(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 786 250**

(51) Int. CI.:

H04W 12/08 (2009.01)
H04W 12/00 (2009.01)
G06F 21/57 (2013.01)
H04W 88/02 (2009.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **14.04.2014 PCT/EP2014/000996**

(87) Fecha y número de publicación internacional: **23.10.2014 WO14170006**

(96) Fecha de presentación y número de la solicitud europea: **14.04.2014 E 14719621 (6)**

(97) Fecha y número de publicación de la concesión europea: **04.03.2020 EP 2987350**

(54) Título: **Estación móvil que comprende recursos de seguridad con diferentes niveles de seguridad**

(30) Prioridad:

15.04.2013 DE 102013006470

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
09.10.2020

(73) Titular/es:

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

(72) Inventor/es:

DIETZE, CLAUS y
GALKA, GERO

(74) Agente/Representante:

ARIAS SANZ, Juan

DESCRIPCIÓN

Estación móvil que comprende recursos de seguridad con diferentes niveles de seguridad

La invención se refiere a una estación móvil que comprende un terminal móvil y que comprende recursos de seguridad, así como a un sistema de carga de aplicaciones y a un sistema de evaluación de riesgos, en cada caso con una estación móvil.

Una estación móvil comprende un terminal móvil y, por regla general, también un módulo de identidad de abonado (también denominado Secure Element SE), que puede hacerse funcionar en el terminal y con el que puede hacerse funcionar el terminal en una red de radiotelefonía móvil. En muchos sistemas de radiotelefonía móvil, el módulo de identidad de abonado o Secure Element SE está diseñado como una tarjeta de abonado extraíble (tarjeta con chip de microprocesador), por ejemplo, como una tarjeta SIM, o como una eUICC implementada permanentemente (UICC integrada; UICC = *Universal Integrated Circuit Card*, tarjeta de circuitos integrados universal).

Por terminal móvil se entiende un aparato para usar un sistema de radiotelefonía móvil, por ejemplo un teléfono móvil, teléfono inteligente o un PDA (*Personal Digital Assistant*, asistente digital personal) con una función de teléfono móvil.

Con la denominación de arquitectura Trustzone (marca de la empresa ARM) se conoce una arquitectura de tiempo de ejecución en dos partes para un sistema de microprocesador, que comprende dos entornos de tiempo de ejecución. Un primer entorno de tiempo de ejecución no seguro denominado "Normal Zone" o "Normal World" es controlado por un sistema operativo normal (por ejemplo, Android, Windows Phone, iOS). Un segundo entorno de tiempo de ejecución seguro o de confianza denominado "Trustzone" o "Trusted World" o "Secure World" o "Trusted Execution Environment, TEE" es controlado por un sistema operativo de seguridad.

El módulo de identidad de abonado, el entorno de tiempo de ejecución normal y el entorno de tiempo de ejecución seguro constituyen recursos de seguridad de la estación móvil que ofrecen diferentes niveles de seguridad. El entorno de tiempo de ejecución normal es relativamente inseguro, por lo que tiene un bajo nivel de seguridad. Una tarjeta SIM tiene un nivel de seguridad relativamente alto y el entorno de tiempo de ejecución seguro TEE uno medio.

Muchos usuarios de aplicaciones para estaciones móviles exigen que las aplicaciones que usan en su estación móvil cumplan un cierto nivel de seguridad. De lo contrario, es posible que no estén dispuestos a usar la aplicación en su estación móvil. Por lo tanto, los proveedores de aplicaciones para estaciones móviles están interesados en poder garantizar un nivel de seguridad definido de su aplicación. Sin embargo, el nivel de seguridad de una aplicación depende de los recursos de seguridad de la estación móvil. La aplicación solo puede garantizar una seguridad adecuada si los recursos de seguridad de la estación móvil cumplen un cierto estándar mínimo.

El documento WO 2011/131365 A1 describe un sistema y un procedimiento para la configuración posterior de una aplicación que ya se encuentra en un terminal móvil. A este respecto, un servidor central tiene información sobre posibles recursos de seguridad (configuraciones de terminal con diferentes entornos de tiempo de ejecución y/o elementos de seguridad) de terminales móviles y sobre los niveles de seguridad (grados de seguridad) que corresponden a los recursos de seguridad. En función del nivel de seguridad del terminal que haya determinado el servidor central, el servidor selecciona una configuración de aplicación adecuada y configura la aplicación que ya se encuentra en el terminal para que se ajuste al nivel de seguridad. A este respecto, solo una variante de aplicación debe mantenerse disponible en el servidor. No obstante, se establece una configuración de aplicación correspondiente al nivel de seguridad a través de la configuración posterior.

El sistema y el procedimiento del documento WO 2011/131365 A1 requieren que los recursos de seguridad (configuración de terminal) de un terminal sean conocidos por el propio terminal o al menos sean conocidos teóricamente. Esta es la única forma en que el terminal puede solicitar la configuración adecuada al servidor.

Sin embargo, los recursos de seguridad de una estación móvil pueden cambiar. Por ejemplo, se puede añadir o eliminar un entorno de tiempo de ejecución seguro. También se puede quitar una tarjeta SIM. Por lo tanto, no se garantiza que los supuestos recursos de seguridad, por ejemplo, de acuerdo con el número de modelo del terminal, coincidan con los recursos de seguridad reales.

El documento US 2008/194296 A1 divulga una estación móvil con un módulo de determinación con el que se puede derivar un nivel de seguridad de las áreas de memoria de la estación móvil. También se asigna un nivel de seguridad a los datos que se han de almacenar, tal como correos electrónicos. En función del nivel de seguridad de los datos se utiliza un área de almacenamiento con un nivel de seguridad correspondiente para almacenar los datos.

