ITUPublications
Recomendaciones

Unión Internacional de Telecomunicaciones
Sector de la Normalización

Recomendación

UIT-T X.1817 (09/2023)

SERIE X: Redes de datos, comunicaciones de sistemas abiertos y seguridad

Seguridad de las IMT-2020

Requisitos de seguridad del servicio de mensajería 5G

RECOMENDACIONES UIT-T DE LA SERIE X

Redes de datos, comunicaciones de sistemas abiertos y seguridad

REDES PÚBLICAS DE DATOS	X.1-X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200-X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300-X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400-X.499
DIRECTORIO	X.500-X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600-X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700-X.799
SEGURIDAD	X.800-X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850-X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900-X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	X.1000-X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD (1)	X.1100-X.1199
SEGURIDAD EN EL CIBERESPACIO	X.1200-X.1299
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	X.1300-X.1499
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	X.1500-X.1599
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	X.1600-X.1699
Visión general de la seguridad de la computación en nube	X.1600-X.1601
Diseño de la seguridad de la computación en nube	X.1602-X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640-X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660-X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680-X.1699
COMUNICACIÓN CUÁNTICA	X.1700-X.1729
SEGURIDAD DE LOS DATOS	X.1750-X.1799
SEGURIDAD EN LAS REDES IMT-2020	**X.1800-X.1819**

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

Recomendación UIT-T X.1817

Requisitos de seguridad del servicio de mensajería 5G

Resumen

En la Recomendación UIT-T X.1817 se describen los requisitos de seguridad del servicio de mensajería 5G, incluidos los relativos al acceso, la gestión y el control del servicio de mensajería 5G.

Historia*

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único
1.0	ITU-T X.1817	2023-09-08	17	11.1002/1000/15524

Palabras clave

Marco de seguridad, requisito de seguridad, servicio de mensajería 5G.

* Para acceder a la Recomendación, introduzca el URL https://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación.

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/.

ÍNDICE

Página

1 Alcance 1

2 Referencias 1

3 Definiciones 1

3.1 Términos definidos en otros documentos 1

3.2 Términos definidos en esta Recomendación 2

4 Abreviaturas y siglas 2

5 Convenios 3

6 Consideraciones generales 3

6.1 Servicio de mensajería 5G 3

6.2 Arquitectura de los requisitos de seguridad del servicio de mensajería 5G 3

6.3 Diferencia funcional entre los requisitos de seguridad del servicio de mensajería 5G y de los servicios 4G/3G/5G/WLAN 4

7 Requisitos de seguridad para el acceso al servicio de mensajería 5G 5

7.1 Requisitos de seguridad de las tarjetas de usuario para recomposiciones y cambios 5

7.2 Autentificación de usuarios 5

7.3 Seguridad en la recepción de mensajes 8

7.4 Seguridad en el envío de mensajes 8

7.5 Seguridad en el acceso a los mensajes 8

8 Requisitos de seguridad para la gestión del servicio de mensajería 5G 9

8.1 Seguridad en la gestión de usuarios 9

8.2 Gestión de claves y certificados 9

8.3 Auditoría de seguridad 10

8.4 Seguridad en la gestión del *software* 11

9 Requisitos de seguridad para el control del servicio de mensajería 5G 11

9.1 Restricciones aplicables a la capacidad del servicio 11

9.2 Lista negra de partes llamantes 11

9.3 Lista negra de partes llamadas 11

Bibliografía 12

Recomendación UIT-T X.1817

Requisitos de seguridad del servicio de mensajería 5G

1 Alcance

El servicio de mensajería 5G es una versión mejorada del servicio de mensajes cortos (SMS). Se trata de un servicio comercial de telecomunicaciones básico, que integra el servicio de mensajes cortos (SMS) definido por el 3GPP y el servicio de comunicación enriquecida (RCS) definido por la GSMA. En concreto, admite tanto mensajes entre personas, o entre aplicaciones y personas, como distintos tipos de medios (por ejemplo, textos largos, imágenes, vídeos, audios, archivos y localizaciones) en dichos mensajes. En la presente Recomendación se describen requisitos de seguridad que podrían atenuar las amenazas y los retos en materia de seguridad del servicio de mensajería 5G. En concreto, se detallan los requisitos de seguridad del servicio de mensajería 5G, incluidos los relativos al acceso, la gestión y el control del servicio de mensajería 5G. Por último, se detallan las diferencias funcionales entre los requisitos de seguridad del servicio de mensajería 5G y de los servicios 4G/3G/5G/WLAN.

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.

[ETSI TS 123 040] ETSI TS 123 040 v17.2.0 (2022), *Digital cellular telecommunications system (Phase 2+) GSM; Universal Mobile Telecommunications System (UMTS); LTE;5G; Technical realization of the Short Message Service (SMS)*

[ETSI TS 124 229] ETSI TS 124 229 (2017), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3*

[ETSI TS 129 109] ETSI TS 129 109 (2018), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Stage 3*

[ISO/IEC 11770-1] ISO/IEC 11770-1:2010, *Information technology – Security techniques – Key management – Part 1: Framework.*

3 Definiciones

3.1 Términos definidos en otros documentos

En esta Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 chatbot [b-GSMA RCC.71]: Servicio automatizado basado en el servicio de comunicación enriquecida (RCS) y proporcionado a usuarios, cuyo resultado se presenta en forma de conversación.

