(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 398 141**

(51) Int. CI.:

G06F 21/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **07.04.2008 E 08735898 (2)**

(97) Fecha y número de publicación de la concesión europea: **05.12.2012 EP 2132676**

(54) Título: **Dispositivo de terminación de comunicación, dispositivo de comunicación, tarjeta electrónica, procedimiento para un dispositivo de terminal de comunicación y procedimiento para un dispositivo de comunicación para proporcionar verificación**

(30) Prioridad:

05.04.2007 US 910249 P
05.04.2007 DE 102007016538

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.03.2013

(73) Titular/es:

INTEL MOBILE COMMUNICATIONS GMBH (100.0%)
Am Campeon 10-12
85579 Neubiberg, DE

(72) Inventor/es:

LUFT, ACHIM;
SCHMIDT, ANDREAS y
SCHWAGMANN, NORBERT

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Dispositivo de terminación de comunicación, dispositivo de comunicación, tarjeta electrónica, procedimiento para un dispositivo de terminal de comunicación y procedimiento para un dispositivo de comunicación para proporcionar verificación

Campo técnico

Las realizaciones se refieren en general a un dispositivo terminal de comunicación, un dispositivo de comunicación, una tarjeta electrónica, un procedimiento para un dispositivo terminal de comunicación y un procedimiento para un dispositivo de comunicación para proporcionar una verificación.

Antecedentes

Se desea un uso de un dispositivo terminal de comunicación, como por ejemplo un dispositivo de radio móvil para efectuar una verificación de los datos referidos a la persona.

El documento US2005/0250472 proporciona un procedimiento para proporcionar seguridad a un equipo. El usuario tiene acceso al equipo sólo si el ordenador reconoce la identificación de un dispositivo electrónico Bluetooth y es capaz de validar la información de autenticación proporcionada por el dispositivo electrónico Bluetooth.

Breve descripción de los dibujos

En los dibujos, caracteres de referencia similares se refieren generalmente a las mismas partes en todas las vistas diferentes. Los dibujos no están necesariamente a escala, colocándose generalmente el énfasis en cambio en ilustrar los principios de la invención. En la siguiente descripción, diversas realizaciones de la invención se describen con referencia a los siguientes dibujos, en los que:

La figura 1 muestra una disposición de un dispositivo terminal de comunicación y un dispositivo de comunicación para la transmisión de mensajes de acuerdo con una realización;
La figura 2A muestra un dispositivo terminal de comunicación de acuerdo con una realización, generando el dispositivo terminal de comunicación un mensaje de verificación;
La figura 2B muestra un dispositivo de comunicación de acuerdo con una realización, solicitando el dispositivo de comunicación un mensaje de verificación;
La figura 3 muestra un diagrama de flujo de mensajes con los mensajes intercambiados entre las entidades implicadas en conformidad con una realización;
La figura 4 muestra un diagrama de flujo de un procedimiento para generar un mensaje de solicitud de mensaje de verificación de acuerdo con una realización;
La figura 5 muestra un diagrama de flujo de un procedimiento para comprobar la firma digital del dispositivo de comunicación solicitando el mensaje de verificación de acuerdo con una realización;
La figura 6 muestra un diagrama de flujo de un procedimiento para autenticar el usuario de acuerdo con una realización;
La figura 7 muestra un diagrama de flujo de un procedimiento para generar el mensaje de verificación solicitado de acuerdo con una realización;
La figura 8 muestra un diagrama de flujo de un procedimiento para comprobar la firma digital del dispositivo terminal de comunicación y la comprobación de la verificación solicitada por medio del dispositivo de comunicación de acuerdo con una realización;
La figura 9 muestra un mensaje para solicitar una verificación de acuerdo con una realización;
La figura 10 muestra un mensaje para solicitar un acuse de recibo por parte del usuario de acuerdo con una realización;
La figura 11 muestra un mensaje que incluye la respuesta del usuario de la solicitud de acuse de recibo de acuerdo con una realización;
La figura 12 muestra un mensaje que incluye la verificación generada por el dispositivo terminal de comunicación de acuerdo con una realización;
La figura 13A muestra un procedimiento para proporcionar una verificación digital con respecto a un dispositivo terminal de comunicación de acuerdo con una realización;
La figura 13B muestra un procedimiento para proporcionar una verificación digital con respecto a un dispositivo de comunicación de acuerdo con una realización;
La figura 14 muestra la estructura de un certificado digital de conformidad con el estándar ITU-T X.509, y
La figura 15 muestra un diagrama de flujo con respecto a las firmas digitales.

Descripción

En el contexto de esta descripción, los términos “conectado” y “acoplado” están destinados a describir una conexión directa o indirecta o de un acoplamiento directo o indirecto, respectivamente.

Un dispositivo terminal de radio móvil tiende a convertirse en una herramienta universal debido a su alta penetración en el mercado y su presencia permanente con los abonados. A modo de ejemplo, ya en la actualidad, muchos

dispositivos de terminales de radio móviles se utilizan como asistentes personales digitales y el dispositivo terminal de radio móvil se utiliza para gestionar direcciones, fechas, notas, etc. También el campo del comercio electrónico y las posibilidades asociadas al mismo para utilizar el dispositivo de radio del terminal móvil como una tarjeta de efectivo actualmente probada en muchos lugares o que ya están en uso con el fin de pagar las billetes por ejemplo, para autobuses o trenes.

Por lo tanto, sería deseable si una tarea del día a día adicional se pudiera resolver de una manera mejorada por medio de un dispositivo terminal de radio móvil. Esta tarea es la de efectuar una verificación. El espectro de las aplicaciones llega a través de la verificación de la edad para adquirir alcohol, juegos, cigarrillos o para el acceso a los salones recreativos, tiendas de video, a través de la verificación del género para foros de internet para la autenticación digital por ejemplo, en las máquinas de la tienda de video.

En este caso, se puede distinguir entre dos tipos de una verificación, a saber, en cuanto a si la verificación debe llevarse a cabo hacia una persona o una entidad con la que el verificador ya tiene una relación de negocios y la que o la cual ya tiene un registro de datos sobre el verificador, o de si se trata de una verificación hacia una persona o entidad, a la que o para la cual el verificador es totalmente desconocido. En el segundo tipo de una verificación, deberá estar involucrada una tercera persona o entidad que sea de confianza para ambas otras partes.

También en este caso existe una diferenciación de los dos tipos de una verificación:

En caso de que se trate de una verificación hacia una persona o entidad a quien o a la cual el verificador ya tiene una relación de negocios, entonces, la verificación se lleva a cabo normalmente utilizando un documento, que ha sido emitido por la entidad que solicita la verificación. En este caso, por ejemplo, una tienda de vídeo proporciona al cliente una tarjeta de identificación del cliente, por medio de la cual el cliente puede verificar su afiliación en el futuro. Un enlace entre la tarjeta de identificación del cliente y el registro de los datos recopilados en la tienda de vídeo proporciona el suministro de los datos requeridos, por ejemplo en cuanto a si la edad del cliente autoriza al cliente a alquilar una película específica. Regularmente, una tarjeta de identificación del cliente se proporciona con características adicionales, que hacen difícil un abuso. A modo de ejemplo, una imagen del cliente puede ser proporcionada en la tarjeta o se lleva a cabo la entrada de un PIN (número de identificación personal), además de la presentación de la tarjeta de identificación del cliente, que se compara con el registro de datos del cliente. Estas medidas deberán impedir que alguien se haga pasar por otra persona por medio de una tarjeta de identificación de cliente encontrada o robada.

Por lo tanto, el cliente acumula una gran cantidad de diferentes tarjetas de identificación del cliente. Estas pueden estar asociadas con diferentes PINs. El cliente está en la situación que tiene o bien que llevar una pluralidad de tarjetas plásticas con él o mantener la tarjeta correcta respectiva.

La seguridad de las diferentes tarjetas de los clientes varía mucho. En muchos casos, el nivel de seguridad es bajo debido a razones de coste de las tarjetas y de que los clientes por lo general no incluyen mecanismos de protección criptográficos y a menudo tampoco hay información biométrica.

Las tarjetas son físicamente accesibles y así pueden ser robadas o se pierden de cualquier otro modo. Como ejemplo típico, debe ser mencionado el lavado de las tarjetas de cliente después de haber sido olvidadas en la ropa junto con la ropa.

Las tarjetas pueden ser inspeccionadas por terceras personas de una manera muy simple. Las tarjetas a menudo, además del nombre, contienen datos adicionales tales como número de cuenta por ejemplo con una tarjeta de cliente de un banco. En el caso de que se pierda todo un maletín de tarjetas de identificación, una gran cantidad de información sobre su propietario se divulga, lo que hace que el robo de identificación sea más fácil.

Tales tarjetas son también objeto de signos de desgaste.

Una transmisión de datos entre la tarjeta y el sistema de datos del cliente se puede implementar por medio de procedimientos adicionales (por ejemplo, utilizando tiras magnéticas). Estos procedimientos no son generalmente sin contacto, lo que resulta en que las tarjetas son sometidas a un desgaste adicional y que la tarjeta se entrega fuera de la mano. La comunicación a menudo no es cifrada debido a la falta de un circuito de procesamiento de datos en la tarjeta y por lo tanto, la comunicación es susceptible de manipulación.

Además, se necesita el material para la fabricación de las tarjetas.

Para la primera compilación de un registro de datos de clientes, como se describe más arriba, así como para cada verificación hacia una persona o entidad a quien o con la cual (en ese momento) no tiene una relación de negocios, la verificación, la cual ha sido emitida por una entidad de confianza, se hace necesaria. En el ejemplo de la tienda de videos, por lo general una tarjeta de identidad personal se solicita para la elaboración de un registro de datos de clientes: esta verificación emitida por el gobierno incluye el nombre, lugar de residencia, fecha de nacimiento, lugar de nacimiento, y un poco de información biométrica como por ejemplo fotografías de pasaporte, el tamaño y el color de los ojos.

Se desea evitar la divulgación de mucha información que no sería necesaria para la verificación real. No existe la necesidad de que el cajero de una tienda durante la venta de cigarrillos, cuando se requiere sólo una verificación de la edad (por ejemplo, mayores de 16 años), llegue a conocer el nombre, la fecha de nacimiento y la dirección del comprador.

La operación a una distancia (por ejemplo, Internet) y la evitación de la participación de un humano es deseada en comparación con los dos tipos convencionales de llevar a cabo una verificación, con el fin de lograr un esfuerzo mucho menor y una automatización completa.

La figura 1 muestra una disposición 100 de acuerdo con una realización, que incluye un dispositivo terminal de comunicación 102 (en otras realizaciones, cualquier número de dispositivos de comunicación terminales) y un dispositivo de comunicación 106 (en otras realizaciones, cualquier número de dispositivos de comunicación). El dispositivo de comunicación 106 puede estar integrado por ejemplo en una máquina expendedora o en otro dispositivo. El dispositivo de comunicación 106 de acuerdo con esta realización incluye un circuito de generación de mensaje 122 para generar un mensaje 108, que se envía al dispositivo terminal de comunicación 102. El mensaje 108 que es recibido por el dispositivo terminal de comunicación 102 se reenvía y se evalúa mediante una aplicación 124, que se ejecuta en una unidad de procesamiento 104, por ejemplo un microprocesador u otro tipo de una lógica programable. La unidad de procesamiento 104 puede ser una parte integral fija del dispositivo terminal de comunicación 102, o puede ser una tarjeta extraíble 202 tal como por ejemplo una tarjeta SIM de un dispositivo terminal de radio móvil 218, como se muestra como ejemplo en la figura 2A.

En caso de que las condiciones previas, que se exponen a continuación, se cumplen, la aplicación 124 en la unidad de procesador 104, que incluye al menos un procesador, genera un mensaje de respuesta 110, que a su vez se envía al dispositivo de comunicación 106 y que será evaluado allí por la unidad de procesador local 122.

El dispositivo de comunicación 106 puede ser por ejemplo parte de una máquina expendedora, que requiere una información confirmada acerca de una característica personal de un usuario para una acción, con el fin de obtener el permiso para ejecutar esta acción. A modo de ejemplo, la máquina expendedora es una máquina expendedora de cigarrillos que requiere la verificación de la edad de la persona que quiere comprar un paquete de cigarrillos en esta máquina expendedora de cigarrillos. El dispositivo de comunicación 106 envía una solicitud acerca de una característica personal por medio de un mensaje de solicitud 108 al dispositivo terminal de comunicación 102.

De acuerdo con una realización, la verificación se envía desde el dispositivo terminal de comunicación 102 al dispositivo de comunicación 106 como un mensaje de verificación digital, incluyendo la respuesta a la solicitud en el mensaje de respuesta.

En esta descripción, un mensaje de verificación digital, por ejemplo, puede entenderse como datos estructurados, que confirman y verifican el usuario, así como otras características de una clave pública. En una realización, el mensaje de verificación digital incluye un certificado digital. Por medio de un certificado digital, los usuarios de un sistema criptográfico asimétrico, como por ejemplo RSA (la abreviatura RSA representa los inventores Ronald L. Rivest, Adi Shamir y Leonard Adleman) pueden asignar la clave pública a una identidad (por ejemplo, de una persona o un sistema de IT) y se puede determinar su campo de aplicación. Por lo tanto, el certificado digital permite la protección de la confidencialidad, la integridad y la autenticidad de los datos por medio de la aplicación correcta de la clave pública. De acuerdo con una realización, un certificado digital incluye la clave pública de un usuario y una firma digital a través de la clave pública.

De esta manera, se garantiza que por ejemplo, la edad de una persona se determina por el dispositivo que emite el mensaje de verificación - por ejemplo, la aplicación en el dispositivo procesador 104 en el dispositivo terminal de comunicación 102 - correctamente. De acuerdo con una realización, una firma digital se utiliza en el mensaje de verificación a fin de asegurar que el mensaje de verificación y, en su caso, el certificado para la verificación por ejemplo, la edad contenida en el mismo llega al dispositivo de comunicación receptor 106 de una manera inalterada y realmente provenir del usuario correspondiente, o, en función del resultado está contenido en el mensaje de verificación (por ejemplo, positivo o negativo) y la determinación de que el mensaje recibido es auténtico, se lleva a cabo una reacción correspondiente por ejemplo en la máquina expendedora. En otras palabras, esto significa que el mensaje es realmente la respuesta a la solicitud para el mensaje de verificación y que no ha sido alterado y que el remitente de la respuesta que incluye el mensaje de verificación es realmente el dispositivo que está autorizado para hacerlo, tal como por ejemplo, la aplicación 124 en la unidad de procesador 104 en el dispositivo terminal de comunicación 102.

La figura 1 muestra además el mensaje de solicitud del mensaje de verificación 108 y el mensaje de respuesta 110. Los mensajes incluyen porciones diferentes, en la figura 1 representado por los bloques 112, 114, 116, y 118, 120, 122, respectivamente, que se describirán en más detalle más adelante.

El dispositivo de comunicación 106 envía de acuerdo con una realización de un mensaje 108, que incluye una solicitud para una verificación 112, al dispositivo terminal de comunicación 102. Los bloques 112 a 122 de los mensajes 108 y 110 en la figura 1 han de entenderse sólo de manera simbólica. Entre los ejemplos de posibles formatos de los mensajes se describirán en detalle en el curso posterior de esta descripción con referencia a las

figuras 9 a 12.

De acuerdo con una realización, el mensaje 108 incluye, opcionalmente, un certificado del solicitante de verificación incluyendo por ejemplo una primera firma digital.

Aquí, una firma digital puede ser entendida como un procedimiento criptográfico o una secuencia de dígitos generada por medio de un procedimiento criptográfico, que ha sido generada por medio de una denominada clave privada a partir del llamado valor hash de un mensaje en con arreglo a un algoritmo de cifrado específico y que puede ser descifrado utilizando de nuevo una denominada clave pública. El valor descifrado puede ser comparado con el valor hash, que se genera a partir del mensaje recibido, en el receptor del mensaje. Por lo tanto, el remitente del mensaje puede ser verificado. Además, se determina la integridad del mensaje. La aplicación del algoritmo de cifrado se lleva a cabo de acuerdo con una realización en una función hash.

