(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 367 809**

(51) Int. Cl.:
H04L 29/06 (2006.01)
H04L 12/22 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06757837 .7**
(96) Fecha de presentación : **13.07.2006**
(97) Número de publicación de la solicitud: **2011301**
(97) Fecha de publicación de la solicitud: **07.01.2009**

(54) Título: **Disposición y método para la transmisión segura de datos.**

(30) Prioridad: **10.04.2006 EP 06112432**

(45) Fecha de publicación de la mención BOPI:
08.11.2011

(45) Fecha de la publicación del folleto de la patente:
08.11.2011

(73) Titular/es: **TRUST INTEGRATION SERVICES B.V.**
Ambachtsweg 22
3542 DG Utrecht, NL

(72) Inventor/es: **Sonnega, Marco, Alexander, Henk y Kalenda, Zdenek**

(74) Agente: **Tomás Gil, Tesifonte Enrique**

DESCRIPCIÓN

Disposición y método para la transmisión segura de datos

Campo de la invención

[0001] La invención se refiere al campo de la protección en la comunicación de datos en el que se utilizan claves secretas para codificar/decodificar datos, y posiblemente firmar datos digitalmente, dichos datos se transmiten a través de una ruta de comunicación y deben protegerse.

Antecedentes tecnológicos

[0002] El Instituto Tecnológico de Massachusetts ha desarrollado un protocolo de autenticación en red conocido como "Kerberos". Kerberos está disponible como software de código abierto, aunque también como producto de software de mercado. Kerberos usa criptografía de clave secreta. El servidor de Kerberos distribuye "tiquets" a las unidades de comunicación una vez estas unidades de comunicación se han autorizado a sí mismas el acceso al servidor Kerberos.

[0003] Otra manera conocida de comunicaciones secretas es el uso de servicios de tarjeta inteligente virtual (Virtual Smartcard Services, VSS). El VSS es un sustituto de una tarjeta inteligente física en una solución de PKI a escala completa (PKI = Public Key Infrastructure o infraestructura de clave pública).

[0004] El documento WO 98/09209 divulga un sistema y un método de gestión de transacciones seguras y de protección de los derechos electrónicos.

[0005] El documento WO 02/23798 divulga un sistema para la protección de objetos almacenados en servidores de red. Los servidores son un software en funcionamiento que designa qué objetos deben protegerse, así como una política de seguridad para tal objeto. Un servidor de objetos realiza una petición mejorada que contiene datos codificados bajo petición de un objeto protegido y los vuelve a enviar a un servidor de seguridad que autentica la petición, recupera y codifica el objeto requerido mediante una clave de codificación de un solo uso.

[0006] El documento WO 02/07377 divulga un sistema y un método de transacciones electrónicas seguras entre socios de negocios en una red electrónica de acceso limitado. Esta red electrónica de acceso limitado es accesible sólo para los socios autorizados. Una Autoridad de certificación (CA por sus siglas en inglés *Certificacion Authority*) es accesible en una red pública y puede emitir un certificado digital corporativo a un socio de negocios una vez éste socio ha sido autorizado por la CA. El certificado digital debe usarse como una credencial *online* para acceder a la red electrónica de acceso limitado.

Resumen de la invención

[0007] En el mercado se da la necesidad de proporcionar un alto nivel de seguridad en las comunicaciones sin tener que esperar a una implementación a escala completa de la infraestructura de clave pública (PKI), que podría tardar de 10 a 15 años más si lo implementa una organización gubernamental central.

[0008] Con ese fin, la invención proporciona algunos métodos y disposiciones como se especifica en las reivindicaciones anexas.

[0009] La invención permite el intercambio de datos de manera segura a través de, por ejemplo, Internet. La invención permite este intercambio usando certificados digitales sin la carga normal de expedir y gestionar los certificados digitales, pues es esta carga la que hace que otras aplicaciones en las que se usan claves públicas y privadas sean tan caras.

[0010] La invención se refiere a una manera fiable de autenticación y, posteriormente, de asegurar la conexión entre dos clientes o entre un cliente y un servidor usando un ejecutor de política administrado centralmente.

Breve descripción de los dibujos

[0011] La invención se explicará a continuación en relación con algunos dibujos realizados únicamente para ilustrar la invención y no para limitarla de ninguna manera. El ámbito de la invención se define mediante las reivindicaciones anexas y sus equivalentes técnicos.

La Figura 1 muestra una perspectiva general esquemática de una disposición de red usada en la presente invención;

La Figura 2 muestra una perspectiva general esquemática de la disposición de un ordenador;

La Figura 3 muestra una perspectiva general esquemática de la disposición de red adecuada para enviar y recibir e-mails de forma segura.

Descripción detallada de las formas de realización

1. INTRODUCCIÓN

[0012] La gran mayoría de servicios que se ofrecen a través de Internet son aplicaciones web. Estas aplicaciones dependen de comunicaciones seguras y fiables. Internet usa TCP-IP como *lingua franca*. La potencia del IP se debe

a sus paquetes con rutas fáciles y flexibles. Estos paquetes son también la debilidad principal. La manera en que el IP establece la ruta de estos paquetes hace que las redes de IP sean vulnerables ante riesgos de seguridad. El presente documento divulga una solución para reducir dicha debilidad.

Aumento de la demanda de seguridad

[0013] En las últimas décadas, muchos servicios tradicionales se han transformado en servicios digitales y de negocios electrónicos. Hoy en día, millones personas encargan productos y servicios *online* sin mantener ningún contacto personal con sus proveedores. Tiendas *online*, billetes electrónicos, pagos, sistema de seguimiento "track & trace", configuración de productos y muchos otros servicios están completamente digitalizados. Del mismo modo en que aumenta la cantidad de dinero implicado en los negocios *online*, así crece el interés de las organizaciones criminales en usar Internet para su beneficio. Esta situación requiere una comunicación segura y/o una autenticación fuerte. En otras palabras: a quién estamos hablando, y cómo estar seguros de que nadie más está escuchando o manipulando la conversación.

Soluciones

[0014] En efecto hay soluciones para este problema. Las dos técnicas que se usan para este fin son la firma y la codificación. Y aquí vemos lo esencial de los certificados digitales que contienen parejas de claves con una clave pública y una clave privada, dichos certificados digitales se diseñan tanto para la firma como para la codificación. Los certificados digitales cumplen muy bien con su objetivo *siempre y cuando* se usen *correctamente*. Esto implica una correcta administración, disciplina por parte del usuario y ningún contratiempo. Si este no es el caso, uno puede empezar de nuevo. También conlleva grandes inversiones en infraestructura y educación, por no mencionar el tiempo, el esfuerzo y los costes del mantenimiento de esta denominada infraestructura de clave pública (PKI).

[0015] PKI es el futuro, pero sólo es viable si se implementa a gran escala centralizada. Del mismo modo en que todos tenemos un pasaporte u otros medios de identificación en los que se puede confiar porque han sido expedidos por el estado. Sin embargo, estas soluciones PKI no se implementarán a gran escala centralizada hasta dentro de 5 o 10 años. Por lo tanto, se necesita una alternativa hasta que llegue tal momento. La presente invención proporciona dicha alternativa mediante el uso de un servidor de seguridad en un entorno de red que proporciona certificados digitales con un tiempo de vida limitado, como se explicado más abajo.

Servidor de seguridad

[0016] En la presente invención, se usa un servidor de seguridad 4 que se muestra, por ejemplo, en la figura 1. Este documento explica cómo el servidor de seguridad 4 permite el uso de los beneficios de los certificados digitales sin sus dificultades, por sólo una pequeña parte de su coste y dejando abierta la opción de cambiar a una infraestructura PKI totalmente desarrollada en un futuro. El primer capítulo muestra a grandes rasgos el principio general del servidor de seguridad 4. Los capítulos siguientes tratan aspectos más técnicos de los componentes individuales y el modo en que estos dirigen las cuestiones que implican proteger la seguridad de la comunicación con certificados digitales.

