(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 668 357**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/06 (2009.01)
H04W 12/04 (2009.01)
H04W 84/12 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **10.11.2004 PCT/EP2004/052909**

(87) Fecha y número de publicación internacional: **19.05.2005 WO05046157**

(96) Fecha de presentación y número de la solicitud europea: **10.11.2004 E 04804525 (6)**

(97) Fecha y número de publicación de la concesión europea: **28.03.2018 EP 1683324**

(54) Título: **Procedimiento para asegurar el tráfico de datos entre un primer aparato terminal y una primera red así como un segundo aparato terminal y una segunda red**

(30) Prioridad:

11.11.2003 DE 10352538
16.12.2003 DE 10358987

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.05.2018

(73) Titular/es:

SIEMENS AKTIENGESELLSCHAFT (100.0%)
WITTELSBACHERPLATZ 2
80333 MÜNCHEN, DE

(72) Inventor/es:

HORN, GÜNTHER

(74) Agente/Representante:

LOZANO GANDIA, José

PROCEDIMIENTO PARA ASEGURAR EL TRÁFICO DE DATOS ENTRE UN PRIMER APARATO TERMINAL Y UNA PRIMERA RED ASÍ COMO UN SEGUNDO APARATO TERMINAL Y UNA SEGUNDA RED

DESCRIPCIÓN

La invención se refiere a un procedimiento para asegurar el tráfico de datos entre un primer aparato terminal y una primera red, así como un segundo aparato terminal y una segunda red. Además se refiere la invención al correspondiente primer y al correspondiente segundo aparato terminal con los que puede realizarse el procedimiento de acuerdo con la invención.

Hoy en día existe para el usuario de un teléfono móvil la necesidad de lograr, a través de un acceso a red adecuado, no sólo un acceso a una red de telefonía móvil, sino también un acceso a otras redes, como por ejemplo Internet. En el acceso a Internet es especialmente deseable que los datos transmitidos no se muestren en el teléfono móvil, sino en otro aparato terminal, como por ejemplo un laptop.

Por el estado de la técnica se conocen procedimientos en los que un primer aparato terminal en forma de un teléfono móvil, que contiene un módulo SIM o USIM (SIM = Subscriber Identity Module, módulo de identidad de abonado; USIM = Universal Subscriber Identity Module, módulo universal de identidad de abonado) se conecta a través de una interfaz local con un segundo aparato terminal en forma de un laptop, haciendo posible el laptop un acceso a otra red, como por ejemplo una red WLAN, y/o Internet. El segundo aparato terminal se autentifica entonces en otra red mediante un protocolo de autentificación, utilizándose en el protocolo claves que recurren al módulo SIM y/o USIM. Como protocolos de autentificación adecuados se utilizan por ejemplo los protocolos EAP-SIM (EAP = Extensible Authentication Protocol, protocolo de autentificación adaptable; SIM = Subscriber Identity Module, módulo de identidad de abonado; ver documento [1]) o EAP-AKA (EAP = Extensible Authentication Protocol; AKA = Authentication Key Agreement, acuerdo de clave de autentificación; ver documento [2]). El protocolo EAP-SIM se utiliza al respecto para teléfonos móviles GSM y el protocolo EAP-AKA se utiliza para teléfonos móviles UMTS.

Los protocolos de autentificación EAP-SIM y EAP-AKA precisan por un lado de una comunicación con la red, así como por otro lado de la participación del módulo SIM o USIM en la autentificación. Por ello participan tanto el segundo aparato terminal como también el primer aparato terminal en la ejecución del protocolo de identificación. Así es necesario un intercambio de datos entre el segundo aparato terminal y el primer aparato terminal a través de una interfaz local, por ejemplo una interfaz Bluetooth. Entonces, para lograr la autentificación se transmiten a través de esta interfaz datos de autentificación, mediante un perfil adecuado. Por el estado de la técnica se conocen como perfiles adecuados en particular perfiles Bluetooth, como por ejemplo el Bluetooth SIM Access Profile (Perfil Bluetooth de Acceso a la SIM) (ver documento [3]). A través de la interfaz local se transmiten primeras claves de sesión, que sirven realmente para la comunicación del teléfono móvil con la correspondiente red de telefonía móvil. A partir de estas primeras claves de sesión se calculan a continuación en el segundo aparato terminal nuevas claves de sesión, con las que corre la autentificación mediante el protocolo de autentificación. Se ha comprobado que entonces es problemático que las primeras claves de sesión se conozcan en el segundo aparato terminal. Así tiene un atacante que consigue control sobre el segundo aparato terminal incluso acceso a las primeras claves de sesión y puede personificar al usuario del primer aparato terminal, pudiendo por ejemplo mantener el mismo conversaciones a costa del usuario en la primera red.

