(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 304 583**

(51) Int. Cl.:
H04Q 7/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **04104978 .4**
(86) Fecha de presentación : **11.10.2004**
(87) Número de publicación de la solicitud: **1646254**
(87) Fecha de publicación de la solicitud: **12.04.2006**

(54) Título: **Método de identificación y/o de autentificación mediante huellas digitales.**

(45) Fecha de publicación de la mención BOPI:
16.10.2008

(45) Fecha de la publicación del folleto de la patente:
16.10.2008

(73) Titular/es: **Swisscom Mobile AG.**
3050 Bern, CH

(72) Inventor/es: **Ritter, Rudolf y**
Lauper, Eric

(74) Agente: **Sugrañes Moliné, Pedro**

DESCRIPCIÓN

Método de identificación y/o de autentificación mediante huellas digitales.

La presente invención se refiere a un método y a un sistema para la identificación y/o para la autenticación de un usuario. La presente invención se refiere, especialmente, a un método y a un sistema para la identificación y/o para la autenticación del usuario de un aparato móvil en una aplicación de servidor.

Con algunos aparatos móviles actuales, como por ejemplo teléfonos móviles, PDA (*personal dactilar assistant*), ordenadores portátiles, etc. con interfaz de radiotelefonía móvil integrada, etc. pueden establecerse conexiones de datos a través de una red de radiotelefonía móvil. A través de tales conexiones el usuario de un aparato móvil puede acceder por ejemplo a un servidor remoto (por ejemplo a través de Internet, a través de una red externa o a través de una red WAP) e intercambiar datos con este servidor en ambos sentidos.

A este respecto el acceso a algunos datos (por ejemplo datos confidenciales o protegidos) en el servidor remoto puede protegerse o sólo autorizarse a usuarios identificados o autenticados. Puesto que los aparatos móviles y las tarjetas SIM pueden ser sustraídos o utilizarse por varios usuarios diferentes, no puede garantizarse una identificación personal.

A menudo se consigue una identificación y/o autenticación adicional exigiendo un código secreto (por ejemplo una contraseña o la combinación de una identificación de usuario con una contraseña secreta).

Cuando los datos introducidos coinciden con los datos de referencia, entonces el usuario se considera autenticado y se le autoriza el acceso los datos protegidos en el servidor remoto.

La introducción de tales datos de identificación y/o autenticación puede no resultar práctica en determinadas circunstancias, por ejemplo cuando deben introducirse en el teclado numérico de un teléfono móvil. Además, tal como se conoce, a menudo se escogen contraseñas demasiado simples que pueden adivinarse fácilmente, o se exigen contraseñas demasiado complicadas que se olvidan y se apuntan en alguna parte.

También se conocen procedimientos de identificación y autenticación biométricos en los que la identidad de un usuario se reconoce y/o comprueba mediante parámetros biométricos. También se conocen ya PDA, ordenadores portátiles, teléfonos de radiotelefonía móvil y medios de entrada (por ejemplo teclados y ratones) con lectores de huellas dactilares y se utilizan para detectar parámetros personales del usuario y enviarlos a un servidor remoto. Si se reconoce la huella dactilar entonces el usuario se considera autenticado.

El texto de la patente US 2002/0095586 A1 da a conocer una autenticación continua de un usuario de un ordenador. Se utilizan preferiblemente sensores biométricos para obtener información de identificación biométrica del usuario del ordenador. Esta información obtenida se compara con información biométrica almacenada previamente, que identifica al propietario legal del aparato. En el caso de que la información coincida, puede suponerse que el usuario es el dueño del aparato y se permite la realización de una transacción de seguridad crítica mientras no se interrumpa la introducción biométrica.

El texto de la patente US 5.420.936 da a conocer un método en el que se proporcionan en una pantalla de ordenador campos sensibles al tacto para que escoja un usuario. Cuando se toca uno de los campos con la punta del dedo, se analiza la huella dactilar y se compara con una lista de huellas dactilares autorizadas. Tras una comprobación satisfactoria de la huella dactilar, el usuario obtiene acceso al programa escogido.

La solicitud de patente US 2002/0194003 da a conocer un sistema de seguridad cliente-servidor. El sistema de seguridad cliente-servidor contiene un sistema de cliente, que recibe primeros datos biométricos y dispone de una primera etapa del procedimiento de autorización. En un ejemplo de realización, en el caso de los primeros datos biométricos se trata de datos de voz y la primera etapa del procedimiento de autorización comprende un primer algoritmo de reconocimiento de voz. Se proporciona un sistema de servidor para recibir segundos datos biométricos. El sistema de servidor contiene una segunda etapa del procedimiento de autorización. En un ejemplo de realización los segundos datos biométricos son datos de voz y la segunda etapa del procedimiento de autorización comprende un segundo algoritmo de reconocimiento de voz. En otro ejemplo de realización las primera y segunda etapas del procedimiento de autorización comprenden algoritmos biométricos diferentes.

Tales procedimientos requieren sin embargo en la mayoría de los casos un sensor adicional en el aparato móvil, que resulta difícil de integrar en aparatos muy miniaturizados. Además, durante el acceso al servidor protegido se requiere una etapa adicional para detectar los parámetros biométricos, lo que hace que el acceso no resulte muy cómodo.

