(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 651 684**

(51) Int. CI.:

G06Q 20/32 (2012.01)
G06Q 20/34 (2012.01)
H04W 4/00 (2009.01)
H04W 12/04 (2009.01)
H04W 12/08 (2009.01)
H04L 9/12 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **17.04.2013 PCT/AU2013/000400**

(87) Fecha y número de publicación internacional: **24.10.2013 WO13155563**

(96) Fecha de presentación y número de la solicitud europea: **17.04.2013 E 13778203 (3)**

(97) Fecha y número de publicación de la concesión europea: **11.10.2017 EP 2839602**

(54) Título: **Arquitectura de partición de elemento seguro mutiemisor para dispositivos habilitados para NFC**

(30) Prioridad:

17.04.2012 AU 2012901495
22.03.2013 WO PCT/AU2013/000299

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.01.2018

(73) Titular/es:

SECURE NFC PTY. LTD. (100.0%)
450 St Kilda Road
Melbourne Victoria 3004, AU

(72) Inventor/es:

NICOLAU, CONSTANTIN M.

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Arquitectura de partición de elemento seguro mutiemisor para dispositivos habilitados para NFC

Aplicación relacionada

Esta solicitud se basa y reivindica el beneficio de las fechas de presentación y prioridad de la solicitud AU no. 2012901495 presentada el 17 de abril de 2012.

Campo de la invención

La invención se refiere al campo de la seguridad de las tecnologías de la información (ITS), y en particular, pero no exclusivamente, a una arquitectura de multiemisor para habilitar la coexistencia de las particiones de elemento seguro asignadas a cada emisor de tarjetas dentro de los dispositivos habilitados para NFC tales como los teléfonos inteligentes móviles.

Antecedentes de la invención

La norma comunicaciones de campo cercano (NFC) (18000-3) define el protocolo de comunicación entre dispositivos activos de NFC punto a punto y también entre los dispositivos activos de NFC y las “etiquetas” de NFC pasivas en términos de control de flujo, formatos de mensaje, velocidad (106 Kbs/Miller que codifica el 100 % de modulación a 424 Kbs/Manchester que codifica el 1 % de modulación) y frecuencia (13,56 MHz), pero no una metodología para gestionar múltiples particiones de elemento seguro (SE).

Un SE es un módulo tarjeta/micro-SD (digital seguro) chip/SIM tarjeta de circuito integrado (ICC) (PCI/PED-similar) a prueba de manipulación capaz de incrustar las características de seguridad de aplicaciones de tarjetas de grado inteligente (por ejemplo, pago, emisión de billetes, control de acceso, etc.). El SE está conectado a un chip de NFC, que actúa como una interfaz de radiofrecuencia (RFID) de sistema frontal sin contacto y contiene entre otras cosas, los datos de control de acceso de dominio de seguridad de la tarjeta de emisor (usados para gestionar múltiples dominios de seguridad de aplicaciones que a su vez contienen los datos de control de acceso de dominio de seguridad del desarrollador de aplicaciones).

La tecnología de NFC ofrece alta velocidad de transmisión de datos, sencillez de protocolo de comunicaciones y bajo coste, pero la tecnología de NFC ha introducido vulnerabilidades de seguridad que permiten, por ejemplo: i) escuchas por terceras partes no autorizadas (‘fisgón’), modificación de datos o inserción, ii) manipulación de datos, corrupción e inserción por imitadores (‘suplantador’), y iii) denegación de servicio (‘interferencia’) y ataques de virus por parte de terceros supuestamente de confianza.

Para proteger el intercambio de datos de NFC, el procesamiento y la privacidad e integridad de almacenamiento, los principales emisores de tarjetas han formado alianzas con, o los desarrolladores de sistemas operativos móviles o los fabricantes de dispositivos de NFC, y han implementado protocolos a prueba de punto final propietarios usando firmas de clave pública y cifrado y autenticación de mensajes.

Sin embargo, un dispositivo habilitado para NFC (tal como un teléfono inteligente) en general es propiedad de, o al menos para uso exclusivo de, un consumidor individual. Un consumidor de este tipo puede tener múltiples tarjetas de crédito, billeteras electrónicas o similares proporcionadas por una pluralidad de instituciones financieras u otras instituciones, pero las soluciones de seguridad dedicadas actuales y las metodologías de gestión de SE no permiten la existencia de múltiples SE en el mismo dispositivo habilitado para NFC. Los siguientes documentos estándar son una técnica anterior pertinente a la invención:

“Secure Element Access Control, Version 0.10.0 Public Review” por Globalplatform Inc. que desvela en particular la arquitectura de control de acceso en el caso de un único emisor (sección 2.2).

“Card Specification Version 2.2” por GlobalPlatform Inc. que desvela en particular la infraestructura de los dominios de seguridad (Capítulo 7).

El manual “Near Field Communication From THeory To Practice” por Vedat Coskun (Wiley & Sons) desvela un colector de opciones de diseño del sistema de NFC.

Sumario de la invención

La invención se define por las características de las reivindicaciones 1-12 en la presente memoria descriptiva.

Breve descripción de los dibujos

Con el fin de que la invención pueda determinarse más claramente, se describirán a continuación las realizaciones, por medio de un ejemplo, haciendo referencia a los dibujos adjuntos, en los que:

La figura 1 es un diagrama de bloques esquemático de un teléfono inteligente habilitado para NFC de acuerdo con una realización de la presente invención;
La figura 2 es un diagrama de bloques esquemático de algunos de los componentes operacionales del sistema operativo y la micro-SD del teléfono inteligente de la figura 1;
La figura 3 es un diagrama de bloques esquemático del sistema operativo y la micro-SD del teléfono inteligente de la figura 1 y su relación con los sistemas de varias partes externas;
La figura 4 es un diagrama de bloques esquemático de la arquitectura del teléfono inteligente de la figura 1; y
La figura 5A es un diagrama de flujo de la instalación de los módulos de programa que incorporan la presente invención en el teléfono inteligente de la figura 1;
La figura 5B es un diagrama de flujo del uso de los módulos de programa que incorporan la presente invención en el teléfono inteligente de la figura 1; y
La figura 6 es un diagrama de bloques esquemático de la arquitectura del gestor de particiones de SE de multiemisor del sistema operativo del teléfono inteligente de la figura 1.

Descripciones detalladas de las figuras

La figura 1 es un diagrama de bloques esquemático de un dispositivo habilitado para NFC, en este ejemplo un teléfono inteligente 10, de acuerdo con una realización de la presente invención. Para mayor claridad, solo las características que son específicamente relevantes para comprender la presente invención se ilustran en la figura y se describen a continuación.

El teléfono inteligente 10 incluye un procesador 12, un sistema operativo 14 (por ejemplo Android (marca comercial), iOS (marca comercial), Symbian (marca comercial), BlackBerry OS (marca comercial) o Windows 8 (marca comercial)), y dos formas de memoria: la memoria de dispositivo 16 y una tarjeta de memoria micro-SD (digital segura) extraíble 18 (en lo sucesivo en el presente documento, “micro-SD 18”). Además, el teléfono inteligente 10 incluye una tarjeta SIM 20, que tiene memoria incorporada, y una interfaz de usuario mostrada esquemáticamente en 22, pero que incluye una pantalla táctil 24, un micrófono 26 y un altavoz 28. El teléfono inteligente 10 también incluye un chip de NFC 30.

La figura 2 es un diagrama de bloques esquemático de algunos de los componentes operacionales del sistema operativo 14 y una micro-SD 18 de acuerdo con la presente realización. El sistema operativo 14 incluye un kernel 30 de sistema operativo (SO), que incluye una o más aplicaciones de dispositivo 32 (de las que solo se muestra una primera aplicación de dispositivo a modo de ejemplo por claridad), un gestor de aplicaciones 34, un módulo de servicios de utilidad 36, un módulo de servicios de comunicaciones 38 y una API de acceso de elemento seguro (SE) 40. Cada aplicación de dispositivo 32 incluye una firma digital 42 y un certificado digital 44, y está en comunicación de datos con el gestor de aplicaciones 34, el módulo de servicios de utilidad 36 y el módulo de servicios de comunicaciones 38. La API de acceso de SE 40 incluye un ejecutor de control de acceso 46 (una API definida por GlobalPlatform (marca comercial)) y unos módulos de programa que implementan varias funciones de la presente realización, incluyendo un gestor de particiones de SE 48, cuya función principal es identificar y seleccionar la partición de SE asignada en una tarjeta específica para un emisor de tarjetas específico, un cargador de particiones de SE 50, cuya función principal es actualizar (o reemplazar) o cargar códigos ejecutables y datos (reglas, SCST, etc.) en la partición de SE seleccionada, y un módulo criptográfico de partición de SE 52, cuya función principal es garantizar únicamente el acceso autorizado a las reglas de acceso de dominio de seguridad (SD) y las SCST cargadas en el ARA-M del emisor de tarjetas seleccionado de la partición de SE específica.

