(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 373 489**

(51) Int. CI.:
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08164499 .9**
(96) Fecha de presentación: **17.09.2008**
(97) Número de publicación de la solicitud: **2166697**
(97) Fecha de publicación de la solicitud: **24.03.2010**

(54) Título: **PROCEDIMIENTO Y SISTEMA PARA AUTENTICAR A UN USUARIO MEDIANTE UN DISPOSITIVO MÓVIL.**

(45) Fecha de publicación de la mención BOPI:
06.02.2012

(45) Fecha de la publicación del folleto de la patente:
06.02.2012

(73) Titular/es:
GMV SOLUCIONES GLOBALES INTERNET S.A.
C/ ISAAC NEWTON 11 PTM
28760 TRES CANTOS (MADRID), ES

(72) Inventor/es:
León Cobos, Juan Jesús y
Celis De La Hoz, Pedro

(74) Agente: **Carpintero López, Mario**

DESCRIPCIÓN

Procedimiento y sistema para autenticar a un usuario mediante un dispositivo móvil

Campo de la invención

La presente invención se refiere a mecanismos de autenticación y, más específicamente, se refiere a un mecanismo de autenticación que usa un dispositivo móvil.

Antecedentes de la invención

La Publicación 200 del FIPS (Estándar Federal de Procesamiento de Información) define la Autenticación como la "verificación de la identidad de un usuario, proceso o dispositivo, a menudo como requisito previo para permitir el acceso a recursos en un sistema de información". La entidad a identificar y verificar positivamente se llama usualmente un "Principal" en la literatura, aunque esta convención se simplificará y se usará el término "usuario" a lo largo del texto. El sistema a cargo de verificar la identidad se llama usualmente el "sistema de autenticación". El ordenador que se usa para acceder al sistema de autenticación se llama el "ordenador cliente".

La autenticación ha impuesto tradicionalmente grandes desafíos a la ciencia informática y a las industrias de seguridad, y se ha propuesto un buen número de mecanismos para garantizar la autenticación eficiente y segura. Entre los riesgos relevantes relacionados con la autenticación de usuarios, los más obvios son los dos siguientes:

- El riesgo primero y obvio es el acceso no autorizado. Si el procedimiento usado para la autenticación es vulnerable al ataque, una persona no autorizada podría obtener acceso fraudulento a un sistema fingiendo ser un usuario distinto. Por lo tanto, es importante que el procedimiento de autenticación sea fiable, en el sentido de que haga extremadamente difícil para un atacante fingir ser algún otro.

- Un riesgo adicional es el robo de identidades. Si el procedimiento usado para la autenticación establece la identidad del usuario por medio de algunas credenciales (usualmente alguna información en forma de claves o contraseñas en el contexto de un sistema criptográfico), entonces la seguridad de estas credenciales es crucial para la seguridad del sistema. A menudo se da el caso de que un usuario se autentica en distintos sistemas usando las mismas credenciales. En el caso de que un sistema de autenticación sea vulnerable, o de que el usuario sea llevado a autenticarse ante un sistema malicioso, las credenciales podrían quedar expuestas y ser robadas, comprometiendo, por lo tanto, la seguridad de todos los otros sistemas de autenticación. El robo de identidades, por lo tanto, es un riesgo más general, en el sentido de que permite el acceso no autorizado a sistemas incluso si el procedimiento de autenticación es fiable y no tiene una vulnerabilidad conocida.

Desde la invención del mecanismo sencillo y bien conocido de usuario-contraseña, se han propuesto varias técnicas, hasta el momento, para aumentar la fiabilidad de los procedimientos de autenticación:

- La autenticación fuerte está definida por el Glosario Nacional de Garantía de la Información del gobierno estadounidense como un enfoque de autenticación por capas, que se apoya en dos o más autenticadores para establecer la identidad. Esto también se llama autenticación de dos factores, ya que implica a dos autenticadores tales como, por ejemplo, algo que Ud. sabe, digamos una contraseña, y algo que Ud. tiene, digamos una prenda.

- La mayoría de las soluciones emplean la criptografía para garantizar que las credenciales puedan verificarse sin comprometer su seguridad (p. ej., usando Criptografía de Clave Pública o generadores de Contraseñas Únicas). Esencialmente, la autenticación se apoya en un secreto que no se intercambia en el protocolo de autenticación. Por ejemplo, en lugar de proporcionar una contraseña, el usuario calcula una respuesta a un desafío, usando la contraseña, y comunica la respuesta, y nunca la contraseña.

- Otra técnica recientemente propuesta, llamada autenticación de dos canales, mejora la seguridad usando dos trayectos distintos de comunicación (por ejemplo, un banco puede llamar por teléfono a un usuario para verificar el acceso). El primer canal es el canal desde el ordenador cliente al sistema de autenticación, y el segundo canal es, en este caso, la línea telefónica.

Las técnicas mencionadas anteriormente mitigan los riesgos existentes, pero son incapaces de afrontar de manera eficiente las amenazas más recientes, tales como los ataques del Hombre-En-El-Medio o de Troyanos (véase, por ejemplo, las Comunicaciones de la ACM, Vol. 48, nº 4, abril de 2005, Riesgos Internos 178 por Bruce Schneier). Esto da como resultado, entre otros, un aumento de transacciones fraudulentas en la banca en línea o el acceso de usuarios remotos no autorizados a sistemas empresariales.

Esta situación se explica porque el escenario actual de autenticación ha evolucionado en los años recientes, y ahora está caracterizado por dos hechos nuevos:

- Los sistemas de autenticación no son seguros. Más aún, algunos sistemas de autenticación podrían ser de naturaleza maliciosa. Por lo tanto, toda la información que se almacena en estos sistemas podría ser mal usada, y todos los sistemas de autenticación deben considerarse como no fiables.