Una función hash puede entenderse aquí como una función que genera, para una entrada de un conjunto fuente generalmente grande, una salida de un conjunto objetivo más pequeño general, por ejemplo, mediante la generación de una suma de verificación. Las sumas de verificación se utilizan con el fin de detectar cambios en los datos, que pueden ocurrir debido a las inducciones parásitas técnicas o manipulación intencionada. Sin embargo, también otros algoritmos utilizados podrán generar, por ejemplo, una suma transversal, una paridad, un dígito de verificación, una función de módulo o una verificación de redundancia cíclica o por ejemplo, trabaja de acuerdo con los siguientes procedimientos convencionales: Adler-32, tabla hash, procedimiento meta de Merkle o hash Salted. Un uso de una función hash, sin embargo, resulta en que un mayor nivel de seguridad está garantizado. La razón de esto es por ejemplo una función hash que cumple los requisitos de seguridad adicionales. A modo de ejemplo, una función hash proporciona una colisión menor (dos textos diferentes no deben resultar en el mismo valor hash, si es posible). Además, una función hash asegura que ninguna inferencia puede ser realizada sobre los datos iniciales y que un cambio garantizado del valor hash se produce en respuesta al menor cambio de los datos básicos. Los algoritmos convencionales hash en la criptografía que se pueden utilizar en diversas realizaciones, por ejemplo, se MD2, MD4, MD5, SHA, RIPEMD-160, Tiger, HAVAL, o WHIRLPOOL.

El procedimiento de la firma digital se describirá con más detalle en la descripción adicional.

De acuerdo con una realización, el dispositivo terminal de comunicación 102 incluye una aplicación 124, que se ejecuta en el dispositivo del procesador 104. De acuerdo con una realización, el mensaje 108 incluyendo el mensaje de solicitud de verificación es recibido por el procesador del dispositivo 104 y es procesado por su aplicación 124. Como se describirá en más detalle a continuación, de acuerdo con una realización, la aplicación 124 comprueba en primer lugar el certificado del solicitante de verificación (si está presente) y la primera firma digital (si está presente) con el fin de asegurar que el remitente del mensaje es el dispositivo de comunicación 106 autorizado para ello y que el mensaje no ha sido alterado durante la transmisión. El mensaje de solicitud 108 puede incluir campos adicionales, que pueden ser controlados de acuerdo con las realizaciones descritas más adelante.

De acuerdo con otra realización, después de una verificación exitosa de la primera firma digital, la solicitud de la información se procesa y el resultado del procesamiento se inserta en el mensaje de respuesta 110 como una verificación, que es generada por la aplicación 124 en el dispositivo del procesador 104. El dispositivo terminal de comunicación 102 envía el mensaje de respuesta 110 al dispositivo de comunicación 106.

A fin de permitir que el dispositivo de comunicación 106 asegure que el mensaje de respuesta 110 ha sido realmente enviado por el dispositivo terminal de comunicación 102 y ha sido recibido inalterado, de acuerdo con una realización, la aplicación 124 se agrega una segunda firma digital al mensaje de respuesta 110 antes de enviarlo.

La figura 2A muestra una realización de un dispositivo terminal de comunicación 102, que es móvil, en la figura 2A. Por ejemplo, implementado como un dispositivo terminal de radio móvil 218, que tiene una antena 208, una interfaz de comunicación de campo próximo 210, una interfaz óptica 212, una interfaz hombre-máquina que incluye una pantalla 204, un teclado 206 y un altavoz 216; una tarjeta SIM 202 , y una aplicación 124 implementada en el mismo. El dispositivo terminal de comunicación 102 puede de acuerdo con una realización incluir una memoria de datos, en la que está almacenada la aplicación 124, y un procesador, por medio del que se ejecuta la aplicación 124.

La aplicación 124 también puede ser realizada por lo menos parcialmente en hardware.

De acuerdo con una realización, una tarjeta SIM puede ser insertada en el dispositivo terminal de comunicación móvil 102, en el que la tarjeta SIM puede incluir una memoria de la tarjeta SIM, en la que está almacenada la aplicación 124.

La aplicación 124 puede solicitar al usuario del dispositivo terminal de comunicación 102, para el que debe ser generada una verificación en la forma de un mensaje de verificación, de acuerdo con una realización ópticamente por medio de la pantalla 204 o acústicamente por medio del altavoz 216, para confirmar que el mensaje de verificación debe ser generado y ser transmitido al dispositivo de comunicación 106.

Los mensajes 108, 110 que se intercambian entre el dispositivo terminal de comunicación 102 y el dispositivo de comunicación 106 pueden ser transmitidos a través de la interfaz de datos de un estándar de comunicación de radio

móvil, como por ejemplo GSM (sistema global para comunicaciones móviles), UMTS (sistema de telecomunicaciones móvil universal), FSPTMT (sistema de telecomunicaciones móviles terrestres público futuro), CDMA 2000 (acceso múltiple de división de código 2000) o a través de una interfaz orientada a paquetes o una interfaz de Internet, como por ejemplo de acuerdo con GPRS (servicio de radio de paquete general), como parte de GSM, o, alternativamente, utilizando UMTS.

De acuerdo con una realización adicional, el dispositivo terminal de comunicación 102 puede ser también un dispositivo terminal de comunicación inalámbrica 102, en el que los mensajes se transmiten a través de una interfaz 210 de un estándar de comunicación de campo cercano, como por ejemplo Bluetooth, un estándar de un sistema de comunicación inalámbrica, como por ejemplo IEEE 802.11, WiMAX (interoperabilidad mundial para el acceso por microondas), una interfaz de datos óptica 212 como por ejemplo IrDA (asociación de datos infrarrojos) o un escáner óptico, tal como por ejemplo un lector de código de barras o una cámara, u otros estándares inalámbricos. El dispositivo terminal de comunicación 102 puede ser por ejemplo un PDA (asistente personal digital), un ordenador portátil o también un reproductor de música que tiene capacidades de comunicación digital u otro dispositivo electrónico portátil, en el que se implementan las funciones requeridas por la aplicación 124. En el caso de un escáner óptico, por ejemplo, un código de barras puede ser leído en una pantalla 220 (véase la figura 2B) del dispositivo de comunicación 106.

También una interfaz de línea fija a través de un cable de datos se proporciona en una realización alternativa. En caso de que se trata de una conexión de radio, la recepción y el envío se realizan a través de una antena 208, que puede estar integrado en el dispositivo terminal de comunicación 102 o, alternativamente, también se guíe fuera del dispositivo terminal de comunicación 102.

De acuerdo con una realización, la aplicación 124 puede ser actualizada a través de un canal de transmisión seguro. A modo de ejemplo, la estructura de datos, el código ejecutable o los datos se pueden cambiar de una manera flexible. En este caso, por ejemplo, también el campo de aplicación puede ser cambiado, por ejemplo, por medio de una solicitud adicional de información o un cambio de la solicitud. A modo de ejemplo, en el ejemplo de la máquina expendedora del cigarrillo, de una manera sencilla, un posible cambio en la ley con respecto a la edad mínima para comprar los cigarrillos puede ser acomodado. El canal de transmisión seguro para la actualización de la aplicación puede ser un canal de transmisión por cable o un canal de transmisión inalámbrica. Además, el canal de transmisión seguro para la actualización de la aplicación puede ser un canal de transmisión de telecomunicaciones, por ejemplo, un canal de cable de transmisión de telecomunicaciones o de un canal de transmisión de telecomunicaciones inalámbricas.

Los procedimientos descritos en la presente memoria de acuerdo con una realización sirven por ejemplo para la sustitución de una tarjeta de cliente por una solución digital y para efectuar una verificación hacia una entidad, con la que en ese momento no ha existido relación de negocios.

En caso de que en la realización anterior, el dispositivo terminal de comunicación 102 es un dispositivo terminal de radio móvil 218, las verificaciones se llevan a cabo por medio de este dispositivo terminal de radio móvil 218.

El dispositivo terminal de radio móvil 218 de un cliente de acuerdo con esta realización tiene una aplicación instalada 124. Esta aplicación 124 puede ser de confianza, es decir, una entidad arregla de forma demostrable la existencia de la aplicación 124 y que sea invariable. Esta entidad podría, por ejemplo, en caso de que la aplicación 124 está dispuesta en el terminal, es decir, por ejemplo en el dispositivo terminal de radio móvil 218, en sí mismo, ser el fabricante del dispositivo terminal de radio móvil 218. Alternativamente, la entidad podría ser también el proveedor de la red de radio móvil en sí mismo. Ilustrativamente, como se describirá en más detalle a continuación, se proporciona una entidad de confianza, que firma digitalmente la verificación. En el caso de un dispositivo terminal de radio móvil 218, la entidad de confianza podría ser el proveedor de la red de radio móvil para sí mismo y la verificación por ejemplo, podría ser firmada digitalmente utilizando la clave secreta del proveedor de la red de radio móvil, que puede ser almacenada por ejemplo en la tarjeta SIM del usuario del dispositivo terminal de radio móvil 218.

El dispositivo procesador 104 que tiene un procesador y una memoria de datos para almacenar información y datos ejecutables por el procesador del dispositivo procesador 104, que forman los datos de la aplicación, de acuerdo con una realización puede estar dispuesta en el dispositivo terminal de comunicación 102 en sí, que puede por ejemplo, el dispositivo terminal de radio móvil 218.

De acuerdo con una realización, la aplicación 124 puede estar dispuesta en una tarjeta electrónica, que incluye al menos una memoria de datos y/o procesador. De acuerdo con una realización, el procesador es un procesador programable, por ejemplo un microcontrolador. Un ejemplo de tal una tarjeta electrónica es una tarjeta SIM (módulo de identidad del abonado) 202 de un proveedor de la red de radio móvil.

La tarjeta SIM 202 en la implementación de una denominada tarjeta inteligente tiene por ejemplo las siguientes características:

- Incluye una unidad de procesamiento (por ejemplo, un microcontrolador).

- Está protegida contra una manipulación desde el exterior (en otras palabras, desde el exterior de la tarjeta SIM).

- La interfaz es utilizable únicamente en una manera definida y después de la autorización.

- Representa, en contraste con un dispositivo terminal de radio móvil que tiene un sistema operativo, posiblemente abierto y las interfaces para la programación, datos de procesamiento de un sistema cerrado.

- Es relacionado con una persona y permanece intacto después de un cambio del dispositivo terminal de radio móvil, que también juega a la tarea de proporcionar una verificación relacionada con una persona.

En el segundo caso mencionado, el proveedor de la red de radio móvil es la entidad de confianza, que puede proporcionar sus servicios a terceros (como por ejemplo, la tienda de videos mencionada como un ejemplo).

Bajo estas condiciones previas, la entidad de verificación de emisión logra así la posibilidad de depositar un certificado digital, que ha sido generado por sí mismo, en la aplicación 124 de la entidad de confianza. Además, esta entidad obtiene la posibilidad de que se autentifique a la aplicación 124 en forma de un certificado digital emitido por el proveedor de red de radio móvil. Este certificado de acuerdo con una realización reemplaza una tarjeta de cliente convencional. La entidad de confianza puede depositar también información sobre el abonado de radio móvil por sí misma en la aplicación 124, cuya información es adecuada para la verificación.

De acuerdo con una realización, un número de secuencia aleatoria 114 puede ser adicionalmente insertado en el primer mensaje 108 enviado por el dispositivo de comunicación 106, en el que el número de secuencia aleatoria 114 también puede ser insertado en el mensaje de respuesta 110. La inserción de un número de secuencia aleatoria 114 sirve para prevenir un llamado ataque de solicitud adicional. Cada solicitud es diferente de las anteriores solicitudes debido a la secuencia de número cambiante, de modo que una simple transmisión repetida de un mensaje de respuesta generado previamente 110 resulta en un caso de error.

De acuerdo con una realización, una unidad de encriptación se puede proporcionar en el dispositivo terminal de comunicación 102, que por ejemplo puede cifrar el ejemplo, la secuencia de número de aleatoria usando la clave pública del verificador, de tal manera que el dispositivo terminal de comunicación 102 puede insertar la secuencia de número aleatoria cifrada en el mensaje de respuesta 110, aumentando así la fuerza de la autenticación.

Además, de acuerdo con una realización, la fecha y/o la hora 116 se puede insertar en el mensaje de respuesta 110 con el fin de evitar que una falsa verificación haya sido generada por el cambio del reloj interno.

De acuerdo con una realización, para la autenticación del usuario del dispositivo terminal de comunicación 102, el dispositivo de comunicación 106 puede solicitar la entrada de una característica como por ejemplo, un PIN (número de identificación personal) del usuario del dispositivo terminal de comunicación 102, la cual el usuario puede introducir a través del teclado 206. Esto asegura que el usuario es el usuario autorizado real del dispositivo de comunicación 102 terminal o el dispositivo terminal de radio móvil 218. Sin embargo, también otros procedimientos, como por ejemplo, procedimientos biométricos, tales como huellas dactilares por ejemplo, el escaneo de las características de la cara o de las características de la voz o el reconocimiento del iris, se pueden utilizar para la autenticación.

Dado que la aplicación 124 solicita una confirmación por parte del usuario del dispositivo terminal de comunicación 102 que el dispositivo terminal de comunicación 102 debe generar un mensaje de verificación incluyendo la respuesta a la solicitud y debe enviarlo al dispositivo de comunicación, el usuario mantiene el control sobre el proceso y sobre la cuestión de si debe ser transmitido.

La solicitud, que debe ser contestada por la generación del mensaje de verificación, por ejemplo, podría ser la información acerca de las características personales del usuario del dispositivo terminal de radio móvil 218, como por ejemplo la edad o de si una edad específica es inferior o excedida, un número de cliente o el género, sólo por mencionar algunos ejemplos.

La figura 2B muestra una realización de un dispositivo de comunicación 106 que corresponde a la del dispositivo terminal de comunicación 102.

De acuerdo con esta realización, el dispositivo de comunicación 106 incluye un dispositivo procesador 224 que genera el mensaje de solicitud 108 y lo envía al dispositivo terminal de comunicación 102. El mensaje de solicitud 108 incluye al menos una solicitud para una verificación y una primera firma digital. La firma digital en el mensaje de solicitud 108 asegura de que no cualquiera puede solicitar una verificación. Sin embargo, se debe mencionar que la primera firma digital es opcional. El mensaje de solicitud 108 puede también, como se describirá más adelante con referencia a la figura 9, incluyen datos adicionales, tales como por ejemplo un número aleatorio, la fecha actual y la hora y una cabecera de mensaje. De acuerdo con una realización, la solicitud se refiere a la información sobre el usuario del dispositivo terminal de comunicación 102.

De acuerdo con una realización, el dispositivo de comunicación 106 puede además insertar una información sobre el tipo de la verificación solicitada en el mensaje.

De acuerdo con una realización, el dispositivo procesador 104, en respuesta al envío del mensaje de solicitud 108, recibe un mensaje de respuesta 110 desde el dispositivo terminal de comunicación 102 y comprobará su contenido. El mensaje de respuesta 110 de acuerdo con una realización incluye por ejemplo una segunda firma digital, generada por el dispositivo terminal de comunicación 102, la verificación solicitada, el envío de retorno, posiblemente cifrado, la secuencia de números aleatorios, fecha y hora, y una cabecera de mensaje. Un mensaje de respuesta de ejemplo 110 se describirá más adelante con referencia a la figura 12.

