(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 398 827**

(51) Int. CI.:

G06F 21/00 (2006.01)
H04L 29/06 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.01.2005 E 05706404 (0)**

(97) Fecha y número de publicación de la concesión europea: **31.10.2012 EP 1803251**

(54) Título: **Método y aparato para proveer autenticación mutua entre una unidad de envío y un receptor**

(30) Prioridad:

18.10.2004 US 967669

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.03.2013

(73) Titular/es:

ENTRUST LIMITED (100.0%)
1000 INNOVATION DRIVE
OTTAWA, ONTARIO K2K 3E7, CA

(72) Inventor/es:

VOICE, CHRISTOPHER BRIAN

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Método y aparato para proveer autenticación mutua entre una unidad de envío y un receptor

Campo de la invención

La invención se relaciona en general con un método y aparato para proveer la autenticación entre un usuario y una fuente objetivo o entidad de envió de información, y más particularmente para métodos y aparatos que emplean señalizaciones de programas o señalizaciones físicas para proveer autenticación mutua entre un usuario y una fuente objetivo.

Antecedentes de la invención

Se conocen sistemas y métodos de autenticación mutua que intentan autenticar un usuario o receptor de información que está siendo provisto por un proveedor de servicios de contenido u otro recurso objetivo que es, por ejemplo, accesible a través de un enlace de comunicación en línea tal como a través de internet, intranet o cualquier otra red de trabajo alámbrica o inalámbrica adecuada. Tales métodos y aparatos intentan evitar intrusiones maliciosas por hackers y otros que intentan robar la identidad de un usuario. Por ejemplo, una entidad maliciosa puede enviar un correo electrónico utilizando la dirección de un banco legítimo y direcciona el receptor a una “sitio de la red falso”. El receptor, creyendo que es un sitio legítimo, puede ser engañado para proveer información tal como número de cuenta y clave de acceso los cuales pueden ser utilizados por la entidad maliciosa para tener acceso a la cuenta en línea del receptor. El problema puede ser particularmente agudo en el mundo del consumidor donde los métodos convencionales de autenticación mutua en línea pueden ser muy complejos, requiriendo típicamente el despliegue de hardware costoso e interacciones complejas con el usuario que hacen que tales técnicas de autenticaciones mutuas sean imprácticas. Como tal, sería deseable proveer un sistema y método que permita la confirmación de usuarios o receptores que estén teniendo acceso a una organización objetivo buscada (por ejemplo, entidad de envió) de una manera relativamente no costosa pero segura.

Se conocen técnicas de autenticación de dos factores que, por ejemplo, utilizan un primer factor de autenticación para autenticar la identidad de un usuario final y un segundo factor que se utiliza para autenticación con el fin de complementar el nombre del usuario y la clave de acceso utilizadas típicamente en el primer factor de autenticación. El concepto de un segundo factor es que un usuario pueda autenticar utilizando algo que ellos conocen (por ejemplo, su clave de acceso) y algo que tienen (por ejemplo, el segundo factor, el cual puede ser, por ejemplo, un señalizador de hardware). Típicamente, los mecanismos del segundo factor están basados en hardware y se distribuyen físicamente al usuario final. Por ejemplo, se conocen señalizadores sincrónicos en tiempo y son denominadas algunas veces como técnicas de autenticación multifactor. Se describen adicionalmente más adelante varias técnicas conocidas.

También, se conocen diversos métodos para llevar a cabo la autenticación de una organización objetivo en relación con las aplicaciones de internet que incluyen, por ejemplo, la autenticación con un servidor de capas de conexión seguras que proveen certificación a partir de una tercera parte de confianza con base en la identidad de la organización que aloja una aplicación de red dada. Sin embargo, esto puede requerir que el usuario lleve a cabo la etapa manual de doble pulsación sobre el icono de la pantalla y lectura de información. El requerimiento de la acción manual frecuentemente persuade de ejecutarla consistentemente y así, socava la efectividad del método. Además, las aplicaciones de conexión de seguridad también son conocida porque involucran la descarga e instalación por parte del usuario de software del lado del cliente lo cual provee una indicación visual de cuando el usuario se está comunicando con el sitio legítimo. Sin embargo, puede ser incómodo para los usuarios finales descargar e instalar software o pasar a través de varias etapas manuales para confirmar la identidad de la organización objetivo.

Además, los métodos de autenticación tanto del usuario como de la organización objetivo pueden ser imprácticos cuando se extienden a otros canales de comunicación tales como los sistemas de respuesta de voz interactivos o comunicación a través de dispositivos móviles, tales como teléfonos celulares, asistentes digitales personales, dispositivos de internet, y otros dispositivos móviles, puesto que pueden basarse sobre métodos de despliegue y entrada de un usuario únicos para las aplicaciones basadas en la red.

Asegurarse de que un mensaje de correo electrónico u otro mensaje electrónico han sido enviado por un originador que puede ser confiable, también denominado como autentico, ayuda a asegurarse contra el robo de información importante por parte de partes inescrupulosas y puede ayudar a limitar la basura y la intrusión. La intrusión es una forma de basura de internet que involucra usualmente el envío masivo de correos electrónicos que parecen provenir de una organización legitima tal como un banco u otra institución financiera u otra organización. Estos correos electrónicos frecuentemente direccionan al receptor a un sitio en la red fraudulento o forma donde es engañado para divulgar información personal o financiera. Un intento de intromisión alternativo puede no preguntar tal información pero, al entrar a la URL, ejecuta una descarga de un programa portador de clave que permite que el intruso recolecte información de la máquina del receptor. La información puede ser utilizada para robo de identidad y fraude.

Los ataque de los intrusos pueden ser costosos y pueden consumir los recurso de una compañía puesto que, por ejemplo un gran número de ataques puede ser revisado contra compañías objetivo en grandes volúmenes y billones de mensajes de intrusión pasan a través de los sistemas de filtro lo cual puede hacer más lento el envío de correos electrónicos, utilizando tiempos de procesamiento valiosos de los servidores y finalmente pueden dar como resultado la pérdida de datos financieros importantes que pasan a manos inescrupulosas.

Se conocen varias soluciones para intentar atacar este problema. Puesto que los ataques de intrusión frecuentemente comienzan con grandes volúmenes de correo electrónico enviados desde una dirección de envió forjada, los esfuerzos para reducir el correo basura pueden de alguna manera ser efectivos en la reducción del número de ataques de intrusión. Por ejemplo, un método denominado *Sender Policy Framework*, un originador de un mensaje o dominio de originador publica en un directorio o cualquier otra forma adecuada de direcciones de ordenador legitimas que son verificadas por los agentes de transferencia del mensaje en recepción. El agente de transferencia del mensaje puede verificar un mensaje recibido a través de un servidor DNS (servidor de nombre de dominio). Sin embargo, está técnica puede requerir la adopción amplia de agentes de transferencia de mensajes capacitados para SPF que pueden ser potencialmente costosos de implementar y desplegar.

Otra técnica denominada *Coordinated Spam Reduction Initiative* requiere de nuevos originadores en el dominio del originador para publicar direcciones de computador de envió legítimo que son verificadas por los agentes de transferencia del mensaje receptor de una manera relativamente similar a la que se describió anteriormente.

Otra técnica requiere dominios para firmar digitalmente correos que son verificados por la gente de transferencia del mensaje receptor a través de servidores DNS. De nuevo, esto puede requerir la adopción amplia de versiones modificadas de agentes de transferencia de mensajes.

Otra técnica utiliza el mismo protocolo S/MIME cuando envía correos firmados individuales o dominios digitalmente que son verificados al recibir agentes de transferencia de mensajes entrantes receptores o clientes de usuarios de correo electrónico. Esto puede requerir características de clientes de correo electrónico especiales o agentes de transferencia de mensajes receptores que no son soportados comúnmente en los clientes de correo electrónico basados en la red.

Otra técnica emplea imágenes secretas que son compartidas entre un enviador y un receptor. Tal como se entiende, una imagen personalizada es enviada por un usuario a un servidor de autenticación. El servidor almacena la imagen enviada por el receptor. El servidor de autenticación puede enviar la imagen personalizada al receptor con un correo electrónico y el usuario al ver la imagen reconoce que es la que el envió. También, durante el ingreso a un sitio, el servidor puede incluir la imagen de la página de ingreso de tal manera que un usuario confía en la página de ingreso cuando el usuario ve su imagen personalizada (véase, por ejemplo, www.passmarksecurity.com). Entre otras desventajas, este sistema parece utilizar la misma imagen para ingresos múltiples hasta que la imagen compartida es cambiada y pueda requerir que el receptor escoja y envié la imagen a un servidor de envió.

Además, son conocidos los otros sistemas que intentan proveer, en vez de autenticación de quién envía, autenticación del receptor. Por ejemplo, la Patente de los Estados Unidos No. 5, 712,627 divulga, entre otras cosas, una tarjeta de identificación emitida que tiene indicios en una de las posiciones direccionales sobre una tarjeta asignada. La tarjeta puede tener filas y columnas con diferentes números, caracteres o símbolos que son direccionables por las filas y columnas. Para determinar si una persona que busca acceso a los datos está autorizada para obtener el acceso requerido, la tarjeta de identificación es distribuida a los usuarios autorizados. Una persona que hace un requerimiento que busca acceso provee los indicios en una o más posiciones direccionables sobre la tarjeta según lo específica un sistema de seguridad. Para notificar a la persona que indicio entrar y enviar, el sistema selecciona indicios de coordenadas conocidas por estar presentes en la tarjeta particular. El receptor de eventos envía los indicios localizados en la dirección enviada por el sistema de seguridad. Si los indicios coinciden con los asignados a la persona que busca acceso se otorga el acceso entonces. Sin embargo, tales sistemas no resuelven el problema con respecto a la intrusión puesto que el sistema provee autenticación de un receptor y no un agente de envió y requiere que la persona que busque acceso se identifique así mismo por el sistema y el sistema requiere la entrada y envió por parte del usuario de información localizada en la tarjeta de seguridad.

También se conocen otros sistemas de autenticación que han sido empleados, por ejemplo, en los sistemas de cifrado/autenticación de numerales militares que emplean tarjetas que son mantenidas por un agente de envió y un receptor. Una transmisión es autenticada por ejemplo utilizando un esquema de autenticación de pregunta y respuesta. Quién envía una transmisión electrónica por ejemplo puede utilizar la tarjeta y seleccionar aleatoriamente una fila y una columna para transmitir los identificadores de fila y columna como pregunta. Para responder, se utilizan los identificadores de fila y columna para buscar una letra alfabética que es comunicada de regreso. Como tal, el agente de envió puede asegurarse de que el receptor está en posesión de una tarjeta. Sin embargo, la autenticación del agente de envío al receptor se hace típicamente repitiendo la misma pregunta y respuesta en reversa, y tanto el agente de envío como el receptor deben estar en posesión de la misma tarjeta de autenticación para alcanzar una autenticación mutua.

Otra técnica también utiliza una tarjeta que incluye filas y columnas de información tanto por parte del agente de envío como del receptor, sin embargo, este esquema de autenticación de transmisión se utiliza para autenticar transmisiones. Por ejemplo, durante la autenticación de una transmisión, se localizan diagráficos de autenticación en columnas de transmisión en la parte posterior de una tarjeta de cifrado y se utilizan para autenticar un agente de envío. Las asignaciones de columnas se hacen por parte de un representante designado tal como el comandante de una unidad. Las asignaciones de columna son conocidas tanto para el agente de envío como para el receptor a priori. Los diagráficos de autenticación de transmisión se utilizan solamente una vez. El primer autenticador no utilizado en la columna asignada se utiliza y se traza una línea a través de ese autenticador para evitar su reutilización. Tales esquemas no utilizan una selección aleatoria de información sobre la tarjeta y no utilizan el envío de información de coordenadas puesto que la información de columnas es conocida a priori. Como tal, solamente la información de autenticación es comunicada de manera evidente. Si el agente de envío envía información de autenticación y es válida según lo determina el receptor, el receptor tacha la información de autenticación de la tarjeta. La siguiente vez que se requiera autenticación, se utilizan entonces la siguiente información de autenticación en la misma columna. Como tal, se utiliza una metodología secuencial y no aleatoria. Sin embargo, si la tarjeta de autenticación de un receptor se pierde o es obtenida por una parte inescrupulosa, sabrían cómo actuar como agente de envío puesto que saben que información de autenticación es la siguiente en la columna puesto que no se utilizan selección aleatoria puesto que la tarjeta tiene marcas sobre sí misma. En este sistema no se envía información de coordenadas puesto que la columna de información utilizada para autenticar un agente de envío es conocida antes por el agente de envío y el receptor. Además, si el receptor no recibe la transmisión del agente de envío, la sincronización entre el agente de envío y el receptor se perdería lo cual podría causar que fallen intentos subsiguientes de autenticación.

También, la seguridad de la información y la seguridad de la identificación del usuario se hacen crecientemente importantes a medida que la tecnología se hace más sofisticada. Por ejemplo, se utilizan esquemas de autenticación multifactor en un intento para eludir hackers o para eludir otros usos inapropiados de la información e identidad del usuario. Por ejemplo, puede utilizarse un esquema de autenticación de dos factores conocido para un receptor o un usuario tal como una clave de acceso o un número de identificación personal (PIN) así como algún tipo de señalización física tal como una tarjeta de banco, tarjeta de crédito, señalizador de clave de acceso u otro señalizador el cual debe estar en posición física de un usuario con el fin de iniciar y completar una transacción en línea. Otro nivel de identificación puede incluir autenticación biométrica que puede incluir el barrido de una huella digital, ojo u otra biometría para verificar de nuevo que el usuario que está intentando obtener acceso a un proceso, dispositivo, aplicación u otros derechos es en efecto el usuario apropiado.

Son conocidas tarjetas de transacción que pueden incluir por ejemplo tarjetas inteligentes, tarjetas basadas en bandas magnéticas, u otras tarjetas de transacción que facilitan las transacciones bancarias, transacciones con tarjetas de crédito u otras transacciones adecuadas. Tal como es conocido en la técnica, se requiere usualmente un número de identificación personal (PIN) además de la posesión de una tarjeta de banco para obtener efectivo de una máquina dispensadora de efectivo o de alguna otra manera llevar a cabo una transacción en línea. Una técnica de autenticación multifactores conocida emplea el uso de un señalizador de hardware tal como una pequeña tarjeta operada por baterías que despliega un número aleatorio que cambia periódicamente y de forma aleatoria sobre una porción de la tarjeta inteligente. Cuando un usuario desea ejecutar una transacción con la tarjeta inteligente, por ejemplo, el usuario entra el número aleatorio que cambia frecuentemente. El servidor de transacción receptor compara el código recibido introducido por el usuario tal como se despliega sobre la tarjeta inteligente con un número correspondiente generado por un generador de fuentes de código. Si el código introducido por el usuario coincide con el número generado por el generador de fuente de códigos, la transacción es aprobada y al usuario se le otorga un derecho particular tal como acceder a una cuenta bancaria, comprar artículos, obtener información, obtener acceso a una página de la red o a otra aplicación de software, o cualquier otro derecho adecuado según se desee. Sin embargo, tales señalizaciones de hardware pueden ser bastantes costosas y son operadas por baterías por lo cual se requiere cambio de la batería y el potencial de una mal función electrónica debido a problemas de humedad o cualquier otro problema relacionado con los circuitos electrónicos.

Otras tarjetas inteligentes que no emplean tales pantallas requieren típicamente de un lector de tarjetas que lean, por ejemplo, una banda magnética. Esto puede ser una restricción cuando el usuario desea ejecutar una transacción en línea pero no está sentado frente a un terminal que contenga o tenga acceso a un lector de banda magnética.

En un campo aparentemente no relacionado, se utilizan tarjetas traslucidas tales como tarjetas prácticas que contienen una imagen como patrón semitransparentes que cuando se evalúan visualmente parecen no contener ninguna información en particular. Sin embargo, cuando la carta traslucida es mantenida frente a una pantalla con un patrón de filtro de fondo correspondiente, la combinación del patrón sobre la tarjeta con el patrón de fondo en la pantalla de despliegue se combinan para presentar un mensaje o palabra reconocible visualmente tal como la palabra “lo siento” o “usted es un ganador”. Estos son mensajes estáticos que no son únicos para cualquier usuario típicamente incluyen solamente un mensaje individual. Tales tarjetas plásticas pueden ser utilizadas por ejemplo para ver si un portador ha ganado un premio. La tarjeta puede ser enviada por correo por ejemplo a miembros de una población. Estos receptores luego van a una página de la red identificada sobre la tarjeta traslucida o de alguna otra forma indicadas en la información de correo para ver si han ganado un premio. Sin embargo, tales tarjetas plásticas no proveen autenticación

de factores múltiples, no son específicas del usuario, no incluyen mensajes múltiples y típicamente incluyen mensajes estáticos.

De acuerdo con lo anterior, existe una necesidad para un método y aparato que supere uno o más de los problemas anteriores. El uno o más de los problemas anteriores son superados con un método de acuerdo con las reivindicaciones 1, 8 y 11 y un dispositivo de acuerdo con las reivindicaciones 16, 20 y 22.

Descripción detallada de los dibujos

La figura 1 es un diagrama de bloque que ilustra un ejemplo de un sistema para proveer de manera segura información de identificación de acuerdo con una realización de la invención;

La figura 2 es un diagrama de flujo que ilustra un ejemplo de un método para proveer de manera segura información de identificación de acuerdo con una realización de la invención;

La figura 3 es un diagrama que ilustra un despliegue adicional del método mostrado en la figura 2;

La figura 4 es un diagrama que ilustra un ejemplo de un miembro de información de identificación segura de acuerdo con una realización de la invención;

La figura 5 es un diagrama que ilustra de manera gráfica un ejemplo de una pantalla de ingreso para facilitar la autenticación de un usuario o para proveer de manera segura información de identificación de acuerdo con una realización de la invención;

La figura 6 ilustra de manera diagramática un ejemplo de un patrón de filtro visual desplegado de acuerdo con una realización de la invención;

La figura 7 ilustra gráficamente un ejemplo de un identificador diseñado identificado visualmente de uno o más identificadores oscurecidos que están localizados sobre un miembro de identificación translúcido de acuerdo con una realización de la invención;

La figura 8 es un diagrama de un sistema para proveer información de identificación de manera segura de acuerdo con una realización de la invención;

La figura 9 es un diagrama de bloques que ilustran en más detalle un ejemplo de un emisor de un miembro de identificación translúcido de acuerdo con una realización de la invención;

Las figuras 10 y 11 ilustran un diagrama de flujo que muestra un ejemplo de un método para proveer de manera segura información de identificación de acuerdo con una realización de la invención;

La figura 12 ilustra un ejemplo de una tarjeta de transacciones que incluye una porción que contiene un miembro de identificación translúcido de acuerdo con una realización de la invención;

La figura 13 ilustra otro ejemplo de una tarjeta de transacciones que contiene un miembro de identificación translúcido de acuerdo con una realización de la invención;

La figura 14 es un diagrama que ilustra un ejemplo de un miembro de información de identificación seguro de acuerdo con otra realización de la invención;

La figura 15 ilustra de manera diagramática un ejemplo de información de identificador oscurecida desplegada de acuerdo con una realización de la invención;

La figura 16 es un diagrama de bloques que ilustra otro ejemplo de un sistema para proveer de manera segura información de identificación de acuerdo con una realización de la invención;

La figura 17 es un diagrama de flujo que ilustra un ejemplo de un método para proveer de manera segura información de identificación de acuerdo con una realización de la invención;

La figura 18 es una ilustración que representa un ejemplo de un artículo, tal como una tarjeta, que puede ser utilizado en un método para proveer autenticación de mensajes electrónicos de acuerdo con una realización de la invención;

La figura 19 ilustra un ejemplo de una tarjeta de transacciones que incluye información de autenticación del agente de envío e información de coordenadas de localización para utilización en el suministro de autenticación de mensajes electrónicos de acuerdo con una realización de la invención;

La figura 20 es un diagrama de flujo que ilustra un ejemplo de un método para proveer autenticación en mensajes electrónicos de acuerdo con una realización de la invención;

La figura 21 es una ilustración gráfica que muestra un ejemplo de un mensaje con información anexa de autenticación del agente de envío e información de coordenadas de localización de acuerdo con una realización de la invención;

La figura 22 es un diagrama de bloque que ilustra un ejemplo de un sistema para proveer autenticación de mensajes electrónicos de acuerdo con una realización de la invención;

La figura 23 es un diagrama de flujo que ilustra un ejemplo de un método para proveer autenticación de mensajes electrónicos de acuerdo con una realización de la invención;

La figura 24 es un diagrama de bloques que ilustra un ejemplo de un sistema para proveer autenticación mutua entre un usuario y un recurso objetivo de acuerdo con una realización de la invención;

La figura 25 es un diagrama de flujo que ilustra un ejemplo de un método para proveer autenticación mutua entre un usuario y un recurso objetivo de acuerdo con una realización de la invención;

La figura 26 es un diagrama de flujo que ilustra un ejemplo de otra realización de un método que provee autenticación mutua entre un usuario y un recurso objetivo de acuerdo con una realización de la invención;

La figura 27 es un diagrama de flujo que ilustra otro ejemplo de un método para proveer la autenticación mutua entre un usuario y un recurso objetivo de acuerdo con una realización de la invención; y

La figura 28 es un diagrama de bloque que ilustra un ejemplo de un dispositivo para proveer autenticación mutua entre un usuario y un recurso objetivo en la forma de una representación diagramática, de acuerdo con una realización de la invención.

Descripción detallada de una realización preferida de la invención

En resumen, un método para proveer una autenticación mutua entre un usuario y una unidad de envío (esto es, recurso objetivo) en una realización, incluye la determinación, por parte de un usuario a quien se ha asignado un artículo, tal como una tarjeta u otro artículo adecuado que tiene indicios sobre sí mismo, información de autenticación deseada de la gente de envío que corresponde con información de autenticación real del agente de envío que está incorporada en el artículo. La información de autenticación del agente de envío puede ser localizada sobre el artículo utilizando la información de localización provista por la unidad de envío en una pregunta. El método incluye determinar para el usuario, información de identificación correspondiente al artículo, tal como un número de serie que ha sido asignado al artículo, o un secreto compartido, y enviar una pregunta al usuario en donde la pregunta incluya al menos información de localización, para permitir que el usuario identifique la información de autenticación del agente del envío deseado localizada sobre el artículo, y el envío de la información de identificación del artículo. El usuario recibe entonces la información de localización y la información de identificación del artículo y utiliza la información de identificación del artículo como información de autenticación que indica que el agente de envío que ha enviado la información es confiable puesto que el artículo que está en la posesión del usuario también incluye la información de identificación del artículo sobre sí mismo. El usuario utiliza entonces la información de localización que ha sido enviada al dispositivo del usuario, para determinar por ejemplo la información de autenticación del agente de envío deseada correspondiente que está localizada sobre el artículo, tal como una información de columnas y filas enviada por el recurso objetivo y envía una respuesta a la pregunta de regreso al recurso objetivo (esto es, la unidad de envío). El agente de envío autentica entonces el usuario con base en la respuesta a la pregunta. La respuesta incluye información de autenticación del usuario obtenida del artículo a saber la información de autenticación del agente de envío deseada. Si la información de autenticación del agente de envío recibida enviada por el dispositivo del usuario (y obtenida del artículo), con base en la información de localización, coincide con la información de autenticación del agente de envío deseada, el recurso objetivo otorga entonces un acceso adecuado al usuario (esto es, al dispositivo del usuario) como tal, la información de identificación del artículo es enviada junto con la información de localización por un agente de envío después, por ejemplo, después de que se ha determinado como exitoso un primer nivel de autenticación. El primer nivel de autenticación puede incluir, por ejemplo, que el usuario envié una clave de acceso y una identificación de usuario al recurso objetivo en una etapa inicial de un procedimiento de ingreso, tal como se conoce en la técnica, después de lo cual el envío de la información de localización y la información del identificador de artículo es enviada subsecuentemente con base en un primer proceso de factor de autenticación exitoso.

En otro ejemplo, un método para proveer información mutua no requiere el envío de la información de identificación del artículo del usuario, sino que en vez de ello solamente se requiere el envío de información de localización para permitir que el usuario identifique la información de autenticación correspondiente sobre el artículo y envié una respuesta de vuelta al recurso objetivo para verificación. Sin embargo, en esta realización, la respuesta no incluye la información de autenticación de recurso objetivo esperada tal como es esperada por la unidad de envío, el método incluye repetir la misma pregunta para el usuario que incluye la misma información de localización que fue enviada previamente. Este proceso se repite, por ejemplo, en cada sesión sucesiva, hasta que el usuario envíe la información de autenticación de fuente objetivo apropiada que fue derivada del artículo con base en la información de localización enviada en la pregunta.

Además, también se divulgan dispositivos adecuados que llevan a cabo los métodos anteriores. También, se emplea una combinación de los dos métodos para efectuar un tipo de proceso de autenticación mutuo reforzado.

También se divulga un método para proveer autenticación de mensajes electrónicos que emplea un artículo (también denominado como miembro o señalizador), tal como una tarjeta, adhesivo, o cualquier otro artículos adecuado, que incluye información de autenticación del agente de envío e información de localización, tal como encabezamiento de filas y columnas. En un ejemplo, a cada receptor de interés se emite un artículo que incorpora información de autenticación del agente de envío que es identificable mediante la información de localización correspondiente tal como identificadores de columna y fila. Cuando el agente de envío de un mensaje electrónico quiere enviar un mensaje a un receptor de interés, el agente de envío envía el mensaje electrónico y la información de localización y la correspondiente información de autenticación del agente de envío localizada en la localización identificada por la información de localización. Esto incluye datos que representan la localización e información de autenticación (tal como un índice a, una referencia a la información de localización o información de autenticación misma, o cualquier representación adecuada de los mismos). Por lo tanto el receptor puede, en una realización, buscar en su artículo (por ejemplo, tarjeta) en la localización correspondiente y ver si la información de autenticación de envío deseada coincide con la información de autenticación de envío localizada sobre el artículo (también denominada como información de autenticación esperada por el agente de envío). Si se presenta la coincidencia, entonces el receptor confía en el agente de envío del mensaje. El receptor no necesita enviar ninguna información al agente de envío. Como tal, una tarjeta individual u otro artículo puede ser utilizado para autenticar al agente de envío de un mensaje para eludir intrusiones, u otros problemas de autenticación del agente de envío. Otros ejemplos serán reconocidos por una persona experimentada en la técnica.

