(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 667 485**

(51) Int. CI.:

***H04L 29/06*** (2006.01)
***H04L 29/08*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **02.11.2015 E 15192615 (1)**

(97) Fecha y número de publicación de la concesión europea: **21.02.2018 EP 3185501**

(54) Título: **Sistemas y procedimientos para la transmisión de datos específicos de usuario con protección de datos mejorada**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**11.05.2018**

(73) Titular/es:

**TALIHU GMBH (100.0%)**
**Vangerowstr. 18**
**69115 Heidelberg, DE**

(72) Inventor/es:

**JANKOWFSKY, ERIC y**
**SCHNEIDER, ALEXANDER**

(74) Agente/Representante:

**CARPINTERO LÓPEZ, Mario**

## DESCRIPCIÓN

Sistemas y procedimientos para la transmisión de datos específicos de usuario con protección de datos mejorada

**Campo técnico**

La presente invención se refiere en general al intercambio de datos digitales entre dispositivos informáticos en una red informática y más específicamente se refiere a una protección de datos mejorada para preservar la privacidad de los datos durante el intercambio de datos.

**Antecedentes**

En algunos escenarios de aplicaciones, los usuarios interactúan con sistemas informáticos en entornos abiertos. Un entorno abierto en el contexto de esta descripción se refiere a un entorno en el que un terminal de ordenador es operado por un usuario en un espacio público y el mismo terminal puede ser utilizado por otros usuarios posteriormente. Por ejemplo, un usuario puede interactuar con un terminal en una tienda para definir una colección individual de artículos para comprar, o un usuario puede interactuar con un terminal de planificación de ruta en una estación de tren para definir una ruta de viaje individual. Normalmente, la interacción del usuario con el ordenador requiere la entrada de algunos datos que proporcionan información personal sobre el individuo en sí. Por ejemplo, la ruta de viaje de un individuo o el contenido del carrito de compra del individuo representan datos personales que el individuo normalmente no desea compartir con otras personas en el entorno público del terminal respectivo. Tales datos que están asociados con la información personal proporcionada por el individuo se denominan "datos personales" de aquí en adelante.

En algunos escenarios de aplicaciones donde el individuo necesita usar múltiples terminales en puntos consecutivos para procesar los datos personales, típicamente los datos personales se almacenan centralmente (por ejemplo, en un servidor web o cualquier otro dispositivo de almacenamiento apropiado) y los diversos terminales pueden acceder los datos almacenados centralmente a través de conexiones predefinidas.

La solicitud de patente estadounidense US2014/214564 A1 desvela un procedimiento para permitir que múltiples dispositivos móviles contribuyan con artículos a un único carrito de compra. De este modo, los dispositivos móviles se emparejan electrónicamente y un primer dispositivo puede transmitir información sobre un artículo del carrito de compra a un segundo dispositivo para crear una copia sincronizada del carrito de compra electrónico en el segundo dispositivo (resumen). La solución intenta ayudar a múltiples personas a contribuir con la compra de artículos en una única lista de compra y evitar compras múltiples del mismo artículo al dividir la lista de compra. Cada cliente que controla tal dispositivo emparejado de este tipo puede modificar el carrito de compra. Cada dispositivo consulta periódicamente el servidor para obtener las actualizaciones del carrito de compra modificado. El servidor garantiza que el carrito de compra se visualice correctamente en cada dispositivo móvil sin diferencias y periódicamente transmite copias completas del carrito de compra a los dispositivos móviles.

Sin embargo, existe el riesgo de que los usuarios no autorizados tengan acceso a los datos personales del individuo en un terminal mientras el individuo interactúa con otro terminal. Por ejemplo, un usuario que colecciona algunos artículos usando un primer terminal en un primer departamento de una tienda puede abandonar el primer terminal y continuar comprando en un segundo terminal en un segundo departamento. Durante este tiempo, después de que el usuario haya salido del primer terminal, otras personas pueden obtener acceso no deseado a los datos personales del individuo en el primer terminal. Este problema se conecta en cascada cuando se trata de terminales adicionales (por ejemplo, en otros departamentos, un dispositivo móvil del individuo o un sistema de caja para el pago final de los artículos recolectados).

Por lo tanto, es necesario mejorar la protección de los datos personales en entornos abiertos para escenarios en los que un individuo continúa el procesamiento de dichos datos personales en múltiples ordenadores.

**Sumario**

Los problemas técnicos descritos anteriormente se resuelven mediante realizaciones de la invención como se describe en las reivindicaciones independientes.

En una realización, un sistema informático actúa como un sistema de memoria temporal entre un dispositivo informático de origen y un dispositivo informático de destino para transmitir datos personales desde el dispositivo informático de origen al dispositivo informático de destino con protección de datos mejorada. El uso del sistema de memoria temporal divulgado permite que los sistemas informáticos de origen y de destino transfieran físicamente los datos personales de un individuo de un dispositivo a otro a través del sistema de memoria temporal de forma tal que, después de la transferencia de datos, solo una única copia persistente de los datos personales está disponible en el dispositivo informático de destino en el que el dispositivo informático de destino corresponde al terminal que está siendo utilizado actualmente por el individuo. No hay copias persistentes de los datos personales disponibles en ningún otro dispositivo informático. Una copia persistente de la estructura de datos, tal como se usa a continuación, se refiere a una copia que está permanentemente almacenada en una memoria del respectivo dispositivo terminal o sistema de memoria temporal. Las copias que se generan, por ejemplo, en el contexto de rellenar una página de

interfaz de usuario sin estado con el contenido de la estructura de datos local para fines de visualización no se consideran copias persistentes dentro del contexto de esta divulgación. Como consecuencia, es físicamente imposible para los usuarios no autorizados acceder a los datos personales del individuo desde cualquier dispositivo informático que actualmente no sea utilizado por el individuo pero que pueda haber sido utilizado previamente por el individuo.

De este modo, el sistema de memoria temporal es un sistema complementario que interactúa con el sistema informático que incluye los dispositivos informáticos de origen y de destino. Para facilitar la explicación, el sistema de memoria temporal y el sistema informático complementario se describen juntos a continuación mediante la explicación de sus funciones respectivas que permiten la interacción que conduce al efecto técnico anterior. En la siguiente descripción, el dispositivo informático de origen y el dispositivo de origen son sinónimos. Del mismo modo, el dispositivo informático de destino y el dispositivo de destino son sinónimos.

El dispositivo informático de origen inicialmente recibe datos personales de un individuo en particular. Los datos personales incluyen una o más representaciones digitales de uno o más elementos físicos en los que los elementos físicos pertenecen a una selección de elementos del individuo. Por ejemplo, los artículos físicos pueden ser artículos seleccionados en venta en una tienda o vehículos seleccionados (por ejemplo, trenes, autobuses, tranvías, etc.) que se utilizan en una ruta de viaje. Otros escenarios que implican otros elementos físicos en los que puede aplicarse el concepto de la invención son evidentes para una persona experta en la técnica.

Las representaciones digitales se pueden crear de cualquier manera apropiada. En una realización, se puede recibir una representación digital particular desde un dispositivo de escáner en respuesta al escaneo de un identificador de artículo correspondiente asociado con un artículo físico particular respectivo. En otras palabras, un dispositivo escáner puede escanear un código legible por máquina (por ejemplo, un código de barras, código QR o código RFID) asociado con el elemento físico (por ejemplo, un producto o artículo de fabricación) y proporcionar el resultado de la operación de escaneo como la representación digital al dispositivo informático de origen. En una realización, se puede recibir una representación digital particular desde un dispositivo informático en respuesta a una entrada del usuario de un identificador de elemento particular asociado con un artículo físico particular respectivo. Por ejemplo, un usuario (por ejemplo, el individuo o una persona de ventas que brinda servicio al individuo), puede ingresar códigos de producto respectivos o seleccionar artículos que representen los elementos físicos reales de un catálogo en línea. En otro ejemplo, el individuo puede seleccionar medios de transporte que representen vehículos de transporte reales para una ruta de viaje planificada desde un sistema de información de viaje.

El dispositivo informático de origen genera entonces una estructura de datos local y almacena la una o más representaciones digitales en la estructura de datos local. En otras palabras, la estructura de datos local persiste en una memoria del dispositivo informático de origen. Se puede usar cualquier tecnología de almacenamiento apropiada. Por ejemplo, la estructura de datos puede generarse en una base de datos, una hoja de cálculo, un archivo XML u otros formatos de datos apropiados para almacenar una lista de representaciones digitales.

En un punto en el tiempo, después de que la estructura de datos local se ha mantenido, el dispositivo informático de origen recibe una solicitud de transmisión para transmitir la estructura de datos local al dispositivo informático de destino. La solicitud de transmisión puede ser una solicitud explícitamente generada por un usuario (por ejemplo, el individuo o el vendedor). Por ejemplo, el usuario ingresa la dirección del dispositivo informático de destino porque el individuo tiene la intención de ampliar aún más la estructura de datos con datos personales adicionales en el dispositivo informático de destino. La solicitud de transmisión también puede ser generada automáticamente por el sistema informático de origen. Por ejemplo, siempre que se genere una estructura de datos local o cuando se modifique o cuando la página de interfaz de usuario respectiva se vuelva a renderizar, el sistema informático de origen puede anticipar una transmisión de datos futura y activar una solicitud de transmisión correspondiente.

En respuesta a la solicitud de transmisión, el dispositivo informático de origen transmite una copia de la estructura de datos local al sistema de memoria temporal. El sistema de memoria temporal almacena temporalmente la copia recibida. El de memoria temporal es una memoria del sistema de memoria temporal que es adecuada para almacenar la estructura de datos recibida. Lo último en tecnología RAM o componentes de memoria ROM se pueden usar para este propósito. La transmisión no necesita ocurrir instantáneamente después de la recepción de la solicitud de transmisión. Existen realizaciones que se describen más adelante en las que se producen etapas adicionales entre la recepción de la solicitud de transmisión y la transmisión final de la copia. Sin embargo, sin una solicitud de transmisión recibida, no se activa la transmisión de la estructura de datos local.

Una vez que la copia de la estructura de datos local se ha enviado al sistema de memoria temporal, el dispositivo informático de origen elimina la estructura de datos local del dispositivo informático de origen, de modo que ya no es posible el acceso no autorizado a la estructura de datos local a través del dispositivo informático de origen. La eliminación no necesariamente ocurre inmediatamente después de la transmisión de la estructura de datos local. Por ejemplo, en una realización, el dispositivo informático de origen puede esperar hasta que reciba un mensaje de éxito del dispositivo informático de destino que indique que la estructura de datos transmitida fue recibida con éxito por el dispositivo informático de destino. En esta realización, el dispositivo informático de origen elimina la estructura de datos local después de que se recibe el mensaje de éxito.

Para evitar el acceso no autorizado al dispositivo informático de destino por parte de usuarios que no sean el individuo cuyos datos personales se transmiten, el dispositivo informático de destino se bloquea frente a un acceso no autorizado. En otras palabras, el dispositivo informático de destino espera credenciales de inicio de sesión particulares para desbloquear el dispositivo nuevamente.

En una realización, tales credenciales de inicio de sesión son generadas por el sistema de memoria temporal, por ejemplo, como un PIN o contraseña que está asociado con la estructura de datos almacenados temporalmente. En general, las credenciales de inicio de sesión incluyen un secreto que está asociado con la estructura de datos almacenados temporalmente. Los detalles de implementación se explican en la descripción detallada. El sistema de memoria temporal luego envía instrucciones de bloqueo al dispositivo de destino para bloquear el dispositivo en donde las instrucciones de bloqueo proporcionan el secreto al dispositivo de destino que se espera que desbloquee el dispositivo. Además, las credenciales de inicio de sesión se envían al dispositivo de origen para proporcionar las credenciales de inicio de sesión al individuo que interactúa con el dispositivo de origen. Por ejemplo, el dispositivo de origen puede mostrar las credenciales de inicio de sesión recibidas en la pantalla del terminal del dispositivo. En el caso de que las credenciales de inicio de sesión sean una contraseña o un PIN, el individuo puede recordar las credenciales de inicio de sesión. En caso de que las credenciales de inicio de sesión sean un código legible por máquina (por ejemplo, código de barras o código QR), el individuo puede tomar una foto del código mostrado con un dispositivo móvil personal (por ejemplo, teléfono inteligente, tableta, cámara, etc.). El individuo ahora está equipado con las credenciales de inicio de sesión necesarias para acceder y desbloquear el dispositivo de destino. El dispositivo de destino tiene conocimiento del secreto y, por lo tanto, puede validar las credenciales de inicio de sesión recibidas y, finalmente, autentificar al individuo como usuario autorizado del dispositivo de destino.

Si el dispositivo de destino autentifica al usuario (es decir, las credenciales de inicio de sesión proporcionan el secreto correcto al dispositivo de destino), el dispositivo de destino notifica al sistema de memoria temporal que el usuario solicitante fue autentificado y envía una solicitud de recuperación para la estructura de datos almacenados temporalmente. La solicitud de recuperación puede indicar un identificador para la estructura de datos almacenados temporalmente (por ejemplo, el identificador puede estar codificado en el secreto). Alternativamente, el sistema de memoria temporal asocia la copia recibida de la estructura de datos local con el secreto una vez que se genera el secreto en respuesta a la recepción de la copia de la estructura de datos local. En este caso, el secreto puede enviarse desde el dispositivo de destino al sistema de memoria temporal para identificar la respectiva estructura de datos almacenados temporalmente.

