(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 635 293**

(51) Int. CI.:

G06F 9/445 (2006.01)
G07F 7/10 (2006.01)
G06Q 20/34 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **18.06.2009 PCT/EP2009/004408**

(87) Fecha y número de publicación internacional: **28.01.2010 WO10009789**

(96) Fecha de presentación y número de la solicitud europea: **18.06.2009 E 09776770 (1)**

(97) Fecha y número de publicación de la concesión europea: **10.05.2017 EP 2318921**

(54) Título: **Carga y actualización de una aplicación que requiere personalización**

(30) Prioridad:

21.07.2008 DE 102008033976

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.10.2017

(73) Titular/es:

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

(72) Inventor/es:

BERNARD, EDDY;
NEUBAUER, LUCAS y
MÖNCH, JOACHIM

(74) Agente/Representante:

DURAN-CORRETJER, S.L.P

DESCRIPCIÓN

Carga y actualización de una aplicación que requiere personalización

La invención se refiere a un procedimiento para cargar una aplicación que requiere personalización en un medio de almacenamiento portátil, un procedimiento para actualizar una aplicación almacenada en un medio de almacenamiento portátil, así como a un medio de almacenamiento portátil y a un sistema.

Los medios de almacenamiento portátiles se utilizan para mantener a disposición aplicaciones para diferentes campos de aplicación. El medio de almacenamiento portátil cuenta con una memoria de aplicaciones y un dispositivo de gestión de memoria, p. ej. un controlador de memoria, a través del cual se gestiona la memoria de aplicaciones. El medio de almacenamiento cuenta opcionalmente con un microprocesador, que opcionalmente realiza la tarea de gestionar la memoria. Ejemplos de este tipo de medios de almacenamiento portátiles son las tarjetas inteligentes provistas con un microprocesador y las tarjetas de memoria provistas con un controlador de memoria. Si se utiliza el medio de almacenamiento portátil en el ámbito de la telefonía móvil, el medio de almacenamiento portátil puede realizarse, por ejemplo, como tarjeta inteligente con un módulo de seguridad para el uso de un dispositivo terminal (p. ej. teléfono móvil) en una red de telefonía móvil o estar integrado en una tarjeta inteligente de este tipo. La tarjeta inteligente es, por ejemplo, una tarjeta SIM para el sistema GSM o una tarjeta USIM para el sistema UMTS o una tarjeta inteligente similar. Opcionalmente, el medio de almacenamiento portátil puede estar configurado como tarjeta Pay TV para el uso de televisión de pago o estar integrado en una tarjeta Pay TV de este tipo. Opcionalmente, el medio de almacenamiento portátil es una tarjeta inteligente integrada en una tarjeta Secure Flash, contando la tarjeta Secure Flash con un controlador Flash de orden superior a la tarjeta inteligente.

El medio de almacenamiento portátil se puede leer y escribir mediante un dispositivo terminal. Como dispositivo terminal está previsto, por ejemplo, un dispositivo terminal móvil para una red de telefonía móvil, p. ej. un teléfono móvil, PDA, teléfono inteligente, etc., o un Set-Top Box (decodificador) para televisión de pago (Pay TV). En el caso de un medio de almacenamiento portátil configurado como tarjeta inteligente integrada en una tarjeta Secure Flash, como dispositivo terminal puede estar previsto un controlador Flash o alternativamente un dispositivo terminal móvil como, p. ej. un teléfono móvil, etc., PDA o teléfono inteligente.

Una aplicación para un medio de almacenamiento portátil generalmente debe ser personalizada para el usuario de la aplicación. Inicialmente, la aplicación no está personalizada, es decir, es anónima, y por tanto idéntica y utilizable por cualquier usuario potencial. Después de la personalización, la aplicación inicialmente anónima se convierte en única para el usuario con los datos de personalización. Los datos de personalización comprenden, por ejemplo, datos de identificación personal relacionados con el usuario y datos del dispositivo para el uso del medio de almacenamiento y son necesarios, al menos parcialmente, para que la aplicación pueda ser utilizada en el medio de almacenamiento. Para la personalización, la aplicación se pone a disposición inicialmente en forma no personalizada. A continuación se cargan los datos de personalización en la aplicación y la aplicación es de esta manera personalizada.

Las modificaciones de la aplicación por parte del fabricante o el proveedor (provider) de la aplicación requieren de vez en cuando la carga de una aplicación actualizada en el medio de almacenamiento portátil. Una aplicación actualizada se pone a disposición, p. ej. para solucionar errores de la aplicación o poner a disposición del usuario servicios adicionales o modificados que ofrece la aplicación.

Tradicionalmente, para actualizar una aplicación se cargan en el medio de almacenamiento portátil desde un servidor del fabricante o el proveedor tanto la aplicación actualizada, que inicialmente vuelve a estar no personalizada, como los datos de personalización para personalizar la aplicación a través de una conexión del lado del servidor. En los procedimientos tradicionales para la actualización de una aplicación se requiere que, para cada carga de una aplicación actualizada, el fabricante o el proveedor de la aplicación disponga de los datos de personalización, para que puedan volver a ser cargados en el medio de almacenamiento. Por esta razón, las actualizaciones de aplicaciones tradicionales implican un elevado esfuerzo de gestión para el fabricante o el proveedor de la aplicación. Además, los datos de personalización deben cargarse para cada actualización de la aplicación a través de la conexión del lado del servidor. Puesto que los costes de la conexión del lado del servidor frecuentemente aumentan con la cantidad de datos transmitidos y/o la duración de la conexión, los datos de personalización que deben transmitirse nuevamente con cada actualización generan costes adicionales para el fabricante o el proveedor de la aplicación y para el usuario del medio de almacenamiento. Los costes de la conexión del lado del servidor pueden ser incluso bastante considerables en el caso de actualizaciones de aplicaciones "over the air" (OTA), es decir, en caso de que se utilice como conexión del lado del servidor una conexión por radiofrecuencia (de telefonía móvil). Otro peligro en la transmisión de datos de personalización a través de una conexión del lado del servidor consiste en que los datos de personalización son completamente confidenciales y pueden ser interceptados en cada transmisión del lado del servidor. En el caso de la personalización de una aplicación cargada por primera vez en el entorno seguro del fabricante del medio de almacenamiento ("preissuance"), el peligro de que los datos de personalización puedan ser interceptados a través de la conexión del lado del servidor aún puede ser asumible. Por el contrario, al cargar las aplicaciones actualizadas tras la expedición del medio de almacenamiento por el fabricante ("post-issuance"), el peligro de que los datos de personalización puedan ser interceptados a través de la conexión del lado del servidor es grande.