Si no se reconoce la huella dactilar (por ejemplo porque el usuario tiene el dedo sucio o sudado) o porque ha pasado el dedo por el sensor de huellas digitales en otra dirección o con otra presión debe repetirse la operación y se pide al usuario que permita detectar una nueva huella dactilar. Esto resulta poco práctico.

La autenticación del usuario se realiza además mediante el resultado de una única lectura de las huellas dactilares, lo que conlleva una cierta inseguridad que depende de la precisión del método de reconocimiento.

Un objetivo de la invención es por tanto proponer un método para la identificación y/o para la autenticación del usuario de un aparato móvil que no presente las desventajas de los métodos del estado de la técnica.

Otro objetivo de la invención es proponer un método seguro para la identificación y/o para la autenticación del usuario de un aparato móvil en una aplicación de servidor.

Un objetivo adicional de la invención es proponer un método de identificación y/o autenticación más práctico y sencillo para el usuario.

Estos objetivos se consiguen mediante un método, un servidor y un producto de programa que presentan las características de las reivindicaciones independientes correspondientes. Se indican además formas de realización preferidas mediante las reivindicaciones dependientes.

Estos objetivos se consiguen especialmente mediante un método para la identificación y/o para la autenticación de un usuario de un aparato móvil en una aplicación de servidor mediante las huellas dactilares de dicho usuario, que se detectan mediante medios de entrada táctiles, comprendiendo dicho método las siguientes etapas:

- el usuario navega con dichos medios de entrada táctiles en una parte libre del servidor y/o introduce con dichos medios de entrada táctiles instrucciones para desplazarse por dicha parte libre del servidor,
- al mismo tiempo se detectan huellas dactilares de dicho usuario mediante dichos medios de entrada táctiles,
- como muy tarde cuando dicho usuario quiere acceder a una parte del servidor que requiere una identificación o una autenticación, el usuario se identifica o autentica mediante dichas huellas dactilares,
- el acceso a dicha parte del servidor se autoriza sin petición de identificación o autenticación explícita si dicho usuario se ha identificado o autenticado en la etapa anterior.

Esto tiene la ventaja de que el usuario a menudo puede acceder directamente y sin autenticación explícita a la parte protegida del servidor. En una variante preferida, el menú del servidor está diseñado de tal manera que se leen suficientes huellas dactilares durante el manejo normal de los medios táctiles, por ejemplo durante la navegación del usuario por dicho menú, antes de que el usuario llegue a esta parte protegida del servidor.

Este método también tiene la ventaja de que es totalmente compatible con aparatos móviles que no disponen de medios de entrada táctiles con lectores de huellas dactilares incorporados. En este caso se requiere sencillamente una autenticación habitual (por ejemplo mediante contraseñas), cuando el usuario quiere entrar en la zona protegida.

Estos objetivos se consiguen también mediante un servidor con una parte de acceso libre y una parte protegida, con:

- un sistema de menús por el que un usuario puede desplazarse y/o navegar mediante instrucciones al menos en dicha parte libre,
- un comparador para comparar las huellas dactilares del usuario detectadas durante una sesión con huellas dactilares de referencia,

estando diseñado dicho sistema de menús de tal manera que el acceso a dicha parte del servidor se da sin petición de identificación o autenticación explícita si dicho usuario se identificó o autenticó mediante dicho comparador durante su desplazamiento o la navegación en dicha parte de acceso libre.

Estos objetivos se consiguen especialmente también mediante un producto de programa que puede cargarse directamente en una zona de memoria con un programa que realiza el procedimiento anteriormente indicado cuando se ejecuta en un procesador.

Gracias al método de la invención y al servidor y/o producto de programa correspondiente, el usuario se identifica y/o autentica de forma iterativa mediante sus huellas dactilares que se leen mientras navega por la parte de acceso libre del servidor. Por tanto no tiene que pedírsele de manera explícita que introduzca sus datos de identificación y/o autenticación. La identificación y/o autenticación se realiza además mediante una mayor cantidad de datos de huellas dactilares y la seguridad se aumenta de este modo.

El análisis de datos de huellas dactilares requiere además una potencia de procesamiento de datos considerable. Si la identificación y/o autenticación del usuario en un aparato móvil se realiza con una potencia limitada, entonces esta operación puede durar relativamente mucho tiempo. Gracias al método de la invención y al servidor y/o producto de programa correspondientes la identificación y/o autenticación del usuario se realiza preferiblemente durante su navegación por la parte de acceso libre del servidor, antes de que quiera acceder a una parte protegida. La identificación

y/o autenticación se realiza por tanto, por ejemplo, durante tiempos muertos, y no es por tanto crítica con respecto al tiempo. Preferiblemente el usuario puede por tanto acceder directamente a la parte protegida del servidor cuando lo requiere.

La invención se entenderá mejor mediante la descripción de una forma de realización preferida y mediante el dibujo. Muestra:

la figura 1, una representación esquemática de un sistema según una forma de realización de la invención.

