RECOMENDACIÓN UIT-R M.1223

EVALUACIÓN DE LOS MECANISMOS DE SEGURIDAD PARA LAS IMT-2000

(Cuestión UIT-R 39/8)

(1997)

ÍNDICE

1 Introducción

Las telecomunicaciones móviles internacionales-2000 (IMT-2000) son sistemas móviles de la tercera generación cuya puesta en servicio está prevista alrededor del año 2000, dependiendo de las condiciones del mercado. Dichos sistemas proporcionarán acceso, mediante uno o más radioenlaces, a una amplia gama de servicios de telecomunicación soportados por las redes de telecomunicaciones fijas (por ejemplo, la RTPC/RDSI) y a otros servicios específicos a los usuarios móviles.

Engloba un conjunto de tipos de terminales móviles que acceden a las redes terrenales o por satélite, habiéndose diseñado sus terminales para la utilización móvil o fija.

Las características fundamentales de las IMT-2000 son las siguientes:

– un alto grado de comunidad de diseño en todo el mundo;

– compatibilidad de los servicios dentro de las IMT-2000 y con las redes fijas;

– alta calidad;

– utilización de pequeños terminales de bolsillo con capacidad de itinerancia a escala mundial;

– bajo coste.

Las IMT-2000 son definidos por un conjunto de Recomendaciones UIT interdependientes de las que ésta forma parte.

El asunto de las IMT-2000 es complejo y su presentación en forma de Recomendaciones está en constante evolución. Para mantener el ritmo de progresos que está experimentando este tema es necesario elaborar una serie de Recomendaciones sobre una amplia variedad de aspectos. Debe intentarse que las Recomendaciones no caigan en contradicciones evidentes entre ellas mismas. No obstante, para resolver cualquier discrepancia se elaborarán futuras Recomendaciones o se modificarán las existentes.

Debido a la naturaleza particular de las comunicaciones inalámbricas, las IMT-2000 deben incorporar medidas de seguridad para evitar el acceso de partes no autorizadas a los datos transmitidos. Además, la naturaleza de las comunicaciones móviles exige tomar medidas de seguridad para impedir el acceso fraudulento a los servicios y la utilización ilegal de los recursos del suministrador y del organismo explotador.

2 Ámbito

Esta Recomendación pretende identificar las clases de mecanismos de seguridad adecuados para establecer las características de seguridad de las IMT-2000 definidas en la Recomendación UIT-R M.1078 sobre principios de seguridad para las IMT-2000 y satisfacer de esta forma los requisitos de seguridad de las IMT-2000 identificados en dicha Recomendación. El Anexo 1 presenta algunos candidatos específicos para mecanismos de seguridad y realiza una evaluación sobre la pertinencia de su utilización en las IMT-2000.

Esta Recomendación pretende ser un punto de arranque para la elaboración de Recomendaciones más detalladas relativas a la seguridad de las IMT-2000 que serán desarrolladas por las diversas Comisiones de Estudio de la UIT.

3 Estructura de la Recomendación

En el § 7.1 figuran diversos requisitos de los mecanismos de seguridad. En el § 7.2 se identifican varias clases de mecanismos de seguridad y se considera su conveniencia para satisfacer las características de seguridad de las IMT-2000 identificadas en la Recomendación UIT-R M.1078. En el Anexo 1 se describen algunos candidatos para mecanismos de seguridad de las IMT-2000, evaluándose su pertinencia.

4 Documentos conexos

Las siguientes Recomendaciones de la UIT contienen información sobre las IMT-2000 relacionadas con la presente Recomendación:

Recomendación UIT-R M.687:	Telecomunicaciones móviles internacionales-2000 (IMT-2000)
Recomendación UIT-R M.1078:	Principios de seguridad para las telecomunicaciones móviles internacionales-2000 (IMT-2000)
Recomendación UIT-T F.115:	Objetivos de servicio y principios para los futuros sistemas públicos de telecomunicaciones móviles terrestres.

5 Definiciones

En la presente Recomendación se utilizan las siguientes siglas:

IMUI: Identidad de usuario móvil internacional (international mobile user identity)
TMUI: Identidad de usuario móvil temporal (temporary mobile user identity)
IMTI: Identidad del terminal móvil internacional (international mobile terminal identity)
TMTI: Identidad del terminal móvil temporal (temporary mobile terminal identity)
SPID: Identidad del suministrador de servicio (service provider identity)
NOID: Identidad de operador de red (network operator identity)

Knu: Clave secreta usuario-operador de red (esquemas de clave simétrica)
Ksu: Clave secreta usuario-suministrador de servicio (esquemas de clave simétrica)
Kpu: Clave de verificación pública de usuario (esquemas de clave asimétrica)
Ksigu: Clave de signatura privada de usuario (esquemas de clave asimétrica)
Kss: Clave de signatura privada del suministrador de servicio (esquemas de clave asimétrica)
Kps: Clave de verificación pública del suministrador de servicio (esquemas de clave asimétrica)
Ksn: Clave de descifrado privada del operador de red (esquemas de clave asimétrica)
Kpn: Clave de cifrado pública del operador de red (esquemas de clave asimétrica)
Ks: Clave de sesión

Au: Algoritmo de autenticación de usuario
At: Algoritmo de autenticación de terminal
As: Algoritmo de autenticación del suministrador de servicio
An: Algoritmo de generación de clave del operador de red
Ak: Algoritmo de generación de clave de sesión

Cu: Algoritmo de ocultación de identidad
E: Transformación de cifrado (algoritmo de cifrado de clave pública)
D: Transformación de descifrado (algoritmo de cifrado de clave pública)
S: Transformación de signatura (signatura digital)
V: Transformación de verificación (signatura digital)

H: Función de Hash

RND: Pregunta de autenticación aleatoria (random authentication challenge)
RES: Valor de verificación de autenticación (authentication check value)

CERT: Certificación
CIPH: Cadena de bits utilizada para ocultar la identidad
SIG: Signatura
KO: Desplazamiento de la clave

6 Consideraciones

En la elaboración de esta Recomendación se han considerado los siguientes factores:

a) la necesidad de que la calidad del servicio de las IMT-2000 sea comparable a la que presta la RTPC/RDSI;

b) la importancia cada vez mayor de los diversos tipos de servicios de telecomunicaciones no vocales;

c) debido a la naturaleza particular de las comunicaciones inalámbricas, éstas permiten una fácil recepción por otras partes además del destinatario previsto;

d) por la razón indicada en c), las IMT-2000 deben incorporar las medidas oportunas de seguridad para lograr la privacidad de las comunicaciones en la interfaz radioeléctrica;

e) debido a la naturaleza de las comunicaciones móviles, es necesario tomar medidas concretas para evitar un acceso fraudulento a los servicios así como el uso indebido de los recursos del suministrador y del organismo explotador;

f) la descripción general del sistema que figura en el § 6 de la Recomendación UIT-R M.1078;

g) las Recomendaciones UIT-T y UIT-R pertinentes y los estudios en curso;

h) la necesidad de lograr una estructura flexible en el sistema que sea capaz de adaptarse fácilmente a las inversiones necesarias en la red a fin de aumentar los ingresos y a los factores ambientales, así como de responder a los nuevos desarrollos sin introducir restricciones en las innovaciones;

j) la necesidad de que los terminales móviles (incluidos los que tienen capacidad de satélite) puedan transitar entre redes de telecomunicaciones móviles situadas en distintos países;

k) que las IMT-2000 deberán funcionar en una gran variedad de entornos, cada uno de ellos con distintas características de propagación y diferentes densidades de tráfico y tipos de movilidad.

