(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 278 271**

(51) Int. Cl.:
H04Q 7/32 (2006.01)
G07F 7/10 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **04076715 .4**
(86) Fecha de presentación : **11.06.2004**
(87) Número de publicación de la solicitud: **1492366**
(87) Fecha de publicación de la solicitud: **29.12.2004**

(54) Título: **Sistema que permite asegurar datos transmitidos por medio de teléfonos móviles programables con intermedio de una red de telefonía móvil.**

(30) Prioridad: **11.06.2003 FR 03 06985**

(45) Fecha de publicación de la mención BOPI:
01.08.2007

(45) Fecha de la publicación del folleto de la patente:
01.08.2007

(73) Titular/es:
Ercom Engineering Réseaux Communications
13, avenue Morane Saulnier
78140 Vélizy-Villacoublay, FR

(72) Inventor/es: **Laubacher, Eric**

(74) Agente: **Durán Moya, Carlos**

DESCRIPCIÓN

Sistema que permite asegurar datos trasmitidos por medio de teléfonos móviles programables con intermedio de una red de telefonía móvil.

Sector técnico al que pertenece la invención

La presente invención se refiere a un sistema que permite asegurar datos transmitidos por medio de un terminal de tipo teléfono móvil programable con intermedio de una red de telefonía móvil en tiempo real, obteniéndose el aseguramiento de los datos a proteger gracias a la realización de un criptófono integrado en el terminal.

Estado de la técnica

El documento FR 2812419 describe una tarjeta de usuario con microprocesador, que contiene varias aplicaciones internas en un terminal. Un procedimiento asegura el acceso de una aplicación externa a dicha tarjeta. La realización de un criptófono integrado en el terminal portátil necesita tradicionalmente o bien la modificación del terminal portátil o bien la adición de un módulo material adicional.

En los dos casos ello hace la realización del terminal dotado de un criptáfono especialmente difícil, y en la práctica está reservado al fabricante del terminal portátil.

Por esta razón, la compatibilidad con otras terminales portátiles y la continuidad son difíciles de asegurar, teniendo en cuentas que el mercado de la criptofonía es insignificante con respecto al mercado de terminales portátiles.

Por otra parte, la añadidura de un módulo físico adicional aumenta notablemente el peso del terminal portátil, atrae la atención sobre el usuario y hace más difícil la utilización del terminal portátil.

Finalmente se debe observar que es conocido el codificar la comunicación entre un terminal y la red, pero, por una parte, esta codificación o encriptado no asegura la seguridad de la comunicación entre dos terminales y, por otra parte, la codificación utilizada puede ser insatisfactoria para el usuario del terminal.

En oposición, un criptófono es un dispositivo que permite el encriptado o codificación de una comunicación de “extremo a extremo” es decir, de un terminal a otro con intermedio de la red.

Objeto de la invención

La presente invención está destinada a solucionar por lo menos uno de los inconvenientes anteriormente mencionados. Resulta de la comprobación que la nueva generación de teléfonos programables da la oportunidad de realizar un criptófono lógico portátil en una gran variedad de terminales.

La invención resulta también de la comprobación de que un enfoque puramente lógico de la criptofonía no es satisfactorio desde el punto de vista de seguridad, en especial por la ausencia de generador aleatorio de buena calidad, de protección contra la descodificación y contra el acceso a los elementos secretos, y ello a pesar del reducido coste de producción de un criptófono lógico de este tipo.

Es por ello que la invención se refiere a un sistema que permite asegurar datos confidenciales transmitidos por medio de teléfonos móviles programables con intermedio de una red de telefonía móvil. Los datos confidenciales se presentan en especial en forma de informaciones multimedia, tales como tipo de voz, telecopia, imagen y/o video. Los teléfonos móviles programables de acuerdo con la invención se caracterizan porque comprenden:

- una aplicación lógica de criptofonía,
- un módulo de seguridad que comprende algoritmos de criptografía.

Este módulo de seguridad se caracteriza porque presenta:

- informaciones secretas memorizadas,
- un módulo lógico específico.

El módulo lógico específico está destinado en especial a:

- generar y transmitir a la aplicación lógica de criptofonía claves de sesión destinadas al cifrado y/o sellado de las informaciones confidenciales y/o
- autentificar los teléfonos móviles programables y/o
- cifrar las informaciones confidenciales sin comunicar claves de sesión a la aplicación de criptofonía.

La invención permite por lo tanto realizar un criptófono integrado a un terminal portátil y programable, garantizando un alto nivel de seguridad, puesto que utiliza elementos físicos (hardware) dedicados a la seguridad y, además, con un coste reducido, puesto que utiliza elementos físicos (hardware) ya fabricados en gran cantidad para el mercado de la telefonía móvil.

La invención consiste en utilizar una aplicación a medida introducida en el módulo de seguridad del terminal portátil, utilizándose dicha aplicación a medida por una aplicación de criptofonía instalada en el terminal portátil programable.