3.2 Términos definidos en esta Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 centro de mensajes 5G: Servidor que presta el servicio de mensajería 5G.

3.2.2 plataforma de mensajes: Plataforma utilizada para que las aplicaciones de terceras partes puedan conectarse al centro de mensajes 5G.

3.2.3 equipo de usuario (EU) de mensajes 5G: Equipo de usuario (EU) 5G, cuya aplicación de mensajes soporta tanto el servicio de mensajes cortos (SMS) como el servicio de comunicación enriquecida (RCS).

3.2.4 servicio de mensajería 5G: Servicio de mensajería 5G, que integra el servicio de mensajes cortos (SMS) y el servicio de comunicación enriquecida (RCS). El servicio de mensajería 5G admite tanto mensajes entre personas, o entre aplicaciones y personas, como distintos tipos de medios (por ejemplo, textos largos, imágenes, vídeos, audios, archivos y localizaciones) en dichos mensajes.

4 Abreviaturas y siglas

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

3GPP	Proyecto de asociación tercera generación (*3rd Generation Partnership Project*)
A2P	Aplicación a persona (*application to person*)
AKA	Acuerdo de autentificación y claves (*authentication and key agreement*)
GBA	Arquitectura de inicialización genérica (*generic bootstrapping architecture*)
GSMA	Asociación del Sistema Mundial para Comunicaciones Móviles (*Global System for Mobile communications Association*)
HSS	Servicio de abonado en el hogar (*home subscriber service)*
HTTPS	Protocolo de transferencia de hipertexto seguro (*hypertext transfer protocol secure*)
IMS	Subsistema multimedia IP (*IP multimedia subsystem*)
MO	Origen móvil (*mobile originate*)
MT	Terminación móvil (*mobile terminate*)
OTP	Contraseña de uso único (*one-time password*)
P2P	Persona a persona (*person to person*)
RCS	Servicio de comunicación enriquecida (*rich communication service*)
SIM	Módulo de identidad de abonado (*subscriber identity module*)
SIP	Protocolo de inicio de sesión (*session initiation protocol*)
SMS	Servicio de mensajes cortos (*short message service*)
EU	Equipo de usuario (*user equipment*)
UDM	Gestión de datos unificada (*unified data management*)
VoLTE	Voz por evolución a largo plazo (*voice over long-term evolution*)
WLAN	Red de área local inalámbrica (*wireless local area network*)

5 Convenios

En la presente Recomendación se utilizan los siguientes convenios:

La expresión "**se requiere**" indica que el requisito debe cumplirse estrictamente, no permitiéndose desviación alguna si se pretende declarar la conformidad con la presente Recomendación.

La expresión "**se recomienda**" indica que se trata de un requisito recomendado y que, por ende, no es absolutamente obligatorio. El cumplimiento de ese requisito no es necesario para acreditar la conformidad.

6 Consideraciones generales

6.1 Servicio de mensajería 5G

De acuerdo con el perfil universal del servicio de comunicación enriquecida (RCS) elaborado por la GSMA, el servicio de mensajería 5G facilita la prestación de servicios avanzados, entre ellos, servicios de mensajería multimedios, chats de grupo y plataformas de mensajes. El servicio de mensajería 5G se basa en el portal del servicio de mensajes cortos (SMS) nativo del terminal, permite a los usuarios enviar y recibir texto, imágenes, audio, vídeos, datos de localización, información de contactos y otros contenidos multimedios, e incluye las siguientes funciones de servicio:

- Mensajes de persona a persona (P2P):

Los mensajes P2P son mensajes enviados entre usuarios individuales y admiten los siguientes contenidos multimedios: texto (incluidos emoticonos), imágenes, audio, vídeos, datos de localización, contactos (vCard) y documentos.

- Mensajes de grupo:

Un mensaje de grupo es un mensaje enviado por un usuario individual a varios usuarios individuales al mismo tiempo. El usuario puede introducir los números de los distintos contactos simultáneamente, o seleccionar varios destinatarios de la agenda, para enviarles un mensaje de grupo. Todos los destinatarios reciben el mismo mensaje, enviado por el remitente con su número de teléfono móvil real, y pueden responder directamente al mismo a través de un mensaje P2P.

- Mensajes de chats de grupos:

Se entiende por mensajes de chat de grupo la interacción de mensajes entre los usuarios individuales que integran un grupo.

