(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 713 673**

(51) Int. CI.:

H04L 9/16 (2006.01)
H04L 12/24 (2006.01)
H04L 9/00 (2006.01)
H04L 9/32 (2006.01)
H04L 9/14 (2006.01)
G06F 21/41 (2013.01)
G06F 21/60 (2013.01)
H04L 9/08 (2006.01)
H04L 9/12 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **12.06.2015 PCT/CA2015/050543**

(87) Fecha y número de publicación internacional: **17.12.2015 WO15188277**

(96) Fecha de presentación y número de la solicitud europea: **12.06.2015 E 15806851 (0)**

(97) Fecha y número de publicación de la concesión europea: **24.10.2018 EP 3155754**

(54) Título: **Procedimientos, sistemas y producto de programa de ordenador para proporcionar encriptado en una pluralidad de dispositivos**

(30) Prioridad:

13.06.2014 US 201462011837 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.05.2019

(73) Titular/es:

BICDROID INC. (100.0%)
84 Milne Drive
Petersburg, Ontario N0B 2H0, CA

(72) Inventor/es:

YANG, EN-HUI;
YU, XIANG y
MENG, JIN

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

Observaciones:

Véase nota informativa (Remarks, Remarques o Bemerkungen) en el folleto original publicado por la Oficina Europea de Patentes

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Procedimientos, sistemas y producto de programa de ordenador para proporcionar encriptado en una pluralidad de dispositivos

Campo

Las realizaciones de la presente invención se refieren en general a la protección y al encriptado de datos, y más específicamente a procedimientos para la sincronización de archivos encriptados y al intercambio de archivos encriptados.

Antecedentes

A medida que las personas se vuelven más dependientes de las tecnologías informáticas y de Internet, la seguridad de los datos es cada vez más importante que nunca. Con las conexiones a Internet cada vez más ubicuas, es relativamente fácil acceder y distribuir los datos ampliamente a través del uso de nubes. Para disfrutar de los beneficios de la computación en la nube, las personas y las empresas a menudo cargan sus datos en servidores en la nube. Esto a menudo incluye datos privados o confidenciales, o cualquier dato que un usuario quiera proteger. Esto aumenta la posibilidad de que los datos privados e importantes se vean innecesariamente expuestos si se dejan sin proteger.

Por lo general, las personas dependen de los proveedores de servicios en la nube para garantizar la seguridad de sus datos. Sin embargo, el almacenamiento en la nube puede tener varias vulnerabilidades de seguridad asociadas. En su informe de 2013 ("The notorious nine: Cloud computing top threats in 2013, "http://www.cloudsecuritvalliance.org/topthreats"), la Alianza de Seguridad en la Nube identificó las nueve amenazas de seguridad más importantes para la computación en la nube, incluidas las violaciones de datos, la pérdida de datos, información interna maliciosa y problemas de tecnología compartida. Dichos problemas de seguridad de los datos no son deseables y pueden ralentizar la utilización de los servicios en la nube.

Una forma de mitigar los problemas de seguridad de datos es a través de la encriptación. Por ejemplo, se pueden usar herramientas independientes como Winzip y PDF seguro para encriptar archivos antes de que esos archivos se guarden y almacenen, carguen y/o transmitan. Sin la clave de desencriptado correspondiente, el archivo encriptado puede no ser comprensible.

Sin embargo, el uso de herramientas independientes tales como Winzip y PDF seguro para encriptar varios archivos en una carpeta tiene varios inconvenientes. Por ejemplo, a un usuario se le puede solicitar que ingrese una contraseña para encriptar cada archivo, y que ingrese la contraseña correspondiente para desencriptar el archivo encriptado para su visualización y/o modificación. Cuando aumenta el número de archivos, este enfoque se vuelve tedioso y no es fácil de usar. Además, el usuario puede confundirse fácilmente acerca de qué contraseña descifra qué archivo si se usan contraseñas diferentes para encriptar archivos diferentes. Además, la fuerza de encriptado en estos ejemplos depende de qué tan seguras sean las contraseñas elegidas por el usuario. Debido a la dificultad que experimentan los usuarios para crear y memorizar contraseñas aleatorias seguras, tienden a elegir contraseñas más débiles, y el encriptado resultante a menudo puede ser débil. Como resultado, los archivos encriptados con herramientas independientes pueden ser vulnerables a ataques sofisticados. Además, si las contraseñas se olvidan o se pierden, puede ser difícil o imposible recuperar los archivos de texto sin formato originales de los archivos encriptados. Esto da como resultado de manera efectiva una pérdida permanente de datos. Finalmente, cuando los archivos se encriptan utilizando herramientas independientes, compartir archivos encriptados entre un grupo de personas puede ser tedioso y, a menudo, requiere el uso de canales laterales para intercambiar contraseñas.

El documento US 2011/154041 A1 describe un procedimiento para transferir de forma segura un servicio desde un primer dispositivo móvil a un segundo dispositivo móvil, estando asociado el servicio con un servidor configurado para facilitar la provisión de servicios a los dispositivos móviles en una red de comunicaciones inalámbricas.

Sumario

La invención se define mediante las características de las reivindicaciones independientes. Realizaciones preferidas se definen mediante las características de las reivindicaciones dependientes.

De acuerdo con una primera realización descrita en el presente documento, se proporciona un procedimiento para proporcionar el encriptado en una pluralidad de dispositivos configurados para la comunicación electrónica con un servidor, incluyendo la pluralidad de dispositivos al menos un primer dispositivo y un segundo dispositivo. El procedimiento puede incluir generar una primera cuenta para un primer usuario que controle la pluralidad de dispositivos, donde la primera cuenta almacena los datos de la cuenta en una memoria de servidor no volátil, y los datos de la cuenta incluyen un identificador del primer usuario e información de autentificación de la cuenta. El procedimiento también puede incluir, para cada dispositivo en la pluralidad de dispositivos, instalar un agente de encriptado en ese dispositivo y operar un procesador del primer dispositivo bajo el control del agente de encriptado para generar aleatoriamente una pluralidad de indicadores de claves para: generar una la pluralidad de indicadores de claves encriptados de la pluralidad de indicadores de claves que utilizan una clave de encriptado del segundo

dispositivo, correspondiendo cada indicador de clave encriptado a uno de los indicadores de claves en la pluralidad de indicadores de claves; transmitir la pluralidad de indicadores de claves encriptados al servidor para impedir la exposición de los indicadores de claves al servidor; generar una pluralidad de valores de inicialización de clave basadas en la pluralidad de indicadores de claves, donde para cada valor de inicialización de clave, el agente de encriptado puede ser operable para controlar el procesador del primer dispositivo para generar una pluralidad de claves de encriptado independientes; y almacenar información de valor de inicialización de clave en base a la pluralidad de valores de inicialización de clave en la memoria del primer dispositivo no volátil. El procedimiento puede incluir además generar una cadena de estado de clave para la primera cuenta, incluyendo la cadena de estado de clave una porción de indicador de clave de servidor generada en función de la pluralidad de indicadores de claves encriptados; almacenar la cadena de estado clave en la memoria del servidor no volátil; recibir información de autentificación putativa en el segundo dispositivo; operar un procesador del segundo dispositivo, bajo el control del agente de encriptado instalado en el segundo dispositivo, para generar información de autentificación putativa del servidor en base a la información de autentificación putativa y transmitir la información de autentificación putativa del servidor al servidor; y operar el procesador del servidor para comparar la información de autentificación del servidor putativo con la información de autentificación de la cuenta, y proporcionar al segundo dispositivo acceso a la cadena de estado de clave si y solo si la información de autentificación del servidor putativo corresponde a la información de autentificación de la cuenta. El procedimiento también puede incluir operar el procesador del segundo dispositivo bajo el control del agente de encriptado para determinar la pluralidad de indicadores de claves de la pluralidad de indicadores de claves encriptados en la cadena de estado de clave usando la clave de desencriptado del segundo dispositivo; generar la pluralidad de valores de inicialización de clave en función de la pluralidad de indicadores de claves, donde para cada valor de inicialización de clave, el agente de encriptado puede ser operable para controlar el procesador del segundo dispositivo para generar la misma pluralidad de claves de encriptado independientes que el primer dispositivo, sin cualquiera de los valores de inicialización de clave, proporcionándose la información de valores de inicialización de clave y las claves de encriptado al segundo dispositivo; y almacenar la información de valor de inicialización de clave basada en la pluralidad de valores de inicialización de clave en la memoria del segundo dispositivo no volátil.

En algunas realizaciones, el procedimiento puede incluir la generación de la pluralidad de valores de inicialización de clave mediante la operación adicional del procesador del servidor para generar aleatoriamente los valores de clave de servidor para la primera cuenta, almacenar el servidor de valores de clave en la memoria del servidor no volátil, y transmitir los valores de la clave del servidor al primer dispositivo; y operar el procesador del primer dispositivo bajo el control del agente de encriptado para generar la pluralidad de valores de inicialización de clave basadas en los valores de clave del servidor y la pluralidad de indicadores de claves; donde el procesador del servidor puede operarse para proporcionar al segundo dispositivo acceso a los valores de clave del servidor si y solo si la información de autentificación del servidor putativo corresponde a la información de autentificación de la cuenta; y el procesador del segundo dispositivo puede ser operado, bajo el control del agente de encriptado, para generar la pluralidad de valores de inicialización de clave basadas en la pluralidad de indicadores de claves y los valores de clave del servidor.

En algunas realizaciones, el procedimiento puede incluir la operación del procesador del primer dispositivo, bajo el control del agente de encriptado, para generar la pluralidad de indicadores de claves encriptados por: definir un primer código de verificación; definir la clave de encriptado del segundo dispositivo basada en el primer código de verificación; y encriptar la pluralidad de indicadores de claves utilizando la clave de encriptado del segundo dispositivo; donde la clave de desencriptado del segundo dispositivo se puede generar al operar el procesador del segundo dispositivo bajo el control del agente de encriptado para definir un segundo código de verificación y generar la clave de desencriptado del segundo dispositivo basándose en el segundo código de verificación; y el segundo código de verificación puede ser el primer código de verificación.

En algunas realizaciones, el procedimiento puede incluir la operación de un procesador del primer dispositivo bajo el control del agente de encriptado para generar un código de servidor de encriptado basado en el primer código de verificación y transmitir el código de servidor encriptado al servidor, y almacenar el código de servidor encriptado en la información de autentificación de la primera cuenta, donde la información de autentificación putativa recibida en el segundo dispositivo puede ser un código de verificación putativo, la información de autentificación de servidor putativo puede ser un código de servidor encriptado putativo generado basándose en el código de verificación putativo, y la información de autentificación de servidor putativo corresponde a la información de autentificación de la cuenta si y solo si el código de servidor encriptado putativo coincide con el código de servidor encriptado.

En algunas realizaciones, el procedimiento puede incluir además proporcionar un archivo para ser encriptado y almacenado en el primer dispositivo, operando el procesador del primer dispositivo bajo el control del agente de encriptado para derivar una de las claves de encriptado de la información del valor de inicialización de clave que utiliza la información de codificación, encriptando y almacenando el archivo como un archivo encriptado en la memoria del primer dispositivo no volátil mediante la clave de encriptado derivada, y almacenando la información de la clave con el archivo encriptado en la memoria del primer dispositivo no volátil, donde la información del valor de inicialización de clave puede ser encriptada usando el primer código de verificación antes del almacenamiento.

En algunas realizaciones, el procedimiento puede además incluir recibir el archivo encriptado y la información de generación de claves en el segundo dispositivo, y operar el procesador del segundo dispositivo bajo el control del

agente de encriptado para derivar la clave de encriptado de la información de los valores de inicialización de clave almacenada en la memoria del segundo dispositivo no volátil utilizando la información de codificación recibida y desencriptar el archivo encriptado utilizando la clave de codificación derivada.

En algunas realizaciones, el procedimiento puede incluir además seleccionar de manera aleatoria información de generación de claves cuando el agente de encriptado recibe una indicación del archivo a encriptar.

En algunas realizaciones, el procedimiento puede incluir además operar el procesador del primer dispositivo bajo el control del agente de encriptado para definir un primer código de verificación, generar un código local encriptado basado en el primer código de verificación y almacenar el código encriptado local en la memoria del primer dispositivo no volátil. El procedimiento puede incluir además recibir una solicitud para acceder a los archivos y un código de verificación putativo local en el primer dispositivo, y operar el procesador del primer dispositivo bajo el control del agente de encriptado para generar un código local encriptado putativo, comparar el código local encriptado putativo con el código local encriptado para determinar si el código de verificación putativo local es el primer código de verificación, y proporcionar acceso a los archivos encriptados por el agente de encriptado si y solo si el código local encriptado putativo coincide con el código local encriptado.

En algunas realizaciones, el procedimiento puede incluir almacenar la información de valores de inicialización de clave mediante el encriptado de la pluralidad de valores de inicialización de clave usando el primer código de verificación, y almacenar la pluralidad encriptada de valores de inicialización de clave en la primera memoria del dispositivo no volátil.

En algunas realizaciones del procedimiento, el primer usuario puede incluir una pluralidad de usuarios del grupo, que puede incluir al menos un usuario del grupo administrativo y un segundo grupo de usuarios. En algunas realizaciones del procedimiento, cada uno de los usuarios del grupo puede tener el control de al menos uno de los dispositivos en la pluralidad de dispositivos, donde el usuario del grupo administrativo puede tener el control del primer dispositivo y el segundo usuario del grupo puede estar en control del segundo dispositivo. En algunas realizaciones del procedimiento, para cada usuario del grupo en la pluralidad de usuarios del grupo, los datos de la cuenta pueden comprender además una clave pública específica del usuario, donde la clave pública específica del usuario para cada usuario puede generarse basándose en una clave privada específica del usuario almacenada en una memoria no volátil de un dispositivo correspondiente en la pluralidad de dispositivos. En algunas realizaciones del procedimiento, para cada usuario del grupo en la pluralidad de usuarios del grupo, el procesador del primer dispositivo puede ser operado bajo el control del agente de encriptado para generar la pluralidad de indicadores de claves encriptados generando una pluralidad de indicadores de claves encriptados que utilizan la clave pública específica del usuario para ese usuario. En algunas realizaciones del procedimiento, la porción del indicador de clave del servidor de la cadena de estado de clave para la primera cuenta puede incluir, además, para cada usuario del grupo en la pluralidad de usuarios del grupo, una parte de la cadena específica del usuario que se puede generar en función de la pluralidad de los indicadores de claves encriptados específicos del usuario para ese usuario del grupo. En algunas realizaciones del procedimiento, el procesador del segundo dispositivo puede ser operado bajo el control del agente de encriptado para determinar la pluralidad de indicadores de claves de la pluralidad de indicadores de claves encriptados específicos del usuario en la parte específica del usuario de la porción del indicador de la clave del servidor correspondiente al segundo usuario del grupo que usa la clave privada del segundo dispositivo.

En algunas realizaciones del procedimiento, la información de autentificación de cuenta para la primera cuenta puede incluir, para cada grupo de usuarios en la pluralidad de usuarios del grupo, un código de encriptado del servidor específico del usuario. En algunas realizaciones del procedimiento, el código encriptado del servidor específico del usuario para cada usuario se genera al operar un procesador de un dispositivo en la pluralidad de dispositivos correspondientes a ese usuario, bajo el control del agente de encriptado para: definir un usuario específico el código de verificación, generar el código encriptado del servidor específico del usuario basado en el código de verificación específico del usuario y transmitir el código encriptado del servidor específico al usuario; y almacenar el código encriptado del servidor específico del usuario en la información de autentificación de la cuenta de la primera cuenta.

En algunas realizaciones del procedimiento, el primer usuario puede incluir una pluralidad de usuarios, lo que puede a su vez incluir un usuario administrativo en el control del primer dispositivo y un segundo usuario en el control del segundo dispositivo. En algunas realizaciones, el procedimiento puede incluir además transmitir una autorización del segundo usuario al segundo usuario transmitiendo un identificador del segundo usuario del segundo usuario desde el primer dispositivo al servidor y operar el procesador del servidor: generar una información de registro del segundo usuario basada en el identificador del segundo usuario y una contraseña del segundo usuario, almacenar la información de registro del segundo usuario en la memoria del servidor no volátil, y transmitir una autorización de servidor de segundo usuario al segundo usuario. En algunas realizaciones, el procedimiento puede incluir además: recibir, por el segundo usuario, la autorización del servidor del segundo usuario, y posteriormente instalar un agente de encriptado en el segundo dispositivo; recibir una contraseña del segundo usuario putativo en el segundo dispositivo; operar el procesador del segundo dispositivo bajo el control del agente de encriptado para generar información de registro de segundo usuario putativo basada en el identificador del segundo usuario y la contraseña de segundo usuario putativo y transmitir la información de registro de segundo usuario putativo al servidor; operar el

procesador del servidor para comparar la información de registro de segundo usuario putativo con la información de registro de segundo usuario almacenada, y autentificar el segundo dispositivo para la primera cuenta solo si la información de registro de segundo usuario putativo corresponde a la información de registro de segundo usuario almacenada; operar el procesador del segundo dispositivo autentificado bajo el control del agente de encriptado para generar la clave de desencriptado del segundo dispositivo, generar la clave de encriptado del segundo dispositivo basada en la clave de desencriptado del segundo dispositivo y transmitir la clave de encriptado del segundo dispositivo al servidor; recibir la clave de encriptado del segundo dispositivo en el primer dispositivo; y operar el procesador del primer dispositivo bajo el control del agente de encriptado para generar la pluralidad de indicadores de claves encriptados a partir de la pluralidad de indicadores de claves utilizando la clave de encriptado del segundo dispositivo recibido.

En algunas realizaciones del procedimiento, la clave de desencriptado del segundo dispositivo puede ser una clave privada específica de usuario del segundo usuario. En algunas realizaciones del procedimiento, la clave privada específica del usuario puede almacenarse en la memoria no volátil del segundo dispositivo. En algunas realizaciones del procedimiento, la clave de encriptado del segundo dispositivo puede ser una clave pública específica del usuario correspondiente generada basándose en la clave privada específica del usuario.

En algunas realizaciones del procedimiento, el primer usuario puede incluir una pluralidad de usuarios, incluyendo un usuario administrativo en el control del primer dispositivo y un segundo usuario en el control del segundo dispositivo. En algunas realizaciones del procedimiento, el procedimiento incluye además: proporcionar un archivo para ser encriptado al primer dispositivo; operar el procesador del primer dispositivo bajo el control del agente de encriptado para derivar una de las claves de encriptado a partir de la información del valor de inicialización de la clave utilizando la información de la clave, y encriptar el archivo como un archivo encriptado con la clave de encriptado derivada; y transmitir el archivo encriptado, la información de codificación y una autorización del segundo usuario al segundo usuario. En algunas realizaciones, el procedimiento puede incluir además: recibir, por el segundo usuario, la autorización del segundo usuario y, posteriormente, instalar un agente de encriptado en el segundo dispositivo; recibir el archivo encriptado y la información de codificación en el segundo dispositivo; operar el procesador del segundo dispositivo bajo el control del agente de encriptado para obtener la clave de encriptado a partir de la información de valor de inicialización almacenada en la memoria del segundo dispositivo no volátil usando la información de clave recibida y desencriptar el archivo encriptado usando la clave de encriptado derivada.

En algunas realizaciones del procedimiento, el primer usuario puede ser un solo usuario en el control de la pluralidad de dispositivos, y el identificador del primer usuario puede incluir una pluralidad de identificadores de alias de usuario. En algunas realizaciones del procedimiento, cada identificador de alias de usuario puede compartir la misma información de autentificación de cuenta.

En algunas realizaciones del procedimiento, el primer usuario puede incluir una pluralidad de usuarios, teniendo cada usuario el control de al menos uno de los dispositivos de la pluralidad de dispositivos y teniendo un identificador específico del usuario, y para al menos una de los usuarios en la pluralidad de usuarios, el identificador específico del usuario para ese usuario puede incluir una pluralidad de identificadores de alias específicos del usuario, con cada identificador de alias específico del usuario compartiendo la información de autentificación de la cuenta para ese usuario.

De acuerdo con otro ejemplo de realización descrito en este documento, se proporciona un producto de programa de ordenador para su uso en una pluralidad de dispositivos para proporcionar encriptado para la pluralidad de dispositivos, la pluralidad de dispositivos está configurado para comunicación electrónica con un servidor y que incluye al menos un primer dispositivo con un primer procesador de dispositivos y una primera memoria de dispositivos no volátil y un segundo dispositivo; teniendo el servidor almacenado en el mismo una primera cuenta para un primer usuario que controla la pluralidad de dispositivos, almacenando la primera cuenta los datos de la cuenta, incluyendo un identificador del primer usuario e información de autentificación de cuenta en una memoria de servidor no volátil, e incluyendo el producto de programa de ordenador un medio de grabación no transitorio e

instrucciones grabadas en el medio de grabación, con las instrucciones para configurar el primer procesador del dispositivo para: generar aleatoriamente una pluralidad de indicadores de claves; generar una pluralidad de indicadores de claves encriptados a partir de la pluralidad de indicadores de claves utilizando una clave de encriptado del segundo dispositivo, correspondiendo cada indicador de clave encriptado a uno de los indicadores de claves de la pluralidad de indicadores de claves, correspondiendo la clave de encriptado del segundo dispositivo a una clave de desencriptado del segundo dispositivo desconocido para el servidor; transmitir la pluralidad de indicadores de claves encriptados al servidor para impedir la exposición de los indicadores de claves al servidor, pudiendo operar el servidor para generar una cadena de estado de clave para la primera cuenta que incluye una porción de indicador de clave del servidor basada en la pluralidad de indicadores de claves encriptados y para proporcionar al segundo dispositivo acceso a la cadena de estado de clave si y solo si la información de autentificación del servidor putativo recibida del segundo dispositivo corresponde a la información de autentificación de la cuenta; generar una pluralidad de valores de inicialización de clave basadas en la pluralidad de indicadores de claves, donde para cada valor de inicialización de clave, el primer procesador del dispositivo puede ser operable para generar una pluralidad de claves de encriptado independientes; y almacenar información de valor de inicialización de clave basada en la pluralidad de valores de inicialización de clave en la memoria del primer

dispositivo no volátil. En algunas realizaciones del producto de programa de ordenador, la pluralidad de indicadores de claves se puede determinar en el segundo dispositivo a partir de la pluralidad de indicadores de claves encriptados en la cadena de estado de clave utilizando la clave de desencriptado del segundo dispositivo de manera que se pueda generar la misma pluralidad de valores de inicialización de clave basado en la pluralidad de indicadores de claves, y para cada valor de inicialización de clave, un procesador del segundo dispositivo puede generar la misma pluralidad de claves de encriptado independientes que el primer dispositivo, sin proporcionar ninguna de las claves clave, información de valor de inicialización clave y claves de encriptado al segundo dispositivo.

En algunas realizaciones, el producto de programa de ordenador puede incluir adicionalmente instrucciones para configurar el primer procesador del dispositivo para generar la pluralidad de valores de inicialización de clave mediante la recepción de una pluralidad de valores de clave de servidor generados de forma aleatoria desde el servidor, almacenándose los valores de clave de servidor en la primera cuenta, y generar la pluralidad de valores de inicialización de clave basadas en los valores de clave del servidor y la pluralidad de indicadores de claves.

En algunas realizaciones, el producto de programa de ordenador puede incluir adicionalmente instrucciones para configurar el primer procesador del dispositivo para definir un primer código de verificación, definir la clave de encriptado segundo dispositivo basado en el primer código de verificación, y encriptar la pluralidad de indicadores de claves utilizando el clave de encriptado del segundo dispositivo, donde también se puede generar la clave de desencriptado del segundo dispositivo en función del primer código de verificación.

En algunas realizaciones, el producto de programa de ordenador puede incluir adicionalmente instrucciones para configurar el primer procesador del dispositivo para generar un código de servidor de encriptado basado en el primer código de verificación y transmitir el código de servidor de encriptado al servidor para su almacenamiento en la información de autentificación de la cuenta de la primera cuenta, donde el servidor puede configurarse para proporcionar acceso a la cadena de estado de clave si y solo si la información de autentificación del servidor putativo recibida desde el segundo dispositivo corresponde al código de servidor encriptado almacenado en la información de autentificación de la primera cuenta.

En algunas realizaciones, el producto de programa de ordenador puede incluir adicionalmente instrucciones para configurar el primer procesador dispositivo para recibir un archivo para ser codificados, derivar una de las claves de encriptado de la información de clave de valores de inicialización que utilizan modulación información, encriptar y almacenar el archivo como un archivo encriptado en la memoria del primer dispositivo no volátil que utiliza la clave de encriptado derivada, almacenar la información de codificación con el archivo encriptado en la memoria del primer dispositivo no volátil y encriptar la información de valor de inicialización de clave utilizando el primer código de verificación antes del almacenamiento.

En algunas realizaciones, el producto de programa de ordenador puede incluir adicionalmente instrucciones para configurar el primer procesador del dispositivo para recibir un archivo encriptado y la información de generación de claves, derivar la clave de encriptado de la información inicial de clave almacenada en la memoria primer dispositivo no volátil usando la información de clave recibida; y desencriptar el archivo encriptado utilizando la clave de encriptado derivada.

En algunas realizaciones, el producto de programa de ordenador puede incluir adicionalmente instrucciones para configurar el primer procesador del dispositivo para seleccionar de manera aleatoria la información de generación de claves después de recibir una indicación del archivo a encriptar.

En algunas realizaciones, el producto de programa de ordenador puede incluir adicionalmente instrucciones para configurar el primer procesador del dispositivo para definir un primer código de verificación, generar un código local encriptado basado en el primer código de verificación, almacenar el código local encriptado en la primera memoria del dispositivo no volátil, luego recibir una solicitud para acceder a los archivos y un código de verificación putativo local, generar un código local encriptado putativo, comparar el código local encriptado putativo con el código local encriptado para determinar si el código de verificación putativo local es el primer código de verificación, y proporcionar acceso a los archivos encriptados por el agente de encriptado si y solo si el código local encriptado putativo coincide con el código local encriptado.

En algunas realizaciones, el producto de programa de ordenador puede incluir adicionalmente instrucciones para configurar el primer procesador del dispositivo para almacenar la información de clave de valores de inicialización mediante el encriptado de la pluralidad de valores de inicialización de clave usando el primer código de verificación, y almacenar la pluralidad encriptada de valores de inicialización de clave en la memoria del primer dispositivo no volátil.

En algunas realizaciones del producto de programa de ordenador, el primer usuario puede incluir una pluralidad de usuarios del grupo incluyendo al menos un usuario del grupo administrativo y un segundo grupo de usuarios, teniendo cada uno de los usuarios del grupo el control de al menos uno de los dispositivos en la pluralidad de dispositivos, donde el usuario del grupo administrativo puede tener el control del primer dispositivo y el segundo usuario del grupo puede tener el control del segundo dispositivo. En algunas realizaciones del producto de programa

de ordenador, para cada usuario del grupo en la pluralidad de usuarios del grupo, los datos de la cuenta pueden incluir además una clave pública específica del usuario, donde la clave pública específica del usuario para cada usuario se genera basándose en una clave privada específica del usuario almacenada en una memoria no volátil de un dispositivo correspondiente en la pluralidad de dispositivos. En algunas realizaciones, el producto de programa de ordenador puede incluir además instrucciones para configurar el primer procesador de dispositivo para generar la pluralidad de indicadores de claves encriptados, para cada grupo de usuarios en la pluralidad de usuarios del grupo, generando una pluralidad de indicadores de claves encriptados específicos del usuario usando la clave pública específica del usuario para ese usuario. En algunas realizaciones, el producto de programa de ordenador puede incluir además instrucciones para transmitir la pluralidad de indicadores de claves encriptados específicos del usuario al servidor. En algunas realizaciones del producto de programa de ordenador, el servidor puede ser operable para generar la porción del indicador de clave del servidor de la cadena de estado de clave al generar, para cada usuario del grupo en la pluralidad de usuarios del grupo, una porción de la cadena específica del usuario basada en la pluralidad de los indicadores de claves encriptados específicos del usuario para ese usuario del grupo. En algunas realizaciones del producto de programa de ordenador, la pluralidad de indicadores de claves se puede determinar en el segundo dispositivo a partir de la pluralidad de indicadores de claves encriptados específicos del usuario en la parte específica del usuario de la porción del indicador de clave del servidor correspondiente al segundo usuario del grupo usando el segundo dispositivo de clave privada.

En algunas realizaciones del producto de programa de ordenador, la información de autentificación de cuenta para la primera cuenta puede incluir, para cada grupo de usuarios en la pluralidad de usuarios del grupo, un código de encriptado del servidor específico del usuario. En algunas realizaciones, el producto de programa de ordenador puede incluir además instrucciones para configurar un procesador de un dispositivo en la pluralidad de dispositivos correspondientes a ese usuario del grupo para definir un código de verificación específico del usuario, generar el código encriptado del servidor específico del usuario basado en el código de verificación específico del usuario, y transmitir el código encriptado del servidor específico del usuario al servidor para su almacenamiento en la información de autentificación de la primera cuenta.

En algunas realizaciones del producto de programa de ordenador, el primer usuario puede incluir una pluralidad de usuarios, incluyendo un usuario administrativo en el control del primer dispositivo y un segundo usuario en el control del segundo dispositivo. En algunas realizaciones, el producto de programa de ordenador puede incluir además instrucciones para configurar el primer procesador de dispositivo para transmitir una autorización del segundo usuario al segundo usuario transmitiendo un identificador del segundo usuario del segundo usuario desde el primer dispositivo al servidor, siendo el servidor operable para generar información de registro de segundo usuario basada en el identificador del segundo usuario y una contraseña del segundo usuario, almacenar la información de registro de segundo usuario en la memoria del servidor no volátil y transmitir una autorización de servidor de segundo usuario al segundo usuario. En algunas realizaciones, el producto de programa de ordenador puede incluir además instrucciones para configurar un procesador del segundo dispositivo, cuando se instala en el mismo, para: recibir una contraseña del segundo usuario putativo; generar información de registro de segundo usuario putativo basada en el identificador del segundo usuario y la contraseña del segundo usuario putativo; transmitir la información de registro de segundo usuario putativo al servidor, pudiendo operar el servidor para comparar la información de registro de segundo usuario putativo con la información de registro de segundo usuario almacenada, y autentificar el segundo dispositivo para la primera cuenta solo si la información de registro de segundo usuario putativo corresponde a la información de registro de segundo usuario almacenada; y una vez autentificado el segundo dispositivo; generar la clave de desencriptado del segundo dispositivo; generar la clave de encriptado del segundo dispositivo basada en la clave de desencriptado del segundo dispositivo; y transmitir la clave de encriptado del segundo dispositivo al servidor. En algunas realizaciones, el producto de programa de ordenador puede incluir además instrucciones para configurar el primer procesador de dispositivo para recibir la clave de encriptado del segundo dispositivo y generar la pluralidad de indicadores de claves encriptados a partir de la pluralidad de indicadores de claves utilizando la clave de encriptado del segundo dispositivo recibido.

En algunas realizaciones del producto de programa de ordenador, la clave de desencriptado del segundo dispositivo puede ser la clave privada específica de usuario del segundo usuario y la clave de encriptado del segundo dispositivo puede ser la clave pública correspondiente del segundo usuario.

En algunas realizaciones del producto de programa de ordenador, el primer usuario puede incluir una pluralidad de usuarios, que a su vez puede incluir un usuario administrativo en el control del primer dispositivo y un segundo usuario en el control del segundo dispositivo. En algunas realizaciones, el producto de programa de ordenador puede incluir además instrucciones para configurar el primer procesador del dispositivo para recibir un archivo que se va a encriptar, derivar una de las claves de encriptado de la información de valor de inicialización de clave utilizando información de clave, encriptar el archivo como un archivo encriptado utilizando la clave de encriptado derivada y transmitir el archivo encriptado, la información de generación de claves y una autorización del segundo usuario al segundo usuario. En algunas realizaciones, el producto de programa de ordenador incluye además instrucciones para configurar un procesador del segundo dispositivo, cuando se instala en el mismo, para: registrar el segundo dispositivo con el servidor en base a la autorización del segundo usuario; determinar la pluralidad de indicadores de claves en función de la pluralidad de indicadores de claves encriptados en la cadena de estado de clave utilizando la clave de desencriptado del segundo dispositivo; generar la pluralidad de valores de inicialización de clave basadas en la pluralidad de indicadores de claves; almacenar información de valores de inicialización de

claves basada en los valores de inicialización de claves en una memoria del segundo dispositivo no volátil; recibir el archivo encriptado y la información de generación de claves; obtener la clave de encriptado a partir de la información de valor de inicialización de clave almacenada en la memoria del segundo dispositivo no volátil utilizando la información de clave recibida; y desencriptar el archivo encriptado utilizando la clave de encriptado derivada.

En algunas realizaciones del producto de programa de ordenador, el primer usuario puede ser un solo usuario en control de la pluralidad de dispositivos, y el identificador del primer usuario puede incluir una pluralidad de identificadores de alias de usuario, con cada identificador de alias de usuario compartiendo la información de autentificación de la cuenta.

En algunas realizaciones del producto de programa de ordenador, el primer usuario puede incluir una pluralidad de usuarios, teniendo cada usuario el control de al menos uno de los dispositivos de la pluralidad de dispositivos y teniendo un identificador específico del usuario, y para al menos una de los usuarios en la pluralidad de usuarios, el identificador específico del usuario para ese usuario puede incluir una pluralidad de identificadores de alias específicos del usuario, con cada identificador de alias específico del usuario compartiendo la información de autentificación de la cuenta para ese usuario.

De acuerdo con otro ejemplo de realización descrito en este documento, se describe un dispositivo para proporcionar encriptado para una pluralidad de dispositivos, incluyendo el dispositivo. En algunas realizaciones del dispositivo, cada dispositivo dentro de la pluralidad de dispositivos que incluye el dispositivo puede configurarse para la comunicación electrónica con un servidor. En algunas realizaciones del dispositivo, el servidor puede haber almacenado en el mismo una primera cuenta para un primer usuario en control de la pluralidad de dispositivos. En algunas realizaciones del dispositivo, la primera cuenta puede almacenar datos de la cuenta que incluyen un identificador del primer usuario e información de autentificación de la cuenta en una memoria de servidor no volátil. En algunas realizaciones, el dispositivo puede incluir un procesador y una memoria de dispositivo no volátil que tiene almacenadas en el mismo instrucciones para configurar el procesador para: generar aleatoriamente una pluralidad de indicadores de claves; generar una pluralidad de indicadores de claves encriptados a partir de la pluralidad de indicadores de claves utilizando una clave de encriptado del segundo dispositivo, correspondiendo cada indicador de clave encriptado a uno de los indicadores de claves de la pluralidad de indicadores de claves, correspondiendo la clave de encriptado del segundo dispositivo a una clave de desencriptado del segundo dispositivo desconocido para el servidor; transmitir la pluralidad de indicadores de claves encriptados al servidor para impedir la exposición de los indicadores de claves al servidor, pudiendo operar el servidor para generar una cadena de estado de clave para la primera cuenta que incluye una porción de indicador de clave del servidor basada en la pluralidad de indicadores de claves encriptados y para proporcionar a un segundo dispositivo en la pluralidad de dispositivos acceso a la cadena de estado de clave si y solo si la información de autentificación del servidor putativo recibida de ese dispositivo corresponde a la información de autentificación de la cuenta; generar una pluralidad de valores de inicialización de clave basados en la pluralidad de indicadores de claves, donde para cada valor de inicialización de clave, el procesador puede ser operable para generar una pluralidad de claves de encriptado independientes; y almacenar información de valor de inicialización de clave basada en la pluralidad de valores de inicialización de clave en la memoria del dispositivo no volátil. En algunas realizaciones del dispositivo, la pluralidad de indicadores de claves se puede determinar en el segundo dispositivo a partir de la pluralidad de indicadores de claves encriptados en la cadena de estado de clave utilizando la clave de desencriptado del segundo dispositivo de manera que se pueda generar la misma pluralidad de valores de inicialización de clave basado en la pluralidad de indicadores de claves, y para cada valor de inicialización de clave, un procesador del segundo dispositivo puede generar la misma pluralidad de claves de encriptado independientes que el primer dispositivo, sin proporcionar ninguna de las claves clave, información de valor de inicialización clave y claves de encriptado al segundo dispositivo.

Breve descripción de los dibujos

Para una mejor comprensión de las realizaciones descritas y para mostrar más claramente cómo pueden llevarse a efecto, se hará ahora referencia, a modo de ejemplo, a los dibujos adjuntos, en los que:

La figura 1 muestra un diagrama de bloques de un sistema que se puede usar para proporcionar encriptado en una pluralidad de dispositivos de acuerdo con una realización;

La figura 2 muestra un diagrama de bloques de otro sistema que puede usarse para proporcionar encriptado en una pluralidad de dispositivos de acuerdo con una realización;

La figura 3 muestra un diagrama de bloques que ilustra los estados del sistema de la figura 2 de acuerdo con una realización;

Las figuras 4A-4C muestran una serie de diagramas de flujo de una realización de ejemplo de un procedimiento para proporcionar encriptado en una pluralidad de dispositivos;

La figura 5 muestra un diagrama de bloques de otro sistema que se puede usar para proporcionar encriptado en una pluralidad de dispositivos de acuerdo con una realización;

La figura 6A muestra un diagrama de flujo de una realización de ejemplo de un procedimiento para encriptar un

archivo;

La figura 6B muestra un diagrama de flujo de una realización de ejemplo de un procedimiento para desencriptar un archivo;

La figura 6C muestra un diagrama de flujo de otra realización de ejemplo de un procedimiento para desencriptar un archivo;

La figura 7 muestra un diagrama de bloques de un sistema que puede usarse para proporcionar encriptación y uso compartido de archivos en una pluralidad de dispositivos para una pluralidad de usuarios de grupos de acuerdo con una realización;

La figura 8 muestra un diagrama de flujo de una realización de ejemplo de un procedimiento para proporcionar encriptado en una pluralidad de dispositivos para el grupo de usuarios de la figura 7;

La figura 9 muestra un diagrama de flujo de una realización de ejemplo de un procedimiento para recuperar un código de verificación;

La figura 10 muestra un diagrama de flujo de una realización de ejemplo de un procedimiento para generar códigos de recuperación locales y remotos que se pueden usar con el procedimiento de recuperación de códigos de verificación de la figura 9;

La figura 11 muestra un diagrama de flujo de una realización de ejemplo de un procedimiento para autentificar de forma remota a un usuario.

Descripción detallada

Varios sistemas o procedimientos se describirán a continuación para proporcionar un ejemplo de una realización de la materia objeto reivindicada. Ninguna realización descrita a continuación limita ninguna materia objeto reivindicada y cualquier materia objeto reivindicada puede cubrir procedimientos o sistemas que difieran de los descritos a continuación. La materia objeto reivindicada no se limita a los sistemas o procedimientos que tienen todas las características de cualquier sistema o procedimiento descrito a continuación o a las características comunes a múltiples o todos los aparatos o procedimientos descritos a continuación. Es posible que un sistema o procedimiento descrito a continuación no sea una realización que se indique en ninguna materia objeto reivindicada. Cualquier materia objeto divulgada en un sistema o procedimiento descrito a continuación que no se reivindica en este documento puede ser objeto de otro instrumento de protección, por ejemplo, una solicitud de patente de continuación, y los solicitantes, inventores o propietarios no tienen la intención de abandonar, renuncian o dedicar al público ninguna materia objeto de este tipo mediante su divulgación en este documento.

Además, se apreciará que, por simplicidad y claridad de ilustración, cuando se considere apropiado, los números de referencia pueden repetirse entre las figuras para indicar elementos correspondientes o análogos. Además, se exponen numerosos detalles específicos para proporcionar una comprensión completa de las realizaciones descritas en el presente documento. Sin embargo, se entenderá por los expertos en la técnica que las realizaciones descritas en el presente documento pueden llevarse a la práctica sin estos detalles específicos. En otros casos, procedimientos y componentes bien conocidos no se han descrito en detalle para no oscurecer las realizaciones descritas en el presente documento. Además, los dibujos y la descripción no deben considerarse como limitativas del alcance de las realizaciones descritas en este documento.

También hay que señalar que, tal como se usa en el presente documento, la expresión "y/o" está destinada a representar una o inclusiva. Es decir, "X y/o Y" pretende significar X o Y o ambos, por ejemplo. Como un ejemplo adicional, "X, Y y/o Z" pretende significar X o Y o Z o cualquier combinación de los mismos.

En el presente documento se describen diversas realizaciones de sistemas, procedimientos, productos de programas de ordenador y dispositivos para proporcionar protección de datos para una pluralidad de dispositivos. Las diversas realizaciones descritas en este documento pueden permitir la sincronización y el uso compartido de archivos encriptados entre múltiples dispositivos controlados por un solo usuario y/o entre uno o más dispositivos controlados por múltiples usuarios diferentes. Varias realizaciones descritas en el presente documento también pueden proporcionar sistemas, procedimientos y productos de programas de ordenador para recuperar un código de verificación definido por un usuario. Varias realizaciones también pueden proporcionar sistemas, procedimientos y productos de programas de ordenador para autentificar remotamente a un usuario. En general, las características de las diversas realizaciones descritas en el presente documento pueden usarse en cualquier combinación entre sí, excepto cuando se indique lo contrario.

Algunas realizaciones descritas aquí proporcionan un sistema de seguridad que permite el encriptado y desencriptado automático de archivos de datos de un usuario en los dispositivos del usuario. Algunas realizaciones descritas en este documento pueden almacenar claves de encriptado y desencriptado de archivos (FED) en los dispositivos del usuario. En algunos casos, es posible que las claves FED no estén almacenadas en los dispositivos. Más bien, los valores de inicialización de claves se pueden almacenar en el dispositivo. Estos valores de

inicialización de claves pueden permitir que las claves FED se deriven utilizando información de generación de claves. En algunos casos, las claves FED se pueden generar aleatoriamente para aumentar la potencia de encriptado resultante.

