(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 632 795**

(51) Int. CI.:

H04L 9/08 (2006.01)
G07F 7/12 (2006.01)
G06Q 20/32 (2012.01)
H04L 9/32 (2006.01)
G06Q 20/38 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **02.04.2012 PCT/GB2012/050737**

(87) Fecha y número de publicación internacional: **11.10.2012 WO12136986**

(96) Fecha de presentación y número de la solicitud europea: **02.04.2012 E 12718316 (8)**

(97) Fecha y número de publicación de la concesión europea: **10.05.2017 EP 2695148**

(54) Título: **Sistema de pago**

(30) Prioridad:

05.04.2011 GB 201105765

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.09.2017

(73) Titular/es:

VISA EUROPE LIMITED (100.0%)
1 Sheldon Square
London W2 6TT, GB

(72) Inventor/es:

FISKE, STUART

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Sistema de pago

Campo de la invención

La presente invención se refiere al campo de los sistemas de pago electrónico y proporciona métodos de y sistemas para la autorización de una transacción de pago EMV entre un dispositivo de usuario y un terminal de punto de venta.

Antecedentes de la invención

Los sistemas de pago electrónico facilitan la transferencia electrónica de dinero desde una cuenta a otra a través de sistemas basados en ordenador. Para permitir un amplio uso de los sistemas de pago electrónico, se usan comúnmente tarjetas de circuitos integrados (ICC) aprovisionadas con aplicaciones de pago; estas proporcionan una alternativa al efectivo cuando se realizan compras. Una ICC es una tarjeta portátil que contiene circuitos integrados embebidos. Las ICC se emiten típicamente por instituciones financieras, conocidas comúnmente como bancos de emisión o emisores, a sus clientes. Se ejecuta en la ICC una aplicación de pago y contiene información en relación con la cuenta mantenida por el cliente con el banco emisor.

La Figura 1 ilustra los componentes de un sistema de pago electrónico convencional. Una ICC 102, emitida por el banco emisor 100, permite al usuario interactuar con un terminal 104 en un punto de venta (PoS) para realizar una compra de un comerciante. El terminal 104 notifica posteriormente los detalles de la transacción al banco del comerciante 106, comúnmente conocido como el banco adquiriente. La transacción se fija posteriormente entre el banco emisor 100 y el banco adquiriente 106, y se dispone la apropiada transferencia de fondos.

La ICC 102 puede interrelacionarse con el terminal del PoS 104 a través de tecnologías vía contacto o sin contacto. Las ICC con contacto son alimentadas por el terminal de PoS, y están de acuerdo con la serie de normas ISO/IEC 7810 e ISO/IEC 7816. Las tarjetas sin contacto pueden ser auto-alimentadas, o alimentadas inductivamente por el terminal del PoS y de acuerdo con las normas ISO/IEC 14443 o ISO/IEC 15693.

Antes de que se complete la transacción, el terminal del PoS 104 debe asegurarse de que la ICC 102 presentada es tanto genuina, como autorizada para completar la transacción. La autenticación de las ICC y la autorización de las transacciones se gestionan de acuerdo con protocolos de transacción, que aseguran la interoperabilidad de un intervalo de las ICC y los terminales de PoS.

Muchos sistemas de pago electrónico usan protocolos de transacción EMV (Europay®, Mastercard®, Visa®), tal como se define por ejemplo en las especificaciones EMV 4.2 o las especificaciones sin contacto EMV para Sistemas de Pago, que están públicamente disponibles y publicadas por EMVCo LLC. Se hace referencia a estos protocolos en el presente documento simplemente como “EMV”.

Para que una ICC pruebe su autenticidad al terminal de PoS, la ICC está equipada con un cierto número de parámetros de datos, tales como certificados únicos y claves secretas que permiten que tenga lugar la validación sin poner en riesgo el secreto de los datos. Estos parámetros de datos se conocen colectivamente como claves de pago.

Los circuitos integrados embebidos en las ICC aprovisionadas con aplicaciones de pago consisten típicamente en elementos de procesamiento y memoria resistentes a falsificación, que permiten que se almacenen en la tarjeta parámetros de datos secretos, tales como un cierto número de claves de pago descritas anteriormente, en tanto que se mantiene un alto grado de confianza de que los datos no pueden obtenerse externamente.

La resistencia a falsificación puede proporcionarse por el uso de un criptoprocesador seguro en la ICC, que almacena instrucciones de programas y datos en forma cifrada, descifrándolos solamente en el interior del procesador cuando se ejecutan. Adicionalmente, el criptoprocesador puede embeberse con el empaquetado que emplea medidas de seguridad físicas, por ejemplo haciendo que los datos sean borrados del almacenamiento si se sondean por una fuente externa. Este entorno de procesamiento resistente a falsificación se denomina comúnmente como un elemento seguro.

Recientemente, se han realizado intentos para incorporar la funcionalidad de tarjetas de pago en otros dispositivos. Notablemente, ha habido esfuerzos para desplegar aplicaciones de pago sobre dispositivos de usuario, tales como teléfonos móviles, equipados con tecnología inalámbrica de corto alcance, tal como una antena de Comunicaciones de Campo Cercano (NFC), para emular una tarjeta de pago sin contacto. El protocolo de comunicación NFC está normalizado en ISO/IEC 18092.

Sin embargo, como las tarjetas de pago estándar, estos dispositivos han requerido convencionalmente un elemento seguro para almacenar y procesar los datos secretos necesarios, y mantener el nivel de seguridad requerido para

asegurar el secreto de los datos. Los elementos seguros pueden embeberse como parte del hardware del dispositivo, sobre una tarjeta de almacenamiento extraíble tal como una tarjeta Secure Digital (SD), o, en el caso de un dispositivo de telefonía móvil, incorporado en la tarjeta del módulo de identidad de abonado (SIM). Otros métodos conocidos de proporcionar un elemento seguro han incluido la implementación de un elemento seguro externo accesible a través de una interfaz periférica, tal como una interfaz del Bus Serie Universal (USB), o a través del protocolo de comunicación inalámbrica Bluetooth®.

Sin embargo, hay varias razones por la que un elemento seguro puede no estar disponible para su uso por una aplicación de pago. En primer lugar, el dispositivo sobre el que se implementa la aplicación de pago puede no estar equipado con dicho elemento seguro (o una interfaz mediante la que pueda accederse a un elemento seguro externo). En segundo lugar, la aplicación de pago puede no tener permitido acceder al elemento seguro proporcionado, quizás debido a que la aplicación de pago se implementó en el dispositivo posteriormente al elemento seguro.

En el caso de un dispositivo de telefonía móvil, es posible entregar aplicaciones o actualizaciones a una SIM “por el aire” a través del uso de una herramienta de aplicación SIM (STK). Sin embargo, la provisión de aplicaciones en esta forma requiere la cooperación del operador de la red móvil y una SIM adaptada y un dispositivo de telefonía móvil, lo que no siempre es posible.

Por ello, es un objetivo de la presente invención proporcionar métodos mejorados para proporcionar funcionalidad de tarjeta de pago en un dispositivo de usuario, mientras se minimiza cualquier inconveniente para el usuario del dispositivo y sin que requiera modificación de la infraestructura EMV, o del hardware de PoS existente.

Se proporcionará ahora un breve sumario de los métodos convencionales relevantes para procesamiento de pagos electrónicos para ayudar a la comprensión de las realizaciones de la invención.

Autenticación de datos.

EMV proporciona para la autenticación de una ICC credenciales de tarjeta a través de una autenticación de datos fuera de línea. La autenticación de datos fuera de línea se lleva a cabo durante el procesamiento de la transacción de pago EMV, y se denomina fuera de línea dado que no hay comunicación entre el terminal de PoS y los bancos adquiriente o emisor. La finalidad de la autenticación de datos fuera de línea es verificar que la ICC está presentando un conjunto válido de credenciales, y usa un esquema de certificación de clave pública en capas. Un esquema de certificación usa firmas digitales para garantizar los datos firmados, y en particular una clave pública contenida dentro de él.

La firma se realiza basándose en un mecanismo de cifrado asimétrico, en el que los datos que se cifran, o “firman”, a través del uso de una clave privada que pueden descifrarse usando una clave pública correspondiente, sin requerir o implicar ningún conocimiento de la clave privada original. Por ello, puede asumirse con seguridad que los datos firmados que pueden descifrarse con una clave pública dada se han codificado por la clave privada correspondiente. EMV aprueba el uso del algoritmo RSA como un mecanismo de cifrado asimétrico adecuado, tal como se describe en R. L. Rivest, A. Shamir, y L. Adleman – “A method for obtaining digital signatures and public key cryptosystems”, Communications of the ACM, vol. 21, 1978, págs. 120-126, y propone el uso de Criptografía de Curva Elíptica para futuras especificaciones.

Como se ha mencionado anteriormente, el esquema de certificación utilizado en EMV es un esquema en capas, en el que se usa una clave obtenida a partir de un primer certificado para descifrar un segundo certificado, y así sucesivamente. Todos los datos necesarios para la verificación de datos fuera de línea se obtienen por el terminal en respuesta al envío de comandos READ RECORD a la ICC u otros comandos tales como GET PROCESSING OPTIONS (GPO). Los comandos READ RECORD se envían al inicio del procesamiento de la transacción o durante el procesamiento de la transacción y se usan para leer todos los parámetros de datos relativos a la transacción desde la ICC. Estos parámetros que se requieren durante el procesamiento de la transacción se listan en un Localizador de Archivo de Aplicación (AFL). El AFL es un archivo de datos almacenado en la ICC que lista todos los registros de datos almacenados en la ICC que puedan requerirse durante el procesamiento de la transacción.

En respuesta a la recepción de comandos READ RECORD u otros comandos (tal como el GPO anteriormente mencionado, la ICC envía todos los registros que se identifican en el AFL al terminal. Los registros relevantes para autenticación de datos fuera de línea incluyen un Índice de Clave Pública de la Autoridad de Certificación (CA), un Certificado de Clave Pública del Emisor, Número de Cuenta Primaria (PAN) y Datos de Aplicación Estática Firmados o un Certificado de Clave Pública ICC dependiendo del método de autenticación de datos fuera de línea que se esté empleando.

EMV proporciona varios métodos de autenticación de datos fuera de línea. Cuya elección depende de las capacidades tanto de la ICC como del terminal de PoS. El método más simple es la Autenticación Estática de Datos (SDA), que es para su uso con las ICC que no soportan la generación de firma digital. La generación de firma digital

es requerida por EMV para transacciones sin contacto; por lo tanto la SDA no está permitida para su uso con transacciones EMV sin contacto.

EMV también proporciona métodos que soportan generación de firma dinámica, entre los que la Autenticación Dinámica de Datos (DDA) es el más simple. Adicionalmente, EMV proporciona un método denominado DDA rápido (fDDA) que se optimiza para transacciones sin contacto, y un método denominado CDA, que combina DDA con la etapa posterior de Generación de Criptograma de Aplicación (descrito a continuación), para permitir que se completen ambas operaciones en paralelo.

La Figura 2 ilustra un diagrama de flujo de DDA de ejemplo de acuerdo con los protocolos de transacción EMV conocidos.

En la etapa 200, el terminal lee datos de aplicación desde la ICC mediante el envío de comandos READ RECORD, tal como se ha descrito anteriormente.

En la etapa 202, el terminal usa el Índice de Clave Pública de la CA para identificar qué Clave Pública de la CA se ha usado para firmar el Certificado de Clave Pública del Emisor, y por ello que Clave Pública de la CA correspondiente se requiere para descifrar el Certificado de Clave Pública del Emisor. La CA es una entidad criptográfica altamente segura que firma unas claves públicas del emisor para garantizar su autenticidad. La CA debe ser de confianza tanto para el banco emisor como para el banco adquiriente para proporcionar confianza en los datos firmados.