7 Recomendación

A continuación figuran los requisitos de los mecanismos de seguridad y las clases de mecanismos de seguridad recomendados para las IMT-2000.

7.1 Requisitos de los mecanismos de seguridad

a) Los mecanismos de seguridad deben requerir el mínimo de señalización en tiempo real a larga distancia. Por ejemplo, debe evitarse la necesidad de establecer conexiones de señalización internacional en cada llamada o actualización del emplazamiento cuando se está en itinerancia (tránsito).

b) Los mecanismos de seguridad deben exigir un mínimo de acuerdos previos bilaterales entre los suministradores de servicio y los operadores de red.

c) Los mecanismos de seguridad deben incluir los medios necesarios para gestionar las claves criptográficas que deban intercambiar los suministradores de servicio y los operadores de red.

d) Deber ser fácil la distribución y modificación de las claves criptográficas de los mecanismos de seguridad necesarios a los usuarios.

e) Los mecanismos de seguridad deben estar normalizados únicamente en la medida necesaria para lograr interfuncionamiento y capacidad de tránsito (itinerancia).

f) Los mecanismos de seguridad deben soportar la gestión de control de versión para permitir posteriores mejoras y revisiones en los mecanismos.

g) Los mecanismos de seguridad deben incluir los medios precisos para detectar violaciones de la seguridad e informar sobre las mismas, así como los métodos adecuados para restaurar el sistema al estado de seguridad.

h) Los mecanismos de seguridad deben satisfacer los requisitos legales impuestos por las autoridades nacionales; por ejemplo, controles a la exportación, intercepción legal, etc.

j) Los mecanismos de seguridad deben permitir un tratamiento independiente de las características de seguridad relativas al usuario y al terminal para que las IMT-2000 puedan soportar la movilidad de usuario, cuando sea necesaria, y la movilidad del terminal.

7.2 Clases de mecanismos de seguridad

Las características de seguridad indican el tipo de seguridad que se proporciona y los mecanismos de seguridad se refieren a la manera de proporcionar dicha seguridad. En este punto se identifican varias clases de mecanismos de seguridad y se discute su idoneidad para proporcionar las características de seguridad que deben incorporar las IMT-2000. Las clases identificadas se basan en la clasificación utilizada por la ISO, siempre que sea posible. Además, se enumeran las posibles ventajas e inconvenientes de los diversos métodos.

Sólo se dan descripciones de alto nivel de las clases de mecanismos. En el Anexo 1 figuran descripciones más detalladas de algunos mecanismos en particular. Las clases de mecanismos aparecen ordenadas de acuerdo con la característica de seguridad que satisfacen más adecuadamente.

El término «entidad» se utiliza a lo largo del texto para indicar un cometido sin especificar (por ejemplo, usuario, terminal, suministrador de servicio, operador de red, etc.).

7.2.1 Mecanismos de autenticación

Una distinción fundamental entre los mecanismos de seguridad es la división entre mecanismos «de clave simétrica» (o de clave secreta) y mecanismos «de clave asimétrica» (o de clave pública). Los mecanismos de clave simétrica han sido utilizados con éxito en los actuales sistemas móviles y los mecanismos de clave asimétrica constituyen una novedad para los sistemas móviles pero se han empleado con buen resultado en las actuales redes de ordenadores.

7.2.1.1 Clave simétrica

En los mecanismos de clave simétrica, cada entidad tiene asociada una clave secreta. Las claves son conocidas únicamente por la entidad propietaria y las entidades acreditadas por la misma, y deben estar almacenadas en lugar seguro, posiblemente en un módulo de identidad de usuario (UIM – user identity module) transportable (por ejemplo, una tarjeta pequeña) o en una base de datos segura. La autenticación se basa en el principio de que la clave secreta de una entidad sólo es conocida por dicha entidad y por un número limitado de entidades acreditadas; por ejemplo, aquellas que desean autenticar al propietario.

Para obtener la autenticación, la entidad que va a autenticarse debe demostrar el conocimiento de la clave secreta a la parte de autenticación. Ello puede hacerse generando pares de pregunta-respuesta, utilizando quizá la clave secreta como entrada (junto con otros datos) a un algoritmo criptográfico unidireccional.

Ventajas:

– para la autenticación entre el usuario y el operador de red, puede ser posible la utilización de algoritmos específicos al suministrador de servicio. Si el operador de red cuenta con parámetros de autenticación previamente calculados procedentes del suministrador de servicio, el algoritmo de autenticación puede ser específico del suministrador de servicio. De forma alternativa, si el operador de red recibe una clave de autenticación (temporal), es el algoritmo de cálculo de dicha clave de autenticación el que puede ser específico del suministrador de servicio;

– puede adaptarse fácilmente para calcular las claves de sesión;

– cuenta con algoritmos relativamente rápidos y sencillos;

– se requiere un volumen de datos pequeño para la autenticación.

Inconvenientes:

– la red debe disponer de bases de datos seguras;

– si el operador de red recibe una clave de autenticación temporal, en todas las redes y UIM debe utilizarse un algoritmo de autenticación normalizado;

– puede que sea difícil adaptar los mecanismos para realizar la autenticación entre entidades arbitrarias, debido a la necesaria distribución de las claves secretas;

– debe existir una relación de confianza entre el suministrador de servicio y los operadores de red para el intercambio de las claves o de los mecanismos de autenticación previamente calculados;

– es necesario contar con una comunicación segura entre el suministrador de servicio y los operadores de red;

– puede que sea más difícil obtener otras características tales como tarificación incuestionable y confidencialidad de la identidad de usuario.

7.2.1.2 Clave asimétrica

En los mecanismos de clave asimétrica, cada entidad que debe autenticarse tiene una clave pública y la correspondiente clave secreta. La clave secreta es conocida únicamente por el propietario (por ejemplo, usuario o componente de red) y la clave pública puede estar distribuida.

El solicitante logra la autenticación demostrando el conocimiento de la clave secreta apropiada a la entidad de autenticación. La autenticación generalmente funciona de la forma siguiente: para proporcionar autenticación, el solicitante utiliza su clave secreta a fin de obtener la información de autenticación adecuada a partir de los datos de entrada de autenticación especificados. El verificador puede utilizar la correspondiente clave pública para la verificación.

Para la distribución de la clave pública existen varios métodos. Por ejemplo, una entidad puede poseer un certificado, calculado por una entidad acreditada, que certifica la autenticidad de la clave pública. Este certificado puede distribuirse si se precisa. De forma alternativa, puede disponerse de una base de datos en la red que contenga certificados para todas las entidades. Ambos métodos exigen la disponibilidad de otra entidad acreditada para calcular los certificados o gestionar la base de datos. Otra alternativa consiste en realizar una preinstalación de claves públicas de posibles corresponsales en la comunicación dentro de una entidad.

