

SISTEMA Y MÉTODO PARA COMUNICAR CREDENCIALES

CAMPO DE LA INVENCION

La presente invención pertenece al campo de
5 tecnología de información y de comunicación,
confidencialidad de intercambio de datos confiados a la
tecnología de información y de comunicación, así como
conservar y proteger la confidencialidad que prevalece en
credenciales comunicadas con información y tecnología de
10 comunicación. La confidencialidad se refiere a la posesión
de o participación en cualquier información que pertenece a
una entidad, o cualquier grupo de credenciales que conectan
una entidad y cualquier individuo particular. En
particular, la presente invención está relacionada con,
15 pero no limitada a liberación permitida de datos que
comprenden grupos de detalles personales privados y
credenciales controladas que una parte a quien pertenece el
grupo de credenciales, puede desear consentir y permitir
liberar de manera confidencial en una forma protegida y
20 segura mientras asegura la conservación y mantenimiento
continuo de la confidencialidad y privacidad de los
detalles personales y credenciales controladas para una
variedad de propósitos. Las credenciales controladas se
refieren a tal información que conecta al
25 propietario/emisor de las credenciales controladas y al

titular/poseedor de las credenciales controladas.

ANTECEDENTES DE LA INVENCIÓN

En la sociedad moderna, los individuos están asociados con un gran conjunto de datos personales. Algunos
5 ejemplos de tales datos personales incluyen pero no están limitados a nombre, dirección, fecha de nacimiento, nacionalidad, número de seguro social, número de pasaporte, número de licencia para conducir, número de membresía (para una organización dada), apellido de soltera (si es
10 aplicable), apellido de soltera de la madre, información de empleador, número de cuenta bancaria, número de tarjeta de crédito, etc. Estos datos personales se utilizan en una multitud de formas como y cuando los individuos interactúan con otros individuos y organizaciones. Muchas de estas
15 interacciones dependen fuertemente de la precisión de un grupo de datos que es tanto particular para el individuo como necesario para la interacción en cuestión. Por consiguiente, debido a que cada grupo de datos (en lo sucesivo denominado como un "grupo de credencial") es tanto
20 particular para un individuo como necesario para la interacción, esa información delicada que deseablemente se retiene en un estado de confidencialidad. La información son datos relevantes adicionales delicados (y deseablemente retenidos en un estado de confidencialidad), tal como datos
25 que pertenecen a características de seguridad adicionales,

por ejemplo, un código clave secreto asociado con un instrumento dado. Se entenderá que incluso si se desea liberar un grupo de credenciales de un registro, puede ser necesario asegurar que los datos asociados nunca se liberen, particularmente cuando pertenecen a características de seguridad adicionales.

Tales entradas de registro típicamente se llenan de la siguiente forma. El grupo de credenciales que pertenecen a un presentador se elabora para el controlador y el grupo de credenciales se verifica y valida. Una vez que se verifica y valida el grupo de credenciales, se produce un instrumento que tiene el grupo de credenciales, y este grupo de credenciales se proporciona al presentador. El grupo de credenciales también se ingresa en un nuevo registro sobre la entrada de registro y típicamente se complementa con cualquier dato que pertenezca al instrumento correspondiente (tal como número de serie, etc.) y cualquier otro dato relevante (tal como datos de característica de seguridad adicionales que incluyen pero no se limitan a biométricas, etc.).

Han evolucionado formas para presentar grupos de credenciales en tales instrumentos personalizados. Históricamente, tales datos pudieron haber sido entintados, escritos o etiquetados sobre el instrumento emitido. Subsecuentemente, tales datos pudieron haber sido repujados

o grabados o codificados o incorporados sobre el instrumento emitido. Más recientemente, medios legibles por máquina (tal como tiras magnéticas o chips) se han utilizado como instrumentos. Los grupos de credenciales
5 relevantes se almacenan electrónicamente en tales medios. El formato de muchos instrumentos (y el formato en el cual se almacenan ahí grupos de credenciales) es regido por la Organización Internacional para Estandarización. Por ejemplo, ISO 7501 rige el formato de documentos de
10 desplazamiento legible por máquina; ISO 7810 e ISO 7811 rigen el formato de Tarjetas de Identificación; e ISO 7812 e ISO 7816 rigen la forma en la cual las tarjetas pueden proporcionarse a partir de diferentes emisores.

A pesar de los avances en la estipulación de
15 instrumentos que tienen grupos de credenciales de presentador, sigue existiendo el peligro de fraude. Sigue siendo necesario ser capaz de verificar tanto el presentador que tiene el instrumento que comprende el grupo de credenciales es el presentador válido/auténtico (es
20 decir, que el instrumento no haya sido robado o clonado y por ello que no se utilice de manera fraudulenta) y también verificar que el instrumento ofrecido que comprende el grupo de credenciales en efecto es auténtico (es decir, que las credenciales sean precisas y que el instrumento no sea
25 una completa falsificación). Éste es un problema de interés

creciente ya que los portadores de tales instrumentos liberan sus grupos de credenciales en una base cada vez más frecuente. Aunque los grupos de credenciales se mantienen inicialmente en un ambiente de confidencialidad/privacidad, que existe entre los presentadores de grupos de credenciales y sus controladores, este ambiente de confidencialidad/privacidad es puesto en peligro en cualquier momento que se libera el grupo de credenciales durante un intercambio con una tercera parte. Aunque las mejoras en la seguridad de los medios por los cuales se liberan grupos de credenciales han buscado reforzar este ambiente de confidencialidad/privacidad, aún persiste la debilidad.

Por ejemplo, incluso con la llegada de sistemas automatizados para leer instrumentos de pasaporte, cuando un pasajero presenta su pasaporte a un representante de punto de control o cualquier agencia de control fronterizo (el "aceptador"), las credenciales controladas en el instrumento emitido son visibles a y manejadas por el aceptador antes y después de capturar las credenciales controladas en el dispositivo lector. Si, transgrediendo la política de privacidad, dichas credenciales cuando se ven, son copiadas y compartidas por el aceptador, no sólo capturadas y procesadas, se compromete el estado de confidencialidad en el cual originalmente residían las

credenciales de instrumento de pasaporte. Existen diferencias similares para otros instrumentos para los cuales se han desarrollado sistemas de captura de credencial automatizados, tal como licencias para conducir, 5 tarjetas de lealtad/membresía, y tarjetas de pago.

Sigue habiendo una necesidad de métodos y sistemas mejorados por los cuales los presentadores pueden ofrecer grupos de credenciales durante intercambios con otros individuos u organizaciones en una forma que 10 garantiza tanto la autenticidad del grupo de credenciales, y la autenticidad del presentador que tiene el grupo de credenciales. Sería altamente deseable proporcionar métodos y sistemas para asegurar un ambiente de completa confidencialidad/privacidad para grupos de credenciales 15 cuando se están describiendo. Sería muy preferible para cualquiera de tales métodos y sistemas mejorados ser compatibles con versiones anteriores, con métodos y sistemas existentes que están en uso común de manera que los métodos y sistemas mejorados puedan introducirse 20 progresivamente de manera uniforme y gradual. Esto sería altamente ventajoso ya que eliminaría la necesidad de transiciones costosas y lentas a nuevos sistemas y métodos. Además sería preferible cualquier nuevo método y sistema mejorado que sea escalable de manera que pueda atender una 25 pluralidad de diversos grupos de credenciales a través de

un sistema y método individual.

