(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 517 865**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **08.03.2006 E 06251242 (1)**

(97) Fecha y número de publicación de la concesión europea: **08.10.2014 EP 1833219**

(54) Título: **Métodos, aparatos y software para usar un testigo para calcular contraseña limitada en tiempo en teléfono celular**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.11.2014

(73) Titular/es:

MONITISE LIMITED (100.0%)
PROFILE WEST 950 GREAT WEST ROAD
BRENTFORD, MIDDLESEX TW8 9EE, GB

(72) Inventor/es:

ATKINSON, STEVEN PAUL

(74) Agente/Representante:

UNGRÍA LÓPEZ, Javier

DESCRIPCIÓN

Métodos, aparatos y software para usar un testigo para calcular contraseña limitada en tiempo en teléfono celular

Campo de la invención

Esta invención se refiere a los mecanismos de control de acceso para servicios accedidos a través de internet. En particular esta invención se refiere a la autenticación y verificación independiente de un cliente o empleado para que obtengan acceso legítimamente a una sección privada o segura de una aplicación de internet u obtengan acceso a una red empresarial.

Antecedentes de la invención

El problema al que se refiere esta invención, se refiere a los métodos actuales para identificación y autorización posterior de un empleado o cliente para acceder legítimamente a una red empresarial o a una sección segura de una aplicación de internet. En este caso el acceso podría iniciarse desde, pero sin limitación, un ordenador personal, asistente digital personal, televisión o consola de juegos conectada a internet. La conexión a internet en este caso podría ser a través de una línea fija, Wi-Fi o conexión de datos celular (por ejemplo GPRS o conexión de red de 3G).

Los mecanismos actuales para autenticación de un individuo incluyen la emisión y uso mediante el individuo de un nombre de usuario y contraseña o la emisión y uso mediante el individuo de un nombre de usuario, PIN y código numérico generado automáticamente desde una tarjeta de testigo. Estos mecanismos para autenticación y verificación tienen un número de serias desventajas que incluyen (1) gestión de los credenciales del usuario por la empresa o el comerciante; (2) el coste asociado con el registro, emisión y mantenimiento continuo de los credenciales; y (3) la capacidad para obtener acceso maliciosamente a unos credenciales en línea del consumidor o usuario.

En el caso de credenciales de autenticación de nombre de usuario y contraseña sencillos, se requiere que un individuo introduzca estos cuando se pidan para identificarle. Estos credenciales normalmente se transmiten electrónicamente a través de un enlace seguro para verificarse y una vez verificados se concede acceso al individuo al recurso; por ejemplo este puede acceder a una red segura o porción segura de una aplicación de internet. Para que este sistema de autenticación opere eficazmente, se requiere que la empresa o el comerciante hagan funcionar los procedimientos de registro, verificación y gestión operacional. Por lo tanto se requiere que un empleado o cliente se registre y elija por sí mismo o se le emita con un nombre de usuario y contraseña únicos. Estos credenciales tienen que almacenarse de manera segura y cuando se requiera compararse con los credenciales introducidos mediante un individuo para autenticarle a sí mismo para acceder a un recurso.

En el caso de credenciales de nombre de usuario, PIN y tarjeta de testigo, un individuo introduce su nombre de usuario, PIN y valor numérico actual desde la tarjeta de testigo cuando se pida. Estos credenciales se transmiten normalmente a través de un enlace seguro y se verifican mediante sistemas empleados mediante el empleado o el comerciante. En este caso, la verificación incluye verificación basada en algoritmo para asegurar que el nombre de usuario, PIN y testigo numérico generado son válidos. Si se probó que estos credenciales son correctos a continuación se permite acceso al empleado o cliente a la aplicación de internet o a la red empresarial. Puede observarse que el uso de una tarjeta de testigo mejora significativamente la fortaleza de los credenciales de autenticación puesto que la tarjeta de testigo genera matemáticamente una serie de códigos limitados en tiempo de uso único y como tal se requiere que el empleado o cliente tenga la tarjeta de testigo en su posesión cuando se autentiquen a sí mismos. Por supuesto, esto requiere la emisión de tarjetas de testigo, con costes consiguientes, y también la inconveniencia para el usuario.

La gestión y control de credenciales de autenticación requiere que las empresas y comerciantes empleen una amplia variedad de servicios. Estos servicios incluyen procesos de registro, suministro seguro, verificación y control en el caso de usuarios que pierden u olvidan sus credenciales personales. A medida que el número de hogares conectados a internet aumenta y el número de servicios de internet aumenta se deduce que los costes de operación asociados a empresas y comerciantes aumentará.

