(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 694 953**

(51) Int. CI.:

H04W 12/04 (2009.01)
H04W 12/06 (2009.01)
H04L 29/06 (2006.01)
H04L 29/08 (2006.01)
H04L 12/22 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.05.2007 E 14002040 (5)**

(97) Fecha y número de publicación de la concesión europea: **29.08.2018 EP 2779722**

(54) Título: **Procedimiento para personalizar un módulo de seguridad de un dispositivo terminal de telecomunicación**

(30) Prioridad:

23.05.2006 DE 102006024041

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.12.2018

(73) Titular/es:

GIESECKE+DEVRIENT MOBILE SECURITY GMBH (100.0%)
Prinzregentenstraße 159
81677 München, DE

(72) Inventor/es:

RANKL, WOLFGANG;
VEDDER, KLAUS;
RICHTER, OLIVER;
MÜLLER, BERND;
GARBERS, CHRISTIAN;
OTTE, GÜNTER y
STÖHR, VOLKER

(74) Agente/Representante:

DURAN-CORRETJER, S.L.P

DESCRIPCIÓN

Procedimiento para personalizar un módulo de seguridad de un dispositivo terminal de telecomunicación

La invención se refiere a la personalización de un módulo de seguridad en un dispositivo terminal de telecomunicación. Por dispositivos terminales de telecomunicación deben entenderse todos los dispositivos que se comunican a través de GSM, UMTS, CDMA o redes similares en una PLMN (public land mobile network), es decir, en particular, dispositivos de telefonía móvil, PDA y similares. En este contexto de aplicación deben considerarse funciones de seguridad, por ejemplo, la autentificación del dispositivo terminal de telecomunicación respecto a la red de telefonía móvil o la autentificación del usuario respecto al dispositivo terminal de telecomunicación. Este tipo de funciones de seguridad se ejecutan a través de módulos de seguridad contenidos en el dispositivo terminal de telecomunicación, habitualmente en tarjetas SIM. Recientemente se ha propuesto realizar dichos módulos de seguridad como TMP (trusted platform module) ampliado. Los TMP, al contrario que las tarjetas SIM tradicionales, están integrados de forma fija en el dispositivo terminal de telecomunicación.

Para que un dispositivo terminal de telecomunicación pueda conectarse a una red de telefonía móvil y autentificarse respecto al Trustcenter (centro de confianza) de un operador de telefonía móvil, el módulo de seguridad del dispositivo terminal de telecomunicación debe equiparse con los datos necesarios, en particular, con los algoritmos de autentificación secretos necesarios y las claves adecuadas del operador de red correspondiente. El proceso de equipar el módulo de seguridad con estos datos necesarios y específicos del operador de red debe entenderse como personalización en el contexto de la presente invención. Los propios datos se denominan a continuación datos específicos del operador de red.

Hasta ahora, generalmente se suministran a los clientes módulos de seguridad que ya están equipados con estos datos específicos del operador de red. Esto aplica a tarjetas SIM tradicionales para dispositivos de telefonía móvil. En el caso de los módulos de seguridad integrados de forma fija en los dispositivos terminales de telecomunicación existe la desventaja de que ya debe conocerse el operador de red en el momento de la producción del módulo de seguridad y antes de su montaje en un dispositivo terminal de telecomunicación o deben fabricarse diferentes módulos de seguridad para diferentes operadores de red, lo que no permite una producción estandarizada y económica de módulos de seguridad idénticos.

El documento EP 1 002 440 B1 da a conocer un procedimiento para la personalización por parte del cliente de chips GSM a través de una interfaz aérea. Un chip previamente personalizado por el operador de red se termina de personalizar de forma automática cuando el usuario se conecta por primera vez a la red de usuarios. Durante la personalización final, después de establecerse una conexión entre el dispositivo terminal de telecomunicación y el centro de confianza del operador de red, se acuerda una nueva y segunda clave secreta con el centro de confianza y, a continuación, se transmite al dispositivo terminal de telecomunicación para su incorporación en el módulo de seguridad. Sigue existiendo la desventaja de que el módulo de seguridad ya debe contener datos específicos del operador de red cuando se integra en el dispositivo terminal de telecomunicación.

El documento EP 0 956 730 B1 da a conocer un procedimiento para asignar una identificación de usuario temporal a través de la interfaz aérea. Esta identificación de usuario se exige y utiliza únicamente para un establecimiento de conexión especial. No tiene lugar una personalización duradera del dispositivo terminal de telecomunicación.

El documento US 2004/0246071 A1 describe la transmisión de claves de aplicación de un servidor a una tarjeta SIM en un dispositivo terminal mediante un SMS que es descifrado en la tarjeta SIM.

El documento EP 1 276 339 A1 se refiere a un sistema para cargar un programa de un servidor a una tarjeta SIM, tal que el usuario selecciona un programa de una lista y el servidor selecciona un método de cifrado en base a una lista de características de la tarjeta SIM.

El objetivo de la invención consiste en proponer medidas que permitan personalizar de forma eficiente y segura un módulo de seguridad que está fijamente instalado en un dispositivo terminal de telecomunicación y aún no contiene ningún dato específico del operador de red.

Este objetivo se consigue mediante un procedimiento con las características de las reivindicaciones secundarias. En las reivindicaciones dependientes se indican configuraciones y perfeccionamientos ventajosos de la invención.

Según la invención, para personalizar un módulo de seguridad en un dispositivo terminal de telecomunicación con datos específicos del operador de red, en el dispositivo terminal de telecomunicación se ejecutan los siguientes pasos.

- Recepción de una secuencia de comandos de un servidor para el módulo de seguridad;
- Ejecución de la secuencia de comandos mediante

Extracción de comandos individuales de la secuencia de comandos por parte del dispositivo terminal de telecomunicación,
Trasmisión de los comandos al módulo de seguridad y recepción de las respuestas de comando del módulo de seguridad; y

- Transferencia de la última respuesta de comando del módulo de seguridad al servidor.

Los datos de identificación necesarios para la personalización, que el operador de red transmite al usuario tras firmar el contrato, pueden estar disponibles para el usuario en primer lugar fuera del dispositivo terminal de telecomunicación y ser transferidos por el usuario al módulo de seguridad del dispositivo terminal de telecomunicación. Estos datos de identificación pueden estar disponibles para el usuario de diferentes formas e incorporarse correspondientemente y de diferentes formas en el módulo de seguridad del dispositivo terminal de telecomunicación, concretamente, por ejemplo, mediante introducción manual de secuencias de cifras alfanuméricas, lectura de una etiqueta RFID, trasferencia de los datos a través de interfaz Bluetooth o WiFi, escaneo de un código de barras, fotografía y extracción OCR subsiguiente, procesamiento de información acústica y similares.