Según la invención a través de una red de radiotelefonía móvil 3 se establece una conexión de datos entre un aparato móvil 2 de un usuario 1 y un servidor 4, por ejemplo, una Web o un servidor Wap, que se operan por ejemplo por un proveedor de múltiples servicios o por la empresa del usuario. El servidor 4 puede corresponder también a una LAN (*Local Area Network*, red de área local), por ejemplo una LAN corporativa con varios servidores a los que puede accederse desde Internet para usuarios autenticados.

El aparato móvil 2 dispone de una interfaz de radiotelefonía móvil 24, para comunicarse en la red de radiotelefonía móvil 3 y enviar y recibir datos. El aparato móvil 2 comprende preferiblemente un módulo de identificación no representado para la identificación del usuario 1 y/o del aparato móvil 2 en la red de radiotelefonía móvil 3. El módulo de identificación es por ejemplo una tarjeta chip extraíble con una zona de memoria en la que están almacenados datos de identificación del usuario. Si la red de radiotelefonía móvil 3 es por ejemplo una red GSM, entonces la tarjeta chip es por ejemplo una tarjeta SIM. El aparato móvil 2 también dispone preferiblemente de una pantalla 23 y de medios de entrada táctiles, que se utilizan con los dedos, para controlar el aparato móvil 2 y/o el servidor remoto a través de la red de radiotelefonía móvil 3. Los medios de entrada táctiles pueden ser por ejemplo un teclado, un teclado numérico, un elemento giratorio (por ejemplo un denominado "botón giratorio"), un ratón, un lápiz con el que puede controlarse un cursor, una pantalla táctil o una pantalla activada de manera táctil, una superficie sensible al tacto, etc.

Según la invención los medios de entrada táctiles 20 comprenden un lector de huellas dactilares, de manera que se detectan huellas dactilares cuando se dan instrucciones, por ejemplo cuando se pulsa una tecla o cuando se desplaza el cursor.

En una variante preferida los medios de entrada táctiles comprenden un sensor sensible al tacto capacitivo, con varias filas de electrodos capacitivos que reaccionan al movimiento de un dedo para controlar un cursor sobre la pantalla del aparato móvil y/o para hacer clic sobre opciones u objetos. Con el mismo sensor pueden detectarse al mismo tiempo también huellas dactilares. Tales medios de entrada táctiles permiten por ejemplo detectar de forma imperceptible huellas dactilares durante la introducción de instrucciones. Si se mueve un dedo sobre la superficie capacitiva, al mismo tiempo se detecta una huella dactilar y la dirección, velocidad y duración del movimiento se utiliza como instrucción para controlar el aparato móvil local y/o un servidor remoto mediante un cursor.

El lector de huellas dactilares también podría integrarse en otra tecla de navegación 21 que se utiliza normalmente para seleccionar opciones en menús visualizados en la pantalla 23.

El lector de huellas dactilares es por ejemplo un lector pequeño y ancho con, por ejemplo, una resolución de 8 puntos por 196 puntos. Un lector de huellas dactilares de este tipo puede detectar preferiblemente el movimiento de un dedo sobre su superficie, por ejemplo de forma capacitiva y/u óptica y, por ejemplo, controlar un cursor sobre la pantalla 23 del aparato móvil 2 según la dirección y/o la velocidad de este movimiento y, al mismo tiempo, escanear la huella dactilar del dedo. Un lector de huellas dactilares de este tipo también puede utilizarse como tecla de navegación en el marco de la invención.

Preferiblemente, la interfaz de radiotelefonía móvil 24, el módulo de identificación, los medios de entrada táctiles 20 están integrados con el lector de huellas dactilares y la pantalla 23 en un único aparato 2, tal como por ejemplo un único teléfono móvil o PDA (*Personal Digital Assistant*). Sin embargo, en una variante de la invención estos elementos están separados en dos o más aparatos. El aparato móvil 3 de la invención consiste entonces, por ejemplo, en la unión de un teléfono móvil y una PDA, comprendiendo el teléfono móvil por ejemplo una interfaz de radiotelefonía móvil y un módulo de identificación, y disponiendo la PDA de medios de entrada táctiles con un lector de huellas dactilares. Como pantalla del aparato móvil se utiliza entonces por ejemplo la pantalla de la PDA. El teléfono móvil y la PDA se comunican entonces preferiblemente a través de una conexión inalámbrica o sin contacto de corto alcance o a través de una conexión por cable. La conexión inalámbrica de corto alcance es por ejemplo una conexión Bluetooth, de infrarrojos o WiFi. En el caso de una conexión por cable, el teléfono móvil y la PDA se comunican entre sí por ejemplo a través de una conexión serie o USB.

En una forma de realización de la invención, la red de radiotelefonía móvil 3 es por ejemplo una red GSM, HSCSD, GPRS, UMTS, Bluetooth, WLAN (*wireless local area network*). No obstante, también son posibles otras formas de realización en el marco de la invención.

El servidor 4 es preferiblemente un servidor Web, Wap o SMS, un servidor SQL con una base de datos, un servidor de datos, una red de varios servidores en una LAN, etc., y puede llegarse al mismo a través de un canal de datos de la red de radiotelefonía móvil (por ejemplo a través de Internet u otro canal por paquetes). El servidor puede interpretar

instrucciones del usuario, teniendo el concepto "instrucción" en este marco un significado amplio y debiendo comprender cualquier dato que se reciba por parte del usuario y que afecte al comportamiento del servidor. El servidor lo puede facilitar por ejemplo un proveedor de servicios de valor añadido, por ejemplo una empresa, un banco, un gobierno, un operador de radiotelefonía móvil, etc.