Junto con los costes de operación asociados con gestionar y controlar credenciales de usuario existe un problema grave con la seguridad inherente de los dispositivos conectados a internet. Es bien entendido por la industria de la tecnología de la información que el entorno informático personal es propenso a ataques maliciosos y este problema está aumentando a medida que el número de hogares conectados a internet aumenta. La Asociación de Servicios de Pago y Compensación (APACS) ha identificado un número de métodos usados mediante estafadores que afecta gravemente la seguridad de recursos en línea que usan un nombre de usuario y contraseña sencillos. Estos métodos incluyen ataques de suplantación de identidad (Phising) y ataques de caballos de Troya. El fin de ambos de estos tipos de ataque es obtener acceso a credenciales de un cliente o usuarios de internet posibilitando, por lo tanto, la capacidad para un estafador de asumir la identidad del cliente o usuario. Un ataque de suplantación de identidad (phising) toma normalmente la forma de un mecanismo de comunicación electrónica tal como correo electrónico que pide al cliente o usuario suministrar sus credenciales de internet mediante un correo electrónico que

pretende ser desde la empresa o el comerciante. Un ataque de caballo de Troya está diseñado para recoger información de pulsación de teclas a medida que el cliente o usuario introduce sus credenciales y transfiere automáticamente estos al estafador. Una vez que se ha obtenido el nombre de usuario y contraseña simplemente posibilita a un tercero asumir la identidad del cliente o usuario para obtener acceso al recurso de internet o empresarial específico.

La invención tiene por objeto proporcionar un mecanismo de acceso de servicio alternativo que reduce algunos de estos problemas.

La Patente de Estados Unidos Número US 6.928.558 B1 presenta un método y disposición para identificar a un usuario en un sistema informático, en el que se implementa una conexión al sistema informático mediante una estación móvil.

Sumario de la invención

De acuerdo con un aspecto de la invención, se proporciona un método para proporcionar acceso a un servicio basado en internet desde un dispositivo de teléfono celular, comprendiendo el método:

usar un testigo para calcular una contraseña limitada en tiempo para un usuario específico que busca acceso al servicio basado en internet desde un dispositivo de teléfono celular;
recibir una contraseña limitada en tiempo a partir de la calculada del usuario usando el testigo; y
verificar la contraseña limitada en tiempo para conceder acceso al servicio basado en internet;
y caracterizado por generar el testigo en un servidor de un proveedor del servicio basado en internet y proporcionar el testigo al dispositivo de telefonía celular de un usuario que busca acceso al servicio basado en internet, y en el que el testigo tiene validez limitada en tiempo,
donde durante la validez del testigo, se posibilita el acceso al servicio basado en internet sin requerir comunicación con el servidor usado para generar el testigo.

Preferentemente se recibe al menos un parámetro de identificación de usuario adicional con la contraseña limitada en tiempo, y donde verificar la contraseña limitada en tiempo y el al menos un parámetro de identificación de usuario adicional se verifica con la contraseña limitada en tiempo para conceder acceso al servicio basado en internet.

Esta invención proporciona a las empresas y comerciantes un mecanismo significativamente más seguro y más comercialmente eficaz que las soluciones existentes. La invención usa un subconjunto de las características de un teléfono celular para proporcionar seguridad adicional. En particular, la invención proporciona un sistema de autenticación de doble factor basado en teléfono celular.

La invención proporciona un mecanismo pragmático, seguro y rentable para empresas y comerciantes de todos los tamaños. Utilizando servicios y dispositivos existentes que los clientes y empleados tienen en su posesión (teléfonos celulares o dispositivos de conectividad celular similares), la invención proporciona una ventaja significativa para abordar tanto los costes de operación asociados como los problemas de seguridad inherentes de los métodos de autenticación existentes comunes. Adicionalmente, la invención proporciona mecanismos para posibilitar la gestión de identidad pragmática adecuada para el aumento del número y sofisticación de los servicios de internet y proporciona un servicio holístico para gestión de autenticación e identidad adecuado para la amplia variedad de servicios que están en existencia hoy en día, así como un fundamento para servicios a medida que la industria de la comunicación y tecnología se adapta rápidamente especialmente como los servicios proporcionados mediante las compañías de comunicación global. Estos servicios pueden incluir una amplia variedad de servicios desde voz hasta servicios de datos y servicios de entretenimiento que se proporcionan mediante las compañías de comunicación.