BREVE DESCRIPCIÓN DE LA INVENCION

Un aspecto de la invención comprende un sistema para permitir una comunicación de al menos un grupo de credenciales controladas conectado a un presentador, a un punto final de red, mientras se mantiene la confidencialidad que permanece 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 grupo de credenciales controladas conectadas a un presentador. Cada entrada pertenece al menos a un grupo de credenciales asociadas con dicho presentador dado. Cada entrada también puede pertenecer al menos a un alias, cada alias conectado respectivamente con una de dichos grupos de credenciales. Cada punto final de red es un receptor designado de un tipo de credenciales controladas, conectadas a presentadores, dicho punto final es cualquiera del aparato de aceptación o aquel de una tercera parte designada conectada al aparato

de aceptación; en donde permitir una comunicación de al menos un grupo de credenciales controladas conectadas al presentador se realiza en el contexto de una interacción entre el interactor de presentación y el interactor de

5 aceptación; en donde el grupo de credenciales al cual pertenece el permiso está asociado con el interactuar de presentación. Una de dichas funciones de servidores como un servidor de control además configurado para (a) recibir una comunicación de un aparato de aceptación en lo sucesivo

10 denominado como una comunicación de aparato de aceptación, dicha comunicación contiene un código clave secreto que pertenece al presentador y un código clave compartido una vez apagado; (b) recibir una comunicación de un aparato de presentación en lo sucesivo denominado como una

15 comunicación de aparato de presentación, dicha comunicación contiene un identificador de presentador que pertenece al presentador y un código clave compartido una vez apagado; (c) buscar coincidencia del código clave compartido una vez apagado, contenido en la comunicación de aparato de

20 aceptación y el código clave compartido una vez apagado correspondiente contenido en la comunicación de aparato de presentación; (d) iniciar una búsqueda de un registro objetivo al conectar el código clave secreto contenido en dicha comunicación de aparato de aceptación y el

25 identificador de presentación contenido en dicha

comunicación de aparato de presentación, en donde ambas de dichas comunicaciones contienen el mismo código clave compartido; (e) conducir una búsqueda de dicho registro objetivo que comprende tanto dicho código clave secreto y dicho identificador del presentador; (f) identificar una entrada afiliada con dicho registro objetivo, dicha entrada pertenece a un grupo de credenciales controladas conectadas al presentador; (g) permitir la recuperación de dicho grupo de credenciales que pertenece a dicha entrada y permitir la liberación de dicho grupo de credenciales a dicho punto final de red, dicho punto final es el receptor permitido de un grupo de credenciales controladas conectadas a dicho presentador, y dicho punto final es cualquiera del aparato de aceptación o aquel de una tercera parte designada conectada al aparato de aceptación².

Otro aspecto de la invención comprende un método para permitir una comunicación de al menos un grupo de credenciales controladas conectadas a un presentador, desde un servidor un punto final de red, mientras se mantiene la confidencialidad que prevalece en dichas credenciales controladas conectadas al presentador; y en donde un servidor comprende uno o más registros, cada registro pertenece a un presentador (dada parte involucrada con el servidor, un presentador y/o como un aceptador), y cada registro comprende un identificador de presentador (y/o

identificador de aceptador⁴) y un código clave secreto (de presentador y/o de aceptador⁴) unido a dicho identificador de presentador, y cada registro está afiliado con una entrada que pertenece a un grupo de credenciales controladas (asociadas con dicha parte⁴) conectada a dicho presentador; el método comprende: (a) en un aparato de aceptación, poner a disponibilidad un código clave compartido una vez apagado a un/el interactor de presentación; (b) en el aparato de aceptación, recibir un código clave secreto (de presentador⁴) que pertenece al interactor de presentación en donde dicho código clave secreto (de presentador⁴) es ingresado en el aparato de aceptación por el interactor de presentación; (c) en el aparato de aceptación, comunicar una comunicación de aparato de aceptación al menos a uno de los servidores, dicha comunicación de aparato de aceptación contiene el código clave compartido una vez apagado y el código clave secreto (de presentador⁴); (d) en un aparato de presentación del interactor de presentación, recibir el código clave compartido una vez apagado; (e) en el aparato de presentación, recuperar un identificador de presentador que pertenece al interactor de presentación de 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 contiene el código clave compartido una vez apagado y el identificador de presentador, en donde (g) después de recibir dicha comunicación de aparato de aceptación y dicha comunicación de aparato de presentación, en el servidor que procesa la comunicación para evaluarse se permite comunicar un grupo de credenciales controladas conectadas al presentador, permitiendo con ello su recuperación en un servidor y permitiendo con ello su liberación en un punto final de red, dicho punto final es un receptor permitido, y dicho punto final es cualquiera del aparato de aceptación o aquel de una tercera parte designada conectada al aparato de aceptación.

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

En otro aspecto de la invención, todos los grupos de credenciales conectados al presentador (y alias afiliados) pueden estar comprendidos como entradas separadas en un servidor diferente que se puede comunicar con un servidor de control. Alternativamente, algunos grupos de credenciales conectados al presentador y alias afiliados pueden estar comprendidos como entradas en dicho registro, mientras otros pueden estar comprendidos como

entradas separadas en dicho servidor o entradas separadas en diferentes servidores.

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

En un aspecto de la invención, el código clave compartido una vez apagado puede generarse en el servidor* y comunicarse al aparato de aceptación antes que dicho código clave compartido una vez apagado se ponga a disponibilidad para el interactor de presentación y/o el aparato de presentación.

En otro aspecto de la invención, el código clave compartido una vez apagado puede generarse en el aparato de aceptación antes que se ponga a disponibilidad dicho código clave compartido una vez apagado al interactor de presentación y/o el aparato de presentación.

Puede comunicarse una copia del código clave compartido una vez apagado del aparato de aceptación al aparato de presentación a través de una tecnología inalámbrica, la tecnología inalámbrica opcionalmente seleccionada de un grupo que comprende Wi-Fi, Bluetooth, NFC o RFID.

En un aspecto de la invención, puede asignarse un

periodo de validez a la comunicación de aparato de aceptación y comunicaciones de aparato de presentación y/o el código clave compartido. Esto asegura que si no se hace coincidir una comunicación de aparato de aceptación con una comunicación de aparato de presentación como se discute a continuación dentro de cierto periodo (el periodo de validez), entonces tal comunicación transcurre y con ello se vuelve vacía haciendo los procesos adicionales redundantes. En donde transcurre tal comunicación y se vuelve vacía haciendo los procesos adicionales redundantes, los datos que pertenecen a la comunicación pueden purgarse, liberando recursos para el procesamiento de comunicaciones adicionales. En donde se generan, transmiten o reciben comunicaciones, que contienen códigos clave compartidos que tienen un periodo de validez, el periodo de validez puede asegurar que pueden utilizarse códigos clave compartidos más cortos, menos complejos debido a que con ello es factible la reutilización de código clave compartido. Después de la expiración del periodo de validez de un código clave compartido, el mismo código clave compartido puede reutilizarse en una iteración subsecuente del método.

En un aspecto de la invención puede ponerse a disponibilidad una copia del código clave compartido una vez apagado al interactor de presentación y/o aparato de presentación a través de una pantalla comprendida en el

aparato de aceptación o en una impresión del aparato de aceptación, en donde cualquiera de: (a) una copia de código clave compartido una vez apagado se pone a disponibilidad en formato de carácter legible por máquina, por ejemplo UTF-8, y la copia del código clave compartido una vez apagado se recibe en el componente periférico de presentación a través de entrada desde el interactor de presentación y/o interactor de aceptación o/y aparato de aceptación; o (b) una copia del código clave compartido una vez apagado está comprendido en un código QR, y la copia del código clave compartido una vez apagado se recibe en el aparato de presentación a través de una función de cámara comprendida en el aparato de presentación que se utiliza para capturar el código de respuesta rápida y extraer una copia del código clave compartido una vez apagado.

La comunicación del aparato de aceptación además puede comprender uno o más parámetros auxiliares predeterminados, y la comunicación del aparato de presentación además también puede contener dichos uno o más parámetros auxiliares predeterminados. Opcionalmente también estos parámetros auxiliares tienen que hacerse coincidir como se describirá adicionalmente a continuación antes que la corroboración sea exitosa para iniciar y conducir una búsqueda de cualquiera de los registros objetivo. Esta condición de coincidencia adicional en el

proceso de corroboración, en donde se indique sobre y por encima del código clave compartido, además mejora el método ya que introduce criterios adicionales en el proceso de buscar coincidencia de una comunicación de aparato de aceptación y comunicación de aparato de presentación. El parámetro auxiliar predeterminado puede ser un código acordado entre el interactor de aceptación y el interactor de presentación, o puede ser un valor pertinente para la interacción entre el interactor de presentación y el interactor de aceptación, tal como el valor de la transacción deseada.