[0017] Para entender mejor la presente invención, se presenta primero una breve explicación sobre los certificados digitales. La explicación es la siguiente y se ha copiado de Computer Desktop Encyclopedia, 1981-2005, The Computer Language Company Inc., Ver. 18.4, 4º Trimestre 2005:

"certificado digital

[0018] El equivalente digital de un carnet de identidad usado en conjunto con un sistema de codificación de clave pública. También conocido como "certificado electrónico", los certificados digitales son expididos por un tercero de confianza conocido como "autoridad de certificación" (CA) como VeriSign (www.verisign.com) y Thawte (www.thawte.com). La CA verifica que una clave pública pertenece a una compañía específica o a un particular (el "sujeto"), y el proceso de validación por el que pasa para determinar si el sujeto es quien afirma ser depende del nivel de certificación y de la propia CA.

Creación del certificado

[0019] Una vez completado el proceso de validación, la CA crea un certificado X.509 que contiene información de la CA y del sujeto, incluyendo la clave pública del sujeto (detalles más abajo). La CA firma el certificado mediante la creación de un resumen (un hash) de todos los campos del certificado y codificando el valor hash con su clave privada. El resumen codificado se llama "firma digital," y cuando se introduce en el certificado X. 509, se dice que el certificado ha sido "firmado."

[0020] La CA matiene su clave privada muy bien protegida, porque si se descubriese, podrían crearse certificados falsos. Véase HSM.

Verificación del certificado

[0021] El proceso de verificación del "certificado firmado" lo realiza el software del receptor, que es típicamente un navegador web. El navegador cuenta con una lista interna de CA populares y sus claves públicas y usa la clave pública apropiada para decodificar la firma otra vez en el resumen. Entonces, recalcula su propio resumen procedente del texto sencillo del certificado y hace una comparación de ambos. Si los dos resúmenes se

corresponden, se verifica la integridad del certificado (éste no se altera), y se asume que la clave pública del certificado es la clave pública válida del sujeto.

Entonces...

[0022] Llegados a este punto, la identidad del sujeto y la integridad del certificado (no hay alteración) se ha verificado. El certificado se combina típicamente con un mensaje firmado o con un fichero ejecutable firmado, y la clave pública se utiliza para verificar las firmas (.. ..). La clave pública del sujeto también se puede usar para proporcionar un intercambio de clave seguro y, de este modo, tener una sesión de comunicación en dos direcciones que está codificada (..) ...

Principales elementos de datos en un certificado X.509:

[0023]

- *Número de versión del modelo de certificado*
- *Número de serie (número único de la CA)*
- *Algoritmo del certificado de firma*
- *Emisor (nombre de la CA)*
- *Periodo de validez*
- *Sujeto (nombre de la compañía o de la persona certificada)*
- *Clave pública y algoritmo del sujeto*
- *Firma digital creada con la clave privada de la CA*

Firma y verificación de un certificado digital

[0024] El certificado firmado se utiliza para verificar la identidad de una persona u organización."

[0025] Usando una clave pública y una clave privada, se puede aplicar la codificación asimétrica en comunicaciones: una parte usa una clave pública para codificar un mensaje dirigido a un tercero, y el tercero que posee una clave privada asociada a esta clave pública usa esta clave privada para decodificar el mensaje codificado. La decodificación no puede hacerse con la clave pública sola.

[0026] Por otra parte, una clave pública y una clave privada se pueden usar en un proceso de firma digital de la siguiente manera: una parte firma un mensaje con una firma digital que se calcula a partir del contenido del propio mensaje usando una clave privada. La firma digital tiene una relación única con el contenido del mensaje. Un tercero que posee las claves públicas asociadas verifica la relación entre la firma digital y el contenido del mensaje recibido. Si se corresponden, el tercero sabe que el contenido del mensaje no ha sido alterado.

El producto y los servicios

El concepto básico

[0027] En una forma de realización, como se muestra en la figura 1, la arquitectura según la invención comprende tres partes que interactúan para crear un canal seguro entre un servicio digital y un cliente: a saber, el servicio digital soportado por un servidor 6, por ejemplo un servidor web, un cliente 2(n) (n = 1, 2, ..., N) y el servidor de seguridad 4. Un cliente se define aquí como una disposición de ordenador haciendo el papel de cliente. Un cliente puede ser cualquier tipo de terminal, como un ordenador personal, un portátil, un PDA (asistente personal digital), un *smart phone*, etc., pero puede, de manera alternativa, tratarse de un router.

[0028] La figura 1 muestra estas entidades conectadas unas a otras en un entorno de red. La figura 1 muestra varios clientes 2(1) ... 2(N), un servidor de seguridad 4, un servidor 6 capaz de poner en funcionamiento un servicio que soporta el estándar X.509, o compatible, como un servidor de banco o un servidor web. Se proporciona a los clientes 2(n) y al servidor 6 el software adecuado y, así, se disponen para ejecutar comunicaciones seguras en la red, por ejemplo, usando un certificado digital SSL u otro protocolo de comunicación en red seguro. Por otra parte, el servidor de seguridad 4 dispone de software adecuado de manera que el servidor de seguridad 4 puede comunicarse de forma segura con el servidor 6, por ejemplo, usando un certificado digital SSL u otro protocolo de comunicación en red seguro. Se observa que un cliente puede ser el ordenador personal localizado en las instalaciones de un particular. Hoy en día, la mayoría de la gente tiene al menos uno de dicho ordenador personal equipado con dicho software adecuado, obtenido a través del software de un banco, por ejemplo, instalado en el ordenador personal a través de un CD-ROM o DVD, para poder realizar operaciones de "banca privada" con un servidor bancario a través de Internet.

[0029] Para autenticar usuarios de clientes 2(n), el servidor de seguridad 4 dispone de un módulo de autenticación que ejecuta la autenticación y que se puede implementar como un programa de software en un procesador adecuado. De otro modo, el servidor de seguridad 4 se puede conectar a un servicio de autenticación externo 8 que funciona en un servidor adecuado, el cual proporciona la autenticación deseada a petición del servidor de seguridad 4.

[0030] La figura 2 muestra una perspectiva general esquemática de la disposición de un ordenador en general. Tal disposición del ordenador se puede usar como cliente 2(n), pero el servidor de seguridad 4 y el servidor 6 también pueden tener la mayor parte de los componentes de la disposición del ordenador que se muestran en la figura 2. Cada uno de los clientes 2(n), el servidor de seguridad 4 y el servidor 6 tendrán al menos un procesador y alguna forma de memoria de almacenamiento de datos e instrucciones para que el procesador ponga en funcionamiento un programa predeterminado que ejecute la funcionalidad conforme a la invención.

[0031] La disposición del ordenador que se muestra en la figura 2 comprende un procesador 1 para realizar operaciones aritméticas. El procesador 1 se conecta a una pluralidad de componentes de memoria, que incluyen un disco duro 5, memoria sólo de lectura (ROM) de ROM 7, memoria de sólo lectura programable con borrado electrónico (EEPROM) 9, y memoria de acceso aleatorio (RAM) 11. No es necesario proporcionar todos estos tipos de memoria. Por otra parte, no es necesario que estos componentes de memoria se encuentren físicamente cerca del procesador 1, sino que pueden encontrarse apartados del procesador 1.

[0032] El procesador 1 también está conectado a medios para introducir instrucciones, datos etc. por un usuario, como un teclado 13, y un ratón 15. También se pueden proporcionar otros medios de entrada conocidos por personas expertas en la técnica, como una pantalla táctil, un ratón *trackball* y/o un convertidor de voz.

[0033] Se proporciona una unidad de lectura 17 conectada al procesador 1. La unidad de lectura 17 está dispuesta para leer datos y posiblemente para grabar datos en un soporte de datos como un disquete 19 o un CDROM 21. Otros soportes de datos pueden ser cintas, DVD, etc. como es sabido por los expertos en la técnica.

[0034] El procesador 1 también está conectado a una impresora 23 para imprimir datos de salida en papel, así como a una pantalla 3, por ejemplo, un monitor o una pantalla LCD (pantalla de cristal líquido), o cualquier otro tipo de pantalla conocida por los expertos en la técnica.

