(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 542 706**

(51) Int. CI.:

G07D 11/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.03.2012 E 12717206 (2)**

(97) Fecha y número de publicación de la concesión europea: **29.04.2015 EP 2689401**

(54) Título: **Procedimiento de operación de un cofre de dinero con claves específicas de los clientes**

(30) Prioridad:

21.03.2011 DE 102011001430

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.08.2015

(73) Titular/es:

WINCOR NIXDORF INTERNATIONAL GMBH (100.0%)
Heinz-Nixdorf-Ring 1
33106 Paderborn, DE

(72) Inventor/es:

SCHMIDT, CHRISTOPH y
RINGEL, SASCHA

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento de operación de un cofre de dinero con claves específicas de los clientes

La invención concierne a un procedimiento de operación de un cofre de dinero en el que se almacenan en fábrica en un elemento de memoria de una unidad de control del cofre de dinero los datos de un programa de arranque de producción para poner en funcionamiento el cofre de dinero y una clave de producción para cifrar datos emitidos por el cofre de dinero y/o para descifrar datos recibidos.

El cofre de dinero se utiliza especialmente en dispositivos de manejo de documentos de valor, tales como sistemas de caja automática, cajas fuertes automáticas y/o cajeros automáticos, así como en estaciones de acoplamiento en centros de dinero. Cuando los cofres de dinero están instalados en uno de los dispositivos anteriormente citados, se establece entonces entre el cofre de dinero y el dispositivo un enlace de comunicación de datos a través del cual se pueden transmitir datos entre el dispositivo y el cofre de dinero. En particular, se pueden transmitir datos mediante los cuales se puedan realizar ajustes del cofre de dinero, tal como, por ejemplo, la activación y desactivación de unidades de inutilización, como, por ejemplo kits de tinta, para inutilizar documentos de valor recibidos en el cofre de dinero. En particular, se pueden variar los criterios referentes al momento en que se pone en marcha una unidad de inutilización de esta clase. Asimismo, es posible ajustar y variar temporizadores que están disponibles para los distintos pasos del procedimiento durante el manejo del cofre de dinero.

Para asegurar la transmisión de tales datos relevantes para la seguridad y, por tanto, prevenir intentos de manipulación se cifran los datos transmitidos entre los dispositivos y el cofre de dinero. Un procedimiento de cifrado de los datos transmitidos es conocido, por ejemplo, por el documento DE 10 2009 032 355. En el procedimiento de cifrado conocido es problemático el hecho de que, debido al empleo de una clave de producción unitaria, cualquiera que conozca estas claves de producción podría descifrar los datos de todos los cofres de dinero que están en circulación y, por tanto, podría variar los ajustes de los cofres de dinero. Los operadores de los cofres de dinero, es decir, los clientes, adaptan especialmente los ajustes relevantes para la seguridad a sus circunstancias individuales. Debido al empleo de esta clave de producción unitaria los cofres de dinero de un cliente se podrían utilizar también en el dispositivo de otro cliente, de modo que este otro cliente podría variar el ajuste del primer cliente.

Por el documento DE 10 2010 061 070 aún no publicado es conocido el recurso de emplear varias claves para diferentes grupos de aparatos.

Por el documento WO 2011/003712 A1 se conoce un procedimiento de operación de un cofre de dinero en el que está almacenada de fábrica en un elemento de memoria del cofre de dinero una clave de producción para cifrar datos emitidos por el cofre de dinero y/o para descifrar datos recibidos.

El documento FR 2 929 429 A1 describe la sustitución de programas de arranque en sistemas de ordenador, por ejemplo cuando deban sustituirse programas anticuados por otros nuevos.

El problema de la invención consiste en indicar un procedimiento de operación de un cofre de dinero con cuya ayuda sea posible una operación del cofre de dinero segura frente a manipulaciones.

Este problema se resuelve por un procedimiento dotado de las características de la reivindicación 1. En las reivindicaciones subordinadas se indican perfeccionamientos ventajosos de la invención.

Según la invención, el cofre de dinero es insertado después de su fabricación, para la puesta en servicio del mismo, en un dispositivo destinado a recibir cofres de dinero y se establece entonces un enlace de transmisión de datos entre este dispositivo y el cofre de dinero. A continuación, se sustituyen los datos del programa de arranque de producción por datos de un programa de arranque de operación para poner en funcionamiento el cofre de dinero y se sustituye la clave de producción por una clave de operación específica del cliente para cifrar datos emitidos por el cofre de dinero y/o para descifrar datos recibidos.

Debido al empleo de claves de operación específicas de los clientes, con cuya ayuda se cifra la comunicación entre el cofre de dinero y los dispositivos para el manejo de documentos de valor del cliente en los que debe instalarse el cofre de dinero, se consigue que el cofre de dinero pueda ser operado solamente en estos dispositivos de dicho cliente. En particular, se consigue así que se puedan variar ajustes del cofre de dinero, especialmente ajustes de seguridad, tales como, por ejemplo, los ajustes de unidades de inutilización, solamente por el operador del cofre de dinero, es decir, por el cliente. Por tanto, se consigue un alto grado de seguridad. La sustitución del programa de arranque de producción por el programa de arranque de operación asegura que el firmware del cofre de dinero no pueda ser variado por personas no autorizadas, de modo que no se puede orillar el cifrado por medio de la clave de operación específica del cliente. Los clientes son especialmente bancos e institutos de crédito.

Por sustitución de los datos del programa de arranque o sustitución de la clave se entiende en general que, después de la sustitución, solamente se puede emplear todavía el programa de arranque de operación para la puesta en funcionamiento del cofre de dinero y solamente se puede emplear todavía la clave de operación específica del

cliente para la comunicación. En este caso, se sobreescriben especialmente los datos del programa de arranque de producción con los datos del programa de arranque de operación y/o se sobreescribe la clave de producción con la clave de operación específica del cliente. Como alternativa, también pueden no sobreescribirse los datos correspondientes, sino que los datos del programa de arranque de producción y la clave de producción pueden seguirse almacenando como antes en el elemento de memoria del cofre de dinero. En este caso, se almacenan adicionalmente en el elemento de memoria los datos del programa de arranque de operación y la clave de operación específica del cliente. El programa de arranque de producción y la clave de producción pierden su validez, de modo que solamente puede emplearse todavía el programa de arranque de operación para la puesta en funcionamiento y solamente puede emplearse todavía la clave de operación para el cifrado.

El dispositivo destinado a recibir cofres de dinero, en el que se instala el cofre de dinero para la puesta en servicio, consiste especialmente en una llamada estación de acoplamiento mediante la cual se puede establecer un enlace de transmisión de datos con el cofre de dinero. Este enlace de transmisión de datos está formado especialmente por una conexión de enchufe. Como alternativa, la transmisión de datos puede efectuarse también por vía inalámbrica, por ejemplo a través de WLAN o radio. Por estación de acoplamiento se entiende especialmente un dispositivo en el que se instalan los cofres de dinero para su llenado y/o vaciado en un entorno securizado, por ejemplo un centro de dinero.

El programa de arranque de producción es sustituido especialmente por un programa de arranque de operación específico del cliente. Como alternativa, el programa de arranque de producción puede sustituirse también primeramente por un programa de arranque de operación estándar, transmitiéndose seguidamente datos con informaciones sobre la clave de operación específica del cliente a través del enlace de transmisión de datos desde el dispositivo hasta el cofre de dinero y sustituyéndose la clave de producción por la clave de operación específica del cliente. Gracias a esta transmisión de la clave de operación específica del cliente el programa de arranque de operación estándar se convierte entonces también en un programa de arranque de operación específico del cliente. Se consigue así que un programa de operación estándar pueda almacenarse ciertamente de momento en los elementos de memoria de una manera unitaria y, no obstante, sea posible, debido a la individualización específica del cliente mediante la clave de operación, una operación del cofre de dinero solamente en los dispositivos destinados a manejar documentos de valor de este mismo cliente.

Los datos del programa de arranque de operación, los datos con las informaciones sobre la clave de operación específica del cliente y/o la clave de operación específica del cliente se cifran preferiblemente de momento por el dispositivo con ayuda de la clave de producción y se transmiten como datos cifrados al cofre de dinero a través del enlace de transmisión de datos. La unidad de control del cofre de dinero descifra seguidamente estos datos cifrados con ayuda de la clave de producción y sustituye por ellos el programa de arranque de producción y/o la clave de producción. Se consigue así una transmisión de datos segura, de modo que se evitan manipulaciones en la transmisión de datos y, por tanto, eventuales manipulaciones posteriores del cofre de dinero. En particular, se consigue así que se almacene realmente también la clave de operación específica del cliente que deba ser igualmente almacenada.

La clave de operación específica del cliente se almacena preferiblemente también en un elemento de memoria de al menos un dispositivo destinado a manejar documentos de valor, en el que se debe instalar el cofre de dinero durante la operación. En la comunicación entre el dispositivo y el cofre de dinero instalado en el mismo se cifran los datos transmitidos con ayuda de esta clave de operación específica del cliente. Por tanto, se consigue el cofre de dinero pueda hacerse funcionar solamente en los dispositivos de manejo de documentos de valor a los cuales esté destinado dicho cofre. En particular, en todos los dispositivos de manejo de documentos de valor en los que deba instalarse el cofre de dinero durante la operación, se almacena la clave de operación específica del cliente en un respectivo elemento de memoria.

