(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 631 002**

(21) Número de solicitud: 201590019

(51) Int. CI.:

G06Q 20/38 (2012.01)
G06Q 20/40 (2012.01)
G07F 7/10 (2006.01)

(12) SOLICITUD DE PATENTE A2

(22) Fecha de presentación:

03.09.2013

(30) Prioridad:

04.09.2012 US 61/696,726

(43) Fecha de publicación de la solicitud:

25.08.2017

(71) Solicitantes:

NET1 UEPS TECHNOLOGIES, INC (100.0%)
4th Floor President's Place CNR Jan Smuts Avenue and Bolton Roads
2196 Rosebank, Johannesburg, Gauteng ZA

(72) Inventor/es:

BELAMANT, Serge Christian Pierre

(74) Agente/Representante:

CURELL AGUILÁ, Mireia

(54) Título: **Dispositivo para facilitar transacciones financieras, procedimiento e instalación correspondientes**

(57) Resumen:

Dispositivo para facilitar transacciones financieras, procedimiento e instalación correspondientes. Dicho dispositivo presenta una unidad de almacenamiento de datos, un dispositivo de entrada que puede hacer funcionar una persona que realiza la transacción para introducir una petición de un PIN, un dispositivo de entrada de identificador biométrico, una unidad de verificación, un generador de PIN y un dispositivo de salida. El identificador biométrico puede ser una señal de sonido, una señal visual o una huella dactilar. De manera correspondiente, una instalación de procesamiento de transacciones financieras de un emisor de tarjetas de crédito o débito presenta una unidad de recepción, una unidad de verificación para verificar el PIN y una unidad de aprobación de transacciones para aprobar la transacción si se verifica el PIN recibido. El PIN recibido puede verificarse con un generador de PIN de comprobación y un comparador para comparar el PIN de comprobación y el PIN recibido.

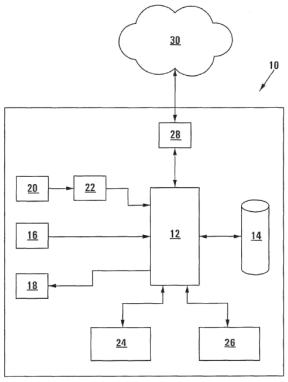

FIG 1

ES 2 631 002 A2

DESCRIPCIÓN

Dispositivo para facilitar transacciones financieras, procedimiento e instalación correspondientes.

La presente invención se refiere a transacciones financieras electrónicas. Más particularmente, se refiere a un dispositivo de facilitación de transacciones financieras, a una instalación de procesamiento de entidad financiera, a un procedimiento para facilitar una transacción financiera y a un procedimiento para procesar una transacción financiera.

Durante los últimos cincuenta años aproximadamente, las entidades financieras tales como bancos han emitido tarjetas de plástico para sus clientes para realizar transacciones financieras en dispositivos de cajeros automáticos (ATM) y de punto de venta (POS). Más recientemente, se han introducido códigos de número de identificación personal (PIN) para proteger estas tarjetas frente a un uso no autorizado. Se conoce bien y está documentado en la industria que a partir de la introducción de los sistemas basados en PIN se han originado una serie de problemas.

El primer problema es que los números PIN deben distribuirse o seleccionarse de alguna manera por el titular de la tarjeta sin que se vean comprometidos. El segundo problema es que debe implementarse un sistema completo para permitir el cambio de los PIN o bien porque lo desee el titular de la tarjeta o bien en el caso de que se haya olvidado, bloqueado o se haya visto comprometido el PIN inicial.

Por un lado, estos sistemas son caros pero, lo que es más importante, a menudo se encuentran en el punto central de ataque para estafadores que comprometen los PIN en general.

Sin embargo, el área más problemática es que el PIN se vea comprometido debido al aumento de los ataques simples tales como visualización, cámaras, registro electrónico, lectura rápida y similares hasta técnicas de análisis criptográfico más sofisticadas.

Esto lleva a fraude, pérdidas y a un aumento en el riesgo sistémico de los sistemas de pago nacionales.

En entornos menos sofisticados, el uso de PIN es incluso más problemático puesto que

los usuarios tienen menos formación y es más probable que olviden y/o simplemente den sus PIN a organizaciones criminales o individuos perversos.