Las claves FED o valores de inicialización de claves pueden almacenarse en la memoria del dispositivo no volátil en formato encriptado y estar protegidas por un código de verificación definido por el usuario. En algunas realizaciones, el código de verificación puede ser conocido solo por el usuario. La información de autentificación local se puede generar según el código de verificación y se puede almacenar en el dispositivo de un usuario. La información de autentificación se puede utilizar para autentificar a un usuario que intenta acceder o modificar archivos encriptados. En algunos casos, es posible que el código de verificación no se pueda determinar a partir de la información de autentificación almacenada.

Los archivos administrados por los sistemas de ejemplo descritos en el presente documento pueden permanecer encriptados en todo momento cuando se almacenan en una memoria no volátil, ya sea en dispositivos del usuario u otros dispositivos, como un servidor en la nube. Las realizaciones descritas en este documento también pueden garantizar que los archivos de texto sin formato correspondientes a los archivos encriptados almacenados se puedan ver y/o modificar solo dentro de los agentes de encriptado instalados. Los archivos de texto simple pueden ser accesibles solo después de ser desencriptados a pedido del usuario y solo se almacenan temporalmente en la memoria volátil de los dispositivos del usuario mientras se accede.

Un primer ejemplo de sistema puede denominarse como un sistema de seguridad en cuarentena con sincronización manual de valores de inicialización de claves FED (QSSMS). La figura 1 muestra un ejemplo de un sistema 100 que puede usarse para implementar el sistema QSSMS.

El sistema 100 puede incluir una pluralidad de dispositivos 102a-102l controlados por un primer usuario 140. Las aplicaciones denominadas agentes Q o agentes 104 de encriptado pueden instalarse en cada uno de los dispositivos 102 controlados por el usuario 140. Se puede instalar un agente Q 104 en cada dispositivo 102. El agente Q 104 instalado en cada dispositivo 102 puede ser responsable de las operaciones de encriptado y desencriptado en ese dispositivo 102. El agente Q 104 también puede generar claves de encriptado/desencriptado y proteger las claves una vez generadas. Los agentes Q 104 pueden generar valores de inicialización 106 de claves FED que pueden almacenarse en cada dispositivo 102. El agente Q 104 puede utilizar los valores de inicialización 106 de claves FED para generar una o más claves de encriptado/desencriptado. En algunos casos, el agente Q 104 puede generar un gran conjunto de claves FED, es decir, el almacén de claves FED, a partir de los valores de inicialización 106 de claves FED.

En algunos casos, el primer usuario 140 puede desear mover archivos 108/110 encriptados desde el primer dispositivo 102a a uno o más de los otros dispositivos 102b-102L. El primer usuario 140 puede transmitir uno o más archivos 108/110 encriptados desde el primer dispositivo 102a a un segundo dispositivo 102b de varias maneras, tal como usando servicios en la nube, redes de telecomunicaciones u otros mecanismos de transferencia de archivos, como un USB o una clave Firewire. Una vez que los archivos se han recibido en el segundo dispositivo 102b, puede ser necesario desencriptar los archivos en el segundo dispositivo 102b. Para permitir que los archivos 108/110 encriptados por el agente Q 104 en el primer dispositivo 102a sean desencriptados por el agente Q 104 en el segundo dispositivo 102b, la clave FED 106 utilizada por los agentes Q 104 en el primer dispositivo 102a y el segundo dispositivo 102b puede sincronizarse. En el sistema 100, los valores de inicialización 106 de claves FED se pueden sincronizar manualmente. Sin embargo, puede ser conveniente habilitar los valores de inicialización 106 de claves FED para que se sincronicen automáticamente. Esto podría permitir que los valores de inicialización 106 de claves FED se sincronicen entre los dispositivos 102 ubicados remotamente de un usuario. Esto también puede permitir que diferentes usuarios sincronicen los valores de inicialización 106 de claves FED sin tener que compartir los valores de inicialización de claves directamente. Además, esto puede simplificar el proceso para sincronizar los valores de inicialización de claves FED para una pluralidad de dispositivos controlados por uno o más usuarios.

La figura 2 muestra un sistema 200 que se puede usar para implementar una realización de ejemplo de un sistema para proporcionar encriptado en una pluralidad de dispositivos. El sistema 200 es una realización de ejemplo de un sistema al que se puede hacer referencia como un sistema de seguridad en cuarentena con sincronización automática de valores de inicialización de claves FED (QSSAS). El sistema 200 se puede usar para sincronizar automáticamente los valores de inicialización 206 de claves FED entre una pluralidad de dispositivos 202 asociados con el primer usuario 240. El sistema 200 incluye un servidor 230 (que puede denominarse un servidor Q o un servidor de seguridad) y la pluralidad de dispositivos 202a-202l. Cada dispositivo 202 puede tener instalado en el mismo un cliente 204 al que se puede hacer referencia como un cliente Q o un agente de encriptado. El agente 204 de encriptado en un dispositivo 202 es similar a agente Q 104 en que es responsable de las operaciones de encriptado y desencriptado en ese dispositivo 202. El servidor 230 puede comunicarse con los dispositivos 202 a través de la red 220.

Los agentes 204 de encriptado pueden ser utilizados para generar valores de inicialización 206 de claves FED. Los valores de inicialización 206 de claves FED se pueden usar para derivar claves FED. En algunos casos, los valores de inicialización 206 de claves FED pueden generarse involucrando la comunicación entre un agente 204 de encriptado particular y un servidor Q 230. En algunos casos, puede que no haya comunicación directa entre los

agentes 204 de encriptado en diferentes dispositivos 202. Por lo tanto, el servidor Q 230 se puede utilizar para sincronizar automáticamente las claves de encriptado y desencriptado utilizadas en los dispositivos 202.

El sistema 200 puede poner en práctica los conceptos relacionados con las funciones de un solo sentido y criptosistemas de clave pública para proporcionar sincronización automática y segura de las claves. En algunas realizaciones, el servidor Q 230 puede no tener acceso a ninguno de los archivos 208/210 almacenados en los dispositivos 202. El servidor Q 230 tampoco puede estar expuesto a ninguna de los valores de inicialización 206 de claves FED y/o claves FED.

En algunos casos, el sistema 200 puede también extenderse para permitir el intercambio de archivos encriptados entre un grupo de usuarios. El primer usuario puede ser un superusuario para el grupo y puede incluir una pluralidad de usuarios del grupo, incluyendo la pluralidad de usuarios del grupo al menos un usuario administrativo y un segundo usuario del grupo. Un ejemplo de este sistema se describirá a continuación con referencia a la figura 7. En general, el nivel de seguridad que se puede alcanzar en las realizaciones de los sistemas de seguridad de sincronización automática (QSSAS) es comparable al de QSSMS.

Las características de los sistemas y procedimientos de las realizaciones descritas, tales como los sistemas 100 y 200 pueden implementarse en uno o más ordenadores de servidor, ordenadores de escritorio, ordenadores portátiles, tabletas, PDA, teléfonos inteligentes u otros ordenadores programables. Los ordenadores programables pueden incluir una conexión con una red, tal como la red 220. La red 220 puede ser una conexión por cable o inalámbrica a Internet. En algunos casos, la red 220 puede incluir otros tipos de redes informáticas o de telecomunicaciones.

En algunas realizaciones, cada uno de los ordenadores programables pueden incluir un dispositivo de entrada para introducir información en el dispositivo. Por ejemplo, el dispositivo de entrada puede ser un teclado, almohadilla, dispositivo de control de cursor, pantalla táctil, cámara, escáner o micrófono. En algunas realizaciones, la información de entrada se puede recibir a través de la interfaz de comunicación desde otros ordenadores programables a través de una red. En algunas realizaciones, los dispositivos informáticos pueden incluir un dispositivo de visualización para presentar información visual. Por ejemplo, el dispositivo de visualización puede ser un monitor de ordenador, una pantalla plana, un proyector o un panel de visualización. En algunas realizaciones, el dispositivo de visualización muestra uno o más archivos al usuario que han sido encriptados por un agente de encriptado de acuerdo con los sistemas y procedimientos descritos en este documento.

Las realizaciones de los sistemas, procesos y procedimientos descritos en este documento pueden implementarse en hardware o software, o una combinación de ambos. Alternativamente, estas realizaciones también pueden implementarse en programas de ordenador ejecutados en ordenadores programables, cada uno de los cuales comprende al menos un procesador (por ejemplo, un microprocesador), un sistema de almacenamiento de datos (que incluye elementos de memoria y/o almacenamiento volátiles y no volátiles), al menos un dispositivo de entrada, y al menos un dispositivo de salida. Por ejemplo, y sin limitación, los ordenadores programables (referidos a continuación como dispositivos, dispositivos informáticos o servidores) pueden ser un ordenador personal, ordenador portátil, asistente de datos personales, teléfono celular, dispositivo de teléfono inteligente, ordenador de tableta y/o dispositivo inalámbrico. Para cualquier componente de software, el código del programa se aplica a los datos de entrada para realizar las funciones descritas en este documento y generar información de salida. La información de salida se aplica a uno o más dispositivos de salida, de manera conocida.

Cada componente de software o programa se puede implementar en un alto nivel de programación orientado a objetos o y/o lenguaje de script para comunicarse con un sistema informático. Sin embargo, los programas pueden implementarse en ensamblador o lenguaje de máquina, si así lo desea. En cualquier caso, el lenguaje puede ser un lenguaje compilado o interpretado. Además, los procesos y procedimientos de las realizaciones descritas pueden distribuirse en un producto de programa de ordenador que comprende un medio legible por ordenador que contiene instrucciones utilizables por ordenador para uno o más procesadores. El medio puede proporcionarse en diversas formas, incluidos uno o más disquetes, discos compactos, cintas, chips, transmisiones por cable, transmisiones por satélite, transmisiones o descargas por Internet, medios de almacenamiento magnéticos y electrónicos, señales digitales y analógicas, y similares. Las instrucciones de uso del ordenador también pueden ser de varias formas, incluido código compilado y no compilado.

Realizaciones de ejemplo del sistema de QSSMS que emplean sincronización manual de los valores de inicialización de claves FED se describirán primero. También se describirán varias realizaciones de ejemplo del sistema QSSAS con sincronización automática de valores de inicialización de claves FED. Además, se describirán las realizaciones del sistema QSSAS que permiten compartir archivos encriptados entre un grupo de usuarios. También se describirán realizaciones adicionales de sistemas para proporcionar la recuperación de un código de verificación definido por un usuario.

QSSMS

En esta sección, realizaciones de ejemplo del sistema de QSSMS se describen con referencia a la figura 1. Como antecedente, se discute el concepto de una función unidireccional.

Definición 1 *Una función f(x) es una función de una sola vía si es fácil de calcular f(x) para cada x en el dominio de f, pero para casi todos y en el rango de f, computacionalmente no es factible encontrar un x tal que f(x) = y. (*W. Diffie and M. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, n.º 6, páginas 644 - 654, Nov. 1976.*)*

En general, el sistema 100 puede usarse por un primer usuario 140 en el control de una pluralidad de dispositivos 102. Por ejemplo, la pluralidad de dispositivos 102 puede incluir L dispositivos 102a-102/. El primer usuario 140 puede querer usar los dispositivos 102 para administrar y almacenar ciertos tipos de archivos 108/110 encriptados. Para cada dispositivo 102 en la pluralidad de dispositivos, el primer usuario 140 puede instalar un agente de encriptado o agente Q 104 en ese dispositivo 102. Por ejemplo, el primer usuario 140 puede descargar un agente Q 104 e instalar el agente Q 104 en el primer dispositivo 102. En algunos ejemplos, el primer usuario 140 puede inicializar el agente Q 104 antes de usar el agente Q 104 para encriptar y desencriptar archivos.

El primer usuario 140 puede usar la agente Q 104 para definir un código de verificación. Por ejemplo, el primer usuario 140 puede definir un código de verificación C. En algunos casos, el agente Q 104 puede usar el código de verificación *C*, o los valores generados basándose en el código de verificación *C*, para verificar el primer usuario 140. Por ejemplo, tal verificación podría tener lugar cuando el primer usuario 140 quiera abrir el agente Q 104 para acceder a los archivos 108/110 administrados por el agente Q 104 en el primer dispositivo 102a. En general, si un agente Q 104 se instaló e inicializó con éxito en otro dispositivo 102l, el primer usuario 140 debería poder usar el mismo código de verificación que el definido para el dispositivo 102l para verificar con el agente Q 104 instalado en el primer dispositivo 102a.

Después de que el primer usuario 140 define el primer código de verificación, por ejemplo, en el primer dispositivo 102a, el agente 104 de encriptado puede generar un código local encriptado basado en el primer código de verificación. El agente 104 de encriptado puede entonces almacenar el código local encriptado en la memoria no volátil del primer dispositivo 102a. Por ejemplo, el agente 104 de encriptado puede generar el código local encriptado al computar $\beta = \varphi(C)$, donde $\varphi(\cdot)$ es una función de una sola vía invertible. El agente 104 de encriptado puede luego guardar β en la memoria no volátil del primer dispositivo 102a.

El agente 104 de encriptado puede entonces determinar una pluralidad de valores de inicialización de clave para el primer dispositivo 102a. En algunos casos, la pluralidad de valores de inicialización de clave se puede importar desde otro dispositivo 102. Por ejemplo, cuando el primer usuario 140 ha generado previamente valores de inicialización de clave en otro dispositivo 102, el primer usuario 140 puede importar los mismos valores de inicialización de clave al primer dispositivo 102a. Si el primer usuario 140 aún no ha generado valores de inicialización de clave en ningún otro dispositivo 102, entonces el agente 104 de encriptado del primer dispositivo 102a puede generar los valores de inicialización de claves.

El agente 104 de encriptado en el primer dispositivo 102a puede generar una pluralidad de valores de inicialización de claves. Por ejemplo, el agente Q 104 puede generar aleatoriamente una pluralidad de valores de inicialización de claves FED independientes $K_1, K_2, \cdots, K_J$. El agente 104 de encriptado puede entonces almacenar información de valor de inicialización de clave basada en la pluralidad de valores de inicialización de claves en la memoria no volátil del primer dispositivo 102a. Por ejemplo, la información de valor de inicialización de clave puede generarse encriptando los valores de inicialización de claves y luego almacenando los valores de inicialización de claves encriptadas como la información de valor de inicialización de clave. En algunos casos, el código de verificación *C* se puede utilizar para encriptar los valores de inicialización de clave $K_1, K_2, \cdots, K_J$, en valores de inicialización de claves encriptadas $E_C(K_1, K_2, \cdots, K_J)$. Estos valores de inicialización de claves encriptadas $E_C(K_1, K_2, \cdots, K_J)$ pueden guardarse en la memoria no volátil del primer dispositivo 102a.

Si otro dispositivo 102/ tiene un agente Q 104 instalado en el mismo y tiene los valores de inicialización de claves generadas y almacenadas en el dispositivo 102/, el primer usuario 140 puede importar los valores de inicialización de claves desde el dispositivo 102/. En el sistema 100, el primer usuario 104 puede acceder al agente Q 104 en el dispositivo 102/ para obtener una copia de los valores de inicialización de claves FED encriptadas $E_C(K_1, K_2, \cdots, K_J)$ generada por ese agente Q 104. El primer usuario 140 puede transferir los valores de inicialización de claves copiadas al agente Q 104 en el primer dispositivo 102a. El agente 104 de encriptado puede luego importar los valores de inicialización de claves y almacenarlas en la memoria no volátil del primer dispositivo 102a.

Una vez que los valores de inicialización de claves han sido generadas en el primer dispositivo 102a, el agente Q 104 en ese dispositivo puede generar una o más claves FED. En algunos casos, el agente Q 104 puede generar una pluralidad de claves de encriptado/desencriptado, es decir, el almacén de claves FED en el primer dispositivo 102a. En general, la pluralidad de claves de encriptado/desencriptado generadas por un agente de encriptado pueden ser claves de encriptado/desencriptado simétricas. La pluralidad de claves de encriptado se puede almacenar en la memoria no volátil del primer dispositivo 102a. En algunos casos, la pluralidad de claves de encriptado puede estar encriptada (por ejemplo, utilizando el código de verificación) antes de ser almacenadas en la memoria no volátil del primer dispositivo 102a.

Por ejemplo, el agente Q 104 puede derivar una pluralidad de claves de encriptado (es decir, almacén de claves FED Ψ) $\Psi = \{k_1: 1 \leq i \leq \Lambda\}$ de los valores de inicialización de claves aleatorias $K_1, K_2, \cdots, K_J$, donde Λ es un número

grande. Cuando el agente Q 104 recibe un archivo para encriptar, el archivo puede encriptarse utilizando una de las claves de encriptado derivadas del almacén de claves FED Ψ. De manera similar, cuando un archivo se mueve al agente 104 de encriptado, o se modifica bajo el control del agente 104 de encriptado, el agente 104 de encriptado puede encriptar y almacenar el archivo nuevo o modificado utilizando la clave de encriptado derivada. Por ejemplo, el agente Q 104 puede seleccionar una clave de encriptado del almacén de claves para usarse para encriptar el archivo. En algunos casos, el agente 104 de encriptado puede seleccionar aleatoriamente la clave de encriptado particular de la pluralidad de claves de encriptado cuando el agente 104 de encriptado recibe una indicación del archivo a encriptar (por ejemplo, una indicación de que un archivo se está moviendo al agente 104 de encriptado), creado en el agente 104 de encriptado para almacenamiento, o modificado en el agente 104 de encriptado). El agente Q 104 puede entonces almacenar el archivo encriptado junto con la información de codificación, que indica cómo derivar la clave de encriptado particular para ese archivo de los valores de inicialización de claves K_1 , K_2, ⋯, K_J o del almacén de claves FED Ψ.

Por ejemplo, el agente Q 104 puede generar un índice de claves para la pluralidad de claves de encriptado derivadas. El índice de claves puede definir un valor de índice de clave para cada clave de encriptado en la pluralidad de claves de encriptado o almacén de claves FED. Cuando se selecciona una clave de encriptado particular de la pluralidad de claves de encriptado y se utiliza para encriptar un archivo, la información de clave para ese archivo puede incluir el valor del índice de clave para esa clave de encriptado particular.

En algunos casos, el agente Q 104 puede no derivar todas las claves de encriptado de los valores de inicialización de claves para generar un almacén de claves con antelación. El agente Q 104 puede obtener las claves de encriptado a partir de los valores de inicialización de claves solo cuando sea necesario, es decir, cuando se recibe una indicación de un archivo que debe encriptarse. En tales casos, el agente 104 de encriptado también puede almacenar información de codificación junto con el archivo encriptado que indica cómo derivar la clave de encriptado a partir de la información de valor de inicialización de clave almacenada en la memoria no volátil del primer dispositivo. Además, el agente Q 104 puede borrar la clave de encriptado derivada del primer dispositivo 102a después de encriptar el archivo.

El agente Q 104, instalado por ejemplo en el primer dispositivo 102a, puede asegurarse de que los archivos 108/110 gestionados bajo su control permanecen encriptados para la duración en que dichos archivos se almacenan en la memoria no volátil de dicho dispositivo. Cuando el primer usuario 140 desea acceder a estos archivos 108/110, el agente de encriptado puede autentificar al usuario antes de proporcionar acceso a los archivos 108/110.

El agente 104 de encriptado en el primer dispositivo 102a puede recibir una solicitud para acceder a los archivos 108/110 y un código de verificación local putativo. Por ejemplo, al recibir una solicitud para acceder a los archivos 108/110, el agente Q 104 puede pedir al primer usuario 140 que ingrese el código de verificación C. El primer usuario 140 puede luego ingresar el código de verificación local putativo.

El agente 104 de encriptado puede generar un código local encriptado putativo basado en el código de verificación local putativo. El agente 104 de encriptado puede entonces comparar el código local encriptado putativo con el código local encriptado para determinar si el código de verificación local putativo es el primer código de verificación. El agente 104 de encriptado puede entonces proporcionar acceso a los archivos encriptados administrados por el agente 104 de encriptado si y solo si el código local putativo coincide con el código local encriptado.

Por ejemplo, el agente de encriptado puede aplicar la misma función φ unidireccional $(\cdot)$ para el código de verificación local putativo para generar el código local encriptado putativo. La salida de la función unidireccional $\varphi(\cdot)$ se puede comparar con el valor del código local encriptado β guardado por el agente Q 104 para determinar si el código de verificación ingresado es el correcto. Una vez que el primer usuario 140 ha sido autentificado, entonces los archivos pueden ser desencriptados y accedidos por el primer usuario 140.

El agente Q 104 puede desencriptar los archivos 108/110 seleccionados por el primer usuario 140 y almacenar los archivos de texto sin formato desencriptados temporalmente en la memoria volátil del primer dispositivo 102a para que el primer usuario 140 los lea y/o edite. Después de que el primer usuario 140a cierre cada archivo de texto sin formato, el agente Q 104 puede borrar el archivo de texto sin formato de la memoria volátil del primer dispositivo 102a si no hay cambios. El agente 104 de encriptado puede encriptar nuevamente el archivo de texto simple usando una clave FED particular (por ejemplo, una nueva clave FED elegida de manera aleatoria desde el almacén de claves Ψ, la misma clave, o una nueva clave de encriptado derivada), y almacenar el archivo encriptado en la memoria no volátil del primer dispositivo 102a.

En algunas realizaciones, la agente Q 104 puede almacenar temporalmente archivos desencriptados en la memoria no volátil del primer dispositivo 102a. Esto puede ser deseable, por ejemplo, cuando el archivo desencriptado es más grande que la memoria volátil disponible en el primer dispositivo 102a. En tales casos, el agente Q 104 puede borrar el archivo desencriptado de la memoria no volátil del primer dispositivo 102a una vez que el primer usuario 140a cierra ese archivo, o deja de acceder al agente Q 104.

El agente 104 de encriptado puede sobrescribir el archivo encriptado original en la memoria no volátil del primer dispositivo 102a con el archivo recién encriptado y, a continuación, eliminar el archivo de texto sin formato de la

memoria volátil del primer dispositivo 102a si, al dejar de accediendo al archivo de texto sin formato, el primer usuario 140 ha realizado algún cambio en el archivo de texto sin formato. Una vez más, el agente 104 de encriptado puede almacenar información de generación de claves junto con el archivo encriptado para permitir que la clave de encriptado para ese archivo se derive de la información de valor de inicialización de claves o del almacén de claves FED.

Para que los archivos encriptados por el agente Q 104 en el primer dispositivo 102a sean desencriptados por el agente Q 104 en el segundo dispositivo 102b (o cualquier otro dispositivo 102) del primer usuario 140 después de que los archivos se mueven desde el primer dispositivo 102a al segundo dispositivo 102b, el conjunto de valores de inicialización de claves FED $\{K_1, K_2, \cdots, K_J\}$, en algunas operaciones de ejemplo, se puede sincronizar en los L dispositivos 102 del primer usuario 140. Como se mencionó anteriormente, en el sistema 100 es posible que los valores de inicialización de claves de FED deban sincronizarse manualmente entre los L dispositivos 102.

En algunos casos, el almacén de claves FED Ψ puede generarse a partir de los valores de inicialización de claves aleatorias $K_1, K_2, ..., K_J$ utilizando cualquier medio tal que para cualquier dos independientes i y j, $1 \leq i, j \leq \Lambda$, la probabilidad de que una primera clave de encriptado sea igual a una segunda clave de encriptado $\Pr\{k_i = k_j\}$ no es significativamente mayor que $1/\Lambda$. Por ejemplo, los medios utilizados para generar el almacén de claves FED a partir de los valores de inicialización de claves aleatorias pueden estar esencialmente libres de colisiones. En algunas realizaciones, esto puede denominarse propiedad (1) del almacén de claves FED.

En algunos casos, el almacén de claves FED Ψ puede generarse a partir de los valores de inicialización aleatorios $K_1, K_2, \cdots, K_J$ tal que para cualquier $1 \leq i \leq \Lambda$, la clave FED k_i está más o menos uniformemente distribuida y, por lo tanto, estadísticamente independiente de i. En tales casos, la información de divulgación i no puede revelar ninguna información esencial sobre k_i. En algunas realizaciones, esto puede denominarse propiedad (2) del almacén de claves FED.

En algunos casos, el almacén de claves FED Ψ puede generarse a partir de los valores de inicialización aleatorios $K_1, K_2, \cdots, K_J$ tal que para cualquiera de las dos independientes i y j, $1 \leq i, j \leq \Lambda$, conociendo $i, j,$ y una sola clave FED k_i no reduce la cantidad de incertidumbre sobre otra clave FED k_j significativamente, es decir, la entropía condicional de Shannon $H(k_j|i,j,k_i)$ está cerca de $H(k_j|j)$. En tales casos, conocer una clave FED k_i no proporciona ninguna información esencial sobre otra clave FED k_j. En algunas realizaciones, esto puede denominarse propiedad (3) del almacén de claves FED.

Un gran Λ puede proporcionar un aumento de entropía con respecto a las claves generadas. Sin embargo, almacenar todas las claves generadas con un gran valor de Λ puede requerir una cantidad significativa de espacio de almacenamiento. Esto puede no ser deseable cuando los sistemas aquí descritos son dispositivos móviles u otros dispositivos con limitaciones de capacidad de almacenamiento. En algunos casos, el almacén de claves FED Ψ puede generarse a partir de valores de inicialización aleatorios $K_1, K_2, \cdots, K_J$ de tal manera que para cualquier $1 \leq i \leq \Lambda$, es fácil calcular k_i de los valores de inicialización $K_1, K_2, \cdots, K_J$ y el índice i. En tales casos, como se mencionó anteriormente, no es necesario almacenar Ψ en los dispositivos 102 del primer usuario 140. Esto puede ser deseable particularmente cuando Λ es grande. En algunas realizaciones, esto puede denominarse propiedad (4) del almacén de claves FED.

En algunos casos, el agente 104 de encriptado puede almacenar valores de inicialización de claves, donde cada valor de inicialización de claves tiene una primera longitud de bits. El agente 104 de encriptado puede derivar una o más claves de encriptado a partir de los valores de inicialización de claves almacenadas, donde cada una de las claves de encriptado derivadas tiene una segunda longitud de bit. En algunas realizaciones, la segunda longitud de bit puede ser más corta que la primera longitud de bit. Por ejemplo, los valores de inicialización de claves pueden tener una primera longitud de bits de 4096 bits, y las claves de encriptado pueden tener, cada una, una segunda longitud de bits de 256 bits.

Ahora se describirá un proceso de ejemplo para generar una o más claves de encriptado de un valor de inicialización de clave. En el ejemplo, se utiliza el valor de inicialización de clave seleccionada aleatoriamente K_1. K_1 tiene una longitud de primer bit de 4096 bits, y cada clave FED k_i tiene una longitud de segundo bit de 256 bits. Podemos escribir el valor de inicialización de clave K_1 como una pluralidad de bits clave de valor de inicialización $K_1 = K_1(0)K_1(1) \cdots K_1(4095)$. Se puede determinar una pluralidad de valores de derivación de clave de encriptado m para cada clave de encriptado, correspondiendo cada clave de encriptado a una pluralidad única de valores de derivación m. Para cada clave de encriptado, la pluralidad de valores de derivación de clave de encriptado m correspondientes a esa clave de encriptado indica cómo derivar esa clave de encriptado a partir del valor de inicialización de clave K.

En algunas realizaciones, para cualquier $0 \leq m_1 < m_2 < \cdots < m_5 \leq 4095$, podemos definir:

$$k(m_1, m_2, \cdots, m_5) = \sum_{i=1}^{5} K_1(m_i)K_1(m_i + 1) \cdots K_1(m_i + 255)$$

donde la suma de cadenas es la adición binaria y la suma de enteros es con respecto al módulo 4096. Una forma de

generar un almacén de claves Ψ que incluya una pluralidad de claves de encriptado a partir del valor de inicialización aleatorio K_1 es la siguiente:

$$\Psi = \{HMAC(k(m_1, m_2, \cdots, m_5), m_1||m_2||m_3||m_4||m_5|| \text{ OtraEntrada}): 0 \leq m_1 < m_2 < \cdots < m_5 \leq 4095\}$$

donde HMAC representa el código de autentificación de mensaje hash con clave, aquí, por ejemplo, el hash SHA-256 como su función hash incrustada (véase, por ejemplo, el Instituto Nacional de Estándares y Tecnología, El Código de Autentificación de Mensajes de clave Hash (HMAC). Publicación de estándares federales de procesamiento de información 198-1, julio de 2008), || indica concatenación, y otras entradas representa otros materiales de clave que, junto con m_1, m_2, ⋯, m_5, pueden adjuntarse a los datos encriptados. En el ejemplo anterior, para generar cualquier clave de encriptado individual a partir de la clave K_1, se pueden especificar los valores de m_1, m_2, ⋯, m_5.

Obsérvese que, en este ejemplo, $\Lambda \geq 2^{53}$. Puede mostrarse además que, en este caso, se satisfacen las propiedades (1) a (4) mencionadas anteriormente. Específicamente, lo siguiente se mantiene:

a) Dado que cualquier $0 \leq m_1 < m_2 < \cdots < m_5 \leq 4095$, $k(m_1, m_2, \cdots, m_5)$ se distribuye de manera uniforme sobre $\{0,1\}^{256}$.

b) Para cualquier $(m_1, m_2, \cdots, m_5) \neq (\hat{m}_1, \hat{m}_2, \cdots, \hat{m}_5)$ con $0 \leq m_1 < m_2 < \cdots < m_5 \leq 4095$ y $0 \leq \hat{m}_1 < \hat{m}_2 < \cdots < \hat{m}_5 \leq 4095$, $\Pr\{k(m_1, m_2, \cdots, m_5) = k(\hat{m}_1, \hat{m}_2, \cdots \hat{m}_5)\} = 2^{-256}$

c) Para dos independientes $(m_1, m_2, \cdots, m_5)$ y $(\hat{m}_1, \hat{m}_2, \cdots, \hat{m}_5)$ con $0 \leq m_1 < m_2 < \cdots < m_5 \leq 4095$ y $0 \leq \hat{m}_1 < \hat{m}_2 < \cdots < \hat{m}_5 \leq 4095$, uno tiene:

$$H(k(\hat{m}_1, \hat{m}_2, \cdots, \hat{m}_5) | m_1, m_2, \cdots, m_5, \hat{m}_1, \hat{m}_2, \cdots, \hat{m}_5, k(m_1, m_2, \cdots, m_5)) \geq 0{,}6 \text{ x } 256$$

Los resultados (a) a (c), junto con las propiedades de HMAC, a su vez implican las propiedades (1) a (4) anteriores.

En algunos casos, los sistemas descritos en este documento pueden no requerir el código de comprobación C para ser recuperables. En tales casos, la función unidireccional utilizada para generar el código local encriptado a partir del código de verificación no necesita ser invertible. Si no se requiere la recuperación de C, cuando C se pierde u olvida, la función unidireccional φ puede no ser invertible. En tales casos, cualquier función de hash criptográfica podría usarse para generar el código local encriptado a partir del código de verificación C. En algunos casos, sin embargo, puede ser deseable que C sea recuperable cuando se pierde o se olvida. La capacidad de inversión de la función unidireccional φ puede posibilitar la recuperación segura de C cuando C se pierde u olvida. Los sistemas y procedimientos para habilitar la recuperación del código de verificación C se describirán con más detalle a continuación.

Supongamos que no hay exposición de $E_C(K_1, K_2, \cdots, K_J)$ cuando el primer usuario 240 lo sincroniza manualmente en esos dispositivos L. Ahora analizamos la seguridad de las realizaciones de ejemplo de QSSMS descritas anteriormente. Hay dos aspectos a considerar: (1) riesgos de seguridad derivados de la posible exposición de datos, como el código local encriptado β y la información de valor de inicialización de clave (por ejemplo, valores de inicialización de claves encriptadas $E_C(K_1, K_2, \cdots, K_J))$ guardadas localmente por cada agente Q 104 (riesgos de seguridad de almacenamiento); y (2) riesgos de seguridad derivados de la posible exposición de archivos 108/110 encriptados (riesgos de seguridad de encriptado).

Los datos almacenados en un dispositivo 102, tales como β y $E_C(K_1, K_2, \cdots, K_J)$ pueden estar expuestos si uno o más dispositivos 102 con agentes Q 104 instalados en el mismo se pierden o son atacados. Sin embargo, la exposición de los archivos 108/110 encriptados puede ocurrir con mayor frecuencia, ya que dichos archivos pueden transmitirse fácilmente a otros dispositivos, cargarse en un servidor en la nube y/o transmitirse a través de Internet. Si asumimos que todos los algoritmos criptográficos de clave simétrica utilizados tienen la misma fuerza criptográfica, entonces debido a que el código local encriptado se genera mediante una función unidireccional φ y los valores de inicialización de clave $K_1, K_2, \cdots, K_J$ se generan aleatoriamente, los riesgos de seguridad de almacenamiento de QSSMS no son mayores que los de cualquier otro sistema protegido por contraseña.

Para los riesgos de seguridad de encriptado, de nuevo bajo la suposición de que todos los algoritmos de encriptado de claves simétricas utilizadas tienen la misma fuerza criptográfica, la seguridad de encriptado puede entonces dependerá de qué tan fuertes son las claves FED. En las realizaciones del sistema QSSMS con claves FED k_i que son aleatorias y distribuidas uniformemente, la fuerza de encriptado de archivos de QSSMS no es más débil que la de cualquier otro sistema de claves simétricas. Por lo tanto, si no hay ningún fallo en la parte del primer usuario 140,

es decir, no se pierde el dispositivo 102 con agente Q 104 en su interior y el código de verificación C es fuerte y no se olvida, entonces las realizaciones descritas anteriormente de QSSMS son tan seguras como cualquier otro sistema utilizando claves simétricas.

Sin embargo, algunas realizaciones de QSSMS descritas anteriormente pueden estar limitadas a sincronización manual. El conjunto de valores de inicialización de claves aleatorias $\{K_1, K_2, \cdots, K_J\}$ puede tener que sincronizarse manualmente a través de esos *L* dispositivos por el primer usuario 240, como se ha mencionado. Esto puede causar inconvenientes al primer usuario 240, pero también puede evitar compartir archivos encriptados entre un grupo de diferentes usuarios. Para superar este problema, puede ser conveniente sincronizar automáticamente los valores de inicialización de claves entre dispositivos. Las realizaciones del sistema QSSAS que se describen a continuación pueden sincronizar de forma automática y segura el conjunto de valores de inicialización aleatorios $\{K_1, K_2, \cdots, K_J\}$ a través de agentes Q en dispositivos del primer usuario 240 y a través de agentes Q en dispositivos de un grupo de usuarios, según sea el caso.

QSSAS

La figura 2 ilustra una configuración de ejemplo de un sistema QSSAS 200. El sistema 200 puede considerarse una extensión o modificación del sistema 100, y las operaciones generales descritas anteriormente con referencia al sistema 100 también pueden aplicarse en el sistema 200. En la descripción que sigue, el sistema 200 se describirá generalmente con referencia a realizaciones en las que el primer usuario 240 es un único usuario en control de cada uno de los dispositivos 202. Sin embargo, en algunas realizaciones, el primer usuario 240 puede incluir una pluralidad de usuarios del grupo, con cada usuario del grupo en control de uno de los dispositivos 202.

El sistema 200 incluye una pluralidad de dispositivos 202 configurados para la comunicación electrónica con un servidor 230 que puede denominarse como un servidor Q 230. La pluralidad de dispositivos 202 incluye un primer dispositivo 202a y un segundo dispositivo 202b. Cada dispositivo ha instalado en el mismo un agente 204 de encriptado, que pueden denominarse agentes Q o agentes de encriptado. En algunas realizaciones, una vez que un agente 204 de encriptado se instala en un dispositivo 202 y se registra con éxito con el servidor Q 230, puede funcionar en línea o fuera de línea. En general, los agentes 204 de encriptado pueden realizar las mismas operaciones que los agentes 104 de encriptado. Los dispositivos 202 pueden comunicarse con el servidor 230 utilizando una red 220.

En algunos casos, cuando el agente 204 de encriptado se ejecuta en un dispositivo 202 y no hay conexión de red entre el dispositivo 202 y servidor Q 230, el agente 204 de encriptado puede comunicarse periódicamente con el servidor Q 230. Por ejemplo, el agente 204 de encriptado puede comunicarse con servidor Q 230 para verificar el estado del sistema 200 y/o solicitar o iniciar ciertas acciones. En algunos casos, puede que no haya comunicación directa entre los agentes 204 de encriptado en diferentes dispositivos 202 del primer usuario 240. En algunas realizaciones, el sistema 200 permite que los agentes 204 de encriptado en diferentes dispositivos 202 funcionen de manera autónoma, mientras que el conjunto de claves FED (por ejemplo, los valores de inicialización de claves aleatorias y/o el almacén de claves FED) utilizado por los dispositivos 202 se puede sincronizar de forma automática y segura. Las realizaciones del sistema 200 descritas en este documento pueden incorporar conceptos tales como la función unidireccional y los criptosistemas de clave pública para permitir la sincronización segura.

Debe observarse que en algunas realizaciones, los agentes 204 de encriptado en la figura 2 pueden instalarse y registrarse con servidor Q 230 con varios días, meses o años de diferencia. Por ejemplo, el primer usuario 240 puede comprar un nuevo dispositivo 202 e instalar un agente 204 de encriptado en el nuevo dispositivo 202. Luego, el agente 204 de encriptado en el nuevo dispositivo 202 puede configurarse para sincronizar de forma automática y segura los valores de inicialización de claves FED y/o las claves FED para el nuevo dispositivo con el conjunto de claves FED utilizadas por uno o más agentes 204 de encriptado instalados en otros dispositivos controlados por el primer usuario 240 y previamente registrados con el servidor 230.

Las operaciones de varias realizaciones del sistema 200 se describirán ahora en dos partes. La primera parte describe las operaciones del sistema en realizaciones de ejemplo desde la perspectiva del primer usuario 240 y el agente 204 de encriptado en el primer dispositivo 202a. La segunda parte describe algunos procedimientos de ejemplo de acciones entre el agente 204 de encriptado, el primer usuario 240, el servidor Q 230 y, en algunos casos, los otros dispositivos 202.

Operación del sistema

Desde la perspectiva del primer usuario 240 y el agente 204 de encriptado en el primer dispositivo 202a, puede parecer que el sistema 200 opera como una máquina de estados finitos. Como tal, comenzamos con la descripción de algunos estados de ejemplo que se pueden encontrar en varias realizaciones del sistema QSSAS 200. Estos estados de ejemplo incluyen:

- Un estado de usuario no registrado (**NRU**). NRU indica que el primer usuario 240 no se ha registrado en servidor Q 230.

- Un usuario registrado con estado de agente de encriptado no registrado (**RUNRC**). Este estado puede indicar

que el primer usuario 240 se ha registrado en el servidor Q 230, pero el agente 204 de encriptado para el primer dispositivo 202a no se ha registrado en el servidor Q 230.

- Un agente de encriptado en ejecución y abierto al estado del usuario (**ROU**). Este estado puede indicar que el primer usuario 240 y el agente 204 de encriptado en el primer dispositivo 202a se registraron en el servidor Q 230, el agente 204 de encriptado se está ejecutando, y el primer usuario 240 fue autentificado por el agente 204 de encriptado para acceder a los archivos 208/210 administrados por el agente 204 de encriptado, crea o agrega nuevos archivos para que el agente 204 de encriptado administre, y/o toma o solicita al agente 204 de encriptado que tome ciertas medidas. El primer usuario 240 puede autentificarse de la misma manera que se describe anteriormente en el sistema 100.

- Un agente de encriptado que se ejecuta en segundo plano, pero cerrado al estado del usuario (**RCU**). Este estado puede indicar que tanto el primer usuario 240 como el agente 204 de encriptado en el primer dispositivo 202a se han registrado en el servidor Q 230, el agente 204 de encriptado se está ejecutando en segundo plano, pero el primer usuario 240 no ha sido autentificado por el agente 204 de encriptado.

- Un estado de ejecución de agente de encriptado finalizado (**EXIT**). Este estado puede indicar que tanto el primer usuario 240 como el agente 204 de encriptado en el primer dispositivo 202a se registraron en servidor Q 230, y que la ejecución del agente 204 de encriptado se terminó.

- Un estado de visualización y/o edición de contenido (**CVE**). Este estado puede ser un estado transitorio. En algunas realizaciones, el sistema 200 puede transitar al estado de **CVE** desde el estado de **ROU** cuando el primer usuario 240 selecciona algunos archivos 208/210 encriptados en el agente 204 de encriptado para su visualización y/o edición.

- Un estado de reencriptado de contenido (**CRE**). Este estado puede ser un estado transitorio. En algunas realizaciones, el sistema 200 pasa al estado de **CRE** desde el estado de **ROU** cuando el primer usuario 240 solicita al agente 204 de encriptado que utilice nuevas claves FED para volver a encriptar los archivos encriptados antiguos administrados por el agente 204 de encriptado. Las nuevas claves FED se pueden generar como se describió anteriormente con referencia a la figura 1.

- Un nombre de usuario y/o contraseña cambió de estado (**UPC**). Este estado puede indicar que el primer usuario 240 ha cambiado el nombre de usuario y/o la contraseña en el servidor Q 230 a través de medios distintos al agente 204 de encriptado que se ejecuta en el primer dispositivo 202a.

- Un código de verificación cambió de estado (**VCC**). Este estado puede indicar que el primer usuario 240 ha cambiado el código de verificación usando un agente 204 de encriptado en otro dispositivo 202 controlado por el primer usuario 240.

En diversas realizaciones, puede haber más o menos estados del sistema 200. También puede haber muchas transiciones de estado en las que el sistema transita de uno de los estados anteriores a otro, o a otros estados no mencionados específicamente. El sistema 200 puede transitar de un estado a otro en respuesta a las acciones del primer usuario 240, el agente 204 de encriptado, el primer dispositivo 202a, otro dispositivo 202 y/o el servidor 230.

