(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 988 543**

(51) Int. Cl.:

H04L 9/40 (2012.01)
H04W 12/00 (2011.01)
H04W 12/50 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **22.06.2021 PCT/EP2021/066960**

(87) Fecha y número de publicación internacional: **13.01.2022 WO22008231**

(96) Fecha de presentación y número de la solicitud europea: **22.06.2021 E 21735909 (0)**

(97) Fecha y número de publicación de la concesión europea: **24.07.2024 EP 4179697**

(54) Título: **Emparejamiento seguro de extremo a extremo de un elemento seguro a un dispositivo móvil**

(30) Prioridad:

08.07.2020 EP 20315343

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
21.11.2024

(73) Titular/es:

THALES DIS FRANCE SAS (100.0%)
6, rue de la Verrerie
92190 Meudon, FR

(72) Inventor/es:

CHAFER, SYLVAIN y
FAVREAU, VALENTIN

(74) Agente/Representante:

DEL VALLE VALIENTE, Sonia

DESCRIPCIÓN

Emparejamiento seguro de extremo a extremo de un elemento seguro a un dispositivo móvil

Antecedentes de la invención

La presente invención se refiere, en general, a elementos seguros y dispositivos móviles y, más particularmente, a un emparejamiento seguro de unos elementos seguros a unos dispositivos móviles.

Un elemento seguro (SE) es un componente electrónico a prueba de manipulaciones que se utiliza en general para almacenar aplicaciones principales (host) y los datos confidenciales y criptográficos que están asociados con esas aplicaciones principales. En la presente memoria, la expresión *elemento seguro* se define como un circuito integrado empotrado que emplea unas características a prueba de manipulaciones para proteger las aplicaciones y los datos que están almacenados en el mismo.

En "Introduction to Secure Elements", Global Platform (https://globalplatform.org/wp-content/uploads/2018/05/Introduction-to-Secure-Element-15May2018.pdf [2018]) se describen elementos seguros.

Si bien los elementos seguros adoptan muchas formas diferentes, un uso de particular interés en la presente memoria es su utilización en las tarjetas bancarias y las tarjetas de pago electrónico. Un consumidor puede utilizar una tarjeta bancaria y de pago electrónico para realizar transacciones financieras, por ejemplo, para comprar bienes o servicios.

Así, un elemento seguro puede alojar unas aplicaciones de servicios financieros y de pago y unas credenciales asociadas. El elemento seguro proporciona servicios tales como la autenticación, la firma digital y la gestión de PIN.

En aras de la brevedad, en lo sucesivo se utilizará la expresión *tarjeta SE* para referirse a una tarjeta, por ejemplo, una tarjeta de pago o de servicios financieros, que tiene un elemento seguro empotrado.

Aunque los elementos seguros resultan útiles en las tarjetas de pago y de servicio financiero, también se encuentran en muchos otros dispositivos, tales como cajas de escritorio, vehículos, dispositivos del Internet de las cosas (IoT), relojes, etc.

Las transacciones financieras digitales son muy convenientes para los usuarios. Sin embargo, existen riesgos de seguridad. Por lo tanto, resulta beneficioso añadir unas prestaciones de seguridad que eviten el riesgo de un uso fraudulento de servicios de pago y de otros servicios financieros proporcionados por una tarjeta SE. Naturalmente, el elemento seguro proporciona muchas prestaciones de seguridad, por ejemplo, la verificación de PIN. No obstante, la provisión de factores de autenticación adicionales mejora la seguridad asociada con una tarjeta SE. Un factor de autenticación basado en la verificación de PIN determina lo que *sabe* la persona que realiza la verificación de PIN. ¿Conoce el PIN? Un segundo factor de autenticación se basa en lo que *tiene*.

Así, sería deseable que el elemento SE confirmara que el portador de la tarjeta SE estuviese en posesión de otro dispositivo que esté enlazado a la misma. Además, sería deseable que tal emparejamiento de dispositivos fuera seguro y que sólo pudiera realizarse si lo autorizara el propietario de la tarjeta SE. En el documento US2011/0028091A1 se describe un método para realizar un emparejamiento de dispositivos inalámbricos de campo cercano en el que se intercambia una clave.

De lo anterior resulta evidente que hay necesidad de tener un método mejorado para emparejar un elemento seguro a un segundo dispositivo.

Resumen

Entre un elemento seguro y un dispositivo inteligente se establece un enlace seguro en un segundo protocolo, que puede ser Bluetooth Low Energy (BLE), a través de un enlace en un segundo protocolo, que puede ser Near-Field Communication (NFC). El proceso incluye establecer un enlace en el primer protocolo entre el elemento seguro y el dispositivo inteligente y, en respuesta al mismo, generar, por parte del elemento seguro, una clave de cifrado de comunicación, y asociar un estado con la clave de cifrado y asignar al estado un primer nivel, que en una realización se denomina estado *candidato*. Posteriormente, transmitir al dispositivo inteligente por el enlace establecido en el primer protocolo un mensaje que encapsula la clave de cifrado y el estado de la clave de cifrado de comunicación del elemento seguro. El elemento seguro y el dispositivo inteligente se emparejan a través del segundo protocolo, estableciéndose así un enlace de segundo protocolo. El elemento seguro transmite un mensaje cifrado utilizando la clave de cifrado de comunicación al dispositivo inteligente por el enlace de segundo protocolo.

En un aspecto, en respuesta a la detección de un emparejamiento a través del segundo protocolo, determinar, por parte del dispositivo inteligente, el estado de la clave de cifrado de comunicación, proporcionar al titular de tarjeta en el dispositivo inteligente un mensaje informativo que indica el emparejamiento del elemento seguro y el dispositivo

inteligente, así como el estado de la clave de cifrado de la comunicación, por ejemplo, mostrando un mensaje de este tipo en el teléfono inteligente o proporcionando un mensaje de voz.

El emparejamiento puede ir seguido de una autenticación de un titular de tarjeta del elemento seguro y, en respuesta a la verificación del titular de tarjeta como titular de tarjeta autorizado del elemento seguro, de una subida del estado de la clave de cifrado de comunicación del primer nivel a un segundo nivel, que en una realización se denomina *de confianza*.

En un aspecto, en respuesta a la realización de una transacción utilizando el elemento seguro y un terminal de punto de venta, determinar el estado de la clave de cifrado de comunicación y, si el estado de la clave de cifrado de comunicación es el segundo nivel, transmitir unos detalles de transacción al dispositivo inteligente por el enlace de segundo protocolo o, de lo contrario, no transmitir ningún detalle de transacción al dispositivo inteligente; y, en respuesta a la recepción, por parte del dispositivo inteligente, de los detalles de transacción, mostrar los detalles de transacción para el titular de tarjeta en una pantalla del dispositivo inteligente.

En otro aspecto, en respuesta a la realización de una transacción utilizando el elemento seguro y un terminal de punto de venta, determinar el estado de la clave de cifrado de comunicación y, a partir del estado de la clave de cifrado de comunicación, unos aspectos concretos de transacción y una política de seguridad, realizar una acción seleccionada de entre proceder con la transacción, impedir la transacción o solicitar una aprobación de la transacción del titular de tarjeta transmitiendo un mensaje de solicitud de aprobación al dispositivo inteligente.

En un aspecto, un elemento seguro y un dispositivo inteligente incluyen, respectivamente, unas instrucciones que ordenan a un procesador de estos respectivos dispositivos llevar a cabo los procesos descritos anteriormente. Ventajosamente, estas instrucciones pueden almacenarse en una memoria de programa del elemento seguro y del dispositivo inteligente, respectivamente. La invención se divulga en las reivindicaciones adjuntas.

Breve descripción de las figuras

La figura 1 es una ilustración de una tarjeta que tiene un elemento seguro que está siendo utilizado en combinación con un teléfono inteligente por un titular de tarjeta para llevar a cabo una transacción de pago a través de un terminal de punto de venta (POS).

La figura 2 es una ilustración de los elementos de la figura 1 que se utilizan en una transacción de pago.

La figura 3 es un diagrama de bloques de alto nivel de una arquitectura de dispositivo de una tarjeta de elemento seguro de las figuras 1 y 2.

La figura 4 es un diagrama de bloques de unos programas y unos datos que están almacenados en una memoria de la tarjeta de elemento seguro de las figuras 1 a 3.

La figura 5 es un diagrama de arquitectura de alto nivel del teléfono inteligente de las figuras 1 y 2.

La figura 6 es un diagrama de secuencia de temporización que ilustra una provisión segura de unas claves de cifrado de comunicación por un canal NFC que se ha establecido entre la aplicación de pago que se está ejecutando en el elemento seguro de las figuras 1-4 y una correspondiente app TeléfonoaSE que se está ejecutando en el teléfono inteligente de la figura 5.

La figura 7 es un diagrama de secuencia de temporización que ilustra la autenticación de usuario del titular de tarjeta y un ascenso de un estado de la clave de cifrado de comunicación de ser una clave *candidata* a convertirse en una clave *de confianza*.