La verificación biométrica resuelve la mayoría de los problemas mencionados anteriormente puesto que los clientes no disponen de ningún PIN secreto que pueda verse comprometido o que pueda utilizar cualquier otra persona. Además, los clientes no pueden perder algo que forma parte de ellos.

Sin embargo, el reto es que la verificación biométrica requiere alguna forma de dispositivo de aceptación para su incorporación en el ATM o POS en cuestión. Estos dispositivos de captura biométrica a menudo son caros y requieren una integración de hardware y desarrollo de software intensos. El resultado es que muchas entidades financieras, a pesar de estar a favor de la verificación biométrica, en principio no respaldan su implementación debido al coste que supone actualizar su base de adquisición existente. El resultado neto es que los clientes siguen utilizando números PIN, muy a menudo bajo su propio riesgo puesto que las entidades financieras les avisan de que sus PIN deben guardarse de manera segura para garantizar que no se vean comprometidos de ningún modo.

Esta postura simplemente transfiere la responsabilidad de un sistema basado en PIN no seguro a los titulares de las tarjetas protegiendo así a las entidades financieras frente a demandas que superan los mil millones de dólares estadounidenses cada año.

El estado de la técnica conocido, a partir del correspondiente Informe de Búsqueda Internacional (IBI) incluye los documentos WO2012112921 (D1), US2008028230 (D2), DE102007018604 (D3) y US 2004/0030660 (D4).

D1 divulga un procedimiento de no repudio para peticiones de crédito de consumo basado en autentificación afirmativa de un pin de un solo uso (one-time-pin o “OTP” en inglés) generado desde una tarjeta inteligente biométrica de consumidor. La tarjeta inteligente biométrica puede autentificar información biométrica (por ejemplo, huella digital, imagen facial, imagen del iris, etc.) del consumidor basado en patrones biométricos almacenados en la tarjeta inteligente biométrica. En por lo menos alguna de las varias formas de realización, el OTP puede ser autentificado por una autoridad identificadora, de forma que puede autentificarse una petición de crédito asociada hacia un proveedor.

D2 divulga una tarjeta de proximidad biométrica y un sistema de acceso que coopera con dicha tarjeta. La tarjeta dispone de un sensor biométrico, y una memoria que almacena unos datos de referencia biométricos, por ejemplo, una huella digital, para un usuario autorizado. Únicamente cuando los datos biométricos de un cliente coinciden con los datos biométricos almacenados, un generador de PIN pseudoaleatorio genera un código de acceso de un solo uso que puede ser detectado y validado por un panel de una puerta o algún otro sensor de proximidad que controla el acceso a un edificio o a otro recurso.

D3 divulga una tarjeta con un sensor biométrico para leer información biométrica obtenida de un usuario, y producir dinámicamente un número de identificación personal (PIN), usando un módulo generador de PIN, cuando existe una correlación entre dicha información y una referencia de usuario.

D4 divulga una invención que permite el acceso a información utilizando un sistema de autentificación para verificar que un usuario es un usuario autorizado de un dispositivo de acceso de información. El sistema de autentificación incluido en el dispositivo emitido para un usuario autorizado, lee la huella digital de un usuario utilizando un lector y la compara con una huella digital almacenada del usuario autorizado, un generador pseudoaleatorio genera un número de identificación personal para ser usado por el usuario, para validar la activación del dispositivo para el acceso de información.

Un objetivo de la presente invención es reducir esas deficiencias asociadas con los PIN estáticos y la presente verificación biométrica.

Por tanto, según la invención se proporciona un dispositivo de facilitación de transacciones financieras, que incluye un dispositivo de procesamiento electrónico; una unidad de almacenamiento de datos; un dispositivo de entrada que puede hacer funcionar una persona que realiza la transacción para introducir una petición de un PIN; un dispositivo de entrada de identificador biométrico para introducir un identificador biométrico de la persona que realiza la transacción; una unidad de verificación para verificar un identificador biométrico proporcionado, en uso, por la persona que realiza la transacción; un generador de PIN para generar un PIN si se verifica el identificador biométrico introducido y un dispositivo de salida para suministrar el PIN a la persona que realiza la transacción.

Además según la invención se proporciona un procedimiento para facilitar una transacción financiera que incluye introducir, por una persona que realiza la transacción, una petición de un PIN en un dispositivo electrónico de la persona que realiza la transacción; introducir un identificador biométrico de la persona que realiza la transacción; verificar el identificador biométrico introducido; generar un PIN si se verifica el identificador biométrico introducido y suministrar el PIN a la persona que realiza la transacción.