En diferentes realizaciones, el primer usuario 240, el agente 204 de encriptado, y/o el primer dispositivo 202a pueden tomar una serie de acciones diferentes. Ejemplos de tales acciones incluyen el registro de usuarios (UR); el registro de agente de encriptado y generación de valor de inicialización de almacén de claves (CRKG); el nuevo registro del agente de encriptado (CRR); el cambio de ID (nombre de usuario y contraseña) en el servidor Q 230 (IDCS); el cierre de agente de encriptado (CC), es decir, cierre del agente 204 de encriptado, pero manteniendo el agente 204 de encriptado ejecutándose en segundo plano; la autentificación de usuario por el agente 204 de encriptado (UAC); la ejecución del agente de encriptado (CE); la terminación del agente de encriptado (CT); el cambio de ID a través del agente de encriptado registrado en ejecución 204 (IDCC); el cambio de ID a través de medios diferentes al agente de encriptado registrado en ejecución 204 en el primer dispositivo 202a (IDCO); el acceso al contenido (CA); el reencriptado mediante el uso de un nuevo algoritmo criptográfico de clave simétrica (RE); nueva generación activa de valores de inicialización de almacén de claves (ANKG); nueva generación de valores de inicialización de almacén de claves pasivas (PNKG); cambio de código de verificación activo (AVCC); cambio de código de verificación pasivo (PVCC); cambio de pin (PC); actualización del código de verificación (VCU); y creación y/o adición de contenidos (CCA).

Algunas de las acciones de ejemplo mencionadas anteriormente pueden requerir la colaboración del servidor Q 230. En general, el servidor Q 230 es pasivo y actúa en respuesta a las solicitudes de uno de los agentes 204 de encriptado en un dispositivo 202 y/o el primer usuario 240. En algunas realizaciones, el servidor Q 230 puede no tener acceso a los 240 archivos del primer usuario. Además, en algunas realizaciones, el servidor Q 230 puede no conocer ninguna de los valores de inicialización de claves y/o claves FED. Estas realizaciones pueden minimizar los riesgos que surgen de los ataques al servidor Q 230 y personas maliciosas.

La figura 3 muestra un ejemplo de diagrama de transición de estado, en una realización del sistema 200, desde la

perspectiva del agente 204 de encriptado en el primer dispositivo 202a y el primer usuario 240. En general, el sistema 200 puede comenzar con el estado de **NRU** si el primer usuario 240 no se ha registrado en el servidor Q 230. Si el primer usuario 240 se ha registrado en el servidor 230, el sistema 200 puede comenzar en el estado de **RUNRC.**

Si el primer usuario 240 está registrado en el servidor 230, se puede generar una primera cuenta para el primer usuario 240. La primera cuenta puede almacenar datos de la cuenta en la memoria no volátil del servidor 230. Los datos de la cuenta pueden incluir un identificador del primer usuario que identifica al primer usuario en el control de los dispositivos 202. Los datos de la cuenta también pueden incluir información de autentificación de la cuenta, la información de autentificación de la cuenta se puede usar para autentificar a un usuario que intenta acceder a los archivos almacenados en un agente 204 de encriptado asociado con la primera cuenta o para acceder a información o datos asociados con la primera cuenta que se almacena en el servidor 230. Por ejemplo, como se describirá con más detalle a continuación, la información de autentificación de la cuenta se puede usar para autentificar a un usuario y/o dispositivo cuando se sincronizan valores de inicialización de claves entre dispositivos 202.

Para la transición de **NRU** a **RUNRC**, se puede tomar la acción de UR. Un ejemplo del procedimiento de UR se describirá en detalle más adelante. En respuesta a la acción de UR, el sistema 200 puede transitar de **NRU** a **RUNRC.** En el estado **RUNRC,** el primer usuario 240 puede realizar la acción de IDCS. IDCS puede permitir que el primer usuario 240 cambie su ID directamente en el servidor Q 230. Esto puede ser útil cuando uno de los L dispositivos 202 con un agente 204 de encriptado instalado se pierde o es robado y el primer usuario 240 no tiene acceso a otros agentes 204 de encriptado en ese momento. En tales casos, el primer usuario 240 puede comunicarse con el servidor Q 230 directamente para cambiar su ID en el servidor Q 230. En algunas realizaciones, si el dispositivo perdido o robado 202 tiene una conexión de red y el agente 204 de encriptado se está ejecutando, el agente 204 de encriptado en el dispositivo 202 perdido o robado puede cerrar sesión automáticamente después de descubrir mediante comunicación con el servidor 230 que el primer ID del usuario 240 ha sido cambiado.

Otra acción de ejemplo que se puede tomar en el estado de **RUNRC** es CRKG. La acción de CKRG puede permitir que el agente 204 de encriptado en el primer dispositivo 202a se registre en el servidor Q 230. En algunos casos, el agente 204 de encriptado puede configurar un PIN para autentificar al primer usuario 240 cada vez que el primer usuario 240 quiera acceder a los archivos administrados por el agente 204 de encriptado más adelante a través del agente 204 de encriptado. En algunos casos, se puede configurar un código de verificación C, por ejemplo, si el agente 204 de encriptado en el primer dispositivo 202a es el primer agente de encriptado que el primer usuario 240 ha instalado en cualquiera de los L dispositivos 202.

En algunos casos, un conjunto de valores de inicialización de claves FED (es decir, una pluralidad de valores de inicialización de claves) puede generarse por el agente 204 de encriptado. El agente de encriptado puede utilizar la pluralidad de valores de inicialización de claves para derivar una o más claves de encriptado, por ejemplo, al encriptar un archivo o para generar un almacén de claves FED. En algunos casos, la pluralidad de valores de inicialización de claves se puede generar a través de la comunicación entre el agente 204 de encriptado y el servidor Q 230. El agente de encriptado puede determinar la información de valor de inicialización de clave en base a la pluralidad de valores de inicialización de clave y almacenar la información de valor de inicialización de clave en la memoria no volátil del primer dispositivo 202a. Por ejemplo, el agente de encriptado puede generar la información de valor de inicialización de clave mediante el encriptado de los valores de inicialización de clave utilizando el código de verificación C como su clave de encriptado. Los valores de inicialización de claves encriptadas se pueden almacenar como la información de valores de inicialización de clave en la memoria no volátil del primer dispositivo 202a.

Si el primer usuario 240 ya ha generado una pluralidad de valores de inicialización de claves en otro dispositivo 202, el primer usuario 240 puede generar la pluralidad de valores de inicialización de claves en el primer dispositivo para que sea igual a los valores de inicialización de claves utilizados por el agente de encriptado en el otro dispositivo. Las realizaciones de ejemplo del sistema 200 en las que los valores de inicialización de claves están sincronizados entre dispositivos 202 se describirán con más detalle más adelante.

El sistema 200 puede transitar desde el estado de **RUNRC** al estado de ROU, por ejemplo, después de CKRG. En el estado de **ROU,** el primer usuario 240 puede realizar una serie de acciones diferentes. Por ejemplo, el primer usuario 240 puede cambiar el PIN de autentificación utilizado por el agente 204 de encriptado, cambiar su ID a través del agente 204 de encriptado, crear y/o agregar nuevos archivos para que el agente 204 de encriptado pueda administrar, cambiar el código de verificación y solicitar para generar un nuevo conjunto de valores de inicialización de claves FED a través de las acciones de PC, IDCC, CCA, AVCC y ANKG, respectivamente. En el ejemplo que se muestra, el primer usuario 240 puede realizar estas acciones sin que el sistema 200 abandone el estado de **ROU**.

En algunos casos, mientras está en el estado **ROU,** el agente 204 de encriptado puede generar automáticamente un nuevo conjunto de valores de inicialización de claves alimentado a través basa en la comunicación con el servidor Q 230 a través de la acción de PNKG. Por ejemplo, esto puede ocurrir si el agente 204 de encriptado determina, en base a la comunicación con el servidor Q 230, que otro agente 204 de encriptado del primer usuario 240 ha generado un nuevo conjunto de valores de inicialización de claves FED del primer usuario, en algunos casos con la colaboración del servidor Q 230. Cualquier archivo recién creado y/o agregado puede ser encriptado automáticamente por el agente 204 de encriptado utilizando una clave FED seleccionada desde el almacén de

claves de FED o derivada de los valores de inicialización de claves (por ejemplo, por archivo) disponible en el agente 204 de encriptado y designada para el primer usuario 204, a menos que el archivo agregado ya esté encriptado por otro agente 204 de encriptado del primer usuario 204. El archivo encriptado resultante junto con la información de generación de claves (como el índice de la clave FED utilizada en el almacén de claves, o la información que indica cómo derivar la clave de los valores de inicialización de claves) a partir de las cuales se puede derivar la clave FED se puede guardar como el archivo encriptado en la memoria no volátil del primer dispositivo 202a.

En algunos casos, el sistema 200 puede permanecer en el estado de **ROU** a menos que se tome una de las acciones de CA, RE, PVCC, IDCO, CC, CT. Ahora se describirán ejemplos de estas acciones.

CA: Con el sistema 200 en el estado de **ROU,** el primer usuario 240 puede querer acceder a sus archivos 208/210 administrados por el agente 204 de encriptado para ver y/o realizar cambios. En este caso, el agente 204 de encriptado puede desencriptar los archivos 208/210 seleccionados por el primer usuario 240 y almacenar los archivos de texto sin formato desencriptados en la memoria volátil del primer dispositivo 202a para que el primer usuario 240 los lea y modifique. En tales casos, el sistema 200 puede transitar desde el estado de **ROU** al estado de **CVE** transitorio.

Después de que el primer usuario 240 cierre cada archivo de texto sin formato, el agente 204 de encriptado puede borrar el archivo de texto sin formato de la memoria volátil del primer dispositivo 202a si no hay cambios. En algunos casos, el agente 204 de encriptado puede volver a encriptar el archivo de texto sin formato utilizando una clave FED derivada de la información del valor de inicialización de clave (por ejemplo, por archivo o seleccionada del almacén de claves) y sobrescribir el archivo encriptado original en la memoria no volátil del primer dispositivo 202a con el archivo recién encriptado. Esto puede ocurrir si el primer usuario 240 ha realizado algún cambio en el archivo de texto sin formato o no. Luego, el agente 204 de encriptado puede borrar el archivo de texto sin formato de la memoria volátil del primer dispositivo 202a. Después de que se cierran todos los archivos seleccionados, el sistema 200 puede volver al estado de **ROU.**

RE: En algunas realizaciones, cuando el agente 204 de encriptado se actualiza con un nuevo algoritmo criptográfico de clave simétrica debido a la evolución estándar del encriptado u otras razones, los archivos 208/210 encriptados con el antiguo algoritmo criptográfico de clave simétrica dentro del agente 204 de encriptado deben ser reencriptados con el nuevo algoritmo criptográfico de clave simétrica. Si se toma la acción de RE, el sistema 200 puede transitar temporalmente al estado transitorio de **CRE,** en el que el agente 204 de encriptado puede usar primero el antiguo algoritmo criptográfico para desencriptar todos los archivos 208/210 bajo su administración en el primer dispositivo 202a, y luego usar el nuevo algoritmo criptográfico para volver a encriptar todos los archivos desencriptados nuevamente. Luego, QSSAS puede volver al estado de **ROU.** Esto puede permitir que el mismo agente 204 de encriptado permanezca actual y actualizado con el nivel de seguridad deseado, por ejemplo, si se detectan vulnerabilidades en el algoritmo de encriptado que utiliza el agente 204 de encriptado, o si se desarrollan algoritmos de encriptado más seguros.

PVCC: En algunas realizaciones, si el primer usuario 240 ha cambiado el código de verificación a través de uno de sus otros dispositivos 202 a través del agente 204 de encriptado, el agente 204 de encriptado en el primer dispositivo 202a en el estado de **ROU** puede cerrar automáticamente la sesión después de detectar tal cambio basado en la comunicación con el servidor Q 230. En tales realizaciones, el sistema 200 puede transitar desde el estado de **ROU** al estado de **VCC,** en el cual el agente 204 de encriptado en el primer dispositivo 202a puede no funcionar a menos que el primer usuario 240 ingrese los códigos de verificación antiguos y nuevos para habilitar el agente 204 de encriptado en el primer dispositivo 202a para actualizar su código local encriptado, y la información de valor de inicialización de clave almacenada en el primer dispositivo 202a a través de la acción de VCU. Después de la acción de VCU, QSSAS puede volver al estado de **ROU.**

IDCO: En algunas realizaciones, si el primer usuario 240 ha cambiado su ID a través de otros medios distintos al agente 204 de encriptado en el primer dispositivo 202a, con el sistema 200 en el estado de **ROU**, el agente 204 de encriptado en el primer dispositivo 202a puede cerrar sesión automáticamente después de detectar un ID modificado basado en la comunicación con el servidor Q 230. En tales casos, el sistema 200 puede transitar desde el estado de **ROU** al estado de **UPC.** En el estado de **UPC,** el agente 204 de encriptado en el primer dispositivo 202a puede dejar de estar registrado. Si el agente 204 de encriptado en el primer dispositivo 202a deja de estar registrado, es posible que el agente 204 de encriptado no opere a menos que se vuelva a registrar con el servidor Q 230 con el nuevo ID del primer usuario 240 (por ejemplo, a través de la acción de CRR). Después de la acción de CRR, el sistema 200 puede volver al estado de **ROU.**

CC: En algunas realizaciones, si el sistema 200 se deja en el estado de **ROU** durante un cierto período de tiempo sin ninguna actividad del primer usuario 240 o si el primer usuario 240 cierra el agente 204 de encriptado (por ejemplo, cerrando la pantalla o la carpeta del agente de encriptado) en el primer dispositivo 202a), el sistema 200 puede transitar de **ROU** al estado de **RCU.** En el estado de **RCU**, el agente 204 de encriptado puede ejecutarse en segundo plano, pero el primer usuario 240 no podrá acceder a los archivos 208/210 bajo su administración a menos que el primer usuario 240 sea autentificado nuevamente por el agente 204 de encriptado ingresando el PIN correcto o código de verificación (es decir, a través de la acción de UAC). Después de la acción de UAC, el sistema 200 puede volver a **ROU.**

CT: En algunas realizaciones, si la ejecución del agente de encriptado finaliza ya sea por el primer usuario 240 o el primer dispositivo 202a, el sistema 200 puede transitar desde **ROU** al estado de **EXIT.** Para volver a **ROU** desde **EXIT,** el agente 204 de encriptado debe ejecutarse nuevamente ingresando el nombre de usuario, la contraseña y el código de verificación correctos (es decir, a través de la acción de CE), y luego el primer usuario 240 debe ser autentificado nuevamente por el agente 204 de encriptado a través de la acción de UAC.

Las transiciones del sistema 200 de **RCU** a **UPC** a través de la acción de IDCO, a **VCC** a través de la acción de PVCC, a **EXIT** a través de la acción de CT, y a **RCU** a través de la acción de PNKG en la figura 3 pueden ser similares a las respectivas transiciones del sistema 200 desde **ROU** descritas anteriormente.

En general, los archivos 208/210 administrados por agentes 204 de encriptado y almacenados en una memoria no volátil (ya sea en los *L* dispositivos 202 del primer usuario 240 o en otro lugar, tal como en un servidor en la nube) pueden permanecer encriptados todo el tiempo. Sus archivos de texto sin formato pueden ser visibles solo dentro de los agentes 204 de encriptado del primer usuario 240 cuando se descifran y se almacenan temporalmente en la memoria volátil de los dispositivos 202 del primer usuario 240 en el estado transitorio de **CVE.** En algunas realizaciones, aparte de los agentes 204 de encriptado del primer usuario 240, ninguna otra parte, incluido el servidor Q 230, conoce ninguna de los valores de inicialización de claves FED y/o las claves FED disponibles en los agentes 204 de encriptado, los archivos 208/210 no pueden ser desencriptados y, por lo tanto, no son significativos fuera de los agentes 204 de encriptado del primer usuario 240 para tales realizaciones. En tales realizaciones, los archivos 208/210 pueden considerarse "vivos" solo dentro de los agentes 204 de encriptado y "muertos" siempre que se eliminen de los agentes 204 de encriptado. De esta manera, se puede considerar que los agentes 204 de encriptado proporcionan un sistema de seguridad en cuarentena en el que los archivos solo son accesibles dentro de la zona de cuarentena del agente de encriptado. Dado que el conjunto de valores de inicialización de claves FED utilizadas por cada agente 204 de encriptado y designadas para el primer usuario 240 se pueden sincronizar de forma automática y segura en todos los agentes 204 de encriptado del primer usuario 240, los archivos administrados por los agentes 204 de encriptado del primer usuario 240 pueden ser desencriptados por cualquiera de esos agentes 204 de encriptado. Esto, junto con la naturaleza en cuarentena del sistema 200, también puede permitir que el primer usuario 240 sincronice de forma segura los archivos administrados por esos agentes 204 de encriptado a través de algún servicio informático en la nube de terceros u otros medios a través de Internet.

La figura 5 ilustra una realización de ejemplo de un sistema 500 implementado junto con un servicio informático en la nube 550. El sistema 500 generalmente corresponde al sistema 200, con una pluralidad de dispositivos 502a-502*l* configurados para comunicarse con el servidor 530. Los archivos 508/510 administrados por los agentes 504 de encriptado del primer usuario 540 se pueden sincronizar con la nube 550 y en esos L dispositivos 502 del primer usuario 540 a través del servicio informático en la nube 550. Debido a la naturaleza en cuarentena de los sistemas 200/500, los riesgos de seguridad inherentes a la computación en la nube pueden reducirse significativamente, lo que permite al primer usuario 540 disfrutar de los beneficios de la computación en la nube sin mayores preocupaciones de seguridad.

Procedimientos de Acciones

A continuación, se describirán los procedimientos de esas acciones en la figura 3 que no han sido explicados completamente en la subsección anterior, a saber, UR, IDCS, IDCC, CRKG, AVCC, VCU, ANKG, y PNKG. Una vez más, con referencia a la figura 2, usamos el agente 204 de encriptado en el primer dispositivo 202a como ejemplo.

Procedimiento de UR

Cuando el primer usuario 240 quiere registrarse con el servidor Q 230, el primer usuario 240 puede proporcionar primero un par de nombre de usuario o identificador del primer usuario, U y una primera contraseña de usuario P. El servidor Q 230 puede almacenar el identificador del primer usuario en la primera cuenta para el usuario *U.* El servidor 230 también puede hacer dos copias de *U*, una guardada y designada como U_o, que puede usarse para indicar el identificador del primer usuario antiguo cuando el primer usuario 240 desea cambiar el identificador del primer usuario más adelante, y el otro guardado y designado como el registro inicial, identificador del primer usuario U_r para el primer usuario 240.

El sistema 200 (por ejemplo, cualquiera de los dispositivos 202a o el servidor 230) puede determinar primero la contraseña de usuario basándose en la primera contraseña de usuario. El servidor 230 puede almacenar la primera información de la contraseña del usuario como la información actual de la primera contraseña del usuario. El servidor también puede almacenar una copia de la información de la contraseña del primer usuario como la información de la contraseña del primer usuario anterior y otra copia de la información de la contraseña del primer usuario como la información de la contraseña del primer usuario del registro inicial para el primer usuario 240.

Por ejemplo, el sistema 200 puede determinar la primera información de la contraseña del usuario calculando un valor hash $E(P)$ de la contraseña *P.* El servidor Q 230 puede almacenar la clave hash $E(P)$ como la primera contraseña actual del usuario información, y también hacer dos copias de $E(P)$, una guardada y designada como la información antigua de la contraseña del primer usuario $E(P_o)$ y la otra guardada y designada como la información inicial de la contraseña del primer usuario $E(P_r)$ para el primer usuario 240. En algunos casos, la información de la

contraseña del primer usuario $E(P_r)$ del registro inicial no se puede cambiar incluso cuando el primer usuario 240 cambia la primera contraseña del usuario más adelante.

El servidor Q 230 puede inicializar una cadena llamada cadena de estado de clave. La cadena de estado de clave puede incluir una parte de estado de clave y una parte de indicador de clave de servidor. La cadena de estado de clave puede inicializarse para tener una parte de estado de clave que indica que no se han generado valores de inicialización de clave para el primer usuario 240. En algunos casos, en la etapa de fuente, antes de la generación de valores de inicialización de clave, la porción del indicador de clave del servidor puede estar en blanco, o puede incluir datos aleatorios. Por ejemplo, cuando la cadena de estado de clave se representa como $S = S_0S_1S_2 \cdots S_{2(i+1)}$, la cadena de estado de clave se puede inicializar para que sea $S = 0$.

En algunos casos, el sistema 200 puede solicitar al primer usuario 240 que proporcione una dirección de correo electrónico o número de teléfono válido para servidor Q si el nombre de usuario proporcionado no es una dirección de correo electrónico. En tales casos, la dirección de correo electrónico o el número de teléfono pueden considerarse el identificador del primer usuario. En algunos casos, como se explica más adelante, el primer usuario 240 puede tener una pluralidad de identificadores de alias (tal como varias direcciones de correo electrónico, nombres de usuario y/o números de teléfono u otros identificadores). El identificador del primer usuario puede incluir cada uno de los identificadores de alias.

Procedimientos de IDCS y IDCC

Como se ha mencionado antes, en algunos casos, el primer usuario 240 puede cambiar su ID directamente al servidor Q 230 para proporcionar una seguridad adicional. En este ejemplo, usamos el cambio de contraseña como ejemplo para ilustrar el procedimiento. La primera contraseña de usuario que el primer usuario 240 tiene actualmente con el servidor Q 230 puede denominarse la primera contraseña de usuario actual P_c, y la contraseña a la que el primer usuario 240 quiere cambiar se llama la nueva contraseña de primer usuario P_n. Ahora se describirá un procedimiento de ejemplo para cambiar la primera contraseña de usuario directamente en el servidor Q 230.

El primer usuario 240 puede transmitir una solicitud de cambio de contraseña al servidor 230. En respuesta, el servidor Q 230 puede solicitar el identificador del primer usuario (por ejemplo, el nombre de usuario U), la contraseña actual del primer usuario P_c, y la nueva contraseña del primer usuario P_n. El primer usuario 240 puede entonces proporcionar el identificador del primer usuario y una contraseña de primer usuario putativo al servidor 230.

El servidor 230 puede determinar la información de la contraseña del primer usuario putativo basándose en la contraseña del primer usuario putativo. El servidor 230 puede entonces usar el identificador del primer usuario para identificar la primera cuenta y comparar la información de la contraseña del primer usuario putativo con la información de la primera contraseña de usuario almacenada en la información de autentificación de la primera cuenta.

Por ejemplo, el sistema 200 (por ejemplo, el dispositivo 202a o el servidor 230) puede calcular valores hash de la contraseña del primer usuario putativo y la nueva contraseña (P_c y P_n), y verificar el nombre de usuario U y el hash de contraseña de primer usuario putativo $E(P_c)$ con el registro del nombre de usuario actual y el hash de contraseña almacenados en servidor Q para la autentificación.

Una vez que el primer usuario 240 ha sido autentificado, el servidor Q 230 puede actualizar el hash de la contraseña actual en su registro a $E(P_n)$, y el hash de la contraseña anterior en su registro a $E(P_o) = E(P_c)$ manteniendo la contraseña de registro inicial hash $E(P_r)$ sin tocar.

Se aplican procedimientos similares para cambiar el identificador del primer usuario/nombre de usuario o cambiar el nombre de usuario y la contraseña directamente en el servidor Q 230. Una vez que el primer usuario 240 se autentifica con éxito, el servidor Q 230 puede, para cualquier credencial que el primer usuario 240 quiere cambiar (y está autorizado a cambiar), actualizar la credencial actual correspondiente de su registro a la credencial anterior respectiva y actualizar la respectiva nueva credencial a la respectiva credencial actual en su registro. Del mismo modo, cuando se realizan cambios de ID a través del agente 204 de encriptado en el primer dispositivo 202a, los cambios se pueden registrar tanto en el agente 204 de encriptado como en el servidor Q 230 una vez que el primer usuario 240 se autentifica con éxito.

Procedimiento de CRKG sin recuperación de código de verificación

Para sincronizar de forma segura y automática el conjunto de valores de inicialización de claves FED utilizadas por cada agente 204 de encriptado y designadas para el primer usuario 240 en todos los agentes 240 de encriptado del primer usuario 240, podemos integrar los conceptos de función unidireccional y sistema de encriptado de clave pública en el funcionamiento del sistema 200, incluidos CRKG, AVCC, VCU, ANKG y PNKG. La generación y sincronización de valores de inicialización de claves se describirán ahora con referencia a las figuras 2 y 4A-4C.

Las figuras 4A-4C muestran una serie de diagramas de flujo de un ejemplo de realización de un procedimiento 400 para proporcionar el encriptado en una pluralidad de dispositivos. Por ejemplo, el sistema 200 se puede usar para implementar el procedimiento 400 para proporcionar encriptado en los dispositivos 202 controlados por el primer

usuario 240. Las extensiones del procedimiento 400 cuando el primer usuario incluye diferentes usuarios con el control de los dispositivos 202 o una pluralidad de usuarios de grupos se describirán más adelante con referencia a las figuras 6C, 8 y 9.

En el procedimiento 400, el servidor 230 ha generado una primera cuenta para el primer usuario 240 en el control de la pluralidad de dispositivos 202. Como se mencionó anteriormente, la primera cuenta almacena los datos de la cuenta en la memoria del servidor no volátil, donde los datos de la cuenta incluyen un identificador del primer usuario e información de autentificación de la cuenta.

Aunque las operaciones del sistema 200 y el procedimiento 400 se describirán en detalle, en algunos casos, se describirán ejemplos específicos de aspectos incorporados de un sistema de encriptado de clave pública bien conocido. Dado que existen varios sistemas criptográficos de clave pública conocidos como RSA (R. L. Rivest, A. Shamir, y L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Comm. ACM, vol. 21, n.º 2, páginas 120 - 126, Feb. 1978) ElGamal (T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," IEEE Transactions on Information Theory, vol. 31, n.º 4, páginas 469 - 472, Julio 1985), y "ECC public key cryptosystems" (I. F. Blake, G. Seroussi, y N. P. Smart, Elliptic Curves in Cryptography. Cambridge University Press, 1999), para ser específicos, se describirán a continuación algunos ejemplos específicos que incorporan aspectos del sistema público de ElGamal como ejemplo. Sin embargo, será evidente para los expertos que otras realizaciones de los sistemas y procedimientos descritos en este documento pueden no incorporar ningún aspecto del sistema criptográfico ElGamal.

En algunos ejemplos específicos a continuación, los aspectos del sistema 200 pueden describirse en el contexto de un gran número primo seguro N (es decir, $(N - 1)/2$ también es un primo) y el campo finito $GF(N) = \{0,1,2, \cdots, N - 1\}$. Una raíz primitiva α de $GF(N)$, se fija también en estos ejemplos (es decir, $1 \leq \alpha \leq N - 1$ donde α es un número entero cuyas potencias debajo del módulo de N producen cada elemento no nulo en $GF(N)$).

En 405, para cada dispositivo 202 en la pluralidad de dispositivos 202, un agente 204 de encriptado está instalado sobre el mismo. El agente 204 de encriptado se puede utilizar para controlar la operación del procesador del dispositivo, cuando se implementan aspectos del procedimiento 400. El agente 204 de encriptado puede instalarse utilizando los diversos procesos de registro de clientes descritos en este documento.

Por ejemplo, el primer usuario 240 puede ingresar el identificador del primer usuario y la primera contraseña de usuario putativo en el agente 204 de encriptado instalado en el primer dispositivo 202a. El agente 204 de encriptado puede generar información de la contraseña del primer usuario putativo basada en la contraseña del primer usuario putativo, y transmitir el identificador del primer usuario, la información de la contraseña del primer usuario putativo y un primer identificador del dispositivo al servidor 230. Por ejemplo, el agente 204 de encriptado puede calcular un valor de hash $E(P)$ de la contraseña de primer usuario putativo P, que no es necesariamente el mismo que el hash de contraseña de usuario primero almacenado en servidor Q, y luego envía el nombre de usuario U, la clave hash $E(P)$ y el identificador de dispositivo (D) del primer dispositivo 202a (por ejemplo, una dirección MAC) al servidor Q 230 para la autentificación. En algunas realizaciones, el identificador de dispositivo D del primer dispositivo 202a de usuario es único.

El servidor Q 230 puede comparar el identificador del primer usuario U y la información de contraseña de primer usuario putativo $E(P)$ con su registro actual (es decir, el nombre de usuario actual y el hash de la contraseña actual registrados en el servidor Q 230). Si se encuentra una coincidencia, la autentificación del nombre de usuario y la contraseña se realiza correctamente. En algunos casos, se puede realizar otra ronda de verificación al permitir que el servidor Q 230 envíe algunos mensajes de verificación de autentificación a la dirección de correo electrónico o número de teléfono proporcionado por el primer usuario 240 en la etapa de registro de usuario. El servidor Q 230 solicita al primer usuario 240 que proporcione los mensajes al agente de encriptado, que a su vez reenvía los mensajes al servidor Q para su confirmación. En algunos casos, el proceso de autentificación del usuario puede incluir información de identificación biométrica del primer usuario 240. Un ejemplo de tal proceso de autentificación remota se describirá en detalle más adelante.

Si el primer usuario 240 se autentifica, el servidor Q 230 asocia el primer identificador de dispositivo D del primer dispositivo 202a con el primer usuario 240. Si el primer usuario 240 no está autentificado, el proceso de autentificación descrito anteriormente puede repetirse hasta que se logre la autentificación exitosa y la confirmación del mensaje.

El servidor Q 230 puede enviar un acuse de recibo de autentificación exitosa junto con la cadena de estado de clave $S = S_0S_1S_2 \cdots S_{2(i+1)}$ al agente 204 de encriptado. Al recibir el acuse de recibo de una autentificación exitosa junto con la cadena de estado de clave $S = S_0,S_1S_2 \cdots S_{2(i+1)}$, el agente 204 de encriptado puede almacenar el identificador del primer usuario (por ejemplo, nombre de usuario U) e información de la contraseña del primer usuario (por ejemplo, hash de contraseña $E(P)$) en la memoria no volátil del primer dispositivo 202a.

Si la porción del indicador de estado de la cadena de estado de clave recibida indica que no se han generado valores de inicialización de clave, esto sugiere que el primer dispositivo 202a es el primer dispositivo 202 registrado por el primer usuario 240 con el servidor 230 (esto no es necesariamente el caso, pero indica que los valores de

inicialización de clave aún no se han generado en otro dispositivo 202 asociado con el primer usuario 202a). Por ejemplo, si la cadena de estado de clave S comienza con 0, es decir, $S_0 = 0$, esto puede indicar que el agente 204 de encriptado en el primer dispositivo 202a es el primer agente 204 de encriptado registrado por el primer usuario 240 con el servidor Q 230. El agente 204 de encriptado puede solicitar al primer usuario 240 configurar un primer código de verificación C. En algunas realizaciones, el código de verificación C se puede usar para administrar y sincronizar los valores de inicialización de claves a través de los dispositivos 202 controlados por el primer usuario. El código de verificación también puede permitir la generación de la clave privada del primer usuario 240 en todos los agentes 204 de encriptado del primer usuario 240.

El agente 204 de encriptado puede generar una pluralidad de contraseñas desde el código de verificación. La pluralidad de contraseñas se puede generar de tal manera que el código de verificación sea determinable a partir de todas las contraseñas en la pluralidad de contraseñas, pero no es determinable a partir de menos de todas las contraseñas. En algunos casos, la pluralidad de contraseñas puede consistir en una primera contraseña y una segunda contraseña.

Por ejemplo, el agente 204 de encriptado puede convertir el código de verificación C en un par de contraseñas C_1 y C_2 a través de $f(C) = (C_1, C_2)$. La conversión se puede realizar a través de una función de uno a uno *f de* modo que tanto C_1 como C_2 se vean como números aleatorios de $GF(N)$. El código de verificación C puede determinarse a partir de la primera contraseña C_1 y la segunda contraseña C_2, pero no de C_1 o C_2 solamente.

El agente 204 de encriptado puede determinar un código local encriptado basado en el primer código de verificación. Por ejemplo, el agente de encriptado puede determinar un primer valor local encriptado a partir de la primera contraseña y la segunda contraseña, en el que ninguna de la primera contraseña y la segunda contraseña se pueden determinar solo a partir del primer valor local encriptado. En algunos casos, el primer valor local encriptado puede generarse multiplicando la segunda contraseña con α elevado a la potencia de la primera contraseña. El agente 204 de encriptado también puede determinar un segundo valor local encriptado a partir de la segunda contraseña. La segunda contraseña puede ser un logaritmo discreto del segundo valor local encriptado con una base α.

Por ejemplo, el agente de encriptado puede determinar el código local encriptado $\beta = (\beta_1, \beta_2) = (\alpha^{C1}C_2, \alpha^{C2})$, (donde β_1 corresponde al primer valor local encriptado, y β_2 corresponde al segundo valor local encriptado). El agente 204 de encriptado puede guardar el código local encriptado β en la memoria no volátil del primer dispositivo 202a con el fin de verificar una entrada del código de verificación putativo local por parte del primer usuario 240 en el futuro.

El agente 204 de encriptado también puede determinar un código de servidor de encriptado basado en el primer código de verificación. El código de servidor encriptado puede incluir un primer valor de servidor encriptado determinado a partir de la primera contraseña y la segunda contraseña. El código de servidor encriptado también puede incluir un segundo valor de servidor encriptado determinado a partir de la primera contraseña. En algunas realizaciones, ni la primera contraseña ni la segunda contraseña se pueden determinar a partir del primer valor del servidor encriptado. En general, la primera contraseña y la segunda contraseña pueden ser computacionalmente imposibles de determinar a partir del primer valor de servidor encriptado y/o el segundo valor de servidor encriptado ya sea solo o en combinación, es decir, debido a la dificultad de determinar logaritmos discretos. Por ejemplo, el agente 204 de encriptado puede determinar el código del servidor encriptado como $\hat{\beta} = (\hat{\beta}_1, \hat{\beta}_2) = (\alpha^{C1C2}, \alpha^{C1})$. El código del servidor encriptado se puede transmitir al servidor Q 230. El servidor 230 puede almacenar el código de servidor encriptado en la información de autentificación de la primera cuenta.

En algunos casos, el servidor 230 puede generar valores de encriptado del servidor independientes y aleatorizar (o más encriptar) el código del servidor encriptado basado en los valores independientes de encriptado del servidor antes de su almacenamiento. El servidor 230 puede generar los valores de encriptado de servidor independientes como números aleatorios independientes V_{-1}, V_{-2} basados en U_r, $E(P_r)$, y su propia clave secreta v. Los números aleatorios independientes V_{-1}, V_{-2} puede ser distribuido uniformemente sobre $\{1, 2, \cdots, N - 1\}$. El servidor 230 puede entonces aleatorizar $\hat{\beta}$ convirtiéndolo en $D(\beta) = (D(\hat{\beta}_1, V_{-1}), D(\hat{\beta}_2, V_{-2}))$, y guardar $D(\hat{\beta})$ junto con el nombre de usuario y la contraseña hash. La función $D(\cdot,\cdot)$ puede ser de uno a uno y desde $\{1,2, \cdots, N - 1\}$ a $\{1,2, \cdots, N - 1\}$ dado ya sea $\hat{\beta}_j$ o V_{-j}. En algunos casos, el código de servidor encriptado del servidor puede generarse utilizando un valor de hash (por ejemplo, un valor de hash derivado de HMAC) con la clave de servidor secreta v como su clave y el código de servidor encriptado $\hat{\beta}$ como su entrada.

En 410, el agente 204 de encriptado puede generar de forma aleatoria una pluralidad de indicadores de claves. Por ejemplo, el agente 204 de encriptado puede generar independientemente números aleatorios X_j, $j = 0,1, \cdots, J$ como la pluralidad de indicadores de claves. En algunos casos, cada número aleatorio (es decir, cada indicador de clave) se puede distribuir de manera uniforme en $\{1,2, \cdots, N - 1\}$.

En 415, el agente 204 de encriptado puede generar una pluralidad de indicadores de claves encriptados desde la pluralidad de indicadores de claves utilizando una clave de encriptado del segundo dispositivo. Cada uno de los indicadores de claves encriptados puede corresponder a uno de los indicadores de claves en la pluralidad de indicadores de claves. La clave de encriptado del segundo dispositivo puede corresponder a una clave de desencriptado del segundo dispositivo desconocida para el servidor.

En algunos casos (por ejemplo, cuando se utiliza el sistema ElGamal), el agente 204 de encriptado puede también generar aleatoriamente una pluralidad de valores de encriptado. Por ejemplo, el agente de encriptado puede generar la pluralidad de valores de encriptado como números aleatorios independientes Y_j. El agente 204 de encriptado puede generar la pluralidad de indicadores de claves encriptados a partir de la pluralidad de indicadores de claves utilizando la clave de encriptado del segundo dispositivo y la multitud de valores de encriptado. En tales casos, cada uno de los indicadores de claves encriptados también corresponde a uno de los valores de encriptado en la pluralidad de valores de encriptado. El agente 204 de encriptado también puede generar una pluralidad de claves públicas de indicadores de claves. Cada clave pública del indicador de clave puede corresponder a uno de los valores de encriptado en la pluralidad de valores de encriptado. Por ejemplo, el agente de encriptado puede calcular la pluralidad de indicadores de claves encriptados como $\varepsilon_j = \hat{\beta}_2^{Y_j} X_j$ y la pluralidad de claves públicas de indicador de clave como $\mu_j = \alpha^{Y_j}$, $j = 0, 1, \cdots, J,$.

En 420, el agente 204 de encriptado puede transmitir la pluralidad de indicadores de claves encriptados al servidor 230. Los indicadores de claves encriptados pueden transmitirse al servidor 230 para impedir la exposición de los indicadores de claves al servidor 230. Al mismo tiempo, el servidor 230 puede utilizar los indicadores de claves encriptados para actualizar la cadena de estado de clave de la primera cuenta. La cadena de estado de clave actualizada se puede usar para sincronizar los valores de inicialización de claves en otros dispositivos controlados por el primer usuario.

En algunos casos, el agente 204 de encriptado también puede transmitir la pluralidad de claves públicas indicador de clave al servidor 230. Por ejemplo, el agente 204 de encriptado puede enviar (ε_j, μ_j), $j = 0, 1, \cdots, J$, al servidor Q 230.

En 425, el agente 204 de encriptado puede generar una pluralidad de valores de inicialización de clave basándose en la pluralidad de indicadores de claves. Para cada valor de inicialización de clave, el agente 204 de encriptado puede ser operable para generar una pluralidad de claves de encriptado independientes. Como se mencionó anteriormente, en algunas realizaciones, el agente 204 de encriptado puede generar un almacén de claves de encriptado que comprende una pluralidad de claves de encriptado. En otras realizaciones, el agente 204 de encriptado puede derivar claves de encriptado según sea necesario en respuesta a una indicación de un archivo a encriptar.

En algunos casos, el agente 204 de encriptado puede generar la pluralidad de valores de inicialización de clave con asistencia desde el servidor 230. El servidor 230 puede generar aleatoriamente valores de clave de servidor para la primera cuenta. Los valores de clave del servidor pueden almacenarse en la memoria no volátil del servidor y transmitirse al primer dispositivo 202a. El agente 204 de encriptado puede generar la pluralidad de valores de inicialización de clave basadas en los valores de clave del servidor y la pluralidad de indicadores de claves.

En algunas realizaciones, el agente 204 de encriptado puede enviar una cantidad de indicador de clave al servidor Q 230. La cantidad de indicador de clave puede identificar el número de indicadores de claves generados por el agente de encriptado en 410. La cantidad de indicadores de claves puede tener la forma de un par de enteros (0, J). La cantidad del indicador de clave puede indicar al servidor 230 que se solicita su asistencia para generar valores de inicialización de claves FED.

Al recibir la cantidad del indicador de clave (por ejemplo, el par de enteros (0, J), el servidor Q 230 puede generar, basándose en U_r, $E(P_r)$, y su propia clave secreta v, los valores de la clave del servidor como números aleatorios independientes V_0, V_1, $\cdots$, V_J. Los valores de la clave del servidor pueden ser números aleatorios distribuidos uniformemente sobre {1,2, $\cdots$, N - 1}. El servidor 230 puede enviar V_0, V_1, $\cdots$, V_J de vuelta al agente 204 de encriptado. Basado en V_0, V_1, $\cdots$, V_J y X_0, X_1, $\cdots$, X_J, el agente 204 de encriptado puede generar J valores de inicialización de clave FED independientes $K_j = A(X_j, V_j)$, $j = 1,2, \cdots, J$.

En algunos casos, el agente 204 de encriptado también puede generar una primera clave de desencriptado de usuario basándose en la pluralidad de indicadores de claves (y, en algunas realizaciones, la pluralidad de valores de claves del servidor). El agente 204 de encriptado puede generar una primera clave de encriptado del usuario basada en la primera clave de desencriptado del usuario y transmitir la primera clave de encriptado del usuario al servidor 230. La primera clave de encriptado del usuario se puede almacenar en la primera cuenta.

Por ejemplo, el agente 204 de encriptado puede generar la clave de desencriptado del primer usuario 240 como $K_0 = A(X_0, V_0)$, donde la función $A(\cdot,\cdot)$ es de uno a uno y va desde {1, 2, $\cdots$, N - 1} a (1,2, $\cdots$, N - 1} dados, ya sea X_j o V_j. El agente 204 de encriptado puede enviar la clave pública $\gamma = \alpha^{K0}$ del primer usuario 240 al servidor Q 230, que a su vez guarda y registra γ junto con el hash de nombre de usuario y contraseña para el primer usuario.

En 430, la información inicial de clave basada en la pluralidad de valores de inicialización de claves puede almacenarse en la memoria no volátil del primer dispositivo 202a. En algunas realizaciones, el almacenamiento de la información de valores de inicialización de clave puede incluir el encriptado de la pluralidad de valores de inicialización de clave utilizando el primer código de verificación, y el almacenamiento de la pluralidad encriptada de

valores de inicialización de claves en la memoria no volátil del primer dispositivo 202a.