De acuerdo con una realización, el dispositivo de comunicación 106 incluye también una interfaz hombre máquina, por ejemplo, teniendo una pantalla 220 y un dispositivo de entrada mecánica o electrónica, como por ejemplo uno o una pluralidad de botones de entrada, un teclado o una pantalla sensible al tacto. El dispositivo de comunicación 106 incluye, además, una o una pluralidad de interfaces 226, 228 correspondientes al dispositivo terminal de comunicación 102. Estos correspondientemente pueden ser una o una pluralidad de interfaces de comunicación de radio móviles, las interfaces de comunicación inalámbrica, o interfaces de comunicación óptica. En caso de que los mensajes se transmitan a través de una conexión de radio móvil, el dispositivo de comunicación de acuerdo con una realización incluye al menos una antena. De acuerdo con una realización, la unidad de procesamiento 224 genera el mensaje de solicitud 108, que se transmite al dispositivo terminal de comunicación 102 a través de una de las interfaces y, posiblemente, la antena 230. En la dirección inversa, el mensaje de respuesta 110 transmite a través de, posiblemente, la antena 230 y una de las interfaces 226, 228, se envía a la unidad de procesamiento 224, que finalmente evalúa el contenido del mensaje de respuesta 110 y dispara las acciones correspondientes, tales como por ejemplo, la expulsión de un paquete de cigarrillos en el ejemplo de la máquina expendedora de cigarrillos.

En el diagrama 300 en la figura 3 se muestra el flujo de mensajes entre las siguientes entidades de acuerdo con una realización, cuando un generador de verificación, como por ejemplo un abonado móvil de radio desea identificar a sí mismo hacia una entidad 306.

Los mensajes que son transmitidos entre las entidades 302, 304, 306, se describirá en detalle más adelante con referencia de la figura 9 a la figura 12.

1. De acuerdo con una realización, la entidad 306 solicita una verificación genera en 308 un mensaje de verificación de mensaje de solicitud 108 y envía una solicitud al dispositivo terminal de comunicación 102 del abonado de radio móvil 304 por medio de este mensaje de solicitud del mensaje de verificación 108 de manera digital, ya sea a través de comunicación de campo cercano, por ejemplo, Bluetooth, comunicación óptica, por ejemplo, a través de IrDA, o a través de otro sistema de transmisión de información (por ejemplo, Internet). En el dispositivo terminal de comunicación 102, el mensaje de solicitud del mensaje de verificación 108 será enviada a la SIM 302 se muestra en la figura. 3. En realizaciones alternativas, se proporcionan otras vías de transmisión, tales como por ejemplo, una transmisión óptica, en el que, por ejemplo, se lee un código de barras (por ejemplo, Semacode) presentado en la pantalla de verificación de la entidad solicitante 306, o una transmisión a través de la red de radio móvil en sí.

En este caso, a modo de ejemplo, la siguiente información puede ser incluida en el mensaje de solicitud del mensaje de verificación 108:

- Certificado de la entidad solicitante 306;

- Tipo codificado binario de la verificación (por ejemplo, correspondencia del número de cliente, “¿más de X años?”, “¿varón?”;

- Secuencia de números aleatorios.

2. El mensaje de verificación del mensaje de solicitud 108 se envía a la aplicación 124 en la tarjeta SIM 202 de acuerdo con esta realización.

3. El abonado de radio móvil 304 confirma, de acuerdo con esta realización mediante el mensaje de “acuse de recibo” 316 en respuesta a una solicitud de “solicitud de acuse de recibo” 314 en su dispositivo terminal de radio móvil 218 que le gustaría proporcionar esta verificación utilizando su dispositivo terminal de radio móvil 218 a la entidad autorizada 306.

4. De acuerdo con esta realización, el certificado de la entidad solicitante 306 se comprueba en la aplicación 124 y en caso de una verificación positiva, la solicitud contenida en el mensaje de solicitud del mensaje de verificación 108 será procesada. En el caso negativo, un mensaje de error es emitido y el procedimiento se cancela en esta etapa.

5. Además, de acuerdo con esta realización, el abonado de radio móvil ahora se autentifica a sí mismo frente a la aplicación 124. Esto puede llevarse a cabo por ejemplo por medio del par de mensajes “solicitud de autorización” 320 y “autorización” 322 por medio de la introducción del PIN seleccionado por el usuario de la tarjeta SIM 202 y la verificación posterior 324. Esto sirve para garantizar que la verificación no puede ser llevada a cabo por una persona, que ilegítimamente ha entrado en la posesión del dispositivo terminal de radio móvil 218. Es de señalar que la autenticación es opcional.

6. Las aplicaciones 124 controla en 326 la característica a ser verificada. En caso de que por ejemplo, la verificación

se solicita que el abonado de telefonía móvil 304 tiene 16 años o más, una respuesta sí-o-no se genera a partir de los datos almacenados de la fecha de nacimiento y la fecha actual.

7. Para el caso de que la verificación es positiva, la aplicación prepara una respuesta, que incluye la secuencia de número aleatoria 114 transmite en el mensaje de solicitud de mensaje de verificación “solicitud de certificado” 108, la fecha actual y el certificado para depositar o guardar o la respuesta calculada en el punto 6., y firma digitalmente el mismo utilizando una firma del proveedor de la red de radio móvil. El principio de la firma digital se ilustrará más adelante con referencia a la figura 14 y a la figura 15. El mensaje de respuesta generado 110, en la figura 3 denominado mensaje “certificado” 110, se transmite a la entidad solicitante de la verificación 306. En caso de que en el ejemplo anterior el abonado no tenga 16 años de edad o más, o bien no se genera una respuesta o a favor de una mejora de la usabilidad de una respuesta negativa, es decir, una respuesta de que la característica que debe verificar no se cumple.

8. La entidad solicitante 306 comprueba de acuerdo con un desarrollo de esta realización utiliza una clave pública proporcionada por el proveedor de red de radio móvil, en cuanto a si la firma digital del mensaje de respuesta 110 de la aplicación 124 es válido. En caso de que sea válida, la verificación puede ser de confianza. En caso de que la firma no pueda ser verificada, esto resulta en un mensaje de error. El proceso posiblemente puede repetirse, si se desea.

La verificación del certificado también podría llevarse a cabo antes del mensaje solicitud de acuse de recibo 314. Este ejemplo podría tener el efecto de que al generador de verificación 304 no se pide autorización en el caso de un error. Por otro lado, la verificación del certificado debe poder ordenador de manera que puede ocurrir un ataque DoS (Denial of Service) utilizando con frecuencia mensajes transmitidos de “solicitud de certificado” 108. Dado que la autorización podría ser muy automatizada utilizando las preferencias de abonado (sin la participación del verificador 304), en una realización, se proporciona el orden como se describe aquí.

El mensaje que se utiliza de acuerdo con las formas de realización se describirá en más detalle a continuación con referencia a la figura 9 a la figura 12.

En lo siguiente, los procesos mostrados en el diagrama de flujo de mensajes se ilustran en detalle:

La figura 4 muestra un diagrama de flujo de acuerdo con una realización para la generación 308 del mensaje de solicitud del mensaje de verificación (mensaje solicitud de certificado) 108. Al principio, después de haber iniciado el proceso en 400, en 402, se genera una secuencia de número aleatorio y, a continuación, en 404, la solicitud real, que incluye por ejemplo la solicitud de verificación de la edad, se inserta en el mensaje de solicitud del mensaje de verificación 108. Eventualmente, el mensaje es firmado digitalmente en 406. Esto puede llevarse a cabo por ejemplo utilizando un procedimiento bien conocido como se mencionó anteriormente. Entonces, el proceso se completa en 408.

La figura 5 muestra en un diagrama de flujo de acuerdo con una realización de la verificación 318 del certificado del solicitante de verificación 306 por medio de la aplicación 124 en el dispositivo procesador 104 (por ejemplo, la tarjeta SIM 202) del dispositivo terminal de comunicación 102 (por ejemplo, el dispositivo terminal de radio móvil 218). Al hacer esto, después de haber iniciado el proceso en 500, en 502, el valor hash se calcula sobre el mensaje recibido 108 hasta (exclusivo) el campo de mensaje “mensaje de autenticación” 914, que se describirá en más detalle a continuación en la figura 9 (en la figura 5 indicado con 512). En 504, el valor hash, que se ha transmitido en el mensaje de campo “autentificación del mensaje” 914 (en la figura 5 indicado con 514) de forma cifrada, se descifra. Los valores de ambos se comparan entre sí en 506. En caso de una correspondencia positiva (“Sí” en 506) se procede en el 508 para la autenticación del usuario, en caso de una correspondencia negativa (“No” en el 506), un mensaje de error se genera en 510 y en el proceso se cancela en 516.

La figura 6 muestra un diagrama de flujo de la autenticación de usuario 324 de acuerdo con una realización. Después de haber iniciado el proceso en 600, en 602, se solicita al usuario para introducir un PIN. En 604, el pin de entrada se compara con el PIN almacenado 610. En caso de una correspondencia positiva (“Sí” en 604) además se procedió en 606 para el proceso de verificación, en caso de una correspondencia negativa (“No” en el 604), un mensaje de error se genera en 608 y el proceso se cancela en 612. Sin embargo, también otros procedimientos, como por ejemplo, podrían ser utilizados procedimientos biométricos para la autenticación.

La figura 7 muestra un diagrama de flujo para el control de la característica debe ser verificado en el dispositivo terminal de comunicación 102 de acuerdo con una realización. Después de haber iniciado el proceso en 700, en 702, los valores almacenados (en la figura 7 señalados con 708) se comparan con la verificación solicitada (en la figura 7 señalada con 710). Este es, por ejemplo en la continuación del ejemplo de la verificación de la edad de la verificación real de si el usuario tiene la edad mínima o no. En caso de un resultado positivo (“Sí” en 702), el mensaje de “certificado” 110 se genera en 704, que se envía a la entidad solicitante de verificación 306. En caso de un resultado negativo (“No” en el 702), un mensaje de error se genera en 706. Entonces, el proceso se completa en 712.

La figura 8 muestra un diagrama de flujo para comprobar el 332 mensaje de “certificado” 110 de acuerdo con una realización. Similar a los procedimientos para el mensaje de “solicitud de certificado” 108, después de haber iniciado

el proceso en 800, en 802, en un primer momento, el valor hash se calcula para el mensaje 110, que se ilustrará con más detalle a continuación en la figura 12, hasta que (exclusivo) el campo “autentificación del mensaje” 1212 (véase la figura 12) (en la figura 8 denotado con 814), y, en 804, el valor en el campo de mensaje de “mensaje de autenticación” 1212 (en la figura 8 denotado con 814) transmite de forma cifrada, se descifra. Estos dos valores se comparan entre sí en 806. En caso de un resultado negativo (“No” en 806), un mensaje de error se genera en 812 y el proceso se cancela en 818. En el caso de la comparación es positivo (“Sí” en 806), en 808, la verificación llevada a cabo (en la figura 8 denotada con 820) se compara con la verificación solicitada (en la figura 8 denotada con 822). En este punto, por ejemplo, la entidad solicitante de verificación 306 por lo tanto comprueba si la verificación de la edad se ha efectuado. En caso de un resultado positivo (“Sí” en 808), la entidad solicitante de verificación 306 puede ejecutar acciones adicionales por medio de un mensaje o una señal, como por ejemplo la salida del mensaje o en el ejemplo de la máquina expendedora de cigarrillos la eyección de un paquete de cigarrillos. En otras palabras, en caso de un resultado positivo (“Sí” en 808), la verificación se ha efectuado en 810. En caso de un resultado negativo (“No” en 808), un mensaje de error se genera en 812 y el proceso se completa en 818.

En lo siguiente, los mensajes de acuerdo con formas de realización se describirán en mayor detalle:

La figura 9 muestra el mensaje de “solicitud de certificado” 108, también conocida como mensaje de solicitud del mensaje de verificación 108, que puede incluir de acuerdo con una realización:

- Encabezado del mensaje de cabecera 902:

El encabezado del mensaje 902 incluye de acuerdo con una realización por ejemplo, el destinatario, el tipo de emisor del mensaje, (en este caso el mensaje de tipo “solicitud de certificado”) y, opcionalmente, un “ID de mensaje” (identificación única del mensaje). Para este propósito, también se puede utilizar una secuencia de números aleatorios (RAND). Mediante la introducción de un “mensaje de ID” en el encabezado del mensaje 902, el “ID de mensaje”, que es más pequeño en comparación con la secuencia de números aleatorios, se puede procesar por lo tanto, más fácil y más rápido.

- Secuencia de número aleatoria RAND 904:

La secuencia de número aleatoria 904 denota el número de secuencia aleatoria, que se utiliza para la asignación entre un mensaje de solicitud del mensaje de verificación (también referido como mensaje de “solicitud de certificado”) 108 y un mensaje de “certificado” 110 y para la autenticación del verificador 304.

- Fecha y hora 906:

Este campo es opcional en este mensaje 108. Un efecto de la introducción de este campo se puede ver en que los errores que pueden ocurrir debido a las desviaciones entre los relojes del solicitante de la verificación 306 y el verificador 304, se evitan. Finalmente, para el cálculo de la verificación, la fecha y la hora del solicitante de la verificación 306 deben ser utilizadas. En el caso de estos valores se transmiten y se toman para el cálculo, por lo tanto, una fuente de posible error puede ser eliminada. Un efecto adicional es que esto hace un ataque de repetición, en el que un atacante repeticiones de un mensaje previamente interceptado y grabado a un verificador 304, más difícil.

- Verificación de tipo 908:

Este campo del mensaje incluye el tipo de verificación que se solicita. Se determina por ejemplo en cuanto a si se trata de una verificación previamente depositada (relación comercial ya existente) o una verificación anónima generada dinámicamente.

- Parámetro de verificación 910:

Los parámetros de verificación 910 se han de interpretar en dependencia del campo de “tipo de verificación” 908. Este campo incluye los parámetros asociados con la verificación solicitada dependiendo del tipo de la verificación solicitada, como por ejemplo, la edad mínima para ser verificada.

- Certificado X.509 912:

Este es el certificado del solicitante de la verificación 306. Este ejemplo podría seguir el estándar ITU-X.509 o de lo contrario puede existir en otra estructura predefinida. El estándar X.509 se describirá más adelante.

- Autorización del mensaje 914:

Este campo incluye la firma digital del mensaje de solicitud del mensaje de verificación 108 por el solicitante de verificación 306. Este campo asegura la integridad del mensaje de solicitud del mensaje de verificación 108. Si un campo del mensaje se cambia, el campo de “autorización del mensaje” 914 ya no coincidirá con el resto del mensaje de solicitud del mensaje de verificación 108 y el mensaje de solicitud del mensaje de verificación 108 puede ser descartado sin más procesamiento.

El mensaje de “solicitud de certificado” 108 podría ser codificado en binario y/o comprimido de acuerdo con una realización para minimizar el ancho de banda.

El mensaje de solicitud del mensaje de verificación 108 puede, de acuerdo con realizaciones adicionales también incluir campos más o menos de los que se enumeran en la figura 9 como ejemplo.

La figura 10 muestra el mensaje de “solicitud de acuse de recibo” 314, que incluye los siguientes campos de acuerdo con una realización:

- Encabezado del mensaje 1002:

El encabezado del mensaje 1002 incluye de acuerdo con una realización, al menos el tipo de mensaje (en este caso el mensaje de tipo “solicitud de acuse de recibo”).

- Tipo de mensaje 1004:

Este campo del mensaje incluye el tipo de la verificación, el cual se solicita. En cuanto al contenido, esta es la entrada transmitida en el “solicitud de certificado” 108. Sirve al verificador 304 para decidir sobre si él o ella quieren llegar a un acuerdo a este tipo de verificación.

- Verificación parámetro 1008:

Los parámetros de la verificación solicitada también se proporcionan para la autorización por parte del verificador 304. En cuanto al contenido, estas son las entradas transmitidas en el “solicitud de certificado” 108.

