(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 542 142**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 12/22 (2006.01)
G06F 21/00 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **29.08.2007 E 07016894 (3)**

(97) Fecha y número de publicación de la concesión europea: **22.04.2015 EP 1903744**

(54) Título: **Procedimiento y dispositivos para la transmisión de contenidos autenticables de un servidor de proveedor a un terminal móvil**

(30) Prioridad:

20.09.2006 DE 102006044750

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
31.07.2015

(73) Titular/es:

VODAFONE HOLDING GMBH (100.0%)
MANNESMANNUFER 2
40213 DÜSSELDORF, DE

(72) Inventor/es:

PALAU, JOFRE

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento y dispositivos para la transmisión de contenidos autenticables de un servidor de proveedor a un terminal móvil

Campo técnico

La invención se refiere a un procedimiento para la transmisión de contenidos de un servidor de proveedor a un terminal móvil. La invención se refiere además a un terminal móvil, así como a un servidor de proveedor, que están realizados para la ejecución del procedimiento.

Antecedentes y estado de la técnica

Es conocido ampliar la funcionalidad de terminales móviles, como en particular teléfonos móviles, de tal modo que se cargan contenidos proporcionados por un servidor de proveedor, en particular aplicaciones, en el terminal móvil. Esto se realiza mediante una plataforma, que se describe para redes de telefonía móvil de la tercera generación, por ejemplo en la especificación TS 23.057 (versión 6.2.0, septiembre de 2003) del 3rd Generation Partnership Project (3GPP).

El proceso de carga se realiza en particular con ayuda de una comunicación entre el terminal móvil y el servidor de proveedor, que está basada por ejemplo en el Hypertext Transfer Protocolo (HTTP). En el marco de esta comunicación, el teléfono móvil envía por regla general una petición (HTTP-Request) de la aplicación deseada al servidor de proveedor, que indica habitualmente también informaciones acerca de una configuración del teléfono móvil, así como de los formatos de contenidos admitidos por éste. Estas informaciones forman habitualmente parte de los datos de la cabecera de la petición (Request-Header). Debido a la petición, el servidor de proveedor selecciona a continuación de acuerdo con las informaciones contenidas en los datos de la cabecera los contenidos que han de transmitirse al teléfono móvil.

En vista de una autenticación en un servidor, el documento WO 2005/006703 A2 da a conocer un sistema y un procedimiento para la autenticación de clientes. En el procedimiento, un cliente envía informaciones de autenticación al servidor, que comprenden un certificado de cliente digital, así como una firma digital. El servidor comprueba la firma digital mediante una clave pública contenida en el certificado de cliente. Después de haberse realizado la comprobación con éxito, el cliente obtiene acceso a los datos del servidor.

Las aplicaciones usan habitualmente interfaces del software existente del terminal móvil, para acceder a funciones existentes del terminal móvil o a datos almacenados en el terminal móvil. Para impedir accesos no autorizados a datos y funciones sensibles, como por ejemplo la posibilidad de establecer una conexión por internet o para la realización de transacciones de pago, solo se conceden derechos de acceso a estas interfaces a aquellas aplicaciones que son clasificadas como fiables o que han sido transmitidas por un servidor de proveedor clasificado como fiable. Los contenidos transmitidos por un servidor de proveedor al terminal móvil son autenticados, por lo tanto, con ayuda de un procedimiento criptográfico.

Para ellos, los contenidos son provistos por el servidor de proveedor de una firma digital, que se genera mediante una clave de cifrado privada del servidor de proveedor. La firma está formada por una suma de comprobación de los contenidos cifrada con la clave de cifrado privada. En el seno del terminal móvil se compara la firma con ayuda de un certificado digital asignado a la clave de cifrado. Para ello, la suma de comprobación contenida en los contenidos recibidos se descifra mediante una clave de comprobación contenida en el certificado digital y se compara con una suma de comprobación que se ha generado en el seno del terminal móvil. Típicamente, la clave de cifrado y la clave de comprobación son una pareja asimétrica de claves, en la que la clave de comprobación corresponde a la clave pública del servidor de proveedor. El certificado digital puede ser o bien un certificado raíz emitido por un organismo de certificación o un certificado intermedio autenticable mediante el certificado raíz o un certificado de proveedor emitido por el proveedor de los contenidos, que es autenticable mediante un certificado raíz o un certificado intermedio. Habitualmente, un terminal móvil dispone de varios certificados raíz y certificados intermedios para poder cargar contenidos de distintos servidores de proveedor, siendo almacenados los certificados raíz por el fabricante antes de la entrega en el terminal móvil o siendo depositados por un proveedor de telefonía móvil en una tarjeta SIM o USIM del terminal móvil, antes de ser entregada la misma al usuario.

En particular en vista del número de aplicaciones en continuo crecimiento para terminales móviles y de los proveedores de las mismas, en la plataforma conocida existe el problema que en la zona del servidor de proveedor no están disponibles ningunas informaciones acerca de los certificados raíz y certificados intermedios disponibles en el seno del terminal móvil. Debido a ello, el comportamiento del servidor de proveedor no puede adaptarse a los certificados disponibles y se transmiten en muchas ocasiones contenidos de un servidor de proveedor a un terminal móvil que están provistos de una firma que no puede ser comprobada y, por lo tanto, no usada debido a que falta un certificado correspondiente. En este caso, el usuario debe obtener los certificados que faltan de una forma costosa y complicada.

Sumario de la invención

Por lo tanto, la presente invención tiene el objetivo de poder adaptar el comportamiento de un servidor de proveedor durante la transmisión de contenidos a un terminal móvil a los certificados digitales almacenados en el seno del terminal móvil.

De acuerdo con la invención, este objetivo se consigue mediante un procedimiento con las características de la reivindicación 1, mediante un terminal móvil de acuerdo con la reivindicación 14, así como mediante un servidor de proveedor de acuerdo con la reivindicación 15. De acuerdo con la invención, el objetivo se consigue también mediante un producto de programa informático de acuerdo con la reivindicación 13.