El documento EP 1 936 574 A1 describe la carga de una aplicación Java Card que requiere personalización en una tarjeta Java Card. La aplicación y los datos de personalización se cargan juntos en un paquete en la tarjeta Java Card para la personalización de la aplicación. La aplicación se instala en la tarjeta Java Card y a continuación la aplicación instalada es personalizada con los datos de personalización del paquete.
El documento GB 2 358 500 A da a conocer un procedimiento para cargar una aplicación desde un terminal en un medio de almacenamiento portátil (target smart card). Para ello se cargan los datos de personalización (customer details) y una aplicación no personalizada (generic application) en un chip del terminal. Dentro del chip del terminal se personaliza la aplicación no personalizada con los datos de personalización. A continuación, la aplicación personalizada se carga en el medio de almacenamiento portátil.
La invención tiene como objetivo crear un procedimiento para cargar una aplicación que requiere personalización en un medio de almacenamiento portátil de forma eficiente, económica y al mismo tiempo segura, así como un procedimiento para actualizar una aplicación almacenada en un medio de almacenamiento portátil. También se plantea proporcionar un medio de almacenamiento portátil correspondiente y un sistema con medio de almacenamiento y dispositivo terminal. El objetivo se consigue mediante un procedimiento de carga según la reivindicación independiente 1. Además se especifican un procedimiento de actualización según la reivindicación independiente 3, un medio de almacenamiento portátil según la reivindicación 8 y un sistema con un medio de almacenamiento portátil según la reivindicación 14. Las realizaciones preferentes de la invención se especifican en las reivindicaciones dependientes. A continuación se explica la invención en detalle en base a ejemplos de realización y haciendo referencia a los dibujos, donde se muestran:

la figura 1, un diagrama que ilustra la carga de una aplicación que requiere personalización, según un primer modo de realización de la invención;
la figura 2, la carga de una aplicación que requiere personalización, según un segundo modo de realización de la invención;
la figura 3, la carga de una aplicación que requiere personalización, según un tercer modo de realización de la invención;
la figura 4, la carga de una aplicación que requiere personalización, según un cuarto modo de realización de la invención;
la figura 5, la carga de una aplicación actualizada, según un primer modo de realización de la invención;
la figura 6, la carga de los datos de personalización en el procedimiento de la figura 5;
la figura 7, la carga de datos de personalización en una aplicación actualizada, según un segundo modo de realización de la invención;
la figura 8, la carga de la aplicación actualizada y personalizada en el procedimiento de la figura 7;
la figura 9, una representación esquemática de la estructura de un medio de almacenamiento portátil, según un modo de realización de la invención;
la figura 10, una representación esquemática de un medio de almacenamiento portátil interactuando con un dispositivo terminal, según un modo de realización de la invención;
la figura 11, una representación esquemática de un medio de almacenamiento portátil interactuando con un dispositivo terminal, según otro modo de realización de la invención;
la figura 12, una representación esquemática de un medio de almacenamiento portátil interactuando con un dispositivo terminal, según otro modo de realización de la invención.

La reivindicación 1 especifica un procedimiento para cargar una aplicación que requiere personalización, para un medio de almacenamiento portátil configurado para operar en un dispositivo terminal, dicha aplicación siendo cargada en el medio de almacenamiento, tal que

- la aplicación y los datos de personalización se ponen a disposición en un servidor dispuesto fuera del medio de almacenamiento y fuera del dispositivo terminal, dicho servidor pudiéndose conectar para la transmisión de aplicaciones y datos de personalización, a través de una conexión del lado del servidor, con el medio de almacenamiento portátil y/o el dispositivo terminal,
- la aplicación se carga al menos parcialmente a través de la conexión del lado del servidor en una memoria de aplicaciones del medio de almacenamiento,
- los datos de personalización se cargan en la aplicación de forma que la aplicación es personalizada con los datos de personalización y
- los datos de personalización se cargan en un módulo de recuperación que es independiente de las aplicaciones almacenadas en la memoria de aplicaciones, está configurado como memoria no volátil y está dispuesto dentro del medio de almacenamiento portátil.

Además de ser cargados en la aplicación, los datos de personalización son cargados al menos parcialmente y almacenados de forma no volátil en un módulo de recuperación independiente de la aplicación y, dado el caso, de otras aplicaciones. Gracias a que los datos de personalización se mantienen a disposición en el módulo de recuperación del propio medio de almacenamiento, una aplicación actualizada a cargar posteriormente en el medio de almacenamiento puede ser personalizada con los datos de personalización del módulo de recuperación. No es necesario que el fabricante o el proveedor de la aplicación mantengan disponibles los datos de personalización fuera del medio de almacenamiento y fuera del dispositivo terminal. Además, la personalización de la aplicación

actualizada puede tener lugar sin establecer una conexión del lado del servidor. Gracias a ello se reduce el esfuerzo de gestión para el fabricante o el proveedor de la aplicación. Además se reducen los costes para la carga posterior de la aplicación actualizada, ya que a través de la conexión del lado del servidor solo se debe transmitir la aplicación, pero no los datos de personalización. El ahorro de costes beneficia tanto al fabricante o proveedor de la aplicación, como también al usuario del medio de almacenamiento. Además, las actualizaciones posteriores de las aplicaciones son especialmente seguras porque ya no se transmiten datos de personalización a través de la conexión del lado del servidor.

Según la invención, el módulo de recuperación está dispuesto dentro del medio de almacenamiento. Esta característica tiene la ventaja de que el módulo de recuperación está previsto de forma independiente del dispositivo terminal utilizado y dispuesto de forma inmediatamente contigua a la memoria de aplicaciones. Esto permite proteger el módulo de recuperación de forma más sencilla contra el acceso no autorizado al contenido de la memoria a como si estuviera fuera del medio de almacenamiento.

Por lo tanto, según la reivindicación 1 se obtiene un procedimiento para cargar una aplicación que requiere personalización en un medio de almacenamiento portátil de forma eficiente, económica y segura.