El cálculo de la contraseña limitada en tiempo puede tener en cuenta el tiempo actual así como un parámetro de identidad del dispositivo de telefonía celular. Por ejemplo, el cálculo puede usar la función:

Contraseña = f(IP *XOR* NT *XOR* t), donde t es una medición del tiempo actual, IP es un parámetro de identidad del dispositivo de telefonía celular y NT es el testigo numérico. La función f puede comprender entonces:
f(x) = RightTrunc(Decimal(SHA(x))), donde RightTrunc es una función para extraer un número de bits más bajo, Decimal es una función para convertir una serie de bytes a un valor entero y SHA es un algoritmo de troceo seguro.

El al menos un parámetro de identificación de usuario adicional puede comprender un nombre de usuario y opcionalmente una contraseña de usuario o número de identificación personal. Por lo tanto, el nombre de usuario y los números de PIN convencionales se complementan mediante una contraseña limitada en tiempo, y una que se genera localmente en respuesta a un testigo (por ejemplo en la forma de un valor de sal).

El testigo puede tener también validez limitada en tiempo, por ejemplo entre 1 hora y 1 semana.

Durante la validez del testigo, el acceso al servicio basado en internet puede posibilitarse sin requerir comunicación con el servidor usado para generar el testigo. Esto aborda los posibles problemas de cobertura de red, y proporciona por lo tanto tanto un servicio de autenticación de red encendida como de red apagada, para posibilitar acceso al servicio. Esto potencia adicionalmente la flexibilidad de la invención al posibilitar la autenticación de un empleado o cliente para acceder a un recurso de web seguro o red de compañía ya sea en o fuera de la cobertura de red de teléfono celular. La validez del testigo puede definirse como una ventana de tiempo, con ventanas de tiempo para testigos secuenciales solapantes. Esto aborda problemas de temporización.

La provisión del testigo al dispositivo de telefonía celular depende preferentemente de la autenticación del dispositivo de telefonía celular, de modo que la autenticación puede denegarse tan pronto como se informa que un dispositivo de telefonía móvil se ha robado o perdido. Por ejemplo, la autenticación puede comprender verificar el al menos un parámetro de identificación de usuario adicional como que está asociado con el dispositivo de telefonía celular específico usando una base de datos de usuarios registrados. El dispositivo de telefonía celular específico puede identificarse usando el MSISDN.

Cuando se proporciona el testigo, se implementa también la sincronización de reloj entre el dispositivo de teléfono celular y el proveedor del servicio basado en internet, y esto proporciona la temporización correcta para la contraseña limitada en tiempo.

La invención proporciona también un programa informático que comprende código para implementar los métodos de la invención cuando se ejecutan en un ordenador.

La invención proporciona también un sistema para proporcionar acceso a un servicio basado en internet a partir de un dispositivo de telefonía celular, comprendiendo el sistema:

un servidor de un proveedor del servicio basado en internet, y que comprende medios para generar un testigo; y
una aplicación de software para instalación en un dispositivo de telefonía celular, posibilitando la aplicación de software el cálculo de una contraseña limitada en tiempo a partir del testigo,
donde el servidor comprende adicionalmente medios para verificar la contraseña limitada en tiempo para posibilitar o prohibir acceso al servicio basado en internet.

Breve descripción de los dibujos

Se describirá ahora un ejemplo de la invención con referencia a la figura adjunta que muestra el sistema de la invención.

Descripción detallada

La invención se describirá con respecto a usar teléfonos móviles celulares como un testigo en un mecanismo de control de acceso de testigo múltiple pero no se pretende que se restrinja la invención en su sentido más amplio a tales dispositivos.

La invención está comprendida de un número de componentes que juntos suministran un mecanismo de autenticación de doble factor seguro para empresas y comerciantes. El servicio proporciona tanto un mecanismo de red apagada como de red encendida para generar una contraseña limitada en tiempo de uso único que se usa junto con otros componentes de autenticación mediante un empleado o cliente para acceder legítimamente a una red empresarial o asegura la aplicación de internet o el servicio de un dispositivo conectado a internet.

