(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 666 839**

(51) Int. CI.:

G06Q 20/32 (2012.01)
G06Q 20/38 (2012.01)
G06K 19/06 (2006.01)
H04W 12/02 (2009.01)
G06F 21/14 (2013.01)
H04L 9/00 (2006.01)
G06F 21/60 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **03.03.2015 PCT/EP2015/054382**

(87) Fecha y número de publicación internacional: **11.09.2015 WO15132244**

(96) Fecha de presentación y número de la solicitud europea: **03.03.2015 E 15713387 (7)**

(97) Fecha y número de publicación de la concesión europea: **24.01.2018 EP 3114599**

(54) Título: **Transacciones seguras de dispositivos móviles**

(30) Prioridad:

03.03.2014 GB 201403728

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.05.2018

(73) Titular/es:

MASTERCARD INTERNATIONAL, INC. (100.0%)
2000 Purchase Street
Purchase, NY 10577, US

(72) Inventor/es:

RADU, CRISTIAN;
COLLINGE, MEHDI y
GAITANOS, JOHN

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Transacciones seguras de dispositivos móviles

Campo de la Invención

La presente invención se refiere a transacciones seguras de dispositivos móviles. Más específicamente, se refiere a métodos y aparatos que permiten que un dispositivo móvil funcione como un dispositivo de pago de manera segura sin necesidad de soporte físico seguro.

Antecedentes de la Invención

Cuando los dispositivos móviles (tal como teléfonos móviles, tabletas y computadoras portátiles) necesitan realizar operaciones o almacenar datos que podrían comprometer los activos del usuario (u otros) si los ven terceros malintencionados, es una práctica normal que un procesador realice estas operaciones o una memoria almacene estos datos para ubicarlos en un elemento seguro (SE) dentro del dispositivo móvil. El elemento seguro suele estar física y lógicamente protegido contra la subversión por un tercero malintencionado. El programa informático criptográfico y las claves criptográficas utilizadas por un dispositivo móvil se mantendrán típicamente en un elemento seguro - una tarjeta SIM de teléfono móvil es un ejemplo de un elemento seguro, y un SE también se usa típicamente para la comunicación inalámbrica local bajo protocolos NFC.

Las transacciones, particularmente las transacciones financieras, implican autenticación y datos que son confidenciales tanto para los usuarios como para otras partes. Cada vez más, un dispositivo informático móvil puede utilizarse como un dispositivo de pago. Tal dispositivo de pago es efectivamente una nueva forma de tarjeta de pago - las tarjetas de pago tal como las tarjetas de crédito y las tarjetas de débito se usan ampliamente para todas las formas de transacción financiera. El uso de tarjetas de pago ha evolucionado significativamente con los avances tecnológicos en los últimos años. Muchos pagos se realizan en tiendas minoristas, generalmente con una tarjeta de transacción física que interactúa con un terminal de punto de venta (POS) para realizar una transacción. Estas tarjetas de transacción pueden interactuar con un POS pasando a través de un lector de banda magnética, o una "tarjeta con chip" o "tarjeta inteligente" mediante contacto directo con un lector de tarjeta inteligente (según la norma ISO/IEC 7816) o mediante interacción sin contacto a través de comunicación inalámbrica local de corto alcance (según la norma ISO/IEC 14443).

Para una tarjeta sin contacto, el número de cuenta puede leerse automáticamente desde la tarjeta mediante un terminal POS, que utiliza generalmente una tecnología inalámbrica de corto alcance tal como la Identificación por Radio Frecuencia (RFID) - este enfoque se conoce generalmente como pago "sin contacto" o de "proximidad". Esto se habilita normalmente mediante la incrustación de una etiqueta RFID en un cuerpo de tarjeta junto con una antena adecuada para permitir la transmisión y recepción de señales inalámbricas - las transmisiones pueden alimentarse por una señal de interrogación de radio frecuencia emitida por un lector de proximidad en el terminal POS. Para que se establezca una conexión efectiva, es posible que sea necesario acercar la tarjeta de pago al lector de proximidad - esto tiene ventajas de seguridad y evita confusiones si hay varias tarjetas de pago habilitadas en las proximidades generales del lector de proximidad, así como normalmente es el caso en un establecimiento minorista, por ejemplo. Esto puede lograrse tocando la antena de la tarjeta de pago contra el lector de proximidad del terminal POS.

Los presentes solicitantes han desarrollado un sistema patentado, conocido como *PayPass®,* para realizar transacciones sin contacto. Los solicitantes presentes también han apreciado que sería posible utilizar un dispositivo informático tal como un teléfono móvil como un proxy para una tarjeta de pago. También han desarrollado una aplicación de pago móvil, Mobile *PayPass*$_{TM}$, que puede descargarse a un teléfono móvil para actuar como un proxy para una tarjeta de pago utilizando estándares de tecnología de Comunicación de Campo Cercano (NFC), que se incorporan en la mayoría de los teléfonos móviles actuales. La NFC es un desarrollo basado en RFID, y los dispositivos habilitados para NFC pueden operar de la misma manera que los dispositivos RFID - aunque un dispositivo NFC es activo en lugar de pasivo, ya que es alimentado por la batería del teléfono móvil en lugar de depender de la recolección inductiva desde un dispositivo lector. Usando Mobile *PayPass*$_{TM}$, un usuario puede realizar transacciones basadas en tocar con un lector de proximidad, así como realizar operaciones de administración de cuentas a través de una interfaz de red apropiada (celular, red inalámbrica local) en una interfaz de banca en línea con el proveedor de cuenta del usuario.

Como se indicó anteriormente, una aplicación de transacción tal como una aplicación de pago sin contacto utilizará datos confidenciales que no deberían exponerse a un tercero malintencionado. Por esta razón, tales aplicaciones de transacción utilizarán normalmente un elemento seguro tal como una tarjeta SIM de teléfono móvil o un elemento seguro integrado en un teléfono móvil - esto puede proporcionarse en una implementación del fabricante de protocolos NFC en el teléfono móvil, por ejemplo. Sin embargo, este enfoque depende de la cooperación del Operador de Red Móvil (MNO) para una tarjeta SIM o un fabricante de equipo original para un SE en un teléfono móvil. Incluso si dicha cooperación está disponible, la diversidad de SIM y teléfonos móviles hará que sea muy difícil utilizar un enfoque coherente, lo que significa que puede requerirse una personalización significativa del usuario para instalar y ejecutar una aplicación de transacción de manera efectiva. Esto impedirá que los usuarios adopten tales aplicaciones de transacción.

El documento WO 2013/151797 es una solicitud anterior del solicitante presente que describe el uso de claves de uso único para proporcionar aplicaciones de transacción móvil con credenciales de pago cuando el entorno informático del dispositivo móvil no comprende un elemento seguro. En Van Damme y otros, "A PKI-Based Mobile Banking Demonstrator", en "Public Key Infrastructures, Services and Applications", pp 147-158, Springer, septiembre de 2011, se sugiere que las técnicas criptográficas de caja blanca podrían utilizarse en aplicaciones de banca móvil. Wyseur, "White-Box Cryptography: Hiding Keys in Software" describe una variedad de técnicas criptográficas de caja blanca.

Resumen de la Invención

En un primer aspecto, la invención proporciona un dispositivo informático móvil que tiene un procesador y una memoria, en donde el procesador se programa con una aplicación de transacción móvil, en donde: la memoria comprende una base de datos local para contener elementos de datos para uso de la aplicación de transacción móvil, en donde una entrada en la base de datos local comprende un índice, un parámetro encriptado para uso por el algoritmo de transacción móvil, y un parámetro adicional asociado con la etapa de cifrado/descifrado para el parámetro encriptado para esa entrada; y
en donde la aplicación de transacción móvil se adapta para cifrar elementos de datos para el almacenamiento en la base de datos local y para descifrar elementos de datos almacenados en la base de datos local usando técnicas criptográficas de caja blanca.

Este enfoque permite el uso de una aplicación de transacción genérica que no se personaliza para un usuario sin comprometer la seguridad del usuario o del emisor. Esto permite que la experiencia del usuario sea esencialmente similar a la proporcionada con otras aplicaciones móviles.

En un tipo de modalidad, la aplicación de transacción móvil se adapta para utilizar criptografía de caja blanca estática y utiliza un algoritmo de derivación de clave en el cifrado y almacenamiento de datos en la base de datos encriptada local. El parámetro adicional puede ser entonces un contador de secuencia de aplicación para indicar una transacción en la que se realizó una operación asociada con la entrada.

En otro tipo de modalidad, la aplicación de transacción móvil se adapta para utilizar criptografía de caja blanca dinámica y utiliza un algoritmo de transporte de clave en el cifrado y almacenamiento de datos en la base de datos encriptada local. En este caso, el parámetro adicional puede ser una clave encriptada para esa entrada. En ciertas modalidades de este tipo, la aplicación de transacción móvil se comunica con un servidor adaptado para asegurar uno o más parámetros usados por la aplicación de transacción móvil.

En modalidades, la aplicación de transacción móvil y la base de datos local se protegen mediante ofuscación de programa informático.

Preferiblemente, la aplicación de transacción móvil se descarga al dispositivo informático móvil sin personalización para el dispositivo informático móvil o su usuario. En algunos casos, en la instalación o inicialización, la aplicación de transacción móvil puede personalizarse luego al dispositivo informático móvil o a su usuario.

En modalidades particulares, el dispositivo informático móvil se adapta para actuar como un dispositivo de pago y en donde la aplicación de transacción móvil es una aplicación de pago. El dispositivo informático móvil puede adaptarse para emular una tarjeta de pago sin contacto.

En las modalidades, el dispositivo informático móvil es o comprende un teléfono móvil.

En un aspecto adicional, la descripción proporciona un método para operar una aplicación de transacción móvil en un dispositivo informático móvil, en donde el dispositivo informático móvil comprende un procesador adaptado para ejecutar la aplicación de transacción móvil y una memoria que comprende una base de datos local para contener elementos de datos para uso de la aplicación de transacción móvil, el método comprende: identificar uno o más elementos de datos para su almacenamiento o recuperación desde la base de datos local; y encriptar el uno o más elementos de datos para el almacenamiento en la base de datos local usando técnicas criptográficas de caja blanca, o descifrar el uno o más elementos de datos almacenados en la base de datos local utilizando técnicas criptográficas de caja blanca; en donde una entrada en la base de datos local comprende un índice, un parámetro encriptado para uso por el algoritmo de transacción móvil, y un parámetro adicional asociado con la etapa de cifrado/descifrado para el parámetro encriptado para esa entrada.