En el caso de un procedimiento según la invención para operar un medio de almacenamiento portátil en un dispositivo terminal, el medio de almacenamiento portátil contiene una aplicación que ha sido cargada en el medio de almacenamiento portátil según la invención, tal como se ha descrito anteriormente. Durante la operación del medio de almacenamiento, la aplicación almacenada en la memoria de aplicaciones y personalizada genera datos de aplicación, a través de los cuales se modifica la aplicación almacenada y personalizada, o la aplicación recibe dichos datos de aplicación de fuera del medio de almacenamiento.

Los datos de aplicación son cargados según la invención en su totalidad o al menos parcialmente en el módulo de recuperación. En una actualización posterior de la aplicación, las modificaciones realizadas a la aplicación originalmente almacenada en la memoria de aplicaciones pueden transmitirse a la aplicación actualizada cargando los datos de aplicación cargados desde la aplicación original en el módulo de recuperación desde el módulo de recuperación en la aplicación actualizada.

Como datos de aplicación generados por la aplicación están previstos, por ejemplo, los contenidos o estados de contadores de archivos de registro o contadores que son modificados durante la ejecución de la aplicación. Como datos de aplicación cargados desde fuera del medio de almacenamiento en la aplicación y recibidos por la aplicación están previstos, por ejemplo, para una tarjeta Pay TV, autorizaciones de recepción para la recepción de contenidos de datos (p. ej. programas de televisión). Dichas autorizaciones de recepción se modifican a intervalos regulares o irregulares por iniciativa del propietario de la tarjeta o del proveedor de datos. Alternativamente, como datos de aplicación están previstos otros datos generados en la aplicación o recibidos durante la operación del medio de almacenamiento, que actúan modificando la aplicación.

Opcionalmente, la aplicación se carga en su totalidad a través de la conexión del lado del servidor desde el servidor directamente en la memoria de aplicaciones dentro del medio de almacenamiento. Opcionalmente, si la aplicación solo se carga parcialmente a través de la conexión del lado del servidor, la aplicación se carga, por ejemplo, a través de la conexión del lado del servidor en el dispositivo terminal y a continuación, a través de una conexión externa entre el dispositivo terminal y el medio de almacenamiento (más adelante denominada conexión externa, por contraposición a una conexión interna de dentro del medio de almacenamiento) desde el dispositivo terminal en el medio de almacenamiento.

La aplicación es personalizada con los datos de personalización opcionalmente fuera de la memoria de aplicaciones o dentro de la memoria de aplicaciones. En el caso de una personalización fuera de la memoria de aplicaciones, tal como se muestra en la figura 1, se cargan opcionalmente, en primer lugar, los datos de personalización en la aplicación para luego personalizar la aplicación con los datos de personalización y, a continuación, se carga la aplicación personalizada en la memoria de aplicaciones. En el caso de una personalización dentro de la memoria de aplicación, que se muestra en la figura 2 y la figura 3, en primer lugar se carga la aplicación no personalizada, es decir, que aún requiere personalización, en la memoria de aplicaciones. A continuación se cargan los datos de personalización en la aplicación que ya se encuentra en la memoria de aplicaciones, tal que la aplicación es personalizada con los datos de personalización dentro de la memoria de aplicaciones. Los datos de personalización son almacenados opcionalmente, en primer lugar, en la memoria de aplicaciones y a continuación almacenados desde la memoria de aplicaciones en el módulo de recuperación (figura 2) o, en primer lugar, almacenados en el módulo de recuperación y a continuación desde el módulo de recuperación en la memoria de aplicaciones (figura 3).

En el caso en que la aplicación sea personalizada fuera de la memoria de aplicaciones, la aplicación puede ser personalizada opcionalmente en el servidor incluso por el fabricante o el proveedor de la aplicación. De este modo, a través de la conexión del lado del servidor se transmite la aplicación personalizada. Alternativamente, la aplicación es personalizada en el dispositivo terminal pero fuera del medio de almacenamiento y la aplicación personalizada se carga a través de la conexión externa desde el dispositivo terminal en el medio de almacenamiento, más

precisamente en la memoria de aplicaciones. En esta variante, los datos de personalización y la aplicación no personalizada son transmitidos a través de la conexión del lado del servidor.

La aplicación cargada en la memoria de aplicaciones se instala en caso necesario en la memoria de aplicaciones. En caso necesario, los datos de personalización se cargan en la aplicación instalada.

Opcionalmente, la aplicación es una aplicación Java Card o una Java Card Applet según la especificación de la máquina virtual de Java Card (JCVM Spec, p. ej. versión 2.0, 2.2, 2.2.1, 2.2.2, 3.0). En este caso, la aplicación y los datos de personalización en un paquete común se cargan opcionalmente en el dispositivo terminal o en el medio de almacenamiento. El paquete es, por ejemplo, un archivo Java Card CAP, opcionalmente almacenado en un archivo Java Card JAR. Los datos de personalización están contenidos opcionalmente en un «Custom Component» (JCVM Spec 3.0, capítulo 6.1.2) de un archivo CAP o archivo JAR. El Custom Component es almacenado, según la invención, en su totalidad o al menos parcialmente en el módulo de recuperación. Una aplicación actualizada cargada posteriormente se puede personalizar con el Custom Component del módulo de recuperación.

La invención proporciona además un procedimiento para actualizar una aplicación personalizada para el medio de almacenamiento, almacenada en un medio de almacenamiento portátil configurado para operar en un dispositivo terminal, mediante la carga de una aplicación actualizada, por la cual se debe sustituir la aplicación almacenada, y mediante la carga de datos de personalización para personalizar la aplicación actualizada, tal que - la aplicación actualizada se pone a disposición en un servidor dispuesto fuera del medio de almacenamiento y fuera del dispositivo terminal, dicho servidor pudiéndose conectar para la transmisión de aplicaciones actualizadas a través de una conexión del lado del servidor con el medio de almacenamiento portátil y/o el dispositivo terminal,

- la aplicación actualizada se carga en una memoria de aplicaciones del medio de almacenamiento, lo que tiene lugar al menos parcialmente a través de la conexión del lado del servidor, y
- los datos de personalización se cargan desde un módulo de recuperación en la aplicación actualizada, de forma que la aplicación actualizada es personalizada con los datos de personalización, tal que el módulo de recuperación es independiente de las aplicaciones y/o aplicaciones actualizadas almacenadas en la memoria de aplicaciones, está configurado como memoria no volátil y está dispuesto dentro del medio de almacenamiento portátil.

