(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **3 015 231**

(51) Int. CI.:

G06Q 20/40 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **19.06.2019 PCT/EP2019/066274**

(87) Fecha y número de publicación internacional: **09.01.2020 WO20007618**

(96) Fecha de presentación y número de la solicitud europea: **19.06.2019 E 19735228 (9)**

(97) Fecha y número de publicación de la concesión europea: **19.03.2025 EP 3818486**

(54) Título: **Recuperar un código de seguridad de tarjeta original usado en una transacción basada en tarjeta**

(30) Prioridad:

06.07.2018 SE 1850858

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.04.2025

(73) Titular/es:

NO COMMON PAYMENT AB (100.00%)
Box 1345
111 83 Stockholm, SE

(72) Inventor/es:

CARLEMALM, FREDRIK

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Recuperar un código de seguridad de tarjeta original usado en una transacción basada en tarjeta

Solicitudes de patente relacionadas

Esta solicitud de patente se relaciona con la solicitud de patente sueca núm. SE1651165-1, que se presentó el 30 de agosto de 2016.

Esta solicitud de patente también se relaciona con la solicitud de patente internacional PCT núm. PCT/SE2017/050858, que se presentó el 24 de agosto de 2017.

Campo técnico

La presente divulgación se refiere generalmente al campo de las transacciones basadas en tarjetas. En más detalle, la presente divulgación se refiere a un desarrollo adicional de la tecnología que se describe en los documentos SE1651165-1 y PCT/SE2017/050858.

Más específicamente, las realizaciones descritas en la presente memoria se refieren a procedimientos y sistemas de servidor (por ejemplo, que incluyen uno o más servidores informáticos) para recuperar el CSC original de un CSC temporal, por ejemplo, usado en una transacción basada en tarjeta. El CSC original puede, por ejemplo, ser un Valor de Verificación de Tarjeta (CVV), un CVV2, un Código de Verificación de Tarjeta (CVC), un CVC2, un Número de Validación de Tarjeta (CVN), un CVN2 o un Número de Identificación de Tarjeta (CID).

Antecedentes

La industria bancaria ha desarrollado un tipo de “contraseña” para su uso con tarjetas tales como tarjetas de crédito y tarjetas de débito. Esta contraseña típicamente toma la forma de un código de autenticación (a veces denominado CSC) y se denomina comúnmente en la industria “valor de verificación de tarjeta” o “CVV”. El CVV se formatea y usa de acuerdo con los estándares de la industria aceptados. Inicialmente, el CVV era una cadena numérica adicional codificada en la banda magnética de las tarjetas de crédito y débito.

Más recientemente, se ha impreso un código adicional de tres dígitos en la parte posterior, o lado trasero, de las tarjetas de crédito y débito. Este código impreso se denomina comúnmente dentro de la industria bancaria como un código “CVV2” y el código almacenado magnéticamente se denomina comúnmente como un código “CVV1”. El código impreso puede, por ejemplo, solicitarse y verificarse por los comerciantes en transacciones donde el comerciante no tiene otra forma de verificar realmente que el cliente tiene posesión de la tarjeta física.

Por ejemplo, en transacciones móviles o en transacciones en línea, se puede solicitar al consumidor que ingrese el código CVV2 de la parte posterior de su tarjeta. El código CVV2 puede proporcionar cierta garantía de que el consumidor tiene posesión de la tarjeta de crédito o débito física, y no simplemente ha obtenido el número de tarjeta y la fecha de vencimiento de manera fraudulenta. Un código CW impreso a veces también se denomina por los consumidores y los vendedores en línea como un “código de seguridad de 3 dígitos”, “código de seguridad” o “dígitos de verificación”.

SE1651165-1 *entre otros* describe un procedimiento para generar un CSC temporal realizado por un terminal móvil (por ejemplo, un teléfono móvil). El procedimiento es adecuado para su uso en una transacción basada en tarjeta con un sistema de servidor que tiene uno o varios servidores informáticos. De acuerdo con ciertas realizaciones de SE1651165-1, el procedimiento propuesto incluye: obtener un CSC de una tarjeta, tal como una tarjeta de crédito o una tarjeta de débito; obtener una semilla de datos, la semilla de datos incluye un identificador de terminal móvil y una marca de tiempo; y generar, o calcular de otro modo, una suma total de la semilla de datos y el CSC y, después, aplicar una función hash perfecta mínima a la suma total generada para generar el CSC temporal.

El documento WO 2018/044221A1 describe un procedimiento para generar un CSC temporal para su uso en una transacción basada en tarjeta.

Sumario

Esta descripción reconoce que algunas soluciones existentes para transacciones basadas en tarjetas, y particularmente transacciones móviles y en línea, aún pueden ser inadecuadas. Por lo tanto, es un objeto general de las realizaciones descritas en la presente memoria desarrollar aún más la tecnología que se conoce en la técnica existente.

Por lo tanto, en vista del trasfondo anterior, se han realizado las diversas realizaciones divulgadas en la presente memoria.

Es un objetivo general de las realizaciones descritas en la presente memoria permitir un desarrollo adicional de transacciones basadas en tarjetas que ofrezcan prevención, o al menos complicación, del uso no autorizado de tarjetas (por ejemplo, tarjetas de crédito o de débito) al limitar el acceso a cuentas asociadas con dichas tarjetas a entidades, procesos y/o individuos no autorizados.

Este objeto general se ha abordado mediante las reivindicaciones independientes adjuntas. Las realizaciones ventajosas se definen en las reivindicaciones dependientes adjuntas.

En un primer aspecto, esta descripción se refiere a un procedimiento para recuperar un Código de Seguridad de tarjeta (CSC) original de un CSC temporal usado en una transacción basada en tarjeta. El procedimiento comprende obtener un CSC temporal, en el que el CSC temporal se ha generado aplicando previamente una función hash perfecta mínima al CSC así como también una primera semilla de datos; obtener o producir de cualquier otra manera una segunda semilla de datos; y aplicar una misma función hash perfecta mínima a la segunda semilla de datos obtenida junto con cada uno de varios CSC de una lista almacenada de CSC disponibles hasta que se encuentre una coincidencia entre el CSC temporal obtenido y un CSC de la lista almacenada de CSC disponibles, para recuperar de esta manera el CSC original.

La segunda semilla de datos es una misma semilla de datos como la primera semilla de datos. En otras palabras, se puede decir que la primera semilla de datos es igual a la segunda semilla de datos. Es decir, la segunda semilla de datos es típicamente la misma semilla de datos que se usó durante la generación anterior del CSC temporal.

En algunas realizaciones, el procedimiento puede realizarse por un sistema de servidor que comprende uno o varios ordenadores, o servidores informáticos. Por ejemplo, en algunas realizaciones el procedimiento puede realizarse por uno cualquiera o una combinación de i) un sistema de proveedor de servicios que tiene uno o varios servidores informáticos y ii) un sistema emisor de crédito que tiene uno o varios servidores informáticos.

Ventajosamente, pero no necesariamente, el CSC temporal puede haberse generado aplicando previamente una función hash perfecta mínima a un CSC original, así como también una semilla de datos de acuerdo con las enseñanzas de SE1651165-1 (o, PCT/SE2017/050858), ver también la sección Antecedentes en la presente descripción.

Como se apreciará, el procedimiento puede comprender adicionalmente, en respuesta a que se haya encontrado una coincidencia, continuar una transacción basada en tarjeta iniciada.

En realizaciones ventajosas, la primera semilla de datos incluye un identificador de terminal móvil y una marca de tiempo. Como se apreciará, la segunda semilla de datos puede por lo tanto incluir también un identificador de terminal móvil correspondiente y una marca de tiempo correspondiente. En consecuencia, la segunda semilla de datos puede incluir el mismo identificador de terminal móvil y la misma marca de tiempo que la primera semilla de datos.

En algunas realizaciones, obtener el CSC temporal puede comprender recibir una señal de un dispositivo remoto o un sistema de servidor remoto, en el que la señal comprende el CSC temporal. En una realización ilustrativa, el CSC temporal puede recibirse desde un terminal móvil. Por ejemplo, el CSC temporal puede recibirse desde el terminal móvil que generó el CSC temporal. Ventajosamente, pero no necesariamente, el CSC temporal puede recibirse desde el terminal móvil que generó el CSC temporal durante una transacción basada en tarjeta.

La segunda semilla de datos puede obtenerse o producirse de cualquier otra manera, como apreciarán los expertos en la técnica a la que se refiere esta solicitud de patente. Por ejemplo, la obtención de la segunda semilla de datos (es decir, típicamente la misma semilla de datos que se usó durante la generación del CSC temporal como se describió anteriormente en la presente descripción) puede lograrse mediante la recepción o determinación de partes no estáticas de esa semilla de datos (por ejemplo, una marca de tiempo asociada con una transacción actual (por ejemplo, en curso) basada en tarjeta) y/o mediante la recepción o recuperación de partes estáticas de esa semilla de datos (por ejemplo, un identificador de terminal móvil, como un IMSI). En otras palabras, es posible reproducir una misma semilla de datos como la semilla de datos que se usó durante la generación del CSC temporal.

Como se apreciará, en algunas realizaciones el identificador de terminal móvil (por ejemplo, IMSI) de la segunda semilla de datos puede obtenerse al recibir el identificador de terminal móvil desde el terminal móvil (por ejemplo, durante una transacción basada en tarjeta) que generó el CSC temporal. Alternativamente, el identificador de terminal móvil (por ejemplo, IMSI) de la segunda semilla de datos puede obtenerse al recuperar el identificador de terminal móvil de un almacenamiento interno o externo. Además, puede recibirse una marca de tiempo de la segunda semilla de datos (por ejemplo, la marca de tiempo asociada con una transacción basada en tarjeta actual (posiblemente en curso)) desde el terminal móvil que generó el CSC temporal. Alternativamente, la marca de tiempo de la segunda semilla de datos puede ser determinada o establecida de otro modo por el sistema servidor.

