UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T X.1122

(04/2004)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE X: REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

Seguridad de las telecomunicaciones

Directrices para la implementación de sistemas móviles seguros basados en la infraestructura de claves públicas

Recomendación UIT-T X.1122

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

REDES PÚBLICAS DE DATOS	
Servicios y facilidades	X.1–X.19
Interfaces	X.20–X.49
Transmisión, señalización y conmutación	X.50–X.89
Aspectos de redes	X.90–X.149
Mantenimiento	X.150–X.179
Disposiciones administrativas	X.180–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Modelo y notación	X.200–X.209
Definiciones de los servicios	X.210–X.219
Especificaciones de los protocolos en modo conexión	X.220–X.229
Especificaciones de los protocolos en modo sin conexión	X.230–X.239
Formularios para declaraciones de conformidad de implementación de protocolo	X.240–X.259
Identificación de protocolos	X.260–X.269
Protocolos de seguridad	X.270–X.279
Objetos gestionados de capa	X.280–X.289
Pruebas de conformidad	X.290–X.299
INTERFUNCIONAMIENTO ENTRE REDES	
Generalidades	X.300–X.349
Sistemas de transmisión de datos por satélite	X.350–X.369
Redes basadas en el protocolo Internet	X.370–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	
Gestión de redes	X.600–X.629
Eficacia	X.630–X.639
Calidad de servicio	X.640–X.649
Denominación, direccionamiento y registro	X.650–X.679
Notación de sintaxis abstracta uno	X.680–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Marco y arquitectura de la gestión de sistemas	X.700–X.709
Servicio y protocolo de comunicación de gestión	X.710–X.719
Estructura de la información de gestión	X.720–X.729
Funciones de gestión y funciones de arquitectura de gestión distribuida abierta	X.730–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Compromiso, concurrencia y recuperación	X.850–X.859
Procesamiento de transacciones	X.860–X.879
Operaciones a distancia	X.880–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LAS TELECOMUNICACIONES	**X.1000–**

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

Recomendación UIT-T X.1122

Directrices para la implementación de sistemas móviles seguros basados en la infraestructura de claves públicas

Resumen

Aunque la infraestructura de claves públicas (PKI) es una tecnología de seguridad de gran utilidad que permite realizar un gran número de funciones de seguridad (cifrado, firma digital, integridad de datos, etc.) en las comunicaciones móviles de datos extremo a extremo, es necesario adaptar la tecnología PKI para utilizarla en las comunicaciones móviles de datos extremo a extremo. No obstante, aún no se ha definido un método que permita construir y gestionar sistemas móviles seguros basados en la tecnología PKI. En esta Recomendación se ofrecen directrices para la construcción de sistemas móviles seguros basados en la tecnología PKI.

Orígenes

La Recomendación UIT-T X.1122 fue aprobada el 29 de abril de 2004 por la Comisión de Estudio 17 (2001-2004) del UIT-T por el procedimiento de la Recomendación UIT-T A.8.

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) 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 adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, 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 patente, 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 la base de datos sobre patentes de la TSB.

ÍNDICE

Recomendación UIT-T X.1122

Directrices para la implementación de sistemas móviles seguros basados en la infraestructura de claves públicas

1 Alcance

En esta Recomendación se presentan directrices para la construcción de sistemas móviles seguros basados en la tecnología PKI. La gama de aplicaciones de esta Recomendación será la siguiente:

- Tratará del control de certificados en las comunicaciones móviles de datos extremo a extremo en general.
- No obstante, se excluirá del ámbito de aplicación de esta Recomendación la definición de un método de liquidación móvil como modelo de liquidación.

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.

- Recomendación UIT-T F.116 (2000), *Características del servicio y disposiciones operacionales en las telecomunicaciones móviles internacionales-2000 (IMT-2000)*.
- Recomendación UIT-T Q.814 (2000), *Especificación de un agente interactivo de intercambio electrónico de datos*.
- Recomendación UIT-T Q.1701 (1999), *Marco para las redes de las telecomunicaciones móviles internacionales-2000 (IMT-2000)*.
- Recomendación UIT-T Q.1711 (1999), *Modelo funcional de red para las telecomunicaciones móviles internacionales-2000 (IMT-2000)*.
- Recomendación UIT-T Q.1761 (2004), *Principios y requisitos para la convergencia de los sistemas fijos y los sistemas IMT-2000 existentes*.
- Recomendación UIT-T X.509 (2000) | ISO/CEI 9594-8:2001, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marco para certificados de claves públicas y de atributos*.
- Recomendación UIT-T X.800 (1991), *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT*.
- Recomendación UIT-T X.842 (2000) | ISO/CEI TR 14516:2002, *Tecnología de la información – Técnicas de seguridad: Directrices sobre el uso y gestión de servicios a tercera parte confiable*.
- Recomendación UIT-T X.1121 (2004), *Marco general de tecnologías de seguridad para las comunicaciones móviles de datos de extremo a extremo*.

3 Términos y definiciones

3.1 Definiciones del marco del certificado de clave pública y atributo

Los siguientes términos se definen en la Rec. UIT-T X.509 | ISO/CEI 9594-8:

a) autoridad de atributo;

b) certificado de atributo;

c) autoridad de certificación (CA, *certification authority*);

d) lista de revocación de certificados (CRL, *certificate revocation list*);

e) clave pública;

f) certificado de clave pública (*certificado*);

g) infraestructura de claves públicas (PKI, *public key infrastructure*).

3.2 Definiciones de la arquitectura de seguridad del modelo de referencia OSI

Los siguientes términos se definen en la Rec. UIT-T X.800 | ISO 7498-2:

a) información de autenticación;

b) confidencialidad;

c) criptografía;

d) clave;

e) contraseña.

3.3 Directrices para el uso y la gestión de definiciones de servicios de tercera parte confiable

El siguiente término se define en la Rec. UIT-T X.842 | ISO/CEI TR 14516:

a) autoridad de registro.

3.4 Características del servicio y disposiciones operacionales en las definiciones de las IMT-2000

El siguiente término se define en la Rec. UIT-T F.116:

a) Módulo de identidad de usuario.

3.5 Definiciones adicionales

En esta Recomendación se definen los términos siguientes.

3.5.1 sistema móvil seguro: Sistema que permite realizar las comunicaciones móviles de datos extremo a extremo entre un usuario móvil y un ASP o entre usuarios móviles.

3.5.2 repositorio de certificados: Base de datos en la que se almacenan los certificados, CRL y demás información relacionada con la PKI y a la que se puede acceder en línea.

3.5.3 autoridad de validación: Autoridad que presta el servicio de verificación en línea de la validez de un certificado, estableciendo un trayecto del certificado de verificación entre un firmante y un usuario que desee confirmar la validez de la firma del firmante, y confirma si todos los certificados contenidos en el trayecto del certificado de verificación son fiables y no están revocados. Verifica asimismo si un determinado certificado ha sido revocado.

4 Siglas

En esta Recomendación, se utilizan las siguientes siglas.

AA Autoridad de atributos (*attribute authority*)
ASP Proveedor de servicio de aplicación (*application service provider*)
CA Autoridad de certificación (*certification authority*)
CMC Gestión del certificado sobre CMS (*certificate management over CMS*)
CMP Protocolo de gestión de certificados (*certificate management protocol*)
CRL Lista de revocación de certificados (*certificate revocation list*)
ID Identificador (*identifier*)
PIN Número de identificación personal (*personal identification number*)
PKI Infraestructura de claves públicas (*public-key infrastructure*)
POP Prueba de posesión (*proof of posesión*)
RA Autoridad de registro (*registration authority*)
RSA Algoritmo de clave pública RSA (*RSA public key algorithm*)
TLS Seguridad de la capa de transporte (*transport layer security*)
UIM Módulo de identidad de usuario (*user identity module*)
VA Autoridad de validación (*validation authority*)

5 Categorías en las que se enmarcan las tecnologías PKI

La PKI es una tecnología de seguridad que se aplica a la relación entre los terminales móviles y los servidores de aplicaciones en un modelo general de comunicaciones móviles de datos extremo a extremo entre usuarios móviles y ASP o bien a la relación entre terminales móviles y pasarelas de seguridad móviles y entre pasarelas de seguridad móviles y servidores en un modelo de pasarela de comunicaciones móviles de datos extremo a extremo entre usuarios móviles ASP.

La PKI es una tecnología de seguridad que se utiliza para realizar las siguientes funciones de seguridad:

1) cifrado;
2) intercambio de claves;
3) firma digital;
4) control de acceso;
5) integridad de datos;
6) intercambio de autenticación;
7) notarización.

Cuadro 1/X.1122 – Funciones y aplicación de la tecnología PKI

Aplicación de la tecnología / Funciones realizadas por estas tecnologías	Terminales móviles	Servidor de aplicaciones/ pasarela de seguridad móvil	Relación entre usuarios móviles y terminales móviles	Relación entre terminales móviles y servidores de aplicaciones u otras relaciones
Cifrado				X
Intercambio de claves				X
Firma digital				X
Control de acceso				X
Integridad de datos				X
Intercambio de autenticación				X
Notarización				X

Aunque la tecnología PKI se utiliza con frecuencia en redes abiertas para realizar las funciones de seguridad mencionadas, las características de las comunicaciones móviles de datos extremo a extremo, especialmente cuando la potencia de procesamiento es baja y el tamaño de la memoria pequeño, impone ciertas adaptaciones de las tecnologías PKI para su utilización en las comunicaciones móviles de datos extremo a extremo.

6 Modelos de sistemas móviles seguros basados en PKI

Al igual que en otros sistemas móviles seguros, los modelos de sistemas móviles seguros basados en PKI se clasifican del siguiente modo: modelo general de sistemas móviles seguros basados en PKI para la comunicación entre el usuario móvil y el ASP y modelo de pasarela de sistemas móviles seguros basados en PKI para la comunicación entre el usuario móvil y el ASP.

No obstante, a los efectos de las operaciones PKI (por ejemplo, gestión del ciclo de vida del certificado), se añaden a los modelos ciertas entidades (CA, RA, VA, repositorio, etc.).

6.1 Modelo general de sistemas móviles seguros basados en PKI

En la figura 1 se representa el modelo general de sistemas móviles seguros basados en PKI para la comunicación entre usuarios móviles y ASP.

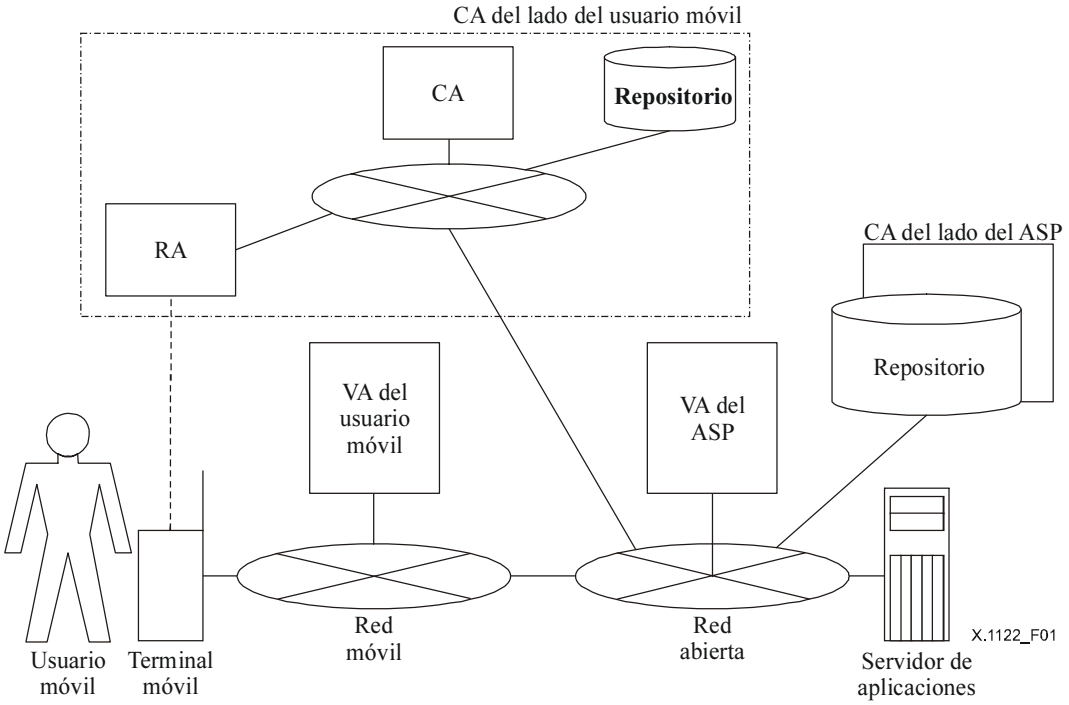

Figura 1/X.1122 – Modelo general de sistemas móviles seguros basados en PKI

En este modelo existen entidades adicionales al modelo general de comunicación móvil de datos extremo a extremo entre usuarios móviles y ASP; a saber: la CA del lado del usuario móvil (contiene la RA y los repositorios), la VA del usuario móvil, la CA del lado del ASP y la VA del ASP.