El servidor comprende una parte de acceso libre 5 y una parte protegida 6. En la parte de acceso libre puede encontrarse por ejemplo información general sobre el proveedor de servicios y los servicios de valor añadido ofrecidos por el proveedor de servicios, información comercial, publicidad, etc. que se reparten por ejemplo en una o varias páginas web o tarjetas Wap. El usuario 1 preferiblemente no necesita estar identificado para poder acceder a esta información. Sin embargo, también es posible en el marco de la invención que se requiera una identificación de usuario cuando el usuario quiere acceder a determinadas páginas o datos de la parte de acceso libre; en este caso puede pedirse al usuario por ejemplo que introduzca manualmente su identidad. Esta identidad no se comprueba, o al menos no con medios biométricos y puede depositarse por ejemplo en una *cookie* en el aparato móvil.

En la parte protegida 6 del servidor puede estar presente por ejemplo información financiera, información médica, datos de usuarios o empresas, etc. Mediante esta parte 6 pueden ofrecerse también servicios de valor añadido, tal como por ejemplo la posibilidad de dar órdenes de pago desde una cuenta bancaria o desde una cuenta de una tarjeta de crédito, obtener asesoramiento médico personal y dirigido, hacer pedidos de productos o servicios, etc. También son posibles otros tipos de información y servicios confidenciales en el marco de la invención.

Para acceder a esta información confidencial 6 y a los servicios asociados, el usuario 1 debe estar identificado y autenticado. Esto significa que debe conocerse y controlarse su identidad.

La identificación del usuario puede realizarse por ejemplo mediante el número de teléfono del aparato móvil o mediante otros datos que se leen desde el módulo de identificación en el aparato móvil. También es posible una identificación mediante comparación de las huellas dactilares del usuario detectadas con huellas de referencia de varios usuarios. En el marco de la invención el usuario también puede teclear su identidad, pronunciarla en voz alta o deletrearla oralmente a través de un servidor de voz.

En una forma de realización de la invención el servidor 4 comprende preferiblemente una zona de memoria 40 que sirve por ejemplo para almacenar temporalmente datos de identificación y/o autenticación. Tal como se explicará más adelante, los datos de identificación y/o autenticación almacenados temporalmente comprenden por ejemplo las huellas dactilares del usuario 1 leídas por el aparato móvil 2.

En esta forma de realización el servidor 4 comprende preferiblemente también una base de datos de referencia 41, que contiene datos de identificación y/o autenticación de referencia de los usuarios registrados en el servidor 4. Los datos de referencia comprenden por ejemplo huellas dactilares de referencia que se tomaron y almacenaron, por ejemplo, durante una operación de registro del usuario.

Las huellas dactilares pueden almacenarse y procesarse o bien como imagen o bien preferiblemente como vector o signatura, que se determinan preferiblemente en el aparato móvil 2 o posiblemente en el servidor 4 a partir de la huella dactilar.

El servidor 4 también comprende preferiblemente un comparador 42 para el análisis y para la comparación de los datos de huellas dactilares digitales. El comparador 42 se utiliza preferiblemente para establecer con una cierta seguridad si las huellas dactilares leídas por el aparato móvil 2 corresponden a determinadas huellas dactilares de referencia. El comparador se implementa preferiblemente en forma de un programa que se ejecuta por ejemplo en el servidor no representado o en el aparato móvil 2. Pueden utilizarse por ejemplo modelos de Markov ocultos (HHM, *Hidden Markov Models*), redes neuronales y/o redes Viterbi para comparar huellas dactilares. El comparador también realiza preferiblemente una normalización de las huellas dactilares para compensar giros, ruidos, otras distorsiones geométricas que aparecen por ejemplo debido a desviaciones de presión.

El establecimiento de la conexión entre el aparato móvil 2 y el servidor 4 se activa por ejemplo en el lado del aparato móvil 2 mediante el accionamiento con una tecla determinada, mediante la selección de una opción determinada en un menú, mediante la introducción de una dirección en un navegador, etc. Una vez establecida la conexión, el usuario 1 llega por ejemplo a una página de inicio pública del servidor 4. La página de inicio se visualiza preferiblemente en la pantalla 23 del aparato móvil 2. La página de inicio comprende preferiblemente un menú desde el que pueden seleccionarse diferentes opciones (que por ejemplo corresponden a diferentes servicios de valor añadido). Para seleccionar una opción en el menú, el usuario 1 necesita preferiblemente los medios de entrada táctiles 20 del aparato móvil 2, preferiblemente medios de entrada táctiles 21 con un lector de huellas dactilares integrado, para desplazar por ejemplo un cursor por una superficie gráfica o de texto.

Según la invención, con un accionamiento de los medios de entrada táctiles 21 durante la navegación del usuario 1 por la parte de acceso libre del servidor 4 se leen al mismo tiempo las huellas dactilares del usuario 1 que realiza la activación mediante el lector de huellas dactilares integrado. Las huellas dactilares se transmiten conjuntamente o por separado de las instrucciones al servidor 4, y se almacenan como imagen o preferiblemente como vector en la zona de memoria 40 del servidor 4. La conversión en un vector se realiza preferiblemente en el lector de huellas dactilares.

