(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 528 916**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **29.09.2010 E 10759662 (9)**

(97) Fecha y número de publicación de la concesión europea: **27.08.2014 EP 2484078**

(54) Título: **Procedimiento para asegurar la ejecución de una aplicación NFC instalada en un elemento seguro que forma parte de un terminal móvil**

(30) Prioridad:

30.09.2009 EP 09305920

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.02.2015

(73) Titular/es:

GEMALTO SA (100.0%)
6, rue de la Verrerie
92190 Meudon, FR

(72) Inventor/es:

AMIEL, PATRICE;
POUJOL, STÉPHANE;
MARTIN, MICHEL RENÉ y
BERNABEU, GIL

(74) Agente/Representante:

ISERN CUYAS, María Luisa

DESCRIPCIÓN

Procedimiento para asegurar la ejecución de una aplicación NFC instalada en un elemento seguro que forma parte de un terminal móvil.

El campo de la invención es el de las telecomunicaciones por los dispositivos móviles y más precisamente un método para asegurar la ejecución de una aplicación de la tecnología NFC (Near Field Communication en Inglés, Communication par champú proche en francés) instalada en un elemento seguro que forma parte de un terminal móvil.

Una aplicación NFC es un programa que permite intercambiar datos entre dos entidades remotas por escasos centímetros. Esta aplicación permite por ejemplo a un titular de un terminal móvil, de tipo GSM por ejemplo, realizar una transacción (de pago) a un comerciante.

Un terminal móvil comprende convencionalmente un elemento de seguridad, tal como una tarjeta extraíble SIM o USIM que permite autentificar la red de telecomunicaciones.

Si un suscriptor desea poder pagar a través de la NFC o, en general, utilizar un servicio NFC utilizando su teléfono móvil, una aplicación *ad-hoc* se debe instalar en la tarjeta (U)SIM del terminal móvil. Esta instalación se realiza generalmente a través de OTA, es decir que el operador, tras haber verificado con la entidad bancaria del abonado, o más generalmente con el proveedor de los servicios NFC, que esté autorizado a realizar dichas transacciones (que no tiene, por ejemplo, una prohibición del banco), descargar a través de OTA una aplicación m-NFC (m significa que la aplicación NFC está destinada a un terminal móvil) en la tarjeta (U)SIM del abonado. Tras esta descarga, la iniciación de la aplicación permite al abonado realizar transacciones NFC.

Cada tarjeta (U)SIM es única y bajo la propiedad del operador que tiene una capacidad directa de comunicación OTA segura con la tarjeta. Además, no es posible duplicar una tarjeta (U)SIM. Por lo tanto, el operador tiene la certeza de que la aplicación m-NFC descargada lo ha sido en la tarjeta (U)SIM de su abonado, y que el servicio m-NFC no se puede duplicar de forma no autorizada en otra tarjeta del mismo o de otro abonado.

Recientemente han aparecido terminales móviles que incorporan de manera forma permanente o temporal elementos de seguridad adicionales. Estos elementos de seguridad son tarjetas de multi-aplicación que se sueldan en los terminales (llamados ESE - Embedded Secure Element en Inglés - Elément sécurisé intégré en francés) o tarjetas de multi-aplicación que son insertables/extraíbles de los terminales (llamados SMC - Secure Memory Card en Inglés - Carte mémoire sécurisée en francés).

Un ESE o un SMC no tiene capacidad OTA "nativa" y no está bajo el control del operador de red. Sin embargo, el operador puede almacenar datos a través de OTA apoyándose en los mecanismos de comunicación nativos del terminal móvil, pero estos mecanismos no utilizar la tarjeta (U)SIM. Por tanto, es posible para el MNO la instalación vía OTA - en un ESE o un SMC - de aplicaciones m-NFC similares a las instaladas en una (U)SIM. Sin embargo, esta instalación se realiza a través de un canal de comunicación que no está bajo el control del operador, en un elemento de seguridad que no pertenece al operador, cuyo elemento está contenido en un terminal que no está controlado por el operador.