El terminal mantiene un almacén local de Claves Públicas de la Autoridad de Certificación, y usa el Índice de Clave Pública de la Autoridad de Certificación obtenido desde la ICC para identificar el apropiado a usar en relación con la aplicación de pago. Habiendo identificado la Clave Pública de CA apropiada, el terminal usa esto para descifrar el Certificado de Clave Pública del Emisor en la etapa 204. El descifrado se realiza de acuerdo con el mecanismo de recuperación apropiado para el esquema de cifrado que se usó para firmar el Certificado de Clave Pública del Emisor. Dado que EMV aprueba el uso del algoritmo RSA, el descifrado se realiza de acuerdo con los mecanismos de recuperación de RSA apropiados basándose en la clave pública obtenida.

Los datos contenidos en el certificado de clave pública del emisor incluyen una clave pública del emisor y datos asociados, tal como un Identificador de Emisor, Fecha de Expiración del Certificado, Número de Serie del Certificado, Longitud de la Clave Pública del Emisor, Longitud del Exponente de la Clave Pública del Emisor, y Resultado Criptográfico. Todos estos campos de datos se firman por la clave privada de CA, y por ello la validez de la información es garantizada por la CA.

En la etapa 206, el terminal realiza un cierto número de comprobaciones para determinar si el certificado de clave pública del emisor se descifró apropiadamente, y si la información descifrada es válida. En primer lugar el terminal, compara el contenido de la cabecera, cola y parámetros de datos de formato descifrados contra valores esperados conocidos. Se aplica entonces un algoritmo criptográfico la concatenación de los campos de datos en el Certificado de Clave Pública del Emisor (excluyendo el parámetro Resultado Criptográfico), la Clave Pública del Emisor restante y el Exponente de Clave Pública del Emisor. El resultado del algoritmo criptográfico se compara entonces con el valor del Resultado Criptográfico proporcionado en el Certificado de Clave Pública del Emisor.

Un algoritmo criptográfico, es una operación matemática de una dirección que se usa para generar un resultado de tamaño fijo basándose en una entrada de datos de tamaño grande o variable. El resultado depende de toda la entrada de datos, y es computacionalmente difícil determinar los datos de las entradas que producirían un resultado dado. El EMV recomienda el uso del Algoritmo Criptográfico Seguro (Secure Hash Algorithm (SHA-1)) como es se normaliza en ISO/IEC 10118-3.

El terminal comprueba entonces el Identificador del Emisor recuperado desde el Certificado de Clave Pública del Emisor contra las primeras 3-8 cifras del Número de Cuenta Primaria leída desde la ICC. El terminal comprueba también la fecha de expiración del Certificado de Clave Pública del Emisor (expresado en términos de un mes de expiración y un año de expiración) contra la fecha actual para asegurarse de que no ha pasado el último día del mes de expiración, y que el Certificado de Clave Pública del Emisor es aún válido.

Si cualquiera de estas comprobaciones falla, entonces el proceso de autenticación de datos fuera de línea ha fallado. Sin embargo, si se pasan todas estas comprobaciones, entonces el terminal ha obtenido y verificado la Clave Pública del Emisor, que se usa para descifrar el certificado de Clave Pública de la ICC en la etapa 208.

Los datos contenidos en el Certificado de Clave Pública de la ICC incluyen la Clave Pública de la ICC y credenciales de la aplicación de pago asociada, incluyendo el PAN, Fecha de Expiración del Certificado, Número de Serie del Certificado, Longitud de Clave Pública de la ICC, Longitud del Exponente de Clave Pública del ICC y Resultado Criptográfico. Todos estos campos de datos se firman por la Clave Privada del Emisor, y por ello la validez de la información es garantizada por el emisor, cuya identidad ha sido garantizada a su vez por la CA.

En la etapa 210, el terminal realiza un cierto número de comprobaciones para determinar si el Certificado de Clave Pública de la ICC se descifró apropiadamente, y si la información descifrada es válida. En primer lugar el terminal comprueba el contenido de la cabecera, cola y parámetros de datos de formato descifrados contra valores esperados conocidos.

El algoritmo criptográfico se aplica entonces a la concatenación de los campos de datos en el Certificado de Clave Pública de la ICC (excluyendo el Resultado Criptográfico), el Resto de Clave Pública de la ICC, el Exponente de Clave Pública de la ICC y un conjunto de datos estáticos a ser autenticados, que se compone de una selección de otros archivos de datos almacenados en la ICC y recuperados al inicio del procesamiento de la transacción, o durante el procesamiento de la transacción, usando el comando READ RECORD. El resultado del algoritmo criptográfico se compara entonces con el valor del Resultado Criptográfico proporcionado en el Certificado de Clave Pública de la ICC.

Los registros de datos que componen los datos estáticos a ser autenticados se indican en el AFL mediante un valor de etiqueta específico. Solo se procesan aquellos registros que están etiquetados como usados en la autenticación de datos fuera de línea. Los elementos de datos adicionales pueden identificarse como una Lista de Etiquetas de Autenticación de Datos Estática opcional contenida en la ICC. La inclusión de estos datos estáticos en la entrada criptográfica permite que estos parámetros de datos extra sean autenticados por un resultado criptográfico verificado.

El terminal comprueba entonces el PAN desde el Certificado de Clave Pública de la ICC contra el PAN tal como se ve desde la tarjeta ICC en respuesta al comando READ RECORD. También, se comprueba la Fecha de Expiración del Certificado de la ICC (expresado en términos de un mes de expiración y un año de expiración) contra la fecha actual para asegurar que no ha pasado el último día del mes de expiración, y que el Certificado de Clave Pública de la ICC es aún válido.

Si cualquiera de estas comprobaciones falla, entonces ha fallado el proceso de autenticación de datos fuera de línea. Sin embargo, si se pasan todas estas comprobaciones, entonces el terminal ha obtenido y verificado la Clave Pública de la ICC, que se usa entonces para confirmar que la ICC está equipada con la Clave Privada de ICC.

Esto se consigue dando instrucciones a la ICC para generar una firma digital mediante la firma de un conjunto de datos especificado usando la Clave Privada de ICC. El resultado se denomina Datos de Aplicación Dinámicos Firmados. Los datos que deben firmarse por la ICC se definen en una Lista de Objetos de Datos Dinámica (DDOL). La ICC puede contener una DDOL, pero si no, se proporciona una DDOL por el terminal. Algunos datos definidos en la DDOL deben proporcionarse por el terminal, y otros parámetros pueden leerse desde la ICC. Cualquier DDOL debe incluir el parámetro del Número Impredecible, que se genera por el terminal. La inclusión del número impredecible asegura que los datos a ser firmados no pueden ser predichos, y por lo tanto que los datos de Aplicación de Firma resultantes no pueden ser burlados mediante un precálculo del resultado.

En la etapa 212, el terminal solicita a la ICC aplicar su firma digital mediante el envío de un comando INTERNAL AUTHENTICATE. El comando INTERNAL AUTHENTICATE incluye un campo de datos que contiene los datos necesarios originados en el terminal que han de ser firmados por la ICC.

Los datos de Aplicación Dinámica Firmados se transmiten al terminal en la etapa 214. En la etapa 216, el terminal usa la Clave Pública de ICC obtenida previamente para descifrar los Datos de Aplicación Dinámica Firmados. Los datos contenidos en los Datos de Aplicación Dinámica Firmados incluyen los Datos Dinámicos y un Resultado Criptográfico.

De nuevo, en la etapa 218, el terminal realiza un número comprobaciones para determinar si se descifraron apropiadamente los Datos de Aplicación Dinámica Firmados, y si es válida la información descifrada. En primer lugar el terminal comprueba al contenido de la cabecera, cola y parámetros de datos de formato descifrados contra valores esperados conocidos.

Se aplica entonces un algoritmo criptográfico a la concatenación de los campos de datos en los Datos de Aplicación Dinámica Firmados (excluyendo el Resultado Criptográfico) y los datos dinámicos a ser autenticados. El resultado del algoritmo criptográfico se compara entonces con el valor del Resultado Criptográfico proporcionado en los Datos de Aplicación Dinámica Firmados.

Si cualquiera de estas comprobaciones falla, entonces ha fallado el proceso de autenticación de datos fuera de línea. Sin embargo, si se pasan todas estas comprobaciones, entonces el terminal ha verificado que la ICC tiene acceso a la Clave Privada de ICC, y el DDA tiene éxito.

Sí, alternativamente, se usa SDA, las etapas de verificación son las mismas tal como se muestra en la Figura 2 hasta la etapa 204, después de lo que se usa en su lugar la Clave Pública del Emisor para descifrar los Datos de Aplicación Estática Firmados. Los datos contenidos en los Datos de Aplicación Estática Firmados incluyen un Código de Autenticación de Datos y un Resultado Criptográfico. Todos estos datos se firman por la Clave Privada

del Emisor, y por ello la validez de la información es garantizada por el Emisor, cuya identidad se ha garantizado a su vez por la CA.

El terminal realiza de nuevo un cierto número de comprobaciones para determinar si los Datos de Aplicación Estática Firmados se descifraron apropiadamente, y si la información descifrada es válida. En primer lugar el terminal comprueba el contenido de la cabecera, cola y parámetros de datos de formato descifrados contra valores esperados conocidos.

Se aplica entonces un algoritmo criptográfico a la concatenación de los campos de datos en los Datos de Aplicación Estática Firmados, y al conjunto de datos estáticos a ser autenticado identificado por la AFL tal como se ha descrito anteriormente. El resultado del algoritmo criptográfico se compara con el campo de Resultado Criptográfico obtenido desde los Datos de Aplicación Estática Firmados. La inclusión de los datos estáticos en la entrada criptográfica permite que estos parámetros de datos sean autenticados por un resultado criptográfico verificado.

Si se usa CDA en lugar de DDA, entonces las etapas de verificación son las mismas que en la Figura 3 hasta la etapa 210, después de lo que el terminal solicita un Criptograma de Aplicación mediante el envío de un comando GENERATE AC a la ICC (tal como se define a continuación), pero también solicita que sea firmado con una firma CDA. Esto permite que la firma digital sea verificada al mismo tiempo que el procesamiento del Criptograma de Aplicación.

De acuerdo con algunas implementaciones del terminal de PoS, solo se proporciona soporte para autorización en línea, y la etapa de autenticación de datos fuera de línea puede omitirse opcionalmente dado que la transición siempre se enviará en línea para autorización y la responsabilidad de la autenticación puede pasarse también al banco emisor.

Generación del criptograma de aplicación

EMV proporciona autorización de transacción a través de la generación de criptogramas de aplicación. Dependiendo de qué opciones se usen desde varias especificaciones de EMV, hay varios mecanismos disponibles para la generación del criptograma se aplicación. La generación de criptogramas de aplicación se describirá en el presente documento según las especificaciones EMV 4.2, sin embargo estará claro para un experto en la materia que son también adecuados mecanismos alternativos. A todo lo largo del procesamiento de la transacción, el éxito o fallo de ciertas comprobaciones y acciones, tales como los descritos anteriormente con relación a la autenticación de datos fuera de línea, pueden registrarse en una cadena de Resultados de Verificación del Terminal (TVR).

Los TRV se revisan durante el Análisis de Acción del Terminal, y basándose en su contenido, el terminal toma la decisión preliminar acerca de si la transacción debería aprobarse fuera de línea, autorizarse en línea, o rechazarse. La aprobación fuera de línea comprende la decisión del terminal de que la transacción puede tener lugar sin pedir permiso expreso desde el Banco Emisor. La autorización en línea comprende el envío de detalles de la transacción al Banco Emisor para autorización antes de aprobar la transacción. En algunas circunstancias, el terminal rechazará la transacción fuera de línea, antes de pedir la autorización desde el Banco Emisor.

La decisión del apropiado curso de la acción a tomar por el terminal se realiza basándose en Códigos de Acción del Terminal (TAC) y Códigos de Acción del Emisor (IAC). Los TAC se programan dentro del terminal por el banco adquiriente, y definen las circunstancias bajo las que una traslación debería aprobarse fuera de línea, autorizarse en línea, o rechazarse. Los IAC se implementan dentro de la ICC por el banco emisor, y definen también un conjunto de circunstancias bajo las que una transacción debería aprobarse fuera de línea, autorizarse en línea o rechazarse. El terminal usa tanto los TAC como los IAC para tomar una decisión preliminar sobre cómo procesar la transacción.

