(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 792 986**

(51) Int. CI.:

H04L 9/32 (2006.01)
G07F 7/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **17.09.2015 E 15306450 (6)**

(97) Fecha y número de publicación de la concesión europea: **15.04.2020 EP 3145116**

(54) Título: **Método y sistema para comunicación de un terminal con un elemento seguro**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.11.2020

(73) Titular/es:

IDEMIA FRANCE (100.0%)
2, Place Samuel de Champlain
92400 Courbevoie, FR

(72) Inventor/es:

CHAMBEROT, FRANCIS y
CLIMEN, BRUNO

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método y sistema para comunicación de un terminal con un elemento seguro

Antecedentes

En varios protocolos de comunicación se utiliza un intercambio desafío-respuesta entre las partes. La Figura 1 muestra un ejemplo sencillo. Alice envía a Bob un desafío 2 como, por ejemplo, un mensaje que contiene la cadena de caracteres “MQR”. Bob transforma esta cadena que utiliza un algoritmo criptográfico, T, con una clave, k: T(“MQR”, k) para obtener una respuesta “SAT”, por ejemplo. Bob le envía a Alice la respuesta 3. Alice ejecuta el mismo algoritmo con su copia de la clave, k’: T(“MQR”, k’). Si Alice obtiene el mismo resultado que la respuesta de Bob, “SAT”, comprueba que Bob tiene una copia de su clave, k’. Cuando se encuentra una coincidencia, se puede decir que la respuesta corresponde al desafío. Este tipo de intercambio encuentra aplicación en muchos protocolos de autenticación. Para cualquier desafío dado únicamente existe una respuesta que correspondiente.

Las Tarjetas de Circuitos Integrados (ICC) pueden utilizar un intercambio desafío-respuesta como parte de un intercambio de comunicación entre la tarjeta y un terminal.

El documento EP 2711903 divulga un método para gestionar y confirmar la transacción de forma segura.

El documento US 2014/0164771 divulga un método para gestionar un elemento seguro embebido.

Resumen

De acuerdo con la presente invención, se proporcionan métodos y dispositivos de acuerdo con las reivindicaciones independientes 1, 7, 8 y 12.

Un aspecto de la divulgación proporciona un método de comunicación entre un terminal y un elemento seguro que comprende, en el elemento seguro:

determinar un desafío;

enviar el desafío al terminal;

recibir una respuesta del terminal que comprende el desafío y datos de un número de identificación personal, PIN, estando la respuesta encriptada con una clave;

determinar si el desafío recibido en la respuesta coincide con el desafío enviado al terminal; y

si el desafío recibido en la respuesta no coincide con el desafío enviado al terminal, comprende además:

ejecutar un cálculo utilizando el desafío recibido y el desafío enviado; y

recuperar un elemento de datos transportado por la respuesta, en donde el elemento de datos indica una acción para ser ejecutada por el elemento seguro.

Realizar el cálculo puede comprender la ejecución de una operación entre bits con el desafío recibido y el desafío enviado.

La operación entre bits puede ser una operación OR exclusivo, XOR.

El elemento de datos puede ser un código de operación que indica una acción de seguridad a realizar por parte del elemento seguro. El método puede comprender, además, realizar una acción de seguridad en función del valor del código de operación.

El elemento de datos puede ser un código de operación encriptado. La encriptación del código de operación es diferente de la encriptación de la respuesta recibida desde el terminal.

El método puede comprender desencriptar la respuesta antes de determinar si el desafío recibido en la respuesta coincide con el desafío enviado al terminal.

El método se puede ejecutar como parte de una transacción fuera de línea.

Otro aspecto de la divulgación proporciona un método de comunicación entre un terminal y un elemento seguro que comprende, en el terminal:

recibir un desafío desde el elemento seguro;

determinar si es necesario enviar un elemento de datos al elemento seguro;

si no es necesario enviar un elementos de datos al elemento seguro, enviar una respuesta encriptada al elemento seguro, comprendiendo la respuesta el desafío y los datos del número de identificación personal, PIN; y

si es necesario enviar un elemento de datos al elemento seguro:

realizar un cálculo del desafío con el elemento de datos para obtener un desafío modificado; y

enviar una respuesta encriptada al elemento seguro, comprendiendo la respuesta el desafío modificado y los datos del número de identificación personal, PIN, en donde el elemento seguro puede recuperar el elemento de datos a partir del desafío modificado, y el elemento de datos indica una acción a ejecutar por parte del elemento seguro.

La determinación de si es necesario enviar un elemento de datos al elemento seguro puede comprender determinar si el número del elemento seguro se encuentra en una lista negra de números, y si el número del elemento seguro se encuentra en una lista negra de números, enviar un elemento de datos que indica una acción para bloquear el elemento seguro.

Otro aspecto de la divulgación proporciona un elemento seguro que comprende un procesador, una memoria y una interfaz de comunicaciones, conteniendo la memoria instrucciones ejecutables por parte del procesador para hacer que el procesador:

determine un desafío;

envíe el desafío a un terminal a través de una interfaz de comunicaciones;

reciba una respuesta desde el terminal que comprende el desafío y datos del número de identificación personal, PIN, estando la respuesta encriptada con una clave;

determine si el desafío recibido en la respuesta se corresponde con el desafío enviado al terminal; y

si el desafío recibido en la respuesta no se corresponde con el desafío enviado al terminal, las instrucciones hacen que el procesador, además:

realice un cálculo utilizando el desafío recibido y el desafío enviado; y

recupere un elemento de datos incluido en la respuesta, en donde el elemento de datos indica una acción a realizar por parte del elemento seguro.

El cálculo puede ser una operación entre bits con el desafío recibido y el desafío enviado.

El elemento de datos puede ser un código de operación que indica una acción de seguridad a realizar por parte del elemento seguro, y las instrucciones pueden hacer que el procesador ejecute la acción de seguridad en función del valor del código de operación.

El elemento de datos puede ser un código de operación encriptado.

Otro aspecto de la divulgación proporciona un terminal que comprende un procesador, una memoria y una interfaz de comunicaciones, conteniendo la memoria instrucciones ejecutables por parte del procesador para hacer que el procesador:

reciba un desafío desde un elemento seguro;

determine si es necesario enviar un elemento de datos al elemento seguro;

si no es necesario enviar un elementos de datos al elemento seguro, envíe una respuesta encriptada al elemento seguro, comprendiendo la respuesta el desafío y los datos del número de identificación personal, PIN; y

si es necesario enviar un elemento de datos al elemento seguro:

realice un cálculo del desafío con el elemento de datos para obtener un desafío modificado; y

envíe una respuesta encriptada al elemento seguro, comprendiendo la respuesta el desafío modificado y los datos del número de identificación personal, PIN, en donde el elemento seguro puede recuperar el elemento de datos a partir del desafío modificado, y el elemento de datos indica una acción a ejecutar por parte del elemento seguro.

Las instrucciones que hacen que el procesador determine si es necesario enviar un elemento de datos al elemento seguro pueden hacer que el procesador determine si el número del elemento seguro se encuentra en una lista negra de números, y si el número del elemento seguro se encuentra en una lista negra de números, envíe un elemento de datos que indica una acción para bloquear el elemento seguro.

El elemento seguro puede comprender un microprocesador con memoria no volátil para almacenar una aplicación y las claves criptográficas asociadas. El elemento seguro se puede comunicar con un terminal a través de varias APDU ISO 7816. El elemento seguro puede comprender elementos hardware para ejecutar algoritmos criptográficos como, por ejemplo, algoritmos criptográficos simétricos y asimétricos. El elemento seguro se puede embeber en una tarjeta con formato ISO 7810 como, por ejemplo, una tarjeta con formato ID-1 (por ejemplo, utilizada típicamente para tarjetas de banco y tarjetas de crédito/débito) o una tarjeta con formato ID-000 (por ejemplo, utilizada típicamente para tarjetas SIM). El elemento seguro se puede embeber directamente en una placa de circuitos como, por ejemplo, una placa de circuitos de un teléfono móvil.

La funcionalidad descrita aquí se puede implementar mediante hardware, software ejecutado por un equipo de procesamiento, o mediante una combinación de hardware y software. El equipo de procesamiento puede comprender un ordenador, un procesador, una máquina de estados, un matriz lógica o cualquier otro equipo de procesamiento apropiado. El equipo de procesamiento puede ser un procesador de propósito general que ejecuta un software que hace que el procesador de propósito general realice las tareas necesarias, o el equipo de procesamiento puede estar dedicado a realizar las funciones necesarias. Otro aspecto de la invención proporciona instrucciones legibles por una máquina (software) que, cuando son ejecutadas por un procesador, realizan cualquiera de los métodos descritos o reivindicados. Las instrucciones legibles por una máquina se pueden almacenar en un dispositivo de memoria electrónica, un disco duro, un disco óptico u otro medio de almacenamiento legible por una máquina. El medio legible por una máquina puede ser un medio no transitorio legible por una máquina. El término “medio no transitorio legible por una máquina” comprende todos los medios legibles por una máquina excepto una señal transitoria que se propaga. Las instrucciones legibles por una máquina se pueden descargar al medio de almacenamiento mediante una conexión de red.