Se apreciará que el identificador biométrico puede ser una señal de sonido, una señal visual o una huella dactilar. Si es una señal de sonido, tal como un mensaje de voz, el dispositivo de entrada de identificador biométrico puede incluir un micrófono. Si es una señal visual, tal como una representación de la persona que realiza la transacción, el dispositivo de entrada de identificador biométrico puede incluir una cámara. Si es una huella dactilar, entonces el dispositivo de entrada de identificador biométrico puede incluir un escáner de huellas dactilares. Si el identificador biométrico es un mensaje de voz puede ser una contraseña o discurso libre.

El generador de PIN puede utilizar un algoritmo predeterminado. El algoritmo puede ser un algoritmo criptográfico, que utiliza claves criptográficas predeterminadas. Además, puede generarse un PIN nuevo cada vez que se solicita un PIN. De manera conveniente, los PIN pueden generarse de manera secuencial.

El dispositivo de salida puede ser de manera conveniente una pantalla.

Los expertos en la materia apreciarán que es deseable que el dispositivo de facilitación de transacciones financieras pueda funcionar fuera de línea. Por tanto, el identificador biométrico de la persona que realiza la transacción puede almacenarse en la unidad de almacenamiento de datos y el identificador biométrico introducido puede compararse con el identificador almacenado y verificarse si ambos son lo suficientemente similares. Además se apreciará que, por motivos de seguridad, un emisor de la tarjeta de crédito o débito tendrá que autenticar el identificador biométrico almacenado. Por tanto, la persona que realiza la transacción puede autenticar su identidad con el emisor y a continuación se le permitirá introducir su identificador biométrico y almacenarlo, o el emisor puede obtener el identificador biométrico de la persona que realiza la transacción una vez que se ha autenticado la identidad de la persona que realiza la transacción, preferiblemente en persona, y a continuación almacenarlo, u ordenar que se almacene, en la unidad de

almacenamiento de datos. Por tanto, el dispositivo de facilitación de transacciones financieras puede incluir un módulo de comunicación mediante el que puede comunicarse con la entidad financiera.

El dispositivo de facilitación de transacciones financieras puede ser un teléfono móvil, una tableta, un ordenador portátil o un ordenador de sobremesa.

Además según la invención, se proporciona una instalación de procesamiento de transacciones financieras de un emisor de tarjetas de crédito o débito, que incluye una unidad de recepción para recibir una petición de transacción de una persona que realiza la transacción para la cual se ha emitido una tarjeta de crédito o débito junto con un PIN; una unidad de verificación para verificar el PIN; y una unidad de aprobación de transacciones para aprobar la transacción si se verifica el PIN.

Aún según la invención, se proporciona un procedimiento para procesar una transacción financiera, que incluye recibir, por un emisor de una tarjeta de crédito o débito, una petición de transacción junto con un PIN, de una persona que realiza la transacción para la cual se ha emitido la tarjeta; verificar el PIN; y aprobar la transacción si se verifica el PIN.

Como se indicó anteriormente, la invención tiene aplicación particular con tarjetas de crédito y débito que pueden verificarse de manera biométrica. Por tanto la instalación de procesamiento de transacciones financieras puede incluir un módulo de identificación para identificar que la petición de transacción está asociada con una tarjeta que puede verificarse de manera biométrica y que es necesario verificar de manera apropiada el PIN suministrado.

El PIN recibido puede verificarse generándose un PIN de comprobación por la instalación de procesamiento y comparando este PIN con el PIN recibido. Por tanto, la instalación de procesamiento puede incluir un generador de PIN de comprobación y un comparador para comparar los dos PIN. El generador de PIN de comprobación puede utilizar un algoritmo predeterminado que sea igual, o complementario a, el algoritmo utilizado por el dispositivo de facilitación de transacciones financieras. Este algoritmo puede utilizar claves criptográficas asociadas con la cuenta pertinente de la persona que realiza la transacción.