Por lo tanto es objetivo de la invención lograr un procedimiento para asegurar el tráfico de datos entre un primer aparato terminal y una primera red, así como un segundo aparato terminal y una segunda red que satisfaga elevadas exigencias de seguridad. En particular debe proteger el procedimiento frente al ataque antes descrito.

Este objetivo se logra mediante las reivindicaciones independientes. En las reivindicaciones dependientes se definen perfeccionamientos de la invención.

En el procedimiento de acuerdo con la invención se utiliza un primer aparato terminal, que con ayuda de una o varias primeras claves de sesión puede comunicar en una primera red, así como un segundo aparato terminal, que con ayuda de una o varias segundas claves de sesión puede comunicar en una segunda red. En el procedimiento se conecta el primer aparato terminal con el segundo aparato terminal a través de una interfaz local. En el primer aparato terminal se determinan la o las primera/s clave/s de sesión y se deducen la o las segunda/s clave/s de sesión a partir de las primeras claves de sesión. La o las segunda/s clave/s de sesión se transmiten a través de la interfaz local mediante un protocolo de seguridad al segundo aparato terminal. El segundo aparato terminal se autentifica finalmente en la segunda red con ayuda de la o de las segunda/s clave/s de sesión y/o con ayuda de claves derivadas de la o de las segunda/s clave/s de sesión mediante un protocolo de autentificación. El procedimiento de acuerdo con la invención se basa en la idea de no proporcionar al segundo aparato terminal la o las primera/s clave/s de sesión. Por ello funciones que realmente realiza el segundo aparato terminal, se desplazan al primer aparato terminal. En particular se deducen en el primer aparato terminal ya la o las

segunda/s clave/s de sesión a partir de las primeras claves de sesión. Así ya no puede un atacante que consigue control sobre el segundo aparato terminal acceder a las primeras claves de sesión, no logrando así acceso a la primera red.

En una variante preferida está configurado el protocolo de autentificación tal que como parte del protocolo se generan claves deducidas de la o de las segunda/s clave/s de sesión y se utilizan para proteger los mensajes del protocolo de autentificación y/o para proteger la comunicación en la segunda red.

La primera red es en una forma de realización una red GSM y la o las primera/s clave/s de sesión se generan entonces en un módulo SIM en el primer aparato terminal. En este caso el protocolo de autentificación es con preferencia un protocolo EAP-SIM (EAP = Extensible Authentication Protocol; SIM = Subscriber Identity Module). En una forma de realización alternativa la primera red es una red UMTS y la o las primera/s clave/s de sesión se generan en un módulo USIM (USIM = Universal Subscriber Identity Module) en el primer aparato terminal. En este caso es el protocolo de autentificación con preferencia EAP-AKA (EAP = Extensible Authentication Protocol; AKA = Authentication Key Agreement).

La interfaz local entre el primer y el segundo aparato terminal se realiza con preferencia a través de una interfaz inalámbrica. Al respecto procede en particular una interfaz de Bluetooth y/o interfaz de infrarrojos.

La segunda red, que en el procedimiento de acuerdo con la invención comunica con el segundo aparato terminal, es con preferencia una red local, en particular una red LAN y/o WLAN. La red local puede estar conectada a su vez con otras redes, como por ejemplo Internet.

En otra variante preferida de la invención, está configurado el protocolo de seguridad, con el que se intercambian informaciones entre el primer y el segundo aparato terminal, como sigue:

- se envía un primer mensaje de señalización desde el segundo aparato terminal al primer aparato terminal, activándose con el primer mensaje de señalización la deducción de la o de las segunda/s clave/s de sesión a partir de las primeras claves de sesión en el primer aparato terminal;
- como respuesta al primer mensaje de señalización, envía el primer aparato terminal un segundo mensaje de señalización al segundo aparato terminal, transmitiéndose con el segundo mensaje de señalización la o las segunda/s clave/s de sesión.