Descripción detallada de la invención

En la descripción detallada que sigue se hace referencia a los dibujos adjuntos, que muestran, a modo de ilustración, realizaciones específicas en las que puede ponerse en práctica la invención. Estas realizaciones se describen con detalle suficiente para permitir que los expertos en la técnica pongan en práctica la invención. Debe entenderse que, aunque sean diferentes, las diversas realizaciones de la invención no son necesariamente mutuamente excluyentes. Por ejemplo, un rasgo, estructura o característica particular descrito en el presente documento en relación con una realización puede implementarse en otras realizaciones sin salirse del alcance de la invención. Además, debe entenderse que la ubicación o la disposición de elementos individuales en cada realización descrita puede modificarse sin salirse del alcance de la invención. Por lo tanto, no hay que tomar la siguiente descripción detallada en sentido limitativo, y el alcance de la presente invención está definido únicamente por las reivindicaciones adjuntas, debidamente interpretadas, junto con la gama completa de equivalentes a los que tienen derecho las reivindicaciones. En los dibujos, números similares se refieren a la misma o similar funcionalidad en las varias vistas.

La siguiente descripción incluye referencias a varios métodos ejecutados por un procesador de un chip de circuito integrado. Como es habitual en este campo, puede haber frases en la presente memoria que indiquen que estos métodos o etapas del método se realizan mediante instrucciones de software o módulos de software. Como sabrá un experto en la técnica, dichas descripciones deben interpretarse en el sentido de que un procesador, de hecho, ejecuta los métodos, las instrucciones de software y los módulos de software.

La tecnología descrita en la presente memoria prevé un emparejamiento seguro de unos dispositivos, en particular, el emparejamiento seguro de un elemento seguro, que está empotrado en una tarjeta SE, y un dispositivo móvil, por ejemplo, un teléfono inteligente.

La figura 1 es una ilustración de una tarjeta SE 101 que está siendo utilizada en combinación con un teléfono inteligente 103 por un titular 100 de tarjeta para realizar una transacción de pago a través de un terminal 105 de punto de venta (POS). La tarjeta SE 101 contiene un elemento seguro 107. La tarjeta SE 101 y el teléfono inteligente 103 pertenecen al mismo titular 100 de tarjeta y se utilizan, tal y como se explicará más adelante con más detalle, para asegurar unas transacciones realizadas utilizando la tarjeta SE 101 o para dotar al titular 100 de tarjeta de una información relativa a las transacciones realizadas.

Entre el elemento seguro 107 y el teléfono inteligente 103 se puede establecer un primer canal 108 de comunicación de corto alcance.

Posteriormente, entre el elemento seguro 107 y el teléfono inteligente 103 se puede establecer un segundo canal 109 de comunicación de corto alcance. El segundo canal 109 de comunicación aporta muchas opciones a la hora de asegurar las transacciones llevadas a cabo utilizando la tarjeta SE 101. Por ejemplo, para realizar determinadas transacciones puede que sea necesaria la presencia del teléfono inteligente 103. Esto impide que se lleven a cabo transacciones fraudulentas con una tarjeta SE 101 robada. El segundo canal 109 de comunicación no se puede establecer si la tarjeta 101 ha sido robada o encontrada después de haberse perdido y el correspondiente teléfono inteligente 103 no está presente dentro del alcance del canal 109 de comunicación de corto alcance. Alternativamente, el teléfono inteligente 103 puede usarse para proporcionar información transaccional al usuario 100.

El primer canal 108 de comunicación de corto alcance se puede usar para transmitir una clave de cifrado de comunicación del elemento seguro 107 al teléfono inteligente 103 para que se puedan cifrar las comunicaciones entre el elemento seguro 107 y el teléfono inteligente 103 que tengan lugar en el segundo canal 109 de comunicación de corto alcance.

En una realización, la tarjeta SE 101 está equipada para comunicarse con el teléfono inteligente 103 según dos protocolos de comunicación. En una realización, estos protocolos son el protocolo de comunicaciones de campo cercano (NFC) y el protocolo Bluetooth® Low Energy (BLE). No obstante, la tecnología descrita en la presente memoria es de aplicación a cualquiera de una gran cantidad de protocolos de comunicación, incluidos WiFi y Zigbee.

Una característica del NFC y del BLE que los hace atractivos para la aplicación analizada en la presente memoria es que funcionan a lo largo de una distancia muy corta. En el caso del NFC, las comunicaciones están limitadas a 4 cm y se activan mediante una operación de "toque NFC" en la que un titular de tarjeta hace que los dispositivos de comunicación se toquen entre sí. En el caso del BLE, la distancia máxima teórica es de unos 100 m; no obstante, en la práctica se pueden esperar distancias mucho más cortas (10-20 m). El BLE también es muy sensible a las barreras físicas. Así, a un canal de comunicaciones establecido entre un elemento seguro y un teléfono inteligente a través del BLE se le garantiza una estrecha proximidad física de los dos dispositivos.

La figura 2 es una ilustración de los elementos de la figura 1 que se utilizan en una transacción de pago llevada a cabo utilizando la tarjeta SE 101. La tarjeta SE 101 se ha emparejado con el teléfono inteligente 103 para una comunicación por un canal 109 de comunicaciones BLE.

Para realizar la transacción, el titular de tarjeta inserta la tarjeta 101 en el terminal POS 105, mediante el cual el terminal y el elemento seguro pueden comunicarse a través de un adaptador 203 de contacto, por ejemplo, de acuerdo con la norma ISO 7816 de comunicaciones con tarjetas inteligentes con contactos. La comunicación entre la tarjeta SE 101 y el terminal POS 105 puede tener lugar utilizando otros medios de comunicación, por ejemplo, una comunicación inalámbrica en virtud de la norma ISO 14443 o del NFC.

En una realización, el canal BLE que va del elemento seguro 107 al teléfono inteligente 103 se usa para proporcionar información al titular de tarjeta. Por ejemplo, cuando está a punto de tener lugar una transacción, se transmite un mensaje informativo al teléfono inteligente 103 del titular de tarjeta para permitirle conocer los detalles de transacción. Los detalles de transacción también pueden guardarse en el teléfono inteligente 103 a efectos de registro.

En unas realizaciones alternativas, el teléfono inteligente 103 se utiliza para aportar una seguridad adicional a fin de garantizar que las transacciones sean como pretende que sean el titular de tarjeta.

Los detalles de transacción pueden comunicarse de la tarjeta SE 101 al teléfono inteligente 103 por el canal BLE 109, y estos detalles de transacción pueden mostrarse 205 para que los confirme el titular de tarjeta. En otras realizaciones, el teléfono inteligente 103 informa al titular de tarjeta de otras maneras. Por ejemplo, el teléfono inteligente 103 puede proporcionar un mensaje de voz al titular de tarjeta para informarle de los detalles de transacción.

Un protocolo de seguridad de transacción puede prever muchas opciones diferentes que incluyan o no el teléfono inteligente 103:

- Permitir todas las transacciones y proporcionar información en el teléfono inteligente 103 por el enlace BLE
- Las transacciones pequeñas, por ejemplo, menores que 10,00 dólares estadounidenses o 10,00 euros, no requieren una comunicación con el teléfono inteligente
- Las transacciones medianas, por ejemplo, de entre 10,00 (USD o euros) y 100,00 (USD o euros), requieren que la tarjeta SE 101 confirme que el teléfono inteligente es alcanzable, es decir, que está dentro del alcance del protocolo utilizado
- Las transacciones grandes, por ejemplo, de más de 100,00 (USD o euros), deben ser confirmadas por el titular de tarjeta en el teléfono inteligente 103

La utilización del teléfono inteligente 103 en combinación con el elemento inteligente 101 durante la ejecución de transacciones financieras requiere su emparejamiento.

La comunicación entre el teléfono inteligente 103 y el elemento seguro 101 debe ser segura. En consecuencia, el teléfono inteligente 103 y el elemento seguro 101 entablan un proceso de emparejamiento, que se describe más adelante en la presente memoria, para establecer una clave de cifrado de comunicaciones de confianza para cifrar los mensajes que se comuniquen entre los dos.

La figura 3 es un diagrama de bloques de alto nivel de una arquitectura de dispositivo de una tarjeta SE 101 que incluye un elemento seguro 107. El dispositivo móvil 107 puede incluir un procesador 301 que está conectado, a través de un bus 202, a una memoria 303 de acceso aleatorio (RAM), a una memoria 304 de sólo lectura (ROM) y a una memoria no volátil (NVM) 305. El dispositivo móvil 107 incluye además una interfaz 307 de entrada/salida para conectar el procesador 301 –de nuevo, por lo general, a través del bus 302– a un adaptador 203 de contacto mediante el cual el elemento seguro 107 puede conectarse al terminal POS 105. Alternativamente (o adicionalmente), la tarjeta SE 103 contiene una antena 311 mediante la cual el dispositivo SE 103 puede conectarse inalámbricamente al terminal POS 105 a través de la interfaz 307 de entrada/salida a través de un protocolo inalámbrico, por ejemplo, según ISO 14443.

