(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 648 117**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06Q 20/20 (2012.01)
G06Q 20/32 (2012.01)
G06Q 20/40 (2012.01)
G06F 21/62 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **09.01.2015 PCT/EP2015/050354**

(87) Fecha y número de publicación internacional: **16.07.2015 WO15104387**

(96) Fecha de presentación y número de la solicitud europea: **09.01.2015 E 15700285 (8)**

(97) Fecha y número de publicación de la concesión europea: **08.11.2017 EP 3092774**

(54) Título: **Sistema y método para comunicar credenciales**

(30) Prioridad:

10.01.2014 EP 14150856

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.12.2017

(73) Titular/es:

PRIVITI PTE. LTD. (100.0%)
Level 24, Suite 03-36 31 Rochester Drive
Singapore 138637, SG

(72) Inventor/es:

BARRY, GERARD y
BARRY, DECLAN

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Sistema y método para comunicar credenciales

Campo de la invención

La presente invención pertenece al campo de las tecnologías de la información y las comunicaciones, la privacidad de intercambio de datos confiada a las tecnologías de la información y las comunicaciones, así como la preservación y protección de la privacidad que prevalece en credenciales comunicadas con las tecnologías de la información y las comunicaciones. Privacidad se refiere a la posesión de o participación en cualquier información que pertenece a una entidad, o cualquier conjunto de credenciales que conectan una entidad y cualquier individuo particular. En particular, la presente invención se ocupa de, pero no se limita a liberación permitida de datos que comprenden conjuntos de detalles personales privados y credenciales controladas que una parte a quien pertenece el conjunto de credenciales, puede desear consentir y permitir haber liberado confidencialmente de una manera protegida y segura mientras que se asegura la conservación y mantenimiento en curso de la confidencialidad y privacidad de los detalles personales y credenciales controladas para una variedad de propósitos. Credenciales controladas se refieren a tal información que conecta al propietario/emisor de las credenciales controladas y al tenedor/poseedor de las credenciales controladas.

Antecedentes de la invención

En una sociedad moderna, los individuos están asociados con una vasta agrupación de datos personales. Algunos ejemplos de tales datos personales incluyen pero no están limitados a nombre, dirección, fecha de nacimiento, nacionalidad, número de la seguridad social, número de pasaporte, número de carnet de conducir, número de afiliación (para una organización dada), nombre de soltera (si es aplicable), nombre de soltera de la madre, información de empleado, número de cuenta bancaria, número de tarjeta de crédito, etc. Estos datos personales se usan de una multitud de formas como y cuando los individuos interactúan con otros individuos y organizaciones. Muchos de estas interacciones dependen fuertemente de la exactitud de un conjunto de datos que son tanto particulares para el individuo como necesarios para la interacción en cuestión. Por consiguiente, debido a que cada uno de tal conjunto de datos (en lo sucesivo conocidos como “conjunto de credenciales”) es tanto particular para un individuo como necesario para la interacción, es información sensible que se retiene deseablemente en un estado de privacidad. La información son datos relevantes adicionales sensibles (y deseablemente conservados en un estado de privacidad), tales como datos que pertenecen a rasgos de seguridad adicionales, por ejemplo, un código clave secreto asociado con un instrumento dado. Se entenderá que incluso si se pretende liberar un conjunto de credenciales de un registro, puede ser necesario asegurar que los datos asociados nunca se liberen, particularmente cuando pertenecen a rasgos de seguridad adicionales.

Tales registros de registro se llenan típicamente de la siguiente forma. El conjunto de credenciales que pertenece a un presentador se proporciona al controlador y se verifica y valida el conjunto de credenciales. Una vez que se verifica y valida el conjunto de credenciales, se produce un instrumento que soporta el conjunto de credenciales, y este conjunto de credenciales se proporciona al presentador. El conjunto de credenciales también se introduce a un nuevo registro en el registro de registro y típicamente se complementa con cualquier dato que pertenece al instrumento correspondiente (tal como número de serie, etc.) y cualquier otro dato relevante (tal como datos de rasgos de seguridad adicionales incluyendo pero no limitado a biométricos, etc.).

Han evolucionado las formas de reproducir los conjuntos de credenciales sobre tales instrumentos a medida. Históricamente, tales datos pueden haber sido entintados, mecanografiados o etiquetados en el instrumento emitido. Posteriormente, tales datos pueden ser grabados en relieve o grabados o codificados o incrustados en el instrumento emitido. Más recientemente, se han usado como instrumentos medios legibles por máquina (tales como bandas magnéticas o chips), los conjuntos de credenciales relevantes que están almacenados electrónicamente en tales medios. El formato de muchos instrumentos (y el formato en el que los conjuntos de credenciales se almacenan en los mismos) se rige por la Organización Internacional de Estandarización. Por ejemplo, el documento ISO 7501 rige el formato de documentos de viaje legibles por máquina; el documento ISO 7810 e ISO 7811 rigen el formato de Tarjetas de Identificación; y el documento ISO 7812 e ISO 7816 rigen la manera en la que las tarjetas se pueden proporcionar desde diferentes emisores.

A pesar de los avances en la provisión de instrumentos que soportan los conjuntos de credenciales de presentador, sigue existiendo el peligro de fraude. Sigue siendo necesario ser capaces tanto de verificar que el presentador que porta el instrumento que comprende el conjunto de credenciales es el presentador válido/auténtico (es decir, que el instrumento no ha sido robado o clonado y por lo tanto no está siendo usado fraudulentamente) y también de verificar que el instrumento proferido que comprende el conjunto de credenciales es verdaderamente auténtico (es decir, que las credenciales son exactas y que el instrumento no es una completa falsificación). Este es un problema de aumento de preocupación en la medida que portadores de tales instrumentos liberan sus conjuntos de credenciales de una forma cada vez más frecuente. Mientras que los conjuntos de credenciales se mantienen inicialmente en un entorno de confidencialidad/privacidad, existente entre los presentadores de conjuntos de credenciales y sus controladores, este entorno de confidencialidad/privacidad se pone en peligro siempre que el conjunto de credenciales se libera durante un intercambio con un tercero. Aunque las mejoras en la seguridad de los

medios por los cuales se liberan conjuntos de credenciales han tratado de reforzar este entorno de confidencialidad/privacidad, la debilidad aún persiste.

Por ejemplo, incluso con el advenimiento de sistemas automatizados para leer instrumentos de pasaporte, cuando un pasajero presenta su pasaporte a cualquier oficial de punto de control o agencia de control de fronteras (el "aceptador"), las credenciales controladas en el instrumento emitido son visibles para y manejadas por el aceptador antes de y después de capturar las credenciales controladas en el dispositivo de lectura. Si - en la infracción de la política de privacidad dichas credenciales que se ven se copian y comparten por el aceptador, no sólo se capturan y procesan, se compromete el estado de privacidad en el que residían originalmente las credenciales del instrumento de pasaporte. Existen deficiencias similares para otros instrumentos para los cuales se han desarrollado sistemas de captura de credenciales automatizados, tales como carnets de conducir, tarjetas de fidelidad/afiliación, y tarjetas de pago.

Sigue existiendo una necesidad de métodos y sistemas mejorados por los cuales los presentadores pueden ofrecer conjuntos de credenciales durante intercambios con otros individuos u organizaciones de una manera que garanticen tanto la autenticidad del conjunto de credenciales, como la autenticidad del presentador que porta el conjunto de credenciales. Sería altamente deseable proporcionar métodos y sistemas que aseguren un entorno de confidencialidad/privacidad completa para los conjuntos de credenciales cuando están siendo revelados. Sería fuertemente preferible para cualquiera de tales métodos y sistemas mejorados que sean compatibles hacia atrás con métodos y sistemas existentes que están en uso común de manera que los métodos y sistemas mejorados se puedan introducir suavemente y gradualmente. Esto sería altamente ventajoso ya que eliminaría la necesidad de transiciones costosas y que consumen tiempo a nuevos sistemas y métodos. Sería además preferible para cualquier nuevo método y sistema mejorado que sea escalable de manera que puedan atender una pluralidad de diversos conjuntos de credenciales a través de un único sistema y método.

El documento US-A-2013/0246203 describe la realización de transacciones de pago en las que se reduce el fraude. Las credenciales de pago de un cliente nunca se proporcionan a un comerciante y no pueden ser accedidas para uso en la transacción de pago a menos que se proporcione una solicitud de acceso desde el dispositivo autorizado designado por el cliente. En una realización, el dispositivo autorizado comprende un teléfono móvil.

El documento WO-A-2004/049621 describe un sistema de autenticación en el que un primer terminal comunica con un facilitador sobre un primer canal de telecomunicaciones y un segundo terminal comunica con un operador sobre un segundo canal de comunicaciones, el facilitador y el operador que son capaces de comunicar uno con otro. No se proporcionan datos de identidad al primer terminal por el operador, el facilitador o el segundo terminal, y no se proporcionan datos de identidad del primer terminal al segundo terminal por el operador, el facilitador o el primer terminal, y, la comunicación entre el primer terminal y el facilitador y entre el segundo terminal y el operador no contiene datos con respecto a los detalles de identidad del usuario.

El documento WO-A-2013/034192 describe un método para validar una transacción electrónica en la cual se transfieren datos de identificación desde el teléfono móvil a un terminal punto de venta y que necesita ser validada mediante un código PIN proporcionado al servidor durante una llamada telefónica de voz.

Compendio de la invención

Un aspecto de la invención comprende un sistema según la reivindicación 1 para permitir una comunicación de al menos un conjunto de credenciales controladas conectadas a un presentador, a un punto final de red, mientras que mantiene la privacidad que prevalece en dichas credenciales controladas conectadas al presentador, en donde el sistema comprende al menos un aparato de aceptación, al menos un aparato de presentación, al menos un punto final de red y al menos un servidor, y en donde uno de dichos servidores comprende uno o más registros. Cada registro pertenece a un presentador dado, comprende un identificador de presentador, y un código clave secreto unido a cada identificador de presentador, y está afiliado con al menos una entrada que pertenece a un conjunto de credenciales controladas conectadas al presentador. Cada entrada pertenece a al menos un conjunto de credenciales asociado con dicho presentador dado. Cada entrada también puede pertenecer a al menos un alías, cada alías conectado respectivamente con uno de dichos conjuntos de credenciales. Cada punto final de red es un destinatario designado de un tipo de credenciales controladas conectadas a presentadores, dicho punto final que es o bien el aparato de aceptación o bien el de un tercero designado vinculado al aparato de aceptación; en donde permitir una comunicación de al menos un conjunto de credenciales controladas conectadas al presentador se realiza en el contexto de una interacción entre el interlocutor de presentación y el interlocutor de aceptación; y en donde el conjunto de credenciales al que pertenece el permiso está asociado con el interlocutor de presentación. Uno de dichos servidores funciona como un servidor de control configurado además para (a) recibir una comunicación desde un aparato de aceptación en lo sucesivo conocida como comunicación de aparato de aceptación, dicha comunicación que contiene un código clave secreto que pertenece al presentador y un código clave compartido de uso único; (b) recibir una comunicación desde un aparato de presentación en lo sucesivo conocida como una comunicación de aparato de presentación, dicha comunicación que contiene un identificador de presentador que pertenece al presentador y un código clave compartido de uso único; (c) buscar hacer coincidir el código clave compartido de uso único contenido en la comunicación de aparato de aceptación y el código clave compartido de uso único correspondiente contenido en la comunicación de aparato de presentación; (d) iniciar una

búsqueda de un registro objetivo vinculando el código clave secreto contenido en dicha comunicación de aparato de aceptación y el identificador de presentador contenido en dicha comunicación de aparato de presentación, en donde ambas de dichas comunicaciones contienen el mismo código clave compartido; (e) dirigir una búsqueda de dicho registro objetivo que comprende tanto dicho código clave secreto como dicho identificador de presentador; (f) identificar una entrada afiliada con dicho registro objetivo, dicha entrada que pertenece a un conjunto de credenciales controladas conectadas al presentador; (g) permitir la recuperación de dicho conjunto de credenciales que pertenecen a dicha entrada y permitir la liberación de dicho conjunto de credenciales a dicho punto final de red, dicho punto final que es el destinatario permitido de un conjunto de credenciales controladas conectadas a dicho presentador, y dicho punto final que es o bien el aparato de aceptación o bien el de un tercero designado vinculado con el aparato de aceptación.

Otro aspecto de la invención comprende un método según la reivindicación 25 que permite una comunicación de al menos un conjunto de credenciales controladas conectadas a un presentador, desde un servidor a un punto final de red, mientras que se mantiene la privacidad que prevalece en dicha credenciales controladas conectadas al presentador; y en donde un servidor comprende uno o más registros, cada registro que pertenece a un presentador (parte dada inscrita con el servidor como presentador y/o como aceptador), y cada registro que comprende un identificador de presentador (y/o identificador de aceptador) y un código clave secreto (de presentador y/o de aceptador) unido a dicho identificador de presentador, y cada registro está afiliado con una entrada que pertenece a un conjunto de credenciales controladas (asociadas con dicha parte) conectadas a dicho presentador; el método que comprende: (a) en un aparato de aceptación, poner a disposición un código clave compartido de uso único para un/el interlocutor de presentación; (b) en el aparato de aceptación, recibir un código clave secreto (presentador) que pertenece al interlocutor de presentación en donde dicho código clave secreto (de presentador) se introduce en el aparato de aceptación por el interlocutor de presentación; (c) en el aparato de aceptación, comunicar una comunicación de aparato de aceptación a al menos uno de los servidores, dicha comunicación de aparato de aceptación que contiene el código clave compartido de una sola vez y el código clave secreto (de presentador); (d) en un aparato de presentación del interlocutor de presentación, recibir el código clave compartido de uso único; (e) en el aparato de presentación, recuperar un identificador de presentador que pertenece al interlocutor de presentación desde una ubicación de almacenamiento en el aparato de presentación; y (f) en el aparato de presentación, comunicar una comunicación de aparato de presentación a dicho servidor, dicha comunicación de aparato de presentación que contiene el código clave compartido de uso único y el identificador de presentador, en donde (g) a la recepción de dicha comunicación de aparato de aceptación y dicha comunicación de aparato de presentación, en el servidor procesar las comunicaciones para averiguar si se permite comunicar un conjunto de credenciales controladas conectadas al presentador, permitir por ello su recuperación en un servidor y permitir por ello su liberación a un punto final de red, dicho punto final de red que es un destinatario permitido, y dicho punto final que es o bien el aparato de aceptación o bien el de un tercero designado vinculado al aparato de aceptación.

En un aspecto de la invención, todos los conjuntos de credenciales conectadas al presentador (o alias afiliados a conjuntos de credenciales) pueden estar comprendidas como entradas en dicho registro.

En otro aspecto de la invención, todos los conjuntos de credenciales conectadas al presentador (o alias afiliados) pueden estar comprendidas como entradas separadas en un servidor diferente comunicable con un servidor de control. Alternativamente, algunos conjuntos de credenciales conectadas al presentador y alias afiliados pueden estar comprendidas como entradas en dicho registro, mientras que otras pueden estar comprendidas como entradas separadas en dicho servidor o entradas separadas en diferentes servidores.

La comunicación de aparato de aceptación se puede comunicar a dicho servidor sobre un primer canal de comunicación y la comunicación de aparato de presentación se puede comunicar a dicho servidor sobre un segundo canal de comunicación.

En un aspecto de la invención, el código clave compartido de uso único se puede generar en el servidor y comunicar al aparato de aceptación antes de que se ponga a disposición dicho código clave compartido de uso único al interlocutor de presentación y/o al aparato de presentación.

En otro aspecto de la invención, el código clave compartido de uso único se puede generar en el aparato de aceptación antes de que se ponga a disposición dicho código clave compartido de uso único al interlocutor de presentación y/o el aparato de presentación.

Una copia del código clave compartido de uso único se puede comunicar desde el aparato de aceptación al aparato de presentación a través de una tecnología inalámbrica, la tecnología inalámbrica seleccionada opcionalmente de un grupo que comprende Wifi, bluetooth, NFC o RFID.

En un aspecto de la invención, se puede asignar un periodo de validez a la comunicación de aparato de aceptación y a la comunicación de aparato de presentación y/o el código clave compartido. Esto asegura que si una comunicación de aparato de aceptación no coincide con una comunicación de aparato de presentación como se trata más adelante dentro de un cierto intervalo de tiempo (el periodo de validez), entonces tal comunicación caduca y por ello queda sin efecto presentando procesos adicionales redundantes. Cuando tal comunicación caduca y queda sin efecto haciendo los procesos adicionales redundantes, los datos que pertenecen a la comunicación se

pueden purgar, liberando recursos para el procesamiento de comunicaciones adicionales. Cuando las comunicaciones se generan, transmiten o reciben, conteniendo códigos clave compartidos que portan un periodo de validez, el periodo de validez puede asegurar que se pueden usar códigos clave compartidos más cortos y menos complejos debido a que es factible por ello la reutilización de códigos clave compartidos. A la expiración del periodo de validez de un código clave compartido, el mismo código clave compartido se puede reutilizar en una iteración posterior del método.

En un aspecto de la invención una copia del código clave compartido de uso único se puede poner a disposición del interlocutor de presentación y/o del aparato de presentación a través de una pantalla comprendida en el aparato de aceptación o en una impresión del aparato de aceptación, en donde o bien: (a) una copia del código clave compartido de uso único se pone a disposición en un formato de carácter legible por máquina, por ejemplo UTF-8, y la copia del código clave compartido de uso único se recibe en el periférico de presentación a través de la entrada del interlocutor de presentación y/o del interlocutor de aceptación y/o del aparato de aceptación; o bien (b) una copia del código clave compartido de uso único está comprendida en un código QR, y la copia del código clave compartido de uso único se recibe en el aparato de presentación a través de una función de cámara comprendida en el aparato de presentación que se usa para capturar el código de respuesta rápida y extraer una copia del código clave compartido de uso único.