Por consiguiente, se pone a disposición un procedimiento del tipo indicado al principio, en el que los contenidos comprenden un componente de autenticación, que se cifra en el seno del servidor de proveedor mediante una clave de cifrado privada y que puede ser comprobado mediante un certificado digital para autenticar los contenidos transmitidos. El procedimiento está caracterizado porque en el servidor de proveedor se recibe una información enviada en una primera etapa de comunicación desde el terminal móvil mediante varios certificados digitales almacenados en el seno del terminal móvil. La información es evaluada en el seno del servidor de proveedor, de modo que el servidor de proveedor obtiene conocimiento de varios certificados digitales disponibles en el terminal móvil y los contenidos se transmiten en una segunda etapa de comunicación en función de un resultado de la evaluación de las informaciones recibidas al terminal móvil.

Además, se pone a disposición un terminal móvil para la recepción de contenidos de un servidor de proveedor. Los contenidos comprenden un componente de autenticación que es cifrado mediante una clave de cifrado privada del servidor de proveedor. En el seno del terminal móvil, el componente de autenticación puede ser autenticado mediante un certificado digital asignado a la clave de cifrado. El terminal móvil está caracterizado porque está realizado para transmitir en una etapa de comunicación una información acerca de varios certificados digitales almacenados en el seno del terminal al servidor de proveedor, de modo que el servidor de proveedor obtiene conocimiento de varios certificados digitales disponibles en el terminal móvil.

Además, se crea un servidor de proveedor para la transmisión de contenidos a un terminal móvil. Los contenidos comprenden un componente de autenticación, que puede ser cifrado en el seno del servidor de proveedor mediante una clave de cifrado privada y que puede ser comprobado mediante un certificado digital. El servidor de proveedor está realizado para recibir y evaluar una información enviada en una etapa de comunicación por el terminal móvil mediante varias claves de comprobación certificadas, almacenadas en el seno del terminal móvil, de modo que el servidor de proveedor obtiene conocimiento de varios certificados digitales disponibles en el terminal móvil.

En el marco de la invención, el concepto certificado digital comprende en particular certificados raíz digitales, certificados intermedios digitales y certificados de proveedor digitales. Los certificados raíz están almacenados en el seno del terminal móvil en una zona de memoria que está asegurada contra el acceso del usuario del terminal móvil. Los certificados intermedios y certificados de proveedor contienen un componente de autenticación que puede ser comprobado mediante el certificado raíz o uno o varios otros certificados intermedios. Al menos uno de estos otros certificados intermedios puede ser autenticado mediante un certificado raíz. Los certificados digitales están asignados respectivamente a una clave de cifrado y se usan para la comprobación de datos cifrados con la clave de cifrado. En particular, los certificados digitales comprenden respectivamente una clave de comprobación asignada a la clave de cifrado para el descifrado de los datos.

El concepto componente de autenticación también ha de entenderse en su significado más amplio y comprende datos en cualquier forma, que pueden ser autenticados mediante un certificado digital. En particular, el componente de autenticación puede ser una firma digital, que puede ser comprobada mediante un certificado digital.

La invención tiene en particular la ventaja de que el servidor de proveedor obtiene conocimiento de los certificados digitales disponibles en el terminal móvil gracias a la información que puede ser transmitida por el terminal móvil acerca de los certificados digitales almacenados en el terminal móvil. Según este conocimiento puede adaptarse el comportamiento del servidor de proveedor.

En una forma de realización del procedimiento, del terminal móvil y del servidor de proveedor está previsto que en el servidor de proveedor se reciba un mensaje enviado por el terminal móvil en la primera etapa de comunicación, que contiene la información acerca de los certificados digitales almacenados en el seno del terminal móvil en un formato estándar.

Por formato estándar se entiende en particular un formato que puede ser interpretado por un servidor de proveedor, sin que el terminal móvil deba transmitir reglas de interpretación al servidor de proveedor. Las reglas de interpretación son fijadas preferiblemente anteriormente y son depositadas en el terminal móvil así como en el servidor de proveedor. Pueden formar parte de un protocolo admitido por una pluralidad de servidores de proveedor y terminales móviles.

Típicamente, la comunicación entre el terminal móvil y el servidor de proveedor está basada en el Hyptertext Transfer Protocol (HTTP). En el marco de este protocolo se intercambian mensajes entre el terminal móvil y el

servidor de proveedor, que comprenden una zona de datos útiles y una zona de datos de la cabecera. La zona de datos de la cabecera contiene en particular indicaciones estándar acerca de la configuración del terminal móvil. En el servidor de proveedor pueden adaptarse con ayuda de estas indicaciones el tipo y la forma de los contenidos a transmitir al terminal móvil.

Una configuración del procedimiento, del terminal móvil y del servidor de proveedor prevé, por lo tanto, que la primera etapa de comunicación esté basada en el Hypertext Transfer Protocol, recibiéndose en la primera etapa de comunicación una petición HTTP enviada por el terminal móvil en el servidor de proveedor y formando la información acerca de las claves de comprobación certificadas almacenadas en el seno del terminal móvil parte de una zona de datos de la cabecera de la petición HTTP.

Es ventajoso que la información acerca de las claves de comprobación contenidas en el terminal móvil se incorpore en esta configuración en la zona de datos de la cabecera de la petición HTTP, con la que el terminal móvil solicita contenidos al servidor de proveedor. Esto ha resultado ser preferible, en particular, porque la zona de datos de la cabecera contiene otras informaciones acerca de la configuración y los contenidos preferidos del terminal móvil, que se evalúan en el servidor de proveedor y que se usan para la adaptación de los contenidos a transmitir. Por petición HTTP se entiende aquí el mensaje con el que se solicitan contenidos al servidor de proveedor.

Otra configuración del procedimiento, del terminal móvil y del servidor de proveedor comprende que, gracias a la evaluación de la información acerca de los certificados digitales almacenados en el seno del terminal móvil, se determina en el seno del servidor de proveedor para cuáles de las claves de cifrado disponibles en el servidor de proveedor está almacenado un certificado asignado en el terminal móvil.

Una forma de realización del procedimiento, del terminal móvil y del servidor de proveedor está caracterizada porque en el servidor de proveedor se selecciona una clave de cifrado, para la que está almacenado en el terminal móvil un certificado digital asignado y porque el componente de autenticación de los contenidos se cifra con la clave de cifrado seleccionada.