Así se transmiten de manera sencilla la o las segunda/s clave/s de sesión desde el primer aparato terminal al segundo aparato terminal. En una variante preferida se transmiten entonces con el primer mensaje de señalización parámetros del protocolo de autentificación. Con preferencia es el protocolo de seguridad un protocolo Bluetooth-SIM-Access-Profile ampliado, que contiene el primer y el segundo mensaje de señalización. En la descripción especial se definen las especificaciones y exigencias exactas a un tal protocolo ampliado.

Además del procedimiento de aseguramiento del tráfico de datos de acuerdo con la invención, incluye la invención un aparato terminal, que está configurado tal que puede utilizarse en el procedimiento de acuerdo con la invención como primer aparato terminal. El aparato terminal incluye al respecto con preferencia medios para determinar la o las primera/s clave/s de sesión y medios para deducir la o las segunda/s clave/s de sesión a partir de las primeras claves de sesión.

Además incluye la invención adicionalmente un aparato terminal, que está configurado tal que en el procedimiento de acuerdo con la invención puede utilizarse como segundo aparato terminal.

A continuación se describen en detalle ejemplos de realización de la invención en base al dibujo adjunto.

Se muestra en:

figura 1 a modo de ejemplo, un escenario en el que se utiliza el procedimiento de aseguramiento del tráfico de datos de acuerdo con la invención.

La figura 1 muestra un primer aparato terminal en forma de un teléfono móvil 1, que está conectado a través de una interfaz de Bluetooth local 3 con un segundo aparato terminal 4 en forma de un laptop 4. El segundo aparato terminal 4 está conectado a su vez a través de otra interfaz inalámbrica 5 con una segunda red 6, que en la figura 1 es una red WLAN. Para la autentificación en la red WLAN corre entre el laptop 4 y la red 6 un protocolo de autentificación. La red WLAN 6 está conectada a su vez con otra red 7, que por ejemplo es Internet. Igualmente está conectado el teléfono móvil 1 con una red de telefonía móvil 2, por ejemplo una red GSM o UMTS, a través de una interfaz de aire. El teléfono móvil se identifica en la red de telefonía móvil mediante un módulo de identidad, que en el caso de GSM es un módulo SIM y en el caso de UMTS es un módulo USIM. Para la comunicación del teléfono móvil con la red de telefonía móvil se utilizan una o varias primeras claves de sesión, que se generan en el módulo de identidad del teléfono

móvil. Análogamente se utilizan para la comunicación entre el laptop 4 y la red WLAN 6 una o varias segundas claves de sesión.

En el escenario de la figura 1 ha de posibilitarse a un usuario del teléfono móvil autentificarse en la red WLAN a través del laptop 4 con ayuda de la primera clave de sesión generada en el módulo de identidad del teléfono móvil. Para ello se deducen las segundas claves de sesión a partir de las primeras claves de sesión. Al respecto es problemático un ataque en el que el atacante consigue el control sobre el laptop 4, cuando las primeras claves de sesión se transmiten a través de la interfaz de Bluetooth 3 al laptop 4 y se deducen en el laptop. En este caso obtendría el atacante conocimiento de las primeras claves de sesión y podría por lo tanto personificar al usuario en la red de telefonía móvil 2. Para evitar tales ataques, no se deducen según el procedimiento de aseguramiento de datos de acuerdo con la invención las segundas claves de sesión en el laptop 4, sino ya en el teléfono móvil 1 a partir de las primeras claves de sesión. Las segundas claves de sesión deducidas se transmiten a continuación a través de la interfaz de Bluetooth 3 mediante un protocolo de seguridad al laptop, que con ayuda de estas segundas claves de sesión o con ayuda de otras claves deducidas de las segundas claves de sesión, realiza la autentificación en la red WLAN mediante el protocolo de autentificación. Así ya no están memorizadas las primeras claves de sesión en el laptop, con lo que un atacante que consigue el control sobre el laptop no tiene la posibilidad de establecer un enlace de telefonía móvil mediante la primera clave de sesión.

A continuación se describirá la invención en detalle en base a dos ejemplos de realización, considerándose en el primer ejemplo de realización como primer aparato terminal un teléfono móvil GSM con módulo SIM y en el segundo ejemplo de realización un teléfono móvil UMTS con módulo USIM.