Además, también se divulga un sistema para proveer autenticación de mensajes electrónicos que ejecuta la metodología anterior, y también se divulga una tarjeta de transacción que incluya la información de localización y la información de autenticación del agente de envío en la misma en la forma de un adhesivo o como una parte de la tarjeta de transacción misma. En aún otra realización, el artículo puede ser un artículo translúcido que permite que la luz pase a través del mismo de tal manera que puede enviarse un patrón de filtro visual y una información de autenticación del agente de envío por un agente de envío junto con el mensaje. Un usuario puede sostener el artículo frente a una pantalla de despliegue y superponerlo sobre el patrón de filtración visual enviada por el agente de envío. Si la información de autenticación del agente de envío resultante coincide con los resultados enviados en el mensaje, el receptor puede confiar en el agente de envío del mensaje.

En otra realización, un aparato y método para proveer información de identificación de manera segura genera uno o más usuarios oscurecidos (por ejemplo, receptores) con identificadores para un receptor, de tal manera que se genera una pluralidad de identificadores con base en los datos secretos del usuario tales como clave de acceso, número de identificación personal u otra información o identificadores secretos o no secretos que no están basados en los datos secretos del usuario, tales como una generación aleatoriamente generada del identificador y luego asociada con el usuario. En este caso, se utiliza información no relacionada con el usuario, pero el identificador puede aún identificar al usuario. En otra realización, puede utilizarse un identificador oscurecido individual.

En una realización, el método y aparato genera un miembro de identificación translúcido (TIDM), tal como una porción de, o una tarjeta plástica, lámina, película u otro miembro adecuado enteros que tengan un área traslucida que incluye el uno o más identificadores oscurecidos. Tal como se utiliza aquí, el área traslucida puede incluir también un área trasparente. Por ejemplo, el miembro de identificación translúcido puede ser hecho de láminas trasparentes o claras, incluyendo plástico ahumado u otra coloración adecuada con los identificadores oscurecidos (incluyendo información no característica) impresos en tinta o colocados de alguna otra manera sobre o en la misma. El uno o más identificadores oscurecidos pueden ser por ejemplo identificadores de autenticación de una vez que son únicos para un receptor del miembro de identificación translúcido. Como tal, el miembro o tarjeta de identificación translúcidos contienen lo que parece ser visualmente un patrón aleatorio de información.

También se genera un patrón de filtración visual correspondiente para despliegue sobre un dispositivo de pantalla cuando el usuario desea utilizar el miembro de identificación translúcido. Por ejemplo, el patrón de filtro visual también parece ser aleatorio desde un punto de vista visual pero cuando se combina visualmente con uno o más identificadores oscurecidos sobre el miembro de identificación translúcido, se revela visualmente uno de los uno o más identificadores oscurecidos designados. En una realización, un usuario puede superponer el miembro de identificación translúcido sobre una porción designada de un dispositivo de presentación o en la porción designada de una pantalla que despliega

el patrón de filtro visual. Una combinación del patrón de filtro visual con el patrón de identificadores oscurecidos diferentes sobre el miembro de identificación traslucida se combinan para formar un identificador o mensaje individual revelado del uno o más identificadores. Por lo tanto, por ejemplo en una realización, se genera un patrón aleatorio aparentemente sobre una pantalla que solamente se expone un identificador individual visualmente a un usuario que está observando el miembro de identificación translúcido el cual está superpuesto sobre el patrón de filtración visual que está siendo desplegado sobre la pantalla.

De acuerdo con lo anterior, si se desea, un oficial de seguridad que tenga acceso, por ejemplo, a un emisor de miembros de identificación traslucida puede usar un paquete de tarjetas de celofán en blanco para hacer los miembros de identificación translúcidos en una impresora local. Los miembros de identificación translúcidos pueden ser impresos con un patrón de color translúcido que sirve como uno o más identificadores oscurecidos, obtener otros indicios adecuados que parezcan ser semialeatorios u oscurecidos para un usuario. El uso de color o fondo de color también puede ser utilizado para prevenir ataques por fotocopiado. Se reconocerá que porciones de o todas las funciones del emisor del miembro de identificación traslucida pueden proveerse a través de una distribución de suministradores y redes o a través de un servicio basado en la red. Por ejemplo, un receptor puede tener acceso a un servicio de emisión de TIDM a través de una conexión de la red y a imprimir localmente el TIDM o recibir el TIDM a través del correo. También, los identificadores pueden ser provistos por una parte y enviados a otra parte para impresión o manufactura. También puede emplearse otra distribución de operaciones según se desee.

Una vez se presente un identificador revelado visualmente a un usuario, un usuario entra al identificador revelado visualmente a través de una interfaz de usuario en donde se compara con un identificador esperado. Si el identificador introducido coincide con el identificador esperado, se indica una autenticación apropiada y al receptor se le puede garantizar el acceso a un dispositivo, aplicación o proceso u otros derechos deseados (o se aceptan los datos enviados, por ejemplo, tales como un voto). Además, también puede mantenerse una lista de miembros de identificación translúcidos revocados para evitar el compromiso debido a robo o pérdida de miembros de identificación translúcidos. La lista puede ser almacenada en cualquier localización adecuada y actualizada por un proveedor de servicios, emisor de miembros de identificación traslucida o cualquier entidad adecuada. Puesto que los miembros de identificación traslucida no requieren electrónica para generar números aleatorios, el coste de tales miembros de identificación traslucida puede ser bastante baja y su confiabilidad puede ser también relativamente alta puesto que no son susceptibles de daño por humedad u otros daños típicamente asociados con las tarjetas inteligentes.

En una realización alternativa, una tarjeta inteligente u otra tarjeta de transacción o tarjeta de no transacciones (por ejemplo, tarjeta de voto u otra tarjeta adecuada) pueden incluir un miembro de identificación traslucida si se desea. Por lo tanto se divulga una tarjeta de transacción e incluye por ejemplo una porción que contiene información de identificación de la tarjeta (tal como un número de tarjeta de transacción, el cual puede ser impreso sobre la misma tal como por ejemplo mediante impresión en relieve o electrónicamente a través de cualquier otro mecanismo de almacenamiento adecuado tal como una banda magnética o cualquier otro mecanismo adecuado), así como una porción que contiene un miembro de identificación traslucida que tiene un área traslucida que incluye uno o más identificadores oscurecidos. Como tales tarjetas de transacción tales como tarjetas de crédito, tarjetas de banco, o cualquier otra tarjeta de transacción pueden incluir una ventana que contenga el miembro de identificación translúcido o puede tener un número de identificación de transacción u otra información de identificación fijada a una tarjeta de transacción convencional para aumentar la seguridad.

En otra realización, el papel del miembro de identificación translúcido y la unidad receptora son reversados. Por ejemplo, en esta realización, el miembro de identificación translúcido contiene el patrón de filtración visual y la pantalla de presentación despliega al menos un identificador oscurecido que puede ser por ejemplo datos de identificación que representan el usuario que son únicos para un usuario, u otros datos si se desea. La combinación de superponer el miembro de identificación translúcido (filtro visual) sobre la pantalla que despliega un identificador oscurecido, revela (desoscurece) en al menos un identificador oscurecido sobre la pantalla. El patrón de filtración visual sobre el miembro permanece igual puesto que está impreso sobre el miembro, y el identificador oscurecido desplegado cambia durante cada sesión o en otros intervalos adecuados.

De acuerdo con lo anterior, puede dar como resultado una o más de las siguientes ventajas. Puesto que los miembros de identificación translúcidos pueden ser impresos por un oficial de seguridad de la organización, no se incurre en costes de manufactura y pueden ser generados localmente para un receptor. Puesto que no hay necesidad de que sea electrónico, no hay baterías para reemplazar y no ocurren daños por exposición a la humedad. No se requiere conectividad en red o de radio tal como los dispositivos requeridos típicamente que emplean bandas magnéticas. El miembro de identificación translúcido puede ser hecho de plástico o cualquier otro material adecuado y en cualquier espesor adecuado. Son durables y fáciles de reemplazar en el evento de un riesgo cuando pueden ser producidos localmente para una organización. También puede evitarse una inversión sustancial en una estructura de red para generar continuamente códigos maestros que coincidan con los códigos que cambian dinámicamente sobre una pantalla y una tarjeta inteligente.

En una realización, el patrón de filtración visual desplegado ilumina selectivamente una porción de un miembro de identificación translúcido para revelar visualmente uno de los uno o más identificadores oscurecidos. El patrón de

filtración visual puede ser cambiado con cada sesión de autenticación. El uno o más identificadores oscurecidos son indicios impresos sobre una tarjeta semitransparente (o transparente) y es preferiblemente único dentro de un dominio particular de usuarios. Los uno o más identificadores oscurecidos son oscurecidos visualmente a través de muchas técnicas adecuadas tales como matices de color, ordenamiento de los caracteres, una combinación de los mismos o cualquier otra técnica de ofuscación visual adecuada. La figura 1 ilustra un ejemplo de un sistema 10 para proveer con seguridad información de identificación que incluye un emisor de miembros de identificación translúcido 12 operativo para generar un miembro de identificación segura, tal como un miembro de identificación translúcido 14, un generador de filtro visual 16, un módulo de autenticación del miembro de identificación translúcido 18, una unidad receptora 20 y una memoria 22. En este ejemplo, el generador de filtro visual 16 y el módulo de autenticación de miembro de identificación translúcido 18 se incluyen como parte del autenticador de miembro de identificación translúcido 24 que puede ser implementado como uno o más módulos de software que se ejecutan sobre una unidad de ordenador tal como un ordenador personal, estación de trabajo, servidor, dispositivo portátil, o cualquier otro dispositivo o dispositivos múltiples conectados en red adecuados. El autenticador de miembro de identificación translúcido 24 está acoplado operativamente, en este ejemplo, a un servidor de red el cual a su vez está acoplado operativamente a una red tal como el internet 26 para facilitar a la comunicación basada en la red entre una unidad receptora 20 y un autenticador de miembro de identificación translúcido 24. Como tal, se forman circuitos múltiples mediante el software y el dispositivo de procesamiento. También, tal como se utilizan aquí, circuitos se refieren también a cualquier sistema de programa electrónico adecuado en cualquier forma adecuada incluyendo pero no limitándose a hardware (microprocesadores), programas discretos, máquinas de estado, procesadores de señales digitales, etc.), software, firmware o cualquier combinación adecuada de los anteriores.

El emisor de miembros de identificación translúcidos 12, el generador de filtro visual 16, y el módulo de autenticación de miembro de identificación translúcido 18 pueden ser implementados de cualquier manera adecuada y es preferiblemente, pero no limitándose a, módulos de software que se ejecutan sobre uno o más dispositivos de computación que contienen uno o más dispositivos de procesamiento que ejecutan instrucciones que son almacenadas en la memoria.

En este ejemplo, el emisor de miembros de identificación translúcidos 12 será descrito como un servidor local que genera el miembro de identificación translúcido 14 que utilizan una impresora u otro mecanismo adecuado para generar un miembro de identificación translúcido 14. El miembro de identificación translúcido incluye un área traslucida que incluye una o más identificadores oscurecidos en la misma. Sin embargo, se reconocerá que el emisor de miembro de identificación translúcido 12 pueden ser incluido como parte del autenticador de miembros de identificación translúcidos 24, o puede ser localizado en cualquier otro dispositivo adecuado incluyendo un servidor de red y será reconocido que cualquier programa de software descrito aquí puede ser localizado adecuadamente sobre cualquier dispositivo o dispositivos adecuados también.

La memoria 22 puede ser cualquier memoria local o distribuida adecuada y puede estar localizada sobre el servidor en red o localmente si se desea. La memoria puede ser RAM, ROM o cualquier tecnología de memoria adecuada. La unidad receptora 20 puede ser cualquier dispositivo adecuado tal como un ordenador portátil, un ordenador de mesa, un dispositivo portátil o cualquier otro dispositivo adecuado que incluye una pantalla 30 y una interfaz de usuario, y puede incluir uno o más dispositivos de procesamiento que ejecuten las instrucciones almacenadas en cualquier memoria adecuada. El dispositivo receptor incluye la circuitería requerida para proveer una o más interfaces tales como interfaces gráficas de usuario a través de buscadores en la red u otras aplicaciones o sistemas operativos y pueden incluir interfaces de reconocimiento de voz o cualquier interfaz de entrada de usuario adecuada. Como tal las unidades incluyen un circuito de despliegue operativo para presentar un patrón de filtración visual definido de tal manera que cuando el patrón de filtración visual se combina visualmente con uno o más identificadores oscurecidos localizados sobre un miembro de identificación traslucida, uno de los uno o más identificadores designados se revela visualmente; y una interfaz de entrada operativa para recibir datos que representan un identificador revelado visualmente. En un ejemplo, una interfaz de usuario se utiliza para requerir entrada de un número de serie asociado con el miembro de identificación translúcido; y una solicitud de entrada del identificador revelado para determinar si se otorga o no un derecho deseado para el receptor.

También si se desea, una unidad receptora puede recibir los identificadores de filtro u oscurecidos para desplegar sobre una pantalla y enviar la respuesta de regreso a través de un dispositivo completamente diferente (o a través de un canal completamente diferente) tal como un teléfono celular, por mensaje SMS, mensaje de correo electrónico o cualquier otro canal y/o dispositivo adecuado.

Con referencia también a las figuras 2 y 3, se describirá un método para proveer con seguridad información de identificación. Como se muestra en el bloque 200, un receptor envía una solicitud al emisor de miembros de identificación translúcido 12 a través de internet o a través de cualquier otro mecanismo adecuado para solicitar la emisión de un miembro de identificación translúcido 14. Esto puede hacerse por ejemplo mediante un receptor que se registra con una institución financiera en línea con datos suministrados por el usuario tales como una clave de acceso u otra información secreta. Esto se muestra como una información específica del receptor 32 que es recibida por el emisor del miembro de identificación translúcido 12.

Como se muestra en el bloque 202, el método incluye generar uno o más identificadores oscurecidos para un receptor, los cuales pueden basarse, por ejemplo, en información específica del receptor 32 y/u otra información 34. La otra información 34 puede ser un número de serie de miembro de identificación translúcido u otra información adecuada si se desea. Esto puede hacerse por ejemplo mediante el emisor del miembro de identificación translúcido 12, o cualquier otra entidad adecuada. Como se muestra en el bloque 204, el método incluye generar el miembro de identificación translúcido 14 que tiene un área traslucida 36 que incluye uno o más identificadores oscurecidos 38. El uno o más identificadores oscurecidos 38 son generados por el emisor de miembro de identificación translúcido 12 en este ejemplo y almacenados en la memoria 22 en forma de base de datos. El uno o más identificadores oscurecidos se almacenan en la memoria 22 de tal manera que se pueda tener acceso a ellos subsecuentemente cuando se hace necesario crear patrones visuales apropiados 40 para revelar el identificador revelado deseado 700 o cuando se verifica el identificador revelado retornado 700.

Por ejemplo, el emisor de miembros de identificación translúcidos 12 puede controlar una impresora para imprimir una tarjeta de celofán como un miembro de identificación translúcido 14 que tiene impreso sobre sí uno o más identificadores oscurecidos. Un ejemplo de un miembro de identificación translúcido se muestra en la figura 4. El miembro de identificación translúcido 14 puede ser hecho de cualquier material adecuado tal como plástico u otro material adecuado que provea algún nivel de transparencia de tal manera que una combinación del uno o más identificadores oscurecidos cuando se superponen sobre una pantalla que emite luz, permite que la energía lumínica (o la falta de energía lumínica) de la pantalla se combine con uno o más identificadores oscurecidos para designar visualmente uno de los uno o más identificadores sobre un miembro de identificación translúcido. El uno o más identificadores sobre un miembro de identificación translúcido puede ser también una pluralidad de diferentes identificadores oscurecidos.

El miembro de identificación translúcido 14 puede ser una tarjeta, lámina, película u otro miembro que pueda incluir si se desea cualquier adhesivo o estructura de conexión para ser aplicado sobre una ventana de una tarjeta de transacción o cualquier otro material adecuado. El miembro de identificación translúcido también puede ser conectado a una tarjeta de transacción, tal como, por ejemplo, utilizando una estructura de conexión adecuada para unir el miembro de identificación translúcido con un extremo o lado de la tarjeta de transacción. Los uno o más identificadores oscurecidos 38 que se imprimen sobre el miembro de identificación translúcido 38, como se anotó anteriormente, pueden ser caracteres (por ejemplo ASCII), símbolos, patrones de impresión, versiones coloreadas de los mismos o cualquier otro indicio adecuado. Los uno o más identificadores oscurecidos 38 parecen ser oscurecidos visualmente y por lo tanto aparentemente aleatorios cuando son observados por un receptor. En otras realizaciones puede ser deseable imprimir patrones de tinta que no conlleven caracteres sino en vez de ellos representen visualmente un mensaje u otra información de tal manera que cuando se superponen sobre la parte superior de una pantalla el patrón generado por la pantalla en combinación con la imagen impresa permita que el observador descifre visualmente un identificador revelado.

El área traslucida 36 incluye un patrón de información que representa uno o más identificadores que pueden ser información de identificación única que puede ser utilizada para una o más sesiones de autenticación u otros propósitos. El patrón de información representado por uno o más identificadores oscurecidos es preferiblemente único para un dominio dado de usuarios para reducir la probabilidad de que el mismo usuario obtenga un mismo miembro de identificación translúcido con los mismos identificadores oscurecidos. El área traslucida 36 se configura (por ejemplo se dimensiona) para superponerse al menos a una porción de la pantalla de despegue 30 sobre la unidad receptora 20. En una realización, cada uno de los uno o más identificadores oscurecidos pueden servir como identificadores de autenticación una vez para el receptor del miembro de identificación translúcido. Hay que anotar, tal como se utiliza aquí, que la información de identificación incluye cualquier información utilizada para autenticar directa o indirectamente a un usuario (por ejemplo, un receptor TIDM) u otros procesos de interés, o para obtener acceso a un derecho deseado asociado con un proceso o dispositivo, o cualquier otra información adecuada que pretenda ser mantenida en secreto excepto en el momento de que se va a efectuar una transacción.

Para hacer el TIDM, el método puede incluir la recepción de una solicitud por parte de un usuario para uno o más identificadores oscurecidos y registrar un enlace entre el usuario y la información de identificación asociada con el uno o más identificadores de usuario oscurecidos. El método puede incluir proveer en uno o más identificadores de usuarios oscurecidos al usuario en donde el uno o más identificadores de usuario oscurecidos están sobre un miembro de identificación translúcido que es enviado al usuario, el uno o más identificadores de usuario oscurecidos han enviado una tercera parte para ser colocado sobre un miembro de identificación translúcido para el usuario, el uno o más identificadores de usuario oscurecidos que son enviados al usuario para colocación sobre un miembro de identificación translúcido, y el uno o más identificadores de usuario oscurecidos son seleccionados de una reserva preexistente de identificadores de usuario oscurecidos. La solicitud del usuario puede incluir información específica del usuario y la información específica del usuario puede ser utilizada para crear el uno o más identificadores oscurecidos o puede ser combinada con otra información para producir el uno o más identificadores de usuario oscurecidos.

Como se muestra en el bloque 206, una vez que el miembro de identificación translúcido 14 ha sido generado y provisto a un receptor, el generador de filtración visual 16, u otro mecanismo adecuado genera un patrón de filtración visual para desplegar sobre la pantalla 30 del dispositivo del receptor. Cuando el patrón de filtración visual 40 es desplegado por el

dispositivo receptor, el patrón de filtración visual se combina visualmente con el uno o más identificadores oscurecidos localizados sobre el miembro de identificación translúcido 14 para designar uno de los uno o más identificadores. En otras palabras, el patrón de filtración visual elimina por filtración identificadores indeseados para revelar uno seleccionado de los uno o más identificadores.

Como se muestra en el bloque 208, el método puede incluir la superposición, tal como por parte de un receptor, o un dispositivo, de número de identificación translúcido visual 14 sobre el patrón de filtración desplegado 40 para identificar visualmente uno designado de los identificadores oscurecidos sobre el miembro de identificación translúcido 40. El identificador identificado visualmente es introducido entonces por el receptor para facilitar una transacción u obtener acceso a un derecho deseado específico asociado con cualquier proceso o dispositivo de interés.

Como se muestra de nuevo en la figura 3, las etapas de la figura 2 se presentan en más detalle. Como se muestra en el bloque 300, la generación de uno o más identificadores oscurecidos para un receptor puede hacerse por ejemplo mediante el emisor de miembros de identificación translúcido 12 o cualquier otra entidad adecuada obteniendo información específica del receptor, tal como datos secretos o no secretos o información relacionada con no usuarios. Este proceso puede ser logrado utilizando material que no pertenece a usuarios o suministrado por no usuarios, en cuyo caso, los uno o más identificadores oscurecidos son asociados subsecuentemente con un usuario. Cuando se utiliza información es específica del receptor, esta puede ser un número de identificación personal, clave de acceso, nombre de usuario, número de cuenta u otros datos provistos por el receptor a través de la unidad receptora 20 o de cualquiera otra fuente adecuada. Esto se indica como información específica del receptor 32. Como se muestra en el bloque 302, la información específica del receptor 32 se combina adecuadamente, tal como a través de una función matemática adecuada o algoritmo, para producir uno o más identificadores oscurecidos 38. La otra información 34 puede ser, por ejemplo, generada a partir de un generador de números aleatorios, el número de serial del miembro de identificación translúcido real 44 (u otra información de identificación TIDM) que puede ser impresa sobre el miembro de identificación traslucida 14 o almacenado por el emisor de miembro de identificación translúcido 12, o cualquier otra información adecuada. Tal como se muestra en el bloque 204, un número de serie de un miembro de identificación traslucida, o cualquier otra información adecuada para identificar el miembro de identificación translúcido, se asigna a la zona oscurecida o más identificadores 38. Se reconocerá que mediante una solicitud inicial o generación de un miembro de identificación translúcido que el emisor del miembro de identificación translúcido 12 puede seleccionar un número de serie de un miembro de identificación translúcido y asociarlo con la información específica del receptor 32. Esta información puede ser combinada para generar el uno o más identificadores oscurecidos 38. El número de serial de miembro de identificación translúcido 44 puede ser almacenado en la memoria 22 para uso posterior por parte del autenticador del miembro de identificación translúcido 24 (que autentica un receptor utilizando el miembro de identificación translúcido 14). El orden de las etapas tal como se describe aquí con respecto a cualquier método puede ser reorganizado adecuadamente con base en el resultado deseado.

Como se muestra en el bloque 306, la generación del miembro de identificación translúcido 14 puede incluir la impresión de los diferentes identificadores oscurecidos en un formato deseado sobre una película, lámina o tarjeta plástica para producir el miembro de identificación translúcido 14. Como se muestra en el bloque 308, la presentación del patrón de filtración 40 sobre una pantalla puede incluir la selección aleatoria, a partir de los identificadores oscurecidos, de un identificador seleccionado para producir un patrón de filtración visual 40 sobre la pantalla 30 que revela el seleccionado de los identificadores oscurecidos como el identificador que debe ser revelado cuando el miembro de identificación translúcido 14 es superpuesto al patrón de filtración visual 40.

Como se muestra en las figuras 4 a 7, y para ilustrar adicionalmente un ejemplo, como se muestra en la figura 4, el miembro de identificación translúcido 14 tiene impreso sobre sí el número de serie de miembro de identificación translúcido 44 u otra información de identificación y el uno o más identificadores 38 impresos en el área traslucida 36. Como se anotó anteriormente esta puede ser impresa sobre un material de celofán u otro material que sea aceptado fácilmente por las impresoras convencionales, si se desea, para reducir costes de fabricación. Sin embargo puede utilizarse cualquier material o proceso de manufactura adecuados. Una vez que el receptor está en posesión del miembro de identificación translúcido 14, se provee autenticación multifactor utilizando el miembro de identificación translúcido 14.

Puede generarse un filtro de cualquier manera adecuada. Por ejemplo, puede escogerse un identificador oscurecido seleccionado del uno o más identificadores oscurecidos almacenados cuya posición en el TIDM está definida. El generador del patrón de filtro visual 16 produce un patrón de filtración basado en una superposición predefinida del TIDM para asegurar que el filtro bloquea las localizaciones de caracteres apropiadas. Puede utilizarse cualquier otra técnica adecuada.

Como se muestra en la figura 5, el dispositivo receptor 20 puede desplegar, a través de un navegador en la red u otra interfaz de usuario adecuada, una pantalla de entrada, con base en una página HTML recibida si se está utilizando un navegador de red, que contiene campos que reciben entradas de usuario tales como un campo de identificador de usuario 500, un campo de acceso 502 y número de serie de campo del miembro de identificación translúcido 44. El usuario envía la información introducida a través de botones de interface adecuados 504. Esta información es enviada entonces al servidor de la red a través de internet y si se desea puede ser reenviada al autenticador del miembro de

identificación translúcido 24. Como se muestra en este ejemplo la información introducida en el campo de identificación del usuario 500 o en el campo de clave de acceso 502 puede considerarse como información específica del receptor 32 que fue introducida previamente cuando el emisor del miembro de identificación translúcido 12 genero inicialmente el miembro de identificación translúcido 14.

La figura 6 ilustra un ejemplo de una interfaz gráfica de usuario (generada con base en una página HTML recibida) desplegados sobre una pantalla 30 para facilitar proveer de manera segura la información de identificación utilizando el miembro de identificación translúcido 14. La interfaz gráfica de usuario puede ser generada por ejemplo a través de un navegador en la red y un procesado huésped adecuado sobre la unidad receptora o cualquier otro procesador adecuado, e indica un área de superposición 600 que puede ser del mismo tamaño o de un tamaño diferente que un patrón de filtración visual 40 que se presenta en la pantalla 30. Por lo tanto en respuesta a la pantalla de ingreso en la figura 5, el autenticador del miembro de identificación translúcido 24 envía una respuesta que contiene el patrón de filtración visual 40 y la pantalla de interfaz de respuesta mostrada en la figura 6. La unidad receptora 20 despliega el patrón de filtración visual 40 y un campo de identificador revelado 602 para permitir la entrada de la identificación revelada del uno o más identificadores oscurecidos.

