(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 367 435**

(51) Int. Cl.:
G07C 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **04778354 .3**
(96) Fecha de presentación : **16.07.2004**
(97) Número de publicación de la solicitud: **1646937**
(97) Fecha de publicación de la solicitud: **19.04.2006**

(54) Título: **Control de acceso a una zona.**

(30) Prioridad: **18.07.2003 US 488645 P**
24.09.2003 US 505640 P

(45) Fecha de publicación de la mención BOPI:
03.11.2011

(45) Fecha de la publicación del folleto de la patente:
03.11.2011

(73) Titular/es: **CORESTREET, Ltd.**
One Alewife Center, Suite 200
Cambridge, Massachusetts 02140, US

(72) Inventor/es: **Libin, Phil;**
Micali, Silvio y
Engberg, David

(74) Agente: **Lehmann Novo, María Isabel**

DESCRIPCIÓN

Control de acceso a una zona

ANTECEDENTES DE LA INVENCIÓN

CAMPO TÉCNICO

Esta solicitud de patente se refiere al campo del control de acceso físico y más en particular, al campo del control de acceso físico utilizando cerraduras accionadas por procesador y datos relacionados.

DESCRIPCIÓN DE LA TÉCNICA RELACIONADA

Asegurar que solamente personas autorizadas puedan acceder a zonas protegidas y dispositivos bajo protección puede ser importante en muchos casos, tales como en el caso de acceso a un aeropuerto, instalación militar, edificio de oficinas, etc. Las puertas y paredes tradicionales se pueden utilizar para protección de zonas sensibles, pero las puertas con cerraduras y llaves tradicionales pueden ocupar un espacio excesivo a gestionar en una instalación con numerosos usuarios. Por ejemplo, una vez que se despida un empleado, puede ser difícil recuperar las llaves físicas que había emitido el empleado anterior mientras estuvo contratado. Además, puede ser peligroso que se hicieran copias de dichas llaves y nunca se entregaran en devolución.

Las puertas inteligentes proporcionan control del acceso. En algunos casos, una puerta inteligente puede estar provista de un teclado mediante el cual un usuario introduce su número PIN o una contraseña. El teclado puede tener una memoria conectada y/o un procesador elemental en el que se puede almacenar una lista de números PIN/contraseñas válidas. De este modo, una puerta puede comprobar si el número PIN, actualmente introducido pertenece, o no, a la lista válida en ese momento. Si es así, la puerta podrá abrirse. En caso contrario, la puerta puede permanecer bloqueada. Por supuesto, en lugar de confiar (exclusivamente) en las llaves tradicionales o en teclados simples, una puerta inteligente más moderna puede funcionar con tarjetas (tal como tarjetas inteligentes y tarjetas de banda magnética) o dispositivos sin contactos (p.e., PDAs, teléfonos móviles, etc.). Dichas tarjetas o dispositivos se pueden utilizar además de, o en lugar de, las llaves tradicionales o teclados electrónicos. Dichas tarjetas de banda magnética, tarjetas inteligentes o dispositivos sin contactos, diseñados para transportarse por usuarios, pueden tener la capacidad de almacenar información que se transmita a las puertas. Tarjetas más avanzadas pueden tener también la capacidad de cálculo y de comunicación. Los dispositivos correspondientes en las puertas pueden ser capaces de leer información desde las tarjetas y quizás, establecer protocolos interactivos con las tarjetas, comunicarse con ordenadores, etc.

Un aspecto de una puerta es su nivel de conectividad. Una puerta completamente conectada es una puerta que está, en todo momento, conectada con alguna base de datos (u otro sistema informático). Por ejemplo, la base de datos puede contener información sobre las tarjetas actualmente válidas, usuarios, números PINs, etc. En algunos casos, para impedir que un intruso modifique la información que fluye a la puerta, dicha conexión está asegurada (p.e., mediante la instalación del hilo de conexión, desde la puerta a la base de datos, dentro de un tubo de acero). Por otro lado, una puerta completamente desconectada no se comunica con el exterior de su proximidad inmediata. Entre estos dos extremos, pueden existir puertas que tengan una conectividad intermitente (p.e., una puerta “móvil” conectada de forma inalámbrica, que puede comunicarse con el exterior solamente cuando esté dentro del alcance de una estación terrestre, tal como la puerta de una aeronave o de un vehículo de transporte terrestre).

Los mecanismos tradicionales de control del acceso presentan numerosos inconvenientes. Las puertas completamente conectadas pueden ser de muy alto coste. El coste de instalación de una tubería segura, a una puerta inteligente distante, puede exceder, en gran medida, el coste de la propia puerta inteligente. La protección criptográfica de un hilo de conexión posiblemente sea más barata, pero sigue presentando sus propios costes (p.e., los de protección y gestión de claves criptográficas). Además, la criptografía sin conductos de acero y guardas de seguridad no puede impedir el corte de un hilo de conexión, en cuyo caso la puerta ya no conectada se podrá forzar para elegir entre dos alternativas extremas: a saber, permanecer siempre cerrada o siempre abierta, ninguna de las cuales son condiciones deseables. En cualquier caso, la conexión completa de una puerta no suele ser una opción viable. (Por ejemplo, la puerta de un contenedor de carga, por debajo del nivel del mar, en medio del océano Atlántico es, para todos los fines prácticos, una puerta completamente desconectada).

Las puertas inteligentes desconectadas pueden ser más baratas que las puertas conectadas. Sin embargo, los métodos tradicionales para las puertas inteligentes tienen su propio problema. Considérese, por ejemplo, una puerta inteligente desconectada capaz de reconocer un número PIN. Un empleado despedido ya no puede estar autorizado para atravesar dicha puerta, pero si todavía recuerda su propio PIN, puede no tener dificultad para abrir dicha puerta inteligente elemental. Por lo tanto, sería necesario “desprogramar” los números PINs de empleados despedidos, lo que es difícil para puertas desconectadas. En realidad, dicho procedimiento puede ser muy ocupador de espacio y costoso: una instalación de aeropuerto puede tener centenares de puertas y el traslado de un equipo especial de empleados para desprogramar la totalidad de dichas puertas, siempre que un empleado abandone, o sea despedido, puede ser también inviable.

El problema de la invención es aumentar un nivel de seguridad sin incurrir en sus costes adicionales.

Este problema se resuelve por el método según la reivindicación 1.

El control del acceso puede incluir proporcionar una barrera al acceso, que incluya un controlador que permita un acceso selectivo, al menos una entidad de administración que genere credenciales/pruebas de identidad en donde ninguna prueba válida sea determinable con la única presentación de las credenciales y valores para pruebas caducadas, recibiendo el controlador las credenciales/pruebas de identidad, determinando el controlador si el acceso está actualmente autorizado o no y, si el acceso está actualmente autorizado, el controlador permitirá el acceso. Las credenciales/pruebas de identidad pueden constituir una sola parte o pueden estar en partes separadas. Puede existir una primera entidad de administración que genere las credenciales y otras entidades de administración que generen pruebas de identidad. La primera entidad de administración puede generar también pruebas de identidad o la primera entidad de administración puede no generar pruebas. Las credenciales pueden corresponder a un certificado digital que incluye un valor final que es un resultado de aplicar una función unidireccional a una primera de las pruebas. Cada una de las pruebas puede ser un resultado de aplicar una función unidireccional a una futura de las pruebas. El certificado digital puede incluir un identificador para el dispositivo electrónico. Las credenciales pueden incluir un valor final que es un resultado de aplicar una función unidireccional a una primera de las pruebas. Cada una de las pruebas puede ser un resultado de aplicar una función unidireccional a una futura de las pruebas. Las credenciales pueden incluir un identificador para un usuario que solicita acceso. Las credenciales/pruebas de identidad pueden incluir una firma digital. La barrera para acceder puede incluir paredes y una puerta. El control del acceso puede incluir también proporcionar una cerradura de puerta acoplada al controlador, en donde el controlador que permite el acceso incluye el controlador que acciona la cerradura de la puerta para permitir la apertura de dicha puerta. El control del acceso puede incluir también proporcionar un lector acoplado al controlador, en donde el controlador recibe credenciales/pruebas de identidad desde el lector. Las credenciales/pruebas de identidad se pueden proporcionar en una tarjeta inteligente presentada por un usuario. El control del acceso puede incluir, además, proporcionar una conexión externa al controlador. La conexión externa puede ser intermitente. El controlador puede recibir al menos una parte de las credenciales/pruebas de identidad utilizando la conexión externa o el controlador puede recibir la totalidad de las credenciales/pruebas de identidad utilizando la conexión externa. El control del acceso puede incluir, además, proporcionar un lector acoplado al controlador, en donde el controlador recibe una parte restante de las credenciales/pruebas de identidad desde el lector. Las credenciales/pruebas de identidad pueden incluir una contraseña introducida por un usuario. Las credenciales/pruebas de identidad pueden incluir una información biométrica del usuario. Las credenciales/pruebas de identidad pueden incluir una firma manuscrita. Las credenciales/pruebas pueden incluir un valor secreto proporcionado en una tarjeta mantenida por un usuario. Las credenciales/pruebas de identidad pueden caducar en un momento predeterminado.

Además, una entidad que controla el acceso de una pluralidad de usuarios a por lo menos una puerta desconectada puede comprender la puesta en correspondencia de la pluralidad de usuarios con un grupo, para cada intervalo de tiempo *d* de una secuencia de fechas, que tiene una autorización para presentar una firma digital SIGUDd, que indica que los miembros del agrupo pueden acceder a la puerta durante el intervalo de tiempo *d*, lo que hace que al menos uno de los miembros del grupo reciba SIGUDd durante el intervalo de tiempo d para presentación a la puerta con el fin de pasar a través de ella, teniendo el al menos un miembro del grupo que presentar el SIGUDd a la puerta D y haciendo que se habrá la puerta después de verificar que: (i) SIGUDd es una firma digital de la autoridad que indica que los miembros del grupo pueden acceder a la puerta en el intervalo de tiempo d y (ii) que el tiempo actual está dentro del intervalo de tiempo d. El al menos un miembro del grupo puede tener una tarjeta de usuario y la puerta puede tener un lector de tarjetas acoplado para una cerradura electromecánica y el al menos un miembro del grupo puede recibir el SIGUDd memorizándolo en la tarjeta de usuario y puede presentar el SIGUDd a la puerta al ser la tarjeta del usuario leída por el lector de tarjetas. La autoridad puede hacer que SIGUDd sea recibida por el al menos un miembro del grupo durante el intervalo de tiempo d registrando SIGUDd en una base de datos accesible por el al menos un miembro del grupo. SIGUDd puede ser una firma de clave pública y la puerta puede almacenar la clave pública de la autoridad. La puerta puede comprobar, además, la información de identidad sobre el al menos un miembro del grupo. La información de identidad sobre el al menos un miembro del grupo puede incluir, como mínimo, uno de entre: un número PIN y la respuesta a un denominado desafío operativo de la puerta.

Además, el control del acceso físico puede comprender también la asignación de credenciales en tiempo real a un grupo de usuarios, la revisión de las credenciales en tiempo real, en donde las credenciales en tiempo real comprenden una primera parte que es fija y una segunda parte que se modifica sobre una base periódica, en donde la segunda parte proporciona una prueba de que las credenciales en tiempo real están en curso, comprobando la validez de las credenciales en tiempo real realizando una operación en la primera parte y comparando el resultado con la segunda parte y permitiendo el acceso físico a los miembros del grupo solamente si las credenciales en tiempo real están verificadas como válidas. La primera parte puede ser digitalmente firmada por una autoridad. La autoridad puede proporcionar la segunda parte. La segunda parte puede ser provista por una entidad distinta a la autoridad. Las credenciales en tiempo real se pueden proporcionar en una tarjeta inteligente. Los miembros del grupo pueden obtener la segunda parte de las credenciales en tiempo real en una primera localización. A los miembros del grupo les puede estar permitido el acceso a una segunda localización diferente y separada de la primera. Al menos una porción de la primera parte de las credenciales en tiempo real puede representar una función-resumen de identificación, denominada *hash*, unidireccional aplicada, varias veces, a una porción de la segunda parte de las credenciales en tiempo real. La pluralidad

de veces puede corresponder a una cantidad de tiempo transcurrido desde que se emitieron la primera parte de las credenciales en tiempo real. El control del acceso físico puede comprender, además, el control del acceso a través de una puerta.

Además, la determinación del acceso puede comprender la determinación de si credenciales/pruebas de identidad particulares indican que está permitido el acceso, la determinación de si existen datos adicionales asociados con las credenciales/pruebas de identidad, en donde los datos adicionales están separados de las credenciales/pruebas de identidad y, si las credenciales/pruebas de identidad particulares indican que el acceso está permitido y si hay datos adicionales asociados con las credenciales/pruebas de identidad particulares, entonces decidir si denegar, o no el acceso en función de la información proporcionada por los datos adicionales. Las credenciales/pruebas pueden estar en una sola parte o en partes separadas. Puede existir una primera entidad de administración que genera las credenciales y otras entidades de administración que generan pruebas. La primera entidad de administración puede generar también pruebas o puede no generar pruebas. Las credenciales pueden corresponder a un certificado digital que incluye un valor final, que es un resultado de aplicar una función unidireccional a una primera de las pruebas. Cada una de las pruebas puede ser un resultado de aplicar una función unidireccional a una futura de entre las pruebas. El certificado digital puede comprender un identificador para el dispositivo electrónico. Las credenciales pueden incluir un valor final que es un resultado de aplicar una función unidireccional a una primera de las pruebas. Cada una de las pruebas puede ser un resultado de aplicar una función unidireccional a una futura de las pruebas. Las credenciales pueden comprender un identificador para un usuario que solicita el acceso. Las credenciales/pruebas pueden incluir una firma digital.

El acceso puede ser el acceso a una zona cerrada por paredes y un puertas. La determinación del acceso puede incluir proporcionar una cerradura de puerta, en donde la cerradura se acciona en función de que el acceso sea denegado o no lo sea. La determinación del acceso puede comprender, además, proporcionar un lector que reciba las credencialess/pruebas de identidad. Dichas credenciales/pruebas se pueden proporcionar en una tarjeta inteligente presentada por un usuario. Las credenciales/pruebas pueden incluir una contraseña introducida por un usuario. Las credenciales/pruebas pueden comprender, asimismo, una información biométrica del usuario así como una firma manuscrita. Las credenciales/pruebas pueden incluir un valor secreto proporcionado en una tarjeta mantenida por un usuario. Las credenciales/pruebas pueden caducar en un momento predeterminado. Los datos adicionales pueden tener una firma digital y pueden ser un mensaje que esté vinculado a las credenciales/pruebas. El mensaje puede identificar las credenciales/pruebas particulares en incluir una indicación de si dichas credenciales/pruebas particulares han sido revocadas o no. La indicación puede ser una cadena vacía. Los datos adicionales pueden incluir una fecha. Asimismo, los datos adicionales pueden ser un mensaje que contenga información sobre las credenciales/pruebas particulares y que contenga información sobre una o más de entre otras credenciales/pruebas. La determinación del acceso puede comprender, además, el almacenamiento de los datos adicionales. Los datos adicionales pueden incluir un tiempo de caducidad que indique el periodo de tiempo en que han de guardarse los datos adicionales. El tiempo de caducidad puede corresponder a una caducidad de las credenciales/pruebas particulares. La determinación del acceso puede incluir también el almacenamiento de los datos adicionales durante un periodo de tiempo predeterminado. Las credenciales/pruebas pueden caducar todas ellas transcurrido un tiempo predeterminado. Los datos adicionales pueden proveerse utilizando una tarjeta inteligente. La tarjeta inteligente puede presentarse por un usuario que intente tener acceso a una zona. El acceso a la zona puede ser restringido utilizando paredes y al menos una puerta. Los datos adicionales pueden ser para un usuario diferente del usuario que intenta obtener acceso. La determinación del acceso puede comprender, además, proporcionar un enlace de comunicación y transmitir los datos adicionales utilizando dicho enlace de comunicación. El enlace de comunicación puede estar provisto de los datos adicionales mediante una tarjeta inteligente. La tarjeta inteligente puede exigir una comunicación periódica con el enlace de comunicaciones con el fin de permanecer operativa. La tarjeta inteligente puede ser provista de los datos adicionales a través de otra tarjeta inteligente. Los datos adicionales se pueden proporcionar, de forma selectiva, a un subconjunto de tarjetas inteligentes. La determinación del acceso puede incluir, además, proporcionar un nivel de prioridad a los datos adicionales. Los datos adicionales pueden proporcionarse, de forma selectiva, a un subconjunto de tarjetas inteligentes en función del nivel de prioridad proporcionado a los datos adicionales. Los datos adicionales se pueden proporcionar, de forma aleatoria, a un subconjunto de tarjetas inteligentes.

Además, la emisión y difusión de unos datos sobre una credencial pueden comprender la disposición de una entidad que emite datos autenticados que indican que la credencial ha sido cancelada, lo que hace que dichos datos autenticados sean memorizados en una primera tarjeta de un primer usuario, utilizando la primera tarjeta para transmitir los datos autenticados a una primera puerta, teniendo dicha primera puerta que almacenar información sobre los datos autenticados, y dependiendo dicha primera puerta de la información sobre los datos autenticados para denegar el acceso a la credencial. Los datos autenticados pueden ser objeto de autenticación mediante una firma digital y la primera puerta puede verificar dicha firma digital. La firma digital puede ser una firma digital de clave pública. La clave pública para la firma digital puede estar asociada con la credencial. La firma digital puede ser una firma digital de clave privada. La credencial y la primera tarjeta pueden pertenecer ambas al primer usuario. La credencial puede memorizarse en una segunda tarjeta diferente de la primera tarjeta y la primera puerta puede basarse en información sobre los datos autenticados recuperando dicha información del medio de almacenamiento. La credencial puede pertenecer a un segundo usuario diferente del primer usuario. Los datos autenticados pueden ser almacenados primero en al menos otra tarjeta diferente de la primera tarjeta y los datos autenticados se pueden transmitir desde la al menos otra tarjeta a la primera tarjeta. Los datos autenticados pueden transmitirse desde la al menos otra tarjeta a la primera tarjeta transmitiendo primero a por lo menos una otra puerta diferente de la primera puerta. La entidad puede hacer que se

almacenen los datos autenticados en la primera tarjeta haciendo primero que los datos autenticados se almacenen en un respondedor y a continuación, hacer que la primera tarjeta obtenga los datos autenticados desde el respondedor. El respondedor puede estar desprotegido. La primera puerta puede recibir información sobre los datos autenticados desde la primera tarjeta por los datos autenticados que se transfieren primero a al menos otra tarjeta diferente de la primera tarjeta. La al menos otra tarjeta diferente puede recibir información sobre los datos autenticados desde la primera tarjeta mediante los datos autenticados que se transmiten primero a al menos una otra puerta diferente de la primera puerta. La primera puerta puede estar completamente desconectada o puede conectarse de forma intermitente.

Además, una primera puerta puede recibir datos autenticados sobre una credencial de un primer usuario, incluyendo el proceso la recepción de los datos autenticados desde una primera tarjeta perteneciente a un segundo usuario diferente del primer usuario, el almacenamiento de información sobre los datos autenticados, la recepción de la credencial y la dependencia de la información almacenada sobre los datos autenticados para denegar el acceso a la credencial. Los datos autenticados pueden ser objeto de autenticación mediante una firma digital y la primera puerta verifica la firma digital. La firma digital puede una firma digital de clave pública. La clave pública para la firma digital puede estar asociada con la credencial. La firma digital puede ser una firma digital de clave privada. Los datos autenticados se pueden memorizar en la primera tarjeta almacenándose primero en al menos una otra tarjeta y luego, transmitirse desde la al menos otra tarjeta a la primera tarjeta. Los datos autenticados se pueden transmitir desde la al menos una otra tarjeta a la primera tarjeta transmitiendo primero a al menos una puerta diferente de la primera puerta. Los datos autenticados se pueden memorizar en la primera tarjeta almacenándolos primero en un respondedor y a continuación, obteniéndose por la primera tarjeta desde el respondedor. El respondedor puede estar desprotegido. La primera puerta puede recibir información sobre los datos autenticados desde la primera tarjeta mediante los datos autenticados que se transmiten primero a al menos una otra tarjeta diferente de la primera tarjeta. La al menos una otra tarjeta puede recibir información sobre los datos autenticados desde la primera tarjeta mediante la transmisión primero de los datos autenticados a al menos una otra puerta diferente de la primera puerta. La primera puerta puede estar completamente desconectada o puede conectarse de forma intermitente.

Además, la asistencia en una revocación inmediata de acceso puede incluir la recepción de datos autenticados sobre una credencial, el almacenamiento de información sobre los datos autenticados en una primera tarjeta y hacer que una primera puerta reciba información sobre los datos autenticados. Los datos autenticados pueden ser objeto de autenticación mediante una firma digital. La firma digital puede ser una firma digital de clave pública. La clave pública para la firma digital puede estar asociada con la credencial. La firma digital puede ser una firma digital de clave privada. La credencial y la tarjeta pueden pertenecer ambas a un primer usuario. La primera tarjeta puede hacerse inutilizable para el acceso si la primera tarjeta deja de recibir un tipo pre-especificado de señal en una cantidad de tiempo pre-especificada. La credencial puede pertenecer a otro usuario diferente del primer usuario. Los datos autenticados se pueden recibir por la primera tarjeta memorizando primero, en al menos otra tarjeta diferente de la primera tarjeta, y luego transmitirse desde la al menos otra tarjeta a la primera tarjeta. Los datos autenticados se pueden transmitir desde la al menos una otra tarjeta a la primera tarjeta transmitiendo primero a al menos una otra puerta diferente de la primera puerta. La primera tarjeta puede obtener los datos autenticados desde un respondedor. El respondedor puede estar desprotegido. La primera tarjeta puede hacer que la primera puerta reciba información sobre los datos autenticados transmitiendo primero los datos autenticados a al menos una otra tarjeta diferente de la primera tarjeta. La primera tarjeta puede hacer que la al menos una otra tarjeta reciba información sobre los datos autenticados transmitiendo primero los datos autenticados a al menos una otra puerta diferente de la primera puerta. La primera puerta puede estar completamente desconectada o puede conectarse de forma intermitente. La primera tarjeta puede eliminar, ocasionalmente, la información almacenada sobre los datos autenticados desde el soporte de almacenamiento. La credencial puede tener una fecha de caducidad y la primera tarjeta puede eliminar la información almacenada sobre los datos autenticados desde el soporte de almacenamiento una vez que la credencial esté caducada. La fecha de caducidad de la credencial se puede deducir de la información especificada dentro de la credencial.