En otra realización, las credenciales de inicio de sesión pueden ser generadas por el dispositivo de origen. Por ejemplo, cuando el individuo interactúa con el dispositivo de origen, el dispositivo de origen muestra los datos personales en una página de interfaz de usuario correspondiente de una aplicación respectiva (por ejemplo, una vista de carrito de compra con los artículos pedidos por un individuo o una vista de planificación de ruta con los medios de transporte seleccionados individuales, etc.). El dispositivo de origen puede generar credenciales de inicio de sesión para el individuo en cualquier momento cuando dicha página de interfaz de usuario se vuelva a procesar. Una reescritura de la página de interfaz de usuario puede indicar que el estado de la estructura de datos local ha cambiado o que otro usuario ha comenzado a interactuar con el dispositivo de origen. Por lo tanto, la nueva representación de la página de la interfaz de usuario es un buen indicador para anticipar una próxima transmisión de la estructura de datos local. En esta realización, el dispositivo de origen genera nuevas credenciales de inicio de sesión con cada nueva representación de la página que garantiza que al individuo se le proporcionan credenciales de inicio de sesión válidas en cualquier momento mientras interactúa con el dispositivo de origen.

Las credenciales de inicio de sesión pueden representarse mediante un código legible por máquina, tal como un código de barras, un código QR o cualquier otro código que sea apropiado para codificar un secreto asociado con la estructura de datos local. En otras palabras, las credenciales de inicio de sesión pueden codificar un identificador de la estructura de datos local o el contenido de la estructura de datos local como un todo junto con un secreto (por ejemplo, un testigo que se generó en función de un número aleatorio). El individuo puede solicitar el código legible por la máquina desde el dispositivo de origen. El individuo puede tomar una foto del código legible por la máquina que permite al individuo iniciar sesión en el dispositivo de destino. Alternativamente, el dispositivo de origen puede generar una impresión del código legible por la máquina para el individuo.

Ventajosamente, el dispositivo de origen muestra el código legible por la máquina al individuo solo durante un intervalo de tiempo predefinido o hasta que el individuo recibe una confirmación explícita de que el código ha sido guardado por el individuo. Ventajosamente, el dispositivo de origen se bloquea después del intervalo de tiempo predefinido o la recepción de la confirmación. En esta realización, el estado predeterminado del dispositivo de destino está bloqueado. El dispositivo de destino está a la espera de recibir las credenciales de inicio de sesión.

El dispositivo de destino puede estar equipado con un dispositivo de escáner configurado para escanear y leer el código legible por la máquina de la foto o impresión proporcionada por el individuo. El dispositivo de destino reconoce que el código legible por máquina se refiere a la estructura de datos local que se va a transmitir al dispositivo de destino. El dispositivo de destino puede extraer adicionalmente el secreto codificado del código legible por la máquina. Sin embargo, en esta realización, el dispositivo de destino no tiene conocimiento del secreto y, por lo tanto, no puede realizar la autentificación del usuario. El dispositivo de destino envía una solicitud de recuperación para la estructura de datos que se indica en el código legible por la máquina al sistema de memoria temporal.

Además, el dispositivo de destino envía el testigo extraído al sistema de memoria temporal. En algunas realizaciones, la dirección del dispositivo de origen también puede estar codificada en el código legible por máquina que incluye las credenciales de inicio de sesión. En este caso, la dirección del dispositivo de origen también se puede enviar al sistema de memoria temporal. El sistema de memoria temporal luego genera una solicitud de autentificación con el testigo recibido. En caso de que la dirección del dispositivo de origen ya sea conocida por el sistema de memoria temporal, el sistema de memoria temporal puede reenviar directamente la solicitud de autentificación con el testigo al dispositivo de origen. En caso de que el sistema de origen no estuviera codificado en el código legible por máquina con las credenciales de inicio de sesión, el sistema de memoria temporal puede reenviar la solicitud de autentificación a todos los dispositivos terminales conectados. En este caso, el dispositivo de origen también recibirá la solicitud de autentificación del sistema de memoria temporal.

El dispositivo de origen ha generado originalmente la credencial de inicio de sesión de la máquina que incluye el testigo y, por lo tanto, es capaz de validar el testigo. Por ejemplo, el dispositivo de origen puede almacenar una lista de todos los testigos que se usaron para la generación de un código legible por máquina asociado con una visualización de estructura de datos local por parte del terminal del dispositivo de origen. Si el testigo recibido a través de la solicitud de autentificación se incluye en la lista de testigos generados por el dispositivo de origen, entonces el testigo es válido y el dispositivo de origen autentifica al usuario que intenta iniciar sesión en el dispositivo de destino con este testigo.

En esta realización, el dispositivo de origen interpreta la solicitud de autentificación como la solicitud de transmisión para transmitir una copia de la estructura de datos local al sistema de memoria temporal. Si la autentificación de usuario es exitosa (es decir, el testigo es válido), se envía una copia de la estructura de datos local al sistema de memoria temporal en respuesta a la solicitud de transmisión (solicitud de autentificación). La recepción de la copia de la estructura de datos por parte del sistema de memoria temporal indica al sistema de memoria temporal que la autentificación del usuario en respuesta a la solicitud de autentificación fue exitosa. Es decir, la recepción de la copia almacenada temporalmente en el sistema de memoria temporal es interpretada por el sistema de memoria temporal como una notificación de autentificación desde el sistema de origen al sistema de memoria temporal con respecto a la autentificación del usuario del dispositivo de destino.

En todas las realizaciones, el sistema de memoria de memoria temporal finalmente proporciona una copia de la estructura de datos almacenada temporalmente al dispositivo de destino en respuesta a la solicitud de recuperación y la autentificación exitosa del usuario solicitante. Es decir, si el usuario solicitante posee las credenciales de inicio de sesión correctas para acceder a la estructura de datos almacenada temporalmente, existe una alta probabilidad de que el usuario solicitante se corresponda con el individuo cuyos datos personales están codificados en la estructura de datos almacenados temporalmente.

Una vez que el dispositivo de destino ha recibido la copia de la estructura de datos almacenada temporalmente, el sistema de destino puede liberar la estructura de datos recibida para el usuario que inició sesión con las credenciales de inicio de sesión correspondientes. El sistema de memoria temporal luego elimina la estructura de datos almacenados temporalmente. Si aún no se ha hecho, el dispositivo de origen también elimina la estructura de datos local. En una realización, esto puede ocurrir en respuesta a un mensaje de éxito del dispositivo de destino al sistema de memoria temporal que indica que el dispositivo de destino ha recibido con éxito la copia de la estructura de datos almacenados temporalmente. El sistema de memoria temporal puede reenviar el mensaje de éxito al dispositivo de origen como un activado de una función para eliminar la estructura de datos local.

Sin embargo, el dispositivo de origen y el sistema de memoria temporal pueden eliminar sus copias independientemente de un mensaje de éxito. Por ejemplo, pueden eliminar sus copias locales de la estructura de datos justo después de haber reenviado una copia de la estructura de datos al destino respectivo (por ejemplo, sistema de memoria temporal, dispositivo de destino). Esperar un mensaje de éxito puede mejorar la solidez de la transmisión de datos porque al menos una copia de la estructura de datos local siempre estará disponible hasta que el dispositivo de destino finalmente reciba una copia. En este caso, se puede recuperar una pérdida de una copia durante la transmisión de datos.

En todas las realizaciones, al final de la transmisión de la estructura de datos desde el dispositivo de origen al dispositivo de destino, la copia de la estructura de datos persistida en el dispositivo de destino sigue siendo la única copia conservada de los datos personales del individuo en la totalidad sistema informático. Esto asegura que no se puede usar ningún otro dispositivo terminal que el dispositivo de destino para acceder a los datos personales del individuo.

Las realizaciones de la invención incluyen el sistema de memoria temporal, un procedimiento implementado por ordenador ejecutado por el sistema de memoria temporal y un producto de programa informático correspondiente, así como el sistema informático complementario que incluye los dispositivos terminales que interactúan con el sistema de memoria temporal, los procedimientos implementados por ordenador ejecutados por los dispositivos terminales y los correspondientes productos de programas informáticos.

Se realizarán y alcanzarán otros aspectos de la invención por medio de los elementos y combinaciones señalados particularmente en las reivindicaciones adjuntas. Debe entenderse que tanto la descripción general anterior como la

siguiente descripción detallada son solamente ejemplares y explicativas y no son restrictivas de la invención como se describe.

**Breve descripción de los dibujos**

La figura 1 es un diagrama de componentes simplificado de un sistema informático para la transmisión de datos con un dispositivo informático de origen, un dispositivo informático de destino y un sistema de memoria temporal operado de acuerdo con las realizaciones de la invención;
La figura 2 es un diagrama de flujo simplificado de un procedimiento implementado por ordenador para la transmisión de datos realizada por los dispositivos informáticos de origen y destino de acuerdo con una realización de la invención;
La figura 3 es un diagrama de flujo simplificado de un procedimiento implementado por ordenador para la transmisión de datos realizada por el sistema de memoria temporal de acuerdo con una realización de la invención;
La figura 4 ilustra la autentificación del usuario por el sistema informático de acuerdo con una primera realización de la invención;
La figura 5 ilustra la autentificación del usuario por el sistema informático de acuerdo con una segunda realización de la invención; y
La figura 6 es un diagrama que muestra un ejemplo de un dispositivo informático genérico y un dispositivo informático móvil genérico, que se puede usar en realizaciones de la invención.

**Descripción detallada**

La figura 1 es un diagrama de componentes simplificado de un sistema informático 100 para la transmisión de datos con un dispositivo informático de origen 110, un dispositivo informático de destino 120 y un sistema de memoria temporal 130 operado según las realizaciones de la invención. Los componentes del sistema con una trama punteada se consideran componentes opcionales para el dispositivo o sistema correspondiente. La figura 1 se describe en el contexto de las figuras 2 y 3 y signos de referencia de las figuras 1, 2 y 3 se usan por lo tanto en la siguiente descripción. Debe observarse que las etapas del procedimiento de los procedimientos 1000 y 2000 como se ilustra en los diagramas de flujo simplificados no se ejecutan necesariamente en el orden que se muestra. La descripción describe realizaciones alternativas en las que algunas de las etapas del procedimiento se pueden ejecutar en un orden diferente.

Para la descripción de las diversas realizaciones, se describe un escenario de ejemplo en detalle. Sin embargo, no se pretende que la invención esté limitada de ninguna manera por el ejemplo descrito. Por el contrario, una persona experta en la técnica podrá aplicar la enseñanza técnica de esta descripción a cualquier escenario de aplicación apropiado. En el escenario de ejemplo, un individuo 10 está en una tienda para comprar algunos productos (artículos físicos 1, 2, 3) ofrecidos por la tienda. La tienda puede tener varios departamentos y el individuo 10 puede visitar un primer departamento para seleccionar algunos productos para comprar y luego visitar un segundo departamento para seleccionar otros productos. Finalmente, el individuo se retira en un cajero. Pero en lugar de transportar físicamente los productos identificados (en un carrito de compra físico) del primer al segundo departamento, el individuo 10 puede usar el sistema informático 100 con un carrito de compra virtual de acuerdo con las realizaciones de la invención. Para este propósito, el individuo (o un vendedor que atiende al individuo) crea un carrito de compra virtual (estructura de datos local 111) que incluye las representaciones digitales 1a, 2a, 3a de los productos seleccionados 1, 2, 3 en un primer terminal público (dispositivo de origen 110). El dispositivo de origen 110 puede instalarse en un departamento particular de la tienda (por ejemplo, deportes). Suponiendo que los productos son un par de esquís 1, botas de esquí 2 y un casco de esquí 3, por ejemplo, las representaciones digitales pueden incluir números de artículos en virtud de los cuales los productos están registrados en el sistema informático 100 de la tienda. Dicha funcionalidad es típicamente proporcionada por los llamados sistemas de planificación de recursos empresariales. El sistema informático 100 puede incluir tales funciones o puede estar acoplado de forma comunicativa con un sistema que proporcione tales funciones. Para facilitar la ilustración, los componentes respectivos que proporcionan tales funciones no se muestran en la figura 1. Las personas expertas en la técnica pueden implementar tales funciones sin más explicaciones. El individuo puede querer continuar comprando en otro departamento para comprar más artículos/productos. Por ejemplo, ella puede querer obtener ropa interior específica para el esquí. Para este fin, el carrito de compra local 111 necesita ser transmitido a un segundo terminal (dispositivo de destino 121) ubicado en el departamento de compras de ropa interior, mientras que después de la transmisión el carrito de compra no debería estar disponible en el dispositivo de origen 110 en el departamento de deportes para evitar que cualquier otro usuario posterior del primer terminal pudiera obtener acceso no autorizado al carrito de compra del individuo.

