(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 750 250**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04L 29/06 (2006.01)
H04W 12/04 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **22.10.2007 PCT/FI2007/000255**

(87) Fecha y número de publicación internacional: **02.05.2008 WO08049959**

(96) Fecha de presentación y número de la solicitud europea: **22.10.2007 E 07823115 (6)**

(97) Fecha y número de publicación de la concesión europea: **24.07.2019 EP 2078371**

(54) Título: **Método y sistema para utilizar el registro PKCS en un entorno móvil**

(30) Prioridad:

23.10.2006 FI 20060930

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.03.2020

(73) Titular/es:

GEMALTO OY (100.0%)
Myllynkivenkuja 4
01620 Vantaa, FI

(72) Inventor/es:

HEINONEN, PETTERI;
WEBSTER, MICHAEL ALEXANDER y
LINDSTRÖM, JUHA

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método y sistema para utilizar el registro PKCS en un entorno móvil

Campo técnico de la invención

La invención se refiere a un método y sistema para usar el registro PKCS en un entorno móvil y especialmente en un entorno WPKI (PKI inalámbrica) que comprende un servidor de registro y un cliente, tal como un terminal. En particular, la invención se refiere a un método de registro, donde una solicitud de registro para una clave pública de un par de claves generada en el terminal es proporcionada al servidor de registro para que se registre usando la estructura PKCS, en particular, la estructura PKCS#10. Aun así, la invención es aplicable no solo para claves generadas en el terminal, la SIM, la UICC o el módulo de hardware (resistente a la manipulación), sino también para claves pregeneradas, tal como las claves almacenadas durante la fabricación o personalización del terminal, la SIM, la UICC, y/o el módulo de hardware (cliente).

Antecedentes de la invención

Para ser identificado en un entorno WPKI (PKI inalámbrica), un usuario debe tener un cierto certificado de identificación que incluya la clave pública PKI (y la clave privada correspondiente almacenada de forma segura) utilizada para firmar y abrir mensajes enviados por el usuario, por ejemplo. Se sabe de la técnica anterior que se proporciona un par de claves PKI previamente, por ejemplo, por un fabricante del terminal, o tarjeta SIM/UICC (SIM son las siglas en inglés para “Módulo de identidad del suscriptor” y UICC para “Tarjeta de circuito integrado universal”) del terminal, si se utiliza el par de claves de la tarjeta SIM/UICC, así como también para generar claves "integradas". También se sabe que se utiliza una ruta de transmisión segura entre el servidor OTA (*Over The Air* o “por el aire”) y la tarjeta SIM cuando se entrega un par de claves a la tarjeta SIM. Cuando el fabricante genera el par de claves o solo una clave (clave PKI privada o una clave simétrica), la clave pública del par de claves puede registrarse y conectarse a la información de identificación del usuario de manera confiable cuando el usuario es conocido cuando se almacena el par de claves en su terminal o bien se da al usuario el terminal con el par de claves, por ejemplo.

Sin embargo, hoy en día las situaciones en las que un cliente debe generar un par de claves PKI, tal como un terminal o mediante algún componente en el terminal (tal como la tarjeta SIM/UICC), solo en caso de ser necesario, se vuelven más habituales, como también las situaciones donde las claves pregeneradas no se registran hasta que sea necesario. Para ser fiable, la clave pública del par de claves generadas debe estar registrada o certificada con una autoridad de certificación, como un operador móvil, un banco o una agencia gubernamental.

En la técnica anterior, por ejemplo, se conocen estándares especiales, tales como los Estándares de criptografía de clave pública (PKCS), que son especificaciones producidas por los Laboratorios RSA en cooperación con desarrolladores de sistemas seguros en todo el mundo con el fin de acelerar el despliegue de la criptografía de clave pública. Especialmente un PKCS#10 (Estándar de sintaxis de solicitud de certificación) describe la sintaxis para una solicitud de certificación de una clave pública, un nombre y posiblemente un conjunto de atributos. Se sabe de la técnica anterior que se utiliza el estándar PKCS#10 para registrar o certificar una clave pública generada por un terminal con un servidor de registro, tal como el servidor de registro de una autoridad de certificación.

Sin embargo, existen algunas desventajas en las soluciones de la técnica anterior, a saber, en primer lugar, en una determinada solución de la técnica anterior, solo se devuelve una clave pública generada, por lo que no se puede estar seguro de si la clave pública es la clave pública original generada por el terminal asumido, o si es el mensaje manipulado. En segundo lugar, la clave pública no se puede poner en un formato autofirmado dentro del estándar PKCS#10, porque carece de firma. Además, si se devuelve toda la estructura PKCS#10, se necesitan muchos mensajes SMS para enviarse entre el terminal y el servidor de registro y, por lo tanto, se requiere mucha capacidad de transferencia de datos del sistema de transmisión. Además, si toda la información se devuelve como estructura PKCS#10, el canal de retorno necesita estar asegurado de extremo a extremo mediante autenticación y cifrado, algo que no es siempre posible, especialmente en un entorno móvil.

El borrador del Grupo de trabajo IETF sobre PKIX de YOON (KISA) *et al.*, titulado “Protocolo y formato de mensaje de solicitud de certificado de infraestructura de clave pública x.509 de internet inalámbrico (WCRMFP, por sus siglas en inglés), draft-yoon-pkix-wireless-internet-01.txt", de mayo de 2002, es técnica anterior adicional.

Compendio de la invención

Un objetivo de la invención es proporcionar un método y un sistema para un proceso de registro PKCS estándar para una clave pública cuyo registro es solicitado por un cliente en un canal de comunicación que tiene una capacidad de datos limitada y donde también la seguridad podría ser limitada. En particular, el objeto de la invención es minimizar una cantidad de mensajes SMS utilizados para el proceso de registro PKCS cuando se usa la tarjeta SIM/UICC (o similar) en un entorno móvil y especialmente en un entorno WPKI que comprende un terminal y un servidor de registro.

El objetivo de la invención se cumple al proporcionar a un cliente que solicita un registro de un par de claves solo una parte de la información de solicitud de certificado definida en el estándar de registro PKCS, formando mediante el cliente una estructura PKCS estándar de dicha parte de la información de solicitud de certificado recibida y de la clave

pública a registrar, o al menos información relacionada con dicha clave pública a registrar, usando al menos parte de dicha estructura de registro PKCS estándar formada, formada para determinar un código de verificación y entregar dicho código de verificación y la clave pública a dicho servidor de registro ventajosamente sin entregar dicha parte de la información de solicitud de certificado recibida al principio por el cliente.