El documento US 2007/240205 A1 divulga una estación móvil con diferentes aplicaciones de arranque, recursos de seguridad (por ejemplo, tarjeta SIM, UICC, etc.) y con un módulo de determinación, formado por un servidor GAA y un cliente GAA de la estación móvil, que se comunican entre sí. Con el cliente GAA se puede determinar un nivel de

seguridad de aplicación, que se alcanza cuando se ejecuta una aplicación de arranque con credenciales a partir de un determinado recurso de seguridad. Si el nivel de seguridad de aplicación es demasiado bajo, la aplicación de arranque no se ejecutará. Si el nivel de seguridad de las credenciales es suficientemente alto, la aplicación de arranque se considera suficientemente segura.

El documento US 2010/306107 A1 divulga un servidor de autenticación con un módulo de determinación TIM para determinar los niveles de seguridad de los recursos de seguridad (por ejemplo, tarjeta SIM o UICC o TPM) de una estación móvil y los riesgos de seguridad que emanan de los recursos de seguridad.

La invención se basa en el objetivo de crear una estación móvil que pueda garantizar un nivel de seguridad definido a nivel de aplicación. En particular, se indicará una estación móvil con la que pueda garantizarse un nivel de seguridad de aplicación definido para aplicaciones implementadas o que van a ser implementadas en la estación móvil. Además, se indicará un sistema de carga de aplicaciones para cargar una aplicación en una estación móvil, con el que se puede garantizar un nivel de seguridad de aplicación definido para las aplicaciones cargadas en la estación móvil.

El objetivo se logra mediante una estación móvil según la reivindicación 1. En las reivindicaciones dependientes se indican configuraciones ventajosas de la invención.

La estación móvil de acuerdo con la invención según la reivindicación independiente 1 comprende un terminal móvil y comprende recursos de seguridad. La estación móvil contiene un módulo de determinación (o módulo Discovery) implementado en la estación móvil, con el que se pueden determinar los recursos de seguridad de la estación móvil, se puede derivar al menos un nivel de seguridad de la estación móvil que se puede alcanzar por medio de los recursos de seguridad, y se pueden emitir los niveles de seguridad de la estación móvil que se han derivado.

El módulo de determinación permite determinar qué recursos de seguridad están realmente presentes en la estación móvil. En particular, el módulo de determinación permite reconocer cuándo se han eliminado recursos de seguridad de la estación móvil o se han añadido a la estación móvil. Los recursos de seguridad determinados por el módulo de determinación corresponden así al estado de seguridad actual real de la estación móvil. Sobre esta base, el módulo de determinación puede derivar un nivel de seguridad actual real de la estación móvil, teniendo en cuenta los recursos de seguridad que pueden haberse eliminado o añadido recientemente. Dado que un nivel de seguridad derivado y emitido por el módulo de determinación siempre está actualizado, un nivel de seguridad de la estación móvil no solo se puede asumir sino que se garantiza realmente con una estación móvil que contiene el módulo de determinación.

De acuerdo con la invención, la estación móvil contiene además información de aplicación sobre al menos una aplicación implementada o implementable en la estación móvil. A este respecto, con el módulo de determinación se puede derivar, como nivel de seguridad de la estación móvil, un nivel de seguridad de aplicación que se puede alcanzar durante el funcionamiento de la aplicación en la estación móvil utilizando los recursos de seguridad. Por tanto, de acuerdo con la invención se puede derivar y emitir un nivel de seguridad que se alcanza cuando la aplicación se ejecuta en la estación móvil. Por lo tanto, se determina un nivel de seguridad a nivel de aplicación. Además, se puede derivar y emitir un nivel de seguridad a nivel de dispositivo, que es independiente de la ejecución de una aplicación en la estación móvil. Sin embargo, es de particular importancia práctica un nivel de seguridad a nivel de aplicación con el que pueda estimarse la seguridad de una estación móvil en relación con una aplicación que se ejecuta en la estación móvil.

Por lo tanto, de acuerdo con la reivindicación 1 se crea una estación móvil que puede garantizar un nivel de seguridad definido a nivel de aplicación.

Uno o más de los siguientes módulos de seguridad están previstos opcionalmente como recursos de seguridad: un entorno de tiempo de ejecución normal del terminal, en particular con o sin funciones criptográficas; un módulo de identidad de abonado virtual implementado en el terminal; un entorno de tiempo de ejecución seguro del terminal; un módulo de identidad de abonado que puede hacerse funcionar en el terminal, en particular un módulo de identidad de abonado extraíble (por ejemplo, tarjeta SIM o tarjeta USIM), un módulo de identidad de abonado implementado permanentemente (por ejemplo, eUICC), un módulo de identidad de abonado extraíble certificado, un módulo de identidad de abonado implementado permanentemente certificado; una tarjeta de memoria de microprocesador segura, en particular una tarjeta SD segura y/o una tarjeta Micro SD segura.

El nivel de seguridad de la estación móvil puede ser derivado y emitido opcionalmente por el módulo de determinación para cada módulo de seguridad y/o para cada combinación de uno o más módulos de seguridad de la estación móvil. Opcionalmente, se puede emitir una pluralidad de al menos varios o todos los niveles de seguridad de varios o todos los recursos de seguridad / módulos de seguridad de la estación móvil.

El módulo de determinación, junto con el nivel de seguridad, opcionalmente también puede emitir el recurso de seguridad o el módulo de seguridad para el que es válido el nivel de seguridad.

El módulo de determinación puede generar opcionalmente una lista de varios o todos los recursos de seguridad / módulos de seguridad junto con los niveles de seguridad asociados, por ejemplo, como tabla.