Además de la presente invención, el registro de eventos operativos asociados con el acceso a una zona puede incluir el registro de un evento operativo asociado con el acceso a la zona para proporcionar un registro de eventos y la autenticación de al menos el registro de eventos para proporcionar un registro autenticado. El registro de un evento operativo puede incluir el registro de un tiempo del evento. El registro de un evento operativo puede incluir el registro de un tipo de evento. El evento puede ser un intento de acceder a la zona. El registro de un evento puede incluir el registro de credenciales/pruebas utilizadas en relación con el intento de acceder a la zona. El registro de un evento puede incluir el registro de un resultado de la tentativa. El registro de un evento puede incluir el registro de la existencia de datos que no sean las credenciales/pruebas que indiquen que se debe denegar el acceso. El registro de un evento puede incluir el registro de datos adicionales relacionados con la zona. La autenticación del registro puede incluir la firma digital de dicho registro. La autenticación de al menos el registro de eventos puede incluir la autenticación del registro de eventos y la autenticación de otros registros de eventos para proporcionar un registro autenticado único. El registro autenticado único puede memorizarse en una tarjeta. El registro autenticado puede memorizarse en una tarjeta. La tarjeta puede tener almacenado otro registro autenticado. El otro registro autenticado puede proporcionarse por la tarjeta en relación con la tarjeta que se utiliza para acceder a la zona. El acceso puede ser denegado si el otro registro autenticado no se puede verificar. Un controlador se puede proporcionar en relación con el acceso a la zona y en donde el controlador realiza la autenticación, además, del otro registro autenticado. El otro registro autenticado puede ser objeto de autenticación utilizando un certificado digital. El registro de eventos operativos puede comprender, además, un usuario que presenta una tarjeta para intentar acceder a la zona. El registro de eventos puede comprender, además, la tarjeta que realiza la

autenticación, además, del registro autenticado en relación con el usuario que intenta acceder a la zona. Un controlador puede estar provisto en relación con el acceso a la zona y en donde el controlador y la tarjeta realizan una autenticación conjunta del registro autenticado. El registro de eventos operativos puede incluir proporcionar datos de generación de correlación que indican el contenido del registro autenticado. Los datos de generación de correlación pueden estar vinculados con el registro autenticado. Los datos de generación de correlación pueden estar vinculados al registro autenticado y el vínculo resultante puede ser también autenticado. El vínculo resultante puede tener una firma digital. Los datos de generación de correlación pueden ser una secuencia de números y en particular, uno de los números se puede asignar al evento operativo. El registro de eventos puede comprender, además, la autenticación de un vínculo del número particular y del evento. La autenticación del vínculo puede incluir la firma digital del vínculo. La autenticación puede comprender, además, una forma de la función *hashing* del vínculo y luego, la firma digital de su resultado. Los datos de generación de correlación para el evento pueden incluir información que identifique otro evento. El otro evento puede ser un evento anterior. El otro evento puede ser también un evento futuro. El registro de eventos puede comprender, además, la asociación de un primero y un segundo valor aleatorio para el evento, la asociación de al menos uno del primero y segundo valores aleatorios con el otro evento y el vínculo en al menos uno de los primero y segundo valores para el otro evento. El suministro de datos de generación de correlación puede incluir la utilización de un polinomio para generar la información de correlación. El suministro de datos de generación de correlación puede comprender, además, la utilización de una cadena de funciones *hash* para generar la información de correlación. Los datos de generación de correlación pueden incluir información sobre una pluralidad de otros eventos. Los datos de generación de correlación pueden incluir códigos de corrección de errores. El registro de eventos puede comprender, además, la difusión del registro autenticado. La difusión del registro autenticado puede incluir proporcionar el registro autenticado en tarjetas presentadas por usuarios que intenten acceder a la zona. La zona se puede definir por paredes y una puerta.

Además, al menos una entidad de administración puede controlar el acceso a un dispositivo electrónico por la al menos una entidad de administración que genera credenciales y una pluralidad de pruebas correspondientes para el dispositivo electrónico, en donde ninguna prueba válida es susceptible de determinarse solamente dando las credenciales y valores para pruebas caducadas, con la recepción por el dispositivo electrónico de las credenciales, si el acceso está autorizado en un momento particular, el dispositivo electrónico que recibe una prueba correspondiente a ese momento particular y el dispositivo electrónico que confirma la prueba utilizando las credenciales. La al menos una entidad de administración puede generar pruebas después de generar las credenciales. Una entidad de administración única puede generar las credenciales y generar las pruebas. Puede existir una primera entidad de administración que genere las credenciales y otras entidades de administración que generen pruebas. La primera entidad de administración puede generar también pruebas o puede no hacerlo. Las credenciales pueden ser un certificado digital que incluye un valor final, que es un resultado de aplicar una función unidireccional a una primera de las pruebas. Cada una de las pruebas puede ser un resultado de aplicar una función unidireccional a una futura de las pruebas. El certificado digital puede incluir un identificador para el dispositivo electrónico. Las credenciales pueden incluir un valor final, que es un resultado de aplicar una función unidireccional a una primera de las pruebas. Cada una de las pruebas puede ser un resultado de aplicar una función unidireccional a una futura de las pruebas. Las credenciales pueden incluir un identificador para el dispositivo electrónico. El dispositivo electrónico puede ser un ordenador, que puede inicializarse solamente si el acceso está autorizado. El dispositivo electrónico puede ser una unidad de disco. Al menos una entidad de administración, que controla el acceso a un dispositivo electrónico, puede incluir el suministro de pruebas utilizando al menos una entidad de distribución de pruebas separada de la al menos una entidad administrativa. Puede existir una entidad de distribución de pruebas única o una pluralidad de entidades de distribución de pruebas. Al menos una entidad de administración, que controla el acceso a un dispositivo electrónico, puede incluir el suministro de pruebas utilizando una conexión al dispositivo electrónico. La conexión puede ser a través de Internet. Al menos alguna de las pruebas pueden almacenarse, a nivel local, en el dispositivo electrónico. Al menos una entidad de administración, que controla el acceso a un dispositivo electrónico puede incluir, si la prueba correspondiente al momento en que no esté disponible a nivel local, el dispositivo electrónico solicita las pruebas a través de una conexión externa. Cada una de las pruebas puede estar asociada con un intervalo de tiempo particular. Después de transcurrir un intervalo de tiempo particular asociado con una particular de entre las pruebas con resultado satisfactorio, el dispositivo electrónico puede recibir una nueva prueba. Dicho intervalo de tiempo puede ser un día.

Además, un dispositivo electrónico puede controlar su acceso recibiendo credenciales y al menos una de entre una pluralidad de pruebas correspondientes para el dispositivo electrónico, en donde ninguna prueba válida es susceptible de determinación solamente proporcionando las credenciales y valores para pruebas caducadas y comprobando que al menos una de entre una pluralidad de pruebas está utilizando las credenciales. Las credenciales pueden ser un certificado digital que incluye un valor final que es un resultado de aplicar una función unidireccional a una primera de las pruebas. Cada una de las pruebas puede ser un resultado de aplicar una función unidireccional a una futura de las pruebas. El certificado digital puede incluir un identificador para el dispositivo electrónico. Las credenciales pueden incluir un valor final que es un resultado de aplicar una función unidireccional a una primera de las pruebas. Cada una de las pruebas puede ser un resultado de aplicar una función unidireccional a una futura de las pruebas. Las credenciales pueden incluir un identificador para el dispositivo electrónico. El dispositivo electrónico puede ser un ordenador. Un dispositivo electrónico que controla su acceso puede comprender, además, la inicialización del ordenador solamente si el acceso está autorizado. El dispositivo electrónico puede ser una unidad de disco. Un dispositivo electrónico que controla su acceso puede comprender, además, la obtención de pruebas utilizando una conexión al dispositivo electrónico. La conexión puede ser a través de Internet. Al menos algunas de las pruebas pueden memorizarse localmente en el

dispositivo electrónico. Un dispositivo electrónico que controla su acceso puede comprender, además, si la prueba correspondiente al momento no está disponible a nivel local, el dispositivo electrónico que solicita las pruebas a través de una conexión externa. Cada una de las pruebas puede estar asociada por un intervalo de tiempo particular. Después de transcurrir un intervalo de tiempo particular, asociado con una particular de las pruebas de resultado satisfactorio, el dispositivo electrónico puede recibir una nueva prueba. Dicho intervalo de tiempo puede ser un día.

Además, el control del acceso a un dispositivo electrónico puede incluir el suministro de credenciales al dispositivo electrónico y, si el acceso está permitido en un momento particular, proporcionar una prueba al dispositivo electrónico correspondiente a ese momento particular, en donde la prueba no es susceptible de determinación proporcionando solamente las credenciales y valores para pruebas caducadas. Las credenciales pueden ser un certificado digital que incluye un valor final que es un resultado de aplicar una función unidireccional a una primera de las pruebas. Cada una de las pruebas puede ser el resultado de aplicar una función unidireccional a una futura de las pruebas. El certificado digital puede incluir un identificador para el dispositivo electrónico. Las credenciales pueden incluir un valor final que es un resultado de aplicar una función unidireccional a una primera de las pruebas. Cada una de las pruebas puede ser un resultado de aplicar a una función unidireccional a una futura de las pruebas. Las credenciales puede incluir un identificador para el dispositivo electrónico. El dispositivo electrónico puede ser un ordenador. El control del acceso a un dispositivo electrónico puede incluir la inicialización del ordenador solamente si el acceso está autorizado. El dispositivo electrónico puede ser una unidad de disco. El control del acceso a un dispositivo electrónico puede incluir el suministro de pruebas utilizando al menos una entidad de distribución de pruebas separada de la al menos una entidad administrativa. Puede existir una entidad de distribución de pruebas única. Puede existir, asimismo, una pluralidad de entidades de distribución de pruebas. El control del acceso a un dispositivo electrónico puede incluir el suministro de pruebas utilizando una conexión a ese dispositivo electrónico. La conexión puede ser a través de Internet. Al menos algunas de las pruebas pueden memorizarse, a nivel local, en el dispositivo electrónico. El control del acceso a un dispositivo electrónico puede incluir, si la prueba correspondiente al momento no está disponible a nivel local, el dispositivo electrónico que solicite las pruebas a través de una conexión externa. Cada una de las pruebas puede estar asociada con un intervalo de tiempo particular. Después de transcurrir un intervalo de tiempo particular, asociado con una particular de las pruebas de resultado satisfactorio, el dispositivo electrónico puede recibir una nueva prueba. Dicho intervalo de tiempo puede ser un día.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Figura 1A es un diagrama que ilustra una forma de realización que incluye una conexión, una pluralidad de dispositivos electrónicos, una entidad de administración y una entidad de distribución de pruebas según el sistema aquí descrito.

La Figura 1B es un diagrama que ilustra una forma de realización alternativa que incluye una conexión, una pluralidad de dispositivos electrónicos, una entidad de administración y una entidad de distribución de pruebas según el sistema aquí descrito.

La Figura 1C es un diagrama que ilustra una forma de realización alternativa que incluye una conexión, una pluralidad de dispositivos electrónicos, una entidad de administración y una entidad de distribución de pruebas según el sistema aquí descrito.

La Figura 1D es un diagrama que ilustra una forma de realización alternativa que incluye una conexión, una pluralidad de dispositivos electrónicos, una entidad de administración y una entidad de distribución de pruebas según el sistema aquí descrito.

La Figura 2 es un diagrama que representa un dispositivo electrónico, en más detalle, según el sistema aquí descrito.

La Figura 3 es un diagrama de flujo que ilustra las etapas realizadas en relación con un dispositivo electrónico que determina si realizar, o no, la validación según el sistema aquí descrito.

La Figura 4 es un diagrama de flujo que ilustra las etapas realizadas en relación con la ejecución de la validación según el sistema aquí descrito.

La Figura 5 es un diagrama de flujo que ilustra las etapas realizadas en relación con la generación de credenciales según el sistema aquí descrito.

La Figura 6 es un diagrama de flujo que ilustra las etapas realizadas en relación con la comprobación de las pruebas con respecto a las credenciales según el sistema aquí descrito.

La Figura 7 es un diagrama que ilustra un sistema que incluye una zona en la que su acceso físico ha de restringirse según el sistema aquí descrito.

DESCRIPCIÓN DETALLADA DE VARIAS FORMAS DE REALIZACIÓN

Haciendo referencia a la Figura 1A, un diagrama 20 ilustra una conexión general 22 que presenta una pluralidad de dispositivos electrónicos 24 a 26 acoplados. Aunque el diagrama 20 ilustra tres dispositivos electrónicos 24 a 26, el sistema aquí descrito puede funcionar con cualquier número de dispositivos electrónicos. La conexión 22 puede ponerse en práctica mediante una conexión directa de datos electrónicos, una conexión a través de líneas telefónicas, una red LAN, una red WAN, la red Internet, una red privada virtual o cualquier otro mecanismo para proporcionar la comunicación de datos. Los dispositivos electrónicos 24 a 26 pueden representar uno o más ordenadores portátiles, ordenadores de sobremesa (en una oficina o en el domicilio de un empleado u otra localización), dispositivos PDAs, teléfonos móviles, unidades de disco, dispositivos de almacenamiento masivo o cualquier otro dispositivo electrónico en el que pueda ser de utilidad restringir su acceso. En una forma de realización de la presente invención, los dispositivos electrónicos 24 a 26 representan ordenadores portátiles o de sobremesa que se utilizan por empleados de una organización que desea restringir su acceso en caso de que un usuario/empleado abandone la organización y/o uno de los ordenadores sea extraviado o robado. Por supuesto, pueden existir otros motivos para restringir el acceso a uno o más de los dispositivos electrónicos 24 a 26 y el sistema aquí descrito se puede utilizar en relación con cualquier puesta en práctica adecuada.

Una entidad de administración 28 establece una política para permitir el acceso por los usuarios a los dispositivos electrónicos 24 a 26. Por ejemplo, la entidad de administración 28 puede determinar que un usuario particular, U1, ya no pueda tener acceso a cualquiera de los dispositivos electrónicos 24 a 26, mientras que otro usuario U2, puede acceder al dispositivo electrónico 24 pero no a los demás dispositivos electrónicos 25, 26. La entidad administrativa 28 puede utilizar cualquier política para establecer el acceso de usuarios.

La entidad administrativa 28 proporciona una pluralidad de pruebas que se transmiten a los dispositivos electrónicos 24 a 26 a través de la conexión 22. Las pruebas se pueden proporcionar a los dispositivos electrónicos 24 a 26 por otros medios, que se examinan en más detalle a continuación. Los dispositivos electrónicos 24 a 26 reciben las pruebas distribuidas y, utilizando las credenciales almacenadas en su interior, (descritas con más detalle en otro lugar de la presente descripción), determinan si debe permitirse, o no, su acceso. De forma opcional, una entidad de distribución de pruebas 32 puede acoplarse, además, a la conexión 22 y a la entidad de administración 28. La entidad de distribución de pruebas 32 proporciona pruebas a los dispositivos electrónicos 24 a 26. En una forma de realización de la invención, una prueba solamente sería efectiva para un usuario y uno de los dispositivos electrónicos 24 a 26 y, de forma opcional, solamente para una fecha determinada o una gama de fechas.

Las pruebas se pueden proporcionar utilizando un mecanismo similar al dado a conocer en la patente de Estados Unidos número 5.666.416, en donde cada uno de los dispositivos electrónicos 24 a 26 recibe, como credenciales, un certificado digital firmado por la entidad administrativa 28 (u otra entidad autorizada), en donde el certificado digital contiene un valor especial que representa un valor inicial que tiene una función unidireccional aplicada N veces. En cada nuevo intervalo de tiempo, los dispositivos electrónicos pueden presentarse con una prueba que consiste en uno de los valores de entre el conjunto de N valores obtenidos por la aplicación de la función unidireccional. En tal caso, los dispositivos electrónicos 24 a 26 pueden confirmar que la prueba es legítima aplicando la función unidireccional, varias veces, para obtener el valor especial proporcionado en el certificado digital. Este y otros posibles mecanismos se describen con más detalle a continuación.

Asimismo, es posible utilizar uno o más de los productos proporcionados por CoreStreet, Ltd. de Cambridge, MA para proporcionar las credenciales y pruebas adecuadas según aquí se establece o utilizar cualquier otro mecanismo para generar pruebas únicas que 1) solamente podrían haberse generado por una autoridad administrativa (con ausencia de un incumplimiento de seguridad administrativa) y 2) no se puede utilizar para generar cualesquiera otras pruebas. En consecuencia, las pruebas son tales que, dada una prueba P1 legítima, un usuario no autorizado no puede generar otra prueba P2 aparentemente legítima para una finalidad diferente (p.e., para un intervalo de tiempo diferente, un dispositivo distinto, etc.). De este modo, las pruebas emitidas se pueden memorizar y distribuir de una manera insegura, lo que reduce, en gran medida, los costes asociados con el sistema. Por supuesto, es conveniente mantener una seguridad adecuada para la entidad o entidades que generen las credenciales y/o pruebas así como mantener una seguridad apropiada para cualesquiera pruebas no emitidas (p.e., futuras).

Además, un usuario no autorizado, en posesión de pruebas legítimas P1-PN, no puede generar una nueva prueba PN+1. Esto es ventajoso en varios casos. Por ejemplo, un empleado despedido no puede, por sí mismo, generar nuevas pruebas para proporcionar acceso no autorizado a su ordenador portátil de empresa después del despido, aun cuando todavía esté en posesión de todas las demás pruebas legítimas anteriores que utilizó para el ordenador portátil, mientras estaba todavía empleado por la empresa.

En una forma de realización de la presente invención, los dispositivos electrónicos 24 a 26 son ordenadores que tienen firmware y/o sistema operativo. El software que realiza el procesamiento aquí descrito, en donde las pruebas se utilizan para presentar un registro a la entrada no autorizado y/o su acceso. Al inicializarse y/o después de transcurrido un intervalo de tiempo suficiente, los ordenadores exigirían una prueba adecuada para iniciar su funcionamiento. En esta forma de realización, la funcionalidad aquí descrita se puede integrar con el sistema de login de Windows estándar (así como en entornos de BIOS o de PXE). La entidad de administración 28 puede estar integrada con las herramientas de administración de usuarios normales de redes corporativas de Microsoft y para permitir a los administradores establecer

políticas de registro de entrada (login) para cada usuario. En numeroso casos, la entidad de administración 28 puede ser capaz de derivar toda la información necesaria a partir de la información administrativa existente, lo que hace a esta nueva funcionalidad casi transparente para el administrador y se reducen los gastos de formación profesional y de adopción. La entidad de administración 28 puede ejecutarse dentro de una red de empresa o concentrarse como un modelo de ASP por un fabricante de ordenadores portátiles, fabricante de BIOS u otro socio de confianza. La entidad de distribución de pruebas 32 puede ejecutarse parcialmente dentro de la red corporativa y en parte, en un sitio global. Puesto que las pruebas no son información sensible, los depósitos globalmente accesibles del sistema de distribución de pruebas pueden realizarse como servicios de la web, con lo que se obtiene las pruebas disponibles para los usuarios fuera de sus redes corporativas.

En otras formas de realización de la presente invención, cada uno de los ordenadores exigiría una nueva prueba cada día. Sin embargo, se apreciará por los expertos en esta materia que el incremento del tiempo puede cambiarse de modo que, por ejemplo, los ordenadores puedan exigir una nueva prueba cada semana o exigir una nueva prueba cada hora.

Además, es también posible sacar partido de una característica poco utilizada de las unidades de disco duro IDE, que permite el establecimiento de una contraseña en una unidad, que se debe presentar a la unidad antes de que se hiciere operativa y permitir el acceso a sus contenidos. Si el firmware para la unidad fuera modificado para utilizar el sistema aquí descrito, es posible que el acceso a una unidad de disco duro pueda restringirse de modo que, por ejemplo, no sería posible obtener acceso a una unidad de disco duro del ordenador incluso colocándola en un ordenador diferente. Esta característica se puede poner en práctica con otros tipos de unidades de disco duro.

En otras formas de realización, el sistema se puede utilizar en relación con el acceso a archivos de datos, volúmenes de almacenamiento físico, volúmenes lógicos, etc. En algunos casos, dicha restricción de acceso a los archivos puede ser de utilidad para proporcionar modificaciones adecuadas al sistema operativo correspondiente.

Haciendo referencia a la Figura 1B, un diagrama 20' ilustra una forma de realización alternativa con una pluralidad de entidades administrativas 28a-28c. Aunque el diagrama 20' representa tres entidades administrativas 28a-28c, el sistema aquí descrito puede funcionar con cualquier número de entidades administrativas. En la forma de realización ilustrada por el diagrama 20', es posible para una de las entidades administrativas 28a-28c (p.e., la entidad administrativa 28a) generar las credenciales mientras que otras de las entidades administrativas 28a-28c (p.e., las entidades administrativas 28b, 28c) generan las pruebas o la totalidad de las entidades administrativas 28a-28c generan las pruebas. De forma opcional, la entidad de distribución de pruebas 32 se puede utilizar a este respecto.

Haciendo referencia a la Figura 1C, un diagrama 20" ilustra una forma de realización alternativa con una pluralidad de entidades de distribución de pruebas 32a-32c. Aunque el diagrama 20" ilustra tres entidades de distribución de pruebas 32a-32c, el sistema aquí descrito puede funcionar con cualquier número de entidades de distribución de pruebas. La forma de realización ilustrada por el diagrama 20" se puede poner en práctica utilizando la tecnología proporcionada por Akamai Technologies Incorporated, de Cambridge, Massachusetts.

Haciendo referencia a la Figura 1D, un diagrama 20"' ilustra una forma de realización alternativa con una pluralidad de entidades administrativas 28a'-28c' y una pluralidad de entidades de distribución de pruebas 32a'-32c'. Aunque el diagrama 20"' ilustra tres entidades administrativas 28a'-28c' y tres entidades de distribución de pruebas 32a'-32c', el sistema aquí descrito puede funcionar con cualquier número de entidades de administración y entidades de distribución de pruebas. La forma de realización ilustrada por el diagrama 20"' combina características de la forma de realización ilustrada por la Figura 1B con características de la forma de realización ilustrada por la Figura 1C.

Haciendo referencia a la Figura 2, un diagrama ilustra el dispositivo electrónico 24 con más detalles incluyendo una unidad de validación 42, datos de credenciales 44 y datos de pruebas 46. La unidad de validación 42 se puede poner en práctica utilizando hardware, software, firmware, o cualquiera de sus combinaciones. En condiciones determinadas, tal como en una inicialización, la unidad de validación 42 recibe una señal de inicialización que hace que la unidad de validación 42 examine los datos de credenciales 44 y los datos de pruebas 46 y, en función de su resultado, generan una señal de paso que indica que se ha presentado una prueba legítima o en caso contrario, genera una señal de acceso fallido. La salida de la unidad de validación 42 se puede utilizar siguiendo un determinado procesamiento/dispositivos tales como firmware de iniciación de ordenador para determinar si se puede proseguir, o no, la operación.

En otra forma de realización, el dispositivo electrónico 24 comprende una interfaz externa 48 que se controla por la unidad de validación 42. Como en el caso de la unidad de validación 42, la interfaz externa 48 se puede poner en práctica utilizando hardware, software, firmware, o cualquiera de sus combinaciones. La interfaz externa 48 está acoplada a, por ejemplo, la conexión 22 y se utiliza para la búsqueda de nuevas pruebas que puedan almacenarse en los datos de pruebas 46. De este modo, si la unidad de validación 42 determina que las pruebas almacenadas en los datos de pruebas 46 no son suficientes (p.e., han caducado), la unidad de validación 42 proporciona una señal a la interfaz externa 48 para hacer que la interfaz externa 48 solicite nuevas pruebas a través de la conexión 22. Por supuesto, si el dispositivo electrónico 24 ha sido extraviado y/o robado o si el usuario es un empleado despedido o si existe cualquier otro motivo para denegar el acceso al dispositivo electrónico 24, en tal caso, la interfaz externa 48 no será capaz de obtener una prueba válida. En algunas formas de realización, la interfaz externa 48 solicita a un usuario realizar una conexión electrónica adecuada (p.e., la conexión de un ordenador portátil a una red).

En otra forma de realización de la presente invención, los datos de tiempos 52 proporcionan información a la unidad de validación 42 para indicar la última vez que se presentó una prueba válida a la unidad de validación 42. Esta información se puede utilizar para impedir la solicitud de prueba con demasiada frecuencia y al mismo tiempo, evitar una espera demasiado larga antes de solicitar una nueva prueba. La interacción y el uso de la unidad de validación 42, la interfaz externa 48, los datos de credenciales 44, los datos de pruebas 46 y los datos de tiempos 52 se describen con más detalle a continuación.

Haciendo referencia a la Figura 3, un diagrama de flujo 70 ilustra las etapas realizadas en relación con la determinación de si enviar, o no, la señal de inicio a la unidad de validación 42 para determinar si la unidad de validación 42 debe examinar, o no, los datos de credenciales 44 y los datos de pruebas 46 para generar una señal de paso o de acceso fallido. El procesamiento comienza en una primera etapa 72 en donde se determina si se realiza, o no, una operación de inicialización. En otra forma de realización, las pruebas se comprueban siempre en relación con una operación de inicialización. En consecuencia, si se determina en la etapa de prueba 72 que se está realizando una inicialización, en tal caso, el control se transfiere desde la etapa 72 a una etapa 74 en donde se envía la señal de inicio a la unidad de validación 42. Después de la etapa 74 se realiza la etapa 76 en donde el proceso espera una magnitud predeterminada de tiempo antes de realizar un funcionamiento cíclico de nuevo. En otra forma de realización, la cantidad de tiempo predeterminada puede ser un día, aunque se pueden utilizar también otras magnitudes de tiempo. Después de la etapa 76, el control se transfiere de nuevo a la etapa de prueba 72, anteriormente descrita.

