro de inscripción del cliente MEF identificado.

La MEF elaborará una respuesta de actualización de la inscripción del cliente MEF en la que se indicará que la operación se ha llevado a cabo satisfactoriamente. La MEF enviará la respuesta al cliente MEF.

8.3.5.2.7 Procedimiento de inscripción de claves MEF

Finalidad: Este procedimiento permite a un cliente MEF de origen establecer una clave simétrica con la MEF que puede obtenerse para su utilización por un cliente MEF de destino, o varios.

El procedimiento se realiza entre el cliente MEF de origen y la MEF.

Condiciones previas: El cliente MEF de origen recibe (o determina previamente) la información relativa a la configuración de inscripción de claves MEF (cláusula 8.3.7.3).
El cliente MEF de origen lleva a cabo el procedimiento de inscripción de clientes MEF (cláusula 8.3.5.2.3) con la MEF para la parte interesada administradora identificada en la configuración de inscripción de claves MEF.

Descripción del procedimiento: El procedimiento comprende las etapas siguientes:

El cliente MEF de origen debe establecer una sesión TLS o DTLS con la MEF mediante el procedimiento de toma de contacto de la MEF que se describe en la cláusula 8.3.5.2.2. Otra modalidad de dicho procedimiento se basa en que la MEF establezca una identidad autentificada para el cliente MEF de origen.

El cliente MEF de origen selecciona el valor de la clave de conexión segura M2M (Kc) que debe distribuir la MEF. El valor deberá ser uno de los siguientes:

El cliente MEF de origen genera el valor de la clave simétrica resultante a partir de los valores secretos de sesión (D)TLS mediante exportación de claves TLS ([IETF RFC 5705]), como se describe en la cláusula 10.3.1 "Información detallada sobre exportación de claves TLS".

El valor de la clave simétrica resultante es autogenerado por el cliente MEF de origen, independientemente de los valores secretos de sesión (D)TLS.

El cliente MEF de origen deberá componer una lista de clientes MEF de destino con respecto a los cuales la MEF tiene autorización para proporcionar el valor de la clave simétrica resultante.

Para un SAEF basado en MEF o ESPrim basada en MEF: la lista deberá contener exactamente un AE-ID o un CSE-ID absolutos.

Para ESData basada en MEF: la lista contendrá cualquier número distinto de cero de AE-ID o CSE-ID absolutos.

NOTA 1 – La forma en que el cliente MEF de origen selecciona la lista de clientes MEF de destino depende de la aplicación.

El cliente MEF de origen enviará una petición de inscripción de claves MEF, incluida la información que figura en el Cuadro 8.3.5.2.7-1.

Cuadro 8.3.5.2.7-1 – Información del mensaje de petición de inscripción de claves MEF

Parámetro	Descripción	Multiplicidad
MEF-FQDN	FQDN de la MEF, basado en la configuración de la instrucción de la MEF	1
expirationTime	Periodo de validez propuesto para la inscripción de la clave.	1
labels	Etiquetas para facilitar la detección de la inscripción de la clave	0..1
adminFQDN	Identificador de la parte interesada administradora	1
SUID	Identificador de uso de seguridad que limita la función de seguridad para la que se puede utilizar la clave simétrica.	1
targetIDs	Lista (opcional) de identificadores para el conjunto inicial de clientes MEF de destino autorizados a obtener la clave simétrica.	0..1
Key Value	Este parámetro (opcional), de estar presente, contiene un valor de clave simétrica resultante que es autogenerado por el cliente MEF de origen. Si este parámetro no está presente, el cliente MEF de origen y la MEF generarán dicho valor de clave simétrica resultante mediante TLS Exporter	0..1

La MEF procesará la petición. Si se producen errores, la MEF enviará una respuesta de error. Si la petición se procesa satisfactoriamente, la MEF autorizará el establecimiento de un valor de clave, basado en la identidad autentificada para el cliente MEF de origen.

NOTA 2 – La presente especificación no proporciona información pormenorizada para la autorización de esta petición.

Si la petición incluye un valor en el parámetro de valor de la clave, la MEF almacenará este valor. En caso contrario, generará el valor de la clave a partir de la sesión (D)TLS mediante la exportación de claves TLS ([IETF RFC 5705]), tal y como se describe en la cláusula 10.3.1 "Información pormenorizada sobre exportación de claves TLS".

La MEF inicializará la lista de clientes MEF de destino autorizados (clientes MEF que pueden obtener esta credencial) con respecto a la lista proporcionada en la petición.

Para ESData basada en MEF: Esa lista pueden actualizarla ulteriormente las partes interesadas administradoras durante el procedimiento de inscripción de claves MEF, o después del mismo.

NOTA 3 – Las presentes especificaciones no proporcionan información pormenorizada sobre la actualización por las partes interesadas administradas de la lista de clientes MEF autorizados. La MEF puede proporcionar su propia lógica e interfaz que permita a dichas partes interesadas administradoras gestionar esta lista.

La MEF seleccionará un valor de RelativeKeyID no utilizado previamente.

La MEF puede asignar diferentes valores a los parámetros recibidos del cliente MEF, sobre la base de las instrucciones de la parte interesada administradora.

La MEF enviará una respuesta al cliente MEF de origen, incluida la información que figura en el Cuadro 8.3.5.2.-7-2.

Cuadro 8.3.5.2.7-2 – Información del mensaje de respuesta de inscripción de claves MEF

Parámetro	Descripción	Multiplicidad
RelativeKeyID	Parte relativa del identificador de la clave asociada a la inscripción de la clave	1
expirationTime	Periodo de validez de la inscripción de la clave.	1
Source MEF Client ID	Identificador del cliente MEF de origen	1
labels	Etiquetas para facilitar la detección de la inscripción de la clave	0..1
adminFQDN	Identificador de la parte interesada administradora	1
SUID	Identificador de uso de seguridad que limita la función de seguridad para la que se puede utilizar la clave simétrica.	
targetIDs	Lista de identificadores para el conjunto inicial de clientes MEF de destino autorizados a obtener la clave simétrica. Esta lista puede modificarse sobre la base de la lista proporcionada por el cliente MEF, o elaborarla la MEF (si el cliente MEF no proporciona previamente ninguna lista).	1

El cliente MEF de origen y la MEF almacenarán el valor de la clave simétrica resultante y el identificador de clave correspondiente.

El identificador de clave se genera a partir del parámetro RelativeKeyID y el FQDN de la función de autentificación M2M mediante el cliente MEF de origen y la MEF, como se describe en la cláusula 10.3.5 "Generación del KcID".

8.3.5.2.8 Procedimiento de obtención de la clave de la MEF

Finalidad: Este procedimiento permite a un cliente MEF de destino obtener el valor de la clave a través de una MEF correspondiente a un RelativeKeyID recibido por el cliente MEF de destino.

Condiciones previas:

El cliente MEF de destino realiza la configuración de credenciales del cliente MEF (cláusula 8.3.5.2.1) con la MEF, incluida la configuración del URI de obtención de la clave de la MEF.

El cliente MEF de origen lleva a cabo el procedimiento de inscripción de la clave MEF (cláusula 8.3.5.2.2) con la MEF, lo que da lugar a un valor de clave inscrito y a un RelativeKeyID asignado para una parte interesada administradora específica y un identificador de uso de seguridad (SUID).

El cliente MEF de destino recibe un Identificador de clave del cliente MEF iniciador a través de una función de seguridad con el SUID que el cliente MEF de origen haya proporcionado previamente a la MEF durante el procedimiento de inscripción de la clave MEF (cláusula 8.3.5.2.7). El identificador de clave está compuesto por el FQDN de la MEF y el RelativeKeyID asignado a la clave inscrita.

Cabe esperar que el cliente MEF de destino esté autorizado a obtener el correspondiente valor de la clave simétrica resultante.

NOTA – El cliente MEF de destino no debe repetir este procedimiento si dicho cliente MEF de destino ya posee el valor de la clave correspondiente.

Descripción del procedimiento: El procedimiento comprende las etapas siguientes:

El cliente MEF de destino debe establecer una sesión TLS o DTLS con la MEF mediante el procedimiento de toma de contacto de la MEF descrito en la cláusula 8.3.5.2.2. Otra modalidad de dicho procedimiento se basa en que la MEF establezca una identidad autentificada para el cliente MEF de destino.

El cliente MEF de destino envía una petición de obtención de clave MEF a la MEF, incluida la información que figura en el Cuadro 8.3.5.2.8-1.

Cuadro 8.3.5.2.8-1 – Información del mensaje de petición de obtención de claves MEF

Parámetro	Descripción	Multiplicidad
RelativeKeyID	Parte relativa del identificador de clave recibida del cliente MEF de origen a través de una función de seguridad	1

La MEF procesará la petición. Si se producen errores, la MEF enviará una respuesta de error. Si la petición se procesa satisfactoriamente, la MEF identificará la inscripción de la clave por medio del parámetro *RelativeKeyID*.

La MEF determinará si el cliente MEF de destino está autorizado a obtener la clave y los metadatos inscritos comparando el identificador autentificado para el cliente MEF de destino con la lista de identificadores para los clientes MEF de destino autorizados. Si el cliente MEF de destino no está autorizado, la MEF enviará a ese cliente MEF de destino un mensaje de error. En caso contrario, la MEF aplicará la etapa siguiente.

La MEF enviará una respuesta al cliente MEF de destino, incluida la información que figura en el Cuadro 8.3.5.2.-82.

Cuadro 8.3.5.2.8-2 – Información del mensaje de respuesta de inscripción de claves MEF

Parámetro	Descripción	Multiplicidad
expiraciónTiempo	Periodo de validez de la inscripción de la clave.	1
Source MEF Client ID	Identificador del cliente MEF de origen	1
labels	Etiquetas para facilitar la detección de la inscripción de la clave	0..1
adminFQDN	Identificador de la parte interesada administradora	1
SUID	Identificador de uso de seguridad que limita la función de seguridad para la que se puede utilizar la clave simétrica.	
Valor clave	Valor inscrito de la clave simétrica resultante	1

El cliente MEF de destino deberá asociar los parámetros al identificador de clave.

8.3.5.2.9 Procedimiento de actualización de la inscripción de la clave de la MEF

Finalidad: Este procedimiento permite a un cliente MEF de origen actualizar los metadatos asociados a una clave inscrita.

Este procedimiento tiene lugar entre el cliente MEF de origen y la MEF.

Condiciones previas: El cliente MEF lleva a cabo previamente el procedimiento de inscripción de claves MEF para efectuar dicha inscripción.

La validez de la inscripción de la clave no ha vencido.

Descripción del procedimiento: El procedimiento comprende las etapas siguientes:

El cliente MEF debe establecer una conexión TLS (o DTLS), con arreglo a lo descrito en la etapa 1 de la cláusula 8.3.5.2.7.

El cliente MEF de origen deberá elaborar una lista de clientes MEF de destino para los que la MEF está autorizada a proporcionar el parámetro Kc:

Para un SAEF basado en MEF o ESPrim basada en MEF: la lista deberá contener exactamente un AE-ID o un CSE-ID absolutos.

Para ESData basada en MEF: la lista contendrá cualquier número distinto de cero de AE-ID o CSE-ID absolutos.

NOTA – En las presentes especificaciones no se proporciona ningún detalle sobre la manera en que el cliente MEF de origen selecciona la lista de clientes MEF de destino.

El cliente MEF de origen enviará una petición de actualización de inscripción de claves MEF, incluida la información actualizada que figura en el Cuadro 8.3.5.2.9-1.

Cuadro 8.3.5.2.9-1 – Información del mensaje petición de actualización de la inscripción de claves MEF

Parámetro	Descripción	Multiplicidad
MEF-FQDN	FQDN de la MEF, basado en la configuración de la instrucción de la MEF	1
RelativeKeyID	Parte relativa del identificador de la clave asociada a la inscripción de la clave	1
expirationTime	Periodo de validez propuesto para la inscripción de la clave.	0..1
labels	Etiquetas propuestas para facilitar la detección de la clave inscrita	0..1
targetIDs	Lista propuesta (opcional) de identificadores para el conjunto de clientes MEF de destino autorizados a obtener la clave simétrica.	0..1
NOTA 1 – Se debe proporcionar al menos uno de los parámetros *expirationTime*, *labels* o *targetIDs*		

La MEF procesará la petición. Si se producen errores, la MEF enviará una respuesta de error adecuada. Si la petición se procesa satisfactoriamente, la MEF actualizará los metadatos con los valores propuestos si lo autoriza la parte interesada administradora. La MEF podrá asignar valores diferentes a los parámetros recibidos del cliente MEF, sobre la base de las instrucciones de la parte interesada administradora.

La MEF enviará una respuesta al cliente MEF de origen, incluida la información que figura en el Cuadro 8.3.5.2.-9-2.

Cuadro 8.3.5.2.9-2 – Información del mensaje de respuesta de actualización de la inscripción de claves MEF

Parámetro	Descripción	Multiplicidad
expirationTime	Periodo de validez de la inscripción de la clave, si ésta ha variado desde la última vez que se proporcionó al cliente MEF dicho periodo de validez	0..1
labels	Lista actualizada de etiquetas para facilitar la detección de la inscripción de la clave, en su caso	0..1
targetIDs	Lista actualizada de identificadores para el conjunto inicial de clientes MEF de destino autorizados a obtener la clave simétrica. Esta lista puede modificarse sobre la base de la lista proporcionada por el cliente MEF.	0..1
NOTA: La respuesta incluye sólo los parámetros que incluidos en la petición correspondiente.		

8.3.5.2.10 Procedimiento de anulación de inscripción de claves MEF

Finalidad: Este procedimiento permite a un cliente MEF de origen solicitar a la MEF que interrumpa la distribución de una clave inscrita.

El procedimiento tiene lugar entre el cliente MEF de origen y la MEF.

Condiciones previas: El cliente MEF lleva a cabo previamente el procedimiento de inscripción de claves MEF para realizar la inscripción de claves.

La validez de la inscripción de la clave no ha vencido.

Descripción del procedimiento: El comprende las etapas siguientes:

El cliente MEF debe establecer una conexión TLS (o DTLS) con la MEF, tal y como se describe en la etapa 1 de la cláusula 8.3.5.2.7.

El cliente MEF enviará una petición de anulación de inscripción de la clave MEF que incluya la información que figura en el Cuadro 8.3.5.2.10-1.

Cuadro 8.3.5.2.10-1 – Información del mensaje de petición de anulación de inscripción del cliente MEF

Parámetro	Descripción	Multiplicidad
MEF-FQDN	FQDN de la MEF, sobre la base de la configuración de la instrucción de la MEF	1
RelativeKeyID	Parte relativa del identificador de la clave asociada a la inscripción de la clave	1

Al recibir la solicitud, la MEF la procesará. Si se producen errores, la MEF enviará una respuesta de error. Si la petición se procesa satisfactoriamente, la MEF suprimirá la información asociada a la inscripción de la clave identificada.

La MEF elaborará una respuesta de anulación de inscripción relativa al cliente MEF, confirmando que ello se lleva a cabo satisfactoriamente. La MEF enviará la respuesta al cliente MEF.

8.3.5.3 Asignación con respecto al protocolo [ITU-T Y.4500.32]

La interfaz Mmef definida en [UIT-T Y.4500.32] se utilizará para los procedimientos de provisión de clave simétrica. La asignación de los procedimientos MEF descritos en la cláusula 8.3.5.2 a la interfaz Mmef se describe en [UIT-T Y.4500.32].

8.3.6 Información pormenorizada sobre el procedimiento de provisión de certificados

8.3.6.1 Introducción

El procedimiento de provisión de certificados incluye las siguientes partes:

Cliente MEF: entidad de seguridad que solicita la provisión de un certificado por la MEF. El cliente MEF utiliza el certificado provisto por la MEF para la posterior autentificación de sí mismo con respecto a la MEF. Dicha entidad de seguridad puede utilizar el certificado proporcionado por la MEF para la posterior autentificación de sí misma con respecto a otras entidades de seguridad oneM2M.

MEF CA: emisión de certificados provistos por la MEF.

MEF: procesamiento de las peticiones del cliente de MEF en calidad de Autoridad de inscripción (RA) para remitir las peticiones de firma de certificados (CSR) a la MEF CA. La MEF puede solicitar a MEF CA que añada atributos a los que ya incluye la CSR, y pedir la supresión o modificación de los atributos incluidos en la CSR.

El procedimiento de provisión de certificados sólo especifica la interacción entre el cliente MEF y la MEF.

NOTA 1 – La presente especificación no describe la interacción entre la MEF y la MEF CA.

El procedimiento de provisión de certificados tiene por objeto:

Que el cliente MEF obtenga el certificado facilitado por la MEF.

Que el cliente MEF obtenga los certificados de la MEF CA. El cliente MEF utilizará esos certificados para la posterior validación de los certificados que autentifiquen la MEF. Dichos certificados podrá utilizarlos la entidad de seguridad a los efectos de validación posterior de los certificados que autentifiquen otras entidades de seguridad y MAF.

NOTA 2 – También se pueden proporcionar certificados CA de puntos de anclaje de confianza adicionales a los efectos de validación de otras entidades de seguridad y MAF mediante la configuración de MO sobre la base del recurso [*trustAnchorCred*].

El procedimiento de provisión de certificados comprende a su vez dos procedimientos:

Procedimiento inicial de provisión de certificados: aplicable si el cliente MEF no posee un certificado válido proporcionado por la MEF.

Procedimiento de nueva provisión de certificados: utilizado por un cliente MEF para renovar o volver a obtener su certificado válido existente proporcionado por la MEF.

En esta especificación se describe la aplicación de los siguientes protocolos para el procedimiento de provisión de certificados:

Inscripción mediante transporte seguro (EST), especificado en [IETF RFC 7030]. La aplicación de este protocolo se describe en la cláusula 8.3.6.2.

Las funciones de provisión de certificados utilizan el protocolo simple de inscripción de certificados (SCEP) [IETF RFC 8824]. La aplicación de este protocolo se describe en la cláusula 8.3.6.3.

8.3.6.2 Procedimientos de provisión de certificados mediante EST

8.3.6.2.1 Introducción

El protocolo de inscripción mediante transporte seguro (EST) se especifica en [IETF RFC 7030]. Al aplicar EST en los procedimientos de provisión de certificados, se llevará a cabo la siguiente asignación de conceptos.

El cliente MEF actúa como cliente EST.

La MEF actúa como servidor EST.

La MEF CA actúa como EST CA.

El certificado proporcionado por la MEF es equiparable al certificado de cliente EST.

Si una MEF o un cliente MEF solicita compatibilidad con el procedimiento de provisión de certificados mediante EST:

La MEF o el cliente MEF deberá admitir las operaciones EST obligatorias y las operaciones opcionales de "Atributos CSR" (véase la Figura 5 de [IETF RFC 7030]).

La MEF o el cliente MEF deberá admitir la autentificación del servidor TLS con certificados y la autentificación de cliente TLS mediante certificados, tal como se especifica para EST en las secciones 3.3.1 y 3.3.2 de [IETF RFC 7030].

NOTA 1 – Se utiliza cuando se emplea un RSPF basado en certificados. El RSPF basado en certificados requiere que el cliente MEF y la MEF utilicen únicamente certificados CA de puntos de anclaje de confianza que hayan sido identificados explícitamente para su uso a los efectos de validación de certificados MEF y certificados de cliente MEF. Corresponden a los puntos de anclaje de confianza explícitos (TA) que se definen en la sección 1.1 de [IETF RFC 7030]. En consecuencia, el cliente MEF o EST utiliza una base de datos de TA explícita del cliente EST, y el cliente MEF o EST utiliza una base de datos TA explícita del cliente EST, habida cuenta de que dichas bases de datos se definen en la Figura 4 de [IETF RFC 7030].

Si la MEF o el cliente MEF admite un RSPF basado en PPSK, la MEF o el cliente MEF deberá admitir la autentificación recíproca TLS sin certificado EST (sección 3.3.3 de [IETF RFC 7030]).

La MEF o el cliente MEF pueden aceptar la vinculación de la información de identidad y la de prueba de posesión (sección 3.5 [IETF RFC 7030]).

NOTA 2 – Hasta que no se disponga de conjuntos criptográficos de uso generalizado compatibles con esa funcionalidad, es poco probable que ésta sea aceptada por la MEF o el cliente MEF.

La MEF o el cliente MEF no utilizarán la función de autentificación de cliente basada en HTTP de EST (sección 3.2.3 de [IETF RFC 7030]).

NOTA 3 – La autentificación de cliente basada en HTTP en EST puede ser utilizada en casos en los que el cliente MEF está autorizado por medio de la autentificación de usuario que se aborda en la sección 2.2.3 [IETF RFC 7030]. Esos casos aún no han sido considerados en la presente especificación. Pueden ser compatibles en el futuro si se aceptan a nivel de autentificación de cliente basada en HTTP.

El cliente MEF deberá aceptar la generación de pares de claves privadas o públicas. Dicho cliente MEF y la MEF deberán utilizar la función EST de generación de claves a nivel de servidor (sección 2.4, 4.4 [IETF RFC 7030]).

8.3.6.2.2 Procedimiento de provisión inicial de certificados mediante EST

Finalidad: Permitir que un cliente MEF solicite su primer certificado a la MEF. Véanse también los casos operacionales de inscripción inicial que figuran en la sección 2.2 de [IETF RFC 7030], habida cuenta de los métodos de autentificación admitidos enumerados en la cláusula 8.3.6.2.1.

Condiciones previas: Condiciones previas comunes para todos los procedimientos de provisión de certificados:

El cliente MEF y la MEF aceptan EST.

El cliente MEF recibe elestBaseURI, cuyo FQDN debe corresponder al FQDN de la MEF.

El cliente MEF se activa para llevar a cabo la EST.

NOTA 1 – El estBaseURI relativo a la condición previa A.ii puede proporcionarse en el mensaje que activa la EST con arreglo a la condición previa A.iii.

El cliente MEF y la MEF llevan a cabo satisfactoriamente un procedimiento de toma de contacto MEF y la MEF asocia un identificador al cliente MEF. Para el procedimiento de provisión inicial de certificados, se utilizará uno de los siguientes RSPF:

RSPF basado en PPSK (cláusula 8.3.2.1), correspondiente a la autentificación TLS sin certificado para EST, según se describe en la sección 3.3.3 de [IETF RFC 7030].

RSPF basado en certificados (cláusula 8.3.2.2), correspondiente a autentificación TLS recíproca basada en certificados para EST.

El certificado utilizado para autentificar el servidor MEF/EST corresponde al certificado de servidor EST (definido en la Figura 3 de [IETF RFC 7030]) que el cliente MEF/ EST valida con respecto a la base de datos de puntos de anclaje de confianza de forma explícita para clientes EST (véase la Nota 1 en la cláusula 8.3.6.2.1). EST describe la autentificación de servidor EST que figura en la sección 3.3.1 de [IETF RFC 7030], en virtud de la cual el cliente EST debe realizar comprobaciones de autorización a nivel de servidor EST, con arreglo a lo establecido en la sección 3.6 de [IETF RFC 7030], con información específica de las comprobaciones de autorización para una base de datos TA explícita de cliente EST en la sección 3.6.1 de [IETF RFC 7030].

El certificado utilizado para autentificar el cliente MEF/EST corresponde a un certificado de cliente EST de terceros (definido en la Figura 3 de [IETF RFC 7030]) que valida el servidor MEF/ EST con respecto a la base de datos de puntos de anclaje de confianza explícita del servidor EST (véase la Nota 1 de la cláusula 8.3.6.2.1). EST describe la autentificación del cliente EST, según la sección 3.3.2 de [IETF RFC 7030], en virtud de la cual el servidor EST debe efectuar comprobaciones de autorización con arreglo a lo establecido en la sección 3.7 de [IETF RFC 7030].

NOTA 2 – La autentificación de usuario o del cliente EST basada en HTTP no es compatible con el procedimiento de provisión inicial de certificados. Véase la nota 3 de la cláusula 8.3.6.2.1.

Descripción del procedimiento:

Obtención de certificados CA de puntos de anclaje de confianza. Véase la sección 4.1 de [IETF RFC 7030].

El cliente MEF solicitará el conjunto de certificados CA de puntos de anclaje de confianza, tal y como se describe en la sección 4.1.2 de [IETF RFC 7030].

La MEF responderá mediante un conjunto certificados CA de puntos de anclaje de confianza, tal y como se describe en la sección 4.1.3 de [IETF RFC 7030].

Cabe esperar que el cliente MEF instale los certificados CA de puntos de anclaje de confianza.

NOTA – La validación de la ruta de certificación y la verificación del estado del certificado deben ser realizadas por el cliente MEF como se especifica en la cláusula 8.1.2.2.

Obtención del conjunto de atributos del CSR. Véase la sección 4.5 de [IETF RFC 7030].

El cliente MEF solicitará el conjunto de atributos CSR a la MEF, tal y como se describe en la sección 4.5.1 de [IETF RFC 7030].

La MEF responderá con el conjunto de atributos CSR requeridos, tal como se describe en la sección 4.5.2 de [IETF RFC 7030]. El conjunto de atributos CSR necesarios deberá cumplir con el perfil CSR de la cláusula 10.1.4. Dicho conjunto incluye el atributo *challengePassword* y un atributo de identidad para el tipo de identificador que la MEF asocia al cliente MEF (véanse las condiciones previas).

Obtención de un certificado.

El cliente MEF deberá generar un par de claves públicas o privadas de longitud de clave adecuada, o seleccionar un par de claves públicas o privadas existente de longitud de clave adecuada.

El cliente MEF generará una CSR con los atributos CSR solicitados mediante el par de claves.

El cliente MEF solicitará un certificado de cliente EST mediante "Inscripción simple de clientes", tal y como se describe en la sección 4.2.1 de [IETF RFC 7030].

La MEF validará los atributos, incluido el *challengePassword*, con respecto a los proporcionados en la etapa 2. La MEF validará el atributo de identidad con respecto a la identidad autentificada asociada al cliente MEF (véase la condición previa B).

NOTA 3 – La MEF, en calidad de Autoridad de Registro (RA), remite la CSR a una Autoridad de Certificación (CA). La CA emite el certificado de cliente EST (definido en la Figura 3 de [IETF RFC 7030]) y devuelve el certificado a la MEF.

La MEF enviará el certificado de cliente EST (definido en la Figura 3 de [IETF RFC 7030]) al cliente MEF en la respuesta, tal como se describe en la sección 4.2.3 de [IETF RFC 7030].

Cabe esperar que el cliente MEF instale el certificado de cliente EST y lo asocie a la clave privada correspondiente. El certificado de cliente EST se utilizará para la autentificación ulterior con la MEF. El certificado de cliente EST también puede utilizarse como certificado de entidad de extremo en otros protocolos de seguridad.

8.3.6.2.3 Procedimiento de nueva provisión de certificados mediante EST

Finalidad: Permitir a un cliente MEF que renueve un certificado inscrito válido, o solicite una nueva clave para el mismo. Véase a tal efecto el caso operacional de nueva emisión de certificados de cliente en la sección 2.3 de [IETF RFC 7030].

Condiciones previas: Condiciones previas comunes para todos los procedimientos de provisión de certificados: véase la condición previa A en la cláusula 8.3.6.2.2.

El cliente MEF lleva a cabo previamente el procedimiento de provisión inicial de certificados o el procedimiento de nueva provisión de certificados con la MEF, y el cliente MEF ha instalado su certificado de cliente EST y la base de datos de puntos de anclaje de confianza explícita de Cliente EST sobre la base del procedimiento más reciente.

El cliente MEF y la MEF llevan a cabo un procedimiento de toma de contacto MEF para el RSPF basado en certificados (cláusula 8.3.2.2), y el cliente MEF utiliza su certificado de cliente EST y la base de datos de puntos de anclaje de confianza explícita del cliente EST, tal y como se aborda en la condición previa B. Ello es idéntico a la condición previa B.ii de la cláusula 8.3.6.2.2, con la diferencia de que el cliente MEF/EST se autentifica con un certificado de cliente EST (definido en la Figura 4 de [IETF RFC 7030]), en lugar de un certificado de cliente EST de terceros con respecto a la condición previa B.ii.2.

Descripción del procedimiento: Obtención de certificados CA de puntos de anclaje de confianza; al igual que en la etapa 1 de la cláusula 8.3.6.2.2.

Obtención del conjunto de atributos CSR. Al igual que en la etapa 2 de la cláusula 8.3.6.2.2.

Obtención de un certificado; al igual que en la etapa 3 de la cláusula 8.3.6.2.2, salvo que las etapas 3.c y 3.d se sustituyen por las siguientes:

c) El cliente MEF solicitará la renovación de su certificado de cliente EST, o el establecimiento de una nueva clave para el mismo, mediante una "nueva inscripción sencilla de clientes", tal y como se describe en la sección 4.2.2 de [IETF RFC 7030].

d) La MEF validará el parámetro *challengePassword* y las EKU con respecto a los proporcionados en la etapa 2. La MEF valida la identidad proporcionada con respecto a la identidad asociada al cliente MEF (véase la condición previa C).

8.3.6.3 Procedimientos de provisión de certificados mediante SCEP

8.3.6.3.1 Introducción

El protocolo simple de inscripción de certificados (SCEP) se especifica en [IETF RFC 8824]. Existen muchas aplicaciones disponibles que se ajustan a [IETF RFC 8824]. Para documentar las implementaciones existentes, cabe remitirse a [IETF RFC 8824].

Al utilizar un SCEP para los procedimientos de provisión de certificados, cabe aplicar la siguiente asignación de conceptos.

El cliente de la función de inscripción M2M (MEF) actúa como cliente SCEP.

La MEF actúa como servidor SCEP (o respondedor SCEP).

La MEF CA actúa como SCEP CA.

El certificado proporcionado por la MEF es equiparable al certificado de cliente SCEP.

Si una MEF o un cliente MEF solicitan compatibilidad con el procedimiento de provisión de certificados mediante SCEP:

La MEF o el cliente MEF pueden admitir la vinculación de la información sobre identidad y prueba de posesión.

NOTA 1 – Hasta que no se disponga de bibliotecas criptográficas de uso generalizado compatibles con esa funcionalidad, es poco probable que dicha funcionalidad sea compatible con la MEF o el cliente MEF.

La MEF o el cliente MEF no utilizarán la autentificación de cliente basada en HTTP.

NOTA 2 – La autentificación del cliente basada en HTTP en SCEP puede utilizarse en casos en los que el cliente MEF esté autorizado mediante autentificación de usuario. Esos casos aún no han sido abordados en la presente especificación. Podrán ser compatibles en el futuro mediante la ampliación de su admisibilidad con respecto a la autentificación de cliente basada en HTTP.

El cliente MEF deberá admitir la generación de pares de claves privadas o públicas.

8.3.6.3.2 Información pormenorizada sobre los procedimientos de provisión de certificados mediante SCEP

Finalidad: Permitir que un cliente MEF solicite su primer certificado, y los siguientes, a la MEF mediante SCEP, como se especifica en [IETF RFC 8824].

Condiciones previas: Condiciones previas comunes para todos los procedimientos de provisión de certificados.

El cliente MEF y la MEF soportan SCEP.

El cliente MEF recibe el URI de base cuyo FQDN debe coincidir con el FQDN de la MEF.

El cliente MEF se activa para llevar a cabo el SCEP.

NOTA 1 – El URI de base para la condición previa A.ii puede proporcionarse en la instrucción de control del cliente MEF que activa el SCEP para la condición previa A.iii.

Si el cliente no dispone de un certificado adecuado, deberá generar a escala local un certificado autofirmado. La extensión *keyUsage* del certificado deberá indicar que su validez para *digitalSignature* y *keyEncipherment*. El certificado autofirmado deberá utilizar la misma denominación que en la peteición PKCS #10. Véase la sección 2.4 de [IETF RFC 8824].

Descripción del procedimiento: Obtención de certificados CA de puntos de anclaje de confianza. Véase la sección 4.2 de [IETF RFC 8824].

El cliente MEF solicitará el conjunto de certificados CA de puntos de anclaje de confianza.

La MEF responderá mediante un conjunto de certificados CA de puntos de anclaje de confianza.

Cabe esperar que el cliente MEF instale los certificados CA de puntos de anclaje de confianza.

NOTA 2 – La validación de la ruta de certificación y la verificación del estado del certificado deben ser realizadas por el cliente MEF, tal y como se especifica en la cláusula 8.1.2.2.

Obtención de funciones de la CA. Véase la sección 3.5 de [IETF RFC 8824].

El cliente MEF solicitará a la MEF el conjunto de funciones de la CA, tal como se describe en la sección 3.5.1 de [IETF RFC 8824].

La MEF responderá mediante el conjunto de atributos CSR necesarios, tal y como se describe en la sección 3.5.2 de [IETF RFC 8824].

Obtención de un certificado.

El cliente MEF deberá generar un par de claves públicas o privadas autofirmadas de longitud de clave adecuada, o seleccionar un par de claves públicas o privadas existente de longitud de clave adecuada.

El cliente MEF generará una CSR con los atributos solicitados de la CSR mediante el par de claves.

El cliente MEF solicitará un certificado de cliente SCEP mediante "inscripción de certificados", tal y como se describe en la sección 4.3 de [IETF RFC 8824].

La MEF validará los atributos, y de forma factitiva, un parámetro *challengePassword*. La MEF validará el atributo de identidad con respecto a la identidad autentificada asociada al cliente MEF.

NOTA 3 – La MEF, en calidad de Autoridad de Registro (RA), envía la CSR a una Autoridad de Certificación (CA). Ésta emite el certificado de cliente SCEP y devuelve el certificado a la MEF.

La MEF enviará el certificado de Cliente SCEP al cliente MEF en la respuesta, tal como se describe en la sección 4.3.1 de [IETF RFC 8824].

Cabe esperar que el cliente MEF instale el certificado de cliente SCEP y lo asocie a la clave privada correspondiente. El certificado de cliente SCEP se utilizará para la ulterior autentificación con respecto a la MEF. El certificado de cliente SCEP también puede utilizarse como certificado de entidad de extremo en otros protocolos de seguridad.

8.3.7 Información pormenorizada sobre configuración de clientes MEF

8.3.7.1 Información pormenorizada sobre configuración de credenciales de clientes MEF

El cliente MEF y la MEF deben configurarse con credenciales para la autentificación reciproca del cliente MEF y la MEF.

Las credenciales de autentificación recíproca debe configurarlas previamente o proveerlas a distancia otra MEF mediante marcos de provisión de seguridad a distancia, o por medio de la configuración de dispositivo, según se especifica en [UIT-T Y.4500.22]. Se pueden proveer credenciales de clave simétrica o credenciales de certificado. Las credenciales de clave simétrica pueden utilizarse para autentificar determinados clientes MEF y las credenciales de certificados pueden utilizarse para autentificar otros clientes MEF. La selección puede basarse en las funciones del cliente MEF.

El proceso depende del tipo de credencial (de clave simétrica o certificados) y, en el caso de las claves simétricas, del tipo de provisión (preconfiguración o provisión a distancia).

Información específica de las **claves simétricas preconfiguradas (PPSK)**: La clave simétrica preconfigurada de la parte inscrita (Kpm) y el correspondiente identificador de clave (KpmID) se proporcionarán al cliente MEF (que desempeñará el papel de parte inscrita) y a la MEF.

Información específica sobre de las **claves simétricas provistas a distancia (RPSK)**: Deberá proveerse al cliente MEF y a una función de inscripción M2M (MEF) de credenciales para establecer un marco de provisión de seguridad a distancia (RSPF). El cliente MEF deberá contar con autorización para utilizar los servicios de la MEF. Para ampliar información, véase la cláusula 8.3.2.

NOTA 1 – En este caso, la clave simétrica de la parte inscrita preconfigurada (Kpm) y el identificador de la clave (KpmID) se establecen durante el procedimiento de inscripción del cliente MEF.

Información específica de los **certificados (preconfigurados o provistos a distancia)**: Debe proveerse al cliente MEF un certificado de cliente MEF con una cadena de certificados opcional. El certificado de cliente MEF deberá ser un certificado de dispositivo, un certificado AE-ID o un certificado CSE-ID.

NOTA 2 – La configuración de los certificados CA de puntos de anclaje de confianza para la MEF se aborda en la configuración de la inscripción del cliente MEF, y puede llevarse a cabo de manera independiente de la configuración de credenciales del cliente MEF.

La especificación de configuración de dispositivos oneM2M [ITU-T Y.4500.22] proporciona un conjunto de especializaciones < *mgmtObj*> que se utilizarán para la configuración de credenciales del cliente MEF si este admita gestión de dispositivos (ya sea a distancia o a través de configuración manual). Esta Recomendación no especifica cómo se representa la configuración de credenciales del cliente MEF si éste no admite gestión de dispositivos.

8.3.7.2 Información pormenorizada sobre configuración de la inscripción del cliente MEF

Finalidad: La configuración de la inscripción del cliente MEF determina la información proporcionada a un cliente MEF para permitirle llevar a cabo procedimientos MEF autorizados por una parte interesada administradora. Ésta se encarga de que la configuración de inscripción del cliente MEF se proporcione al cliente MEF.

Condiciones previas: El cliente MEF y la MEF se configuran mediante credenciales que pueden utilizarse para la autentificación recíproca: véase la configuración de credenciales de clientes MEF en la cláusula 8.3.7.1.

Si el cliente MEF y la MEF van a utilizar certificados para autentificación recíproca:

La parte interesada administradora (u otra parte interesada en nombre de la parte interesada administradora) posee una copia de la información del certificado del cliente MEF, tal como se define en la cláusula 8.1.2.4. La MEF recibe una copia de la información del certificado del cliente MEF. La presente Recomendación no especifica cómo proporciona esa información a la MEF la parte interesada administradora (u otra parte interesada que actúe en nombre de la parte interesada administradora).

La parte interesada administradora (u otra parte interesada que actúe en nombre de la parte interesada administradora) posee una copia de los certificados CA de puntos de anclaje de confianza de la MEF. El cliente MEF recibe una copia de dichos certificados.

La parte interesada administradora se encarga de que la MEF permita al cliente MEF realizar la inscripción del cliente MEF. Ello podría implicar una autorización previa o una autorización en tiempo real.

Información pormenorizada: La configuración de inscripción del cliente MEF (*mefClientRegCfg*) incluye la información que figura en el Cuadro 8.3.7.2-1, y tiene el tipo de datos *sec:ClientRegCfg* (véase la cláusula 12.4.2).

Cuadro 8.3.7.2-1 – Información relativa a la configuración de inscripción del cliente MEF

Nombre del elemento	Multiplicidad	Notas
expirationTime	0..1	Periodo de validez de la configuración
labels	0..1	Lista de etiquetas para facilitar la detección del registro de inscripción de clientes MEF
fqdn	1	MEF-FQDN (o MEF-ID)
adminFQDN	1	FQDN de la parte interesada administradora
httpPort	0..1	Número de puerto al utilizar HTTP [b-IETF RFC 7730]
coapPort	0..1	Número de puerto al utilizar CoAP [b-IETF RFC 7252]
websocketPort	0..1	Número de puerto al utilizar WebSocket [b-IETF RFC 6455]

8.3.7.3 Información pormenorizada sobre configuración de la inscripción de la clave MEF

Finalidad: La configuración de la inscripción de la clave MEF describe la información proporcionada a un cliente MEF para que lleve a cabo procedimientos MEF autorizados por una parte interesada administradora. La parte interesada administradora se encarga de que la configuración de la inscripción del cliente MEF se proporcione al cliente MEF.

Condiciones previas: El cliente MEF lleva a cabo el procedimiento de inscripción del cliente MEF para la parte interesada administradora.

El cliente MEF tiene credenciales válidas para la autentificación recíproca con la MEF.

Información pormenorizada: La configuración de inscripción de claves MEF (*mefKeyRegCfg*) incluye la información que figura en el Cuadro 8.3.7.3-1, y posee el tipo de datos *sec:keyRegCfg* (véase la cláusula 12.4.3).

Cuadro 8.3.7.3-1 – Información relativa la configuración de inscripción de claves MEF

Nombre del elemento	Multiplicidad	Notas
expirationTime	0..1	Periodo de validez
labels	0..1	Lista de etiquetas para facilitar la detección de la inscripción de claves
adminFQDN	1	FQDN de la parte interesada administradora
SUID	1	SUID que limita el uso del valor de la clave establecido durante el procedimiento de inscripción de la clave MEF.
targetIDs	0..1	Lista de identificadores para los clientes MEF de destino autorizados

8.3.8 Perfil de configuración de dispositivos para intercambio de inscripciones

La norma [UIT-T Y.4500.22] especifica un conjunto de tipos de recursos, y procedimientos sobre esos tipos de recursos, para la configuración de AE y CSE en dispositivos sobre el terreno.

Como se indica en la cláusula 8.3.4.5, la configuración de dispositivos puede realizarse en el marco de un intercambio inscripciones con una MEF, o en una sesión DM con otros servidores DM (de forma independiente de un intercambio de inscripciones). Si la configuración de dispositivos se utiliza para un intercambio inscripciones, cabe distinguir dos restricciones en materia especializaciones de configuración < *mgmtObj*> dispositivos:

[*myCertFileCred*]: Esta especialización < *mgmtObj*> no la configura una MEF. En su lugar, una MEF utilizará los procedimientos de provisión de certificados de la cláusula 8.3.6 para proveer un certificado para que el cliente MEF lo utilice a los efectos de autentificación.

[*authenticationProfile*]: El atributo *symmKeyValue* de esta especialización < *mgmtObj*> para la provosión de claves simétricas no lo usa la MEF (véase la Nota a continuación). En su lugar, la MEF utilizará los procedimientos de provisión de claves simétricas que figuran en la cláusula 8.3.5 para proveer claves simétricas al cliente MEF. Ello requiere dos etapas:

La MEF utiliza la configuración del dispositivo para configurar un MO correspondiente a [*authenticationProfile]*, con las siguientes restricciones:

[*authenticationProfile]* se vinculará al valor de [*MEFClientRegCfg*] asociado a la inscripción en la MEF para la parte interesada administradora que autorizó [*authenticationProfile]*.

[authenticationProfile] incluirá los atributos expirationTime y MAFKeyRegDuration, y puede comprender asimismo MAFKeyRegLabels.

El recurso [*authenticationProfile]* no incluye los valores correspondientes a los atributos *symmKeyID* y *symmKeyValue*.

A continuación, la MEF emite una instrucción de control MO_NODE del cliente MEF que corresponde al nodo MO [*authenticationProfile*], como se describe en la cláusula 8.3.4.3. Ello da lugar a la ejecución de un procedimiento de inscripción de claves MEF que establece una clave simétrica y un identificador de clave simétrica en el cliente MEF y la MEF.

NOTA – *symmKeyValue* se incluye en [*authenticationProfile]* para los casos de configuración de dispositivos en los que el servidor de DM no es una MEF. Los procedimientos de provisión de clave simétrica especificados en esta Recomendación proporcionan mayor seguridad, de ahí que sean obligatorios cuando el servidor de DM es una MEF.

8.3.9 Procesamiento de instrucciones de control de clientes MEF

8.3.9.1 Introducción

Finalidad: Las instrucciones de control de clientes MEF son utilizadas por una MEF para controlar la secuencia de los procedimientos de intercambio de inscripciones ejecutados por un cliente MEF.

Una instrucción de control de clientes MEF es emitida, o reemitida, por la MEF al cliente MEF en la respuesta de un procedimiento de obtención de instrucción de control de cliente MEF (cláusula 8.3.9.2) o un procedimiento de actualización de instrucción de control de cliente MEF (cláusula 8.3.9.3). El resultado, tras el intento de analizar y ejecutar dicha instrucción, se comunica al cliente MEF en la petición de un procedimiento de actualización de instrucciones de control de cliente MEF (cláusula 8.3.9.3).

Una respuesta de obtención de una instrucción de control de cliente MEF o una respuesta de actualización de una instrucción de control de cliente MEF incluye *cmdID, cmdDescription* y *cmdStatusCode* inicial de una instrucción de control de cliente MEF que la MEF emite, o vuelve a emitir, al cliente MEF. Una petición de actualización de una instrucción de control de cliente MEF, enviada desde el cliente MEF a la MEF, incluye *cmdID* y *cmdStatusCode* para indicar el resultado del intento de análisis y ejecución de dicha instrucción de control.

Estos tres elementos permiten alcanzar los objetivos siguientes:

cmdID: evita la ambigüedad entre las instrucciones de control secuenciales de cliente MEF emitidas en el marco de una inscripción de cliente MEF (que, en algunos casos, puede ser una de las múltiples inscripciones de cliente MEF en la MEF). Por otro lado, *cmdID* permite: garantizar que una instrucción de control no se ejecute accidentalmente dos veces; y vincular el estado de una instrucción de control de cliente MEF a la correspondiente instrucción de control emitida.

cmdDescription: proporciona una descripción de la instrucción de control que debe ejecutarse.

cmdStatusCode: permite a la MEF indicar si una instrucción de control es una instrucción reemitida o no, y al cliente MEF indicar el resultado del intento de análisis y ejecución de la instrucción.

Los procedimientos de instrucciones de control de cliente MEF tienen lugar en el marco de una inscripción de cliente MEF (cuya validez no haya vencido) con respecto a la MEF.

8.3.9.2 Procedimiento de obtención de instrucciones de control de cliente MEF

Activación del procedimiento: Véase en la cláusula 8.3.4.6 los mecanismos que pueden activar los procedimientos de las instrucciones de control de cliente MEF.

Condiciones previas: La MEF y el cliente MEF llevan a cabo un procedimiento de toma de contacto a nivel de MEF, según se especifica en la cláusula 8.3.5.2.2.

La inscripción de un cliente MEF sigue siendo válida y el cliente MEF ha obtenido *MEFClientRegID* a los efectos de inscripción.

El cliente MEF no enviará ninguna instrucción de control del cliente MEF en el periodo comprendido entre el instante en que un cliente MEF recibe de la MEF una instrucción de control del cliente MEF, y el momento en que el cliente MEF envía la correspondiente actualización de instrucción de control del cliente MEF para informar sobre el estado al respecto.

El cliente MEF no iniciará el proceso de obtención de una instrucción de control de cliente MEF mientras espera la respuesta de otra instrucción de control de cliente MEF, a menos que la MEF tarde demasiado en responder. La duración de la espera de una respuesta de la MEF es una decisión que viene dada por la implementación del cliente MEF.

Procedimiento: El cliente MEF enviará una petición de obtención de una instrucción de control de cliente MEF que incluya la información que figura en el Cuadro 8.3.9.2-1.

Cuadro 8.3.9.2-1 – Información del mensaje de petición de obtención de una instrucción de control de cliente MEF

Elemento	Descripción	Multiplicidad
MEFClientRegID	Identificador del registro de inscripción del cliente MEF para el que se solicita la instrucción de control de cliente MEF. Véase la condición previa B. Se trata del identificador del recurso de nivel jerárquico superior <mefClientReg> de la instrucción de control de cliente MEF.	1

Tras recibir dicha petición, la MEF la procesará. Si se producen errores, la MEF enviará una respuesta de error.

Si la petición se procesa satisfactoriamente, la MEF intentará obtener la instrucción de control de cliente MEF asociada al registro de inscripción del cliente MEF identificado.

Si no existen más instrucciones de control de cliente MEF que deban enviarse al cliente MEF, la MEF constituirá el parámetro *cmdDescription* como se especifica en la cláusula 8.3.9.6.

Si la instrucción de control de cliente MEF activa un procedimiento de provisión de certificados, la MEF constituirá el parámetro *cmdDescription* como se especifica en la cláusula 8.3.9.7.

Si la instrucción de control de cliente MEF activa la configuración del dispositivo, la MEF constituirá el parámetro *cmdDescription* como se especifica en la cláusula 8.3.9.8.

En el caso de una instrucción de control de cliente MO_NODE, la MEF constituirá el parámetro *cmdDescription* como se especifica en la cláusula 8.3.9.9.

La MEF deberá componer una respuesta para la obtención de la instrucción de control de cliente MEF que contenga los parámetros enumerados en el Cuadro 8.3.9.2-2.

Cuadro 8.3.9.2-2 – Información del mensaje de respuesta para la obtención de la instrucción de control de cliente MEF

Elemento	Descripción	Multiplicidad
cmdID	Identificador de una instrucción de control de cliente MEF emitida por la MEF (véase la definición del tipo de datos en la cláusula 8.6.1 que figura en [UIT-T Y.4500.32])	1
cmdDescription	Descripción de la instrucción de control de cliente MEF que se emite o vuelve a emitirse.	1
cmdStatusCode	Valor de cmdStatusCode correspondiente a MEF_CLIENT_CMD_ISSUED o MEF_CLIENT_CMD_REISSUED, en su caso (véanse las cláusulas 8.3.9.5.2 y 8.3.9.5.3)	1

La MEF enviará la respuesta al cliente MEF.

El cliente MEF intentará analizar y procesar la información de respuesta.

El cliente MEF intentará analizar la información del mensaje de respuesta para los elementos *cmdID*, *cmdDescription* y *cmdStatusCode*, y analizar *cmdDescription* respecto de sus elementos constitutivos *cmdClassID* y *cmdArgs*. Si el análisis se efectúa satisfactoriamente, el cliente MEF pasará a la etapa 5b. En caso contrato, el cliente MEF puede interrumpir el procedimiento o retomar la etapa 1.

El cliente MEF comparará el *cmdID* del mensaje de respuesta con el parámetro *cmdID* enviado en el procedimiento de actualización de instrucción de control del cliente MEF más reciente. Si los valores de *cmdID* son distintos, el cliente MEF pasará a la etapa 5.c. Si los valores de *cmdID* son idénticos, el cliente MEF interrumpirá el procedimiento, y activará el procedimiento de actualización de instrucción de control de cliente MEF para dicho *cmdID;* el valor de *cmdStatusCode* corresponderá a MEF_CLIENT_CMD_REPEATED_CMD_ID.

El cliente MEF interpreta *cmdClassID* para determinar la correspondiente clase de instrucción de control de cliente MEF. Si el cliente MEF admite la clase de instrucción de control de cliente MEF, éste pasará a la etapa 5.d. Si el cliente MEF no admite la clase de instrucción de control de cliente MEF, éste interrumpirá el procedimiento, y activará el procedimiento de actualización de instrucciones de control de cliente MEF para dicho *cmdID;* el valor de *cmdStatusCode* corresponderá a MEF_CLIENT_CMD_CLASS_NOT_SUPPORTED.

El cliente MEF inicia los procedimientos específicos de la clase de instrucciones de control de cliente MEF:

Los procedimientos específicos de la clase de instrucciones de control de cliente MEF NO_MORE_COMMANDS figuran en la cláusula 8.3.9.6.

Los procedimientos específicos de la clase de instrucciones de control de cliente MEF CERT_PROV figuran en la cláusula 8.3.9.7.

Los procedimientos específicos de la clase de instrucciones de control de cliente MEF DEV_CFG figuran en la cláusula 8.3.9.8.

Los procedimientos específicos de la clase de instrucciones de control de cliente MEF MO_NODE figuran en la cláusula 8.3.9.9.

8.3.9.3 Procedimiento de actualización de instrucciones de control de cliente MEF

Activación: El cliente MEF deberá iniciar el procedimiento de actualización de instrucciones de control de cliente MEF sólo cuando se active a través del procedimiento de obtención de instrucciones de control de cliente MEF (cláusula 8.3.9.2), el procedimiento de actualización de instrucciones de control de cliente MEF (como se define en la presente cláusula) o un procedimiento específico de clase de instrucciones de control de cliente MEF (cláusulas 8.3.9.6, 8.3.9.7, 8.3.9.8, 8.3.9.9). El elemento activador incluye los valores de *cmdID* y *cmdStatusCode*.

Condiciones previas: La MEF y el cliente MEF llevan a cabo un procedimiento de toma de contacto a nivel de MEF, según se establece en la cláusula 8.3.5.2.2.

La inscripción de cliente MEF sigue siendo válida y el cliente MEF obtiene *MEFClientRegID* a los efectos de inscripción.

Procedimiento: El cliente MEF enviará una solicitud de actualización de la instrucción de control de cliente MEF que incluya la información que figura en el Cuadro 8.3.9.3-1.

Cuadro 8.3.9.3-1 – Información del mensaje de petición de actualización de la instrucción de control de cliente MEF

Elemento	Descripción	Multiplicidad
MEFClientRegID	Identificador del registro de inscripción del cliente MEF para el que se solicita la instrucción de control de cliente MEF. Véase la condición previa B.	1
cmdID	Proporcionado al activarse el procedimiento	1
cmdStatusCode	Proporcionado al activarse el procedimiento	1

Tras recibir dicha petición, la MEF la procesará.

La MEF intentará analizar la información del mensaje de petición respecto de los elementos *MEFClientRegID, cmdID* y *cmdStatusCode*. Si el análisis se realiza satisfactoriamente, la MEF pasa a la etapa 2b. En caso contrario, la MEF enviará una respuesta de actualización de la instrucción de control de cliente MEF con el código de estado de solicitud BAD_REQUEST que figura en el Cuadro 5.1.2-3 en [UIT-T Y.4500.32], y no se alcanzan nuevas etapas.

La MEF compara el valor de *cmdID* de la petición con respecto al *cmdID* de las instrucciones de control del cliente MEF emitidas más recientemente. Si no coinciden, el *cmdID* y el *cmdStatusCode* se descartan. Si coinciden, la MEF puede inscribir el *cmdID* y el *cmdStatusCode.*

La MEF determina la siguiente instrucción de control del cliente MEF que se emitirá al cliente MEF, como se describe en la etapa 3 de la cláusula 8.3.9.2.

La MEF deberá componer una respuesta de actualización relativa a la instrucción de control de cliente MEF que contenga los mismos elementos que una respuesta relativa a la obtención de instrucciones de control del cliente MEF, con arreglo a lo especificado en el Cuadro 8.3.9.2-2 en la etapa 4 de la cláusula 8.3.9.2. La MEF enviará la respuesta al clienteMEF.

El cliente MEF intentará analizar y aplicar la información del mensaje de respuesta, como se especifica en la etapa 5 de la cláusula 8.3.9.2.

8.3.9.4 Elemento cmdDescription

El elemento *cmdDescription* posee el tipo de datos *sec:cmdDescription* definido en la cláusula 12.4.4 e incluye los siguientes elementos:

cmdClassID, que identifica una clase de instrucciones de control de cliente MEF.

(condicionado al *cmdClassID*) *cmdArgs,* que contiene argumentos específicos para la *cmdClass*.

(opcional) *targetID*: si el cliente MEF es un nodo que actúa en nombre de una CSE y/o varias AE, *targetID* identificará la entidad a que es aplicable dicha instrucción.

El procesamiento de instrucciones de control de cliente MEF admite las siguientes clases de instrucciones de control de cliente MEF:

NO_MORE_COMMANDS: indica que la MEF no tiene más instrucciones de control de cliente MEF para el cliente MEF. La instrucción de control de cliente MEF NO_MORE_COMMANDS se especifica en la cláusula 8.3.9.6.

CERT_PROV: para activar los procedimientos de provisión de certificados. Las instrucciones de control de cliente MEF CERT_PROV figuran en la cláusula 8.3.9.7.

DEV_CFG: para activar la configuración del dispositivo. Las instrucciones de control de cliente MEF DEV_CFG se especifican en la cláusula 8.3.9.8.

MO_NODE: para activar procedimientos. Las instrucciones de control de cliente MEF CERT_PROV MEF Client se especifican en la cláusula 8.3.9.9.

8.3.9.5 Elemento *cmdStatusCode*

8.3.9.5.1 Introducción

El elemento *cmdStatusCode* lo utilizan la MEF y el cliente MEF para indicar el estado de una instrucción de control emitida. El valor del elemento *cmdStatusCode* es del tipo de datos *sec:cmdStatusCode*, especificado en la cláusula 12.3.2.4. En el Cuadro 8.3.9.5.1-1 se proporciona un resumen informativo de *cmdStatusCode*, incluida una descripción normativa en las demás subcláusulas de 8.3.9.5.

Cuadro 8.3.9.5.1-1 – Descripción general del elemento *cmdStatusCode*

cmdStatusCode	Asignado por	cmdClass de la instrucción de control de cliente MEF emitida	Cláusula
MEF_CLIENT_CMD_ISSUED	MEF	Cualquiera	8.3.9.5.2
MEF_CLIENT_CMD_REISSUED	MEF	Cualquiera	8.3.9.5.3
MEF_CLIENT_CMD_OK	Cliente MEF	Cualquiera. Véase la Nota	8.3.9.5.4
MEF_CLIENT_CMD_REPEATED_CMD_ID	Cliente MEF	Cualquiera	8.3.9.5.5
MEF_CLIENT_CMD_CLASS_NOT_SUPPORTED	Cliente MEF	Cualquiera. Véase la Nota	8.3.9.5.6
MEF_CLIENT_CMD_BAD_ ARGUMENTS	Cliente MEF	Cualquiera.	8.3.9.5.7
MEF_CLIENT_CMD_UNACCEPTABLE_ARGUMENTS	Cliente MEF	CERT_PROV, DEV_CFG, MO_NODE	8.3.9.5.8
MEF_CLIENT_CMD_CERT_PROV_SERVER_ERROR	Cliente MEF	CERT_PROV	8.3.9.5.9
MEF_CLIENT_CMD_CERT_PROV_CLIENT_ERROR	Cliente MEF	CERT_PROV	8.3.9.5.10
MEF_CLIENT_CMD_DEV_CFG_SERVER_ERROR	Cliente MEF	DEV_CFG	8.3.9.5.11
MEF_CLIENT_CMD_DEV_CFG_CLIENT_ERROR	Cliente MEF	DEV_CFG	8.3.9.5.12
MEF_CLIENT_CMD_MO_NODE_NOT_FOUND	Cliente MEF	MO_NODE	8.3.9.5.13
MEF_CLIENT_CMD_MO_NODE_TYPE_CONFLICT	Cliente MEF	MO_NODE	8.3.9.5.14
MEF_CLIENT_CMD_MO_NODE_BAD_ARGS	Cliente MEF	MO_NODE	8.3.9.5.15
MEF_CLIENT_CMD_MO_NODE_UNACCEPTABLE_ARGS	Cliente MEF	MO_NODE	8.3.9.5.16
MEF_CLIENT_CMD_MO_NODE_INCONSISTENT_CONFIG	Cliente MEF	MO_NODE	8.3.9.5.17
MEF_CLIENT_CMD_MO_NODE_PROCESSING_FAILED	Cliente MEF	MO_NODE	8.3.9.5.18
NOTA 1 – En circunstancias normales, un cliente MEF no debe proporcionar este valor de *cmdStatusCode* si la instrucción de control emitida incorpora un elemento *cmdClass* que indica NO_MORE_COMMANDS.			

8.3.9.5.2 *cmdStatusCode* MEF_CLIENT_CMD_ISSUED

La MEF va a emitir la instrucción de control y espera que sea la primera vez que el cliente MEF recibe dicha instrucción.

8.3.9.5.3 *cmdStatusCode* MEF_CLIENT_CMD_REISSUED

La MEF ha emitido la instrucción de control, sin recibir del cliente MEF la correspondiente actualización de la instrucción de control de cliente MEF (para facilitar, en particular, el estado de la instrucción de control ejecutada); en consecuencia, la MEF vuelve a emitir la instrucción de control.

Si el cliente MEF ya ha aplicado la instrucción de control, informará de su estado, de lo contrario el cliente MEF aplicará dicha instrucción de control.

8.3.9.5.4 *cmdStatusCode* MEF_CLIENT_CMD_OK

El cliente MEF ha aplicado satisfactoriamente la instrucción de control.

8.3.9.5.5 *cmdStatusCode* MEF_CLIENT_CMD_ REPEATED_CMD_ID

El valor de *cmdID* en el mensaje de respuesta de la instrucción de control del cliente MEF coincide con el *cmdID* enviado en el procedimiento de actualización de la instrucción de control del cliente MEF más reciente. Ello indicaría un posible error de procesamiento en la MEF.

8.3.9.5.6 *cmdStatusCode* MEF_CLIENT_CMD_CLASS_NOT_SUPPORTED

El cliente MEF no admite el valor de *cmdClass* solicitado.

8.3.9.5.7 *cmdStatusCode* MEF_CLIENT_CMD_BAD_ARGUMENTS

El cliente MEF admite el valor de *cmdClass*, si bien no puede analizar *cmdArgs*.

8.3.9.5.8 *cmdStatusCode* MEF_CLIENT_CMD_UNACCEPTABLE_ARGUMENTS

El cliente MEF admite el valor de *cmdClass* y analiza el elemento *cmdArgs*, pero al menos uno de los elementos de *cmdArgs* que podía procesar el cliente MEF tenía un valor inadecuado.

8.3.9.5.9 *cmdStatusCode* MEF_CLIENT_CMD_CERT_PROV_SERVER_ERROR

El cliente MEF admite CERT_PROV *cmdClass* y analiza el elemento *cmdArgs*, si bien no puede ejecutar la instrucción de control por algún error relativo a la comunicación con el servidor de provisión de certificados, o algún error interno del servidor de provisión de certificados.

8.3.9.5.10 *cmdStatusCode* MEF_CLIENT_CMD_CERT_PROV_CLIENT_ERROR

El cliente MEF admite CERT_PROV *cmdClass* y analiza el elemento *cmdArgs*, si bien no puede ejecutar la instrucción de control por algún error de procesamiento en el cliente MEF.

8.3.9.5.11 *cmdStatusCode* MEF_CLIENT_CMD_DEV_CFG_SERVER_ERROR

El cliente MEF admite DEV_CFG *cmdClass* y analiza el elemento *cmdArgs*, si bien no puede ejecutar la instrucción de control por algún error relacionado con la comunicación con el servidor de configuración del dispositivo, o un error interno del servidor de configuración del dispositivo.

8.3.9.5.12 *cmdStatusCode* MEF_CLIENT_CMD_DEV_CFG_CLIENT_ERROR

El cliente MEF admite DEV_CFG *cmdClass* y analiza el elemento *cmdArgs*, si bien no puede ejecutar la instrucción de control por algún error de procesamiento en el cliente MEF.

8.3.9.5.13 *cmdStatusCode* MEF_CLIENT_CMD_MO_NODE_NOT_FOUND

El cliente MEF admite MO_Node *cmdClass* y analiza el elemento *cmdArgs*, si bien no puede encontrar el nodo MO en el elemento *objectPath* en los argumentos de la instrucción de control del cliente MEF.

8.3.9.5.14 *cmdStatusCode* MEF_CLIENT_CMD_MO_NODE_TYPE_CONFLICT

El cliente MEF admite *MO_Node cmdClass*, analiza el elemento *cmdArgs* y encuentra el nodo MO en el elemento *objectPath*, si bien el tipo de nodo MO no corresponde al elemento *objectType* en los argumentos de la instrucción de control del cliente MEF.