La micro-SD 18 incluye uno o más elementos seguros (SE) de multipartición 60 (de los que solo un primer SE de multipartición a modo de ejemplo se muestra para mayor claridad). Cada SE de multipartición 60 se particiona en una pluralidad de particiones de elemento seguro (SE) 62 (1), 62 (2),..., 62 (n); cada partición de SE 62 (1), 62 (2),... 62 (n) está asignada a un emisor de tarjetas respectivo 1, 2,..., n. En esta realización, cada SE 60 tiene, en esta realización, 8, 16 o 32 particiones de SE 62 (1), 62 (2),..., 62 (n).

Cada partición de SE 62 (1), 62 (2),..., 62 (n) tiene un maestro de aplicación de reglas de acceso (ARA-M) 64 que incluye, en el ejemplo de la partición de SE 62 (1), un primer registro 66 que almacena reglas de acceso y datos de control del emisor de tarjetas respectivo y un segundo registro 68 que almacena una tabla de seguridad de tarjeta inteligente única (SCST) de claves aleatorias generadas por el emisor de tarjetas respectivo para proteger las tarjetas de NFC del emisor de tarjetas. Cada partición de SE 62 (1), 62 (2),..., 62 (n) también tiene un registro de número de versión de SCST (indicado en 69 para la partición de SE 62 (1)) con el número de versión de SCST usado por el emisor de tarjetas correspondiente. Cada tarjeta de NFC emitida por un emisor de tarjetas se inicializa con la única SCST en el segundo registro de ese emisor de tarjetas, de tal manera que cada dispositivo de NFC se carga con las SCST respectivas y los números de versión de SCST asociados a las tarjetas de NFC que se esperan usar con el dispositivo (en este ejemplo, el teléfono inteligente 10).

Cada emisor de tarjetas por lo tanto puede estipular, con sus respectivas reglas de acceso y datos de control, su propio conjunto de reglas de acceso para la gestión y el control de los datos en su partición de SE dedicada dentro del SE de multipartición 60. El ejecutor de control de acceso (ACE) 46 del sistema operativo 14 controla el acceso al ARA-M 64.

La SCST en cada partición de SE 62 (1), 62 (2),..., 62 (n) mantiene diferentes conjuntos de claves de seguridad para garantizar los datos en cada partición de SE respectiva 62 (1), 62 (2),..., 62 (n). Puede emplearse cualquier técnica adecuada para generar claves de seguridad, pero en esta realización cada SCST se genera, por el emisor de tarjetas respectivo, y se emplea usando un módulo de gestión de claves implícitas (IKM) 70, de acuerdo con el método de IKM desvelado en la solicitud de patente australiana n.º 2012901149 presentada el 22 de marzo de 2012 y la solicitud de patente internacional n.º PCT/AU2013/000299 presentada el 22 de marzo de 2013. Por lo tanto, la SCST en la partición de SE 62 (1) contiene 256 claves de byte aleatorias de 8 bits cada una, empleadas para encriptar/desencriptar los datos almacenados en la partición de SE respectiva como se describe en esas solicitudes de patente de acuerdo con el módulo de IKM 70 para proporcionar integridad de datos, privacidad y no repudio de los mensajes intercambiados con otros dispositivos activos (teléfonos inteligentes pares, EFTPOS y otros dispositivos) o pasivos (tales como las tarjetas inteligentes de contacto y sin contacto y las TAG). Las otras particiones de SE contienen unas SCST comparables, con diferentes conjuntos de claves.

Además, cada partición de SE 62 (1), 62 (2),..., 62 (n) puede usar uno o más dominios de seguridad de aplicaciones (SD). Cada SD de aplicación en una partición de SE específica 62 (1), 62 (2),..., 62 (n) puede contener una aplicación autorizada por el emisor de tarjetas a la que se asigna la partición de SE correspondiente; cada aplicación se proporciona por un proveedor de aplicaciones respectivo.

La figura 2 representa unos ejemplos de SD de aplicación 72 (1), 72 (2),..., 72 (i) asociados con la partición de SE 62 (1) del emisor de tarjetas 1, pero se entenderá que cada una de las particiones de SE 62 (1), 62 (2),..., 62 (n) pueden tener ninguna, uno o más SD de aplicación. En esta realización, cada partición de SE 62 (1), 62 (2),..., 62 (n) contiene 2, 4 u 8 SD de aplicación 72 (1), 72 (2),..., 72 (i) y, por tanto, en general 2, 4 u 8 aplicaciones (aunque en otras realizaciones puede haber más SD de aplicación por partición de SE y, por lo tanto, correspondientemente más aplicaciones). Al igual que con el número de particiones de SE de emisor de tarjetas por SE, el número de SD de aplicación por partición de SE de emisor de tarjetas está limitado por el tamaño de memoria del medio usado para almacenar los SE, en este ejemplo una micro-SD 18, y está previsto que un mayor número de particiones de SE de emisor de tarjetas por SE y de SD de aplicación por partición de SE de emisor de tarjetas será posible a medida que aumente el tamaño de la memoria de los medios disponibles.

El SD de aplicación 72 (1) de partición de SE 62 (1) se describe a continuación como un ejemplo, pero los otros SD de aplicación de la partición de SE 62 (1) tienen características comparables (aunque diferentes aplicaciones respectivas). En este ejemplo, la aplicación almacenada en el SD de aplicación 72 (1) es la Cyber Security Shield (CSS) 74, una aplicación para proteger los contenidos de NFC y otras tarjetas inteligentes, así como las comunicaciones entre tales tarjetas inteligentes y los dispositivos habilitados para NFC en términos de integridad de datos, privacidad y no repudio. El SD de aplicación 72 (1) también incluye un cliente de aplicaciones de reglas de acceso (ARA-C) 76 que se gestiona por el ARA-M 64 de la partición de SE de emisor de tarjetas 62 (1) y un registro de aplicaciones 77 que contiene los ID de cualquier otro emisor de tarjetas que comparta la aplicación (CSS 74) con el emisor de tarjetas a quien se asigna la partición de SE 62 (1). El ARA-C 76 incluye un conjunto de reglas de acceso y datos de control 78.

El registro de aplicaciones 77 de aplicaciones compartidas (y los registros de aplicación correspondientes en los otros SD de aplicación) se mantienen por gestor de particiones de SE 48. Como se ha mencionado anteriormente, estos registros de aplicación incluyen datos indicativos de los otros emisores de tarjetas autorizados, de tal manera que el ejecutor de control de acceso 46, que, como se ha descrito anteriormente, controla el acceso al ARA-M 64 de la partición de SE 62 (1) y a los ARA-M de las otras particiones de SE de emisor de tarjetas, puede garantizar que solo los emisores de tarjetas autorizados (otros) puedan usar tales aplicaciones.

En este ejemplo, el SD de aplicación 72 (2) de la partición de SE 62 (1) contiene una EMV (que significa ‘Europay, MasterCard, Visa’), una aplicación que proporciona seguridad mejorada para tarjetas inteligentes de pago a crédito y/o débito. El SD de aplicación 72 (2) incluye su propio cliente de aplicaciones de reglas de acceso (consulte ARA-C 76 del SD de aplicación 72 (1)) que incluye un conjunto de reglas de acceso y datos de control y que también se gestiona por el ARA-M 64 de la partición de SE de emisor tarjetas 62 (1) y un registro de aplicación (consulte el registro de aplicación del SD de aplicación 72 (1)) que contiene los ID de los emisores de tarjetas que comparten esta aplicación con el emisor de tarjetas a quien se asigna la partición de SE 62 (1).

Uno o más SD de aplicación adicionales pueden crearse para aplicaciones adicionales como se desee.

En esta realización, los SE 60 están contenidos en una micro-SD 18, pero pueden, en otras realizaciones localizarse en la tarjeta SIM 20, en una caché de dispositivo (tal como en la memoria de dispositivo 16) o en algún otro módulo de seguridad PCI PED.

La figura 3 es un diagrama de bloques esquemático de sistema operativo 14 y una micro-SD 18 y su relación con los sistemas de varias partes, tales como los emisores de tarjetas, y los módulos de programa (indicado por 'APL.' en la figura) de acuerdo con la presente realización, que incluye el gestor de particiones de SE 48, el cargador de particiones de SE 50 y el módulo criptográfico de partición de SE 52. Haciendo referencia a la figura 3, se observará que una autoridad de control (CA) 80 emite certificados para el proveedor de aplicaciones de NFC 82 que proporciona los módulos de programa (y quién los recibe desde un desarrollador o propietario de la aplicación de NFC 84). El proveedor de aplicaciones de NFC 82 proporciona los módulos de programa, los certificados y las claves criptográficas (para la SCST en el segundo registro 68) a los dispositivos habilitados para NFC a través de un adquirente de transacción de dispositivo (que realiza la gestión de SSD) o habilitador de tarjetas 86, bajo el control de un emisor de tarjetas de NFC 88 (que también otorga autoridad al desarrollador de aplicaciones de NFC o al propietario 84 de los módulos de programa).

