(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 426 747**

(51) Int. CI.:

H04W 12/00 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **28.09.2005 E 05021164 (8)**

(97) Fecha y número de publicación de la concesión europea: **26.06.2013 EP 1650994**

(54) Título: **Estación móvil y tarjeta de abonado aseguradas contra ataques desde redes inseguras**

(30) Prioridad:

21.10.2004 DE 102004051308

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.10.2013

(73) Titular/es:

GIESECKE & DEVRIENT GMBH (100.0%)
PRINZREGENTENSTRASSE 159
81677 MÜNCHEN, DE

(72) Inventor/es:

RANKL, WOLFGANG y
HORAK, MONIKA DR.

(74) Agente/Representante:

ARPE FERNÁNDEZ, Manuel

DESCRIPCIÓN

Estación móvil y tarjeta de abonado aseguradas contra ataques desde redes inseguras

La invención se refiere a una estación móvil, con un equipo terminal móvil y una tarjeta de abonado, en la que está prevista una protección contra ataques desde una red no segura (por ejemplo Internet) durante la recepción de datos desde la red no segura, así como a una tarjeta de abonado correspondiente.

Por equipo terminal móvil se entiende un aparato para la utilización de un sistema de radiotelefonía móvil en combinación con una tarjeta de abonado, por ejemplo un teléfono móvil, un *Smart Phone (teléfono inteligente)* o un PDA (Personal Data Assistant [agenda digital]) con función de teléfono móvil. El corazón de la tarjeta de abonado es el módulo de seguridad, que contiene datos de identidad, como por ejemplo el IMSI y la clave de autenticación Ki, que son específicos de la tarjeta de abonado y con ello indirectamente del usuario de la tarjeta de abonado o del equipo terminal móvil que se hace funcionar con la misma. En relación con la invención, la unidad de equipo terminal móvil y tarjeta de abonado se denomina estación móvil.

Con sistema de radiotelefonía móvil quiere indicarse un sistema global con una red de radiotelefonía móvil, un sistema de base y una pluralidad de estaciones móviles (compuestas de equipo terminal y tarjeta de abonado). A través de la red de radiotelefonía móvil se realiza la comunicación inalámbrica por medio de la estación móvil. En el sistema de base están registrados datos de identidad de los usuarios de todas las estaciones móviles o tarjetas de abonado. Durante el funcionamiento de un equipo terminal móvil con tarjeta de abonado en una red de radiotelefonía móvil, los datos de identidad que se hallan en el módulo de seguridad de la tarjeta de abonado se utilizan para autenticar la estación móvil o el equipo terminal móvil o la tarjeta de abonado frente a la red de radiotelefonía móvil o el sistema de base.

Como ejemplos de sistemas de radiotelefonía móvil pueden mencionarse: GSM (Global System for Mobile Communications [sistema mundial para comunicaciones móviles]), UMTS (Universal Mobile Telecommunications System [sistema de comunicaciones móviles universales]), IMT-2000 (International Mobile Communication 2000 [telecomunicaciones móviles internacionales]). En el sistema de radiotelefonía móvil GSM el módulo de seguridad se denomina SIM (SIM = Subscriber Identity Module [módulo de identidad de abonado]), y en el sistema de radiotelefonía móvil UMTS se denomina USIM (USIM = Universal SIM [módulo de identidad de abonado universal]). En estos casos, la tarjeta de abonado se denomina frecuentemente tarjeta SIM o tarjeta USIM.

Entretanto se ha hecho posible obtener con los equipos terminales móviles datos de diferentes redes, distintas de la red de radiotelefonía móvil. Por ejemplo pueden descargarse datos de Internet. A diferencia de la red de radiotelefonía móvil, por regla general tales redes no son dignas de confianza, ya que están controladas por una instancia que no es el operador del sistema de radiotelefonía móvil. Los datos pueden llevar acoplado un software de ataque peligroso, tal como por ejemplo virus informáticos o troyanos, que inevitablemente se acepta al aceptarse los datos. En relación con la invención, una red no segura se refiere a una red distinta de la red de radiotelefonía móvil y sobre la cual ejerce el control una instancia que no es el sistema de radiotelefonía móvil.

Para proteger los equipos terminales móviles contra ataques procedentes de redes no seguras, el equipo terminal tiene instalado un software de protección, tal como por ejemplo filtros de paquetes personales (*firewall (cortafuegos)* personales) y programas antivirus. Dado que el software de protección está implementado con libre acceso en el equipo terminal móvil, también está expuesto a ataques procedentes de redes no seguras, al igual que otras aplicaciones de software y datos que se hallen en el equipo terminal móvil o en la tarjeta de abonado que hayan de ser protegidos por el software de protección.