En el primer ejemplo de realización se utiliza como protocolo de autentificación para la autentificación en la red WLAN el protocolo EAP-SIM conocido por el estado de la técnica (véase [1]). Se presupone que el módulo SIM del teléfono móvil sólo participa en una llamada "Full Authentication" (autentificación completa), (véase el documento [1], apartado 3) y no en una llamada "Re-Authentication" (re-autentificación) (véase el documento [1], apartado 4.3). El flujo exacto de mensajes del proceso de autentificación se describe en el apartado 3 del documento [1] (véase en particular la figura 1). Para la autentificación corren las siguientes etapas:

El teléfono móvil 1 recibe del laptop 4 la identidad del protocolo (EAP-SIM), dos o tres challenges (retos) GSM RAND, así como los parámetros "Identity"(identidad), "NONCE_MT", "Version List" (lista de versiones) y "Selected Version" (versión elegida). Los parámetros "Identity", "NONCE_MT", "Version List" y "Selected Version" se describen más en detalle en el documento [1]. El teléfono móvil retransmite uno tras otro cada RAND recibido en su módulo SIM. El siguiente RAND sólo puede retransmitirse al módulo SIM cuando ha tenido lugar la respuesta desde el módulo para el RAND anterior.

En el módulo SIM se ejecutan para cada RAND las siguientes funciones:

Ejecución de los algoritmos GSM A3/A8, tal como se describe en [4], es decir, deducción de una Response (respuesta) SRES y de una clave de sesión GSM Kc. Los parámetros SRES y Kc se transmiten desde el SIM al teléfono móvil. El teléfono móvil posee así tras finalizar la comunicación con el SIM dos o tres respuestas SRES y dos o tres claves de sesión Kc, según la cantidad de RAND recibidos. Las claves de sesión Kc son las primeras claves de sesión en el sentido de las reivindicaciones.

El teléfono móvil calcula a continuación la Master Key (clave maestra) MK EAP-SIM, tal como se describe en [1], apartado 4.6, según la siguiente fórmula (MK representa aquí una segunda clave de sesión en el sentido de las reivindicaciones):

MK = SHA1 (Identity| n*Kc| NONCE_MT | Version List | Selected Version)

y envía MK y las respuestas SRES al laptop.

En la fórmula anterior "|" significa encadenamiento. Identity significa la Peer-Identity (identidad de pares) de la cadena (string) sin el carácter cero al final. Se trata aquí de la identidad del atributo AT_IDENTITY del último paquete EAP-Response/SIM/Start (respuesta EAP/SIM/arranque) o, si no se ha utilizado ninguna AT_IDENTITY, de la identidad del paquete EAP-Response/Identity. La cadena de identidad se utiliza sin modificaciones e incluye la posible decoración de identidad. La notación n*KC designa los n valores Kc encadenados. Las claves Kc se utilizan en la misma secuencia que los challenges (retos) RAND en el atributo AT_RAND. NONCE_MT designa los valores NONCE_MT (no el atributo AT_NONCE_MT, sino sólo el valor NONCE). La "Version List" incluye números de versión de 2 bytes de la AT_VERSION_LIST, precisamente en la misma secuencia que en el atributo. La "Selected Version" es una versión de 2 bytes de AT_SELECTED_VERSION. Se utiliza el ordenamiento de bytes de la red, al igual que en los atributos. La función hash SHA-1 está especificada en [5]. Si se utilizan varios bucles

EPA/SIM/Start en un intercambio EAP/SIM, se utilizan los parámetros NONCE_MT, "Version List" y "Selected Version" del último bucle EAP/SIM/Start y se ignoran los bucles EAP/SIM/Start anteriores.

El laptop calcula entonces todas las otras claves a partir de MK, en particular las llamadas "session keys" (claves de sesión). El laptop realiza también la prueba "verifies AT_MAC" ("verificar AT_MAC") mostrada en la figura 1 en el apartado 3 del documento [1]. La deducción de claves para calcular MK a partir de las claves de sesión Kc es suficiente para impedir que el laptop pueda obtener conclusiones sobre las claves de sesión Kc.

Para transmitir los parámetros que se necesitan para calcular la Master Key (clave maestra) en el teléfono móvil 1, se utiliza un Bluetooth-SIM-Access-Profile ampliado. Para ello se amplía el mensaje "TRANSFER_APDU_REQ" utilizado en el SIM-Access-Profile existente en los parámetros "AuthProt", "EAP-Id", "NONCE_MT", "Version List" y "Selected Version". La transmisión del EAP-Id es opcional cuando el teléfono móvil puede deducir el EAP-Id a partir de datos propios. Además han de transmitirse dos o tres GSM-Challenges RAND. La transmisión de estos challenges (retos) ya se ha tenido en cuenta en el documento [3].