8.3.9.5.15 *cmdStatusCode* MEF_CLIENT_CMD_MO_NODE_BAD_ARGS

El cliente MEF admite MO_Node *cmdClass*, analiza el elemento *cmdArgs*, encuentra el nodo MO en el elemento *objectPath*, y el tipo de nodo MO corresponde al elemento *objectTypeID*, si bien el cliente MEF no puede analizar *el* elemento *objectTypeSpecifcArgs*.

8.3.9.5.16 *cmdStatusCode* MEF_CLIENT_CMD_MO_NODE_UNACCEPTABLE_ARGS

El cliente MEF admite MO_Node *cmdClass*, analiza el elemento *cmdArgs*, encuentra el nodo MO en el elemento *objectPath*, el tipo de nodo MO corresponde al elemento *objectType*, y el cliente MEF no puede analizar el elemento *objectTypeSpecifcArgs*, si bien los demás argumentos específicos del tipo MO en los argumentos de la instrucción de control del cliente MEF son inaceptables para el cliente MEF.

8.3.9.5.17 *cmdStatusCode* MEF_CLIENT_CMD_MO_NODE_INCONSISTENT_CONFIG

El cliente MEF admite *cmdClass* MO_Node, analiza el elemento *cmdArgs* y encuentra el nodo MO en el elemento *objectPath*,el tipo de nodo MO corresponde al elemento *objectTypeID*, y los demás argumentos específicos del tipo MO en los argumentos de la instrucción de control de cliente MEF son aceptables, si bien la configuración de los nodos MO es incoherente e impide el procesamiento del nodo MO.

8.3.9.5.18 *cmdStatusCode* MEF_CLIENT_CMD_MO_NODE_PROCESSING_FAILED

El cliente MEF admite MO_Node *cmdClass*, analiza el elemento *cmdArgs*, encuentra el nodo MO en el elemento *objectPath*, y el tipo de nodo MO corresponde al elemento *objectType*, y los demás argumentos específicos del tipo MO en los argumentos de la instrucción de control del cliente MEF son aceptables, si bien se produce otro error en la ejecución del procesamiento del nodo MO.

8.3.9.6 Procesos específicos para la clase de instrucciones de control de cliente MEF NO_MORE_COMMANDS

Finalidad: Si *cmdClassID* indica NO_MORE_COMMANDS, la MEF señalará que no tiene más instrucciones de control de cliente MEF para el cliente MEF.

Elementos de *cmdArgs*: Si *cmdDescription* contiene *cmdClassID* que indica NO_MORE_COMMANDS, *cmdArgs* contendrá el elemento *noMoreCmdArgs* de tipo de datos *sec:noMoreCmdArgs* que incluye los siguientes elementos:

retryDuration: indica duración, tras la cual cabe esperar que el cliente MEF intente obtener la instrucción de control de cliente MEF. El valor del parámetro *retryDuration* se anula si el cliente MEF lleva a cabo satisfactoriamente otro procedimiento de instrucción de control de cliente MEF, en relación con la inscripción del cliente MEF, antes de llevar a cabo *retryDuration*. En la la cláusula 8.3.4.6 se especifican otros mecanismos que pueden activar procedimientos de instrucciones de control de cliente MEF.

Constitución de *cmdDescription*: La MEF constituirá *cmdArgs* con los elementos que se describen anteriormente en "Elementos de cmdArgs":

retryDuration: establece el periodo de tiempo antes de que la MEF autorice al cliente MEF a intentar obtener la siguiente instrucción de control de cliente MEF, habida cuenta de que *retryDuration* se anulará si el cliente MEF lleva a cabo satisfactoriamente otro procedimiento de instrucción de control de cliente MEF.

La MEF constituirá *cmdDescription* con *cmdClassID* indicando NO_MORE_COMMANDS, y *cmdArgs* constituido en la etapa 1.

Análisis y ejecución de *cmdArgs*: El cliente MEF intentará analizar *cmdArgs* en los elementos descritos en "Elementos de cmdArgs". Si el análisis se lleva a cabo satisfactoriamente, el cliente MEF pasa a la etapa 4. Si el análisis no se lleva a cabo satisfactoriamente, el cliente MEF interrumpe el

procedimiento y activa el procedimiento de actualización de instrucción de control de cliente MEF para ese *cmdID*, con el valor de *cmdStatusCode* correspondiente a MEF_CLIENT_CMD_BAD_ARGUMENTS.

La instrucción de control de cliente MEF no realizará ningún procedimiento de obtención de la instrucción de control de cliente MEF, ni ningún procedimiento de actualización de dicha instrucción de control de cliente MEF, a menos que se active.
El cliente MEF deberá establecer un temporizador basado en *retryDuration*.

Dicho temporizador se anulará si, mediante uno de los mecanismos descritos en la cláusula 8.3.4.6, el cliente MEF se activa para llevar a cabo un procedimiento de obtención de una instrucción de control de cliente MEF o un procedimiento de actualización de instrucción de cliente MEF antes de que venza el periodo de validez del temporizador.

Si dicho periodo vence, el cliente MEF deberá realizar un procedimiento de obtención de instrucción de cliente MEF (cláusula 8.3.9.2) cuando lo decida el cliente MEF.

8.3.9.7 Procesos específicos para la clase de instrucciones de control de cliente MEF CERT_PROV

Finalidad: Si *cmdClassID* indica CERT_PROV, la MEF señalará que el cliente MEF debe llevar a cabo un procedimiento de provisión de certificados con respecto a la MEF.

Elementos de *cmdArgs*: Si *cmdDescription* contiene *cmdClassID* que indica CERT_PROV, *cmdArgs* incluirá el elemento *certProvArgs,* de tipo de datos *sec:certProvArgs*, que comprende los siguientes elementos:

certProvProtocol: indica el protocolo de provisión de certificados (EST o SCEP) que debe utilizar el cliente MEF.

URI: indica el URI de base que se utilizará para el protocolo de provisión de certificados señalado.

certSubjectType: indica si el sujeto del certificado provisto será un nodo, una CSE o una AE.

certSubjectID: el Node-ID, CSE-ID o AE-ID del sujeto del certificado.

Constitución de *cmdDescription*: La MEF constituirá *cmdArgs,* con los elementos descritos anteriormente en "Elementos de *cmdArgs"*:

certProvProtocolo: la MEF asignará este elemento para indicar el protocolo (EST o SCEP) que el cliente MEF debe utilizar a los efectos de provisión de certificados.

URI: la MEF asignará este elemento al URI de base que se utilizará para el protocolo de provisión de certificados indicado. El FQDN del URI de base deberá corresponder al FQDN de la MEF que emite la instrucción de control de cliente MEF.

certSubjectType: el cliente MEF deberá asignar este elemento para indicar si el sujeto del certificado provisto será un nodo, una CSE o una AE.

certSubjectID: la MEF asignará a este elemento los parámetros Node-ID, CSE-ID o AE-ID del sujeto del certificado.

La MEF constituirá *cmdDescription* con *cmdClassID* indicando los valores de CERT_PROV y *cmdArgs* constituidos en la etapa 1.

Análisis y ejecución de *cmdArgs*: Véase la etapa 3 que figura en la cláusula 8.3.9.6.

El cliente MEF deberá verificar que los elementos *cmdArgs* sean aceptables:

certProvProtocolo: la verificación de este elemento sólo tiene lugar satisfactoriamente si el protocolo indicado (EST o SCEP) es compatible con el cliente MEF. Si la verificación se lleva a cabo satisfactoriamente, el cliente MEF selecciona el protocolo de provisión de certificados señalado por el elemento.

URI: La verificación de este elemento sólo tiene lugar satisfactoriamente si el FQDN del URI de base coincide con el FQDN de la MEF que emite la instrucción de control de cliente MEF. Si la verificación tiene lugar satisfactoriamente, el cliente MEF establece el URI de base con respecto al valor de este elemento.

certSubjectType: Si el cliente MEF pertenece a un nodo que desempeña su función en nombre de una CSE y/o varias AE, la verificación de este elemento sólo tendrá lugar satisfactoriamente si el valor indica un nodo, una CSE o una AE.

Si el cliente MEF pertenece a una CSE, la verificación de este elemento sólo tiene lugar satisfactoriamente si el valor indica una CSE.

Si el Cliente MEF pertenece a una CSE, la verificación de este elemento sólo tiene lugar satisfactoriamente si el valor indica una CSE.

Si la verificación tiene lugar satisfactoriamente, el cliente MEF inscribe *certSubjectType* como tipo de sujeto del certificado.

certSubjectID: La verificación de este elemento depende del valor de *certSubjectType:*

Si *subjectType* indica un nodo, la verificación de este elemento sólo tiene lugar satisfactoriamente si el valor es *Node-ID*.

Si *certSubjectType* indica una CSE, la verificación de este elemento sólo tiene lugar satisfactoriamente si el valor es *AE-ID*.

Si *certSubjectID* indica una AE, la verificación de este elemento sólo tiene lugar satisfactoriamente si el valor es *CSE-ID*.

Si la verificación tiene lugar satisfactoriamente, el cliente MEF inscribe *certSubjectID* como identidad del sujeto del certificado.

Si la verificación de cualquier argumento no tiene lugar satisfactoriamente, el cliente MEF interrumpe el procedimiento, y activa el procedimiento de actualización de la instrucción de control de cliente MEF para ese *cmdID*, y el valor de *cmdStatusCode* corresponde a MEF_CLIENT_CMD_UNACCEPTABLE_ARGUMENTS.

El cliente MEF intentará ejecutar el procedimiento de provisión de certificados seleccionado (EST, según se especifica en la cláusula 8.3.6.2, o SCEP, según se especifica en la cláusula 8.3.6.3), con el URI de base, el tipo de sujeto del certificado y la identidad del sujeto del certificado determinados en la etapa 4. La identidad del sujeto del certificado se proveerá en la extensión *SubjectAltName* de la petición de firma de certificado.

Tras el intento de ejecutar el procedimiento de provisión de certificados seleccionado, el cliente MEF llevará a cabo el procedimiento de actualización de instrucciones de control de cliente MEF con *cmdID* asignado al *cmdID* de la instrucción de control recibida, y el valor de *cmdStatusCode* asignado de la siguiente manera:

Si el procedimiento de suministro de certificados se lleva a cabo satisfactoriamente, el cliente MEF establecerá el valor de *cmdStatusCode* de manera que corresponda al de MEF_CLIENT_CMD_OK.

Si el procedimiento de provisión de certificados no se lleva a cabo satisfactoriamente debido a un error de comunicación con el servidor de provisión de certificados, o a un error interno del servidor de provisión de certificados, el cliente MEF establecerá el valor de *cmdStatusCode* de forma que corresponda al de MEF_CLIENT_CMD_CERT_PROV_SERVER_ERROR.

Si el procedimiento de provisión de certificados no se lleva a cabo satisfactoriamente debido a un error en el cliente de provisión de certificados (en el cliente MEF), el cliente MEF establecerá el valor de *cmdStatusCode* de forma que corresponda al de MEF_CLIENT_CMD_CERT_PROV_CLIENT_ERROR.

8.3.9.8 Procesos específicos para la clase de instrucciones de control de cliente MEF DEV_CFG

Finalidad: Si *cmdClassID* indica DEV_CFG, la MEF señalará que el cliente MEF va a realizar una configuración de dispositivo ([UIT-T Y.4500.22]), con el cliente MEF desempeñando la función de cliente DM y la MEF la de servidor DM.

Elementos de *cmdArgs*: Si *cmdDescription* contiene *cmdClassID,* indicando DEV_CFG, *cmdArgs* incluirá el elemento *devCfgArgs,* que comprende los siguientes elementos:

devMgmtID: indica el protocolo DM (por ejemplo, OMA DMv1.3, OMA DMv2.0, OMA LwM2M, BBF TR-069), que el cliente MEF debe utilizar a los efectos de configuración del dispositivo.

URI: URI del servidor de DM.

Constitución de *cmdDescription:* La MEF constituirá *cmdArgs* con los elementos descritos anteriormente en "Elementos de cmdArgs":

devMgmtID: la MEF asignará este elemento para indicar el protocolo (por ejemplo, OMA DMv1.3, OMA DMv2.0, OMA LwM2M, BBF TR-069) que el cliente MEF debe utilizar a los efectos de configuración del dispositivo.

URI: la MEF asignará este elemento al URI del servidor de DM. El FQDN del URI de base deberá corresponder al FQDN de la MEF que emite la instrucción de control de cliente MEF.
La MEF constituirá *cmdDescription* con *cmdClassID,* indicando los valores de DEV_CFG y *cmdArgs* constituidos en la etapa 1.

Análisis y ejecución de *cmdArgs:*

Véase la etapa 3 en la cláusula 8.3.9.6.

El cliente MEF deberá verificar que los elementos *cmdArgs* son aceptables:

devMgmtID: la verificación de este elemento sólo tiene lugar satisfactoriamente si el protocolo indicado (por ejemplo, OMA DMv1.3, OMA DMv2.0, OMA LwM2M, BBF TR-069) es compatible con el cliente MEF. Si la verificación tiene lugar satisfactoriamente, el cliente MEF selecciona el protocolo DM indicado por el elemento.

URI: la verificación de este elemento sólo tiene lugar satisfactoriamente si el FQDN del URI de base corresponde al FQDN de la MEF que emite la instrucción de control deliente MEF. Si la verificación tiene lugar satisfactoriamente, el cliente MEF establece el valor del URI del servidor DM con arreglo al de dicho elemento.

Si la verificación de cualquier argumento no tiene lugar satisfactoriamente, el cliente MEF interrumpe el procedimiento, y activa el procedimiento de actualización de la instrucción de control de cliente MEF para ese *cmdID,* con valor de *cmdStatusCode* correspondiente al de MEF_CLIENT_CMD_UNACCEPTABLE_ARGUMENTS.

El cliente MEF intentará ejecutar la configuración del dispositivo según lo establecido en [UIT-T Y.4500.22] mediante el protocolo DM y el URI del servidor DM determinado en la etapa 4.

Tras el intento de ejecutar la configuración del dispositivo, el cliente MEF deberá llevar a cabo el procedimiento de actualización de instrucciones de control de cliente MEF con un *cmdID* asignado al *cmdID* de la instrucción de control recibida y *cmdStatusCode* asignado de la siguiente manera:

Si el procedimiento de configuración del dispositivo tiene lugar satisfactoriamente, el cliente MEF deberá asignar a *cmdStatusCode* el valor de MEF_CLIENT_CMD_OK.

Si el procedimiento de configuración del dispositivo no tiene lugar satisfactoriamente debido a un error de comunicación con el servidor DM, o a un error interno del servidor DM, el cliente MEF asignará a *cmdStatusCode* el valor MEF_CLIENT_CMD_DEV_CFG_SERVER_ERROR.

Si el procedimiento de configuración del dispositivo no tiene lugar satisfactoriamente debido a un error que se ha producido en el cliente DM (en el cliente MEF), el cliente MEF asignará a *cmdStatusCode* el valor MEF_CLIENT_CMD_DEV_CFG_CLIENT_ERROR.

8.3.9.9 Procesos específicos para la clase de instrucciones de control de cliente MEF MO_NODE

8.3.9.9.1 Procesos genéricos MO_NODE

Finalidad: Si *cmdClassID* indica MO_NODE, la MEF señalará que el cliente MEF debe procesar un MO_NODE que ya ha sido configurado para el cliente DM del Cliente MEF (por ejemplo, mediante la configuración de dispositivos que figura en [UIT-T Y.4500.22]).

Elementos de *cmdArgs*: Si *cmdDescription* contiene *cmdClassID* y se indica MO_NODE, *cmdArgs* deberá incluir el elemento *MONodeCmdArgs*, que comprende los siguientes elementos:

objectPath: la ruta del nodo MO que debe procesarse.

objectTypeID: el tipo de la especialización del recurso < *mgmtObj*> que proporciona el modelo de datos para el nodo MO que debe procesarse.

(Opcional) objectTypeSpecificArgs: argumentos adicionales dependientes del tipo de especialización del recurso < *mgmtObj*> (véase *objectTypeID*):

Si *objectTypeID* coincide con la especialización [*authenticationProfile*] del *recurso* < *mgmtObj*>, el elemento *objectTypeSpecificArgs* estará incluido, según se define en la cláusula 8.3.9.9.2.

Con respecto a las demás especializaciones, este elemento no está incluido.

Constitución de *cmdDescription*: La MEF constituirá *cmdArgs* de forma que se incluyan los elementos descritos anteriormente en "Elementos de *cmdArgs*":

objectPath: la MEF asignará este elemento a la ruta del nodo de la MO que debe procesarse.

objectTypeID: la MEF asignará este elemento al identificador del tipo de nodo MO que debe procesarse.

(Opcional) objectTypeSpecificArgs: Si *objectTypeID* corresponde a la especialización [*authenticationProfile*] del *recurso* < *mgmtObj*>, el elemento *objectTypeSpecificArgs* se constituirá como se especifica en "Constitución de *objectTypeSpecificArgs*", en la cláusula 8.3.9.9.2.

Con respecto a las demás especializaciones, este elemento no está incluido.

La MEF constituirá *cmdDescription* con *cmdClassID* y se indicarán los valores de MO_NODE y *cmdArgs* constituidos en la etapa 1.

Análisis y ejecución de *cmdArgs*: Véase la etapa 3 que figura en la cláusula 8.3.9.6.

El cliente MEF deberá verificar que los elementos *cmdArgs* son aceptables:

objectPath: la verificación de estos elementos sólo tiene lugar satisfactoriamente si existe un nodo MO asociado a *objectPath*. Si la verificación tiene lugar satisfactoriamente, el cliente MEF pasa a la etapa 4b. Si la verificación de este argumento no tiene lugar satisfactoriamente, el cliente MEF interrumpirá el procedimiento, y activará el procedimiento de actualización de la instrucción de control de cliente MEF para ese *cmdID*, y a *cmdStatusCode* se asignará el valor de MEF_CLIENT_CMD_MO_NODE_NOT_FOUND.

objectTypeID: la verificación de estos elementos sólo tiene lugar satisfactoriamente si *objectTypeID* corresponde al nodo de tipo MO asociado a *objectPath* (véase la etapa 4a). Si la verificación tiene lugar satisfactoriamente, el cliente MEF pasará a la etapa 5. Si la verificación de este argumento no tiene lugar satisfactoriamente, el cliente MEF interrumpirá el procedimiento, y activará el procedimiento de actualización de la instrucción de control de cliente MEF para ese *cmdID*, y a *cmdStatusCode* se asigna el valor de MEF_CLIENT_CMD_MO_NODE_TYPE_CONFLICT.

El cliente MEF aplica el procesamiento específico de *objectTypeID*:

Si *objectTypeID* coincide con la especialización [*authenticationProfile*] del recurso < *mgmtObj*>, el cliente MEF deberá llevar a cabo el "Procesamiento de un nodo MO [*authenticationProfile*]" que figura en la cláusula 8.3.9.9.2.

Si *objectTypeID* coincide con la especialización [*trustAnchorCred*] del recurso < *mgmtObj*>, el cliente MEF deberá llevar a cabo el "Procesamiento de un Nodo MO [*trustAnchorCred]"* que figura en la cláusula 8.3.9.9.7.

Si *objectTypeID* corresponde a la especialización [*MAFClientCfgReg*] del recurso < *mgmtObj*>, el cliente MEF lleva cabo el "Procesamiento de un nodo MO [*MAFClientCfgReg]"* que figura en la cláusula 8.3.9.9.8.

8.3.9.9.2 Procesos específicos para [*authenticationProfile*]

Finalidad: El procesamiento de un nodo MO [*authenticationProfile]* permite al cliente MEF establecer las credenciales necesarias para utilizar ese nodo MO [*authenticationProfile]* a los efectos de autentificación recíproca.

Elementos de *objectTypeSpecificArgs*: Si objectTypeID corresponde a la especialización [*authenticationProfile*] del recurso < *mgmtObj*>, el elemento *objectTypeSpecificArgs* estará incluido y contendrá el elemento *authProfileMONodeArgs* que comprende los siguientes elementos:

SUID: valor correspondiente al SUID del nodo MO direccionado.

Constitución de *objectTypeSpecificArgs*: La MEF constituirá *objectTypeSpecificArgs* que contengan *authProfileMONodeArgs* con los elementos descritos anteriormente en "Elementos de *objectTypeSpecificArgs"*:

SUID: La MEF asignará este elemento al valor del elemento *SUID* que se espera que esté en el nodo MO localizado en el *objectPath* del cliente MEF.

Procesamiento de un nodo MO [*authenticationProfile*]: El cliente MEF intentará analizar *objectTypeSpecificArgs* en los elementos descritos en "Elementos de *objectTypeSpecificArgs*". Si el análisis tiene lugar satisfactoriamente, el cliente MEF pasará a la etapa 3. Si el análisis no tiene lugar satisfactoriamente, el cliente MEF interrumpirá el procedimiento y activará el procedimiento de actualización de la instrucción de control de cliente MEF para este *cmdID*, y el valor de *cmdStatusCode* corresponderá al de MEF_CLIENT_CMD_MN_NODE_BAD_ARGS.

El cliente MEF deberá verificar que los elementos *objectTypeSpecificArgs* son aceptables:

SUID: La verificación tiene lugar satisfactoriamente si el SUID de *objectTypeSpecificArgs* corresponde al *SUID* en el MO_NODE direccionado.

Si la verificación de los elementos *objectTypeSpecificArgs* tiene lugar satisfactoriamente, el cliente MEF pasará a la etapa 5. Si la verificación de los elementos *objectTypeSpecificArgs no* tiene lugar satisfactoriamente para algún elemento, el cliente MEF interrumpirá el procedimiento y activará el procedimiento de actualización de instrucciones de control de cliente MEF para este *cmdID*, y el valor de *cmdStatusCode* corresponderá al valor de MEF_CLIENT_CMD_MO_NODE_UNACCEPTABLE_ARGS.

El cliente MEF verificará que el *SUID* corresponde a la configuración del nodo MO [*authenticationProfile]* y sus nodos MO de niveles superior e inferior:

Si el *SUID* pertenece al conjunto {11, 21, 31, 41}, la verificación no tendrá lugar satisfactoriamente si el nodo MO de nivel jerárquico superior del nodo MO [*authenticationProfile]* no corresponde a la especialización [*MAFClientRegCfg]* del recurso < *mgmtObj*>.

Si el *SUID* pertenece al conjunto {12, 22, 32, 42}, la verificación no tendrá lugar satisfactoriamente si el nodo MO de nivel jerárquico superior del nodo MO [*authenticationProfile]* no corresponde a la especialización [*registration]* del recurso < *mgmtObj*>.

Si el *SUID* pertenece al conjunto {13, 23, 33, 43}, la verificación no tendrá lugar satisfactoriamente si el nodo MO de nivel jerárquico superior del nodo MO [*authenticationProfile]* no corresponde a la especialización [*dataCollection]* del recurso < *mgmtObj*>.

Si el *SUID* pertenece al conjunto {11,12,13}, la verificación no tendrá lugar satisfactoriamente si el atributo *symmKeyID* no se incluye en el nodo MO [*authenticationProfile*].

Si el *SUID* pertenece al conjunto {21,22,23}, la verificación no tendrá lugar satisfactoriamente si:

El atributo *keyRegDuration* no se incluye en el nodo MO [*authenticationProfile*], o

El nodo MO de nivel jerárquico inferior del nodo MO [*authenticationProfile*] no corresponde a la especialización [*MEFClientRegCfg*] del recurso < *mgmtObj*>.

Si el *SUID* pertenece al conjunto {31,32,33}, la verificación no tendrá lugar satisfactoriamente si:

El atributo *keyRegDuration* no pertenece al nodo MO [*authenticationProfile*], o

El nodo MO de nivel jerárquico inferior del nodo MO [*authenticationProfile*] no corresponde a la especialización [*MAFClientRegCfg]* del recurso < *mgmtObj*>.

Si el *SUID* pertenece al conjunto {11, 12, 21, 22, 31, 32}, la verificación no tendrá lugar satisfactoriamente si:

El atributo *TLSCiphersuites* no se incluye en el nodo MO [*authenticationProfile*], o

El atributo *TLSCiphersuites* se incluye, pero no comprende los cifrados DTLS o TLS obligatorios para los marcos de seguridad basados en TLS-PSK que figuran en la cláusula 10.2.2.

Si el *SUID* pertenece al conjunto {41, 42, 43}, la verificación no tendrá lugar satisfactoriamente si:

El atributo *myCertFingerprint* no se incluye en el nodo MO [*authenticationProfile*], o

El atributo *TLSCiphersuites* no se incluye en el nodo MO [*authenticationProfile*] o el atributo *TLSCiphersuites* se inluye, pero no comprende cifrados DTLS o TLS obligatorios para los marcos de seguridad basados en certificados relativos a la cláusula 10.2.3, o

El nodo MO [*authenticationProfile*] tiene uno o más nodos MO de nivel jerárquico inferior correspondientes a la especialización [*trustAnchorCred*] del recurso < *mgmtObj*>.

Si la verificación tiene lugar satisfactoriamente, el cliente MEF pasará a la etapa 5. Si la verificación de ese argumento no tiene lugar satisfactoriamente para algún elemento, el cliente MEF interrumpirá el procedimiento y se activará el procedimiento de actualización de la instrucción de control del cliente MEF para ese *cmdID*, con valor de *cmdStatusCode* correspondiente al valor de MEF_CLIENT_CMD_MO_NODE_INCONSISTENT_CONFIG.

El cliente MEF aplica el tratamiento específico del *SUID*:
Si el *SUID* pertenece al conjunto {11,12,13}, correspondiente a un SUID de clave simétrica preconfigurada, el cliente MEF lleva a cabo el "Procesamiento de un nodo MO [authenticationProfile] con SUID de clave simétrica preconfigurada" que figura en la cláusula 8.3.9.9.3.

Si el *SUID* pertenece al conjunto {21,22,23}, correspondiente a un SUID de clave simétrica establecida por la MEF, el cliente MEF lleva a cabo el "Procesamiento de un nodo MO [authenticationProfile] con SUID de clave simétrica establecida por la MEF" que figura en la cláusula 8.3.9.9.4.

Si el *SUID* pertenece al conjunto {31,32,33}, correspondiente a un SUID de clave simétrica establecida por la MAF, el cliente MEF lleva cabo el "Procesamiento de un nodo MO

[authenticationProfile] con SUID de clave simétrica establecida por la MAF" que figura en la cláusula 8.3.9.9.5.

Si el *SUID* pertenece al conjunto {41,42,43}, correspondiente a un SUID de certificado, el cliente MEF lleva cabo el "Procesamiento de un nodo MO [authenticationProfile] con SUID de certificado" que figura en la cláusula 8.3.9.9.6.

8.3.9.9.3 Procesamiento de un nodo MO [*authenticationProfile*] con clave simétrica preconfigurada

Finalidad: El procesamiento de un nodo MO [*authenticationProfile*] con SUID de clave simétrica preconfigurada (para el conjunto {11, 12, 13}) permite que el cliente MEF tenga acceso a una copia local de la clave simétrica preconfigurada, para su ulterior utilización con el nodo MO [*authenticationProfile*].

Condiciones previas: Este procedimiento sólo se llevará a cabo satisfactoriamente si existe una copia local del valor de la clave simétrica preconfigurada a la que pueda acceder la MEF.

Procedimiento: El Cliente MEF deberá determinar si el atributo *symmKeyValue* se incluye en el nodo MO [*authenticationProfile*].

Si el atributo no se incluye, el cliente MEF deberá pasar a la etapa 2.

Si el atributo se incluye, el cliente MEF tendrá acceso al valor de la clave simétrica preconfigurada. El cliente MEF interrumpirá el procedimiento y se activará el procedimiento de actualización de la instrucción de control de cliente MEF para ese *cmdID*, y el valor de *cmdStatusCode* corresponderá al de MEF_CLIENT_CMD_OK.

El cliente MEF obtiene el valor del atributo *symmKeyID* del nodo MO [*authenticationProfile*]. El cliente MEF determina si el cliente MEF tiene una copia local del valor de la clave simétrica con un identificador que corresponda al atributo *symmKeyID*.

Si no se incluye ninguna copia local del valor de la clave simétrica, el cliente MEF no tendrá acceso al valor de la clave simétrica preconfigurada. El cliente MEF interrumpirá el procedimiento y se activará el procedimiento de actualización de la instrucción de control de cliente MEF para ese *cmdID,* y el valor de *cmdStatusCode* corresponderá al de MEF_CLIENT_CMD_MO_NODE_PROCESSING_FAILED.

Si se incluye una copia local del valor de la clave simétrica, el cliente de MEF tendrá acceso al valor de la clave simétrica preconfigurada. El cliente MEF interrumpirá el procedimiento y se activará el procedimiento de actualización de la instrucción de control de cliente MEF para ese *cmdID,* y el valor de *cmdStatusCode* corresponderá al de MEF_CLIENT_CMD_OK.

8.3.9.9.4 Procesamiento de un nodo NO [*authenticationProfile*] con clave simétrica establecida por una MEF

Finalidad: El procesamiento de un nodo MO [*authenticationProfile]* con un SUID de clave simétrica establecida por una MEF (para el conjunto {21, 22, 23}) permite que el cliente MEF establezca una clave simétrica con la MEF para su ulterior utilización con el nodo MO [*authenticationProfile*].

Condiciones previas: Este procedimiento sólo tiene lugar de forma satisfactoria si el nodo MO [*authenticationProfile*] posee un nodo MO de nivel jerárquico inferior [*MEFClientRegCfg*] y un nodo MO de nivel jerárquico superior que puede ser de tipo [*MAFClientRegCfg*], [*registration*] o [*dataCollection*].

Para este procedimiento se realiza la hipótesis de que el cliente MEF posee un registro de cliente MEF válido con respecto a la MEF y la parte interesada administradora identificada en el nodo MO de nivel jerárquico inferior [*MEFClientRegCfg*].

Procedimiento: El cliente MEF intentará llevar a cabo el procedimiento de inscripción de clave MEF que se describe en la cláusula 8.3.5.2.7, en el que cliente MEF desempeñará la función de cliente MEF de origen, habida cuenta de lo siguiente:

En la etapa 4 de la cláusula 8.3.5.2.7, el cliente MEF debe constituir la petición de inscripción de clave MEF (véase el Cuadro 8.3.5.2.7-1) de la siguiente manera:

MEFFQDN: se establecerá el valor del atributo *fqdn* en el nodo MO de nivel jerárquico inferior [*MEFClientRegCfg*];

expirationTime se calculará sumando el valor temporal en curso al valor de *keyRegDuration* para el nodo MO [*authenticationProfile*];

Se asignará a *labels* el valor del atributo *keyRegLabels* en el nodo MO [*authenticationProfile*];

adminFQDN: se asignará al valor del atributo *adminFQDN* en el nodo MO de nivel jerárquico inferior [*MEFClientRegCfg*];

SUID: se asignará al valor del atributo *SUID* en el nodo MO de nivel jerárquico inferior [*authenticationProfile*];

targetIDs: se asignará con arreglo al nodo MO de nivel jerárquico superior del nodo MO [*authenticationProfile*]:

En el caso de un nodo MO de nivel jerárquico superior [*registration*], a los valores de *targetID se les* asignará el CSE-ID de la CSE encargada de la inscripción.

En el caso de un nodo MO de nivel jerárquico superior [*dataCollection]*, se asignará a los valores de *targetID* el CSE-ID determinado por medio del atributo *containerPath del* nodo MO [*dataCollection*].

En el caso de un nodo MO [*MAFClientRegCfg]* de nivel jerárquico superior, se asignará a los valores *targetIDs* el atributo *FQDN del* nodo MO [*MAFClientRegCfg*].
keyValue: no debe incluirse.

El cliente MEF deberá seleccionar un protocolo (HTTP, CoAP, WebSocket) basado en los protocolos admitidos por el cliente MEF, y los protocolos admitidos por la MEF se indican mediante la inclusión de *httpPort*, *coapPort* y *websocketPort* en el nodo MO de nivel jerárquico inferior [*MEFClientRegCfg]*. El cliente MEF deberá utilizar el número de puerto proporcionado en el atributo *httpPort*, *coapPort* o *websocketPort* apropiado del nodo MO de nivel jerárquico inferior [*MEFClientRegCfg]*.

En la etapa 10 de la cláusula 8.3.5.2.7, si el cliente MEF recibe una respuesta de inscripción de clave MEF satisfactoria (véase el Cuadro 8.3.5.2.7-2), dicho cliente MEF verificará la siguiente información recibida en la respuesta de inscripción de clave MEF:

expirationTime: La verificación no se realizará de forma satisfactoria si este valor es anterior al valor temporal para el que se realiza la verificación.

Source MEF Client ID: La verificación no se realizará de forma satisfactoria si este valor difiere del identificador del cliente MEF.

adminFQDN: La verificación no se realizará de forma satisfactoria si este valor es distinto del valor correspondiente enviado en la petición de inscripción de claves MEF en la etapa 4 de la cláusula 8.3.5.2.7.

SUID: La verificación no se realizará de forma satisfactoria si este valor es distinto del valor correspondiente enviado en la petición de inscripción de claves MEF en la etapa 4 de la cláusula 8.3.5.2.7.

targetIDs: La verificación no se realizará de forma satisfactoria si este valor es distinto del valor correspondiente enviado en la petición de inscripción de claves MEF en el etapa 4 de la cláusula 8.3.5.2.7.

Si la verificación se realiza de forma satisfactoria, el cliente MEF almacenará la información en la respuesta de inscripción de claves MEF y asociará esa información al nodo MO [*authenticationProfile*]. El cliente MEF interrumpirá el procedimiento, y se activará el procedimiento de actualización de la instrucción de control del cliente MEF para ese *cmdID*, y el valor de *cmdStatusCode* corresponderá a MEF_CLIENT_CMD_OK.

Si la verificación no se realiza de forma satisfactoria, o si el procedimiento no se lleva a cabo por cualquier otra razón, el cliente MEF interrumpe el procedimiento, y se activa el procedimiento de actualización de instrucción de control de cliente MEF para ese *cmdID*, y el valor de *cmdStatusCode* corresponderá a MEF_CLIENT_CMD_MO_NODE_PROCESSING_FAILED.

8.3.9.9.5 Procesamiento de un nodo MO [*authenticationProfile*] con clave simétrica establecida por MAF

Finalidad: El procesamiento de un nodo MO [*authenticationProfile]* con SUID de clave simétrica establecida por una MEF (para el conjunto {31,32,33}) permite al cliente MEF, en calidad de cliente MAF de origen, establecer una clave simétrica con la MAF para su ulterior utilización con el nodo MO [*authenticationProfile*].

Condiciones previas: Este procedimiento sólo tiene lugar de forma satisfactoria si el nodo MO [*authenticationProfile*] posee un nodo MO de nivel jerárquico inferior [*MAFClientRegCfg*] y un nodo MO de nivel jerárquico superior que puede ser de tipo [*registration*] o [*dataCollection*].

Para este procedimiento se realiza la hipótesis de que el cliente MEF, en calidad de cliente MAF, posee un registro de cliente MAF válido con respecto a la MAF y la parte interesada administradora identificada en el nodo MO de nivel jerárquico inferior [*MAFClientRegCfg*].

Procedimiento: El cliente MEF intentará llevar a cabo el procedimiento de inscripción de clave MEF que se describe en la cláusula 8.8.2.7, en el que el cliente MAF desempeña la función de cliente MAF de origen, habida cuenta de lo siguiente:

En la etapa 4 de la cláusula 8.8.2.7, el cliente MEF constituirá la petición de inscripción de clave MEF (véase el Cuadro 8.8.2.7-1) de la siguiente manera:

MAF-FQDN: se establecerá el valor del atributo *fqdn* en el nodo MO de nivel jerárquico inferior [*MAFClientRegCfg*];

expirationTime se calculará sumando el valor temporal en curso al valor de *keyRegDuration* en el nodo MO [*authenticationProfile*];

Se asignará a *labels* el valor del atributo *keyRegLabels* en el nodo MO [*authenticationProfile*];

adminFQDN: se asignará al valor del atributo *adminFQDN* en el nodo MO de nivel jerárquico inferior [*MAFClientRegCfg]*;

SUID: se asignará al valor del atributo *SUID* en el nodo MO de nivel jerárquico inferior [*authenticationProfile*];

targetIDs: se asignará según el nodo MO de nivel jerárquico superior del nodo MO [*authenticationProfile*]:

En el caso de un nodo MO de nivel jerárquico superior [*registration*], a los valores de *targetIDs se les* asignará el CSE-ID del CSE encargada de la inscripción.

En el caso de un nodo MO de nivel jerárquico superior [*dataCollection]*, se asignará a valores de *targetIDs* el CSE-ID determinado por medio del atributo *containerPath del* nodo MO [*dataCollection*].

keyValue: no debe incluirse.

El Cliente MEF deberá seleccionar un protocolo (HTTP, CoAP, WebSocket) basado en los protocolos admitidos por el cliente MEF, y los protocolos admitidos por la MAF se indican mediante la inclusión de *httpPort*, *coapPort* y *websocketPort* en el nodo MO de nivel jerárquico inferior [*MAFClientRegCfg]*. El cliente MEF utilizará el número de puerto proporcionado en el atributo *httpPort*, *coapPort* o *websocketPort* apropiado del nodo MO de nivel jerárquico inferior [*MAFClientRegCfg]*.

En la etapa 10 de la cláusula 8.8.2.7, si el cliente MEF recibe una respuesta de inscripción de clave MAF satisfactoria (véase el Cuadro 8.8.2.7-2), dicho cliente MEF verificará la siguiente información recibida en la respuesta de inscripción de clave MAF:

expirationTime: La verificación falla si este valor es anterior al momento en que se realiza la verificación.

Source MEF Client ID: La verificación no se realizará de forma satisfactoria si este valor es distinto del identificador del Cliente MEF.

adminFQDN: La verificación no se realizará de forma satisfactoria si este valor es distinto del valor correspondiente enviado en la petición de inscripción de claves MEF en la etapa 4 de la cláusula 8.8.2.7.

SUID: La verificación no se realizará de forma satisfactoria si este valor es distinto del valor correspondiente enviado en la petición de inscripción de claves MEF en la etapa 4 de la cláusula 8.8.2.7.

targetIDs: La verificación no se realizará de forma satisfactoria si este valor es distinto del valor correspondiente enviado en la petición de inscripción de claves MEF en la etapa 4 de la cláusula 8.8.2.7

Si la verificación se realiza de forma satisfactoria, el cliente MEF almacenará la información en la respuesta de inscripción de claves MEF y asociará esa información al nodo MO [*authenticationProfile*]. El cliente MEF interrumpirá el procedimiento, y se activará el procedimiento de actualización de la instrucción de control del cliente MEF para ese *cmdID*, y el valor de *cmdStatusCode* corresponderá a MEF_CLIENT_CMD_OK.

Si la verificación no se realiza de forma satisfactoria, o si el procedimiento no se lleva a cabo por cualquier otra razón, el cliente MEF interrumpe el procedimiento, y se activa el procedimiento de actualización de instrucción de control de cliente MEF para ese *cmdID*, y el valor de *cmdStatusCode* corresponderá a MEF_CLIENT_CMD_MO_NODE_PROCESSING_FAILED.

8.3.9.9.6 Procesamiento de nodo MO [*authenticationProfile*] con certificado

Finalidad: El procesamiento de un nodo MO [*authenticationProfile]* con SUID de certificado (para el conjunto {41,42,43}) facilita al cliente MEF acceso a una copia local del certificado de cliente MEF y la clave privada correspondiente, para su ulterior utilización con el nodo MO [*authenticationProfile*].

Condiciones previas: Este procedimiento sólo tiene lugar de forma satisfactoria si se ha provisto al nodo el certificado que corresponde al atributo *myCertFingerprint* en el nodo MO [*authenticationProfile*].

Procedimiento: El cliente MEF obtiene el valor del atributo *myCertFingerprint* en el nodo MO [*authenticationProfile*]. El cliente MEF determina si posee una copia local de una clave privada correspondiente al certificado que coincida con la clave privada correspondiente al atributo *myCertFingerprint*.

Si no se incluye ninguna copia local del certificado ni de la clave privada correspondiente, el cliente MEF asocia el certificado y la clave privada correspondiente al nodo MO [*authenticationProfile]* para

su utilización ulterior. El cliente MEF interrumpe el procedimiento, y se activa el procedimiento de actualización de instrucción de control de cliente MEF para ese *cmdID,* y el valor de *cmdStatusCode* corresponderá a MEF_CLIENT_CMD_MO_NODE_PROCESSING_FAILED.

Si se incluye una copia local del certificado y la clave privada correspondiente, el cliente MEF interrumpe el procedimiento, y se activa el procedimiento de actualización de instrucción de control de cliente MEF para ese *cmdID,* y el valor de *cmdStatusCode* corresponderá a MEF_CLIENT_CMD_OK.

8.3.9.9.7 Procesos específicos para [*trustAnchorCred*]

Finalidad: El procesamiento de un nodo MO [*trustAnchorCred]* permite al cliente MEF tener una copia local del certificado CA de puntos de anclaje de confianza identificado por el nodo MO [*trustAnchorCred*].

Elementos de *objectTypeSpecificArgs*: El elemento *objectTypeSpecificArgs* no se incluye en la especialización [*trustAnchorCred*].

Procesamiento de un nodo MO [*trustAnchoCred*]: El cliente MEF recupera el valor del atributo *certFingerprint* del nodo MO [*trustAnchorCred*]. El cliente MEF determina si posee una copia local de algún certificado que coincida con el atributo *certFingerprint*.

Si se incluye una copia local del certificado, el cliente MEF asocia el certificado al nodo MO [*trustAnchorCred*] para su ulterior utilización. El cliente MEF interrumpe el procedimiento, y se activa el procedimiento de actualización de instrucción de control de cliente MEF para ese *cmdID,* y el valor de *cmdStatusCode* corresponderá a MEF_CLIENT_CMD_OK.

Si no existe ninguna copia local del certificado, el cliente MEF pasará a la etapa 2.

El cliente MEF obtiene el valor del atributo *URI* del nodo MO [*trustAnchorCred*]. El cliente MEF intenta obtener el certificado de puntos de anclaje de confianza por medio de un procedimiento HTTPS GET dirigido al *URI*.

Si el procedimiento HTTPS GET no tiene lugar de forma satisfactoria, el cliente MEF interrumpe el procedimiento, y se activa el procedimiento de actualización de instrucción de control de cliente MEF para ese este *cmdID,* y el valor de *cmdStatusCode* corresponderá a MEF_CLIENT_CMD_MO_NODE_PROCESSING_FAILED.

Si el procedimiento HTTPS GET tiene lugar de forma satisfactoria, el cliente MEF obtiene la cabida útil útil. El cliente MEF analiza la cabida útil para determinar si se trata de un certificado y, si el análisis se realiza correctamente, el cliente MEF verifica que el certificado recibido coincide con el atributo *certFingerprint* del nodo MO [*trustAnchorCred]*.

Si el análisis tiene lugar de forma satisfactoria y el certificado recibido corresponde al atributo *certFingerprint* del nodo MO [*trustAnchorCred], el cliente MEF* asocia el certificado al nodo MO [*trustAnchorCred]* para su utilización ulterior. El cliente MEF interrumpe el procedimiento, y se activa el procedimiento de actualización de instrucción de control de cliente MEF para ese *cmdID,* y el valor de *cmdStatusCode* corresponderá a MEF_CLIENT_CMD_OK.

En otro caso, el cliente MEF interrumpe el procedimiento, y se activa el procedimiento de actualización de instrucción de control de cliente MEF para ese *cmdID,* y el valor de *cmdStatusCode* corresponderá a MEF_CLIENT_CMD_MO_NODE_PROCESSING_FAILED.

8.3.9.9.8 Procesos específicos para [*MAFClientRegCfg*]

Finalidad: El procesamiento de un nodo MO [*MAFClientRegCfg]* permite al cliente MEF, en calidad de cliente MAF, realizar una inscripción adecuada con respecto a la MAF mediante los atributos del nodo MO [*MAFClientRegCfg*].

Elementos de *objectTypeSpecificArgs*: El elemento *objectTypeSpecificArgs* no se incluye para la especialización [*MAFClientRegCfg*].

Procesamiento de un nodo MO [*MAFClientRegCfg*]: El cliente MEF intentará realizar el procedimiento de inscripción de cliente MAF que se describe en la cláusula 8.8.2.3, para el que el cliente MAF desempeñará la función de cliente MAF de origen, habida cuenta de lo siguiente:

En la etapa 2 de la cláusula 8.8.2.3, el cliente MEF constituirá la petición de registro de cliente MAF (véase el Cuadro 8.8.2.3-1) sobre la base de los atributos del nodo MO [*MAFClientRegCfg],* de la siguiente manera:

MAF-FQDN: su valor corresponderá al del atributo *fqdn*;

expirationTime: su valor corresponderá al del atributo *expirationTime*;

labels: su valor corresponderá al del atributo *labels*;

adminFQDN: su valor corresponderá al del atributo *adminFQDN*;

El cliente MEF seleccionará un protocolo (HTTP, CoAP, WebSocket) basado en los protocolos admitidos por el cliente MAF, y los protocolos admitidos por la MAF se indican mediante la inclusión de *httpPort*, *coapPort* y *websocketPort* en el nodo MO de nivel jerárquico inferior [*MAFClientRegCfg]*. El cliente MEF utilizará el número de puerto proporcionado en el atributo *httpPort*, *coapPort* o *websocketPort* apropiado del nodo MO [*MAFClientRegCfg]* de nivel jerárquico inferior.

En la etapa 3 de la cláusula 8.8.2.3, si el cliente MEF recibe una respuesta satisfactoria relativa a la inscripción de una clave MEF (véase el Cuadro 8.8.2.3-2), el cliente MEF verificará la siguiente información recibida en la respuesta relativa a la inscripción de la clave MEF:

expirationTime: La verificación no se llevará a cabo satisfactoriamente si este valor es anterior al valor temporal en que tiene lugar la verificación.

MAF Client ID: La verificación no se llevará a cabo satisfactoriamente si este valor es distinto del identificador del Cliente MEF.

adminFQDN: La verificación no se llevará a cabo satisfactoriamente si este valor es distinto del valor correspondiente enviado en la petición de inscripción de claves MEF en la etapa 2 de la cláusula 8.8.2.3.

Si la verificación se lleva a cabo satisfactoriamente, el cliente MEF almacenará la información en la respuesta de inscripción de clave MEF y asociará esa información al nodo MO [*MAFClientRegCfg*]. El cliente interrumpe el procedimiento, y se activa el procedimiento de actualización de instrucción de control de cliente MEF para ese *cmdID*, y el valor de *cmdStatusCode* corresponderá a MEF_CLIENT_CMD_OK.

Si la verificación no se realiza de forma satisfactoria, o si el procedimiento no se lleva a cabo por cualquier otra razón, el cliente MEF interrumpe el procedimiento, y se activa el procedimiento de actualización de instrucción de control de cliente MEF para ese *cmdID*, y el valor de *cmdStatusCode* corresponderá a MEF_CLIENT_CMD_MO_NODE_PROCESSING_FAILED.

8.4 Seguridad de extremo a extremo de las primitivas (ESPrim)

8.4.1 Finalidad de la seguridad de extremo a extremo de las primitivas (ESPrim)

La seguridad de extremo a extremo de las primitivas (ESPrim) proporciona un marco interoperable para la protección de las primitivas oneM2M, de modo que no sea necesario confiar en las CSE (que reenvían las primitivas) para la confidencialidad y la integridad de las mismas. ESPrim proporciona autentificación mutua, confidencialidad, protección de la integridad y garantía de vigencia (limitando la edad de los objetos ESPrim). Los casos de utilización y los requisitos aplicables se analizan en el informe técnico TR-0012 de oneM2M [b-oneM2M TR0012].

En esta Recomendación se asume que los extremos de ESPrim son el punto de origen y el punto de recepción de la primitiva.

En esta Recomendación se especifican aspectos de la gestión de las credenciales y de la protección de los datos para la ESPrim. El transporte de los objetos ESPrim se describe en [UIT-T Y.4500.1].

8.4.2 Arquitectura de la seguridad de extremo a extremo de las primitivas (ESPrim)

Los aspectos de la gestión de las credenciales y de la protección de los datos para la ESPrim se especifican en esta cláusula. En la cláusula 11.3.2 de [UIT-T Y.4500.1] se especifica el transporte de los objetos ESPrim.

La primitiva que hay que proteger se llama *primitiva interna*, y la primitiva que se utiliza para transportar una primitiva protegida se llama *primitiva externa*. La primitiva interna está protegida mediante encriptación y protección de la integridad que utiliza una clave simétrica *sessionESPrimPrimKey* como entrada. La clave *sessionESPrimKey* se obtiene de una *pairwiseESPrimKey*, establecida entre el origen y el receptor, y un *receiverESPrimRandObject* y un *originatorESPrimRandObject*.

La secuencia de eventos para la ESPrim consiste en tres fases principales:

Establecimiento de una pairwiseESPrimKey.

Establecimiento de una sessionESPrimKey en el originador.

Protección del intercambio de un primitiva.

En la Figura 8.4.2-1 se muestra el flujo de mensajes ESPrim para el establecimiento de una *pairwiseESPrimKey* y una *sessionESPrimKey* en el origen. En la Figura 8.4.2-2 se muestra el flujo de mensajes ESPrim para la protección del intercambio de una primitiva.

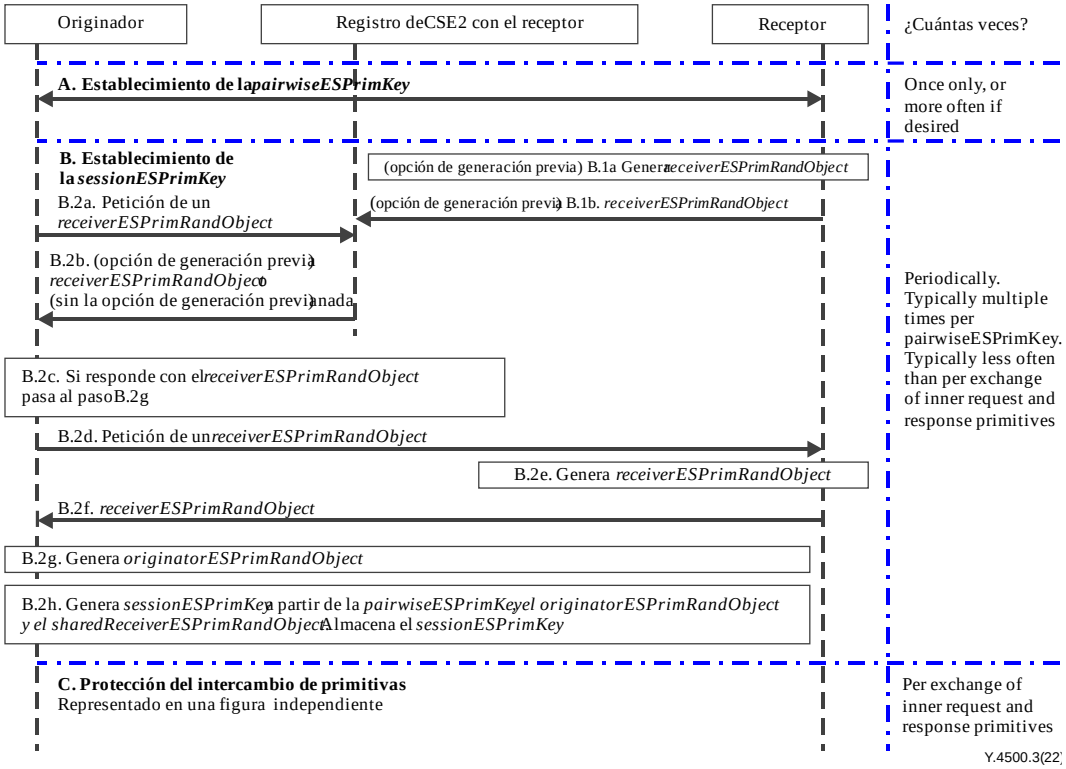


Figura 8.4.2-1 – Flujo de mensajes para el establecimiento de una *pairwiseESPrimKey* y una *sessionESPrimKey* en el origen para el procedimiento de seguridad de extremo a extremo de las primitivas (ESPrim)

A Establecimiento de la clave *pairwiseESPrimKey*: La *pairwiseESPrimKey* puede establecerse utilizando uno de los siguientes marcos:

Marco de *pairwiseESPrimKey* provisionadas: El origen y el receptor deben tener provisionadas las *pairwiseESPrimKey*. Estas credenciales se provisionan mediante uno de los siguientes mecanismos:

una provisión previa;

un marco de provisión de seguridad a distancia (RSPF), especificado en la cláusula 8.3; o

El establecimiento de claves basadas en certificados de seguridad de extremo a extremo (ESCertKE) entre el originador y el receptor, especificado en la cláusula 8.7 "Establecimiento de claves de extremo a extremo basadas en certificados (ESCertKE)".

El originador y el receptor también establecen un *pairwiseESPrimKeyID* y, de manera opcional, un *pairwiseESPrimKeyLifetime* durante el proceso. Si no se proporciona un *pairwiseESPrimKeyLifetime*, entonces la *pairwiseESPrimKey* no caduca nunca. El originador y el receptor memorizan el objeto (*pairwiseESPrimKeyID*, *pairwiseESPrimKey*, *pairwiseESPrimKeyLifetime* (opcional)) para utilizarlo en el tratamiento de primitivas posteriores.

Marco ESPrim con MAF: El originador y la función de autentificación de M2M (MAF) se autentifican mutuamente utilizando claves simétricas (que pueden estar provisionadas previamente o provisionadas a distancia) y obtienen una clave de conexión segura M2M (Kc) y el identificador de clave correspondiente (KcID). El originador genera una *pairwiseESPrimKey* a partir de Kc y una cadena reservada. El valor de KcID se utiliza en la fase C como un *pairwiseESPrimKeyID* en el objeto JWE/XML-ENC. El originador almacena la pareja (*pairwiseESPrimKeyID*, *pairwiseESPrimKey*) para utilizarlo en el tratamiento de primitivas posteriores. El receptor recupera Kc y un tiempo de vida de la credencial en la MAF después de recibir una primitiva de petición interna protegida mediante la correspondiente *pairwiseESPrimKey*, véase la etapa C.6.a.

Cuando se establece la *pairwiseESPrimKey* utilizando la opción de MAF, entonces su tiempo de vida es, normalmente, más corto que en la opción anterior.

El receptor indica que soporta ESPrim: Si el receptor soporta ESPrim, el receptor debe garantizar los siguientes aspectos para el recurso <*remoteCSE*> del receptor en todas las CSE que estén registrados con el receptor:

El recurso <*remoteCSE*> del receptor debe incluir el atributo *e2eSecInfo*.

El atributo *e2eSecInfo* en este recurso debe indicar el soporte de ESPrim.

B Establecimiento de la *sessionESPrimKey* en el originador: El receptor debe seleccionar si (a) genera previamente un *receiverESPrimObject* que se distribuye para que lo utilicen múltiples originadores para establecer la *sessionESPrimKey*, o (b) genera un *receiverESPrimRandObject* único bajo petición (en cuyo caso, no se requiere ninguna acción antes de recibir una petición de este tipo). Si un receptor selecciona generar un *receiverESPrimRandObject* único bajo petición, entonces, en este último caso, el receptor debe garantizar que el parámetro *sharedReceiverESPrimRandObject* no está presente en el atributo *e2eSecInfo* en el recurso <*remoteCSE*> del receptor en todas las CSE que estén registradas con el receptor. La ausencia del parámetro *sharedReceiverESPrimRandObject* indica que el receptor proporcionará un *receiverESPrimRandObject* único bajo petición.

B.1 **(Si el receptor selecciona la utilización de una generación previa) Generación previa del *sharedReceiverESPrimRandObject***: Si el receptor seleccionó generar previamente y distribuir un *receiverE2SPrimandObject*, el receptor realiza los siguientes pasos cada vez que desea proporcionar un nuevo *receiverESPrimRandObject* compartido.

B.1a.1 El receptor debe generar un *receiverESPrimRandObject* incluyendo los siguientes parámetros:

El receptor debe generar un nuevo valor aleatorio de 128 bits *ESPrimRandValue*.

El receptor debe asignar un *ESPrimRandExpiry*, que indica cuándo el *receiverESPrimRandObject* deja de ser válido.

El receptor debe asignar un *ESPrimRandID* para el *receiverESPrimRandObject* que cumpla los siguientes criterios: (a) el *ESPrimRandID* debe indicar que el *receiverESPrimRandObject* es compartido; (b) el *ESPrimRandID* debe ser único entre los *receiverESPrimRandObject* compartidos emitidos por el receptor y válido en el momento de la emisión. Estos criterios garantizan que el *receiverESPrimRandObject* pueda identificarse de manera unívoca hasta que caduca.

El receptor debe incluir una lista de valores de *sessionESPrimKeyGenerationAlgorithmID* que identifican los algoritmos que el receptor desea utilizar para generar la *sessionESPrimKey* utilizando este *receiverESPrimRandObject*.

El receptor debe incluir una lista de valores de *AEADAlgorithmID* que identifican los algoritmos AEAD que el receptor desea utilizar con este *receiverESPrimRandObject*.

B.1b El receptor debe actualizar el parámetro *sharedReceiverESPrimRandObject* del atributo *e2eSecInfo* en el recurso <*remoteCSE*> del receptor en todas las CSE registradas con el receptor.

NOTA 1 – En un momento dado, varios originadores utilizarán valores idénticos para el *sharedReceiverESPrimRandObject* actual.

B.2 **El originador recibe un *receiverESPrimRandObject***: El originador debe realizar los siguientes pasos cada vez que establece una *sessionESPrimKey* con el receptor:

B.2a El originador debe realizar una función de recuperación sobre el atributo *e2eSecInfo* del recurso <*remoteCSE*> del receptor en una CSE, denominado en este caso CSE2, registrado con el receptor.

B.2b En el caso de que esté presente el atributo *e2eSecInfo* en el recurso <re*moteCSE*> del receptor en CSE2, entonces CSE2 debe enviar el atributo *e2eSecInfo*. En caso contrario, CSE2 devuelve un mensaje de error al originador.

B.2c El originador determina si el receptor soporta ESPrim, en cuyo caso debe estar presente el atributo *e2eSecInfo* que es el indicador del soporte de ESPrim.

B.2.c.1 Si el receptor no soporta ESPrim, el originador debe cancelar el procedimiento.

B.2c.2 Si el receptor soporta ESPrim, y el atributo *e2eSecInfo* incluye un parámetro *sharedReceiverESPrimRandObject*, el originador examina el *ESPrimRandExpiry* de este parámetro para determinar si el *sharedReceiverESPrimRandObject* ha caducado. Si el *sharedReceiverESPrimRandObject* no ha caducado, el originador debe poner *receiverESPrimRandObject* en el valor de *sharedReceiverESPrimRandObject* y pasar al paso B.2g. Si el *sharedReceiverESPrimRandObject* ha caducado, el originador pasará al paso B.2d.

B.2c.3 Si el receptor soporta ESPrim, y el atributo *e2eSecInfo* no incluye un parámetro *sharedReceiverESPrimRandObject*, el originador debe pasar al paso B.2d.

B.2d El originador debe enviar un mensaje al receptor solicitando un r*eceiverESPrimRandObjec*t.

B.2e El receptor, al recibir la petición, debe generar un *receiverESPrimRandObject* incluyendo los siguientes parámetros:

El receptor debe generar un nuevo valor aleatorio de 128 bits *ESPrimRandValue*.

El receptor debe asignar un *ESPrimRandExpiry*, que indica cuándo el *receiverESPrimRandObject* deja de ser válido.

El receptor debe asignar un identificador *ESPrimRandID* para el *receiverESPrimRandObject* que cumpla los siguientes criterios: (a) el *ESPrimRandID* debe indicar que el *receiverESPrimRandObject* no es compartido; (b) el *ESPrimRandID* debe ser único entre los *receiverESPrimRandObject* no

compartidos emitidos por el receptor y válido en el momento de la emisión. Estos criterios garantizan que el *receiverESPrimRandObject* pueda identificarse de manera unívoca hasta que caduca

El receptor debe incluir una lista de valores de *sessionESPrimKeyGenerationAlgorithmID* que identifiquen los algoritmos que el receptor desea utilizar para generar la *sessionESPrimKey* utilizando este *receiverESPrimRandObject*.

El receptor debe incluir una lista de valores de *AEADAlgorithmID* que identifiquen los algoritmos AEAD que el receptor desea utilizar con este *receiverESPrimRandObject*.

B.2f El receptor debe enviar un mensaje al originador con el *receiverESPrimRandObject*.

B.2g El originador debe generar un *originatorESPrimRandObject* incluyendo los siguientes parámetros:

– El originador debe generar un nuevo valor aleatorio de 128 bits *ESPrimRandValue*.

– El originador debe asignar el *ESPrimRandExpiry*, que indica cuándo el *originatorESPrimRandObject* deja de ser válido. El *ESPrimRandExpiry* no debe ser posterior al *ESPrimRandExpiry* del *receiverESPrimRandObject* establecido en los pasos B.2c o B.2f.

– El originador debe asignar un *ESPrimRandID* para el *originatorESPrimRandObjectID* que cumpla los siguientes criterios: (a) el *ESPrimRandID* debe indicar que el *originatorESPrimRandObject* no es compartido; (b) el *ESPrimRandID* debe ser único entre los *originatorESPrimRandObject* no compartidos emitidos por el originador y válido en el momento de la emisión. Estos criterios garantizan que el *originatorESPrimRandObject* pueda identificarse de manera unívoca hasta que caduca.

– El originador debe incluir un único identificador *sessionESPrimKeyGenerationAlgorithmID* para el algoritmo que el originador está aplicando para generar la *sessionESPrimKey* utilizando este *originatorESPrimRandObject*. Debe ser uno de los algoritmos identificados en los valores del *sessionESPrimKeyGenerationAlgorithmID* en el *receiverSPrimERandObject* establecido en los pasos B.2c o B.2f.

– El originador debe incluir una lista de valores de *AEADAlgorithmID* que identifiquen los algoritmos AEAD que el originador desea utilizar con este *originatorESPrimRandObject*. Debe ser uno o más de los algoritmos identificados por el *AEADAlgorithmID* en el *receiverESPrimRandObject* establecido en los pasos B.2c o B.2f.

B.2h El originador debe generar la *sessionESPrimKey* a partir de la *pairwiseESPrimKey*, el r*eceiverESPrimRandObject* recibido en el paso B.2c y el *originatorESPrimRandTuple* generado en el paso B.2.g.

NOTA 2 – La *sessionESPrimKey* utilizada para proteger una primitiva de petición interna se utiliza siempre para proteger la primitiva de respuesta interna, por tanto, la *sessionESPrimKey* debe almacenarse al menos hasta que se prevea que se haya recibido la primitiva de respuesta interna correspondiente. El originador generalmente almacena la *sessionESPrimKey* durante un periodo de tiempo más largo pues la *sessionESPrimKey* puede utilizarse para proteger múltiples intercambios de primitivas.