El cifrado de los datos transmitidos entre el dispositivo de manejo de documentos de valor y el cofre de dinero durante la operación y/o el cifrado de los datos transmitidos desde el dispositivo de alojamiento de los cofres de dinero y el cofre de dinero durante la puesta en servicio se efectúan especialmente con ayuda de un algoritmo de cifrado por bloques. Se consigue así un cifrado sencillo, pero, no obstante, seguro. En particular, se emplean para el cifrado un algoritmo de cifrado Blowfish, un algoritmo de cifrado del estándar de encriptado avanzado (AES), un algoritmo de cifrado del estándar de encriptado de datos (DES) y un algoritmo de encriptado diminuto extendido (XTEA).

En una forma de realización preferida de la invención se almacenan varias claves de operación específicas del cliente en el elemento de memoria del cofre de dinero. En el elemento de memoria de varios dispositivos de manejo de documentos de valor está almacenada cada vez al menos una de estas claves de operación, efectuándose la comunicación entre uno de estos dispositivos y el cofre de dinero instalado en este dispositivo de tal manera que los datos transmitidos pueden ser cifrados con ayuda de la clave de operación correspondiente específica del cliente almacenada en el elemento de memoria del dispositivo y en el elemento de memoria del cofre de dinero. Se consigue así que el cofre de dinero pueda operarse en los dispositivos de manejo de documentos de valor de varios

clientes y, por tanto, de varios grupos de aparatos.

Asimismo, es ventajoso que los datos se transmitan en un llamado procedimiento de desafío-respuesta entre el cofre de dinero y el dispositivo de manejo de documentos de valor. Este procedimiento de desafío-respuesta es conocido, por ejemplo, por el documento DE 10 2009 032 355 A1. El desarrollo del procedimiento de desafío-respuesta es recogido con esta mención por referencia en la presente descripción.

En una forma de realización especialmente preferida de la invención el procedimiento de desafío-respuesta comprende al menos los cinco pasos siguientes: En un primer paso se transmiten, a través del enlace de transmisión de datos, unos datos con informaciones para solicitar un número aleatorio desde el dispositivo de manejo de documentos de valor hasta el cofre de dinero instalado en el mismo. A continuación, en un segundo paso el cofre de dinero genera un número aleatorio con ayuda de un algoritmo de generación de números aleatorios archivado en la unidad de control y cifra este número aleatorio antes de que el cofre de dinero lo transmita al dispositivo a través del enlace de transmisión de datos. En un tercer paso el dispositivo descifra el número aleatorio cifrado y genera datos con al menos una orden de control, comprendiendo estos datos los números aleatorios. A continuación, en el cuarto paso el dispositivo cifra estos datos con la clave de operación específica del cliente y transmite los datos cifrados al cofre de dinero. En un quinto paso el cofre de dinero descifra los datos transmitidos al mismo con ayuda de la clave de operación específica del cliente y compara el número aleatorio contenido en los datos descifrados con el número aleatorio que fue generado por el algoritmo de generación de números aleatorios en el segundo paso.

Si esta comparación arroja el resultado de que coinciden el número aleatorio generado y el número aleatorio transmitido en el cuarto paso, el cofre de dinero ejecuta entonces la orden de control transmitida. Por el contrario, si la comparación arroja el resultado de que no coinciden los números aleatorios, el cofre de dinero no ejecuta entonces la orden de control. En particular, el cofre de dinero genera en este caso un aviso de error y almacena los datos con informaciones sobre este aviso de error en un elemento de memoria y/o transmite datos con informaciones sobre este aviso de error al dispositivo en el que está alojado el cofre de dinero. Éste a su vez indica especialmente el aviso de error por medio de una unidad indicadora.

Mediante el procedimiento de desafío-respuesta anteriormente descrito se consigue una transmisión de datos muy segura entre el dispositivo y el cofre de dinero instalado en el mismo. Gracias al cifrado con la clave de operación específica del cliente se consigue también que la comunicación entre el cofre de dinero y el dispositivo sea posible únicamente cuando esta clave de operación específica del cliente esté almacenada tanto en el elemento de memoria con el cofre de dinero como en el elemento de memoria del dispositivo. Por tanto, el cofre de dinero puede operarse solamente en los dispositivos a los que está también destinado.

La clave de operación actual específica del cliente, que está almacenada actualmente en el elemento de memoria del cofre de dinero y con cuya ayuda se cifran o descifran los datos emitidos por el cofre de dinero y los datos recibidos por el cofre de dinero, puede variarse especialmente tan solo con ayuda de esta clave de operación actual específica del cliente. Esto se consigue especialmente debido a que se procesan por el cofre de dinero o la unidad de control del cofre de dinero únicamente los datos recibidos que realmente han sido cifrados con la clave de operación actual específica del cliente. Los datos que se hayan cifrado con otra clave de operación no pueden ser descifrados por el cofre de dinero y no se ejecutan especialmente los datos no cifrados. Se consigue así especialmente que una comunicación entre el cofre de dinero y otro dispositivo sea posible solamente a través de datos cifrados con la clave de operación actual específica del cliente y, por tanto, una variación de la clave de operación puede efectuarse solamente en conocimiento de la clave de operación actual específica del cliente.

El elemento de memoria del cofre de dinero comprende especialmente una memoria flash en la que están almacenados los datos del programa de arranque de producción, los datos del programa de arranque de operación, la clave de producción y/o la clave de operación. Por tanto, se garantiza una constitución sencilla del elemento de memoria del cofre de dinero.

En el elemento de memoria del cofre de dinero está almacenado preferiblemente un firmware de operación del cofre de dinero. La firma es especialmente un código de autenticación de mensajes de una clave (OMAC) que se basa en un algoritmo de cifrado por bloques.

En una forma de realización preferida de la invención se almacena la clave de operación específica del cliente como parte de este firmware. Se consigue así un grado de seguridad especialmente alto, ya que una manipulación de la clave de operación específica del cliente conduce en general a que también sea manipulado el firmware y, por tanto, ya no sea posible operar el cofre de dinero.

El firmware comprende especialmente una firma. La unidad de control establece, en función de esta firma, la admisibilidad del firmware, a cuyo fin dicha unidad comprueba con ayuda de la firma si se ha variado el firmware. La firma es especialmente una firma que identifica unívocamente al fabricante del cofre de dinero y/o a una empresa de servicios que esté encargada del mantenimiento del cofre de dinero. La operación del cofre de dinero es posible especialmente tan solo cuando la firma del firmware identifica unívocamente a este fabricante o a esta empresa de

servicios que están también realmente autorizados para variar el firmware, y/o cuando la unidad de control ha establecido con ayuda de la firma que no se ha variado inadmisiblemente la firma.

Si la comprobación de la admisibilidad da como resultado que el firmware comprende una firma diferente y, por tanto, falsa, no es posible la operación del cofre de dinero. Se previenen así una manipulación del firmware y una manipulación del cofre de dinero. La comprobación del firmware se efectúa especialmente en cada puesta en funcionamiento del cofre de dinero. Además o alternativamente, esta comprobación puede efectuarse también a intervalos de tiempo preajustados.

Asimismo, es ventajoso que el firmware pueda variarse solamente con ayuda de la clave de operación específica del cliente. Se consigue que así que el firmware pueda ser variado solamente por personas autorizadas, concretamente por personas que dispongan ellas mismas de la clave de operación específica del cliente. Se previene así una manipulación del firmware y, por tanto, del cofre de dinero. En particular, la unidad de control del cofre de dinero ejecuta solamente los datos transmitidos a ella que están cifrados con la clave de operación específica del cliente. Los datos que están cifrados con otra clave no pueden ser descifrados por el cofre de dinero, y los datos que no están en absoluto cifrados no son procesados por el cofre de dinero. Preferiblemente, la firma transmitida junto con el firmware es cifrada con ayuda de la clave de operación específica del cliente, de modo que la firma solamente puede ser procesada y/o variada con ayuda de la clave de operación específica del cliente.

Otras características y ventajas de la invención se desprenden de la descripción siguiente, que explica la invención con más detalle ayudándose de ejemplos de realización en relación con las figuras adjuntas.

Muestran:

La figura 1, una representación esquemática de un cofre de dinero;

La figura 2, una representación esquemática de un cajero automático y del cofre de dinero según la figura 1 instalado en este cajero automático;

La figura 3, un diagrama de desarrollo de un procedimiento para la puesta en servicio del cofre de dinero;

La figura 4, una representación esquemática de la operación del cofre de dinero según un primer ejemplo de realización;

La figura 5, una representación esquemática de la operación del cofre de dinero conforme a un segundo ejemplo de realización;

La figura 6, una representación esquemática de la operación del cofre de dinero según un tercer ejemplo de realización; y

La figura 7, una representación esquemática de la operación del cofre de dinero según un cuarto ejemplo de realización.