En lugar de requerir un nombre de usuario y contraseña sencillos o el PIN de nombre de usuario y testigo para obtener acceso seguro el usuario tiene una aplicación basada en teléfono celular que se usa para generar una contraseña de uso único. La contraseña de uso único es configurable pero puede consistir, por ejemplo, de un código numérico de seis dígitos. El usuario introduce su nombre de usuario denominado, código de paso (si se requiere) y la contraseña de uso único generada. Estos credenciales se transmiten y autentican de manera segura en el servidor de RADIUS de la empresa o de los comerciantes y si la autenticación es satisfactoria se concede el acceso al usuario.

Como se muestra en la figura, el sistema de la invención está comprendido de un número de componentes que incluyen:

Aplicación basada en teléfono celular (en el teléfono 10 celular)
Servidor 20 de autenticación de doble factor (para el proceso de autenticación)
Servidor 30 de administración (para proporcionar servicio al usuario)
Módulo 40 de autenticación conectable

Estos componentes se describen en mayor detalle en las siguientes secciones.

Aplicación basada en teléfono celular

La aplicación basada en teléfono celular se desarrolla usando el lenguaje de programación apropiado para adecuarse al país de despliegue. Esto incluye, pero sin limitación Java, BREW y Symbian. El fin de la aplicación de teléfono celular es generar de manera segura la contraseña de uso único para usarse como parte de los credenciales de autenticación. Para ofrecer el máximo nivel de seguridad y flexibilidad la aplicación de teléfono celular tiene dos modos de operación (1) operación de red encendida; y (2) operación de red apagada.

La operación de red encendida proporciona la funcionalidad para:

- Abrir una conexión segura al servidor de autenticación de doble factor.
- Transmitir el identificador de cliente único, tiempo actual (basándose en el reloj interno del teléfono celular) y la versión de la aplicación celular.
- Recibir desde el servidor de autenticación de doble factor un nuevo valor de sal y tiempo de expiración de sal
- Almacenar el valor de sal y la fecha de expiración de sal de manera segura en el área de almacenamiento de datos interna del teléfono celular.
- Calcular una nueva contraseña de uso único usando el algoritmo de contraseña de uso único descrito a continuación.
- Mostrar la contraseña de uso único en la pantalla del teléfono celular para que el usuario entre en la pantalla de entrada de autenticación del terminal de internet que está usando.

La operación de red apagada proporciona la funcionalidad para:

- Intentar abrir una conexión segura al servidor de autenticación de doble factor.
- Si el intento falla la aplicación celular examina el almacenamiento de datos interno para extraer el valor de sal y la fecha de expiración de sal
- Si existe el valor de sal y la fecha de expiración de sal no ha expirado la aplicación calcula la contraseña de uso único usando el algoritmo descrito a continuación.
- Mostrar la contraseña de uso único en la pantalla de visualización celular para que el usuario entre en la pantalla de entrada de autenticación del terminal de internet que está usando.
- Si la fecha de expiración de sal ha expirado mostrar un mensaje de error que indica que el usuario tiene que moverse a la cobertura de red para re-sincronizar el valor de sal y la fecha de expiración de sal.

Para reducir el riesgo de un ataque de escucha clandestina, la contraseña de uso único no se transmite a la aplicación de teléfono celular sino que se genera en la aplicación de teléfono celular. La generación está basada en un valor de sal aleatorio que se transmite a la aplicación de teléfono celular para usarse en el siguiente algoritmo. Al calcular la contraseña de uso único, la aplicación de teléfono celular usa el siguiente algoritmo:

Contraseña de único uso = RIGHTTRUNC(DECIMAL(SHA1(semilla XOR sal XOR tiempo))))

Donde:

Tiempo = número de minutos desde 1 de enero de 1970 a minuto más cercano (16 bytes)
Semilla = valor aleatorio aprovisionado en el entorno de aplicación de teléfono celular (16 bytes)
Sal = valor aleatorio enviado al cliente durante re-sincronización (16 bytes)
XOR = operación XOR booleana
SHA1 = algoritmo de troceo seguro versión 1.0 digestor
DECIMAL = función para convertir serie de 16 bytes a un valor entero
RICHTTRUNC = función para extraer 6 dígitos más a la derecha (más bajos) de valor

Servidor de autenticación de doble factor

El servidor 20 de autenticación de doble factor está alojado como un servicio gestionado para clientes del servicio de autenticación de doble factor. El servidor de autenticación de doble factor completa un número de funciones requeridas para la ejecución eficaz del servicio incluyendo:

- Proporciona acceso seguro al servidor de autenticación de doble factor
- Gestión y distribución de aplicación de teléfono celular
- Gestión de clientes y opciones de configuración de clientes
- Generación de informes para clientes individuales del servicio
- Funcionalidad de ensayo para funciones en vivo pre-servicio.