La personalización de la aplicación actualizada tiene lugar con los datos de personalización almacenados en el módulo de recuperación y sin establecer una conexión del lado del servidor. Por lo tanto, no es necesario ni que el fabricante o el proveedor de la aplicación actualizada mantengan a disposición los datos de personalización, ni una conexión del lado del servidor. Las transmisiones de los datos de personalización para personalizar la aplicación actualizada tienen lugar exclusivamente dentro del sistema cerrado formado por el medio de almacenamiento portátil y el dispositivo terminal, pero no a través de conexiones del lado del servidor. Por esta razón, el procedimiento según la invención para actualizar una aplicación es especialmente económico y especialmente seguro.

La aplicación que debe ser sustituida por la aplicación actualizada ha sido cargada, por ejemplo, conforme al procedimiento según la invención para cargar una aplicación en el medio de almacenamiento, habiendo sido cargados también los datos de personalización en el módulo de recuperación.

Opcionalmente, en el procedimiento para actualizar una aplicación, la aplicación que debe sustituirse, almacenada en la memoria de aplicaciones (y dado el caso instalada) y personalizada, ha generado datos de aplicación durante una operación previa del medio de almacenamiento, a través de los cuales se ha modificado la aplicación almacenada y personalizada. Los datos de aplicación se han cargado en su totalidad o al menos parcialmente en el módulo de recuperación. En una actualización de la aplicación mediante la carga de la aplicación actualizada, los datos de aplicación que se han cargado desde la aplicación original en el módulo de recuperación, son cargados desde el módulo de recuperación en la aplicación actualizada, de forma que la aplicación actualizada es modificada con los datos de aplicación. De este modo, las modificaciones realizadas a la aplicación originalmente almacenada en la memoria de aplicaciones pueden transmitirse a la aplicación actualizada.

Opcionalmente, la aplicación es borrada de la memoria de aplicaciones. Opcionalmente, la aplicación es borrada después de haber cargado la aplicación actualizada en la memoria de aplicaciones. Opcionalmente, la aplicación es sobrescrita con la aplicación actualizada.

La variante de la invención en la que también los datos de aplicación son almacenados en el módulo de recuperación y son cargados en la aplicación actualizada tiene la ventaja adicional de que los datos de aplicación, que podrían perderse especialmente en el caso de borrar la aplicación original, se mantienen disponibles para la aplicación actualizada.

Opcionalmente, la aplicación actualizada se carga en su totalidad a través de la conexión del lado del servidor desde el servidor directamente en la memoria de aplicaciones dentro del medio de almacenamiento. Opcionalmente, si la aplicación actualizada solo se carga parcialmente a través de la conexión del lado del servidor, la aplicación actualizada se carga, por ejemplo, a través de la conexión del lado del servidor en el dispositivo terminal y, a

continuación, a través de una conexión externa entre el dispositivo terminal y el medio de almacenamiento en el medio de almacenamiento.

La aplicación actualizada es personalizada opcionalmente dentro de la memoria de aplicaciones (mostrado a modo de ejemplo en las figuras 4 y 5) o fuera de la memoria de aplicaciones, p. ej. dentro del dispositivo terminal, (mostrado a modo de ejemplo en las figuras 6 y 7) con los datos de personalización. No obstante, la aplicación actualizada es personalizada siempre con los datos de personalización del módulo de recuperación y sin establecer una conexión del lado del servidor.

Opcionalmente, la conexión del lado del servidor está configurada como conexión por radiofrecuencia (OTA, "over the air"), especialmente como conexión de telefonía móvil.

Opcionalmente, el módulo de recuperación está protegido contra el acceso. La protección de acceso se consigue opcionalmente a través de un requerimiento de autenticación y/o mediante un almacenamiento cifrado de los datos en el módulo de recuperación. Opcionalmente, el acceso a los datos de personalización almacenados en el módulo de recuperación se permite a lo sumo para una carga autorizada de una aplicación o aplicación actualizada en el medio de almacenamiento. Por ejemplo, para cargar una aplicación o aplicación actualizada es necesaria una autenticación. La autenticación para la carga de la aplicación comprende opcionalmente una autenticación para un acceso a los datos de personalización en el módulo de recuperación. Opcionalmente, los datos de personalización son almacenados de tal modo en el módulo de recuperación que permanecen almacenados de forma cifrada en el módulo de recuperación.

Un medio de almacenamiento portátil según la invención está configurado para realizar un procedimiento según la invención y cuenta con una memoria de aplicaciones que está configurada para almacenar aplicaciones, así como con un módulo de recuperación que está configurado como memoria no volátil y es independiente de las aplicaciones almacenadas en la memoria de aplicaciones. El módulo de recuperación está configurado para mantener a disposición los datos de personalización para personalizar aplicaciones o aplicaciones actualizadas en la memoria de aplicaciones, de forma que es posible una personalización de una aplicación (actualizada) sin que el fabricante o proveedor de la aplicación mantenga a disposición los datos de personalización y sin una conexión del lado del servidor.

El medio de almacenamiento portátil está provisto opcionalmente con un microprocesador. Opcionalmente, el medio de almacenamiento es una tarjeta Java Card. La aplicación está configurada opcionalmente como aplicación Java Card o Java Card Applet. Opcionalmente, el medio de almacenamiento está configurado como tarjeta Pay TV para el uso de televisión de pago o integrado en una tarjeta Pay TV de este tipo. Opcionalmente, el medio de almacenamiento está configurado como tarjeta inteligente con un módulo de seguridad para el uso de un dispositivo terminal en una red de telefonía móvil, p. ej. tarjeta (U)SIM, o está integrado en una tarjeta inteligente de este tipo (p. ej. tarjeta (U)SIM). Opcionalmente, el medio de almacenamiento está configurado como tarjeta Secure Flash, presentando un controlador y una memoria Flash, o está integrado en una tarjeta Secure Flash de este tipo.

Como dispositivo terminal está previsto, por ejemplo, un dispositivo terminal móvil como, p. ej., un teléfono móvil, PDA, teléfono inteligente o similar, un Set-Top Box (decodificador) para televisión de pago (Pay TV) o un controlador de una tarjeta Secure Flash.