[0035] El procesador 1 puede estar conectado a una red de comunicación 27, por ejemplo, una red telefónica pública conmutada (RTPC), una red de área local (LAN), una red de área amplia (WAN), Internet, etc. mediante medios de entrada/salida 25. El procesador 1 está dispuesto para comunicarse con otras disposiciones de comunicación a través de la red 27.

[0036] El soporte de datos 19, 21 puede comprender un producto de programa informático en forma de datos e instrucciones dispuestas para darle al procesador la capacidad de ejecutar el método conforme a la invención. No obstante, dicho producto de programa informático puede, de otro modo, descargarse a través de la red de telecomunicación 27.

[0037] El procesador 1 se puede implementar como un sistema autónomo, o como una pluralidad de procesadores que operan paralelamente, cada uno dispuesto para llevar a cabo subtareas de un programa informático más grande, o como uno o más procesadores principales con diferentes subprocesadores. Algunas partes de la funcionalidad de la invención pueden incluso ser realizadas por procesadores remotos comunicados con el procesador 1 a través de la red 27.

[0038] Las características de las diferentes entidades de la figura 1 pueden ser de la siguiente manera:

Servicio digital mediante un servidor 6:

[0039] Cualquier servidor 6 capaz de ejecutar un servicio que soporta el estándar X.509, o un equivalente, y que requiere una conexión segura a un cliente 2(n) se puede usar en combinación con el servidor de seguridad 4.

Cliente 2(n):

[0040]

- El usuario final del cliente 2(n) puede instalar un software adecuado procedente del servidor de seguridad 4. Cualquier vía segura conocida para descargar software de un servidor a un cliente como, por ejemplo, el uso de la firma de código o el uso de la tecnología X509 tradicional, se puede utilizar para tal fin.
- Una vez instalado, el software del cliente 2(n) controla la interfaz del usuario y contiene la lógica que establece canales seguros con el servidor de seguridad 4.
- El software del cliente 2(n) puede usar credenciales recuperadas del servidor de seguridad para establecer canales seguros con servicios digitales, usando tecnologías abiertas y estándares, como los protocolos bilaterales SSL/TLS.

Servidor de seguridad 4:

[0041]

- El servidor de seguridad central 4 se encarga de las peticiones de entrada de los clientes 2(n). Dependiendo de los módulos activados y de los niveles de seguridad y aumento seleccionados, el servidor de seguridad 4 se ocupa de petición de entrada de acuerdo con los ajustes seleccionados para el servicio digital correspondiente en el servidor 6. Cuando se está atacando al servicio, el nivel de seguridad puede cambiarse rápidamente a un nivel más alto, para evitar daños.

2. CONCEPTOS

Seguridad de las líneas de comunicación

[0042] Hoy en día, los certificados digitales se usan habitualmente. Cuando uno entra a una página web "segura" en Internet, por ejemplo, al reservar un vuelo *online*, se usa un certificado digital por parte del servidor 6. Este certificado digital se usa con dos objetivos. Se usa para la codificación de la conexión y le dice al navegador web del cliente 2(n) que la página web a la que el navegador está conectado es realmente la página web a la que el navegador *cree* estar conectado. En este sentido, el certificado digital que usa el servidor 6 sirve para autenticar al servidor 6, del mismo modo que un pasaporte se puede usar para identificar al propietario del mismo. El navegador del cliente 2(n) verifica la autenticidad de cada información procedente del servidor 6 durante la toda la sesión.

[0043] Si se observa la información que pasa del navegador al servidor 6, no obstante, es evidente que la situación no es totalmente segura. Mientras que la información que viene del servidor 6 se valida durante toda la sesión, la autenticidad de la información que viene del cliente 2 (N) se controla sólo una vez: es decir, cuando el usuario inicia sesión. Después de eso, el servidor 6 no tiene modo alguno de saber si la siguiente información procede del mismo cliente 2(n) y si no ha sido alterada. Para verificar continuamente al cliente 2(n) durante toda la sesión de comunicación, el cliente 2(n) necesita un certificado digital que el servidor también pueda verificar. Si tanto el servidor 6 como el cliente 2(n) tienen y usan un certificado digital válido, la comunicación es segura por ambas partes.

[0044] Para la comunicación por e-mail funciona el mismo principio. Los certificados digitales deben usarse en las dos partes para codificar y/o firmar mensajes. Si está firmado, el receptor de un e-mail puede verificar la autenticidad del mensaje y si está codificado, no puede leerlo nadie salvo el receptor, siempre y cuando el receptor tenga una clave de decodificación.

Gestión de certificados digitales

[0045] Para los servidores 6, la gestión de certificados digitales no supone un gran problema. Hay pocos servidores 6, los certificados digitales se pueden disponer e instalar según sea necesario y los incidentes se pueden tratar *ad hoc*. Se puede mantener fácilmente el conocimiento de los administradores y de otra gente implicada.

[0046] Para los clientes 2(n), la situación es diferente. El usuario final del PC y otros clientes 2(n) son más vulnerables a los fallos de seguridad, los virus y otros incidentes que hacen que el certificado digital pierda su valor. Puede haber sido copiado. Si es así, se debe disponer e instalar un certificado digital nuevo. Y el certificado digital viejo debe colocarse en la "lista negra" del servidor 6. El propio certificado digital vulnerado puede ser válido otro año o incluso más tiempo. ¿Y cómo enseñar a *cada* usuario final a manejar certificados digitales y a ocuparse de los incidentes?

[0047] En la invención, el servidor de seguridad 4 se encarga de la parte del certificado digital *de usuario* final. El servidor de seguridad 4 autentica al cliente 2(n) conforme a un nivel de fiabilidad predeterminado, y, si funciona bien, proporciona al cliente 2(n) los medios para usar un certificado digital, como se explica más abajo. Se pueden seleccionar diferentes formas de autenticación para proporcionar diferentes niveles de fiabilidad.

[0048] Usando el concepto de la invención, la comunicación entre el cliente 2(n) y el servidor 6 está completamente protegida sin que el usuario final tenga ningún conocimiento técnico.

[0049] Como se explica detenidamente más abajo, la expedición un certificado digital a un cliente 2(n), la instalación del certificado digital y la gestión de la validez del certificado digital, etc. son controladas por el servidor de seguridad 4, cada vez que sea necesario.

Aumento

[0050] En la seguridad, el nivel de seguridad depende en gran medida de las inversiones (costes) para evitar un uso inapropiado en oposición al daño (costes) cuando se da dicho uso inapropiado. Este es también el caso en el entorno de las TIC. Por lo cual uno puede preguntarse: "¿En una organización todo el mundo es consciente de lo que supone un daño?" Para una organización financiera, una intrusión podría significar una pérdida (temporal) de dinero, que puede controlarse usando límites de transacción. Una pérdida de imago, no obstante, puede tener como resultado la introducción tardía de servicios nuevos, lo que supone una pérdida de ingresos y beneficios a corto y largo plazo. Con el concepto de la presente invención, se pueden reconocer varios niveles de seguridad necesarios y las organizaciones que usan esta plataforma pueden aumentar su nivel de seguridad cuando su participación en una empresa es mayor o surge la necesidad. Este nivel de seguridad se une con el proceso de autentificación realizado por el servidor de seguridad 4 para autenticar al cliente 2(n).

[0051] Para entender el concepto de aumento, se hace primero una explicación general sobre los posibles niveles de seguridad en un entorno cliente-servidor.

[0052] En el nivel de autenticación (cuando se inicia sesión en una página web) hay diferentes opciones disponibles, cada una relacionada con un nivel de seguridad distinto:

- Uso de contraseña
- Uso de contraseña de un solo uso (es decir, con cada incio de sesión se usa una contraseña nueva)
- Uso de un protocolo pregunta-respuesta (el cliente 2(n) recibe una pregunta del servidor que sólo el cliente 2(n) puede entender)
- Uso de un dispositivo de autenticación (p. ej. USB);
- Uso de una tarjeta inteligente (p. ej. GemPlus, Schlumberger);
- Uso de un identificador biométrico (p. ej. huella digital, reconocimiento de iris).