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

Otro aspecto de la invención comprende un método para permitir una comunicación de al menos un grupo de credenciales controladas conectadas al presentador, en un servidor para un punto final de red, aunque mantiene la privacidad que prevalece en el grupo 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 del presentador, y una comunicación de aparato de presentación que contiene un código clave compartido y un

identificador de presentador, el método comprende: (a) en un/el servidor que recibe la comunicación de aparato de aceptación; (b) en un/el servidor que recibe la comunicación de aparato de presentación; (c) en un/el

5 servidor que busca hacer coincidir el código clave compartido una vez apagado contenido en la comunicación de aparato de aceptación con el código clave compartido una vez apagado correspondiente contenido en la comunicación de aparato de presentación, (d) en un/el servidor que inicia

10 una búsqueda de un registro objetivo al conectar el código clave secreto (de presentador) contenida en la comunicación de aparato de aceptación y el identificador de presentador contenido en la comunicación de aparato de presentación, en donde ambas de dichas comunicaciones contienen el mismo

15 código clave compartido; (e) en un/el servidor que conduce una búsqueda de un registro objetivo que comprende tanto dicho código secreto (de presentador) y dicho identificador de presentador; (f) si se identifica un registro objetivo, en un/el servidor que identifica una entrada afiliada con

20 dicho registro objetivo, dicha entrada pertenece a las credenciales controladas conectadas al presentador; (g) en un/el servidor que pertenece a una recuperación de dicho grupo de credenciales identificado por dicha entrada afiliada al registro objetivo, y que permite una liberación

25 de dicho grupo de credenciales a dicho punto final de red,

dicho punto final es el receptor permitido de un grupo de credenciales controladas conectadas al presentador, y dicho punto final es cualquiera del aparato de aceptación o aquel de una tercera parte designada conectada al aparato de aceptación.

El registro objetivo en dicho servidor además también puede comprender un alias asociado con dicha entrada que pertenece a cada grupo de credenciales conectado al presentador, y la comunicación de aparato de presentación además puede contener una copia de un alias seleccionado de una lista de alias detallada en el aparato de presentación, en donde el paso de conducir 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 alias además del mismo identificador de presentador y código clave secreto.

La entrada que pertenece al grupo de credenciales conectado al presentador también puede estar comprendida en dicho registro objetivo en dicho servidor de control configurado para permitir la recuperación y liberación del grupo de credenciales conectado al presentador, y los pasos de recuperar el grupo de credenciales conectado al presentador y liberar el grupo de credenciales conectado al

presentador se realizan en dicho servidor de control configurado para permitir la recuperación y liberación del grupo de credenciales conectado al presentador.

El grupo de credenciales conectado al presentador puede estar comprendido en entradas separadas en un servidor diferente de manera separada de dicho servidor de control configurado para permitir la recuperación y liberación del grupo de credenciales conectado al presentador, la entrada separada está afiliada con el registro objetivo, en donde los pasos de recuperar y liberar el grupo de credenciales se realiza en cualquiera de dicho servidor de control configurado para permitir la recuperación y liberación del grupo de credenciales conectado al presentador o dicho servidor diferente separado de ese servidor de control configurado para permitir la recuperación y liberación del grupo de credenciales conectado al presentador.

Un periodo de validez puede ser asignado 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 aceptación o/y en la comunicación de aparato de presentación, en donde el paso de buscar coincidencia del código clave compartido contenido en una comunicación de aparato de aceptación y el código clave compartido contenido en la comunicación de

aparato de presentación además comprende establecer si ha expirado el periodo de validez. Esto asegura que si una comunicación de aparato de aceptación no coincide con una comunicación de aparato de presentación como se discute a continuación dentro de cierto periodo (el periodo de validez), entonces tal interacción/notificación/comunicación transcurre y con ello se vuelve vacía haciendo procesos adicionales redundantes. En donde cualquier periodo de validez transcurre y se vuelve vacío haciendo procesos adicionales redundantes, pueden purgarse los datos que pertenecen a la comunicación, liberando recursos para el procesamiento de comunicaciones adicionales. En donde se generan/transmiten/reciben cualquiera de las comunicaciones y contienen códigos clave compartidos que tienen un periodo de validez, el periodo de validez puede asegurar los códigos clave compartidos más cortos, menos complejos que pueden utilizarse debido a que con ello es factible la reutilización de código clave compartido. Después de la expiración del periodo de validez de un código clave compartido, el mismo código clave compartido puede ser reutilizado en una iteración subsecuente del método.

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

La comunicación de aparato de aceptación además puede contener 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 para hacer coincidir códigos clave compartidos además comprende el paso de buscar 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 aceptación.

Un aspecto adicional de la invención comprende un método para permitir una comunicación de un grupo de credenciales controladas conectadas a un presentador, en un servidor a un punto final de red, mientras se mantiene la privacidad que prevalece en las credenciales conectadas al presentador, un permiso hecho/otorgado de conformidad con cualquiera de los aspectos de la invención descrita anteriormente, el método comprende: (a) en un/el servidor que recibe la comunicación de aparato de aceptación; (b) en un/el servidor que recibe la comunicación de aparato de aceptación; (c) en el servidor que busca hacer coincidir el código clave compartido una vez apagado contenido en la comunicación de aparato de aceptación y el código clave compartido una vez apagado correspondiente contenido en la

comunicación de interactor de presentación, (y con ello hacer coincidir 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 al conectar 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 que conduce una búsqueda de un registro objetivo que comprende dicho código clave secreto y dicho identificador de presentador; (f) si se identifica un registro objetivo, identificar una entrada que pertenece a un grupo de credenciales conectado al presentador y asociado; (g) si se identifica un grupo de credenciales conectado al presentador, en un/el servidor que permite una recuperación del grupo de credenciales conectado al presentador, y permitir una liberación de dicho grupo de credenciales conectado al presentador a dicho punto final de red, dicho punto final es el receptor permitido del grupo de credenciales conectado al presentador, y dicho punto final es cualquiera del aparato de aceptación o aquel de una tercera parte designada conectada al aparato de aceptación.

Si dichos grupos de credenciales conectados al presentador están comprendidos en dichos registros y dicho servidor de control configurado para permitir la

recuperación y liberación de las credenciales controladas, los pasos de recuperar el grupo de credenciales de presentador conectado y comunicar el grupo de credenciales de presentador conectado puede realizarse en dicho servidor de control configurado para permitir la recuperación y liberación de las credenciales controladas.

Si dichos grupos de credenciales conectados 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 identificar una entrada que pertenece a un grupo de credenciales de presentador conectado puede realizarse en dicho servidor diferente separado a dicho servidor de control configurado para permitir la recuperación y liberación de las credenciales controladas), los pasos de recuperar el grupo de credenciales conectado y liberar el grupo de credenciales conectado pueden realizarse en cualquiera del servidor de control configurado para permitir la recuperación y liberación del grupo de credenciales conectado al presentador o el servidor diferente separado de ese servidor de control configurado para permitir la recuperación y liberación del grupo de credenciales conectado al presentador.

El paso de buscar coincidencia de los códigos

clave compartidos además puede comprender establecer si ha expirado el periodo de validez.

El paso de buscar coincidencia de los códigos clave compartidos además puede comprender buscar
5 coincidencia del 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 periodo de validez al código
10 clave compartido una vez apagado, dicho código clave compartido puede ser único por la duración de su periodo de validez.

En otro aspecto de la invención, un método que comprende (a) un aparato de aceptación que pone a
15 disponibilidad un código clave compartido una vez apagado al interactor de presentación; (b) recibir un código clave secreto de presentador que pertenece al interactor de presentación en el aparato de aceptación de dicho código clave secreto de presentador se ingresa en la terminal
20 mediante el interactor de presentación; (c) comunicar una comunicación de aparato de aceptación del aparato de aceptación al servidor, la comunicación de aparato de aceptación comprende el código clave compartido una vez apagado y el código clave secreto de presentador; (d) el
25 aparato de presentación recibe el código clave compartido

una vez apagado; (e) el aparato de presentador recupera un identificador de presentador que pertenece al interactor de presentación de una ubicación de almacenamiento en el componente periférico o aparato de presentación; y (f) el

5 componente periférico de presentación comunica una comunicación de aparato de presentación al servidor de control, la comunicación de aparato de presentación comprende el código clave compartido una vez apagado, y el identificador del presentador.

10 El registro objetivo en dicho servidor además también puede comprender un alias asociado con dicha entrada que pertenece a cada grupo de credenciales conectado al presentador, y la comunicación de aparato de presentación además puede contener una copia de un alias

15 seleccionado de una lista de alias detallados en el aparato de presentación, y en donde el paso de conducir una búsqueda de un registro objetivo que comprende el mismo identificador de presentador y código clave secreto también utiliza el alias contenido en la comunicación de aparato de

20 presentador para buscar un registro objetivo que comprende el mismo alias además del mismo identificador de presentador y código clave secreto.