La Figura 3 ilustra un diagrama de flujo del comando de Generación de Criptograma de Aplicación de ejemplo de acuerdo con los protocolos de transacción de EMV.

El flujo comienza en la etapa 300 comparando el contenido del TVR con los TAC almacenados en el terminal y los IAC recuperados desde la ICC. Basándose en la comparación, el terminal toma una decisión preliminar acerca de si la transacción debería aprobarse fuera de línea, autorizarse en línea, o rechazarse en la etapa 302.

Dependiendo del resultado de la decisión tomada en la etapa 302, el terminal solicita un tipo específico de Criptograma de Aplicación a ser generado mediante el envío de un comando GENERATE AC a la ICC. Si el terminal decide rechazar la transacción fuera de línea, el comando GENERATE AC solicita un Criptograma de Autenticación de la Aplicación (AAC) en la etapa 304. Si el terminal decide intentar autorizar la transacción en línea, el comando GENERATE AC solicita un Criptograma de Solicitud de Autorización (ARQC) en la etapa 306. Si el terminal decide aprobar la transacción fuera de línea, el comando GENERATE AC solicita un Certificado de Transacción (TC) en la etapa 308.

En respuesta al comando GENERATE AC enviado por el terminal, la ICC puede realizar su propia gestión de riesgos en la forma de Análisis de Acción de la Tarjeta. El análisis de acción de la tarjeta se realiza basándose en los

parámetros determinados por el emisor y almacenados en la ICC. El resultado del Análisis de Acción de la Tarjeta puede elegir solamente un método de autorización, el mismo que el determinado por el terminal o más estricto.

Si el terminal decide rechazar la transacción fuera de línea solicitando un AAC según la etapa 304, la ICC debe responder con AAC en la etapa 310. Cualquier otra respuesta desde la ICC provocará que el procesamiento de la transacción falle.

Si el terminal decide intentar enviar la transacción en línea para autorización por el banco emisor solicitando un ARQC según la etapa 306, como un resultado del Análisis de Acción de la Tarjeta en la etapa 312, la ICC puede decidir responder con un ARQC en la etapa 314 según solicitado, o elegir rechazar la transacción fuera de línea respondiendo con un AAC en la etapa 310. Una respuesta desde la ICC que comprenda un TC provocará que el procesamiento de la transacción falle.

Si el terminal decide permitir la transacción fuera de línea solicitando un TC según la etapa 308, como un resultado del Análisis de Acción de la Tarjeta en la etapa 312 la ICC puede decidir responder con un TC en la etapa 316 según solicitado, elegir enviar la transacción en línea para autorización por el banco emisor respondiendo con un ARQC en la etapa 314, o elegir rechazar la transacción respondiendo con un AAC en la etapa 310.

Si la ICC responde con un ARQC, el terminal intenta enviar ésta al banco emisor para autorización en la etapa 318. Si el resultado del procedimiento de autorización en línea es rechazar la transacción, el terminal solicita un AAC en la etapa 320 mediante el envío de un segundo comando GENERATE AC, y el AAC es devuelto por la ICC en la etapa 310. Si el resultado del procedimiento de autorización en línea es autorizar la transacción, el terminal solicita un TC en la etapa 322 mediante el envío de un segundo comando GENERATE AC, y el AAC es devuelto por la ICC en la etapa 316.

Alternativamente, si el procedimiento de autorización en línea no puede completarse, el terminal vuelve al modo por omisión tal como se define en el TAC/IAC, mediante el envío de un segundo comando GENERATE AC que o bien solicita un AAC según la etapa 320, que se devuelve por la ICC en la etapa 310, o bien un TC en la etapa 322, que se devuelve por la ICC en la etapa 316.

Una vez la ICC ha respondido con o bien un AAC o bien un TC según las etapas 310 o 316 respectivamente, se completa el flujo del comando de Generación del Criptograma de Aplicación.

Para responder a un comando GENERATE AC remitido por el terminal, la ICC debe producir un Criptograma de Aplicación. Un Criptograma de Aplicación se produce basándose en datos enviados a la ICC en el campo de datos del comando GENERATE AC. Los datos a ser usados se especifican en una Lista de Objetos de Datos de Gestión de Riesgos de Tarjeta (CDOL), que se almacena en la ICC. La ICC almacena dos CDOL, uno para su uso con el primer comando GENERATE AC enviado en una transacción dada, y el otro para ser usado si se envía un segundo comando GENERATE AC.

El cifrado de los datos de aplicación y la generación del criptograma de aplicación se preforma basándose en una Clave de Sesión de ICC de 16 bytes. Una Clave de Sesión de ICC es una clave única generada por la ICC que es válida solo para uso con una transacción. Cada Clave de Sesión de ICC se deduce de una Clave Maestra de ICC única de 16 bytes, implementada con seguridad sobre la ICC por el banco emisor, y un Contador de Transacción de Aplicación (ATC) de 2 bytes. El ATC se emplea como dato de diversificación, lo que asegura la variación entre las Claves de Sesión de ICC usadas en cada transacción.

La Figura 4 ilustra el proceso de deducir una Clave de Sesión de ICC a partir de una Clave Maestra de ICC 400 única de acuerdo con los protocolos EMV.

Se usa el ATC 402 para crear datos de diversificación izquierda 404 añadiéndole un valor de datos hexadecimal “F0” y rellenando los restantes 5 bytes con ceros. De modo similar, los datos de diversificación derecha 406 se generan añadiendo al valor ATC el valor de datos hexadecimal “0F” y rellenando los restantes 5 bytes con ceros.

La Clave de Sesión se genera en dos mitades mediante el uso del algoritmo Estándar de Descripción de Datos Triple (3DES). El 3DES se especifica en ISO/IEC 18033-3, y se usa para cifrar una entrada de 8 bytes en una salida de texto cifrado de 8 bytes usando una clave secreta de 16 bytes.

Los 8 bytes más a la izquierda de la clave de sesión 408 se generan mediante la aplicación del algoritmo 3DES 410 a los datos de diversificación izquierda 404, usando la Clave Maestra de ICC 400 como clave secreta. De modo similar, los 8 bytes más a la derecha de la clave de sesión 412 se generan mediante la aplicación del algoritmo 3DES 414 a los datos de diversificación derecha 406, usando la Clave Maestra de ICC 400 como la clave secreta.

Los 8 bytes más a la izquierda de la clave de sesión 408 y los 8 bytes más a la derecha de la clave de sesión 412 se concatenan entonces para formar la Clave de Sesión de ICC 416.

La Clave de Sesión de ICC puede usarse entonces para generar un criptograma de aplicación. Cómo se usa la clave de sesión para generar el criptograma aplicación es específico del sistema de pago que esté siendo implementado.

Si se selecciona CDA como el método para autenticación de datos fuera de línea (como se ha descrito previamente), el terminal solicitará criptogramas de aplicación a ser firmados por la firma digital de la ICC, permitiendo que la autenticación de datos fuera de línea se realice simultáneamente con las etapas descritas anteriormente.

Los comandos usados en la generación del criptograma de aplicación pueden diferir de los descritos anteriormente dependiendo de cuál de las opciones de entre las diversas especificaciones EMV se usa. Por ejemplo, en lugar de usar GENERATE AC, el procesamiento de pago requerido puede incorporarse en un comando alternativo, tal como el GPO.

La solicitud de patente de Estados Unidos US 2005/0156026 A1 describe la realización de transacciones de pago EMV de modo inalámbrico usando un terminal móvil.

La solicitud de patente de Estados Unidos US 2011/0038481 A1 describe un sistema de almacenamiento de claves jerárquico para circuitos electrónicos, y explica dos enfoques para mejorar la protección de las claves contra intentos de piratería, concretamente (1) usando un mecanismo de deducción de claves en el que solo se usan las claves deducidas de una clave maestra y (2) usando claves temporales transmitidas por un elemento distante.

Sumario de la invención

De acuerdo con realizaciones de la presente invención, se proporciona un método, aparato y software de ordenador para autorizar una transacción EMV de acuerdo con las reivindicaciones adjuntas.

Más específicamente, en un primer aspecto de la presente invención, se proporciona un método para autorizar una transacción de pago EMV entre un dispositivo de usuario y un terminal de punto de venta, siendo dicha transacción de pago EMV una que se autoriza como parte de la transacción de pago por un banco emisor, en el que dicho banco emisor mantiene datos indicativos de una Clave Maestra de ICC correspondiente a una aplicación de pago aprovisionada al dispositivo de usuario, teniendo la aplicación de pago un primer estado operativo en el que dicha aplicación de pago tiene permitido llevar a cabo dicha transacción de pago EMV, y un segundo estado operativo, diferente de dicho primer estado operativo, comprendiendo el método:

en respuesta a la recepción de una clave de sesión generada por dicho banco emisor basándose en dicha Clave Maestra de ICC, aprovisionar a dicha aplicación de pago con la clave de sesión, mediante lo que se configura dicha aplicación de pago en dicho primer estado operativo; y posteriormente en respuesta a la recepción de la solicitud de un criptograma de aplicación en la aplicación de pago desde el terminal de punto de venta, usar la aplicación de pago para realizar un proceso de autorización, comprendiendo el proceso de autorización las etapas de:

generar dicho criptograma de aplicación basándose en la clave de sesión recibida; y
transmitir el criptograma de aplicación generado al terminal de punto de venta para verificación del mismo por el banco emisor y autorización de la transacción de pago EMV.

Una aplicación de pago puede referirse a software configurado de modo que sea capaz de controlar la comunicación con un terminal de punto de venta de acuerdo con los protocolos de transacción EMV. Un dispositivo de usuario puede relacionarse con un dispositivo portátil electrónico que comprende hardware de ordenador. Un ejemplo de un dispositivo de usuario es un dispositivo de telefonía móvil, tal como un teléfono inteligente.

La clave maestra de ICC es una clave única asociada con la aplicación de pago, a partir de la que pueden deducirse las claves de sesión. Las claves de sesión son claves requeridas durante el procesamiento de la transacción EMV, y cada clave de sesión es válida para su uso solamente con una única transacción. Un criptograma de aplicación es un conjunto de datos cifrados usando una clave de sesión por una aplicación de pago. Un criptograma de aplicación es requerido por el terminal de punto de venta durante el procesamiento de una transacción EMV.

Al mantener la Clave Maestra de ICC en el banco emisor, al contrario que en la técnica anterior en la que la Clave Maestra de ICC se mantiene por la aplicación de pago, y mediante la autorización de transacciones basándose en una clave de sesión deducida de la misma, las realizaciones de la presente invención son capaces de reducir el riesgo asociado con un ataque exitoso sobre la aplicación de pago. Un ataque exitoso contra la aplicación de pago que almacena solo un número limitado de claves de sesión conduciría a credenciales de pago válidas solo para una única transacción, o un número limitado de transacciones, y por ello la efectividad de dicho ataque se reduce significativamente. Al reducir el riesgo asociado con un ataque exitoso sobre la aplicación de pago, las realizaciones de la presente invención facilitan la provisión de la aplicación de pago de tal manera que no requiera el uso de características de seguridad proporcionadas por un elemento seguro.

Preferentemente, el dispositivo de usuario comprende una primera parte de procesamiento y una segunda parte de procesamiento, comprendiendo la primera parte de procesamiento un primer entorno de aplicación dentro de un elemento seguro y una segunda parte de procesamiento que comprende un segundo entorno de aplicación externo al elemento seguro, y en el que la segunda parte de procesamiento comprende dicha aplicación de pago.