Una ventaja de al menos un ejemplo de la divulgación es que en el momento de enviar la respuesta el terminal puede enviar datos adicionales al elemento seguro. El elemento de datos se puede utilizar para transportar información, o un comando, que puede ordenarle al elemento seguro que ejecute una acción como, por ejemplo, una acción relacionada con la seguridad para bloquear el elemento seguro. Los datos adicionales se pueden enviar sin aumentar la longitud del mensaje que transporta la respuesta, haciendo de este modo que el método sea compatible con los sistemas existentes.

Breve descripción de los dibujos

Los modos de realización de la invención se describirán, únicamente a modo de ejemplo, haciendo referencia a los dibujos adjuntos, en los que:

la Figura 1 muestra un intercambio desafío-respuesta;

la Figura 2 muestra un ejemplo de intercambio de comunicación entre un terminal y un elemento seguro;

la Figura 3 muestra un método ejecutado en el elemento seguro;

las Figuras 4A y 4B muestran dos ejemplos de procesamiento de mensajes en un terminal;

las Figuras 5A y 5B muestran dos ejemplos de procesamiento de mensajes en un terminal;

la Figura 6 muestra una tabla almacenada en el elemento seguro;

la Figura 7 muestra una tabla almacenada en el terminal;

la Figura 8 muestra una tarjeta de circuito integrado (ICC), un terminal y una entidad de autorización que se pueden utilizar para implementar uno de los métodos;

la Figura 9 muestra un equipo para una implementación basada en un ordenador.

Descripción detallada

La Figura 2 muestra un ejemplo de un método de comunicación realizado entre un elemento seguro 10, un terminal 20 y una entidad 30 de autorización. La siguiente descripción utiliza una tarjeta de circuito integrado (ICC) como ejemplo ilustrativo de una entidad que comprende un elemento seguro. Otro término para “tarjeta de circuito integrado” (ICC) es una tarjeta chip. El elemento seguro en la tarjeta puede soportar aplicaciones de pago como, por ejemplo, una aplicación de pago de crédito y/o una aplicación de pago de débito. La tarjeta 10 puede ser conforme con las Especificaciones de Europay, MasterCard y Visa (EMV). El terminal 20 también se puede denominar lector de tarjetas. El terminal se puede proporcionar en un punto de venta (TPV) de un comercio. La entidad 30 de autorización puede ser un banco, un emisor de tarjetas, o alguna otra entidad que autorice transacciones de tarjeta en nombre del emisor de tarjetas.

En 100, la entidad 30 de autorización le envía al terminal una lista de detalles de tarjeta que identifican ciertas tarjetas. Esta lista se puede denominar lista negra. La lista negra identifica tarjetas que no deberían autorizarse si se presentan en el terminal para una transacción. El terminal 20 puede utilizar la lista negra cuando procesa transacciones fuera de línea o transacciones en línea. Una transacción fuera de línea es una transacción en la que el terminal no se comunica con una entidad 30 de autorización antes de autorizar la transacción en el terminal. Una transacción en línea es una transacción en la que el terminal se comunica con la entidad 30 de autorización para recibir una autorización, o una denegación, de la entidad 30 de autorización antes de proceder a aceptar o denegar la transacción en el terminal. Las tarjetas identificadas en la lista negra pueden ser tarjetas que los propietarios de las mismas han notificado como robadas. Por ejemplo, una tarjeta puede haber sido robada y al emisor de la tarjeta le gustaría a continuación bloquear la tarjeta para que no pueda hacer más transacciones. La entidad 30 de autorización puede identificar números de cuenta principales sospechosos de otras formas como, por ejemplo, a partir de patrones de transacciones fraudulentas, registros de tarjetas robadas o perdidas, o de parámetros de seguridad recuperados de la tarjeta durante transacciones anteriores. En el terminal se almacena 102 la lista enviada al terminal 20. Tal como se describirá de forma más detallada, la lista enviada al terminal también puede incluir una pareja de detalles de tarjeta y un código de operación (u otro elemento de datos) para enviar a la tarjeta junto con los detalles de tarjeta especificados.

La comunicación entre el terminal 20 y la tarjeta 10 comprende una etapa 110 de autenticación de tarjeta y una etapa 120 de verificación de PIN. En la etapa 110 de autenticación de tarjeta, el terminal 20 se comunica con la tarjeta para obtener los detalles de la misma. La tarjeta 10 puede soportar más de una aplicación de pago como, por ejemplo, una aplicación de débito y una aplicación de crédito. La tarjeta 10 puede soportar una comunicación basada en contacto y/o una comunicación sin contacto. El terminal 20 empieza seleccionando un ‘punto de entrada’. La tarjeta 10 responde con una lista de las aplicaciones soportadas por la tarjeta. A continuación, el terminal 20 selecciona una aplicación específica de la lista. En los intercambios que siguen, el lector recibe una indicación de los ficheros que es necesario leer para completar la transacción. Como parte de la etapa 111 de autenticación de tarjeta, el lector recupera el PAN (Número de Cuenta Principal) de la tarjeta y la Fecha de Caducidad de la tarjeta 10.

A continuación, el método continúa con la etapa 120 de verificación de PIN. Cuando un usuario hace una transacción el terminal le solicita al usuario que introduzca un Número de Identificación Personal (PIN) en el teclado numérico del terminal 20. Típicamente, una pantalla del terminal 20 muestra un mensaje que solicita al usuario que introduzca su PIN. El PIN se envía a la tarjeta 10. Se verifica el usuario comparando el PIN recibido desde el terminal 20 con el PIN almacenado de forma segura en la tarjeta 10. Si el PIN se ha introducido correctamente, el método puede continuar con una etapa de autorización de transacción (no se muestra). Tal como se ha explicado más arriba, la transacción se puede autorizar en línea, mediante una comunicación entre la tarjeta 10 y el terminal 20 (y una entidad 30 de autorización). La tarjeta recibe una respuesta que autoriza la transacción o rechaza la transacción. Alternativamente, la transacción se puede autorizar fuera de línea. El terminal puede almacenar reglas que determinen cuando puede realizar una autorización de transacción fuera de línea. Por ejemplo, una regla puede indicar la máxima cantidad monetaria de una transacción que se puede autorizar fuera de línea. La etapa 120 de verificación de PIN se describirá en detalle a continuación.

El terminal 20 utiliza encriptación cuando le comunica a la tarjeta 10 los datos del PIN. La tarjeta 10 tiene una clave pública y una clave privada. El terminal 20 puede utilizar la clave pública de la tarjeta para encriptar los datos enviados a la tarjeta 10. Las claves y los certificados se describen en las especificaciones de EMV en la sección 7.1 del Libro 2 de la EMV 4.3. El Cifrado y la Verificación del PIN se describen en las especificaciones de EMV en la sección 7.2 del Libro 2 de la EMV 4.3. El terminal solicita 121 un “desafío” de la tarjeta 10. El desafío es una cadena aleatoria. En las especificaciones de EMV el desafío se describe como “un número impredecible”. La tarjeta 10 le envía al terminal 20 el desafío 122.

En un método convencional de verificación de PIN, el terminal forma a continuación un mensaje encriptado que incluye los datos del PIN y le envía el mensaje a la tarjeta. En algunos ejemplos de esta divulgación, en esta etapa el terminal 20 puede enviar datos adicionales. En 123, el terminal 20 determina si es necesario enviar datos a la tarjeta 10. El terminal determina si la tarjeta se encuentra en la lista negra. El terminal puede comparar los detalles de la tarjeta (por

ejemplo, el número de tarjeta, la fecha de caducidad) obtenidos durante la etapa 110 de autenticación de tarjeta con los detalles de tarjeta en la lista negra recibida en 100. Si los detalles de tarjeta coinciden, entonces la tarjeta debería bloquearse. Esto es, la transacción actual se debería denegar. El terminal puede hacer que la tarjeta se bloquee para transacciones futuras comunicándose con la tarjeta.

Si en el bloque 123 se determina que la tarjeta no se encuentra en la lista negra, entonces en 124 se le puede enviar de forma normal a la tarjeta 10 los datos de PIN encriptados. Si en el bloque 123 se determina que la tarjeta se encuentra en la lista negra, entonces se le puede enviar a la tarjeta 10 un tipo modificado de mensaje con los datos de PIN encriptados. El mensaje se prepara en el bloque 126 y se le envía a la tarjeta en 127. El mensaje modificado de datos de PIN puede incluir un código de operación (OPCODE) 125. Por ejemplo, el opcode puede ordenarle a la tarjeta que bloquee la tarjeta para futuras transacciones.