De este modo queda garantizado de forma ventajosa que los contenidos transmitidos al terminal móvil o el componente de autenticación de los mismos puedan ser comprobados en el terminal móvil mediante un certificado digital. Además, se evita una transmisión innecesaria de certificados digitales ya existentes en el terminal móvil.

Una variante del procedimiento, del terminal móvil y del servidor de proveedor comprende que el componente de autenticación de los contenidos se cifra en el servidor de proveedor mediante una clave de cifrado, que tiene asignado un certificado de proveedor digital, siendo transmitido el certificado de proveedor digital por el servidor de proveedor al terminal móvil.

De forma ventajosa, los contenidos son comprobados en esta variante por un certificado asignado al servidor de proveedor o al proveedor que opera el servidor.

Una forma de realización del procedimiento, del terminal móvil y del servidor de proveedor prevé que el certificado de proveedor digital pueda ser autenticado mediante un certificado digital almacenado en el terminal móvil.

De forma ventajosa, el certificado de proveedor es comprobado en esta forma de realización a su vez por un certificado almacenado en el terminal móvil.

No obstante, posiblemente puede darse el caso de que un certificado digital directamente necesario para la comprobación del certificado de proveedor no esté contenido en el terminal móvil.

En una variante del procedimiento, del terminal móvil y del servidor de proveedor, por lo tanto, está previsto que el servidor de proveedor transmita un certificado intermedio digital al terminal móvil, pudiendo usarse el certificado intermedio digital para la comprobación del certificado de proveedor y pudiendo comprobarse el certificado intermedio digital mediante un certificado digital almacenado en el terminal móvil.

De este modo pueden ponerse a disposición los certificados intermedios que faltan en el terminal móvil, que se necesitan en una cadena de certificados usada por el certificado de proveedor. Por una cadena de certificados se entiende una cantidad de certificados digitales, que comprende al menos un certificado raíz, así como un certificado de proveedor, que es autenticable mediante el certificado raíz. Por lo general, una cadena de certificados contiene además al menos un certificado intermedio, que se usa para la autenticación del certificado de proveedor y que puede ser autenticado a su vez mediante el certificado raíz.

Una configuración del procedimiento, del terminal móvil y del servidor de proveedor prevé que al menos un certificado digital almacenado en el terminal móvil sea un certificado raíz digital.

Además, una configuración del procedimiento, del terminal móvil y del servidor de proveedor está caracterizada porque el certificado raíz digital está almacenado en un módulo de identificación de abonado, que está contenido en el terminal móvil.

El módulo de identificación de abonado es entregado habitualmente por el operador de una red de telecomunicaciones, en la que se usa el terminal móvil. El operador de la red de telecomunicaciones actúa en muchos casos también como proveedor de contenidos, como en particular de aplicaciones de software para la ampliación de la funcionalidad del terminal móvil. En la configuración anteriormente descrita de la invención, el operador tiene de forma ventajosa la posibilidad de incorporar en el módulo de identificación de abonado los certificados raíz necesarios para la comprobación de los contenidos proporcionados por él y garantizar de este modo que éstos estén disponibles en el terminal móvil.

Una forma de realización del procedimiento, del terminal móvil y del servidor de proveedor prevé, además, que el terminal móvil contenga al menos otro certificado digital, que es un certificado intermedio que puede ser autenticado mediante el certificado raíz.

Una forma de realización del procedimiento, del terminal móvil y del servidor de proveedor comprende, además, que los contenidos contienen un código de programa que es ejecutable en el seno del terminal móvil, después de haberse autenticado los contenidos transmitidos en el seno del terminal móvil.

Además, se pone a disposición un producto de programa informático, que contiene un programa informático para la ejecución de un procedimiento del tipo anteriormente descrito.

Además, se pone a disposición un sistema de comunicación, en el que puede conectarse al menos un terminal móvil con al menos un servidor de proveedor. El sistema de comunicación está caracterizado porque contiene al menos un terminal móvil del tipo anteriormente descrito así como al menos un servidor de proveedor del tipo anteriormente indicado.

En una forma de realización, el terminal móvil está realizado para recibir contenidos que son transmitidos por el servidor de proveedor al terminal móvil en función de un resultado de la evaluación de la información.

Además, el servidor de proveedor está realizado preferiblemente para transmitir en una etapa de comunicación contenidos al terminal móvil en función de un resultado de la evaluación de las informaciones recibidas mediante certificados digitales almacenados en el terminal móvil.

Las ventajas, particularidades y configuraciones recomendables indicadas de la invención se ilustrarán también con ayuda de los ejemplos de realización y se explicarán a continuación con ayuda de las figuras respecto a los ejemplos de realización.

Breve descripción de los dibujos

De las Figuras muestran:

La Figura 1 una representación esquemática de un terminal móvil que está conectado mediante una red con un servidor de proveedor.

La Figura 2 una representación esquemática de distintas cadenas de certificados con un certificado raíz.

Descripción de ejemplos de realización

La Figura 1 muestra en una representación esquemática un terminal móvil 101, que puede ser por ejemplo un teléfono móvil. El terminal móvil 101 está conectado mediante una red 102, 103, 104 con un servidor de proveedor 105. La red 102, 103, 104 comprende una red de telecomunicaciones 102, con la que el terminal móvil está conectado mediante una interfaz de aire 106 y que está realizada por ejemplo como red GSM (GSM: Global System for Mobile Communications) o como red UMTS (UMTS: Universal Mobile Telecommunication System). La red de telecomunicaciones 102 está conectada mediante una pasarela 103 con una red de datos 104, que es por ejemplo internet o una intranet. Con la red de datos está conectado el servidor de proveedor 105. En una forma de realización alternativa, el terminal móvil 101 también puede estar conectado mediante otra interfaz con un ordenador de interfaces, que está conectado a su vez con la red de datos o una pasarela. Esta posibilidad de conexión alternativa se indica en la Figura 1 mediante una flecha 107. La interfaz puede estar realizada por ejemplo como interfaz infrarroja o bluetooth o puede estar realizada como conexión por cable. Por lo general, pueden conectarse una pluralidad de terminales móviles 101 así como varios servidores de proveedor 105 con la red de datos 104.