- Mensajes de aplicación a persona (A2P):

Un mensaje A2P es un mensaje originado con ayuda de una aplicación y destinado al equipo móvil de un usuario. La mensajería A2P permite a las marcas comerciales comunicarse con los usuarios a través de chatbots. Los usuarios pueden enviar mensajes RCS a chatbots con texto (incluidos emoticonos), imágenes, audio, vídeos, datos de localización, contactos (vCard) y documentos. Los chatbots pueden ponerse en contacto con los usuarios de forma individualizada o colectiva y enviarles mensajes enriquecidos con texto (emoticonos incluidos), imágenes, audio, vídeos, datos de localización, contactos (vCard) y documentos. Los chatbots podrían enviar "tarjetas enriquecidas" con una lista fija de respuestas y acciones propuestas, conocida como *suggested chip list*.

6.2 Arquitectura de los requisitos de seguridad del servicio de mensajería 5G

La Figura 1 muestra la arquitectura de los requisitos de seguridad del servicio de mensajería 5G, que se articula en torno a los requisitos de seguridad del plano de usuario, del plano de gestión y del plano de control del servicio de mensajería 5G.

Entre los requisitos de seguridad del plano de usuario del servicio de mensajería 5G figuran los requisitos de seguridad de las tarjetas de usuario para recomposiciones y cambios, la autentificación

de usuarios, la seguridad en la recepción de mensajes, la seguridad en el envío de mensajes y la seguridad en el acceso a los mensajes.

Entre los requisitos de seguridad del plano de gestión del servicio de mensajería 5G figuran la seguridad en la gestión de usuarios, la gestión de claves y certificados, la auditoría de seguridad y la seguridad en la gestión de los programas informáticos.

Entre los requisitos de seguridad del plano de control del servicio de mensajería 5G figuran la restricción de la capacidad de servicio, el control por lista negra de partes llamantes y el control por lista negra de partes llamadas.

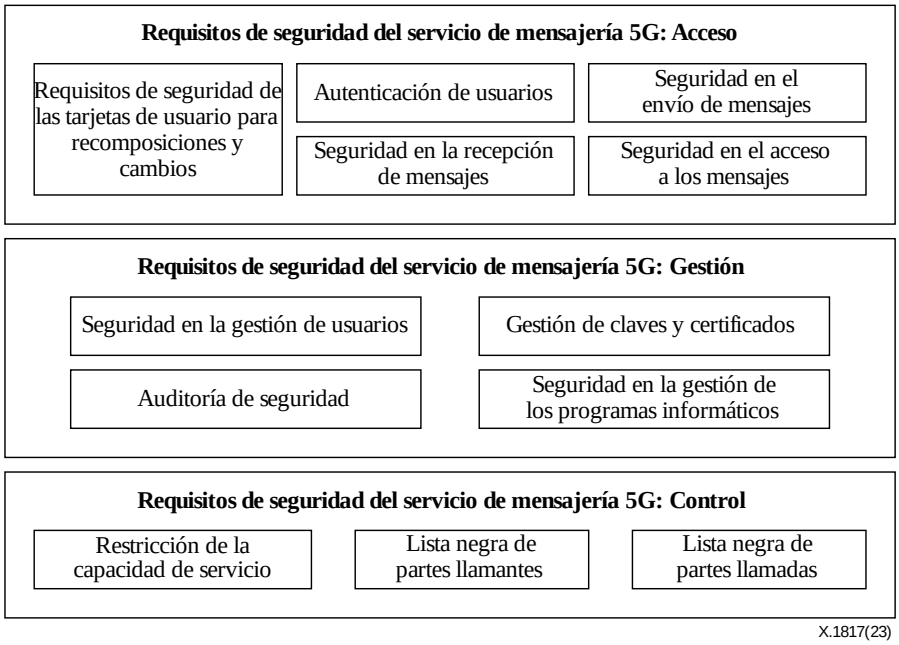

Figura 1 – Arquitectura de los requisitos de seguridad del servicio de mensajería 5G

6.3 Diferencia funcional entre los requisitos de seguridad del servicio de mensajería 5G y de los servicios 4G/3G/5G/WLAN

El servicio de mensajería 5G y el servicio SMS tradicional se diferencian en que el segundo solo admite el envío de mensajes de texto, mientras que el primero permite enviar diversos tipos de medios, por ejemplo, texto (incluidos emoticonos), miniaturas, imágenes, audio, vídeo, datos de localización, contactos y documentos.

Cuando se utilizan servicios de mensajería 5G, los terminales pueden acceder a los módulos de funciones a través de redes 3G, 4G, 5G o de área local inalámbrica (WLAN). Una vez completado el acceso a la red, los terminales obtienen primero los parámetros de servicio del servidor de configuración y, a continuación, inician un proceso de registro de protocolo de inicio de sesión (SIP) en el punto de acceso. Una vez registrados con éxito, pueden enviar y recibir mensajes 5G, incluidos mensajes personales y comerciales.

La arquitectura de los requisitos de seguridad de los mensajes 5G descrita en la cláusula 6.2 contempla la arquitectura de protección de la seguridad de los mensajes 5G. Los servicios de mensajería 5G estarán protegidos con independencia del modo de red a través del cual se acceda a los terminales.

