(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 555 970**

(51) Int. CI.:

H04W 8/20 (2009.01)
G06F 21/00 (2013.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **05.12.2011 E 11794103 (9)**

(97) Fecha y número de publicación de la concesión europea: **29.04.2015 EP 2649827**

(54) Título: **Procedimiento para exportar datos de una UICC a un servidor seguro**

(30) Prioridad:

06.12.2010 EP 10306359

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.01.2016

(73) Titular/es:

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

(72) Inventor/es:

MERRIEN, LIONEL y
BERARD, XAVIER

(74) Agente/Representante:

ISERN CUYAS, María Luisa

DESCRIPCIÓN

Procedimiento para exportar datos de una UICC a un servidor seguro.

La presente invención se refiere a un método para exportar a un servidor seguro datos incluidos en una UICC (Tarjeta de Circuito Integrado Universal) comprendida en un terminal.

Los elementos de seguridad, como las UICC, incorporan aplicaciones Sim. Los elementos de seguridad pueden ser instalados, de manera fija o no, en los terminales, como por ejemplo los teléfonos móviles. En algunos casos, los terminales están constituidos por máquinas que se comunican con otras máquinas para aplicaciones M2M (Máquina a Máquina).

Una UICC puede tener el formato de una tarjeta inteligente, o puede tener cualquier otro formato como por ejemplo, pero no limitado a éste, un chip de empaquetado como el descrito en la PCT/SE2008/050380, o cualquier otro formato. Se puede utilizar en terminales móviles en redes GSM y UMTS, por ejemplo. La UICC garantiza la autenticación de red, la integridad y la seguridad de todo tipo de datos personales.

En una red GSM, la UICC contiene principalmente una aplicación SIM y en una red UMTS es la aplicación USIM. Una UICC puede contener varias otras aplicaciones, haciendo posible que la misma tarjeta inteligente proporcione acceso tanto a la red GSM como a la UMTS, y también proporcionar almacenamiento de una guía telefónica y otras aplicaciones. También es posible acceder a una red GSM usando una aplicación USIM y es posible acceder a las redes UMTS mediante una aplicación SIM con terminales móviles preparados para ello. Con la UMTS Release 5 y más tarde la red escenario como la LTE, es necesaria una nueva aplicación, el Módulo de de Servicios de Identidad Multimedia IP (ISIM) para los servicios en el IMS (Subsistema IP Multimedia). La guía telefónica es una aplicación independiente y no forma parte de ninguno de los módulos de información de suscripción.

En una red CDMA, la UICC contiene una aplicación CSIM, además de aplicaciones SIM y USIM 3GPP. Una tarjeta con las tres características se llama una tarjeta de identidad de usuario extraíble, o R-UIM. Así, la tarjeta R-UIM se puede insertar en terminales CDMA, GSM ó UMTS y trabajará en los tres casos.

En las redes 2G, la tarjeta SIM y la aplicación SIM se encontraban unidas, por lo que "la tarjeta SIM" podría significar la tarjeta física, o cualquier tarjeta física con la aplicación SIM.

La tarjeta inteligente UICC consiste en una CPU, ROM, RAM, EEPROM y circuitos I/O. Las primeras versiones consistían en todo el tamaño completo de la tarjeta inteligente (85 x 54 mm, ISO/IEC 7810 ID-1). Pronto, la carrera por teléfonos más pequeños exigió una versión más pequeña de la tarjeta.

Dado que la ranura de la tarjeta ha sido estandarizada, un abonado puede mover fácilmente su cuenta inalámbrica y su número de teléfono de un terminal a otro. Esto también transferirá su guía de teléfonos y sus mensajes de texto. Del mismo modo, usualmente un abonado puede cambiar de operador mediante la inserción de la tarjeta UICC de un nuevo operador en su terminal existente. Sin embargo, esto no es siempre posible debido a que algunas compañías (por ejemplo, en Estados Unidos) bloquean la SIM de los teléfonos que se venden, evitando así que se puedan utilizar tarjetas de la competencia.

La integración del marco ETSI y el marco de gestión de aplicaciones de la Plataforma Global ha sido estandarizada en la configuración de la UICC.

Las UICCs están estandarizadas por 3GPP y ETSI.