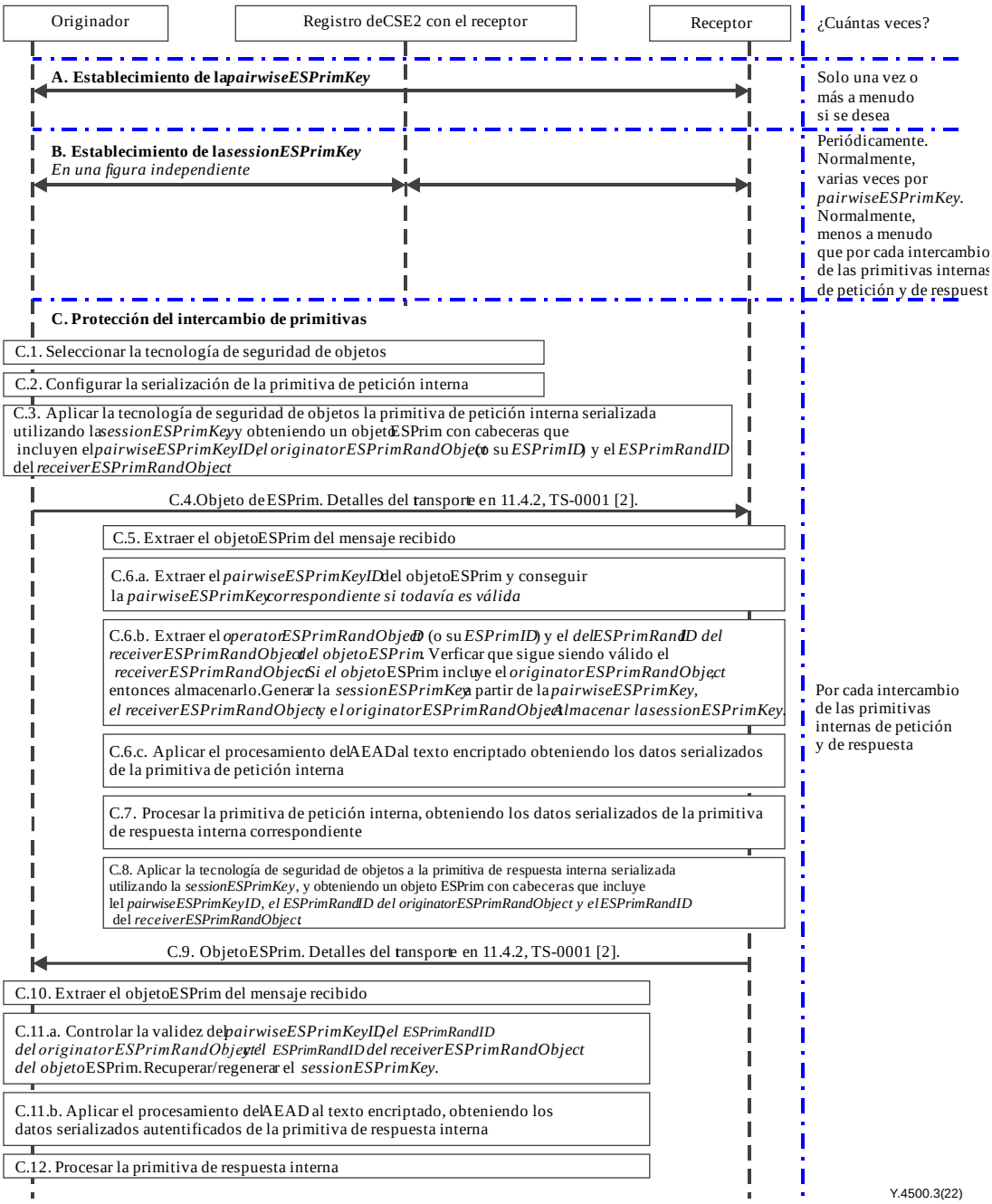


Figura 8.4.2-2 – Flujo de mensajes para proteger el intercambio de una primitiva en el procedimiento de seguridad de extremo a extremo de las primitivas (ESPrim)

C Protección del intercambio de primitivas:

NOTA 3 – El originador selecciona el tipo de serialización (es decir, JSON, XML) de la primitiva de petición interna que se debe proteger.

C.1 El originador selecciona la tecnología de seguridad de objetos en función de la tecnología que soporta y del tipo de serialización de la primitiva de petición interna.

C.2 El originador debe configurar la serialización de la primitiva de petición interna.

C.3 El originador debe generar un objeto ESPrim aplicando la tecnología de seguridad de objetos de la manera siguiente:

Una o más cabeceras de un objeto ESPrim deben incluir la siguiente información:

– el pairwiseESPrimKeyID

– el *originatorESPrimRandObject* utilizado para generar la *sessionESPrimKey*, o el correspondiente *ESPrimRandID*. Si existe la posibilidad de que este objeto ESPrim pueda ser el primero objeto ESPrim recibido por el receptor que esté protegido por el originador utilizando un *originatorESPrimRandObject* específico entonces debe incluirse todo el *originatorESPrimRandObject.* En caso contrario, debe incluirse el *originatorESPrimRandObject* o el *ESPrimRandID*.

– el *ESPrimRandID* del *receiverESPrimRandObject* utilizado para generar la *sessionESPrimKey*.

– el *AEADAlgorithmID* para el objeto ESPrim. Debe ser uno de los algoritmos AEAD identificados en *originatorESPrimRandObject*.

El texto sin formato (que irá encriptado) constituirá los datos serializados de la primitiva de petición interna.

La *sessionESPrimKey* debe utilizarse directamente como clave simétrica para realizar la encriptación autentificada del texto sin formato generando el texto encriptado del objeto ESPrim. Se supone que el texto encriptado contiene el MIC para verificar la integridad de la primitiva de petición interna.

C.4 El originador debe configurar una primitiva de petición externa para el transporte del objeto ESPrim como se describe en [UIT-T Y.4500.1]. El originador debe enviar la primitiva de petición externa al receptor.

C.5 El receptor procesa la primitiva de petición externa recibida, para extraer el objeto ESPrim como se describe en [UIT-T Y.4500.1].

C.6 El receptor debe procesar el objeto ESPrim.

C.6a El receptor debe extraer el *pairwiseESPrimKeyID* de las cabeceras del objeto ESPrim para obtener la *pairwiseESPrimKey*:

En el caso de que el *pairwiseESPrimKeyID* tenga el formato de una *pairwiseESPrimKey* provisionada, el receptor utilizará la correspondiente *pairwiseESPrimKey* (provisionada previamente).

En el caso de que el *pairwiseESPrimKeyID* tenga el formato de una *pairwiseESPrimKey* de la MAF, si es la primera vez que el receptor recibe un mensaje con el *pairwiseESPrimKeyID*, es necesario seguir el siguiente proceso.

C.6a.1 El receptor debe identificar la MAF a partir del *pairwiseESPrimKeyID* (que es un KcID)

C.6a.2 El receptor debe establecer una conexión TLS segura con la MAF y solicitar la clave de conexión segura M2M (Kc) y el tiempo de vida de Kc correspondiente al *pairwiseESPrimKeyID* (que es idéntico a KcID).

C.6a.3 La MAF debe proporcionar Kc y el tiempo de vida de Kc al receptor.

C.6a.4 El receptor debe generar la *pairwiseESPrimKey* a partir de Kc y una cadena reservada.

C.6a.5 El receptor debe poner el valor del *pairwiseESPrimKeyLifetime* en el tiempo de vida de Kc.

C.6a.6 El receptor debe almacenar (p*airwiseESPrimKeyID, pairwiseESPrimKey, pairwiseESPrimKeyLifetime)* para su utilización en el procesamiento de primitivas posteriores.

Si el receptor ha almacenado previamente (*pairwiseESPrimKeyID*, *pairwiseESPrimKey*, *pairwiseESPrimKeyLifetime*), y el *pairwiseESPrimKeyLifetime* todavía no ha caducado, entonces el receptor puede utilizar la *pairwiseESPrimKey* almacenada.

C.6b El receptor debe seguir el siguiente proceso para generar la *sessionESPrimKey*:

C.6b.1 El receptor debe extraer el *ESPrimRandID*, del contenido de las cabeceras del objeto ESPrim *receiverESPrimRandObject*, e intentar recuperar el valor correspondiente de

receiverESPrimRandObject almacenado. Si no se encuentra ningún valor almacenado, o el valor almacenado ha caducado, entonces el receptor debe responder a la primitiva de petición externa con un error.

C.6b.2 El receptor debe extraer la codificación del *originatorESPrimRandObject* o el *ESPrimRandID* del *originatorESPrimRandObject*, del contenido de las cabeceras del objeto ESPrim, y aplicar la descodificación adecuada. Si se proporciona un *originatorESPrimRandObject*, éste debe almacenarse. Si se proporciona un *ESPrimRandID,* el receptor debe recuperar el valor correspondiente almacenado del *originatorESPrimRandObject*. Si no se encuentra ningún valor almacenado, o el valor almacenado ha caducado, entonces el receptor debe responder a la primitiva de petición externa con un error.

El receptor debe procesar el objeto *originatorESPrimRandObject*:

C.6b.2.i El receptor debe controlar el *ESPrimExpiry* en el *originatorESPrimRandObject* para verificar (a) que no ha caducado ya y (b) que el *ESPrimExpiry* no es posterior al *ESPrimExpiry* del *receiverESPrimRandObject*.

C.6b.2.ii El receptor debe extraer el *sessionESPrimKeyGenerationAlgorithmID* y verificar que el algoritmo identificado concuerda con uno de los *sessionESPrimKeyGenrationAlgorithmID* del *receiverESPrimRandObject*.

C.6b.2.iii El receptor debe generar la clave *sessionESPrimKey* a partir de la *pairwiseESPrimKey*, el r*eceiverESPrimRandObject* y el *originatorESPrimRandObject* o recuperar el valor de la *sessionESPrimKey* si se ha generado anteriormente y almacenado.

NOTE 4 – La *sessionESPrimKey* utilizada para proteger una primitiva de petición interna se utiliza siempre para proteger la primitiva de respuesta interna correspondiente, y, por tanto, la *sessionESPrimKey* debe almacenarse al menos hasta que se haya enviado la correspondiente primitiva de respuesta interna. El receptor normalmente almacena la *sessionESPrimKey* durante un periodo de tiempo más largo pues el originador puede utilizar la *sessionESPrimKey* para proteger múltiples intercambios de primitivas.

C.6c Pasos de la desencriptación autentificada en el receptor:

C.6c.1 El receptor debe extraer los *AEADAlgorithmID* del *originatorESPrimRandObject* y verificar que el conjunto de algoritmos identificados es un subconjunto del conjunto definido en los *AEADAlgorithmID* del *receiverESPrimRandObject*.

El receptor debe procesar el *AEADAlgorithmID* de las cabeceras del objeto ESPrim y verificar que el algoritmo identificado concuerda con uno de los *AEADAlgorithmID* del *originatorESPrimRandObject*.

C.6c.2 El receptor debe aplicar el identificador del algoritmo AEAD de la cabecera del objeto ESPrim, al parámetro de texto encriptado del objeto ESPrim obteniendo el texto sin formato, utilizando la *sessionESPrimKey*. Se supone que el texto encriptado contiene el MIC para verificar la integridad de la primitiva de petición interna. Los datos serializados autentificados de la primitiva de petición interna son el texto verificado sin formato, de salida del algoritmo AEAD.

C.7 El receptor debe procesar la primitiva de petición interna, dando como resultado la serialización de la primitiva de respuesta interna correspondiente.

NOTA 5 – Los pasos de C.2 a C.7 tienen una correspondencia estrecha con los pasos de C.8 a C.12, donde el originador y el receptor cambian sus papeles en el intercambio, y las primitivas de petición son remplazadas por las primitivas de respuesta. Existen pequeñas diferencias, en concreto algunos de los procesamientos de las peticiones en los pasos C.2 a C.7 no son necesarios en el procesamiento de la respuesta, pues el originador ya ha generado la *sessionESPrimKey;* solo es necesario identificar la *sessionESPrimKey* adecuada, como se hace en el paso C.11.a.

C.8 El receptor debe utilizar la misma *sessionESPrimKey* que se utiliza en el objeto ESPrim recibido en el paso C.5. En consecuencia, el *pairwiseESPrimKeyID*, el *originatorESPrimRandObject* y el *receiverESPrimRandObject* son los mismos que los recibidos en el paso C.5.

El receptor debe generar un objeto ESPrim aplicando la tecnología de seguridad de objetos de la manera siguiente

Una o más cabeceras del objeto ESPrim deben incluir la siguiente información:

– el pairwiseESPrimKeyID

– el *ESPrimRandID* del *originatorESPrimRandObject*

– el *ESPrimRandID* del *receiverESPrimRandObject*

– el *AEADAlgorithmID* del objeto ESPrim. Debe ser uno de los algoritmos AEAD identificados en *originatorESPrimRandObject*.

El texto sin formato (que irá encriptado) será los datos serializados de la primitiva de petición interna.

La *sessionESPrimKey* debe utilizarse directamente como clave simétrica para proporcionar la encriptación autentificada del texto sin formato que genera el texto encriptado del objeto ESPrim. Se supone que el texto encriptado contiene el MIC para verificar la integridad de la primitiva de petición interna.

C.9 El receptor debe configurar una primitiva de petición externa para el transporte del objeto ESPrim como se describe en [UIT-T Y.4500.1]. El originador debe enviar la primitiva de petición externa al receptor.

C.10 El originador procesa la primitiva de petición externa recibida para extraer el objeto ESPrim como se describe en [UIT-T Y.4500.1].

C.11 El originador debe procesar el objeto ESPrim.

C.11a El originador debe extraer de las cabeceras del objeto ESPrim los valores de los identificadores *pairwiseESPrimKeyID*, *ESPrimRandID* del *originatorESPrimRandObject*, y el *ESPrimRandID* del *receiverESPrimRandObject*. Estos valores deben corresponder con el *pairwiseESPrimKeyID*, el *ESPrimRandID* del *originatorESPrimRandObject* y el *ESPrimRandID* del *receiverESPrimRandObject* de una sesión que el originador considere válida en ese momento.

Si cualquiera de estos valores ha caducado, debe descartarse la primitiva de respuesta externa.

NOTE 6 – Por esta razón, los plazos de caducidad de estos valores deben ser suficientemente amplios como para permitir la recepción de la primitiva de respuesta interna correspondiente.

En caso contrario, el originador utilizará el valor almacenado de la *sessionESPrimKey* correspondiente a estos valores, o puede generar una *sessionESPrimKey*.

C.11b El originador debe aplicar el identificador del algoritmo AEAD, de la cabecera del objeto ESPrim, al parámetro de texto encriptado del objeto ESPrim para obtener el texto sin formato verificado, utilizando la *sessionESPrimKey*. Se supone que el texto encriptado contiene el MIC para verificar la integridad de la primitiva de petición interna. La serialización autentificada de la primitiva de petición interna es el texto sin formato verificado de salida del algoritmo AEAD.

C.12 El originador debe procesar la primitiva de petición interna.

8.4.3 Detalles del protocolo de seguridad de extremo a extremo de las primitivas (ESPrim)

8.4.3.1 Definiciones de los parámetros de la seguridad de extremo a extremo de las primitivas (ESPrim)

8.4.3.1.1 Definición del parámetro originatorESPrimRandObject

La estructura del parámetro originator2ERandObject se muestra en el Cuadro 8.4.3.1.1-1. Este parámetro se utiliza para establecer la *sessionESPrimKey* como parte de la seguridad de extremo a extremo de las primitivas (ESPrim) descrita en la cláusula 8.4.2. El tipo de datos del parámetro originatorESPrimRandObject está especificado en [UIT-T Y.4500.4].

Cuadro 8.4.3.1.1-1 – Estructura del parámetro *originatorESPrimRandObject*

Elemento de trayecto	Multiplicidad	Descripción
esprimRandID	1	Identificador del originatorESPrimRandObject, asignado por la CSE o la AE que genera el originatorESPrimRandObject
esprimRandValue	1	Valor de 128 bits generado aleatoriamente.
esprimRandExpiry	1	Tiempo en el que el originatorESPrimRandObject caduca
esprimKeyGenAlgID	1	Identificadores numerados del algoritmo seleccionado, para la generación de sessionESPrimKey, por la CSE o la AE que genera el originatorESPrimRandObject
esprimProtocolAndAlgIDs	1	Lista de identificadores numerados para los algoritmos AEAD soportados por la CSE o la AE que genera el originadorESPrimRandObject

8.4.3.1.2 Definición del parámetro receiverESPrimRandObject

La estructura del parámetro originator2ERandObject se muestra en el Cuadro 8.4.3.1.2-1. Este parámetro se utiliza para establecer la sessionESPrimKey como parte de la seguridad de extremo a extremo de las primitivas (ESPrim) descrita en la cláusula 8.4.2. El tipo de datos del parámetro receiverESPrimRandObject está especificado en [UIT-T Y.4500.4].

Cuadro 8.4.3.1.2-1 – Estructura del parámetro *receiverESPrimRandObject*

Elemento de trayecto	Multiplicidad	Descripción
esprimRandID	1	Identificador del receiverESPrimRandObject, asignado por la CSE o la AE que genera el receiverESPrimRandObject
esprimRandValue	1	Valor de 128 bits generado aleatoriamente.
esprimRandExpiry	1	Tiempo en el que el receiverESPrimRandObject caduca.
esprimKeyGenAlgIDs	1	Lista de identificadores numerados para los algoritmos soportados para la generación de sessionESPrimKey por la CSE o la AE que genera el receiverESPrimRandObject
esprimProtocolAndAlgIDs	1	Lista de identificadores numerados para los algoritmos AEAD soportados por la CSE o la AE que genera el receiverESPrimRandObject

8.4.3.1.3 Definición del atributo de recurso *e2eSecInfo*

El atributo de recurso *e2eSecInfo* aparece en los tipos de recursos <*CSEBase*>, <*remoteCSE*> y <*AE*>. La estructura del atributo de recurso *e2eSecInfo* se muestra en el Cuadro 8.4.3.1.3-1. Este parámetro se utiliza para establecer la sessionESPrimKey como parte de la seguridad de extremo a extremo de las primitivas (ESPrim) descrita en la cláusula 8.4.2. Los tipos de datos están especificados en [UIT-T Y.4500.4].

Cuadro 8.4.3.1.3-1 – Estructura del atributo *e2eSecInfo*

Elemento de trayecto	Multiplicidad	Descripción
supportedE2ESecurityFeatures	1	Lista de identificadores de uso de seguridad (SUID) para las funciones de seguridad de extremo a extremo soportadas por la CSE o la AE asociada con los recursos <*CSEBase*>, <*remoteCSE*> o <*AE*> que incluyen el atributo del recurso *e2eSecInfo*.
e2ECertificates	0..1	Lista de certificados asociados con la CSE o la AE asociada con los recursos <*CSEBase*>, <*remoteCSE*> o <*AE*> que incluyen el atributo del recurso *e2eSecInfo*.
sharedReceiverESPrimRandObject	0..1	Parámetro receiverESPrimRandObject (véase la cláusula 8.4.3.1.2) generado por la CSE o la AE asociada a los recursos <*CSEBase*>, <*remoteCSE*> o <*AE*> que contienen el atributo del recurso *e2eSecInfo*.

8.4.3.2 Formateo y procesamiento de objetos ESPrim utilizando la serialización compacta JWE

Antecedentes: La encriptación web JSON (JWE) especificada en [IETF RFC 7516], proporciona un formato sencillo para encriptar cualquier objeto de datos. Existen dos serializaciones JWE: una serialización compacta y segura para los URI, y una serialización JSON.

El formateo y el análisis sintáctico necesarios para la serialización compacta JW de la seguridad de extremo a extremo de las primitivas (ESPrim) pueden codificarse fácilmente sin herramientas genéricas para el formateo o el análisis sintáctico de JSON.

En la serialización compacta JWE, un JWE se representa como la concatenación de cinco parámetros JWE:

BASE64URL(UTF8(Cabecera protegida JWE)) || '.' ||

BASE64URL(Clave encriptada JWE) || '.' ||

BASE64URL(Vector de inicialización JWE) || '.' ||

BASE64URL(Texto encriptado JWE) || '.' ||

BASE64URL(Etiqueta de autentificación JWE)

donde BASE64URL(OCTETOS) representa la codificación base64url de OCTETOS, según la sección 2 de la especificación JSON Web Signature [IETF RFC 7515].

NOTA 1 – Si OCTETOS es una secuencia de octeto vacía, entonces [IETF RFC 7515] define que BASE64URL(OCTETOS) sea una cadena vacía.

NOTA 2 – La serialización JWE compacta no es tan flexible como la serialización JWE JSON, sin embargo, la serialización JWE compacta proporciona suficiente flexibilidad para los Objetos ESPrim. Además, la facilidad de formateo y análisis sintáctico de la serialización JWE compacta proporciona una solución sencilla tanto para las representaciones XML como JSON de las primitivas

Definiciones de los parámetros JWE para ESPrim: En el Cuadro 8.4.3.2-1, se especifican los valores de los cinco parámetros JWE para la serialización JWE compacta

Cuadro 8.4.3.2-1 – Componentes JWE utilizados en los objetos ESPrim

Valor JWE	Tipo de elemento	Vacío	Contenido del componente
Cabecera protegida JWE	JSON	Nunca	Véase el Cuadro 8.4.3.2-2 Parámetros de la cabecera protegida JWE
Clave de encriptación JWE	Valor binario	Siempre	Este valor está vacío para el modo de gestión de claves utilizado para ESPrim
Vector de inicialización JWE	Valor binario	Condicional	De acuerdo con [IETF RFC 7516]
Texto encriptado JWE	Valor binario	Nunca	
Etiqueta de autentificación JWE	Valor binario	Condicional	
NOTA – El hecho de que estos componentes estén vacíos o no depende del algoritmo seleccionado para el cifrado.			

En el Cuadro 8.4.3.2-2 "Parámetros de la cabecera protegida JWE" se describen los parámetros de la cabecera protegida JWE cuando se utiliza JWE para la ESPrim.

Cuadro 8.4.3.2-2 – Parámetros de la cabecera protegida JWE

Elemento de trayecto	Multiplicidad para ESPrim	Finalidad	Especificación del elemento	Descripción del valor asignado
"alg"	1	Modo de gestión de claves	[IETF RFC 7516]	"dir" indica encriptación directa.
"enc"	1	Algoritmo de encriptación		Las opciones disponibles son las mismas que para la utilización de JWE por ESData. Véase la cláusula 8.7.3 "Detalles del protocolo ESData"
"kid"	1	Identificador de clave	[IETF RFC 7516]	Identificador para la pairwiseESPrimKey
"cty"	0..1	Tipo de medio del contenido protegido	[IETF RFC 7516]	Definido en función de la serialización de la primitiva (XML o JSON) seleccionada por el originador.
"ori"	1	Identifica la información del originador para la generación de la clave de sesión	Cláusula 8.4.3.1.1	El esprimRandID del originatorESPrimRandObject utilizado para generar la sessionESPrimKey para este objeto ESPrim.
"rri"	1	Identifica la información del receptor para la generación de la clave de sesión	Cláusula 8.4.3.1.2	El esprimRandID del receiverESPrimRandObject utilizado para generar la sessionESPrimKey para este objeto ESPrim.
"oro"	0..1	originatorESPrimRandObject	Cláusula 8.4.3.1.1 utilizando la serialización JSON	Representación JSON de un originatorESPrimRandObject generado por el originador. Enviado solo por el originador.

Cuadro 8.4.3.2-2 – Parámetros de la cabecera protegida JWE

Elemento de trayecto	Multiplicidad para ESPrim	Finalidad	Especificación del elemento	Descripción del valor asignado
"rro"	0..1	receiverESPrimRandObject	Cláusula 8.4.3.1.2 utilizando la serialización JSON	Representación JSON de un receiverESPrimRandObject generado por el receptor. Enviado solo por el receptor.

El texto siguiente proporciona una explicación más detallada de los parámetros de la cabecera protegida JWE cuando se utiliza JWE para la ESPrim.

Hay que recordar que un objeto ESPrim está formado por la encriptación de la primitiva interna utilizando la clave simétrica sessionESPrimKey. La generación de la sessionESPrimKey a partir de la pairwiseESPrimKey, el originatorESPrimRandObject y el receiverESPrimRandObject es independiente de la gestión de claves disponible a través de JWE – desde la perspectiva de JWE, sessionESPrimKey es simplemente un valor de clave simétrica secreta compartida entre el originador y el receptor. JWE utiliza el modo de gestión de claves de encriptación directa en este escenario. La serialización JWE será necesaria para transportar el identificador de la pairwiseESPrimKey, los esprimRandID del originatorESPrimRandObject y del receiverESPrimRandObject, y de manera opcional un receiverESPrimRandObject o un originatorESPrimRandObject para que el originador y el receptor puedan generar la sessionESPrimKey correcta.

El parámetro "alg" (Algoritmo) de la cabecera JWE [IETF RFC 7516] tendrá el valor "dir" para indicar el modo de gestión de claves de encriptación directa.

El parámetro "enc" (algoritmo de encriptación) de la cabecera JWE [IETF RFC 7516] puede ser seleccionado por el emisor del objeto ESPrim. El algoritmo de encriptación debe corresponder a los esprimProtocolAndAlgIDs del originatorESPrimRandObject identificado y a los esprimProtocolAndAlgIDs del receiverESPrimRandObject identificado.

El parámetro "kid" (Identificador de clave) de la cabecera JWE [IETF RFC 7516] tendrá como valor el identificador de la pairwiseESPrimKey.

El parámetro "cty" identificará el tipo de medio de la representación (JSON o XML) de la primitiva interna.

Los esprimRandID del originatorESPrimRandObject y del receiverESPrimRandObject se deben comunicar en los parámetros "ori" (Originator Rand ID) y "rri" (Receiver Rand ID) incluidos en la cabecera protegida JWE. Estos parámetros son específicos de oneM2M y deben cumplir con la definición del esprimRandID en las cláusulas 8.4.3.1.1 y 8.4.3.1.2.

El originador puede incluir un originatorESPrimRandObject en un parámetro "oro" (Originator Rand Object), ya sea al comienzo de una sesión ESPrim o para actualizar las claves de sesión "en banda" durante una sesión ESPrim existente. En el primer caso, "ori" debe coincidir con el esprimRandID del originatorESPrimRandObject, pero esta restricción no se aplica en el segundo caso. Este parámetro se define en las cláusulas 8.4.2 y 8.4.3.1.1, y debe utilizarse la representación JSON.

El receptor puede incluir un receiverESPrimRandObject en un "rro" (Receiver Rand Object) – para refrescar las claves de sesión "en banda" durante una sesión ESPrim existente. Este parámetro se define en las cláusulas 8.4.2 y 8.4.3.1.2, y debe utilizarse la representación JSON.

Formación de un objeto ESPrim: La representación de la primitiva interna deberá encriptarse como se especifica para la encriptación de mensajes en [IETF RFC 7516]. La cabecera protegida JWE debe estar formada como se ha descrito anteriormente.

La clave de encriptación del contenido (CEK) debe ser la sessionESPrimKey generada utilizando la pairwiseESPrimKey, el originatorESPrimRandObject y el receiverESPrimRandObject identificados en la cabecera protegida JWE.

El texto sin formato será la representación de la primitiva interna.

El vector de inicialización JWE, el texto encriptado JWE y la etiqueta de autentificación JWE deben generarse a partir de la cabecera protegida JWE, el texto sin formato y la CEK, tal como se especifica en [IETF RFC 7516], de acuerdo con el algoritmo de cifrado identificado.

La serialización JWE compacta se compondrá a partir de los parámetros JWE.

El objeto ESPrim está formado por los datos de la serialización JWE compacta.

Procesamiento de un objeto ESPrim: El procesamiento de la serialización JWE compacta se debe hacer según lo especificado para la desencriptación de mensajes en [IETF RFC 7516], con la siguiente aclaración:

La cabecera protegida JWE debe estar formada como se ha descrito anteriormente.

Si el originatorESPrimRandObject o el receiverESPrimRandObject están incluidos, estos deben conservarse.

La clave de encriptación del contenido (CEK) debe ser la sessionESPrimKey generada utilizando la pairwiseESPrimKey, el originatorESPrimRandObject y el receiverESPrimRandObject identificados en la cabecera protegida JWE. La generación de la SessionESPrimKey se especifica en la cláusula 8.4.2.

El texto sin formato se generará a partir del vector de inicialización JWE, el texto encriptado JWE, la etiqueta de autentificación JWE y la CEK, tal como se especifica en [IETF RFC 7516], de acuerdo con el algoritmo de encriptación identificado.

8.5 Seguridad de extremo a extremo de los datos (ESData)

8.5.1 Finalidad de la seguridad de extremo a extremo de los datos (ESData)

La seguridad de extremo a extremo de los datos (ESData) proporciona un marco interoperable para la protección de los datos que deben transportarse utilizando puntos de referencia oneM2M, de modo que no sea necesario confiar en las CSE por las que pasan los datos. Los datos que debe protegerse forman el *ESData Payload* (Carga útil de ESData). La carga útil de ESData constituye normalmente todo o parte del valor de un atributo (por ejemplo, el valor del atributo *content* de un recurso <*contentInstance*>) o el parámetro de una primitiva (por ejemplo, un testigo de acceso firmado y autocontenido, comunicado en una primitiva de petición para conseguir una autorización dinámica).

NOTA – En el ámbito de la cláusula 8.5, los términos que incluyen la palabra "ESData" pueden acortarse eliminando "ESData" para facilitar la lectura. Por ejemplo, "carga útil de ESData" se simplifica a menudo con "carga útil".

Los casos de uso y los requisitos aplicables se analizan en el informe técnico TR-0012 de oneM2M [b-oneM2M TR0012].

En ESData se supone que existe un único extremo de origen de ESData que aplica el procesamiento de ESData a la carga útil para obtener una envolvente de ESData constituida por los datos protegidos y las cabeceras necesarias, y uno o varios extremos de destino de ESData que aplican el procesamiento de ESData a la envolvente para extraer los datos verificados. La carga útil se compone de texto sin formato (que debe encriptarse y protegerse en su integridad) y de los datos autentificados asociados (que sólo deben protegerse en su integridad).

No hay ninguna restricción inherente sobre qué entidades pueden ser extremo de origen y extremo de destino; estos extremos pueden ser entidades dentro de un sistema oneM2M (es decir, las EA y las

CSE) o entidades fuera de un sistema oneM2M (entidades, por ejemplo, que forman parte de un sistema que interactúa con oneM2M).

En esta Recomendación se especifican aspectos de la gestión de las credenciales y de la protección de datos para ESData. La Recomendación no aborda el transporte de las envolventes de ESData.

8.5.2 Arquitectura de ESData

8.5.2.1 Lista de clases de seguridad ESData y opciones de protección ESData

Se proporcionan las siguientes clases de seguridad ESData:

Solo con encriptación: (véase la nota) que ofrece confidencialidad y protección de la integridad. La carga útil se protege utilizando claves simétricas y estas claves simétricas se establecen utilizando uno o más de los siguientes métodos:

Claves simétricas establecidas de otro modo con los extremos de destino. En este caso, el extremo de origen puede autentificarse, a menos que la clave simétrica haya sido compartida con varios extremos de destino.

Certificado de los extremos de destino: cuando se utiliza un certificado de extremos de destino, el extremo de destino no puede autentificar el extremo de origen.

NOTA – Hablando con precisión, esta clase proporciona encriptación y protección de la integridad, pero este nombre se ajusta al uso de protocolos como la encriptación web JSON (JWE) y la encriptación XML, que pueden proporcionar tanto encriptación como protección de la integridad.

Solo con firma: Que proporciona la autentificación del origen, protección de la integridad y (cuando se utilizan firmas digitales asimétricas) ausencia de rechazo. Para ello se utilizan MIC basados en claves simétricas o firmas digitales asimétricas verificadas mediante certificados del extremo de origen.

Con firma y encriptación anidadas: Se utiliza en los casos en los que se requiere una encriptación además de la autentificación del origen y/o el no rechazo mediante un certificado del extremo de origen. Se firma primero una o varias firmas digitales en la carga útil y luego se aplica una encriptación a la combinación de la carga útil y las firmas digitales.

ESData soporta la utilización de múltiples credenciales para proteger una sola unidad de carga útil.

Cada clase de seguridad ESData soporta tres opciones de protección ESData, como se muestra en el Cuadro 8.5.2.1-1.

Cuadro 8.5.2.1-1 – Opciones de protección ESData

Clase de seguridad ESData	Opción de protección ESData	Gestión de claves	Verificación de origen	No rechazo
Solo con encriptación (8.5.2.2)	Encriptación utilizando claves ESData simétricas provisionadas	Clave simétrica provisionada	Simétrica	-
	Encriptación utilizando la TEF	TEF	Simétrica	-
	Encriptación utilizando un certificado del extremo de destino	Certificado	-	-
Solo con firma (8.5.2.3)	MIC utilizando una clave ESData simétrica provisionada	Clave simétrica provisionada	Simétrica	-
	MIC utilizando la TEF	TEF	Simétrica	-
	Firma digital utilizando un certificado del extremo de origen	Certificado	Certificado	Certificado

Clase de seguridad ESData	Opción de protección ESData	Gestión de claves	Verificación de origen	No rechazo
Con firma y encriptación anidadas (8.5.2.4)	Firma digital utilizando el certificado del extremo de origen seguido de cualquier combinación de opciones de protección de sólo encriptado	Clave(s) simétrica(s) provisionada(s) y/o TEF(s) y/o Certificado(s) de encriptación. Certificado de firma	Certificado	Certificado

8.5.2.2 Clase de seguridad ESData solo con encriptación

8.5.2.2.1 Visión general de la clase de seguridad ESData solo con encriptación

Las opciones de protección ESData soportadas para la clase de seguridad solo con encriptación se indican en el Cuadro 8.5.2.1-1 "Opciones de protección ESData".

La ESData solo con encriptación soporta la encriptación utilizando cualquier combinación de opciones de protección y utilizando múltiples credenciales para cada opción de protección.

Modo ESData de encriptación. La clase de seguridad ESData soporta solamente dos modos principales de encriptación:

Modo ESData de encriptación directa: En este modo, se utiliza una clave simétrica directamente en el algoritmo de encriptación para proteger la carga útil. El modo de encriptación directa se recomienda sólo en escenarios que cumplan los siguientes criterios:

Escenarios en los cuales minimizar las cabeceras de los objetos de los datos tiene una prioridad muy alta.

La función de encriptación no se utilizará con el mismo valor de clave más de 2^{32} veces, al menos para AES GCM, por las razones expuestas en la cláusula 8.4 de [IETF RFC 7518].

Este modo sólo se debe utilizar cuando se utiliza una única clave simétrica para proteger la carga útil.

Modo ESData de clave encriptada: En este modo, la clave de encriptación del contenido (CEK) (utilizada en el algoritmo de encriptación para proteger la carga útil) se encripta utilizando una o más credenciales y se proporciona la CEK encriptada en una cabecera junto con los datos protegidos**.**

Restricciones para la aplicación del modo de encriptación. En escenarios donde:

La encriptación mediante una clave simétrica ESData provisionada se aplica mediante una única clave; o bien

La encriptación mediante la TEF se aplica utilizando una única clave simétrica registrada en la TEF;

En estos casos, puede aplicarse el modo de encriptación directa o el modo de clave encriptada.

En todos los otros casos, debe aplicarse el modo de clave encriptada.

Secuencia general de eventos. El texto siguiente describe la secuencia de eventos cuando se utiliza una clase de seguridad sólo con encriptación.

NOTA – En esta Recomendación no se describen los procesos por los que el extremo de origen y el extremo, o los extremos, de destino deciden las credenciales que se utilizarán para proteger una carga útil, ni el algoritmo de encriptación que debe aplicarse.

A Configuración de credenciales: El extremo de origen obtiene las credenciales necesarias a fin de proteger la carga útil para el o los extremos de destino previstos. Esto puede incluir cualquier

combinación de las opciones de protección, se permiten múltiples credenciales para cada opción de protección:

Encriptación utilizando claves ESData simétricas provisionadas: El extremo de origen y el extremo, o los extremos, de destino están dotados de una clave simétrica ESData provisionada, como se describe en la cláusula 8.5.2.2.2 "Encriptación utilizando una clave simétrica ESData".

Encriptación utilizando la TEF: El extremo de origen genera una clave simétrica aleatoria secreta registrada en la TEF, realizando el registro de esta clave en la TEF tal y como se describe en la cláusula 8.5.2.2.3 "Encriptación utilizando una función habilitadora de confianza".

Encriptación utilizando certificados: El extremo de origen obtiene el certificado del extremo de destino como se describe en la cláusula 8.5.2.2.4 "Encriptación utilizando certificados de los extremos de destino".

B Gestión de la clave de encriptación del contenido (CEK) del extremo de origen:

Si se va a aplicar el modo de encriptación directa, se debe utilizar directamente como CEK la clave simétrica ESData provisionada o la clave simétrica TEF registrada. La utilización del modo de encriptación directa debe indicarse en las *ESData Headers*: parámetros de las cabeceras de la envolvente de datos ESData. La clave simétrica ESData provisionada o la clave simétrica TEF registrada debe identificarse en las cabeceras.

En los demás casos, el extremo de origen debe generar un valor aleatorio secreto para la clave de encriptación del contenido (CEK) y encriptará la CEK utilizando la(s) credencial(es) obtenida(s) en la fase A "Gestión de credenciales", tal como se describe en las cláusulas 8.5.2.2.2, 8.5.2.2.3 y 8.5.2.2.4. Cada CEK encriptada se añadirá a las cabeceras, junto con el identificador de la credencial que debe utilizar para desencriptar la CEK encriptado. El valor de la CEK puede utilizarse para una sola carga útil o puede utilizarse para múltiples cargas útiles.

C Encriptación del extremo de origen:

C.1 El algoritmo de encriptación debe identificarse en las cabeceras.

C.2 El extremo de origen debe aplicar el proceso de encriptación a la carga útil para el algoritmo identificado utilizando la CEK. El texto sin formato se encripta para obtener el texto encriptado, y la combinación del texto sin formato y los datos autentificados asociados (AAD) está protegida en su integridad por el MIC generado.

C.3 El extremo de origen debe formar la envolvente a partir de las cabeceras, el texto encriptado, los AAD y el MIC; este proceso puede incluir la codificación de los datos utilizando, por ejemplo, base64.

En esta Recomendación no se especifica cómo se obtiene la envolvente o cómo se proporciona a los extremos de destino. Los siguientes pasos se llevan a cabo en cada uno de los extremos de destino:

D Gestión de la CEK del extremo de destino:

D.1 El extremo de destino analiza la envolvente, aplicando la codificación necesaria, y extrae los parámetros de cabecera.

D.2 Si en las cabeceras se indica el modo de encriptación directa, el extremo de destino debe utilizar los identificadores de las credenciales de las cabeceras para obtener la clave simétrica ESData provisionada o la clave simétrica TEF registrada (como se describe en las cláusulas 8.2.2.2 o 8.5.2.2.3, respectivamente). El extremo de destino debe utilizar esta clave simétrica directamente como CEK.

D.3 En los demás casos, el extremo de destino debe utilizar los identificadores de las credenciales de las cabeceras para identificar una CEK cifrada que pueda desencriptarse mediante una credencial conocida por el extremo de destino o disponible para él. El extremo de destino obtendrá esa credencial y debe desencriptar la CEK encriptada como se describe en las cláusulas 8.5.2.2.2 (caso de la clave simétrica ESData provisionada), 8.5.2.2.3 (caso de la TEF) y 8.5.2.2.4 (caso de los certificados de los

extremos de destino). El extremo de destino utilizará la CEK resultante para procesar la carga útil protegida de la envolvente. El extremo de destino puede almacenar el valor CEK debido a la posibilidad de que dicho valor CEK se utilice para proteger cargas útiles posteriores.

E Desencriptación del extremo de destino:

E.1 El extremo de destino debe identificar el algoritmo de encriptación adecuado indicado en las cabeceras.

E.2 El extremo de destino debe aplicar el proceso de desencriptación al texto encriptado, los AAD y el MIC para el algoritmo identificado, utilizando la CEK, para obtener como resultado el texto sin formato verificado y los AAD verificados.

8.5.2.2.2 Encriptación utilizando una clave simétrica ESData

Para esta opción de protección, se debe provisionar al extremo de origen y a cada uno de los extremos de destino, una clave ESData simétrica provisionada, un identificador de clave ESData simétrica provisionado y, opcionalmente, una duración de la clave ESData simétrica provisionada. Las credenciales deben proporcionarse a través de uno de los siguientes medios:

Provisión previa;

Un marco de provisión de seguridad a distancia (RSPF), especificado en la cláusula 8.3; o

El establecimiento de claves de seguridad de extremo a extremo en base a certificados entre el origen y el receptor, como se especifica en la cláusula 8.7 "Establecimiento de claves de extremo a extremo basadas en certificados".

8.5.2.2.3 Encriptación utilizando una función habilitadora de confianza

Especificado en la cláusula 8.6.

8.5.2.2.4 Encriptación utilizando certificados de los extremos de destino

8.5.2.2.4.1 Asociación de certificados de clave pública con los extremos de destino

En esta opción de protección, cada extremo de destino debe disponer de un certificado de clave pública en el que confíe el extremo de origen para asociarse con dicho extremo de destino. Se soportan las siguientes opciones:

Los certificados de extremo de destino pueden utilizar los siguientes tipos de certificados de clave pública identificados en la cláusula 8.1.2.1 "Marcos de certificados de clave pública":

En el caso de un certificado de clave pública bruta, el extremo de origen debe estar configurado de forma segura (directamente o a distancia) para asociarse al extremo de destino con la clave pública bruta o su hash. Los detalles de esta configuración no se proporcionan en la presente especificación.

En el caso de un certificado de dispositivo:

El extremo de origen debe estar configurado de forma segura, con el ancla de confianza en la cadena de certificados del dispositivo; normalmente durante la provisión inicial.

El extremo de origen debe estar configurado de forma segura para asociar el extremo de destino con el identificador exclusivo a nivel mundial de equipo de hardware. Los detalles de esta configuración no se proporcionan en la presente especificación.

En el caso de un certificado AE-ID o CSE-ID, el extremo de origen debe estar configurado de forma segura, con el ancla de confianza en la cadena de certificados del certificado AE-ID o del certificado CSE-ID; normalmente durante la provisión inicial. El extremo de origen confía entonces en que el extremo de destino con un AE-ID o CSE-ID determinado está asociado con el certificado que contiene ese AE-ID o CSE-ID.

Los certificados de extremo de destino pueden utilizar otras infraestructuras de clave pública, en particular cuando el extremo de destino se encuentra en un sistema que no es oneM2M que interactúa con el sistema oneM2M. Esta Recomendación no ofrece garantías de interoperabilidad cuando se utilizan dichos certificados.

No pueden utilizarse claves públicas para verificar la firma en esta opción de protección.

8.5.2.2.4.2 Obtención de certificados de extremo de destino

El extremo de origen no puede proteger un mensaje hacia el extremo de destino antes de conseguir el certificado del extremo de destino. Esta especificación no impone el mecanismo por el cual se proporciona el certificado del extremo de destino al extremo de origen, y existen diversos mecanismos que son adecuados. El *e2ESecurityParameters* es un mecanismo proporcionado por oneM2M que permite al extremo de origen recuperar los certificados asociados a una CSE o una AE.

Una AE de un extremo de destino puede hacer que los certificados estén disponibles en el atributo *e2ESecurityParameters* del recurso <*AE*> que representa a esa AE. Este proceso de recuperación no es un mecanismo fiable y seguro para asociar el extremo de destino con el certificado; también se debe aplicar la cláusula 8.5.2.2.4.1 "Asociación del certificado de clave pública con los extremos de destino".

Una CSE de extremo de destino puede hacer que los certificados estén disponibles en el atributo *e2ESecurityParameters* de los recursos <*CSE*> y <*remoteCSE*> que representan a esa CSE. Este proceso de recuperación no es un mecanismo fiable y seguro para asociar el extremo de destino con el certificado; también se debe aplicar la cláusula 8.5.2.2.4.1 "Asociación del certificado de clave pública con los extremos de destino".

8.5.2.3 Clase de seguridad ESData solo con firma

8.5.2.3.1 Visión general de la clase de seguridad ESData solo con firma

Las opciones de protección ESData soportadas para la clase de seguridad solo con firma se indican en el Cuadro 8.5.2.1-1 "Opciones de protección ESData".

NOTA 1 – La presente especificación sólo soporta una opción de protección de ESData sólo con firma, pero la cláusula está estructurada para soportar opciones adicionales de protección de ESData sólo con firma si se desea en el futuro.

La ESData solo con firma soporta la encriptación utilizando cualquier combinación de opciones de protección y utilizando múltiples credenciales para cada opción de protección.

Secuencia general de eventos: El texto siguiente describe la secuencia de eventos cuando se utiliza una clase de seguridad sólo con firma.

NOTA 2 – En esta Recomendación no se describen los procesos por los que el extremo de origen y el extremo, o los extremos, de destino deciden las credenciales que se utilizarán para proteger una carga útil, ni el algoritmo de encriptación que debe aplicarse.

A Configuración de credenciales: El extremo de origen obtiene las credenciales necesarias para firmar la carga útil para el o los extremos de destino previstos. Esto puede incluir cualquier combinación de las opciones de protección, se permiten múltiples credenciales para cada opción de protección:

MIC utilizando claves ESData simétricas provisionadas: El extremo de origen y el extremo o los extremos de destino disponen de una clave ESData simétrica provisionada, como se describe en la cláusula 8.5.2.2.2 "Encriptación utilizando una clave simétrica ESData".

MIC utilizando la TEF: El extremo de origen genera una clave simétrica aleatoria secreta registrada en la TEF, registrando esta clave en la TEF tal y como se describe en la cláusula 8.5.2.2.3 "Encriptación utilizando una función habilitadora de confianza".

Firma digital utilizando los certificados de los extremos de destino: El extremo de origen selecciona una clave privada y el certificado de extremo de origen correspondiente como se describe en la cláusula 8.5.2.3.2 "Firma digital utilizando certificados de los extremos de destino".

B Firma de los puntos de origen:

B.1 La carga útil se codifica utilizando, por ejemplo, base 64.

B.2 Para cada credencial, el extremo de origen debe generar un conjunto de elementos de datos de la manera siguientes:

B.2.i El extremo de origen debe formar una cabecera, que identifica la firma digital o el algoritmo del MIC, y la credencial que pueda utilizar un extremo de destino para verificar dicha firma digital o el MIC. Si es necesario, la cabecera también se codifica, por ejemplo, utilizando base64.

B.2.ii El extremo de origen debe generar una firma/MIC aplicando la firma digital adecuada o el algoritmo de MIC a la carga útil y al encabezado utilizando la credencial apropiada, y codificando, por ejemplo, en base 64.

B.2.iii El extremo de origen debe formar un elemento de datos a partir de las cabeceras, la carga útil y la firma/MIC.

B.3 El extremo de origen debe formar una envolvente a partir de la carga útil encriptada y el conjunto de elementos de datos generados en el paso B.2.

En esta Recomendación no se especifica cómo se obtiene la envolvente o cómo se proporciona a los extremos de destino. Los siguientes pasos se llevan a cabo en cada uno de los extremos de destino:

C Verificación del punto de destino:

C.1 El extremo de destino analiza la envolvente, extrayendo la carga útil codificada y el conjunto de elementos de datos, cada uno de los cuales contiene una cabecera y una firma/MIC.

C.2 El extremo de destino debe examinar el conjunto de elementos de datos para identificar los elementos de datos que puedan verificarse mediante una credencial en la que pueda confiar dicho extremo de destino. Para cada uno de estos elementos de datos:

C.2.i El extremo de destino debe obtener la credencial identificada de acuerdo con los cláusulas 8.5.2.2.2 (caso de la clave simétrica ESData provisionada), 8.5.2.2.3 (caso de la TEF) y 8.5.2.3.2 (caso del certificado del extremo de origen).

C.2.ii El extremo de destino debe verificar el MIC o la firma al utilizar la credencial.

C.3 El extremo de destino debe descodificar la carga útil codificada y verificada para obtener la carga útil original y guardar la(s) credencial(es) utilizada(s) para verificar la carga útil.

8.5.2.3.2 Firma digital utilizando el certificado del extremo de origen

8.5.2.3.2.1 Asociación del certificado de clave pública con el extremo de origen

En esta opción de protección, cada extremo de origen debe estar provisto de un certificado de clave pública, en el que confíe el extremo de destino para asociarse con el extremo de origen considerado. Se soportan las siguientes opciones:

Los certificados de los extremos de origen pueden utilizar los siguientes tipos de certificados de clave pública identificados en la cláusula 8.1.2.1 "Marcos de certificados de clave pública":

En el caso de un certificado de clave pública bruta, el extremo de destino debe estar configurado de forma segura (directamente o a distancia) para asociar al extremo de origen con la clave pública bruta o su hash. Los detalles de esta configuración no se proporcionan en la presente especificación.

En el caso de un certificado de dispositivo:

El extremo de destino debe estar configurado de forma segura, con el ancla de confianza en la cadena del certificado del dispositivo; normalmente durante la provisión inicial.

El extremo de destino debe estar configurado de forma segura para asociar el extremo de origen con el identificador exclusivo a nivel mundial de equipo de hardware. Los detalles de esta configuración no se proporcionan en la presente especificación

En el caso de un certificado AE-ID o CSE-ID, el extremo de destino debe estar configurado de forma segura, con el ancla de confianza en la cadena de certificados del certificado AE-ID o CSE-ID; normalmente durante la provisión inicial. El extremo de destino confía entonces en que el extremo de origen con un AE-ID o CSE-ID determinado está asociado con el certificado que contiene ese AE-ID o CSE-ID.

Los certificados de extremo de origen pueden utilizar otras infraestructuras de clave pública, en particular cuando el extremo de origen se encuentra en un sistema que no es oneM2M y que interactúa con el sistema oneM2M. Esta Recomendación no ofrece garantías de interoperabilidad cuando se utilizan dichos certificados.

No pueden utilizarse claves públicas para verificar la firma en esta opción de protección.

8.5.2.3.2.2 Obtención de los certificados del extremo de origen

El extremo de destino no puede proteger un mensaje hacia el extremo de origen antes de conseguir el certificado del extremo de origen. Esta especificación no impone el mecanismo por el cual se proporciona el certificado del extremo de origen al extremo de destino, y existen diversos mecanismos que son adecuados. El *e2ESecurityParameters* es un mecanismo proporcionado por oneM2M que permite al extremo de destino recuperar los certificados asociados a una CSE o una AE.

Una AE de un extremo de origen puede hacer que los certificados estén disponibles en el atributo *e2ESecurityParameters* del recurso <*AE*> que representa a esa AE. Este proceso de recuperación no es un mecanismo fiable y seguro para asociar el extremo de origen con el certificado; también se debe aplicar la cláusula 8.5.2.3.2.1 "Asociación del certificado de clave pública con los extremos de origen".

Una CSE de un extremo de origen puede hacer que los certificados estén disponibles en el atributo *e2ESecurityParameters* de los recursos <*CSE*> y <*remoteCSE*> que representan a esa CSE. Este proceso de recuperación no es un mecanismo fiable y seguro para asociar el extremo de origen con el certificado; también se debe aplicar la cláusula 8.5.2.3.2.1 "Asociación del certificado de clave pública con los extremos de origen".

8.5.2.4 Firma y encriptación anidadas

Para estas opciones, se realizan los siguientes pasos de alto nivel (no se muestran los pasos de configuración de credenciales ni los de gestión de CEK):

El extremo de origen debe generar una envolvente interna que contiene una o más firmas digitales para la carga útil interna utilizando uno o más certificados de acuerdo con la "Firma digital utilizando el certificado del extremo de origen" de la opción de protección solo con firma de la cláusula 8.5.2.3.

El extremo de origen debe definir que la envolvente interna generada en el paso 1 sea el texto sin formato de la carga útil externa, que se encriptará a continuación utilizando cualquier combinación de opciones de protección solo con encriptación de la cláusula 8.5.2.2. El resultado es una envolvente externa.

En esta Recomendación no se especifica cómo se obtiene la envolvente externa o cómo se proporciona a los extremos de destino. Los siguientes pasos se aplican en cada extremo de destino:

El extremo de destino debe desencriptar la envolvente externa generada en el paso 1 utilizando una de las opciones de protección sólo con encriptación de la cláusula 8.5.2.2, con lo que se obtendrá la carga útil externa, que es también la envolvente interna.

El extremo de destino debe verificar las firmas digitales de la envolvente interna utilizando uno o varios certificados de acuerdo con la "Firma digital utilizando el certificado de los extremos de origen" de la opción de protección solo con firma de la cláusula 8.5.2.3, con lo que se obtendrá la carga útil interna verificada.

8.5.3 Detalles de los protocolos de la seguridad de extremo a extremo de los datos (ESData)

8.5.3.1 Introducción

Las clases de seguridad de la seguridad de extremo a extremo de los datos (ESData) soportan los protocolos que se indican en el Cuadro 8.5.3.1-1.

Cuadro 8.5.3.1-1 – Clases de seguridad ESData, y correspondencia con los protocolos de seguridad basados en XML y basados en JSON

Clase de seguridad ESData	Basado en XML	JOSE: Seguridad basada en JSON
Solo con encriptación	XML-ENC aplicada a la carga útil de ESData	JWE aplicada a la carga útil de ESData
Solo con firma	XML-SIG aplicada a la carga útil de ESData	JWS aplicada a la carga útil de ESData
Con firma y encriptación anidadas	XML-SIG aplicada a la carga útil de ESData, y XML-ENC aplicada al resultado.	JWS aplicada a la carga útil de ESData, y JWE aplicada al resultado.

La opción JOSE permite una serialización JSON flexible además de serializaciones compactas menos flexibles (que también son seguras para URI). Así que hay tres opciones de serialización: XML, JWE/JWS con serialización JSON y JWE/JWS con serializaciones compactas.

8.5.3.2 Detalles de los protocolos de la clase de seguridad ESData solo con encriptación

Para mantener la coherencia, se proporcionan los algoritmos de gestión de claves que están disponibles tanto en la encriptación directa de XML-ENC [W3C XMLENC] como en la encriptación JSON Web (JWE) [IETF RFC 7516].

Encriptación directa.

Encriptación AES de claves, utilizando claves de 128-bit, 256-bit.

RSA-OAEP con MGF1 y SHA256.

Acuerdo de claves Diffie-Hellman de curva elíptica (ECDH) en modo efímero-estático utilizando encriptación AES de claves.

En el Cuadro 8.5.3.2-1 se indican los algoritmos de gestión de claves soportados en la encriptación XML para la clase de seguridad ESData solo con encriptación.

Cuadro 8.5.3.2-1 – Algoritmos de gestión de claves soportados en la encriptación XML para la clase de seguridad ESData solo con encriptación

Gestión de claves	Algoritmo		<xenc:EncryptionMethod Algorithm=".."> para encriptar la clave	Otros parámetros
Encriptación de la dirección	n. d.		n. d.	<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> <ds:KeyName>John Smith</ds:KeyName>
Encriptación simétrica de claves	Encrip-tación AES de claves con	Clave de 128 bits	http://www.w3.org/2001/04/xmlenc#kwaes128	
		Clave de 192 bits	http://www.w3.org/2001/04/xmlenc#kwaes192	
		Clave de 256 bits	http://www.w3.org/2001/04/xmlenc#kwaes256	
RSA	RSA-OAEP con MFG1 y SHA-256		http://www.w3.org/2009/xmlenc11#rsa-oaep	<xenc11:MGF Algorithm="http://www.w3.org/2009/xmlenc11#mgf1sha256>
Acuerdo de claves ECDH	ECDH-ES con encrip-tación AES de claves	Clave de 128 bits	http://www.w3.org/2001/04/xmlenc#kwaes128	<xenc:AgreementMethod Algorithm="http://www.w3.org/2009/xmlenc11#ECDH-ES">
		Clave de 192 bits	http://www.w3.org/2001/04/xmlenc#kwaes192	
		Clave de 256 bits	http://www.w3.org/2001/04/xmlenc#kwaes256	

En el Cuadro 8.5.3.2-2 se indican los algoritmos de encriptación de la carga útil soportados en la encriptación XML para la clase de seguridad ESData solo con encriptación.

Cuadro 8.5.3.2-2 – Algoritmos de encriptación de la carga útil soportados en la encriptación XML para la clase de seguridad ESData solo con encriptación

Algoritmos de encriptación de la carga útil		<EncryptionMethod Algorithm="..">
AES GCM con	Clave de 128 bits	http://www.w3.org/2009/xmlenc11#aes128gcm
	Clave de 192 bits	http://www.w3.org/2009/xmlenc11#aes192gcm
	Clave de 256 bits	http://www.w3.org/2009/xmlenc11#aes256gcm

El resultado generado por la encriptación XML está serializada como un objeto XML. El objeto de la encriptación XML puede transportarse sin codificación, o puede codificarse en base64.

En el Cuadro 8.5.3.2-3 se indican los algoritmos de gestión de claves soportados en JWE para la clase de seguridad ESData solo con encriptación.

Cuadro 8.5.3.2-3 – Algoritmos de gestión de claves soportados en la encriptación web JSON (JWE) para la clase de seguridad ESData solo con encriptación

Gestión de claves	Algoritmo		"alg":".."
Encriptación de la dirección	n. d.		dir
Encriptación simétrica de claves	Encrip-tación AES de claves con	Clave de 128 bits	A128KW
		Clave de 192 bits	A192KW
		Clave de 256 bits	A256KW
RSA	RSA-OAEP con MFG1 y SHA-256		"alg": "RSA-OAEP-256"
Acuerdo de claves ECDH	ECDH-ES con encrip-tación AES de claves	Clave de 128 bits	ECDH-ES+A128KW
		Clave de 192 bits	ECDH-ES+A192KW
		Clave de 256 bits	ECDH-ES+A256KW

En el Cuadro 8.5.3.2-4 se indican los algoritmos de la carga útil soportados en JWE para la clase de seguridad ESData solo con encriptación.

Cuadro 8.5.3.2-4 – Algoritmos de encriptación de la carga útil soportados en la encriptación web JSON (JWE) para la clase de seguridad ESData solo con encriptación

Algoritmos de encriptación de la carga útil		"enc":".."
AES GCM con	Clave de 128 bits	A128GCM
	Clave de 192 bits	A192GCM
	Clave de 256 bits	A256GCM

El resultado generado por JWE cumple con la serialización JSON de JWE o con una serialización JWE compacta y segura para URI. La serialización JSON de JWE puede transportarse sin codificación, o puede codificarse en base64. La norma [UIT-T Y.4500.4] define el tipo de datos m2m:e2eCompactJWE para la serialización JWE compacta.

8.5.3.3 Detalles de los protocolos de la clase de seguridad ESData solo con firma

Para mantener la coherencia, se proporcionan tipos de firmas que están disponibles tanto en la firma de XML-Signature [W3C XMLSIG] como en la firma JSON Web (JWS) [IETF RFC 7515].

HMAC con SHA-256, SHA-384 o SHA-512.

Firma RSA utilizando PKCS1-v1.5 y MGF1 con SHA-256, SHA-384 o SHA-512.

Firma ECDSA utilizando P-256, P-384 o P-512 con SHA-256, SHA-284 o SHA-512 respectivamente.

En el Cuadro 8.5.3.3-1 se indican los algoritmos soportados en XML-SIG para la clase de seguridad ESData solo con firma.

Cuadro 8.5.3.3-1 – Algoritmos soportados en la firma de XML-Signature para la clase de seguridad ESData solo con firma

Tipo de firma	Algoritmo		<SignatureMethod Algorithm="..">
HMAC	SHA-256		http://www.w3.org/2001/04/xmldsigmore#hmacsha256
	SHA-384		http://www.w3.org/2001/04/xmldsigmore#hmacsha384
	SHA-512		http://www.w3.org/2001/04/xmldsigmore#hmacsha512
RSA	RSA PKCS1-v1.5 y MGF1 con:	SHA-256	http://www.w3.org/2001/04/xmldsigmore#rsasha256
		SHA-384	http://www.w3.org/2001/04/xmldsigmore#rsasha384
		SHA-512	http://www.w3.org/2001/04/xmldsigmore#rsasha512
ECDSA	P-256 y SHA-256		http://www.w3.org/2001/04/xmldsigmore#ecdsasha256
	P-384 y SHA-384		http://www.w3.org/2001/04/xmldsigmore#ecdsasha384
	P-512 y SHA-512		http://www.w3.org/2001/04/xmldsigmore#ecdsasha512

El objeto XML-Signature puede transportarse sin codificación, o puede codificarse en base64.

En el Cuadro 8.5.3.3-2 se indican los algoritmos soportados en JWS para la clase de seguridad ESData solo con firma.

Cuadro 8.5.3.3-2 – Algoritmos soportados en la firma web JSON (JWS) para la clase de seguridad ESData solo con firma

Tipo de firma	Algoritmo		"alg":".."
HMAC	SHA-256		HS256
	SHA-384		HS384
	SHA-512		HS512
RSA	RSA PKCS1-v1.5 y MGF1 con:	SHA-256	RS256
		SHA-384	RS384
		SHA-512	RS512
ECDSA	P-256 y SHA-256		ES256
	P-384 y SHA-384		ES384
	P-512 y SHA-512		ES512

La salida generada por JWS cumple con la serialización JSON de JWS o con una serialización JWS compacta y segura para URI. La serialización JSON de JWS puede transportarse sin codificación, o puede codificarse en base64. La norma [UIT-T Y.4500.4] define el tipo de datos m2m:e2eCompactJWS para la serialización JWS compacta.

8.5.3.4 Detalles de los protocolos de la clase de seguridad ESData con firma y encriptación anidadas

Los pasos de alto nivel para la clase de seguridad ESData con firma y encriptación anidadas están descritos en la cláusula 8.5.2.4. La envolvente interna debe generarse y procesarse de acuerdo con uno o más tipos de firmas RSA o ECDSA especificados en la cláusula 8.5.3.3. La envolvente interna debe generarse y procesarse de acuerdo con cualquier combinación de uno o más algoritmos de gestión de claves especificados en la cláusula 8.5.3.2.

8.6 Marcos de seguridad a distancia para la seguridad de extremo a extremo

8.6.1 Visión general de la gestión y el registro a distancia de credenciales para la seguridad de extremo a extremo

8.6.1.1 Introducción

El sistema de provisión a distancia para la seguridad de extremo a extremo debe disponer de la capacidad para una entidad de registrar y emitir credenciales de extremo a extremo por medio de una función habilitadora de confianza para la seguridad de extremo a extremo. Una función de inscripción M2M, una función de autentificación M2M o una entidad de servicio común MN-CSE que dispone de la capacidad de registrar y proporcionar credenciales de seguridad de extremo a extremo pueden actuar como función habilitadora de confianza para la seguridad de extremo a extremo.