[0053] En general: a mayor seguridad, mayores costes.

[0054] El nivel de seguridad usado depende del valor de los servicios que debe proporcionar el servidor 6, así como de las amenazas existentes. Los dos parámetros pueden cambiar con el tiempo. El incremento del nivel de seguridad se llama aumento.

[0055] Puede usarse el mismo concepto de autenticación cuando el cliente 2(n) tiene que iniciar sesión en el servidor de seguridad 4. Con el servidor de seguridad 4, el administrador puede hacer varios aumentos, sin molestar a los usuarios finales. Otras intensificaciones de seguridad requieren acciones por parte *de usuario* (p. ej. las actualizaciones de seguridad de Microsoft, la instalación de software del cliente necesario para la invención o quizá el uso de un dispositivo de autenticación). La invención proporciona una plataforma y no tanto una herramienta, y por lo tanto permite la integración de todo tipo de medidas de seguridad sin afectar a la funcionalidad básica. Por ejemplo, el método de autenticación (contraseña, pregunta-respuesta, dispositivo de autenticación) se puede cambiar mientras que el resto de módulos y funciones implementados continúan trabajando como antes. Esto se explica detalladamente más abajo.

3. Plataforma

[0056] La invención se desarrolló teniendo en cuenta que el producto debería no sólo encargarse de las necesidades de seguridad de hoy, sino también de las del futuro. Como resultado, se construyó como una plataforma con módulos enchufables. La plataforma se encarga de la funcionalidad genérica que se necesita para todos los servicios. Los módulos se encargan de funcionalidades especializadas, como la autenticación y soporte de e-mail. Esto deja lugar para mejorar funcionalidades a la vez que deja la plataforma en su lugar. Se pueden integrar fácilmente nuevos servicios sin molestar a los otros servicios.

Integración fluida, elección de plataformas

[0057] Se ha reconocido la importancia de que los componentes del servidor tienen que integrarse perfectamente en los entornos TIC existentes. El entorno central de la invención se puede implementar en una elección de plataforma que varía de Linux a entornos de importancia fundamental, como la plataforma HP NonStop.

[0058] La comunicación y la integración que cuenta con sistemas TIC existentes, como bases de datos e infraestructuras de autenticación, se hace fácil gracias al uso de tecnologías abiertas y basadas en estándares.

PC, PDA y dispositivos futuros

[0059] Los beneficios no se restringen solo al uso en el PC, sino que pueden abarcar dispositivos móviles como los PDA y los *smart phones*. El uso de tecnologías abiertas y basadas en estándares garantiza que los dispositivos futuros también soporten la tecnología aquí descrita.

Arquitectura de la plataforma

[0060] En una forma de realización, la arquitectura de autenticación consiste en tres partes que interactúan para crear una conexión segura entre un cliente y un servidor web.

Software de aplicación de cliente.

[0061] El cliente 2(n), una vez autenticado el usuario, recibe el software de aplicación de cliente procedente del servidor de seguridad 4. Se puede utilizar cualquier técnica conocida de descarga segura de tal software desde el servidor de seguridad 4. De otro modo, el software puede haber sido cargado desde un CD-ROM adecuado o similar. El software de aplicación es un software de aplicación ligero responsable de la recuperación de un certificado digital válido temporalmente, por ejemplo un certificado digital X.509, procedente del servidor de seguridad 4. El software de aplicación de cliente proporciona la interfaz al usuario para la solución de la presente invención. Le presenta al usuario del cliente 2(n) las ventanas de diálogo necesarias y contiene la lógica que crea una conexión segura con el servidor de seguridad 4. La conexión segura se puede basar en el protocolo Diffie-Hellman. Implementa la comunicación codificada entre el servidor de seguridad 4 y el cliente 2(n).

Proceso básico

[0062] El proceso básico se explica como una situación en la que el cliente 2(n) desea configurar una conexión segura con el servidor 6 que es un servidor de banco que mantiene comunicaciones seguras usando su propio certificado digital de servidor de banco que incluye una clave pública de banco BPrK y una clave privada de servidor de banco asociada BPrK almacenada en su memoria de manera segura. Se asume que el cliente 2(n) ha almacenado software adecuado en su memoria para comunicar con el servidor de seguridad 4, como se explica en la sección anterior. Luego hay dos fases diferentes en el establecimiento de la conexión segura. Estas dos fases se realizan en secuencia y son independientes la una de la otra:

- Primera fase:

  En la primera fase, el cliente 2(n) recibe un certificado digital y una clave privada después de ser autenticado, de la siguiente manera.

  Con ese fin, el cliente 2(n) establece una conexión con el servidor de seguridad 4. Durante el establecimiento de la conexión, se intercambian varios datos entre el cliente 2(n) y el servidor de seguridad 4. El cliente 2(n) envía datos para que el servidor de seguridad 4 lo autentique, usando uno de los métodos a los que se hace referencia más arriba. La autenticación se puede basar en un servicio de autenticación controlado por el propio servidor de seguridad 4 o por un servicio de autenticación externa 8. Tras realizar la autenticación satisfactoriamente, el servidor de seguridad 4 envía un certificado digital temporal al cliente 2(n), así como una clave privada asociada a la clave pública del certificado digital temporal. La clave privada asociada a la clave pública puede transmitirse del servidor de seguridad 4 al cliente 2(n) usando el software del cliente 2(n) que puede mantener una conexión segura entre los dos, por ejemplo, un software basado en el protocolo Diffie-Hellman. El certificado digital y la clave privada pueden, por ejemplo, transmitirse de forma segura en un paquete denominado PCKS #12. No obstante, la invención no se limita a lo dicho.

- Segunda fase:

  En la segunda fase, el cliente 2(n) realiza la sesión de comunicación segura con el servidor de banco 6. Esta comunicación puede ahora protegerse desde ambos lados, ya que, ahora, el cliente 2(n) y el servidor de banco 6 poseen su propio certificado digital y sus propias claves privadas. Así, pueden disponer del denominado protocolo bilateral SSL (SSL = *Secure Sockets Layer*), que es controlado por el software de aplicación y el par de clave descargado del servidor de seguridad 4 de la primera fase. La segunda fase no está controlada por el servidor de seguridad 4.

[0063] Conforme a la invención, el certificado enviado por el servidor de seguridad 4 al cliente 2(n) cuenta con un tiempo de vida predeterminado y limitado. Este tiempo de vida predeterminado se puede expresar en forma de período de tiempo, por ejemplo, varias horas (como un máximo de 24 horas o 1 hora), varios minutos (menos de 60 minutos), o varios segundos (menos de 60 segundos). De otro modo, la duración se puede caracterizar por estar asociada a un número predeterminado de sesiones de comunicación con un tercero, por ejemplo, una sesión. En otra alternativa, el tiempo de vida se puede caracterizar por estar asociado a un número predeterminado de acciones, como la recuperación de uno o más mensajes de un servidor web o un servidor de e-mail, como se explicará más adelante. En otra alternativa, el tiempo de vida limitado puede caracterizarse por contar con un máximo predeterminado de usos, por ejemplo 1 o menos de 10. El tiempo de vida limitado se incluye en uno de los atributos del certificado digital temporal. Por ejemplo, si la validez se expresa en unidades de tiempo, se puede usar el atributo del periodo de validez. De otro modo, se puede usar un atributo adicional para indicar el tiempo de vida limitado. El software instalado en el cliente 2(n) está preparado para reconocer este atributo y usarlo para eliminar el certificado digital una vez la validez ha expirado.

Servicio *online*

[0064] Uno de los beneficios más significativos de la arquitectura es que el servicio *online* normalmente se puede hacer disponible sin modificación. Siempre que se trate la seguridad por medio de certificados digitales estándar (que es el caso de la mayoría de servicios *online*), la solución de la invención se integra con el servicio *online* sin necesidad de modificar el servicio. Por supuesto, en el caso de un servicio *online* que no esté basado en estándares, se podría desarrollar un módulo adaptado que haga la seguridad disponible para este servicio también.