La comunicación de aparato de aceptación puede contener además uno o más parámetros auxiliares predeterminados, y la comunicación de aparato de presentación también puede contener además dicho uno o más parámetros auxiliares predeterminados, Estos parámetros auxiliares también opcionalmente pueden tener que coincidir como se describirá además a continuación antes de la corroboración de que tenga éxito iniciar y dirigir una búsqueda de cualquier registro objetivo. Esta condición de coincidencia adicional en el proceso de corroboración, cuando se manda sobre o por encima del código clave compartido, mejora además el método en la medida que introduce criterios adicionales en el proceso de búsqueda de hacer coincidir una comunicación de aparato de aceptación y una comunicación de aparato de presentación. El parámetro auxiliar predeterminado puede ser un código acordado entre el interlocutor de aceptación y el interlocutor de presentación, o puede ser un valor pertinente a la interacción entre el interlocutor de presentación y el interlocutor de aceptación, tal como el valor de la transacción prevista.

Si se asigna un periodo de validez al código clave compartido de uso único, dicho código clave compartido puede ser único durante la duración de su periodo de validez.

Otro aspecto de la invención comprende un método que permite una comunicación de al menos un conjunto de credenciales controladas conectadas al presentador, en un servidor a un punto final de red, mientras que se mantiene la privacidad que prevalece en el conjunto de credenciales controladas conectadas al presentador en donde el permiso comprende una comunicación de aparato de aceptación que contiene un código clave compartido y un código clave secreto de presentador, y una comunicación de aparato de presentación que contiene un código clave compartido y un identificador de presentador, el método que comprende: (a) en un/el servidor recibir la comunicación de aparato de aceptación; (b) en un/el servidor recibir la comunicación de aparato de presentación; (c) en un/el servidor buscar hacer coincidir el código clave compartido de uso único contenido en la comunicación de aparato de aceptación con el código clave compartido de uso único correspondiente contenido en la comunicación de aparato de presentación, (d) en un/el servidor iniciar una búsqueda para un registro objetivo vinculando el código clave secreto (de presentador) contenido en la comunicación de aparato de aceptación y el identificador de presentador contenido en la comunicación de aparato de presentación, en donde tanto dichas comunicaciones contienen el mismo código clave compartido; (e) en un/el servidor dirigir una búsqueda de un registro objetivo que comprende tanto dicho código clave secreto (de presentador) como dicho identificador de presentador; (f) si se identifica un registro objetivo, en un/el servidor identificar una entrada afiliada con dicho registro objetivo, dicha entrada que pertenece a las credenciales controladas conectadas al presentador; (g) en un/el servidor permitir una recuperación de dicho conjunto de credenciales identificadas por dicha entrada afiliada al registro objetivo, y permitir una liberación de dicho conjunto de credenciales a dicho punto final de red, dicho punto final que es el destinatario permitido de un conjunto de credenciales controladas conectadas al presentador, y dicho punto final que es o bien el aparato de aceptación o bien el de un tercero designado vinculado al aparato de aceptación.

El registro objetivo en dicho servidor también puede comprender además un alias asociado a dicha entrada que pertenece a cada conjunto de credenciales conectadas al presentador, y la comunicación de aparato de presentación puede contener además una copia de un alias seleccionado de una lista de alias detallados en el aparato de presentación, en donde el paso de dirigir una búsqueda de un registro objetivo que comprende el mismo identificador de presentador y código clave secreto también utiliza la copia del alias contenido en la comunicación de aparato de presentación para buscar un registro objetivo que comprende el mismo dicho alias además del mismo identificador de presentador y código clave secreto.

La entrada que pertenece al conjunto de credenciales conectadas al presentador pueden estar comprendidas en dicho registro objetivo en dicho servidor de control configurado para permitir la recuperación y liberación del conjunto de credenciales conectadas al presentador, y los pasos de recuperación del conjunto de credenciales conectadas al presentador y de liberación del conjunto de credenciales conectadas al presentador se realizan en dicho servidor de

control configurado para permitir la recuperación y liberación del conjunto de credenciales conectadas al presentador.

El conjunto de credenciales conectadas al presentador pueden estar comprendidas en entradas separadas en un servidor diferente por separado de dicho servidor de control configurado para permitir la recuperación y la liberación del conjunto de credenciales conectadas al presentador, la entrada separada que está afiliada con el registro objetivo, en donde los pasos de recuperación y de liberación del conjunto de credenciales se realizan o bien en dicho servidor de control configurado para permitir la recuperación y liberación del conjunto de credenciales conectadas al presentador o dicho servidor diferente separado de ese servidor de control configurado para permitir la recuperación y liberación del conjunto de credenciales conectadas al presentador.

Un periodo de validez se puede asignar a la comunicación de aparato de aceptación y/o la comunicación de aparato de presentación y/o el código clave compartido contenido en la comunicación de aparato de aceptación y/o en la comunicación de aparato de presentación, en donde el paso de búsqueda para hacer coincidir el código clave compartido contenido en una comunicación de aparato de aceptación y el código clave compartido contenido en la comunicación de aparato de presentación comprende además establecer si ha expirado el periodo de validez. Esto asegura que si una comunicación de aparato de aceptación no se hace coincidir con una comunicación de aparato de presentación como se trata a continuación con un cierto intervalo de tiempo (el periodo de validez), entonces tal interacción/notificación/comunicación caduca y por ello queda sin efecto hacer los procesos adicionales redundantes. Cuando cualquier periodo de validez caduca y queda sin efecto hacer los procesos adicionales redundantes, se puede purgar los datos que pertenecen a la comunicación, liberando recursos para el procesamiento de comunicaciones adicional. Cuando cualquier comunicación se genera/transmite/recibe y contiene códigos clave compartidos que portan un periodo de validez, el periodo de validez puede asegurar que se pueden usar códigos clave compartido más cortos y menos complejos debido a que es por ello factible la reutilización del código clave compartido. A la expiración del periodo de validez de un código clave compartido, el mismo código clave compartido se puede reutilizar en una iteración posterior del método.

Si se asigna un periodo de validez al código clave compartido, dicho código clave compartido puede ser único durante la duración de su periodo de validez.

La comunicación de aparato de aceptación puede contener además uno o más parámetros auxiliares predeterminados, y la comunicación de aparato de presentación también puede contener además dicho uno o más parámetros auxiliares predeterminados, en donde el paso de búsqueda de hacer coincidir los códigos clave compartidos comprende además el paso de búsqueda de corroborar el parámetro auxiliar predeterminado contenido en la comunicación de aparato de aceptación y el parámetro auxiliar predeterminado correspondiente contenido en la comunicación de aparato de presentación.

Un aspecto adicional de la invención comprende un método que permite una comunicación de un conjunto de credenciales controladas conectadas a un presentador, en un servidor a un punto final de red, mientras que se mantiene la privacidad que prevalece en las credenciales conectadas al presentador, un permiso hecho/concedido según cualquiera de los aspectos de la invención descritos anteriormente, el método que comprende: (a) en un/el servidor recibir la comunicación de aparato de aceptación; (b) en un/el servidor recibir la comunicación de aparato de presentación; (c) en el servidor buscar hacer coincidir el código clave compartido de uso único contenido en la comunicación de aparato de aceptación y el código clave compartido de uso único correspondiente contenido en la comunicación del interlocutor de presentación (y, que, hace coincidir por ello dicha comunicación de aparato de aceptación con dicha comunicación de aparato de presentación); (d) en un/el servidor, iniciar una búsqueda de un registro objetivo vinculando el código clave secreto contenido en la comunicación de aparato de aceptación y el identificador de presentador contenido en la comunicación de aparato de presentación; (e) en un/el servidor dirigir una búsqueda de un registro objetivo que comprende tanto dicho código clave secreto como dicho identificador de presentador; (f) si se identifica un registro objetivo, identificar una entrada que pertenece a un conjunto de credenciales conectadas al presentador y asociadas; (g) si se identifica un conjunto de credenciales conectadas al presentador, en un/el servidor permitir una recuperación del conjunto de credenciales conectadas al presentador, y permitir una liberación de dicho conjunto de credenciales conectadas al presentador a dicho punto final de red, dicho punto final que es el destinatario permitido del conjunto de credenciales conectadas al presentador, y dicho punto final que es o bien el aparato de aceptación o bien el de un tercero designado vinculado al aparato de aceptación.

Si dichos conjuntos de credenciales conectadas al presentador están comprendidos en dichos registros en dicho servidor de control configurado para permitir la recuperación y liberación de las credenciales controladas, los pasos de recuperación del conjunto de credenciales de presentador conectadas y de comunicación del conjunto de credenciales de presentador conectadas se puede realizar en dicho servidor de control configurado para permitir la recuperación y liberación de las credenciales controladas.

Si dichos conjuntos de credenciales conectadas al presentador están comprendidos en entradas separadas en un servidor diferente que está separado de dicho servidor de control configurado para permitir la recuperación y liberación de las credenciales controladas (el paso de identificación de una entrada que pertenece a un conjunto de credenciales de presentador conectadas se puede realizar en dicho servidor diferente separado de dicho servidor de control configurado para permitir la recuperación y liberación de las credenciales controladas), los pasos de

recuperación del conjunto de credenciales conectadas y de liberación del conjunto de credenciales conectadas se pueden realizar o bien en el servidor de control configurado para permitir la recuperación y liberación del conjunto de credenciales conectadas al presentador o bien en el servidor diferente separado de ese servidor de control configurado para permitir la recuperación y liberación del conjunto de credenciales conectadas al presentador.

El paso de búsqueda de hacer coincidir los códigos clave compartidos puede comprender además establecer si ha expirado el período de validez.

El paso de búsqueda de hacer coincidir los códigos clave compartidos puede comprender además la búsqueda de hacer coincidir el parámetro auxiliar predeterminado contenido en la comunicación de aparato de aceptación con el parámetro auxiliar predeterminado correspondiente contenido en la comunicación de aparato de presentación.

Si se asigna un período de validez al código clave compartido de uso único, dicho código clave compartido puede ser único durante la duración de su período de validez.

En otro aspecto de la invención, un método que comprende (a) un aparato de aceptación que pone a disposición del interlocutor de presentación un código clave compartido de uso único; (b) recibir un código clave secreto de presentador que pertenece al interlocutor de presentación en el aparato de aceptación en donde dicho código clave secreto de presentador se introduce en el terminal por el interlocutor de presentación; (c) comunicar una comunicación de aparato de aceptación desde el aparato de aceptación al servidor, la comunicación de aparato de aceptación que comprende el código clave compartido de uso único y el código clave secreto de presentador; (d) el aparato de presentación que recibe el código clave compartido de uso único; (e) el aparato del presentador que recupera un identificador de presentador que pertenece al interlocutor de presentación de una ubicación de almacenamiento en el aparato de presentación; y (f) el aparato de presentación que comunica una comunicación de aparato de presentación al servidor de control, la comunicación de aparato de presentación que comprende el código clave compartido de uso único, y el identificador de presentador.

El registro objetivo en dicho servidor también puede comprender además un alias asociado con dicha entrada que pertenece a cada conjunto de credenciales conectadas al presentador, y la comunicación de aparato de presentación puede contener además una copia de un alias seleccionado de una lista de alias detallada en el aparato de presentación, y en donde el paso de dirigir una búsqueda de un registro objetivo que comprenda el mismo identificador de presentador y código clave secreto también utiliza el alias contenido en la comunicación de aparato de presentación para buscar un registro objetivo que comprenda el mismo dicho alias además del mismo identificador de presentador y código clave secreto.

El conjunto de credenciales puede estar comprendido como una entrada en dicho registro objetivo en dicho servidor de control configurado para permitir la recuperación y liberación de las credenciales controladas, y los pasos de recuperación del conjunto de credenciales y de liberación del conjunto de credenciales se realizan en dicho servidor de control configurado para permitir la recuperación y liberación de las credenciales controladas.

El conjunto de credenciales puede estar comprendido como una entrada en un servidor diferente separado de dicho servidor de control configurado para permitir la recuperación y liberación de las credenciales controladas, la entrada separada que está afiliada con el registro objetivo, y en donde los pasos de recuperación y de liberación del conjunto de credenciales se pueden realizar o bien en dicho servidor de control configurado para permitir la recuperación y liberación de las credenciales controladas o bien en el servidor diferente separado de ese servidor de control configurado para permitir la recuperación y liberación de las credenciales controladas.

Un aspecto adicional de la invención comprende un aparato de presentación configurado para realizar uno o más de los pasos del aparato de presentación descritos anteriormente.

Otro aspecto de la invención comprende un aparato de aceptación configurado para realizar uno o más de los pasos del aparato de aceptación descritos anteriormente.

Un aspecto adicional de la invención comprende un servidor configurado para realizar uno o más de dichos pasos de servidor descritos anteriormente.

Un aspecto adicional de la invención comprende un sistema que comprende dos o más de los aparatos de presentación, dos o más de los aparatos de aceptación, y dicho servidor de control configurado para realizar una o más de las realizaciones que se han descrito anteriormente.

Un aspecto adicional de la invención comprende un medio de almacenamiento legible por ordenador que lleva un programa de ordenador almacenado en el mismo, dicho programa que comprende instrucciones ejecutables por ordenador adaptadas para realizar uno o más de los pasos del método descritos anteriormente cuando se ejecutan por uno o más módulos de procesamiento.

Descripción detallada

La Figura 1 es un diagrama que ilustra el sistema central para preservar la privacidad de una manera que también facilite la liberación permitida de un conjunto de credenciales almacenadas a un destinatario aprobado por el participante al que pertenece el conjunto de credenciales. El sistema 100 es seguro porque protege los conjuntos de credenciales del acceso no autorizado por posibles destinatarios no autorizados de los conjuntos de credenciales, y también evita que los conjuntos de credenciales sean usados por aquellos que presentarían fraudulentamente un conjunto de credenciales como que son las suyas propias. Las partes inscritas con el sistema se designan como "presentadores" y "aceptadores" según su papel en el método de la invención y su manera de interactuar con el sistema de la invención. En el transcurso de una interacción entre un presentador y un aceptador, puede ser necesario para el presentador liberar un conjunto de credenciales con el que está asociado. Presentadores y aceptadores que participan activamente en tal interacción se designan específicamente como "interlocutores de presentación" e "interlocutores de aceptación" Se apreciará que en muchas realizaciones de la invención, los presentadores se asocian cada uno con conjuntos de credenciales que son únicos para ellos, de manera que los presentadores están relacionados con los conjuntos de credenciales de una forma "uno a uno". No obstante, la invención también prevé escenarios donde hay una relación "muchos a uno" entre los presentadores y los conjuntos de credenciales, donde muchos presentadores están asociados con un único conjunto de credenciales, y aún es deseable mantener dicho conjunto de credenciales en un estado de privacidad.

Según una realización de la invención, el sistema y el método de la invención se usa por tal interlocutor de presentación para liberar un conjunto de credenciales asociadas con dicho interlocutor de presentación a uno o más destinatarios designados de una manera que mantenga la privacidad del conjunto de credenciales. Según otras realizaciones de la invención, el sistema y el método de la invención se pueden usar por un interlocutor de aceptación para liberar un conjunto de credenciales asociadas con el interlocutor de aceptación a uno o más destinatarios designados mientras se preserva dicho estado de privacidad. Otras realizaciones de la invención prevén la divulgación concurrente de conjuntos de credenciales tanto de presentador como de aceptador asociadas respectivamente con el interlocutor de presentación y el interlocutor de aceptación. Tanto el presentador como el aceptador cooperan para facilitar la liberación de tales conjuntos de credenciales del sistema. El destinatario designado puede ser el interlocutor de aceptación, el interlocutor de presentación o puede ser un tercero de confianza.

El sistema 100 comprende al menos un servidor 101, el servidor que comprende una colección de registros de presentador 102. Cada registro de presentador pertenece a un participante dado que se ha inscrito como presentador con dicho servidor 101, y cada uno de dichos registros comprende uno o más conjuntos de credenciales que pertenecen a ese presentador. Más en particular, cada registro de presentador comprende un identificador de presentador, un código clave secreto de presentador, al menos un conjunto de credenciales asociadas con dicho presentador, y al menos un alias, en donde cada conjunto de credenciales está conectado respectivamente con un alias por lo cual cada alias dentro de un registro de presentador es distinguible de los alias restantes para ese registro de presentador. El identificador de presentador es una cadena única que se usa para identificar un registro de presentador dado para la recopilación de registros de presentador. El código clave secreto de presentador es una cadena conocida solamente por el presentador. Cuando un presentador interactúa con el sistema con vistas a liberar un conjunto de credenciales de presentador a un destinatario designado (tal presentador se conoce como "interlocutor de presentación"), proporcionan su identificador de presentador, y su código clave secreto de presentador se puede utilizar entonces para autenticar el interlocutor de presentación antes de que se libere cualquier conjunto de credenciales. Además del identificador de presentador y el código clave secreto de presentador, cada registro de presentador comprende al menos un conjunto de credenciales. Como se ha descrito previamente, cada conjunto de credenciales comprende un conjunto de datos personales que es particular para un individuo y necesario para una interacción dada. Cada conjunto de credenciales también está asociado con un alias distinguible. A modo de ilustración, un individuo mediante el nombre de "John Brown" puede tener un primer conjunto de credenciales que pertenecen a un carnet de conducir, y un segundo conjunto de credenciales que pertenecen a una tarjeta de fidelidad de una tienda. El primer conjunto de credenciales puede comprender el nombre "John Brown", una fecha de nacimiento, un número de carnet de conducir, y una fecha de expiración. El segundo conjunto de credenciales puede comprender el nombre "John Brown", una dirección, y un número de afiliación de club de fidelidad. El primer conjunto de credenciales se puede asociar con el alias "carnet de conducir", mientras que el segundo conjunto de credenciales se puede asociar con el alias "tarjeta de fidelidad 1". Se apreciará que en realizaciones de la invención donde se prevé que cada registro de presentador comprenderá solamente un conjunto de credenciales, puede que no sea necesario que los registros del presentador comprendan además un alias conectado a cada conjunto de credenciales. Más bien, en tales casos, la identificación del registro que pertenece al presentador que interactúa también indicará automáticamente el conjunto de credenciales a ser liberado.