7 Requisitos de seguridad para el acceso al servicio de mensajería 5G

7.1 Requisitos de seguridad de las tarjetas de usuario para recomposiciones y cambios

En cuanto a los usuarios de servicios de voz por evolución a largo plazo (VoLTE) y mensajería 5G que deban cambiar su tarjeta de módulo de identidad de abonado (SIM) debido al robo o la pérdida irreversible de la misma, se recomienda que el centro de mensajes 5G actualice la información conexa para que los usuarios puedan utilizar el servicio de mensajería 5G sin problemas después de cambiar la tarjeta SIM.

7.2 Autentificación de usuarios

Se requiere que la autentificación de usuarios entre el emisor y el receptor del mensaje cumpla los requisitos de autentificación y que la plataforma de servicio sólo abra el servicio de mensajería 5G a usuarios autentificados.

7.2.1 Autentificación personal de usuarios

Los mensajes 5G abarcan una serie de métodos de implementación de servicios, que incluyen diversos mecanismos de autentificación de usuarios. En el Cuadro 1 se muestran los distintos tipos de servicios de mensajería 5G y sus correspondientes requisitos de seguridad en materia de autentificación.

Cuadro 1 – Requisitos de seguridad en materia de autentificación de los servicios de mensajería 5G

Servicio de mensajería 5G	Requisitos de seguridad en materia de autentificación
Mensajería 5G (diversas interacciones de mensajería instantánea, incluidos mensajes P2P, chats de grupo, mensajes de chatbots y otros elementos de señalización y de medios)	USIM IMS AKA (el registro SIP admite la autentificación AKA)
Mensajería 5G (almacenamiento de mensajes, incluida la carga y descarga de contenidos multimedios en mensajes)	USIM GBA_ME
Descubrimiento de chatbots	
Consulta de información a chatbots	
Gestión de configuración del terminal	La primera vez, se utiliza la autentificación por inserción del número de teléfono móvil (red celular) o la contraseña de uso único (OTP) por SMS (red no celular), en el proceso ulterior de obtención de la configuración. La gestión de configuración del terminal puede elegir la autentificación de arquitectura de inicialización genérica (GBA), según sea necesario. También puede seleccionar el mecanismo de firma colaborativa para la autentificación. Se recomienda que el SMS OTP sea conforme con [ETSI TS 123 040 v17.2.0]

A continuación, se describen los métodos de autentificación:

a) USIM IMS AKA: Para un usuario de mensajes 5G, durante el registro del subsistema multimedia IP (IMS) en el centro de mensajes 5G, el centro de mensajes 5G obtiene el vector de autentificación de acuerdo de autentificación y claves (AKA) del usuario del HSS/UDM propiedad del usuario a través de la interfaz Zh y completa la autentificación IMS AKA del usuario basándose en dicho vector de autentificación. Se recomienda que la certificación AKA se ajuste a la especificación [ETSI TS 124 229].

b) USIM GBA_ME: Se requiere que los terminales que soportan los mensajes 5G soporten también interfaces GBA. Se requiere que los servidores de aplicaciones no SIP del sistema de mensajería 5G soporten interfaces GBA Zn. Se recomienda que la certificación GBA se ajuste a la especificación [ETSI TS 124 229].

c) Gestión de configuración del terminal: La primera vez, se utiliza la autentificación por inserción del número de teléfono móvil (red celular) o la OTP por SMS (red no celular), en el proceso ulterior de obtención de la configuración. Para proteger las claves de posibles filtraciones, puede utilizarse el mecanismo de firma colaborativa.

