(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 623 702**

(51) Int. CI.:

H04W 12/12 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **12.08.2013 PCT/EP2013/002419**

(87) Fecha y número de publicación internacional: **20.02.2014 WO2014026760**

(96) Fecha de presentación y número de la solicitud europea: **12.08.2013 E 13750850 (3)**

(97) Fecha y número de publicación de la concesión europea: **18.01.2017 EP 2885907**

(54) Título: **Procedimiento para la instalación de aplicaciones relevantes para la seguridad en un elemento de seguridad de un terminal**

(30) Prioridad:

14.08.2012 DE 102012016164

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.07.2017

(73) Titular/es:

GIESECKE & DEVRIENT GMBH (100.0%)
Prinzregentenstrasse 159
81677 München, DE

(72) Inventor/es:

SCHÄFER, FRANK;
ALBERT, DANIEL;
DIETZE, CLAUS;
LUYKEN, JOHANNES;
SCHEDEL, RALF y
SCHUSTER, HELMUT

(74) Agente/Representante:

DURÁN MOYA, Luis Alfonso

DESCRIPCIÓN

Procedimiento para la instalación de aplicaciones relevantes para la seguridad en un elemento de seguridad de un terminal

La presente invención se refiere a un procedimiento para la instalación de una parte relevante para la seguridad de una aplicación en un elemento de seguridad de un terminal portátil, un elemento de seguridad correspondiente, así como un terminal portátil con un elemento de seguridad de este tipo.

La funcionalidad de terminales portátiles, como, por ejemplo, terminales móviles, teléfonos móviles inteligentes, tabletas y similares, se puede ampliar por medio de la instalación de funcionalidades de software, las llamadas “aplicaciones” o “apps”. Diferentes aplicaciones de este tipo sirven, en este caso, para aplicaciones que también comprenden y/ o procesan datos relevantes para la seguridad. Los datos relevantes para la seguridad pueden ser, en este caso, por ejemplo, datos personales de un usuario del terminal que han de mantenerse en secreto, por ejemplo, datos biométricos, o datos que se usan para llevar a cabo transacciones financieras, como, por ejemplo, números de tarjetas de crédito, datos de cuentas, contenido de bolsas electrónicas, claves criptográficas, etc. Por “parte relevante para la seguridad de una aplicación” se entiende, en relación con la presente invención, tanto los datos relevantes para la seguridad comprendidos o procesados por la aplicación como también funcionalidades (parciales) de la aplicación que sirven para el procesamiento de estos datos.

Se conoce el proteger este tipo de partes relevantes para la seguridad de una aplicación frente a manipulaciones y accesos no autorizados haciendo que estas partes se almacenen o se instalen en el terminal en una zona especialmente asegurada.

Estas zonas aseguradas adecuadas representan, en particular, elementos de seguridad que se pueden integrar o que se pueden montar de modo fijo en un terminal. Los elementos de seguridad integrables desmontables son, por ejemplo, las tarjetas SIM/UICC de telefonía móvil, tarjetas multimedia seguras o elementos similares. Como elementos de seguridad incorporados en el terminal pueden servir, por ejemplo, tarjetas de telefonía móvil SIM/UICC integradas, TPM (“Trusted Platform Modules”) o módulos NFC. Finalmente, también pueden servir como elementos de seguridad los entornos de ejecución seguros dentro de una arquitectura de hardware específica del terminal, por ejemplo, dentro de una arquitectura ARM de “TrustZone”, como, por ejemplo, un “Trusted Execution Environment” según la especificación de “Global Platform”.

Una instalación de datos y/o de aplicaciones o partes de aplicaciones en un elemento de seguridad de este tipo está asegurada, por regla general, de modo criptográfico. Cada vez más, partes relevantes para la seguridad de aplicaciones instaladas en terminales móviles se ejecutan con ayuda de instancias de confianza, los denominados “Trusted Service Manager” (denominados en los sucesivo “TSM”). Estos, como prestadores de servicio, reciben las partes relevantes para la seguridad y ejecutan el proceso de instalación, es decir, la instalación segura de las partes en el elemento de seguridad. En lo sucesivo, en este contexto se usa la formulación según la cual el TSM “administra” el elemento de seguridad. Antes del paso de la instalación, se intercambian claves criptográficas entre el TSM y la institución que proporciona la aplicación, por ejemplo, un banco en el caso de una aplicación de pago que se haya de personalizar, y se introducen en el elemento de seguridad de un modo asegurado. Por medio de estas claves se puede asegurar el proceso de instalación de modo criptográfico.

Se ha de tener en cuenta que un elemento de seguridad del tipo descrito anteriormente puede comprender una pluralidad de zonas aseguradas. Es decir, por ejemplo, una tarjeta SIM puede comprender, como elemento de seguridad físico, una pluralidad de zonas aseguradas en una memoria de la tarjeta. En particular, estas zonas aseguradas pueden presentarse a modo de “Security Domains” según la especificación de Global Platform (véase, por ejemplo, Global Platform, Card Specification, versión 2.2). Un “Security Domain” de este tipo está asignado por regla general a una instancia externa prefijada, por ejemplo, al editor del soporte de datos, a un operador de red, a un proveedor de aplicaciones o similar. Esta instancia también se designa en lo sucesivo como “propietario” del “Security Domain”. De modo análogo, en lo sucesivo también se habla de un “propietario” de un elemento de seguridad cuando se ha de designar la instancia a la que está asignada el elemento de seguridad. El propietario del elemento de seguridad es responsable, en particular, de la arquitectura de claves del elemento de seguridad.

Un “Security Domain” representa una aplicación privilegiada que dispone de una arquitectura de claves criptográficas propia. Esto hace posible, en particular, la instalación asegurada de datos y de aplicación en la zona administrada por el “Security Domain” de una memoria del soporte de datos o del módulo de seguridad correspondiente. Los “Security Domains” pueden presentarse de un modo dispuesto jerárquicamente sobre un elemento de seguridad. En particular, se pueden administrar diferentes “Security Domains” sobre un elemento de seguridad físico, por ejemplo, una tarjeta SIM, del modo descrito anteriormente para la instalación de partes relevantes para la seguridad de una aplicación por medio de diferentes TSM.

En el procedimiento descrito para la instalación de partes relevantes para la seguridad de una aplicación en un elemento de seguridad resulta desventajoso el hecho de que un desarrollador que programa aplicaciones y las ofrece a través de un proveedor de aplicaciones, por ejemplo, a través de un denominado “AppStore” para que sean

descargadas en un terminal, no pueda ofrecer de esta manera prácticamente ninguna aplicación con partes relevantes para la seguridad. Debido a ello, se limita y se dificulta de modo considerable el desarrollo libre de aplicaciones con partes relevantes para la seguridad.