La figura 7 ilustra gráficamente la condición donde el miembro de identificación translúcido 14 esta superpuesto sobre la parte superior del patrón de filtración visual 40 para revelar uno de los uno o más identificadores oscurecidos. El usuario posiciona el miembro de identificación translúcido 14 y por lo tanto el uno o más identificadores oscurecidos impresos 38 sobre el patrón de filtración visual 40 y la combinación del patrón de filtración visual 40 y los identificadores oscurecidos impresos diferentes 38 revelan en este ejemplo un identificador revelado 700 el cual es introducido por el receptor en el campo del identificador 602 revelado. El usuario envía entonces el identificador 700 revelado al autenticador de miembros de identificación translúcido 24 para autenticar el usuario para la transacción particular o para acceso a un derecho particular. De acuerdo con lo anterior, el autenticador del miembro de identificación translúcido 24 recibe datos que representan el identificador revelado 700 en respuesta a un usuario u otra entidad que se superpone al miembro de identificación translúcido 14 sobre la pantalla 30. El módulo de autenticación del miembro de identificación translúcido 18 compara el identificador revelado recibido 700 con un identificador esperado correspondiente 702 (véase figura 1) para determinar si es apropiada una autenticación apropiada del receptor. El módulo de autenticación del miembro de identificación translúcido 18 contiene el identificador 702 correspondiente esperado de la memoria 22 se puede generar el identificador esperado sobre la marcha conociendo el patrón de filtro visual y teniendo acceso a los identificadores oscurecidos 38, o puede obtener el identificador esperado 702 en cualquier otra forma apropiada.

Con referencia a las figura 8 y 9 la emisión de un miembro de identificación translúcido 14 se describirá en más detalle a manera de una realización de ejemplo. Con el fin de obtener un miembro de identificación translúcido 14, un receptor se registra con un banco en línea o en otra institución utilizando información específica del usuario 32, tal como un número de cuenta u otra información según lo indique el requerimiento de registro 800. Este requerimiento se pasa luego a través de un servidor de red 802. El servidor de red 802 comunica entonces con un servidor de banco 804 el cual incluye por ejemplo un sistema de manejo de clientes y un solicitador de miembros de identificación translúcidos 806 que puede ser una aplicación de software adecuado que se ejecuta sobre un dispositivo de procesamiento si se desea o cualquier otra estructura adecuada. El servidor de banco 804 genera entonces una solicitud de emisión de miembro de identificación translúcido 808 al emisor de miembros de identificación translúcido 12 que puede estar incluido en o separado de un servidor adecuado 810. La solicitud de emisión del miembro de identificación translúcido 808 incluye la información específica del receptor 32 introducida por el usuario. En respuesta, el emisor de miembro de identificación translúcido 12 provee los identificadores oscurecidos 38 en un mensaje de respuesta 810 y registra un número de serial del miembro de identificación translúcido 44 en la memoria 22 junto con los identificadores 38 oscurecidos asociados que aparecerán sobre el miembro de identificación traslucida 14 para el receptor que lo solicita. En este ejemplo, el servidor de banco 804 enlaza la cuenta del receptor con el número de serial del miembro de identificación translúcido 44 y luego almacena la información enlazada en una base de datos 810 para uso posterior. El servidor de banco 804 genera entonces el miembro de identificación translúcido 14, por ejemplo, formateando los identificadores oscurecidos 38 para impresión y enviando la información a una impresora 814 u otro dispositivo que imprime entonces o manufactura el miembro de identificación translúcido 14. Aquí el número de serial del miembro de identificación translúcido 44 es designado por el emisor del miembro de identificación translúcido 12 y está asociado (por ejemplo, enlazado) con uno o más identificadores oscurecidos 38 y con el usuario en la memoria 22 en una base de datos.

El emisor del miembro de identificación translúcido 12 puede incluir cualquier aleatorizador 900 de información y un formateador del miembro de identificación translúcido 902. El aleatorizador de información 900 puede utilizar el número de serial del miembro de identificación translúcido 44 como otra información 34 para ser combinada con la información específica del receptor 32 para generar el uno o más identificadores oscurecidos 38. Esto puede hacerse utilizando un algoritmo hash u otra técnica de codificación adecuada según se desee para generar uno o más identificadores oscurecidos 38. El formateador 902 del miembro de identificación translúcido puede ser otra aplicación de software que se ejecuta sobre un dispositivo de procesamiento adecuado o dispositivo que de formato a la información para dar salida hacia una impresora u otro dispositivo de manufactura.

Las figuras 10 y 11 ilustran otra realización de la operación del sistema después de que ha ocurrido la emisión del miembro de identificación translúcido. Como se muestra en el bloque 1000, el método incluye solicitar y obtener

información específica al receptor 32 tal como se describió previamente con referencia a la figura 5. Una vez que el miembro 14 de identificación traslucida ha sido impreso o manufacturado, se provee al receptor por mano o a través de correo o por cualquier otra técnica adecuada como se muestra en el bloque 1002. Como se muestra en el bloque 1004, un servidor de banco de un banco determina si un receptor ha requerido autenticación, tal como un requerimiento de ingreso. Si se ha recibido un requerimiento, una página web puede ser enviada requiriendo entrada de la información 32 del receptor incluyendo la clave de acceso y el número 44 de serie del miembro de identificación translúcido como un primer nivel de un proceso de autenticación de factores múltiples como se muestra en el bloque 1006. Esto puede hacerse por ejemplo a través de la pantalla mostrada en la figura 5. Como se muestra en el bloque 206, el servidor del banco determina si la información 32 específica del receptor introducida y la clave de acceso y el número de serie 44 del miembro de identificación translúcido son correctos por ejemplo pasando junto con la información al autenticador 24 del miembro de identificación translúcido. Si el primer nivel de autenticación pasa, el método incluye, como se muestra en el bloque 1010, la presentación del patrón de filtración visual 44 que cuando se combina visualmente con uno o más identificadores oscurecidos 38 sobre el miembro 14 de identificación translúcido, revela solamente del uno o más identificadores oscurecidos según el identificador apropiado que va a ser introducido para la sesión o transacción actual. El servidor del banco puede entonces, a través del servidor de red, solicitar la entrada del identificador 700 revelado según sea revelado selectivamente a través del patrón de filtración desplegado en la pantalla proveyendo la pantalla como se muestra en la figura 6. Esto se muestra en el bloque 1010. En respuesta a la solicitud, el autenticador 24 del miembro de identificación translúcido 24 recibe el identificador 700 revelado de un uso y compara el identificador recibido con la identificación esperada correspondiente determinada por ejemplo mediante el generador de filtro visual o autenticador 24. Esto se muestra en el bloque 1012. Dado el “filtro” el ingreso de los datos del usuario y la información almacenada acerca de ese usuario, el autenticador puede validar si el usuario introdujo datos correctos o no (bien sea por sí mismo o pasándolo a un “servidor”). Si el identificador deseado se genera antes de requerirlo del usuario, el sistema también genera un filtro correcto para revelar el identificador predeterminado (todo antes de presentarlo al usuario). Alternativamente, si el usuario está provisto con un patrón (el filtro) y luego el sistema valida el identificador que el usuario introdujo con el identificador que habría resultado de ese patrón, no se requiere seleccionar un identificador deseado más adelante en el tiempo y el “generador de filtro”, por lo tanto no requiere un conocimiento de nada más. Los datos que representan el identificador revelado visualmente (por ejemplo, los datos mismos, una forma encriptada de los mismos u otros datos adecuados, también pueden ser recibidos utilizando un dispositivo diferente al dispositivo en el cual se despliega el patrón de filtración visual. Por ejemplo, el identificador puede ser revelado sobre una pantalla de un dispositivo y un dispositivo manual o un dispositivo no manual pueden ser utilizados para introducir y enviar el identificador revelado visualmente a otro dispositivo o sistema que verifique si hay coincidencia.

Como se muestra en el bloque 1014 si no existe una coincidencia, al receptor se enviará un error y se le solicitará reintroducir el identificador revelado. El sistema puede cambiar al uso de un identificador diferente para el nuevo intento. También, el sistema puede asegurar el usuario después de un cierto número de intentos fallidos. Sin embargo, como se muestra en el bloque 1016, si ocurre una coincidencia, se determina que el segundo factor de autenticación es exitoso y el usuario recibe el derecho deseado.

Las figuras 12 y 13 ilustran ejemplos de tarjetas de transacción que emplean miembros 14 de identificación translúcidos (incluyendo el tipo mostrado en la figura 14). Las tarjetas de transacción pueden ser tarjetas inteligentes o tarjetas no inteligentes y tienen la información convencional asociadas con tarjetas de crédito, tarjetas de débito o cualquier otra tarjeta de transacción adecuada y además incluyen el miembro 14 de identificación translúcido. El miembro 14 de identificación translúcido aparece sobre una porción de la tarjeta de transacción. Una porción de la tarjeta de transacción incluye información de la cuenta tal como un número de cuenta, número de tarjeta de crédito, o cualquier otro identificador 1300 adecuados si se desea, otros identificadores de usuario tales como nombres de usuario 1402. En un ejemplo mostrado en la figura 12, la tarjeta de transacción incluye una abertura 1306 que puede ser, por ejemplo, cortada en la tarjeta plástica de transacción provista de alguna otra manera en la tarjeta plástica y un miembro 14 de identificación translúcido con adhesivo puede ser colocado sobre la abertura o puede ser moldeado integralmente en la misma o unido de alguna otra forma tal como pero no limitándose a una estructura de conexión configurada para recibir y sostener el TIDM en o sobre la tarjeta de transacción de tal manera que el tamaño de la tarjeta de transacción sea el mismo tamaño de una de cualquier tarjeta de transacción convencional o cualquier otro tamaño adecuado según se desee. Si se utiliza, la estructura de conexión puede ser una estructura de encaje, deslizamiento, conexión basada en un adhesivo o cualquier estructura de conexión según se desee.

La figura 13 ilustra un ejemplo diferente en el cual el miembro 14 de identificación traslucida está unido a una superficie lateral o cualquier otra superficie de una tarjeta de transacción convencional. El miembro 14 de identificación translúcido puede ser plegable a lo largo de una línea de plegamiento 1400 o puede ser de un espesor en donde no es plegable y está conformado como parte de la tarjeta de transacción si se desea. También se contempla cualquier otro mecanismo adecuado para unir adecuadamente el miembro de identificación translúcido con o a una tarjeta de transacción.

Las figuras 14 y 15 ilustran una realización alternativa que básicamente reversa el papel de miembro de identificación translúcido y la unidad receptora. En esta realización, el identificador 14 translúcido contiene el filtro visual o patrón de potenciamiento 40 y la pantalla de despliegue presenta al menos un identificador oscurecido que puede ser por ejemplo datos que representan datos de autenticación del usuario que es único para un usuario o no único para un usuario según se desee (véase figura 15). Como sucede con la realización previa, la combinación de la superposición del

miembro de identificación translúcido (filtro visual) sobre la pantalla que despliega un identificador oscurecido, revela (desoscurece) o potencia el al menos un identificador oscurecido sobre la pantalla. Los datos de identificación de usuarios revelados pueden entonces ser introducidos en un dispositivo de transacción adecuado como clave de acceso u otra información de autenticación del usuario. También, cuando el área traslucida está unida o incorporada en una tarjeta de transacción convencional, la tarjeta de transacción incluye como se muestra por ejemplo en las figuras 12 y 13, una primera porción que contiene un número de tarjeta de transacción y una segunda porción que contiene un número de identificación translúcido u otra información de identificación que tiene un área traslucida que incluye un patrón de filtración visual.

La figura 16 ilustra un ejemplo de un sistema 1600 que emplea el TIDM 14 de la figura 14. En este ejemplo, el autenticador 24 de TIDM incluye un generador 1602 de identificador oscurecido similar al tipo utilizado para generar el uno o más identificadores descritos con referencia a la figura 1. El generador 1602 de identificador oscurecido genera el identificador oscurecido después de recibir información específica del receptor de un usuario, tal como un nombre de usuario, número de serie de TIDM, u otra información adecuada, para asegurar que el identificador oscurecido apropiado es desplegado para ese usuario. Con parte del proceso de registro, el usuario puede ya haber provisto la misma información específica de usuario y el generador 1602 del identificador oscurecido puede haber generado ya el identificador oscurecido y haberlo almacenado en la memoria 22.

El emisor 12 del miembro de identificación translúcido, en este ejemplo genera un TIDM 14 que tiene un área traslucida que tiene un patrón 40 de filtración visual sobre la misma configurado para filtrar visualmente un identificador 38 del usuario oscurecido presentado y está configurado para superponerse al menos a una porción de la pantalla de despliegue. Utilizando una entrada del usuario en información específica del usuario para iniciar una sesión puede ser deseable cuando el mismo patrón de filtración está impreso sobre los miembros identificadores translúcidos para una pluralidad de usuarios. Es deseable saber que el portador del TIDM es un usuario apropiado en oposición a un ladrón que roba el TIDM. El autenticador, u otra fuente, envían el identificador oscurecido generado al dispositivo receptor. El dispositivo receptor despliega el al menos un identificador oscurecido visualmente como datos de autenticación del usuario y recibe datos que representan los datos de autenticación del usuario revelados (tal como la identificación revelada misma o una representación de ella) con base en el miembro de identificación translúcido que tiene un patrón de filtración sobre sí. Por ejemplo cuando el miembro de identificación translúcido que tiene el patrón de filtración sobre sí es sostenido sobre la pantalla, el filtro revela el identificador del usuario. Si se desea, puede asignarse un número de serie del identificador translúcido a cada TIDM aun cuando el mismo patrón de filtración pueda ser impreso sobre más de un TIDM. Como tal, varios usuarios pueden tener miembros de identificación translúcido con el mismo patrón de filtración.

El emisor 12 del miembro de identificación translúcido es operativo para generar un miembro 14 de identificación translúcido que tiene un área traslucida que incluye un patrón de filtración visual 40 sobre la misma configurado para filtrar visualmente un identificador de usuario oscurecido desplegado y configurado para superponerse a al menos una porción de la pantalla de despliegue. El generador 1602 del identificador oscurecido genera al menos un identificador oscurecido visualmente para desplegar sobre una pantalla, en respuesta a la información recibida del usuario tal como información específica del usuario. El autenticador 18 del miembro de identificación translúcido, en este ejemplo recibe datos que representan el identificador revelado tal como a través del usuario que introduce la información a través de una interfaz de usuario después de que el patrón de filtración es superpuesto sobre la pantalla y como se describió previamente, el autenticador del miembro de identificación translúcido compara el identificador revelador recibido con un identificador esperado correspondiente (puesto que fue generado por el generador identificador oscurecido) para determinar si la autenticación apropiada de un receptor es apropiada. Alternativamente, el autenticador del miembro de identificación translúcido puede enviar el identificador revelado recibido a una tercera parte que lleva a cabo la comparación y envía un mensaje de regreso al autenticador o unidad receptora. Cualquier otra división adecuada de operaciones también puede ser utilizada según se desee. El autenticador del miembro de identificación translúcido o tercera parte envía entonces información para otorgar derechos a una unidad de recepción en respuesta a los datos recibidos que coinciden con el identificador esperado correspondiente.

La figura 17 ilustra un ejemplo de un método para proveer con seguridad información de identificación que incluye la generación de al menos un identificador oscurecido para un receptor basado en, por ejemplo, datos secretos del receptor recibidos o datos no secretos o datos que no están relacionados a o recibidos del receptor. Esto se muestra en el bloque 1700. Como se muestra en el bloque 1702, el método incluye generar un miembro 14 de identificación translúcido que tiene un patrón 40 de filtración visual sobre el mismo. Después de que se ha hecho el TIDM, el método incluye recibir información de identificación del usuario, tal como un PIN: u otros datos como un primer factor de autenticación para el usuario. Como se muestra en el bloque 1704, el método incluye enviar el uno o más identificadores oscurecidos al receptor desplegando al menos un identificador oscurecido visualmente como segundo factor de datos de autenticación del usuario que cuando se combinan visualmente con el patrón 40 de filtración visual sobre el miembro de identificación translúcido, revela un identificador oscurecido para un usuario. Como se muestra en el bloque 1706, el método incluye, que el usuario por ejemplo, superponga el miembro de identificación translúcido sobre la pantalla para identificar visualmente el identificador oscurecido a través del filtro. El método también incluye recibir datos que representan los datos de autenticación del usuario revelados con base en el miembro de identificación translúcido que tiene un patrón de filtración sobre sí mismo. El método también incluye recibir información específica del

usuario, tal como antes de la etapa de desplegar el identificador oscurecido, para determinar el identificador oscurecido visualmente para ser desplegado sobre la pantalla. Por ejemplo, el sistema necesita determinar cual identificador oscurecido desplegar puesto que cada usuario tiene preferiblemente un identificador diferente. Esto puede ser diseminado por ejemplo haciendo que el usuario introduzca información específica del usuario, a través de una interfaz de usuario de la unidad de recepción, tal como una clave de acceso u otra información secreta o no secreta según se desee.

Dicho de otra manera, el método incluye recibir información de identificación del usuario como un primer factor de autenticación para un usuario y usar, tal como mediante el autenticador TIDM, un proveedor de servicios u otra entidad adecuada tal como información de identificación del usuario para identificar un miembro de identificación translúcido en memoria que contiene un patrón de filtración visual particular conocido por haber sido asociado con tal usuario. El método incluye generar un identificador esperado para ser usado como segundo factor de autenticación para el usuario asociado con la información de identificación del usuario recibida y generar un patrón de identificadores de usuarios oscurecidos que contienen el identificador esperado de tal forma que cuando el patrón de los identificadores de usuarios oscurecidos se combinan con el patrón de filtración visual sobre el miembro de identificación translúcido identificado asociado con el usuario se revelará el identificador esperado. El método incluye la trasmisión del patrón de identificadores del usuario oscurecidos a una pantalla (por ejemplo un GUI desplegado) y requiere la introducción de un identificador revelado; y la recepción de los datos que representa el identificador revelado. Como se anotó anteriormente, el autenticador de TIDM por ejemplo, o cualquier otro número adecuado de servidores, o dispositivos actúan como los circuitos para llevar a cabo las operaciones anteriores.

La funcionalidad primaria del aparato, métodos y sistemas divulgados puede proveerse a través de interfaces de programación de aplicaciones (API) que son ejecutados por uno o más dispositivos de procesamiento que pueden ser integrados fácilmente en infraestructuras actuales. Además, cada miembro de identificación translúcido en una realización es diferente y tiene información aleatoria de apariencia diferente puesto que la información aparentemente aleatoria es típicamente, pero no necesariamente, generada a partir de información única para un receptor, tal como una clave de acceso, nombre de usuario, número de identificación personal o cualquier otra información. En cada realización, los miembros de identificación translúcidos y/o los filtros visuales y/o los identificadores oscurecidos pueden ser premanufacturados y asociados subsecuentemente con un usuario. Adicionalmente, los identificadores oscurecidos y/o los patrones de filtración pueden ser pregenerados y aplicados subsecuentemente a miembros de identificación translúcidos. Tal aplicación subsecuente a miembros de identificación translúcidos puede ser hecha por el creador de los patrones de filtración o identificadores oscurecidos o puede hacerse por parte de la entidad que provee el servicio o por una tercera parte contratista del proveedor de servicios. Puesto que la manufactura de los miembros de identificación translúcidos puede hacerse con materiales muy simples tales como plástico trasparente, también es posible para el proveedor de servicio enviar los identificadores oscurecidos o los patrones visuales a usuarios que puedan por si mismo aplicar el patrón de filtración a los identificadores oscurecidos a un miembro de identificación translúcido.

El mismo miembro de identificación translúcido puede ser utilizado un número repetido de veces puesto que puede haber una pluralidad de diferentes identificadores oscurecidos en el mismo en donde cada vez se requiere autenticación con uno diferente de los identificadores oscurecidos expuesto a través del patrón de filtración visual. Aquí el identificador revelado visualmente sobre el miembro de identificación translúcido puede cambiar durante cada sesión de autenticación si se desea. Los miembros de identificación translúcidos descritos aquí pueden ser utilizados para autenticación del usuario, activación de aplicaciones de software o cualquier otro propósito adecuado. Los identificadores oscurecidos diferentes pueden ser caracteres, imágenes u otra información adecuada.

La figura 18 ilustra un ejemplo de un artículo 1800 (por ejemplo un miembro), tal como una película traslucida o no traslucida, adhesivo, tarjeta o cualquier otro material o artículo adecuado. Se reconocerá que la información mostrada sobre el artículo 1800 es mostrada como un ejemplo solamente y se reconocerá que puede usarse cualquier información adecuada. En este ejemplo, el artículo 1800 incluye información de localización 1802 y 1804 (mostrada como indicios en filas y columnas) respectivamente e información de autenticación del agente de envío 1806 en la forma de números que son direccionables o localizables por la información de localización de coordenadas (por ejemplo información de filas y columnas). Además el artículo 1800 incluye un identificador de artículos 1808 opcional tal como un número de serie generado (por ejemplo asignado) por el emisor del artículo 1800.

Hablando en general, el artículo 1800 si se desea, puede ser generado como se describió anteriormente con respecto a miembro de identificación translúcido para generar por ejemplo la información de identificación del agente de envío. Sin embargo, además la información de localización 1802 y 1804 también necesita ser agregada en una realización. Además, se reconocerá que el miembro 14 de identificación translúcido también puede ser utilizado como un artículo de autenticación del agente de envío y los identificadores 38 oscurecidos también pueden servir como información de autenticación del agente de envío.

Además, en esta realización no se requiere que haya información específica del receptor si el sistema no lo requiere, y la información de autenticación del agente de envío puede ser generada bien sea independientemente desde o con base en información específica del receptor si se desea. Esto puede suceder cuando el recipiente se inscribe para el

servicio. Además, tal como se utiliza aquí, la información de localización incluye la información, por ejemplo, enviada con un mensaje o indexada mediante un mensaje enviado por el agente de envío el cual indica cual información de autenticación del agente de envío en el artículo 1800 debe verificar al receptor. Por ejemplo, la información de localización no requiere ser información de filas y columnas, sino que solamente pueden ser términos tales como "esquina superior izquierda", "esquina inferior izquierda", "tercero desde la derecha", o cualquier otra información adecuada para notificar al receptor cual es la información de autenticación del agente de envío sobre el artículo que se va a utilizar como información de autenticación para la sesión, transacción u otra comunicación dadas. Alternativamente, la información de autenticación del agente de envío puede ser un señalador de una localización que contiene la información de autenticación del agente de envío, tal como, por ejemplo, un localizador de recursos universal (URL) que señala la información de autenticación del agente de envío para la sesión, transacción u otra comunicación dada. Adicionalmente, la información de localización puede ser un señalador de una localización que contiene la información de localización real, la cual a su vez indica donde buscar en el artículo la información de autenticación del agente de envío para la sesión, transacción u otra comunicación dada. En otra realización, la información de localización es un patrón de filtro visual.

La figura 19 ilustra una tarjeta de transacción 1900 que puede incluir, por ejemplo, una banda magnética 1902 o cualquier otra información adecuada que pueda proveer información de una cuenta o información del agente de envío de un mensaje. La tarjeta de transacción 1900 puede ser por ejemplo una tarjeta de banco, una tarjeta de crédito, una tarjeta de débito o cualquier otra tarjeta de transacción tal como se describió anteriormente y puede incluir información del identificador de la tarjeta de transacción tal como un número de tarjeta etc., tal como se describió anteriormente. Está tarjeta de transacción 1900 es diferente de las tarjetas de transacción convencionales porque, entre otras cosas, incluye el artículo 1800 sobre si (o miembro), o asegura la misma de cualquier manera adecuada. Como tal, las variaciones en la tarjeta de transacción 1900 está administrada por ejemplo en la figura 13. En un ejemplo, el miembro 1800, tal como una pieza de papel con respaldo adhesivo o cualquier otro miembro adecuado, se asegura a una tarjeta de transacción convencional si se desea. También se reconocerá como se describió anteriormente que el miembro o artículo puede ser asegurado o fijado adecuadamente en cualquier forma adecuada incluyendo, pero no limitándose a un adhesivo, o cualquier otro mecanismo adecuado. El miembro 1800 puede ser enviado a un receptor como una porción para desprender de un estado financiero, estado de facturación, etc. Preferiblemente esta dimensionado para encajar en una tarjeta de transacción.

La figura 20 ilustra un ejemplo de un método para proveer autenticación de un mensaje electrónico que puede ser llevada a cabo por un elemento adecuado. En este ejemplo, puede ser llevado a cabo por ejemplo mediante un servidor o pluralidad de servidores u otras aplicaciones adecuadas que se ejecuten en uno o más dispositivos de procesamiento. Como se muestra en el bloque 2000, el método incluye, por ejemplo, cuando un agente de envío tal como un servidor de un banco u otro agente de envío de mensajes quiere enviar un mensaje a un receptor, determina la información de localización deseada, tal como una fila y columna que también existe en el artículo del receptor particular, e información y autenticación del agente de envío deseado correspondiente para ser enviada y coincidente con la información de autenticación del agente de envío localizada sobre el artículo y es localizable de acuerdo con la información de localización enviada. Esto puede hacerse por ejemplo teniendo acceso a una base de datos que enlaza una dirección de correo electrónico del receptor por ejemplo, a campos de base de datos correspondientes que representan por ejemplo el contenido de un artículo que fue emitido para ese receptor. Como se muestra en el bloque 2002, el método incluye enviar el mensaje electrónico y la información de localización deseada e información de autenticación del agente de envío deseada correspondiente, al receptor en donde la información de autenticación del agente de envío deseada es localizable sobre el artículo con base en la información de localización deseada enviada. Como tal por ejemplo, el agente de envío o unidad de envío pueden ser asociados (por ejemplo, apéndice, prependientes, insertos u otro anexo de alguna otra manera) e información de filas y columnas e información de autenticación del agente de envío correspondiente que deberían aparecer en esas localizaciones sobre el artículo como aparte de un mensaje electrónico para un receptor. El receptor puede entonces localizar, con base en el número de columna y fila recibido, la información de autenticación del agente de envío sobre su artículo que fue emitido a ellos por (o en nombre de) el agente de envío, y confirma que la información de autenticación del agente de envío deseada coincide con la misma información en las localizaciones indicadas por la información de localización enviada por la unidad de envío. Si ocurre una coincidencia, entonces el receptor puede confiar en el agente de envío del mensaje. Se reconocerá que la información de localización enviada y la información de autenticación del agente de envío pueden ser los datos mismos, un índice de, función de, referencia a, o cualquier otra representación adecuada bien sea de la información de localización y/o información de la autenticación del agente de envío.