De acuerdo con una forma de realización de la estación móvil, el módulo de determinación está integrado en una interfaz de programación, en particular en una denominada interfaz de programación de aplicaciones, API, por medio de la cual puede emitirse información de salida desde la estación móvil en relación con los niveles de seguridad de la estación móvil y/o puede introducirse información de control en la estación móvil para controlar los niveles de seguridad.

Una o más de las siguientes opciones pueden emitirse opcionalmente como información de salida en la interfaz de programación: un nivel de seguridad de la estación móvil; un recurso de seguridad disponible de la estación móvil; un nivel de seguridad de un recurso de seguridad; todos los niveles de seguridad de todos los recursos de seguridad de la estación móvil; todos los recursos de seguridad disponibles de la estación móvil; el nivel de seguridad más alto disponible de la estación móvil; un nivel de seguridad actualmente establecido de la estación móvil; información de funcionalidad sobre funcionalidades disponibles para uno o cada nivel de seguridad o para uno o cada recurso de seguridad. A este respecto, en la interfaz de programación el módulo de determinación tiene la funcionalidad de determinar y emitir recursos de seguridad y niveles de seguridad. Otras partes de la interfaz de programación llevan a cabo funcionalidades adicionales, como por ejemplo proporcionar información de funcionalidad. Como nivel de seguridad establecido está previsto, por ejemplo, el nivel de seguridad que la estación móvil debe cumplir durante su funcionamiento (opcionalmente como mínimo o de manera exacta). A partir del nivel de seguridad establecido se deduce, por ejemplo, qué recurso de seguridad (por ejemplo, tarjeta SIM o TEE, etc.) debe usar la estación móvil durante su funcionamiento.

Con respecto a las funcionalidades de la estación móvil, por regla general se aplica el principio de que cuanto mayor sea el nivel de seguridad, más funcionalidades de la estación móvil estarán disponibles. Cuanto más bajo es el nivel de seguridad de la estación móvil, menos funcionalidades de la estación móvil están disponibles (es decir, pueden usarse, por ejemplo, activarse). Por ejemplo, una funcionalidad de la estación móvil con la que se pueden realizar cálculos criptográficos se desactiva si el nivel de seguridad determinado es demasiado bajo. Si se añade un nuevo recurso de seguridad a la estación móvil, por medio del cual se aumenta el nivel de seguridad de la estación móvil, se determina el nuevo nivel de seguridad y se habilita o activa la funcionalidad con la que se pueden realizar cálculos criptográficos, por lo que puede usarse posteriormente.

Dado que como niveles de seguridad se derivan y emiten niveles de seguridad de aplicación, la información de funcionalidad en particular también se relaciona con una aplicación. Por ejemplo, como información de funcionalidad relacionada con una aplicación está prevista información sobre qué funcionalidades de aplicación están disponibles en un nivel de seguridad de aplicación derivado o, en general, qué funcionalidad de aplicación está disponible en qué nivel de seguridad de aplicación derivado. Un nivel de seguridad de aplicación establecido se puede implementar, por ejemplo, en el hecho de que una aplicación se debe cargar en un recurso de seguridad correspondiente al nivel de seguridad de aplicación establecido. Opcionalmente, se puede establecer un nivel de seguridad de aplicación mínimo, de modo que una aplicación debe cargarse en un recurso de seguridad que cumpla al menos el nivel de seguridad de aplicación mínimo.

Opcionalmente, la información de control contiene uno o más de los siguientes: definir el uso de un determinado recurso de seguridad con un determinado nivel de seguridad; definir el uso del recurso de seguridad que tiene el nivel de seguridad más alto. En el caso de que como nivel de seguridad esté previsto un nivel de seguridad de aplicación, el hecho de definir el uso de un determinado recurso de seguridad con un determinado nivel de seguridad se materializa, por ejemplo, en el hecho de que una aplicación que se va a implementar y/o a ejecutar se implementa y/o se ejecuta en el recurso de seguridad con ese determinado nivel de seguridad. El hecho de definir el uso del recurso de seguridad con el nivel de seguridad de aplicación más alto significa, por ejemplo, que la aplicación se implementa o ejecuta en el recurso de seguridad con el nivel de seguridad más alto.

El módulo de determinación está implementado opcionalmente en el recurso de seguridad de la estación móvil que suministra o confiere a la estación móvil el nivel de seguridad más alto. De este modo se garantiza que el módulo de determinación esté protegido frente a manipulaciones. Las manipulaciones podrían, por ejemplo, aspirar a simular recursos de seguridad inexistentes, derivar a partir de ello incorrectamente un nivel de seguridad inexacto y activar un alcance funcional inadmisiblemente alto de la estación móvil o una aplicación implementada en ella.

El módulo de determinación está implementado opcionalmente en un recurso de seguridad de la estación móvil implementado permanentemente en el terminal con el fin de evitar que el módulo de determinación DIS sea eliminado de la estación móvil.

Si la estación móvil tiene una tarjeta SIM extraíble, el requisito de prever el módulo de determinación en un recurso de seguridad implementado permanentemente puede colisionar con el requisito también deseable de que el módulo de determinación esté implementado en el recurso de seguridad que proporciona el nivel de seguridad más alto. De acuerdo con una opción, el módulo de determinación está previsto en el recurso de seguridad implementado permanentemente que tiene el nivel de seguridad más alto, por ejemplo en un módulo de identidad de abonado

implementado permanentemente (por ejemplo eUICC), alternativamente en un entorno de tiempo de ejecución seguro. En el caso del entorno de tiempo de ejecución seguro se renuncia a la seguridad frente a ataques a cambio de la estabilidad del módulo de determinación. De acuerdo con otra opción, el módulo de determinación está previsto en un módulo de identidad de abonado extraíble (por ejemplo, tarjeta SIM). En este caso, a cambio de la seguridad frente a ataques se renuncia a evitar la eliminación del módulo de determinación.