Esto es así ya que una instalación de partes relevantes para la seguridad en un elemento de seguridad del terminal hasta ahora solo es posible en cooperación con el TSM correspondiente del elemento de seguridad. Este TSM, sin embargo, por regla general no es conocido por el desarrollador, en particular, ya que a día de hoy existe un gran número de TSM. Además, diferentes usuarios de terminales pueden prever, para la administración de un elemento de seguridad en cada caso que está previsto fundamentalmente para la instalación de la misma aplicación o su parte relevante para la seguridad, diferentes TSM, cada uno de ellos para la administración de los elementos de seguridad correspondientes. Finalmente, un desarrollador de una aplicación no tiene ningún acceso y ninguna influencia sobre la arquitectura de claves de un elemento de seguridad de un terminal de un usuario aleatorio que desee bajar e instalar la aplicación a través de una “AppStore”, es decir, sin interacción directa con el desarrollador. Es decir, incluso si el desarrollador, en el caso concreto, conociera y pudiera ponerse en contacto con el TSM competente, no se podría llevar a cabo una instalación de datos en el elemento de seguridad. Por parte del desarrollador se podrían intercambiar claves criptográficas con el TSM, sin embargo, no sería posible para el desarrollador introducir estas claves en el elemento de seguridad ya que este no tiene ningún acceso a un elemento de seguridad de este tipo.

El documento EP 1076279 A1 muestra un módulo TPM en un PC que comprueba la huella digital y una firma de un software que se ha de instalar en un PC. Para un cliente de transferencia de ficheros se propone, en el documento US2005/0132227A1, una interfaz común para las diferentes unidades de comprobación, tales como unidades de comprobación de virus o de firmas.

El objetivo de la presente invención es hacer posible de un modo sencillo y seguro una instalación de una aplicación proporcionada por un proveedor de aplicaciones cualquiera con una parte relevante para la seguridad en un terminal portátil con un elemento de seguridad integrado en este.

Este objetivo se consigue por medio de un procedimiento, un elemento de seguridad, así como un terminal portátil con elemento de seguridad con las características de las reivindicaciones independientes. En las reivindicaciones dependientes se indican perfeccionamientos y configuraciones ventajosas.

La presente invención se basa en la idea básica de que la parte relevante para la seguridad de la aplicación no es transmitida por el desarrollador al TSM y después se instala en el elemento de seguridad, sino que se envía al terminal conjuntamente con el resto de partes de la aplicación que no son relevantes para la seguridad y que han de ser instaladas en el terminal. La transmisión de la parte relevante para la seguridad de la aplicación enviada al TSM correspondiente se realiza desde el terminal. El TSM instala el resto de la parte relevante para la seguridad de la aplicación que se ha enviado en el elemento de seguridad. La transmisión al TSM se puede realizar a través del terminal o a través del propio elemento de seguridad. Una determinación (selección) del TSM correspondiente se realiza con ayuda de las informaciones almacenadas en el elemento de seguridad y /o en el terminal (selección de datos).

De este modo, por un lado, el desarrollador -independientemente del elemento de seguridad y de su propietario, así como independientemente del TSM correspondiente que administra el elemento de seguridad en el que se ha de instalar la parte relevante para la seguridad- puede ofrecer la aplicación completa. Ya no se requiere una coordinación -necesaria según el procedimiento que existía hasta el momento- del fabricante de la parte de la aplicación relevante para la seguridad, a saber, el desarrollador, con el TSM, en particular, por lo que se refiere a las claves criptográficas necesarias para la instalación en el elemento de seguridad. Estas están ya disponibles -como consecuencia de la relación ya existente del propietario del elemento de seguridad con el TSM que administra el elemento de seguridad- tanto en el elemento de seguridad como en el TSM. De este modo, la instalación de la parte relevante para la seguridad de la aplicación se puede realizar -ahora independientemente del desarrollador y del proveedor de aplicación- interactuando el elemento de seguridad con el TSM.

En concreto, un procedimiento conforme a la invención para la instalación de una parte relevante para la seguridad de una aplicación proporcionada por un desarrollador a través de un proveedor de aplicaciones en un elemento de seguridad de un terminal portátil comprende los siguientes pasos: el terminal solicita la aplicación al proveedor de aplicaciones y, a continuación, recibe la aplicación, como resultado de la solicitud, del proveedor de aplicaciones. La aplicación puede descargarse mediante el terminal, por ejemplo, desde un portal de internet del proveedor de aplicaciones. Por regla general, el terminal recibe la aplicación ya en una forma en la que la parte relevante para la seguridad y las partes no relevantes para la seguridad se presentan separadas. En otro caso, el terminal o el elemento de seguridad del terminal pueden estar configurados para determinar la parte relevante para la seguridad de la aplicación y, dado el caso, separarla del resto de partes.

En otro paso, se transmite la parte relevante para la seguridad de la aplicación a una instancia de confianza que administra el elemento de seguridad, por ejemplo, un TSM. Este paso puede llevarlo el módulo de seguridad y/o el terminal. Una transmisión de este tipo se puede llevar a cabo, por ejemplo, a través de Internet o a través de una red de comunicaciones móviles, por ejemplo, por SMS. El elemento de seguridad que está integrado en el terminal se

puede usar para la transmisión de estos datos a interfaces de comunicación de datos del terminal, por ejemplo, por medio de un SIM Toolkit.

Finalmente, la instancia de confianza instala la parte relevante para la seguridad de la aplicación en el elemento de seguridad. La instancia de confianza puede preparar la parte relevante para la seguridad de la aplicación antes de la instalación en el elemento de seguridad de un modo adecuado, por ejemplo, por lo que se refiere a un formato de instalación, diferentes especificaciones de seguridad o similares.

Según esto, un elemento de seguridad conforme a la invención para un terminal portátil se configura cuando se integra en el terminal portátil para transmitir una parte relevante para la seguridad de una aplicación recibida por el terminal a una instancia de confianza que administra el elemento de seguridad.

Finalmente, un terminal portátil conforme a la invención comprende un elemento de seguridad conforme a la invención, integrado de modo que se puede desmontar o montado de modo fijo, y está configurado para soportar un procedimiento conforme a la invención del modo descrito.

Usando un terminal de este tipo y por medio del procedimiento conforme a la invención, se puede realizar de un modo sencillo y seguro una instalación de una aplicación proporcionada por un desarrollador cualquiera a través de un proveedor de aplicaciones, instalándose una parte relevante para la seguridad de la aplicación en el elemento de seguridad del terminal.

Preferentemente, la parte relevante para la seguridad de la aplicación se comprueba antes de instalarse en el elemento de seguridad. Una comprobación de este tipo resulta útil e incrementa la seguridad del procedimiento en especial cuando la parte relevante para la seguridad comprende código ejecutable o interpretable que se ha de ejecutar en el elemento de seguridad. No obstante, también se pueden comprobar datos no ejecutables, por ejemplo, datos de personalización.

Una comprobación se puede referir a diferentes aspectos en cada caso. Conjuntamente con código ejecutable, se puede comprobar, por ejemplo, si la parte relevante para la seguridad es compatible con el elemento de seguridad, por ejemplo, para un procesador y/ o un intérprete del elemento de seguridad, un sistema operativo del elemento de similar y elementos similares. También puede ser objeto de la comprobación el cumplimiento de especificaciones técnicas, por ejemplo, si los comandos usados son suficientes para una especificación dada. Además, se puede comprobar la parte relevante para la seguridad en cuanto se refiere a la funcionalidad proporcionada por dicha parte, en particular, también en el sentido de si la parte relevante para la seguridad comprende código dañino. Otros aspectos de seguridad, por ejemplo, la susceptibilidad de la parte relevante para la seguridad ante ataques conocidos a elementos de seguridad, tales como, por ejemplo, los denominados “ataques de canal lateral”, pueden ser comprobados alternativa o adicionalmente.