Las informaciones para el registro en la red de telecomunicaciones 102 están almacenadas en un módulo de identificación de abonado 109, que por lo general proporciona el operador de la red de telecomunicaciones 102. El módulo de identificación de abonado 109 es una tarjeta chip, que en combinación con redes GSM se denomina tarjeta SIM (SIM: Subscriber Identification Module) y en combinación con redes UMTS se denomina tarjeta USIM (USIM: Universal Subscriber Identification Module) y que se ha insertado en el terminal móvil 101. El terminal móvil 101 comprende, además, un dispositivo procesador 110, que está conectado con el módulo de identificación de abonado 109, un teclado 111, un dispositivo visualizador 112 y una memoria 113, que por lo general presenta una zona de memoria volátil así como una no volátil. La memoria 113 contiene un sistema operativo que controla las funciones del terminal móvil 101 y que comprende en particular un entorno de ejecución de programas, que permite ejecutar otro software que está almacenado en la memoria 113 o en el módulo de identificación de abonado 109. El

entorno de ejecución de programas puede ser por ejemplo la “Plataforma Java 2, Micro Edition” (J2ME) de la sociedad Sun Microsystems. El software ejecutado mediante el entorno de ejecución de programas puede acceder mediante interfaces software, que se denominan habitualmente APIs (Application Programming Interfaces), a funciones del terminal móvil 101 y del módulo de identificación de abonado 109, así como a datos que están almacenados en la memoria 113 o en el módulo de identificación de abonado 109. Además, el terminal móvil 101 presenta una antena de radio 115, que permite establecer una conexión con la red de telecomunicaciones 102 a través de la interfaz de aire 106.

El servidor de proveedor 105 es operado por un proveedor que pone a disposición contenidos, que pueden cargarse mediante la red 102, 103, 104 en el terminal móvil 101. Los contenidos comprenden en particular códigos de programa para aplicaciones software, que son ejecutables mediante el entorno de ejecución de programas en el seno del terminal móvil 101 para ampliar la funcionalidad del terminal móvil 101. La comunicación entre el terminal móvil 101 y el servidor de proveedor 104 para la transmisión de contenidos se realiza basada en un protocolo de comunicación conocido por el experto, preferiblemente el Hypertext Transfer Protocol (HTTP) o un protocolo derivado de éste. Los protocolos de este tipo prevén varias etapas de comunicación para la transmisión de contenidos. En una primera etapa de comunicación se negocian el tipo y la forma de los contenidos a transmitir entre el terminal móvil 101 y el servidor de proveedor 105. Para ello, el terminal móvil 101 envía junto con la petición de los contenidos informaciones acerca de las funcionalidades disponibles en el terminal móvil, así como acerca de los formatos e idiomas preferibles que pueden ser interpretados por el terminal móvil 101 o que prefiere el usuario del terminal móvil 101. Los formatos e idiomas preferidos por el usuario están almacenados en un perfil de usuario en la memoria 113 o en el módulo de identificación de abonado 109. Las informaciones transmitidas por el terminal móvil 101 pueden comprender, en particular, indicaciones acerca del tipo y la versión del entorno de ejecución de programas existente, el tipo y el tamaño o la resolución del dispositivo visualizador 112, el tipo de teclado 111, una lista de decodificadores audio o video disponibles, una lista de tablas de caracteres admitidos o una lista de los idiomas preferidos. Con ayuda de las informaciones puede determinarse en el seno del servidor de proveedor 105 una de varias versiones disponibles de los contenidos solicitados, que está adaptada lo mejor posible a las informaciones recibidas o se puede generar una versión adaptada. En una etapa de comunicación posterior, se envían los contenidos adaptados del servidor de proveedor 105 al terminal móvil 101.

Al usar el HTTP, la petición de los contenidos se realiza con ayuda de una petición HTTP, que es un mensaje enviado por el terminal móvil 101 al servidor de proveedor 105, que comprende una zona de datos de la cabecera (Request-Header) y una zona de datos útiles. La zona de datos útiles contiene en particular una indicación de los contenidos específicos que se solicitan. En la cabecera de la petición están contenidas en particular informaciones acerca de la configuración del terminal móvil 101, de las que se han indicado anteriormente algunas a título de ejemplo. La cabecera de petición de por sí conocida para el experto contiene por lo general varios campos de cabecera que se designan respectivamente mediante una palabra clave estándar y que indican las informaciones correspondientes también con ayuda de denominaciones estándar. En caso de una petición de contenidos que se realiza en muchas ocasiones con ayuda de un método GET, la cabecera de petición tiene por ejemplo la forma que se indica a continuación. Las palabras clave de los distintos campos de la cabecera indicados a título de ejemplo están impresas en negrita, siendo los campos de cabecera de por sí conocidos por el experto, por lo que no se explican más detalladamente:

GET / HTTP/1.1
Host: www.vodafone.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1)
Gecko/20060508 Firefox/1.5.0.4
Accept: text/xml,application/xml,application/xhtml+xml,
text/html; q=0.9, text/plain; q=0.8, image/png, */*; q=0.5
Accept-Language: en-gb, en; q=0.5
Accept-encoding: gzip, deflate
Accept-Charset: ISO-8859-1, utf-8; q=0.7,*,q=0.7
Keep-Alive: 300
Proxy-Connection: keep-alive

Para impedir accesos no autorizados a APIs y datos sensibles del terminal móvil 101, en primer lugar se autentican los contenidos recibidos del servidor de proveedor 105 en el terminal móvil 101. Es después de haberse realizado con éxito la autenticación cuando se concede a las aplicaciones software recibidas el acceso a las APIs o datos. Si los contenidos no pueden autenticarse con éxito, no se concede el acceso a las APIs o datos correspondientes. En particular, también puede estar previsto que se borren los contenidos de la memoria 113, cuando la autenticación falla o cuando las aplicaciones software contenidas no pueden ejecutarse. La autenticación se realiza habitualmente en el marco de una llamada Public-Key-Infrastructure (PKI) con ayuda de un componente de autenticación de los contenidos, que se comprueba mediante un certificado digital. El componente de autenticación está realizado como firma digital, que comprende un valor hash de los contenidos o de una parte de los contenidos que está cifrado mediante una clave de cifrado privada del proveedor de los contenidos. La clave de cifrado privada tiene asignada una clave de comprobación, que se usa para la comprobación de la firma digital y que es parte de un certificado digital del proveedor emitido por un organismo de certificación. El certificado de proveedor se autentica aquí mediante una cadena de certificados, que comprende adicionalmente al menos un certificado raíz y, dado el caso,

uno o varios certificados intermedios. Mediante una autenticación del certificado de proveedor en el seno del terminal móvil 101 se garantiza que los contenidos hayan sido puestos a disposición por un proveedor clasificado como fiable. La comprobación posterior de la firma digital de los contenidos permite determinar si los contenidos se han recibido en el terminal móvil 101 en una forma no alterada.