Breve Descripción de las Figuras

Las modalidades de la invención se describirán ahora, solamente a manera de ejemplo, con referencia a las Figuras acompañantes, en las cuales:
la Figura 1 muestra elementos de una infraestructura de pago en la que pueden utilizarse modalidades de la invención;
la Figura 2 muestra un teléfono móvil adaptado para su uso como una modalidad de la invención;
las Figuras 3A a 3D ilustran los siguientes modelos: caja negra, caja blanca, caja blanca con criptografía de caja blanca y caja gris;

la Figura 4 ilustra una aplicación de transacción móvil con una base de datos local encriptada de acuerdo con las modalidades de la invención;
las Figuras 5A y 5B comparan enfoques criptográficos de caja blanca estáticas y dinámicas;
la Figura 6 ilustra un diseño apropiado para el uso de una base de datos encriptada local cuando se usa un elemento seguro personalizado en una disposición que no es una modalidad de la invención pero que es útil para explicar las modalidades de la invención;
la Figura 7 muestra una primera transformación para adaptar el diseño de la Figura 6 a una implementación de caja blanca estática;
la Figura 8 muestra una segunda transformación para adaptar el diseño de la Figura 6 a una implementación de caja blanca estática;
la Figura 9 muestra la interacción entre una aplicación de transacción móvil y una base de datos local encriptada de acuerdo con una modalidad de la invención;
la Figura 10 muestra una construcción de caja blanca dinámica para su uso en una modalidad adicional de la invención;
la Figura 11 muestra una aplicación de transacción móvil con una base de datos local encriptada de acuerdo con las modalidades de la invención que implementa la construcción de caja blanca dinámica de la Figura 10;
la Figura 12 muestra los principios operativos para las modalidades soportadas por el primer y segundo servidor ilustradas en las Figuras 13 y 14 respectivamente; y
la Figura 15 muestra una modalidad adicional soportada por servidor, con la Figura 16 que ilustra cómo se emplea esto en el funcionamiento de una aplicación de transacción móvil de acuerdo con una modalidad de la invención.

Descripción de Modalidades Específicas

Las modalidades específicas de la invención se describirán a continuación con referencia a las Figuras. Las modalidades descritas a continuación se refieren a un teléfono móvil utilizado como un dispositivo de pago para pagos sin contacto con terminales POI (punto de interacción) (tal como un terminal POS - punto de venta) bajo los protocolos EMV indicados anteriormente, pero como se analiza más adelante, otras modalidades pueden utilizarse en otros contextos y sistemas de transacción.

Se proporciona un usuario (no mostrado) con un dispositivo de pago en la forma de un dispositivo informático móvil - esto se muestra aquí como teléfono móvil 1, pero puede ser por ejemplo una computadora portátil o una tableta. El teléfono móvil 1 se adapta para actuar como un proxy para una tarjeta de pago física (o puede utilizarse para una tarjeta de pago virtual sin contraparte física directa). El teléfono móvil 1 equipado con medios para comunicarse con otros elementos de una infraestructura de pago, en el sentido de que comprende antenas y soporte físico y programa informático asociados para permitir la comunicación mediante NFC y protocolos de tarjeta sin contacto asociados tal como los definidos en ISO/IEC 14443.

Normalmente, se fijan otros equipos informáticos en la infraestructura, tal como los terminales 4 de puntos de interacción (POI), cuyo ejemplo se muestra en un terminal de punto de venta (POS) utilizado por un comerciante que interactúa con el usuario. El terminal 4 POS interactúa con el teléfono móvil 1 a través del lector 3 de tarjeta sin contacto. El terminal 4 POS de comerciante se conecta normalmente o puede conectarse a un banco de adquisición 6 u otro sistema de una manera segura (a través de un canal dedicado o a través de un mecanismo de comunicación seguro a través de un canal público o inseguro). También puede haber un mecanismo para permitir la conexión entre el teléfono móvil 1 (u otro dispositivo informático de usuario) y un banco emisor 5 de tarjeta o sistema asociado con el usuario. Una infraestructura bancaria 7 también conectará al emisor 5 de la tarjeta y al banco de adquisición 6, permitiendo que las transacciones se lleven a cabo entre ellos. Esta infraestructura bancaria será normalmente proporcionada por un proveedor de tarjeta de transacción que proporciona servicios de tarjeta de transacción al banco emisor 5 de la tarjeta. La infraestructura bancaria 7 proporciona autorización en el momento de la compra, autorización de la transacción y conciliación normalmente dentro del mismo día hábil, y depósito de los pagos poco después. La infraestructura bancaria 7 comprende una pluralidad de conmutadores, servidores y bases de datos, y no se describe más aquí ya que los detalles de la infraestructura bancaria utilizada no son necesarios para comprender cómo funcionan y pueden implementarse las modalidades de la invención.

La Figura 2 muestra partes esquemáticamente relevantes de una arquitectura representativa de soporte físico y programa informático para un dispositivo informático móvil adecuado para implementar una modalidad de la invención. En el ejemplo mostrado, cada dispositivo informático móvil es un dispositivo móvil de telecomunicaciones celulares ("teléfono móvil" o "dispositivo móvil") - en otras modalidades, el dispositivo informático puede ser otro tipo de dispositivo informático tal como una computadora portátil o una tableta y el dispositivo informático no necesita tener capacidades de telecomunicaciones celulares.

El teléfono móvil 1 comprende un procesador de aplicación 12, una o más memorias 13 asociadas con el procesador de aplicaciones, una SIM o USIM 14 que comprende tanto capacidades de procesamiento y memoria como un controlador NFC 15. El teléfono móvil también tiene una pantalla 16 (mostrada como una superposición a los elementos informáticos representados esquemáticamente del dispositivo), que proporciona en este ejemplo una interfaz de usuario de pantalla táctil. El teléfono móvil está equipado con un aparato de telecomunicaciones inalámbrico 17 para la comunicación con una red de telecomunicaciones inalámbrica y un aparato de comunicación inalámbrica local 18 para la interacción mediante NFC.

En la disposición mostrada, el procesador de aplicación 12 y las memorias asociadas 13 comprenden (mostradas dentro del espacio del procesador, pero con código y datos almacenados dentro de las memorias) una aplicación de pago móvil 101 - mostrada explícitamente dentro de las memorias 13 está la base de datos local encriptada 102. También contendrá otras aplicaciones normalmente necesarias para dicho dispositivo, tal como un navegador 103 y un módem 104. La SIM/USIM 4 comprenderá un dominio de seguridad 105 adaptado para soportar acciones criptográficas y una aplicación de NFC 106 que interactúa con el controlador de NFC 15, que tiene interfaces 107 a dispositivos y etiquetas NFC - aquí puede proporcionarse un extremo frontal sin contacto 108, que interactúa con una aplicación de elemento seguro asociada a la aplicación de pago 1. La SIM/USIM 14 se protegerá normalmente física y lógicamente contra la subversión. Debe observarse que la aplicación de pago 101 y la base de datos local encriptada 102 se ubican ambas dentro del procesador de aplicación 12 y espacio de memorias asociadas 13, no confían en el dominio de seguridad 105 provisto dentro de la SIM/USIM 104 o en cualquier otro dominio de seguridad protegido por soporte físico seguro.

Los requisitos para las transacciones con tarjeta sin contacto y los protocolos asociados se describen con más detalle en las Especificaciones Sin Contacto EMV para Sistemas de Pago, disponibles en https://www.emvco.com/specifications.aspx?id=21, lo que se dirige al experto en la técnica. Esto no se discutirá con más detalle aquí, ya que los protocolos específicos usados no son relevantes para la implementación de las modalidades de la invención. Para estos fines, es suficiente señalar que la aplicación de pago móvil 101 y la base de datos local encriptada 102 contienen datos que son extremadamente confidenciales para el usuario, y también pueden ser muy confidenciales para otras partes tal como el emisor 5 de la tarjeta. Por lo tanto, es necesario que la aplicación de pago móvil 101 y la base de datos local encriptada 102 existan, y funcionen, de tal manera que estos datos confidenciales no estén expuestos a terceros malintencionados. Como la aplicación de pago móvil 101 y la base de datos local encriptada 102 se ubican en las memorias asociadas 13 con el procesador principal 12, esto proporciona un desafío técnico significativo debido a que no está disponible la solución técnica normal de mantener tales datos confidenciales en una región físicamente protegida (tal como la SIM/USIM 14).

La importancia de la disponibilidad de un entorno operativo seguro, y la solución operativa lograda en las modalidades de la invención, se muestran en las Figuras 3A a 3D. La Figura 3A muestra unas disposiciones convencionales en las que un proceso E se ejecuta dentro de un elemento seguro SE, con material confidencial tal como la clave K también disponible solo dentro del SE. El SE se encuentra dentro pero protegido de un entorno operativo "hostil" (es decir sin protección) que se supone puede observarse por terceros malintencionados - todo lo que pueden observar estos terceros son las entradas I y las salidas E del proceso E, que no son confidenciales o si son confidenciales, normalmente se encriptan mediante el proceso E para su descifrado por un destinatario previsto (tal como el terminal POS del comerciante en una transacción). El SE aquí puede considerarse una "caja negra" desde el punto de vista de un tercero, y esto puede denominarse un modelo de caja negra.

Cuando el proceso E es (o es parte de) una aplicación de pago móvil 101, será necesario para el proceso que se suministre por el emisor de la tarjeta o en nombre del emisor de la tarjeta una o más claves para permitir que el usuario se autentique al emisor de la tarjeta como el legítimo titular de la tarjeta. En este modelo convencional, el emisor de la tarjeta puede utilizar una clave de emisor de tarjeta K_{ISS} para derivar una clave de dispositivo discreto K_D para cada dispositivo informático móvil, por ejemplo, usando la huella digital móvil junto con K_{ISS} como entradas a un algoritmo de derivación de clave. En una transacción, la clave del dispositivo K_D luego puede utilizarse para generar una clave de sesión K_S para utilizar en esa transacción (o para parte de una transacción) usando otro proceso de derivación de clave, por ejemplo, usando el contador de secuencia de aplicación (ASC) de la aplicación móvil como una entrada así como K_D. Este enfoque protege a la K_{ISS} como esta clave no necesita transmitirse a ninguna parte por el emisor, proporciona una clave de dispositivo discreta K_D para cada dispositivo informático móvil que se protege dentro del elemento seguro, y en operaciones de transacción utiliza una clave de sesión K_S que si es descubierto por un tercero malintencionado no debería afectar futuras transacciones.

Si bien este modelo parece satisfactorio a efectos de seguridad, tiene importantes desventajas prácticas. En un teléfono móvil, la SIM/USIM proporciona un elemento seguro, pero esto está bajo el control del operador de red móvil (MNO) - para utilizar esta SIM/USIM para cualquier propósito adicional se requerirá un acuerdo específico entre el proveedor de la infraestructura de pago y el MNO, y dada la confidencialidad de la información ya presente en la SIM/USIM, la configuración de cualquier aplicación que use la SIM/USIM como recurso será compleja y deberá asegurar al MNO que la integridad de la SIM/USIM no está comprometida. Esta es una barrera importante para la aceptación del usuario - un usuario deseará normalmente poder instalar una aplicación genérica desde una tienda de aplicaciones, y luego poder utilizar esa aplicación de la misma manera que cualquier otra aplicación móvil, con un máximo de una etapa de inicialización limitado en la instalación. Otro enfoque sería persuadir a los fabricantes de equipos originales (OEM) para que proporcionen un elemento seguro adicional directamente en el teléfono móvil - en efecto, una memoria adicional que también es segura - pero esto aumenta el costo del teléfono móvil sin afectar significativamente la facilidad de instalación o uso de una aplicación móvil.

La Figura 3B muestra el modelo que existe cuando se elimina el SE - no solo las entradas I y las salidas O son visibles para terceros, sino también las claves K. Las etapas intermedias en la ejecución de E también son visibles - esto significa que si no se sabe, el proceso E puede modificarse normalmente por ingeniería inversa para que se conozca cada parte de este proceso. Esto se conoce como un modelo de "caja blanca" - en efecto, para el proceso que se

muestra no hay seguridad aparente en absoluto. Sin embargo, este enfoque es barato de implementar, y permite que una aplicación móvil funcione en la memoria principal no protegida de la misma manera que otras aplicaciones móviles. Los presentes inventores han determinado de este modo que sería deseable permitir la operación en este paradigma con la condición de que haya una manera de obtener suficiente seguridad para la operación práctica.