Conjuntamente con código ejecutable o no ejecutable, puede tener lugar, por ejemplo, una comprobación en relación con la integridad y/o autenticidad de los datos correspondientes. Para ello se puede usar métodos conocidos, tales como, por ejemplo, sumas de comprobación, los denominados “Message Authentication Codes” o bien certificados, por ejemplo, basados en una arquitectura asimétrica de claves.

Una comprobación de este tipo se puede realizar a través de diferentes posiciones. Por un lado, la instancia de confianza puede comprobar la parte relevante para la seguridad. Una comprobación de este tipo tiene lugar antes de la instalación de la parte en el elemento de seguridad. Una instalación se realiza solo cuando la comprobación ha discurrido de modo exitoso, es decir, cuando la parte relevante para la seguridad de la aplicación satisface requisitos predeterminados que se han comprobado en el marco de la comprobación.

Del mismo modo, la comprobación también se puede realizar a través de una instancia de comprobación externa, por ejemplo, un organismo de certificación de software, el editor del elemento de seguridad, el proveedor de la aplicación o instancias similares. Para ello, el desarrollador, antes de proporcionar la aplicación para que sea descargada a través del proveedor de aplicaciones, puede presentar la parte relevante para la seguridad de la aplicación a la instancia de comprobación o al organismo de certificación. Este comprueba la parte y la dota, una vez realizada la comprobación con resultado satisfactorio, de un certificado correspondiente.

En caso de que la parte relevante para la seguridad -cuando es recibida por la instancia de confianza- comprenda ya un certificado de este tipo de un organismo de certificación, entonces el paso de comprobación por medio de la instancia de confianza puede consistir únicamente en la verificación del certificado. No obstante, de forma alternativa o adicional, en caso de existir el certificado, la instancia de confianza también puede llevar a cabo comprobaciones propias.

El procedimiento conforme a la invención puede considerarse especialmente seguro si el certificado con el que se ha certificado la parte relevante para la seguridad que se ha de instalar en el elemento de seguridad procede de la instancia que representa al mismo tiempo al propietario del elemento de seguridad. En el caso de una tarjeta de comunicaciones móviles SIM/ UICC, este podría ser el editor del elemento de seguridad. Del mismo modo, el

proveedor de aplicaciones podría ser al mismo tiempo el propietario del elemento de seguridad, y la instancia de comprobación, en particular, podría ser el propietario de un “Security Domain” en un módulo de seguridad físico, desempeñando el “Security Domain” el papel de un elemento de seguridad en el sentido de la presente invención. Normalmente, únicamente este propietario es el que hace posible una instalación de la parte relevante para la seguridad en el elemento de seguridad por medio de la instancia de confianza del modo descrito a continuación.

Como ya se ha mencionado, el paso de la instalación de la parte relevante para la seguridad en el elemento de seguridad se lleva a cabo por medio de la instancia de confianza, preferentemente, de modo asegurado de manera criptográfica. Las claves criptográficas usadas a tal fin se intercambian entonces, en un paso previo a la instalación, entre el propietario del elemento de seguridad y la instancia de confianza. Un juego de claves correspondiente se deposita en el elemento de seguridad.

Las partes no relevantes para la seguridad de la aplicación se instalan por regla general en el terminal, independientemente de un elemento de seguridad. Una instalación de este tipo se lleva a cabo preferentemente antes de la instalación de la parte relevante para la seguridad de la aplicación en el elemento de seguridad.

La instancia de confianza es una instancia dispuesta alejada (del terminal). La parte relevante para la seguridad de la aplicación se transmite a la instancia de confianza a través de una red.

En el caso más sencillo, en el terminal se encuentra únicamente un elemento de seguridad, en el que se puede instalar la parte relevante para la seguridad de la aplicación. En el caso de que sean adecuados varios elementos de seguridad, por ejemplo, varios “Security Domains”, para una instalación de la parte relevante para la seguridad de la aplicación, entonces la aplicación puede seleccionar uno de ellos. Una selección de este tipo se puede llevar a cabo por una parte de la aplicación no relevante para la seguridad. De modo correspondiente, la aplicación también determina, dependiendo del elemento de seguridad seleccionado, la instancia de confianza que administra el elemento de seguridad correspondiente.

En el caso de que para la administración de un elemento de seguridad -por ejemplo, del elemento de seguridad seleccionado del modo descrito- esté disponible una pluralidad de instancias de confianza, entonces la aplicación puede seleccionar nuevamente una de ellas y, de este modo, determinar qué instancia de confianza ha de instalar la parte relevante para la seguridad de la aplicación en el elemento de seguridad. Sin embargo, también puede estar previsto que un elemento de seguridad seleccionado -o bien un elemento de seguridad existente como único elemento de seguridad adecuado en el caso de una pluralidad de instancias de confianza disponibles para este elemento de seguridad- seleccione, por ejemplo, en función de la aplicación, una instancia de este tipo para la administración en conexión con dicha aplicación.

Una vez que se hayan determinado del modo descrito anteriormente el elemento de seguridad en el que se ha de instalar la parte relevante para la seguridad y la instancia de confianza que administra en este caso concreto este elemento de seguridad, el elemento de seguridad transmite la parte relevante para la seguridad de la aplicación a la instancia de confianza. Ya se ha descrito la instalación que se ha de realizar en un paso posterior.

Como se ha mencionado ya, el término “elemento de seguridad” en el contexto de la presente invención comprende, por un lado, un elemento o unos módulos de seguridad físicos que, o bien se pueden integrar de modo que se pueden desmontar en un terminal portátil, o bien están montados en este de modo fijo. Por otro lado, un “elemento de seguridad” en el sentido de la invención también puede ser sencillamente una zona asegurada de modo lógico en una memoria de un elemento o módulo de seguridad físico. En este caso, un módulo de seguridad físico puede comprender una pluralidad de este tipo de zonas aseguradas, es decir, “elementos de seguridad” lógicos de este tipo. En el contexto de la presente invención solo resulta fundamental que permita al elemento de seguridad instalar partes de la aplicación relevantes para la seguridad de modo seguro, es decir, en particular, protegidas frente a accesos no autorizados, sea por medio de lectura, ejecución o manipulación de otro tipo.

En la clase de los elementos de seguridad que se pueden integrar en un terminal se incluyen soportes de datos de seguridad portátiles conocidos, en particular, tarjetas de comunicaciones móviles SIM/UICC, tarjetas multimedia seguras o elementos similares. La clase de los elementos de seguridad montados de modo fijo en un terminal comprende, por ejemplo, las denominadas tarjetas de comunicaciones SIM/UICC incrustadas, TPM, módulos NFC y elementos similares. Del mismo modo, por “montado de modo fijo” se han de entender entornos de ejecución seguros dentro de una arquitectura de hardware específica del terminal, por ejemplo, un “Trusted Execution Environment” según la especificación de “Global Platform”. Los elementos de seguridad lógicos del tipo mencionado anteriormente se proporcionan, en particular, por medio de “Security Domains” según la especificación de “Global Platform”.