Por ejemplo, el agente 204 de encriptado puede usar el código de verificación C para encriptar la pluralidad de indicadores de claves (X_0, X_1, ⋯, X_J) y la pluralidad de valores de inicialización de clave (K_0, K_1, ⋯, K_J) en el primer dispositivo, los indicadores de claves encriptados $E_C(X_0, X_1, \cdots, X_J)$ y las claves de encriptado $E_C(K_0, K_1, \cdots, K_J)$ respectivamente. El agente 204 de encriptado puede entonces guardar $E_C(X_0,X_1, \cdots, X_J)$ y $E_C(K_0, K_1, \cdots, K_J)$ en la memoria no volátil del primer dispositivo 202a. El agente 204 de encriptado puede luego encriptar y desencriptar los archivos 208/210 bajo la administración del agente 204 de encriptado, incluso cuando la conexión de red entre el agente 204 de encriptado y el servidor Q 230 no está disponible cuando el primer usuario 240 está autentificado y verificado por el agente de encriptado 204 en el primer dispositivo 202a. Las realizaciones de ejemplo del encriptado y desencriptado de archivos se describirán con más detalle a continuación con referencia a las figuras 6A-6C.

En 435, una cadena de estado de clave para la primera cuenta se puede generar. La cadena de estado de clave puede incluir una porción del indicador de la clave del servidor generada en función de la pluralidad de indicadores de claves encriptados. En algunos casos, la cadena de estado de clave para la primera cuenta ya puede existir. Por ejemplo, como se mencionó anteriormente, la cadena de estado de clave puede inicializarse cuando el primer usuario 240 registra el agente 204 de encriptado en el primer dispositivo 202a con el servidor 230. En tales casos, la cadena de estado de clave para la primera cuenta puede generarse actualizando la cadena de estado de clave previamente almacenada.

En algunos casos, la porción del indicador de clave del servidor se puede generar en función de la pluralidad de indicadores de claves encriptados y la pluralidad de claves públicas del indicador de clave. Por ejemplo, al recibir ($\varepsilon_0,\mu_0,\varepsilon_1,\mu_1,\cdots,\varepsilon_J,\mu_J$), el servidor 230 puede actualizar la cadena de estado de clave de $S = 0$ a $S = S_0S_1\cdots S_{2(J+1)} = 1\varepsilon_0\mu_0\cdots\varepsilon_J\mu_J$. La cadena de estado de clave se puede actualizar agregando la pluralidad de indicadores de claves encriptados a la cadena de estado de clave. Cuando se utilizan claves públicas de indicadores de claves, también se pueden agregar a la cadena de estado de clave y asociarse con los indicadores de claves encriptados a los que corresponden. La porción del indicador de estado también se puede actualizar para identificar la porción del indicador de la clave del servidor actual.

En 440, la cadena de estado de clave se puede almacenar en la memoria no volátil del servidor 230. En general, la cadena de estado de clave se puede usar para sincronizar los valores de inicialización de claves en los dispositivos 202 asociados con el primer usuario 240.

Si la cadena de estado de clave recibida por el primer dispositivo 202a indica que la porción del indicador de clave del servidor ya se ha generado para la primera cuenta, el primer dispositivo 202a puede sincronizar los valores de inicialización de claves usando la cadena de estado de clave. Por ejemplo, cada dispositivo puede usar los valores almacenados en la porción del indicador de clave del servidor para generar la pluralidad de indicadores de claves y luego generar la pluralidad de valores de inicialización de clave en función de la pluralidad de indicadores de claves.

Por ejemplo, la cadena de estado de clave recibida $S = S_0S_1S_2\cdots S_{2(i+1)}$ puede tener una porción de indicador de estado como $S_0 = 1$, lo que indica que al menos otro agente 204 de encriptado en uno de esos L dispositivos 202 del primer usuario 240 ya se ha registrado en el servidor Q 230, se ha definido el código de verificación C y se ha generado el conjunto de valores de inicialización de claves FED $\{K_1, K_2, \cdots, K_i\}$, donde i es un múltiplo entero de J. En algunos casos, también se habrá generado la clave privada K_0 del primer usuario 240 (correspondiente a la clave pública $\gamma = \alpha^{K0}$ del primer usuario 240).

Por simplicidad, el proceso de sincronización de valores de inicialización de clave se describirá con referencia al segundo dispositivo 202b. Sin embargo, como se indicó anteriormente, los procesos descritos en este documento generalmente pueden ser realizados por un agente 204 de encriptado en cualquiera de los dispositivos 202 en el sistema 200. Además, el proceso se describe en el contexto de un usuario único que controla el primer dispositivo 202a y el segundo dispositivo 202b, pero se puede usar un proceso similar cuando diferentes usuarios controlan los dispositivos 202, como se describirá en detalle más abajo.

En general, antes de proporcionar el segundo dispositivo 202b con acceso a la cadena de estado de clave, el servidor 230 puede autentificar el primer usuario 240 en el segundo dispositivo 202b. En algunos casos, el servidor 230 puede transmitir la porción del indicador de estado de la cadena de estado de clave al agente 204 de encriptado en el segundo dispositivo 202b antes de requerir la autentificación. Por ejemplo, el servidor 230 puede recibir una solicitud de registro para el segundo dispositivo 202b. La solicitud de registro puede incluir el identificador del primer usuario de la primera cuenta y una contraseña de usuario putativo.

En respuesta, el servidor 230 puede comparar el identificador del primer usuario y contraseña de usuario putativo a los datos de la cuenta almacenados y datos de autentificación de cuenta. La porción del indicador de estado de la cadena de estado de clave se puede transmitir al segundo dispositivo 202b y puede indicar al agente 204 de encriptado en el segundo dispositivo 202b que se ha definido el código de verificación y que se requiere la autentificación del primer usuario 240. El servidor 230 también puede enviar una solicitud de autentificación al segundo dispositivo 202b junto con la porción del indicador de estado. El agente 204 de encriptado en el segundo dispositivo 202b puede solicitar al primer usuario 240 que ingrese el código de verificación C.

En 445, la información de autentificación putativa puede ser recibida en el segundo dispositivo 202b. La información de autentificación putativa puede ser un código de verificación putativo.

En 450, el agente 204 de encriptado en el segundo dispositivo 202b puede generar información de autentificación del servidor putativo basado en la información de autentificación putativa. El agente 204 de encriptado puede transmitir la información de autentificación del servidor putativo al servidor 230. Por ejemplo, el agente 204 de encriptado puede generar la información de autentificación putativa del servidor como un código de servidor encriptado putativo basado en el código de verificación putativo. El agente 204 de encriptado puede calcular $\hat{\beta}$ utilizando la misma función que la anterior y enviar este valor al servidor 230.

En 455, el servidor 230 puede comparar la información de autentificación del servidor putativo con la información de autentificación de cuentas. El servidor 230 puede comparar la información de autentificación putativa del servidor con el código de servidor encriptado almacenado en la información de autentificación de la cuenta de la primera cuenta. El servidor 230 puede comparar el valor recibido de $\hat{\beta}$ recibido del segundo dispositivo 202b con el valor almacenado de $\hat{\beta}$.

En algunos casos, el servidor 230 puede generar además información de autentificación de servidor putativo encriptada del servidor. Esto se puede usar cuando el código de servidor encriptado es un código de servidor encriptado adicional generado en el servidor antes del almacenamiento. Por ejemplo, el servidor 230 puede calcular $D(\hat{\beta})$ del código de servidor encriptado recibido utilizando la misma función D (es decir, con los valores V_{-1} y V_{-2}) utilizados para aleatorizar el código encriptado del servidor antes del almacenamiento. Esto se puede comparar con el valor almacenado de $D(\hat{\beta})$ guardado en la memoria no volátil del servidor 230 para determinar si el código de servidor encriptado putativo coincide con el código de servidor encriptado.

En 460, el servidor 230 puede proporcionar al segundo dispositivo 202b acceso a la cadena de estado de clave si y solo si la información de autentificación del servidor putativo corresponde a la información de autentificación de cuentas. En algunos casos, la información de autentificación de servidor putativo corresponde a la información de autentificación de cuenta si y solo si el código de servidor encriptado putativo coincide con el código de servidor encriptado. En realizaciones en las que los valores de inicialización de claves se generaron utilizando valores de clave de servidor, el servidor 230 también puede proporcionar al segundo dispositivo 202b acceso a los valores de claves del servidor si y solo si la información de autentificación de servidor putativo corresponde a la información de autentificación de cuenta. El servidor 230 puede transmitir los valores de la clave del servidor almacenados en la primera cuenta al agente 204 de encriptado en el segundo dispositivo 202b después de que el primer usuario 240 se autentifique en el segundo dispositivo 202b.

Si la autentificación es exitosa en 460, el agente 204 de encriptado en el segundo dispositivo 202b puede aceptar el código de verificación putativo recibido desde el primer usuario 240 como el código de verificación correcto. El agente 204 de encriptado puede calcular el código local encriptado y almacenar el código local encriptado en la memoria no volátil del segundo dispositivo 202b. Por ejemplo, el agente 204 de encriptado puede calcular el código local encriptado como se describe anteriormente (por ejemplo, $\beta = (\alpha^{C1}C_2, \alpha^{C2})$) y guardar β en la memoria no volátil del segundo dispositivo 202b de usuario.

En 465, el agente 204 de encriptado en el segundo dispositivo 202b puede determinar la pluralidad de indicadores de claves de la pluralidad de indicadores de claves de encriptado en la cadena de estado de clave utilizando la clave de desencriptado del segundo dispositivo. Por ejemplo, la pluralidad de indicadores de claves encriptadas puede encriptarse utilizando la clave de encriptado del segundo dispositivo. La clave de encriptado del segundo dispositivo corresponde a la clave de desencriptado del segundo dispositivo y se puede generar en función de la clave de desencriptado del segundo dispositivo.

Por ejemplo, la clave de encriptado del segundo dispositivo se puede generar en función del código de verificación. Del mismo modo, la clave de desencriptado del segundo dispositivo también se puede generar en función del código de verificación. En el escenario de un solo usuario, el código de verificación definido en el primer dispositivo 202a y el segundo dispositivo 202b puede ser el mismo. Por consiguiente, la clave de desencriptado del segundo dispositivo y la clave de encriptado del segundo dispositivo pueden generarse por separado. Por ejemplo, el primer dispositivo 202a puede generar la clave de encriptado del segundo dispositivo y encriptar la pluralidad de indicadores de claves utilizando la clave de encriptado del segundo dispositivo incluso antes de que el segundo dispositivo 202b se registre con el servidor 230. Cuando el segundo dispositivo 202b se registra con el servidor 230, el segundo dispositivo 202b puede generar la correspondiente clave de desencriptado del segundo dispositivo en función del código de verificación definido en el segundo dispositivo 202b.

En algunas realizaciones, como se describe a continuación, el segundo dispositivo 202b puede generar la clave de desencriptado del segundo dispositivo y transmitir la segunda clave de encriptado dispositivo al servidor 230. El primer dispositivo 202a puede generar la pluralidad de indicadores de claves encriptadas para el segundo dispositivo 202b utilizando la clave de encriptado del segundo dispositivo recibida desde el servidor 230. En algunos casos, esto puede ocurrir incluso después de que algunos archivos 208/210 se hayan transmitido desde el primer dispositivo 202a al segundo dispositivo 202b.

En algunas realizaciones, el agente 204 de encriptado en el segundo dispositivo 202b puede determinar la pluralidad de indicadores de claves de la porción de indicador de clave de la cadena de estado de clave mediante la determinación de X_j, j = 0,1,⋯,i, fuera de la cadena de estado de clave $S = S_0S_1S_2\cdots S_{2(i+1)}$ usando $X_{j-1} = S_{2j-1}S_{2j}^{-C_1}$, j = 1,2,⋯,i + 1. Los indicadores de claves determinados por el agente 204 de encriptado en el segundo dispositivo 202b pueden ser los mismos que la pluralidad de indicadores de claves generados en el primer dispositivo 202a. Esto permite que el agente 204 de encriptado en el segundo dispositivo 202b genere la misma pluralidad de valores de inicialización de clave que las generadas por el agente 204 de encriptado en el primer dispositivo 202a.

En 470, el agente 204 de encriptado en el segundo dispositivo 202b puede generar la pluralidad de valores de inicialización de clave basándose en la pluralidad de indicadores de claves. Para cada valor de inicialización de claves, el agente 204 de encriptado en el segundo dispositivo 202b puede generar la misma pluralidad de claves encriptadas independientes que el primer dispositivo 202a, sin que se proporcione ninguna clave, información de valor de inicialización de claves y claves de encriptado al segundo dispositivo 202b. La pluralidad de valores de inicialización de clave se puede generar en el segundo dispositivo 202b de la misma manera que se describió anteriormente para el primer dispositivo 202a. En algunas realizaciones, al igual que con el primer dispositivo 202a, el agente 204 de encriptado en el segundo dispositivo 202b puede generar la pluralidad de valores de inicialización de clave en función de la pluralidad de indicadores de claves y los valores de claves del servidor recibidos desde el servidor 230.

El agente 204 de encriptado en el segundo dispositivo 202b puede generar la pluralidad de valores de inicialización de claves de una manera similar a la descrita anteriormente para el primer dispositivo 202a en 425. Por ejemplo, con el código de verificación C y los números aleatorios X_j, j = 0,1, ⋯, i, disponibles, el agente 204 de encriptado en el segundo dispositivo 202b puede realizar las operaciones descritas en 425 con J reemplazado por i. Cuando la clave pública del primer usuario 240 ya se ha generado y almacenado en la primera cuenta, no es necesario que el segundo dispositivo 202b envíe la clave pública γ al servidor Q 230. El agente 204 de encriptado en el segundo dispositivo 202b puede completar el registro del segundo dispositivo 202b y generar los valores de inicialización de claves y la clave privada del primer usuario 240 (o la clave de desencriptado del segundo dispositivo) para el agente 204 de encriptado.

En algunas realizaciones, todos los cálculos que implican números en el procedimiento 400 descrito anteriormente puede llevarse a cabo en el campo finito *GF(N).* También podemos verificar que la pluralidad de valores de inicialización de claves FED y la clave privada del primer usuario 240 generadas y guardadas por el agente 204 de encriptado en el segundo dispositivo 202b son las mismas que las utilizadas por todos los agentes 204 de encriptado actualizados en otros dispositivos 202 registrados ante el nuevo agente de encriptado registrado (en el caso de un solo usuario). Por ejemplo, supongamos que $i = J$ en el párrafo [0192]. Se puede verificar que la pluralidad de indicadores de claves X_j, j = 0,1,2, ⋯, J, determinados por el agente 204 de encriptado del segundo dispositivo 202b en 465 son los mismos que los generados por el agente 204 de encriptado del primer dispositivo 202a en 410:

$$S_{2j-1}S_{2j}^{-C_1} = \hat{\beta}_2^{Y_{j-1}}X_{j-1}\alpha^{-Y_{j-1}C_1} = X_{j-1} \text{ for } j = 1,2,\cdots,J+1.$$

En 475, el agente 204 de encriptado en el segundo dispositivo 202b puede almacenar la información de valor de inicialización de clave basada en la pluralidad de valores de inicialización de claves en la memoria no volátil del segundo dispositivo 202b. El agente 204 de encriptado en el segundo dispositivo 202b puede almacenar la información de valor de inicialización de clave de la misma manera que se describió anteriormente para el primer dispositivo 202a, en 430.

En algunas realizaciones, las comunicaciones y los acuerdos entre el agente 204 de encriptado y el servidor Q 230 se pueden asumir como seguros. Además, el entero i en la descripción anterior puede ser un múltiplo entero de J y aumentar en J cada vez que cualquiera de los agentes de encriptado registrados 204 del primer usuario 240 solicite un nuevo conjunto de valores de inicialización de claves FED. Cuando cada K_j es largo, pero cada clave FED k es relativamente corta, J puede ser pequeño. Por ejemplo, uno puede seleccionar J = 1 cuando K_j tiene una longitud de 4096 bits y k tiene una longitud de 256 bits. En realizaciones de la descripción anterior, cuando los valores de servidor aleatorios independientes y distribuidos uniformemente y los valores de claves del servidor V_{-2}, V_{-1}, V_0, V_1, ⋯, V_i se generan por primera vez, pueden ser encriptados por el servidor Q 230 con su propia clave secreta v y luego guardado en la primera cuenta para el primer usuario 240 para otras posibles solicitudes de generación de valores de inicialización de claves y la clave privada del primer usuario 240 realizada posteriormente por los agentes de encriptado registrados del primer usuario 240.

En algunas realizaciones, si o no el agente 204 de encriptado en el primer dispositivo de usuario 202a es el primer agente de encriptado del primer usuario 240 registrado con el servidor Q 230, al final del proceso de CRKG, el agente 204 de encriptado registrado en el primer dispositivo 202a de usuario puede tener parte o toda la siguiente información almacenada en la memoria no volátil del primer dispositivo 202a de usuario:

el identificador de usuario o nombre de usuario *U*;

información de la contraseña del primer usuario, como el hash de contraseña $E(P)$;

el hash de PIN $E(R)$;

el código local encriptado, por ejemplo, $\beta = (\beta_1,\beta_2) = (\alpha^{C1}C_2, \alpha^{C2})$ basado en el código de verificación C;

la pluralidad de indicadores de claves encriptados (por ejemplo, números aleatorios $E_C(X_0, X_1, \cdots, X_i)$) e;

información de valores de inicialización de claves, como valores de inicialización de claves encriptadas $E_C(K_0, K_1, \cdots, K_i)$.

En consecuencia, en algunas realizaciones, el servidor Q 230 puede tener parte o toda la siguiente información almacenada en su memoria no volátil, por ejemplo, en la primera cuenta para el primer usuario 240:

el identificador del primer usuario, por ejemplo, los nombres de usuario de registro actual, antiguo e inicial U, U_o, y U_r;

la primera información de la contraseña del usuario, por ejemplo, los valores hash de la contraseña de registro actual, anterior e inicial $E(P)$, $E(P_o)$ y $E(P_r)$;

los identificadores de dispositivo de todos los dispositivos 202 del primer usuario 240 que tienen instalados en el mismo agente 204 de encriptado y están registrados con el servidor 230;

la clave de encriptado del segundo dispositivo del primer usuario 240, como la clave pública γ;

el código de servidor encriptado, o un código de servidor encriptado adicional basado en el código de verificación C, por ejemplo, $\hat{\beta}$ y/o $D(\hat{\beta})$; y

la cadena de estado de clave que incluye la porción del indicador de la clave del servidor y, en algunos casos, la porción del indicador de estado, por ejemplo, $S = S_0S_1S_2 \cdots S_{2(i+1)}$.

En algunas realizaciones, la información almacenada por un agente 204 de encriptado registrado en la memoria no volátil del primer dispositivo 202a de usuario y la información almacenada en la memoria no volátil del servidor 230 para el primer usuario 240 pueden satisfacer una o más de las siguientes propiedades:

$$U \text{ en Cliente } Q = U \text{ en Servidor } Q \quad (1)$$

$$E(P) \text{ en el Cliente } Q \equiv E(P) \text{ en el Servidor } Q \quad (2)$$

$$\beta \equiv D(\hat{\beta}) \quad (3)$$

$$X_{j-1} = S_{2j-1}S_{2j}^{-C_1}, \quad j = 1,2,\cdots,i+1 \quad (4)$$

$$K_0 \equiv \gamma \quad (5)$$

$$K_j = A(X_j, V_j), \quad j = 0,1,2,\cdots,i \quad (6)$$

En las propiedades (2), (3), y (5), ≡ indica que el lado derecho es consistente con el lado izquierdo. En general, estas seis propiedades consistentes pueden permanecer válidas hasta que el primer usuario 240 solicite algún cambio en el nombre de usuario, la contraseña, el código de verificación C y/o la generación de nuevos valores de inicialización de claves y las claves privadas y públicas del primer usuario 240 a través de servidor Q 230 u otro agente de encriptado registrado 204 en uno de esos L dispositivos 202 del primer usuario 240. Por lo tanto, al marcar una o más de estas propiedades consistentes, el agente 204 de encriptado registrado en el primer dispositivo 202a de usuario puede detectar si los cambios solicitados por el primer usuario 240 se han realizado a través de servidor Q 230 u otro agente de encriptado registrado en uno de esos L dispositivos 202 del primer usuario 240 (según sea el caso). En caso afirmativo, el agente 204 de encriptado registrado en el primer dispositivo 202a de usuario puede actualizar su información correspondiente para garantizar que estas propiedades consistentes vuelvan a ser válidas y, al hacerlo, también se sincronice con estos cambios. Para facilitar el proceso de detección, el agente 204 de encriptado en el primer dispositivo 202a de usuario, una vez registrado con éxito con el servidor Q 230, puede ser requerido para comparar su información almacenada localmente con la información respectiva en el servidor Q 230 durante su proceso de autentificación de intercambio con el servidor Q 230 siempre que quiera hablar con el servidor Q 230. La detección de cambios y la actualización de la información relacionada para obtener el agente de encriptado registrado 204 en el primer dispositivo de usuario 202a sincronizado con los cambios se analizará más adelante a través de los procedimientos de AVCC, VCU, ANKG y PNKG.

Debido a la dificultad de computar logaritmos discretos, el servidor 230 puede tener dificultades significativas para determinar el código de verificación del código de servidor encriptado, especialmente porque tanto la primera contraseña como la segunda contraseña pueden ser requeridas para determinar el código de verificación. Además, un código de servidor encriptado adicional, por ejemplo, generado como una aleatorización o un hash con clave de β, puede hacer que esta tarea sea aún más difícil (es decir, el servidor Q 230 puede tener dificultades para desencriptar el código de verificación C, en particular C_1, de $D(\beta)$). Por lo tanto, el servidor Q 230 puede no conocer el conjunto de valores de inicialización de claves FED y la clave privada del primer usuario 240 utilizadas por todos los agentes 204 de encriptado registrados del primer usuario 240.

En el sistema 200, la pluralidad de valores de inicialización de clave (y la clave privada del primer usuario 240 o la clave de desencriptado del dispositivo) solo puede ser expuesta a los agentes 204 de encriptado registrados en los dispositivos 202 de primer usuario 240, típicamente en un formato encriptado. La cadena de estado de clave S no puede exponer ninguna información sobre la pluralidad de valores de inicialización de claves FED, la clave privada del primer usuario 240 y/o el código de verificación C en un sentido de la teoría de la información. Del mismo modo, cada agente 204 de encriptado registrado puede tener dificultades para determinar también el código de verificación C del código encriptado local β. Como tal, en algunas realizaciones, incluso en los agentes 204 de encriptado registrados del primer usuario 240, la pluralidad de valores de inicialización de claves FED (y la clave privada de desencriptado del dispositivo o la clave de desencriptado del dispositivo del primer usuario 240) solo pueden estar disponibles para cada agente 204 de encriptado registrado después de que el primer usuario 240 proporcione información de autentificación putativa correspondiente al código de verificación correcto C para ese agente de encriptado.

La descripción anterior explica diversas realizaciones de cómo la pluralidad de indicadores de claves, la pluralidad de valores de inicialización de claves, y de este modo las claves de encriptado se pueden sincronizar en múltiples dispositivos que utilizan un servidor 230. Algunas realizaciones de ejemplo del encriptado y desencriptado de archivos que utilizan el sistema 200 se describirán ahora con referencia a las figuras 6A-6C. En la descripción de las figuras 6A-6C, las operaciones se describirán con referencia al primer dispositivo 202a y al segundo dispositivo 202b para mayor claridad. Sin embargo, en general, las operaciones realizadas por cada uno de estos dispositivos 202a y 202b pueden ser realizadas por cualquiera de la pluralidad de dispositivos 202 que tienen instalado un agente 204 de encriptado.

La figura 6 muestra un procedimiento 600 de ejemplo que puede ser utilizado por un agente 204 de encriptado para encriptar y almacenar un archivo proporcionado al primer dispositivo 202a.

En 605, un archivo para ser encriptado se proporciona al primer dispositivo 202a. El archivo que se va a encriptar se puede encriptar para su almacenamiento en el primer dispositivo 202a, para transmitirlo a un servidor en la nube para su almacenamiento, para transmitirlo a un segundo dispositivo 202b (por ejemplo, directamente al segundo dispositivo 202b a través de una red tal como la red 230 o a través del servidor en la nube, o de otro modo transmitido al segundo dispositivo) u otro dispositivo o plataforma de almacenamiento para almacenamiento encriptado, o desencriptado y revisión o edición.

En 610, una de las claves de encriptado se puede derivar de la información de valor de inicialización de clave almacenada en el primer dispositivo 202a usando información de clave. La clave de encriptado se puede derivar de varias maneras, como se describió anteriormente, como al seleccionar una clave de encriptado particular de un almacén de claves utilizando información de clave que indica un valor de índice de esa clave de encriptado particular, o generando/derivando la clave de encriptado particular de los valores de inicialización de claves correspondientes a la información de valores de inicialización de claves almacenada en el primer dispositivo 202a. La clave de encriptado puede seleccionarse aleatoriamente cuando el agente 204 de encriptado recibe una indicación del archivo que se va a encriptar.

En 615, el archivo se puede encriptar utilizando la clave de encriptado derivada. En algunos casos, la clave de encriptado derivada puede borrarse del primer dispositivo 202a después de encriptar el archivo.

En 620, el archivo encriptado puede entonces ser almacenado en la memoria no volátil del primer dispositivo 202a. La información de codificación utilizada para derivar el archivo encriptado también se puede almacenar con el archivo encriptado.

En algunos casos, el archivo encriptado no necesita almacenarse en el primer dispositivo 202a. Por ejemplo, el archivo encriptado puede transmitirse a otro dispositivo 202 o a un servidor en la nube junto con la información de codificación. En algunas realizaciones, el archivo y el archivo encriptado se pueden borrar del primer dispositivo 202a después de la transmisión.

La figura 6B muestra un procedimiento 630 de ejemplo que se puede usar para desencriptar un archivo encriptado de acuerdo con algunas realizaciones. En 635, el archivo encriptado y la información de codificación se reciben en el segundo dispositivo 202b.

En 640, el segundo dispositivo 202b puede derivar la clave de encriptado de la información inicial de clave almacenada en la memoria no volátil del segundo dispositivo 202b usando la información de generación de claves

recibida. En algunas realizaciones, la clave de encriptado puede ser derivada por el segundo dispositivo 202b de muchas maneras diferentes, como los procedimientos de ejemplo descritos anteriormente, dependiendo de la naturaleza de la información de valor de inicialización de clave almacenada en el segundo dispositivo 202b.

En 645, el segundo dispositivo 202b puede desencriptar el archivo encriptado usando la clave de encriptado derivada en 640. El usuario del segundo dispositivo 202b puede acceder entonces al archivo para su revisión y/o modificación o cualquiera de las otras acciones relacionadas con el archivo descritas anteriormente. En algunas realizaciones, el archivo desencriptado puede almacenarse en texto sin formato en la memoria volátil del segundo dispositivo 202b, y borrarse de la memoria volátil cuando el usuario ha completado las acciones deseadas. El archivo desencriptado también se puede almacenar en la memoria no volátil del segundo dispositivo 202b, después de encriptarse con una clave de encriptado derivada (la misma clave o una nueva), junto con la información de codificación.

La figura 6C muestra un procedimiento 650 de ejemplo para desencriptar el archivo encriptado cuando un usuario diferente tiene el control del segundo dispositivo 202b. En la descripción del procedimiento 650, el primer usuario 240 puede considerarse como una pluralidad de usuarios. La pluralidad de usuarios puede incluir un usuario administrativo que controla el primer dispositivo 202a y un segundo usuario que controla el segundo dispositivo 202b.

En general, el encriptado de un archivo antes del procedimiento 650 puede proceder de acuerdo con el procedimiento 600 descrito anteriormente. El primer dispositivo 202a puede derivar una de las claves de encriptado a partir de la información de valor de inicialización de clave utilizando la información de codificación, encriptar el archivo como un archivo encriptado utilizando el encriptado derivado y transmitir el archivo encriptado y la información de codificación al segundo dispositivo 202b. En algunas realizaciones del procedimiento 650, el archivo encriptado y la información de codificación pueden enviarse al segundo dispositivo 202b con una segunda autorización del usuario, que se explicará más adelante.

En 655, el archivo encriptado y la información de codificación se reciben en el segundo dispositivo 202b. Para desencriptar el archivo encriptado, un agente 204 de encriptado instalado en el segundo dispositivo 202b puede derivar la clave de encriptado a partir de la información de valor de inicialización de clave almacenada en la memoria no volátil del segundo dispositivo 202b y luego puede desencriptar el archivo encriptado utilizando la clave de encriptado derivada.

Sin embargo, en algunas realizaciones, el segundo dispositivo 202b puede recibir el archivo encriptado antes de la información de valor de inicialización de clave que se genera en el segundo dispositivo 202b. No obstante, las realizaciones de los sistemas y procedimientos descritos en este documento pueden permitir que el segundo dispositivo 202b desencripte los archivos encriptados incluso si se reciben antes de instalar un agente de encriptado y/o registrar el segundo dispositivo 202b en el servidor 230.

El usuario administrativo puede transmitir una autorización del segundo usuario al segundo usuario mediante la transmisión de un identificador del segundo usuario al servidor 230, por ejemplo, usando uno de los dispositivos asociados con el usuario de administración, o de otra manera. El servidor 230 puede generar una segunda autorización de servidor de usuario basada en el identificador del segundo usuario y una contraseña del segundo usuario. La contraseña del segundo usuario puede ser una contraseña temporal asignada por el servidor 230 a un usuario asociado con el identificador del segundo usuario (es decir, el segundo usuario). La autorización del servidor del segundo usuario generalmente puede indicar al servidor 230 que, al segundo usuario, una vez autentificado, se le puede proporcionar acceso a la primera cuenta.

El servidor 230 también puede generar una información de registro del segundo usuario basada en el identificador del segundo usuario y una contraseña del segundo usuario. La contraseña del segundo usuario puede ser utilizada por el segundo usuario cuando el segundo usuario registra el segundo dispositivo 202b con el servidor 230. La información de registro del segundo usuario se puede almacenar en la memoria no volátil del servidor 230.

En 660, el segundo usuario, tras recibir la autorización del servidor del segundo usuario, puede registrar el segundo dispositivo 202b con el servidor 230. En algunos casos, el segundo usuario puede instalar un agente 204 de encriptado en el segundo dispositivo 202b durante el proceso de registro (o puede que uno ya esté instalado). El segundo usuario puede registrarse con el servidor 230 en asociación con la primera cuenta de usuario, y también puede registrar el segundo dispositivo 202b con la primera cuenta de usuario. Esto puede permitir que el segundo dispositivo 202b (u otros dispositivos del segundo usuario) accedan a la cadena de estado de clave almacenada en la memoria no volátil del servidor 230 (después de autentificarse).

El segundo usuario puede entonces introducir una contraseña del segundo usuario putativo (es decir, el usuario intenta introducir la contraseña del segundo usuario) en el segundo dispositivo 202b. El agente 204 de encriptado del segundo dispositivo 202b puede generar información de registro del segundo usuario putativo basándose en el identificador del segundo usuario y la contraseña del segundo usuario putativo. La información de registro de segundo usuario putativo se puede transmitir al servidor 230.

El servidor 230 puede comparar la información de registro del segundo usuario putativo con la información de registro del segundo usuario almacenada. El servidor 230 puede autentificar el segundo dispositivo 202b para la primera cuenta solo si la información de registro del segundo usuario putativo corresponde a la información de registro del segundo usuario almacenada. El servidor 230 puede proporcionar al segundo dispositivo acceso a la cadena de estado de clave para la primera cuenta si, y solo si, el segundo dispositivo 202b se autentifica para la primera cuenta.

Sin embargo, si el segundo dispositivo 202b no se ha registrado previamente con la primera cuenta y/o la clave de encriptado del segundo dispositivo para el segundo dispositivo 202b no se conocía previamente en el primer dispositivo 202a, la cadena de estado clave almacenada en la primera cuenta puede no proporcionar información suficiente para que el segundo dispositivo 202b determine la pluralidad de indicadores de claves y, por lo tanto, la clave de encriptado. En algunas realizaciones, para evitar tales problemas, el primer dispositivo 202a puede generar una porción específica de usuario de la cadena de estado de clave para el segundo usuario.

En 665, el segundo dispositivo 202b puede generar una clave de encriptado del segundo dispositivo. El segundo dispositivo 202b puede generar una clave de desencriptado del segundo dispositivo y generar la clave de encriptado del segundo dispositivo basándose en la clave de desencriptado del segundo dispositivo. En algunas realizaciones, la clave de desencriptado del segundo dispositivo puede ser la clave privada del segundo usuario, también denominada clave privada específica del usuario (que se puede generar de manera similar a la clave privada K_0 como se mencionó anteriormente), y la clave de encriptado del segundo dispositivo puede ser la clave pública del segundo usuario, también conocida como clave pública específica del usuario (que se puede generar de manera similar a la clave pública γ mencionada anteriormente). El segundo dispositivo 202b puede transmitir la clave de encriptado del segundo dispositivo al servidor 230.

El servidor 230 puede almacenar la clave de encriptado del segundo dispositivo para el segundo dispositivo 202b en una segunda cuenta de usuario para el segundo usuario. El servidor 230 también puede proporcionar la clave de encriptado del segundo dispositivo para el segundo dispositivo 202b al primer dispositivo 202a para ayudar al agente 204 de encriptado en el primer dispositivo 202a a generar la pluralidad de indicadores de claves encriptados. Por ejemplo, el servidor 230 puede almacenar la clave de encriptado del segundo dispositivo para el segundo dispositivo 202b en los datos de la cuenta de la primera cuenta como una clave pública específica del usuario para el segundo usuario.

En 670, el primer dispositivo 202a puede generar una pluralidad de indicadores de claves encriptados a partir de la pluralidad de indicadores de claves almacenados en el mismo usando la clave de encriptado del segundo dispositivo para el segundo dispositivo 202b recibido desde el servidor 230. Por ejemplo, el primer dispositivo 202a puede generar la pluralidad de indicadores de claves encriptados para incluir una pluralidad de indicadores de claves encriptados específicos del usuario utilizando la clave pública específica del usuario para el segundo dispositivo 202b.

El primer dispositivo 202a puede transmitir la pluralidad de indicadores de claves encriptados específicos del usuario para el segundo usuario al servidor 230. El servidor 230 puede generar una porción de cadena específica del usuario (para el segundo usuario) en la cadena de estado de clave (de la primera cuenta) en función de la pluralidad de indicadores de claves encriptados específicos del usuario para el segundo usuario. El servidor 230 puede autentificar el segundo dispositivo 202b y autentificar al segundo usuario antes de proporcionar al agente 204 de encriptado en el segundo dispositivo 202b con acceso a la cadena de estado de clave para la primera cuenta. El servidor 230 puede proporcionar al segundo dispositivo 202b acceso a la parte específica del usuario de la cadena de estado de clave para el segundo usuario (almacenada en la primera cuenta) si y solo si el segundo dispositivo 202b está autentificado para la primera cuenta.

En 675, una vez que el segundo dispositivo 202b está registrado y autentificado para la primera cuenta (y el segundo usuario ha sido verificado/autentificado en el segundo dispositivo 202b, por ejemplo, usando un código de verificación tal como se describe más arriba) el segundo dispositivo 202b puede recibir la cadena de estado clave (o la segunda parte específica del usuario de la cadena de estado clave).

En 680, el agente 204 de encriptado en el segundo dispositivo 202b puede entonces derivar la información inicial de clave de la segunda porción específica del usuario de la cadena de estado de clave utilizando la segunda clave de desencriptado dispositivo, generalmente de la misma manera que la descrita anteriormente. El agente 204 de encriptado en el segundo dispositivo 202b puede luego derivar la clave de encriptado a partir de la información de valor de inicialización de clave utilizando la información de clave recibida, y desencriptar el archivo encriptado.

Procedimiento de CRKG con recuperación de código de verificación

En algunas realizaciones de CRKG descrito anteriormente, si el primer usuario 240 se olvida de su código de verificación *C,* el sistema 200 puede no ser capaz de recuperarlo (o puede ser computacionalmente imposible de recuperar). En algunos casos, esta puede ser una propiedad deseable para garantizar la seguridad del sistema 200. Sin embargo, esto puede causar problemas al primer usuario 240 si se olvida el código de verificación *C.*

En algunas realizaciones descritas en esta subsección, las realizaciones del proceso de CRKG descrito anteriormente se puede modificar ligeramente para permitir la recuperación de un código de verificación *C* perdido u olvidado. Algunas realizaciones permiten que el código de verificación sea recuperado a través de la colaboración entre el primer usuario 240, uno o más agentes 204 de encriptado en los dispositivos 202, y el servidor Q 230 o un servidor de proveedor de servicio remoto. Estas realizaciones todavía pueden mantener el mismo nivel de seguridad que antes.

En algunas realizaciones, además del servidor Q 230, los agentes 204 de encriptado, y el primer usuario 240, un servidor de proveedor de servicio remoto separado también se puede utilizar. El servidor del proveedor de servicio remoto puede estar asociado con el proveedor de servicio que proporciona el sistema 200. Sin embargo, en otras realizaciones, puede que no sea necesario utilizar un servidor adicional. Aunque, por simplicidad, las realizaciones específicas del sistema y el procedimiento de recuperación del código de verificación se describen a continuación en combinación con el sistema 200 de sincronización automática, los sistemas y procedimientos del código de verificación descritos en este documento también se pueden usar en otros sistemas o procedimientos para recuperar un código de verificación definido por el usuario en un dispositivo controlado por el usuario.

La figura 9 muestra un procedimiento de ejemplo para recuperar un código de verificación definido por un usuario en un agente de encriptado instalado en al menos un dispositivo controlado por el usuario. Cada dispositivo puede configurarse para la comunicación con un servidor de proveedor de servicio remoto. Para mayor claridad, la descripción de las figuras 9 y 10 que sigue se describirá con referencia al primer usuario 240 que es un solo usuario en control de la pluralidad de dispositivos 202. Además, en la descripción que sigue, el servidor del proveedor de servicio remoto puede estar separado del servidor 230, o puede ser el mismo servidor 230.

En 905, para cada dispositivo, el agente 204 de encriptado puede generar un código de recuperación local basado en el código de verificación y un código de recuperación remoto basado en el código de verificación. El código de verificación se puede determinar a partir de una combinación del código de recuperación local y el código de recuperación remoto, pero no se puede determinar solo con el código de recuperación remoto.

Para cada dispositivo 202, el agente 204 de encriptado instalado en ese dispositivo puede generar una pluralidad de contraseñas a partir del código de verificación. La pluralidad de contraseñas se puede generar de tal manera que el código de verificación sea determinable a partir de todas las contraseñas en la pluralidad de contraseñas, pero no es determinable a partir de menos de todas las contraseñas. El agente 204 de encriptado puede generar el código de recuperación local utilizando la pluralidad de contraseñas. El código de recuperación local puede incluir un valor de función unidireccional generado a partir del código de verificación. Por ejemplo, el código de recuperación local puede ser el código local encriptado descrito anteriormente. Por lo tanto, en algunas realizaciones, el agente 204 de encriptado puede generar el código de recuperación local calculando $\beta = \varphi(C)$, es decir, $\beta = (\beta_1,\beta_2) = (\alpha^{C1}C_2,\alpha^{C2})$. El agente 204 de encriptado también puede generar el código de recuperación remoto utilizando la pluralidad de contraseñas.

Ahora se describirá un procedimiento de ejemplo para generar el código de recuperación local y el código de recuperación remoto con referencia a la figura 10. El procedimiento 1000 es un ejemplo de un procedimiento para generar un código de recuperación local y un código de recuperación remoto de acuerdo con una realización.

En 1005, el agente 204 de encriptado puede generar una primera contraseña y una segunda contraseña basadas en el código de verificación. La pluralidad de contraseñas mencionadas anteriormente puede incluir la primera contraseña y la segunda contraseña. El agente de encriptado puede generar la primera y la segunda contraseñas de tal manera que el código de verificación se puede determinar a partir de una combinación de la primera contraseña y la segunda contraseña, pero no se puede determinar a partir de la primera contraseña y la segunda contraseña solamente.

En el ejemplo específico dado anteriormente, el agente 204 de encriptado puede convertir el código de verificación *C* en una primera contraseña C_1 y una segunda contraseña C_2 a través de $f(C) = (C_1, C_2)$. En algunas realizaciones, la conversión se puede realizar a través de una función de uno a uno *f de* modo que tanto C_1 como C_2 se vean como números aleatorios de $GF(N)$.

En 1010, el agente 204 de encriptado puede generar un primer valor de recuperación local de la primera contraseña y la segunda contraseña. El primer valor de recuperación local se puede generar de tal manera que ni la primera contraseña ni la segunda contraseña sean determinables solo a partir del primer valor de recuperación local. Por ejemplo, el primer valor de recuperación local puede generarse multiplicando la segunda contraseña (por ejemplo, C_2) con el número entero α (donde α es un número entero mayor que 1) elevado a la potencia de la primera contraseña (por ejemplo, α^{C1}). Por lo tanto, en algunas realizaciones, el primer valor de recuperación local se puede generar como $\beta_1 = \alpha^{C1}C_2$.

En 1015, el agente 204 de encriptado puede generar un segundo valor de recuperación local de la segunda contraseña. La segunda contraseña puede ser un logaritmo discreto del segundo valor de recuperación local con una base α. Por lo tanto, aunque en algunas realizaciones la segunda contraseña se puede determinar a partir del segundo valor de recuperación, la segunda contraseña puede ser computacionalmente imposible de determinar

como resultado de la dificultad asociada con el cálculo de logaritmos discretos. Por ejemplo, el segundo valor de recuperación local se puede determinar como $\beta_2 = \alpha^{C2}$.

En 1020, el agente 204 de encriptado puede determinar el código de recuperación local desde el primer valor de recuperación local y el segundo valor de recuperación local. Por ejemplo, el código de recuperación local puede incluir el primer valor de recuperación local y el segundo valor de recuperación local.