Durante la resincronización de la aplicación de teléfono celular, la aplicación se conecta de manera segura al servidor 20 de autenticación de doble factor. La autenticación del teléfono celular está basada en un número de factores incluyendo el número de serie de la aplicación de teléfono celular y el MSIDN del teléfono celular que se conecta y el tiempo del reloj interno del teléfono celular. La aplicación de teléfono celular se verifica contra la base

de datos de usuarios registrados usando el MSISDN y el número de serie de aplicación de cliente. Una vez que se ha verificado el valor de sal y se calcula y transmite de manera segura la fecha de expiración de sal de vuelta a la aplicación de teléfono celular para generar la contraseña de único uso. El servicio empresarial alojado en la localización de los clientes se actualiza también con la información relevante para autenticación posterior, esto incluye el número de serie del teléfono celular, valor de sal y tiempo de sistema recibido desde la aplicación de teléfono celular.

El servidor 20 de autenticación de doble factor gestiona también el aprovisionamiento de un nuevo usuario final del servicio. Una vez ordenado mediante el servicio de administración el servidor de autenticación de doble factor transmitirá un mensaje de Inserción WAP (usando la pasarela 22 de WAP) al usuario relevante y gestionará posteriormente la descarga e instalación de la aplicación de teléfono celular. Durante este proceso se elige la aplicación de teléfono celular más apropiada basándose en los detalles de conexión recibidos a medida que el teléfono celular pide la aplicación. Durante las conexiones posteriores el servidor de autenticación de doble factor actualizará también la aplicación de teléfono celular según sea necesario, por ejemplo si se ha desarrollado una nueva aplicación.

El servidor de autenticación de doble factor posibilita un número de opciones para configurarse por los clientes del servicio. Las opciones de configuración incluyen actualmente la capacidad para especificar los testigos de autenticación requeridos siendo estos el nombre de usuario y contraseña de uso único o el nombre de usuario, PIN y contraseña de único uso. En el caso de requerir un PIN el servidor 20 de autenticación de doble factor gestiona la distribución del PIN mediante SMS al usuario final.

Una variedad de informes están disponibles desde el servidor de autenticación de doble factor. Estos incluyen informes de uso a través de compañías que usan el servicio e informes para uso de compañías individuales que usan el servicio. Los informes se generan en una base ad hoc o se generan a intervalos de tiempo específicos.

Una variedad de herramientas de ensayo están disponibles desde el servidor 20 de autenticación de doble factor incluyendo ensayo de URL, ensayo de SMS y ensayos de generación de contraseña de uso único individuales. Los servicios de ensayo están diseñados para ensayar servicios de compañía individuales como parte del proceso de puesta en servicio para el servicio.

Servidor de administración

El servidor 30 de administración y la consola 32 están diseñados para proporcionar todas las tareas necesarias para administrar el servicio para un cliente. Las tareas de administración disponibles incluyen gestión de usuarios, la activación de procesos de aprovisionamiento para usuarios finales y la emisión o re-emisión de códigos de paso para usarse como parte de los credenciales de autenticación.

Puesto que el servicio se gestiona como un servicio alojado el servicio soporta múltiples organizaciones. La consola de administración posibilita a administradores especificados crear nuevas cuentas empresariales. En estas cuentas empresariales la consola de administración posibilita que se añadan usuarios finales. La información introducida incluye el MSISDN del usuario final, descripción del usuario final y detalles de contacto de correo electrónico del usuario final. Como parte de la creación de nuevos usuarios finales el servidor de administración asigna una aplicación de teléfono celular que enlaza el MSISDN con el número de serie de la aplicación y mensajes del servidor de autenticación de doble factor para suministrar la aplicación al usuario final.

Módulo de autenticación conectable

A través de un PAM 40 (Módulo de Autenticación Conectable) personalizado, el sistema de autenticación de doble factor basado en teléfono celular está diseñado para integrarse con cualquier norma basada en el servidor 42 de autenticación de RADIUS. Este papel de módulos es para validar credenciales de usuario introducidos en el inicio de sesión y presentados al servidor de RADIUS para autenticación comprobando tablas en una base de datos 44 empresarial para la semilla, sal y diferencia de tiempo de cliente de los usuarios finales y calcular la contraseña de único uso apropiada (OTP).