Se determina, en la etapa de prueba 72, que una operación de inicialización no se está realizando, en cuyo caso, el control se transfiere desde la etapa de prueba 72 a una etapa de prueba 78 en donde se determina si ha transcurrido una cantidad de tiempo predeterminada desde la última ejecución realizada por la unidad de validación 42. Esta circunstancia operativa se determina utilizando el elemento de datos de tiempos 52 y quizás el tiempo del sistema actual. En otra forma de realización, la cantidad de tiempo predeterminada utilizada en la etapa de prueba 78 es un día. Si se determina, en la etapa de prueba 78, que la cantidad de tiempo desde la última ejecución de la unidad de validación 42 es mayor que la cantidad de tiempo predeterminada, en tal caso, el control se transfiere desde la etapa de prueba 78 a la etapa 74, en donde se envía la señal de inicio a la unidad de validación 42. Después de la etapa 74 o después de la etapa de prueba 78, si la cantidad de tiempo no es mayor que la cantidad de tiempo predeterminada, se pasa a la etapa 76, anteriormente examinada.

Haciendo referencia a la Figura 4, un diagrama de flujo 90 ilustra las etapas realizadas en relación con la unidad de validación 42 para determinar si se ha recibido una prueba suficiente. Según se describe en otro lugar de la presente, la unidad de validación 42 envía una señal de paso o una señal de intento fallido para el seguimiento del procesamiento/dispositivos (tal como un firmware de inicialización de ordenador o firmware de unidad de disco). El procesamiento comienza en una primera etapa 92 en donde la unidad de validación 42 determina la prueba necesaria. La prueba necesaria es la prueba determinada por la unidad de validación 42 suficiente para ser capaz de enviar una señal de paso. La unidad de validación 42 determina la prueba necesaria examinando los datos de credenciales 44, los datos de pruebas 46, los datos de tiempos 52 y quizás, incluso el reloj del sistema/interno. Después de la etapa 92 existe una etapa de prueba 94 que determina si la prueba adecuada está disponible al nivel local (esto es, en los datos de pruebas 46) y si la prueba proporcionada, a nivel local, cumple los requisitos necesarios (descritos en otro lugar de la presente). Si es así, entonces el control se transfiere desde la etapa 94 a una etapa 96, en donde la unidad de validación 42 emite una señal de paso. Después de la etapa 96, el procesamiento está concluido.

En alguna formas de realización, es posible y deseable obtener y almacenar pruebas futuras en los datos de pruebas 46. Por ejemplo, un usuario que espera estar sin una conexión a la entidad de administración 28 y/o la entidad de distribución de pruebas 32 puede obtener y almacenar futuras pruebas. En esta forma de realización, el dispositivo electrónico puede efectuar automáticamente un sondeo para futuras pruebas, cuando se conecta a la entidad de administración 28 y/o la entidad de distribución de pruebas 32, que se pueden proporcionar según una política predefinida. Como alternativa (o en adición), puede ser posible para un usuario y/o dispositivo electrónico solicitar concretamente futuras pruebas que puedan o no proporcionarse en conformidad con la política vigente.

Si se determina, en la etapa de prueba 94, que la prueba adecuada no está disponible a nivel local (esto es, en los datos de pruebas 46), en tal caso, el control se transfiere desde la etapa de prueba 94 a una etapa de prueba 98 en donde la unidad de validación 42 determina si una prueba adecuada está disponible exteriormente proporcionando, por ejemplo, una señal para hacer que la interfaz externa 48 intente la búsqueda de la prueba, según se describió anteriormente. Si se determina que la etapa de prueba 98, y que la prueba proporcionada exteriormente cumple los requisitos necesarios (examinados en otro lugar de la presente), en tal caso, el control se transfiere desde la etapa de prueba 98 a la etapa 96, anteriormente descrita, en donde la unidad de validación 42 emite una señal de paso. En otra forma de realización, la prueba exteriormente proporcionada se almacena en los datos de pruebas 46.

Si se determina, en la etapa de prueba 98, que una prueba adecuada no está disponible exteriormente, puesto que no existe ninguna condición adecuada o por algún otro motivo, en tal caso, el control se transfiere desde la etapa de prueba 98 a una etapa 102, en donde al usuario se le solicita que introduzca una prueba adecuada. En otra forma de realización, si un usuario está en una posición sin una conexión eléctrica adecuada, el usuario puede llamar a un número de teléfono particular y recibir una prueba adecuada en la forma de un número que puede introducirse manualmente en el dispositivo

electrónico en relación con la solicitud proporcionada en la etapa 102. Por supuesto, el usuario puede recibir la prueba por otros medios, tales como de forma manuscrita o mecanografiada o incluso publicada en un periódico (p.e., en la sección de anuncios clasificados).

Después de la etapa 102 es una prueba 104 la que determina si el usuario ha introducido una prueba que cumple los requisitos necesarios (según se describe en otro lugar de la presente). Si es así, entonces el control se transfiere desde la etapa de prueba 104 a la etapa 96, anteriormente descrita, en donde la unidad de validación 42 emite una señal de paso. De no ser así, el control se transfiere desde la etapa de prueba 104 a una etapa 106 en donde la unidad de validación 42 emite una señal de fallo. Después de la etapa 106, el procesamiento está concluido.

Haciendo referencia a la Figura 5, un diagrama de flujo 120 ilustra las etapas realizadas en relación con la generación de credenciales utilizadas por la unidad de validación 42. Las etapas del diagrama de flujo 120 se pueden realizar por la entidad de administración 28 que genera las credenciales (y una serie de pruebas) y proporciona las credenciales al dispositivo electrónico 24. Otras entidades adecuadas (p.e., entidades autorizadas por la entidad de administración 28) pueden generar las credenciales. El valor aleatorio se utiliza en relación con la generación de las credenciales y las pruebas y, en otra forma de realización, suele ser imprevisible. Después de la etapa 122 existe una etapa 124 en donde una variable de índice, I, se pone a 'uno'. En otra forma de realización, las credenciales que se proporcionan se utilizan para un año completo y se necesita una nueva prueba cada día de modo que trescientas sesenta y cinco pruebas separadas se puedan generar en relación con la generación de las credenciales. La variable de índice, I, se utiliza para mantener un registro del número de pruebas que se generan. Después de la etapa 124 existe una etapa 126 en donde el valor de prueba inicial, Y(0) se establece igual al valor aleatorio RV determinado en la etapa 122.

Después de la etapa 126 existe una etapa de prueba 128 que determina si la variable de índice, I, es mayor que un valor de finalización, IEND. Como se examinó anteriormente, en otra forma de realización, trescientas sesenta y cinco pruebas se generan en relación con la generación de las credenciales de modo que, en esta forma de realización, IEND, tiene un valor de trescientos sesenta y cinco. Sin embargo, para otras formas de realización, es posible establecer el valor de IEND en cualquier otro número.

Si se determina, en la etapa de prueba 128, que el valor de I no es mayor que el de IEND, en tal caso, el control se transfiere desde la etapa 128 a una etapa 132 en donde Y(I) se establece igual a la función unidireccional aplicada a Y(I-1). La función unidireccional utilizada en la etapa 132 es tal que, dado el resultado de aplicar la función unidireccional, resulta casi imposible determinar el valor que fue introducido para la función unidireccional. De este modo, para la función unidireccional utilizada en la etapa 132, dada Y(I), es muy difícil, sino imposible, averiguar el valor de la entrada (en este caso Y(I-1)). Tal como aquí se utiliza, el término de función unidireccional incluye cualquier función u operación que proporcione, de forma adecuada, esta propiedad incluyendo, sin limitación, funciones *hash* unidireccionales convencionales y firmas digitales. Esta propiedad de la función unidireccional utilizada en la etapa 132 es de utilidad en relación con su capacidad para almacenar y distribuir pruebas emitidas de una manera insegura, según se examina en otro lugar de la presente descripción. Las credenciales y las pruebas pueden generarse en diferentes momentos o las pruebas se pueden regenerar en una fecha posterior por la entidad que generó las credenciales o por otra entidad. Conviene señalar que, para otras formas de realización, es posible tener Y(I) no siendo una función de Y(I-1) o cualquier otro valor de Y a tal respecto.

El procesamiento se inicia en una primera etapa 122 en donde se genera un valor aleatorio, RV. Después de la etapa 132 existe una etapa 134 en donde se incrementa la variable de índice, I. Después de la etapa 134, el control se transfiere de nuevo a la etapa de prueba 128, anteriormente descrita. Si se determina, en la etapa de prueba 128, que I es mayor que IEND, en tal caso el control se transfiere desde la etapa de prueba 128 a una etapa 136 en donde un valor final, FV, se establece igual a Y(I-1). Conviene señalar que se resta "1" del valor I porque I fue incrementado más allá de IEND. Después de la etapa 136 existe una etapa 138 en donde la entidad de administración 28 (o alguna otra entidad que genera las pruebas y las credenciales) realiza una firma digital del valor final, la fecha actual y otra información que se utiliza en relación con las pruebas. En otra forma de realización, dicha otra información se puede utilizar para identificar el dispositivo electrónico particular (p.e., ordenador portátil), el usuario particular o cualquier otra información que está vinculada con las credenciales y la prueba para un dispositivo electrónico particular y/o usuario y/o alguna otra propiedad. De forma opcional, la fecha y/o el valor FV se pueden combinar con la otra información. Por ejemplo, es posible utilizar un mensaje firmado como OCSP que simplemente indique "dispositivo nº 123456 es válido el 1/1/2004" o tenga un bit en un miniCRL que corresponde a un dispositivo específico que está activado o desactivado. En dichos casos, la credencial en el dispositivo puede efectuar la autenticación del dispositivo (es decir, determinar que el dispositivo es realmente el dispositivo nº 123456, etc.). OCSP y los miniCRLs se conocen en esta técnica. Después de la etapa 138, se concluye el procesamiento.

Haciendo referencia a la Figura 6, un diagrama de flujo 150 ilustra las etapas realizadas por la unidad de validación 42 en relación con la determinación de la validez de una prueba. El procesamiento comienza en una primera etapa 152 en donde la unidad de validación 42 recibe la prueba (p.e., mediante la lectura de la prueba a partir de los datos de pruebas 44). Después de la etapa 152 existe una etapa 154 en donde la unidad de validación 42 recibe las credenciales (p.e., mediante la lectura de los datos de credenciales 46).

Después de la etapa 154 existe una etapa de prueba 156 que determina si la otra información que se proporciona con las credenciales es correcta. Como se describió en otro lugar de la presente descripción, la otra información incluye, por ejemplo, una identificación del dispositivo electrónico, una identificación del usuario, u otra propiedad que identifica la información. Si se determina, en la etapa de prueba 156, que la otra información asociada con las credenciales no coincide con la propiedad particular descrita por la otra información (p.e., las credenciales son para un dispositivo electrónico diferente o un usuario diferente), en tal caso el control se transfiere desde la etapa de prueba 156 a una etapa 158 en donde se proporciona una señal de fallo. Después de la etapa 158, se concluye el procesamiento.

Si se determina, en la etapa de prueba 156, que la otra información asociada con las credenciales está correcta, entonces el control se transfiere desde la etapa de prueba 156 a una etapa 162, en donde una variable N se establece igual a la fecha actual menos la fecha asociada con las credenciales (es decir, el número de días transcurridos desde que se emitieron las credenciales). Después de la etapa 162 existe una etapa 164 en donde el valor de prueba proporcionado en la etapa 152 tiene una función unidireccional aplicada N veces. La función unidireccional, utilizada en la etapa 164, corresponde a la función unidireccional utilizada en la etapa 132, anteriormente descrita.

Después de la etapa 164 existe una etapa de prueba 166 que determina si el resultado obtenido en la etapa 164 es igual al valor final FV, que es parte de las credenciales recibidas en la etapa 154. Si es así, entonces el control se transfiere desde la etapa de prueba 166 a una etapa 168 en donde se proporciona una señal de paso por la unidad de validación 42. De no ser así, si se determina, en la etapa de prueba 166, que el resultado obtenido en la etapa 164 no es igual al valor final FV proporcionado con las credenciales en la etapa 154, en tal caso, el control se transfiere desde la etapa de prueba 166 a una etapa 172 en donde se genera una señal de fallo por la unidad de validación 42. Después de la etapa 172, se concluye el procesamiento.

Las firmas digitales pueden proporcionar una forma efectiva de autenticación de Internet. A diferencia de las contraseñas tradicionales y de los números PINs, las firmas digitales pueden proporcionar autenticación que puede ser universalmente verificable y no repudiable. Las firmas digitales pueden producirse mediante una clave de signatura, SK, y verificarse mediante una clave de verificación de coincidencia, PK. Un usuario U mantiene su propia clave SK secreta (de modo que solamente el usuario U pueda firmar en nombre de U). Lamentablemente, la clave PK no "revela" la clave de coincidencia SK, es decir, el conocimiento de la clave PK no proporciona a un intruso ninguna ventaja práctica en el cálculo de SK. Por lo tanto, un usuario U podría hacer su propia PK tan pública como sea posible (de modo que cualquiera pueda verificar las firmas de U). Por este motivo, PK es preferentemente denominada la clave pública. Conviene señalar que el término "usuario" puede significar un usuario, una entidad, un dispositivo o un conjunto de usuarios, dispositivos y/o entidades.

Las claves públicas se pueden utilizar, además, para la encriptación asimétrica. Una clave de encriptación pública PK se puede generar junto con una clave de desencriptación de coincidencia de SK. De nuevo, el conocimiento de PK no revela a SK. Cualquier mensaje se puede encriptar fácilmente con la clave PK, pero el texto cifrado así determinado sólo puede desencriptarse fácilmente mediante el conocimiento de la clave SK. Por lo tanto, un usuario U podría hacer su propia PK tan pública como sea posible (de modo que cualquiera pueda encriptar mensajes para U), pero manteniendo la clave SK privada (de modo que solamente U pueda leer mensajes encriptados para U).

El sistema RSA, bien conocido en esta técnica, proporciona un ejemplo de ambas firmas digitales y encriptación asimétrica.

Las cadenas alfanuméricas, denominadas certificados, establecen que una clave PK dada sea una clave pública de un usuario dado U. Una entidad, con frecuencia denominada autoridad de certificación (CA), genera y emite un certificado para un usuario. Los certificados caducan después de un periodo de tiempo especificado, que suele ser de un año en el caso de las autoridades CAs públicas. En esencial, un certificado digital C consiste en una firma digital de CAs que se vincula, de forma segura, junto con varias magnitudes: SN, un número de serie único para el certificado, PK, la clave pública del usuario, U, el nombre del usuario, D_1, la fecha de emisión, D_2, la fecha de caducidad e información adicional (incluyendo ninguna información), AI. En símbolos, $C=SIG_{CA}(SN,PK,U,D_1,D_2,AI)$.

Las claves de encriptación públicas pueden proporcionar, además, un medio de autenticación/identificación. Por ejemplo, una parte que conoce que una clave de encriptación pública privada PK pertenece a un usuario dado U (p.e., porque la parte ha verificado un certificado digital correspondiente para U y PK) y si desea identificar a U, puede utilizar la clave PK para encriptar un desafío aleatorio C y pedir a U que responda con la desencriptación correcta. Puesto que solamente el poseedor de la clave SK (y por lo tanto, U) puede realizar esta operación, si la respuesta al desafío es correcta, U está adecuadamente identificado.

Es posible proporcionar un sistema para controlar el acceso físico a una zona utilizando una puerta inteligente (y/o una puerta virtual inteligente; véase la correspondiente descripción en otro lugar de la presente). Una puerta inteligente puede verificar que la persona que entra está actualmente autorizada para hacerlo. Puede ser conveniente proporcionar a la puerta no solamente la credencial de un usuario dado, sino también una prueba separada de que la credencial/usuario tiene todavía validez de una forma que se pueda utilizar, con seguridad, incluso por una puerta desconectada. En una forma de realización, dichas pruebas se generan como sigue. Suponiendo que una credencial especifica las puertas, un usuario puede entrar. En tal caso, para cada credencial y cada intervalo de tiempo (p.e., cada día), una entidad adecuada

E (p.e., la misma entidad que decide quién está autorizado para qué puerta en cualquier momento, o una segunda entidad que trabaje para esa entidad) calcula una indicación de prueba autenticada (PROOF), de que una credencial dada es válida en el intervalo de tiempo dado. (Si las credenciales no identifican las puertas para las que los usuarios están autorizados a entrar, una indicación PROOF puede especificar también las puertas para las que la credencial es adecuada en el intervalo de tiempo dado).

Una PROOF de E puede consistir en una firma digital de E que indica, en una forma autenticada, que una credencial dada es válida para un intervalo de tiempo dado, por ejemplo: SIG_E(ID, Día, Válida, AI), en donde ID es la información que identifica la credencial (p.e., el número de serie de la credencial), Día es una indicación del intervalo de tiempo dado (sin pérdida de generalidad prevista, un día dado), Válida es una indicación de que la credencial se considera válida (esta indicación se puede omitir si E nunca firma una cadena de datos similar a no ser que la credencial se considere válida) y AI indica cualquier información adicional (incluyendo ninguna información) estimada de utilidad. En algunos casos, la firma de E puede ser una firma de clave pública. (No obstante, podría ser también una firma de clave privada, es decir, una firma que puede generarse y verificarse mediante una clave secreta única, conocida por el firmante y por el verificador). Si la credencial consiste en un certificado digital, una sub-forma de realización puede consistir en un certificado de vida útil corta, es decir, una firma digital que re-emite la credencial para el intervalo de tiempo deseado (p.e., un certificado digital que especifica la misma clave pública, el mismo usuario U y alguna otra información básica como antes, pero que especifica la fecha de inicio y la fecha de caducidad con el fin de identificar el día deseado – sin pérdida de generalidad prevista). Por ejemplo, permitir, sin pérdida de generalidad prevista, un último certificado de corta duración para un día, en dicha sub-forma de realización, una PROOF puede adoptar la forma de SIG_E(PK, U, D_1, D_2, AI), en donde la fecha de inicio D_1 indica el principio de un día dado D y la fecha final D_2 el final correspondiente del día D, o en donde D_1=D_2=D; o más simplemente, utilizando un campo de información de fecha única con el fin de identificar el día en cuestión, SIG_E(PK, U, Día, AI). Si E coincide con la autoridad de certificación original, un certificado de corta duración PROOF puede adoptar la forma SIG_{CA}(PK, U, D_1, D_2, AI) o SIG_{CA}(PK, U, Día, AI).

Siendo objeto de autenticación, un usuario no puede fabricar su propia PROOF del día (es decir, la PROOF del día de su propia credencial), ni puede cambiar su PROOF de ayer en su propia PROOF de hoy, ni la PROOF de otro usuario para hoy en la suya propia para hoy. Puesto que las PROOFs son esencialmente no susceptibles de olvido ni de modificación, estas PROOFs no necesitan protegerse. De este modo, la entidad E puede hacer que las PROOFs estén disponibles con un coste insignificante. Por ejemplo, E puede registrar todas las pruebas PROOF de un día dado en Internet (p.e., hacer que las PROOFs estén disponibles a través de servidores Akamai o equivalente), o enviar las PROOFs a respondedores/servidores que puedan alcanzarse con facilidad por los usuarios. Por ejemplo, para un servidor localizado a la entrada de un aeropuerto (o edificio de oficinas) en donde estén localizadas gran parte de las puertas a accederse de forma correcta. De esta manera, un empleado que llega a su trabajo puede recoger fácilmente su propia PROOF (p.e., insertando su propia tarjeta en un lector de tarjetas acoplado con el servidor) y asimismo, memorizar la PROOF en su propia tarjeta, junto con su propia credencial. De este modo, cuando el usuario presente su tarjeta a una puerta que su credencial le autoriza para acceder, la puerta no solamente puede verificar la credencial sino que también recibe y verifica una PROOF de autorización actual, sin necesidad de conectarse en absoluto. La puerta verifica la PROOF (p.e., la firma digital de E mediante una clave pública de E que se puede memorizar desde su instalación) y que el intervalo de tiempo especificado por la PROOF es adecuado (p.e., mediante su propio reloj local). Si todo está correcto, la puerta concede el acceso y si no lo está, la puerta deniega el acceso. En esencia, la puerta se puede desconectar y no obstante, su verificación de PROOF puede ser relativamente fácil (porque la puerta puede recibir la PROOF por la parte más disponible: el propio usuario que demanda el acceso) y al mismo tiempo, relativamente segura (aunque la puerta reciba la PROOF desde la parte más sospechosa: el propio usuario que demanda el acceso). De hecho, un usuario que demanda el acceso puede estar normalmente en la proximidad física de la puerta y de este modo, puede proporcionar la PROOF con facilidad, sin utilizar ninguna conexión a un emplazamiento distante y de este modo, operar con independencia de la conectividad de la puerta. Al mismo tiempo, el usuario que demanda el acceso puede ser la fuente de información menos fiable en ese momento crucial. No obstante, puesto que el usuario no puede fabricar ni modificar una PROOF de su propia validez actual en modo alguno, la puerta puede tener la seguridad de que una PROOF adecuadamente verificada debe producirse por E, y E no habría producido la PROOF si E conociera que el usuario no está autorizado durante el intervalo de tiempo dado. Cuando un usuario deja de estar autorizado, E interrumpirá la emisión de PROOF de autorización para el usuario y de este modo, el usuario ya no puede entrar a través de puertas incluso desconectadas, porque el usuario carecerá de la PROOF que una puerta necesita verificar para poder conceder su acceso. De este modo, utilizando el usuario que demanda el acceso pruebas de autorización adecuada y actual, el sistema aquí descrito dispensa las inconveniencias asociadas con otros sistemas, esto es, la necesidad de encargar a un grupo de trabajo la reprogramación de las puertas desconectadas.

Este método permite, además, gestionar el acceso de las puertas desconectadas por "cargo" (o por "privilegio"). Es decir, en lugar de tener una credencial que especifique las puertas que su usuario está autorizado para entrar y luego emitir - p.e., cada día – una PROOF de validez actual de una credencial (o en lugar de emitir una PROOF que especifique que una credencial dada autoriza a su usuario a entrar por algunas puertas en un intervalo de tiempo dado), las puertas desconectadas se pueden programar (p.e., en el momento de la instalación) para conceder acceso solamente a usuarios que tengan un cargo profesional dado. Por ejemplo, una puerta de la cabina en un avión puede ser programada para conceder acceso solamente a PILOTOS e INSPECTORES. Las credenciales se pueden emitir a empleados principalmente para comprobar su identidad (que no se cambie), mientras que cada PROOF que E - p.e., emite diariamente para una credencial dada, puede especificar además (p.e., en el campo AI) los cargos de su usuario

correspondiente en ese día. Por ejemplo, PROOF = SIG_E(ID, Día, PILOTO, AI) prueba en el Día indicado que el usuario correspondiente a la credencial identificada por ID es un piloto. De esta manera, los empleados pueden "migrar" desde un cargo al siguiente sin tener que volver a emitir su credencial y sin necesidad de especificar dentro de una credencial de usuario o en su PROOF diaria correspondiente, a qué puertas el usuario puede acceder ese día. Conviene señalar que el número de dichas puertas puede ser muy grande. De este modo, especificando dentro de una credencial de usuario todas las puertas a las que un usuario puede estar autorizado a acceder, puede ser una tarea que exija un tiempo excesivo. Además, si se añaden nuevas puertas (p.e., porque se adquieren nuevas aeronaves), entonces, la credencial del piloto puede tener que volverse a emitir, lo que resulta también oneroso, para especificar las puertas adicionales.

Los intervalos de tiempo adecuados para una credencial dada se pueden especificar dentro de la propia credencial o se pueden especificar por la credencial y la PROOF conjuntamente. Por ejemplo, una credencial puede especificar un día de inicio dado y que necesita probarse válida cada día, mientras que la PROOF puede especificar el intervalo de tiempo 244, lo que significa que la PROOF se refiere al día 244 después del día de inicio especificado en la propia credencial.