La figura 4 es un diagrama de bloques esquemático 90 de la arquitectura de software del teléfono inteligente 10, y la integración de un SE 60 generada por un emisor de tarjetas con el sistema operativo 14. La ejecución de varias funciones de seguridad de NFC es transparente para el teléfono inteligente 10 y los usuarios de tarjetas. La API de seguridad de NFC propietaria permite que las aplicaciones tales como la aplicación comercial 92 residente en el teléfono inteligente 10 realicen las funciones criptográficas necesarias para proporcionar integridad de datos, privacidad y no repudio.

Las figuras 5A y 5B son diagramas de flujo 100, 102 de la instalación y el uso, respectivamente, de los módulos de programa que constituyen la realización de las figuras 1 a 3, haciendo referencia al teléfono inteligente 10; los diagramas de flujo 100, 102 describen cómo se asignan nuevas particiones de SE dentro del SE 60 a nuevos emisores de tarjetas o se reemplazan para emisores de tarjetas existentes, y cómo se usan las particiones de SE específicas (datos, programas, etc.) para proteger los mensajes intercambiados con los dispositivos activos o pasivos de terceros.

El diagrama de flujo 100 de la figura 5A muestra cómo los dispositivos de NFC, tal como un teléfono inteligente 10, se cargan con una SCST única para cada emisor de tarjetas y con los módulos de programa que implementan la realización de las figuras 1 a 3, que constituyen un producto de software de seguridad de NFC para proteger el teléfono inteligente 10 contra ataques de seguridad, y cómo cada una de las particiones de SE 62 (1), 62 (2),..., 62 (n) asignadas a los emisores de tarjetas se usan para procesar los mensajes entrantes y salientes entre el teléfono inteligente 10 y o una tarjeta de NFC u otro dispositivo habilitado para NFC. El diagrama de flujo 102 de la figura 5B ilustra el uso de una partición de SE del emisor de tarjetas (es decir, la partición de SE 62 (1), 62 (2),... o 62 (n)).

Haciendo referencia al diagrama de flujo 100 de la figura 5A, la SCST y los módulos de programa mencionados anteriormente se descargan, o en local por el fabricante del equipo (del teléfono inteligente 10, de la micro-SD 18 o si el SE 60 se instala en la tarjeta SIM en lugar de en la tarjeta SIM micro-SD 20), supervisados por el emisor de tarjetas, o de manera remota por unos adquirentes de transacción seleccionados (procesadores). En la etapa 104, por lo tanto, los módulos del programa para crear y administrar una partición de SE de emisor de tarjetas del emisor de tarjetas 'm' (denominado en esta figura colectivamente como 'Apl. de SE' para un emisor de tarjetas nocional 'm') se cargan en la micro-SD 18 y, en la etapa 106, se validan la firma y el certificado de la Apl. de SE del emisor de tarjetas 'm'. Estas dos operaciones pueden realizarse mediante funciones convencionales de cualquier dispositivo habilitado para NFC que esté adaptado para validar la fuente (a prueba del punto final) y los certificados de cualquier aplicación cargada en el dispositivo a través de cualquier tipo de interfaz (por ejemplo, Wi-Fi), NFC, WAN, LAN) o desde cualquier medio (por ejemplo, SIM, SAM, micro-SD, caché de memoria).

En la etapa 108, se instala la Apl. de SE de emisor de tarjetas 'm' con el fin de proporcionar funciones seguras para la partición de SE de emisor de tarjetas del SE 60. En la etapa 110, el cargador de particiones de SE 50 comprueba el ID del emisor de tarjetas para determinar si el emisor de tarjetas es un emisor de tarjetas existente (es decir, una partición de SE ya se ha asignado en el SE 60 al emisor de tarjetas 'm') o un nuevo emisor de tarjetas.

Si el cargador de particiones de SE 50 determina que el ID de emisor de tarjetas es indicativo de un emisor de tarjetas existente, el procesamiento continúa en la etapa 112, donde la Apl. de SE reemplaza los contenidos de SE antiguos (aplicaciones, reglas, SCST, etc.) del emisor de tarjetas 'm' con unos nuevos y, al hacerlo, aplica un control de versión estricto, de tal manera que la nueva versión debe tener un número de versión superior que la versión actual almacenada en el segundo registro 68 de la partición de SE asignada al emisor de tarjetas 'm'. El procesamiento pasa a continuación a la etapa 114, donde se muestra un mensaje de finalización del trabajo mediante un programa de informe de actividad, y a continuación finaliza el procesamiento.

Si el cargador de particiones de SE 50 determina en la etapa 110 que el ID de emisor de tarjetas es indicativo de un nuevo emisor de tarjetas, el procesamiento continúa en la etapa 116, en donde el cargador de particiones de SE 50 determina si el SE 60 tiene suficiente espacio de memoria para asignar una nueva partición de SE al emisor de tarjetas 'm'. De lo contrario, el procesamiento continúa en la etapa 114, donde se muestra un mensaje de finalización del trabajo mediante un programa de informe de actividad (que indica espacio insuficiente), a continuación finaliza el procesamiento. Si en la etapa 116 el cargador de particiones de SE determina que el SE 60 tiene suficiente espacio de memoria, el procesamiento continúa en la etapa 118, donde el cargador de particiones de SE 50 asigna una

nueva partición de SE en el SE 60 al emisor de tarjetas ‘m’. El segundo registro 68 se actualiza con el número de control de versión de la SCST del emisor de tarjetas. Posteriormente, en la etapa 120, una o más aplicaciones autorizadas de emisor de tarjetas nuevas, una vez validadas, pueden cargarse en la partición de SE del SE 60 asignada al emisor de tarjetas ‘m’ si en cada caso hay suficiente espacio de memoria disponible para ese nuevo emisor de tarjetas. El procesamiento pasa a continuación a la etapa 114, donde se muestra un mensaje de finalización del trabajo mediante un programa de informe de actividad, a continuación finaliza el procesamiento.

El diagrama de flujo 102 de la figura 5B ilustra el funcionamiento de una aplicación de lectura/escritura a modo de ejemplo que está configurada para emitir comandos de NFC. En la etapa 130, se leen los datos de la tarjeta de NFC y el gestor de particiones de SE 48 determina el ID de emisor de tarjetas a partir del prefijo de tarjeta del número de cuenta personal (PAN) de la tarjeta de NFC. En la etapa 132, el gestor de particiones de SE 48 inicia la aplicación de lectura/escritura que, en la etapa 134, comprueba si se le ha pasado un comando de lectura o un comando de escritura.

Si se detecta un comando de escritura, el procesamiento continúa en la etapa 136 donde la aplicación de lectura/escritura selecciona la partición de SE correspondiente asignada al emisor de tarjetas identificado. La función de escritura de tarjeta de NFC requiere que los datos a escribir se autentiquen y se encripten antes de su transmisión a la tarjeta de NFC. Usando la SCST del emisor de tarjetas en el segundo registro 68, en la etapa 138 los módulos del programa generan un conjunto de claves implícitas y los vectores asociados. En la etapa 140, el mensaje se cifra con la clave ENCRYPT 1 recientemente generada y en la etapa 142 se autentica por la clave AUTH 2. En la etapa 144, las claves de cifrado y autenticación se destruyen, y en la etapa 146 el mensaje se construye prefijando un mensaje cifrado y autenticado con los vectores asociados con las claves implícitas. En la etapa 148, el mensaje resultante se envía (es decir, se escribe) a la micro-SD 18 (o, en otros ejemplos, se escribe en otra tarjeta de NFC o almacenamiento de memoria, o se envía (se publica) a un dispositivo habilitado para NFC). A continuación, el procesamiento termina.

Si en la etapa 134, la aplicación de lectura/escritura determina que se ha pasado un comando de lectura, el procesamiento continúa en la etapa 150, donde la aplicación de lectura/escritura selecciona el dominio de SE correspondiente asignado al emisor de tarjetas identificado. A continuación, en la etapa 152, la función de lectura de tarjeta de NFC usa los vectores adjuntos al mensaje/registro para regenerar la clave implícita usada para encriptar y autenticar el mensaje. Una vez que se han regenerado las claves DES/3DES (CRYPTO y AUTH), en la etapa 154 el mensaje se descifra usando la clave CRYPTO 1 y en la etapa 156 se verifica la autenticidad del mensaje usando la clave AUTH 2 para su integridad. En la etapa 158, se procesan los contenidos del mensaje (es decir, se leen) y en la etapa 160 las claves y los vectores se destruyen. A continuación, el procesamiento termina.