Se describe brevemente un escenario de aplicación adicional que no se usará más en la descripción detallada. Sin embargo, una persona experta en la técnica puede aplicar fácilmente el concepto inventivo a este escenario adicional, así como a otras situaciones similares. En el escenario adicional, el individuo está en un centro de servicio itinerante en un terminal de planificación de ruta pública (dispositivo de origen 110) que permite planificar rutas de viaje a un destino particular combinando diferentes medios de transporte para diferentes partes de la ruta de viaje. En este escenario, los elementos físicos seleccionados por los individuos pueden ser un autobús de enlace 1 para el camino a la estación de tren, un tren 2 para la mayor parte de la ruta y un metro 3 en el destino final para llegar a un

hotel. El individuo puede seleccionar los medios de transporte para crear una estructura de datos de ruta con las representaciones digitales 1a, 2a, 3a de los respectivos medios de transporte 1, 2, 3. La estructura de datos de ruta necesita ser transmitida a una terminal de billetes público (dispositivo de destino 120) para generar e imprimir las respectivas entradas para el individuo. De nuevo, una vez que el individuo se ha movido al terminal de billete 120, los datos personales con respecto a la información de ruta personal ya no deberían poder accederse desde el terminal de planificación de ruta público 110.

Volviendo al escenario de la tienda, después de que el individuo 10 haya hecho la selección de los productos 1, 2, 3 para agregarlos a su carrito de compra virtual 111, los productos pueden ser escaneados por un lector de códigos respectivo. Por ejemplo, el lector de códigos está acoplado de forma comunicativa con el dispositivo de origen 110 como parte de los medios de E/S 210 del dispositivo de origen. Los lectores estándar, tales como lectores de RFID, lectores de códigos de barras o lectores de códigos QR se pueden usar para leer automáticamente el artículo o código de producto de los elementos físicos 1, 2, 3 y proporcionar una representación digital de cada elemento al dispositivo de origen 110. En otra realización, las representaciones digitales pueden ingresarse directamente a través de una interfaz de usuario apropiada (por ejemplo, usar un teclado 210 para escribir los identificadores del producto o usar un ratón 210 o una pantalla táctil 210 para seleccionar las representaciones digitales de un catálogo en línea que almacena representaciones digitales 1a, 2a, 3a de los respectivos productos físicos 1, 2, 3. En otras palabras, el dispositivo de origen recibe 1100 las representaciones digitales 1a, 2a, 3a que son parte de los datos personales del individuo 10. La información de que el individuo 10 ha seleccionado los productos 1, 2, 3 está protegida contra el acceso no autorizado, como se explica a continuación.

Una aplicación de software que es ejecutada por el dispositivo de origen genera 1110 el carrito de compra como estructura de datos local 111 en una porción de memoria del dispositivo de origen 110. Para este propósito, las representaciones digitales se almacenan en la estructura de datos local en cualquier formato apropiado. Por ejemplo, las representaciones digitales pueden simplemente almacenarse en una tabla de base de datos respectiva. Alternativamente, pueden almacenarse en una hoja de cálculo o en un archivo XML. Se puede usar cualquier otro formato apropiado. La estructura de datos del carrito de compra local 111 solo persiste en el dispositivo de origen 110 en este momento. Es decir, inmediatamente después de la generación de la estructura de datos del carrito de compra, solo hay una copia local conservada del carrito de compra en el dispositivo de origen y no se almacena ninguna copia adicional en ningún dispositivo informático central o remoto.

En una realización, el individuo 10 puede ser un usuario registrado en el sistema informático 100. En esta realización, el usuario tiene una cuenta de usuario con un identificador de usuario (ID) 212. La identificación de usuario 212 del individuo 10 puede asociarse con la estructura de datos local 111 que almacena el contenido personal del carrito de compra del individuo.

El dispositivo de origen 110 recibe a continuación 1120 una solicitud de transmisión para transmitir una copia del carrito de compra local 111 del individuo desde el terminal de origen 110 en el departamento de deportes a un terminal de destino 120 en el departamento de ropa interior. En una realización, la solicitud de transmisión puede ser activada directamente por el individuo o un vendedor a través de los medios E/S 210. Por ejemplo, una aplicación de software que se ejecuta en el dispositivo de origen puede proporcionar una descripción general de los dispositivos de destino potenciales actualmente no utilizados. El usuario del dispositivo de origen puede seleccionar el terminal de destino 120 a través de los medios de interfaz de usuario 210 de la lista de terminales de destino actualmente disponibles. En otra realización, la solicitud de transmisión se genera automáticamente en respuesta al intento del usuario de iniciar sesión en el dispositivo de destino 120. Las dos realizaciones se describen en detalle en las figuras 4 y 5. El generador de credenciales de inicio de sesión de componentes opcionales 116 y la autentificación de usuario 117 del dispositivo de origen 110 se refieren a la realización de la figura 5 donde el dispositivo de origen está involucrado en la autentificación 1220 de un usuario para otorgar acceso al dispositivo de destino 120. Se incluye una descripción detallada en la descripción de la figura 5.

En respuesta a la solicitud de transmisión, el dispositivo de origen 110 transmite 1130 una copia del carrito de compra local 111 al sistema de memoria temporal 130. Opcionalmente, en caso de que una ID de usuario 212 esté asociada con el carrito de compra local 111, la ID de usuario también se transmite al sistema de memoria temporal 130. En una realización, el dispositivo de origen puede eliminar 1140 el carrito de compra local 111 justo después de la transmisión de la copia al sistema de memoria temporal. En otra realización, la eliminación 1140 del carrito de compra local puede diferirse hasta que el dispositivo de origen 110 reciba la confirmación del dispositivo de destino 120 de que el contenido del carrito de compra local fue recibido con éxito por el dispositivo de destino.

El sistema de memoria temporal 130 cumple una función de encaminamiento central para enrutar el contenido de las estructuras de datos locales desde cualquier dispositivo de origen a cualquier dispositivo de destino del sistema informático 100. De ese modo, el sistema de memoria temporal 130 recibe 2100 la copia de la estructura de datos local desde el dispositivo de origen 110 y almacena temporalmente 2110 la copia en la memoria temporal 139. Es decir, la copia recibida se almacena o persiste en un componente de memoria del sistema de memoria temporal que se configura en consecuencia.

En una realización, el sistema de memoria temporal tiene un generador de credenciales de inicio de sesión 136 y un módulo de bloqueo 138. Estos componentes opcionales pueden ejecutar las etapas de procedimiento opcionales

2101, 2102 y 2103 del procedimiento 2000. De ese modo, las etapas opcionales también pueden ejecutarse después de la etapa de almacenamiento temporal 2110. El generador de credenciales de inicio de sesión 136 puede generar 2101 credenciales de inicio de sesión para que un usuario (por ejemplo, el individuo 10) acceda al dispositivo de destino 120. Sin embargo, en este momento el individuo todavía está interactuando con el dispositivo de origen 110. Por lo tanto, el generador 136 está enviando 2102 las credenciales de inicio de sesión generadas al dispositivo de origen 110 donde el dispositivo de origen proporciona las credenciales de inicio de sesión recibidas al individuo 10 a través de los medios de E/S 210. Por ejemplo, las credenciales de inicio de sesión se pueden generar como un PIN secreto, contraseña u otro código secreto que se muestra al individuo en una pantalla del terminal del dispositivo de origen. Por ejemplo, en una realización, el dispositivo de origen puede informar al individuo que se recibieron las credenciales de inicio de sesión para el terminal de destino en el departamento de ropa interior y están disponibles para su visualización. El individuo 10 puede desencadenar la visualización de la información secreta si el espacio público alrededor del terminal 110 del departamento de deportes está lo suficientemente vacío para que no exista riesgo de escuchas ilegales. En una alternativa, el dispositivo de origen 110 puede imprimir las credenciales de inicio de sesión para el dispositivo de destino en una hoja de papel.

Cuando el sistema de memoria temporal envía 2102 las credenciales de inicio de sesión al dispositivo de origen, también envía 2103, sustancialmente simultáneamente (es decir, al mismo tiempo o poco antes o poco después de la etapa de envío 2102), bloqueando instrucciones al dispositivo de destino 120. Las instrucciones de bloqueo hacen que el módulo de bloqueo 128 del dispositivo de destino del dispositivo de destino bloquee el dispositivo 1200 contra el acceso no autorizado. Las instrucciones de bloqueo también incluyen las credenciales de inicio de sesión generadas de modo que, en esta realización, el dispositivo de destino 120 se habilita para autentificar a un usuario que intenta acceder al sistema de destino ingresando credenciales de inicio de sesión. las etapas opcionales de autentificación de usuario en el dispositivo de destino pueden ser realizados por el componente 127 de autentificación de usuario opcional del dispositivo de destino. El componente de credenciales de inicio de sesión 129 está configurado para recibir las credenciales de inicio de sesión de un usuario a través de los medios de E/S 220 del dispositivo de destino y procesar adicionalmente las credenciales de inicio de sesión como se describe para las diferentes realizaciones. De ese modo, el usuario puede ingresar una contraseña o PIN o similar o el usuario puede proporcionar un código legible por máquina que codifica las credenciales de inicio de sesión a un dispositivo lector de códigos respectivo. Si las credenciales de inicio de sesión recibidas 1210 por el dispositivo de destino de un usuario corresponden a las credenciales de inicio de sesión que se recibieron del sistema de memoria temporal 130, el componente de autentificación de usuario 127 autentifica 1220 al usuario como el individuo 10 y otorga acceso al dispositivo de destino 1220.

En todas las realizaciones, el sistema 130 de memoria temporal recibe 2120 una solicitud de recuperación para la estructura 131 de datos almacenados temporalmente. Sin embargo, el punto en el tiempo cuando la solicitud de recuperación es recibida por el sistema de memoria temporal depende de la realización respectiva del mecanismo 1220 de autentificación de usuario. En la realización de la figura 4, el sistema de memoria temporal recibe 2130 la solicitud de recuperación después de la autentificación del usuario por el dispositivo de destino como se describe con más detalle en la descripción de la figura 4. La notificación de autentificación también se recibe 2130 desde el dispositivo de destino.

En la realización de la figura 5, la solicitud de recuperación se recibe desde el dispositivo 120 de destino antes de que el dispositivo de origen 110 autentifique al usuario como se describe con más detalle en la descripción de la figura 5. En esta realización, el dispositivo 120 de destino ya genera la solicitud de recuperación en respuesta a la exploración de un código legible por máquina que fue generado por el generador 116 de credenciales de inicio de sesión del dispositivo de origen como las credenciales de inicio de sesión para el individuo 10. El código legible por máquina recibido por el componente de credenciales de inicio de sesión 129 incluye un secreto que es extraído por el extractor de testigo 126 del dispositivo de destino. La solicitud de recuperación y el testigo extraído se envían al sistema de memoria temporal 130. Como, en esta realización, la autentificación del usuario la realiza el dispositivo de origen, la notificación de autentificación se recibe 2130 desde el dispositivo de origen 110, mientras que la solicitud de recuperación se recibió 2120 desde el dispositivo de destino.

En todas las realizaciones, el sistema de memoria temporal 130 envía 2140 una copia 121 de la estructura de datos almacenados temporalmente 131 al dispositivo de destino 120 después de que se haya recibido una solicitud de recuperación correspondiente 2120 y se haya recibido una notificación de autentificación 2130 respectiva. Además, el sistema de memoria temporal borra 2150 la estructura de datos almacenados temporalmente después de que la copia 121 se haya enviado al dispositivo de destino 120.

En una realización, el dispositivo de destino envía un mensaje de éxito al sistema de memoria temporal 130 al recibir con éxito la copia 121 de la estructura de datos del carrito de compra para indicar al sistema de memoria temporal que el individuo 10 ahora puede tener acceso completo a su carrito de compra personal en el dispositivo de destino. Los datos personales se han transmitido con éxito desde el dispositivo de origen donde el carrito de compra personal se creó inicialmente como una estructura de datos local. En esta realización, el sistema de memoria temporal borra 2150 la estructura de datos almacenados temporalmente 131 tras la recepción 2131 del mensaje de confirmación. Además, en esta realización, el sistema de memoria temporal puede reenviar el mensaje de éxito al dispositivo de origen que puede retrasar la eliminación 1140 de la estructura de datos de carrito de compra local 111 hasta la recepción del mensaje de éxito. Esta realización mejora la solidez de la transmisión de datos personales

debido a que un fallo del sistema después de la generación de la estructura 111 de datos del carrito de compra local no dará como resultado la pérdida de los datos personales. La estructura de datos local solo se elimina después de la transmisión de datos exitosa. No obstante, al final de la transmisión exitosa de datos personales, la única copia que queda de la estructura de datos del carrito de compra es la copia 121 recibida por el dispositivo de destino 120. Esto asegura que no se puede realizar ningún acceso no autorizado al carrito de compra personal desde cualquiera de los otros dispositivos en el sistema informático 100.

La figura 4 ilustra la autentificación del usuario por el sistema informático 400 de acuerdo con una primera realización de la invención. En esta realización, el dispositivo de origen 410 genera 411 la estructura de datos de carrito de compra local mientras interactúa con el individuo o vendedor y envía 412 una copia de la estructura de datos local al sistema de memoria temporal 430 al recibir la solicitud de transmisión para transmitir el carrito de compra al dispositivo de destino 420. Por ejemplo, la aplicación de software que se ejecuta en el dispositivo de origen puede proporcionar una visión general de todos los terminales de dispositivos de destino disponibles en el taller e indicar terminales que actualmente no están siendo utilizados por otros usuarios. El individuo puede seleccionar uno de los terminales disponibles como el dispositivo de destino, por ejemplo, en un departamento de la tienda donde el individuo desea continuar comprando. La selección del dispositivo de destino como el destino para la estructura de datos del carrito de compra local puede ser la solicitud de transmisión o puede activar la solicitud de transmisión.