La invención permite producir módulos de seguridad estandarizados e instalarlos en dispositivos terminales de telecomunicación. No es necesario un conocimiento previo del operador de red específico que se utilizará posteriormente, ya que, a diferencia del estado de la técnica, no debe tener lugar una personalización previa. Después de haber sido recibidos por el dispositivo terminal de telecomunicación, los datos de identificación pueden ser utilizados directamente por el dispositivo terminal de telecomunicación, sin intervención manual, para la personalización. No es necesaria una modificación de las actuales redes de telefonía móvil. Con el mismo módulo de seguridad también es posible un cambio del operador de red.

El procedimiento de personalización continúa estableciendo el dispositivo terminal de telecomunicación una conexión con un centro de confianza. Los datos necesarios para el primer establecimiento de contacto con el centro de confianza pueden estar disponibles de forma estándar en todos los módulos de seguridad, por ejemplo, claves y algoritmos de un operador de red virtual (MVNO) que se utiliza una única vez para la primera conexión con el centro de confianza, pero no se encuentra relacionado de ningún modo con el operador de red específico a cuyas necesidades debe adaptarse el dispositivo terminal mediante la personalización, o ser transferidos por el usuario al módulo de seguridad junto con los datos de identificación.

En otro paso del procedimiento de personalización se transfieren los datos de identificación al centro de confianza. Los datos de identificación comprenden los datos de usuario conocidos para el operador de red tras la firma del contrato (datos de suscripción) y que permiten su identificación, por ejemplo, para fines de información y facturación. Además, los datos de identificación pueden contener información adicional, por ejemplo, el operador de red, el centro de confianza, el modo de acceso y similares. Estos datos de identificación contienen toda la información necesaria que requiere el usuario para continuar automáticamente el proceso de personalización tras incorporar estos datos en el módulo de seguridad y establecer la conexión con el centro de confianza, sin necesidad de tomar otras medidas.

El centro de confianza valora que los datos de identificación recibidos sean correctos y, en caso positivo, establece una conexión segura al dispositivo terminal de telecomunicación. Además, el centro de confianza puede extraer de los datos de identificación qué datos de personalización específicos del operador de red necesita el usuario e inicia una transferencia de estos datos al módulo de seguridad del dispositivo terminal de telecomunicación. Es decir, tiene lugar una personalización completamente automática. Dado el caso, el usuario puede ser informado sobre el desarrollo del proceso, por ejemplo, a través de una pantalla.

Se prefiere que el dispositivo terminal de telecomunicación se establezca en un modo especial antes de incorporar los datos de identificación. Esto simplifica el proceso de personalización, ya que en este modo especial no hay otras funciones activas y, por tanto, una personalización puede ejecutarse automáticamente. Además, el modo puede estar configurado de forma que se garantice una comunicación segura. Este modo especial se denominará en relación con la presente invención modo de personalización.

Tras la transferencia de los datos de personalización, el dispositivo terminal de telecomunicación puede volver al modo de servicio normal y utilizarse para los fines de comunicación habituales. Si el dispositivo terminal de telecomunicación cambia de usuario, por ejemplo, por venta, préstamo o regalo, o si el usuario cambia el operador de red, el proceso de personalización descrito puede volver a iniciarse en el modo de personalización. Este puede estar protegido con una contraseña para evitar usos accidentales o inadecuados.

A continuación, se explica la invención en base a las figuras adjuntas a modo de ejemplo. Muestran:

La figura 1, una vista general de un sistema adecuado para el proceso de personalización según la invención,

La figura 2, una secuencia de comandos codificada en XML,

La figura 3, un desarrollo del proceso dentro de un MIDlet,

La figura 4, un proceso de comunicación entre un módulo de seguridad, un MIDlet y un servidor,

La figura 5, un proceso de comunicación entre un MIDlet y un servidor,

La figura 6, una vista general de la arquitectura de un sistema para gestionar módulos de seguridad a través de una interfaz aérea y

La figura 7, una representación del ciclo de vida de un módulo de seguridad.

A continuación se representa más detalladamente un ejemplo de realización preferido de un proceso de personalización según la invención, dividido en pasos individuales. La figura 1 muestra una vista general de un sistema adecuado para realizar el proceso de personalización. Este comprende datos -100- de identificación, un dispositivo -200- terminal de telecomunicación, fuera del cual están disponibles los datos -100- de identificación y que cuenta con un módulo -300- de seguridad, un centro -400- de confianza de un personalizador -1000-, que comprende una base -500- de datos y un servidor -600-, uno o varios operadores -700-, -710-, -720- de red y una red -800- de telefonía móvil. La siguiente es una descripción detallada del proceso de personalización, dividido en pasos individuales:

1. Para el proceso de personalización, el dispositivo -200- terminal de telecomunicación se encuentra en el modo de personalización o se establece en este modo. Los datos -100- de identificación necesarios para la personalización, que están disponibles fuera del dispositivo -200- terminal de telecomunicación, se incorporan en el dispositivo -200- de una de las formas descritas anteriormente, concretamente, por ejemplo, mediante introducción manual de secuencias de cifras alfanuméricas, lectura de una etiqueta RFID, trasferencia de los datos a través de interfaz Bluetooth o WiFi, escaneo de un código de barras, fotografía y extracción OCR subsiguiente, procesamiento de información acústica y similares. (El documento WO 2006/ 006001 A1 describe el planteamiento aislado de incorporar datos comprimidos disponibles de forma similar fuera de un dispositivo de telefonía móvil con las técnicas de lectura correspondientes en un dispositivo de telefonía móvil, descomprimirlos allí y desencadenar de este modo automáticamente una acción especial, por ejemplo, una entrada de calendario).
2. A continuación, el usuario inicia la conexión del dispositivo -200- terminal de telecomunicación a la red -800- de telefonía móvil. Esto puede tener lugar, por ejemplo, con claves y algoritmos de autentificación, incorporados de forma estandarizada en todos los módulos -300- de seguridad, de un operador de red virtual que se utiliza una única vez para la primera conexión con el centro -400- de confianza, pero no se encuentra relacionado de ningún modo con el operador -700-, -710-, -720- de red específico a cuyas necesidades debe adaptarse en primer lugar el dispositivo -200- terminal mediante la personalización. No obstante, preferentemente también estas claves y algoritmos de autentificación son incorporados por primera vez por el usuario en el dispositivo -200- terminal de telecomunicación, por ejemplo, al mismo tiempo que los datos -100- de identificación para hacer posible un uso ampliamente universal del dispositivo -200- terminal de telecomunicación. La conexión establecida en este paso está configurada por la infraestructura de red de forma que solo es posible en exclusiva un intercambio de datos entre el centro -400- de confianza del personalizador -1000- y el módulo -300- de seguridad.
3. Los datos -100- de identificación son enviados al centro -400- de confianza del personalizador -1000- a través de la red -800- de telefonía móvil. Esto puede tener lugar tanto mediante iniciación por parte del usuario, como también automáticamente mediante activación por parte del módulo -300- de seguridad.
4. El centro -400- de confianza determina mediante una consulta a la base -500- de datos qué operadores -700-, -710-, -720- de red posibles están disponibles para los datos -100- de identificación recibidos.
5. La información sobre los operadores -700-, -710-, -720- de red posibles se envía al dispositivo terminal de telecomunicación mediante un servicio de datos adecuado (por ejemplo, GPRS, SMS). Esta información se puede transmitir al usuario, por ejemplo, a través de una pantalla.
6. El usuario selecciona ahora el operador -700- de red deseado. Esta selección puede tener lugar de forma ventajosa mediante comandos SIM Toolkit. De este modo, la información sobre la selección de un operador -700-, -710-, -720- de red se transmite directamente al módulo -300- de seguridad, por ejemplo, una tarjeta SIM.
7. El módulo -300- de seguridad envía la selección del usuario a través de la red -800- de telefonía móvil al centro -400- de confianza del personalizador -1000-. Esto puede tener lugar, a elección, de forma cifrada y/o con una suma de verificación criptográfica para realizar la comunicación de forma segura. (Si en el paso 4 solo existe un posible operador de red, se puede prescindir de los pasos 5 a 7).
8. En el centro -400- de confianza se extraen ahora los datos de personalización correspondientes, particularmente los datos específicos del operador de red como el algoritmo de autentificación y la clave correspondiente, pero posiblemente también el código de programa para aplicaciones adicionales, de una base -500- de datos.
9. Los datos de personalización se envían al módulo -300- de seguridad. Esto tiene lugar preferentemente de forma cifrada y/o con una suma de verificación criptográfica para realizar la comunicación de forma segura.