Opcionalmente, la estación móvil también tiene un módulo de control de aplicación que está acoplado o puede acoplarse al módulo de determinación, por medio del cual, en función del nivel de seguridad de aplicación derivado para una aplicación, puede controlarse la ejecución de la aplicación en un alcance funcional correspondiente al nivel de seguridad de aplicación. Controlar la ejecución de la aplicación opcionalmente incluye, a este respecto, ejecutar la aplicación directamente en el alcance funcional definido. Alternativamente, controlar la ejecución incluye activar la aplicación en el alcance funcional definido, es decir, fijar su capacidad funcional para que se ejecute en el alcance funcional definido sin ejecutar directamente la aplicación.

Opcionalmente, como ejecución de la aplicación en un alcance funcional correspondiente al nivel de seguridad está previsto uno de los siguientes, en orden de alcance funcional decreciente: ejecución de la aplicación en un alcance funcional ampliado; ejecución de la aplicación en un alcance funcional completo; ejecución de la aplicación en un alcance funcional restringido; no ejecución de la aplicación. A este respecto, un alcance funcional ampliado puede estar ampliado en comparación con el alcance funcional completo, en particular, por funcionalidades adicionales o servicios adicionales que se desvían de la funcionalidad central de la aplicación.

Una estación móvil con un módulo de determinación con el que se puede derivar y emitir un nivel de seguridad a nivel de aplicación funciona, por ejemplo, de la siguiente manera.

En la estación móvil hay implementada una aplicación. La aplicación no se está ejecutando actualmente y debe ejecutarse. Con el módulo de determinación se determinan los recursos de seguridad actualmente disponibles y operativos de la estación móvil, por ejemplo, entorno de tiempo de ejecución normal y/o seguro, tarjeta SIM, eUICC, tarjeta (Micro) SD segura, etc. El módulo de determinación recibe información sobre qué aplicación en la estación móvil ha de hacerse funcionar. A este respecto, por regla general es irrelevante si primero se determinan los recursos de seguridad o si primero se proporciona al módulo de determinación la información sobre la aplicación. Con ayuda de los recursos de seguridad determinados se deriva y se emite un nivel de seguridad de aplicación. En función del nivel de seguridad derivado y emitido, la ejecución de la aplicación se controla en un alcance funcional correspondiente al nivel de seguridad, o bien ejecutando directamente la aplicación o bien al menos se pone en un estado ejecutable (se activa) para ser ejecutada más tarde.

Por ejemplo, si el nivel de seguridad determinado es bajo, la aplicación no se ejecuta en absoluto y permanece desactivada porque el riesgo de seguridad por la ejecución de una aplicación en la estación móvil se considera demasiado grande. Esto evita que los recursos de seguridad deficientes de una estación móvil dañen la imagen de una aplicación que es confiable en sí misma.

De acuerdo con otro ejemplo, la aplicación se ejecuta en un alcance funcional restringido (o se activa en tal alcance funcional) en el caso de un nivel de seguridad determinado medio. En particular, las funcionalidades de la aplicación críticas para la seguridad pueden permanecer desactivadas, y solo las funcionalidades de la aplicación que son críticas para la seguridad en un nivel bajo o como máximo medio se activan y son, por tanto, ejecutables.

De acuerdo con otro ejemplo, la aplicación se ejecuta o activa, es decir, se hace ejecutable, en un alcance funcional completo si se determina un nivel de seguridad alto. En particular, se activan funcionalidades de la aplicación particularmente críticas para la seguridad y son, por tanto, ejecutables.

Una interfaz de programación con un módulo de determinación con el que se pueden derivar y emitir niveles de seguridad de aplicación puede estar configurada, en particular, para ofrecer las siguientes funcionalidades, que se indican a continuación en un lenguaje de pseudocomando concebible con la siguiente descripción de la funcionalidad:
getSecDevices(): Determinar todos los recursos de seguridad disponibles en la estación móvil y derivar y emitir el nivel de seguridad de aplicación de cada recurso de seguridad determinado;
validateSecService(): Proporcionar información de funcionalidad sobre con qué nivel de seguridad de aplicación y con qué variante de aplicación están disponibles qué funcionalidades de aplicación; o alternativa o adicionalmente: Determinar qué nivel de seguridad de aplicación debe seleccionarse para que esté disponible una funcionalidad de aplicación deseada;
getHighestSecLevel(): Derivar y emitir el nivel de seguridad más alto disponible en la estación móvil;
selectSecLevel(): Definir el nivel de seguridad de aplicación para una aplicación que se va a implementar y/o ejecutar, y de ese modo definir implícitamente un recurso de seguridad correspondiente al nivel de seguridad de aplicación en el que se implementa o ejecuta la aplicación;
getSelectedSecLevel(): Determinar el nivel de seguridad de aplicación actualmente establecido, que generalmente fue establecido por un selectSecLevel() previo;
HighestSecLevel(): Definir el nivel de seguridad de aplicación más alto disponible para una aplicación que se va a

implementar y/o ejecutar, y de ese modo definir implícitamente un recurso de seguridad correspondiente al nivel de seguridad de aplicación más alto en el que se implementa o ejecuta la aplicación.