La Figura 3C muestra una forma de mejorar la seguridad dentro de este modelo. En este enfoque las entradas I y las salidas O todavía están disponibles para su inspección en el entorno operativo principal, pero las claves K se incluyen en el proceso E de manera que ninguno de los atacantes puede interceptarlo eficazmente. Esto puede hacerse mediante el uso de "criptografía de caja blanca" - se describen los principios generales de la criptografía de caja blanca, por ejemplo, en "On White-Box Cryptography" por Marc Joye en A. Elçi, S.B. Ors, y B. Preneel, Eds, " Security of Information and Networks", pp. 7-12, editorial Trafford, 2008, y las implementaciones comerciales de caja blanca de algoritmos criptográficos ampliamente utilizados están disponibles. El objetivo de la criptografía de caja blanca (WBC) es implementar un algoritmo criptográfico *E*(*K*) en el programa informático de manera que los activos criptográficos - claves y transformaciones secretas equivalentes -- permanezcan seguros incluso cuando el atacante tenga acceso al programa informático.

Hay dos enfoques básicos para la criptografía de caja blanca: la criptografía de caja blanca estática (SWB) y la de caja blanca dinámica (DWB). Estos se describirán adicionalmente a continuación, y como se observa más adelante a continuación, ambos pueden utilizarse para proporcionar modalidades de la presente invención.

En la Figura 3D se muestra un modelo intermedio - en este enfoque, nuevamente no hay un elemento seguro presente, pero el proceso confidencial E y las claves K se mantienen dentro de una capa protegida lógicamente, con protección provista en programa informático por técnicas tales como ofuscación de programa informático. Esto puede llamarse un modelo de caja gris (GB). Tal técnica será efectiva para proteger los algoritmos E y las claves K, pero solo por un corto período de tiempo. Consecuentemente el modelo GB podría utilizarse para proteger una clave de sesión K_S y su uso en la ejecución del proceso E, pero no sería lo suficientemente fuerte para la protección a largo plazo de una clave de dispositivo K_D, y sería claramente inadecuado para proteger una clave de emisor K_{ISS}.

La estructura general de la aplicación móvil 101 y la base de datos local encriptada 102 utilizada en las modalidades de la invención se muestran en la Figura 4. La aplicación móvil 101 se usa para transacciones con otra parte - es particularmente apropiada para su uso en un dispositivo de pago para realizar transacciones sin contacto bajo los protocolos EMV sin contacto como se menciona anteriormente. La aplicación móvil 101 se adapta para escribir en (41) y leer desde (42) la base de datos local encriptada 102. La base de datos local encriptada 102 puede contener cualquier parámetro necesario para el funcionamiento de la aplicación móvil 101 que sea potencialmente confidencial al usuario o a cualquier otra parte, tal como un emisor de tarjeta o un comerciante.

En la modalidad mostrada, cada entrada 43 en la base de datos local encriptada 102 tiene tres elementos: un índice 44; un valor de contador de secuencia de aplicación 45; y un parámetro encriptado 46. La longitud de las entradas 43 es variable. El índice 44 corrige la posición en la base de datos local encriptada 102 donde se almacena un parámetro específico. El valor contador de secuencia de aplicación 45 (que se representa gráficamente como ASN) proporciona una referencia a la transacción durante la cual se realizó una operación relevante (que da como resultado, normalmente, la escritura del parámetro en la base de datos). El parámetro encriptado 46 (EPARAM) contiene contenido encriptado en un formato apropiado (tal como TLV) para protección a largo plazo.

Los inventores han determinado que, al utilizar este enfoque, es posible que la aplicación de transacción móvil 101 sea una aplicación genérica que no se diferencia inicialmente para cada usuario. Esto significa que la aplicación puede descargarse por el usuario desde una tienda de aplicaciones e instalarse en la memoria principal de la misma manera que una aplicación móvil normal, por lo que la experiencia del usuario en la instalación es familiar. Esto significa que cualquier iniciación por un usuario debe ocurrir en o después de la instalación de la aplicación móvil 101 en el dispositivo informático móvil. Esto requiere inmediatamente un modelo de confianza diferente al utilizado en un modelo de caja negra convencional, porque en este modelo la clave del dispositivo K_D se personaliza para el dispositivo por el emisor de la clave y se aprovisiona para el elemento seguro bajo el control de clave del emisor.

La aplicación móvil 101 y la base de datos local encriptada 102 deben ser resistentes tanto a los ataques pasivos como a los activos, ya que existen en un entorno de operación no protegido. La protección contra ataques estáticos se proporciona por las técnicas criptográficas de caja blanca y (si se utiliza un enfoque de caja gris) mediante ofuscación de programa informático. También se necesita protección contra ataques activos tal como el levantamiento de códigos y datos. En dichos ataques, un atacante intenta acceder a los elementos de la base de datos encriptados desde un dispositivo móvil específico, los copia, y los ejecuta para su ejecución en su propio entorno de ejecución móvil, utilizando la misma aplicación móvil 101 - que es genérica y no personalizada para un usuario individual - para implementar los mismos procesos criptográficos utilizando las mismas claves del sistema. A continuación, se proporciona una discusión más detallada de cómo se abordan los ataques activos en relación con las modalidades específicas de la invención.

El sistema puede construirse de manera que los parámetros encriptados 46 en la base de datos local encriptada 102 tengan confidencialidad (solo pueden leerse por la aplicación móvil 101 y la integridad (solo pueden modificarse por la aplicación móvil 101). La confidencialidad y la integridad pueden ser provistas con los mismos mecanismos, como se

discutirá a continuación. Estos parámetros pueden utilizarse por la aplicación móvil 101 para cualquiera o todos los procesos generales, como material clave para primitivas criptográficas, o específicamente como material clave para primitivas criptográficas que utilizan un modelo de WBC (en el que se supone que un atacante tiene acceso completo a la aplicación móvil 101).

Como se indicó anteriormente, la aplicación móvil 101 es genérica y puede descargarse de una tienda de aplicaciones. En diferentes modalidades, la aplicación móvil puede ser inicializable o no inicializable antes de que comience su vida operativa. Las modalidades de cada uno se describen a continuación - cuando es posible la inicialización, el usuario puede crear claves criptográficas específicas para el usuario y/o para el dispositivo informático móvil.

Como se ha indicado anteriormente, en modalidades de la invención se usan técnicas criptográficas de caja blanca para la aplicación móvil 101. Para proporcionar protección adicional, las técnicas de caja gris también pueden utilizarse en modalidades de la invención. Cuando solo se usa un enfoque de caja blanca, un atacante tiene acceso ilimitado a la base de datos local encriptada 102 y a la lógica de la aplicación móvil 101, pero cuando se usa un enfoque de caja gris la lógica de la aplicación al menos se protege usando técnicas adicionales tal como ofuscación de programa informático. Para mejorar la seguridad, actualmente se prefieren las modalidades que utilizan un enfoque de caja gris.

Las modalidades de la invención se describirán adicionalmente a continuación usando técnicas criptográficas de caja blanca estática (SWB) y de caja blanca dinámica (DWB). La diferencia conceptual entre estos dos enfoques se describirá ahora con referencia a las Figuras 5A y 5B.

La Figura 5A muestra una implementación de SWB en la que se fija una clave secreta K, pero se "funde" en la estructura de cifrado de bloques para que un atacante no pueda realizar una ingeniería inversa. Se convierte en parte integral de la implementación en la compilación de la aplicación móvil 101.

La Figura 5B muestra una implementación de DWB en la que la clave K puede cambiar en cada llamada a la aplicación móvil 101. En una implementación de este tipo la clave dinámica K se pasa como un parámetro, pero en primer lugar se transforma de manera segura antes de transmitirse a través del entorno no protegido. Hay dos posibles tipos de transformación:

- Transformaciones t sin clave *o(K)*, en donde la seguridad se basa en el secreto de la transformación misma - o(K) puede considerarse una función de ofuscación. Esto puede implementarse como una transformación de ofuscación con una tabla secreta de codificación/descodificación. Así $o^{-1}(K)$ es la transformación de ofuscación inversa que permite la recuperación de la clave de sesión en el destino, después de pasar el entorno no seguro. Este enfoque es particularmente adecuado cuando no será práctico que haya ninguna etapa de inicialización para una aplicación de transacción móvil descargada.

- Cifrado con un algoritmo de cifrado/descifrado de propósito general e_R (K). La implementación generada usa una clave *R*, que es único por usuario/dispositivo móvil, que se utiliza para encriptar la clave dinámica K después de su generación y para descifrarla internamente a la primitiva DWB(E) para utilizarse por el algoritmo de cifrado E.

Ahora se describirá una implementación de caja blanca estática de una modalidad de la invención con referencia a las Figuras 7 a 9, y también a la Figura 5A descrita anteriormente.

En primer lugar, debe tenerse en cuenta que es necesario tener cuidado para proteger contra ataques pasivos en primitivas criptográficas cuando se utiliza una aplicación de transacción móvil genérica. El emisor no puede establecer una clave maestra por tarjeta K_D, ya que esto requeriría una aplicación de transacción móvil por usuario. En las disposiciones de la técnica anterior que utilizan un elemento seguro, una clave de dispositivo K_D se calcula generalmente a partir de la clave maestra del emisor K_{ISS} en las instalaciones seguras del usuario derivadas en parte de la información del usuario (tal como el Número de Cuenta Principal (PAN) de un usuario.

Para una aplicación de transacción móvil genérica, la clave maestra K_{ISS} debe incrustarse de manera segura en la aplicación de transacción móvil. La aplicación de transacción móvil calculará el equivalente de una K_D en cada carrera. Por lo tanto, la caja blanca estática (SWB) necesita tener la K_{ISS} codificada directamente en su algoritmo de cifrado (por ejemplo, un algoritmo de cifrado AES256).

Un riesgo es que el atacante intente obtener la K_{ISS} incrustada desde la aplicación de transacción móvil al intentar criptoanalizar la implementación de la caja blanca. Para las implementaciones de SWB actuales, este riesgo puede considerarse lo suficientemente grande como para que sea deseable proporcionar protección adicional, aunque esto puede cambiar para futuras implementaciones de SWB. Puede ser deseable como resultado el uso en la práctica de una implementación de caja gris, en la que la disposición descrita a continuación se protege adicionalmente mediante ofuscación de programa informático. Las técnicas específicas de ofuscación de programa informático no se describen aquí adicionalmente, pero el experto podrá sin dificultad identificar recursos de ofuscación de programa informático apropiados de la literatura técnica existente. Por lo tanto, la ofuscación de la caja gris no se mostrará explícitamente en

los dibujos, que se centrarán en la implementación de la caja blanca de la aplicación de transacción móvil y el diseño de la base de datos local encriptada.

La Figura 6 indica una solución "ideal" que se aplicaría si la aplicación de transacción móvil se personalizara en el emisor (como podría ser el caso con un elemento seguro, pero no con una aplicación de transacción móvil genérica descargable). La clave maestra K_{SYS} (equivalente a K_{ISS} utilizada anteriormente) se utiliza por el emisor para derivar la clave del dispositivo de usuario K_C (equivalente a K_D utilizada anteriormente) en una fase de personalización con información del usuario tal como el PAN utilizado como diversificador, con K_{SYS} nunca visible fuera del emisor y con K_D guardada en la memoria permanente de, y así protegido en, el elemento seguro. El elemento seguro puede establecerse en una etapa de "vida operativa" inicializada antes de que llegue al usuario. Puede realizarse una operación de escritura de la siguiente manera, como se muestra en la Figura 6.