Las credenciales de seguridad de extremo a extremo obtenidas pueden utilizarse para proporcionar los siguientes mecanismos de protección de seguridad:

Integridad y autenticidad de los mensajes (primitivas) mediante un código de integridad del mensaje (MIC).

Confidencialidad de los mensajes (primitivas).

Integridad y autenticidad de los datos (atributos) mediante la etiqueta de integridad de los datos (DIT).

Confidencialidad de los datos (atributos).

Los mensajes y los datos (atributos) protegidos pueden introducirse en una envolvente utilizando la ESPrim y la ESData, respectivamente, mediante los mecanismos descritos en la cláusula 8.4 "Seguridad de extremo a extremo de las primitivas" y 8.5 "Seguridad de extremo a extremo de los datos". La autenticidad/integridad y la confidencialidad de los mensajes se proporcionan utilizando ESPrim, mientras que la integridad y la confidencialidad de los datos de las aplicaciones (atributos) se proporcionan utilizando objetos ESData.

La seguridad de extremo a extremo puede proporcionarse utilizando:

Aprovechando el proceso de provisión de seguridad a distancia basado en la cláusula 8.3 y descrito en la cláusula 8.6.2.

Utilizando las credenciales generadas por el origen descritas en la cláusula 8.6.3.

8.6.1.2 Descripción general del registro y la provisión a distancia para la seguridad de extremo a extremo

En esta cláusula se describen los mecanismos que pueden emplearse para la generación, el registro y la provisión de credenciales que debe utilizarse para la seguridad de extremo a extremo. En base a requisitos de seguridad o perfiles de seguridad asociados a una entidad (por ejemplo, una AE), e indicados en el recurso *<e2ESecurityCapabilities>* descrito en la cláusula 9.6.1.3.2 de [UIT-T Y.4500.1], se generarán las credenciales de seguridad de extremo a extremo pertinentes. Los mecanismos de provisión remota aprovechan los mecanismos descritos en la cláusula 8.3 sobre los marcos de provisión de seguridad a distancia y extienden el mecanismo para que las credenciales de seguridad de extremo a extremo puedan registrarse y proveerse a entidades que están a más de un salto de distancia entre sí. La Figura 8.6.1.2-1 proporciona una secuencia de pasos de alto nivel que pueden seguirse para el registro y la provisión a distancia de credenciales de extremo a extremo.

Los pasos necesarios para proteger la seguridad de extremo a extremo son los siguientes:

Un extremo de origen de la ESP que identifica el conjunto adecuado de mecanismos de seguridad y genera las credenciales apropiadas.

Registro de las credenciales en una función habilitadora de confianza (TEF).

La TEF proporciona las credenciales de extremo a extremo a un extremo ESP de destino.

Procesamiento de ESData/ESPrim utilizando las credenciales de extremo a extremo.

Cuando se utiliza un proceso de provisión de seguridad a distancia, en los pasos 1) y 2) debe intervenir esencialmente una TEF. En el caso de que se utilicen credenciales de seguridad de extremo a extremo generadas en origen, los pasos 1) y 2) serán realizados por el extremo de origen de la ESF.

En la Figura 8.6.1.2-1 se muestra un resumen general del proceso de registro y provisión de credenciales.

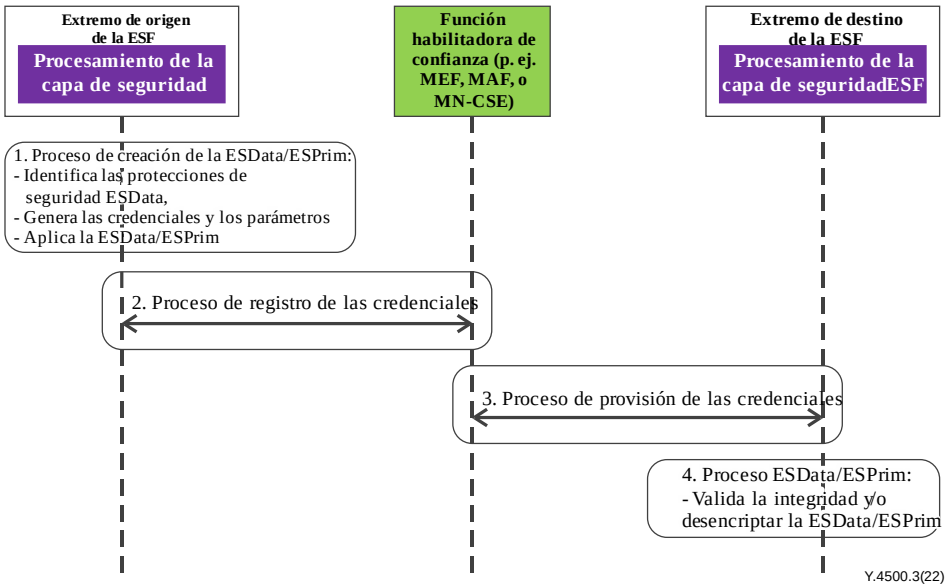


Figura 8.6.1.2-1 – Resumen general del proceso de registro y provisión de credenciales

El proceso de registro y provisión de las credenciales de extremo a extremo para proporcionar la ESData/ESPrim implica los siguientes pasos:

La creación de la ESData/ESPrim por el proceso del extremo de origen de la ESF implica:

a) Identificación de los mecanismos de protección de la seguridad en función de los requisitos de seguridad asociados con los datos de las aplicaciones.

b) En base a los requisitos de seguridad, se generan las credenciales de seguridad adecuadas y los parámetros asociados.

c) A continuación, los datos de las aplicaciones se protegen mediante las credenciales de seguridad y los parámetros asociados, para generar la ESData/ESPrim.

NOTA 1 – En el caso del proceso de provisión de seguridad a distancia, estos pasos a) y b) los realiza una función habilitadora de confianza. Mientras que, en el caso de la generación por parte del origen, dicho origen sigue los pasos descritos anteriormente.

El proceso de registro de las credenciales:

a) El extremo de origen de la ESF registra la o las credenciales y los parámetros asociados en una función habilitadora de confianza.

b) El extremo de origen de la ESP debe proporcionar la identidad de los extremos de destino de la ESF que tienen autorización para que le provisionen las credenciales de extremo a extremo y los parámetros asociados.

NOTA 2 – En el caso del proceso de provisión de seguridad a distancia, el proceso de registro de las credenciales lo realizado una función habilitadora de confianza. Mientras que, en el caso de la generación por parte del origen, dicho origen sigue los pasos descritos anteriormente.

Proceso de provisión/requisición de credenciales:

a) Un extremo de destino de la ESF puede solicitar las credenciales de la ESData/ESPrim utilizando un ID de credencial obtenido como parte de la ESData/ESPrim.

b) En base a la información de autorización proporcionada como parte del proceso de registro de las credenciales y utilizando el ID de credencial, la función habilitadora de confianza provisiona las credenciales adecuadas y los parámetros de encriptación correspondientes en el extremo de destino de la ESF autenticado y autorizado.

Procesamiento de la ESData/ESPrim:

a) El extremo de destino de la ESF utiliza las credenciales provisionadas por la función habilitadora de confianza para procesar la ESData/ESPrim.

b) El procesamiento de la ESData/ESPrim supone la verificación/autentificación de la integridad de los datos de las aplicaciones y/o la desencriptación de los datos y los mensajes, respectivamente.

8.6.2 Proceso de provisión de seguridad a distancia para las credenciales de seguridad de extremo a extremo

En esta cláusula se describe la provisión a distancia de credenciales de seguridad de extremo a extremo simétricas. Las credenciales de seguridad de extremo a extremo deben generarse después de haber completado la provisión a distancia de credenciales simétricas, utilizando la clave simétrica provisionada o los procesos de establecimiento de una asociación de seguridad de clave simétrica basados en una MAF, como se describe en la cláusula 8.3.

En base a los requisitos de alto nivel, se pueden generar las credenciales de extremo a extremo adecuadas utilizando el proceso de provisión de seguridad a distancia mediante la utilización de credenciales pre-provisionadas. En la Figura 8.6.2-1 se muestra el proceso general de generación de claves.

Como parte del mecanismo de "generación de claves de extremo a extremo", el inscrito y el objetivo de inscripción generan las credenciales de extremo a extremo utilizando la Kpsa como clave maestra para generar la clave maestra de extremo a extremo. Si el inscrito es una AE (extremo de origen de la ESF), y objetivo de inscripción es una CSE (extremo de destino de la ESF), se genera una credencial maestra de extremo a extremo, Ke2e_master. A continuación, se ofrece un ejemplo de generación de claves de extremo a extremo utilizando la [IETF RFC 5869].

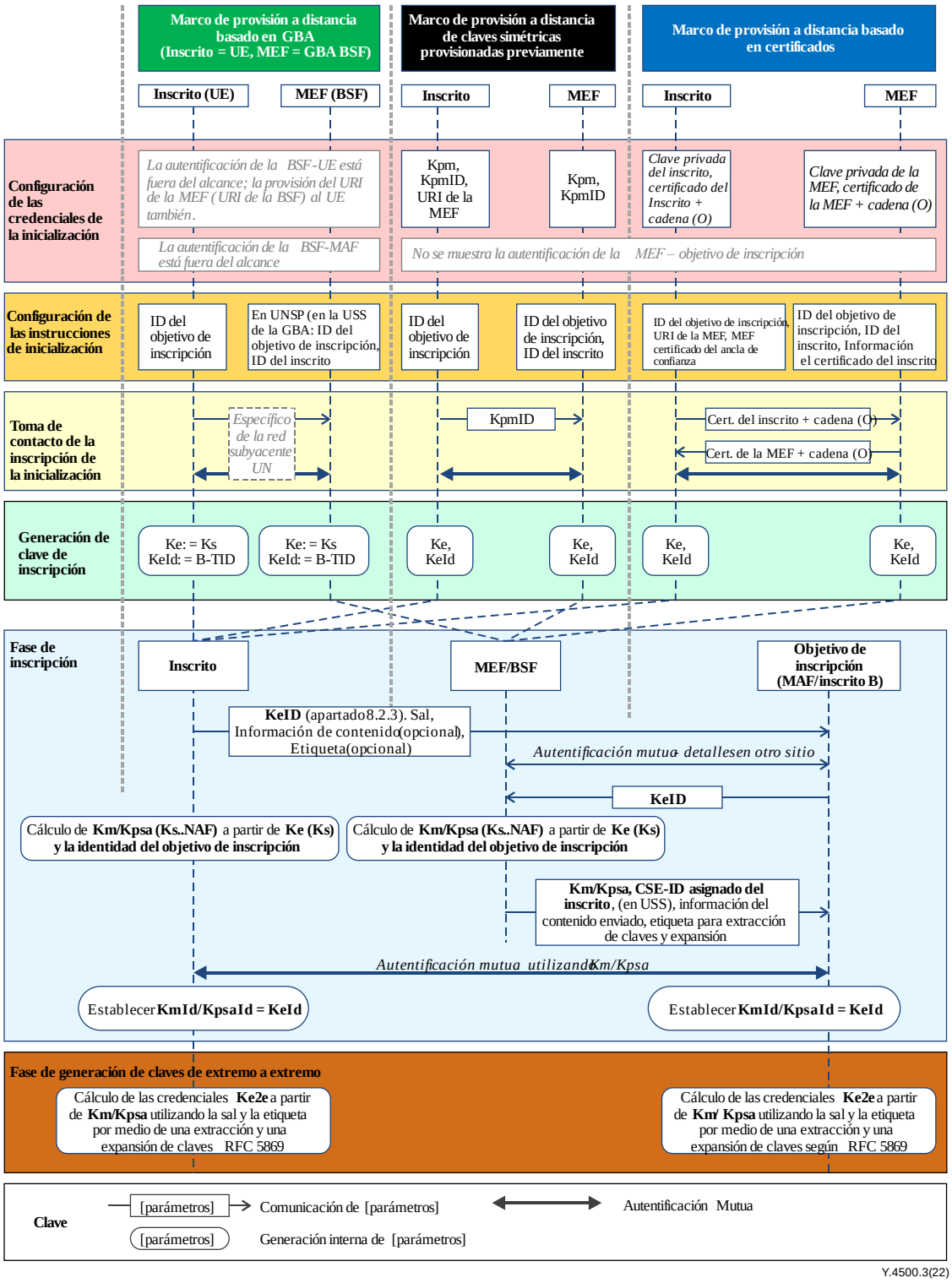


Figura 8.6.2-1 – Resumen general de los marcos de provisión de seguridad de extremo a extremo

Configuración de las credenciales de la inicialización: La configuración de las credenciales de inicialización puede basarse en el tipo de marco de provisión a distancia que se utiliza. Cuando se utiliza la provisión a distancia de claves simétricas, el inscrito, que puede ser el extremo de origen de la ESF, y los objetivos de inscripción (el extremo de destino de la ESF) se provisionan previamente cada uno con la clave simétrica del inscrito (Kpm) y el correspondiente identificador de la clave simétrica, KpmID. Además, se provisiona el extremo de origen de la ESF con la dirección de la función habilitadora de confianza (URI de la TEF). El mecanismo sigue los procedimientos descritos en la cláusula 8.3.2.1.

Configuración de las instrucciones de la inicialización: El extremo de origen de la ESF (inscrito) y la función habilitadora de confianza se configuran con la información necesaria para autorizar la provisión a distancia:

El extremo de origen de la ESF (inscrito) se configura con los siguientes argumentos para iniciar la provisión a distancia:

a) El perfil de seguridad del extremo de destino de la ESF: El perfil de seguridad del extremo de destino de la ESF y las capacidades de seguridad asociadas, descritas en el recurso <*e2ESecurityCapabilities*>, pueden utilizarse para identificar los tipos de mecanismos de protección de seguridad que se deben utilizarse para la seguridad de extremo a extremo.

b) La identidad del extremo de destino de la ESF: que identifica el extremo de destino de la ESF para quien el extremo de origen de la ESF debe proporcionar las credenciales de seguridad de extremo a extremo.

c) El perfil de seguridad del extremo de destino de la ESF: El perfil de seguridad del extremo de destino de la ESF y las capacidades de seguridad correspondientes, descritas en el recurso <*e2ESecurityCapabilities*>, pueden utilizarse para identificar los tipos de mecanismos de protección de seguridad que se utilizarán para la seguridad de extremo a extremo.

d) El extremo de origen de la ESF asocia estos argumentos con la función habilitadora de confianza (TEF). La función habilitadora de confianza puede identificarse en el extremo de origen de la ESF utilizando el identificador de clave simétrica del inscrito (KpmID) previamente provisionado y el URI de la función habilitadora de confianza.

La función de inscripción M2M o habilitadora de confianza se configura con los siguientes argumentos para autorizar a dicha función de inscripción M2M a provisionar a distancia el extremo de origen de la ESF para un extremo de destino de la ESF:

a) La identidad del extremo de destino de la ESF: Identificación del extremo de destino de la ESF para el que se provisiona el extremo de origen de la ESF.

b) El CSE-ID o el AE-ID asignado al extremo de origen de la ESF (ID del extremo de origen de la ESF). La función habilitadora de confianza debe proporcionar esta identidad de entidad del extremo de origen de la ESF, con la Km o la Kpsa, al extremo de destino de la ESF, cuando lo solicite dicho extremo de destino de la ESF.

c) El perfil de seguridad del extremo de origen de la ESF: El perfil de seguridad del extremo de origen de la ESF proporciona el nivel de seguridad esperado descrito en el recurso <*e2ESecurityCapabilities*> (véase la cláusula 9.6.3 de [UIT-T Y.4500.1]) asociado al extremo de origen de la ESF.

d) El perfil de seguridad del extremo de destino de la ESF: El perfil de seguridad del extremo de destino de la ESF proporciona el nivel de seguridad esperado descrito dentro del recurso <*e2ESecurityCapabilities*> asociado al extremo de destino de la ESF.

e) La función habilitadora de confianza debe proporcionar los parámetros detallados para la extracción y la expansión de claves que se utilizarán al extraer las credenciales de extremo a extremo de la Km o Kpsa para el extremo de origen y el extremo de destino de la ESF.

f) La función habilitadora de confianza debe proporcionar el alcance y los parámetros de seguridad asociados al extremo de origen y al extremo de destino de la ESF que determinan los protocolos y los algoritmos de encriptación que deben utilizarse para conseguir la seguridad de extremo a extremo.

Toma de contacto de seguridad de la inicialización: El extremo de origen de la ESF y la función habilitadora de confianza realizarán una toma de contacto (D)TLS PSK [IETF RFC 4279] para establecer una sesión segura. Los mecanismos siguen el proceso detallado en la cláusula 8.3.2.

Generación de claves de extremo a extremo:

a) La clave de inscripción (Ke) y el relativeKeID se generan a partir de los secretos de sesión (D)TLS por parte del extremo de origen de la ESF y la función habilitadora de confianza utilizando la exportación de claves TLS ([IETF RFC 5705]), como se describe en la cláusula 10.3.1 "Detalles de la exportación de claves TLS". Del mismo modo, el identificador de la clave de inscripción (KeID) se genera a partir del RelativeKeID y del FQDN de la función habilitadora de confianza por parte del extremo de origen de la ESF y la función habilitadora de confianza, como se describe en la cláusula 10.3.4 "Generación del KeID". El extremo de origen de la ESF y la función habilitadora de confianza almacenan la Ke y el KeID correspondiente.

b) La clave maestra de extremo a extremo (Ke2e_master) y el E2EKeyId se generan de manera similar a la Kpsa y el KpsaID correspondiente. Si el extremo de origen de la ESF solicita la provisión de claves de extremo a extremo, se debe realizar una extracción de claves basada en Kpsa/Km.

c) La clave maestra de extremo a extremo (Ke2e_master) se utiliza para generar claves específicas para la protección de seguridad, como la clave de autentificación de extremo a extremo, la clave de confidencialidad de extremo a extremo y otras claves en función de los parámetros de extracción y expansión de claves que se hayan proporcionado. La extracción y la expansión de claves se basan en [IETF RFC 5869].

NOTA – La generación de claves de extremo a extremo para el marco de provisión de seguridad a distancia de las claves simétricas de inscritos es idéntica a la generación de claves de extremo a extremo para el marco de provisión de seguridad a distancia basado en certificados.

8.6.3 Descripción detallada de las credenciales de extremo a extremo generadas en origen

En esta cláusula se describe la generación y el registro de las credenciales de seguridad simétricas de extremo a extremo por parte del extremo de origen de la ESF. Las credenciales de seguridad de extremo a extremo autogeneradas por un origen deben registrarse en la función habilitadora de confianza. Un mecanismo de este tipo es especialmente útil cuando se requieren datos (atributos) y mensajes dirigidos a más de un destino. En los casos en que se requiera proteger un recurso <*contentInstance*> utilizado por múltiples entidades de destino, deben utilizarse las credenciales generadas por el origen.

Un origen que genere datos utilizados por una o más entidades de destino puede generar las credenciales adecuadas para que un único atributo (por ejemplo, el valor del atributo de contenido de un recurso <*contentInstance*> o el *customAttribute* de un recurso <*flexContainer*>) o un único elemento direccionable dentro del atributo puedan protegerse en cuanto a integridad y confidencialidad mediante la ESData/ESPrim. En el caso de una autorización dinámica, todo o parte del valor de un parámetro de una primitiva (por ejemplo, un testigo de acceso firmado y autocontenido comunicado en una primitiva de petición para obtener una autorización dinámica) también puede protegerse mediante ESData/ESPrim. La entidad que ha generado los ESData/ESPrim registra entonces las credenciales en una función habilitadora de confianza.

En la Figura 8.6.3-1 se muestra un resumen general de la utilización de una función habilitadora de confianza (TEF) para la distribución de credenciales generados por el origen.

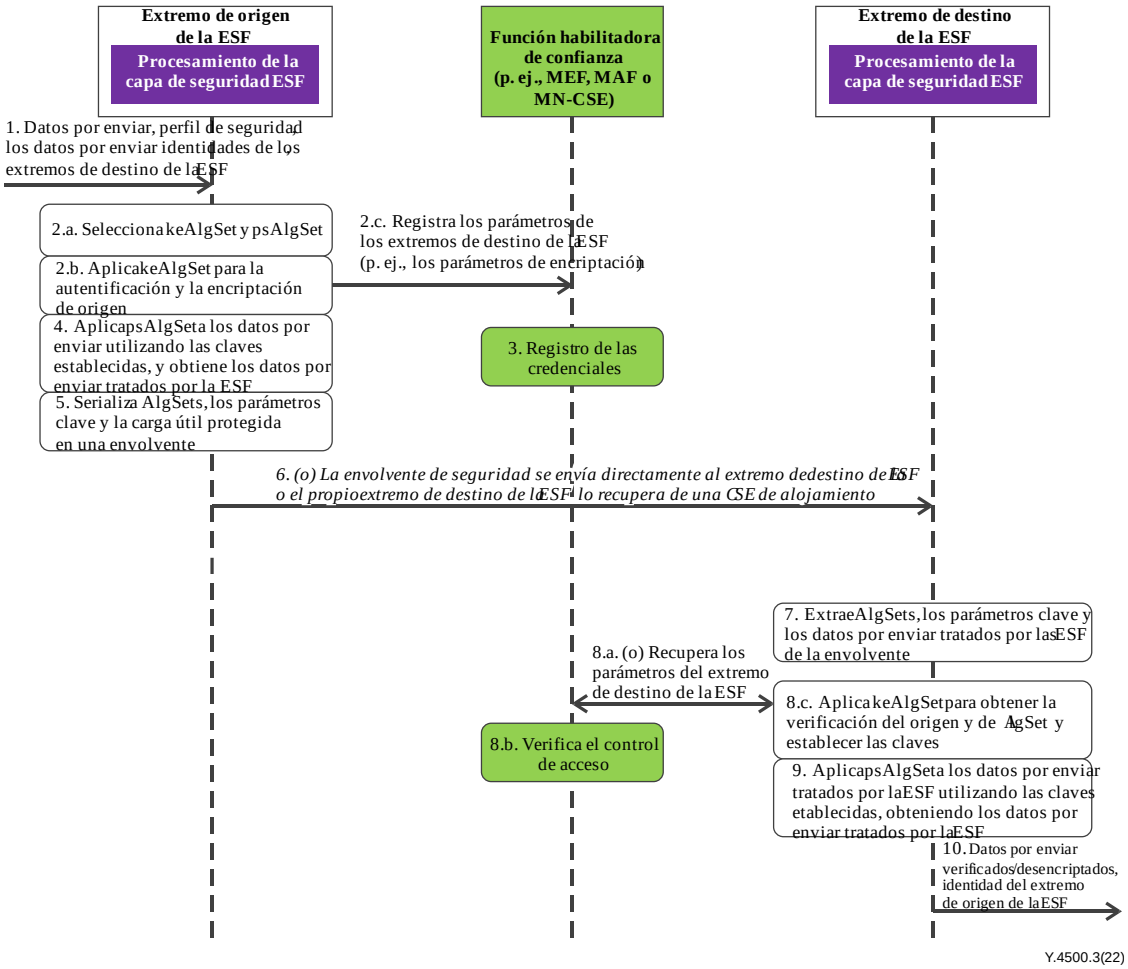


Figure 8.6.3-1 – Resumen general de la utilización de una función habilitadora de confianza (TEF) para la distribución de credenciales generados por el origen

Configuración de las credenciales de la inicialización: Se supone que se provisiona el extremo de origen de la ESF con la Ke/KeID que se generó en el marco de provisión a distancia con una función habilitadora de confianza (por ejemplo, la función de inscripción M2M), como se describe en la cláusula 8.2. Puede provisionarse el extremo de origen de la ESF con la Km/KmID que se generó como parte del marco de provisión a distancia con una función habilitadora de confianza, como se describe en la cláusula 8.3. El extremo de destino de la ESF puede provisionarse con la Ke/KeID si la función habilitadora de confianza es una función de inscripción M2M, o con la Km/KmID si la asociación de seguridad se estableció con una función de autentificación M2M.

Configuración de las instrucciones de la inicialización: El extremo de origen de la ESF, así como los extremos de destino de la ESF, se provisionan con los URI de la función habilitadora de confianza que soportan la provisión y el registro de credenciales de seguridad de extremo a extremo.

El extremo de origen de la ESF se configura con los siguientes argumentos para iniciar la provisión a distancia:

a) La identidad del extremo de destino de la ESF que debe proporcionarse con los ESData/ESPrim y las credenciales de seguridad de extremo a extremo asociadas.

b) Los requisitos de seguridad asociados con los datos (atributos): preconfigurados y proporcionados por la aplicación. En función de los mecanismos de protección de seguridad, se utilizarán las tecnologías de seguridad adecuadas para la protección.

c) Preconfigurado mediante un cuadro en el que se enumeran los requisitos de seguridad y el modo en que éstos pueden satisfacerse utilizando los mecanismos de protección de seguridad

adecuados (por ejemplo, protocolos de seguridad, algoritmos para la integridad, la confidencialidad o la generación de claves).

d) El perfil de seguridad del extremo de destino de la ESF (opcional): El perfil de seguridad del extremo de destino de la ESF y las capacidades de seguridad asociadas del extremo de destino de la ESF, como se describen en el recurso <*e2ESecurityCapabilities*>, pueden utilizarse para identificar los tipos de mecanismos de protección de seguridad que se utilizarán para proporcionar la ESData/ESPrim.

La función habilitadora de confianza se configura con los siguientes argumentos para registrar las credenciales de seguridad ESData/ESPrim del extremo de origen de la ESF y para autorizar a la función habilitadora de confianza a provisionar, sólo en un conjunto de extremos de destino de la ESF autorizados, los parámetros de seguridad de la encriptación de ESData/ESPrim pertinentes:

a) Parámetros de encriptación: Una lista de parámetros de encriptación de extremo a extremo que se identifica con un identificador de credenciales (Credential-Id) y que tiene asociados valores de encriptación como la(s) credencial(es), el (los) algoritmo(s) de encriptación, la(s) etiqueta(s) y el (los) valor(es) aleatorio(s) (por ejemplo, nonce, IV). El extremo de origen de la ESF proporciona estos parámetros durante el proceso de registro de las credenciales. Puede haber una o más credenciales asociadas a uno o más mecanismos de protección de seguridad (por ejemplo, integridad de los datos, confidencialidad de los datos). La lista también puede incluir el alcance y la utilización de los parámetros de seguridad de extremo a extremo para que el extremo de destino de la ESF sea capaz de procesar los ESData/ESPrim (por ejemplo, verificar la integridad y/o desencriptar los ESData/ESPrim).

b) Identidad del extremo de destino de la ESF: Identidad de los extremos de destino de la ESF que deben provisionarse con las credenciales solicitadas identificadas por un Credential-Id. La autorización puede proporcionarse y aplicarse mediante unas políticas de control de acceso (ACP).

El extremo de destino de la ESF se configura con los siguientes argumentos:

a) ESData/ESPrim: El extremo de destino de la ESF recibe los ESData/ESPrim directamente de un extremo de origen de la ESF, o el extremo de destino de la ESF recupera los ESData/ESPrim de una entidad de alojamiento (por ejemplo, la CSE de alojamiento).

b) Identificador de credenciales (Credential-Id): Se provisiona en el extremo de destino de la ESF la Credential-Id, que puede incluirse como parte de la ESData/ESPrim.

c) Parámetros de encriptación: La función habilitadora de confianza proporciona los parámetros de encriptación después de verificar las políticas de control de acceso asociadas con la petición del extremo de origen de la ESF.

Toma de contacto de la seguridad

a) El extremo de origen de la ESF y la función habilitadora de confianza realizan una toma de contacto (D)TLS [IETF RFC 4279] para el establecimiento de una sesión segura. Los mecanismos siguen el proceso descrito en la cláusula 8.3.2. Todas las comunicaciones entre el extremo de origen de la ESF y la función habilitadora de confianza están protegidas por medio de la conexión (D)TLS establecida.

b) El extremo de destino de la ESF y la función habilitadora de confianza realizan una toma de contacto (D)TLS [IETF RFC 4279] para el establecimiento de una sesión segura. Los mecanismos siguen el proceso descrito en la cláusula 8.3.2. Todas las comunicaciones entre el extremo de origen de la ESF y la función habilitadora de confianza están protegidas por medio de la conexión (D)TLS establecida.

Generación de claves de extremo a extremo

a) El extremo de origen de la ESF genera las credenciales que pueden estar basadas en:
   - Credenciales generadas utilizando la clave de inscripción, Ke/KeID que se ha generado mediante el proceso de provisión a distancia de credenciales de inicialización
   - Credenciales generadas de forma aleatoria por el extremo de origen de la ESF y registradas en la función habilitadora de confianza.

8.7 Establecimiento de claves de extremo a extremo basadas en certificados (ESCertKE)

8.7.1 Finalidad del ESCertKE

El establecimiento de claves de extremo a extremo basadas en certificados (ESCertKE) proporciona un marco interoperable para que dos extremos utilicen certificados para establecer una clave simétrica secreta denominada *pairwiseE2EKey* a partir de la cual se obtienen claves simétricas para su uso en otros marcos de seguridad de extremo a extremo, como la seguridad de extremo a extremo de los datos (ESData) o la seguridad de extremo a extremo de las primitivas (ESPrim).

Los casos de utilización y los requisitos aplicables se analizan en el informe técnico TR-0012 de oneM2M [b-oneM2M TR0012].

En esta Recomendación se especifican los mensajes ESCertKE y los procesos asociados para el ESCertKE. El transporte de los mensajes ESCertKE se especifica en [UIT-T Y.4500.1].

8.7.2 Arquitectura del ESCertKE

8.7.2.1 Modelo de referencia del ESCertKE

Las entidades del modelo de referencia del ESCertKE son el extremo de inicio del ESCertKE (*ESCertKE Initiating end-point*) que inicia el procedimiento y el extremo de terminación único del ESCertKE (*ESCertKE terminating end-point*) con el que el extremo de inicio del ESCertKE desea establecer una clave *pairwiseE2EKey.*

NOTA – En el ámbito de la cláusula 8.7, los términos que incluyen la palabra "ESCertKE" pueden acortarse eliminando "ESCertKE" para facilitar su lectura. Por ejemplo, "extremo de inicio del ESCertKE" suele acortarse a "extremo de inicio".

El procedimiento de ESCertKE (*ESCertKE Procedure*) consiste en que el extremo de inicio y el extremo de terminación intercambian una secuencia de mensajes ESCertKE (*ESCertKE messages*) y realizan procesamientos en base a esos mensajes ESCertKE. Si el procedimiento ESCertKE tiene éxito, el extremo de inicio y el extremo de terminación exportan una clave pairwiseE2EKey basada en los parámetros intercambiados en los mensajes ESCertKE.

No existe ninguna restricción implícita sobre qué entidades pueden ser un extremo de inicio; estos extremos pueden ser entidades dentro de un sistema oneM2M (es decir, las EA y las CSE) o entidades fuera de un sistema oneM2M (por ejemplo, entidades que forman parte de un sistema que interactúa con un sistema oneM2M).

La única restricción en cuanto a las entidades que pueden ser puntos extremos de terminación es que el punto extremo de terminación debe ser capaz de recibir el mensaje ESCertKE no solicitado que inicia el procedimiento ESCertKE. Dado que en la [UIT-T Y.4500.1] se especifica el transporte de los mensajes ESCertKE, en la [UIT-T Y.4500.1] también se especifica qué entidades pueden ser extremos de terminación.

8.7.2.2 Flujo de mensajes del procedimiento de ESCertKE

Los mensajes ESCertKE se deben transportar como se especifica en la [UIT-T Y.4500.1]; por ejemplo, se puede utilizar el recurso <*e2EKeyCSE*>.

Los mensajes ESCertKE deben incluir los mensajes TLS v1.2 [IETF RFC 5246] definidos en el Cuadro 8.7.2.2-1 "Definición de mensajes ESCertKE".

El flujo de mensajes del procedimiento de ESCertKE se muestra en la Figura 8.7.2.2-1, y se describe en el texto posterior.

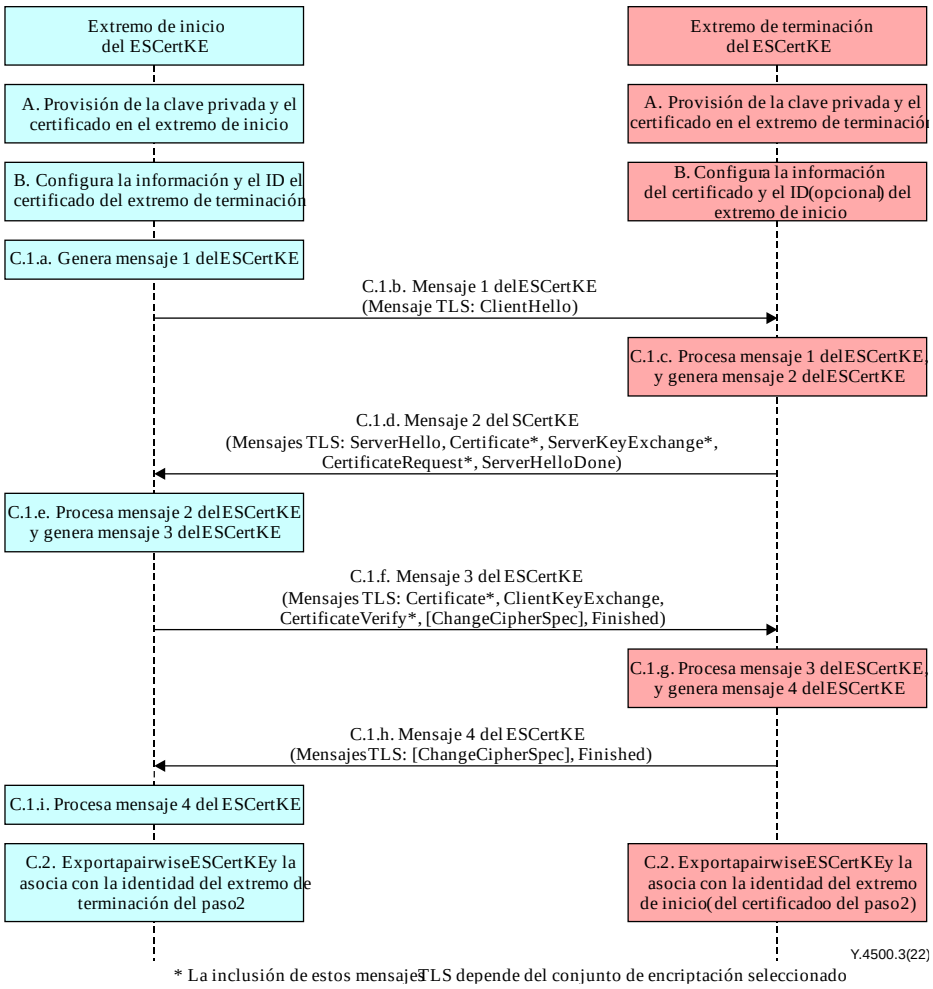


Figura 8.7.2.2-1 – Flujo de mensajes del procedimiento de ESCertKE

A **Provisión de certificados**: Los extremos del ESCertKE deben provisionarse con la clave privada y los certificados descritos en la cláusula 8.1.2.3 "Configuración de credenciales para marcos de seguridad basados en certificados". Los certificados del extremo de inicio y de los extremos de terminación se ajustarán a la cláusula 10.1 "Detalles del marco de seguridad basado en certificados".

B **Activación**: El extremo de inicio y el extremo de terminación deben configurarse con la información necesaria para la autentificación y la identificación del extremo de terminación y del extremo de inicio, respectivamente.

El extremo de inicio recibe la orden de iniciar el procedimiento ESCertKE, y la orden debe incluir los siguientes elementos:

La información del certificado del extremo de terminación descrita en la cláusula 8.1.2.4 "Información necesaria para la autentificación del certificado de otra entidad".

La identidad del extremo de terminación. Dicha identidad se utiliza para:

Determinar dónde se envía el mensaje 1 de ESCertKE; y

Asociarla con la clave pairwiseE2EKey establecida.

El extremo de terminación debe configurarse con los siguientes argumentos que describen la entidad de inicio autorizada a realizar el procedimiento ESCertKE:

La información del certificado del extremo de inicio está descrita en la cláusula 8.1.2.4 "Información necesaria para la autentificación del certificado de otra entidad":

En el caso de que el certificado del extremo de inicio sea un certificado de clave pública bruta, el extremo de terminación también debe configurarse con una identidad para asociarla con la clave pairwiseE2EKey establecida.

Los extremos pueden configurarse en cualquier orden.

C Establecimiento de la *pairwiseE2EKey*:

C.1 El extremo de inicio y el extremo de terminación intercambian la secuencia de cuatro mensajes del ESCertKE. Los mensajes ESCertKE se deben generar y procesar de acuerdo con el protocolo de toma de contacto de TLS v1.2 [IETF RFC 5246]. Las encriptaciones TLS utilizados para el procedimiento ESCertKE deben cumplir al cláusula 10.2.3 "Encriptaciones TLS y DTLS para marcos de seguridad basados en certificados":

C.1.a El extremo de inicio debe generar el mensaje 1 del ESCertKE.

C.1.b El extremo de inicio debe enviar el mensaje 1 del ESCertKE al extremo de terminación identificado en el paso 2.

C.1.c El extremo de terminación debe procesar el mensaje 1 del ESCertKE, y generar el mensaje 2 del ESCertKE.

C.1.d El extremo de terminación debe enviar el mensaje 2 del ESCertKE al extremo de inicio.

C.1.e El extremo de inicio debe procesar el mensaje 2 del ESCertKE, y generar el mensaje 3 del ESCertKE.

C.1.f El extremo de inicio debe enviar el mensaje 3 del ESCertKE al extremo de terminación.

C.1.g El extremo de terminación debe procesar el mensaje 3 del ESCertKE, y generar el mensaje 4 del ESCertKE.

C.1.h El extremo de terminación debe enviar el mensaje 4 del ESCertKE al extremo de inicio.

C.1.i El extremo de inicio debe procesar el mensaje 4 del ESCertKE.

C.2 Si el protocolo de toma de contacto TLS tiene éxito, los extremos de inicio y de terminación deben exportar y almacenar la clave pairwiseE2EKey utilizando la especificación del exportador TLS (IETF RFC 5705 [IETF RFC 5705]) que se describe en la cláusula 10.3.1 "Detalles de la exportación de claves TLS".

Cuadro 8.7.2.2-1 – Definición de los mensajes de ESCertKE

Mensaje del ESCertKE	Extremo emisor	Posibles mensajes TLS v1.2 (caso de éxito) [IETF RFC 5246]	Descripción informativa (la descripción normativa está en la especificación TLS v1.2 [IETF RFC 5246])
1	inicio	ClientHello	Lista de encriptaciones permitidas, valor aleatorio e indicador para la exportación de pairwiseE2EKey.
2	terminación	ServerHello	Encriptación seleccionada, valor aleatorio, indicador para la exportación de pairwiseE2EKey.
		Certificate*	Certificado del extremo de terminación (y opcionalmente cadena de certificados).

Cuadro 8.7.2.2-1 – Definición de los mensajes de ESCertKE

Mensaje del ESCertKE	Extremo emisor	Posibles mensajes TLS v1.2 (caso de éxito) [IETF RFC 5246]	Descripción informativa (la descripción normativa está en la especificación TLS v1.2 [IETF RFC 5246])
		ServerKeyExchange*	Parámetros de intercambio de claves generados por el extremo de terminación. El contenido de este parámetro depende de la encriptación seleccionada.
		CertificateRequest*	Petición al extremo de inicio de que se autentifique con un certificado.
		ServerHelloDone	Indica el final del mensaje.
3	inicio	Certificate*	Certificado del extremo de inicio (y opcionalmente cadena de certificados).
		ClientKeyExchange*	Parámetros de intercambio de claves generados por el extremo de inicio. El contenido de estos parámetros depende de la encriptación seleccionada.
		CertificateVerify	Proporciona una verificación explícita de un certificado del extremo de inicio.
		[ChangeCipherSpec]	Notifica al extremo receptor que los registros posteriores estarán protegidos con las claves y el CipherSpec recién negociados.
		Finished	MIC sobre todos los parámetros precedentes intercambiados en el procedimiento. El MIC se genera utilizando los secretos de sesión establecidos mediante los parámetros anteriores.
4	terminación	[ChangeCipherSpec]	Véase lo anterior
		Finished	MIC sobre todos los parámetros precedentes intercambiados en el procedimiento. El MIC se genera utilizando los secretos de sesión.
NOTA – La inclusión de los mensajes TLS marcados con (*) depende del conjunto de encriptación seleccionado.			

8.8 Detalles de un marco de seguridad con MAF

8.8.1 Introducción a los detalles de un marco de seguridad con MAF

En la cláusula 8.8 se describen los detalles y procedimientos comunes utilizados en los marcos de seguridad basados en MAF; en la presente especificación estos marcos incluyen:

El marco de establecimiento de asociaciones de seguridad (SAEF) basado en MAF

El marco de seguridad de extremo a extremo de las primitivas (ESPrim) basado en MAF.

El marco de seguridad de extremo a extremo de los datos (ESData) basado en MAF.

Estos marcos utilizan una MAF para proporcionar la autentificación y la distribución de claves simétricas para que las utilice un extremo de origen que inicia el establecimiento de la clave simétrica, y uno o más extremos de destino. En el Cuadro 8.8.1-1 "Correspondencia de las funciones de un marco genérico con MAF con las funciones de los marcos específicos con MAF", los clientes de la MAF pueden conseguir en la MAF la clave simétrica de salida. La MAF proporciona sus servicios en nombre de las *partes administradoras interesadas* como los proveedores de servicios M2M o

terceros partes habilitadoras de confianza M2M (MTE). Una parte administradora interesada autoriza a la MAF a prestar servicios a los clientes MAF y supervisa la autorización de la distribución de claves simétricas. En el Cuadro 8.8.1-1 se describe la correspondencia de los clientes MAF de origen y los clientes MAF de destino con las funciones de los marcos específicos basados en MAF, así como el número permitido de clientes MAF de destino.

Cuadro 8.8.1-1 – Correspondencia con las funciones de los marcos específicos basados en MAF

Marco de seguridad basado en MAF	Cliente MAF de origen	Cliente MAF de destino	Número de clientes MAF de destino	Clave simétrica de salida
Marco de establecimiento de asociaciones de seguridad (SAEF)	Entidad A	Entidad B	1	Clave de conexión M2M segura (Kc)
Marco de seguridad de extremo a extremo de las primitivas (ESPrim)	Origen	Destino	1	pairwiseESPrimKey
marco de seguridad de extremo a extremo de los datos (ESData)	Extremo de origen ESData	Extremo de destino ESData	1..n	ESData Key

En este cláusula 8.8 se especifican los *procedimientos MAF* entre los clientes MAF y los mensajes asociados. La operación y la gestión de la MAF, más allá de los detalles proporcionados para los procedimientos MAF, no se especifican en esta Recomendación.

La secuencia general para la utilización de los procedimientos MAF se muestra en la Figura 8.8.1-1 y se describe a continuación:

Cada Cliente MAF debe establecer por separado las credenciales para una autentificación mutua con la MAF como se describe en la **configuración de credenciales de clientes MAF** (cláusula 8.8.3.1).

Cada cliente MAF debe configurarse por separado, para registrarse en el MAF con una parte administradora interesada específica. La **configuración del registro de cliente MAF** (cláusula 8.8.3.2) proporciona los parámetros necesarios.

Cada cliente MAF debe realizar con la MAF un **procedimiento de registro de clientes MAF**. De esta forma, se confirma que el cliente MAF está dispuesto a utilizar los servicios de la MAF, con la autorización de la parte administradora interesada. El cliente MAF debe registrarse por separado con cada parte administradora interesada, incluso cuando se registre a través de una única MAF. Si el cliente MAF se configura a distancia para la autentificación mutua con la MAF, ésta debe proporcionar al cliente MAF el KmID que se utilizará para la autentificación posterior con la MAF.

Posteriormente, e independientemente de esta secuencia de eventos, el **procedimiento de actualización de un registro de cliente MAF** puede llevarse a cabo para confirmar que el cliente MAF desea utilizar los servicios de la MAF y/o establecer una nueva Km y un KmID, y se puede realizar el **procedimiento de supresión de un registro de cliente MAF** para indicar que el cliente MAF deja de utilizar los servicios de la MAF.

El cliente MAF del origen debe estar configurado para establecer una comunicación segura utilizando una función de seguridad (SAEF, ESPrim o ESData) con claves simétricas establecidas a través de la MAF. Los detalles de esta configuración son específicos de la función de seguridad que se invoque, pero deben incluir la **configuración de registro de clave MAF** (cláusula 8.4.4.3)

El cliente MAF de origen debe realizar un **procedimiento de registro de clave MAF** para establecer una clave simétrica y el identificador correspondiente. El cliente MAF de origen también debe proporcionar el identificador de uso de seguridad (SUID) que limita el alcance de la credencial mediante la identificación de la función de seguridad (SAEF, ESPrim o ESData). Este procedimiento debe incluir el **procedimiento de toma de contacto de la MAF** para la autentificación mutua del cliente MAF de origen y la MAF.

Posteriormente, e independientemente de esta secuencia de eventos, el **procedimiento de actualización del registro de una clave MAF** puede llevarse a cabo para actualizar el plazo de caducidad de la clave registrada o actualizar la lista de clientes MAF de destino, y se puede realizar el **procedimiento de supresión del registro de una clave MAF** para eliminar de la MAF el registro de la clave.

El cliente MAF de origen debe proporcionar al cliente o clientes MAF de destino el identificador de clave simétrica establecido en el procedimiento de registro de la clave MAF. Los detalles de este paso dependen de la función de seguridad identificada por el SUID.

El cliente MAF de destino debe realizar el **procedimiento de recuperación de claves MAF**, para recuperar la clave simétrica y su información correspondiente. Este procedimiento debe incluir el **procedimiento de toma de contacto de la MAF** para la autentificación mutua del cliente MAF de destino y la MAF.

La clave simétrica debe utilizarse en el protocolo de seguridad entre el cliente MAF de origen y el cliente MAF de destino. Si el protocolo de seguridad requiere una clave simétrica única, se deberá utilizar la primera mitad de la clave simétrica distribuida. Si el protocolo de seguridad requiere dos claves simétricas (por ejemplo, una clave de encriptación y otra de integridad), se utilizarán las dos mitades de la clave simétrica distribuida como las dos claves simétricas del protocolo de seguridad. Los detalles de este paso dependen de la función de seguridad.

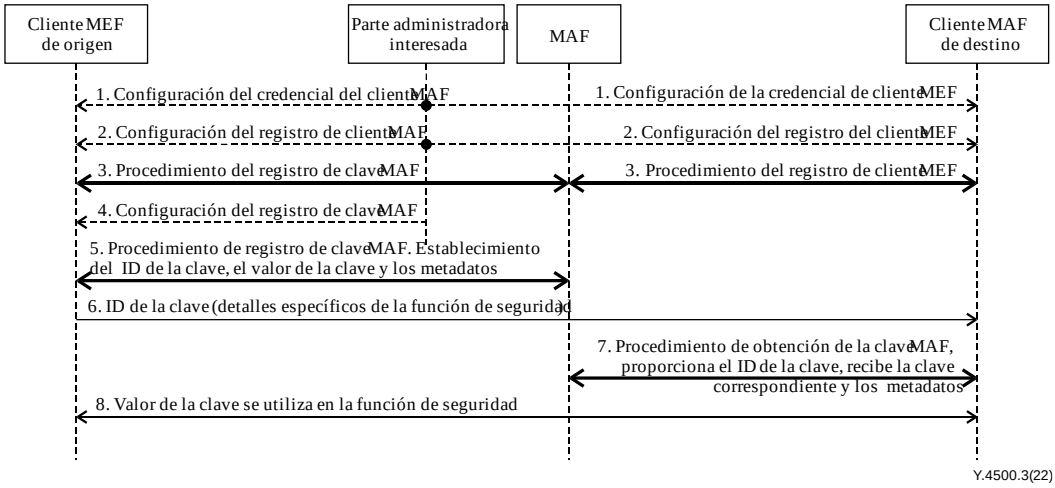


Figura 8.8.1-1 – Secuencia de eventos en la utilización del marco de seguridad con MAF como parte de una función de seguridad

La cláusula 8.8 está organizado de la siguiente manera, en la cláusula 8.8.2 se describe el procesamiento y los flujos de información de los procedimientos MAF. En la cláusula 8.8.3 se describe la información de la configuración de las credenciales de los clientes MAF, la configuración del registro de los clientes MAF y la configuración del registro de claves MAF.

8.8.2 Flujos de información y procesamiento de un marco de seguridad con MAF

8.8.2.1 Introducción

En la cláusula 8.8.2 se especifican los flujos de información y procesamiento de los procedimientos MAF.

8.8.2.2 Procedimiento de toma de contacto de la MAF

Finalidad: Un procedimiento de toma de contacto de la MAF establece una sesión TLS o DTLS mutuamente autentificada para proteger la comunicación entre un cliente MAF y la MAF. En el caso del procedimiento de registro de claves MAF, el cliente MAF de origen y la MAF pueden utilizar la sesión TLS o DTLS para establecer el valor de la clave.

Condiciones previas: Debe cumplirse una de las siguientes condiciones:

Se ha provisionado tanto en el cliente MAF como en la MAF los certificados, como se describe en los detalles de configuración de las credenciales de cliente MAF en la cláusula 8.8.3.1, y se les ha configurado con certificados de CA para validar los certificados, como se describe en los detalles de configuración del registro de cliente MAF en la cláusula 8.8.3.2.

El cliente MAF y la MAF han establecido una credencial maestra simétrica (Km) con el correspondiente identificador de credencial maestra (KmID). La Km y el KmID pueden provisionarse de antemano, o puede establecerse la Km mediante un marco de provisión de seguridad a distancia con el KmID determinado mediante el procedimiento de registro de la MAF.

NOTA – En el caso de establecer la Km a través de la provisión a distancia, la toma de contacto de la MAF no puede realizarse durante el registro del cliente MAF porque (a) la MAF no conoce la Km antes del registro del cliente MAF y (b) no se ha asignado el KmID antes del registro del cliente MAF.

Descripción del procedimiento

Si el cliente MAF y la MAF han establecido una credencial maestra simétrica (Km) con el correspondiente identificador de credencial maestra (KmID), el cliente MAF y la MAF deben establecer la sesión TLS o DTLS utilizando la toma de contacto TLS-PSK de acuerdo con la cláusula 10.2.2, con los siguientes detalles:

Se debe fijar el parámetro "psk_identity" [IETF RFC 4279] en el valor del identificador de la credencial maestra (KmID).

Se debe fijar el parámetro "psk" [IETF RFC 4279] en el valor de la credencial maestra (Km).

Si el cliente MAF y la MAF deben autentificarse utilizando certificados, entonces el cliente MAF y la MAF deben establecer la sesión TLS o DTLS utilizando la toma de contacto TLS basada en certificados de acuerdo con la cláusula 10.2.2, con los siguientes detalles:

El certificado del servidor TLS debe ser el certificado de la MAF. El cliente MAF debe verificar el certificado de la MAF con el conjunto provisionado de anclas de confianza del certificado MAF, como se describe en la cláusula 8.1.2.5.

El certificado del cliente TLS debe ser el certificado del "cliente MAF". La MAF debe verificar el certificado del "cliente MAF" con la información provisionada del certificado del cliente MAF, tal como se describe en la cláusula 8.1.2.5.

8.8.2.3 Procedimiento de registro de clientes MAF

Finalidad: El cliente MAF se registra en la MAF para confirmar que está dispuesto a utilizar los servicios de la MAF, bajo la autorización de la parte administradora interesada. Si se utiliza la provisión a distancia para establecer una clave simétrica entre un cliente MAF y la MAF, entonces el cliente MAF activa la MAF (en la toma de contacto TLS) para recuperar la Km desde la MEF, y la MAF proporciona al cliente MAF el identificador de credencial maestro (KmID) para su utilización en los procedimientos posteriores de la toma de contacto de la MAF.

NOTA – El procedimiento de registro de clientes MAF es equivalente al registro de CSE o de AE, pero en este caso el cliente MAF se está "registrando" en la MAF, y no en la CSE encargada del registro.

Condiciones previas: El cliente MAF, la MAF y (si procede) la MEF están provisionado con los parámetros descritos en las cláusulas 8.8.3.1 y 8.8.3.2.

Descripción del procedimiento

El cliente MAF debe establecer una conexión TLS (o DTLS) con la MAF.

Si se utiliza la provisión a distancia, el cliente MAF (que asume el papel de inscrito), la MEF y la MAF (que asume el papel de objetivo de registro) deben llevar a cabo los pasos b) y siguientes de la "Utilización de una credencial provisionada" de la cláusula 8.3.2.1. El SUID de la clave provisionada a distancia debe ser "21", "Clave simétrica, provisionada a través de un marco de provisión de seguridad a distancia (RSPF), y destinada a ser compartida con una MAF", como se especifica en [UIT-T Y.4500.4]. La MAF recupera la Km en la MEF como parte de este proceso.

En caso contrario, el cliente MAF y la MAF deben realizar los procedimientos de toma de contacto de la MAF (cláusula 8.8.2.2).

De este modo, se proporciona a la MAF una identidad autentificada para el cliente MAF.

El cliente MAF debe enviar una petición de registro de cliente MAF incluyendo la información indicada en el Cuadro 8.8.2.3-1.

Cuadro 8.8.2.3-1 – Información del mensaje de petición de registro de cliente MAF

Parámetro	Descripción	Multiplicidad
MAF-FQDN	FQDN de la MAF, de la configuración de instrucciones de la MAF	1
expirationTime	Plazo de caducidad propuesto del registro.	1
labels	Etiquetas para ayudar a localizar el registro de cliente MAF.	0..1
adminFQDN	FQDN de la parte administradora interesada, proporcionado en la configuración de registro del cliente MAF	1

Al recibir la petición, la MAF debe procesarla. Si se encuentran errores, la MAF debe enviar un mensaje de error. La MAF puede asignar valores diferentes para los parámetros recibidos del cliente MAF, en base a instrucciones de la parte administradora interesada. Si la petición se procesa con éxito, entonces la MAF debe elaborar una respuesta a la petición de registro del cliente MAF incluyendo la información indicada en el Cuadro 8.8.2.3-2.

Cuadro 8.8.2.3-2 – Información del mensaje de respuesta del registro de cliente MAF

Parámetro	Descripción	Multiplicidad
mafClientRegID	Un identificador para el nuevo registro de cliente MAF.	1
labels	Etiquetas para ayudar a localizar el registro de cliente MAF	0..1
expirationTime	Plazo de caducidad del archivo de registro del cliente MAF.	1
MAF Client ID	Identificador del cliente MAF	1
adminFQDN	FQDN de la parte administradora interesada	1

Cuadro 8.8.2.3-2 – Información del mensaje de respuesta del registro de cliente MAF

Parámetro	Descripción	Multiplicidad
assignedSymmKeyID	Identificador de la credencial maestra asignada por la MAF (KmID), en el caso de que la Km se provisiona a distancia	0..1

La MAF debe enviar la respuesta al cliente MAF.

El cliente MAF y la MAF deben almacenar los parámetros. Si se incluyó el assignedSymmKeyID, el cliente MAF debe utilizarlo como ID de la credencial maestra (KmID) en lo sucesivo cuando establezca sesiones TLS (o DTLS) con la MAF.

8.8.2.4 Procedimiento de recuperación de configuración de cliente MAF

Finalidad: Este procedimiento permite a un cliente MAF recuperar las configuraciones de clientes MAF proporcionadas por la parte administradora interesada al MAF.

Condiciones previas

El cliente MAF ha realizado previamente el procedimiento de registro de cliente MAF para crear el archivo de registro del cliente MAF.

El archivo de registro del cliente MAF no ha caducado.

Descripción del procedimiento. El procedimiento incluye los siguientes pasos:

El cliente MAF debe establecer una conexión TLS (o DTLS) con la MAF como se describe en la cláusula 8.8.2.3.

El cliente MAF debe enviar una petición de recuperación de la configuración de cliente MAF incluyendo la información indicada en el Cuadro 8.8.2.4-1.

Cuadro 8.8.2.4-1 – Información del mensaje de petición de recuperación de configuración de cliente MAF

Parámetro	Descripción	Multiplicidad
MAF-FQDN	FQDN de la MAF, de la configuración de instrucciones de la MAF	1
mafClientRegID	Identificador del archivo de registro de cliente MAF que se actualiza	1

Al recibir la petición, la MAF debe procesarla. Si se encuentran errores, incluido el caso de que no haya una configuración de cliente MAF asociada en ese momento al registro de cliente MAF identificado, la MAF debe enviar una respuesta de error. Si la petición se procesa correctamente, la MAF debe intentar recuperar la configuración del cliente MAF asociada en ese momento al registro de la inscripción del cliente MAF identificado.

La MAF debe elaborar una respuesta para la recuperación de configuración de cliente MAF que contenga los siguientes parámetros.

Cuadro 8.8.2.4-2 – Información del mensaje de respuesta de la recuperación de configuración de cliente MAF

Parámetro	Descripción	Multiplicidad
mafClientCfg	Configuración de cliente MAF asociada en ese momento al archivo de registro del cliente MAF identificado	1

La MAF debe enviar la respuesta al cliente MAF.

El cliente MAF debe aplicar la configuración de cliente MAF.

8.8.2.5 Procedimiento de actualización de un registro de cliente MAF

Finalidad: Este procedimiento permite a un cliente MAF actualizar el registro del cliente MAF combinando la ampliación del plazo de caducidad (*expirationTime*) del archivo de registro del cliente MAF, la actualización de las etiquetas o el establecimiento de una nueva Km y su KmID.

Condiciones previas

El cliente MAF ha realizado previamente el procedimiento de registro de cliente MAF para crear el archivo de registro de cliente MAF.

El archivo de registro de cliente MAF no ha caducado.

Descripción del procedimiento. El procedimiento incluye los siguientes pasos:

El cliente MAF debe establecer una conexión TLS (o DTLS) con la MAF como se describe en la cláusula 8.8.2.3.

El cliente MAF debe enviar una petición de actualización de un registro de cliente MAF incluyendo la información indicada en el Cuadro 8.8.2.5-1.

Cuadro 8.8.2.5-1 – Información del mensaje de petición de actualización de un registro de cliente MAF

Parámetro	Descripción	Multiplicidad
MAF-FQDN	FQDN de la MAF, de la configuración de instrucciones de la MAF	1
mafClientRegID	Identificador del archivo de registro del cliente MAF que se actualiza	1
expirationTime	Plazo de caducidad propuesto del archivo de registro del cliente MAF.	0..1
labels	Etiquetas para ayudar a localizar el registro de cliente MAF	0..1
NOTA – Se debe incluir al menos uno entre los parámetros expirationTime y labels (etiquetas)		

Al recibir la petición, la MAF debe procesarla. Si se encuentran errores, la MAF debe enviar un mensaje de error. En caso de que la petición se procese con éxito, la MAF debe actualizar el archivo de registro del cliente MAF con los valores propuestos si lo autoriza la parte administradora interesada. La MAF puede asignar diferentes valores para los parámetros recibidos del cliente MAF, en base a instrucciones de la parte administradora interesada.

La MAF deberá elaborar una respuesta para la actualización del registro de cliente MAF incluyendo los parámetros del Cuadro 8.8.2.5-2.

Cuadro 8.8.2.5-2 – Información del mensaje de respuesta para la actualización del registro de cliente MAF

Parámetro	Descripción	Multiplicidad
expirationTime	Plazo de caducidad actualizado del archivo del registro de cliente MAF.	0..1
labels	Etiquetas actualizadas para ayudar a localizar el registro de cliente MAF.	0..1
assignedSymmKeyID	ID de la credencial maestra (KmID) asignada por el MAF, en los casos en que se provisiona a distancia una nueva Km.	0..1
NOTA – La respuesta solo incluye expirationTime y/o labels (etiquetas) si dichos parámetros estaban presentes en la petición correspondiente.		

La MAF debe enviar la respuesta al cliente MAF.

El cliente MAF y la MAF deben almacenar los parámetros. Si se incluyó *assignedSymmKeyID*, el cliente MAF lo utilizará como ID de la credencial maestra en lo sucesivo en el establecimiento de sesiones TLS (o DTLS) con la MAF.

8.8.2.6 Procedimiento de supresión de registro de cliente MAF

Finalidad: Este procedimiento permite a un cliente MAF poner fin a su registro con la MAF.

Condiciones previas: El cliente MAF ha realizado previamente el procedimiento de registro de cliente MAF para crear el archivo de registro de cliente MAF.

El archivo de registro de cliente MAF no ha caducado.

Descripción del procedimiento. El procedimiento incluye los siguientes pasos:

El cliente MAF debe establecer una conexión TLS (o DTLS) con la MAF como se describe en la cláusula 8.8.2.3.

El cliente MAF debe enviar una petición de supresión de registro de cliente MAF incluyendo la información indicada en el Cuadro 8.8.2.6-1.

Cuadro 8.8.2.6-1 – Información del mensaje de petición de supresión del registro de cliente MAF

Parámetro	Descripción	Multiplicidad
MAF-FQDN	FQDN de la MAF, de la configuración de instrucciones de la MAF	1
mafClientRegID	Identificador del registro de cliente MAF que se finaliza	1

Al recibir la petición, la MAF debe procesarla. Si se encuentran errores, la MAF debe enviar un mensaje de error. En caso de que la petición se procese con éxito, la MAF suprimirá la información asociada al archivo de registro del cliente MAF identificado.

La MAF debe elaborar una respuesta de actualización del registro del cliente MAF indicando que la operación se ha realizado con éxito. La MAF debe enviar la respuesta al cliente MAF.

8.8.2.7 Procedimiento de registro de clave MAF

Finalidad: Este procedimiento permite a un cliente MAF de origen establecer con la MAF una clave simétrica que uno o más clientes MAF de destino pueden recuperar para utilizarla.

Este procedimiento se realiza entre el cliente MAF de origen y la MAF.

Condiciones previas: El cliente MAF de origen ha sido provisionado con la información (o la ha definido de otro modo) en la configuración del registro de clave MAF (cláusula 8.8.3.3).

El cliente MAF de origen ha realizado el procedimiento de registro de clientes MAF (cláusula 8.8.2.3) con la MAF para la parte administradora interesada identificada en la configuración de registro de clave MAF.

