(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 758 706**

(51) Int. CI.:

H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **28.02.2005 PCT/US2005/006535**

(87) Fecha y número de publicación internacional: **15.09.2005 WO05084293**

(96) Fecha de presentación y número de la solicitud europea: **28.02.2005 E 05724139 (0)**

(97) Fecha y número de publicación de la concesión europea: **13.11.2019 EP 1730866**

(54) Título: **Métodos y sistemas para la transmisión segura de información de identificación a través de redes públicas**

(30) Prioridad:

27.02.2004 US 548824 P
25.02.2005 US 67306

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
06.05.2020

(73) Titular/es:

METAVANTE CORPORATION (100.0%)
4900 WEST BROWN DEER ROAD BROWN DEER
WISCONSIN 53223, US

(72) Inventor/es:

GRACE, DAVID y
TURGEON, PAUL

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Métodos y sistemas para la transmisión segura de información de identificación a través de redes públicas

Esta solucitud se refiere en general a la seguridad de la información. Más específicamente, esta solucitud se refiere a métodos y sistemas para la transmisión segura de información de identificación a través de redes públicas.

El documento US-A-2002/152180 divulga un sistema y un método para realizar transacciones financieras remotas seguras en tiempo real sobre una infraestructura de comunicaciones públicas que permite compras en línea con PIN en tiempo real.

El documento US4933971B divulga un método de encriptación de datos transmitidos usando una clave única y que permite la generación periódica de claves de encriptación dinámica únicas para cada uno de una pluralidad de terminales que se requieren para comunicarse con un ordenador servidor de manera segura. Además, el documento US6182220B divulga un sistema y un método para construir e intercambiar contraseñas encriptadas dentro de una relación cliente/servidor.

Existen numerosas instancias en las que los integrantes pueden desear acceder a un sistema servidor a través de una red pública. En muchos casos, el sistema servidor está configurado con protocolos de seguridad para limitar el acceso a los intetgrantes legítimos, y dichos protocolos de seguridad generalmente se basan en la recepción y verificación de la información de identificación. Por ejemplo, la información de identificación podría comprender una combinación de un identificador de usuario y una contraseña secreta, y el acceso al sistema servidor solo se otorgará cuando el usuario presente ambos integrantes de la información de identificación. Si bien la capacidad de los integrantes para acceder a un sistema servidor a través de una red pública presenta numerosas comodidades, también presenta el peligro de que la seguridad de la información de identificación se comprenda como resultado de la intercepción por parte de un fisgón.

En la figura 1 se ilustra una disposición básica que actualmente se usa comúnmente para conectar integrantes a un sistema servidor a través de una red pública. La red 108 pública está configurada para establecer una conexión entre el sistema 112 servidor y el integrante 104 en respuesta a una solicitud del integrante 104. Por lo general, el sistema 112 servidor incluye un protocolo 116 de seguridad que verifica la información de identificación proporcionada por el integrante 104 y transmitida con la red 108 pública. En muchos casos, el protocolo 116 de seguridad está equipado con algoritmos de detección de fraude, un ejemplo simple de los cuales es un algoritmo que marca intentos repetidos para obtener acceso al sistema 112 servidor. Por ejemplo, uno de esos algoritmos de detección de fraude permite a un integrante 104 hacer no más de tres intentos incorrectos para ingresar una contraseña; si se realiza un cuarto intento incorrecto, el algoritmo bloquea a ese integrante 104 hasta que se tome alguna medida correctiva, tal vez iniciada por una llamada telefónica del integrante 104.

Tal un protocolo 116 de seguridad de este modo ayuda a evitar que un integrante hostil intente adivinar la contraseña de un integrante legítimo, pero es menos eficaz cuando la información de identificación puede ser interceptada por un fisgón 120. El peligro de intercepción por parte de fisgones 120, ha aumentado, además a medida que las redes públicas se utilizan más ampliamente. En lugar de recordar múltiples contraseñas diferentes, los integrantes 104 usan con frecuencia la misma contraseña para acceder a múltiples sistemas 112 servidor diferentes. Si un espía intercepta una transmisión de un integrante 104 particular para cualquier sistema 112 servidor, puede obtener información para acceder de nuevo a múltiples sistemas 112 servidor

Una técnica que se ha utilizado para compensar tales posibilidades es proporcionar un sistema intermedio que mantenga un registro de información de identificación para múltiples sistemas 112 servidor en nombre de un integrante, y que requiera solo una contraseña única para ese integrante 104. Cuando el integrante desea acceder a cierto sistema 112 servidor, la transmisión se enruta a través del sistema intermedio, que detecta si la contraseña única es correcta, transmitiendo la contraseña de servidor apropiada solo si es así. Dicha técnica protege el sistema 112 servidor de posibles fraudes al truncar la transmisión cuando se proporciona una contraseña incorrecta.

Una desventaja de tal disposición, sin embargo, es que esta técnica también elude el protocolo 116 de seguridad que puede existir en el sistema 112 servidor. Esto es cierto para todas las disposiciones que utilizan el truncamiento de la transmisión al sistema 112 servidor como parte de prevención de fraude. La elusión del protocolo 116 de seguridad del sistema servidor priva así a ese protocolo de información que puede ser útil para analizar patrones de intentos de violaciones de seguridad. Además, generalmente no es deseable implementar el protocolo 116 de seguridad del sistema servidor en el sistema intermedio. Dicha implementación no solo requeriría la duplicación de la inversión significativa ya realizada por múltiples sistemas 112 servidor, sino que también eliminaría el control del protocolo de seguridad de los sistemas 112 servidor. Esto es particularmente desventajoso ya que los protocolos de seguridad para cada sistema 112 servidor reflejan con frecuencia preocupaciones de seguridad específicas de ese sistema 112 servidor y pueden beneficiarse de una revisión periódica a medida que cambian esas preocupaciones de seguridad particulares.

En consecuencia, existe una necesidad general en la técnica de métodos y sistemas mejorados para la transmisión segura de información de identificación a través de redes públicas.

Breve resumen de la invención

El problema mencionado anteriormente se resuelve mediante las características de las reivindicaciones independientes.

Otras realizaciones son el tema de las reivindicaciones dependientes.

Breve descripción de los dibujos

Una comprensión adicional de la naturaleza y las ventajas de la presente invención puede realizarse por referencia a las porciones restantes de la especificación y los dibujos en donde se usan números de referencia similares en todos los dibujos para referirse a componentes similares. En algunos casos, una subetiqueta se asocia con un número de referencia y sigue un guión para indicar uno de los múltiples componentes similares. Cuando se hace referencia a un número de referencia sin especificación a una subetiqueta existente, se pretende hacer referencia a todos esos componentes múltiples similares.

La figura 1 es una representación en diagrama de bloques de una disposición de la técnica anterior para conectar un integrante a un sistema servidor;

La figura 2A es una representación en diagrama de bloques de una disposición para conectar un integrante a un sistema servidor en una realización de la invención;

La figura 2B es una ilustración esquemática de un flujo de autentificadores estáticos y dinámicos en la implementación de una realización de la invención;

La figura 3 es un diagrama de flujo que ilustra un método para proporcionar autentificadores estáticos y dinámicos a un integrante de acuerdo con una realización de la invención;

La figura 4 es una ilustración esquemática de una estructura de datos para un autentificador estático de un integrante en una realización de la invención;

La figura 5 es un diagrama de flujo que ilustra un método para conectar un integrante con un sistema servidor de acuerdo con una realización de la invención; y

La figura 6 es una ilustración esquemática de un sistema de ordenador en el que se pueden incorporar los métodos de la invención.

Descripción detallada de la invención

Las realizaciones de la invención permiten establecer conexiones entre un integrante y un sistema servidor a través de una red pública al proporcionar una transmisión segura de información de identificación a través de la red pública. Como se usa en el presente documento, una "red pública" está destinada a referirse a una red que permite el acceso a un grupo de integrantes que pertenecen a una comunidad común. Por ejemplo, en algunas realizaciones, la red pública podría corresponder a una red tal como Internet, en la que la comunidad común incluye esencialmente al mundo entero. Sin embargo, en otros casos, la comunidad común podría ser más restrictiva, tal como corresponder a una comunidad académica en una universidad, siendo la red pública la red accesible para los miembros de esa comunidad académica.

Hay una variedad de aplicaciones específicas en las que se pueden usar conexiones a una red pública. Por ejemplo, en el caso específico donde la red pública comprende Internet, el sistema servidor podría ser cualquier sistema al que un integrante desee acceder de forma segura. Por ejemplo, el sistema servidor podría administrar un sitio web financiero donde un integrante podría administrar fondos que están en una o más cuentas, tal como un sitio web de fondos mutuos, un sitio web de un banco y similares. En otra realización, el sistema servidor podría proporcionar acceso restringido al material de publicación a los integrantes que han pagado por el acceso. En una realización adicional, el sistema servidor podría ser un sistema de ordenador de un empleador de un integrante para que el empleado integrante pueda acceder de forma remota a los archivos, programas y similares.

Se enfatiza que estos ejemplos son meramente ilustrativos y que hay muchos más ejemplos de sistemas servidor que están dentro del alcance de la invención y están destinados a permitir el acceso restringido a los integrantes a través de una red pública. Muchos de estos ejemplos adicionales serán evidentes para los expertos en la materia. Además, si bien los ejemplos anteriores se dibujan en conexión con Internet, existen otras aplicaciones con otros ejemplos de redes públicas.