La presente invención se refiere a un método de la reivindicación 1 y a un sistema de la reivindicación 8. Además, la presente invención se refiere a un servidor de registro de la reivindicación 10, un cliente de la reivindicación 11 y productos de programas informáticos de las reivindicaciones 12 y 13.

En este documento, un cliente representa un terminal, o SIM, UICC o módulo de hardware (como una memoria flash de confianza o un chip integrado), que es resistente a la manipulación y/o a prueba de manipulación, o con otros medios de resistencia a la manipulación utilizados normalmente en el terminal. Además, debe tenerse en cuenta que el cliente genera una clave o un par de claves para registrarse ("integradas"), pero la clave o el par de claves también pueden generarse previamente aparte del cliente, tal como por ejemplo por el fabricante del cliente (terminal, SIM, UICC o módulo de hardware) después de lo cual el cliente recibe la clave y/o las claves pregeneradas y finalmente, cuando es necesario, dicho cliente solicita un registro de la clave (y/o claves). El cliente también puede implementarse mediante un circuito o producto de programa informático que comprende medios de código de software que normalmente se ejecutan en el terminal, tal como en un ordenador o un teléfono móvil.

Más detalladamente, una clave pública de un par de claves (incluidas las claves privadas y públicas), la cual es proporcionada al cliente, debe registrarse en un servidor de registro de una autoridad de certificación, por ejemplo. El servidor de registro, ventajosamente, envía parte de la información de solicitud de certificado definida en el PKCS al cliente, utilizable para formar una estructura de registro PKCS estándar. Ambas partes (el cliente y el servidor de registro finalizan) saben cómo agregar el resto de la información a la información de solicitud de certificado a fin de completarla.

Cabe señalar que ventajosamente solo parte de dicha información de solicitud de certificado se entrega al cliente para minimizar los datos que se entregarán. Según una realización de la invención, al menos parte de la información de solicitud de certificado, o bien la solicitud, se cifra antes de enviarse. El cifrado se realiza ventajosamente utilizando la clave pública de un cliente, cuando la clave pública ha sido proporcionada previamente al cliente, por ejemplo, por un fabricante del cliente, tal como un terminal, una tarjeta SIM/UICC o por una operadora. El cifrado también se realiza normalmente usando claves asimétricas y, por ejemplo, el algoritmo RSA. Además, la información de solicitud de certificado se envía ventajosamente a través de una primera conexión de comunicación de datos establecida entre el servidor de registro y el cliente.

Cuando se recibe dicha información de solicitud de certificado, dicho cliente descifra una posible parte encriptada de ella utilizando su clave privada, después de lo cual el cliente forma una estructura de registro PKCS estándar usando al menos una porción de dicha parte de la información de solicitud recibida desde el servidor de registro y la clave pública que se registrará. Sin embargo, también es posible utilizar la totalidad de dicha información de solicitud de certificado recibida, y/o solo una parte relevante de la información de clave pública de la clave pública a registrarse.

Después de formar dicha estructura de registro PKCS, se determina un código de verificación sobre dicha estructura de registro PKCS estándar. También es posible usar solo porciones relevantes de dicha estructura PKCS sobre las cuales se determina el código de verificación. El cliente puede firmar el código de verificación determinado, así como la clave pública a registrar, después de lo cual el código de verificación y la clave pública se entregan a dicho servidor de registro. El código de verificación, que es ventajosamente un código *hash* de la combinación, se determina ventajosamente utilizando un algoritmo unidireccional, como SHA-1 o SHA-2, MD5, RIPEMD, RIPEMD-160, (RIPEMD-128, RIPEMD-256 y RIPEMD-320), el algoritmo Tiger o el WHIRLPOOL.

Además, la segunda información (como una contraseña de comprobación y/o datos de entorno del cliente, tal como el ICCID (siglas en inglés para “ID de tarjeta de circuito integrado”) leído de la tarjeta) también se puede utilizar para formar dicha estructura PKCS estándar, donde los datos de entorno son también conocidos ventajosamente por dicho servidor de registro. Dicha segunda información utilizada para formar la estructura PKCS estándar también puede ser información entregada al cliente a través de una segunda conexión separada de una conexión de comunicación de datos utilizada para entregar dicha parte de la información de solicitud de certificado al terminal. La segunda información puede ser una prueba de posesión o una contraseña de comprobación, pero también puede ser cualquier otra información, tal como una cadena de caracteres aleatorios conocida también por el servidor de registro. Según una realización de la invención, dicha segunda información puede ser una combinación de al menos datos o información descrita anteriormente, tal como una combinación de datos de entorno e información enviada por el servidor de registro. Además, dicha segunda información o al menos parte de ella puede contener la suma de verificación de Luhn o cualquier otra suma de verificación, pudiéndose hacer una comprobación de validez local de la segunda información.

Dicho código de verificación y la clave pública (y la posible segunda información) se reciben y se forma además una estructura de registro PKCS estándar en el servidor de registro, que también conoce dicha porción de dicha parte de la información de solicitud utilizada en el terminal para formar dicha estructura de registro PKCS estándar, así como dicha segunda información (si se usa). Entonces, el servidor de registro forma una estructura de registro PKCS

estándar también por sí mismo y usando dicha porción de dicha parte de la información de solicitud utilizada por el cliente para formar la estructura de registro PKCS estándar y la clave pública recibida generada por el cliente, después de lo cual el servidor de registro determina un código de verificación sobre la misma porción de dicha estructura de registro PKCS estándar formada en el servidor de registro tal como es utilizada por el cliente. Cuando el servidor de registro ha determinado el código de verificación, el servidor de registro lo compara con el código de verificación recibido del cliente, y si estos dos son idénticos, la clave pública se registra en el servidor de registro.

En la invención, el cliente es una tarjeta SIM, una tarjeta UICC, medios de resistencia a la manipulación o un terminal, donde el terminal es ventajosamente un teléfono móvil o un ordenador portátil que comprende una tarjeta SIM, una tarjeta UICC y/o medios de resistencia a la manipulación. El par de claves se puede generar, por ejemplo, en el terminal utilizando los medios del terminal adaptados a esta generación o en la tarjeta SIM y/o la UICC del terminal.

El cliente puede firmar el código de verificación antes de enviarlo al servidor de registro, como se describió con anterioridad en este documento. Según una realización ventajosa de la invención, el código de verificación está firmado por la clave privada del par de claves, cuya clave pública está en dicha estructura de registro PKCS.

Según una realización adicional de la invención, se activa una determinada ventana de tiempo durante la cual el código de verificación y la clave pública a registrar deben recibirse en el servidor de registro a fin de registrarse. De lo contrario, la solicitud de registro se rechaza automáticamente en el servidor de registro. La entrega de la parte de la información de solicitud de certificado se puede utilizar para activar la ventana de tiempo determinado, por ejemplo.