Descripción del procedimiento. El procedimiento incluye los siguientes pasos:

El cliente MAF de origen debe establecer una sesión TLS o DTLS con la MAF utilizando el procedimiento de toma de contacto de la MAF, descrito en la cláusula 8.8.2.2. Una consecuencia del procedimiento de toma de contacto de la MAF es que la MAF establece una identidad autentificada para el cliente MAF de origen.

El cliente MAF de origen selecciona el valor de la clave de conexión segura M2M (Kc) que debe distribuir la MAF. El valor debe ser uno de los siguientes:

El cliente MAF de origen genera el valor de la clave simétrica de salida a partir de los secretos de sesión (D)TLS utilizando la exportación de claves TLS ([IETF RFC 5705]), tal como se describe en la cláusula 10.3.1 "Detalles de la exportación de claves TLS".

El cliente MAF de origen genera por sí mismo el valor de la clave simétrica de salida, independientemente de los secretos de sesión (D)TLS.

El cliente MAF de origen debe elaborar una lista de clientes MAF de destino a los que la MAF está autorizada a proporcionar el valor de la clave simétrica de salida:

En el caso de la SAEF basada en la MAF o la ESPrim basada en la MAF: La lista deberá contener exactamente un AE-ID absoluto o un CSE-ID absoluto.

En el caso de la ESData basada en MAF: La lista deberá contener cualquier número no nulo de AE-ID absolutos o CSE-ID absolutos.

NOTA 1 – La forma en que el cliente MAF de origen selecciona la lista de clientes MAF de destino depende de la aplicación.

El cliente MAF de origen debe enviar una petición de registro de clave MAF, incluyendo la información indicada en el Cuadro 8.8.2.7-1.

Cuadro 8.8.2.7-1 – Información del mensaje de petición de registro de clave MAF

Parámetro	Descripción	Multiplicidad
MAF-FQDN	FQDN de la MAF, de la configuración de instrucciones de la MAF	1
expirationTime	Plazo de caducidad propuesto del registro de la clave.	1
labels	Etiquetas para ayudar a localizar el registro de la clave	0..1
adminFQDN	Identificador de la parte administradora interesada	1
SUID	Identificador de uso de seguridad que limita las funciones de seguridad en las que se puede utilizar la clave simétrica.	1
targetIDs	(Opcional) lista de identificadores del conjunto inicial de clientes MAF de destino autorizados a recuperar la clave simétrica.	0..1
Key Value	(Opcional) Cuando está presente, este parámetro contiene un valor de clave simétrica de salida que el cliente MAF de origen genera por sí mismo. Si este parámetro no está presente, el cliente MAF de origen y la MAF generarán el valor de la clave simétrica de salida utilizando TLS Exporter	0..1

La MAF debe procesar la petición. Si se encuentran errores, la MAF debe enviar un mensaje de error. En caso de que la petición se procese con éxito, la MAF debe autorizar el establecimiento de un valor de clave, basado en la identidad autentificada del cliente MAF de origen.

NOTA 2 – La presente especificación no proporciona ningún detalle sobre la autorización de esta petición.

Si la petición incluyó un valor en el parámetro *Key Value* (valor de la clave), la MAF debe almacenar este valor. En caso contrario, la MAF debe generar el valor de la clave a partir de la sesión (D)TLS utilizando TLS Key Export ([IETF RFC 5705]), como se describe en la cláusula 10.3.1 "Detalles de la exportación de claves TLS".

La MAF debe actualizar la lista de clientes MAF de destino autorizados (los clientes MAF que pueden recuperar esta credencial) con la lista proporcionada en la petición.

En el caso de la ESData basada en la MAF: las parte administradoras interesadas pueden actualizar posteriormente esta lista durante el procedimiento de registro de la clave MAF o después de dicho registro.

NOTA 3 – Esta especificación no proporciona ningún detalle sobre la actualización por las partes administradoras interesadas de la lista de clientes MAF autorizados en la MAF. La MAF podría proporcionar su propia interfaz y funcionalidad para que las partes administradoras interesadas puedan gestionar esta lista.

La MAF debe seleccionar un valor de RelativeKeyID que no se haya utilizado previamente.

La MAF puede asignar diferentes valores para los parámetros recibidos del cliente MAF, en base a instrucciones de la parte administradora interesada.

La MAF debe enviar una respuesta, al cliente MAF de origen, incluyendo la información indicada en el Cuadro 8.8.2.7 2.

Cuadro 8.8.2.7-2 – Información del mensaje de respuesta del registro de clave MAF

Parámetro	Descripción	Multiplicidad
RelativeKeyID	La parte correspondiente del identificador de la clave asociada con el registro de la clave.	1
expirationTime	Plazo de caducidad del registro de la clave.	1
Source MAF Client ID	Identificador del cliente MAF de origen.	1
labels	Etiquetas para ayudar a localizar el registro de la clave.	0..1
adminFQDN	Identificador de la parte administradora interesada.	1
SUID	Identificador de uso de seguridad que limita las funciones de seguridad en las que se puede utilizar la clave simétrica.	
targetIDs	Lista de identificadores del conjunto inicial de clientes MAF de destino autorizados a recuperar la clave simétrica. Esta lista puede ser una modificación de la lista proporcionada por el cliente MAF, o creada por la MAF (cuando el cliente MAF no proporcionó una lista).	1

El cliente MAF de origen y la MAF almacenarán el valor de la clave simétrica de salida y el identificador de clave correspondiente.

El cliente MAF de origen y la MAF generan el identificador de clave a partir del RelativeKeyID y el FQDN de la función de autentificación M2M, como se describe en la cláusula 10.3.5 "Generación del KcID".

8.8.2.8 Procedimiento de recuperación de clave MAF

Finalidad: Este procedimiento permite a un cliente MAF de destino recuperar el valor de la clave MAF que corresponde con un RelativeKeyID recibido por dicho cliente MAF de destino.

Condiciones previas: El cliente MAF de destino ha realizado la configuración de credenciales de cliente MAF (cláusula 8.8.2.1) con la MAF, incluida la configuración del URI de recuperación de claves MAF.

El cliente MAF de origen ha llevado a cabo el procedimiento de registro de la clave MAF (cláusula 8.8.2.2) con la MAF, con lo que se ha registrado un valor de clave y se ha asignado un RelativeKeyID para una parte administradora interesada específica y un identificador de uso de seguridad (SUID).

El cliente MAF de destino recibió un identificador de clave procedente del cliente MAF de inicio en una función de seguridad con el SUID que el cliente MAF de origen proporcionó a la MAF durante el procedimiento de registro de la clave MAF (cláusula 8.8.2.7). El identificador de clave debe estar compuesto por el FQDN de la MAF y el RelativeKeyID asignado a la clave registrada.

El cliente MAF de destino puede suponer que está autorizado a recuperar el valor de la clave simétrica de salida correspondiente.

NOTA – El cliente MAF de destino no tiene que repetir este procedimiento si ya dispone del valor de la clave correspondiente.

Descripción del procedimiento. El procedimiento incluye los siguientes pasos:

El cliente MAF de destino debe establecer una sesión TLS o DTLS con la MAF utilizando el procedimiento de toma de contacto de la MAF, descrito en la cláusula 8.8.2.2. Una consecuencia de los procedimientos de toma de contacto de la MAF es que la MAF establece una identidad autentificada para el cliente MAF de destino.

El cliente MAF de destino debe enviar una petición de recuperación de clave MAF a la MAF incluyendo la información mostrada en el Cuadro 8.8.2.8-1.

Cuadro 8.8.2.8-1 – Información del mensaje de petición de recuperación de clave MAF

Parámetro	Descripción	Multiplicidad
RelativeKeyID	La parte correspondiente del identificador de la clave recibido del cliente MAF de origen en una función de seguridad	1

La MAF debe procesar la petición. Si se encuentran errores, la MAF debe enviar un mensaje de error. En caso de que la petición se procese con éxito, la MAF debe identificar el registro de la clave utilizando el *RelativeKeyID*.

La MAF debe determinar si el cliente MAF de destino está autorizado a recuperar la clave registrada y los metadatos comparando el identificador autentificado del cliente MAF de destino con la lista de los identificadores de los clientes MAF de destino autorizados. Si el cliente MAF de destino no está autorizado, la MAF enviará al cliente MAF de destino un mensaje de error. En caso contrario, la MAF pasará al siguiente paso.

La MAF debe enviar una respuesta, al cliente MAF de destino, incluyendo la información indicada en el Cuadro 8.8.2.8-2.

Cuadro 8.8.2.8-2 – Información del mensaje de respuesta al registro de clave MAF

Parámetro	Descripción	Multiplicidad
expirationTime	Plazo de caducidad del registro de la clave.	1
Source MAF Client ID	Identificador del cliente MAF de origen.	1
labels	Etiquetas para ayudar a localizar el registro de la clave.	0..1
adminFQDN	Identificador de la parte administradora interesada.	1
SUID	El identificador de uso de seguridad que limita las funciones de seguridad en las que se puede utilizar la clave simétrica.	
Key Value	El valor registrado de la clave simétrica de salida.	1

El cliente MAF de destino debe asociar los parámetros con el identificador de clave.

8.8.2.9 Procedimiento de actualización de registro de clave MAF

Finalidad: Este procedimiento permite a un cliente MAF de origen actualizar los metadatos asociados con una clave registrada.

Este procedimiento se realiza entre el cliente MAF de origen y la MAF.

Condiciones previas: El cliente MAF ha realizado previamente el procedimiento de registro de la clave MAF para crear el registro de la clave.

El registro de la clave no ha caducado.

Descripción del procedimiento. El procedimiento incluye los siguientes pasos:

El cliente MAF debe establecer una conexión TLS (o DTLS) con la MAF como se describe en el paso 1 de la cláusula 8.8.2.7.

El cliente MAF de origen debe elaborar una lista de clientes MAF de destino a los que la MAF está autorizada a proporcionar la Kc:

En el caso de la SAEF basada en la MAF o la ESPrim basada en la MAF: La lista deberá contener exactamente un AE-ID absoluto o un CSE-ID absoluto.

En el caso de la ESData basada en la MAF: La lista deberá contener cualquier número no nulo de AE-ID absolutos o CSE-ID absolutos.

NOTA 1 – La presente especificación no proporciona la forma en que el cliente MAF de origen selecciona la lista de clientes MAF de destino.

El cliente MAF de origen debe enviar una petición de actualización de registro de clave MAF, incluyendo la información indicada en el Cuadro 8.8.2.9-1.

Cuadro 8.8.2.9-1 – Información del mensaje de petición de actualización de registro de clave MAF

Parámetro	Descripción	Multiplicidad
MAF-FQDN	FQDN de la MAF, de la configuración de instrucciones de la MAF	1
RelativeKeyID	La parte correspondiente del identificador de la clave asociada con el registro de la clave	1
expirationTime	Plazo de caducidad propuesto del registro de la clave	0..1
labels	Etiquetas propuestas para ayudar a localizar el registro de la clave	0..1

Cuadro 8.8.2.9-1 – Información del mensaje de petición de actualización de registro de clave MAF

Parámetro	Descripción	Multiplicidad
targetIDs	(Opcional) lista propuesta de identificadores del conjunto inicial de clientes MAF de destino autorizados a recuperar la clave simétrica.	0..1
NOTA – Se debe proporcionar al menos uno entre los parámetros expirationTime, labels (etiquetas) o targetID (ID de destino)		

La MAF debe procesar la petición. Si se encuentran errores, la MAF debe enviar la respuesta adecuada de error. En caso de que la petición se procese con éxito, la MAF debe actualizar los metadatos con los valores propuestos si le autoriza la parte administradora interesada. La MAF puede asignar diferentes valores para los parámetros recibidos del cliente MAF, en base a instrucciones de la parte administradora interesada.

La MAF debe enviar una respuesta, al cliente MAF de origen, incluyendo la información indicada en el Cuadro 8.8.2.9-2.

Cuadro 8.8.2.9-2 – Información del mensaje de respuesta a la actualización de registro de clave MAF

Parámetro	Descripción	Multiplicidad
expirationTime	Plazo actual de caducidad del registro de clave, en el caso de que haya cambiado desde la última vez que se proporcionó dicha caducidad al cliente MAF.	0..1
labels	Lista actualizada de etiquetas para ayudar a localizar el registro de clave, en caso de necesidad.	0..1
targetIDs	Lista actual de identificadores del conjunto inicial de clientes MAF de destino autorizados a recuperar la clave simétrica. Dicha lista puede haber sufrido modificaciones con respecto a la lista proporcionada por el cliente MAF.	0..1
NOTA – La respuesta solo incluye los parámetros que estaban presentes en la petición correspondiente.		

8.8.2.10 Procedimiento de supresión de registro de clave MAF

Finalidad: Este procedimiento permite a un cliente MAF de origen solicitar a la MAF que deje de distribuir la clave registrada.

Este procedimiento se realiza entre el cliente MAF de origen y la MAF.

Condiciones previas: El cliente MAF ha realizado previamente el procedimiento de registro de clave MAF para crear el registro de clave.

El registro de clave no ha caducado.

Descripción del procedimiento. El procedimiento incluye los siguientes pasos:

El cliente MAF debe establecer una conexión TLS (o DTLS) con la MAF como se describe en la cláusula 8.8.2.7.

El cliente MAF debe enviar la petición de supresión de registro de clave MAF incluyendo la información indicada en el Cuadro 8.8.2.10-1.

Cuadro 8.8.2.10-1 – Información del mensaje de petición de supresión de registro de clave MAF

Parámetro	Descripción	Multiplicidad
MAF-FQDN	FQDN de la MAF, de la configuración de instrucciones de la MAF	1
RelativeKeyID	La parte correspondiente del identificador de la clave asociada con el registro de la clave	1

Al recibir la petición, la MAF debe procesarla. Si se encuentran errores, la MAF debe enviar un mensaje de error. En caso de que la petición se procese con éxito, la MAF debe eliminar la información asociada con el registro de la clave identificada.

La MAF debe elaborar una respuesta de supresión del registro de cliente MAF indicando el éxito de la operación. La MEF debe enviar la respuesta al cliente MAF.

8.8.3 Detalles de la configuración de clientes MAF

8.8.3.1 Configuración de las credenciales de cliente MAF

Los clientes MAF y la MAF deben configurarse con credenciales para su autentificación mutua.

Las credenciales para la autentificación mutua deben provisionarse previamente o provisionarse a distancia a través de los marcos de provisión de seguridad a distancia. Pueden provisionarse credenciales de clave simétrica o credenciales de certificado. Las credenciales de clave simétrica pueden utilizarse para la autentificación de algunos de los clientes MAF y las credenciales de certificado pueden utilizarse para la autentificación de los otros clientes MAF. La elección puede basarse en las capacidades del cliente MAF.

Los detalles dependen del tipo de credencial (claves simétricas o certificados) y, en el caso de las claves simétricas, del tipo de provisión (provisión previa o provisión a distancia).

Detalles específicos de la **provisión previa de claves simétricas (PPSK)**: la credencial maestra (Km) y su correspondiente identificador de credencial maestra (KmID) deben proporcionarse al cliente MAF (en su papel de inscrito) y a la MAF. El formato del KmID se define en la cláusula 10.6 "Formato del KmID".

Detalles específicos de la **provisión a distancia de claves simétricas (RPSK)**: Se deberá dotar al cliente MAF y a una función de inscripción M2M (MEF) de credenciales para la realización de un marco de provisión de seguridad a distancia (RSPF). El cliente MAF debe estar autorizado a utilizar los servicios de la MEF. Para más detalles, véase la cláusula 8.3.

NOTA 1 – En este caso, la credencial maestra (Km) y el identificador de credencial maestra (KmID) se establecen durante el procedimiento de registro de cliente MAF.

Detalles específicos de los **certificados (provisionados previamente o provisionados a distancia)**: Se debe provisionar al cliente MAF con un certificado de cliente MAF con una cadena de certificados opcional. El certificado de cliente MAF debe ser un certificado de dispositivo, un certificado de AE-ID o un certificado de CSE-ID.

NOTA 2 – La configuración de los certificados CA del ancla de confianza se aborda en la configuración del registro de cliente MAF, y puede producirse independientemente de la configuración de las credenciales del cliente MAF.

La especificación de la configuración de dispositivos oneM2M [UIT-T Y.4500.22] proporciona un conjunto de <*mgmtObj*> especializados que deben utilizarse para la configuración de credenciales de cliente MAF cuando el cliente MAF soporta la gestión de los dispositivos (ya sea a distancia o manualmente). Esta Recomendación no especifica cómo se representa la configuración de credenciales del cliente MAF cuando éste no soporta la gestión de dispositivos.

8.8.3.2 Detalles de la configuración de registro de cliente MAF

Finalidad: La configuración de registro de cliente MAF describe la información provisionada en un cliente MAF para permitirle realizar procedimientos de la MAF autorizados por una parte administradora interesada. La parte administradora interesada se encarga de que la configuración de registro de cliente MAF se proporcione al cliente MAF.

Condiciones previas: El cliente MAF y la MAF se han configurado con credenciales que pueden utilizarse para una autentificación mutua: véase la configuración de credenciales del cliente MAF en la cláusula 8.8.3.1.

Si tanto el cliente MAF como la MAF van a utilizar certificados para la autentificación mutua, entonces:

– La parte administradora interesada (u otra parte que actúe en nombre de la parte administradora interesada) posee una copia de la información del certificado de cliente MAF, como se define en la cláusula 8.1.2.4. La MAF recibe una copia de la información del certificado de cliente MAF. En esta Recomendación no se especifica cómo la parte administradora interesada (u otra parte interesada que actúe en nombre de la parte administradora interesada) proporciona esta información a la MAF.

– La parte administradora interesada (u otra parte que actúe en nombre de la parte administradora interesada) dispone de una copia de los certificados de CA del ancla de confianza de la MAF. El cliente MAF recibe una copia de los certificados de CA del ancla de confianza de la MAF.

La parte administradora interesada se encarga de que la MAF permita al cliente MAF realizar el registro de cliente MAF. Esta acción puede suponer una autorización previa o una autorización en tiempo real.

Detalles: La configuración del registro de cliente MAF (*mafClientRegCfg*) incluye la información indicada en el Cuadro 8.8.3.2-1, y tiene el tipo de datos sec:ClientRegCfg (véase la cláusula 12.4.2.

Cuadro 8.8.3.2-1 – Información de la configuración del registro de cliente MAF

Nombre del elemento	Multiplicidad	Notas
expirationTime	0..1	Plazo de caducidad de la configuración
labels	0..1	Lista de etiquetas para facilitar la localización del registro de cliente MAF
fqdn	1	MAF-FQDN (también denominado MAF-ID)
adminFQDN	1	FQDN de la parte administradora interesada
httpPort	0..1	Número de puerto cuando se utiliza HTTP [b- IETF RFC 7730]
coapPort	0..1	Número de puerto cuando se utiliza CoAP [b-IETF RFC 7252]
websocketPort	0..1	Número de puerto cuando se utiliza WebSocket [b-IETF RFC 6455]

8.8.3.3 Detalles de la configuración del registro de clave MAF

Finalidad: La configuración del registro de clave MAF describe la información provisionada en un cliente MAF para permitirle realizar procedimientos de la MAF autorizados por una parte administradora interesada. La parte administradora interesada se encarga de que la configuración de registro de cliente MAF se proporcione al cliente MAF.

Condiciones previas: El cliente MAF ha realizado el procedimiento de registro de cliente MAF con la MAF para la parte administradora interesada.

El cliente MAF tiene en ese momento credenciales válidas para la autentificación mutua con la MAF.

Detalles: La configuración del registro de clave MAF (*mafKeyRegCfg*) incluye la información indicada en el Cuadro 8.8.3.3-1, y tiene el tipo de datos sec:keyRegCfg (véase la cláusula 12.4.3).

Cuadro 8.8.3.3-1 – Información de la configuración del registro de clave MAF

Nombre del elemento	Multiplicidad	Notas
expirationTime	0..1	Plazo de caducidad
labels	0..1	Lista de etiquetas para facilitar la localización del registro de la clave
adminFQDN	1	FQDN de la parte administradora interesada
SUID	1	SUID que limita el uso del valor de la clave establecido durante el procedimiento de registro de la clave MAF.
targetIDs	0..1	Lista de los identificadores de los clientes MAF autorizados

9 Procedimientos y parámetros de los marcos de seguridad

9.0 Introducción

En esta cláusula se especifican los procedimientos y los parámetros de las fases de los marcos de establecimiento de asociaciones de seguridad (cláusula 8.2) y de los marcos de provisión de seguridad a distancia (cláusula 8.3).

9.1 Procedimientos y parámetros del marco de establecimiento de asociaciones de seguridad

9.1.1 Parámetros de configuración de las credenciales

9.1.1.0 Introducción

En la presente cláusula se describen los siguientes procedimientos de configuración de credenciales:

configuración de las credenciales de la Entidad A y la Entidad B, véase la cláusula 9.1.1.1.

configuración de las credenciales de las funciones de autentificación M2M, véase la cláusula 9.1.1.2.

9.1.1.1 Configuración de las credenciales de la Entidad A y la Entidad B

En el Cuadro 9.1.1.1-1 se recogen los parámetros que pueden configurarse en la Entidad A durante la fase de configuración de las credenciales y que son comunes a todos los marcos de establecimiento de asociaciones de seguridad.

Cuadro 9.1.1.1-1 – los parámetros que pueden configurarse en la Entidad A durante la fase de configuración de las credenciales y que son comunes a todos los marcos de establecimiento de asociaciones de seguridad

Parámetros comunes a todos los marcos de establecimiento de asociaciones de seguridad
(Si la Entidad A es una CSE) CSE-ID de la entidad A

En el Cuadro 9.1.1.1-2 se recogen los parámetros que pueden configurarse en los extremos de una asociación de seguridad en el dominio del campo durante la fase de configuración de las credenciales y que son específicos de un marco de establecimiento de asociaciones de seguridad.

Cuadro 9.1.1.1-2 – Parámetros configurados en los extremos de una asociación de seguridad en el dominio del campo durante la fase de configuración de las credenciales y que son específicos de un marco de establecimiento de asociaciones de seguridad

Marco de establecimiento de una asociación de seguridad		Parámetro
Clave simétrica provisionada		Kpsa
		KpsaID
Basado en certificados	La entidad se autentifica utilizando un certificado de clave pública bruta	Clave privada de la entidad
		Certificado de clave pública bruta de la entidad
	La entidad se autentifica utilizando un certificado de dispositivo	Clave privada de la entidad
		Certificado y cadena de la entidad
	La entidad se autentifica utilizando un certificado de CSE-ID	CSE-ID de la entidad
		Clave privada de la entidad
		Certificado y cadena de la entidad
	La entidad se autentifica utilizando un certificado de AE-ID	AE-ID de la entidad
		Clave privada de la entidad
		Certificado y cadena de la entidad
Basado en una MAF	Entidad A	Identificador de la MAF (MAF-ID)
		Credencial maestra (KmID)
		Identificador de la credencial maestra (KmID)
	Entidad B	La entidad B y la MAF deben poder establecer una comunicación segura mutuamente autentificada. En esta Recomendación no se especifican los detalles

La configuración de las credenciales de la Entidad A y de la Entidad B para el marco de establecimiento de una asociación de seguridad de clave simétrica provisionada, o el marco de establecimiento de una asociación de seguridad basado en una MAF se consigue mediante una de las dos soluciones siguientes:

Una provisión previa a través de mecanismos no especificados en esta Recomendación.

Una provisión a distancia a través de uno de los marcos de provisión de seguridad a distancia de la cláusula 8.3.

La configuración de las credenciales de la Entidad A y la Entidad B para el marco de establecimiento de una asociación de seguridad con certificados se realiza mediante la provisión previa a través de mecanismos que no se especifican en esta Recomendación.

9.1.1.2 Configuración de las credenciales de las funciones de autentificación M2M

El Cuadro 9.1.1.2-1 recoge los parámetros configurados para las funciones de autentificación M2M en la fase de configuración de la credencial. Se supone que el identificador de la función de autentificación M2M (MAF-ID) ha sido configurado antes de la fase de configuración de las credenciales.

Cuadro 9.1.1.2-1 – Parámetros configurados para las funciones de autentificación M2M en la fase de configuración de las credenciales

Marco de establecimiento de una asociación de seguridad		Parámetro
Basado en una MAF	Autentificación de A en la MAF	Credencial maestra (Km)
		Identificador de la credencial maestra (KmID)
	Autentificación de B en la MAF	La entidad B y la MAF deben poder establecer una comunicación segura mutuamente autentificada. En esta Recomendación no se especifican los detalles

La configuración de las credenciales del marco de autentificación M2M debe realizarse mediante: las aplicaciones de negocio de la parte interesada que opera la función de autentificación M2M, y cuyos detalles no se describen en esta Recomendación.

La provisión a distancia a través de uno de los marcos de provisión de seguridad a distancia de la cláusula 8.3.

9.1.2 Procedimientos y parámetros de configuración de las asociaciones

9.1.2.0 Introducción

En esta cláusula se describen los siguientes procedimientos de configuración de asociaciones:

Configuración de una asociación de la entidad A, en la cláusula 9.1.2.1.1.

Configuración de una asociación de la entidad B, en la cláusula 9.1.2.1.2.

Configuración de una asociación de las funciones de autentificación M2M, en la cláusula 9.1.2.2.

9.1.2.1 Configuración de una asociación de la entidad A y la entidad B

9.1.2.1.1 Configuración de una asociación de la entidad A

En el Cuadro 9.1.2.1.1-1 figuran los parámetros configurados en la entidad A en la fase de configuración de la asociación y que son comunes a todos los marcos de establecimiento de una asociación de seguridad.

Cuadro 9.1.2.1.1-1 – Parámetros configurados en la entidad A en la fase de configuración de la asociación y que son comunes a todos los marcos de establecimiento de una asociación de seguridad

Parámetros comunes a todos los marcos de establecimiento de una asociación de seguridad
CSE-ID de la entidad B

En el Cuadro 9.1.2.1.1-2 figuran los parámetros configurados en la entidad A en la fase de configuración de la asociación y que son específicos del marco de establecimiento de una asociación de seguridad.

Cuadro 9.1.2.1.1-2 – Parámetros configurados en la entidad A en la fase de configuración de la asociación y que son específicos del marco de establecimiento de una asociación de seguridad

Marco de establecimiento de una asociación de seguridad		Parámetros específicos del marco de establecimiento de una asociación de seguridad
Clave simétrica provisionada		Ninguno
Basado en certificados	La entidad B se autentifica utilizando un certificado de clave pública bruta	Identificador de la clave pública de la entidad B
	La entidad B se autentifica utilizando un certificado de dispositivo	Identificador exclusivo del hardware de la entidad B
		Información del ancla de confianza de la entidad B
	La entidad B se autentifica utilizando un certificado de CSE-ID	Información del ancla de confianza de la entidad B
	La entidad B se autentifica utilizando un certificado de AE-ID	Información del ancla de confianza de la entidad B
Basado en una MAF		Ninguno

Los mecanismos de configuración de la asociación de la entidad A deben autentificar el origen de la configuración y proporcionar protección de la integridad de la información configurada transmitida a la entidad desde el origen de la configuración.

9.1.2.1.2 Configuración de una asociación de la entidad B

En el Cuadro 9.1.2.1.2-1 se indican los parámetros configurados en el registrador (entidad B) en la fase de configuración de la asociación.

Cuadro 9.1.2.1.2-1 – Parámetros configurados en la entidad B en la fase de configuración de la asociación

Marco de establecimiento de una asociación de seguridad		Parámetros específicos del marco de establecimiento de una asociación de seguridad
Clave simétrica provisionada		Ninguno
Basado en certificados	La entidad B se autentifica utilizando un certificado de clave pública bruta	Ninguno
	La entidad B se autentifica utilizando un certificado de dispositivo, un certificado de CSE-ID o un certificado de AE-ID	Información del ancla de confianza de la entidad A
Basado en una MAF		Ninguno

Los mecanismos de configuración de la asociación de la entidad B debe autentificar el origen de la configuración y proporcionar protección de la integridad de la información configurada transmitida a la entidad desde el origen de la configuración

9.1.2.2 Configuración de una asociación de las funciones de autentificación M2M

En el Cuadro 9.1.2.2-1 se indican los parámetros configurados en las funciones de autentificación M2M en la fase de configuración de la asociación.

Cuadro 9.1.2.2-1 – Parámetros configurados en las funciones de autentificación M2M en la fase de configuración de la asociación

Marco de establecimiento de una asociación de seguridad		Parámetro
Basado en una MAF	Autentificación de A en la MAF	CSE-ID o AE-ID de la entidad B(IdB)

En esta Recomendación se asume que la configuración de la asociación de las funciones de autentificación M2M utilizará la función lógica de negocio de la parte interesada que opera la función de autentificación M2M, y los detalles no se describen en la Recomendación.

9.2 Procedimientos y parámetros del marco de provisión de seguridad a distancia

9.2.1 Procedimientos y parámetros de configuración de las credenciales de inicialización

9.2.1.0 Introducción

En esta cláusula se describen los siguientes procedimientos de configuración de credenciales de inicialización:

Configuración de las credenciales de inicialización de los inscritos y de los objetivos de inscripción (excepto para el caso basado en la GBA, como se indica a continuación), véase la cláusula 9.2.1.1.

Configuración de las credenciales de inicialización de las funciones de inscripción M2M (excepto en el caso basado en GBA, como se indica a continuación), véase la cláusula 9.2.1.2.

Los siguientes procedimientos de configuración de credenciales de inicialización están especificados por otras organizaciones:

Configuración de las credenciales de inicialización de los servidores de autentificación del proveedor de servicios de red subyacente (por ejemplo, HLR, HSS o AAA) para el marco de establecimiento de una asociación de seguridad basada en GBA. Estos detalles se especifican en las normas 3GPP TS 33.220 [ETSI TS 133 220] y 3GPP2 S.S0109-A [TIA-1098-A].

Configuración de las credenciales de inicialización de los inscritos para el marco de establecimiento de una asociación de seguridad basada en GBA. Estos detalles se especifican en las normas 3GPP TS 33.220 [ETSI TS 133 220] y 3GPP2 S.S0109-A [TIA-1098-A].

9.2.1.1 Configuración de las credenciales de inicialización de los inscritos

En el Cuadro 9.2.1.1-1 se indican los parámetros configurados en los inscritos en la fase de configuración de las credenciales de inicialización para la autentificación con la función de inscripción M2M en el marco de provisión de seguridad a distancia con clave simétrica provisionada previamente y en el marco de provisión de seguridad a distancia basado en certificados.

Cuadro 9.2.1.1-1 – Parámetros configurados en los inscritos en la fase de configuración de las credenciales de inicialización

Marco de provisión de seguridad a distancia	Parámetro
Autentificación con la clave de conexión segura M2M provisionada previamente. No es aplicable a una MAF.	Kpm
	KpmID
	URI de la MEF

Cuadro 9.2.1.1-1 – Parámetros configurados en los inscritos en la fase de configuración de las credenciales de inicialización

Marco de provisión de seguridad a distancia		Parámetro
Autentificación basada en certificados	El inscrito se autentifica utilizando un certificado de clave pública bruta	Clave privada del inscrito
		Certificado de clave pública bruta del inscrito
	El inscrito se autentifica utilizando un certificado de dispositivo	Clave privada del inscrito
		Certificado y cadena del inscrito
	El inscrito se autentifica utilizando un certificado de CSE-ID o un certificado de AE-ID	Clave privada del inscrito
		Certificado y cadena del inscrito

La configuración de credenciales de inicialización de un inscrito para el marco de provisión de seguridad a distancia de clave simétrica provisionada previamente y el marco de provisión de seguridad a distancia basado en certificados debe autentificar la fuente de la configuración y proporcionar confidencialidad y protección de la integridad a la información configurada transmitida al entorno seguro del inscrito desde el origen de la configuración. En la presente Recomendación no se especifica ningún mecanismo de este tipo.

La configuración de las credenciales de inicialización de un objetivo de inscripción del dominio de la infraestructura (incluida una función de autentificación M2M) debería utilizar la función lógica de negocio de la parte interesada que gestiona la inscripción en el dominio de la infraestructura, y sus detalles no se describen en esta Recomendación.

9.2.1.2 Configuración de credenciales de inicialización de las funciones de inscripción M2M

Se supone que una función de inscripción M2M ya conoce su FQDN.

En el Cuadro 9.2.1.2-1 se indican los parámetros configurados en las funciones de inscripción M2M en la fase de configuración de credenciales de inicialización para la autentificación mutua con los inscritos y los objetivos de inscripción utilizando el marco de provisión de seguridad a distancia con claves simétricas de inscritos provisionadas previamente y el marco de provisión de seguridad a distancia basado en certificados.

Cuadro 9.2.1.2-1 – parámetros configurados en las funciones de inscripción M2M en la fase de configuración de credenciales de inicialización para la autentificación mutua con los inscritos y los objetivos de inscripción utilizando el marco de provisión de seguridad a distancia con claves simétricas de inscritos provisionadas previamente y el marco de provisión de seguridad a distancia basado en certificados

Marco de provisión de seguridad a distancia	Parámetros específicos de los marcos de provisión de seguridad a distancia
Autentificación con clave de inscripción simétrica provisionada previamente del inscrito o del objetivo de inscripción	Kpm
	KpmID
Autentificación basada en certificados del inscrito o del objetivo de inscripción	Clave privada de la MEF
	Certificado y cadena de la MEF

Se supone que la configuración de las credenciales de inicialización de las funciones de inscripción M2M debería utilizar la función lógica de negocio de la parte interesada que opera la función de inscripción M2M, y los detalles no se describen en esta Recomendación.

9.2.2 Procedimientos y parámetros de configuración de las instrucciones de inicialización

9.2.2.0 Introducción

En esta cláusula se describen los siguientes procedimientos de configuración de las instrucciones de inicialización:

Configuración de las instrucciones de inicialización de los inscritos, en la cláusula 9.2.2.1.

Configuración de las instrucciones de inicialización de las funciones de inscripción M2M, en la cláusula 9.2.2.3.

Configuración de las instrucciones de inicialización de los servidores de autentificación del proveedor de servicio de la red subyacente (por ejemplo, HLR, HSS o AAA), en la cláusula 9.2.2.4.

9.2.2.1 Configuración de las instrucciones de inicialización de los inscritos

En el Cuadro 9.2.2.1-1 se indican los parámetros configurados en un inscrito durante la fase de configuración de las instrucciones de inicialización que son comunes a todos los marcos de provisión de seguridad a distancia.

Cuadro 9.2.2.1-1 – Parámetros configurados en un inscrito durante la fase de configuración de las instrucciones de inicialización que son comunes a todos los marcos de provisión de seguridad a distancia

Parámetros comunes a todos los marcos de provisión de seguridad a distancia
Identificador del objetivo de inscripción (AE-ID o CSE-ID del inscrito B, o MAF-ID)

En el Cuadro 9.2.2.1-2 se indican los parámetros específicos del marco de provisión de seguridad a distancia que se configuran en un inscrito en la fase de configuración de las instrucciones de inicialización del marco de provisión de seguridad a distancia.

Cuadro 9.2.2.1-2 – Marco de provisión de seguridad a distancia – Parámetros específicos que se configuran en un inscrito en la fase de configuración de las instrucciones de inicialización del marco de provisión de seguridad a distancia

Marco de provisión de seguridad a distancia	Marco de provisión de seguridad a distancia – parámetros específicos
Clave de inscripción simétrica provisionada previamente	Caducidad de la inscripción
Basado en certificados	URI de la MEF
	Información del ancla de confianza de la MEF
Basado en GBA	Ninguno

Los mecanismos de configuración de las instrucciones de inicialización de los inscritos deben autentificar el origen de la configuración y proporcionar al menos protección de la integridad de la información configurada transmitida desde el origen de la configuración al inscrito.

9.2.2.2 Este párrafo se deja deliberadamente en blanco.

9.2.2.3 Configuración de las instrucciones de inicialización de las funciones de inscripción M2M

En el Cuadro 9.2.2.3-1 se indican los parámetros configurados en una función de inscripción M2M durante la fase de configuración de las instrucciones de inicialización, que son comunes al marco de provisión de seguridad a distancia con clave simétrica de inscrito y al marco de provisión de seguridad a distancia basado en certificados.

Cuadro 9.2.2.3-1 – Parámetros configurados en una función de inscripción M2M durante la fase de configuración de las instrucciones de inicialización, que son comunes al marco de provisión de seguridad a distancia con clave simétrica de inscrito y al marco de provisión de seguridad a distancia basado en certificados

Parámetros comunes a todos los marcos de provisión de seguridad a distancia
Identificador del objetivo de inscripción (CSE-ID o AE-ID del inscrito B, o MAF-ID)

En el Cuadro 9.2.2.3-2 se indican los parámetros específicos del marco de provisión de seguridad a distancia que se configuran en las funciones de inscripción M2M durante la fase de configuración de las instrucciones de inicialización del marco de provisión de seguridad a distancia con clave simétrica provisionada previamente y del marco de provisión de seguridad a distancia basado en certificados.

Cuadro 9.2.2.3-2 – Parámetros específicos del marco de provisión de seguridad a distancia que se configuran en las funciones de inscripción M2M durante la fase de configuración de las instrucciones de inicialización del marco de provisión de seguridad a distancia con clave simétrica provisionada previamente y del marco de provisión de seguridad a distancia basado en certificados

<table>
<tr><th colspan="2">Marco de provisión de seguridad a distancia</th><th>Parámetros específicos del marco de provisión de seguridad a distancia</th></tr>
<tr><td colspan="2">Clave de inscripción simétrica provisionada previamente</td><td>Caducidad de la inscripción</td></tr>
<tr><td rowspan="4">Basado en certificados</td><td>El inscrito se autentifica utilizando un certificado de clave pública bruta</td><td>Identificador de la clave pública del inscrito</td></tr>
<tr><td rowspan="2">El inscrito se autentifica utilizando un certificado de dispositivo</td><td>ID del dispositivo M2M del inscrito</td></tr>
<tr><td>Información del ancla de confianza del inscrito</td></tr>
<tr><td>El inscrito se autentifica utilizando un certificado de CSE-ID o un certificado de AE-ID</td><td>Información del ancla de confianza del inscrito</td></tr>
</table>

En esta Recomendación se asume que la configuración de las instrucciones de inicialización de las funciones de inscripción M2M utiliza la función lógica de negocio de la parte interesada que opera la función de inscripción M2M, y los detalles no se describen en la Recomendación.

9.2.2.4 Configuración de las instrucciones de inicialización de los servidores de autentificación del proveedor de servicio de la red subyacente

En el Cuadro 9.2.2.4-1 se indican los parámetros configurados en un servidor de autentificación de un proveedor de servicios de red subyacente (por ejemplo, HLR, HSS o AAA) durante la fase de

configuración de las instrucciones de inicialización del marco de provisión de seguridad a distancia basado en GBA.

Cuadro 9.2.2.4-1 – Parámetros que se configuran en las funciones de inscripción M2M durante la fase de configuración de las instrucciones de inicialización del marco de provisión de seguridad a distancia basado en GBA

Parámetro	Obligatorio/Opcional para todos los marcos de provisión de seguridad a distancia
Identificador del objetivo de inscripción (CSE-ID o AE-ID del inscrito B, o MAF-ID)	Obligatorio

La configuración de las instrucciones de inicialización del servidor de autentificación del proveedor de servicios de la red subyacente se efectúa mediante la actualización de la configuración de seguridad de los usuarios GBA (GUSS) (3GPP TS 33.220 [ETSI TS 133 220]) del equipo de usuario (UE) en el cual se realiza la inscripción. Esta Recomendación asume que esta configuración de las instrucciones de inicialización utiliza la función lógica de negocio del proveedor de servicios de la red subyacente, y los detalles no se describen en la Recomendación.

9.2.3 Procedimientos y parámetros de la configuración de las credenciales de extremo a extremo

9.2.3.0 Introducción

En esta cláusula se describen los siguientes procedimientos de configuración de credenciales de extremo a extremo:

Configuración de las credenciales de extremo a extremo de los extremos de origen y de los extremos de destino de la ESF, en la cláusula 9.2.3.1.

Configuración de las credenciales de extremo a extremo de las funciones habilitadoras de confianza, en la cláusula 9.2.3.2.

Parámetros de configuración para habilitar la seguridad de extremo a extremo en los extremos de origen y los extremos de destino de la ESF, véase la cláusula 9.2.3.3.

9.2.3.1 Configuración de las credenciales de extremo a extremo de los extremos de origen y los extremos de destino de la ESF

Se supone que el extremo de origen de la ESF y los extremos de destino de la ESF están configurados con el URI de la función habilitadora de confianza y han sido configurados con los parámetros apropiados, específicos de los marcos de provisión de seguridad a distancia, como se describe en la cláusula 9.2. Además, se provisionan las credenciales de extremo a extremo y se suministran los parámetros de seguridad adecuados en los extremos de destino de la ESF, mientras que el extremo de origen de la ESF puede determinar las credenciales de extremo a extremo por sí mismo utilizando los parámetros de seguridad pertinentes provisionados. El Cuadro 9.2.3.1-1 ofrece una lista de los parámetros.

Cuadro 9.2.3.1-1 – Credenciales y parámetros de seguridad provisionados en los extremos de destino y de origen de la ESF

Protección de seguridad	Parámetros del marco de provisión de seguridad de extremo a extremo	Descripción
Credenciales de seguridad de extremo a extremo	KpsaID	Identificador de la credencial provisionada para la clave simétrica M2M provisionada.
	Kpsa	Clave simétrica M2M provisionada. Se utiliza para determinar el secreto maestro de extremo a extremo, Ke2e_master, como se describe en la cláusula 10.3.6.
	URI de la TEF	URI de la entidad de un tercero de confianza (TEF) que se utiliza como generador/registro de credenciales y permite el registro y la generación de credenciales de seguridad de extremo a extremo.
Parámetros de encriptación	Sal	Sal utilizada para generar las credenciales de extremo a extremo. Parámetro opcional.
	Algoritmo de extracción de claves: HMAC-Hash	El algoritmo de extracción de claves que se utiliza para generar las distintas claves debe seguir los mecanismos descritos en [IETF RFC 5869].
	Etiquetas de encriptación	Etiquetas utilizadas por los algoritmos de encriptación. Las etiquetas se deben utilizar de acuerdo con la cláusula 10.3.6.1.
Tipos de credenciales	Autenticidad del mensaje (primitiva)	Clave utilizada para la autentificación de los mensajes y la integridad de las primitivas oneM2M. Si se proporcionan los elementos de generación de claves, el extremo de destino de la ESF la genera.
	Confidencialidad del mensaje (primitiva)	Clave utilizada para la confidencialidad de los mensajes de las primitivas oneM2M. Si se proporcionan los elementos de generación de claves, el extremo de destino de la ESF la genera.
	Integridad de los datos (atributo)	Clave utilizada para proporcionar la integridad de los datos/atributos. Si se proporcionan los elementos de generación de claves, el extremo de destino de la ESF la genera.
	Confidencialidad de los datos (atributo)	Clave utilizada para proporcionar la confidencialidad de los datos/atributos. Si se proporcionan los elementos de generación de claves, el extremo de destino de la ESF la genera.

9.2.3.2 Configuración de las credenciales de extremo a extremo en las funciones habilitadoras de confianza M2M

Se supone que la función habilitadora de confianza está configurada con las identidades de las entidades (extremos de origen y destino de la ESF) y los parámetros adecuados específicos de los marcos de provisión de seguridad a distancia, tal como se describe en la cláusula 9.2.

Además, se provisiona la función habilitadora de confianza con los parámetros de seguridad adecuados, de modo que se puedan determinar las credenciales de seguridad de extremo a extremo y se pueda provisionar el conjunto de parámetros de encriptación en los extremos de destino de la ESF

una vez que se hayan autenticado dichos extremos. En el Cuadro 9.2.3.2-1 se muestra la lista de los parámetros.

Cuadro 9.2.3.2-1 – Parámetros de seguridad provisionados en la función de inscripción M2M o la función de habilitación de confianza y los extremos de destino de la ESF

Protección de seguridad de extremo a extremo	Parámetros del marco de provisión de seguridad de extremo a extremo	Descripción
Credenciales de seguridad de extremo a extremo	Kpm	Credenciales provisionadas previamente entre el extremo de origen de ESF y la TEF
	KpmID	Identidad de las credenciales provisionada previamente
	Identidad del extremo de origen de la ESF (AE-ID/CSE-ID) Identidad del extremo de destino de la ESF (CSE-ID)	Identidad de la entidad provisionada previamente con las credenciales de seguridad de extremo a extremo
Lista de las protecciones de seguridad requeridas y su nivel.	Autentificación del mensaje: (baja – alta)	Proporciona el nivel requerido para el mecanismo de autentificación de los mensajes
	Confidencialidad del mensaje: (baja – alta)	Proporciona el nivel requerido para el mecanismo de confidencialidad de los mensajes
	Integridad de los atributos: (baja – alta)	Proporciona el nivel necesario para proporcionar la integridad de los atributos
	Confidencialidad de los atributos: (baja – alta)	Proporciona el nivel necesario para proporcionar la confidencialidad de los atributos

9.2.3.3 Parámetros de configuración para habilitar la seguridad de extremo a extremo en los extremos de origen de la ESF y en los extremos de destino de la ESF

Los extremos de origen de la ESF y los extremos de destino de la ESF se provisionan con los parámetros de encriptación que se utilizan para habilitar y verificar la protección de seguridad de extremo a extremo. En el caso del extremo de destino de la ESF, la función habilitadora de confianza le provisiona los parámetros tras realizar con éxito la autentificación y obtener la clave de conexión segura (Kpsa). En el caso del extremo de origen de la ESF, los parámetros pueden configurarse previamente o provisionarse de manera similar a la del extremo de destino de la ESF, es decir, una vez que se ha obtenido la clave de conexión segura (Kpsa) y se ha compartido entre el extremo de origen de la ESF y el extremo de destino de la ESF. En el Cuadro 9.2.3.3-1 se muestra la lista de los parámetros.

Cuadro 9.2.3.3-1 – Parámetros de seguridad provisionados en el extremo de destino y en el extremo de origen de la ESF

Protección de seguridad de extremo a extremo	Parámetros del marco de provisión de seguridad de extremo a extremo	Descripción
Credenciales de seguridad de extremo a extremo	e2e_master	Credencial maestra de extremo a extremo
	E2EKeyId	Identidad de la credencial maestra de extremo a extremo
	Identidad del extremo de destino de la ESF (CSE-ID) Identidad del extremo de origen de la ESF (AE-ID/CSE-ID)	Identidad de la entidad final a la que se asocia la credencial de extremo a extremo
Parámetros de encriptación	Protocolo: JWS/JWE, XML Sec	Tipo de codificación y representación que se utiliza
	Clase de los algoritmos de encriptación: AEAD (clave única) o no AEAD	Define la clase de algoritmos de encriptación que deben utilizarse
	Algoritmo/tamaño de la autentificación de los mensajes: HMAC-SHA-256, HMAC-SHA-512	Indica el algoritmo de autentificación de los mensajes y el tamaño de la clave
	Algoritmo/tamaño de la confidencialidad de los mensajes: AES-192/256	Indica el algoritmo de confidencialidad de los mensajes y el tamaño de la clave
	Algoritmo de confidencialidad de los atributos: AES-192/256	Algoritmo de confidencialidad de los atributos y tamaño de la clave
	Algoritmo/tamaño de la autenticidad de los atributos: HMAC-SHA-256	Algoritmo de autenticidad e integridad de los atributos y tamaño de la clave
Uso de la encriptación	Autenticidad de los mensajes/atributos: Nonce	Valor aleatorio que se utiliza para proporcionar vigencia. Sólo se almacena temporalmente asociado con un tiempo de caducidad y se comunica al otro extremo
	Confidencialidad de los mensajes/atributos: vector de inicialización	Valor aleatorio que se utiliza como vector de inicialización para el algoritmo de confidencialidad

NOTA – Para los algoritmos de la clase AEAD en los que se utiliza una sola clave, sólo se generaría una única clave e identificaría un algoritmo criptográfico asociado (por ejemplo, AES-GCM o AES-CCM). Además, para los algoritmos de la clase AEAD, no se generará un vector de inicialización (IV) y un Nonce, sino que se generará un único valor aleatorio, el Nonce.

10 Detalles de los protocolos y los algoritmos

10.1 Detalles de un marco de seguridad basado en certificados

10.1.1 Perfiles de los certificados

Las RFC de esta sección que identifican los algoritmos de encriptación se indican sólo a título informativo. No pretenden ser una lista exclusiva o definitiva. No forman parte del contenido normativo de esta Recomendación.

10.1.1.0 General

NOTA – Estos perfiles de certificado cumplen con la especificación CoAP [b-IETF RFC 7252].

10.1.1.1 Detalles comunes de los certificados

Todos los certificados deben cumplir el siguiente perfil:

Los certificados deben cumplir la norma [IETF RFC 5280].

Los certificados deben incluir un SubjectPublicKeyInfo que indique un algoritmo de id-ecPublicKey con namedCurves secp256r1 [IETF RFC 5280]; esta curva es equivalente a la curva P-256 del NIST [NIST EC].

El formato de la clave pública debe ser sin comprimir [IETF RFC 5480].

El algoritmo de hash (troceado) debe ser SHA-256.

Se debe incluir la extensión de la utilización de la clave y debe indicar al menos digitalSignature.

10.1.1.2 Perfil de certificados de una clave pública bruta

Los certificados de clave pública bruta deben ser conformes con la cláusula 10.1.1.1 "Detalles comunes de los certificados" y la norma [IETF RFC 7250].

10.1.1.3 Detalles comunes a los certificados con cadenas de certificados

Los certificados con cadenas de certificados deben ajustarse a la siguiente descripción:

Estos certificados deben ser conformes con la cláusula 10.1.1.1 "Detalles comunes de los certificados".

Los certificados deben estar firmados con ECDSA usando secp256r1, y la firma debe usar SHA-256.

Las cadenas de certificados deben limitar el número de certificados de CA intermedias para evitar que tengan un impacto negativo en los entornos restringidos.

10.1.1.4 Perfil para los certificados de dispositivos y sus cadenas de certificados

10.1.1.4.1 Perfil de los certificados de los dispositivos

Los certificados de los dispositivos deben ajustarse a la siguiente descripción:

Los certificados de dispositivos deben ser conformes con la cláusula 10.1.1.3 "Detalles comunes a los certificados con cadenas de certificados".

La extensión subjectAltName de los certificados de los dispositivos debe incluir uno o más identificadores exclusivos a nivel mundial de equipo de hardware.

EJEMPLO: El Anexo H "Identificador de dispositivo M2M basado en un identificador de objeto" [UIT-T Y.4500.1] define un identificador de dispositivo M2M basado en un identificador de objeto que puede utilizarse para proporcionar uno o más identificadores exclusivos a nivel mundial de equipo de hardware. Un identificador de dispositivo M2M basado en un identificador de objeto puede representarse en un campo otherName en la extensión subjectAltName, donde:

el componente "type-ID" de otherName se fija en el arco del ID de indicación del dispositivo M2M (cláusula H.2.1 "ID de indicación de un dispositivo M2M" [UIT-T Y.4500.1]) del ID de dispositivo M2M del identificador del objeto; y

el componente "value" de otherName se establece con el resto del ID de dispositivo M2M del identificador de objeto: el arco del ID del fabricante, el arco del ID del modelo, el arco del ID del número de serie y el arco del ID expandido opcional (véase el Anexo H.2 "Identificador de dispositivo M2M basado en OID" [UIT-T Y.4500.1]).

NOTA – Proporcionar el ID del modelo como parte del ID del dispositivo M2M puede tener implicaciones de privacidad en algunos escenarios.

10.1.1.4.2 Perfil de los certificados de las autoridades de certificación para los certificados de los dispositivos

Los certificados de las autoridades de certificación incluidos en la cadena de certificación de un certificado de dispositivo deberán ajustarse a la siguiente descripción:

Estos certificados deben ser conformes con la cláusula 10.1.1.3 "Detalles comunes a los certificados con cadenas de certificados".

Se recomienda que los certificados de las autoridades de certificación para los certificados de los dispositivos utilicen la extensión relativa a las restricciones de nombre (véase la cláusula 4.2.1.10 "Restricciones de nombre" de [IETF RFC 5280]) para restringir los identificadores exclusivos a nivel mundial de los equipos de hardware en los siguientes certificados de los dispositivos en una ruta de certificación.

EJEMPLO: Las restricciones de nombre se definen en términos de subárboles de nombres permitidos o excluidos. Los subárboles de un espacio de nombres del ID del dispositivo M2M basado en un identificador de objeto se representan mediante un campo otherName con:

"type-ID" fijado en el arco del ID de indicación de dispositivo M2M (cláusula H.2.1 "ID de indicación de dispositivo M2M" [UIT-T Y.4500.1]) del espacio de nombres aplicable del ID de dispositivo M2M del identificador de objeto; y

"valor" fijado en el resto del identificador del objeto que identifica el subárbol.

10.1.1.5 Perfil de los certificados de los AE-ID y sus cadenas de certificados

Los certificados de los AE-ID y todos los demás certificados de la cadena de certificados correspondiente deben cumplir la cláusula 10.1.1.3 "Detalles comunes a los certificados con cadenas de certificados".

La representación completa del URI del AE-ID debe incluirse en la extensión subjectAltName.

El certificado utilizado para firmar el certificado del AE-ID debe incluir las nameConstraints (restricciones de nombre) satisfechas por la parte del hostname (nombre del anfitrión) de la representación URI completa del AE-ID.

Los certificados de los AE-ID no deben incluir comodines.

10.1.1.6 Perfil de los certificados de los FQDN y sus cadenas de certificados

Los certificados de los FQDN y todos los demás certificados de la cadena de certificados correspondiente deben cumplir la cláusula 10.1.1.3 "Detalles comunes a los certificados con cadenas de certificados".

Un certificado FQDN debe incluir el FQDN de la función de inscripción M2M en cuestión en la extensión subjectAltName.

Los certificados de los FQDN no deben incluir comodines.

10.1.1.7 Perfil de los certificados de los CSE-ID y sus cadenas de certificados

Los certificados de los CSE-ID y todos los demás certificados de la cadena de certificados correspondiente deben cumplir la cláusula 10.1.1.3 "Detalles comunes a los certificados con cadenas de certificados".

La extensión subjectAltName debe incluir la representación del nombre de dominio público del CSE-ID como se define en [UIT-T Y.4500.1].

Los certificados de los CSE-ID no deben incluir comodines.

10.1.1.8 Perfil de los certificados de los Node-ID y sus cadenas de certificados

Los certificados de los Node-ID y todos los demás certificados de la cadena de certificados correspondiente deben cumplir la cláusula 10.1.1.3 "Detalles comunes a los certificados con cadenas de certificados".

La extensión subjectAltName debe incluir el Node-ID como se define en [UIT-T Y.4500.1].

Los certificados de los Node-ID no deben incluir comodines.

10.1.2 Identificadores de claves públicas

El identificador de clave pública para un certificado de clave pública bruta debe calcularse como se describe en la [IETF RFC 7507] y la [IETF RFC 6920] utilizando el algoritmo hash SHA-256. El identificador de clave pública debe generarse utilizando uno de los algoritmos hash sha-256-120, sha-256-128 o sha-256 especificados en [IETF RFC 6920].

Se recomienda que el identificador de la clave pública sea tan largo como resulte práctico dentro de las limitaciones del despliegue.

El identificador de clave pública de confianza (recibido durante la configuración de la asociación o la configuración de las instrucciones de inicialización) se compara con el certificado de clave pública bruta (recibido durante la toma de contacto de seguridad) mediante el siguiente procedimiento:

Se calcula un valor de resumen (digest value) de control de acuerdo con la sección 2 de [IETF RFC 6920] utilizando el algoritmo hash de troceo, identificado en el identificador de clave pública de confianza.

El valor del resumen de control se compara con el valor del resumen encriptado del identificador de clave pública de confianza. Si los valores son idénticos, el certificado de clave pública bruta coincide con el identificador de clave pública de confianza. En caso contrario, el certificado de clave pública bruta no coincide con el identificador de clave pública de confianza.

10.1.3 Requisitos de soporte para cada tipo de certificado de clave pública

En el Cuadro 10.1.3 se indican, para cada uno de los distintos tipos de entidades (CSE del dominio del campo, AE del dominio del campo, IN-CSE, IN-AE, función de autentificación M2M y función de inscripción M2M), el tipo de certificado que puede expedirse para la entidad y el tipo de certificados de otras entidades que la entidad debe poder procesar. En este cuadro, "O" indica que es opcional, "M" indica que es obligatorio, "CA" indica que se requiere dicha opción si la entidad soporta el marco de establecimiento de una asociación de seguridad basado en certificados, "CB" indica que está condicionado a que la entidad soporte el marco de provisión de seguridad a distancia basado en certificados.

Cuadro 10.1.3-1 – Aplicación de los tipos de certificado que puede expedirse para una entidad y tipos de certificados de otras entidades que la entidad debe poder procesar

Entidad	Tipos de certificados que pueden expedirse para una entidad					Tipos de certificados de otras entidades que la entidad debe poder procesar				
	Raw	Device	CSE–ID	AE–ID	FQDN	Raw	Device	CSE–ID	AE–ID	FQDN
CSE del dominio del campo	O	O	O	–	–	CA	CA	CA	CA	CB
AE del dominio del campo	O	O	–	O	–	CA	CA	CA	–	CB
IN–CSE	O	–	O	–	–	CA	CA	CA	CA	–
IN–AE	O	–	–	O	–	CA	–	CA	–	–
MAF	–	–	–	–	M	–	–	–	–	M
MEF	–	–	–	–	M	CB	CB	–	–	M

La autentificación mutua entre los servidores de gestión a distancia y los clientes de la gestión a distancia no se considera en esta Recomendación. Cuando se soporte, la administración de la seguridad a distancia puede utilizarse para provisionar los certificados.

10.1.4 Perfil de las solicitudes de firma de certificado

Una solicitud de firma de certificado (CSR) es un objeto firmado que se proporciona al servidor de provisión de certificados (servidor EST o servidor SCEP) para solicitar la emisión de un certificado. La provisión de certificados, tal y como se especifica en la cláusula 8.3.6, puede utilizarse para emitir un certificado a un Nodo, CSE o AE. La solicitud de firma de certificado incluirá el subjectPublicKeyInfo: la clave pública y el algoritmo con el que se utiliza la clave.

SubjectAltName: este campo debe contener el AE-ID, CSE-ID o Node-ID utilizando el tipo de nombre definido para cada tipo de certificado de las cláusulas 10.1.1.5, 10.1.1.7 y 10.1.1.8.

La solicitud de firma de certificado puede incluir campos adicionales y extensiones proporcionadas por el servidor de provisión de certificados, por ejemplo, utilizando la solicitud de atributos de la solicitud de firma de certificado EST (CSR) descrita en la sección 2.6 de [IETF RFC 7030].

10.2 Detalles sobre el TLS y el DTLS

10.2.1 Versiones del TLS y el DTLS

En los casos en que deban asegurarse cabidas útiles TCP, se utilizará la versión 1.2 del TLS [IETF RFC 5246].

En los casos en que deban asegurarse cabidas útiles UDP, se utilizará la versión 1.2 del DTLS [IETF RFC 6347]; obsérvese que los conjuntos de cifrado del DTLS v1.2 y el TLS v1.2 son idénticos.

Todas las implementaciones han de admitir la indicación del nombre de servidor (SNI) para señalar su autoridad mediante el campo SNI HostName, como se explica en la sección 3 de [IETF RFC 6066]. Esto es necesario para que un anfitrión que haga las veces de servidor virtual para múltiples autoridades, al recibir una nueva conexión TLS o DTLS, sepa qué claves utilizar para la sesión TLS o DTLS.

Los clientes (D)TLS en cualquier nodo y los servidores (D)TLS en nodos maestros (MN) admitirán al menos uno de los conjuntos de cifrado del TLS que se indican en la cláusula 10.2.2, Conjuntos de cifrado TLS y DTLS para marcos de seguridad basados en TLS-PSK, o en la cláusula 10.2.3, Conjuntos de cifrado del TLS y el DTLS para marcos de seguridad basados en certificados.

NOTA – Los servidores (D)TLS en el nodo maestro MN serán compatibles con los conjuntos de cifrado TLS para los clientes (D)TLS con los que se espera que interactúen.

Los servidores (D)TLS en los nodos intermedios soportarán todos los conjuntos de cifrado TLS indicados en la cláusula 10.2.2, Conjuntos de cifrado TLS y DTLS para marcos de seguridad basados en TLS-PSK, y en la cláusula 10.2.3, Conjuntos de cifrado TLS y DTLS para marcos de seguridad basados en certificados".

10.2.2 Conjuntos de cifrado TLS y DTLS para marcos de seguridad basados en TLS-PSK

Los marcos de seguridad que figuran a continuación:

marco de establecimiento de asociaciones de seguridad de clave simétrica provisionada;

marco de establecimiento de asociaciones de seguridad basado en MAF;

marco de provisión de seguridad a distancia de clave precompartida;

marco de provisión de seguridad a distancia basado en GBA;

utilizarán uno de los algoritmos de intercambio de calves que se describen en [IETF RFC 4279].

Las implementaciones TLS en las entidades compatibles con estos marcos de seguridad aplicarán, por lo menos, el siguiente conjunto de cifrado:

TLS_PSK_WITH_AES_128_CBC_SHA256 ([IETF RFC 5487]).

Las implementaciones DTLS compatibles con estos marcos de seguridad aplicarán, por lo menos, el siguiente conjunto de cifrado:

TLS_PSK_WITH_AES_128_CCM_8 ([IETF RFC 6655]).

Las consideraciones de seguridad recogidas en la sección 7 de [IETF RFC 4279] son aplicables. En particular, las aplicaciones deberían considerar cuidadosamente si necesitan o no el secreto perfecto hacia adelante (PFS) y escoger un conjunto de cifrado apropiado (sección 7.1 de [IETF RFC 4279]).

10.2.3 Conjuntos de cifrado de TLS y DTLS para marcos de seguridad basados en certificados

Los marcos de seguridad que figuran a continuación:

marco de establecimiento de asociaciones de seguridad mediante certificado;

marco de inicializaciones de seguridad mediante certificado;

utilizarán la toma de contacto TLS regular ([IETF RFC 5246]) con el intercambio de claves ECDHE_ECDSA ([IETF RFC 4492]).

Las implementaciones TLS que soporten estos marcos de seguridad aplicarán, por lo menos, el siguiente conjunto de cifrado:

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 [IETF RFC 5289].

Las implementaciones DTLS compatibles con estos marcos de seguridad aplicarán, por lo menos, el siguiente conjunto de cifrado TLS:

TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 [IETF RFC 7251].