La Figura 3 muestra un método en la tarjeta 10. La tarjeta 10 bien recibe un mensaje convencional 124 de datos de PIN encriptados, o bien un mensaje modificado 126 de datos de PIN encriptados, donde el mensaje 126 incluye datos adicionales. En el bloque 130 el mensaje (124 ó 126) de datos de PIN se desencripta utilizando la clave 131 de tarjeta. El mensaje 124, 126 se encripta utilizando la clave pública de la tarjeta. La clave 131 es la clave privada correspondiente de la tarjeta. El bloque 132 determina si el desafío (enviado en 122, Fig. 2) se corresponde con el desafío recibido desde el terminal. Si el desafío no se corresponde entonces existen varias razones posibles: (i) el terminal 20 ha enviado un mensaje modificado de tipo 126 que incluye datos adicionales, combinados con el desafío; o (ii) el mensaje no se ha encriptado correctamente. Por ejemplo, se ha utilizado una clave incorrecta para encriptar el mensaje. El bloque 133 comprueba la presencia de datos en el mensaje recibido. El bloque 133 utiliza como entradas el desafío 143 recibido extraído del mensaje 126 recibido y el desafío 122 enviado. El bloque 133 genera un opcode 136. El opcode 136 se puede comparar con una tabla de posibles opcodes almacenada. Si se encuentra una correspondencia, en el bloque 137 se utiliza el opcode, o una instrucción correspondiente al opcode. Si no se encuentra una correspondencia para el opcode 136, entonces el mensaje 124, 126 se puede haber encriptado de forma incorrecta.

Las Figuras 4A, 4B y 5A, 5B muestran más detalle sobre cómo el terminal 20 y la tarjeta 10 procesan los mensajes 124, 126. Las Figuras 4A, 4B muestran el procesamiento de los mensajes 124, 126 en el terminal 20. Los datos 140 a cifrar para el cifrado del PIN comprenden:

una cabecera 141 de datos (por ejemplo, longitud 1 byte, valor hexadecimal ‘7F’);

un bloque PIN 142 (por ejemplo, longitud 8 bytes);

un desafío, también denominado número impredecible ICC (por ejemplo, longitud 8 bytes);

relleno aleatorio.

El relleno aleatorio tiene una longitud de $N_{IC} – 17$ bytes, donde N_{IC} es la longitud total de la clave pública utilizada para el cifrado. El bloque PIN es una forma codificada del PIN, descrita en la sección 6.5.12 del Libro 2 del EMV 4.3. El bloque PIN puede incluir: un campo de control; un campo que indica la longitud del PIN; los dígitos del PIN; campos de datos de relleno. Los campos de datos listados anteriormente y las longitudes de campos de ejemplo se describen en las especificaciones de EMV. Se debería entender que los datos 140 enviados a la tarjeta pueden incluir uno o más campos de datos adicionales, o podrían omitir ciertos campos de datos mencionados anteriormente como, por ejemplo, el relleno. Las longitudes de los campos de datos mencionadas anteriormente son únicamente valores de ejemplo.

La Figura 4A muestra un procesamiento para crear un mensaje convencional 124 de PIN sin datos adicionales. Los datos 140 se encriptan 147 con la clave pública 148 de la tarjeta para formar el mensaje 124 de datos PIN encriptados.

La Figura 4B muestra el procesamiento para crear un mensaje modificado 126 de PIN con datos adicionales. Los datos 140 se combinan con los datos adicionales 145. Se realiza una operación lógica booleana entre los datos 140 y los datos adicionales 145. La operación lógica booleana puede ser una operación OR exclusivo (XOR). Los datos adicionales 145 están alineados con el desafío 143. La razón para este alineamiento es porque el desafío es el único valor de datos conocido por la tarjeta 10. El resto de datos 142, 144 son desconocidos por la tarjeta 10 y no se pueden utilizar para comprobar (Figura 3, 133) si el mensaje incluye datos adicionales. En un ejemplo EMV el campo desafío tiene una longitud de 8 bytes. Si los datos 145 a combinar con los datos 140 tienen una longitud menor de 8 bytes, entonces el terminal puede alinear los datos 145 con el inicio del campo desafío 143, un extremo del campo desafío 143, o cualquier otra alineación conocida tanto por el terminal 20 como por la tarjeta 10 de forma que se pueda comprobar de forma fiable si el mensaje recibido contiene datos adicionales. Los datos generados por el bloque 146 se encripta 147 con la clave pública 148 de la tarjeta para formar el mensaje modificado 126 de datos PIN encriptados.

Las Figuras 5A, 5B muestran el procesamiento de mensajes 124, 126 en el terminal 20. La Figura 5A muestra el procesamiento de un mensaje convencional 124 de PIN encriptado sin datos adicionales. Los datos 124 de PIN

encriptado se desencriptan 151 con la clave privada 152 de la tarjeta para obtener los datos 140 del PIN desencriptado. El desafío 143 recibido se compara con el desafío 122 enviado. Si el desafío 143 recibido coincide con el desafío 122 enviado, entonces el mensaje no transporta datos adicionales.

La Figura 5B muestra el procesamiento de un mensaje modificado 126 de PIN encriptado con datos adicionales. Los datos 126 de PIN encriptado se desencriptan 151 con la clave privada 152 de la tarjeta para obtener los datos del PIN desencriptado. Los datos del PIN desencriptado comprenden una cabecera 141, un bloque PIN 142 y un relleno aleatorio 144. Los datos del PIN desencriptado también comprenden un campo 155 que transporta una combinación del desafío 122 enviado y datos adicionales (opcode 145, Figura 5B). Se ejecuta una operación lógica 158 (por ejemplo, un XOR booleano) entre el campo 155 del desafío modificado y el desafío 122 enviado. El opcode 136 generado por la operación 158 se compara con uno de los opcodes almacenados en la tarjeta 10.

Tal como se ha descrito más arriba, se puede ejecutar el método de envío de datos de PIN junto con un procesamiento de transacciones fuera de línea o un procesamiento de transacciones en línea. El método es particularmente ventajoso con el procesamiento de transacciones fuera de línea ya que proporciona una forma de enviar datos adicionales a la tarjeta (por ejemplo, para bloquear la tarjeta) lo cual no es posible de forma convencional.

La Figura 6 muestra una tabla de ejemplo que se puede almacenar en la tarjeta 10. La tabla se puede grabar en la tarjeta como parte del proceso de personalización de la tarjeta. Las operaciones – definidas por códigos de operación OPn – se pueden considerar puntos de entrada a procedimientos a ser ejecutados por la tarjeta. Los valores almacenados en la columna del código de operación se corresponden con los valores encontrados por el bloque 133, Figura 3.

Las operaciones definidas por los códigos de operación OPn pueden estar asociadas con la seguridad de la tarjeta. Pueden representar comandos de la Unidad de Datos del Protocolo de Aplicación (APDU) ISO 7816 definidos en el estándar de EMV. Pueden representar acciones para los que no existe un comando APDU como, por ejemplo, bloquear una aplicación de pago, o bloquear todas las aplicaciones en la tarjeta, o conmutar la tarjeta de una Autenticación de Datos Estática (SDA) a una Autenticación de Datos Dinámica (DDA) o una Autenticación de Datos Combinada (CDA).

La tarjeta 10 está equipada con medios para ejecutar comandos que se reciben sobre una interfaz de E/S en forma de APDU. Si, por ejemplo OP1, se corresponde con uno de estos comandos, entonces el 'punto de entrada' proporciona los medios para que el programa que ejecuta estas operaciones adicionales ejecute un comando de tarjeta llamándolo internamente en lugar de mediante una APDU.

En los casos en los que el OPn no se corresponda con un comando que se puede llamar mediante una APDU, el 'punto de entrada' puede: proporcionar los medios para llamar a una función de sistema operativo (por ejemplo, "finalizar tarjeta"), o proporcionar los medios para llamar a una función que se ha escrito específicamente para conseguir el efecto deseado. Ejemplos de esto último incluyen:

modificar los límites relacionados con la seguridad almacenados en ficheros concretos de la tarjeta, dichos datos se refieren a menudo a datos de 'gestión de riesgos';

conmutar de SDA a DDA o CDA.

Las operaciones OP1, etc., se pueden ejecutar antes de devolverle al terminal la respuesta a la APDU que contiene el código de operación. Haciendo de nuevo referencia a la Figura 6, exec(OPn) se puede considerar como una llamada dentro del código del comando VERIFY PIN (verificar PIN):

```
VERIFY PIN {
…
exec(OPn);
…
 return response to reader (devolver respuesta al lector);
}
```

Una alternativa es utilizar un modelo dirigido por eventos para implementar el control. En este caso, la columna "punto de entrada" en la Figura 6 se puede sustituir por "evento". Los posibles eventos son:

- inmediatamente después de devolver el comando que incluye el código de operación;
- inmediatamente, que es efectivamente el punto de entrada anterior;
- fin de la transacción.