El sistema aquí descrito puede ser también ventajoso en relación con sistemas de puertas conectadas de más alto coste. Por ejemplo, suponiendo que todas las puertas fueron conectadas, de forma segura, a una base de datos central y que se produce una parada técnica imprevista (p.e., por sabotaje). En tal caso, las puertas conectadas pueden verse obligadas a elegir entre dos alternativas extremas: SIEMPRE ABIERTA (buena para seguridad, pero de protección deficiente, en particular, si fueron terroristas los que causaron la parada técnica) y SIEMPRE CERRADA (mala para seguridad pero buena para la protección personal). En contraste, en caso de una parada técnica imprevista, el sistema aquí descrito ofrece una respuesta mucho más flexible, algunas (no ya) puertas conectadas pueden permanecer siempre cerradas, otras siempre abiertas y otras, no obstante, pueden seguir funcionando según el control de acceso de puertas desconectadas aquí descrito. Es decir, las puertas, que funcionen con baterías, pueden abrirse solamente si se presenta la credencial correcta y las PROOFs correctas. De hecho, antes de que se produzca la parada técnica es posible para todos los empleados recibir periódicamente sus PROOFs previstas.

Por supuesto, la entidad E puede generar PROOFs que especifican diferentes intervalos de tiempo para diferentes credenciales. Por ejemplo, en una instalación de aeropuerto, los oficiales de policía y personal de emergencia pueden, cada día, tener una PROOF que especifique a las dos semanas siguientes como el intervalo de tiempo pertinente, mientras que todos los empleados ordinarios pueden tener, cada día, PROOFs que especifiquen solamente el día en cuestión. Dicho sistema puede proporcionar un mejor control en caso de una parada técnica larga e imprevista. Si se produce dicha parada técnica, la distribución usual diaria de PROOFs se puede interrumpir y los empleados ordinarios pueden no recibir sus PROOFs diarias, pero los policías y los responsables de gestión de casos de emergencia pueden poseer todavía, en sus tarjetas, las pruebas de dos semanas que recibieron el día antes y por lo tanto, pueden continuar accionando todas las puertas para las que estén autorizados a entrar (p.e., todas las puertas).

Debe entenderse que el método aquí descrito abarca la utilización de credenciales que consisten en una forma de certificado reducida, que puede denominarse como certificados mínimos. Un certificado mínimo puede omitir esencialmente el nombre del usuario y/o el identificador ID del certificado o sustituir el nombre de usuario y/o el identificador ID por una clave pública del certificado, (que puede ser única para cada certificado). Por ejemplo, una credencial de certificado mínimo puede adoptar la forma C=SIG_{CA}(PK,D_1,D_2, AI), con el entendimiento de que la presentación adecuada de esta credencial incluye probar el conocimiento de la clave secreta SK correspondiente a PK (p.e., mediante un método de desafío-respuesta). La puerta puede conocer, de antemano, si la presentación adecuada (o no) de una credencial relativa a PK (preferentemente, si está actualmente validada) debe dar lugar a la concesión del acceso. Como alternativa, una credencial C mínima puede especificar (p.e., en AI) si un usuario que conoce la SK correspondiente está autorizado, o no, para entrar por una puerta dada. Una PROOF relativa a un certificado mínimo cuya clave pública es PK, puede adoptar la forma SIG_E(ID, Día, Válida, AI) o SIG_E(PK, Día, Válida, AI) o SIG_E(ID, Día, AI) si se entiende que cualquier firma similar indica la validez por implicación. Como alternativa, una PROOF de vigencia de un certificado mínimo puede adoptar la forma de la re-emisión de un certificado mínimo de corta duración: p.e., SIG_E(PK,D_1,D_2, AI), en donde la fecha de inicio D_1 indica el comienzo de un día dado D y D_2 el final correspondiente del día D, o D_1=D_2=D; o SIG_E(PK, Día, AI); o permitiendo que E coincida con la autoridad de certificación original, SIG_{CA}(PK,D_1,D_2,AI) o SIG_{CA}(PK, Día, AI). En general, cualquier método aquí descrito dirigido a certificados debe entenderse que se aplica también a certificados mínimos.

Una puerta inteligente puede verificar la validez y la vigencia de las credenciales de un usuario, que pueden ir acompañadas por una prueba correspondiente. Las credenciales/pruebas utilizadas por un usuario, para obtener acceso a una zona, pueden ser similares a las credenciales/pruebas utilizadas en relación con el control del acceso a dispositivos electrónicos, según se describe en otro lugar de la presente. A continuación, se proporcionan ejemplos de credenciales/pruebas, algunos de los cuales se pueden combinar con otros:

1. Un número PIN o contraseña, introducido a través de un teclado asociado con la puerta o comunicarse a la puerta por una tarjeta de usuario;
2. Información biométrica, proporcionada por un usuario a través de un lector especial asociado con la puerta;
3. Una firma tradicional (manuscrita), proporcionada por un usuario a través de un teclado especial asociado con la puerta;

4. Un certificado digital para una clave pública PK (p.e., dicha credencial se puede memorizar en una tarjeta de usuario y el usuario correcto/tarjeta puede utilizar la clave secreta correspondiente SK para autenticarse/identificarse por sí mismo a la puerta - p.e., mediante un protocolo de desafío-respuesta). Por ejemplo, si PK es una clave pública de firma, la puerta puede exigir la firma de un mensaje dado y el usuario correcto es el único que conoce la tecla de firma secreta SK correspondiente que podrá proporcionar así la firma solicitada correcta; si PK es una clave de encriptación pública, la puerta puede exigir la presentación de un texto cifrado desencriptado dado, que se puede realizar por el usuario correcto, que conoce la clave de desencriptación secreta correspondiente SK;
5. Un certificado digital mejorado que incluye un "valor de validación" diario (que garantiza que el certificado es válido en esta fecha particular), memorizado en una tarjeta de usuario y comunicado a la puerta;
6. Una firma digital de una autoridad central que confirme que un certificado de usuario es válido en el momento actual, comunicado a la puerta por un servidor o un respondedor;
7. Un certificado digital que se memoriza en una tarjeta de usuario y se comunica a la puerta, así como un "valor de validación" diario comunicado a la puerta por un servidor o un respondedor;
8. Un valor secreto, memorizado en una tarjeta de usuario, cuyo conocimiento se comprueba para la puerta por intermedio de un protocolo interactivo (posiblemente de conocimiento cero) con la puerta;
9. Una firma de clave secreta de una autoridad, memorizada en una tarjeta de usuario, que indica que el usuario está autorizado para entrar en un día particular.

De este modo, en algunos casos, se proporcionan credenciales/pruebas en una parte única mientras que, en otros casos, las credenciales/pruebas se proporcionan en partes separadas, por un lado las credenciales y por separado, las pruebas. Por ejemplo, en donde las credenciales/pruebas consisten en un certificado digital mejorado que incluye un valor de validación diaria que indica que el certificado es válido en esa fecha particular y está asociado con un usuario y comunicado a la puerta, las credenciales (el certificado digital mejorado) se pueden proporcionar por separado (por medios diferentes y/o en momentos diferentes) de las pruebas (el valor de validación diaria). De forma similar, las credenciales y las pruebas pueden ser todas ellas generadas por la misma autoridad o se pueden generar por autoridades diferentes.

Haciendo referencia a la Figura 7, un diagrama ilustra un sistema 200 que incluye una zona 202 en la que ha de restringirse su acceso físico. La zona 202 está encerrada por una pluralidad de paredes 204-207. La pared 207 tiene una puerta 212 para proporcionar salida a la zona 202. En otras formas de realización, se pueden utilizar más de una puerta. Las paredes 204-207 y la puerta 212 proporcionan una barrera para el acceso a la zona 202. La puerta 212 se puede bloquear utilizando una cerradura electrónica que impide la apertura de la puerta 212 a no ser que y hasta que la cerradura electrónica 214 reciba una señal adecuada. La cerradura electrónica 214 se puede poner en práctica utilizando cualquier elemento adecuado que proporcione la funcionalidad aquí descrita, incluyendo, sin limitación, la utilización de cerraduras electrónicas de uso ordinario.

La cerradura electrónica 214 puede acoplarse a un controlador 216, que proporciona una señal adecuada para la cerradura electrónica 214 para permitir la apertura de la puerta 212. En algunas formas de realización, la cerradura electrónica 214 y el controlador 216 pueden proporcionarse en una sola unidad. El controlador 216 puede acoplarse con una unidad de entrada 218, que puede recibir credenciales de un usuario y de forma opcional, recibir también una prueba correspondiente que indique que un usuario está actualmente autorizado para entrar en la zona 202. La unidad de entrada 218 puede recibir también una alerta de revocación directa (HRA) que indique que al usuario ya no le está permitido entrar en la zona 202. Las alertas HRAs se describen, con más detalle, a continuación. La unidad de entrada 218 puede ser cualquier dispositivo de entrada adecuado, tal como un teclado, un lector de tarjetas, una unidad biométrica, etc.

De forma opcional, el controlador 216 puede tener una conexión externa 222 que se puede utilizar para transmitir datos a y desde el controlador 216. La conexión externa 222 puede ser segura aunque, en algunas formas de realización, la conexión externa 222 puede no necesitar ser segura. Además, la conexión externa 222 puede no ser necesaria porque la funcionalidad aquí descrita puede proporcionarse utilizando unidades autónomas que no tengan conexiones exteriores. En aquellos casos en que se proporciona la conexión externa 222, dicha conexión externa 222 se puede utilizar para transmitir credenciales, pruebas, HRAs y/o se puede emplear en relación con el registro del acceso a la zona 202. El registro del acceso se describe con más detalle en otro lugar en esta misma descripción. Conviene señalar que la conexión externa 222 puede ser intermitente de modo que, por ejemplo, en algunos momentos la conexión externa 222 proporciona conectividad para el controlador 216 mientras que, en otros momentos, puede no existir ninguna conexión externa para el controlador 216. En algunos casos, la conexión externa 222 puede utilizarse para transmitir una parte de las credenciales/pruebas (p.e., un certificado digital PKI) mientras que un usuario presenta a la unidad de entrada 218 una parte restante de las credenciales/pruebas (p.e., un valor de validación diaria utilizado en relación con el certificado digital).

En algunas formas de realización, un usuario puede presentar una tarjeta 224 a la unidad de entrada. Según se describe en otro lugar de la presente, la tarjeta 224 puede ser una tarjeta inteligente, una PDA, etc. que proporciona datos (p.e., credenciales/pruebas) a la unidad de entrada 218. La tarjeta 224 puede obtener algunos o la totalidad de los datos desde un transpondedor 226. En otros casos, la tarjeta 224 puede obtener datos de otras tarjetas (no representadas), desde la unidad de entrada 218 (o algún otro mecanismo asociado con el acceso a la zona 202), o alguna otra fuente adecuada.

En un primer ejemplo, las credenciales y pruebas se pueden mantener utilizando un número PIN/contraseña con protección física. En este ejemplo, cada mañana un servidor genera una nueva contraseña secreta SU para cada usuario autorizado U y comunica la nueva SU a puertas específicas a las que le está permitido acceder al usuario U. La comunicación puede ser encriptada para enviarse utilizando líneas no seguras o se puede transmitir a las puertas a través de algunos otros medios seguros. Cuando el usuario U informa de que tiene que trabajar por la mañana, el servidor central hace que la tarjeta del usuario U reciba la contraseña secreta actual SU. La contraseña secreta SU se guarda en la memoria de seguridad de la tarjeta, que se puede leer solamente cuando la tarjeta está adecuadamente autorizada (p.e., por el usuario que introduce un número PIN secreto en relación con la tarjeta o mediante la conexión con hardware de confianza en el servidor o las puertas). Siempre que el usuario intente acceder por una puerta, la tarjeta comunica, de forma segura, la contraseña SU a la puerta. A continuación la puerta comprueba si el valor SU recibido desde la tarjeta coincide con el valor recibido desde el servidor por la mañana y, si es así, permite el acceso.

De este modo, SU es la credencial del usuario para un día. Este sistema tiene la ventaja de que cada credencial es de duración limitada: si un empleado se despide o su tarjeta es sustraida, sus credenciales no serán útiles en el día siguiente. El sistema, sin embargo, exige alguna conectividad: al menos un breve periodo de conectividad (preferentemente cada mañana) se necesita para actualizar la puerta. Esta transmisión debe asegurarse (p.e., físicamente o de forma criptográfica).

En otro ejemplo, las credenciales del usuario incluyen firmas con claves secretas. Este ejemplo utiliza firmas, que pueden ser firmas de claves públicas (p.e., firmas RSA) o firmas de claves secretas (p.e., Códigos de Autenticación de Mensajes o MACs). Por ejemplo, un servidor de control de acceso utiliza una clave secreta SK para generar firmas y la puerta dispone de medios para verificar dichas firmas (p.e., mediante una clave pública correspondiente o compartiendo el conocimiento de la misma clave SK). Cuando un usuario U informa de que va a trabajar por la mañana en un día D, el servidor hace que la tarjeta del usuario reciba una firma Sig que autentica la información de identificación del usuario U (p.e., el número de tarjeta único o la contraseña secreta del usuario U o información biométrica, tal como huellas dactilares del usuario U) y la fecha D. Cuando el usuario U intenta acceder por una puerta, la tarjeta comunica la firma Sig a la puerta, que verifica su validez posiblemente en conjunción con la información de identificación suministrada por el propio usuario U y la fecha suministrada por el reloj local de la puerta. Si todo ello es correcto, la puerta permite el acceso.

En esta técnica, la firma Sig se puede considerar como las credenciales del usuario y su prueba conjuntamente. Este método tiene sus propias ventajas: las tarjetas no necesitan memorizar secretos y las puertas no necesitan mantener conexiones seguras con un servidor central, ni una larga lista de credenciales válidas.

En otro ejemplo, las credenciales del usuario incluyen un certificado digital con pruebas de validez de cadena de funciones *hash* similares a las generadas en relación con el diagrama de flujo 120 de la Figura 5. Este ejemplo utiliza firmas de claves públicas y una función-resumen *hash* unidireccional H (que pone en práctica un tipo especial de firma digital). Una autoridad central tiene un par de claves: una clave pública PK (conocida para las puertas) y una clave secreta SK que no se suele conocer. Para un usuario U, la autoridad genera un valor secreto aleatorio X0 y un valor calculado X1 = H(X0), X2 = H(X1), …, X365 = H(X364). Puesto que H es una función *hash* unidireccional, cada valor de X no se puede calcular a partir del valor siguiente de X. La autoridad emite para el usuario U un certificado digital Cert, firmado utilizando la clave SK y que contiene el valor X365, válido para un año. En tal caso, cuando el usuario U informa que va a trabajar el día i, la autoridad hace que la tarjeta del usuario reciba el valor de validación de ese día Xj, donde j = 365 - i. Cuando U intenta acceder a una puerta, la tarjeta comunica el valor de validación Xj y el certificado Cert que contiene X365 a la puerta. La puerta verifica la validez del certificado Cert con la clave pública PK de la autoridad y comprueba también que H aplicada i veces a Xj produce X365. Conviene señalar que el término de "un año" y 365 se puede sustituir por cualquier otro periodo de tiempo.

De este modo, el certificado Cert del usuario así como el valor de validación Xj constituyen las credenciales/pruebas del usuario. Este sistema tiene numerosas ventajas: ni la puerta ni la tarjeta necesitan memorizar ningún secreto; la puerta no necesita tener ninguna conexión segura; el certificado se puede emitir una vez al año y en adelante, la carga de cálculo diaria sobre la autoridad central es mínima (porque la autoridad solamente necesita recuperar Xj); los valores de validación diaria se pueden proporcionar por respondedores distribuidos no seguros (de bajo coste) porque no necesitan ser secretos.

Una credencial/prueba para un usuario U suele estar limitada en su duración, lo que es de utilidad en varias circunstancias. Por ejemplo, si el usuario U es un empleado de un aeropuerto y es objeto de despido, sus credenciales/pruebas pueden caducar al final del día y ya no podrá acceder a las puertas del aeropuerto. Para un control de acceso más preciso, puede ser deseable disponer de credenciales de más corta duración. Por ejemplo, si la credencial/prueba para U incluye la hora y los minutos así como la fecha, entonces el usuario U puede ser bloqueado con respecto al acceso al aeropuerto transcurrido un solo minuto desde su despido. Sin embargo, las credenciales/pruebas de más corta duración exigen una actualización más frecuente, lo que añade gastos al sistema. Podría ser inconveniente si cada empleado, en un aeropuerto, tuviera que cargar nuevas credenciales/pruebas en su tarjeta cada minuto. De este modo, puede producirse un conflicto inherente entre los deseos de tener credenciales a corto plazo y de tener un sistema de más bajo coste, lo que puede dar lugar a credenciales que a veces ya no sean

deseadas. Por ejemplo, el usuario U puede necesitar bloquearse del acceso al aeropuerto de forma inmediata, pero su credencial no caduca hasta la medianoche. Por lo tanto, es deseable proporcionar una cancelación inmediata de las credenciales que todavía no han caducado.

Conviene señalar que si las credenciales/pruebas son siempre memorizadas en una base de datos segura, que sea consultada por las puertas cada vez que se solicita un acceso, es relativamente sencillo cancelar las credenciales/pruebas mediante, por ejemplo, la eliminación de las credenciales/pruebas canceladas desde la base de datos. Sin embargo, al tener una puerta que consultar una base de datos segura cada vez, resulta de alto coste. En primer lugar, porque esto añade un retardo significativo a la operación puesto que el usuario necesita acceder a la puerta de inmediato, pero tiene que esperar a que la consulta sea adecuadamente concluida. En segundo lugar, porque esta comunicación es preferentemente realizada a través de un canal seguro, que puede costar fácilmente 4.000 dólares por puerta (o más) o estar completamente indisponible en algunos casos (p.e., para puertas de aviones o contenedores de carga). En tercer lugar, porque una base de datos segura única sólo puede gestionar una carga de consulta limitada y la replicación de una base de datos segura es en sí misma de alto coste y exigente en dedicación de tiempo (p.e., porque los costes de mantener la base de datos segura deben duplicarse y debe medirse el esfuerzo para mantener estas copias sincronizadas). Por lo tanto, a diferencia del método completamente conectado, los métodos desconectados o intermitentemente conectados (tales como los descritos en los ejemplos anteriores) necesitan menos comunicación y suelen memorizar las credenciales/pruebas en respondedores no asegurados o en las propias tarjetas. En tal caso, simplemente retirando las credenciales/pruebas desde la base de datos puede no ser suficiente. Para referirse de nuevo a los ejemplos anteriores, la contraseña SU, o la firma de la autoridad competente o el valor de validación Xj tendrían que eliminarse, de alguna manera, desde una tarjeta de usuario o desde las puertas. Además, incluso dicha eliminación puede no garantizar siempre la revocación de una credencial, puesto que una credencial memorizada en un respondedor no seguro puede estar disponible para cualquier usuario, incluyendo un intruso malicioso que podría guardarla e intentar emplearla después de su eliminación desde la tarjeta de usuario. De este modo, aun cuando existan soluciones de menor coste con credenciales de duración limitada, estas soluciones, por sí mismas, no proporcionan necesariamente una revocación suficiente de una credencial/prueba no caducada.

La cancelación de credenciales/pruebas se puede realizar utilizando una Alerta de Revocación Directa (HRA), que es un elemento de datos (preferentemente autenticados) que se transmiten a la puerta que impedirán que la puerta conceda acceso a un usuario con credenciales/pruebas canceladas (aunque posiblemente no caducadas). Por ejemplo, una HRA puede consistir en un mensaje con firma digital que indique que las credenciales/pruebas dadas han sido canceladas. Conviene señalar, sin embargo, que una firma no siempre puede estar implicada en una HRA. Por ejemplo, en el caso de una puerta con conexión segura, simplemente enviando una HRA a lo largo de la conexión protegida puede ser suficiente. Sin embargo, según se indicó anteriormente, las puertas con conexión segura pueden ser de alto coste en algunos casos e imposible (o casi imposible) en otros casos

Es de utilidad el que las HRAs sean autenticadas de modo que una entidad a la que se presenta una HRA pueda tener una relativa certeza de que la HRA es auténtica. Permitiendo que el identificador ID sea un identificador para las credenciales/pruebas C canceladas (en particular, el identificador ID puede coincidir con la propia C), entonces SIG(ID, "CANCELADA", AI) puede ser una HRA, en donde "CANCELADA" significa cualquier manera de señalización de que C ha sido cancelada ("CANCELADA" posiblemente sea la cadena vacía si el hecho de que las credenciales/pruebas sean canceladas podría deducirse por otros medios, tales como un convenio al nivel de sistema de que dichos mensajes firmados no sean enviados excepto en caso de cancelación), y AI significa cualquier información adicional (posiblemente información de fecha, tal como el momento en que las credenciales/pruebas han sido canceladas y/o el momento en que la HRA fue producida o ninguna información). La firma digital SIG puede ser, en particular, una firma digital de clave pública, una firma digital de clave secreta o un código de autenticación de mensaje. También es posible emitir una HRA autenticada mediante una encriptación adecuada de la información. Por ejemplo, una HRA autenticada puede adoptar la forma ENC(ID, "CANCELADA", AI).

Otro ejemplo notable de una HRA autenticada se describe en la Patente de Estados Unidos 5.666.416, que se incorpora aquí por referencia. La autoridad emisora incorpora en una credencial/prueba C una clave pública PK (de un sistema de firma digital) que es única para C, de modo que una firma digital relativa a esa clave PK indica que C se cancela. En una forma de realización especial de dicho sistema, PK puede consistir en un valor Y1 calculado como Y1 = H (Y0), en donde H es una función unidireccional (preferentemente de la función *hashing*) y Y0 es un valor secreto. Cuando se cancela la credencial/prueba C, se emite la HRA que consiste en solamente Y0. Dicha HRA se puede verificar mediante la función *hashing* Y0 y comprobando que el resultado coincide con el valor Y1 que pertenece a la credencial/prueba C.

Conviene señalar que una firma puede no requerirse para una HRA. Por ejemplo, en caso de una puerta conectada con seguridad, simplemente enviando (ID, "CANCELADO", AI) a lo largo de la conexión protegida puede ser suficiente como una HRA. Sin embargo, la ventaja de las HRAs autenticadas es que las propias HRAs no necesitan ser secretas. Las HRAs autenticadas, una vez autenticadas por la autoridad competente, se pueden memorizar en uno o más respondedores (posiblemente geográficamente dispersos). Además, estos respondedores pueden no estar protegidos (a diferencia de la autoridad emisora), porque no están memorizando información secreta. Se puede proporcionar una mayor fiabilidad, a un más bajo coste, efectuando una replicación de múltiples respondedores no protegidos. Algunas ventajas adicionales del ejemplo de HRA autenticado de la Patente de Estados Unidos 5.666.416 son: (1) la HRA es relativamente corta (puede ser tan corta como de 20 bytes), (2) se calcula con relativa facilidad (simplemente una

consulta del Y0 anteriormente memorizado) y (3) es relativamente fácil de verificar (simplemente una aplicación de una función resumen *hash* unidireccional).

Las HRAs autenticadas pueden ser particularmente ventajosas para una amplia difusión eficiente, según se describe a continuación. Cuando una HRA transita a través de múltiples puntos en dirección a la puerta, pueden existir múltiples posibilidades de una HRA incorrecta a insertarse en el sistema. En realidad, una HRA recibida por la puerta no directamente a través o desde el emisor, a través de una conexión segura, puede ser no más de un simple rumor de cancelación de una credencial particular. Si la HRA es autenticada, sin embargo, este rumor se puede confirmar fácilmente por la puerta, que puede verificar su autenticidad.

En general, una HRA puede ser específica para una credencial/prueba única o puede proporcionar información de cancelación en relación con una multiplicidad de credenciales/pruebas. Por ejemplo, ID1,…IDk son identificadores para credenciales canceladas, una HRA puede consistir en la firma digital única SIG(ID1,…IDk; "CANCELADA"; AI). Considérese el caso de una puerta que memoriza información que identifica las credenciales/pruebas que tiene el derecho de acceder a la puerta. Si dicha puerta recibe una HRA que indica que una o más credenciales/pruebas son canceladas, la puerta no necesita memorizar la HRA. Basta para la puerta borrar las credenciales/pruebas identificadas desde su memoria (o marcarlas como "CANCELADA" de alguna otra forma). A continuación, si un usuario con una credencial/prueba cancelada intenta el acceso, la puerta no le permitirá el acceso porque la credencial/prueba presentada no la tiene actualmente memorizada o, si la tiene memorizada, está marcada como "REVOKED" (CANCELADA).