En las redes informáticas locales, como por ejemplo redes de empresas, frecuentemente está previsto un software con la función de un filtro de paquetes (*firewall [cortafuegos]*) para la protección de la red informática contra ataques procedentes de fuera de la misma. En un filtro de paquetes así (*firewall [cortauegos]*), todos los paquetes de datos entrantes desde el exterior en un sistema cerrado que se desea proteger se comprueban y, si es necesario, se filtran y en caso dado se rechazan. Otro software con la función de un mecanismo de protección para redes locales es un, así llamado, *Intrusion Detection System* (IDS) [sistema de detección de intrusión], que puede reconocer y en caso dado bloquea el software de ataque.

Por el documento DE 10300897 A1 se conoce un procedimiento para hacer funcionar un equipo terminal móvil con una tarjeta de abonado (tarjeta de telecomunicación) en un sistema de radiotelefonía móvil, en el que las llamadas entrantes en el equipo terminal se filtran mediante una función de comprobación instalada en la tarjeta de abonado. Por lo tanto, en este procedimiento es posible por ejemplo, en un teléfono móvil GSM/UMTS, eliminar las llamadas no deseadas filtrándolas mediante la tarjeta SIM/USIM. Así pues, el documento DE 10300897 A1 ofrece un procedimiento para filtrar llamadas dentro de la red de radiotelefonía móvil.

El documento EP 1420600 A1 describe una estación móvil con una tarjeta de abonado y un equipo terminal y un módulo de seguridad implementado en el equipo terminal con un dispositivo de protección para proteger la estación móvil contra ataques procedentes de una red no segura (red de teléfono móvil).

El documento WO 03/065654 A1 describe una estación móvil con un dispositivo de protección contra ataques procedentes de una red no segura (Internet) distinta de la red de radiotelefonía móvil, según el preámbulo de la reivindicación 1.

El objetivo de la invención es crear una estación móvil, con un equipo terminal móvil y una tarjeta de abonado, que ofrezca una protección segura y eficaz contra ataques procedentes de redes no seguras (por ejemplo Internet) distintas del sistema de radiotelefonía móvil y que se hallen bajo el control de una instancia que no sea el operador de radiotelefonía móvil.

El objetivo se logra mediante una estación móvil según la reivindicación 1.

La estación móvil según la reivindicación 1 presenta un equipo terminal móvil y una tarjeta de abonado que están configurados para hacer funcionar el equipo terminal con dicha tarjeta de abonado en un sistema de radiotelefonía móvil. Según la invención está implementado en el equipo terminal un módulo de seguridad que está bloqueado contra accesos desde el exterior del sistema de radiotelefonía móvil. El módulo de seguridad presenta a su vez un dispositivo de protección para proteger la estación móvil contra ataques procedentes de una red no segura distinta de la red de radiotelefonía móvil, dispositivo de protección con el que los datos entrantes en la estación móvil desde la red no segura pueden comprobarse y tratarse posteriormente en función del resultado de la comprobación. Según la invención, el equipo terminal incluye un microprograma *(firmware)*. El microprograma comprende diferentes funcionalidades, que por regla general sólo requiere el equipo terminal mismo. Por lo tanto, no es necesario que sea posible acceder al microprograma desde fuera de la estación móvil. Como es habitual en microprogramas, el microprograma tiene la característica de estar bloqueado contra accesos desde fuera de la estación móvil. Así pues, el dispositivo de protección está configurado de manera que una comunicación entre el equipo terminal y el módulo de seguridad pueda realizarse sólo por intermedio del microprograma del equipo terminal. Por consiguiente, el microprograma del equipo terminal adopta la función de un filtro adicional contra datos con ataques de software procedentes de redes no seguras.

Gracias a que el módulo de seguridad, y por lo tanto también el dispositivo de protección, está bloqueado contra accesos desde fuera del sistema de radiotelefonía móvil, el dispositivo de protección mismo está protegido contra ataques. Los datos que lleguen a la estación móvil desde redes no seguras, tales como por ejemplo Internet, no pueden acceder al módulo de seguridad. Por consiguiente, se impide un puenteo del dispositivo de protección mediante una manipulación indebida del dispositivo de protección mismo.

Así pues, según la reivindicación 1 se crea una estación móvil que ofrece una protección segura y eficaz contra ataques procedentes de redes no seguras (por ejemplo Internet) distintas del sistema de radiotelefonía móvil y que se hallen bajo el control de una instancia que no sea el operador de radiotelefonía móvil.