A continuación se definen más en detalle los parámetros utilizados en el Bluetooth SIM Access Profile ampliado:

Parámetro: AuthProt

Este parámetro muestra el protocolo de autentificación utilizado.
Longitud: 1 byte
Parámetro ID: Valores del parámetro, a definir mediante el Bluetooth Special Interest Group (grupo de interés especial Bluetooth) (SIG) (no esencial para la invención): valor EAP-SIM = 0x01

Parámetro: EAP-Id

Este parámetro contiene la identidad EAP del usuario utilizada en la deducción de la Master Key (identidad permanente o identidad de pseudónimo en el sentido de [1], apartado 4.6).
Longitud: variable
Parámetro ID: Valores del parámetro, a definir mediante el Bluetooth Special Interest Group) (SIG) (no esencial para la invención): Codificación adecuada de la identidad EAP (la codificación no es esencial para la invención)

Parámetro: "NONCE_MT"

Este parámetro contiene el valor NONCE_MT del EAP - Peer utilizado en la deducción de la master key (en el sentido de [1], apartado 4.6).
Longitud: 16 bytes
Parámetro ID: Valores del parámetro, a definir mediante el Bluetooth Special Interest Group (grupo de interés especial Bluetooth) (SIG) (no esencial para la invención): Codificación adecuada de NONCE_MT (la codificación no es esencial para la invención)

Parámetro: "Version List",

Este parámetro contiene la Version List utilizada en la deducción de la master key (en el sentido de [1], apartado 4.6).
Longitud: 2 bytes
Parámetro ID: Valores del parámetro, a definir mediante el Bluetooth Special Interest Group) (SIG) (no esencial para la invención): Codificación adecuada de Version List (la codificación no es esencial para la invención)

Parámetro: "Selected Version",

Este parámetro contiene la Selected Version del EAP-Peer utilizada en la deducción de la master key (en el sentido de [1], apartado 4.6).
Longitud: 2 bytes
Parámetro ID: Valores del parámetro, a definir mediante el Bluetooth Special Interest Group) (SIG) (no esencial para la invención): Codificación adecuada de Selected Version (la codificación no es esencial para la invención)

El mensaje "TRANSFER_APDU_ RESP" está incluido en la especificación actual del SIM Access Profile (ver [3], apartado 5.2). Este mensaje ha de ampliarse en el parámetro "MK". Además han de transmitirse dos o tres respuestas GSM SRES. La transmisión de las respuestas GSM ya se ha considerado en [3].

Parámetro: MK

Este parámetro contiene la master key calculada en el teléfono móvil según [1], apartado 4.6.
Longitud: 20 bytes.
Parámetro ID: Valores del parámetro, a definir mediante el Bluetooth Special Interest Group) (SIG) (no esencial para la invención): Codificación adecuada de la master key MK (la codificación no es esencial para la invención)

Cuando se utiliza un teléfono móvil UMTS, se utiliza como protocolo de autentificación para la autentificación en la red WLAN 6 el protocolo EAP-AKA conocido por el estado de la técnica (ver el documento [2]). La autentificación discurre entonces como en [2], apartado 3 (ver allí en particular la figura). Se supone que el módulo USIM y el teléfono móvil sólo toman parte en una "Full Authentication" (ver el documento [2], apartado 3) y no en una "Re-Authentication" (ver [2], apartado 4.2). El teléfono móvil realiza las siguientes funciones, describiéndose más en detalle los parámetros que se citan a continuación en el documento [2]:

El teléfono móvil recibe del laptop la identidad del protocolo (EAP-AKA), el Challenge (reto) AKA RAND|AUTN, así como el parámetro "Identity" y retransmite RAND y AUTN al módulo USIM. El parámetro "Identity" designa aquí la identidad utilizada por el usuario en EAP, como se describe más en detalle en [2], apartado 4.5.

En el USIM se realizan las siguientes funciones: Ejecución de los algoritmos UMTS f1 a f5 y f5*, tal como se describe en [6], en particular verificación de AUTN y MAC y deducción de la respuesta RES y de la clave de la sesión AKA CK e IK, que representan las primeras claves de sesión en el sentido de las reivindicaciones. Los parámetros RES, CK e IK se transfieren desde el módulo USIM al teléfono móvil.

El teléfono móvil calcula a continuación la clave maestra MK EAP-AKA, tal como se describe en [2], apartado 4.5, según la siguiente fórmula (MK representa aquí una segunda clave de sesión en el sentido de las reivindicaciones):

MK = SHA1 (Identity | IK | CK)

y envía MK y RES al laptop.