Como terminales portátiles conformes a la invención están indicados, en particular, terminales de comunicaciones móviles, teléfonos móviles inteligentes, tabletas, netbooks, ordenadores portátiles, dispositivos multimedia inteligentes (Smart TV, Set-Top-Box…), Smart Meter o dispositivos similares, que están configurados para alojar un elemento de seguridad conforme a la invención o en los que ya está implementado o montado de modo fijo un elemento de seguridad conforme a la invención.

La invención se describe a continuación a título de ejemplo haciendo referencia a los dibujos adjuntos. En estos muestran lo siguiente:

Figura 1, un sistema que comprende un terminal con elemento de seguridad, un proveedor de aplicaciones y un TSM,

Figura 2, pasos de una forma de realización preferida de un procedimiento conforme a la invención.

La figura 1 muestra un sistema que comprende un terminal -1-, un proveedor de aplicaciones -2- y un TSM -3-. La comunicación entre los componentes del sistema se realiza a través de una red -4-.

El proveedor de aplicaciones -2- ofrece en Internet diferentes aplicaciones para descargar en los terminales. Los TSM administran elementos de seguridad en terminales. El TSM -3- administra, en el elemento de seguridad -20-, la al menos una zona segura -23- del elemento de seguridad -20-.

A continuación, se parte de un terminal -1- en forma de un teléfono móvil inteligente que está conectado de modo correspondiente, por ejemplo, a través de una red de comunicaciones móviles, con el TSM -3- y, con un proveedor de aplicaciones -2-, por ejemplo, a través de Internet. De forma alternativa, el terminal -1- también puede estar configurado, por ejemplo, como un terminal de telefonía móvil, una tableta, un ordenador portátil, un ordenador portátil ultra ligero (ultrabook), un ordenador portátil pequeño (netbook) o dispositivos similares.

El terminal -1- comprende un microprocesador -10- que está configurado para almacenar y ejecutar aplicaciones (descargables). Por ejemplo, la parte no relevante para la seguridad -201- de una aplicación descargada desde un proveedor de aplicaciones -2- se ejecuta en el procesador -10- del terminal -1-. El terminal -1- comprende un entorno de ejecución -11- para la ejecución de la parte no relevante para la seguridad -201-. La aplicación comprende la parte no relevante para la seguridad -201- y una parte relevante para la seguridad -202- que se ha de instalar en un elemento de seguridad -20-.

El terminal -1- puede comprender uno o varios elementos de seguridad -20-. Con el microprocesador -10- está conectado un elemento de seguridad -20- que, en el ejemplo mostrado, está indicado como tarjeta SIM. El elemento de seguridad -20- está integrado en el terminal -1- de modo que se puede desmontar. Alternativa o adicionalmente, podría haber también un elemento de seguridad -20- como tarjeta de memoria segura o similar. Alternativa o adicionalmente a un elemento de seguridad -20- integrado de modo que se pueda desmontar, el terminal -1- también podría estar equipado con un elemento de seguridad -20- montado de modo fijo, por ejemplo, una tarjeta de comunicaciones móviles SIM/UICC incrustada, un TPM, un módulo NFC o un elemento similar. Finalmente, también podría servir como elemento de seguridad -20- un entorno de ejecución seguro -12- dentro de una arquitectura de hardware específica del terminal -1-, por ejemplo, como “Trusted Execution Environment” según la especificación de “Global Platform”. El entorno de ejecución seguro -12- se ejecuta, junto con el entorno de ejecución normal -11-, en el procesador 10 del terminal -1-.

Un elemento de seguridad -20- puede comprender una o varias zonas seguras -23-. Las zonas seguras pueden ser, tal como se ha descrito anteriormente, “Security Domains” según la especificación de “Global Platform”. A cada elemento de seguridad está asignado un TSM que administra dicho elemento de seguridad o al menos una zona segura del elemento de seguridad. Las zonas seguras -23- son adecuadas fundamentalmente para instalar, del modo descrito posteriormente en relación a la figura 2, la parte relevante para la seguridad -202- de una aplicación.

El terminal -1- puede comprender, sin embargo, una pluralidad de elementos de seguridad -20-, -12-. Cada elemento de seguridad -20-, -12- puede comprender además, por su parte, una pluralidad de zonas seguras -23-. Diferentes elementos de seguridad pueden estar asignados a diferentes TSM. Del mismo modo, diferentes zonas seguras pueden estar asignadas a diferentes TSM. Por tanto, en el elemento de seguridad -20-, -12- está almacenada una información de asignación -21-. La información de asignación -21- indica qué TSM administra

- el elemento de seguridad del terminal,
- los elementos de seguridad del terminal,
- las zonas seguras del elemento de seguridad del terminal o
- las zonas seguras de los elementos de seguridad del terminal.

El elemento de seguridad -20- comprende finalmente una unidad de control -22-, por ejemplo, en forma de un módulo de software. La unidad de control -22- está configurada para establecer una conexión de comunicación de datos con una instancia de confianza -3- que administra el elemento de seguridad -20-. A través de esta conexión, el elemento de seguridad -20- puede transmitir entonces a la instancia de confianza -3-, por medio de la unidad de control -22-, una parte relevante para la seguridad -202- de una aplicación -200- antes de que esta se instale en el elemento de seguridad -20-, tal y como se describe posteriormente en relación con la figura 2. La unidad de control -22- puede estar configurada además para seleccionar el elemento de seguridad y/o la zona segura en la que se ha de instalar la parte relevante para la seguridad. La unidad de control -22- usa la información de asignación -21-, pero

también puede estar adaptada para generar la información de asignación -21- para todos los lugares de instalación existentes en el terminal. La unidad de control -22- puede estar realizada en el módulo de seguridad -20- o en el terminal.

La figura 2 muestra pasos de un procedimiento para la instalación de una parte relevante para la seguridad -202- de una aplicación -200- proporcionada por un proveedor de aplicaciones -2- en un elemento de seguridad -20- de un terminal -1-.

Un desarrollado cualquiera proporciona, en el paso -S0-, la aplicación -200- al proveedor de aplicaciones -2-. Es decir, el proveedor de aplicaciones -2- proporciona únicamente la infraestructura para proporcionar aplicaciones -200- para su descarga por usuarios interesados, mientras que diferentes desarrolladores que fabrican aplicaciones -200- correspondientes usan al proveedor de aplicaciones -2- como canal para distribuir las aplicaciones -200- desarrolladas por ellos. Los proveedores de aplicaciones -2- de este tipo se conocen como “AppStores”, y las aplicaciones -200- correspondientes se conocen como “Apps”.