- La evolución del software malicioso (como los Troyanos) y la proliferación del acceso a Internet ha dejado asimismo inseguros a nuestros ordenadores clientes. Por ejemplo, nuestro ordenador personal doméstico, que usamos para acceder a la banca en línea, no puede ser de fiar, ya que la presencia de Troyanos está haciéndose más común cada día. El Troyano reconocerá el proceso de autenticación del usuario y bien capturará las credenciales del usuario, o bien suplantará al usuario para realizar transacciones fraudulentas. Por lo tanto, nuestro ordenador cliente también debe considerarse como no fiable.

Como resultado de ello, surge la necesidad de un procedimiento de autenticación que no sólo brinde una autenticación fuerte y no requiera intercambio de secretos, sino que también considere como no fiables tanto al sistema de autenticación como al ordenador cliente. Específicamente, se requiere un procedimiento de autenticación que goce de las siguientes características:

- No almacena ninguna información de autenticación en absoluto en el sistema de autenticación.

- No interactúa con el ordenador cliente durante el proceso de autenticación.

Las siguientes tecnologías previas son relevantes para la presente invención y, por lo tanto, se introducen a continuación para mayor comodidad:

Un esquema de Cifrado Basado en Identidad (IBE) es un esquema de cifrado público de clave en el cual la clave pública de un usuario es alguna información única y pública acerca de la identidad del usuario. Esta clave pública puede ser una cadena arbitraria, y permite a cualquiera generar una clave pública a partir de un valor de identidad conocido, tal como una cadena en código ASCII. Un tercero fiable, llamado el Generador de Clave Privada (PKG), genera las correspondientes claves privadas. Para funcionar, el PKG genera primero una clave pública maestra, y retiene la correspondiente clave privada maestra (denominada clave maestra). Dada la clave pública maestra, cualquiera puede calcular una clave pública correspondiente al Identificador de identidad, combinando la clave pública maestra con el valor de identidad. Para obtener una correspondiente clave privada, la parte autorizada para usar el Identificador de identidad se pone en contacto con el PKG, que usa la clave privada maestra para generar la clave privada para el Identificador de identidad. Este esquema, en particular, permite la creación de firmas digitales que pueden ser verificadas por cualquiera sin distribución y almacenamiento previos de una clave pública, ya que la clave pública puede generarse a partir de la identidad pública del firmante. El esquema puede implementarse ventajosamente usando la Criptografía de Curva Elíptica y los apareos bilineales, tales como, por ejemplo, el apareo de Weil o el apareo de Tate.

Los códigos de barras bidimensionales son representaciones (imágenes) gráficas de datos en forma de puntos, barras u otras formas que obedecen a patrones predefinidos. Su definición incluye las reglas que son necesarias para codificar / descodificar datos en / de las imágenes (esto se llama su simbolismo). Estos códigos de barras están diseñados de modo tal que un dispositivo móvil dotado de una cámara pueda capturar fácilmente la imagen y descodificar su contenido.

La tecnología promocional se usa como un término genérico para referirse a todos los procedimientos por los cuales un ordenador servidor puede enviar información a un ordenador cliente sin la solicitud previa del ordenador cliente. Según la arquitectura del sistema que comunica al sistema de autenticación con el ordenador cliente, la promoción se implementará por medio de tecnologías adecuadas, tales como los flujos de http, las aplicaciones promotoras de Java o el sondeo prolongado.

El documento JP-A-2007-193762 revela un sistema de autenticación de usuarios que incluye una parte de cámara y una parte de descodificación de código de barras, para leer información de identificación de terminal y de servicio proveniente de los códigos de barras, y una parte de gestión de información de autenticación que transmite la información de autenticación a un dispositivo servidor. Una parte de procesamiento de autenticación autentica un derecho de uso de servicio en base a la información de autenticación enviada desde un dispositivo de comunicación portátil. Una parte de gestión de resultados de autenticación envía una información de notificación que muestra el permiso, o la prohibición, de la prestación de un servicio al dispositivo terminal para el dispositivo servidor proveedor, en base al resultado de autenticación.

El documento “Un procedimiento y su usabilidad para la autenticación de usuarios, utilizando un lector de códigos matriciales en teléfonos móviles” (TANAKA M. et al., Aplicaciones de Seguridad de la Información (Notas de Conferencias en Ciencia Informática), Springer, Vol. 4298, 28 de agosto de 2006, páginas 225 a 236, ISBN: 978-3-540-71092-9) revela un procedimiento de autenticación de usuarios que usa una prenda de uso único, que es emitido por el proveedor y exhibido como un código matricial en el terminal del usuario, y el usuario lee la información con un lector de códigos matriciales en el teléfono móvil del usuario, y la convierte y transmite al proveedor mediante una red de portador fiable de telefonía móvil.

Sumario de la invención

La invención se refiere a un procedimiento y un sistema para autenticar a un usuario de un dispositivo móvil, según las reivindicaciones 1 y 9, respectivamente. Las realizaciones preferidas del procedimiento y del sistema se definen en las reivindicaciones dependientes.

Un primer aspecto de la presente invención se refiere a un procedimiento para autenticar a un usuario de un dispositivo móvil ante un sistema de autenticación remota que está conectado con al menos un ordenador cliente accesible para dicho usuario, que comprende:

i – leer un código bidimensional exhibido en el ordenador cliente por medio de un lector de códigos bidimensionales proporcionado en dicho dispositivo móvil, en donde al menos una dirección de URL (Localizador Universal de Recurso) del sistema de autenticación y un desafío codificado, generado por el sistema de autenticación, están integrados en dicho código bidimensional;

ii – procesar dicho desafío codificado y calcular una respuesta al desafío usando un secreto personal, siendo dicho secreto personal una cadena de caracteres unívocamente relacionados con un identificador de usuario – Identificador de usuario – de dicho usuario del dispositivo móvil y con un sello temporal;

iii – enviar un mensaje al sistema de autenticación, incluyendo dicho mensaje un vector cuyos elementos son al menos dicho identificador de usuario, dicho desafío y dicha respuesta al desafío;

iv – analizar dichos elementos del vector y determinar que el vector es un vector válido si puede garantizarse que la respuesta al desafío ha sido generada usando el secreto personal del usuario cuyo identificador de usuario está en el vector durante un periodo dado de tiempo y, en caso de que dicho vector sea válido:

v – buscar en una lista de usuarios almacenada en el sistema de autenticación para ver si el identificador de usuario en el vector está en dicha lista de usuarios y, si el identificador de usuario está en la lista de usuarios, se verifica si el desafío en el vector está en una lista de sesiones almacenada en el sistema de autenticación y, si el desafío está en la lista de sesiones, el sistema de autenticación envía unilateralmente una pantalla de bienvenida al ordenador cliente, que corresponde a un número de identificación de sesión en la lista de sesiones donde está el desafío.