Por lo tanto, un dispositivo habilitado para NFC puede seleccionar, bajo el control del ACE residente 46, la partición de emisor de tarjetas correcta tras presentarse con un PAN válido o cuando se selecciona una tarjeta virtual a partir de la tarjeta/método del menú de pago por el usuario, de la siguiente manera:

LOOK PAN prefix (Tabla de prefijos de emisor de tarjetas)

COMPARE PAN prefix range

{YES} ACCESS CI-SE domain (es decir, la partición)

{NO} Invalid PAN, EXIT

Los datos y programas firmados y certificados pueden cargarse en las particiones de emisor de tarjetas, y mantenerse, tras la validación de la identidad del remitente y la autenticación de los contenidos de datos recibidos, y procederse de la siguiente manera:

POEP UNSIGN (CI-ID firmado)

COMPARE CI-ID value (Tabla de prefijos de emisor de tarjetas)

{YES} Authenticate Certificate (CA)

{YES} Authenticate Message (MAC),

{YES} Decrypt Message (DATOS, Programas)

Store DATA and/or Programs in CI-SE, EXIT

{NO} Invalid CI-ID, or CA or MAC, EXIT

Los contenidos de la partición del emisor de tarjetas pueden descifrarse antes del uso de la información del emisor de tarjetas específico y los datos pueden encriptarse y escribirse de nuevo en la partición del emisor de tarjetas, de la siguiente manera:

Write Card/Record Process

DECRYPT CI-SE contents using Implicit Key Management

GENERATE random# to create Card Code Factor (CCF)

ENCIPHER data message using CCF key,

WRITE to NFC card, EXIT

Read Card/Record Process

DECRYPT CI-SE contents using Implicit Key Management

GET random# (desafío) to create Card Code Factor (CCF)

DECIPHER data message using CCF key, EXIT

La figura 6 es un diagrama de bloques esquemático 170 de la arquitectura del gestor de particiones de SE de multiemisor 48 del sistema operativo 14, de acuerdo con esta realización. El ejecutor de control de acceso 46 usa los servicios del gestor de particiones de SE 48 para gestionar la carga, el mantenimiento, el acceso y el uso de cada partición de SE del emisor de tarjetas individual en el teléfono inteligente 10.

En esta realización, el tamaño de la SCST en el segundo registro 68 de la partición de SE 62 (1) es de solo 256 bytes y los componentes de software de esta realización que implementan la presente invención son de un tamaño pequeño en una forma ejecutable (del orden de 1 KB) y compartido por todas las particiones de SE. Como se ha tratado anteriormente, el registro de aplicación 77 mantiene simplemente una lista de los ID y los niveles de autoridad de los emisores de tarjetas (ejecución, actualización, eliminación) para el intercambio de aplicaciones específicas en el SD de aplicación 72 (1). En consecuencia, el espacio de memoria necesario por esta realización es muy pequeño en comparación con el espacio de memoria de la micro-SD 10 (es decir, 32 GB) o de la memoria de dispositivo 16 (es decir, 16 GB) del teléfono inteligente 10, o incluso cuando se compara con las tarjetas activas de NFC (que comúnmente tienen al menos 8 KB).

Pueden efectuarse fácilmente modificaciones dentro del alcance de la invención por los expertos en la materia.

Por ejemplo, será evidente para un experto en la materia que las realizaciones de la presente invención tienen aplicaciones en muchos casos donde se requiere un almacenamiento de datos seguro y una seguridad de las comunicaciones entre dos dispositivos de NFC, y que pueden hacerse numerosas alteraciones y modificaciones al método de seguridad y a la arquitectura de las realizaciones descritas anteriormente, sin alejarse de los conceptos básicos de la invención. Debería entenderse, por lo tanto, que esta invención no está limitada a las realizaciones específicas descritas a modo de ejemplo anteriormente en el presente documento.

En las reivindicaciones siguientes y en la descripción anterior de la invención, excepto cuando el contexto requiera lo contrario debido al lenguaje expreso o implicación necesaria, la palabra “comprender” o variaciones tales como “comprende” o “que comprende” se usan en un sentido inclusivo, es decir, para especificar la presencia de las características indicadas pero no excluir la presencia o adición de características adicionales en diversas realizaciones de la invención.

REIVINDICACIONES

1. Un método para proporcionar particiones de elemento seguro para un dispositivo habilitado para NFC (10) para una pluralidad de emisores de tarjetas, comprendiendo el método:

proporcionar un gestor de partición de elemento seguro (48), un cargador de particiones de elemento seguro (50) y un módulo criptográfico de partición de elemento seguro (52) en una interfaz de programación de aplicación de acceso de elemento seguro (40) del dispositivo habilitado para NFC (10), en el que el gestor de particiones de elemento seguro (48) funciona para identificar y seleccionar la partición segura asignada a un emisor de tarjetas específico, el cargador de particiones de elemento seguro (50) funciona para actualizar, reemplazar o cargar un código ejecutable y datos en una partición de elemento seguro seleccionada, y el módulo criptográfico de partición de elemento seguro (52) funciona para garantizar el acceso autorizado a las reglas de acceso y a los datos de control (66) cargados en un maestro de aplicación de reglas de acceso ARA-M (64) de la partición de elemento seguro de un emisor de tarjetas seleccionado;
dividir un elemento seguro (60) de una memoria (18) del dispositivo habilitado para NFC (10) en una pluralidad de particiones de elemento seguro (62);
asignar dichas particiones de elemento seguro (62) del elemento seguro (60) a los emisores de tarjetas respectivos; y
proporcionar en el elemento seguro (60) para una pluralidad de particiones de elemento seguro (62) respectivamente uno o más dominios de seguridad de aplicaciones (72);
en el que las particiones de elemento seguro (62) incluyen respectivamente un maestro de aplicación de reglas de acceso ARA-M (64) que tiene las reglas de acceso y los datos de control (66) del emisor de tarjetas respectivo y una tabla de seguridad de tarjeta inteligente única (68) de claves aleatorias generadas por el emisor de tarjetas respectivo para proteger las tarjetas de NFC del emisor de tarjetas, y
los uno o más dominios de seguridad de aplicaciones correspondientes a una partición de elemento seguro respectivo (62) incluyen, respectivamente, una aplicación (74), un cliente de aplicación de reglas de acceso ARA-C (76) que tiene un conjunto de reglas de acceso y de datos de control (78) y un registrador de aplicaciones (77) que contiene las identidades de los emisores de tarjetas que comparten la aplicación (74) con el emisor de tarjetas a quien se asigna la partición de elemento seguro respectiva (62).

2. Un método de acuerdo con la reivindicación 1, que incluye crear o localizar el elemento seguro (60) en la memoria (18) del dispositivo habilitado para NFC (10).

3. Un método de acuerdo con la reivindicación 1 o 2, que incluye uno o más de los emisores de tarjetas que cargan datos y programas de elemento seguro en las particiones de elemento seguro respectivas (62) asignadas a los emisores de tarjetas respectivos.

4. Un método de acuerdo con una cualquiera de las reivindicaciones 1 a 3, que incluye crear 8, 16 o 32 de las particiones de elemento seguro (62) en al menos uno de los elementos seguros (60).

5. Un método de acuerdo con una cualquiera de las reivindicaciones 1 a 4, que incluye asignar las particiones de elemento seguro (62) a las tarjetas respectivas de los emisores de tarjetas respectivos.

6. Un método de acuerdo con la reivindicación 1, que incluye proporcionar uno primero de dicha pluralidad de dominios de seguridad de aplicaciones (72) con una aplicación de seguridad y unos datos de seguridad.

7. Un método de acuerdo con una cualquiera de las reivindicaciones 1 a 6, en el que la memoria está en una tarjeta SIM del dispositivo, una micro-SD (18) del dispositivo (10) o una caché del dispositivo (10).