La figura 2A proporciona una visión general esquemática de una arquitectura en la que un integrante 104 puede acceder a un sistema 112 servidor a través de una red 108 pública de acuerdo con una realización de la invención. Las mismas etiquetas de referencia para el integrante 104, la red 108 pública y el sistema 112 servidor se usan como se muestra en la figura 1 para enfatizar que las realizaciones de la invención pueden efectuarse, si se desea, sin cambios en estos componentes. En particular, no se necesita ningún cambio arquitectónico en un sistema servidor heredado existente o en una red pública existente para acomodar estas realizaciones. Ventajosamente, el sistema 112 servidor puede retener el control sobre su propio protocolo de seguridad, como se analiza con mayor detalle a continuación. El acceso del integrante 104 al sistema 112 servidor es proporcionado por un dispositivo 204 de acceso a la red pública que está interconectado con la red 108 pública. Cuando la red 108 pública comprende una red computacional tal como Internet, el dispositivo 204 de acceso a la red pública podría comprender un dispositivo computacional, tal como un ordenador personal, ordenador portátil, asistente digital personal y similares. Cuando la red 108 pública comprende una red de cable, el dispositivo 204 de acceso a la red pública podría comprender una combinación de un televisor y un decodificador. En otros casos, podrían usarse otros dispositivos apropiados como un dispositivo 204 de acceso a la red pública dependiendo de las características específicas de la red 108 pública. Se proporciona una intercepción 212 de la red pública para interceptar la comunicación de información de identificación desde la red 108 pública al sistema 112 servidor y actuar sobre esa información de identificación como se describe a continuación.

En algunos casos, la información de identificación puede pasar a través de un sistema intermediario antes de llegar a la intercepción 212 de la red pública o al sistema 112 servidor, lo que aumenta el riesgo de intercepción de la información de identificación por parte de un fisgón 120. Por ejemplo, en el contexto del comercio electrónico, el sistema 112 servidor podría corresponder a un sistema bancario que administra una cuenta que tiene fondos pertenecientes al integrante y el sistema intermediario podría corresponder a un sistema que administra el sitio web de ventas de un comerciante. Para realizar una compra, el integrante 104 podría acceder a un sitio web administrado por el sistema 216 intermediario a través de la red pública para buscar bienes y hacer una selección para comprarlos. Una interfaz proporcionada por el sistema 216 intermediario podría entonces permitir al integrante identificar el sistema 112 servidor donde se podrían buscar fondos para la transacción, junto con la información de identificación del integrante. Al recibir información de identificación aceptable y autorización del integrante para proporcionar los fondos especificados al comerciante, el sistema 112 servidor puede organizar la transferencia de los fondos al control del comerciante.

La arquitectura mostrada en la figura 2A también incluye un preparador 208 autentificador, que se usa como se describe con mayor detalle a continuación para preparar autentificadores que están compuestos por la información de identificación. La figura 2B ilustra la manera en que se pueden transmitir los autentificadores y el papel general desempeñado por el preparador 208 autentificador y la intercepción 212 de la red pública. En esta figura, las líneas verticales corresponden a algunos de los elementos que se muestran en la figura 2A, a saber, el integrante 104, el preparador 208 autentificador, la intercepción 212 de la red pública y el sistema 112 servidor, con las flechas horizontales que muestran esquemáticamente la transferencia de autentificadores estáticos y dinámicos entre tales elementos en las realizaciones efectuadas de la invención.

Como se usa en este documento, los "autentificadores" se refieren genéricamente a la información de identificación que se usa para obtener acceso a un sistema servidor seguro. La información de identificación tiene al menos dos componentes, uno de los cuales es un "autentificador estático" y el otro es un "autentificador dinámico". El autentificador estático es un identificador generalmente fijo que corresponde únicamente al integrante 104, o en algunos casos a un grupo relacionado de integrantes. Por ejemplo, en una realización, el autentificador estático podría comprender una identificación de usuario, comúnmente conocida en la técnica como "ID de usuario". Cada ID de usuario distinto podría identificar un integrante distinto, aunque en algunos casos varios integrantes podrían compartir un ID de usuario común, tal como dónde un equipo de proyecto podría establecer un ID de usuario para acceder a materiales relacionados con un proyecto, tal como cuando los miembros de una familia comparten un ID de usuario familiar común y similares. El autentificador dinámico está asociado con el autentificador estático, y esa asociación se usa para confirmar la validez de la combinación al proporcionar acceso al sistema 112 servidor. Por ejemplo, en el caso de que el autentificador estático sea un ID de usuario, el autentificador dinámico asociado podría ser una contraseña. En algunos casos, particularmente en los casos en que se usa un solo autentificador estático para identificar un grupo relacionado de integrantes, se podría asociar una pluralidad de autentificadores dinámicos con cada autentificador estático, tal vez con cada autentificador dinámico asociado que identifique a uno de los integrantes. Por ejemplo, un ID de usuario común podría tener varias contraseñas válidas asociadas, cada una de las cuales es conocida solo por un grupo de integrantes y, por lo tanto, identifica a ese integrante del grupo. En otras realizaciones, tal como en el contexto donde el sistema servidor es un sistema servidor financiero, el autentificador estático podría corresponder a un número de cuenta principal ("PAN"), con el autentificador dinámico correspondiente a un número de identificación personal ("PIN") . En otras realizaciones más, los autentificadores estáticos y dinámicos pueden tomar otras formas.

Las realizaciones de la invención permiten que diferentes autentificadores estáticos y dinámicos sean utilizados por el sistema 112 servidor y por el integrante 104. Los ejemplos proporcionados anteriormente, en forma de ID de usuario/contraseña, PAN/PIN, y similares, son típicos ejemplos de autentificadores estáticos y dinámicos de un servidor que pueden ser utilizados por los sistemas 112 servidor existentes para identificar a los integrantes 104. De

acuerdo con las realizaciones de la invención, el preparador 208 autentificador asigna al integrante 104 diferentes autentificadores estáticos y dinámicos, que incorporan los autentificadores estaticos y dinámicos del servidor, pero permiten que se transmitan de forma segura a través de la red pública. La intercepción de red pública puede extraer los autentificadores estáticos y dinámicos del servidor de los autentificadores estáticos y dinámicos del integrante después de su transmisión a través de la red 108 pública para su presentación y autenticación por el sistema 112 servidor.

Por lo tanto, como se ilustra en la figura 2B, hay dos fases que pueden estar involucradas en proporcionar los métodos de transmisión seguros y los autentificadores relevantes de transporte de sistemas al integrante 104, mostrados esquemáticamente por encima de la línea de puntos, y usando los autentificadores relevantes para obtener acceso al sistema 112 servidor, que se muestra esquemáticamente debajo de la línea de puntos. Al transmitir los autentificadores relevantes al integrante 104, el sistema 112 servidor inicialmente proporciona el autentificador 240 estático de identificación del servidor y el autentificador 244 dinámico del servidor al preparador 208 autentificador. El preparador 208 autentificador genera el autentificador 248 estático del integrante y el autentificador 252 dinámico del integrante, tales como según el método descrito en detalle en relación con la figura 3 a continuación. Cuando un integrante desea para obtener acceso al sistema 112 servidor, un autentificador 248' estático de integrante suministrado y un autentificador 252' dinámico de integrante se interceptan con la intercepción 212 de la red pública. La intercepción 212 de la red pública extrae el autentificador 240' estático de servidor y autentificador 244' dinámico de servidor para la transmisión al sistema 112 servidor, tal como de acuerdo con el método descrito en detalle en relación con la figura 5 a continuación.

El diagrama de flujo de la figura 3 proporciona una ilustración de un método para proporcionar al integrante 104 los autentificadores 248 y 252 estáticos y dinámicos en una realización. En el bloque 304, el preparador 208 autentificador se proporciona con el autentificador 240 estático del servidor y el autentificador 244 dinámico del servidor, y quizás también con el autentificador 252 dinámico del integrante. El autentificador 240 estático del servidor y el autentificador 244 dinámico del servidor definen la combinación de información de identificación que el sistema 112 servidor espera recibir para permitir el acceso. Mientras que en muchos casos, se puede dejar que el integrante 104 seleccione el autentificador 252 dinámico de integrante, en algunos casos puede ser preferible que sea asignado por el sistema 112 servidor. Dicha asignación puede hacerse de forma aleatoria, lo que evita tendencia de los integrantes 104 a seleccionar autentificadores que sean más fáciles de recordar y, por lo tanto, más fácilmente comprometidos, porque representan una combinación significativa para el integrante 104. La invención no está restringida por el formato de los autentificadores 240 y 244 estáticos y dinámicos del servidor, que puede ser numérico, alfabético, alfanumérico, sensible a mayúsculas o minúsculas, de longitud arbitraria y similares.

En el bloque 308, el preparador 208 autentificador genera un autentificador 404 dinámico de servidor falso. El autentificador 404 dinámico de servidor falso generalmente puede tomar la forma de cualquier autentificador que no sea idéntico al autentificador 244 dinámico de servidor de modo que la presentación del autentificador 404 dinámico de servidor falso en combinación con el autentificador 240 estático del servidor al sistema 112 servidor dará como resultado una denegación de acceso. Sin embargo, puede ser conveniente que el autentificador 404 dinámico falso se genere con aproximadamente el mismo formato que el autentificador 244 dinámico de servidor en algunas realizaciones. Además, la presentación de tal combinación está destinada a impulsar la implementación de cualquier protocolo 116 de seguridad incluido con el sistema 112 servidor para que se mantengan los beneficios de registrar intentos falsos de acceso de acuerdo con ese protocolo 116 de seguridad.