Ventajas:

– no es necesario almacenar o transmitir las claves secretas de autenticación dentro de una red;

– puede que no sea necesaria la señalización al suministrador de servicio;

– se adapta fácilmente a la autenticación entre cualquier par de entidades;

– no es necesario contar con una comunicación segura entre el suministrador de servicio y los operadores de red.

Inconvenientes:

– los algoritmos de autenticación normalmente presentan una mayor complejidad de cálculo;

– se dispone de un número menor de posibles algoritmos;

– debe llegarse a un acuerdo a escala mundial sobre el algoritmo de autenticación, aunque es posible utilizar varias versiones negociables;

– los intercambios de mensajes tienden a ser más largos;

– pueden ser necesarias las autoridades de certificación.

7.2.1.3 Conocimiento cero

Con este método el usuario tiene dos identidades, una identidad pública (PI – public identity) y una correspondiente identidad secreta (SI – secret identity). Estas identidades son establecidas por el suministrador de servicio y se comunican al UIM. Para establecer de las identidades es preciso conocer algunos parámetros secretos (por ejemplo, los factores de un número entero *N* elevado), pero la relación entre las entidades puede verificarse utilizando un parámetro que no es necesario proteger contra la divulgación (por ejemplo, el propio entero *N*).

La verificación de la identidad de una entidad utiliza un protocolo de conocimiento cero que permite al verificador convencerse de que la entidad conoce la identidad secreta sin que el verificador (o cualquier escuchador furtivo) tenga acceso a esta identidad, aunque viole el protocolo.

Ventaja:

– nivel de seguridad ajustable.

Inconvenientes:

– los mecanismos tienden a ser complejos;

– el acuerdo/distribución de la clave de sesión no puede integrarse fácilmente;

– deben transmitirse grandes volúmenes de datos.

7.2.2 Mecanismos de anonimato

7.2.2.1 Identidades temporales que utilizan clave simétrica

Una identidad temporal es desechable y únicamente es válida durante un periodo de tiempo limitado. Una identidad temporal puede ser única solamente en una zona de emplazamientos y puede reatribuirse, por ejemplo, en cada actualización de emplazamientos.

La identidad temporal puede utilizarse en los enlaces que no proporcionan seguridad a efectos de identificación, garantizando el anonimato de las entidades. La asignación de la identidad temporal debe protegerse; por ejemplo, mediante encripción. En algunos mecanismos, puede permitirse, en casos excepcionales, la utilización de la identidad permanente.

Ventaja:

– las identidades temporales son más cortas.

Inconvenientes:

– la asignación de identidades temporales puede exigir cierta gestión suplementaria para evitar las duplicaciones;

– cuando aparecen errores puede que sea necesario utilizar la identidad permanente.

7.2.2.2 Confidencialidad de la identidad utilizando clave asimétrica

La confidencialidad de la identidad de la entidad puede proporcionarse mediante un sistema de encripción de clave pública.

La entidad puede ampliar su identidad permanente (por ejemplo, con un número aleatorio) y a continuación cifrarla utilizando un algoritmo de clave pública (por ejemplo, Rivest-Shamir-Adleman (RSA)) con la clave pública de la parte de recepción: por ejemplo, operador de red, suministrador de servicio o usuario.

La ampliación es necesaria para evitar que los intrusos puedan reproducir la identidad cifrada y de esa forma verificar la propia identidad.

Ventajas:

– no se necesitan identidades temporales;

– la identidad nunca tiene que enviarse sin protección.

Inconveniente:

– las identidades cifradas (utilizando algoritmos asimétricos) son más largas que la identidad del texto en claro.

7.2.2.3 Acceso anónimo

También deben considerarse los mecanismos que no hacen uso de ningún tipo de identificación para lograr el anonimato; por ejemplo, el empleo de tarjetas de previo pago.

Ventaja:

– se elimina completamente el riesgo de divulgación de las identidades.

Inconveniente:

– son raros los casos en que se permite el acceso anónimo.

7.2.3 Mecanismos de confidencialidad

El mecanismo de confidencialidad puede utilizar un cifrado de tren o un cifrado de bloque. La función de cifrado normalmente reside en los terminales móviles de las IMT-2000.

– Puede que sea necesario más de un algoritmo para satisfacer las diversas restricciones jurídicas/de política nacional;

– a efectos de itinerancia, será necesario introducir un cierto grado de normalización.

7.2.3.1 Cifrados de bloque

Los cifrados de bloque se caracterizan por el cifrado de los datos de un campo de longitud fija bajo control de una clave. Normalmente, los cifrados de bloque se emplean con un modo de funcionamiento adecuado tal como el ECB, CBC, CFB y OFB (véase ISO/CEI 10116, «Modes of operation for *n*-bit block cipher algorithm», 1991).

Ventaja:

– los cifrados de bloque normalmente están bien documentados.

Inconvenientes:

– pueden aparecer algunos errores de propagación;

– son inevitables los retardos en el descifrado.

7.2.3.2 Cifrados de tren

Un cifrado de tren es un sistema en el que se introduce una clave en un generador de secuencia que utiliza dicha clave para crear una secuencia de longitud arbitraria. A continuación se añade ese tren de clave a los datos bit a bit.

Ventaja:

– los errores normalmente no se propagan.

7.2.4 Mecanismos de seguridad no criptográficos

7.2.4.1 Verificación de usuario

Los mecanismos de verificación comprueban si el usuario actual es el usuario genuino del UIM o al menos si está autorizado por el usuario genuino. Si el UIM puede separarse del terminal, éste también puede verificar al usuario. A menudo se utilizan dos métodos: protocolo unidireccional y protocolo de pregunta/respuesta. Generalmente, se llega a un compromiso entre el grado de esfuerzo exigido al usuario y el grado de seguridad que se logra.

Un protocolo unidireccional típico para verificación de usuario es el empleo de un Número de Identidad Personal (PIN – personal identity number) que consiste en un número secreto conocido únicamente por el propietario (u otra identidad autorizada) del terminal/UIM y por el propio terminal/UIM. Se solicita al usuario que introduzca su PIN mediante teclado. A continuación se verifica el PIN en el terminal/UIM.

Un método típico de protocolo pregunta-respuesta para verificación de usuario es una interacción en la que el terminal/UIM genera un número aleatorio de unas cuantas cifras y el usuario proporciona el resultado de un cálculo sencillo sobre dicho número, que puede verificar el terminal/UIM.

Ventaja:

– no se necesita ninguna interacción de red.

Inconveniente:

– es necesaria la interacción humana, en consecuencia sólo pueden utilizarse mecanismos de autenticación muy poco potentes.

7.2.4.2 Registro

Cada terminal certificado presenta una identidad de terminal única. La red puede interrogar al terminal y solicitar la identidad. De forma alternativa, la identidad puede acompañar a otros datos enviados durante los procedimientos particulares. La red almacena bases de datos que contienen las listas de las identidades de terminal únicas. Las bases de datos pueden incluir diversas listas: lista blanca, lista gris y lista negra. Esta última contiene las identidades de los terminales que ya no están autorizados a utilizar la red. La lista gris contiene las identidades de terminales sospechosos y en la lista blanca figuran las identidades autorizadas.