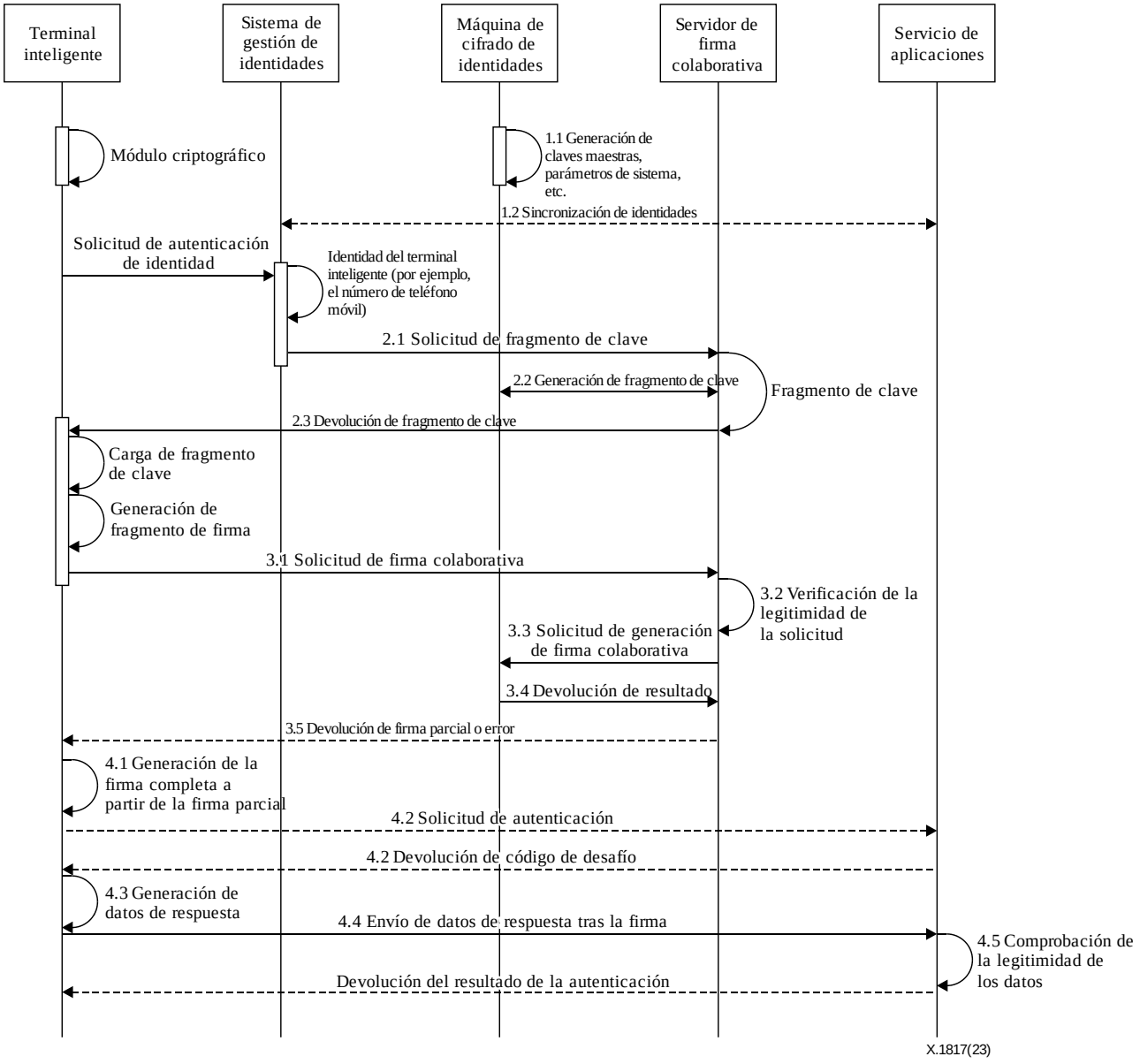

Figura 2 – Mecanismo de firma colaborativa para el servicio de mensajería 5G

El mecanismo de firma colaborativa que ilustra la Figura 2 se utiliza para la autentificación de identidades en la mensajería 5G. El proceso principal consiste en lo siguiente:

1 La máquina de cifrado de identidades genera la clave maestra, los parámetros del sistema y el componente de clave de identidad. La sincronización de identidades entre el sistema de gestión de identidades y el servicio de aplicaciones puede basarse en el algoritmo preestablecido en función de la clave maestra, los parámetros del sistema y el componente de clave de identidad. El algoritmo preestablecido incluye al menos uno de los algoritmos de

generación de claves, de firma y de verificación. A continuación se describe el proceso paso a paso:

- Paso 1.1: La máquina de cifrado de identidades genera la clave maestra, los parámetros del sistema y el componente de clave de identidad.
- Paso 1.2: La sincronización de identidades entre el sistema de gestión de identidades y el servicio de aplicaciones puede basarse en el algoritmo preestablecido en función de la clave maestra, los parámetros del sistema y el componente de clave de identidad.

2 Tras la sincronización de identidades entre el sistema de gestión de identidades y el servicio de aplicaciones, la identidad del terminal inteligente se utiliza para la autentificación de identidad mediante firma colaborativa con el servidor de firma colaborativa. El terminal inteligente envía su identidad (por ejemplo, el número de teléfono móvil) al sistema de gestión de identidades. El sistema de gestión de identidades envía una solicitud de clave al servidor de firma colaborativa basándose en la identidad del terminal inteligente. El servidor de firma colaborativa devuelve un fragmento de clave al terminal inteligente basándose en la solicitud de clave. A continuación se describe el proceso paso a paso:

- Paso 2.1: El terminal inteligente envía una solicitud de autentificación de identidad y solicita un fragmento de clave al servidor de firma colaborativa.
- Paso 2.2: El servidor de firma colaborativa genera un fragmento de clave.
- Paso 2.3: El servidor de firma colaborativa devuelve el fragmento de clave al terminal inteligente basándose en la solicitud de clave recibida.