El problema de usar una ESE es el siguiente: cuando el abonado suscribe un abono a una m-NFC, la aplicación NFC-m se descarga a través de OTA en el ESE (y no en la tarjeta extraíble (U)SIM). El terminal del abonado, llamado terminal 1, incorpora entonces la aplicación m-NFC. El abonado podría entonces, con ánimo de estafar a su operador, insertar su tarjeta extraíble (U)SIM en otro terminal (terminal llamado 2) incluyendo también un ESE e indicar a su operador que la aplicación m-NFC no funciona o que el terminal 1 tiene un problema. El operador entonces procedería a una nueva descarga de la aplicación m-NFC, pero esta vez en el ESE del terminal 2 que contiene la tarjeta (U)SIM del abonado. De esta manera, los dos terminales 1 y 2 incluyen la aplicación m-NFC que se habría así duplicado y el titular del terminal 2 podría hacer transacciones m-NFC sin haber sido autorizado por el operador.

Del mismo modo, el problema de usar un CMS es el siguiente: cuando el abonado suscribe una abono a una m-NFC, la aplicación NFC-m se descarga a través de OTA en el SMC 1 de su terminal. El abonado podría entonces, con ánimo de estafar a su operador, insertar otra tarjeta extraíble SMC (llamada SMC 2) en su terminal y solicitar una nueva descarga en SMC 2. De esta manera, la SCM 1 y 2 incluyen la aplicación m-NFC que habría sido duplicada.

Para superar estos inconvenientes, algunos operadores han desplegado servidores encargados de detectar una duplicación de servicios. Por ejemplo, en la banca, las tarjetas bancarias son registradas en una lista negra cuando se señalan como perdidas o excedida su fecha de validez. Esta lista negra se comprueba en cada transacción.

El problema con esta solución conocida es que requiere una inversión financiera importante para la interconexión no sólo con todos los terminales de pago NFC de los comerciantes con una red central, sino que requiere que se realicen comprobaciones en tiempo real. Este tipo de infraestructura no está al alcance de los proveedores de servicio de venta de billetería (transporte público), de fidelidad (grandes superficies), o incluso de cupones (grandes marcas) y está reservada para las redes financieramente acomodadas, tales como las redes bancarias. De hecho, estos proveedores de servicios no pueden financiar la interconexión de. todos sus terminales NFC a una red central, ni realizar comprobaciones en tiempo real.

El documento CN 101291494 describe un procedimiento que permite emparejar un terminal móvil y una tarjeta Sim. El emparejamiento está asegurado por un chip NFC insertado en el terminal móvil. Al conectar el terminal móvil, el chip NFC lee un identificador de la tarjeta Sim (por ejemplo, el MCC, el MNC o el IMSI) y lo compara con un identificador memorizado previamente. Si los identificadores son diferentes (lo que significa que la tarjeta Sim original ha sido reemplazada por una tarjeta Sim), se apaga la alimentación de la nueva tarjeta Sim. Se le priva así de la posibilidad de ser oteable y al terminal móvil de recibir o realizar llamadas.

En cambio, la aplicación NFC instalada en el chip NFC permanece operacional, es decir que el chip podrá aún ser utilizado para realizar transacciones NFC (su alimentación no se corta).

Este documento no describe pues la solución que permita asegurar la ejecución de una aplicación NFC insertada en un elemento seguro.

Este documento no aborda el aseguramiento de la ejecución de una aplicación NFC insertada en un elemento seguro. Se beneficia de la existencia de un chip NFC, que es un elemento seguro, para realizar el emparejamiento del terminal y de la tarjeta. Este chip puede también ser un chip Bluetooth o de otro tipo. El chip tiene la sola función de asegurar el terminal móvil y no la parte NFC del terminal.

La presente invención tiene principalmente como objetivo superar estos inconvenientes.