El mensaje “solicitud de acuse de recibo” 314 podría ser codificado en binario y/o comprimido de acuerdo con una realización para minimizar el ancho de banda.

También el mensaje solicitud de acuse de recibo 314 puede, de acuerdo con realizaciones adicionales, incluir más o menos campos de los que se enumeran en la figura 10 como ejemplo.

La figura 11 muestra el mensaje “acuse de recibo” 316, que de acuerdo con una realización incluye los siguientes campos:

- Encabezado del mensaje 1102:

El encabezado del mensaje 1102 incluye de acuerdo con esta realización, al menos el tipo de mensaje (en este caso el tipo de mensaje “acuse de recibo”).

-Valor acuse de recibo 1104:

Este campo proporciona de acuerdo con una realización, la respuesta a la solicitud de autorización en el mensaje de solicitud acuse de recibo 314 de vuelta a la SIM 202. El campo “valor acuse de recibo” incluye al menos una expresión booleana (verdadero/falso). Los códigos de error o las razones para el rechazo a verificaciones alternativas, que podrían ser entregadas en lugar de la verificación solicitada, también son posibles en realizaciones alternativas.

El mensaje “acuse de recibo” podría ser codificado en binario y/o comprimido de acuerdo con una realización para minimizar el ancho de banda.

La figura 12 muestra el mensaje de “certificado” 110, que de acuerdo con una realización incluye los siguientes campos:

- Encabezado del mensaje 1202:

El encabezado del mensaje 1202 incluye, por ejemplo destinatario, remitente, tipo de mensaje (en este caso el tipo de mensaje “certificado”) y, opcionalmente, la “ID de mensaje”. La “ID de mensaje” es idéntica al mensaje de “solicitud de certificado” 108 y se incluye sólo en caso de que hubiera un “ID de mensaje” en el mensaje de “solicitud de certificado” 108.

- Secuencia de número aleatorio (RAND) 1204:

La secuencia de números aleatorios 1204 denota la secuencia de números aleatorios, que se ha transmitido en el mensaje de “solicitud de certificado” 108. Se proporciona para lograr una asignación unívoca entre el mensaje de “solicitud de certificado” 108 y el mensaje de “certificado” 110. Dado que todo el mensaje 110 es firmado (“Mensaje de autorización” 1212), la secuencia de números aleatorios 1204 sirve para evitar el enviando de vuelta un previamente interceptado mensaje de “certificado” 110 nuevo como respuesta al actual mensaje de “solicitud de certificado” 108 en un punto más tardío en el tiempo. La secuencia de números aleatorios asegura así la oportunidad de la respuesta. La seguridad del procedimiento puede aumentarse por el fuerte cifrado asimétrico de la secuencia de números aleatorios 1204. En este caso, la secuencia de números aleatorios 1204 se cifra utilizando la clave

pública del verificador 304 (para el caso de que ya existe una relación comercial con el verificador 304) o utilizando la clave pública de la entidad de autenticación (por ejemplo, de un operador o proveedor de red de radio móvil). En caso de que esta secuencia de números aleatorios se transmite de una manera no cifrada o encriptada usando la clave pública del solicitante de verificación 306, se garantiza que el verificador 304 está en posesión de la clave secreta correspondiente que aumenta sustancialmente la fuerza de la autenticación del verificador 304.

- Fecha y hora 1206:

Este campo del mensaje incluye la fecha y la hora correspondiente en el SIM 202 que es la base para el cálculo de la verificación. Esta podría ser la fecha y la hora del dispositivo terminal o los valores que se han transmitido en el mensaje de “solicitud de certificado” 108.

- Tipo de Verificación 1208:

Este campo del mensaje es opcional e incluye el tipo de la verificación de que se ha solicitado. Este campo, si está presente, corresponde con el campo de la correspondiente mensaje de “solicitud de certificado” 108. Un efecto de la solicitud adicional del tipo de la verificación consiste en que se garantiza que no se ha producido un error de transmisión durante la transmisión de la solicitud de verificación y la respuesta realmente incluye la verificación solicitada y no erróneamente una verificación interpretada incorrectamente. Es de señalar que en caso de un error de transmisión de la firma no se correspondería y se puede confiar en la evaluación en la SIM 202.

- Verificación 1210:

Este campo incluye la verificación real que se ha solicitado. En caso de que se haya solicitado en cuanto a si el verificador tenga al menos 18 años de edad, esto, como se refiere a contenidos, el presente campo incluye la respuesta “El verificador tiene más de 18 años”. Esto también podría llevarse a cabo en el estándar X.509 o puede incluir otra estructura de datos predeterminada o predefinida.

- “Autorización del mensaje” 1212:

Este campo incluye la firma digital del mensaje por el verificador 304. Este campo asegura la integridad del mensaje 110. En el caso de que un campo del mensaje se cambie, el campo “autorización del mensaje” 1212 ya no coincide con el resto del mensaje 110 y el procesamiento se traduciría en un caso de error. La citada verificación no puede en este caso ser aceptada.

El mensaje “certificado” 110 podría ser codificado en binario y/o comprimido de acuerdo con una realización para minimizar el ancho de banda.

El mensaje de “certificado” 110 puede, de acuerdo con otras realizaciones incluir más o menos campos que los que se indican en la figura 12 como ejemplo.

Los mensajes de la figura 9 a la figura 12 representan formas de realización, que la persona experta podría cambiar de una manera adecuada o puede adaptar para un caso de aplicación específico. A modo de ejemplo, el orden de los campos de mensaje se puede variar, siempre y cuando lo sepan los tres participantes. Los campos adicionales para mayor optimización son también posibles.

En lugar del mensaje de respuesta 110 generado en la tarjeta SIM 202, también un mensaje de verificación generado previamente almacenado podría ser enviado de vuelta como respuesta. El uso de este consistiría en un tratamiento menos complejo en la tarjeta SIM 202 o el almacenamiento seguro sin la tarjeta SIM 202. Se estaría afectando que sólo ese mensaje de verificación generado previamente podría ser transmitido y que éstos no podrían ser generados dinámicamente. En particular, en la verificación de la edad que no se produce raramente, sin embargo, una generación dinámica puede ser útil. Además, el sistema sería en este caso más susceptible a los ataques de solicitud adicional mencionados anteriormente en el punto 7. Esto es cierto en particular en el caso de la información necesaria para la verificación se transmite a través de un medio que se considera como siendo inseguro (como por ejemplo, Internet).

La figura 13A muestra un procedimiento 1300 para un dispositivo terminal de comunicación 102 de acuerdo con una realización para efectuar una verificación digital.

En 1302, un dispositivo terminal de comunicación 102 recibe un primer mensaje 108 que incluye al menos una solicitud para una verificación y una primera firma digital, así como una solicitud de información que describe el usuario.

El mensaje 108 puede de acuerdo con una realización, además de la solicitud y la firma digital incluye información adicional, tal como por ejemplo, la información como se muestra en la figura 9. Esta información puede incluir, por ejemplo, una secuencia de números aleatorios 904, fecha y hora 906, el tipo de verificación 908, el parámetro de verificación 910 y la información 912, 914 en relación con una firma digital, como por ejemplo de acuerdo con la estructura del estándar X.509 (véase la figura 14) o de acuerdo con una estructura predefinida de otro modo. La firma digital puede, como ya se indicó en la descripción anterior, por ejemplo, incluir un valor hash que se calcula

sobre el mensaje de acuerdo con una función hash.

La información personal del usuario puede ser por ejemplo, datos que autorizan a una persona para una acción específica, por ejemplo, una verificación de la edad.

El dispositivo terminal de comunicación 102 puede de acuerdo con una realización ser un dispositivo terminal de comunicación móvil, como por ejemplo, un dispositivo terminal de radio móvil, un asistente personal digital (PDA), un ordenador portátil u otro dispositivo portátil que tenga capacidades de comunicación digitales.

La recepción del mensaje 108 se puede llevar a cabo de acuerdo con una realización a través de una interfaz 210 de un estándar de comunicación de campo cercano, como por ejemplo Bluetooth, un estándar de un sistema de comunicación inalámbrica, como por ejemplo IEEE 802,11, WiMax; un conjunto de datos de interfaz óptica 112, como por ejemplo IrDA, o por medio de un escáner óptico, tal como por ejemplo un lector de código de barras, o a través de una interfaz de otro estándar inalámbrico. En el caso de un escáner óptico, por ejemplo, un código de barras puede ser leído en una pantalla 204 (véase la figura 2) del dispositivo de comunicación 206.

En 1304, el dispositivo terminal de comunicación 102 comprueba la firma digital y genera después de una verificación exitosa un mensaje de respuesta 110, que incluye la verificación y la respuesta a la solicitud en la solicitud. Esto puede llevarse a cabo por una aplicación 124 de acuerdo con una realización, que se almacena en una memoria de datos del dispositivo terminal de comunicación 102 y que es ejecutado por un procesador en el dispositivo terminal de comunicación 102.

El dispositivo terminal de comunicación 102 inserta de acuerdo con una realización una segunda firma digital en el mensaje de respuesta 110, en el que la segunda firma digital se calcula, por ejemplo, en los campos 1202 a 1210 del mensaje de respuesta 110.

El dispositivo terminal de comunicación 102 puede de acuerdo con una realización adicional comprobar la autenticidad del usuario 304, por ejemplo, se pide al usuario 304 la entrada de su PIN. Sin embargo, también otro procedimiento, como por ejemplo, procedimientos biométricos, se puede utilizar para la autenticación. El proceso para la generación de la verificación es de acuerdo con una realización sólo continua en caso de que la autenticidad del usuario haya sido determinada.

Además, de acuerdo con una realización del procedimiento, el usuario puede pedir su acuerdo con la generación y transmisión del mensaje de respuesta 110, incluyendo la verificación y la respuesta a la solicitud de la información que describe el usuario, de forma interactiva a través de la interfaz de máquina hombre del dispositivo terminal de comunicación 102.

En el caso de un dispositivo terminal de comunicación móvil que se comunica de acuerdo con un estándar de radio móvil, la aplicación 124 también puede ser almacenada en una tarjeta SIM 202.

En 1306, el dispositivo terminal de comunicación 102 envía el mensaje de respuesta 110 por ejemplo, al dispositivo de comunicación 106.

La figura 13B muestra un procedimiento 1310 para un dispositivo de comunicación 106 de acuerdo con una realización para efectuar una verificación digital.

En 1312, un dispositivo de comunicación 106 de acuerdo con una realización genera un primer mensaje 108, que incluye al menos una solicitud de una verificación de una primera firma digital, y una solicitud de información que describe el usuario. El mensaje 108 puede incluir de acuerdo con una realización, además de la solicitud y la firma digital, información adicional, tal como por ejemplo, la información que se muestra en la figura 9. Esta información puede incluir una secuencia de números aleatorios 904, y fecha y hora 906, el tipo de verificación 908 y los parámetros de verificación 910 con respecto a la verificación solicitada, y la información 912, 914 con respecto a una firma digital, como por ejemplo de acuerdo con la estructura con del estándar X.509 (ver figura 14) o de acuerdo con una estructura predefinida de otro modo. La firma digital puede, como ya se indicó en la descripción anterior, por ejemplo, ser un valor hash calculado sobre el mensaje de acuerdo con una función hash.

Los datos personales pueden ser por ejemplo los datos que autorizan a una persona para una acción específica, como por ejemplo, una verificación de la edad.

En 1314, el dispositivo de comunicación 106 envía el mensaje 108 a un dispositivo terminal de comunicación 102. El dispositivo de comunicación 106 puede de acuerdo con una realización ejemplo, ser un dispositivo de comunicación móvil, como por ejemplo un dispositivo terminal de radio móvil (por ejemplo, un teléfono radio móvil) 218, una PDA, un ordenador portátil o también un reproductor de música digital u otro dispositivo electrónico portátil que tiene capacidades de comunicación digital, en el que las funciones necesarias para la ejecución del procedimiento se implementan, por ejemplo, por medio de la aplicación 124.

El envío del mensaje 108 se puede llevar a cabo de acuerdo con una realización a través de una interfaz 210 de un estándar de comunicación de campo cercano, como por ejemplo Bluetooth; de un estándar de un sistema de

comunicación inalámbrica tal como por ejemplo IEEE 802,11, WiMax; de un conjunto de datos de interfaz óptica 112, como por ejemplo IrDA, o a través de un escáner óptico, tal como por ejemplo un lector de código de barras o por medio de una interfaz de otro estándar inalámbrico. En el caso de un escáner óptico, por ejemplo, un código de barras puede ser leído a partir de una pantalla 204 (véase la figura 2) del dispositivo de comunicación 206.

En 1306, el dispositivo de comunicación 106 recibe un mensaje de respuesta 110, que incluye la verificación (por ejemplo, incluyendo un segundo certificado digital) que incluye una respuesta a la pregunta en la solicitud, y comprueba el segunda certificado digital y/o la segunda firma digital, de forma que el dispositivo de comunicación puede asegurar que obtiene una auténtica respuesta a su pregunta de la solicitud.

Debido a las verificaciones digitales de acuerdo con formas de realización, por ejemplo, los siguientes efectos pueden ser obtenidos con respecto a la tarjeta de identidad física:

- Verificaciones digitales son posibles sin ningún tipo de problemas a lo largo de grandes distancias. Sólo esto hace posible las verificaciones de los servicios digitales, como Internet o una Video-on-Demand.

- Las verificaciones son fáciles de automatizar y puede funcionar sin la intervención humana, que puede ser importante en aplicaciones tales como por ejemplo, máquinas expendedoras de cigarrillos o máquinas expendedoras de vídeo de alquiler.

- La seguridad de las verificaciones digitales es significativamente mayor en comparación con los procedimientos convencionales, debido al consecuente uso de la fuerte criptografía.

- Una actualización de los datos y de los componentes de seguridad pertinentes, como por ejemplo, claves criptográficas son posibles en una forma barata y en grandes distancias utilizando el dispositivo terminal de comunicación 102. Por lo tanto, la seguridad (cambio frecuente del contexto de seguridad) y la puntualidad de los datos se puede asegurar sin generar nuevas verificaciones y sin retirar las anteriores.

- Debido a la autenticación del verificador 304 en la aplicación 124 para ser ejecutada, las verificaciones son más difíciles de ser asignadas a otras personas y están protegidas del uso ilegítimo de terceras personas.

- En una realización, una autenticación común se lleva a cabo para todas las verificaciones de tal manera que el verificador 304 ya no memoriza una gran cantidad de diferentes contraseñas y PINs.

- Terceras personas no pueden ver los datos necesarios para la verificación. Las verificaciones incluyen sólo la información a verificar y ninguna otra información además de esta. Esto, por ejemplo, verificaciones de edad anónimas son posibles sin problemas.

- Verificaciones digitales no están sujetas a ningún tipo de desgaste. Las mismas se pueden transferir más fácilmente a otros dispositivos.

- Mediante el uso de un dispositivo terminal de comunicación 102 como el portador de las verificaciones, una transmisión digital de datos entre el cliente y el verificador de datos del sistema 304 se implementa automáticamente y no da lugar a costes adicionales. También existe la posibilidad de almacenar no sólo un número de cliente pero inmediatamente una clave criptográfica del cliente, que puede ser utilizada para la comunicación entre ambas partes para un cifrado.

- Las verificaciones digitales también pueden incluir datos biométricos, como por ejemplo una imagen o fotografía del abonado como las tarjetas de identidad o tarjetas de clientes convencionales. Además sólo es posible la lectura mecánica de datos biométricos (patrón de la cara, huella digital). Esto aumentar el nivel de seguridad y también se puede utilizar en algunas aplicaciones totalmente automatizadas.

- Para la generación de las verificaciones digitales, no se utiliza ningún material.

Además, los efectos del procedimiento para efectuar verificaciones digitales deben ser mencionados:

- Es posible llevar a cabo todas las verificaciones utilizando un dispositivo central que se ha demostrado como un compañero permanente del verificador 304 en la vida diaria.