La tarjeta SE 103 contiene además las interfaces 313 y 309 de comunicaciones para comunicarse utilizando el protocolo de comunicaciones BLE y el protocolo de comunicaciones NFC, respectivamente.

La ROM 304 y/o la NVM 305 puede(n) incluir una memoria 401 de programas para almacenar unos programas ejecutables por el procesador 301, tal y como se ha ilustrado en la figura 4. Aunque en la figura 4 se haya ilustrado que los programas informáticos 401 están todos coubicados en la ROM 304 y la NVM 305, en la práctica no existe tal restricción, ya que los programas pueden estar repartidos por múltiples memorias e incluso instalarse temporalmente en la RAM 303. Además, la tarjeta SE 103 puede incluir múltiples ROM o NVM.

La memoria 401 de programas incluye unos programas 407 de sistema de tarjeta, que pueden incluir una máquina virtual 409, así como un controlador 411 para NFC y un controlador 413 para BLE, para comunicarse por unas interfaces BLE y NFC 313 y 309, respectivamente. El sistema 407 de tarjeta también puede incluir un controlador 415 para comunicarse a través del protocolo ISO 7816.

Los programas 401 también incluyen una aplicación 403 de pago a través de la cual un usuario 100 ejecuta unos pagos. La aplicación 403 de pago interactúa con el proveedor de servicios comerciales a través del terminal POS 105. La aplicación 403 de pago contiene un módulo 405 para comunicarse con un teléfono inteligente 103 emparejado. Así, por ejemplo, cuando la aplicación 403 de pago intenta realizar una compra a través del terminal POS 105 que desencadena una acción del teléfono inteligente 103, el módulo de SE a teléfono envía unos mensajes apropiados al teléfono a través de la interfaz BLE 313.

Tal y como se explicará más adelante con más detalle, la aplicación 403 de pago genera una o más claves 417 de cifrado de comunicaciones y almacena esas claves en la memoria no volátil 305.

La figura 5 es un diagrama de arquitectura de alto nivel del teléfono inteligente 103. El teléfono inteligente 103 contiene un procesador 501 y una memoria 505, así como unas interfaces NFC 507 y BLE 509. La memoria 505 contiene unos programas 511, que incluyen una aplicación 503 de teléfono a SE para comunicarse con la correspondiente aplicación de SE a teléfono en el módulo 405 de SE a teléfono de la aplicación 403 de pago del elemento seguro 107.

La memoria 511 de programas también contiene unos controladores 513 y 515 para comunicarse a través de los protocolos NFC y BLE a través de las interfaces NFC 507 y BLE 509, respectivamente.

La memoria no volátil 505 también se puede usar para almacenar la clave 517 de cifrado de comunicación, que corresponde a la(s) clave(s) de cifrado de comunicación almacenada(s) en la tarjeta SE 101 (la clave 417 de cifrado de comunicación).

La figura 6 es un diagrama de secuencia de temporización que ilustra una provisión segura de las claves 417/517 de cifrado de comunicación por un canal NFC establecido entre la aplicación 403 de pago que se está ejecutando en el elemento seguro 107 en la tarjeta SE 101 y la correspondiente app 503 Teléfono a SE que se está ejecutando en el teléfono inteligente 103. La clave de cifrado de comunicación transferida por el canal NFC se usa para asegurar una comunicación BLE posterior cuando el teléfono inteligente 103 se empareja con el elemento seguro 107 para establecer un canal BLE entre los dos cifrando los mensajes transmitidos entre el elemento seguro 107 y el teléfono inteligente 103. Se puede utilizar cualquiera de diversas normas de cifrado, incluidas, sin limitación, Advanced Encryption Standard (AES) y RSA, así como las variaciones de las mismas. Para facilitar la explicación, la descripción que se hace en la presente memoria corresponde a un cifrado simétrico, por ejemplo, AES. Sin embargo, la tecnología también es aplicable a un cifrado asimétrico, por ejemplo, RSA.

El titular 100 de tarjeta "toca" el teléfono inteligente 103 con la tarjeta SE 101, paso 601. El NFC funciona en un alcance de menos de 4 cm. Así, un toque coloca la tarjeta SE 101 y el teléfono inteligente 103 dentro de este alcance. El toque establece un canal NFC 603 del elemento seguro 107 al teléfono inteligente 103. En la capa de software, este canal permite una comunicación entre la app 403 de pago, que incluye unas instrucciones a tal efecto (denominada aquí módulo 405 SE a Teléfono), y la correspondiente aplicación, es decir, la app 503 Teléfono a SE que se está ejecutando en el teléfono inteligente 103.

El canal NFC 603 puede ser un canal unidireccional del elemento seguro 107 al teléfono inteligente 103 que permita al teléfono inteligente 103 leer unas etiquetas formateadas para el intercambio de datos por NFC (NDEF). Las etiquetas NDEF encapsulan una clave de cifrado de comunicación del elemento seguro 107.

El teléfono inteligente 103 lee la etiqueta NDEF que encapsula una clave de cifrado de comunicación, paso 605.

Cada vez que el teléfono inteligente 103 lee una etiqueta NDEF del elemento seguro 107, el elemento seguro 107 proporciona una nueva clave de cifrado de comunicación. La clave de cifrado de comunicación puede generarse a partir de una clave maestra que esté almacenada en el elemento seguro 107 o puede ser un número aleatorio.

El teléfono inteligente 103 almacena la clave de cifrado de comunicación de la última operación de toque como una clave candidata en una memoria persistente, por ejemplo, la NVM 505, paso 607. Una clave *candidata* es una clave de cifrado de comunicaciones que ha sido recibida por el teléfono inteligente 103 procedente del elemento seguro 107 sin que haya sido confirmada validando al titular de tarjeta. Una vez que se ha verificado al titular de tarjeta, la clave de cifrado de comunicaciones es ascendida a clave *de confianza*.

En una realización, si la clave de cifrado de comunicaciones es simplemente una clave *candidata*, el enlace BLE sólo se usa para enviar información sobre el enlace propiamente dicho, es decir, que se ha producido un emparejamiento entre el elemento seguro 107 y el teléfono inteligente 103 y que la clave 417/517 de cifrado de comunicaciones es una clave *candidata*. En esta realización, la aplicación 503 Teléfono a SE informa al titular de tarjeta de que la clave 517 de cifrado de comunicaciones es una clave *candidata* y que, para obtener la funcionalidad completa del teléfono inteligente 103 en combinación con la tarjeta SE 101, se debe realizar una autenticación de titular de tarjeta.

En esa realización, si la clave 517 de cifrado de comunicaciones ha sido ascendida a clave *de confianza*, el enlace BLE puede usarse para enviar una información personal, tal como unos detalles de transacción, que sólo debería conocer un titular de tarjeta correcto.

El elemento seguro 107 almacena la última clave de cifrado de comunicación que ha generado en respuesta al evento de toque NFC o puede almacenar una secuencia de claves de cifrado de comunicación si el teléfono inteligente 103 es tocado múltiples veces con la tarjeta SE 101 (que contiene el elemento seguro 107) ,paso 609. Como el enlace NFC puede ser un enlace unidireccional del elemento seguro 107 al teléfono inteligente 103, el elemento seguro 107 no puede saber cuál de las claves de la secuencia de claves de cifrado de comunicación generadas está almacenada en el teléfono inteligente 103. Por lo tanto, el elemento seguro 107 envía unos mensajes cifrados que corresponden a cada clave candidata que está almacenada en el elemento seguro 107. Si el teléfono inteligente 103 es capaz de decodificar uno de esos mensajes usando la clave de cifrado de comunicación almacenada en el mismo y producir una respuesta correcta al mismo, el elemento seguro 107 puede entonces inferir de esa respuesta qué clave de cifrado de comunicación de la secuencia almacenada tiene que usar en la comunicación con el teléfono inteligente 103. El enfoque más seguro es almacenar únicamente la última clave. Sin embargo, eso puede hacer que falle el emparejamiento en el enlace BLE.

Se usa una clave de cifrado de comunicación que es una clave *candidata* para asegurar la comunicación del enlace BLE entre el elemento seguro 107 y el teléfono inteligente 103 cifrando los mensajes enviados en el enlace usando la clave. Sin embargo, hasta que el titular de tarjeta no haya sido validado, la clave de cifrado de comunicación que es una clave *candidata* no se trata como si fuera de confianza, y el elemento seguro 107 puede restringir qué acciones se pueden realizar hasta que el titular de tarjeta haya sido verificado y la clave de cifrado de comunicación haya sido ascendida a *de confianza.*

Antes de la verificación del titular 100 de tarjeta, la clave 517 de cifrado de comunicación almacenada por el teléfono inteligente 103 y la(s) clave(s) 417 de cifrado de comunicación almacenada(s) por el elemento seguro 107 se consideran claves candidatas que no son de confianza.

Posteriormente, el elemento seguro 107 y el teléfono inteligente 103 se emparejan para crear un enlace BLE entre los dos, paso 611.