Las diversas redes pueden decidir si proporcionan tales bases de datos. Es necesario establecer bases de datos centrales que contengan todos los terminales disponibles (internacionalmente) y su estado asociado a fin de permitir un completo interfuncionamiento y una itinerancia internacional.

Ventaja:

– puede utilizarse para identificar un cierto número de distintos problemas en los equipos; por ejemplo, robo, funcionamiento incorrecto y terminales no certificados.

Inconvenientes:

– puede modificarse y predecirse una identidad; no constituye una protección contra terminales clonados (de imitación);

– es necesario realizar regularmente actualizaciones (también internacionalmente) para que la información sea fiable;

– son necesarios mensajes adicionales de señalización.

7.2.4.3 Cómputo de llamadas

Una forma de detección de clónicos es la utilización de un parámetro de «cómputo de llamada» que puede actualizarse en el UIM tras recibir una instrucción de la red. Un contador similar será también actualizado por el suministrador de servicio doméstico. Si un UIM en particular presenta valores discontinuos de «cómputo», es probable que se esconda un clónico tras el UIM legítimo que puede acceder al servicio antes que el usuario legitimado. Este mecanismo detecta únicamente la clonización de UIM.

Un «cómputo de llamadas» debe también estar ligado al terminal y actualizado en el mismo y en una base de datos global que contenga las identidades de terminales y los cómputos de llamada asociados. Esta variante detecta la clonización de los terminales.

Ventaja:

– no se necesitan mecanismos de protección físicos costosos.

Inconvenientes:

– puede que sea necesario establecer en la red una gestión del cómputo de llamadas;

– puede que sea necesario contar con mensajes adicionales de señalización.

7.2.5 Mecanismos de integridad

7.2.5.1 Cifrado

Si los datos transferidos contienen la redundancia adecuada, el cifrado puede proporcionar la suficiente seguridad de que los datos transmitidos no han sido modificados.

Ventaja:

– no existe más coste adicional que la prestación de confidencialidad.

Inconvenientes:

– no existe prevención contra los ataques basados en la reproducción (deben añadirse números aleatorios o contadores);

– puede utilizarse únicamente con datos muy redundantes.

7.2.5.2 Clave simétrica

Existen dos técnicas básicas para lograr la integridad de un mensaje: códigos de autenticación de mensajes (MAC – message authentication codes), que comprenden una cadena de datos que constituye una función criptográfica del mensaje y una clave secreta, y códigos de detección de la manipulación (MDC – manipulation detection codes), que comprenden una cadena de datos que consiste solamente en una función del mensaje. Como la función de generación del MDC es públicamente conocida, es preciso realizar una encripción al menos del MDC.

Ventaja:

– algoritmos relativamente sencillos.

Inconvenientes:

– no existe protección contra los ataques basados en la reproducción (deben añadirse números aleatorios o contadores);

– es necesario conocer las claves secretas de los corresponsales en la comunicación;

– sólo protege contra ataques por terceras partes.

7.2.5.3 Clave asimétrica

Al valor «hash» del mensaje original se le añade una signatura con la clave secreta del remitente. Esta signatura se incorpora al mensaje transmitido y puede ser verificada por cualquier receptor que posea la clave pública de los remitentes.

Ventaja:

– cualquier tercera parte puede verificar los datos.

Inconvenientes:

– los algoritmos tienden a presentar una mayor complejidad de cálculo;

– se dispone de un número menor de algoritmos candidatos.

7.2.6 Mecanismos de no repudio

Las signaturas digitales calculadas sobre los datos conocidos pueden utilizarse para obtener el no repudio de los datos enviados y recibidos.

Pueden obtenerse diferentes niveles de no repudio según el volumen de datos en los que va a incluirse una signatura y la forma de obtener y almacenar las signaturas calculadas y los datos originales.

Ventaja:

– puede lograrse distintos niveles de no repudio.

Inconveniente:

– deben utilizarse algoritmos asimétricos para evitar que el verificador genere signaturas falsas.

7.2.7 Gestión de la seguridad

7.2.7.1 Gestión de clave

Se dispone de varias formas de generación, distribución, certificación, etc., de la clave. Los requisitos para la gestión de clave dependerán de los mecanismos específicos de las IMT-2000 elegidos para soportar las características de seguridad de estos sistemas.

7.2.7.2 Gestión de versión

La gestión de versión es un mecanismo que permite al sistema actualizar o sustituir los mecanismos o procedimientos de seguridad sin que sea necesario reemplazar los terminales móviles de las IMT-2000 existentes. Una razón para contar con UIM desmontables es poder actualizar los mecanismos y algoritmos emitiendo nuevos UIM (sin que resulten afectados, en consecuencia, los terminales).

ANEXO 1

Mecanismos de seguridad candidatos

Este Anexo describe con detalle varios ejemplos de mecanismos de seguridad sin establecer correspondencia con la arquitectura funcional de las IMT-2000 como se indica en la Recomendación UIT-R M.817. Estos mecanismos de seguridad se muestran únicamente a título de ejemplo, también pueden aplicarse otros mecanismos alternativos.

1 Mecanismo de autenticación mutua basado en una función de verificación de clave secreta

Este punto describe un ejemplo de mecanismo de autenticación mutua basado en la utilización de criptografía de clave secreta previo intercambio de pregunta-respuesta. Combina en un solo mecanismo la característica de confidencialidad de la identidad de usuario, autenticación de entidad y generación de clave de sesión.

1.1 Características proporcionadas

El mecanismo proporciona las siguientes características de seguridad:

– Autenticación de entidad mutua entre el usuario y el operador de red.

– Confidencialidad de la identidad de usuario en el trayecto de comunicaciones entre el usuario y el operador de red.

– Establecimiento de la clave de sesión entre el usuario y el operador de red (para su utilización proporcionando otras características de seguridad, posiblemente incluidas la confidencialidad y/o la integridad de los datos intercambiados entre el usuario y el operador de red).

1.2 Requisitos iniciales

El mecanismo hace uso de los siguientes algoritmos criptográficos:

– Algoritmo de autenticación de usuario, Au. Este algoritmo tiene como entrada una clave secreta y una cadena de datos y como salidas un RES de valor verificado.

– Algoritmo de autenticación de suministrador de servicio, As. Este algoritmo tiene como entrada una clave secreta y una cadena de datos y como salidas un RES de valor verificado. Este algoritmo puede ser el mismo o distinto del algoritmo Au.

– Algoritmo de ocultación de identidad, Cu. Este algoritmo tiene como entrada una clave secreta y una cadena de datos y como salidas una cadena CIPH utilizada para proteger la identidad de usuario.

– Algoritmo de generación de clave de sesión, Ak. Este algoritmo tiene como entrada una clave secreta y una cadena de datos y como salidas una clave de sesión, Ks.

– Algoritmo de generación de clave de operador de red, An. Este algoritmo tiene como entrada una clave secreta y una cadena de datos y como salidas una clave secreta de usuario-operador de red, Knu. Este algoritmo puede ser el mismo o distinto del algoritmo Ak.