Dicho código bidimensional puede ser cualquier representación gráfica de datos que obedece a una forma predeterminada, que pueda ser leída y descodificada con un lector de códigos bidimensionales.

Preferiblemente, el lector de códigos bidimensionales es una cámara.

Dicho secreto personal se almacena preferiblemente en el dispositivo móvil y admite el acceso tras ingresar una contraseña.

La etapa de procesar dicho desafío codificado y de calcular una respuesta comprende preferiblemente:

- solicitar al usuario del dispositivo móvil que ingrese una contraseña a fin de acceder a un secreto personal almacenado en el dispositivo móvil;
- tras ingresar dicha contraseña, extraer dicho secreto personal;
- calcular una respuesta al desafío integrado en el código bidimensional, usando dicho secreto personal.

La respuesta al desafío puede calcularse usando un algoritmo de firma digital según un esquema de Cifrado en Base a Identidad, de modo tal que la validez de dicha firma pueda verificarse posteriormente para cualquier fecha dada y cualquier identificador de usuario dado, usando sólo información públicamente disponible referida a dicho esquema.

Preferiblemente, dicho secreto personal está proporcionado de manera segura por un servidor fiable, que calcula dicho secreto personal usando un secreto maestro y dicho identificador de usuario y dicho sello temporal.

También es posible que el secreto personal se calcule en una secuencia de etapas e intercambios de datos entre el servidor fiable y el dispositivo móvil.

La etapa de analizar los elementos del vector es llevada a cabo por el sistema de autenticación y es realizada usando primitivas criptográficas públicas.

De esta manera, el procedimiento de autenticación de la presente invención ha de usarse para autenticar (es decir, identificar positivamente) a un principal de seguridad, habitualmente – pero no necesariamente – un usuario humano que es el dueño del dispositivo móvil. El principal se autentica ante un sistema basado en ordenadores como, por ejemplo, un servidor de red, un quiosco de autoservicio, un Cajero Automático (ATM), una red remota, etc.

La autenticación se apoya en dos factores, un dispositivo móvil en poder del usuario y un secreto personal sólo accesible mediante una contraseña (o secreto) que el usuario conoce. Ambos son necesarios para la autenticación. Por lo tanto, es un mecanismo de autenticación fuerte. Además, el secreto personal nunca se almacena en ningún sistema de autenticación; sólo se ingresa al dispositivo móvil. Estos son requisitos usuales para un procedimiento de autenticación. Pero, adicionalmente, el procedimiento propuesto tiene dos características diferentes e innovadoras:

- El sistema de autenticación se considera no fiable. En consecuencia, no se almacena ninguna información de autenticación en el sistema de autenticación. Sólo es necesario almacenar el identificador de usuario (p. ej., su nombre, identificador de conexión o información de identidad similar) con fines de autorización. Esencialmente, el sistema de autenticación puede considerarse como totalmente no fiable, sin pérdida de seguridad.

- El usuario accede al sistema de autenticación usando un ordenador cliente local, que también se considera no fiable. Una vez que el usuario se enfrenta a una pantalla de autenticación (o de conexión) visible en un ordenador cliente, el ordenador cliente no participa en el proceso de autenticación (específicamente, el ordenador cliente ni siquiera es tocado por el usuario). La autenticación tiene lugar en otro canal, al que accede el dispositivo móvil, que está completamente desvinculado del ordenador cliente. Después de la autenticación exitosa, es el sistema de autenticación quien envía unilateralmente la página autenticada (o pantalla de bienvenida) al ordenador cliente. Por lo tanto, no es un procedimiento de autenticación de “dos canales”, sino un procedimiento de autenticación de “canales distintos”.

El hecho de que tanto el sistema de autenticación como el ordenador cliente sean considerados como no fiables mitiga en gran medida los riesgos actuales asociados al proceso de autenticación.

Los inconvenientes descritos en la sección anterior se mitigan en gran medida por medio del procedimiento de la presente invención, que:

- proporciona una autenticación fuerte en base a dos factores (dispositivo móvil y contraseña);

- mantiene la seguridad de la contraseña, en particular, la contraseña nunca es intercambiada o almacenada en ningún sistema no fiable;

- no requiere que el sistema de autenticación almacene ninguna información referida al usuario, ya que la respuesta al desafío contiene toda la información necesaria para verificar la identidad del usuario; y

- lleva a cabo todo el proceso de autenticación sin que el usuario interactúe con su ordenador cliente (no fiable). Obsérvese que un posible Troyano en el ordenador cliente no puede saber cuándo se capta una imagen de su pantalla y no puede reconocer la pantalla de bienvenida que se envía unilateralmente desde el sistema de autenticación como una pantalla autenticada.

Además, un rasgo distintivo de la presente invención es que el sistema de autenticación no necesita comunicarse en línea con ningún otro sistema a fin de autenticar al usuario. Por lo tanto, es un sistema autónomo.