Después de cada emparejamiento, la app 503 Teléfono a SE del teléfono inteligente 103 puede comprobar el estado (*candidata* o *de confianza*) de la clave 517 de cifrado de comunicación que ha almacenado el teléfono inteligente 103 y mostrar un mensaje informativo en el mismo, paso 612. El mensaje puede decir que el teléfono inteligente 103 se ha emparejado con una tarjeta SE 101 e identificarla, por ejemplo, "Su Eurocard BNP con número de cuenta terminado en 'XYZW' se ha emparejado con este teléfono inteligente". También se puede mostrar el estado de la clave de cifrado de comunicación. Antes de que se haya verificado al titular de tarjeta, el estado de la clave de cifrado de comunicación es de clave *candidata.* Así, antes de la verificación, el mensaje mostrado sería "En el enlace a la tarjeta se ha utilizado una clave que no es de confianza".

En un caso de uso, los pasos anteriores se pueden realizar en un entorno fuera de línea, por ejemplo, en el hogar o la oficina del titular de tarjeta. Los pasos posteriores, que incluyen la verificación del titular de tarjeta, se pueden realizar en una terminal POS ubicada en la ubicación de vendedor o fuera de línea utilizando un lector de tarjetas en la ubicación del titular de tarjeta.

A partir de este momento puede haber muchas secuencias de uso diferentes. Por ejemplo, el titular 100 de tarjeta puede intentar realizar una compra en un sitio de vendedor, tal y como se ilustra en la figura 7, que es un diagrama de secuencia de temporización que ilustra la autenticación de usuario del titular de tarjeta y el ascenso de estado de la clave de cifrado de comunicación de ser una clave *candidata* a convertirse en una clave *de confianza*. Por ejemplo, el titular 100 de tarjeta presenta la tarjeta SE, es decir, inserta la tarjeta SE 101 en el terminal POS 105 para realizar una conexión con contacto o coloca la tarjeta SE 101 cerca del terminal POS 105 para establecer un enlace sin contacto al terminal POS 105, paso 713. *Conectada* se utiliza en la presente memoria para referirse tanto a una conexión con contacto como a un enlace sin contacto entre la tarjeta SE 101 y el terminal POS 105.

En respuesta a que se le presente la tarjeta SE 101, el terminal POS 105 crea un canal de comunicación a la tarjeta SE 101, paso 715. En una realización, este canal de comunicación es un canal para transmitir APDU, tal y como se describe en la norma ISO 7816. Si no hay un enlace BLE activo, la tarjeta SE 101 intenta una nueva operación de emparejamiento, paso 717 y, al establecerse un enlace, se mostrarían nuevos mensajes de estado en el teléfono inteligente 103, paso 719, incluido el estado de la clave 517 de cifrado de comunicación.

En respuesta a conectarse al terminal POS 103, la tarjeta SE 101 envía uno o más mensajes cifrados al teléfono inteligente 103 por el enlace BLE previamente establecido, paso 721. En caso de tener almacenadas múltiples claves candidatas, el elemento seguro 107 envía un mensaje cifrado utilizando cada una de esas claves candidatas. Los mensajes pueden ser una prueba de dar el alto-recibir una respuesta para confirmar que el teléfono inteligente 103 ha almacenado la clave de cifrado de comunicación correcta, verificándose así que el teléfono inteligente es el teléfono inteligente correcto.

El teléfono inteligente 103 responde al mensaje, paso 723.

Si la clave de cifrado de comunicación es de confianza, paso 725, la transacción continúa, y la app 503 Teléfono a SE puede mostrar unos mensajes informativos en el teléfono inteligente 103.

Si la clave de cifrado de comunicación no es de confianza, paso 725, el elemento seguro 107 intenta verificar al titular 100 de tarjeta, por ejemplo, pidiéndole que introduzca un PIN. Así, el elemento seguro 107 transmite un mensaje en la interfaz POS 415 al terminal POS 105 para solicitarle que obtenga un PIN del titular 100 de tarjeta, paso 727.

En una pantalla del terminal POS se muestra un mensaje que le dice al titular 100 de tarjeta que introduzca su PIN, paso 729. El usuario introduce entonces el PIN, paso 731, que el terminal POS 105 envía al elemento seguro 107, paso 733.

El elemento seguro 101 verifica el PIN, paso 735, y si se verifica el PIN, el elemento seguro 101 cambia el estado de la clave 415 de cifrado de comunicación de *candidata* a *de confianza, paso* 737, y comunica el cambio de estado a la app 503 Teléfono a SE que está en el teléfono inteligente 103 por el enlace BLE, paso 739. El teléfono inteligente 103

muestra el cambio de estado de la clave 517 de cifrado de comunicación al titular 100 de tarjeta,paso 741. Una vez que la clave se ha marcado como *de confianza*, las comunicaciones en el canal BLE se consideran seguras, y se pone a disposición del titular de tarjeta la funcionalidad plena de la aplicación 503 Teléfono a SE, tal como la visualización de mensajes personales.

Si bien la figura 7 representa una verificación de titular de tarjeta que se está realizando en combinación con una transacción de pago, en una realización alternativa, la verificación del titular 100 de tarjeta se realiza antes de que éste presente la tarjeta SE 101 a un terminal POS 105. Por ejemplo, un titular de tarjeta con un lector de tarjetas que sea capaz de comunicarse en virtud de la norma ISO 7816 o la norma ISO 14443 puede realizar el procedimiento de verificación de titular de tarjeta utilizando ese lector de tarjetas en, por ejemplo, su casa o su oficina.

Caso de uso: reemparejamiento no autorizado de una tarjeta SE a un segundo teléfono inteligente.

Considérese un escenario en el que se ha realizado un emparejamiento legítimo entre el elemento seguro 107 y el teléfono inteligente 103. El titular 100 de tarjeta legítimo entrega la tarjeta SE 101 a un comerciante, otorgando así el control temporal de la tarjeta SE 101 a otra persona. Si esa persona intenta emparejar la tarjeta SE 101 con otro teléfono inteligente 103', se transmite un mensaje por el enlace BLE de la tarjeta SE 101 al teléfono inteligente 103 original. El titular 100 de tarjeta puede entonces rechazar el intento de emparejamiento al segundo teléfono inteligente 103'.

Caso de uso: reemparejamiento autorizado de una tarjeta SE a un segundo teléfono inteligente.

Por otro lado, si obtiene un nuevo teléfono inteligente 103'', el titular 100 de tarjeta puede autorizar el nuevo emparejamiento repitiendo la secuencia ilustrada y explicada en combinación con la figura 6.

En una realización alternativa, en la verificación de titular de tarjeta se utilizan otros mecanismos para verificar al titular de tarjeta. Entre los ejemplos se incluye el uso de datos biométricos como las huellas dactilares, el escaneo del iris y la huella de voz.

De lo anterior resultará evidente que se proporciona un mecanismo eficaz y seguro para emparejar un teléfono inteligente a un elemento seguro.

Aunque se han descrito e ilustrado realizaciones específicas de la invención, la invención no se limitará a las formas o disposiciones específicas de las partes descritas e ilustradas. La invención está limitada únicamente por las reivindicaciones.

REIVINDICACIONES

1. Un método para establecer un enlace seguro en un segundo protocolo entre un elemento seguro (107) y un dispositivo inteligente (103) a través de un enlace en un primer protocolo, comprendiendo dicho dispositivo inteligente una primera aplicación (503) que está configurada para proporcionar una pluralidad de funcionalidades en combinación con el elemento seguro (107), comprendiendo el método:

establecer un enlace (108) en el primer protocolo entre el elemento seguro y el dispositivo inteligente;
en respuesta al establecimiento de un enlace en el primer protocolo, generar, por parte del elemento seguro, una clave de cifrado de comunicación, y asociar un estado con la clave de cifrado de comunicación y asignar al estado un primer nivel;
transmitir un mensaje que encapsula la clave de cifrado de comunicación y el estado de la clave de cifrado de comunicación del elemento seguro al dispositivo inteligente por el enlace establecido en el primer protocolo; autorizando dicha clave de cifrado de comunicación a la primera aplicación a proporcionar menos de todas las funcionalidades de la pluralidad de funcionalidades que se están poniendo a disposición de la primera aplicación (503) sólo si se ha asignado a dicho estado dicho primer nivel,
emparejar el elemento seguro y el dispositivo inteligente a través del segundo protocolo, estableciéndose así un enlace (109) de segundo protocolo;
transmitir un mensaje cifrado usando la clave de cifrado de comunicación del elemento seguro al dispositivo inteligente por el enlace de segundo protocolo;
autenticar a un titular (100) de tarjeta del elemento seguro, siendo dicha autenticación realizada por el elemento seguro comprobando unos datos de identificación personal proporcionados por el titular de tarjeta a través de un dispositivo físico enlazado al elemento seguro;
en respuesta a que, en el paso de autenticación, se verifique al titular de tarjeta como un titular de tarjeta autorizado del elemento seguro, subir el estado de la clave de cifrado de comunicación del primer nivel a un segundo nivel; poniéndose todas las funcionalidades de la pluralidad de funcionalidades a disposición de la primera aplicación (503) sólo si se ha asignado a dicho estado dicho segundo nivel.