Por ejemplo, la información de coordenadas de localización y la información correspondiente de la autenticación del agente de envío podrían incluir los datos trasmitidos electrónicamente para desplegar sobre un dispositivo de pantalla, tal como un patrón de filtración visual e información de autenticación del usuario. En está realización, el artículo seria un artículo trasparente que permita al usuario colocar el artículo sobre un área de una pantalla de despliegue. El mensaje enviado incluiría el patrón de filtración visual junto con la información de autenticación del agente de envío deseada que aparecería visualmente ante el usuario cuando el usuario superpone el artículo sobre una pantalla de despliegue. Si el receptor reconoce visualmente o ve la información de autenticación del agente de envío que se revela a través del patrón de filtración visual sobre la pantalla con la información de autenticación del agente de envío deseada y coinciden, entonces el usuario puede confiar en el agente de envío del mensaje. Como tal, las técnicas de filtración visual tal como

se describieron previamente con respecto al miembro de identificación translúcido para la autenticación del receptor pueden ser utilizadas en parte para autenticar un agente de envío.

Con referencia también a la figura 21, se muestra un ejemplo específico de un mensaje y de la información de autenticación del agente de envío asociada y la información de localización como 2100. En una realización particular, también con referencia a la figura 18, el mensaje es anexo con información de autenticación del agente de envío y en particular los números “98413” e información de coordenadas “A2, E4, F1, H4, J2” Como tal, la unidad de envío envía el mensaje electrónico junto con la información de autenticación deseada del agente de envío y la información de localización deseada como se muestra. El usuario utiliza entonces el artículo 1800 y busca, por ejemplo, en la localización de coordenadas A2 y ve el número 9, busca en la localización de coordenadas E4 y ve el número 8, busca en la localización de coordenadas F1 y ve el número 4, busca en la localización de coordenadas H4 y ve el número 1, y busca en la localización de coordenadas J2 y ve el número 3. Si el usuario ve la misma información de autenticación del agente de envío sobre el artículo 1800 tal como fue enviada por la unidad de envío, entonces el receptor confía en que el agente de envío es un agente de envío autentico del mensaje. En este ejemplo, la información de autenticación del agente de envío representa visualmente información de autenticación del agente de envío que es identificable por información de coordenadas de localización en la forma de filas y columnas. Sin embargo, se reconocerá que no es necesario usar el formato de filas y columnas y como tal las celdas tal como se muestran no requieren ser empleadas. Por ejemplo, si se utilizan objetos en oposición a letras y números, los objetos pueden estar localizados en la parte superior izquierda, superior derecha, media o en cualquier otra localización adecuada del artículo y la información de autenticación del agente de envío, la cual podría ser el objetivo puede enviarse como tal en la forma de un objeto gráfico u otro adecuado, en la información de localización de coordenadas puede ser realmente palabras que puedan leer “esquina superior izquierda”. Puede usarse cualquier otra información de localización de coordenadas o de información de autenticación del agente de envío adecuadas.

El artículo 1800 tal como se anotó anteriormente puede ser por ejemplo una pieza de papel, una tarjeta plástica, una tarjeta plástica transparente, un adhesivo que puede ser fijado a tarjetas plásticas existentes o cualquier otro artículo adecuado. En este ejemplo, a cada receptor de correo electrónico está provisto con el artículo con su propio contenido generado aleatoriamente (o aparentemente de manera aleatoria). Cuando se envía un correo electrónico, un agente de transferencia de mensajes del originador u otros componentes del servidor se asocian con cada correo electrónico enviado directa o indirectamente tal como por ejemplo mediante una página HTML utilizando una URL u otra referencia adecuada, coordenadas u otras direcciones para localizar uno o más celdas o localizaciones en la tarjeta. También se anexan, preunen, se insertan o de alguna otra manera se unen al correo electrónico los contenidos en esas localizaciones. En la recepción, el usuario confirma los resultados que aparecen utilizando su artículo de autenticación de agente de envío individual, por ejemplo mediante la lectura de las coordenadas listadas en el correo electrónico y su búsqueda sobre su propio artículo de autenticación del agente de envío. En la realización donde se usa una versión traslucida del artículo de autenticación, el artículo de autenticación puede ser colocado sobre un patrón de filtración visual provisto con el correo electrónico y la información de autenticación del agente de envío es comparada con el receptor con la información de autenticación del agente de envío deseada que está provista en el correo electrónico. Si los caracteres u otra información no coinciden, la autenticación ha fallado.

La figura 23 ilustra en más detalle un método para proveer la autenticación de mensajes electrónicos en donde el método incluye, como se muestra en el bloque 2300, la generación por ejemplo, de información de autenticación del agente de envío aleatoria para ser colocada en el artículo y si se desea información de localización que también puede ser colocada sobre el artículo y relacionar las dos con el receptor seleccionado. Aleatorio incluye información seudoaleatoria o cualquier otro nivel adecuado de aleatorización de la información. Esto puede hacerse como se describió anteriormente con respecto a miembro de identificación translúcido a través de una interfaz adecuada sobre uno o más ordenadores del servidor o sobre cualquier dispositivo adecuado. Como se muestra en el bloque 2302, está información se almacena como la información de autenticación y la información de localización correspondiente en una base de datos adecuada. Como se muestra en el bloque 2304, el método incluye crear un artículo, tal como un artículo 1800 que contiene la información de coordenadas de localización y la correspondiente información de autenticación del agente de envío y si se desea un identificador de artículo 1808 tal como un número de serie para emitir a un receptor específico. Esto puede hacerse, por ejemplo, en una forma básicamente similar a la descrita anteriormente. Por ejemplo, una tarjeta puede ser impresa, una tarjeta de transacción puede ser conformada adecuadamente, o un adhesivo puede ser generado de manera que pueda ser adherido a un artículo adecuado. El artículo es enviado entonces al receptor por correo o por cualquier otro canal adecuado.

En una realización alternativa, en lugar de utilizar un tipo de instrumento físico (por ejemplo un artículo) puede utilizarse un instrumento virtual cuando la representación (puede no ser una imagen real) de una tarjeta por ejemplo o representación de un artículo puedan ser enviados electrónicamente para desplegar a través de una pantalla a un usuario o mediante otro tipo de acceso electrónico para tal usuario, bien sea durante cada sesión o una vez y el usuario puede almacenar el artículo de autenticación del agente de envío electrónico en un archivo y puede tener acceso a él cuando sea necesario. Como tal, puede tenerse acceso a la representación electrónica del artículo mediante una aplicación de software de tal manera que provea al receptor con la información de autenticación del agente de envío localizada en la localización identificada por la información de localización enviada.

Como se muestra en el bloque 2306, el método también incluye, por ejemplo, como se describe anteriormente con respecto a la figura 20, la determinación, tal como por parte del agente de envío, de al menos un ítem deseado de información de localización y la correspondiente información de autenticación del agente de envío para agregar, preagregar, insertar o de alguna otra manera unir el mensaje actual. La selección de la información de localización y la información de autenticación puede hacerse de cualquier manera adecuada, tal como aleatoriamente o de cualquier otra forma adecuada según se desee. Como se muestra en el bloque punteado 2308, en una realización alternativa, la información de localización y la información de autenticación del agente de envío se comunica de manera efectiva en la forma de un patrón de filtración visual que puede, si se desea, cubrir todos los encabezamientos de filas y columnas y en lugar de ello permitir solamente que la información de autenticación del agente de envío sea desplegada visualmente cuando el artículo esta superpuesto. Como tal, el método puede incluir el envío de un patrón de filtración visual para desplegar al receptor de manera que permita que el receptor determine visualmente si el agente de envío es auténtico. El receptor puede colocar al menos una porción de la información de autenticación del agente de envío que está sobre el artículo, sobre un patrón de filtración visual que está desplegado en la pantalla de despliegue, para determinar si la información de autenticación del agente de envío enviada con el mensaje coincide con la información de autenticación del agente de envío hecha visible por el patrón de filtración visual.

En un ejemplo el método incluye anexar al menos un ítem deseado de información de localización y la correspondiente información de autenticación del agente de envío a un mensaje electrónico para el receptor. La información de autenticación del agente de envío representa visualmente información de autenticación identificable por la información de coordenadas de localización. Como tal, el mensaje mismo puede ser agregado, preagregado, insertado o unido de alguna otra manera a la información o puede contener una referencia de información tal como un sitio en la red o cualquier otro enlace adecuado o cualquier otra representación adecuada de la información de autenticación del agente de envío y la información de coordenadas de localización.

Como se muestra en el bloque 2310, el método incluye enviar el mensaje electrónico y los datos que representan tanto la información de coordenadas de localización como la información de autenticación del agente de envío correspondiente a un receptor. El receptor puede entonces mirar en la información sobre el artículo y ver si coinciden con la que fue enviada por la unidad de envío.

También se reconocerá que la determinación en al menos una coordenada de localización, con base en la información de localización y la correspondiente información de autenticación del agente de envío puede hacerse, por ejemplo, dinámicamente en oposición a buscar la información almacenada en la base de datos. Por ejemplo, el agente de envío (por ejemplo unidad de envío de mensajes) puede programarse simplemente con una función para generar información de autenticación del agente de envío para enviar en oposición a buscar la información prealmacenada.

También si se desea, la información de autenticación del agente de envío puede ser información por ejemplo, tal como el balance final de una cuenta de banco, cualquier información adecuado de un estado de facturación o estado de cuenta que el agente de envío pueda haber enviado previamente al receptor que pueda contener la información de autenticación del agente de envío. La información de localización puede ser la fecha de un estado de cuenta particular y la información de autenticación del agente de envío puede ser el balance actual en una cuenta de tarjeta de crédito. Puede usarse cualquier otro estado o cualquier otra información conocida, o provista por, la unidad de agente de envío que este en posición del receptor y pueda ser usada.

La figura 22 ilustra un ejemplo en un sistema para proveer autenticación de un mensaje electrónico que puede, si se desea, llevar a cabo las etapas descritas en referencia a la figura 23. Por ejemplo, una unidad de envío 2200, tal como cualquier ordenador servidor, pluralidad de servidores, dispositivos móviles o cualquier otra estructura adecuada puede incluir un emisor 2202 de artículos de autenticación del agente de envío, o una tercera parte puede emitir el artículo de autenticación del agente de envío según se desee. Por ejemplo, el emisor 2202 del artículo de autenticación del agente de envío puede generar la información de autenticación del agente de envío aleatoria y la correspondiente información de coordenadas de localización y enlazarla con un receptor y almacenar la información en la base de datos 2204. El artículo 1800 puede entonces ser enviado por correo, por ejemplo, a un receptor, o en el caso de un medio virtual, ser enviado electrónicamente al receptor. En esta ilustración (figura 22), se muestra un artículo translúcido. Como tal, el receptor 20 incluye una pantalla 30 y el mensaje 2100 por ejemplo se despliega sobre la pantalla junto con un patrón de filtración visual y la información de autenticación del agente de envío enviada. El patrón de filtración visual se utiliza entonces para revelar la información de autenticación del agente de envío esperado que luego es comparada por el receptor con la enviada en el mensaje 2100. En esta realización cuando el artículo de autenticación del agente de envío es un tipo translúcido, el patrón de filtración visual enviado por la unidad de envío incorpora la información de localización puesto que el resultado de la superposición por el receptor del artículo de autenticación del agente de envío sobre una pantalla de despliegue dará como resultado una información de autenticación del agente de envío revelada visualmente en localizaciones particulares en el artículo. Como tal, el patrón de filtración visual incluye la información de localización. Además, se reconocerá que el termino información se refiere a cualquier indicio adecuado.

La unidad 2200 de envío la cual puede ser un servidor adecuado en una red, o cualquier otro dispositivo adecuado, incluye uno o más circuitos que pueden estar en la forma de uno o más dispositivos de procesamiento que ejecutan instrucciones de software que son almacenadas en la memoria, o puede ser implementado utilizando programas

discretos, o cualquier combinación de hardware, software o firmware para llevar a cabo las operaciones descritas aquí. Como tal, la unidad de envío 2200 incluye circuitos que son operativos para llevar a cabo las etapas como se describieron anteriormente.

En otra realización, el uso del artículo de autenticación del agente de envío puede combinarse por ejemplo con los sistemas descritos anteriormente con respecto al miembro de identificación translúcido de tal manera que el miembro de identificación translúcido incluya la información de localización y la información de autenticación del agente de envío sobre sí. Por ejemplo los identificadores oscurecidos si se desea también pueden servir como información de autenticación del agente de envío o en realizaciones alternativas el miembro de identificación translúcido puede tener una porción que incluya los identificadores oscurecidos y otra porción que incluya la información de localización y la información de autenticación del agente de envío. En cualquier evento, el uso de un artículo o miembro individual que es translúcido tal como se describe aquí puede proveer autenticación multiniveles. Por ejemplo, para autenticación del agente de envío, los métodos descritos más arriba con respecto a las figuras 18 – 22 pueden emplearse para confirmar que el agente de envío es auténtico. Una vez que un receptor por ejemplo está convencido de que el agente de envío de un correo electrónico es auténtico, el receptor puede entonces oprimir sobre una URL enviada en el mensaje de correo electrónico y luego recibir la presentación de una forma HTML adecuada para introducir información de la cuenta u otra información confidencial. Sin embargo, antes de entrar a esta información confidencial puede llevarse a cabo un segundo nivel de autenticación empleando el miembro de identificación translúcido e identificadores oscurecidos de tal manera que la unidad de envío pueda autenticar el receptor en este paso de la sesión o transacción. También se reconocerá que puede emplearse cualquier otro orden adecuado de operaciones o combinaciones de los esquemas de autenticación.

Además, el uso de los términos reivindicados incluye cualquier representación de los mismos. Por ejemplo, el término información de autenticación del agente de envío incluye los datos mismos, cualquier índice para los datos, cualquier referencia o señalador de los datos, o cualquier otra representación de los mismos.

Entre otras ventajas, no hay necesidad de modificación alguna a un agente de transferencia de mensajes o un cliente de correo electrónico de un receptor. También si se desea, no se requiere registrar los ordenadores del receptor permitiendo que la autenticación sea llevada a cabo desde cualquier ordenador si se desea. El sistema puede ser también aplicable a dispositivos móviles en donde las coordenadas de búsqueda puedan desplegarse fácilmente sobre una pantalla de despliegue pequeña. Otros propósitos de autenticación pueden incluir autenticación en la red, autenticación con respuesta interactiva a voz o cualquier escenario de autenticación. Además, el sistema y método ofrecen un tipo de mecanismo no costoso tal como las tarjetas de autenticación que pueden ser distribuidas en comparación con otras tecnologías más complejas que pueden requerir tarjetas inteligentes, infraestructura de claves virtuales o públicas. Otras ventajas serán reconocidas por las personas de experiencia normal en la técnica.

La figura 24 muestra un ejemplo de un sistema 2400 que provee autenticación mutua entre un usuario (por ejemplo una unidad receptora) y una unidad de envío también denominada como recurso objetivo. Tal como se describió por ejemplo con respecto a las figuras 18 – 23 y en otros lugares, en este ejemplo, el artículo 1800 sirve como una tarjeta de autenticación la cual está asignada a cada usuario final e incluye, por ejemplo, marcaciones aleatorias y/o únicas conocidas solamente por la unidad de envío (por ejemplo recursos objetivos) y el usuario final. Proveyendo evidencia de ese conocimiento al receptor, la unidad de envío puede demostrar su identidad y por parte del usuario final hacer que la unidad receptora regrese información localizada en la tarjeta de autenticación, demostrando así el usuario final su identidad como usuario final apropiado.

Como se anotó anteriormente, el sistema 2400 puede incluir un emisor 2202 de miembro de autenticación de agente de envío que produce el artículo 1800 con base en, por ejemplo, información 32 específica del receptor (esto es, información de autenticación del usuario) la cual puede ser, pero no se limita a, por ejemplo una clave de acceso y/o una identificación de un usuario. El sistema 2400 también incluye unidad 2402 de envío la cual puede ser un servidor o cualquier dispositivo adecuado tal como se describió previamente y puede incluir también, como se anotó anteriormente, un grupo de servidores o circuitos que llevan a cabo las operaciones descritas aquí. El sistema 2400 también incluye una base de datos 2404 similar a las bases de datos descritas previamente en las cuales, en este ejemplo, también se almacena la información de autenticación del usuario 32 para permitir que se lleve a cabo una operación de autenticación del usuario de primer nivel. Además, como se describió anteriormente, la base de datos 2404 también almacena la información de autenticación del agente de envío que está localizado en el artículo así como el identificador del artículo de tal manera que la unidad de envió 2402 puede proveer el proceso de autenticación de segundo nivel tal como se describió aquí.

La unidad de envío 2402 también incluye, por ejemplo, una memoria que contiene instrucciones ejecutables que cuando se ejecutan por parte de uno o más dispositivos de procesamiento opera como un autenticador 2406 de primer nivel y un autenticador 2408 de segundo nivel. Como se anotó anteriormente, se reconocerá sin embargo que estas operaciones pueden llevarse a cabo mediante servidores separados u otras unidades de cómputo localizadas o accesibles a través del internet, una intranet o cualquier red adecuada. También se reconocerá que las comunicaciones descritas aquí pueden ser comunicadas por vía inalámbrica por ejemplo cuando la unidad receptora 20 es un dispositivo de mano inalámbrico o cualquier otro dispositivo inalámbrico portátil.

Con referencia también a la figura 25, se describe un método para proveer autenticación mutua entre un usuario y una unidad de envío, tal como un recurso objetivo. El artículo tal como se anotó anteriormente puede incluir una tarjeta de transacción, una tarjeta que no tenga información de transacción, una tarjeta traslucida, una tarjeta electrónica (por ejemplo, una tarjeta desplegada visualmente) que puede ser, por ejemplo, almacenada en la memoria de la unidad receptora o cualquier otra unidad adecuada y luego desplegada a un usuario según solicitud o automáticamente en respuesta a la restricción de la pregunta, o el artículo puede tomar cualquier otra forma adecuada. También, la información de localización enviada en la pregunta incluye, por ejemplo, datos transmitidos electrónicamente para desplegar en un dispositivo de pantalla. Como se anotó anteriormente, esto puede tomar la forma de información de filas y columnas o cualquier otra información adecuada que pueda ser transmitida electrónicamente y, por ejemplo, desplegada en una pantalla 30 para el usuario o presentada audiblemente. Se asumirá que para esta realización, un usuario ha recibido el artículo de autenticación del agente de envío 1800 y en este ejemplo no es un artículo translúcido de tal manera que no se necesita utilizar un filtro visual en este ejemplo. Sin embargo, se reconocerá que las operaciones descritas aquí pueden ser llevadas a cabo adecuadamente para cualquier artículo adecuado incluyendo una tarjeta o artículo translúcidos. Este método puede llevarse a cabo, por ejemplo, mediante el sistema mostrado en la figura 24, o por cualquier sistema o estructura adecuados. En este ejemplo, la información de identificación del artículo no necesita ser enviada a la unidad receptora por la unidad del agente de envío 2402. Sin embargo, si se desea, puede hacerse. En este ejemplo, la unidad de envío 2402 verifica repetidamente para ver si una respuesta a una pregunta enviada incluye información de autenticación del agente de envío que fue identificada por la información de localización en una pregunta enviada que coincide con lo esperado (por ejemplo, lo deseado por el agente de envío) por información de autenticación del agente de envío. Si no, la pregunta es enviada repetidamente múltiples veces durante una sesión, o durante múltiples sesiones hasta que la información de autenticación del agente de envío deseada que es recibida por la unidad de envío coincida con la información de autenticación esperada.

Aunque no se muestra en la figura 25, puede llevarse a cabo inicialmente un proceso de autenticación de primer nivel. Por ejemplo, esto puede incluir recibir información 2410 de autenticación del usuario que puede incluir, por ejemplo, una clave de acceso del usuario y una identificación de usuario, desde la unidad receptora 20, y por lo tanto del usuario. Esta se recibe por ejemplo, por parte del autenticador 2406 de primer nivel. El autenticador de usuario 2406 de primer nivel autentica entonces el usuario con base en la información 2410 de autenticación de usuario recibida utilizando la información 32 de autenticación de usuario obtenida, por ejemplo, de la base de datos 2402. Si coinciden, la autenticación del usuario es exitosa. Se envía una indicación de “sí” 2412 al autenticador 2408 de segundo nivel indicando que puede llevarse a cabo un segundo proceso de autenticación. Es preferible, por ejemplo, también que durante el proceso de autenticación de primer nivel, se implemente un mecanismo de búsqueda tal como uno que limite el número de intentos de autenticación durante el proceso de autenticación de primer nivel evitando un ataque forzado bruto. Al terminar exitosamente la primera etapa de autenticación, se indica al usuario que autentique con información específica del artículo como se describió anteriormente.

Como se muestra en el bloque 2500, el método incluye la determinación, para un usuario al cual ha sido asignado el artículo 1800, información de autenticación del agente de envío deseada que corresponda con la información de autenticación del agente de envío que está incorporada en el artículo. Esto puede hacerse, por ejemplo, mediante el autenticador 2408 de segundo nivel seleccionando adecuadamente información de autenticación del agente de envío de la base de datos 2404 que está localizada en el artículo 1800 con base en la información 32 de autenticación del usuario. Como se anotó anteriormente, estos indicios sobre el artículo se almacenan por parte del emisor 2202 del miembro de autenticación del agente de envío en la base de datos 2404. La información de autenticación del agente de envío puede localizarse sobre el artículo 1800 mediante un usuario usando la información de localización, tal como identificadores de filas y columnas, o cualquier otra información de localización adecuada tal como se describió anteriormente.

Como se muestra en el bloque 2502, el método incluye el envío, tal como por parte de la unidad de envío 2402, de una pregunta para el usuario que incluya al menos información de localización que identifica la información de autenticación del agente de envío deseada y que puede ser localizada sobre el artículo 1800. Una pregunta puede incluir, por ejemplo, uno o más conjuntos de coordenadas que son por ejemplo, desplegados a un usuario a través de la pantalla 30. La pregunta es preferiblemente particular para cada usuario y puede ser recuperada, con base en la identidad o en la información de autenticación del usuario del proceso de autenticación del usuario de primer nivel. Esto asegura que el usuario recibe la misma pregunta hasta que se complete una autenticación exitosa. La repetición de la misma pregunta puede evitar que un atacante monte un ataque de fuerza bruta con base en el conocimiento de solamente algunos pocos de los contenidos de la tarjeta del usuario los cuales, por ejemplo, pueden haber sido obtenidos utilizando diversos mecanismos de ataques potenciales. Se lleva a cabo entonces la pregunta generada aleatoriamente y almacenada una vez que el usuario ha autenticado exitosamente a través de un proceso de autenticación de segundo nivel. La pregunta 2414 puede ser enviada de cualquier manera adecuada y puede tomar cualquier forma adecuada incluyendo, pero no limitándose, a una comunicación SSL o a una comunicación no segura si se desea. Como se muestra en el bloque 2504, el método incluye recibir una respuesta a la pregunta enviada. En este ejemplo, una respuesta designada como 2416 es recibida de la unidad receptora 20 y es generada por la unidad receptora bajo control del usuario, por ejemplo, utilizando la información de localización enviada en la pregunta 2414, tal como una identificación de filas y columnas para determinar la información de autenticación del agente de envío localizada en la tarjeta. El usuario introduce esta información a través de una interfaz de usuario adecuada en respuesta a la pregunta.

Como tal, con respecto a la realización de las figuras 24 – 28, la respuesta incluye información de autenticación del agente de envío deseada (deseada por la unidad de envío) obtenida del artículo. Esta información de respuesta, aunque denominada como “información de autenticación del agente de envío” se usa realmente para autenticar el usuario por parte del agente de envío, u otra entidad, puesto que la respuesta contiene información solamente obtenible por el poseedor de la tarjeta de autenticación.

Como se muestra en el bloque 2506, el método incluye la determinación, por ejemplo mediante la unidad de envío 2402, de si la respuesta recibida a la pregunta incluye la información de autenticación del agente de envío deseada que fue identificada por la información de localización enviada en la pregunta. Como se muestra en el bloque 2508, si la información de autenticación del agente de envío recibida en la respuesta no es la información de autenticación del agente de envío deseada que fue identificada en la pregunta por la información de localización, la unidad de envío 2402, en este ejemplo, reenvía entonces la misma pregunta que contiene la misma información de localización que fue enviada previamente, a la unidad receptora 20. Como se muestra en el bloque 2510, el método incluye repetir las etapas de analizar la respuesta recibida y si la respuesta no incluye información de autenticación del agente de envío que era esperada con base en la información de localización enviada en la pregunta, la unidad de envío envía la misma pregunta durante la misma sesión hasta que la respuesta recibida incluya la información de autenticación del agente de envío deseada que esta sobre el artículo o hasta que se haya intentado un número adecuado de ensayos tal como lo haya definido la unidad de envío, por ejemplo. La pregunta repetida hasta que la respuesta incluya la información de autenticación del agente de envío deseada esperada.

La figura 26 ilustra otro método para proveer autenticación mutua entre un usuario y un agente de envío y puede llevarse a cabo, por ejemplo, mediante el sistema 2400 de la figura 24, o cualquier otro sistema o dispositivos adecuados. En este ejemplo, no se lleva a cabo el envío repetido de la misma pregunta hasta que se reciba una respuesta apropiada. En esta realización, la información de identificación del artículo, tal como un número de serie localizado en el artículo, o cualquier otra identificación del artículo adecuada se envía también al usuario además de la información de localización en una pregunta. Tal como se muestra en el bloque 2600 el método incluye determinar, por ejemplo mediante la unidad de envío 2402, información de autenticación del agente de envío deseada que corresponde con información de autenticación del agente de envío que está incorporada en el artículo y también la determinación para el mismo usuario, de la correspondiente información de identificación del artículo, tal como el número de serie del artículo o secreto compartido o cualquier otra información de identificación adecuada. Como se muestra en el bloque 2602, el método incluye enviar una pregunta para el usuario que incluye la información de localización determinada y la información de identificación del artículo para autenticar la unidad de envío al usuario.