En la figura 1 se ofrece una representación esquemática de un cofre de dinero 10. El cofre de dinero 10 comprende una unidad de inutilización 12 para inutilizar de manera irreversible documentos de valor recibidos en el cofre de dinero, no representados, y una unidad de control 14 para controlar la unidad de inutilización 12. La unidad de control 14 controla la unidad de inutilización 12 especialmente de tal manera que ésta inutiliza los documentos de valor recibidos en el cofre de dinero 10 únicamente cuando existe un intento de manipulación. A este fin, el cofre de dinero 10 comprende especialmente un gran número de sensores no representados con cuya ayuda se pueden detectar los intentos de manipulación. Tales sensores pueden ser, por ejemplo, sensores de posición, sensores de sacudidas, sensores de gas, sensores de líquido y/o sensores para determinar la apertura de una tapa del cofre de dinero 10.

La unidad de inutilización 12 está realizada especialmente en forma de un llamado kit de tinta que, al dispararse, tiñe irreversiblemente, con ayuda de un colorante, los documentos de valor recibidos en el cofre de dinero 10, de moto que estos documentos de valor teñidos no pueden ser puestos en circulación por un potencial ladrón y, por tanto, carecen de valor para él.

Los documentos de valor pueden estar recibidos en el cofre de dinero 10 tanto en forma apilada en una zona de alojamiento como en forma enrollada sobre un acumulador de rodillo. Un acumulador de de rodillo de esta clase comprende especialmente dos cintas de material pelicular entre las cuales están recibidos los documentos de valor.

La unidad de control 14 comprende un microprocesador 16, un primer elemento de memoria 18 y un segundo elemento de memoria 20. El primer elemento de memoria 18 y el segundo elemento de memoria 20 están realizados especialmente cada uno de ellos en forma de una memoria no volátil, por ejemplo en forma de una memoria flash o una EEPROM. En una forma de realización alternativa los elementos de memoria primero y segundo 18, 20 pueden estar realizados también en forma de otras clases de elementos de memoria. Como alternativa, es posible también

que la unidad de control 14 comprenda únicamente un elemento de memoria 18, 20. En el segundo elemento de memoria 20 están almacenados especialmente datos con informaciones sobre el inventario del cofre de dinero 10 en documentos de valor, datos con informaciones sobre intentos de manipulación y/o datos con informaciones sobre el mantenimiento del cofre de dinero 10.

En el primer elemento de memoria 18 están almacenados especialmente datos de un firmware de operación de un cofre de dinero 10 y datos de un programa de arranque para poner en funcionamiento el cofre de dinero 10. El firmware comprende especialmente un algoritmo de generación de números aleatorios para generar números aleatorios y al menos una clave para cifrar los datos a emitir y para descifrar los datos recibidos. El cifrado y el descifrado de los datos, así como la administración de las claves empleadas para ello se explican seguidamente con más detalle en relación con las figuras 2 a 7.

Asimismo, el cofre de dinero 10 tiene un conector de enchufe 22 a través del cual se puede establecer un enlace de transmisión de datos entre el cofre de dinero 10 y dispositivos 30 en los que está instalado este cofre de dinero 10. En una forma de realización alternativa puede estar prevista también, adicional o alternativamente al conector de enchufe 22, otra unidad de emisión y/o recepción para emitir y/o recibir datos. En particular, la emisión y la recepción de los datos pueden efectuarse también por vía inalámbrica, por ejemplo por telefonía móvil.

En la figura 2 se representa el modo en que el cofre de dinero 10 está instalado en un dispositivo 30. Este dispositivo 30 puede consistir, por ejemplo, en un cajero automático, una caja fuerte automática, un sistema de caja automática y/o un bastidor de almacenamiento intermedio de cofres de dinero 10. Este bastidor puede estar dispuesto, por ejemplo, en un vehículo de transporte de valores.

El dispositivo 30 comprende una unidad de emisión y recepción 32 para emitir datos hacia el cofre de dinero 10 y para recibir datos del cofre de dinero 10. Esta unidad de emisión y recepción 32 tiene un conector de enchufe 34 que está configurado de manera complementaria al conector de enchufe 22 del cofre de dinero 10, de modo que, cuando el cofre de dinero 10, como se muestra en la figura 2, está instalado en el dispositivo 10, se puede establecer un enlace de transmisión de datos a través de la conexión de enchufe establecida entre los conectores de enchufe 34 y 22.

Asimismo, el dispositivo 30 tiene una unidad de control 36 que, en el ejemplo de realización mostrado en la figura 2, comprende una primer subunidad de control 38 y una segunda subunidad de control 40 que están unidas una con otra a través de un enlace de transmisión de datos USB 42. En una forma de realización alternativa de la invención la unidad de control 36 puede también no comprender dos subunidades de control 38, 40, sino que puede estar configurada como una única unidad de control 36. La unidad de control 36, especialmente la segunda subunidad de control 40, está unida con la unidad de emisión y recepción 32 a través de un bus CAN 44 para la transmisión de datos. Por tanto, se puede efectuar una transmisión de datos entre la unidad de control 36 del dispositivo 30 y la unidad de control 14 del cofre de dinero 10 a través del enlace de transmisión de datos formado entre los conectores de enchufe 22, 34.

La primera subunidad de control 38 consiste especialmente en un ordenador en el que se emplea un software usual en el mercado para operar este ordenador, especialmente un sistema operativo estándar. La segunda subunidad de control 40 es particularmente una electrónica desarrollada especialmente para el dispositivo 30, en la que se emplean datos de programa de un firmware maestro que está acondicionado especialmente para su utilización en el dispositivo 30 y para el manejo de los datos relevantes para la seguridad. En una forma de realización alternativa de la invención se pueden emplear también otras subunidades de control 38, 40. En particular, los enlaces de transmisión de datos 42, 44 pueden estar configurados también de manera distinta a la anteriormente descrita, no a través de un enlace de transmisión de datos USB o un bus CAN, sino a través de otros enlaces de transmisión de datos.

El cofre de dinero 10 puede operarse en diferentes modos de operación, no disparando la unidad de control 14 a la unidad de inutilización 12 en un modo de operación desconectado, con independencia de si se detecta o no por los sensores un intento de manipulación. Por el contrario, en un modo de operación activado están activados todos los sensores, de modo que la unidad de control 14, cuando al menos uno de estos sensores detecta un intento de manipulación, dispara la unidad de inutilización 12, con lo que se inutilizan los documentos de valor recibidos en el cofre de dinero 10. En un modo de transporte están activados solamente una parte de los sensores. En particular, en el modo de transporte están desactivados los sensores de almacenamiento.

Cuando el cofre de dinero 10 está recibido en el dispositivo 30, se pueden transmitir especialmente, a través de los enlaces de datos establecidos entre los conectores de enchufe 22, 34, unos datos con cuya ayuda se puede ajustar el modo de operación del cofre de dinero 10. Asimismo, se pueden ajustar o variar también por medio de los datos transmitidos otros ajustes relevantes para la seguridad del cofre de dinero 10, tal como, por ejemplo, la fijación de temporizadores para pasos individuales del proceso durante la operación del cofre de dinero 10.

Para impedir intentos de manipulación, especialmente un cambio de posición no autorizado de los modos de operación o de los temporizadores, y para proteger datos confidenciales, se transmiten cifrados los datos a través

del enlace de transmisión de datos entre la unidad de emisión y recepción 32 y el cofre de dinero 10. A este fin, en la unidad de control 36 del dispositivo 30 y en el elemento de memoria 18 de la unidad de control 14 del cofre de dinero 10 está almacenada una clave de operación específica del cliente. Esta clave de operación específica del cliente asegura que el cofre de dinero 10 solamente pueda operarse en los dispositivos 30 que opera el cliente, es decir, el operador del cofre de dinero 10, o sea, los dispositivos 30 para los cuales se debe emplear el cofre de dinero 10. Mediante estas claves de operación específicas del cliente se consigue especialmente que, cuando el cofre de dinero 10 está instalado en dispositivos extraños, no se puedan variar los ajustes del cofre de dinero 10 y no se puedan leer datos del cofre de dinero 10. Por tanto, se incrementa aún más la seguridad.

El cifrado con ayuda de la clave de operación específica del cliente se efectúa especialmente mediante un algoritmo de cifrado por bloques, para lo cual están almacenados datos de este algoritmo de cifrado por bloques en la unidad de control 30 y la unidad de control 14, y estos datos se ejecutan durante el cifrado.

En la figura 3 se representa un diagrama de flujo del desarrollo de la puesta en servicio del cofre de dinero 10. Después de que se haya iniciado el procedimiento en el paso S10, se almacenan en el paso S12, durante la producción en fábrica del cofre de dinero 10, los datos de un programa de arranque de producción para poner en funcionamiento el cofre de dinero 10 y una clave de producción para cifrar los datos a emitir por el cofre de dinero 10 y para descifrar los datos recibidos en el elemento de memoria 18 de la unidad de control 14 del cofre de dinero 10. Esta clave de producción y este programa de arranque de producción se almacenan unitariamente en el respectivo elemento de memoria 18 en todos los cofres de dinero producidos por el fabricante de los cofres de dinero 10, de modo que, con independencia del cofre de dinero 10, todos los datos a transmitir durante la puesta en servicio y/o todas las pruebas de funcionamiento antes del suministro del cofre de dinero 10 al cliente pueden ejecutarse con ayuda de esta clave de producción y este programa de arranque de producción.