Un sistema de carga de aplicaciones de acuerdo con la invención comprende un servidor de aplicaciones y una estación móvil tal y como se indicó anteriormente. A este respecto, el servidor de aplicaciones está caracterizado por un módulo de selección de aplicaciones que está acoplado o puede acoplarse al módulo de determinación, por medio del cual, en función del nivel de seguridad de aplicación derivado para una aplicación, puede seleccionarse una variante de aplicación con un alcance funcional correspondiente al nivel de seguridad y proporcionarse para su descarga a la estación móvil.

De manera similar a como se activó anteriormente un alcance funcional correspondiente al nivel de seguridad de una aplicación ya implementada, en este caso se proporciona para su descarga en la estación móvil una variante de aplicación que está ajustada a los recursos de seguridad de la estación móvil. Si se deriva y emite un alto nivel de seguridad, se proporciona, por ejemplo, una variante de aplicación con un alto alcance funcional. Si se deriva y emite un bajo nivel de seguridad, se proporciona, por ejemplo, una variante de aplicación con un bajo alcance funcional. A este respecto, el alcance funcional está definido opcionalmente por la presencia o ausencia de componentes funcionales de la aplicación en la variante funcional respectiva. El alcance funcional está definido opcionalmente por el hecho de que los componentes funcionales estén activados o desactivados, conforme al alcance funcional deseado.

La variante de aplicación que se puede proporcionar opcionalmente incluye: la aplicación con el alcance funcional correspondiente al nivel de seguridad y/o funciones adicionales (servicios adicionales) destinadas a complementar la aplicación.

En un procedimiento para descargar una variante de aplicación en una estación móvil, el módulo de selección de aplicaciones del servidor de aplicaciones se acopla al módulo de determinación de la estación móvil. En particular, la estación móvil y el servidor de aplicaciones se acoplan por tanto entre sí, opcionalmente a través de una conexión por contacto o alternativamente a través de una conexión radio sin contacto, en particular una conexión de radiotelefonía móvil u otra conexión radio. El nivel de seguridad de aplicación se determina y se emite mediante el módulo de determinación. Esto se puede hacer, opcionalmente, mientras la estación móvil está conectada al servidor de aplicaciones o en un momento previo. El nivel de seguridad de aplicación determinado y emitido se transmite al módulo de selección de aplicaciones. En función del nivel de seguridad de aplicación, el módulo de selección de aplicaciones selecciona una variante de aplicación correspondiente al nivel de seguridad de aplicación con una alcance funcional correspondiente al nivel de seguridad de aplicación y la proporciona en el servidor de aplicaciones para su descarga a la estación móvil. Finalmente, la variante de aplicación proporcionada es descargada desde el servidor de aplicaciones a la estación móvil.

Un sistema de evaluación de riesgos de acuerdo con la invención comprende una o más estaciones móviles y un servidor de riesgos. Al menos una aplicación está contenida (implementada) en al menos una estación móvil. El servidor de aplicaciones está caracterizado por un módulo de evaluación de riesgos que está acoplado o puede acoplarse al módulo de determinación, mediante el cual, en función del nivel de seguridad de aplicación de la aplicación o aplicaciones contenidas en la estación móvil o en las estaciones móviles, puede derivarse un riesgo que emana de la estación móvil o de las diversas estaciones móviles. Opcionalmente, se incluyen otros parámetros en el riesgo, por ejemplo, el número de estaciones móviles en circulación, el número o la proporción (por ejemplo, porcentaje) de las estaciones móviles en circulación en las que hay implementadas aplicaciones con un nivel de seguridad insuficiente, y similares.

La invención se explica con más detalle a continuación con ayuda de ejemplos de realización y haciendo referencia al dibujo, en el que muestran:

La Fig. 1 una estación móvil con recursos de seguridad y un módulo de determinación, de acuerdo con una forma de realización de la invención;

La Fig. 2 una tabla de asociación entre recursos de seguridad y niveles de seguridad, de acuerdo con una forma de realización de la invención;

La Fig. 3 una tabla de asociación entre recursos de seguridad, niveles de seguridad de aplicación, alcances funcionales y variantes de aplicación, de acuerdo con una forma de realización de la invención;

La Fig. 4 una activación de una aplicación ya implementada, de acuerdo con una forma de realización de la invención;

La Fig. 5 una selección y descarga de una aplicación que se va a implementar, de acuerdo con una forma de realización de la invención;

La Fig. 6 una selección y descarga de una aplicación que se va a implementar, de acuerdo con otra forma de

realización de la invención.

La figura 1 muestra una estación móvil. La estación móvil comprende un terminal ME. La estación móvil comprende además tres módulos de seguridad como recursos de seguridad SR, en concreto, en primer lugar, un entorno de tiempo de ejecución normal REE (*Rich Execution Environment*), en segundo lugar un entorno de tiempo de ejecución seguro TEE (*Trusted Execution Environment*) y, en tercer lugar, una tarjeta SIM, SIM. La estación móvil comprende además un módulo de determinación DIS (módulo *Discovery*), de acuerdo con una forma de realización de la invención. De los tres módulos de seguridad que constituyen los recursos de seguridad SR de la estación móvil, la tarjeta SIM tiene el nivel de seguridad más alto, el entorno de tiempo de ejecución seguro tiene el segundo nivel más alto y el entorno de tiempo de ejecución normal tiene el nivel de seguridad más bajo. El módulo de determinación DIS está dispuesto (implementado) en la tarjeta SIM, SIM, de la estación móvil, que tiene el nivel de seguridad más alto de entre los recursos de seguridad.