Una UICC normalmente puede ser eliminada de un terminal móvil, por ejemplo cuando el usuario desea cambiar su terminal móvil. Después de haber insertado su UICC en su nuevo terminal, el usuario tendrá acceso todavía a sus aplicaciones, contactos y credenciales (operador de red).

También se suelda o fusiona la UICC en un terminal, con el fin de conseguir la dependencia a este terminal. Esto se hace en aplicaciones M2M (Máquina a Máquina). El mismo objetivo se logra cuando un chip (un elemento seguro) que contiene las aplicaciones y archivos SIM o USIM está contenido en el terminal. El chip, por ejemplo, se suelda a la placa madre del terminal o máquina y constituye una e-UICC.

La presente invención también se aplica a estas UICCs soldadas o a estos chips que contienen las mismas aplicaciones que los chips integrados en las UICCs. Se puede hacer un paralelo para UICCs que no estén unidas totalmente a dispositivos pero que son extraíbles con dificultad debido a que no están pensadas para ser extraídas, localizadas en terminales que se encuentran distantes o profundamente integradas en máquinas. Un factor de forma especial de la UICC (muy pequeña, por ejemplo, y por lo tanto nada fácil de manejar) también puede ser una razón para considerar como de hecho integrado en un terminal. Lo mismo se aplica cuando una UICC está integrada en una máquina que no está destinada a ser abierta: Dichas UICCs soldadas o chips que contienen, o han sido

diseñados para contener, las mismas aplicaciones que las UICCs se denominaran generalmente UICCs integradas o elementos de seguridad integrados (en contraste con las UICCs extraíbles o los elementos de seguridad extraíbles). Esto también se aplica a UICCs o elementos de seguridad que se extraigan con dificultad.

El documento US 2008//0261561 A1 describe un método para transferir credenciales SIM desde un dispositivo móvil transferidor a un dispositivo móvil objetivo al propio tiempo que se asegura de que únicamente un dispositivo móvil contiene credenciales activas a la vez.

La presente invención se refiere a la exportación de datos sensibles de un componente seguro (chip UICC) que se enviarán a un depósito de seguridad (por ejemplo, un servidor seguro) sin riesgo de clonación de los datos, y sin enlace de datos directo entre la UICC y el servidor seguro. Más precisamente, la invención se refiere a un método para la exportación en un servidor de datos seguro comprendido en una UICC incluida en un terminal.

Al cambiar los terminales, como terminales móviles, por ejemplo teléfonos móviles, terminales inalámbricos o terminales conectados, los usuarios quieren tener facilidad para mantener los servicios que tenían activados en su antiguo terminal. Estos servicios, tales como los servicios de telefonía móvil o servicios bancarios, están confiando en claves y datos sensibles cargados en una UICC del terminal.

Si el componente de seguridad (UICC) es extraíble, como una tarjeta SIM clásica, y si el nuevo terminal soporta este componente extraíble, entonces el usuario puede simplemente quitar el componente de seguridad del terminal antiguo e insertarlo en el nuevo terminal.

Pero si la UICC no es extraíble (UICC incorporado) o si el nuevo terminal no admite este tipo de componente, entonces es necesario que haya una manera de trasladar todas las claves y los datos relacionados con ese servicio al componente de seguridad del nuevo terminal.

Otro problema que surge en el caso de UICCs integradas es que el viejo y el nuevo terminal a veces no están disponibles al mismo tiempo. El usuario quiere asegurar sus datos sensibles (personales) y las claves antes de adquirir su nuevo terminal.

La invención proporciona una forma de exportar de forma segura las claves y los datos relacionados con un servicio a un depósito de seguridad, para luego descargarlos en otro (o el mismo) terminal, de tal manera que las claves y los datos no pueden ser clonados.

Además, la invención aborda el problema de que puede que no sea posible establecer un enlace directo IP entre el depósito de seguridad y el componente de seguridad.