A continuación, en el paso S14 se instala el cofre de dinero en una llamada estación de acoplamiento, y en el paso S16 se establece un enlace de transmisión de datos entre el cofre de dinero 10 y la estación de acoplamiento. Como medida siguiente se transmiten en el paso S18 los datos de un programa de arranque de operación a través de este enlace de transmisión de datos desde la estación de acoplamiento hasta el cofre de dinero 10, sustituyendo estos datos del programa de arranque de operación a los datos del programa de arranque de producción. Por sustitución se entiende en general que solo se puede seguir utilizando exclusivamente el programa de arranque de operación y ya no se puede emplear el programa de arranque de producción. A este fin, los datos del programa de producción pueden sobreescribirse en el elemento de memoria 18 con los datos del programa de arranque de operación. Como alternativa, es posible que tanto los datos del programa de producción como los datos del programa de arranque de operación estén almacenados en el elemento de memoria 18, pero los datos del programa de arranque de producción han perdido su validez.

En una forma de realización preferida de la invención la estación de acoplamiento cifra los datos del programa de arranque de operación con la clave de producción y la unidad de control 14 del cofre de dinero 10 descifra los datos transmitidos de una manera correspondiente con la clave de producción. Se consigue así una transmisión de datos segura.

A continuación, en el paso S20 se transmiten datos con una clave de operación específica del cliente desde la estación de acoplamiento hasta el cofre de dinero 10, sustituyendo esta clave de operación específica del cliente a la clave de producción. En este caso, preferiblemente la estación de acoplamiento cifra nuevamente esta clave de operación específica del cliente con la clave de producción y transmite cifrados los datos correspondientes al cofre de dinero 10, que a su vez descifra los datos recibidos con la clave de producción y sustituye la clave de producción por la clave de operación específica del cliente. A continuación, se concluye el procedimiento en el paso S22.

Mediante este procedimiento se consigue que se puedan emplear de momento claves de producción y programas de arranque de producción unitarios durante la fabricación de los cofres de dinero 10, de modo que se pueda efectuar unitariamente la prueba de funcionamiento de los cofres de dinero 10 y sea posible una producción unitaria. La individualización del cofre de dinero 10 según el cliente específico se efectúa únicamente durante la puesta en servicio, de modo que a continuación, durante la operación del cofre de dinero 10, éste puede operarse solamente en dispositivos 30 que dispongan también de la clave de operación específica del cliente. Se consiguen así en conjunto una fabricación sencilla del cofre de dinero 10 y, no obstante, una alta seguridad específica del cliente.

En una forma de realización alternativa de la invención los pasos S18 y S20 pueden estar también permutados, es decir que se pueden transmitir primero la clave de operación específica del cliente y luego el programa de arranque de operación. Además, es posible alternativamente que el programa de arranque de operación y la clave de operación específica del cliente se transmitan conjuntamente en un solo paso.

Una variación de la clave de operación específica del cliente es posible en particular solamente en conocimiento de la clave de operación específica del cliente actualmente almacenada en el elemento de memoria 18. Sin la clave de operación específica del cliente actualmente almacenada en el elemento de memoria 18, ésta no pueda ser variada. A este fin, la unidad de control 14 está diseñada especialmente de tal manera que procesa solamente datos o

ejecuta solamente órdenes que se han cifrado con ayuda de la clave de operación específica del cliente actualmente almacenada en el elemento de memoria 18. Por el contrario, no se procesan los datos que se hayan cifrado con otra clave y/o se hayan transmitidos sin cifrar a la unidad de control 14, o no se ejecutan las órdenes correspondientes.

El firmware del cofre de dinero 10 contiene especialmente una firma que identifica unívocamente al constructor del firmware y/o que asegura que no se haya variado el firmware. El programa de arranque de operación comprende preferiblemente una clave de firma con cuya ayuda la unidad de control 14 puede comprobar si el firmware ha sido construido por el fabricante autorizado y/o si el firmware ha sido variado durante la transmisión. Si la unidad de control 14 detecta que el fabricante de la firma autorizada en el elemento de memoria 18 no estaba autorizado para ello y/o se había variado el firmware, no es posible entonces una operación del cofre de dinero 10 y se almacena especialmente un aviso de error en el segundo elemento de memoria 20 y/o se emite un aviso de error. La clave de firma corresponde especialmente a la clave de operación específica del cliente. La firma es especialmente una firma electrónica, preferiblemente una firma digital.

Se impide de esta manera que se manipule el firmware. Por tanto, se incrementa aún más la seguridad, ya que, debido a que se impida la manipulación del firmware, se excluye también que se eluda el cifrado por medio de la clave de operación.

Adicional o alternativamente al firmado, se evita también una variación del firmware debido a que una variación del firmware es posible solamente en conocimiento de la clave de operación específica del cliente. Sin la clave de operación específica del cliente no se puede variar el firmware, de modo que las personas carentes de autorización no tienen acceso a éste.

La figura 4 es una representación esquemática de la operación del cofre de dinero 10 según un primer ejemplo de realización. En este ejemplo de realización únicamente está almacenada una primera clave de operación A específica del cliente en el primer elemento de memoria 18 del cofre de dinero 10.

Asimismo, en la figura 4 se representan dos bancos 50, 52 que operan cada uno de ellos un grupo de aparatos 56, 58 que comprende un gran número de cajeros automáticos 54. Asimismo, está representada una empresa comercial 60 que opera un grupo de aparatos 64 consistentes en varias cajas fuertes automáticas 62. Además, se muestra esquemáticamente una empresa 66 de transporte de valores que tiene un grupo de aparatos 68 que comprende varios vehículos 70 de transporte de valores en cada uno de los cuales está presente al menos un bastidor 72 para recibir cofres de dinero 10.

El primer banco 50 emplea la primera clave de operación A para la transmisión de datos entre los cajeros automáticos 54 de su grupo de aparatos 56 y los cofres de dinero 10 instalados en estos cajeros automáticos 54. En contraste con esto, el segundo banco 58 emplea para los cajeros automáticos 54 de su grupo de aparatos 58 una clave de operación B diferente de la primera clave de operación A. Asimismo, la empresa comercial 60 y la empresa 66 de transporte de valores emplean también claves de operación propias C y D específicas del cliente, respectivamente, para la comunicación de los aparatos 62, 72 de su grupo de aparatos 64, 68 con cofres de dinero 10.

Dado que en el primer ejemplo de realización está almacenada en el cofre de dinero 10 únicamente la clave de operación A específica del cliente, el cofre de dinero 10 puede operarse solamente en los cajeros automáticos 54 del primer grupo de aparatos 56 del primer banco 50. Si se instala el cofre de dinero 10 en un cajero automático 54 del segundo grupo de aparatos 58, una caja fuerte automática 62 del tercer grupo de aparatos 64 o un bastidor 72 del cuarto grupo de aparatos 68, no se puede efectuar entonces una comunicación entre el cofre de dinero 10 y el aparato correspondiente 54, 62, 72 ya que la unidad de control 14 del cofre de dinero 10 no puede descifrar los datos cifrados transmitidos por el aparato 54, 62, 72 y, recíprocamente, los aparatos 54, 62, 72 no pueden descifrar los datos transmitidos a ellos por el cofre de dinero 10.

En la figura 5 se muestra una representación esquemática de la operación del cofre de dinero 10 conforme a un segundo ejemplo de realización. En este segundo ejemplo de realización están almacenadas en el elemento de memoria 18 del cofre de dinero 10 tanto la clave de operación A específica del cliente, la clave de operación B específica del cliente y la clave de operación C específica del cliente como la clave de operación D específica del cliente. Por tanto, es posible una comunicación entre el cofre de dinero 10 y los cajeros automáticos 54 del primer grupo de aparatos 56, el cofre de dinero 10 y los cajeros automáticos 54 del segundo grupo de aparatos 58, el cofre de dinero 10 y las cajas fuertes automáticas 62 del tercer grupo de aparatos 64 y el cofre de dinero 10 y los bastidores 72 del cuarto grupo de aparatos 68, de modo que el cofre de dinero 10 puede ser operado en los cuatro grupos de aparatos 56, 58, 64, 68.

En la figura 6 se muestra una representación esquemática de la operación del cofre de dinero 10 según un tercer ejemplo de realización. En este tercer ejemplo de realización está almacenada en el elemento de memoria 18 del cofre de dinero 10 únicamente la primera clave de operación A específica del cliente. A diferencia de los dos primeros ejemplos de realización, el primer banco 50 proporciona su clave de operación A específica del cliente tanto al segundo banco 52 como a la empresa comercial 60 y a la empresa 66 de transporte de documentos de

valor, de modo que los aparatos de los grupos de aparatos 58, 64, 68 pueden emplear también esta clave de operación A específica del cliente para la comunicación con el cofre de dinero 10, con lo que el cofre de dinero 10 puede operarse en los cuatros grupos de aparatos 56, 58, 64, 68.