Considérese ahora un caso de una puerta que no memoriza información que identifica todas las credenciales/pruebas permitidas, pero que verifica si una credencial/prueba está permitida cuando se presenta. Cuando un usuario presenta una credencial/prueba a dicha puerta, la puerta puede verificar primero si la credencial/prueba es válida, desechando las HRAs. (Por ejemplo, si la credencial/prueba incluye una firma digital, la puerta verifica la firma. Además, si la credencial/prueba incluye un tiempo de caducidad, la puerta puede verificar también que la credencial/prueba no está caducada, p.e., utilizando un reloj interno). No obstante, aun cuando todas las comprobaciones sean pasadas, la puerta puede todavía denegar el acceso si la credencial/prueba se indica como siendo cancelada por una HRA. Por lo tanto, es de utilidad si dicha puerta tiene información respecto a las HRAs pertinentes. Una manera de conseguirlo es, para la puerta, memorizar todas las HRAs presentadas a la puerta. Por otro lado, en algunos casos, esta operación puede llegar a ser inviable. Considérese un sistema en donde numerosas credenciales/pruebas se podrían utilizar para pasar a través de esa puerta. Por ejemplo, el Departamento de Transporte de Estados Unidos está considerando la posibilidad de un sistema de 10.000.000 de credenciales para una diversidad de personas (incluyendo pilotos, personal de aeropuerto, empleados de líneas aéreas, mecánicos, manipuladores de equipajes, conductores de carretillas elevadoras, policía, etc.) que pueden en uno u otro momento tener acceso permitido para una puerta dada. En una tasa de cancelación anual del 10% reducida, la puerta puede tener un 1.000.000 HRAs que memorizar al final de un año, que puede ser una tarea onerosa (si no, inviable). Además, si la cantidad de las HRAs no pueden determinarse con precisión por anticipado, los diseñadores de un sistema pueden tener que sobreestimar la magnitud del almacenamiento para las HRAs con el fin de estar en el lado seguro y construir incluso más capacidad de almacenamiento (e incluso más coste) en la puerta.

Este problema se puede resolver por medio de las denominadas HRAs eliminables. Esto significa tener una HRA que indique una componente de tiempo que especifica cuándo la HRA se puede eliminar con seguridad del almacenamiento. Por ejemplo, en un sistema con credenciales/pruebas de duración limitada, esto se puede conseguir: (1) haciendo que una credencial/prueba incluya un tiempo de caducidad transcurrido el cual la credencial/prueba no debe admitirse por la puerta como válida para su acceso; (2) disponer de una HRA que cancele las credenciales/prueba que incluyen el tiempo de caducidad y (3) hacer que la puerta elimine de su memoria la HRA que cancela las credenciales/pruebas después del tiempo de caducidad. Por ejemplo, el tiempo de caducidad para una credencial/prueba podría ser el tiempo en el que caduca la credencial/prueba (y el tiempo de caducidad podría ser explícitamente incluido y autenticado dentro de la credencial/prueba o podría ser implícito por convenios al nivel de sistema). La eliminación de dicha HRA después de transcurrir su tiempo de caducidad, no menoscaba la seguridad. En realidad, si la puerta no memoriza la HRA que cancela una credencial/prueba particular, puede ser porque la puerta borró la HRA de la memoria después de su caducidad, en cuyo momento la credencial/prueba obsoleta tendrá su acceso denegado por la puerta en cualquier forma.

Conviene señalar que etapa (2) anterior puede ser opcional en casos en que el tiempo de caducidad pueda indicarse en una HRA de forma implícita o indirecta. Por ejemplo, la HRA puede adoptar la forma SIG(C, "CANCELADA", AI), y las credenciales/pruebas pueden incluir su propia fecha de caducidad. Además, la etapa (1) anterior puede ser opcional puesto que las HRAs eliminables se pueden realizar también con HRAs que no indiquen los tiempos de caducidad de las credenciales canceladas en absoluto. Por ejemplo, si todas las credenciales, en un sistema particular, son válidas para como máximo un día, en tal caso, todas las HRAs se pueden borrar después de memorizarse para un día. (Más en general, si la duración máxima de una credencial/prueba se puede deducir en alguna manera, entonces se puede borrar una HRA correspondiente después de memorizarse para dicha cantidad de tiempo). A modo de otro ejemplo, cuando se presenta con la credencial/prueba con un tiempo de caducidad particular, la puerta puede buscar una HRA que cancele la credencial. Si existe y el tiempo de caducidad ya ha transcurrido, entonces la puerta puede eliminar, con seguridad, la HRA. En cualquier otro caso, la puerta puede memorizar el tiempo de caducidad en relación con la HRA memorizada y eliminar la HRA transcurrido dicho tiempo.

Una puerta puede eliminar HRAs después de su caducidad en una diversidad de formas. En algunos casos, la eliminación de HRA puede realizarse de forma eficiente manteniendo una estructura de datos (tal como una cola de espera de prioridad) de las HRAs basadas en tiempos de caducidad. Como alternativa, la puerta puede revisar periódicamente todas las HRAs en memoria y purgar las que ya no se necesiten. Como otra alternativa, la puerta puede borrar una HRA si, cuando encuentra la HRA, la puerta constata que la HRA ya no es pertinente. Por ejemplo, las HRAs se pueden memorizar en una lista que se comprueba cada vez que se presente una credencial para su verificación. Siempre que una HRA caducada se encuentre en dicha lista, la HRA caducada se puede eliminar. En otra alternativa, la puerta puede eliminar las HRAs solamente cuando sea necesario, cuando la memoria necesite espacio libre (quizás para otras HRAs).

Las HRAs eliminables pueden reducir, en gran medida, la capacidad de almacenamiento requerida en la puerta. Utilizando el ejemplo anterior de 10.000.000 de usuarios y una tasa de cancelación anual del 10%, en tal caso, si las HRAs caducan y se eliminan, por término medio, en un día, solamente 2.740 (en lugar de 1.000.000), puede ser necesario memorizar las HRAs. Este requisito de almacenamiento reducido es una gran ventaja potencial de HRAs eliminables.

Es de utilidad para las HRAs hacerse disponibles para las puertas con la mayor rapidez posible, con el fin de informar a las puertas de las credenciales/pruebas que ya no son admisibles. Lo anterior puede constituir un problema para las puertas desconectadas, pero también puede ser un problema para las puertas completamente conectadas. Por supuesto, a alguna puerta completamente conectada se puede enviar una HRA a través de la conexión de la puerta cuando se emita la HRA. Sin embargo, esta transmisión puede todavía bloquearse u obstaculizarse por un intruso determinado (p.e., si la conexión a la puerta está asegurada por medios criptográficos, un intruso puede simplemente cortar el hilo de conexión o modificar/filtrar las señales de desplazamiento. Si la conexión a la puerta está asegurada mediante la instalación de un hilo de conexión en un tubo de acero, entonces dicha obstaculización y bloqueo puede ser más difícil, pero sigue siendo no imposible). Dicha otra obstaculización y bloqueo malintencionado de una HRA puede ser incluso más fácil de realizar para puertas con conectividad intermitente (p.e., inalámbricas).

Con el fin de hacer más difícil para un intruso impedir que una puerta reciba una HRA, una HRA se puede transmitir por una propia tarjeta cancelada. Por ejemplo, cuando una tarjeta se comunica con una base de datos o una puerta conectada (o cualquier puerta que tenga conocimiento de la HRA pertinente), la puerta puede enviar la HRA a la tarjeta, que puede memorizar la HRA. En particular, esta operación se puede realizar sin ninguna indicación al usuario con el fin de la protección contra usuarios que puedan desear manipular individualmente la tarjeta y eliminar la HRA. Este método es más efectivo si la tarjeta transmite una componente de hardware a prueba de manipulación indebida o datos (p.e., datos encriptados) que no sean fácilmente leídos/eliminados por el usuario. Cuando la tarjeta se utiliza posteriormente en un intento de tener acceso a cualquier puerta (incluso completamente desconectada), la tarjeta puede comunicar su HRA a la puerta, que, después de la verificación adecuada, puede denegar el acceso (y, en algunos casos, memorizar la HRA).

La HRA se puede enviar a través de un canal inalámbrico (p.e., a través de un dispositivo buscapersonas (pager) o una red celular o vía satélite) a la tarjeta. Esta operación se puede realizar aun cuando la tarjeta tenga capacidades de comunicaciones limitadas – por ejemplo, colocando un transmisor inalámbrico en un lugar por el que cada usuario sea probable que pase. Por ejemplo, en un edificio, dicho transmisor puede colocarse en cada entrada del edificio para proporcionar una oportunidad para cada tarjeta de recibir la transmisión siempre que un usuario de una de las tarjetas entre en el edificio. Como alternativa, el transmisor puede situarse en las entradas de la parcela de aparcamiento, etc.

Para impedir a un usuario malintencionado bloquear la transmisión (mediante, por ejemplo, envolviendo la tarjeta en material que fuere impenetrable por la señal transmitida), la tarjeta puede requerir, de hecho, que reciba transmisiones periódicas para poder funcionar adecuadamente. Por ejemplo, la tarjeta puede esperar una señal cada cinco minutos para poder sincronizar su reloj con el de los sistemas, o puede esperar recibir otra señal periódica (preferentemente con firma digital) tal como una señal de GPS, o simplemente esperar un ruido apropiado a las frecuencias apropiadas. Si dicha señal no se recibe con un intervalo de tiempo razonable, la tarjeta puede "bloquearse" y simplemente rechazar la comunicación con cualquier puerta, lo que le hace no apta para el acceso. Conviene señalar que dicho sistema puede ser más económico y cómodo que simplemente difundir todas las HRAs para todas las tarjetas, porque las HRAs son mensajes personalizados y de cambio continuo. De este modo, la difusión de las HRAs a todas las tarjetas puede exigir el establecimiento de un satélite de uso especial o la personalización de uno ya existente. El método anterior, en cambio, tiene la ventaja de disponer ya de señales para amplias transmisiones e instala transmisores de nivel local para los mensajes personalizados.

Como alternativa, se puede impedir a un usuario bloquear las transmisiones a una tarjeta si la policía de seguridad exige al usuario llevar la tarjeta en un lugar visible, como una tarjeta de identificación de seguridad o para presentarla en un lugar adecuado (dentro de un margen de transmisión) a un vigilante. Una técnica adicional para difundir una HRA para una tarjeta/credencial/prueba particular puede incluir la utilización de OTRAS tarjetas para transmitir la HRA a las puertas. En una de sus versiones, la Tarjeta 1 puede (p.e., cuando se recoge su propia credencial/prueba diaria o de forma inalámbrica o cuando se comunica con una puerta conectada o cuando realiza cualquier clase de conexión) recibir una HRA, HRA2, que cancele una credencial/prueba asociada con una tarjeta diferente, Tarjeta 2. La Tarjeta 1 puede

memorizar, entonces, HRA2 y comunicar HRA2 a una puerta, que luego memoriza también HRA2. La Tarjeta 1 puede, de hecho, proporcionar HRA2 a múltiples puertas, por ejemplo, a todas las puertas o a todas las puertas desconectadas a las que se accede o comunica con la Tarjeta 2 durante un periodo de tiempo particular (p.e., durante un día completo). En este punto, cualquier puerta (aun cuando esté desconectada), alcanzada por la Tarjeta 1 puede ser capaz de denegar el acceso al titular de la Tarjeta 2 que contiene la credencial/prueba cancelada. En una forma de realización preferida, HRA2 tiene una firma digital o una propia autenticación y cualquier puerta alcanzada por la Tarjeta 1 comprueba la autenticidad de HRA2, de modo que impida la difusión malintencionada de HRAs falsas.

Lo anterior se puede perfeccionar haciendo que una puerta alcanzada por la Tarjeta 1 comunique la HRA2 aprendida a otra tarjeta, Tarjeta 3, que posteriormente accede o se comunica con la puerta. Esto es de utilidad porque la Tarjeta 3 puede alcanzar puertas que la Tarjeta 1 no alcanzare o lo hiciere después que la Tarjeta 3. Este proceso puede continuar haciendo que estas puertas adicionalmente alcanzadas se comuniquen con otras tarjetas, etc. Además, es posible que algunas puertas, aun cuando no estén completamente conectadas a una base de datos central, puedan tener conexiones entre sí. Dichas puertas, de este modo, pueden intercambiar HRAs disponibles de forma similar. Si las tarjetas tienen una capacidad de comunicación entre sí, por ejemplo, cuando están en proximidad, pueden intercambiar también información sobre las HRAs que memorizan.

Conviene señalar que las HRAs autenticadas pueden ser especialmente ventajosas con las técnicas de difusión de HRA aquí examinadas. En realidad, el envío de HRAs a través de múltiples intermediarios (tarjetas y puertas) puede proporcionar múltiples puntos de fallo en donde las HRAs pueden ser HRAs modificadas o falsas que se pueden inyectar por un intruso. En cierto sentido, las HRAs no autenticadas pueden llegar a ser simples rumores en el momento en que alcancen las puertas. Por el contrario, las HRAs autenticadas, pueden estar garantizadas para ser correctas sin importar que alcancen las puertas.

En aquellos casos en que los recursos no son una preocupación importante, todas las HRAs podrían memorizarse y difundirse de esta manera. Puede ser también posible adoptar algunas organizaciones. Por ejemplo, una tarjeta puede gestionar el almacenamiento de HRA como una puerta y eliminar las HRAs caducadas para liberar memoria de tarjeta interna y para evitar una comunicación innecesaria con otras puertas. Reducir al mínimo las tareas de almacenamiento y comunicación puede ser de utilidad dentro de dicho sistema porque, cuando el número de credenciales canceladas no caducadas pueda ser pequeño, es posible que algunos componentes (p.e., algunas tarjetas o puertas) puedan no tener suficiente memoria o ancho de banda para gestionar todas las HRAs no caducadas.

Otra posibilidad para reducir al mínimo las tareas de almacenamiento y comunicación incluye la selección de qué HRAs han de difundirse a través de qué tarjetas. Por ejemplo, las HRAs pueden contener información de prioridad, que indique la importancia relativa de la difusión de conocimientos sobre una credencial/prueba particular con la mayor rapidez posible. Por ejemplo, algunas HRAs pueden ser etiquetadas como "urgentes" mientras que otras pueden ser etiquetadas como de "rutina". (Una graduación de prioridades pueden ser lo más fina o aproximada como sea adecuado). Los dispositivos con memoria o ancho de banda limitado pueden registrar e intercambiar información sobre las HRAs de más alta prioridad y solamente si lo permiten los recursos, pueden dedicar su atención a las de más baja prioridad. A modo de otro ejemplo, una HRA que impida a una tarjeta acceder a una puerta dada puede difundirse a través de tarjetas que sean más probable que alcancen con rapidez esa puerta (p.e., tarjetas cuya credenciales permiten el acceso a esa puerta o puertas en su proximidad). En realidad, la tarjeta y la puerta pueden establecer una comunicación con el objetivo de establecer qué HRAs admiten su almacenamiento y/o difusión posterior. Como alternativa, la HRAs o tarjetas para su memorización se pueden seleccionar de una forma que implique una aleatoriedad o una puerta puede proporcionar una HRA para un determinado número de tarjetas (p.e., las primeras k tarjetas que "encuentre" la puerta).

El uso de dichas técnicas de difusión puede reducir la probabilidad de que un usuario con credenciales/pruebas canceladas fuere capaz de obtener acceso puesto que, incluso para una puerta desconectada, un usuario tendría que obtener de la puerta, antes que cualquier otro usuario proporcione HRA adecuada con una tarjeta de actualización. El intercambio de información entre tarjetas y puertas puede ayudar a garantizar que numerosas tarjetas sean rápidamente informadas de una cancelación. Este método puede utilizarse también como una contramedida frente a los ataques “obstaculizantes” que intenten desconectar una puerta conectada e impedir que la puerta reciba la HRA. Aun cuando dicho ataque tenga éxito y la puerta nunca sea informada de la HRA por los servidores centrales o respondedores, una tarjeta de usuario individual puede informar probablemente a la puerta de la HRA en cualquier otra forma. Conviene señalar que el método real de intercambio de las HRAs entre tarjetas y puertas puede variar. En caso de HRAs de corta duración, puede ser más eficiente intercambiar y comparar todas las HRAs conocidas. Si numerosas HRAs se ponen juntas en una sola lista, la lista puede contener un tiempo que indique cuándo la lista fue emitida por el servidor. En tal caso, las tarjetas y puertas pueden comparar primero los tiempos de emisión de sus listas de HRAs y la que sea la lista más antigua puede sustituirse con la lista más reciente. En otros casos, se pueden utilizar algoritmos más sofisticados para encontrar y reconciliar diferencias.

Una difusión de HRA eficiente se puede realizar:

(1) emitiendo una HRA autenticada;
(2) enviando la HRA autenticada a una o más tarjetas;
(3) haciendo que las tarjetas se envíen la HRA autenticada a otras tarjetas y/o puertas;

(4) haciendo que las puertas memoricen y/o transmitan a otras tarjetas las HRAs recibidas.

Puede ser de utilidad, en detalle, algún uso de HRA muestra:

SECUENCIA 1 (directamente desde la "autoridad" a la puerta):

1. La entidad E cancela una credencial/prueba para un usuario U y emite un HRA A que contiene la información de que la credencial/prueba ha sido cancelada;
2. A se transmite a través de una combinación cableada o inalámbrica a una puerta D;
3. D verifica la autenticidad de A, y si la verificación tiene éxito, memoriza la información sobre A;
4. Cuando U intentan acceder a D presentando la credencial/prueba, la puerta D observa que la información memorizada sobre A indica que la credencial/prueba está cancelada y se deniega el acceso.

SECUENCIA 2 (desde la "autoridad" a una tarjeta de usuario para la puerta):

1. La entidad E cancela una credencial/prueba para un usuario U y emite una HRA A que contiene la información de que la credencial/prueba ha sido cancelada;
2. Otro usuario U' informa de que va a trabajar y preestablece su tarjeta para E con el fin de obtener su credencial/prueba actual;
3. Junto con la credencial/prueba para U', la HRA A se transmite a la tarjeta del usuario U'; la tarjeta memoriza A (la tarjeta puede, o no, verificar la autenticidad de A, dependiendo de las capacidades de la propia tarjeta);
4. Cuando U' intenta acceder a una puerta D, su tarjeta transmite la credencial/prueba junto con A a D;
5. D verifica la autenticidad de A y, si la verificación tiene éxito, memoriza A;
6. Cuando el usuario U intenta acceder a D presentando una credencial/prueba, la puerta D observa que A tiene la cancelación de la credencial/prueba del usuario U y deniega el acceso.

SECUENCIA 3 (desde la "autoridad" a otra puerta para una tarjeta de usuario en la puerta):

1. La entidad E cancela una credencial/prueba para un usuario U y emite una HRA A que contiene la información de que la credencial/prueba de U’ ha sido cancelada;
2. A se transmite a través de una combinación cableada o inalámbrica a una puerta D';
3. D' verifica la autenticidad de A y, si la verificación tiene éxito, memoriza A;
4. Otro usuario U', con su propia credencial/prueba, presenta su tarjeta a la puerta D' con el fin de obtener acceso a D'. La puerta D', además de verificar las credenciales/pruebas del usuario U' y de conceder acceso si fuera apropiado, transmite A a la tarjeta de U'. La tarjeta memoriza A (la tarjeta puede, o no, memorizar la autenticidad de A, dependiendo de las capacidades de la tarjeta);
5. Cuando el usuario U' intenta acceder a una puerta D, su tarjeta transmite su propia credencial/prueba junto con A a D;
6. La puerta D' verifica la autenticidad de A y, si la verificación tiene éxito, memoriza A;
7. Cuando el usuario U intentan acceder a la puerta D presentando su credencial/prueba, la puerta D observa a A, cancelando la credencial/prueba de usuario U y deniega su acceso.

SECUENCIA 4 (desde la "autoridad" a la tarjeta de usuario en la puerta):

1. La entidad E cancela una credencial C para un usuario U y emite una HRA A que contiene la información de que C ha sido cancelada;
2. El usuario U, portador de su tarjeta, pasa un punto de transmisión situado cerca de la entrada del edificio, lo que hace que su tarjeta reciba A; la tarjeta memoriza A (la tarjeta puede, o no, verificar la autenticidad de A, dependiendo de las capacidades de la tarjeta);
3. Cuando U intenta acceder a una puerta D, su tarjeta transmite A junto con C a D;

4. D verifica la autenticidad de A y, si la verificación tiene éxito, memoriza A y deniega el acceso al usuario U;

5. Si el usuario U intenta de nuevo acceder a D presentando C, la puerta D observa la A anteriormente memorizada que cancela C y deniega el acceso.

A veces, puede ser de utilidad establecer, después del hecho, que intentó acceder a una puerta particular, en qué momento, qué credenciales/pruebas se presentaron y si el acceso fue denegado o concedido. Puede también ser de utilidad conocer si el mecanismo de una puerta llegó a ser obstaculizado, si un conmutador o sensor tuvo fallos, etc. Con esta finalidad, puede ser deseable mantener registros de los eventos que tengan lugar. Dichos registros pueden ser particularmente útiles si están fácilmente disponibles en alguna localización central, de modo que se puedan inspeccionar y actuar en consecuencia. Por ejemplo, en caso de fallo de hardware, un equipo de reparación puede necesitar trasladarse con prontitud. Existen, sin embargo, dos importantes problemas con dichos registros .

En primer lugar, si una puerta está conectad, puede ser más fácil recoger registros enviándoles a través de la conexión. Sin embargo, la recogida de registros de eventos puede ser más difícil para las puertas desconectadas. Por supuesto, una manera de recoger registros es enviar una persona para cada puerta desconectada para entregar físicamente los registros de nuevo a la localización central, pero este método resulta de alto coste.

En segundo lugar, para que se cree un registro de eventos, la integridad del sistema completo que rodea a la generación, recogida y almacenamiento de los registros debe estar garantizada. De no ser así, por ejemplo, un intruso puede crear entradas de registros falsas o suprimir las válidas. Los métodos tradicionales, tales como asegurar físicamente los canales de distribución y las instalaciones de almacenamiento de datos son de muy alto coste (y pueden no ser suficientes por sí mismos).

Los registros convencionales pueden comprobar que “un determinado usuario se trasladó a una determinada puerta” por la mera existencia de dicha entrada del registro, que debe suponerse que es válida. Sin embargo, esto no puede ser apropiado para una aplicación de alta seguridad. Considérese el caso de un usuario U acusado de deteriorar alguna propiedad detrás de una puerta bloqueada D. Una entrada de registro tradicional puede proporcionar solamente una evidencia débil de que U entró a través de D: tendría que confiar en que no se produjo ninguna entrada de registro malintencionadamente falsificada. En consecuencia, es deseable disponer de registros que proporcionen una evidencia mucho más fuerte, porque no pueden ser “fabricados” por un intruso. En particular, los registros indiscutibles pueden probar que la puerta D (posiblemente con la cooperación de la tarjeta del usuario U) creó el registro en su agenda.

El sistema aquí descrito resuelve este problema de la manera siguiente: Cuando una puerta recibe una credencial/prueba presentada como parte de una petición de acceso, la puerta puede crear una entrada de registro (p.e., una cadena de datos) que contenga información sobre el evento, por ejemplo:

Tiempo de petición;
Tipo de petición (si más de una petición es posible - por ejemplo, si la petición es para salida o para entrada o para activar o desactivar el motor, etc.);
Credencial/prueba e identidad presentada (si la hubiere);
Si la credencial/prueba tuvo éxito en su verificación;
Si la credencial/prueba tenía una HRA correspondiente;
Si el acceso fue concedido o denegado.

Las entradas de registro puede contener, además, datos operativos o información sobre cualesquiera eventos inusuales, tales como fluctuaciones de corriente de tensión, fallos de sensores, posiciones de conmutadores, etc. Una manera de obtener un registro indiscutible incluye hacer que las puertas tengan información de eventos con firma digital por medio de una clave secreta (SK). El registro indiscutible resultante se puede representar por SIG(evento, AI), en donde AI significa cualquier información adicional. El método de firma utilizado por puerta D puede ser una clave pública o una clave privada.