Los códigos de operación OPn pueden tener la misma longitud que el CHALLENGE (desafío), esto es, 8 bytes. Podrían ser, por ejemplo, cadenas aleatorias de 64 bits. Los códigos de operación pueden ser propietarios del emisor de la tarjeta.

Códigos de operación encriptados

La autoridad emisora (por ejemplo, un banco) de una tarjeta tiene una clave maestra, K0. La clave maestra K0 se utiliza para generar la clave K1 de la tarjeta en función del PAN (Número de Cuenta Principal). K1 se genera en los primeros pasos de la personalización de la tarjeta y se almacena en una memoria no volátil. Se mantiene constante durante toda la vida de la tarjeta. Una función de derivación de clave (kdf) genera una clave K2 utilizando la clave K1 y un Contador de Transacciones de Aplicación (ATC). Como el valor del ATC se incrementa con cada transacción, K2 es único para una transacción concreta:

kdf(ATC, K1) => K2

En general, a partir de la clave K1 de tarjeta se derivan nuevas claves para propósitos específicos:

kdf(datos de diversificación, K1) => K_n

Las posibles funciones kdf incluyen triple DES y AES. Los datos de diversificación pueden ser cualesquiera datos que sean conocidos por ambas partes que utilizan la clave. Esto es debido al hecho de que la derivación de clave tiene que ser un procedimiento acordado para permitir al receptor de un mensaje encriptado generar la clave correcta para poder descifrar el mensaje.

Si se viera comprometido el código de operación (OPn) correspondiente a, por ejemplo, una operación de “APPLICATION BLOCK (bloque de aplicación)”, permitiría a un atacante realizar un ataque de denegación de servicio. Una defensa contra este ataque es encriptar el código de operación:

encrypt(OPn, K3) => $\{OPn\}_{K3}$

donde: $\{X\}_K$ significa X cifrado con la clave K.

Esto significa que el resultado 136 de la operación ejecutada en el bloque 133 de la Figura 3 y que también se muestra en la Figura 5B es:

$\{OPn\}_{K3}$

Una primera posibilidad para la clave K3 es una clave fija derivada, por ejemplo, a partir de una clave K1 de tarjeta del siguiente modo:

kdf(cadena fija, K1) => K3

En este caso, los códigos de operación en la tabla de resultados (Figura 6) almacenados en la tarjeta 10 se sustituyen por las versiones encriptadas de dichos códigos, por ejemplo, $\{OP1\}_{K3}$, $\{OP2\}_{K3}$, etc. cuando la tabla se graba en la tarjeta durante el proceso de personalización de la misma. En el lado del servidor, la entidad de autorización puede almacenar una tabla para cada tarjeta o puede obtener la clave cuando sea necesario. La opción de obtener la clave cuando sea necesario es ventajosa y minimiza los requisitos de almacenamiento.

Las claves K0, K1, K2, K3 descritas más arriba son diferentes al par de claves de clave pública y clave privada utilizadas para encriptar el mensaje que transporta los datos de PIN. Haciendo de nuevo referencia a la Figura 4B, el OPCODE 145 se encripta con la clave K3. Los datos resultantes, que incluyen un campo que es una combinación lógica del desafío 143 y el OPCODE 145 encriptado, se encriptan a continuación utilizando la clave pública 148 de la tarjeta. Igualmente, en la Figura 5B, el mensaje recibido en 126 en primer lugar se desencripta utilizando la clave privada 152 de la tarjeta. A partir de los datos desencriptados se extrae un OPCODE 136 encriptado mediante una operación lógica en el campo 155. El OPCODE 136 encriptado se puede desencriptar a continuación utilizando la clave K3.

La Figura 7 muestra una tabla de ejemplo de datos almacenados en el terminal. Los datos de esta tabla se reciben desde la entidad 30 de autorización en la lista (lista negra) 100. Los datos comprenden los detalles de la tarjeta (por ejemplo, PAN) y un código de operación a enviar a la tarjeta si el terminal se comunica con una tarjeta que tiene dichos detalles de tarjeta. El código de operación se puede almacenar de forma encriptada. La encriptación del código de operación se puede realizar como se ha descrito más arriba. Por ejemplo, cada uno de los códigos de operación en la Figura 7 están almacenados de forma encriptada, con el código de operación encriptado utilizando la clave K3 de una tarjeta concreta.

Haciendo de nuevo referencia a la Figura 2, si el PIN se introduce correctamente en la etapa 120 de verificación de PIN, el método puede continuar con la etapa de autorización de la transacción. Durante la etapa de autorización de la transacción la tarjeta puede enviarle al terminal 20 un criptograma, el cual se reenvía a la entidad 30 de autorización. La tarjeta recibe como respuesta un criptograma, a través del terminal 20. Es posible modificar el criptograma enviado a la tarjeta 10 para transportar un elemento de datos como, por ejemplo, un código de operación. Es posible que la tarjeta 10 pueda recibir dos elementos de datos (por ejemplo, códigos de operación): un primer código de operación durante la etapa 120 de verificación de PIN y un segundo código de operación durante la etapa de autorización de transacción. La tarjeta 10 puede realizar una priorización de los dos códigos de operación. En un ejemplo, la tarjeta 10 puede dar una prioridad más alta al código de operación recibido durante la etapa de autorización de transacción y puede dar una prioridad más baja (o simplemente ignorar) el código de operación recibido durante la etapa 120 de verificación de PIN. Por ejemplo, la lista negra mantenida por la entidad 30 de autorización debería estar más actualizada que la mantenida por el terminal 20 y, por lo tanto, el código de operación enviado durante la etapa de autorización de transacción debería estar los más actualizado posible.

La Figura 8 muestra un ejemplo de una tarjeta de circuito integrado (ICC) 10, o una tarjeta chip que se puede configurar para ejecutar el método descrito más arriba. La tarjeta chip 10 comprende un procesador 15 conectado operativamente a un almacenamiento 16. El almacenamiento 16 incluye un almacenamiento no volátil. El almacenamiento no volátil puede almacenar aplicaciones y claves criptográficas. La tarjeta chip 10 tiene al menos una interfaz externa 11, 12 para comunicarse con un terminal 20. Las interfaces externas pueden ser una interfaz 11 de contacto y/o una interfaz 12 sin contacto. La comunicación con el terminal 20 se realiza típicamente mediante unas APDU ISO 7816. El terminal 20 se comunica con la entidad 30 de autorización a través de una red. El elemento seguro puede estar embebido en una tarjeta de formato ISO 7810 como, por ejemplo, una tarjeta con formato ID-1 (por ejemplo, utilizada típicamente para tarjetas de banco y tarjetas de crédito/débito) o una tarjeta con formato ID-000 (por ejemplo, utilizada típicamente para tarjetas SIM). En otros ejemplos, el elemento seguro se puede embeber directamente en una placa de circuitos como, por ejemplo, una placa de circuitos de un teléfono móvil.

La Figura 9 muestra un ejemplo de equipo 300 de procesamiento que se puede implementar como cualquier forma de dispositivo de ordenador y/o electrónico, y en el que se pueden implementar los modos de realización del sistema y los métodos descritos más arriba. El equipo 300 de procesamiento se puede proporcionar en la tarjeta 10 y/o en el terminal 20. El equipo de procesamiento puede participar en cualquiera de los métodos descritos más arriba. El equipo 300 de procesamiento comprende uno o más procesadores 301, los cuales pueden ser microprocesadores, microcontroladores o cualquier otro tipo de procesador apropiado que ejecute instrucciones para controlar la operación del dispositivo. El procesador 301 está conectado a otros componentes del dispositivo a través de uno o más buses 306. Las instrucciones 303 ejecutables por el procesador se pueden proporcionar utilizando cualquier medio legible por un ordenador como, por ejemplo, una memoria 302. Las instrucciones 303 ejecutables por el procesador pueden comprender instrucciones para implementar la funcionalidad de los métodos descritos. La memoria 302 es de cualquier tipo apropiado como, por ejemplo, memoria no volátil, memoria de sólo lectura (ROM), memoria de acceso aleatorio (RAM), un dispositivo de almacenamiento de cualquier tipo como, por ejemplo, un dispositivo de almacenamiento magnético u óptico. Para almacenar los datos 305 utilizados por el procesador 301 se puede proporcionar la memoria 302, o cualquier memoria adicional 304. Los datos 305 pueden comprender la tabla de códigos de operación descrita más arriba. El equipo 300 de procesamiento comprende una o más interfaces 308 de comunicación.

A una persona experimentada en la técnica se le ocurrirán modificaciones y otros modos de realización de la invención divulgada con el beneficio de las enseñanzas presentadas en las descripciones y los dibujos asociados. Por lo tanto, se debe entender que la invención no se encuentra limitada a los modos de realización específicos divulgados y que se pretende que las modificaciones y otros modos de realización se encuentren incluidos dentro del alcance de la divulgación. Aunque en la presente solicitud se pueden haber utilizado términos específicos, se han utilizado únicamente en sentido genérico y descriptivo y no con el propósito de limitar.