– *CA del usuario móvil*

  La CA del lado del usuario móvil emite y gestiona el certificado del usuario móvil o el del terminal móvil. Éste contiene la RA responsable de la identificación y autenticación del usuario móvil y del repositorio que guarda el certificado del usuario móvil y la CRL.

– *VA del usuario móvil*

  La VA del usuario móvil presta un servicio de verificación en línea de la validez del certificado recibido por un usuario móvil procedente de otro usuario móvil.

– *CA del lado del ASP*

  La CA del lado del ASP emite y gestiona el certificado del ASP o el certificado del servidor de aplicaciones. Asimismo contiene la RA responsable de la identificación y autenticación del ASP y el repositorio que almacena el certificado del ASP y la CRL.

– *VA del ASP*

  La VA del ASP presta el servicio de verificación en línea de la validez del certificado recibido por el ASP.

6.2 Modelo de pasarela de los sistemas móviles seguros basados en PKI

En la figura 2 se representa el modelo de pasarela de sistemas móviles basados en PKI para la comunicación entre usuarios móviles y ASP.

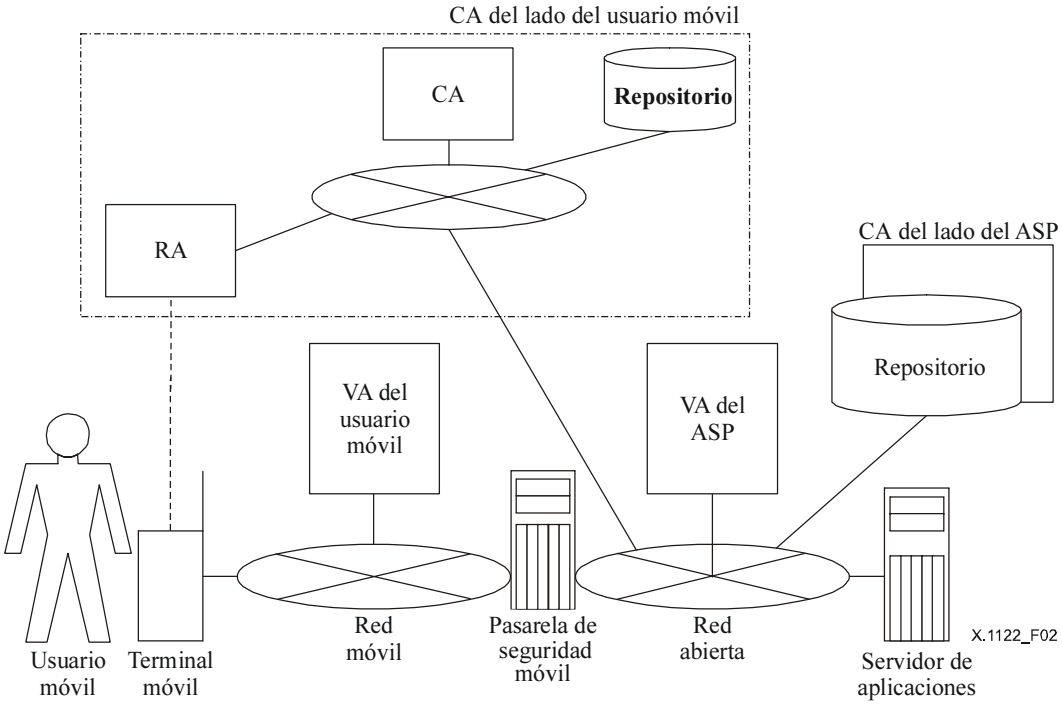

Figura 2/X.1122 – Modelo de pasarela de sistemas móviles seguros basados en PKI

Como en el modelo general de sistemas móviles seguros basados en PKI para la comunicación entre usuarios móviles y ASP, éste contiene entidades adicionales al modelo de pasarela de comunicaciones móviles de datos extremo a extremo entre usuarios móviles y ASP; a saber: la CA del lado del usuario móvil (que contiene la RA y el repositorio), la VA del usuario móvil, la CA del lado del ASP y la VA del ASP.

7 Operaciones PKI para las comunicaciones móviles de datos extremo a extremo

7.1 Operaciones PKI relacionadas con el ciclo de vida del certificado

El ciclo de vida general del certificado es el siguiente:

1) generación de un par de claves privada y pública;
2) aplicación, emisión y activación del certificado;
3) utilización del certificado;
4) revocación del certificado y
5) renovación del certificado.

7.1.1 Generación del par de claves privada y pública

Para la generación de un par de claves privada y pública, existen distintos modelos dependiendo de quién genere la clave o de dónde se genere ésta.

7.1.1.1 Entidad que genera las claves

Aunque el modelo en el que el usuario móvil genera las claves resulta interesante desde el punto de vista de la seguridad, puede existir un modelo en que la CA genere las claves en vez de hacerlo el usuario móvil y otro modelo en el que las claves sean generadas por un tercero.

Entre los modelos en los que un tercero procesa las claves, existe uno en el que el usuario adquiere el dispositivo en el que están instaladas las claves (este dispositivo podría ser el propio terminal

móvil o bien un componente conectado al terminal móvil). En tal caso, el fabricante del dispositivo es el productor de la clave.

7.1.1.2 Lugar de generación de las claves

Puede haber modelos en los que las claves se generen en el dispositivo y modelos en los que las claves se generen fuera del dispositivo pero se instalen en éste.

7.1.2 Solicitud, emisión y activación del certificado

Para la solicitud, emisión y activación del certificado, existen distintos modelos dependiendo de si la aplicación, emisión y activación se efectúa en línea o fuera de línea en cada paso.

Hay casos en los que el certificado se considera activado en el momento de su emisión.

Debe escogerse el modelo en función de la persona a la que se emite el certificado (usuario móvil), emisor (CA), objeto de la garantía del certificado y fines de uso del mismo, etc.

Además, en un entorno móvil, los modelos son diferentes en función de la relación entre los momentos de:

a) generación de las claves;

b) emisión del certificado;

c) activación del certificado y

d) obtención del dispositivo.

7.1.2.1 Modelo en el que el dispositivo se obtiene tras la activación del certificado [modelo en el que el orden de los puntos anteriores es (a)→(b)→(c)→(d)]

Este modelo corresponde al caso en el que el usuario móvil adquiere un dispositivo en el que ya están instalados previamente las claves y el certificado. En este modelo es posible vender un dispositivo que tenga instalado previamente el certificado con un sujeto no vinculado al usuario móvil (por ejemplo, cuando el dispositivo sea un terminal móvil, puede utilizarse como sujeto el número de teléfono o algún otro número de serie del dispositivo electrónico), o en el que se instale el certificado en el momento de adquisición del dispositivo en el comercio (por ejemplo, el certificado se procesa y se instala en base a la información que se facilita en el momento de solicitud del dispositivo). En este caso, es conveniente que (b), (c) y (d) tengan lugar simultáneamente.

7.1.2.2 Modelo en el que un usuario obtiene un dispositivo en el que ya se ha emitido el certificado [modelo en el que el orden es (a)→(b)→(d)→(c)]

Éste es básicamente el mismo que el anterior, pero es necesario un procedimiento de activación del certificado tras la obtención del dispositivo. Conviene que el tiempo transcurrido entre los instantes ((b) y (d) sea lo más breve posible.

7.1.2.3 Modelo en el que el usuario obtiene un dispositivo que sólo almacena las claves [modelo en el que el orden es (a)→(d)→(b)→(c)]

Este modelo corresponde al caso en el que el usuario solicita el certificado en línea tras haber adquirido un dispositivo instalado con las claves.

7.1.2.4 Modelo en el que el usuario obtiene un dispositivo que no lleva instaladas claves ni certificados [modelo en el que el orden es (d)→(a)→(b)→(c)]

En este modelo, el usuario genera las claves y solicita un certificado tras haber adquirido el dispositivo. Se trata de un modelo que respeta el carácter privado de las claves del terminal móvil. No obstante, se requiere más capacidad de computación, almacenamiento de memoria y tiempo de procesamiento para generar las claves en el dispositivo.

7.1.3 Utilización del certificado

7.1.3.1 Firmante

El firmante asocia su certificado al mensaje firmado y lo envía al verificador. Existen distintos modelos en función del método de asociación (tal como adjuntar el certificado al mensaje o adjuntar el lugar del repositorio).

7.1.3.2 Verificador

En la verificación de la autenticidad del mensaje recibido del firmante, es necesario que se ejecuten los siguientes procesos:

1) *Verificación de la validez del certificado*

   Se trata de verificar la autenticidad del certificado del firmante. Concretamente, se pretende descubrir un trayecto de autenticación del certificado y verificar la validez de cada certificado en el trayecto de autenticación.

   Dependiendo del método de verificación, se puede utilizar uno de los dos modelos siguientes:

   a) *Modelo en el que el verificador efectúa por sí mismo la verificación*

      En el momento de verificación, el verificador descubre un trayecto de autenticación y verifica la validez de cada certificado en el trayecto de autenticación.

      Para la verificación de cada certificado, el verificador verifica la validez del certificado por adquisición de la CRL del repositorio de la CA, o interrogando a la CA, que a su vez proporciona la información de estado de los certificados en línea, o por cualquier otro medio.

      Obsérvese que la frecuencia de las adquisiciones de la CRL o de las interrogaciones a la CA depende de la utilización e importancia del certificado (en principio, es necesaria cada vez que se verifica el certificado).

   b) *Modelo en el que se utiliza una autoridad de verificación (VA) fiable*

      Se formula a la VA una interrogación sobre la validez del certificado asociado al mensaje, de modo que el proceso real de verificación (descubrimiento del trayecto de autenticación y verificación de la validez de cada certificado) lo realiza la VA.

      Este proceso podría omitirse con un certificado de corta duración o por algún otro medio.

2) *Verificación de la firma adjunta al mensaje*

   Se trata de verificar si la firma adjunta al mensaje es auténtica.

   Suele ocurrir que el propio verificador verifica la firma utilizado la clave pública de certificado, pero puede haber modelos en los que sea la VA quien ejecute esta función.

7.1.4 Revocación del certificado

Se trata de solicitar a la CA la revocación del certificado y de que ésta lo revoque. En función del método de solicitud, hay dos modelos de revocación del certificado, a saber: un modelo en el que la solicitud de revocación se efectúa en línea y otro en el que la solicitud de revocación se efectúa fuera de línea.

7.1.5 Renovación del certificado

Se trata de revocar un certificado existente, de generar un nuevo par de claves y de recibir un nuevo certificado emitido por la CA. Básicamente la solicitud de revocación y la emisión del certificado se efectúan consecutivamente, pero hay distintos modelos en función del orden de los procesos y de si el certificado existente (o la información del mismo) se utiliza en la solicitud del nuevo certificado.

8 Modelo de utilización en los servicios de telecomunicaciones

Esta cláusula presenta el modelo de utilización que estará disponible cuando se utilice la PKI.

Hay dos tipos de modelo de utilización: un modelo de utilización de capa de sesión y un modelo de utilización de capa de aplicación. El modelo de utilización de capa de sesión proporciona las funciones de comunicaciones criptadas, autenticación e integridad de datos en la capa de sesión en el modelo de referencia OSI (tal como la TLS). Mientras que el modelo de utilización de capa de aplicación proporciona las funciones de integridad y confidencialidad en la capa de aplicación.

Muchas de las implementaciones del modelo de utilización de capa de sesión existentes (de las que una de las más conocidas es la TLS) se han diseñado para proporcionar transporte seguro extremo a extremo así como un túnel seguro entre servidor y cliente. Por consiguiente, el cliente y el servidor pueden otorgarse recíprocamente autorización, y las autenticaciones pueden llevarse a acabo mediante PKI.

El modelo de utilización de capa de sesión se basa en las siguientes funciones de seguridad:

- autenticación de servidor;
- autenticación de cliente;
- criptación e integridad del trayecto de comunicación.

El modelo de utilización de capa de aplicación se basa en las siguientes funciones de seguridad:

- la función de firma digital a nivel de aplicación (para integridad y autenticación);
- la función de criptación de datos a nivel de aplicación (para confidencialidad).