La preparación del autentificador estático del integrante incluye una serie de técnicas de encriptado realizadas con uno o más algoritmos de encriptado de clave simétrica. Tales algoritmos de clave simétrica son tales que una de las claves de encriptado y clave de descifrado puede calcularse a partir de la otra; en muchos de estos algoritmos, las claves de encriptado y descifrado son simplemente las mismas. Los algoritmos de clave simétrica incluyen encriptados de flujo, en los que el texto sin formato se convierte en texto encriptado de un bit (o byte) a la vez, y los encriptados de bloque, que operan en bloques de texto sin formato. Muchos ejemplos de tales algoritmos de clave simétrica son bien conocidos por los expertos en la materia e incluyen, simplemente a modo de ejemplo, el Estándar de Cifrado de Datos ("DES"), el Algoritmo de Cifrado de Datos triple ("3DEA") y el Estándar de encriptado Avanzado ("AES"), entre otros.

En el bloque 312, el preparador 208 autentificador utiliza un algoritmo de clave simétrica que usa las primeras claves designadas "A" para encriptar el autentificador 244 dinámico de servidor. De manera similar, en el bloque 316 el autentificador 404 dinámico de servidor falso también está encriptado con un algoritmo de clave simétrica, que puede usar convenientemente las mismas claves "A". Si el sistema 112 de servidor no proporcionó el autentificador 252 dinámico del integrante en el bloque 304, uno puede ser generado por el preparador 208 de autentificador en el bloque 320. Dicha generación puede realizarse en concierto con el integrante 104, tal como mediante el uso de un autentificador 252 dinámico de integrante solicitado por el integrante 104, o puede ser realizado aleatoriamente por el preparador 208 autentificador, tal vez de conformidad con los requisitos de formato especificados por el sistema 112 servidor y/o el integrante 104.

En el bloque 328, el preparador 208 autentificador genera un autentificador dinámico de integrante "natural". Este autentificador se conoce como el autentificador dinámico de integrante "natural" porque se determina de acuerdo con

un algoritmo especificado a partir de un valor (412) inicial específico, que puede generarse aleatoriamente. En una realización, el algoritmo especificado puede comprender un algoritmo de clave simétrica que usa segundas claves designadas "B". Este algoritmo se aplica al valor 412 inicial aleatorio, con todo o una porción específica del resultado que se extrae para definir el autentificador dinámico del integrante natural. Un mapeo entre el autentificador dinámico de integrante natural y el autentificador 252 dinámico de integrante se define en el bloque 332 determinando un complemento 408 de autentificador dinámico de integrante del autentificador 252 dinámico de integrante y el autentificador dinámico de integrante natural. La determinación de un complemento puede realizarse de cualquier manera matemáticamente única. Por ejemplo, si el autentificador dinámico de integrante y el autentificador dinámico de integrante natural son números de 6 dígitos, el complemento podría definirse como la diferencia entre ellos. Se podría definir un complemento similar para autentificadores alfabéticos o alfanuméricos. Además, aunque dichos cálculos de diferencia son convenientemente simples, las realizaciones alternativas podrían usar definiciones de complemento más complicadas.

La combinación del complemento 408 de autentificador dinámico de integrante y el valor 412 inicial aleatorio se encriptan en el bloque 336 usando un algoritmo de clave simétrica con terceras claves designadas "C". La combinación del complemento 408 de autentificador dinámico de integrante y la inicial 412 aleatoria podría ser una simple concatenación de esas dos cantidades o podría ser una combinación más complicada en diferentes realizaciones.

El autentificador 248 estatico del integrante se genera en el bloque 340 encriptando una combinación del resultado encriptado del bloque 336, el autentificador 244 dinámico del servidor encriptado, el autentificador 404 dinámico del servidor falso encriptado y el autentificador 240 estático del servidor. Esta combinación, que puede estar formada por una simple concatenación de las cantidades o por una combinación más complicada, se encripta utilizando un algoritmo de clave simétrica con cuartas claves designadas "D".

En este punto, el preparador 208 autentificador tiene tanto el autentificador 248 estático del integrante como el autentificador 252 dinámico del integrante, que por lo tanto se puede proporcionar al integrante 104 en el bloque 344. Para proporcionar una seguridad mejorada, cada uno de estos autentificadores será usualmente proporcionado al integrante 104 de una manera diferente. Por ejemplo, el autentificador 248 estático del integrante podría descargarse al integrante 104 a través de la red 108 pública y el dispositivo 204 de acceso a la red pública, mientras que el autentificador dinámico del integrante se proporciona por separado por correo electrónico, correo postal o similar. Típicamente, el autentificador 248 estático del integrante se almacenará localmente al integrante 104 en un medio de almacenamiento legible por ordenador, que podría ser portátil como en el caso de un CD-ROM o un almacén de datos similar o podría o fijarse como en el caso de un disco duro de un ordenador.

Como se indica en la descripción anterior, el preparador 208 autentificador realiza varios encriptados al preparar el autentificador 248 estático del integrante. En algunas realizaciones, se puede usar el mismo algoritmo de encriptado para cada encriptado; en tales casos, es posible incluso usar las mismas claves para cada encriptado, aunque se proporciona una seguridad mejorada cuando se usan claves diferentes de la manera descrita. En otras realizaciones, podrían usarse diferentes algoritmos de encriptación para las diferentes encriptaciones, con, por ejemplo, un algoritmo DES para una de las encriptaciones, un algoritmo AES para otra de las encriptaciones y aún otros algoritmos de encriptación de clave simétrica. utilizado para el resto de los encriptados.

Ejemplo La generación de los autentificadores de integrante de acuerdo con la figura 3 puede ilustrarse con un ejemplo simplificado. Para estos fines de ilustración, suponga que en el bloque 304, el sistema 112 servidor provee al preparador 208 autentificador con un autentificador estático de servidor S_H = SMITH y un autentificador dinámico de servidor D_H = 1234. En el bloque 308, el preparador autentificador genera un falso servidor dinámico autentificador $\overline{D}_H$ = 9876, que es diferente de D_H y, en este caso, tiene un formato similar a D_H. En el bloque 312, el autentificador dinámico del servidor se encripta con las primeras claves “A” simétricas para producir

$$E_A\left[D_H\right] = E_A\left[1234\right] = 827395,$$

y en el bloque 316, el autentificador dinámico falso se encripta con las primeras claves “A” simétricas para producir

$$E_A\left[\overline{D}_H\right] = E_A\left[9876\right] = 662883.$$

En el bloque 320, el preparador 208 autentificador genera el autentificador dinámico de integrante aleatoriamente para producir D_P = 2468. En el bloque 324, el preparador 208 autentificador genera un valor de inicial aleatorio para producir S = 629663. Generación del autentificador en 328 dinámico de integrante natural puede realizarse encriptando la inicial S con segundas claves “B” simétricas y extrayendo los cuatro dígitos en las posiciones 3ª a 6ª más significativas:

$$E_B\left[S\right] = E_B\left[629663\right] = 145\underline{8}\underline{2}\underline{5}\underline{5}73,$$

de modo que

$$D_P^{(\mathrm{nat})} = 8255.$$

El complemento de autentificador dinámico de integrante determinado en el bloque 332 puede tomar la forma de una diferencia entre DP y

$$D_P^{(\mathrm{nat})}$$

de modo que el complemento sea

$$C_P = D_P^{(\mathrm{nat})} - D_P = 8255 - 2468 = 5787.$$

El encriptado de la combinación del valor S inicial y el complemento Cp de autentificador dinámico de integrante puede producir

$$\begin{aligned} E_C\left[S \oplus C_P\right] &= E_C\left[629663 \oplus 5787\right] \\ &= E_C\left[6296635787\right] \\ &= 9820003628. \end{aligned}$$

cuando la combinación se produce por concatenación. La formación del autentificador estático S_P en el bloque 340 puede entonces proceder combinando las cantidades identificadas y encriptando la combinación con cuartas claves "D":

$$\begin{aligned} S_P &= E_D\left[E_A\left[D_H\right] \oplus E_A\left[\bar{D}_H\right] \oplus E_C\left[S \oplus C_P\right] \oplus S_H\right] \\ &= E_D\left[827395 \oplus 662883 \oplus 982000362\,8 \oplus \mathrm{SMITH}\right] \\ &= E_D[827395662883982000362 8\mathrm{SMITH}] \\ &= 726\mathrm{B}2626\mathrm{FZ}28463\mathrm{KR}8650025\mathrm{LPO}3. \end{aligned}$$

La estructura de datos del autentificador 248 estático del integrante después de su generación con el método descrito en relación con la figura 3 se muestra esquemáticamente en la figura 4. Cada una de las elipses en la figura representa un bloque de datos y corresponde a los bloques de datos descritos en la formación del autentificador 248 estático del integrante. Esas elipses que se designan con subíndices identifican que los datos en esos bloques de datos se han generado al menos en parte mediante el encriptado de información. Por lo tanto, dentro de la estructura de datos del autentificador 248 estático del integrante hay bloques de datos que corresponden al autentificador 244 dinámico del servidor encriptado, el autentificador 404 dinámico del servidor falso encriptado, el autentificador 240 estático del servidor y la combinación 416 encriptada del complemento 408 de autentificador dinámico del integrante y valor (412) inicial aleatorio. En algunos casos, la transmisión del autentificador 248 estático del integrante en el bloque 344 de la figura 3 puede ser realizado como parte de un bloque 404 de datos que incluye uno o más bloques de datos 420 suplementarios además del autentificador 248 estático del integrante. Tales datos 420 suplementarios podrían incluir información de enrutamiento y similares que podrían usarse para transmitir los datos al integrante 104.