10. En el módulo -300- de seguridad se comprueba que los datos recibidos sean correctos y, en caso positivo, se integran a continuación en el lugar correspondiente del módulo -300- de seguridad.
11. En caso de un desarrollo sin fallos del último paso, el centro -400- de confianza recibe un mensaje al respecto del módulo -300- de seguridad. De este modo, el módulo -300- de seguridad está personalizado para un nuevo operador -700- de red y puede funcionar en servicio normal en cuanto el operador -700- de red lo autoriza.
12. La información sobre la transferencia exitosa de los datos de personalización que el centro -400- de confianza recibe del módulo -300- de seguridad se deriva al operador -700- de red. Estos datos se corresponden esencialmente con los datos transferidos actualmente por el personalizador al operador de red como “datos response”. Tras la entrada correcta de estos datos, el operador -700- de red autorizará el módulo -300- de seguridad de forma que el dispositivo -200- terminal de telecomunicación correspondiente pueda volver al modo normal y utilizarse para fines de comunicación habituales.

A continuación se describe una posibilidad preferente de realización técnica de la transferencia de datos entre el centro -400- de confianza y el módulo -300- de seguridad del dispositivo -200- terminal de telecomunicación, y en particular, en relación con los pasos anteriormente denominados 9, 10 y 11.

Preferentemente, como dispositivo -200- terminal de telecomunicación sirve un teléfono móvil compatible con J2ME con módulo -300- de seguridad integrado según los estándares JavaCard 2.x y Global Platform 2.2.1. En un principio, en el módulo -300- de seguridad no se encuentra ningún Java Applet ni ningún Global Platform Security Domains. Las claves del Issuer Security Domain (ENC, KEK, MAC) son claves iniciales que pueden ser o bien individuales para el chip o bien corresponder a un Master Key Set. En este estado, el módulo -300- de seguridad no puede utilizarse para ninguna aplicación, en particular, tampoco para la autentificación en un operador -700- de red.

En relación con las figuras 2 a 5 se describe ahora en detalle el proceso de comunicación entre el módulo -300- de seguridad del teléfono -200- móvil y el servidor -600- del centro -400- de confianza del personalizador -1000-.

Preferentemente, para la comunicación entre el módulo -300- de seguridad y el servidor -600- se utiliza el denominado protocolo APDU (application protocol data units). En este caso, los datos se transfieren en bloque, estando compuesto un bloque de datos siempre o bien por un comando, o bien por una respuesta a un comando. En este sentido, el módulo de seguridad asume habitualmente el rol pasivo (esclavo) y espera comandos que son enviados por el servidor (maestro) y a los cuales contesta a continuación. La estructura especificada de los bloques de datos deja espacio (data field) en cada bloque de datos para la transferencia de cualquier dato. Es decir, los datos a transferir por el servidor -600- al módulo -300- de seguridad se empaquetan en comandos APDU. Una serie de este tipo de comandos se combina para formar una secuencia de comandos. La figura 2 muestra a modo de ejemplo una secuencia de comandos codificada en XML (Extensible Markup Language).

En las figuras 3 y 4 está representada de forma esquemática la comunicación entre el módulo -300- de seguridad y el servidor -600-. En el teléfono -200- móvil se encuentra un denominado MIDlet -900- (según especificación J2ME, MIDP2.0), que tiene acceso al módulo -300- de seguridad del teléfono -200- móvil a través de una API (application programming interface) y puede establecer contacto con el servidor -600-.

El contacto se establece a través de una interfaz -600a- del servidor, a través de un denominado Servlet. La figura 3 ilustra la comunicación entre el MIDlet -900- y el servidor -600- a través del Servlet -600a-. Tras un primer establecimiento de contacto por parte del MIDlet -900-, el Servlet -600a- recoge la primera secuencia de comandos en el servidor -600- y la envía luego, por ejemplo codificada en XML, al MIDlet -900-. En la figura 4 se muestra cómo el MIDlet -900- continúa procesando entonces esta secuencia de comandos. Los comandos individuales son enviados sucesivamente del MIDlet -900- al módulo -300- de seguridad, que responde respectivamente con una respuesta al comando antes recibido. Después de ejecutar todos los comandos, por ejemplo, n comandos, el MIDlet -900- envía la respuesta del módulo -300- de seguridad al enésimo comando a través del Servlet -600a- al servidor -600-. Ahora se puede repetir el proceso múltiples veces tal como se ha descrito anteriormente, dependiendo de la respuesta del módulo -300- de seguridad al enésimo comando y de la abundancia de los datos a transmitir y, por tanto, de las secuencias de comandos a transferir, tal como se desprende de las figuras 3 y 4.

A continuación se representa más detalladamente el proceso dentro del MIDlet -900- en relación con la figura 5. El MIDlet -900-, que ya ha establecido una conexión al módulo -300- de seguridad a través de una API, abre un canal al servidor -600- del personalizador -1000- para iniciar el proceso de personalización, por ejemplo, a través de una conexión https. El servidor -600- comprueba si se trata de una consulta válida y, en caso positivo, prepara los datos determinados para el módulo -300- de seguridad en forma de una secuencia de comandos. Esta secuencia de comandos se envía, por ejemplo, como respuesta a la solicitud https al MIDlet -900-. La secuencia de comandos es ejecutada ahora por el MIDlet -300- extrayendo los comandos individuales de la secuencia de comandos y enviándolos sucesivamente al módulo -300- de seguridad, que responde respectivamente a dichos comandos tal como se ha descrito anteriormente. Si el módulo -300- de seguridad responde según lo esperado, entonces se envía el siguiente comando de la secuencia al módulo -300- de seguridad. Por el contrario, si la respuesta difiere de la respuesta esperada, el MIDlet -900- finaliza la transferencia de la secuencia de comandos y envía la última respuesta recibida por el módulo -300- de seguridad de vuelta al servidor -600- del personalizador -1000- junto con

una lectura del contador de comandos. En el caso de que todos los comandos de la secuencia hayan sido ejecutados con éxito, el MIDlet envía la última respuesta recibida por el módulo -300- de seguridad y la lectura del contador de comandos al servidor.