- Todas las entidades participantes (entidad solicitante 306, abonado de radio móvil 304, solicitud 124, y el proveedor de datos) pueden autenticarse mutuamente mediante certificados digitales sin necesidad de llevar a cabo la comunicación permanente o muy frecuente entre las entidades debido a la criptografía asimétrica que se utiliza. Simplemente las claves públicas deben ser distribuidas en un punto inicial en el tiempo. Cambiando regularmente las claves, el nivel de seguridad se puede aumentar y entidades individuales por ejemplo, pueden ser excluidas después de la expiración del período contable.

- El verificador 304 tiene el control final sobre la información que él o ella quiere verificar acerca de sí mismo y por lo tanto dar a conocer.

- Es posible generar comprobaciones dinámicas. Por lo tanto, un abonado puede, por ejemplo, en su 18º cumpleaños verificar inmediatamente su edad actual, sin necesidad de cambiar ningún tipo de certificado, y sin divulgar su cumpleaños.

- Mediante la inserción o la unión de la secuencia de números aleatorios (por ejemplo, en un procedimiento de desafío-respuesta), se proporciona una implementación robusta contra ataques de solicitud adicional.

- Mediante la inserción o la unión de manipulaciones de la fecha y/u hora al cambiar el reloj interno se evitan y no es necesario un tiempo del sistema de confianza que sólo puede aplicarse mediante comunicación elaborada.

- Mediante el uso de los mensajes de error opcionales todos los participantes podrán estar informados acerca de las razones para el fracaso de una verificación.

Tres ejemplos se describen a continuación.

Verificación de la edad anónima durante la compra de cigarrillos en una máquina expendedora de cigarrillos

Prerrequisitos:

Un fabricante de máquinas expendedoras de cigarrillos participa en un programa de verificación a través de dispositivos de telefonía móvil, que se ofrece por un consorcio de operadores o proveedores nacionales de redes de radio móviles.

La clave pública de los operadores o proveedores de redes móviles de radio se almacena en las máquinas expendedoras del fabricante.

Además, el fabricante proporciona a sus máquinas expendedoras con una interfaz Bluetooth para la comunicación inalámbrica con dispositivos terminales móviles de radio y con un reloj interno.

Un abonado móvil de radio de 17 años 304 utiliza una máquina expendedora de la empresa mencionada anteriormente para comprar cigarrillos. De acuerdo con la ley alemana, que sólo se puede permitir la compra de cigarrillos para los adolescentes que tienen al menos 16 años de edad. Por este motivo, la máquina expendedora, después de haber recibido el dinero, envía una solicitud de verificación de edad a través de Bluetooth. La proximidad espacial al máquina expendedora causada por principio puede dar lugar a un abandono de una autenticación de la máquina expendedora hacia la aplicación que efectúa la verificación 124. Después de la confirmación de la verificación de la edad “mayor que o igual a 16” por el abonado y la entrada del PIN de la tarjeta SIM 202, la aplicación 124 en la tarjeta SIM 202 calcula usando la fecha de nacimiento del abonado almacenada por el operador o proveedor de red de radio móvil y la fecha actual la edad actual del abonado y la compara con la condición requerida para la verificación. La secuencia de números aleatorios entregado por la máquina expendedora junto con la solicitud, la fecha actual proporcionada por el reloj interno incluido en el dispositivo terminal de radio móvil y la verificación real “abonado es de 16 años de edad o más” serán ensamblados a un mensaje 110, se firmada digitalmente utilizando la clave secreta que se encuentra en la tarjeta SIM 202 y se envía de nuevo al máquina expendedora. La máquina expendedora verifica utilizando la clave pública de los uno o más operadores o proveedores de móviles de radio de la red almacenados en la máquina expendedora de la firma digital del mensaje de respuesta 110 y entrega, con el mensaje demostrable sin cambios 110, los cigarrillos deseados, si la secuencia de números aleatoria recibida corresponde al número de secuencia enviado previamente al azar, y si la fecha de recepción y/o la hora corresponde a la fecha y/o hora proporcionada por el reloj interno de la máquina expendedora dentro de una tolerancia preestablecida.

Foros de Internet para chicas

Prerrequisitos:

Un proveedor de una plataforma de comunicación en Internet para chicas de edades entre 12 y 15 años participa en un programa de verificación a través de dispositivos móviles de radio del terminal 218, los cuales se ofrece por un consorcio de operadores o proveedores nacionales de redes de radio móviles.

La clave pública de los operadores o proveedores nacionales móviles de red de radio se almacena en el sistema de los operadores o proveedores nacionales móviles de red de radio.

Una clave generada por el proveedor de la plataforma por los operadores o proveedores nacionales de radio móviles de red se entrega digitalmente al proveedor de la plataforma y también se almacena en el sistema.

Una mujer de 13 años de edad, abonada de telefonía móvil 304 trata de obtener acceso a la plataforma del proveedor. Durante la aplicación en el sitio de portal, a los abonados 304 se les pedirá que proporcionen una verificación de la edad y el género. Una pluralidad de procedimientos puede ser seleccionada.

El abonado mujer 304 selecciona la opción de leer en un Semacode (código de barras bidimensional) utilizando la cámara que se incluye en su dispositivo móvil de la radio 212 terminal. El código se descodifica en y por una

aplicación 124 que se incluye en su dispositivo terminal de radio móvil 212 y los datos de forma descodificados se envían a la aplicación 124 dispuesta en la tarjeta SIM 202. Debido a la distancia espacial al proveedor de la plataforma causado por principio, también el nombre del proveedor y la fecha actual con la hora 905 se incluyen en la solicitud 108. El mensaje completo 108 está firmado digitalmente con la clave secreta del proveedor de la plataforma. Después de la confirmación de la verificación "femenino y edad mayor o igual a 12 y menor de 16 años de edad" por el abonado mujer 304, se comprueba la firma digital 914 del proveedor de la plataforma. Después de haber verificado la firma 914, el abonado mujer 304 se le pide autenticarse a sí misma por medio de la entrada del PIN de la tarjeta SIM 202. Utilizando la fecha de nacimiento del abonado mujer 304 almacenada en la tarjeta SIM 202 de los operadores o proveedores de redes de radio móviles y la fecha actual proporcionada por el reloj interno, la edad actual del abonado mujer 304 se calcula y se compara con la condición requerida en la verificación. También el uso de la aplicación 124, el género del abonado mujer 304, que se almacena en la tarjeta SIM 202 del proveedor de radio móvil, se compara con la condición requerida para la verificación. La secuencia de números aleatorios 904 entregada junto con la solicitud del proveedor, la fecha actual proporcionada por el reloj interno del dispositivo de radio del terminal móvil 218, y el abonado verificación efectiva "es mujer y tiene es de una edad entre 12 y 15 años" se ensambla junto a un mensaje 110, se firma digitalmente con la clave secreta del operador o proveedor de la red de radio móvil ubicado en la tarjeta SIM 202 y se visualiza en la pantalla 204 del dispositivo terminal de radio móvil 218. Después de la entrada del mensaje a través del teclado 206 (a la transmisión de los datos a través de Bluetooth también sería posible), el proveedor de la plataforma comprueba la firma digital 1212 del mensaje de respuesta 110 usando la clave pública del operador o proveedor de la red de radio móvil almacenado en el sistema, y permite que en el caso del mensaje demostrablemente sin cambios 110 el acceso anónimo al portal, si la secuencia de números aleatorios 1204 se corresponde con el número de secuencia enviado previamente al azar 904, y si la fecha 1206 y/o la hora corresponde a la fecha y/u hora proporcionada por el reloj interno del sistema dentro de una tolerancia predeterminada (en su caso, se proporciona una conversión a UTC (Tiempo Universal Coordinado)). En una realización alternativa, puede estar previsto para el caso de que la fecha y/o la hora haya sido enviada junto con la solicitud, para comparar la fecha y/o la hora con el reloj interno y que es sólo se continúa en el procesamiento en caso de que coincida dentro de unos límites predeterminados. La coincidencia puede llevarse a cabo después de la divulgación del certificado (si no se transmite también la fecha y/o la hora), sin embargo, de esta manera, sería posible acercarse a la fecha de nacimiento de una gran cantidad de peticiones.

Tarjeta de tienda de vídeo digital

Prerrequisitos:

Un proveedor de videoclub participa en un programa de verificación a través de dispositivos terminales de radio móvil 218, los cuales se ofrece por un consorcio de operadores o proveedores de redes de radio móviles nacionales.

La clave pública de los operadores o proveedores móviles de red de radio nacionales se almacena en el sistema de los operadores o proveedores móviles de red de radio nacionales.

Además, el fabricante ofrece su sistema de almacenamiento de vídeo con una interfaz Bluetooth 210 para comunicación inalámbrica con dispositivos terminales de radio móviles 218 y un reloj interno.

Un abonado de radio móvil de 17 años de edad 304 se registra para el uso de una tienda de videos. Para ello, proporciona su cédula de identidad personal con el fin de verificar los datos, como por ejemplo nombre, dirección y fecha de nacimiento, almacenados en la base de datos de clientes. Participa en el programa "Tarjeta de Tienda de Video Electrónica". Por lo tanto, durante el registro, un certificado digital, incluyendo el número de cliente del abonado 304 se genera y se almacena en la aplicación 124 para la verificación digital de la tarjeta SIM 202. Esto puede llevarse a cabo a través del operador o proveedor de red de radio móvil de o después de la autenticación de la tienda de videos en comunicación directa con la aplicación 124 para verificaciones digitales. De acuerdo con la ley alemana, sólo a los adultos comenzando a la edad de 18 años se les puede permitir el acceso a la región de adultos de un videoclub. Si el abonado 304 quiere pedir prestado un vídeo, el sistema del cajero de la tienda de vídeo envía una solicitud de cliente 108 a través de Bluetooth. La solicitud 108 incluye de nuevo una secuencia de números aleatorios 904. Debido a la proximidad espacial en el sistema de cajero causada por principio, una autenticación de la tienda de video hacia la aplicación de verificación efectuar 124 está abandonada. De ello se deduce la confirmación de la verificación de los clientes por el abonado 304 y la entrada del PIN de la tarjeta SIM 202. La secuencia de números aleatorios 904 suministrada junto con la solicitud del sistema y el número de cliente almacenado se ensamblan, firmados digitalmente con la clave secreta del operador o proveedor de la red de radio móvil ubicado en la tarjeta SIM 202, y se envía de nuevo al sistema. El sistema verifica la firma digital 1212 del mensaje de respuesta 110 usando la clave pública almacenada del operador o proveedor de la red de radio móvil, y, en caso de un mensaje demostrable sin cambios 110, recupera el registro de datos del cliente, si la secuencia de números aleatorios 1204 corresponde a la secuencia de número aleatorio 904 enviada previamente. También una verificación de edad para el acceso a la sección de adultos se puede realizar de esta manera. Además, la tienda de video ofrece máquinas expendedoras de alquiler, que son también accesibles fuera de las horas normales de trabajo. La autenticación del cliente se lleva a cabo, como se describe en este ejemplo, sin la participación de personal. La oferta de películas tiene en cuenta la edad del cliente incluido en el registro de datos de clientes, y las películas prestadas en la máquina expendedora se apuntan y se almacenan en el registro de datos de clientes.

La figura 14 muestra la estructura de un ejemplar del certificado UIT-T X.509.

La figura 15 muestra un diagrama que se refiere a las firmas digitales. Por un lado, en el lado del receptor 1526, utilizando una función hash 1520, un valor hash 1522 se calcula a partir de la información original 1502 de una manera no cifrada. Por otro lado, en el lado del remitente 1524, utilizando una función hash 1504, un valor hash 1406 se calcula a partir de la información original 1502, que es, sin embargo, cifrada en 1508 usando la clave secreta 1516. Esto genera la firma digital 1510, que se descifra de nuevo en 1512 en el lado del receptor utilizando la clave pública 1518. La firma digital descifrada así generada 1514 se compara con el valor hash cifrado 1522.

Otro campo de aplicación de diversas formas de realización se puede ver en una tarjeta de identidad o pasaporte digital personal, en el que se implementa la verificación de efectuar la funcionalidad, como se describió anteriormente.

De acuerdo con una realización, se proporciona un dispositivo terminal de comunicación para proporcionar un certificado, comprendiendo el dispositivo terminal de comunicación una aplicación, configurada para recibir un primer mensaje desde un dispositivo de comunicación solicitante, en el que el primer mensaje comprende una solicitud para una verificación y una solicitud para información que describe al usuario, en el que la aplicación está configurada además para generar un mensaje de respuesta para el dispositivo de comunicación solicitante, en el que el mensaje de respuesta comprende la verificación que comprende una respuesta a la solicitud, en el que la verificación es firmada digitalmente usando una clave secreta de una entidad de confianza.

En esta realización, el primer mensaje puede comprender una primera firma digital, y la aplicación puede estar configurada además para comprobar la primera firma digital y para procesar la solicitud en caso de una verificación exitosa.

Además, en esta realización, el primer mensaje puede comprender al menos un certificado.

Además, en esta realización, el dispositivo terminal de comunicación puede ser un dispositivo terminal de comunicación móvil.

Además, en esta realización, el dispositivo terminal de comunicación móvil puede ser un dispositivo terminal móvil.

Además, en esta realización, el dispositivo terminal de comunicación puede comprender además una memoria de datos, en el que la aplicación se almacena, y un procesador para ejecutar la aplicación.

Además, en esta realización, el dispositivo terminal de comunicación puede comprender además una tarjeta SIM que comprende una memoria de la tarjeta SIM en el que la aplicación se almacena en la memoria de la tarjeta SIM.

Además, en esta realización, la aplicación puede ser configurada para ser actualizada a través de un canal de transmisión seguro.

Además, en esta realización, el canal de transmisión seguro para la actualización de la aplicación puede ser un canal de transmisión por cable o un canal de transmisión inalámbrico.

Además, en esta realización, el canal de transmisión seguro para la actualización de la aplicación puede ser un canal de transmisión de telecomunicaciones.

Además, en esta realización, el dispositivo terminal de comunicación puede comprender además una interfaz configurada para transmitir mensajes al dispositivo de comunicación y para recibir mensajes desde el dispositivo de comunicación.

Además, en esta realización, la interfaz puede configurarse como al menos uno de los siguientes tipos de interfaces:

una interfaz de datos de un estándar de comunicación de radio;
una interfaz de datos óptica, o
una interfaz de Internet.

Además, en esta realización, el primer mensaje y/o el mensaje de respuesta puede comprender además una secuencia de números aleatorios y/o la fecha y/o hora de la generación del primer mensaje o el mensaje de respuesta.

Además, en esta realización, el dispositivo terminal de comunicación puede comprender además un circuito de codificación configurado para codificar la secuencia de números aleatorios; en el que el dispositivo terminal de comunicación está configurado para insertar la secuencia de número aleatorio cifrada en el mensaje de respuesta.

Además, en esta realización, la aplicación puede estar configurada además para comprobar la autenticidad del usuario.

Además, en esta realización, la aplicación puede estar configurada además para comprobar la autenticidad del

usuario en la aplicación mediante la verificación de una característica de entrada a través de una interfaz de usuario.

Además, en esta realización, el dispositivo terminal de comunicación puede comprender además un circuito de solicitud de confirmación configurado para solicitar una confirmación al usuario del dispositivo terminal de comunicación que el dispositivo terminal de comunicación genera el mensaje de respuesta que comprende la respuesta a la solicitud en el mensaje de solicitud.

Además, en esta realización, la verificación puede comprender un certificado digital.