3 El terminal inteligente carga el fragmento de clave y genera el fragmento de firma correspondiente. El terminal inteligente envía una solicitud de firma colaborativa al servidor de firma colaborativa basándose en dicho fragmento de firma. El servidor de firma colaborativa verifica la legitimidad de la solicitud de firma colaborativa. Una vez autenticada la identidad de la firma colaborativa, el servidor de firma colaborativa reenvía la solicitud de firma colaborativa a la máquina de cifrado de identidades. La máquina de cifrado de identidades genera una firma parcial de acuerdo con la solicitud de firma colaborativa y el servidor de firma colaborativa devuelve esa firma parcial al terminal inteligente. A continuación se describe el proceso paso a paso:

- Paso 3.1: El terminal inteligente envía una solicitud de firma colaborativa al servidor de firma colaborativa basándose en el fragmento de firma recibido.
- Paso 3.2: El servidor de firma colaborativa verifica la legitimidad de la solicitud de firma colaborativa.
- Paso 3.3: Una vez autenticada la identidad de la firma colaborativa, el servidor de firma colaborativa reenvía la solicitud de firma colaborativa a la máquina de cifrado de identidades.
- Paso 3.4: La máquina de cifrado de identidades genera una firma parcial de acuerdo con la solicitud de firma colaborativa y devuelve esa firma parcial al servidor de firma colaborativa.
- Paso 3.5: El servidor de firma colaborativa devuelve la firma parcial al terminal inteligente.

4 El terminal inteligente genera una firma completa basándose en la firma parcial. El proceso de autentificación de identidad mediante firma conjunta con el servicio de aplicaciones basado en la firma completa consiste en lo siguiente. El terminal inteligente envía una solicitud de autentificación al servicio de aplicaciones basándose en la firma completa. El servicio de aplicaciones devuelve al terminal inteligente un código de desafío basado en la solicitud de autentificación. El terminal inteligente genera datos de respuesta en función del fragmento de clave local y del código de desafío recibidos y envía los datos de respuesta al servicio de aplicaciones. Tras recibir los datos de respuesta, el servicio de aplicaciones

verifica la legitimidad de los mismos y verifica la identidad del terminal inteligente basándose en la firma completa. La autentificación de la identidad se completa con ayuda de la firma conjunta y el servicio de aplicaciones devuelve el resultado de la autentificación al terminal inteligente. A continuación se describe el proceso paso a paso:

- Paso 4.1: El terminal inteligente genera la firma completa a partir de la firma parcial.
- Paso 4.2: El terminal inteligente envía al servicio de aplicaciones una solicitud de autentificación basada en la firma completa y el servicio de aplicaciones envía un código de desafío al terminal inteligente.
- Paso 4.3: El terminal inteligente genera datos de respuesta en función del fragmento de clave local y del código de desafío recibidos. El fragmento de clave local es el fragmento de clave enviado por el servidor de firma colaborativa.
- Paso 4.4: El terminal inteligente envía los datos de respuesta al servicio de aplicaciones.
- Paso 4.5: El servicio de aplicaciones verifica la legitimidad de los datos de respuesta. La autentificación de la identidad se completa con ayuda de la firma conjunta y el servicio de aplicaciones devuelve el resultado de la autentificación al terminal inteligente.

7.2.2 Autentificación de servidores de chatbots

Antes de conectarse a la plataforma de mensajes, los chatbots deben autenticarse. A tal efecto se combinan lo sistemas de autentificación de plataforma y de autentificación de capa de aplicación. La autentificación de la plataforma puede realizarse a partir de un certificado digital basado en el protocolo de transferencia de hipertexto seguro (HTTPS) y la autentificación de la capa de aplicación puede basarse en un nombre de usuario y una contraseña.

Los servidores de los chatbots deben solicitar un certificado de servidor a través de una autoridad de certificación (CA) legal y proporcionar el certificado raíz de la CA, el nombre de dominio legal o la dirección IP de los propios servidores a la plataforma de mensajes para el examen del registro durante el proceso de registro del usuario. Una vez completado el registro, la plataforma de mensajería lleva a cabo el proceso de autentificación de identidad en los servidores de los chatbots durante el proceso de acceso de estos últimos. Dicho proceso de autentificación incluye la verificación de los certificados de los servidores de los chatbots, la autentificación de la identidad de los chatbots, etc.

7.3 Seguridad en la recepción de mensajes

Las aplicaciones de mensajería 5G podrían cooperar con el sistema del terminal para ser las únicas capaces de recibir mensajes 5G y garantizar así que estos últimos no se utilicen de forma malintencionada y que los datos privados de los mensajes de los usuarios no se filtren.

7.4 Seguridad en el envío de mensajes

Las aplicaciones de mensajería 5G podrían cooperar con el sistema del terminal para ser las únicas capaces de enviar mensajes 5G y que no se concedan permisos para enviar mensajes a ninguna otra aplicación, a fin de garantizar que estos últimos no se utilicen de forma malintencionada.

7.5 Seguridad en el acceso a los mensajes

Las aplicaciones de mensajería 5G podrían cooperar con los sistemas de los terminales para restringir las capacidades de acceso autorizado de los mensajes 5G. Se requiere que la aplicación de mensajería 5G sea la única capaz de leer los archivos de los mensajes en el marco del terminal, o de realizar otras operaciones de gestión (por ejemplo, borrar datos, realizar copias de seguridad, etc.). Se recomienda que, en el marco de la plataforma, los mensajes puedan ser consultados y leídos (incluidos los datos relacionados con el registro) por sus propietarios y que otros usuarios (incluidos los administradores) carezcan de acceso a los mismos por norma general.