Para que el servidor -600- pueda comprobar si los datos enviados fueron transferidos correctamente al módulo -300- de seguridad solo necesita la respuesta del módulo -300- de seguridad al último comando y la lectura del contador de comandos, que registra cuántos comandos fueron transferidos del MIDlet -900- al módulo -300- de seguridad, incrementándolo en 1 respectivamente tras procesar un comando, después de haber sido restablecido a 0 antes del procesamiento de una nueva secuencia de comandos. De este modo, la transferencia de secuencias de comandos del servidor -600- al módulo -300- de seguridad ahorra volumen de comunicación en comparación con la transferencia de comandos individuales y hace que la transmisión de datos sea más rápida y efectiva, ya que el servidor -600- no debe esperar la respuesta del módulo -300- de seguridad a cada comando individual y tampoco es necesario transmitir cada una de dichas respuestas al servidor.

La secuencia de comandos puede estar codificada, por ejemplo, en XML (véase figura 2). Alternativamente, también son posibles otros formatos como, por ejemplo, comandos separados por comas o similares. En la secuencia de comandos mostrada a modo de ejemplo en la figura 2, el campo "ExpectedResponse" está rellenado respectivamente con "90 00". Este campo "90 00" es opcional, ya que esta es la respuesta estándar de una JavaCard en caso de un comando correctamente ejecutado y se asume implícitamente que con esta respuesta se puede garantizar una ejecución posterior exitosa de la secuencia de comandos. Por esta razón, esta respuesta estándar esperada no tiene que transferirse, lo que ahorra adicionalmente volumen de transferencia.

Tanto en caso de una ejecución correcta y completa de la secuencia de comandos, como también en caso de interrupción debido a datos de respuesta inesperados del módulo -300- de seguridad, tras la transmisión de los datos de respuesta del módulo -300- de seguridad a través del MIDlet -900- al servidor -600- del personalizador -1000-, este puede volver a enviar una secuencia de comandos y el proceso vuelve a comenzar tal como se ha descrito anteriormente. Si esto no ocurre, entonces el MIDlet -900- finaliza la comunicación con el servidor -600- y emite, dado el caso, un mensaje de estado al usuario.

La conexión del MIDlet al servidor -600- del personalizador -1000-, por un lado, y al módulo -300- de seguridad del teléfono -200- móvil, por el otro, puede estar contenida en diferentes hilos de ejecución.

De forma similar a la personalización de módulos de seguridad en dispositivos terminales de telecomunicación tal como se ha descrito anteriormente, los módulos de seguridad también se pueden configurar para diferentes aplicaciones de proveedores de servicios, por ejemplo, aplicaciones NFC. Near Field Communication (NFC) es una tecnología para la transferencia de datos sin contacto mediante campos magnéticos en la gama de frecuencias de 13,56 MHz a corta distancia (de hasta aprox. 20 cm) y permite a los aparatos actuar, no solo como tarjeta sin contacto, sino también como lector de tarjetas. Actualmente se pueden lograr tasas de transferencia de datos de 424 KB/s. Hasta ahora se ha impedido una extensa aplicación de la tecnología en áreas de aplicación sensibles a la seguridad por el hecho de que el estándar NFC en sí mismo no prevé ninguna medida de seguridad. Una NFC segura, realizada en combinación con aparatos NFC según el estándar con módulos de seguridad como, por ejemplo, Embedded Security Controller, tarjetas SIM, Secure Flash Cards y similares, permite una pluralidad de aplicaciones, entre otras, funciones de pago, control de acceso, Digital Rights Management (DRM), control de identidad, descarga de contenidos, ticketing, configuración de aparatos y similares. Es posible instalar y gestionar varias aplicaciones NFC independientemente entre sí dentro de un módulo de seguridad de un dispositivo terminal de telecomunicación.

A continuación, en base a las figuras 6 y 7 se describe un sistema para gestionar módulos de seguridad en dispositivos terminales de telecomunicación compatibles con NFC a través de una interfaz aérea (OTA, Over The Air), que a continuación se denomina OTA Secure Chip Management System. Para describir el sistema completo, la figura 6 muestra el ciclo de vida de un módulo de seguridad, dividido en diez fases. Una vez que se ha producido el módulo de seguridad (fase 1), en la fase 2 tiene lugar la individualización, en la que, por ejemplo, se incorpora la clave ISD inicial (ISD, issuer security domain) en el módulo de seguridad y este recibe un ID inequívoco. En la fase 3 se instala el módulo de seguridad en un dispositivo terminal. La personalización con respecto al operador de red, tal como se ha descrito anteriormente, tiene lugar en la fase 4, antes de que, en la fase 5, en la denominada fase de activación, tengan lugar preparaciones para incorporar nuevas aplicaciones, en particular, aplicaciones NFC, en el módulo de seguridad. En la fase 6 se instala entonces el software de aplicación correspondiente en el módulo de seguridad y se adapta al usuario, antes de que pueda comenzar la fase 7 como fase de uso. En la fase 8 tienen lugar las adaptaciones eventuales de las aplicaciones o se instalan aplicaciones nuevas que se comienza a utilizar en la fase 9, una fase de uso adicional (siendo posible cambiar múltiples veces entre las fases 8 y 9), antes de que finalice el ciclo de vida del módulo de seguridad en la fase 10.

A continuación se describen en detalle las fases 5, 6 y 8, en las que se utiliza el OTA Secure Chip Management System. La realización técnica de la transferencia de datos entre un proveedor -1001- de servicios y un módulo -301- de seguridad de un dispositivo -201- terminal de telecomunicación tiene lugar preferentemente tal como se ha descrito anteriormente en el ejemplo de realización preferente en relación con las figuras 3 a 5.

La figura 7 muestra la arquitectura de sistema completa, en la que está previsto que un Card Application Management Server (CAMS) -601-, que está alojado en un centro -401- de confianza de un proveedor -1001- de servicios, se comunique directamente con el módulo -301- de seguridad de un dispositivo -201- terminal de telecomunicación compatible con NFC, que comprende un módulo -250- NFC, para configurar el módulo de seguridad para aplicaciones de uno o varios proveedores -701-, -711-, -721- de aplicaciones. Esta comunicación tiene lugar a través de una red -800- de telefonía móvil, exclusivamente a través de una interfaz aérea. Después de que los datos -101- de identificación, que están disponibles para el usuario fuera del dispositivo terminal de telecomunicación, han sido incorporados de una de las formas anteriormente descritas en el dispositivo -201- terminal de telecomunicación en la fase de personalización (fase 4), el módulo -301- de seguridad se puede activar en la fase 5.