Un segundo aspecto de la presente invención se refiere a un sistema para autenticar a un usuario de un dispositivo móvil ante un sistema de autenticación remota que está conectado con al menos un ordenador cliente accesible para dicho usuario, que comprende:

- un lector de códigos bidimensionales en dicho dispositivo móvil, para leer un código bidimensional, en donde al menos una dirección de URL del sistema de autenticación y un desafío codificado, generado por el sistema de autenticación, están integrados en dicho código bidimensional;

- medios de procesamiento en dicho dispositivo móvil, para procesar dicho desafío codificado y calcular una respuesta al desafío, usando un secreto personal; en donde dicho secreto personal es una cadena de caracteres unívocamente referidos a un identificador de usuario (Identificador de usuario) de dicho usuario del dispositivo móvil, y a un sello temporal;

- medios de comunicación entre dicho dispositivo móvil y el sistema de autenticación, configurados para, tras calcular dicha respuesta, enviar un mensaje al sistema de autenticación, incluyendo dicho mensaje un vector cuyos elementos son al menos dicho identificador de usuario, dicho desafío y dicha respuesta al desafío;

- medios de procesamiento en el sistema de autenticación, configurados para analizar dichos elementos del vector y determinar el vector como un vector válido cuando la respuesta al desafío ha sido generada usando el secreto personal del usuario cuyo identificador de usuario está en el vector durante un periodo de tiempo dado y, en caso de que dicho vector sea válido, los medios de procesamiento están configurados para:

- comprobar, en una lista de usuarios almacenada en el sistema de autenticación, si el identificador de usuario en el

vector está en dicha lista de usuario y, si el identificador de usuario está en la lista de usuarios, los medios de procesamiento están configurados para:

- verificar si el desafío en el vector está en una lista de sesiones almacenada en el sistema de autenticación y, si el desafío está en la lista de sesiones:
- el sistema de autenticación está configurado para enviar unilateralmente una pantalla de bienvenida al ordenador cliente que corresponde a un número de identificación de sesión en la lista de sesiones donde está el desafío.

Las ventajas de la invención propuesta devendrán evidentes en la siguiente descripción.

Breve descripción de los dibujos

Para completar la descripción y a fin de proporcionar una mejor comprensión de la invención, se proporciona un dibujo. El dibujo forma parte integral de la descripción e ilustra las realizaciones preferidas de la invención, que no deberían interpretarse como restrictivas del alcance de la invención, sino sólo como un ejemplo de cómo puede realizarse la invención.

El dibujo comprende la Figura 1, que muestra un esquema de autenticación según una realización preferida de la invención.

Descripción detallada de las realizaciones preferidas

El procedimiento de autenticación de la presente invención funciona sobre una arquitectura de autenticación específica, que se muestra en la figura 1. Los elementos de esta arquitectura son los siguientes:

- DISPOSITIVO MÓVIL 10: El primer elemento es un dispositivo móvil que alberga una aplicación móvil (que se describirá en detalle más adelante). El dispositivo móvil proporciona cuatro características distintas:

  a. Capacidad de almacenamiento seguro.

  b. Capacidad de comunicaciones seguras con un Servidor Fiable 20 (este servidor también se describe adicionalmente más adelante).

  c. Capacidad de comunicación inalámbrica con un sistema 30 de autenticación (también descrito adicionalmente más adelante). Esta capacidad de comunicación estará habitualmente disponible mediante Internet inalámbrico, y el canal de comunicación referido no necesita estar asegurado.

  d. Una cámara integrada a la que puede accederse desde la aplicación móvil.

Cada dispositivo móvil en la arquitectura está directa y unívocamente asociado a un usuario que será autenticado. Este usuario, a su vez, está asociado a un nombre de usuario o 'Identificador de usuario" que es público y reconocible por parte del sistema de autenticación. Este 'Identificador de usuario' podría, por ejemplo, ser el nombre del usuario, la dirección de correo electrónico del usuario o un identificador móvil del usuario (IMEI, IMSI, MSISDN). Sólo necesita ser único y público.

La capacidad de almacenamiento seguro se usa para almacenar en el dispositivo móvil un denominado secreto personal. El hecho de que el almacenamiento sea seguro significa que se requiere una contraseña para extraer este secreto por parte de cualquier aplicación móvil, y sin esta contraseña es informáticamente inviable extraer este secreto.

- APLICACIÓN MÓVIL: una aplicación móvil se ejecuta dentro del dispositivo móvil. Esta aplicación podría estar integrada en el dispositivo móvil o podría cargarse desde un servidor. La aplicación tiene tres funciones básicas:

  1. Capturar una imagen que contiene un código de barras bidimensional (también llamado etiqueta visual) y descodificar su contenido. La captura se realiza accediendo a la cámara del dispositivo. La imagen se descodifica para obtener el contenido del código de barras. El contenido es una cadena de caracteres que incluye dos elementos de información: un URL y un desafío codificado.

  2. Procesar el desafío codificado y calcular una respuesta válida. El desafío toma la forma usual de una cadena de caracteres que contiene un número muy grande. A fin de calcular la respuesta, se solicita al usuario una contraseña que el dispositivo móvil usa para acceder a, y descifrar, un secreto personal almacenado de forma segura. Este secreto personal, a su vez, es usado por la aplicación móvil para calcular una firma digital breve del desafío, y esta firma constituye la respuesta. La firma se calcula según un esquema de Cifrado Basado en Identidad (IBE). El cálculo de la firma se realiza usando primitivas criptográficas del IBE que garantizan que es informáticamente inviable calcular una respuesta válida a cualquier desafío dado coherente con un Identificador de usuario dado, sin el conocimiento del secreto personal vinculado con ese Identificador de usuario. El secreto personal fue calculado por el PKG del IBE a partir de un valor de identidad obtenido a partir del Identificador de usuario y de una fecha (preferiblemente, la fecha

actual), por lo que cualquiera que conozca este Identificador de usuario y la fecha es capaz de verificar la validez de la firma sin información adicional (que no sea la información pública que define el esquema del IBE). El secreto se almacena de forma segura en el dispositivo móvil, y el acceso al secreto está protegido por la contraseña mencionada, sin la cual es informáticamente inviable su extracción.

3. Enviar un mensaje al servidor 31 en el sistema de autenticación mediante el canal inalámbrico, habitualmente mediante Internet. La dirección del servidor de autenticación está contenida en el URL que se incluyó en la imagen capturada. El mensaje que se envió es, específicamente, un vector 100 que incluye tres valores (es decir, elementos de información):

a. El Identificador de usuario

b. El desafío

c. La respuesta

- SERVIDOR FIABLE 20: el fin del Servidor Fiable es gestionar la creación y distribución de secretos personales a los usuarios (a sus dispositivos móviles).