Tras la recepción de la copia de la estructura de datos del carrito de compra, el sistema de memoria temporal 430 genera 431 credenciales de inicio de sesión para el individuo que se utilizará en el dispositivo de destino 420 para obtener acceso. En el ejemplo, las credenciales de inicio de sesión incluyen un secreto en el formato de un PIN. Sin embargo, una contraseña o un código legible por máquina (por ejemplo, código de barras, código QR) pueden generarse igualmente como secreto. Las credenciales de inicio de sesión generadas se envían 432 a ambos, el dispositivo de origen 410 y de destino 420. En el dispositivo de origen 410, las credenciales de inicio de sesión se comunican al individuo. Por ejemplo, el secreto se muestra 413 en una pantalla del dispositivo de origen. En la figura 5 algunas realizaciones se describen para mostrar el secreto de una manera para mejorar aún más la protección de datos para los datos personales. Estas realizaciones también pueden combinarse con la función de visualización de la realización en la figura 4 para una mejor protección de datos. Las credenciales de inicio de sesión generadas están asociadas a la estructura de datos del carrito de compra almacenados temporalmente por el sistema de memoria temporal 430.

El dispositivo de destino 420 interpreta la recepción de las credenciales de inicio de sesión como instrucciones de bloqueo para bloquear 421 el dispositivo de destino contra el acceso no autorizado y luego espera recibir 422 una entrada de usuario que proporciona las credenciales de inicio de sesión (PIN, contraseña, etc.) que se recibieron del sistema de memoria temporal El individuo, después de haberse movido desde el dispositivo de origen al dispositivo de destino, proporciona las credenciales de inicio de sesión transmitidas al individuo por el dispositivo de origen 410. En el caso de un PIN o contraseña secreta, el usuario puede ingresar el secreto a través de un teclado o pantalla táctil. En el caso de un código secreto legible por máquina, el usuario puede usar un dispositivo lector de código (por ejemplo, un código de barras o un escáner de código QR) para ingresar las credenciales de inicio de sesión. Si el secreto en las credenciales de inicio de sesión recibidas del usuario en el dispositivo de destino corresponde al secreto que se recibió del sistema de memoria temporal 430, el sistema de destino ha autentificado al usuario como el individuo que tiene derecho a acceder al carrito de compra que está almacenado en el sistema de memoria temporal. El dispositivo de destino envía una notificación de autentificación al sistema 430 de almacenamiento temporal que indica el secreto que se utilizó para autentificar al usuario. Esta notificación de autentificación sirve al mismo tiempo que la solicitud de recuperación para el carrito de compra almacenado temporalmente que está asociado con dicho secreto.

El sistema de memoria temporal está ahora en posesión de la solicitud de recuperación y la notificación de autentificación y envía 433 la copia solicitada de la estructura de datos del carrito de compra almacenada temporalmente en el dispositivo 420 de destino donde la copia recibida de la estructura de datos finalmente se libera 423 al usuario.

La eliminación del carrito de compra local en el dispositivo de origen 410 y el carrito de compra almacenado temporalmente en el sistema de memoria temporal 430 puede ocurrir inmediatamente después de enviar las respectivas copias del carrito de compra a su destino o al recibir un mensaje de éxito desde el sistema de destino 420 que indica el recibo exitoso del carrito de compra. Las ventajas e inconvenientes de las respectivas realizaciones se detallan adicionalmente en la descripción de la figura 5.

La figura 5 ilustra la autentificación del usuario por el sistema informático 500 de acuerdo con una segunda realización de la invención. Después de que se ha generado el carrito de compra local del individuo, una aplicación de software muestra el carrito de compra en el terminal 510 del dispositivo de origen al individuo. Por ejemplo, la aplicación de software puede incluir una página de interfaz de usuario que es utilizada por el individuo o un vendedor para interactuar con el dispositivo de origen 510 para generar el carrito de compra local. En el ejemplo, la página de interfaz de usuario es una página que se ejecuta en un navegador estándar del dispositivo de origen. Por ejemplo, la aplicación de software puede ejecutarse localmente por el dispositivo de origen o se proporciona como un servicio web por un servidor web a través de Internet. Una persona experta en la materia sabe cómo implementar software

en el dispositivo de origen 510 para tales escenarios de aplicación. La página de interfaz de usuario en sí misma generalmente no tiene estado. Es decir, el contenido mostrado se carga desde la estructura de datos del carrito de compra local cada vez que se vuelve a procesar la página de la interfaz del usuario. La página de la interfaz de usuario puede reproducirse cuando un nuevo usuario comienza a usar la aplicación, pero también cada vez que se modifica el carrito de compra local. Es decir, cada vez que se modifica una representación digital, la página se vuelve a renderizar y refleja el estado actual del carrito de compra local. El dispositivo de origen 510 puede generar un nuevo código legible por máquina cada vez que se reescribe la página. Este código legible por máquina incluye un testigo que es una clave secreta que se puede generar como un valor hash de un número aleatorio. Los procedimientos para generar tales testigos son bien conocidos en la técnica. Además, el código legible por máquina incluye información sobre la estructura de datos del carrito de compra local. Por ejemplo, un identificador para el carrito de compra local está codificado en el código legible por máquina. En una realización, incluso el contenido completo del carrito de compra puede estar codificado. Esto permite no solo la identificación de un carrito de compra en particular, sino también, opcionalmente, la identificación de los artículos incluidos en el carrito de compra. Por ejemplo, el código legible por máquina puede ser un código de barras o un código QR. En una realización alternativa, la ficha puede proporcionarse al individuo como una cadena de caracteres junto con una identificación para el carrito de compra. La secuencia puede ser memorizada por el individuo y luego proporcionada al dispositivo de destino a través de la entrada manual de datos a través del individuo.

El dispositivo de origen muestra 511 el código legible por máquina actualmente válido para el individuo. Es decir, cada vez que la página se vuelve a procesar en el navegador, se actualiza la visualización del código legible por la máquina en el terminal del dispositivo de origen. El dispositivo de origen 511 es el único dispositivo en el sistema informático 511 que conoce el código secreto oculto en el código legible por la máquina. El dispositivo de origen puede almacenar el historial de todos los testigos generados por el dispositivo de origen que permite que el dispositivo de origen 510 valide cualquier solicitud de testigo con respecto a la validez del testigo. El individuo puede tomar una copia del código legible por la máquina y puede llevar esta copia a un terminal adicional (por ejemplo, al terminal de destino). Por ejemplo, el código puede ser impreso por el dispositivo de origen para el individuo o el individuo puede tomar una foto del código legible por la máquina con un dispositivo móvil personal (por ejemplo, teléfono inteligente, cámara, tableta, etc.). Ventajosamente, la copia del código legible por máquina es visual en el sentido de que se muestra en una pantalla del dispositivo de origen (es decir, a través de un elemento de interfaz de usuario), y que puede comunicarse mediante dispositivos de captura (como cámaras digitales) que están disponibles para el individuo.

Esta copia del código legible por máquina se presenta luego al dispositivo de destino 520 (por ejemplo, por el individuo después de haber alcanzado el terminal en el departamento de ropa interior). En esta realización, el dispositivo de destino 520 está equipado con un dispositivo lector de códigos correspondiente que puede explorar 521 el código legible por la máquina y, de ese modo, extraer la información codificada sobre la información del carrito de compra y la ficha. En este momento, el dispositivo de destino 520 no sabe si el usuario que presentó el código legible por máquina está autorizado para acceder al sistema de destino. Por lo tanto, el testigo extraído se envía 522 al sistema 530 de memoria temporal junto con una solicitud de recuperación para el carrito de compra que se codifica en el código legible por máquina. La solicitud de recuperación y el testigo también se pueden enviar en mensajes separados. Enviados juntos en este contexto significa que ambos se envían al sistema de memoria temporal antes de la autentificación del usuario. El sistema 530 de memoria temporal reconoce la solicitud de recuperación para la estructura de datos del carrito de compra respectivo, pero no puede proporcionar el carrito de compra al dispositivo 520 de destino porque todavía no ha recibido una copia del carrito de compra local del dispositivo de origen y no conoce la autorización del usuario solicitante en este momento. Por lo tanto, el sistema 530 de memoria temporal genera 531 una solicitud de autorización que incluye la ficha recibida y reenvía esta solicitud de autorización al dispositivo 510 de origen. Si el sistema de memoria temporal está conectado a más de un dispositivo de origen, reenviará la solicitud de autorización a todos los dispositivos de origen que puedan realizar las siguientes etapas de autentificación. En caso de que la información en la solicitud de recuperación con respecto al carrito de compra incluya además del ID del carrito de compra el ID de usuario del individuo que está asociado con el carrito de compra, el sistema de memoria temporal puede identificar dichos dispositivos de origen que tuvieron una interacción con el individuo en el pasado. En este caso, el sistema de memoria temporal puede enviar las solicitudes de autentificación solo a los dispositivos de origen identificados para reducir el tráfico de red y ahorrar ancho de banda.

El dispositivo de origen está esperando 512 solicitudes de autorización que pueden corresponder a uno de los códigos legibles por máquina que ha sido generado por el dispositivo de origen hasta este momento. Al recibir la solicitud de autorización, el dispositivo de origen 510 comprueba 513 la validez del testigo incluido comparando el testigo recibido con el archivo histórico de testigos generados en el pasado. Si el testigo no se incluye en el archivo de historial, el dispositivo de origen no autentificará al usuario como un usuario que interactuó con el dispositivo de origen en el pasado y continúa esperando 512 para otra solicitud de autentificación. En caso de que el testigo sea validado por el dispositivo de origen como un testigo generado previamente por el dispositivo, envía 514 automáticamente la estructura de datos del carrito de compra local al sistema de memoria temporal 530.

En esta realización, la recepción de una copia de la estructura de datos local por el sistema de memoria temporal desde el dispositivo de origen corresponde a una notificación de autentificación para el usuario asociada con la solicitud de recuperación que se recibió anteriormente porque la copia solo la envía el dispositivo de origen después

de la autentificación exitosa del usuario basada en el testigo que estaba codificado en el código legible por máquina generado anteriormente. Como consecuencia, el sistema de memoria temporal 530 ahora está en posesión de una notificación de autentificación para los usuarios y de una solicitud de recuperación válida para la estructura de datos de carrito de compra almacenado temporalmente. Por lo tanto, la solicitud de recuperación puede ser respondida por el sistema de memoria temporal enviando 532 una copia de la estructura de datos almacenados temporalmente en el dispositivo de destino 520. En resumen, la protección de datos mejorada para los datos personales de los resultados individuales del uso de diferentes canales de comunicación:

a) el individuo, que proporciona un primer canal, no necesita llevar la estructura de datos completa, sino solo un identificador con un secreto (por ejemplo, un código legible por máquina, que incluye ID de estructura de datos y testigo), y
b) los terminales del dispositivo usan un segundo canal (la comunicación intradispositivo a través del sistema de memoria temporal) para verificar si una estructura de datos de carrito de compra puede reenviarse a un dispositivo de destino solicitante. De este modo, el segundo canal solo está disponible después de la autentificación del usuario a través de la validación del secreto.

El dispositivo de destino puede confirmar 525 con éxito la recepción al sistema de memoria temporal al haber cargado 524 la estructura de datos del carrito de compra recibido. La estructura de datos del carrito de compra cargado ahora está disponible para el individuo en el dispositivo de destino. Ahora el dispositivo de destino 520 puede cambiar al papel de un dispositivo de origen adicional donde el individuo puede modificar la estructura de datos del carrito de compra local, por ejemplo, añadiendo representaciones digitales adicionales o eliminando representaciones digitales existentes. La estructura de datos del carrito de compra modificada puede reenviarse a otros dispositivos de destino de la misma manera.

En la realización de la figura 5, el sistema 530 de memoria temporal reenvía 532 el mensaje de confirmación de éxito al dispositivo 510 de origen que espera 515 para dicha confirmación de éxito hasta que se elimina 516 la estructura de datos del carrito de compra local original. Además, el sistema 530 de memoria temporal borra la copia almacenada temporalmente 533 del carrito de compra una vez recibido el mensaje de confirmación de éxito del dispositivo de destino. Esto corresponde a la realización con una robustez mejorada como ya se explicó anteriormente. En general, en algunas realizaciones del sistema informático 100 (véase la figura 1), puede haber un protocolo de transmisión para la estructura de datos del carrito de compra, en el que las copias se envían desde el origen al dispositivo de destino a través del sistema de memoria temporal, y en ese mensaje de confirmación puede seguir la dirección opuesta y desencadenar la eliminación de copias que no se requieren más. En realizaciones alternativas, el dispositivo de origen puede eliminar el carrito de compra local inmediatamente después de haber enviado la copia al sistema de memoria temporal 530 y el sistema de memoria temporal puede eliminar el carrito de compra almacenado temporalmente después de haber enviado la copia al dispositivo de destino. En esta implementación, se puede evitar que haya varias copias del carrito de compra personal en paralelo durante un breve período de tiempo (hasta que reciban los mensajes de confirmación de éxito). Es decir, esta implementación puede ser menos robusta que la realización descrita anteriormente, pero tiene la ventaja de que la privacidad de los datos personales está mejor asegurada ya que no hay copias coexistentes del carrito de compra que evite el riesgo de que los datos personales Los usuarios no autorizados pueden seguir accediendo al dispositivo de origen mientras el individuo se está moviendo al dispositivo de destino y se autentifica.