En la Figura 2 están representadas a título de ejemplo varias cadenas de certificados, que están basadas en un certificado raíz 201 común. El nivel de jerarquía superior de las cadenas de certificados comprende, por lo tanto, el certificado raíz 201, que se incorpora en el marco de un proceso asegurado mediante un organismo de certificación en una zona segura del terminal móvil 101 y que contiene la clave de comprobación del organismo de certificación. Los certificados representados en los niveles de jerarquía habituales contienen una clave de comprobación, así como una firma digital, que puede comprobarse mediante una clave de comprobación, que está contenida en un certificado digital de un nivel de jerarquía superior. Con excepción del certificado raíz, un certificado de un nivel de jerarquía determinado puede autenticarse, por lo tanto, mediante un certificado de un nivel de jerarquía superior. En la Figura están representados a título de ejemplo certificados intermedios 202_1, …, 202_m, que pueden autenticarse mediante el certificado raíz 201. Además, están representados otros certificados intermedios 203_1,… 203_n, que se autentican respectivamente mediante uno de los certificados intermedios 202_i. Y finalmente están representados en la Figura certificados de proveedor 204_1,… 204_p, que pueden ser autenticados respectivamente mediante uno de los certificados intermedios 202_1, …, 202_m, 203_1,… 203_n o mediante el certificado raíz 201.

Habitualmente, el terminal móvil 1 contiene varios certificados raíz de distintos organismos de certificación, actuando por lo general en particular el fabricante del terminal móvil 101 y/o el operador de la red de telecomunicaciones 102 como organismo de certificación, que en lo sucesivo se denominarán brevemente operadores. El fabricante incorpora un certificado raíz preferiblemente durante la fabricación en una zona segura de la memoria 113 del terminal móvil 101. El certificado raíz del explotador se almacena habitualmente en una zona segura del módulo de identificación de abonado 109, antes de que el mismo sea entregado al usuario de telefonía móvil. Los certificados intermedios son transmitidos habitualmente en un momento posterior por el fabricante, el operador o una tercera parte, por ejemplo mediante la red 102, 103, 104 al terminal móvil 101. El uso de certificados intermedios para la autenticación de certificados de proveedor es preferible en comparación con la autenticación con ayuda del certificado raíz, puesto que los certificados intermedios pueden intercambiarse más fácilmente. Los certificados de proveedor se envían habitualmente junto con los contenidos transmitidos desde el servidor de proveedor 3 al terminal móvil.

Un proceso típico para la autenticación de contenidos y la emisión previa del certificado de proveedor en el sistema PKI comprende, por ejemplo, las siguientes etapas:

En primer lugar, un proveedor de contenidos genera una pareja asimétrica de claves con una clave de cifrado privada y una clave de comprobación o recibe una pareja de este tipo de un organismo de certificación. Además, el proveedor recibe del organismo de certificación un certificado de proveedor. Cuando se solicitan mediante el terminal móvil 101 contenidos al servidor de proveedor 105, los contenidos son provistos de una firma digital, que se genera mediante la clave de cifrado privada del proveedor. Los contenidos son enviados a continuación junto con la firma y el certificado de proveedor y los certificados intermedios dado el caso necesarios al terminal móvil 1. En el seno del terminal móvil 1 se autentica a continuación en primer lugar el certificado de proveedor con ayuda de un certificado raíz existente y, dado el caso, con ayuda de certificados intermedios existentes o recibidos. Después de haberse realizado la comprobación con éxito, la clave de comprobación contenida en el certificado de proveedor se usa para la comprobación de la firma digital de los contenidos. Es después de haberse comprobado con éxito esta firma digital, cuando es posible un acceso a las funciones y datos del terminal móvil 1 por parte de la aplicación software contenida en los contenidos. Los derechos de acceso pueden concederse, por ejemplo, también en función del certificado raíz usado para la comprobación del certificado de proveedor de los certificados intermedios usados. Por ejemplo el acceso a datos determinados solo puede concederse cuando se ha comprobado el certificado de proveedor mediante el certificado raíz o un certificado intermedio determinado del operador. Un acceso a otros datos puede concederse por ejemplo solo si el certificado de proveedor se ha comprobado mediante el certificado raíz del fabricante del terminal móvil 101.

En el seno del sistema PKI anteriormente descrito, los terminales móviles 1 pueden contener varios certificados raíz y certificados intermedios. Los terminales móviles 1 de distintos fabricantes contienen por lo general además distintos certificados raíz y certificados intermedios de los fabricantes. Además, los módulos de identificación de abonado 109 de distintos terminales móviles contienen distintos certificados raíz y certificados intermedios de distintos operadores. Para poder transmitir contenidos autenticables a terminales móviles 1 que han sido producidos por distintos fabricantes y que se usan en redes de telecomunicaciones 102 de distintos operadores, también puede autenticarse el proveedor mediante distintos certificados de proveedor, que pueden ser autenticados respectivamente mediante uno de los certificados raíz o certificados intermedios usados.