Además de los mencionados, puede utilizarse un modelo de utilización de capa de red.

8.1 Funciones a realizar en el modelo de utilización de capa de sesión

El modelo de utilización de capa de sesión proporciona las funciones siguientes: función de autenticación del servidor, función d autenticación del cliente y función de integridad y criptación del trayecto de comunicación, (lo que realmente se llevará a cabo será una combinación de la función de autenticación del servidor y de la función de integridad de criptación del trayecto de comunicación o una combinación de la función de autenticación del servidor, de la función de autenticación del cliente y de la función de integridad y criptación del trayecto de comunicación). Las implementaciones de este modelo de utilización (tales como la TLS) pueden utilizarse en la comunicación móvil de datos extremo a extremo para proporcionar la autenticación de un terminal móvil y de un servidor de aplicaciones y para establecer un túnel seguro entre dos puntos extremos. El certificado desempeña funciones de la mayor importancia para este modelo de utilización. Por consiguiente, es realmente importante especificar el procedimiento de emisión, revocación y suspensión del certificado y el método de autenticación para el usuario y el servidor.

8.1.1 Autenticación del servidor en el modelo de utilización de capa de sesión

La existencia de dos modelos de sistemas móviles seguros basados en PKI, mencionados en la cláusula 6, implica dos tipos de autenticación del servidor en este modelo de utilización; el primero es la autenticación del servidor en el modelo general y el segundo la autenticación del servidor en el modelo de pasarela.

En la autenticación del servidor en el modelo general, el terminal móvil verifica el servidor de aplicaciones por verificación del certificado presentado por el servidor de aplicaciones y la firma digital sobre el mensaje recibido durante el procedimiento de toma de contacto.

La autenticación del servidor en el modelo general se ejecuta de acuerdo con los siguientes procedimientos:

- El servidor de aplicaciones envía el certificado y la información de autenticación pertinente al terminal móvil.
- El terminal móvil verifica si el certificado ha sido emitido por la CA en la que confía el terminal móvil.
- El terminal móvil verifica la validez de la información de autenticación recibida mediante la clave pública del certificado del servidor de aplicaciones.
- Al mismo tiempo, el terminal móvil determina si el servidor de aplicaciones al que el terminal móvil desea acceder es en última instancia correcto.

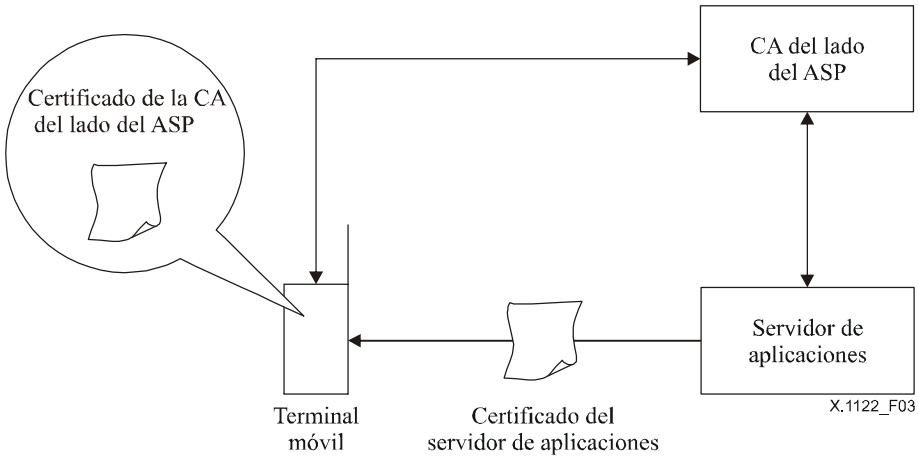

Figura 3/X.1122 – Autenticación del servidor en el modelo general

La autenticación del servidor en el modelo de pasarela es de doble fase: entre el terminal móvil y la pasarela de seguridad móvil y entre la pasarela de seguridad móvil y el servidor de aplicaciones.

La autenticación del servidor de doble fase se ejecuta con arreglo al siguiente procedimiento:

- En primer lugar se establece una sesión protegida entre el terminal móvil y la pasarela de seguridad móvil utilizando el certificado de la pasarela de seguridad móvil.
- A continuación se establece además una sesión protegida entre la pasarela de seguridad móvil y el servidor de aplicaciones.

Así pues, en la autenticación del servidor de doble fase, la pasarela de seguridad móvil debe poder convertir adecuadamente la sesión protegida entre el terminal móvil y la pasarela de seguridad móvil en la sesión protegida entre la pasarela de seguridad móvil y el servidor de aplicaciones.

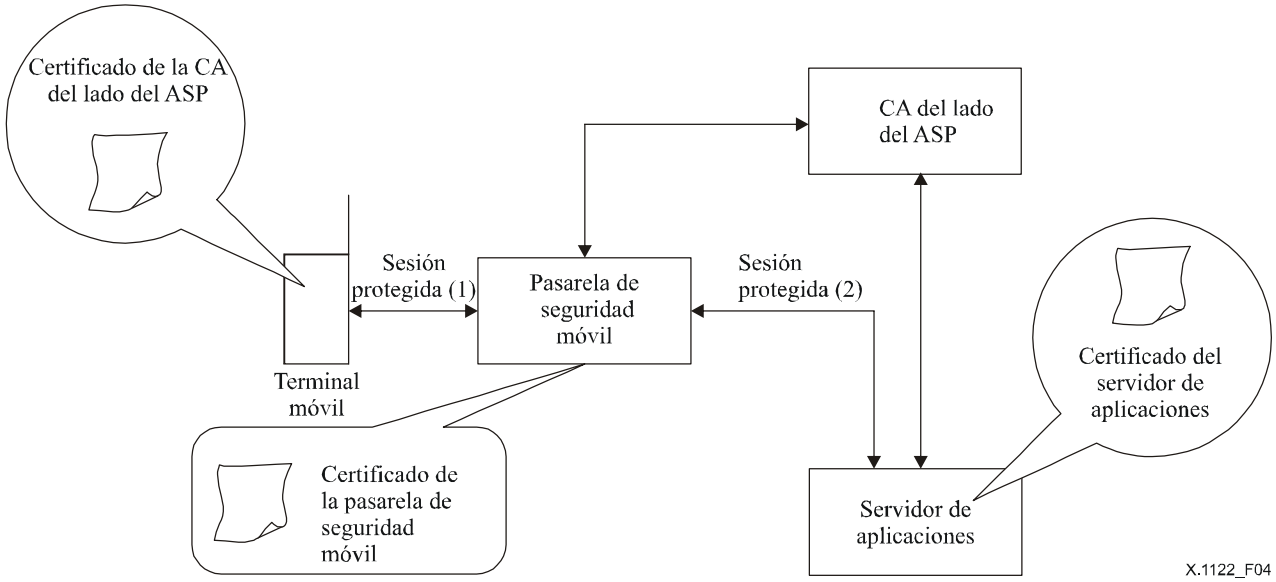

Figura 4/X.1122 – Autenticación del servidor en el modelo de pasarela

8.1.2 Autenticación del cliente en el modelo de utilización de capa de sesión

En la autenticación del modelo de utilización de capa de sesión, el terminal móvil presenta el certificado y la información de autenticación pertinente al servidor de aplicaciones en respuesta a la solicitud de éste, y éste ejecuta la autenticación del cliente.

La autenticación del cliente en este modelo de utilización se ejecuta con arreglo al siguiente procedimiento:

- El terminal móvil envía el certificado al servidor de aplicaciones.
- Al mismo tiempo, el terminal móvil envía el mensaje de verificación firmado (creado con la clave pública del cliente) al servidor de aplicaciones.
- El servidor de aplicaciones verifica el certificado del terminal móvil.
- Además, el servidor de aplicaciones descripta y verifica el mensaje de verificación del certificado con la clave pública del certificado.

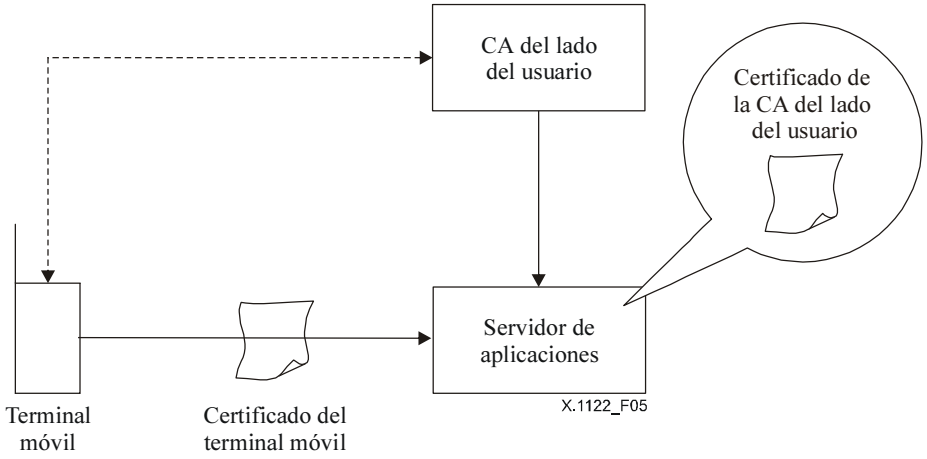

Figura 5/X.1122 – Autenticación del cliente en el modelo de utilización de capa de sesión

Debido a las características de las comunicaciones móviles de datos extremo a extremo, hay implementaciones que modifican el procedimiento de la manera siguiente:

- El terminal móvil envía a la CA del lado del usuario (o a su agente) una petición de certificado.
- La CA autentica el terminal móvil.
- La CA genera el certificado del terminal móvil y envía la información de posición del certificado (por ejemplo la URL) al terminal móvil.
- La CA almacena el certificado del terminal móvil en la zona de almacenamiento.
- Posteriormente, el terminal móvil firma el dato que hay que firmar y envía al servidor de aplicaciones el dato firmado, la firma y la información de posición del certificado.
- El servidor de aplicaciones adquiere del repositorio el certificado del terminal móvil utilizando la información de posición del certificado.
- El servidor de aplicaciones verifica la validez del certificado del terminal móvil (de ser necesario), verifica la firma con su clave pública en el certificado del terminal móvil y autentica el terminal móvil mediante el certificado del terminal móvil.
- Se establece una sesión protegida entre el terminal móvil y el servidor de aplicaciones.

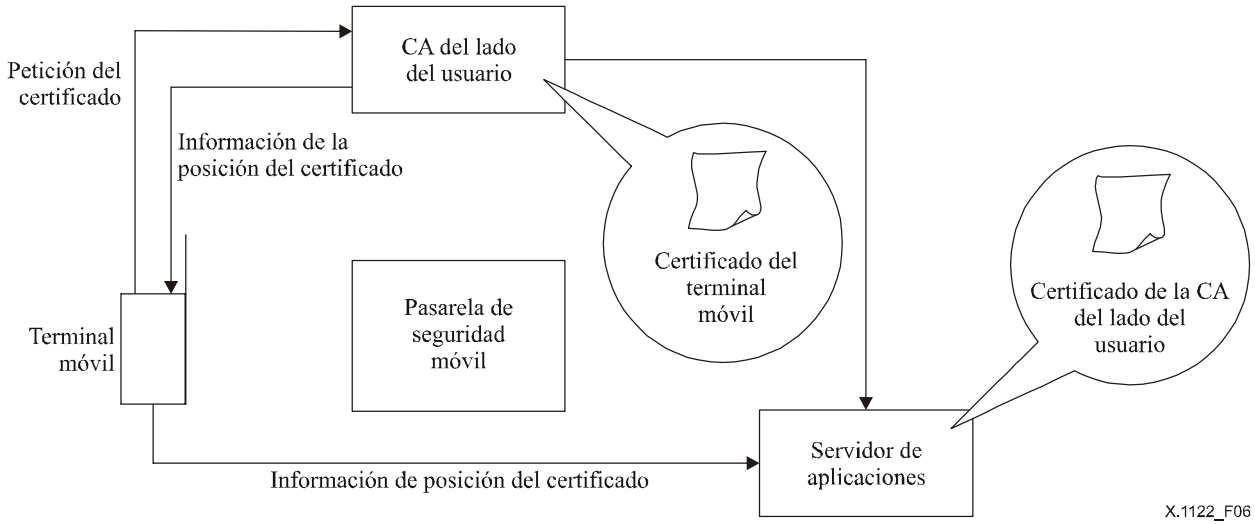

Figura 6/X.1122 – Autenticación del cliente en el modelo de utilización de capa de sesión

8.1.3 Integridad y criptación del trayecto de la comunicación en el modelo de utilización de capa de sesión

La integración y criptación del trayecto de la comunicación en el modelo de utilización de capa de sesión se ejecuta con arreglo al siguiente procedimiento:

- El terminal móvil transmite la serie de algoritmos criptográficos utilizables y un orden de prioridad al servidor de aplicaciones.
- El servidor de aplicaciones selecciona un algoritmo criptográfico específico de la categoría superior dentro de los algoritmos criptográficos de clave común que pueden utilizar ambas partes.
- Se ejecuta la autenticación del servidor para evitar el fraude al servidor de aplicaciones.