En la fórmula anterior "|" significa encadenamiento. Identity designa Peer-Identity-String (cadena de identidad de pares) sin el carácter cero al final. Esta identidad es la identidad del AT_IDENTITY Attribut del último paquete EAP-Response/AKA-Identity o, en el caso de que no se haya utilizado AT_IDENTITY, la identidad del paquete EAP-Response/Identity. El Identity-String se incluye sin modificaciones e incluye sólo la decoración de identidad posible. La función hash SHA-1 se especifica en [5].

El laptop calcula entonces todas las demás claves a partir de MK, en particular las “session keys” mencionadas en el apartado 3 de [2]. La deducción de claves para calcular MK a partir de CK e IK es suficiente para impedir que el laptop pueda deducir conclusiones sobre CK e IK.

Para transmitir los parámetros que se necesitan para calcular la master key en el teléfono móvil, se define un Bluetooth SIM Access Protocol ampliado, con el que se transmiten los parámetros a través de la interfaz de Bluetooth local. A continuación se definen más en detalle los parámetros utilizados en el Bluetooth SIM Access Profile ampliado:

El mensaje "TRANSFER_APDU_ REQ" está incluido en la especificación actual del SIM Access Profiles, véase [3], apartado 5.2. Este mensaje ha de ampliarse en los parámetros "AuthProt" y "EAP-Id". La transmisión del EAP-Id es opcional cuando el teléfono móvil puede deducir EAP-Id a partir de datos propios. Además ha de transmitirse el AKA-Challenge RAND|AUTN. La transmisión del AKA-Challenge ya se ha considerado en [3].

Parámetro: AuthProt

Este parámetro muestra el protocolo de autentificación utilizado.
Longitud: 1 byte
Parámetro ID: Valores del parámetro, a definir mediante el Bluetooth Special Interest Group) (SIG) (no esencial para la invención): EAP-AKA: valor = 0x00

Parámetro: EAP-Id

Este parámetro contiene la identidad EAP del usuario (permanent identity o pseudonym identity en el sentido de [2], apartado 4.5) utilizada en la deducción de la Master Key. Longitud: variable.
Parámetro ID: Valores del parámetro, a definir mediante el Bluetooth Special Interest Group) (SIG) (no esencial para la invención): Codificación adecuada de la identidad EAP (la codificación no es esencial para la invención)

El mensaje "TRANSFER_APDU_RESP" está contenido en la especificación actual del SIM Access Profiles, véase [3], apartado 5.2. Este mensaje ha de ampliarse en el parámetro "MK". Además ha de transmitirse la AKA response RES. La transmisión de la AKA response ya está considerada en [3].
.
Parámetro: MK

Este parámetro contiene la Master Key calculada en el teléfono móvil según [2], apartado 4.5.
Longitud: 20 bytes
Parámetro ID: Valores del parámetro, a definir mediante el Bluetooth Special Interest Group) (SIG) (no esencial para la invención): Codificación adecuada de la Master Key MK (la codificación no es esencial para la invención)

Bibliografía

[1] H. Haverinen, J. Salowey "EAP SIM Authentication" (autentificación EAP SIM), Internet Draft (documento preliminar de Internet), draft-haverinen-pppext-eap-sim-12, octubre 2003; http://www.ietf.org/internet-drafts/draft-haverinen-pppext-eap-sim-12.txt

[2] J. Arkko, H. Haverinen, "EAP AKA Authentication", Internet Draft, draft-arkko-pppext-eap-aka-11, octubre 2003; http://www.ietf.org/internet-drafts/draft-arkko-pppext-eap-aka-11.txt

[3] "SIM access via 'SIM Access Profile' and Bluetooth link" (Acceso SIM via "perfil de acceso SIM" y enlace Bluetooth), documento S3-030436 aportado al encuentro 3GPP SA3#29, San Francisco, 15 -18 julio 2003; ftp://ftp.3gpp.org/TSG_SA/WG3_Security/TSGS3_29_SanFran/Docs/ZIP/S3-030436.zip; redacción revisada de la Version 0.95VD_d, anexo att2

[4] GSM Technical Specification (especificación técnica) GSM 03.20 (ETSI TS 100 929): "Digital cellular telecommunication system (Phase 2+); Security related network functions" (sistema de telecomunicación celular digital (fase 2+; funciones de la red relacionadas con la seguridad), European Telecommunications Standards Institute (Instituto europeo de normativa de telecomunicaciones), julio 1999