Para este propósito, la presente invención propone un método para la exportación en un servidor seguro de los datos comprendidos en una UICC incluida en un terminal. El método consiste en:

- A petición de la exportación, firmar una petición de exportación realizada por la UICC, siendo transmitida la petición de exportación por el terminal al servidor;
- Verificar, a nivel del servidor, la solicitud de exportación firmada mediante la comparación de la firma y la identidad de la UICC;
- Si la verificación es positiva, envío por parte del servidor de un certificado de exportación firmado a la UICC a través del terminal;
- Verificación del certificado de exportación firmado en la UICC y, en caso positivo, la preparación de un paquete de exportación que contiene los datos, el paquete de exportación está firmado y cifrado por la UICC;
- El envío del paquete de exportación al terminal; y establecer los datos exportados como "inservible" en la UICC;
- La transmisión desde el terminal al servidor del paquete de exportación;
- Recepción del paquete y verificar la firma a nivel del servidor;
- Firmar un mensaje de acuse de recibo y transmitirlo a la UICC a través del terminal;
- En la UICC, verificar el mensaje de acuse de recibo y, si se reconoce la firma del servidor, destruir los datos que se han exportado y enviar mensaje de acuse de recibo al servidor a través del terminal;
- Verificación de la firma del mensaje de acuse de recibo en el servidor y, si la firma es reconocida, configurar los datos disponibles para una transferencia futura a un nuevo terminal o UICC.

La UICC está incrustada preferentemente en el terminal y la solicitud de exportación es precedida de una selección de los datos a exportar.

La invención se entenderá mejor mediante la lectura de la siguiente descripción de la figura 1 que representa un diagrama de flujo de una realización preferida de la presente invención.

La invención integra una conexión asíncrona entre el componente seguro (UICC) y el depósito de seguridad

constituido, por ejemplo, por un servidor remoto.

En la figura 1, el usuario final de un terminal selecciona primero los datos a exportar. Estos datos son, por ejemplo números de teléfono o claves privadas que el usuario desea asegurar para poder transferirlos posteriormente a otro (o el mismo) terminal.

Esto puede hacerse mediante la selección de un identificador de aplicación o un identificador de servicio en la UICC. Esto lo puede hacer el usuario a través de una aplicación en el terminal, o automáticamente a través del terminal. Esto corresponde a una solicitud de exportación formulada por el usuario final. Dicha petición de exportación también podría ser formulada por el servidor remoto o por el terminal.

Opcionalmente, al seleccionar los datos/servicios a exportar desde la UICC, el usuario/terminal puede tener que presentar un código o autenticarse ante la UICC o el servicio a fin de tener acceso a los datos.

El terminal inicia entonces la sesión de exportación en el componente de seguridad enviándole una orden "INIC SESIÓN DE EXPORTACIÓN".

En respuesta, la UICC devuelve una "solicitud de exportación firmada" al terminal. Esta petición es únicamente identificada y firmada por la UICC.

La "petición de exportación firmada" se transmite de forma asíncrona al servidor a través de una red, como una red IP, celular, OTA u OTI.

A la recepción, el servidor verifica la "solicitud de exportación firmada", mediante la comparación de la firma y la identidad de la UICC. La invención no impone ningún esquema de seguridad en particular, pero requiere que el servidor puede verificar la firma de la UICC.

El servidor genera entonces un "Certificado de Exportación". Este certificado está firmado únicamente por el servidor, e identifica de forma exclusiva la UICC. Con este certificado, el servidor confirma que la UICC es genuina, y que el proceso de exportación puede ser iniciado.

El "certificado de exportación" se transmite de forma asíncrona a la UICC por el terminal.

La UICC luego verifica el "Certificado de Exportación". La invención no especifica un esquema de seguridad en particular, pero la UICC debe tener la capacidad de verificar una firma desde el servidor.

La UICC aumenta un "contador de exportación". Este contador es mantenido por la UICC.

La UICC prepara un "paquete de exportación". Este paquete de exportación es cifrado y firmado por la UICC. Además, el "paquete de exportación" incluye el "contador de exportación". El paquete de exportación se envía al terminal. Si es necesario (como se muestra en el diagrama), debido a la limitación de I/O entre el terminal y la UICC, el paquete de exportación se puede enviar a través de varios comandos. Después de haber sido enviado al terminal, la imagen del paquete transmitido guardado al nivel de la UICC se vuelve inactiva (con el fin de evitar una posible duplicación del paquete).

El "paquete de exportación" se transmite entonces de forma asíncrona con el servidor. Debido a que está cifrado, sólo el servidor puede leerlo.