Servidores y plataforma

[0065] El servidor de seguridad 4 procesa las peticiones entrantes de los clientes 2(n) controladas por el software de aplicación de cliente instalado en el cliente 2(n). El servidor de seguridad 4 controla el protocolo que se requiere para generar los pares de claves que requiere la petición. Opcionalmente, el servidor de seguridad 4 puede administrar también una base de datos que almacena cuentas, pares de claves disponibles y certificados digitales válidos, procesar preguntas de la base de datos procedentes de otros centinelas y administrar una reserva de claves de codificación disponibles. Cuando la cantidad de claves disponibles desciende por debajo de un cierto umbral inferior, el servidor de seguridad 4 puede generar claves nuevas hasta alcanzar un umbral superior.

4. Opciones de plataforma

Autoridad de certificación

[0066] La plataforma se usa para la distribución y gestión de certificados digitales. Estos certificados digitales primero tienen que generarse. Esto se hace usando una autoridad de certificación. Se trata básicamente de un certificado digital y la clave se utiliza para generar y firmar certificados digitales nuevos. La mayoría de compañías no cuentan con una autoridad de certificación (CA) propia. Por lo tanto, el servidor de seguridad 4 tiene la opción de usar una CA interna para generar certificados digitales. Pero algunas compañías sí tienen su propia CA (de Baltimore, por ejemplo). Por lo tanto, el servidor de seguridad 4 también tiene la opción de usar certificados digitales generados por esta CA, que es un tercero.

Autenticación

[0067] Se pueden distinguir dos grupos de autenticación de usuarios:

a) Autenticación del usuario mediante un mecanismo de autenticación interno. Este mecanismo de autenticación interno puede estar basado en cualquiera de los mecanismos de autenticación explicados anteriormente.

b) Autenticación del usuario mediante un sistema de autenticación externo existente, como a través del servicio de autenticación 8, y usando los resultados de la autenticación externa en el proceso de generación de clave simétrica (por ej. Vasco Digipass con una contraseña de un solo uso). Con ese fin, el servidor de seguridad 4 se conecta a un procesador de autenticación asociado al servidor de banco 6 que realiza la verdadera autenticación después de que el usuario del cliente 2(n) haya enviado sus credenciales. En este caso, se puede usar e integrar en la plataforma una administración de usuario ya existente.

Generación de claves

[0068] Cuando se usa la autoridad de certificación interna, las claves que se generan para ser usadas en los certificados digitales pueden generarse de antemano y almacenarse en la base de datos controlada por el servidor de seguridad 4. Esto se puede hacer a veces cuando el servidor de seguridad 4 no tiene mucho tráfico. Entonces, más tarde cuando el servidor de seguridad 4 está ocupado, no se necesita potencia de procesamiento para generar claves, ya que la clave se puede recuperar de la base de datos.

[0069] Otra opción es la de obtener la clave en el momento en que se necesita. Si la carga del servidor de seguridad no supone un problema, la implementación será fácil. También se puede recuperar el certificado digital de una fuente externa en el momento en que se necesita. En este caso, la generación de la clave tampoco necesita ninguna potencia de procesamiento.

5. Otras formas de realización

[0070] A continuación, se explican otras formas de realización de la presente invención.

a. Módulo de e-mail

Concepto

[0071] El e-mail es una de las funciones más comúnmente adoptadas de las que ofrece Internet. Aunque su uso es sencillo y está difundido, es también una de las maneras menos seguras de comunicación. Este es el caso, a menos que se utilicen la codificación y la firma para proteger la conversación de e-mail. Al igual que ocurre con la navegación web, esto se puede conseguir usando certificados digitales expedidos por el servidor de seguridad 4.

[0072] Con ese fin, en una forma de realización, los clientes 2(n) cuentan con un módulo especial de e-mail seguro.

[0073] En una forma de realización, un par de claves que incluye una clave pública PuK(i) y una clave privada asociada PrK(i) que, juntas, se asocian a un certificado digital expedido, se almacenan en la base de datos del servidor de seguridad 4. Esto se hace para evitar que un e-mail recibido y/o enviado protegido por este certificado digital se haga ilegible porque el certificado digital deje de ser válido. Si el certificado digital deja de ser válido, basándose en este par de claves almacenadas PuK(i) y PrK(i), el servidor de seguridad 4 puede generar un nuevo certificado digital temporal que puede utilizarse para leer el e-mail en cuestión. Una ventaja adicional es que el e-mail protegido se puede transmitir desde cualquier sistema provisto de este módulo de e-mail seguro.

Funcionalidad

[0074] El módulo de e-mail seguro se explicará en relación con la figura 3. Los componentes con el mismo número de referencia que en las figuras 1 y 2 se refieren a los mismos componentes. La figura 3 muestra un servidor de e-mail 10 conectado a los clientes 2(n) y 2(n') ($n \neq n'$). Supongamos que el usuario del cliente 2(n) desea enviar un e-mail al cliente 2(n') de manera segura. Entonces, el usuario da comienzo a una aplicación de e-mail (p. ej. Windows Outlook). De la misma manera, como se explica más arriba, éste recibe un certificado digital temporal que incluye una clave pública PuK(1) del servidor de seguridad 4. Además, como se explica más arriba, éste recibe también una clave asociada privada PrK(1) del servidor de seguridad 4.

[0075] De la misma manera, el cliente 2(n') recoge un certificado digital temporal procedente del servidor de seguridad 4. Entonces, el cliente 2(n') tiene una clave pública PuK(2) y una clave privada PrK(2).

[0076] Ahora, el intercambio seguro de e-mails entre los clientes 2(n) y 2(n') se puede llevarse a cabo. Por ejemplo, el cliente 2(n) puede querer firmar digitalmente un e-mail para enviar al cliente 2(n'). Entonces, el cliente 2(n) firma el e-mail mientras utiliza su clave privada PrK(1). El cliente 2(n) manda su clave pública PuK(1) al cliente 2(n') que usa esta clave pública PuK(1) para verificar que el contenido del e-mail no ha sido alterado.

[0077] Si el cliente 2(n) desea enviar un e-mail codificado al cliente 2(n'), entonces le pide al cliente 2(n') que le envíe su clave pública PuK(2). Al recibir esta clave pública PuK(2), el cliente 2(n) codifica el e-mail con la clave pública PuK(2) y luego envía el e-mail al servidor de e-mail 10. El cliente 2(n') lee el e-mail procedente del servidor de e-mail 10 y decodifica el e-mail con su clave privada PrK(2).

[0078] El certificado digital usado por el cliente 2(n) puede ser válido sólo durante un corto periodo de tiempo predeterminado, como se explica más arriba. De otro modo, el certificado digital también puede ser válido sólo para un e-mail. En otra alternativa, el certificado digital puede ser válido siempre que el software de cliente de e-mail esté activo. Entonces, en cuanto el usuario cierra el software de cliente de e-mail, el certificado digital desaparece del cliente 2(n). La validez del certificado digital del cliente 2(n') también tiene una limitación temporal, por ejemplo, que el certificado digital sólo es válido para un único e-mail y/o durante una hora.

[0079] Una vez más, la manera en que la validez del certificado digital se limita temporalmente se caracteriza por un atributo en el propio certificado digital. El software instalado en los clientes 2(n), 2(n') está dispuesto para reconocer este atributo y usarlo para eliminar el certificado digital una vez ha expirado la validez.

b. Módulo de firma

Concepto

[0080] Al igual que el módulo de e-mail, el cliente 2(n) puede disponer de un módulo de firma digital que se usa para firmar digitalmente documentos digitales.

• Funcionalidad

[0081] Tal como se ha explicado sobre el módulo de e-mail, el cliente 2(n) recibe un certificado digital temporal que incluye una clave pública PuK(1) del servidor de seguridad 4. Por otra parte, como se explica más arriba, también recibe una clave privada asociada Pry(1) procedente del servidor de seguridad 4.