En la estación móvil, el dispositivo de protección está implementado opcionalmente en la tarjeta de abonado. En la tarjeta de abonado está implementada una SIM o USIM o similar como primer módulo de seguridad previsto para la telefonía móvil. Mediante el módulo de seguridad con el dispositivo de protección según la invención se crea un segundo módulo de seguridad dentro de la tarjeta de abonado.

Como alternativa, el módulo de seguridad según la invención está implementado en un soporte de datos (por ejemplo una *Smart Card [tarjeta inteligente]*) distinto de la tarjeta de abonado. El soporte de datos puede estar implementado de modo que pueda desmontarse del equipo terminal o esté fijo en el mismo. Un soporte de datos desmontable puede estar previsto por ejemplo, análogamente a la tarjeta de abonado (por ejemplo una tarjeta (U)SIM), en un dispositivo lector separado del equipo terminal, siempre que el equipo terminal tenga dos dispositivos lectores separados.

En el módulo de seguridad están implementadas además opcionalmente unas reglas de filtrado con las que los datos pueden ser comprobados por el dispositivo de protección.

Las reglas de filtrado son opcionalmente procesables, también opcionalmente por medio de la interfaz aérea del sistema de radiotelefonía móvil. El procesamiento puede comprender en particular una recarga de reglas de filtrado, una actualización de reglas de filtrado, un borrado de reglas de filtrado y similares.

Opcionalmente, en el módulo de seguridad están implementados, al menos, dos juegos de reglas de filtrado separados para diferentes usuarios de la estación móvil. Por ejemplo, para los padres pueden estar implementadas reglas de filtrado para padres que permitan una recepción más amplia de datos que las reglas de filtrado para niños, mediante las cuales se regula la recepción admisible de datos por parte de los hijos de los padres.

Los datos pueden procesarse opcionalmente de manera que se rechacen datos predeterminados. En particular se rechazan opcionalmente los datos que contravengan reglas de filtrado.

En la estación móvil, el módulo de seguridad está implementado opcionalmente, al menos en parte, en forma de aplicación de software, en particular en forma de aplicación de software en la tarjeta de abonado (por ejemplo una tarjeta (U)SIM). Además, en particular el dispositivo de protección puede estar implementado en forma de aplicación de software.

La función de protección puede estar configurada en concreto opcionalmente a modo de un filtro de paquetes (*firewall [cortafuegos]*), un programa antivirus o un *Intrusion Detection System* (IDS) [sistema de detección de intrusión], o presentar varias de las funcionalidades mencionadas.

Como red no segura puede estar prevista opcionalmente Internet.

Como alternativa o adicionalmente puede estar prevista como red no segura una red radioeléctrica de corto alcance, como en particular una RFID (Radio Frequency Identification [identificación por radiofrecuencia]), una NFC (Nearfield Communication [comunicación de campo cercano]), una WLAN (Wireless Local Area Network [red de área local inalámbrica]) y/o una IRDA (Infrared Data Association [asociación de datos por infrarrojos]).

A continuación se explica la invención más detalladamente por medio de ejemplos de realización y haciendo referencia a los dibujos, que muestran:

Figura 1 un diagrama que ilustra una entrada de datos en una estación móvil con un teléfono móvil y una tarjeta SIM desde una red no segura;

Figura 2 un diagrama que ilustra el filtrado de los datos de la figura 1 por un dispositivo de protección, que está implementado en la tarjeta SIM de la figura 1 en forma de aplicación de software.

La figura 1 muestra esquemáticamente una red no segura 10, aquí por ejemplo Internet, un teléfono móvil 20 y una tarjeta de abonado configurada como tarjeta SIM 30. Con vistas a una mayor claridad, la tarjeta SIM 30 se ha representado fuera del teléfono móvil 20 y agrandada. En realidad, la tarjeta SIM 30 se hace funcionar dentro del teléfono móvil 20. Con el teléfono móvil 20 se descargan datos 40 de la red 10. Los datos llegan al teléfono móvil 20 en primer lugar a través de una antena del teléfono móvil y un circuito acoplado a la misma. En el teléfono móvil 20, los datos 40 son recibidos y procesados ulteriormente por el microprograma 21 implementado en el teléfono móvil. Dado que los datos 40 son procesados por el microprograma 21, existe la seguridad de que los datos 40 serán transmitidos sólo a direcciones admisibles dentro de la estación móvil.