En un segundo de sus aspectos, esta descripción se refiere a un programa informático que comprende instrucciones que, cuando se ejecutan en un procesador, hacen que el procesador lleve a cabo el procedimiento de acuerdo con el primer aspecto. También puede proporcionarse un portador que comprende el programa informático de acuerdo con

el segundo aspecto. El portador puede ser una señal electrónica, una señal óptica, una señal de radio o un medio de almacenamiento legible por ordenador.

En un tercio de sus aspectos, esta descripción se refiere a un sistema de servidor que tiene uno o varios servidores informáticos. Por ejemplo, el sistema de servidor informático puede comprender una interfaz de comunicaciones; uno o más procesadores; y una memoria que almacena instrucciones, ejecutables por el uno o más procesadores, de manera que el servidor de proveedor de servicios es operativo para realizar el procedimiento del primer aspecto.

Como se apreciará, algunas realizaciones descritas en la presente memoria permiten recuperar un CSC original (por ejemplo, asociado con una tarjeta tal como una tarjeta de crédito o tarjeta de débito) de un CSC temporal, que es, como implica el nombre, válido solo por un período de tiempo limitado. Aquí, el CSC temporal se asociaría exclusivamente con el CSC original o normal. En comparación con un CSC original o normal, el CSC temporal sería más difícil de obtener fraudulentamente. Por ejemplo, si una transacción de compra se produce en línea, generalmente se requiere el CSC de la parte posterior de la tarjeta como una medida de seguridad adicional para reducir el fraude. Sin embargo, este CSC podría, por ejemplo, obtenerse fraudulentamente por una entidad, proceso o individuo que está en posesión errónea de la tarjeta. Al añadir también la aplicación de una función hash perfecta mínima al CSC original, o normal, así como también una semilla de datos como se analiza en SE1651165-1 y en PCT/SE2017/050858, se hace posible generar un CSC temporal que es más difícil de obtener fraudulentamente. Dado que el CSC temporal es más difícil de obtener fraudulentamente, este CSC temporal también puede ser más seguro de usar en una transacción posterior basada en tarjeta, tal como una transacción de compra móvil o en línea.

Como se apreciará, además, las realizaciones descritas en la presente memoria permiten recuperar el CSC original del CSC temporal mencionado anteriormente. Al aplicar la misma función hash perfecta mínima a la segunda semilla de datos obtenida junto con cada CSC de una lista de CSC disponibles almacenados en el sistema de proveedor de servicios hasta que se encuentre una coincidencia entre un CSC temporal obtenido y un CSC de la lista de CSC disponibles, es posible recuperar el CSC original asociado con el CSC temporal sin realizar cálculos innecesariamente complejos o incluso imposibles. A su vez, esto puede permitir un proceso relativamente rápido para recuperar el CSC original de un CSC temporal. Esto también puede hacer que el procedimiento propuesto sea cada vez más útil en la práctica.

Breve descripción de las figuras

Estos y otros aspectos, características y ventajas serán evidentes y se explicarán a partir de la siguiente descripción de varias realizaciones, con referencia a los dibujos adjuntos, en los que:

La Figura 1 ilustra esquemáticamente una realización ilustrativa de una tarjeta tal como una tarjeta de débito o de crédito;
La Figura 2 ilustra esquemáticamente un lado trasero de la tarjeta mostrada en la FIGURA 1;
La Figura 3 es un diagrama de flujo que ilustra las etapas, o acciones, de acuerdo con una realización de un procedimiento para generar un CSC temporal;
Las Figuras 4A-4B ilustran esquemáticamente un ejemplo de una función de Hash Perfecto Mínimo (MPH);
Las Figuras 5A-5C ilustran esquemáticamente una aplicación de una función MPH a un
CSC, así como también una semilla de datos, de acuerdo con realizaciones ilustrativas;
La Figura 6 es un diagrama de flujo que ilustra las etapas, o acciones, de acuerdo con una realización de un procedimiento para recuperar un CSC original de un CSC temporal;
La Figura 7A es un diagrama de bloques de un sistema donde las realizaciones descritas en la presente memoria podrían reducirse a la práctica;
La Figura 7B es un diagrama de señalización que ilustra esquemáticamente las acciones realizadas en el sistema de la Figura 7A, de acuerdo con algunas realizaciones;
La Figura 8 muestra una implementación de ejemplo de una realización de un sistema de servidor tal como un sistema de proveedor de servicios;
La Figura 9 ilustra un portador que comprende un programa informático, de acuerdo con una realización.

Descripción detallada

La presente invención se describirá ahora más completamente en lo sucesivo. La invención puede, sin embargo, estar incorporada en muchas formas diferentes y no debe interpretarse como limitada a las realizaciones establecidas en la presente memoria; más bien, estas realizaciones se proporcionan a manera de ejemplo para que esta descripción sea exhaustiva y completa, y transmita completamente el alcance de la invención a los expertos en la técnica. Los números de referencia similares se refieren a elementos o etapas del procedimiento similares a lo largo de esta descripción.

Como se describió anteriormente, algunas soluciones existentes para transacciones basadas en tarjetas aún pueden ser inadecuadas. Por lo tanto, es un objeto general de las realizaciones descritas en la presente memoria permitir un desarrollo adicional de transacciones basadas en tarjetas que ofrezcan la prevención, o al menos la complicación, del uso no autorizado de tarjetas (por ejemplo, tarjetas de crédito o de débito) al limitar el acceso a cuentas asociadas con dichas tarjetas a entidades, procesos y/o individuos no autorizados.

Los documentos SE1651165-1 y PCT/SE2017/050858 han propuesto un procedimiento y un sistema para una transacción basada en tarjeta entre un terminal móvil (por ejemplo, un teléfono móvil o una tableta) y un sistema de proveedor de servicios que tiene uno o varios servidores informáticos. Por ejemplo, el terminal móvil puede obtener un CSC de una tarjeta, tal como una tarjeta de crédito o una tarjeta de débito. Además, el terminal móvil puede obtener una semilla de datos, que, en algunas realizaciones, puede incluir una marca de tiempo y/o un identificador tal como un identificador de terminal móvil (por ejemplo, un IMSI). Además, el terminal móvil puede aplicar una función hash perfecta mínima al CSC, así como también la semilla de datos para generar un CSC temporal. Además, el terminal móvil puede iniciar una transacción basada en tarjeta con el sistema de proveedor de servicios mediante el uso del CSC temporal generado así. Además, el sistema del proveedor de servicios puede obtener dicho CSC temporal (por ejemplo, al recibir el CSC temporal generado desde el terminal móvil). Aún más, el sistema de proveedor de servicios también puede aplicar la misma función hash perfecta mínima al CSC temporal en su extremo hasta que se encuentre una coincidencia entre el CSC temporal obtenido y un CSC de una lista almacenada de CSC disponibles. En respuesta a que se haya encontrado una coincidencia, el sistema de proveedor de servicios también puede continuar la transacción basada en tarjeta iniciada con el terminal móvil.

Para abordar los desafíos mencionados anteriormente, de acuerdo con una realización de ejemplo, en la presente memoria se describen un procedimiento y un sistema de servidor para recuperar un CSC original de un CSC temporal, por ejemplo, usado en una transacción basada en tarjeta. El CSC temporal puede haberse generado aplicando previamente una función hash perfecta mínima a un CSC original, así como también una semilla de datos de acuerdo con las enseñanzas de SE1651165-1 (o, PCT/SE2017/050858), ver también la sección Antecedentes en la presente descripción. Por ejemplo, un sistema de servidor (por ejemplo, un sistema de proveedor de servicios) que tiene uno o varios servidores informáticos, puede obtener un CSC temporal, en el que el CSC temporal se ha generado aplicando previamente una función hash perfecta mínima al CSC así como también una primera semilla de datos; obtener una segunda semilla de datos, la segunda semilla de datos es una misma semilla de datos como la primera semilla de datos; y aplicar la misma función hash perfecta mínima a la segunda semilla de datos obtenida junto con cada uno de varios CSC de una lista almacenada de CSC disponibles hasta que se encuentre una coincidencia entre el CSC temporal obtenido y un CSC de la lista almacenada de CSC disponibles.

En respuesta a que se haya encontrado una coincidencia, el sistema del proveedor de servicios también puede incluir continuar una transacción basada en tarjeta iniciada.

Como se apreciará, el sistema de servidor puede obtener el CSC temporal mencionado anteriormente (por ejemplo, al recibir el CSC temporal generado desde el terminal móvil) así como también la misma semilla de datos que se usó en la generación del CSC temporal (por ejemplo, mediante el uso de la marca de tiempo de la transacción basada en tarjeta ya iniciada junto con un identificador de terminal móvil almacenado (por ejemplo, un IMSI) para obtener o producir de cualquier otra manera la segunda semilla de datos, por ejemplo, de la misma manera o de cualquier otra manera que lo haría el terminal móvil. Aún más, el sistema de servidor también puede aplicar la misma función hash perfecta mínima a la misma semilla de datos junto con cada CSC de una lista almacenada de CSC disponibles, hasta que se encuentre una coincidencia entre el CSC temporal obtenido y un CSC de esa lista almacenada de CSC disponibles, por lo tanto, se recupera el CSC original. En respuesta a que se haya encontrado una coincidencia, el sistema de proveedor de servicios también puede continuar la transacción basada en tarjeta ya iniciada con el terminal móvil, directamente o después de verificar el CSC original recuperado con, por ejemplo, el emisor de crédito.

De esta manera, se hace posible recuperar un CSC original de un CSC temporal (que se ha generado previamente a partir de dicho CSC original) sin realizar cálculos innecesariamente complejos o incluso imposibles. Esto también puede permitir un proceso relativamente rápido de recuperación del CSC original, lo que hace que la técnica sea cada vez más útil en la práctica.