[0082] Entonces, el cliente 2(n) firma el documento mientras usa su clave privada PrK(1). El cliente 2(n) puede almacenar el documento firmado en su memoria. De otro modo, el cliente 2(n) puede enviar el documento firmado a otro cliente 2(n'). Si es así, el cliente 2(n) envía su clave pública PuK(1) al cliente 2(n'), que usa esta clave pública PuK(1) para verificar que el contenido del e-mail no ha sido alterado.

[0083] Como otra alternativa más, el cliente 2(n) envía el documento firmado a una base de datos central donde se almacena para cuestiones legales o administrativas. Entonces, cualquier cliente tercero 2(n') puede recuperar este documento de la base de datos central y verificar su contenido mientras usa la clave pública PuK(1).

[0084] Una vez más, el certificado digital usado por el cliente 2(n) puede ser válido sólo durante un corto periodo de tiempo predeterminado, como se explica más arriba. De otro modo, el certificado digital puede ser válido solo para firmar un número limitado y predeterminado de documentos, por ejemplo 1 documento.

[0085] Una vez más, la manera en que la validez del certificado digital se limita temporalmente se caracteriza por un atributo en el propio certificado digital. El software instalado en el cliente 2(n) está dispuesto para reconocer este atributo y usarlo para eliminar el certificado digital una vez la validez ha expirado. Usando criterios en uno o más de los atributos del certificado digital, el certificado digital puede utilizarse también para un uso no estándar, por ejemplo para la validez en un futuro.

c. Módulo *phishing/pharming*

Concepto

[0086] El uso de Internet para hacer transacciones financieras y comerciales continúa creciendo día tras día. Debido a la creciente cantidad de dinero que está implicada en las transacciones *online*, el interés del crimen organizado también aumenta. Por lo tanto, los delitos informáticos también se hacen cada vez mas creativos. Los ataques de *phising* usan emails con "falsificación de IP" para llevar a los consumidores a páginas web falsificadas que han sido diseñadas para engañar a los receptores de modo que revelen datos financieros, como números de tarjetas de crédito, nombres de usuario de las cuentas, contraseñas y números de la seguridad social. "Secuestrando" el nombre comercial de bancos, comercios *online* y compañías de tarjetas de crédito, quienes llevan a cabo el *phishing* consiguen a menudo convencer a los receptores para que respondan.

[0087] En el caso del "*pharming*", también surgen cuestiones de seguridad parecidas en las que alguien crea una nueva página web que es parecida a otra que ya existe.

[0088] La presente invención, mediante un módulo *phishing/pharming*, puede evitar que clientes confiados faciliten sus datos personales de valor a delincuentes. El módulo *phishing/pharming* puede bloquear el acceso a páginas web de *phishing* y/o *farming*, como se explica más abajo.

[0089] Mientras se establece la conexión entre un cliente 2(n) y el servidor de seguridad 4 para obtener un certificado digital temporal, hay un intercambio de datos entre los dos. En esta fase, el servidor de seguridad 4 envía datos al cliente 2(n) relacionados con ataques potenciales de *phishing* y *pharming*. El cliente 2(n) puede usar estos datos para evitar ese ataque *phishing* y/o *pharming*.

Funcionalidad

[0090] La estratagema del *phishing* dirige a las víctimas confiadas a una página web falsa que se hace pasar por una compañía conocida. La estratagema del *pharming* dirige a los usuarios a páginas web parecidas. El módulo *phishing/pharming* instalado en el cliente 2(n) impide que esto ocurra de la siguiente manera.

[0091] El módulo *phishing/pharming* está dispuesto para que el cliente 2(n) esté conectado al servidor de seguridad 4. El momento en que se realiza esta conexión puede ser desencadenado automáticamente por el módulo *phishing/pharming*. El desencadenante puede, por ejemplo, ser el momento en que el cliente 2(n) comienza a utilizar un navegador web que el módulo phishing/pharming reconoce. Al detectar el comienzo del uso del navegador, el módulo *phishing/pharming* recupera automáticamente datos reales del servidor de seguridad 4 relacionados con amenazas reales de *phishing* y/o *pharming*. Estos datos contienen datos sobre páginas relacionadas con amenazas potenciales de *phishing* y/o *pharming*. El módulo *phishing/pharming* informa al navegador web sobre las páginas con estas amenazas potenciales de *phishing/pharming*. El navegador web utiliza esta información para, por ejemplo, impedir el acceso a estas páginas o para enviar una advertencia al usuario del cliente 2(n).

d. Almacenamiento centralizado de certificados digitales y claves privadas

[0092] En las formas de realización ya mencionadas, se ha explicado que el certificado digital temporal y la clave privada asociada son enviados por el servidor de seguridad 4 al cliente 2(n) y se almacenan en la memoria del cliente 2(n). No obstante, para mejorar la seguridad, en una forma de realización alternativa, una vez el certificado digital y la clave privada han sido generados e identificados como asociados al cliente 2(n), se pueden almacenar en una base de datos central monitoreada y posiblemente controlada por el servidor de seguridad 4. Tal base de datos se puede localizar en el servidor de seguridad 4 o en un lugar remoto al mismo. Si es así, el certificado digital y la clave privada asociada almacenados centralmente se pueden usar en una operación de firma digital que se lleva a cabo en el servidor de un tercero 6, por ejemplo, en el servidor de una organización gubernamental. El servidor del tercero puede establecer una conexión segura con el servidor de seguridad 4 para acceder al certificado y a la clave privada asociada almacenados centralmente. El servidor del tercero entonces usa la clave privada recibida para firmar un mensaje destinado al cliente 2(n) y envía el mensaje firmado al cliente 2(n). También envía la clave pública presente en el certificado digital al cliente 2(n), que éste usa para verificar el contenido del mensaje firmado.

[0093] En una forma de realización alternativa a la mencionada, el cliente 2(n) usa un certificado temporal asociado a una clave pública y una clave privada asociada, estando ambas almacenadas centralmente y siendo controladas por el servidor de seguridad 4. Así, en este caso, la clave privada y la clave pública asociadas al certificado son copias de las claves respectivas de un par de claves que permanecen centralmente almacenadas y a las que servidor de seguridad 4 puede acceder después. Tal certificado temporal se recibe desde el servidor de seguridad 4 de la manera en que se explica más arriba. Entonces, la clave privada asociada al certificado temporal es usada por el cliente 2(n) para firmar un formulario oficial cuando se envía, por ejemplo, a una entidad oficial como las autoridades fiscales. La clave pública asociada al certificado temporal se envía a las autoridades también, y estas la utilizan para verificar el contenido del formulario recibido. Esta es una forma de realización ventajosa cuando entidades como las autoridades fiscales requieren que el usuario use claves almacenadas centralmente. Por otra parte, las autoridades fiscales pueden controlar con el servidor de seguridad 4 si la clave pública utilizada pertenece a un conjunto de claves almacenado centralmente.

e. Uso de pares de claves más de una vez.

[0094] En otra forma de realización, el servidor de seguridad 4 almacena uno o más conjuntos de pares de claves que incluyen una clave pública y una clave privada asociada. Cada vez que un cliente pide enviar un certificado temporal, transmite dicho certificado con una copia de uno de estos conjuntos de claves. Así, en estas formas de realización, estos conjuntos de claves se pueden usar más de una vez. Hay que tener en cuenta que el certificado cambia siempre para el mismo conjunto de claves, ya que el certificado contiene más datos además del conjunto de claves.

6. Cuestiones del usuario

[0095] La solución de la invención es técnicamente sólida y fácil de usar, como se explica a continuación. Este párrafo describe los efectos que la invención tendrá en los usuarios de estos servicios que usan la tecnología como se describe aquí.

Instalación

[0096] Las actividades de instalación por parte del cliente se reducen al mínimo absoluto. La instalación de la funcionalidad requerida por el cliente se puede llevar a cabo mientras se use tecnología punta y, en general, no requiere la instalación de hardware.