También pueden transmitirse al mismo tiempo al servidor 4 varias huellas dactilares, o una función que se determina en el aparato móvil a partir de varias huellas dactilares.

Ciertas instrucciones introducidas por el usuario a través de los medios de entrada táctiles pueden interpretarse por el aparato móvil (por ejemplo por el programa de navegación en el aparato móvil) y no transmitirse necesariamente al servidor. Sin embargo si durante la introducción de estas instrucciones se detectan huellas dactilares, estas huellas dactilares preferiblemente se utilizan y se transmiten al servidor.

Por el contrario, también puede suceder que ciertas instrucciones se introduzcan con el aparato móvil sin que se detecte con ello una huella dactilar.

En una primera forma de realización de la invención, el usuario 1 se identifica y autentica mediante sus huellas dactilares.

Las huellas dactilares leídas y almacenadas se analizan preferiblemente mediante el comparador 42 y se comparan con las huellas dactilares de referencia almacenadas en la base de datos de referencia 41 para determinar con una cierta probabilidad predeterminada si corresponden a las huellas dactilares de un usuario registrado en el servidor.

Preferiblemente, la identificación del usuario 1 se produce de manera iterativa. Con cada nueva lectura de las huellas dactilares del usuario 1 mediante la tecla de navegación 21 se completan por ejemplo los datos de huella dactilar almacenados que corresponden al usuario 1 y se comparan de nuevo con los datos de huellas dactilares de referencia. Por tanto, preferiblemente con cada nueva comparación el número de posibles identidades para el usuario se reduce hasta que por ejemplo el comparador reconoce una identidad con una probabilidad predeterminada.

Si el usuario desea acceder a servicios o información protegidos y/o confidenciales 6, entonces se propone al usuario 1 la identidad reconocida por el comparador 42 preferiblemente en la pantalla 23 del aparato móvil 2 por ejemplo en forma de un nombre de usuario. El usuario 1 debe confirmar o rechazar entonces esta identidad preferiblemente accionando medios de entrada táctiles.

Si el usuario 1 no confirma esta identidad, entonces se pide al usuario 1 por ejemplo en una página de menú siguiente del servidor 4 que introduzca él mismo su identidad (por ejemplo mediante el teclado 20). En una variante se propone al usuario 1 una lista de otras identidades de las que puede seleccionar su supuesta identidad preferiblemente mediante la tecla de navegación 21. Estas identidades se proponen por ejemplo por el aparato móvil 2 y/o por el servidor 4. Comprenden por ejemplo identidades que están almacenadas en el aparato móvil 3 (por ejemplo en el módulo de identificación). Preferiblemente comprenden también identidades que se han reconocido con una menor probabilidad como identidades posibles para el usuario 1 por el comparador 42.

El usuario puede identificarse por tanto mediante sus huellas dactilares, sus propias indicaciones, su número de teléfono y/o datos de su módulo de identificación. Si quiere acceder a una parte protegida 6 del servidor 4, sin embargo todavía debe autenticarse, su identidad debe comprobarse.

Si se autenticó durante la navegación por la parte de acceso libre del servidor de manera fiable mediante la comparación entre las huellas dactilares y las huellas dactilares de referencia, puede llegar preferiblemente sin más controles y especialmente sin autenticación explícita a la parte protegida del servidor y realizar operaciones también en esta parte. En una forma de realización preferida, el servidor comprueba únicamente si el usuario que accede sigue siendo el usuario autenticado en ese momento, por ejemplo comprobando una identificación de la sesión. Una autenticación válida sólo dura preferiblemente durante un tiempo predeterminado. La probabilidad con la que se autenticó el usuario 1 en el aparato móvil 2 y/o en el servidor 4 se considera por tanto preferiblemente cada vez inferior con el tiempo, si no se leen nuevas huellas dactilares del usuario 1. En otra forma de realización, la identificación y/o autenticación se inicia de nuevo por ejemplo con cada nuevo establecimiento de conexión.

Por tanto si en ese instante el servidor 4 no puede autenticar al usuario 1 con la seguridad necesaria, se requiere una autenticación explícita antes de que el usuario pueda llegar a la parte protegida del servidor. Se puede pedir al usuario por ejemplo que permita la detección de más huellas dactilares con el lector de huellas dactilares 21, pudiéndose presentar al usuario instrucciones para el correcto uso del sensor (“no tan rápido”, “dirección de desplazamiento correcta”, etc.).

Si a pesar de estos nuevos intentos, no se consigue la autenticación, se puede pedir al usuario que se autentique de otro modo, por ejemplo con una contraseña o con otros parámetros biométricos.

El sistema de menús en la parte de acceso libre del servidor 4 está diseñado preferiblemente de tal manera que el usuario debe dejar que se lean varias veces sus huellas dactilares cuando quiere llegar desde la parte libre a la parte protegida. Por ejemplo, se requieren varios movimientos del cursor o acciones de selección de opciones para que se detecten al menos dos (posiblemente muchas más) huellas dactilares, antes de que el usuario llegue a la página por la que puede entrar a la parte protegida del servidor 4. Puede requerirse también deliberadamente que el usuario realice movimientos de su dedo en varias direcciones diferentes para desplazar el cursor, antes de que llegue a la parte protegida. Esto permite recopilar varias huellas dactilares diferentes y reducir el riesgo de que un usuario deba autenticarse explícitamente.