Una vez recibido, el servidor descifra y verifica el paquete de exportación. Para cada UICC, el servidor mantiene una copia del contador de exportación. El contador de exportación en el paquete de exportación debe ser más alto que la copia del contador de exportación mantenida por el servidor, de lo contrario el paquete de exportación es rechazado. Una vez que el paquete de exportación ha sido aceptado, el servidor actualiza su copia del contador de exportación para que coincida con el valor en el paquete de exportación.

El servidor genera entonces un acuse de recibo firmado. Este acuse de recibo está firmado únicamente por el servidor, e incluye el valor del contador de exportación. Después de haber enviado este comando, el paquete recibido se vuelve inactivo a nivel del servidor.

El acuse de recibo firmado se transmite de forma asíncrona a la UICC (es decir, a través del terminal).

La UICC verifica el acuse de recibo firmado y, si coincide, destruye su copia (imagen) de los datos que han sido exportados.

La UICC genera entonces un acuse de recibo de destrucción firmado, que es firmado únicamente por la UICC, e incluye el valor del contador de exportación.

El acuse de recibo de destrucción firmado se transmite de forma asíncrona al servidor.

El servidor verifica entonces el acuse de recibo de destrucción firmado. Si coincide, los datos exportados están disponibles para ser importados en otra UICC en un nuevo terminal o en el mismo con posterioridad.

Las ventajas de la presente invención son los siguientes:

- En cada punto del proceso, la invención proporciona una buena manera de interrumpir y revertir el proceso. Por lo tanto no hay riesgo de perder los datos.
- Todo el proceso se puede hacer a través de una conexión asíncrona (tal como e-mail).

No hay necesidad de que la UICC se encuentre directamente conectada al servidor.

- No es posible tener información clonada. Los datos están disponibles en el servidor sólo después de la confirmación de que han sido destruidos en la UICC.