Puesto que la OTP se calcula únicamente en el punto de autenticación se deduce que puesto que la OTP está basada en el tiempo actual los valores de OTP expiran automáticamente. Para la mejor experiencia del cliente, el Módulo 40 de Autenticación Conectable puede comprobar no únicamente contra la contraseña de uso único actual sino también para la última contraseña de uso único generada basándose en una regla de ventaja de ‘tiempo deslizante’.

La regla establece que si después de la corrección de tiempo (para llevar el tiempo de servidor en línea con el reloj de sistema del teléfono celular), el tiempo está en los primeros 30 segundos de un minuto particular entonces tanto la contraseña de uso único actual como la contraseña de uso único anterior se comprueban para autenticación. Esto posibilitará al usuario entre 30 y 90 segundos para transferir la contraseña de uso único desde el dispositivo celular a su cuadro de entrada de inicio de sesión y enviarla al servidor de RADIUS.

Aunque en el modo fuera de línea es posible perder sincronización para la aplicación del teléfono celular con el servidor, la ventana de 60-90 segundos está diseñada para permitir un gran margen de error antes de que el cliente experimente cualquier dificultad.

Como se muestra en la figura, una vez que se obtiene la contraseña de único uso correcta, esto posibilita acceso al servicio proporcionado a través de una diversidad de dispositivos 50 habilitados para internet, incluyendo ordenadores personales, PDA, decodificadores de salón de TV y consolas de juegos. Este acceso se concede basándose en la OTP y al menos una identificación adicional del usuario, pero más típicamente una contraseña y PIN además de la OTP.

Por supuesto, la OTP generada mediante el sistema y método de la invención puede usarse para aumentar la seguridad complementando una amplia diversidad de medidas de seguridad conocidas existentes.

En los ejemplos anteriores, la OTP se usa en combinación con otros parámetros para posibilitar acceso a servicios. Sin embargo, en algunas situaciones la OTP en solitario puede usarse, por ejemplo para proporcionar acceso a diferentes áreas en un sitio. Por ejemplo una vez que se ha concedido acceso general a un sitio, puede requerirse una OTP para acceso a partes específicas con diferentes niveles de seguridad o restricciones de edad.

Serán evidentes diversas modificaciones para los expertos en la materia.

REIVINDICACIONES

1. Un método para proporcionar acceso a un servicio basado en internet desde un dispositivo (10) de teléfono celular, comprendiendo el método:

usar un testigo para calcular una contraseña limitada en tiempo para un usuario específico que busca acceso al servicio basado en internet desde un dispositivo de teléfono celular;
recibir una contraseña limitada en tiempo desde el usuario calculada usando el testigo; y
verificar la contraseña limitada en tiempo para conceder acceso al servicio basado en internet;
y **caracterizado por** generar el testigo en un servidor de un proveedor del servicio basado en internet y proporcionar el testigo al dispositivo de teléfono celular de un usuario que busca acceso al servicio basado en internet,
y en que el testigo tiene validez limitada de tiempo.
donde durante la validez del testigo, se posibilita el acceso al servicio basado en internet sin requerir comunicación con el servidor usado para generar el testigo.

2. Un método como se reivindica en la reivindicación 1, donde se recibe al menos un parámetro de identificación de usuario adicional con la contraseña limitada en tiempo, y
donde verificar la contraseña limitada en tiempo y el al menos un parámetro de identificación de usuario adicional se verifica con la contraseña limitada en tiempo para conceder acceso al servicio basado en internet.

3. Un método como se reivindica en cualquier reivindicación anterior, donde el cálculo de la contraseña limitada en tiempo tiene en cuenta el tiempo actual.

4. Un método como se revindica en cualquier reivindicación anterior, donde el cálculo de la contraseña limitada en tiempo tiene en cuenta un parámetro de identidad del dispositivo (10) de teléfono celular.

5. Un método como se reivindica en cualquier reivindicación anterior, donde el cálculo de la contraseña limitada en tiempo usa la función:

Contraseña = f(IP *XOR* NT *XOR* t), donde t es una medición del tiempo actual, IP es un parámetro de identidad del dispositivo (10) de telefonía celular y NT es el testigo numérico.

6. Un método como se reivindica en la reivindicación 7, donde la función f comprende:

f(x) = RightTrunc(Decimal(SHA(x))), donde RightTrunc es una función para extraer un número de bits más bajo, Decimal es una función para convertir una serie de bytes a un valor entero y SHA es un algoritmo de troceo seguro.