En 1025, el agente 204 de encriptado puede generar el código de recuperación remoto basado en la primera contraseña y la segunda contraseña. El código de recuperación remoto se puede generar de tal manera que ni la primera contraseña ni la segunda contraseña sean determinables solo a partir del código de recuperación remoto. En algunas realizaciones, el código de recuperación remoto puede generarse multiplicando α, elevado a la potencia de la segunda contraseña, con la primera contraseña (por ejemplo, $\alpha^{C2}C_1$).

Con referencia nuevamente a la figura 9, en 910 el agente 204 de encriptado puede determinar la información del código de recuperación remoto basándose en el código de recuperación remoto. El agente 204 de encriptado puede transmitir la información del código de recuperación remoto al servidor del proveedor de servicio remoto y borrar el código de recuperación remoto del dispositivo.

En algunos casos, la información del código de recuperación remoto puede ser una versión modificada y/o encriptada del código de recuperación remoto generado en 905. En algunas realizaciones, el proveedor de servicio remoto puede generar una clave de proveedor de servicio privado y una clave de proveedor de servicio público basada en la clave de proveedor de servicio privado. El servidor del proveedor de servicio puede almacenar la clave privada del proveedor de servicio en la memoria no volátil del servidor del proveedor de servicio. El proveedor de servicio también puede proporcionar la clave del proveedor de servicio públicos a cada uno de los dispositivos 202. Por ejemplo, el servidor del proveedor de servicio puede generar la clave de proveedor de servicio privado al elegir un número aleatorio secreto λ de {1,2, ⋯, N - 1} y hacer pública una clave de proveedor de servicio público α^{λ}.

El agente 204 de encriptado sobre el primer dispositivo 202a puede entonces determinar la información remota de código de recuperación mediante la generación de un código de recuperación remoto encriptado basado en el código de recuperación a distancia utilizando la clave de proveedor de servicio público. El agente 204 de encriptado puede transmitir el código de recuperación remoto encriptado al proveedor de servicio remoto. Por ejemplo, el agente 204 de encriptado puede calcular $\hat{\beta}_0 = (\alpha^{\lambda Y}\alpha^{C2}C_1, \alpha^{Y})$, utilizando la clave del proveedor de servicio público y un número aleatorio independiente Y de {1,2, ⋯, N - 1}. El agente 204 de encriptado puede enviar $\hat{\beta}_0$ al servidor Q 230, que a su vez puede pasar $\hat{\beta}_0$ junto con el identificador del primer usuario al servidor del proveedor de servicio remoto. En algunas realizaciones, el servidor 230 puede borrar la información del código de recuperación remoto después de transmitir la información del código de recuperación remoto al servidor del proveedor de servicio remoto que indica que no hay una marca en $\hat{\beta}_0$ en el servidor Q 230. En otros casos, el agente 204 de encriptado puede enviar la información del código de recuperación remoto al servidor del proveedor de servicio remoto directamente o a través de un canal lateral.

En algunas realizaciones, la información de código de recuperación remoto puede ser un código de recuperación específica del dispositivo. El agente 204 de encriptado puede generar aleatoriamente un modificador de código remoto específico del dispositivo. El agente 204 de encriptado puede luego modificar el código de recuperación remoto utilizando el modificador de código remoto específico del dispositivo para generar la información del código de recuperación remoto. El agente de encriptado puede almacenar el código remoto específico del dispositivo modificado en la memoria no volátil del primer dispositivo 202a. En algunos casos, el agente 204 de encriptado también puede encriptar el código de recuperación remoto modificado, por ejemplo, utilizando el proceso descrito anteriormente.

Por ejemplo, el agente 204 de encriptado puede aleatorizar aún más el código de recuperación remoto $\alpha^{C2}C_1$ reemplazando $\alpha^{C2}C_1$ con $D(\alpha^{C2}C_1, X)$ en β_0. El agente 204 de encriptado puede determinar el modificador de código X específico del dispositivo como un número aleatorio de {1,2, ⋯, N-1}. El modificador X del código específico del dispositivo puede ser generado independientemente por cada agente 204 de encriptado y guardado en la memoria no volátil del dispositivo 202 respectivo.

En algunas realizaciones, cuando el primer usuario 240 tiene el control de una pluralidad de dispositivos, el servidor del proveedor de servicio puede mantener varias versiones de códigos de recuperación remota específicos del dispositivo (por ejemplo, versiones múltiples de β_0), una de cada agente 204 de encriptado del primer usuario 240. El servidor del proveedor de servicio puede almacenar un identificador de dispositivo para la información del código de recuperación remoto para cada dispositivo, donde el identificador del dispositivo identifica el dispositivo 202 correspondiente a esa información del código de recuperación remoto.

Debido a la dificultad de calcular logaritmos discretos, el servidor Q 230 y el servidor del proveedor de servicio solos o juntos pueden tener dificultades para determinar el código de verificación C, y en particular la primera contraseña de recuperación C_1, desde el código de servidor encriptado (por ejemplo, $D(\hat{\beta})$) y la información del código de recuperación remoto (por ejemplo, $\hat{\beta}_0$). Como tal, el servidor Q 230, el agente 204 de encriptado y el servidor del proveedor de servicio pueden no ser capaces de recuperar C (sin recursos significativos, lo que hace que la

recuperación sea computacionalmente factible en muchas realizaciones). En algunas realizaciones, el código de verificación *C* se puede recuperar mediante la colaboración entre el agente 204 de encriptado en un dispositivo de recuperación asociado con el primer usuario 240, el servidor del proveedor de servicio y el primer usuario 240.

En 915, el agente 204 de encriptado puede almacenar el código de recuperación local en una memoria no volátil del primer dispositivo 202a. En general, el agente 204 de encriptado en cada dispositivo puede almacenar el código de recuperación local en la memoria no volátil de ese dispositivo. Además, como se mencionó anteriormente, cada dispositivo también puede almacenar el modificador de código remoto específico del dispositivo para ese dispositivo en la memoria no volátil de ese dispositivo.

En 920, el servidor del proveedor de servicio puede recibir una solicitud de recuperación de código. El servidor del proveedor de servicio también puede autentificar al primer usuario. Un procedimiento de ejemplo que se puede usar en algunas realizaciones para autentificar al usuario se describirá en detalle más adelante con referencia a la figura 11. En respuesta a la recepción de la solicitud de recuperación de código, y solo después de autentificar al usuario, el servidor del proveedor de servicio puede determinar la información del código de recuperación del servidor basándose en la información del código de recuperación remoto almacenado en la memoria no volátil del servidor del proveedor de servicio.

En algunas realizaciones, el primer usuario 240 puede enviar una clave de usuario temporal al servidor del proveedor de servicio. Por ejemplo, el primer usuario 240 puede enviar una clave temporal, digamos *K*, al proveedor de servicio del sistema 200. El proveedor de servicio puede generar la información del código de recuperación del servidor mediante el encriptado de la información del código de recuperación remoto mediante la clave temporal. Por ejemplo, el servidor del proveedor de servicio puede usar *K* para encriptar $\alpha^{C2}C_1$ en $E_K(\alpha^{C2}C_1)$, y luego envía $E_K(\alpha^{C2}C_1)$ al primer usuario 240 en un canal lateral o a través del canal entre los agentes 204 de encriptado y el servidor Q 230.

Como se ha mencionado anteriormente, en algunas realizaciones, la información remota código de recuperación es un código de recuperación remoto encriptado generado a partir del código de recuperación a distancia utilizando la clave de proveedor de servicio público. En tales realizaciones, el servidor de proveedor de servicio puede desencriptar el código de recuperación remoto encriptado (por ejemplo, β_0) almacenado para la recuperación utilizando la clave del proveedor de servicio privado (por ejemplo, *λ).* El servidor del proveedor de servicio puede luego determinar la información del código de recuperación del servidor basándose en el código de recuperación remoto desencriptado.

Como se mencionó anteriormente, en algunas realizaciones, la información del código de recuperación remoto puede incluir un código de recuperación remoto específico del dispositivo modificado. La solicitud de recuperación de código recibida en el servidor del proveedor de servicio puede incluir un identificador de dispositivo de recuperación que identifique el dispositivo de recuperación. El servidor del proveedor de servicio remoto puede determinar la información del código de recuperación del servidor para el dispositivo de recuperación identificando la información del código de recuperación remoto correspondiente al dispositivo de recuperación utilizando el identificador de dispositivo de recuperación recibido y los identificadores de dispositivo almacenados. El servidor del proveedor de servicio puede luego determinar la información del código de recuperación del servidor a partir de la información del código de recuperación del identificador. Como será evidente para un lector experto, en algunas realizaciones, las características de los diversos ejemplos para generar la información del código de recuperación remoto y la información del código de recuperación del servidor se pueden usar en combinación entre sí o con otros procedimientos para la transmisión segura de datos.

En 925, el servidor 230 puede transmitir la información de código de recuperación de servidor para el primer usuario 240. Como se mencionó anteriormente, la información del código de recuperación del servidor se puede transmitir al primer usuario 240 de varias maneras, como a través de un canal lateral o directamente al dispositivo de recuperación (por ejemplo, a través del servidor 230). En algunas realizaciones, el primer usuario 240 puede proporcionar la información del código de recuperación del servidor a cualquiera de los dispositivos 202 y usar ese dispositivo como dispositivo de recuperación. Por ejemplo, el primer usuario 240 puede ingresar la información del código del servidor $E_K(\alpha^{C2}C_1)$ y la clave temporal *K* a cualquiera de sus agentes 204 de encriptado registrados. En otras realizaciones, por ejemplo, aquellas que utilizan información del código de recuperación remoto específico del dispositivo, la información del código de recuperación del servidor solo se puede proporcionar al dispositivo de recuperación asociado con la información del código de recuperación remoto específico del dispositivo en función de la cual se generó la información del código de recuperación del servidor.

En 930, el agente 204 de encriptado en un dispositivo 202 de recuperación puede recibir la información del código de recuperación del servidor. El agente 204 de encriptado puede determinar el código de recuperación remoto a partir de la información del código de recuperación del servidor y determinar el código de verificación utilizando el código de recuperación remoto y el código de recuperación local.

En algunos casos, el agente 204 de encriptado puede determinar el código de recuperación a distancia de la información de código de recuperación del servidor utilizando el dispositivo modificador de código remoto específico almacenado en la memoria no volátil para el dispositivo de recuperación. En algunas de tales realizaciones, el

agente 204 de encriptado en el dispositivo de recuperación debe ser el que contiene el número aleatorio correspondiente *X*.

Por ejemplo, el agente 204 de encriptado puede calcular (C_1, C_2) a partir del código de recuperación remoto (por ejemplo, $\alpha^{C2}C_1$) y el código de recuperación local ($\beta = (\beta_1,\beta_2) = (\alpha^{C1}C_2,\alpha^{C2})$). El agente 204 de encriptado puede determinar un código de recuperación remoto inverso (por ejemplo, α^{-C2}) a partir del segundo valor de recuperación local (por ejemplo, α^{C2}). El agente 204 de encriptado puede entonces determinar la primera contraseña (C_1) utilizando el código de recuperación remoto inverso y el código de recuperación remoto. Multiplicar el código de recuperación remoto inverso (por ejemplo, α^{-C2}) con el código de recuperación remoto (por ejemplo, $\alpha^{C2}C_1$) puede proporcionar la primera contraseña (C_1). El agente 204 de encriptado puede entonces determinar la segunda contraseña utilizando la primera contraseña y el primer valor de recuperación local. Por ejemplo, el agente 204 de encriptado puede determinar α^{-C1} y determinar la segunda contraseña (C_2) multiplicando α^{-C1} y $\alpha^{C1}C_2$. El agente 204 de encriptado puede entonces determinar el código de verificación usando la primera contraseña y la segunda contraseña.

En 935, el agente 204 de encriptado puede mostrar el código de comprobación en el dispositivo 202 de recuperación. El primer usuario 240 puede usar el código de verificación para acceder a los archivos almacenados por el agente de encriptado en cualquiera de los dispositivos 202 asociados con el primer usuario 240.

En algunas realizaciones, el agente 204 de encriptado puede validar el código de recuperación remoto recibido del servidor del proveedor de servicio remoto. Esto puede ser útil si el primer usuario 240 no puede usar el código de verificación determinado en 930 para acceder y/o desencriptar archivos almacenados en el agente 204 de encriptado en los dispositivos 202. Por ejemplo, esto puede ocurrir si el proveedor de servicio remoto modifica o corrompe el código de recuperación remoto. Esto puede permitir que el primer usuario 240 demuestre que la pérdida efectiva de datos que se produce porque los archivos no se pueden desencriptar es el resultado de un fallo en la parte del servidor del proveedor de servicio. Cualquier modificación en el código de recuperación remoto cambiará el valor de la primera contraseña (C_1) determinada en 930 y, a su vez, el valor de la segunda contraseña (C_2), que luego será inconsistente con el segundo valor de recuperación local α^{C2} almacenado localmente.

El agente 204 de encriptado puede generar un código de recuperación local putativo usando el código de recuperación a distancia determinada a partir de la información de código de recuperación de servidor y el código de recuperación local. El agente 204 de encriptado puede generar el código de recuperación local putativo determinando un código de verificación putativo utilizando los procedimientos de ejemplo descritos anteriormente en 930. El agente 204 de encriptado puede luego calcular un código de recuperación local putativo a partir del código de verificación putativo utilizando el mismo procedimiento que se utilizó para generar el código de recuperación local almacenado a partir del código de verificación.

El agente 204 de encriptado puede comparar el código de recuperación local putativo con el código de recuperación local almacenado en la memoria no volátil del dispositivo de recuperación. El agente 204 de encriptado puede validar el código de recuperación remoto determinado a partir de la información del código de recuperación del servidor si y solo si el código de recuperación local putativo coincide con el código de recuperación local almacenado.

En algunas realizaciones, el agente 204 de encriptado puede generar un segundo valor de recuperación local putativo usando el código de recuperación a distancia determinada a partir de la información de código de recuperación de servidor y el código de recuperación local. El agente 204 de encriptado puede comparar el segundo valor de recuperación local putativo con el segundo valor de recuperación local almacenado en la memoria no volátil del dispositivo de recuperación. El agente 204 de encriptado puede validar el código de recuperación remoto determinado a partir de la información del código de recuperación del servidor si y solo si el segundo valor de recuperación local putativo coincide con el segundo valor de recuperación local almacenado.

En algunas realizaciones, la autentificación del primer usuario 240 (o cualquier otro usuario) se puede lograr de forma remota utilizando el procedimiento 1100 que se muestra en la figura 11. El procedimiento 1100 es un ejemplo de un procedimiento que se puede usar para autentificar a un usuario de forma remota.

En 1105, el servidor 230 guarda la información de autentificación del usuario para el primer usuario 240 en la memoria no volátil del servidor de proveedor de servicio. La información de autentificación del usuario puede incluir información de identificación biométrica del primer usuario 240. El primer usuario 240 puede proporcionar la información de identificación biométrica a través del agente 204 de encriptado en uno de los dispositivos 202 controlados por el primer usuario 240. La información de identificación biométrica se puede proporcionar al proveedor de servicio del sistema 200 a través del agente 204 de encriptado y el servidor Q 230 o a través de un canal lateral.

En algunas realizaciones, la información de identificación biométrica del usuario puede incluir al menos una grabación de audio del usuario, una grabación de video del usuario, una imagen del usuario, una huella digital, una huella dactilar, una exploración retiniana. En algunos casos, la información de identificación biométrica del usuario 240 puede incluir una pluralidad de tipos de identificación biométrica. En algunos casos, la pluralidad de tipos de

identificación biométrica puede incluir una grabación de audio del usuario y al menos una imagen de la cara del usuario y un video de la cara del usuario.

Por ejemplo, durante el procedimiento de CRKG, se le puede pedir al primer usuario 240 que proporcione una verdadera foto de frente o videoclip del primer usuario 240. También se le puede pedir al primer usuario 240 que proporcione un clip de audio que grabe la voz del primer usuario 240. El clip de audio puede incluir una grabación de la voz del primer usuario 240 para una pluralidad de contraseñas de autentificación. Por ejemplo, las contraseñas de autentificación pueden ser los números del 0 al 9.

En 1110, el servidor del proveedor de servicio puede recibir una solicitud de recuperación de código de verificación. La solicitud de código de verificación puede ser similar a la solicitud de recuperación de código descrita anteriormente en 920 del procedimiento 900.

En 1115, el servidor de proveedor de servicio puede generar una secuencia de autentificación de usuario. El servidor del proveedor de servicio puede generar la secuencia de autentificación del usuario de manera aleatoria en respuesta a la recepción de la solicitud de recuperación del código de verificación. El servidor del proveedor de servicio también puede almacenar la secuencia de autentificación del usuario en la información de autentificación del usuario para el usuario. El servidor del proveedor de servicio también puede determinar un período de validez de secuencia.

En algunas realizaciones, al recibir la petición del primer usuario 240 para la recuperación de código de verificación *C,* el servidor de proveedor de servicio, a través de uno de los agentes 204 de encriptado del primer usuario 240, generar una secuencia de autentificación de usuario de manera aleatoria para el primer usuario 240.

Por ejemplo, la secuencia de autentificación del usuario puede incluir una secuencia aleatoria de contraseñas generadas en función de la pluralidad de contraseñas de autentificación almacenadas en 1105. El primer usuario 140 puede entonces ser requerido para realizar la secuencia de autentificación del usuario diciendo un código de audio verbal. En otros ejemplos, la secuencia de autentificación del usuario puede incluir una secuencia de orientaciones de los dedos, y el usuario debe realizar la secuencia de autentificación del usuario utilizando huellas digitales y orientaciones de los dedos correspondientes a la secuencia de autentificación del usuario. Otro ejemplo de secuencia de autentificación de usuario puede estar relacionada con el ritmo típico de pulsación de teclas del usuario, y el usuario debe realizar la secuencia de autentificación de usuario escribiendo una contraseña generada aleatoriamente. Otro ejemplo de secuencia de autentificación del usuario puede estar relacionada con la imagen del usuario, y el usuario debe realizar la secuencia de autentificación del usuario agitando sus brazos para deletrear una contraseña generada aleatoriamente en semáforo. Otro ejemplo de secuencia de autentificación de usuario puede incluir una secuencia de parpadeos generada aleatoriamente que el primer usuario 240 podría realizar mientras se realizan exploraciones de la retina.

En 1120, antes de transmitir el código de recuperación de servidor al primer usuario 240, el servidor del proveedor de servicio remoto puede transmitir una solicitud de autorización al dispositivo de recuperación. La solicitud de autorización puede incluir la secuencia de autentificación de usuario generada en 1115. Por ejemplo, la solicitud de autorización puede hacer que el primer usuario 240 use un agente 204 de encriptado para tomar un video corto y autofoto mientras habla en voz alta la secuencia aleatoria de las contraseñas.

En 1125, el dispositivo de recuperación puede recibir información de autentificación putativa. El dispositivo de recuperación puede transmitir la información de autentificación putativa al servidor del proveedor de servicio remoto. La información de autentificación putativa puede comprender un rendimiento de la secuencia de autentificación del usuario, por parte del usuario putativo. La información de autentificación putativa también puede incluir información de identificación biométrica putativa que identifica al usuario putativo como resultado del rendimiento. Por ejemplo, la información de autentificación putativa puede incluir una grabación de video de la cara de un usuario putativo coincidente con una grabación de audio del usuario putativo hablando un código de audio putativo. En otras palabras, el usuario puede tomar un video corto autofoto mientras habla en voz alta la secuencia aleatoria de contraseñas que utilizan el dispositivo de recuperación y luego transmite el video al servidor del proveedor de servicio remoto. En otras realizaciones, la información de autentificación putativa puede incluir un videoclip propio corto del usuario que agita los brazos para deletrear una contraseña generada de manera aleatoria en el semáforo. Otro ejemplo de información de autentificación putativa puede incluir la sincronización de las pulsaciones de teclas del usuario a medida que el usuario escribe una contraseña generada aleatoriamente.

En 1130, el servidor del proveedor de servicio remoto puede comparar la información de autentificación putativa con la información de autentificación del usuario almacenada en la memoria no volátil del servidor del proveedor de servicio. La información de autentificación putativa puede corresponder a la información de autentificación de usuario almacenada solo si la información de autentificación putativa incluye la secuencia de autentificación de usuario. El servidor del proveedor de servicio puede transmitir la información del código de recuperación del servidor al primer usuario 240 si y solo si la información de autentificación putativa corresponde a la información de autentificación del usuario almacenada.

En una realización específica descrita anteriormente, la información de autentificación putativa puede corresponder a la información de autentificación del usuario almacenada si y solo si: la cara del usuario putativo corresponde a al menos una de la imagen de la cara del usuario y el video de la cara del usuario; la grabación de audio del usuario putativo corresponde a la grabación de audio del usuario; y el código de audio putativo corresponde al código de audio verbal. Por ejemplo, si el clip de audio/video cargado se corresponde con el código aleatorio y el clip de audio/foto y video almacenado en el servidor del proveedor de servicio para el primer usuario 240, el primer usuario 240 puede considerarse autentificado.

En algunas realizaciones, el servidor de proveedor de servicio puede también generar un período de secuencia de validez para la secuencia de autentificación de usuario. El período de validez de secuencia puede proporcionarse al primer usuario 240 en la solicitud de autorización. La información de autentificación putativa puede corresponder a la información de autentificación de usuario almacenada solo si la información de autentificación putativa que comprende la secuencia de autentificación de usuario se recibe dentro del período de validez de secuencia. En efecto, el período de validez de la secuencia puede corresponder a un tiempo de espera para la secuencia de autentificación aleatoria particular.

En el ejemplo específico dado, si la acción de grabación de audio-video se completa dentro de un período de tiempo limitado (el período de validez de la secuencia) inmediatamente después de la generación del código aleatorio, el clip de audio-video grabado puede considerarse válido. De lo contrario, se puede generar un nuevo código aleatorio (secuencia de autentificación de usuario) y se puede repetir la acción de grabación de audio-video (generación de información de autentificación putativa).

Aunque el procedimiento 1100 se ha descrito en el contexto de una implementación de recuperación de código de verificación, algunos aspectos del procedimiento 1100 de autentificación remota también se pueden aplicar para autentificar usuarios en varias otras circunstancias. Por ejemplo, en algunas realizaciones, la etapa 1110 puede reemplazarse por cualquier solicitud de información o registro o una secuencia de inicio de autentificación en general. Luego, las etapas restantes del procedimiento 1100 se pueden usar para autentificar a un usuario de forma remota.

En la descripción que sigue, las realizaciones de sistema 200 puede ser denominado como QSSAS sin recuperación de código de verificación (QSSAS-NR) si se implementan realizaciones del procedimiento de CRKG sin recuperación de código de verificación, y realizaciones del sistema 200 pueden indicarse como QSSAS con recuperación de código de verificación (QSSAS-R) si se adoptan realizaciones del procedimiento de CRKG con recuperación del código de verificación.

Procedimiento de AVCC

Siempre que surja la necesidad, el primer usuario 240 puede cambiar el código de verificación C a través de cualquier agente 204 de encriptado en ejecución en uno de esos L dispositivos 202 en el **ROU** de estado. Nuevamente, usamos el agente 204 de encriptado en el primer dispositivo 202a como ejemplo. En algunas realizaciones, el procedimiento de AVCC puede funcionar de la siguiente manera:

El primer usuario 240 ingresa un nuevo código de verificación indicado por C^n en el agente 204 de encriptado en el primer dispositivo 202a de usuario. El agente 204 de encriptado determina un código local encriptado actualizado y reemplaza el código local encriptado actualmente almacenado (por ejemplo, el agente de encriptado calcula $\beta^n = (\beta_1^n, \beta_2^n) = (\alpha^{C_1^n} C_2^n, \alpha^{C_2^n})$ y actualiza el β guardado localmente en β^n).

En el caso de QSSAS-NR, el agente 204 de encriptado envía un código de servidor encriptado de actualización $\hat{\beta}^n = (\hat{\beta}_1^n, \hat{\beta}_2^n) = (\alpha^{C_1^n C_2^n}, \alpha^{C_1^n})$ al servidor Q 230, que a su vez actualiza el código de servidor encriptado del servidor guardado localmente $D(\beta^{\wedge})$ en $D(\beta^{\wedge n})$. En el caso de QSSAS-R, el agente 204 de encriptado calcula β^n y un código de recuperación remoto actualizado. En el ejemplo en el que el proveedor de servicio proporciona una clave pública del proveedor de servicio, el código de recuperación remoto actualizado puede determinarse como $\hat{\beta}_0^n = (\alpha^{\lambda Y} \alpha^{C_2^n} C_1^n, \alpha^Y)$, donde Y es un nuevo número aleatorio independiente de {1,2, ⋯, N - 1} y λ es la clave privada del proveedor de servicio. El agente 204 de encriptado puede enviar $\beta^{\wedge n}$ y $\hat{\beta}_0^n$ al servidor Q 230, que a su vez actualiza su $D(\beta^{\wedge})$ guardado localmente en $D(\beta^{\wedge n})$ y pasa el código de recuperación remoto actualizado $\hat{\beta}_0^n$ al proveedor de servicio del sistema 200 para actualizar $\beta^{\wedge}{}_0$ en $\hat{\beta}_0^n$.

El agente 204 de encriptado puede usar el código de verificación C existente para desencriptar $E_C(X_0, X_1, \cdots, X_i)$ y generar nuevos indicadores de claves encriptados basados en el código de verificación actualizado. Los indicadores de claves encriptados actualizados pueden transmitirse al servidor 230 para actualizar la cadena de estado de clave. En la realización de ejemplo de ElGamal, el agente 204 de encriptado puede generar independientemente nuevos números aleatorios Y_j,j = 0,1,2, ⋯, i, donde cada nuevo número aleatorio se distribuye de manera uniforme en {1,2,

⋯ , N -1}, calcular $\varepsilon_j^n = (\hat{\beta}_2^n)^{Y_j} X_j$ y $\mu_j^n = \alpha^{Y_j}$, j = 0,1,2, ⋯, i, y luego enviar $(\varepsilon_j^n, \mu_j^n)$, j = 0,1,2, ⋯, i, al servidor Q, que a su vez actualiza la cadena de estado de clave de $S = 1\varepsilon_0\mu_0 \cdots \varepsilon_i\mu_i$ a $S = 1\varepsilon_0^n\mu_0^n \cdots \varepsilon_i^n\mu_i^n$. El agente 204 de encriptado puede usar el código de verificación existente C para desencriptar $E_C(K_0,K_1,\cdots,K_i)$, usar el código de verificación actualizado C^n para volver a encriptar $(X_0,X_1,\cdots,X_i)$ y $(K_0,K_1,\cdots,K_i)$, y finalmente sobreescribir $E_C(X_0,X_1,\cdots,X_i)$ y $E_C(K_0,K_1,\cdots,K_i)$ con $E_{Cn}(X_0,X_1,\cdots,X_i)$ y $E_{Cn}(K_0,K_1,\cdots,K_i)$, respectivamente.

Al final del procedimiento de AVCC, las propiedades consistentes de la Ec. (1) a la Ec. (6) pueden seguir siendo válidas entre el agente 204 de encriptado en el primer dispositivo 202a de usuario y el servidor Q 230 con respecto al nuevo código de verificación C^n.

Procedimiento de VCU

Después de que el primer usuario 240 cambia el código de verificación a través del agente 204 de encriptado en el primer dispositivo 202a de usuario, las propiedades consistentes Ec. (3) y Ec. (4) puede que ya no sea válido entre cualquiera de los otros agentes 204 de encriptado del primer usuario 240 y el servidor Q 230. Si esos agentes 204 de encriptado se están ejecutando y se comunican con el servidor Q 230, en algunas realizaciones pueden cerrar la sesión automáticamente. En tales casos, cada agente 204 de encriptado puede solicitar al primer usuario 240 que actualice el código de verificación después de que se detecte el cambio del código de verificación. Se toma el agente 204 de encriptado en el segundo dispositivo 202b como ejemplo. El procedimiento de VCU puede funcionar de la siguiente manera:

1) El agente 204 de encriptado en el segundo dispositivo 202b le pide al primer usuario 240 que ingrese el nombre de usuario, la contraseña, el antiguo código de verificación C y el PIN R correctos.

2) El agente 204 de encriptado en el segundo dispositivo 202b usa C para desencriptar $E_C(X_0,X_1,\cdots,X_i)$ and $E_C(K_0,K_1,\cdots,K_i)$.

3) El agente 204 de encriptado en el segundo dispositivo 202b le pide al primer usuario 240 que ingrese el nuevo código de verificación C^n.

4) El agente 204 de encriptado en el segundo dispositivo 202b luego calcula $\beta^{\wedge}$ correspondiente a C^n y lo envía al servidor Q para verificar su consistencia con $D(\beta^{\wedge})$ guardado en el servidor Q.

Si la prueba de consistencia anteriormente en la Etapa 4) tiene éxito, entonces el agente 204 de encriptado en el segundo dispositivo 202b acepta la entrada C^n del primer usuario 240 como el nuevo código de verificación correcto; de lo contrario, las etapas 3) y 4) se repetirían hasta que la prueba de consistencia anterior sea exitosa.

El agente 204 de encriptado en el segundo dispositivo 202b luego calcula $\beta^n = (\alpha^{C_1^n} C_2^n, \alpha^{C_2^n})$, actualiza su β guardado localmente en β^n, utiliza el nuevo código de verificación C^n para volver a encriptar $(X_0,X_1,\cdots,X_i)$ y $(K_0,K_1,\cdots,K_i)$, y finalmente sobreescribe $E_C(X_0,X_1,\cdots,X_i)$ y $E_C(K_0,K_1,\cdots,K_i)$ con $E_{Cn}(X_0,X_1,\cdots,X_i)$ y $E_{Cn}(K_0,K_1,\cdots,K_i)$, respectivamente.

Al final del procedimiento de VCU, las propiedades consistentes de la Ec. (1) a la Ec. (6) puede volver a ser válido entre el agente 204 de encriptado en el segundo dispositivo 202b y el servidor Q 230 con respecto al nuevo código de verificación C^n, y el agente 204 de encriptado en el segundo dispositivo 202b también se puede reiniciar al **ROU** de estado.

Procedimiento de ANKG

En algunas realizaciones, siempre que surja la necesidad, el primer usuario 240 puede solicitar generar un nuevo conjunto de valores de inicialización de claves FED a través de cualquier agente 204 de encriptado en ejecución en uno de esos L dispositivos 202 en el **ROU** de estado. Nuevamente, usamos el agente 204 de encriptado en el primer dispositivo 202a de usuario como ejemplo. El procedimiento de ANKG puede funcionar como sigue:

El agente 204 de encriptado genera una pluralidad actualizada de indicadores de claves. Por ejemplo, el agente 204 de encriptado puede generar independientemente números aleatorios adicionales X_j como la pluralidad actualizada de indicadores de claves. El agente 204 de encriptado puede encriptar la pluralidad actualizada de indicadores de claves y transmitir la pluralidad actualizada de indicadores de claves encriptados al servidor 230. El servidor 230 puede entonces actualizar el indicador de estado de la clave utilizando la pluralidad de indicadores de claves encriptados y actualizados.

En el ejemplo de ElGamal, el agente 204 de encriptado también genera números aleatorios adicionales Y_j, $j = i + 1,2, \cdots, i+J$, donde cada número aleatorio se distribuye uniformemente sobre {1,2, ⋯, N -1}, calcula $\varepsilon_j = \hat{\beta}_2^{Y_j} X_j$ y $\mu_j = \alpha^{Y_j}$, $j = i + 1,2,\cdots,i+J$, y entonces envía (ε_j,μ_j), $j = i + 1,2,\cdots, i+J$, , al servidor Q 230, que a su vez actualiza la cadena de estado de clave S agregando $\varepsilon_{i+1}\mu_{i+1}\cdots\varepsilon_{i+J}\mu_{i+J}$ al extremo derecho de S, es decir, extendiendo S desde $S = 1\varepsilon_0\mu_0\cdots\varepsilon_i\mu_i$

a $S = 1\varepsilon_0\mu_0\cdots\varepsilon_{i+J}\mu_{i+J}$.

En las realizaciones que emplean los valores de clave de servidor, el agente 204 de encriptado puede enviar la cantidad indicador de clave al servidor 230, por ejemplo, como un par de enteros $(i1, i+J)$ al servidor Q 230 a la petición del servidor Q 230 de asistencia para generar un nuevo conjunto de valores de inicialización de claves FED.

Al recibir la cantidad del indicador de clave (por ejemplo, el par de enteros $(i+1, i+J)$), el servidor Q 230 puede generar los valores de la clave del servidor como se describió anteriormente. Por ejemplo, el servidor 230 puede generar valores de clave de servidor basados en U_r, $E(P_r)$ y su propia clave secreta v como números aleatorios independientes adicionales V_{i+1}, V_{i+2}, $\cdots$, V_{i+J}, donde cada número aleatorio adicional se distribuye uniformemente sobre $\{1,2, \cdots, N-1\}$, y envía V_{i+1}, V_{i+2}, $\cdots$, V_{i+J} de vuelta al agente 204 de encriptado.

Basado en los valores de clave del servidor $V_{i+1},V_{i+2},\cdots,V_{i+J}$ y la pluralidad actualizada de indicadores de claves $X_{i+1},X_{i+2},\cdots,X_{i+J}$, el agente 204 de encriptado puede generar un nuevo conjunto de valores de inicialización de claves FED $K_j = A(X_j,V_j)$, $j = i+1,i+2,\cdots, i+J$.

Finalmente, el agente 204 de encriptado puede almacenar información de valor de inicialización de clave basada en los valores de inicialización de clave actualizadas. Por ejemplo, el agente 204 de encriptado puede utilizar el código de verificación C para encriptar $(X_{i+1},X_{i+2},\cdots,X_{i+J})$ y $(K_{i+1},K_{i+2},\cdots,K_{i+J})$ en $E_C(X_{i+1},X_{i+2},\cdots,X_{i+J})$ y $E_C(K_{i+1},K_{i+2},\cdots,K_{i+J})$, respectivamente, y guardarlos en la memoria no volátil del primer dispositivo 202a de usuario.

Una vez más, al final del procedimiento de ANKG, las propiedades consistentes Ec. (1) a la Ec. (6) puede seguir siendo válido entre el agente 204 de encriptado en el primer dispositivo 202a de usuario y el servidor Q 230.

Procedimiento de PNKG

Después de que se genere un nuevo conjunto de valores de inicialización de claves FED a través del agente 204 de encriptado en el primer dispositivo 202a de usuario, cualquiera de los otros agentes 204 de encriptado del primer usuario 240 lo puede detectar si ese agente 204 de encriptado se está ejecutando y está en comunicación con el servidor Q 230. En consecuencia, ese agente 204 de encriptado (por ejemplo, el agente de encriptado en el segundo dispositivo 202b) puede generar automáticamente el mismo conjunto nuevo de valores de inicialización de claves FED para sí mismo a través de su comunicación con el servidor Q 230 mediante el procedimiento de PNKG. En general, el procedimiento de PNKG funciona de manera similar al procedimiento de ANKG combinado con el procedimiento de sincronización inicial de valor de inicialización de clave descrito anteriormente con referencia a las figuras 4B y 4C.

Después de detectar que otro agente de encriptado ha generado un nuevo conjunto de valores de inicialización de claves FED, el agente 204 de encriptado en el segundo dispositivo 202b puede solicitar al servidor Q 230 que devuelva la cadena de estado de clave $S = S_0S_1S_2\cdots S_{2(i+J+1)-1}S_{2(i+J+1)} = 1\varepsilon_0\mu_0\cdots\varepsilon_{i+J}\mu_{i+J}$.

El agente 204 de encriptado en el segundo dispositivo 202b puede determinar la pluralidad de indicadores de claves X_j, $j = i + 1, \cdots, i + J$, fuera de la cadena de estado de clave S mediante el cálculo $X_{j-1} = S_{2j-1}S_{2j}^{-c_1}$, $j = i + 2,\cdots,i + J + 1$.

El agente 204 de encriptado en el segundo dispositivo 202b puede entonces seguir el procedimiento general del ANKG descrito anteriormente, para completar la generación de la nueva serie de valores de inicialización de claves FED por sí mismo.

Al final del procedimiento de PNKG, las propiedades consistentes de la Ec. (1) a la Ec. (6) pueden ser válidas de nuevo entre el agente de encriptado en el segundo dispositivo 202b y el servidor Q 230.

Alias

El primer usuario 240 (o cualquier otro usuario) puede comunicarse con otros usuarios utilizando muchos nombres de usuario diferentes, como diferentes direcciones de correo electrónico y números de teléfono. En muchas aplicaciones (por ejemplo, correo electrónico y comunicaciones móviles), cada uno de estos nombres de usuario a menudo corresponde a su propia cuenta única para la aplicación respectiva, aunque estos nombres de usuario y cuentas pertenecen al mismo primer usuario 240. Sin embargo, en el caso del sistema 200, esta correspondencia uno a uno entre los nombres de usuario y las cuentas puede no ser conveniente en algunos casos. En algunas realizaciones, puede ser preferible tener una cuenta QSSAS por usuario por dispositivo. En algunas otras realizaciones, incluso si se permiten varias cuentas QSSAS por usuario por dispositivo, los archivos del primer usuario 240 administrados bajo una cuenta QSSAS no se pueden desencriptar en general cuando el primer usuario 240 inicia sesión en otra cuenta QSSAS en el mismo dispositivo 202, ya que diferentes cuentas QSSAS suelen tener diferentes conjuntos de valores de inicialización de clave FED, como se describe en el procedimiento de CRKG anterior.

Para superar los problemas mencionados anteriormente, en algunas realizaciones, la noción de alias se puede introducir en QSSAS para permitir que los múltiples nombres de usuario del primer usuario 240 (es decir, alias) compartan la misma cuenta QSSAS y, por lo tanto, la misma contraseña, código de verificación, un conjunto de valores de inicialización de claves FED y un par de claves privadas y públicas en esos *L* dispositivos 202 del primer usuario 240. El primer usuario 240 puede ser un solo usuario que controla la pluralidad de dispositivos 202. Sin embargo, el primer usuario 240 puede tener una pluralidad de identificadores de alias de usuario (por ejemplo, múltiples direcciones de correo electrónico, nombres de usuario de redes sociales, números de teléfono, etc.). En algunas realizaciones, cada identificador de alias de usuario en la pluralidad de identificadores de alias de usuario puede compartir la misma información de autentificación de cuenta.

Cada vez que el primer usuario 240 agrega un nuevo nombre de usuario (es decir, un alias) a la cuenta QSSAS del primer usuario 240 a través de cualquier agente de encriptado registrado 204 en uno de esos *L* dispositivos, ese alias se puede grabar en ese agente 204 de encriptado, enviado al servidor Q 230, que a su vez lo guarda en la primera cuenta de usuario del primer usuario 240, y ese alias se puede sincronizar posteriormente en todos los demás agentes 204 de encriptado registrados en otros dispositivos 202 (existentes o nuevos) del primer usuario 240 automáticamente.

En tales realizaciones, el primer usuario 240 puede iniciar sesión en la cuenta QSSAS del primer usuario 240 a través de cualquiera de los agentes de encriptado registrados 204 en esos *L* dispositivos 202 con el alias de cualquier primer usuario 240. Esto puede ser particularmente conveniente cuando otras personas comparten archivos encriptados con el primer usuario 240 a través de los diferentes alias del primer usuario 240. No importa cuál del alias del primer usuario 240 se utilice para compartir archivos encriptados, todos pueden ser desencriptados cuando el primer usuario 240 ingresa en cualquiera de los agentes 204 de encriptado registrados del primer usuario 240 con cualquier alias del primer usuario 240 siempre y cuando esos archivos encriptados puedan ponerse a disposición de ese dispositivo 202 respectivo.

Extensión de QSSAS para compartir en grupo archivos encriptados

Realizaciones ejemplares se describirán ahora que pueden proporcionar el intercambio en grupo de archivos encriptados entre una pluralidad de grupos de usuarios. La figura 7 muestra una realización de ejemplo de un sistema 700 para proporcionar encriptado para una pluralidad de dispositivos 702 configurados para comunicación electrónica con un servidor 730. El sistema 700 es generalmente similar a los sistemas 200 y 500 descritos anteriormente, pero en el sistema 700 el primer usuario comprende una pluralidad de usuarios *740a-t* del grupo. La pluralidad de usuarios 740 del grupo puede incluir un usuario 740a del grupo administrativo y un segundo usuario 740b del grupo.

Cada uno de los usuarios 740 del grupo puede tener una cuenta específica del usuario registrada con el servidor 730. Cada usuario 740 del grupo puede controlar al menos uno de los dispositivos 702. En el ejemplo que se muestra en la figura 7, el usuario 740a del grupo administrativo tiene el control del primer dispositivo 702a y el segundo usuario del grupo tiene el control del segundo dispositivo 702b. Cada dispositivo 702 puede tener instalado en el mismo un agente 704 de encriptado. Cada agente 704 de encriptado instalado en un dispositivo 702 particular se puede registrar con el servidor Q 730 para el usuario 740 del grupo que tiene el control de ese dispositivo 702 particular.

Es decir, para cada usuario 740 del grupo en la pluralidad de usuarios del grupo, la cuenta específica de usuario correspondiente puede incluir un identificador de usuario del grupo (es decir, el nombre de usuario de ese usuario). La cuenta específica del usuario también puede almacenar otros datos de cuenta, como se describe anteriormente, como los alias, por ejemplo. Cada usuario 740 del grupo también puede tener contraseñas, códigos de verificación, pares de claves públicas y privadas, y un conjunto distinto de valores de inicialización de claves FED. La pluralidad de usuarios 740 del grupo puede estar interesada en compartir entre sí ciertos archivos encriptados. Por ejemplo, los archivos encriptados pueden estar relacionados con un proyecto de interés común (por ejemplo, un proyecto compartido). Las realizaciones del sistema 700 pueden proporcionar este intercambio en grupo de archivos encriptados utilizando aspectos de los sistemas 100, 200 y 500 descritos anteriormente. Además, las realizaciones del sistema 700 también pueden introducir nuevos conceptos tales como carpetas virtuales (VF), superusuarios (SU) y cuentas de superusuarios (SUA). En algunas realizaciones, se pueden usar procesos ligeramente modificados para generar y sincronizar un nuevo conjunto de valores de inicialización de claves FED específicas para cada VF para el proyecto compartido a través de la comunicación entre agentes de encriptado de los usuarios 740 del grupo y el servidor Q 730.