 El grupo de credenciales puede estar comprendido como una entrada en dicho registro objetivo en dicho

25 servidor de control configurado para permitir la

recuperación y liberación de las credenciales controladas, y los pasos de recuperar el grupo de credenciales y liberar el grupo de credenciales se realizan en dicho servidor de control configurado para permitir la recuperación y liberación de las credenciales controladas.

El grupo de credenciales puede estar comprendido como un 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 está afiliada con el registro objetivo, y en donde los pasos de recuperar y liberar el grupo de credenciales puede realizarse en cualquiera de dicho servidor de control configurado para permitir la recuperación y liberación de las credenciales controladas o el servidor diferente separado a aquel 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 de aparato de presentación descritos anteriormente.

Otro aspecto de la invención comprende un aparato de aceptación configurado para realizar uno o más de los pasos de 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 modalidades como se describe anteriormente.

Un aspecto adicional de la invención comprende un medio de almacenamiento legible por computadora que transporta un programa de computadora almacenado en él, dicho programa comprende instrucciones ejecutables por computadora adaptadas para realizar uno o más de los pasos de métodos descritos anteriormente cuando se ejecutan por uno o más módulos de procesamiento.

DESCRIPCIÓN DETALLADA DE LA INVENCION

La Figura 1 es un diagrama que ilustra el sistema central para conservar privacidad, en una forma que también facilita liberación permitida de un grupo de credenciales almacenado a un receptor aprobado por el participante a quién pertenece el grupo de credenciales. El sistema 100 es seguro ya que protege los grupos de credenciales de acceso no autorizado por posibles receptores no autorizados de los grupos de credenciales, y también previene que los grupos de credenciales sean utilizados por aquellos que presentarían de manera fraudulenta un grupo de credenciales

como propio. Partes involucradas con el sistema son designadas como "presentadores" y "aceptadores" de conformidad con su papel en el método de la invención y su forma de interactuar con el sistema de la invención. En el

5 curso de una interacción entre un presentador y un aceptador, puede ser necesario que el presentador libere un grupo de credenciales con el cual está asociado. Los presentadores y aceptadores activamente involucrados en tal interacción son designados respectivamente como

10 "interactores de presentación" e "interactores de aceptación". Se apreciará que en muchas modalidades de la invención, cada uno de los presentadores está asociado con grupos de credenciales que son únicos para ellos de manera que los presentadores están relacionados con los grupos de

15 credenciales en una forma "uno a uno". Sin embargo, la invención también prevé escenarios en donde puede haber una relación "muchos a uno" entre presentadores y grupos de credenciales, en donde muchos presentadores están asociados con un grupo de credenciales único, y aún es deseable

20 mantener dicho grupo de credenciales en un estado de privacidad.

De conformidad con una modalidad de la invención, se utiliza el sistema y método de la invención por tal interactor de presentación para liberar un grupo de

25 credenciales asociado con dicho interactor de presentación

para uno o más receptores designados en una forma que mantiene la privacidad del grupo de credenciales. De conformidad con otras modalidades de la invención, el sistema y método de la invención puede utilizarse por un

5 interactor de aceptación para liberar un grupo de credenciales asociado con el interactor de aceptación para uno o más receptores designados mientras se conserva dicho estado de confidencialidad. Otras modalidades de la invención prevén descripción concurrente de ambos grupos de

10 credenciales de presentador y de aceptador asociando respectivamente con interactor de presentación e interactor de aceptación. Tanto el presentador como el aceptador cooperan para facilitar la liberación de tales grupos de credenciales del sistema. El receptor designado puede ser

15 el interactor de aceptación, el interactor de presentación o puede ser una tercera parte confiada.

El sistema 100 comprende al menos un servidor 101, el servidor comprende una colección de registros de presentador 102. Cada registro de presentador pertenece a

20 un participante dado que se ha inscrito como un presentador con dicho servidor 101, y cada registro comprende el uno o más grupos de credenciales que pertenecen a ese presentador. Más particularmente, cada registro de presentador comprende un identificador de presentador, un

25 código clave secreto del presentador, al menos un grupo de

credenciales asociadas con dicho presentador, y al menos un alias, en donde cada grupo de credenciales está conectado respectivamente con un alias por lo cual cada alias dentro de un registro de presentador se puede distinguir de los alias restantes para ese registro de presentador. El identificador de presentador es una secuencia única que se utiliza para identificar un registro de presentador dado para la colección de registro de presentador. El código clave secreto de presentador es una secuencia conocida únicamente por el presentador. Cuando un presentador interactúa con el sistema con un objetivo para liberar un grupo de credenciales de presentador a un receptor designado (tal presentador es denominado como un "interactor de presentación"), proporcionan su identificador de presentador, y su código clave secreto de presentador que puede utilizarse para autenticar el interactor de presentación antes que se libere cualquiera de los grupos de credenciales. Además del identificador de presentador y el código clave secreto de presentador, cada registro de presentador comprende al menos un grupo de credenciales. Como se describió previamente, cada grupo de credenciales comprende un grupo de datos personales que es particular para un individuo y necesario para una interacción dada. Cada grupo de credenciales también está asociado con un alias distinguible. A manera de

ilustración, un individuo por el nombre de "John Brown" puede tener un primer grupo de credenciales que pertenece a una licencia para conducir, y un segundo grupo de credenciales que pertenece a una tarjeta de lealtad de tienda. El primer grupo de credenciales puede comprender el nombre "John Brown", una fecha de nacimiento, un número de licencia para conducir, y una fecha de expiración. El segundo grupo de credenciales puede comprender el nombre "John Brown", una dirección, y un número de membresía de club de lealtad. El primer grupo de credenciales puede estar asociado con el alias "licencia para conducir", mientras el segundo grupo de credenciales puede estar asociado con el alias "tarjeta de lealtad 1". Se apreciará que en modalidades de la invención en donde se prevé que cada registro de presentador comprende únicamente un grupo de credenciales, puede no ser necesario que los registros de presentador además comprendan un alias conectado a cada grupo de credenciales. Más bien, en tales casos, identificación del registro que pertenece al presentador de interacción automáticamente también indicará que se va a liberar el grupo de credenciales.

Además, en algunas modalidades 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 grupos de credenciales asociados con el aceptador. Cada registro de aceptador además comprende un identificador de aceptador, y opcionalmente un código clave secreto de aceptador. El identificador de aceptador es una secuencia única que se utiliza para identificar un registro de aceptador dado dentro de la colección de registro de aceptador. El código clave secreto de aceptador (si es aplicable) es una secuencia conocida únicamente para el aceptador. Cuando un aceptador interactúa con el sistema con un objetivo de facilitar la liberación de un grupo de credenciales de presentador asociado con el interactor de presentación con un receptor designado (tal aceptador se denomina como un "interactor de aceptación"), el identificador de aceptador del interactor de aceptación se proporciona, y el código clave secreto del aceptador de interactor de aceptación (si se utiliza) entonces puede emplearse para autenticar el interactor de aceptación antes que se describa cualquiera de los grupos de credenciales.

Se apreciará que aunque en esta modalidad descrita de la invención, los registros de presentador y registros de aceptador son distintos y típicamente se mantienen como colecciones de registro separadas, en otras modalidades de la invención, el servidor 101 puede

comprender una colección de registro única que comprende tanto registros de presentador como de aceptador. Además, también se apreciará que aunque en una modalidad, los grupos de credenciales de un aceptador y/o presentador se
5 almacenan en un servidor, también se prevén múltiples servidores, con cada servidor con la tarea del almacenamiento de registros que comprende uno o más tipos de grupo de credenciales.

Adicionalmente se prevé que en algunas
10 modalidades de la invención, el servidor 101 únicamente comprenderá registros de presentador, y no comprenderá registros de aceptador. Preferiblemente, en tales modalidades, el servidor 101 e interactores de aceptación
15 potenciales serán capaces de comunicarse entre sí a través de sus sistemas de software existentes. Esta modalidad de la invención es ventajosa debido a que no se requiere pre-inscripción de aceptadores, y esto remueve un obstáculo para aceptación del sistema y métodos reivindicados entre
20 interactores de aceptación potenciales. Por lo tanto esto mejora facilidad de uso del sistema y método.