Además, en algunas realizaciones de la invención, el servidor 101 también comprende una colección de registros de aceptador separados. Cada registro de aceptador pertenece a un individuo u organización que se ha inscrito como aceptador con el servidor, y comprende uno o más conjuntos de credenciales asociadas con ese aceptador. Cada registro de aceptador comprende además un identificador de aceptador, y opcionalmente un código clave secreto de aceptador. El identificador de aceptador es una cadena única que se usa para identificar un registro de aceptador dado dentro de la colección de registros de aceptador. El código clave secreto de aceptador (si es aplicable) es una cadena conocida solamente por el aceptador. Cuando un aceptador interactúa con el sistema con vistas a facilitar la liberación de un conjunto de credenciales de presentador asociadas con el interlocutor de presentación con un

destinatario designado (tal aceptador se conoce como “interlocutor de aceptación”) se proporciona el identificador de aceptador del interlocutor de aceptación, y el código clave secreto del aceptador del interlocutor de aceptación (si se utiliza) se puede emplear entonces para autenticar al interlocutor de aceptación antes de que se revele cualquier conjunto de credenciales.

Se apreciará que aunque en esta realización de la invención descrita, los registros de presentador y los registros de aceptador son distintos y típicamente se mantienen como colecciones de registros separadas, en otras realizaciones de la invención, el servidor 101 puede comprender una colección de registros única que comprende tanto registros de presentador como de aceptador. Además, se apreciará también que mientras que en una realización, unos conjuntos de credenciales de aceptador y/o de presentador están almacenados en un servidor, también se prevén múltiples servidores, en donde cada servidor tiene la tarea del almacenamiento de registros que comprenden uno o más tipos de conjuntos de credenciales.

Se prevé adicionalmente que en algunas realizaciones de la invención, el servidor 101 comprenderá únicamente registros de presentador, y no comprenderá registros de aceptador. Preferiblemente, en tales realizaciones, el servidor 101 y los interlocutores de aceptación potenciales serán capaces de comunicar entre ellos a través de sus sistemas de software existentes Esta realización de la invención es ventajosa debido a que no se requiere el registro previo de aceptadores, y esto elimina un obstáculo para la captación del sistema y método reivindicados entre los interlocutores de aceptación potenciales. Esto por lo tanto mejora la facilidad de uso del sistema y método.

El servidor 101 es comunicable con uno o más aparatos 109 sobre un canal de comunicación. Se apreciará que el canal de comunicación 107 puede comprender Internet, una red propietaria, o una combinación de las dos. El aparato 109 se puede situar de una manera dispar, y puede conectarse al canal de comunicación 107 por medio de una o más de una variedad de tecnologías, tales como PSTN, Ethernet, DSL, ISDN, Wi-Fi, WiMax, 2G, 3G, LTE, 4G, etc. Los aparatos 109 pueden ser cualquiera de una variedad de dispositivos, incluyendo ordenadores personales de sobremesa, ordenadores portátiles, ordenadores personales de tableta, asistentes digitales personales, teléfonos móviles, teléfonos inteligentes, etc. El aparato 109 puede comprender alternativamente sistemas informáticos a medida como se usan en una variedad de industrias incluyendo banca, finanzas, aviación, viajes, seguridad nacional, control de fronteras, energía, transporte, venta al por menor y/o telecomunicaciones. Por consiguiente, los aparatos pueden comprender dispositivos configurados para actuar como dispositivos de Punto de Venta. En el contexto de la invención, estos aparatos se conocerán como “aparatos de aceptación”.

El servidor 101 también es comunicable sobre un canal de comunicación 106 con uno o más aparatos 108. Tales aparatos pueden comprender, por ejemplo, dispositivos inalámbricos comunicables con el servidor 101 a través de una estación base inalámbrica o encaminador. Los dispositivos inalámbricos pueden comprender cualquier forma de dispositivo inalámbrico incluyendo ordenadores portátiles, ordenadores personales de tableta, asistentes digitales personales, teléfonos móviles, teléfonos inteligentes, etc. Tales dispositivos periféricos pueden comprender además dispositivos comunicables sobre el canal de comunicación 106 a través de una conexión por cable, y de esta manera, por ejemplo, pueden incluir ordenadores de sobremesa, así como sistemas informáticos a medida específicos de la industria mencionados anteriormente, incluyendo pero no limitados a sistemas de Punto de Venta. En el contexto de la invención, estos dispositivos periféricos se conocerán como “aparatos de presentación”. En una realización, el aparato de presentación también puede estar protegido por contraseña o puede requerir un permiso adicional del presentador para iniciar la comunicación. Los periféricos de presentación pueden estar situados de manera dispar, y pueden comunicarse con el servidor 101 sobre el canal de comunicación 108 a través de una variedad de medios tales como PSTN, Ethernet, DSL e ISDN. Los aparatos de presentación que comprenden dispositivos inalámbricos pueden comunicarse con el servidor 101 por medio de una o más de una variedad de tecnologías de comunicaciones inalámbricas, tales como Wi-Fi, WiMax, 2G, 3G, LTE, 4G, etc. El canal de comunicación 106 puede comprender Internet, una red propietaria, o una combinación de las dos. Los aparatos de presentación 108 están configurados con una aplicación que facilita la comunicación con el servidor 101. Como la conexión entre los aparatos de aceptación 109 y el servidor 101 comprenden un primer canal de comunicaciones 107 y la conexión entre los aparatos de presentación 108 y el servidor 101 comprenden un segundo canal de comunicaciones 106, el sistema 100 se puede considerar como que es “multicanal” en su composición. Esto asegura un mecanismo más seguro mediante el cual los conjuntos de credenciales y otros datos sensibles se pueden almacenar y liberar al punto final de red 110 mientras que permanecen en estado de privacidad. El punto final de red 110 en algunas realizaciones puede ser o bien un aparato separado o bien el aparato de aceptación en sí mismo dependiendo del destino designado en la comunicación de aparato de aceptación.

Mientras que en esta realización, se ha descrito que los conjuntos de credenciales y los alias conectados están comprendidos en los registros de presentador y/o de aceptador en el servidor, en otras realizaciones de la invención, se anticipa que dichos conjuntos de credenciales y alias conectados pueden estar afiliados con dichos registros de presentador y/o de aceptador en formas alternativas. Por ejemplo, los conjuntos de credenciales y los alias afiliados pueden estar comprendidos en uno o más conjuntos de registros separados del conjunto o de los conjuntos de registros en el servidor que comprenden los registros que comprenden los identificadores y las claves secretas. Estos conjuntos de registros separados pueden estar alojados en uno o más servidores diferentes. En algunas realizaciones de la invención, los servidores diferentes que alojan los conjuntos de credenciales se administran por los controladores responsables de la emisión de los instrumentos que comprenden dichos conjuntos de credenciales.

La Figura 2 es un diagrama de flujo que ilustra cómo un nuevo solicitante potencial se inscribe con el servidor 101 como presentador según una realización de la invención. En el paso 200, una página web alojada por el servidor 101 es accesible por el nuevo solicitante de presentador, preferiblemente usando sus aparatos de presentación 108. La página web está configurada de manera que en este paso, el nuevo solicitante de presentador proporciona detalles generales de inscripción tales como nombre, dirección, dirección de correo electrónico, país de residencia, etc. y envía éstos al servidor 101. Se apreciará que mientras que en algunas realizaciones de esta invención, los detalles de inscripción se proporcionan directamente al servidor 101, en otras realizaciones, los detalles de inscripción se pueden proporcionar previamente indirectamente para el procesamiento previo anterior a la entrada de los detalles en el servidor 101. Se puede acceder a la página web durante una conexión durante la duración del procedimiento, o de otro modo se pueden usar meramente conexiones seguras solamente cuando está siendo transmitida información sensible (como un conjunto de credenciales o datos adicionales, como un código clave secreto de presentador). También se apreciará que son posibles medios alternativos de inscripción tales como por medio de envío de un formulario completado por correo postal, fax, etc.

Entonces, en el paso 202, se crea una nueva cuenta en el servidor 101 para el solicitante de presentador. Esto se hace generando un nuevo registro de presentador en la colección de registros de presentador. O bien en el paso 200 o bien en el paso 202, se sugiere al nuevo solicitante de presentador que seleccione e introduzca un nuevo código clave secreto de presentador, que entonces se añade al registro de presentador del nuevo solicitante de presentador. En realizaciones alternativas de la invención, el nuevo registro de presentador puede ser dotado automáticamente con un código clave secreto de presentador temporal, que se puede actualizar posteriormente a un código clave secreto de presentador personalizado por el solicitante de presentador a partir de entonces. Tal código clave secreto temporal se puede proporcionar por medio de la página web, o preferiblemente por medio de un segundo canal de comunicación que puede comprender cualquier forma de comunicación, incluyendo correo electrónico, mensajería SMS, llamada telefónica o publicación. En algunas realizaciones de la invención hay un alcance adicional para proporcionar un código clave secreto de sustitución por ejemplo en el caso de que se olvide o comprometa el código clave secreto original. Tales claves secretas de sustitución se pueden proporcionar de manera similar a través de cualquier forma de comunicación incluyendo a través de un sitio web, correo electrónico, SMS, llamada telefónica o publicación.

En el paso 204, se sugiere al nuevo solicitante de presentador que añada conjuntos de credenciales a la cuenta recién creada de un nuevo solicitante de presentador. Como se ha descrito previamente, estos conjuntos de credenciales pueden comprender una variedad de datos personales, y pueden pertenecer a instrumentos de soporte de conjunto de credenciales emitidos por una variedad de diferentes organismos de supervisión gubernamentales o comerciales. Cada conjunto de credenciales se conectará con un alias único a su registro de presentador principal (es decir, cada alias es “localmente único”). En una realización, se puede sugerir en el paso 206 que el nuevo solicitante de presentador proporcione un alias localmente único para cada conjunto de credenciales proporcionado. En otra realización, se puede proporcionar un alias por defecto para cada conjunto de credenciales. En una realización, los alias pueden ser editables posteriormente por el presentador. En algunas realizaciones de la invención, el registro de presentador puede ser editable después de la inscripción en la medida en que los conjuntos de credenciales existentes y los alias conectados se puedan editar o borrar y/o que se puedan añadir nuevos conjuntos de credenciales y alias conectados. En algunas realizaciones de la invención, el registro de interlocutor de presentación puede ser editable después de la inscripción en la medida en que los conjuntos de credenciales existentes y los alias conectados puedan ser editados o borrados y que se puedan añadir nuevos conjuntos de credenciales y alias conectados.

En el paso 206, se da la oportunidad al nuevo solicitante de presentador de establecer preferencias específicas asociadas con el procesamiento y el uso de conjuntos de credenciales asociadas con organismos de supervisión gubernamentales o comerciales particulares y los tipos de interacción a los que pertenecen. A modo de ejemplo, con respecto a un conjunto de credenciales que pertenecen a la afiliación de fidelidad de una aerolínea, se puede dar la opción al presentador de establecer preferencias adicionales según sus preferencias de afiliación, tales como comida, asiento de referencia o aeropuerto local de aerolínea preferida. A modo de ejemplo adicional, con respecto a un conjunto de credenciales que pertenecen a una tarjeta de crédito, se puede dar la opción al presentador de habilitar funcionalidades tales como uso de preferencia de tarjetas, conversión de moneda directa, devolución de impuesto de valor añadido para viajeros o dividir el pago sobre múltiples tarjetas.

En el paso 208, se sugiere entonces al nuevo solicitante de presentador que instale una aplicación a medida en su aparato de presentación 108. La aplicación a medida está configurada para facilitar la comunicación con el servidor, como se requiera durante el proceso de permitir que el servidor libere un conjunto de credenciales y el proceso de autenticación de tal permiso transmitido, como se describirá con mayor detalle a continuación. Durante el transcurso de la instalación de la aplicación a medida, la aplicación se asocia con un identificador de presentador único que se conserva en el aparato de presentación. En una realización preferida, el identificador de presentador se asigna por el servidor, y se incorpora en la aplicación antes, durante o después de que la aplicación se instale en el aparato de presentación. Alternativamente, el identificador de presentador se puede derivar a partir de una secuencia de caracteres nativos del aparato de presentación, por ejemplo, un número de IMEI o un número de serie. Esta secuencia de caracteres se puede modificar para llegar a un identificador de presentador único Además de la retención en el aparato de presentación, el identificador de presentador también se añade al registro de presentador en la recopilación de registros de presentador en el servidor 101. Durante el transcurso de la instalación de la

aplicación a medida, la aplicación también se dota con los alias conectados a los conjuntos de credenciales almacenados en el paso 204 para un presentador dado. Por consiguiente, cuando la aplicación se usa en una interacción por el nuevo presentador, tiene a su disposición tanto un identificador de presentador como los alias conectados a los conjuntos de credenciales del nuevo presentador de manera que el identificador de presentador y un alias se pueden comunicar al servidor 101 según sea adecuado.

En una realización preferida, una versión genérica de la aplicación se puede instalar inicialmente en un aparato de presentación de un nuevo solicitante de presentador. Posterior al proceso representado en los pasos 200-208, se puede sugerir al nuevo solicitante de presentador que autentique su cuenta respondiendo a un correo electrónico, y/o confirmando su código clave secreto de presentador en respuesta a un aviso del servidor. Posterior a esta autenticación, la versión genérica de la aplicación en el aparato de presentación del nuevo solicitante de presentador se puede personalizar con el identificador de presentador del nuevo solicitante de presentador, los alias conectados a los conjuntos de credenciales del nuevo solicitante de presentador, y las preferencias del nuevo solicitante de presentador como se configura en el paso 206. Estos datos se pueden almacenar en un formato cifrado en el aparato de presentación del nuevo solicitante de presentador. La Figura 3 es un diagrama de flujo similar al de la Figura 2 que representa los pasos a través de los cuales una parte puede inscribirse como un aceptador con el servidor ‘101 según una realización de la invención. Como se ha indicado previamente, la invención prevé realizaciones donde el aceptador debe inscribirse activamente con el servidor, así como realizaciones donde no es necesario que el aceptador se inscriba con el servidor Además, en otras realizaciones de la invención, la inscripción del aceptador se puede hacer “pasivamente” como se describirá con mayor detalle a continuación. En el paso 300, se accede a una página web alojada por el servidor 101 por la parte (en lo sucesivo conocida como “nuevo solicitante de aceptador”), preferiblemente usando el aparato de aceptación 109. De una forma análoga al paso 200 de la Figura 2, la página web está configurada de manera que, en este paso, el nuevo solicitante de aceptador proporciona detalles generales de inscripción tales como el nombre del individuo u organización, dirección, dirección de correo electrónico, etc. y envía éstos al servidor 101. Se puede acceder a la página web sobre una conexión segura durante la duración del procedimiento, o de otro modo se pueden usar meramente conexiones seguras solamente cuando esté siendo transmitida información sensible (tal como un código clave secreto de aceptador o un conjunto de credenciales de aceptador). Se apreciará además que la inscripción del nuevo solicitante de aceptador puede tener lugar por medio de otros medios, tales como por correo postal o fax. Alternativamente, si el aceptador opera un aparato de aceptación que está controlado a distancia por un tercero vinculado (tal como, por ejemplo, Sistemas de Gestión de Terminales usados por los Adquirentes para gestionar dispositivos de Punto de Venta de pago con tarjetas, la inscripción de un aceptador se puede iniciar por el tercero vinculado. En tales escenarios, puede no ser necesario para el aceptador proporcionar ninguna información de él mismo.

En el paso 302, se crea una nueva cuenta en el servidor 101 generando un nuevo registro de solicitante de aceptador en la colección de registros de aceptador.

Con el fin de disponer la divulgación de un conjunto de credenciales de presentador, se debe dar permiso como se describe además a continuación. En una realización de la invención, cualquier permiso que emane de un aceptador para la liberación de un conjunto de credenciales de presentador requerirá que el aceptador sea identificado, y por lo tanto, cualquier permiso para la liberación de un conjunto de credenciales de presentador puede requerir la provisión inicial de un conjunto de credenciales de aceptador. Por consiguiente, se prevé que al igual que para los registros de presentador, se requiere un conjunto de credenciales de aceptador separado en un registro de aceptador para cada tipo de interacción en el que un aceptador desee participar. Los tipos de interacción se pueden definir ampliamente - por ejemplo, la liberación de un instrumento de carnet de conducir y la liberación de un instrumento de tarjeta de pago se pueden considerar como tipos de interacción diferentes. Alternativamente, los tipos de interacción se pueden definirse estrechamente - por ejemplo, la liberación de diferentes instrumentos de tarjeta de pago (por ejemplo, Mastercard, Visa de Débito) se puede considerar como tipos de interacción diferentes. Por consiguiente, mientras que en algunas realizaciones, por ejemplo, un conjunto de credenciales de aceptador puede aplicarse de manera general a todas las tarjetas de pago, en otras realizaciones, un aceptador puede tener un conjunto de credenciales diferente para cada tipo de tarjeta de pago diferente manejada por el aceptador.