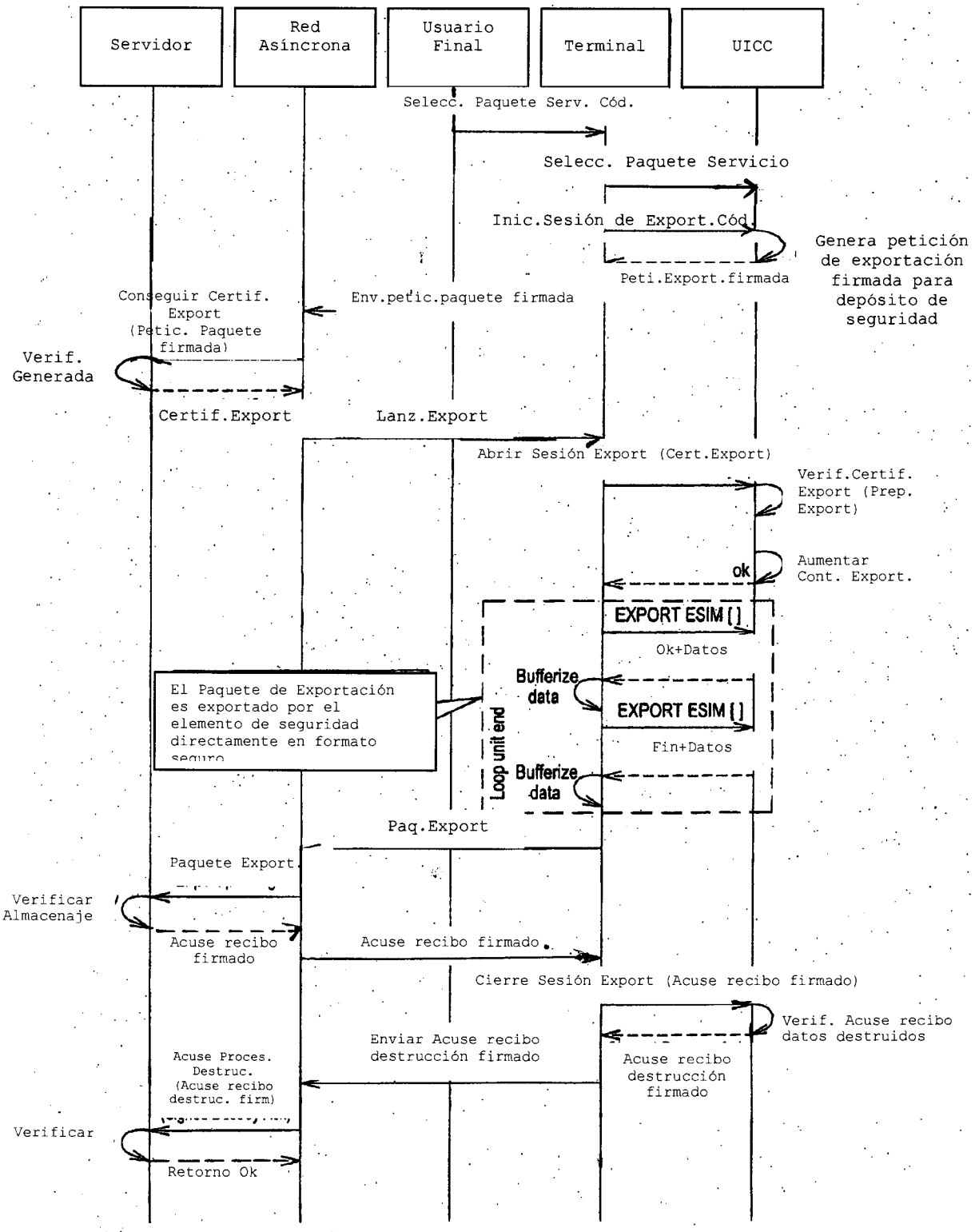
REIVINDICACIONES

1. Método para la exportación en un servidor seguro los datos comprendidos en una UICC incluida en un terminal, dicho método consistente en:

- A petición de la exportación, firmar una petición de exportación realizada por la UICC, siendo transmitida la petición de exportación por el terminal al servidor;
- Verificar, a nivel del servidor, la solicitud de exportación firmada mediante la comparación de la firma y la identidad de la UICC;
- Si la verificación es positiva, envío por parte del servidor de un certificado de exportación firmado a la UICC a través del terminal;
- Verificación del certificado de exportación firmado en la UICC y, en caso positivo, la preparación de un paquete de exportación que contiene los datos, el paquete de exportación está firmado y cifrado por la UICC;
- El envío del paquete de exportación al terminal; y establecer los datos exportados como "inservible" en la UICC;
- La transmisión desde el terminal al servidor del paquete de exportación;
- Recepción del paquete y verificar la firma a nivel del servidor;
- Firmar un mensaje de acuse de recibo y transmitirlo a la UICC a través del terminal;
- En la UICC, verificar el mensaje de acuse de recibo y, si se reconoce la firma del servidor, destruir los datos que se han exportado y enviar mensaje de acuse de recibo al servidor a través del terminal;
- Verificación de la firma del mensaje de acuse de recibo en el servidor y, si la firma es reconocida, configurar los datos disponibles para una transferencia.

2. Método de acuerdo con la reivindicación 1, en donde dicha UICC se encuentra incrustada en dicho terminal.

3. Método de acuerdo con las reivindicaciones 1 o 2, en donde dicha solicitud de exportación es precedida por una selección de los datos a ser exportados.


Servidor
Red Asíncrona
Usuario Final
Terminal
UICC
Selecc. Paquete Serv. Cód.
Selecc. Paquete Servicio
Inic.Sesión de Export.Cód.
Genera petición de exportación firmada para depósito de seguridad
Peti.Export.firmada
Conseguir Certif. Export (Petic. Paquete firmada)
Env.petic.paquete firmada
Verif. Generada
Certif.Export
Lanz.Export
Abrir Sesión Export (Cert.Export)
Verif.Certif. Export (Prep. Export)
ok
Aumentar Cont. Export.
EXPORT ESIM [ ]
Ok+Datos
Bufferize data
EXPORT ESIM [ ]
Fin+Datos
Bufferize data
Loop unit end
El Paquete de Exportación es exportado por el elemento de seguridad directamente en formato seguro
Paq.Export
Paquete Export.
Verificar Almacenaje
Acuse recibo firmado
Acuse recibo firmado.
Cierre Sesión Export (Acuse recibo firmado)
Verif. Acuse recibo datos destruidos
Enviar Acuse recibo destrucción firmado
Acuse recibo destrucción firmado
Acuse Proces. Destruc. (Acuse recibo destruc. firm)
Verificar
Retorno Ok