Esto permitiría entonces el uso de un CSC temporal, que es válido solo por un período de tiempo limitado, por ejemplo, mediante el uso de una semilla de datos que contiene una marca de tiempo cuando se genera. Aquí, el CSC temporal generado se asociaría generalmente de manera única con el CSC original, o normal. En comparación con el CSC original o normal, el CSC temporal es así comparativamente más difícil de obtener fraudulentamente.

Por ejemplo, si una transacción de compra se produce en línea, generalmente se requiere el CSC de la parte posterior de la tarjeta como una medida de seguridad adicional para reducir el fraude. Sin embargo, este CSC podría, por ejemplo, obtenerse fraudulentamente por una entidad, proceso o individuo que está en posesión errónea de la tarjeta. Al añadir también la aplicación de una función hash perfecta mínima al CSC original, o normal, así como también una semilla de datos, se hace posible generar un CSC temporal que es comparativamente más difícil de obtener fraudulentamente. Dado que el CSC temporal es más difícil de obtener fraudulentamente, este CSC temporal también puede ser más seguro de usar en una transacción posterior basada en tarjeta, tal como una transacción de compra móvil o en línea.

Antes de describir las realizaciones de la presente divulgación con más detalle y para dar contexto a estas realizaciones, las funciones hash se describirán brevemente. A *función hash* es cualquier función que puede usarse para mapear datos de tamaño arbitrario a datos de tamaño fijo. Los valores devueltos por una función hash se

denominan típicamente valores hash, códigos hash, sumas hash o simplemente hashes. El "CSC temporal" mencionado anteriormente podría verse como un valor hash. Un uso es una estructura de datos llamada tabla hash, ampliamente utilizada en la tecnología informática para la búsqueda rápida de datos. Las funciones hash aceleran típicamente la búsqueda en tablas o bases de datos al detectar registros duplicados en un archivo grande. Una función hash puede permitir verificar fácilmente que algunos datos de entrada se asignan a un valor hash dado, pero si los datos de entrada son desconocidos, es deliberadamente difícil reconstruirlo (o alternativas equivalentes) al conocer el valor hash almacenado. Esto puede usarse para garantizar la integridad de los datos transmitidos. A *función hash perfecta* para un conjunto S es una función hash que asigna elementos distintos en S a un conjunto de números enteros, sin colisiones. Una función hash perfecta tiene muchas de las mismas aplicaciones que otras funciones hash, pero con la ventaja de que no es necesario implementar la resolución de colisiones. En términos matemáticos, es una función inyectiva total. Además, una función hash perfecta generalmente es de orden de conservación si las claves en el conjunto de claves se disponen en algún orden dado y la función hash típicamente conserva este orden en la tabla hash. Una función hash perfecta para un conjunto específico S que puede evaluarse en tiempo constante, y con valores en un intervalo pequeño, puede encontrarse mediante un algoritmo aleatorio en un número de operaciones que es proporcional al tamaño de S. Cualquier función hash perfecta adecuada para su uso con una tabla hash típicamente usa al menos un número de bits que es proporcional al tamaño de S. Una función hash perfecta con valores en un intervalo limitado puede usarse para operaciones de búsqueda eficientes, al colocar claves de S (u otros valores asociados) en una tabla indexada por la salida de la función. El uso de una función hash perfecta es lo mejor en situaciones donde hay un conjunto grande, S, que se consulta con frecuencia, que rara vez se actualiza. Esto se debe a que cualquier modificación del conjunto conduce a una función hash no perfecta. Como se conoce entre los expertos en la técnica, una función *hash perfecta mínima* es una función hash perfecta que asigna *n* claves a *n* números enteros consecutivos, generalmente [O..n-1]o [1..n], O dicho de otra manera: Sea j y k elementos de un conjunto finito K. F es una función hash perfecta mínima si y solo si F(/) = F(/c) implica que j = k (es decir, una función inyectiva) y existe un entero a tal que el intervalo de F es a..a+|K|-1. Se ha demostrado que un esquema de hash perfecto mínimo de propósito general típicamente requiere al menos 1,44 bits/clave. Los mejores esquemas de hashing perfecto mínimo conocidos actualmente parecen usar alrededor de 2,6 bits/clave.

Con referencia ahora a la FIGURA 1, se describirá una tarjeta 1 tal como una tarjeta de crédito o tarjeta de débito que podría usarse con las realizaciones descritas en la presente memoria. La tarjeta 1 puede ser una tarjeta de plástico que tiene el tamaño y la forma de una tarjeta de crédito/débito convencional. Muchas tarjetas de crédito/débito convencionales tienen un tamaño de aproximadamente 85,60 x 53,98 milímetros y se definen por la norma ISO / IEC 7810 como "ID—1 La tarjeta puede proporcionarse con números de tarjeta elevados 2, letras elevadas para un nombre de titular de tarjeta 3, números elevados que indican la fecha de vencimiento 4 (típicamente en el formato MM/YY, donde MM representa el mes y YY representa el año). La tarjeta 1 también puede incluir información del emisor tal como el nombre del banco 5, o el logotipo del banco. Típicamente, pero no necesariamente, la tarjeta 1 también puede incluir información o una marca 6 del proveedor de pago, tal como VISA, MASTERCARD o AMERICAN EXPRESS. Opcionalmente, la tarjeta 1 también puede incluir un chip 7 como se conoce y es convencional en la técnica existente.

Ahora se hace referencia a la Figura 2, que ilustra esquemáticamente la parte posterior de la tarjeta 1. Como puede verse, la tarjeta 1 puede incluir una banda magnética 8 codificada con información sobre la tarjeta como se conoce en la técnica. Además, puede proporcionarse un bloque de firma 9. Tenga en cuenta que, en este ejemplo, el bloque de firma 9 incluye además un CSC impreso, aquí ejemplificado por un código CVV2 de 3 dígitos "123".

La Figura 3 es un diagrama de flujo que ilustra esquemáticamente un procedimiento para generar un CSC temporal (tal como un CVV o CVV2) para su uso en una transacción basada en tarjeta de acuerdo con las enseñanzas de SE1651165-1. El procedimiento puede realizarse por medio de un terminal móvil, por ejemplo, un teléfono móvil.

Inicialmente, el CSC se obtiene 310 de la tarjeta 1. Por ejemplo, este CSC puede obtenerse leyendo el CSC impreso en la tarjeta. En otras palabras, el CSC puede obtenerse no automáticamente, o manualmente, desde la tarjeta 1. Alternativamente, el CSC puede obtenerse automáticamente de la tarjeta 1. Por ejemplo, en algunas realizaciones, el CSC puede leerse ópticamente desde la tarjeta 1.

Además, se obtiene una semilla de datos 320. Como se apreciará, la semilla de datos puede incluir uno cualquiera o una combinación de los siguientes atributos:

- un número de cuenta bancaria;
- un identificador de instalación (es decir, ID de instalación);
- un identificador de teléfono móvil tal como un IMSI; y
- una marca de tiempo.

En algunas realizaciones, la semilla de datos puede comprender, o representar, un identificador que es común a un titular de tarjeta asociado con la tarjeta 1 y un sistema de proveedor de servicios.

La semilla de datos puede obtenerse 320 de diferentes maneras, por ejemplo, en función de las características de la transacción basada en la intención. Por ejemplo, la semilla de datos puede obtenerse de una manera en la que el usuario (típicamente, pero no necesariamente, el titular de la tarjeta) proporciona la semilla de datos al terminal móvil

que ejecuta el procedimiento. Adicionalmente, o alternativamente, obtener 320 la semilla de datos puede comprender recibir una señal que incluye la semilla de datos del sistema de proveedor de servicios que tiene uno o varios servidores informáticos. Por ejemplo, una ID de instalación puede incluirse en una señal recibida desde el sistema de proveedor de servicios. Adicionalmente, o alternativamente, obtener 320 la semilla de datos comprende recibir una señal que incluye la semilla de datos de un sistema de emisor de tarjetas que tiene uno o varios servidores informáticos. Por ejemplo, un número de cuenta bancaria puede incluirse en una señal recibida desde el sistema emisor de la tarjeta. Adicionalmente, o alternativamente, obtener 320 la semilla de datos puede comprender recuperar la semilla de datos de una SIM asociada con el terminal móvil. Por ejemplo, un IMSI puede recuperarse de dicha SIM.

Con referencia continua a la FIGURA 3, una función hash perfecta mínima puede aplicarse 330 al CSC, así como también a la semilla de datos para generar un CSC temporal.

Volviendo ahora a las Figuras 4 y 5, se describirá con más detalle un ejemplo de aplicación 330 de una función hash perfecta mínima a la CSC y la semilla de datos. La FIGURA 4A ilustra esquemáticamente un ejemplo de función hash perfecta mínima. Las funciones hash perfectas mínimas pueden evitar los desafíos de espacio y tiempo desperdiciados, como a veces ocurre en otras funciones hash. O, dicho de otra manera, cada clave en el conjunto de claves tiene una y solo una clave hash correspondiente en la tabla hash. Por ejemplo, al asumir una aplicación que utiliza un CSC de 3 dígitos, habrá 999 números en el conjunto de claves y 999 números correspondientes en la tabla hash. Un ejemplo se da en la FIGURA 4B. En este ejemplo, hay 999 CSC y 999 CSC hasheados correspondientes. Como puede verse, 0 renderiza 998, 1 renderiza 77, 2 renderiza 31, etcétera en este ejemplo ilustrativo.

La función hash exacta, o algoritmo hash, que se usará en una determinada implementación o aplicación puede determinarse o elegirse arbitrariamente, o aleatoriamente. Más específicamente, la función hash exacta, o algoritmo hash, que se usará en una determinada implementación puede determinarse o elegirse arbitrariamente siempre que cumpla con los requisitos de una función hash perfecta mínima que preferentemente no conserva el orden. Como se apreciará, la función hash exacta, o algoritmo hash, que se usará también debe probarse y evaluarse en dependencia de las necesidades del usuario y los requisitos del sistema para las transacciones basadas en tarjetas previstas.