Tal y como muestra la figura 2, la aplicación -200- comprende una parte relevante para la seguridad -202-, así como partes no relevantes para la seguridad -201-. Por regla general, el desarrollador depositará la aplicación -200- en el proveedor de aplicaciones -2- ya en una forma en la que las partes -201- y -202- estén separadas claramente. Sin embargo, también se puede prescindir totalmente de la parte no relevante para la seguridad -201- de la aplicación -200-. En este caso, la aplicación -200- está formada únicamente por una parte relevante para la seguridad -202-.

Como se ha mencionado ya, por “una parte relevante para la seguridad -202- de una aplicación” se entiende en el presente documento tanto los datos relevantes para la seguridad comprendidos o procesados por la aplicación -200- como también las funcionalidades (parciales) de la aplicación -200- que sirven para el procesado de estos datos. En este caso, los datos relevantes para la seguridad pueden ser, por ejemplo, datos personales de un usuario del terminal -1- que deben mantenerse en secreto, como, por ejemplo, datos biométricos, o datos que se usan para llevar a cabo transacciones financieras, como, por ejemplo, números de tarjetas de créditos, datos de cuentas bancarias, contenido de bolsas electrónicas, claves criptográficas, etc.

Preferentemente, la parte relevante para la seguridad -202- se comprueba al menos antes de la instalación en el elemento de seguridad -20- (véase a continuación el paso -S9-). En relación con código de programa ejecutable o interpretable que puede formar parte de la parte relevante para la seguridad -202-, se pueden comprobar diferentes aspectos. Esto se refiere, por ejemplo, a la compatibilidad de la parte relevante para la seguridad -202- con el elemento de seguridad -20-, por ejemplo, con un procesador y/ o un intérprete del elemento de seguridad -10-, un sistema operativo del elemento de seguridad -10- o similar. También puede ser objeto de la comprobación el cumplimiento de especificaciones técnicas, por ejemplo, si los comandos usados en el código son suficientes para una especificación dada. Además se puede comprobar código ejecutable/interpretable que forma parte de la parte relevante para la seguridad -202- en lo que se refiere a la funcionalidad proporcionada por dicha parte -202-. En este caso, se comprueba, en particular, si la parte relevante para la seguridad -202- comprende código dañino. Otros aspectos de seguridad, por ejemplo, la susceptibilidad de la parte relevante para la seguridad -202- frente a ataques conocidos al elemento de seguridad -20-, por ejemplo, por medio de los denominados “ataques de canal lateral”, pueden ser comprobados alternativa o adicionalmente.

En el marco de la comprobación se puede comprobar, en particular, la integridad y/o autenticidad de los datos correspondiente de las partes de la parte relevante para la seguridad -202- que no representan código ejecutable o interpretable, por ejemplo, con ayuda de sumas de comprobación, MAC o certificados, por ejemplo, basándose en una arquitectura asimétrica de claves.

Preferentemente, se realiza una comprobación de este tipo en un paso previo, no mostrado. Antes de que el desarrollador proporcione la aplicación -200- al proveedor de aplicaciones -2-, el desarrollador puede proporcionar la parte relevante para la seguridad -202- a una instancia de comprobación (no mostrada) que, como proveedor de servicios, lleva a cabo la comprobación descrita y, en caso de que la comprobación sea exitosa, marca la parte -202- como comprobada, por ejemplo, por medio de un certificado correspondiente. Una instancia de comprobación de este tipo puede ser, por ejemplo, un organismo de certificación de software independiente, el editor del elemento de seguridad -10-, o una instancia similar. Este certificado puede ser comprobado entonces de un modo sencillo por cualquier otro organismo que tenga contacto con la parte relevante para la seguridad, por ejemplo, el proveedor de aplicaciones -2-, el terminal -1-, o (véase el paso -S7-) el TSM -3-.

Alternativa o adicionalmente, el proveedor de aplicaciones -2- también puede hacer las veces de instancia de comprobación del tipo descrito. En este caso, el desarrollador puede proporcionar al proveedor de aplicaciones -2- la aplicación -200- con una parte relevante para la seguridad -202- que todavía no ha sido certificada.

De forma alternativa o adicional, la comprobación de la parte relevante para la seguridad -202- la puede realizar, o al menos verificar, el TSM -3-, tal y como se describe posteriormente (véase el paso -S7-).

Preferentemente, el terminal -1- pide la aplicación -200- al proveedor de aplicaciones -2- en -S1-. En el paso -S2-, el

terminal -1- recibe la aplicación -200- desde el proveedor de aplicaciones -2-, por ejemplo, descargando la aplicación -200- a través de un portal de internet del proveedor -2-.

A continuación, en un paso -S3-, cuando existe al menos una parte no relevante para la seguridad -201-, esta parte no relevante para la seguridad -201- se instala en el terminal -1-, es decir, en el microprocesador del terminal -1-. Esta parte -201-, una vez instalada, puede someterse opcionalmente los pasos adicionales -S4- y -S5- del procedimiento.

En el caso de que en el terminal -1- exista una pluralidad de elementos de seguridad -20- que podrían ser adecuados en cada caso para alojar la parte relevante para la seguridad -202- de la aplicación -200- en la forma instalada, se determina, es decir, se selecciona uno de ellos para el resto del procedimiento en el paso -S4-. La determinación del elemento de seguridad -20- a partir de un cierto número de elementos de seguridad la puede realizar la aplicación -200-, es decir, más precisamente, su parte -201-, y/o la unidad de control -22- de la figura 1. El tipo de parte relevante para la seguridad -202- que se ha de instalar puede influenciar la selección. Por ejemplo, la funcionalidad proporcionada por la parte -202- puede presentar una referencia a un propietario (suscriptor) de un elemento de seguridad -20- (tarjeta SIM) correspondiente. Sin embargo, también puede haber un elemento de seguridad -20- específico en el terminal -1- que sea el único de los elementos de seguridad -20- existentes en el terminal -1- previsto para alojar partes relevantes para la seguridad -202- de una aplicación -200- descargable y que, por esta razón, se seleccione en el paso -S4-. Un terminal con una tarjeta de almacenamiento masiva segura, un módulo NFC y una tarjeta SIM constatan, por ejemplo, que solo la tarjeta SIM comprende como elemento de seguridad físico un coprocesador criptográfico adecuado. Para una tarjeta SIM con varios entornos de ejecución o zonas aseguradas como elementos de seguridad se selecciona, por ejemplo, el elemento de seguridad que contiene la función de pago requerida para la aplicación -200- (tarjeta de crédito).