Como se muestra en bloque 2604, el método incluye autenticar el usuario con base en una respuesta a la pregunta en donde la respuesta incluye información de autenticación del agente de envío obtenida del artículo, con base en la información de localización. En este ejemplo, el usuario, por ejemplo, no introduce o envía una respuesta a la pregunta al menos que el usuario verifique que la información de identificación del artículo enviada en la pregunta, coincide con la información de identificación del artículo en el artículo mismo. Como tal, el usuario puede autenticar la unidad de envío con base en la información de autenticación del artículo. Como tal, en este ejemplo, la pregunta incluye información de identificación del artículo además de la información de localización. La respuesta incluye la información de autenticación del agente de envío localizado sobre el artículo, definida por la información de localización. Si el identificador de artículo en la pregunta coincide con el identificador de artículo en el artículo que está en posesión del usuario, entonces el usuario confía en la unidad de envío. Como se muestra en el bloque 2606, el método incluye la autenticación del usuario con base en la respuesta a la pregunta. En este ejemplo, de nuevo se lleva a cabo preferiblemente una autenticación de primer nivel que ha sido descrita previamente con base en la clave de acceso del usuario y/o identificación del usuario. Si ese nivel de autenticación es exitoso, entonces el método mostrado en la figura 26 puede ser ejecutado de manera adecuada. Tal como se anota, la información de identificación del artículo puede incluir un secreto compartido conocido por el usuario y por el agente de envío o puede ser un número de serie de un artículo, o cualquier otra información adecuada.

La figura 27 ilustra otro método para proveer y autenticación mutua entre un usuario y un agente de envío el cual combina efectivamente alguna de las operaciones mostradas en las figuras 25 y 26. Como se muestra en el bloque 2700, el método incluye, llevar a cabo un primer proceso de autenticación tal como la solicitud de una primera información de autenticación del usuario de primer nivel. Esto puede incluir, por ejemplo, que la unidad de envío envié una pregunta o provea una instrucción para el usuario para introducir una clave de acceso y una identificación de usuario. En respuesta, la unidad de envío recibe la información de autenticación de primer nivel del usuario tal como una clave de acceso e información de autenticación almacenada del usuario 32 (por ejemplo un hash de la clave de acceso recibida) se verifica para asegurar que la información de autenticación del usuario de primer nivel recibida es apropiada. Como se muestra en el bloque 2702, si la autenticación de primer nivel es exitosa, el método incluye determinar para el usuario la información de autenticación del agente de envío deseada que corresponda con la información de autenticación del agente de envío que está incorporada en un artículo y determinar, por ejemplo, información de identificación del artículo que puede estar localizada sobre el artículo. Como tal, en este ejemplo, tanto la información de localización como la información de identificación del artículo se envían en una pregunta. Las etapas descritas previamente con referencia a las figuras 25 y 26 se llevan a cabo ahora de tal forma que por ejemplo, se envié una pregunta repetidamente en donde la pregunta es la misma pregunta hasta que se reciba en una respuesta

información de autenticación del agente de envío apropiada. Como tal, el usuario confirma que el despliegue del identificador del artículo de la pregunta coincide con el identificador en su tarjeta. Esto autentica la unidad de envío o la organización objetivo como ella misma y el usuario final tiene conocimiento de este identificador. El usuario introduce una respuesta adecuada a la pregunta observando el contenido de su tarjeta y la información de localización enviada en la pregunta. La unidad de envío puede verificar la respuesta y autenticar al usuario como el único usuario final con esta tarjeta que puede responder correctamente a la pregunta. Se reconocerá que las operaciones fueron descritas en el contexto de por ejemplo, el internet, pero las operaciones son aplicables igualmente a otros canales de comunicación tales como sistemas de respuesta de voz interactivos o cualquier otro sistema de comunicación adecuado. Por ejemplo, cuando se utiliza respuesta de voz interactiva, un usuario será provisto de la posibilidad de transmitir voz en un sistema de red de telefonía inalámbrica o alámbrica a partir de, por ejemplo, un sistema automatizado. La respuesta de un usuario será provista a través de teclados de toque en lugar de, por ejemplo, introducción en una forma de una web. Puede utilizarse cualquier otro sistema de comunicación adecuado.

Entre otras ventajas, los aparatos, sistemas y métodos descritos proveen autenticación segura tanto del usuario final como de la unidad de envío u organización objetivo y puede ser relativamente fácil de usar y relativamente no costoso para producir y distribuir tal como las tarjetas de autenticación frente a tecnologías más complejas tales como tarjetas inteligentes, instrumentos de hardware o infraestructuras clave públicas. Además, el sistema puede ser implementado fácilmente utilizando clientes en la red a través de canales de comunicaciones múltiples para dispositivos móviles, dispositivos no móviles, y dispositivos activados por voz o cualquier otro dispositivo adecuado.

La figura 28 representa diagramáticamente las operaciones descritas anteriormente. Por ejemplo, como se muestra por la parte de la comunicación 2800, un usuario recibe un número de usuario y una clave de acceso convencionales para ingresar a una pantalla e introduce su nombre de usuario y clave de acceso y la envía como una respuesta de ingreso 2800 a la unidad de envío 2402 la cual lleva a cabo entonces un proceso de autenticación, tal como es conocido en la técnica, comparando la clave de acceso y la identificación del usuario recibidos con los almacenados en la base de datos 2802 de claves de acceso, por ejemplo. Si la validación es exitosa, la unidad de envío 2402 envía una pregunta 2414 a una unidad receptora con, por ejemplo, un identificador de tarjeta de usuario y una pregunta que incluye información de localización de tal forma que el usuario pueda localizar indicios específicos en la tarjeta. Esta pregunta, por ejemplo, es desplegada por parte del usuario en la unidad receptora. El usuario confirma el identificador de tarjeta recibido con el identificador de tarjeta en la tarjeta de autenticación en posesión del usuario y responde la pregunta enviando una respuesta 2416 de regreso a la unidad de envío 2402. Esta respuesta es validad entonces por la unidad de envío para validar al usuario hasta una autenticación mutua completa. Sin embargo, si el segundo nivel de autenticación no es exitoso, la unidad de envío envía repetidamente la misma pregunta, a saber la misma información de localización a la unidad receptora hasta que haya sido recibida una respuesta apropiada.

La descripción anterior detallada de la invención y los ejemplos descritos aquí han sido presentados para propósitos de ilustración y descripción y se entiende que otras variaciones serán reconocidas por los experimentados en la técnica. Por ejemplo, se reconocerá que las diversas operaciones descritas aquí pueden ser distribuidas en una configuración de red de trabajo o sin red. Por ejemplo, pueden llevarse a cabo diferentes operaciones del autenticador, unidades de envío o emisores de TIDM u otras operaciones por parte de una o más servidores de red de terceras partes u otras entidades o dispositivos. También se reconocerán otras variaciones para el aparato y métodos de autenticación del agente de envío.

Por lo tanto se contempla que la presente invención cubre cualquiera y todas las modificaciones, variaciones o equivalentes que caigan dentro del alcance de los principios subyacentes básicos divulgados anteriormente y reivindicados aquí.

REIVINDICACIONES

1. Un método para proveer autenticación mutua entre un usuario y un agente de envío que comprende:

(a) determinar, para un usuario al cual se ha asignado un artículo (14), información de autenticación del agente de envío que corresponda con la información de autenticación del agente de envío que está incorporada en el artículo (14), y en donde la autenticación del agente de envío puede ser localizada en el artículo (14) usando información de localización;

(b) enviar una pregunta para el usuario que incluya al menos información de localización que identifica la información de autenticación del agente de envío deseada;

(c) recibir una respuesta a la pregunta enviada;

(d) determinar si la respuesta recibida a la pregunta incluye la información de autenticación del agente de envío deseada que fue identificada por la información de localización en la pregunta enviada;

(e) si la información de autenticación del agente de envío recibida no es la información de autenticación del agente de envío deseada, entonces reenviar la misma pregunta al usuario que incluya al menos la misma información de localización que fue enviada previamente; y

(f) repetir las etapas (d) y (e) hasta que la respuesta recibida incluya la autenticación del agente de envío deseada, información que está en el artículo (14).

2. El método de la reivindicación 1, en donde el artículo (14) incluya al menos una de una tarjeta de transacción una tarjeta y una tarjeta traslucida.

3. El método de la reivindicación 1, en donde la etapa (f) incluye repetición de las etapas (d) y (e) para cada sesión hasta que la respuesta recibida incluya la información de autenticación de la fuente objetivo deseada que está en el artículo (14).

4. El método de la reivindicación 1, en donde antes de enviar la pregunta, el método incluye:

recibir información (32) de autenticación desde el usuario; y

autenticar el usuario con base en la información (32) de autenticación del usuario recibida y si la autenticación del usuario es exitosa, entonces ejecutar la etapa (a) con base en la información (32) de autenticación del usuario.

5. El método de la reivindicación 1, en donde la información de localización incluye datos trasmitidos electrónicamente para despliegue sobre un dispositivo de pantalla (30).

6. El método de la reivindicación 1, en donde el artículo (14) emitido por el usuario contiene información de autenticación del agente de envío que está dispuesta en filas y columnas.

7. El método de la reivindicación 4, en donde la información (32) de autenticación del usuario incluye un nombre de usuario y una clave de acceso.

8. Un método para proveer autenticación mutua entre un usuario y un agente de envío que comprende:

(a) determinar, para un usuario al que se ha asignado un artículo (14), información de autenticación de usuario deseada que corresponda a la información de autenticación de agente de envío que está incorporada en el artículo (14), y en donde la información de autenticación del agente de envío puede estar localizada sobre el artículo (14) utilizando información de localización;

(b) determinar para el mismo usuario, información de autenticación (34) del artículo correspondiente;

(c) enviar una pregunta para el usuario que incluya al menos información de localización que identifique la información de autenticación del agente de envío deseada y enviar información de identificación del artículo (14) para autenticar el agente de envío al usuario; y

(d) autenticar el usuario con base en una respuesta a la pregunta que incluye información de autenticación del agente de envío obtenida del artículo (14), con base en la información de localización.

9. El método de la reivindicación 8, en donde antes de enviar la pregunta, el método incluye:

recibir información (32) de autenticación del usuario; y

autenticar el usuario con base en la información (32) de autenticación del usuario recibida y si la autenticación del usuario es exitosa, entonces ejecutar las etapas (a) y (b) con base en la información (32) de autenticación del usuario.

10. El método de la reivindicación 8, en donde la información (34) de identificación del artículo incluya al menos una de: un secreto compartido conocido por el usuario y el agente de envío y un número (44) de serie del artículo.

11. Un método para proveer autenticación mutua entre un usuario y un agente de envío que comprende:

requerir información de autenticación de primer nivel de un usuario;

recibir información (32) de identificación del usuario de primer nivel del usuario;

verificar la información (32) de autenticación del usuario de primer nivel recibida;

con base en la información (32) de autenticación del usuario de primer nivel recibida, determinar, para un usuario al que se ha asignado un artículo (14), información de autenticación del agente de envío deseado que corresponda con la información de autenticación del agente de envío que está incorporada en el artículo (14) que ha sido asignada al usuario, y donde la información de autenticación del agente de envío puede ser localizada en el artículo (14) utilizando información de localización;

enviar una pregunta para el usuario que incluya al menos. Información de localización que designa información (32) de autenticación del usuario de segundo nivel localizada en el artículo (14) e información (34) de identificación del artículo para autenticar el agente de envío al usuario;

verificar información (32) de autenticación del usuario de segundo nivel recibida del artículo (14), con base en la información de localización, con información (32) de autenticación del usuario de segundo nivel esperada; y

si la información (32) de autenticación del usuario de segundo nivel no es verificada exitosamente entonces continuar el envío de la misma pregunta electrónica con la misma información (32) de autenticación del usuario de segundo nivel designado localizada sobre el artículo (14) e información (34) de identificación del artículo para autenticar el agente de envío al usuario para una siguiente sesión de usuario hasta que la misma pregunta electrónica sea verificada exitosamente.

12. El método de la reivindicación 11, donde la información (34) de identificación del artículo incluya al menos uno de: un secreto compartido conocido para el usuario y para el agente de envío y un número (44) de serie del artículo.

13. El método de la reivindicación 11, en donde la información (32) de autenticación del usuario de primer nivel incluye información de clave de acceso del usuario e información de identificación del usuario.

14. El método de la reivindicación 11, en donde la información de localización y la información (34) de identificación del artículo incluye datos transmitidos electrónicamente para despliegue sobre un dispositivo de pantalla (30).

15. El método de la reivindicación 11, en donde el artículo (14) emitido al usuario contiene información de autenticación del agente de envío que está dispuesta en filas y columnas.

16. Un dispositivo para proveer autenticación mutua con un usuario que comprende:

uno o más dispositivos de procesamiento; y

una memoria que contiene instrucciones ejecutables que hacen que el uno o más dispositivos de procesamiento:

(a) determinen, para un usuario al que ha sido asignado un artículo (14), información de autenticación del agente de envío deseada que corresponda con información de autenticación del agente de envío que está incorporada en el artículo (14), y en donde la información de autenticación del agente de envío puede ser localizada sobre el artículo (14) utilizando información de localización;

(b) envían una pregunta al usuario que incluye al menos información de localización que identifica la información de autenticación del agente de envío deseada;

(c) determinan si una respuesta recibida a la pregunta incluye la información de autenticación del agente de envío deseada que fue identificada por la información de localización en la pregunta enviada;

(d) si la información de autenticación objetivo recibida no es la información de autenticación del agente de envío deseada, entonces reenvían la misma pregunta para el usuario que incluya al menos la misma información de localización que fue enviada previamente; y

(e) repiten las operaciones (c) y (d) hasta que la respuesta recibida incluya la información de autenticación de fuente objetivo deseada que está en el artículo (14).

17. El dispositivo de la reivindicación 16, en donde la memoria incluye instrucciones que hacen que uno o más dispositivos de procesamiento, antes de enviar la pregunta, autentiquen el usuario con base en la información de autenticación de usuario recibida (32) y si la autenticación del usuario es exitosa, entonces la ejecute la operación (a) con base en la información (32) de autenticación del usuario.

18. El dispositivo de la reivindicación 16, en donde la información de localización incluye datos transmitidos electrónicamente para despliegue sobre un dispositivo de pantalla (30).

19. El dispositivo de la reivindicación 16, en donde la información (32) de autenticación del usuario incluye un nombre de usuario y una clave de acceso.

20. Un dispositivo para proveer autenticación mutua con un usuario que comprende:

uno o más dispositivos de procesamiento; y

una memoria que contiene instrucciones ejecutables que hacen que el uno o más dispositivos de procesamiento:

(a) determinen, para un usuario al que se ha asignado un artículo (14), información de autenticación del agente de envío deseada que corresponda con la información de autenticación del agente de envío que está incorporada en el artículo (14), y en donde la información de autenticación del agente de envío puede ser localizada sobre el artículo (14) utilizando información de localización;

(b) determinan para el mismo usuario, información de identificación del artículo (14) correspondiente;

(c) envían una pregunta para el usuario que incluya al menos información que identifica la información de autenticación del agente de envío deseada para autenticar el agente de envío para el usuario y enviar la información de identificación del artículo (14) para autenticar el agente de envío al usuario; y

(d) autenticar el usuario con base en una respuesta a la pregunta que incluya información (32) de autenticación del usuario obtenida del artículo (14), con base en la información de localización.

21. El dispositivo de la reivindicación 20, en donde la información (34) de identificación del artículo incluye al menos uno de: un secreto compartido conocido por el usuario y por el dispositivo y un número (44) de serie del artículo.

22. Un dispositivo para proveer autenticación mutua con un usuario que comprende:

uno o más dispositivos de procesamiento; y

memoria que contiene instrucciones ejecutables que hacen que uno o más dispositivos de procesamiento:

envíen una solicitud de instrucciones para información de autenticación de primer nivel del usuario;

verifiquen la información (32) de autenticación de primer nivel del usuario que fue recibida en respuesta al requerimiento de instrucciones;

con base en la primera información (32) de autenticación de primer nivel del usuario, determinar, para el usuario al que se ha asignado un artículo (14) información de autenticación del agente de envío deseada que corresponda con la información de autenticación del agente de envío que está incorporada en el artículo (14) que ha sido asignado al

usuario, y en donde la información de autenticación del agente de envío puede ser localizada en el artículo (14) utilizando información de localización;

enviar una pregunta para el usuario que incluya al menos: información de localización que designa información (32) de autenticación de segundo nivel del usuario localizada en el artículo (14) e información de identificación del artículo (14) para autenticar el agente de envío al usuario;

verifican la información (32) de autenticación de segundo nivel del usuario obtenida en el artículo (14) con base en la información de localización, con la información (32) de autenticación de segundo nivel del usuario esperada; y

si la información (32) de autenticación de segundo nivel del usuario no se verifica exitosamente, entonces continúan con el envío de la misma pregunta electrónica con la misma información (32) de autenticación del usuario de segundo nivel localizada en el artículo (14) y la información (34) de identificación del artículo para autenticar el agente de envío al usuario para una siguiente sesión de usuario hasta que la misma pregunta electrónica sea verificada exitosamente.

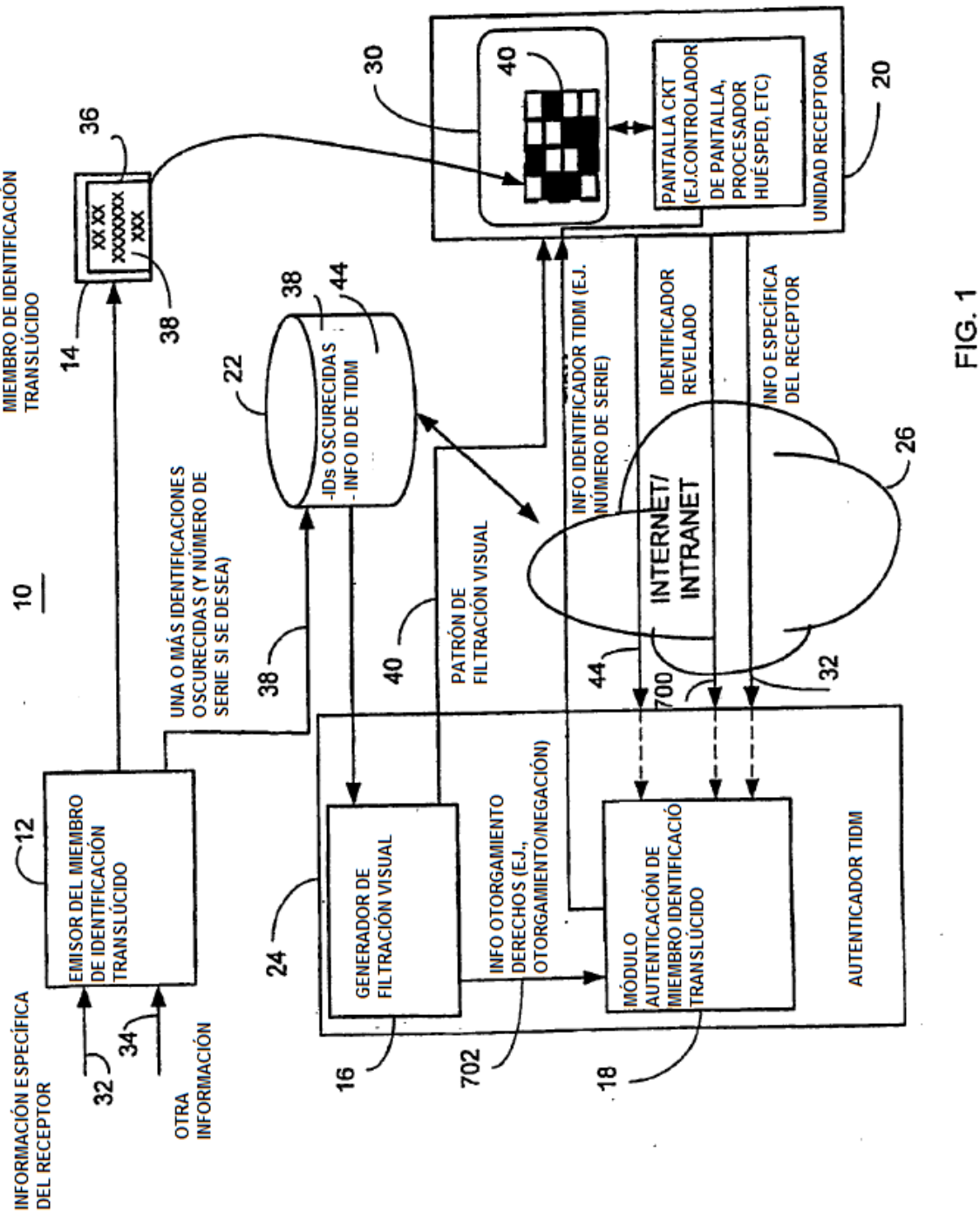

MIEMBRO DE IDENTIFICACIÓN TRANSLÚCIDO
36
XX XX
XXXXXXX
XXX
38
14
10
30
40
PANTALLA CKT (EJ.CONTROLADOR DE PANTALLA, PROCESADOR HUÉSPED, ETC)
UNIDAD RECEPTORA
20
22
38
44
-IDs OSCURECIDAS
- INFO ID DE TIDM
INFO IDENTIFICADOR TIDM (EJ. NÚMERO DE SERIE)
IDENTIFICADOR REVELADO
INFO ESPECÍFICA DEL RECEPTOR
INTERNET/ INTRANET
26
UNA O MÁS IDENTIFICACIONES OSCURECIDAS (Y NÚMERO DE SERIE SI SE DESEA)
38
40
PATRÓN DE FILTRACIÓN VISUAL
44
700
32
12
EMISOR DEL MIEMBRO DE IDENTIFICACIÓN TRANSLÚCIDO
24
GENERADOR DE FILTRACIÓN VISUAL
INFO OTORGAMIENTO DERECHOS (EJ., OTORGAMIENTO/NEGACIÓN)
MÓDULO AUTENTICACIÓN DE MIEMBRO IDENTIFICACIÓ TRANSLÚCIDO
AUTENTICADOR TIDM
INFORMACIÓN ESPECÍFICA DEL RECEPTOR
32
34
OTRA INFORMACIÓN
16
702
18

FIG. 1

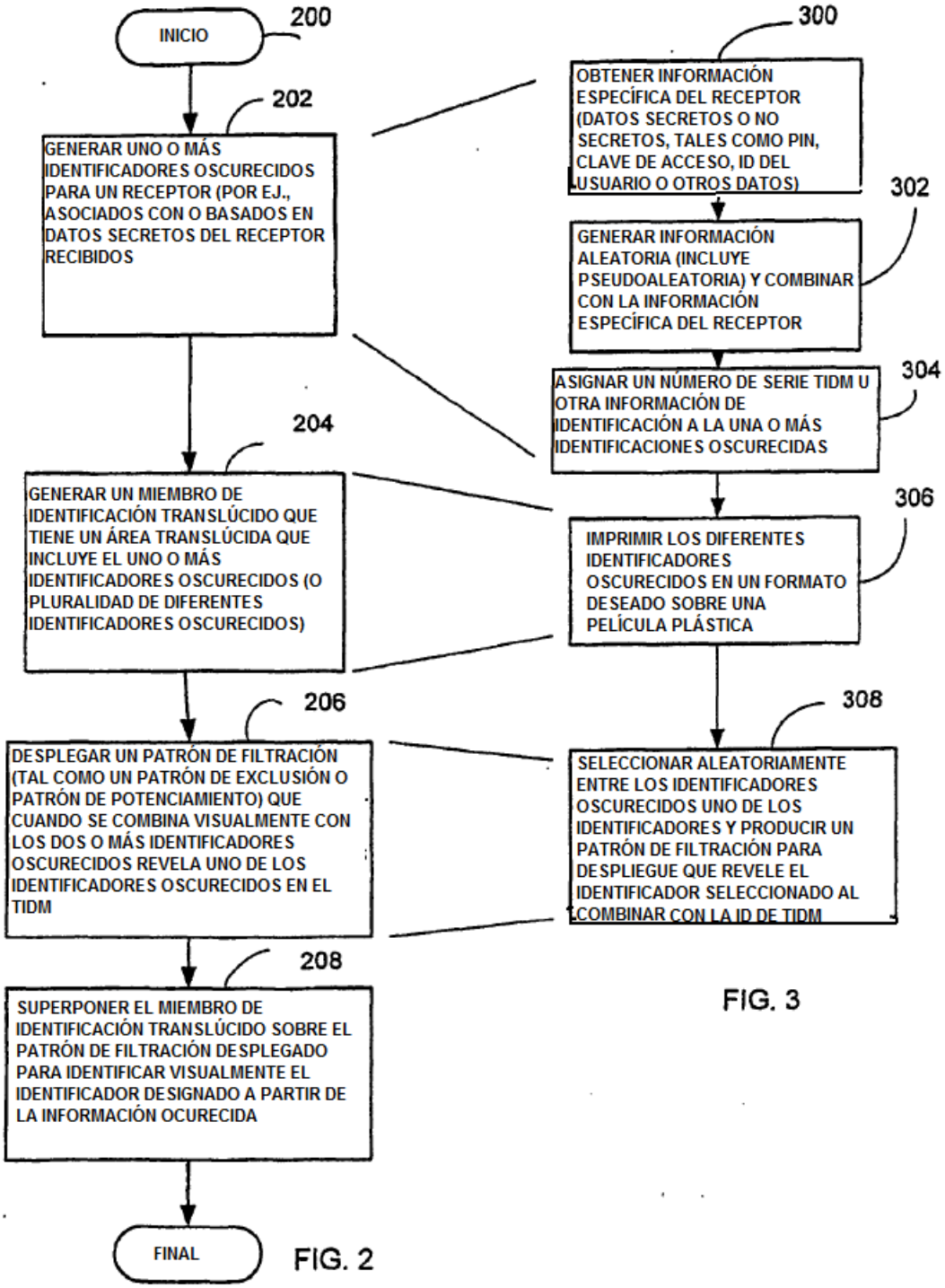

INICIO
200
202
GENERAR UNO O MÁS IDENTIFICADORES OSCURECIDOS PARA UN RECEPTOR (POR EJ., ASOCIADOS CON O BASADOS EN DATOS SECRETOS DEL RECEPTOR RECIBIDOS
204
GENERAR UN MIEMBRO DE IDENTIFICACIÓN TRANSLÚCIDO QUE TIENE UN ÁREA TRANSLÚCIDA QUE INCLUYE EL UNO O MÁS IDENTIFICADORES OSCURECIDOS (O PLURALIDAD DE DIFERENTES IDENTIFICADORES OSCURECIDOS)
206
DESPLEGAR UN PATRÓN DE FILTRACIÓN (TAL COMO UN PATRÓN DE EXCLUSIÓN O PATRÓN DE POTENCIAMIENTO) QUE CUANDO SE COMBINA VISUALMENTE CON LOS DOS O MÁS IDENTIFICADORES OSCURECIDOS REVELA UNO DE LOS IDENTIFICADORES OSCURECIDOS EN EL TIDM
208
SUPERPONER EL MIEMBRO DE IDENTIFICACIÓN TRANSLÚCIDO SOBRE EL PATRÓN DE FILTRACIÓN DESPLEGADO PARA IDENTIFICAR VISUALMENTE EL IDENTIFICADOR DESIGNADO A PARTIR DE LA INFORMACIÓN OCURECIDA
FINAL
300
OBTENER INFORMACIÓN ESPECÍFICA DEL RECEPTOR (DATOS SECRETOS O NO SECRETOS, TALES COMO PIN, CLAVE DE ACCESO, ID DEL USUARIO O OTROS DATOS)
302
GENERAR INFORMACIÓN ALEATORIA (INCLUYE PSEUDOALEATORIA) Y COMBINAR CON LA INFORMACIÓN ESPECÍFICA DEL RECEPTOR
304
ASIGNAR UN NÚMERO DE SERIE TIDM U OTRA INFORMACIÓN DE IDENTIFICACIÓN A LA UNA O MÁS IDENTIFICACIONES OSCURECIDAS
306
IMPRIMIR LOS DIFERENTES IDENTIFICADORES OSCURECIDOS EN UN FORMATO DESEADO SOBRE UNA PELÍCULA PLÁSTICA
308
SELECCIONAR ALEATORIAMENTE ENTRE LOS IDENTIFICADORES OSCURECIDOS UNO DE LOS IDENTIFICADORES Y PRODUCIR UN PATRÓN DE FILTRACIÓN PARA DESPLIEGUE QUE REVELE EL IDENTIFICADOR SELECCIONADO AL COMBINAR CON LA ID DE TIDM