La fig. 2 muestra una tabla de asociación entre los recursos de seguridad SR y los niveles de seguridad SL de una estación móvil, de acuerdo con una forma de realización de la invención. El nivel de seguridad SL y, por lo tanto, la seguridad y confiabilidad de la estación móvil aumenta en la tabla de arriba a abajo. Un entorno de tiempo de ejecución normal REE controlado por un sistema operativo normal, Rich OS, tiene el nivel de seguridad más bajo L1, mínimo, de la tabla de asociación. Un elemento seguro virtual SE implementado en un terminal ME tiene un nivel de seguridad bajo L2, algo más alto. Un entorno de tiempo de ejecución seguro implementado en el terminal ME y controlado por un sistema operativo de seguridad, Secure OS, tiene un nivel de seguridad medio L3. Una tarjeta SIM tiene un nivel de seguridad aumentado L4. Un elemento seguro integrado eSE (p. ej., eUICC), implementado permanentemente, tiene un nivel de seguridad elevado L5. Una tarjeta SIM certificada tiene un nivel de seguridad alto L6, un elemento seguro integrado eSE certificado tiene un nivel de seguridad muy alto L7.

La fig. 3 muestra una tabla de asociación entre recursos de seguridad SR, niveles de seguridad de aplicación ASL en relación con una aplicación APP prevista para una estación móvil, alcances funcionales de la aplicación y variantes de aplicación de la aplicación, de acuerdo con una forma de realización de la invención. De manera análoga a la tabla de asociación de la figura 2, el nivel de seguridad de aplicación en la tabla de asociación de la figura 3 se incrementa de arriba a abajo. El alcance funcional de la aplicación también se incrementa de arriba a abajo. En particular, se añaden al alcance funcional funcionalidades cada vez más críticas para la seguridad de arriba a abajo.

La aplicación APP está prevista para implementarse en una estación móvil. La aplicación APP tiene la opción de garantizar un nivel de seguridad definido, siempre que los recursos de seguridad SR de la estación móvil sean lo suficientemente seguros para ello. En función del recurso de seguridad (módulo de seguridad, componente) (por ejemplo, terminal REE o TEE o tarjeta SIM) de la estación móvil en el que se vaya a implementar la aplicación APP, se proporcionan variantes de aplicación diferentes.

Los dos niveles de seguridad de aplicación más bajos L1, L2 y, por lo tanto, los recursos de seguridad / módulos de seguridad entorno de tiempo de ejecución normal REE y SE virtual se clasifican como insuficientemente seguros como para que a la aplicación no le corresponda ningún alcance funcional. Como resultado, no hay disponible ninguna variante de aplicación para un entorno de tiempo de ejecución normal y un elemento seguro virtual.

Para un entorno de tiempo de ejecución seguro TEE, controlado por un sistema operativo de seguridad, Secure OS, la aplicación garantiza un nivel de seguridad de aplicación medio L3, siempre que la aplicación solo se haga funcionar como máximo en el alcance funcional Estándar. Como resultado, para la implementación en un entorno de tiempo de ejecución seguro TEE de una estación móvil, se proporciona la variante de aplicación Estándar, que abarca el alcance funcional Estándar de la aplicación APP.

Una tarjeta SIM proporciona a la aplicación APP un nivel de seguridad de aplicación aumentado L4. Como resultado, además del alcance funcional para un entorno de tiempo de ejecución seguro TEE, el alcance funcional de la aplicación APP para la tarjeta SIM puede contener algunas funcionalidades más bien críticas para la seguridad, conforme al alcance funcional Medio, que es mayor que el alcance funcional Estándar. Por lo tanto, para la tarjeta SIM se proporciona la variante de aplicación Media.

Para un elemento seguro integrado eSE en el que la aplicación APP, si se implementa en el mismo, garantiza un nivel de seguridad de aplicación L5, se proporciona la variante de aplicación Avanzada con un alcance funcional Avanzado, elevado.

Para una tarjeta SIM certificada se proporciona la variante de aplicación Plus.

Finalmente, para un elemento seguro integrado eSE certificado, se proporciona la variante de aplicación Premium con el alcance funcional más alto disponible, Premium.

Premium es, a este respecto, opcionalmente el alcance funcional completo, siendo los alcances funcionales Estándar, Medio, Avanzado y Plus alcances funcionales restringidos en diferente medida.

Alternativamente, otro alcance funcional, por ejemplo Medio, es el alcance funcional "completo". En esta alternativa, el Estándar es un alcance funcional restringido y Avanzado, Plus y Premium son alcances funcionales ampliados con servicios adicionales o funcionalidades adicionales.

La figura 4 muestra una activación de una aplicación APP que ya se ha implementado en una estación móvil y está destinada a ejecutarse en un entorno de tiempo de ejecución seguro TEE, de acuerdo con una forma de realización de la invención. La estación móvil comprende un terminal ME, para el que se asume que tiene un entorno de tiempo de ejecución seguro TEE. En la estación móvil, preferiblemente en una tarjeta SIM o en un elemento seguro integrado eSE de la estación móvil (no mostrado) hay implementado un módulo de determinación DIS. El módulo de determinación DIS determina que el recurso de seguridad SR entorno de tiempo de ejecución seguro TEE está realmente presente, por ejemplo, no se ha desinstalado mientras tanto. De manera correspondiente, se asigna el nivel de seguridad de aplicación L3 de acuerdo con la figura 3 a la estación móvil en relación con la aplicación APP. La aplicación APP se activa así con un alcance funcional Estándar.