8 Requisitos de seguridad para la gestión del servicio de mensajería 5G

8.1 Seguridad en la gestión de usuarios

8.1.1 División de funciones y permisos

El sistema de seguridad en materia de gestión de usuarios divide la plataforma de servicio en capas y áreas según la zonificación del módulo de servicio y las funciones de los privilegios. Se recomienda crear una cuenta de administrador acorde a los privilegios concedidos, ya sea en calidad de superadministrador, administrador de servicios o auditor:

a) Superadministradores: tienen autoridad de gestión avanzada en la plataforma de función de servicio, lo que significa que pueden gestionar a los administradores de servicios y a los auditores.

b) Administradores de servicios: tienen autoridad parcial o total a efectos de la gestión y el funcionamiento de los servicios. Sin embargo, carecen de autoridad en términos de auditoría y no pueden gestionar a otros administradores de servicios.

c) Auditores: tienen autoridad para realizar auditorías operativas y de registro, pero no para tramitar servicios.

8.1.2 Supervisión de comportamientos anómalos

Consiste en supervisar y auditar comportamientos anómalos tales como un inicio de sesión anómalo, un inicio de sesión desde varios lugares al mismo tiempo o el envío de mensajes por encima de un cierto umbral (para clasificar la acción como envío de mensajes basura). Ante estos comportamientos anómalos, es necesario tomar medidas (por ejemplo, añadir a una lista negra y congelar la cuenta) que pongan límites a esos usuarios anómalos.

8.2 Gestión de claves y certificados

8.2.1 Gestión de claves

La gestión de claves es el mecanismo de gestión mediante el cual el terminal de mensajes 5G y la plataforma de servicios gestionan sus claves de cifrado de datos sensibles. Se recomienda crear distintos conjuntos de claves de cifrado para los distintos tipos de datos sensibles, que la plataforma o el terminal puedan utilizar a efectos del almacenamiento cifrado de datos sensibles. Se recomienda que los requisitos de gestión de claves se ajusten a la especificación [ISO/IEC 11770-1].

El sistema de mensajería 5G podría diseñar claves para proteger diferentes objetos, incluidos al menos los tipos de claves descritos en el Cuadro 2:

Cuadro 2 – Tipos de claves del sistema de mensajería 5G y descripciones conexas

Tipos	Descripciones
Clave de almacenamiento seguro de datos	Protege los datos importantes almacenados y la información sensible.
Clave de comunicación segura	La clave GBA se genera durante el proceso de autentificación de inicio de sesión para terminales y múltiples plataformas a través del proceso GBA (método de generación específico) y se recomienda que los requisitos aplicables se ajusten a la autentificación GBA descrita en la especificación [ETSI TS 129 109].
Clave de cifrado de la información de identificación de los usuarios	Protege la información de identificación de los usuarios
Clave de cifrado de datos de claves	Protege los datos relacionados con las claves
Clave de transferencia segura de datos	Protege datos importantes e información sensible en tránsito

8.2.2 Gestión de certificados

A fin de establecer conexiones HTTPS seguras, es necesario configurar el servidor web con un certificado digital que certifique el tipo de uso del servidor en cuestión. En el caso de los servidores que es preciso configurar con certificados digitales, si existen varios nombres de dominio, debe solicitarse un certificado de servidor para cada nombre de dominio. En el caso de los servidores que utilizan el protocolo Internet (IP) para prestar servicios, si existen múltiples direcciones IP, debe solicitarse un certificado de servidor para cada IP. Estos certificados se ilustran en el Cuadro 3.

Cuadro 3 – Descripción de la configuración del certificado de servidor del sistema de mensajería 5G

Nombre del servidor	Método de acceso	Tipo de certificado
5GMC	Nombre de dominio	Certificado SSL ordinario (requiere que el terminal preconfigure el certificado raíz de la CA).
Plataforma de mensajes	Nombre de dominio	Certificado SSL ordinario (requiere que el terminal preconfigure el certificado raíz de la CA).
Módulo de gestión de la plataforma de mensajes	Nombre de dominio	Certificado SSL ordinario
Chatbot	Nombre de dominio	Certificado SSL ordinario

8.3 Auditoría de seguridad

Los "logs" son registros de comportamientos importantes de los usuarios, usos anómalos de los recursos del sistema y usos de comandos importantes de la plataforma. Estos registros pueden incluir datos tales como la fecha y la hora, el tipo, la identificación del sujeto, la identificación del objeto y los resultados del evento. Entre los contenidos que podrían registrarse en el registro de seguridad del servicio figuran, entre otros, las operaciones de los usuarios, las operaciones de los administradores y los servicios.