El módulo de recuperación y la memoria de aplicaciones se pueden conectar entre sí para el intercambio de datos preferentemente a través de una conexión interna. El medio de almacenamiento, especialmente el módulo de recuperación y la memoria de aplicaciones, se pueden conectar entre sí para el intercambio de datos preferentemente a través de una o varias conexiones externas. La o las varias conexiones externas pueden ser, en particular, conexiones según ISO/IEC 7816-3&4.

Un sistema según la invención con un medio de almacenamiento portátil y un dispositivo terminal para operar el medio de almacenamiento está configurado para realizar un procedimiento según la invención. El sistema dispone de una memoria de aplicaciones en el medio de almacenamiento, configurada para almacenar aplicaciones. El sistema cuenta además con un módulo de recuperación en el medio de almacenamiento, que está configurado como memoria no volátil y es independiente de las aplicaciones almacenadas en la memoria de aplicaciones. El medio de almacenamiento portátil está configurado opcionalmente como se ha descrito anteriormente.

El módulo de recuperación está configurado opcionalmente como aplicación, por ejemplo, como aplicación Java Card o Java Card Applet, opcionalmente como un grupo de varias aplicaciones que interactúan, opcionalmente como biblioteca, p. ej. como Java Card Library, o como grupo de bibliotecas que interactúan.

Una personalización en relación con la invención puede realizarse opcionalmente antes de la expedición del medio de almacenamiento por parte del fabricante del mismo ("pre-issuance") o después de la expedición del medio de almacenamiento por parte del fabricante del mismo ("post-issuance"). Una personalización post-issuance es realizada, por ejemplo, por un proveedor de aplicaciones diferente del fabricante del medio de almacenamiento.

La carga de datos de personalización desde el módulo de recuperación y en el módulo de recuperación tiene lugar opcionalmente por orden de una aplicación personalizada o a personalizar o por orden del módulo de recuperación o por orden de una tercera instancia diferente de la aplicación personalizada o a personalizar y del módulo de recuperación. Esta tercera instancia está configurada opcionalmente como otra aplicación.
Una aplicación cargada en la memoria de aplicaciones o una aplicación actualizada se instala en caso necesario en la memoria de aplicaciones. En caso necesario, los datos de personalización se cargan en la aplicación instalada o en la aplicación actualizada.

Las figuras 1 a 4 muestran cuatro modos de realización de la carga de una aplicación -AP- que requiere personalización en una tarjeta inteligente -SC- (medio de almacenamiento portátil), que es operada en un dispositivo terminal -EG-. La carga de la aplicación -AP- en la tarjeta inteligente -SC- no está representada sino tan solo la carga de los datos de personalización -PD- para personalizar la aplicación -AP-. Con flechas señaladas con -Lx-, x=1,2,3, S están representadas las conexiones para la transmisión de datos, que también están representadas en la figura 9.

En un primer modo de realización según la figura 1, los datos de personalización -PD- para personalizar la aplicación -AP- son almacenados desde un servidor -SER- fuera de la tarjeta inteligente -SC- y fuera del dispositivo terminal -EG-, a través de una conexión del lado del servidor -LS-, por un lado, en la aplicación -AP- almacenada en la memoria de aplicaciones -AS-, de forma que la aplicación -AP- es personalizada, y, por otro lado, en un módulo de recuperación (módulo Backup) - BM-, por lo que son mantenidos a disposición para posteriores personalizaciones de aplicaciones actualizadas cargadas posteriormente.

En un segundo modo de realización según la figura 2, los datos de personalización -PD- para personalizar la aplicación -AP- son almacenados desde un servidor -SER- fuera de la tarjeta inteligente -SC- y fuera del dispositivo terminal -EG-, a través de una conexión del lado del servidor -LS-, a la aplicación -AP- almacenada en la memoria de aplicaciones -AS-, de forma que la aplicación -AP- es personalizada. Los datos de personalización -PD- son almacenados desde la memoria de aplicaciones -AS-, a través de una conexión interna -L3-, en el módulo de recuperación (módulo Backup) -BM-.

En un tercer modo de realización según la figura 3, a diferencia del de la figura 2, los datos de personalización -PD- son almacenados en primer lugar desde un servidor -SER- fuera de la tarjeta inteligente -SC- y fuera del dispositivo terminal -EG- a través de una conexión del lado del servidor -LS- en el módulo de recuperación -BM- y, a continuación del módulo de recuperación -BM-, a través de una conexión interna -L3- en la aplicación -AP- almacenada en la memoria de aplicaciones -AS-, de forma que la aplicación -AP- es personalizada.

En un cuarto modo de realización según la figura 4, la aplicación -AP- es personalizada en el servidor -SER- fuera de la tarjeta inteligente -SC- y fuera del dispositivo terminal -EG-. A través de una conexión del lado del servidor -LS- se cargan los datos de personalización en el módulo de recuperación -BM- y la aplicación personalizada, en la memoria de aplicaciones -AS-.

En modos de realización a partir de las figuras 1 a 4, a diferencia de lo representado en las figuras 1 a 4, la conexión del lado del servidor -LS- desde el servidor -SER- puede llegar opcionalmente solo hasta el dispositivo terminal -EG- y la siguiente conexión a la tarjeta inteligente -SC- estar formada por una conexión -L1- o -L2- externa, tal como se representa en la figura 9.

Las figuras 5 a 8 muestran la carga de una aplicación actualizada -A-AP- en una tarjeta inteligente -SC- (medio de almacenamiento portátil), que es operada en un dispositivo terminal -EG-. Las flechas -Lx- representan conexiones (véase también figura 9).

En un primer modo de realización de la carga de una aplicación actualizada -A-AP-, representada en las figuras 5 y 6, la aplicación actualizada -A-AP- se carga a través de una conexión del lado del servidor -LS- en forma no personalizada en la memoria de aplicaciones -AS- de la tarjeta inteligente -SC- (figura 5). A continuación se cargan al módulo de recuperación (módulo Backup) -BM- los datos de personalización -PD- y, dado el caso, los datos de aplicación -AD-, que fueron cargados, p. ej., según cualquiera de las figuras 1 a 4, a través de una conexión -L3- interna desde el módulo de recuperación -BM- en la aplicación actualizada -A-AP-, de forma que se personaliza la aplicación actualizada -A-AP- (figura 6).