De este modo, se obtiene un alto nivel de seguridad con ayuda de algoritmos tradicionales de criptografía facilitados por el módulo de seguridad y utilizables por la aplicación a medida, y por el almacenamiento de los elementos secretos necesarios para aplicación a medida en el módulo de seguridad.

Según casos particulares de realización, la aportación de la aplicación a medida a la seguridad global del sistema puede consistir en:

- realizar la generación de claves de sesión para el cifrado y/o sellado de las informaciones, pudiendo ser facilitadas estas claves de sesión a la aplicación de criptofonía,
- de manera complementaria asegurar la autentificación de los terminales, es decir, indirectamente la autentificación de los usuarios,
- de forma complementaria realizar el cifrado del flujo de información, sin necesidad de comunicación de claves de sesión a la aplicación de criptofonía.

En una realización, el módulo de seguridad es una tarjeta inteligente.

Según una realización, la tarjeta inteligente está destinada a identificar el usuario y/o el terminal.

En una realización la tarjeta inteligente dispone de un aparato virtual Java.

Según una realización, el módulo lógico específico es un applet.

En una realización las informaciones secretas memorizadas comprenden claves privadas de autentificación.

La invención se refiere también a una tarjeta inteligente destinada al aseguramiento de los datos confidenciales transmitidos por medios de teléfonos móviles programables con intermedio de una red de telefonía móvil, presentándose los datos confidenciales en especial en forma de informaciones multimedia, tales como voz, telecopia, imagen o video, comprendiendo dicha tarjeta inteligente algoritmos de criptografía que presentan:

- informaciones secretas memorizadas
- un módulo lógico específico

El módulo lógico específico está destinado especialmente a trabajar con una aplicación lógica de criptofonía comprendida en un terminal móvil programable para:

- generar y transmitir a la aplicación lógica de criptofonía claves de sesión destinadas al cifrado y/o sellado de las informaciones confidenciales y/o
- autentificar los teléfonos móviles programables y/o
- cifrar las informaciones confidenciales sin comunicar claves de sesión a la aplicación de criptofonía.

La invención se refiere igualmente a un terminal móvil programable destinado a la transmisión segura de datos confidenciales con intermedio de una red de telefonía móvil, presentándose los datos confidenciales en especial en forma de informaciones multimedia tales como voz, telecopia, imagen o video, comportando este terminal móvil programable:

- una aplicación lógica de criptofonía,
- una tarjeta inteligente de acuerdo con la reivindicación 8.

La invención se refiere además a un procedimiento destinado a asegurar tratos confidenciales transmitidos por medio de teléfonos móviles programables por medio de una red de telefonía móvil, presentándose los datos confidenciales en especial en forma de informaciones multimedia, tales como voz, telecopia, imagen o video, comportando los teléfonos móviles programables:

- una aplicación lógica de criptofonía,

- un módulo de seguridad que comprende algoritmos de criptografía que presentan:

- informaciones secretas memorizadas,

- un módulo lógico específico

El módulo lógico específico está destinado especialmente a:

- generar y transmitir a la aplicación lógica de criptofonía claves de sesión destinadas al cifrado y/o sellado de las informaciones confidenciales y/o

- autentificar los teléfonos móviles programables y/

- cifrar las informaciones confidenciales sin comunicar claves de sesión a la aplicación de criptofonia.

Finalmente la invención se refiere a datos confidenciales transmitidos por medio de teléfonos móviles programables con intermedio de una red de telefonía móvil, presentándose estos datos confidenciales, en especial, en forma de informaciones multimedia tales como voz, telecopia, imagen o video, transmitiendo los teléfonos móviles programables estos datos según un procedimiento de acuerdo con la invención.

Otras características y ventajas de la invención aparecerán de la descripción de una realización de la invención efectuada a continuación, a título ilustrativo y no limitativo, con ayuda de la figura 1 que se adjunta, que representa esquemáticamente una forma de puesta en práctica de la invención.

En la figura 1 el procedimiento utiliza un terminal programable de tipo teléfono portátil (1), que dispone de un entorno de programación (2) en el que se ejecuta la aplicación de criptofonía (3) y que contiene una tarjeta SIM (4) que por su parte está dotada de un entorno de programación (5), en el que se ejecuta una aplicación lógica a medida o "applet" (6).

Un teléfono de este tipo puede transmitir, por lo tanto, recepción o emisión, datos confidenciales del tipo de voz, telecopia, imagen o video, codificados en tiempo real por medio de su criptófono.

A este efecto el applet (6) utiliza los medios criptográficos del módulo de seguridad, es decir, de la tarjeta SIM (4) para utilizar por lo menos un algoritmo de criptografía e informaciones secretas memorizadas, tales como claves privadas de autentificación.

Según casos particulares de realización, la contribución de la aplicación a medida ("applet") a la seguridad global del sistema puede consistir en:

- realizar la generación de las claves de sesión para el cifrado y/o sellado de las informaciones, pudiendo ser facilitadas estas claves de sesión a la aplicación de criptofonía,

- de manera complementaria, asegurar la autentificación de los terminales, es decir, indirectamente a la autentificación de los usuarios,

- de forma complementaria realizar el cifrado de flujo de información sin necesidad de comunicación de claves de sesión a la aplicación de criptofonía.