FIG. 2

FIG. 3

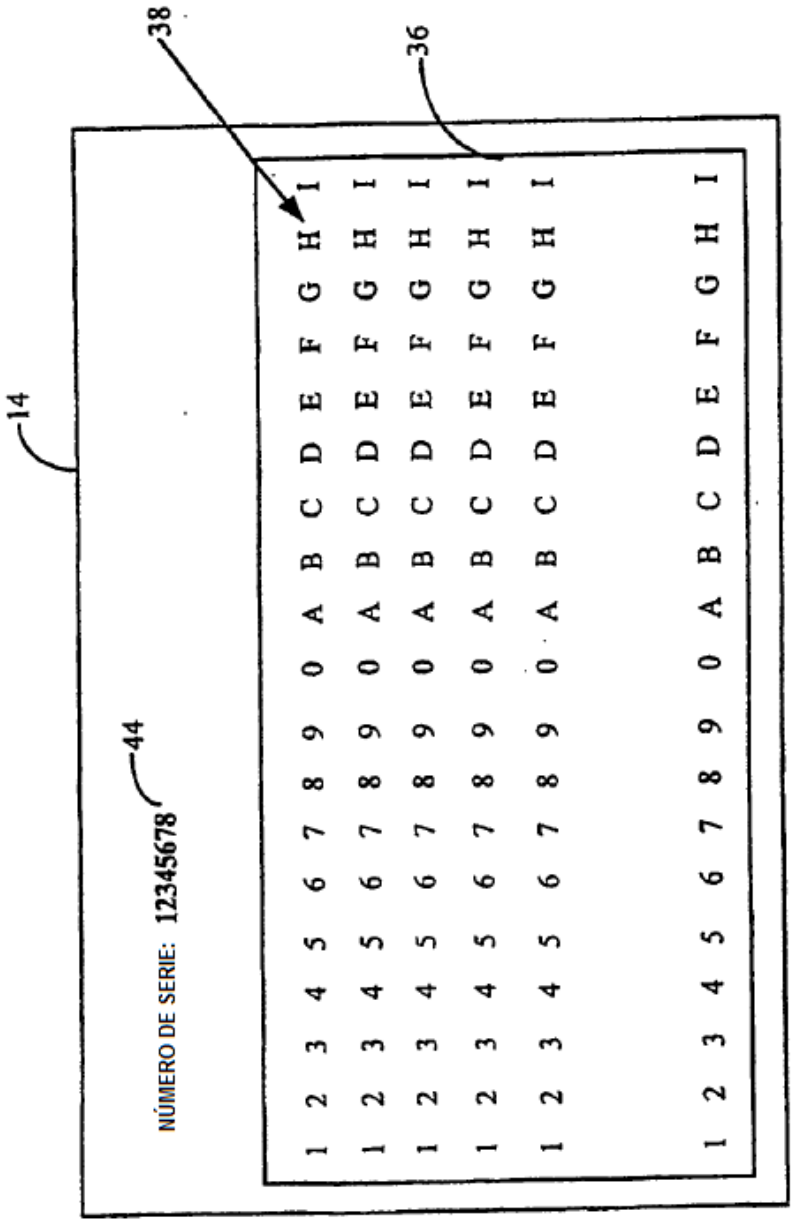


FIG. 4

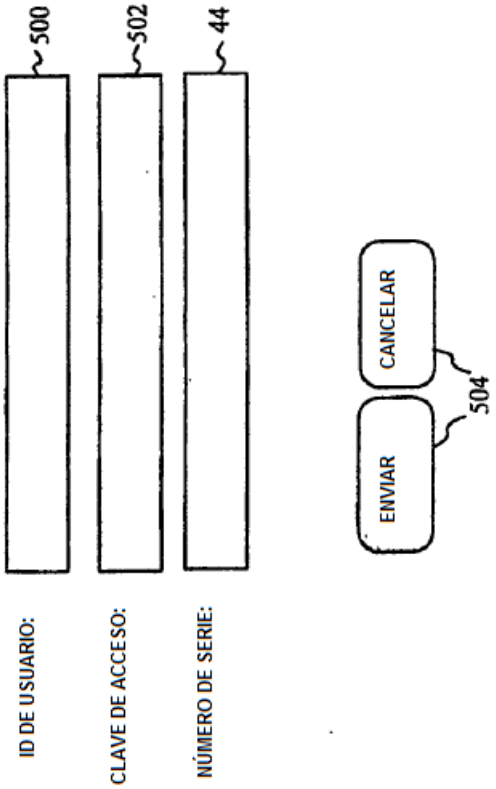

500
502
44
ID DE USUARIO:
CLAVE DE ACCESO:
NÚMERO DE SERIE:
CANCELAR
ENVIAR
504

FIG. 5

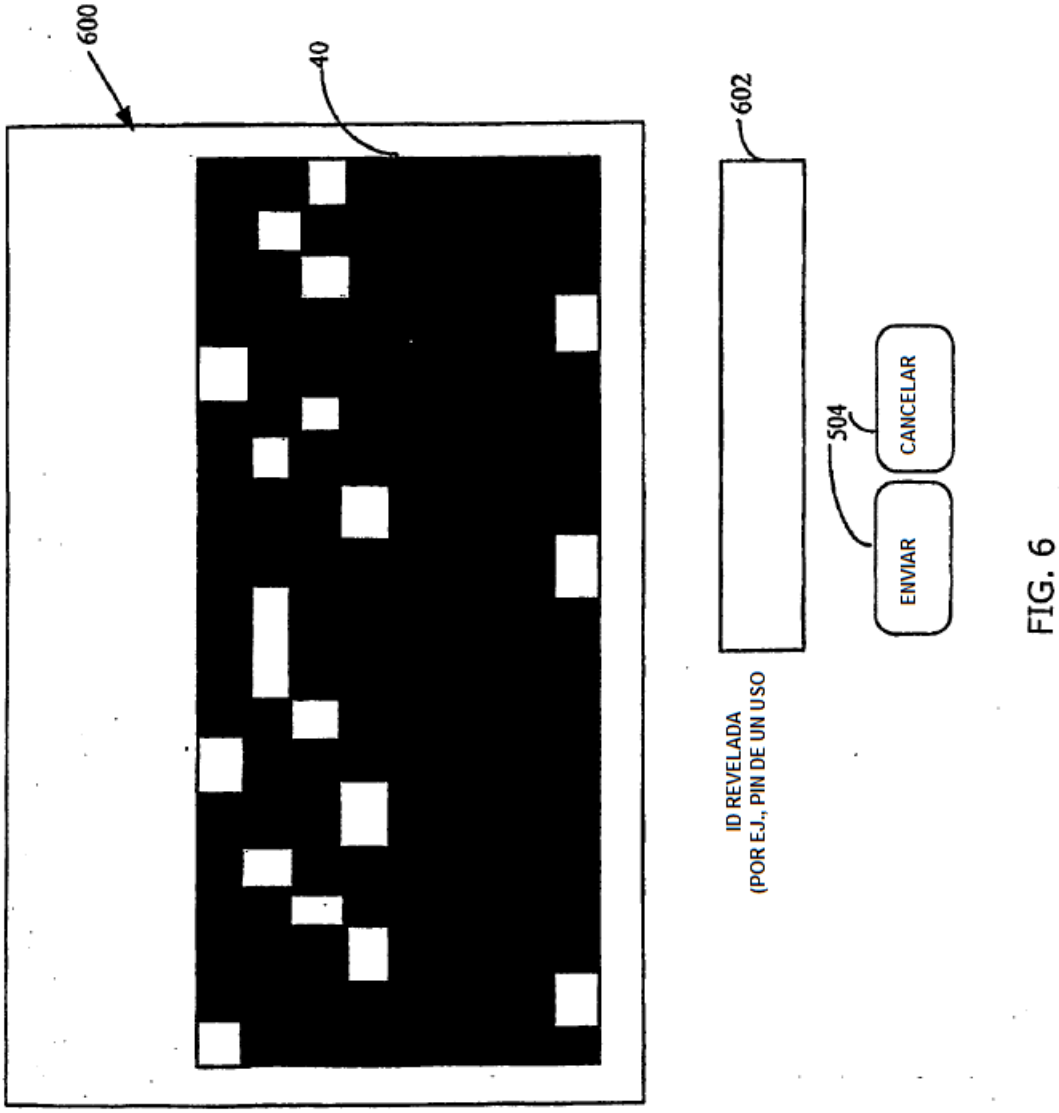

600
40
602
504
CANCELAR
ENVIAR
ID REVELADA
(POR EJ., PIN DE UN USO

FIG. 6

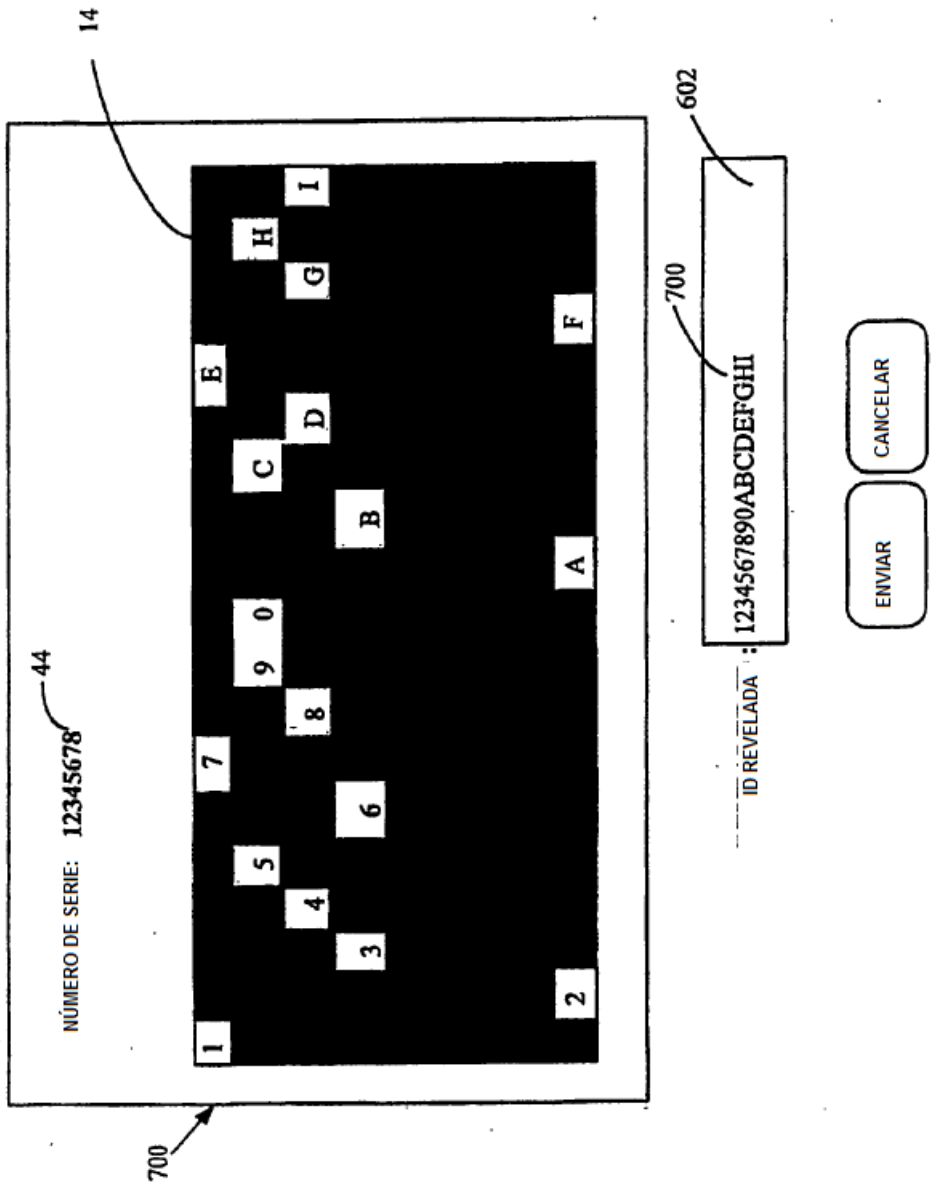

14
602
700
44
NÚMERO DE SERIE: 12345678
ID REVELADA
1234567890ABCDEFGHI
ENVIAR
CANCELAR
700

FIG. 7

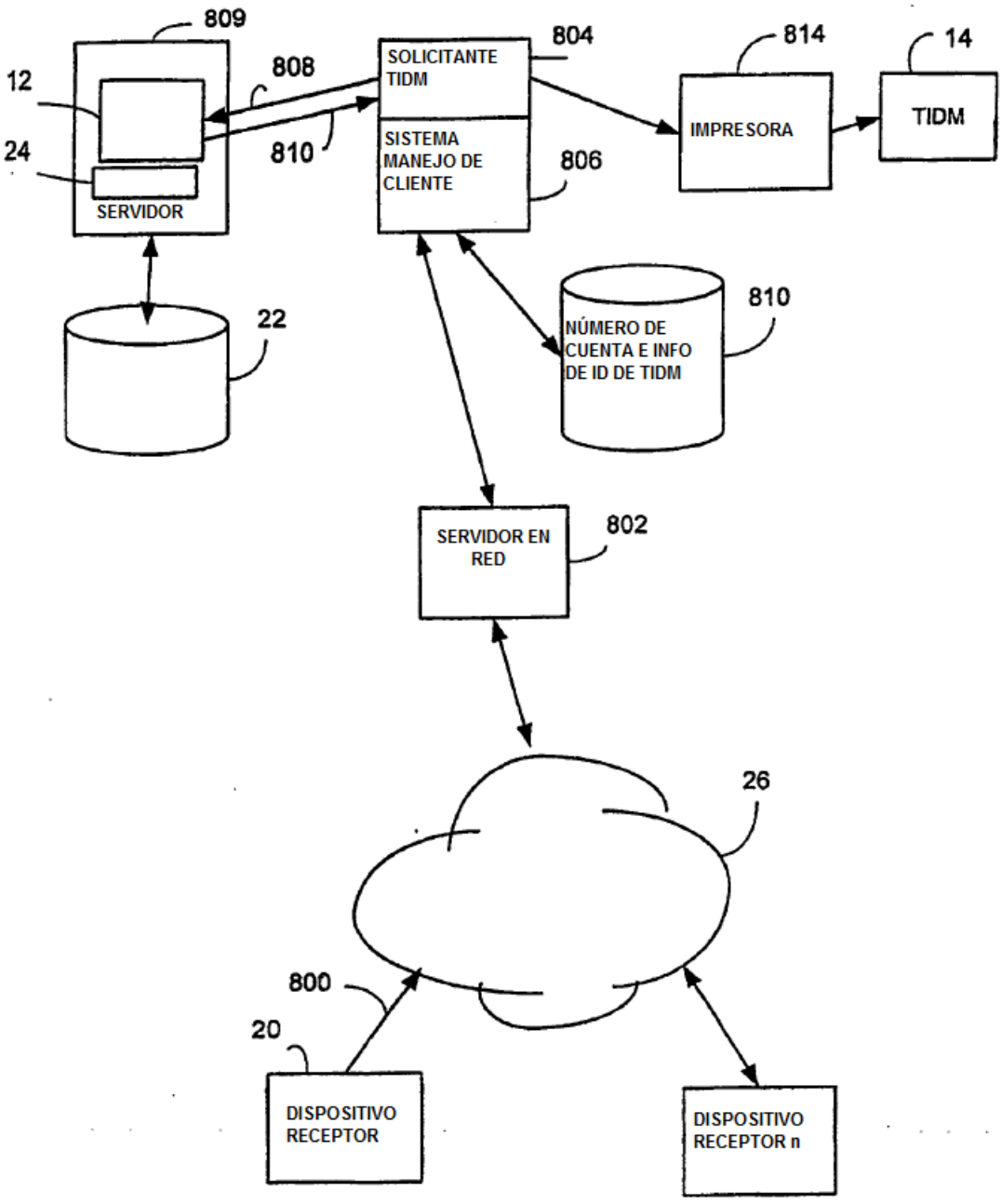

809
12
24
SERVIDOR
808
810
SOLICITANTE TIDM
804
SISTEMA MANEJO DE CLIENTE
806
814
IMPRESORA
14
TIDM
22
NÚMERO DE CUENTA E INFO DE ID DE TIDM
810
SERVIDOR EN RED
802
26
800
20
DISPOSITIVO RECEPTOR
DISPOSITIVO RECEPTOR n

FIG. 8

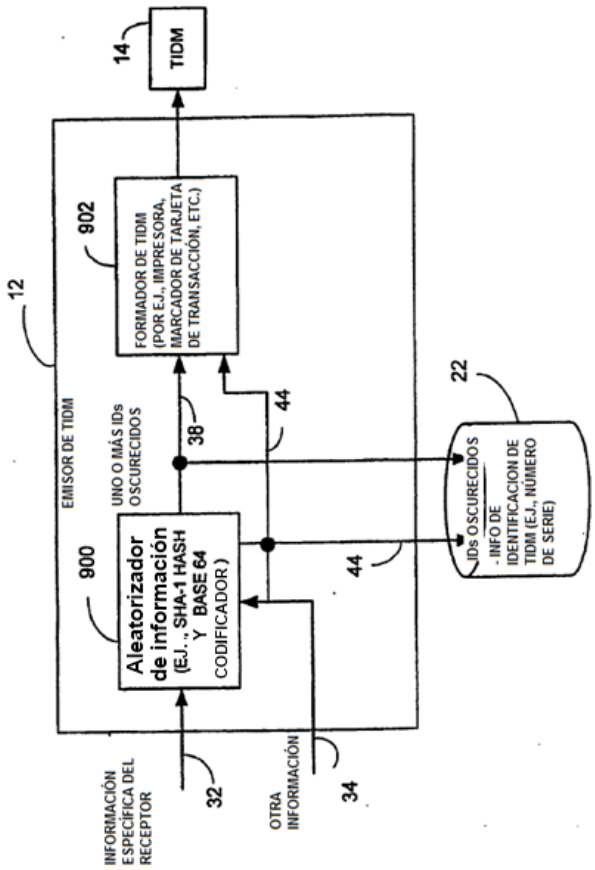

14
TIDM
12
902
FORMADOR DE TIDM (POR E.J., IMPRESORA, MARCADOR DE TARJETA DE TRANSACCIÓN, ETC.)
EMISOR DE TIDM
UNO O MÁS IDs OSCURECIDOS
38
44
22
900
Aleatorizador de información (E.J., SHA-1 HASH Y BASE 64 CODIFICADOR)
IDs OSCURECIDOS - INFO DE IDENTIFICACION DE TIDM (E.J., NÚMERO DE SERIE)
44
INFORMACIÓN ESPECÍFICA DEL RECEPTOR
32
OTRA INFORMACIÓN
34

FIG. 9

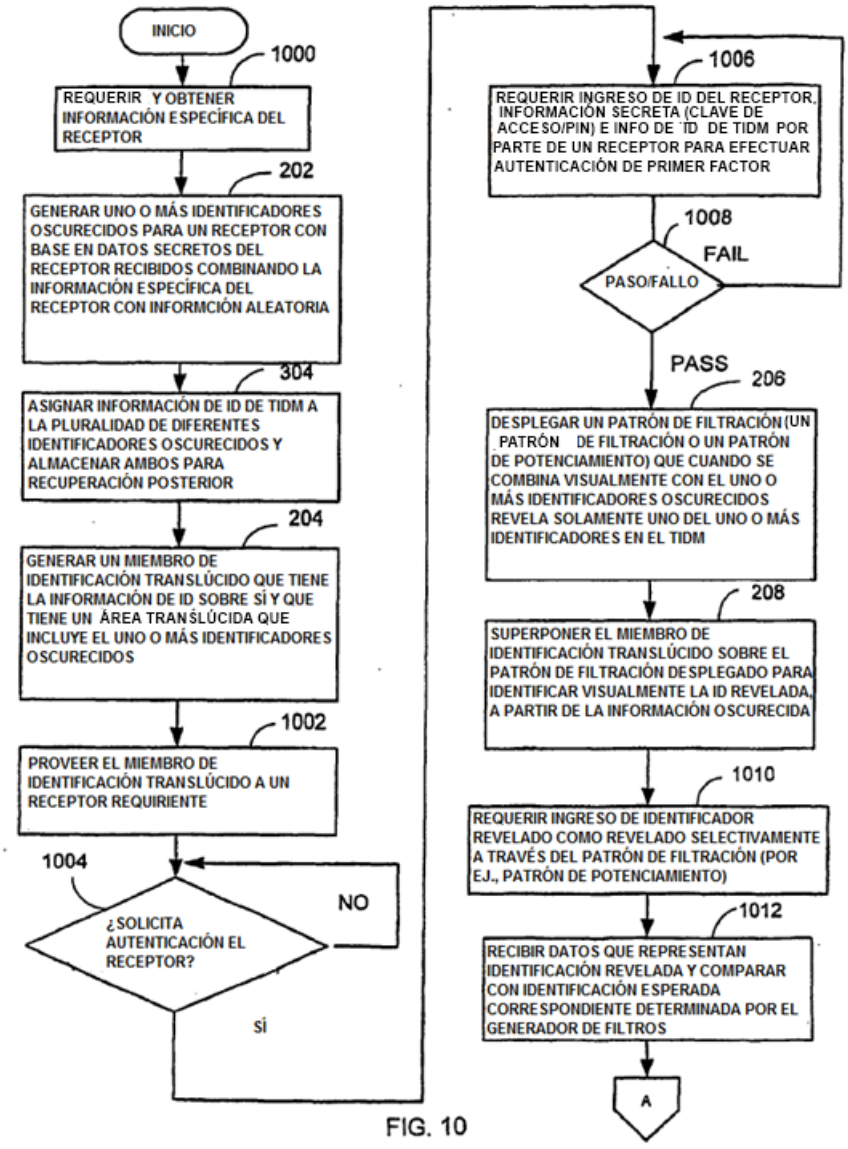

INICIO
1000
REQUERIR Y OBTENER INFORMACIÓN ESPECÍFICA DEL RECEPTOR
202
GENERAR UNO O MÁS IDENTIFICADORES OSCURECIDOS PARA UN RECEPTOR CON BASE EN DATOS SECRETOS DEL RECEPTOR RECIBIDOS COMBINANDO LA INFORMACIÓN ESPECÍFICA DEL RECEPTOR CON INFORMCIÓN ALEATORIA
304
ASIGNAR INFORMACIÓN DE ID DE TIDM A LA PLURALIDAD DE DIFERENTES IDENTIFICADORES OSCURECIDOS Y ALMACENAR AMBOS PARA RECUPERACIÓN POSTERIOR
204
GENERAR UN MIEMBRO DE IDENTIFICACIÓN TRANSLÚCIDO QUE TIENE LA INFORMACIÓN DE ID SOBRE SÍ Y QUE TIENE UN ÁREA TRANSLÚCIDA QUE INCLUYE EL UNO O MÁS IDENTIFICADORES OSCURECIDOS
1002
PROVEER EL MIEMBRO DE IDENTIFICACIÓN TRANSLÚCIDO A UN RECEPTOR REQUIRIENTE
1004
¿SOLICITA AUTENTICACIÓN EL RECEPTOR?
NO
SÍ
1006
REQUERIR INGRESO DE ID DEL RECEPTOR, INFORMACIÓN SECRETA (CLAVE DE ACCESO/PIN) E INFO DE ID DE TIDM POR PARTE DE UN RECEPTOR PARA EFECTUAR AUTENTICACIÓN DE PRIMER FACTOR
1008
PASO/FALLO
FAIL
PASS
206
DESPLEGAR UN PATRÓN DE FILTRACIÓN (UN PATRÓN DE FILTRACIÓN O UN PATRÓN DE POTENCIAMIENTO) QUE CUANDO SE COMBINA VISUALMENTE CON EL UNO O MÁS IDENTIFICADORES OSCURECIDOS REVELA SOLAMENTE UNO DEL UNO O MÁS IDENTIFICADORES EN EL TIDM
208
SUPERPONER EL MIEMBRO DE IDENTIFICACIÓN TRANSLÚCIDO SOBRE EL PATRÓN DE FILTRACIÓN DESPLEGADO PARA IDENTIFICAR VISUALMENTE LA ID REVELADA, A PARTIR DE LA INFORMACIÓN OSCURECIDA
1010
REQUERIR INGRESO DE IDENTIFICADOR REVELADO COMO REVELADO SELECTIVAMENTE A TRAVÉS DEL PATRÓN DE FILTRACIÓN (POR EJ., PATRÓN DE POTENCIAMIENTO)
1012
RECIBIR DATOS QUE REPRESENTAN IDENTIFICACIÓN REVELADA Y COMPARAR CON IDENTIFICACIÓN ESPERADA CORRESPONDIENTE DETERMINADA POR EL GENERADOR DE FILTROS
A