Ahora se hace referencia a la Figura 5, que ilustra un ejemplo de aplicación 330 de una función hash perfecta mínima a una combinación del CSC y la semilla de datos de acuerdo con algunas realizaciones. En este ejemplo, el CSC es un número de 4 dígitos, por ejemplo, como se usa por AMERICAN EXPRESS.

Además, en este ejemplo, la semilla de datos comprende una combinación de i) un identificador de teléfono móvil, ejemplificado aquí por un IMSI; y ii) una marca de tiempo. La FIGURA 5A ilustra lo siguiente:

- IMSI: 310 1509 8765 4321
- Sello de tiempo: 2419 0756
- CSC: 6482.

Como se apreciará, la marca de tiempo mencionada anteriormente puede expresarse de varias maneras. Por ejemplo, es posible expresar el tiempo mediante el uso de una marca de tiempo como se indica públicamente aquí: *http://www.timestampconvert.com.* Es decir, la marca de tiempo, puede usar un sistema para describir puntos en el tiempo, definido como el número de segundos transcurridos desde la medianoche de la Hora Universal Coordinada (UTC) del 1 de enero de 1970, sin contar los segundos intercalados. Esta forma de expresar el tiempo se usa comúnmente no solo en sistemas operativos similares a Unix, sino también en muchos otros sistemas informáticos.

Como puede verse en la Figura 5B, puede determinarse, o generarse, una semilla de datos a partir del IMSI y la marca de tiempo. En este ejemplo, la semilla de datos se genera como una suma total del IMSI y la marca de tiempo:

```
   0310
   1509
   8765
   4321
   2419
+  0756
  18080
```

Como se apreciará, la semilla de datos corresponde a los últimos cuatro dígitos de la suma total del IMSI y la marca de tiempo.

Como se apreciará, una función hash perfecta mínima también se aplica 330 al CSC, así como también a la semilla de datos para generar un CSC temporal. En algunas realizaciones, como se ejemplifica en la FIGURA 5C, es posible determinar, o generar, una suma de la semilla de datos generada anteriormente y el CSC. A veces, esta suma de la semilla de datos generada anteriormente y el CSC puede denominarse conjunto de claves intermedio.

En este ejemplo, puede producirse una suma total de la semilla de datos generada anteriormente y el CSC:

8080
+ 6482
14562

Los últimos cuatro dígitos de la suma total de la semilla de datos generada anteriormente y el CSC forman el conjunto de claves intermedio 4562. Como puede verse en la FIGURA 5C, la aplicación 630 de una función hash perfecta mínima al conjunto de claves intermedias 4562 en este ejemplo puede producir, o generar, un CSC temporal 6719. El CSC temporal a veces se denota como temp-CSC.

Nuevamente, vale la pena mencionar que la función hash exacta, o algoritmo hash, que se usará en la acción 330 en una cierta implementación puede determinarse o elegirse arbitrariamente, o aleatoriamente. Más específicamente, la función hash exacta, o algoritmo hash, que se usará en una determinada implementación puede determinarse o elegirse arbitrariamente siempre que cumpla con los requisitos de una función hash perfecta mínima que preferentemente no conserva el orden. Como se apreciará, la función hash exacta, o algoritmo hash, a utilizar también debe probarse y evaluarse en dependencia de las necesidades del usuario y los requisitos del sistema para las transacciones basadas en tarjetas previstas.

Por ejemplo, la siguiente página web *http://cmph.sourceforge.net/* presenta varias funciones hash disponibles públicamente que pueden usarse en dependencia de, por ejemplo, las necesidades del usuario y los requisitos del sistema (por ejemplo, la capacidad de la unidad central de procesamiento (CPU) y los requisitos de memoria).

En algunas implementaciones, aplicaciones o escenarios, ha resultado que la función CHD (abreviatura de Comprimir, Hash y Desplazar) puede ser ventajosa. La función CHD se describe en detalle en el artículo “Hash, displace, and compress” de Djamal Belazzougui, Fabiano C. Botelho y Martin Dietzfelbinger, que puede descargarse aquí: http://cmph.sourceforge.net/papers/esa09.pdf.

Alternativamente, resultó que las funciones BDZ o BMZ descritas en la página web *http://cmph.sourceforge.net/* puede ser adecuado para aplicar.

Con referencia continua a la Figura 3, una transacción basada en tarjeta también puede iniciarse opcionalmente mediante el uso del CSC temporal generado. Por ejemplo, la transacción basada en tarjeta puede iniciarse entre el terminal móvil que realiza las etapas, o acciones, 310-330 y un sistema de proveedor de servicios.

En realizaciones alternativas, las etapas del procedimiento (o acciones) 310-330 y la etapa del procedimiento (o acción) 340 se realizan, o se ejecutan de cualquier otra manera, mediante diferentes dispositivos de manera distribuida. Por ejemplo, el CSC temporal puede generarse inicialmente mediante un primer dispositivo y la transacción basada en tarjeta puede iniciarse subsecuentemente mediante un segundo dispositivo (es decir, diferente). En una realización de ejemplo, el primer dispositivo puede ser, por ejemplo, un dispositivo de generación de CSC temporal que se diseña específicamente para generar el CSC temporal. Una vez conocido, el CSC temporal generado por el primer dispositivo puede ser utilizado por un segundo dispositivo cuando se inicia una transacción basada en tarjeta.

Ahora se hace referencia a la Figura 6, que es un diagrama de flujo que ilustra esquemáticamente una realización ilustrativa de un procedimiento para recuperar un CSC original de un CSC temporal (tal como un CVV o CVV2) usado en una transacción basada en tarjeta. En la realización ilustrativa detallada en la FIGURA 6, el procedimiento se realiza por medio de un sistema de servidor. Como se apreciará, el sistema de servidor puede comprender un solo servidor informático o varios servidores informáticos. El sistema de servidor puede ser, por ejemplo, un sistema de proveedor de servicios (es decir, un sistema de servidor alojado por un proveedor de servicios) que incluye uno o varios servidores informáticos. En realizaciones alternativas, el sistema de servidor puede, por ejemplo, en lugar de ser un sistema emisor de crédito (es decir, un sistema de servidor alojado por un emisor de crédito) que incluye uno o varios servidores informáticos.

Se obtiene un CSC temporal 610. Como se describió anteriormente con respecto a la Figura 3, el CSC temporal se ha generado mediante la aplicación previa de una función hash perfecta mínima a un CSC, así como también a una primera semilla de datos, por ejemplo, de acuerdo con las enseñanzas en SE1651165-1 (o, PCT/SE2017/050858). Por ejemplo, el CSC temporal puede obtenerse 610 al recibir el CSC temporal desde un dispositivo, por ejemplo, un terminal móvil que ha iniciado una transacción basada en tarjeta con el sistema de proveedor de servicios.

Después, se obtiene una segunda semilla de datos 620. La segunda semilla de datos es la misma semilla de datos que la primera semilla de datos. Es decir, la segunda semilla de datos es típicamente la misma semilla de datos que se usa en la generación del CSC temporal.

Esta acción 620 incluiría ventajosamente tener al menos parte de la segunda semilla de datos almacenada (por ejemplo, en un almacenamiento tal como una memoria) por adelantado en el sistema de servidor 720. Por ejemplo, esto podría incluir ventajosamente tener al menos parte de la segunda semilla de datos almacenada por adelantado en el sistema servidor 720, por razones de seguridad, preferentemente al menos una parte patentada desde el lado

generador que se conoce por adelantado por el sistema de proveedor de servicios 720, por ejemplo, un identificador de terminal móvil (como IMSI), un número de cuenta bancaria y/o un identificador de instalación adquirido durante una posible configuración de la aplicación en el lado que genera el CSC temporal (es decir, el terminal móvil en este ejemplo). Otras partes estáticas (no cambiantes) de la segunda semilla de datos pueden almacenarse con anticipación en el sistema servidor 720 o comunicarse, por ejemplo, durante la iniciación de una transacción basada en tarjeta. Si la segunda semilla de datos comprende una marca de tiempo u otros pares que cambian, por ejemplo, un número de secuencia, esto podría calcularse por medio del sistema de servidor 720 o comunicarse, por ejemplo, durante la iniciación de una transacción basada en tarjeta. Por ejemplo, como se anticipó en la Figura 5B, un IMSI puede almacenarse por el sistema de servidor 720, mientras que la marca de tiempo puede enviarse desde el lado de generación (es decir, el terminal móvil 710 en este ejemplo) como parte de o en conexión con una transacción basada en tarjeta; estas dos partes se combinarían para producir o formar de cualquier otra manera la segunda semilla de datos, como se aprecia en la Figura 5B y se describe además más abajo.

Además, se aplica una misma función hash perfecta mínima 630 a la segunda semilla de datos obtenida o formada de otro modo y cada CSC de una lista almacenada de CSC disponibles hasta que se encuentra una coincidencia entre el CSC temporal obtenido y un CSC de una lista almacenada de CSC disponibles. Es decir, el sistema de servidor aplica la misma función hash perfecta mínima que se usó anteriormente para generar el CSC temporal, generalmente de la misma manera o de una manera generalmente similar. Si la generación del CSC temporal implicaba ejecutar la acción 330 (ver Figura 3) más de una vez, el mismo número de repeticiones también debería tener lugar ventajosamente durante el procedimiento de recuperación en el lado del sistema servidor descrito en relación con la Figura 6.

La función hash perfecta mínima que se usará por el sistema de servidor 720 (es decir, la misma función perfecta mínima) puede determinarse, por ejemplo, almacenarse, por adelantado en el sistema de servidor 720. En otras palabras, la función hash perfecta mínima que se usará puede conocerse de antemano por el sistema de servidor 720. Alternativamente, la información relacionada con la función hash perfecta mínima a usar puede comunicarse, por ejemplo, durante el inicio de una transacción basada en tarjeta. Con este fin, si la generación del CSC temporal implicaba ejecutar la acción 330 (ver Figura 3) más de una vez como se mencionó anteriormente, también debe apreciarse que el número de veces que la función hash perfecta mínima se ejecutará por el sistema de servidor 720 (es decir, generalmente el mismo número que durante la generación del CSC temporal) puede determinarse, por ejemplo, almacenarse, por adelantado en el sistema de servidor 720. En otras palabras, el número de veces que la función hash perfecta mínima se ejecutará puede conocerse de antemano por el sistema de servidor 720. Alternativamente, la información relacionada con el número de veces que se ejecutará la función hash perfecta mínima puede comunicarse, por ejemplo, durante el inicio de una transacción basada en tarjeta.