La estructura de los autentificadores en las realizaciones de la invención incluye información para la cual se realizan esfuerzos para mantener el secreto de la información, así como información que se considera "limpia" y para la cual no se realizan esfuerzos de secreto significativos. La siguiente tabla proporciona una comparación de tales protocolos de secreto para una estructura de ejemplo de la técnica anterior y para los símbolos de la invención. En particular, la estructura de ejemplo de la técnica anterior corresponde a la estructura PAN/PIN discutida previamente y comúnmente utilizada en aplicaciones financieras. El PAN identifica una cuenta financiera y es un ejemplo de la técnica anterior de un autentificador estático, mientras que el PIN del cliente es un código privado utilizado por un cliente para acceder a la cuenta financiera y es un ejemplo de la técnica anterior de un autentificador dinámico. En tal ejemplo, el "desplazamiento de PIN" es un complemento que se utiliza para asignar un PIN natural al PIN del cliente.

Técnica Anterior		Corriente	
Información	Estado de secreto	Información	Estado de secreto
PAN	Limpio	Valor Inicial Aleatorio	Secreto
PIN del cliente	Secreto	Autentificador Dinámico de Integrante	Limpio
PIN Natural	Privado	Autentificador Dinámico de Integrante Natural	Privado
Desplazamiento de PIN	Limpio	Complemento de Autentificador Dinámico de Integrante	Secreto
Claves de encriptado	Privado	Claves de encriptado	Privado

La tabla ilustra que, si bien el PIN del cliente de la técnica anterior, es decir, un ejemplo de un autentificador dinámico de la técnica anterior, se mantiene en secreto, las realizaciones de la invención permiten en cambio que el autentificador dinámico del integrante se trate de forma limpia. Este tratamiento del autentificador dinámico del integrante representa, por lo tanto, una desviación significativa de la forma en que tradicionalmente se ha manejado la seguridad de la información de identificación.

La figura 5 proporciona un diagrama de flujo que ilustra los métodos por los cuales los autentificadores del integrante pueden ser utilizados por el integrante 104 para obtener acceso al sistema 112 servidor. Dicho acceso puede ser adquirido en diferentes realizaciones al interactuar con la intercepción 212 de la red pública directamente a través de la red pública o transmitiendo la información de identificación a través de un sistema 216 intermediario. Por lo tanto, en un caso en el que el acceso se logra directamente con la intercepción 212 de la red pública, el integrante 104 se conecta a la intercepción 212 de la red pública con un dispositivo 204 de acceso a la red pública en el bloque 504. El intercambio de información entre la intercepción 212 de la red pública y el dispositivo 204 de acceso a la red pública se enruta a través de la red 108 pública. En el bloque 508, el integrante 104 indica un deseo de acceder al sistema 112 de servidor a la intercepción 212 de la red pública. Esto podría hacerse, por ejemplo, identificando un localizador universal de recursos ("URL") en una realización donde la red 108 pública comprende Internet y el dispositivo de acceso a la red comprende un ordenador conectado a Internet. En los bloques 512 y 516, respectivamente, el integrante 104 proporciona el autentificador 248 estático del integrante y el autentificador 252 dinámico del integrante a la intercepción 212 de la red pública. Esto podría comprender la descarga del autentificador 248 estático estructuralmente más complicado del almacén de datos local del dispositivo 204 de acceso a la red pública a la intercepción 212 de la red pública, mientras se ingresa el autentificador 252 dinámico más simple de la memoria del integrante a través de una interfaz de usuario.

En el caso de que el acceso se logre con un sistema 216 intermediario, el integrante 104 se conecta al sistema intermediario con un dispositivo 204 de acceso a la red pública en el bloque 552. En el contexto se hizo un ejemplo de un sistema intermediario discutido anteriormente del comercio electrónico, aunque la discusión en este documento se aplica generalmente a cualquier arreglo en el que la información de identificación del integrante pueda pasar a través de un sistema intermediario. En el bloque 556, el integrante 104 indica al sistema 216 intermediario un deseo de acceder al sistema 112 servidor. Por ejemplo, en el contexto del comercio electrónico, dicha indicación puede tomar la forma de proporcionar información financiera después de que el integrante 104 haya decidido hacer una compra al intermediario. En los bloques 560 y 564, el integrante proporciona el autentificador 248 estático del integrante y el autentificador 252 dinámico del integrante al sistema 216 intermediario. Esto puede hacerse de una manera similar a la descrita con respecto a proporcionar dichos autentificadores del integrante directamente a la intercepción de la red pública, es decir, descargando el autentificador 248 estático del integrante de un almacén de datos local e ingresando el autentificador 252 dinámico del integrante desde la memoria del integrante a través de una interfaz. En el bloque 568, el sistema 216 intermediario proporciona los autentificadores 248 y 252 del integrante a la intercepción 212 de la red pública.

Independientemente de si la transmisión se produce directamente, como para los bloques 504 - 516, o indirectamente, como para los bloques 552 - 568, la intercepción 112 de la red pública está provista de autentificadores 248 y 252 de integrante estáticos y dinámicos. El elemento componente de la intercepción 212 de red pública en el bloque 520 se extrae del autentificador 248 estático de integrante descifrando el autentificador 248 de integrante estático con cuartas claves simétricas "D". El elemento componente que incluye el complemento 408 de autentificador dinámico de integrante y el valor 412 inicial se descifra en el bloque 524 usando las terceras claves simétricas "C" para extraer esos componentes. En el bloque 528, el valor (412) inicial descifrado se usa para generar un autentificador dinámico de integrante natural de la misma manera que se describió en relación con el bloque 328 de la figura 3. Específicamente, se puede aplicar un algoritmo de encriptación que usa segundas claves "B" al valor inicial, y una

porción específica del resultado extraído para definir el autentificador dinámico del integrante natural. El autentificador dinámico de integrante natural resultante se combina con el complemento 408 de autentificador dinámico de integrante descifrado en el bloque 532, y se realiza una comprobación en el bloque 536 si el resultado de esa combinación coincide con el autentificador 252 dinámico de integrante que se recibió.

Una coincidencia del resultado con el autentificador 252 dinámico del integrante confirma la identidad del integrante 104. En respuesta, la intercepción 212 de la red pública descifra el autentificador 244 dinámico del servidor con las primeras claves “A” simétricas en el bloque 540. El el autentificador 244 dinámico de servidor descifrado se transmite luego con el autentificador 240 estático de servidor, que se recuperó en el bloque 520, al sistema 112 servidor. Si el resultado del bloque 532 no coincide con el autentificador 252 dinámico de integrante cuando se verifica en el bloque 536, la intercepción 212 de la red pública descifra el autentificador 404 dinámico del servidor falso con las primeras claves “A” simétricas en el bloque 572. Este autentificador 404 dinámico del servidor falso descifrado se transmite luego al sistema 112 servidor con el autentificador 240 estático del servidor en el bloque 576.

El sistema 112 servidor sigue siendo libre de realizar su propia validación de la información de identificación que recibe, permitiendo así el uso completo de su protocolo 116 de seguridad, incluida la capacidad de responder a intentos repetidos de acceso fallidos. Por lo tanto, el sistema 112 servidor intenta validar los datos que recibe en el bloque 580, tal como comparando el autentificador dinámico del servidor con un valor que espera estar asociado con el autentificador estático del servidor que recibe. Si los datos se validan, como se espera en el caso en que la verificación realizada en el bloque 536 confirme la identidad del integrante 104, se puede establecer una conexión segura entre el integrante 104 y el sistema 112 servidor en el bloque 548. Si los datos son no validado, dicha conexión puede ser denegada en el bloque 584, y el intento de conexión puede ser registrado por el sistema 112 servidor de acuerdo con su protocolo 116 de seguridad.

Ejemplo La extracción de información de identificación y su uso para establecer o negar una conexión entre el integrante 104 y el sistema 112 servidor como se describe en la figura 5 se ilustra con el ejemplo simplificado discutido previamente en relación con la figura 3. Independientemente de si la información se transmite directamente desde el dispositivo 204 de acceso a la red pública o a través de un sistema 216 intermediario, la intercepción de la red pública recibe el autentificador estático de integrante S_P = 726B2626FZ28463KR8650025LP03 y el autentificador dinámico de integrante D_P = 2468 en el bloque 520. Descifrado del autentificador estático de la parte S_P en el bloque 520 con cuartas claves simétricas "D", se obtiene la extracción del autentificador dinámico de servidor encriptado $E_A[D_H]$, el autentificador dinámico de servidor falso encriptado $E_A[\overline{D}_H]$, la combinación encriptada del valor inicial y el autentificador dinámico de integrante complementan $E_C[S \oplus C_P]$, y el autentificador estático del servidor S_H:

$$D_D\left[S_P\right] = D_D\left[726\text{B}2626\text{FZ}28463\text{KR}8650025\text{LP}03\right]$$
$$= 827395 \oplus 662883 \oplus 9820003628 \oplus \text{SMITH}.$$

En el bloque 524, la combinación del valor S inicial y el complemento C_P de autentificador dinámico de integrante se identifica con el elemento apropiado y se descifra con las terceras claves simétricas "C" para identificar los elementos individuales:

$$D_C\left[E_C\left[S \oplus C_P\right]\right] = D_C\left[9820003628\right]$$
$$= 629663 \oplus 5787.$$