Una parte de procesamiento puede referirse a la combinación de componentes de computación convencionales, tales como una unidad de procesamiento central, una memoria de acceso aleatorio y una memoria solo de lectura. Un entorno de aplicación puede referirse a una vista lógica de una parte de procesamiento en la que puede ejecutarse una aplicación, compuesta por una combinación de instrucciones de software. Un elemento seguro puede proporcionar una parte de procesamiento y entorno de aplicación con características de seguridad de hardware adicionales, tales como resistencia a falsificación, que puede proporcionarse por medio del uso de un criptoprocesador seguro. Un ejemplo de un elemento seguro es el proporcionado por una tarjeta del Módulo de Identidad de Abonado (SIM) con respecto a un dispositivo de telefonía móvil.

Preferentemente, y en respuesta a un criterio predeterminado que es satisfecho, se aprovisiona una clave de sesión adicional a dicho dispositivo de usuario.

El criterio predeterminado puede comprender el número de claves de sesión sin usar en el dispositivo de usuario que cae por debajo de un cierto valor, enviando el dispositivo de usuario una solicitud de más claves de sesión o un período de tiempo predeterminado que transcurre desde la provisión de la última clave de sesión. La provisión de claves de sesión adicionales puede tener lugar a través de una red de comunicaciones de conmutación de paquetes tales como la Internet, una red de comunicaciones de conmutación de circuitos, tales como una red de telefonía móvil, o una combinación de ambas.

El dispositivo de usuario puede comunicar con el terminal de punto de venta usando tecnologías inalámbricas de corto alcance, por ejemplo un protocolo de comunicación de radiofrecuencia tal como la norma de Comunicaciones de Campo Cercano.

De acuerdo con aspectos adicionales de la presente invención se proporciona un terminal de usuario o dispositivo adaptado para procesar una transacción de pago EMV en conjunto con un terminal de punto de venta de acuerdo con el método anteriormente mencionado. Además se proporciona un programa de ordenador, o un conjunto de programas de ordenador que, cuando se ejecutan, hacen que un dispositivo de usuario realice el método anteriormente mencionado.

Aunque las realizaciones de la invención son adecuadas para entornos de procesamiento que incluyen un elemento seguro, se apreciará que las realizaciones de la invención pueden implementarse en un entorno que no tenga un elemento seguro, dado que la gestión y envío de claves de acuerdo con las realizaciones descritas es independiente de la existencia de un elemento seguro.

Serán evidentes características y ventajas adicionales de la invención a partir de la descripción que sigue de realizaciones preferidas de la invención, dadas solamente a modo de ejemplo, que se realiza con referencia a los dibujos adjuntos.

Breve descripción de los dibujos

La Figura 1 muestra los componentes de un sistema de pago electrónico convencional;
la Figura 2 muestra un diagrama de flujo de DDA de ejemplo de acuerdo con los protocolos de transacción EMV conocidos;
la Figura 3 muestra un diagrama de flujo del comando de Generación de Criptograma de Aplicación de acuerdo con los protocolos de transacción EMV conocidos;
la Figura 4 muestra el proceso de deducir una Clave de Sesión de ICC a partir de la Clave Maestra de ICC de acuerdo con los protocolos de transacción EMV conocidos;
la Figura 5 muestra componentes de un sistema de pago electrónico de acuerdo con una realización de la presente invención; y
la Figura 6 muestra un diagrama de bloques funcional de un dispositivo de usuario configurado de acuerdo con una realización de la presente invención; y
la Figura 7 muestra un diagrama de flujo del mensaje que ilustra un proceso de autorización en línea de acuerdo con una realización de la presente invención.

Descripción detallada de la invención

La Figura 5 ilustra los componentes de un sistema de pago electrónico de acuerdo con una realización de la presente invención.

El dispositivo de usuario 502 se aprovisiona con una aplicación de pago asociada con un banco emisor 500. El usuario del dispositivo 502 puede interactuar con un terminal 504 de un PoS a través del dispositivo de usuario 502

para realizar una compra desde un comerciante. El terminal de PoS 504 puede comunicar con el banco adquiriente 506, y la transacción se fija posteriormente entre el banco emisor 500 y el banco adquiriente 506, una vez que se ha dispuesto la transferencia de fondos apropiada.

De acuerdo con realizaciones de la invención, el dispositivo de usuario 502 puede comunicar con el terminal de PoS a través de una interfaz de comunicación sin contacto 508. Esta puede ser a través de un protocolo de comunicación inalámbrica de corto alcance, tal como NFC.

El dispositivo de usuario 502 es adicionalmente capaz de comunicar con el banco emisor 500 a través de la interfaz de comunicaciones 510. El medio de comunicación usado para comunicaciones entre el banco emisor 500 y el dispositivo de usuario 502 depende de las capacidades del dispositivo de usuario. El dispositivo de usuario 502 puede comunicar con el banco emisor 500 a través de Internet. Alternativamente, si el dispositivo de usuario 502 es un dispositivo de telefonía móvil, el dispositivo de usuario puede comunicar con el banco emisor 500 a través de la red de telefonía móvil.

La Figura 6 ilustra componentes de ejemplo de un dispositivo de usuario de acuerdo con realizaciones de la presente invención en las que el dispositivo de usuario comprende un dispositivo de telefonía móvil.

El dispositivo de usuario 600 comprende hardware de cómputo convencional que incluye una parte de procesamiento 602, memoria solo de lectura 604, memoria de acceso aleatorio 606, y otro hardware estándar tal como un controlador de entrada/salida, controlador de pantalla, etc. (no mostrados). El dispositivo de usuario 600 comprende también hardware de telefonía móvil específico que incluye la antena de telefonía 608, y la tarjeta SIM 610. La tarjeta SIM 610 constituye un entorno de procesamiento seguro en el dispositivo de usuario, también conocido como elemento seguro 612, e incorpora medidas de seguridad adicionales tales como resistencia a falsificación. Los componentes descritos anteriormente son accesibles para la parte de procesamiento 602 a través de una estructura de comunicación interna, tal como un bus del sistema 614. La operación e interacción de estos componentes es bien conocida en la técnica y por lo tanto no se cubrirá con detalle adicional en el presente documento.

El dispositivo de usuario 600 incluye también hardware de comunicaciones inalámbricas de corto alcance, incluyendo una antena inalámbrica de corto alcance 616, que puede usarse para realizar una comunicación sin contacto con el terminal de PoS, y puede ser una antena NFC.

Típicamente, en donde se han proporcionado antenas inalámbricas de corto alcance hasta el momento en dispositivos de telefonía móviles conocidos, han sido controladas por la SIM 610, a través de un canal de comunicación dedicado 618, separado del bus del sistema 614. El canal de comunicación dedicado 618, puede usar, por ejemplo, un Protocolo por Cable Simple para comunicación.

De acuerdo con realizaciones de la presente invención, la antena inalámbrica de corto alcance es accesible desde un área fuera del elemento seguro 612, de aquí en adelante conocida como el entorno de aplicación estándar 620, por ejemplo a través del bus del sistema 614.

El entorno de aplicación estándar 620 comprende también una aplicación de pago implementada en el dispositivo 600. La aplicación de pago puede instalarse en el entorno de aplicación estándar en el momento de la fabricación del dispositivo, o bajo la supervisión del banco emisor. Alternativamente la aplicación de pago puede instalarse por el usuario final del dispositivo. Un usuario final puede instalar la aplicación mediante la descarga de los archivos de instalación en el dispositivo de usuario, por ejemplo a través de Internet. Alternativamente un usuario puede instalar la aplicación mediante la descarga de los archivos de instalación primero en otro dispositivo, tal como en un ordenador personal, y cargando a continuación los archivos en el dispositivo de usuario, por ejemplo a través de una conexión USB. También alternativamente, un usuario puede obtener los archivos de instalación accediendo a un portal de aplicación en el dispositivo de usuario, tal como el Apple® AppStore™, o el Android Market™, que facilitan una descarga e instalación integradas de los archivos de aplicación. La descarga de los archivos de instalación facilitada por un portal de aplicación puede proporcionarse a través de una conexión de Internet disponible, o una provisión a través del aire (OTAP).

De acuerdo con realizaciones de la invención, las claves de pago, que son necesarias para el uso de la aplicación de pago, se proporcionan posteriormente a la instalación de la aplicación de pago, bajo el control del banco emisor. El equipamiento del dispositivo de usuario con las claves de pago en esta forma tiene el efecto de activar la aplicación de pago, asociándola de ese modo con una cuenta en el banco emisor, y permitiéndole llevar a cabo transacciones de pago EMV. Las claves de pago pueden almacenarse en un estado cifrado en una parte de memoria asociada con el entorno de aplicación estándar tal como en la memoria solo de lectura 604 o en una memoria persistente alternativa usando, por ejemplo, la norma de cifrado avanzado (AES). La clave usada para cifrar y descifrar esas claves de pago puede almacenarse en la memoria persistente en el dispositivo 600, o puede deducirse de una entrada recibida desde el usuario, tal como una palabra clave introducida en el dispositivo, una plantilla introducida en la pantalla o mediante la entrada de datos biométricos tales como un escáner de huellas o un reconocimiento de características faciales.

De acuerdo con algunas realizaciones de la invención, el entorno de aplicación estándar 620 puede comprender adicionalmente un entorno de ejecución de confianza (TEE), por ejemplo como se ha descrito por Global Platform Inc en “TEE System Architecture”, disponible en www.globalplatform.org, y otras aplicaciones relacionadas. Un TEE permite la ejecución segura de software o aplicaciones autorizadas mediante el almacenamiento y procesamiento de datos en una forma lógicamente aislada, provocando que varias aplicaciones estén lógicamente segregadas entre sí. Un TEE proporciona protección frente a ataques contra datos protegidos por software malicioso, pero no proporciona la protección física de un elemento seguro, tal como componentes de procesamiento y memoria a prueba de falsificación. En donde está disponible un TEE en el dispositivo 600, al menos una parte de la aplicación de pago puede almacenarse y/o ejecutarse en el TEE. Adicional o alternativamente, las claves de pago pueden almacenarse en el TEE. En donde las claves de pago se almacenan en un estado cifrado fuera del TEE, la clave que se usa para cifrar y descifrar las claves de pago puede almacenarse en el TEE.

Además, la aplicación de pago se configura de modo que la Clave Maestra de ICC no se mantiene localmente en el dispositivo de usuario, y en su lugar se mantiene por una entidad remota tal como el banco emisor. El dispositivo de usuario se aprovisiona con una Clave de Sesión de ICC, generada por el banco emisor basándose en la Clave Maestra de ICC. La Clave de Sesión de ICC puede generarse por el banco emisor de acuerdo con, por ejemplo, el método descrito anteriormente en relación con la Figura 4.

Se delega por lo tanto en el dispositivo de usuario tanto la responsabilidad como la capacidad para generar sus propias Claves de Sesión de ICC. Por ello un ataque con éxito contra los datos cifrados almacenados en el dispositivo de usuario dará como resultado que un atacante obtiene una Clave de Sesión de ICC que es válida solo para una única transacción, no para un gran número de transacciones como sería el caso si se obtuviera la Clave Maestra de ICC.

Dado que una Clave de Sesión de ICC es válida solamente para una única transacción, una vez que se ha usado para generar el (los) Criptograma(s) de Aplicación requeridos durante una transacción EMV simple, ya no es adicionalmente útil para la aplicación de pago. En algunas disposiciones, después de que se haya completado una transacción EMV, la Clave de Sesión de ICC se descarta, lo que puede implicar que el dispositivo de usuario purgue de su memoria la Clave de Sesión de ICC almacenada.

Una vez se ha usado la Clave de Sesión de ICC proporcionada para completar una transacción de pago, la aplicación de pago ya no está equipada para completar una transacción EMV, y de ese modo la aplicación de pago puede considerarse que está en un estado inoperativo. Esto es a diferencia del estado en el que está la aplicación de pago cuando no se usa la Clave de Sesión de ICC, cuando la aplicación de pago puede considerarse que está en un estado operativo. El descarte de la Clave de Sesión de ICC tal como se ha descrito anteriormente puede formar una condición de activación para la configuración de la aplicación de pago en el estado inoperativo.