En el paso 306, se da la oportunidad al nuevo solicitante de aceptador de establecer preferencias específicas asociadas con el procesamiento y uso de conjuntos de credenciales asociados con tipos de interacción particulares. A modo de ejemplo, con respecto a un conjunto de credenciales que pertenecen a una tarjeta de crédito, se puede dar la opción al nuevo solicitante de aceptador de indicar si desea proporcionar funcionalidades posteriores asociadas con el conjunto de credenciales una vez que el conjunto de credenciales de aceptador se haya liberado, tales como conversión de moneda directa, reembolso del impuesto de valor añadido para los viajeros o división del pago sobre múltiples tarjetas.

En el paso 308, el aparato de aceptación se configura entonces de manera que pueda comunicarse con el servidor. Esto se puede hacer de una variedad de formas. En realizaciones de la invención donde el aparato de aceptación se controla remotamente por un tercero, el tercero puede iniciar una reconfiguración automática del aparato de aceptación si se requiere. En otras realizaciones de la invención, el nuevo solicitante de aceptador puede iniciar la reconfiguración a través de la instalación de una aplicación a medida de una manera similar a la descrita en la Figura 2.

La Figura 4 es un diagrama de flujo que ilustra el método de permitir la liberación de al menos un conjunto de credenciales controladas conectadas a un presentador mientras que se mantiene la privacidad que prevalece en dichas credenciales según una realización de la invención. El servidor de control recibe una comunicación de aparato de aceptación que contiene un código clave secreto y un código clave compartido de uso único y una comunicación de aparato de presentación que contiene un identificador de presentación y un código clave compartido de uso único. En el paso 403, se comparan los mensajes de comunicación. Una coincidencia fallida finaliza el método y no se completa la instrucción de interacción. Si los códigos clave compartidos coinciden, en el paso 404 se inicia una búsqueda de un registro objetivo en el servidor vinculando el código clave secreto y el identificador de presentador Una búsqueda de cualquier registro objetivo que comprende el mismo identificador de presentador y código clave secreto como contenidos en la comunicación de aparato de aceptación y la comunicación de aparato de presentación. Si se encuentra un registro objetivo, el conjunto de credenciales que pertenece a la ubicación de almacenamiento presente en el registro se recupera y se permite que sea liberado a un destino designado que es el punto final de red.

Las Figuras 5A y 5B describen el proceso realizado en el aparato de aceptación. Un código clave compartido de uso único se genera por el aparato de aceptación y se transporta al aparato de presentación. El aparato de aceptación recibe además el código clave secreto de presentador y genera una comunicación a ser enviada al servidor de control como se representa por 101 en la figura 1. La citada comunicación comprende el código clave secreto de presentador y el código clave compartido de uso único.

Las Figuras 6A y 6B describen el proceso realizado en el aparato de presentación. El identificador de presentador se recupera de la memoria. Al recibir el código clave compartido de uso único del aparato de aceptación, se transmite una comunicación que comprende el identificador de presentador y el código clave compartido de uso único al servidor de control 101. La figura 7 y la figura 8 son una representación de entradas que pertenecen a las credenciales controladas conectadas al presentador. Cada una de las entradas está asociada con un identificador de presentador y un código clave secreto. Las Figuras 7A a 7E representan diversas realizaciones de registros de almacenamiento en el servidor de control o el servidor de credenciales 101. En algunas realizaciones, los registros de interlocutores de presentación se pueden enmascarar y localizar usando listas de búsqueda como se describe en las figuras 7A y 7C. Puede haber otra realización en donde cada registro de interlocutor de presentador está asociado con un alias.

Las Figuras 9A y 9B describen representaciones gráficas que pertenecen al proceso de comunicación de mensajes al servidor de control desde los interlocutores de presentación y aceptación y el proceso de envío de credenciales controladas a destinos permitidos. La Figura 10 es un diagrama de secuencias que ilustra el proceso por el cual se puede dar permiso según una realización de la invención que implica un servidor 1001, un interlocutor de presentación 1002, un aparato de presentación 1003, un punto final de red 1004, y un aparato de aceptación 1005, para recuperar un conjunto de credenciales en almacenamiento en una ubicación identificada por el interlocutor de presentación 1002 y liberar un conjunto de credenciales a una instalación de un destinatario permitido por el interlocutor de presentación 1002. Se apreciará que dar permiso para recuperar y liberar un conjunto de credenciales de presentador también se puede acompañar con una solicitud para recuperar un conjunto de credenciales de aceptador simultáneamente, en donde el aparato de aceptación 1005 y el aparato de presentación 1003 todavía envían sus respectivas comunicaciones al Servidor 1001. Se apreciará además que en algunas realizaciones de la invención, el permiso para liberar el conjunto de credenciales será específicamente un permiso para liberar un conjunto de credenciales de presentador (asociado con un interlocutor de presentación 1002) al punto final de red 1004 o a un aparato de aceptación 1005. No obstante, en otras realizaciones de la invención, el permiso será compartir el conjunto de credenciales de aceptador o de presentador con el de un tercero de confianza vinculado al punto final de red 1004 o el aparato de aceptación 1005. Por ejemplo, cuando se envía el permiso para compartir un conjunto de credenciales de presentador que pertenece a un instrumento de tarjeta de pago; puede ser que se pretenda que el conjunto de credenciales de la tarjeta de pago sea enviado a un procesador de transacciones de terceros de confianza.

En la Figura 10, un interlocutor de presentación 1002 que posee un aparato de presentación 1003 configurado para generar y transmitir una comunicación de aparato de presentación al servidor 1001, identifica una instalación que opera en un interlocutor de aceptación que comprende un punto final de red 1004 o/y aparato de aceptación 1005 (en donde el punto final de red 1004 es un aparato de aceptación 1005, o en donde el punto final de red 1004 está vinculado a un aparato de aceptación 1005), y por el cual el aparato de aceptación 1005 está configurado para generar y transmitir una comunicación de aparato de aceptación al servidor 1001. El interlocutor de presentación 1002 puede decidir interactuar en tal instalación con vistas a permitir que una lectura de un conjunto de credenciales conectadas al interlocutor de presentación 1002 sea liberada al punto final de red 1004 o al aparato de aceptación 1005. El interlocutor de aceptación también puede decidir interactuar en tal instalación con vistas a solicitar que una lectura de un conjunto de credenciales conectadas al interlocutor de aceptación sea devuelta al punto final de red 1004 o al aparato de aceptación 1005 cuando se recibe el conjunto de credenciales conectadas al interlocutor de presentación 1002 en el punto final de red 1004 o el aparato de aceptación 1005. Más específicamente, un estado de privacidad que prevalece en las credenciales conectadas al interlocutor de presentación 1002 se conserva en la realización preferida de la presente invención, por el cual una lectura del conjunto de credenciales conectadas al interlocutor de presentación 1002 no es visible a o accesible por el interlocutor de aceptación ni comunicada a o por

el aparato de presentación 1003, sino solamente comunicada de manera confidencial al punto final de red 1004 o al aparato de aceptación 1005.

En la Figura 10, y en el caso precedente 1010, se transporta una señal al punto final de red 1004 o al aparato de aceptación 1005 para un interlocutor de presentación 1002, indicando que dicho método ideado en la presente invención es un método disponible en el punto final de red 1004 o el aparato de aceptación 1005 para el interlocutor de presentación 1002, por el cual el punto final de red 1004 está equipado con tal aparato de aceptación 1005 y en donde tal aparato de aceptación 1005 está configurado para comunicarse con el Servidor 1001. En efecto, el citado método ideado en la presente invención es uno de los métodos disponibles en el punto final de red 1004 para obtener credenciales del interlocutor de presentación 1002.

En la Figura 10, y en el caso precedente 1011, un interlocutor de presentación 1002 decide iniciar una interacción en la instalación operada en el interlocutor de aceptación según el proceso del método ideado por la presente invención haciendo uso del aparato de presentación 1003 configurado para generar y transmitir una comunicación de aparato de presentación a tal servidor 1001, y haciendo uso de un aparato de aceptación 1005, configurado para generar y transmitir una comunicación de aparato de aceptación a tal servidor 1001. En efecto, el interlocutor de presentación 1002 selecciona iniciar una interacción en la instalación del interlocutor de aceptación según el proceso del método ideado por la presente invención, declinando iniciar una interacción en la instalación operada en el interlocutor de aceptación según cualquier otro proceso de métodos anteriores disponibles en el punto final de red 1004 para obtener las credenciales del interlocutor de presentación 1002.

En la etapa 1012, se inicia una interacción activando el aparato de aceptación 1005 que está configurado para facilitar las comunicaciones de aparato de aceptación con el servidor 1001. En la activación en 1012, se produce 1012 un código clave compartido de uso único en el aparato de aceptación 1005. En una realización, el código clave compartido se genera por el servidor 1001 y se transmite al aparato de aceptación 1005. En otra realización, el código clave compartido se genera en el aparato de aceptación 1005.

En la etapa 1013, se inicia una interacción activando el aparato de presentación 1003 que facilita las comunicaciones de aparato de presentación con el servidor 1001. En la activación en 1013, se recupera un identificador de presentador de una ubicación de almacenamiento en el aparato de presentación 1003 En una realización, una lista de alias asociados con las credenciales conectadas al interlocutor de presentación 1002 relacionado con el identificador de presentador también se recupera de alguna ubicación de almacenamiento en el aparato de presentación 1003. En tal realización, tal lista de alias asociados con las credenciales conectadas con el interlocutor de presentación se detalla en el aparato de presentación 1003 para selección por el interlocutor de presentación 1002.

En la etapa 1014, se pone a disposición un código clave compartido en el aparato de aceptación 1005 para el interlocutor de presentación 1002 y para el aparato de presentación 1003. En una realización de 1014, se hace legible para el ser humano en el aparato de aceptación 1005. En otra realización de 1014, se hace legible por máquina en el aparato de aceptación 1005.

En la etapa 1015, el código clave compartido se obtiene por consiguiente en el aparato de presentación 1003. En una realización, se obtiene leyéndolo en el aparato de aceptación 1005 e introduciéndolo en el aparato de presentación 1003. En otra realización, se obtiene escaneándolo en el aparato de aceptación 1005 y capturándolo en el aparato de presentación 1003. En una realización, el aparato de aceptación 1005 transmite el código clave compartido de uso único directamente 1014 al aparato de presentación 1003, mientras que en otra realización, el aparato de aceptación 1005 pone a disposición 1014 el código clave compartido para el interlocutor de presentación 1002, quien lo introduce en 1016 en el aparato de presentación 1003. En algunas realizaciones de la invención, se puede asignar un período de validez al código clave compartido. Esto asegura que si una comunicación de aparato de aceptación recibida y una comunicación de aparato de presentación recibida no se corroboran dentro de un cierto intervalo de tiempo buscando hacer coincidir los códigos clave compartidos de uso único (como se trata además a continuación) dentro de un cierto intervalo de tiempo (el período de validez), entonces la interacción puede caducar y, por ello, quedar sin efecto, haciendo los procesos adicionales redundantes. A la expiración del período de validez de un código clave compartido, el mismo código clave compartido se puede reutilizar de esta manera en una iteración posterior del método. Por consiguiente, un período de validez puede asegurar que se puedan usar claves secretas más cortas y menos complejas debido a que la reutilización de códigos clave compartidos es por ello factible. Esto es ventajoso en realizaciones de la invención donde es necesario para el interlocutor de presentación introducir el código clave compartido en el aparato de presentación 1003, en la medida que una complejidad reducida del código clave hace esta realización del método más manejable.

En algunas realizaciones, el aparato de presentación 1003 también puede mostrar una lista de alias que pertenecen a diferentes conjuntos de credenciales de presentador conectadas a dicho interlocutor de presentación 1002. El interlocutor de presentación 1002 entonces selecciona un alias asociado con el conjunto de credenciales deseadas conectadas al interlocutor de presentación 1002.

En la etapa 1016, el aparato de aceptación busca obtener el código clave secreto del interlocutor de presentación 1002 sugiriendo al interlocutor de presentación 1002 introducir el código clave secreto de presentador en el aparato

de aceptación 1005. En una realización, el aparato de aceptación 1005 puede mostrar adicionalmente en 1012 un parámetro auxiliar predeterminado para el interlocutor de presentación 1002 con el fin de correlacionar además la interacción y corroborar la comunicación de aparato de aceptación y la comunicación de aparato de presentación.

En 1017, el código clave secreto se obtiene por el aparato de aceptación 1005. En una realización, el interlocutor de presentación 1002 usa un teclado numérico para introducir el código clave secreto en el aparato de aceptación 1005. En otra realización, el interlocutor de presentación 1002 puede usar un dispositivo para trasladar el código clave secreto al aparato de aceptación 1005.

En la etapa 1019, el aparato de aceptación 1005 transmite entonces una comunicación de aparato de aceptación al servidor 1001 que permite la liberación de un conjunto o conjuntos de credenciales específicas conectadas al interlocutor de presentación 1003 a la instalación del destinatario permitido por el interlocutor de presentación 1002. La comunicación de aparato de aceptación contiene el código clave secreto de presentador como se obtiene en 1017 y el código clave compartido de uso único como se genera en 1012. La comunicación de aparato de aceptación también puede contener un identificador que pertenece al interlocutor de aceptación si se recupera siguiendo 1012 y cualquier parámetro predeterminado auxiliar si se captura siguiendo 1012.

En la etapa 1018, el aparato de presentación 1003 transmite una comunicación de aparato de presentación al servidor 1001 permitiendo la recuperación del conjunto o conjunto de credenciales específicas conectadas al interlocutor de presentación 1002, en almacenamiento en la ubicación identificada por el interlocutor de presentación 1002. La comunicación de aparato de presentación contiene un identificador de presentador recuperado en 1013 y el código clave compartido de uso único obtenido en 1015. La comunicación de aparato de presentación también puede contener un alias asociado con el conjunto de credenciales elegidas si se detalla en 1013 y se selecciona en 1016, y también puede contener cualquier parámetro auxiliar predeterminado si se captura siguiendo 1016.

En 1020, el servidor 1001 busca hacer coincidir las comunicaciones de aparato de aceptación recibidas y las comunicaciones de aparato de presentación recibidas buscando hacer coincidir el código clave compartido de uso único contenido en las comunicaciones de aparato de aceptación y el código clave compartido de uso único contenido en las comunicaciones de aparato de presentación. En algunas realizaciones, se pueden asignar a la comunicación de aparato de aceptación y/o a la comunicación de aparato de presentación un período de validez 1020. Si la comunicación de aparato de aceptación y las comunicaciones de aparato de presentación no se hacen coincidir dentro del período de validez designado, la interacción caduca y se considerará nula haciendo los procesos adicionales redundantes. Cuando una interacción caduca y queda sin efecto haciendo los procesos adicionales redundantes, los datos que pertenecen a la interacción (es decir, las comunicaciones de interlocutor) se pueden purgar del sistema, liberando recursos para el procesamiento de permisos recibidos adicionales. En otras realizaciones, un valor o parámetros auxiliares predeterminados pueden haber estado contenidos en la comunicación de aparato de aceptación en 1019 y la comunicación de aparato de presentación en 1018. Si es así, el valor se usa además del código clave compartido como el parámetro auxiliar predeterminado para buscar una coincidencia de una comunicación de aparato de aceptación y una comunicación de aparato de presentación en 1020.

En la etapa 1021, y en caso de que se encuentre una coincidencia en 1020, el servidor 1001 inicia una búsqueda vinculando 1021 el identificador de presentación contenido en la comunicación de aparato de presentación y el código clave secreto contenido en la comunicación de aparato de aceptación, en donde el código clave compartido contenido en la comunicación de aparato de presentación es el mismo que el código clave compartido contenido en la comunicación de aparato de aceptación según 1020. Si no se encuentra ninguna coincidencia en 1020, el método no procede de esta manera con 1021, y el servidor 1001 puede devolver un mensaje en consecuencia al aparato de aceptación 1005 o al aparato de presentación 1003.

En la etapa 1022, el servidor 1001 dirige una búsqueda de un registro objetivo dentro de su colección de registros de presentador que comprende el identificador de presentador contenido en la comunicación de aparato de presentación coincidente y el código clave secreto contenido en la comunicación de aparato de aceptación coincidente. En una realización, y en el caso 1022, un alias asociado al identificador de presentador está contenido en la comunicación de aparato de presentación según 1018, el alias también se usa para averiguar 1022 un registro objetivo que comprende ese alias además del identificador de presentador y del código clave secreto del interlocutor de presentación 1002.

En la etapa 1023, y en el caso de que un registro que comprende el identificador de presentador y el código clave secreto de presentador esté situado en 1022, se continúa una búsqueda identificando 1023 una entrada afiliada al registro objetivo situado en 1022, en donde la entrada pertenece al conjunto de credenciales conectadas al interlocutor de presentación 1002. (En una realización, el conjunto de credenciales en cuestión puede ser el conjunto de credenciales conectadas al alias seleccionado por el interlocutor de presentación 1002 en el paso 1022). En una realización, la entrada identificada contiene una lectura que comprende las credenciales conectadas con el interlocutor de presentación 1002. En otra realización, la entrada identificada contiene un puntero que localiza las credenciales conectadas al interlocutor de presentación 1002. En caso de que un registro que comprende el identificador de presentador y el código clave secreto de presentador no se localice en el paso 1022, el proceso no

procede de esta manera con 1023 y el servidor 1001 puede devolver un mensaje en consecuencia al aparato de aceptación 1005 y/o al aparato de presentación 1003.

En 1024, se completa una búsqueda permitiendo una recuperación de una lectura de las credenciales conectadas al interlocutor de presentación 1002 en almacenamiento en la ubicación identificada en 1023, y permitiendo una liberación de la lectura de las credenciales conectadas con el interlocutor de presentación a las instalaciones del destinatario permitido por el interlocutor de presentación 1002.