Al enviar solo el código de verificación y la clave pública en lugar de enviar una estructura de registro PKCS completa y/o una segunda información, se puede reducir notablemente la carga en un sistema de comunicación utilizado para la transmisión de datos entre el cliente y el servidor de registro. También se puede lograr un cálculo mucho más simple en el terminal o cliente, ya que todas las operaciones para calcular una estructura ASN.1 se realizan en el servidor de registro en lugar del cliente o terminal o la SIM/UICC, los cuales realmente no pueden hacer todas estas operaciones. [ASN.1 (siglas en inglés para “Notación sintáctica abstracta 1”) es una notación estándar y flexible que describe estructuras de datos para representar, codificar, transmitir y decodificar datos]

También debe tenerse en cuenta que cuando parte de la información de solicitud de certificado (y posiblemente también la segunda información) se cifra antes de entregarse al cliente, los terceros no pueden determinar el código de verificación según lo determinado por el cliente porque no tienen dicha información de solicitud de certificado y/o segunda información con la clave pública, sobre la cual el cliente determina el código de verificación.

Por ejemplo, si un tercero desea enviar su clave al servidor de registro robando el código de verificación y la clave pública del usuario original, y reemplazando la clave pública del usuario original por su propia clave pública, el servidor de registro se percatará de esto porque los códigos de verificación no serían idénticos, es decir, el código de verificación determinado por el servidor de registro que utiliza parte de la información de solicitud de certificado y la posible segunda información con la clave pública del tercero no serían idénticos al código de verificación determinado por el cliente. Por otro lado, si un tercero determina un nuevo código de verificación utilizando su clave pública, el servidor de registro también se percatará porque el tercero no tiene la información de solicitud de certificado ni la segunda información utilizada por el cliente para determinar el código de verificación. Esta es una razón adicional por la cual la información de solicitud de certificado y la posible segunda información no se entregan con el código de verificación y/o la clave pública al servidor de registro.

Según una realización de la invención, la información recopilada del entorno del cliente también se puede usar como segunda información o al menos parte de la segunda información cuando se determina un código de verificación, tal como el número de serie del cliente, la información de una aplicación o producto de programa informático ejecutado en el terminal y/o la información de la tarjeta SIM/UICC del terminal y/o el IMEI y/o el IMSI y/o el número de identificación del procesador y/o el código de identificación único del terminal y/o el ICCID. Una posibilidad es también solicitar cierta información al usuario del terminal. Sin embargo, el servidor de registro también debe conocer la información anterior para determinar el código de verificación correcto. Parte de la información, que el servidor de registro no conoce previamente, también debe transmitirse del cliente al servidor de registro en la 3ª comunicación o utilizando algún otro medio.

Según una realización de la invención, se puede solicitar al usuario un código PIN para activar los procesos de descifrado/cifrado/firma, o la generación de un nuevo par de claves. En una realización, el código PIN también puede tenerse en cuenta cuando se determina un código de verificación.

Además, debe tenerse en cuenta que incluso si este documento establece un cliente como un terminal utilizado para generar y/o al menos solicitar un registro de un par de claves y determinar un código de verificación, también un producto de programa informático ejecutado en el terminal puede realizar estos pasos según una realización de la invención. El producto del programa informático se almacena ventajosamente o al menos se realiza al menos parcialmente en una tarjeta SIM y/o UICC del terminal. Según una realización adicional de la invención, la tarjeta SIM y/o la UICC del terminal también puede usarse al menos en parte para generar y/o al menos solicitar un registro de un par de claves y determinar un código de verificación sobre las porciones de información de solicitud de certificado, una posible segunda información y una clave que se registrará.

La presente invención ofrece ventajas notables sobre las soluciones conocidas de la técnica anterior, porque al usar esta invención se pueden generar nuevos pares de claves PKI y registrarlos en cualquier momento necesario, o solicitar un registro de clave pregenerada, sin un gran temor respecto a los ataques de personas anónimas. Además, la invención hace posible reducir la carga en los sistemas de comunicación usados, porque solo se necesitan un código de verificación y una clave pública para entregarse, no toda la estructura PKCS#10. Además, la invención también es poderosa incluso si las conexiones de comunicación entre un cliente y un servidor de registro no están garantizadas. En otras palabras, la invención permite que el registro se realice usando la estructura autofirmada estándar de registro PKCS sin devolver la estructura PKCS al servidor de registro.

Breve descripción de los dibujos

A continuación, la invención se describirá con mayor detalle con referencia a realizaciones ejemplares según los dibujos adjuntos, en los que

la Figura 1A ilustra un diagrama de flujo de un método ejemplar para formar una solicitud de registro en un terminal según una realización ventajosa de la invención,

la Figura 1B ilustra un diagrama de flujo de un método ejemplar para registrar una clave en un servidor de registro según una realización ventajosa de la invención,

la Figura 2 ilustra un diagrama de bloques de un sistema ejemplar para un proceso de registro de clave en un entorno WPKI que comprende un servidor de registro y un terminal según una realización ventajosa de la invención,

la Figura 3 ilustra un terminal ejemplar para un proceso de registro de clave en un entorno WPKI según una realización ventajosa de la invención,

la Figura 4 ilustra una tarjeta SIM/UICC ejemplar para un proceso de registro de clave en un entorno WPKI según una realización ventajosa de la invención,

la Figura 5 ilustra un diagrama de bloques de un servidor de registro ejemplar para registrar una clave según una realización ventajosa de la invención,

la Figura 6A ilustra un diagrama de bloques de un producto de programa informático ejemplar para formar una solicitud de registro en un terminal según una realización ventajosa de la invención, y

la Figura 6B ilustra un diagrama de bloques de un producto de programa informático ejemplar para registrar una clave en un servidor de registro según una realización ventajosa de la invención.

Descripción detallada

La Figura 1A ilustra un diagrama de flujo de un método ejemplar 100a para formar una solicitud de registro en un terminal (como cliente) según una realización ventajosa de la invención, donde en el paso 102 (solo) parte de la información de solicitud de certificado definida en el estándar de registro PKCS se recibe ventajosamente a través de una primera conexión de comunicación de datos, y en el paso 104 la segunda información se recibe o se recopila alternativamente a partir del entorno del terminal. El paso 104 es, sin embargo, opcional. En el paso 106, se descifran partes cifradas de información, en caso de haber cualquier información cifrada recibida en el paso 102 y/o 104. En el paso 108 se puede generar un par de claves PKI que incluye claves privadas y públicas, si aún no se han pregenerado de antemano, ya sea por el terminal o alternativamente alguna otra parte. Ahora debe tenerse en cuenta que el orden de los pasos 102-108 descritos aquí constituye solo un ejemplo y este orden también puede ser diferente; tal como proporcionar primero la segunda información, luego generar el par de claves y después recibir esta información de solicitud de certificado, por ejemplo, con lo que el paso 108 también podría ser opcional.