Para impedir que la aplicación de pago quede permanentemente inoperativa una vez se ha usado la Clave de Sesión de ICC proporcionada, las realizaciones de la presente invención utilizan la interfaz de comunicaciones entre el dispositivo de usuario y el banco emisor para facilitar la provisión de Claves de Sesión de ICC adicionales.

Dado el secreto de la información que se transfiere desde el banco emisor al dispositivo de usuario, la comunicación debe llevarse a cabo de acuerdo con protocolos seguros. En una disposición el banco emisor y el dispositivo de usuario se comunican a través de Internet de acuerdo con un protocolo de mensajes seguro apropiado tal como el Protocolo de Transferencia de Hipertexto Seguro (HTTPS). En el caso del ejemplo actual, el banco emisor y el dispositivo de usuario pueden comunicar a través de la red de telefonía móvil, por ejemplo usando Acceso por Paquetes a Alta Velocidad (HSPA) y un protocolo de mensajes seguros apropiado, para recuperar las Claves de Sesión de ICC.

La recepción de una nueva Clave de Sesión de ICC en el dispositivo de usuario puede hacer que la Clave de Sesión de ICC previamente almacenada se sobrescriba. Alternativamente, si la Clave de Sesión de ICC previamente usada se descartó después de la finalización de una transacción, la clave de sesión recibida de nuevo puede simplemente almacenarse.

En algunas disposiciones, el dispositivo de usuario se configura para mantener un almacén de múltiples Claves de Sesión de ICC para reducir la frecuencia con la que deben aprovisionarse las Claves de Sesión de ICC al dispositivo de usuario. Esto permite al usuario completar múltiples transacciones sin requerir un número correspondiente de instancias de comunicación entre el dispositivo de usuario y el banco emisor. Esto es particularmente ventajoso si se interrumpe la conexión entre el dispositivo de usuario y el banco emisor, dado que el usuario puede proseguir con varias transacciones durante este periodo. Cuando el dispositivo de usuario mantiene un almacén de múltiples claves de sesión de ICC, una clave de sesión de ICC usada puede descartarse tal como se ha descrito anteriormente, marcarse como usada y por lo tanto no disponible para su uso en transacciones futuras, o simplemente eliminarse de un índice mantenido de Claves de Sesión de ICC no usadas.

La provisión de una nueva Clave de Sesión de ICC puede activarse por un cierto número de diferentes condiciones. En primer lugar, el dispositivo de usuario puede supervisar el número de Claves de Sesión de ICC no usadas

almacenadas en el dispositivo de usuario, y solicitar una nueva Clave de Sesión de ICC cuando todas las Claves de Sesión de ICC disponibles se hayan usado. En segundo lugar, el dispositivo de usuario puede anticipar el agotamiento de las Claves de Sesión de ICC disponibles, y solicitar una nueva Clave de Sesión de ICC cuando el número de Claves de Sesión de ICC disponibles cae por debajo de un cierto umbral. Este método evita la situación en la que se interrumpe el canal de comunicación entre el dispositivo de usuario y el banco emisor cuando se usó la última Clave de Sesión de ICC, dejando al dispositivo de usuario sin ninguna Clave de Sesión de ICC válida para un procesamiento de transacción posterior.

Adicionalmente, pueden aprovisionarse nuevas Claves de Sesión de ICC al dispositivo por el banco emisor sin requerir o que se realice una solicitud por parte del dispositivo de usuario. El banco emisor puede determinar el número de las Claves de Sesión de ICC que se han usado cada vez que se envía una transacción en línea para autorización explícita por el emisor, y decide en consecuencia si deberían aprovisionarse Claves de Sesión de ICC adicionales. De acuerdo con algunas disposiciones, el banco emisor puede aprovisionar periódicamente nuevas Claves de Sesión de ICC al dispositivo de usuario, lo que se describirá con detalle adicional a continuación.

El emisor puede mantener un registro de cuando se ha aprovisionado cada Clave de Sesión de ICC al dispositivo de usuario para determinar cuánto tiempo hace que se ha aprovisionado una Clave de Sesión de ICC dada. Si la transición se envía en línea para autorización, el emisor es capaz de limitar la vida útil efectiva de las Claves de Sesión de ICC aprovisionadas mediante el rechazo de la autorización de transacciones que usen Claves de Sesión de ICC que se hayan aprovisionado al dispositivo de usuario antes de un cierto momento. En algunas disposiciones, el emisor puede utilizar una cantidad de tiempo de umbral cuando se determina si autorizar una transacción, por ejemplo mediante el rechazo de autorizaciones de transacciones que usan un ARQC codificado usando una Clave de Sesión de ICC que se aprovisionó antes de una fecha definida por la cantidad de umbral. Puede hacerse referencia también a la cantidad de tiempo de umbral usada por el emisor cuando se determina si autorizar una transacción como una vida útil de las Claves de Sesión de ICC, desde que una Clave de Sesión de ICC se almacena en el dispositivo de usuario durante más tiempo que esta cantidad de umbral no será aceptada para cada autorizaciones en línea.

El banco emisor puede supervisar la cantidad de tiempo que ha transcurrido desde la provisión de una Clave de Sesión de ICC previamente aprovisionada y aprovisionar una nueva Clave de Sesión de ICC para el dispositivo de usuario en respuesta a la cantidad de tiempo que excede la cantidad de umbral. Alternativamente, el banco emisor puede anticipar la cantidad de tiempo que ha transcurrido desde la provisión de una Clave de Sesión de ICC previamente aprovisionada que exceda la cantidad de umbral y aprovisionar una nueva Clave de Sesión de ICC al dispositivo de usuario antes de que haya pasado el umbral. Como se ha hecho notar anteriormente, en el caso en el que el dispositivo de usuario anticipe el agotamiento de las Claves de Sesión de ICC disponibles, esto tiene la ventaja de evitar la situación en la que el canal de comunicación entre el dispositivo de usuario y el banco emisor se interrumpe en el momento en el que ha transcurrido el umbral, lo que dejaría en caso contrario al dispositivo de usuario sin una Clave de Sesión de ICC que usar en transacciones posteriores.

En otras disposiciones el dispositivo de usuario, o más específicamente la aplicación de pago, puede supervisar la cantidad de tiempo que ha transcurrido desde que se provisionó la última Clave de Sesión de ICC para detectar cuándo la cantidad de tiempo sobrepasa un valor de umbral localmente mantenido, y solicitar en respuesta una o más nuevas Claves de Sesión de ICC desde el banco emisor. Este valor de umbral local puede ser el mismo que el valor usado en el banco emisor, o configurarse para ser más corto, para evitar la situación descrita anteriormente en la que el dispositivo de usuario puede quedarse sin una Clave de Sesión de ICC válida para su uso en transacciones posteriores.

Una nueva Clave de Sesión de ICC recibida en respuesta a una Clave de Sesión de ICC previamente aprovisionada que se acerca o excede su vida útil, puede sobrescribir la Clave de Sesión de ICC previamente aprovisionada para asegurar que solo se usan Claves de Sesión de ICC que no han excedido su vida útil en el procesamiento de transacción posterior. En algunas disposiciones, la aplicación de pago puede descartar Claves de Sesión de ICC que hayan estado almacenadas en el dispositivo de usuario durante más tiempo que un valor de tiempo de umbral local. En disposiciones alternativas, las Claves de Sesión de ICC pueden mantenerse incluso después de que haya pasado el umbral local, para su uso en transacciones fuera de línea.

Para impedir que se rechacen por el emisor transacciones genuinas, el banco emisor puede aprovisionar al dispositivo de usuario con nuevas Claves de Sesión de ICC basándose en la cantidad de tiempo de umbral descrito anteriormente, así como o en lugar de los criterios previamente descritos.

En algunas disposiciones las Claves de Sesión de ICC pueden cifrarse y almacenarse de modo que queden inaccesibles para la aplicación de pago sin una entrada específica desde el usuario. En esta forma, las Claves de Sesión de ICC pueden ponerse a disposición de la aplicación de pago de una en una y tiene la ventaja de permitir que se implemente un nivel de seguridad extra en el dispositivo de usuario forzando al usuario a proporcionar la clave de cifrado, por ejemplo en la forma de una palabra clave, antes de liberar una Clave de Sesión de ICC para que quede disponible para la aplicación de pago. Esta disposición tiene la ventaja adicional también de requerir que cualquier ataque realizado contra las claves de pago cifradas almacenadas en el dispositivo de usuario descifre dos

partes de datos cifradas por separado, comprendiendo una las Claves de Sesión de ICC almacenadas, y comprendiendo la otra las claves de pago restantes. El descifrado de una Clave de Sesión de ICC y proporcionarla a la aplicación de pago en esta forma tiene el efecto de configurar la aplicación de pago en el estado operativo, permitiéndole llevar a cabo una transacción EMV.

La Figura 7 ilustra un diagrama de flujo de un mensaje para autorizaciones en línea de acuerdo con una realización de la presente invención. El proceso se inicia con el terminal de PoS 504 realizando un Análisis de Acción del Terminal (702) para determinar cómo autorizar la transacción. Cuando se completa el Análisis de Acción del Terminal el terminal de PoS 504 envía un comando GENERATE AC al dispositivo de usuario en la etapa 704. Para que se autorice una transacción en línea, el terminal 504 debe solicitar o bien un TC o bien un ARQC. En respuesta a la recepción del comando GENERATE AC, el dispositivo de usuario realiza un Análisis de Acción de Tarjeta en la etapa 706 y responde con un Criptograma de Aplicación en la etapa 708, que en este caso se supone que es un ARQC. Se genera un Criptograma de Aplicación basándose en la Clave de Sesión de ICC anteriormente mencionada y en datos específicos de la transacción. En respuesta a la recepción del Criptograma de Aplicación, el terminal identifica el tipo de Criptograma de Aplicación enviado por el dispositivo de usuario en la etapa 710 y dirige la ARQC al emisor en la etapa 712 para autorización de la transacción.

El emisor examina entonces el ARQC en la etapa 714 para tomar una decisión de si autorizar la transacción. Opcionalmente, el emisor puede identificar qué Clave de Sesión se usó para generar el ARQC, determinar la cantidad de tiempo que ha pasado desde que se aprovisionó la Clave de Sesión de ICC al dispositivo de usuario, y tomar la decisión de si autorizar la transacción en base a si la cantidad de tiempo excede la cantidad de umbral anteriormente mencionada.

El emisor informa de su decisión al terminal de PoS en la etapa 716, y basándose en esa decisión el terminal de PoS solicita un segundo Criptograma de Aplicación al dispositivo de usuario en la etapa 720. Si el emisor decidió rechazar la transacción, el terminal solicita un AAC desde el dispositivo de usuario. Si el emisor decidió autorizar la transacción, el terminal solicita un TC desde el dispositivo de usuario. En respuesta a la recepción de la solicitud de la etapa 720, el dispositivo de usuario genera un segundo Criptograma de Aplicación en la etapa 722, y envía éste al terminal en la etapa 724. El Criptograma de Aplicación se almacena por el terminal en la etapa 726, y se completa el proceso de autorización.

Por ello, realizaciones de la presente invención son capaces de restringir la capacidad de uso de las claves de pago almacenadas en el dispositivo de usuario no solamente en base a un número de usos, sino también a una cantidad de tiempo.

Como se ha explicado previamente, la viabilidad de una aplicación de pago se basa en el mantenimiento de la confidencialidad de un cierto número de claves de pago. Convencionalmente, las claves de pago se implementan en el ICC en el momento de la emisión, y se fijan durante la vida útil de la aplicación de pago, que está típicamente en la zona de los tres años. Debido al uso del elemento seguro en métodos convencionales, puede suponerse con seguridad que las claves de pago no quedarán comprometidas dentro de la vida útil de la aplicación de pago.