En la etapa 1025, se recupera una lectura del almacenamiento en la ubicación indicada por el interlocutor de presentación 1002. En una realización, se almacena y recupera 1025 una lectura en el servidor de control configurado para realizar el método ideado en 1020 a 1024. En otra realización, se almacena y recupera 1025 una lectura en otro servidor diferente al servidor de control configurado para realizar el método ideado en 1020 a 1024.

En la etapa 1026, se libera 1026 una lectura de las credenciales a la instalación del destinatario permitido por el interlocutor de presentación 1002. En una realización, la lectura se libera y se envía al punto final de red 1004. En otra realización, se libera y se envía la lectura al dispositivo de aceptación 1005.

En la Figura 10, y como los casos posteriores a 1027 y 1028, se devuelve un mensaje por el servidor 1001 al aparato de presentación 1003 para el interlocutor de presentación 1002, indicando si la lectura ha sido recuperada como identificada y liberada en la medida de lo permitido por el interlocutor de presentación 1002; en tales realizaciones suplementarias, se conserva un registro en el servidor 1001 que enumera un estado de eventos que ocurren entre 1020 y 1024, como revisable por el interlocutor de presentación 1002 en el aparato de presentación 1003.

Las realizaciones en la invención descrita con referencia a los dibujos comprenden un aparato informático y/o procesos realizados en un aparato informático. No obstante, la invención también se extiende a programas de ordenador, particularmente programas de ordenador almacenados en un portador adaptado para llevar la invención a la práctica. El programa puede ser en forma de código fuente, código objeto, o una fuente intermedia de código y código objeto, tal como en forma parcialmente compilada o en cualquier otra forma adecuada para uso en la implementación del método según la invención. El portador puede comprender un medio de almacenamiento tal como ROM, por ejemplo, CD ROM, o medio de registro magnético, por ejemplo, un disquete o un disco duro. El portador puede ser una señal eléctrica u óptica que se puede transmitir a través de un cable eléctrico o uno óptico o mediante radio u otros medios.

Las palabras “comprende/que comprende” y, las palabras “que tiene/que incluye” cuando se usan en la presente memoria con referencia a la presente invención se usan para especificar la presencia de rasgos, enteros, pasos o componentes fijados pero no excluyen la presencia o adición de uno o más rasgos, enteros, pasos, componentes o grupos de los mismos.

Se aprecia que ciertos rasgos de la invención, que, por claridad, se describen en el contexto de realizaciones separadas, también se pueden proporcionar en combinación en una única realización. Por el contrario, diversos rasgos de la invención que, por brevedad, se describen en el contexto de una única realización, también se pueden proporcionar por separado o en cualquier subcombinación adecuada.

REIVINDICACIONES

1. Un sistema (100) para permitir una comunicación de al menos un conjunto de credenciales controladas conectadas a un presentador desde un servidor a un punto final de red, dicho sistema que comprende:

al menos un punto final de red;

al menos un aparato de aceptación (109) configurado para enviar una comunicación de aparato de aceptación (104), dicha comunicación de aparato de aceptación que contiene un código clave secreto (109a) que pertenece a dicho presentador y un código clave compartido de uso único (109b);

al menos un aparato de presentación (108) configurado para enviar una comunicación de aparato de presentación (105), dicha comunicación de aparato de presentación que contiene un identificador de presentador (108a) que pertenece a dicho presentador y dicho código clave compartido de uso único (108b);

al menos un servidor que comprende además un procesador, al menos una interfaz de comunicaciones y memoria que almacena al menos una entrada (103) que pertenece a dicho al menos un conjunto de credenciales controladas conectadas, cada entrada que está afiliada a al menos un registro (102), el registro que pertenece a cualquier presentador y comprende un identificador de presentador y un código clave secreto unido al identificador de presentador;

en donde dicho al menos un servidor está configurado para:

a) recibir dicha comunicación de aparato de aceptación (104);

b) recibir dicha comunicación de aparato de presentación (105);

c) buscar un coincidencia de dicho código clave compartido de uso único (109b) contenido en dicha comunicación de aparato de aceptación (104) con dicho código clave compartido de uso único (108b) contenido en dicha comunicación de aparato de presentación (105);

d) iniciar una búsqueda de un registro objetivo vinculando dicho código clave secreto en dicha comunicación de aparato de aceptación (104) con dicho identificador de presentador en dicha comunicación de aparato de presentación (105), tanto dicha comunicación de aparato de aceptación como dicha comunicación de aparato de presentación que contiene el mismo código clave compartido de uso único (108b, 109b);

e) dirigir la búsqueda de dicho registro objetivo que comprende tanto dicho código clave secreto (109a) como dicho identificador de presentador (108a);

f) identificar una entrada (103) afiliada con dicho registro objetivo;

g) permitir la recuperación de dicho al menos un conjunto de credenciales controladas conectadas que pertenecen a dicha entrada (103 y permitir la liberación de dicho al menos un conjunto de credenciales controladas conectadas a dicho punto final de red (110), dicho punto final de red que es un destinatario permitido de un tipo de dicho al menos un conjunto de credenciales controladas conectadas.

2. El sistema de la reivindicación 1, en donde dicho al menos un servidor comprende un servidor de control (101).

3. El sistema de la reivindicación 2, en donde el servidor de control (101) está configurado además para generar dicho código clave compartido de uso único, y hacer que esté disponible en el aparato de aceptación (109).

4. El sistema de la reivindicación 2, en donde dicho aparato de aceptación está configurado además para generar dicho código clave compartido de uso único, recibir dicho código clave secreto (109a) de dicho presentador y transmitir dicha comunicación de aparato de aceptación a dicho servidor de control (101).

5. El sistema de la reivindicación 3, en donde dicho aparato de presentación está configurado además para recibir dicho código clave compartido de uso único de dicho aparato de aceptación (109), recuperar dicho identificador de presentador de su memoria y transmitir dicha comunicación de aparato de presentación (105) a dicho servidor de control (101).

6. El sistema de cualquiera de las reivindicaciones precedentes, en donde dicho registro que comprende dicho identificador de presentador y dicho código clave secreto comprende además un alias asociado al identificador de presentador y afiliado a dicha entrada (103) que pertenece a dicho al menos un conjunto de credenciales controladas conectadas.

7. El sistema de cualquiera de las reivindicaciones precedentes, en donde dicha comunicación de aparato de presentación contiene además un alias asociado a dicho identificador de presentador y afiliado a dicha entrada (103) que pertenece a dicho al menos un conjunto de credenciales controladas conectadas, y en donde dicha búsqueda de dicho registro objetivo además utiliza dicho alias contenido en dicha comunicación de aparato de presentación

(105) para buscar dicho registro objetivo que comprende dicho alias además de comprender dicho identificador de presentador (108a) y dicho código clave secreto.

8. El sistema de cualquiera de las reivindicaciones precedentes, en donde dicho punto final de red comprende dicho aparato de aceptación (109) y está configurado como un destinatario designado de uno o más tipos de dicho al menos un conjunto de credenciales controladas conectadas.

9. El sistema de cualquiera de las reivindicaciones 1 a 7, en donde dicho punto final de red está vinculado a dicho aparato de aceptación y está configurado como un destinatario designado de uno o más tipos de dicho al menos un conjunto de credenciales controladas conectadas.

10. El sistema de la reivindicación 2, en donde dicho al menos un conjunto de credenciales controladas conectadas comprende una entrada en dicho registro objetivo (102) de dicho servidor de control (101).

11. El sistema de la reivindicación 2, en donde dicho al menos un conjunto de credenciales controladas conectadas comprende una entrada en otro de dicho al menos un servidor que está afiliado a dicho registro objetivo en dicho servidor de control (101).

12. El sistema de cualquiera de las reivindicaciones precedentes, en donde un periodo de validez se asigna a dicha comunicación de aparato de aceptación (104), y en donde el paso c) además comprende establecer si ha expirado dicho periodo de validez.

13. El sistema de cualquiera de las reivindicaciones 1 a 11, en donde un periodo de validez se asigna a dicha comunicación de aparato de presentación (105), y en donde el paso c) comprende además establecer si ha expirado dicho periodo de validez.

14. El sistema de cualquiera de las reivindicaciones 1 a 11, en donde un periodo de validez se asigna a dicho código clave compartido de uso único, y en donde el paso c) comprende además establecer si ha expirado dicho periodo de validez.

15. El sistema de la reivindicación 14, en donde dicho código clave compartido de uso único es único durante la duración de su periodo de validez.

16. El sistema de cualquiera de las reivindicaciones precedentes, en donde dicha comunicación de aparato de aceptación (104) además contiene uno o más parámetros auxiliares predeterminados, y dicha comunicación de aparato de presentación también comprende además dicho uno o más parámetros auxiliares predeterminados.

17. El sistema de la reivindicación 16, cuando es dependiente de cualquiera de las reivindicaciones 2 a 5, en donde dicho servidor de control (101) busca hacer coincidir al menos uno de dichos parámetros auxiliares predeterminados de dicha comunicación de aparato de presentación (105) con dicho parámetro o parámetros auxiliares predeterminados correspondientes de dicha comunicación de aparato de aceptación (104) para proporcionar además al menos una de: correlación y corroboración.

18. El sistema de cualquiera de las reivindicaciones 2 a 5, en donde, si dichos registros comprenden entradas de al menos un conjunto de credenciales controladas conectadas en dicho servidor de control (101), los pasos f) y g) se realizan en dicho servidor de control, y la comunicación de dicho al menos un conjunto de credenciales controladas conectadas se realiza desde dicho servidor de control.

19. El sistema de cualquiera de las reivindicaciones 2 a 5, en donde, si dichos registros comprenden entradas de al menos un conjunto de credenciales controladas conectadas en un servidor diferente de dicho servidor de control, los pasos f) y g) se realizan en dicho servidor diferente, y la comunicación de dicho al menos un conjunto de credenciales controladas conectadas se realiza usando uno de: dicho servidor de control y dicho servidor diferente.

20. El sistema de cualquiera de las reivindicaciones 2 a 5, en donde, si no se encuentra ninguna coincidencia entre dicha comunicación de aparato de aceptación (104) y comunicación de aparato de presentación (105) en dicho servidor de control (101), dicho servidor de control termina además las acciones configuradas y registra tal estado en el mismo.

21. El sistema de cualquiera de las reivindicaciones 2 a 5, en donde, si no se encuentra ningún registro objetivo en dicho servidor de control (101), dicho servidor de control termina además las acciones configuradas y registra tal estado en el mismo.

22. El sistema de cualquiera de las reivindicaciones 2 a 5, en donde dicho servidor de control (101) está configurado además para registrar el estado de los eventos que ocurren y retransmitir tal estado a al menos uno de: dicho aparato de aceptación (109), y dicho aparato de presentación (108).

23. El sistema de cualquiera de las reivindicaciones precedentes, en donde cada uno de dichos servidores, puntos finales de red (110), y aparatos de presentación y aceptación (108, 109) cada uno comprende además al menos uno de: un procesador, interfaces de comunicación, memoria, consolas de entrada y consolas de salida.

24. El sistema de cualquiera de las reivindicaciones precedentes, en donde el sistema es operable sobre una red de comunicaciones (106, 107, 111).

25. Un método para permitir una comunicación de al menos un conjunto de credenciales controladas conectadas a un presentador desde al menos un servidor a un punto final de red (110), dicho método que comprende los siguientes pasos realizados en al menos un servidor:

(a) recibir una comunicación de aparato de aceptación (104), dicha comunicación que contiene un código clave secreto (109a) que pertenece a dicho presentador y un código clave compartido de uso único (109b);

(b) recibir una comunicación de aparato de presentación (105), dicha comunicación que contiene un identificador de presentador (108a) que pertenece a dicho presentador y código clave compartido de uso único (108b);

(c) buscar una coincidencia de dicho código clave compartido de uso único (109b) contenido en dicha comunicación de aparato de aceptación (104) y dicho código clave compartido de uso único (108b) contenido en dicha comunicación de aparato de presentación (105);

(d) iniciar una búsqueda de un registro objetivo vinculando dicho código clave secreto (109a) de dicha comunicación de aparato de aceptación (104) y dicho identificador de presentador (108a) en dicha comunicación de aparato de presentación (105), tanto dicha comunicación de aparato de aceptación como dicha comunicación de aparato de presentación que contiene el mismo código clave compartido de uso único (108b, 109b);

(e) dirigir la búsqueda del registro objetivo que comprende tanto dicho código clave secreto (109a) como dicho identificador de presentador (108a);

(f) identificar una entrada (103) afiliada con dicho registro objetivo, dicha entrada que pertenece a dicho al menos un conjunto de credenciales controladas conectadas; y

(g) permitir una recuperación de dicho al menos un conjunto de credenciales controladas conectadas que pertenecen a dicha entrada y que permiten una liberación de dicho conjunto de credenciales controladas conectadas a dicho punto final de red (110), dicho punto final de red que es un destinatario permitido de dicho al menos un conjunto de credenciales controladas conectadas.

26. El método de la reivindicación 25, en donde el registro objetivo que comprende dicho identificador de presentador (108a) y código clave secreto (109a) comprende además un alias asociado a dicho identificador de presentador (108a) y afiliado a dicha entrada (103) que pertenece a dicho al menos un conjunto de credenciales controladas conectadas, y dicha comunicación de aparato de presentación (105) además contiene un alias asociado a dicho identificador de presentador (108a) y afiliada a dicha entrada que pertenece a dicho al menos un conjunto de credenciales controladas conectadas, y en donde el paso (e) comprende además hacer coincidir los alias respectivos de dicho registro y dicha comunicación de aparato de presentación.

27. El método de la reivindicación 25 o 26, en donde dicho al menos un servidor comprende un servidor de control (101) y los pasos (a) a (g) se realizan en el mismo.

28. El método de la reivindicación 25 o 26, en donde dicho al menos un servidor comprende un servidor de control (101) y dicho al menos un conjunto de credenciales controladas conectadas comprende una entrada en un servidor diferente a dicho servidor de control (101), dicha entrada que está afiliada con dicho registro objetivo, y en donde el paso de identificación de un conjunto de credenciales se realiza en dicho servidor diferente, y en donde los pasos (e) a (g) se realizan en uno de: dicho servidor de control (101) y dicho servidor diferente.

29. El método de cualquiera de las reivindicaciones 25 a 28, que comprende además asignar un periodo de validez a al menos uno de: comunicación de aparato de aceptación (104), dicha comunicación de aparato de presentación (105) y dicho código clave de uso único, y el paso (c) comprende además establecer si ha expirado dicho periodo de validez.

30. El método de la reivindicación 29, en donde dicho código clave compartido de uso único es único durante la duración de su periodo de validez.

31. El método de cualquiera de las reivindicaciones 25 a 29, en donde cada una de dicha comunicación de aparato de presentación (105) y dicha comunicación de aparato de aceptación (104) contiene además uno o más parámetros auxiliares predeterminados, y en donde el paso (c) además comprende buscar una coincidencia de al menos uno de dichos parámetros auxiliares predeterminados en dicha comunicación de aparato de presentación con al menos uno de los parámetros auxiliares predeterminados correspondientes en dicha comunicación de aparato de aceptación.

32. El método de la reivindicación 27, en donde, si dichos registros comprenden entradas de al menos un conjunto de credenciales controladas conectadas en dicho servidor de control (101), realizar los pasos (f) y (g) en dicho servidor de control, y el método comprende además la liberación de dicho al menos un conjunto de credenciales controladas conectadas de dicho servidor de control.

33. El método de la reivindicación 25 o 26, en donde dicho al menos un servidor comprende un servidor de control (101), y, si dichos registros comprenden entradas de al menos un conjunto de credenciales controladas conectadas en un servidor diferente a dicho servidor de control (101), realizar los pasos (f) y (g) en dicho servidor diferente, y el método comprende además liberar dicho al menos un conjunto de credenciales controladas conectadas de uno de: dicho servidor de control y dicho servidor diferente.

34. El método de la reivindicación 27 o 28, en donde, si no se encuentra ninguna coincidencia entre dicha comunicación de aparato de aceptación (104) y la comunicación de aparato de presentación (105), terminar las acciones configuradas adicionales y registrar tal estado en dicho servidor de control (101).

35. El método de las reivindicaciones 27 o 28, en donde, si no se encuentra ningún registro objetivo, terminar las acciones configuradas adicionales y registrar tal estado en dicho servidor de control (101).

36. El método de la reivindicación 27 o 28, que comprende además registrar el estado de los eventos en dicho servidor de control (101) y retransmitir tal estado a al menos uno de: dicho aparato de aceptación (109) y dicho aparato de presentación (108).