Facilidades para el usuario

[0097] El mecanismo de autenticación que se explica más arriba es muy fácil de usar. Una vez instalado en el cliente 2(n), el software de autenticación en el cliente 2(n) establece una conexión segura sin ninguna interferencia del cliente que no sea la introducción de credenciales, como la identidad del usuario y la contraseña, dependiendo del método de autenticación elegido. También, puesto que el software de cliente es genérico, se puede distribuir por Internet.

Disciplina del usuario final

[0098] El proceso de autenticación es invisible y completamente transparente para el usuario final y no requiere intervención alguna por parte del usuario final. La autenticación le hace la vida más fácil no solo al (usuario del) cliente 2(n) haciendo al cliente 2(n) responsable de la autenticación, sino también al proveedor del servicio de una página web debido a que el servidor web que soporta la página web puede identificar al cliente 2(n) de manera fiable y puede confiar en el hecho de que nadie puede engañar al cliente 2(n).

Implementación

[0099] En general, la introducción de una plataforma de comunicación segura requiere un periodo sustancial de implementación y presupuesto, porque las claves han de distribuirse a todos clientes 2(n). En algunos casos, puede necesitarse un hardware especial. En el caso de la invención, el único requisito es un cliente de software genérico pequeño, que puede descargarse de Internet o distribuírse con un CD-ROM. El impacto técnico de la plataforma descrita también es mínimo. El servidor de seguridad 4 puede colocarse en el exterior o bien en el interior del entorno del proveedor de servicio de una página web.

Impacto organizativo

[0100] Cuando se usa una PKI, el proveedor del servicio debe administrar no sólo qué certificados digitales se han expedido, sino también qué certificados digitales deben revocarse. Esto requiere una administración general y eficaz. Otro impacto organizativo es el aprendizaje. Cuando se introduce una nueva tecnología en una compañía, hay que capacitar al personal. Si un proyecto PKI usa una tarjeta inteligente, el servicio de ayuda técnica a distancia también debe estar capacitado para responder a preguntas relacionadas con este tipo de dispositivos. Se debe configurar el mantenimiento, se debe vigilar el *stock* y el producto debe estar actualizado en todo momento.

[0101] A diferencia de las soluciones de PKI a escala completa, la implementación de la invención no requiere la implementación de procesos complejos ni el aprendizaje exhaustivo en las organizaciones.

Operaciones

[0102] La solución se puede administrar y mantener centralmente de manera sencilla: esta soporta la gestión central en tiempo real de todos privilegios de acceso de clientes remotos, la protección de la comunicación y la gestión de los certificados digitales. Un administrador puede reaccionar con dinamismo a cambios en la situación de seguridad, catalogar los nuevos usuarios o servicios y eliminar los viejos.

Aspecto financiero

[0103] Desde una perspectiva financiera, la invención se distingue de otras soluciones cuando se examina la relación precio-rendimiento. El coste inicial total por usuario es bajo, ya que el cliente no requiere ningún hardware especial. Los costes constantes, que suelen ser altísimos, normalmente se producen por la atención al cliente integral. La autenticación, como se explica más arriba, requiere una implicación mínima por parte del usuario final, ya que su cliente 2(n) hace el trabajo necesario. Una vez el software de cliente se ha instalado en el cliente 2(n), la intervención del usuario final ya no es necesaria. También hay poco impacto en la organización. No hay necesidad de establecer nuevos departamentos.

Contratiempos

[0104] Cuando se usa una PKI, toda la infraestructura se apoya en la integridad de componentes centrales como la autoridad de certificación (CA). En caso de que la integridad de uno de los componentes o procedimientos esenciales ya no pueda garantizarse, todos los certificados digitales expedidos deben revocarse y sustituirse por certificados digitales nuevos. El impacto de tal acontecimineto es sustancial, especialmente cuando, para almacenar certificados digitales, se usan dispositivos de autenticación USB seguros, tarjetas electrónicas o cualquier otro dispositivo hardware de autenticación. Todos los dispositivos de autenticación tendrán que sustituirse. En el mercado de lo seguros de hoy en día, la falta de datos históricos dificulta la protección contra tales riesgos.

[0105] En caso de que el servidor de seguridad 4 esté en peligro, con la reinstalación del servidor de seguridad 4 se restablecerá la integridad de todo el sistema. La reinstalación del servidor de seguridad 4 no causa impacto alguno en los usuarios de los servicios que usan la tecnología descrita.

REIVINDICACIONES

1. Método de transmisión segura de datos en una sesión de comunicación entre un cliente (2(n)) y una disposición informática de un tercero (2(n'); 6), que comprende:

a) el establecimiento de una sesión de comunicación inicial segura y codificada entre dicho cliente (2(n)) y un servidor de seguridad (4) por medio de una red de comunicación pública que conecta dicho cliente (2(n)) y dicho servidor de seguridad (4) mientras usa un software de aplicación de cliente instalado en el cliente (2(n));

b) en dicha sesión de comunicación inicial segura y codificada, la autenticación del usuario de dicho cliente (2(n)) en el proceso de autenticación es controlada por dicho servidor de seguridad (4) mientras usa un protocolo de autenticación con un nivel de seguridad predeterminado;

c) en dicha sesión de comunicación inicial segura y codificada, la transmisión a dicho cliente (2(n)) de una clave privada (PrK(i)) y un certificado digital que comprende una clave pública (PuK(i)) y uno o más atributos, estando dicha clave privada (PrK(i)) asociada a dicha clave pública (PuK(i)), estando dicho certificado digital y dicha clave privada asociados a dicho cliente (2(n));

d) en dicha sesión de comunicación inicial segura y codificada, la instalación automática de dicho certificado digital y clave privada en dicho cliente (2(n));

e) la realización de dicha transmisión segura de datos en dicha sesión de comunicación entre dicho cliente (2(n)) y dicha disposición informática de un tercero (2(n'); 6) mientras usa dicha clave pública (PuK(i)) y dicha clave privada (PrK(i));

donde dicho certificado digital tiene un tiempo de vida limitado y definido por al menos un atributo, y dicho atributo define al menos uno de los siguientes:

- una duración de tiempo predeterminada;
- un número de sesiones de comunicación predeterminado;
- un número de acciones predeterminado.

2. Método según la reivindicación 1, donde dicha sesión de comunicación inicial segura y codificada usa el protocolo Diffie-Hellman.

3. Método según la reivindicación 1 ó 2, donde dicho certificado digital y dicha clave privada se transmiten desde dicho servidor de seguridad (4) a dicho cliente (2(n)) en un paquete PCKS #12.

4. Método según cualquiera de las reivindicaciones 1, 2 ó 3, donde dicho certificado digital que comprende dicha clave pública (PuK(i)) y uno o más atributos, y dicha clave privada (PrK(i)) asociada a dicha clave pública (PuK(i)), tras hacerse disponibles, se envían a dicho cliente (2(n)) y son almacenadas por dicho cliente (2(n)).

5. Método según cualquiera de las reivindicaciones 1, 2 ó 3, donde dicho certificado digital que comprende dicha clave pública (PuK(i)) y uno o más atributos, y dicha clave privada (PrK(i)) asociada a dicha clave pública (PuK(i)), tras hacerse disponibles, son almacenadas por dicho servidor de seguridad (4).

6. Método según cualquiera de las reivindicaciones precedentes, donde dicha acción de autenticación se basa en al menos uno de los siguientes usos:

- Uso de una contraseña,
- Uso de una contraseña de un solo uso,
- Uso de un protocolo pregunta-respuesta,
- Uso de un dispositivo hardware de autenticación,
- Uso de una tarjeta inteligente, y
- Uso de una característica biométrica.

7. Método según cualquiera de las reivindicaciones precedentes, donde dicha transmisión segura de datos se basa al menos en uno de dichos datos codificados con dicha clave pública (PuK(i)) y firmando digitalmente dichos datos con dicha clave privada (PuK(i)).