En su vida operativa la aplicación de transacción móvil realiza una operación de escritura en Índice *i* como sigue:

- La clave K_i se deriva de la clave K_C dependiendo del índice *i* en la base de datos donde el parámetro específico PARAM*i* tiene su lugar y en el número de la transacción actual realizada por la aplicación, es decir el número de secuencia de la aplicación (ASN).
- El parámetro PARAM*i* para establecerse en la base de datos se encripta con la clave K_i para obtener el valor encriptado EPARAM*i*.
- El índice *i*, el ASN y la forma encriptada del parámetro EPARAM*i* se establecen en la base de datos.

En su vida operativa la aplicación de transacción móvil realiza una operación de lectura en Índice *i* como sigue:

- El ASN y la forma encriptada del parámetro EPARAM*i* se retiran de la base de datos en la entrada de fila identificada por Índice *i*.
- El índice *i* y el ASN recuperados de la base de datos se usan para derivar la clave K_i. La clave K_i se deriva de la clave K_C que depende del índice *i* en la base de datos donde el parámetro específico EPARAM*i* tiene su lugar y del número de la transacción cuando la aplicación realizó la escritura, es decir el entonces ASN (y no el ASN actual).
- La clave K_i se usa para descifrar el parámetro encriptado EPARAM*i* como se almacena en la base de datos y recuperar su valor original PARAM*i*.

Como estas "condiciones ideales" no se aplican en el régimen de la caja blanca, el diseño se modifica por transformación. La Figura 7 muestra una primera transformada utilizada para proteger contra un ataque pasivo. Esto muestra que las etapas separadas de derivar K_C de K_{SYS} y Ki de K_C se fusionan en un algoritmo de caja blanca estático apropiado, como se muestra, con K_{SYS}. Varios algoritmos criptográficos adecuados pueden utilizarse para este propósito, tal como AES-256. La Figura 8 muestra una segunda transformada utilizada para proteger contra un ataque de levantamiento de código activo. En este enfoque, la entrada del usuario o una huella digital móvil se utilizan como una entrada adicional para modificar y, por lo tanto, personalizar K_i.

La Figura 9 ilustra la adaptación del protocolo de seguridad "ideal" utilizado en un caso de elemento seguro al caso de criptografía de caja blanca estática utilizado en una modalidad de la invención - esto puede utilizarse para proporcionar las transformaciones necesarias en la estructura general de la aplicación de transacción móvil y las bases de datos locales encriptadas que se muestran en la Figura 4. Una operación de escritura se muestra en el lado izquierdo del diagrama - un índice I y un valor ASN son entradas al algoritmo de caja blanca estática que utiliza una K_{SYS} incrustada para crear una clave K_i para ese valor de índice, que luego se personaliza para el usuario o dispositivo móvil por combinación con la entrada del usuario o la huella digital móvil para formar K'_i. La K'_i se utiliza para encriptar el parámetro $PARAM_i$ para formar el parámetro encriptado $EPARAM_i$, que luego se almacena bajo ese índice i.

La operación de lectura es la inversa del procedimiento de escritura, y se muestra en el lado derecho del diagrama. La K'_i se vuelve a calcular utilizando el mismo procedimiento utilizado originalmente para crearla. La K'_i luego se utiliza para descifrar $EPARAM_i$ para recrear $PARAM_i$.

Todos los procedimientos de la Figura 9 pueden protegerse aún más mediante la ofuscación de programa informático - es decir, todo este proceso puede tener lugar en una "caja gris".

El enfoque de la Figura 9 asume que no hay personalización del usuario de la aplicación de transacción móvil - la entrada del usuario o la huella digital móvil se proporciona cuando se ejecuta la aplicación de transacción móvil, que es completamente genérica. La personalización del usuario en la inicialización puede utilizarse en conexión con un enfoque criptográfico de caja blanca dinámica. Una modalidad de la invención que utiliza tal enfoque se describe con referencia a las Figuras 10 y 11, y también a la Figura 5B descrita anteriormente.

En este modelo la seguridad de la base de datos local encriptada se basa en una clave generada localmente aleatoria DK_i - esta es una diferencia significativa de la modalidad SWB descrita anteriormente. No se depende de una jerarquía clave de K_{SYS}. Por otra parte, la exposición a un ataque potencial por DK_i es muy breve - todas las demás claves se transportan de manera encriptada y las operaciones de cifrado y descifrado se llevan a cabo de acuerdo con un enfoque de caja blanca. Esta disposición proporciona protección contra ataques activos sin necesidad de intervención continuada del usuario más allá del procedimiento de inicialización, que es una diferencia con la modalidad SWB donde

la protección contra ataques activos se realiza mediante el uso de la entrada del usuario o huella digital móvil durante las operaciones de escritura y lectura.

La construcción principal utilizada por la modalidad se muestra en la Figura 10 - esta es una implantación del enfoque mostrado en la Figura 5B, donde la transformación se implementa como cifrado o descifrado con la clave R.

En cuanto a la modalidad anterior, se prefiere que todo este proceso tenga lugar en un entorno de caja gris. El algoritmo de cifrado implementado para la transformación en el entorno de caja gris puede ser por ejemplo SWB AES 256-E con la clave R codificada en su estructura. El algoritmo de descifrado implementado en la construcción de caja blanca dinámica puede ser un algoritmo AES 256-I parametrizado con la clave R establecida como un parámetro en el entorno protegido WB de la construcción DWB.

Durante una etapa de inicialización realizada por el usuario, una aplicación de transacción móvil genérica descargada de una tienda de aplicaciones puede tener una clave de sistema K_{SYS} para SWB AES 256 E reemplazada por un dispositivo o clave específica del usuario R. Es posible que la misma aplicación genérica se pueda utilizar para lograr una implementación de SWB o DWB dependiendo de si la inicialización del usuario tiene lugar o si es compatible con el dispositivo de computación móvil. Después del cambio de clave a R, un atacante ya no podrá realizar un ataque eficaz de levantamiento de código o datos incluso si se evita la protección de la caja gris, ya que el atacante no podrá replicar los procesos relevantes en su propio soporte físico porque la clave R no estará disponible.

No hay un equivalente en este modelo para el uso de K_i como un parámetro para el algoritmo AES-128 E - este bloque de cifrado ahora es específico del usuario o dispositivo y se genera como una implementación de WB dinámica con la clave aleatoria R generada durante el proceso de inicialización utilizada como clave de transporte. Esto elimina un riesgo asociado con la modalidad anterior. La caja gris solo necesita proteger la clave operativa DK*i* desde el momento en que se genera hasta el momento que se encripta con la clave de transportación *R*.

El principio básico de operación es que la aplicación de transacción móvil se instancia con una clave aleatoria *R* solo en el momento en que se invoca el procedimiento de inicialización. Esta clave se utilizará como clave de transporte en el entorno hostil para transferir la clave operativa DKi de manera encriptada desde su generación hasta su uso para el cifrado/descifrado de IN PARAM a EPARAM y de EPARAM a OUT PARAM. La implementación de caja blanca dinámica luego realiza una operación de descifrado utilizando la clave de transporte *R* para obtener la clave DK*i* de manera que no se expone ninguna información sobre esta clave fuera de la caja de arena implementada de la caja blanca.

La secuencia de inicialización consiste en las siguientes llamadas ejemplificativas de la API de cifrado para el cifrado (se necesitan secuencias similares para obtener las funciones de descifrado):

Tabla 1

• Crea la función de encriptación SWBC:
S_encrypt_WBC (entrada, tamaño), donde *entrada* es la clave para transportarse y el tamaño es su longitud de bytes
para el transporte de la DK*i*, utilizando la clave de transporte específica del usuario/dispositivo *tk* como una clave estática incrustada en un modo WBC en el AES256.
Esta función se crea por la llamada API como:
Crear WBC Estática(cifrar, *tk,* S_encrypt_WBC, AES256)
• Crea la función de encriptación DWBC:
D_encrypt_WBC (ekey, entrada, tamaño), donde *ekey* es la forma encriptada de la clave *DKi* que utiliza la clave de transporte *tk, entrada* es el parámetro AES 128 protegido en DBE y el tamaño es su longitud de bytes.
Esta función se crea mediante una llamada API como:
Crear WBC Dinámica (cifrar, tk, D_encrypt_WB, AES 128).
• DK*i* = Aleatorio(16); /* genera la tecla clave de operación de clave DK*i* de 16 bytes* /
• Ekey = S_encrypt_WBC(DKi, 16); /* crea la clave de transportación Ekey*/
• EDATA = D_encrypt_WBC (Ekey, DATA, n* 16)

Una secuencia de inicialización ejemplar se muestra arriba en la Tabla 1. Solo se muestran las funciones de cifrado - se aplican los mismos principios para las funciones de descifrado, y el experto puede determinarlas de manera rutinaria.

El diseño general de esta modalidad en su estado de vida operativa se muestra en la Figura 11. Si bien es similar generalmente a la disposición que se muestra en la Figura 4, tiene ciertas diferencias que se discutirán a continuación.

La clave dinámica se genera a partir de una función de reloj CLK y un generador de números aleatorios programables PRNG para proporcionar una semilla aleatoria al generador criptográfico de caja blanca estática para la clave DK_i, que luego se cifra para formar EDK_i y se usa como entrada para la construcción de caja blanca dinámica DWB(E) que encripta el parámetro para formar $EPARAM_i$. La EDK_i y $EPARAM_i$ se transportan juntos a la base de datos encriptada bajo el índice i.

En su vida operativa, la aplicación de transacción móvil realiza las siguientes llamadas para el cifrado del parámetro INPARAM de n * 16 bytes:

- DKi = Aleatorio (16); /* genera la clave de operación clave DKi de 16 bytes */
- Ekey = S_encrypt_WB(R,16); /* crea la clave de transportación Ekey*/
- EPARAM = D_encrypt_WB(Ekey, IN PARAM, n*16)

Como puede verse en la Figura 11, la estructura de la base de datos encriptada es ligeramente diferente de la de la modalidad SWB descrita anteriormente. Cada entrada en la base de datos puede volver a ser de longitud variable, pero los elementos necesarios para cada entrada son ahora los siguientes:

- Índice - Posición de reparación en el DBE donde se almacena un parámetro específico
- EDK - El criptograma bajo la clave específica de usuario/móvil R de la clave DKi utilizada para el cifrado del contenido.
- EPARAM -- contenido encriptado de longitud variable (por ejemplo, en formato TLV) para proteger a largo plazo.

Pueden realizarse modificaciones adicionales a este enfoque para proporcionar una mayor seguridad mediante el uso de un proceso compatible con el servidor. Un punto de vulnerabilidad es que el modelo de caja gris se utiliza para proteger la clave de operación DK_i y también IN PARAM y OUT PARAM. La Figura 12 muestra dos enfoques alternativos para abordar este punto de vulnerabilidad mediante el uso de soporte de servidor. Estos modelos se describirán con mayor detalle con respecto a las Figuras 13 y 14, describiéndose otro modelo soportado por el servidor con referencia a las Figuras 15 y 16.