a) Registros de las operaciones de los usuarios: registran las operaciones de las cuentas y sus resultados, las operaciones de los servicios y sus resultados, etc. Los registros de las operaciones de los usuarios pueden incluir información sobre los usuarios, las operaciones de los usuarios, los objetos de las operaciones, el tiempo de las operaciones, los resultados de las operaciones, los resultados anómalos, etc.

b) Registros de las operaciones de los administradores: registran las operaciones de las cuentas y sus resultados, las operaciones de los servicios y sus resultados, etc. Los registros de las operaciones de los administradores pueden incluir información sobre los administradores, las operaciones de los administradores, los objetos de las operaciones, el tiempo de las operaciones, los resultados de las operaciones, los resultados anómalos, etc.

c) Registros de servicio: se recomienda que los sistemas puedan almacenar sus registros de servicio. La plataforma podría almacenar todo tipo de registros durante un tiempo determinado para su consulta en línea previa solicitud; para los registros que superen los requisitos de tiempo aplicables al almacenamiento en línea, podría especificarse un tiempo de almacenamiento fuera de línea. Los registros en línea se almacenan en una base de datos o utilizando un método designado por el sistema. La plataforma de servicio gestiona los derechos de acceso a estos registros, que solo pueden ser visualizados, exportados o auditados por un administrador (auditor) designado. En el caso de los registros fuera de línea, cabe la posibilidad de importarlos al sistema o de utilizar herramientas especiales para realizar consultas, auditorías u otras operaciones. Los registros fuera de línea que contengan datos sensibles podrían almacenarse en archivos encriptados una vez exportados.

8.4 Seguridad en la gestión del *software*

8.4.1 Seguridad en la gestión del desarrollo de *software* para la mensajería 5G

Entre los principios de codificación segura del sistema del servicio de mensajería 5G deben figurar los siguientes:

a) Comprobar la eficacia de los datos introducidos por el usuario y filtrar símbolos sensibles.

b) Cifrar los datos sensibles almacenados, por ejemplo, las contraseñas.

c) Transmitir los datos sensibles por HTTPS, por ejemplo, los nombres de usuario y las contraseñas.

d) No acceder directamente a los recursos del sistema, por ejemplo, a los archivos.

e) No utilizar un intérprete de comandos en los códigos asociados a la Web.

f) Utilizar una función de seguridad para programar.

8.4.2 Seguridad en la gestión de las operaciones para el sistema de mensajería 5G

El sistema de mensajería 5G podría supervisar los procesos importantes y la lógica de procesamiento del servicio y emitir una alarma si descubre algún fallo.

9 Requisitos de seguridad para el control del servicio de mensajería 5G

9.1 Restricciones aplicables a la capacidad del servicio

Entre las restricciones aplicables a la capacidad del servicio figuran las relativas al número de personas que pueden participar en un grupo, al control diferenciado de las funciones de los grupos y a los chats de grupo.

a) Restricción del número de personas que pueden participar en un grupo: el grupo que envía operaciones de mensajes 5G ha de establecer un límite aplicable al número máximo de envíos del grupo, a fin de limitar los posibles efectos adversos a un intervalo limitado.

b) Control diferenciado de las funciones de los grupos: las plataformas de servicios podrían soportar el control diferenciado del número de usuarios llamados de un servicio de grupo.

c) Restricciones aplicables a los chats de grupo: las plataformas de servicio podrían admitir la restricción del número de usuarios de los chats de grupo, el número de usuarios puede configurarse en los parámetros del grupo y las plataformas de servicio podrían admitir la restricción de la longitud del nombre del grupo.

9.2 Lista negra de partes llamantes

Para los mensajes de origen móvil (MO) 5G, es necesario añadir una función de control de autentificación ligada a una lista negra de partes llamantes, a fin de prevenir posibles bombardeos de mensajes 5G. Cabe la posibilidad de que el sistema de control establezca un mecanismo de supervisión de los chats de grupo, que analice las acciones de los mensajes maliciosos masivos y los añada a un control de lista negra de partes llamantes mediante adiciones automáticas o revisiones manuales, entre otras opciones. El control de lista negra de partes llamantes podría entonces interceptar y controlar las acciones de dichos mensajes.

9.3 Lista negra de partes llamadas

En el caso de los mensajes de terminación móvil (MT) 5G, es necesario añadir un control de lista negra de partes llamadas, con miras a disminuir las posibles quejas de los usuarios de terminales. Los usuarios personales podrían quejarse o crear una lista negra de partes llamadas llamando al servicio de atención al cliente, accediendo a una interfaz de autoservicio o acudiendo a una oficina comercial, entre otras opciones. Cabe la posibilidad de que el sistema de control u otros sistemas de servicios conexos impongan controles de listas negras para interceptar los mensajes de los usuarios por tipo de usuario o servicio.

Bibliografía

[b-GSMA RCC.71] GSM Association (2019), *RCS Universal Profile Service Definition Document.*

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

Publicado en Suiza
Ginebra, 2024