El servidor 101 se puede comunicar con uno o más aparatos 108 por un canal de comunicación. Se apreciará que el canal de comunicación 106 puede comprender el Internet, una red de propiedad, o una combinación de los dos. El
25 aparato 108 puede estar localizado de manera errónea, y

pueden conectarse al canal de comunicación 106 a manera de una o más de un área de tecnologías, tal como PSTN, Ethernet, DSL, ISDN, Wi-Fi, WiMax, 2G, 3G, LTE, 4G, etc. Los aparatos 108 pueden ser cualquiera de una variedad de dispositivos incluyendo computadoras personales de escritorio, laptops, computadoras personales de tableta, asistentes digitales personales, teléfonos móviles, teléfonos inteligentes, etc. El aparato 108 puede comprender alternativamente sistemas de cómputo personalizados como se utilizan en una variedad de industrias incluyendo bancarias, financieras, de aviación, de viajes, de seguridad nacional, de control fronterizo, de energía, de transporte, minoristas y/o de telecomunicaciones. Por consiguiente, los aparatos pueden comprender dispositivos configurados para actuar como dispositivo de Punto de Venta. En el contexto de la invención, estos aparatos se denominarán como "aparatos de aceptación".

El servidor 101 también se puede comunicar sobre un canal de comunicación 107 con uno o más aparatos 109. Tales aparatos pueden componer, por ejemplo, dispositivos inalámbricos que se pueden comunicar con el servidor 101 a través de una estación de base inalámbrica o enrutador. Los dispositivos inalámbricos pueden comprender cualquier forma de dispositivo inalámbrico incluyendo laptops, computadoras

personales de tableta, asistentes digitales personales, teléfonos móviles, teléfonos inteligentes, etc. Tales dispositivos periféricos además pueden comprender dispositivos que se pueden comunicar por el canal de comunicación 104 a través de una conexión por cable, y de esa forma pueden, por ejemplo, incluir computadoras de escritorio así como sistemas de cómputo personalizados 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 serán denominados como "componentes periféricos de presentación". En una modalidad, el componente periférico de presentación también puede estar protegido por contraseña o puede requerir permiso adicional del presentador para iniciar comunicación. Los componentes periféricos de presentación pueden estar localizados de manera errónea, y pueden comunicarse con el servidor 101 por el canal de comunicación 107 a través de una variedad de medios tal como PSTN, Ethernet, DSL e ISDN. Componentes periféricos de presentación que comprenden dispositivos inalámbricos pueden comunicarse con el enrutador 103 a manera de uno o más de una variedad de tecnologías de comunicaciones inalámbricas tal como Wi-Fi, WiMax, 2G, 3G, LTE, 4G, etc. El canal de comunicación 107 puede comprender el Internet, una red de propiedad, o una combinación de los

dos. Los componentes periféricos de presentación están configurados con una aplicación que facilita comunicación con el servidor 101. Ya que la conexión entre los aparatos de aceptación 109 y el servidor 101 comprende un primer canal de comunicaciones 106 y la conexión entre los aparatos de presentación comprenden un segundo canal de comunicaciones 107, el sistema 100 puede ser considerado como siendo "Multicanal" en composición. Esto asegura un mecanismo más seguro por el cual los grupos de credenciales y otros datos delicados pueden almacenarse y liberarse al punto final de red 110 mientras permanecen en un estado de confidencialidad. El punto final de red 110 en algunas modalidades puede ser un aparato separado o el mismo aparato de aceptación dependiendo del destino designado en la comunicación de aparato de aceptación.

Aunque en esta modalidad, se ha descrito que los grupos de credenciales y alias conectados están comprendidos en los registros de presentador y/o aceptador en el servidor, en otras modalidades de la invención, se anticipa que dichos grupos de credenciales y alias conectados pueden afiliarse con dichos registros de presentador y/o de aceptador en formas alternativas. Por ejemplo, los grupos de credenciales y alias afiliados pueden estar comprendidos en uno o más grupos de registro separados del(de los) grupo(s) de registro en el servidor

que comprende(n) los registros que comprenden los identificadores y claves secretas. Estos grupos de registro separados pueden ser alojados en uno o más servidores diferentes. En algunas modalidades de la invención, los diferentes servidores que alojan los grupos de credenciales se administran por los controladores responsables de la emisión de los instrumentos que comprenden dichos grupos de credenciales.

La Figura 2 es un cuadro de flujo que ilustra como un nuevo solicitante potencial participa con el servidor 101 como un presentador de conformidad con una modalidad de la invención. En el paso 200, se accede a una página web alojada por el servidor 101 mediante el nuevo solicitante de presentador, preferiblemente utilizando su componente periférico de presentación 105, 107, y 109. La página web está configurada de manera que en este paso, el nuevo solicitante de presentador proporciona detalles de inscripción tal como nombre, dirección, dirección de correo electrónico, país de residencia, etc., y envía estos al servidor 101. Se apreciará que aunque en algunas modalidades, esta invención, los detalles de inscripción se proporcionan directamente al servidor 101, en otras modalidades, los detalles de inscripción pueden ser proporcionados previamente de manera indirecta para el pre-procesamiento previo a la entrada de los detalles en el

servidor 101. La página web puede ser accedida por una conexión por la duración del procedimiento, o también simplemente pueden utilizarse conexiones seguras sólo en donde se está transmitiendo información delicada (tal como un grupo de credenciales o datos adicionales tal como un código clave secreto de presentador). También se apreciará que son posibles medios alternativos de inscripción tal como a manera de envío de una forma completada por correo, fax, etc.

Entonces, en el paso 202, se crea una nueva cuenta en el servidor 101 para el solicitante de presentador. Esto se hace al generar un nuevo registro de presentador en la colección de registros de presentador. Ya sea en el paso 200 o en el paso 202, se incita al nuevo solicitante de presentador a seleccionar e ingresar un nuevo código clave secreto de presentador, que entonces se agrega al registro de presentador del nuevo solicitante del presentador. En modalidades alternativas de la invención, el nuevo registro de presentador puede proporcionarse automáticamente con un código clave secreto de presentador temporal, que puede actualizarse subsecuentemente a un código clave secreto de presentador personalizado por el solicitante de presentador después de eso. Tal código clave secreto temporal puede proporcionarse a manera de la página web, o preferiblemente puede a manera de un segundo canal

de comunicación que puede comprender cualquier forma de comunicación, incluyendo correo electrónico, mensajería SMS, llamada telefónica o entrega. En algunas modalidades de la invención hay alcance adicional para proporcionar un
5 código clave secreto de reemplazo por ejemplo, en el caso de que se olvide o esté comprometido el código clave secreto original. Tales claves secretas de reemplazo pueden proporcionarse similarmente a través de cualquier forma de comunicación incluyendo a través de un sitio web, correo
10 electrónico, SMS, llamada telefónica o entrega.

En el paso 204, el nuevo solicitante de presentador es incitado a agregar grupos de credenciales a una cuenta recientemente creada del nuevo solicitante de presentador. Como se describió previamente, estos grupos de
15 credenciales pueden comprender una variedad de datos personales, y pueden pertenecer a instrumentos que tienen grupo de credenciales por una variedad de diferentes cuerpos de supervisión gubernamentales o comerciales. Cada grupo de credenciales estará conectado a un alias único
20 para su registro de presentador padre (es decir, cada alias es "localmente único"). En una modalidad, el nuevo solicitante de presentador puede ser incitado en el paso 206 al proporcionar un alias localmente único para cada grupo de credenciales proporcionado. En otra modalidad,
25 puede proporcionarse un alias predeterminado para cada

grupo de credenciales. En una modalidad, los alias pueden ser subsecuentemente editables por el presentador. En algunas modalidades de la invención, el registro de presentador puede ser editable después de inscripción al grado que los grupos de credenciales existentes y alias conectados puedan editarse o eliminarse y/o que puedan agregarse nuevos grupos de credenciales y alias conectados. En algunas modalidades de la invención, el registro de interactor de presentación puede ser editable después de inscripción al grado que los grupos de credenciales existentes y alias conectados puedan editarse o eliminarse y que pueden agregarse nuevos grupos de credenciales y alias conectados.

En el paso 206, se proporciona el nuevo solicitante de presentador con la oportunidad de establecer preferencias específicas asociadas con el procesamiento y uso de grupos de credenciales asociados con cuerpos de supervisión gubernamentales o comerciales particulares y los tipos de interacción a los cuales pertenecen. A manera de ejemplo, con respecto a un grupo de credenciales que pertenece a una membresía de lealtad de aerolínea, al presentador se le puede proporcionar la opción de establecer preferencias adicionales de conformidad con sus preferencias de membresía, tal como comida de aerolínea preferida, referencia de asiento, o aeropuerto local. A

manera de un ejemplo adicional, con respecto a un grupo de credenciales que pertenece a una tarjeta de crédito, al presentador se le puede proporcionar la opción de permitir funcionalidades tal como uso de preferencia de tarjeta, conversión de divisa directa, reembolso de impuestos al valor agregado para viajeros o dividir pago en múltiples tarjetas.