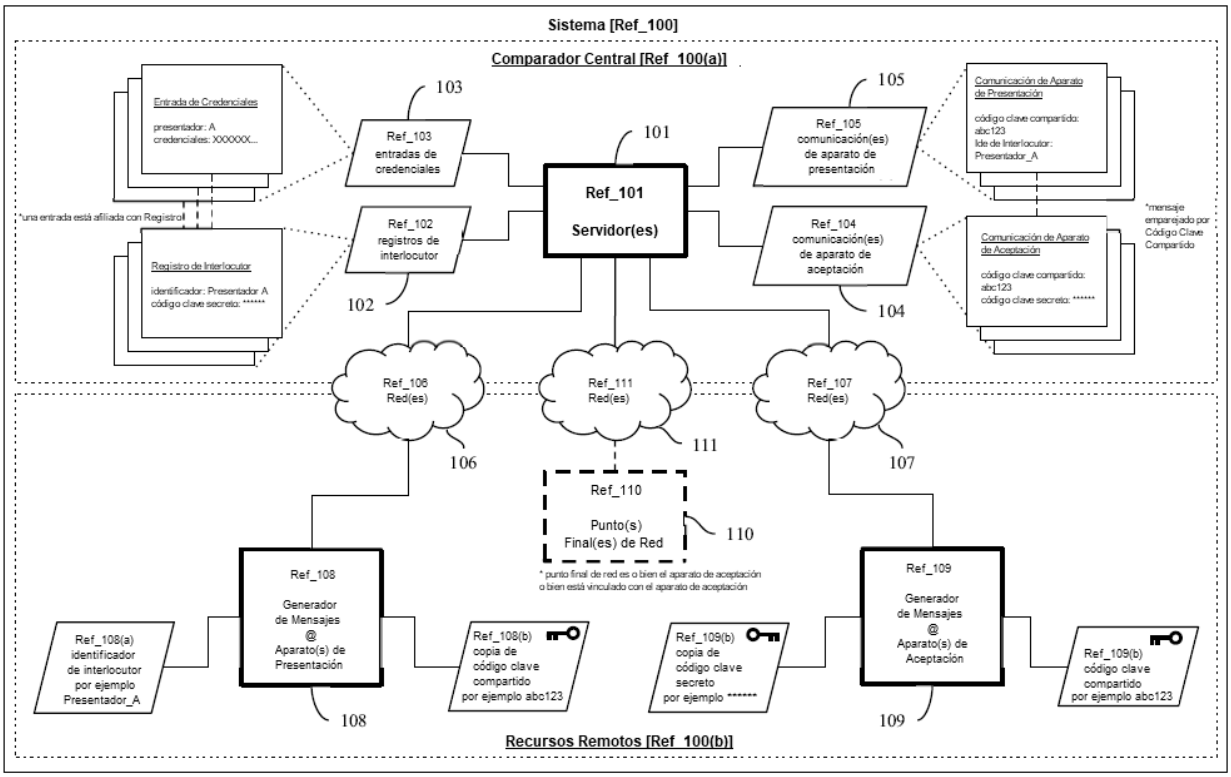

Sistema [Ref_100]
Comparador Central [Ref_100(a)]
Entrada de Credenciales
presentador: A
credenciales: XXXXXX...
*una entrada está afiliada con Registro
Registro de Interlocutor
identificador: Presentador A
código clave secreto: ******
Ref_103
entradas de credenciales
103
Ref_102
registros de interlocutor
102
Ref_101
Servidor(es)
101
Ref_105
comunicación(es) de aparato de presentación
105
Ref_104
comunicación(es) de aparato de aceptación
104
Comunicación de Aparato de Presentación
código clave compartido: abc123
Ide de Interlocutor: Presentador_A
Comunicación de Aparato de Aceptación
código clave compartido: abc123
código clave secreto: ******
*mensaje emparejado por Código Clave Compartido
Ref_106
Red(es)
106
Ref_111
Red(es)
111
Ref_107
Red(es)
107
Ref_110
Punto(s) Final(es) de Red
110
* punto final de red es o bien el aparato de aceptación o bien está vinculado con el aparato de aceptación
Ref_108
Generador de Mensajes @ Aparato(s) de Presentación
108
Ref_108(a)
identificador de interlocutor por ejemplo Presentador_A
Ref_108(b)
copia de código clave compartido por ejemplo abc123
Ref_109(b)
copia de código clave secreto por ejemplo ******
Ref_109
Generador de Mensajes @ Aparato(s) de Aceptación
109
Ref_109(b)
código clave compartido por ejemplo abc123
Recursos Remotos [Ref_100(b)]

Fig. 1

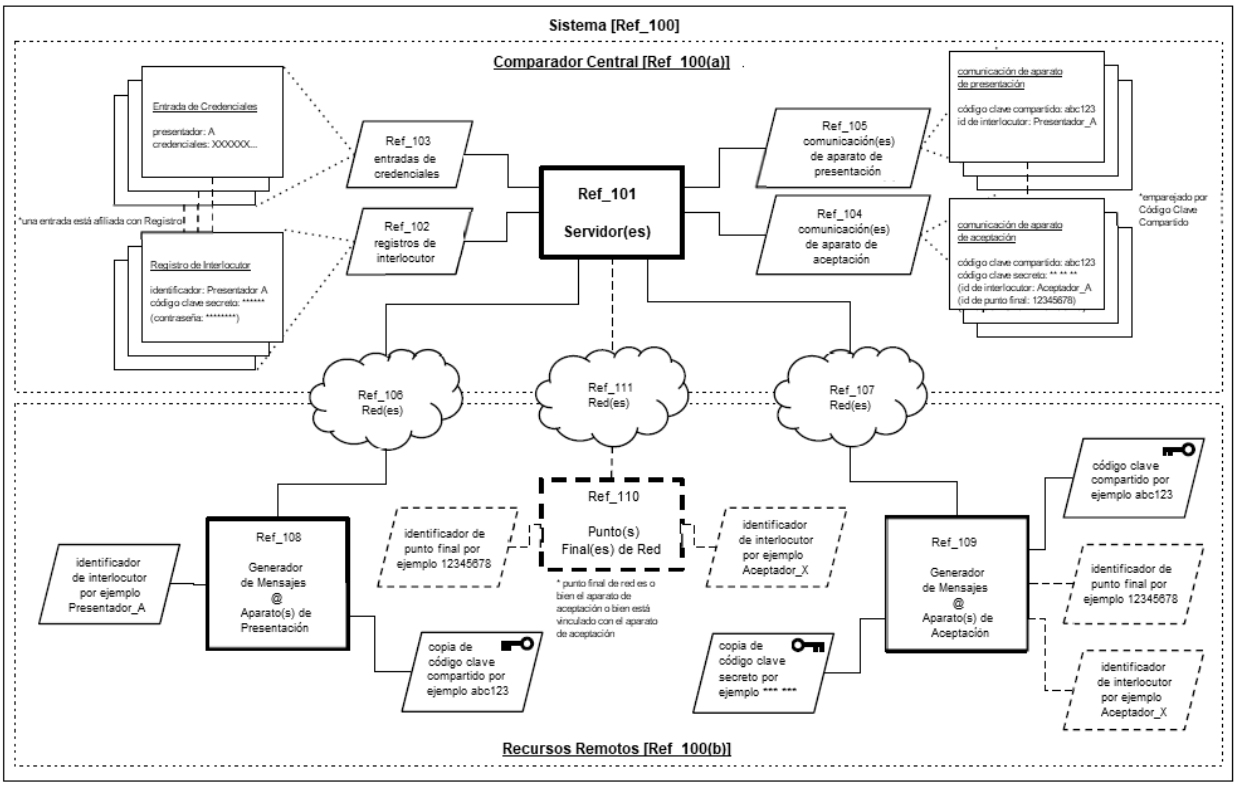

Sistema [Ref_100]
Comparador Central [Ref_100(a)]
Entrada de Credenciales
presentador: A
credenciales: XXXXXX...
*una entrada está afiliada con Registro
Registro de Interlocutor
identificador: Presentador A
código clave secreto: ******
(contraseña: ********)
Ref_103
entradas de credenciales
Ref_102
registros de interlocutor
Ref_101
Servidor(es)
Ref_105
comunicación(es) de aparato de presentación
Ref_104
comunicación(es) de aparato de aceptación
comunicación de aparato de presentación
código clave compartido: abc123
id de interlocutor: Presentador_A
comunicación de aparato de aceptación
código clave compartido: abc123
código clave secreto: ** ** **
(id de interlocutor: Aceptador_A
(id de punto final: 12345678)
*emparejado por Código Clave Compartido
Ref_106
Red(es)
Ref_111
Red(es)
Ref_107
Red(es)
Ref_110
Punto(s) Final(es) de Red
* punto final de red es o bien el aparato de aceptación o bien está vinculado con el aparato de aceptación
identificador de punto final por ejemplo 12345678
identificador de interlocutor por ejemplo Aceptador_X
identificador de interlocutor por ejemplo Presentador_A
Ref_108
Generador de Mensajes @ Aparato(s) de Presentación
copia de código clave compartido por ejemplo abc123
copia de código clave secreto por ejemplo *** ***
Ref_109
Generador de Mensajes @ Aparato(s) de Aceptación
código clave compartido por ejemplo abc123
identificador de punto final por ejemplo 12345678
identificador de interlocutor por ejemplo Aceptador_X
Recursos Remotos [Ref_100(b)]

Fig. 1A

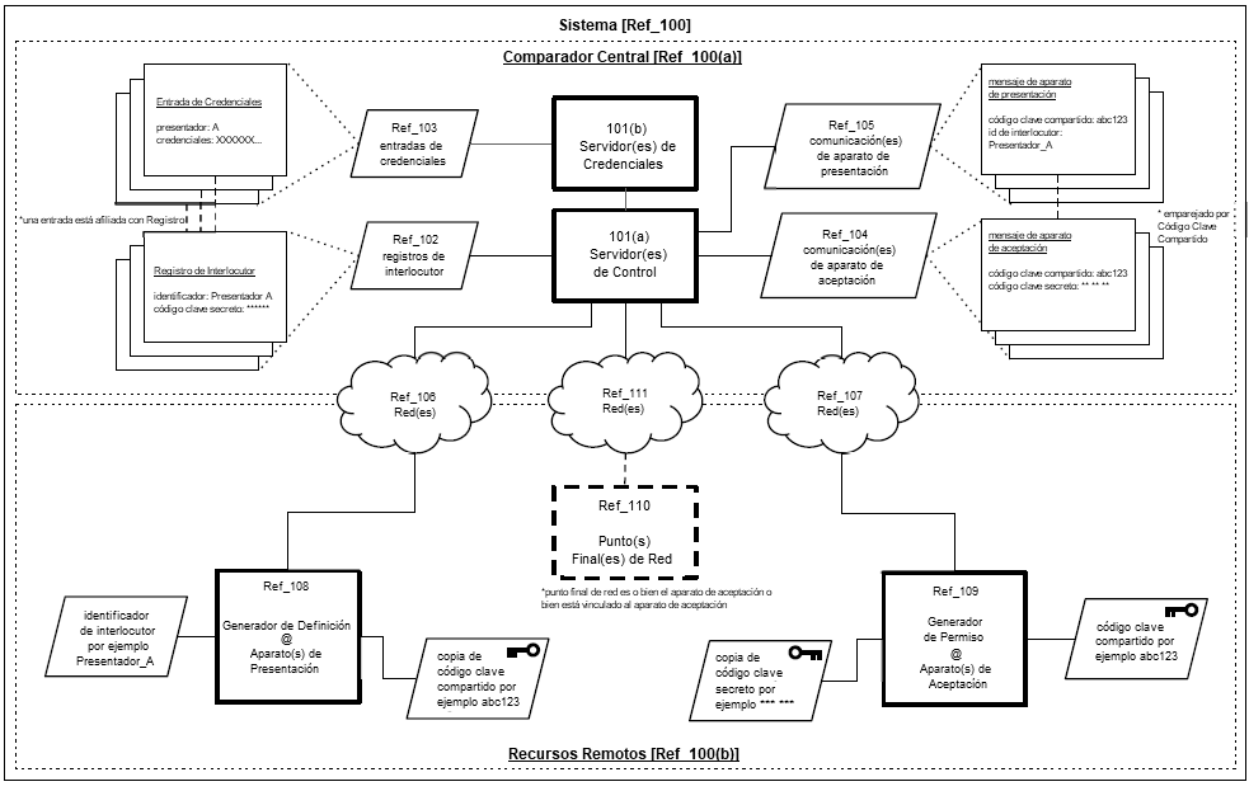

Sistema [Ref_100]
Comparador Central [Ref_100(a)]
Entrada de Credenciales
presentador: A
credenciales: XXXXXX...
*una entrada está afiliada con Registro
Registro de Interlocutor
identificador: Presentador A
código clave secreto: ******
Ref_103
entradas de credenciales
Ref_102
registros de interlocutor
101(b)
Servidor(es) de Credenciales
101(a)
Servidor(es) de Control
Ref_105
comunicación(es) de aparato de presentación
Ref_104
comunicación(es) de aparato de aceptación
mensaje de aparato de presentación
código clave compartido: abc123
id de interlocutor: Presentador_A
mensaje de aparato de aceptación
código clave compartido: abc123
código clave secreto: ** ** **
* emparejado por Código Clave Compartido
Ref_106
Red(es)
Ref_111
Red(es)
Ref_107
Red(es)
Ref_110
Punto(s) Final(es) de Red
*punto final de red es o bien el aparato de aceptación o bien está vinculado al aparato de aceptación
identificador de interlocutor por ejemplo Presentador_A
Ref_108
Generador de Definición @ Aparato(s) de Presentación
copia de código clave compartido por ejemplo abc123
copia de código clave secreto por ejemplo *** ***
Ref_109
Generador de Permiso @ Aparato(s) de Aceptación
código clave compartido por ejemplo abc123
Recursos Remotos [Ref_100(b)]

Fig. 1B

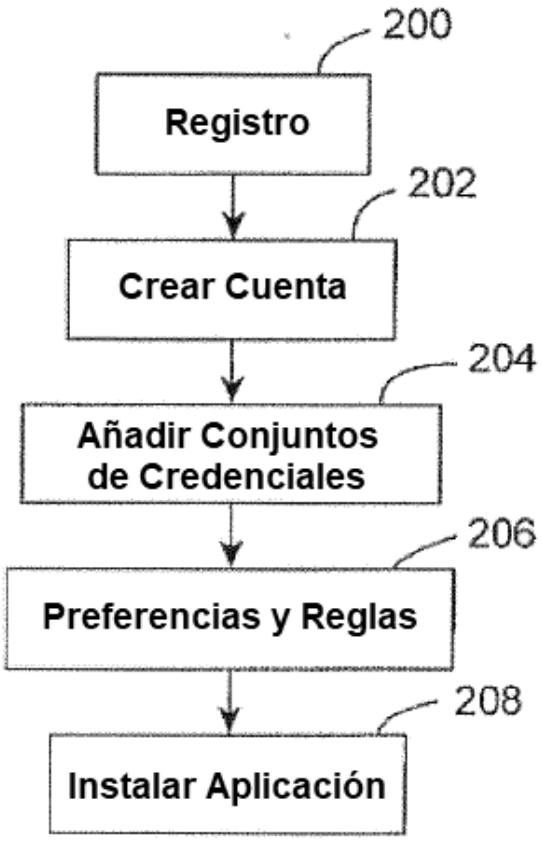

200
Registro
202
Crear Cuenta
204
Añadir Conjuntos de Credenciales
206
Preferencias y Reglas
208
Instalar Aplicación

Fig. 2

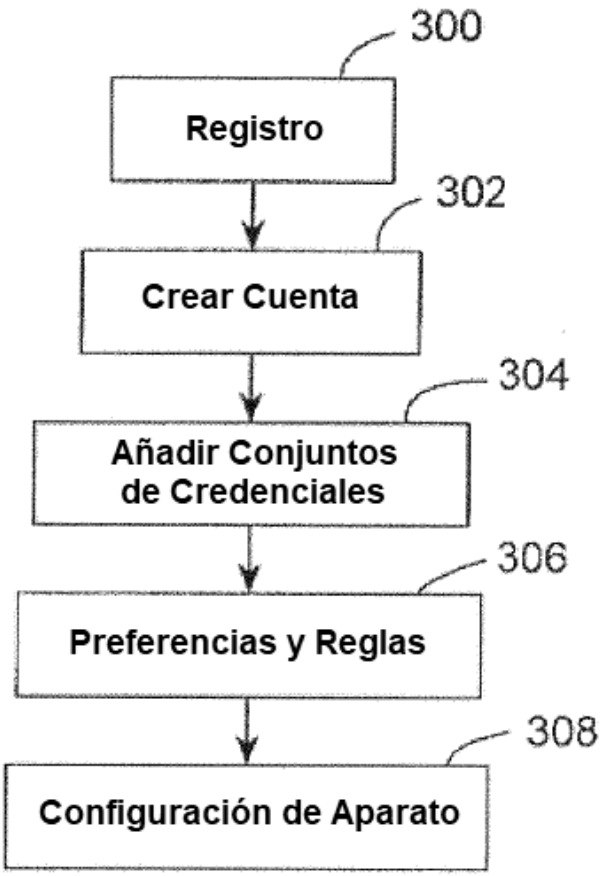

300
Registro
302
Crear Cuenta
304
Añadir Conjuntos de Credenciales
306
Preferencias y Reglas
308
Configuración de Aparato