8. Un método de acuerdo con la reivindicación 1, que incluye:

cargar una aplicación de elemento seguro y una tabla de seguridad de tarjeta inteligente para crear y gestionar una partición de elemento seguro (62) de un emisor de tarjetas respectivo (m) en una tarjeta micro-SD o SIM;
validar una firma y un certificado de la aplicación de elemento seguro;
instalar la aplicación de elemento seguro del emisor de tarjetas (m) con el fin de proporcionar unas funciones seguras para la partición de elementos seguros (62) del elemento seguro (60);
comprobar con el cargador de particiones de elemento seguro (50) una identidad del emisor de tarjetas (m) para determinar si el emisor de tarjetas (m) es un emisor de tarjetas existente o un emisor de tarjetas nuevo;
en el que, si el cargador de particiones de elemento seguro (50) determina que el emisor de tarjetas (m) es un emisor de tarjetas existente, la aplicación de elemento seguro reemplaza los contenidos de elemento seguro anteriores del emisor de tarjetas (m) con los contenidos de elemento seguro nuevos y aplica un control de versión estricto de tal manera que la nueva versión tenga un número de versión superior que la versión actual almacenada en un registro (68) de la partición de elemento seguro (62) asignada al emisor de tarjetas (m); y
si el cargador de particiones de elemento seguro (50) determina que el emisor de tarjetas (m) es un nuevo emisor de tarjetas, el cargador de particiones de elemento seguro (50) determina si el elemento seguro (60) tiene suficiente espacio de memoria para asignar una nueva partición de elemento seguro (62) al emisor de tarjetas

(m) y, si el cargador de particiones de elemento seguro (50) determina que el elemento seguro (60) tiene suficiente espacio de memoria para asignar una nueva partición de elemento seguro (62) al emisor de tarjetas (m), el cargador de particiones de elemento seguro (50) asigna una nueva partición de elemento seguro (62) en el elemento seguro (60) al emisor de tarjetas (m), el registro (69) se actualiza con un número de control de versión de la tabla de seguridad de tarjeta inteligente.

9. Un método de acuerdo con la reivindicación 1, que incluye:

leer los datos de tarjeta de NFC de la tarjeta de NFC;
determinar con el gestor de partición de elemento seguro (48) la identidad del emisor de tarjetas a partir de un prefijo de tarjeta de un número de cuenta personal (PAN) de la tarjeta de NFC;
iniciar una aplicación de lectura/escritura con el gestor de particiones de elemento seguro (48);
comprobar si se ha pasado a la aplicación de lectura/escritura un mensaje que comprende un comando de lectura o un comando de escritura;
en el que, si se detecta un comando de escritura, la aplicación de lectura/escritura selecciona una partición de elemento seguro correspondiente (62) asignada al emisor de tarjetas identificado, una aplicación de elemento seguro genera un conjunto de claves implícitas y vectores asociados usando una tabla de seguridad de tarjeta inteligente del emisor de tarjetas, el mensaje se cifra usando una clave de cifrado recientemente generada, el mensaje se autentica usando una clave de autenticación, el mensaje se construye prefijando el mensaje con vectores asociados con las claves implícitas, el mensaje resultante se envía a una micro-SD, otra tarjeta de NFC, un almacenamiento de memoria o un dispositivo habilitado para NFC de pares; y
si se detecta un comando de lectura, la aplicación de lectura/escritura selecciona una partición de elemento seguro correspondiente (62) asignada al emisor de tarjetas identificado, la función de lectura de tarjetas de NFC usa los vectores adjuntos al mensaje para regenerar las claves implícitas usadas para cifrar y autenticar el mensaje, el mensaje se descifra y su integridad se verifica con las claves implícitas, se lee el mensaje, y las claves implícitas y los vectores se destruyen.

10. Un elemento seguro (60) para una memoria (18) de un dispositivo habilitado para NFC, que comprende:

una interfaz de programación de aplicaciones de acceso de elemento seguro (40) que comprende un gestor de particiones de elemento seguro (48), un cargador de particiones de elemento seguro (50), y un módulo criptográfico de particiones de elemento seguro (52), en la que el gestor de particiones de elemento seguro (48) funciona para identificar y seleccionar la partición segura asignada a un emisor de tarjetas específico, el cargador de particiones de elemento seguro (50) funciona para actualizar, reemplazar o cargar el código ejecutable y los datos en una partición de elemento seguro seleccionada, y el módulo criptográfico de partición de elemento seguro (52) funciona para garantizar el acceso autorizado a las reglas de acceso y los datos de control (66) cargados en un maestro de aplicación de reglas de acceso ARA-M (64) de la partición de elemento seguro de un emisor de tarjetas seleccionado;
unas particiones de elemento seguro (62), siendo las particiones de elemento seguro (62) unas particiones del elemento seguro (60) asignadas a los emisores de tarjetas respectivos, y
uno o más dominios de seguridad de aplicaciones (72) para cada una de una pluralidad de las particiones de elemento seguro;
en el que las particiones de elemento seguro (62) incluyen, respectivamente, un maestro de aplicación de reglas de acceso ARA-M (64), teniendo cada uno de los mismos unas reglas de acceso y unos datos de control (66) del emisor de tarjetas respectivo y una única tabla de seguridad de tarjeta inteligente (68) de claves aleatorias generadas por el emisor de tarjetas respectivo para proteger las tarjetas de NFC del emisor de tarjetas, y
los uno o más dominios de seguridad de aplicaciones correspondientes a una partición de elemento seguro respectivo (62) incluyen, respectivamente, una aplicación (74), un cliente de aplicación de reglas de acceso ARA-C (76) que tiene un conjunto de reglas de acceso y de datos de control (78) y un registrador de aplicaciones (77) que contiene las identidades de los emisores de tarjetas que comparten la aplicación (74) con el emisor de tarjetas a quien se asigna la partición de elemento seguro respectiva (62).

11. Un dispositivo habilitado para NFC, que comprende una memoria (18), comprendiendo la memoria (18) un elemento seguro (60) de acuerdo con la reivindicación 10.

12. Un medio de almacenamiento legible por ordenador con un producto de programa informático que, al ejecutarse en un ordenador, realiza el método de cualquiera de las reivindicaciones 1 a 9.

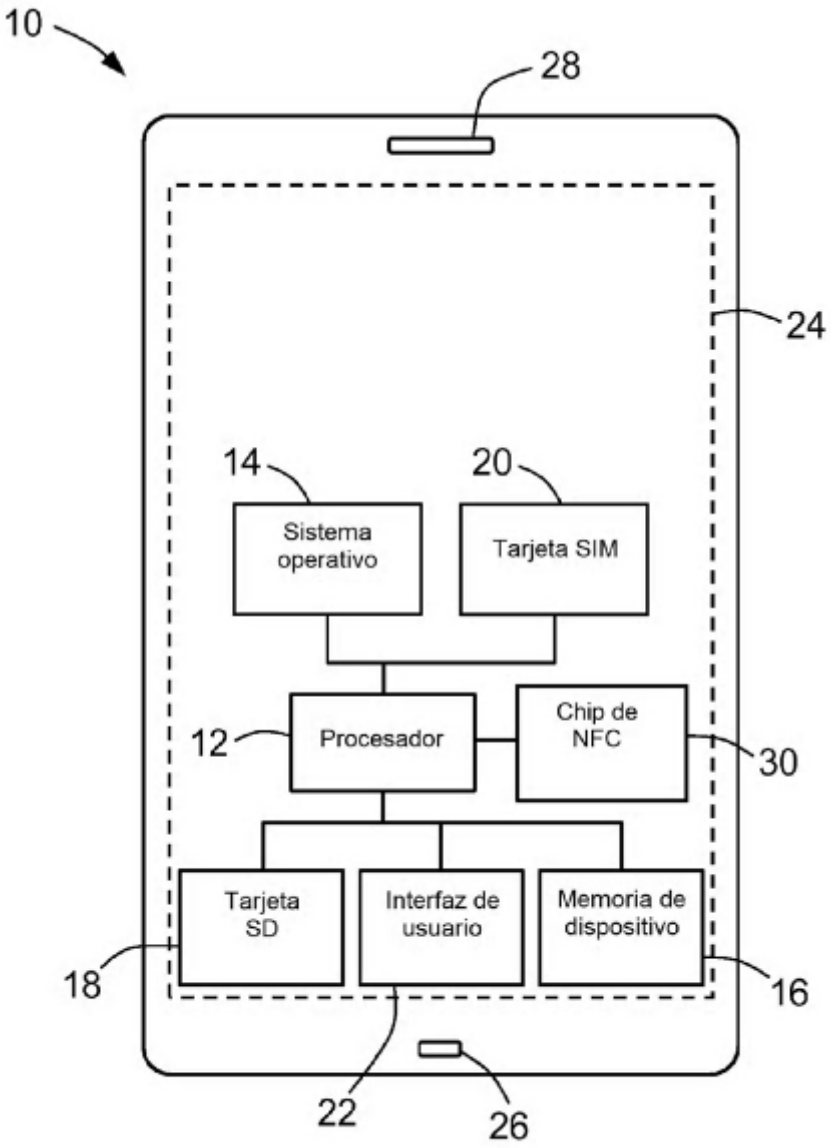
10
28
24
14
Sistema operativo
20
Tarjeta SIM
12
Procesador
Chip de NFC
30
Tarjeta SD
Interfaz de usuario
Memoria de dispositivo
18
16
22
26