El mecanismo utiliza los siguientes tipos de clave criptográfica:

– Clave secreta usuario-suministrador de servicio, Ksu. Se trata de claves secretas conocidas únicamente por el usuario y sus suministradores de servicio. Estas claves secretas permanecen fijas durante largos periodos de tiempo.

– Clave secreta usuario-operador de red, Knu. Se trata de claves secretas conocidas únicamente por el usuario y su operador de red «actual». Estas claves pueden permanecer fijas mientras un usuario está registrado con un operador de red en particular. Asociado a cada clave se encuentra un desplazamiento de clave (KO – key offset) que se utiliza junto a la clave secreta usuario-suministrador de servicio, Ksu, para generar la Knu.

– Clave de sesión, Ks. Se trata de claves secretas conocidas únicamente por el usuario y su operador de red actual (es decir, el operador de red con el que está registrado). Una nueva clave de sesión se genera como resultado de la utilización del mecanismo de autenticación. Estas claves pueden utilizarse para cifrado de datos y/o para la prestación de las características de seguridad.

El mecanismo utiliza los siguientes tipos de identificadores:

– Identidad de usuario móvil internacional (IMUI – international mobile user identity). Se trata de una identidad permanentemente asociada a un usuario. La IMUI nunca pasa por la interfaz aérea evitando de esa forma su divulgación no autorizada.

– Identidad del operador de red (NOID – network operator identity).

– Identidad de usuario temporal para el operador de red (TMUIn). Esta identidad (temporal) se utiliza para identificar un usuario al operador de red con el que está actualmente registrado. Es conocida por el usuario y por el operador de red de las IMT-2000.

– Identidad de usuario temporal para el suministrador de servicio, TMUIs. Esta identidad (temporal) se utiliza para identificar al usuario con el suministrador de servicio. Es conocida por el usuario y por su suministrador de servicio.

El mecanismo tiene el siguiente requisito adicional:

– El operador de red y el suministrador de servicio necesitan un canal seguro para intercambiar el segundo y tercer mensajes de la versión del mecanismo «nuevo registro».

1.3 Descripción del mecanismo

Existen dos versiones del mecanismo dependiendo de si el usuario está actualmente registrado o no con el operador de red. Se consideran estos dos casos por separado (aunque están estrechamente relacionados).

1.3.1 Registros actuales

Se considera en primer lugar el caso en que el usuario ya está registrado con el operador de red. Ello significa que el usuario y el operador de red compartirán una identidad temporal válida TMUIn y la clave secreta Knu. El mecanismo en este caso consiste en el intercambio de tres mensajes entre el usuario y el operador de red. El suministrador de servicio no interviene.

Los tres mensajes son los siguientes:

Mensaje 1:	Usuario	→	operador de red:	TMUIn, RNDu
Mensaje 2:	Operador de red	→	usuario:	RNDn, KO, TMUIn'+CIPHn, RESn
Mensaje 3:	Usuario	→	operador de red:	RESu.

Cabe señalar que el signo + en los anteriores mensajes significa adición binaria bit a bit de dos cadenas.

Los valores RNDu y RNDn son «preguntas» aleatorias generadas por el usuario y el operador de red, respectivamente.

Los valores RESu y RESn son «respuestas a preguntas» generadas por el usuario y el operador de red, respectivamente. El RESn se calcula utilizando el algoritmo de autenticación de usuario Au y como entrada de la cadena de datos la concatenación de RNDn, RENDu y TMUIn'. RESu se calcula utilizando el algoritmo de autenticación de usuario Au tomando como entrada de clave Knu y como entrada de la cadena de datos la concatenación de RNDu y RNDn.

TMUIn' es la «nueva» identidad de usuario temporal para emplear con el operador de la red. Sustituirá a la identidad temporal actual TMUIn.

CIPHn es una cadena de bits utilizada para proteger la nueva identidad temporal TMUIn' mientras está en tránsito entre el operador de red y el usuario. Se calcula utilizando el algoritmo de ocultación de identidad Cu introduciendo como entrada de clave secreta Knu y como entrada de la cadena de datos RNDu.

El usuario y el operador de red pueden calcular la clave de sesión Ks como la salida del algoritmo de generación de la clave de sesión, Ak, tomando como entrada de la clave secreta Knu y como entrada de la cadena de datos la concatenación de RNDu, RNDn y TMUIn'.

Para el caso especial de autenticación unidireccional usuario a red y ocultación de identidad, no deben utilizarse los parámetros RNDu y RESn. En este caso, se calcula CIPHn utilizando el algoritmo Cu y tomando como entrada de clave secreta Knu y como entrada de la cadena de datos RNDn.

1.3.2 Nuevos registros

En segundo lugar se considera el caso en que el usuario no está registrado con el operador de red. Ello significa que el usuario y el operador de red no comparten ninguna información. El mecanismo para este caso consiste en el intercambio de cinco mensajes entre el usuario, el operador de red y el suministrador de servicio del usuario.

Los cinco mensajes son los siguientes:

Mensaje 1:	Usuario	→	operador de red:	TMUIs, RNDu
Mensaje 2:	Operador de red	→	suministrador de servicio:	TMUIs, RNDu
Mensaje 3:	Suministrador de servicio	→	operador de red:	TMUIs'+CIPHs, KO, Knu, RESs
Mensaje 4:	Operador de red	→	usuario:	TMUIs'+CIPHs, RESs, RNDn, KO, TMUIn'+CIPHn, RESn
Mensaje 5:	Usuario	→	operador de red:	RESu.

Cabe señalar en primer lugar que se dispone de un canal seguro para intercambiar los mensajes 2 y 3 entre el operador de red y el suministrador de servicio.

Al igual que antes, los valores RNDu y RNDn son «preguntas» aleatorias generadas por el usuario y el operador de red, respectivamente.

Los valores RESu, RESn y RESs son «respuestas a preguntas» generadas por el usuario, el operador de red y el suministrador de servicio, respectivamente. RESn y RESu se calculan como en el caso anterior. RESs se determina utilizando el algoritmo de autenticación del suministrador de servicio, As, tomando como entrada de clave Ksu y como entrada de la cadena de datos la concatenación de RNDu y TMUIs'.

TMUIs' es la «nueva» identidad de usuario temporal para su utilización con el suministrador de servicio. Sustituirá a la identidad temporal actual TMUIs. Al igual que antes, TMUIn' es la «nueva» identidad de usuario temporal para su utilización con el operador de red.

CIPHs es una cadena de bits utilizada para proteger la nueva identidad temporal, TMUIs', mientras está en tránsito entre el suministrador de servicio y el usuario. Se calcula utilizando el algoritmo de ocultación de identidad Cu tomando como entrada de clave secreta Ksu y como entrada de la cadena de datos RNDu. Al igual que antes, CIPHn es una cadena de bits utilizada para proteger la nueva identidad temporal, TMUIn', mientras está en tránsito entre el operador de red y el usuario.

Al recibir el mensaje 4, el usuario puede calcular la clave secreta del operador de red, Knu, como a la salida el algoritmo de generación de clave del operador de red An cuando se tiene como entrada de la clave secreta Ksu y como entrada de la cadena de datos el desplazamiento de clave KO concatenado con la identidad del operador de red NOID (este mismo cálculo lo realiza el suministrador de servicio al recibir el mensaje 2).