Las aplicaciones de pago implementadas en un entorno de aplicación estándar, tal como se contempla en realizaciones de la presente invención, no se benefician de las medidas de protección mejoradas que puede proporcionar un elemento seguro para almacenamiento y procesamiento de las claves de pago. Las claves de pago se almacenan dentro del entorno de aplicación estándar, por ejemplo en la ROM u otra parte de memoria persistente, y se cifran para ayudar a protegerlas contra ataques realizados contra el dispositivo de usuario con la intención de comprometer las claves de pago. Alternativamente, para dispositivos que incluyen un TEE, las claves de pago pueden almacenarse en el TEE (tanto cifradas como sin cifrar).

Aunque el cifrado de las claves de pago proporciona un cierto nivel de protección contra estos ataques, esto no es equivalente al nivel de protección proporcionado por un elemento seguro. En particular, los datos almacenados en un entorno de aplicación estándar son susceptibles de ataques tales como ataques de desbordamiento de memoria intermedia, modificación del sistema operativo e intrusión física, contra los que es inmune un elemento seguro. En donde las claves de pago se almacenan en un TEE, se proporciona un grado más alto de protección de software, pero las claves de pago permanecen vulnerables a intrusión física.

Sin embargo, limitando o restringiendo la utilidad de una o más de las claves de pago proporcionadas, el riesgo asociado con un ataque exitoso sobre los datos cifrados puede reducirse a un nivel aceptable.

El método proporcionado por la presente invención para limitar la utilidad de una o más de las claves de pago se refiere a la Clave Maestra de ICC utilizada en la generación de las Claves de Sesión de ICC para el proceso de Generación del Criptograma de Aplicación descrito anteriormente. Convencionalmente, en donde se proporciona la Clave Maestra de ICC dentro de la aplicación de pago, la aplicación de pago está equipada para generar Claves de Sesión de ICC según se requiera. La especificación EMV 4.2 limita el número de las Claves de Sesión de ICC que pueden generarse por una Clave Maestra de ICC a 65535, pero no proporciona ningún método para limitar la utilidad de la Clave Maestra de ICC más allá de este nivel en una forma que pueda limitar suficientemente el riesgo de un

ataque con éxito contra las claves de pago. Sin embargo, manteniendo la Clave Maestra de ICC en el banco emisor, y configurando la aplicación de pago con un número limitado de Claves de Sesión de ICC, las realizaciones de la presente invención reducen el riesgo planteado por un ataque con éxito.

Adicionalmente, limitando la vida útil de las Claves de Sesión de ICC, las realizaciones de la invención son capaces de reducir adicionalmente el riesgo asociado con un ataque con éxito sobre las claves de pago. Una forma común de ataque contra datos cifrados es conocida como un ataque por fuerza bruta. Un ataque por fuerza bruta implica la comprobación de modo sistemático de un gran número de posibles claves de cifrado con la intención de eventualmente descubrir la clave correcta requerida para descifrar los datos. Al reducir la vida útil válida de una o más de las claves de pago a menos que un tiempo de descifrado por fuerza bruta predicho requerido para implementar un ataque de fuerza bruta con éxito contra los datos cifrados, es posible hacer ineficaz el ataque por fuerza bruta. Esto es debido a que durante el tiempo que se requiere para que el ataque por fuerza bruta tenga éxito, las claves de pago que se obtienen ya no serán válidas en su totalidad, y por ello no se podrán usar para completar con éxito una transacción de pago en línea.

Para determinar un valor apropiado para la vida útil de una Clave de Sesión de ICC, puede calcularse un tiempo de descifrado por fuerza bruta estimado para los datos cifrados en el dispositivo de usuario. Adicionalmente, pueden tomarse en consideración vulnerabilidades de cualquier método usado para cifrar/descifrar las claves. Por ejemplo, una palabra clave débil (tal como una con pocos caracteres o compuesta de palabras del diccionario) puede conducir a un tiempo de descifrado por fuerza bruta estimado más bajo. Como se ha descrito previamente, al configurar la vida útil de las Claves de Sesión de ICC aprovisionadas a menos de un tiempo de descifrado por fuerza bruta predicho requerido para implementar un ataque con éxito, es posible hacer ineficaz un ataque por fuerza bruta, dado que el ataque llevaría más tiempo que la vida útil de la Clave de Sesión de ICC.

Las realizaciones anteriores han de entenderse como ejemplos ilustrativos de la invención. Se conciben realizaciones adicionales de la invención. Por ejemplo, el dispositivo de usuario puede comprender un dispositivo de telefonía móvil capaz de comunicar con el banco emisor a través de la red telefónica móvil de acuerdo con uno o más protocolos de comunicación de red, tal como el acceso por paquetes de alta velocidad (HSPA) o CDMA2000. Adicionalmente, el dispositivo de usuario podría ser un dispositivo habilitado para Internet, capaz de comunicar con el banco emisor a través de Internet de acuerdo con uno o más protocolos de comunicación basados en paquetes, tales como un protocolo apropiado para la serie de Protocolos de Internet (IP). Adicionalmente, el método de la presente invención puede manejarse mediante la disposición del dispositivo de usuario para comunicar con un agente del banco emisor, en lugar de con el banco emisor en sí, en el que el agente está equipado con los datos necesarios requeridos para aprovisionar a la aplicación de pago.

REIVINDICACIONES

1. Un método para autorizar una transacción de pago EMV entre un dispositivo de usuario (502; 600) y un terminal de punto de venta (504), siendo dicha transacción de pago EMV una que se autoriza como parte de la transacción de pago por un banco emisor (500), en el que dicho banco emisor (500) mantiene datos indicativos de una Clave Maestra de ICC correspondiente a una aplicación de pago aprovisionada al dispositivo de usuario (502; 600), teniendo la aplicación de pago un primer estado operativo en el que dicha aplicación de pago tiene permitido llevar a cabo dicha transacción de pago EMV, y un segundo estado operativo, diferente de dicho primer estado operativo, comprendiendo el método:

en respuesta a la recepción de una clave de sesión generada por dicho banco emisor (500) basándose en dicha Clave Maestra de ICC, aprovisionar dicha aplicación de pago con la clave de sesión, mediante lo que se configura dicha aplicación de pago en dicho primer estado operativo; y posteriormente
en respuesta a la recepción de la solicitud de un criptograma de aplicación en la aplicación de pago desde el terminal de punto de venta (504), usar la aplicación de pago para realizar un proceso de autorización, comprendiendo el proceso de autorización las etapas de:

generar dicho criptograma de aplicación basándose en la clave de sesión recibida; y
transmitir el criptograma de aplicación generado al terminal de punto de venta para verificación del mismo por el banco emisor (500) y autorización de la transacción de pago EMV.

2. Un método de acuerdo con la reivindicación 1, en el que la clave de sesión se aprovisiona al dispositivo de usuario (502; 600) por dicho banco emisor (500).

3. Un método de acuerdo con la reivindicación 1 o 2, que comprende descartar dicha clave de sesión después de completar la transacción de pago EMV.

4. Un método de acuerdo con cualquier reivindicación precedente que comprende configurar la aplicación de pago en el segundo estado operativo en respuesta a finalizar la transacción de pago EMV.

5. Un método de acuerdo con cualquier reivindicación precedente, en el que, en respuesta a que se satisface un criterio predeterminado, se aprovisiona una clave de sesión adicional a dicho dispositivo de usuario (502; 600).

6. Un método de acuerdo con la reivindicación 5, en el que el criterio predeterminado comprende uno o más de entre:

la aplicación de pago está configurada en el segundo estado operativo;
recibir una solicitud de un tipo predeterminado, identificando dicha solicitud al menos el dispositivo de usuario (502; 600);
el día, mes y año mantenido por una entidad de provisión de certificados que coincide con una fecha que corresponde a una cantidad de tiempo predeterminada que ha transcurrido desde el aprovisionamiento de la clave de sesión al dispositivo de usuario (502; 600); y
el número de claves de sesión almacenadas por el dispositivo de usuario (502; 600) cae por debajo de un valor predeterminado.

7. Un método de acuerdo con cualquier reivindicación precedente en el que la clave de sesión es accesible por la aplicación de pago en respuesta a la finalización de un proceso de autenticación del usuario en el dispositivo de usuario (502; 600).

8. Un método acuerdo con cualquier reivindicación precedente, en el que el dispositivo de usuario (600) comprende una primera parte de procesamiento y una segunda parte de procesamiento, comprendiendo la primera parte de procesamiento un primer entorno de aplicación (610) dentro de un elemento seguro (612) y comprendiendo la segunda parte de procesamiento un segundo entorno de aplicación (620) externo al elemento seguro (612), y en el que la segunda parte de procesamiento comprende dicha aplicación de pago.

9. Un método de acuerdo con la reivindicación 8, en el que el dispositivo de usuario comprende un dispositivo de comunicaciones móvil y el elemento seguro comprende un Módulo de Identidad de Abonado (610).

10. Un método de acuerdo con la reivindicación 8 o 9 en el que el segundo entorno de aplicación comprende un Entorno de Ejecución de Confianza.

11. El método de acuerdo con la reivindicación 10 en el que dicha clave de sesión se almacena en dicho Entorno de Ejecución de Confianza.

12. Un dispositivo de usuario (502; 600) para realizar una transacción de pago EMV con un terminal de punto de venta (504), siendo dicha transacción de pago EMV una que se autoriza como parte de la transacción de pago por

un banco emisor (500), en el que dicho banco emisor (500) mantiene datos indicativos de una Clave Maestra de ICC, comprendiendo el dispositivo de usuario (502; 600) una aplicación de pago, teniendo la aplicación de pago un primer estado operativo en el que dicha aplicación de pago está habilitada para realizar dicha transacción de pago EMV, y un segundo estado operativo, diferente a dicho primer estado operativo, y en el que la aplicación de pago es sensible a la recepción de una clave de sesión generada por dicho banco emisor (500) basándose en dicha Clave Maestra de ICC, mediante lo que queda configurado en dicho primer estado operativo y posteriormente se dispone para realizar un proceso de autorización, comprendiendo el proceso de autorización las etapas de:

recibir una solicitud de un criptograma de aplicación desde un terminal de punto de venta (504);
en respuesta a la recepción de la solicitud para el criptograma de aplicación, generar dicho criptograma de aplicación basándose en la clave de sesión recibida; y
transmitir el criptograma de aplicación generado al terminal de punto de venta (504) para verificación del mismo por el banco emisor y autorización de la transacción de pago EMV.

13. Un dispositivo de usuario de acuerdo con la reivindicación 12 que comprende:

una primera parte de procesamiento; y
una segunda parte de procesamiento,
en el que la primera parte de procesamiento comprende un primer entorno de aplicación (610) dentro de un elemento seguro (612) y la segunda parte de procesamiento comprende un segundo entorno de aplicación (620) externo al elemento seguro (612), en el que la segunda parte de procesamiento comprende dicha aplicación de pago.

14. Un producto de programa informático que comprende instrucciones que pueden implementarse por procesador que, cuando se ejecutan en un dispositivo de usuario (502; 600), realizan un método tal como se ha reivindicado en la reivindicación 1.