Figura 1

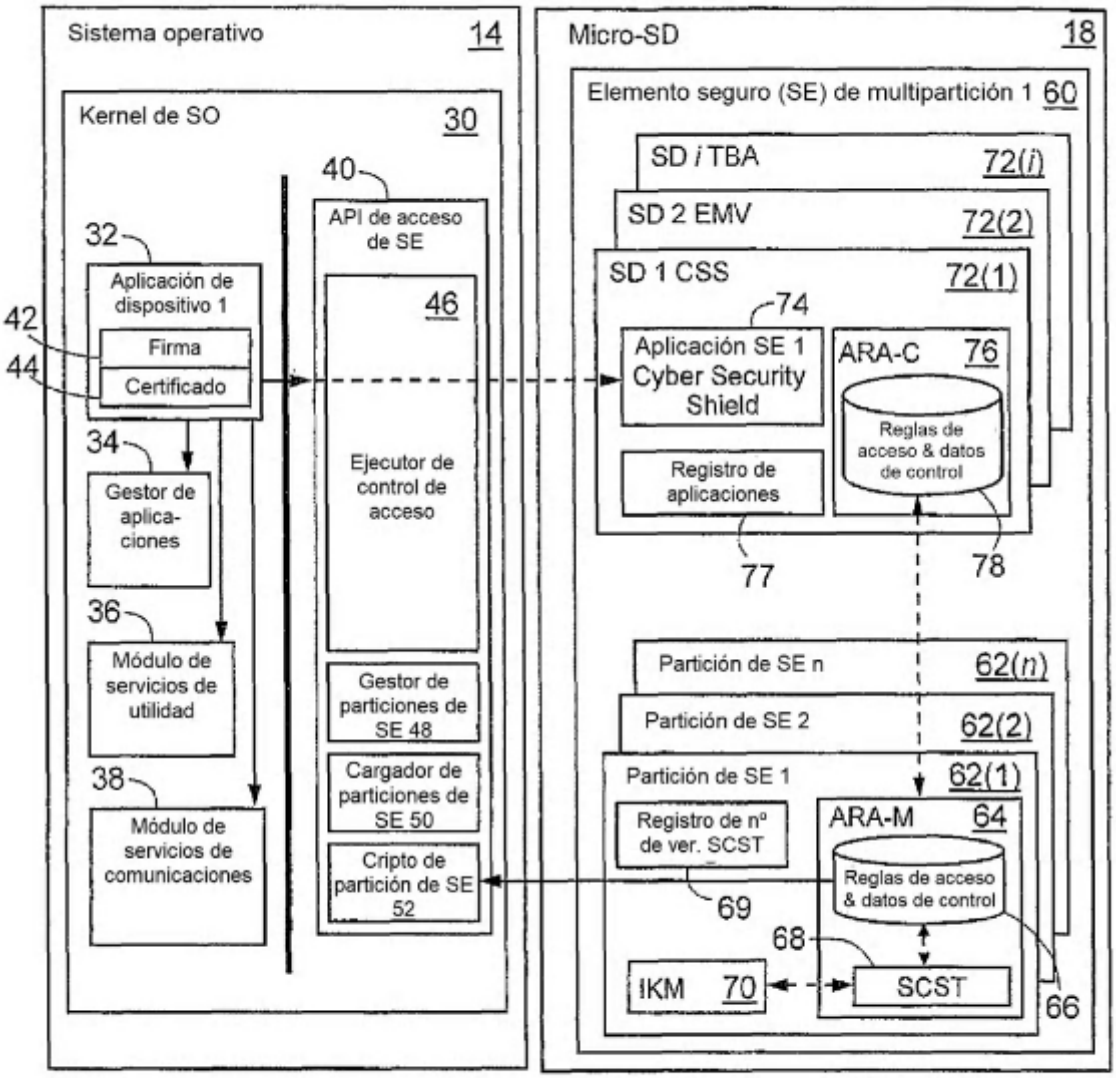
Sistema operativo
14
Kernel de SO
30
40
API de acceso de SE
32
Aplicación de dispositivo 1
42
Firma
44
Certificado
46
Ejecutor de control de acceso
34
Gestor de aplica-ciones
36
Módulo de servicios de utilidad
38
Módulo de servicios de comunicaciones
Gestor de particiones de SE 48
Cargador de particiones de SE 50
Cripto de partición de SE 52
Micro-SD
18
Elemento seguro (SE) de multipartición 1 60
SD i TBA
72(i)
SD 2 EMV
72(2)
SD 1 CSS
72(1)
74
Aplicación SE 1 Cyber Security Shield
ARA-C
76
Reglas de acceso & datos de control
Registro de aplicaciones
77
78
Partición de SE n
62(n)
Partición de SE 2
62(2)
Partición de SE 1
62(1)
Registro de nº de ver. SCST
ARA-M
64
Reglas de acceso & datos de control
69
68
IKM
70
SCST
66

Figura 2

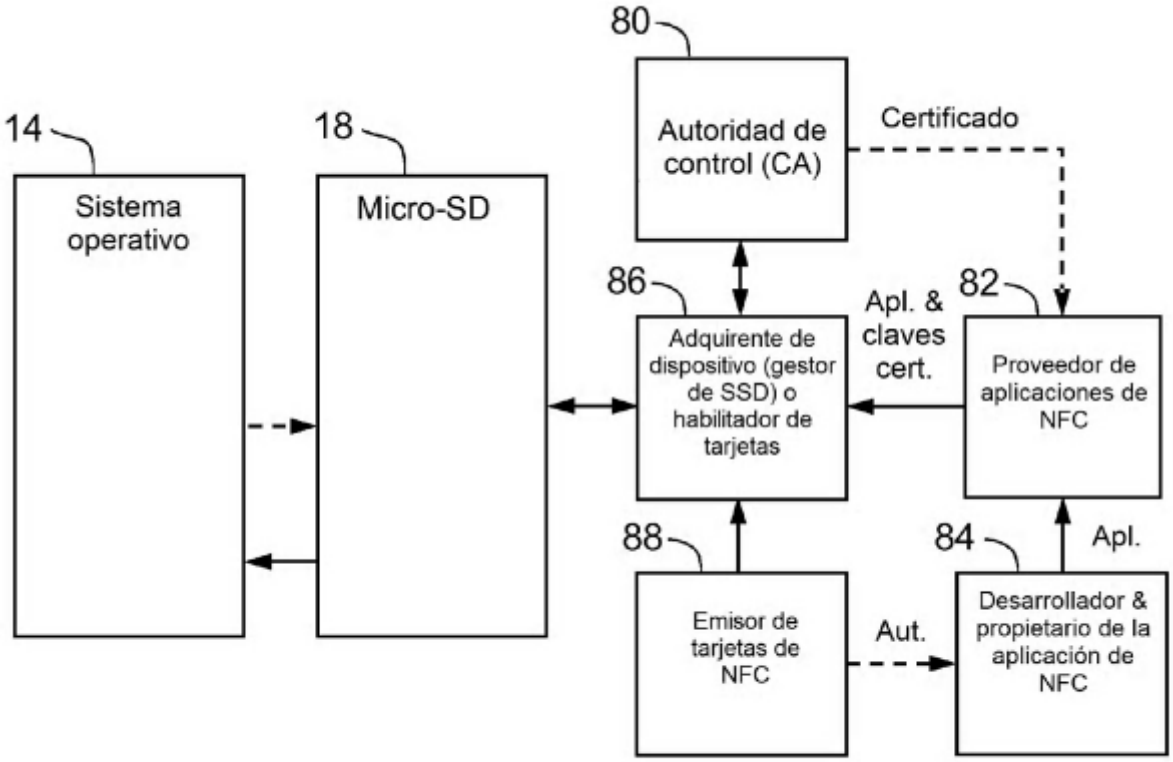
80
Autoridad de control (CA)
Certificado
14
Sistema operativo
18
Micro-SD
86
Adquirente de dispositivo (gestor de SSD) o habilitador de tarjetas
Apl. & claves cert.
82
Proveedor de aplicaciones de NFC
88
Emisor de tarjetas de NFC
Aut.
84
Apl.
Desarrollador & propietario de la aplicación de NFC