El servidor fiable debe proporcionar un canal integrado de comunicación segura a todos los dispositivos móviles. En este contexto, seguro significa cifrado y autenticado. La existencia y seguridad de este canal de comunicación se dan por sentadas. Por otra parte, este canal no necesita estar permanentemente activo; se usará sólo en la fase de distribución secreta (véase más adelante).

El Servidor Fiable almacena de manera segura (o bien tiene acceso seguro de otro modo a) un denominado Secreto Maestro. A este Secreto Maestro se accede por un programa de software llamado el software de cálculo de secretos.

- SOFTWARE DE CÁLCULO DE SECRETOS: es un programa de software que se ejecuta en el Servidor Fiable. Este programa recibe como entrada un Identificador de usuario y una fecha (preferiblemente, la fecha actual) y, usando el Secreto Maestro, calcula un secreto personal válido para ese usuario y un periodo específico de tiempo (por ejemplo, el día que corresponde a esa fecha específica) según primitivas criptográficas del IBE. Además, el componente es capaz de enviar este secreto personal a la aplicación móvil que se ejecuta en el dispositivo que pertenece a ese usuario específico, usando el canal integrado de comunicación segura del Servidor Fiable al dispositivo. El Software de Cálculo de Secretos asume el papel del PKG del IBE.

También es posible que el secreto personal se calcule en una secuencia de etapas e intercambios de datos entre el Servidor Fiable y la aplicación móvil. En este caso más general, el secreto personal se calcula de tal modo de manera distribuida entre el componente de cálculo de secretos y la aplicación móvil.

En cualquier caso, siempre valen dos condiciones:

1. El secreto personal de un usuario está unívocamente vinculado al Identificador de usuario y a una fecha específica, en el sentido de que, para un Secreto Maestro dado, un secreto personal sólo puede corresponder a un Identificador de usuario y a una fecha.

2. El secreto personal no puede calcularse fiablemente sin el Secreto Maestro

- ORDENADOR CLIENTE 40: este puede ser un ordenador personal, un quiosco, un cajero automático, etc., que esté físicamente situado donde está el usuario. El ordenador cliente comprende una pantalla, capaz de presentar una interfaz gráfica de usuario, y esta pantalla es visible por el usuario, de modo tal que el usuario pueda tomar fácilmente una fotografía de la pantalla usando la cámara que está integrada en su dispositivo móvil. Cuando el usuario quiere autenticarse a sí mismo, se pone frente al ordenador cliente.

- SISTEMA 30 DE AUTENTICACIÓN: está a cargo de autenticar efectivamente a los usuarios. Este sistema se implementará efectivamente como un servidor 31 de autenticación, o una red de servidores u ordenadores, actuando de forma coordinada. Incluso podría ser el mismo ordenador cliente. En el caso de que el sistema esté físicamente separado del ordenador cliente, debe tener acceso a un enlace de comunicación (posiblemente no fiable) con uno o más ordenadores clientes (usualmente Internet 41, o bien puede ser la red interna de alguna compañía).

Este sistema de autenticación realiza las siguientes cuatro funciones:

a. Sirve las denominadas “páginas de conexión” (o “pantallas de conexión”). Esto significa que el sistema de autenticación es capaz de generar y enviar al ordenador cliente una interfaz gráfica que posea las siguientes propiedades:

i. Incluye un código de barras bidimensional que integra el URL del sistema de autenticación y un desafío aleatorio seguro con un número dado de bits.

ii. Rastrea los ordenadores clientes donde está sirviendo páginas de conexión, por medio del desafío que ha enviado, usando este desafío como un número de identificación de sesión. El sistema almacena el número de identificación de sesión en una lista de sesiones. De esta manera, el sistema sabe qué ordenador cliente corresponde a cada desafío que ha generado. El número de identificación de sesión para cualquier ordenador cliente es idéntico al último desafío enviado a ese ordenador cliente integrado en la página o pantalla de conexión.

iii. En cualquier momento dado, si el ordenador cliente solicita otra página de conexión, se genera un nuevo desafío aleatorio, se sirve la página de conexión y se actualiza la lista de sesiones con el nuevo desafío (es decir, el nuevo número de identificación de sesión), dejando como inválido el anterior.

En el caso específico de que el ordenador cliente sea un ordenador personal que alberga un explorador de Internet, entonces esta función es una función del servidor de red, y la interfaz servida toma la forma de una página de HTML que incluye una imagen integrada con el código de barras bidimensional.

b. Permanece a la escucha de, y recibe, vectores que son enviados por dispositivos móviles por sus canales de comunicación inalámbrica. Habitualmente, el canal inalámbrico será un acceso inalámbrico a Internet y, en este caso, el sistema recibe los vectores por Internet.

c. Procesa vectores. El procesamiento de vectores se define como el análisis de los tres elementos de cada vector {Identificador de usuario, desafío y respuesta} y la devolución de una Aceptación o Rechazo. El proceso tomará como entrada los tres valores en el vector y una, o posiblemente más, fecha(s) de entrada (habitualmente sólo una fecha, la fecha actual). El proceso devolverá una Aceptación toda vez que el vector sea un vector válido, y devolverá un Rechazo en cualquier otro caso. Un vector válido se define como un vector donde se garantiza que la respuesta al desafío se genera usando el secreto personal que corresponde al usuario cuyo Identificador de usuario está en el vector, para cualquiera de los periodos vinculados con las fechas de entrada. La función de procesamiento de vectores se lleva a cabo usando primitivas criptográficas públicas que se suponen pasibles de conocimiento por cualquiera. Esta función es realizada por un programa de software que no incluye (ni accede a) ningún secreto.

d. Envía unilateralmente “páginas de bienvenida” (o “pantallas de bienvenida”). Una página de bienvenida se define como la primera página (o pantalla) que cada usuario ve en el ordenador cliente después de que se ha autenticado con éxito. A partir de esta página, el usuario podrá acceder al sistema según sus roles autorizados. Esto significa que el sistema tiene la capacidad de identificar, para cualquier desafío dado, el ordenador cliente donde sirvió la página de conexión que incluía ese desafío, y de enviar a continuación (por su propia iniciativa) la página de bienvenida de una sesión autenticada a ese ordenador cliente específico. En el caso específico de que el ordenador cliente sea un ordenador personal que alberga un explorador de Internet, la capacidad de envío unilateral consiste en la capacidad de enviar unilateralmente una página de HTML a este explorador.