- El terminal móvil genera el número aleatorio como generador de una clave de sesión y lo cripta con la clave pública del servidor de aplicaciones en el certificado del servidor de aplicaciones, en el caso del método de intercambio de clave RSA, y envía al servidor de aplicaciones el generador criptado de la clave de la sesión. Tanto el servidor de aplicaciones como el terminal móvil pueden generar a partir del generador una clave de sesión común para las comunicaciones posteriores.
- Se inician las comunicaciones criptadas.

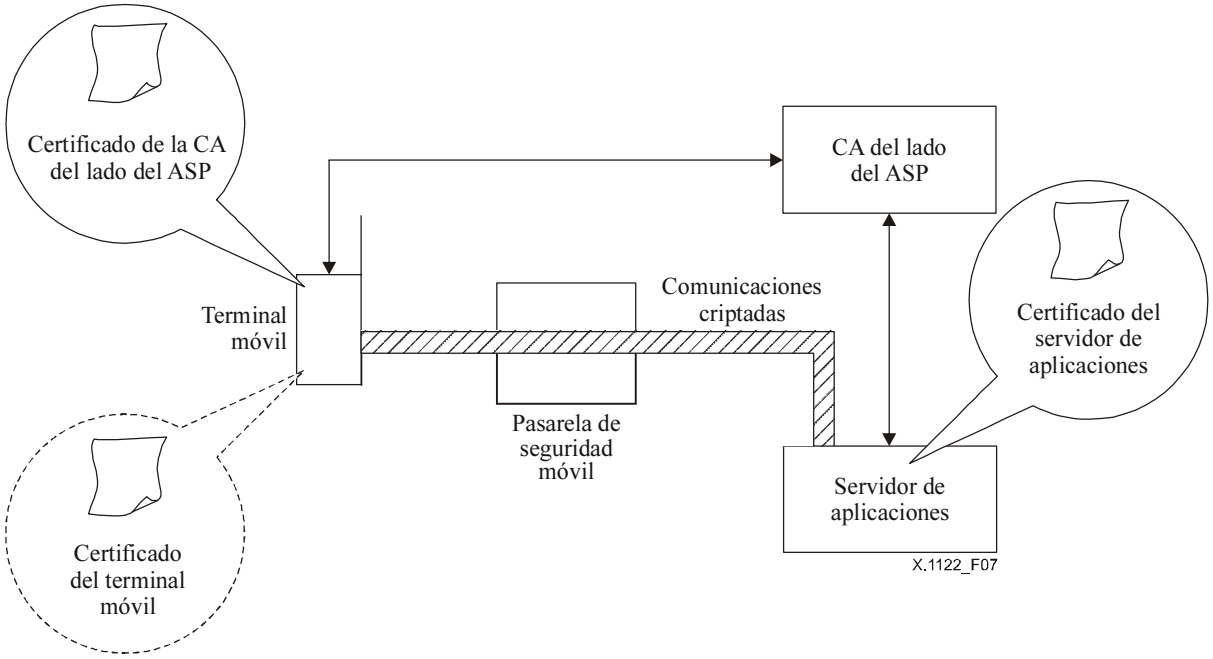

Figura 7/X.1122 – Criptación del trayecto de comunicaciones del modelo de utilización de capa de sesión

8.2 Modelo de utilización en el nivel de aplicación

La PKI puede utilizarse para una función de criptación específica de la aplicación, una función de firma digital, o una comunicación de ambas, que necesite la identificación y confidencialidad en el propio dato y que no pueda cubrirse únicamente por la seguridad en el trayecto de la comunicación tal como autenticación y criptación sobre la capa de sesión. Como ejemplos de implementación de este modelo cabe citar los correos criptados y las aplicaciones de liquidación de cuentas para comercio electrónico.

8.2.1 Función de firma a nivel de aplicación

Esta función garantiza la integridad del dato y crea una firma digital sobre el valor troceado del dato transmitido desde el terminal móvil a fin de garantizar que el origen del dato radica en la persona firmante. La función de firma a nivel de aplicación se realiza mediante las siguientes operaciones:

- Introducir o seleccionar el dato a firmar.
- Procesar una firma digital sobre el valor troceado del dato utilizando la clave privada almacenada en el terminal móvil o dispositivo seguro conectado al terminal móvil.
- Presentar el dato a firmar, la firma digital y el certificado incluida la clave pública correspondiente a la clave privada.
- El destinatario verifica la validez del certificado y la firma digital mediante la clave pública del certificado.

Esta función puede utilizarse para una autenticación del tipo pregunta-respuesta mediante la utilización de una pregunta del servidor (tal como un número aleatorio) correspondiente al dato a firmar.

8.2.2 Función de criptación a nivel de la aplicación

Esta función se utiliza a nivel de la aplicación para asegurar la confidencialidad del dato cuando la criptación en el trayecto de la comunicación no sea suficiente. La función de criptación a nivel de la aplicación se realiza mediante las siguientes operaciones:

- Generar un número aleatorio como clave común.
- Criptar el dato con la clave común utilizando un algoritmo criptográfico simétrico.
- Adquirir el certificado de la persona destinataria de la transmisión.
- Criptar la clave común con la clave pública del certificado.
- Enviar el dato criptado y la clave común criptada.
- Descriptar, el destinatario, la clave común criptada con su propia clave privada.
- Descriptar el dato criptado con la clave común.

9 Ejemplos de configuración del sistema

9.1 Ejemplos de configuración del sistema de gestión de certificados

La figura 8 representa un ejemplo de sistema en el que el operador de comunicaciones emite un certificado para su usuario. La emisión/revocación del certificado se procesa fuera de línea, y se utiliza la VA para verificar el certificado.

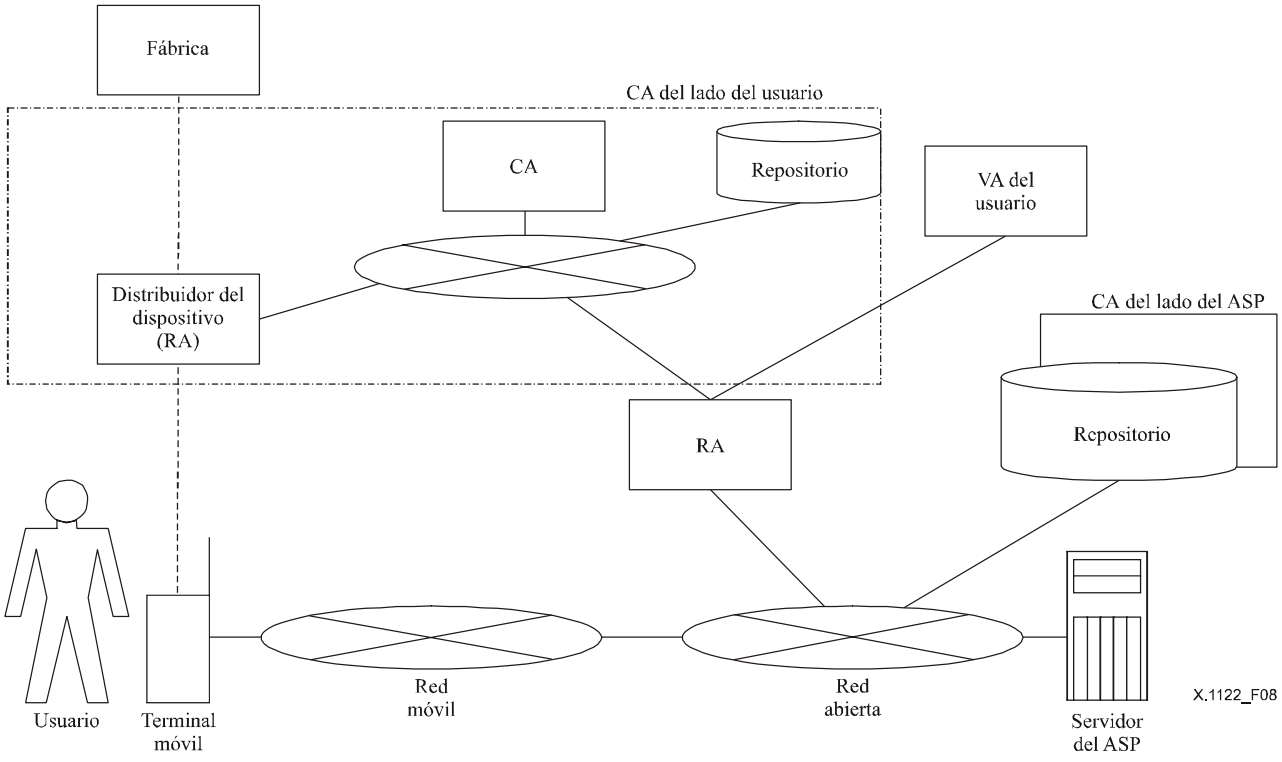

Figura 8/X.1122 – Ejemplo de sistema en el que el operador de comunicaciones emite un certificado para su usuario

9.1.1 Ejemplo de emisión del certificado

Hay dos ejemplos de emisión del certificado en función de la posición en la que se genera la clave: el primero es un método en el que la clave se genera en una fábrica, el segundo es un método en el que la clave se genera en el terminal móvil de un testigo no manipulado como el UIM tras la adquisición del terminal móvil, y deseando el cliente emitir el certificado.

Es muy importante para la solicitud del certificado demostrar la posesión de la clave privada. El protocolo prueba de posesión (POP, *proof of possession*) permite que la CA/RA compruebe la validez del vínculo entre la entidad de extremo y el par de claves. Es necesario que las CA/RA apliquen el certificado correspondiente. La POP específica puede conseguirse de diversas maneras dependiendo del tipo de clave para la que se solicita el certificado.

La figura 9 representa un ejemplo de sistema en el que el operador de comunicaciones emite un certificado para su usuario. El dispositivo viene de fábrica con la clave instalada. El certificado se solicita cuando el usuario adquiere del distribuidor el dispositivo, y lo instala el distribuidor. Este es el momento en el que se realiza la POP.

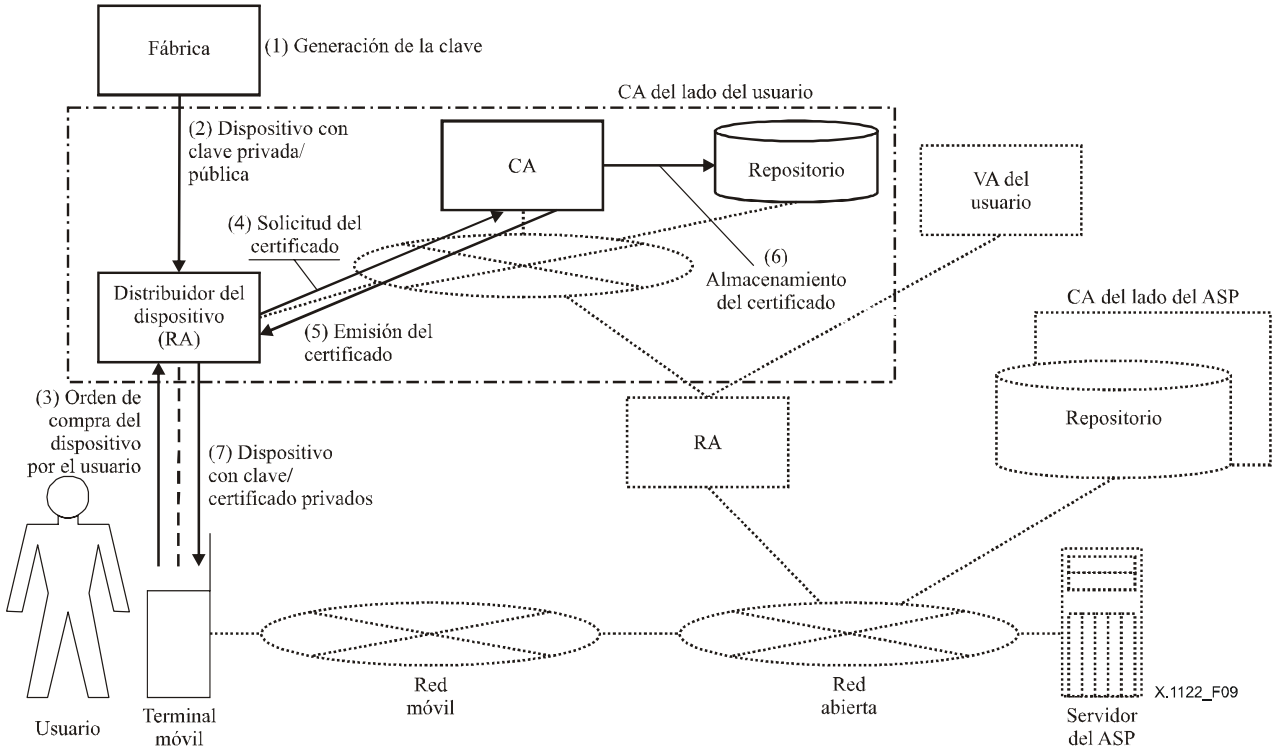

Figura 9/X.1122 – Ejemplo de emisión de certificado (1)

La figura 10 muestra un ejemplo de sistema en el que el cliente genera la clave y emite una solicitud del propio certificado. El certificado se solicita cuando el usuario desea recibirlo de la CA y la clave privada puede mantenerse secreta en el terminal móvil. Antes de la ejecución del protocolo anteriormente descrito, se supone que tanto el terminal móvil como la CA comparten el secreto común para preservar la integridad y autenticidad del mensaje intercambiado. Este método puede proteger el carácter privado de la clave del terminal móvil.