La figura 6 es un diagrama que muestra un ejemplo de un dispositivo informático genérico 900 y un dispositivo informático móvil genérico 950, que puede utilizarse con las técnicas descritas aquí. Por ejemplo, el dispositivo informático 900 puede, por ejemplo, relacionarse con el sistema de memoria temporal 130 o los dispositivos informáticos 110, 120 (véase la figura 1). El dispositivo de computación 950 pretende representar diversas formas de dispositivos móviles, tales como asistentes digitales personales, teléfonos celulares, teléfonos inteligentes y otros dispositivos informáticos similares. En el contexto de esta descripción, el dispositivo informático 950 puede servir, por ejemplo, como terminal móvil, lectores para escanear códigos legibles por máquina o como dispositivo personal del individuo para llevar credenciales de inicio de sesión desde un dispositivo terminal a otro. Los componentes mostrados aquí, sus conexiones y relaciones, y sus funciones, están destinados a ser solo ejemplares, y no están destinados a limitar las implementaciones de las invenciones descritas y/o reivindicadas en este documento.

El dispositivo informático 900 incluye un procesador 902, memoria 904, un dispositivo de almacenamiento 906, una interfaz de alta velocidad 908 que se conecta a la memoria 904 y puertos de expansión de alta velocidad 910, y una interfaz de baja velocidad 912 que conecta al bus de baja velocidad 914 y dispositivo de almacenamiento 906. Cada uno de los componentes 902, 904, 906, 908, 910 y 912 están interconectados usando varios buses, y pueden montarse en una placa base común o de otras maneras, según corresponda. El procesador 902 puede procesar instrucciones para su ejecución dentro del dispositivo informático 900, incluidas las instrucciones almacenadas en la memoria 904 o en el dispositivo de almacenamiento 906 para mostrar información gráfica para una GUI en un dispositivo de entrada/salida externo, como la pantalla 916 acoplada a la interfaz de alta velocidad 908. En otras implementaciones, se pueden usar múltiples procesadores y/o múltiples buses, según corresponda, junto con múltiples memorias y tipos de memoria. Además, se pueden conectar múltiples dispositivos informáticos 900, proporcionando cada dispositivo porciones de las operaciones necesarias (por ejemplo, como un banco servidor, un grupo de servidores blade, o un sistema multiprocesador).

La memoria 904 almacena información dentro del dispositivo informático 900. En una implementación, la memoria 904 es una unidad o unidades de memoria volátil. En otra implementación, la memoria 904 es una unidad o unidades de memoria no volátil. La memoria 904 también puede ser otra forma de medio legible por ordenador, tal como un disco magnético u óptico.

El dispositivo de almacenamiento 906 es capaz de proporcionar almacenamiento masivo para el dispositivo informático 900. En una implementación, el dispositivo de almacenamiento 906 puede ser o contener un medio legible por ordenador, tal como un dispositivo de disquete, un dispositivo de disco duro, un dispositivo de disco óptico o un dispositivo de cinta, una memoria flash u otro dispositivo de memoria de estado sólido similar o una matriz de dispositivos, incluidos dispositivos en una red de área de almacenamiento u otras configuraciones. Un producto de programa informático puede incorporarse de forma tangible en un soporte de información. El producto del programa informático también puede contener instrucciones que, cuando se ejecutan, realizan uno o más procedimientos, como los descritos anteriormente. El soporte de información es un medio legible por ordenador o máquina, tal como la memoria 904, el dispositivo de almacenamiento 906 o la memoria en el procesador 902.

El controlador de alta velocidad 908 maneja operaciones de ancho de banda intensivo para el dispositivo informático 900, mientras que el controlador de baja velocidad 912 gestiona operaciones de menor ancho de banda intensivo. Tal asignación de funciones es solo ejemplar. En una implementación, el controlador de alta velocidad 908 está acoplado a la memoria 904, pantalla 916 (por ejemplo, a través de un procesador de gráficos o acelerador) y a puertos de expansión de alta velocidad 910, que pueden aceptar varias tarjetas de expansión (no mostradas). En la implementación, el controlador de baja velocidad 912 está acoplado al dispositivo de almacenamiento 906 y al puerto de expansión de baja velocidad 914. El puerto de expansión de baja velocidad, que puede incluir varios puertos de comunicación (por ejemplo, USB, Bluetooth, Ethernet, Ethernet inalámbrico) puede acoplarse a uno o más dispositivos de entrada/salida, como un teclado, un dispositivo señalador, un escáner o un dispositivo de red tal como un conmutador o enrutador, por ejemplo, a través de un adaptador de red.

El dispositivo informático 900 puede implementarse en una variedad de formas diferentes, como se muestra en la figura. Por ejemplo, puede implementarse como un servidor estándar 920, o múltiples veces en un grupo de tales servidores. También se puede implementar como parte de un sistema de servidor en bastidor 924. Además, puede implementarse en un ordenador personal como un ordenador portátil 922. Alternativamente, los componentes del dispositivo informático 900 pueden combinarse con otros componentes en un dispositivo móvil (no mostrado), tal como el dispositivo 950. Cada uno de tales dispositivos puede contener uno o más dispositivos informáticos 900, 950, y un sistema completo puede estar compuesto por múltiples dispositivos informáticos 900, 950 que se comunican entre sí.

El dispositivo informático 950 incluye un procesador 952, memoria 964, un dispositivo de entrada/salida tal como una pantalla 954, una interfaz de comunicación 966 y un transceptor 968, entre otros componentes. El dispositivo 950 también puede estar provisto de un dispositivo de almacenamiento, tal como un microdispositivo u otro dispositivo, para proporcionar almacenamiento adicional. Cada uno de los componentes 950, 952, 964, 954, 966 y 968 están interconectados usando varios buses, y varios de los componentes pueden montarse en una placa base común o de otras maneras, según corresponda.

El procesador 952 puede ejecutar instrucciones dentro del dispositivo informático 950, incluidas las instrucciones almacenadas en la memoria 964. El procesador puede implementarse como un conjunto de chips de chips que incluyen procesadores analógicos y digitales separados y múltiples. El procesador puede proporcionar, por ejemplo, para la coordinación de los otros componentes del dispositivo 950, tal como el control de las interfaces de usuario, las aplicaciones ejecutadas por el dispositivo 950, y la comunicación inalámbrica por el dispositivo 950.

El procesador 952 puede comunicarse con un usuario a través de la interfaz de control 958 y la interfaz de visualización 956 acoplada a una pantalla 954. La pantalla 954 puede ser, por ejemplo, una pantalla TFT LCD (pantalla de cristal líquido de transistores de película delgada) o una pantalla OLED (diodo orgánico emisor de luz) u otra tecnología de visualización apropiada. La interfaz de visualización 956 puede comprender una circuitería apropiada para conducir la pantalla 954 para presentar información gráfica y otra información a un usuario. La interfaz de control 958 puede recibir comandos de un usuario y convertirlos para enviarlos al procesador 952. Además, se puede proporcionar una interfaz externa 962 en comunicación con el procesador 952, para permitir la comunicación de área cercana del dispositivo 950 con otros dispositivos. La interfaz externa 962 puede proporcionar, por ejemplo, comunicaciones por cable en algunas implementaciones, o comunicaciones inalámbricas en otras implementaciones, y también se pueden usar múltiples interfaces.

La memoria 964 almacena información dentro del dispositivo informático 950. La memoria 964 puede implementarse como uno o más medio o medios legibles por ordenador, unidad o unidades de memoria volátil, o unidad o unidades de memoria no volátil. La memoria de expansión 984 también puede proporcionarse y conectarse al dispositivo 950 a través de la interfaz de expansión 982, que puede incluir, por ejemplo, una interfaz de tarjeta SIMM (módulo de memoria en línea única). Tal memoria de expansión 984 puede proporcionar espacio de almacenamiento adicional para el dispositivo 950, o también puede almacenar aplicaciones u otra información para el dispositivo 950. Específicamente, la memoria de expansión 984 puede incluir instrucciones para llevar a cabo o complementar los procesos descritos anteriormente, y puede incluir también información segura. De este modo, por ejemplo, la

memoria de expansión 984 puede actuar como un módulo de seguridad para el dispositivo 950, y puede programarse con instrucciones que permitan el uso seguro del dispositivo 950. Además, se pueden proporcionar aplicaciones seguras a través de las tarjetas SIMM, junto con información adicional, como colocar la información de identificación en la tarjeta SIMM de una manera que no se puede piratear.

La memoria puede incluir, por ejemplo, memoria flash y/o memoria NVRAM, como se describe a continuación. En una implementación, un producto de programa informático se materializa de forma tangible en un soporte de información. El producto del programa de ordenador contiene instrucciones que, cuando se ejecutan, realizan uno o más procedimientos, como los descritos anteriormente. El soporte de información es un medio legible por ordenador o máquina, tal como la memoria 964, la memoria de expansión 984, o la memoria en el procesador 952, que puede recibirse, por ejemplo, sobre el transceptor 968 o la interfaz externa 962.

El dispositivo 950 puede comunicarse de forma inalámbrica a través de la interfaz de comunicación 966, que puede incluir circuitos de procesamiento de señal digital cuando sea necesario. La interfaz de comunicación 966 puede proporcionar comunicaciones bajo diversos modos o protocolos, tales como llamadas de voz GSM, SMS, EMS o mensajería MMS, CDMA, TDMA, PDC, WCDMA, CDMA2000 o GPRS, entre otros. Dicha comunicación puede ocurrir, por ejemplo, a través del transceptor 968 de radiofrecuencia. Además, puede producirse una comunicación de corto alcance, como el uso de un Bluetooth, WiFi u otro transceptor de este tipo (no se muestra). Además, el módulo receptor 980 GPS (Sistema de Posicionamiento Global) puede proporcionar datos inalámbricos adicionales relacionados con la navegación y la ubicación al dispositivo 950, que pueden ser utilizados según sea apropiado por las aplicaciones que se ejecutan en el dispositivo 950.

El dispositivo 950 también puede comunicarse de forma audible usando el códec de audio 960, que puede recibir información hablada de un usuario y convertirla en información digital utilizable. El códec de audio 960 también puede generar un sonido audible para un usuario, tal como a través de un altavoz, por ejemplo, en un auricular del dispositivo 950. Tal sonido puede incluir sonido de llamadas telefónicas de voz, puede incluir sonido grabado (por ejemplo, mensajes de voz, archivos de música, etc.) y también puede incluir sonido generado por aplicaciones que operan en el dispositivo 950.

El dispositivo informático 950 puede implementarse en una variedad de formas diferentes, como se muestra en la figura. Por ejemplo, puede implementarse como un teléfono celular 980. También se puede implementar como parte de un teléfono inteligente 982, asistente digital personal u otro dispositivo móvil similar.

Diversas implementaciones de los sistemas y técnicas descritos aquí pueden realizarse en circuitos electrónicos digitales, circuitos integrados, ASIC especialmente diseñados (circuitos integrados específicos de la aplicación), hardware informático, firmware, software y/o combinaciones de los mismos. Estas diversas implementaciones pueden incluir la implementación en uno o más programas informáticos que son ejecutables y/o interpretables en un sistema programable que incluye al menos un procesador programable, que puede ser especial o de propósito general, para recibir datos e instrucciones de, y para transmitir datos e instrucciones para, un sistema de almacenamiento, al menos un dispositivo de entrada, y al menos un dispositivo de salida.

Estos programas informáticos (también conocidos como programas, software, aplicaciones de software o códigos) incluyen instrucciones de la máquina para un procesador programable, y pueden implementarse en un lenguaje de programación orientado a objetos y/o de alto nivel de procesamiento, y/o en ensamblado/lenguaje de máquina. Como se usa en el presente documento, los términos "medio legible por máquina", "medio legible por ordenador" se refiere a cualquier producto, aparato y/o dispositivo de programa informático (por ejemplo, discos magnéticos, discos ópticos, memoria, dispositivos lógicos programables (PLD)) utilizados para proporcionar instrucciones y/o datos de la máquina a un procesador programable, que incluye un medio legible por máquina que recibe instrucciones de la máquina como una señal legible por la máquina. El término "señal legible por máquina" se refiere a cualquier señal utilizada para proporcionar instrucciones y/o datos de la máquina a un procesador programable.

Para proporcionar interacción con un usuario, los sistemas y técnicas descritos aquí pueden implementarse en un ordenador que tiene un dispositivo de visualización (por ejemplo, un monitor CRT (tubo de rayos catódicos) o LCD (pantalla de cristal líquido) para mostrar información al usuario y un teclado y un dispositivo señalador (por ejemplo, un mouse o una bola de seguimiento) mediante los cuales el usuario puede proporcionar información al ordenador. Se pueden usar otros tipos de dispositivos para proporcionar interacción con un usuario también; por ejemplo, la retroalimentación proporcionada al usuario puede ser cualquier forma de retroalimentación sensorial (por ejemplo, retroalimentación visual, retroalimentación auditiva o retroalimentación táctil); y la entrada del usuario se puede recibir en cualquier forma, incluida la entrada acústica, de voz o táctil.

Los sistemas y técnicas descritos aquí pueden implementarse en un dispositivo informático que incluye un componente de fondo (por ejemplo, como un servidor de datos), o que incluye un componente de middleware (por ejemplo, un servidor de aplicaciones), o que incluye un frente componente final (por ejemplo, una ordenador cliente que tiene una interfaz gráfica de usuario o un navegador web a través del cual un usuario puede interactuar con una implementación de los sistemas y técnicas descritos aquí) o cualquier combinación de tales componentes de etapa final, middleware o de entrada. Los componentes del sistema se pueden interconectar mediante cualquier forma o medio de comunicación de datos digitales (por ejemplo, una red de comunicación). Los ejemplos de redes de

comunicación incluyen una red de área local ("LAN"), una red de área amplia ("WAN") e Internet.