Figura 3

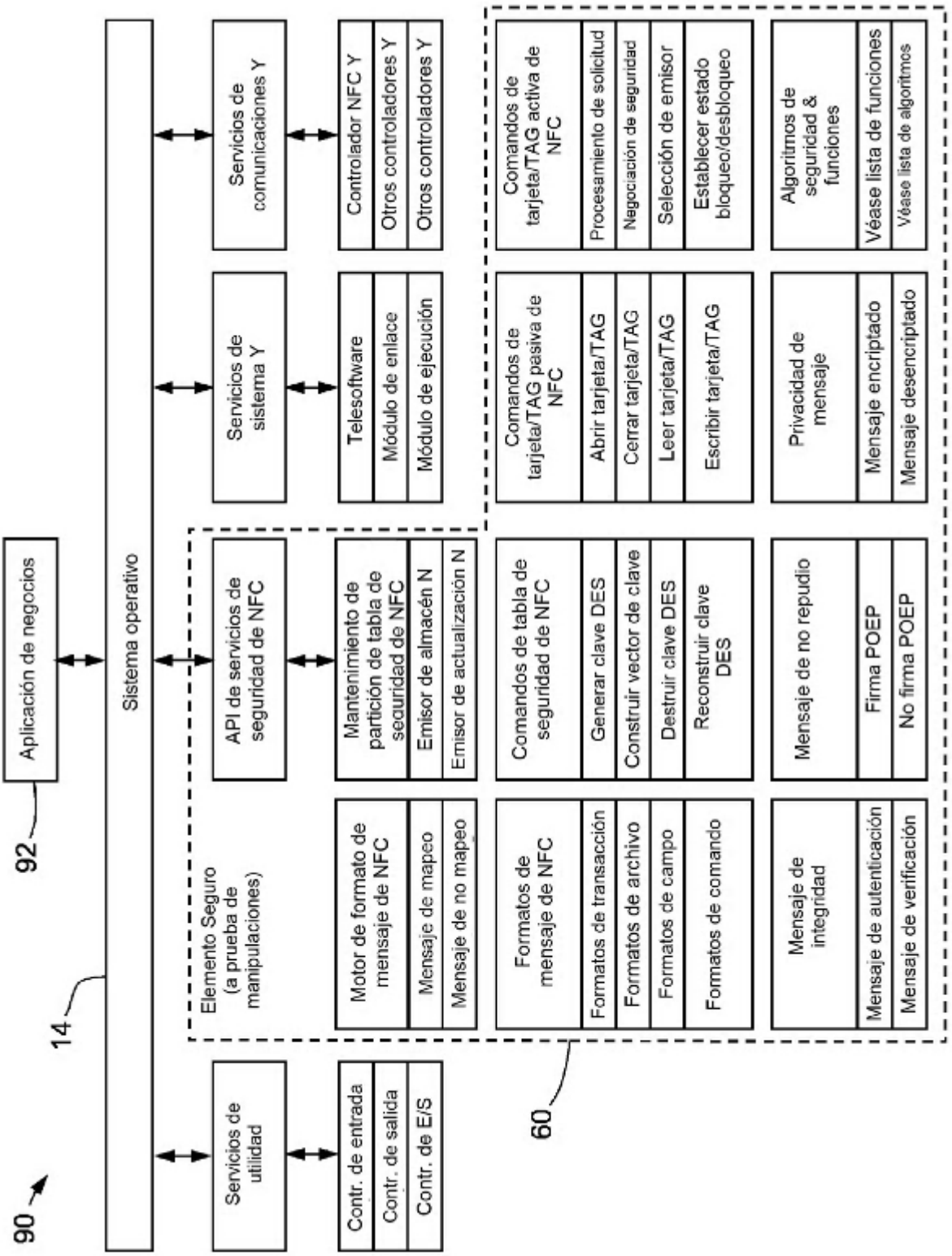
90
92
14
60
Aplicación de negocios
Sistema operativo
Elemento Seguro (a prueba de manipulaciones)
Servicios de utilidad
Contr. de entrada
Contr. de salida
Contr. de E/S
API de servicios de seguridad de NFC
Mantenimiento de partición de tabla de seguridad de NFC
Emisor de almacén N
Emisor de actualización N
Motor de formato de mensaje de NFC
Mensaje de mapeo
Mensaje de no mapeo
Servicios de sistema Y
Telesoftware
Módulo de enlace
Módulo de ejecución
Servicios de comunicaciones Y
Controlador NFC Y
Otros controladores Y
Otros controladores Y
Comandos de tarjeta/TAG pasiva de NFC
Abrir tarjeta/TAG
Cerrar tarjeta/TAG
Leer tarjeta/TAG
Escribir tarjeta/TAG
Comandos de tarjeta/TAG activa de NFC
Procesamiento de solicitud
Negociación de seguridad
Selección de emisor
Establecer estado bloqueo/desbloqueo
Comandos de tabla de seguridad de NFC
Generar clave DES
Construir vector de clave
Destruir clave DES
Reconstruir clave DES
Formatos de mensaje de NFC
Formatos de transacción
Formatos de archivo
Formatos de campo
Formatos de comando
Privacidad de mensaje
Mensaje encriptado
Mensaje desencriptado
Mensaje de no repudio
Firma POEP
No firma POEP
Algoritmos de seguridad & funciones
Véase lista de funciones
Véase lista de algoritmos
Mensaje de integridad
Mensaje de autenticación
Mensaje de verificación

Figura 4

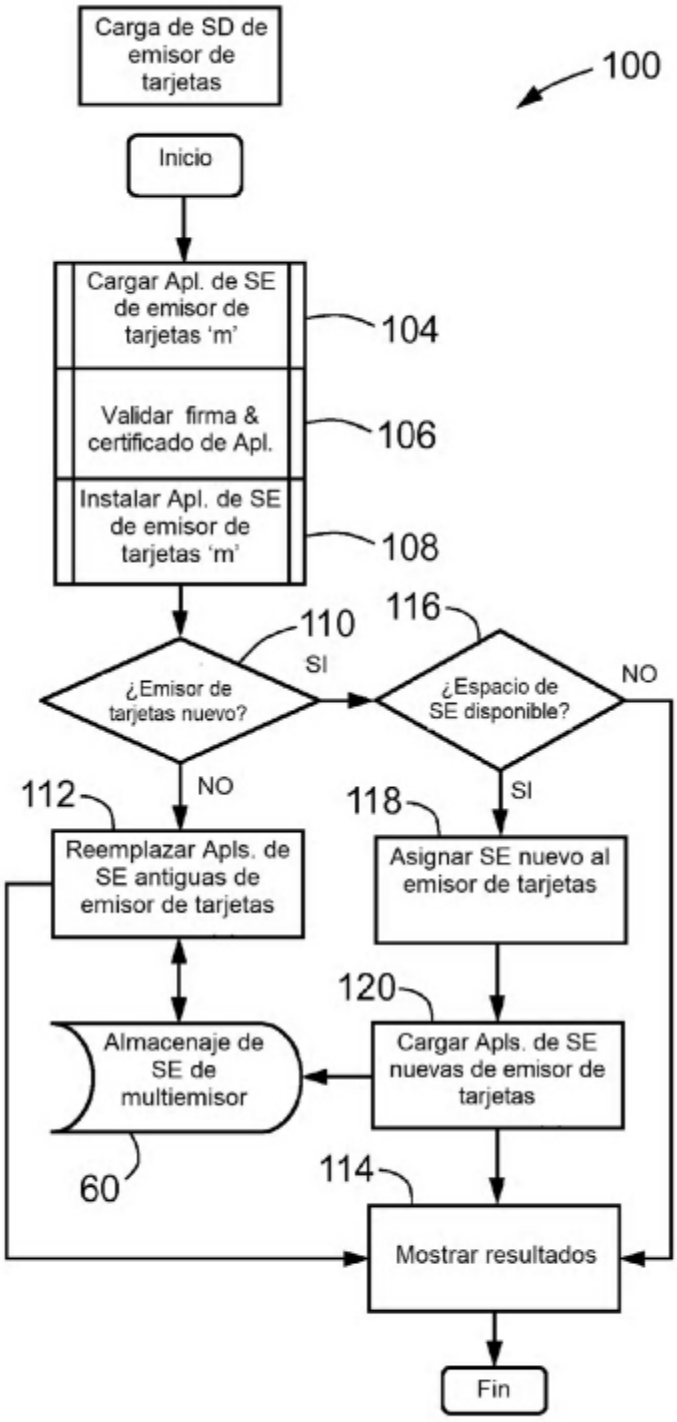
Carga de SD de emisor de tarjetas
100
Inicio
Cargar Apl. de SE de emisor de tarjetas 'm'
104
Validar firma & certificado de Apl.
106
Instalar Apl. de SE de emisor de tarjetas 'm'
108
110
SI
¿Emisor de tarjetas nuevo?
116
¿Espacio de SE disponible?
NO
NO
112
Reemplazar Apls. de SE antiguas de emisor de tarjetas
SI
118
Asignar SE nuevo al emisor de tarjetas
120
Almacenaje de SE de multiemisor
60
Cargar Apls. de SE nuevas de emisor de tarjetas
114
Mostrar resultados
Fin