REIVINDICACIONES

1. Un método de comunicación entre un terminal (20) y un elemento seguro (10) que comprende, en el elemento seguro (10):

determinar un desafío;

enviar el desafío (122) al terminal (20);

recibir una respuesta (124, 126) del terminal (20) comprendiendo el desafío y los datos del número de identificación personal, PIN, estando la respuesta integrada con una clave pública;

desencriptar (130) la respuesta (124, 126) utilizando una clave privada del elemento seguro correspondiente a la clave pública;

determinar (132) si el desafío recibido en la respuesta se corresponde con el desafío enviado al terminal (20); y

si el desafío recibido en la respuesta no se corresponde con el desafío enviado al terminal (20), comprende además:

realizar un cálculo (133) utilizando el desafío recibido y el desafío enviado para detectar la presencia de datos adicionales en la respuesta; y

recuperar, como salida del procesamiento (133), un código de operación (136), en donde el código de operación (136) indica una acción a realizar por el elemento seguro.

2. Un método de acuerdo con la reivindicación 1 en donde la realización del cálculo (133) comprende realizar una operación entre bits con el desafío recibido y el desafío enviado.

3. Un método de acuerdo con la reivindicación 2 en donde la operación entre bits es una operación OR exclusivo, XOR.

4. Un método de acuerdo con una cualquiera de las reivindicaciones anteriores en donde el código de operación indica una acción de seguridad a realizar por el elemento seguro, y el método comprende, además, realizar (137) la acción de seguridad de acuerdo con un valor del código de operación.

5. Un método de acuerdo con una cualquiera de las reivindicaciones anteriores en donde el código de operación está encriptado.

6. Un método de acuerdo con una cualquiera de las reivindicaciones anteriores que se realiza como parte de una transacción fuera de línea.

7. Un método de comunicación entre un terminal (20) y un elemento seguro (10) que comprende, en el terminal (10):

recibir un desafío (121) desde el elemento seguro (20);

determinar (122) si es necesario enviar un código de operación al elemento seguro (10);

si no es necesario enviar un código de operación al elemento seguro (10), enviar una respuesta encriptada (124) al elemento seguro (10), comprendiendo la respuesta el desafío y los datos del número de identificación personal, PIN; y

si es necesario enviar un código de operación al elemento seguro (10):

realizar un cálculo (126) del desafío con el código de operación para producir un desafío modificado; y

enviar una respuesta encriptada (127) al elemento seguro (10), comprendiendo la respuesta el desafío modificado y los datos del número de identificación personal, PIN, en donde el elemento seguro (10) puede recuperar el código de operación a partir del desafío modificado, y el código de operación indica una acción a realizar por el elemento seguro;

en donde la determinación (123) de si es necesario enviar un código de operación al elemento seguro (10) comprende determinar si el número del elemento seguro (10) se encuentra en la lista negra de números, y si el número

del elemento seguro (10) se encuentra en la lista negra de números, enviar un código de operación que indica una acción para bloquear el elemento seguro.

8. Un elemento seguro (10) que comprende un procesador, una memoria y una interfaz de comunicaciones, conteniendo la memoria instrucciones ejecutables por el procesador para hacer que el procesador:

determine un desafío;

envíe el desafío (122) a un terminal (20) a través de la interfaz de comunicaciones;

reciba una respuesta (124, 126) desde el terminal (20) comprendiendo el desafío y datos del número de identificación personal, PIN, estando la respuesta encriptada con una clave pública;

desencriptar (130) la respuesta (124, 126) utilizando una clave privada del elemento seguro correspondiente a la clave pública;

determinar (132) si el desafío recibido en la respuesta se corresponde con el desafío enviado al terminal (20); y

si el desafío recibido en la respuesta no se corresponde con el desafío enviado al terminal (20), las instrucciones hacen además que el procesador:

realice un cálculo (133) utilizando el desafío recibido y el desafío enviado para detectar la presencia de datos adicionales en la respuesta; y

obtenga, como resultado del cálculo (133), un código de operación (136), en donde el código de operación (136) indica una acción a realizar por el elemento seguro.

9. Un elemento seguro (10) de acuerdo con la reivindicación 8 en donde el cálculo (133) es una operación entre bits con el desafío recibido y el desafío enviado.

10. Un elemento seguro (10) de acuerdo con la reivindicación 8 ó 9 en donde el código de operación indica una acción de seguridad a realizar por el elemento seguro, y las instrucciones hacen que el procesador ejecute (137) la acción de seguridad de acuerdo con el valor del código de operación.

11. Un elemento seguro (10) de acuerdo con la reivindicación 10 en donde el código de operación está encriptado.

12. Un terminal (20) que comprende un procesador, una memoria y una interfaz de comunicaciones, conteniendo la memoria instrucciones ejecutables por el procesador para hacer que el procesador:

reciba un desafío (122) desde un elemento seguro (10);

determine (123) si es necesario enviar un código de operación al elemento seguro (10);

si no es necesario enviar un código de operación al elemento seguro (10), enviar una respuesta encriptada (124) al elemento seguro (10), comprendiendo la respuesta el desafío y datos del número de identificación personal, PIN; y

si es necesario enviar un código de operación al elemento seguro (10):

realizar un cálculo (126) del desafío con el código de operación para obtener un desafío modificado; y

enviar una respuesta encriptada (127) al elemento seguro (10), comprendiendo la respuesta el desafío modificado y los datos del número de identificación personal, PIN, en donde el código de operación se puede obtener a partir del desafío modificado por parte del elemento seguro (10), y el código de operación indica una acción a realizar por parte del elemento seguro;

en donde las instrucciones que hacen que el procesador determine (123) si es necesario enviar un código de operación al elemento seguro (10) hacen que el procesador determine si el número del elemento seguro (10) se encuentra en una lista negra de números, y si el número del elemento seguro (10) se encuentra en la lista negra de números, enviar un código de operación que indica una acción para bloquear el elemento seguro.

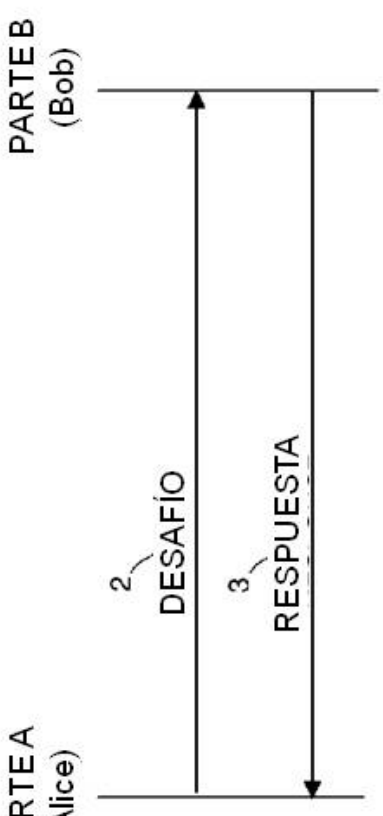


Fig. 1

Código de Operación	Punto de entrada
OP1	exec (OP1)
OP2	exec (OP2)
OP3	exec (OP3)

Fig. 6

PAN	Código de Operación
xxxxxxx	$\{OPn\}_{K3}$
xxxxxxx	$\{OPn\}_{K3}$
xxxxxxx	$\{OPn\}_{K3}$