El usuario se considera autenticado cuando la probabilidad de una identificación (o autenticación) errónea es inferior a un umbral predeterminado. Este umbral se establece preferiblemente por el operador del servidor 4.

Si el usuario según una forma de realización de la invención se identifica y autentica mediante sus huellas dactilares, entonces no es necesario que deba introducir su identidad y/o una clave secreta por ejemplo con el teclado del aparato móvil para autenticarse en la parte protegida del servidor 4.

En otras formas de realización de la invención, la identificación del usuario sólo se realiza mediante datos de huellas dactilares en la aplicación de servidor. Se pide entonces al usuario 1 que permita comprobar esta identidad determinada automáticamente por ejemplo mediante una contraseña.

En una forma de realización de la invención se encuentra una base de datos de referencia en el propio aparato móvil 2. En el módulo de identificación (o en el aparato móvil 2) se depositan por ejemplo durante una operación de registro huellas dactilares. Estas huellas dactilares de referencia son entonces preferiblemente las huellas dactilares del usuario habitual del módulo de identificación en el aparato móvil 2. También pueden almacenarse varias huellas dactilares de referencia, que corresponden a diferentes usuarios del mismo aparato móvil 2. El programa se carga de forma remota por ejemplo como miniaplicación (*applet*) desde el servidor 4. Durante la operación de registro el programa pide por ejemplo al o a los usuarios que activen los medios de entrada táctiles 21 para recibir huellas de referencia hasta que se han leído suficientes datos para cada usuario para formar huellas dactilares de referencia buenas. Estas huellas dactilares de referencia se almacenan entonces en la base de datos de referencia en el aparato móvil y/o en el módulo de identificación.

El programa está preferiblemente firmado electrónicamente por el servidor 4 y/o los correspondientes proveedores de servicios de valor añadido para impedir una falsificación.

La comparación entre la huella de referencia y las huellas detectadas durante una sesión también puede realizarse por un programa en el aparato móvil 2. El resultado de esta comparación se firma entonces electrónicamente y (con o sin petición) se envía al servidor 4. La comparación se realiza por ejemplo por un comparador (por ejemplo en forma de un programa en el módulo de identificación y/o en el aparato móvil 2). Si el módulo de identificación comprende un procesador, entonces el programa del comparador se ejecuta por ejemplo en el procesador del módulo de identificación y/o en el procesador del propio aparato móvil 2. El programa del comparador preferiblemente se carga de manera remota, por ejemplo, como miniaplicación del servidor 4.

Una ventaja de la forma de realización de la invención en la que la base de datos de referencia y el comparador están situados en el aparato móvil 2 es que no se intercambian datos de huellas dactilares entre el aparato móvil y el servidor 4 a través de la red de radiotelefonía móvil. Los datos de huellas dactilares siguen perteneciendo por tanto de forma segura y preferiblemente confidenciales al usuario 1.

En una variante para identificar al usuario 1 se utiliza el comparador en el aparato móvil 2, mientras que para la autenticación se utilizan resultados de comparación de un comparador 42 en el servidor 4, o viceversa.

En otra forma de realización más, las huellas dactilares de referencia se almacenan en un servidor central adicional no representado. El servidor central se gestiona por ejemplo por un tercero o por el operador de la red de radiotelefonía móvil 3 para varios proveedores de servicios y/o varios servidores. El comparador se ejecuta entonces preferiblemente también en el servidor central. Las huellas dactilares leídas se envían entonces por ejemplo al servidor central a través de la red de radiotelefonía móvil 3 al comparador. Esto tiene la ventaja, entre otras, de que el usuario sólo debe registrarse una vez en un único servidor para depositar sus huellas dactilares y obtener un acceso autenticado a diferentes servidores de distintos proveedores de servicios.

Los menús por los que debe navegar el usuario para que puedan leerse varias veces sus huellas dactilares se generan preferiblemente por el servidor 4 y se visualizan en la pantalla 23 del aparato móvil 2.

Sin embargo, en una forma de realización de la invención, estos menús se generan por un programa en el aparato móvil. Los datos de huellas dactilares necesarios del usuario 1 se leen por tanto preferiblemente antes del establecimiento de la conexión con el servidor 4. Si el comparador se ejecuta también en el aparato móvil, entonces la conexión se establece por ejemplo sólo cuando el usuario 1 se ha identificado y/o autenticado.