En general, una carpeta virtual puede referirse al conjunto particular de archivos encriptados asociados con cada pluralidad de valores de inicialización de claves generadas por el usuario. Aunque el ejemplo de un índice se describe en detalle aquí, será evidente que una carpeta virtual puede implementarse de muchas maneras diferentes. La carpeta virtual puede ser en efecto un identificador para un grupo particular de archivos encriptados. La carpeta virtual para los archivos correspondientes a cada proyecto compartido (o cada grupo de usuarios) con los que está involucrado el usuario puede asociarse con los valores de inicialización de claves correspondientes y la información de la cadena de estado de clave para ese grupo de usuarios.

El concepto de una carpeta virtual (VF) que se utiliza en algunas realizaciones de sistema 700 se describirá usando el usuario 740a administrativo como un ejemplo. El usuario 740a administrativo ha registrado una cuenta específica de usuario con el servidor 730, por ejemplo, utilizando una realización del procedimiento de CRKG descrito anteriormente. El usuario 740a administrativo puede haber registrado uno o más agentes 704 de encriptado en los dispositivos 702 controlados por el usuario 740aadministrativo (es decir, un agente 704 de encriptado por dispositivo 702 controlado por el usuario 740a administrativo). Hasta este punto, el usuario 740a administrativo puede haber utilizado su cuenta específica de usuario y los agentes 704 de encriptado solo para proteger y administrar sus archivos no compartidos, ya sea que estén almacenados en sus propios dispositivos 702, en el servidor 750 en la nube o transmitidos a través del servidor 750 en la nube, o en otros lugares, como otros lugares de Internet. El servidor Q 730 puede haber almacenado solo una cadena de estado de clave *S* en la cuenta específica del usuario del usuario 740a administrativo, y el conjunto de valores de inicialización de claves FED utilizadas por los agentes 704 de encriptado del usuario 740a administrativo y se sincronizaron automáticamente utilizando las realizaciones de sistema 200/500 a través de la cadena de estado de clave *S* se puede usar solo para encriptar y desencriptar los archivos no compartidos administrados por los agentes 704 de encriptado del usuario 740a administrativo.

Para facilitar la descripción posterior, los archivos no compartidos gestionados por los agentes 704 de encriptado del usuario 740a administrativo se puede decir que forman una carpeta virtual indexada por 0 (VF0) para el usuario 740a administrativo. En consecuencia, el conjunto de valores de inicialización de claves FED utilizadas por los agentes 704 de encriptado del usuario 740a administrativo para encriptar y desencriptar los archivos no compartidos contenidos en VF0 y la cadena de estado de clave *S* correspondiente registrada por el servidor Q 730 en la cuenta específica del usuario del usuario 740a administrativo que puede decir que se asigna a VF0 para el usuario 740a administrativo. A medida que pasa el tiempo, el usuario 740a administrativo puede querer involucrarse o ser involucrado por otros usuarios, tal como los usuarios 740 del grupo, para compartir archivos encriptados, para participar en proyectos compartidos y compartir archivos encriptados relacionados con cada uno de los proyectos compartidos con el conjunto respectivo de otros usuarios 740.

Para cada proyecto compartido del usuario 740a administrativo, el sistema 700 ahora puede asignarle un VF con un índice *I*, donde *I* puede aumentarse en 1 cada vez que el usuario 740a administrativo participa en un nuevo proyecto compartido. Cada VF *I* puede asociarse con el *I*-ésimo proyecto compartido del usuario 740a administrativo. La asignación a VF*I* puede ser una cadena de estado de clave S^I específica de VF*I* y un conjunto de nuevos valores de inicialización de claves FED utilizadas por los agentes 704 de encriptado del usuario 740a administrativo para encriptar y desencriptar archivos contenidos en VF *I* para el *I* Proyecto compartido del usuario 740a administrativo y generado nuevamente a través de la comunicación entre los agentes 704 de encriptado en los dispositivos 702 del usuario 740a administrativo y del servidor Q 730 (como se describió anteriormente) junto con el superusuario respectivo (SU) y la cuenta de superusuario (SUA). Debe tenerse en cuenta que aunque el usuario 740a administrativo puede usar diferentes agentes de encriptado en diferentes dispositivos para trabajar en diferentes proyectos compartidos, el servidor Q 730 puede saber en todo momento en cuántos proyectos compartidos ha participado el usuario administrativo, y saber cómo asignar los índices a VF del usuario 740a administrativo.

Asociado con cada proyecto compartido del usuario 740a administrativo puede haber un grupo de usuarios (es decir, una pluralidad de usuarios del grupo) que participan en el proyecto compartido. Los usuarios del grupo pueden compartir entre sí archivos encriptados relacionados con el proyecto compartido. Dentro del grupo de usuarios, se puede hacer referencia a uno de los usuarios como el usuario administrativo para el proyecto compartido (para simplificar, usaremos al usuario 740a administrativo como el usuario administrativo en la siguiente descripción). Por ejemplo, cuando el primer usuario incluye una pluralidad de usuarios del grupo, se puede hacer referencia al primer usuario como superusuario.

En algunas realizaciones, el usuario administrativo puede ser el iniciador del proyecto compartido. El usuario administrativo y el conjunto de otros usuarios en el grupo pueden llamarse superusuario. Cada usuario del grupo puede identificarse según su identificador de usuario del grupo o un índice en una base de datos de usuario registrada en el servidor Q 730. En el servidor Q 730, un SU puede estar representado por un par (ω, Ω), donde ω es el índice del usuario administrativo para el proyecto compartido en la base de datos de usuarios, y Ω es el conjunto de índices de otros usuarios en el grupo en la base de datos de usuarios. El sistema 700 puede asignar además a cada SU un identificador de grupo único (por ejemplo, el identificador del primer usuario) tal como un ID indicado por I_l.

Para cada SU, el servidor Q 730 puede crear una cuenta de superusuario. El servidor 730 puede generar la primera cuenta de usuario como la cuenta de superusuario para esa pluralidad de usuarios del grupo. La primera cuenta de usuario (la cuenta de superusuario/SUA) puede incluir el identificador del primer usuario (el ID de ese SU). El identificador del primer usuario puede representarse en forma de un par (ω , Ω).

En algunas realizaciones, el SUA puede generar y almacenar una cadena de estado de clave para permitir que los usuarios del grupo determinen la misma pluralidad de indicadores de claves, y de ese modo generar la misma pluralidad de valores de inicialización de claves y claves de encriptado. Esto puede permitir que los usuarios del grupo compartan de forma segura los archivos encriptados y, al mismo tiempo, proporcionen a cada usuario del grupo acceso a los archivos desencriptados.

De una manera similar a las realizaciones del procedimiento de CRKG descrito anteriormente, el SUA también puede generar una pluralidad de valores de clave de servidor para la primera cuenta, y los valores de clave de servidor pueden almacenarse en el servidor 730 para el SUA. Por ejemplo, los valores de clave del servidor pueden ser una secuencia de números aleatorios independientes V_1, V_2, ⋯, V_i para el primer usuario, que a su vez se pueden usar para ayudar a los agentes 704 de encriptado de los usuarios del grupo 702 dentro de ese SU generado mediante la comunicación con el servidor Q 730, la pluralidad de indicadores de claves y un conjunto de nuevos valores de inicialización de claves FED utilizadas por los agentes de encriptado de los usuarios dentro de ese SU para encriptar y desencriptar archivos relacionados con el proyecto compartido correspondiente a ese SU.

Se toma el usuario 740a administrativo como un ejemplo otra vez. Con la introducción de los conceptos de proyecto compartido, VF, SU y SUA, la información almacenada por cada agente 704 de encriptado del usuario 740a administrativo en la memoria no volátil del dispositivo 702 correspondiente controlado por el usuario 740a administrativo se puede expandir para incluir conjuntos adicionales de indicadores de claves de encriptado basados en el código de verificación para el usuario 740a administrativo y la información clave de valores de inicialización para cada VF del usuario 740a administrativo, junto con la lista de índices VF I y los correspondientes identificadores de superusuario I_I registrados por ese agente de encriptado del usuario 740a administrativo. Por ejemplo, un conjunto adicional de números aleatorios encriptados $E_{C,I}(X_{I,1},X_{I,2},\cdots,X_{I,i})$ y valores de inicialización FED encriptados $E_{C,I}(K_{I,1},K_{I,2},\cdots,K_{I,i})$ I = 1,2,⋯, un conjunto adicional por VF, puede ser almacenado. I_I se refiere al ID del SU asociado con el proyecto compartido correspondiente a VF I del usuario 740a administrativo. El(los) agente(s) 704 de encriptado del usuario administrativo puede(n) utilizar el conjunto de valores de inicialización de claves FED $\{K_{I,1}, K_{I,2},\cdots,K_{I,i}\}$ asignadas a VFI del usuario 740a administrativo para encriptar y desencriptar archivos relacionados con el proyecto compartido correspondiente a VFI. Del mismo modo, la información guardada por el servidor Q 730 en su memoria no volátil para el usuario 740a administrativo también se puede expandir para incluir la lista de todos los índices de FVI del usuario 740 administrativo, los ID de superusuario correspondientes I_I, y una cadenas de estado de claves adicionales $S^I = S_{I,0}S_{I,1}S_{I,2}\cdots S_{I,2i}$ en la forma de $\{(I,I_I,S^I)$: I = 1,2,⋯$\}$, donde S^I es la cadena de estado de clave asignada a VFI del usuario 740a administrativo. En algunas realizaciones, la cadena de estado de clave S^I asignada a VFI del usuario 740a administrativo puede ser iniciada por el usuario administrativo para el proyecto compartido correspondiente a VFI del usuario 740a administrativo a través de un agente de encriptado de funcionamiento del usuario administrativo.

En algunas realizaciones, el usuario 740a administrativo, el segundo usuario 740b del grupo y los usuarios 740 restantes del grupo pueden querer participar en un proyecto compartido y compartir archivos encriptados relacionados con el proyecto compartido a través del sistema 700. Sin pérdida de generalidad, se asume que el usuario 740a administrativo es el iniciador y el administrador del proyecto compartido. En este caso, el SU correspondiente al proyecto compartido consiste en el usuario 740a administrativo y la pluralidad de otros usuarios 740 del grupo. Para cada usuario 740 del grupo, el VF correspondiente al proyecto compartido puede ser VFI_t. Los archivos encriptados reales relacionados con el proyecto compartido se pueden sincronizar con la nube y con los agentes 704 de encriptado de todos los usuarios dentro del SU a través del servicio informático en la nube u otros medios. Sin embargo, para que los usuarios dentro del SU puedan ver los archivos de texto sin formato correspondientes, el conjunto de valores de inicialización de claves FED utilizados por los agentes 704 de encriptado de todos los usuarios 740 del grupo en el primer usuario para encriptar y desencriptar archivos relacionados con el proyecto compartido puede sincronizarse mediante el sistema 700 a través de los agentes 704 de encriptado de todos los usuarios 740 del grupo.

Con referencia a la figura 8, un procedimiento 800 de ejemplo se describe para la generación y la sincronización de valores de inicialización de clave cuando el primer usuario incluye una pluralidad de usuarios del grupo. El conjunto de valores de inicialización de claves FED utilizadas para encriptar y desencriptar archivos relacionados con el proyecto compartido puede ser generado inicialmente por el usuario administrativo para el proyecto compartido, que es el usuario 740a administrativo en el caso actual, de acuerdo con los ejemplos descritos anteriormente.

En 805, se puede registrar una pluralidad de usuarios del grupo con la primera cuenta. El proceso de registro de un usuario con la primera cuenta puede ser similar al descrito anteriormente con referencia a 660 en la figura 6C. En algunas realizaciones, el identificador de usuario de cada usuario del grupo dentro del primer usuario puede ser una dirección de correo electrónico válida de ese usuario. El primer usuario 740a administrativo puede usar uno de sus agentes 704 de encriptado para enviar una solicitud de autorización al servidor 730. La solicitud de autorización de grupo puede incluir los identificadores de usuario de todos los usuarios del grupo en el primer usuario. La solicitud de autorización de grupo puede indicar al servidor Q 730 que se debe generar una primera cuenta para el proyecto compartido.

El servidor Q 730 puede configurar el SUA y también puede transmitir, en nombre del usuario 740a administrativo, una invitación a unirse al proyecto compartido a cada uno de los usuarios 740 del grupo. La invitación puede enviarse como un correo electrónico a una dirección de correo electrónico asociada con el identificador de usuario de ese usuario 740 del grupo. El correo electrónico también puede solicitar a cada usuario del grupo que configure una cuenta específica del usuario con el servidor 730 si ese usuario del grupo no tiene una.

En algunas realizaciones, el servidor 730 puede generar la primera cuenta para que el primer usuario incluya información de autentificación de cuenta correspondiente a cada usuario del grupo. La información de autentificación

de la cuenta puede incluir un código encriptado del servidor específico del usuario para cada usuario 740 del grupo. Para cada usuario, el agente 704 de encriptado puede generar el código encriptado del servidor específico del usuario en uno de los dispositivos controlados por ese usuario. El agente 704 de encriptado puede definir un código de verificación específico del usuario y generar el código encriptado del servidor específico del usuario basándose en el código de verificación específico del usuario. El agente de encriptado puede transmitir el código encriptado del servidor específico del usuario donde se puede almacenar en la información de autentificación de la cuenta de la primera cuenta. En algunos casos, la información de autentificación de la cuenta de la primera cuenta puede simplemente indicar la cuenta específica del usuario donde se puede acceder al código encriptado del servidor específico del usuario para autentificar al usuario.

Después de que los usuarios dentro del SU respondan, el servidor Q 730 puede comunicarse aún más, para cada usuario 740 del grupo que acepta la invitación, con un agente 704 de encriptado de ese usuario del grupo para que se configure el FV correspondiente al proyecto compartido en el agente 704 de encriptado, de ese grupo de usuarios y el índice l_t de VFl_t y el ID del SU asociado con el proyecto compartido están registrados por el servidor Q 730 en la cuenta específica del usuario t y también por ese agente de encriptado del usuario t.

En 810, cada usuario 740 grupo puede generar una clave pública específica del usuario. La clave pública específica del usuario para cada usuario puede generarse basándose en una clave privada específica del usuario almacenada en la memoria no volátil de un dispositivo 702 correspondiente controlado por el usuario 740 del grupo. La clave pública específica del usuario para cada usuario se puede proporcionar al usuario 740a administrativo. La clave privada específica del usuario y la clave pública específica del usuario se pueden generar como se describió anteriormente con referencia a 470 en la figura 4C.

Por ejemplo, para cada usuario 740 del grupo que acepta la invitación, el servidor Q 730 puede devolver al agente 704 de encriptado del usuario 740 administrativo el valor de γ registrado en la cuenta específica del usuario 740a del grupo, donde γ es la clave pública de ese usuario 740 del grupo. El servidor 730 también puede enviar el índice de ese usuario del grupo en la base de datos de usuarios almacenada en el servidor Q 730. La clave pública específica del usuario para un usuario 740t del grupo puede estar indicada por $\beta_{t,2}$ para facilitar nuestras descripciones posteriores.

En 815, el agente 704 de encriptado del primer dispositivo 702a puede generar la pluralidad de indicadores de claves de encriptado para el primer usuario mediante la generación de una pluralidad de indicadores de claves encriptados específicos del usuario. El indicador de clave encriptado se puede generar basándose en los indicadores de claves generados de la misma manera que se describe anteriormente. El agente 704 de encriptado del primer dispositivo 702a puede generar, para cada usuario 740 del grupo, una pluralidad de indicadores de claves encriptados específicos del usuario utilizando la clave pública específica del usuario para ese usuario del grupo.

Por ejemplo, el agente 704 de encriptado del usuario 740a administrativo puede generar los indicadores de claves como una pluralidad de números aleatorios independientes $X_{l1,j}$, j = 1,2,⋯,J, donde cada número aleatorio es distribuido uniformemente sobre {1,2, ⋯, N - 1}. En algunas realizaciones, el agente 704 de encriptado del usuario 740a administrativo puede enviar un par de enteros (1, J) al servidor Q 730 para solicitar la asistencia del servidor Q 730 para generar los valores de inicialización de claves FED para el proyecto compartido. En dichas realizaciones, al recibir el par de enteros (1, J), el servidor Q 730 puede generar, en función del SUA, y su propia clave secreta v, valores de clave de servidor como los números aleatorios independientes V_1, V_2, ⋯, V_J, donde cada número aleatorio se distribuye uniformemente sobre {1,2, ⋯, N - 1}, y envía V_1, V_2, ⋯, V_J de vuelta al agente 704 de encriptado del usuario 740a administrativo.

El agente 704 de encriptado del usuario 740a administrativo puede generar J valores de inicialización de claves FED independientes $K_{l1,j} = A(X_{l1,j}, V_j)$, j = 1,2,⋯,J, para el proyecto compartido basado en $V_1,V_2,\cdots,V_J$ y $X_{l1,1}$, $X_{l1,2},\cdots,X_{l1,J},$.

El agente 704 de encriptado del usuario 740a administrativo puede utilizar el código de verificación C del usuario 740a administrativo junto con el índice l_1 del VF correspondiente al proyecto compartido para el usuario 740a administrativo para encriptar la pluralidad de indicadores de claves ($X_{l1,1},X_{l1,2},\cdots,X_{l1,J}$) en $E_{C,l1}(X_{l1,1},X_{l1,2},\cdots,X_{l1,J})$ y generar la información de valor de inicialización de clave mediante encriptado ($K_{l1,1},K_{l1,2},\cdots,K_{l1,J}$) en $E_{C,l1}(K_{l1,1},K_{l1,2},\cdots,K_{l1,J})$, respectivamente. El agente 704 de encriptado puede luego guardar la pluralidad de indicadores de claves ($E_{C,l1}(X_{l1,1},X_{l1,2},\cdots,X_{l1,J})$) y la información de valor de inicialización de clave $E_{C,l1}(K_{l1,1},K_{l1,2},\cdots,K_{l1,J})$ en la memoria no volátil del primer dispositivo 702a.

En algunas realizaciones, para cada grupo de usuarios t, $1 \le t \le T$, que acepta la invitación, el agente 704 de encriptado del usuario 740a administrativo puede generar, además, una segunda pluralidad de números aleatorios independientes $Y_{t,j}$, j = 1,2, ⋯, J, donde cada número aleatorio se distribuye uniformemente sobre {1,2, ⋯, N -1}, determina los indicadores de claves encriptados específicos del usuario $\varepsilon_{t,j} = \hat{\beta}_{t,2}^{Y_{t,j}} X_{l_1,j}$ y una pluralidad de claves públicas indicadoras específicas del usuario $\mu_{t,j} = \alpha^{Yt,j}$, j = 1,2,⋯,J, y enviar ($\varepsilon_{t,j},\mu_{t,j}$), j = 1,2,⋯,J, junto con el índice de usuario t y el ID (digamos I) del SU asociado con el proyecto compartido al servidor Q 730, donde $\hat{\beta}_{t,2}$ es la clave pública del usuario t.

Al recibir los indicadores de claves encriptados $\{\{(\varepsilon_{t,j}, \mu_{t,j})\}_{j=1}^{J}$ en la implementación específica utilizando ElGamal descrito anteriormente junto con el índice del grupo de usuarios *t* y el ID*I* del primer usuario asociado con el proyecto compartido, el servidor Q 730 puede usar el primer identificador del usuario ID*I* del SU para determinar el índice I_t del FV correspondiente al proyecto compartido para el usuario del grupo *t a* partir de la información de cuenta específica del usuario del usuario del grupo *t,* y luego actualizar la cuenta específica del usuario *t* del usuario reemplazando (I_t,*I*) con (I_t,*I*,S^{It}), donde $S^{It} = S_{It,0}S_{It,1}S_{It,2}\cdots S_{It,2J} = 1\varepsilon_{t,1}\mu_{t,1}\cdots\varepsilon_{t,J}\mu_{t,J}$.

Es decir, la porción del indicador de clave del servidor de la cadena de estado de clave para la primera cuenta puede incluir, para cada usuario 740 del grupo, una porción de la cadena específica del usuario que se genera en función de la pluralidad de indicadores de claves encriptados específicos del usuario para ese usuario 740 del grupo. La porción de la cadena específica del usuario también se puede almacenar en la cuenta específica del usuario para ese usuario del grupo, junto con el primer identificador del usuario.

En 820, el segundo dispositivo 702b puede recibir la porción de cadena específico del usuario para el segundo usuario 740b. El agente 704 de encriptado en el segundo dispositivo 702b puede usar la porción de cadena específica del usuario recibida para determinar la pluralidad de indicadores de claves para la primera cuenta y, por lo tanto, los valores de inicialización de clave y las claves de encriptado para los archivos del proyecto compartido.

En 825, el agente 704 de encriptado del segundo dispositivo 702b puede determinar la pluralidad de indicadores de claves de la pluralidad de indicadores de claves encriptados específicos del usuario en la porción específica de usuario de la porción de indicador de clave servidor (recibida en 820) utilizando la clave privada del segundo dispositivo.

Por ejemplo, supongamos que el agente 704 de encriptado del segundo usuario 740b está en el **ROU** de estado. El conjunto de valores de inicialización de claves FED generadas por el usuario administrativo para la primera cuenta se puede sincronizar de forma automática y segura con el agente 704 de encriptado del segundo usuario 740b.

Durante el proceso de intercambio entre el agente 704 de encriptado del segundo dispositivo 702b y el servidor Q 730, que puede ser iniciado por el agente de encriptado del segundo usuario 740b, el servidor Q 730 puede enviar de vuelta al agente 704 de encriptado del segundo dispositivo 702b la lista {(I, I_I, S^I): I = 1,2, ⋯} de los índices VF I, superusuario ID I_I, y cadenas de estado de claves adicionales $S^I = S_{I,0}\ S_{I,1}\ S_{I,2}\ \cdots\ S_{I,2J}$ contenidas en la cuenta específica del usuario del segundo usuario 702b.

Al comparar la lista {(I, I_I, S^I): I = 1,2, ...} con su información local, el agente 704 de encriptado del segundo dispositivo 702b puede detectar que la nueva carpeta virtual VF I_t que se ha establecido entre el servidor Q 730 y otro agente 704 de encriptado del segundo usuario 740b, si el agente 704 de encriptado del segundo dispositivo 702b no tiene ningún registro de VF I_t. El agente 704 de encriptado del segundo dispositivo 702b también puede determinar que la pluralidad de valores de inicialización de claves FED para el proyecto compartido correspondiente a VF I_t (es decir, para la primera cuenta asociada con el primer usuario) ya ha sido generada por el usuario 740a administrativo para ese proyecto compartido.

El agente 704 de encriptado del segundo dispositivo 702b puede configurar la carpeta virtual VFl$_t$ para sí mismo y registrar la información (I_t, I_{It}) si no tiene ningún registro en VF I_t. El agente 704 de encriptado del segundo dispositivo 702b también puede recuperar la cadena de estado de clave correspondiente $S^{It}=S_{It,0}S_{It,1}S_{It,2}\cdots S_{It,2J}$ de la lista {(I,I_I,S^I): I = 1,2,⋯}. El agente 704 de encriptado del segundo dispositivo 702b puede luego calcular

$$X_{l_t,j} = S_{l_t,2j-1}S_{l_t,2j}^{-K_{t,0}}, \quad j = 1,2,\cdots,J \quad (7)$$

donde $K_{t,0}$ es la clave privada del usuario *t*.

El agente 704 de encriptado del segundo dispositivo 702b puede enviar el par de enteros (1, J) junto con el primer ID de identificador de usuario I_{It} del primer usuario asociado con el proyecto compartido correspondiente a VF I_t al servidor Q 730 para solicitar la asistencia del servidor Q 730 para generar valores de inicialización de claves FED para ese proyecto compartido para que lo utilice el agente 704 de encriptado del segundo dispositivo 702b.

Al recibir (1, J, I_{It}), el servidor Q 730 puede generar, basándose en el SUA correspondiente al primer usuario con el identificador del primer usuario ID $I_{It,}$ y su propia clave secreta v, los valores de la clave del servidor como números aleatorios independientes V_1, V_2, ⋯, V_J, donde cada número aleatorio se distribuye de manera uniforme en {1,2, ⋯, N - 1}, y envía V_1, V_2, ⋯, V_J de vuelta al agente 704 de encriptado del segundo dispositivo 702b.

En función de los valores de clave del servidor V_1, V_2, ⋯, V_J y la pluralidad de indicadores clave $X_{It,1}$, $X_{It,2}$, ⋯, $X_{It,J}$, el agente 704 de encriptado del segundo dispositivo 702b puede generar J valores de inicialización de clave FED independientes $K_{It,j} = A(X_{It,j}, V_j)$, j = 1,2, ⋯, J , para que el proyecto compartido sea utilizado por el agente 704 de encriptado del segundo dispositivo 702b.

El agente 704 de encriptado del segundo dispositivo 702b puede usar el código de verificación C del segundo usuario 740b junto con el índice l_t de la carpeta virtual VFl_t en el agente 704 de encriptado del segundo dispositivo 702b a encriptar ($X_{lt,1},X_{lt,2},\cdots,X_{lt,J}$) y ($K_{lt,1},K_{lt,2},\cdots,K_{lt,J}$) en $E_{C,lt}(X_{lt,1},X_{lt,2},\cdots,X_{lt,J})$ y $E_{C,lt}(K_{lt,1},K_{lt,2},\cdots,K_{lt,J})$, respectivamente, y guardar $E_{C,lt}(X_{lt,1},X_{lt,2},\cdots,X_{lt,J})$ and $E_{C,lt}(K_{lt,1},K_{lt,2},\cdots,K_{lt,J})$ en la memoria no volátil del segundo dispositivo 702b.

En base a la descripción anterior, se deduce que los números aleatorios $X_{lt,j}$, j = 1,2, ..., J, se calculan en la Ec. (7), pueden ser los mismos que los generados por el usuario 740a administrativo en el procedimiento de generación de valores de inicialización de claves FED para compartir en grupo los archivos encriptados descritos anteriormente. Además, la descripción anterior también puede implicar:

$$K_{l_t,j} = K_{l_1,j},\ j = 1,2,\cdots,J. \quad (8)$$

Por lo tanto, el conjunto de valores de inicialización de claves FED $\{K_{l1,1},K_{l1,2},\cdots,K_{l1,J}\}$ se puede sincronizar en todos los agentes 704 de encriptado de todos los usuarios 740 del grupo dentro del primer usuario SU.

Una vez que se genera y sincroniza el conjunto de valores de inicialización de claves FED $\{K_{l1,1},K_{l1,2},\cdots,K_{l1,J}\}$, la carpeta virtual VF$l_t$ en cualquier agente 704 de encriptado del segundo usuario 740b puede funcionar de la misma manera que VF0. Por ejemplo, cualquier archivo creado/modificado dentro o movido a VFl$_{tt}$ puede ser encriptado automáticamente por el agente 704 de encriptado respectivo del usuario del grupo t usando una clave FED elegida de manera aleatoria del almacén de claves FED correspondiente al conjunto $\{K_{l1,1},K_{l1,2},\cdots,K_{l1,J}\}$ a menos que el archivo movido ya esté en el formato encriptado por otro agente 704 de encriptado de un usuario 740 del grupo dentro del primer SU. Los datos encriptados resultantes por archivo junto con la información de generación de claves (como el índice de la clave FED utilizada en el almacén de claves) a partir de la cual se puede derivar la clave FED con la ayuda de los valores de inicialización de claves, y el ID del SU asociado con el proyecto compartido correspondiente a la carpeta virtual VFl_t puede guardarse como el archivo encriptado. Los archivos encriptados con claves del almacén de claves FED correspondientes al conjunto $\{K_{l1,1},K_{l1,2},\cdots,K_{l1,J}\}$ pueden ser desencriptados por el agente de encriptado correspondiente del usuario del grupo a solicitud del usuario t cuando se colocan en la carpeta virtual VFl_t. Dado que los archivos administrados por agentes de encriptado de todos los usuarios 740 del grupo y almacenados en una memoria no volátil pueden permanecer encriptados todo el tiempo, los archivos encriptados con claves del almacén de claves FED correspondientes al conjunto $\{K_{l1,1},K_{l1,2},\cdots,K_{l1,J}\}$ para el proyecto compartido puede denominarse "muerto" una vez que están fuera de todas las carpetas virtuales VFl_t, $1 \le t \le T$.

A través del procedimiento de sincronización de valores de inicialización de claves FED para compartir grupos de archivos encriptados, la información local registrada por los agentes 704 de encriptado de cada usuario 740 del grupo también se puede sincronizar con la información de la cuenta del usuario 740 del grupo registrada en el servidor Q 730. Además, en algunas realizaciones puede haber propiedades consistentes extendidas que, además de las propiedades consistentes Ec. (1) a la Ec. (6), también incluyen propiedades consistentes que involucran índices VF, ID de superusuario correspondientes y conjuntos de números aleatorios $X_{l,1},X_{l,2},\cdots,X_{l,J}$ y valores de inicialización de claves FED $K_{l,1},K_{l,2},\cdots,K_{l,J}$, $1 \le l \le l_t$, para todos los VF del usuario t. Del mismo modo, los procedimientos de AVCC, VCU, ANKG y PNKG se pueden ampliar para cubrir el intercambio de archivos encriptados en grupo.

En otras realizaciones del sistema 700 se pueden usar otras características y componentes de seguridad. Además, muchos de los ejemplos descritos anteriormente para los sistemas 100, 200 y 500 también pueden usarse en realizaciones del sistema 700.

En algunas realizaciones, cuando se crea un archivo encriptado para compartir dentro de un SU a través del sistema 700, uno de los usuarios 740 del grupo puede especificar la cantidad máxima de veces que el archivo encriptado puede ser desencriptado para ser visto por cualquier agente 704 de encriptado en cualquier dispositivo 702 del usuario del grupo u otros usuarios 740 del grupo dentro del SU. Una vez que el agente 704 de encriptado desencripta esa cantidad máxima de veces, ese agente 704 de encriptado puede rechazarla para su posterior desencriptación. En algunas realizaciones, para evitar cualquier alteración, ese número máximo de veces, junto con el archivo de texto simple original, se puede encriptar y formar parte de los datos encriptados del archivo encriptado.

En algunas realizaciones, cuando se crea un archivo encriptado para compartir dentro de un SU a través del sistema 700, uno de los usuarios 740 del grupo puede especificar un periodo de caducidad. El período de caducidad puede definir un período a partir del cual el agente 704 de encriptado denegará el desencriptado del archivo encriptado en cualquier dispositivo 702 del usuario del grupo u otros usuarios del grupo 740 dentro del SU. En algunas realizaciones, para evitar cualquier alteración, el período de caducidad junto con el archivo de texto simple original se puede encriptar y formar parte de los datos encriptados del archivo encriptado.

En algunas realizaciones, el usuario 740a administrativo para un proyecto compartido puede ser capaz de eliminar o quitar uno de los usuarios del grupo, digamos usuario t, de la pluralidad de usuarios del grupo (SU) asociados con el proyecto compartido. El usuario 740a administrativo puede enviar una solicitud al servidor Q 730 para actualizar la cadena de estado de clave S^{lt} del usuario t correspondiente al proyecto compartido a una cadena de estado de clave de eliminación. La cadena de estado de clave de eliminación puede indicar a los agentes de encriptado en los dispositivos asociados con la eliminación del usuario del grupo que el usuario del grupo ya no es uno de los usuarios

del grupo en el primer usuario. Por ejemplo, la cadena de estado de clave puede actualizarse de S^{lt} = $S_{lt,0}S_{lt,1}S_{lt,2}\cdots S_{lt,2J}$ a S^{lt} = $S_{lt,0}00\cdots0$, es decir, $S_{lt,0}$ seguido de $2J$ ceros. La eliminación del usuario puede ser gestionada automáticamente por el procedimiento de sincronización de valores de inicialización de claves FED para compartir en grupo archivos encriptados, como se describe anteriormente. Este proceso se puede aplicar para cambiar el conjunto de valores de inicialización de claves FED (y números aleatorios) correspondientes al proyecto compartido y guardarlas localmente por todos los agentes de encriptado del usuario *t* en un conjunto diferente para que los archivos encriptados con claves FED para el proyecto compartido que ya no puedan desencriptarse por ningún agente de encriptado del usuario *t*.

En algunas realizaciones, el usuario 740a administrativo para un proyecto compartido puede permitir que un usuario eliminado vuelva a unirse al SU asociado con el proyecto compartido. Para lograr esto, el usuario administrativo puede enviar una solicitud al servidor Q 730 para actualizar la cadena de estado clave del usuario eliminado correspondiente al proyecto compartido. Por ejemplo, la solicitud puede indicar al servidor 730 que actualice la cadena de estado de clave S^{lt} del usuario t correspondiente al proyecto compartido de S^{lt} = $S_{lt,0}00\cdots0$ de vuelta a S^{lt} = $S_{lt,0}S_{lt,1}S_{lt,2}\cdots S_{lt,2J}$.$S^{lt}$ = $S_{lt,0}00\cdots0$ de vuelta a S^{lt} = $S_{lt,0}S_{lt,1}S_{lt,2}\cdots S_{lt,2J}$. El resto se puede gestionar automáticamente mediante el procedimiento de sincronización de valores de inicialización de claves FED para compartir grupos de archivos encriptados una vez más.

En las realizaciones de ejemplo descritas anteriormente, el sistema público ElGamal se ha utilizado como ejemplo para describir las realizaciones de los sistemas 200, 500, y 700. Otros sistemas de claves públicas (ver, por ejemplo, W. Diffie y M. Hellman, "New directions in cryptography", Transacciones IEEE sobre la teoría de la información, vol. 22, n.º 6, páginas 644 - 654, noviembre de 1976), tal como RSA y ECC también se pueden utilizar. Además, los sistemas descritos en este documento también pueden proporcionar una solución deseable para la administración de derechos digitales. Por ejemplo, se considere un proyecto compartido entre un proveedor de servicio de contenido y un usuario final, donde el proveedor de servicio de contenido actúa como el usuario administrativo del proyecto compartido. Con las realizaciones de los sistemas descritos en el presente documento, cualquier contenido creado/propiedad por el proveedor de servicio de contenido y comprado por el usuario final puede verse solo dentro de los agentes de encriptado del usuario final en los dispositivos del usuario final.

Se han descrito varias realizaciones de ejemplo en el presente documento. Sin embargo, los expertos en la técnica entenderán que pueden realizarse otras variaciones y modificaciones sin apartarse del alcance de las realizaciones como se define en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un procedimiento para proporcionar encriptado en una pluralidad de dispositivos (102a-1021) configurados para comunicación electrónica con un servidor (230), incluyendo la pluralidad de dispositivos (102a-1021) al menos un primer dispositivo (102a) y un segundo dispositivo (102b), comprendiendo el procedimiento:

generar una primera cuenta para un primer usuario (140) en control de la pluralidad de dispositivos (102a-1021), en el que la primera cuenta almacena datos de cuenta en una memoria de servidor no volátil, comprendiendo los datos de cuenta un identificador del primer usuario (140) e información de autentificación de la cuenta;
para cada dispositivo (102a-1021) en la pluralidad de dispositivos (102a-1021), instalar un agente (104) de encriptado en ese dispositivo (102a-1021);
operar un procesador del primer dispositivo (102a) bajo el control del agente (104) de encriptado para:

generar aleatoriamente una pluralidad de números aleatorios;
generar una pluralidad de números aleatorios encriptados a partir de la pluralidad de números aleatorios utilizando una clave de encriptado del segundo dispositivo, correspondiendo cada número aleatorio encriptado a uno de los números aleatorios en la pluralidad de números aleatorios;
transmitir la pluralidad de números aleatorios encriptados al servidor (230) para impedir la exposición de los números aleatorios al servidor (230);
generar una pluralidad de valores de inicialización (106) de claves basadas en la pluralidad de números aleatorios, en el que para cada valor de inicialización de clave, el agente (104) de encriptado es operable para controlar el procesador del primer dispositivo (102a) para generar una pluralidad de claves de encriptado independientes; y

almacenar información de valores de inicialización de clave basada en la pluralidad de valores de inicialización (106) de claves en la memoria del primer dispositivo no volátil;
generar una cadena de estado de clave para la primera cuenta, incluyendo la cadena de estado de clave una porción de número aleatorio de servidor generada basándose en la pluralidad de números aleatorios encriptados;
almacenar la cadena de estado clave en la memoria del servidor no volátil;
recibir información de autentificación putativa en el segundo dispositivo (102b);
operar un procesador del segundo dispositivo (102b), bajo el control del agente (104) de encriptado instalado en el segundo dispositivo (102b), para generar información de autentificación putativa del servidor basada en la información de autentificación putativa y transmitir la información de autentificación putativa del servidor al servidor (230); y
operar el procesador del servidor (230) para comparar la información de autentificación del servidor putativo con la información de autentificación de la cuenta, y proporcionar al segundo dispositivo (102b) acceso a la cadena de estado de clave si y solo si la información de autentificación del servidor putativo corresponde a la información de autentificación de la cuenta;
operar el procesador del segundo dispositivo (102b) bajo el control del agente (104) de encriptado para:

determinar la pluralidad de números aleatorios a partir de la pluralidad de números aleatorios encriptados en la cadena de estado de clave utilizando la clave de desencriptado del segundo dispositivo;
generar la pluralidad de valores de inicialización (106) de claves basándose en la pluralidad de números aleatorios, en el que para cada valor de inicialización de clave, el agente (104) de encriptado es operable para controlar el procesador del segundo dispositivo (102b) para generar la misma pluralidad claves de encriptado independientes como el primer dispositivo (102a), sin que ninguna de los valores de inicialización (106) de claves, información de valor de inicialización de clave y claves de encriptado se proporcionen al segundo dispositivo (102b); y
almacenar la información de valor de inicialización de clave basada en la pluralidad de valores de inicialización (106) de claves en la memoria del segundo dispositivo no volátil.

2. El procedimiento de acuerdo con la reivindicación 1, en el que:
la generación de la pluralidad de valores de inicialización (106) de claves en el primer dispositivo (102a) comprende, además:

operar el procesador del servidor para generar aleatoriamente los valores de clave de servidor para la primera cuenta, almacenar los valores de clave de servidor en la memoria del servidor no volátil, y transmitir los valores de la clave del servidor al primer dispositivo (102a); y
operar el procesador del primer dispositivo (102a) bajo el control del agente (104) de encriptado para generar la pluralidad de valores de inicialización (106) de claves basándose en los valores de la clave del servidor y la pluralidad de números aleatorios;
en el que:

el procesador del servidor es operado para proporcionar al segundo dispositivo (102b) acceso a los valores de clave del servidor si y solo si la información de autentificación del servidor putativo corresponde a la información de autentificación de la cuenta; y
el procesador del segundo dispositivo (102b) se opera, bajo el control del agente (104) de encriptado, para

generar la pluralidad de valores de inicialización (106) de claves basadas en la pluralidad de números aleatorios y los valores de la clave del servidor.

3. El procedimiento de acuerdo con la reivindicación 1, que comprende, además:

operar el procesador del primer dispositivo (102a), bajo el control del agente (104) de encriptado, para generar la pluralidad de números aleatorios encriptados mediante:

definir un primer código de verificación;
definir la clave de encriptado del segundo dispositivo basada en el primer código de verificación; y
encriptar la pluralidad de números aleatorios utilizando la clave de encriptado del segundo dispositivo;

en el que
la clave de desencriptado del segundo dispositivo se genera al operar el procesador del segundo dispositivo (102b) bajo el control del agente (104) de encriptado para definir un segundo código de verificación y generar la clave de desencriptado del segundo dispositivo basándose en el segundo código de verificación; y
el segundo código de verificación es el primer código de verificación.

4. El procedimiento de acuerdo con la reivindicación 3, que comprende, además:

proporcionar un archivo para encriptar y almacenar en el primer dispositivo (102a);
operar el procesador del primer dispositivo (102a) bajo el control del agente (104) de encriptado para derivar una de las claves de encriptado a partir de la información de valor de inicialización de clave utilizando información de generación de claves;
encriptar y almacenar el archivo como un archivo (108, 110) encriptado en la memoria del primer dispositivo no volátil utilizando la clave de encriptado derivada;
almacenar la información de generación de claves con el archivo (108, 110) encriptado en la memoria del primer dispositivo no volátil;
recibir el archivo (108, 110) encriptado y la información de generación de claves en el segundo dispositivo (102b); y
operar el procesador del segundo dispositivo (102b) bajo el control del agente (104) de encriptado para:

derivar la clave de encriptado a partir de la información de valor de inicialización de clave almacenada en la memoria del segundo dispositivo no volátil utilizando la información de generación de claves recibida; y
desencriptar el archivo (108, 110) encriptado utilizando la clave de encriptado derivada;

en el que la información de valor de inicialización de clave se encripta utilizando el primer código de verificación antes del almacenamiento.

5. El procedimiento de acuerdo con la reivindicación 1, en el que

el primer usuario (140) comprende una pluralidad de usuarios del grupo que incluyen al menos un usuario del grupo administrativo y un segundo usuario del grupo, teniendo cada uno de los usuarios del grupo el control de al menos uno de los dispositivos (102a-1021) en la pluralidad de dispositivos (102a-1021), en el que el usuario del grupo administrativo tiene el control del primer dispositivo (102a) y el segundo usuario del grupo tiene el control del segundo dispositivo (102b);
para cada usuario del grupo en la pluralidad de usuarios del grupo, los datos de la cuenta comprenden además una clave pública específica del usuario, en la que la clave pública específica del usuario para cada usuario se genera basándose en una clave privada específica del usuario almacenada en una memoria no volátil de un dispositivo correspondiente en la pluralidad de dispositivos (102a-1021); y
el procesador del primer dispositivo (102a) opera bajo el control del agente (104) de encriptado para generar la pluralidad de números aleatorios encriptados, para cada usuario del grupo en la pluralidad de usuarios del grupo:
generar una pluralidad de números aleatorios encriptados específicos del usuario utilizando la clave pública específica del usuario para ese usuario;
la porción del número aleatorio del servidor de la cadena de estado de clave para la primera cuenta comprende además, para cada usuario del grupo en la pluralidad de usuarios del grupo, una porción de la cadena específica del usuario que se genera en función de la pluralidad de números aleatorios encriptados específicos del usuario para ese usuario del grupo; y
el procesador del segundo dispositivo (102b) se opera bajo el control del agente (104) de encriptado para:
determinar la pluralidad de números aleatorios a partir de la pluralidad de números aleatorios encriptados específicos del usuario en la porción específica del usuario de la porción del número aleatorio del servidor correspondiente al segundo usuario del grupo que usa la segunda clave privada del dispositivo.