En un segundo modo de realización de la carga de una aplicación actualizada -A-AP-, representada en las figuras 7 y 8, la aplicación actualizada -A-AP- se carga de forma no personalizada desde el servidor -SER- a través de una conexión del lado del servidor -LS- en el dispositivo terminal -EG-. Los datos de personalización -PD- y, dado el caso, los datos de aplicación -AD- son cargados a través de una conexión -L2- externa desde el módulo de recuperación -BM- en la aplicación actualizada -A-AP- mantenida a disposición en el dispositivo terminal -EG-, de forma que la aplicación actualizada -A-AP- es personalizada fuera de la tarjeta inteligente -SC- y al mismo tiempo fuera del dispositivo terminal -EG- (figura 7). A continuación, la aplicación actualizada personalizada -A-AP+PD-(+AD) se carga a través de una conexión -L1- externa en la memoria de aplicaciones -AS- de la tarjeta inteligente -SC- (figura 8).

La figura 9 muestra esquemáticamente la estructura de una tarjeta inteligente -SC- según un modo de realización de la invención. La tarjeta inteligente está configurada como tarjeta Java Card. La tarjeta inteligente -SC- es operada en un dispositivo terminal -EG-. El módulo de recuperación -BM- y la memoria de aplicaciones -AS- están acoplados a través de una interfaz interna -API-, p. ej. una Application Programming Interface (API), a través de la cual se puede establecer una conexión -L3- interna (flecha -L3-). El módulo de recuperación -BM- y la memoria de aplicaciones -AS- están acoplados a través de una interfaz externa -APDU-, p. ej. una interfaz -APDU-, a un dispositivo terminal externo, a través de la cual se pueden establecer las conexiones -L2- o -L1- externas. A través de la interfaz interna -API- se pueden transmitir datos de personalización -PD- y, dado el caso, datos de aplicación -AD- en la conexión -L3- interna, opcionalmente desde el módulo de recuperación -BM- a la memoria de aplicaciones -AS- o desde la memoria de aplicaciones -AS- al módulo de recuperación -BM-. A través de la interfaz externa -APDU- se pueden cargar, p. ej., datos de personalización -PD-, aplicaciones -AP-, aplicaciones actualizadas -A-AP-, aplicaciones actualizadas personalizadas a través de la primera conexión -L1- externa desde el dispositivo terminal -EG- de la tarjeta inteligente -AC- en la memoria de aplicaciones -AS-. A través de una segunda conexión -L2- externa de la interfaz externa -APDU- se pueden trasmitir datos de personalización desde el dispositivo terminal -EG- al módulo de recuperación -BM- y viceversa, desde el módulo de recuperación -BM-, hacia afuera de la tarjeta inteligente -SC-. Las conexiones al servidor -SER- se establecen a través de conexiones del lado del servidor -LS- (flechas -LS-), que se pueden establecer entre el servidor -SER-, por un lado, y el dispositivo terminal -EG-, el módulo de recuperación -BM- o la memoria de aplicaciones -AS-, por el otro lado.

Las figuras 10 a 12 muestran, en representación esquemática, medios de almacenamiento -SC- portátiles interactuando con dispositivos terminales -EG- según modos de realización de la invención. El medio de almacenamiento -SC- portátil, provisto con una memoria de aplicaciones -AS- y un módulo de recuperación -BM-, está configurado como tarjeta inteligente -SC- y construido, por ejemplo, como se representa en las figuras 1 a 9.

La figura 10 muestra una tarjeta inteligente -SC- que está introducida en un dispositivo terminal -EG-, estando controlada la lectura de datos de la tarjeta inteligente -SC- (flecha -R-) y la escritura de datos en la tarjeta inteligente -SC- (flecha -W-) por el dispositivo terminal -EG-. El dispositivo terminal en la figura 10 es, por ejemplo, un teléfono móvil o un dispositivo terminal móvil similar o un Set-Top Box (decodificador) para Pay TV. La tarjeta inteligente -SC- es correspondientemente, p. ej., una tarjeta (U)SIM o una tarjeta Pay TV. La carga según la invención de datos de personalización -PD- desde el módulo de recuperación -BM- en una aplicación actualizada -A-AP-, p. ej., según las figuras 6 o 7, es controlada en la configuración de la figura 10 por el dispositivo terminal -EG-.

La figura 11 muestra una tarjeta inteligente -SC- integrada en una tarjeta Secure Flash -SFC-. La tarjeta Secure Flash -SFC- cuenta además con un controlador -CON- y una memoria Flash -FL- y está introducida en un dispositivo terminal -EG-. La memoria de aplicaciones -AS- para aplicaciones -AP- y aplicaciones actualizadas -A-AP- y el módulo de recuperación -BM- están dispuestos dentro de una tarjeta inteligente -SC-. La lectura de datos de la tarjeta inteligente -SC- (flecha -R-) y la escritura de datos en la tarjeta inteligente -SC- (flecha -W-) están controladas en la configuración de la figura 11 por el controlador -CON- de la tarjeta Secure Flash -SFC-. La carga según la invención de datos de personalización -PD- y, dado el caso, datos de aplicación -AD-, desde el módulo de recuperación -BM- en una aplicación actualizada -A-AP-, p. ej., según las figuras 6 o 7, es controlada en la configuración de la figura 11 por el controlador -CON- de la tarjeta Secure Flash -SFC-.

La figura 12 muestra una configuración similar a la de la figura 11, con la diferencia de que la lectura de datos de la tarjeta inteligente -SC- (flecha -R-) y la escritura de datos en la tarjeta inteligente -SC- (flecha -W-), p. ej. la carga de datos de personalización -PD- y, dado el caso, de datos de aplicación -AD- desde el módulo de recuperación -BM- en una aplicación actualizada -A-AP-, no están controladas por el controlador -CON- de la tarjeta Secure Flash -SFC-, sino por el dispositivo terminal.