Fig. 3

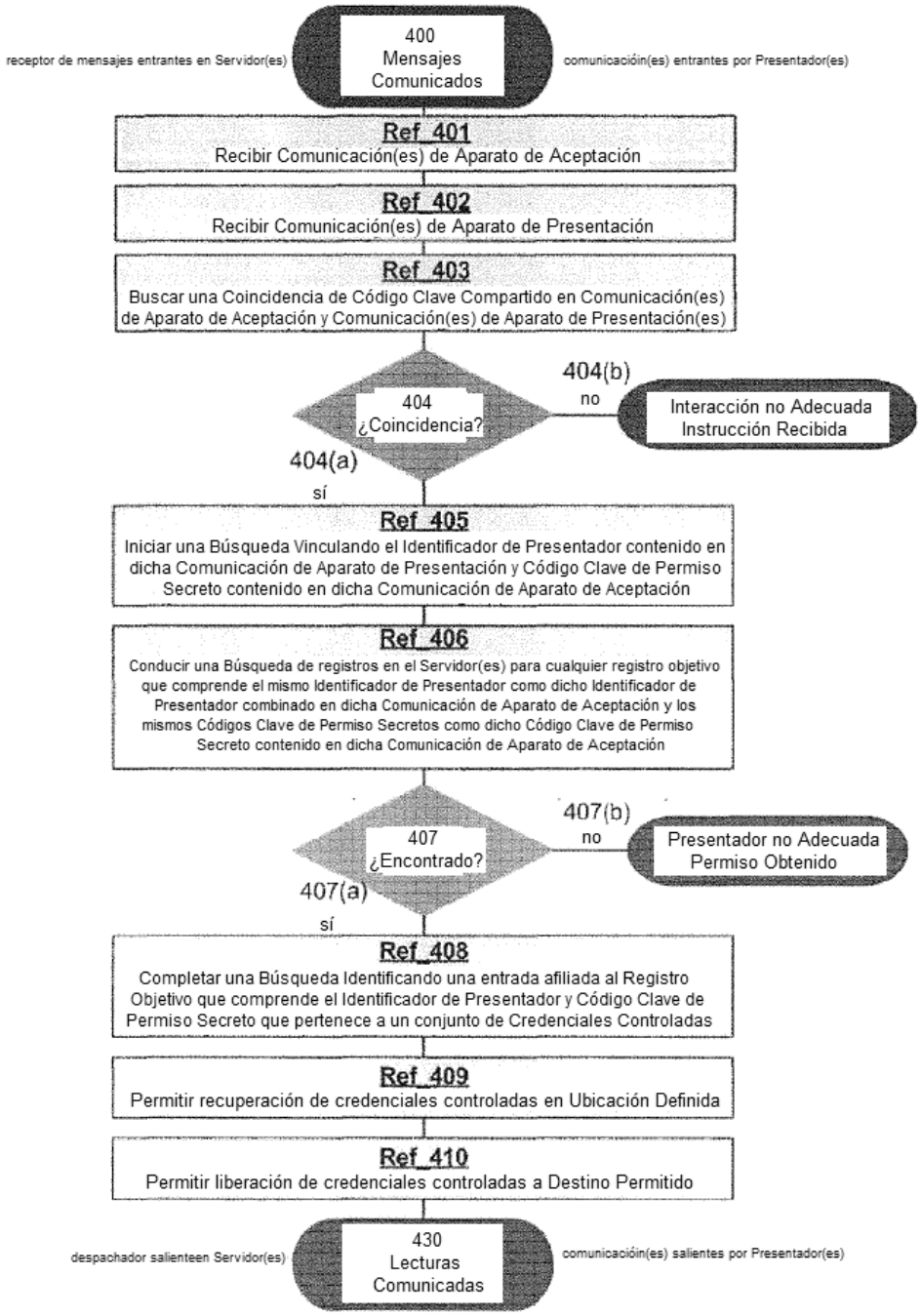

400
Mensajes Comunicados
receptor de mensajes entrantes en Servidor(es)
comunicaciòin(es) entrantes por Presentador(es)
Ref_401
Recibir Comunicación(es) de Aparato de Aceptación
Ref_402
Recibir Comunicación(es) de Aparato de Presentación
Ref_403
Buscar una Coincidencia de Código Clave Compartido en Comunicación(es) de Aparato de Aceptación y Comunicación(es) de Aparato de Presentación(es)
404
¿Coincidencia?
404(b)
no
Interacción no Adecuada Instrucción Recibida
404(a)
sí
Ref_405
Iniciar una Búsqueda Vinculando el Identificador de Presentador contenido en dicha Comunicación de Aparato de Presentación y Código Clave de Permiso Secreto contenido en dicha Comunicación de Aparato de Aceptación
Ref_406
Conducir una Búsqueda de registros en el Servidor(es) para cualquier registro objetivo que comprende el mismo Identificador de Presentador como dicho Identificador de Presentador combinado en dicha Comunicación de Aparato de Aceptación y los mismos Códigos Clave de Permiso Secretos como dicho Código Clave de Permiso Secreto contenido en dicha Comunicación de Aparato de Aceptación
407
¿Encontrado?
407(b)
no
Presentador no Adecuada Permiso Obtenido
407(a)
sí
Ref_408
Completar una Búsqueda Identificando una entrada afiliada al Registro Objetivo que comprende el Identificador de Presentador y Código Clave de Permiso Secreto que pertenece a un conjunto de Credenciales Controladas
Ref_409
Permitir recuperación de credenciales controladas en Ubicación Definida
Ref_410
Permitir liberación de credenciales controladas a Destino Permitido
430
Lecturas Comunicadas
despachador salienteen Servidor(es)
comunicaciòin(es) salientes por Presentador(es)

Fig. 4

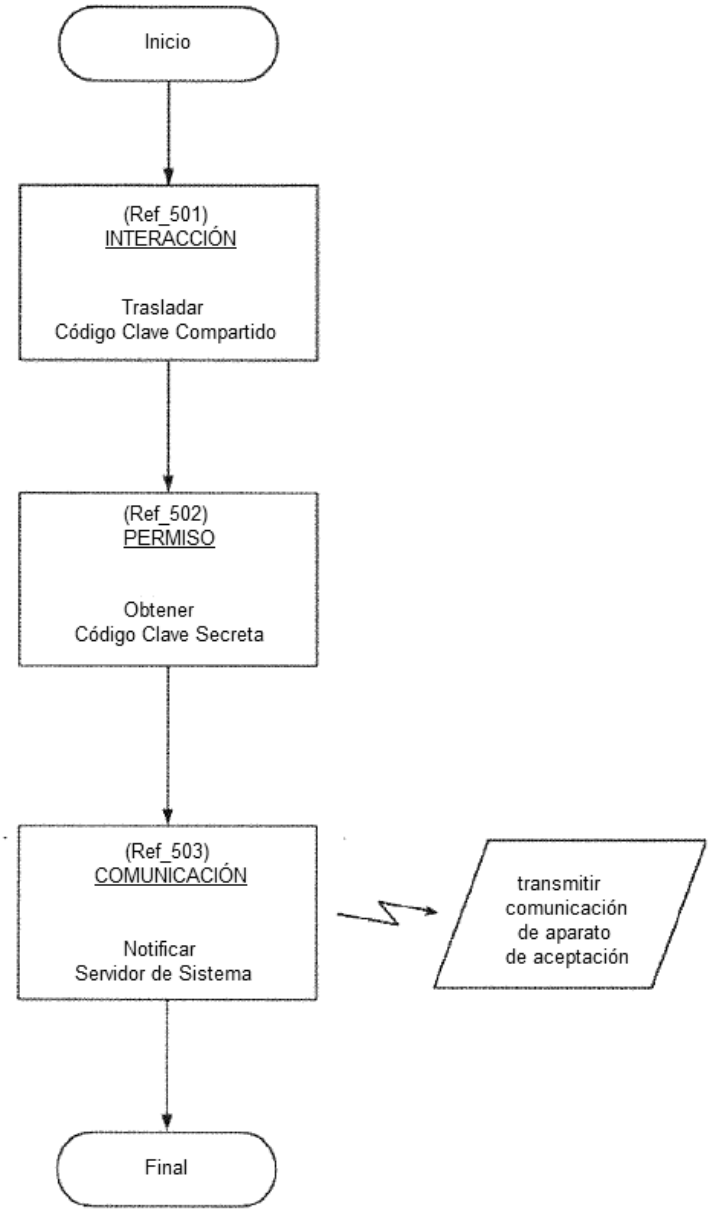

Inicio
(Ref_501)
INTERACCIÓN
Trasladar
Código Clave Compartido
(Ref_502)
PERMISO
Obtener
Código Clave Secreta
(Ref_503)
COMUNICACIÓN
Notificar
Servidor de Sistema
transmitir
comunicación
de aparato
de aceptación
Final

Fig. 5A

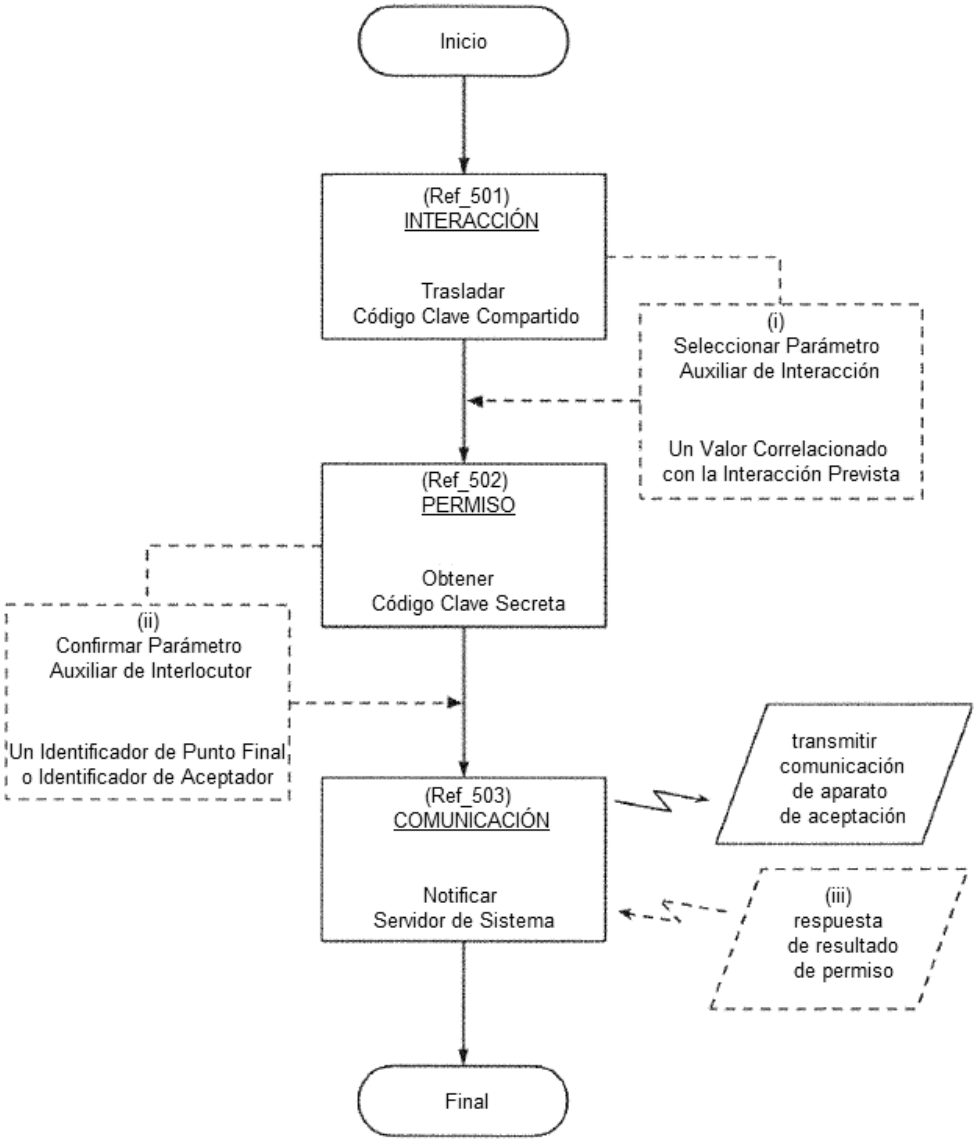

Inicio
(Ref_501)
INTERACCIÓN
Trasladar
Código Clave Compartido
(i)
Seleccionar Parámetro
Auxiliar de Interacción
Un Valor Correlacionado
con la Interacción Prevista
(Ref_502)
PERMISO
Obtener
Código Clave Secreta
(ii)
Confirmar Parámetro
Auxiliar de Interlocutor
Un Identificador de Punto Final
o Identificador de Aceptador
transmitir
comunicación
de aparato
de aceptación
(Ref_503)
COMUNICACIÓN
Notificar
Servidor de Sistema
(iii)
respuesta
de resultado
de permiso
Final

Fig. 5B

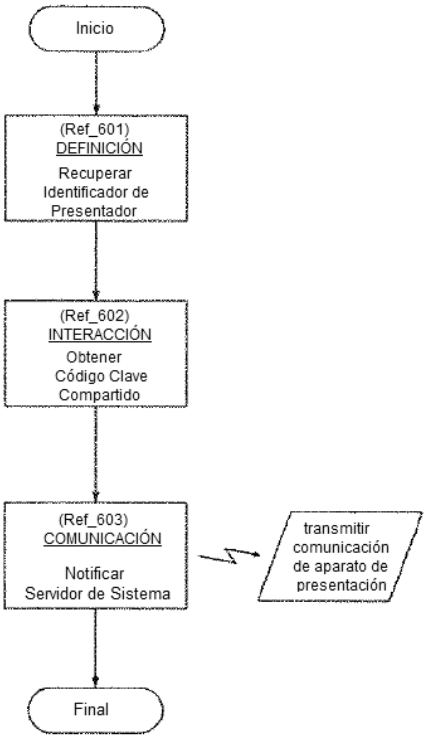

Inicio
(Ref_601)
DEFINICIÓN
Recuperar
Identificador de
Presentador
(Ref_602)
INTERACCIÓN
Obtener
Código Clave
Compartido
(Ref_603)
COMUNICACIÓN
Notificar
Servidor de Sistema
transmitir
comunicación
de aparato de
presentación
Final

Fig. 6A

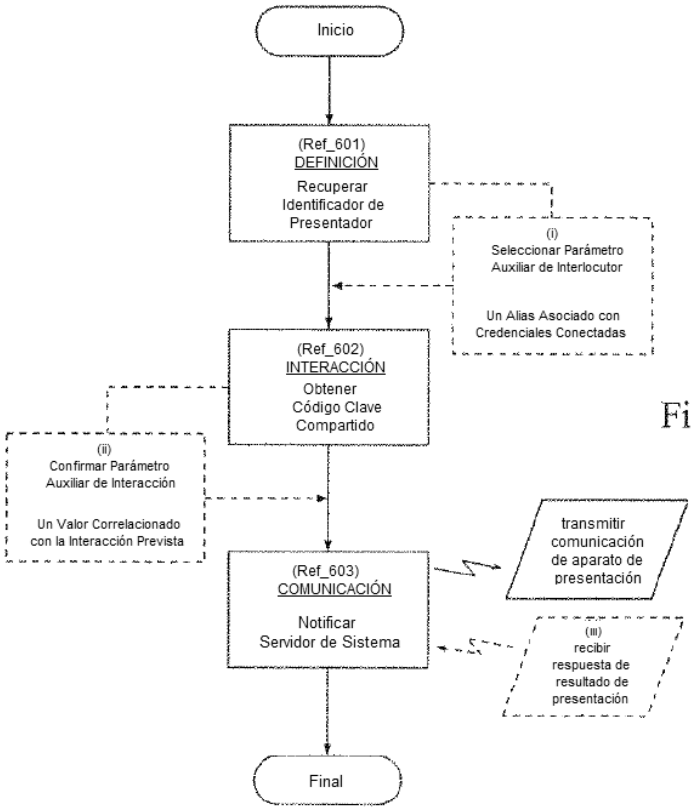
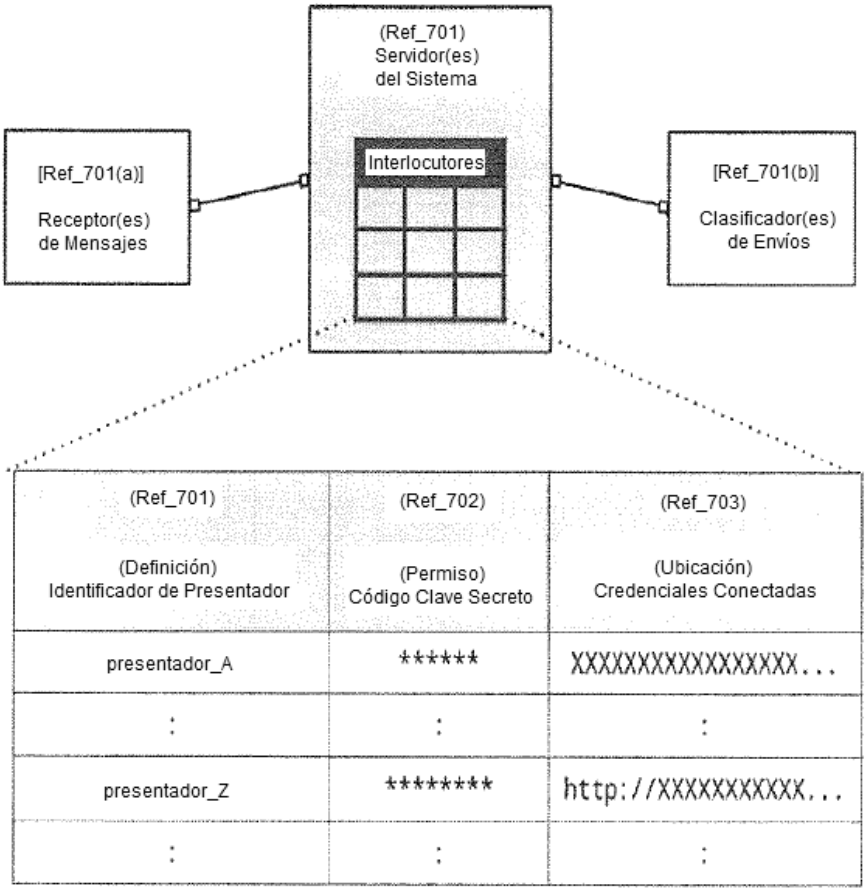

Inicio
(Ref_601)
DEFINICIÓN
Recuperar
Identificador de
Presentador
(i)
Seleccionar Parámetro
Auxiliar de Interlocutor
Un Alias Asociado con
Credenciales Conectadas
(Ref_602)
INTERACCIÓN
Obtener
Código Clave
Compartido
(ii)
Confirmar Parámetro
Auxiliar de Interacción
Un Valor Correlacionado
con la Interacción Prevista
transmitir
comunicación
de aparato de
presentación
(Ref_603)
COMUNICACIÓN
Notificar
Servidor de Sistema
(iii)
recibir
respuesta de
resultado de
presentación
Final