En el paso 208, el nuevo solicitante de presentador entonces es incitado a instalar una aplicación personalizada en su componente periférico de presentación. La aplicación personalizada está configurada para facilitar comunicación con el servidor como se requiera durante el proceso de permitir que el servidor libere un grupo de credenciales y el proceso de autenticar tal permiso transmitido se describirá en mayor detalle a continuación. Durante el curso de instalar la aplicación personalizada, la aplicación está asociada con un identificador de presentador único que se retiene en el componente periférico de presentación. En una modalidad preferida, el identificador de presentador es asignado por el servidor, y se incorpora en la aplicación antes, durante o después que se instala la aplicación en el componente periférico de presentación. Alternativamente, el identificador de presentador puede derivarse de una secuencia de caracteres nativos para el componente periférico de presentación, por

ejemplo, un número IMEI o número de serie. Esta secuencia de caracteres puede modificarse para llegar a un identificador de presentador único. Además de retención en el componente periférico de presentación, el identificador de presentador también se agrega al registro de presentador en la colección de registro de presentador en el servidor 101. Durante el curso de instalar la aplicación personalizada, también se proporciona la aplicación con los alias conectados a los grupos de credenciales almacenados en el paso 204 para un presentador dado. Por consiguiente, cuando se utiliza la aplicación en una interacción por el nuevo presentador, tiene a su disposición tanto un identificador de presentador como alias conectados a los grupos de credenciales del nuevo presentador de manera que el identificador de presentador y un alias puedan comunicarse al servidor 101 como sea apropiado.

En una modalidad preferida, inicialmente puede instalarse una versión genérica de la aplicación en un componente periférico de presentación del nuevo solicitante de presentador. Subsecuente al proceso ilustrado en los pasos 200-208, puede incitarse al nuevo solicitante de presentador a autenticar su cuenta al responder a un correo electrónico, y/o al confirmar su código clave secreto de presentador en respuesta a un aviso del servidor. Subsecuente a esta autenticación, la versión

genérica de la aplicación en el componente periférico de presentación del nuevo solicitante presentador puede personalizarse con el identificador de presentador del nuevo solicitante de presentador, los alias conectados a los grupos de credenciales del nuevo solicitante de presentador, y las preferencias del nuevo solicitante de presentador como se configura en el paso 206. Estos datos pueden almacenarse en un formato codificado criptográficamente en el componente periférico de presentación del nuevo solicitante de presentador. La Figura 3 es un cuadro de flujo similar a aquel de la Figura 2 que ilustra los pasos a través de los cuales una parte puede inscribirse como un aceptador con el servidor '101 de conformidad con una modalidad de la invención. Como se indicó previamente, la invención prevé modalidades en donde el aceptador debe inscribirse activamente con el servidor, así como modalidades en donde no es necesario que el aceptador se inscriba con el servidor. Además, en otras modalidades de la invención, la inscripción del aceptador puede realizarse "pasivamente" como se describirá en 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 denominado como un "nuevo solicitante de aceptador"), que preferiblemente utiliza el aparato de aceptación 111. En una forma análoga el paso 200 de la

Figura 2, la página web está configurada de manera que en este paso, el nuevo solicitante de aceptador proporcione detalles de inscripción generales tal como el nombre del individuo u organización, dirección, dirección de correo electrónico, etc., y envíe a éstos al servidor 101. La página web puede ser accedida por una conexión segura por la duración del procedimiento, o también simplemente pueden utilizarse conexiones seguras sólo en donde se está transmitiendo información sensible (tal como un código clave secreto de aceptador o un grupo de credenciales de aceptador). Además se apreciará que la inscripción del nuevo solicitante de aceptador puede llevarse a cabo a manera de otros medios tal como por correo electrónico o fax. Alternativamente, si el aceptador opera un aparato de aceptación que es controlado de forma remota por una tercera parte conectada (tal como, por ejemplo, Sistemas de Manejo de Terminal utilizados por Adquirientes para manejar dispositivos de Punto de Venta de pago de tarjeta, la inscripción de un aceptador puede iniciarse por la tercera parte conectada. En tales escenarios, puede no ser necesario que el aceptador proporcione cualquiera de las mismas informaciones.

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

Con el fin de disposición para descripción de un grupo de credenciales de presentador, debe proporcionarse permiso como se describe adicionalmente a continuación. En una modalidad de la invención, cualquier permiso que emane de un aceptador para liberación de un grupo de credenciales de presentador requerirá que se identifique al aceptador, y por ello, cualquier permiso para la liberación de un grupo de credenciales de presentador puede requerir la provisión inicial de un grupo de credenciales de aceptador. Por consiguiente, se prevé que sólo para los registros de presentador, se requiera un grupo de credenciales de aceptador separado en un registro de aceptador para cada tipo de interacción en el que desea participar un aceptador. Los tipos de interacción pueden definirse ampliamente, por ejemplo, la liberación de un instrumento o licencia para conducir y la liberación de un instrumento de tarjeta de pago pueden considerarse como diferentes tipos de interacción. Alternativamente, pueden definirse tipos de interacción de manera estrecha, por ejemplo la liberación de diferentes instrumentos de tarjeta de pago (por ejemplo, débito Mastercard, Visa) pueden considerarse como diferentes tipos de interacción. Por consiguiente, aunque en algunas modalidades, por ejemplo, un grupo de credenciales de aceptador puede generalmente aplicar a todas las tarjetas de pago, en otras modalidades, un

aceptador puede tener un grupo de credenciales diferente para cada tipo de tarjeta de pago diferente retenido por el aceptador.

5 En el paso 306, al nuevo solicitante de aceptador se le proporciona la oportunidad de establecer preferencias específicas asociadas con el procesamiento y uso de grupos de credenciales asociados con tipos de interacción particulares. A manera de ejemplo, con respecto a un grupo de credenciales que pertenece una tarjeta de crédito, al
10 nuevo solicitante de aceptador se le puede proporcionar la opción de indicar si desean proporcionar funcionalidades descendentes asociadas con el grupo de credenciales una vez que se ha liberado el grupo de credenciales de aceptador, tal como conversión de divisa directa, reembolso de
15 impuesto al valor agregado para viajeros o dividir pagos en múltiples tarjetas.

 En el paso 308, el aparato de aceptación entonces está configurado de manera que pueda comunicarse con el servidor. Esto puede hacerse en una variedad de formas. En
20 modalidades de la invención en donde el aparato de aceptación es controlado de manera remota por una tercera parte, la tercera parte puede iniciar una reconfiguración automática del aparato de aceptación si se requiere. En otras modalidades de la invención, el nuevo solicitante de
25 aceptador puede iniciar configuración a través de

instalación de una aplicación personalizada en una forma similar a aquella descrita en la Figura 2.

La Figura 4 es un cuadro de flujo que ilustra el método para permitir la liberación de al menos un grupo de credenciales controladas conectado a un presentador mientras mantiene confidencialidad que prevalece en dichas credenciales de conformidad con una modalidad de la invención. El servidor control recibe una comunicación de aparato de aceptación que contiene un código clave secreto y un código clave compartido una vez apagado y una comunicación de aparato de presentación que contiene un identificador de presentador y un código clave compartido una vez apagado. En el paso 403, se comparan mensajes de comunicación. Una coincidencia no exitosa termina 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 al conectar 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 contenido en la comunicación de aparato de aceptación y comunicación de aparato de presentación. Si se encuentra un registro objetivo, el grupo de credenciales que pertenece a la ubicación de almacenamiento presente en el registro se recupera y

permite liberar 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. Se genera un código clave compartido una vez apagado mediante el aparato de aceptación y se transporta un aparato de presentación. El aparato de aceptación además recibe el código clave secreto de presentador y genera una comunicación que se va a enviar al servidor de control como se ilustra por 101 en la Figura 1. Dicha comunicación comprende el código clave secreto del presentador y el código clave compartido una vez apagado.