En el marco de la presente invención está previsto que el comportamiento del servidor de proveedor 105 se adapte a los certificados digitales contenidos en el terminal móvil 101 durante la transmisión de contenidos a un terminal móvil 101. Para ello, el terminal móvil 101 emite en el marco de la petición de contenidos informaciones acerca de los certificados digitales almacenados en la memoria 113 y el módulo de identificación de abonado 109 al servidor de proveedor 105. Durante este proceso se envían al menos informaciones acerca de los certificados raíz existentes en

el terminal móvil 101 al servidor de proveedor 105. Preferiblemente, se transmiten además informaciones acerca de los certificados intermedios disponibles en el terminal móvil 101. Además, también pueden almacenarse certificados de proveedor que se han recibido en una transmisión previa de contenidos en el terminal móvil 101 en la memoria 113 o en el módulo de identificación de abonado 109. Las informaciones acerca de los certificados de proveedor almacenados se transmiten preferiblemente también al servidor de proveedor 105.

En una forma de realización preferible, las informaciones acerca de los certificados digitales disponibles en el terminal móvil 101 se transmiten en el marco de la primera etapa de comunicación anteriormente descrita, prevista según HTTP, negociándose el tipo y la forma de los contenidos a transmitir entre el terminal móvil 101 y el servidor de proveedor 105. En particular, estas informaciones se incorporan en una forma estándar en la zona de datos de la cabecera de la petición HTTP. Esta contiene un campo de cabecera, en el que hay una lista de los certificados digitales disponibles en el terminal móvil 101. Una denominación posible del campo de cabecera es “Accept-Certificates”. La lista contenida en el campo de la cabecera puede indicar para cada certificado, en particular, un titular del certificado, una denominación del certificado y un país. Estos parámetros se marcan mediante denominaciones de parámetros, pudiendo designar por ejemplo una “C” el país, una “O” el titular y “x509v3 Subject Key Identifier” el nombre del certificado. Además, los parámetros pueden estar separados por barras diagonales y las distintas entradas de la lista mediante signos en forma de punto y coma. La lista puede tener, por ejemplo, la siguiente forma:

48:DD:3D:EF:E0:3C:9C:DF:12:B1:30:FD:91:E1:C1:E9:FB:98:DC
:08 (Vodafone Operator Domain);

47:E6:22:01:AA:BE:EB:CO:4F:2C:3E:A5:D1:47:2F:CE:59:1C:82
:FB (Vodafone TTP domain;

F1:5C:CO:OD:6A:71:37:A6:99:84:35:38:52:E2:53:73:67:71:D6
:30 (GeoTrust CA for UTI)

Si esta lista se inserta en la cabecera de petición que ya se ha indicado anteriormente a título de ejemplo, ésta tiene la siguiente forma:

GET / HTTP/1.1
Host: www.vodafone.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1)
Gecko/20060508 Firefox/1.5.0.4
Accept: text/xml,application/xml,application/xhtml+xml,
text/html; q=0.9, text/plain; q=0.8, image/png, */*;q=0.5
Accept-Language: en-gb, en; q=0.5
Accept-encoding: gzip, deflate
Accept-Charset: ISO-8859-1, utf-8; q=0.7,*,q=0.7
Accept-Certificates:

48:DD:3D:EF:EO:3C:9C:DF:12:B1:30:FD:91:E1:C1:E9:FB:97:DC :08;47:E6:22:O1:AA:BE:EB:CO:4F:
2C:3E:A5:D1:47:2F:CE:59:1
C:82:FB;F1:5C:CO:OD:6A:71:37:A6:99:84:35:38:52:E2:53:73: 67:71:D6:30
Keep-Alive: 300
Proxy-Connection: keep-alive

Después de la recepción de la petición HTTP en el servidor de proveedor 105 se evalúan en particular las informaciones acerca de los certificados digitales almacenados en el terminal móvil 101 para determinar qué certificados digitales están disponibles en el terminal móvil 101. Gracias a esta evaluación, el servidor añade a continuación a los contenidos a transmitir al terminal móvil 101 los certificados digitales que son necesarios para la comprobación del componente de autenticación de los contenidos y que no están disponibles en el terminal móvil 101.

En particular, se añade el certificado de proveedor a los contenidos, en caso de que no se haya enviado ya anteriormente durante una transmisión anterior de contenidos al terminal móvil 101 y no se haya almacenado en el terminal móvil 101. En caso de que haya que comprobar el certificado de proveedor con ayuda de uno o varios certificados intermedios que no están disponibles en el terminal móvil 101, se añaden a los contenidos a transmitir también los certificados intermedios necesarios.

En el seno del terminal móvil 101 se comprueba el componente de autenticación tras la recepción de los contenidos dado el caso mediante los certificados digitales recibidos junto con los contenidos. Además, los certificados digitales recibidos junto con los contenidos pueden almacenarse para volver a usarse en un futuro. De este modo, el terminal móvil 101 dispone en una petición posterior de contenidos al mismo servidor de proveedor 105 ya de todos los certificados digitales necesarios para la autenticación de los contenidos.

Gracias a la invención se consigue que en el servidor de proveedor 105 puedan determinarse exactamente los certificados digitales necesarios para la autenticación de los contenidos que no están disponibles en el terminal móvil con ayuda de una evaluación de las informaciones recibidas por el terminal móvil 101. A continuación, el servidor de proveedor 105 puede añadir estos certificados a los contenidos. De este modo se transmiten solo los certificados digitales que faltan con los contenidos. Se evita una transmisión innecesaria de certificados ya disponibles en el terminal móvil 101.

En caso de que por la evaluación de las informaciones recibidas por el terminal móvil 101 se detecte en el servidor de proveedor que los certificados digitales que faltan no están disponibles en el servidor de proveedor 105, por lo que no pueden enviarse junto con los contenidos al terminal móvil 101, el servidor de proveedor genera preferiblemente un mensaje con una lista de los certificados correspondientes. Esta se envía a continuación al terminal móvil 101. De este modo, el usuario del terminal móvil recibe indicaciones exactas de qué certificados digitales debe conseguir para la autenticación de los contenidos. El mensaje también puede contener una indicación de donde pueden conseguirse los certificados digitales que faltan.