El valor S inicial se usa en el bloque 528 para generar el autentificador dinámico del integrante natural

$$D_P^{(\text{nat})}$$

utilizando el algoritmo que incluye el encriptado con las segundas claves “B” simétricas y la extracción de dígitos resultantes específicos:

$$E_B\left[S\right] = E_B\left[629663\right] = 145\underline{8}\underline{2}\underline{5}\underline{5}73,$$

de modo que, como antes,

$$D_P^{(\text{nat})} = 8255.$$

Combinando el autentificador dinámico de integrante natural

$$D_P^{(\mathrm{nat})}$$

y el complemento de autentificador dinámico de integrante Cp en el bloque 532 proporciona un resultado R que puede compararse con el autentificador dinámico de integrante Dp en el bloque 536:

$$\begin{aligned} R &= D_P^{(\mathrm{nat})} - C_P \\ &= 8255 - 5787 = 2468. \end{aligned}$$

En este caso, el resultado coincide con el autentificador dinámico de integrante, R = D_P, de modo que el autentificador dinámico del servidor se descifra en el bloque 540:

$$D_H = D_A\left[E_A\left[D_H\right]\right] = D_A\left[827395\right] = 1234.$$

El autentificador S_H = SMITH estático del servidor y el autentificador D_H = 1234 dinámico del servidor se proporcionan al sistema servidor en el bloque 544 para que el sistema servidor valide los datos recibidos. Si el resultado R no coincidía con el autentificador dinámico del integrante, R ≠ D_P, porque se proporcionó el autentificador dinámico del integrante incorrecta, el autentificador dinámico del servidor falso se descifrar en el bloque 572,

$$\bar{D}_H = D_A\left[E_A\left[\bar{D}_H\right]\right] = D_A\left[662883\right] = 9876,$$

y proporcionado al sistema servidor con el autentificador S_H = SMITH estático del servidor en el bloque 576. El sistema servidor negaría así el establecimiento de una conexión y registraría el intento de acuerdo con sus protocolos de seguridad.

La descripción de los métodos en relación con las figuras 3 y 5 corresponden al caso en el que un único autentificador 244 dinámico de servidor válido está asociado con cada autentificador 240 estático de servidor. En otras realizaciones, el método puede acomodar múltiples autentificadores 244 dinámicos de servidor para cada autentificador 240 estático de servidor en aquellos casos en que múltiples integrantes pueden compartir un autentificador 244 estático del servidor pero ser identificado individualmente por uno respectivo de una pluralidad de autentificadores 244 dinámicos del servidor. En tales casos, el preparador 208 autentificador podría recibir la pluralidad de autentificadores 244 dinámicos del servidor en el bloque 304 de la figura 3, con el autentificador 404 dinámico de servidor falso generado en el bloque 308 es diferente de cada uno de la pluralidad de autentificadores 244 dinámicos de servidores válidos. Cada uno de esos autentificadores 244 dinámicos de servidor puede encriptarse usando las primeras claves “A” simétricas en los bloques 312, con otros bloques en la figura 3 se realiza como se describió previamente con cada autentificador 244 dinámico de servidor para determinar una pluralidad respectiva de complementos 408 de autentificador dinámico de integrante. Esta pluralidad de complementos de autentificador dinámico puede entonces combinarse y codificarse con el valor 412 inicial como se describe en relación con el bloque 336. La estructura resultante del autentificador 248 estático de integrante como se muestra en la figura 4 se modificaría de modo que incluye una pluralidad de autentificadores 244 dinámicos de servidor encriptados en lugar del único mostrado, y con el bloque 416 de datos que incluye una pluralidad correspondiente de complementos 408 de autentificador dinámico de integrante en lugar del único que se muestra. El uso de los autentificadores en la figura 5 se modificaría de modo que se determinara una pluralidad de resultados en el bloque 532, correspondiente a cada uno de la pluralidad de complementos 408 de autentificador dinámico del integrante. La verificación en el bloque 536 se realizaría para determinar si alguno de los resultados coinciden con el autentificador 252 dinámico de integrante, con el autentificador 244 dinámico de servidor correspondiente que se descifra y se transmite al sistema servidor en los bloques 540 y 544, si lo hace. El sistema 112 servidor puede responder como se espera, incluso con disposiciones que pueden incluirse con su protocolo 116 de seguridad, determinando si un autentificador estático de servidor recibido está acompañado por alguno de los autentificadores dinámicos de servidor que ha identificado como válidos.

La figura 6 proporciona una ilustración esquemática de una estructura que puede usarse para implementar la intercepción 212 de la red pública. El sistema 112 servidor y/o el dispositivo 204 de acceso a la red pública podrían tener estructuras análogas en algunas realizaciones. La figura 3 ilustra ampliamente cómo los elementos individuales del sistema pueden implementarse de manera separada o más integrada. La intercepción 212 de la red pública se muestra compuesta por elementos de hardware que están eléctricamente acoplados a través del bus 626, incluido un procesador 602, un dispositivo 604 de entrada, un dispositivo 606 de salida, un dispositivo 608 de almacenamiento, un lector 610a de medios de almacenamiento legible por ordenador, un sistema 614 de comunicaciones, una unidad 616 de aceleración de procesamiento tal como un DSP o procesador de propósito especial, y una memoria 618. El lector 610a de medios de almacenamiento legible por ordenador está conectado además a un medio 610b de almacenamiento legible por ordenador, la combinación que representa integralmente remota, dispositivos de

almacenamiento locales, fijos y/o extraíbles, además de medios de almacenamiento para contener temporalmente y/o más permanentemente información legible por ordenador. El sistema 614 de comunicaciones puede comprender una conexión de interfaz cableada, inalámbrica, de módem y/o de otro tipo y permite el intercambio de datos con la red 108 pública y/o el sistema 112 servidor, como se describió anteriormente.

La intercepción 212 de la red pública también comprende elementos de software, que se muestran actualmente ubicados dentro de la memoria 620 de trabajo, que incluye un sistema 624 operativo y otro código 622, tal como un programa diseñado para implementar métodos de la invención. Será evidente para los expertos en la técnica que se pueden realizar variaciones sustanciales de acuerdo con los requisitos específicos. Por ejemplo, también podría usarse hardware personalizado y/o elementos particulares podrían implementarse en hardware, software (incluyendo software portátil, tal como applets), o ambos. Además, se puede emplear la conexión a otros dispositivos informaticos tales como dispositivos de entrada/salida de red.

REIVINDICACIONES

1. Un método para generar un autentificador (248, 248[1]) estático de integrante para ser usado en combinación con un autentificador (252, 252[1]) dinámico de integrante para identificar un integrante (104) a un sistema (112) servidor, el método comprende:

recibir información de identificación que identifica el integrante (104) en el sistema (112) servidor, comprendiendo la información un autentificador (244, 244[1]) dinámico de servidor y un autentificador (240, 240[1]) estático de servidor;

generar, con un procesador, un autentificador (404) dinámico de servidor falso, en donde el autentificador (404) dinámico de servidor falso difiere del autentificador (244, 244[1]) dinámico de servidor;

encriptar el autentificador (244, 244[1]) dinámico del servidor;

encriptar el autentificador (404) dinámico de servidor falso;

encriptar información que identifica de forma exclusiva el autentificador (252, 252[1]) dinámico del integrante en donde la información que identifica de forma única el autentificador dinámico del integrante comprende un valor (412) inicial y un complemento (408) al autentificador dinámico del integrante, el método comprende además determinar el complemento (408) al autentificador dinámico del integrante a partir del valor inicial y al autentificador dinámico del integrante encriptando el valor (412) inicial, seleccionando una porción del valor inicial cifrado que tiene una longitud predeterminada para producir un autentificador dinámico de integrante natural, y calculando una diferencia entre el autentificador dinámico de integrante natural y el autentificador dinámico de integrante;

y comprendiendo el método además producir el autentificador (248, 2481) estático del integrante encriptando una combinación del autentificador estático del servidor, el autentificador dinámico del servidor encriptado, el autentificador dinámico del servidor falso encriptado y la información encriptada que identifica de forma única el autentificador dinámico del integrante.

2. El método citado en la reivindicación 1, en donde cada uno de los pasos de encriptado se realiza con un algoritmo de encriptado de clave simétrica.

3. El método citado en la reivindicación 2, en donde cada uno de los pasos de encriptado se realiza con una clave diferente.

4. El método citado en la reivindicación 2, en donde el encriptado del autentificador dinámico del servidor y el encriptado del autentificador dinámico del servidor falso se realizan con la misma clave.

5. El método citado en la la reivindicación 1, que comprende además generar el valor de inicial al azar.

6. El método método citado en la la reivindicación 1, que comprende además recibir el autentificador (252) dinámico del integrante desde el sistema servidor.

7. El método método citado en la en la reivindicación 1, que comprende además generar el autentificador dinámico del integrante aleatoriamente.