En el paso -S5- se determina entonces una instancia de confianza -3- que, en este caso concreto, está prevista para administrar el elemento de seguridad -20- determinado en el paso -S4-, es decir, para instalar la parte relevante para la seguridad -202- de la aplicación -200- en el elemento de seguridad -20-. En el presente ejemplo, el TSM -3- hace las veces de instancia de confianza. También la determinación del TSM puede estar apoyada por la parte -201- de la aplicación -200- o por la unidad de control -22- (en el terminal -1- o en el elemento de seguridad -20-, -12-). Por regla general, por medio del elemento de seguridad determinado en el paso -S4- se predetermina ya el TSM -3- “competente”. Sin embargo, es posible que para un elemento de seguridad -20- esté disponible o se pueda seleccionar una pluralidad de TSM -3- para la administración del elemento de seguridad -10-. Preferentemente, el propio elemento de seguridad -20- almacena una lista -21- de TSM. En particular —como se ha mencionado ya— a cada zona segura en el elemento de seguridad puede estar asignado un TSM competente. A cada zona segura puede estar asignado en la lista exactamente uno o varios TSM que, en el paso -S5-, se pueden seleccionar como TSM competente. La dirección de comunicación del TSM competente está almacenada también en el módulo de seguridad o en la lista -21-.

Los pasos -S4- y/o -S5- y/o -S6- se pueden llevar a cabo o bien – tal y como se ha descrito anteriormente – por medio de la parte -202- de la aplicación -200- o bien por medio de una unidad dedicada -22- que se ejecuta en un entorno de ejecución del elemento de seguridad (físico) o en el terminal. La unidad dedicada -22- para la determinación del TSM competente y para la transmisión correspondiente simplifica la configuración de la aplicación -200-. En particular, una unidad dedicada -22- puede realizar preferentemente en el elemento de seguridad (aunque también en el terminal) los pasos -S4- – -S6- con la ayuda de las informaciones de asignación -21- almacenadas en el elemento de seguridad. Las informaciones de asignación -21- almacenadas comprenden también —además de la asignación del elemento de seguridad o de la zona segura al TSM— las direcciones de comunicación del TSM.

Por medio de la unidad de control -22- se establece entonces, en el paso -S6-, una conexión de comunicación de datos con el TSM -3- determinado en el paso -S5-. Esta conexión de comunicación de datos puede discurrir a través de interfaces de comunicación de datos del terminal -1-, por ejemplo, una antena o similar. A través de esta conexión de comunicación de datos, el elemento de seguridad -20- envía además al TSM -3-, en el paso -S6-, la parte relevante para la seguridad -202- que el terminal -1- ha proporcionado previamente al elemento de seguridad -20- para este fin. El elemento de seguridad -20- tiene acceso a los datos de contacto o interfaces de contacto correspondientes del TSM -3-, que están almacenados, por ejemplo, en una memoria del elemento de seguridad -20- o que pueden ser consultados, a través del elemento de seguridad -20-, desde un servidor (no mostrado). La transmisión de la parte -202-, en el paso -S6-, se puede realizar, por ejemplo, por SMS o por Internet, por ejemplo, a través de un servicio web.

En el paso -S7-, el TSM comprueba la parte relevante para la seguridad -202- recibida por el elemento de seguridad -20-. La comprobación se puede referir a todos los aspectos descritos anteriormente y/o a aspectos complementarios. Sin embargo, en el caso de que la parte -202- comprenda ya un certificado de una instancia de comprobación, por medio del cual se confirme una comprobación exitosa de la parte -202-, la comprobación a través del TSM en el paso -S7- se puede limitar a la verificación del certificado. Por regla general esto se lleva a cabo haciendo que una firma, que ha generado la instancia de comprobación con su clave secreta, se verifique por medio de una clave pública de la instancia de comprobación.

Se entiende que el TSM -3- solo lleva a cabo el resto de pasos del procedimiento en el caso de que la comprobación en el paso -S7- haya transcurrido de modo exitoso.

En el paso opcional -S8-, el TSM -3- prepara, en caso de que sea necesario, la parte -202- para una instalación que se realiza a continuación en el paso -S9- de modo adecuado en el elemento de seguridad -20-. Un paso de preparación de este tipo puede transformar, por ejemplo, la parte -202- a un formato prefijado, puede llevar a cabo adaptaciones de seguridad en la parte -202- o acciones similares. Esta preparación puede ser específica para el TSM -3-, depender del tipo de la parte -202- y/ o del propio elemento de seguridad -20-.

Finalmente, con los pasos -S9- y -S10-, el TSM -3- instala la parte relevante para la seguridad -202- preparada, dado el caso, de la aplicación -200- en el elemento de seguridad -20-, que está integrado en el terminal -1-. En el paso -S9-, la parte preparada, dado el caso, se transmite de vuelta al terminal y, por tanto, en el paso -S10-, por medio de la respuesta del TSM -3- se instala la parte relevante para la seguridad -202- de la aplicación -200- en el elemento de seguridad -20-. El paso -S10- comprende, en particular, la carga de la parte en el elemento de seguridad y una activación de la aplicación que se realiza a continuación, si procede.

En una variante, el TSM -3- instala la parte -202- y controla los pasos -S9- y -S10-. Del mismo modo, el paso -S10- también lo puede controlar la unidad de control -22-.

Para la instalación, el TSM -3- usa las claves criptográficas negociadas previamente con el propietario del elemento de seguridad -20- (en un paso no mostrado) que también se presentan de forma correspondiente en el elemento de seguridad -20-. Se conoce la ejecución de una instalación alejada de aplicaciones en elementos de seguridad por medio de una instancia como el TSM -3-. Precisamente, está suficientemente descrita la instalación de aplicaciones en zonas seguras en el sentido de la especificación de Global Platform.

Por tanto, en particular, la parte relevante para la seguridad -202- de la aplicación -200- transmitida por el terminal se transmite de vuelta al terminal a través de la red. La parte -202- transmitida de vuelta se instala en el elemento de seguridad -20-.

Por ejemplo, puede estar previsto fundamentalmente que una instancia externa, en el presente ejemplo, por ejemplo, el proveedor de aplicaciones -2-, pueda alquilar espacio de almacenamiento en un elemento de seguridad -20- del terminal -1-, en particular, para instalar allí la parte -202- de la aplicación -200-. La liquidación de los costes del alquiler de este espacio de almacenamiento se ha de poder hacer entonces de modo automático. Para ello, la aplicación -200-, es decir, la parte no relevante para la seguridad -201- instalada ya en el terminal -1-, en el paso -S3-, realiza preguntas referidas al alquiler de espacio de almacenamiento al propietario de los elementos de seguridad -10- que están en el terminal -1-.

En caso de que se confirme la posibilidad del alquiler por parte del propietario de un elemento de seguridad -10- de este tipo, entonces se puede llevar a cabo un alquiler de espacio de almacenamiento de este tipo en el elemento de seguridad -20- correspondiente, por ejemplo, a través de una interfaz automatizada correspondiente. En este sentido, la selección del elemento de seguridad -10- en el sentido del paso -S4- descrito anteriormente se realiza aquí de forma específica. La liquidación de los costes para el alquiler del espacio de almacenamiento se realiza, así mismo, de modo automático.

En otro paso complementario se le informa al TSM -3-, que también ha sido determinado según esta forma de realización tal y como se ha descrito anteriormente en relación al paso -S5-, sobre que el propietario del elemento de seguridad -10- correspondiente está de acuerdo con la instalación de la parte -202- en el espacio de almacenamiento alquilado del elemento de seguridad.