En particular, un certificado digital que falta no puede ser puesto a disposición por el servidor de proveedor 105 cuando se trata de un certificado raíz. En este caso, el servidor de proveedor 101 puede enviar un mensaje con la denominación del certificado raíz que falta y el titular de este certificado. Con ayuda de este mensaje, el usuario del terminal móvil puede dirigirse a continuación al titular del certificado raíz para obtener el certificado. Cuando se trata por ejemplo del certificado raíz del operador, puede conseguir el certificado raíz que falta con ayuda del mensaje recibido por el servidor de proveedor en una filial del operador. En la filial, el certificado raíz puede identificarse con ayuda del mensaje y puede incorporarse a continuación en un proceso asegurado en una zona asegurada del módulo de identificación de abonado 109.

REIVINDICACIONES

1. Un procedimiento para la transmisión de contenidos de un servidor de proveedor (105) a un terminal móvil (101), comprendiendo los contenidos un componente de autenticación que es cifrado en el seno del servidor de proveedor (105) mediante una clave de cifrado privada y que puede ser comprobado mediante un certificado digital para autenticar los contenidos transmitidos, **caracterizado porque** en el servidor de proveedor (105) se recibe una información enviada en una primera etapa de comunicación desde el terminal móvil (101) mediante varios certificados digitales almacenados en el seno del terminal móvil (101), que son cifrados con una clave de cifrado correspondiente, porque la información es evaluada en el seno del servidor de proveedor (105), de modo que el servidor de proveedor (105) obtiene conocimiento de varios certificados digitales disponibles en el terminal móvil (101) y porque el servidor de proveedor (105) transmite los contenidos en una segunda etapa de comunicación al terminal móvil (101) en función de un resultado de la evaluación de las informaciones recibidas.

2. El procedimiento de acuerdo con la reivindicación 1, **caracterizado porque** en el servidor de proveedor (105) se recibe un mensaje enviado en la primera etapa de comunicación por el terminal móvil (101), que contiene las informaciones acerca de los certificados digitales almacenados en el seno del terminal móvil (101) en un formato estándar.

3. El procedimiento de acuerdo con la reivindicación 1 o 2, **caracterizado porque** la primera etapa de comunicación está basada en el Hypertext Transfer Protocol, recibiéndose en la primera etapa de comunicación una cabecera de petición enviada por el terminal móvil en el servidor de proveedor (105) y siendo la información acerca de los certificados digitales almacenados en el seno del terminal móvil (101) parte de una zona de datos de la cabecera de la petición HTTP.

4. El procedimiento de acuerdo con una de las reivindicaciones anteriores, **caracterizado porque** gracias a la evaluación de la información acerca de los certificados digitales almacenados en el seno del terminal móvil (101) se determina en el seno del servidor de proveedor (105) para cuáles de las claves de cifrado disponibles en el servidor de proveedor (105) está almacenado un certificado asignado en el terminal móvil (101).

5. El procedimiento de acuerdo con una de las reivindicaciones anteriores, **caracterizado porque** en el servidor de proveedor (105) se selecciona una clave de cifrado para la que está almacenado un certificado digital asignado en el terminal móvil y porque el componente de autenticación de los contenidos se cifra con la clave de cifrado seleccionada.

6. El procedimiento de acuerdo con una de las reivindicaciones anteriores, **caracterizado porque** el componente de autenticación de los contenidos se cifra en el servidor de proveedor (105) mediante una clave de cifrado que tiene asignado un certificado de proveedor digital, transmitiéndose el certificado de proveedor digital del servidor de proveedor (105) al terminal móvil (101).

7. El procedimiento de acuerdo con la reivindicación 6, **caracterizado porque** el certificado de proveedor digital puede ser autenticado mediante un certificado digital almacenado en el terminal móvil (101).

8. El procedimiento de acuerdo con la reivindicación 6 o 7, **caracterizado porque** un certificado intermedio digital es transmitido por el servidor de proveedor (105) al terminal móvil (101), pudiendo usarse el certificado intermedio digital para la comprobación del certificado de proveedor y pudiendo ser comprobado el certificado intermedio digital mediante un certificado intermedio digital almacenado en el terminal móvil.

9. El procedimiento de acuerdo con una de las reivindicaciones anteriores, **caracterizado porque** al menos un certificado digital almacenado en el terminal móvil (101) es un certificado raíz digital.

10. El procedimiento de acuerdo con la reivindicación 9, **caracterizado porque** el certificado raíz digital está almacenado en un módulo de identificación de abonado, que está contenido en el terminal móvil.

11. El procedimiento de acuerdo con la reivindicación 9 o 10, **caracterizado porque** el terminal móvil (101) contiene al menos otro certificado digital, que es un certificado intermedio, que puede ser autenticado mediante el certificado raíz.

12. El procedimiento de acuerdo con una de las reivindicaciones anteriores, **caracterizado porque** los contenidos contienen un código de programa, que es ejecutable en el seno del terminal móvil (101), después de haberse autenticado los contenidos transmitidos en el seno del terminal móvil (101).

13. Un producto de programa informático, **caracterizado porque** contiene un programa informático para la ejecución de un procedimiento de acuerdo con una de las reivindicaciones anteriores, cuando es ejecutado por un ordenador.

14. Un terminal móvil (101) para la recepción de contenidos de un servidor de proveedor (105), comprendiendo los contenidos un componente de autenticación que es cifrado mediante una clave de cifrado privada del servidor de proveedor (105) y pudiendo ser autenticado el componente de autenticación en el seno del terminal móvil (101) mediante un certificado digital asignado a la clave de cifrado, **caracterizado porque** el terminal móvil (101) está

realizado para transmitir en una etapa de comunicación una información acerca de varios certificados digitales almacenados en el seno del terminal móvil (101) al servidor de proveedor (105) para la comprobación de datos que están cifrados con una clave de cifrado correspondiente, de modo que el servidor de proveedor (105) obtiene conocimiento de varios certificados digitales disponibles en el terminal móvil (101).