Las Figuras 6A y 6B describen el proceso realizado en el aparato de presentación. El identificador de presentador se recupera de la memoria. Una vez que se recibe el código clave compartido una vez apagado del aparato de aceptación, se transmite una comunicación que comprende el identificador de presentador y el código clave compartido una vez apagado 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 varias modalidades para almacenar registros en el servidor de control o servidor de credencial 101. En algunas modalidades, pueden enmascarse

y localizarse registros de interactores de presentación utilizando listas de búsqueda como se describe en las Figuras 7A y 7C. Puede haber otra modalidad en donde cada registro de interactor de presentador esté asociado con un alias.

Las Figuras 9A y 9B describen representaciones gráficas que pertenecen al proceso para comunicar mensajes en el servidor de control desde los interactores de presentación y de aceptación y el proceso para distribuir credenciales controladas a destinos permitidos. La Figura 10 es un diagrama de secuencia que ilustra el proceso por el cual puede proporcionarse permiso de conformidad con una modalidad de la invención que involucra un servidor 1001, interactor de presentación 1002, aparato de presentación 1003, punto final de red 1004, y aparato de aceptación 1005, para recuperar un grupo de credenciales en almacenamiento en una ubicación identificada por el interactor de presentación 1002 y liberar un grupo de credenciales a una instalación de un receptor permitido por el interactor de presentación 1002. Se apreciará que proporcionar permiso para recuperar y liberar un grupo de credenciales de presentador también puede estar acompañado con solicitud para recuperar un grupo de credenciales de aceptador simultáneamente, en donde el aparato de aceptación 1005 y el aparato de presentación 1003 aún

envían sus comunicaciones respectivas al Servidor 1001. Además se apreciará que en algunas modalidades de la invención, el permiso para liberar el grupo de credenciales específicamente será un permiso para liberar un grupo de credenciales de presentador (asociado con un interactor de presentación 1002) al punto final de red 1004 o a un aparato de aceptación 1005. Sin embargo, en otras modalidades de la invención el permiso compartirá el grupo de credenciales de aceptador o de presentador a aquel de una tercera parte confiada conectada al punto final de red 1004 o el aparato de aceptación 1005. Por ejemplo, en donde se envía permiso para compartir un grupo de credenciales de presentador que pertenece a un instrumento de tarjeta de pago; puede ser que se pretenda que el grupo de credenciales de tarjeta de pago se envíe a un procesador de transacción de tercera parte confiado.

En la Figura 10, un interactor 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 interactor de aceptación que comprende un punto final de red 1004 y/o 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 conectado a un aparato de aceptación 1005), y por lo cual

el aparato de aceptación está configurado para generar y transmitir una comunicación de aparato de aceptación al servidor 1001. El interactor de presentación 1002 puede decidir interactuar en tal instalación con un objetivo de

5 permitir una lectura de un grupo de credenciales conectado al interactor de presentación 1002 para liberarse al punto final de red 1004 o el aparato de aceptación 1005. El interactor de aceptación también puede decidir interactuar en tal instalación con un objetivo de solicitar una lectura

10 de un grupo de credenciales conectado al interactor de aceptación que se va a regresar al punto final de red 1004 o aparato de aceptación 1005 cuando se recibe el grupo de credenciales conectado al interactor de presentación 1002 en el punto final de red 1004 o el aparato de aceptación

15 1005. Más específicamente, se conserva un estado de confidencialidad que prevalece en las credenciales conectadas al interactor de presentación 1002 en la modalidad preferida de la presente invención, por lo cual una lectura del grupo de credenciales conectado al

20 interactor de presentación 1002 no es visible a o accesible por el interactor de aceptación no comunicado a o por el aparato de presentación 1003, pero únicamente comunicado confidencialmente al punto final de red 1004 o aparato de aceptación 1005.

25 En la Figura 10, y en el evento precedente 1010,

se transporta una señal en el punto final de red 1004 o el aparato de aceptación 1005 a un interactor de presentación 1002, que indica que dicho método ideado en la presente invención es un método disponible en el punto final de red 1004 con aparato de aceptación 1005 para el interactor de presentación 1002, por lo 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, dicho método ideado en la presente invención es uno de los datos disponibles en el punto final de red 1004 para obtener credenciales del interactor de presentación 1002.

En la Figura 10, y en el caso precedente 1011, un indicador de presentación 1002 decide iniciar una interacción en la instalación operada en el interactor de aceptación de conformidad con el proceso del método ideado por la presente invención al beneficiarse del aparato de presentación 1003 configurado para generar y transmitir una comunicación de aparato de presentación a tal servidor 1001, y beneficiarse de un aparato de aceptación 1005, configurado para generar y transmitir una comunicación de aparato de aceptación para tal servidor 1001. En efecto, el interactor de presentación 1002 selecciona iniciar una interacción en la instalación del interactor de aceptación de conformidad con el proceso del método ideado por la

presente invención, que rechaza al iniciar una interacción en la instalación operada en el interactor de aceptación de conformidad con cualquier otro proceso de métodos previos disponibles en el punto final de red 1004 para obtener credenciales del interactor de presentación 1002.

En la etapa 1012, se inicia una interacción al activar 1012 el aparato de aceptación 1005 que está configurado para facilitar comunicaciones de aparato de aceptación con el servidor 1001. En la activación en 1012, se produce 1012 un código clave compartido una vez apagado en el aparato aceptación 1005. En una modalidad de 1012, el código clave compartido se genera por el servidor 1001 y se transmite al aparato de aceptación 1005. En otra modalidad de 2012, el código clave compartido se genera en el aparato de aceptación 1005.

En la etapa 1013, se inicia una interacción al activar 1013 el aparato presentación 1003 que facilita comunicaciones de aparato de aceptación 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 modalidad en 1013, una lista de alias asociados con las credenciales conectadas al interactor de presentación 1002 se relaciona con el identificador de presentador también recuperado de la misma ubicación de almacenamiento en el

aparato de presentación 1003. En tal modalidad de 1012, la lista de alias asociada con las credenciales conectadas al interactor de presentación se detalla en el componente periférico de presentación 1003 para selección por el
5 identificador de presentador 1002.

En la etapa 1014, un código clave compartido se considera disponible 1014 en el aparato de aceptación 1005 para el interactor de presentación 1002 y el aparato de presentación 1003. En una modalidad de 1014, se considera
10 legible por humano en el aparato de aceptación 1005. En otra modalidad de 1014, se considera legible por máquina en el aparato de aceptación 1005.

En la etapa 1015, el código clave compartido se obtiene por consiguiente 1015 en el aparato de presentación
15 1003. En una modalidad de 1015, se obtiene al leerlo en el aparato de aceptación 1005 y al ingresarlo en el aparato de presentación 1003. En otra modalidad de 1015, se obtiene al escanearlo en el aparato de aceptación 1005 y al capturarlo en el aparato de presentación 1003. En una modalidad, el
20 aparato de aceptación 1005 transmite el código clave compartido una vez apagado directamente 1014 al aparato de presentación 1003, mientras en otra modalidad, el aparato de aceptación 1005 pone a disponibilidad el código clave compartido 1014 al interactor de presentación 1002, que lo
25 ingresa en el aparato de presentación 1003. En algunas

modalidades de la invención, puede asignarse un periodo de validez al código clave compartido. Esto asegura que si una comunicación de aparato de aceptación y una comunicación de aparato de presentación recibida no se corroboran dentro de

5 cierto período al buscar coincidencia de las claves compartidas una vez apagadas (como se discute además a continuación) dentro de cierto periodo (el periodo de validez), entonces la interacción puede transcurrir y con ello volverse vacía presentando procesos adicionales

10 redundantes. Después de expiración del periodo de validez de un código clave compartido, el mismo código clave compartido de esa forma puede reutilizarse en una iteración subsecuente del método. Por consiguiente, un periodo de validez puede asegurar que pueden utilizarse claves

15 secretas más cortas, menos complejas debido a que con ello es factible reutilización de código clave compartido. Es ventajoso en algunas modalidades de la invención en donde sea necesario que el interactor de presentación ingrese el código clave compartido en el componente periférico de

20 presentación, ya que la complejidad de código clave reducido hace esta modalidad del método más manejable.

En algunas modalidades, el aparato de presentación también puede presentar una lista de alias que pertenecen a diferentes grupos de credenciales de

25 presentador conectados a dicho interactor de presentación.

El interactor de presentación entonces selecciona un alias asociado con el grupo de credenciales deseado conectado al interactor de presentación.