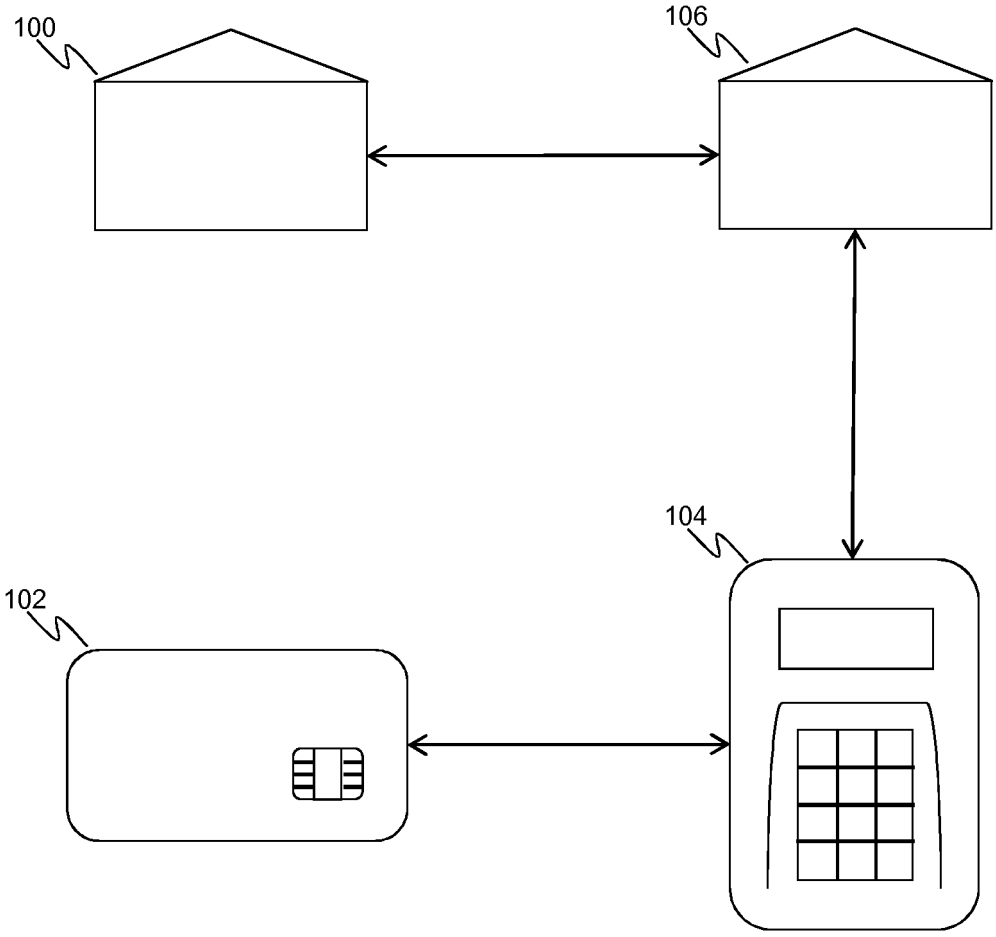

Figura 1

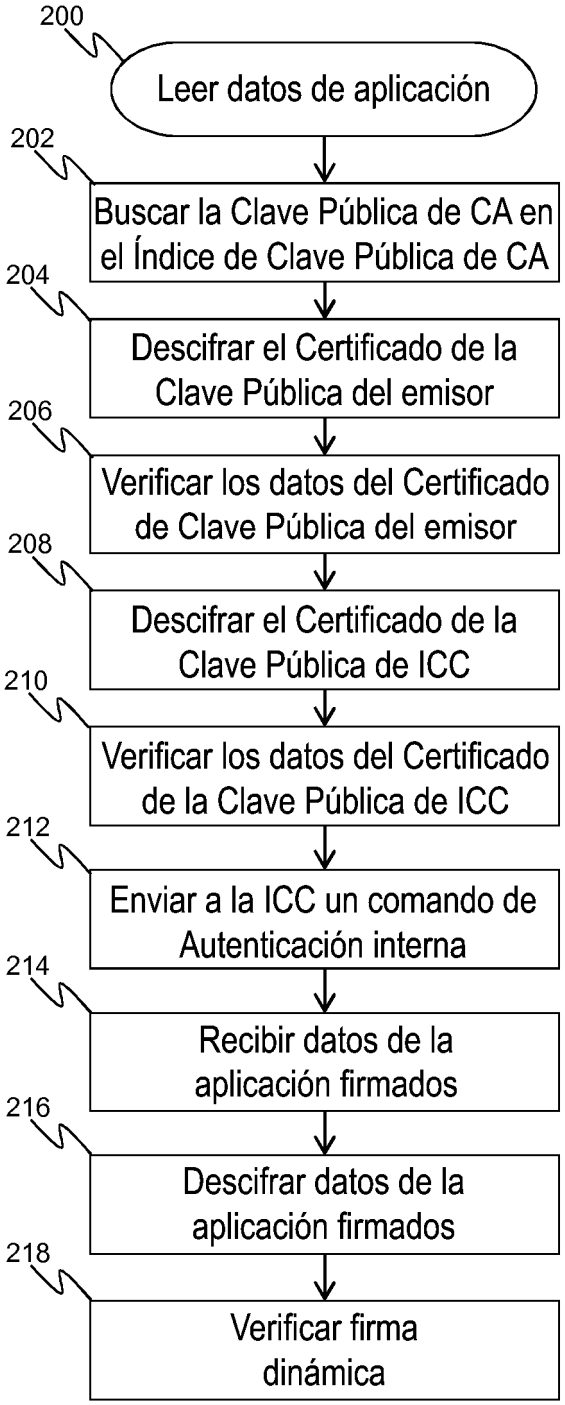
200
Leer datos de aplicación
202
Buscar la Clave Pública de CA en el Índice de Clave Pública de CA
204
Descifrar el Certificado de la Clave Pública del emisor
206
Verificar los datos del Certificado de Clave Pública del emisor
208
Descifrar el Certificado de la Clave Pública de ICC
210
Verificar los datos del Certificado de la Clave Pública de ICC
212
Enviar a la ICC un comando de Autenticación interna
214
Recibir datos de la aplicación firmados
216
Descifrar datos de la aplicación firmados
218
Verificar firma dinámica

Figura 2

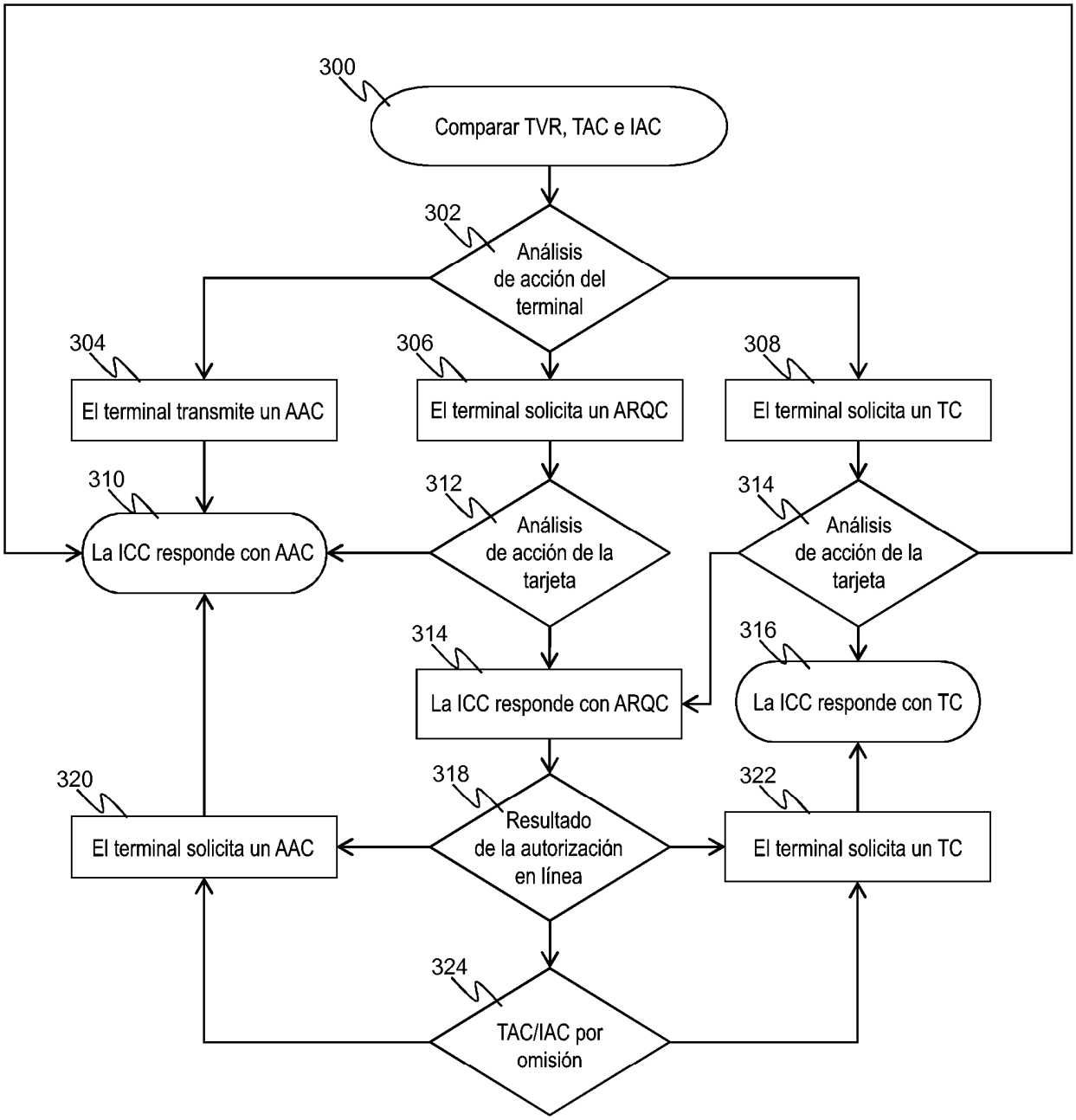
300
Comparar TVR, TAC e IAC
302
Análisis de acción del terminal
304
El terminal transmite un AAC
306
El terminal solicita un ARQC
308
El terminal solicita un TC
310
La ICC responde con AAC
312
Análisis de acción de la tarjeta
314
Análisis de acción de la tarjeta
314
La ICC responde con ARQC
316
La ICC responde con TC
320
El terminal solicita un AAC
318
Resultado de la autorización en línea
322
El terminal solicita un TC
324
TAC/IAC por omisión

Figura 3

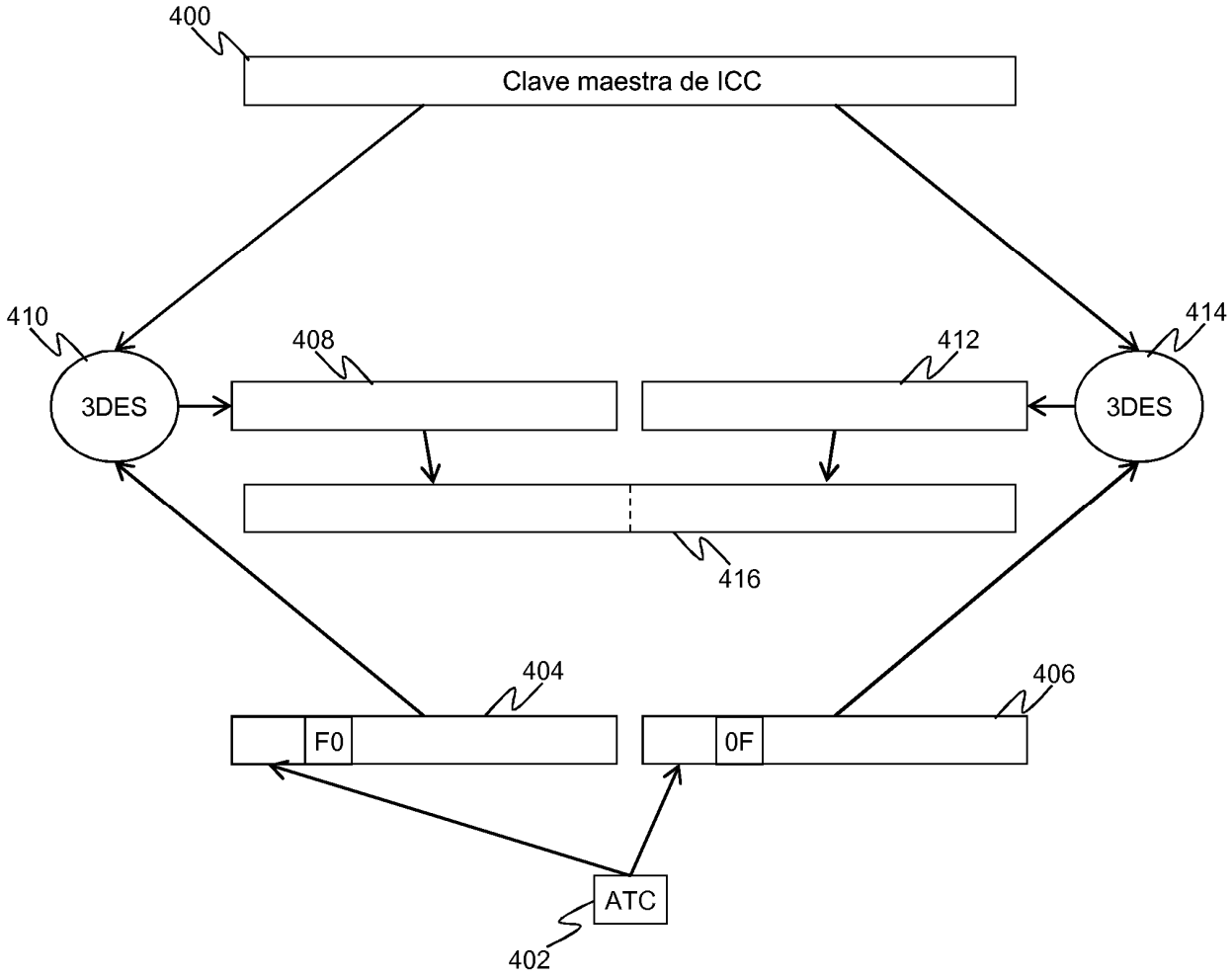
400
Clave maestra de ICC
410
3DES
408
412
414
3DES
416
404
406
F0
0F
ATC
402