En una realización, se proporciona un dispositivo de comunicación para proporcionar un mensaje, comprendiendo el dispositivo de comunicación una aplicación configurada para generar un primer mensaje que comprende una solicitud para una verificación y una solicitud para una información que describe al usuario en el que el dispositivo de comunicación está configurado para enviar la primer mensaje a un dispositivo terminal de comunicación y en el que el dispositivo de comunicación está configurado además para recibir un segundo mensaje desde el dispositivo terminal de comunicación, en el que el segundo mensaje comprende una verificación, que ha sido generada sobre la base de la solicitud, en el que la verificación es digitalmente firmada con una clave secreta de una entidad de confianza.

En esta realización, el primer mensaje puede comprender una primera firma digital.

Además, en esta realización, el primer mensaje puede comprender al menos un certificado.

Además, en esta realización, la verificación puede comprender un certificado digital en el que el dispositivo de comunicación comprende además un circuito de evaluación para evaluar al menos el certificado digital comprendido en el segundo mensaje.

Además, en esta realización, el dispositivo de comunicación puede estar configurado para insertar una secuencia de números aleatorios en el primer mensaje.

Además, en esta realización, el dispositivo de comunicación puede estar configurado para tener en cuenta la secuencia de números aleatorios durante la evaluación de la respuesta a la solicitud después de la recepción del segundo mensaje.

Además, en esta realización, el dispositivo de comunicación puede configurarse para insertar la fecha y/la hora en el segundo mensaje.

Además, en esta realización, el dispositivo de comunicación puede estar configurado para insertar el tipo de la verificación en el primer mensaje.

Además, en esta realización, el dispositivo de comunicación puede comprender además una interfaz configurada para transmitir el mensaje al dispositivo terminal de comunicación y para recibir mensajes desde el dispositivo terminal de comunicación.

Además, en esta realización, la interfaz puede configurarse como al menos uno de los siguientes tipos de interfaces:

una interfaz de datos de un estándar de comunicación de radio;
una interfaz de datos óptica, o
una interfaz de Internet.

En una realización, se proporciona una tarjeta electrónica, que comprende circuitos configurados para procesar las señales electrónicas y la información, en la que la información proporciona al menos una aplicación configurada para recibir un primer mensaje desde un dispositivo de comunicación, en el que el primer mensaje comprende una solicitud para una verificación y una solicitud de información que describe el usuario en el que la aplicación está configurada además para generar un mensaje de respuesta para el dispositivo de comunicación solicitante, en el que el mensaje de respuesta comprende la verificación que comprende una respuesta a la solicitud, en el que la verificación es firmada digitalmente usando una clave secreta de una entidad de confianza.

En esta realización, el primer mensaje puede comprender una firma digital, en la que la primera aplicación está configurada además para comprobar la primera firma digital y para procesar la solicitud en caso de una verificación exitosa.

Además, en esta realización, la tarjeta electrónica puede ser una tarjeta SIM de un dispositivo terminal de radio móvil.

Además, en esta realización, la tarjeta electrónica puede estar configurada para comprobar la autenticidad del usuario.

Además, en esta realización, la tarjeta electrónica puede comprender además un circuito de solicitud de confirmación configurado para solicitar una confirmación al usuario de la tarjeta electrónica que el dispositivo

terminal de comunicación genera, comprendiendo el mensaje de respuesta la respuesta a la solicitud en el mensaje de solicitud.

En una realización, se proporciona un procedimiento para proporcionar un certificado, que comprende un dispositivo terminal de comunicación que recibe un primer mensaje desde un dispositivo de comunicación, en el que el primer mensaje comprende una solicitud para una verificación y una solicitud de información que describe al usuario, generando el dispositivo terminal de comunicación un mensaje de respuesta que comprende la respuesta a la solicitud, en el que la respuesta comprende una verificación, en el que la verificación es firmada digitalmente usando una clave secreta de una entidad de confianza, y el dispositivo terminal de comunicación enviando el mensaje de respuesta a un dispositivo de comunicación.

En esta realización, el primer mensaje puede comprender una firma digital primera y la primera firma digital puede ser revisada y la solicitud puede ser procesada en caso de una verificación exitosa.

Además, en esta realización, el primer mensaje puede comprender al menos un certificado.

Además, en esta realización, el dispositivo terminal de comunicación puede ser un dispositivo terminal de comunicación móvil.

Además, en esta realización, el dispositivo terminal de comunicación puede ser un dispositivo terminal de radio móvil.

Además, en esta realización, al menos la verificación de la primera firma digital y la generación del segundo certificado pueden ser llevadas a cabo por una aplicación almacenada en una tarjeta SIM.

Además, en esta realización, el dispositivo terminal de comunicación puede además comprobar la autenticidad del usuario.

Además, en esta realización, el dispositivo terminal de comunicación puede comprobar la autenticidad del usuario que usa una entrada característica a través de una interfaz de usuario.

Además, en esta realización, el dispositivo terminal de comunicación puede solicitar una confirmación por parte de un usuario para confirmar la transmisión y la subsiguiente generación del mensaje de respuesta que comprende la respuesta a la solicitud de la información que describe al usuario.

Además, en esta realización, el dispositivo terminal de comunicación puede enviar o recibir los mensajes a través de uno de los siguientes tipos de interfaces:

una interfaz de datos de un estándar de comunicación de radio;
una interfaz de datos óptica, o
una interfaz de Internet.

Además, en esta realización, el dispositivo terminal de comunicación además puede insertar en el mensaje de respuesta una secuencia de números aleatorios y/o la fecha y/o la hora de generación del mensaje de respuesta.

En una realización, un procedimiento para proporcionar un certificado se proporciona, el procedimiento comprende un dispositivo de comunicación de la generación de un primer mensaje que comprende una solicitud para una verificación y una solicitud de información que describe el usuario, el dispositivo de comunicación que envía el primer mensaje a un dispositivo terminal de comunicación; el dispositivo de comunicación recibe un mensaje de respuesta que comprende la respuesta a la solicitud, en el que la respuesta comprende una verificación, en la que la verificación es firmada digitalmente usando una clave secreta de una entidad de confianza.

En esta realización, el primer mensaje puede comprender una primera firma digital.

Además, en esta realización, el primer mensaje puede comprender al menos un certificado.

Además, en esta realización, el dispositivo de comunicación puede comprobar la firma digital del certificado digital.

Además, en esta realización, el dispositivo de comunicación puede insertar el tipo de la verificación solicitada en el mensaje de respuesta.

Además, en esta realización, el dispositivo de comunicación puede insertar una secuencia de números aleatorios y/o la fecha y/o la hora de generación del primer mensaje en el primer mensaje.

Además, en esta realización, el dispositivo de comunicación puede enviar o recibir los mensajes a través de al menos uno de los siguientes tipos de interfaces:

una interfaz de datos de un estándar de comunicación de radio;
una interfaz de datos óptica, o
una interfaz de Internet.

Si bien la invención se ha mostrado y descrito particularmente con referencia a realizaciones específicas, debe entenderse por los expertos en la técnica que varios cambios en forma y detalle se pueden hacer en la misma sin apartarse del alcance de la invención como se define por las reivindicaciones adjuntas. El alcance de la invención está indicado por las reivindicaciones adjuntas y por lo tanto todos los cambios que entren dentro del significado y el rango de equivalencia de las reivindicaciones están destinados a ser incluidos.

REIVINDICACIONES

1. Dispositivo terminal de comunicación para proporcionar un mensaje de respuesta para un dispositivo de comunicación solicitante, comprendiendo el dispositivo terminal de comunicación:

una aplicación, configurada para recibir un primer mensaje desde el dispositivo de comunicación solicitante; en el que el primer mensaje comprende una solicitud de verificación de la información sobre las características personales de un usuario del dispositivo terminal de comunicación;
en el que el dispositivo terminal de comunicación autentica al usuario; en el que la aplicación está configurada además para verificar las características personales contra valores almacenados para generar con ello un resultado de la verificación y, para el caso de que el resultado de la verificación de las características personales sea positivo, para
generar el mensaje de respuesta para el dispositivo de comunicación solicitante, en el que el mensaje de respuesta comprende el resultado, en el que el resultado es firmado digitalmente usando una clave secreta de una entidad de confianza, y para el caso de que el resultado es negativo, ya sea para no generar un mensaje de respuesta o para generar un mensaje de respuesta negativa, incluyendo una respuesta de que la característica que se debe verificar no se cumple.

2. El dispositivo terminal de comunicación según la reivindicación 1,
en el que el primer mensaje comprende una primera firma digital, y
en el que la aplicación está configurada además para comprobar la primera firma digital y para procesar la solicitud en caso de una verificación exitosa.

3. El dispositivo terminal de comunicación según la reivindicación 1 ó 2,
en el que el primer mensaje comprende al menos un certificado.

4. El dispositivo terminal de comunicación según una cualquiera de las reivindicaciones 1 a 3, que comprende además:

una tarjeta SIM que comprende una memoria de la tarjeta SIM;
en el que la aplicación se almacena en la memoria de la tarjeta SIM.

5. El dispositivo terminal de comunicación según una cualquiera de las reivindicaciones 1 a 4,
en el que la aplicación está configurada para ser actualizada a través de un canal de transmisión seguro.

6. El dispositivo terminal de comunicación según una cualquiera de las reivindicaciones 1 a 5,
en el que el primer mensaje y/o el mensaje de respuesta además comprende o comprenden una secuencia de números aleatorios y/o la fecha y/o la hora de la generación del primer mensaje o del mensaje de respuesta.

7. El dispositivo terminal de comunicación según la reivindicación 6, que comprende además:

un circuito de codificación configurado para codificar la secuencia de números aleatorios;
en el que el dispositivo terminal de comunicación está configurado para insertar la secuencia de cifrado de números aleatorios en el mensaje de respuesta.

8. El dispositivo terminal de comunicación según una cualquiera de las reivindicaciones 1 a 7, que comprende además:

un circuito solicitante de confirmación configurado para solicitar una confirmación del usuario del dispositivo terminal de comunicación de que el dispositivo terminal de comunicación genera el mensaje de respuesta que comprende la respuesta a la solicitud en el mensaje de solicitud.

9. El dispositivo terminal de comunicación según una cualquiera de las reivindicaciones 1 a 8,
en el que la verificación comprende un certificado digital.

10. Procedimiento para proporcionar un mensaje de respuesta para un dispositivo de comunicación solicitante, comprendiendo el procedimiento:

un dispositivo terminal de comunicación que recibe un primer mensaje desde el dispositivo de comunicación solicitante, en el que el primer mensaje comprende una solicitud de verificación de la información sobre las características personales de un usuario del dispositivo terminal de comunicación, autentificando el aparato terminal de comunicación al usuario, verificando las características personales contra los valores almacenados para generar con ello un resultado de la verificación y, para el caso de que el resultado de la verificación de las características personales es positivo, generando el mensaje de respuesta para el dispositivo de comunicación solicitante, en el que el mensaje de respuesta comprende el resultado, en el que el resultado está firmado digitalmente usando una clave secreta de una entidad de confianza, y para el caso de que el resultado es negativo, no generando un mensaje de respuesta o generando de un mensaje de respuesta negativa, incluyendo una respuesta de que la característica que se debe verificar no se cumple; y
el dispositivo terminal de comunicación envía el mensaje de respuesta o, en su caso, el mensaje de respuesta

negativa, al dispositivo de comunicación solicitante.

FIG 1

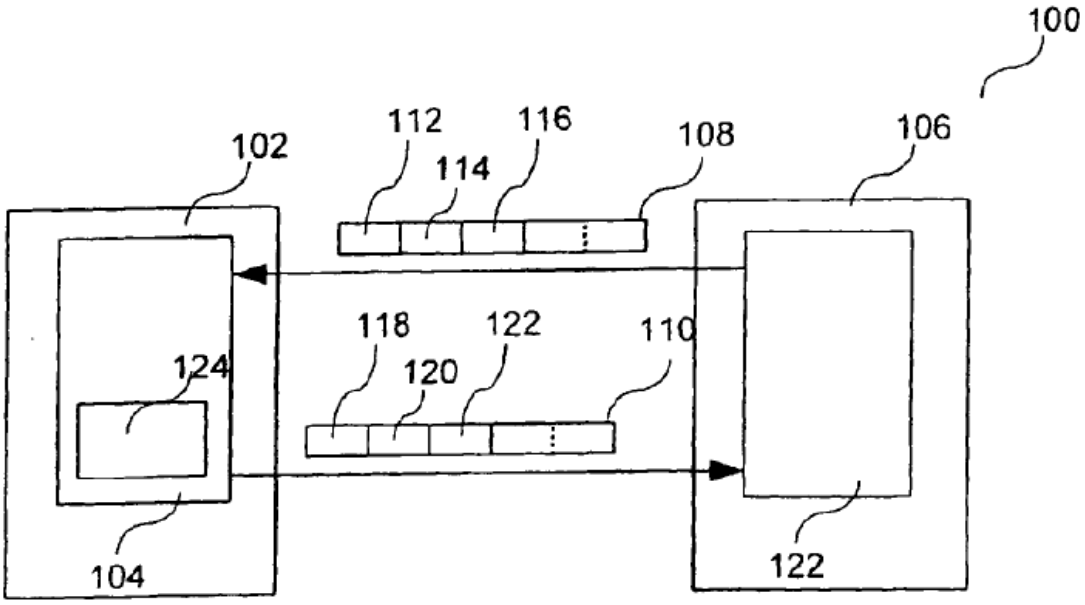
100
102
112
116
114
108
106
118
122
110
120
124
104
122