Fig. 7

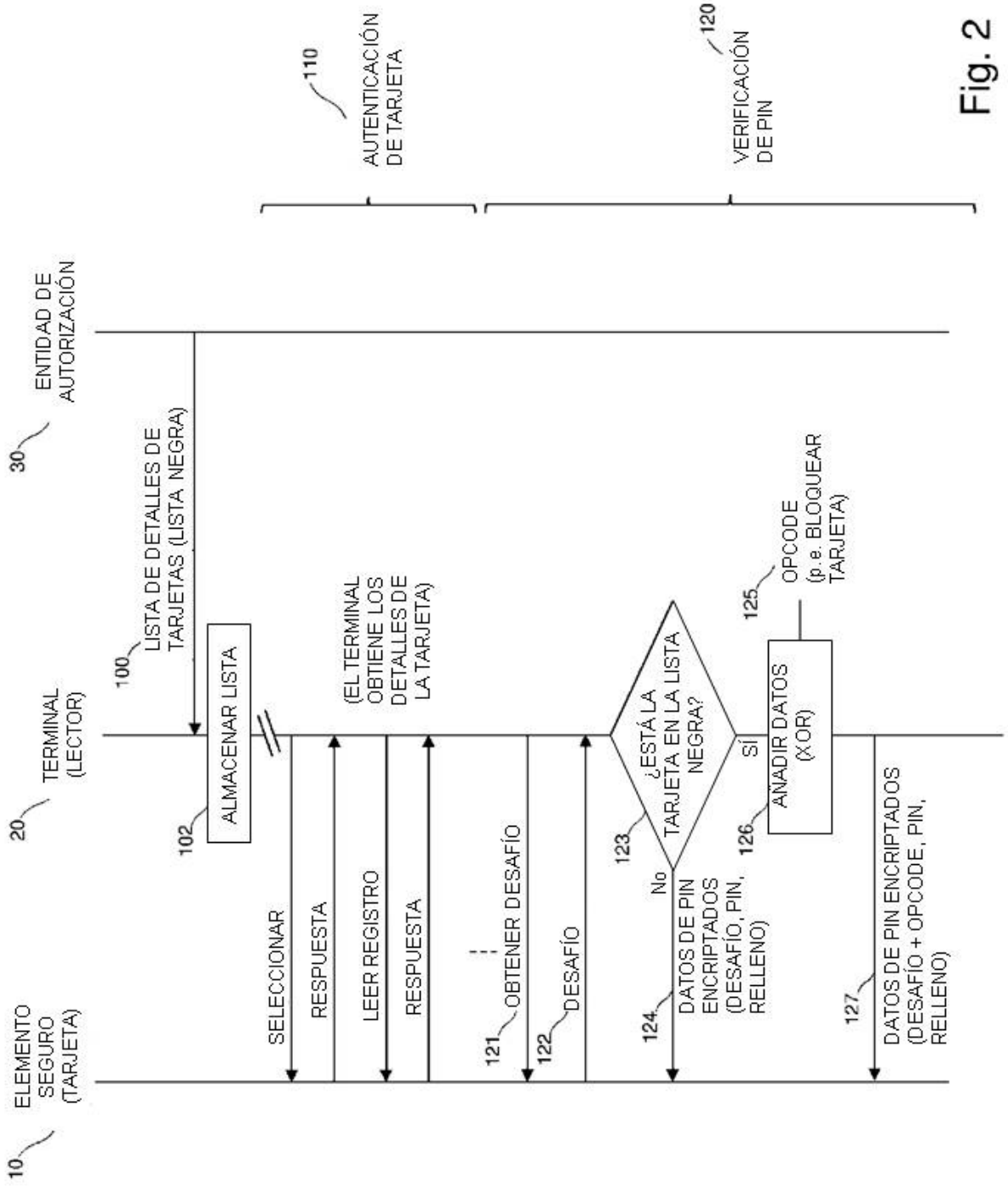

ELEMENTO SEGURO (TARJETA)
10
TERMINAL (LECTOR)
20
ENTIDAD DE AUTORIZACIÓN
30
AUTENTICACIÓN DE TARJETA
110
VERIFICACIÓN DE PIN
120
LISTA DE DETALLES DE TARJETAS (LISTA NEGRA)
100
ALMACENAR LISTA
102
SELECCIONAR
RESPUESTA
LEER REGISTRO
RESPUESTA
(EL TERMINAL OBTIENE LOS DETALLES DE LA TARJETA)
OBTENER DESAFÍO
121
DESAFÍO
122
¿ESTÁ LA TARJETA EN LA LISTA NEGRA?
123
No
DATOS DE PIN ENCRIPTADOS (DESAFÍO, PIN, RELLENO)
124
Sí
OPCODE (p. e. BLOQUEAR TARJETA)
125
AÑADIR DATOS (XOR)
126
DATOS DE PIN ENCRIPTADOS (DESAFÍO + OPCODE, PIN, RELLENO)
127

Fig. 2

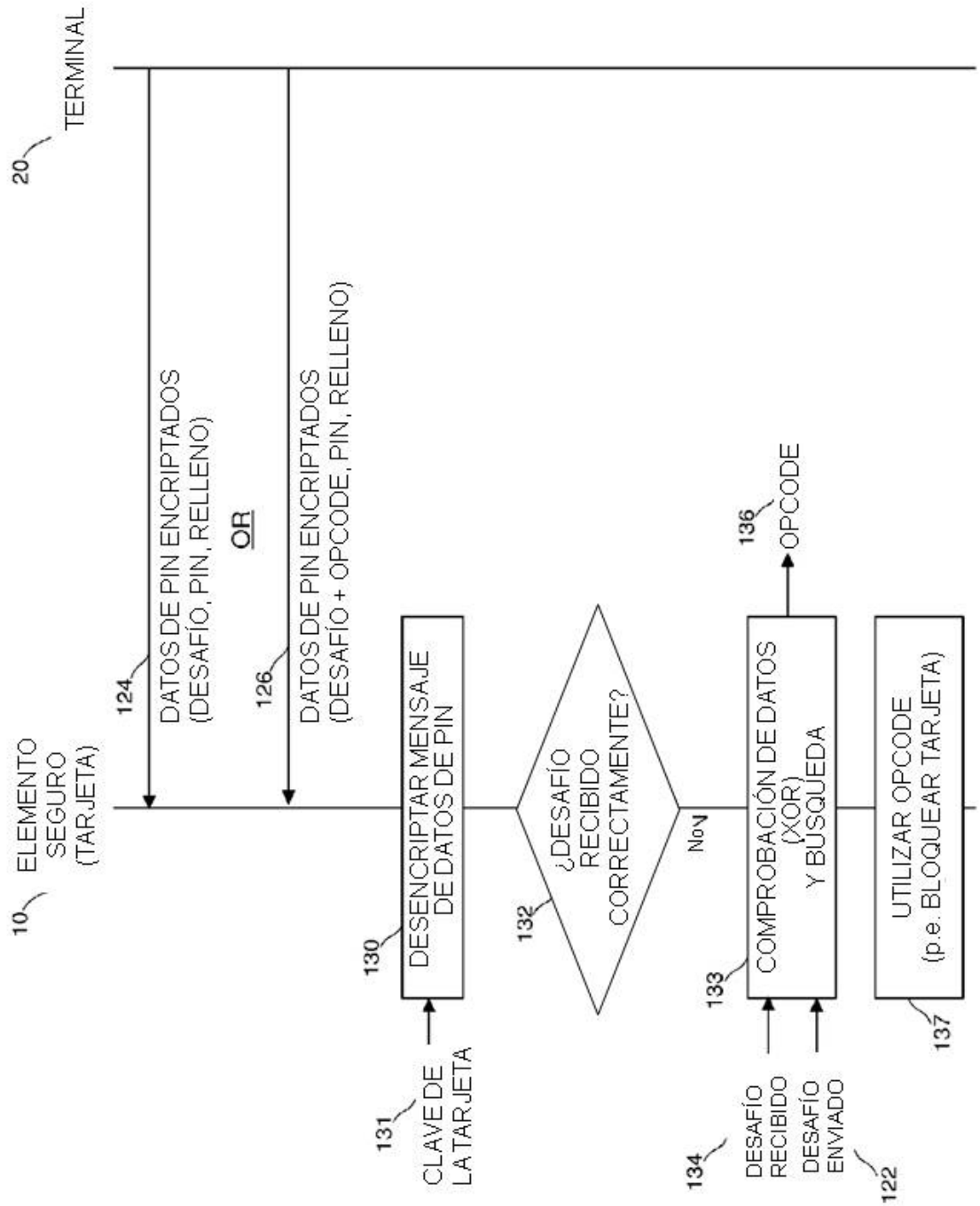

TERMINAL
20
ELEMENTO SEGURO (TARJETA)
10
124
DATOS DE PIN ENCRIPTADOS (DESAFÍO, PIN, RELLENO)
OR
126
DATOS DE PIN ENCRIPTADOS (DESAFÍO + OPCODE, PIN, RELLENO)
130
DESENCRIPTAR MENSAJE DE DATOS DE PIN
131
CLAVE DE LA TARJETA
132
¿DESAFÍO RECIBIDO CORRECTAMENTE?
No
133
COMPROBACIÓN DE DATOS (XOR) Y BÚSQUEDA
134
DESAFÍO RECIBIDO
DESAFÍO ENVIADO
122
136
OPCODE
UTILIZAR OPCODE (p.e. BLOQUEAR TARJETA)
137