Activación (fase 5)

En este paso, el módulo -301- de seguridad se prepara para los requisitos de una o varias aplicaciones específicas. La clave ISD inicial (ISD, issuer security domain), que fue incorporada durante la fase 2 en el módulo -301- de seguridad, se intercambia por la clave ISD específica del proveedor de servicios a través de una interfaz aérea. De este modo, el módulo -301- de seguridad reconoce que los datos enviados por el proveedor -1001- de servicios pueden aceptarse e instalarse. La misma clave también se introduce en una base -501- de datos de gestión de dispositivos del proveedor -1001- de servicios.

Instalación de nuevas zonas de proveedores de aplicaciones (en la fase 6)

En este paso, para cada proveedor -701-, -711-, -721- de aplicaciones seleccionado por el usuario se reservan zonas propias, denominadas SSD (supplementary security domains), en el módulo -301- de seguridad y se equipan respectivamente con una clave SSD propia, que también se almacena en la base -501- de datos de gestión de dispositivos del proveedor -1001- de servicios. Estas zonas se pueden considerar “contenedores seguros”, en los cuales las aplicaciones correspondientes están almacenadas contra el acceso externo y se pueden ejecutar de forma segura. Varios proveedores -701-, -711-, -721- de aplicaciones pueden instalar en el mismo módulo -301- de seguridad sus propias SSD que pueden funcionar de forma independiente y en paralelo sin interferencias. También este paso tiene lugar a través de una interfaz aérea.

Descarga de aplicaciones (en la fase 6)

Después de que a cada proveedor -701-, -711-, -721- de aplicaciones le ha sido asignada su zona propia en el módulo -301- de seguridad, puede iniciarse la descarga del software de aplicación. Esto tiene lugar a través de una interfaz aérea y respectivamente de forma segura con la clave SSD correspondiente. Tanto el proveedor -1001- de servicios, que también se denomina Trusted Third Party (TTP) y realiza la gestión del módulo -301- de seguridad tal como se describe aquí, como también el propio proveedor -701-, -711-, -721- de aplicaciones pueden iniciar la descarga.

Personalización de la aplicación (en la fase 6)

En este paso se configura la aplicación respectiva para el usuario transfiriendo los datos de usuario adaptados a la aplicación codificados con la clave SSD respectiva al módulo -301- de seguridad. Nuevamente, tanto el TTR -1001- como también el proveedor -701-, -711-, -721- de aplicaciones pueden realizar este paso que tiene lugar a través de una interfaz aérea.

Adaptación y nuevas aplicaciones (fase 8)

Durante el funcionamiento, el módulo -301- de seguridad debe adaptarse a nuevas especificaciones de los proveedores -701-, -711-, -721- de aplicaciones y puede recibir, dado el caso, nuevas aplicaciones. El TTP -1001- o el proveedor -701-, -711-, -721- de aplicaciones pueden iniciar y realizar también esta adaptación que tiene lugar a través de una interfaz aérea.

REIVINDICACIONES

1. Procedimiento para personalizar un módulo (300) de seguridad en un dispositivo (200) terminal de telecomunicación, **caracterizado por** los siguientes pasos en el dispositivo terminal de telecomunicación:

- Recepción de una secuencia de comandos de un servidor (600) para el módulo (300) de seguridad;
- Ejecución de la secuencia de comandos **mediante**

Extracción de comandos individuales de la secuencia de comandos por parte del dispositivo (200) terminal de telecomunicación, y trasmisión de los comandos al módulo (300) de seguridad,

tal que el módulo (300) de seguridad no puede utilizarse para la autentificación en un operador (700) de red antes de la personalización, y
- la secuencia de comandos transfiere datos de personalización del usuario específicos del operador de red, tal que
- al ejecutar la secuencia de comandos en el dispositivo (200) terminal de telecomunicación se reciben las respuestas de comando del módulo (300) de seguridad y
- el procedimiento de personalización finaliza con el envío de la última respuesta de comando del módulo (300) de seguridad al servidor (600).

2. Procedimiento, según la reivindicación 1, **caracterizado por que** el dispositivo (200) terminal de telecomunicación se establece en un modo de personalización.

3. Procedimiento, según cualquiera de las reivindicaciones 1 o 2, **caracterizado por que** el servidor (600) prepara los datos a transmitir al módulo (300) de seguridad como secuencia de comandos.

4. Procedimiento, según cualquiera de las reivindicaciones 1 a 3, **caracterizado por que** el servidor (600) evalúa la respuesta de comando transferida; y

• finaliza la comunicación con el dispositivo (200) terminal de telecomunicación si todos los datos han sido transferidos correctamente y ya no hay más datos para transferir, o
• finaliza la comunicación con el dispositivo (200) terminal de telecomunicación si durante la transferencia de la última secuencia de comandos ha ocurrido un fallo no solucionable, o
• vuelve a enviar la misma secuencia de comandos, comenzando con el paso parcial i., si durante la transferencia de la última secuencia de comandos ha ocurrido un fallo solucionable, o
• envía otra secuencia de comandos, comenzando con el paso parcial i., si la última secuencia de comandos ha sido transferida correctamente y aún se deben transferir otros datos.

5. Procedimiento, según la reivindicación 4, **caracterizado por que** la secuencia de comandos se transfiere en un bloque al dispositivo (200) terminal de telecomunicación, tal que al servidor (600, 400) le basta con una respuesta del dispositivo (200) terminal de telecomunicación al último comando de la secuencia para comprobar que la transferencia del bloque completo ha tenido lugar correctamente.

6. Procedimiento, según cualquiera de las reivindicaciones 4 o 5, **caracterizado por que** la transmisión de los comandos al módulo de seguridad tiene lugar mediante transmisión secuencial de comandos individuales, tal que la comprobación de que la transmisión de los comandos individuales ha tenido lugar correctamente tiene lugar en base a una respuesta del módulo (300) de seguridad a cada comando individual, y **por que** la transmisión de los comandos se interrumpe si ya no hay ningún comando para transmitir o la transmisión no ha tenido lugar correctamente.

7. Procedimiento, según cualquiera de las reivindicaciones 1 a 6, **caracterizado por que** como dispositivo (200) terminal de telecomunicación se utiliza un dispositivo terminal compatible con J2ME con JavaCard integrada.

8. Procedimiento, según cualquiera de las reivindicaciones 1 a 7, **caracterizado por que** la comunicación del servidor (600, 400) con el módulo (300) de seguridad tiene lugar a través de una unidad (900) instalada en el dispositivo terminal, en particular, en forma de un MIDlet.

9. Procedimiento, según cualquiera de las reivindicaciones 1 a 8, **caracterizado por que** las conexiones del dispositivo (200) terminal al servidor (400, 600), por un lado, y al módulo (300) de seguridad, por el otro lado, se realizan en hilos de ejecución independientes.