El procedimiento ulterior se explica por medio de la figura 2. El microprograma 21 transmite los datos a la tarjeta SIM 30, y dentro de ésta más concretamente a una aplicación de filtrado 31, implementada en la tarjeta SIM, mediante la cual se realiza el dispositivo de protección según la invención. La aplicación de filtrado 31 utiliza reglas de filtrado 32, que también están implementadas en la tarjeta SIM 30, para comprobar los datos 40 y si es necesario filtrarlos, es decir dejarlos pasar como máximo sólo en parte. La aplicación de filtrado 31 y las reglas de filtrado 32 están implementadas en un módulo de seguridad en la tarjeta SIM 30, que está separado del módulo de seguridad SIM previsto para la telefonía móvil propiamente dicho. En función de los datos 40, de la aplicación de filtrado 31 y de las reglas de filtrado 32, se rechazan de los datos 40 aquellos que contravienen reglas de filtrado 32. Los datos que satisfacen las reglas de filtrado 32 se dejan pasar como datos filtrados 40'. La aplicación de filtrado 31 está configurada opcionalmente para que cree y emita un protocolo de filtrado 33 sobre los procesos de filtrado realizados. El protocolo de filtrado 33 puede presentar por ejemplo información sobre los datos entrantes 40, los datos filtrados 40', los datos eliminados por el filtrado, las reglas de filtrado 32 que han infringido estos últimos, y similares. Opcionalmente se emite una notificación 34 para el usuario del teléfono móvil. La notificación 34 puede incluir por ejemplo la información de que se han eliminado datos mediante el filtrado. Opcionalmente, la notificación 34 incluye información detallada, en particular toda o parte de la información del protocolo de filtrado 33.

REIVINDICACIONES

1. Estación móvil que tiene:

- un equipo terminal móvil (20) y una tarjeta de abonado (30) configurados para hacer funcionar el equipo terminal (20) con dicha tarjeta de abonado (30) en un sistema de radiotelefonía móvil, y

- un módulo de seguridad implementado en el equipo terminal (20), bloqueado contra accesos desde fuera del sistema de radiotelefonía móvil y provisto de un dispositivo de protección (31) para proteger la estación móvil contra ataques procedentes de una red no segura (10) distinta de la red de radiotelefonía móvil, con cuyo dispositivo de protección (31), los datos (40) entrantes en la estación móvil desde la red no segura (10) distinta de la red de radiotelefonía móvil, pueden comprobarse y tratarse posteriormente en función del resultado de la comprobación,

caracterizada porque el equipo terminal (20) incluye un microprograma (21) que está bloqueado contra accesos desde fuera del sistema de radiotelefonía móvil, y estando configurado el módulo de seguridad, de manera que una comunicación entre el equipo terminal (20) y el módulo de seguridad puede realizarse sólo mediante intermedio del microprograma (21) del equipo terminal (20).

2. Estación móvil según la reivindicación 1, en la que el módulo de seguridad está implementado en la tarjeta de abonado (30).

3. Estación móvil según la reivindicación 1, en la que el módulo de seguridad está implementado en un soporte de datos distinto de la tarjeta de abonado (30), que está implementado de manera que puede desmontarse del equipo terminal o está fijo en el mismo.

4. Estación móvil según una de las reivindicaciones 1 a 3, en la que el módulo de seguridad está implementado, al menos en parte, en particular el dispositivo de protección (31), en forma de aplicación de software.

5. Estación móvil según una de las reivindicaciones 1 a 4, en la que en el módulo de seguridad están implementadas además unas reglas de filtrado (32) con las que los datos (40) pueden ser comprobados por el dispositivo de protección (31).

6. Estación móvil según la reivindicación 5, en la que las reglas de filtrado (32) pueden procesarse.

7. Estación móvil según la reivindicación 6, en la que las reglas de filtrado (32) pueden procesarse por medio de la interfaz aérea del sistema de radiotelefonía móvil.

8. Estación móvil según una de las reivindicaciones 5 a 7, en la que en el módulo de seguridad están implementados al menos dos juegos distintos de reglas de filtrado (32) para diferentes usuarios de la estación móvil.

9. Estación móvil según una de las reivindicaciones 1 a 8, en la que los datos (40) pueden procesarse de manera que se rechacen datos (40) predeterminados, en particular datos (40) que contravengan reglas de filtrado (32).

10. Estación móvil según una de las reivindicaciones 1 a 9, en la que como red no segura (10) está prevista Internet.

11. Estación móvil según una de las reivindicaciones 1 a 10, en la que como red no segura (10) está prevista una red radioeléctrica de corto alcance, como en particular RFID, WLAN y/o IRDA.