Si fuera de utilidad resaltar la clave pública PK relativa a que la firma sea válida, o la clave secreta SK utilizada en la generación de la firma o la puerta que generó la firma, se podría representar simbólicamente el registro indiscutible por SIG_{PK}(evento, AI), SIG_{SK}(evento, AI), o SIG_{D}(evento, AI). Dicho registro puede ser indiscutible porque un intruso no puede falsificar la firma de la puerta sin conocer la clave secreta pertinente. En otro modo, la autenticidad del registro se podría comprobar por cualquier verificador adecuadamente informado (p.e., uno que conozca la clave PK de la puerta o la clave SK de la puerta) sin tener que confiar en la integridad de la base de datos que almacena el registro o la del sistema que transmite el registro. En general, los registros pueden hacerse indiscutibles no solamente mediante la firma digital de cada entrada, sino también utilizando una etapa de autenticación digital para múltiples entradas. Por ejemplo, la puerta podría autenticar una multiplicidad de eventos E1, E2, ... por medio de una firma digital: simbólicamente, SIG(E1,… E2,AI). Como es habitual, en cualquier lugar de esta aplicación, una firma digital puede significar el proceso de la firma digital del *hash* unidireccional de los datos que han de autenticarse. En particular, la autenticación continua puede considerarse como un caso especial de firma digital. Por ejemplo, cada entrada autenticada podría utilizarse para la autenticación de la siguiente (o la anterior). Una forma de hacerlo consiste en hacer que una entrada autenticada

incluya la clave pública (en particular, la clave pública de una firma digital de una sola vez) utilizada para la autenticación de la siguiente u otras entradas.

Los registros ordinarios y los registros indiscutibles pueden realizarse también mediante tarjetas (en particular, una tarjeta puede hacerse un registro indiscutible mediante información con firma digital sobre un evento E: en símbolos, SIG(E,AI)). La totalidad de las técnicas de registro, aquí descritas, pueden interpretarse también como relacionadas con registros hechos de tarjetas.

Además, otros registros ordinarios y registros indiscutibles se pueden obtener implicando a la puerta y a la tarjeta. Por ejemplo, durante una petición de acceso de puerta, la tarjeta puede proporcionar a la puerta la propia entrada de registro de la tarjeta (posiblemente indiscutible) a la puerta. La puerta puede inspeccionar la entrada de registro y conceder acceso solamente si la puerta encuentra que la entrada de registro es "admisible". Por ejemplo, la puerta puede verificar la firma digital de la tarjeta que autentica la entrada de registro o la puerta puede verificar que la información del tiempo incluida en la entrada de registro de la tarjeta es correcta en función de un reloj accesible para la puerta.

Otros tipos de registros indiscutibles se pueden obtener haciendo que la puerta y la tarjeta contribuyan a la generación y/o autenticación de una entrada de registro. Por ejemplo, la tarjeta puede autenticar una entrada de registro y la puerta puede luego autenticar también al menos parte de la información de la entrada de registro y viceversa. En una forma de realización particular, una tarjeta C puede proporcionar a la puerta su firma, $x=SIG_C(E,AI)$, de la entrada de registro, que la puerta contrafirmará en símbolos, $SIG_D(x; AI')$ y viceversa. Como alternativa, la puerta y la tarjeta pueden calcular una firma digital conjunta de la información del evento (p.e., calculado por medio de una clave de firma secreta dividida entre la puerta y la tarjeta o combinando la firma de la puerta con la de la tarjeta en una “multifirma” única). Varios sistemas de multifirma se pueden utilizar en particular los de Micali, Ohta y Reyzin.

Es posible incluir información adicional en los registros. Se puede comprobar luego si la información que se comunica con la tarjeta y que se comunica con la puerta están de acuerdo. Por ejemplo, la tarjeta y la puerta pueden incluir información del tiempo en las entradas de registro, utilizando relojes disponibles al respecto. Además, la tarjeta (y posiblemente también la puerta) pueden incluir información de localización (tal como la obtenida de GPS) en la entrada de registro. Como alternativa, si la localización actual no está disponible (p.e., porque la capacidad de recepción del GPS está indisponible), la información sobre la más reciente localización conocida (y posiblemente cuánto tiempo hace de su establecimiento) pueden incluirse. De este modo, particularmente en el caso de una puerta móvil (tal como la puerta de un avión), puede ser posible establecer en dónde la puerta y la tarjeta estuvieron localizadas cuando se produjo el evento.

Por supuesto, incluso una entrada de registro indiscutible, como la anterior, puede ser malintencionadamente suprimida de la base de datos o impedido su alcance de la base de datos conjuntamente. Para proteger contra dichas supresiones, es de utilidad proporcionar sistemas de registro de supresión detectable. Dichos sistemas pueden construirse utilizando: (1) un sistema de autenticación (p.e., un sistema de firma digital), (2) un sistema de generación-correlación y (3) un sistema de detección-correlación como sigue. Dado un evento de registro E (parte de un secuencia de posiblemente eventos pasados y/o futuros), el sistema de generación-correlación se puede utilizar para generar información de correlación CI, que luego se vincula, con seguridad, a E por medio del sistema de generación-correlación que puede garantizar que, aun cuando los propios eventos no estén en correlación y la existencia de un evento no se puede deducir de la existencia de otros eventos, CI se genera de tal manera que garantice que para las entradas de registro no existentes, no se presente ninguna información adecuadamente correlacionada, lo que se puede detectar utilizando el sistema de detección-correlación. En algunos casos, el sistema puede garantizar, además, que aunque falten algunas entradas de registro, otras pueden ser garantizadas como auténticas/individualmente indiscutibles.

En un primer ejemplo, la información de correlación CI de las entradas de registro pueden incluir la numeración secuencial de dichas entradas de registro. El correspondiente sistema de detección-correlación puede consistir en notificar la presencia de una laguna operativa en la secuencia de numeración. No obstante, para tener un sistema de registro de supresión detectable, se encuentra un vínculo adecuado entre CI y las entradas de registro, que puede no ser fácil de realizar, aun cuando se utilicen firmas digitales seguras para la componente de autenticación del sistema. Por ejemplo, tener la i-éxima entrada de registro constituida por (i, SIG(evento, AI)), no es seguro, porque un intruso podría, después de suprimir una entrada de registro, modificar la numeración de entradas posteriores de modo que oculten dicha laguna operativa. En particular, después de suprimir el número de entrada de registro 100, el intruso puede disminuir en uno los números de entradas de registro 101, 102, etc. El intruso puede ocultar así sus supresiones porque, aun cuando la integridad de la información de eventos esté protegida por una firma digital, la propia numeración puede no estarlo. Además, incluso con la firma digital también los números pueden no funcionar adecuadamente. Por ejemplo, supóngase que la i-éxima entrada de registro consiste en (SIG(i),SIG(evento, AI)). En tal caso, un intruso podría: (1) observar y recordar SIG (100), (2) suprimir el número de entrada 100, (3) sustituir SIG (100) en lugar de SIG(101) en la entrada original 101, mientras que recuerda SIG(101), y así sucesivamente, de modo que oculte completamente la supresión.

Ninguno de los dos métodos anteriores produce el vínculo seguro deseado de CI y las entradas de registro. En realidad, al vincular, de forma segura, (1) la información de numeración junto con (2) el evento objeto de numeración, se quiere resaltar que un intruso no puede obtener el vínculo de algún número j junto con la información del evento sobre el i-éximo evento Ei, cuando j es diferente de i, aun cuando esté provisto de (a) un vínculo seguro de número i y Ei y (b) un vínculo

seguro de número j y Ej. Por ejemplo, la i-éxima entrada de registro puede consistir en SIG(i,Ei, AI). De este modo, la supresión de la i-éxima entrada de registro será detectada dadas las posteriores entradas de registro. Esto es así porque una posterior entrada de registro puede transmitir con ella un número mayor que i, que no se puede eliminar, modificar ni conmutar con otra información de numeración de entrada de registro por el intruso, porque está vinculada de forma segura con la entrada de registro. Por ejemplo, suponiendo que el intruso suprima el número de entrada de registro 100: SIG(100,E100,AI). En tanto que el intruso no pueda suprimir todas las entradas de registro posteriores (lo que podría exigir un acceso continuo a la base de datos), para ocultar su supresión, el intruso necesitaría crear otra entrada de registro con el mismo número 100. Sin embargo, esto puede ser difícil porque (a) el intruso no puede generar una nueva marca de 100-éxima entrada de registro SIG(100,E',AI') puesto que no tiene la clave de firma secreta de la puerta; (b) el intruso no puede modificar una entrada de registro existente sin invalidar la firma digital (p.e., no puede cambiar SIG(101,E101, AI101) en SIG(100, E101 ,AI101) aun cuando recuerde la entrada suprimida SIG(100,E100,AI100)); (c) el intruso no puede extraer una firma de una parte de la entrada de registro que indique el número 100 y la vincule con una firma digital para otra entrada de registro.

Dicha vinculación segura puede conseguirse también por medio de otras firmas digitales junto con el número de entrada y el evento objeto de numeración. Por ejemplo, se puede conseguir mediante una función-resumen *hashing* unidireccional del número de entrada y del evento que se numera y luego, firmar simbólicamente el *hash*, con SIG(H(i,Ei,AI)). A modo de otro ejemplo, se puede conseguir incluyendo la función *hash* del número en la firma digital del evento o viceversa: p.e., simbólicamente SIG(i,H(Ei),AI)). Se puede conseguir también con la firma de la información de numeración junto con la firma digital de la información del evento: p.e., simbólicamente SIG (i,SIG(Ei),AI)). En otra alternativa, se puede firmar por separado (1) la información de numeración junto con una cadena única x, y (2) la información del evento junto con la cadena x, simbólicamente (SIG(i,x), SIG(x,Ei,AI)). (Dicha cadena x podría ser un dato aleatorio denominado *nonce*).

Los registros de supresión detectables se pueden conseguir también mediante una vinculación segura con la información de correlación de entrada de registro que no sea la información de numeración secuencial. Por ejemplo, se puede incluir en la entrada de registro i alguna información de identificación desde una entrada de registro anterior, por ejemplo, la entrada i-1. Dicha información puede ser una función *hash* resistente a la colisión de entrada i-1 (o una parte de entrada de registro simbólicamente, la entrada de registro i se puede representar como SIG(H(entrada de registro i+1), Ei, AI). Entonces, si el intruso intenta eliminar la entrada de registro, dicha eliminación sería detectada cuando se reciba la entrada de registro i, porque la función *hash* de la entrada de registro anteriormente recibida, H (entrada de registro i-2), no coincidiría con H(entrada de registro i-1) (debido a la resistencia-colisión de H), mientras que H(entrada de registro i-1), puesto que está vinculado de forma segura a entrada registro-i, no podría modificarse por el intruso sin destruir la validez de una firma digital. En este caso, por entrada de registro i podemos significar también un subconjunto de su información, tal como Ei.

Conviene señalar que no se necesita la entrada de registro i-1 cuya información está vinculada con la entrada i: puede ser otra entrada anterior o futura o, de hecho, una multitud de otras entradas. Además, qué entradas de registro están vinculadas con las que se puede elegir con el uso de la aleatoriedad.

Se puede utilizar, asimismo, otra información de correlación. Por ejemplo, cada entrada de registro i puede haberse vinculado, de forma segura, con dos valores (p.e., valores aleatorios o *nonces*) xi y xi+1: simbólicamente, p.e., SIG(x_i, x_{i+1}, Ei, AI). Entonces, dos entradas de registro consecutivas pueden compartir siempre un solo valor x; por ejemplo, las entradas i y i+1 compartirán x_{i+1}. Sin embargo, si se suprime una entrada de registro, esta ya no se mantendrá (puesto que el intruso no puede modificar las entradas de registro firmadas sin detección, a no ser que conozca la clave secreta para la firma). Por ejemplo, si se suprime el número de entrada 100, la base de datos contendrá SIG(X_{gg}, x_{100}, E99, AI) y SIG(x_{101}, x_{102}, E101, AI) y se puede observar que no están compartiendo un valor x común. Dicha información de correlación puede adoptar otras formas: de hecho, una entrada de registro puede estar en correlación con otras múltiples entradas de registro. Esto se puede realizar, en particular, mediante el uso de polinomios para generar información de correlación (p.e., dos o más entradas de registro pueden contener cada una el resultado de evaluar el mismo polinomio en entradas diferentes). Dicha información de correlación puede hacer también uso de una cadena de funciones *hash*: por ejemplo, comenzando con un valor y_1, que permite y_2=H(y_1), y_3=H(y_2), … etc. y luego, vincular de forma segura y_i con Ei: p.e., la i-éxima entrada de registro se puede representar simbólicamente como SIG(y_i, Ei, AI). Entonces, entradas de registro consecutivas i y i+1 pueden tener valores de correlación y_i y y_{i+1} de modo que y_{i+1} = H(y_i). Si el intruso suprime una entrada de registro, sin embargo, ya no se puede mantener y en consecuencia, se puede detectar la supresión. Por ejemplo, si la entrada 100 está suprimida, la base de datos contendrá SIG(y_{99}, E99, AI) y SIG(y_{101}, E101; AI) (lo que, como antes, no se puede modificar por el intruso sin distorsionar las firmas digitales). Entonces, se puede detectar la supresión porque H(y_{101}) no coincidirá con y_{99}. El uso de múltiples cadenas de funciones-resumen *hash*, quizás entradas no consecutivas usadas y en ambas direcciones, puede proporcionar también dicha información de correlación.

En otra forma de realización, cada entrada de registro puede contener una indicación de alguno o la totalidad de los eventos anteriores o incluso posteriores, por lo que la realización de registros no solamente será con supresión detectable, sino también reconstruible en caso de supresiones. Los sistemas de registros reconstruibles se pueden construir utilizando: (1) un sistema de autenticación (p.e., un sistema de firma digital), (2) un sistema de generación de información-reconstrucción y (3) un sistema de reconstrucción como sigue. Dado un evento de registro E (parte de una secuencia de eventos posiblemente pasados y/o futuros), el sistema de generación de información-reconstrucción se

utiliza para generar información de reconstrucción RI, que luego se vincula, de forma segura, con otras entradas de registro por medio del sistema de autenticación. El sistema de generación de información-reconstrucción garantiza que, aun cuando se pierda la entrada de registro correspondiente al evento i, otras entradas de registro contienen información suficiente sobre E, por lo que permitirán la reconstrucción de E a partir de la información RI presente en otras entradas de registro. Por ejemplo, la i+1-éxima entrada puede contener información sobre la totalidad o algunos de los i eventos anteriores, que se genera por el sistema de generación de información-reconstrucción. Por lo tanto, si un intruso tuviere éxito en el borrado de la j-éxima entrada de registro desde la base de datos, la información sobre el j-éximo evento Ej se mostrará en una o más entradas posteriores, lo que posibilitará la reconstrucción de la información Ej incluso en la ausencia de la j-éxima entrada de registro, utilizando el sistema de reconstrucción. De este modo, no sería suficiente para un intruso tener acceso temporal a la base de datos: tendría que controlar la base de datos "en todo momento" y suprimir múltiples entradas de registro para impedir que se revele la información sobre el j-éximo evento. La elección de qué eventos incluir en una entrada de registro se puede realizar por el sistema de generación de información-reconstrucción en una forma aleatoria, lo que haría más difícil para un intruso predecir cuándo la información sobre un evento dado aparecerá en registros sucesivos. En una forma de realización preferida, el sistema para eventos reconstruibles puede ser también susceptible de detección de supresiones e indiscutible.

Conviene señalar, asimismo, que la información de reconstrucción sobre el evento j incluido en otra entrada de registro no necesita ser directa. Puede consistir en una entrada parcial j o su valor de función *hash* hj (en particular, calculado por el sistema de generación de información-reconstrucción por intermedio de una función *hash* resistente a la colisión/unidireccional), o de su firma digital o de cualquier otra indicación. En particular, si se utiliza una función *hash* H resistente a colisión/unidireccional, entonces será posible reestablecer, de forma indiscutible, información sobre el j-éximo evento a partir de una entrada de registro i que contenga hj: simbólicamente, si la i-éxima entrada está firmada, el registro indiscutible correspondiente puede adoptar la forma SIG(h_j, Ei, AI). Por ejemplo, si se sospecha que un usuario particular entró a través de una puerta particular en un momento particular, se puede comprobar si el valor hj coincide con el de la función *hash* H(Ej) de una entrada de registro Ej, que se hubiera creado en respuesta a dicho evento. Esto es indiscutible debido a la propiedad de resistencia a colisión de H: es esencialmente imposible la aparición de una entrada E'j diferente de Ej, tal que: H(E'j)=H(Ej).

Las entradas de registro Ej se pueden crear de tal modo que faciliten a alguien adivinar (y por lo tanto, verificar), lo que debería ser la entrada de registro para un evento dado (por ejemplo, utilizando un formato normalizado para las entradas de registro, empleando una granularidad temporal aproximada, etc.). Una función *hash* unidireccional puede ser de utilidad en particular debido a su pequeño tamaño: puede ser posible efectuar la función *hash* de numerosas o incluso todas las entradas de registro anteriores para su inclusión en una entrada posterior. Por ejemplo, la entrada i+1 puede incluir $h_1=H(E_1)$, $h_2=H(E_2)$,…. $h_i=H(E_i)$. Como alternativa, se puede efectuar el agrupamiento de (algunas de) las funciones *hash*, con lo que se reduce la cantidad de espacio necesario. Por ejemplo, si se agrupan en su totalidad, en tal caso, la segunda entrada de registro incluiría $h_1=H(E_1)$, la tercera entrada de registro incluiría $h_2 = H(E_2, h_1)$.....

De este modo, se puede reconstruir u observar las entradas de registro 1 a i-1 y la entrada de registro i+1, entonces se puede reconstruir, de forma indiscutible, la entrada de registro i. Este sistema se puede mejorar mediante la encriptación de (parte de) la información en una entrada de registro (p.e., con una clave conocida solamente para la base de datos), de modo que el intruso no pueda conocer qué información debe destruir para poner en compromiso la posibilidad de reconstrucción de un evento particular: en realidad, una vez que el registro esté protegido mediante encriptación, dichos registros encriptados (preferentemente registros encriptados indiscutibles) se pueden remitir a otra (segunda) base de datos sin ninguna pérdida de privacidad. Esto hace que las supresiones se hagan todavía más difíciles para un intruso: ahora tiene que obtener acceso a dos o más bases de datos para falsificar registros .

Los registros reconstruibles se pueden conseguir también mediante el uso de códigos correctores de errores. En particular, esto se puede realizar generando múltiples componentes ("participaciones") de cada entrada de registro y procediendo a su envío por separado (quizás con otras entradas de registro) de tal manera que, cuando se haya recibido una cantidad suficiente de participaciones, la entrada de registro se puede reconstruir mediante el sistema de reconstrucción, lo que puede invocar un algoritmo de decodificación para el código corrector de errores. Estas participaciones se pueden dispersar de forma aleatorio o seudoaleatoria, lo que hace todavía más difícil para el intruso eliminar una cantidad de ella suficiente para impedir la reconstrucción de una entrada de registro cuando lleguen ocasionalmente participaciones suficientes.

Los registros de eventos (creados por tarjetas, por puertas o conjuntamente por ambas) se pueden transmitir por tarjetas para facilitar su recogida. Cuando una tarjeta alcanza una puerta conectada, o se comunica con un servidor central o de cualquier otro modo, es capaz de comunicarse con la base de datos central, puede enviar los registros que memoriza. Esta operación se puede realizar, de forma similar, para la difusión de HRAs, con la excepción de que se pueden enviar HRAs desde un punto central a una tarjeta, mientras que los registros se pueden enviar desde la tarjeta al punto central. Todos los métodos de difusión de HRA, por lo tanto, se aplican a la recogida de registros de eventos. Más concretamente, un método para difundir HRAs se puede transformar en un método para la recogida de registros de eventos (1) sustituyendo un remitente por el receptor y viceversa; (2) sustituyendo un HRA con una entrada de registro.

En particular, una tarjeta C1 puede recoger registros de eventos para los eventos no relacionados con C1, tal como el acceso por otra tarjeta C2, o un funcionamiento anómalo de una puerta D. Además, los registros de eventos para una

puerta D1 se pueden memorizar (quizás temporalmente) en otra puerta D2 (quizás transmitido por una tarjeta C1). Entonces, cuando otra tarjeta C2 esté en comunicación con D2, puede recibir algunas de estas entradas de registro y más adelante, comunicarlas a otra puerta o a una posición central. Esta amplia difusión puede garantizar que los registros de eventos alcancen, con mayor rapidez, el punto central. (Además, es posible que algunas puertas, aun cuando no estén completamente conectadas a una base de datos central, puedan tener conexiones entre sí. Dichas puertas, de este modo, pueden intercambiar registros de eventos disponibles en una forma similar. Si las tarjetas tienen una capacidad de comunicación entre sí - p.e., cuando estén en proximidad – pueden también intercambiar información sobre los registros de eventos que memorizan). En dicho proceso de recogida, los registros indiscutibles son ventajosos, puesto que no necesitan transmitirse a través de canales asegurados, habida cuenta que no se pueden falsificar. Por lo tanto, no necesitan confiar en la seguridad de las tarjetas o conexiones entre tarjetas y puertas. Los registros con supresiones detectables proporcionan ventajas adicionales al garantizar que, si algunas entradas de registro no son recogidas (quizás porque algunas tarjetas nunca alcanzan una puerta conectada), este hecho se puede detectar. Los registros reconstruibles pueden permitir, además, la reconstrucción de entradas de registro en caso de algunas entradas de registro no alcancen una base de datos central (de nuevo, quizás porque algunas tarjetas nunca alcanzan una puerta conectada).

En algunos casos, todos los registros de eventos se podrían memorizar y difundir de esta manera. De no ser así, puede ser de utilidad adoptar algunas optimizaciones. Un método de optimización consiste en hacer que los registros de eventos lleguen provistos de información de prioridad, indicando así la importancia relativa de informar a una autoridad central sobre un evento particular. Algunas entradas de registro pueden ser de interés más urgente que otras: Por ejemplo, si una puerta está fijada en una posición abierta o cerrada, si se intenta un acceso no autorizado o si se detecta un modelo de acceso inusual. Con el fin de acelerar la entrega de dicha información importante al lugar en donde pueda actuar, la información en los registros de acceso puede proveerse de etiquetas que indiquen su importancia (o su importancia se puede deducir de la propia información). Por ejemplo, algunas entradas de registro se pueden etiquetar “urgente” mientas que otras se pueden etiquetar de “rutina” o bien, se pueden etiquetar por números o palabras de código, que indiquen su grado de importancia. (Una gradación de las prioridades puede ser tan fina o aproximada según sea apropiado), más esfuerzo o más alta prioridad se puede dedicar a difundir información de la mayor importancia. Por ejemplo, se puede otorgar más alta prioridad en la información para más tarjetas y/o puertas con el fin de aumentar la probabilidad de que alcancen su destino con mayor prontitud o seguridad. Además, una tarjeta o una puerta, cuando reciban información de alta prioridad, pueden dedicar espacio para ella eliminando la información de baja prioridad desde su memoria. De forma similar, una puerta puede decidir dar información de alta prioridad a cada tarjeta que pase por ella, mientras que puede proporcionar información de baja prioridad a solamente unas pocas tarjetas o puede esperar hasta el momento en que la puerta esté conectada.

Como alternativa, o en adición a las técnicas anteriores, se pueden seleccionar tarjetas para memorizar entradas de registro particulares de tal modo que implique una aleatoriedad o bien, una puerta puede proporcionar una entrada de registro a determinado número de tarjetas (p.e., las primeras k tarjetas que “encuentra”). El uso de dichas técnicas de difusión puede reducir, en gran medida, la probabilidad de que una entrada importante, en un registro de eventos, fuere incapaz de alcanzar el punto central en donde pueda actuar. En particular, se puede utilizar como una contramedida eficaz contra ataques “obstaculizantes” que intenten evitar que una puerta rota comunique dicha circunstancia. El método real de intercambio de los registros entre tarjetas y puertas puede variar según las circunstancias. En caso de unas pocas entradas, puede ser más eficaz intercambiar y comparar todas las entradas conocidas. En otros casos, pueden ser apropiados algoritmos más sofisticados para encontrar y reconciliar las diferencias.