2. El método según la reivindicación 1, en donde el primer protocolo es el protocolo de comunicación de campo cercano (NFC), y el establecimiento del enlace en el primer protocolo se realiza en respuesta a una operación de toque NFC.

3. El método de la reivindicación 1, en donde el segundo protocolo es el protocolo Bluetooth Low Energy.

4. El método según la reivindicación 1 que comprende además:
en respuesta a la detección de un emparejamiento a través del segundo protocolo, determinar, por parte del dispositivo inteligente, el estado de la clave de cifrado de comunicación, e informar al titular de tarjeta proporcionando, por parte del dispositivo inteligente, un mensaje informativo que indica el emparejamiento del elemento seguro y el dispositivo inteligente, así como el estado de la clave de cifrado de comunicación.

5. El método según la reivindicación 4, en donde informar al titular de tarjeta del emparejamiento del elemento seguro y el dispositivo inteligente y del estado de la clave de cifrado de comunicación comprende mostrar el mensaje informativo en el teléfono inteligente.

6. El método según la reivindicación 4, en donde informar al titular de tarjeta del emparejamiento del elemento seguro y el dispositivo inteligente y del estado de la clave de cifrado de comunicación comprende proporcionar, por parte del dispositivo inteligente, un mensaje de voz al titular de tarjeta.

7. El método según la reivindicación 1 que comprende, además:

en respuesta a la realización de una transacción utilizando el elemento seguro y un terminal de punto de venta, determinar el estado de la clave de cifrado de comunicación y, si el estado de la clave de cifrado de comunicación es el segundo nivel, transmitir unos detalles de transacción al dispositivo inteligente por el enlace de segundo protocolo o, de lo contrario, no transmitir ningún detalle de transacción al dispositivo inteligente; y
en respuesta a la recepción, por parte del dispositivo inteligente, de los detalles de transacción, informar al titular de tarjeta de los detalles de transacción proporcionando, por parte del dispositivo inteligente, los detalles de transacción al titular de tarjeta.

8. El método según la reivindicación 7, en donde informar al titular de tarjeta de los detalles de transacción comprende mostrar el mensaje con los detalles de transacción en el dispositivo inteligente.

9. El método según la reivindicación 7, en donde informar al titular de tarjeta de los detalles de transacción comprende proporcionar, por parte del dispositivo inteligente, un mensaje de voz al titular de tarjeta.

10. El método según la reivindicación 1 que comprende, además:
en respuesta a la realización de una transacción utilizando el elemento seguro y un terminal de punto de venta, determinar el estado de la clave de cifrado de comunicación y, a partir del estado de la clave de cifrado de comunicación, unos aspectos concretos de transacción y una política de seguridad, realizar una acción seleccionada de entre proceder con la transacción, impedir la transacción o solicitar una aprobación de la transacción del titular de tarjeta transmitiendo un mensaje de solicitud de aprobación al dispositivo inteligente.

11. Un elemento seguro (107) que tiene un procesador (301) y una memoria de programas, almacenando la memoria de programas unas instrucciones ejecutables por el procesador, incluidas unas instrucciones para hacer que el procesador:

establezca un primer enlace (108) de comunicación en un primer protocolo a un dispositivo inteligente que comprende una primera aplicación (503) que está configurada para proporcionar una pluralidad de funcionalidades en combinación con el elemento seguro;
establecer un enlace (109) de segundo protocolo al dispositivo inteligente;
en respuesta al establecimiento de un primer enlace de comunicación en el primer protocolo, generar una clave de cifrado de comunicación, asociar un estado con la clave de cifrado y asignar al estado un primer nivel;
transmitir al dispositivo inteligente en el primer enlace de comunicación un mensaje que encapsula la clave de cifrado de comunicación y el estado de la clave de cifrado de comunicación; autorizando dicha clave de cifrado de comunicación a la primera aplicación (503) a proporcionar menos de todas las funcionalidades de la pluralidad de funcionalidades sólo si se ha asignado a dicho estado dicho primer nivel,
transmitir al dispositivo inteligente un mensaje cifrado usando la clave de cifrado de comunicación por el segundo enlace de comunicación;
realizar una autenticación de usuario de un titular de tarjeta del elemento seguro comprobando unos datos de identificación personal proporcionados por el titular de tarjeta a través de un dispositivo físico enlazado al elemento seguro;
en respuesta a una verificación satisfactoria de la autenticación de usuario realizada del titular de tarjeta del elemento seguro, subir el estado de la clave de cifrado de comunicación del primer nivel a un segundo nivel y enviar el estado modificado al dispositivo inteligente; poniéndose todas las funcionalidades de la pluralidad de funcionalidades a disposición de la primera aplicación (503) sólo si se ha asignado a dicho estado dicho segundo nivel.

12. El elemento seguro según la reivindicación 11, en donde las instrucciones incluyen además unas instrucciones para hacer que el procesador:
en respuesta a detectar un emparejamiento a través del segundo protocolo, determine el estado de la clave de cifrado de comunicación, y transmita al dispositivo inteligente un mensaje informativo que indique el estado de la clave de cifrado de comunicación.

13. El elemento seguro según la reivindicación 11, en donde las instrucciones incluyen además unas instrucciones para hacer que el procesador:
en respuesta a la realización de una transacción utilizando el elemento seguro y un terminal de punto de venta, determine el estado de la clave de cifrado de comunicación y, si el estado de la clave de cifrado de comunicación es el segundo nivel, transmita unos detalles de transacción al dispositivo inteligente por el enlace de segundo protocolo o, de lo contrario, no transmita ningún detalle de transacción al dispositivo inteligente.

14. El elemento seguro según la reivindicación 11, en donde las instrucciones incluyen además unas instrucciones para hacer que el procesador:
en respuesta a la realización de una transacción utilizando el elemento seguro y un terminal de punto de venta, determine el estado de la clave de cifrado de comunicación y, a partir del estado de la clave de cifrado de comunicación, unos aspectos concretos de transacción, y una política de seguridad, realice una acción seleccionada de entre proceder con la transacción, impedir la transacción, solicitar una aprobación de la transacción del titular de tarjeta transmitiendo un mensaje de solicitud de aprobación al dispositivo inteligente.

15. Un sistema que comprende el elemento seguro de la reivindicación 11 y el dispositivo inteligente de la reivindicación 11, en donde dicho dispositivo inteligente es un teléfono inteligente.