7. Un método como se reivindica en la reivindicación 2, donde el al menos un parámetro de identificación de usuario adicional comprende un nombre de usuario.

8. Un método como se reivindica en la reivindicación 7, donde el al menos un parámetro de identificación de usuario adicional comprende una contraseña de usuario o número de identificación de personal.

9. Un método como se revindica en cualquier reivindicación anterior, donde el testigo comprende un testigo numérico en la forma de un valor de sal.

10. Un método como se reivindica en la reivindicación 1, donde la validez está limitada a un valor entre 1 hora y 1 semana.

11. Un método como se reivindica en la reivindicación 1, donde la validez del testigo se define como una ventana de tiempo, con ventanas de tiempo para testigos secuenciales solapantes.

12. Un método como se reivindica en cualquier reivindicación anterior, donde la provisión del testigo al dispositivo (10) de teléfono celular depende de la autenticación del dispositivo de teléfono celular.

13. Un método como se reivindica en la reivindicación 12, donde la autenticación comprende verificar el al menos un parámetro de identificación de usuario adicional como estando asociado con el dispositivo (10) de teléfono celular específico usando una base de datos de usuarios registrados.

14. Un método como se reivindica en la reivindicación 13, donde el dispositivo (10) de teléfono celular específico se identifica usando el MSISDN.

15. Un método como se revindica en cualquier reivindicación anterior, donde cuando se proporciona el testigo, se implementa también la sincronización de reloj entre el dispositivo (10) de teléfono celular y el proveedor del servicio

basado en internet.

16. Un método como se reivindica en cualquier reivindicación anterior, donde se implementa el acceso al servicio basado en internet a través de un dispositivo conectado a internet.

17. Un método como se reivindica en la reivindicación 16, donde el dispositivo conectado a internet comprende uno de un ordenador personal, un PDA, un decodificador de salón de TV y una consola de juegos.

18. Un programa informático que comprende medios de código adaptados para realizar todas las etapas de cualquier reivindicación anterior cuando se ejecuta dicho programa en un ordenador.

19. Un producto de programa informático que comprende un programa informático como se revindica en la reivindicación 18 realizado en un medio legible por ordenador.

20. Un sistema para proporcionar acceso a un servicio basado en internet desde un dispositivo de teléfono celular, comprendiendo el sistema:

un servidor (20) de un proveedor del servicio basado en internet; y
un dispositivo de telefonía celular que comprende medios para instalación (10), de una aplicación de software que posibilita el cálculo de una contraseña limitada en tiempo desde un testigo para un usuario específico que busca acceso al servicio basado en internet,
donde el servidor (20) comprende adicionalmente medios para recibir la contraseña limitada en tiempo desde el usuario calculada usando el testigo, y para verificar la contraseña limitada en tiempo para posibilitar o prohibir acceso al servicio basado en internet,
y **caracterizado por que** el servidor comprende adicionalmente medios para generar el testigo y para proporcionar el testigo al dispositivo de teléfono celular de un usuario que busca acceso al servicio basado en internet,
y **por que** el testigo tiene validez limitada en tiempo,
donde durante la validez del testigo, el acceso al servicio basado en internet está habilitado sin requerir comunicación con el servidor usado para generar el testigo.