Las implementaciones que sean compatibles con estos marcos de seguridad soportarán la autentificación de otras entidades a través de todos los tipos de certificados de clave pública disponibles (véase la cláusula 8.1.2.1, Tipos de certificados de clave pública):

Certificado de clave pública bruta: al aplicarse el mecanismo especificado en [IETF RFC 7250], la implementación soportará la recepción y el procesamiento de claves públicas brutas que se ajusten a lo descrito en la sección 9.1.3.2 sobre certificados de claves públicas brutas, de [b-IETF RFC 7252].

Todos los demás certificados: certificados UIT-T X.509, incluido el identificador del *hardware* del dispositivo. La implementación podrá recibir y procesar claves públicas brutas que se ajusten a lo descrito en la sección 9.1.3.3 sobre certificados X.509, de [b-IETF RFC 7252].

10.3 Detalles sobre la exportación y derivación de claves

10.3.1 Detalles sobre la exportación de claves TLS

Detalles sobre la exportación de claves TLS para la clave de inscripción

Tras una autentificación TLS satisfactoria entre el inscrito y la función de inscripción M2M (véase la cláusula 8.3.1.2), el inscrito y la función de inscripción M2M generan la clave de inscripción (Ke) y el RelativeKeID a partir de los secretos de la sesión (D)TLS aplicando la exportación de claves TLS ([IETF RFC 5705]) en la que ha de utilizarse la etiqueta "EXPORTER-oneM2M-Bootstrap" y la longitud 48. La clave de inscripción (Ke) se fija al valor de los 32 bytes menos significativos, mientras que el RelativeKeID se fija al valor de los 16 bytes más significativos.

Detalles sobre la exportación de claves TLS para la clave de conexión segura M2M

Tras una autentificación TLS exitosa entre la entidad A y la función de autentificación M2M (MAF) (véase la cláusula 8.8.2.7), la entidad A y la MAF generan la clave de conexión segura M2M (Kc) y el identificador de la clave de conexión segura (KcID) a partir de los secretos de la sesión (D)TLS aplicando la exportación de claves TLS ([IETF RFC 5705]) en la que ha de utilizarse la etiqueta "EXPORTER-oneM2M-Connection" y la longitud 48. La clave de conexión segura M2M (Kc) se fija al valor de los 32 bytes menos significativos, mientras que el identificados de la clave de conexión segura M2M (KcID) se fija al valor de los 16 bytes más significativos.

Detalles sobre la exportación de claves TLS para pairwiseE2EKey

Tras una autentificación TLS exitosa entre el extremo de inicio del ESCertKE y el extremo de terminación del ESCertKE (véase la cláusula 8.7.2.2), el inscrito y la función de inscripción M2M generan la pairwiseE2EKey y el pairwiseE2EKeyID a partir de los secretos de la sesión (D)TLS aplicando la exportación de claves TLS ([IETF RFC 5705]) en la que ha de utilizarse la etiqueta "EXPORTER-oneM2M-ESCertKE" y la longitud 48. La pairwiseE2EKey se fija al valor de los 32 bytes menos significativos, mientras que el pairwiseE2EKeyID se fija al valor de los 16 bytes más significativos.

10.3.2 **Derivación** de la credencial maestra a partir de la clave de inscripción

En esta cláusula se brinda información detallada sobre la generación de una credencial maestra (Km) a partir de una clave de inscripción (Ke) en los marcos de inicializaciones de seguridad.

Al generar una Km a partir de una Ke se utilizará la siguiente información:

el valor de la clave de inscripción (Ke);

el identificador de la función de autentificación M2M (MAF-ID) estará codificado en una cadena de octetos con arreglo a las normas de codificación UTF-8 especificadas en [IETF RFC 3629] y se le aplicará la forma de normalización KC (NFKC) de [Unicode].

El valor de la Km se obtendrá de la siguiente manera:

Km:= HMAC-SHA-256(Ke, "clave de inscripción oneM2M para la derivación de la credencial maestral" || MAF-ID),

donde HMAC-SHA-256 corresponde a su definición en [IETF RFC 2104].

10.3.3 Derivación de la clave de conexión segura provisionada, a partir de la clave de inscripción

En esta cláusula se brinda información detallada sobre la generación de una clave de conexión segura provisionada (Kpsa) a partir de una clave de inscripción (Ke) en los marcos de provisión a distancia.

Al generar la Kpsa a partir de la Ke, se utilizará la siguiente información:

el valor de la clave de inscripción (Ke);

el CSE-ID o AE-ID del inscrito B (Enrolee-B-ID), que se codificará en una cadena de octetos con arreglo a las normas de codificación UTF-8 especificadas en [IETF RFC 3629] y al que se aplicará la forma de normalización KC (NFKC) de [Unicode].

El valor de la Kpsa se obtendrá de la siguiente manera:

Kpsa:= HMAC-SHA-256(Ke, "clave de inscripción oneM2M para la derivación de la clave de conexión segura provisionada" || Enrolee-B-ID);

donde HMAC-SHA-256 corresponde a su definición en [IETF RFC 2104].

10.3.4 Generación del KeID

El valor del KeID se generará de la siguiente manera:

KeID = base64encode(RelativeKeyID)@MEF_FQDN:

donde:

base64encode(RelativeKeID) designa una codificación de tipo base64 ([IETF RFC 3548]) del valor del RelativeKeID; y

MEF_FQDN designa el FQDN de la función de inscripción M2M.

10.3.5 Generación de un identificador de clave para el marco de seguridad MAF

El valor del identificador de clave se generará de la siguiente manera:

Identificador de clave = base64encode(RelativeKeyID)@MAF_FQDN;

donde:

base64encode(RelativeKeyID) designa una codificación de tipo base64 ([IETF RFC 3548]) del valor del RelativeKeyID; y

MAF_FQDN designa el FQDN de la función de autentificación M2M.

10.3.6 Derivación de la clave maestra de extremo a extremo a partir de la clave de conexión segura provisionada

10.3.6.1 Introducción

En esta cláusula se brinda información detallada sobre la generación de una clave maestra de extremo a extremo (Ke2e_master) a partir del establecimiento exitoso de una asociación de seguridad entre un extremo de origen y otro de destino de la ESF utilizando un marco de provisión de seguridad a distancia, según se describe en la cláusula 8.3. Así pues, los mecanismos para generar la clave maestra de extremo a extremo se basan en un proceso de extracción de claves a partir de la clave de conexión segura provisionada (Kpsa).

Al generar la Ke2e a partir de la Kpsa se utilizará la siguiente información:

el valor de la clave de conexión segura provisionada (Kpsa);

el CSE-ID o AE-ID del extremo de origen B de la ESF (end-point-B-ID de origen de la ESF), que se codificará en una cadena de octetos con arreglo a las normas de codificación UTF-8 especificadas en [IETF RFC 3629] y al que se aplicará la forma de normalización KC (NFKC) especificada en [Unicode].

El valor de la Ke2e_master se generará de la siguiente manera:

Ke2e_master = HMAC-Hash (Sal, Kpsa).

NOTA – En el caso de las credenciales generadas en el origen, se utiliza un valor aleatorio facilitado por el extremo de origen de la ESF en lugar de la Kpsa a fin de crear la Ke2e_master.

10.3.6.2 Extracción y expansión de claves a partir de una clave maestra de extremo a extremo

La clave maestra de extremo a extremo (Ke2e_master) se utiliza para generar claves específicas de protección de la seguridad. La generación de las distintas claves se basa en los parámetros y el ámbito establecidos para la extracción y expansión de claves, que se ejecuta de acuerdo con las especificaciones definidas en [IETF RFC 5869]. En el Cuadro 10.3.6.2-1 se presenta una lista de posibles claves de extremo a extremo.

Cuadro 10.3.6.2-1: Claves de seguridad de extremo a extremo

Protección de la seguridad	Claves simétricas generadas
Autenticidad del mensaje (primitiva)	Ke2e_msg_auth
Confidencialidad del mensaje (primitiva)	Ke2e_msg_conf
Integridad de los datos (atributo)	Ke2e_att_auth
Confidencialidad de los datos (atributo)	Ke2e_att_conf

Las claves de protección de la seguridad de extremo a extremo se generan por expansión de claves a partir de la Ke2e_master, utilizando los mecanismos especificados en [IETF RFC 5869]. Tomando como base la clave maestra de extremo a extremo generada, las claves asociadas de autentificación del mensaje de extremo a extremo y/o de confidencialidad del mensaje de extremo a extremo, así como sus claves de atributo, se crean de la siguiente manera:

T(0) = cadena vacía (longitud cero)

Clave de autenticidad del mensaje de extremo a extremo (Ke2e_msg_auth) = T(1) = HMAC-Hash (Ke2e_master, T(0) | "clave de autentificación del mensaje E2E"| 0x01)

Clave de confidencialidad del mensaje de extremo a extremo (Ke2e_msg_conf) = T(2) = HMAC-Hash (Ke2e_master, T(1)| "clave de confidencialidad del mensaje E2E"|0x02)

Clave de autenticidad de atributo de extremo a extremo (Ke2e_att_auth) = T(3) = HMAC-Hash (Ke2e_master, T(2)| "clave de autenticidad de atributo E2E"|0x03)

Clave de confidencialidad de atributo de extremo a extremo (Ke2e_att_conf) = T(4) = HMAC-Hash (Ke2e_master, T(3)| "clave de confidencialidad de atributo E2E"|0x04)

NOTA 1 – Si se emplean algoritmos AEAD, en los casos en que solo se utilice una clave única, puede derivarse la clave Ke2e_msg_auth o Ke2e_msg_conf y utilizarse tanto para la autenticidad del mensaje como para la confidencialidad del mensaje.

NOTA 2 – Es posible efectuar la provisión al extremo de destino de la ESF de todas las claves necesarias o únicamente de la clave maestra de extremo a extremo (Ke2e_master) y de los parámetros criptográficos asociados (por ejemplo, etiquetas, valores aleatorios) de los que luego podrá servirse para generar las claves necesarias para la ESPrim y la ESData.

10.3.7 Derivación de claves simétricas de uso restringido a partir de la clave de inscripción

En esta cláusula se brinda información detallada sobre la generación de una clave simétrica de uso restringido a partir de una clave de inscripción (Ke) en los marcos de provisión de seguridad a distancia.

Se utilizará la siguiente información:

el valor de la clave de inscripción (Ke);

el identificador de uso de seguridad (SUID) aplicable al uso previsto de la clave simétrica;

el identificador del objetivo del inscrito (Enrolment-Target-ID), a saber, un FQDN que se codificará en una cadena de octetos con arreglo a las normas de codificación UTF-8 especificadas en [IETF RFC 3629] y al que se aplicará la forma de normalización KC (NFKC) de [Unicode].

Si el objetivo de la inscripción es una CSE o una AE, se utilizará la representación FQDN del CSE-ID absoluto o el AE-ID absoluto.

El valor de la clave simétrica de uso restringido se generará de la siguiente manera:

HMAC-SHA-256(Ke, "clave de inscripción oneM2M para la derivación de la clave simétrica de uso restringido" || SUID || Enrolment-Target-ID);

donde HMAC-SHA-256 corresponde a su definición en [IETF RFC 2104].

10.3.8 Algoritmos de derivación de la sessionESPrimKey

10.3.8.1 Introducción

La sessionESPrimKey se utiliza en la seguridad de las primitivas de extremo a extremo (ESPrim), y se deriva a partir de la pairwiseESPrimKey, el receiverESPrimRandObject y el originatorESPrimRandObject (véase la cláusula 8.4.2).

En la cláusula 10.3.8 se especifican los algoritmos que permiten derivar la sessionESPrimKey utilizada en la ESPrim. Los algoritmos disponibles se enumeran en el Cuadro 10.3.8.1-1.

Cuadro 10.3.8.1-1: Algoritmos de derivación de la sessionESPrimKey

Algoritmo	Obligatorio/Opcional	Cláusula
HMAC-SHA256	Obligatorio	10.3.8.2

10.3.8.2 Algoritmo HMAC-SHA256 para la derivación de la sessionESPrimKey

La sessionESPrimkey se deriva de la siguiente manera:

sessionESPrimKey = HMAC-SHA256 (pairwiseESPrimKey,
receiverESPrimRandObject || originatorESPrimRandObject ||
"algoritmo HMAC-SHA256 oneM2M para la derivación de la sessionESPrimKey"),

donde HMAC-SHA-256 corresponde a su definición en [IETF RFC 2104].

10.4 Detalles sobre el credential-ID

El Credential-ID se compone de dos partes:

una parte type-ID, que consiste en un número entero positivo definido por el tipo de datos sec:credIDTypeID;

una parte valor, que contiene un identificador globalmente único de la credencial de la entidad. En esta parte puede utilizarse el alfabeto romano, números y los caracteres ".", "_", "-" y "@".

El Credential-ID se forma concatenando la parte sobre el tipo, el carácter "-" y la parte valor.

NOTA – Un Credential-ID es un identificador globalmente único que se utiliza para identificar los recursos serviceSubscribedAppRule ([UIT-T Y.4500.1]) y las credenciales en la información de configuración de seguridad.

10.5 KpsaID

El KpsaID tendrá la siguiente forma:

KpsaID = Issuer_Relative_KpsaID@Issuer_FQDN;

donde:

Issuer_Relative_KpsaID se compone de letras del alfabeto romano, números y los caracteres ".", "_" y "-". El emisor del KpsaID se asegurará de que no haya dos Kpsa con el mismo Issuer_Relative_KpsaID.

Issuer_FQDN es un FQDN que representa la parte interesada que efectuó la provisión de la Kpsa.

NOTA – Este formato del KpsaID permite extraer la identidad del emisor a partir del KpsaID.

10.6 Formato del KmID

El KmID tendrá la siguiente forma:

KmID = MAF_RELATIVE_KmID@MAF_FQDN;

donde:

MAF_RELATIVE_ KmID se compone de letras del alfabeto romano, números y los caracteres ".", "_" y "-". El MAF_RELATIVE_KmID no distingue entre mayúsculas y minúsculas. La MAF se asegurará de que no haya dos Km con el mismo MAF_RELATIVE_ KmID.

MAF_FQDN designa el FQDN de la función de autentificación M2M.

NOTA – Este formato del KmID permite extraer la identidad de la función de autentificación M2M a partir del KmID.

10.7 Expiración de la inscripción

La expiración de la inscripción consiste en el final de la vida útil de la clave generada, a saber, la Ke, en el marco de provisión de seguridad a distancia de clave simétrica preconfigurada. Las claves generadas para el establecimiento de asociaciones de seguridad entre los inscritos y los objetivos de la inscripción (es decir, la Km o la Kpsa) a partir de la clave de inscripción Ke dejarán de ser válidas cuando la vida útil de la credencial de inscripción Ke llegue a su fin. Por lo tanto, la vida útil de la Km o la Kpsa debería ser, como máximo, igual a la vida útil de la Ke. Cuando haya expirado la inscripción, el inscrito debe poner en marcha una vez más la provisión a distancia para volver a generar las claves de los marcos de provisión de seguridad a distancia, como se especifica en la cláusula 8.3.2.1.

11 Arquitectura de protección de la privacidad mediante un gestor de la política de privacidad (PPM)

11.1 Introducción

En esta cláusula se presenta una arquitectura del gestor de la política de privacidad (PPM). El PPM es una arquitectura distribuida de protección de la privacidad por autorizaciones que se basa en las preferencias de privacidad indicadas por el usuario.

El PPM es un marco de gestión de datos personales que se basa en las preferencias de privacidad del usuario. Permite crear políticas de control de acceso a partir de las preferencias de privacidad del usuario y proteger la información de identificación personal (PII) del usuario frente a las partes no autorizadas. Puede ser operado por un proveedor de servicios M2M u otra parte interesada que sea un tercero fiable. Para que un proveedor de servicios u otra parte interesada entregue la información de identificación personal de un usuario a un tercero, se necesita la aceptación del usuario afectado. En caso de que el usuario acepte una política de privacidad que permita la divulgación de información a terceros, el proveedor de servicios podrá proporcionar la información de identificación personal a terceros. Sin embargo, si en la política de privacidad no se prevé la divulgación a terceros, el proveedor de servicios debe actualizar la política y obtener el respectivo consentimiento del usuario.

11.2 Relación entre los componentes del PPM y del sistema oneM2M

El PPM se constituirá de los componentes que se indican a continuación. Puede consultarse información detallada sobre cada componente en TR-0001-Use_Cases_Collection de oneM2M [b-oneM2M TR0002]. En esta cláusula se describe la relación entre esos componentes y los componentes de oneM2M:

Mecanismo de consentimiento sofisticado para la política de privacidad:

El usuario final que se abona a un servicio que utiliza una aplicación proporcionada por una IN-AE se convierte en un sujeto de datos, que crea una preferencia de privacidad y la registra en el PPM.

Esta función se describe en la cláusula 11.4.1.2.

Funciones del punto de decisión de política (PDP) y del punto de recuperación de política (PRP):

PDP:

Cuando una aplicación solicita datos personales de una IN-CSE, el PPM responde con una decisión de acceso adoptada en función de las políticas de control de acceso establecidas sobre la base de la preferencia de privacidad indicada por el usuario.

PRP:

Cuando una aplicación solicita datos personales de una IN-CSE, el PDP solicita al PPM las políticas de control de acceso. En respuesta, el PPM facilita las políticas de control de acceso establecidas sobre la base de la preferencia de privacidad indicada por el usuario.

Los componentes del PDP y del PRP se definen en las cláusulas 6.2.2, Autorización, y 7.1 Mecanismo de control de acceso.

Trazabilidad del uso de los datos personales:

El PPM mantendrá un registro de acceso en el que se deje constancia de qué IN-AE accedió a qué tipo de datos recopilados.

Esta función está pendiente de un examen más detallado en el marco del sistema oneM2M, pero puede utilizarse con los componentes definidos en dicho marco.

11.3 Gestión de la política de privacidad en la arquitectura del sistema oneM2M

11.3.1 Introducción

La utilización del PPM consta de cuatro procedimientos. En esta cláusula se explican las relaciones entre las diferentes etapas del escenario PPM y los componentes de oneM2M:

Un sujeto de datos se une a una IN-CSE, como una plataforma M2M.

Un sujeto de datos se abona a un servicio ofrecido por una IN-AE.

Una IN-AE solicita datos personales almacenados en una ASN-CSE, una MN-CSE o una IN-CSE.

El sujeto de datos comprueba el registro de acceso correspondiente a sus propios datos personales y solicita su eliminación a la IN-AE.

11.3.2 Entidades involucradas

Sujeto de datos:

Los usuarios finales pueden utilizar los servicios disponibles en una IN-CSE abonándose a un servicio de una IN-AE que disponga de funciones de control de acceso a la información almacenada en una IN-CSE.

El usuario final que se abona al servicio de una IN-AE se convierte en un sujeto de datos.

AE:

La AE recopila varios tipos de datos, como los captados por un sensor.

La AE envía los datos a una ASN-CSE, MN-CSE o IN-CSE.

ASN-CSE o MN-CSE:

Punto de aplicación de política (PEP):

El PEP es una de las funciones disponibles en la CSE.

Punto de decisión de política (PDP):

El PDP es una de las funciones disponibles en la CSE.

Datos personales:

Los datos personales son una información que puede utilizarse por sí sola o en complemento con otra información para identificar a un individuo con objeto de recopilar información de identificación personal (PII).

La CSE de dominio de campo recopila y almacena datos personales.

Ejemplos de datos personales: datos de sensores, consumo de energía eléctrica, estado de funcionamiento del aire acondicionado, etc.

IN-AE:

La IN-AE presta servicios a un usuario final que se une a la IN-CSE.

La IN-AE solicita datos personales de en una IN-CSE para poder prestar sus servicios.

IN-CSE:

Portal M2M:

El portal M2M es un tipo de sitio o aplicación web que gestiona los servicios prestados por una plataforma M2M (IN-CSE e IN-AE conexas).

El usuario final accede a un portal para unirse a una IN-CSE. El sujeto de datos accede al portal para abonarse a un servicio de una IN-AE.

PPM:

El PPM guardará las políticas de control de acceso establecidas sobre la base de la preferencia de privacidad del usuario.

Como la MN-CSE utiliza el PPM en calidad de PDP o PRP, el PPM será compatible con las funcionalidades de PDP y PRP:

El portal PPM es un tipo de sitio o aplicación web en el PPM.

El usuario final accede a un portal PPM para configurar su preferencia de privacidad.

11.3.3 Flujo de la gestión en la arquitectura PPM

11.3.3.0 Introducción

En esta cláusula se describe el caso en que una ASN-CSE o MN-CSE almacena datos personales.

11.3.3.1 Unión a una IN-CSE

Cuando un sujeto de datos se une a una IN-CSE, configura su preferencia de privacidad a través del PPM. En la preferencia de privacidad se determina a qué tipo de datos pueden acceder las IN-AE. En la Figura 11.3.3.1-1 se ilustra este proceso de forma general.

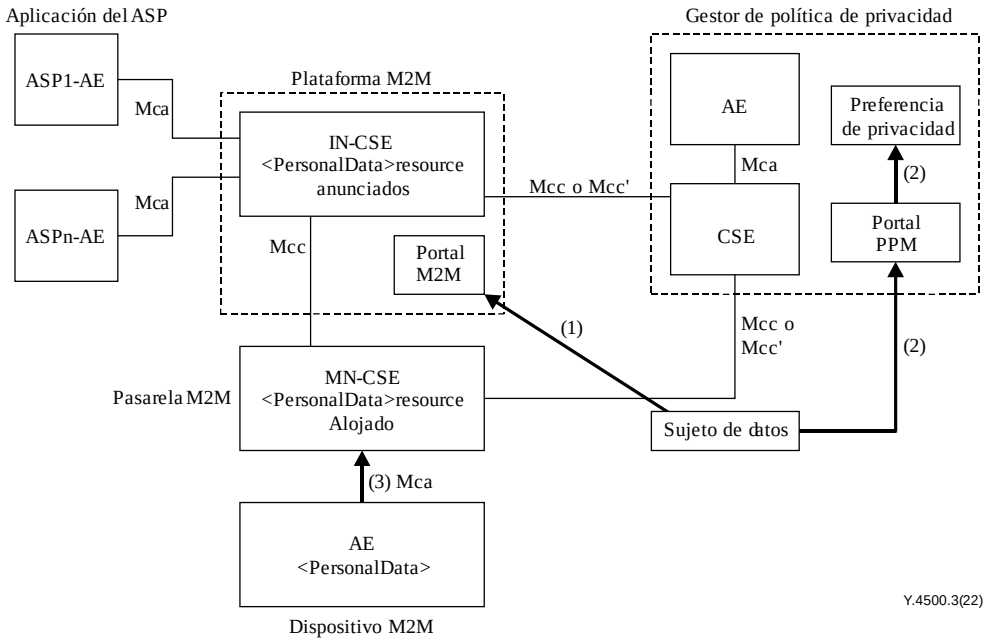


Figura 11.3.3.1-1 – Unión de un sujeto de datos a una IN-CSE

(1) Un sujeto de datos accede al portal M2M de una IN-CSE:

Este proceso suele utilizar protocolos de acceso web, como HTTP, HTTPS, etc.

Este proceso se describe en la cláusula 11.4.1.2.

(2) Un sujeto de datos configura una preferencia de privacidad y la registra en el portal PPM. Posteriormente, el PPM creará las políticas de control de acceso con base en dicha preferencia:

Un sujeto de los datos accede al portal PPM o el portal M2M redirige al sujeto de datos al portal PPM. Este proceso utiliza protocolos de acceso web.

Este proceso se describe en la cláusula 11.4.1.2.

(3) Una ASN-CSE o MN-CSE recopila los datos de la EA y los almacena.

11.3.3.2 Abono a un servicio de una IN-AE

El sujeto de los datos puede abonarse a varios tipos de servicios proporcionados por las IN-AE a través de la IN-CSE. Las listas de servicios se registran en un portal M2M en el que el sujeto de datos puede seleccionar los servicios a los que desea abonarse y, al hacerlo, debe aceptar una política de privacidad. Para que el sujeto de datos comprenda fácilmente dicha política, el PPM creará una política de privacidad personalizada basada en la política facilitada por la IN-AE y en las preferencias de privacidad del sujeto de datos. De tal manera, este puede controlar los datos personales y su consentimiento indica que ha comprendido la política de privacidad. En la Figura 11.3.3.2-1 se ilustra este proceso de forma general.

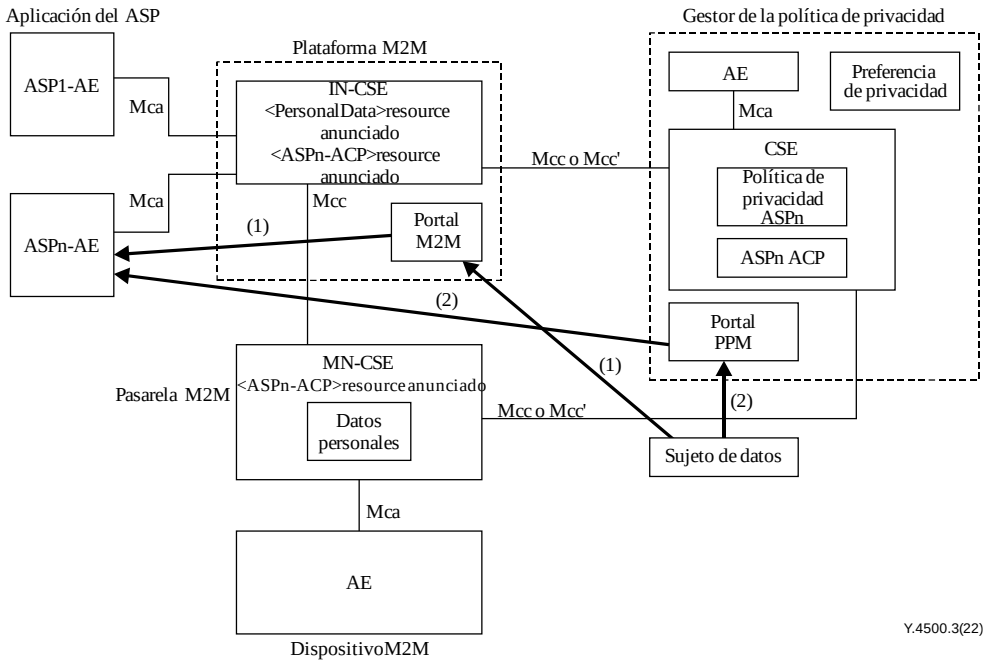


Figura 11.3.3.2-1 – Abono del sujeto de datos a un servicio de la IN-AE

(1) El sujeto de datos accede al portal y selecciona un servicio de la IN-AE al cual abonarse:

Este proceso suele utilizar protocolos de acceso web como HTTP, HTTPS, etc.

Este proceso se describe en la cláusula 11.4.1.1.

(2) El sujeto de datos debe aceptar una política de privacidad para abonarse al servicio de la IN-AE. El PPM creará la política de privacidad personalizada para cada sujeto de datos basándose en sus preferencias de privacidad. El sujeto de datos puede contrastar con facilidad las diferencias entre la preferencia de privacidad y la política de privacidad y entender qué tipo de datos personales recopila la IN-AE. Una vez que acepta la política de privacidad, puede abonarse al servicio de la IN-AE:

La función de creación de una política de privacidad personalizada se describe en la cláusula 11.4.1.3.

(3) El PPM creará o actualizará las políticas de control de acceso sobre la base de la política de privacidad que el sujeto de datos haya aceptado:

La función de creación o actualización de políticas de control de acceso en el PPM puede basarse en los mecanismos de autorización especificados en las cláusulas 7.3 y 7.4. En esta Recomendación no se proporciona información detallada sobre del proceso de sincronización.

11.3.3.3 Solicitud de datos personales a la IN-CSE

En caso de que la IN-AE necesite acceder a los datos personales para prestar un servicio, los solicita a la IN-CSE. El PPM cumplirá las funciones de PDP o PRP.

Cuando el PPM funciona como PDP, el PEP recibe la decisión de acceso del PPM y controla el acceso a los datos sobre la base de dicha decisión. En la Figura 11.3.3.3-1 se ilustra este proceso de forma general.

Cuando el PPM funciona como PRP, el PDP obtiene las políticas de control de acceso del PPM y controla el acceso a los datos sobre la base de dichas políticas. En la Figura 11.3.3.3-2 se ilustra este proceso de forma general

A. El PPM funciona como PDP

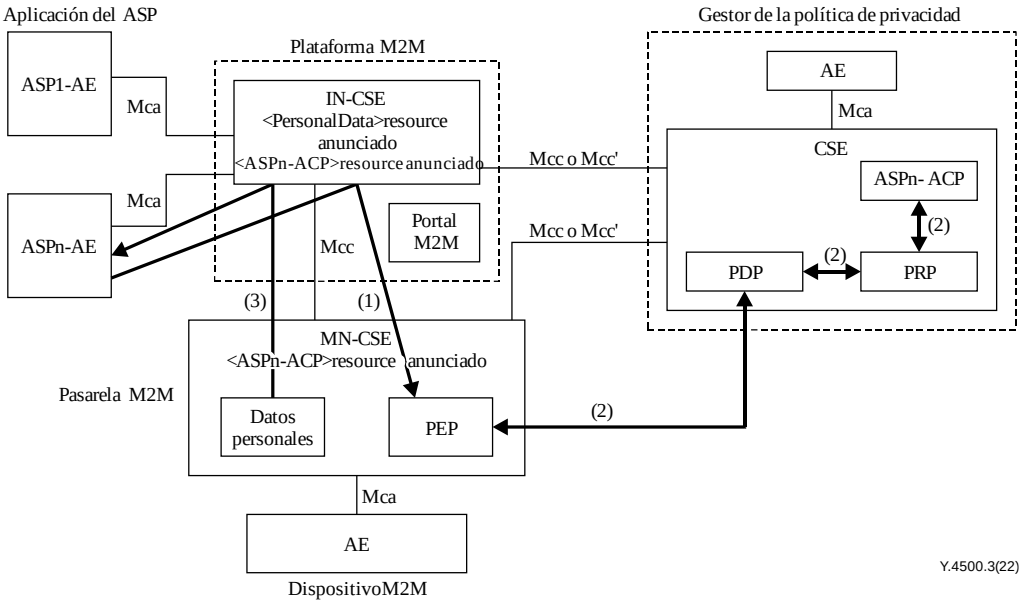


Figura 11.3.3.3-1 – Solicitud de datos personales a la IN-CSE (el PPM funciona como PDP)

(1) Una IN-AE solicita datos personales a la IN-CSE.

(2) El PEP de la ASN-CSE o la MN-CSE formula una "solicitud de decisión" al PPM. El PPM decidirá si autoriza o deniega el acceso a los datos personales sobre la base de las políticas de control de acceso. Posteriormente, el PPM enviará la "decisión de respuesta" a la ASN-CSE o la MN-CSE:

En este caso, el PPM proporcionará una interfaz que permite controlar el acceso a los datos personales por intermedio del PPM como PDP.

(3) De autorizarse el acceso a los datos persones, el PEP accede a estos y los envía a la IN-AE como respuesta.

B. El PPM funciona como PRP

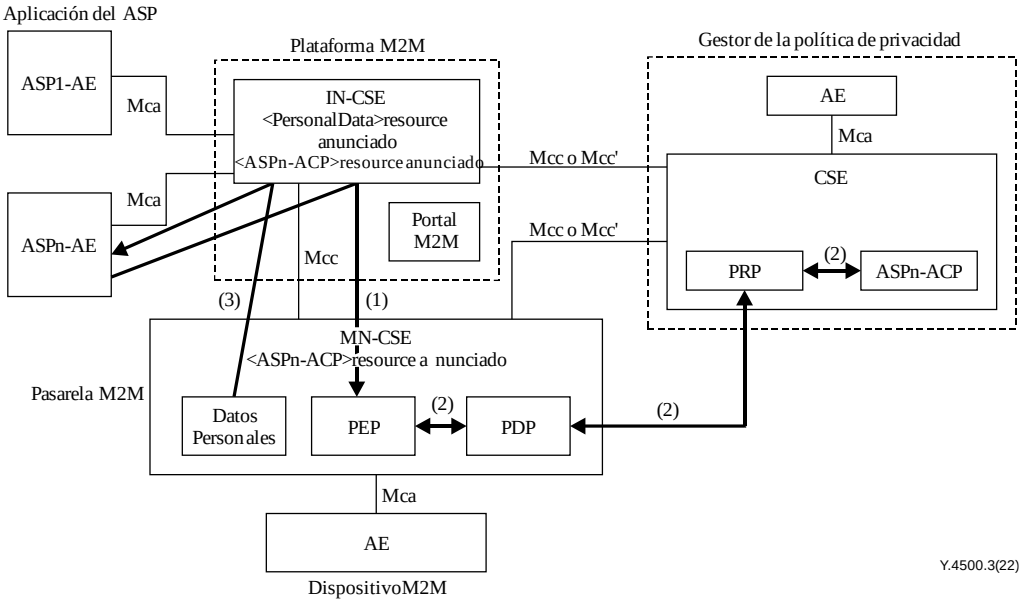


Figura 11.3.3.3-2 – Solicitud de datos personales a la IN-CSE (el PPM funciona como PRP)

(1) Una IN-AE solicita datos personales a la IN-CSE.

(2) El PEP en la ASN-CSE o la MN-CSE formula una "solicitud de decisión" al PDP. El PDP realiza una "solicitud de política" al PPM. El PPM recopilará las políticas de control de acceso relacionadas con la "solicitud de política" y las enviará en forma de "respuesta de política" al PDP en la ASN-CSE o la MN-CSE. A continuación, el PDP decide si autoriza o deniega el acceso a los datos personales sobre la base de las políticas de control de acceso y envía el resultado mediante una "decisión de respuesta" al PEP:

En este caso, el PPM proporcionará una interfaz que permite controlar el acceso a los datos personales por intermedio del PPM como PRP. En la presente versión, se utilizará la autorización dinámica directa, y el PPM funcionará como servidor de autorización dinámica (DAS). Pueden consultarse más detalles en la cláusula 7.3.2.2.

(3) De autorizarse el acceso a los datos personales, el PEP accede a estos y los envía a la IN-AE como respuesta.

11.4 Modelos de implementación del gestor de la política de privacidad

11.4.1 Utilización del lenguaje de marcaje de los términos y condiciones

11.4.1.0 Introducción

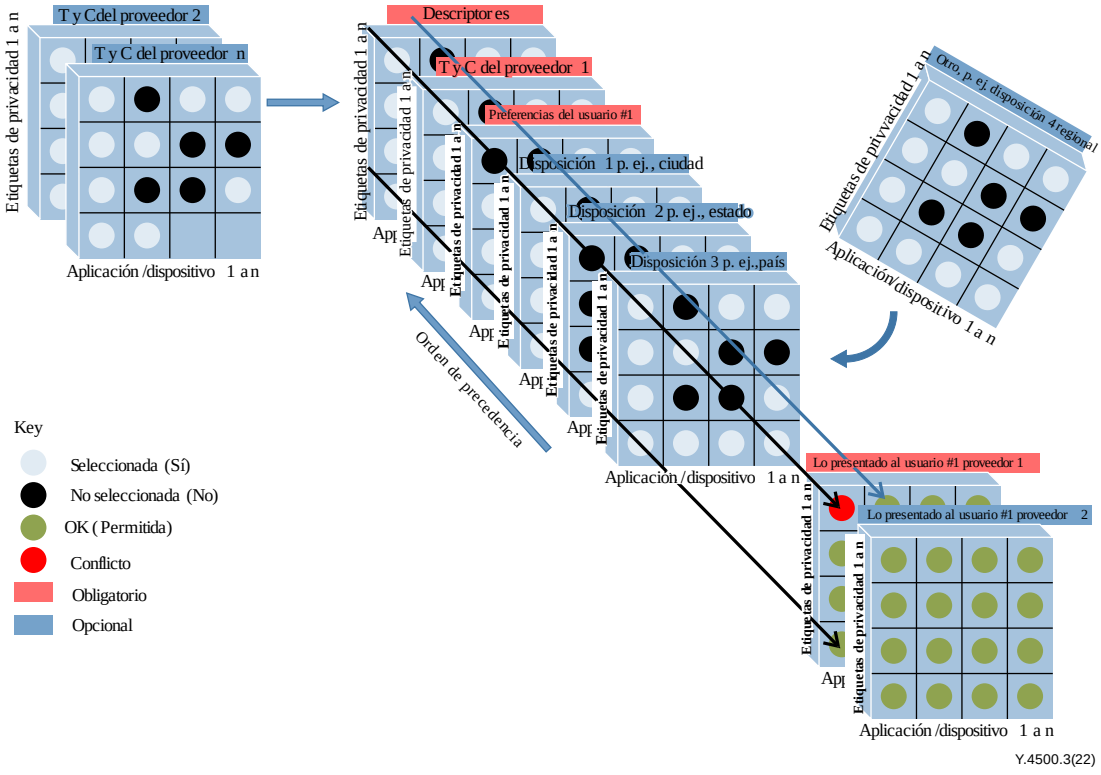


Figura 11.4.1.0-1 – Modelo de implementación del gestor de la política de privacidad utilizando el lenguaje de marcaje de los términos y condiciones, para un usuario final (#1) y un proveedor de servicios de aplicación (proveedor 1)

En la Figura 11.4.1.0-1 se ilustra un modelo en el que se muestran los componentes del gestor de la política de privacidad (PPM) para un usuario final (#1) y un ASP (proveedor 1), organizados en varios filtros correspondientes a una etiqueta "seleccionada" o "no seleccionada" dentro de una serie de cuadros de filtro apilables.

Se han establecido cuatro cuadros de filtro obligatorios:

el cuadro de filtro descriptor;

al menos un cuadro de filtro sobre los "términos y condiciones del proveedor";

el cuadro de filtro sobre las preferencias del usuario; y

al menos un cuadro de filtro sobre lo "presentado al usuario".

Cada cuadro de filtro se compone de cuadrículas que representan las etiquetas de privacidad en el lenguaje de marcaje, en vertical, y las aplicaciones o dispositivos, en horizontal.

Por lo que se refiere al cuadro de filtro sobre los términos y condiciones del proveedor y al cuadro de filtro sobre las preferencias del usuario, cada atributo representado por la etiqueta de privacidad configurada como "seleccionada" o "no seleccionada" con respecto a una aplicación o dispositivo en concreto se modela "poniendo" un disco de filtro del color conveniente.

Los discos que se encuentran en las mismas posiciones dentro de uno o más cuadros de filtro sobre lo "presentado al usuario" de estructura similar trazan trayectos claros a lo largo de la pila de cuadros de filtro:

Cuando los términos y condiciones del proveedor y las preferencias del usuario coinciden, los discos serán de color verde.

Cuando los trayectos están bloqueados a causa de uno o varios conflictos, detectores similares hacen que los discos se vuelvan rojos.

EJEMPLO: Si el proveedor de servicios de aplicación (ASP) espera que el usuario acepte que su información de ubicación se recopile y se comparta con un tercero, entonces selecciona esos dos atributos (discos en blanco). Si el usuario final ha establecido una preferencia de que no quiere que su información de ubicación se recopile ni se comparta, entonces el cuadro de filtro sobre las preferencias del usuario contendrá discos negros y, por lo tanto, se bloqueará trayecto a lo largo de la pila.

Es posible añadir más cuadros de filtro opcionales a la pila a fin de volver a "seleccionar" o "no seleccionar" esas mismas características "poniendo" un disco de filtro del color conveniente. Por ejemplo, la selección de un proveedor de servicios de aplicación o de un usuario final puede verse anulada por un precedente de política o una norma nacional. La posición de estos cuadros de filtro opcionales determina su precedencia; así, los que están ubicados en la parte delantera anulan a los que están en la parte trasera.

Este modelo se basa en el supuesto de que la gran mayoría de los atributos de proveedor seleccionados por el proveedor de servicios de aplicación no entrarán en conflicto con las preferencias del usuario y se mostrarán en verde. Sin embargo, cabe señalar que habrá un gran número de dispositivos, aplicaciones y actualizaciones frecuentes de *software*, así como sustituciones de dispositivos. Si bien en la mayoría de los casos no se producirán conflictos, los que se generen se representarán de inmediato con uno o varios discos rojos que solo se mostrarán al usuario final, evitando de esta manera tener que leer y releer constantemente cientos de páginas de términos y condiciones detalladas.

Todos los usuarios finales que estén registrados en el PPM tendrán acceso a un ejemplar de esta pila, así como todos los proveedores de servicios de aplicación a los que se hayan abonado. Sin embargo, el cuadro de filtro descriptor y los cuadros de filtro opcionales sobre ciudad/estado/país/región pueden figurar como recursos compartidos de esos ejemplares.

11.4.1.1 Registro de la política de privacidad del proveedor de servicios de aplicación

El registro opcional de la política de privacidad de una aplicación formará parte del proceso de obtención de un App-ID registrado para cada aplicación y versión, y del proceso de presentación de

un certificado de seguridad a la autoridad de registro oneM2M que se utiliza para autentificar la aplicación y la versión.

El ASP descargará una plantilla de importación de los términos y condiciones de la aplicación desde el servidor de registro del App-ID del sistema oneM2M, si no dispone ya de la plantilla de importación correcta.

En la plantilla de importación de los términos y condiciones han de figurar en orden numérico las etiquetas que se recogen en el Anexo normativo J.

NOTA – El formato de la plantilla de importación de los términos y condiciones se deja a discreción, siempre y cuando transmita la información especificada en el Anexo J.

Por cada etiqueta que figure en la lista, el ASP proporcionará, con arreglo al formato especificado en el Anexo normativo J, un valor para todos los dispositivos y aplicaciones en el ámbito de la aplicación que el ASP esté registrando.

El ASP procesará la plantilla de importación de los términos y condiciones de la aplicación utilizando sus sistemas y procedimientos locales junto con información facilitada por los proveedores de dispositivos y los terceros que proporcionen componentes de su aplicación para establecer uno o varios conjuntos de términos y condiciones del proveedor.

El registro del App-ID del sistema oneM2M también ha de proporcionar al ASP, como mínimo, la "lista de descriptores" en el idioma soportado por el socio oneM2M a fin de ayudar al ASP a completar las plantillas de importación de los términos y condiciones destinadas a formar el conjunto de términos y condiciones del proveedor para ese ASP.

El certificado de seguridad que se utilizó durante el proceso de registro del App-ID también se utilizará para garantizar la integridad y proteger la plantilla de importación de los términos y condiciones de la aplicación que se ha cumplimentado durante su posterior almacenamiento y transmisión.

El registro del App-ID del sistema oneM2M comprobará la autenticidad e integridad de los términos y condiciones de la ASP verificando la firma con el certificado de clave pública del ASP durante el registro del App-ID.

Los términos y condiciones de cada ASP o proveedor de *software* que se hayan finalizado se asociarán al App-ID recogido en el registro del App-ID del sistema oneM2M.

11.4.1.2 Registro de las preferencias de privacidad del usuario final

El usuario final que se abona a un servicio prestado por un proveedor de servicios de aplicación se convierte en un sujeto de datos, que puede descargar o visualizar la plantilla de preferencias de privacidad del usuario final a través del portal PPM.

La plantilla que utiliza el usuario final para indicar sus preferencias de privacidad habrá de coincidir con la del proveedor de servicios de aplicación, es decir, las etiquetas enumeradas en el Anexo normativo J figurarán en el mismo orden.

El usuario final selecciona y descarta los atributos para indicar sus preferencias de privacidad, que luego se registran en el PPM a través del mismo portal.

11.4.1.3 Creación de una política de privacidad personalizada para cada usuario final

Para facilitar al sujeto de datos la confirmación de las diferencias entre la preferencia de privacidad y la política de privacidad:

a) Si el ASP selecciona la característica representada por el valor de la etiqueta que coincide con la preferencia de privacidad que seleccionó el usuario para esa aplicación o dispositivo, el correspondiente indicador "presentado al usuario" se pondrá en verde.

b) Si el ASP no selecciona la característica representada por el valor de la etiqueta que coincide con la preferencia de privacidad que estableció el usuario para esa aplicación o dispositivo, el correspondiente indicador "presentado al usuario" se pondrá en verde.

c) Si el valor que selecciona el ASP para la característica representada por el valor de la etiqueta coincide con la preferencia de privacidad que seleccionó el usuario para esa aplicación o dispositivo, el correspondiente indicador "presentado al usuario" se pondrá en verde.

d) Si el ASP selecciona la característica representada por el valor de la etiqueta que no coincide con la preferencia de privacidad que seleccionó el usuario para esa aplicación o dispositivo, el correspondiente indicador "presentado al usuario" se pondrá en rojo.

e) Si el ASP no selecciona la característica representada por el valor de la etiqueta que no coincide con la preferencia de privacidad que seleccionó el usuario para esa aplicación o dispositivo, el correspondiente indicador "presentado al usuario" se pondrá en rojo.

f) Si el valor que fija el ASP para la característica representada por el valor de la etiqueta no coincide con la preferencia de privacidad que estableció el usuario para esa aplicación o dispositivo, el correspondiente indicador "presentado al usuario" se pondrá en rojo.

Las reglas anteriores se anularán si se establecen uno o varios perfiles de preferencias.

El orden de precedencia será el siguiente:

1) Precedencia de política – región.

2) Precedencia de política – país.

3) Precedencia de política – ciudad.

4) Precedencia de política – estado.

5) Control parental.

12 Definiciones de los tipos de datos oneM2M específicos de seguridad

12.1 Introducción

En la cláusula 12 se presentan las definiciones de los tipos de datos que aplican únicamente a las especificaciones de seguridad de oneM2M.

Todos los tipos de datos relativos a los elementos XML definidos para su uso exclusivo en el marco de las especificaciones de seguridad de oneM2M utilizarán el espacio de nombres:
http://www.onem2m.org/xml/securityProtocols

En esta Recomendación, y en cualquier documento XML o de esquemas XML elaborado por oneM2M, se empleará el prefijo "sec:" para hacer referencia al espacio de nombres. Los documentos de esquemas XML elaborados por oneM2M que son pertinentes para esta especificación pueden encontrarse en [b-oneM2M.XML].

12.2 Tipos de datos oneM2M específicos de seguridad simples

En el Cuadro 12.2-1 se describen las definiciones de los tipos de datos específicos de seguridad simples. Los tipos indicados en el Cuadro12.2-1 son los siguientes:

tipos de datos atómicos derivados de los tipos de datos de esquemas XML a partir de restricciones distintas de la enumeración;

tipos de datos de lista construidos a partir de otros tipos de datos atómicos de esquemas XML o definidos por oneM2M.

Cuadro 12.2-1 – Tipos de datos oneM2M específicos de seguridad simples

Nombre del tipo XSD	Uso	Ejemplos	Descripción
sec:relKeyID	Parte relativa de los identificadores de clave simétrica	1he83he, my-key_name, firstname.lastname	Cualquier combinación de letras del alfabeto romano, números y los caracteres ".", "_" y "-".
sec:credentialID	Identificador de credencial	10-thiskey@mymef.com	Un sec:credIDTypeID y un xs:anyURI separados por el carácter "-". Véase la cláusula 10.4. El xs:anyURI es la parte valor del credential-ID.
sec:deviceConfigURI	atributo *deviceConfigURI* del recurso <*MEFBase*>, véase [UIT-T Y.4500.32]	1:http://server.dmprovider.com	Un valor sec:devMgmtID (véase la cláusula 12.3.2.2) separado por dos puntos ":" del URI de un servidor de gestión de dispositivos.

12.3 Tipos de datos oneM2M específicos de seguridad enumerados

12.3.1 Introducción

Los tipos de datos oneM2M específicos de seguridad enumerados se tratan de la misma manera que los tipos de datos oneM2M específicos de seguridad enumerados que se definen en la cláusula 6.3.4 de [UIT-T Y.4500.4]. Estos tipos de datos se basan en <xs:integer>, y los valores numéricos se interpretan con arreglo a lo establecido en la cláusula 12.3.2.

12.3.2 Definiciones de los tipos de enumeración

12.3.2.1 sec:credIDTypeID

El tipo de enumeración sec:credIDTypeID se utiliza en sec:credentialID para identificar el tipo de la credencial identificada. En el Cuadro 12.3.2.1-1 se describe la manera en que se interpreta el tipo de enumeración sec:credIDTypeID.

Cuadro 12.3.2.1-1 – Interpretación del tipo de enumeración sec –credIDTypeID

Valor	Interpretación	Nota
10	Clave simétrica utilizada para autentificarse ante una MEF (KpmID)	Véase la cláusula 8.3.2.1
11	Clave simétrica utilizada para autentificarse ante una MAF (KmID)	Véase la cláusula 8.8.3.1
12	Clave simétrica utilizada para autentificarse en un SAEF (KpsaID o KcID)	Véanse las cláusulas 8.2.2.1, 8.2.2.3
13	Clave simétrica utilizada para autentificarse en ESPrim (pairwiseESPrimKeyID)	Véase la cláusula 8.4.2.
14	Clave simétrica utilizada para la encriptación directa en las clases de seguridad ESData solo con encriptación o con firma y encriptación anidadas (formato genérico del identificador de clave simétrica)	Véase la cláusula 8.5.2
15	Clave simétrica utilizada para la encriptación de clave simétrica en las clases de seguridad ESData solo con encriptación o con firma y encriptación anidadas (formato genérico del identificador de clave simétrica)	Véase la cláusula 8.5.2
16	Clave simétrica utilizada para el HMAC en la clase de seguridad ESData solo con firma (formato genérico del identificador de clave simétrica)	Véase la cláusula 8.5.2
30	Certificado de clave pública bruta utilizado en el TLS: (identificador de clave pública)	10.1.2
31	Certificado de dispositivo utilizado en el TLS (identificador exclusivo a nivel mundial de equipo de *hardware*)	10.1.1.4
32	Certificado de CSE-ID utilizado en el TLS (CSE-ID)	[UIT-T Y.4500.1]
33	Certificado de AE-ID utilizado en el TLS (AE-ID)	[UIT-T Y.4500.1]
41	Certificado de clave pública bruta utilizado para la gestión de claves RSA o ECDH en las clases de seguridad ESData solo con encriptación o con firma y encriptación anidadas (identificador de clave pública)	10.1.2
42	Certificado de dispositivo utilizado para la gestión de claves RSA o ECDH en las clases de seguridad ESData solo con encriptación o con firma y encriptación anidadas (identificador exclusive a nivel mundial de equipo de *hardware*)	10.1.1.4
43	Certificado de CSE-ID utilizado para la gestión de claves RSA o ECDH en las clases de seguridad ESData solo con encriptación o con firma y encriptación anidadas (CSE-ID)	[UIT-T Y.4500.1]
44	Certificado de AE-ID utilizado para la gestión de claves RSA o ECDH en las clases de seguridad ESData solo con encriptación o con firma y encriptación anidadas (AE-ID)	[UIT-T Y.4500.1]
51	Certificado de clave pública bruta utilizado para la gestión de claves RSA o ECDH en la clase de seguridad ESData solo con firma: (identificador de clave pública)	10.1.2
52	Certificado de dispositivo utilizado para las firmas RSA o ECDH en la clase de seguridad ESData solo con firma: (identificador exclusivo a nivel mundial de equipo de *hardware*)	10.1.1.4
53	Certificado de CSE-ID utilizado para la gestión de claves RSA o ECDH en la clase de seguridad ESData solo con firma (CSE-ID)	[UIT-T Y.4500.1]
54	Certificado de AE-ID utilizado para la gestión de claves RSA o ECDH en la clase de seguridad ESData solo con firma (AE-ID)	[UIT-T Y.4500.1]
NOTA: La forma correspondiente al identificador del tipo de credencial se describe entre paréntesis.		

12.3.2.2 sec:devMgmtID

El tipo de enumeración sec:devMgmtID se utiliza en sec:deviceConfigURI como identificador de la tecnología de gestión de dispositivos empleada para la configuración de los dispositivos de campo (véase [UIT-T Y.4500.22]). El tipo de enumeración sec:devMgmtID también se utiliza en el elemento *devMgmtID* del elemento *devCfgArgs* del elemento *cmdArgs* del elemento *cmdDescription* de la instrucción de control del cliente MEF (véase la cláusula 8.3.9.8) para indicar el protocolo DM que se utilizará en la configuración de los dispositivos [UIT-T Y.4500.22]. *cmdDescription* es un atributo del tipo de recurso <*mefClientCmd*> especificado en [UIT-T Y.4500.32]). En el Cuadro 12.3.2.2-1 se describe la manera en que se interpreta el tipo de enumeración sec:devMgmtID.

Cuadro 12.3.2.2-1 – Interpretación del tipo de enumeración sec –devMgmtID

Valor	Interpretación	Nota
1	OMA DMv1.3	Véase [b-ITU-T Y.4500.5]
2	OMA DMv2.0	Véase [b-ITU-T Y.4500.5]
3	OMA LwM2M	Véase [b-ITU-T Y.4500.5]
4	BBF TR-069	Véase [b-ITU-T Y.4500.6]

12.3.2.3 sec:cmdClassID

El tipo de enumeración sec:cmdClassID se utiliza en el elemento *cmdDescription* de la instrucción de control del cliente MEF (véase la cláusula 8.3.9.4) para indicar la *cmdClass* de la *cmdDescription*. La *cmdDescription* es un atributo del tipo de recurso <mefClientCmd> especificado en [UIT-T Y.4500.32]). En el Cuadro 12.3.2.3-1 se describe la manera en que se interpreta el tipo de enumeración sec:cmdClassID.

Cuadro 12.3.2.3-1 – Interpretación del tipo de enumeración sec:cmdClassID

Valor	Interpretación	Nota
0	NO_MORE_COMMANDS	La clase de instrucción de control se especifica en la cláusula 8.3.9.6
1	CERT_PROV	La clase de instrucción de control se especifica en la cláusula 8.3.9.7 La provisión de certificados se especifica en la cláusula 8.3.6
2	DEV_CFG	La clase de instrucción de control se especifica en la cláusula 8.3.9.8. La configuración de dispositivos se especifica en [UIT-T Y.4500.22]
3	MO_NODE	La clase de instrucción de control se especifica en la cláusula 8.3.9.9

12.3.2.4 sec:cmdStatusCode

El elemento *cmdStatusCode* utiliza el tipo de enumeración sec:cmdStatusCode para indicar el estado de una instrucción de control del cliente MEF. El *cmdStatus* es un atributo del tipo de recurso <*mefClientCmd*> especificado en [UIT-T Y.4500.32]. En el Cuadro 12.3.2.4-1 se describe la manera en que se interpreta el tipo de enumeración sec:cmdStatusCode.

Cuadro 12.3.2.4-1 – Interpretación del tipo de enumeración sec –cmdStatusCode

Valor	Interpretación	Nota
10	MEF_CLIENT_CMD_ISSUED	Véase 8.3.9.5.2
11	MEF_CLIENT_CMD_REISSUED	Véase 8.3.9.5.3
20	MEF_CLIENT_CMD_OK	Véase 8.3.9.5.4
40	MEF_CLIENT_CMD_ REPEATED_CMD_ID	Véase 8.3.9.5.5
41	MEF_CLIENT_CMD_CLASS_NOT_SUPPORTED	Véase 8.3.9.5.6
42	MEF_CLIENT_CMD_BAD_ ARGUMENTS	Véase 8.3.9.5.7
43	MEF_CLIENT_CMD_UNACCEPTABLE_ARGUMENTS	Véase 8.3.9.5.8
100	MEF_CLIENT_CMD_CERT_PROV_SERVER_ERROR	Véase 8.3.9.5.9
101	MEF_CLIENT_CMD_CERT_PROV_CLIENT_ERROR	Véase 8.3.9.5.10
201	MEF_CLIENT_CMD_DEV_CFG_SERVER_ERROR	Véase 8.3.9.5.11
202	MEF_CLIENT_CMD_DEV_CFG_CLIENT_ERROR	Véase 8.3.9.5.12
300	MEF_CLIENT_CMD_MO_NODE_NOT_FOUND	Véase 8.3.9.5.13
301	MEF_CLIENT_CMD_MO_NODE_TYPE_CONFLICT	Véase 8.3.9.5.14
302	MEF_CLIENT_CMD_MO_NODE_BAD_ARGS	Véase 8.3.9.5.15
303	MEF_CLIENT_CMD_MO_NODE_UNACCEPTABLE_ARGS	Véase 8.3.9.5.16
304	MEF_CLIENT_CMD_MO_NODE_INCONSISTENT_CONFIG	Véase 8.3.9.5.17
305	MEF_CLIENT_CMD_MO_NODE_EXECUTION_ERROR	Véase 8.3.9.5.18

12.3.2.5 sec:certProvProtocolID

El tipo de enumeración sec:certProvProtocolID se utiliza en relación con el elemento *certProvProtocolID* del elemento *certProvCmdArgs* del elemento *cmdArgs* del elemento *cmdDescription* de la instrucción de control del cliente MEF (véase la cláusula 8.3.9.7) para indicar el protocolo de provisión de certificados que debe emplearse. La *cmdDescription* es un atributo del tipo de recurso <*mefClientCmd*> especificado en [UIT-T Y.4500.32]).

Cuadro 12.3.2.5-1 – Interpretación del tipo de enumeración sec:certProvProtocolID

Valor	Interpretación	Nota
1	EST	Véase la cláusula 8.3.6.2
2	SCEP	Véase la cláusula 8.3.6.3

12.3.2.6 sec:certSubjectType

El tipo de enumeración sec:certSubjectType se utiliza en relación con el elemento *certSubjectType* del elemento c*ertProvCmdArgs* del elemento *cmdArgs* del elemento *cmdDescription* de la instrucción de control del cliente MEF (véase la cláusula 8.3.9.7) para indicar si el sujeto del certificado provisionado será un nodo, una CSE o una AE. La *cmdDescription* es un atributo del tipo de recurso <*mefClientCmd*> especificado en [UIT-T Y.4500.32]).

Cuadro 12.3.2.6-1 – Interpretación del tipo de enumeración sec:certSubjectType

Valor	Interpretación	Nota
1	Node-ID	Véase [UIT-T Y.4500.1], cláusula 7.1.5
2	CSE-ID	Véase [UIT-T Y.4500.1], cláusula 7.2
3	AE-ID	Véase [UIT-T Y.4500.1], cláusula 7.2

12.3.2.7 sec:objectTypeID

El tipo de enumeración sec:objectTypelID se utiliza en relación con el elemento *objectTypelID* del elemento *MONodeCmdArgs* del elemento *cmdArgs* del elemento *cmdDescription* de la instrucción de control del cliente MEF (véase la cláusula 8.3.9.9) para indicar el tipo de un nodo MO. La *cmdDescription* es un atributo del tipo de recurso <*mefClientCmd*> especificado en [UIT-T Y.4500.32]).

Cuadro 12.3.2.7-1 – Interpretación del tipo de enumeración sec:certProvProtocolID

Valor	Interpretación	Nota
1	[*authenticationProfile*]	Véase [UIT-T Y.4500.22], cláusulas 7.1.4 y 7.2.4
2	[*trustAnchorCred*]	Véase [UIT-T Y.4500.22], cláusulas 7.1.6 y 7.2.6
3	[*MAFClientRefCfg*]	Véase [UIT-T Y.4500.22], cláusulas 7.1.7 y 7.2.7

12.4 Tipos de datos oneM2M específicos de seguridad complejos

12.4.1 Datos de configuración de los clientes MAF y MEF

En el Cuadro 12.4.1-1 se especifica la asignación de los tipos de datos a los cuatro contenedores de datos que se utilizan en los procedimientos de configuración del registro de clientes y del registro de claves MAF y MEF. Cabe señalar que estos contenedores de datos no se definen en forma de tipos de recursos, ya que no se puede acceder a la información a distancia. Los elementos de información de estos contenedores se gestionan mediante procedimientos de gestión de dispositivos (véase [UIT-T Y.4500.22]) o mediante provisión manual. En el Cuadro 12.4.1-1 se enumeran los tipos utilizados en los procedimientos de configuración del registro MAF y MEF.

Cuadro 12.4.1-1 – Tipos utilizados en los procedimientos de configuración del registro MAF y MEF

Nombre del contenedor de datos	Usos	Tipo de datos	Notas
mefClientRegCfg	Configuración de registro de cliente MEF, véase la cláusula 8.3.7.2	sec:clientRegCfg	Véase la cláusula 12.4.2
mafClientRegCfg	Configuración de registro de cliente MAF, véase la cláusula 8.8.3.2		
mefKeyRegCfg	Configuración de registro de clave MEF, véase la cláusula 8.3.7.3	sec:keyRegCfg	Véase la cláusula 12.4.3
mafKeyRegCfg	Configuración de registro de clave MAF, véase la cláusula 8.8.3.3		

12.4.2 sec:clientRegCfg

El tipo de datos sec:clientRegCfg se aplica a los contenedores de datos *mefClientRegCfg* y *mafClientRegCfg* utilizados en la configuración del registro de cliente MEF y la configuración del

registro de cliente MAF (véanse las cláusulas 8.3.7.2 y 8.8.3.2, respectivamente). En el Cuadro 12.4.2-1 se define el tipo sec:clientRegCfg.

Cuadro 12.4.2-1 – Definición del tipo sec:clientRegCfg

Elemento de trayecto	Tipo de elemento	Multiplicidad	Notas
expirationTime	m2m:timestamp	0..1	[UIT-T Y.4500.4]
labels	m2m:labels	0..1	[UIT-T Y.4500.4]
fqdn	xs:anyURI	1	
adminFQDN	xs:anyURI	1	
httpPort	xs:unsignedByte	0..1	
coapPort	xs:unsignedByte	0..1	
websocketPort	xs:unsignedByte	0..1	

12.4.3 sec:keyRegCfg

El tipo de datos sec:keyRegCfg se aplica a los contenedores de datos *mefKeyRegCfg* y *mafKeyRegCfg* utilizados en la configuración del registro de clave MEF y en la configuración del registro de clave MAF (véanse las cláusulas 8.3.7.3 y 8.8.3.3, respectivamente). En el Cuadro 12.4.3-1 se define el tipo sec:keyRegCfg.

Cuadro 12.4.3-1 – Definición del tipo sec:keyRegCfg

Elemento de trayecto	Tipo de elemento	Multiplicidad	Notas
expirationTime	m2m:timestamp	0..1	[UIT-T Y.4500.4]
labels	m2m:labels	0..1	[UIT-T Y.4500.4]
adminFQDN	xs:anyURI	1	
SUID	m2m:suid	1	[UIT-T Y.4500.4]
targetIDs	m2m:listOfM2MID	0..1	[UIT-T Y.4500.4]

12.4.4 sec:cmdDescription

El elemento *cmdDescription* utiliza el tipo complejo sec:cmdDescription para describir una instrucción de control del cliente MEF, que se describe en la cláusula 8.3.9.5. La *cmdDescription* es un atributo del tipo de recurso <*mefClientCmd*> especificado en [UIT-T Y.4500.32]. En el Cuadro 12.4.4-1 se define el tipo sec:cmdDescription.