Figura 5A

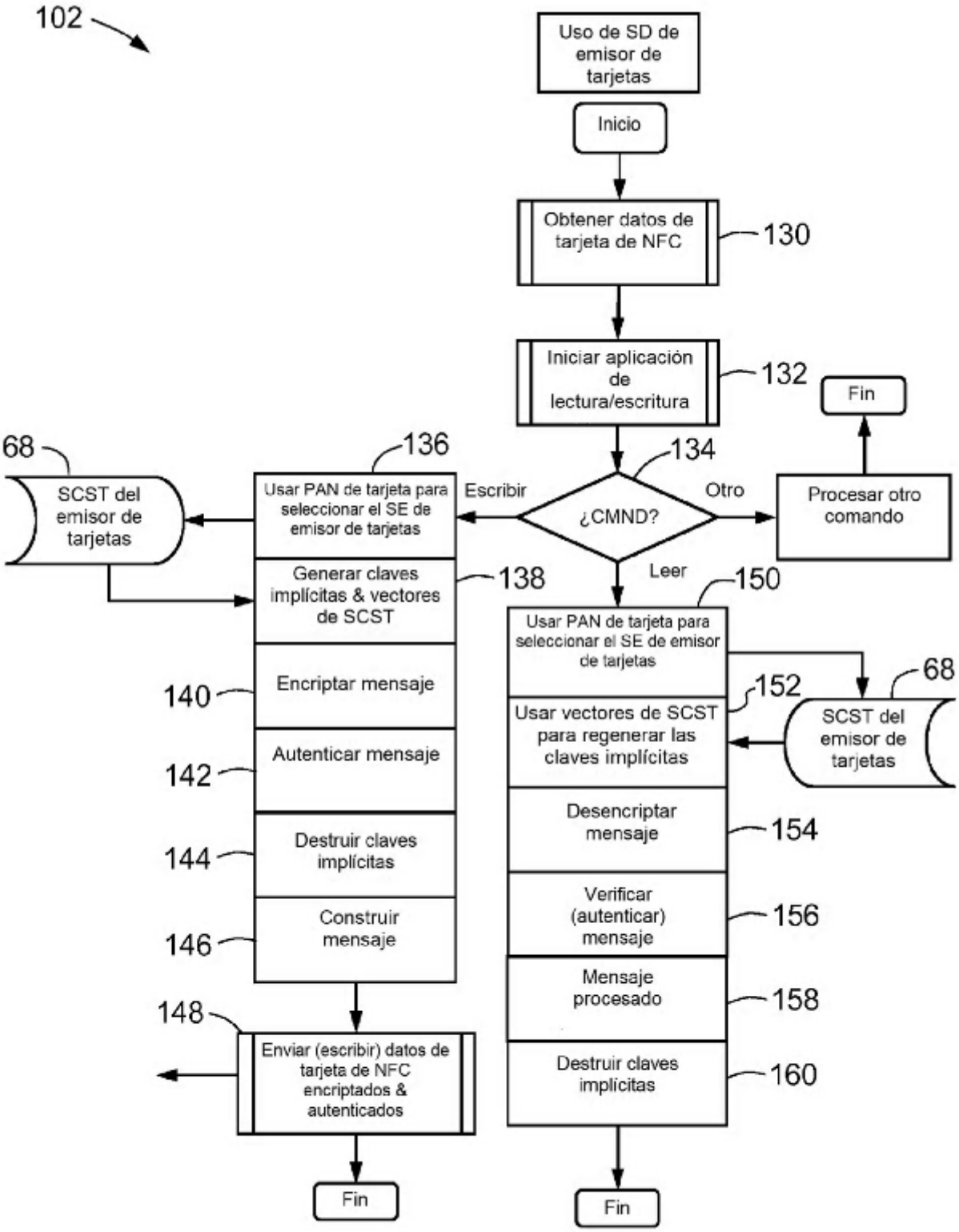
102
Uso de SD de emisor de tarjetas
Inicio
Obtener datos de tarjeta de NFC
130
Iniciar aplicación de lectura/escritura
132
Fin
68
SCST del emisor de tarjetas
136
Usar PAN de tarjeta para seleccionar el SE de emisor de tarjetas
Escribir
134
¿CMND?
Otro
Procesar otro comando
Generar claves implícitas & vectores de SCST
138
Leer
150
Usar PAN de tarjeta para seleccionar el SE de emisor de tarjetas
68
SCST del emisor de tarjetas
152
Usar vectores de SCST para regenerar las claves implícitas
Encriptar mensaje
140
Autenticar mensaje
142
Destruir claves implícitas
144
Construir mensaje
146
Desencriptar mensaje
154
Verificar (autenticar) mensaje
156
Mensaje procesado
158
Destruir claves implícitas
160
148
Enviar (escribir) datos de tarjeta de NFC encriptados & autenticados
Fin
Fin

Figura 5B

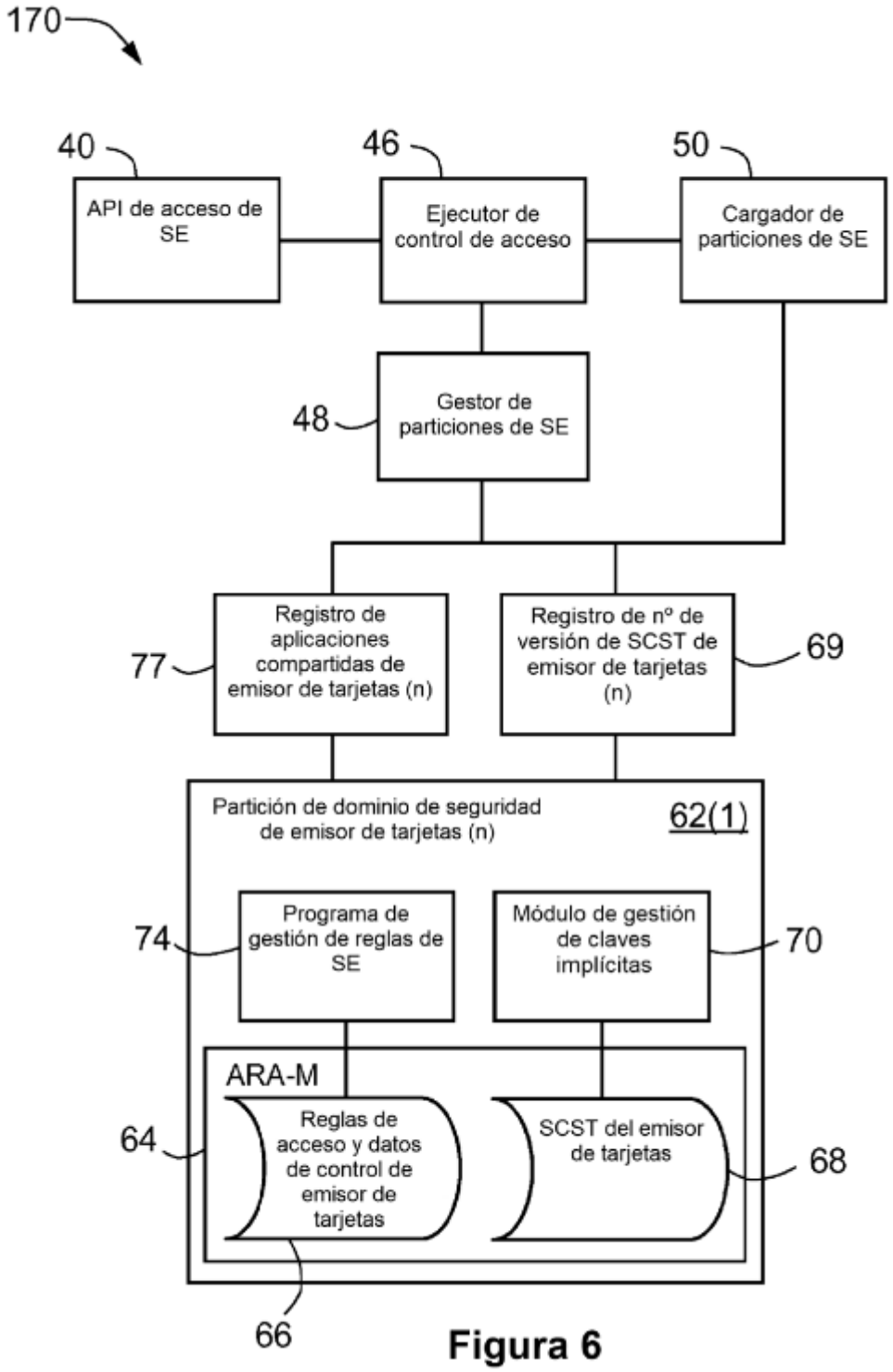
170
40
API de acceso de SE
46
Ejecutor de control de acceso
50
Cargador de particiones de SE
48
Gestor de particiones de SE
77
Registro de aplicaciones compartidas de emisor de tarjetas (n)
Registro de nº de versión de SCST de emisor de tarjetas (n)
69
Partición de dominio de seguridad de emisor de tarjetas (n)
62(1)
74
Programa de gestión de reglas de SE
Módulo de gestión de claves implícitas
70
ARA-M
64
Reglas de acceso y datos de control de emisor de tarjetas
SCST del emisor de tarjetas
68
66

Figura 6