REIVINDICACIONES

1. Procedimiento para la instalación de una parte relevante para la seguridad (202) de una aplicación (200) puesta a disposición por un proveedor de aplicaciones (2) en un elemento de seguridad (20) de un terminal (1), comprendiendo los siguientes pasos:

- recepción (S2) de la aplicación (200) desde el proveedor de aplicaciones (2) en el terminal (1), comprendiendo la aplicación (200) la parte relevante para la seguridad (202) y una parte no relevante para la seguridad (201);
- instalación (S3) de la parte no relevante para la seguridad (201) de la aplicación (200) en el terminal (1), e
- instalación (S4-S10) de la parte relevante para la seguridad (202) de la aplicación (200) en el elemento de seguridad (20) del terminal (1);

realizándose, para la instalación (S4-S10) de la parte relevante para la seguridad (202) de la aplicación (200), los siguientes pasos:

- transmisión (S6) de al menos una parte de la parte relevante para la seguridad (202) recibida de la aplicación (200) a una instancia de confianza (3) alejada que administra el elemento de seguridad (20);
- recepción (S9) de una respuesta de la instancia de confianza (3) para la parte relevante para la seguridad (202) de la aplicación (200);
- carga (S10) de la parte relevante para la seguridad (202) de la aplicación (200) en el elemento de seguridad (20) por medio de la respuesta de la instancia de confianza (3).

2. Procedimiento, según la reivindicación 1, **caracterizado porque** únicamente la respuesta recibida de la instancia de confianza hace posible la carga (S10).

3. Procedimiento según la reivindicación 1 o 2, **caracterizado porque** la instancia de confianza (3) comprueba (S7) la parte relevante para la seguridad (202) de la aplicación (200), en particular, en lo que se refiere a la compatibilidad con el elemento de seguridad (20), especificaciones técnicas que se han de cumplir y/o aspectos de seguridad.

4. Procedimiento, según la reivindicación 3, **caracterizado porque** la instancia de confianza (3) comprueba la parte relevante para la seguridad (202) de la aplicación (200) mediante un certificado de un organismo de certificación, con el que se ha dotado a la parte relevante para la seguridad (202).

5. Procedimiento, según una de las reivindicaciones 1 a 4, **caracterizado por** un paso de determinación (S4) del elemento de seguridad (20) a partir de una pluralidad de elementos de seguridad (20) antes del paso de la transmisión (S6).

6. Procedimiento, según una de las reivindicaciones 1 a 5, **caracterizado por** un paso de determinación (S4) de una zona segura (23), en la que se ha de cargar la parte relevante para la seguridad (202) de la aplicación (200), a partir de una pluralidad de zonas seguras (23) en el elemento de seguridad (20) antes del paso de la transmisión (S6).

7. Procedimiento, según una de las reivindicaciones 1 a 6, **caracterizado por** el paso de determinación (S5) de una instancia de confianza (3) que administra el elemento de seguridad (20) antes del paso de la transmisión (S6).

8. Procedimiento, según una de las reivindicaciones 1 a 7, **caracterizado porque**, en el paso de determinación (S5) de la instancia de confianza (3), la instancia de confianza (3) se selecciona a partir de una pluralidad de instancias de confianza (3) que administran al menos una zona segura (23) del módulo de seguridad (20).

9. Procedimiento, según una de las reivindicaciones 1 a 8, **caracterizado porque** el paso de la instalación (S9) de la parte relevante para la seguridad (202) en el elemento de seguridad (20) lo lleva a cabo de modo asegurado criptográficamente la instancia de confianza (3), intercambiándose claves criptográficas usadas a tal fin en un paso anterior a la instalación, entre un propietario del elemento de seguridad (20) o un propietario de una zona segura (23) en el elemento de seguridad (20) y la instancia de confianza (3).

10. Procedimiento, según una de las reivindicaciones 1 a 9, **caracterizado porque** la parte relevante para la seguridad (202) de la aplicación (200) se transmite (S6) a la instancia de confianza (3), y se vuelve a recibir (S9) por la instancia de confianza (3) en una forma preparada.

11. Procedimiento, según una de las reivindicaciones 1 a 10, **caracterizado porque** el terminal (1) solicita (S1) la aplicación (200) al proveedor de aplicaciones (2).

12. Terminal (1) con un elemento de seguridad (20), en el que el terminal (10) está configurado para llevar a cabo un procedimiento, según una de las reivindicaciones 1 a 11.

13. Elemento de seguridad (20) para un terminal (10), en el que el elemento de seguridad (20) se opera de acuerdo con el procedimiento, según una de las reivindicaciones 1 a 12, y está configurado, cuando está integrado en el terminal (10), para transmitir una parte relevante para la seguridad (202) de una aplicación (200) recibida a través del terminal (10), que se ha de instalar en el elemento de seguridad (20), a una instancia de confianza (3) que

administra el elemento de seguridad (20).

14. Elemento de seguridad (20), según la reivindicación 13, **caracterizado porque** el elemento de seguridad (20) está conformado como

- elemento de seguridad (20) que se puede desmontar del terminal (1), en particular, como tarjeta de comunicaciones móviles SIM/UICC, como tarjeta multimedia segura o similar,
- como elemento de seguridad (20) montado de modo fijo en el terminal (1), en particular, como tarjeta de comunicaciones móviles SIM/UICC incrustada, como TPM, como módulo NFC, o
- como entorno de ejecución seguro (12) que se ejecuta, junto a un entorno de ejecución normal (11), en el procesador (10) del terminal (1), por ejemplo, como “Trusted Execution Environment” según la especificación de “Global Platform”.

15. Instancia de confianza (3) alejada que se opera de acuerdo con el procedimiento, según una de las reivindicaciones 1 a 12, y está configurada para recibir de un terminal (1) una segunda parte (202) de una aplicación (200) que se ha de instalar en un elemento de seguridad (20), en la que la primera parte (201) de la aplicación está instalada en el terminal (1), y la instancia de confianza está configurada para la instalación de la segunda parte (202) de la aplicación en el elemento de seguridad (20) en el terminal (1) como respuesta a la recepción de la segunda parte (202) por el terminal (1).