FIG 2A

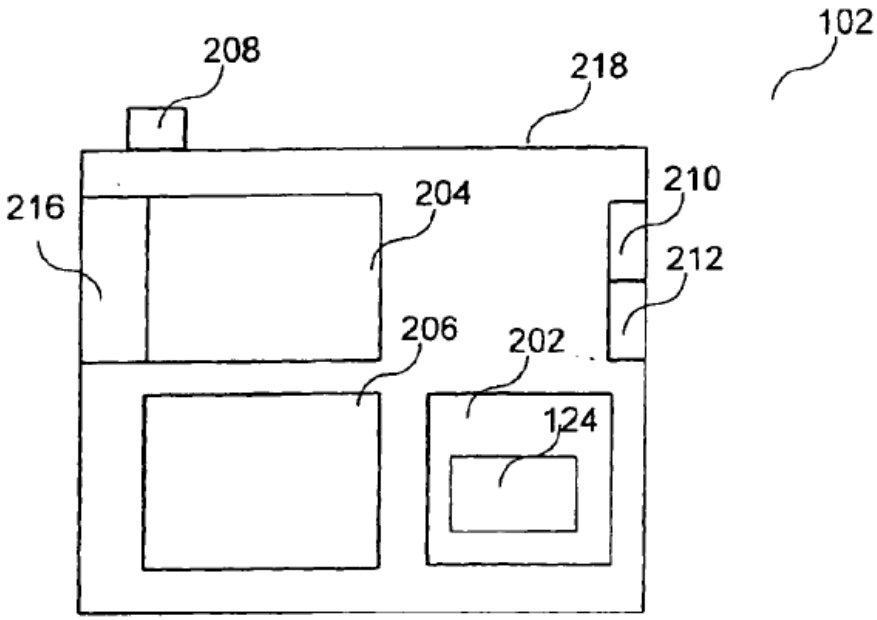
102
208
218
216
204
210
212
206
202
124

FIG 2B

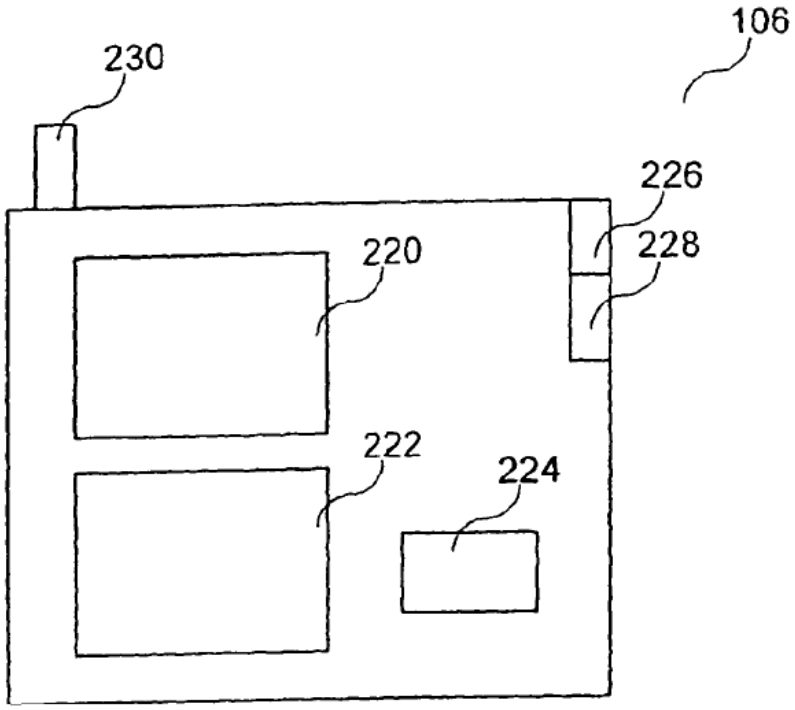

FIG 3

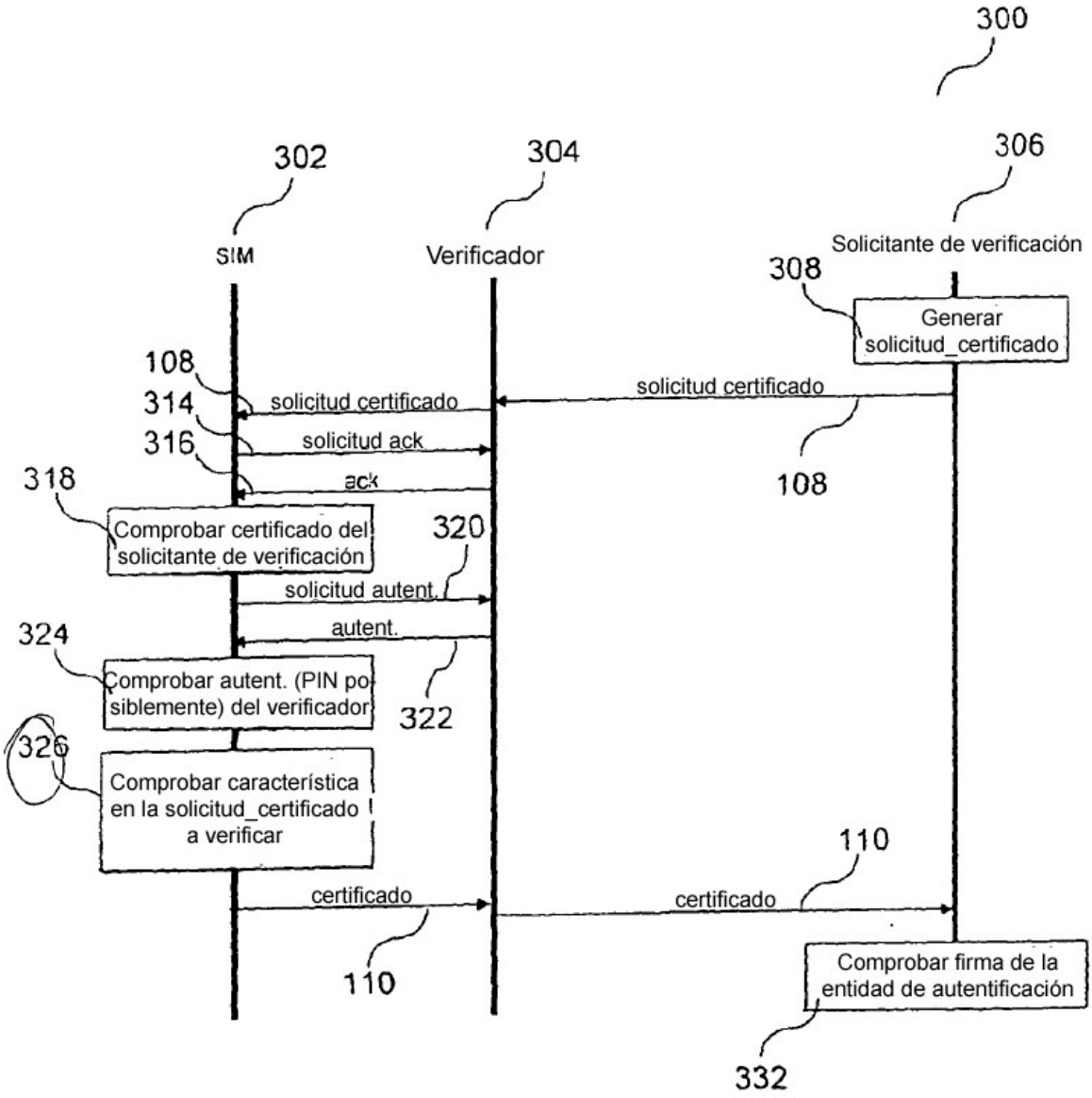
300
302
304
306
SIM
Verificador
Solicitante de verificación
308
Generar solicitud_certificado
108
314
316
318
solicitud certificado
solicitud ack
ack
solicitud certificado
108
Comprobar certificado del solicitante de verificación
320
solicitud autent.
autent.
324
Comprobar autent. (PIN posiblemente) del verificador
322
326
Comprobar característica en la solicitud_certificado a verificar
110
certificado
certificado
110
Comprobar firma de la entidad de autentificación
332

FIG 4

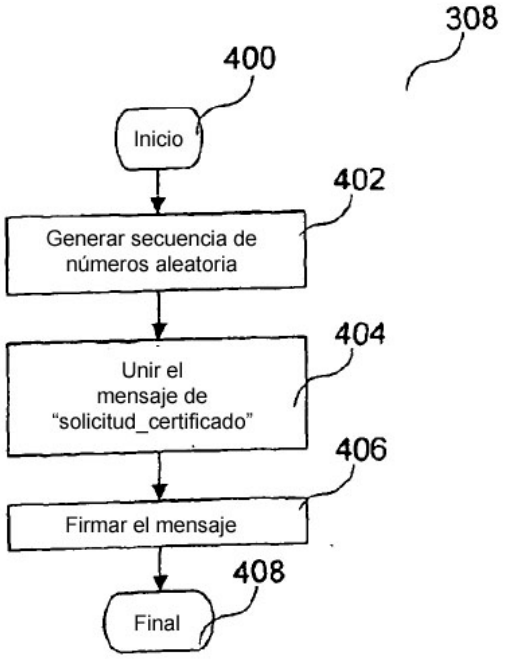
308
400
Inicio
402
Generar secuencia de números aleatoria
404
Unir el mensaje de "solicitud_certificado"
406
Firmar el mensaje
408
Final

FIG 6

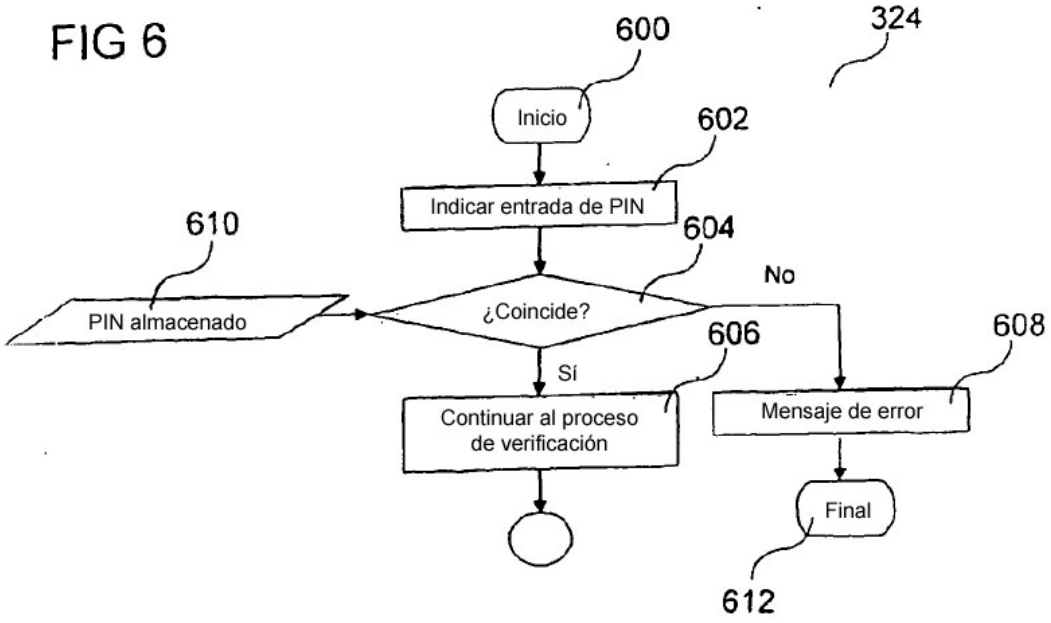
324
600
Inicio
602
Indicar entrada de PIN
610
PIN almacenado
604
¿Coincide?
No
Sí
606
Continuar al proceso de verificación
608
Mensaje de error
Final
612

FIG 5

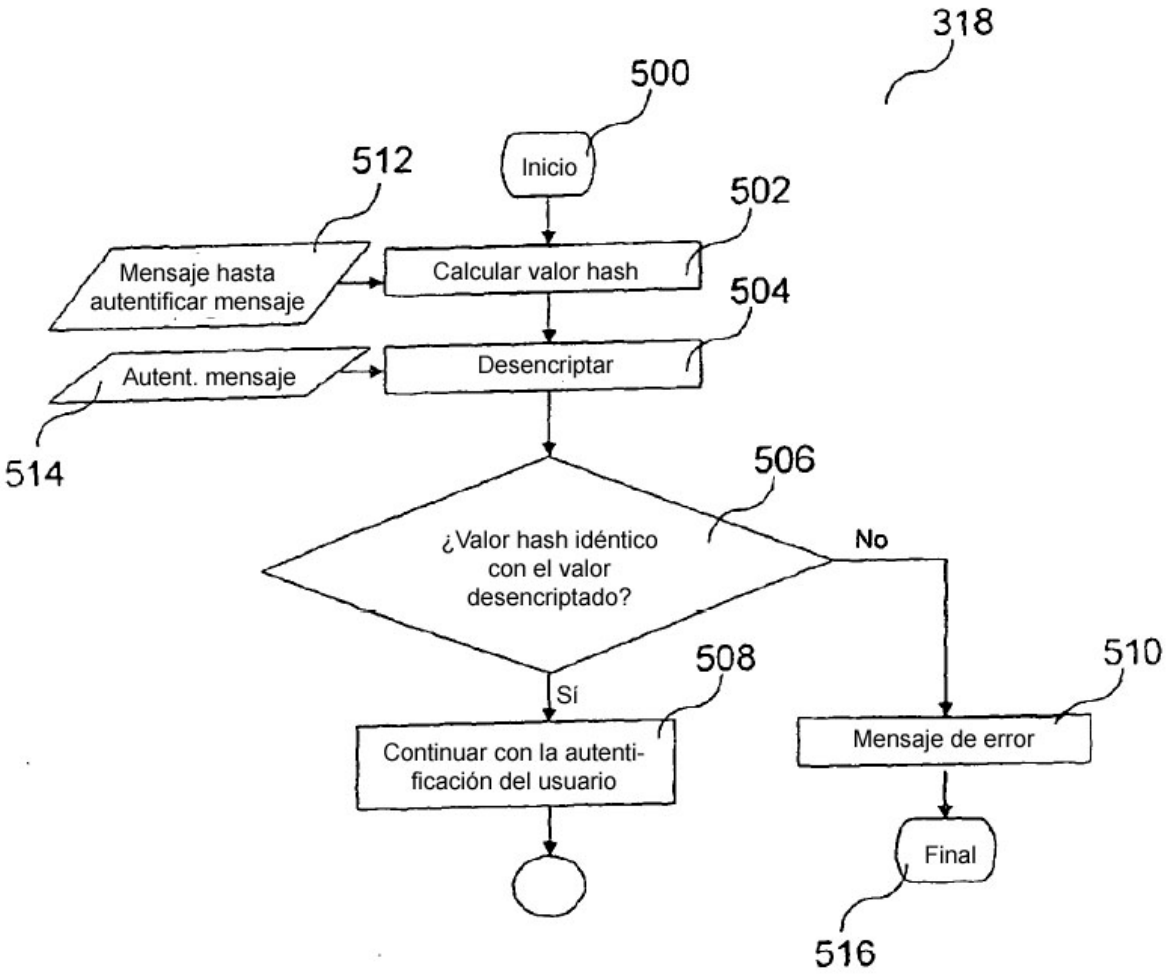
318
500
Inicio
512
Mensaje hasta autentificar mensaje
502
Calcular valor hash
504
Desencriptar
Autent. mensaje
514
506
¿Valor hash idéntico con el valor desencriptado?
No
Sí
508
Continuar con la autenti-ficación del usuario
510
Mensaje de error
Final
516

FIG 7

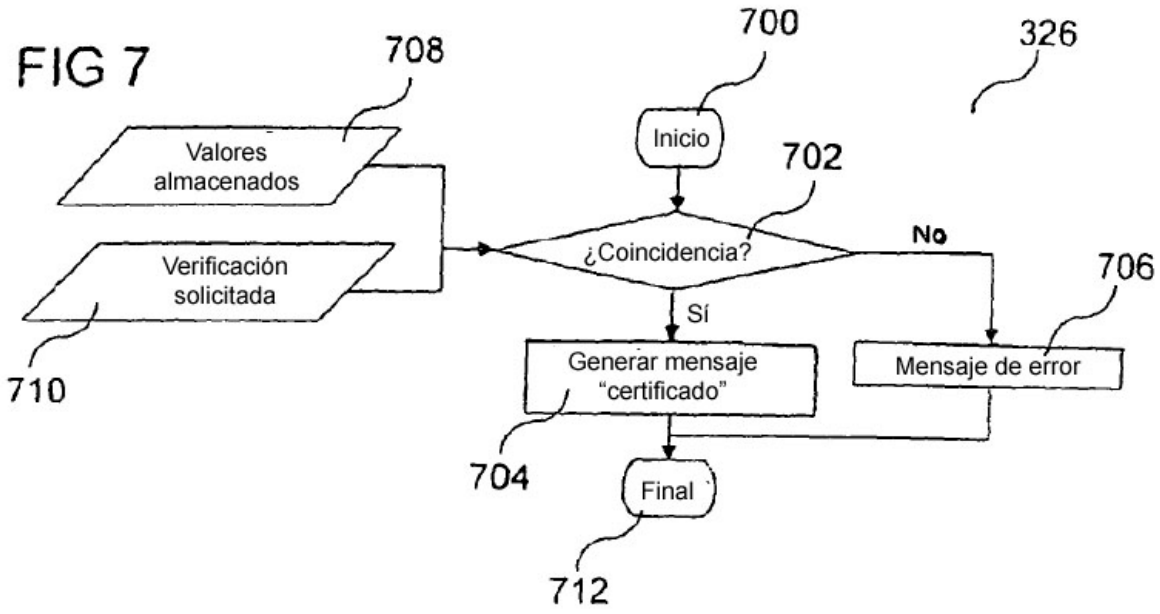
700
326
708
Inicio
Valores almacenados
702
¿Coincidencia?
No
Verificación solicitada
706
Sí
Generar mensaje "certificado"
Mensaje de error
710
704
Final
712