FIG. 10

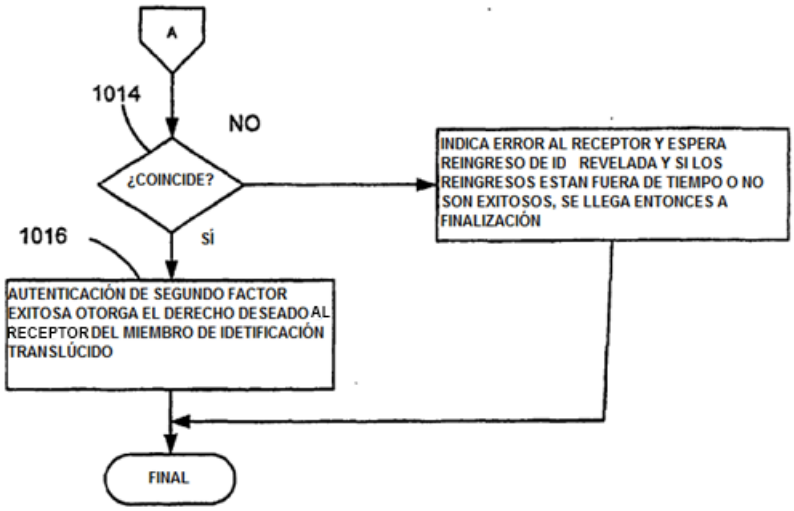

A
1014
NO
¿COINCIDE?
INDICA ERROR AL RECEPTOR Y ESPERA REINGRESO DE ID REVELADA Y SI LOS REINGRESOS ESTAN FUERA DE TIEMPO O NO SON EXITOSOS, SE LLEGA ENTONCES A FINALIZACIÓN
1016
SÍ
AUTENTICACIÓN DE SEGUNDO FACTOR EXITOSA OTORGA EL DERECHO DESEADO AL RECEPTOR DEL MIEMBRO DE IDETIFICACIÓN TRANSLÚCIDO
FINAL

FIG. 11

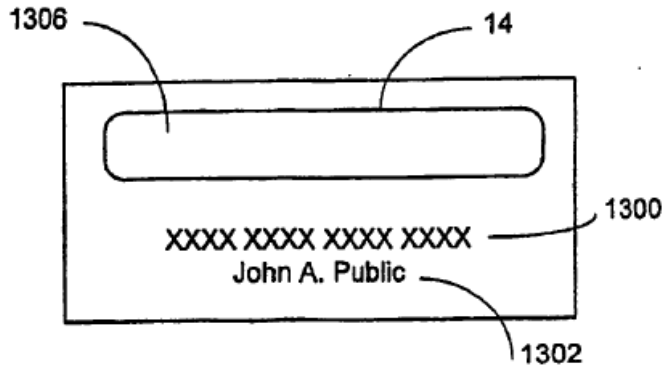

1306
14
1300
XXXX XXXX XXXX XXXX
John A. Public
1302

FIG. 12

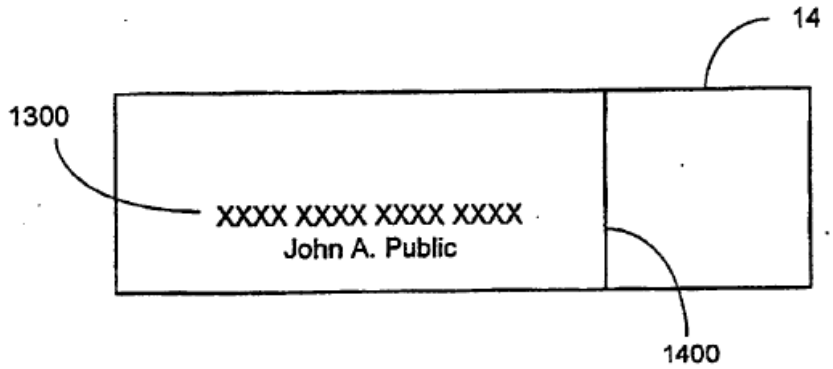

14
1300
XXXX XXXX XXXX XXXX
John A. Public
1400

FIG. 13

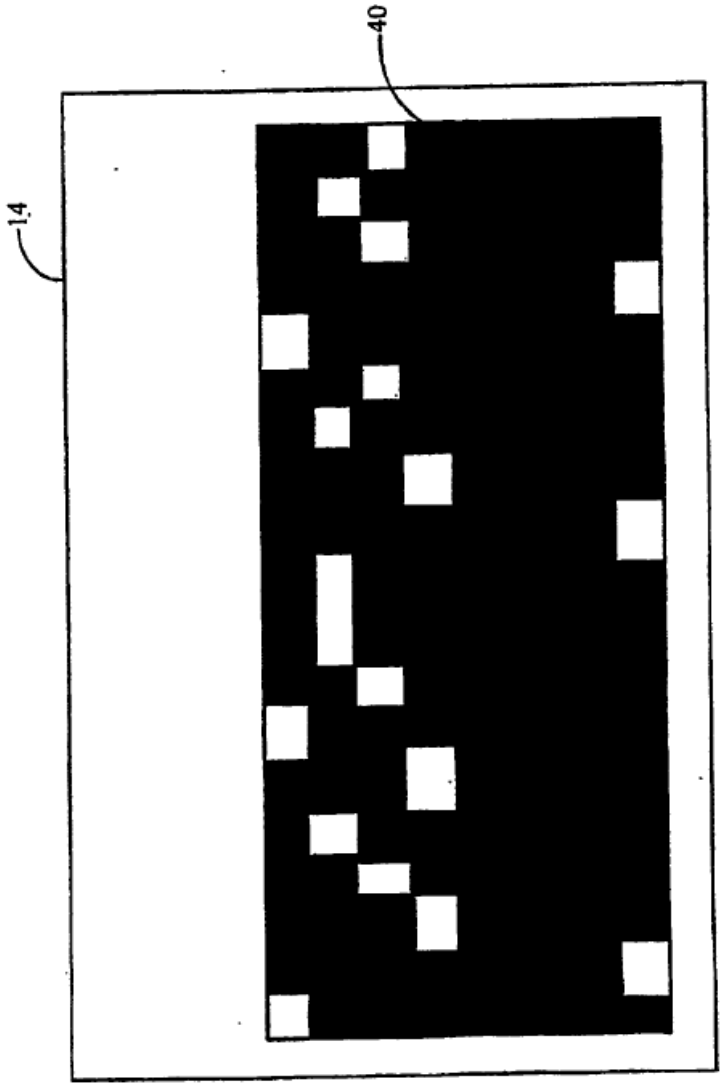


FIG. 14

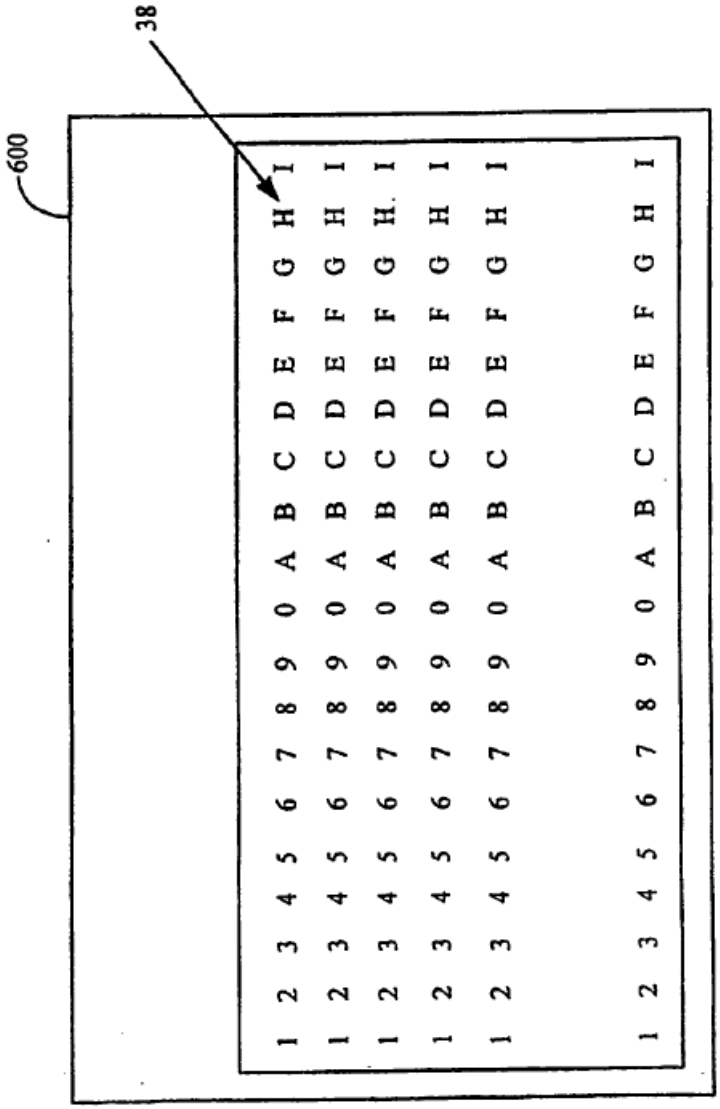

600
38
1 2 3 4 5 6 7 8 9 0 A B C D E F G H I
1 2 3 4 5 6 7 8 9 0 A B C D E F G H I
1 2 3 4 5 6 7 8 9 0 A B C D E F G H I
1 2 3 4 5 6 7 8 9 0 A B C D E F G H I
1 2 3 4 5 6 7 8 9 0 A B C D E F G H I

FIG. 15

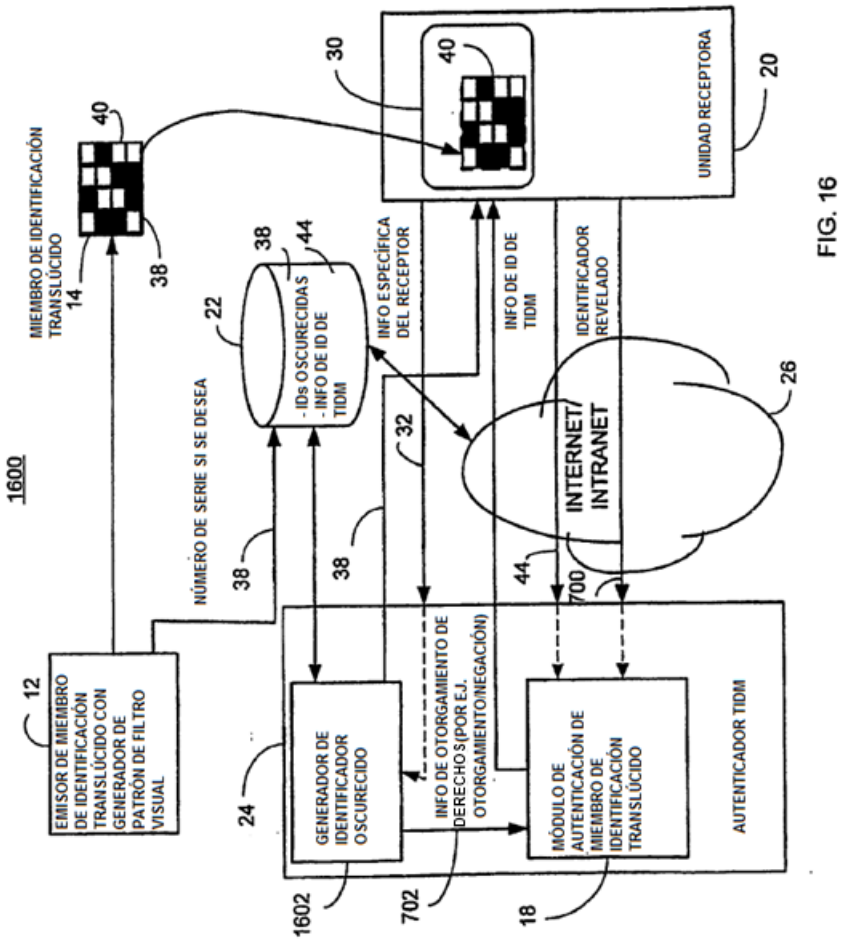

1600
MIEMBRO DE IDENTIFICACIÓN TRANSLÚCIDO
14
40
38
30
40
UNIDAD RECEPTORA
20
22
38
44
- IDs OSCURECIDAS
- INFO DE ID DE TIDM
INFO ESPECÍFICA DEL RECEPTOR
INFO DE ID DE TIDM
IDENTIFICADOR REVELADO
26
INTERNET/ INTRANET
32
NÚMERO DE SERIE SI SE DESEA
38
38
44
700
12
EMISOR DE MIEMBRO DE IDENTIFICACIÓN TRANSLÚCIDO CON GENERADOR DE PATRÓN DE FILTRO VISUAL
24
GENERADOR DE IDENTIFICADOR OSCURECIDO
INFO DE OTORGAMIENTO DE DERECHOS (POR EJ. OTORGAMIENTO/NEGACIÓN)
MÓDULO DE AUTENTICACIÓN DE MIEMBRO DE IDENTIFICACIÓN TRANSLÚCIDO
AUTENTICADOR TIDM
1602
702
18

FIG. 16

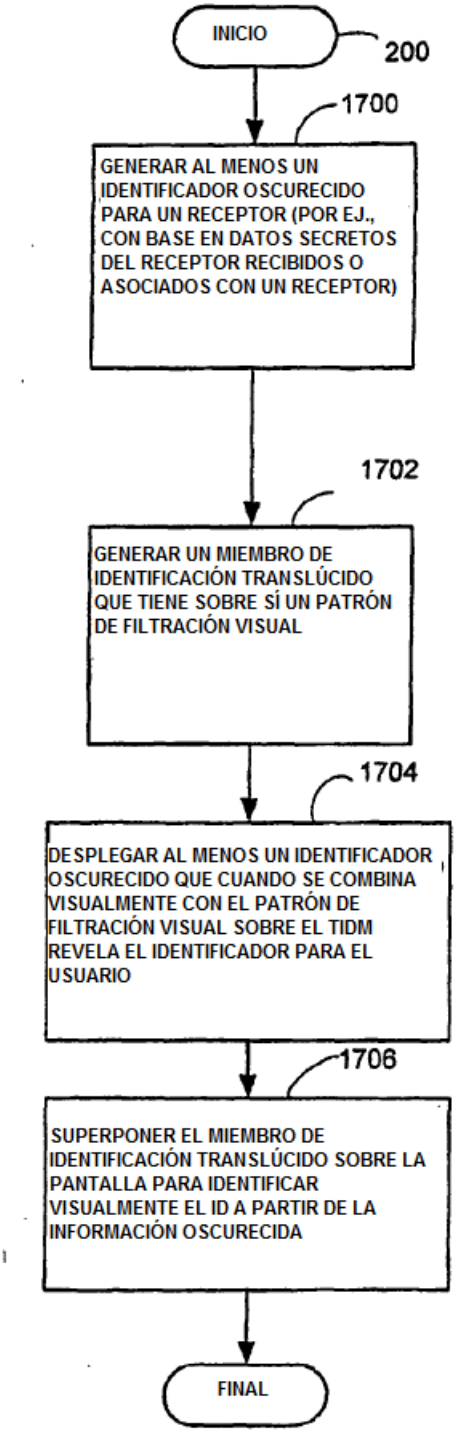

INICIO
200
1700
GENERAR AL MENOS UN IDENTIFICADOR OSCURECIDO PARA UN RECEPTOR (POR EJ., CON BASE EN DATOS SECRETOS DEL RECEPTOR RECIBIDOS O ASOCIADOS CON UN RECEPTOR)
1702
GENERAR UN MIEMBRO DE IDENTIFICACIÓN TRANSLÚCIDO QUE TIENE SOBRE SÍ UN PATRÓN DE FILTRACIÓN VISUAL
1704
DESPLEGAR AL MENOS UN IDENTIFICADOR OSCURECIDO QUE CUANDO SE COMBINA VISUALMENTE CON EL PATRÓN DE FILTRACIÓN VISUAL SOBRE EL TIDM REVELA EL IDENTIFICADOR PARA EL USUARIO
1706
SUPERPONER EL MIEMBRO DE IDENTIFICACIÓN TRANSLÚCIDO SOBRE LA PANTALLA PARA IDENTIFICAR VISUALMENTE EL ID A PARTIR DE LA INFORMACIÓN OSCURECIDA
FINAL

FIG. 17

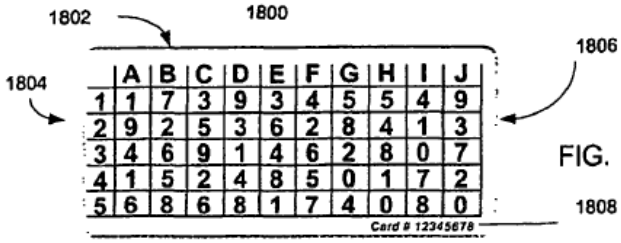


FIG. 18

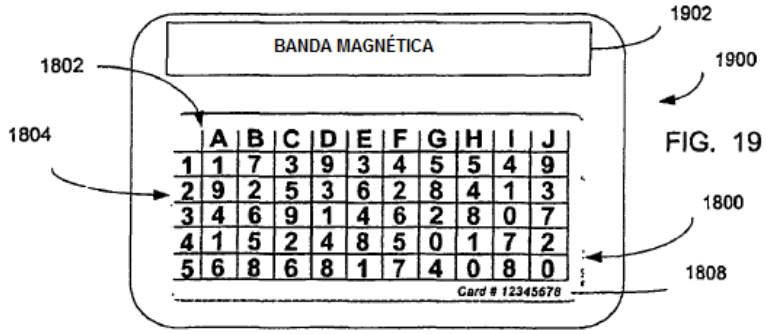


FIG. 19

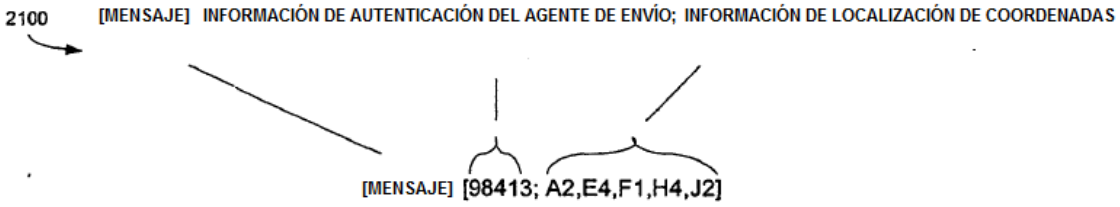


FIG. 21

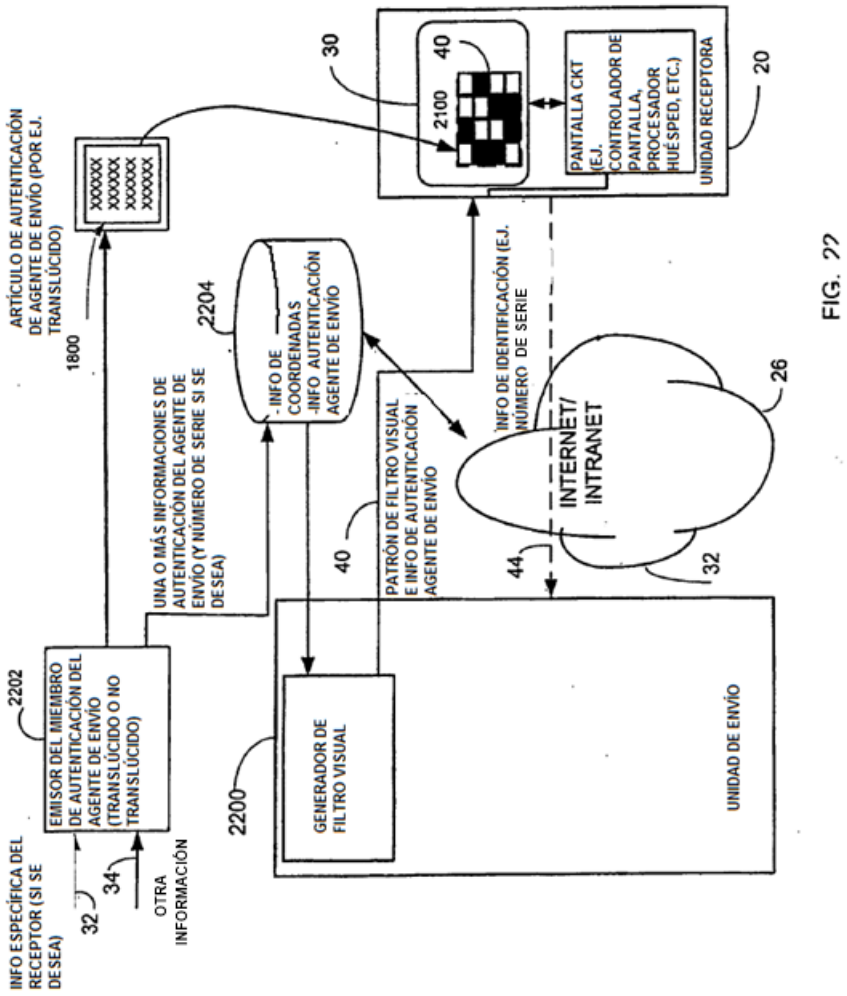

ARTÍCULO DE AUTENTICACIÓN DE AGENTE DE ENVÍO (POR EJ. TRANSLÚCIDO)
1800
XXXXXX
XXXXXX
XXXXXX
XXXXXX
30
2100
40
PANTALLA CKT (EJ. CONTROLADOR DE PANTALLA, PROCESADOR HUÉSPED, ETC.)
UNIDAD RECEPTORA
20
2204
INFO DE COORDENADAS -INFO AUTENTICACIÓN AGENTE DE ENVÍO
INFO DE IDENTIFICACIÓN (EJ. NÚMERO DE SERIE
INTERNET/ INTRANET
26
UNA O MÁS INFORMACIONES DE AUTENTICACIÓN DEL AGENTE DE ENVÍO (Y NÚMERO DE SERIE SI SE DESEA)
PATRÓN DE FILTRO VISUAL E INFO DE AUTENTICACIÓN AGENTE DE ENVÍO
40
44
32
2202
EMISOR DEL MIEMBRO DE AUTENTICACIÓN DEL AGENTE DE ENVÍO (TRANSLÚCIDO O NO TRANSLÚCIDO)
2200
GENERADOR DE FILTRO VISUAL
UNIDAD DE ENVÍO
INFO ESPECÍFICA DEL RECEPTOR (SI SE DESEA)
32
34
OTRA INFORMACIÓN

FIG. 22

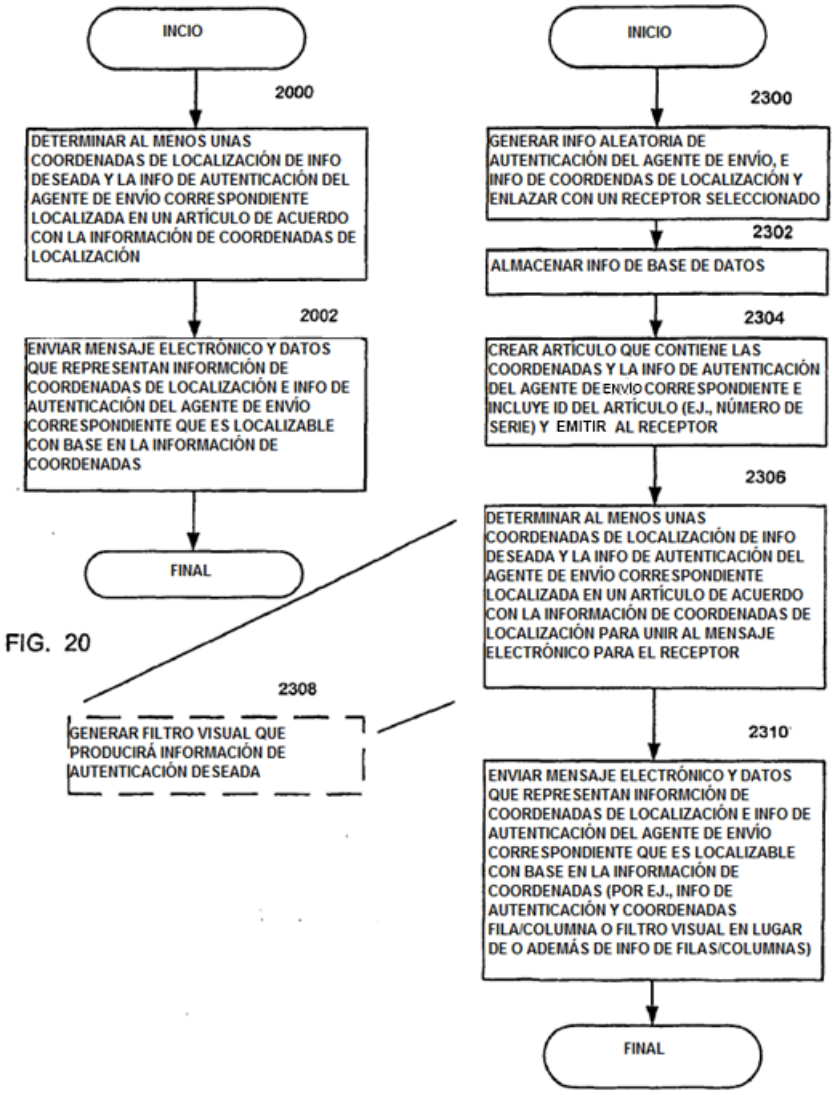

INCIO
2000
DETERMINAR AL MENOS UNAS COORDENADAS DE LOCALIZACIÓN DE INFO DESEADA Y LA INFO DE AUTENTICACIÓN DEL AGENTE DE ENVÍO CORRESPONDIENTE LOCALIZADA EN UN ARTÍCULO DE ACUERDO CON LA INFORMACIÓN DE COORDENADAS DE LOCALIZACIÓN
2002
ENVIAR MENSAJE ELECTRÓNICO Y DATOS QUE REPRESENTAN INFORMCIÓN DE COORDENADAS DE LOCALIZACIÓN E INFO DE AUTENTICACIÓN DEL AGENTE DE ENVÍO CORRESPONDIENTE QUE ES LOCALIZABLE CON BASE EN LA INFORMACIÓN DE COORDENADAS
FINAL
INICIO
2300
GENERAR INFO ALEATORIA DE AUTENTICACIÓN DEL AGENTE DE ENVÍO, E INFO DE COORDENDAS DE LOCALIZACIÓN Y ENLAZAR CON UN RECEPTOR SELECCIONADO
2302
ALMACENAR INFO DE BASE DE DATOS
2304
CREAR ARTÍCULO QUE CONTIENE LAS COORDENADAS Y LA INFO DE AUTENTICACIÓN DEL AGENTE DE ENVÍO CORRESPONDIENTE E INCLUYE ID DEL ARTÍCULO (EJ., NÚMERO DE SERIE) Y EMITIR AL RECEPTOR
2306
DETERMINAR AL MENOS UNAS COORDENADAS DE LOCALIZACIÓN DE INFO DESEADA Y LA INFO DE AUTENTICACIÓN DEL AGENTE DE ENVÍO CORRESPONDIENTE LOCALIZADA EN UN ARTÍCULO DE ACUERDO CON LA INFORMACIÓN DE COORDENADAS DE LOCALIZACIÓN PARA UNIR AL MENSAJE ELECTRÓNICO PARA EL RECEPTOR
2308
GENERAR FILTRO VISUAL QUE PRODUCIRÁ INFORMACIÓN DE AUTENTICACIÓN DESEADA
2310
ENVIAR MENSAJE ELECTRÓNICO Y DATOS QUE REPRESENTAN INFORMCIÓN DE COORDENADAS DE LOCALIZACIÓN E INFO DE AUTENTICACIÓN DEL AGENTE DE ENVÍO CORRESPONDIENTE QUE ES LOCALIZABLE CON BASE EN LA INFORMACIÓN DE COORDENADAS (POR EJ., INFO DE AUTENTICACIÓN Y COORDENADAS FILA/COLUMNA O FILTRO VISUAL EN LUGAR DE O ADEMÁS DE INFO DE FILAS/COLUMNAS)
FINAL