Figura 4

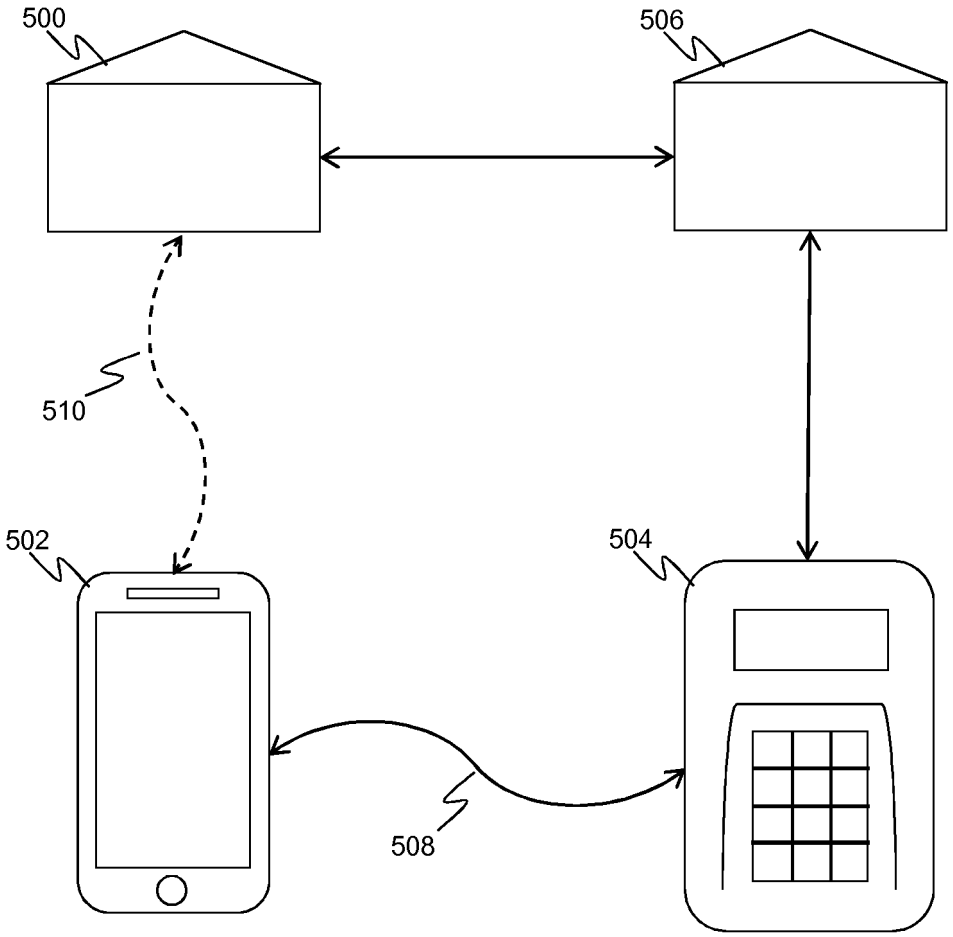

Figura 5

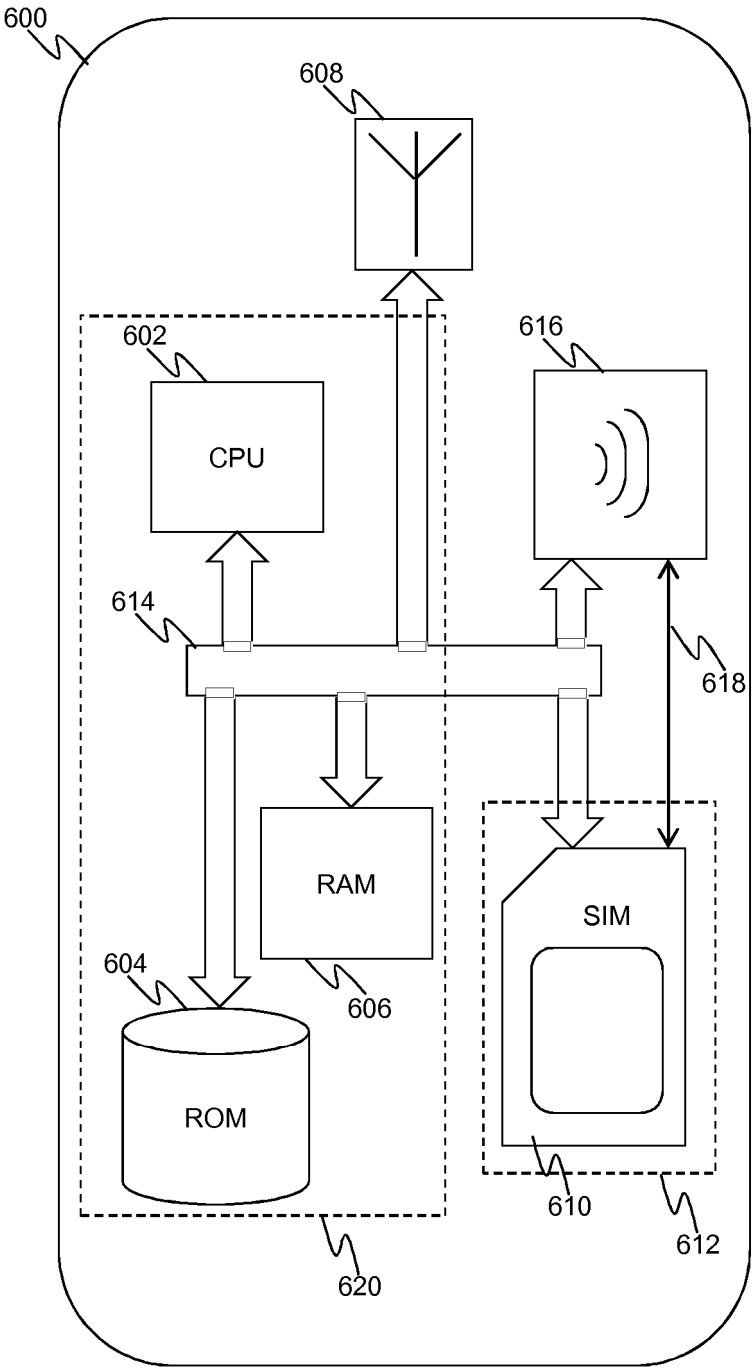

Figura 6

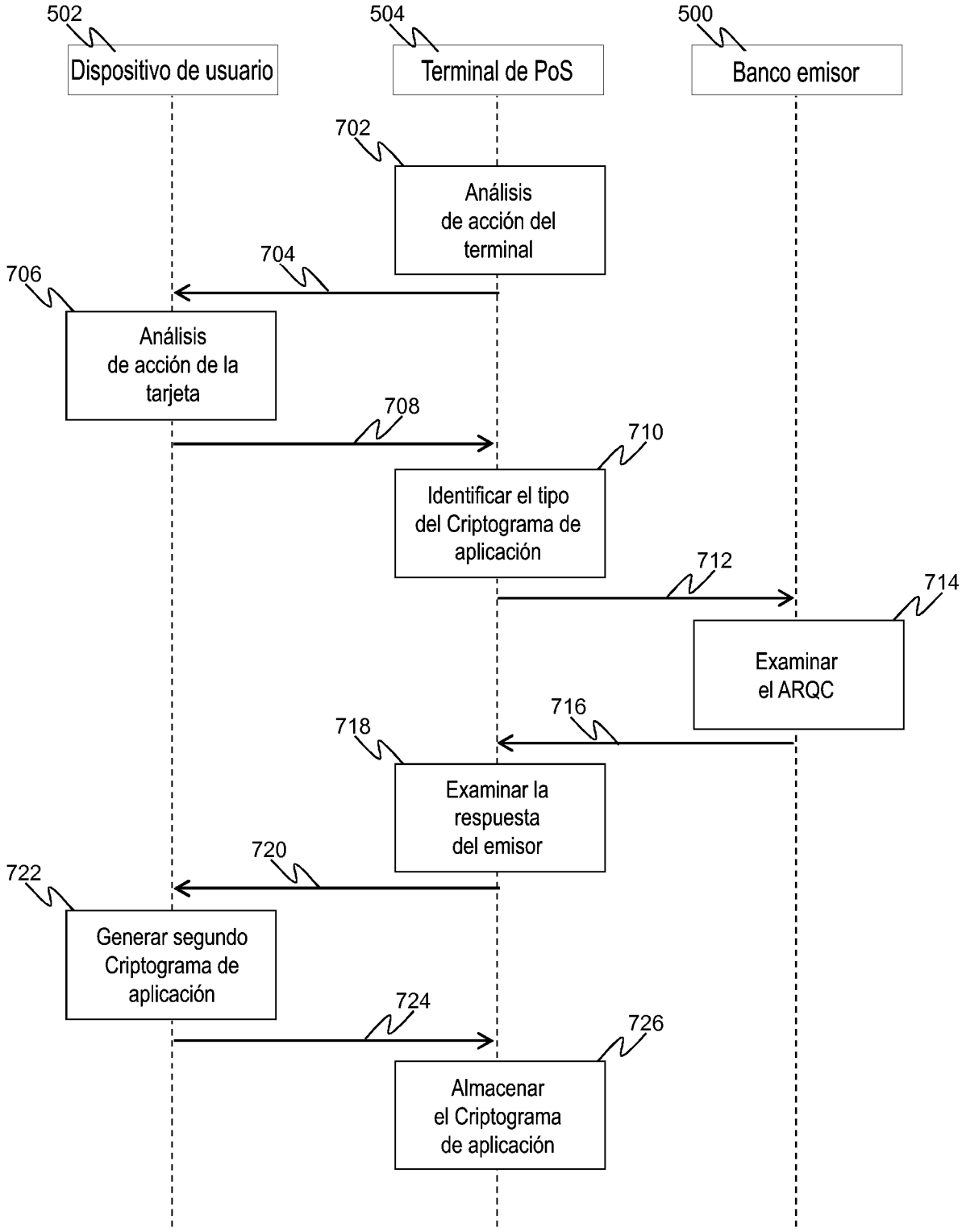
502
Dispositivo de usuario
504
Terminal de PoS
500
Banco emisor
702
Análisis de acción del terminal
704
706
Análisis de acción de la tarjeta
708
710
Identificar el tipo del Criptograma de aplicación
712
714
Examinar el ARQC
716
718
Examinar la respuesta del emisor
720
722
Generar segundo Criptograma de aplicación
724
726
Almacenar el Criptograma de aplicación

Figura 7