En la figura 7 se muestra una representación esquemática de la operación del cofre de dinero 10 según un cuarto ejemplo de realización. En este cuarto ejemplo de realización no se ha sustituido la clave de producción P en el elemento de memoria 18 por una clave de operación específica del cliente. En particular, no se ha ejecutado el procedimiento según la figura 3 para la puesta en servicio del cofre de dinero 10. Los bancos 50, 52, la empresa comercial 60 y la empresa 66 de transporte de documentos de valor disponen también de esta clave de producción estandarizada P, de modo que el cofre de dinero 10 puede operarse en todos los grupos de aparatos 56, 58, 64, 68.

En el primer elemento de memoria 18 están reservados especialmente al menos 64 bits para la clave de operación específica del cliente. En una forma de realización preferida se pueden almacenar en el primer elemento de memoria 18 no solo una clave de operación específica del cliente, sino 32 claves de operación específicas de clientes. Para hacer esto posible se han reservado, para una longitud de clave de al menos 64 bits, al menos 256 bytes del elemento de memoria 18 para las claves de operación específicas de los clientes.

La comunicación entre el cofre de dinero 10 con los dispositivos 30, 54, 62, 72 se efectúa especialmente por medio de un llamado procedimiento de desafío-respuesta. En este procedimiento de desafío-respuesta el dispositivo 30, 54, 62, 72 transmite primeramente al cofre de dinero 10 una orden de generar un número aleatorio. En la unidad de control 14 está almacenado un algoritmo de generación de números aleatorios con cuya ayuda la unidad de control 14 del cofre de dinero 10 genera seguidamente un número aleatorio. Para que este número aleatorio no pueda ser capturado por terceros, el cofre de dinero 10 cifra el número aleatorio con ayuda de una clave de desafío y transmite seguidamente el número aleatorio cifrado al dispositivo 30, 54, 62, 72. El dispositivo 30, 54, 62, 72 descifra a continuación los datos recibidos del cofre de dinero 10 con ayuda de esta clave de desafío y genera datos con informaciones sobre una orden a ejecutar por el cofre de dinero 10, comprendiendo estos datos el número aleatorio. El dispositivo 30, 54, 62, 72 cifra estos datos a través de la clave de operación específica del cliente y transmite los datos cifrados al cofre de dinero 10, que seguidamente descifra de nuevo los datos con ayuda de la clave de operación específica del cliente.

A continuación, la unidad de control 14 compara el número aleatorio contenido en los datos con el número aleatorio originalmente generado por el algoritmo de números aleatorios. Si coinciden los dos números aleatorios, el cofre de dinero 10 ejecuta entonces la orden contenida en los datos. Por el contrario, si no coinciden los números aleatorios, el cofre de dinero 10 no ejecuta entonces la orden y genera datos con informaciones sobre un aviso de error que dicho cofre transmite al dispositivo 30, 54, 62, 72.

Mediante el procedimiento de desafío-respuesta anteriormente descrito se consigue un alto grado de seguridad de transmisión. Por tanto, se previenen especialmente intentos de manipulación.

En una forma de realización alternativa de la invención se pueden emplear también procedimientos distintos al procedimiento de desafío-respuesta anteriormente descrito para la comunicación entre el cofre de dinero 10 y el dispositivo 30, 54, 62, 72. Además, es posible alternativamente que se utilicen también otros procedimientos de comunicación distintos de un procedimiento de desafío-respuesta para esta comunicación.

Lista de símbolos de referencia

10	Cofre de dinero
12	Unidad de inutilización
14	Unidad de control
16	Microcontrolador
18, 20	Elemento de memoria
22, 34	Conector de enchufe
30	Dispositivo
32	Unidad de emisión y recepción
36	Unidad de control
38, 40	Subunidad de control
42	Enlace de transmisión de datos USB
44	Bus CAN
50, 52	Banco
54	Cajero automático
56, 58, 64, 68	Grupos de aparatos
60	Empresa comercial
62	Caja fuerte automática
66	Empresa de transporte de valores
70	Vehículo de transporte de documentos de valor

72	Bastidor
S10 a S22	Paso de procedimiento
A, B, C, D, P	Clave

REIVINDICACIONES

1. Procedimiento de operación de un cofre de dinero, en el que se almacenan en fábrica durante la fabricación del cofre de dinero (10) en un elemento de memoria (18) de una unidad de control (14) del cofre de dinero (10) los datos de un programa de arranque de producción para poner en funcionamiento el cofre de dinero (10) y una clave de producción (P) para cifrar datos emitidos por el cofre de dinero (10) y/o para descifrar datos recibidos,

en el que se instala el cofre de dinero (10) para su puesta en servicio en un dispositivo destinado a recibir cofres de dinero y se establece un enlace de transmisión de datos entre el dispositivo y el cofre de dinero (10), y

en el que se sustituyen los datos del programa de arranque de producción por datos de un programa de arranque de servicio para poner en funcionamiento el cofre de dinero (10) y se sustituye la clave de producción (P) por una clave de operación (A) específica del cliente para cifrar datos emitidos por el cofre de dinero (10) y/o para descifrar datos recibidos.

2. Procedimiento según la reivindicación 1, **caracterizado** por que el programa de arranque de producción es sustituido por un programa de arranque de operación específico del cliente.

3. Procedimiento según la reivindicación 1, **caracterizado** por que el programa de arranque de producción se sustituye primeramente por un programa de arranque de operación estándar, por que seguidamente se transmiten datos con informaciones sobre la clave de operación (A) específica del cliente mediante el enlace de transmisión de datos desde el dispositivo hasta el cofre de dinero (10), y por que se sustituye entonces la clave de producción (P) por la clave de operación (A) específica del cliente.

4. Procedimiento según la reivindicación 3, **caracterizado** por que el dispositivo cifra los datos con las informaciones sobre la clave de operación (A) específica del cliente con ayuda de la clave de producción (P), y por que la unidad de control (14) del cofre de dinero (10) descifra estos datos con ayuda de la clave de producción (P).

5. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado** por que los datos del programa de arranque de operación y/o la clave de operación (A) específica del cliente se cifran primero por el dispositivo con ayuda de la clave de producción (P), se transmiten seguidamente cifrados al cofre de dinero (10) mediante el enlace de transmisión de datos y a continuación se descifran por la unidad de control (14) del cofre de dinero (10) con ayuda de la clave de producción (P).

6. Procedimiento según la reivindicación 4 o 5, **caracterizado** por que se cifran los datos con ayuda de un algoritmo de cifrado por bloques.

7. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado** por que se almacena la clave de operación (A) específica del cliente en un elemento de memoria de al menos un dispositivo (30, 54, 62, 72) de manejo de documentos de valor en el que debe instalarse el cofre de dinero (10) durante la operación, y por que los datos transmitidos entre este dispositivo (30, 54, 62, 72) y el cofre de dinero (10) instalado en el dispositivo (30, 54, 62, 72) se transmiten cifrados con ayuda de la clave de operación (A) específica del cliente.

8. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado** por que se almacenan en el elemento de memoria (18) varias claves de operación (A, B, C, D) específicas del cliente, por que se almacena cada vez en elementos de memoria de varios dispositivos (30, 54, 62, 72) de manejo de documentos de valor al menos una de estas claves de operación (A, B, C, D), y por que los respectivos datos transmitidos entre uno de estos dispositivos (30, 54, 62, 72) y el cofre de dinero (10) instalado en este dispositivo (30, 54, 62, 72) se transmiten cifrados con ayuda de la clave de operación correspondiente (A, B, C, D) específica del cliente.

9. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado** por que se transmiten los datos entre el cofre de dinero (10) y el dispositivo (30, 54, 62, 72) de manejo de documentos de valor por medio de un procedimiento de desafío-respuesta.

10. Procedimiento según la reivindicación 9, **caracterizado** por que en el procedimiento de desafío-respuesta se transmiten en un primer paso unos datos con informaciones para solicitar un número aleatorio desde el dispositivo (30, 54, 62, 72) de manejo de documentos de valor hasta el cofre de dinero (10), por que en un segundo paso el cofre de dinero (10) genera un número aleatorio con ayuda de un algoritmo de generación de números aleatorios archivado en la unidad de control (14) y lo transmite cifrado al dispositivo (30, 54, 62, 72), por que en un tercer paso el dispositivo (30, 54, 62, 72) descifra el número aleatorio cifrado y genera datos con al menos una orden de control, comprendiendo estos datos el número aleatorio, por que en un cuarto paso el dispositivo (30, 54, 62, 72) cifra estos datos con la clave de operación (A) específica del cliente y los transmite al cofre de dinero (10), por que en un quinto paso el cofre de dinero (10) descifra estos datos transmitidos a él con ayuda de la clave de operación (A) específica del cliente y compara el número aleatorio contenido en ellos con el número aleatorio generado y transmitido en el segundo paso, y por que el cofre de dinero (10) ejecuta la orden transmitida por el dispositivo (30, 54, 62, 72)

únicamente cuando la comparación arroja el resultado de que coinciden los números aleatorios.

11. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado** por que la clave de operación (A) específica del cliente puede variarse solamente con ayuda de la clave de operación actual (A) específica del cliente.

12. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado** por que el elemento de memoria (18) del cofre de dinero (10) comprende una memoria no volátil, especialmente una memoria flash, en la que están almacenados los datos del programa de arranque de producción, los datos del programa de arranque de operación, la clave de producción (P) y/o la clave de operación (A, B, C, D).

13. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado** por que en el elemento de memoria (18) del cofre de dinero (10) está almacenado un firmware de operación del cofre de dinero (10), y por que la clave de operación (A) específica del cliente se almacena como parte de este firmware.

14. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado** por que en el elemento de memoria (18) del cofre de dinero (10) está almacenado un firmware de operación del cofre de dinero (10), por que el firmware comprende una firma y por que la unidad de control (14) del cofre de dinero (10) determina la admisibilidad del firmware en función de la firma.

15. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado** por que en el elemento de memoria (18) del cofre de dinero (10) está almacenado un firmware de operación del cofre de dinero (10) y por que el firmware puede ser variado únicamente con ayuda de la clave de operación actual (A) específica del cliente.

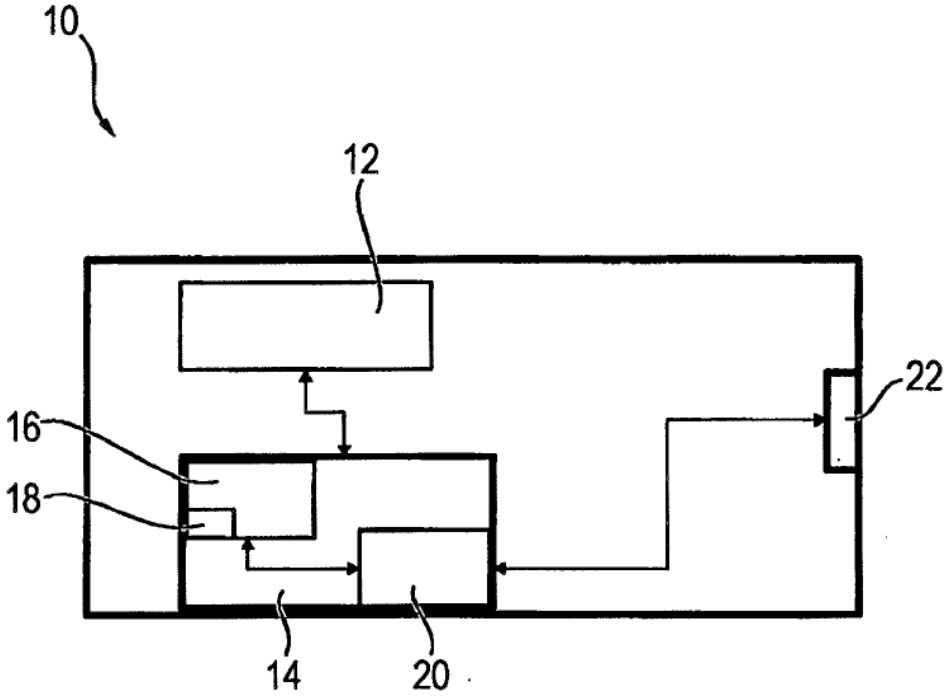

FIG. 1

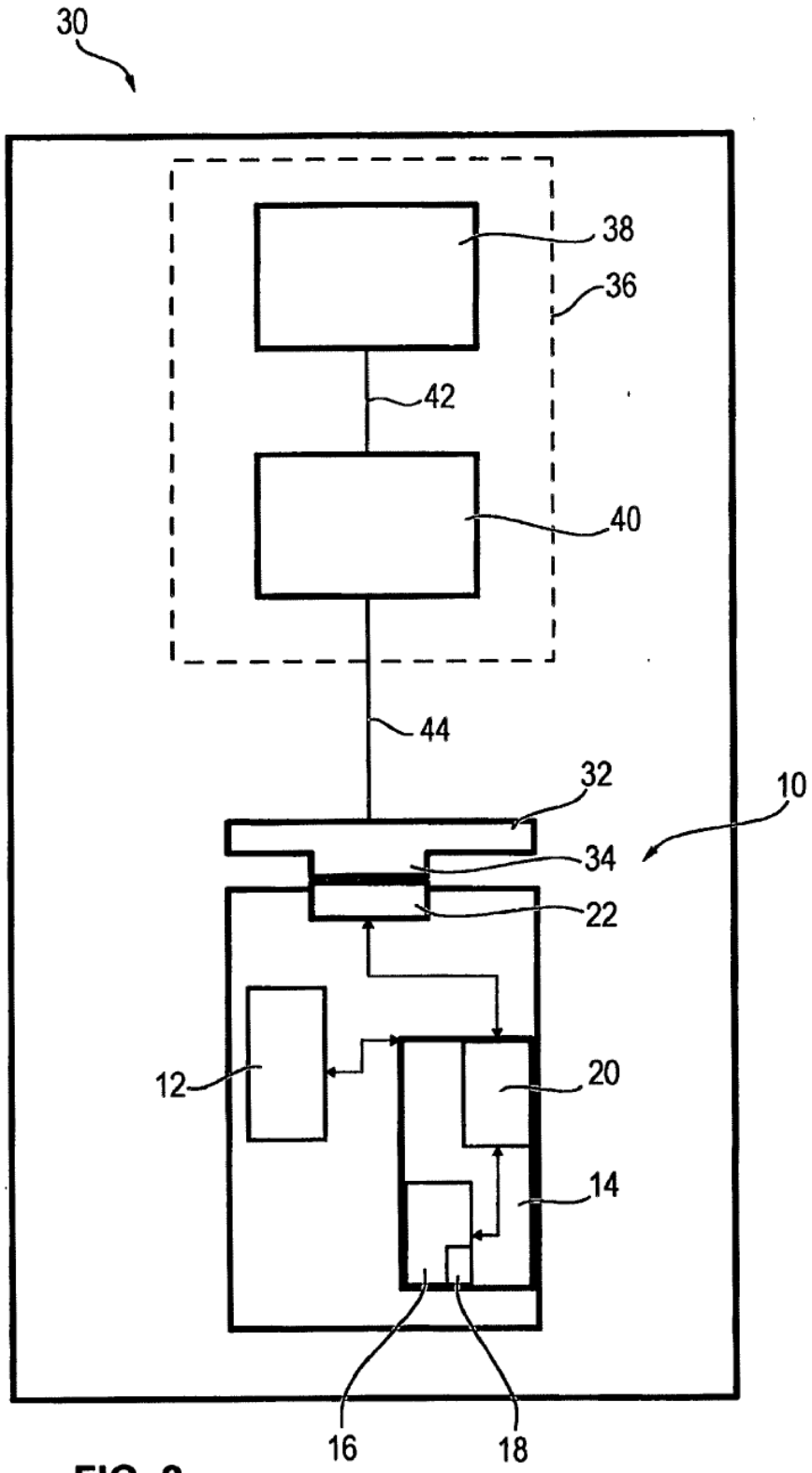

FIG. 2

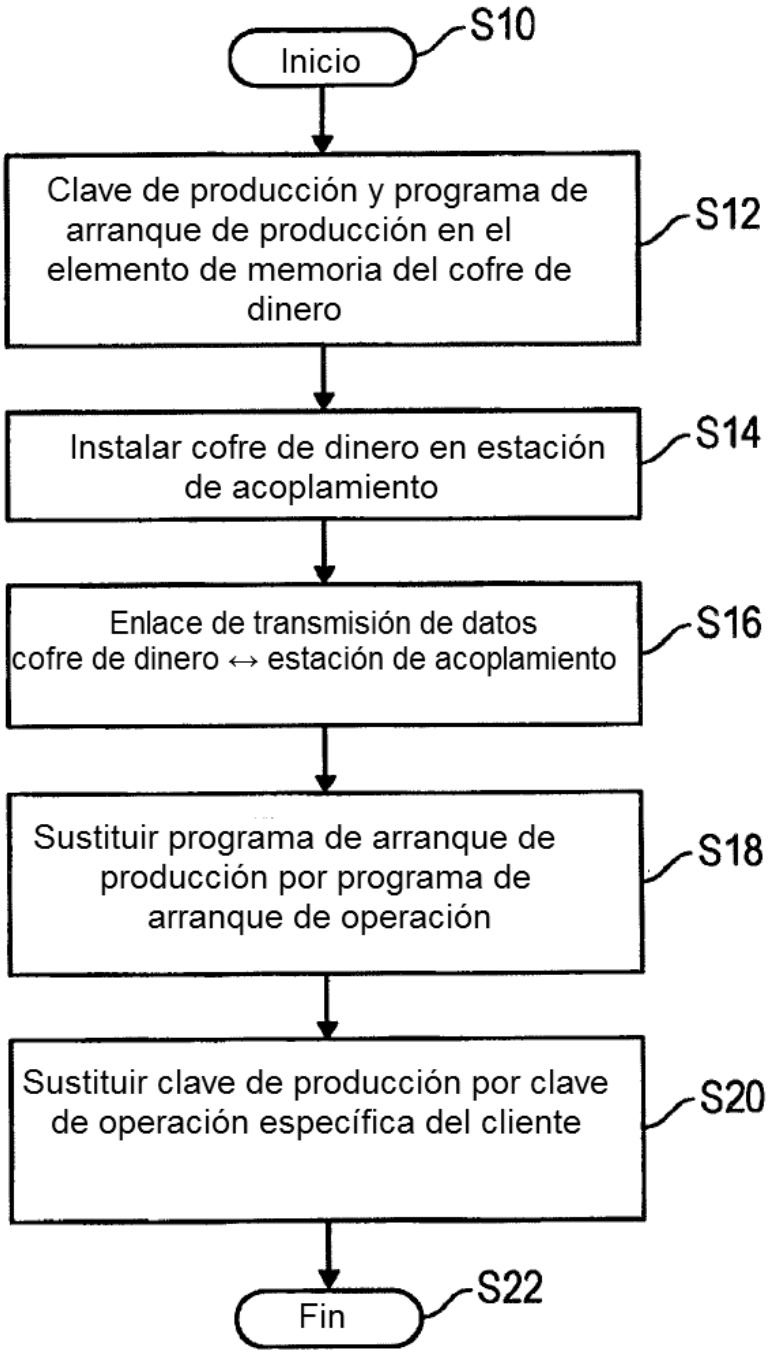
S10
Inicio
Clave de producción y programa de arranque de producción en el elemento de memoria del cofre de dinero
S12
Instalar cofre de dinero en estación de acoplamiento
S14
Enlace de transmisión de datos cofre de dinero ↔ estación de acoplamiento
S16
Sustituir programa de arranque de producción por programa de arranque de operación
S18
Sustituir clave de producción por clave de operación específica del cliente
S20
Fin
S22