10. Procedimiento, según cualquiera de las reivindicaciones 1 a 9, **caracterizado por que** la secuencia de comandos se codifica en XML.

11. Procedimiento, según cualquiera de las reivindicaciones 1 a 10, **caracterizado por que** el dispositivo (200) terminal de telecomunicación es un teléfono móvil o un PDA (Personal Digital Assistent).

12. Procedimiento, según cualquiera de las reivindicaciones 1 a 11, **caracterizado por que** la secuencia de comandos comprende para cada comando una respuesta esperada del módulo de seguridad al comando.

13. Procedimiento, según cualquiera de las reivindicaciones anteriores, **caracterizado por que**

- el módulo de seguridad se integra (3) en el dispositivo (200) terminal de telecomunicación; y
- se personaliza (4) con ayuda de la al menos una secuencia de comandos.

14. Procedimiento, según cualquiera de las reivindicaciones anteriores, **caracterizado por que** antes de una fase de uso (7, 9) se intercambia (5) una clave ISD inicial (ISD, issuer security domain) por una clave ISD específica del proveedor de servicios.

15. Procedimiento, según cualquiera de las reivindicaciones anteriores, **caracterizado por que** antes de una fase de uso (7, 9) se incorpora al menos una nueva aplicación, en particular, una aplicación NFC, en el módulo de seguridad, tal que para los proveedores de aplicaciones (701, 711, 721) se reservan zonas propias en el módulo (301) de seguridad y se equipan respectivamente con una clave propia.

16. Dispositivo terminal de telecomunicación configurado para ejecutar un procedimiento según cualquiera de las reivindicaciones 1 a 15.

FIG 1

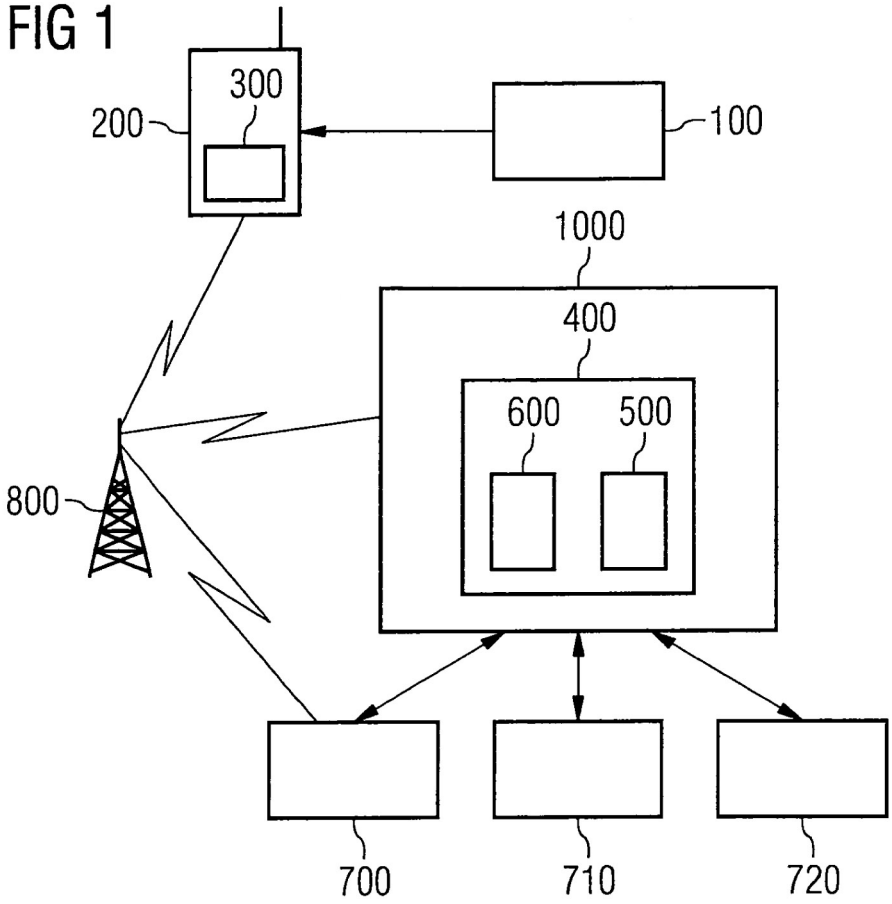

FIG 2

```
-<APDUList>
    -<APDU>
        <ID>1</ID>
        <Value>00 A4 00 0C 02 3F 00</Value>
        <ExpectedResponse>90 00</ExpectedResponse>
    </APDU>
-<APDU>
    <ID>2</ID>
    <Value>00 84 00 00 00</Value>
    <ExpectedResponse>90 00</ExpectedResponse>
</APDU>
-<APDU>
    <ID>3</ID>
    <Value>80 F6 00 00 00</Value>
    <ExpectedResponse>90 00</ExpectedResponse>
    </APDU>
</APDUList>
```