[5] Federal Information Processing Standard (FIPS) (Estándares federales de procesamiento de la información), publicación 180-1, "Secure Hash Standard" (norma segura de Hash), National Institute of Standards and Technology (Instituto nacional de normas y tecnología), U.S. Department of Commerce, Abril 17, 1995

[6] 3GPP Technical Specification (especificación técnica) 3GPP TS 33.102 V5.3.0: "Technical Specification Group Services and System Aspects; 3G Security; Security Architecture (Release 5)" (Grupo de especificaciones técnicas, aspectos de servicio y del sistema; seguridad 3G, arquitectura de seguridad (5ª edición), 3rd Generation Partnership Project (Proyecto de colaboración de la tercera generación), septiembre 2003; ftp://ftp.3gpp.org/Specs/latest/Rel-5/33_series/

REIVINDICACIONES

1. Procedimiento para asegurar el tráfico de datos entre un primer aparato terminal (1) y una primera red (2), así como un segundo aparato terminal (4) y una segunda red (6), en el que el primer aparato terminal (1), con ayuda de una o varias primeras claves de sesión, no disponibles para el segundo aparato terminal, puede comunicar en una primera red (2) y el segundo aparato terminal (4), con ayuda de una o varias segundas claves de sesión, puede comunicar en una segunda red (6).
caracterizado por las siguientes etapas:
   - el primer aparato terminal (1) se conecta con el segundo aparato terminal (4) a través de una interfaz local (3):
   - en el primer aparato terminal (1) se determinan la o las primera/s clave/s de sesión y se deducen la o las segunda/s clave/s de sesión a partir de las primeras claves de sesión;
   - la o las segunda/s clave/s de sesión se transmiten a través de la interfaz local (3) mediante un protocolo de seguridad al segundo aparato terminal (4);
   - el segundo aparato terminal (4) se autentifica en la segunda red (6) con ayuda de la o de las segunda/s clave/s de sesión y/o con ayuda de claves derivadas de la o de las segunda/s clave/s de sesión mediante un protocolo de autentificación.

2. Procedimiento de acuerdo con la reivindicación 1,
en el que como parte del protocolo de autentificación, se generan las claves deducidas de la o de las segunda/s clave/s de sesión y se utilizan para proteger los mensajes del protocolo de autentificación y/o para proteger la comunicación en la segunda red.

3. Procedimiento de acuerdo con la reivindicación 1 ó 2,
en el que la primera red (2) es una red GSM y la o las primera/s clave/s de sesión se generan en un SIM (SIM = Subscriber Identity Module) en el primer aparato terminal (1).

4. Procedimiento de acuerdo con la reivindicación 3,
en el que el protocolo de autentificación es EAP-SIM (EAP = Extensible Authentication Protocol; SIM = Subscriber Identity Module).

5. Procedimiento de acuerdo con la reivindicación 1 ó 2,
en el que la primera red (1) es una red UMTS y la o las primera/s clave/s de sesión se generan en un módulo USIM (USIM = Universal Subscriber Identity Module) en el primer aparato terminal (1).

6. Procedimiento de acuerdo con la reivindicación 5,
en el que el protocolo de autentificación es EAP-AKA (EAP = Extensible Authentication Protocol; AKA = Authentication Key Agreement).

7. Procedimiento de acuerdo con una de las reivindicaciones precedentes,
en el que la interfaz local (3) es una interfaz inalámbrica, en particular una interfaz de Bluetooth y/o de infrarrojos.

8. Procedimiento de acuerdo con una de las reivindicaciones precedentes,
en el que una parte de la segunda red (6) es una red local, en particular una red LAN y/o WLAN.

9. Procedimiento de acuerdo con una de las reivindicaciones precedentes,
en el que el protocolo de seguridad está configurado tal que:
   - se envía un primer mensaje de señalización desde el segundo aparato terminal (4) al primer aparato terminal (1), activándose con el primer mensaje de señalización la deducción de la o de las segunda/s clave/s de sesión a partir de las primeras claves de sesión en el primer aparato terminal (1);
   - como respuesta al primer mensaje de señalización, envía el primer aparato terminal (1) un segundo mensaje de señalización al segundo aparato terminal (4), transmitiéndose con el segundo mensaje de señalización la o las segunda/s clave/s de sesión.