La figura 5 muestra una selección y descarga de una aplicación APP que se va a implementar, de acuerdo con una forma de realización de la invención. La aplicación APP está disponible en un servidor de aplicaciones SER y se va a cargar en la tarjeta SIM, SIM, de una estación móvil que comprende un terminal móvil ME y la tarjeta SIM. En la tarjeta SIM hay implementado un módulo de determinación DIS. El módulo de determinación DIS determina que la estación móvil tiene la tarjeta SIM y el entorno de tiempo de ejecución seguro TEE del terminal ME como recursos de seguridad SR. En particular, se determina que la tarjeta SIM está realmente presente. A la aplicación APP se le asigna el nivel de seguridad de aplicación L4 utilizando el módulo de determinación DIS de la estación móvil en relación con la tarjeta SIM de acuerdo con la tabla de asociación de la figura 3. El nivel de seguridad de aplicación L4 se transmite desde la estación móvil al servidor de aplicaciones SER. En el servidor de aplicaciones SER, el nivel de seguridad de aplicación L4 transmitido es recibido por el módulo de selección de aplicaciones SEL, que selecciona la variante de aplicación Media correspondiente al nivel de seguridad de aplicación L4 para la tarjeta SIM y la envía a la estación móvil para su implementación en la tarjeta SIM. Finalmente, la aplicación APP se implementa en la variante de aplicación Media en la tarjeta SIM.

La figura 6 muestra una selección y descarga, análogas a la figura 5, de una aplicación APP que se va a implementar, de acuerdo con otra forma de realización de la invención. A diferencia de la figura 5, en la figura 6 se descarga una aplicación para un entorno de tiempo de ejecución seguro TEE. El módulo de determinación DIS está implementado en la tarjeta SIM (recurso de seguridad SR que proporciona el nivel de seguridad más alto). La tarjeta SIM y el entorno de tiempo de ejecución seguro TEE se determinan como recursos de seguridad SR. Dado que la aplicación se va a cargar en el entorno de tiempo de ejecución seguro TEE, el nivel de seguridad de aplicación ASL relevante es ahora el del entorno de tiempo de ejecución seguro TEE, es decir, L3. El módulo de determinación DIS determina L3 como nivel de seguridad de aplicación ASL relevante y lo proporciona al servidor de aplicaciones SER. El módulo de selección de aplicaciones SEL selecciona la variante de aplicación Estándar correspondiente al nivel de seguridad de aplicación L3 y la envía a la estación móvil para su implementación en el entorno de tiempo de ejecución seguro TEE. Finalmente, la aplicación APP se implementa en la variante de aplicación Estándar en el entorno de tiempo de ejecución seguro TEE.

En las formas de realización de las figuras 5, 6, el módulo de determinación DIS está implementado en la tarjeta SIM, ya que esta proporciona el nivel de seguridad más alto. Alternativamente, puede estar previsto que el módulo de determinación DIS esté siempre implementado en un recurso de seguridad implementado permanentemente en el terminal ME, con el fin de evitar que el módulo de determinación DIS sea eliminado de la estación móvil.

REIVINDICACIONES

1. Estación móvil que comprende:

- un terminal móvil (ME),
- recursos de seguridad (SR),
- un módulo de determinación (DIS) implementado en la estación móvil configurado para:

  - determinar los recursos de seguridad (SR) de la estación móvil,
  - derivar al menos un nivel de seguridad (SL) de la estación móvil alcanzado por medio de los recursos de seguridad (SR) y
  - emitir el nivel de seguridad (SL) de la estación móvil que se ha derivado,

caracterizada por que

- la estación móvil contiene, además, información de aplicación sobre al menos una aplicación (APP) implementada o que va implementarse en la estación móvil, en donde, con el módulo de determinación (DIS), como nivel de seguridad se determina y se emite un nivel de seguridad de aplicación (ASL) alcanzado durante un funcionamiento de la aplicación (APP) en la estación móvil utilizando los recursos de seguridad (SR), además de un nivel de seguridad (SL) emitido independientemente del funcionamiento de la aplicación (APP) en la estación móvil, y
- por que un módulo de control de la aplicación acoplado al módulo de determinación (DIS) está configurado para controlar la ejecución de la aplicación (APP) en un alcance funcional que depende del nivel de seguridad de aplicación (ASL) de la aplicación (APP) que se ha derivado, en donde la aplicación puede ejecutarse en un alcance funcional ampliado, en un alcance funcional completo, en un alcance funcional restringido y de manera desactivada y, a medida que se incrementa el alcance funcional de la aplicación (APP), se añaden al alcance funcional funcionalidades críticas para la seguridad.

2. Estación móvil según la reivindicación 1, en donde, como recursos de seguridad (SR), están previstos uno o más de los siguientes módulos de seguridad: un entorno de tiempo de ejecución normal (REE) del terminal (ME), en particular con o sin funciones criptográficas; un módulo de identidad de abonado virtual implementado en el terminal (ME); un entorno de tiempo de ejecución seguro (TEE) del terminal (ME); un módulo de identidad de abonado que puede hacerse funcionar en el terminal (ME), en particular un módulo de identidad de abonado extraíble (SIM), un módulo de identidad de abonado implementado permanentemente (eSE), un módulo de identidad de abonado extraíble certificado, un módulo de identidad de abonado implementado permanentemente certificado; una tarjeta de memoria de microprocesador segura, en particular una tarjeta SD segura y/o una tarjeta Micro SD segura.

3. Estación móvil según la reivindicación 2, en donde se deriva y se emite un nivel de seguridad (SL) para cada módulo de seguridad y/o para cada combinación de uno o más módulos de seguridad de la estación móvil.

4. Estación móvil según una de las reivindicaciones 1 a 3, en donde el módulo de determinación (DIS) está integrado en una interfaz de programación (API) que está configurada:

- para emitir desde la estación móvil información de salida relacionada con los niveles de seguridad (SL) de la estación móvil y/o
- introducir información de control para controlar los niveles de seguridad en la estación móvil.