Sin embargo, después de los pasos 102-108, dicha parte de la información de solicitud de certificado y la posible segunda información con la clave pública (PKI) a registrarse es colocada en la estructura PKCS en el paso 110 con objeto de formar una estructura PKCS según un estándar de registro PKCS. Cabe señalar que solo la información relevante que se necesita es colocada en la estructura PKCS en el paso 110.

En el paso 112, se determina un código de verificación, tal como un código *hash*, sobre la (al menos parte de la) estructura PKCS formada, que incluye la clave que se registrará, después, en el paso 114, el código de verificación puede ser firmado por la clave generada o pregenerada, cuya clave pública a registrar se entrega al servidor de registro. Sin embargo, el paso 114 es opcional. Cuando se determina el código de verificación, se entrega ventajosamente con la clave pública a ser registrada en un servidor de registro de una autoridad de certificación en el paso 116.

La Figura 1B ilustra el diagrama de flujo de un método ejemplar 100b para registrar una clave en un servidor de registro según una realización ventajosa de la invención, donde en el paso 101a (solo) parte de la información de solicitud de certificado definida en el estándar de registro PKCS y la segunda información del paso 101b se envía a un terminal. Sin embargo, estos pasos son opcionales, porque según una realización de la invención, alguna otra parte también puede proporcionar al terminal dicha primera y/o segunda información, y según una realización de la invención, dicha

segunda información también puede ser información recopilada por el terminal a partir de su entorno. Además, el orden de los pasos 101a, 101b puede ser diferente a como se describe aquí.

Después del paso 116 representado en la Figura 1A, el código de verificación y la clave a registrar se reciben en el paso 118, tras lo cual se descifra el posible cifrado del código de verificación y/o la clave a registrar, o se verifica la posible firma en el paso 120. También el paso 120 es opcional.

Cuando el servidor de registro ha recibido dicho código de verificación, el servidor de registro forma en el paso 121 una estructura PKCS que coloca la misma información de solicitud de certificado y la posible segunda información tal como lo hizo el terminal con la clave pública recibida del terminal en la estructura PKCS para formar una estructura PKCS según un estándar de registro PKCS, después de lo cual se determina en el paso 122 un código de verificación sobre (al menos parte de) la estructura PKCS formada que incluye la clave a registrar (como lo hizo el terminal). Cabe señalar que el servidor de registro debe conocer el método de cómo preparar una estructura PKCS, qué información se debe utilizar y cómo determinar el código de verificación, de forma que sea un método similar al usado por el terminal.

En el paso 124 se comparan los códigos de verificación (el primero enviado por el terminal y el segundo determinado por el servidor de registro). Si son idénticos, el servidor de registro puede estar seguro de que la clave pública que se va a registrar proviene del terminal al que se enviaron dicha primera y segunda información, después de lo cual la clave pública se registra en el paso 126 y el proceso finaliza 130. Si los códigos de verificación no son idénticos, se envía ventajosamente un código de error al terminal en el paso 128 (sin embargo, esto es opcional) y el proceso finaliza 130.

La Figura 2 ilustra un diagrama de bloques de un sistema ejemplar 200 según una realización ventajosa de la invención para un proceso de registro de clave en un entorno WPKI que comprende un servidor de registro 202 que está en comunicación de datos a través de una primera conexión de comunicación de datos 201 con un terminal 204.

Parte de la información de solicitud de certificado definida en el estándar de registro PKCS y utilizable para formar una solicitud de registro se envía desde el servidor de registro 202 a través de dicha primera conexión de comunicación de datos 201 al terminal 204. La segunda información (o al menos parte de ella) utilizada para la formación de la solicitud de registro y conocida también por el servidor de registro 202 también puede proporcionarse al terminal 204 según una realización de la invención a través de una segunda conexión 203 separada de la primera conexión de comunicación de datos 201, pero esto es opcional. Sin embargo, una ruta de transmisión utilizada para los segundos datos puede ser la misma que la utilizada para los primeros datos, aunque los primeros y segundos datos no se envían durante la misma conexión.

Un código de verificación (determinado en el terminal de dicha parte de la información de solicitud de certificado y una posible segunda información con una clave pública a registrar) y la clave pública se entregan al servidor de registro 202 a través de una tercera conexión de comunicación 205, que es según una realización de la invención una conexión diferente a la conexión 201 utilizada para entregar dicha primera información. Sin embargo, una ruta de transmisión utilizada para entregar el código de verificación y la clave puede ser la misma que la utilizada para los primeros datos.

La Figura 3 ilustra un terminal ejemplar 204 para un proceso de registro de clave en un entorno WPKI según una realización ventajosa de la invención, donde el terminal comprende medios 204a para recibir (solo) parte de la información de solicitud de certificado definida en el estándar de registro PKCS y medios 204b para recibir y/o recopilar una segunda información, donde el medio 204b es, según una realización de la invención, un teclado, por ejemplo, especialmente cuando la segunda información debe escribirse en el terminal. Además, el terminal 204 comprende medios 204c para cifrar, descifrar, firmar y/o verificar la firma de información, así como medios 204d para generar un par de claves PKI que incluye claves privadas y públicas.

Además, el terminal 204 comprende medios 204e para formar una estructura PKCS según un estándar de registro PKCS de dicha parte de la información de solicitud de certificado y una posible segunda información con la clave pública (PKI) que se registrará de cierta manera como se muestra en otra parte de este documento. El terminal también comprende medios 204f para determinar un código de verificación, tal como un código *hash*, sobre la estructura PKCS formada (o sobre al menos parte de ella) incluyendo la clave a registrar, y medios 204g para entregar el código de verificación ventajosamente con la clave pública para registrarse en un servidor de registro de una autoridad de certificación.