Más específicamente, un objetivo de la invención es proporcionar un método que permita, en el caso de utilizar un ESE solidario de un terminal móvil o de un SMC extraíble, detectar el uso, usando ese terminal, de un servicio del tipo m-NFC, cuando el usuario de ese servicio no es uno que ha sido previamente autorizado por su operador que le ha descargado a través de OTA la aplicación m-NFC. En otras palabras, el objetivo principal de la invención es proporcionar un método para detectar la duplicación no autorizada de un servicio de m-NFC.

Otro objetivo de la invención es prevenir al operador que presta el servicio a un abonado de la utilización fraudulenta de tal servicio-m NFC, a fin de que tome las medidas adecuadas.

Estos objetivos y otros que se harán evidentes a continuación, se consiguen mediante un procedimiento para asegurar la ejecución de una aplicación NFC insertada en un elemento seguro NFC que no incluye una aplicación OTA nativa bajo el control del operador, cooperando el elemento seguro con un terminal móvil, comprendiendo el terminal móvil además una tarjeta extraíble, comprendiendo dicho procedimiento:

- registrar en el elemento seguro un identificador de la tarjeta extraíble (U)SIM después de cargar la aplicación NFC en el elemento seguro;

- en caso de un evento, comprobar en el elemento seguro si el identificador de la tarjeta extraíble (U)SIM presente en el terminal móvil se corresponde con el identificador memorizado previamente en el elemento seguro, a fin de detectar un posible cambio de la tarjeta extraíble.

En una primera forma de realización, el identificador es el ICCID de la tarjeta extraíble (U)SIM.

En una segunda forma de realización, el identificador es el IMSI de la tarjeta extraíble (U)SIM.

En una tercera forma de realización, el identificador es el MSISDN de la tarjeta extraíble (U)SIM.

Preferiblemente, el evento que desencadena la comparación del identificador memorizado en el elemento de seguro con el de la tarjeta extraíble (U)SIM es la realización de una transacción NFC.

En otra forma de realización, el evento desencadenante es la activación del terminal móvil.

Ventajosamente, el procedimiento según la invención consiste también en notificar al emisor de la aplicación NFC una indicación de cambio de la tarjeta extraíble NFC (U)SIM si tal cambio se ha detectado.

Esta notificación puede ser realizado por un canal OTA o un canal NFC.

En una forma de realización preferida, el procedimiento de la invención consiste en bloquear la ejecución de la aplicación NFC si se detecta un cambio en loa tarjeta extraíble (U)SIM.

Ventajosamente, el procedimiento de la invención consiste en bloquear, por el emisor de la aplicación NFC, la ejecución de la aplicación NFC a través de un canal OTA o NFC.

Otras características y ventajas de la invención se harán evidentes tras la lectura de la siguiente descripción de una forma de realización ventajosa de la invención, dada a modo ilustrativo y no limitativo, y la figura única adjunta representa una forma de realización preferida del procedimiento según la invención.

Situados, como se indicó anteriormente, en el contexto de un terminal móvil que comprende por un lado una tarjeta extraíble del tipo tarjeta (U)SIM y, por el otro lado, un elemento seguro que es parte integrante (soldado o no) de este terminal móvil. El elemento seguro no incluye una aplicación OTA nativa, es decir, que es incapaz de realizar una operación de tipo OTA (a través del terminal móvil) cuando se entrega a su usuario final. No incluye identificador de tipo MSISDN y no puede por tanto ser contactado por el operador de la red de telecomunicaciones. Este elemento de seguridad coopera con el terminal móvil (se incluye allí, de manera fija o desmontable), comprendiendo este último también una tarjeta extraíble.

La figura única adjunta muestra una forma de realización preferida del procedimiento según la invención.

En esta figura, la etapa 10 corresponde a una etapa de inicio.