REIVINDICACIONES

1. Procedimiento para cargar una aplicación (AP) que requiere personalización, para un medio de almacenamiento (SC) portátil configurado para operar en un dispositivo terminal (EG), dicha aplicación siendo cargada en el medio de almacenamiento (SC) portátil, tal que

- la aplicación (AP) y los datos de personalización (PD) se ponen a disposición en un servidor (SER) dispuesto fuera del medio de almacenamiento y fuera del dispositivo terminal (EG), dicho servidor pudiéndose conectar para la transmisión de aplicaciones (AP) y datos de personalización (PD) a través de una conexión del lado del servidor (LS) con el medio de almacenamiento (SC) portátil y/o el dispositivo terminal (EG),
- la aplicación (AP) se carga al menos parcialmente a través de la conexión del lado del servidor en una memoria de aplicaciones (AS) del medio de almacenamiento (SC),
-los datos de personalización (PD) se cargan en la aplicación (AP) de forma que la aplicación (AP) es personalizada con los datos de personalización (PD) y
- los datos de personalización (PD) se cargan al menos parcialmente en un módulo de recuperación (BM) que es independiente de las aplicaciones (AP) almacenadas en la memoria de aplicaciones (AS), está configurado como memoria no volátil y está dispuesto dentro del medio de almacenamiento (SC) portátil.

2. Procedimiento para operar un medio de almacenamiento (SC) portátil con una aplicación (AP), que fue cargada según el procedimiento de la reivindicación 1 en el medio de almacenamiento (SC) portátil, en un dispositivo terminal (EG), tal que

- durante la operación del medio de almacenamiento (SC), la aplicación (AP) almacenada en la memoria de aplicaciones y personalizada genera o recibe datos de aplicación (AD), a través de los cuales se modifica la aplicación (AP) almacenada y personalizada, y
- los datos de aplicación (AD) se cargan al menos parcialmente en el módulo de recuperación (BM).

3. Procedimiento para actualizar una aplicación (AP) para un medio de almacenamiento (SC), almacenada en el medio de almacenamiento (SC) portátil configurado para operar en un dispositivo terminal (EG), mediante la carga de una aplicación actualizada (A-AP), por la cual se debe sustituir la aplicación (AP) almacenada, y mediante la carga de datos de personalización (PD) para personalizar la aplicación actualizada (A-AP), tal que

- la aplicación actualizada (A-AP) se pone a disposición en un servidor (SER) dispuesto fuera del medio de almacenamiento (SC) y fuera del dispositivo terminal (EG), dicho servidor pudiéndose conectar para la transmisión de aplicaciones actualizadas (A-AP) a través de una conexión del lado del servidor (LS) con el medio de almacenamiento (SC) portátil y/o el dispositivo terminal (EG),
- la aplicación actualizada (A-AP) se carga al menos parcialmente a través de la conexión del lado del servidor (LS) en una memoria de aplicaciones (AS) del medio de almacenamiento (SC), y
- los datos de personalización (PD) se cargan desde un módulo de recuperación (BM) en la aplicación actualizada (A-AP), de forma que la aplicación actualizada (A-AP) es personalizada con los datos de personalización (PD), tal que el módulo de recuperación (BM) es independiente de las aplicaciones (AP) y/o aplicaciones actualizadas (A-AP) almacenadas en la memoria de aplicaciones (AS), está configurado como memoria no volátil y está dispuesto dentro del medio de almacenamiento (SC) portátil.

4. Procedimiento, según la reivindicación 3, en el que la aplicación (AP) almacenada en la memoria de aplicaciones y personalizada ha generado o recibido datos de aplicación (AD) durante una operación previa del medio de almacenamiento (SC), a través de los cuales se ha modificado la aplicación (AP) almacenada y personalizada y los datos de aplicación (AD) se han cargado al menos parcialmente en el módulo de recuperación (BM), tal que

- los datos de aplicación (AD) son cargados desde el módulo de recuperación (BM) en la aplicación actualizada (A-AP) de forma que la aplicación actualizada (A-AP) es modificada con los datos de aplicación (AD).

5. Procedimiento, según una cualquiera de las reivindicaciones 3 o 4, en el que la aplicación (AP) es borrada de la memoria de aplicaciones (AS).

6. Procedimiento, según una cualquiera de las reivindicaciones 1 a 5, en el que la conexión del lado del servidor (LS) está configurada como conexión por radiofrecuencia.

7. Procedimiento, según una cualquiera de las reivindicaciones 1 a 6, en el que el módulo de recuperación (BM) está asegurado contra el acceso y un acceso a los datos de personalización (PD) así como, dado el caso, a los datos de aplicación (AD) almacenados en el módulo de recuperación (BM) se permite a lo sumo para una carga autorizada de una aplicación (AP) o aplicación actualizada (A-AP) en el medio de almacenamiento (SC).

8. Medio de almacenamiento (SC) portátil configurado para realizar un procedimiento según una cualquiera de las reivindicaciones 1 a 7, que presenta:

- una memoria de aplicaciones (AS) configurada para almacenar aplicaciones (AP; A-AP),
- un módulo de recuperación (BM) que está configurado como memoria no volátil y es independiente de las aplicaciones (AP; A-AP) almacenadas en la memoria de aplicaciones (AS).

9. Medio de almacenamiento (SC) portátil, según la reivindicación 8, tal que el medio de almacenamiento (SC) está provisto con un microprocesador.

10. Medio de almacenamiento (SC) portátil, según una cualquiera de las reivindicaciones 8 o 9, tal que la aplicación (AP; A-AP) está configurada como aplicación Java Card o Java Card Applet.

11. Medio de almacenamiento (SC) portátil, según una cualquiera de las reivindicaciones 8 a 10, tal que el medio de almacenamiento (SC) está configurado como tarjeta Pay TV para el uso de televisión de pago o integrado en una tarjeta Pay TV de este tipo.

12. Medio de almacenamiento (SC) portátil, según una cualquiera de las reivindicaciones 8 a 11, tal que el medio de almacenamiento (SC) está configurado como tarjeta inteligente con un módulo de seguridad para el uso de un dispositivo terminal (EG) en una red de telefonía móvil o está integrado en una tarjeta inteligente de este tipo.

13. Medio de almacenamiento (SC) portátil, según una cualquiera de las reivindicaciones 8 a 12, tal que el medio de almacenamiento (SC) está configurado como tarjeta Secure Flash (SFC) o está integrado en una tarjeta Secure Flash (SFC) de este tipo.