La Figura 13 ilustra un primer modelo soportado por el servidor en el que una de las operaciones de caja gris - la generación de la clave operativa DKi - se asegura mediante un servidor remoto. Este servidor remoto puede considerarse como un entorno de ejecución protegido que proporciona un mayor nivel de seguridad que la caja gris proporcionada por la ofuscación de programa informático en el entorno de ejecución principal del dispositivo informático móvil. En este enfoque, es el servidor el que ejecuta el mecanismo AES 256 E con la clave de usuario R como parámetro - solo la EDK*i* se envía a la aplicación de transacción móvil. La construcción de caja blanca dinámica usa DK*i* como la clave de operación para el cifrado de IN PARAM y su escritura como EPARAM exactamente como se muestra en la Figura 11.

La Figura 14 ilustra un segundo modelo soportado por el servidor en el cual el servidor no solo asegura la clave de operación DK*i* sino también el parámetro en sí. IN PARAM también se proporciona en el servidor, y solo las versiones encriptadas de DK*i* y IN PARAM se envían a la aplicación de transacción móvil para guardar en la base de datos encriptada.

Las Figuras 13 y 14 muestran solo escritura en la base de datos encriptada. El experto apreciará que la operación de lectura es inversa a la operación de escritura de la manera descrita anteriormente para las modalidades anteriores.

La Figura 15 ilustra un enfoque diferente soportado por el servidor. En este enfoque, el servidor produce una clave de uso único (SUK) y la almacena en la base de datos encriptada lista para utilizarse por la aplicación de transacción móvil como una clave de operación para asegurar una transacción de pago.

En este enfoque, el servidor implementa un algoritmo de derivación de clave de sesión usando el contador de secuencia de aplicación ASN como una entrada. El servidor ya ha utilizado funciones de identificación del usuario o del dispositivo informático móvil (tal como el PAN y/o la PSN de la cuenta de usuario asociada) para crear una clave maestra de tarjeta MK_{AC} de la Clave Maestra del Emisor para el cálculo de AC. MK_{AC} se utiliza para calcular el SUK con respecto al ASN para el cual se utilizará la clave en la aplicación de transacción móvil. Este SUK luego se cifra con la clave de transporte del usuario R como $ESUK = E_R(SUK)$, y se envía junto con el ASN a la aplicación de transacción móvil para su almacenamiento en la base de datos local encriptada.

La Figura 16 ilustra cómo la aplicación de transacción móvil usa registros que contienen un SUK encriptado para realizar una transacción de pago.

La aplicación de transacción móvil usa un valor ASN actual para buscar en la base de datos local la existencia de un SUK encriptado. Si tal clave existe en forma encriptada ESUK = E_R(SUK), la base de datos local la proporcionará a la aplicación de transacción móvil.

La aplicación de transacción móvil utilizará esta clave encriptada recuperada en el mecanismo DWB(E) en primer lugar para recuperar el SUK, aplicando el mecanismo de transformación SWB AES256-I con la clave R para descifrar ESUK. SUK puede utilizarse para calcular la AC de prueba de pago (criptograma de aplicación) utilizada bajo el estándar EMV (por ejemplo) en los datos de transacción recibidos de un terminal.

Las modalidades de una aplicación de transacción móvil descrita anteriormente se refieren generalmente al pago, y son particularmente útiles para un dispositivo informático móvil tal como un teléfono móvil que implementa protocolos de tarjeta sin contacto para permitir que el dispositivo informático móvil funcione como un dispositivo de pago. Este, sin embargo, no es el único contexto operacional disponible. Además del uso en protocolos de pago distintos de las transacciones con tarjeta sin contacto, las modalidades de la invención pueden utilizarse fuera del contexto del pago - por ejemplo, las modalidades pueden utilizarse para proporcionar una aplicación de viaje para la gestión segura de boletos electrónicos utilizados para interactuar con un sistema de puertas de boletos de una red de transporte. Las transacciones individuales en este caso son las interacciones entre la aplicación de viaje y las puertas individuales del sistema de puertas de boletos, y el uso de enfoques como se describe aquí impide la adquisición y clonación de boletos electrónicos u otros permisos de viaje.

Reivindicaciones

1. Un dispositivo informático móvil que tiene un procesador y una memoria, en donde el procesador se programa con una aplicación de transacción móvil (101), en donde:
la memoria comprende una base de datos local (102) para contener elementos de datos para uso por la aplicación de transacción móvil (101), en donde una entrada (43) en la base de datos local comprende un índice (44), un parámetro encriptado (46) para su uso por la aplicación de transacción móvil (101), y un parámetro adicional (45) asociado con la etapa de cifrado/descifrado para el parámetro cifrado para esa entrada;
en donde la aplicación de transacción móvil (101) se adapta para cifrar elementos de datos para su almacenamiento en la base de datos local (102) y para descifrar elementos de datos almacenados en la base de datos local (102) usando técnicas criptográficas de caja blanca.

2. Un dispositivo informático móvil de acuerdo con la reivindicación 1, en donde la aplicación de transacción móvil se adapta para utilizar criptografía de caja blanca estática y utiliza un algoritmo de derivación de clave en el cifrado y almacenamiento de datos en la base de datos local encriptada.

3. Un dispositivo informático móvil de acuerdo con la reivindicación 2, en donde el parámetro adicional en la entrada es un contador de secuencia de aplicación para indicar una transacción en la que se realizó una operación asociada con la entrada.

4. Un dispositivo informático móvil de acuerdo con la reivindicación 1, en donde la aplicación de transacción móvil se adapta para utilizar criptografía de caja blanca dinámica y utiliza un algoritmo de transporte de clave en el cifrado y almacenamiento de datos en la base de datos local encriptada.

5. Un dispositivo informático móvil de acuerdo con la reivindicación 4, en donde el parámetro adicional en la entrada es una clave encriptada para esa entrada.

6. Un dispositivo informático móvil de acuerdo con la reivindicación 4 o la reivindicación 5, en donde la aplicación de transacción móvil se comunica con un servidor adaptado para proteger uno o más parámetros utilizados por la aplicación de transacción móvil.

7. Un dispositivo informático móvil de acuerdo con cualquier reivindicación anterior, en donde la aplicación de transacción móvil se descarga al dispositivo informático móvil sin personalización del dispositivo informático móvil o su usuario, y en donde en la instalación o inicialización, la aplicación de transacción móvil se personaliza para el dispositivo informático móvil o su usuario.

8. Un dispositivo informático móvil de acuerdo con cualquier reivindicación anterior, en donde el dispositivo informático móvil se adapta para actuar como un dispositivo de pago y en donde la aplicación de transacción móvil es una aplicación de pago.

9. Dispositivo informático móvil de acuerdo con la reivindicación 8, en donde el dispositivo informático móvil se adapta para emular una tarjeta de pago sin contacto.

10. Un método para operar una aplicación de transacción móvil (101) en un dispositivo informático móvil, en donde el dispositivo informático móvil comprende un procesador adaptado para ejecutar la aplicación de transacción móvil (101) y una memoria que comprende una base de datos local (102) para contener elementos de datos para uso por la aplicación de transacción móvil (101), el método comprende:
identificar uno o más elementos de datos para su almacenamiento o recuperación desde la base de datos local (102); y también
encriptar el uno o más elementos de datos para su almacenamiento en la base de datos local (102) usando técnicas criptográficas de caja blanca, o
descifrar uno o más elementos de datos almacenados en la base de datos local (102) usando técnicas criptográficas de caja blanca;
en donde una entrada (43) en la base de datos local (102) comprende un índice (44), un parámetro encriptado (46) para uso por la aplicación de transacción móvil (101), y un parámetro adicional (45) asociado con la etapa de cifrado/descifrado para el parámetro encriptado para esa entrada.

11. El método de acuerdo la reivindicación 10, en donde la aplicación de transacción móvil utiliza criptografía de caja blanca estática y utiliza un algoritmo de derivación de clave en el cifrado y almacenamiento de datos en la base de datos local encriptada.

12. El método de acuerdo la reivindicación 10, en donde la aplicación de transacción móvil utiliza criptografía de caja blanca dinámica y utiliza un algoritmo de transportación de clave en el cifrado y almacenamiento de datos en la base de datos local encriptada.

13. El método de acuerdo con cualquiera de las reivindicaciones 10 a 12 comprende además:

descargar la aplicación de transacción móvil al dispositivo informático móvil sin personalización para el dispositivo informático móvil o su usuario; y
en la instalación o inicialización, personalizando la aplicación de transacción móvil para el dispositivo informático móvil o su usuario.

14. El método de acuerdo con cualquiera de las reivindicaciones 10 a 13, en donde el dispositivo informático móvil se adapta para actuar como un dispositivo de pago y en donde la aplicación de transacción móvil es una aplicación de pago.

15. El método de acuerdo con la reivindicación 14, en donde el dispositivo informático móvil se adapta para emular una tarjeta de pago sin contacto.