Estas cuatro funciones se implementan por medio de un cierto número de programas de ordenador distribuidos y coordinados.

Además, el sistema de autenticación almacena una lista 300 de usuarios. Esta lista contiene los Identificadores de usuario de todos los usuarios que están autorizados a acceder al sistema y, posiblemente, otra información adicional que el sistema podría usar para personalizar la página de bienvenida de cada usuario.

Si el sistema con el cual el usuario se autentica requiere que se lleve a cabo cualquier otra función para la autenticación (por ejemplo, almacenar alguna información en un directorio, iniciar algún proceso de auditoría, etc.), entonces esta función también es llevada a cabo por el sistema de autenticación.

Ninguna de las funciones anteriormente descritas del sistema de autenticación requiere el acceso a ningún otro sistema externo, es decir, sólo las funciones anteriormente descritas son requeridas para la autenticación.

El procedimiento de autenticación de la presente invención puede funcionar usando cualquier tipo de código de barras bidimensional que esté diseñado de modo tal que la lectura y la descodificación sean factibles y eficientes usando la cámara y la potencia informática disponible en un dispositivo móvil. Ejemplos de estos tipos son Datamatrix, el código QR o Semacode.

El procedimiento de autenticación de la presente invención consiste en tres fases:

- CONFIGURACIÓN: durante esta fase de Configuración, se genera el Secreto Maestro y todos los componentes descritos anteriormente se instalan y se inician todas las aplicaciones. Esto se hace sólo una vez.

- DISTRIBUCIÓN DE SECRETOS: el fin de la fase de distribución de Secretos es calcular y distribuir todos los secretos

personales a cada dispositivo móvil del usuario. Esta fase se ejecuta periódicamente (por ejemplo, una vez por día). El secreto personal que se distribuye se calcula usando la fecha actual del sistema del Servidor Fiable y se define como válido para un periodo de tiempo cuya duración coincide con el periodo del cálculo de secretos. Por ejemplo, si esta fase se ejecuta una vez por día, entonces todos los secretos personales son válidos por un día; si esta fase se ejecuta una vez por semana, entonces todos los secretos personales son válidos por una semana.

- AUTENTICACIÓN: la fase de Autenticación es la autenticación efectiva del usuario ante el sistema de autenticación. Esta fase es un proceso que tiene lugar en las siguientes etapas:

  1) El usuario accede al ordenador cliente y solicita una pantalla de conexión;

  2) El sistema de autenticación sirve una pantalla de conexión que incluye un código de barras bidimensional.

  3) El usuario inicia la aplicación móvil en su dispositivo móvil.

  4) El usuario usa la aplicación móvil para tomar una imagen del código de barras bidimensional en la pantalla del ordenador cliente.

  5) La aplicación móvil solicita al usuario una contraseña a fin de acceder al secreto personal almacenado en el dispositivo.

  6) El usuario ingresa la contraseña y la aplicación móvil extrae el secreto personal.

  7) La aplicación móvil calcula la respuesta que corresponde al desafío integrado en el código de barras, usando el secreto personal.

  8) La aplicación móvil envía, mediante comunicación inalámbrica, el vector {Identificador de usuario, desafío, respuesta} al URL que estaba integrado en el código de barras.

  9) El sistema de autenticación recibe el vector.

  10) El sistema de autenticación procesa el vector.

  11) Si se devuelve un Rechazo, el vector no es válido y al proceso de autenticación falla y termina.

  12) Si se devuelve una Aceptación, el vector es válido y el usuario está autenticado, lo que significa que el sistema de autenticación se fía de que el vector proviene del usuario que corresponde al Identificador de usuario. Sin embargo, a fin de proporcionar acceso al usuario, el proceso aún tiene que avanzar más, según lo siguiente.

  13) El sistema de autenticación busca en su lista de usuarios para ver si el Identificador de usuario que llega en el vector está en la lista.

  14) Si el Identificador de usuario no está en la lista, se supone que el usuario no está autorizado para acceder, el proceso falla y termina.

  15) Si el Identificador de usuario está en la lista, el sistema de autenticación busca el desafío en el vector en la lista de sesiones. Si el desafío que llegó con el vector no está en la lista de sesiones, el proceso falla y termina.

  16) Si el desafío está en la lista de sesiones, el sistema de autenticación envía unilateralmente la pantalla de bienvenida al ordenador cliente que corresponde al número de identificación de sesión (posiblemente una pantalla de bienvenida personalizada para el Identificador de usuario). El proceso ha acabado con éxito.

La tecnología promocional se usa porque en el mecanismo descrito la iniciativa para reemplazar la pantalla de conexión por una pantalla autenticada (y la sesión inicial por una sesión autenticada) proviene del sistema de autenticación, y no del ordenador cliente. En una típica arquitectura de cliente-servidor, esto sólo requiere una implementación específica de software. En una arquitectura basada en la Red, es necesario usar un mecanismo específico de envío unilateral. Este mecanismo se implementará usualmente por medio de tecnologías adecuadas, tales como el flujo de http, las aplicaciones promotoras de Java o el sondeo prolongado.