6. El procedimiento de acuerdo con la reivindicación 1, en el que el primer usuario (140) comprende una pluralidad de usuarios que incluyen un usuario administrativo que controla el primer dispositivo (102a) y un segundo usuario que controla el segundo dispositivo (102b), comprendiendo también el procedimiento transmitir una autorización del segundo usuario al segundo usuario mediante:

transmitir un identificador del segundo usuario del segundo usuario desde el primer dispositivo (102a) al servidor (230);
operar el procesador del servidor (230) para generar información de registro de segundo usuario basada en el identificador del segundo usuario y una contraseña del segundo usuario, almacenar la información de registro del segundo usuario en la memoria del servidor no volátil y transmitir una autorización de servidor del segundo usuario al segundo usuario;
recibir, por el segundo usuario, la autorización del servidor del segundo usuario y posteriormente instalar un agente (104) de encriptado en el segundo dispositivo (102b);
recibir una contraseña del segundo usuario putativo en el segundo dispositivo (102b);
operar el procesador del segundo dispositivo (102b) bajo el control del agente (104) de encriptado para generar información de registro del segundo usuario putativo basada en el identificador del segundo usuario y en la contraseña del segundo usuario putativo y transmitir la información de registro del segundo usuario putativo al servidor (230);
operar el procesador del servidor (230) para:

comparar la información de registro del segundo usuario putativo con la información de registro del segundo usuario almacenada;
autentificar el segundo dispositivo (102b) para la primera cuenta solo si la información de registro del segundo usuario putativo corresponde a la información de registro del segundo usuario almacenada;

operar el procesador del segundo dispositivo (102b) autentificado bajo el control del agente (104) de encriptado para:

generar la clave de desencriptado del segundo dispositivo;
generar la clave de encriptado del segundo dispositivo basada en la clave de desencriptado del segundo dispositivo; y
transmitir la clave de encriptado del segundo dispositivo al servidor (230);

recibir la clave de encriptado del segundo dispositivo en el primer dispositivo (102a); y
operar el procesador del primer dispositivo (102a) bajo el control del agente (104) de encriptado para generar la pluralidad de números aleatorios encriptados a partir de la pluralidad de números aleatorios usando la clave de encriptado del segundo dispositivo recibido.

7. El procedimiento de acuerdo con la reivindicación 1, en el que el primer usuario (140) comprende una pluralidad de usuarios que incluyen un usuario administrativo que controla el primer dispositivo (102a) y un segundo usuario que controla el segundo dispositivo (102b), comprendiendo el procedimiento también:

proporcionar un archivo para ser encriptado al primer dispositivo (102a);
operar el procesador del primer dispositivo (102a) bajo el control del agente (104) de encriptado para:

derivar una de las claves de encriptado a partir de la información de valor de inicialización de clave utilizando información de generación de claves; y
encriptar el archivo como un archivo (108, 110) encriptado utilizando la clave de encriptado derivada;

transmitir el archivo (108, 110) encriptado, la información de generación de claves y una autorización del segundo usuario al segundo usuario;
recibir, por el segundo usuario, la autorización del segundo usuario y posteriormente instalar un agente (104) de encriptado en el segundo dispositivo (102b);
recibir el archivo (108, 110) encriptado y la información de generación de claves en el segundo dispositivo (102b); y
operar el procesador del segundo dispositivo (102b) bajo el control del agente (104) de encriptado para:

derivar la clave de encriptado a partir de la información de valor de inicialización de clave almacenada en la memoria del segundo dispositivo no volátil utilizando la información de generación de claves recibida; y
desencriptar el archivo (108, 110) encriptado utilizando la clave de encriptado derivada.

8. Un producto de programa de ordenador para usar en una pluralidad de dispositivos (102a-1021) para proporcionar encriptación para la pluralidad de dispositivos (102a-1021), estando configurados la pluralidad de dispositivos (102a-1021) para comunicación electrónica con un servidor (230) e incluyendo al menos un primer dispositivo (102a) que tiene un primer procesador de dispositivo y una primera memoria de dispositivo no volátil y un segundo dispositivo (102b), teniendo el servidor (230) almacenado en el mismo una primera cuenta para un primer usuario (140) en control de la pluralidad de dispositivos (102a-1021), almacenando la primera cuenta datos de cuenta que comprenden un identificador del primer usuario (140) e información de autentificación de cuenta en una memoria de servidor no volátil, comprendiendo el producto de programa de ordenador:

un medio de grabación no transitorio; y
instrucciones grabadas en el medio de grabación, siendo las instrucciones para configurar el primer procesador del dispositivo para:

generar aleatoriamente una pluralidad de números aleatorios;
generar una pluralidad de números aleatorios encriptados a partir de la pluralidad de números aleatorios utilizando una clave de encriptado del segundo dispositivo, correspondiendo cada número aleatorio encriptado a uno de los números aleatorios en la pluralidad de números aleatorios, correspondiendo la clave de encriptado del segundo dispositivo a una clave de desencriptado del segundo dispositivo desconocido al servidor (230);
transmitir la pluralidad de números aleatorios encriptados al servidor (230) para impedir la exposición de los números aleatorios al servidor (230), siendo el servidor (230) operable para generar una cadena de estado de clave para la primera cuenta que incluye una porción de número aleatorio del servidor basado en la pluralidad de números aleatorios encriptados y para proporcionar al segundo dispositivo (102b) acceso a la cadena de estado de clave si y solo si la información de autentificación del servidor putativo recibida desde el segundo dispositivo (102b) corresponde a la información de autentificación de la cuenta;
generar una pluralidad de valores de inicialización (106) de claves basadas en la pluralidad de números aleatorios, en el que para cada valor de inicialización de clave, el primer procesador del dispositivo es operable para generar una pluralidad de claves de encriptado independientes;
almacenar información de valor de inicialización de clave basada en la pluralidad de valores de inicialización (106) de claves en la memoria del primer dispositivo no volátil;

en el que:
la pluralidad de números aleatorios se puede determinar en el segundo dispositivo (102b) a partir de la pluralidad de números aleatorios encriptados en la cadena de estado de clave utilizando la clave de desencriptado del segundo dispositivo, de manera que la misma pluralidad de valores de inicialización (106) de claves se puede generar en débase a la pluralidad de números aleatorios, y para cada valor de inicialización de clave, un procesador del segundo dispositivo (102b) puede generar la misma pluralidad de claves de encriptado independientes que el primer dispositivo (102a), sin proporcionar ninguno de valores de inicialización (106) de claves, información de valores de inicialización de claves y claves de encriptado al segundo dispositivo (102b).

9. El producto de programa de ordenador de acuerdo con la reivindicación 8, que comprende además instrucciones para configurar el primer procesador de dispositivo para generar la pluralidad de valores de inicialización (106) de claves mediante:

recibir una pluralidad de valores de claves de servidor generados aleatoriamente desde el servidor (230), almacenándose los valores de claves de servidor en la primera cuenta; y
generar la pluralidad de valores de inicialización (106) de claves basadas en los valores de claves del servidor y la pluralidad de números aleatorios.

10. El producto de programa de ordenador de acuerdo con la reivindicación 8, que comprende además instrucciones para configurar el primer procesador de dispositivo para:

definir un primer código de verificación;
definir la clave de encriptado del segundo dispositivo basada en el primer código de verificación; y
encriptar la pluralidad de números aleatorios utilizando la clave de encriptado del segundo dispositivo;
en el que la clave de desencriptado del segundo dispositivo también se genera basándose en el primer código de verificación.

11. El producto de programa de ordenador de acuerdo con la reivindicación 10, que comprende además instrucciones para configurar el primer procesador de dispositivo para:

recibir un archivo para ser encriptado;
derivar una de las claves de encriptado a partir de la información de valor de inicialización de clave utilizando información de generación de claves;
encriptar y almacenar el archivo como un archivo (108, 110) encriptado en la memoria del primer dispositivo no volátil utilizando la clave de encriptado derivada;
almacenar la información de generación de claves con el archivo (108, 110) encriptado en la memoria del primer dispositivo no volátil;
encriptar la información de valor de inicialización de clave utilizando el primer código de verificación antes del almacenamiento;
y el producto de programa de ordenador comprende instrucciones para configurar el procesador del segundo dispositivo (102b) para
recibir el archivo (108, 110) encriptado e información de generación de claves;
derivar la clave de encriptado a partir de la información de valor de inicialización de claves almacenada en una memoria no volátil del segundo dispositivo del segundo dispositivo (102b) utilizando la información de generación de claves recibida; y
desencriptar el archivo (108, 110) encriptado utilizando la clave de encriptado derivada.

12. El producto de programa de ordenador de acuerdo con la reivindicación 8, en el que:

el primer usuario (140) comprende una pluralidad de usuarios del grupo que incluyen al menos un usuario del grupo administrativo y un segundo usuario del grupo, teniendo cada uno de los usuarios del grupo el control de al menos uno de los dispositivos en la pluralidad de dispositivos (102a-1021), en el que el usuario del grupo administrativo tiene el control del primer dispositivo (102a) y el segundo usuario del grupo tiene el control del segundo dispositivo (102b);
para cada usuario del grupo en la pluralidad de usuarios del grupo, los datos de la cuenta comprenden además una clave pública específica del usuario, en la que la clave pública específica del usuario para cada usuario se genera en base a una clave privada específica del usuario almacenada en una memoria no volátil de un dispositivo correspondiente en la pluralidad de dispositivos (102a-1021); y
el producto de programa de ordenador comprende además instrucciones para configurar el primer procesador de dispositivo para:

generar la pluralidad de números aleatorios encriptados, para cada usuario del grupo en la pluralidad de usuarios del grupo, generando una pluralidad de números aleatorios encriptados específicos del usuario utilizando la clave pública específica del usuario para ese usuario; y
transmitir la pluralidad de números aleatorios encriptados específicos del usuario al servidor (230), siendo el servidor (230) operable para generar la porción del número aleatorio del servidor de la cadena de estado de clave generando, para cada usuario del grupo en la pluralidad de usuarios del grupo, una porción de cadena específica del usuario basada en la pluralidad de números aleatorios encriptados específicos del usuario para ese usuario del grupo; y

la pluralidad de números aleatorios es determinable en el segundo dispositivo (102b) a partir de la pluralidad de números aleatorios encriptados específicos del usuario en la porción específica del usuario de la porción del número aleatorio del servidor correspondiente al segundo usuario del grupo que usa la segunda clave privada del dispositivo.

13. El producto de programa de ordenador de acuerdo con la reivindicación 8, en el que:

el primer usuario (140) comprende una pluralidad de usuarios que incluyen un usuario administrativo que controla el primer dispositivo (102a) y un segundo usuario que controla el segundo dispositivo (102b); y
el producto de programa de ordenador comprende además instrucciones para configurar el primer procesador de dispositivo para transmitir una autorización del segundo usuario al segundo usuario transmitiendo un identificador del segundo usuario del segundo usuario desde el primer dispositivo (102a) al servidor (230), siendo el servidor (230) operable para generar información de registro de segundo usuario basada en el identificador del segundo usuario y una contraseña del segundo usuario, almacenar la información de registro de segundo usuario en la memoria del servidor no volátil y transmitir una autorización de servidor de segundo usuario al segundo usuario; y
el producto de programa de ordenador comprende además instrucciones para configurar un procesador del segundo dispositivo (102b), cuando se instala en el mismo, para:

recibir una contraseña del segundo usuario putativo;
generar información de registro del segundo usuario putativo basada en el identificador del segundo usuario y la contraseña del segundo usuario putativo;
transmitir la información de registro del segundo usuario putativo al servidor (230), siendo el servidor (230) operable para comparar la información de registro del segundo usuario putativo con la información de registro de segundo usuario almacenada, y autentificar el segundo dispositivo (102b) solo para la primera cuenta si la información de registro de segundo usuario putativo corresponde a la información de registro de segundo usuario almacenada; y una vez autentificado el segundo dispositivo (102b),
generar la clave de desencriptado del segundo dispositivo;
generar la clave de encriptado del segundo dispositivo basada en la clave de desencriptado del segundo dispositivo; y
transmitir la clave de encriptado del segundo dispositivo al servidor (230); y

el producto de programa de ordenador comprende además instrucciones para configurar el primer procesador de dispositivo para recibir la clave de encriptado del segundo dispositivo y generar la pluralidad de números aleatorios encriptados a partir de la pluralidad de números aleatorios utilizando la clave de encriptado del segundo dispositivo recibida.

14. El producto de programa de ordenador de acuerdo con la reivindicación 8, en el que:

el primer usuario (140) comprende una pluralidad de usuarios que incluyen un usuario administrativo que controla el primer dispositivo (102a) y un segundo usuario que controla el segundo dispositivo (102b); y
el producto de programa de ordenador, que comprende además instrucciones para configurar el primer procesador de dispositivo para:

recibir un archivo para ser encriptado;
derivar una de las claves de encriptado a partir de la información de valor de inicialización de clave utilizando información de generación de claves;
encriptar el archivo como un archivo (108, 110) encriptado utilizando la clave de encriptado derivada;
transmitir el archivo (108, 110) encriptado, la información de generación de claves y una autorización del segundo usuario al segundo usuario; y

el producto de programa de ordenador comprende además instrucciones para configurar un procesador del segundo dispositivo (102b), cuando se instala en el mismo, para:

registrar el segundo dispositivo (102b) con el servidor (230) según la autorización del segundo usuario;
determinar la pluralidad de números aleatorios basándose en la pluralidad de números aleatorios encriptados en la cadena de estado de clave utilizando la clave de desencriptado del segundo dispositivo;
generar la pluralidad de valores de inicialización (106) de claves basadas en la pluralidad de números aleatorios;
almacenar información de valor de inicialización de clave basada en los valores de inicialización (106) de claves en una memoria del segundo dispositivo no volátil;
recibir el archivo (108, 110) encriptado y la información de generación de claves;
derivar la clave de encriptado a partir de la información de valor de inicialización de clave almacenada en la memoria del segundo dispositivo no volátil utilizando la información de generación de claves recibida; y
desencriptar el archivo (108, 110) encriptado utilizando la clave de encriptado derivada.

15. Un dispositivo para proporcionar encriptado para una pluralidad de dispositivos (102a-1021) incluyendo el dispositivo, estando cada dispositivo configurado para la comunicación electrónica con un servidor (230), teniendo el servidor (230) almacenado en el mismo una primera cuenta para un primer usuario (140) en control de la pluralidad de dispositivos (102a-1021), almacenando la primera cuenta datos de cuenta que comprenden un identificador del primer usuario (140) e información de autentificación de cuenta en una memoria de servidor no volátil, comprendiendo el dispositivo:

un procesador; y
una memoria de dispositivo no volátil que tiene almacenadas en la misma instrucciones para configurar el procesador para:

generar aleatoriamente una pluralidad de números aleatorios;
generar una pluralidad de números aleatorios encriptados a partir de la pluralidad de números aleatorios utilizando una clave de encriptado del segundo dispositivo, correspondiendo cada número aleatorio encriptado a uno de los números aleatorios en la pluralidad de números aleatorios, correspondiendo la clave de encriptado del segundo dispositivo a una clave de desencriptado del segundo dispositivo desconocido para el servidor (230);
transmitir la pluralidad de números aleatorios encriptados al servidor (230) para impedir la exposición de los números aleatorios al servidor (230), pudiendo el servidor (230) operar para generar una cadena de estado de clave para la primera cuenta que incluye una porción de número aleatorio del servidor basada en la pluralidad de números aleatorios encriptados y para proporcionar un segundo dispositivo (102b) en la pluralidad de dispositivos (102a-1021) con acceso a la cadena de estado de clave si y solo si la información de autentificación del servidor putativo que se recibe de ese dispositivo corresponde a la información de autentificación de la cuenta;
generar una pluralidad de valores de inicialización (106) de claves basadas en la pluralidad de números aleatorios, en el que para cada valor de inicialización de clave, el procesador es operable para generar una pluralidad de claves de encriptado independientes;
almacenar información de valor de inicialización de clave basada en la pluralidad de valores de inicialización (106) de claves en la memoria del dispositivo no volátil;
en el que la pluralidad de números aleatorios se puede determinar en el segundo dispositivo (102b) a partir de la pluralidad de números aleatorios encriptados en la cadena de estado de clave usando la clave de desencriptado del segundo dispositivo de tal manera que la misma pluralidad de valores de inicialización (106) de claves se puede generar basándose en una pluralidad de números aleatorios, y para cada valor de inicialización de claves, pudiendo generar un procesador del segundo dispositivo (102b) la misma pluralidad de claves de encriptado independientes que el dispositivo, sin proporcionar ninguno de valores de inicialización (106) de claves, información de valores de inicialización de claves y las claves de encriptado al segundo dispositivo (102b).

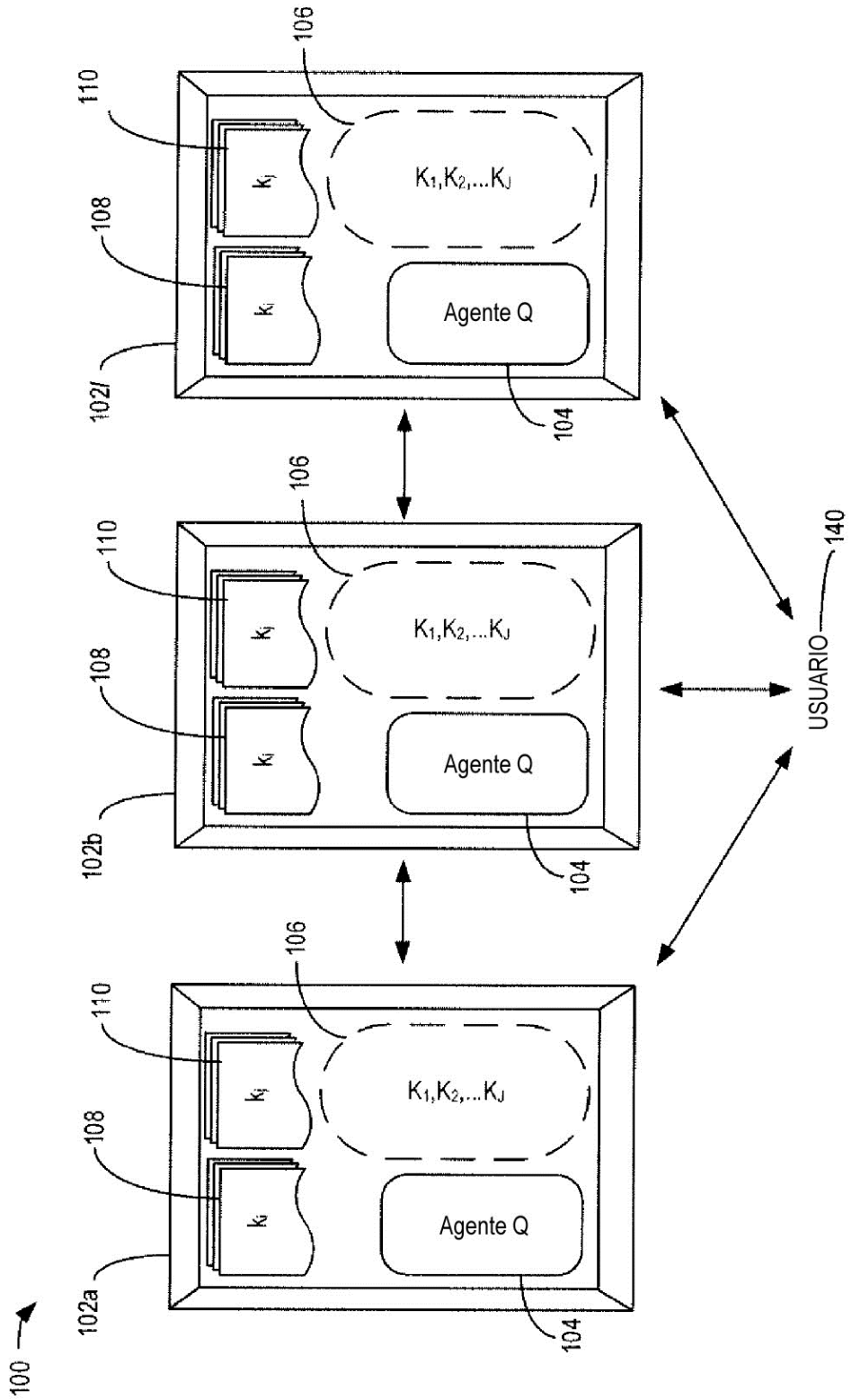
100
102a
102b
102l
104
106
108
110
140
USUARIO
Agente Q
K1,K2,...KJ

FIG. 1

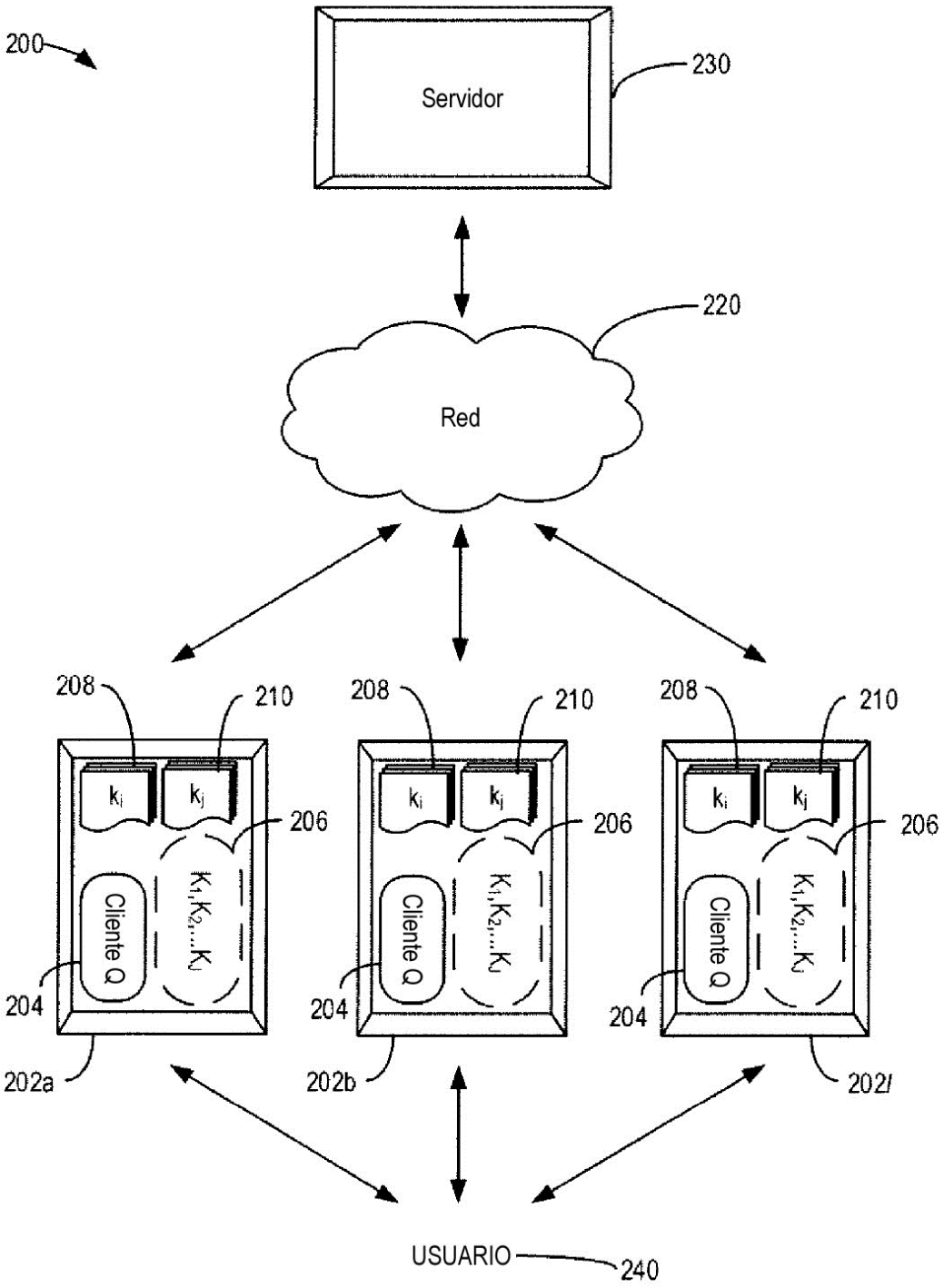
200
Servidor
230
220
Red
208
210
206
k_i
k_j
Cliente Q
$K_1,K_2,...K_J$
204
202a
202b
202l
USUARIO
240

FIG. 2

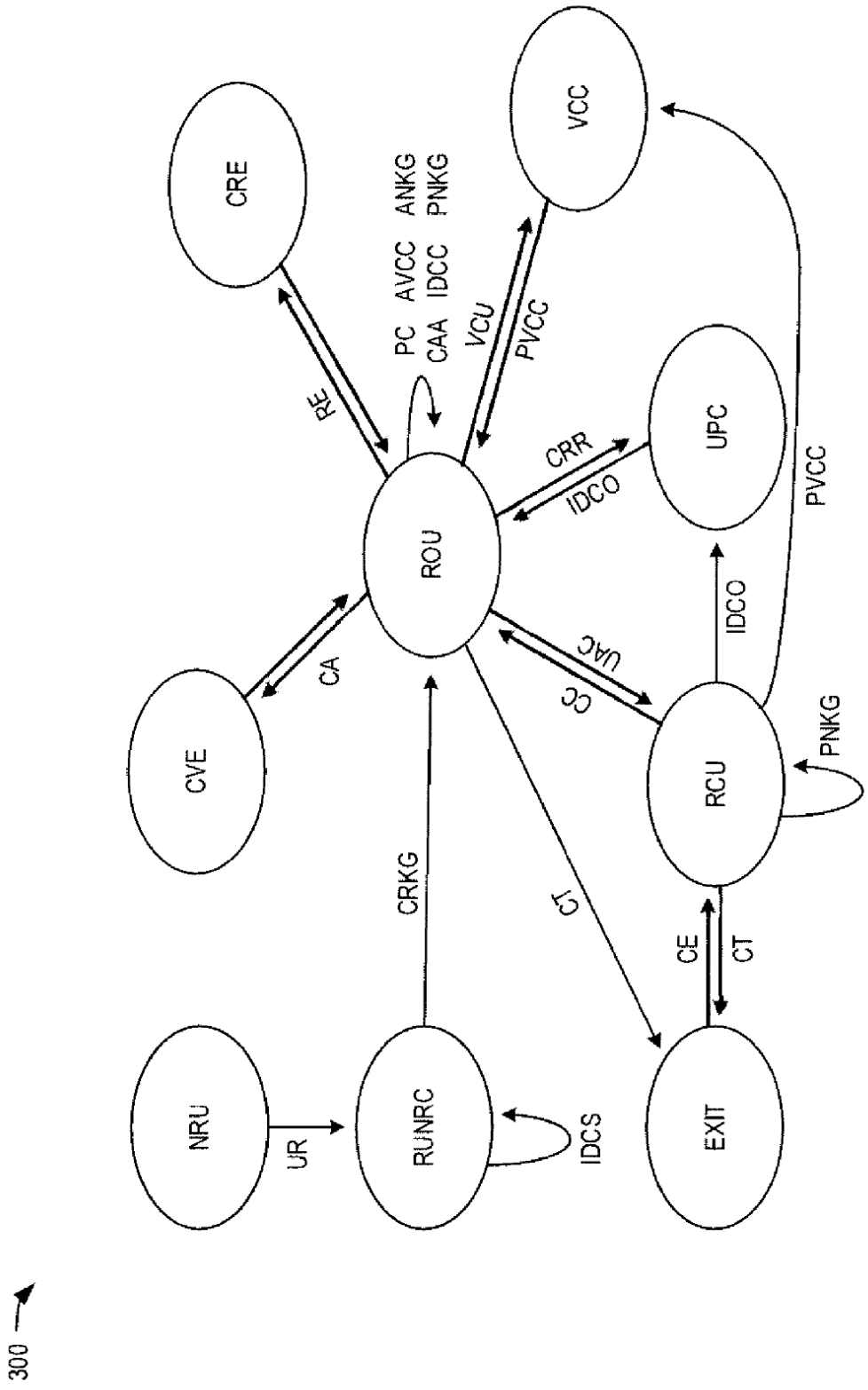
300
NRU
UR
RUNRC
IDCS
CRKG
CVE
CA
ROU
RE
CRE
PC AVCC ANKG
CAA IDCC PNKG
VCU
PVCC
VCC
CRR
IDCO
UPC
PVCC
UAC
CC
IDCO
RCU
PNKG
CJ
CE
CT
EXIT

FIG. 3

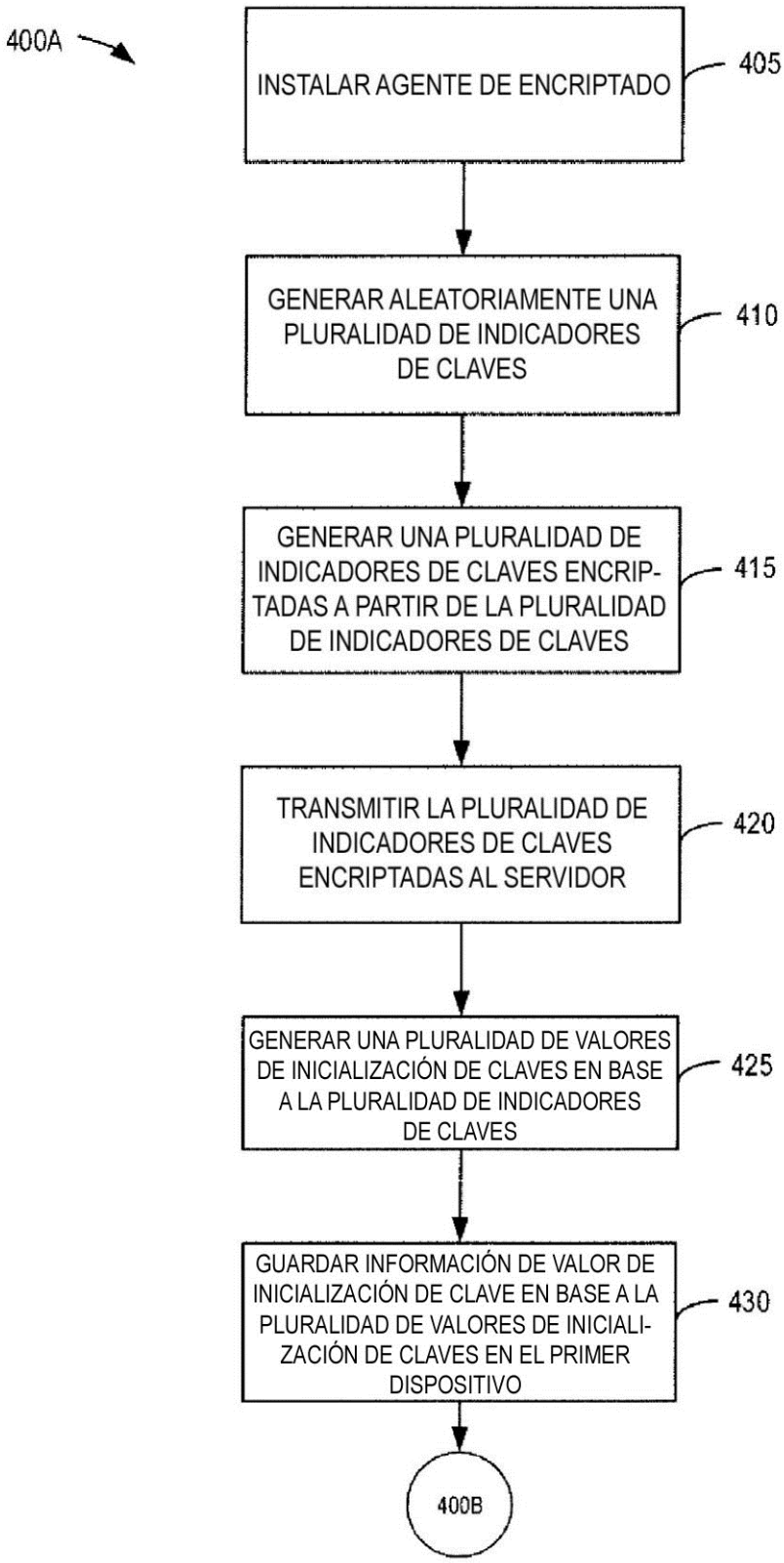
400A
INSTALAR AGENTE DE ENCRIPTADO
405
GENERAR ALEATORIAMENTE UNA PLURALIDAD DE INDICADORES DE CLAVES
410
GENERAR UNA PLURALIDAD DE INDICADORES DE CLAVES ENCRIPTADAS A PARTIR DE LA PLURALIDAD DE INDICADORES DE CLAVES
415
TRANSMITIR LA PLURALIDAD DE INDICADORES DE CLAVES ENCRIPTADAS AL SERVIDOR
420
GENERAR UNA PLURALIDAD DE VALORES DE INICIALIZACIÓN DE CLAVES EN BASE A LA PLURALIDAD DE INDICADORES DE CLAVES
425
GUARDAR INFORMACIÓN DE VALOR DE INICIALIZACIÓN DE CLAVE EN BASE A LA PLURALIDAD DE VALORES DE INICIALIZACIÓN DE CLAVES EN EL PRIMER DISPOSITIVO
430
400B

FIG. 4A

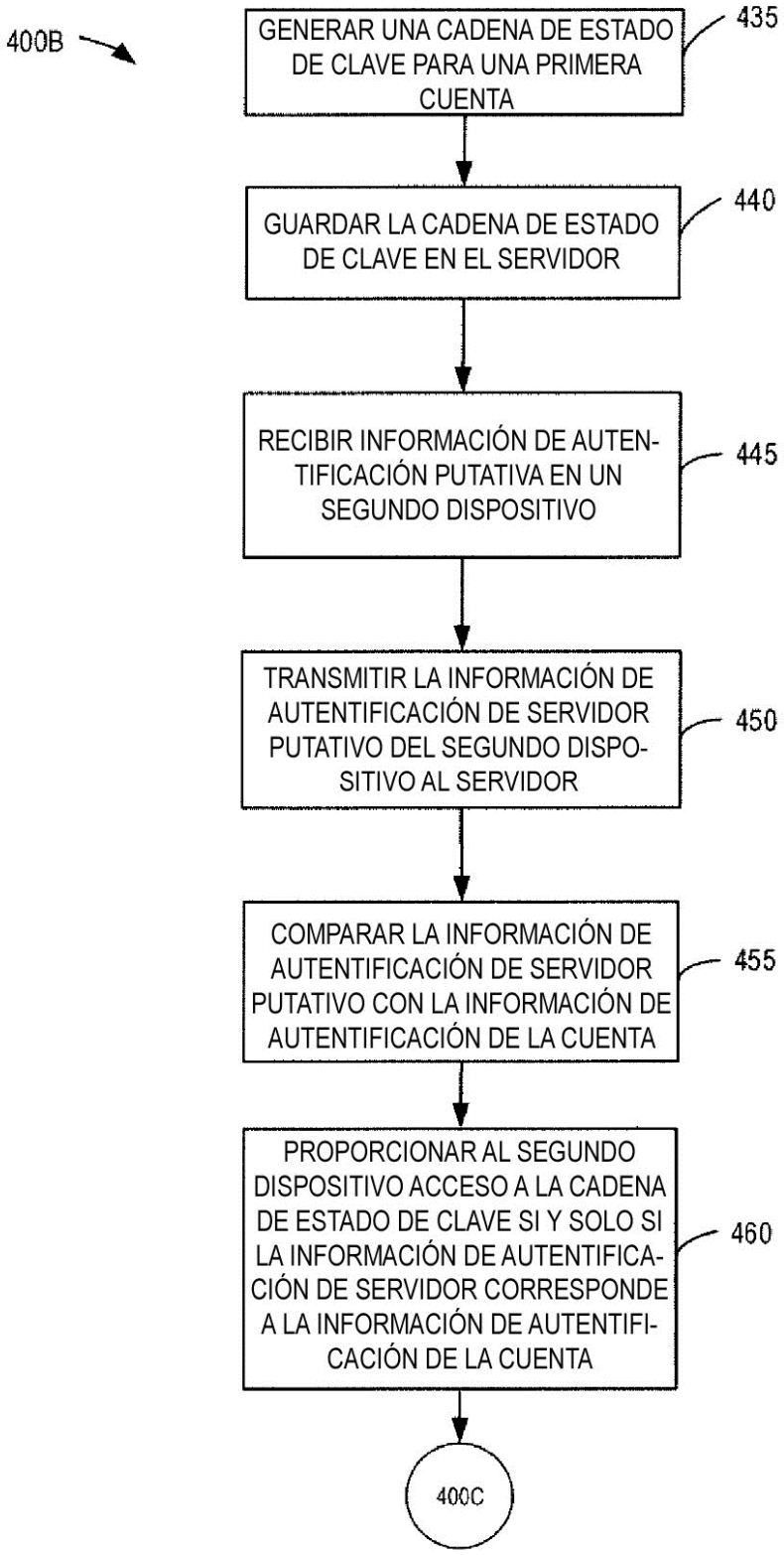
400B
GENERAR UNA CADENA DE ESTADO DE CLAVE PARA UNA PRIMERA CUENTA
435
GUARDAR LA CADENA DE ESTADO DE CLAVE EN EL SERVIDOR
440
RECIBIR INFORMACIÓN DE AUTENTIFICACIÓN PUTATIVA EN UN SEGUNDO DISPOSITIVO
445
TRANSMITIR LA INFORMACIÓN DE AUTENTIFICACIÓN DE SERVIDOR PUTATIVO DEL SEGUNDO DISPOSITIVO AL SERVIDOR
450
COMPARAR LA INFORMACIÓN DE AUTENTIFICACIÓN DE SERVIDOR PUTATIVO CON LA INFORMACIÓN DE AUTENTIFICACIÓN DE LA CUENTA
455
PROPORCIONAR AL SEGUNDO DISPOSITIVO ACCESO A LA CADENA DE ESTADO DE CLAVE SI Y SOLO SI LA INFORMACIÓN DE AUTENTIFICACIÓN DE SERVIDOR CORRESPONDE A LA INFORMACIÓN DE AUTENTIFICACIÓN DE LA CUENTA
460
400C

FIG. 4B

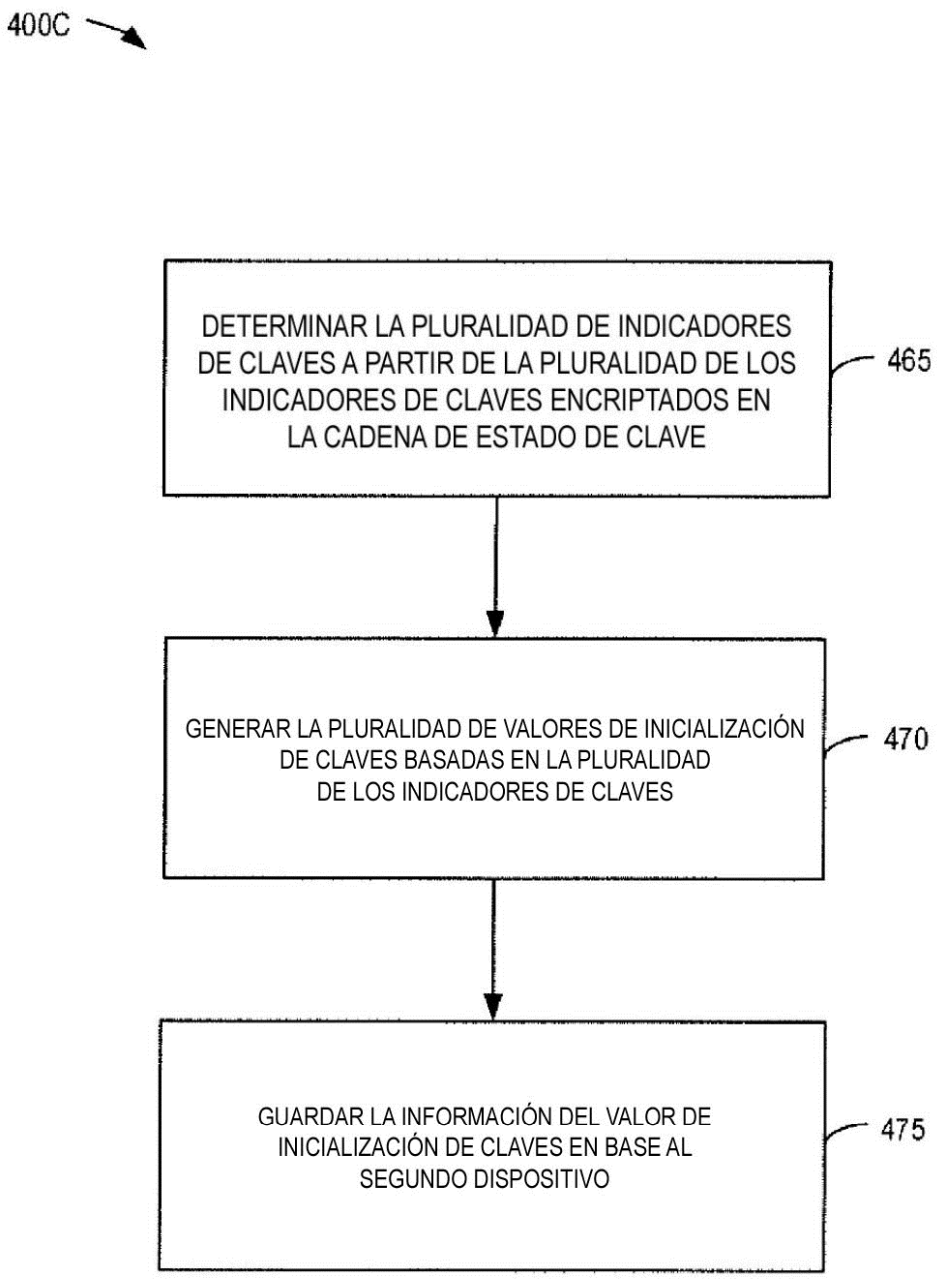
400C
DETERMINAR LA PLURALIDAD DE INDICADORES DE CLAVES A PARTIR DE LA PLURALIDAD DE LOS INDICADORES DE CLAVES ENCRIPTADOS EN LA CADENA DE ESTADO DE CLAVE
465
GENERAR LA PLURALIDAD DE VALORES DE INICIALIZACIÓN DE CLAVES BASADAS EN LA PLURALIDAD DE LOS INDICADORES DE CLAVES
470
GUARDAR LA INFORMACIÓN DEL VALOR DE INICIALIZACIÓN DE CLAVES EN BASE AL SEGUNDO DISPOSITIVO
475