En algunas realizaciones, partes de la información anterior, por ejemplo, el algoritmo hash a utilizar, el número de veces que ejecutarlo, así como también ciertas partes de la semilla de datos, como un número de secuencia, pueden originarse del sistema de servidor 720 y por lo tanto se comunicarán al lado generador de CSC 330 (es decir, el terminal móvil 710 en este ejemplo), por ejemplo, durante el inicio de una transacción basada en tarjeta.

Se ha hecho referencia a la FIGURA 5 anteriormente en la presente descripción, que ilustra un ejemplo de aplicación 330 de una función hash perfecta mínima a una combinación de un valor de CSC y la semilla de datos de acuerdo con algunas realizaciones. En este ejemplo, el CSC es un número de 4 dígitos, por ejemplo, como se usa por AMERICAN EXPRESS. Ahora se hace referencia a la Figura 5 nuevamente.

La segunda semilla de datos puede comprender una combinación de i) un identificador de terminal móvil tal como un identificador de teléfono móvil, ejemplificado aquí por un IMSI; y ii) una marca de tiempo. La Figura 5A, por ejemplo, ilustra lo siguiente:

- IMSI: 310 1509 8765 4321
- Marca de tiempo: 2419 0756
- Valor de CSC: 6482.

Como se apreciará y como se describió anteriormente, la marca de tiempo mencionada anteriormente puede expresarse de varias maneras. Por ejemplo, es posible expresar el tiempo mediante el uso de una marca de tiempo como se encuentra disponible públicamente aquí: *http://www.timestampconvert.com.* Es decir, la marca de tiempo puede usar un sistema para describir puntos en el tiempo, definido como el número de segundos transcurridos desde la medianoche de la Hora Universal Coordinada (UTC) del 1 de enero de 1970, sin contar los segundos intercalares. Esta forma de expresar el tiempo se usa comúnmente no solo en sistemas operativos similares a Unix, sino también en muchos otros sistemas informáticos.

Como puede verse en la Figura 5B, puede determinarse, o generarse, una segunda semilla de datos a partir del IMSI y la marca de tiempo. En este ejemplo, la segunda semilla de datos se genera como una suma total del IMSI y la marca de tiempo:

```
  0310
  1509
  8765
  4321
  2419
+ 0756
 18080
```

Como se apreciará, la segunda semilla de datos corresponde a los últimos cuatro dígitos de la suma total del IMSI y la marca de tiempo.

Como se apreciará además, una misma función hash perfecta mínima se aplica entonces 630 (ver Figura 6) a la segunda semilla de datos junto con cada CSC de una lista de CSC disponibles para generar un resultado para comparar con el CSC temporal que se ha obtenido 610; cuando estos dos (es decir, el resultado y el CSC temporal) son iguales, el CSC original que se usó para producir el CSC temporal será igual al CSC de la lista de CSC disponibles que se usó justo para producir el resultado que correspondió al CSC temporal. Por lo tanto, se recupera el CSC original.

En algunas realizaciones, como se ejemplifica en la Figura 5C, es posible determinar, o generar, una suma de la semilla de datos generada anteriormente y el CSC. A veces, esta suma de la semilla de datos generada anteriormente y el CSC puede denominarse conjunto de claves intermedio.

En este ejemplo, puede producirse una suma total de la semilla de datos generada anteriormente y el CSC:

```
  8080
+ 6482
 14562
```

Los últimos cuatro dígitos de la suma total de la semilla de datos generada anteriormente y el CSC forman el conjunto de claves intermedias 4562. Como puede verse en la FIGURA 5C, la aplicación 630 de una función hash perfecta mínima al conjunto de claves intermedias 4562 en este ejemplo puede producir, o generar, un resultado 6719, que luego se compararía con el CSC temporal, a veces denominado temp-CSC, producido en 330.

Por lo tanto, como el resultado 6719 aquí es el mismo que el CSC temporal, el CSC original también sería el mismo, es decir, 6482.

La Figura 7A ilustra esquemáticamente un entorno posible, en el que pueden aplicarse las realizaciones descritas hasta ahora. En este escenario de ejemplo, el entorno 700 comprende un terminal móvil 710, tal como un teléfono móvil, como un ejemplo de un dispositivo que es capaz de generar un CSC temporal, y un sistema de servidor ejemplificado aquí como un sistema de proveedor de servicios 720, que es recuperar un CSC original de dicho CSC temporal. La Figura 7B es un diagrama de señalización que ilustra varias acciones que pueden realizarse, así como también la señalización entre el terminal móvil 710 y el sistema de proveedor de servicios 720 mostrado en la FIGURA 7A.

El terminal móvil 710 puede conectarse a través de una red u otra conexión 730, en un ejemplo a través de Internet. El terminal móvil 710 puede conectarse a través de una conexión por cable o una conexión inalámbrica o cualquier combinación de procedimientos de conexión conocidos, por ejemplo, a través de redes o conexiones dedicadas. Se debe señalar que cualquier terminal puede conectarse a la red 730 y el número y tipo de terminales 100 en la Figura 7A no deben interpretarse como limitantes.

El sistema 700 ejemplificado aquí comprende al menos un servidor 720. En la Figura 7A solo se muestra un servidor 720, pero debe señalarse que puede implementarse cualquier número de servidores 720 en una red informática. Generalmente, un servidor es una computadora física (un sistema de hardware) dedicada a ejecutar uno o más Servicios (como un anfitrión), para satisfacer las necesidades de los usuarios de otras computadoras o terminales 710 en la red 730. En una realización, el servidor 720 es un servidor de proveedor de servicios. Generalmente, un servidor de proveedor de servicios 720 puede referirse a hardware (un ordenador) o software (una aplicación informática) que ayuda a suministrar contenido al que se puede acceder a través de una red de comunicación mutua, tal como la Internet 730.

La Figura 7B muestra acciones ilustrativas y mensajes ilustrativos que pueden señalarse, de acuerdo con la Figura 7A, entre un terminal móvil 710 y un sistema de proveedor de servicios 720 para realizar una transacción basada en tarjeta. En este ejemplo, el terminal móvil, aquí ejemplificado como un teléfono móvil, obtiene 310 un CSC tal como un CVV o un CVV2 de una tarjeta, tal como una tarjeta de crédito o una tarjeta de débito. El terminal móvil obtiene además 320 una semilla de datos, por ejemplo, que incluye un identificador de terminal móvil y una marca de tiempo. Aún más, el terminal móvil aplica 330 una función hash perfecta mínima al CSC, así como también la semilla de datos

para generar un CSC temporal (por ejemplo, de acuerdo con las enseñanzas en el documento SE1651165-1 (o, en el documento PCT/SE2017/050858). En este ejemplo, el terminal móvil también inicia 340, o activa de cualquier otra manera, una transacción basada en tarjeta con y el sistema de proveedor de servicios 720 que utiliza, o usa de cualquier otra manera, el CSC temporal generado. El sistema de proveedor de servicios 720 obtiene 610 dicho CSC temporal. Por ejemplo, el sistema de proveedor de servicios 720 puede recibir el CSC temporal desde el terminal móvil. En respuesta a obtener 610 el CSC temporal, el servidor del proveedor de servicios 720 también puede obtener 620 una misma semilla de datos que se usó durante la generación del CSC temporal y aplicar además 630 la misma función hash perfecta mínima a la semilla de datos obtenida junto con, o junto con, cada uno de varios CSC de una lista almacenada de CSC disponibles hasta que se encuentre una coincidencia entre el CSC temporal obtenido y un CSC de la lista almacenada de CSC disponibles. Por lo tanto, el Servicio de proveedor de servicios es capaz de recuperar el CSC original del CSC temporal obtenido. Una transacción iniciada basada en tarjeta entre el terminal móvil 710 y un sistema de proveedor de servicios 720 puede continuarse después 640.

Ahora se hace referencia a la Figura 8 que ilustra esquemáticamente una implementación de ejemplo de una realización de un sistema de servidor ejemplificado en la presente descripción por un sistema de proveedor de servicios 720 (ver, por ejemplo, también las Figuras 7A-7B). El sistema de proveedor de servicios 720 puede, por ejemplo, ser un servidor informático alojado por un proveedor de servicios como se describió anteriormente. El sistema de proveedor de servicios 720 puede configurarse para realizar, o ejecutar de cualquier otra manera, el procedimiento de acuerdo con una cualquiera de las realizaciones descritas en la presente memoria, por ejemplo, la Figura 6 o la Figura 7.

Con este fin, el sistema de proveedor de servicios 720 puede comprender opcionalmente un UI 721. Además, el sistema de proveedor de servicios 720 comprende recursos de hardware. Por ejemplo, el sistema de proveedor de servicios 720 puede comprender uno o más procesadores 722 y una o más memorias 723. Además, puede proporcionarse una interfaz de comunicaciones 724, o un circuito de comunicaciones, para permitir que el sistema de proveedor de servicios 720 se comunique con otros dispositivos tales como un terminal móvil 710.

Con este fin, la interfaz de comunicaciones 724 puede comprender un transmisor (Tx) y un receptor (Rx). Alternativamente, la interfaz de comunicaciones 724 puede comprender un transceptor (Tx/Rx) que combina capacidades de transmisión y recepción. La interfaz de comunicaciones 724 puede incluir una interfaz de radiofrecuencia (RF) que permite que el sistema de proveedor de servicios 720 se comunique con otros servidores informáticos y/o dispositivos tales como el terminal móvil 710 a través de una banda de radiofrecuencia mediante el uso de diferentes tecnologías de radiofrecuencia tales como 5G NR (5G Nueva Radio), LTE (Evolución a Largo Plazo), WCDMA (Acceso Múltiple por División de Código de Banda Ancha), cualquier otra red celular estandarizada por el Proyecto de Asociación de 3ra Generación (3GPP), o cualquier otra tecnología inalámbrica tal como Wi-Fi, Bluetooth®, etcétera.