FIG. 3

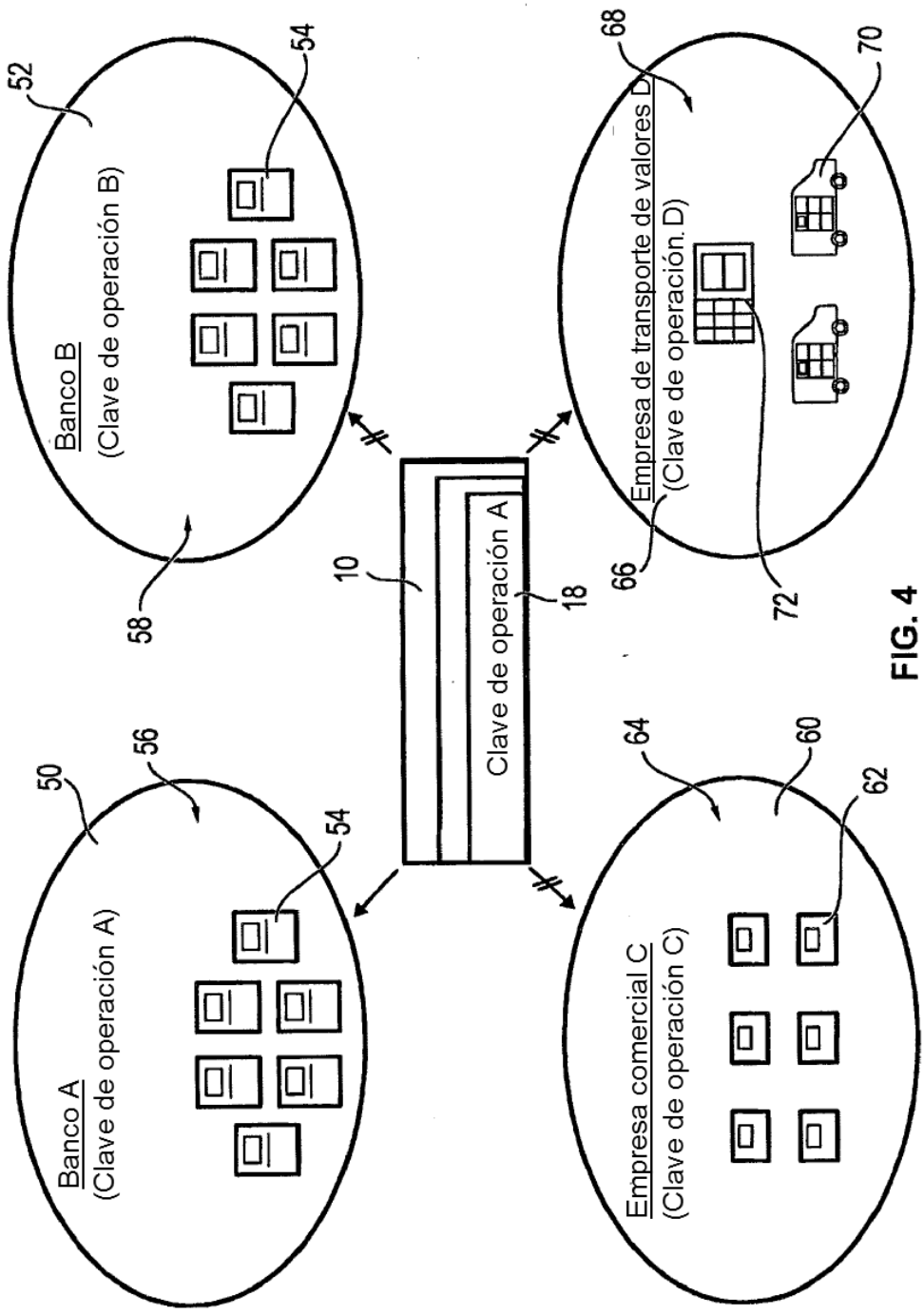
Banco B
(Clave de operación B)
Empresa de transporte de valores D
(Clave de operación D)
Clave de operación A
Banco A
(Clave de operación A)
Empresa comercial C
(Clave de operación C)
10
18
50
52
54
56
58
60
62
64
66
68
70
72

FIG. 4

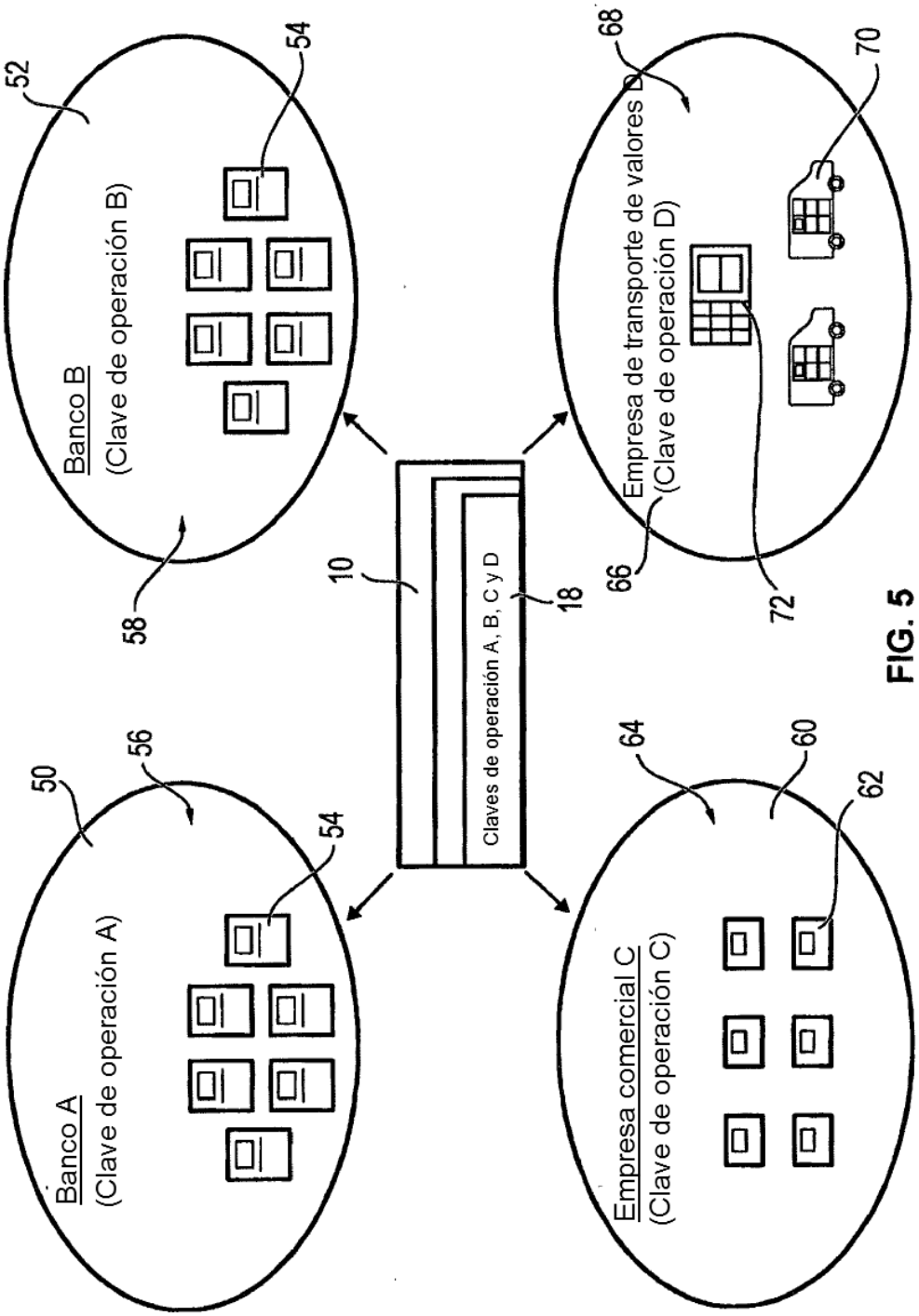
Banco A
(Clave de operación A)
Banco B
(Clave de operación B)
Empresa comercial C
(Clave de operación C)
Empresa de transporte de valores D
(Clave de operación D)
Claves de operación A, B, C y D
10
18
50
52
54
56
58
60
62
64
66
68
70
72