FIG 8

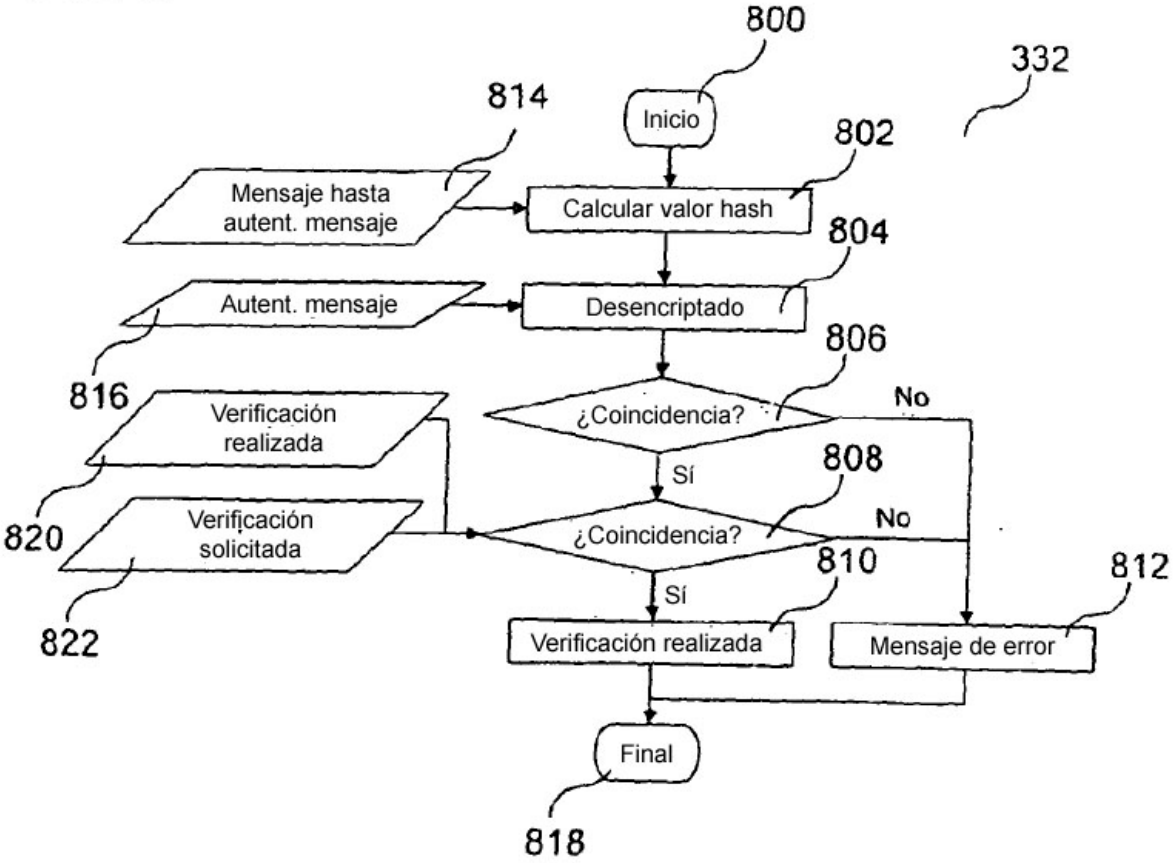
800
332
814
Inicio
802
Mensaje hasta autent. mensaje
Calcular valor hash
804
Autent. mensaje
Desencriptado
806
816
¿Coincidencia?
No
Verificación realizada
Sí
808
820
Verificación solicitada
¿Coincidencia?
No
810
812
Sí
822
Verificación realizada
Mensaje de error
Final
818

FIG 9

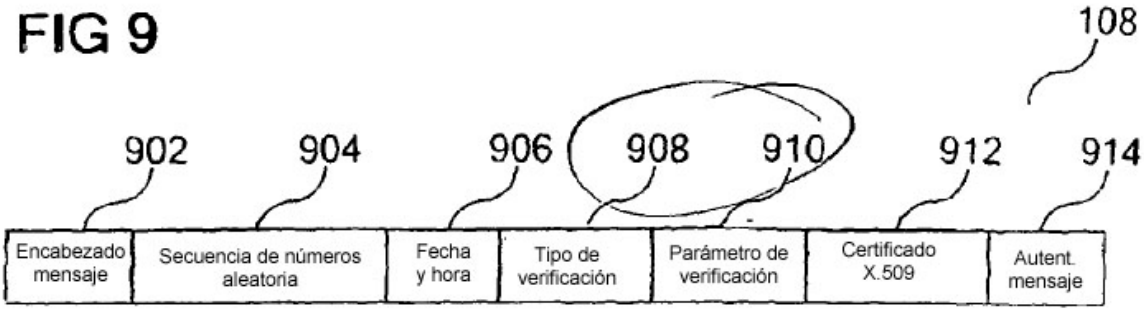

FIG 10

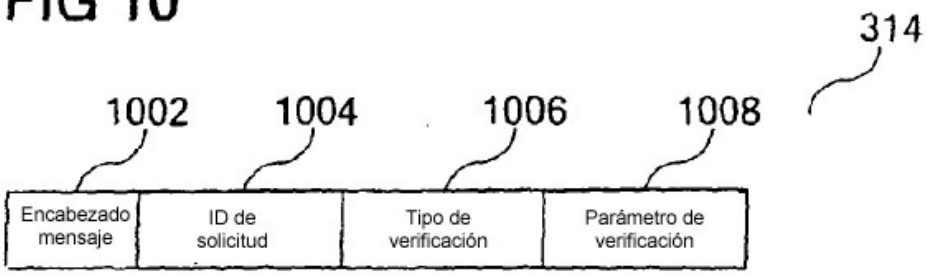

FIG 11

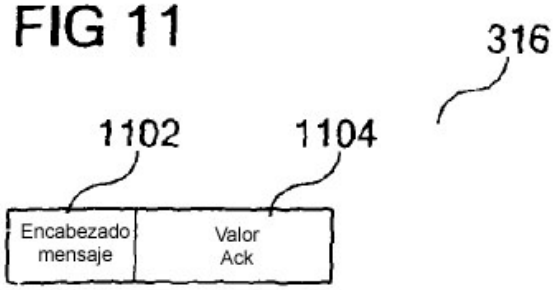

FIG 12

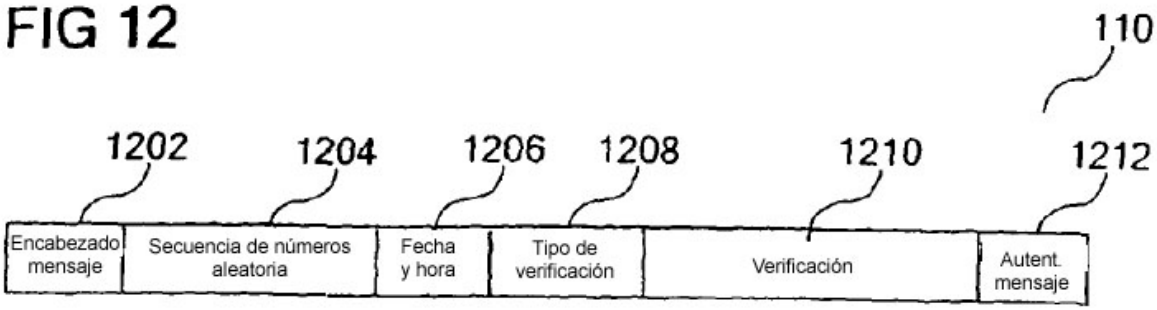

FIG 13A

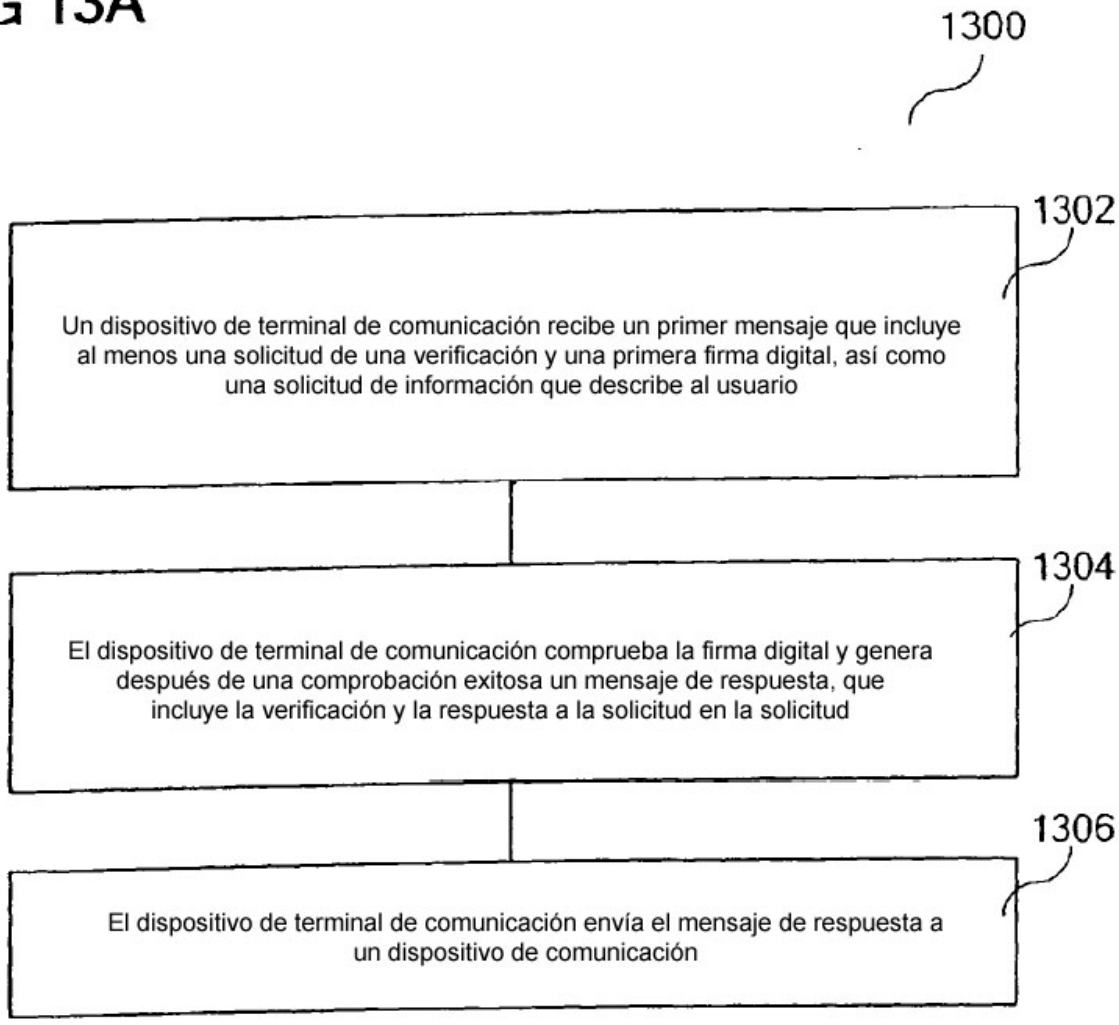
1300
1302
Un dispositivo de terminal de comunicación recibe un primer mensaje que incluye al menos una solicitud de una verificación y una primera firma digital, así como una solicitud de información que describe al usuario
1304
El dispositivo de terminal de comunicación comprueba la firma digital y genera después de una comprobación exitosa un mensaje de respuesta, que incluye la verificación y la respuesta a la solicitud en la solicitud
1306
El dispositivo de terminal de comunicación envía el mensaje de respuesta a un dispositivo de comunicación

FIG 13B

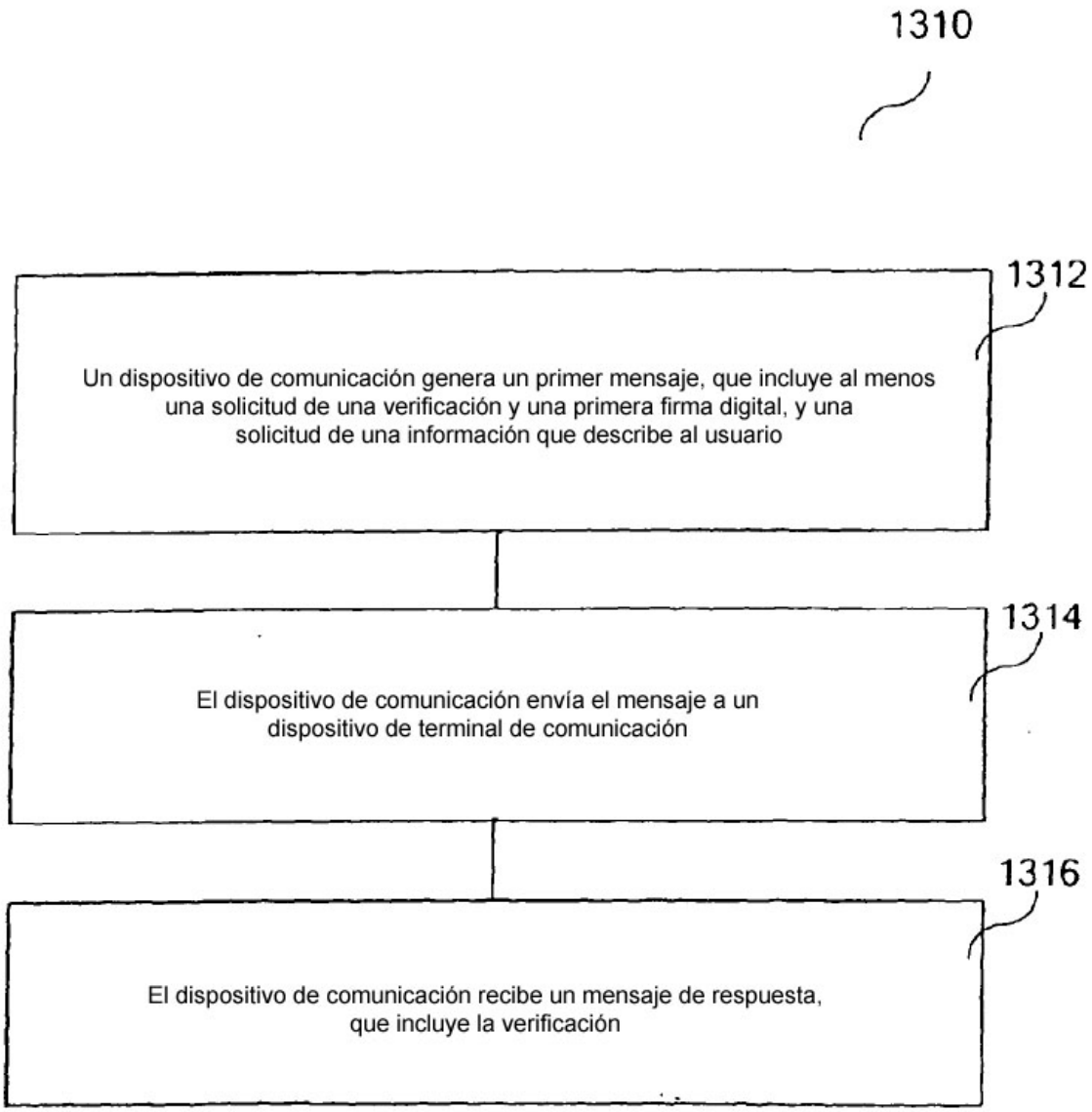
1310
1312
Un dispositivo de comunicación genera un primer mensaje, que incluye al menos una solicitud de una verificación y una primera firma digital, y una solicitud de una información que describe al usuario
1314
El dispositivo de comunicación envía el mensaje a un dispositivo de terminal de comunicación
1316
El dispositivo de comunicación recibe un mensaje de respuesta, que incluye la verificación

FIG 14

- Certificado
  - Versión
  - Número de serie
  - ID algoritmos
  - Emisor
  - Validez
    - desde
    - hasta
  - Sujeto
  - Información de clave pública sujeto
    - Algoritmo de clave pública
    - Clave pública sujeto
  - ID única del emisor (opcional)
  - ID única del propietario (opcional)
  - Extensiones
    - ....
- Algoritmo de firma del certificado
- Firma del certificado

FIG 15