8. Un método para transmitir información de identificación del integrante a un sistema servidor, el método comprende:

recibir un autentificador (248[1]) estático de integrante y un autentificador (252[1]) dinámico supesto de un integrante (104);

descifrar el autentificador (248[1]) estático de integrante para extraer un autentificador dinámico de servidor encriptado, un autentificador dinámico de servidor falso encriptado, un autentificador (240[1]) estático de servidor e información encriptada que identifica de forma única un autentificador (252[1]) dinámico de integrante, en donde el autentificador (240) estático de servidor y el (244) autentificador dinámico de servidor identifican al integrante (104) en el sistema (112) servidor y el autentificador dinámico de servidor falso difiere del autentificador dinámico de servidor;

generar, con un procesador, el autentificador dinámico del integrante a partir de la información encriptada que identifica de manera única el autentificador dinámico del integrante en donde generar el autentificador (252[1]) dinámico del integrante comprende descifrar la información encriptada que identifica de manera única el autentificador (252[1]) dinámico del integrante para extraer un valor (412) inicial y un complemento (408) al autentificador dinámico de integrante, y generar el autentificador dinámico de integrante a partir del valor inicial y el complemento encriptando el valor inicial, seleccionando una porción del valor inicial encriptado que tiene una longitud predeterminada para producir un autentificador dinámico de integrante natural, y calcular una diferencia entre el autentificador dinámico de integrante natural y el complemento;

y el método incluye transmitir el autentificador (240) estático del servidor y uno descifrado del autentificador dinámico del servidor y un autentificador dinámico del servidor falso al sistema (112) servidor dependiendo de una comparación del autentificador dinámico del integrante y el autentificador dinámico del supuesto integrante.

9. El método citado en la reivindicación 8, que comprende además descifrar el del autentificador dinámico del servidor y el autentificador dinámico del servidor falso dependiendo de la comparación del autentificador dinámico del integrante y el autentificador dinámico del supuesto integrante.

10. El método citado en la reivindicación 8, en donde recibir el autentificador (248^1) estático del integrante y el autentificador dinámico del integrante supuesta comprende recibir el autentificador (248^1) estático del integrante y el autentificador dinámico del integrante supuesta a través de una red (108) pública desde un dispositivo (204) de acceso a la red pública accedido por el integrante (104).

11. El método citado en la reivindicación 8, en donde recibir el autentificador estático del integrante y el autentificador dinámico del integrante supuesta comprende recibir el autentificador estático del integrante y el autentificador dinámico del supuesto integrante a través de una red (108) pública desde un sistema (216) intermediario al que accedel integrante con un dispositivo de acceso a la red pública.

12. El método citado en la reivindicación 8, en donde cada uno de los pasos de descifrado se realiza con un algoritmo de descifrado de clave simétrica.

13. El método citado en la reivindicación 12, en donde cada uno de los pasos de descifrado se realiza con una clave diferente.

14. Un medio (610b) de almacenamiento legible por ordenador que tiene un programa legible por ordenador incorporado para dirigir la operación de un preparador (208) autentificador que incluye un sistema de comunicaciones, un procesador y un dispositivo de almacenamiento, en donde el programa legible por ordenador incluye instrucciones para operar el preparador (208) autentificador para generar un autentificador (248, 248^1) estático de integrante que se utilizará en combinación con un autentificador (252, 252^1) dinámico de integrante para identificar un integrante (104) a un sistema (112) servidor de acuerdo con lo siguiente:

recibir, con el sistema de comunicaciones, información de identificación que identifica al integrante (104) en el sistema (112) servidor, la información comprende un autentificador (244, 244^1) dinámico de servidor y un autentificador (240, 240^1) estático de servidor;

generar, con el procesador, un autentificador (404) dinámico de servidor falso, en donde el autentificador dinámico de servidor falso difiere del autentificador (244, 244^1) dinámico de servidor;

encriptar, con el procesador, el autentificador (244, 244^1) dinámico del servidor;

encriptar, con el procesador, el autentificador (404) dinámico de servidor falso;

encriptar, con el procesador, la información que identifica de forma exclusiva el autentificador (252, 252^1) dinámico del integrante en donde la información que identifica de forma única el autentificador (252, 252^1) dinámico del integrante comprende un valor (412) inicial y un complemento (408) para el autentificador dinámico del integrante, el programa legible por ordenador que incluye además instrucciones para determinar, con el procesador, el complemento del autentificador dinámico del integrante encriptando, con el procesador, el valor (412) inicial, seleccionando, con el procesador, una porción del valor inicial encriptado que tiene una longitud predeterminada para producir un autentificador dinámico de integrante natural, y

calcular, con el procesador, una diferencia entre el autentificador dinámico de integrante natural y el autentificador dinámico de integrante; y

producir, con el procesador, el autentificador (248, 248^1) estático del integrante mediante el encriptado de una combinación del autentificador estático del servidor, el autentificador dinámico del servidor encriptado, el autentificador dinámico del servidor falso encriptado y la información encriptada que identifica de forma única el autentificador dinámico del integrante.

15. El medio de almacenamiento legible por ordenador mencionado en la reivindicación 14 en donde el programa legible por ordenador incluye además instrucciones para recibir, con el sistema de comunicaciones, el autentificador dinámico del integrante del sistema servidor.

16. El medio de almacenamiento legible por ordenador mencionado en la reivindicación 14 en donde el programa legible por ordenador incluye además instrucciones para generar, con el procesador, el autentificador dinámico del integrante aleatoriamente.

17. Un medio de almacenamiento legible por ordenador que tiene un programa legible por ordenador incorporado para dirigir la operación de una intercepción de red pública que incluye un sistema de comunicaciones, un procesador y un dispositivo de almacenamiento, en donde el programa legible por ordenador incluye instrucciones para operar la intercepción de la red pública para transmitir información de identificación del integrante a un sistema servidor de acuerdo con lo siguiente:

recibir, con el sistema de comunicaciones, un autentificador (248^1) estático de integrante y un autentificador (252^1) dinámico de integrante supuesta de un integrante (104);

descifrar, con el procesador, el autentificador (248) estático de integrante para extraer un autentificador dinámico de servidor encriptado, un autentificador dinámico de servidor falso encriptado, un autentificador (240) estático de servidor e información encriptada que identifica de forma única un autentificador (252^1) dinámico de integrante, en donde el autentificador (240^1) estático del servidor y el autentificador (252^1) dinámico del servidor identifican al integrante (104) del sistema (112) servidor y el autentificador dinámico del servidor falso difiere del autentificador dinámico del servidor;

generar, con el procesador, el autentificador dinámico del integrante a partir de la información encriptada que identifica de forma exclusiva el autentificador dinámico del integrante descifrando, con el procesador, la información encriptada que identifica de forma única el autentificador (252^1) dinámico del integrante para extraer un valor (412) inicial y un complemento (408) al autentificador (252^1) dinámico de integrante; y

generar, con el procesador, el autentificador dinámico del integrante a partir del valor inicial y el complemento, encriptando, con el procesador, el valor (412) inicial, seleccionando, con el procesador, una porción del valor inicial encriptado que tiene una longitud predeterminada para producir un autentificador dinámico de integrante natural y calcular, con el procesador, una diferencia entre el autentificador dinámico de integrante natural y el complemento; y

transmitir, con el sistema de comunicaciones, el autentificador (240) estático del servidor y uno descifrado del autentificador dinámico del servidor y el autentificador dinámico del servidor falso al sistema servidor, según una comparación del autentificador dinámico del integrante y el autentificador dinámico del supuesto integrante.

18. El medio de almacenamiento legible por ordenador mencionado en la reivindicación 17, en donde el programa legible por ordenador incluye además instrucciones para descifrar, con el procesador, el autentificador (252^1) dinámico del servidor y el autentificador dinámico del servidor falso dependiendo de la comparación del autentificador dinámico del integrante y el supuesto autentificador dinámico del integrante.

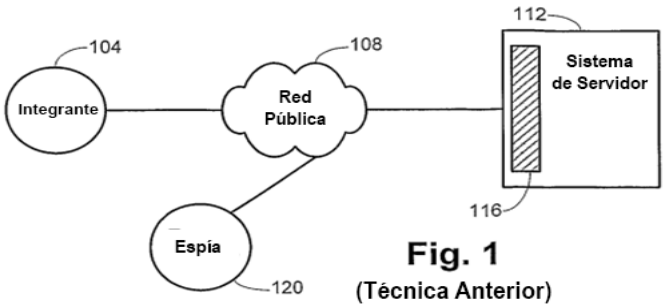

Fig. 1
(Técnica Anterior)