Fig. 3

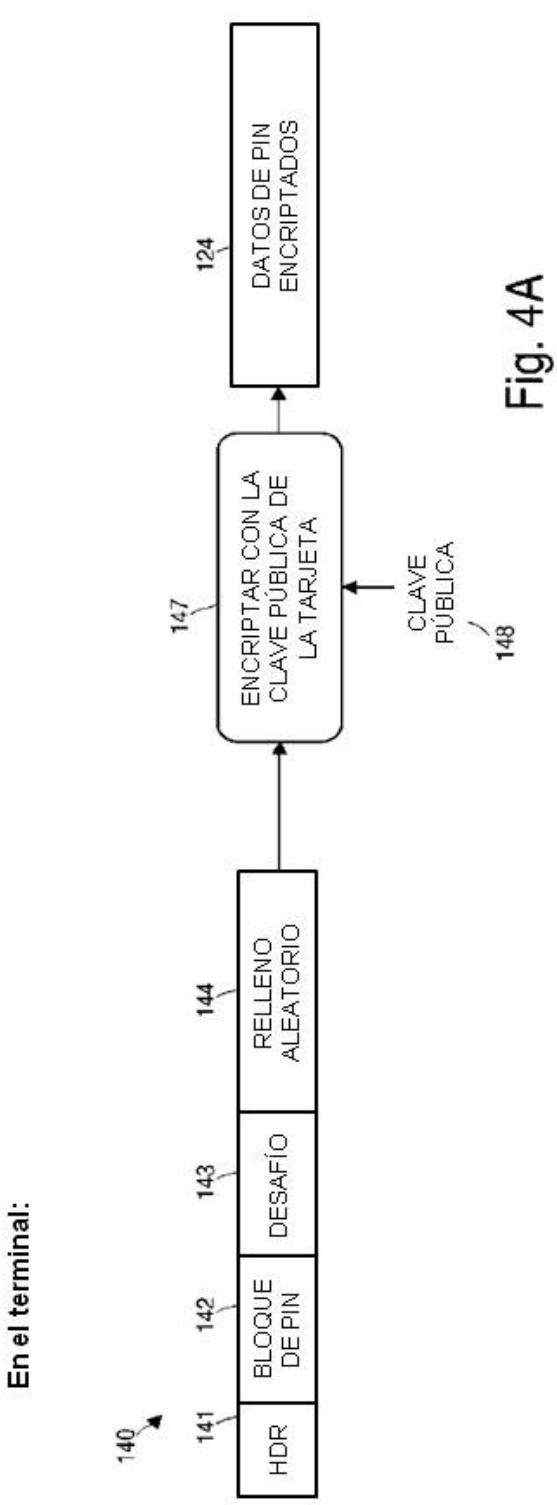

En el terminal:
140
141
HDR
142
BLOQUE DE PIN
143
DESAFÍO
144
RELLENO ALEATORIO
147
ENCRIPTAR CON LA CLAVE PÚBLICA DE LA TARJETA
148
CLAVE PÚBLICA
124
DATOS DE PIN ENCRIPTADOS

Fig. 4A

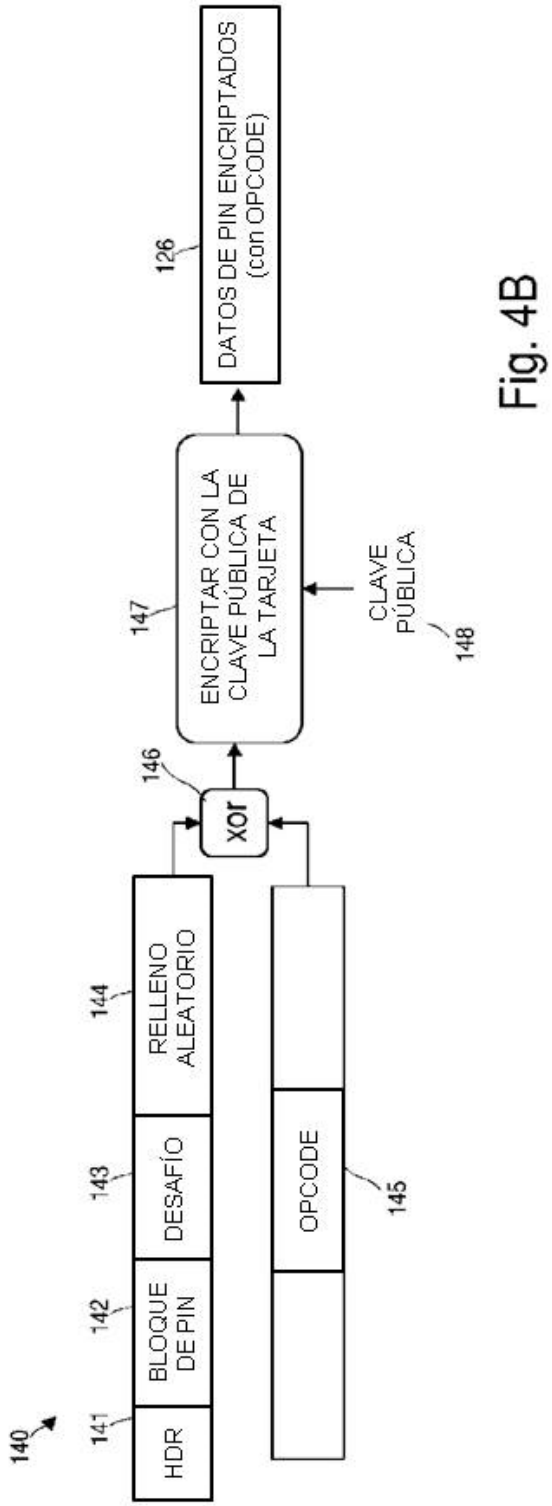
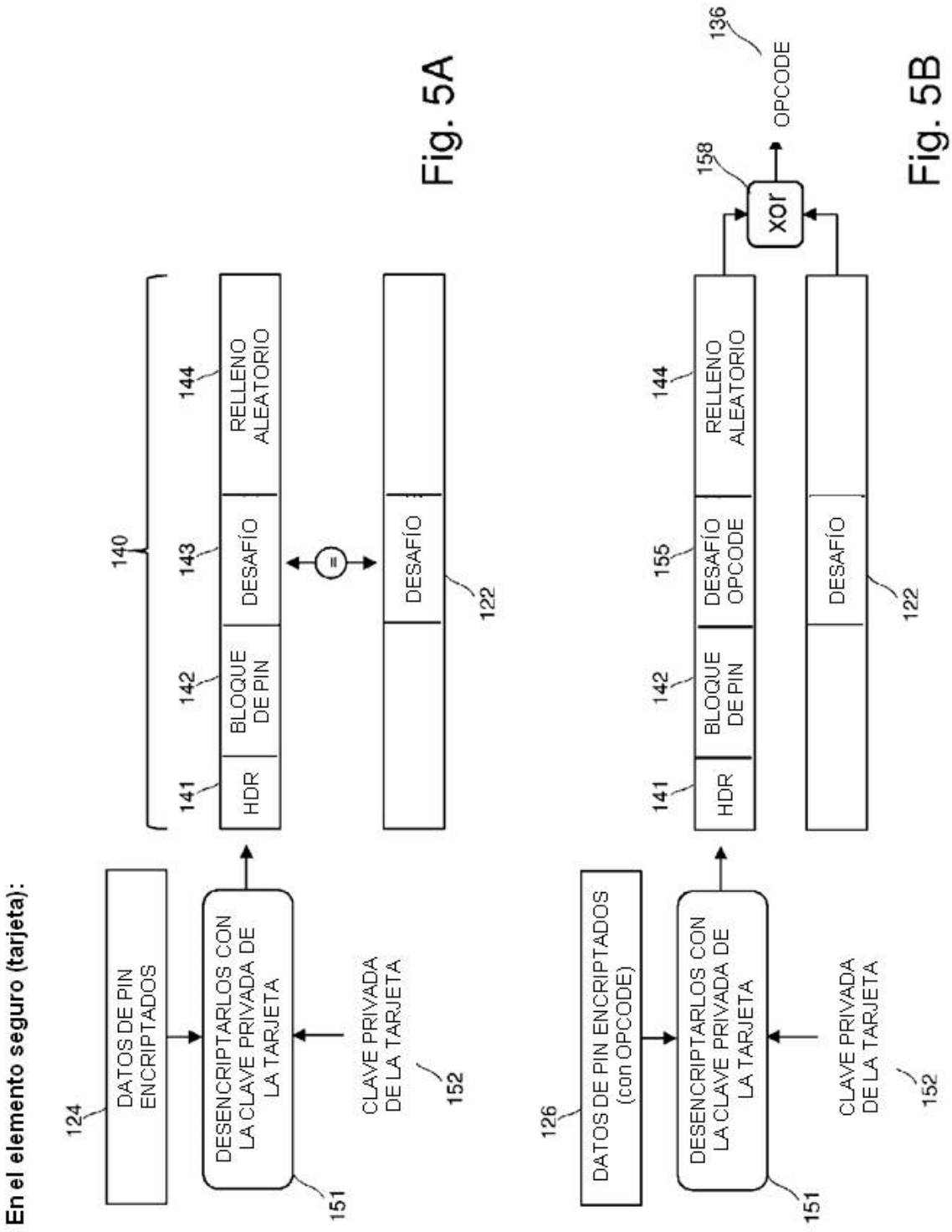