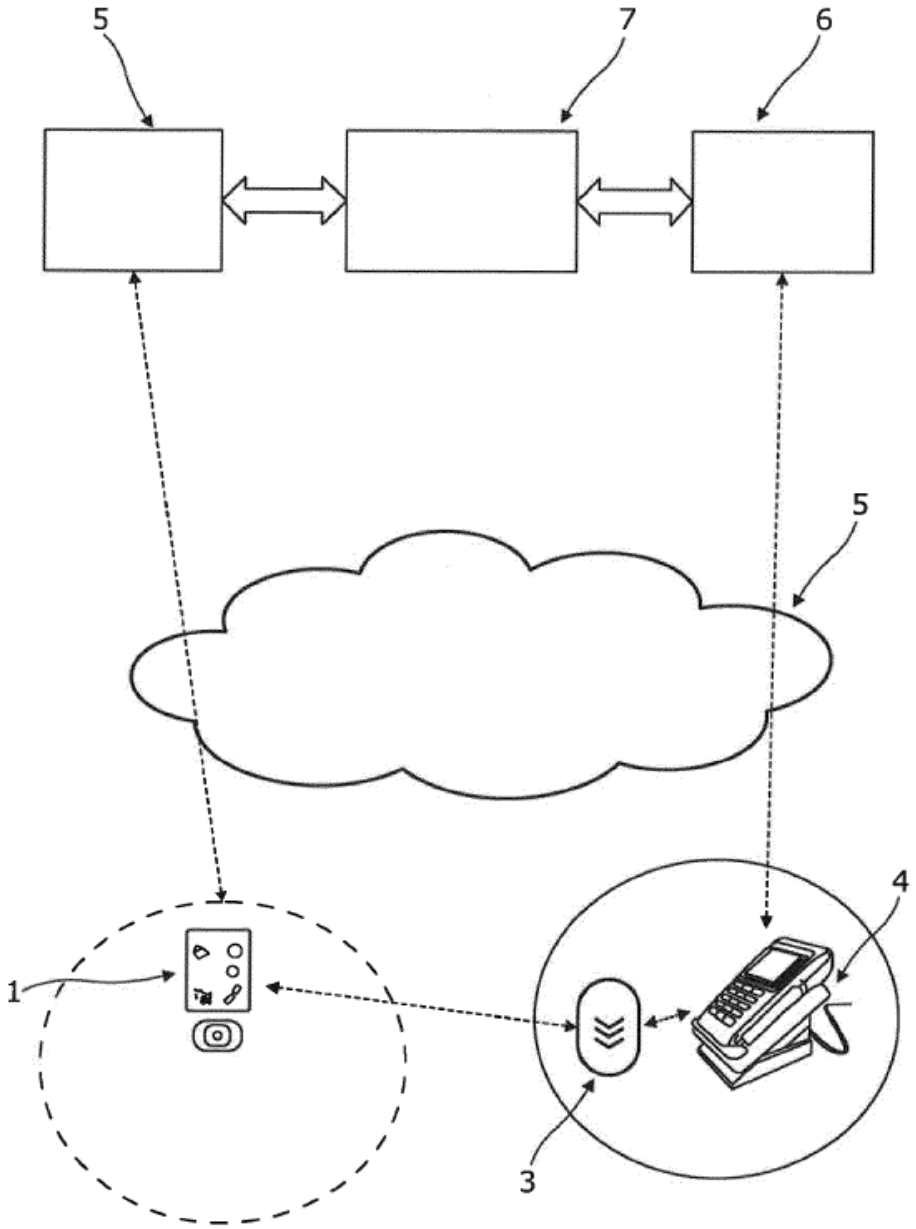


Figura 1

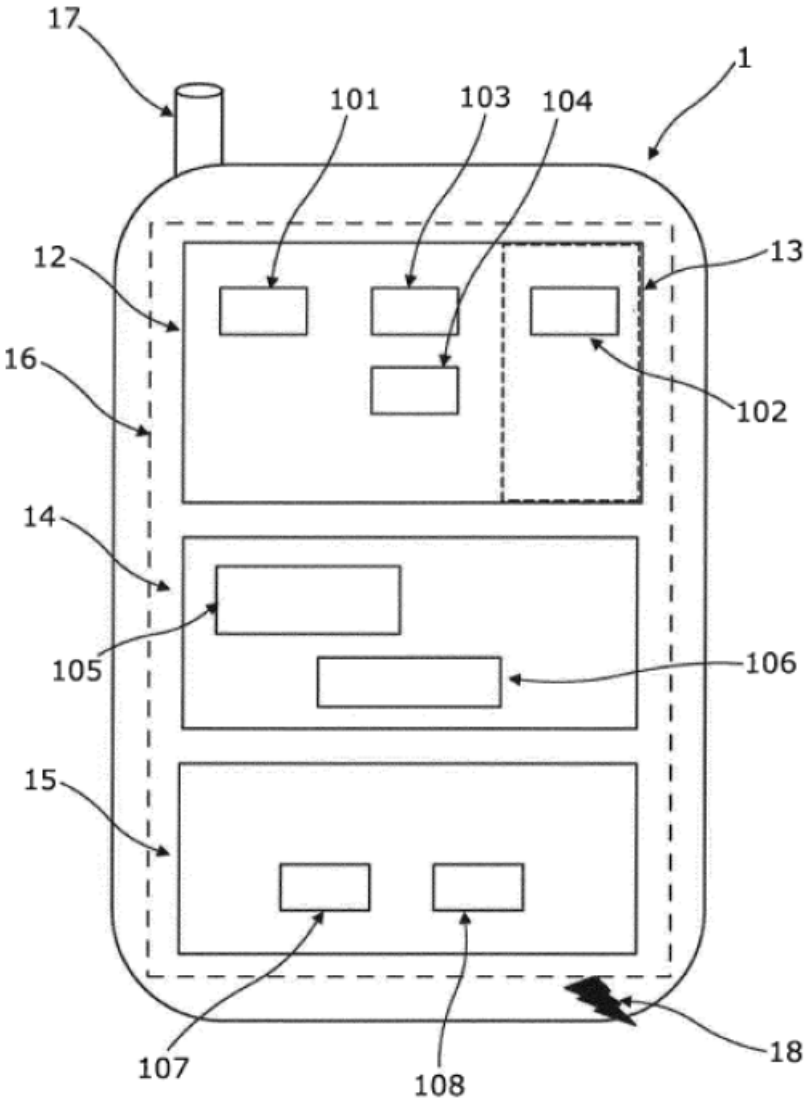


Figura 2

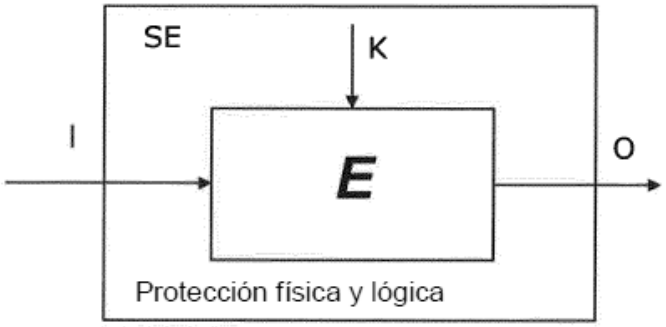


Figura 3A

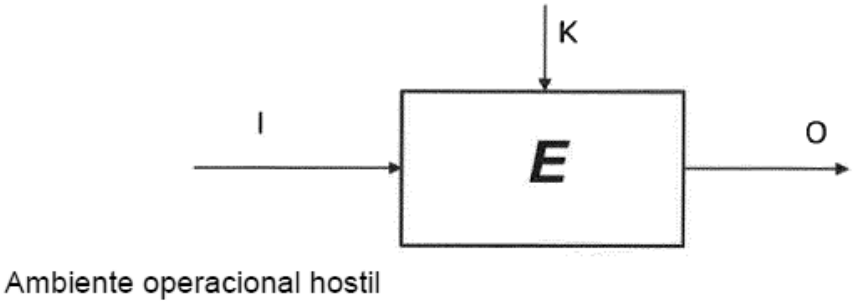
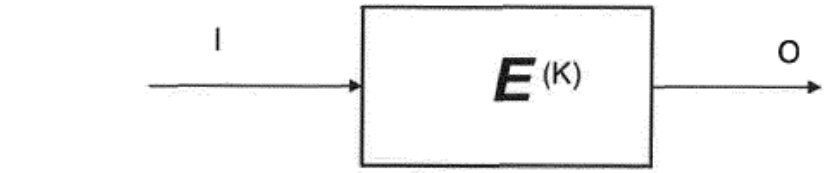
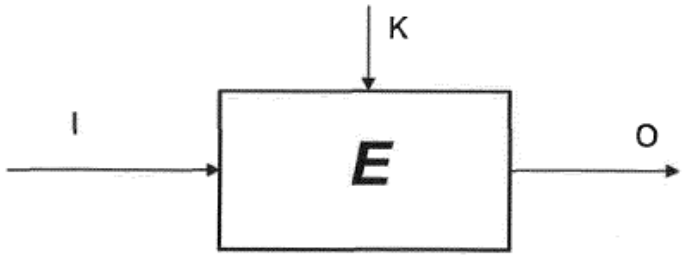


Figura 3B



Ambiente operacional hostil

Figura 3C



Protección lógica

Ambiente operacional hostil

Figura 3D

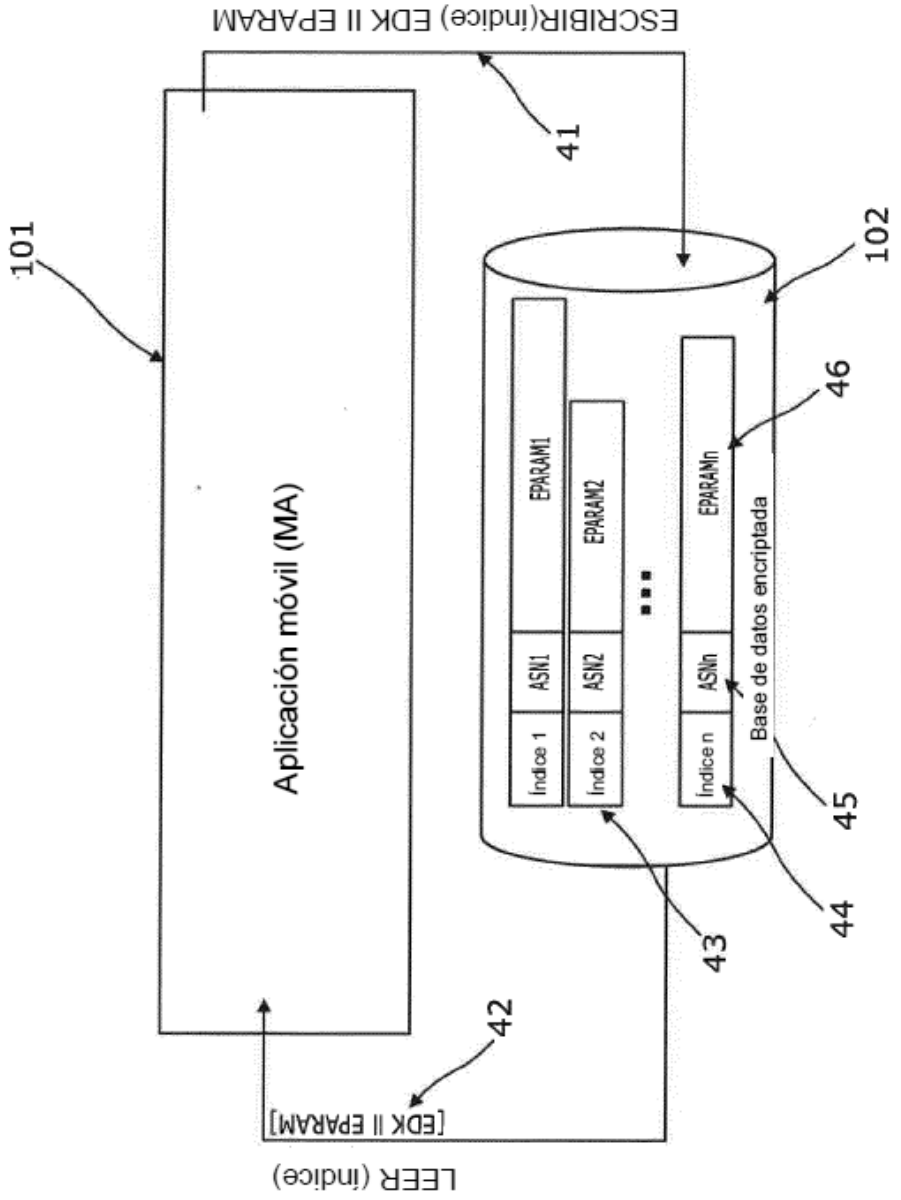

ESCRIBIR(índice) EDK || EPARAM
41
101
102
Aplicación móvil (MA)
EPARAM1
EPARAM2
EPARAMn
ASN1
ASN2
ASNn
Índice 1
Índice 2
Índice n
46
Base de datos encriptada
45
44
43
42
[EDK || EPARAM]
LEER (índice)