Los expertos en la materia apreciarán que una metodología de PIN variable de este tipo también puede utilizarse cuando se realiza un inicio de sesión en una cuenta con una entidad financiera a través de Internet, y puede utilizarse un PIN variable tal como se suministra y contempla mediante la invención en lugar de un PIN estático. Además, el PIN variable de la invención puede utilizarse en lugar de, o además de, la denominada "autenticación por segundo canal" tal como ocurre cuando se envía un "PIN único" a través de un canal diferente o se utiliza un testigo de autenticación. Por consiguiente, las frases "un dispositivo de facilitación de transacciones financieras para facilitar una transacción financiera" y "un procedimiento para facilitar una transacción financiera" se entenderán como que también incorporan el inicio de sesión en una cuenta con una entidad financiera.

A continuación se describirá la invención a modo de ejemplos no limitativos, haciendo referencia a los dibujos esquemáticos adjuntos, en los que:

la figura 1 muestra un dispositivo de facilitación de transacciones financieras según la invención; y

la figura 2 muestra una instalación de procesamiento de transacciones financieras según la invención.

Haciendo referencia a la figura 1, se hace referencia en general a un dispositivo de facilitación de transacciones financieras con el número de referencia 10. El dispositivo de facilitación de transacciones financieras 10 comprende un teléfono móvil que pertenece a un cliente de una entidad financiera para el cual se ha emitido una tarjeta de crédito. El dispositivo de facilitación de transacciones financieras 10 presenta un procesador 12, una unidad de almacenamiento de datos 14, un teclado numérico 16, una pantalla 18, un micrófono 20 con un convertidor de analógico a digital 22, un generador de PIN 24 y una unidad de verificación 26. Además presenta una interfaz 28 de entrada/salida mediante la que puede conectarse a Internet 30. El teclado numérico 16 puede ser físico o virtual.

En uso, se descargan una aplicación de generación de PIN y un mensaje de voz autenticado, a través de Internet 30 desde la instalación de procesamiento de transacciones financieras mostrada en la figura 2 y se almacenan en la unidad de almacenamiento de datos 14. La aplicación de generación de PIN implementa un algoritmo predeterminado con claves criptográficas, que también se almacenan de

manera segura en la unidad de almacenamiento de datos 14.

Cuando el cliente desea realizar una transacción que requiere un PIN, invoca a la aplicación de generación de PIN por medio del teclado numérico 16. A continuación se le pide que proporcione el mismo mensaje de voz, que se capta mediante el micrófono 20 y el convertidor A/D 22. Este identificador biométrico suministrado se compara entonces, mediante la unidad de verificación 26 con el mensaje de voz autenticado almacenado. Si son lo suficientemente similares, se verifica el mensaje de voz suministrado y se suministra una señal apropiada por la unidad de verificación 26 al procesador 12. A continuación el procesador 12 activa el generador de PIN que genera un PIN que se suministra a la pantalla 18, generándose cada vez un PIN nuevo. El PIN lo utiliza el cliente para realizar su transacción introduciéndolo en un dispositivo ATM o POS, para realizar una transacción por Internet o para iniciar sesión en una cuenta con una entidad financiera. Se apreciará que el dispositivo de facilitación de transacciones financieras 10 puede funcionar fuera de línea.

A continuación se ilustra un ejemplo de cómo se genera el PIN variable. Éste utiliza claves criptográficas y parámetros almacenados en la unidad de almacenamiento de datos 14:

1. Crear el bloque de Borrar Datos de PIN variable.

2. Crear certificado de PIN variable (Claves Diversificadas)

3. Incrementar número de secuencia.

4. Convertir el certificado a decimales (dígitos numéricos ASCII)

5. Extraer dígitos de PIN del certificado decimal.

6. Mostrar los dígitos de PIN. (Máximo 12 dígitos).

Los detalles de transacción junto con el PIN, se transmiten a través de redes de comunicación bancarias convencionales al banco emisor que tiene una instalación de procesamiento de transacciones financieras tal como se muestra en general en la figura 2 con el número de referencia 50. Se apreciará que el PIN se genera en un formato que es

compatible con las instalaciones de transacciones financieras convencionales tales como dispositivos ATM y POS sin cambios adicionales de sus sistemas asociados.

La instalación 50 de procesamiento de transacciones financieras presenta un componente de área de atención al público 52 y un componente de área administrativa 54. En el área de atención al público 52 hay un procesador 56, un teclado numérico 58, una pantalla 60 y un micrófono 62 con un convertidor A/D 64.