La etapa 11 consiste en registrar en el elemento seguro un identificador de la tarjeta extraíble, como muy tarde al cargar la aplicación NFC en el elemento seguro. Este identificador es un identificador único de la tarjeta extraíble, es decir que cada tarjeta tiene su propio identificador y el identificador de cada tarjeta es único.

El registro puede realizarse en la primera activación del terminal móvil que incluye la tarjeta extraíble y el elemento seguro integrado en el terminal móvil. El elemento seguro se asocia de ese modo con la tarjeta extraíble, y de manera definitiva.

El registro del identificador se lleva a cabo con la ayuda de un canal de comunicación establecido entre fa tarjeta extraíble y el elemento seguro.

En una primera forma de realización, el identificador es el ICCID de la tarjeta extraíble.

En una segunda forma de realización, el identificador es el IMSI de la tarjeta extraíble.

En una tercera forma de realización, el identificador es el MSISDN de la tarjeta extraíble.

Este registro del identificador se realiza de manera segura, de modo que una vez registrado, el identificador no puede ser modificado.

También es posible realizar este registro durante la descarga de la aplicación m-NFC en el terminal móvil, lo esencial es que el identificador se haya registrado antes de finalizar la descarga de la aplicación m-NFC en el terminal móvil.

En la etapa 12, la aplicación m-NFC es descargada completamente en el terminal móvil y está lista para ser ejecutada.

En la etapa 13, se comprueba si se produce un evento (que se describirá más adelante). Si esto sucede, se pasa a una etapa 14 que consiste en verificar en el elemento seguro si el identificador de la tarjeta extraíble presente en el terminal móvil se corresponde con el identificador memorizado previamente en el elemento seguro, a fin de detectar un posible cambio de tarjeta extraíble.

Sí el identificador memorizado se corresponde con el de la tarjeta extraíble presente en el terminal móvil, significa que no ha habido ningún cambio de tarjeta extraíble en el terminal: el abonado que ha solicitado el servicio m-NFC es, por lo tanto, el que ha sido autorizado por el operador para descargar la aplicación m-NFC. En este caso, puede realizarse una transacción NFC en la etapa 15.

En caso contrario, es decir si el identificador memorizado no se corresponde con el de la tarjeta extraíble presente en el terminal móvil, significa que ha habido un cambio de tarjeta extraíble del terminal: el abonado que solicitado el servicio m-NFC no es el que fue autorizado por el operador para descargar la aplicación m-NFC. En este caso, fa ejecución de la transacción NFC se deniega en una etapa 16.

Las etapas 15 y 16 son seguidas por una etapa final17.

El evento verificado en la etapa 13 es el caso típico de una transacción NFC: el usuario intenta realizar una transacción de este tipo a pagar por un bien o un servicio o se identifica en un lector para comprar un billete de transporte público, beneficiarse de un descuento en un producto o presentar su tarjeta de fidelización.

Este evento puede consistir también en una activación del terminal móvil.

Si como resultado de estos eventos se detecta que los identificadores no son idénticos, la etapa 16 también puede consistir en notificar al emisor de la aplicación NFC una indicación de cambio de la tarjeta extraíble. Esta notificación puede ser realizada por un canal OTA (en caso de verificación del identificador al producirse la activación) o por el canal NFC (en caso de verificación del identificador en caso de producirse una transacción NFC).

En la etapa 16, también puede ser posible bloquear automáticamente la ejecución de la aplicación NFC.

También se puede contemplar en el caso en que el terminal informa al transmisor de la aplicación NFC de un cambio de tarjeta extraíble, que este transmisor bloquee la ejecución de la aplicación NFC a través de un canal OTA o NFC.

El procedimiento de la invención permite, por ejemplo, en caso de detección de cambio de la tarjeta extraíble en el terminal que inserta el ESE o el MSC, bloquear una transacción NFC e informar al transmisor de la aplicación NFC que no es, en principio, el operador sino un establecimiento del tipo Eurocard, Mastercard o Visa (marcas registradas), de un cambio de tarjeta extraíble en el terminal móvil previamente autorizado para realizar este tipo de transacciones, por ejemplo, la aparición de una nueva tentativa de transacción NFC.