5. Estación móvil según la reivindicación 4, en donde, como información de salida, pueden emitirse uno o más de los siguientes: un nivel de seguridad (SL) de la estación móvil; un recurso de seguridad (SR) disponible de la estación móvil; un nivel de seguridad (SL) de un recurso de seguridad (SR); todos los niveles de seguridad (SL) de todos los recursos de seguridad (SR) de la estación móvil; todos los recursos de seguridad (SR) disponibles de la estación móvil; el nivel de seguridad (SL) más alto disponible de la estación móvil; un nivel de seguridad (SL) establecido actualmente de la estación móvil; información de funcionalidad sobre las funcionalidades disponibles para uno o para cada nivel de seguridad (SL) o para uno o para cada recurso de seguridad (SR).

6. Estación móvil según la reivindicación 4 o 5, en donde la información de control contiene uno o más de los siguientes: definir el uso de un determinado recurso de seguridad (SR) con un determinado nivel de seguridad (SL); definir el uso del recurso de seguridad (SR) que tiene el nivel de seguridad (SL) más alto.

7. Estación móvil según una de las reivindicaciones 1 a 6, en donde el módulo de determinación (DIS) está implementado en el recurso de seguridad (SR) de la estación móvil que proporciona a la estación móvil el nivel de seguridad (SL) más alto.

8. Estación móvil según una de las reivindicaciones 1 a 6, en donde el módulo de determinación (DIS) está implementado en un recurso de seguridad (SR) de la estación móvil implementado permanentemente en el terminal (ME).

9. Sistema de carga de aplicaciones que comprende una estación móvil según una de las reivindicaciones 1 a 8 y

que comprende un servidor de aplicaciones (SER),
en donde el servidor de aplicaciones (SER) **está caracterizado por**
un módulo de selección de aplicación (SEL) acoplado al módulo de determinación (DIS), configurado para seleccionar una variante de aplicación con un alcance funcional correspondiente al nivel de seguridad de aplicación (ASL) y proporcionar la variante de aplicación seleccionada para su descarga a la estación móvil en función del nivel de seguridad de aplicación (ASL) derivado para una aplicación (APP).

10. Sistema de carga de aplicaciones según la reivindicación 9, en donde la variante de aplicación proporcionada comprende: la aplicación (APP) con el alcance funcional correspondiente al nivel de seguridad de aplicación (ASL) y/o determinadas funcionalidades, en particular funcionalidades adicionales, para complementar la aplicación (APP).

11. Sistema de evaluación de riesgos que comprende una o más estaciones móviles según una de las reivindicaciones 1 a 8 y un servidor de riesgos,
en donde al menos una aplicación (APP) está contenida en al menos una estación móvil,
estando el servidor de riesgos **caracterizado por**
un módulo de evaluación de riesgos acoplado al módulo de determinación (DIS), configurado para derivar un riesgo que emana de la estación móvil o de las diversas estaciones móviles, en función del nivel de seguridad de aplicación (ASL) de la aplicación o aplicaciones (APP) contenidas en la estación móvil o en las estaciones móviles.

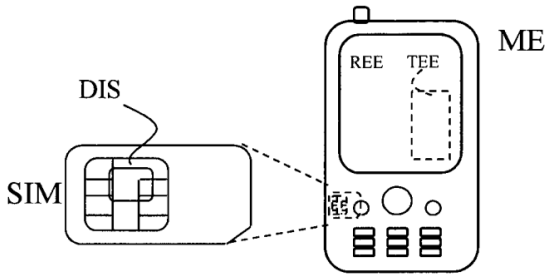

Fig. 1

Recurso de seguridad SR	Nivel de seguridad SL
REE - Rich OS; dado el caso con funciones criptográficas	L1 – mínimo
Elemento seguro virtual	L2 – bajo
TEE – Secure OS	L3 – medio
Tarjeta SIM	L4 – aumentado
Elemento seguro integrado (eSE)	L5 – elevado
Tarjeta SIM certificada	L6 – alto
eSE certificado	L7 – muy alto

Fig. 2

SR	ASL	Alcance funcional App	Variante de aplicación
REE	L1	----	----
SE virt.	L2	----	----
TEE	L3	Estándar	Estándar
SIM	L4	Medio	Media
eSE	L5	Avanzado	Avanzada
SIM cert.	L6	Plus	Plus
eSE cert.	L7	Premium	Premium

Fig. 3

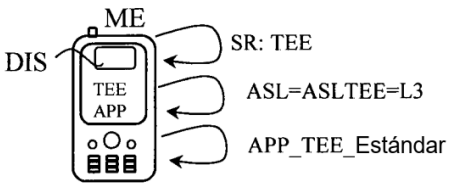

Fig. 4

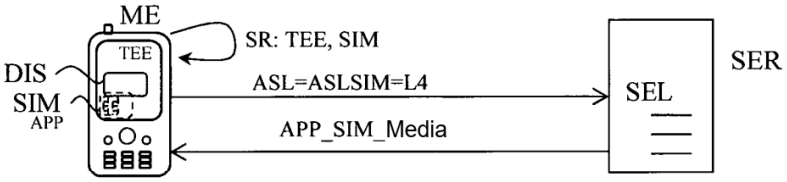

Fig. 5

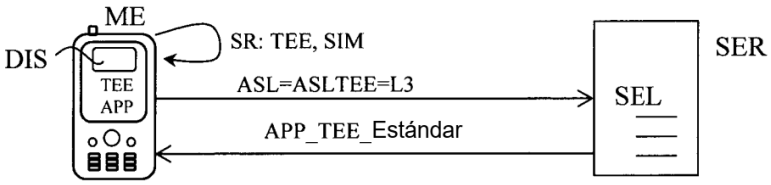

Fig. 6