Como antes, el usuario y el operador de red pueden calcular una clave de sesión Ks como la salida del algoritmo de generación de clave de sesión Ak cuando se tiene como entrada de clave secreta Knu y como entrada de cadena de datos la concatenación de RNDu, RNDn, y TMUIn'.

Obsérvese que como resultado de este mecanismo, el usuario y el operador de red compartirán la clave secreta Knu y una identidad temporal TMUIn'. Obsérvese igualmente que en el mecanismo descrito no se le informa automáticamente al operador de red de la IMUI de usuario. En caso de ser necesario por razones jurídicas y/o de explotación puede incluirse en el tercer mensaje del mecanismo de autenticación «nuevo registro».

Para el caso especial de autenticación unidireccional usuario a red y ocultación de identidad, no deben utilizarse los parámetros RNDu y RESn. Sin embargo, en este caso especial, los mensajes 3 y 4 deben cursar RNDs, la «pregunta» aleatoria generada por el suministrador de servicio, además de los indicados anteriormente. Además, CIPHs se calcula utilizando el algoritmo Cu tomando como entrada de clave secreta Ksu y como entrada de cadena de datos RNDs; CIPHn se determina mediante el algoritmo Cu tomando como entrada de clave secreta Knu y como entrada de cadena de datos RNDn.

1.4 Evaluación

El mecanismo tiene las siguientes características significativas.

1.4.1 Prestación del servicio de seguridad

El mecanismo de seguridad proporciona los servicios para los que se ha diseñado. Se han elaborado demostraciones de seguridad formales para dicho mecanismo. El establecimiento de funciones de verificación adecuadas es un procedimiento relativamente directo.

1.4.2 Taras de comunicaciones

Las dos versiones del esquema requieren tres y cinco mensajes respectivamente. Se trata del mínimo necesario para la autenticación mutua teniendo en cuenta que debe consultarse al suministrador de servicio y que no se utilizan marcas de tiempo (los otros dos servicios se proporcionan sin el requisito de ningún mensaje adicional). Los mensajes serán todos ellos relativamente breves.

1.4.3 Taras de administración

El mecanismo exige que las entidades almacenen preguntas aleatorias durante breves periodos de tiempo. También deberán almacenarse las identidades temporales y las claves. Es necesario que intervenga el suministrador de servicio; sin embargo esta intervención se limita a los casos en que un usuario desea hacer uso de un nuevo operador de red.

1.4.4 Procesamiento y otras taras de soporte físico

Todos los algoritmos criptográficos pueden ser sencillos de calcular.

1.4.5 Cumplimiento de normas internacionales

La versión de tres pases del mecanismo se adapta a la Norma ISO/CEI 9798-4: 1995 (siempre que los elementos de los mensajes figuren en el orden correcto).

1.4.6 Limitaciones en la utilización

El mecanismo utiliza únicamente funciones de verificación y no emplea operaciones de cifrado. Por consiguiente, es probable que las disposiciones para el transporte de los equipos que llevan a cabo este mecanismo a través de fronteras internacionales sean bastante sencillas. No se conocen restricciones en cuanto a licencias de patentes.

2 Mecanismo de autenticación unilateral basado en signaturas digitales

En este punto se describe un ejemplo de mecanismo de autenticación unilateral basado en el empleo de un esquema de signatura digital y un intercambio de pregunta-respuesta. Combina en un solo mecanismo la prestación de confidencialidad de la identidad de usuario y autenticación de la entidad unilateral.

2.1 Características proporcionadas

El mecanismo proporciona las siguientes características de seguridad:

– Autenticación de entidad unilateral del usuario al operador de red.

– Confidencialidad de la identidad de usuario en el trayecto de comunicaciones entre el usuario y el operador de red.

2.2 Requisitos iniciales

El mecanismo utiliza los siguientes algoritmos criptográficos:

– Algoritmo de signatura digital de usuario. Este algoritmo consistirá en dos transformaciones, la transformación de signatura S y la transformación de verificación V. La transformación de signatura tendrá como entrada una clave de signatura privada y una cadena de datos y como salidas una signatura SIG. La transformación de verificación tendrá como entrada una clave de verificación pública, una signatura SIG y una cadena de datos, y como salidas un valor binario (Sí/No) que indique si la entrada SIG es o no es una signatura válida para la cadena de datos de entrada.

El mecanismo utiliza los siguientes tipos de clave criptográfica:

– Clave de signatura privada de usuario, Ksigu. Se trata de claves privadas conocidas únicamente por un usuario. Estas claves privadas permanecen fijas durante largos periodos de tiempo y podrán utilizarse como entradas para la transformación de signatura de usuario S.

– Clave de verificación pública de usuario, Kpu. Se trata de claves públicas que pueden ser conocidas por diversos operadores de red y se utilizarán como entrada para la transformación de verificación pública V.

El mecanismo utiliza los siguientes tipos de identificadores:

– Identidad de usuario móvil internacional, IMUI. Se trata de una identidad permanentemente asociada a un usuario. La IMUI nunca pasa a través de la interfaz aérea evitando de esa forma su divulgación no autorizada.

– Identidad de usuario móvil temporal, TMUI. Esta identidad (temporal) se utiliza para identificar un usuario al operador de red con el que está actualmente registrado. Es conocida por el usuario y por el operador de red IMT-2000 de que se trate.

2.3 Descripción del mecanismo

Existen dos versiones del mecanismo dependiendo de que el usuario esté o no registrado con el operador de red. Se consideran los dos casos por separado.

2.3.1 Registros actuales

Se considera en primer lugar el caso en el que el usuario ya está registrado con el operador de red. Ello significa que el usuario y el operador de red compartirán una identidad temporal válida TMUI y el operador de red irá equipado con una copia de la clave de verificación pública de usuario Kpu. El mecanismo en este caso consiste en el intercambio de tres mensajes entre el usuario y el operador de red. El suministrador de servicio no interviene.

Los tres mensajes son los siguientes:

Mensaje 1:	Usuario	→	operador de red:	TMUI
Mensaje 2:	Operador de red	→	usuario:	RNDn
Mensaje 3:	Usuario	→	operador de red:	RNDu, RESu.

El valor RNDn es una «pregunta» aleatoria generada por el operador de red.

El valor RNDu es un número aleatorio generado por el usuario.

El valor RESu es una «respuesta a pregunta» generada por el usuario. RESu se calcula utilizando la transformación de signatura S, tomando como entrada de clave Ksigu y como entrada de la cadena de datos la concatenación de RNDn y RNDu.

Al recibir la TMUI del usuario, el operador de red genera de forma aleatoria el valor RNDn y lo almacena para su posterior verificación. El valor RNDn es enviado al usuario como segundo mensaje del mecanismo.

Al recibir RNDn del operador de red, el usuario genera aleatoriamente el valor RNDu. Los valores RNDn y RNDu se utilizan para generar RESu, que se envía al operador de red en el tercer mensaje del mecanismo.

Al recibir RESu el operador de red lo utiliza como la entrada SIG a la transformación de verificación V, utilizando como clave de entrada la concatenación de los valores almacenados de RESn y la RESu recibida que constituye la entrada de la cadena de datos. La salida de V se utilizará para determinar si el usuario es o no válido.