FIG. 5

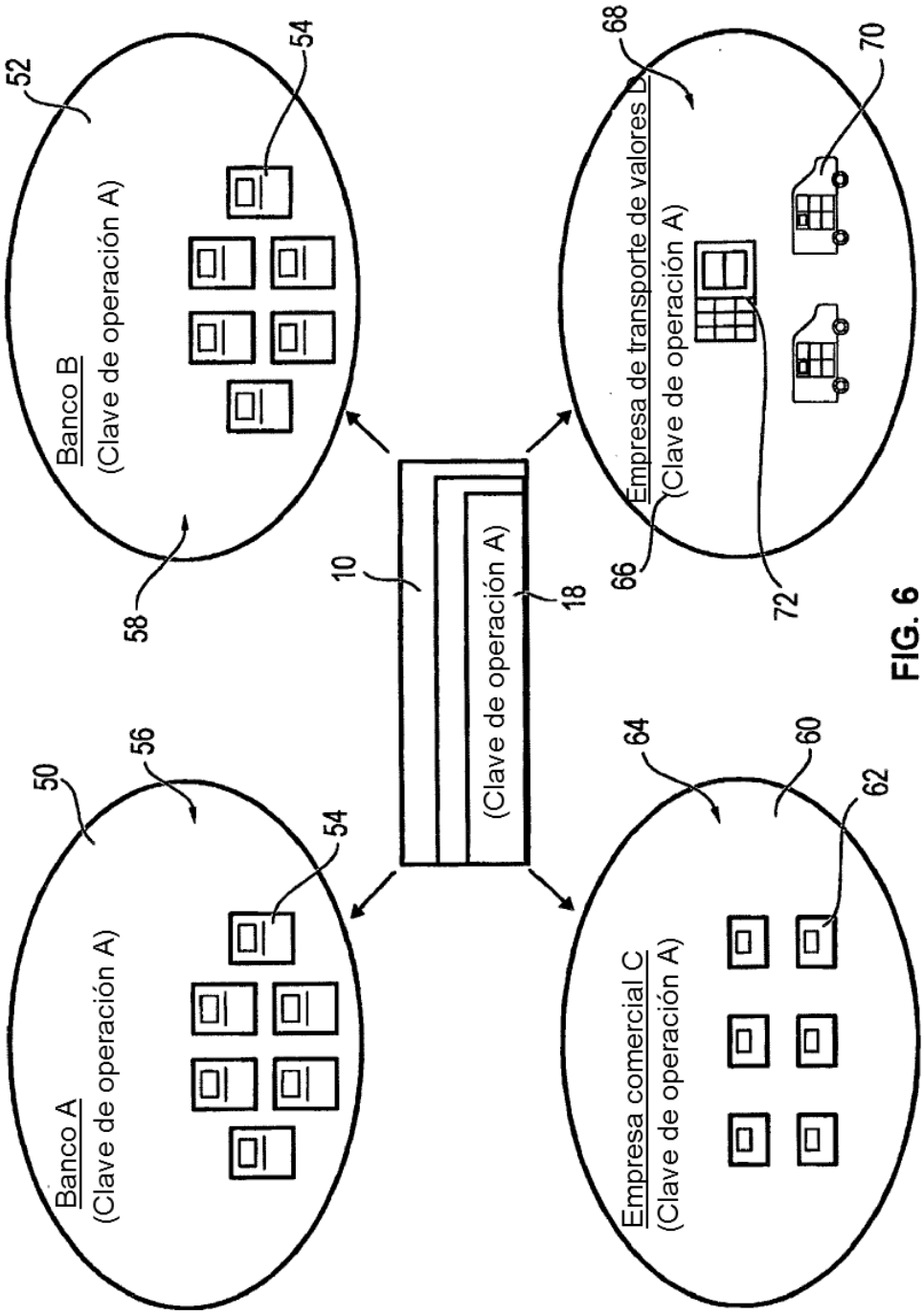
Banco B
(Clave de operación A)
Empresa de transporte de valores D
(Clave de operación A)
(Clave de operación A)
Banco A
(Clave de operación A)
Empresa comercial C
(Clave de operación A)
10
18
50
52
54
56
58
60
62
64
66
68
70
72

FIG. 6

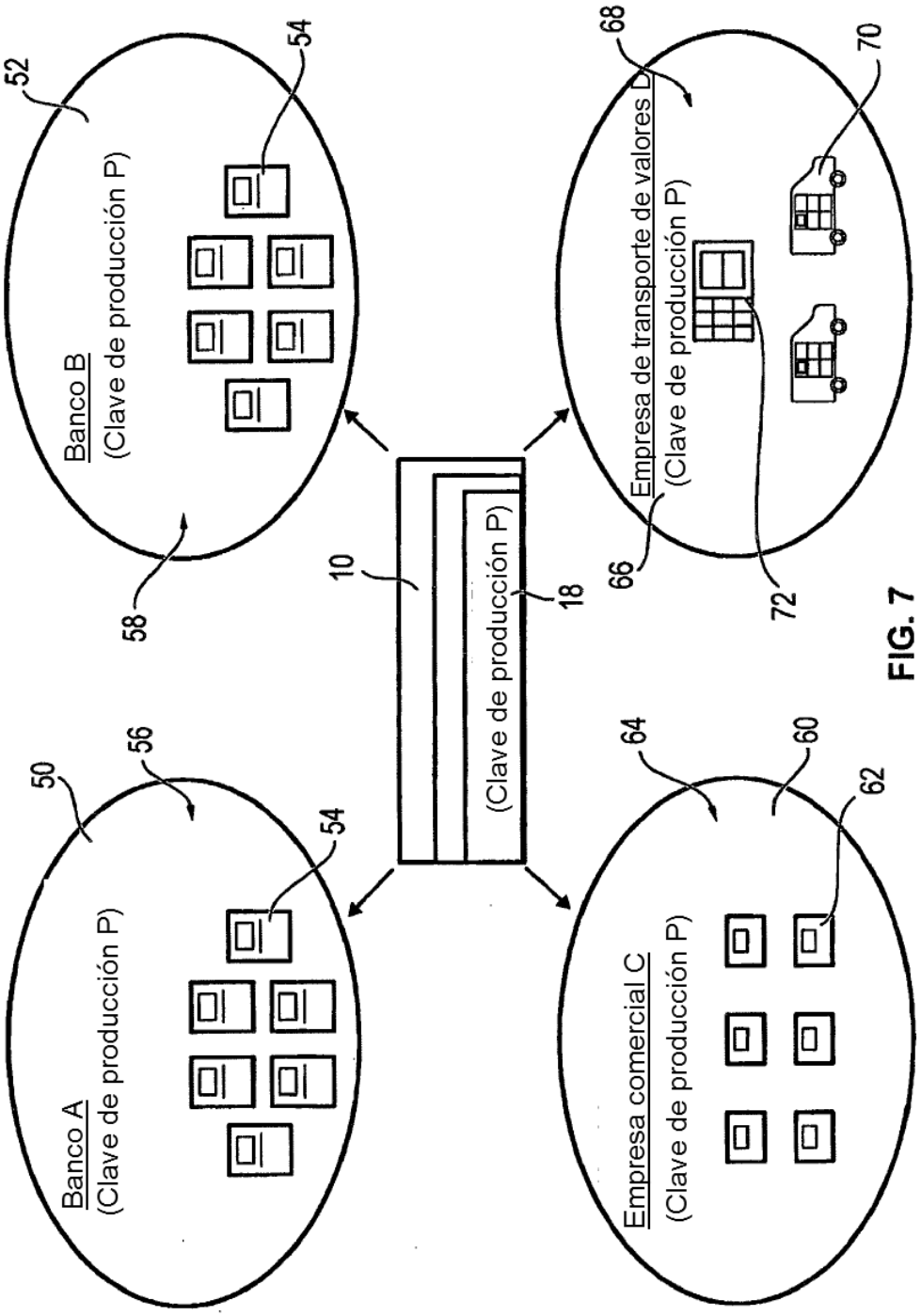
Banco B
(Clave de producción P)
Empresa de transporte de valores D
(Clave de producción P)
(Clave de producción P)
Banco A
(Clave de producción P)
Empresa comercial C
(Clave de producción P)
10
18
50
52
54
56
58
60
62
64
66
68
70
72

FIG. 7