Como se apreciará, el sistema de proveedor de servicios 720 puede comprender por lo tanto una interfaz de comunicaciones 724, uno o más procesadores 722 y una memoria 723 que almacena instrucciones, ejecutables por el uno o más procesadores, de manera que el servidor de proveedor de servicios 720 es operativo para obtener un CSC temporal, en el que el CSC temporal se ha generado aplicando previamente una función hash perfecta mínima al CSC así como también una semilla de datos; obtener una segunda semilla de datos, la segunda semilla de datos es una misma semilla de datos como la primera semilla de datos; y aplicar una misma función hash perfecta mínima a la segunda semilla de datos obtenida junto con cada uno de varios CSC de una lista almacenada de CSC disponibles hasta que se encuentre una coincidencia entre el CSC temporal obtenido y un CSC de la lista almacenada de CSC disponibles, para recuperar de esta manera el CSC original.

Volviendo ahora a la Figura 9, se describirá brevemente otra realización. La Figura 9 muestra un ejemplo de un medio legible por ordenador, en este ejemplo en forma de un disco de datos 900.

En una realización, el disco de datos 900 es un disco de almacenamiento de datos magnético. El disco de datos 900 se configura para transportar instrucciones 910 que pueden cargarse en una memoria de un aparato, por ejemplo, un sistema de proveedor de servicios 720 que incluye uno o varios servidores informáticos. Tras la ejecución de dichas instrucciones por un procesador del aparato, el aparato se hace ejecutar un procedimiento o procedimiento de acuerdo con una cualquiera de las realizaciones descritas en la presente memoria, por ejemplo, junto con las Figuras 6 y 7. El disco de datos 900 se dispone para conectarse a o dentro de y leerse mediante un dispositivo de lectura (no mostrado), para cargar las instrucciones en el procesador. Un ejemplo de un dispositivo de lectura en combinación con uno (o varios) disco(s) de datos 900 es un disco duro.

Cabe señalar que el medio legible por ordenador también puede ser otros medios tales como discos compactos, memorias flash u otras tecnologías de memoria comúnmente usadas. En tal realización, el disco de datos 900 es un tipo de medio legible por ordenador tangible. Las instrucciones pueden descargarse alternativamente en un dispositivo de lectura de datos de ordenador, tal como un aparato capaz de leer datos codificados por ordenador en un medio legible por ordenador, que comprende las instrucciones en una señal legible por ordenador (no mostrada) que se transmite a través de una interfaz inalámbrica (o cableada) (por ejemplo, a través de Internet) al dispositivo de lectura de datos de ordenador para cargar las instrucciones en un procesador del aparato. En tal realización, la señal legible

por ordenador es un tipo de medio legible por ordenador no tangible.

En la descripción detallada anterior, con fines de explicación y no de limitación, se exponen detalles específicos para proporcionar una comprensión completa de varias realizaciones descritas en esta descripción. En algunos casos, se han omitido descripciones detalladas de dispositivos, componentes, circuitos y procedimientos bien conocidos para no oscurecer la descripción de las realizaciones divulgadas en la presente memoria con detalles innecesarios.

Las declaraciones AH en la presente memoria que relatan principios, aspectos y realizaciones descritos en la presente memoria, así como también ejemplos específicos de estos, pretenden abarcar tanto los equivalentes estructurales como funcionales de estos. Adicionalmente, se pretende que tales equivalentes incluyan tanto los equivalentes conocidos actualmente como los equivalentes desarrollados en el futuro, es decir, cualquier elemento desarrollado que realice la misma función, independientemente de la estructura. Por lo tanto, por ejemplo, se apreciará que los diagramas de bloques en la presente memoria pueden representar vistas conceptuales de circuitos ilustrativos u otras unidades funcionales que incorporan los principios de las realizaciones descritas. De manera similar, se apreciará que cualquier diagrama de flujo y similares representan varios procesos que pueden representarse sustancialmente en un medio legible por ordenador y así ejecutarse por un ordenador o procesador, ya sea que dicho ordenador o procesador se muestre explícitamente o no.

Las funciones de los diversos elementos que incluyen bloques funcionales, pueden proporcionarse mediante el uso de hardware tal como hardware de circuito y/o hardware capaz de ejecutar software en forma de instrucciones codificadas almacenadas en el medio legible por ordenador mencionado anteriormente. Por lo tanto, tales funciones y bloques funcionales ilustrados deben entenderse como implementados por hardware y/o implementados por ordenador, y por lo tanto implementados por máquina. En términos de implementación de hardware, los bloques funcionales pueden incluir o abarcar, sin limitación, hardware de procesador de señales digitales (DSP), procesador de conjunto de instrucciones reducido, hardware (por ejemplo, digital o analógico) circuitos que incluyen, pero sin limitarse a, circuitos integrados de aplicación específica [ASIC], y/o matrices de puertas programables en campo (FPGA), y (cuando sea apropiado) máquinas de estado capaces de realizar tales funciones.

En términos de implementación informática, generalmente se entiende que un ordenador comprende uno o más procesadores o uno o más controladores. Cuando se proporciona por un ordenador o procesador o controlador, las funciones pueden proporcionarse por un único ordenador o procesador o controlador dedicado, por un único ordenador o procesador o controlador compartido, o por una pluralidad de ordenadores o procesadores o controladores individuales, algunos de los cuales pueden compartirse o distribuirse.

Además, el uso del término “procesador” o “controlador” también puede interpretarse como que se refiere a otro hardware capaz de realizar tales funciones y/o ejecutar software, tal como el hardware de ejemplo mencionado anteriormente.

Las modificaciones y otras variantes de las realizaciones descritas se le ocurrirán a un experto en la técnica que tenga el beneficio de las enseñanzas presentadas en la descripción y los dibujos asociados anteriores.

Por ejemplo, aunque las realizaciones descritas en la presente memoria se han ejemplificado para aplicar, o hacer uso de, funciones hash perfectas mínimas, los expertos en la técnica apreciarán que no es necesario aplicar, o hacer uso de, funciones hash perfectas mínimas. Se prevé que, en algunas aplicaciones o escenarios, se puedan aplicar alternativamente otras funciones hash.

REIVINDICACIONES

1. Un procedimiento para recuperar un Código de Seguridad de Tarjeta, CSC, de un CSC temporal usado en una transacción basada en tarjeta, en el que el procedimiento se realiza por un sistema de servidor que tiene uno o varios servidores informáticos y el procedimiento que comprende:

obtener (610) un CSC temporal, en el que el CSC temporal se ha generado aplicando previamente una función hash perfecta mínima a un CSC original, así como también una primera semilla de datos, la primera semilla de datos incluye un identificador de terminal móvil de un terminal móvil y una marca de tiempo generada por dicho terminal móvil; y

obtener (620) una segunda semilla de datos, la segunda semilla de datos es una misma semilla de datos que la primera semilla de datos e incluye el mismo identificador de terminal móvil y la misma marca de tiempo que la primera semilla de datos, en el que al menos dicho identificador de terminal móvil se ha almacenado previamente en el sistema servidor de manera que obtener (620) la segunda semilla de datos comprende obtener el identificador de terminal móvil localmente del sistema servidor;

aplicar (630) una misma función hash perfecta mínima a la segunda semilla de datos obtenida junto con cada uno de varios CSC de una lista almacenada de CSC disponibles hasta que se encuentre una coincidencia entre el CSC temporal obtenido y un CSC de la lista almacenada de CSC disponibles; y en respuesta a que se haya encontrado una coincidencia:

continuar (640) una transacción basada en tarjeta iniciada

2. El procedimiento de acuerdo con la reivindicación 1, en el que la marca de tiempo se ha comunicado durante el inicio de la transacción basada en tarjeta de manera que obtener (620) la segunda semilla de datos implica recibir la marca de tiempo desde el terminal móvil que genera la marca de tiempo.

3. El procedimiento de acuerdo con la reivindicación 1 o 2, en el que el procedimiento se realiza por uno cualquiera o una combinación de i) un sistema de proveedor de servicios que tiene uno o varios servidores informáticos y ii) un sistema emisor de crédito que tiene uno o varios servidores informáticos.

4. Un programa informático que comprende instrucciones (1110) que, cuando se ejecutan en un procesador, hacen que el procesador lleve a cabo el procedimiento de acuerdo con una cualquiera de las reivindicaciones 1 - 3.

5. Un portador que comprende el programa informático de acuerdo con la reivindicación 4, en el que el portador es una señal electrónica, una señal óptica, una señal de radio, o un medio de almacenamiento legible por ordenador (1100).

6. Un sistema de servidor (720) que tiene uno o varios servidores informáticos, que comprende:

una interfaz de comunicaciones (724);

uno o más procesadores (722); y

una memoria (723) que almacena instrucciones, ejecutables por uno o más procesadores, de manera que el servidor del proveedor de servicios es operativo para realizar el procedimiento de acuerdo con una cualquiera de las reivindicaciones 1 - 5.