En el área administrativa hay un procesador 66, una unidad de almacenamiento de datos 68, un generador de claves criptográficas 70, un generador de aplicaciones de generación de PIN 72, una unidad de identificación de tipo de tarjeta 74, un generador de PIN de comprobación 76, un comparador 78, un generador de mensajes 80 y una interfaz 83 de entrada/salida para la conexión a Internet 30 o una red 82 de comunicación bancaria.

En uso, cuando el cliente desea adquirir la aplicación de generación de PIN, se presenta frente a un empleado del banco en el área de atención al público 52. Cuando el cliente ha verificado su identidad frente al empleado del banco el cliente dice el mensaje de voz que se captura por el micrófono 62 y el convertidor A/D 64 como mensaje de voz autenticado. Este mensaje de voz autenticado se almacena en la unidad de almacenamiento de datos 68 asociada con la cuenta del cliente. A continuación se proporcionan las claves criptográficas requeridas mediante el generador de claves criptográficas 70 y también se almacenan en la unidad de almacenamiento de datos 68 asociadas con la cuenta del cliente. Estas claves y el mensaje de voz autenticado se suministran entonces al generador de aplicaciones de generación de PIN 72 que proporciona la aplicación de generación de PIN que a continuación se descarga al teléfono del cliente 10 a través de Internet 30.

Cuando se recibe una petición de transacción, a través de la red 82 de comunicación, junto con un PIN que ha proporcionado la persona que realiza la transacción, se identifica la cuenta pertinente y se realiza una comprobación mediante la unidad de identificación de tipo de tarjeta 74 para ver si es necesario verificar el PIN suministrado. En este caso, se suministran las claves criptográficas apropiadas al generador de PIN de comprobación 76. El generador de PIN de comprobación 76 genera entonces un PIN de comprobación utilizando un algoritmo similar al descrito anteriormente y el PIN de comprobación y el PIN suministrado se comparan mediante el comparador 78. Si son iguales, entonces se

proporciona un mensaje de aprobación mediante el generador de mensajes 80 y se transmite al banco adquiriente. Evidentemente, si no hay coincidencia entonces se genera y transmite un mensaje de rechazo.

La invención descrita anteriormente permite que la verificación biométrica tenga lugar en un teléfono móvil, o similar, fuera de línea y que este resultado de verificación se represente en forma de PIN que entonces puede introducirse en cualquier dispositivo de POS o ATM.

Esta invención presenta la ventaja de que los números PIN son más seguros puesto que varían con cada transacción efectuada.

Se apreciará que la presente invención vincula intrínsecamente la verificación biométrica al PIN variable, proporcionando por tanto verificación biométrica en cualquier dispositivo de POS o ATM no dotado de tecnología de captura biométrica.

REIVINDICACIONES

1. Dispositivo (10) de facilitación de transacciones financieras, caracterizado por que comprende:

un dispositivo de procesamiento electrónico (12);
una unidad de almacenamiento de datos (14);
un dispositivo de entrada (16);
un dispositivo de entrada de identificador biométrico (20); y
un dispositivo de salida (18);

caracterizado por que además comprende:
una unidad de verificación (26) para verificar un identificador biométrico proporcionado, en uso, por la persona que realiza una transacción; y
un generador de PIN (24) para generar un PIN si se verifica el identificador biométrico introducido;

en el que
dicho dispositivo de entrada (16) puede hacerse funcionar por una persona que realiza la transacción para introducir una petición de un PIN;
dicho dispositivo de entrada de identificador biométrico (20) puede hacerse funcionar para introducir un identificador biométrico de la persona que realiza la transacción; y
dicho dispositivo de salida (18) se hace funcionar para suministrar el PIN a la persona que realiza la transacción.

2. Dispositivo (10) de facilitación de transacciones financieras según la reivindicación 1, caracterizado por que el identificador biométrico es una señal de sonido, y por que el dispositivo de entrada de identificador biométrico (20) comprende un micrófono.

3. Dispositivo (10) de facilitación de transacciones financieras según la reivindicación 1, caracterizado por que el identificador biométrico es una señal visual, y por que el dispositivo de entrada de identificador biométrico (20) comprende una cámara.

4. Dispositivo (10) de facilitación de transacciones financieras según la reivindicación 1, caracterizado por que el identificador biométrico es una huella dactilar, y por que el dispositivo de entrada de identificador biométrico (20) comprende un escáner de huellas

dactilares.