La Figura 4 ilustra una tarjeta SIM/UICC ejemplar 300 utilizada en un terminal 204 de la Figura 2 para un proceso de registro de clave en un entorno WPKI según una realización ventajosa de la invención, donde se puede realizar al menos parte de la funcionalidad del terminal 204 con la tarjeta SIM/UICC 300. La tarjeta SIM/UICC 300 comprende, según una realización de la invención, al menos uno de los siguientes medios: medios 304a para recibir (solo) parte de la información de solicitud de certificado definida en el estándar de registro PKCS, medios 304b para recibir y/o recopilar la segunda información, por ejemplo, desde el teclado u otros medios de E/S o desde el entorno de la tarjeta SIM/UICC o el terminal, medios 304c para cifrar, descifrar la firma y/o verificar una firma de información, así como medios 304d para generar un par de claves PKI que incluye claves privadas y públicas, medios 304e para formar una estructura PKCS según un estándar de registro PKCS de dicha parte de la información de solicitud de certificado y la

posible segunda información con la clave pública (PKI) que se registrará de cierta manera como se muestra en otra parte de este documento, medios 304f para determinar un código de verificación sobre la estructura PKCS formada (o sobre al menos parte de ella) incluyendo la clave que se registrará, y medios 304g para generar el código de verificación ventajosamente con la clave pública que se entregará a un servidor de registro de una autoridad de certificación.

La Figura 5 ilustra un diagrama de bloques de un servidor de registro ejemplar 202 para registrar una clave según una realización ventajosa de la invención, donde el servidor de registro 202 comprende medios 202a para enviar y generar parte de la información de solicitud de certificado y medios 202b para enviar y generar una segunda información o al menos parte de ella. Además, el servidor de registro 202 comprende medios 202c para recibir un código de verificación y la clave a registrar, así como medios 202d para descifrar, cifrar, firmar y/o verificar una firma de información.

Además, el servidor de registro 202 comprende medios 202e para formar una estructura PKCS según un estándar de registro PKCS de dicha parte de la información de solicitud de certificado y una posible segunda información con la clave pública recibida (PKI) que se registrará de cierta manera como se muestra en otro lugar en este documento, así como los medios 202f para determinar un código de verificación sobre la estructura PKCS formada (o sobre al menos parte de ella) incluyendo la clave pública recibida (PKI) que se registrará de manera similar a como lo hizo el terminal. También, el servidor de registro 202 comprende medios 202g para comparar los códigos de verificación (el primero enviado por el terminal y el segundo determinado por el propio servidor de registro) de modo que si son idénticos, el servidor de registro está adaptado para registrar la clave pública utilizando los medios 202h, o de otro modo adaptado para enviar un código de error usando los medios 202i.

La Figura 6A ilustra un diagrama de bloques de un producto de programa informático ejemplar 400 para un terminal para formar una solicitud de registro en un terminal según una realización ventajosa de la invención. El producto de programa informático 400 comprende los siguientes medios 400a-400g, donde el medio 404a está adaptado para recibir solo una parte de la información de solicitud de certificado definida en el PKCS y entregarse ventajosamente a través de una primera conexión de comunicación de datos, los medios 404b están adaptados para recibir y/o recopilar segunda información, por ejemplo, del teclado u otro medio de E/S o del entorno de la tarjeta SIM/UICC o terminal, los medios 404c están adaptados para cifrar, descifrar, firmar y/o verificar una firma de información, además de medios 404d que están adaptados para generar un par de claves PKI que incluye claves privadas y públicas, medios 404e adaptados para formar una estructura PKCS según un estándar de registro PKCS de dicha parte de la información de solicitud de certificado y una posible segunda información con la clave pública (PKI) que se registrará de cierta manera como se muestra en otra parte de este documento, medios 404f que están adaptados para determinar un código de verificación sobre la estructura PKCS formada (o sobre al menos parte de ella), incluyendo la clave que se registrará, y medios 404g que están adaptados para generar el código de verificación ventajosamente con la clave pública que se entregará a un servidor de registro de una autoridad de certificación, cuando el producto del programa informático se ejecuta en un medio de procesamiento de datos, tal como un terminal 204 ilustrado en la Figura 4, o una tarjeta SIM/UICC ilustrada en la Figura 4 u otros medios de procesamiento de datos, tal como un ordenador portátil.

La Figura 6B ilustra un diagrama de bloques de un producto de programa informático ejemplar 500 para registrar una clave en un servidor de registro según una realización ventajosa de la invención. El producto de programa informático 500 comprende los siguientes medios 500a-500i, donde los medios 502a están adaptados para enviar y generar (solo) parte de la información de solicitud de certificado, los medios 502b están adaptados para enviar y generar una posible segunda información o al menos parte de ella, los medios 502c están adaptados para recibir un código de verificación y la clave que se registrará, además de los medios 502d que están adaptados para descifrar, cifrar, firmar y/o verificar una firma de información, los medios 502e están adaptados para formar una estructura PKCS según un estándar de registro PKCS de dicha parte de la información de solicitud de certificado y la posible segunda información con la clave pública recibida (PKI) que se registrará de cierta manera como se muestra en otra parte de este documento, así como los medios 502f que están adaptados para determinar un código de verificación sobre la estructura PKCS formada (o sobre al menos parte de ella), incluyendo la clave pública recibida (PKI) que se registrará de manera similar a como lo hizo el terminal, los medios 502g están adaptados para comparar los códigos de verificación (el primero enviado por el terminal y el segundo determinado por el propio servidor del producto del programa informático) de modo que si son idénticos, el producto del programa informático está adaptado para registrar la clave pública utilizando los medios 202h, o de otro modo adaptado para enviar un código de error utilizando los medios 202i, cuando dicho producto de programa informático se ejecuta en un medio de procesamiento de datos, tal como un servidor de registro 202 ilustrado en la Figura 5.

La invención ya ha sido explicada anteriormente con referencia a las realizaciones mencionadas con anterioridad, y han sido demostradas varias ventajas de la invención. Está claro que la invención no solo se limita a estas realizaciones, sino que comprende todas las realizaciones posibles dentro del alcance del pensamiento inventivo y las siguientes reivindicaciones de patente.

Incluso si la entrega de una clave pública es descrita en este documento, debe tenerse en cuenta que solo la información relacionada con la clave pública y que resulta esencial para registrar dicha clave en el servidor de registro puede ser suficiente en ciertas situaciones, por lo que la clave o la estructura de registro no se entregará totalmente. En resumen, se puede decir que solo se envía información relevante que sea necesaria para configurar la estructura

PKCS, donde se establece cierta información previamente, solo entregándose al servidor la información mínima. Además, debe tenerse en cuenta que incluso si en este documento se dice que una clave pública que será registrada, se entrega a un servidor de registro, también podría ser suficiente en una situación determinada entregar solo partes relevantes de dicha clave pública. Más aún, debe observarse que la presente invención es aplicable en particular cuando se usan estándares de registro PKCS#10, pero también puede usarse para otros estándares PKCS (como alguna versión futura del mismo o el caso de nuevos estándares) *mutatis mutandis*.