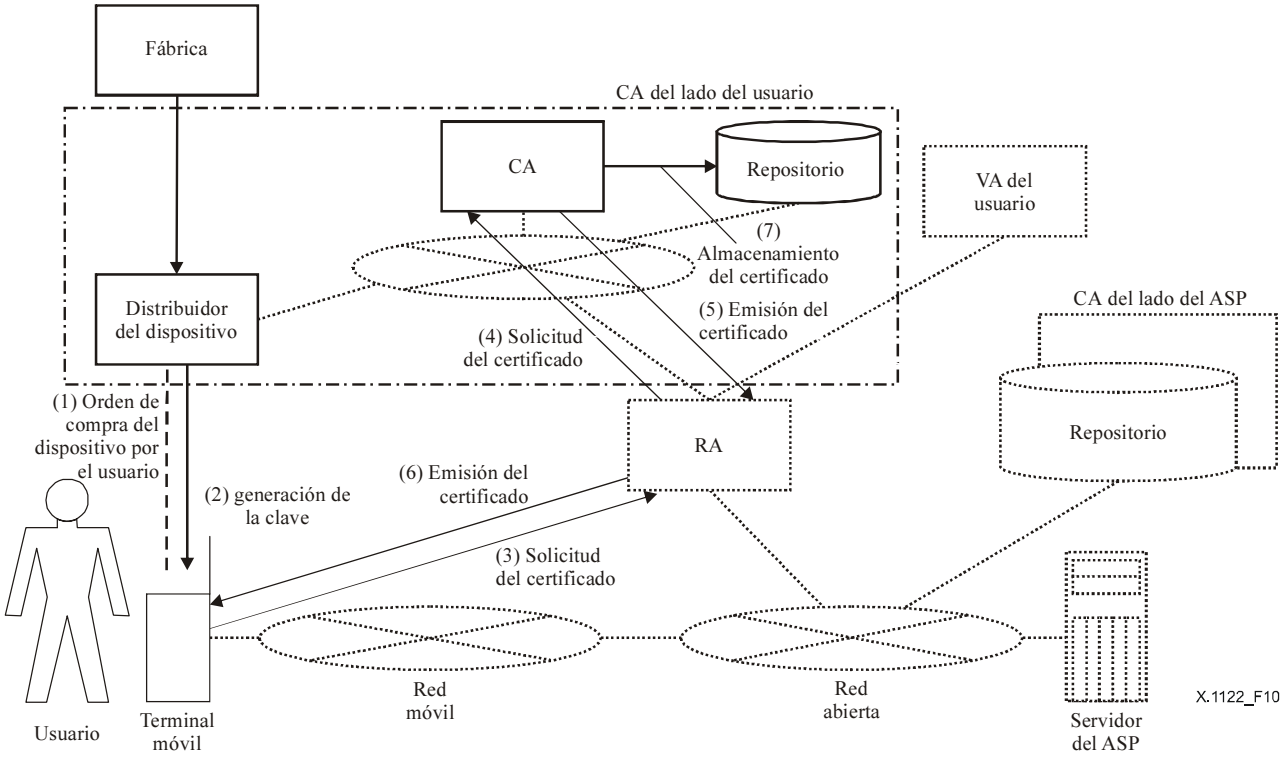

Figura 10/X.1122 – Ejemplo de emisión del certificado (2)

9.1.2 Ejemplo de verificación del certificado

En general, el terminal móvil tiene una potencia de computación limitada y un tamaño de memoria limitado. Por consiguiente, el sistema de verificación del certificado en el terminal móvil basado en CRL presenta bastantes dificultades. El sistema de verificación de certificados en línea en el terminal móvil utilizando la VA resulta mucho más interesante. La figura 11 representa un ejemplo de verificación de certificados en línea.

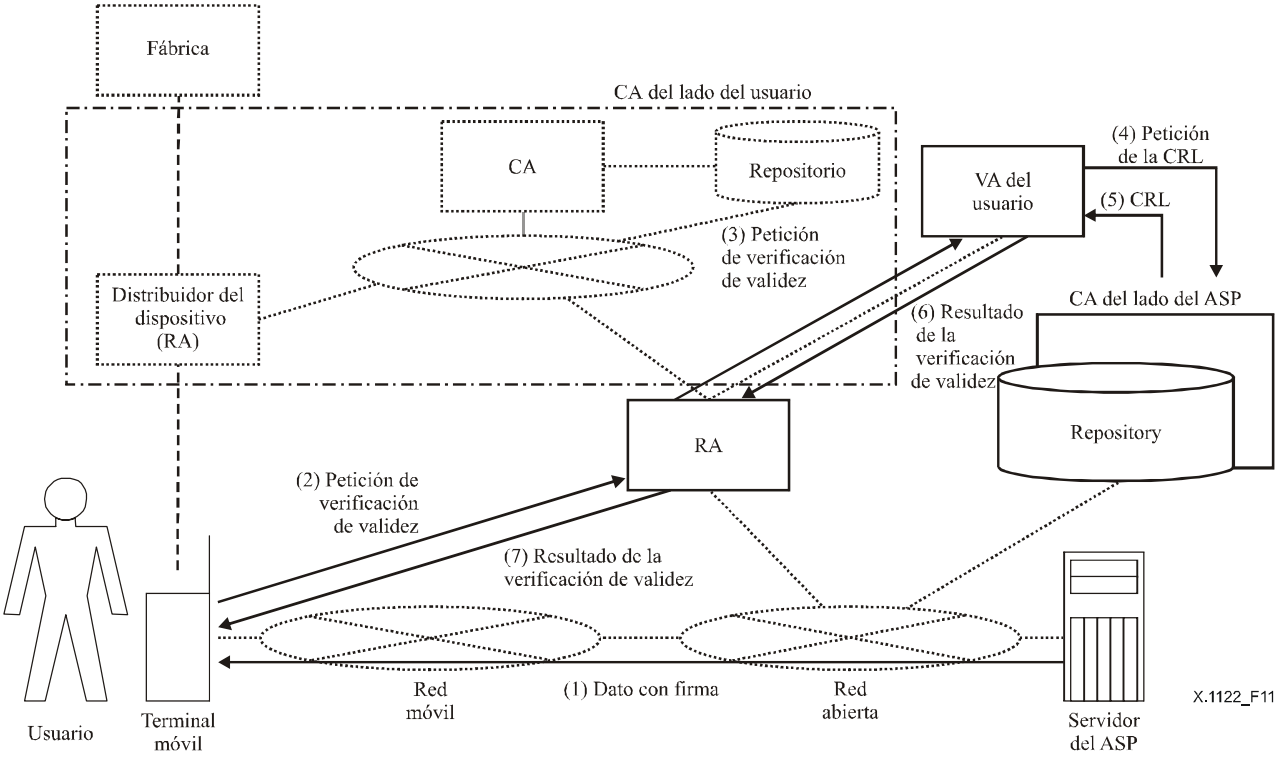

Figura 11/X.1122 – Ejemplo de verificación de certificado

Para verificar el dato recibido procedente de un ASP, el usuario pregunta a la VA si el certificado del ASP es válido a través de la RA. La VA verifica la validez del certificado adquiriendo la CRL a la CA del lado del ASP. El resultado de la verificación se devuelve al usuario a través de la RA. Es indispensable que el usuario móvil pueda verificar el resultado de la verificación (véase 10.2.3.2).

9.1.3 Ejemplo de revocación de certificado

Para revocar un certificado, el usuario visita además al distribuidor a fin de someterse al procedimiento de revocación. No obstante, en una situación de emergencia, se facilitará el servicio de suspensión de la validez del certificado en la red. Para suspender la validez, se presentará la solicitud a la CA a través de la RA. La revocación podría completarse presentando la solicitud firmada a la CA a través de la RA. En caso de robo o pérdida del terminal móvil, es necesario contar con alternativas a la suspensión de la validez. Por ejemplo, el usuario puede efectuar la suspensión llamando al distribuidor del dispositivo para solicitar la suspensión. La figura 12 muestra un ejemplo de revocación de certificado.

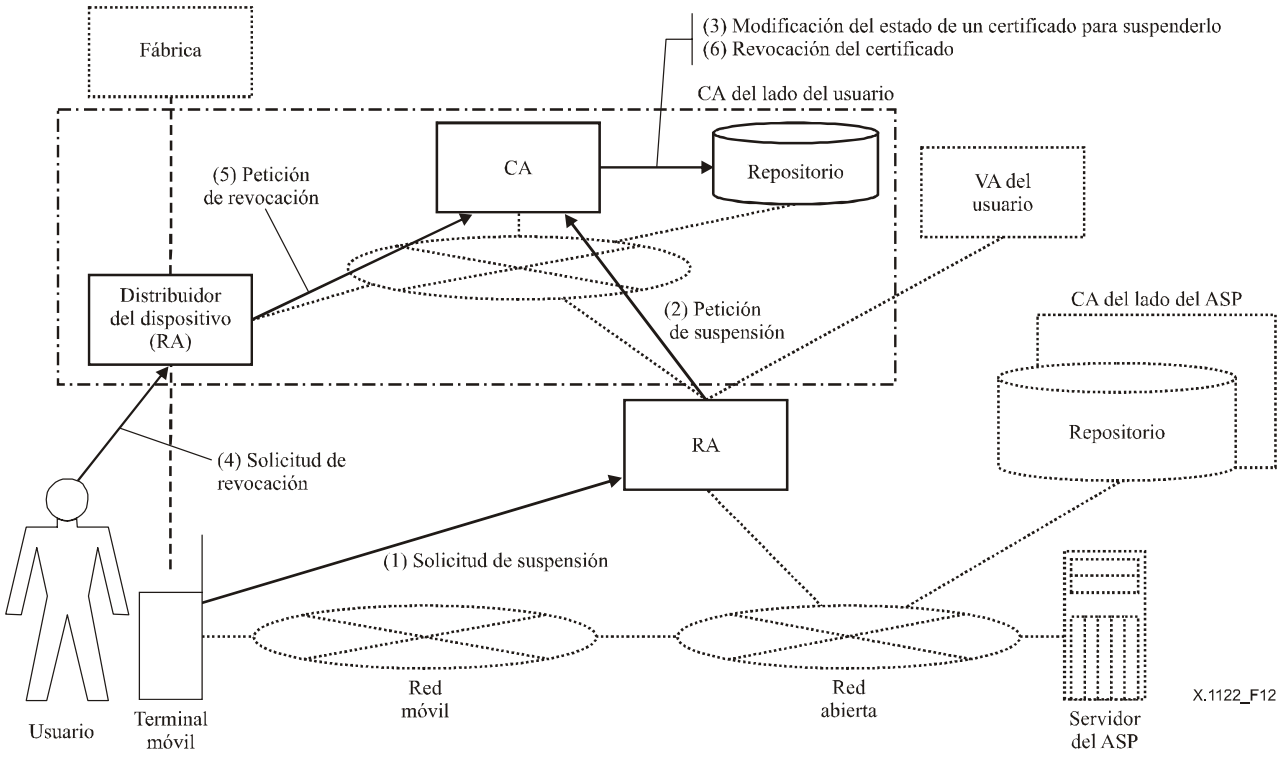

Figura 12//X.1122 – Ejemplo de revocación de certificado

9.2 Ejemplo de modelo de autenticación basado en certificado

A continuación se presenta un ejemplo de modelo de autenticación cuando se utiliza un certificado.