El procedimiento según la invención está por lo tanto destinado particularmente a la protección de conversaciones telefónicas gubernamentales y de altas personalidades con respecto al riesgo de interceptación por adversarios poderosos.

Es conveniente igualmente para la protección de trasmisiones de datos y de telecopias realizadas por medio de terminales programables portátiles, así como por redes de transmisión por paquetes.

Es conveniente observar que la presente invención es susceptible de numerosas variantes, debiéndose comprender que puede ser puesta en práctica ventajosamente en todo tipo de medio de comunicación dotado de una tarjeta inteligente del tipo de una tarjeta SIM.

REIVINDICACIONES

1. Sistema destinado a la seguridad de datos confidenciales transmitidos por medio de teléfonos móviles (1) programables con intermedio de una red de telefonía móvil, presentándose los datos confidenciales en especial en forma de informaciones de tipo voz o telecopia, comportando los teléfonos móviles programables:

- una aplicación lógica (3) de criptofonía,
- un módulo (4) de seguridad que comprende algoritmos de criptografía que presentan:
- medios de almacenamiento de elementos secretos,
- un módulo lógico específico (6).

Comportando el módulo lógico:

- medios para generar y transmitir a la aplicación lógica de criptofonía claves de sesión destinadas al cifrado y/o sellado de las informaciones confidenciales y/o,
- medios para autentificar los teléfonos móviles programables y/o
- medios para cifrar las informaciones confidenciales sin comunicar claves de sesión a la aplicación de criptofonía.

2.Sistema, según la reivindicación 1, en el que los datos confidenciales se presentan en forma de informaciones multimedia tales como imagen y/o video.

3. Sistema, según la reivindicación 1 ó 2, **caracterizado** porque el módulo de seguridad (4) es una tarjeta inteligente.

4. Sistema, según la reivindicación 3, **caracterizado** porque la tarjeta inteligente (4) está destinada a identificar al usuario del terminal y/o el terminal.

5. Sistema, según la reivindicación 4, **caracterizado** porque la tarjeta inteligente (4) dispone de un aparato virtual Java.

6. Sistema, según una de las reivindicaciones anteriores, **caracterizado** porque el módulo lógico (6) específico es un applet.

7. Sistema, según una de las reivindicaciones anteriores, **caracterizado** porque las informaciones secretas memorizadas comprenden claves privadas de autentificación.

8. Tarjeta inteligente (4) destinada a la seguridad de los datos confidenciales transmitidos por medio de teléfonos móviles programables (1) con intermedio de una red de telefonía móvil, presentándose los datos confidenciales especialmente en forma de informaciones de tipo voz o telecopia, imagen o video, comprendiendo esta tarjeta inteligente logaritmos de criptografía que presentan:

- medios de almacenamiento de elementos secretos,
- un módulo lógico específico (6),

estando destinado el módulo lógico específico (6) a trabajar con una aplicación lógica de criptofonía comprendida en un terminal móvil programable y que presenta medios para:

- generar y transmitir a la aplicación lógica de criptofonía claves de sesión destinadas al cifrado y/o al sellado de las informaciones confidenciales y/o
- autentificar los teléfonos móviles programables y/o
- cifrar las informaciones confidenciales sin comunicar las claves de sesión en la aplicación de criptofonía.

9. Tarjeta inteligente, según la reivindicación 8, en la que los datos confidenciales se presentan en forma de informaciones multimedia tales como imagen y/o video.

10. Terminal móvil programable (1) destinado a la transmisión segura de datos confidenciales con intermedio de una red de telefonía móvil, presentándose los datos confidenciales en especial en forma de informaciones de voz o de telecopia, comportando este terminal móvil programable:

- una aplicación lógica de criptofonía,

- una tarjeta inteligente (4) según la reivindicación 8 ó 9.

11. Terminal móvil, según la reivindicación 10, en el que los datos confidenciales se presentan en forma de informaciones multimedia tales como imagen y/o video.

12. Procedimiento destinado a la seguridad de datos confidenciales transmitidos por medio de teléfonos móviles programables (1) con intermedio de una red de telefonía móvil, presentándose los datos confidenciales en especial en forma de informaciones de tipo voz o telecopia, comportando los teléfonos móviles programables:

- una aplicación lógica de criptofonía,

- un módulo de seguridad (4) que comprende algoritmos de criptografía que comprenden:

    - medios de almacenamiento de elementos secretos,

    - un módulo lógico específico (6),

estando destinado el módulo lógico específico (6) a:

- generar y transmitir a la aplicación lógica de criptofonía claves de sesión destinadas al cifrado y/o sellado de las informaciones confidenciales y/o

- autentificar los teléfonos móviles programables y/o

- cifrar las informaciones confidenciales sin comunicar claves de sesión a la aplicación de criptofonía.

13. Procedimiento, según la reivindicación 12, en el que los datos confidenciales se presentan en forma de informaciones multimedia tales como imágenes y/o video.

FIG_1