FIG. 4C

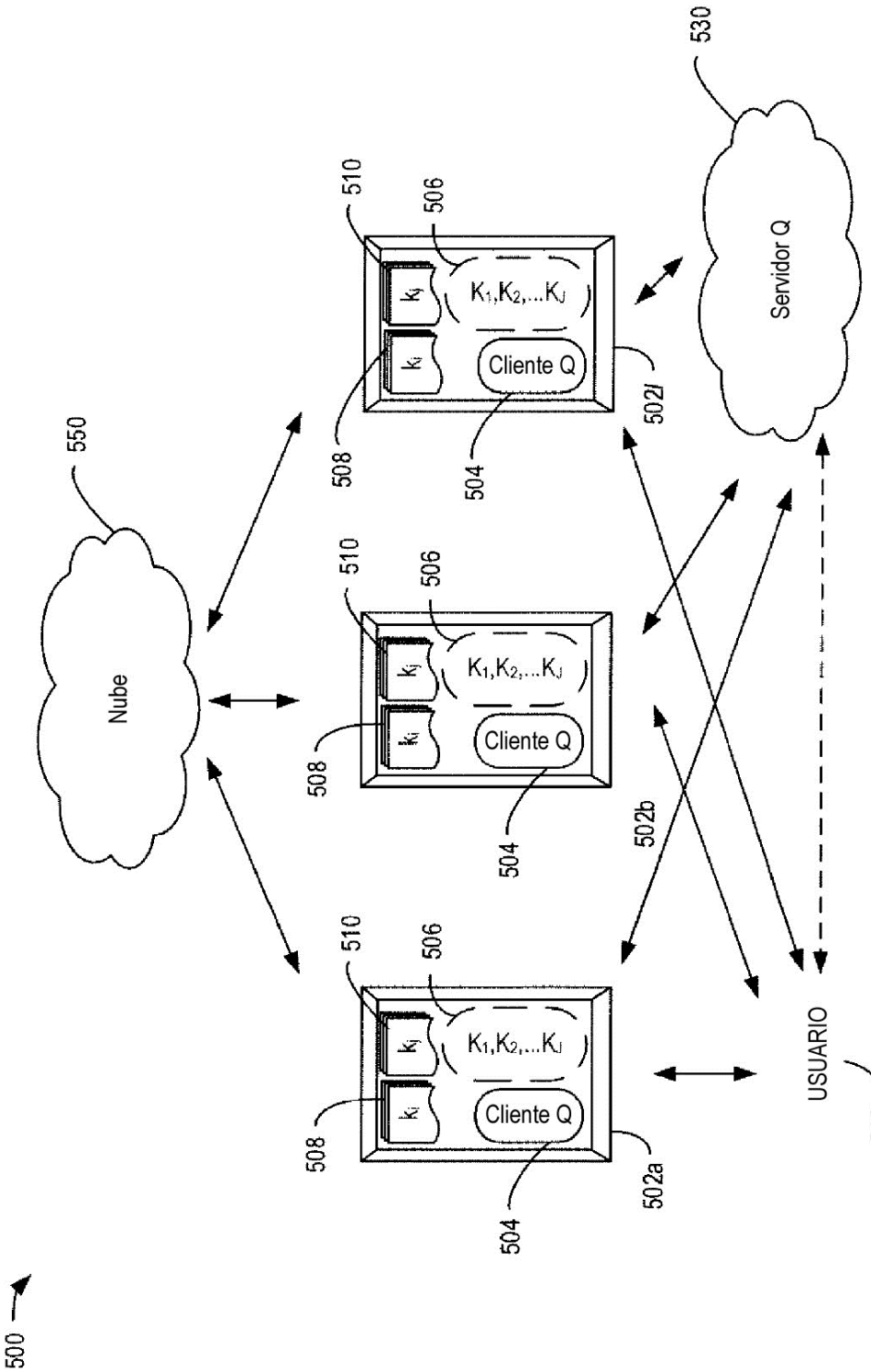
500
Nube
550
Servidor Q
530
USUARIO
540
Cliente Q
$K_1, K_2, ...K_J$
k_j
k_i
502a
502b
502l
504
506
508
510

FIG. 5

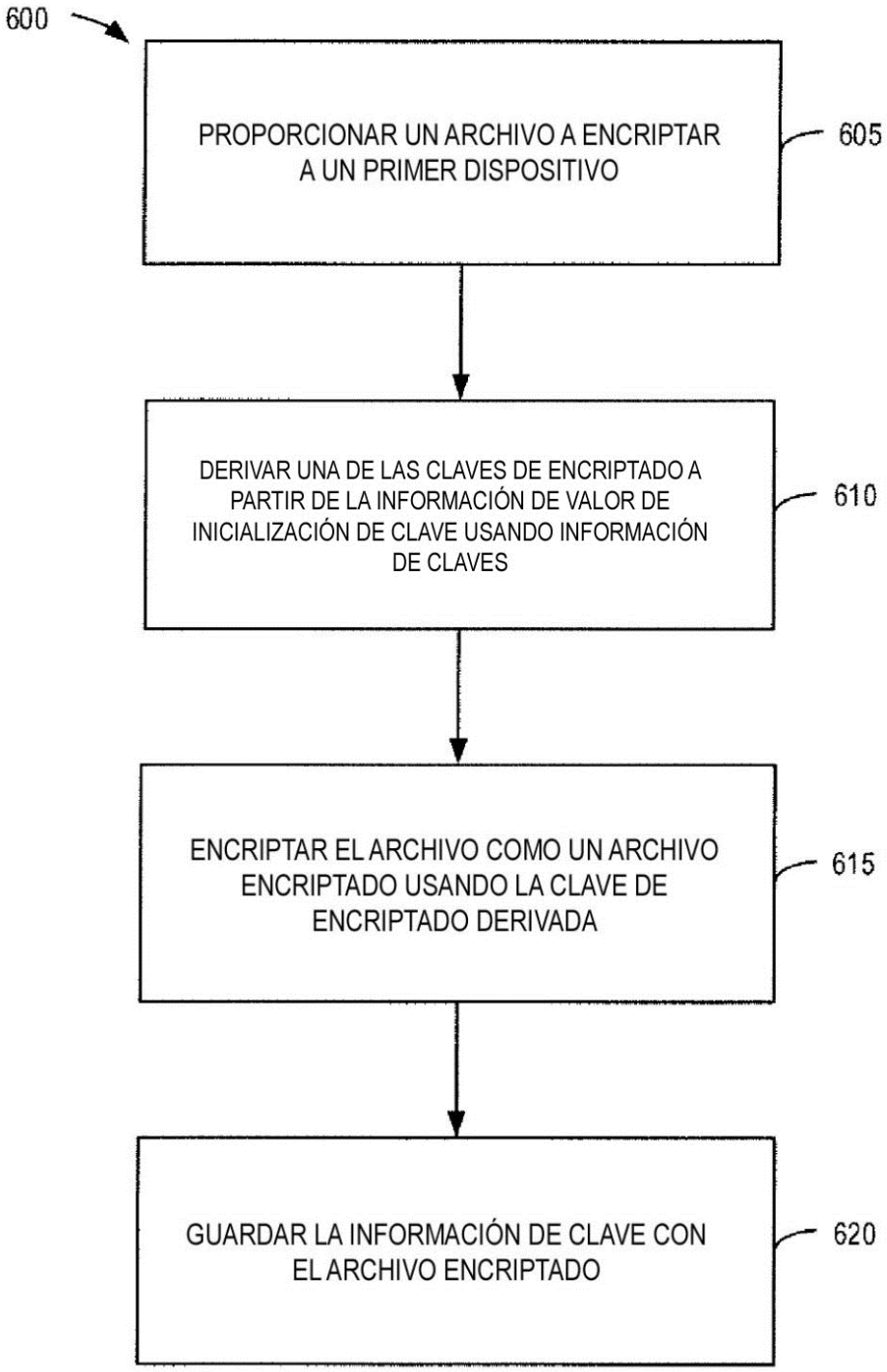
600
PROPORCIONAR UN ARCHIVO A ENCRIPTAR A UN PRIMER DISPOSITIVO
605
DERIVAR UNA DE LAS CLAVES DE ENCRIPTADO A PARTIR DE LA INFORMACIÓN DE VALOR DE INICIALIZACIÓN DE CLAVE USANDO INFORMACIÓN DE CLAVES
610
ENCRIPTAR EL ARCHIVO COMO UN ARCHIVO ENCRIPTADO USANDO LA CLAVE DE ENCRIPTADO DERIVADA
615
GUARDAR LA INFORMACIÓN DE CLAVE CON EL ARCHIVO ENCRIPTADO
620

FIG. 6A

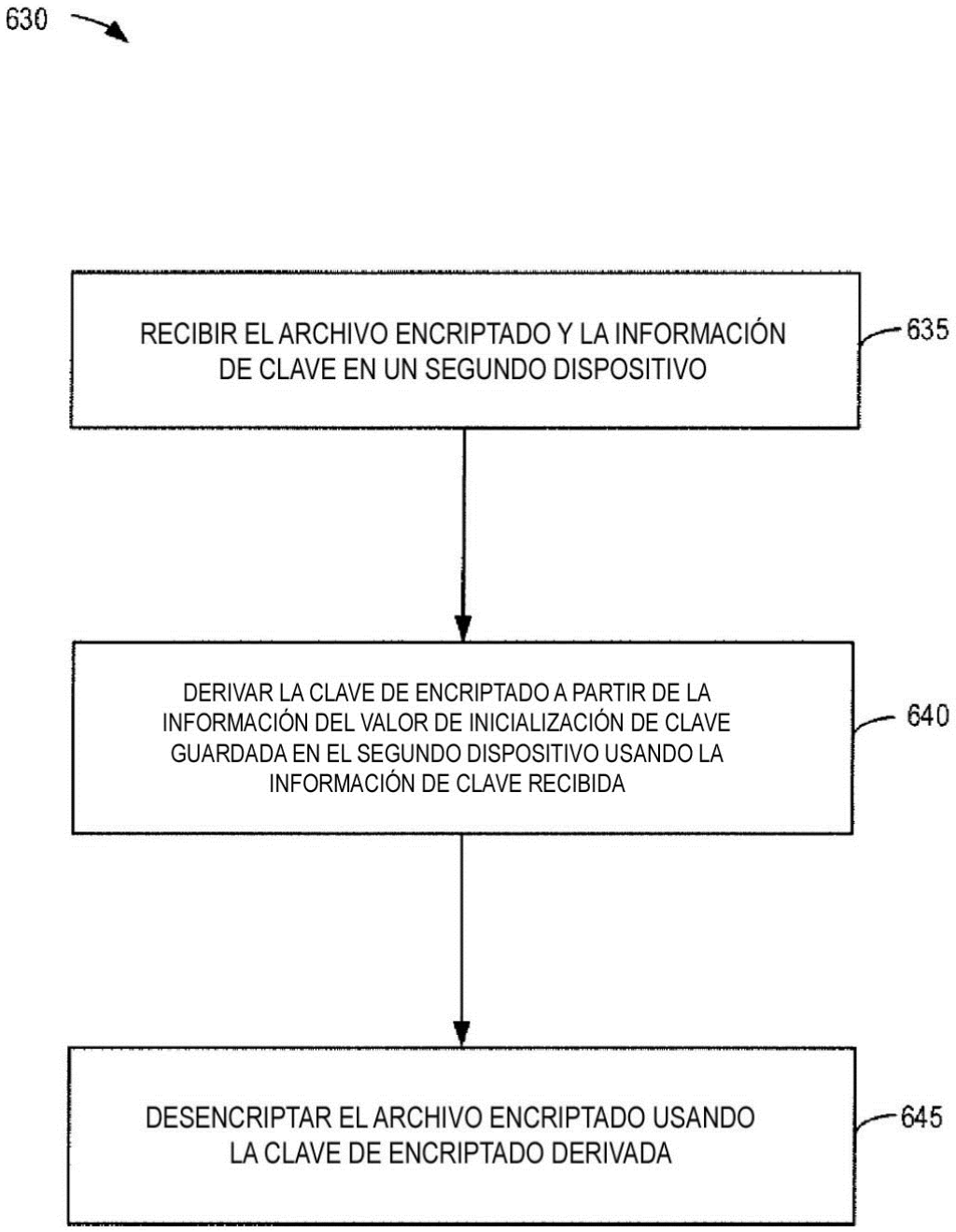
630
RECIBIR EL ARCHIVO ENCRIPTADO Y LA INFORMACIÓN DE CLAVE EN UN SEGUNDO DISPOSITIVO
635
DERIVAR LA CLAVE DE ENCRIPTADO A PARTIR DE LA INFORMACIÓN DEL VALOR DE INICIALIZACIÓN DE CLAVE GUARDADA EN EL SEGUNDO DISPOSITIVO USANDO LA INFORMACIÓN DE CLAVE RECIBIDA
640
DESENCRIPTAR EL ARCHIVO ENCRIPTADO USANDO LA CLAVE DE ENCRIPTADO DERIVADA
645

FIG. 6B

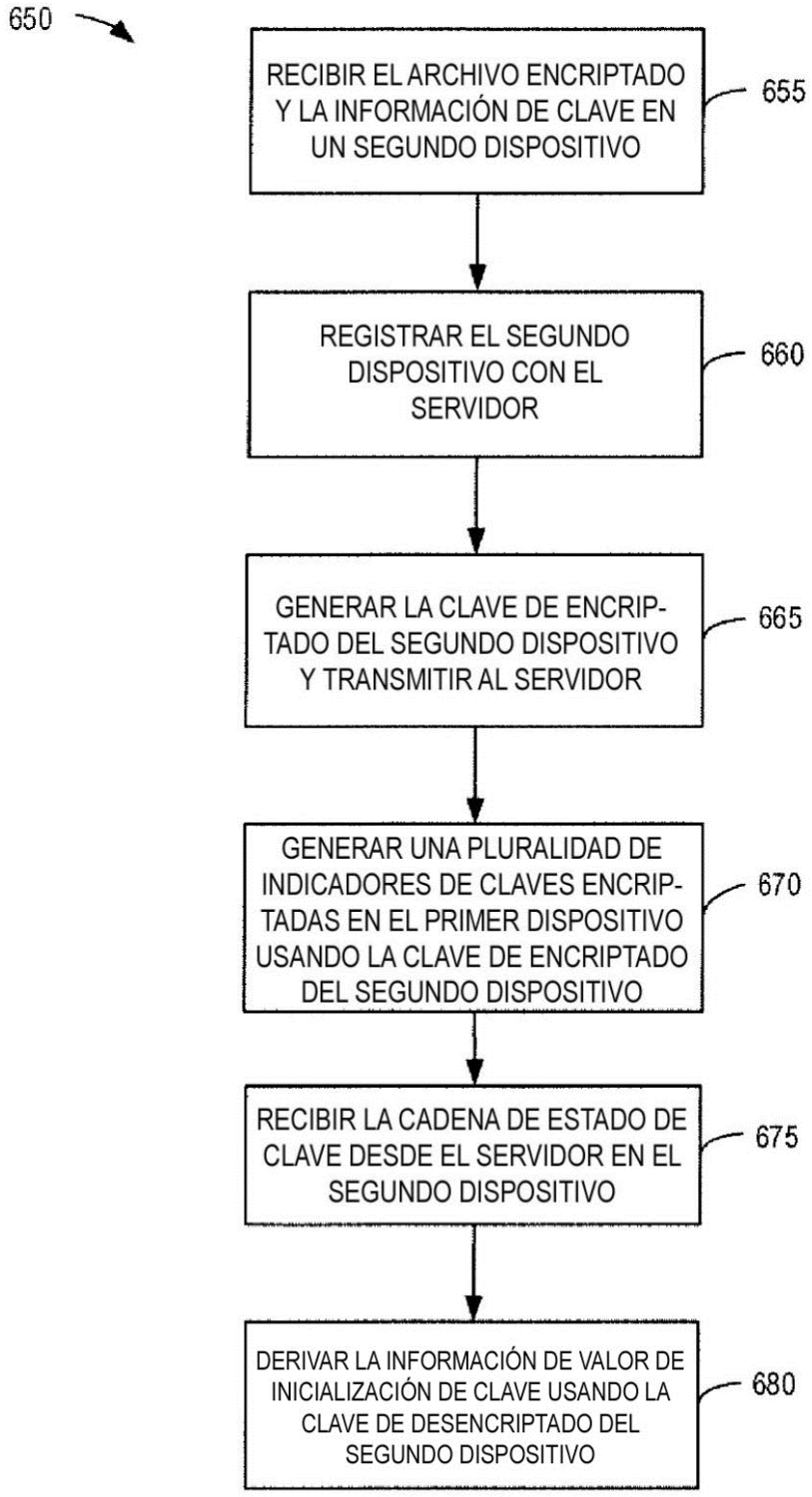
650
RECIBIR EL ARCHIVO ENCRIPTADO Y LA INFORMACIÓN DE CLAVE EN UN SEGUNDO DISPOSITIVO
655
REGISTRAR EL SEGUNDO DISPOSITIVO CON EL SERVIDOR
660
GENERAR LA CLAVE DE ENCRIP-TADO DEL SEGUNDO DISPOSITIVO Y TRANSMITIR AL SERVIDOR
665
GENERAR UNA PLURALIDAD DE INDICADORES DE CLAVES ENCRIP-TADAS EN EL PRIMER DISPOSITIVO USANDO LA CLAVE DE ENCRIPTADO DEL SEGUNDO DISPOSITIVO
670
RECIBIR LA CADENA DE ESTADO DE CLAVE DESDE EL SERVIDOR EN EL SEGUNDO DISPOSITIVO
675
DERIVAR LA INFORMACIÓN DE VALOR DE INICIALIZACIÓN DE CLAVE USANDO LA CLAVE DE DESENCRIPTADO DEL SEGUNDO DISPOSITIVO
680

FIG. 6C

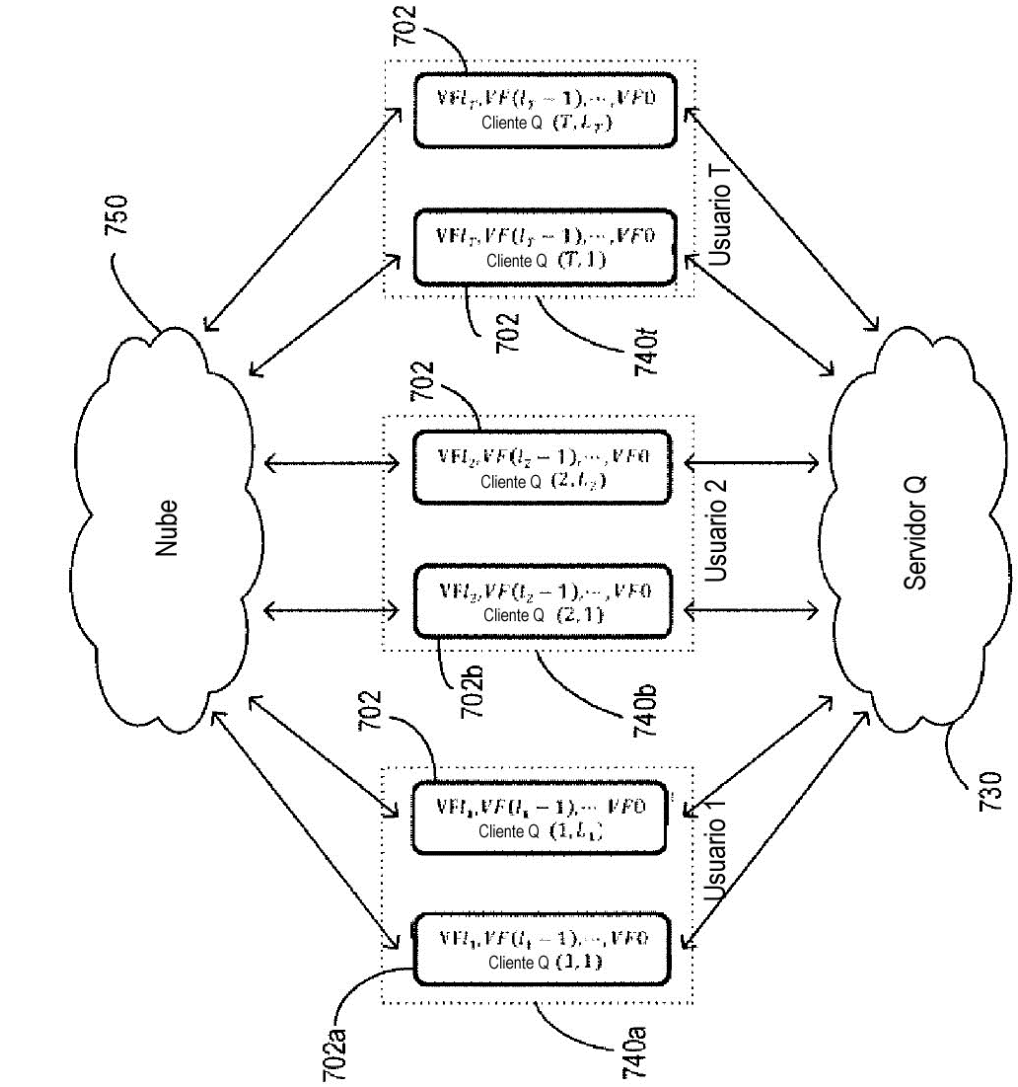
700
750
Nube
Servidor Q
730
Usuario T
Usuario 2
Usuario 1
Cliente Q (T, L_T)
Cliente Q $(T, 1)$
Cliente Q $(2, L_2)$
Cliente Q $(2, 1)$
Cliente Q $(1, L_1)$
Cliente Q $(1, 1)$
702
740t
702b
740b
702a
740a

FIG. 7

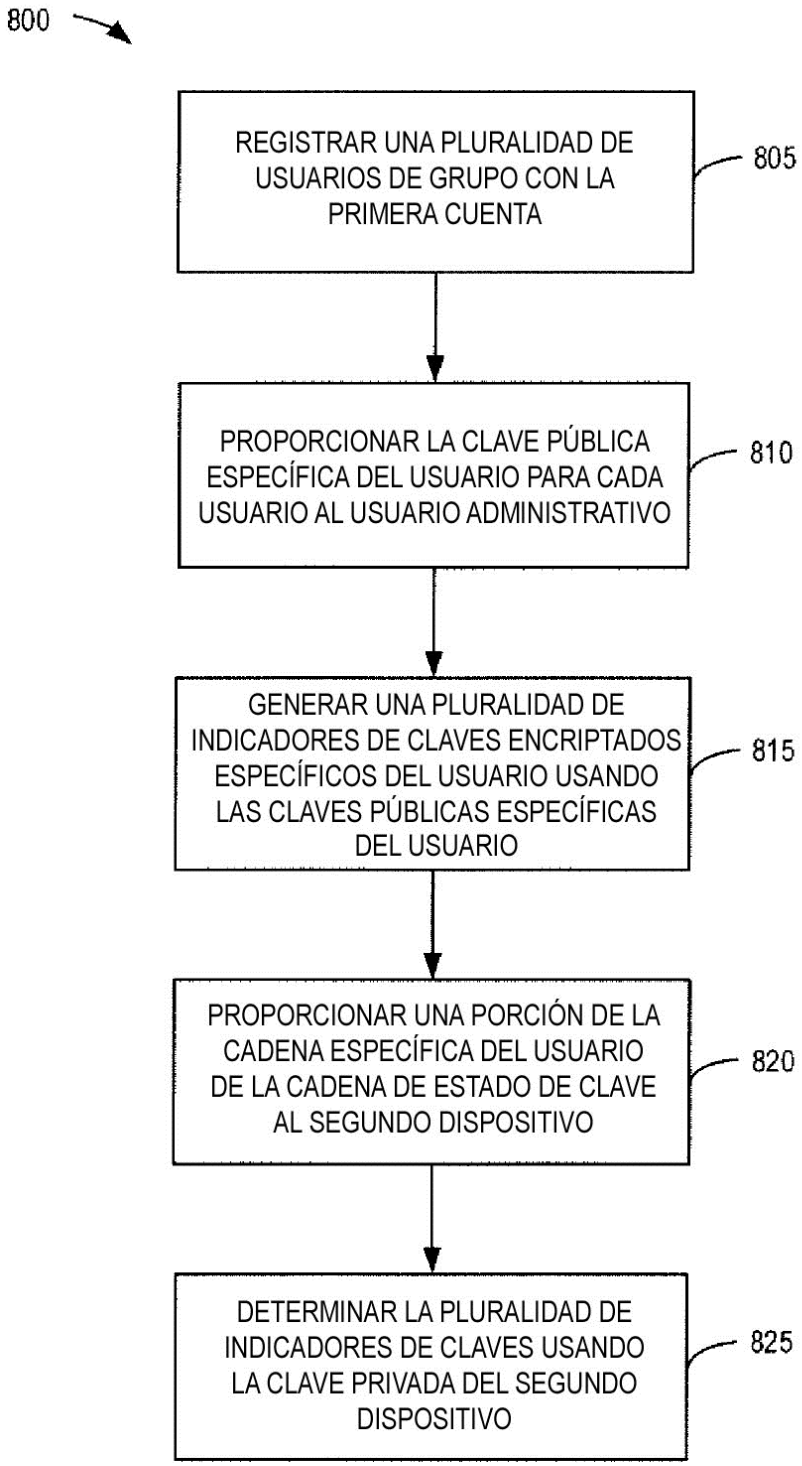
800
REGISTRAR UNA PLURALIDAD DE USUARIOS DE GRUPO CON LA PRIMERA CUENTA
805
PROPORCIONAR LA CLAVE PÚBLICA ESPECÍFICA DEL USUARIO PARA CADA USUARIO AL USUARIO ADMINISTRATIVO
810
GENERAR UNA PLURALIDAD DE INDICADORES DE CLAVES ENCRIPTADOS ESPECÍFICOS DEL USUARIO USANDO LAS CLAVES PÚBLICAS ESPECÍFICAS DEL USUARIO
815
PROPORCIONAR UNA PORCIÓN DE LA CADENA ESPECÍFICA DEL USUARIO DE LA CADENA DE ESTADO DE CLAVE AL SEGUNDO DISPOSITIVO
820
DETERMINAR LA PLURALIDAD DE INDICADORES DE CLAVES USANDO LA CLAVE PRIVADA DEL SEGUNDO DISPOSITIVO
825

FIG. 8

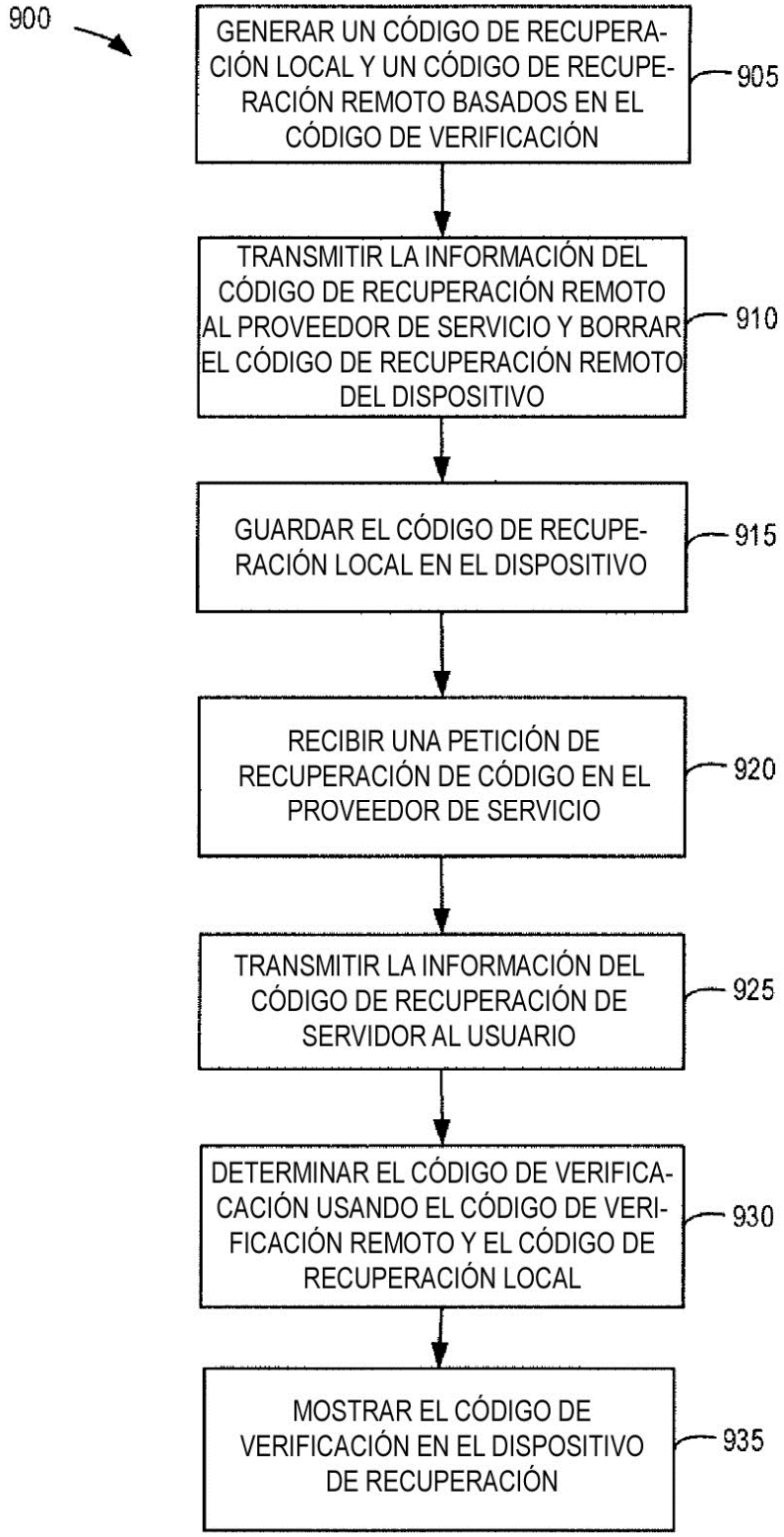
900
GENERAR UN CÓDIGO DE RECUPERACIÓN LOCAL Y UN CÓDIGO DE RECUPERACIÓN REMOTO BASADOS EN EL CÓDIGO DE VERIFICACIÓN
905
TRANSMITIR LA INFORMACIÓN DEL CÓDIGO DE RECUPERACIÓN REMOTO AL PROVEEDOR DE SERVICIO Y BORRAR EL CÓDIGO DE RECUPERACIÓN REMOTO DEL DISPOSITIVO
910
GUARDAR EL CÓDIGO DE RECUPERACIÓN LOCAL EN EL DISPOSITIVO
915
RECIBIR UNA PETICIÓN DE RECUPERACIÓN DE CÓDIGO EN EL PROVEEDOR DE SERVICIO
920
TRANSMITIR LA INFORMACIÓN DEL CÓDIGO DE RECUPERACIÓN DE SERVIDOR AL USUARIO
925
DETERMINAR EL CÓDIGO DE VERIFICACIÓN USANDO EL CÓDIGO DE VERIFICACIÓN REMOTO Y EL CÓDIGO DE RECUPERACIÓN LOCAL
930
MOSTRAR EL CÓDIGO DE VERIFICACIÓN EN EL DISPOSITIVO DE RECUPERACIÓN
935

FIG. 9

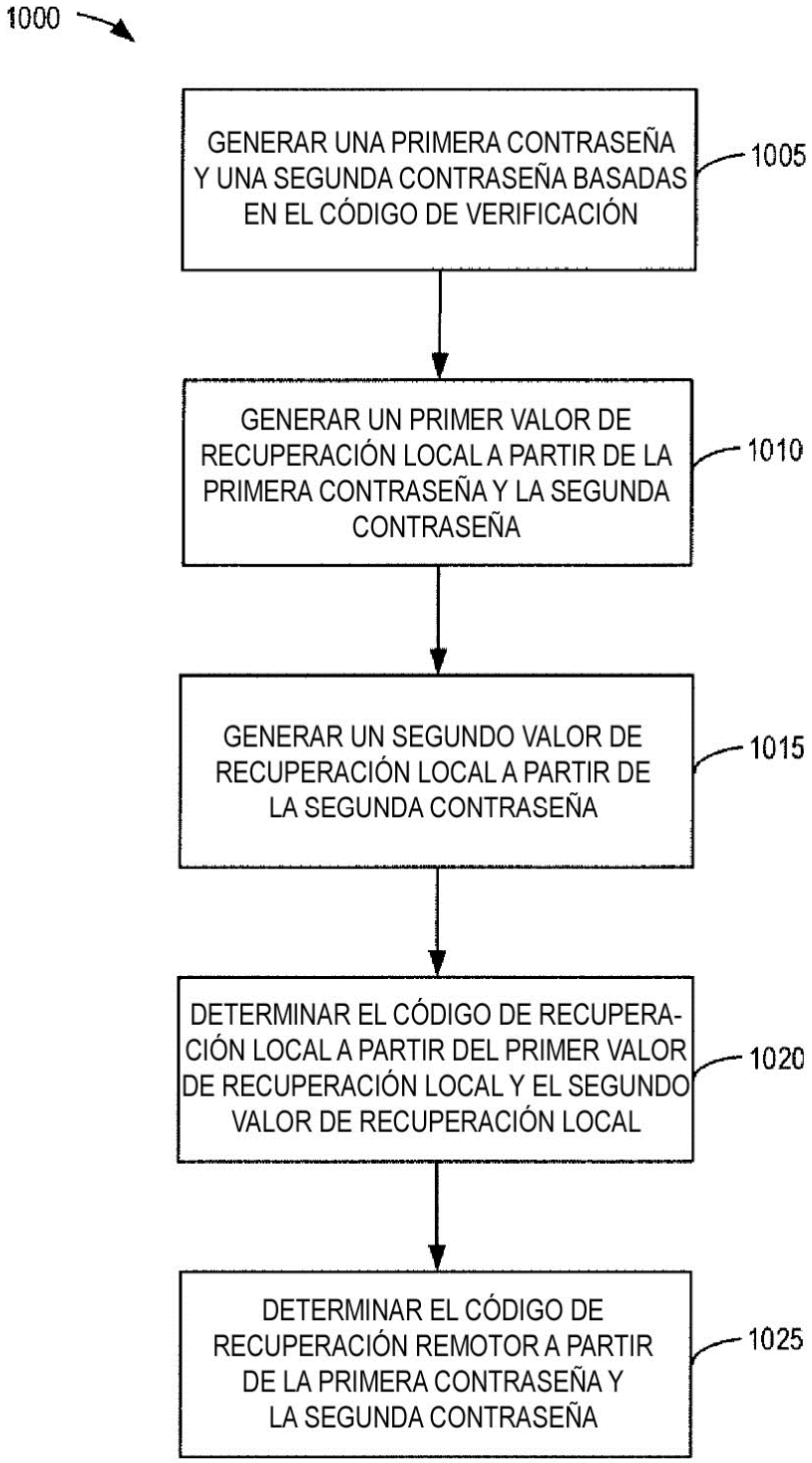
1000
GENERAR UNA PRIMERA CONTRASEÑA Y UNA SEGUNDA CONTRASEÑA BASADAS EN EL CÓDIGO DE VERIFICACIÓN
1005
GENERAR UN PRIMER VALOR DE RECUPERACIÓN LOCAL A PARTIR DE LA PRIMERA CONTRASEÑA Y LA SEGUNDA CONTRASEÑA
1010
GENERAR UN SEGUNDO VALOR DE RECUPERACIÓN LOCAL A PARTIR DE LA SEGUNDA CONTRASEÑA
1015
DETERMINAR EL CÓDIGO DE RECUPERACIÓN LOCAL A PARTIR DEL PRIMER VALOR DE RECUPERACIÓN LOCAL Y EL SEGUNDO VALOR DE RECUPERACIÓN LOCAL
1020
DETERMINAR EL CÓDIGO DE RECUPERACIÓN REMOTOR A PARTIR DE LA PRIMERA CONTRASEÑA Y LA SEGUNDA CONTRASEÑA
1025

FIG. 10

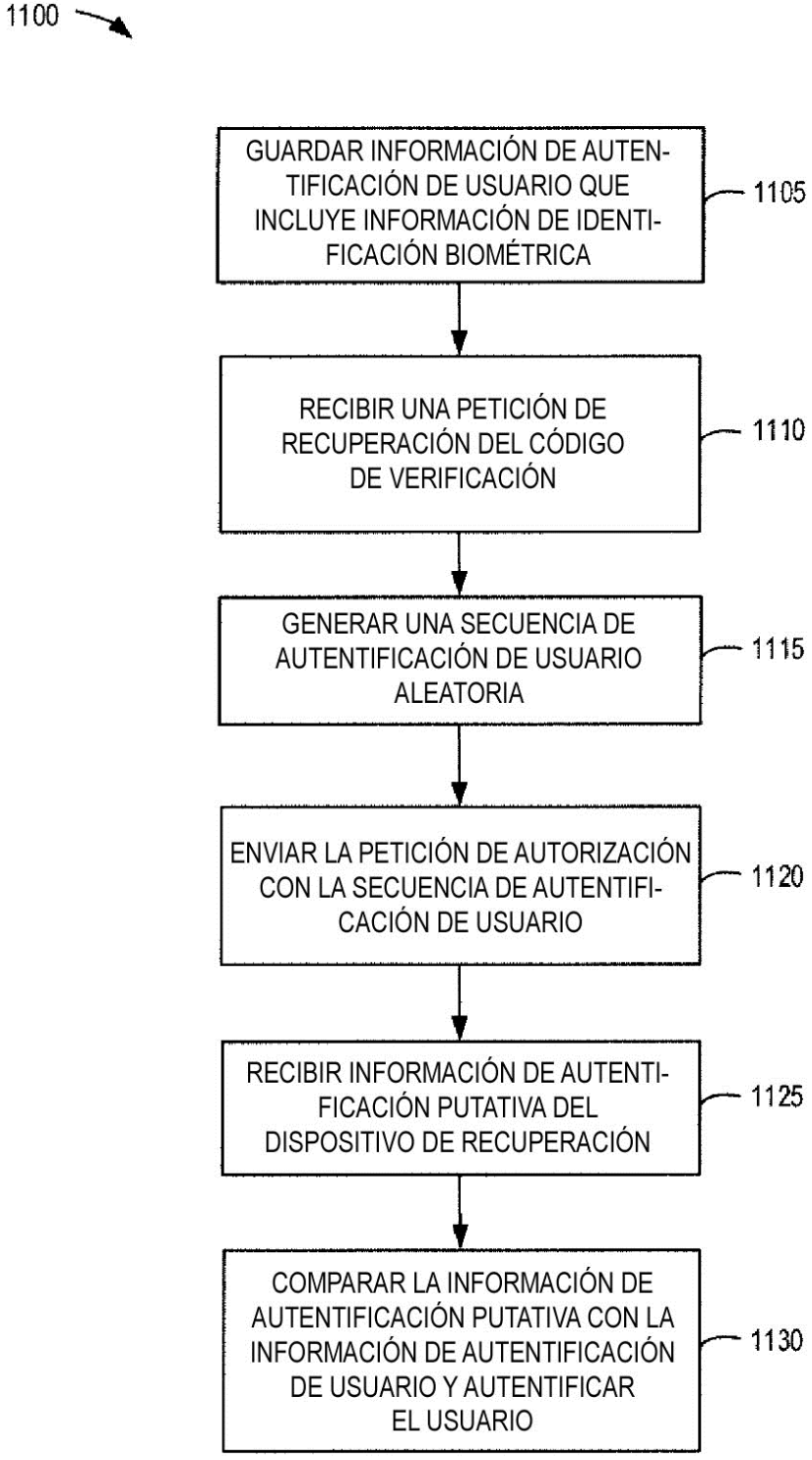
1100
GUARDAR INFORMACIÓN DE AUTENTIFICACIÓN DE USUARIO QUE INCLUYE INFORMACIÓN DE IDENTIFICACIÓN BIOMÉTRICA
1105
RECIBIR UNA PETICIÓN DE RECUPERACIÓN DEL CÓDIGO DE VERIFICACIÓN
1110
GENERAR UNA SECUENCIA DE AUTENTIFICACIÓN DE USUARIO ALEATORIA
1115
ENVIAR LA PETICIÓN DE AUTORIZACIÓN CON LA SECUENCIA DE AUTENTIFICACIÓN DE USUARIO
1120
RECIBIR INFORMACIÓN DE AUTENTIFICACIÓN PUTATIVA DEL DISPOSITIVO DE RECUPERACIÓN
1125
COMPARAR LA INFORMACIÓN DE AUTENTIFICACIÓN PUTATIVA CON LA INFORMACIÓN DE AUTENTIFICACIÓN DE USUARIO Y AUTENTIFICAR EL USUARIO
1130

FIG. 11