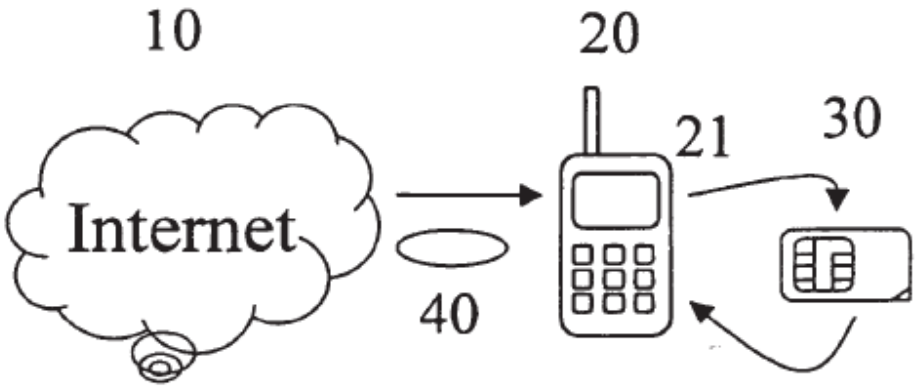

Fig. 1

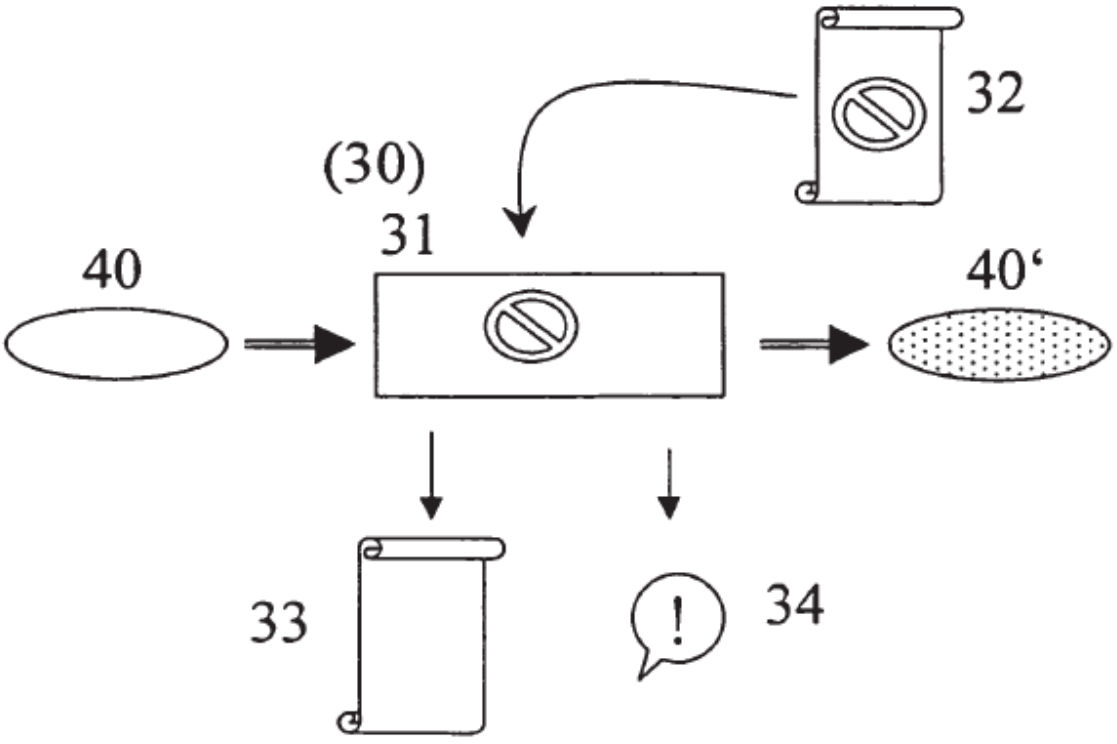

Fig. 2

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

La lista de referencias citada por el solicitante lo es solamente para utilidad del lector, no formando parte de los documentos de patente europeos. Aún cuando las referencias han sido cuidadosamente recopiladas, no pueden excluirse errores u omisiones y la OEP rechaza toda responsabilidad a este respecto.

Documentos de patente citados en la descripción

- DE 10300897 A1 **[0008]**
- EP 1420600 A1 **[0009]**
- WO 03065654 A1 **[0010]**