Puede ser de utilidad presentar, en detalle, algunas formas muestras en las que se pueden recoger los registros de eventos. A continuación, el término de “autoridad” A incluye algún punto central o base de datos en donde se recogen registros de eventos.

SECUENCIA 1 (directamente desde la puerta a la autoridad):

1. La puerta conectada D crea una entrada de registro E indiscutible, en respuesta un evento.

2. La entrada de registro E se transmite, mediante combinación cableada o inalámbrica, a la autoridad A.

3. La autoridad A verifica la autenticidad de E y, si la verificación tiene éxito, memoriza E.

SECUENCIA 2 (desde la puerta a una tarjeta de usuario y a la autoridad):

1. La puerta D crea una entrada de registro E indiscutible en respuesta a un evento.

2. Una tarjeta C de un usuario U, que se presenta para acceso a la puerta D, recibe y memoriza E (en adición a la comunicación relacionada con el acceso). La tarjeta puede verificar, o no, la autenticidad de E.

3. Cuando el usuario U deja su trabajo y presenta su tarjeta a A al final del día laboral, E se transmite a A por intermedio de la tarjeta.

4. A verifica la autenticidad de E y, si la verificación es positiva, memoriza E.

SECUENCIA 3 (desde la puerta a una tarjeta de usuario para otra puerta (conectada) a la autoridad):

1. La puerta D crea una entrada de registro E indiscutible, en respuesta un evento.

2. Una tarjeta C de un usuario U, que se presenta para acceso a la puerta D, recibe y memoriza E (en adición a la comunicación relacionada con el acceso). La tarjeta puede verificar, o no, la autenticidad de E.

3. Más adelante, el usuario U presenta su tarjeta C para acceso a otra puerta (conectada) de D'. La puerta D', además de verificar las credenciales y conceder acceso, si es apropiado, recibe E desde C. La puerta D' puede verificar, o no, la autenticidad de E.

4. E se transmite por la puerta D' por intermedio de una combinación cableada o inalámbrica a la autoridad A.

5. A verifica la autenticidad de E y, si la verificación es positiva, memoriza E.

Las zonas protegidas se pueden definir por paredes y puertas físicas, tales como puertas a través de las cuales puede entrar una persona o puertas de un contenedor, de una caja de seguridad, de un vehículo, etc. Las zonas protegidas se pueden definir también por puertas y paredes virtuales. Por ejemplo, una zona se puede proteger por un detector que pueda detectar una intrusión y posiblemente, hacer sonar una alarma o enviar otra señal si no se proporciona la autorización correspondiente. Dicho sistema de alarma es un ejemplo de una puerta virtual: en un aeropuerto, se suele penetrar en la zona de puertas a través de un pasillo de salida lo que disparará dicha alarma, aun cuando no se haya violado ninguna puerta o pared física. Otro ejemplo de una puerta virtual es una cabina de peaje: aun cuando muchas cabinas de peaje no contengan barras o puertas físicas, un vehículo dado puede estar autorizado, o no, para pasar a través de la cabina. Dicha autorización puede depender, por ejemplo, de la validez de una ficha de pago de peaje electrónica de un vehículo. Otro ejemplo es el de una zona de control de tráfico. Por ejemplo, para entrar en los suburbios de una ciudad dada, o en una carretera que conduce a una instalación nuclear, una barrera del ejército u otra área sensible, un vehículo deberá tener una autorización adecuada, para fines tales como facturación, seguridad o control de congestión del tráfico.

Además, una protección puede no ser necesaria solamente para zonas, sino también para dispositivos, tales como motores de aeronaves o equipos militares. Por ejemplo, puede ser necesario para garantizar que solamente una persona autorizada pueda arrancar los motores de una aeronave o de un vehículo que transporta materias peligrosos.

Existen numerosas maneras de utilizar credenciales/pruebas para control del acceso. Conviene señalar que, en estos ámbitos, el término "día" debe entenderse como significando un periodo de tiempo general en una secuencia de periodos de tiempo y el término de "mañana" significa el comienzo de un periodo de tiempo.

A través de toda esta solicitud de patente el término de "puertas" debe interpretarse como incluyendo todos los tipos de zonas de acceso (p.e., físicas y/o virtuales), dispositivos/sistemas de control de acceso y dispositivos/sistemas de supervisión. En particular, incluyen los mecanismos bajo llave utilizados para el arranque de motores y equipo de control (por lo que nuestra invención, en particular, se puede utilizar para garantizar que solamente usuarios con autorización actual puedan poner en marcha una aeronave, accionar una excavadora o de cualquier otro modo, acceder y controlar varios objetos peligrosos y/o de valor, así como dispositivos y elementos de maquinaría). De forma coherente con este convenio, nos referiremos a la "entrada" como siendo concedida para el acceso deseado (físico o virtual).

De forma similar, para mayor concreción, pero sin pérdida de generalidad prevista, una tarjeta puede entenderse que significa cualquier dispositivo de acceso de un usuario. Ha de entenderse que la noción de una tarjeta es suficientemente general para incluir a los teléfonos móviles, PDAs y otros dispositivos inalámbricos y/o de tecnología avanzada y una tarjeta puede incluir o actuar en conjunción con otras medidas de seguridad, tales como números PINs, contraseñas y biométrica, aunque algunos de ellos puedan “residir” en el cerebro o cuerpo del titular y no en la propia tarjeta.

Además, la expresión "usuario" (que suele referirse como "él" o "ella"), en términos amplios, puede entenderse que abarca no solamente a los usuarios y personas, sino también a dispositivos, entidades (y conjuntos de usuarios, dispositivos y entidades) incluyendo, sin limitación, las tarjetas de usuarios.

El sistema aquí descrito se puede poner en práctica utilizando cualquier combinación adecuada de hardware y software incluyendo, sin limitación, el software memorizado en un soporte legible por ordenador al que se accede por uno o más procesadores. Además, las técnicas utilizadas para las operaciones de encriptación, autenticación, etc. se pueden combinar y utilizar de forma intercambiable, cuando sea conveniente.

REIVINDICACIONES

1. Un método de control de acceso, que comprende:

la utilización de una barrera de acceso provista de un controlador que permite un acceso selectivo;

al menos una entidad de administración que genera credenciales de identidad y pruebas de identidad, en donde las credenciales incluyen un valor final y una fecha, en donde el valor final se obtiene aplicando, varias veces, una función unidireccional a un valor aleatorio, estando cada una de las pruebas asociada con un intervalo de tiempo particular, en donde se obtiene diferentes pruebas aplicando la función unidireccional al valor aleatorio, en un número diferente de veces, en donde una prueba que ha de presentarse al controlador en un momento determinado, es el resultado de aplicar la función unidireccional a una prueba a presentarse al controlador en el futuro;

el controlador recibe la credencial de identidad de al menos una de las pruebas correspondientes a la tentativa de acceso realizada por un usuario;

en respuesta a la tentativa de acceso por el usuario, el controlador determina si el acceso está actualmente autorizado aplicando la función unidireccional a por lo menos una de las pruebas, un determinado número de veces y comparando el resultado con el valor final, correspondiendo el número de veces a una duración de tiempo transcurrido desde la fecha asociada con las credenciales y

si el acceso está actualmente autorizado, el controlador autoriza el acceso.

2. Un método según la reivindicación 1, en donde las credenciales y las pruebas de identidad son una sola parte.

3. Un método según la reivindicación 1, en donde las credenciales y pruebas son partes distintas.

4. Un método según la reivindicación 3, en donde existe una primera entidad de administración que genera las credenciales y otras entidades de administración que generan las pruebas de identidad.

5. Un método según la reivindicación 4, en donde la primera entidad de administración genera también pruebas de identidad.

6. Un método según la reivindicación 4, en donde la primera entidad de administración no genera pruebas.

7. Un método según la reivindicación 1, en donde las credenciales corresponden a un certificado digital.

8. Un método según la reivindicación 7, en donde el certificado digital incluye un identificador para el dispositivo electrónico.

9. Un método según la reivindicación 1, en donde las credenciales incluyen un identificador para un usuario que solicita acceso.

10. Un método según la reivindicación 1, en donde las credenciales/pruebas de identidad incluyen una firma digital.

11. Un método según la reivindicación 1, en donde la barrera de acceso incluye paredes y una puerta.

12. Un método según la reivindicación 11, que comprende, además:

una cerradura de puerta acoplada al controlador, en donde el controlador, que permite el acceso, incluye el controlador que acciona la cerradura de la puerta para permitir la apertura de dicha puerta.

13. Un método según la reivindicación 1 que comprende, además:

proporcionar un lector acoplado al controlador, en donde el controlador recibe credenciales/pruebas desde el lector.

14. Un método según la reivindicación 13, en donde las credenciales/pruebas se proporcionan en una tarjeta inteligente presentada por un usuario.

15. Un método según la reivindicación 1 que comprende, además:

proporcionar una conexión externa al controlador.

16. Un método según la reivindicación 15, en donde la conexión externa es intermitente.

17. Un método según la reivindicación 15, en donde el controlador recibe al menos una parte de las credenciales/pruebas de identidad utilizando la conexión externa.

18. Un método según la reivindicación 17, en donde el controlador recibe la totalidad de las credenciales/pruebas de identidad utilizando la conexión externa.

19. Un método, según la reivindicación 17, que comprende, además:

proporcionar un lector acoplado al controlador, en donde el controlador recibe una parte remanente de las credenciales/pruebas de identidad desde el lector.

20. Un método, según la reivindicación 19, en donde las credenciales/pruebas de identidad se proporcionan en una tarjeta inteligente presentada por un usuario.

21. Un método, según la reivindicación 1, en donde las credenciales/pruebas de identidad incluyen una contraseña introducida por un usuario.

22. Un método según la reivindicación 1, en donde las credenciales/pruebas de identidad incluyen información biométrica del usuario.

23. Un método, según la reivindicación 1, en donde las credenciales/pruebas de identidad incluyen una firma manuscrita.

24. Un método según la reivindicación 1, en donde las credenciales/pruebas de identidad incluyen un valor secreto proporcionado en una tarjeta mantenida por un usuario.

25. Un método según la reivindicación 1, en donde las credenciales/pruebas de identidad caducan en un instante predeterminado.