El dispositivo informático puede incluir clientes y servidores. Un cliente y un servidor generalmente son remotos entre sí y suelen interactuar a través de una red de comunicación. La relación del cliente y el servidor surge en virtud de los programas de ordenador que se ejecutan en los respectivos ordenadores y que tienen una relación cliente-servidor entre sí.

Se han descrito varias realizaciones. Sin embargo, se entenderá que pueden realizarse diversas modificaciones sin apartarse del alcance de la invención.

Además, los flujos lógicos representados en las figuras no requieren el orden particular mostrado, o el orden secuencial, para lograr resultados deseables. Además, se pueden proporcionar otros pasos, o se pueden eliminar las etapas, de los flujos descritos, y se pueden agregar otros componentes o eliminarlos de los sistemas descritos. Por consiguiente, otras realizaciones están dentro del alcance de las siguientes reivindicaciones.

REIVINDICACIONES

1. Un sistema informático de memoria temporal (130) para la transmisión de datos específicos de usuario desde un dispositivo informático de origen (110) a un dispositivo informático de destino (110) con protección de datos mejorada, comprendiendo el sistema de memoria temporal:

un componente de interfaz configurado para recibir una copia de una estructura de datos local (111) desde el dispositivo informático de origen (110), estando la copia recibida destinada a ser transmitida al dispositivo informático de destino (120), en el que la copia recibida incluye datos con una o más representaciones digitales (1a, 2a, 3a) de uno o más elementos físicos (1, 2, 3) en el que los elementos físicos pertenecen a una selección de elementos de un individuo particular (10);
un componente de almacenamiento (139) configurado para almacenar temporalmente la copia recibida como una estructura de datos almacenados temporalmente (131);
estando el componente de interfaz configurado además para recibir, desde el dispositivo informático de destino, una solicitud de recuperación para la estructura de datos almacenados temporalmente (131);
un componente de verificación de autentificación (137) configurado para recibir una notificación de autentificación en el que la notificación de autentificación indica al sistema de memoria temporal (130) que un usuario fue autentificado en base a credenciales de inicio de sesión que fueron generadas específicamente para que el usuario acceda a una copia (121) de la estructura de datos almacenados temporalmente (131) en el dispositivo informático de destino (120), codificando las credenciales de inicio de sesión un identificador de la estructura de datos local (111) o el contenido de la estructura de datos local (111) como un todo, junto con un secreto; estando el componente de interfaz configurado además para enviar la copia (121) de la estructura de datos almacenados temporalmente (131) al dispositivo informático de destino (120) en respuesta a la solicitud de recuperación y la notificación de autentificación; y
estando el componente de almacenamiento (139) configurado además para eliminar la estructura de datos almacenados temporalmente (131) después de que la copia (121) de la estructura de datos almacenados temporalmente sea enviada al dispositivo informático de destino (120).

2. El sistema de memoria temporal de la reivindicación 1, que comprende, además:

un componente generador de credenciales de inicio de sesión (136) configurado para generar las credenciales de inicio de sesión en respuesta a la recepción de la copia (131) de la estructura de datos local (111); y
un módulo de bloqueo (138) configurado para enviar las credenciales de inicio de sesión al dispositivo informático de origen (110) y para enviar instrucciones de bloqueo al dispositivo informático de destino (121) para bloquear el dispositivo informático de destino contra el acceso no autorizado.

3. El sistema de memoria temporal de la reivindicación 1 o 2, en el que el componente de interfaz está configurado además para recibir un mensaje de éxito desde el dispositivo informático de destino (121) tras la recepción con éxito de la copia (121) de la estructura de datos almacenados temporalmente; y en el que el componente de almacenamiento (139) está configurado además para eliminar la estructura de datos almacenados temporalmente (131) en respuesta a la recepción del mensaje de éxito y para reenviar el mensaje de éxito al dispositivo informático de origen (110) como un activador de una función para eliminar la estructura de datos local (111) en el dispositivo informático de origen.

4. Un sistema informático (100) para la transmisión de datos entre diferentes dispositivos informáticos, comprendiendo el sistema informático:

un dispositivo informático de origen (110) configurado para:

recibir datos que incluyen una o más representaciones digitales (1a, 2a, 3a) de uno o más elementos físicos (1, 2, 3) en el que los elementos físicos pertenecen a una selección de elementos de un individuo particular (10);
generar una estructura de datos local (111) y almacenar la una o más representaciones digitales en la estructura de datos local;
recibir una solicitud de transmisión para transmitir la estructura de datos local (111) a un dispositivo informático de destino (120);
transmitir, en respuesta a la solicitud de transmisión, una copia de la estructura de datos local (111) a un sistema de memoria temporal para almacenar temporalmente la copia (131) de la estructura de datos local;
eliminar la estructura de datos local (111) del dispositivo informático de origen (110); y

el dispositivo informático de destino (120) configurado para:

recibir credenciales de inicio de sesión de un usuario para acceder al dispositivo informático de destino en el que las credenciales de inicio de sesión incluyen un secreto asociado con la estructura de datos local (111);
codificando las credenciales de inicio de sesión un identificador de la estructura de datos local o el contenido de la estructura de datos local como un todo, junto con el secreto; autentificar al usuario para otorgarle acceso al dispositivo informático de destino (120) basado en las credenciales de inicio de sesión recibidas;
enviar una solicitud de recuperación al sistema de memoria temporal (130) en el que la solicitud de

recuperación se genera en base a las credenciales de inicio de sesión para solicitar la recuperación de la estructura de datos almacenados temporalmente (131);
recibir, en respuesta a la solicitud de recuperación, una copia (121) de la estructura de datos almacenados temporalmente (131) y otorgar acceso a la copia de estructura de datos recibida (121) para el usuario autentificado en el que la copia de estructura de datos recibida (121) sigue siendo la única copia persistente de la estructura de datos local (111).

5. El sistema informático (100) de la reivindicación 4, en el que el dispositivo informático de origen (110) está configurado adicionalmente para:

mostrar una página de interfaz de usuario para visualizar los datos que incluyen la una o más representaciones digitales;
generar, en respuesta a una nueva representación de la página de interfaz de usuario, un código legible por máquina para el usuario como las credenciales de inicio de sesión, incluyendo el código legible por máquina información codificada con respecto a la estructura de datos local (111) y el secreto;
recibir un testigo desde el sistema de memoria temporal (130) en el que el testigo se extrae a partir del secreto en el código legible por máquina;
autentificar al usuario comprobando el testigo; y
enviar una notificación de autentificación con respecto al usuario al sistema de memoria temporal (139) si el testigo es correcto; y

en el que el dispositivo informático de destino está configurado además para:

escanear el código legible por máquina y generar la solicitud de recuperación basada en la información codificada con respecto a la estructura de datos local en el código legible por máquina escaneado.

6. El sistema informático (100) de la reivindicación 4 o 5, que comprende, además:

el sistema de memoria temporal (130) de acuerdo con una cualquiera de las reivindicaciones 1 a 3.

7. Un procedimiento implementado por ordenador (1000) para la transmisión de datos desde un dispositivo informático de origen a un dispositivo informático de destino con protección de datos mejorada, comprendiendo el procedimiento:

recibir (1100), por el dispositivo informático de origen, datos que incluyen una o más representaciones digitales de uno o más elementos físicos en el que los elementos físicos pertenecen a una selección de elementos de un individuo particular;
generar (1110), en el dispositivo informático de origen, una estructura de datos local y almacenar la una o más representaciones digitales en la estructura de datos local;
recibir (1120), en el dispositivo informático de origen, una solicitud de transmisión para transmitir la estructura de datos local al dispositivo informático de destino;
en respuesta a la solicitud de transmisión, transmitir (1130) una copia de la estructura de datos local a un sistema de memoria temporal para almacenar temporalmente la estructura de datos local;
eliminar (1140) la estructura de datos local del dispositivo informático de origen;
recibir (1210), en el dispositivo informático de destino, credenciales de inicio de sesión de un usuario para acceder al dispositivo informático de destino en el que las credenciales de inicio de sesión incluyen un secreto asociado con la estructura de datos local; codificando las credenciales de inicio de sesión un identificador de la estructura de datos local o el contenido de la estructura de datos local como un todo, junto con el secreto;
autentificar (1220) al usuario para otorgar acceso al dispositivo informático de destino basado en las credenciales de inicio de sesión recibidas;
enviar (1230), por el dispositivo informático de destino, una solicitud de recuperación al sistema de memoria temporal en el que la solicitud de recuperación se genera en base a las credenciales de inicio de sesión para solicitar la recuperación de la estructura de datos almacenados temporalmente;
en respuesta a la solicitud de recuperación, recibir (1240), en el dispositivo informático de destino, una copia de la estructura de datos almacenados temporalmente y otorgar acceso a la estructura de datos recibida para el usuario autentificado en el que la estructura de datos recibida sigue siendo la única copia persistente de la estructura de datos.

8. El procedimiento implementado por ordenador de la reivindicación 7, en el que se recibe una representación digital particular desde un dispositivo de escáner en respuesta a la exploración de un identificador de elemento correspondiente asociado con un artículo físico particular respectivo.

9. El procedimiento implementado por ordenador de la reivindicación 7, en el que se recibe una representación digital particular desde un dispositivo informático en respuesta a una entrada del usuario de un identificador de elemento particular asociado con un artículo físico particular respectivo.

10. El procedimiento implementado por ordenador según una cualquiera de las reivindicaciones 7 a 9, que comprende, además:

mostrar, mediante el dispositivo informático de origen, una página de interfaz de usuario para visualizar los datos que incluyen una o más representaciones digitales;
en respuesta a una nueva representación de la página de interfaz de usuario, generar, en el dispositivo informático de origen, un código legible por máquina para el usuario como credenciales de inicio de sesión, incluyendo el código legible por máquina información codificada con respecto a la estructura de datos local y el secreto;
escanear, en el dispositivo informático de destino, el código legible por máquina y generar la solicitud de recuperación en base al código legible por máquina escaneado;
recibir, en el dispositivo informático de origen, un testigo desde el sistema de memoria temporal en el que el testigo se genera a partir del secreto en el código legible por la máquina;
autentificar al usuario comprobando el testigo en el dispositivo informático de origen; y si el testigo es correcto, enviar, mediante el dispositivo informático de origen, una notificación de autentificación con respecto al usuario al sistema de memoria temporal.

11. Un procedimiento implementado por ordenador (2000) ejecutado por un sistema de memoria temporal para la transmisión de datos desde un dispositivo informático de origen a un dispositivo informático de destino con protección de datos mejorada, comprendiendo el procedimiento:

recibir (2100) una copia de una estructura de datos local desde el dispositivo informático de origen, estando la estructura de datos recibida destinada a ser transmitida al dispositivo informático de destino, en el que la estructura de datos recibida incluye datos con una o más representaciones digitales de uno o más elementos físicos en el que los elementos físicos pertenecen a una selección de elementos de un individuo en particular;
almacenar temporalmente (2110) la estructura de datos recibida;
recibir (2120), desde el dispositivo informático de destino, una solicitud de recuperación para la estructura de datos almacenados temporalmente;
recibir (2130) una notificación de autentificación en la que la notificación de autentificación indica al sistema de memoria temporal que un usuario fue autentificado en base a las credenciales de inicio de sesión que se generaron específicamente para que el usuario acceda a la estructura de datos en el dispositivo informático de destino, en el que las credenciales de inicio de sesión codifican un identificador de la estructura de datos local o el contenido de la estructura de datos local como un todo, junto con un secreto; en respuesta a la solicitud de recuperación y la notificación de autentificación, enviar una copia de la estructura de datos almacenados temporalmente al dispositivo informático de destino; y
eliminar (2140) la estructura de datos almacenados temporalmente tras la recepción de la copia de la estructura de datos almacenados temporalmente por el dispositivo informático de destino.

12. El procedimiento implementado por ordenador de la reivindicación 11, que comprende, además:

en respuesta a la recepción (2100) de la estructura de datos local:

generar (2101) las credenciales de inicio de sesión;
enviar (2102) las credenciales de inicio de sesión al dispositivo informático de origen; y
enviar (2103) instrucciones de bloqueo al dispositivo informático de destino para bloquear el dispositivo informático de destino contra el acceso no autorizado.

13. El procedimiento implementado por ordenador de la reivindicación 11 o 12, que comprende, además:

recibir (2131) un mensaje de éxito desde el dispositivo informático de destino tras la recepción con éxito de la estructura de datos almacenados temporalmente; y
ejecutar la eliminación (2140) de la estructura de datos almacenados temporalmente en respuesta a la recepción del mensaje de éxito y reenviar el mensaje de éxito al dispositivo informático de origen como un activador de una función para eliminar la estructura de datos local en el dispositivo informático de origen.

14. Un producto de programa informático para transmisión de datos desde un dispositivo informático de origen a un dispositivo informático de destino con protección de datos mejorada; comprendiendo el producto de programa informático instrucciones que cuando se cargan en porciones de memoria correspondientes de dispositivos terminales de un sistema informático y se ejecutan por una pluralidad de procesadores de los dispositivos terminales hacen que los dispositivos terminales realicen las etapas del procedimiento de acuerdo con una cualquiera de las reivindicaciones 7 a 10.