REIVINDICACIONES

1. Un método (100a, 100b) para un proceso seguro de registro de clave PKI (siglas en inglés para “Infraestructura de clave pública”) en un entorno WPKI (PKI inalámbrica) que utiliza un estándar de registro PKCS (siglas en inglés para “Estándar de criptografía de clave pública”), donde el entorno WPKI (200) comprende un servidor de registro (202) que está en comunicación de datos con un cliente (204) provisto de un par de claves, y cuando se proporciona una solicitud de registro para una clave pública de dicho par de claves a dicho servidor de registro (202) que utiliza el estándar de registro PKCS, en donde

a) solo parte de la información de solicitud de certificado definida en el estándar de registro PKCS se entrega (101a, 101b) al cliente (204) a través de una primera conexión de comunicación de datos (201),

a') los datos del entorno del cliente (204) se recopilan (104) como segunda información,

b) el cliente (204) forma una estructura PKCS (110) usando

b1) al menos una porción de dicha parte de la información de solicitud de certificado recibida en el paso a),

b2) la clave pública que se registrará, y

b3) los datos de entorno recopilados del cliente,

de modo que dicha al menos porción de la parte de la información de solicitud de certificado y los datos de entorno recopilados del cliente con la clave pública que se registrará se coloquen en la estructura PKCS que está de acuerdo con el estándar de registro PKCS,

c) se determina un código de verificación (112) sobre al menos parte de la estructura PKCS formada en el paso b),

d) dicho código de verificación es firmado (114) por el cliente (204), y

e) los datos del entorno del cliente, el código de verificación firmado y la clave pública se entregan (116, 118) a dicho servidor de registro (202) para el registro (126), en donde dichos datos de entorno se transmiten desde el cliente (204) al servidor de registro (202) en una segunda conexión de comunicación de datos (205), si dichos datos de entorno no son conocidos previamente por el servidor de registro (202).

2. Un método según la reivindicación 1, en donde el código de verificación firmado y la clave pública se reciben (118) y se forma una estructura de registro PKCS (121) en el servidor de registro (202) usando:

- dicha porción de dicha parte de la información de solicitud de certificado utilizada por el cliente (204) en el paso b) para formar la estructura de registro PKCS y

- la clave pública a registrar, por lo que

- se determina un código de verificación (122) sobre al menos parte de dicha estructura de registro PKCS formada en el servidor de registro (202), y

- la clave pública se registra (126) en el servidor de registro (202), si el código de verificación formado en el servidor de registro es idéntico (124) al código de verificación recibido del cliente (204).

3. Un método según la reivindicación 2, en donde dicha segunda información también es conocida por dicho servidor de registro (202) y dicha segunda información también se usa para formar dicha estructura de registro PKCS en el servidor de registro.

4. Un método según cualquiera de las reivindicaciones anteriores, en donde el par de claves es generado (108) por el cliente (204) o el par de claves es pregenerado fuera del cliente (204).

5. Un método según cualquiera de las reivindicaciones anteriores, en donde dicho código de verificación y/o clave pública que se registrará está firmado (114) por la clave privada del par de claves cuya clave pública está en dicha estructura de registro PKCS.

6. Un método según cualquiera de las reivindicaciones anteriores, en donde se activa una determinada ventana de tiempo durante la cual el código de verificación y la clave pública a registrar deben recibirse en el servidor de registro (202) para registrarse.

7. Un método según la reivindicación 6, en donde una determinada ventana de tiempo es activada por la entrega (101a) de la parte de la información de solicitud de certificado.

8. Un sistema (200) para un proceso seguro de registro de clave PKI (Infraestructura de clave pública) en un entorno WPKI (PKI inalámbrica) que utiliza un estándar de registro PKCS (Estándar de criptografía de clave pública), donde el sistema (200) comprende un servidor de registro (202) que está en comunicación de datos con un cliente

(204) provisto de un par de claves, y cuando se proporciona una solicitud de registro para una clave pública de dicho par de claves a dicho servidor de registro (202) que utiliza el estándar de registro PKCS, en donde el sistema está adaptado para:

a) enviar (101a) solo parte de la información de solicitud de certificado definida en el estándar de registro PKCS al cliente (204) a través de una primera conexión de comunicación de datos (201),

a') recopilar (104), como segunda información, datos del entorno del cliente (204),

b) formar (110) una estructura de registro PKCS por el cliente (204) usando:

b1) al menos una porción de dicha parte de la información de solicitud de certificado del paso a),

b2) la clave pública que se registrará, y

b3) los datos de entorno recopilados del cliente,

de modo que dicha al menos porción de la parte de la información de solicitud de certificado y los datos de entorno recopilados del cliente con la clave pública que se registrará se coloquen en la estructura PKCS que está de acuerdo con el estándar de registro PKCS,

c) determinar (112) un código de verificación sobre al menos parte de la estructura de registro PKCS formada en el paso b),

d) firmar (114) dicho código de verificación con la clave del cliente (204), y

e) entregar (116, 118) los datos del entorno del cliente, el código de verificación firmado y la clave pública a dicho servidor de registro (202) para el registro (126), en donde dichos datos de entorno se transmiten desde el cliente (204) al servidor de registro (202) en una segunda conexión de comunicación de datos (205), si dichos datos de entorno no son conocidos previamente por el servidor de registro (202).

9. Un sistema según la reivindicación 8, en donde el sistema está adaptado además para formar (121) una estructura de registro PKCS en el servidor de registro (202) usando:

- dicha porción de dicha parte de la información de solicitud de certificado utilizada por el cliente en el paso b) para formar la estructura de registro PKCS y

- la clave pública a registrar, por lo que

- el sistema está adaptado para determinar (122) un código de verificación sobre al menos parte de dicha estructura de registro PKCS formada en el servidor de registro (202), y

- el sistema está adaptado para registrar (126) la clave pública en el servidor de registro (202), si el código de verificación formado en el servidor de registro es idéntico (124) al código de verificación determinado por el cliente.