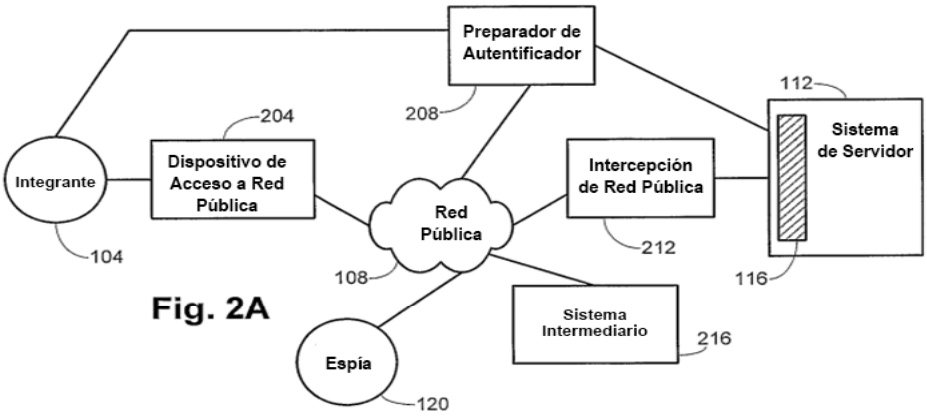

Fig. 2A

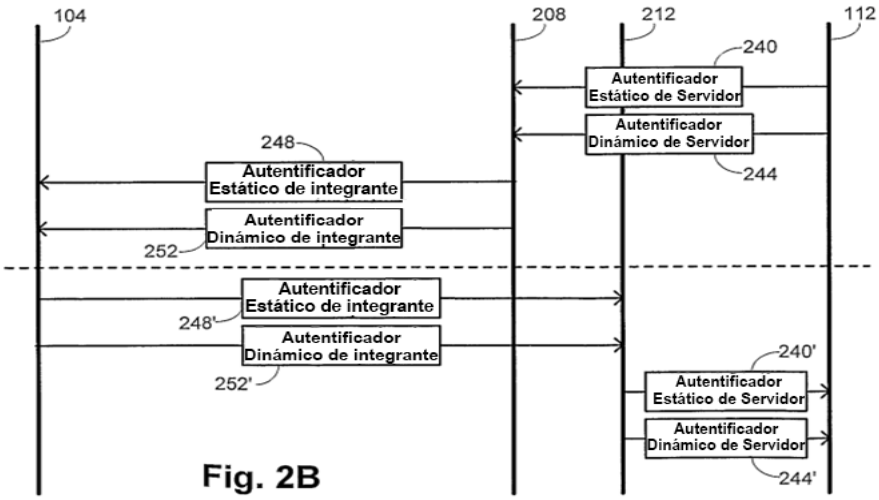

Fig. 2B

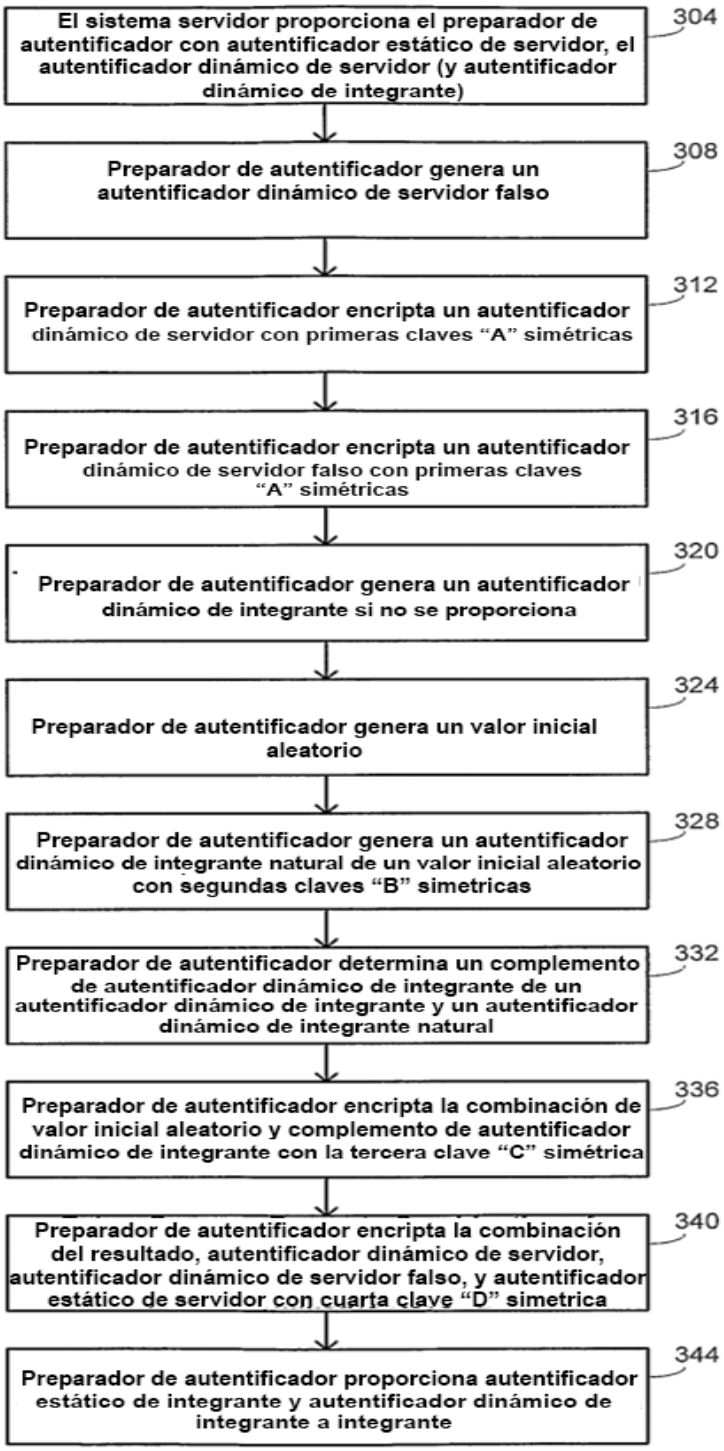
El sistema servidor proporciona el preparador de autentificador con autentificador estático de servidor, el autentificador dinámico de servidor (y autentificador dinámico de integrante)
304
Preparador de autentificador genera un autentificador dinámico de servidor falso
308
Preparador de autentificador encripta un autentificador dinámico de servidor con primeras claves "A" simétricas
312
Preparador de autentificador encripta un autentificador dinámico de servidor falso con primeras claves "A" simétricas
316
Preparador de autentificador genera un autentificador dinámico de integrante si no se proporciona
320
Preparador de autentificador genera un valor inicial aleatorio
324
Preparador de autentificador genera un autentificador dinámico de integrante natural de un valor inicial aleatorio con segundas claves "B" simetricas
328
Preparador de autentificador determina un complemento de autentificador dinámico de integrante de un autentificador dinámico de integrante y un autentificador dinámico de integrante natural
332
Preparador de autentificador encripta la combinación de valor inicial aleatorio y complemento de autentificador dinámico de integrante con la tercera clave "C" simétrica
336
Preparador de autentificador encripta la combinación del resultado, autentificador dinámico de servidor, autentificador dinámico de servidor falso, y autentificador estático de servidor con cuarta clave "D" simetrica
340
Preparador de autentificador proporciona autentificador estático de integrante y autentificador dinámico de integrante a integrante
344

Fig. 3

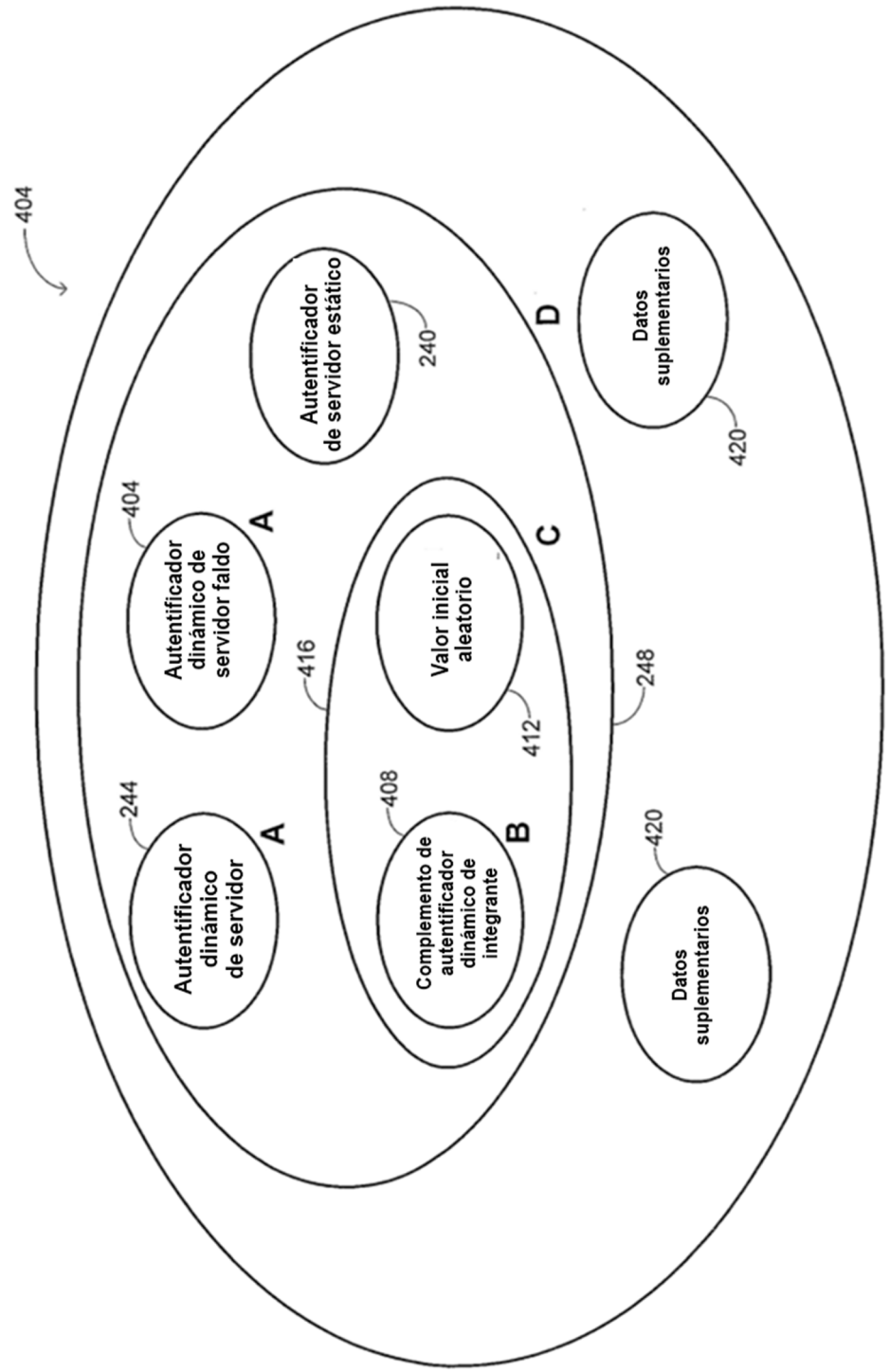
404
Autentificador dinámico de servidor
244
A
Autentificador dinámico de servidor faldo
404
A
Autentificador de servidor estático
240
D
Datos suplementarios
420
Valor inicial aleatorio
412
C
Complemento de autentificador dinámico de integrante
408
B
416
248
Datos suplementarios
420