La identificación o autenticación del usuario 1 puede realizarse preferiblemente con las huellas dactilares de diferentes dedos del usuario 1. En una forma de realización de la invención los menús en la parte de acceso libre del servidor 4, en la parte protegida del servidor 4 y/o en el aparato móvil 2 dependen del dedo o de los dedos que ha utilizado el usuario 1 para activar por ejemplo las tecla de navegación 21 y que han llevado posiblemente a su identificación o autenticación. Se generan por ejemplo diferentes menús en caso de que el usuario 1 utilice la mano derecha o la izquierda para navegar por el sistema de menús y posiblemente para identificarse o autenticarse con los datos de huellas dactilares de esta mano. Por tanto el usuario también puede acceder por ejemplo a diferentes opciones utilizando una determinada mano y/o un determinado dedo. También pueden utilizarse sin embargo otros criterios para generar diferentes menús. Estos criterios comprenden por ejemplo la identidad del usuario, el grado de autenticación del usuario 1, etc.

La identificación o autenticación del usuario con un lector de huellas dactilares puede tener en cuenta también, según la invención, la dirección, el desplazamiento, la duración y/o el ritmo personal del desplazamiento del dedo del usuario por el sensor; de este modo se utiliza una huella dactilar dinámica que contiene más información que una estática. La determinación de la dirección de desplazamiento y la velocidad puede emplearse también para normalizar las huellas dactilares, por ejemplo para girarlas en función de la dirección de desplazamiento.

REIVINDICACIONES

1. Método para la identificación y/o para la autenticación de un usuario (1) de un aparato móvil (2), que comprende un módulo de identificación para la identificación del usuario y/o del aparato móvil (2), en una aplicación de servidor mediante huellas dactilares de dicho usuario (1), **caracterizado** porque dichas huellas dactilares se detectan mediante medios de entrada táctiles (21), comprendiendo dicho método las siguientes etapas:

- el usuario (1) introduce con dichos medios de entrada táctiles (21) instrucciones para desplazarse por una parte de acceso libre del servidor (4),
- al mismo tiempo se detectan huellas dactilares de dicho usuario mediante dichos medios de entrada táctiles (21),
- como muy tarde cuando dicho usuario quiere acceder a una parte protegida del servidor que requiere una identificación o una autenticación, el usuario se identifica o autentica mediante dichas huellas dactilares,
- el acceso a dicha parte protegida del servidor se da sin petición de identificación o autenticación explícita si dicho usuario se ha identificado o autenticado en la etapa anterior.

2. Método según la reivindicación 1, en el que se requiere una identificación o autenticación explícita si dicho usuario no se ha identificado o autenticado de manera fiable mediante dichas huellas dactilares.

3. Método según la reivindicación 2, en el que se pide al usuario que permita leer otra vez sus huellas dactilares si no se ha identificado o autenticado de manera fiable mediante dichas huellas dactilares.

4. Método según una de las reivindicaciones 2 ó 3, en el que se pide al usuario que introduzca una contraseña si no se ha identificado o autenticado de manera fiable mediante dichas huellas dactilares.

5. Método según una de las reivindicaciones 1 a 4, en el que el usuario se identifica o autentica comparando varias huellas dactilares detectadas una tras otra durante la misma sesión con huellas dactilares de referencia del usuario.

6. Método según una de las reivindicaciones 1 a 5, en el que el usuario se considera identificado o autenticado cuando la probabilidad de una identificación o autenticación errónea es inferior a un umbral predeterminado.

7. Método según la reivindicación 6, en el que dicho umbral se establece por el operador de dicho servidor.

8. Método según una de las reivindicaciones 5 a 7, en el que se utilizan modelos ocultos de Markov y/o redes neuronales para comparar huellas dactilares detectadas durante una sesión con huellas dactilares de referencia del usuario.

9. Método según una de las reivindicaciones 1 a 8, en el que dicho usuario se identifica mediante datos en dicho módulo de identificación o mediante indicaciones introducidas por él mismo en una primera etapa,

y en el que la identidad del usuario determinada durante dicha primera etapa se comprueba mediante huellas dactilares detectadas durante el desplazamiento del usuario por dicha parte de acceso libre del servidor para autenticar a dicho usuario.

10. Método según una de las reivindicaciones 1 a 9, en el que dicho servidor está diseñado de tal manera que se leen varias huellas dactilares del usuario con dichos medios de entrada táctiles cuando este usuario navega con dichos medios de entrada táctiles por dicha parte de acceso libre para llegar hasta dicha parte protegida.

11. Método según una de las reivindicaciones 1 a 10, con una operación de registro en la que se almacenan huellas dactilares de referencia del usuario en una base de datos de referencia (41) de dicho servidor (4).

12. Método según una de las reivindicaciones 1 a 10, con una operación de registro en la que se almacenan huellas dactilares de referencia del usuario en una base de datos de referencia (41) en dicho aparato móvil (2).

13. Método según una de las reivindicaciones 1 a 10, con una operación de registro en la que se almacenan huellas dactilares de referencia del usuario en una base de datos de referencia (41) en el servidor de un tercero, que realiza identificaciones de usuario para varios servidores de diferentes proveedores.

14. Método según una de las reivindicaciones 1 a 13, en el que dicha identificación o autenticación se realiza en dicho servidor (4).

15. Método según una de las reivindicaciones 1 a 13, en el que dicha identificación o autenticación se realiza en el servidor de un tercero, que realiza identificaciones de usuario para varios servidores de diferentes proveedores.

16. Método según una de las reivindicaciones 1 a 13, en el que dicha identificación o autenticación se realiza en dicho aparato móvil (2).

17. Método según la reivindicación 16, en el que un programa de identificación de usuario se carga de manera remota en dicho aparato móvil.