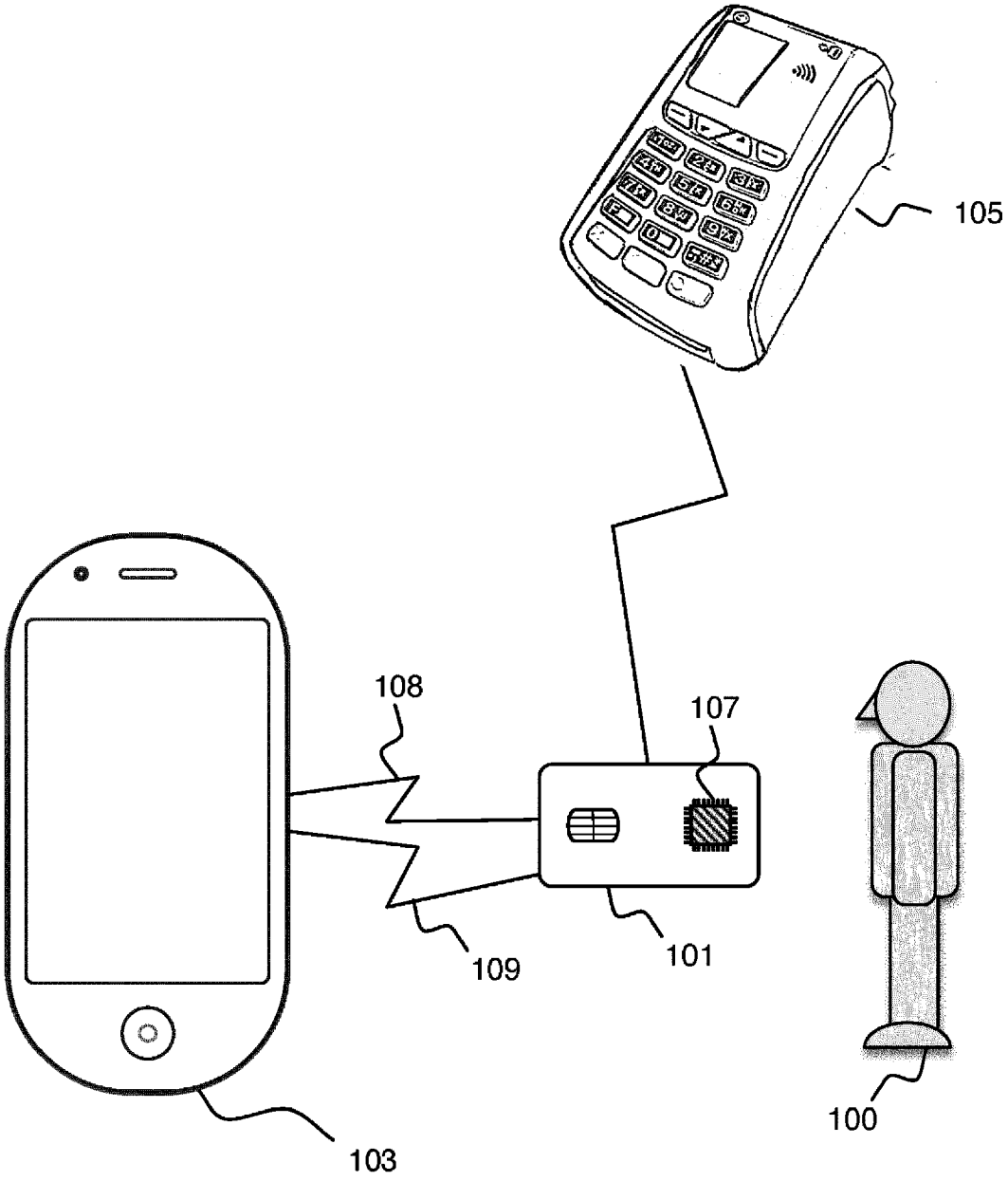

Figura 1

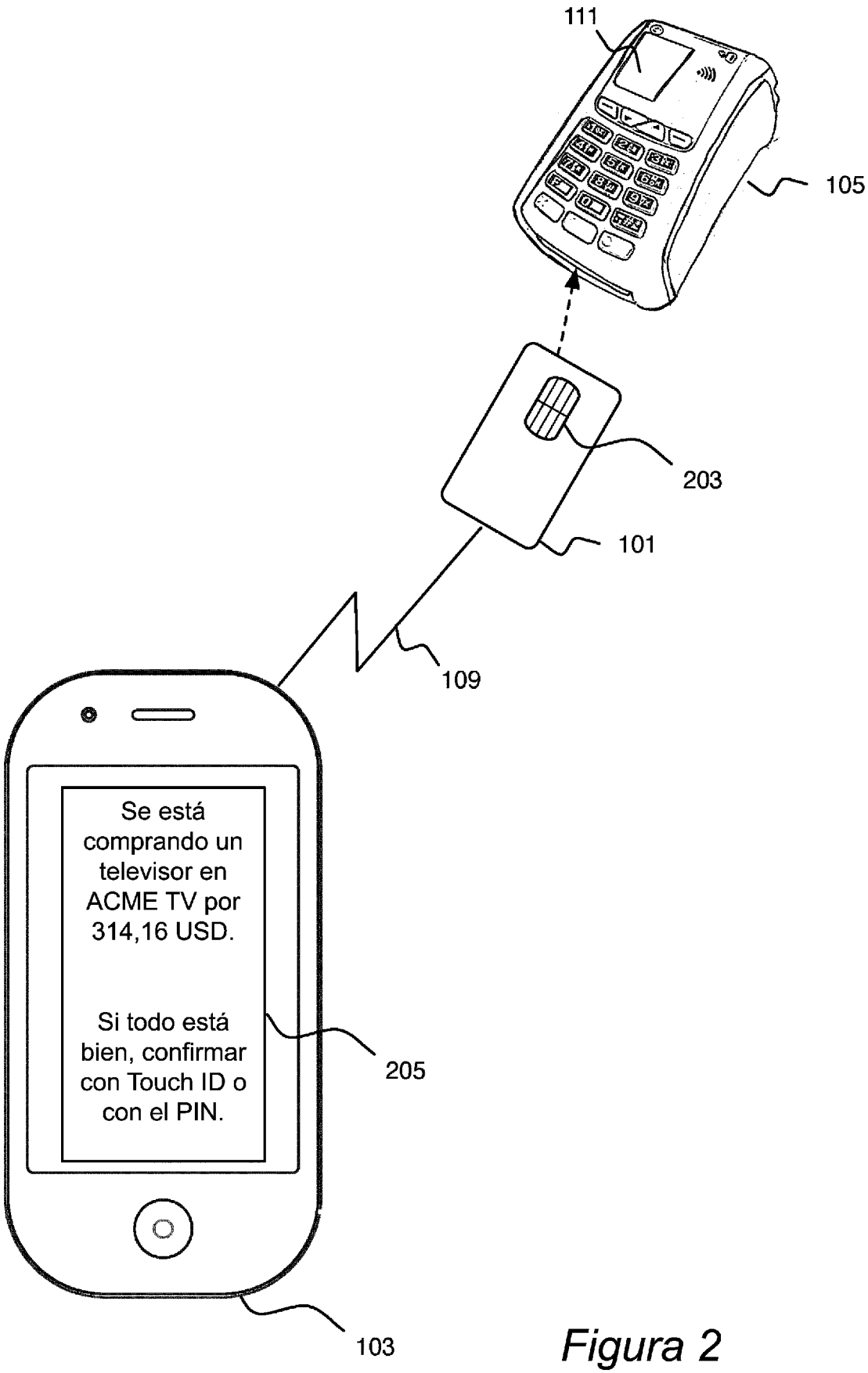
111
105
203
101
109
Se está comprando un televisor en ACME TV por 314,16 USD.
Si todo está bien, confirmar con Touch ID o con el PIN.
205
103

Figura 2

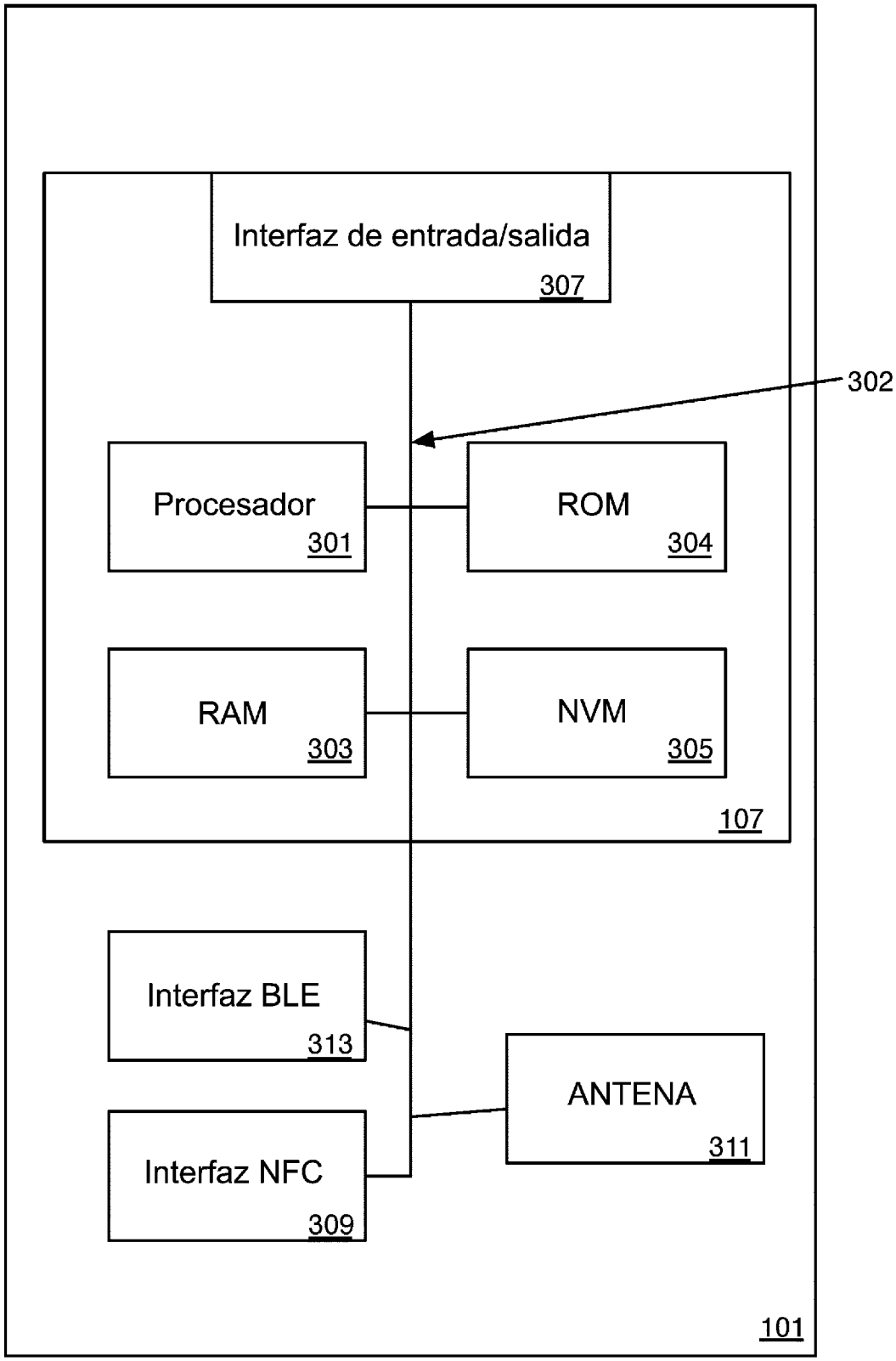
Interfaz de entrada/salida
307
302
Procesador
301
ROM
304
RAM
303
NVM
305
107
Interfaz BLE
313
ANTENA
311
Interfaz NFC
309
101