2.3.2 Nuevos registros

En segundo lugar se considera el caso en el que el usuario no está registrado con el operador de red. Ello significa que el usuario y el operador de red no comparten ninguna información. El mecanismo en este caso debe especificarse. A continuación se indican los requisitos para este mecanismo:

– El usuario y el operador de red deben disponer de una identidad de usuario temporal TMUI para habilitar al usuario e identificar por sí mismo al operador de red a través de la interfaz aérea sin comprometer el valor de su IMUI.

– Debe darse al operador de red una copia de la clave de verificación pública de usuario Kpu.

Idealmente deben cumplirse estos requisitos sin necesidad de transmitir la IMUI del usuario y/o un certificado de clave pública para el usuario a través de la interfaz aérea (a menos que esos valores estén cifrados de alguna forma).

2.4 Evaluación

El mecanismo tiene las siguientes características significativas.

2.4.1 Prestación del servicio de seguridad

El mecanismo de seguridad proporciona el servicio de autenticación para el que está diseñado. Sin embargo, la prestación de confidencialidad de la identidad de usuario es menos cierta. El mecanismo no contiene disposiciones para actualizar una TMUI; si se utiliza la misma TMUI de forma repetida, existe la posibilidad de que un interceptor pueda captar todo el tráfico perteneciente a un individuo. Ello podría comprometer parcialmente el servicio de confidencialidad de la identidad.

También hay un problema con la «inicialización» del esquema. Debe elaborarse un método para tratar los nuevos registros. Sin embargo no es un problema insuperable y puede diseñarse un nuevo mecanismo de registro utilizando una variante del esquema descrito en el punto siguiente.

Existe un cierto número de algoritmos de signatura digital adecuados. La presencia del segundo número aleatorio, Ru, en el ámbito de los cálculos de RESu significa que el usuario no tiene que proporcionar al operador de red la versión de signatura de la cadena de datos especificada completamente por el operador de red. Si se utiliza la misma clave de signatura para establecer signaturas de otros tipos de datos, ello puede suponer una amenaza para la seguridad. Si esta amenaza no existe, el número aleatorio RNDu puede hacerse nulo; es decir, puede elegirse de forma que tenga una longitud cero.

2.4.2 Taras de comunicaciones

El esquema requiere el envío de tres mensajes. De hecho con este número de mensajes puede diseñarse un mecanismo de autenticación mutua utilizando el método de pregunta-respuesta y, si lo inicia el operador de red, puede elaborarse fácilmente un esquema de autenticación unilateral que requiere únicamente dos mensajes. El servicio de confidencialidad de identidad se proporciona sin necesidad de ningún mensaje adicional. Todos los mensajes serán relativamente breves con la excepción del tercer mensaje; en dicho mensaje, el campo SIG puede contener normalmente entre 512 y 1 024 bits.

2.4.3 Taras de administración

El mecanismo exige que las entidades almacenen preguntas aleatorias durante breves periodos de tiempo. También será necesario almacenar las identidades temporales y las claves. En ese proceso debe intervenir el suministrador de servicio; sin embargo, esta intervención se limita a los casos en que el usuario desee hacer uso del nuevo operador de red.

Las claves para el algoritmo de signatura digital normalmente serán bastante largas (por ejemplo, 1 024 bits) comparadas con las de 64 a 128 bits para el algoritmo convencional.

2.4.4 Procesamiento y otras taras de soporte físico

Los cálculos de signatura y verificación pueden ser relativamente complejos; el grado exacto de complejidad dependerá del algoritmo y del tamaño de las claves utilizadas.

2.4.5 Cumplimiento de normas internacionales

El mecanismo cumple la Norma ISO/CEI 9798-3: 1993 (siempre que los elementos de los mensajes se agrupen en el orden correcto).

2.4.6 Limitaciones en la utilización

El mecanismo hace uso únicamente de una función de signatura digital y no utiliza operaciones de cifrado. Por consiguiente, es probable que las disposiciones para el transporte de los equipos que llevan a cabo este mecanismo a través de fronteras internacionales sean relativamente sencillas. No existen restricciones conocidas en cuanto a licencias de patentes en el propio mecanismo si bien algunos algoritmos de signatura digital están sujetos a patentes.

3 Mecanismo de autenticación unilateral basado en esquemas de clave pública

En este punto se describe un ejemplo de mecanismo de autenticación unilateral basado en la utilización de un esquema de signatura digital, un esquema de cifrado de clave pública, certificados de clave pública y marcas de tiempo. Combina en un solo mecanismo la confidencialidad de la identidad de usuario y la autenticación de entidad unilateral.

3.1 Características proporcionadas

El mecanismo proporciona las siguientes características de seguridad:

– Autenticación de la entidad unilateral del usuario al operador de red.

– Confidencialidad de la identidad de usuario en el trayecto de comunicaciones entre el usuario y el operador de red.

3.2 Requisitos iniciales

El mecanismo utiliza los siguientes algoritmos criptográficos:

– Algoritmo de signatura digital. Este algoritmo consistirá en dos transformaciones, la transformación de signatura S y la transformación de verificación V. La transformación de signatura tomará como entrada una clave de signatura privada y una cadena de datos y como salidas una signatura SIG. La transformación de verificación tomará como entrada una clave de verificación pública, una signatura SIG y una cadena de datos, y como salidas un valor binario (Sí/No) que indica si la entrada SIG es o no una signatura válida para la cadena de datos de entrada.

– Algoritmo de cifrado de clave pública. Este algoritmo consistirá en dos transformaciones, la transformación de cifrado E y la transformación de descifrado D. La transformación de cifrado tomará como entrada una clave de cifrado pública y una cadena de datos y como salidas una cadena de datos cifrada. La transformación de descifrado tomará como entrada una clave de descifrado privada y una cadena de datos cifrada y como salidas una cadena de datos de texto sin codificar (en claro).

El mecanismo utiliza los siguientes tipos de clave criptográfica:

– Clave de signatura privada de usuario, Ksigu. Se trata de una clave privada conocida únicamente por un usuario. Estas claves privadas permanecen fijas durante largos periodos de tiempo y se utilizarán como entrada a la transformación de signatura S.

– Clave de verificación pública de usuario Kpu. Se trata de claves públicas conocidas por el suministrador de servicio al usuario. Estas claves se utilizarán como entrada para la transformación de verificación V.

– Clave de signatura privada de suministrador de servicio, Kss. Se trata de una clave privada conocida únicamente por un suministrador de servicio. Estas claves privadas permanecen fijas durante largos periodos de tiempo y se utilizarán como entrada a la transformación de signatura S.

– Clave de verificación pública de suministrador de servicio, Kps. Se trata de una clave pública conocida por todos los operadores de redes que han concluido un acuerdo de prestación de servicio con un suministrador de servicio. Estas claves se utilizarán como entrada a la transformación de verificación V.

– Clave de descifrado privada del operador de red, Ksn. Se trata de claves privadas conocidas únicamente por un operador de red. Estas claves permanecen fijas durante largos periodos de tiempo y se utilizarán como entrada para la transformación de descifrado de la clave pública D.