15. Un servidor de proveedor (105) para la transmisión de contenidos a un terminal móvil (101), comprendiendo los contenidos un componente de autenticación que puede ser cifrado en el seno del servidor de proveedor (105) mediante una clave de cifrado privada y pudiendo ser autenticado el componente de autenticación en el seno del terminal móvil (101) mediante un certificado digital, **caracterizado porque** el servidor de proveedor (105) está realizado para recibir y evaluar una información enviada en una etapa de comunicación por el terminal móvil (101) mediante varias certificados digitales almacenados en el seno del terminal móvil (101) para la comprobación de datos que están cifrados con una clave de cifrado correspondiente, de modo que el servidor de proveedor (105) obtiene conocimiento de varios certificados digitales disponibles en el terminal móvil (101)

16. Un sistema de comunicación, en el que puede conectarse al menos un terminal móvil (101) con al menos un servidor de proveedor (105), **caracterizado porque** el sistema de comunicación comprende al menos un terminal móvil (101) de acuerdo con la reivindicación 14, así como al menos un servidor de proveedor (105) de acuerdo con la reivindicación 15.

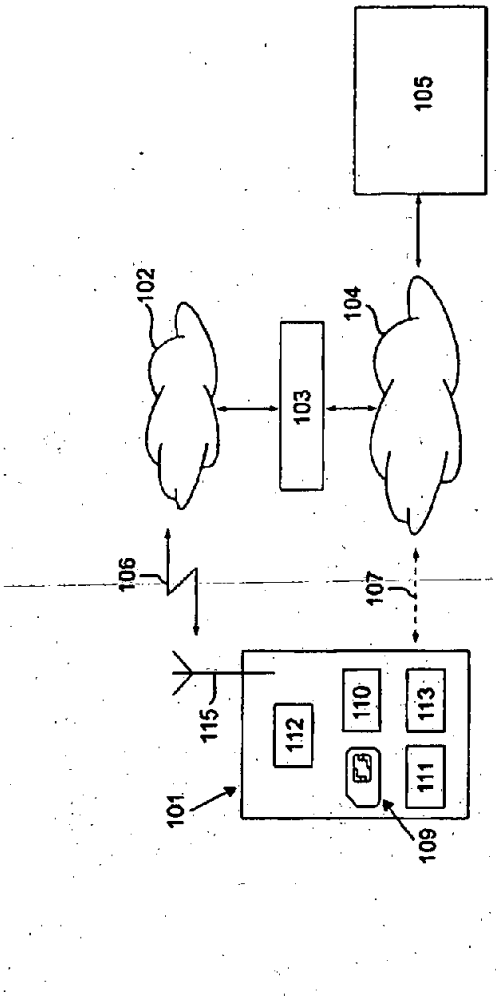

Fig. 1

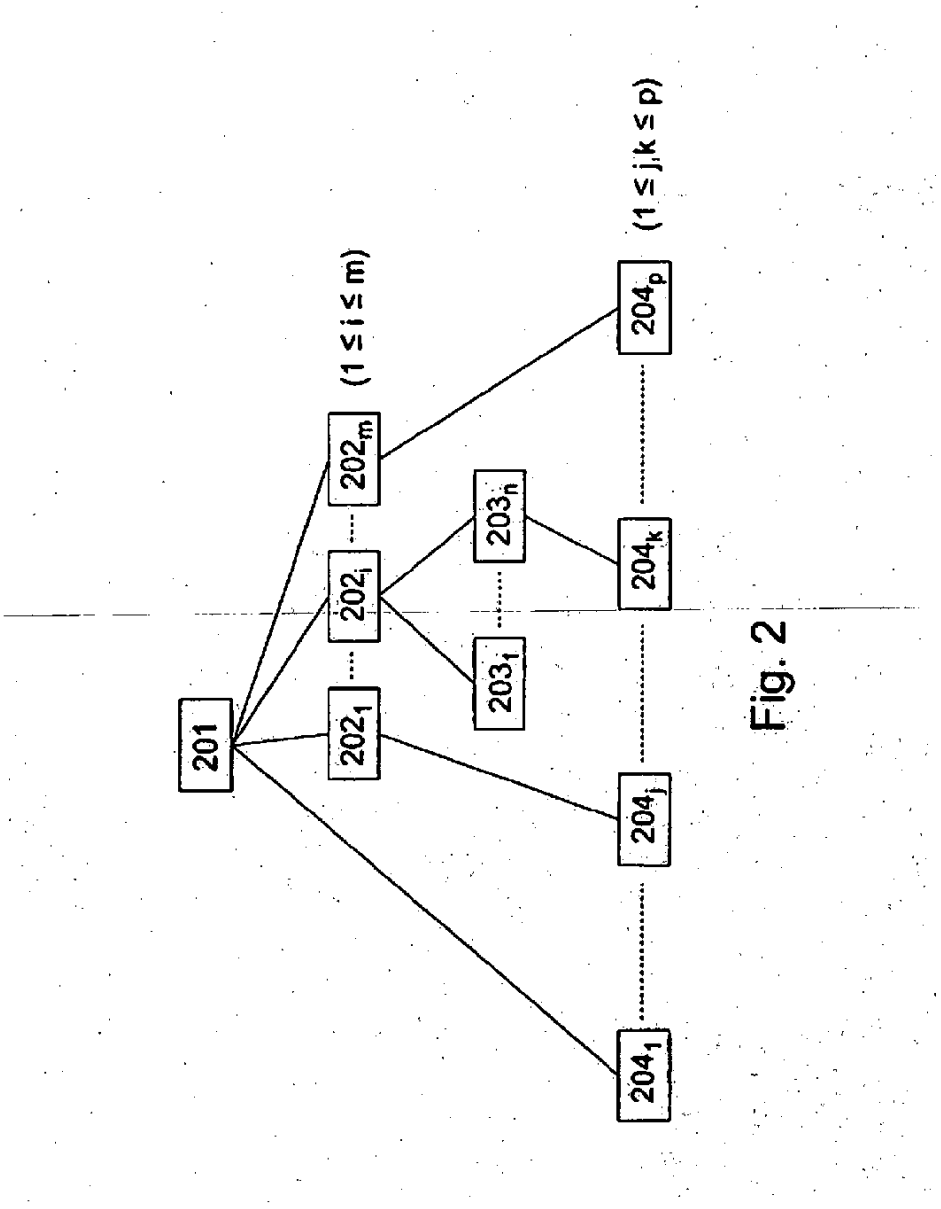
201
202_1
202_i
202_m
$(1 \leq i \leq m)$
203_1
203_i
203_n
204_1
204_j
204_k
204_p
$(1 \leq j,k \leq p)$

Fig. 2