9.2.1 Ejemplo de modelo de autenticación entre un usuario, un operador y un ASP

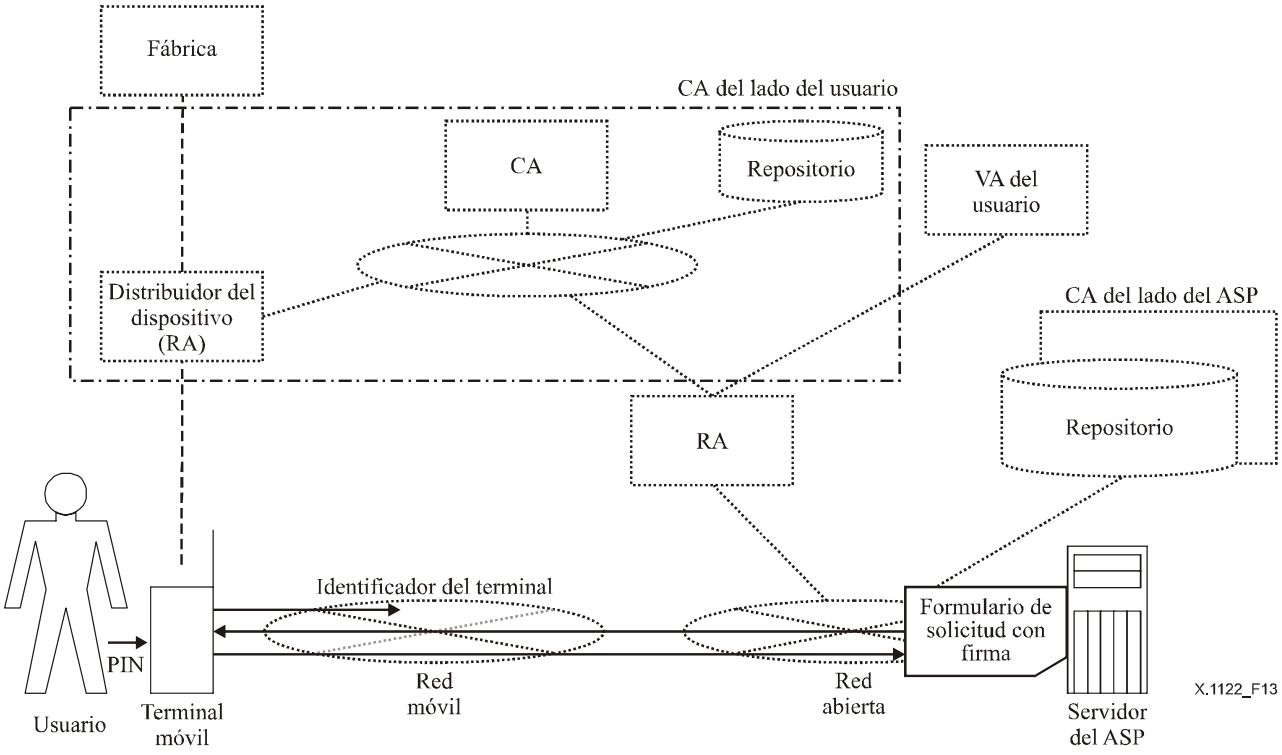

Figura 13/X.1122 – Ejemplo de modelo de autenticación entre un usuario, un operador y un ASP

9.2.1.1 Autenticación del usuario del terminal móvil por el operador de comunicaciones

El terminal móvil se identifica como abonado legítimo presentando el identificador del terminal móvil al operador de comunicaciones.

9.2.1.2 Autenticación del ASP por el usuario del terminal móvil

Para comprobar si se trata de un ASP fiable, se verifica el certificado del ASP. A tal efecto, el usuario puede recibir el certificado del propio ASP y el dato de autenticación pertinente, tal como la firma digital, el código de autenticación del mensaje, y el dato criptado, utilizando la clave privada del ASP a fin de verificarla en el terminal móvil del usuario. El usuario puede asimismo solicitar a la VA que verifique el certificado recibido a través de la RA. El usuario puede especificar asimismo la URL del certificado en vez del propio certificado. Para la autenticación del ASP, el usuario verifica el dato de autenticación pertinente utilizando la clave pública correspondiente a la clave pública del certificado.

9.2.1.3 Autenticación del usuario móvil por el terminal móvil (derecho del usuario de la tarjeta)

Para evitar la utilización ilegítima del terminal móvil por un tercero, cuando se utiliza la información de un chip tal como una tarjeta inteligente integrada en el terminal móvil (como el UIM), debe ejecutarse la autenticación mediante un número PIN. También podría utilizarse otro sistema de autenticación tal como el de las huellas dactilares.

Además debe facilitarse un mecanismo de bloqueo para desactivar la utilización de la tarjeta inteligente en caso de pérdida o robo del dispositivo.

9.2.1.4 Autenticación del terminal móvil (o del usuario móvil) por el ASP

El usuario se certifica en el lado del ASP. Al igual que la autenticación del ASP por parte del terminal móvil, el ASP puede recibir el certificado del terminal móvil (o el certificado del usuario móvil) y el dato de autenticación pertinente, tal como la firma digital, el código de autenticación del mensaje y el dato criptado, utilizando la clave privada del usuario a fin de verificarla en el ASP. El ASP puede asimismo solicitar a la VA que verifique el certificado recibido. El ASP puede especificar además la información de posición del certificado en vez del propio certificado. Para su autenticación, el ASP verifica el dato de autenticación pertinente utilizando la clave pública correspondiente a la clave pública del certificado.

9.2.1.5 Legitimidad de la solicitud

Para verificar si la solicitud se ha originado realmente en el terminal móvil autenticado en 9.2.1.4, el ASP verifica la firma digital adjunta a la solicitud. Es posible utilizar la función de firma a nivel de aplicación. Además, el formulario de solicitud puede criptarse a los efectos de protección contra la divulgación.

9.2.2 Ejemplo de modelo de autenticación utilizado por una institución financiera

Resulta asimismo posible definir un modelo de autenticación que utilice la información de una tarjeta de crédito o de otras infraestructuras existentes, véase la figura 14.

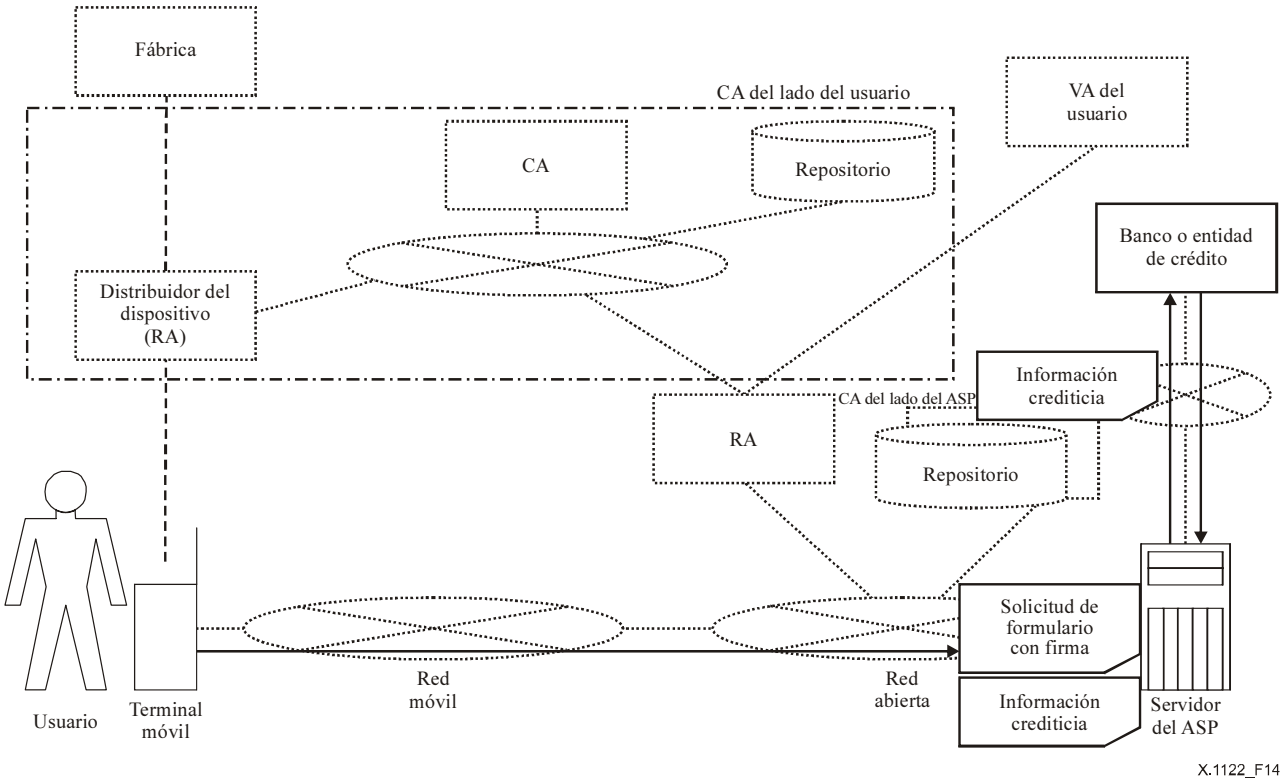

Figura 14/X.1122 – Ejemplo de modelo de autenticación que utiliza una institución financiera

9.2.2.1 Autenticación del usuario por banco o empresa de tarjetas de crédito

Los bancos o empresas de tarjetas de crédito adquieren información financiera (número de cuenta, número de la tarjeta de crédito, etc.) del usuario para autenticar a éste como legítimo propietario de la tarjeta.

En el lado del usuario, se utilizan el número de la tarjeta de crédito y su fecha de validez almacenados en el chip (UIM) de la tarjeta inteligente de modo que ya no sea necesario introducirlos en cada autenticación. Será necesaria la autenticación del usuario, tal como el PIN, cuando se utilice esta información en el terminal móvil a fin de identificar al usuario legítimo con derecho de acceso a la misma.

Esta información financiera puede implementarse asimismo como certificado de atributo.

Cuando se transmita la información de la entidad financiera, deberá criptarse con una clave de sesión aleatoria que esté criptada por la clave pública de la entidad financiera en cuestión pero no por la clave pública del ASP.

La entidad financiera devolverá al ASP el resultado de la autenticación.

9.2.2.2 Autenticación del ASP por parte del banco o empresa de tarjetas de crédito

Cuando se utilice una red abierta en vez de una red de pago existente, el ASP deberá autenticarse como distribuidor afiliado autorizado, presentando un certificado y la información de autenticación pertinente que indique su condición de distribuidor afiliado autorizado, emitida por un banco o empresa de tarjetas de crédito.

9.2.2.3 Autenticación del ASP por el usuario

El ASP debe autenticarse como distribuidor afiliado autorizado por presentación al usuario de un certificado y de la información de autenticación pertinente que indique que se trata de un distribuidor afiliado autorizado, emitida por un banco o empresa de tarjetas de crédito. Por ejemplo,

puede utilizarse un certificado de atributo emitido por el banco para certificar al distribuidor autorizado.

10 Consideraciones sobre la utilización de la PKI para la comunicación móvil de datos extremo a extremo

10.1 Consideraciones sobre el interfuncionamiento con los sistemas existentes

Cuando se adapte un sistema existente basado en PKI que ya esté desarrollado con la red abierta, a un entorno móvil, los certificados para el ASP u otros usuarios de la red abierta se habrán emitido y habrán sido utilizados en el ASP (y tras éste).

En estos casos, el terminal móvil debe ser capaz de verificar la validez de los certificados existentes.

Por otra parte, si el formato del certificado utilizado en un entorno móvil es diferente del formato del certificado del ASP debido a restricciones de la capacidad del caudal o de la capacidad de la memoria, hay que modificar el sistema ASP existente para que el ASP pueda verificar la validez de los certificados para los terminales móviles.