FIG 3

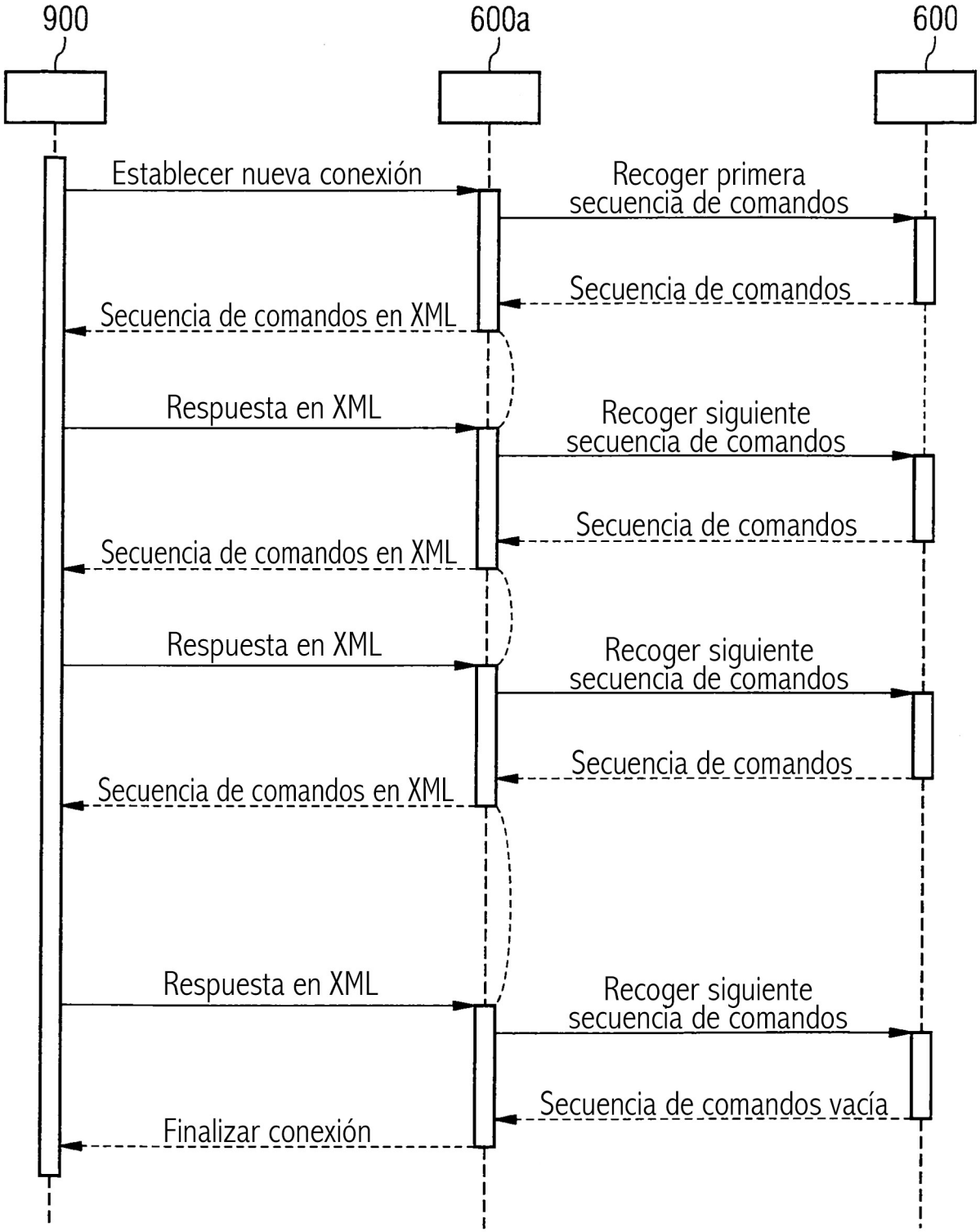
900
600a
600
Establecer nueva conexión
Recoger primera secuencia de comandos
Secuencia de comandos
Secuencia de comandos en XML
Respuesta en XML
Recoger siguiente secuencia de comandos
Secuencia de comandos
Secuencia de comandos en XML
Respuesta en XML
Recoger siguiente secuencia de comandos
Secuencia de comandos
Secuencia de comandos en XML
Respuesta en XML
Recoger siguiente secuencia de comandos
Secuencia de comandos vacía
Finalizar conexión

FIG 4

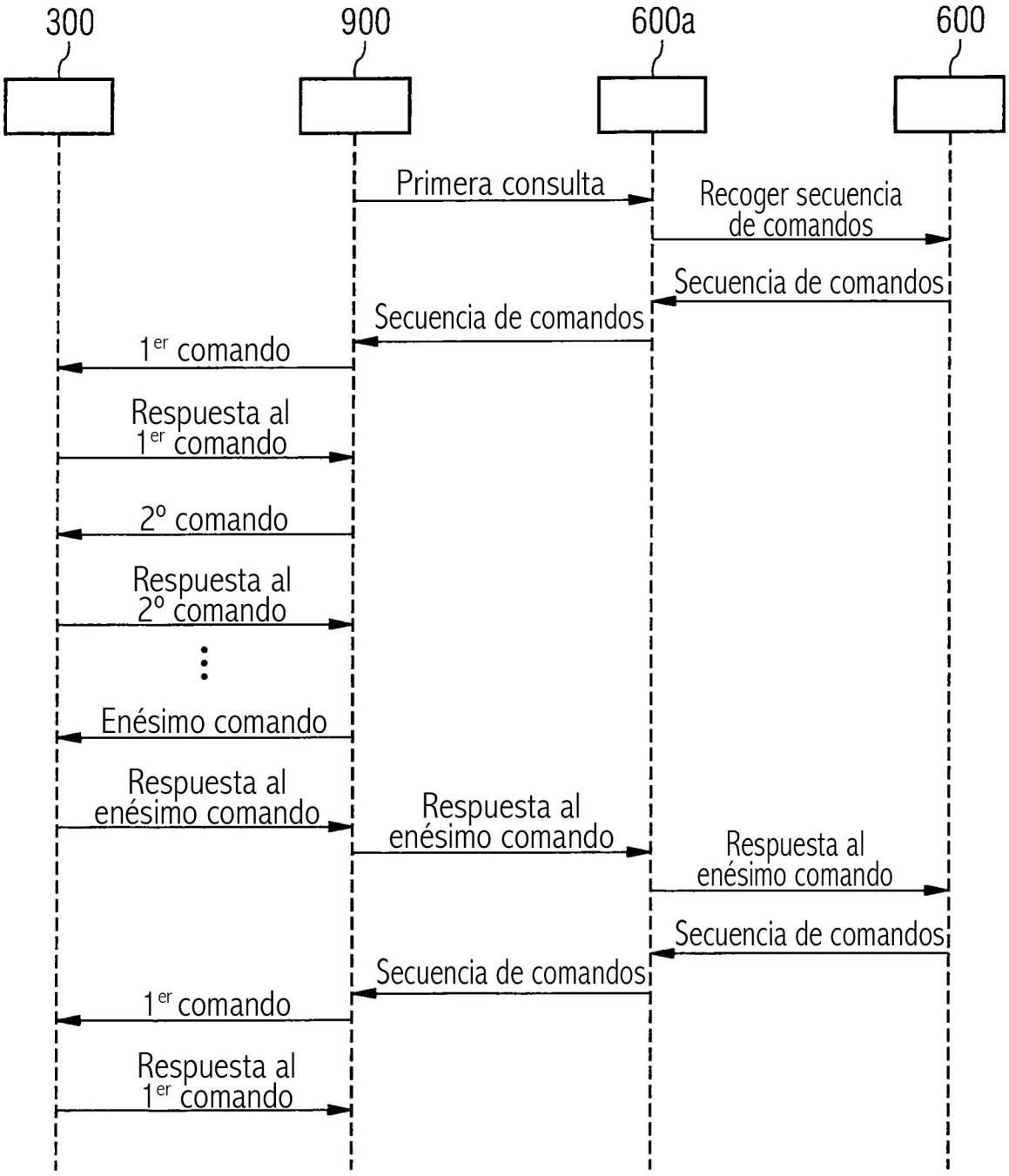
300
900
600a
600
Primera consulta
Recoger secuencia de comandos
Secuencia de comandos
Secuencia de comandos
1er comando
Respuesta al 1er comando
2º comando
Respuesta al 2º comando
Enésimo comando
Respuesta al enésimo comando
Respuesta al enésimo comando
Respuesta al enésimo comando
Secuencia de comandos
Secuencia de comandos
1er comando
Respuesta al 1er comando