Figura 3

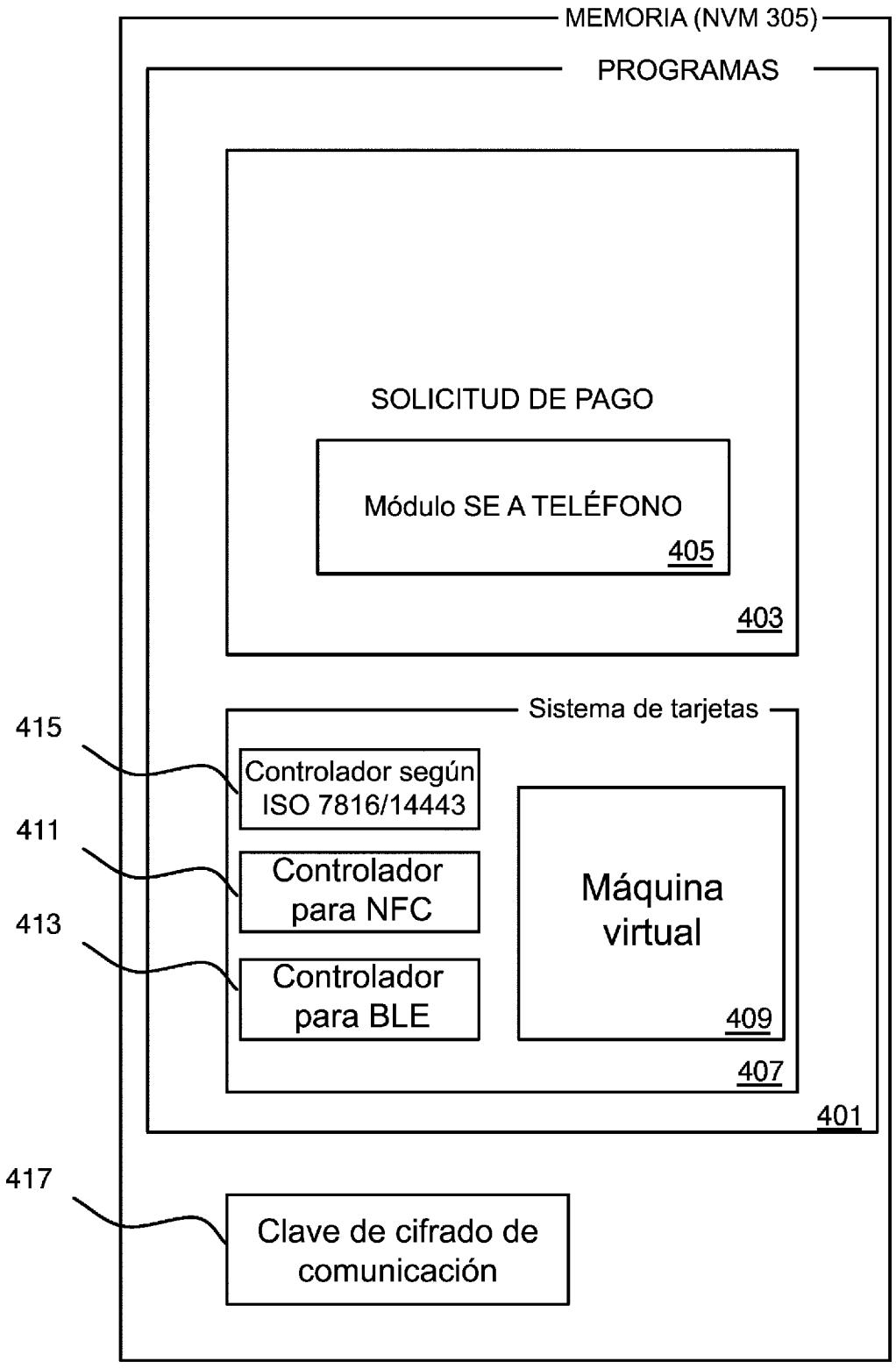
MEMORIA (NVM 305)
PROGRAMAS
SOLICITUD DE PAGO
Módulo SE A TELÉFONO
405
403
Sistema de tarjetas
415
Controlador según ISO 7816/14443
411
Controlador para NFC
413
Controlador para BLE
Máquina virtual
409
407
401
417
Clave de cifrado de comunicación

Figura 4

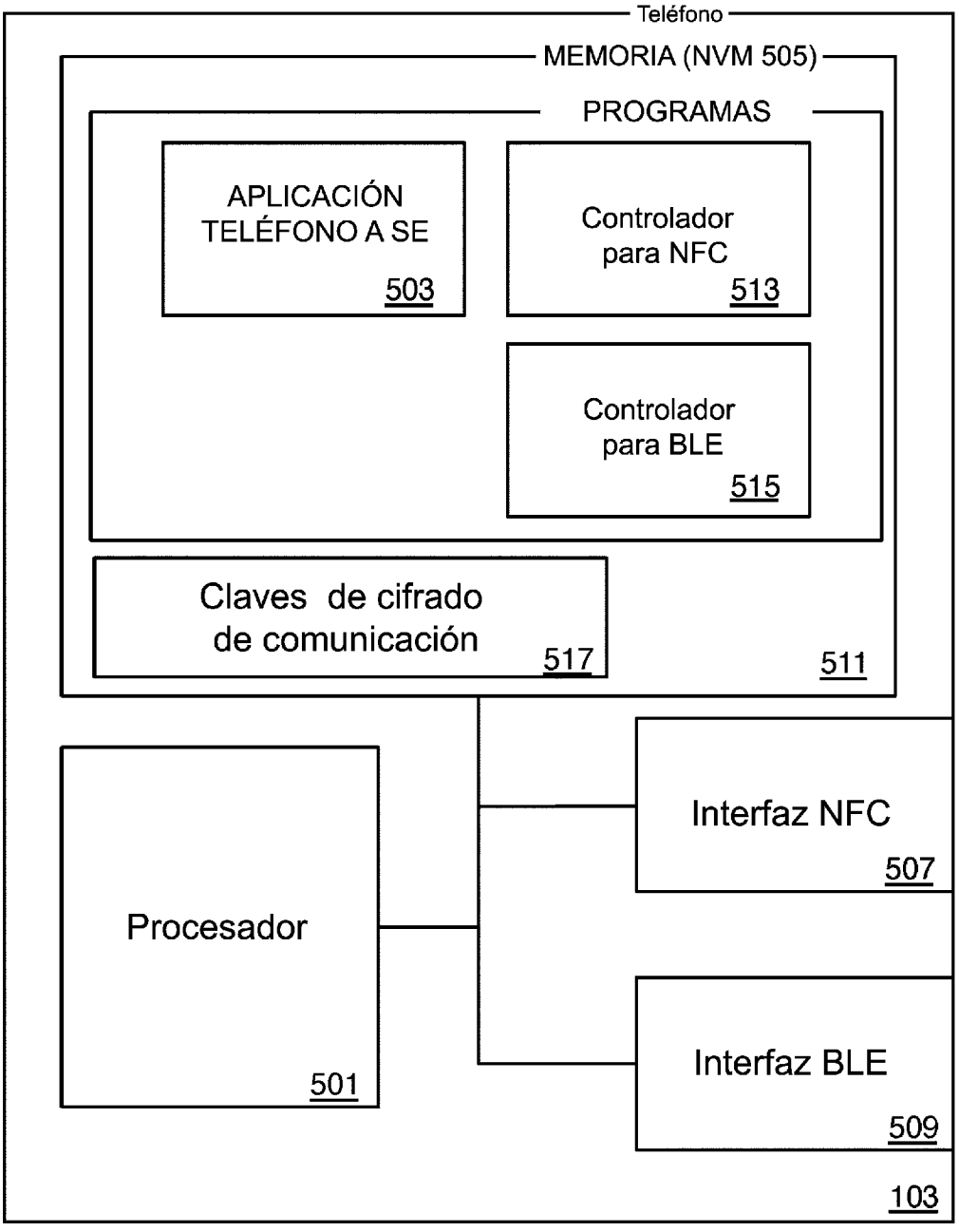
Teléfono
MEMORIA (NVM 505)
PROGRAMAS
APLICACIÓN TELÉFONO A SE
503
Controlador para NFC
513
Controlador para BLE
515
Claves de cifrado de comunicación
517
511
Procesador
501
Interfaz NFC
507
Interfaz BLE
509
103