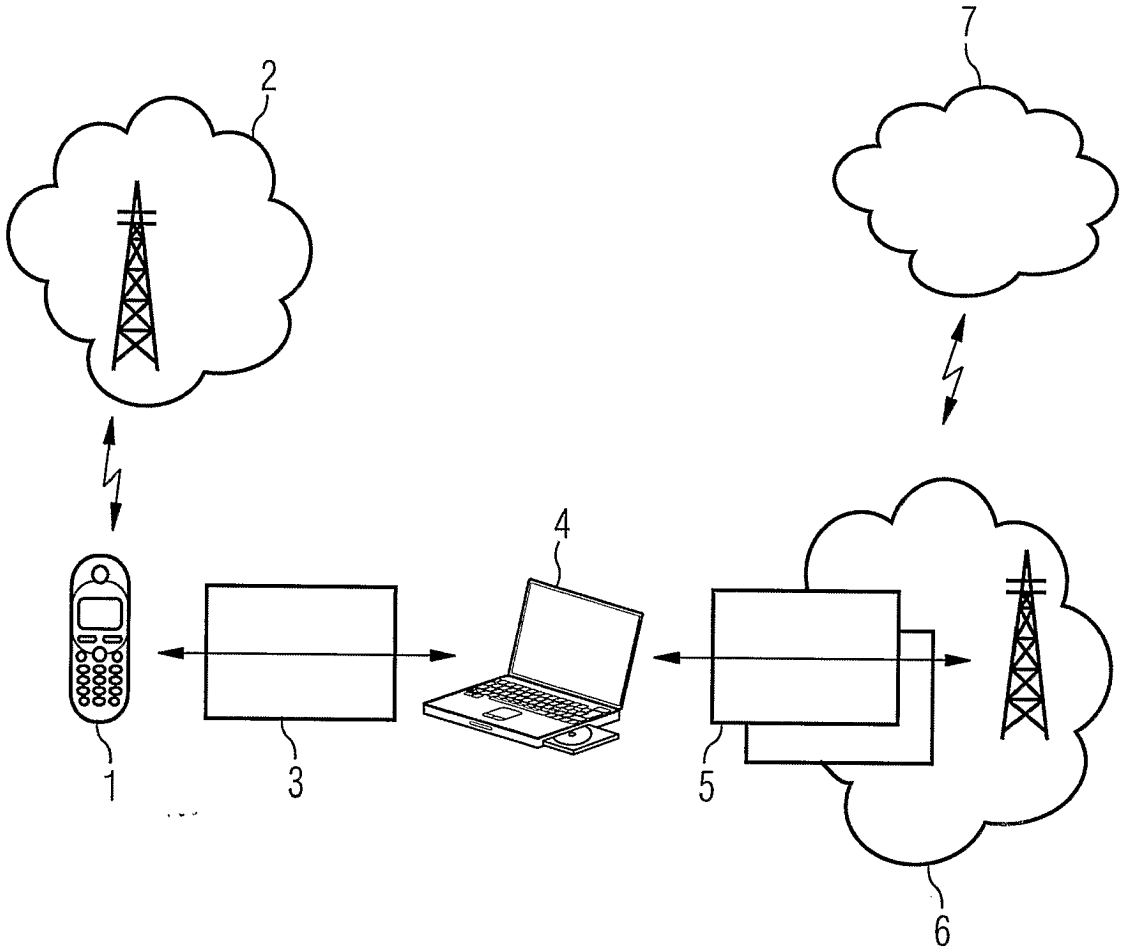
10. Procedimiento de acuerdo con una de las reivindicaciones precedentes,
en el que con el primer mensaje de señalización se transmiten parámetros del protocolo de autentificación.

11. Procedimiento de acuerdo con la reivindicación 9 ó 10,
en el que el protocolo de seguridad es un protocolo Bluetooth-SIM-Access-Profile ampliado, que contiene el primer y el segundo mensajes de señalización.

12. Aparato terminal, que está configurado tal que puede utilizarse en el procedimiento de acuerdo con una de las reivindicaciones precedentes como primer aparato terminal (1).

13. Aparato terminal de acuerdo con la reivindicación 12, tal que el aparato terminal presenta medios para determinar la o las primera/s clave/s de sesión y medios para deducir la o las segunda/s clave/s de sesión a partir de las primeras claves de sesión.

14. Aparato terminal, que está configurado tal que en el procedimiento de acuerdo con una de las reivindicaciones 1 a 11 puede utilizarse como segundo aparato terminal.


2
7
4
1
3
5
6