Cuadro 12.4.4-1 – Definición del tipo sec:cmdDescription

Elemento de trayecto	Tipo de elemento	Multiplicidad	Notas
cmdClassID	sec:cmdClassID	1	Véase la cláusula 12.3.2.3
cmdArgs	sec:cmdArgs	1	Véase la cláusula 12.4.5
targetID	m2m:ID	1	[UIT-T Y.4500.4]

12.4.5 sec:cmdArgs

El elemento *cmdArgs* del tipo de datos sec:cmdDescription utiliza el tipo complejo sec:cmdArgs. En el Cuadro 12.4.5-1 se define el tipo sec:cmdArgs.

Cuadro 12.4.5-1 – Definición del tipo sec:cmdArgs

Elemento de trayecto	Tipo de elemento	Multiplicidad	Notas
noMoreCmdArgs	sec:noMoreCmdArgs	0..1	Véase la cláusula 12.4.6
certProvCmdArgs	sec:certProvCmdArgs	0..1	Véase la cláusula 12.4.7
devCfgCmdArgs	sec:devCfgCmdArgs	0..1	Véase la cláusula 12.4.8
MONodeCmdArgs	sec:MONodeCmdArgs	0..1	Véase la cláusula 12.4.9

Este tipo consiste en una xs:choice. Deberá contener los elementos indicados en una sola fila del Cuadro12.4.5-1.

12.4.6 sec:noMoreCmdArgs

El tipo complejo sec:noMoreCmdArgs se utiliza en sec:cmdDescription. En el Cuadro 12.4.6-1 se define el tipo sec:noMoreCmdArgs.

Cuadro 12.4.6-1 – Definición del tipo sec:noMoreCmdArgs

Elemento de trayecto	Tipo de elemento	Multiplicidad	Notas
retryDuration	xs:duration	1	

12.4.7 sec:certProvCmdArgs

El tipo complejo sec:certProvCmdArgs se utiliza en sec:cmdDescription. En el Cuadro 12.4.7-1 se define el tipo sec:certProvCmdArgs.

Cuadro 12.4.7-1 – Definición del tipo sec:certProvCmdArgs

Elemento de trayecto	Tipo de elemento	Multiplicidad	Notas
certProvProtocolID	sec:certProvProtocolID	1	Véase la cláusula 12.3.2.5
URI	xs:anyURI	1	
certSubjectType	sec:certSubjectType	1	Véase la cláusula 12.3.2.6
certSubjectID	xs:union of m2m:nodeID y m2m:ID	1	Véase [UIT-T Y.4500.4], cláusula 6.3.3

12.4.8 sec:devCfgCmdArgs

El tipo complejo sec:devCfgCmdArgs se utiliza en sec:cmdDescription. En el Cuadro 12.4.8-1 se define el tipo sec:devCfgCmdArgs.

Cuadro 12.4.8-1 – Definición del tipo sec:devCfgCmdArgs

Elemento de trayecto	Tipo de elemento	Multiplicidad	Notas
deviceConfigURI	sec:deviceConfigURI	1	Véase la cláusula 12.2

12.4.9 sec:MONodeCmdArgs

El tipo complejo sec:MONodeCmdArgs se utiliza en sec:cmdDescription. En el Cuadro 12.4.9-1 se define el tipo sec:MONodeCmdArgs.

Cuadro 12.4.9-1 – Definición del tipo sec:MONodeCmdArgs

Elemento de trayecto	Tipo de elemento	Multiplicidad	Notas
objectPath	xs:anyURI	1	
objectTypeID	sec:objectTypeID	1	Véase la cláusula 12.3.2.7
objectTypeSpecifcArgs	sec:authProfileMONodeArgs	0..1	Véase la cláusula 12.4.10

12.4.10 sec:authProfileMONodeArgs

El tipo complejo sec:authProfileMONodeArgs se utiliza en sec:MONodeCmdArgs. En el Cuadro 12.4.10-1 se define el tipo sec:authProfileMONodeArgs.

Cuadro 12.4.10-1 – Definición del tipo sec:authProfileMONodeArgs

Elemento de trayecto	Tipo de elemento	Multiplicidad	Notas
SUID	m2m:suid	1	Véase [UIT-T Y.4500.4], cláusula 6.3.4.2.39.

Anexo A

Anexo en blanco

Este Anexo se ha dejado deliberadamente en blanco.

Anexo B

Anexo en blanco

Este Anexo se ha dejado deliberadamente en blanco.

Anexo C

Protocolos de seguridad asociados a tecnologías SE específicas

(El presente anexo es parte integrante de la Recomendación.)

C.0 Introducción

El entorno seguro que soporta las funciones de seguridad especificadas en el marco del sistema oneM2M proporciona cierto nivel y cierto tipo de protección (por ejemplo, protección de la integridad, confidencialidad, resistencia a la manipulación) a la información contenida en él, independientemente del método de protección aplicado (por ejemplo, una UICC, un elemento de seguridad integrado, un TEE, etc.). La administración de su contenido depende de la implementación y se basa en normas existentes en relación con determinadas tecnologías de entorno seguro. A continuación se enumeran algunas de ellas a título informativo.

C.1 UICC

En el caso de la UICC (SE conforme con [ETSI TS 102 671]), se soportarán los mecanismos por vía aérea (OTA) especificados en [ETSI TS 102 225] y [ETSI TS 102 226], y sus ampliaciones [ETSI TS 131 115], [ETSI TS 131 116], para redes subyacentes 3GPP, o [ARIB STD-T64-C.S0078-0] y [ARIB STD-T64 C.S0079-0], para redes subyacentes 3GPP2, a fin de permitir la administración de seguridad de los datos sensibles de la capa de servicios M2M. La UICC proporciona el nivel de protección más alto (nivel 3) contra ataques, de acuerdo con la clasificación de los niveles de protección.

C.2 Otro elemento seguro y elemento seguro incorporado compatible con la interfaz basada en ISO 7816

En caso de que el entorno seguro se implemente como un elemento de seguridad o como un elemento de seguridad incorporado compatible con una interfaz basada en ISO/IEC 7816 [ISO/IEC 7816-4], cabe citar como ejemplo de administración a distancia la administración a distancia conforme con las especificaciones de GlobalPlatform [b-GP DTSERAM]. Un elemento de seguridad incorporado proporciona el nivel de protección más alto (nivel 3) contra ataques, de acuerdo con la clasificación de los niveles de protección.

C.3 Entorno de ejecución confiable

En caso de que el entorno seguro se implemente como un entorno de ejecución confiable (TEE) conforme con GlobalPlatform [b-GP TEESystem], se soportará la administración a distancia con arreglo a las especificaciones de GlobalPlatform sobre administración a distancia [b-GP TEEAdmin]. El TEE proporciona un nivel de protección medio (nivel 3) contra ataques, de acuerdo con la clasificación de los niveles de protección.

C.4 Vinculación entre el SE y la CSE

Cuando el SE se implementa como un elemento de seguridad independiente compatible con [ETSI TS 102 221], el canal seguro de plataforma a plataforma especificado en [ETSI TS 102 484] facilita la vinculación lógica entre el SE y una CSE o AE específica. Esto también protege la información que se intercambia entre el SE y la entidad asociada en interfaces físicas, por lo que se recomienda para los dispositivos que están físicamente expuestos a los atacantes.

Anexo D

Marco de seguridad UICC para dar soporte a los servicios oneM2M

(El presente anexo es parte integrante de la Recomendación.)

D.0 Introducción

Este anexo es aplicable cuando una UICC (un tipo de elemento de seguridad independiente conforme con [ETSI TS 102 221] y [ETSI TS 102 671]) participa en la seguridad de la capa de servicios M2M, ya sea solo como medio para efectuar la provisión previa del material relativo a la capa de servicios M2M en los dispositivos/pasarelas M2M, o también como un entorno seguro en un dispositivo/pasarela M2M.

Concretamente, la participación de una UICC en la seguridad oneM2M puede abarcar cualquiera de los siguientes pasos:

Provisión previa de credenciales iniciales en los nodos M2M a través de cualquiera de los métodos siguientes:

Provisión previa y administración simples del material relativo a los servicios M2M (credenciales iniciales y otros parámetros provisionados previamente), es decir, provisión de servicios M2M basada en UICC.

Apoyo a la inicialización asistida mediante infraestructura de credenciales simétricas M2M mediante la derivación de credenciales simétricas de red de acceso almacenadas en la UICC, utilizando la GBA.

Derivación de una clave de asociación de seguridad directamente a partir de credenciales simétricas de red de acceso, utilizando la GBA. Cabe señalar que este proceso es compatible con una aplicación de acceso de red disponible en la UICC, independientemente de la presencia de la estructura de información especificada en el presente Anexo.

El soporte al suministro de información sobre el abono a un servicio M2M por parte de la UICC se indicará en el cuadro de servicios M2M para el correspondiente abono a un servicio M2M, como se especifica en el presente anexo.

El soporte a la derivación de claves mediante la GBA que puedan utilizarse para la inicialización o la asociación de seguridad se indicará siempre en el cuadro de servicios de la aplicación UICC del operador de la red de acceso que da soporte a la infraestructura GBA.

En el nivel más elemental, la provisión previa M2M basada en UICC requiere un marco interoperativo para almacenar y administrar la información conexa en la UICC. Para una interacción más importante, se necesita un marco que permita descubrir los servicios de la UICC disponibles para el nodo de campo M2M anfitrión. El objeto del presente Anexo es especificar ese marco, que permite la provisión previa del servicio inicial y la administración de seguridad a distancia de la información de abono mientras este esté vigente.

Es común un escenario en el que un nodo de campo M2M está dotado de una aplicación UICC que protege las credenciales de seguridad de la red de acceso y en que dichas credenciales se utilizan para derivar las credenciales de seguridad de la capa de servicios M2M destinadas a la inicialización de un servicio M2M o el establecimiento de una asociación de seguridad en la capa de servicios. Como esos escenarios requieren un acuerdo de confianza entre el operador de la red de acceso involucrado y el proveedor de servicios M2M, en esa situación el soporte que brinda la UICC a los servicios M2M se gestionará dentro del contexto de la aplicación de acceso de red asociada disponible en la UICC. En particular, el soporte de la UICC para la derivación de credenciales M2M mediante la GBA se indicará en la aplicación UICC del operador de la red de acceso. En la cláusula D.1 se ofrece información específica al respecto.

Incluso cuando las credenciales de la capa de servicios M2M no se derivan a partir de las credenciales de la red de acceso, es posible utilizar la UICC como un entorno seguro que protege debidamente las credenciales simétricas o asimétricas utilizadas para asegurar un nodo de campo M2M. En tales casos, la información de abono M2M y los métodos conexos constituyen una aplicación independiente que reside en una UICC, en el sentido de [ETSI TS 102 221]. En particular, en [ETSI TS 102 221] se especifican las propiedades independientes de aplicación de la interfaz UICC-terminal, tales como las características físicas y la estructura lógica.

NOTA – De conformidad con [ETSI TS 102 221], un terminal es la parte del nodo de campo M2M que contiene la UICC, por ejemplo, un módem de comunicación o un entorno de procesamiento de nodo M2M.

Las propiedades específicas de la aplicación del módulo de identidad del proveedor de servicios M2M que contiene credenciales simétricas se especifican en la cláusula D.2.

El almacenamiento de elementos de información M2M en la UICC y los procedimientos utilizados para entablar comunicaciones entre el nodo de campo M2M anfitrión y la UICC se ajustarán a las especificaciones del presente Anexo. En este Anexo se utilizan las abreviaturas y las reglas de codificación que se han definido en [ETSI TS 102 221].

D.1 Marco de servicios oneM2M basado en UICC de la red de acceso

D.1.1 Características del marco de servicio oneM2M basado en UICC de la red de acceso

El marco de servicios oneM2M basado en UICC de la red de acceso siempre está asociado a un único abono a servicios M2M y consta de un único DF, a saber, el DF_{1M2M}, que se ajusta a lo especificado en la cláusula D.1.3, implementado en el ADF de una aplicación de acceso de red disponible en la UICC. Esta situación se refiere al caso en que se ha establecido una relación de confianza entre el proveedor de servicios M2M y el operador de la red de acceso que posee el ADF anfitrión.

NOTA 1 – Esto no significa necesariamente que las credenciales de la red de acceso del correspondiente ADF se utilizan para derivar las credenciales de la capa de servicios M2M; por ejemplo, si bien un operador de la red de acceso puede denegar a un proveedor de servicios M2M la derivación a partir de las credenciales de red de acceso, aún puede acceder a brindar espacio en su UICC para efectuar la provisión previa de credenciales independientes o dar soporte a la inicialización del servicio asistida mediante infraestructura.

Pueden existir varios marcos de servicios oneM2M (DF_{1M2M}) en el ADF de un solo abono a la red de acceso, en caso de que varios abonos a servicios M2M independientes utilicen dicho abono a la red de acceso. Los identificadores de fichero del DF_{1M2M} en cualquier ADF se enumerarán en la entrada correspondiente en el EF_{DIR}, como se especifica en la cláusula D.1.2.

NOTA 2 – Un abono único a la capa de servicio M2M también puede utilizar múltiples redes de acceso; este tipo de abonos se benefician de una mejor provisión en un ADF específico, como se explica en la cláusula D.2.

El contenido de cualquier DF_{1M2M} en un ADF de una aplicación de red de acceso corresponderá a lo especificado en la cláusula D.1.3.

D.1.2 Descubrimiento del marco de servicios M2M para una UICC de la red de acceso

Cuando una aplicación de acceso a la red basada en una UICC soporta uno o varios abonos a servicios M2M, con un DF_{1M2M}, la entrada EF_{DIR} correspondiente a dicha aplicación de acceso a la red basada en una UICC contendrá los siguientes objetos de datos relacionados con M2M que figuran en los cuadros D.1 a D.3:

Objeto de datos del marco de servicios oneM2M: define la asociación entre el identificador de un abono a servicios M2M provisionado en el ADF y el DF correspondiente a ese abono M2M. Análogamente, cada abono a servicios M2M está asociado a un DF. En adelante, cada una de estos DF se denomina DF_{1M2M}.

La cantidad de objetos de datos del marco de servicios oneM2M será igual a la cantidad de abonos a servicios M2M provisionados en el ADF.

Cuadro D.1 – Codificación de los objetos de datos relacionados con oneM2M

Bytes	Longitud	Descripción	Situación
1	1	Etiqueta de plantilla opcional = "73"	Obligatorio
2	1	Longitud de la plantilla opcional = X	Obligatorio
3 a (2+X)	X	Plantilla opcional	X

Cuadro D.2 – Codificación de los objetos de datos relacionados con la plantilla opcional oneM2M

Bytes	Longitud	Descripción	Situación
1	1	Etiqueta del contenido de datos específica de los servicios oneM2M = "A2"	Obligatorio
2	1	Longitud del contenido de datos específica de los servicios M2M = Y	Obligatorio
3 a (2+Y)	Y	Contenido de los datos específico de los servicios M2M	Obligatorio

Cuadro D.3 – Codificación de los objetos de datos relacionados con el contenido de datos específico de los servicios oneM2M

Bytes	Longitud	Descripción	Situación
1	1	Etiqueta de provisión de servicios soportados oneM2M = "80"	Obligatorio
2	1	Longitud de la etiqueta de provisión de servicios soportados oneM2M = A	Obligatorio
3 a 4	2	Identificador de fichero dedicado M2M para el seguimiento de abono a servicios M2M	Obligatorio
5 a (A+2)	(A-2)	Identificador del abono M2M	Obligatorio

Codificación:

Identificador del fichero dedicado M2M:

Contiene el identificador de fichero del DF_{1M2M} asociado a la provisión del abono a servicios M2M que se ha identificado en el objeto de datos.

Identificador del abono M2M:

El identificador del abono a servicios M2M provisionado en el DF_{1M2M} se indica en el objeto de datos, codificado en formato binario.

D.1.3 Contenido de los ficheros a nivel del DF_{1M2M}

D.1.3.0 Introducción

En esta cláusula se especifican los EF para la provisión de servicios M2M específicos de un único proveedor de servicios M2M, y se definen las condiciones de acceso, los elementos de datos y la codificación. Los elementos de datos forman parte de un EF que representa una entidad lógica completa.

La estructura de fichero para DF_{1M2M} se ilustra en la Figura D.1.

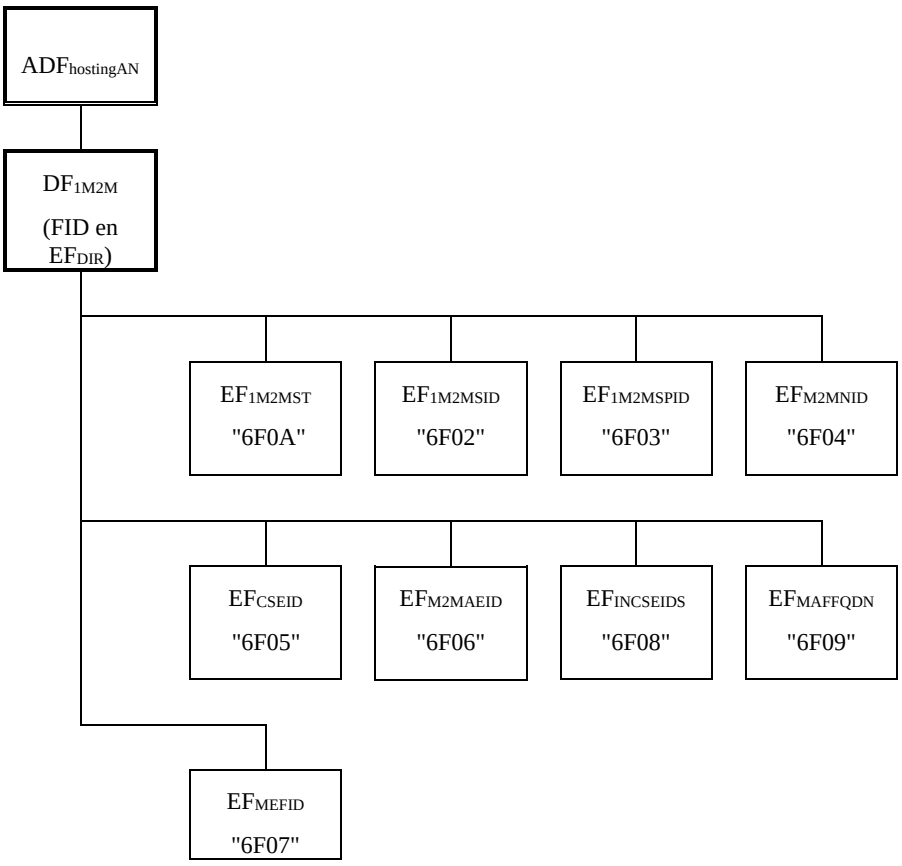


Figura D.1 – Identificadores de fichero y estructuras de directorio del DF_{1M2M} en un ADF de una aplicación de red de acceso anfitrión

D.1.3.1 EF_{1M2MST} (cuadro de servicios oneM2M)

En este EF se indican los servicios oneM2M opcionales a los que es posible abonarse. Si en el DF oneM2M no se indica que un servicio está disponible, el nodo de campo M2M anfitrión no seleccionará ese servicio. La presencia de este fichero es obligatoria si el abono conlleva la prestación de servicios opcionales.

Identificador: "6F0A"	Estructura: transparente	Obligatorio (M)
SFI: "0A"		
Tamaño del fichero: X bytes, X ≥ 1	Frecuencia de actualización: baja	

Condiciones de acceso:

READ (Leer)	ALW
UPDATE (Actualizar)	ADM
DEACTIVATE (Desactivar)	ADM
ACTIVATE (Activar)	ADM

Bytes	Descripción	Obligatorio/Opcional	Longitud
1	Servicios núms.1 a 8	Obligatorio	1 byte
2	Servicios núms. 9 a 16	Opcional	1 byte
3	Servicios núms. 17 a 24	Opcional	1 byte
4	Servicios núms. 25 a 32	Opcional	1 byte
etc.			
X	Servicios núms. (8X-7) a (8X)	Opcional	1 byte

-Servicios

Contenido:		
	Servicio núm. 1	Provisión del CSE-ID local
	Servicio núm. 2	Provisión de la lista de IN-CSE-ID
	Servicio núm. 3	Provisión del FQDN de la MAF
	Servicio núm. 4	Provisión de la lista de AE-ID M2M local
	Servicio núm. 5	Inicialización: provisión de dirección MEF
	Servicio núm. 6	Información del M2M-Node-ID
	Servicio núm. 7	Provisión segura de la GBA (véase la nota)
	Servicio núm. 8	Conexión segura de la GBA (véase la nota)

NOTA: Los servicios núms. 7 y 8 solo pueden estar disponibles en un cuadro de servicios oneM2M ubicado en un DF_{1M2M} alojado en el ADF de la aplicación de acceso a la red de la que se espera derivar las credenciales de la capa de servicios M2M.

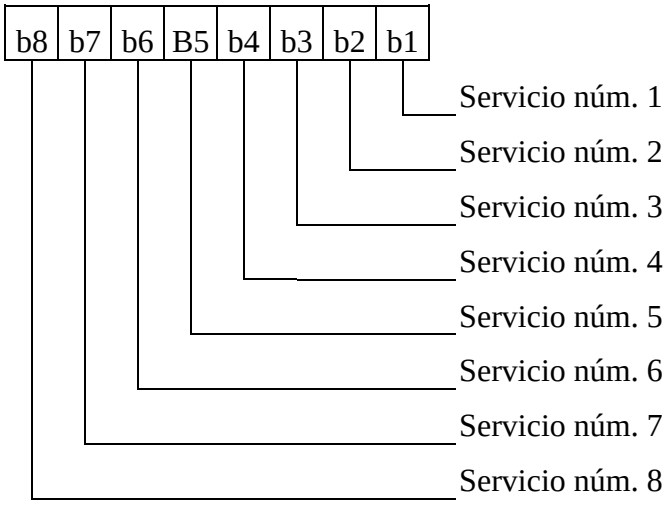
El EF contendrá al menos un byte. Podrán incluirse más bytes, y en caso de que el EF contenga un byte opcional, será obligatorio que antes de ese byte opcional figuren todos los demás bytes. En el futuro podrán añadirse otros servicios, que se codificarán con bytes adicionales en el EF. La codificación será como se muestra a continuación:

Se utiliza 1 bit para codificar cada servicio:
bit = 1: servicio disponible;
bit = 0: servicio no disponible.

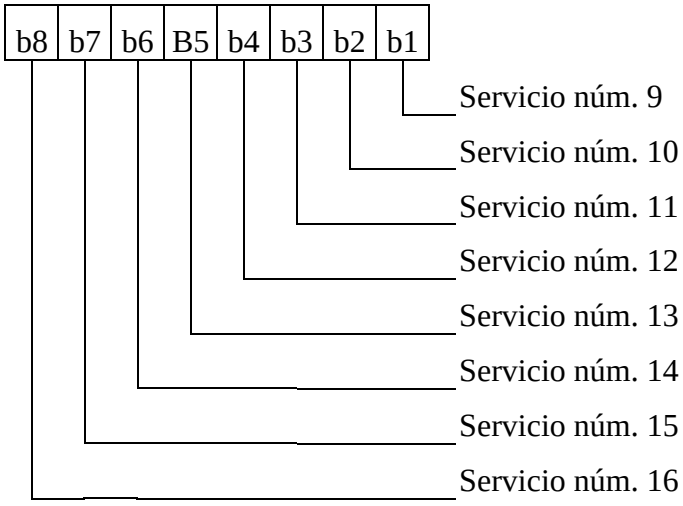
Por servicio disponible se entiende que el abono a servicios M2M provisionado en el DF o ADF de que se trate puede dar soporte a dicho servicio y que el usuario del abono a servicios M2M puede utilizarlo.

Por servicio no disponible se entiende que el usuario del abono a servicios M2M no podrá utilizar el servicio, aun cuando dicho abono soporte ese servicio.

Primer byte:



Segundo byte:



etc.

D.1.3.2 $EF_{1M2MSID}$ (identificador de abono oneM2M)

Este EF contiene el identificador de abono oneM2M, a saber, M2M-Sub-ID. En este EF figurará únicamente un objeto TLV.

Identificador: "6F02"	Estructura: transparente		Obligatorio
SFI: "02"			
Tamaño del fichero: X bytes	Frecuencia de actualización: baja		
Condiciones de acceso: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM			
Bytes	Descripción	Obligatorio/Opcional	Longitud
1	Objeto de datos TLV del identificador de abono M2M	Obligatorio	X bytes

El campo de valor del identificador de bono M2M contendrá el M2M-Sub-ID codificado como se especifica en [UIT-T Y.4500.4]. El valor de etiqueta del objeto de datos TLV del identificador de abono oneM2M será "80".

D.1.3.3 $EF_{1M2MSPID}$ (identificador de proveedor de servicios oneM2M)

Este EF contiene el identificador de proveedor de servicios oneM2M, M2M-SP-ID, del proveedor de servicios M2M del abono en $EF_{1M2MSID}$. En este EF figurará únicamente un objeto TLV.

Identificador: "6F03"	Estructura: transparente		Obligatorio
SFI: '03'			
Tamaño del fichero: X bytes	Frecuencia de actualización: baja		
Condiciones de acceso: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM			
Bytes	Descripción	Obligatorio/Opcional	Longitud
1	Objeto de datos TLV del M2M-SP-ID	Obligatorio	X bytes

El campo de valor del M2M-SP-ID contendrá el M2M-SP-ID codificado con arreglo a los especificado en [UIT-T Y.4500.4]. El valor de etiqueta del objeto de datos TLV del M2M-SP-ID será "80".

D.1.3.4 EF_{M2MNID} (identificador de nodo M2M)

Este EF contiene el M2M-Node-ID que da soporte a la CSE local. Puede utilizarse para vincular lógicamente una UICC a un nodo M2M específico. Si el servicio núm. 6 está "disponible", este fichero deberá estar presente. En este EF figurará únicamente un objeto TLV.

Identificador: "6F04"	Estructura: transparente	Opcional
SFI: "04"		
Tamaño del fichero: X bytes	Frecuencia de actualización: baja	
Condiciones de acceso: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Descripción	Obligatorio/Opcional	Longitud
1 a X	Objeto TLV del M2M-Node-ID	Obligatorio	X bytes

El campo de valor del M2M-Node-ID contendrá el M2M-Node-ID codificado con arreglo a lo especificado en [UIT-T Y.4500.4].

D.1.3.5 EF_{CSEID} (Identificador CSE local)

Este EF contiene el identificador CSE local, CSE-ID, correspondiente al nodo de campo M2M asociado al abono en $EF_{1M2MSID}$. De estar presente, el nodo de campo M2M utiliza este fichero para efectuar la provisión previa del CSE-ID. Si el servicio núm. 1 está "disponible", este fichero deberá estar presente. En este EF figurará únicamente un objeto TLV.

Identificador: "6F05"	Estructura: transparente	Opcional
SFI: "05"		
Tamaño del fichero: X bytes	Frecuencia de actualización: baja	
Condiciones de acceso: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Descripción	Obligatorio/Opcional	Longitud
1	Objeto de datos TLV del CSE-ID	Obligatorio	X bytes

TLV del CSE-ID

Contenido:

El campo de valor del CSE-ID contendrá el CSE-ID local en forma de URI.

Codificación:

El URI se codificará en una cadena de octetos conforme con las reglas de codificación UTF-8 especificadas en [IETF RFC 3629]. El valor de etiqueta del objeto de datos TLV del URI será "80".

D.1.3.6 $EF_{M2MAE\text{-}ID}$ (lista de identificadores de aplicaciones M2M)

Este EF contiene la lista de identificadores de aplicaciones M2M (AE-ID) para los abonos M2M locales que sean compatibles con el abono en $EF_{1M2MSID}$. Si el servicio núm. 4 está "disponible", este fichero deberá estar presente.

Identificador: "6F06"	Estructura: fija lineal		Opcional
SFI: "06"			
Longitud del registro: X bytes		Frecuencia de actualización: baja	
Condiciones de acceso: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM			
Bytes	Descripción	Obligatorio/Opcional	Longitud
1 a X	Objeto de datos LV del AE-ID M2M	Obligatorio	X bytes

LV del AE-ID M2M

Contenido:

El campo de valor contendrá el AE-ID M2M en forma de URI.

Codificación:

El URI se codificará en una cadena de octetos conforme con las reglas de codificación UTF-8 especificadas en [IETF RFC 3629].

D.1.3.7 $EF_{INCSEIDS}$ (lista de identificadores IN-CSE M2M)

Este EF contiene una lista de IN-CSE-ID provisionados previamente que se utilizan para determinar el siguiente punto de contacto tras la provisión o la inicialización de un servicio M2M. Si el servicio núm. 2 está "disponible", este fichero deberá estar presente.

Identificador: "6F08"	Estructura: fija lineal		Opcional
Longitud de registro: X bytes		Frecuencia de actualización: baja	
Condiciones de acceso: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM			
Bytes	Descripción	Obligatorio/Opcional	Longitud
1 a X	Objeto de datos LV del IN-CSE-ID	Obligatorio	X bytes

LV del IN-CSE-ID

Contenido:

El campo de valor contendrá el IN-CSE-ID en forma de URI.

Codificación:

El URI se codificará en una cadena de octetos conforme con las reglas de codificación UTF-8 especificadas en [IETF RFC 3629].

D.1.3.8 $EF_{MAFFQDN}$ (MAF-FQDN)

Este EF se utiliza para efectuar la provisión previa del FQDN de la MAF que se utilizará para la conexión a servicios M2M tras la inicialización de un servicio M2M. Si el servicio núm. 3 está "disponible", este fichero deberá estar presente. En este EF figurará únicamente un objeto TLV.

Identificador: "6F09"	Estructura: Transparente	Opcional
Longitud: X bytes	Frecuencia de actualización: baja	
Condiciones de acceso: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Descripción	Obligatorio/Opcional	Longitud
1	Objeto de datos TLV del FQDN de la MAF	Obligatorio	X bytes

FQDN de la MAF

Contenido:

Dirección FQDN de la MAF.

Codificación:

El MAF-FQDN se codificará en una cadena de octetos conforme con las reglas de codificación UTF-8 especificadas en [IETF RFC 3629]. El valor de etiqueta del objeto de datos TLV del FQDN de la MAF será "80".

D.1.3.9 EF_{MEFID} (identificador de la función de inscripción M2M)

Este EF contiene una o varias direcciones de la función de inscripción M2M. El primer registro que figura en el EF se considerará de máxima prioridad; el último, de menor prioridad. Si el servicio núm. 5 está "disponible", este fichero deberá estar presente.

Identificador: "6F07"	Estructura: fija lineal	Opcional
Longitud del registro: X bytes	Frecuencia de actualización: baja	
Condiciones de acceso: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Descripción	Obligatorio/Opcional	Longitud
1 a X	Objeto de datos LV de la dirección MEF	Obligatorio	X bytes

Objeto de datos LV de la dirección MEF

Contenido:

Dirección de la MEF, en forma de un FQDN, una dirección IPv4 o una dirección IPv6.

Codificación:

El formato del objeto de datos es el siguiente:

Campo	Longitud (bytes)
Longitud	1
Tipo de dirección	1
Dirección MEF	Longitud de la dirección

Tipo de dirección: tipo de dirección MEF.

Este campo se fijará en el tipo de dirección MEF de acuerdo con los siguientes parámetros:

Valor	Nombre
0x00	FQDN
0x01	IPv4
0x02	IPv6
Los demás valores están reservados	

Dirección MEF: dirección de la función de inicialización de servicios M2M.

Este campo corresponderá a la dirección de la función de inscripción M2M. Cuando el tipo MEF se fija en 0x00, la dirección MEF correspondiente se codificará en una cadena de octetos conforme con las reglas de codificación UTF-8 especificadas en [IETF RFC 3629].

Los bytes sin utilizar se pondrán en "FF".

D.2 Aplicación del módulo de servicios oneM2M (1M2MSM) para credenciales simétricas en la UICC

D.2.0 Introducción

En esta cláusula se define el módulo de servicios oneM2M (1M2MSM), una aplicación utilizada para las funcionalidades de seguridad de la capa de servicios oneM2M y la provisión de los abonos sobre la base de credenciales simétricas. Esta aplicación reside en la UICC, una tarjeta IC especificada en [ETSI TS 102 221]. En particular, en [ETSI TS 102 221] se especifican las propiedades independientes de aplicación de la interfaz UICC-terminal, como las características físicas y la estructura lógica. Un sola UICC puede contener varios ADF 1M2MSM, correspondientes a abonos a servicios oneM2M independientes.

D.2.1 Estructura de los ficheros de la aplicación del módulo de servicios oneM2M

En esta cláusula se especifican los EF de la capa de servicios oneM2M en los que se definen las condiciones de acceso, los elementos de datos y la codificación. Un elemento de datos forma parte de un EF que representa una entidad lógica completa.

D.2.1.1 Contenido de los ficheros UICC a nivel del fichero maestro (MF)

Los ficheros a nivel del MF en la UICC son independientes de la aplicación, como se especifica en [ETSI TS 102 221]. Solo los ficheros EF_{DIR} y EF_{ICCID} son obligatorios en la UICC a efectos de las aplicaciones 1M2MSM. En cualquier caso, todos los ficheros deberán ajustarse a lo especificado en [ETSI TS 102 221].

D.2.1.2 Contenido de los ficheros a nivel del fichero dedicado de aplicación (ADF) 1M2MSM

Los EF del ADF 1M2MSM contienen información relacionada con los abonos oneM2M necesaria para los nodos de campo M2M que operan en un entorno oneM2M. Se seleccionará este ADF utilizando su AID y la información en el EF_{DIR}. El AID de las aplicaciones 1M2MSM se construirá de conformidad con lo especificado en [ETSI TS 101 220].

NOTA – Puede utilizarse el ETSI RID en el marco del sistema oneM2M mientras se asigna un RID específico a oneM2M en [b-ISO/IEC 7816-5].

Los identificadores de fichero "6F1X" (para los EF), "5F1X" y "5F2X" (para los DF), en los que X varía entre "0" y "F", se reservan en el ADF 1M2MSM para usos administrativos por el expedidor de la tarjeta.

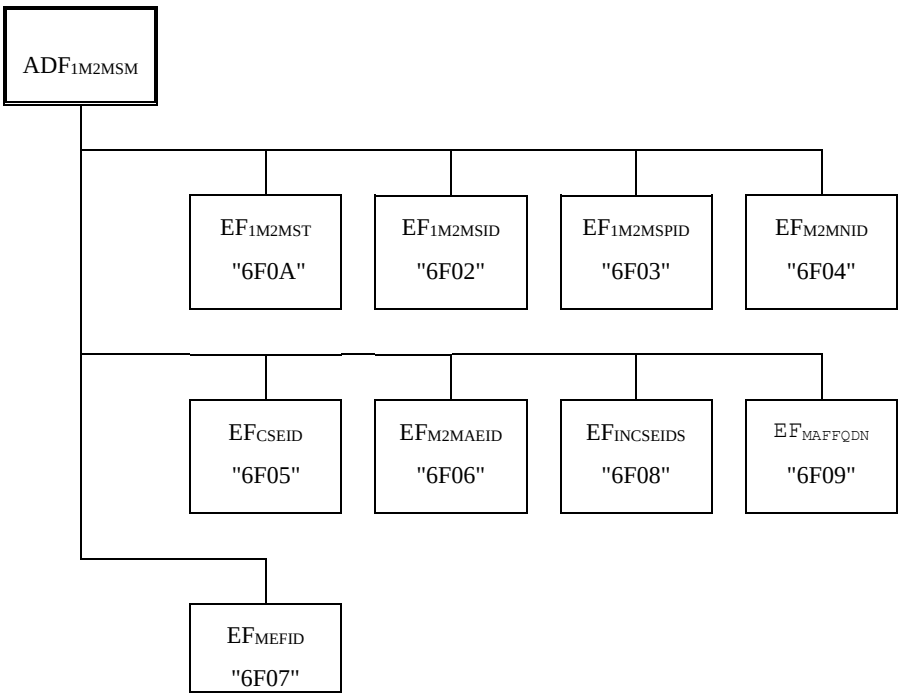


Figura D.2 – Identificadores de fichero y estructuras de directorio del ADF_{1M2MSM}

D.2.2 Procedimientos relacionados con abonos oneM2M para el servicio M2M

D.2.2.0 Introducción

En esta cláusula se especifican los procedimientos que ejecutarán los nodos de campo M2M para interactuar con un abono a servicios oneM2M en la UICC. Estos procedimientos son aplicables independientemente de la estructura de fichero que soporte el abono a servicios oneM2M (ADF 1M2MSM o DF_{1M2M} de un ADF de una aplicación de acceso a la red), a menos que se indique lo contrario.

D.2.2.1 Inicialización – selección de la aplicación 1M2MSM

Este procedimiento se aplica únicamente a un abono M2M soportado en un ADF 1M2MSM.

Si el nodo de campo M2M desea intervenir en la operación M2M, después de la activación de la UICC (véase [ETSI TS 102 221]), seleccionará una aplicación 1M2MSM, que ha de figurar en el fichero EF_{DIR}, utilizando la instrucción "SELECT by DF name" (selección por nombre de DF) como se define en [ETSI TS 102 221].

Tras seleccionar de forma exitosa una aplicación oneM2M, el AID oneM2M seleccionado se almacena en la UICC. Esta aplicación se identifica como la última aplicación 1M2MSM seleccionada. La última aplicación 1M2MSM seleccionada estará disponible en la UICC después de desactivar y volver a activar la UICC.

Si se selecciona una aplicación oneM2M utilizando un nombre de DF parcial, el nombre indicado en la instrucción designará únicamente una aplicación 1M2MSM. Además, si se selecciona una aplicación 1M2M utilizando un nombre de DF parcial, como se especifica en [ETSI TS 102 221], indicando en la instrucción SELECT la última ocurrencia, la UICC seleccionará la aplicación oneM2M almacenada como la última aplicación oneM2M. Si en la instrucción SELECT se indican las opciones "first" (primera) o "next/previous" (siguiente/anterior), estas carecerán de significado si, en la misma sesión, no se ha seleccionado previamente una aplicación, y aparecerá un código de error apropiado.

D.2.2.2 Terminación de la sesión 1M2MSM

Este procedimiento es aplicable únicamente a un abono oneM2M soportado en un ADF 1M2MSM.

El nodo de campo M2M puede finalizar la sesión UICC oneM2M de la siguiente manera:

El nodo de campo M2M indicará a la aplicación de la UICC oneM2M que el procedimiento de terminación va a comenzar, enviando una instrucción "STATUS" (estado) particular.

Por último, el nodo de campo M2M borra de su memoria todos los elementos de información relacionados con el abono M2M.

Para terminar efectivamente la sesión, el nodo de campo M2M utilizará uno de los mecanismos descritos en [ETSI TS 102 221].

D.2.2.3 Procedimiento de descubrimiento de los servicios oneM2M

Este procedimiento se utiliza para descubrir los servicios relacionados con el sistema oneM2M que ofrece una UICC oneM2M.

El nodo de campo M2M ejecutará el procedimiento de lectura con el EF_{1M2MST}. Si se indica que ningún servicio relacionado con el sistema oneM2M está disponible, el nodo de campo M2M asumirá que en ese ADF solo puede efectuarse la provisión de los parámetros obligatorios.

D.2.2.4 Procedimiento de provisión de servicios oneM2M

Estos procedimientos son utilizados por un nodo de campo M2M con el objeto de inicializar un abono a servicios M2M provisionado en la UICC.

El nodo de campo M2M ejecutará el procedimiento de lectura con el $EF_{1M2MSID}$ y el $EF_{1M2MSPID}$, y con el EF_{CSEID}, el EF_{M2MNID}, el $EF_{INCSEID}$ y el $EF_{MAFFQDN}$ en función los servicios que figuren disponibles en el EF_{1M2MST}.

D.2.2.5 Procedimiento de provisión de identificadores de aplicaciones oneM2M

Este procedimiento permite efectuar la provisión de una lista de identificadores de aplicaciones M2M que puede habilitarse en el nodo M2M en relación con el abono a servicios oneM2M.

Condición: El servicio número 4 debe estar disponible en el cuadro de servicios oneM2M.

Bajo esta condición, el nodo de campo M2M ejecutará el procedimiento de lectura con el $EF_{M2MAEID}$.

D.2.2.6 Procedimientos relativos a la provisión segura oneM2M

El nodo de campo M2M aplica estos procedimientos a fin de ejecutar la provisión segura M2M con la ayuda de la UICC, dependiendo de los servicios disponibles en el EF_{1M2MST} y de los contextos de las instrucciones "AUTHENTICATE" (autentificar) soportados (por ejemplo, el soporte a la GBA mediante una aplicación de acceso a la red) que se hayan indicado para el ADF anfitrión.

Provisión segura: provisión de direcciones MEF:

Condición: El servicio número 5 deberá estar disponible en el cuadro de servicios oneM2M.

Bajo esta condición, el nodo de campo M2M ejecutará el procedimiento de lectura con el EF_{MEFID}, si el servicio correspondiente está disponible.

Provisión segura de GBA:

Este procedimiento depende del marco de autentificación soportado por la UICC e indicado en el cuadro de servicios del ADF anfitrión.

Tras identificar el marco de autentificación soportado, el nodo de campo M2M verificará si el servicio número 7 está disponible en el EF_{1M2MST}: de ser así, el nodo M2M del dispositivo/pasarela ejecutará los procedimientos GBA mediante la instrucción "AUTHENTICATE" en el contexto de seguridad GBA (modo de inicialización y modo de derivación) con los parámetros aplicables a la provisión de segura de GBA.

D.2.2.7 Procedimientos relativos a la asociación de seguridad oneM2M

Conexión segura de GBA:

Este procedimiento depende del marco de autentificación soportado por la UICC e indicado en el cuadro de servicios del ADF anfitrión.

Tras identificar el marco de autentificación soportado, el nodo de campo M2M verificará si el servicio número 12 está disponible en el EF_{1M2MST}: de ser así, el nodo de campo M2M ejecutará los procedimientos GBA mediante la instrucción "AUTHENTICATE" en el contexto de seguridad GBA (modo de inicialización y modo de derivación) con los parámetros aplicables la asociación de seguridad de GBA.

Anexo E

Anexo en blanco

Este Anexo se ha dejado deliberadamente en blanco.

Anexo F

Adquisición de información de ubicación para el control de acceso basado en la ubicación

(El presente anexo es parte integrante de la Recomendación.)

F.0 Introducción

Cuando una CSE anfitriona evalúa una solicitud (acceso a un recurso) y se define un parámetro accessControlLocationRegions en el atributo privilegios de los recursos <accessControlPolicy>, la CSE anfitriona comprobará si la ubicación del originador de una solicitud se encuentra en las regiones especificadas o no. Así pues, la CSE anfitriona conservará la ubicación del originador, la adquirirá o denegará el acceso. En este Anexo se indica cómo describir las regiones de ubicación y obtener la ubicación del originador.

F.1 Descripción de la región

F.1.1 Descripción circular

La manera práctica de describir una región o zona es mediante la presentación circular, en la que por lo general el círculo se caracteriza por las coordenadas entre un punto central y un radio. Geográficamente, el punto central y el radio se describen como la longitud y latitud y el metro, respectivamente. En esta descripción, el parámetro accessControlLocationRegions se representará como un círculo, tal como se muestra en la Figura F.1.

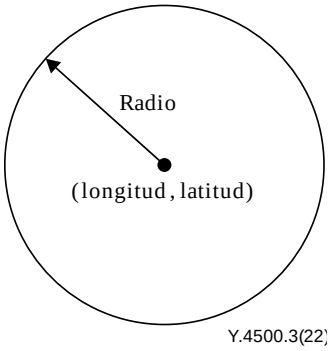


Figura F.1 – Representación circular del parámetro accessControlLocationRegions

F.1.2 Descripción por país

En la descripción por país, se utilizará un código ISO 3166-1 alfa 2, tal como se define en [b-ISO 3166-1]. Se trata de códigos de dos letras utilizados para representar los países y las regiones especiales de interés geográfico. Por ejemplo, KR es el código para Corea (la República de).

NOTA – De conformidad con lo dispuesto en [b-ISO 3166-1], los elementos de código asignados por el usuario son códigos a disposición de los usuarios que necesitan añadir más nombres de países, territorios u otras entidades geográficas a su aplicación interna de la norma ISO 3166-1, y el organismo de mantenimiento de ISO 3166 nunca tendrá en cuenta esos códigos en el proceso de actualización de la norma. Los siguientes son códigos que los usuarios pueden asignar:

Alfa-2: AA, QM a QZ, XA a XZ, y ZZ

Alfa-3: AAA a AAZ, QMA a QZZ, XAA a XZZ, y ZZA a ZZZ

Códigos numéricos: 900 a 999

En el sistema oneM2M no se impedirá que los usuarios recurran a esa posibilidad para asignar sus propios códigos, pero no se mantendrá un registro de dichos códigos, por lo que existe el riesgo de

duplicación en las implementaciones que puede provocar un funcionamiento incongruente de las acciones de interoperabilidad entre las implementaciones.

F.2 Adquisición de la información de ubicación

F.2.0 Introducción

Como se ha señalado anteriormente, cuando se define el parámetro accessControlLocationRegions, la CSE anfitriona verificará la ubicación del originador a efectos del control de acceso. En esta cláusula se describe la manera en que la CSE anfitriona comprueba u obtiene la ubicación. Los procedimientos pueden variar en función de la descripción de la región, el círculo y el país.

F.2.1 Descripción circular

Si se utiliza la descripción en forma de restricción relativa al contexto de ubicación, la CSE anfitriona verificará si tiene acceso a la ubicación actual del originador o no. De no ser el caso, la obtendrá del originador. En [UIT-T Y.4500.1] se define un tipo de recurso para la adquisición de la ubicación de un nodo de destino, <locationPolicy>. Por lo tanto, para obtener la ubicación del originador, la CSE anfitriona creará la <locationPolicy> y establecerá los atributos pertinentes como se indica a continuación:

locationSource: La fiabilidad de la información de ubicación es fundamental, por lo que la ubicación debe obtenerse a través de una red de confianza. Si se hace a través de las otras fuentes, la información de ubicación puede fácilmente ser objeto de adulteración (es decir, suplantación de GPS). Así pues, el atributo locationSource dependerá de la red.

locationTargetID: El nodo de destino será el originador que necesita autorizar las solicitudes enviadas. El atributo locationTargetID será el identificador del originador.

Cabe señalar que los demás atributos se determinan a través de las políticas locales de la CSE anfitriona, como se describe en la cláusula 9.6.9 de [UIT-T Y.4500.1]. A fin de obtener la ubicación por medio de la red, la CSE anfitriona convertirá la solicitud de ubicación especificada por oneM2M en una solicitud especificada por la red.

NOTA 1 – En el Anexo F de [UIT-T Y.4500.4] se describe cómo convertir la solicitud especificada por oneM2M en una solicitud especificada por "OMA RESTful NetAPI para ubicación de terminales".

Dado que la información de la región (descripción circular) está definida por el parámetro accessControlLocationRegions, la CSE anfitriona puede utilizar la información de región circular cuando solicita la información de ubicación a la red. En la especificación OMA RESTful NetAPI para la ubicación de terminales [b-OMA REST] se describen los tipos de recursos, como un servicio de notificación de ubicación basado en la zona (región), a saber "CircleNotificationSubscription". Por lo tanto, si la CSE anfitriona se abona al servicio de notificación en el que la región circular constituye el parámetro acccessControlLocationRegions, esta puede determinar siempre si el originador se encuentra en las regiones o no. En la Figura F.2 se ilustra la manera de adquirir la ubicación del originador cuando el parámetro accessControlLocationRegions está definido.

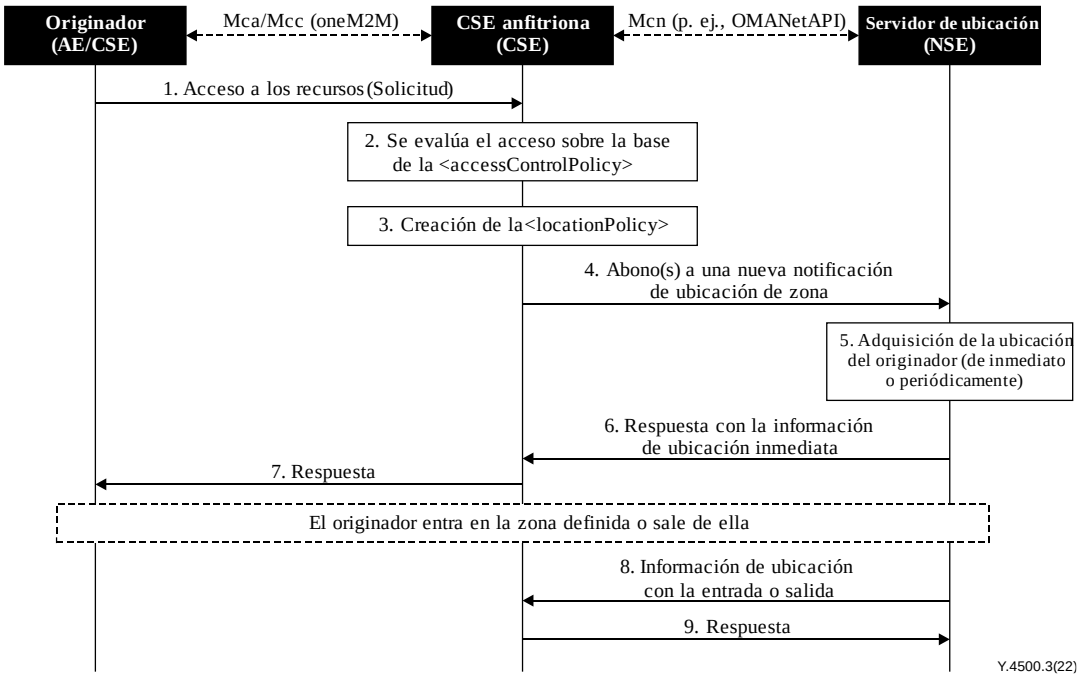


Figura F.2 – Ubicación del originador cuando el parámetro accessControlLocationRegions está definido

1. El originador envía una solicitud para acceder a un recurso.

2. La CSE anfitriona evaluará la solicitud recibida basándose en el recurso <accessControlPolicy> vinculado. Si en una de las tuplas de regla relativas al originador de la solicitud figura el parámetro accessControlLocationRegions (descripción circular) y la CSE anfitriona no almacena la ubicación del originador, la CSE anfitriona continuará con el siguiente paso o denegará el acceso.

Si la CSE anfitriona conoce la ubicación del iniciador, esta se utiliza para aplicar la política de control de acceso.

La CSE anfitriona puede denegar el acceso si el originador no está abonado a la red o por cualquier otro motivo (por ejemplo, pérdida de la conexión, funcionamiento inadecuado del servidor).

3. La CSE anfitriona creará el recurso <locationPolicy> y establecerá los atributos pertinentes según se ha indicado antes.

4. La CSE anfitriona se abonará a un nuevo servicio de notificación de ubicación de zona dirigida al servidor de ubicación de la red. La información de zona se basará en la zona definida por los parámetros accessControlLocationRegions. En caso de que se hayan definido varias regiones, se establecerán varios abonos.

NOTA 2 – Tras la adquisición inmediata de la ubicación, el servidor de ubicación obtiene periódicamente la ubicación del originador para comprobar si este se encuentra en la zona o no. La frecuencia y la duración pueden definirse en políticas locales.

6. El servidor de ubicación responde a la CSE anfitriona con la información de ubicación inmediata del originador.

7. En función de la ubicación del originador que se haya recibido y de otras políticas de control de acceso, se evalúa la solicitud a efectos de su aprobación o denegación. La CSE anfitriona envía una respuesta en relación con la solicitud (paso 1).

8. Cada vez que el originador entre en la zona o salga de ella, el servidor de ubicación notificará a la CSE anfitriona el cambio de ubicación. De este modo, la CSE anfitriona puede llevar un

seguimiento de la ubicación del originador y evaluar fácilmente el acceso basándose en la restricción relativa al contexto de ubicación.

9. La CSE anfitriona responde a la notificación.

F.2.2 Descripción por país

Por lo general, la ubicación a escala de país del originador puede determinarse mediante la dirección IP del originador. Si la CSE anfitriona puede identificar el país de que se trate mediante la dirección IP del originador y si este coincide además con el parámetro acccessControlLocationRegions definido, la CSE anfitriona puede aprobar la solicitud previa evaluación de todas las políticas de control de acceso.

NOTA 1 – La identificación de un país a través de una dirección IP queda fuera del alcance de esta Recomendación.

Sin embargo, si la CSE anfitriona no logra identificar el país a partir dirección IP del originador, obtendrá la coordenada de ubicación (es decir, longitud y latitud) del originador a través de la red y podrá identificar el país utilizando la ubicación, si está disponible. En el Anexo F de [UIT-T Y.4500.4] se define la forma de obtener la coordenada de ubicación.

NOTA 2 – La identificación del país a partir de la ubicación queda fuera del alcance de esta Recomendación.

Anexo G

Anexo en blanco

Este Anexo se ha dejado deliberadamente en blanco.

Anexo H

Anexo en blanco

Este Anexo se ha dejado deliberadamente en blanco.

Anexo I

Anexo en blanco

Este Anexo se ha dejado deliberadamente en blanco.

Anexo J

Lista de atributos de privacidad

(El presente anexo es parte integrante de la Recomendación.)

Véase el Table J.1.

Cuadro J.1 – Atributos de privacidad

ID de la etiqueta	Nombre de la etiqueta	Valor	Parámetro	Descripción corta de la etiqueta	Descripción completa de la etiqueta	Notas
1.0	Quién	Nulo	Nulo	Nombre de parte	Nombre comercial del dispositivo o prestador de servicio que solicita acceso a los dispositivos inteligentes/red/datos de los usuarios.	
		Variable	Texto	Nombre de empresa	Nombre de la empresa que solicita acceso a los dispositivos inteligentes del usuario y que especifica sus condiciones.	
		Dos letras variables	Código de país	Ubicación	País de ubicación del dispositivo o proveedor de servicio.	
		Variable	Texto	Número de registro de empresa	Número de registro de una empresa que puede utilizarse como ayuda para comprobar la autenticidad de la empresa. Puede consultarse a las autoridades de los distintos países como ayuda para comprobar la autenticidad de la empresa que solicita hacer uso de los datos y el grado de confianza que puede depositarse en ella.	
1.1	ID				Opciones para la identificación única de las aplicaciones y los dispositivos.	
			Texto	Número de modelo	Números móviles de los dispositivos que estén incluidos en el servicio del ASP.	

Cuadro J.1 – Atributos de privacidad

ID de la etiqueta	Nombre de la etiqueta	Valor	Parámetro	Descripción corta de la etiqueta	Descripción completa de la etiqueta	Notas
			Texto	Versión	Números de versión de los dispositivos que estén incluidos en el servicio del ASP.	
			Formato definido por el sistema oneM2M	ID de la aplicación registrada	Identificadores de las aplicaciones registradas que estén incluidos en el servicio del ASP.	
			Códigos de país	Códigos de los países en los que se ha concedido autorización, en los casos necesarios	La acreditación de un dispositivo o aplicación puede ser válida solo en determinados países.	
2.0	Qué			Tipo de clasificación de los datos	¿A qué tipo de datos accederá el dispositivo/servicio? Mientras más alto sea el valor, más sensibles serán los datos.	
		No recopilación de datos	Sí/No	No se recopilan datos.	El dispositivo no recopila ningún dato; podría ser un dispositivo de salida, como un interruptor de luz, que solo recibe instrucciones.	
		No datos personales	Sí/No	Datos no vinculados a una persona.	Los datos no pueden vincularse a una persona. Este podría ser el caso si el dispositivo fuera un sensor en una puerta que solo puede informar de cuando se abre o se cierra la puerta.	
		Datos anónimos	Sí/No	Se recopilan datos sobre una persona pero de forma anónima.	Recopilación de datos sobre una persona de forma anónima para eliminar o resumir cualquier dato que permita identificar o perfilar a un individuo.	
		Datos personales	Sí/No	Datos que pueden vincularse directamente a una identidad.	Los datos recopilados pueden vincularse a un identificador único de una persona o grupo pequeño (por ejemplo, miembros de una familia que habitan en la misma vivienda).	
		Datos personales sensibles	Sí/No	Datos más sensibles que pueden vincularse a una identidad.	Las autoridades de protección de datos de la UE definen determinados tipos de datos personales sensibles. Cabe también examinar si otros tipos de datos, como los bancarios, pueden entran en este ámbito	

Cuadro J.1 – Atributos de privacidad

ID de la etiqueta	Nombre de la etiqueta	Valor	Parámetro	Descripción corta de la etiqueta	Descripción completa de la etiqueta	Notas
		Datos médicos	Sí/No	Datos relacionados con la salud, el estado físico, etc. de una persona.	Datos sobre enfermedades o tratamientos, o sobre el bienestar general.	
3.0	Cuándo	Nulo	Nulo	Momento en que se recopilan los datos.	Periodicidad del envío de los datos.	
		No recopilación de datos	Sí/No	No se recopilan datos.	El dispositivo o servicio no recopila datos, por ejemplo, un dispositivo de extremo, como una luz.	
		Según los eventos	Sí/No	Se activa por un evento.	El dispositivo solo recopila datos cuando se activa; por ejemplo, un sensor en una puerta que activa una cámara.	
		Variable por mes	1 a 12	Los datos se envían mensualmente.	El dispositivo o servicio solo recopila los datos en el marco de transferencias mensuales. Por ejemplo, un frigorífico inteligente que envía un informe de rutina sobre su estado de funcionamiento.	
		Semanalmente	Sí/No	Los datos se envían semanalmente.	El dispositivo o servicio solo recopila datos en el marco de una transferencia semanal. Por ejemplo, un informe sobre el estado de diagnóstico elaborado por su sistema de detección de incendios, en el que figuran los resultados de las pruebas de los sensores y la duración prevista de la batería.	
		Diariamente	Sí/No	Los datos se envían diariamente	El dispositivo o servicio solo recopila datos en el marco de una transferencia diaria. Por ejemplo, un frigorífico inteligente que envía los artículos que se han consumido en forma de lista de compra al vendedor preferido del usuario para que los incluya en la cesta de compra.	

Cuadro J.1 – Atributos de privacidad

ID de la etiqueta	Nombre de la etiqueta	Valor	Parámetro	Descripción corta de la etiqueta	Descripción completa de la etiqueta	Notas
		Por horas	1 a 24	Los datos se envían cada X horas.	El dispositivo o servicio solo recopila datos en el marco de una transferencia por horas. Por ejemplo, una alarma domiciliaria que informa de que está encendida y que todos los sensores están activos. Así, la aplicación de la alarma o el servicio de control de alarmas del usuario sabe que el sistema sigue funcionando y que nadie ha podido desactivar la función de envío de alertas de la alarma.	
		Minutos	1 a 60	Los datos se envían cada X minutos.	El dispositivo o servicio solo recopila datos cada 15 minutos. Por ejemplo, los contadores inteligentes que informan de las cifras de consumo.	
		En tiempo real por accionamiento	Sí/No	Los datos se envían continuamente cuando se accionan.	Los datos se envían en tiempo real a raíz de un evento específico. Por ejemplo, la alarma de la casa informa de que se ha abierto una puerta interior mientras esta estaba activada, lo que desencadena la transmisión de las cámaras de seguridad.	
		En tiempo real continuamente	Sí/No	Los datos se envían continuamente en todo momento.	Los datos se envían en tiempo real mientras el dispositivo está activo. Por ejemplo, el envío de datos de televisión en circuito cerrado (CCTV) para su almacenamiento externo.	
3.1	Periodo de tiempo	Nulo		Periodo de tiempo de los datos	¿El momento en que se envían los datos abarca un período de tiempo?	
		No recopilación de datos	Sí/No	No se recopilan datos.	El dispositivo o servicio no recopila datos, por ejemplo, un dispositivo extremo como una luz.	
		Resumen/estado actual	Sí/No	El dispositivo envía su estado actual.	El dispositivo envía los datos del estado actual, sin historial; por ejemplo, el estado actual de un sensor de una puerta (abierta/cerrada), y no el registro de cuándo se abrió y se cerró.	

Cuadro J.1 – Atributos de privacidad

ID de la etiqueta	Nombre de la etiqueta	Valor	Parámetro	Descripción corta de la etiqueta	Descripción completa de la etiqueta	Notas
		Muestra	Sí/No	Los datos abarcan un corto período de tiempo.	Los datos cubren una muestra de datos de un breve período de tiempo, como una muestra periódica del ritmo cardíaco que se mide varias veces al día.	
		Registro completo	Sí/No	Se proporcionan los datos completos capturados por el dispositivo.	Se proporcionan todos los datos capturados por el dispositivo, ya sea en tiempo real (3.0) o en forma de historial retrospectivo.	
3.2	Frecuencia de muestreo	Nulo		Período de tiempo entre los muestreos de datos.	Diferencia en segundos entre las tomas de muestras.	
		No recopilación de datos.	Sí/No	No se recopilan datos.	El dispositivo o servicio no recopila datos, por ejemplo, un dispositivo de extremo, como una luz.	
		Variable		El valor se expresa en segundos entre los puntos de captura de datos.	Tiempo entre las lecturas llevadas a cabo por el dispositivo medido en segundos.	
		Datos difundidos en directo	Sí/No	Los datos se capturan de forma continua.	Los datos se capturan de forma continua, como las cámaras de seguridad inteligentes capaces de trasmitir las imágenes al usuario.	
4.0	Lugar de almacenamiento	Nulo		Lugar donde se almacenan los datos.	Lugar en el que se almacenan los datos creados por el dispositivo o utilizados por el servicio.	
		No recopilación de datos	Sí/No	No se recopilan datos.	El dispositivo o servicio no recopila datos; por ejemplo, un dispositivo de extremo, como una luz.	
		Local	Sí/No	Los datos solo se almacenan localmente	Los datos se almacenan en la red de dispositivos inteligentes (por ejemplo, en el hogar).	
		Variable		País/grupo	País donde se almacenan los datos o parte en un marco más amplio (por ejemplo, la UE).	