10. Un servidor de registro (202) para un proceso seguro de registro de clave PKI (Infraestructura de clave pública) en un entorno WPKI (PKI inalámbrica) que utiliza un estándar de registro PKCS (Estándar de criptografía de clave pública), donde el entorno WPKI (200) comprende un servidor de registro (202) que está en comunicación de datos con un cliente (204) provisto de un par de claves, y cuando se proporciona una solicitud de registro para una clave pública de dicho par de claves a dicho servidor de registro (202) que utiliza el estándar de registro PKCS, en donde

a) el servidor de registro (202) es provisto de una parte de la información de solicitud de certificado definida en el PKCS y que se entrega (101b) también al cliente (204) a través de una primera conexión de comunicación de datos (201),

b) el servidor de registro (202) está adaptado para recibir (118) datos del entorno del cliente, un código de verificación firmado y formado por el cliente y una clave pública para registrar, en donde dichos datos de entorno se transmiten desde el cliente (204) al servidor de registro (202) en una segunda conexión de comunicación de datos (205), si dichos datos de entorno no son conocidos previamente por el servidor de registro (202),

c) el servidor de registro (202) está adaptado para formar (121) una estructura de registro PKCS usando:

c1) la misma porción de dicha parte de la información de solicitud de certificado utilizada también por el cliente (204),

c2) la clave pública recibida para ser registrada y

c3) los datos del entorno del cliente,

de modo que dicha misma porción de la parte de la información de solicitud de certificado y los datos de entorno del cliente con la clave pública que se registrará se coloquen en la estructura PKCS que está de acuerdo con el estándar de registro PKCS,

d) el servidor de registro (202) está adaptado para determinar (122) un código de verificación por sí mismo sobre al menos parte de la estructura de registro PKCS formada en el paso c), y

e) el servidor de registro (202) está adaptado para registrar (126) la clave pública, si el código de verificación formado en el servidor de registro (202) es idéntico (124) al código de verificación recibido del cliente (204).

11. Un cliente (204) para un proceso seguro de registro de clave PKI (Infraestructura de clave pública) en un entorno WPKI (PKI inalámbrica) (200) que utiliza un estándar de registro PKCS (Estándar de criptografía de clave pública), donde el entorno WPKI comprende un servidor de registro (202) que está en comunicación de datos con dicho cliente (204) provisto de un par de claves, y donde se proporciona una solicitud de registro para una clave pública de dicho par de claves a dicho servidor de registro (202) que utiliza el estándar de registro PKCS, en donde el cliente (204) está adaptado para:

a) recibir (101a) solo parte de la información de solicitud de certificado definida en el PKCS a través de una primera conexión de comunicación de datos (201),

a') recopilar (104), como segunda información, datos de entorno del cliente (204),

b) formar (110) una estructura PKCS usando:

b1) al menos una porción de dicha parte de la información de solicitud de certificado recibida en el paso a),

b2) la clave pública que se registrará, y

b3) los datos de entorno recopilados del cliente,

de modo que dicha al menos porción de la parte de la información de solicitud de certificado y los datos de entorno recopilados del cliente con la clave pública que se registrará se coloquen en la estructura PKCS que está de acuerdo con el estándar de registro PKCS,

c) determinar (112) un código de verificación sobre al menos parte de la estructura de registro PKCS formada en el paso b),

d) firmar (114) dicho código de verificación, y

e) enviar (116) los datos de entorno del cliente, el código de verificación firmado y la clave pública a dicho servidor de registro (202), en donde dichos datos de entorno se transmiten desde el cliente (204) al servidor de registro (202) en una segunda conexión de comunicación de datos (205), si dichos datos de entorno no son conocidos previamente por el servidor de registro (202).

12. Un producto de programa informático (400) para un proceso seguro de registro de clave PKI (Infraestructura de clave pública) en un entorno WPKI (PKI inalámbrico) que usa un estándar de registro PKCS (Estándar de criptografía de clave pública), donde dicho producto de programa informático (400) está adaptado para hacer que un cliente (204) realice al menos una operación para la cual el cliente (204) según la reivindicación 11 está adaptado a realizar.

13. Un producto de programa informático (500) para un proceso seguro de registro de clave PKI (Infraestructura de clave pública) en un entorno WPKI (PKI inalámbrica) que usa un estándar de registro PKCS (Estándar de criptografía de clave pública), donde dicho producto de programa informático (500) está adaptado para hacer que un servidor de registro (202) realice al menos una operación para la cual el servidor de registro (202) según la reivindicación 10 está adaptado a realizar.