15. Producto de programa informático para transmisión de datos desde un dispositivo informático de origen a un dispositivo informático de destino con protección de datos mejorada; comprendiendo el producto de programa informático instrucciones que cuando se cargan en una memoria de un sistema de memoria temporal y se ejecutan por uno o más procesadores del sistema de memoria temporal hacen que el sistema de memoria temporal realice las etapas del procedimiento de acuerdo con una cualquiera de las reivindicaciones 11 a 13.

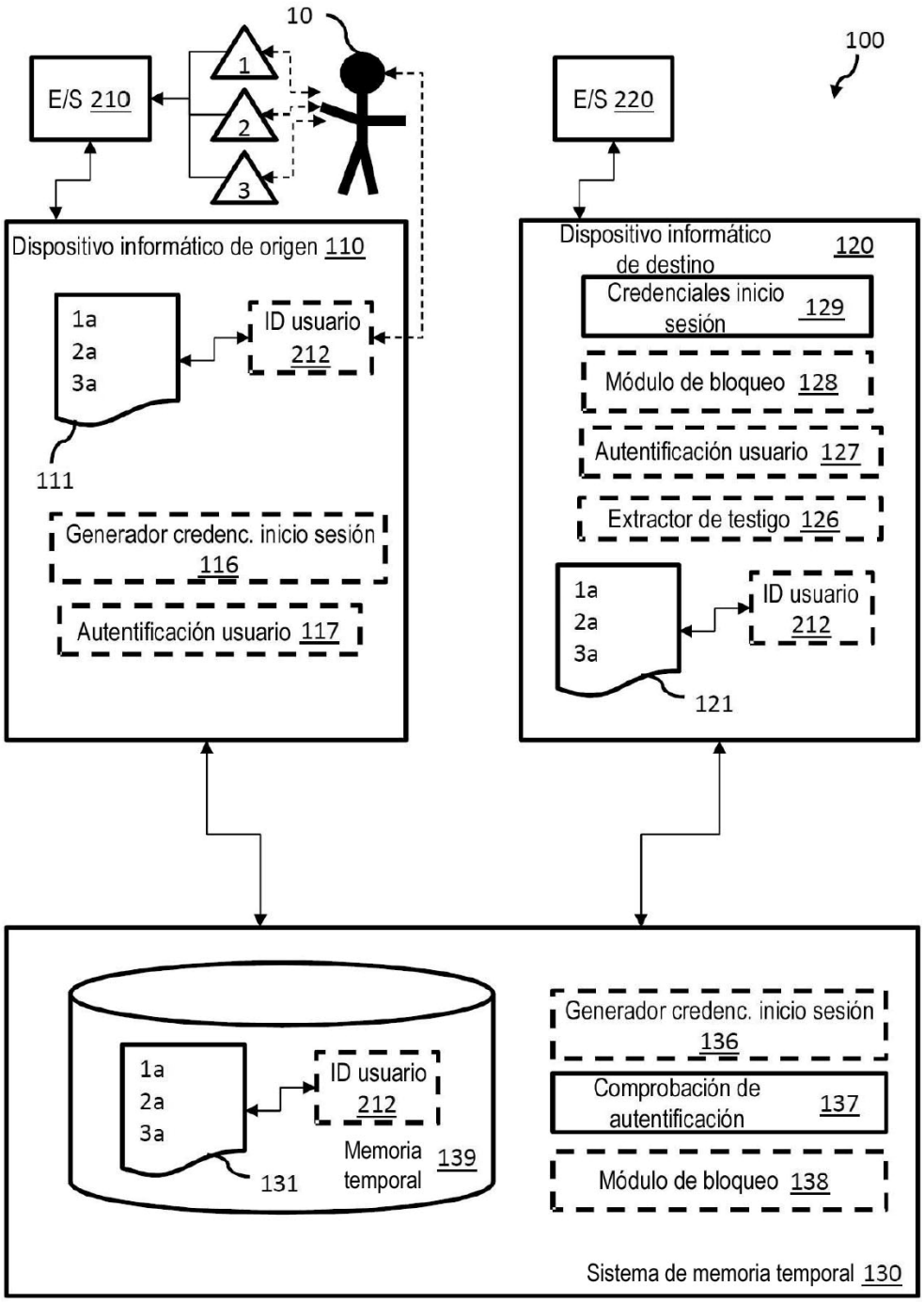
10
100
E/S 210
E/S 220
1
2
3
Dispositivo informático de origen 110
Dispositivo informático de destino 120
1a
2a
3a
ID usuario 212
111
Generador credenc. inicio sesión 116
Autentificación usuario 117
Credenciales inicio sesión 129
Módulo de bloqueo 128
Autentificación usuario 127
Extractor de testigo 126
121
Generador credenc. inicio sesión 136
Comprobación de autentificación 137
Módulo de bloqueo 138
Memoria temporal 139
131
Sistema de memoria temporal 130

FIG. 1

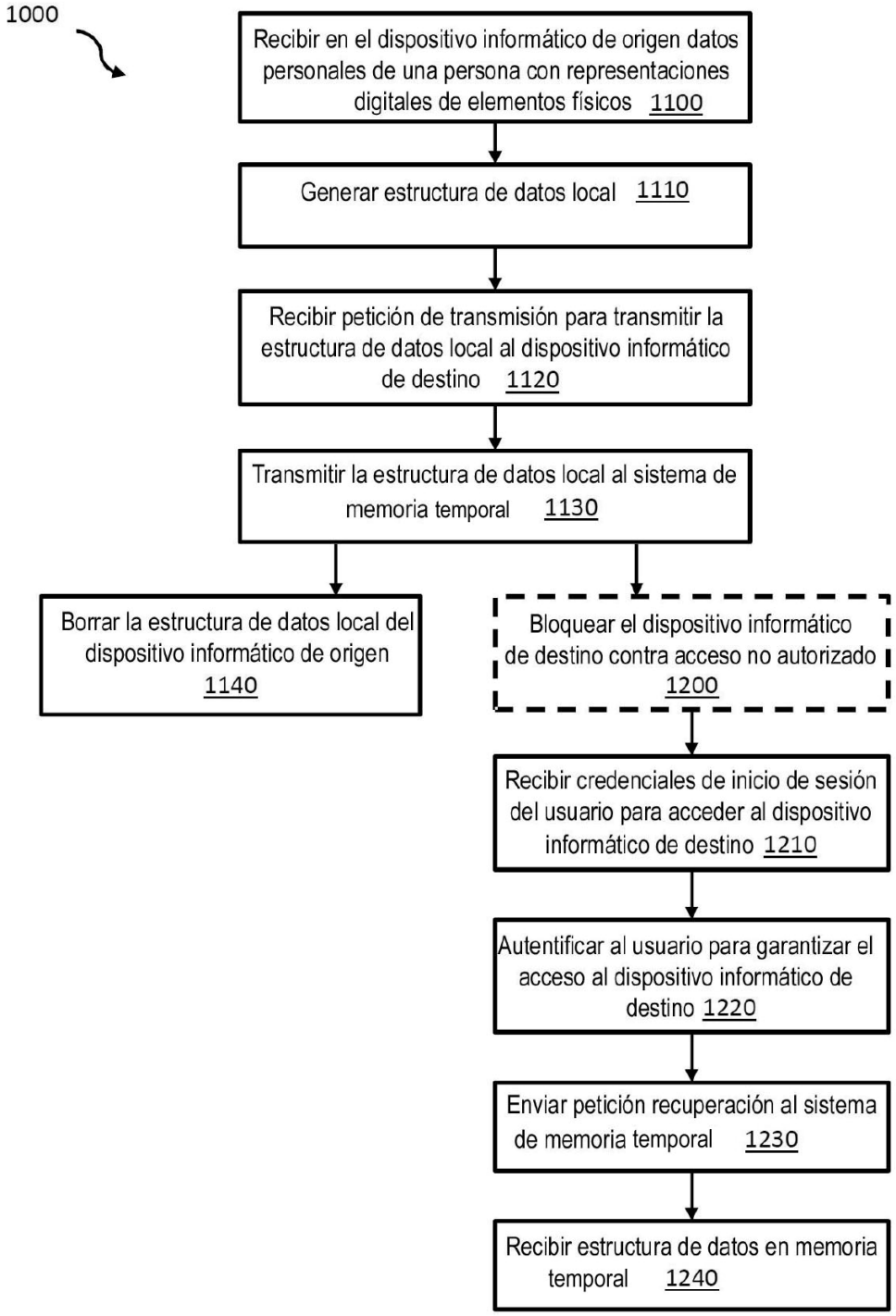
1000
Recibir en el dispositivo informático de origen datos personales de una persona con representaciones digitales de elementos físicos 1100
Generar estructura de datos local 1110
Recibir petición de transmisión para transmitir la estructura de datos local al dispositivo informático de destino 1120
Transmitir la estructura de datos local al sistema de memoria temporal 1130
Borrar la estructura de datos local del dispositivo informático de origen 1140
Bloquear el dispositivo informático de destino contra acceso no autorizado 1200
Recibir credenciales de inicio de sesión del usuario para acceder al dispositivo informático de destino 1210
Autentificar al usuario para garantizar el acceso al dispositivo informático de destino 1220
Enviar petición recuperación al sistema de memoria temporal 1230
Recibir estructura de datos en memoria temporal 1240

FIG. 2

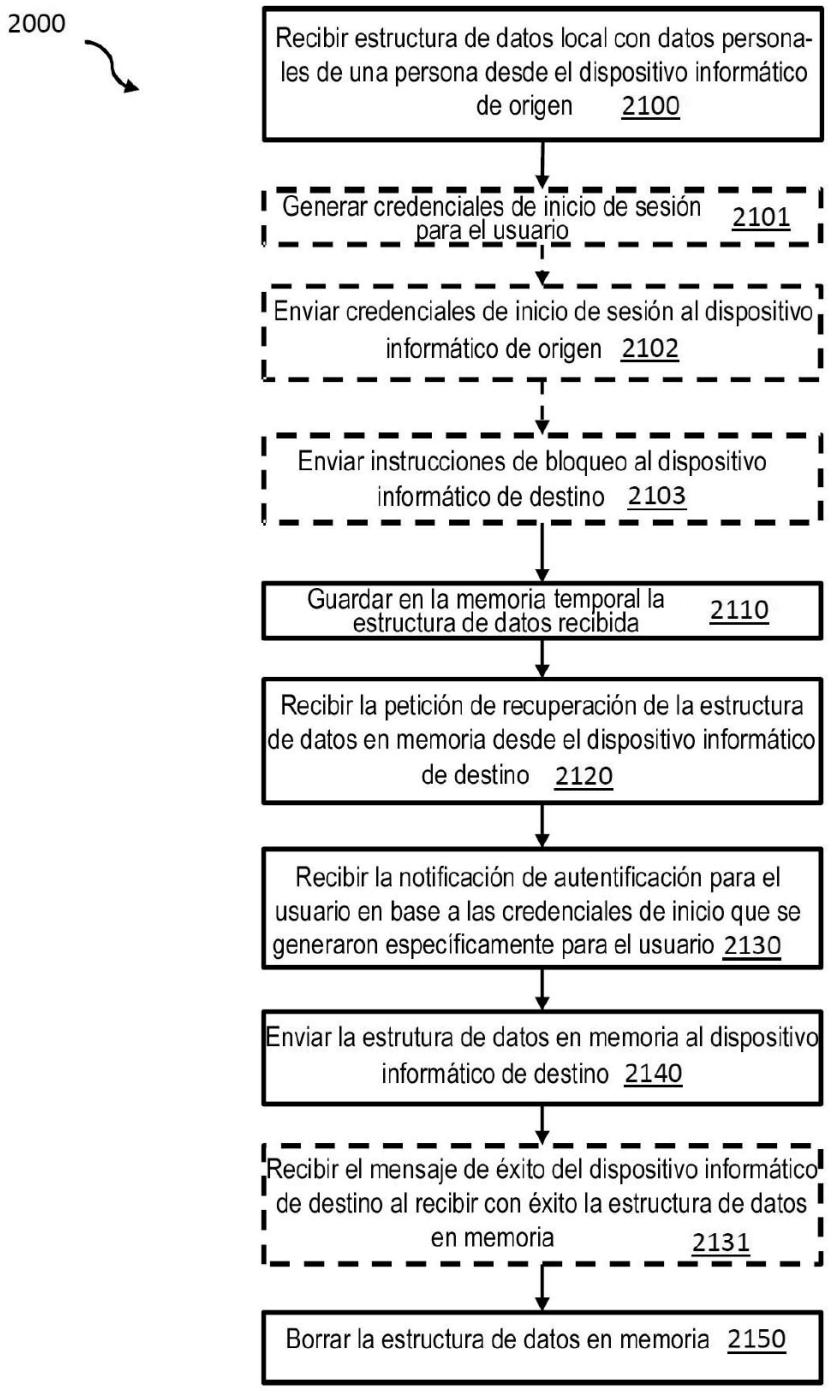
2000
Recibir estructura de datos local con datos personales de una persona desde el dispositivo informático de origen 2100
Generar credenciales de inicio de sesión para el usuario 2101
Enviar credenciales de inicio de sesión al dispositivo informático de origen 2102
Enviar instrucciones de bloqueo al dispositivo informático de destino 2103
Guardar en la memoria temporal la estructura de datos recibida 2110
Recibir la petición de recuperación de la estructura de datos en memoria desde el dispositivo informático de destino 2120
Recibir la notificación de autentificación para el usuario en base a las credenciales de inicio que se generaron específicamente para el usuario 2130
Enviar la estrutura de datos en memoria al dispositivo informático de destino 2140
Recibir el mensaje de éxito del dispositivo informático de destino al recibir con éxito la estructura de datos en memoria 2131
Borrar la estructura de datos en memoria 2150