5. Dispositivo (10) de facilitación de transacciones financieras según la reivindicación 1, caracterizado por que el generador de PIN (24) utiliza un algoritmo predeterminado.

6. Dispositivo (10) de facilitación de transacciones financieras según la reivindicación 5, caracterizado por que el algoritmo es un algoritmo criptográfico que utiliza claves criptográficas predeterminadas.

7. Dispositivo (10) de facilitación de transacciones financieras según la reivindicación 5, caracterizado por que el generador de PIN (24) está configurado para generar un PIN nuevo cada vez que se solicita un PIN.

8. Dispositivo (10) de facilitación de transacciones financieras según la reivindicación 5, caracterizado por que el generador de PIN (24) está configurado para generar unos PIN de una manera secuencial.

9. Dispositivo (10) de facilitación de transacciones financieras según la reivindicación 1, caracterizado por que el dispositivo de salida (18) es una pantalla.

10. Dispositivo (10) de facilitación de transacciones financieras según la reivindicación 1, caracterizado por que comprende además un módulo de comunicación (28) para la comunicación con una entidad financiera.

11. Dispositivo (10) de facilitación de transacciones financieras según la reivindicación 1, caracterizado por que el dispositivo (10) de facilitación de transacciones financieras se selecciona de entre el grupo que consiste en un teléfono móvil, una tableta, un ordenador portátil y un ordenador de sobremesa.

12. Procedimiento para facilitar una transacción financiera, caracterizado por que comprende las etapas siguientes:

introducir, por parte de una persona que realiza la transacción, una petición de un PIN en un dispositivo (10) electrónico según cualquiera de las reivindicaciones 1 a 11 de la persona que realiza la transacción;
introducir un identificador biométrico de la persona que realiza la transacción;

verificar el identificador biométrico introducido;
generar un PIN si se verifica el identificador biométrico introducido; y
suministrar el PIN a la persona que realiza la transacción.

13. Procedimiento según la reivindicación 12, caracterizado por que el identificador biométrico se selecciona de entre el grupo que consiste en una señal de sonido, una señal visual o una huella dactilar.

14. Procedimiento según la reivindicación 12, caracterizado por que el identificador biométrico es una señal de sonido, y por que el dispositivo de entrada de identificador biométrico (20) comprende un micrófono.

15. Procedimiento según la reivindicación 14, caracterizado por que la señal de sonido es un mensaje de voz que comprende una contraseña o discurso libre.

16. Procedimiento según la reivindicación 12, caracterizado por que el identificador biométrico es una señal visual, y por que el dispositivo de entrada de identificador biométrico (20) comprende una cámara.

17. Procedimiento según la reivindicación 16, caracterizado por que la señal visual es una representación de la persona que realiza la transacción.

18. Procedimiento según la reivindicación 12, caracterizado por que el identificador biométrico es una huella dactilar, y por que el dispositivo de entrada de identificador biométrico (20) comprende un escáner de huellas dactilares.

19. Procedimiento según la reivindicación 12, caracterizado por que cada vez que se solicita un PIN se genera un PIN nuevo.

20. Procedimiento según la reivindicación 12, caracterizado por que los PIN se generan de manera secuencial.

21. Instalación (50) de procesamiento de transacciones financieras de un emisor de tarjetas de crédito o débito, que comprende:

una unidad de recepción para recibir una petición de transacción de una persona que

realiza la transacción para la cual se ha emitido una tarjeta de crédito o débito junto con un PIN;

una unidad de verificación para verificar el PIN; y

una unidad de aprobación de transacciones para aprobar la transacción si se verifica el PIN;

caracterizada por que además comprende un módulo de identificación (74) para identificar que la petición de transacción está asociada con una tarjeta que puede verificarse de manera biométrica mediante un dispositivo (10) de facilitación de transacciones financieras según cualquiera de las reivindicaciones 1 a 11, y que es necesario verificar el PIN suministrado.

22. Instalación de procesamiento de transacciones financieras según la reivindicación 21, caracterizada por que comprende además un generador de PIN de comprobación (76) para generar un PIN de comprobación y un comparador (78) para comparar el PIN de comprobación y el PIN recibido.