140
141
HDR
142
BLOQUE DE PIN
143
DESAFÍO
144
RELLENO ALEATORIO
145
OPCODE
146
xor
147
ENCRIPTAR CON LA CLAVE PÚBLICA DE LA TARJETA
148
CLAVE PÚBLICA
126
DATOS DE PIN ENCRIPTADOS (con OPCODE)

Fig. 4B


En el elemento seguro (tarjeta):
124
DATOS DE PIN ENCRIPTADOS
DESENCRIPTARLOS CON LA CLAVE PRIVADA DE LA TARJETA
151
CLAVE PRIVADA DE LA TARJETA
152
140
141
HDR
142
BLOQUE DE PIN
143
DESAFÍO
144
RELLENO ALEATORIO
=
DESAFÍO
122
Fig. 5A
126
DATOS DE PIN ENCRIPTADOS (con OPCODE)
DESENCRIPTARLOS CON LA CLAVE PRIVADA DE LA TARJETA
151
CLAVE PRIVADA DE LA TARJETA
152
141
HDR
142
BLOQUE DE PIN
155
DESAFÍO OPCODE
144
RELLENO ALEATORIO
158
xor
136
OPCODE
DESAFÍO
122
Fig. 5B

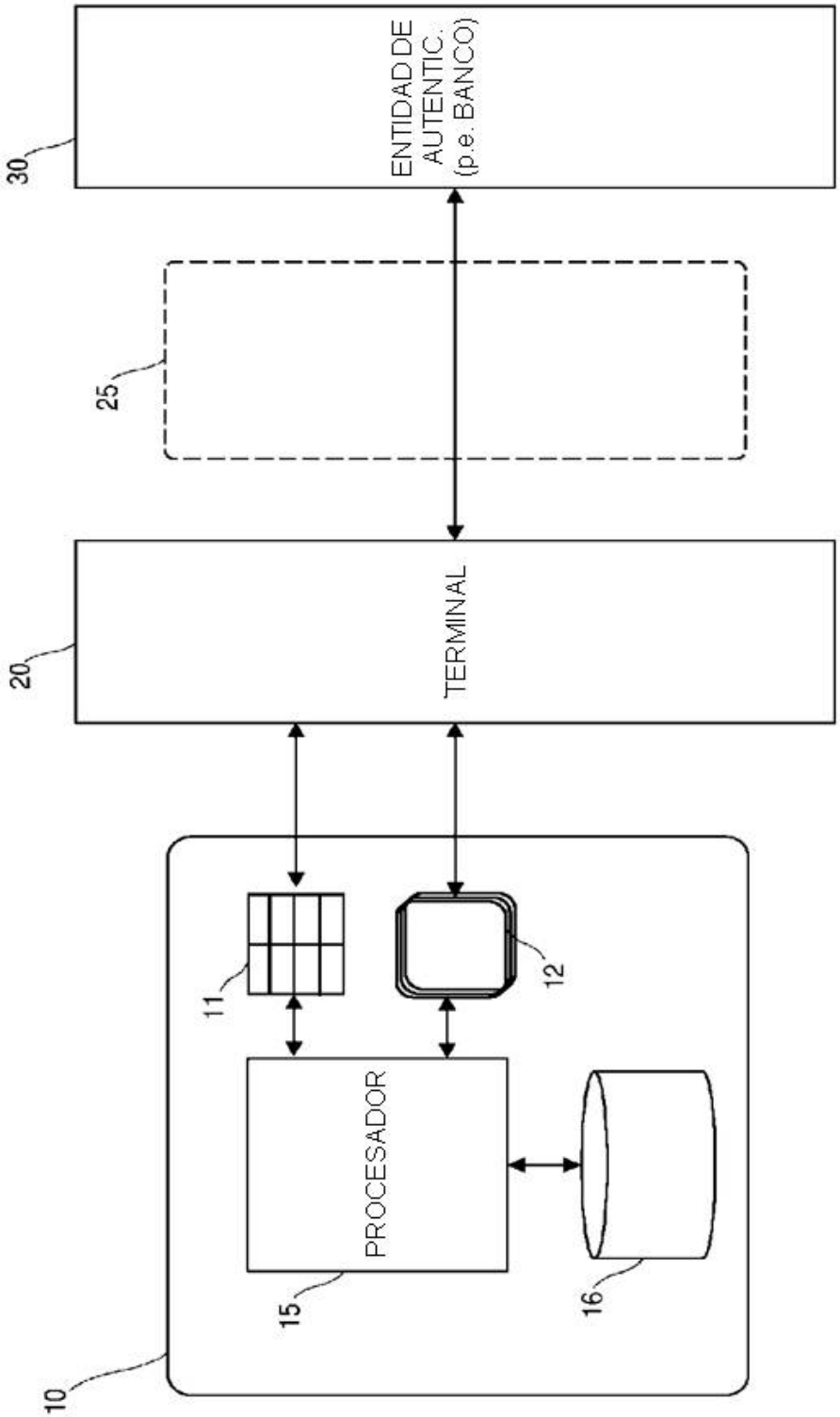

ENTIDAD DE AUTENTIC. (p.e. BANCO)
30
25
TERMINAL
20
11
12
PROCESADOR
15
16
10

Fig. 8

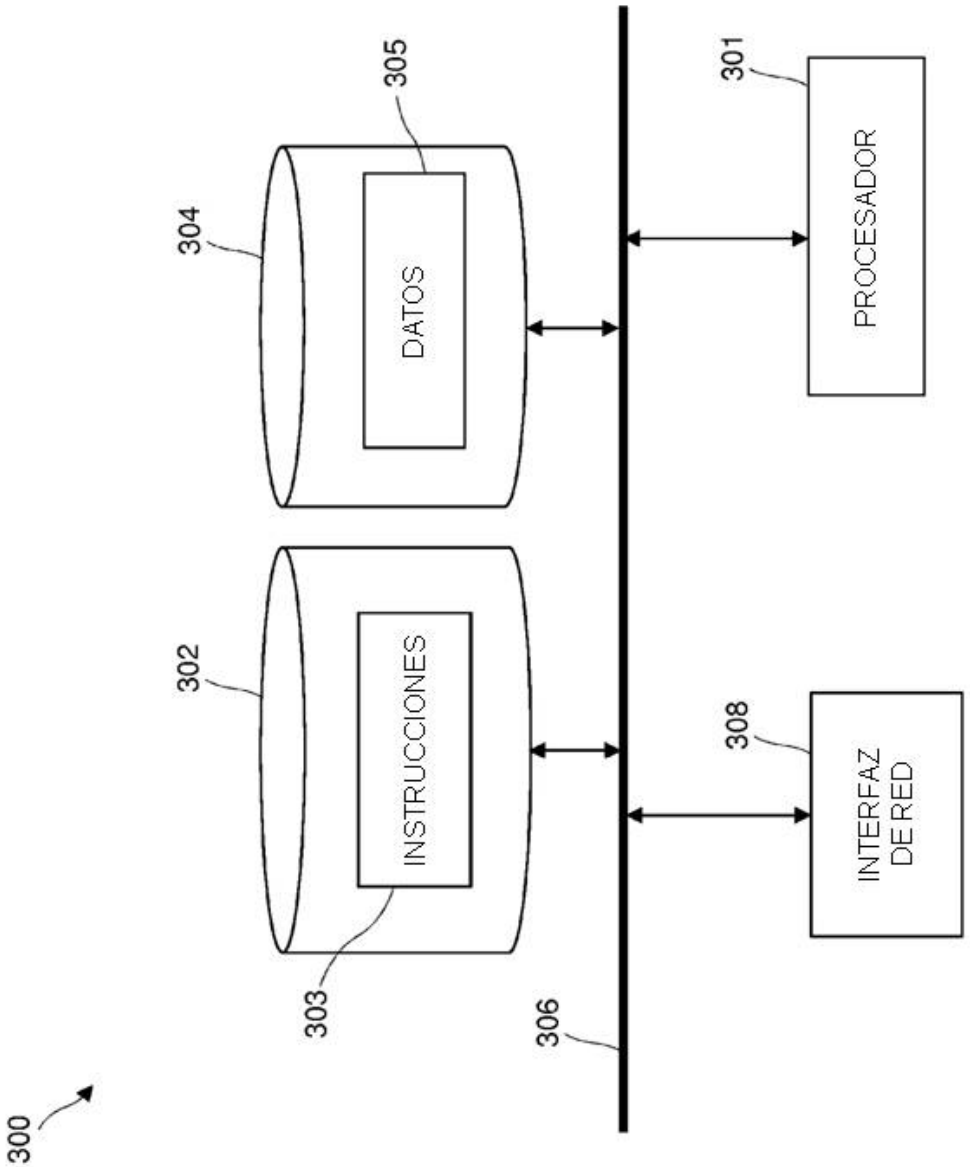

300
302
INSTRUCCIONES
303
304
DATOS
305
306
301
PROCESADOR
308
INTERFAZ
DE RED

Fig. 9