FIG 5

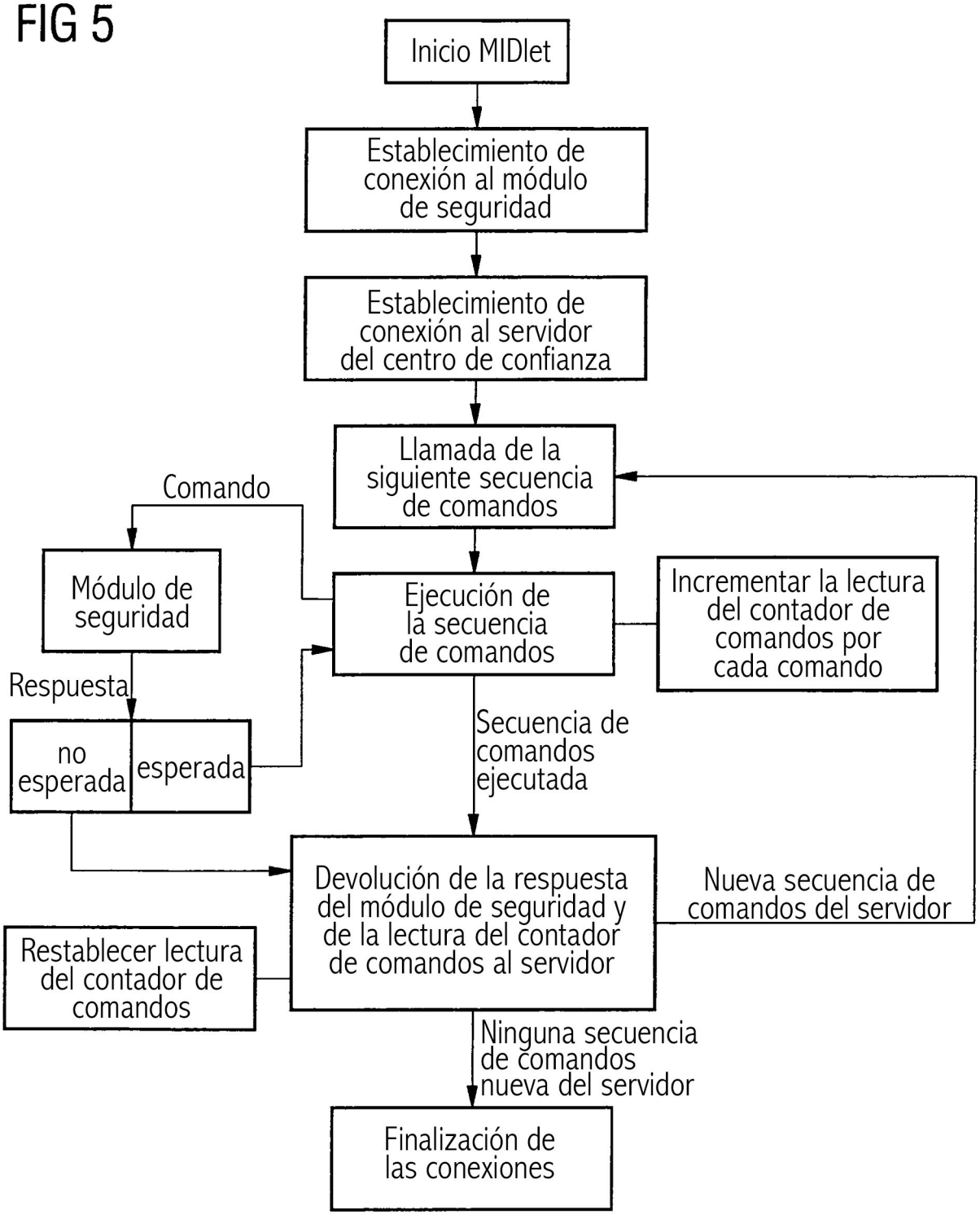
Inicio MIDlet
Establecimiento de conexión al módulo de seguridad
Establecimiento de conexión al servidor del centro de confianza
Llamada de la siguiente secuencia de comandos
Comando
Módulo de seguridad
Ejecución de la secuencia de comandos
Incrementar la lectura del contador de comandos por cada comando
Respuesta
no esperada
esperada
Secuencia de comandos ejecutada
Devolución de la respuesta del módulo de seguridad y de la lectura del contador de comandos al servidor
Nueva secuencia de comandos del servidor
Restablecer lectura del contador de comandos
Ninguna secuencia de comandos nueva del servidor
Finalización de las conexiones

FIG 6

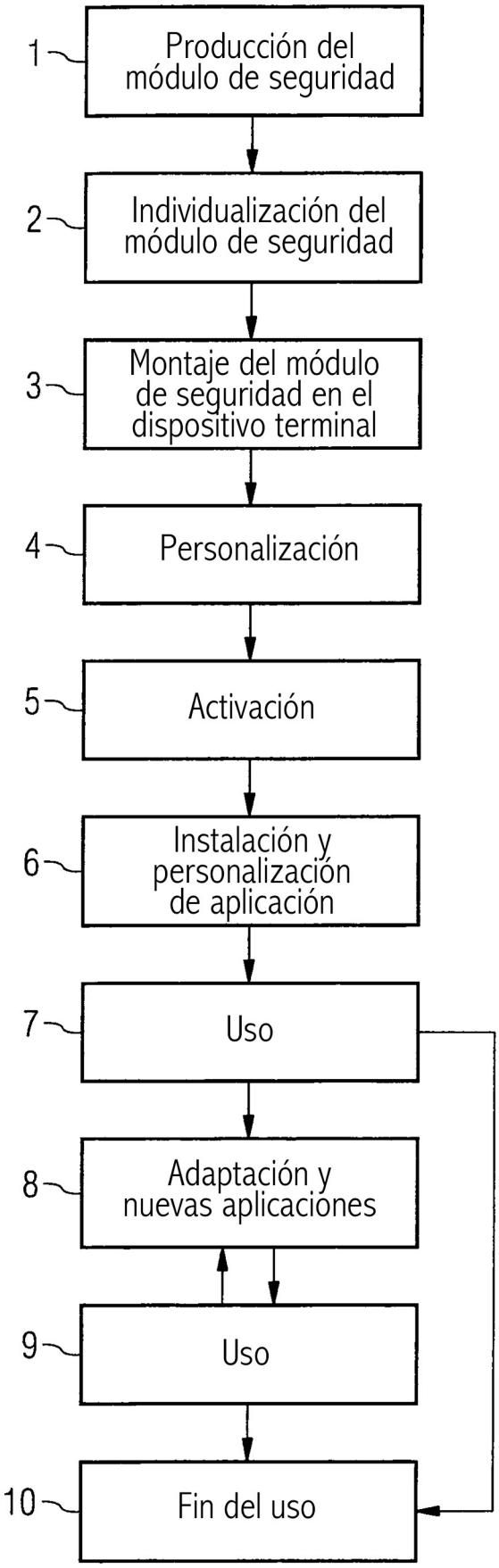
1
Producción del módulo de seguridad
2
Individualización del módulo de seguridad
3
Montaje del módulo de seguridad en el dispositivo terminal
4
Personalización
5
Activación
6
Instalación y personalización de aplicación
7
Uso
8
Adaptación y nuevas aplicaciones
9
Uso
10
Fin del uso

FIG 7