Además, si el terminal móvil no dispone de espacio suficiente para almacenar su certificado, el terminal móvil puede mantener la URL del certificado en vez del propio certificado, y enviar al ASP la URL del certificado. El ASP necesitará recuperar el certificado a partir de su URL

Actualmente, se utiliza con carácter general SSL/TLS como protocolos de protección de mensaje (y protocolos de autenticación) para la comunicación de datos de extremo a extremo.

No obstante, el algoritmo criptográfico y/o formato de certificado que puede utilizarse para TLS tal vez no resulte adecuado para la calidad de funcionamiento de procesamiento del terminal móvil.

Por ejemplo, en muchos de los sistemas existentes que utilizan PKI, se utiliza también el algoritmo criptográfico RSA como algoritmo de firma. No obstante, el algoritmo criptográfico RSA puede necesitar más potencia de procesamiento que la disponible en el terminal móvil. Es preferible la utilización en el entorno móvil de un algoritmo criptográfico de baja potencia que necesite menos memoria. Una de las alternativas al RSA es el algoritmo de curva elíptica. El algoritmo criptográfico de curva elíptica es más rápido que el RSA, y el terminal móvil puede procesarlo en un tiempo que resulta práctico. El algoritmo criptográfico de curva elíptica, no obstante, no ha sido adoptado aún en las especificaciones TLS, etc. Además, cuando se utiliza la criptografía de curva elíptica, la longitud del bit de troceo puede sobrepasar la longitud de la clave, por lo que puede ser necesario procesar la criptografía en varias veces.

Aunque el planteamiento para resolver lo anterior consiste en presentar a la VA la función destinada a verificar la firma, hay que tener en cuenta otra consideración sobre cómo proteger la comunicación entre el terminal móvil y la VA

Dado que un algoritmo criptográfico de clave común es mucho más rápido que otro de clave pública, no hay ningún problema técnico en su adopción para el terminal móvil.

Además, como SSL/TLS intercambian sus certificados en la etapa de inicialización, puede necesitarse más capacidad de memoria de la disponible en el terminal.

Aunque se ha propuesto un planteamiento de conversión de protocolo utilizando una plataforma de seguridad móvil, como se ha indicado anteriormente, puede ser necesario utilizar el protocolo de autenticación entre el ASP y el usuario en la capa superior.

10.2 Consideraciones sobre la utilización de PKI en un entorno móvil

10.2.1 Consideraciones sobre la generación de claves

10.2.1.1 Generador de claves

Cuando se adopta un modelo en el que el usuario genera un par de claves, aunque se requiere la función de generación de claves dentro del dispositivo (es decir que se adopte un modelo en el que lugar de generación de la clave sea el interior del dispositivo), la capacidad de almacenamiento y el rendimiento del proceso constituirán probablemente un problema para el terminal móvil.

Cuando se adopte un modelo en el que la CA o un tercero generen un par de claves, se requerirán consideraciones operacionales y un mecanismo que evite exponer la clave.

10.2.1.2 Lugar de generación de las claves

Por motivos de seguridad, resulta conveniente generar una clave privada dentro de un dispositivo, aunque el rendimiento del proceso pueda suponer un problema adicional.

Cuando se adopte un modelo en el que se instale en el dispositivo una clave generada externamente, se requerirá un mecanismo que evite exponer dicha clave.

10.2.1.3 Lugar de almacenamiento de la clave o certificado

En general, no es posible extraer una clave privada de un dispositivo. La clave privada debe almacenarse en la zona protegida. Hay dos tipos de zonas protegidas:

– la zona protegida físicamente: la clave privada se graba en una zona protegida físicamente tal como una ROM dentro del terminal móvil o en dispositivos externos tales como tarjetas inteligentes;

– la zona protegida por soporte lógico: la clave privada se almacena dentro del terminal móvil en la zona protegida por soporte lógico.

Obsérvese que la zona protegida por soporte lógico debe ser una zona segura en la que sólo un usuario válido pueda regrabar la clave privada o acceder a la misma con protección de control de acceso y/o criptográfica. La protección criptográfica característica de dicha información consiste en utilizar el sistema de criptación basado en contraseña.

Además, es preferible que la clave pública del usuario (certificado) y el certificado de la CA raíz se almacenen en la zona protegida del dispositivo.

10.2.2 Consideraciones sobre la solicitud y emisión del certificado

10.2.2.1 Caso en el que certificado está preinstalado en el dispositivo

En los modelos en los que el usuario móvil adquiere el dispositivo con el certificado preinstalado, es difícil actualizar la clave y el certificado.

Además, en el caso de que el que el certificado no esté vinculado al usuario móvil, puede ser necesario, dependiendo de su uso, emitir un certificado de atributo que describa la asociación del certificado con el usuario móvil.

10.2.2.2 Caso en que la clave está preinstalada en el dispositivo

Dada la dificultad de actualización de la clave, el dispositivo se descarta cuando se revoca el certificado.

10.2.3 Consideraciones sobre utilización del certificado

10.2.3.1 Consideraciones cuando el terminal móvil firma digitalmente

Para TLS, se adopta el método de adjuntar los certificados (todos los certificados, desde el certificado de la CA raíz hasta el certificado del firmante) al mensaje como método de asociar el certificado de la CA raíz al certificado del firmante.

No obstante, si se adjuntan todos lo certificados, desde el certificado de la CA raíz hasta el certificado de firmante, cuando se adjunta la firma, puede producirse una carga excesiva debido a restricciones tales como la capacidad de almacenamiento del terminal móvil.

Aunque también está disponible la técnica de adjuntar una URL que describa el lugar de almacenamiento del certificado del mensaje, no está soportada todavía por TLS.

10.2.3.2 Consideraciones cuando el terminal móvil verifica la firma

Los modelos en las que la validez del certificado es verificada por el propio verificador podrían no ser adecuados para los terminales móviles debido a las muchas restricciones de potencia de procesamiento y de capacidad de almacenamiento.

En los modelos que utilizan una VA, la aplicación que utiliza el certificado debe conocer la VA en la que se confía. Además, cuando se comunica con la VA debe ser capaz de garantizar que la VA es válida.

En el ejemplo de 9.1.2, el terminal móvil accede a la VA a través de la RA. En este caso, el terminal móvil requiere una función que reconozca anticipadamente a la RA en la que confía, así como una función que certifique (autentique) que la RA es correcta en su comunicación con la VA. Para la RA, se necesita una función que conozca la VA en la que el terminal móvil confía y se requiere una función que certifique que la VA es válida en su comunicación con la VA.

10.2.4 Consideraciones sobre la CA

Para los sistemas existentes que utilizan PKI, se establecen relaciones fiables entre distintos dominios de certificación construyendo una jerarquía con varias CA y estableciendo certificaciones cruzadas.

No obstante, cuando se verifica la validez de certificados de cada CA para verificación de firma, la potencia de procesamiento del terminal móvil puede plantear problemas.

Cuando no se utiliza una VA, es conveniente construir una estructura de CA sencilla.

10.3 Consideraciones sobre la PKI en general

10.3.1 Consideraciones sobre la generación de claves

10.3.1.1 Generador de claves

En los modelos en los que el usuario genera las claves, puede darse el caso de que alguien encuentre las claves de otro, buscando en los certificados que concuerdan con la clave pública generada y aparentando ser el propietario de dicho certificado.

Así pues, en los modelos en los que el usuario genera las claves, se requiere la adopción de una clave de suficiente longitud para el número de usuarios previsto.

Por otra parte, puede ser necesario utilizar sistemas que impidan que los certificados de otros se adquieran con facilidad.

10.3.2 Consideraciones sobre la solicitud/emisión/activación de certificados

10.3.2.1 Caso de que se requiera el procedimiento de activación del certificado

Cuando el usuario se somete explícitamente al procedimiento de activación del certificado, se requiere un mecanismo que garantice que es el propio usuario el que ejecuta el procedimiento.

Cuando un certificado se activa en línea, el usuario firma el dato de solicitud de la activación y lo transmite a la RA, etc. En los procesos fuera de línea, puede utilizarse el mismo mecanismo que el de una tarjeta de crédito (incluida la llamada a un operador para solicitar la activación).

10.3.2.2 Caso de que se solicite el certificado en línea

Se requiere un mecanismo que garantice la integridad y autenticidad durante la solicitud. De hecho, se requiere la verificación de la CA, la del solicitante, la protección del trayecto de la comunicación, etc.

10.3.3 Consideraciones sobre la revocación del certificado

Para adoptar un modelo con revocación en línea, se requiere un mecanismo que permita verificar que el solicitante es el usuario. En particular, para revocar un certificado por pérdida de una clave privada, no puede utilizarse la identificación del solicitante con una signatura digital, así que debe facilitarse otro método (tal como el PIN).

Para adoptar un modelo con revocación fuera de línea, tal vez sea necesaria la provisión de un mecanismo para "suspender" el certificado en línea en caso de emergencia.

10.3.4 Consideraciones sobre la renovación de certificados

Además de las consideraciones sobre solicitud y revocación de certificados, hay un problema singular sobre la actualización de certificados que consiste en que, desde el punto de vista de disponibilidad del sistema, es indispensable contar con una solución que evite la omisión de la actualización del certificado.

10.3.5 Problemas con la descripción del certificado

La información contenida en el certificado debe revisarse cuidadosamente ante la eventualidad de que el certificado se difunda más allá de los deseos del emisor.

Apéndice I

Ejemplos de modelo de servicio

En este apéndice se describen los modelos de servicio de la PKI móvil.

I.1 Modelos del servicio de gestión de certificados

En la cláusula 9, se facilita un ejemplo de utilización del sistema fuera de línea en el que un operador de comunicaciones emite certificados. En este apéndice se presentan otros modelos de servicio de gestión de certificados.

I.1.1 Ejemplo de sistema en el que el ASP emite el certificado

En este ejemplo mostrado en las figuras I.1 y I.2, hay dos tipos de certificados; el primer certificado lo facilita la CA de la primera sección (véase la figura I.1) que es la CA del operador que proporciona el certificado que ha de utilizar el terminal móvil en el transporte de sesión segura,

mientras que el segundo certificado lo facilita la CA de la segunda sección (véase la figura I.2) que es la CA del ASP que proporciona el certificado al terminal móvil para utilizarlo en las aplicaciones del terminal móvil. El ASP utiliza un certificado de CA emitido por un operador de comunicaciones que emite su propio certificado. Para emitir/revocar un certificado, el sistema en el lado del operador (CA de la primera sección) utiliza el procesamiento fuera de línea mientras que el sistema en el lado del ASP (CA de la segunda sección) utiliza el procesamiento en línea. Mientras tanto, cuando se solicita el certificado, el sistema en el lado del ASP (CA de la segunda sección) utiliza un certificado emitido por el operador de comunicaciones (CA de la primera sección) como protección del trayecto de comunicación y autenticación del solicitante, y acepta la solicitud en línea.