Cuadro J.1 – Atributos de privacidad

ID de la etiqueta	Nombre de la etiqueta	Valor	Parámetro	Descripción corta de la etiqueta	Descripción completa de la etiqueta	Notas
4.1	Lugar de recopilación			Lugar del que se recopilan los datos.	Lugar del que se recopilan los datos. Nota: esto puede ser redundante para el usuario, pero puede usarse en el caso de fuentes externas como, los informes meteorológicos. También puede ser útil en el caso de los servicios, a fin de que puedan indicar los tipos de dispositivos de los que extraerán los datos, ya que es posible que no quieran acceder a todos los dispositivos inteligentes que se encuentran en el lugar.	
		No recopilación de datos.	Sí/No	No se recopilan datos.	El dispositivo o servicio no recopila datos, por ejemplo, un dispositivo de extremo, como una luz.	
		Dispositivo	Sí/No	Los datos se recopilan solo del dispositivo específico al que se aplican los términos y condiciones.	Los términos y condiciones (así como la configuración de privacidad de los usuarios) se evalúan solamente sobre la base de los datos recogidos por el dispositivo específico.	
		Red de dispositivo inteligente	Sí/No	Los datos se recopilan de todos los dispositivos conectados a la red del usuario.	Los datos se recopilan de todos los dispositivos* que conforman la red de dispositivos inteligentes del usuario.	
		Variable		Fuente externa.	Información procedente de una fuente externa que se combina con los datos recopilados. Por ejemplo, las previsiones meteorológicas se combinan con los hábitos de utilización de un edificio de los usuarios para prever la calefacción necesaria y luego encenderla a fin de que el edificio esté a la temperatura adecuada cuando el usuario llegue.	Esto sería descriptivo y el usuario tendría la opción de desactivar o sustituir la función (por ejemplo, puede escoger su propia estación meteorológica compatible, en lugar de que la información provenga de la oficina meteorológica).
4.2	Lugar de procesamiento	Nulo		Lugar en el que se procesan los datos.	Lugar físico en el que se procesan los datos, que puede diferir del lugar en el que se almacenan los datos.	

Cuadro J.1 – Atributos de privacidad

ID de la etiqueta	Nombre de la etiqueta	Valor	Parámetro	Descripción corta de la etiqueta	Descripción completa de la etiqueta	Notas
		No recopilación de datos	Sí/No	No se recopilan datos.	El dispositivo o servicio no recopila datos, por ejemplo, un dispositivo extremo, como una luz.	
		Local	Sí/No	Los datos solo se procesan localmente.	Los datos recopilados solo se procesan en el dispositivo, o con la red de dispositivos inteligentes del usuario.	
		Variable		País/grupo.	País donde se almacenan los datos, o parte en un marco más amplio (por ejemplo, la UE).	
4.3	Lugar de acceso	Nulo		Lugar desde el que se puede accedes a los datos.	Lugar desde el que las restricciones del proveedor/vendedor/precedente de política permiten acceder a los datos almacenados.	
		No recopilación de datos	Sí/No	Los datos no se recopilan.	El dispositivo o servicio no recopila datos, por ejemplo, un dispositivo de extremo, como una luz.	
		Local	Sí/No	Los datos solo se procesan localmente.	Los datos recopilados solo se procesan en el dispositivo, o con la red de dispositivos inteligentes del usuario.	
		Variable		País/grupo.	País donde se almacenan los datos, o parte en un marco más amplio (por ejemplo, la UE).	
5.0	Por qué	Nulo			Motivo principal por el que se recopilan los datos personales y para permite que cualquier cambio de uso sea notificado al usuario.	
		Sí/No	Sí/No	Para prestación directa del servicio.	El ASP recoge información a efectos de la prestación directa del servicio.	Por ejemplo, utilización de la ubicación para la radiobúsqueda desde una estación base en la que el usuario esté registrado en el momento.
		Sí/No	Sí/No	Para mejorar los productos y servicios del ASP y sus socios.	El ASP recopila información para mejorar sus productos y servicios y los de sus socios.	

Cuadro J.1 – Atributos de privacidad

ID de la etiqueta	Nombre de la etiqueta	Valor	Parámetro	Descripción corta de la etiqueta	Descripción completa de la etiqueta	Notas
		Sí/No	Sí/No	Para personalizar los servicios.	El ASP recopila información para personalizar sus productos y servicios y los de sus socios.	"Los usuarios que seleccionaron esta opción también seleccionaron esta otra".
		Sí/No	Sí/No	Precedente de política, requisito.	El ASP recopila información para cumplir un precedente de política o requisito.	Por ejemplo, aplicación de una edad mínima para determinar el acceso del usuario a los recursos.
6.0	Conservación	Nulo		Tiempo durante el que se conservan los datos.	Tiempo durante el que conservan los datos (definidos anteriormente) en su nivel de detalle actual.	
		No recopilación de datos	Sí/No	No se recopilan datos.	El dispositivo o servicio no recopila datos, por ejemplo, un dispositivo de extremo, como una luz.	
		Sin conservación	Sí/No	No se conserva ningún dato.	Tras su procesamiento, los datos se eliminan de inmediato.	
		Minutos	1 a 60	Los datos se conservan durante X minutos.	Los datos se conservan durante 15 minutos antes de ser eliminados. Por ejemplo, el dispositivo solo conserva la última serie de mediciones y recopila otras nuevas cada 15 minutos.	
		Horas	1 a 24	Los datos se conservan durante X horas.	Los datos se conservan durante X horas.	
		Días	1 a 7	Los datos se conservan durante X días.		
		Semanas	1 a 4	Los datos se conservan durante X semanas.		
		Meses	1 a 12	Los datos se conservan durante X meses.		
		Años	1 a 10	Los datos se conservan durante X años.		
		Siempre		Los datos se conservarán para siempre.	Los datos se almacenarán sin una política concreta de conservación o eliminación.	

Cuadro J.1 – Atributos de privacidad

ID de la etiqueta	Nombre de la etiqueta	Valor	Parámetro	Descripción corta de la etiqueta	Descripción completa de la etiqueta	Notas
6.1	Conservación de manera anónima	Nulo		Tiempo durante el que se conservan los datos de forma anónima.	Tiempo durante el que se conserva cualquier dato de forma anónima o datos derivados que no estén directamente vinculado a una identificación única. Por ejemplo, estadísticas sobre consumo de energía eléctrica por ubicación geográfica.	
		Sin conservación	Sí/No	No se conserva ningún dato.	Tras su procesamiento, los datos se eliminan de inmediato.	
		Minutos	1 a 60	Los datos se conservan durante X minutos.	Los datos se conservan durante 15 minutos antes de ser eliminados. Por ejemplo, el dispositivo solo conserva la última serie de mediciones y recopila otras nuevas cada 15 minutos.	
		Horas	1 a 24	Los datos se conservan durante X horas.	Los datos se conservan durante X horas.	
		Días	1 a 7	Los datos se conservan durante X días.		
		Semanas	1 a 4	Los datos se conservan durante X semanas.		
		Meses	1 a 12	Los datos se conservan durante X meses.		
		Años	1 a 10	Los datos se conservan durante X años.		
		Siempre		Los datos se conservarán para siempre.	Los datos se almacenarán sin una política concreta de conservación o eliminación.	
6.2	Conservación en forma resumida	Nulo		Tiempo durante el que se conservan los datos de forma resumida.	Tiempo durante el que se conserva cualquier dato de forma resumida. Por ejemplo, la cantidad total de energía eléctrica consumida al mes, según mediciones realizadas cada 15 minutos.	
		Sin conservación	Sí/No	No se conserva ningún dato.	Tras su procesamiento, los datos se eliminan de inmediato.	

Cuadro J.1 – Atributos de privacidad

ID de la etiqueta	Nombre de la etiqueta	Valor	Parámetro	Descripción corta de la etiqueta	Descripción completa de la etiqueta	Notas
		Minutos	1 a 60	Los datos se conservan durante X minutos.	Los datos se conservan durante 15 minutos antes de ser eliminados. Por ejemplo, el dispositivo solo conserva la última serie de mediciones y recopila otras nuevas cada 15 minutos.	
		Horas	1 a 24	Los datos se conservan durante X horas.	Los datos se conservan durante X horas.	
		Días	1 a 7	Los datos se conservan durante X días.		
		Semanas	1 a 4	Los datos se conservan durante X semanas.		
		Meses	1 a 12	Los datos se conservan durante X meses.		
		Años	1 a 10	Los datos se conservan durante X años.		
		Siempre		Los datos se conservarán para siempre.	Los datos se almacenarán sin una política concreta de conservación o eliminación.	
7.0	Compartición completa	Nulo		Entidades con las que se comparten todos los datos.	Entidad fuera de la empresa que tiene acceso a los datos completos por tipo.	
		No compartición de datos	Sí/No	Los datos no se comparten fuera de la empresa.	Los datos no se comparten fuera de la empresa que proporciona el dispositivo o el servicio en ausencia de un contrato de procesamiento.	
		Grupo	No/alcance y motivo	Los datos solo se comparten con empresas del mismo grupo.	Los datos solo se comparten con otras empresas del mismo grupo.	
		Proveedor de infraestructura	Sí/No	Los datos se almacenan en la infraestructura de un tercero.	Los datos se almacenan en los servidores de una empresa independiente. Por ejemplo, la empresa que proporciona el dispositivo o servicio utiliza un proveedor de servicios en la nube para el almacenamiento o el procesamiento de los datos.	Nota: en las respuestas al lugar figuran el tercero concernido y la empresa que ofrece el servicio o dispositivo.
		Subcontratista	Sí/No	Los datos se comparten con subcontratistas.	Los datos se comparten con uno o varios subcontratistas que prestan parte del servicio.	Nota: en las respuestas a la ubicación, etc. se reflejan todos los subcontratistas utilizados.

Cuadro J.1 – Atributos de privacidad

ID de la etiqueta	Nombre de la etiqueta	Valor	Parámetro	Descripción corta de la etiqueta	Descripción completa de la etiqueta	Notas
		Otras partes con contrato de funciones auxiliares	No/alcance y motivo	Los datos se comparten con otras partes con contrato.	Los datos se comparten con otras partes con contrato que proporcionan funciones adicionales (auxiliares) para la utilización y funcionamiento del dispositivo. Por ejemplo, envío de boletines informativos, realización de ofertas comerciales, etc. Sitios locales de reparación con garantía, etc.	
		Socios	No/alcance y motivo	Los datos se comparten con otras entidades privadas.	Los datos se comparten con otras partes que no intervienen directa ni indirectamente en el dispositivo o servicio. Por ejemplo, proveedores de dispositivos que comparten datos con sus asociados de canal para que puedan enfocar sus campañas.	
		Organismos públicos	No/alcance, motivo, organismos	Los datos se comparten con determinados organismos públicos.	Los datos se comparten en determinadas condiciones con ciertos organismos. Por ejemplo, cuando salta una alarma, los datos de los dispositivos de seguridad se comparten con la policía para que pueda responder de forma adecuada o, si se activa una alarma médica, se envían los datos al servicio de ambulancias o al hospital, etc., para que puedan responder.	
7.1	Compartición de forma anónima	Nulo		Entidades con las que se comparten los datos.	Entidad fuera de la empresa que tiene acceso a los datos anónimos por tipo de usuario.	
		No compartición de datos	Sí/No	Los datos no se comparten fuera de la empresa.	Los datos no se comparten fuera de la empresa que proporciona el dispositivo o el servicio en ausencia de un contrato de procesamiento.	
		Grupo	No/alcance y motivo	Los datos solo se comparten con empresas del mismo grupo.	Los datos solo se comparten con otras empresas del mismo grupo.	
		Proveedor de infraestructura	Sí/No	Los datos se almacenan en la infraestructura de un tercero.	Los datos se almacenan en los servidores de una empresa independiente. Por ejemplo, la empresa que proporciona el dispositivo o servicio utiliza un proveedor de servicios en la nube para el almacenamiento o el procesamiento de los datos.	

Cuadro J.1 – Atributos de privacidad

ID de la etiqueta	Nombre de la etiqueta	Valor	Parámetro	Descripción corta de la etiqueta	Descripción completa de la etiqueta	Notas
		Subcontratista	Sí/No	Los datos se comparten con subcontratistas.	Los datos se comparten con uno o varios subcontratistas que prestan parte del servicio.	
		Otras partes con contrato de funciones auxiliares de	No/alcance y motivo	Los datos se comparten con otras partes con contrato.	Los datos se comparten con otras partes con contrato que proporcionan funciones adicionales (auxiliares) para la utilización y funcionamiento del dispositivo. Por ejemplo, envío de boletines informativos, realización de ofertas comerciales, etc. Sitios locales de reparación con garantía, etc.	
		Socios	No/alcance y motivo	Los datos se comparten con otras entidades privadas.	Los datos se comparten con otras partes que no intervienen directa ni indirectamente en el dispositivo o servicio. Por ejemplo, proveedores de dispositivos que comparten datos con sus asociados de canal para que puedan enfocar sus campañas.	
		Organismos públicos	No/alcance, motivo, organismos	Los datos se comparten con determinados organismos públicos.	Los datos se comparten en determinadas condiciones con ciertos organismos. Por ejemplo, cuando salta una alarma de seguridad, los datos de los dispositivos se comparten con la policía para que pueda responder de forma adecuada o, si se activa una alarma médica, se envían los datos al servicio de ambulancias o al hospital, etc., para que puedan responder.	
7.2	Compartición de forma resumida	Nulo		Entidades con las que se comparten los datos.	Entidad fuera de la empresa que tiene acceso a los datos resumidos por tipo de usuario.	
		No compartición de datos	Sí/No	Los datos no se comparten fuera de la empresa.	Los datos no se comparten fuera de la empresa que proporciona el dispositivo o el servicio en ausencia de un contrato de procesamiento.	
		Grupo	No/alcance y motivo	Los datos solo se comparten con empresas del mismo grupo.	Los datos solo se comparten con otras empresas del mismo grupo.	

Cuadro J.1 – Atributos de privacidad

ID de la etiqueta	Nombre de la etiqueta	Valor	Parámetro	Descripción corta de la etiqueta	Descripción completa de la etiqueta	Notas
		Proveedor de infraestructura	Sí/No	Los datos se almacenan en la infraestructura de un tercero.	Los datos se almacenan en los servidores de una empresa independiente. Por ejemplo, la empresa que proporciona el dispositivo o servicio utiliza un proveedor de servicios en la nube para el almacenamiento o el procesamiento de los datos.	
		Subcontratista	Sí/No	Los datos se comparten con subcontratistas.	Los datos se comparten con uno o varios subcontratistas que prestan parte del servicio.	
		Otras partes con contrato de funciones auxiliares de	No/alcance y motivo	Los datos se comparten con otras partes con contrato.	Los datos se comparten con otras partes con contrato que proporcionan funciones adicionales (auxiliares) para la utilización y funcionamiento del dispositivo. Por ejemplo, envío de boletines informativos, realización de ofertas comerciales, etc. Sitios locales de reparación con garantía, etc.	
		Socios	No/alcance y motivo	Los datos se comparten con otras entidades privadas.	Los datos se comparten con otras partes que no intervienen directa ni indirectamente en el dispositivo o servicio. Por ejemplo, proveedores de dispositivos que comparten datos con sus asociados de canal para que puedan enfocar sus campañas.	
		Organismos públicos	No/alcance, motivo, organismos	Los datos se comparten con determinados organismos públicos.	Los datos se comparten en determinadas condiciones con ciertos organismos. Por ejemplo, las autoridades locales que recopilan datos sobre el consumo medio de agua por ubicación geográfica.	
8.0	Notificación	Nulo				
		Sí/No	Sí/No	Los términos y condiciones se envían a la dirección de correo electrónico registrada del usuario final.	Los proveedores de dispositivos o aplicaciones envían los valores de sus etiquetas que figuran en este cuadro a una dirección de correo electrónico registrada por el usuario final.	
		URL	ACME.com/English/device type/model/T&C	Términos y condiciones en un URL mostrado.	Los proveedores de dispositivos o aplicaciones publican los valores de sus etiquetas que figuran en este cuadro en un URL.	El portal del PPM puede realizar este proceso de manera automática.

Cuadro J.1 – Atributos de privacidad

ID de la etiqueta	Nombre de la etiqueta	Valor	Parámetro	Descripción corta de la etiqueta	Descripción completa de la etiqueta	Notas
		URL	ACME.com/English/ device type/model/ T&C	Términos y condiciones en un URL almacenado en el dispositivo.	Los proveedores de dispositivos o aplicaciones publican los valores de sus etiquetas que figuran en este cuadro en un URL almacenado en el dispositivo.	El portal del PPM o el dispositivo pueden realizar este proceso de manera automática.
		Sí/No	Sí/No	Términos y condiciones en la pantalla local (si la hay).	Los proveedores de dispositivos o aplicaciones publican los valores de sus etiquetas que figuran en este cuadro en la pantalla del dispositivo (si la hay).	
		Sí/No	Sí/No	Pantalla remota asociada al usuario.	Los proveedores de dispositivos o aplicaciones publican los valores de sus etiquetas que figuran en este cuadro en una pantalla remota asociada al usuario.	
		Sí/No	Sí/No	Por correo postal.	Los proveedores de dispositivos o aplicaciones envían los valores de sus etiquetas que figuran en este cuadro a una dirección de correo postal registrada por el usuario final.	
		Sí/No	Sí/No	SMS (texto).	Los proveedores de dispositivos o aplicaciones envían los valores de sus etiquetas que figuran en este cuadro a un número SMS registrado por el usuario final.	
9.0	Obtención de consentimiento	Nulo				
			Sí/No	Consentimiento por defecto en la aplicación.	El usuario tiene que aceptar los valores por defecto con un solo clic en la aplicación.	
			Sí/No	Consentimiento mediante firma de un documento por el usuario final.	Resumen en XML firmado con la clave privada del usuario final, por ejemplo, una firma digital.	
			Sí/No	Consentimiento por un método oneM2M recomendado.	Método oneM2M recomendado {por determinar}.	Si se establece en el futuro.

Cuadro J.1 – Atributos de privacidad

ID de la etiqueta	Nombre de la etiqueta	Valor	Parámetro	Descripción corta de la etiqueta	Descripción completa de la etiqueta	Notas
10.0	Protección	Nulo			Se han establecido cinco niveles para describir el grado de protección de la privacidad y la seguridad del usuario final. El nivel 1 es el más bajo y el 5 el más elevado. En cada uno de estos niveles se establecen los requisitos que se espera que cumplan al reivindicarse.	Estos niveles concuerdan con los niveles propuestos por el GT4 sobre oneM2M.
		Nivel de protección reivindicado	1	Nivel de protección reivindicado = 1	Nivel 1: es el nivel más bajo, con exigencias mínimas de protección de la privacidad y la seguridad del usuario final. Este nivel se utiliza cuando la vulneración de la seguridad y la privacidad del usuario final trae asociada un riesgo mínimo.	
		Nivel de protección reivindicado	2	Nivel de protección reivindicado = 2	Nivel 2: proporciona cierto nivel de confianza en relación con la protección de la privacidad y la seguridad del usuario final. Las entidades demuestran, mediante un protocolo de autentificación seguro, que la entidad tiene el control de los datos sensibles y credenciales. Existen controles para proteger los datos sensibles y credenciales almacenados contra los ataques.	
		Nivel de protección reivindicado	3	Nivel de protección reivindicado = 3	Nivel 3: proporciona una alta confianza en relación con la protección de la privacidad y la seguridad del usuario final. Este nivel es necesario cuando la vulneración de la seguridad y la privacidad del usuario final trae asociada un riesgo considerable. Se utiliza la autentificación multifactor. Todos los datos o toda la información sensible que se intercambien en los protocolos de autentificación están protegidos criptográficamente en tránsito y en reposo.	

Cuadro J.1 – Atributos de privacidad

ID de la etiqueta	Nombre de la etiqueta	Valor	Parámetro	Descripción corta de la etiqueta	Descripción completa de la etiqueta	Notas
		Nivel de protección reivindicado.	4	Nivel de protección reivindicado = 4	Nivel 4: proporciona una confianza muy alta en relación con la protección de la privacidad y la seguridad del usuario final. Este nivel se utiliza cuando la vulneración de la seguridad y la privacidad del usuario final trae asociada un riesgo muy elevado. Este nivel proporciona el nivel más alto de seguridad y privacidad del usuario final. Además de lo previsto en nivel 3, se requiere la utilización de dispositivos físicos a prueba de alteración para el almacenamiento de todos los datos sensibles, como las claves criptográficas.	
		Nivel de protección reivindicado	5	Nivel de protección reivindicado = 5	Igual que en el nivel 4, más disponibilidad de una prueba de acreditación o garantía externa.	Puede depender del funcionamiento del sistema oneM2M en la certificación de dispositivos.
11.0	Edad	Nulo			Cuando convenga para las opciones de configuración de la privacidad a efectos de determinar la edad de los usuarios finales, por ejemplo, fecha de nacimiento, rango de edad, etc.	
		DD/MM/AAAA		Fecha de nacimiento.	Fecha de nacimiento declarada del usuario final para determinar el acceso a los recursos.	
		Valor numérico o rango de valores		Edad mínima del usuario objetivo.	Edad mínima del usuario objetivo utilizada para determinar el acceso a los recursos.	
		DD/MM/AAAA		Edad máxima del dispositivo (vida útil).	Edad máxima del dispositivo (vida útil) utilizada para determinar el acceso a los recursos.	Para los dispositivos con baterías integradas que tienen una vida útil o para productos químicos en dispositivos médicos, etc.

Apéndice I

Correspondencia de la terminología 3GPP GBA

(Este apéndice no forma parte integrante de la presente Recomendación.)

En el Cuadro I.1 se presenta una correspondencia entre la terminología y las abreviaturas utilizadas en la GBA con arreglo a la especificación 3GPP [ETSI TS 133 220] y la terminología y las abreviaturas equivalentes de oneM2M utilizadas en la presente Recomendación.

Cuadro I.1 – Correspondencia de la terminología y las abreviaturas utilizadas en la GBA

Entidades, claves y procesos GBA	**Entidades, claves y procesos de la inicialización de seguridad oneM2M**
UE	Enrolee (inscrito)
BSF	MEF
NAF	MAF
Bootstrapping Procedure (procedimiento de inicialización)	Bootstrap Security Handshake + Temporary Enrolment Key Generation (toma de contacto de seguridad de la inicialización + generación de clave temporal de inscripción)
Ks	Ke
B-TID	KeID
Bootstrapping Usage Procedure (procedimiento de utilización de la inicialización)	Usage in MAF Handshake (utilización en la toma de contacto MAF)
NAF FQDN (FQDN de la NAF)	MAF-ID
Ks_(ext/int)_NAF	Km (credencial maestra)

Apéndice II

Mecanismo general de autentificación mutua

(Este Apéndice no forma parte integrante de la presente Recomendación.)

II.0 Introducción

Los sistemas de autentificación mutua de oneM2M permiten a las entidades oneM2M demostrar que conocen las credenciales correspondientes, como las credenciales maestras, sin tener que intercambiar los valores de estas ni los datos sensibles, como las identidades de seguridad y los identificadores de seguridad. Para evitar la lectura y la copia de credenciales, la CSF de seguridad cuenta con un entorno seguro que protege contra la manipulación de esas credenciales y de la información procesada conexa.

Se aplica un protocolo general de autentificación mutua a los sistemas basados en claves simétricas y asimétricas. Los mensajes y parámetros precisos del protocolo dependen del sistema elegido y de los parámetros de seguridad seleccionados. Normalmente, el protocolo abarca las siguientes etapas que se muestran en la Figura II.1.

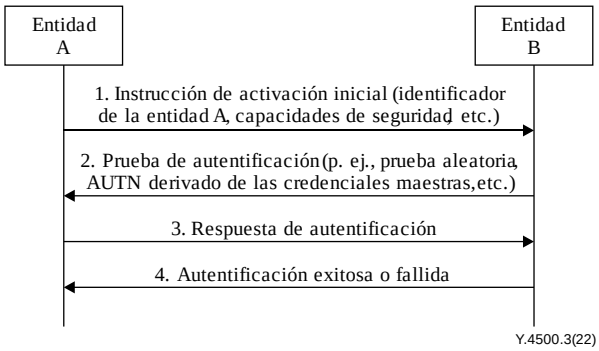


Figura II.1 – Autentificación mutua

1. La primera etapa consiste en la identificación segura de una entidad A ante una entidad B con la que se ha establecido o no un contacto previo. En esta etapa, la entidad A se identifica ante una entidad B protegida contra interceptaciones, es decir, no se realiza ningún intercambio de materiales de clave (credenciales maestras).

2. En la segunda etapa, la entidad B envía una prueba a la entidad A. En la prueba de autentificación se formula una prueba, se pide el testigo de autentificación (AUTN) de la entidad B derivado de las credenciales maestras, etc. La prueba, que puede ser aleatoria o no, depende del sistema de autentificación elegido y de los parámetros de seguridad seleccionados para los sistemas basados en claves simétricas y asimétricas.

3. La entidad A envía una respuesta de autentificación que contiene un testigo de autentificación (AUTN) derivado de sus credenciales maestras conocidas y la prueba de autentificación recibida. Esta respuesta se envía si la entidad A ha logrado autentificar a la entidad B con éxito.

4. Posteriormente, la entidad B verifica la relación entre la identidad de la entidad A y la respuesta recibida en la etapa 3. Si la verificación es satisfactoria, la entidad B considera que la respuesta ha sido creada por la entidad A utilizando un secreto asociado a la identidad de la entidad A proporcionada en el paso 1.

II.1 Autentificación de grupos

Evidentemente, en las transacciones oneM2M pueden participar a grupos de entidades M2M y no solo entidades individuales. Es posible clasificar como grupo a una serie de entidades habida cuenta de su proximidad, características idénticas, pertenencia al mismo propietario o cualquier otro criterio.

Para acceder a los servicios, todas las entidades de esos grupos deberían autentificarse primero. El mecanismo tradicional ofrece dos soluciones principales a tal efecto; a saber: un primer mecanismo de autentificación, que consiste en que el proveedor de servicios autentifique cada una de las entidades que forman parte del grupo, y un segundo mecanismo, que consiste en que cada entidad efectúe una autentificación mutua con un agente de grupo, que posteriormente se autentifica mutuamente con el proveedor de servicios. En los casos en que se utiliza el primer mecanismo, la carga de los cálculos y comunicaciones resultante puede ser excesiva. En el caso del segundo mecanismo, se producen las siguientes debilidades de seguridad:

1) Posibilidad de un ataque de intermediario por el agente de grupo: el agente de grupo estaría ubicado en un lugar inseguro o pertenecería a un proveedor distinto del proveedor de servicios. Si el agente de grupo es vulnerable o miente al proveedor de servicios, podría actuar como un atacante intermediario para efectuar una autentificación falsa de las entidades y transmitir identidades falsas al proveedor de servicios, ya que no se lleva a cabo una autentificación directa entre el proveedor de servicios y cada entidad M2M.

2) Problemas de privacidad: toda la información de las entidades M2M se transfiere a través del agente de grupo, que conoce toda la información generada por cada entidad. Por motivos de seguridad, si el agente de grupo pertenece a un propietario distinto del propietario de las entidades y de los proveedores de servicios, el agente de grupo no debería recibir el mensaje.

Así pues, las entidades M2M (por ejemplo, ASN o ADN) que compartan la misma característica pueden recurrir a la autentificación de grupo con el proveedor de servicios (por ejemplo, el nodo de infraestructura) a fin de proporcionar un túnel seguro de extremo a extremo, así como de reducir la sobrecarga de comunicación.

Apéndice III

Apéndice en blanco

Este Apéndice se ha dejado deliberadamente en blanco.

Apéndice IV

Apéndice en blanco

Este Apéndice se ha dejado deliberadamente en blanco.

Apéndice V

Precisiones para que el marco UICC soporte los servicios M2M

(Este apéndice no forma parte integrante de la presente Recomendación.)

V.0 Introducción

En el presente Apéndice se presenta información práctica adicional sobre el marco UICC compatible con oneM2M que se describe en el Anexo D.

V.1 Contenido sugerido de los EF en la etapa previa a la personalización

Si no se ha asignado un valor a los EF, es probable que no pueda determinarse cuál debe ser dicho valor a partir del texto principal. En el Cuadro V.1 de este Apéndice se sugieren los valores en esos casos.

Cuadro V.1 – Valores prepersonalizados de los EF

Identificación del fichero	Descripción	Valor
"6F02"	Identificador del abono a servicios 1M2M	"8000FF…FF"
"6F03"	Identificador del proveedor de servicios 1M2M	"8000FF…FF"
"6F04"	Identificador del nodo M2M	"8000FF…FF"
"6F05"	Identificador CSE local	"8000FF...FF"
"6F06"	Lista de identificadores de aplicaciones M2M	"00FF...FF" para cada registro
"6F07"	Identificador MEF	"00FF…FF" para cada registro
"6F08"	Lista de identificadores IN-CSE	"00FF...FF" para cada registro
"6F09"	FQDN de la MAF	"8000FF...FF"
"6F0A"	Cuadro de servicios 1M2M	En función del operador o del proveedor de servicios

V.2 Cambios en los EF mediante descarga de datos o aplicaciones CAT

En esta cláusula se define si es aconsejable cambiar el contenido de un EF mediante un protocolo UICC OTA o una aplicación CAT. La actualización de determinados EF "por vía aérea" o "por Internet" podría ocasionar un comportamiento imprevisible del equipo del usuario; estos cambios se señalan con la marca "Con precaución" en el Cuadro V.2. Algunos EF se marcan con un "No"; esto significa que por ningún motivo debe considerarse la posibilidad de introducir cambios "por vía aérea o por Internet" en esos FA.

Cuadro V.2 – Comportamiento al actualizar los EF

Identificación del fichero	Descripción	Cambio aconsejable
"6F02"	Identificador del abono a servicios 1M2M	No
"6F03"	Identificador del proveedor de servicios 1M2M	No
"6F04"	Identificador del nodo M2M	Con precaución
"6F05"	Identificador CSE local	Con precaución
"6F06"	Lista de identificadores de aplicaciones M2M	Con precaución
"6F07"	Identificador MEF	Con precaución
"6F08"	Lista de identificadores IN-CSE	Con precaución
"6F09"	FQDN de la MAF	Con precaución
"6F0A"	Cuadro de servicios 1M2M	Con precaución

V.3 Lista de los valores SFI a nivel del ADF_{M2MSM} o el DF_{M2M}

Cuadro V.3 – Valores SFI

Identificación del fichero	SFI	Descripción
"6F02"	"02"	Identificador del abono a servicios M2M
"6F03"	"03"	Identificador del proveedor de servicios M2M
"6F04"	"04"	Identificador del nodo M2M
"6F05"	"05"	Identificador CSE local
"6F06"	"06"	Lista de identificadores de aplicaciones M2M
"6F0A"	"0A"	Cuadro de servicios 1M2M

Los demás valores SFI quedan reservados para uso futuro.

V.4 Etiquetas UICC definidas en el Anexo J

Cuadro V.4 – Etiquetas UICC

Etiqueta	Nombre del elemento de datos	Uso
"80"	Objeto de datos TLV del FQDN de la MAF	$EF_{MAFFQDN}$
"80"	Objeto de datos TLV del M2M-Node-ID	EF_{M2MNID}
"80"	Objeto de datos TLV del CSE-ID local	EF_{CSEID}
"80"	Objeto de datos TLV del M2M-SP-ID	$EF_{1M2MSPID}$
"80"	Objeto de datos TLV del identificador de abono M2M	$EF_{1M2MSID}$
NOTA – El valor de etiqueta "FF" no es válido.		

Apéndice VI

Solicitud de decisión de control de acceso

(Este apéndice no forma parte integrante de la presente Recomendación.)

El PEP genera una solicitud de decisión de control de acceso, como se define en la cláusula 6.2.2, de acuerdo con la solicitud de acceso de un originador y la información adicional que facilita la CSE anfitriona utilizando el formato especificado por el PDP. El PEP puede enviar a un PDP una solicitud de decisión de control de acceso para que tome una decisión relativa al control del acceso a la información.

El PDP pide al PRP que recupere todas las políticas de control de acceso aplicables de acuerdo con la solicitud de decisión de control de acceso, y luego utiliza la solicitud para evaluar las políticas de control de acceso encontradas a fin de adoptar una decisión. La solicitud de decisión de control de acceso que envía el PEP al PDP puede contener la siguiente información:

– Un originador: es el ID del originador que envía una solicitud de acceso al recurso de destino.
– Un recurso: es el URI del recurso de destino al que el originador quiere acceder.
– Una operación: es la operación que el originador quiere efectuar en el recurso de destino.
– Una AccessTime: es la hora de acceso.
– Una LocationRegion: es la ubicación del originador.
– Una IPAddress: es la dirección IP del originador.

El URI del recurso de destino se utiliza para ubicar el recurso de destino y, posteriormente, encontrar las políticas de control de acceso asociadas.

El identificador del originador se utiliza para comparar con los sujetos que componen la regla a fin de comprobar si una regla es aplicable a la solicitud de decisión de control de acceso.

La operación se utiliza para comparar con las operaciones que componen la regla a fin de comprobar si la operación está permitida en la regla.

Las AccessTime, LocationRegion y/o LocationRegion se utilizan para comprobar los contextos que componen la regla a fin de garantizar que se cumplan algunas condiciones adicionales y, de esta manera, utilizar la regla para adoptar una decisión de control de acceso.

Apéndice VII

Orientaciones de aplicación e índice de soluciones

(Este apéndice no forma parte integrante de la presente Recomendación.)

La aplicación de esta Recomendación implica un proceso de evaluación de riesgos específicos según el contexto a partir del cual se determinan las soluciones de seguridad pertinentes.

En la cláusula 6 se muestran de forma general los procedimientos de seguridad oneM2M. En la cláusula 6.1.1 se presentan las interacciones entre capas, en la cláusula 6.1.2 la secuencia de eventos, y en la cláusula 6.2 información de fondo adicional, en especial a efectos de la autorización (cláusula 6.2.2).

La cláusula 7 sobre autorización y control de acceso se aplica independientemente del tipo de credenciales utilizadas. En la cláusula 7.1 se describe el marco general de gestión de las políticas de control de acceso oneM2M, que puede mejorarse con el soporte de marcos de control de acceso basado en funciones (cláusula 7.4) y la autorización dinámica (cláusula 7.3). Además, en la cláusula 11, sobre la base de las consideraciones anteriores, se proporciona una arquitectura de protección de la privacidad que facilita el establecimiento y la gestión de los perfiles de privacidad de los usuarios.

En este Apéndice se ha incluido el Cuadro VII.1 para ayudar a los responsables de la aplicación de la Recomendación a determinar las cláusulas que son pertinentes para un determinado tipo de credencial. Las cláusulas específicas que se aplican para apoyar la seguridad de extremo a extremo figuran en cursiva.

Cuadro VII.1 – Índice de cláusulas que especifican procedimientos según los tipos de credenciales

Procedimiento/ Solución	**PSK**	**Certificados**	**TEF (GBA, MEF, MAF)**
Provisión de seguridad a distancia	8.3.2.1	8.3.2.2, *8.7*	8.3.2.3 (GBA)
	9.2.1.1		9.2.1.2, 9.2.2.3, 9.2.2.4 (GBA), *9.2.3*
Establecimiento de asociación de seguridad	8.2.1, *8.4 (ESPrim), 8.5.2.3 (ESData con firma), 8.5.2.4 (ESData con firma y encriptación)*		
	9.1.1.1, 9.1.2.1		9.1.1.2, 9.1.2.2 (MAF)
	8.1.1, 8.2.2.1, *8.5.2.2.2 (ESData con encriptación)*	8.1.2, 8.2.2.2, *8.5.2.2.4 (ESData con encriptación)*	8.1.3, 8.2.2.3 (MAF), *8.8, 8.5.2.2.3 (ESData con encriptación)*
Detalles de algoritmo	10.2.1, *10.3.6*		
	10.2.2, 10.3	10.1, 10.2.3, 10.3	

Apéndice VIII

Apéndice en blanco

Este Apéndice se ha dejado deliberadamente en blanco.

Apéndice IX

Apéndice en blanco

Este Apéndice se ha dejado deliberadamente en blanco.

Apéndice X

Reglas de aplicación del lenguaje de marcaje de los términos y condiciones

(Este apéndice no forma parte integrante de la presente Recomendación.)

Las reglas típicas de aplicación se muestran a continuación y en la Figura X.1, y se repiten para cada fila.

Nota sobre las convenciones: las {} identifican las respuestas a la sentencia "if" anterior, los [] identifican el cuadro de filtro y los () contienen comentarios. La lógica se indica con sangrías a fin de mostrar mejor el anidamiento de las sentencias. La lógica funciona comprobando las mismas filas en los cuadros de filtro objeto de verificación.

Para generar el valor resumido de cada fila se aplica la siguiente lógica:

¿Si valor [cuadro de filtro actual] no es igual a "no recopilación de datos" o "no compartición de datos", etc = (Sin preferencia o límite)?

{Sí} ¿Es valor [cuadro de filtro actual] igual a valor resumido (valor compuesto) [cuadro de filtro anterior] de?

{Sí} Valor resumido [cuadro de filtro actual] igual al valor establecido.

{No} ¿Es valor establecido [cuadro de filtro actual] = "Sí"?

{Sí} Valor resumido [cuadro de filtro actual] establecido como valor resumido [cuadro de filtro anterior]

{No} Valor resumido [cuadro de filtro actual] establecido como valor resumido [cuadro de filtro actual].

{No} Valor resumido [cuadro de filtro actual] establecido como valor resumido [cuadro de filtro anterior]

Para generar el símbolo de aceptación de los términos y condiciones se utiliza la siguiente lógica:

¿Si valor [cuadro de filtro actual] es igual a "Sí"?

{Sí} Símbolo de aceptación de los términos y condiciones [cuadro de filtro actual] establecido como "☺" (se utiliza el emoji para que el resultado que vea el usuario sea independiente del idioma y necesite solo una pequeña cantidad de espacio en pantalla).

{No} ¿Valor [cuadro de filtro actual] igual a [cuadro de filtro anterior]?

{Sí} Símbolo de aceptación de los términos y condiciones [cuadro de filtro actual] establecido como "☺"

{No}Símbolo de aceptación de los términos y condiciones [cuadro de filtro actual] establecido como "☹"

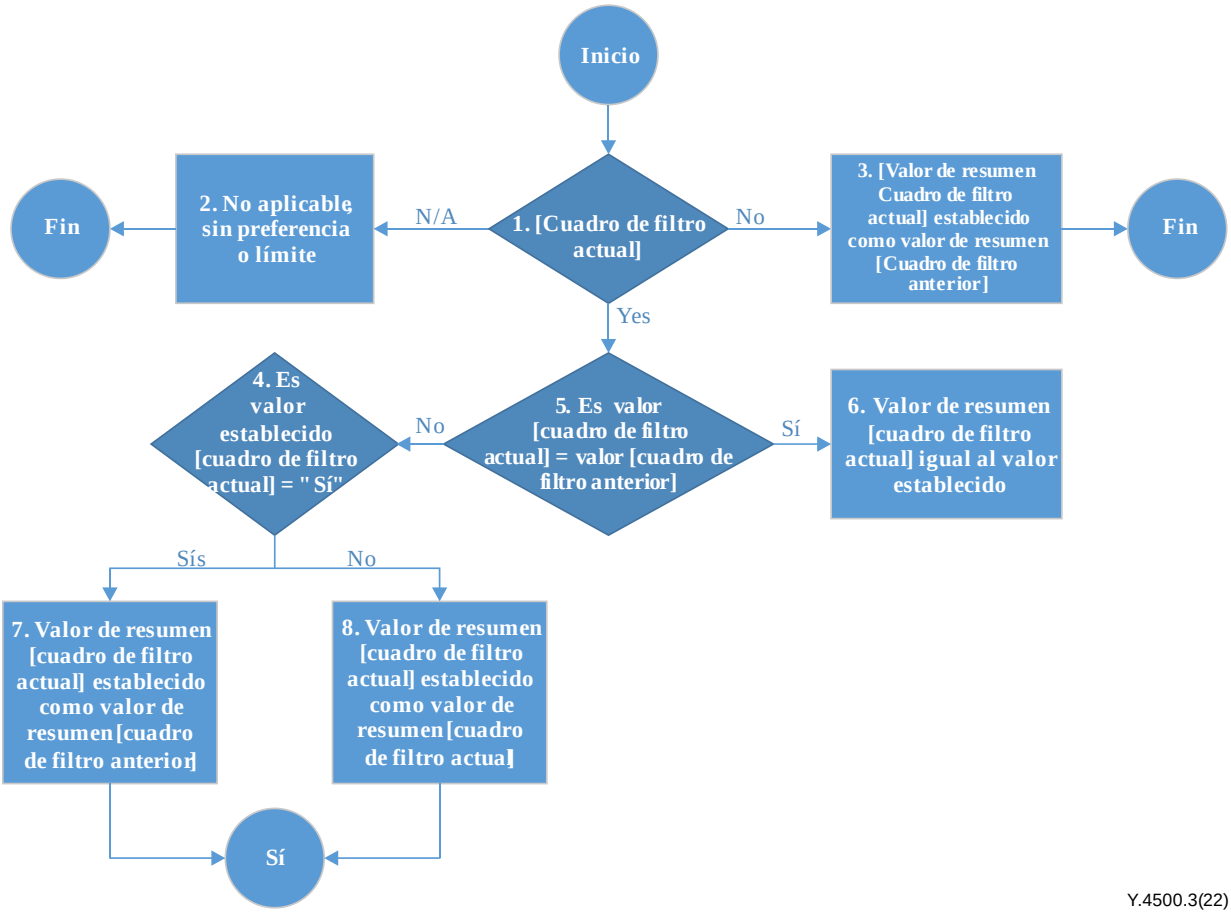


Figura X.1 – Reglas de aplicación del lenguaje de marcaje

Apéndice XI

Ejemplo de aplicación del SCEP

(Este apéndice no forma parte integrante de la presente Recomendación.)

XI.1 Introducción

En este Apéndice se describe una aplicación del protocolo simple de inscripción de certificados (SCEP). Puede encontrarse un guion que ejecuta los procedimientos aquí descritos en el repositorio Gitlab de oneM2M http://git.onem2m.org/

XI.2 Procedimiento de provisión de certificados utilizando el SCEP

En la Figura XI.2-1 se ilustra un diagrama de alto nivel de los procedimientos SCEP que contiene los siguientes bloques fundamentales de un servicio de automatización de certificados utilizando el SCEP [IETF RFC 8824].

– La provisión de perfiles es el actor principal y autorizado en cualquier sistema de automatización. La provisión informa al *cliente de automatización del dispositivo* y al servicio PKI, el emisor de credenciales, mediante el establecimiento de credenciales de dispositivo preautorizadas, de que varios dispositivos únicos entablarán contacto para solicitar certificados de cliente únicos.

– La capacidad de provisión informa tanto al dispositivo a distancia como al servicio PKI a través de un canal autentificado y confidencial de sus perfiles de provisión únicos. Dichos perfiles pueden revisarse en cualquier momento, lo que permite forzar el cambio de las credenciales existentes de ser necesario. Los protocolos de provisión habituales son TR-069, OMA-DM, etc.

– El *cliente de automatización del dispositivo*, o la inteligencia de la aplicación de certificados, proporciona una máquina de estados que utiliza los datos de provisión, es decir, los perfiles de provisión, para generar claves y solicitar y reemplazar certificados en periodos de tiempo predeterminados mediante la formulación de solicitudes de un cliente SCEP nativo. Por lo general, la inteligencia se basa en el tiempo, lo que garantiza la renovación oportuna de las claves y certificados existentes; sin embargo, también puede basarse en eventos, mediante la recepción de perfiles de provisión revisados desde el sistema de provisión. El cliente SCEP es una aplicación nativa instalada en sistemas, servidores o dispositivos, que se comunica con un respondedor SCEP a través de un protocolo definido en el proyecto de especificación histórica del IETF [IETF RFC 8824]. Cada respondedor SCEP se identifica en los distintos perfiles de provisión.

– En la Figura L.2-1 se muestran varios ejemplos de mensajes de respuesta a solicitudes de mensajes SCEP, documentados en los proyectos de especificación histórica del IETF [IETF RFC 8824]. El respondedor SCEP, al recibir una solicitud de certificado de cadena, responde proporcionando el certificado solicitado. A su vez, al recibir una solicitud de certificado de cliente, valida primero la identidad del solicitante y la prueba de posesión de una credencial única, antes de solicitar a la autoridad de certificación (CA) emisora que emita un nuevo certificado, y reenvía el nuevo certificado al cliente SCEP.

– El respondedor SCEP también puede rechazar la solicitud de certificado o indicar que la emisión está pendiente a la espera de una acción de la autoridad de certificación emisora. Al recibir una cadena de certificados de sustitución, el *cliente de automatización del dispositivo* valida la cadena de certificados recibida, lo que conllevar realizar una comprobación sobre la base de las respuestas CRL o OCSP. Solo al determinarse que la nueva cadena de certificados es apropiada, se guardará en la tienda de certificados de la aplicación y se sobrescribirá el certificado anterior. En caso de renovación, también pueden renovarse los custodios de confianza de pares.

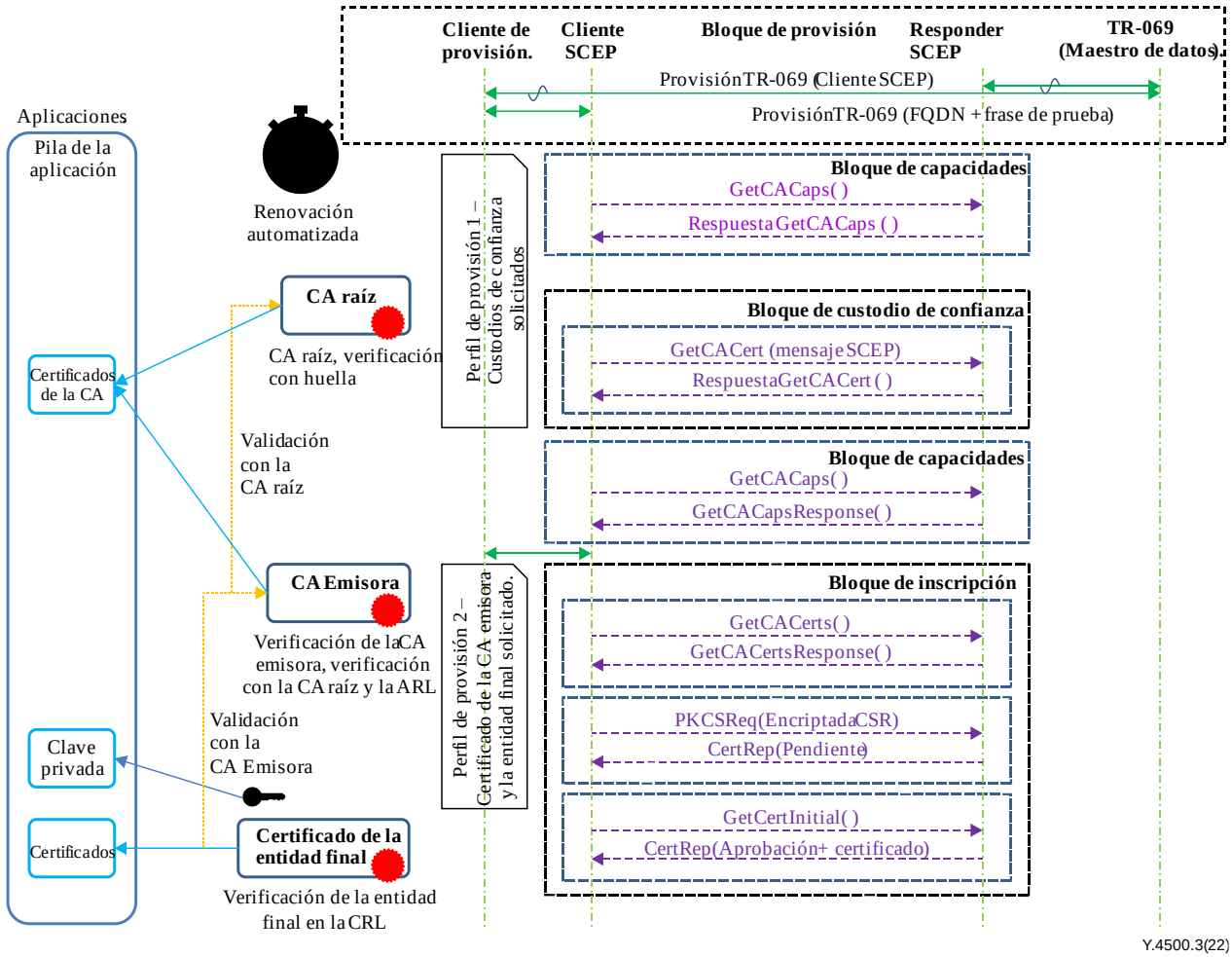


Figura XI.2-1 – Procedimiento de provisión de certificados SCEP

La solución de automatización de certificados SCEP se compone de las cinco funciones siguientes:

1) Configuración inicial del cliente SCEP con perfiles de provisión

La configuración inicial del cliente SCEP atiende la necesidad de establecer conjuntos de perfiles de provisión adaptados al contexto en un dispositivo de extremo. Las dos opciones obvias para crear perfiles de provisión son las siguientes:

1. configuración manual de cada dispositivo, y
2. provisión automatizada a partir de un servicio de gestión de dispositivos o de gestión de elementos, por ejemplo, mediante los procedimientos especificados en [UIT-T Y.4500.22].

El número de conjuntos de perfiles de provisión es igual al número de pilas de seguridad de la aplicación que sean necesarias.

Esta función descarga un conjunto de perfiles de provisión desde el servicio de gestión de dispositivos o de gestión de elementos con objeto de permitir las siguientes acciones:

– el establecimiento de un encadenamiento de credenciales criptográficas [únicas x509v3] hacia una CA raíz de confianza, lo que permite al dispositivo de extremo inicializar posteriormente su configuración [IETF RFC 5280];

– el establecimiento de un par de claves únicas localmente significativas;

– la generación de una solicitud de firma de certificado asociada;

– la validación fuera de banda de un custodio de confianza mediante la verificación de una huella contenida en el perfil de provisión;

– la validación individual de cada CA subordinada que se haya encontrado con su superior;
– la autentificación y aseguramiento, mediante un nombre de usuario y contraseña, de la solicitud de un certificado de cliente procedente de un emisor preautorizado (el respondedor SCEP);
– asimismo, la posible descarga y validación del custodio de confianza de un par fiable; estos custodios de confianza de los pares pueden actualizarse a partir de un perfil de provisión revisado.

2) Inteligencia del dispositivo y máquina de estados

La inteligencia del dispositivo y la máquina de estado son componentes fundamentales de cualquier solución de tipo SCEP, protocolo de gestión de certificados, versión 2, (CMPv2) o EST. Lógicamente, una buena máquina de estados puede accionar cualquier respondedor de mensajes en el que se soporte el SCEP.

La máquina de estados se activa a partir de un conjunto completo y válido de perfiles de provisión.

Esta función, se bien se ha concebido para operar de forma autónoma en el contexto de dispositivos IoT no atendidos que no dispongan de una interfaz de usuario para navegador web, se ha desarrollado para reflejar un recorrido de usuario basado en navegador. La intención es mantener la compatibilidad con cualquier proceso manual de prueba y diagnóstico que deban cumplir los dispositivos IoT y con los elementos del servicio que cuentan con una interfaz de usuario tradicional, por ejemplo, el uso de un teléfono inteligente en el dominio de domicilio oneM2M.

Esta función se compone de las siguientes etapas fundamentales:

1. El dispositivo solicita su propio custodio de confianza (CA raíz).
2. El custodio de confianza del dispositivo (CA raíz) se valida con una huella proporcionada por un perfil de provisión.
3. El dispositivo solicita sus propios certificados intermedios de manera sucesiva.
4. Los certificados intermedios del dispositivo se validan ante el emisor superior para evitar los riesgos de ataques de intermediario.
5. El dispositivo solicita un primer certificado de cliente, lo que presupone que el dispositivo no está en posesión de dicho certificado, pero sí de un conjunto válido de perfiles de provisión. En esta etapa siempre se solicita a la CA emisora que garantice la confidencialidad de las solicitudes de certificado. El cliente SCEP recupera la clave pública para la CA expedidora. La solicitud de certificado se encripta con la clave pública de modo que la solicitud pueda desencriptarse únicamente a través de la clave privada de la CA o la RA.
6. De requerirlo la autoridad de provisión, el dispositivo solicita un nuevo certificado o la renovación inmediata de uno existente. La solicitud de un nuevo certificado puede realizarse con una PKI diferente.
7. También se soporta la renovación automatizada de un certificado existente, basada, por ejemplo, en un porcentaje previsto de la vida útil transcurrida de los certificados actuales.
8. Todos los certificados se analizan para solicitar la respuesta CRL u OCSP asociada.
9. El cliente solicita el custodio de confianza de los pares si difiere del suyo propio.
10. De ser necesario, se solicita a la CA intermedia y la CA emisora de un par la autentificación mutua. Una vez que se ha establecido una cadena de certificados nueva, o de reemplazo, se valida dicha cadena, ya que es probable que se utilice para sustituir a la cadena de certificados buena existente.
11. Las claves se transfieren a las tiendas de aplicación seguras que corresponda.
12. Se notifica a la autoridad de provisión del certificado actual la información, de ser necesario.
13. Se eliminan los artefactos de certificado caducados.

NOTA – La lista anterior no establece un orden de máquinas de estados ni una solución concreta. Sin embargo, se asume que las soluciones sofisticadas superarán los estados identificados y las soluciones más sencillas pueden optar por omitir los estados que la solución de dispositivo no requiera.

3) Cliente SCEP

Por lo general, un cliente SCEP es una pieza de *software* de código abierto desarrollada para realizar acciones de solicitud de certificados al respondedor SCEP. La máquina de estados antes descrita dirige el cliente SCEP utilizando los datos objeto de provisión en el procedimiento de configuración inicial.

El cliente SCEP se ajusta a lo especificado en [IETF RFC 8824] y puede obtenerse a través de las comunidades de código abierto, si no se dispone de un cliente nativo en el momento. Véase, por ejemplo, [b-SSCEP], que se basa en el trabajo original de Martin Bartosch.

Se ha seleccionado este cliente SCEP ya que los autores han modificado su comportamiento para que sea compatible con una PKI de cadena larga (véase [b-SSCEP-I]).

Otra alternativa es el cliente SCEP basado en Java, puesto a disposición por Dave Grant y su equipo en [b-JSCEP].

NOTA – Este cliente también ha sido modificado para soportar una PKI de cadena larga y recientemente ha sido bifurcado por Wes Bunton para ajustarse específicamente a los requisitos de Android.

4) Respondedor SCEP

Un respondedor SCEP es un componente adicional de los servicios de empresa y de los servicios de PKI gestionada. Básicamente, un respondedor SCEP puede considerarse como un servicio adicional de autoridad de registro (RA).

Al recibir una petición, los respondedores SCEP proporcionarán custodios de confianza, CA intermedias, CA emisoras y certificados localmente significativos. Es necesario generar un par de claves privadas/públicas en el dispositivo.

Las solicitudes de emisión de certificados se examinarían sobre la base de un nombre de usuario y contraseña únicos mantenidos de forma segura dentro de los campos de nombre alternativo del sujeto de la solicitud y de frase de prueba que figuren en la solicitud de firma del certificado (véase [IETF RFC 8824]).

Normalmente, estas contraseñas, que son de un solo uso, caducan al emitirse el certificado, por lo que deben volver a establecerse cuando se soliciten servicios de renovación de certificados.

La solución de provisión identificada sería de autoridad (rastrearía los dispositivos y elementos gestionados), y efectuaría la provisión previa al respondedor SCEP de pares de nombre de usuario y contraseña válidos, antes de que el cliente SCEP los utilice.

Las autentificaciones que no sean satisfactorias se rechazan, mientras que las CSR autentificadas con éxito se transmiten a la PKI para su ejecución. Si la autentificación es satisfactoria, se devuelve un certificado de entidad final.

La solución de provisión puede incluso solicitar la revocación de los certificados de dispositivo que ya no se consideren de confianza.

5) PKI y certificados localmente significativos

Un servicio PKI proporciona el marco de conocimientos, competencias y conformidad que se necesita para dar soporte a la emisión de certificados SCEP. Entre los bloques fundamentales de una solución SCEP figuran: una PKI y CA, un respondedor SCEP (RA), un autentificador de solicitudes y un autorizador de solicitudes.

Es habitual que, en los equipos ubicados en los locales del cliente (CPE) o en el espacio IoT, las PKI se conciban sobre la base de una buena comprensión de los volúmenes de certificados, y de una comprensión de la separación operativa criptográfica requerida que debe aplicarse.

Autoridad de certificación

La autoridad de certificación (CA) SCEP firma los certificados de cliente. El nombre de la CA se guarda en el campo que corresponde al emisor de los certificados producidos. Antes de solicitar una operación PKI, el respondedor SCEP comparte con el cliente SCEP un certificado de "CA" emisora que se ajuste al perfil especificado en [IETF RFC 5280], y, opcionalmente, determinados certificados RA. Puede tratarse de un certificado CA emitido por una CA de nivel superior. El cliente construye una cadena de certificados completa a partir del custodio de confianza, validando cada certificado a su vez.

Autoridad de registro

La autoridad de registro (RA) SCEP, al igual que el respondedor SCEP, ejecuta controles de validación y autorización del solicitante SCEP y transfiere las solicitudes de certificación a la CA. El respondedor SCEP recibe un certificado de la CA y lo reenvía al cliente SCEP. El nombre de la RA no aparece en el campo del emisor de los certificados producidos.

Autentificación del solicitante

Al igual que en los demás protocolos basados en la criptografía de clave pública, la asociación entre las claves públicas utilizadas en el protocolo y las identidades a las que corresponden se autentifican de una forma criptográficamente segura. Este requisito es necesario para evitar un "ataque de intermediario", en el que el atacante puede manipular los datos mientras circulan entre los participantes del protocolo y subvertir la seguridad del mismo. La comunicación entre el solicitante y la autoridad de certificación se asegura empleando objetos de mensaje seguro SCEP, que especifican la manera en que debe utilizarse la sintaxis PKCS #7 para encriptar y firmar los datos de la CSR.

Autorización de la solicitud

Pueden soportarse los siguientes métodos de autentificación SCEP para autorizar certificados:

– utilización de nombres de usuario y contraseñas únicos;
– utilización de un certificado de entidad final único y de una prueba de posesión de la clave privada.

Bibliografía

[b-ITU-T X.510] Recomendación UIT-T X.510 (2020), *Tecnología de la información – Interconexión de sistemas abiertos – Directorio: especificaciones de protocolo para operaciones seguras*.

[b-ITU-T Y.4500.5] Recomendación UIT-T Y.4500.5 (2018), *Habilitación de la gestión del sistema oneM2M (OMA).*

[b-ITU-T Y.4500.6] Recomendación UIT-T Y.4500.6 (2018), *Habilitación de la gestión de Sistema oneM2M (BBF).*

[b-ATIS.oneM2M.TS0003] oneM2M Security Solutions TS-0003 V2.4.1-2016 ATIS
https://www.onem2m.org/technical/partners-releases

[b-ETSI TS 103 645] ETSI TS 103 645 (2019), *Cyber Security For Consumer Internet Of Things*.
https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

[b-ETSI TS 118 103] oneM2M Security solutions TS-0003 v2.4.1 ETSI
https://www.etsi.org/deliver/etsi_ts/118100_118199/118103/02.04.01_60/ts_118103v020401p.pdf

[b-IETF RFC 6455] IETF RFC 6455 (2011), *The Web Socket Protocol*, December.

[b-IETF RFC 7252] IETF RFC 7252 (2014), *The Constrained Application Protocol (CoAP)*.

[b-IETF RFC 7230] IETF RFC 7230 (2014), *Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing*.

[b-ISO 3166-1] ISO 3166-1:2020, *Codes for the representation of names of countries and their subdivisions – Part 1: Country codes*.

[b-ISO/IEC 7816-5] ISO/IEC 7816-5:2004, *Identification cards – Integrated circuit cards – Part 5: Registration of Application Providers*.

[b-GP DTSERAM] GlobalPlatform (2015), *Device Technology Secure Element Remote Application Management* v1.0 GPD_SPE_008.
https://globalplatform.org/specs-library/secure-element-remote-application-management-v1-0-1/

[b-GP TEEAdmin] GlobalPlatform, *Device Technology TEE Administration framework, DRAFT*.

[b-GP TEESystem] GlobalPlatform (2017), *Device Technology TEE System Architecture*, Version 1.0.
https://globalplatform.org/specs-library/tee-system-architecture/

[b-GSMA IoT-SGA] IoT Security Guidelines and Assessment
https://www.gsma.com/iot/iot-security/iot-security-guidelines/

[b-IANA JWT] IANA JSON Web Token (JWT) registry.
http://www.iana.org/assignments/jwt/jwt.xhtml

[b-IoTSF SD-BP] Secure Design: Best Practice Guide. Release 2. November 2019
https://www.iotsecurityfoundation.org/wp-content/uploads/2019/12/Best-Practice-Guides-Release-2_Digitalv3.pdf

[b-JSCEP] A Java implementation of the Simple Certificate Enrolment Protocol.
https://github.com/jscep/jscep

[b-Menezes] *Handbook of Applied Cryptography*, A.J. Menezes, P. C. van Oorschot, S. A. Vanstone, CRC Press, 1996.

[b-NIST 800-162] *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*, NIST Special Publication 800-162. http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf

[b-OASIS XACML] *eXtensible Access Control Markup Language (XACML)*, Version 3.0., 22 January 2013. OASIS Standard.

[b-OMA REST] OMA-TS-REST-NetAPI-TerminalLocation-V1-0-20130924-A: *RESTful Network API for Terminal Location*, Version 1.0.

[b-oneM2M.XML] *oneM2M XML Schemas*. http://www.onem2m.org/technical/developers-corner/tools/xml-schemas

[b-oneM2M TR0002] oneM2M TR-0002: *Use Case collection*.

[b-oneM2M TR0008] oneM2M TR-0008: *Security*.

[b-oneM2M TR0012] oneM2M TR-0012: *End to End security*.

[b-oneM2M TR0019] oneM2M TR-0019: *Dynamic annex Authorization*.

[b-SSCEP] A command line client for the SCEP protocol. https://github.com/certnanny/sscep

[b-SSCEP-I] https://github.com/certnanny/sscep/issues/42

[b-TSDSI STD T1.oneM2M TS-0003-2.4.1 V1.0.0] TSDSI Technical Standard TSDSI STD T1.oneM2M TS-0003-2.4.1 V1.0.0 (2017), *Security Solutions*. https://www.onem2m.org/technical/partners-releases (under release 2)

[b-TTAT.MM-TS.0003 v2.4.1] TTAT, *oneM2M Security Solutions TS-0003 v2.4.1 TTAM*. https://www.onem2m.org/technical/partners-releases (under release 2) https://www.tta.or.kr/tta/ttaSearchView.do?key=77&rep=1&searchStandardNo=TTAT.MM-TS.0003%20v2.4.1&searchCate=TTAS

[b-TTC TS-M2M-0003v2.4.1] TTC Japan technical specification (2016), *oneM2M Security Solutions TS-0003 v2.4.1*. https://www.ttc.or.jp/application/files/8415/5442/6047/TS-M2M-0003v2.4.1.pdf

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos, comunicaciones de sistemas abiertos y seguridad
Serie Y	**Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes**
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2023