FIG 1

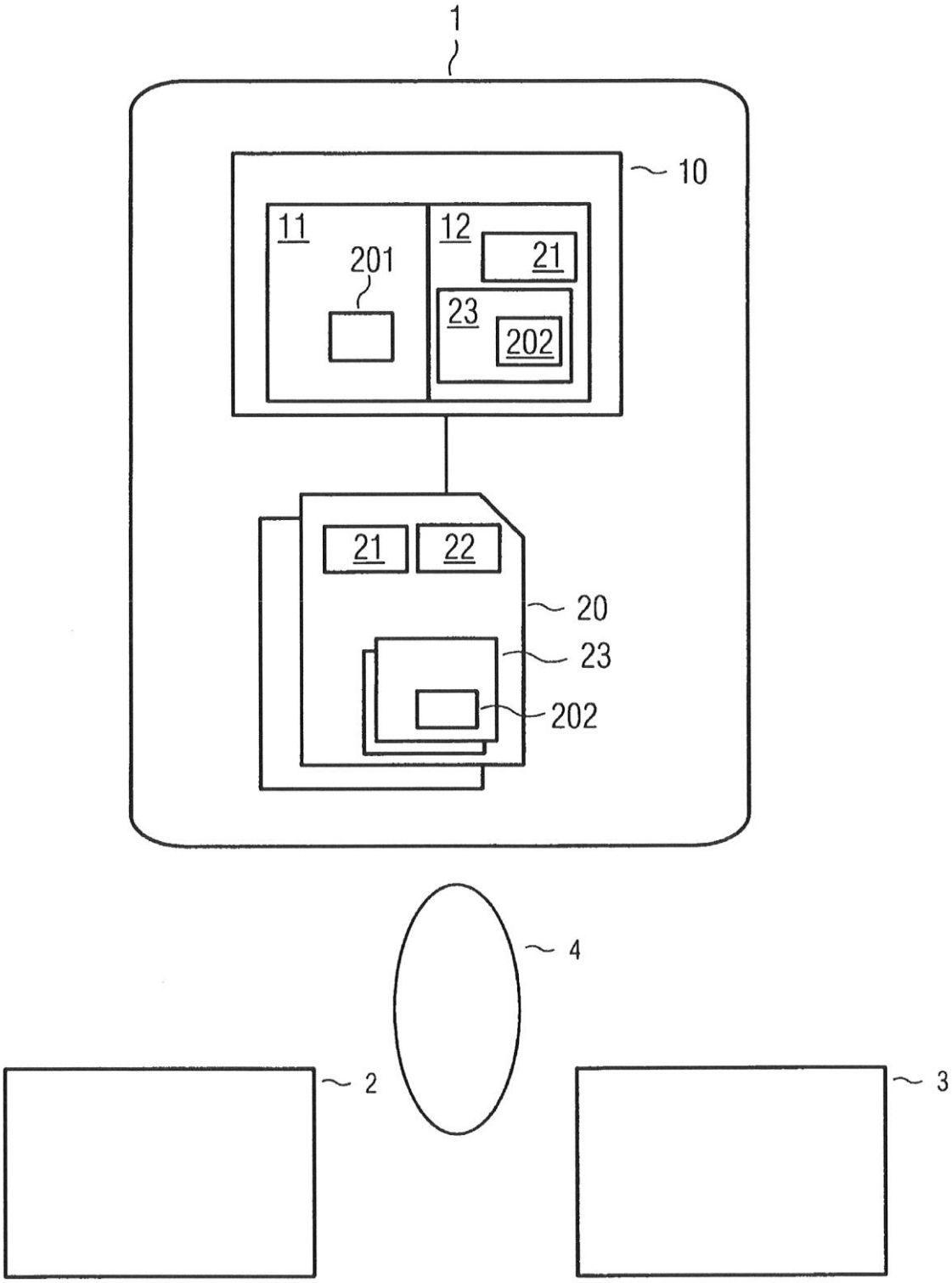
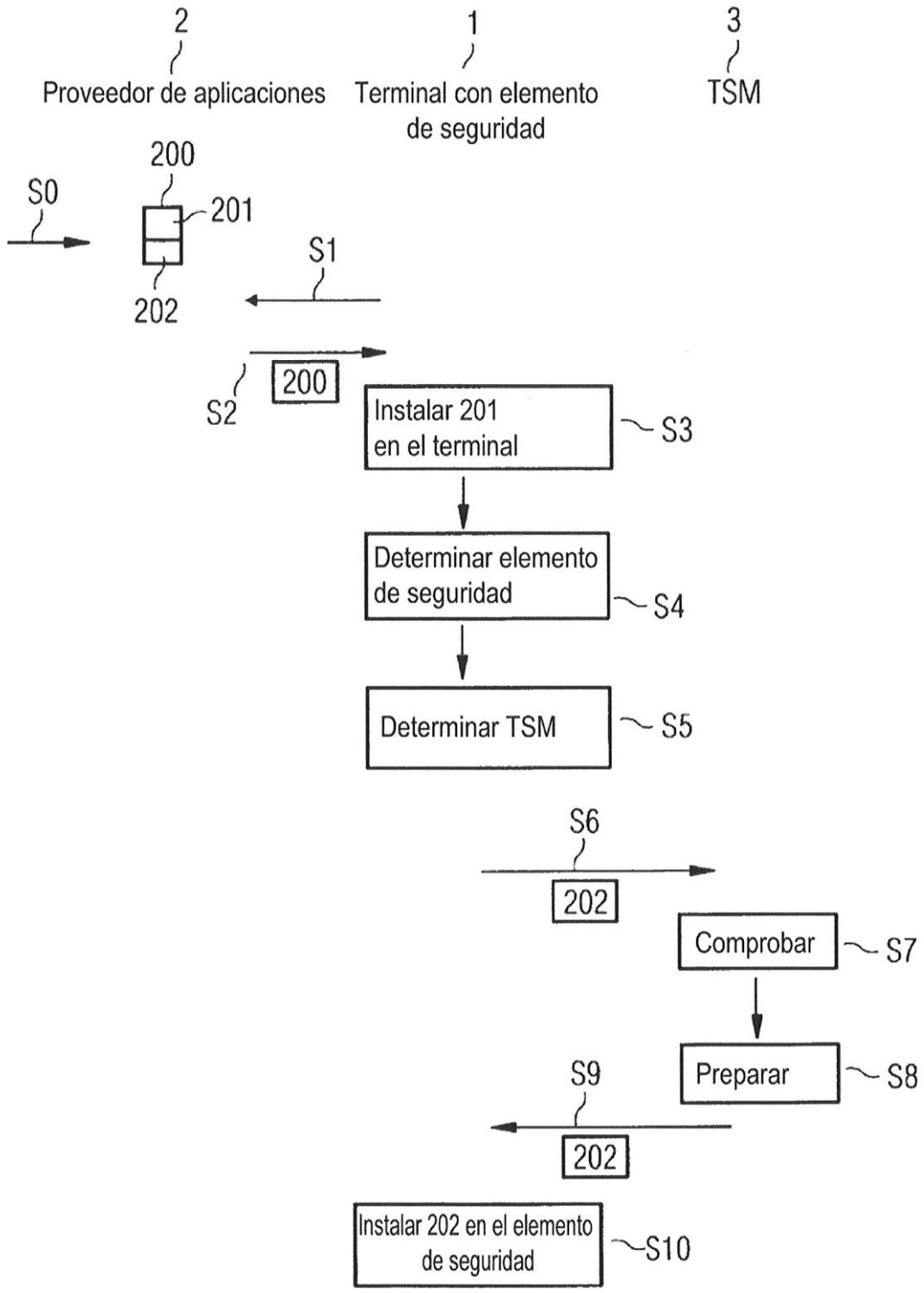


FIG 2


2
Proveedor de aplicaciones
1
Terminal con elemento de seguridad
3
TSM
200
S0
201
202
S1
S2
200
Instalar 201 en el terminal
S3
Determinar elemento de seguridad
S4
Determinar TSM
S5
S6
202
Comprobar
S7
Preparar
S8
S9
202
Instalar 202 en el elemento de seguridad
S10