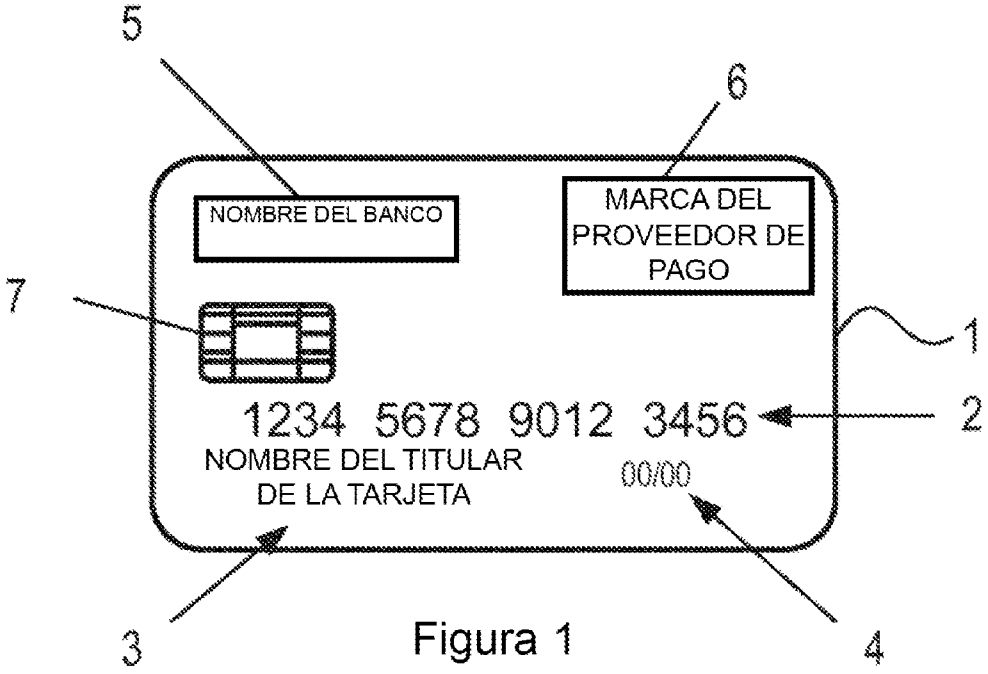

Figura 1

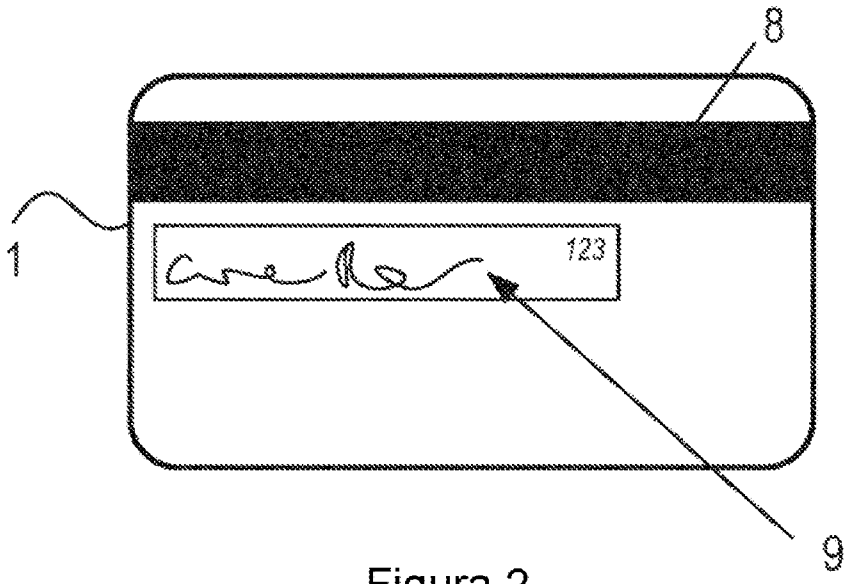

Figura 2

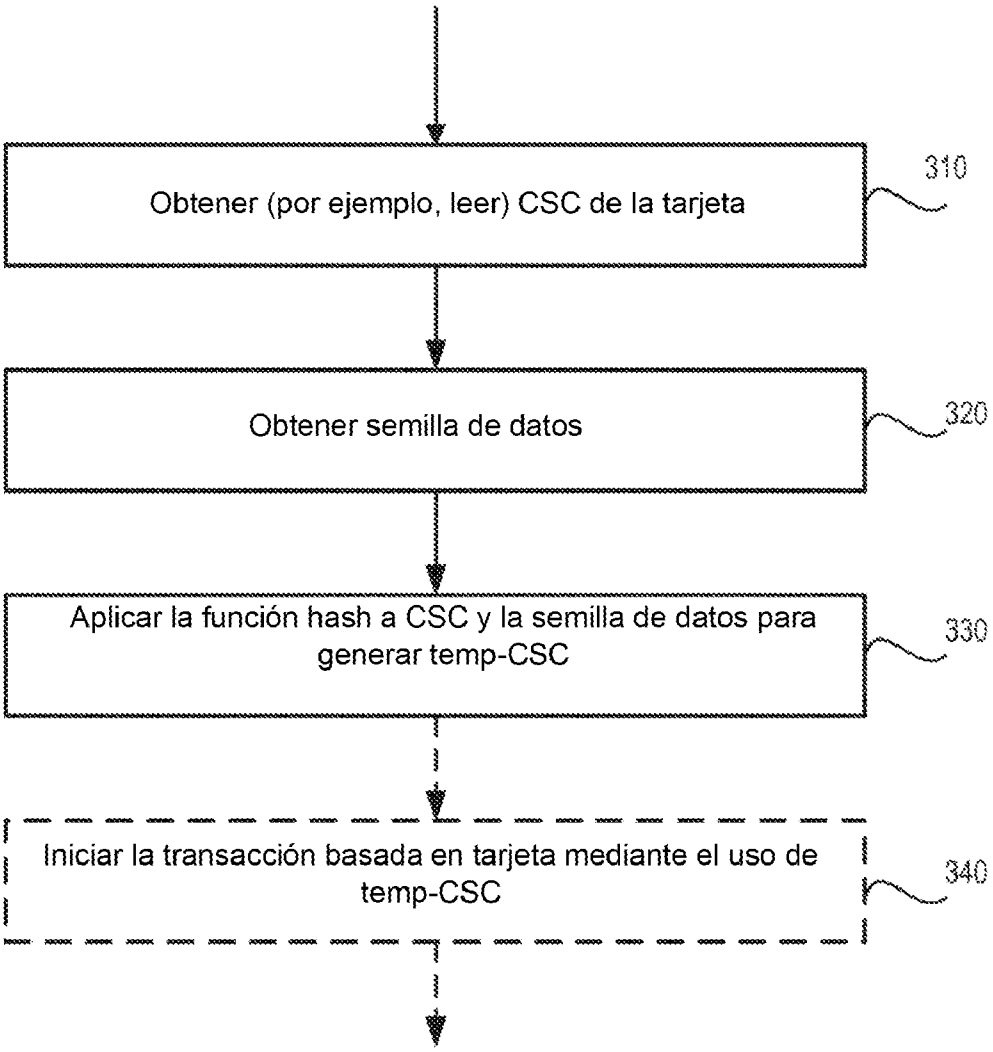
Obtener (por ejemplo, leer) CSC de la tarjeta
310
Obtener semilla de datos
320
Aplicar la función hash a CSC y la semilla de datos para generar temp-CSC
330
Iniciar la transacción basada en tarjeta mediante el uso de temp-CSC
340