Figura 4

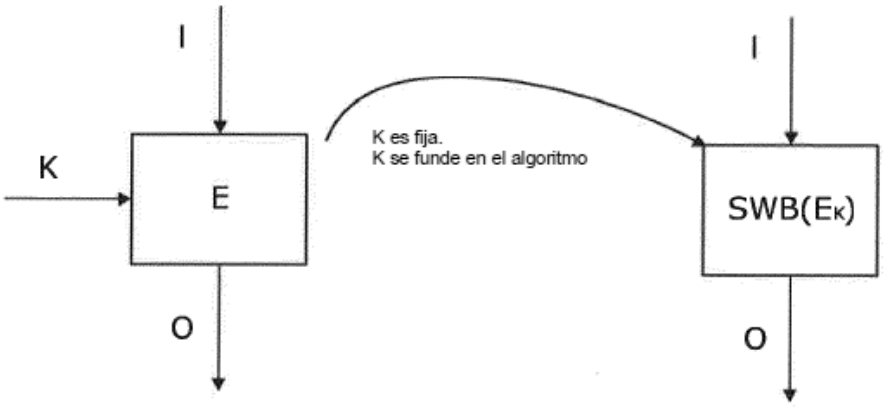


Figura 5A

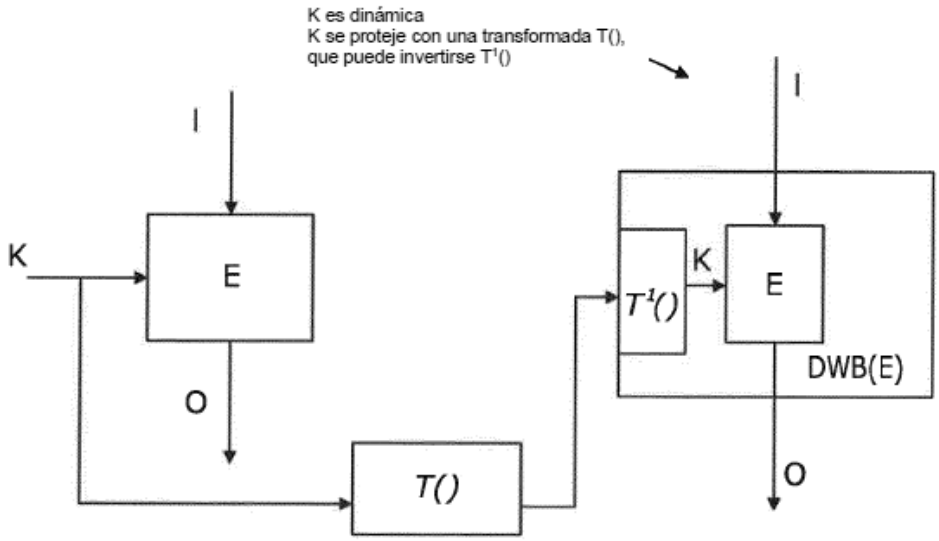


Figura 5B

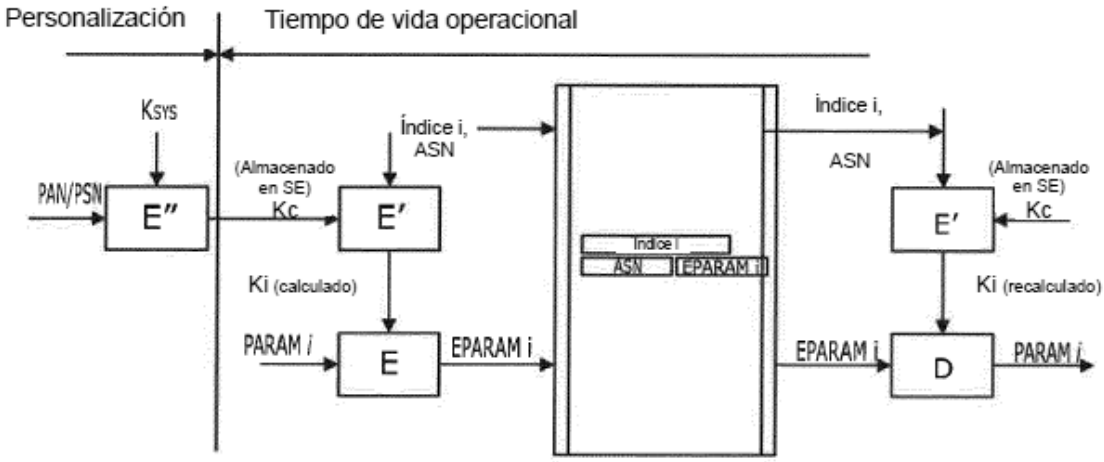


Figura 6

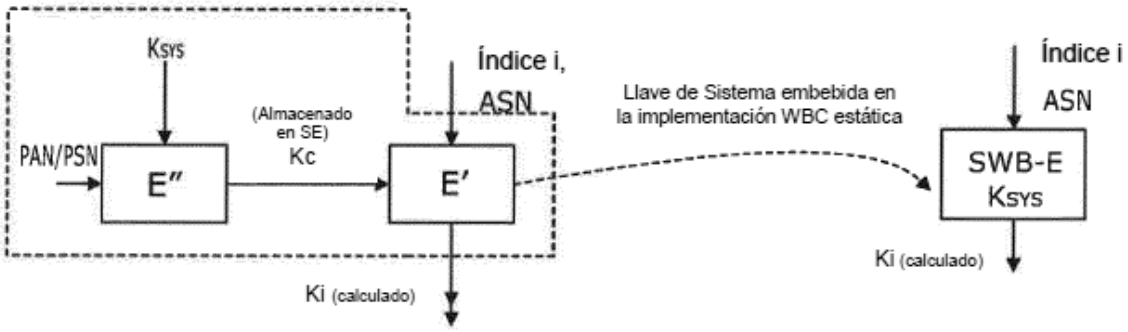


Figura 7

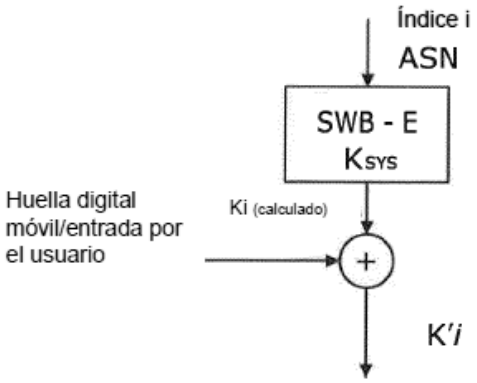


Figura 8

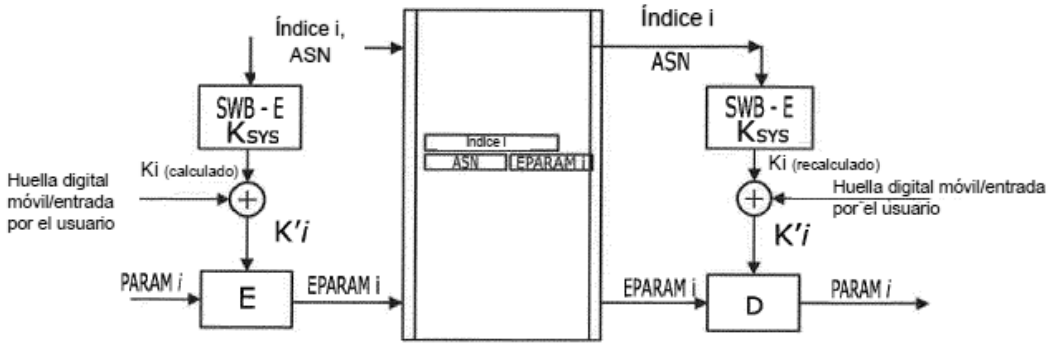


Figura 9

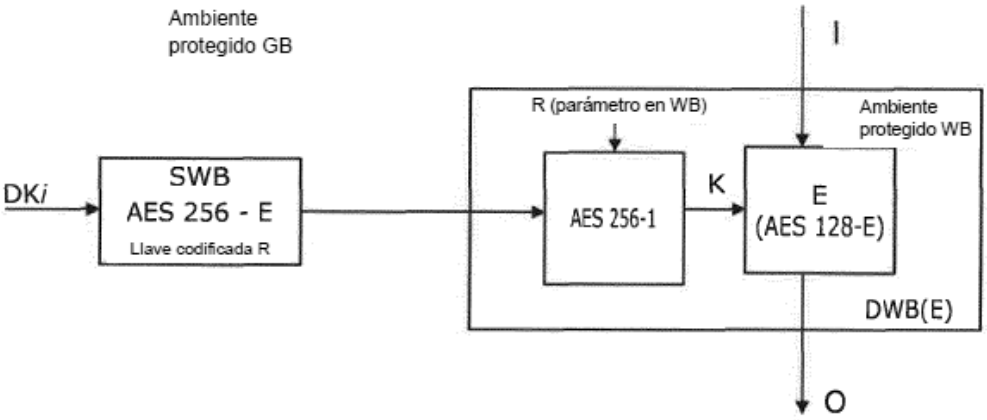


Figura 10

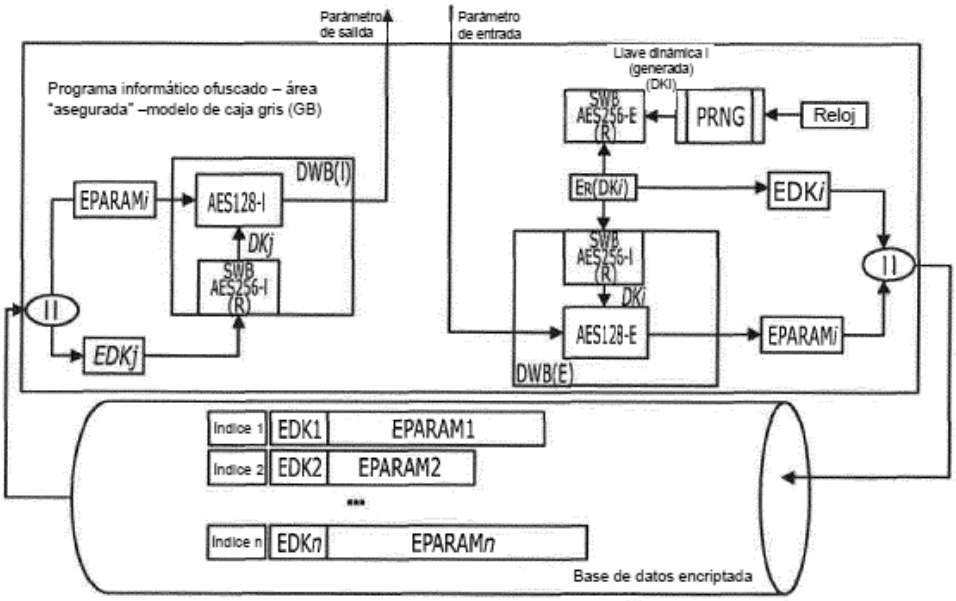


Figura 11

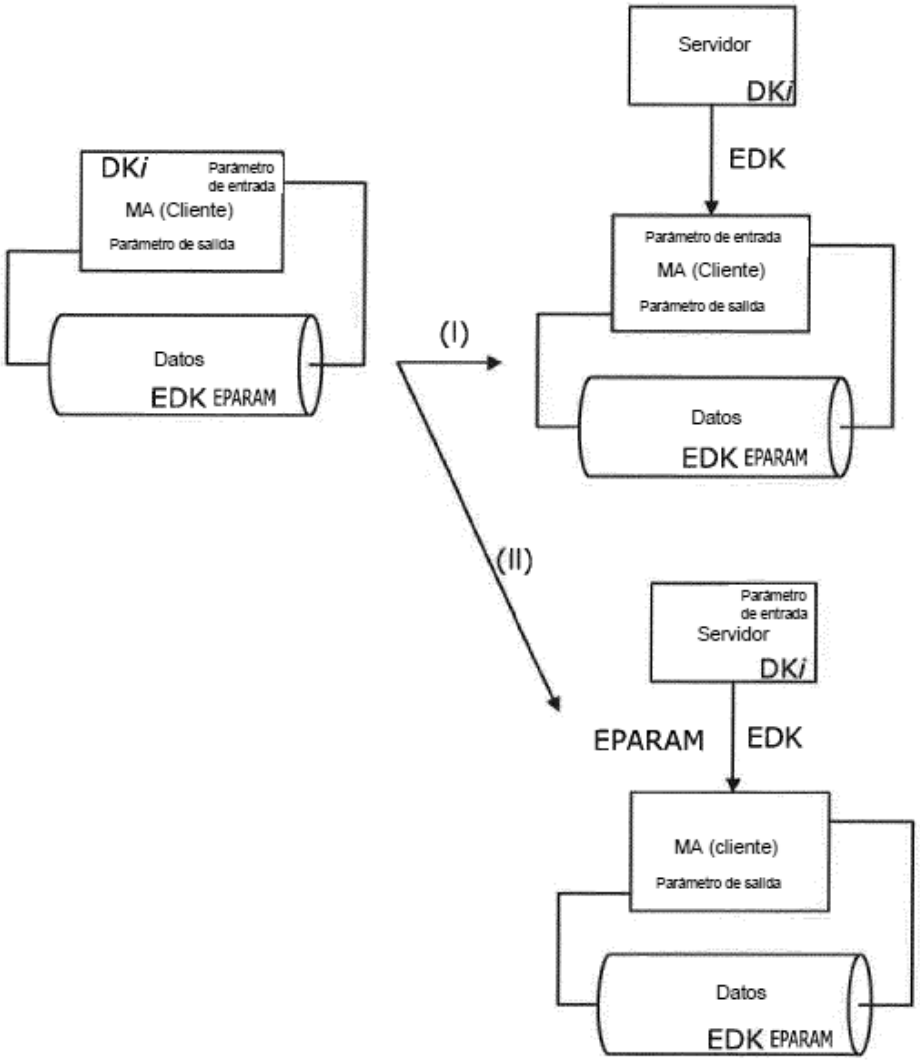

Servidor
DKi
EDK
DKi
Parámetro de entrada
MA (Cliente)
Parámetro de salida
Datos
EDK EPARAM
(I)
Parámetro de entrada
MA (Cliente)
Parámetro de salida
Datos
EDK EPARAM