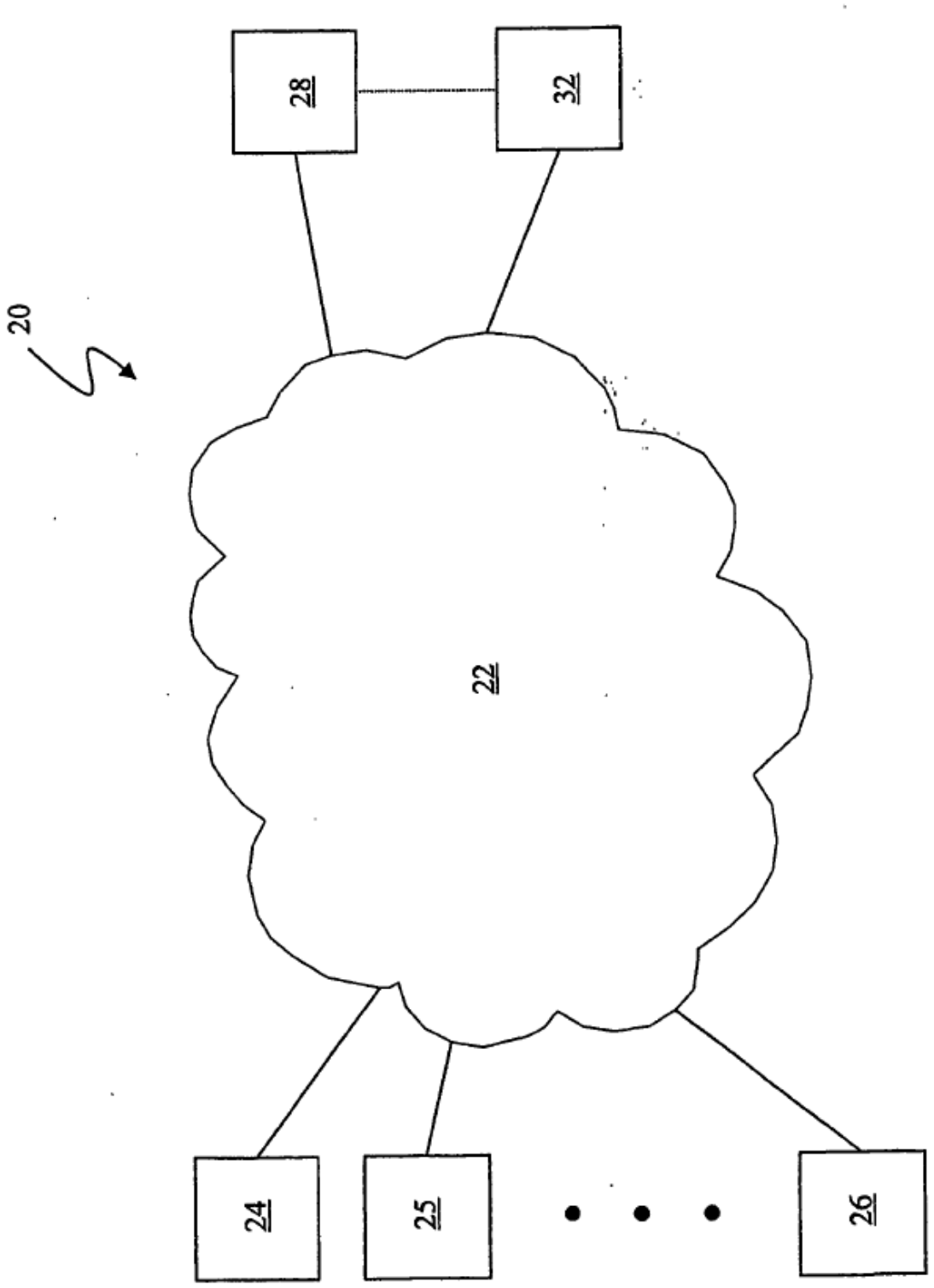

Figura 1A

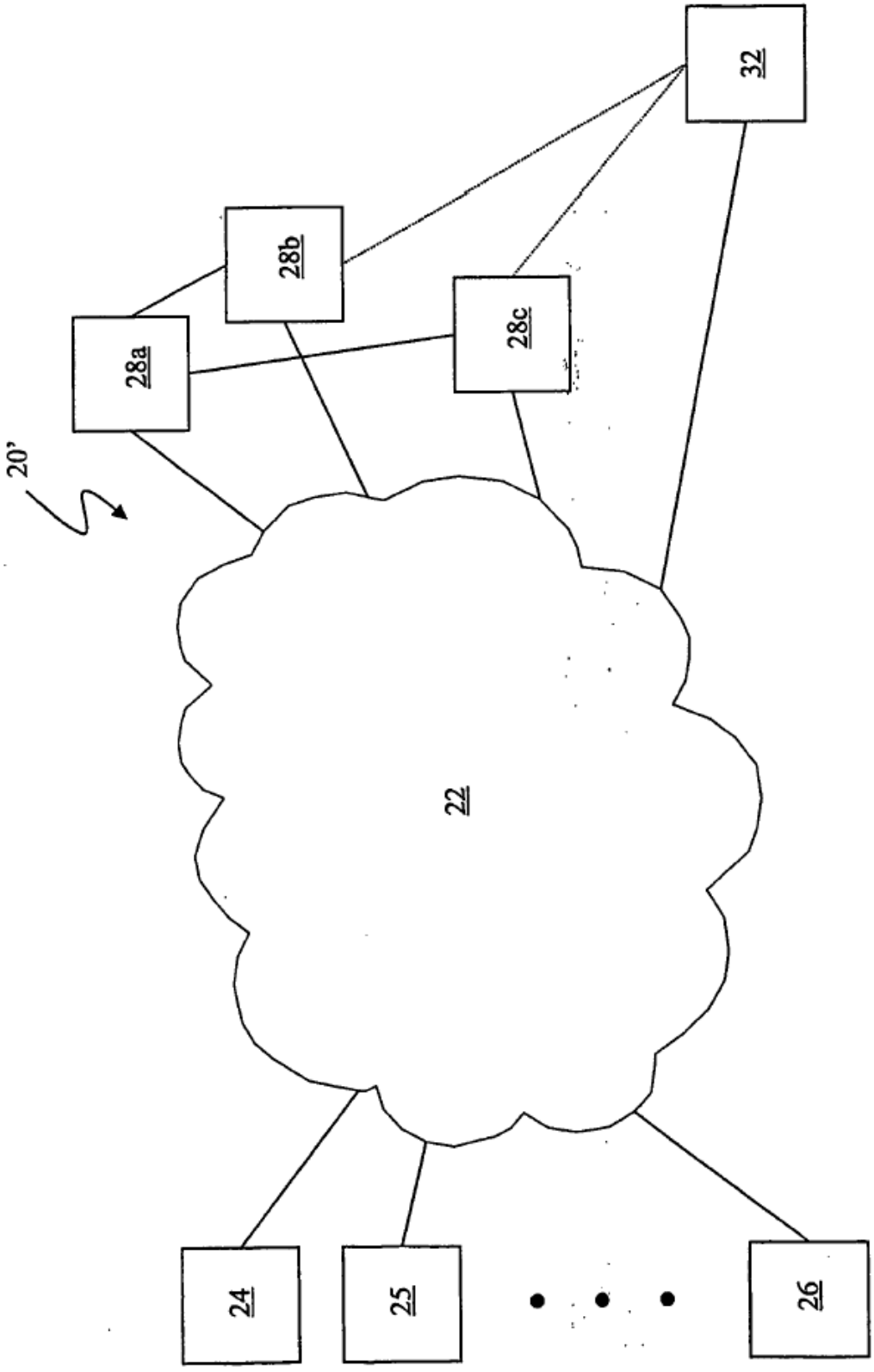

Figura 1B

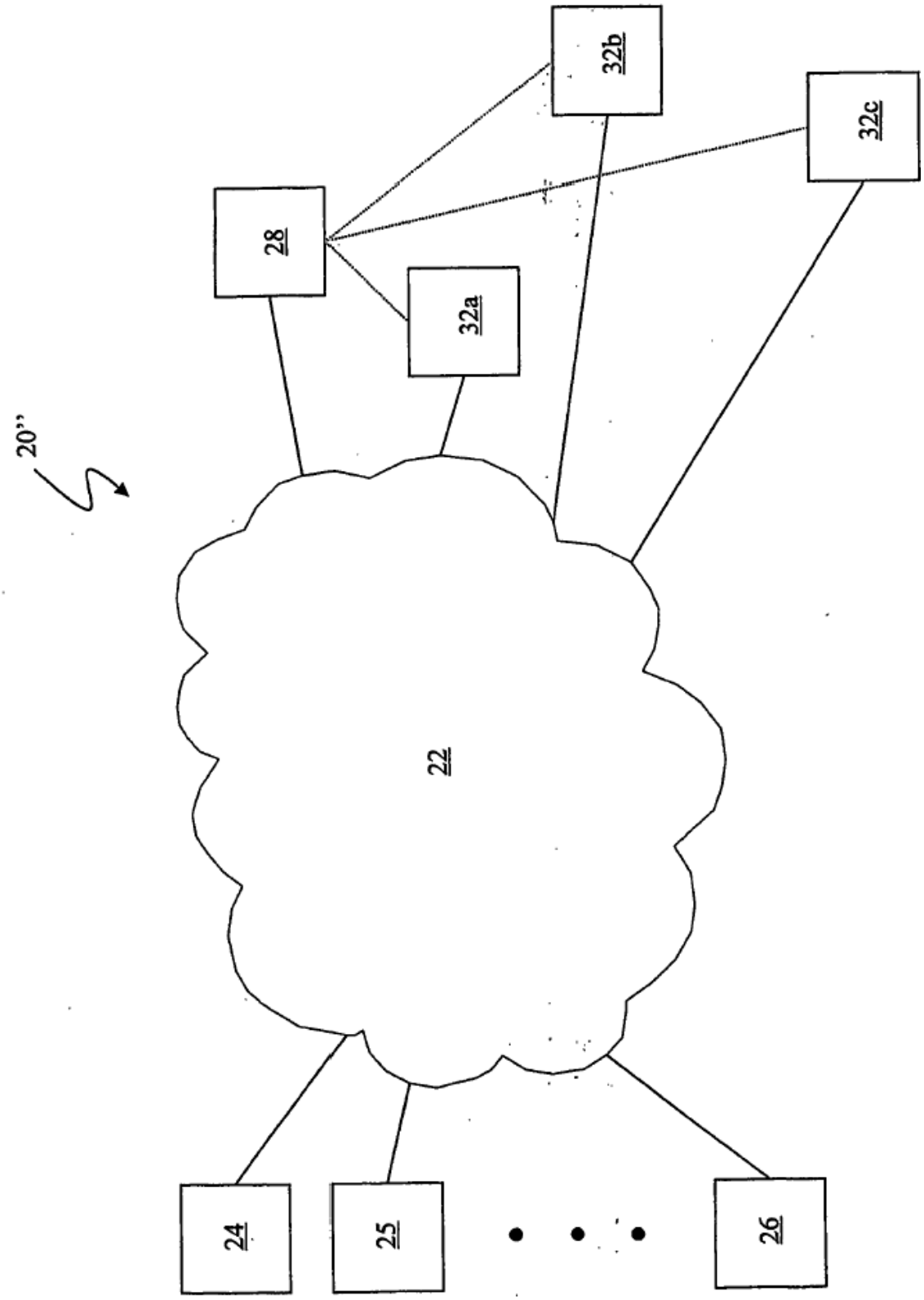

Figura 1C

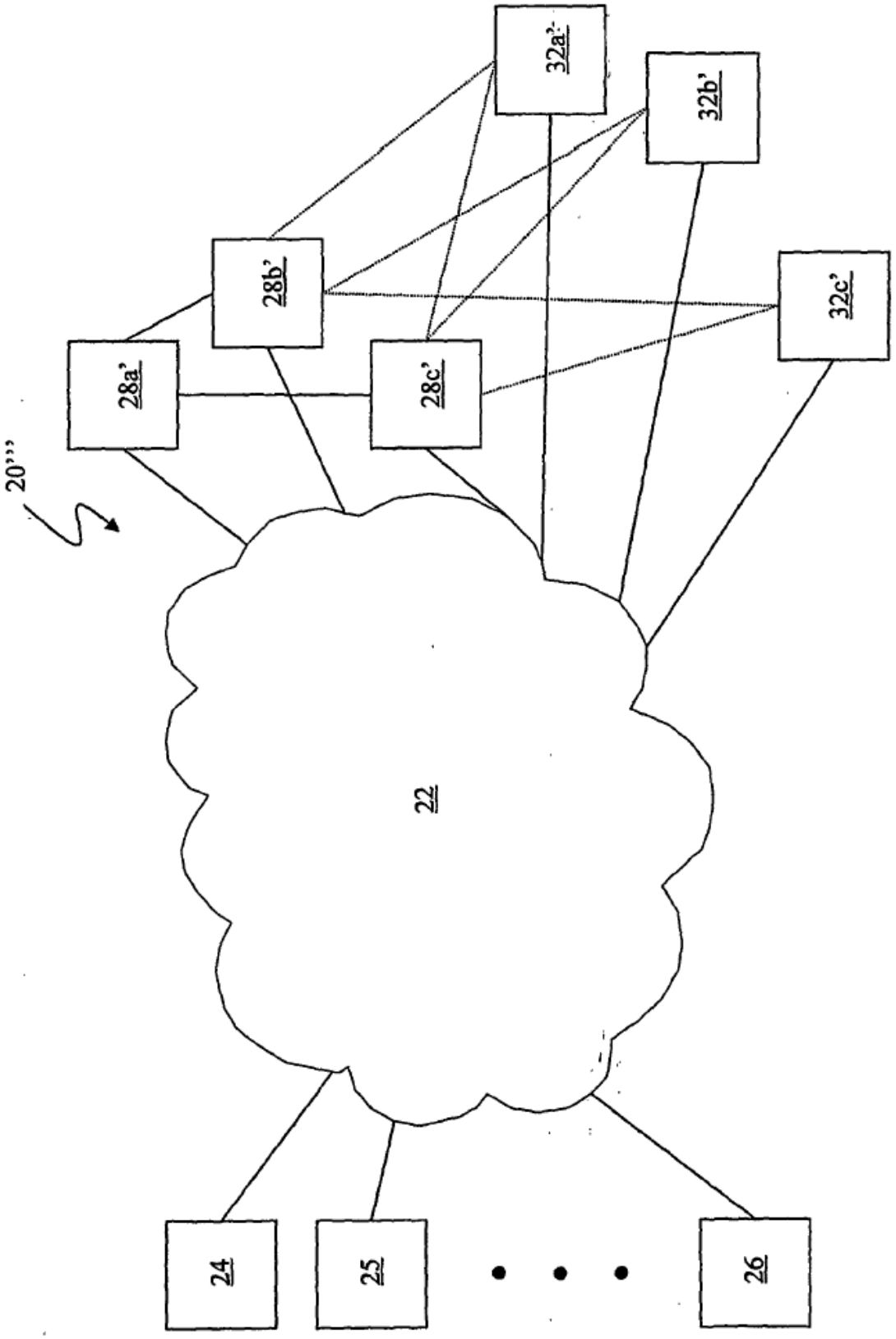

Figura 1D

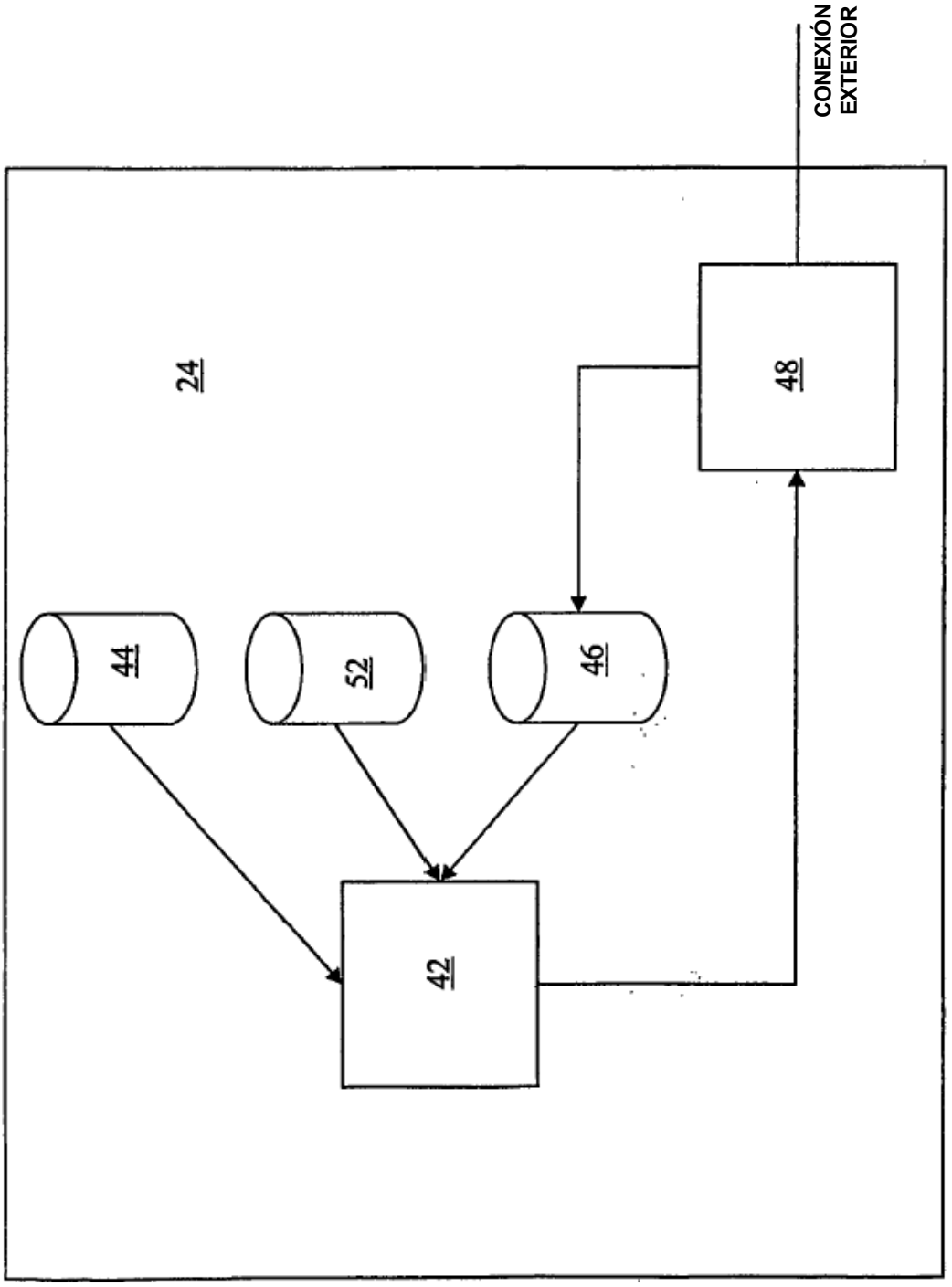

Figura 2

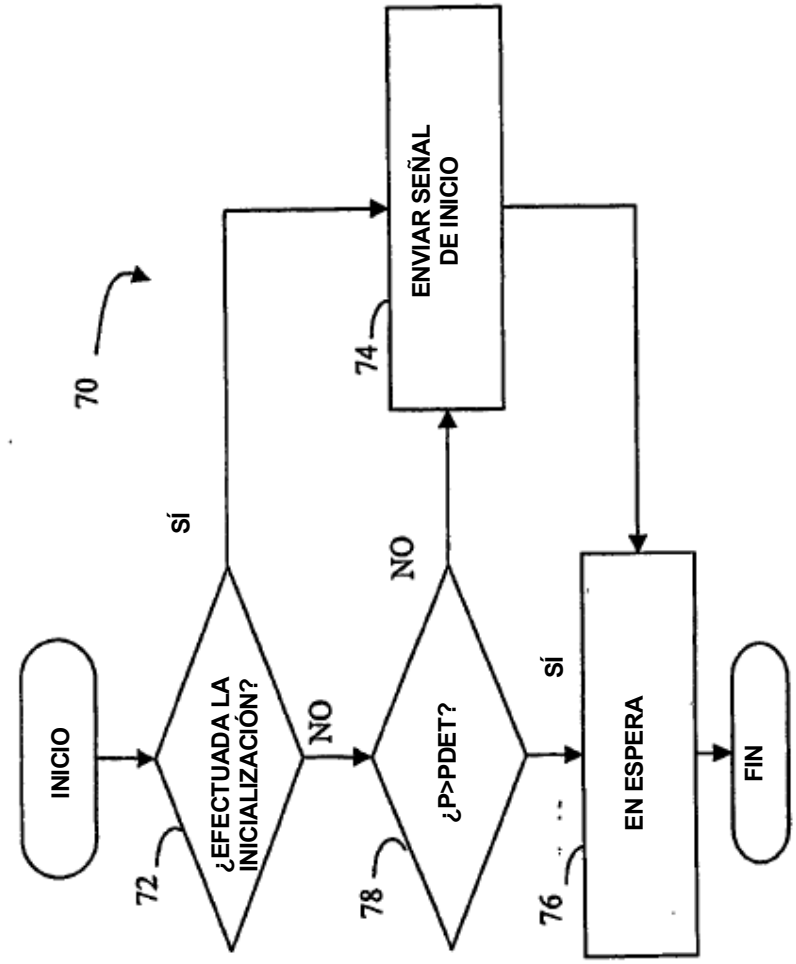
70
INICIO
¿EFECTUADA LA INICIALIZACIÓN?
72
sí
NO
ENVIAR SEÑAL DE INICIO
74
¿P>PDET?
78
NO
sí
EN ESPERA
76
FIN

Figura 3

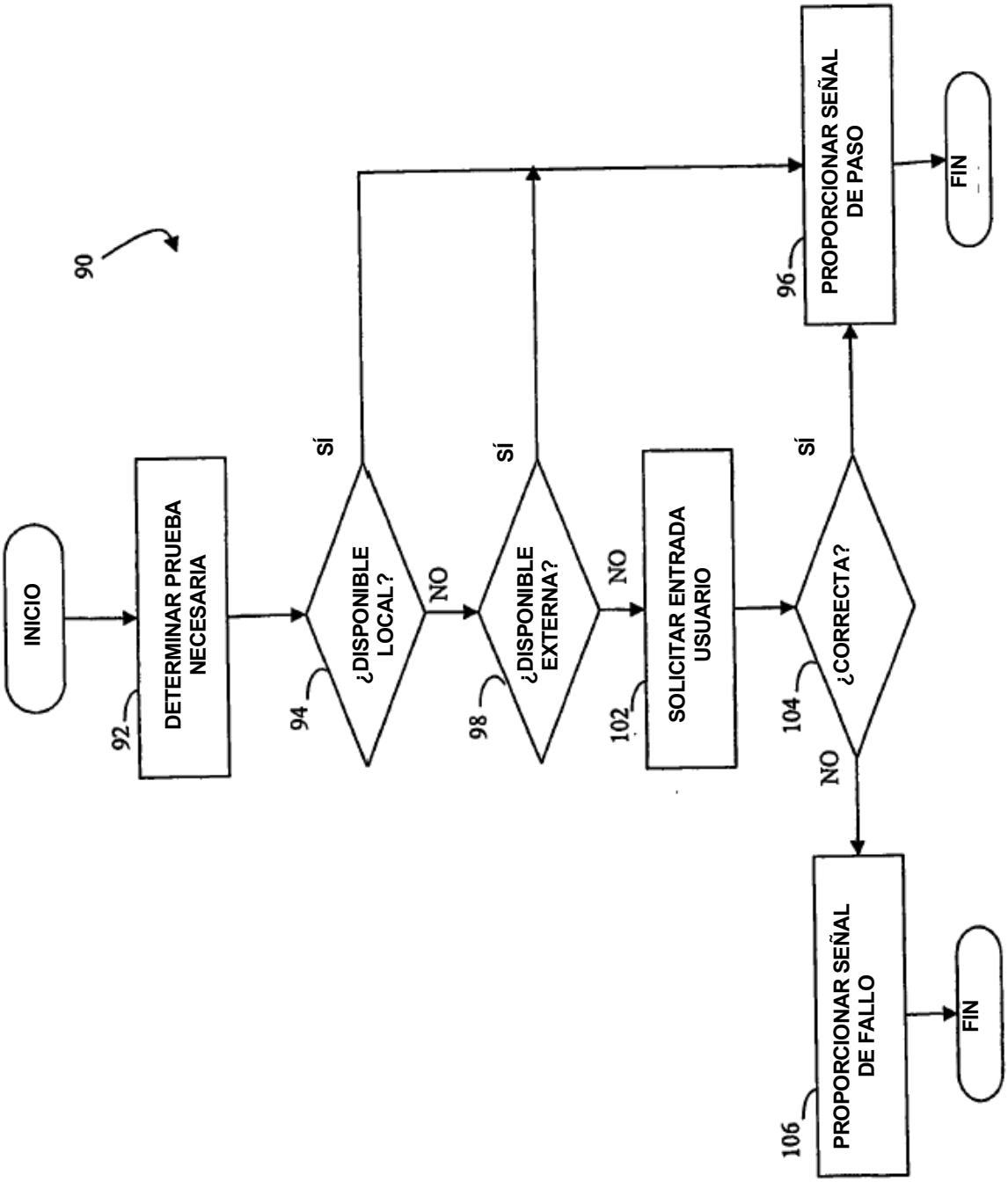
90
INICIO
DETERMINAR PRUEBA NECESARIA
92
¿DISPONIBLE LOCAL?
94
SÍ
NO
¿DISPONIBLE EXTERNA?
98
SÍ
NO
SOLICITAR ENTRADA USUARIO
102
¿CORRECTA?
104
SÍ
NO
PROPORCIONAR SEÑAL DE PASO
96
FIN
PROPORCIONAR SEÑAL DE FALLO
106
FIN

Figura 4

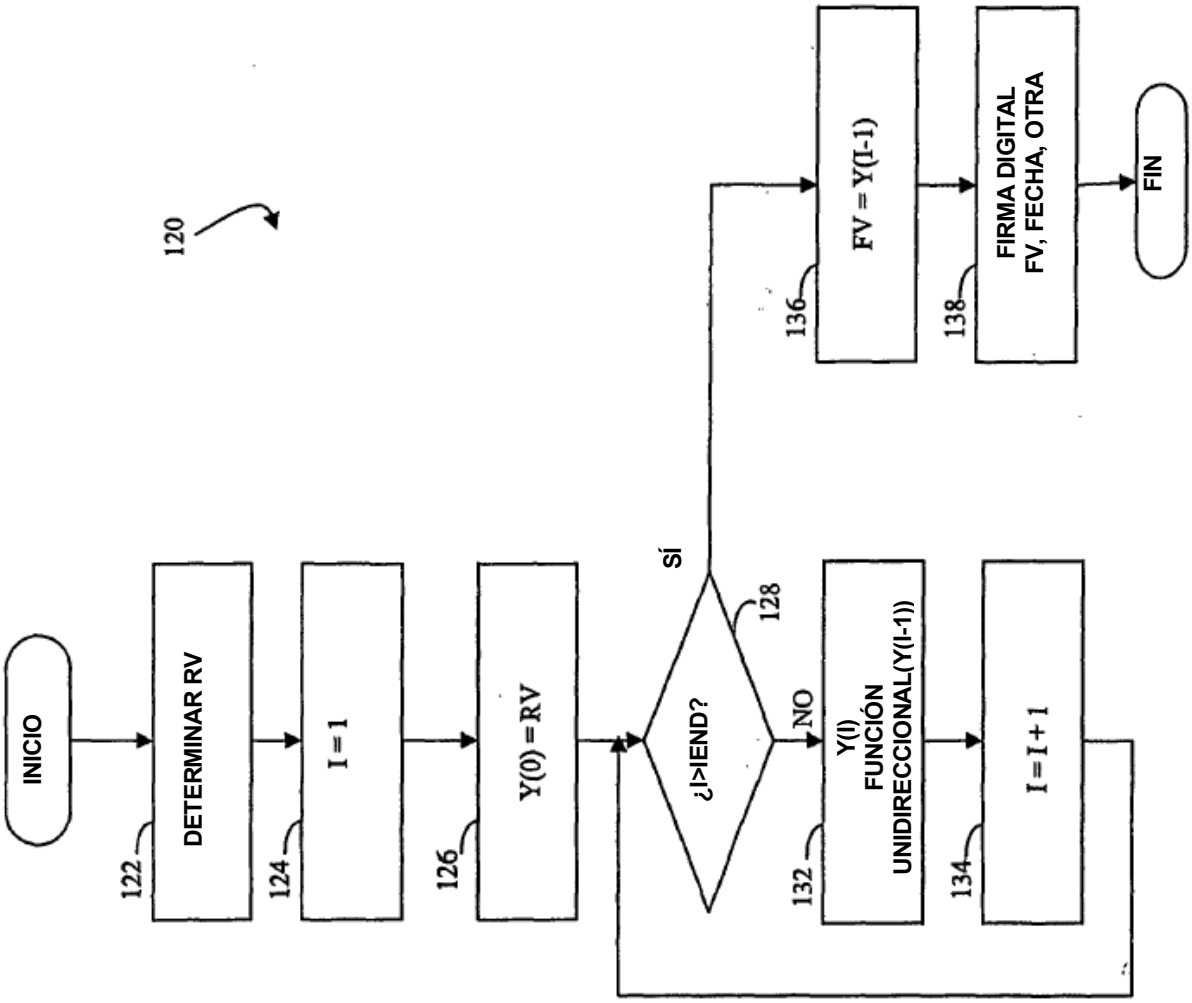
120
INICIO
DETERMINAR RV
122
I = 1
124
Y(0) = RV
126
¿I>IEND?
128
SÍ
NO
Y(I) FUNCIÓN UNIDIRECCIONAL(Y(I-1))
132
I = I + 1
134
FV = Y(I-1)
136
FIRMA DIGITAL FV, FECHA, OTRA
138
FIN

Figura 5

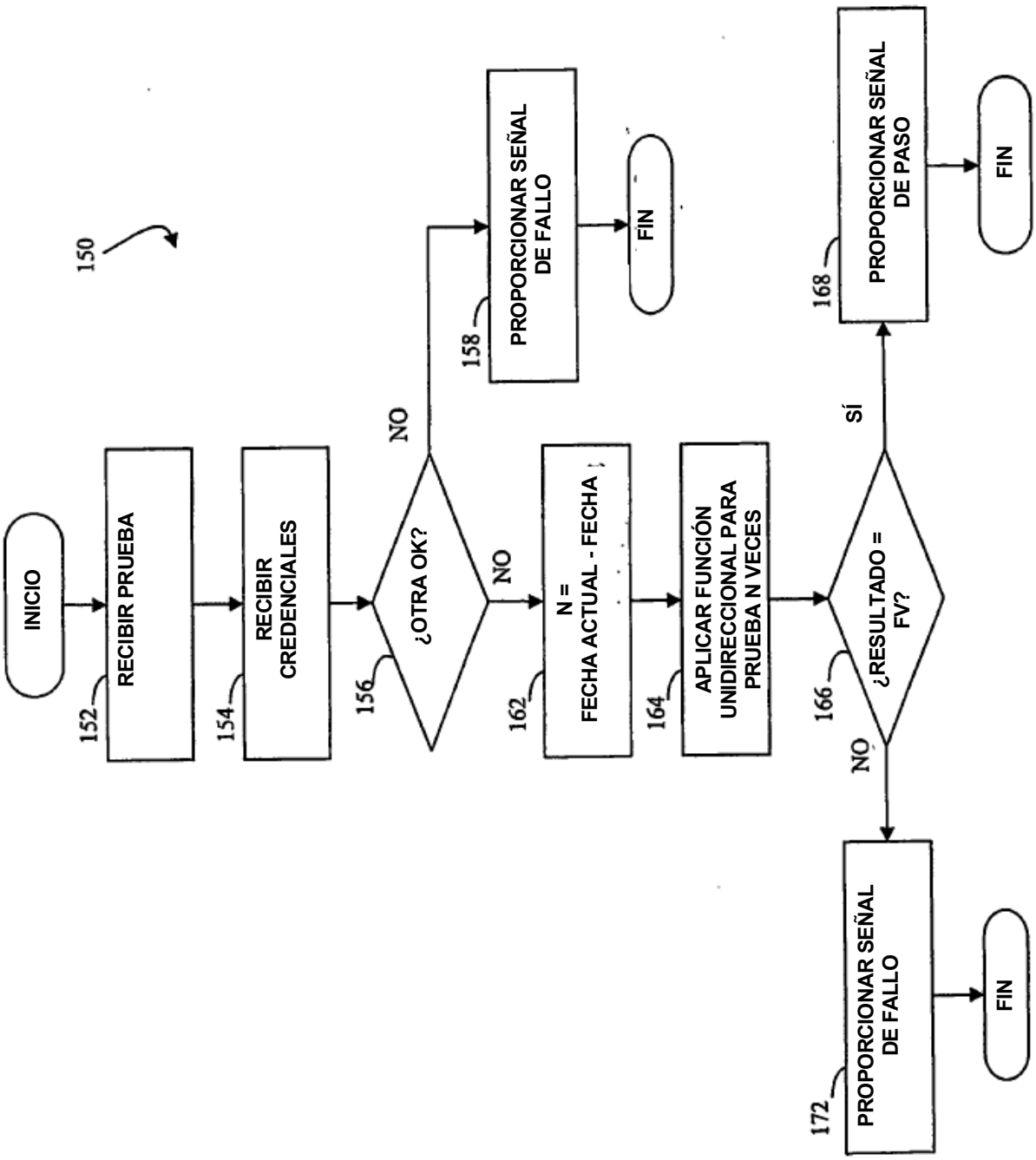
150
INICIO
RECIBIR PRUEBA
152
RECIBIR CREDENCIALES
154
¿OTRA OK?
156
NO
PROPORCIONAR SEÑAL DE FALLO
158
FIN
NO
N = FECHA ACTUAL - FECHA
162
APLICAR FUNCIÓN UNIDIRECCIONAL PARA PRUEBA N VECES
164
¿RESULTADO = FV?
166
SÍ
PROPORCIONAR SEÑAL DE PASO
168
FIN
NO
PROPORCIONAR SEÑAL DE FALLO
172
FIN

Figura 6

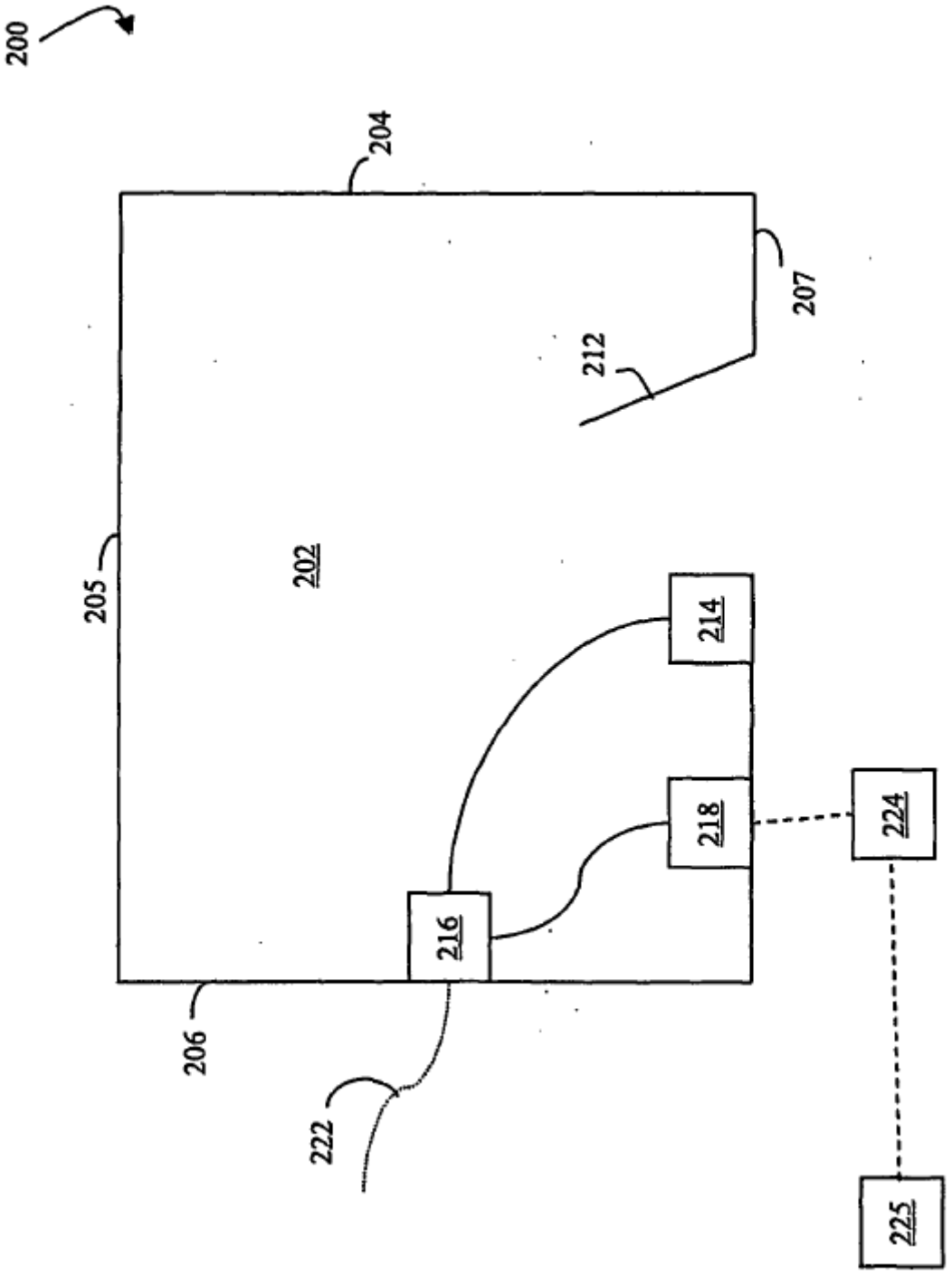

Figura 7