En la etapa 1016, el aparato de aceptación busca
5 obtener el código clave secreto del interactor de presentación al incitar al interactor de presentación 1002 a ingresar el código clave secreto del presentador en el aparato de aceptación 1005. En una modalidad, el aparato de aceptación 1005 puede presentar adicionalmente en 1012 un
10 parámetro auxiliar predeterminado al interactor de presentación 1002 con el fin de correlacionar además la interacción y corroborar la comunicación del aparato de aceptación y la comunicación del aparato de presentación.

En 1017, el código clave secreto se obtiene 1017
15 mediante el aparato de aceptación 1005. En una modalidad, el interactor de presentación 1002 utiliza un teclado numérico para ingresar el código clave secreto en el aparato de aceptación 1005. En otra modalidad, el interactor de presentador 1002 puede utilizar un
20 dispositivo para transmitir el código clave secreto al aparato de aceptación 1005.

En la etapa 1019, el aparato de aceptación 1005 entonces transmite una comunicación de aparato de aceptación al servidor 1001 que permite liberación de un
25 grupo(s) de credenciales específico(s) conectado(s) al

interactor de presentación 1003 a la instalación del receptor permitido por el interactor de presentación 1002. La comunicación de aparato de aceptación contiene el código clave secreto de presentador como se obtiene en 1017 y el
5 código clave compartido una vez apagado como se genera en 1012. La comunicación de aparato de aceptación también puede contener un identificador que pertenece el interactor de aceptación si se recupera después de 1002 y cualquiera de los parámetros predeterminados auxiliares si se capturan
10 después de 1012.

En la etapa 1018, el aparato de presentación 1003 transmite una comunicación de aparato de presentación al servidor 1001 que permite recuperación del(de los) grupo(s) de credenciales específico(s) conectado(s) al interactor de
15 presentación 1002, en almacenamiento en la ubicación identificada por el interactor de presentación 1002. La comunicación de aparato de presentación contiene un identificador de presentador recuperado en 1013 y el código clave compartido una vez apagado obtenido en 1015. La
20 comunicación de aparato de presentación también contener un alias asociado con el grupo de credenciales elegido si se detalla en 1013 y seleccionado en 1016, y también puede contener cualquiera de los parámetros auxiliares predeterminados si se captura después de 1016.

25 En 1020, el servidor 1001 busca hacer coincidir

comunicaciones de aparato de aceptación recibidas y comunicaciones de aparato de presentación recibidas al buscar coincidencia de código clave compartido una vez apagado contenido en comunicaciones de aparato de aceptación y el código clave compartido una vez apagado contenido en comunicaciones de aparato de presentación. En algunas modalidades de 1020, la comunicación de aparato de aceptación y/o la comunicación de aparato de presentación puede asignarse con un periodo de validez 1020. Si la comunicación de aparato de aceptación y comunicaciones de aparato de presentación no coinciden con el periodo de validez designado, la interacción transcurre y se considera vacía presentando procesos adicionales redundantes. En donde una interacción transcurre y se vuelve vacía presentando procesos adicionales redundantes, los datos que pertenecen a la interacción (es decir, las comunicaciones de interactor) pueden purgarse del sistema, liberando recursos para el procesamiento de permisos recibidos adicionales. En otras modalidades de 1020, un valor o parámetros auxiliares predeterminados pudieron haberse combinado en la comunicación de aparato de aceptación en 1019 y comunicación de aparato de presentación en 1018. Si es así, se utiliza el valor además de código clave compartido como el parámetro auxiliar predeterminado para buscar una coincidencia de una comunicación de aparato de

aceptación y comunicación de aparato de aceptación en 1020.

En la etapa 1021, y en el caso que se encuentre una coincidencia en 1020, el servidor 1001 inicia una búsqueda al conectar 1021 el identificador de presentación contenido en la comunicación de aparato de aceptación 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 aparato de aceptación de conformidad con 1020. Si no se encuentra ninguna coincidencia en 1020, el método de esa forma no procede con 1021, y el Servidor 1001 puede regresar un mensaje de conformidad con el aparato de aceptación 1005 o el aparato de presentación 1003.

En la etapa 1022, el servidor 1001 conduce 1022 una búsqueda de un registro objetivo dentro de su colección de registro de presentador que comprende el identificador de presentador contenido en la comunicación de aparato de presentación coincidida y el código clave secreto contenido en la comunicación de aparato de aceptación coincidida. En una modalidad de 1022, y en el caso 1022 que un alias asociado con el identificador de presentador esté contenido en la comunicación de aparato de aceptación de conformidad con 1018, el alias también se utiliza para evaluar 1022 un registro objetivo que comprende ese alias además del

identificador de presentador y código clave secreto del interactor de presentación 1002.

En la etapa 1023, y en caso que un registro que comprende el identificador de presentador y código clave secreto del presentador que esté localizado en 1022, se continúa una búsqueda al identificar 1023 una entrada afiliada al registro objetivo localizado en 1022, en donde la entrada pertenece al grupo de credenciales conectadas al interactor de presentación 1002. (En una modalidad, el grupo de credenciales indicado puede ser el grupo de credenciales conectadas al alias seleccionado por el interactor de presentación en el paso 1022). En una modalidad, la entrada identificada contiene 1022 una lectura que comprende las credenciales conectadas al interactor de presentación 1002. En otra modalidad, la entrada identificada contiene 1022 un indicador que localiza las credenciales conectadas al interactor de presentación 1002. En caso de que un registro que comprende el identificador de presentador y código clave secreto de presentador no esté localizado en el paso 1022, el proceso de esa forma no procede con 1023 y el Servidor 1001 puede regresar un mensaje por consiguiente al aparato de aceptación 1005 y/o al aparato de presentación 1003.

En 1024, se completa una búsqueda al permitir una recuperación de una lectura de las credenciales al

interactor de presentación 1002 en almacenamiento en la ubicación identificada en 1023, y que permite una liberación de la lectura de las credenciales conectadas al interactor de presentación a la instalación del receptor permitido por el interactor de presentación 1002.

En la etapa 1025, se recupera una lectura del almacenamiento en la ubicación indicada por el interactor de presentación 1002. En una modalidad, se almacena y recupera 1025 una lectura en el servidor de control configurado para realizar el método ideado en 1020 a 1024. En otra modalidad, 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 receptor permitido por el interactor de presentación 1002. En una modalidad de 1026, se libera y distribuye el lector al punto final de red 1004. En otra modalidad de 1026, se libera y distribuye el lector al aparato de aceptación 1005.

En la Figura 10, y como los eventos subsecuentes a 1027 y 1028, se regresa un mensaje por el servidor 1001 al aparato de presentación 1003 para el interactor de presentación 1002, que indica si la lectura ha sido recibida como se identifica y se libera como se permite por el interactor de presentación 1002; en tales modalidades

complementarias, se retiene un registro en el servidor 1001 que enlista un estado de eventos ocurren entre 1020 y 1024, y se puede revisar entre el interactor de presentación 1002 en el aparato de presentación 1003.

5 Las modalidades de la invención descrita con referencia a las figuras comprenden un aparato de computadora y/o procesos realizados en un aparato de computadora. Sin embargo, la invención también se extiende a programas de computadora, particularmente programas de
10 computadora almacenados en o dentro de un portador adaptado para llevar la invención a la práctica. El programa puede estar en la forma de código de fuente, código de objeto, o una fuente intermedia de código y código de objeto, tal como en forma parcialmente recopilada o en cualquier otra
15 forma adecuada para uso en la implementación del método de conformidad con la invención. El portador puede comprender un medio de almacenamiento tal como ROM, por ejemplo, CD ROM, o medio de grabación magnético, por ejemplo, un disco flexible o disco duro. El portador puede ser una señal
20 eléctrica u óptica que puede transmitirse a través de un cable eléctrico u óptico o mediante radio u otros medios.

 Las palabras "comprende/que comprende" y las palabras "que tiene/que incluye" cuando se utilizan aquí con referencia a la presente invención se utilizan para
25 especificar la presencia de características, números

enteros, pasos o componentes mencionados, pero no obstaculizan la presencia o adición de una o más de otras características, números enteros, pasos, componentes o grupos de los mismos.

5 Se aprecia que ciertas características de la invención, que, para claridad, se describen en el contexto de modalidades separadas, también pueden proporcionarse en combinación con una sola modalidad. De manera inversa, varias características de la invención que, para brevedad,
10 se describen en el contexto de una sola modalidad, también pueden proporcionarse de manera separada o en cualquier sub-combinación.