(II)
Parámetro de entrada
Servidor
DKi
EPARAM
EDK
MA (cliente)
Parámetro de salida
Datos
EDK EPARAM

Figura 12

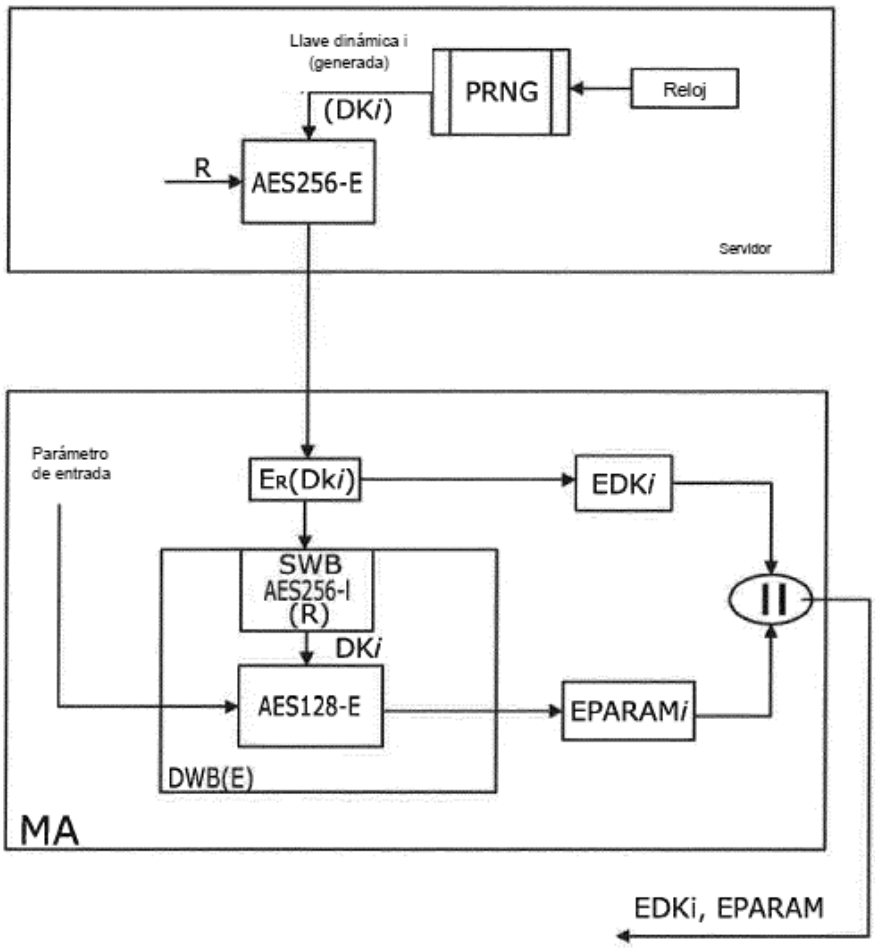

Llave dinámica i
(generada)
(DKi)
PRNG
Reloj
R
AES256-E
Servidor
Parámetro
de entrada
ER(Dki)
EDKi
SWB
AES256-I
(R)
DKi
AES128-E
EPARAMi
DWB(E)
MA
EDKi, EPARAM

Figura 13

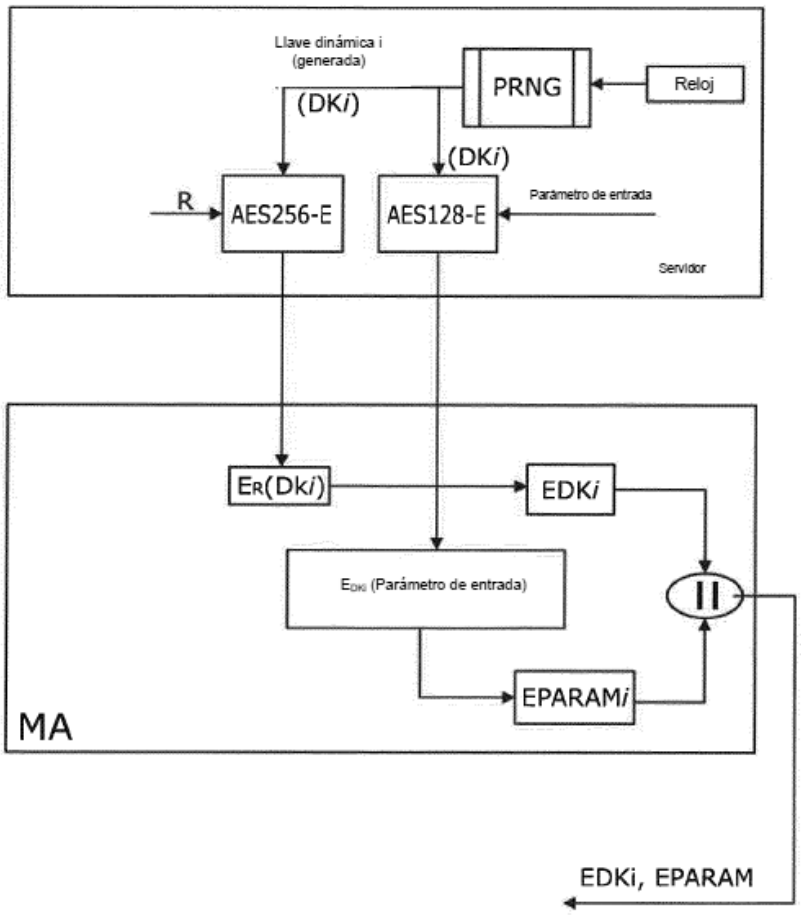

Llave dinámica i
(generada)
PRNG
Reloj
(DKi)
(DKi)
R
AES256-E
AES128-E
Parámetro de entrada
Servidor
ER(DKi)
EDKi
EDKi (Parámetro de entrada)
EPARAMi
MA
EDKi, EPARAM

Figura 14

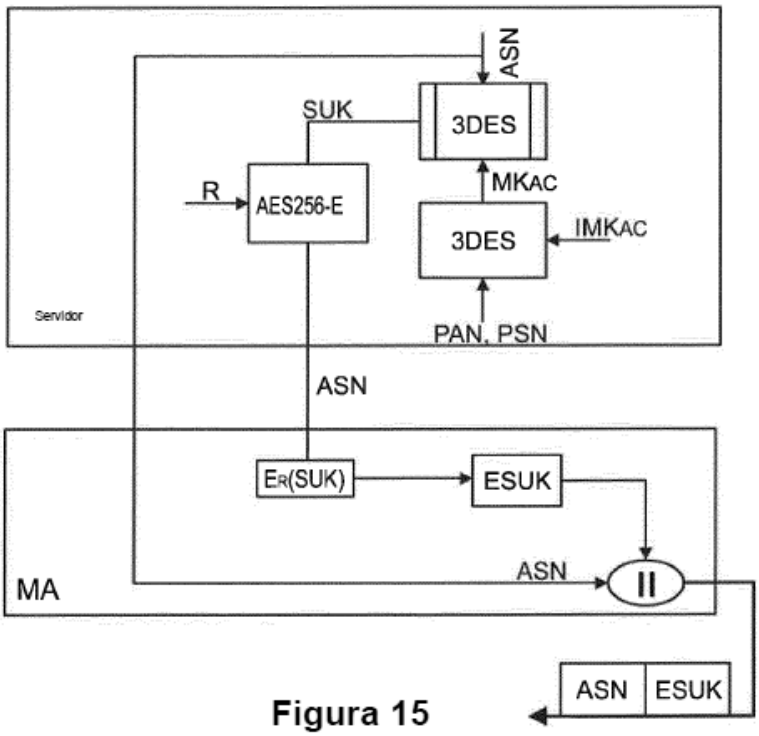


Figura 15

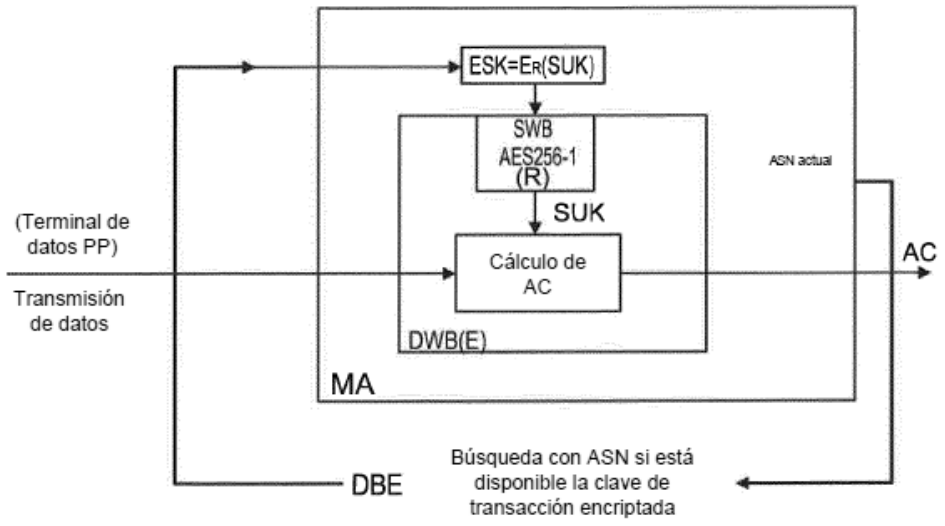


Figura 16