FIG. 3

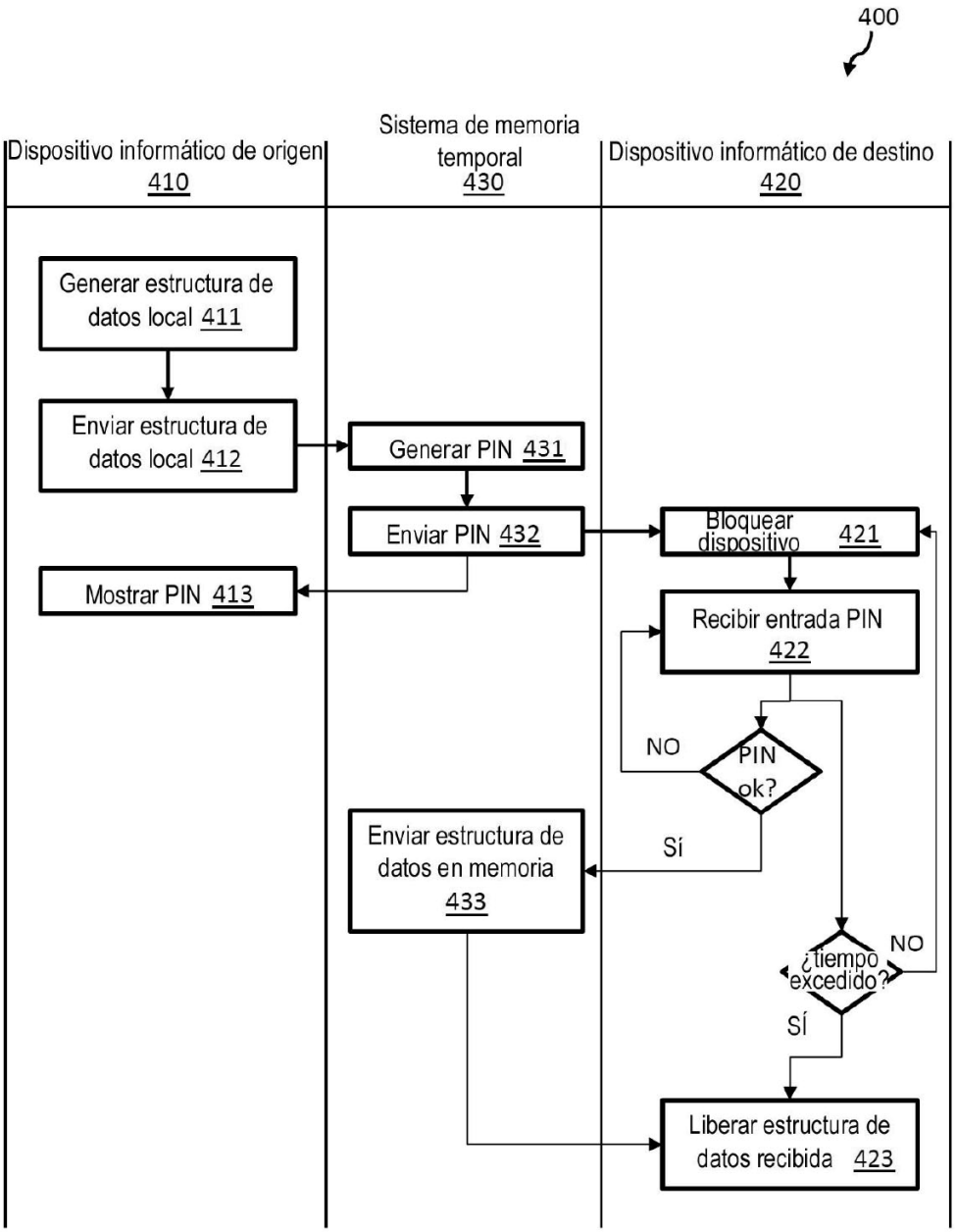
400
Dispositivo informático de origen 410
Sistema de memoria temporal 430
Dispositivo informático de destino 420
Generar estructura de datos local 411
Enviar estructura de datos local 412
Generar PIN 431
Enviar PIN 432
Mostrar PIN 413
Bloquear dispositivo 421
Recibir entrada PIN 422
NO
PIN ok?
Sí
Enviar estructura de datos en memoria 433
¿tiempo excedido?
NO
SÍ
Liberar estructura de datos recibida 423

FIG. 4

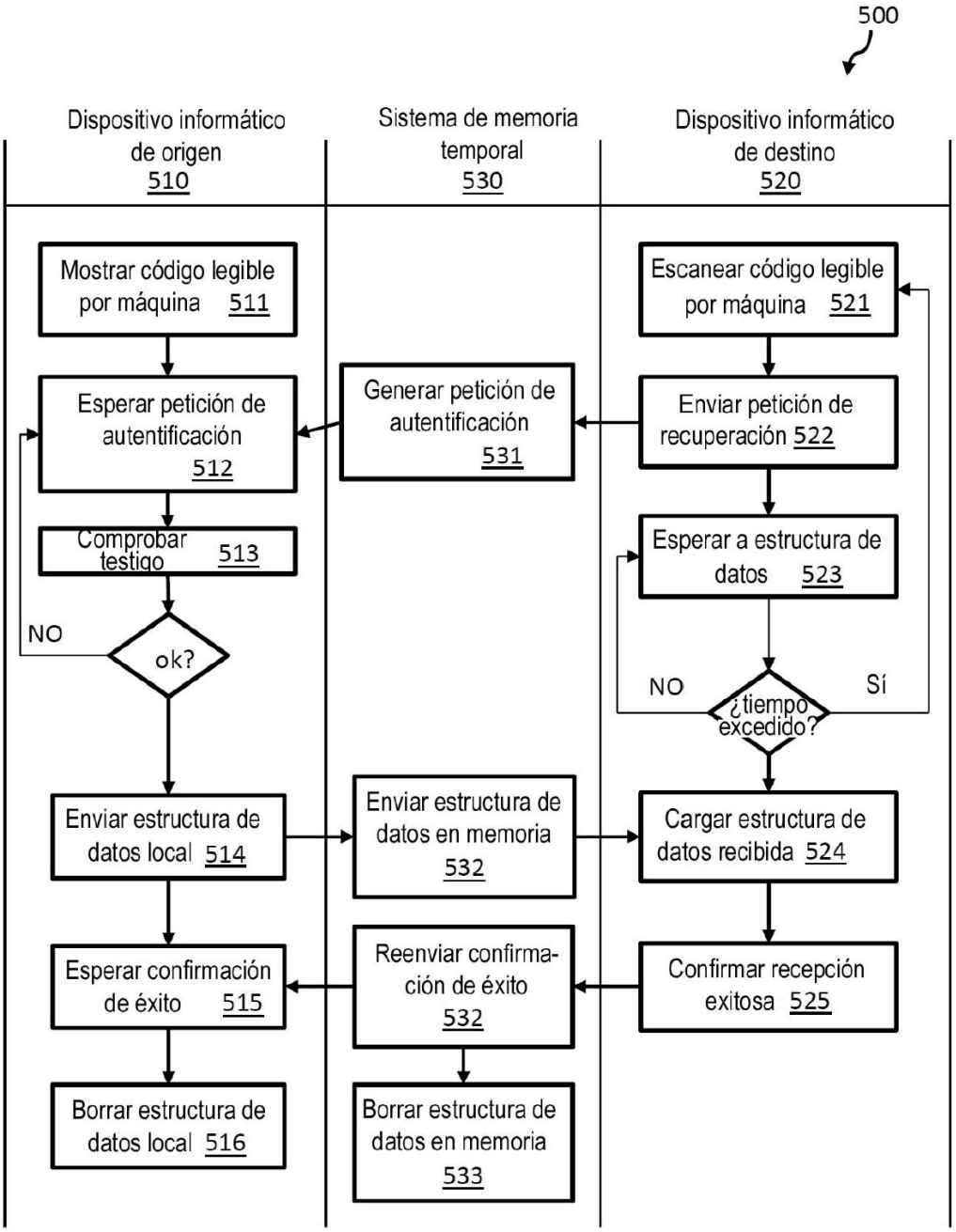
500
Dispositivo informático de origen 510
Sistema de memoria temporal 530
Dispositivo informático de destino 520
Mostrar código legible por máquina 511
Esperar petición de autentificación 512
Comprobar testigo 513
ok?
NO
Enviar estructura de datos local 514
Esperar confirmación de éxito 515
Borrar estructura de datos local 516
Generar petición de autentificación 531
Enviar estructura de datos en memoria 532
Reenviar confirmación de éxito 532
Borrar estructura de datos en memoria 533
Escanear código legible por máquina 521
Enviar petición de recuperación 522
Esperar a estructura de datos 523
¿tiempo excedido?
NO
Sí
Cargar estructura de datos recibida 524
Confirmar recepción exitosa 525

FIG. 5

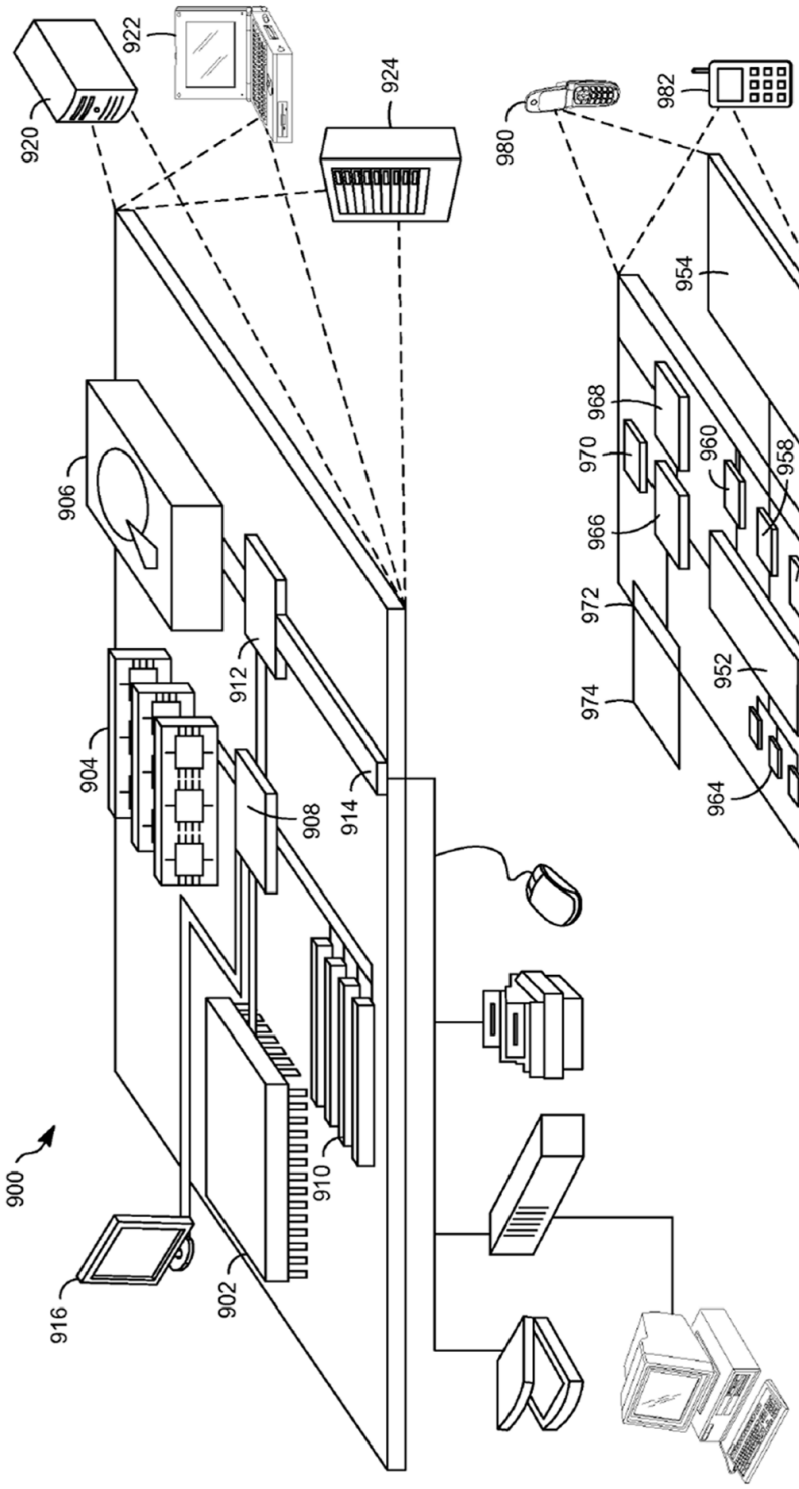
920
922
924
980
982
954
968
970
960
958
906
966
956
972
912
952
974
962
904
908
914
964
950
900
910
916
902

FIG. 6