FIG. 20

FIG. 23

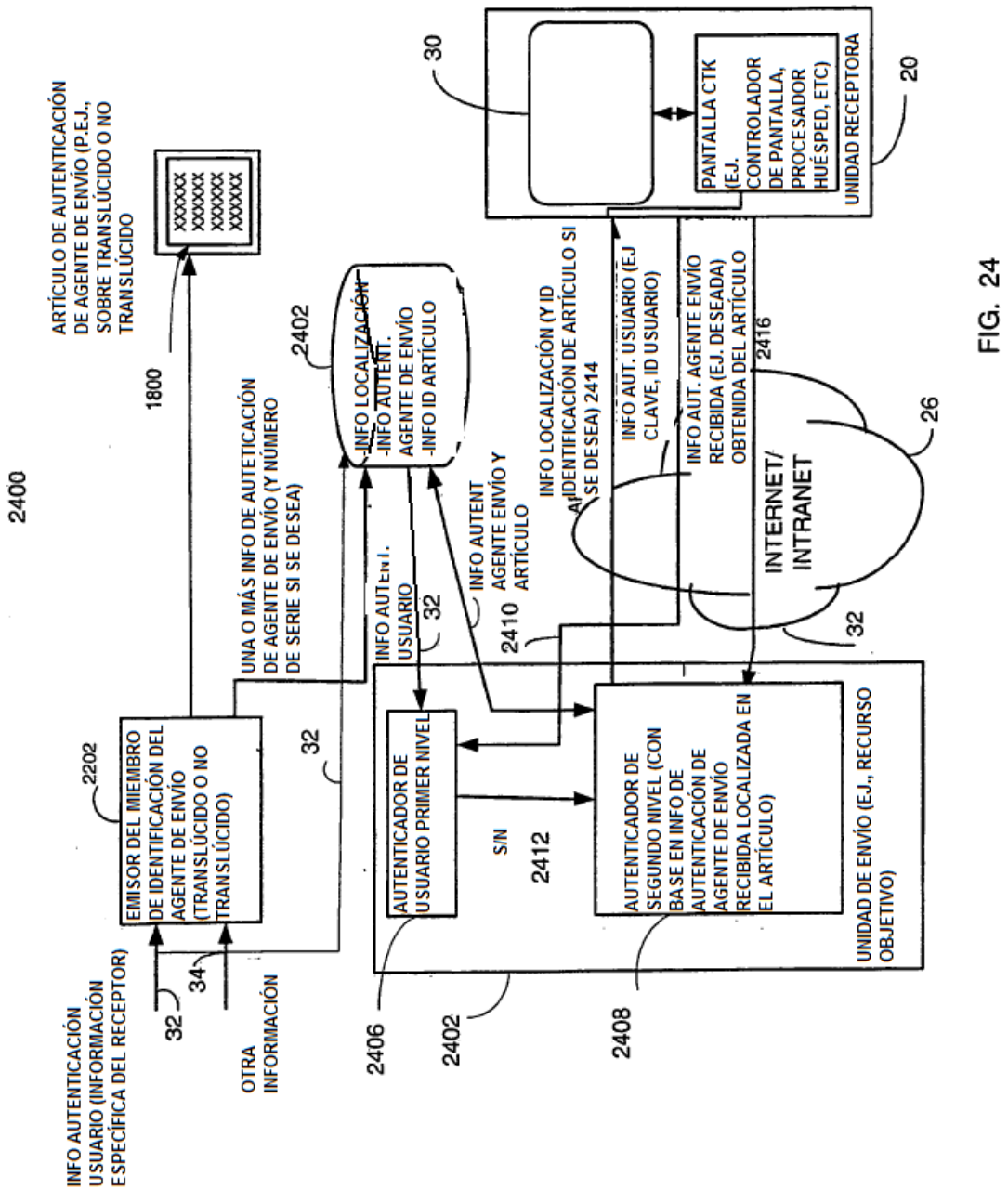

2400
ARTÍCULO DE AUTENTICACIÓN DE AGENTE DE ENVÍO (P.EJ., SOBRE TRANSLÚCIDO O NO TRANSLÚCIDO
1800
XXXXXX XXXXXX XXXXXX XXXXXX
30
PANTALLA CTK (EJ. CONTROLADOR DE PANTALLA, PROCESADOR HUÉSPED, ETC)
UNIDAD RECEPTORA
20
2402
-INFO LOCALIZACIÓN -INFO AUTENT. AGENTE DE ENVÍO -INFO ID ARTÍCULO
INFO LOCALIZACIÓN (Y ID IDENTIFICACIÓN DE ARTÍCULO SI SE DESEA) 2414
INFO AUT. USUARIO (EJ CLAVE, ID USUARIO)
INFO AUT. AGENTE ENVÍO RECIBIDA (EJ. DESEADA) OBTENIDA DEL ARTÍCULO
2416
26
INTERNET/ INTRANET
32
UNA O MÁS INFO DE AUTETICACIÓN DE AGENTE DE ENVÍO (Y NÚMERO DE SERIE SI SE DESEA)
INFO AUTENT. USUARIO
32
INFO AUTENT AGENTE ENVÍO Y ARTÍCULO
2410
2202
EMISOR DEL MIEMBRO DE IDENTIFICACIÓN DEL AGENTE DE ENVÍO (TRANSLÚCIDO O NO TRANSLÚCIDO)
32
AUTENTICADOR DE USUARIO PRIMER NIVEL
S/N
2412
AUTENTICADOR DE SEGUNDO NIVEL (CON BASE EN INFO DE AUTENTICACIÓN DE AGENTE DE ENVÍO RECIBIDA LOCALIZADA EN EL ARTÍCULO)
UNIDAD DE ENVÍO (EJ., RECURSO OBJETIVO)
INFO AUTENTICACIÓN USUARIO (INFORMACIÓN ESPECÍFICA DEL RECEPTOR)
32
34
OTRA INFORMACIÓN
2406
2402
2408

FIG. 24

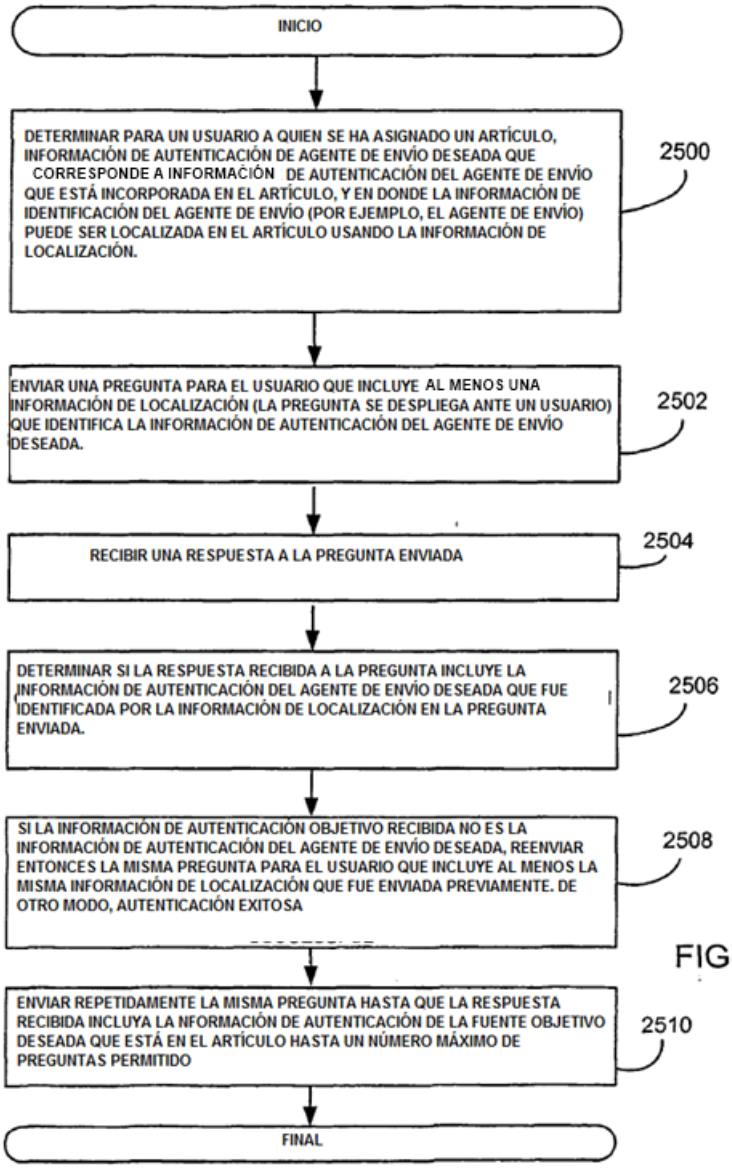

INICIO
DETERMINAR PARA UN USUARIO A QUIEN SE HA ASIGNADO UN ARTÍCULO, INFORMACIÓN DE AUTENTICACIÓN DE AGENTE DE ENVÍO DESEADA QUE CORRESPONDE A INFORMACIÓN DE AUTENTICACIÓN DEL AGENTE DE ENVÍO QUE ESTÁ INCORPORADA EN EL ARTÍCULO, Y EN DONDE LA INFORMACIÓN DE IDENTIFICACIÓN DEL AGENTE DE ENVÍO (POR EJEMPLO, EL AGENTE DE ENVÍO) PUEDE SER LOCALIZADA EN EL ARTÍCULO USANDO LA INFORMACIÓN DE LOCALIZACIÓN.
2500
ENVIAR UNA PREGUNTA PARA EL USUARIO QUE INCLUYE AL MENOS UNA INFORMACIÓN DE LOCALIZACIÓN (LA PREGUNTA SE DESPLIEGA ANTE UN USUARIO) QUE IDENTIFICA LA INFORMACIÓN DE AUTENTICACIÓN DEL AGENTE DE ENVÍO DESEADA.
2502
RECIBIR UNA RESPUESTA A LA PREGUNTA ENVIADA
2504
DETERMINAR SI LA RESPUESTA RECIBIDA A LA PREGUNTA INCLUYE LA INFORMACIÓN DE AUTENTICACIÓN DEL AGENTE DE ENVÍO DESEADA QUE FUE IDENTIFICADA POR LA INFORMACIÓN DE LOCALIZACIÓN EN LA PREGUNTA ENVIADA.
2506
SI LA INFORMACIÓN DE AUTENTICACIÓN OBJETIVO RECIBIDA NO ES LA INFORMACIÓN DE AUTENTICACIÓN DEL AGENTE DE ENVÍO DESEADA, REENVIAR ENTONCES LA MISMA PREGUNTA PARA EL USUARIO QUE INCLUYE AL MENOS LA MISMA INFORMACIÓN DE LOCALIZACIÓN QUE FUE ENVIADA PREVIAMENTE. DE OTRO MODO, AUTENTICACIÓN EXITOSA
2508
ENVIAR REPETIDAMENTE LA MISMA PREGUNTA HASTA QUE LA RESPUESTA RECIBIDA INCLUYA LA NFORMACIÓN DE AUTENTICACIÓN DE LA FUENTE OBJETIVO DESEADA QUE ESTÁ EN EL ARTÍCULO HASTA UN NÚMERO MÁXIMO DE PREGUNTAS PERMITIDO
2510
FINAL

FIG. 25

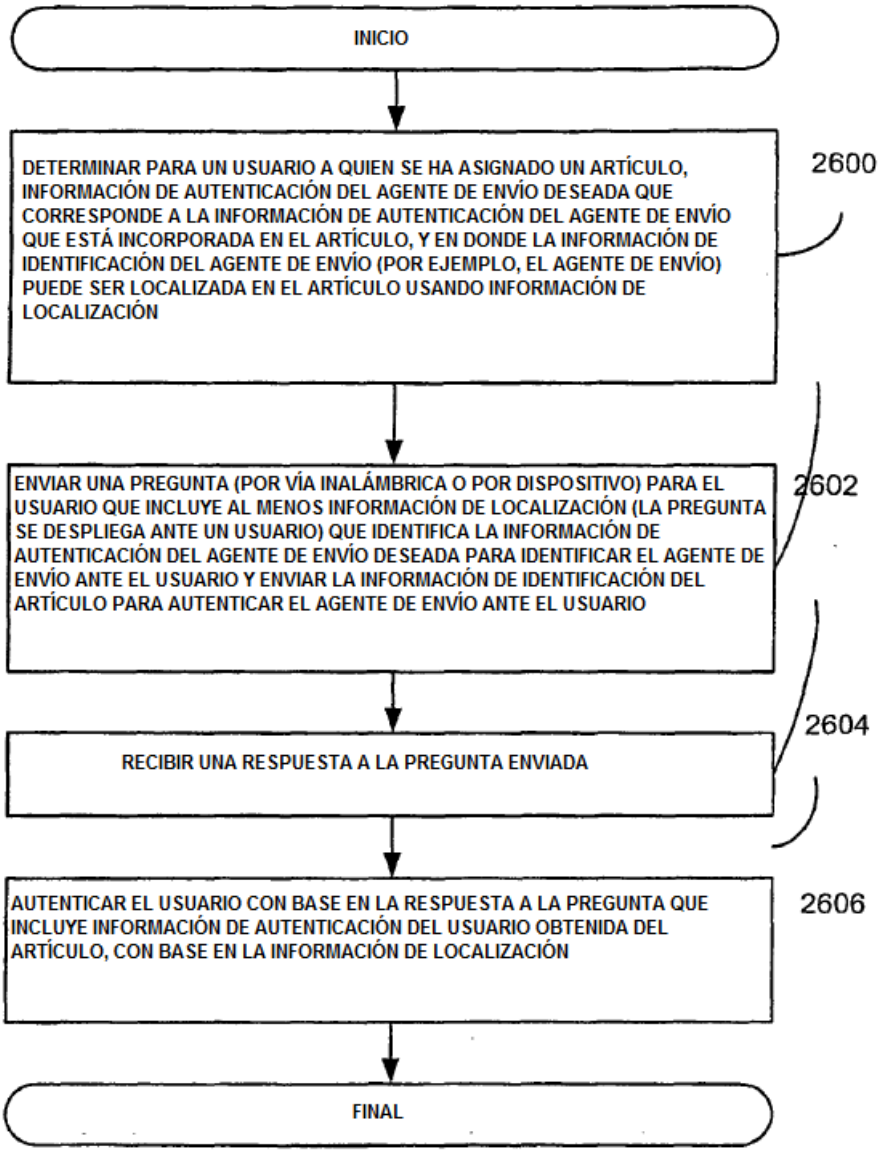

INICIO
DETERMINAR PARA UN USUARIO A QUIEN SE HA ASIGNADO UN ARTÍCULO, INFORMACIÓN DE AUTENTICACIÓN DEL AGENTE DE ENVÍO DESEADA QUE CORRESPONDE A LA INFORMACIÓN DE AUTENTICACIÓN DEL AGENTE DE ENVÍO QUE ESTÁ INCORPORADA EN EL ARTÍCULO, Y EN DONDE LA INFORMACIÓN DE IDENTIFICACIÓN DEL AGENTE DE ENVÍO (POR EJEMPLO, EL AGENTE DE ENVÍO) PUEDE SER LOCALIZADA EN EL ARTÍCULO USANDO INFORMACIÓN DE LOCALIZACIÓN
2600
ENVIAR UNA PREGUNTA (POR VÍA INALÁMBRICA O POR DISPOSITIVO) PARA EL USUARIO QUE INCLUYE AL MENOS INFORMACIÓN DE LOCALIZACIÓN (LA PREGUNTA SE DESPLIEGA ANTE UN USUARIO) QUE IDENTIFICA LA INFORMACIÓN DE AUTENTICACIÓN DEL AGENTE DE ENVÍO DESEADA PARA IDENTIFICAR EL AGENTE DE ENVÍO ANTE EL USUARIO Y ENVIAR LA INFORMACIÓN DE IDENTIFICACIÓN DEL ARTÍCULO PARA AUTENTICAR EL AGENTE DE ENVÍO ANTE EL USUARIO
2602
RECIBIR UNA RESPUESTA A LA PREGUNTA ENVIADA
2604
AUTENTICAR EL USUARIO CON BASE EN LA RESPUESTA A LA PREGUNTA QUE INCLUYE INFORMACIÓN DE AUTENTICACIÓN DEL USUARIO OBTENIDA DEL ARTÍCULO, CON BASE EN LA INFORMACIÓN DE LOCALIZACIÓN
2606
FINAL

FIGURA 26

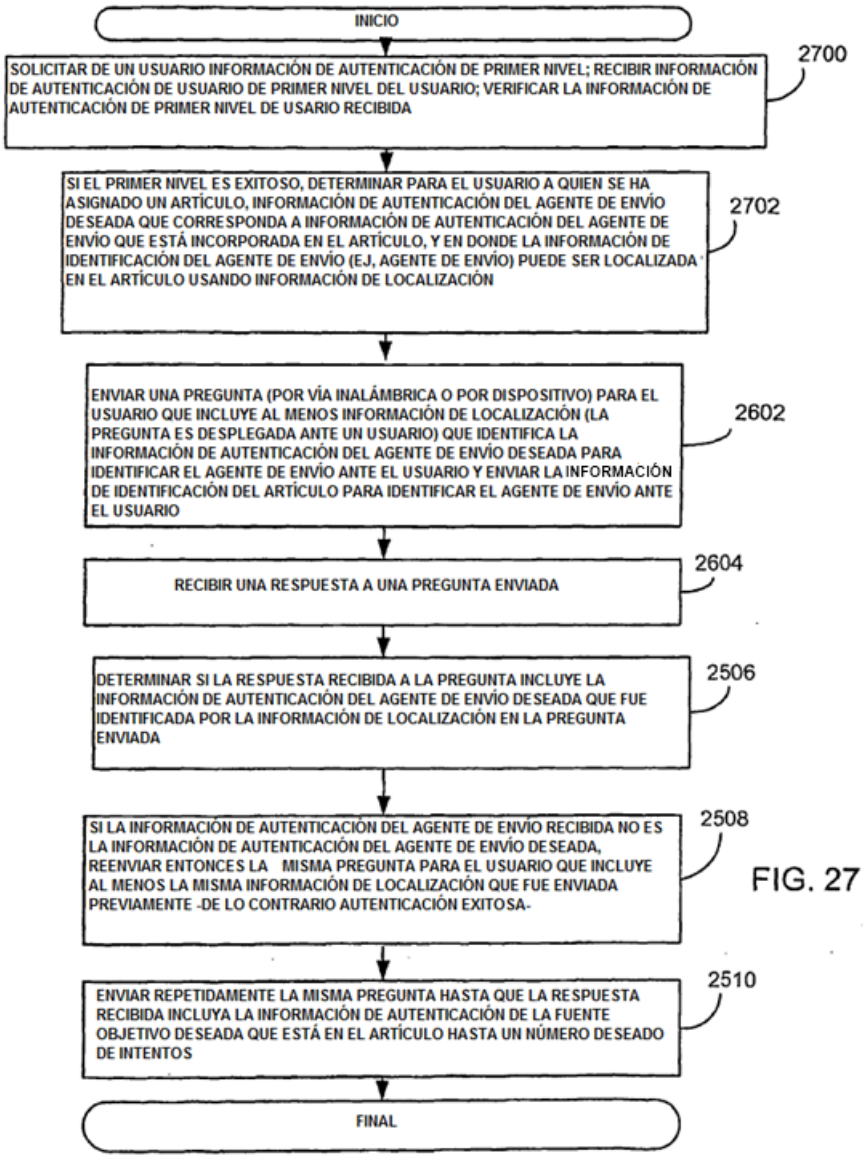
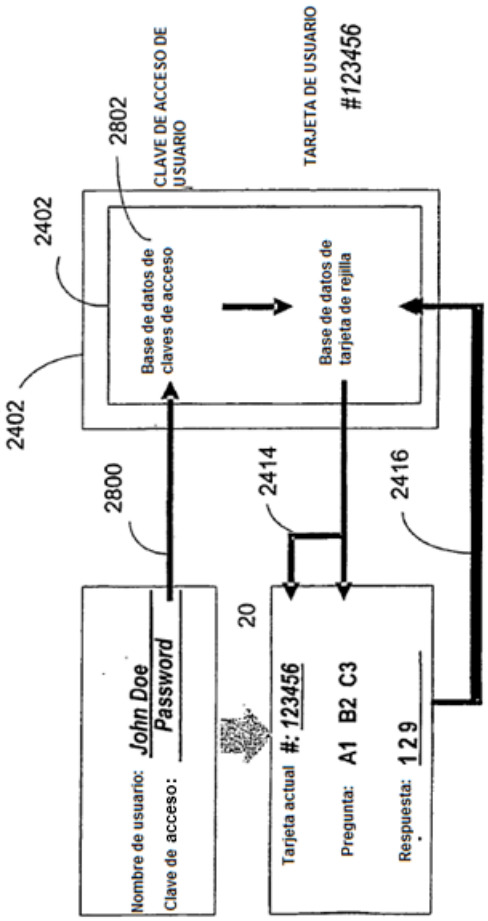

INICIO
SOLICITAR DE UN USUARIO INFORMACIÓN DE AUTENTICACIÓN DE PRIMER NIVEL; RECIBIR INFORMACIÓN DE AUTENTICACIÓN DE USUARIO DE PRIMER NIVEL DEL USUARIO; VERIFICAR LA INFORMACIÓN DE AUTENTICACIÓN DE PRIMER NIVEL DE USARIO RECIBIDA
2700
SI EL PRIMER NIVEL ES EXITOSO, DETERMINAR PARA EL USUARIO A QUIEN SE HA ASIGNADO UN ARTÍCULO, INFORMACIÓN DE AUTENTICACIÓN DEL AGENTE DE ENVÍO DESEADA QUE CORRESPONDA A INFORMACIÓN DE AUTENTICACIÓN DEL AGENTE DE ENVÍO QUE ESTÁ INCORPORADA EN EL ARTÍCULO, Y EN DONDE LA INFORMACIÓN DE IDENTIFICACIÓN DEL AGENTE DE ENVÍO (EJ, AGENTE DE ENVÍO) PUEDE SER LOCALIZADA EN EL ARTÍCULO USANDO INFORMACIÓN DE LOCALIZACIÓN
2702
ENVIAR UNA PREGUNTA (POR VÍA INALÁMBRICA O POR DISPOSITIVO) PARA EL USUARIO QUE INCLUYE AL MENOS INFORMACIÓN DE LOCALIZACIÓN (LA PREGUNTA ES DESPLEGADA ANTE UN USUARIO) QUE IDENTIFICA LA INFORMACIÓN DE AUTENTICACIÓN DEL AGENTE DE ENVÍO DESEADA PARA IDENTIFICAR EL AGENTE DE ENVÍO ANTE EL USUARIO Y ENVIAR LA INFORMACIÓN DE IDENTIFICACIÓN DEL ARTÍCULO PARA IDENTIFICAR EL AGENTE DE ENVÍO ANTE EL USUARIO
2602
RECIBIR UNA RESPUESTA A UNA PREGUNTA ENVIADA
2604
DETERMINAR SI LA RESPUESTA RECIBIDA A LA PREGUNTA INCLUYE LA INFORMACIÓN DE AUTENTICACIÓN DEL AGENTE DE ENVÍO DESEADA QUE FUE IDENTIFICADA POR LA INFORMACIÓN DE LOCALIZACIÓN EN LA PREGUNTA ENVIADA
2506
SI LA INFORMACIÓN DE AUTENTICACIÓN DEL AGENTE DE ENVÍO RECIBIDA NO ES LA INFORMACIÓN DE AUTENTICACIÓN DEL AGENTE DE ENVÍO DESEADA, REENVIAR ENTONCES LA MISMA PREGUNTA PARA EL USUARIO QUE INCLUYE AL MENOS LA MISMA INFORMACIÓN DE LOCALIZACIÓN QUE FUE ENVIADA PREVIAMENTE -DE LO CONTRARIO AUTENTICACIÓN EXITOSA-
2508
ENVIAR REPETIDAMENTE LA MISMA PREGUNTA HASTA QUE LA RESPUESTA RECIBIDA INCLUYA LA INFORMACIÓN DE AUTENTICACIÓN DE LA FUENTE OBJETIVO DESEADA QUE ESTÁ EN EL ARTÍCULO HASTA UN NÚMERO DESEADO DE INTENTOS
2510
FINAL

FIG. 27

FIG. 28


2802
CLAVE DE ACCESO DE USUARIO
TARJETA DE USUARIO
#123456
2402
Base de datos de claves de acceso
Base de datos de tarjeta de rejilla
2402
2800
2414
2416
20
Nombre de usuario: John Doe
Clave de acceso: Password
Tarjeta actual #: 123456
Pregunta: A1 B2 C3
Respuesta: 1 2 9