La descripción anterior se ha realizado de manera meramente ilustrativa y no limitativa, y el experto fácilmente imaginará otras formas de realización de la presente invención dentro del alcance de las reivindicaciones.

REIVINDICACIONES

1. Procedimiento para asegurar la ejecución de una aplicación NFC instalada en un elemento seguro que no comprende una aplicación OTA nativa, cooperando dicho elemento seguro con un terminal móvil, comprendiendo asimismo dicho terminal móvil una tarjeta extraíble, **caracterizado** porque consiste en:

- registrar (11) en dicho elemento seguro un identificador de dicha tarjeta extraíble después de cargar dicha aplicación NFC en dicho elemento seguro;

- en caso de un evento (13), comprobar (14) en dicho elemento seguro si el identificador de la tarjeta extraíble presente en dicho terminal móvil se corresponde con el identificador memorizado previamente en dicho elemento seguro, a fin de detectar un posible cambio de la tarjeta extraíble y porque incluye bloquear la ejecución de dicha aplicación NFC si se detecta un cambio de la tarjeta extraíble.

2. Procedimiento de acuerdo con la reivindicación 1, **caracterizado** porque dicho identificador es el ICCID de dicha tarjeta extraíble.

3. Procedimiento de acuerdo una de las reivindicaciones 1 y 2, **caracterizado** porque dicho identificador es el IMSI de dicha tarjeta extraíble.

4. Procedimiento de acuerdo una de las reivindicaciones 1 y 2, **caracterizado** porque dicho identificador es el MSISDN de dicha tarjeta extraíble.

5. Procedimiento de acuerdo una de las reivindicaciones 1 a 4, **caracterizado** porque dicho evento (13) es la realización de una transacción NFC.

6. Procedimiento de acuerdo una de las reivindicaciones 1 a 4, **caracterizado** porque dicho evento (13) es una activación de dicho terminal móvil.

7. Procedimiento de acuerdo una de las reivindicaciones 1 a 6, **caracterizado** porque también consiste en notificar (16) al emisor de dicha aplicación NFC una indicación de cambio de la tarjeta extraíble si tal cambio se ha detectado.

8. Procedimiento de acuerdo con la reivindicación 7, **caracterizado** porque dicha notificación se realiza por un canal OTA.

9. Procedimiento de acuerdo con la reivindicación 7, **caracterizado** porque dicha notificación se realiza por un canal NFC.

10. Procedimiento de acuerdo con una de las reivindicaciones 8 y 9, **caracterizado** porque consiste en bloquear (16), por parte del emisor de dicha aplicación NFC, la ejecución de dicha aplicación NFC a través de un canal OTA o NFC.

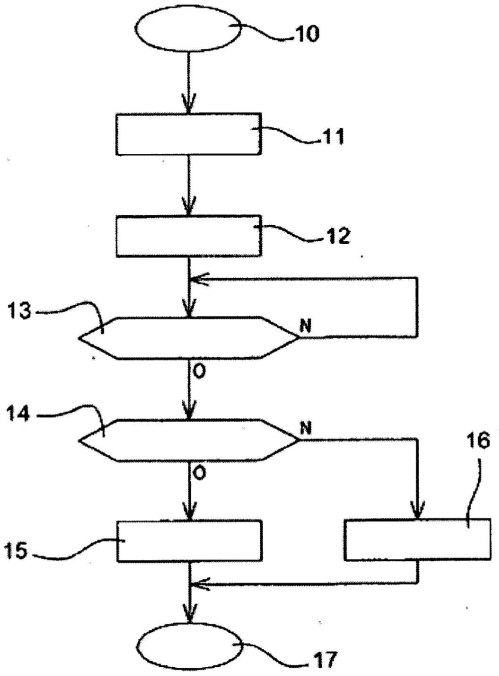

Figura única