Figura 3

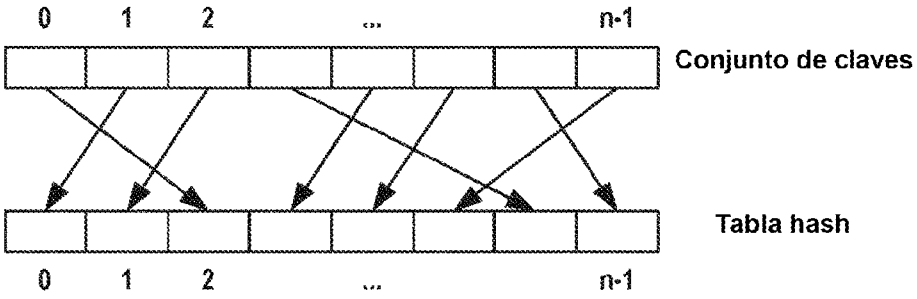

Figura 4A

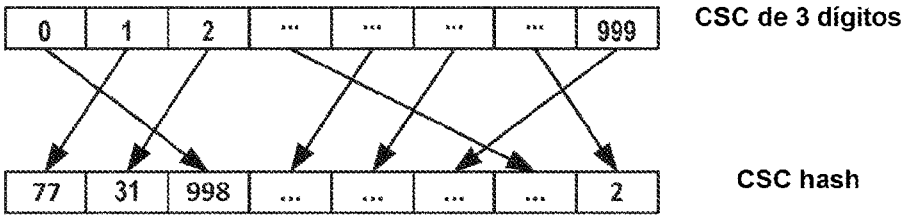

Figura 4B

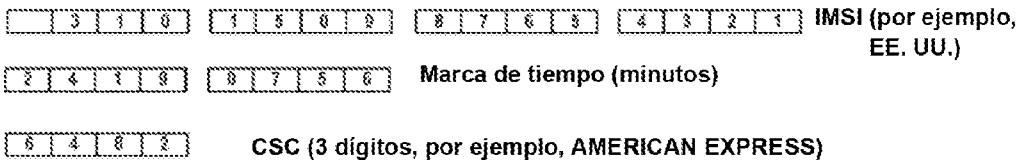

Figura 5A

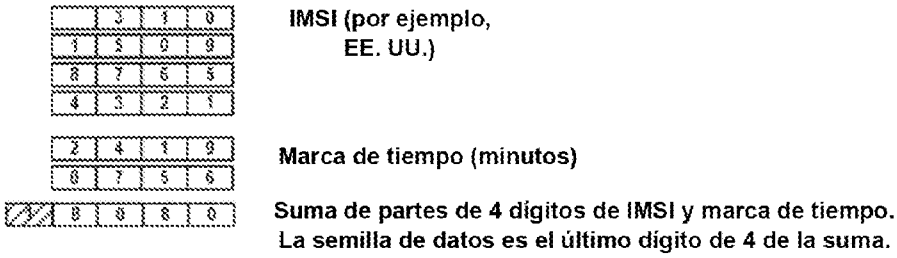

Figura 5B

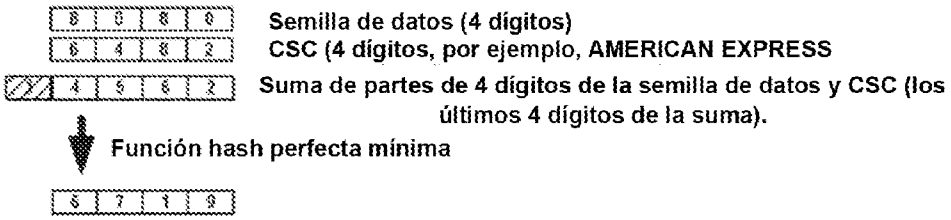

Figura 5C

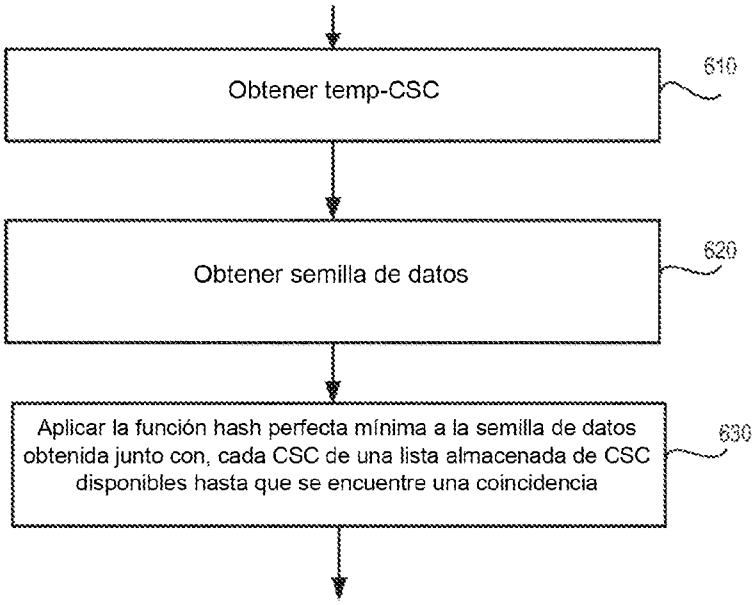

Figura 6

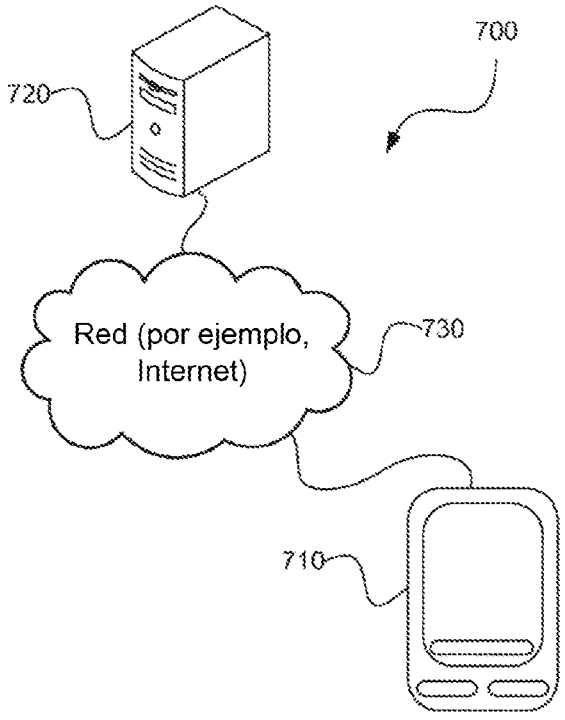

Figura 7A

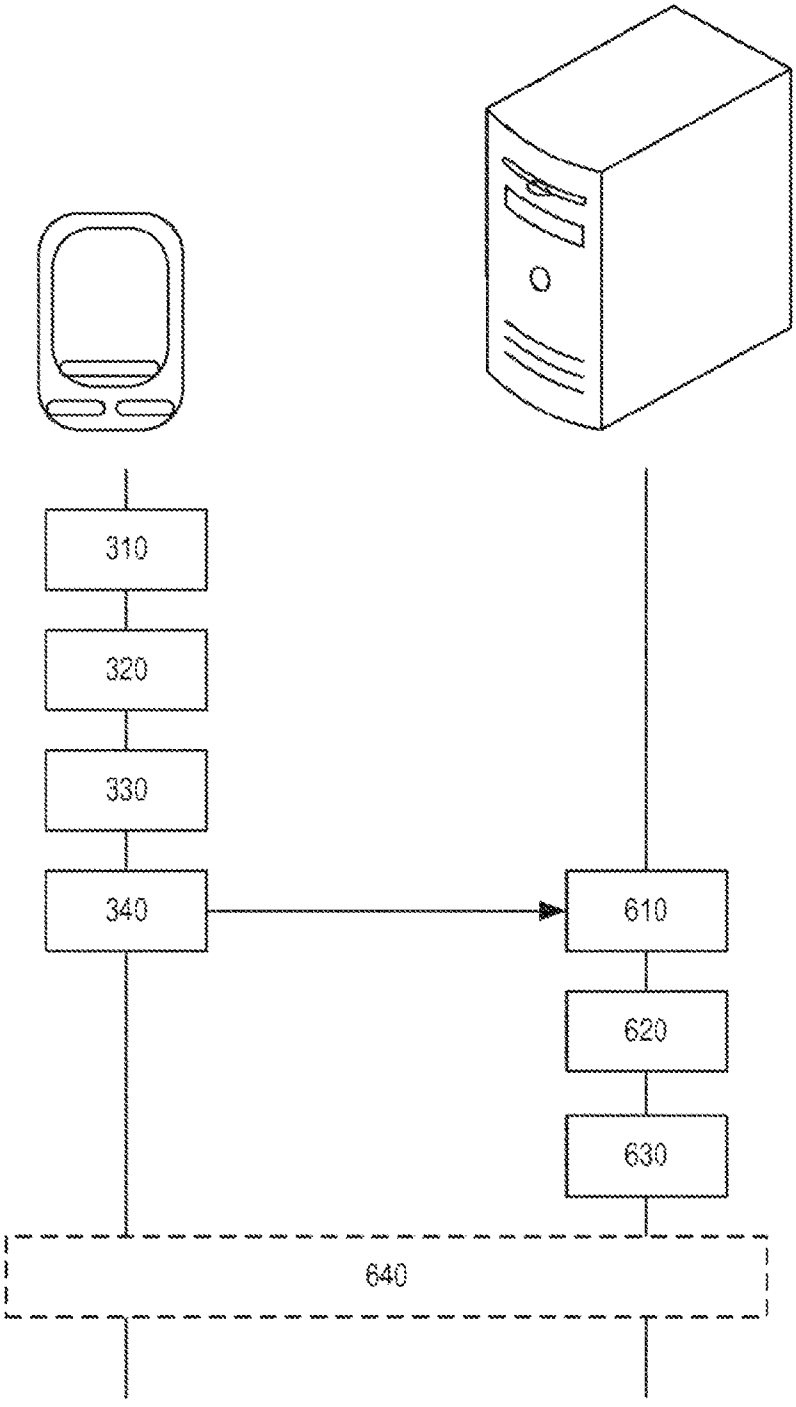

Figura 7B

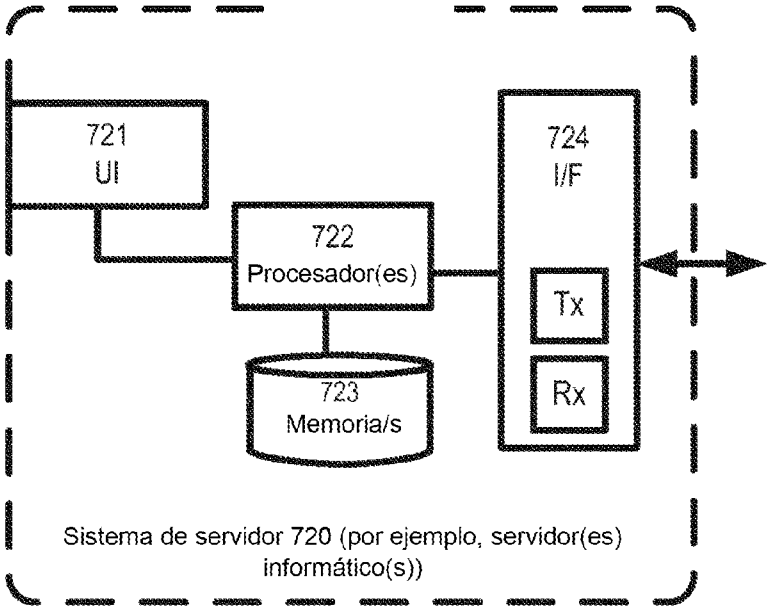

Figura 8

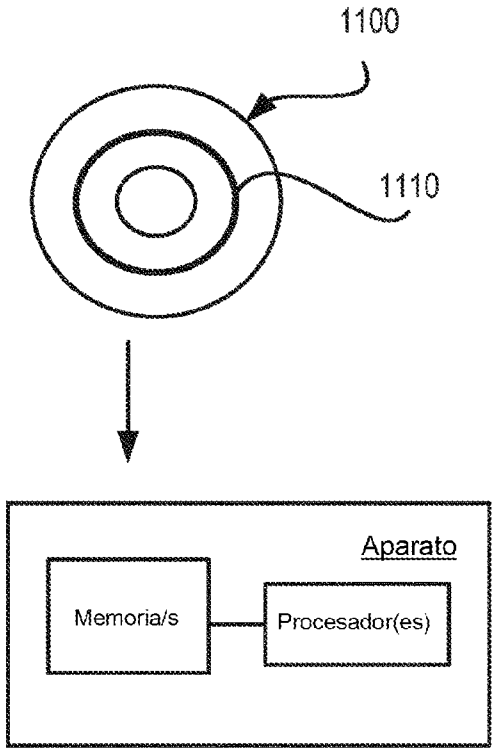

Figura 9