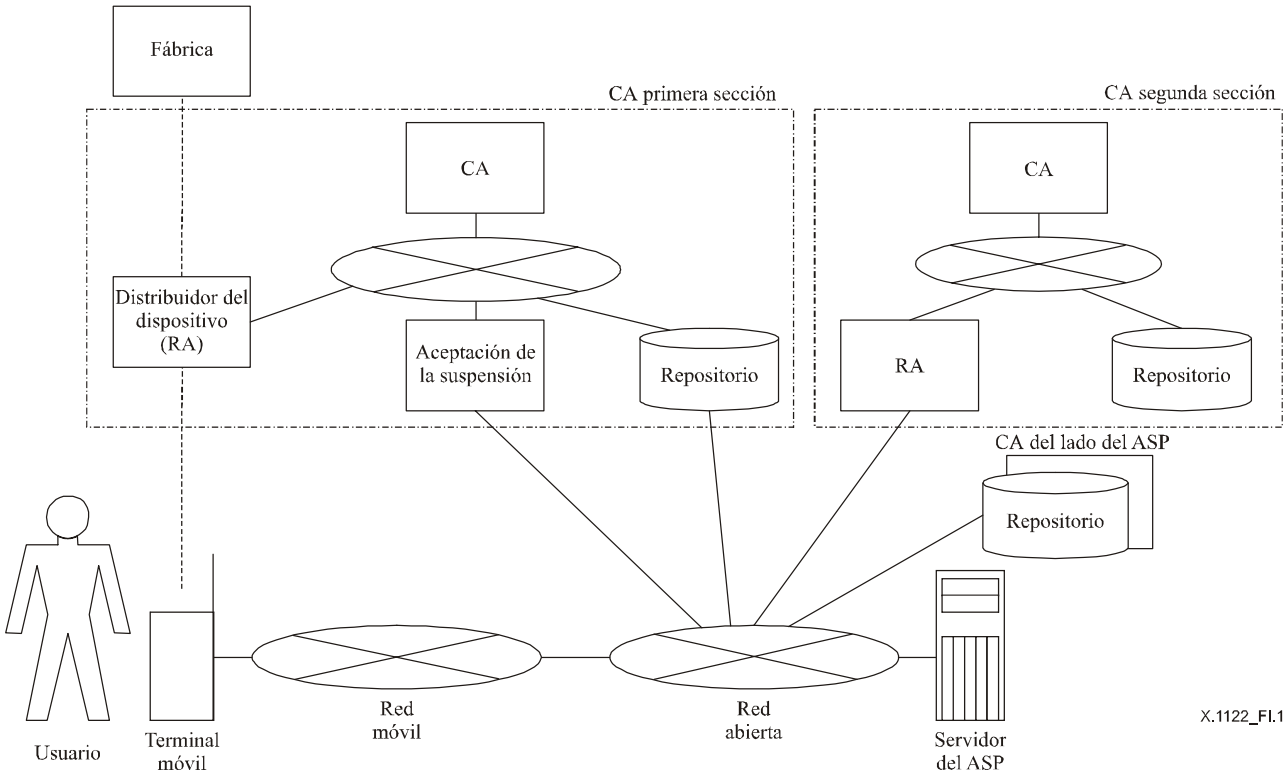

Figura I.1/X.1122 – Ejemplo de sistema en el que el ASP emite el certificado

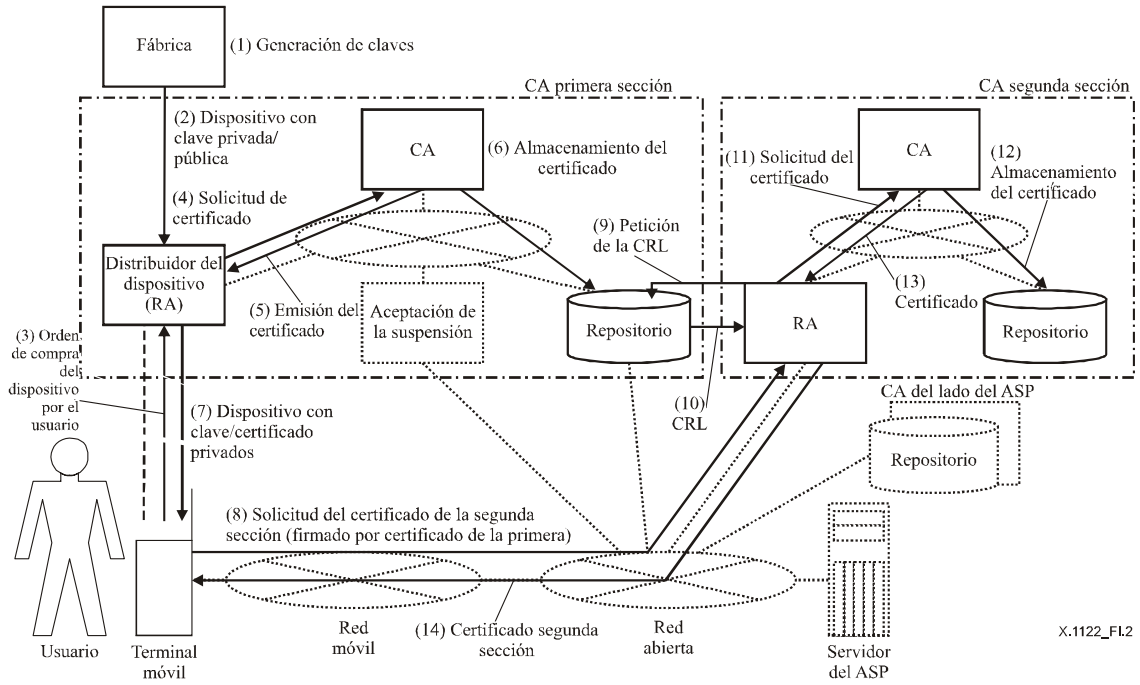

Figura I.2/X.1122 – Ejemplo de emisión del certificado de la segunda sección

Para revocar un certificado emitido por la CA de la segunda sección, el usuario accede también a la RA a través de la red y ejecuta el procedimiento de revocación.

I.1.2 Ejemplo de sistema en el que se utiliza el certificado de atributo

En este ejemplo (véase la figura I.3) se supone que el ASP que utiliza el certificado emitido por un operador de comunicaciones para la identificación de un solicitante, etc., utiliza un certificado de atributo a fin de implementar, por ejemplo, un control de acceso más sofisticado. Aunque se utiliza una AA de usuario para emitir un certificado de atributo para el usuario, se utiliza la CA de usuario para emitir un certificado para el usuario.

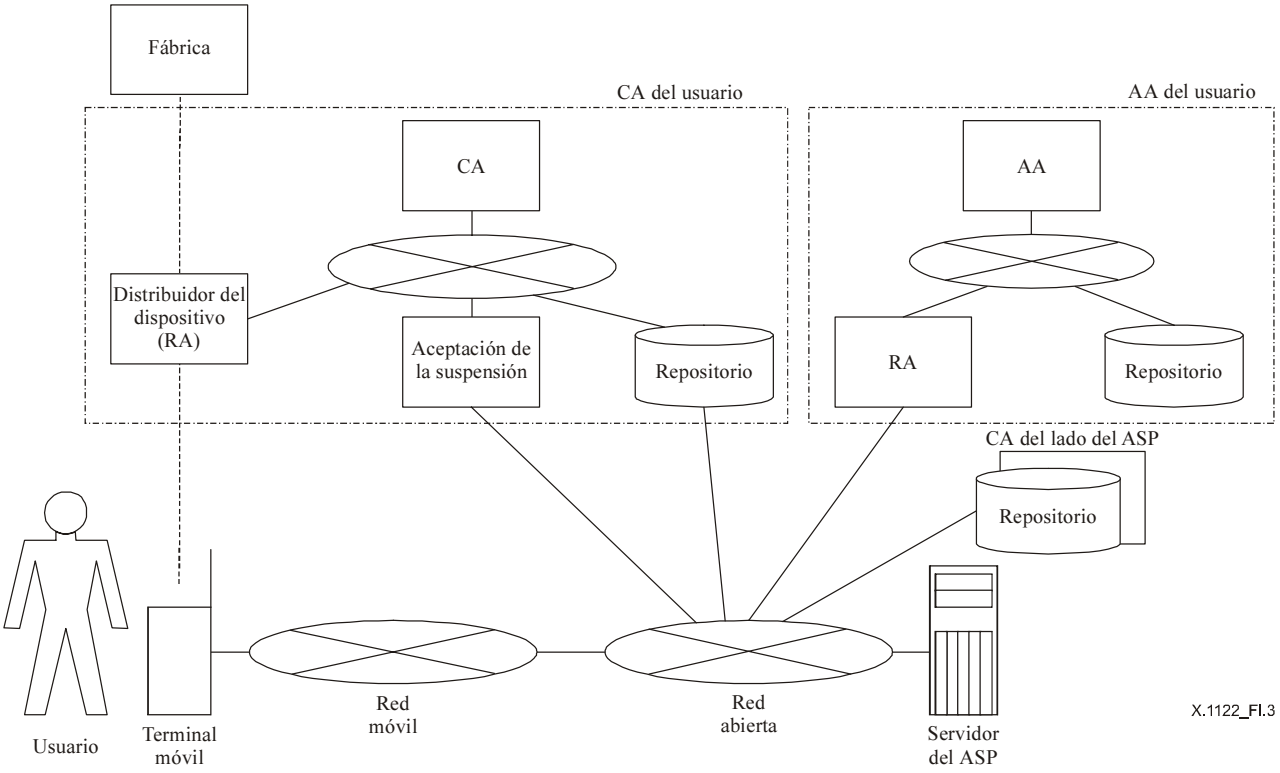

Figura I.3/X.1122 – Ejemplo de sistema en el que se utiliza certificado de atributo

El sistema en el lado del operador de comunicaciones (CA del usuario) utiliza procesamiento fuera de línea para la emisión y revocación de certificados, y utiliza una VA para la verificación de certificados.

El sistema en el lado del ASP (AA del usuario) acepta la solicitud procedente de un usuario en línea, genera un certificado de atributo basado en las políticas de solicitud, y lo asocia al certificado emitido por el operador de comunicaciones. El certificado de atributo se almacena en el repositorio de la AA (también puede definirse un modelo en el que el certificado del atributo se transmita al usuario).

Si un ASP ha recibido un dato con una firma procedente de su usuario, adquiere primero a la CA del lado del operador la CRL del repositorio para verificar la validez del certificado. (En la tienda se verifica asimismo la firma del dato transmitido por el usuario.) A continuación, el ASP adquiere a la AA del lado ASP el certificado de atributo para verificar si el usuario tiene derecho a utilizar el servicio, véase la figura I.4.

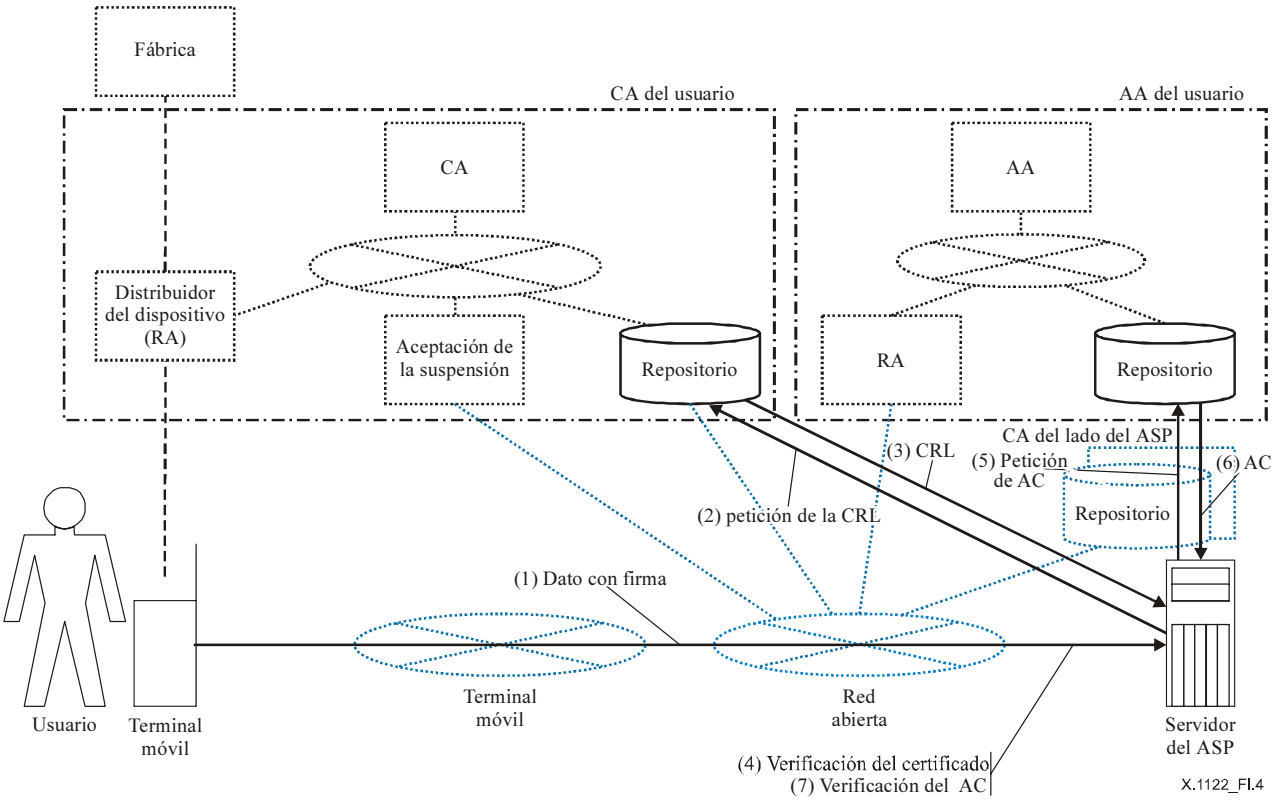

Figura I.4/X.1122 – Ejemplo de modelo de autenticación que utiliza certificado de atributo

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie B	Medios de expresión: definiciones, símbolos, clasificación
Serie C	Estadísticas generales de telecomunicaciones
Serie D	Principios generales de tarificación
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 multimedios
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedios
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	Conmutación y señalización
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 y comunicación entre sistemas abiertos**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet y Redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2004