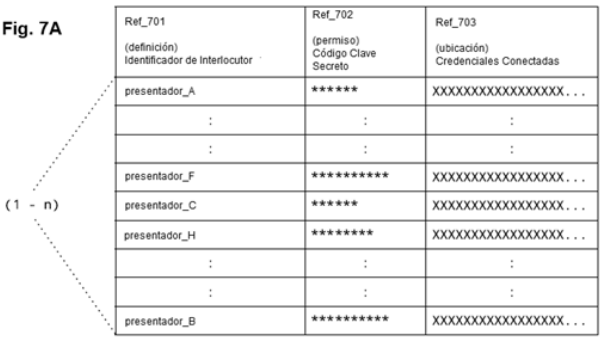
Fig. 6B



(Ref_701) (Definición) Identificador de Presentador	(Ref_702) (Permiso) Código Clave Secreto	(Ref_703) (Ubicación) Credenciales Conectadas
presentador_A	******	XXXXXXXXXXXXXXXXX...
:	:	:
presentador_Z	********	http://XXXXXXXXXXX...
:	:	:

Fig. 7

Fig. 7A



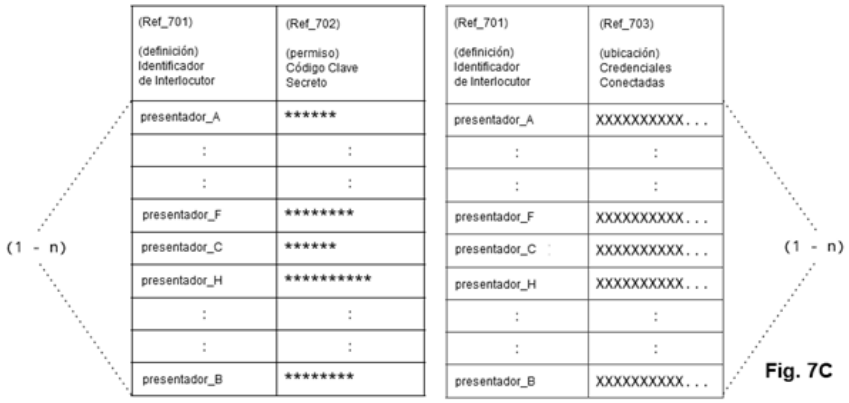
Ref_701 (definición) Identificador de Interlocutor	Ref_702 (permiso) Código Clave Secreto	Ref_703 (ubicación) Credenciales Conectadas
presentador_A	******	XXXXXXXXXXXXXXXXX...
:	:	:
:	:	:
presentador_F	**********	XXXXXXXXXXXXXXXXX...
presentador_C	******	XXXXXXXXXXXXXXXXX...
presentador_H	********	XXXXXXXXXXXXXXXXX...
:	:	:
:	:	:
presentador_B	**********	XXXXXXXXXXXXXXXXX...

(1 - n)

Fig. 7B

Ref_701 (definición) Identificador de Interlocutor	Ref_702 (permiso) Código Clave Secreto	Ref_703 (ubicación) Credenciales Conectadas
8c48847bcc...	s2YisvHPL+...	%B555555...
:	:	:
:	:	:
9415bfefcc...	0a5lYaQqR9...	P<XXXBLOGGS<<JOHN...
d299997ce5...	tncmmXw3Qp...	%B444444...
c4345d0f05...	uGkM35SWPs...	%Z999999...
:	:	:
:	:	:
c4e417c0f9...	LBUcbRQmIP...	https://registry?...

(1 - n)



(Ref_701) (definición) Identificador de Interlocutor	(Ref_702) (permiso) Código Clave Secreto
presentador_A	******
:	:
:	:
presentador_F	********
presentador_C	******
presentador_H	**********
:	:
:	:
presentador_B	********

(1 - n)

(Ref_701) (definición) Identificador de Interlocutor	(Ref_703) (ubicación) Credenciales Conectadas
presentador_A	XXXXXXXXXX...
:	:
:	:
presentador_F	XXXXXXXXXX...
presentador_C	XXXXXXXXXX...
presentador_H	XXXXXXXXXX...
:	:
:	:
presentador_B	XXXXXXXXXX...

(1 - n)

Fig. 7C

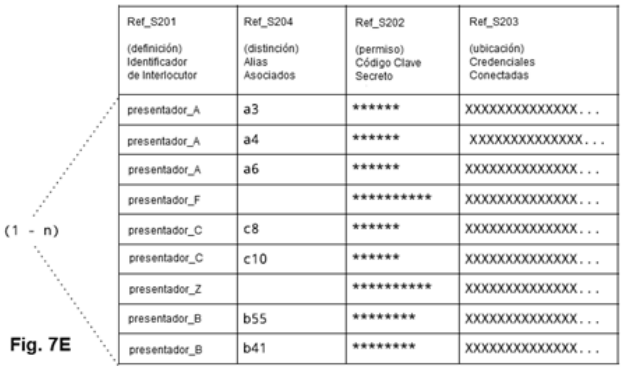
Ref_701 (definición) Identificador de Interlocutor	Ref_702 (permiso) Código Clave Secreto
8c48847bcc...	s2YisvHPL+...
:	:
:	:
9415bfefcc...	0a5lYaQqR9...
d299997ce5...	tncmmXw3Qp...
c4345d0f05...	uGkM35SWPs...
:	:
:	:
c4e417c0f9...	LBUcbRQmIP...

(1 - n)

Ref_701 (definición) Identificador de Interlocutor	Ref_703 (ubicación) Credenciales Conectadas
8c48847bcc...	%B555555...
:	:
:	:
9415bfefcc...	P<XXXBLOGG...
d299997ce5...	%B444444...
c4345d0f05...	%Z999999...
:	:
:	:
c4e417c0f9...	https://re...

(1 - n)

Fig. 7D



Ref_S201 (definición) Identificador de Interlocutor	Ref_S204 (distinción) Alias Asociados	Ref_S202 (permiso) Código Clave Secreto	Ref_S203 (ubicación) Credenciales Conectadas
presentador_A	a3	******	XXXXXXXXXXXXXX...
presentador_A	a4	******	XXXXXXXXXXXXXX...
presentador_A	a6	******	XXXXXXXXXXXXXX...
presentador_F		**********	XXXXXXXXXXXXXX...
presentador_C	c8	******	XXXXXXXXXXXXXX...
presentador_C	c10	******	XXXXXXXXXXXXXX...
presentador_Z		**********	XXXXXXXXXXXXXX...
presentador_B	b55	********	XXXXXXXXXXXXXX...
presentador_B	b41	********	XXXXXXXXXXXXXX...

(1 - n)

Fig. 7E

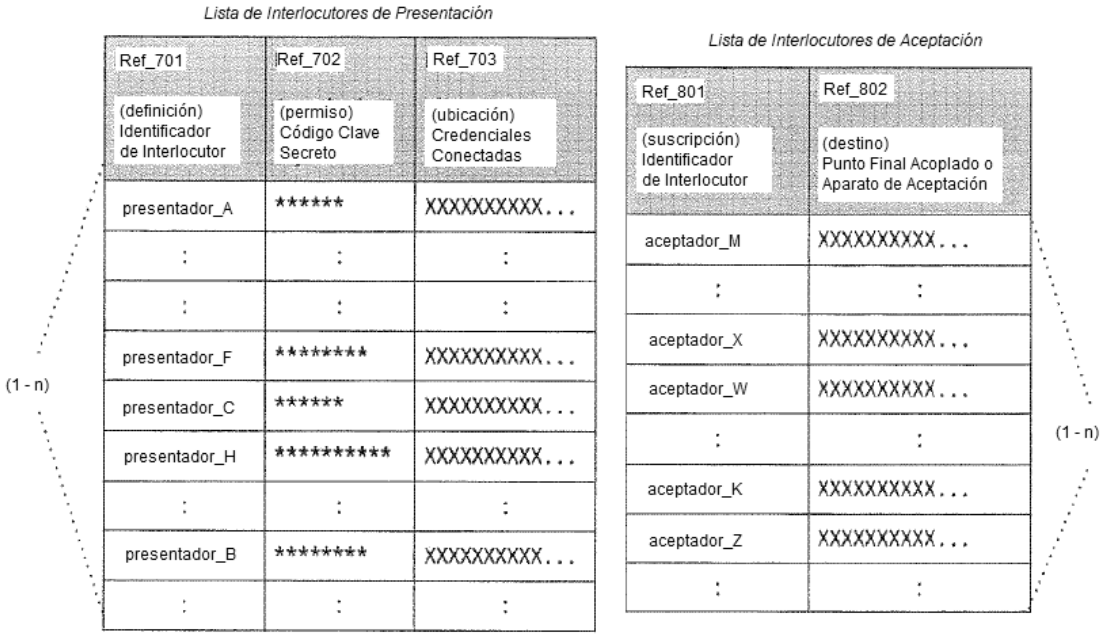

Lista de Interlocutores de Presentación
Ref_701
(definición) Identificador de Interlocutor
Ref_702
(permiso) Código Clave Secreto
Ref_703
(ubicación) Credenciales Conectadas
presentador_A
******
XXXXXXXXXX...
presentador_F
****
XXXXXXXXXX...
presentador_C
******
XXXXXXXXXX...
presentador_H
****
XXXXXXXXXX...
presentador_B
****
XXXXXXXXXX...
(1 - n)
Lista de Interlocutores de Aceptación
Ref_801
(suscripción) Identificador de Interlocutor
Ref_802
(destino) Punto Final Acoplado o Aparato de Aceptación
aceptador_M
XXXXXXXXXX...
aceptador_X
XXXXXXXXXX...
aceptador_W
XXXXXXXXXX...
aceptador_K
XXXXXXXXXX...
aceptador_Z
XXXXXXXXXX...
(1 - n)

Fig. 8

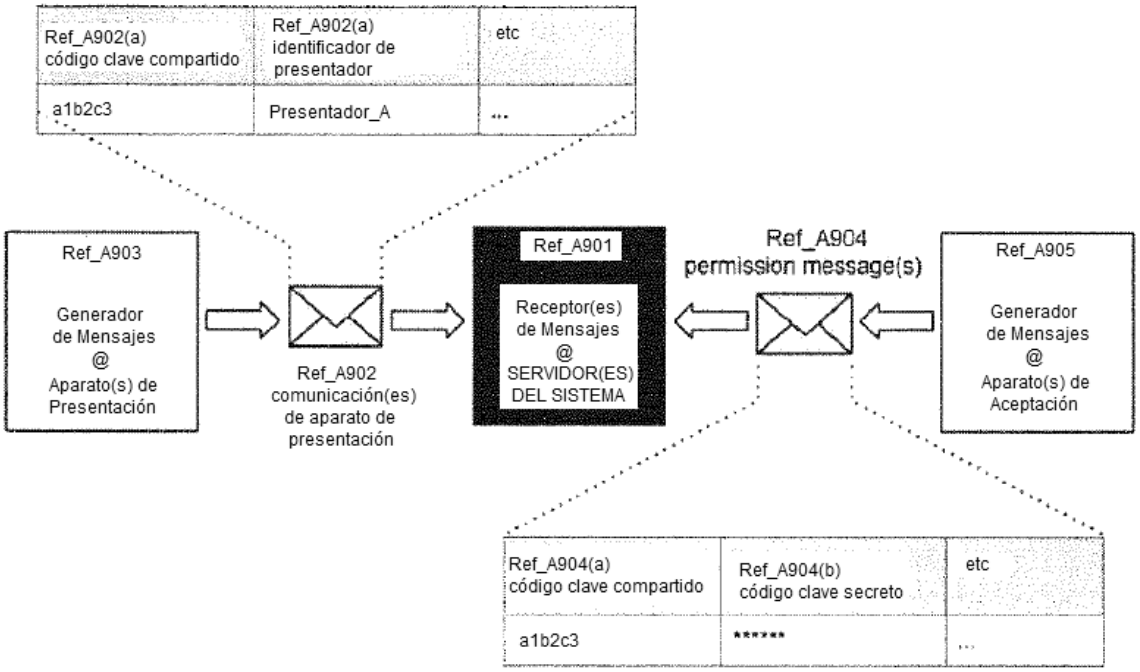

Ref_A902(a)
código clave compartido
Ref_A902(a)
identificador de presentador
etc
a1b2c3
Presentador_A
...
Ref_A903
Generador de Mensajes @ Aparato(s) de Presentación
Ref_A902 comunicación(es) de aparato de presentación
Ref_A901
Receptor(es) de Mensajes @ SERVIDOR(ES) DEL SISTEMA
Ref_A904 permission message(s)
Ref_A905
Generador de Mensajes @ Aparato(s) de Aceptación
Ref_A904(a)
código clave compartido
Ref_A904(b)
código clave secreto
etc
a1b2c3
******
...

Fig. 9A

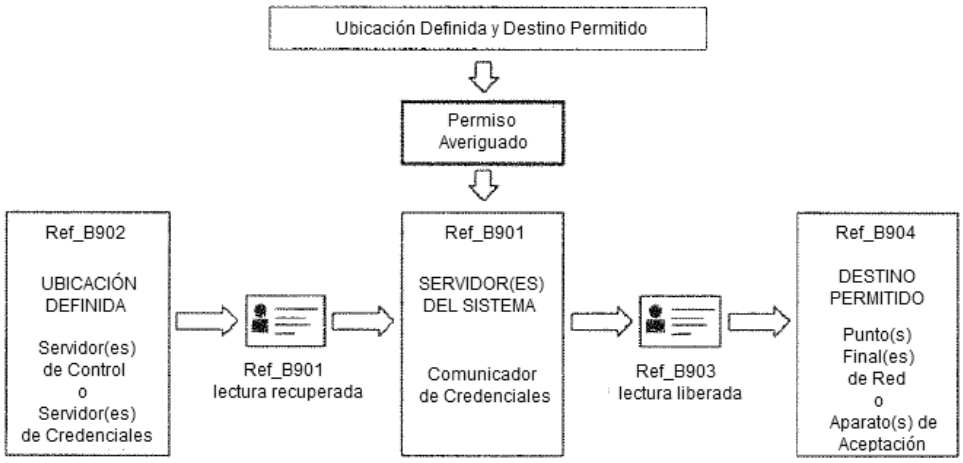

Ubicación Definida y Destino Permitido
Permiso Averiguado
Ref_B902
UBICACIÓN DEFINIDA
Servidor(es) de Control o Servidor(es) de Credenciales
Ref_B901
lectura recuperada
Ref_B901
SERVIDOR(ES) DEL SISTEMA
Comunicador de Credenciales
Ref_B903
lectura liberada
Ref_B904
DESTINO PERMITIDO
Punto(s) Final(es) de Red o Aparato(s) de Aceptación

Fig. 9B

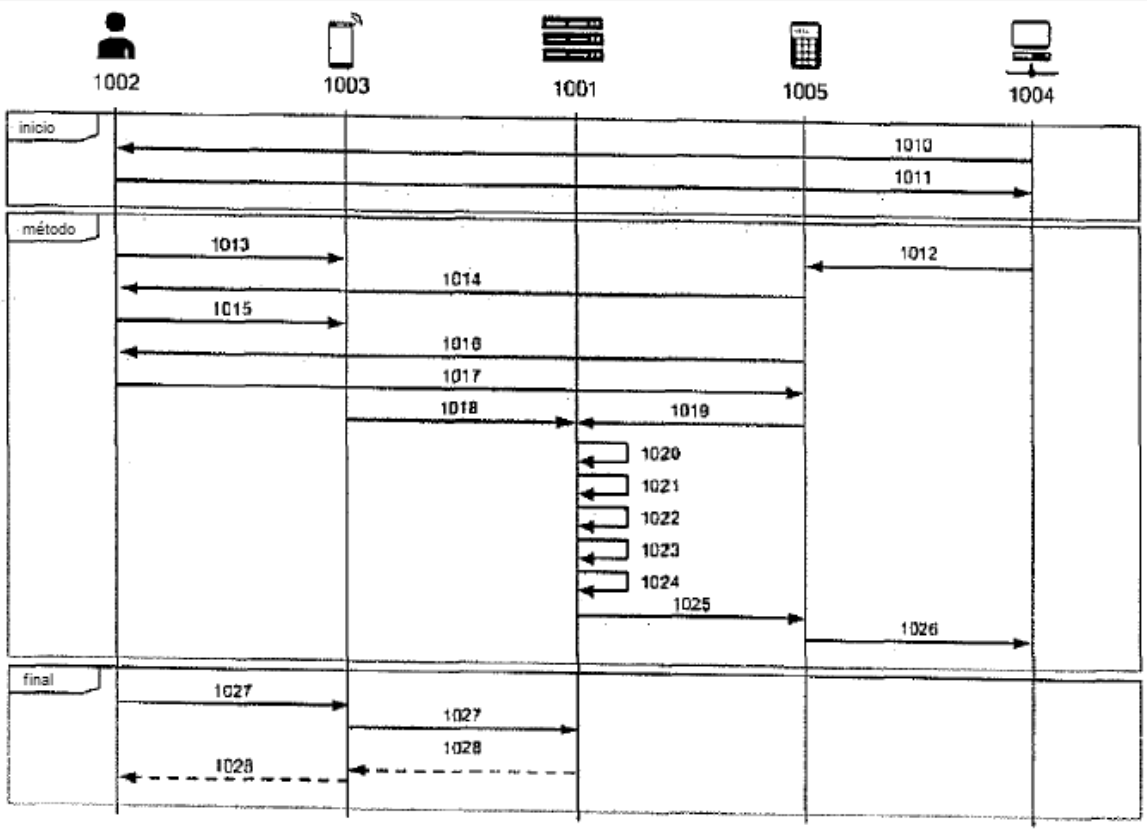

1002
1003
1001
1005
1004
inicio
método
final
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1027
1028
1028

Fig. 10