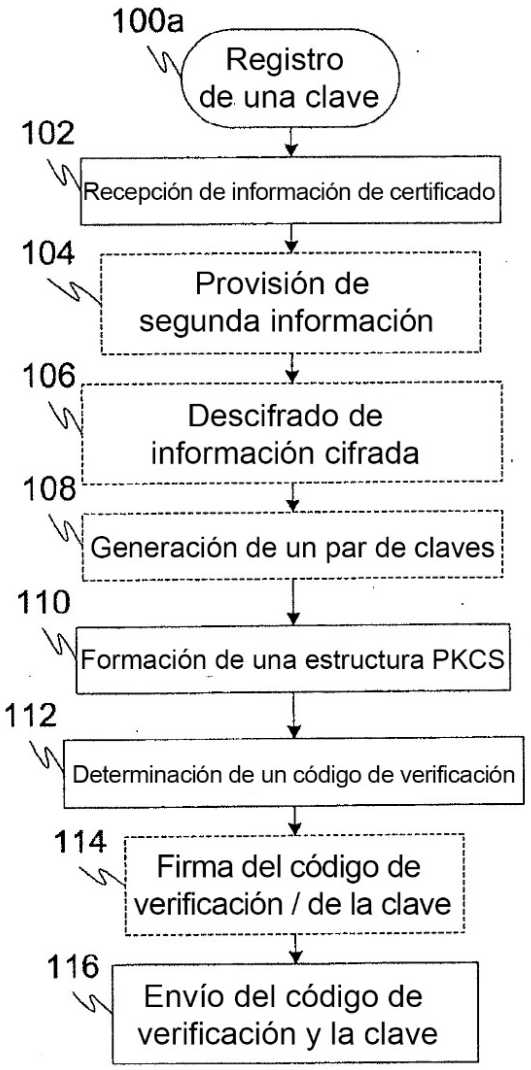

FIG. 1A

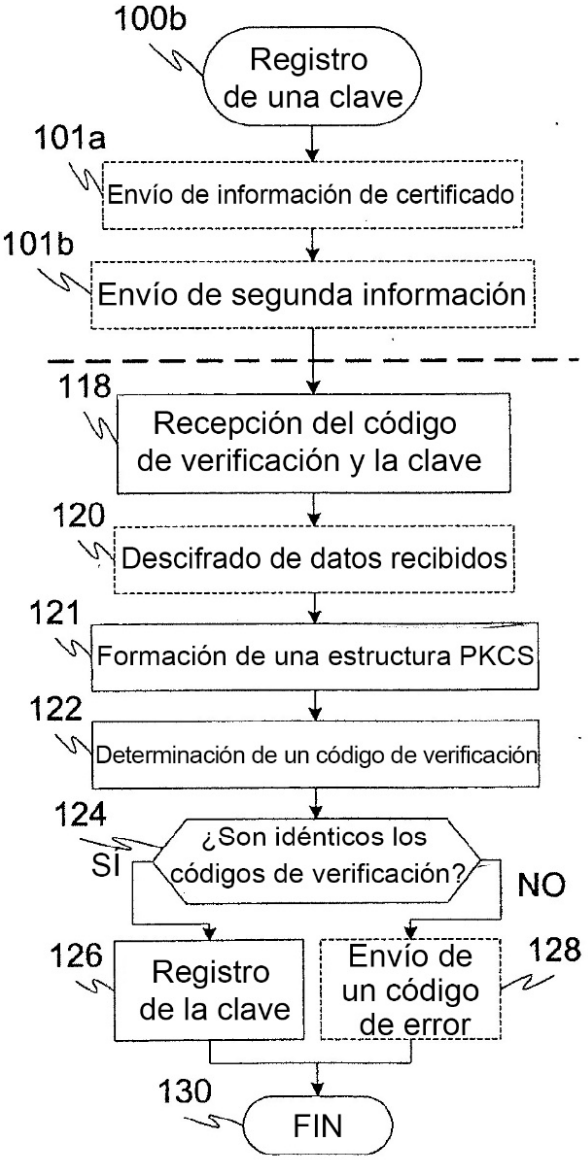

FIG. 1B

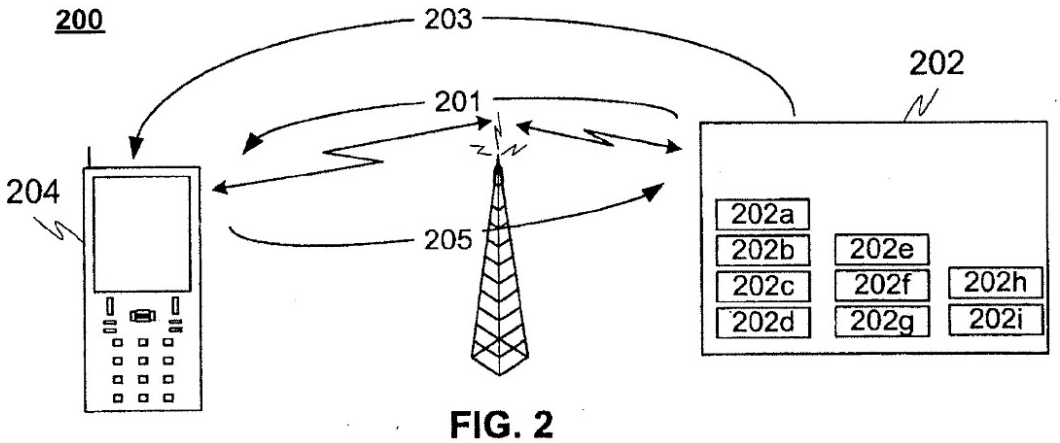

FIG. 2

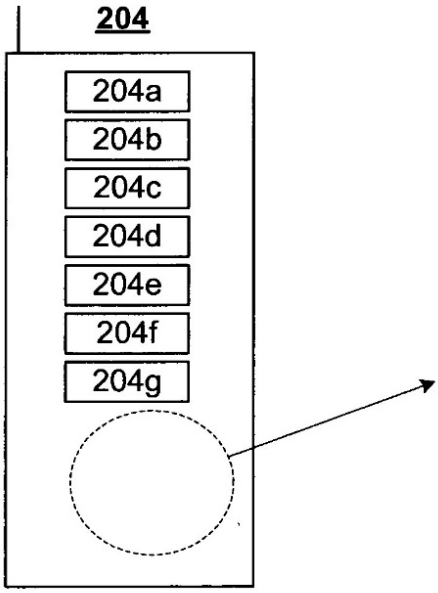

FIG. 3

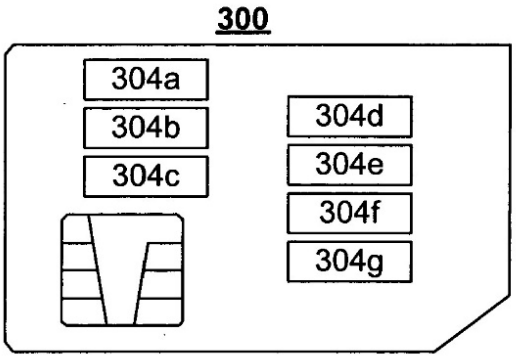

FIG. 4

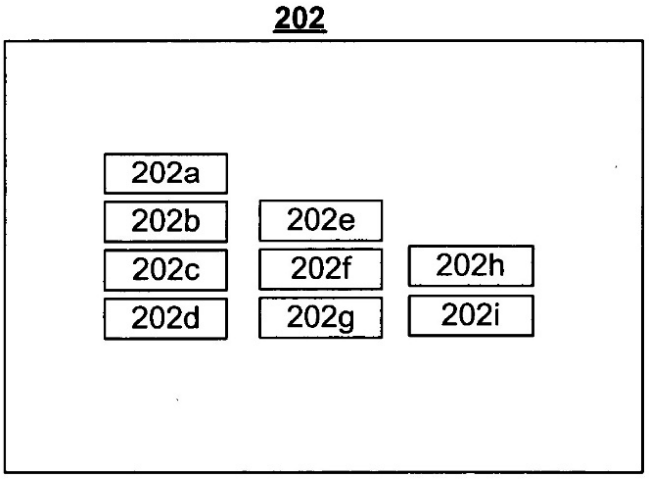

FIG. 5 (Servidor)

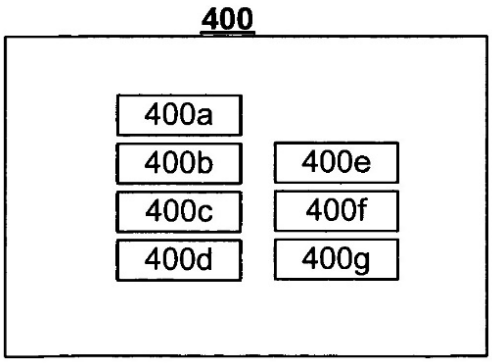

FIG. 6A (para un terminal)

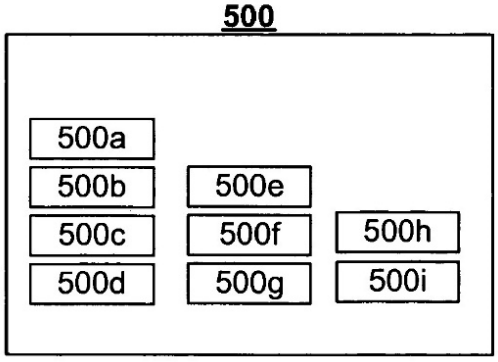

FIG. 6B (para un servidor)