Figura 5

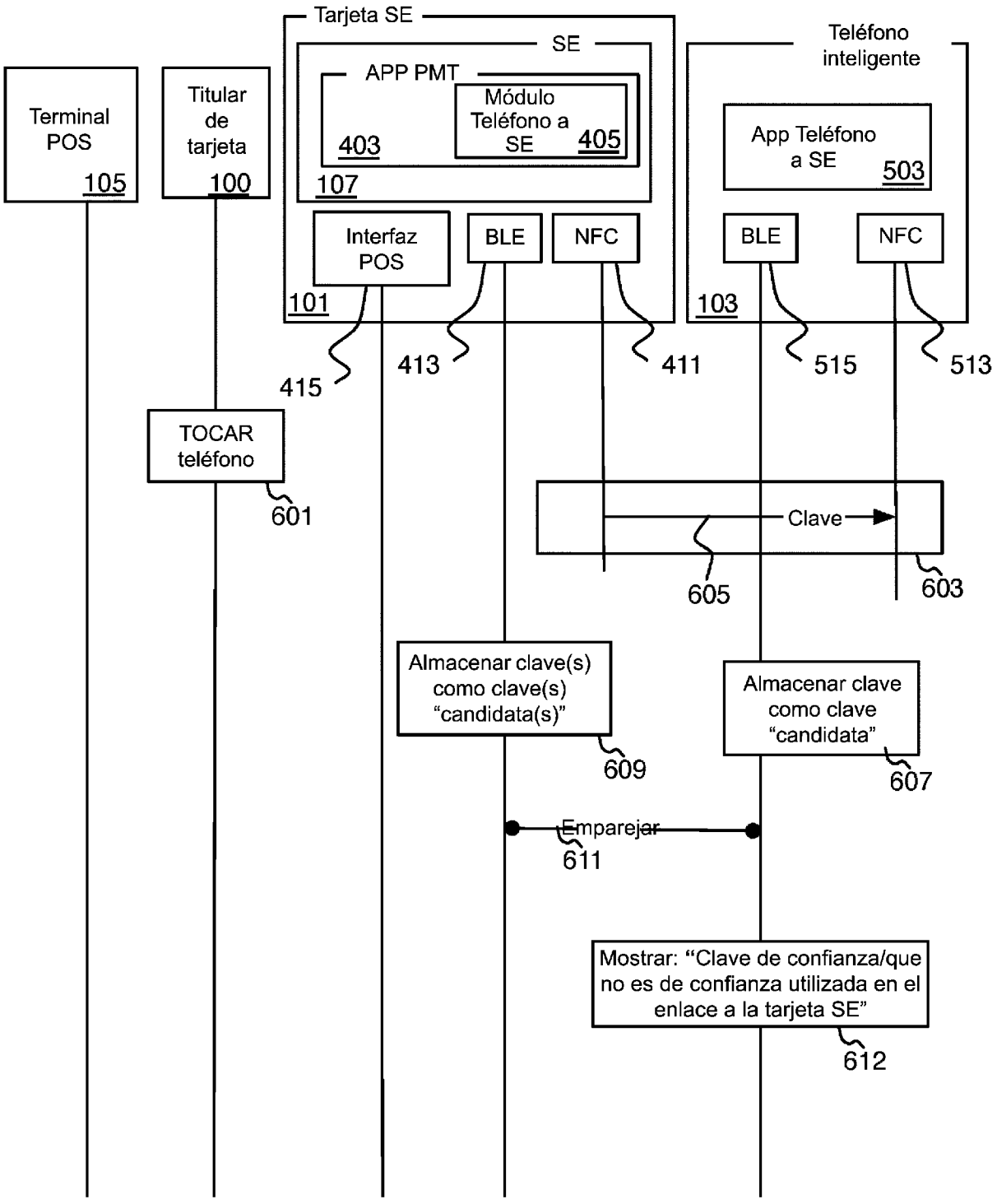
Tarjeta SE
SE
APP PMT
Módulo Teléfono a SE
405
403
107
Interfaz POS
BLE
NFC
101
Teléfono inteligente
App Teléfono a SE
503
BLE
NFC
103
Terminal POS
105
Titular de tarjeta
100
415
413
411
515
513
TOCAR teléfono
601
Clave
605
603
Almacenar clave(s) como clave(s) "candidata(s)"
609
Almacenar clave como clave "candidata"
607
Emparejar
611
Mostrar: "Clave de confianza/que no es de confianza utilizada en el enlace a la tarjeta SE"
612

Figura 6

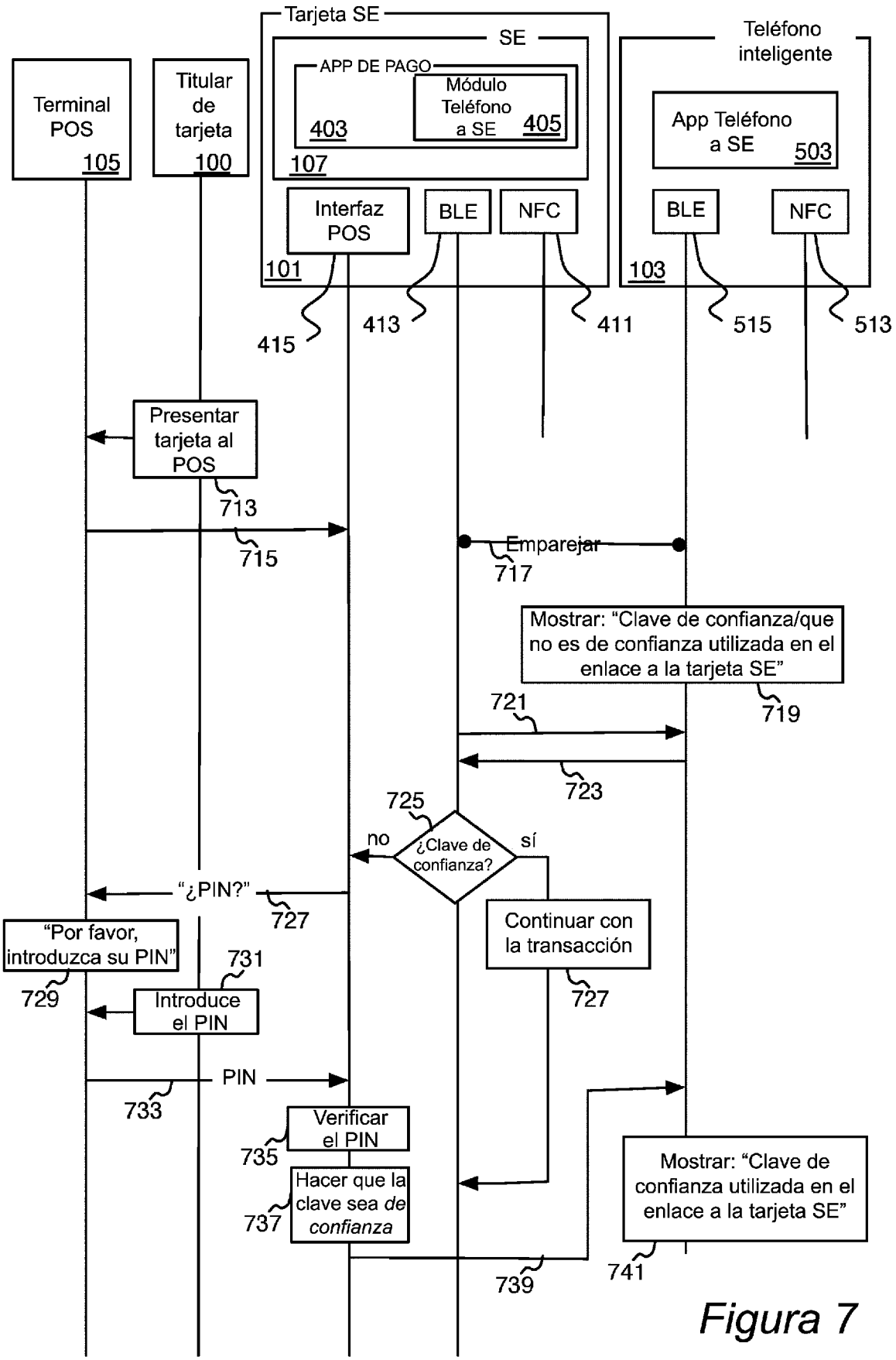
Tarjeta SE
SE
APP DE PAGO
Módulo Teléfono a SE
405
403
107
Interfaz POS
BLE
NFC
101
Teléfono inteligente
App Teléfono a SE
503
BLE
NFC
103
Terminal POS
105
Titular de tarjeta
100
415
413
411
515
513
Presentar tarjeta al POS
713
715
Emparejar
717
Mostrar: "Clave de confianza/que no es de confianza utilizada en el enlace a la tarjeta SE"
719
721
723
725
¿Clave de confianza?
no
sí
"¿PIN?"
727
Continuar con la transacción
727
"Por favor, introduzca su PIN"
729
731
Introduce el PIN
PIN
733
Verificar el PIN
735
Hacer que la clave sea de confianza
737
739
Mostrar: "Clave de confianza utilizada en el enlace a la tarjeta SE"
741

Figura 7