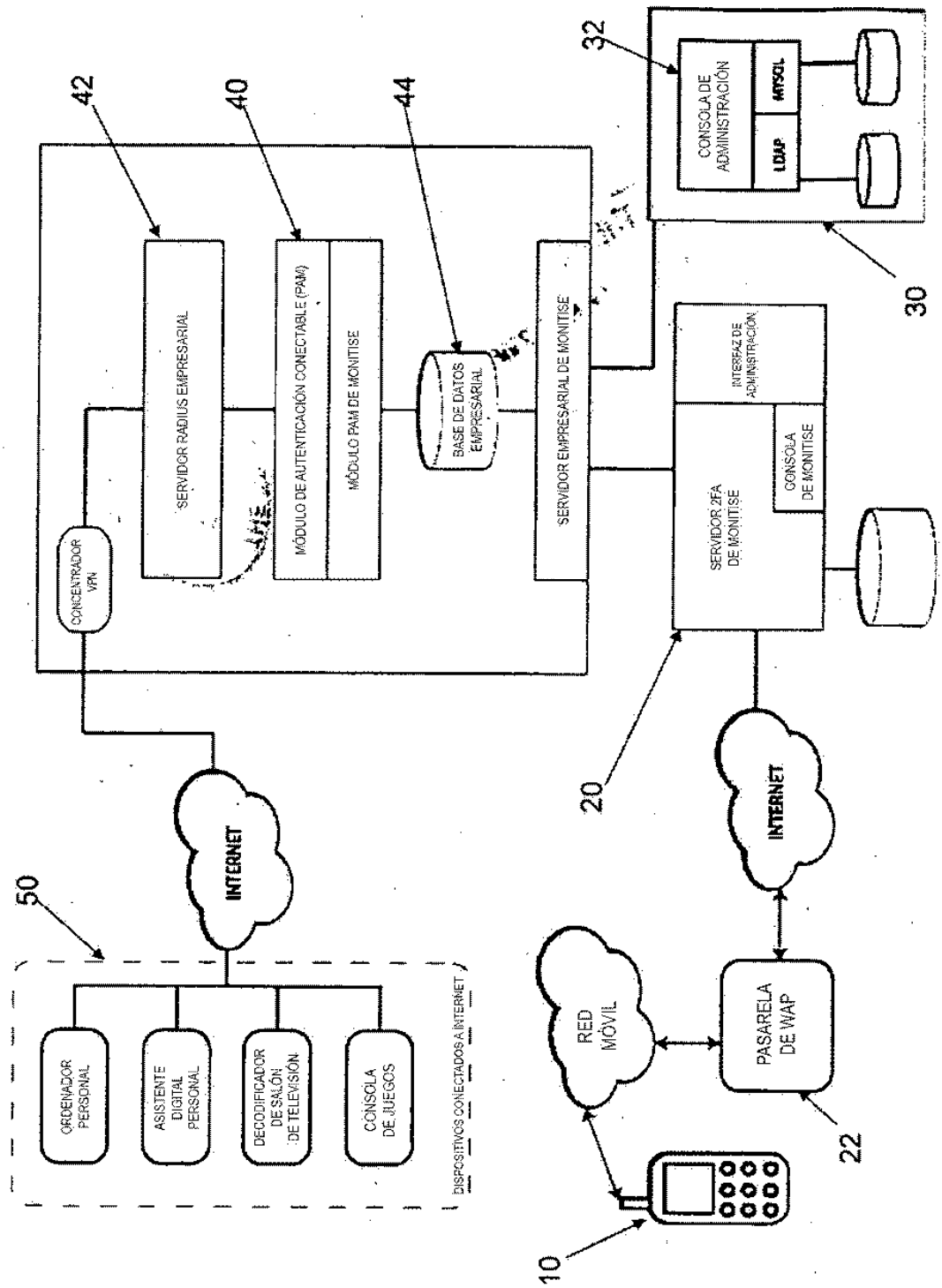
21. Un sistema como se reivindica en la reivindicación 20, donde el servidor comprende adicionalmente medios (40) para verificar al menos un parámetro de identificación de usuario adicional.

22. Un sistema como se reivindica en la reivindicación 20 o 21, donde el cálculo de la contraseña limitada en tiempo usa la función:

Contraseña = f(IP XOR NT XOR t), donde t es una medición del tiempo actual, IP es un parámetro de identidad del dispositivo (10) de teléfono celular y NT es el testigo numérico.

23. Un sistema como se reivindica en la reivindicación 23, donde la función f comprende:

f(x) = RightTrunc(Decimal(SHA(x))), donde RightTrunc es una función para extraer un número de bits más bajo, Decimal es una función para convertir una serie de bytes a un valor entero y SHA es un algoritmo de troceo seguro.


42
40
44
32
CONSOLA DE ADMINISTRACIÓN
LDAP
MYSQL
SERVIDOR RADIUS EMPRESARIAL
MÓDULO DE AUTENTICACIÓN CONECTABLE (PAM)
MÓDULO PAM DE MONITISE
BASE DE DATOS EMPRESARIAL
SERVIDOR EMPRESARIAL DE MONITISE
CONCENTRADOR VPN
INTERFAZ DE ADMINISTRACIÓN
CONSOLA DE MONITISE
SERVIDOR 2FA DE MONITISE
30
20
INTERNET
INTERNET
50
ORDENADOR PERSONAL
ASISTENTE DIGITAL PERSONAL
DECODIFICADOR DE SALÓN DE TELEVISIÓN
CONSOLA DE JUEGOS
DISPOSITIVOS CONECTADOS A INTERNET
RED MÓVIL
PASARELA DE WAP
22
10