Fig. 4

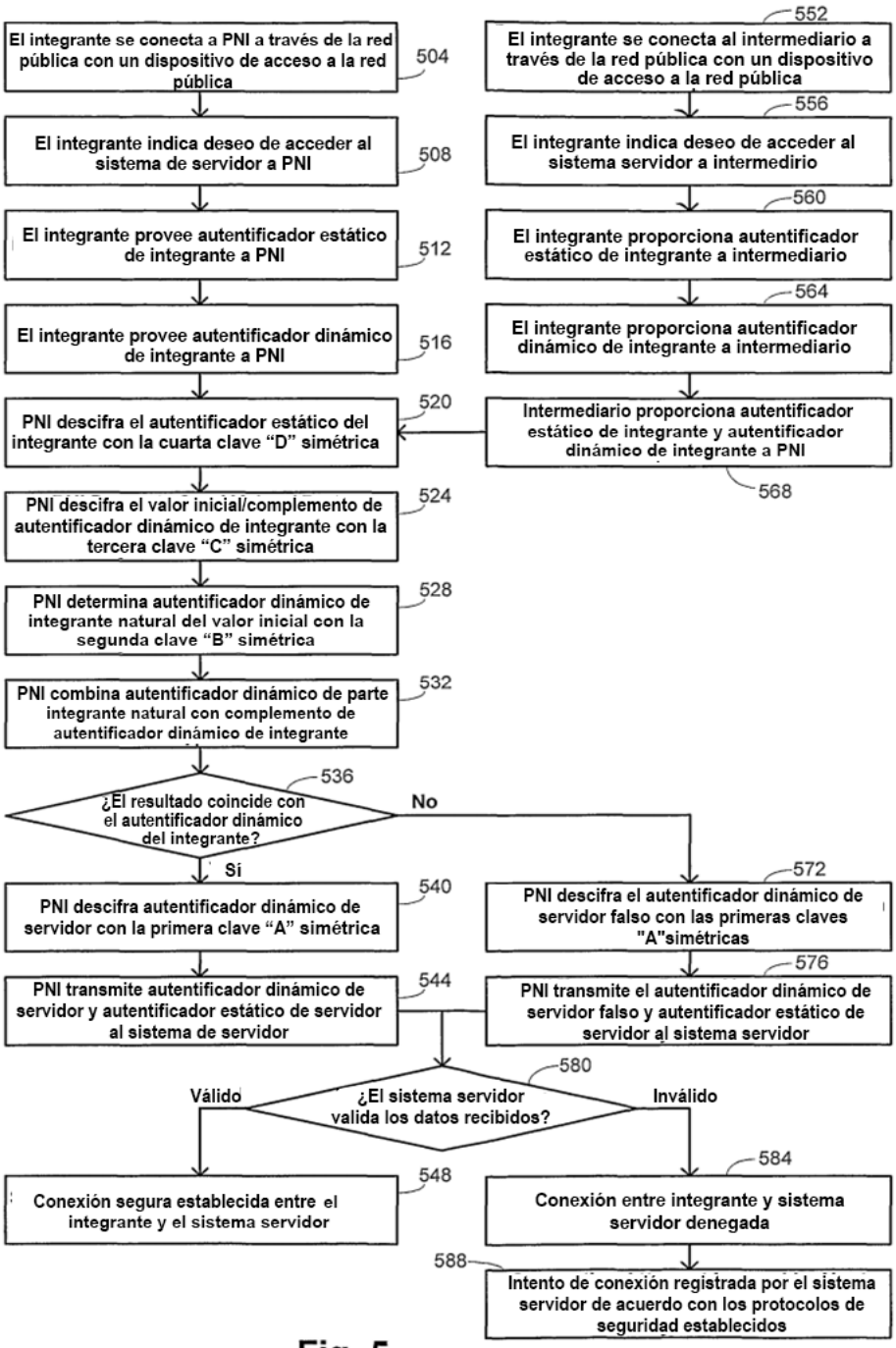
El integrante se conecta a PNI a través de la red pública con un dispositivo de acceso a la red pública
504
El integrante indica deseo de acceder al sistema de servidor a PNI
508
El integrante provee autentificador estático de integrante a PNI
512
El integrante provee autentificador dinámico de integrante a PNI
516
PNI descifra el autentificador estático del integrante con la cuarta clave "D" simétrica
520
PNI descifra el valor inicial/complemento de autentificador dinámico de integrante con la tercera clave "C" simétrica
524
PNI determina autentificador dinámico de integrante natural del valor inicial con la segunda clave "B" simétrica
528
PNI combina autentificador dinámico de parte integrante natural con complemento de autentificador dinámico de integrante
532
¿El resultado coincide con el autentificador dinámico del integrante?
536
No
Sí
PNI descifra autentificador dinámico de servidor con la primera clave "A" simétrica
540
PNI transmite autentificador dinámico de servidor y autentificador estático de servidor al sistema de servidor
544
¿El sistema servidor valida los datos recibidos?
580
Válido
Inválido
Conexión segura establecida entre el integrante y el sistema servidor
548
El integrante se conecta al intermediario a través de la red pública con un dispositivo de acceso a la red pública
552
El integrante indica deseo de acceder al sistema servidor a intermedirio
556
El integrante proporciona autentificador estático de integrante a intermediario
560
El integrante proporciona autentificador dinámico de integrante a intermediario
564
Intermediario proporciona autentificador estático de integrante y autentificador dinámico de integrante a PNI
568
PNI descifra el autentificador dinámico de servidor falso con las primeras claves "A"simétricas
572
PNI transmite el autentificador dinámico de servidor falso y autentificador estático de servidor al sistema servidor
576
Conexión entre integrante y sistema servidor denegada
584
Intento de conexión registrada por el sistema servidor de acuerdo con los protocolos de seguridad establecidos
588

Fig. 5

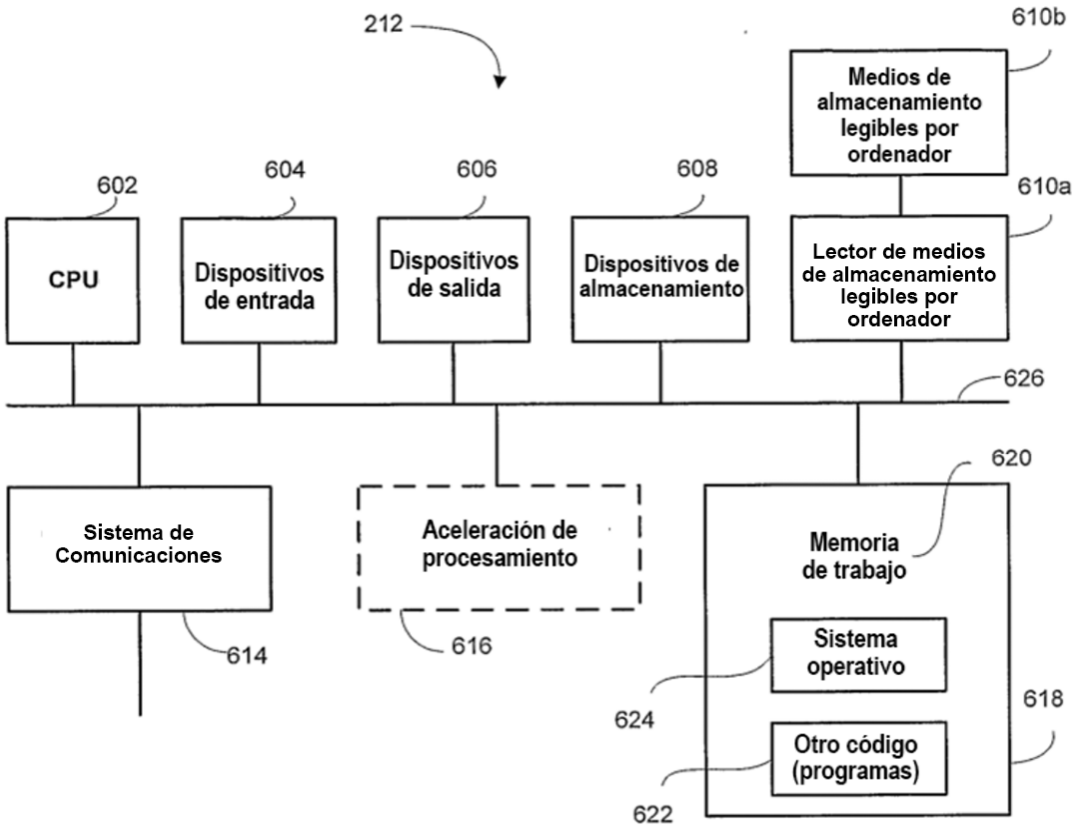
212
610b
Medios de almacenamiento legibles por ordenador
602
604
606
608
610a
CPU
Dispositivos de entrada
Dispositivos de salida
Dispositivos de almacenamiento
Lector de medios de almacenamiento legibles por ordenador
626
620
Sistema de Comunicaciones
Aceleración de procesamiento
Memoria de trabajo
Sistema operativo
614
616
624
618
Otro código (programas)
622

Fig. 6