Según la realización preferida, el sistema de autenticación usa un canal de comunicación regular para enviar al ordenador cliente una pantalla de conexión. Esta pantalla contiene un código de barras bidimensional que contiene información sobre el URL del sistema de autenticación y, lo que es sumamente notable, un desafío aleatorio (un número aleatorio usado sólo una vez, o “ninguna vez”) generado por el sistema de autenticación. El usuario, que preferiblemente se coloca frente al ordenador cliente, no necesita usar el teclado o ratón del ordenador cliente, sino que sólo necesita capturar la imagen con la cámara incluida en su dispositivo móvil y descodificar el URL y el desafío. El usuario ingresa entonces una contraseña en el dispositivo móvil y, como consecuencia, se calcula una respuesta a este desafío. Esta respuesta no puede ser

calculada por ningún otro dispositivo que no sea el del usuario, y no puede calcularse sin la contraseña del usuario. Una vez calculada, la respuesta se envía, junto con la identidad del usuario, al URL del sistema de autenticación, mediante un canal establecido ad hoc desde el dispositivo móvil. El sistema de autenticación es capaz de comprobar que la respuesta al desafío aleatorio proviene necesariamente del usuario antes de verificar su identidad. A fin de cerrar el ciclo, el sistema de autenticación finalmente envía unilateralmente al ordenador cliente (identificado por el desafío aleatorio) una pantalla de “bienvenida” autenticada, para permitir que el usuario continúe su interacción con el sistema por medio del ordenador cliente.

El procedimiento de autenticación, según lo anteriormente descrito, proporciona una autenticación fuerte, en el sentido de que las contraseñas, u otras credenciales, no se intercambian nunca entre el usuario y el sistema de autenticación. Por otra parte, el sistema de autenticación no necesita almacenar ninguna información relacionada con el usuario en absoluto con fines de autenticación, aunque se le requiere almacenar los Identificadores de usuarios con fines de autorización.

La invención, obviamente, no está limitada a las realizaciones específicas descritas en el presente documento, sino que también abarca todas las variaciones que puedan ser consideradas por cualquier persona experta en la técnica (por ejemplo, en lo que respecta a la elección de componentes, configuración, etc.), dentro del alcance general de la invención, según lo definido en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Procedimiento para autenticar a un usuario de un dispositivo móvil (10) ante un sistema (30) de autenticación remota, que está conectado con al menos un ordenador cliente accesible para dicho usuario, que comprende:

i – leer un código bidimensional exhibido en el ordenador cliente (40) por medio de un lector de códigos bidimensionales proporcionado en dicho dispositivo móvil, en donde al menos una dirección de URL del sistema de autenticación, y un desafío codificado, generado por el sistema de autenticación, están integrados en dicho código bidimensional;

ii – procesar dicho desafío codificado y calcular una respuesta al desafío, usando un secreto personal, siendo dicho secreto personal una cadena de caracteres unívocamente vinculados con un identificador de usuario, Identificador de usuario, de dicho usuario del dispositivo móvil, y con un sello temporal;

iii – enviar un mensaje al sistema de autenticación, incluyendo dicho mensaje un vector (100), cuyos elementos son al menos dicho identificador de usuario, dicho desafío y dicha respuesta al desafío;

iv – analizar dichos elementos del vector y determinar que el vector es un vector válido, cuando la respuesta al desafío ha sido generada usando el secreto personal del usuario cuyo identificador de usuario está en el vector durante un periodo de tiempo dado y, en caso de que dicho vector sea válido:

v – buscar en una lista (300) de usuarios almacenada en el sistema de autenticación, para ver si el identificador de usuario en el vector está en dicha lista de usuarios y, si el identificador de usuario está en la lista de usuarios, verificar si el desafío en el vector está en una lista de sesiones almacenada en el sistema de autenticación y, si el desafío está en la lista de sesiones, el sistema de autenticación envía unilateralmente una pantalla de bienvenida al ordenador cliente que corresponde a un número de identificación de sesión en la lista de sesiones donde está el desafío.

2. Procedimiento según la reivindicación 1, en el cual dicho secreto personal está almacenado en el dispositivo móvil y se accede a él tras ingresar una contraseña.

3. Procedimiento según cualquiera de las reivindicaciones 1 a 2, en el cual la etapa de procesar dicho desafío codificado y de calcular una respuesta comprende:

- solicitar al usuario del dispositivo móvil que ingrese una contraseña a fin de acceder a un secreto personal almacenado en el dispositivo móvil;

- tras ingresar dicha contraseña, extraer dicho secreto personal;

- calcular una respuesta al desafío integrado en el código bidimensional usando dicho secreto personal.

4. Procedimiento según cualquier reivindicación precedente, en el cual la respuesta al desafío se calcula usando un algoritmo de firma digital según un esquema de Cifrado Basado en Identidad, de modo tal que la validez de dicha firma pueda ser verificada posteriormente para cualquiera fecha dada y cualquier identificador de usuario dado, usando sólo información públicamente disponible vinculada con dicho esquema.

5. Procedimiento según cualquier reivindicación precedente, en el cual dicho secreto personal es proporcionado por un servidor fiable (20), que calcula dicho secreto personal usando un secreto maestro, y dicho identificador de usuario y dicho sello temporal.

6. Procedimiento según cualquier reivindicación precedente, en el cual la etapa de analizar los elementos del vector es llevada a cabo por el sistema de autenticación y realizada usando primitivas criptográficas públicas.

7. Procedimiento según cualquier reivindicación precedente, en el cual dicho lector de códigos bidimensionales es una cámara.

8. Procedimiento según cualquier reivindicación precedente, en el cual dicho código bidimensional es cualquier representación gráfica de datos que obedece a una forma predeterminada, y que puede ser leída y descodificada con un lector de códigos bidimensionales.