14. Sistema con un medio de almacenamiento (SC) portátil y un dispositivo terminal (EG) para operar el medio de almacenamiento (SC),
configurado para realizar un procedimiento según una cualquiera de las reivindicaciones 1 a 7, que presenta:

- en el medio de almacenamiento (SC) portátil, una memoria de aplicaciones (AS) configurada para almacenar aplicaciones (AP; A-AP),
- en el medio de almacenamiento (SC) portátil, un módulo de recuperación (BM) que está configurado como memoria no volátil y es independiente de las aplicaciones (AP; A-AP) almacenadas en la memoria de aplicaciones (AS).

15. Sistema, según la reivindicación 14, en el que el medio de almacenamiento (SC) portátil está configurado según una cualquiera de las reivindicaciones 8 a 13.

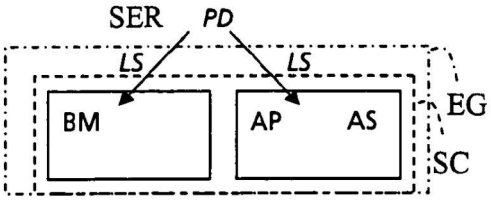

Fig. 1

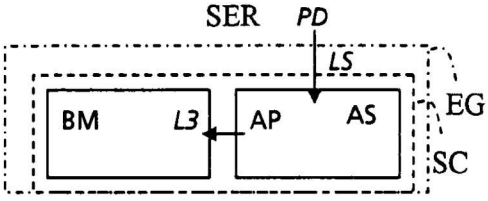

Fig. 2

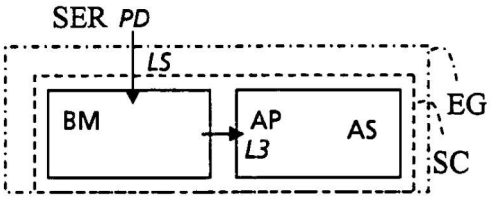

Fig. 3

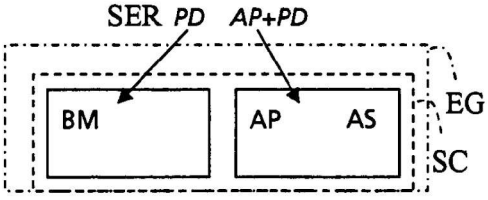

Fig. 4

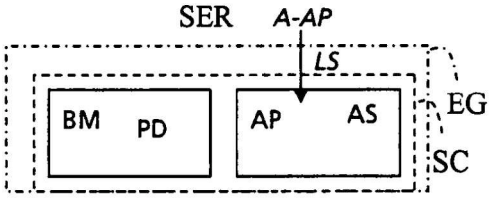

Fig. 5

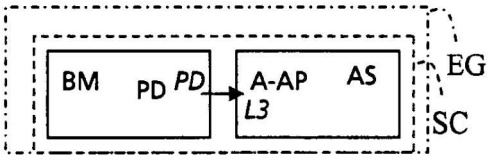

Fig. 6

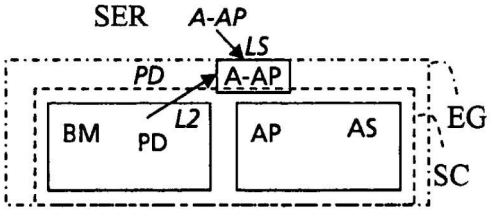

Fig. 7

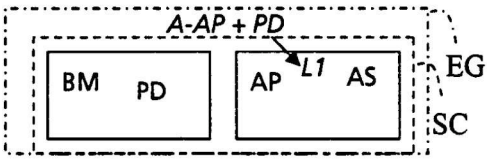

Fig. 8

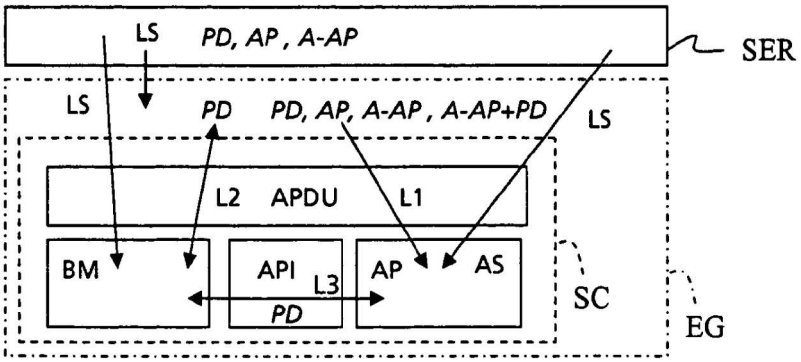

Fig. 9

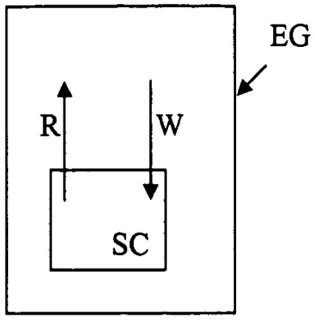

Fig. 10

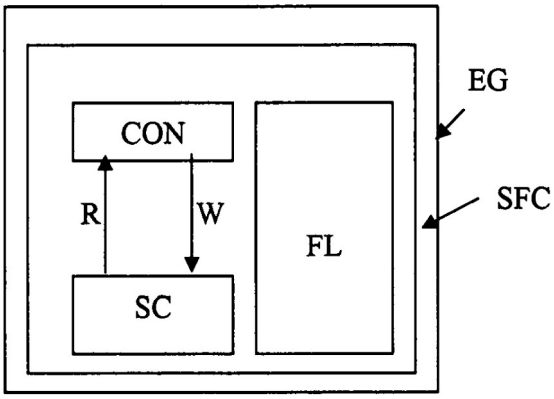

Fig. 11

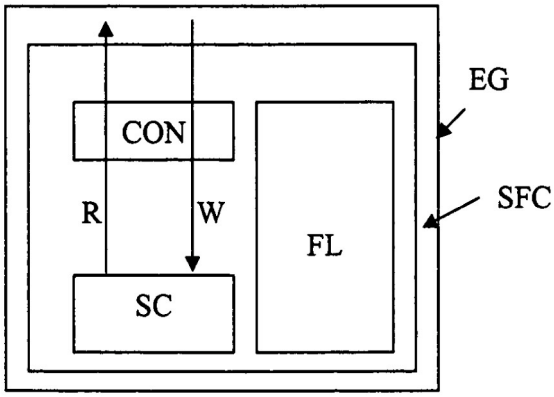

Fig. 12