– Clave de cifrado pública del operador de red, Kpn. Se trata de claves públicas conocidas por todos los usuarios que deseen hacer uso de un operador de red. Estas claves se utilizarán como entrada a la transformación de cifrado de la clave pública E.

El mecanismo hace uso de los siguientes tipos de identificadores:

– Identidad de usuario móvil internacional, IMUI. Se trata de una identidad permanentemente asociada a un usuario. La IMUI nunca pasa a través de la interfaz aérea evitando de esa forma su divulgación no autorizada.

– Identidad de usuario móvil temporal, TMUI. Esta identidad (temporal) se utiliza para identificar un usuario al operador de red en el que está actualmente registrado. Es conocida por el usuario y por los operadores de redes de las IMT-2000.

– Identidad del suministrador de servicio, SPID.

El mecanismo presenta el siguiente requisito adicional:

– Los usuarios, los operadores de redes y los suministradores de servicio deben tener los relojes sincronizados.

3.3 Descripción del mecanismo

Existe sólo una versión del mecanismo que se describe a continuación.

A diferencia del caso anterior, este mecanismo no exige que el usuario ya esté registrado con el operador de red. El mecanismo en este caso consta de un mensaje enviado por el usuario al operador de red. El suministrador de servicio no interviene. Sin embargo, es necesario cursar un certificado de clave pública del suministrador de servicio al usuario, en un momento determinado al inicio del proceso. En primer lugar se describe la forma del certificado antes de pasar a describir el propio mecanismo.

3.3.1 Certificados de clave pública

El certificado para un usuario, denominado CERTu, consiste en la concatenación de las siguientes cadenas de datos:

– la IMUI de usuario;

– la SPID;

– el instante de emisión;

– la vida útil del certificado;

– la clave de verificación pública de usuario Kpu;

– la salida de la transformación de signatura S cuando la entrada es la clave de signatura privada del suministrador de servicio y la cadena de datos consistente en la concatenación de IMUI, SPID, el tiempo de emisión, la vida útil del certificado y Kpu.

El usuario puede entonces proporcionar el certificado a cualquier operador de red, que puede utilizarlo para obtener una copia verificada de la clave pública del usuario, sin ninguna intervención por parte del suministrador de servicio del usuario.

3.3.2 Mecanismo de autenticación

El mensaje enviado por el usuario al operador de red es el siguiente:

– Usuario $\rightarrow$ operador de red: AUTH.

El valor AUTH es la salida de la transformación de cifrado de clave pública E cuando la entrada de clave es la clave de cifrado pública del operador de red Kpn y la entrada de la cadena de datos es la concatenación del certificado de usuario CERTu, una marca de tiempo actual Tu y el valor RESu.

El valor RESu se calcula como la salida de la transformación de signatura S tomando como entrada de clave la clave de signatura privada de usuario Ksigu y como entrada de la cadena de datos la marca de tiempos Tu.

La marca de tiempos Tu se genera a partir del reloj de usuario.

Al recibir AUTH del usuario, el operador de red en primer lugar la descifra utilizando la transformación de descifrado de clave pública con la clave de descifrado privada del operador de red Ksn. Con ello se obtendrá CERTu, Tu y RESu. A continuación el operador de red realiza las siguientes operaciones:

– Se verifica la marca de tiempos Tu para comprobar que es actual, es decir, que se encuentra dentro de la «ventana de aceptación».

– El operador de red utiliza la clave de verificación pública del suministrador de servicio Kps para verificar la signatura dentro del certificado. Si pasa la verificación, también se verifica el periodo de validez del certificado.

– Por último, se introduce el valor RESu en la transformación de verificación (como entrada de signatura), introduciendo como cadena de datos la marca de tiempos Tu y como clave la clave de verificación pública de usuario Kpu.

– Si todas las verificaciones tienen un resultado positivo y la transformación de verificación da como salida «Sí», se acepta al usuario.

3.3.3 Variante

Cabe señalar que cuando un usuario y un operador de red han utilizado el mecanismo anterior, puede simplificarse sustituyendo CERT por TMUI (suponiendo que el operador de red oculte la clave de verificación pública de usuario y la correspondiente TMUI). Con ello se ahorrará anchura de banda y se evitará una operación de verificación por parte del operador de red.

3.4 Evaluación

El mecanismo presenta las siguientes características significativas.

3.4.1 Prestación del servicio de seguridad

El mecanismo de seguridad proporciona los servicios de autenticación para los que está diseñado.

Existen un cierto número de algoritmos de signatura digital y cifrado de clave pública adecuados.

3.4.2 Taras de comunicaciones

El esquema exige que sólo se envíe un mensaje. Se trata evidentemente del mínimo necesario para la autenticación unilateral; el servicio de confidencialidad de la identidad se proporciona sin necesidad de ningún mensaje adicional. Todos los mensajes serán relativamente largos; el campo SIG en la cadena sin descifrar puede contener normalmente entre 512 y 1 024 bits y el funcionamiento de cifrado puede ampliar aún más el mensaje.

3.4.3 Taras de administración

El mecanismo exige que las entidades almacenen preguntas aleatorias durante breves periodos de tiempo. También será necesario que los usuarios y operadores de redes almacenen identidades temporales. No es preciso que el suministrador de servicio intervenga en estas acciones, salvo para la emisión de certificados a nuevos usuarios.

Las claves para los algoritmos asimétricos serán normalmente bastante largas (por ejemplo, 1 024 bits o más) en comparación con los 64 a 128 bits necesarios para un algoritmo convencional.

Los usuarios necesitarán almacenar claves de cifrado públicas para todos los operadores de redes con los que deban establecer comunicaciones. Cabe esperar que estas claves sean distribuidas a los usuarios por sus suministradores de servicio.

Los operadores de red deben almacenar las claves de verificación pública para todos los suministradores de servicio con los que hayan concluido un acuerdo de prestación de servicio.

Como se ha indicado anteriormente, es preciso que los usuarios, operadores de redes y suministradores de servicio tengan acceso a relojes sincronizados.

3.4.4 Procesamiento y otras taras de soporte físico

Los cálculos de signatura y verificación pueden ser relativamente complejos; el grado exacto de complejidad dependerá del algoritmo y del tamaño de las claves utilizadas. De forma similar, las operaciones de cifrado y descifrado de clave pública pueden ser también relativamente complicadas.

3.4.5 Cumplimiento de normas internacionales

El mecanismo puede cumplir la Norma ISO/CEI 9798-3: 1993 (siempre que los elementos del mensaje presenten el orden correcto); no es evidente que la norma permita el cifrado de los intercambios de autenticación (es un tema sujeto a interpretación).

3.4.6 Limitaciones en la utilización

El mecanismo utiliza un algoritmo de signatura digital y un algoritmo de cifrado de clave pública. Por consiguiente, como incorpora una función de cifrado, las disposiciones para el transporte de equipos que llevan a cabo este mecanismo a través de fronteras internacionales puede presentar cierta complicación. No se conocen restricciones de licencia de patentes en el propio mecanismo si bien algunos algoritmos de signatura digital y de cifrado de clave pública están sujetos a patentes.