23. Instalación (50) de procesamiento de transacciones financieras según la reivindicación 22, caracterizada por que el generador de PIN de comprobación (76) utiliza un algoritmo predeterminado que es igual, o complementario, a un algoritmo utilizado por dicho dispositivo (10) de facilitación de transacciones financieras.

24. Procedimiento para procesar una transacción financiera, caracterizado por que comprende las etapas siguientes:

recibir en una instalación (50) según cualquiera de las reivindicaciones 21 a 23, por un emisor de una tarjeta de crédito o débito, una petición de transacción junto con un PIN, de una persona que realiza la transacción para la cual se ha emitido la tarjeta;

verificar el PIN recibido; y

aprobar la transacción si se verifica el PIN.

25. Procedimiento según la reivindicación 24, caracterizado por que el PIN recibido se verifica generando un PIN de comprobación y comparándolo con el PIN recibido.

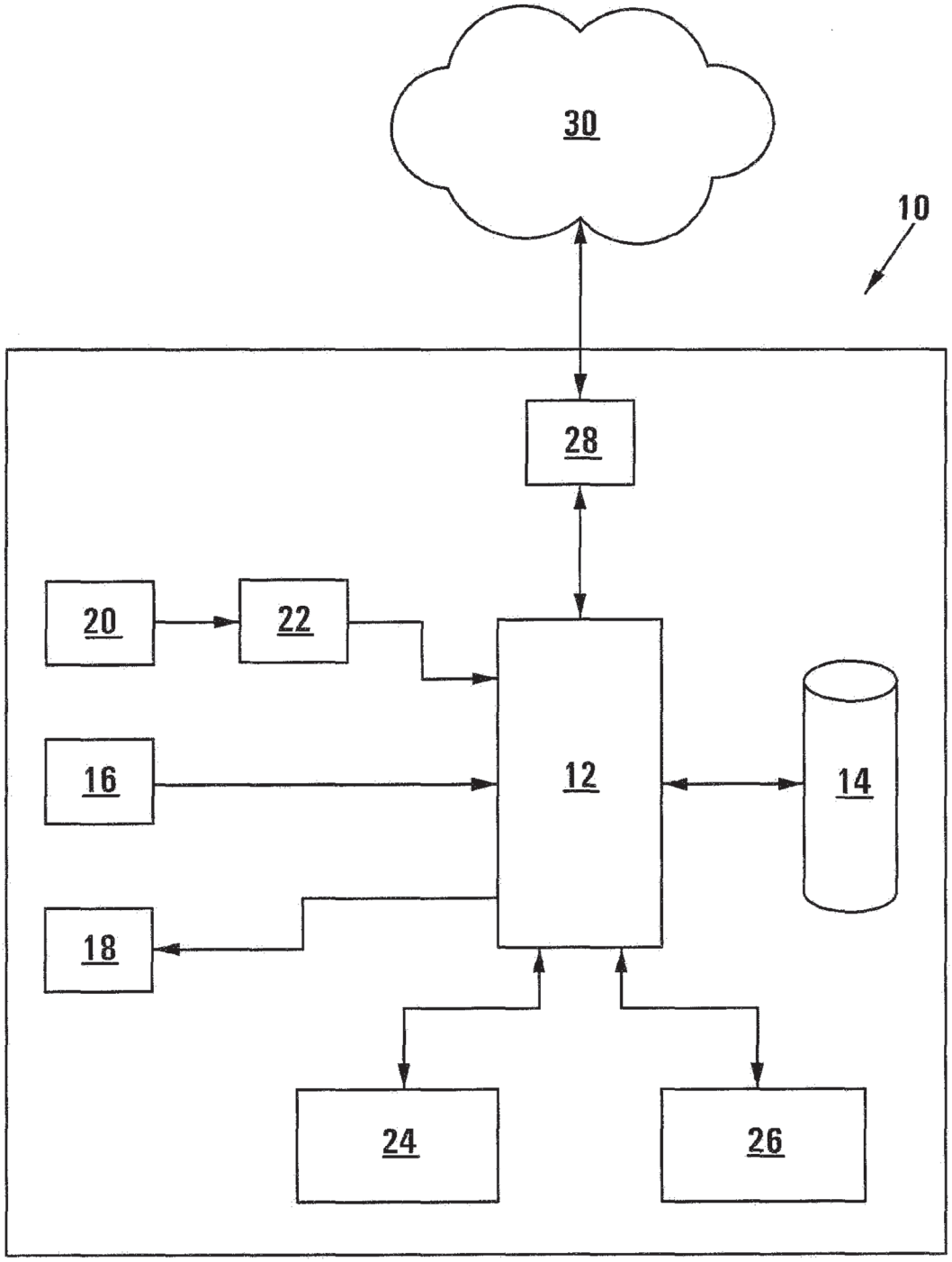

FIG 1

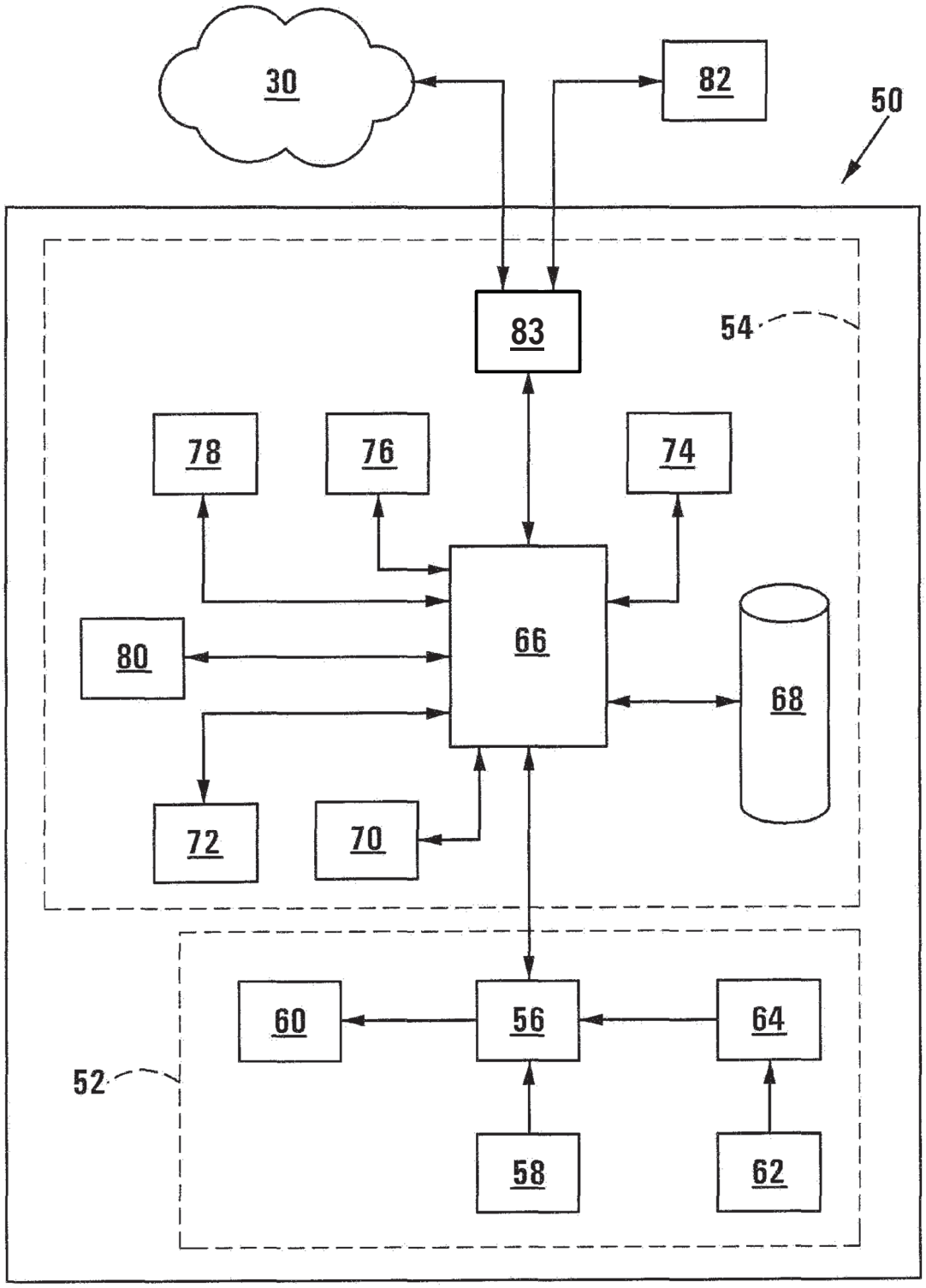

FIG 2