18. Método según la reivindicación 17, en el que dicho programa se firma electrónicamente.

19. Servidor (4), **caracterizado** por una parte de acceso libre y una parte de acceso protegido, con:

- un sistema de menús, por el que puede desplazarse un usuario (1) mediante instrucciones al menos por dicha parte de acceso libre,

- un comparador (42) para comparar huellas dactilares del usuario detectadas durante una sesión con huellas dactilares de referencia,

estando diseñado dicho sistema de menús de tal manera que el acceso a dicha parte protegida del servidor se da sin petición de identificación o autenticación explícita si dicho usuario se ha identificado o autenticado durante su desplazamiento por dicha parte de acceso libre mediante dicho comparador.

20. Servidor según la reivindicación 19, en el que se pide al usuario que permita leer varias veces sus huellas dactilares cuando quiere llegar desde dicha parte de acceso libre hasta dicha parte protegida y no se ha identificado o autenticado previamente.

21. Servidor (4) según una de las reivindicaciones 19 a 20, con una base de datos de referencia para el almacenamiento de dichas huellas dactilares de referencia.

22. Producto de programa que puede cargarse directamente en una zona de memoria con un programa que realiza el procedimiento según una de las reivindicaciones 1 a 18, cuando se ejecuta en un procesador.

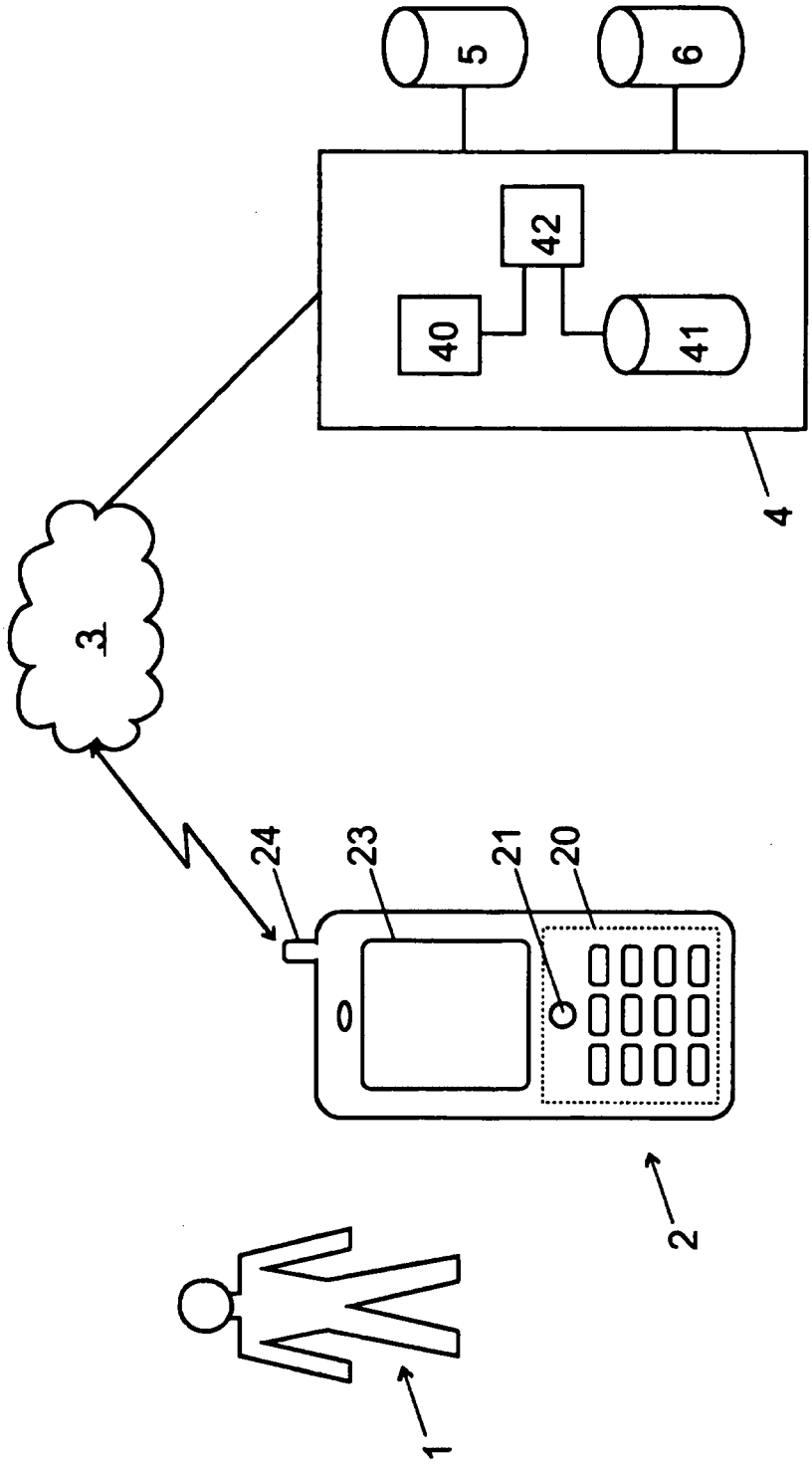

Fig. 1