9. Sistema para autenticar a un usuario de un dispositivo móvil (10) ante un sistema (30) de autenticación remoto que está conectado con al menos un ordenador cliente accesible para dicho usuario, que comprende:

- un lector de códigos bidimensionales en dicho dispositivo móvil para leer un código bidimensional, en donde al menos una dirección de URL del sistema de autenticación y un desafío codificado, generado por el sistema de autenticación, están integrados en dicho código bidimensional;

- medios de procesamiento en dicho dispositivo móvil para procesar dicho desafío codificado y calcular una respuesta al desafío usando un secreto personal; en donde dicho secreto personal es una cadena de caracteres unívocamente relacionados con un identificador de usuario, Identificador de usuario, de dicho usuario del dispositivo móvil, y con un sello temporal;

- medios de comunicación entre dicho dispositivo móvil y el sistema de autenticación, configurados, tras calcular dicha respuesta, para enviar un mensaje al sistema de autenticación, incluyendo dicho mensaje un vector (100) cuyos elementos son al menos dicho identificador de usuario, dicho desafío y dicha respuesta al desafío;

- medios de procesamiento en el sistema de autenticación, configurados para analizar dichos elementos del vector y determinar si el vector es un vector válido cuando la respuesta al desafío ha sido generada usando el secreto personal del usuario cuyo identificador de usuario está en el vector durante un periodo de tiempo dado y, en caso de que dicho vector sea válido, los medios de procesamiento están configurados para:

- comprobar en una lista de usuarios almacenada en el sistema de autenticación si el identificador de usuario en el vector está en dicha lista de usuarios y, si el identificador de usuario está en la lista de usuarios, los medios de procesamiento están configurados para:

- verificar si el desafío en el vector está en una lista de sesiones almacenada en el sistema de autenticación y, si el desafío está en la lista de sesiones:

- el sistema de autenticación está configurado para enviar unilateralmente una pantalla de bienvenida al ordenador cliente que corresponda a un número de identificación de sesión en la lista de sesiones donde está el desafío.

10. Sistema según la reivindicación 9, en el cual dicho secreto personal se almacena en el dispositivo móvil y se accede a él tras ingresar una contraseña.

11. Sistema según cualquiera de las reivindicaciones 9 a 10, en el cual la respuesta al desafío se calcula usando un algoritmo de firma digital según un esquema de Cifrado Basado en Identidad, de modo tal que la validez de dicha firma pueda ser verificada posteriormente para cualquiera fecha dada y cualquier identificador de usuario dado, usando sólo información públicamente disponible vinculada con dicho esquema.

12. Sistema según cualquiera de las reivindicaciones 9 a 11, en el cual dicho secreto personal está proporcionado por un servidor fiable (20), que está configurado para calcular dicho secreto personal usando un secreto maestro, y dicho identificador de usuario y dicho sello temporal.

13. Sistema según cualquiera de las reivindicaciones 9 a 12, en el cual dicho lector de códigos bidimensionales es una cámara.

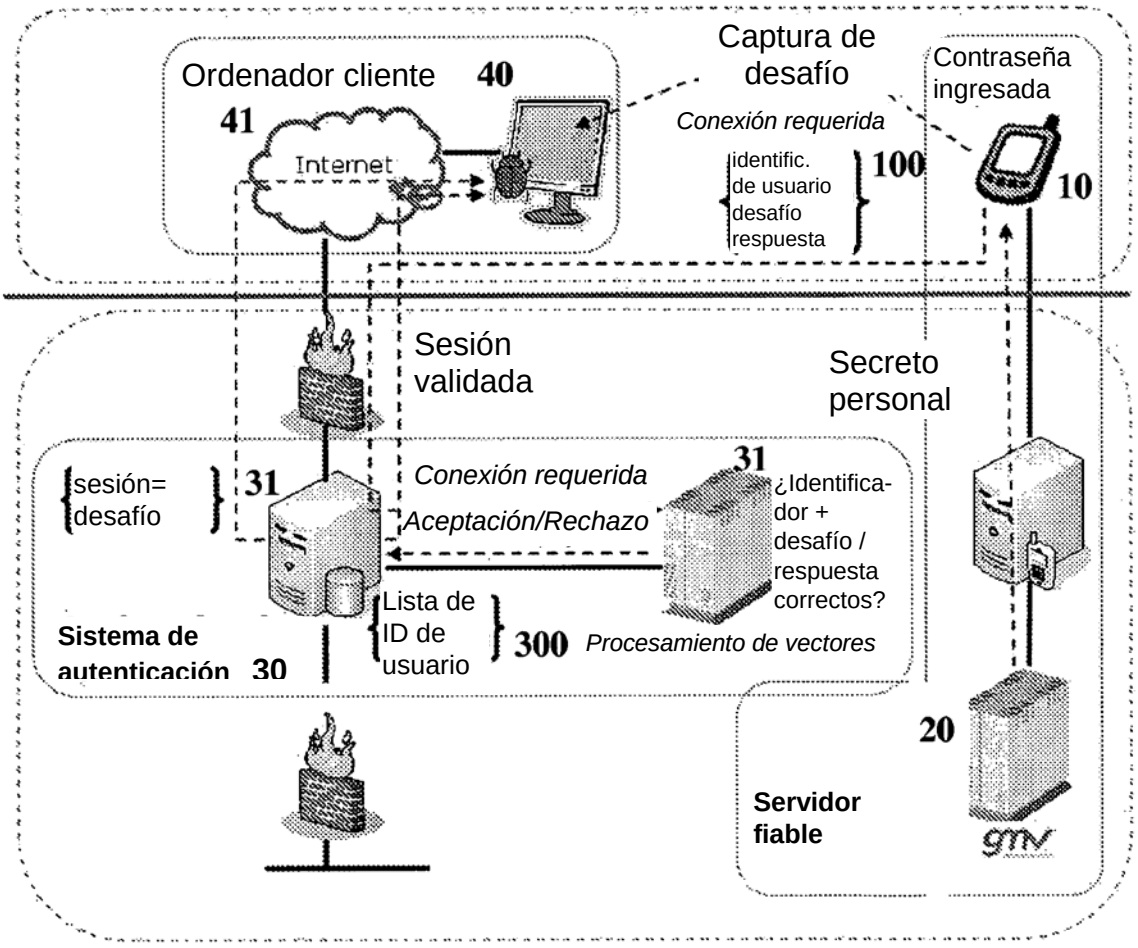
Ordenador cliente 40
41
Internet
Captura de desafío
Conexión requerida
identific. de usuario
desafío
respuesta
100
Contraseña ingresada
10
Sesión validada
Secreto personal
sesión= desafío
31
Conexión requerida
Aceptación/Rechazo
31
¿Identificador + desafío / respuesta correctos?
Lista de ID de usuario
300
Procesamiento de vectores
Sistema de autenticación 30
20
Servidor fiable

FIG. 1