8. Método según cualquiera de las reivindicaciones precedentes, donde

- si dicho atributo define una duración temporal, esta duración es un tiempo de vida de menos de 24 horas, preferiblemente de menos de 1 hora,
- si dicho atributo define un número predeterminado de sesiones de comunicación, dicho número de sesiones de comunicación es uno,

- si dicho atributo define un número predeterminado de acciones, dicho número de acciones es uno.

9. Método según la reivindicación 8, donde dicha acción se define como un periodo activo de un navegador web funcionando en cliente (2(n)).

10. Método según cualquiera de las reivindicaciones precedentes, donde dicha acción de autenticación es realizada al menos por un servicio de autenticación interno a dicho servidor de seguridad (4) y un servicio de autentificación (8) externo a dicho servidor de seguridad (4).

11. Método según cualquiera de las reivindicaciones precedentes, donde dicha clave pública (PuK(i)) y dicha clave privada (PrK(i)) son copias de claves de un conjunto de claves almacenado centralmente que permanece almacenado una vez dicha clave pública (PuK(i)) y dicha clave privada (PrK(i)) se han hecho disponibles y donde dichas copias de dichas claves se hacen disponibles una o más veces.

12. Sistema que comprende un cliente (2(n)), un servidor de seguridad (4) y una disposición informática de un tercero (2(n'): 6) en el que:

a) dicho cliente (2(n)) y dicho servidor de seguridad (4) están dispuestos para establecer una sesión de comunicación inicial segura y codificada entre sí a través de una red de comunicación pública que conecta dicho cliente (2(n)) y dicho servidor de seguridad (4) mientras usa un software de aplicación de cliente que está instalado en el cliente (2(n));

b) dicho servidor de seguridad (4) está dispuesto para controlar en dicha sesión de comunicación inicial segura y codificada la autenticación del usuario de dicho cliente (2(n)) mientras usa un protocolo de autenticación con un nivel de seguridad predeterminado;

c) dicho servidor de seguridad (4) está dispuesto para transmitir, en dicha sesión de comunicación inicial segura y codificada, a dicho cliente (2(n)) una clave privada (PrK(i)) y un certificado digital que comprende una clave pública (PuK(i)) y uno o más atributos. Dicha clave privada (PrK(i)) está asociada a dicha clave pública (PuK(i)), y dicho certificado digital y dicha clave privada están asociados a dicho cliente (2(n));

d) dicho cliente (2(n)) está dispuesto para instalar automáticamente dicho certificado digital y clave privada en dicha sesión de comunicación inicial segura y codificada;

e) dicho cliente (2(n)) y dicha disposición informática de un tercero (2(n'); 6) están dispuestos para realizar una transmisión segura de datos en una sesión de comunicación entre sí mientras usan dicha clave pública (PuK(i)) y dicha clave privada (PrK(i)):

donde dicho sistema comprende un procesador para identificar que dicho certificado digital tiene un tiempo de vida limitado definido por al menos un atributo y para eliminar dicho certificado digital al término de dicho tiempo de vida, y dicho atributo define al menos uno de los siguientes:

- una duración de tiempo predeterminada;
- un número de sesiones de comunicación predeterminado;
- un número de acciones predeterminado.

13. Sistema según la reivindicación 12, donde el sistema está dispuesto para realizar cualquiera de los métodos según las reivindicaciones de la 2 a la 11.

14. Servidor de seguridad que comprende un procesador y una memoria, la memoria almacenando datos e instrucciones para que dicho procesador ejecute un programa informático predeterminado, dicho programa permitiendo que dicho servidor de seguridad:

a) establezca una sesión de comunicación inicial segura y codificada con un cliente (2(n)) a través de una red de comunicación pública que conecta dicho cliente (2(n)) y dicho servidor de seguridad (4) mientras usa un software de aplicación de cliente instalado en el cliente (2(n);

b) en dicha sesión de comunicación inicial segura y codificada, autentique al usuario de dicho cliente (2(n)) mientras usa un protocolo de autenticación con un nivel de seguridad predeterminado:

c) en dicha sesión de comunicación inicial segura y codificada, transmita a dicho cliente (2(n)) una clave privada (PrK(i)) y un certificado digital que comprende una clave pública (PuK(i)) y uno o más atributos, estando dicha clave privada (PrK(i)) asociada a dicha clave pública (PuK(i)), y dicho certificado digital y dicha clave privada estando asociadas a dicho cliente (2(n));

donde dicho certificado digital tiene un tiempo de vida limitado definido por al menos un atributo,

dicho atributo definiendo al menos uno de los siguientes:

- una duración de tiempo predeterminada;

- un número de sesiones de comunicación predeterminado;
- un número de acciones predeterminado.

15. Cliente (2(n)) que comprende un procesador y una memoria, la memoria almacenando datos e instrucciones para que dicho procesador ejecute un programa informático predeterminado, dicho programa permitiendo que dicho cliente (2(n)):

a) configure una sesión de comunicación inicial segura y codificada con un servidor de seguridad (4) a través de una red de comunicación pública que conecta dicho cliente (2(n)) y dicho servidor de seguridad (4) mientras usa un software de aplicación de cliente instalado en el cliente (2(n));

b) después de ser autenticado con un nivel de seguridad predeterminado, reciba, en dicha sesión de comunicación inicial segura y codificada, un certificado digital que comprende una clave pública (PuK(i)) y uno o más atributos, y reciba una clave privada (PrK(i)) asociada a dicha clave pública (PuK(i));

c) instale automáticamente en dicha sesión de comunicación inicial segura y codificada, dicho certificado digital y clave privada;

d) realice una transmisión de datos segura en una sesión de comunicación entre dicho cliente (2(n)) y una disposición informática de un tercero <2(n'): 6) mientras usa dicha clave pública (PuK(i)) y dicha clave privada (PrK(i));

donde dicho cliente (2(n)) comprende un procesador para identificar que dicho certificado digital tiene un tiempo de vida limitado definido por al menos un atributo y para eliminar dicho certificado digital al término de dicho tiempo de vida, dicho atributo definiendo al menos uno de los siguientes:

- una duración de tiempo predeterminada;
- un número de sesiones de comunicación predeterminado;
- un número de acciones predeterminado.

16. Método que realiza una transmisión de datos segura en una sesión de comunicación entre un cliente (2(n)) y una disposición informática de un tercero (2(n')); 6), que comprende en dicho cliente (2(n)):

a) el establecimiento de una sesión de comunicación inicial segura y codificada con un servidor de seguridad (4) a través de una red de comunicación pública que conecta dicho cliente (2(n)) y dicho servidor de seguridad (4) mientras usa un software de aplicación de cliente instalado en el cliente (2(n));

b) después de ser autenticado con un nivel de seguridad predeterminado, la recepción en dicha sesión de comunicación inicial segura y codificada de un certificado digital que comprende una clave pública (PuK(i)) y uno o más atributos, y la recepción de una clave privada (PrK(i)) asociada a dicha clave pública (PuK(i)):

c) la instalación automática en dicha sesión de comunicación inicial segura y codificada de dicho certificado digital y clave privada;

d) la realización de una transmisión segura de datos en una sesión de comunicación entre dicho cliente (2(n)) y una disposición informática de un tercero (2(n')); 6) mientras usa dicha clave pública (PuK(i)) y dicha clave privada (PrK(i));

e) la identificación de que dicho certificado digital tiene un tiempo de vida limitado definido por al menos un atributo y la eliminación de dicho certificado digital al término de dicho tiempo de vida, y dicho atributo define al menos uno de los siguientes:

- una duración de tiempo predeterminada;
- un número de sesiones de comunicación predeterminado;
- un número de acciones predeterminado.

17. Servidor de seguridad tal y como se define en la reivindicación 14, donde dicha sesión de comunicación inicial segura y codificada usa el protocolo Diffie-Hellman.

18. Cliente (2(n)) tal y como se define en la reivindicación 14, donde dicha sesión de comunicación inicial segura y codificada usa el protocolo Diffie-Hellman.

19. Método tal y como se define en la reivindicación 16, donde dicha sesión de comunicación inicial segura y codificada usa un protocolo Diffie-Hellman.

Fig 1

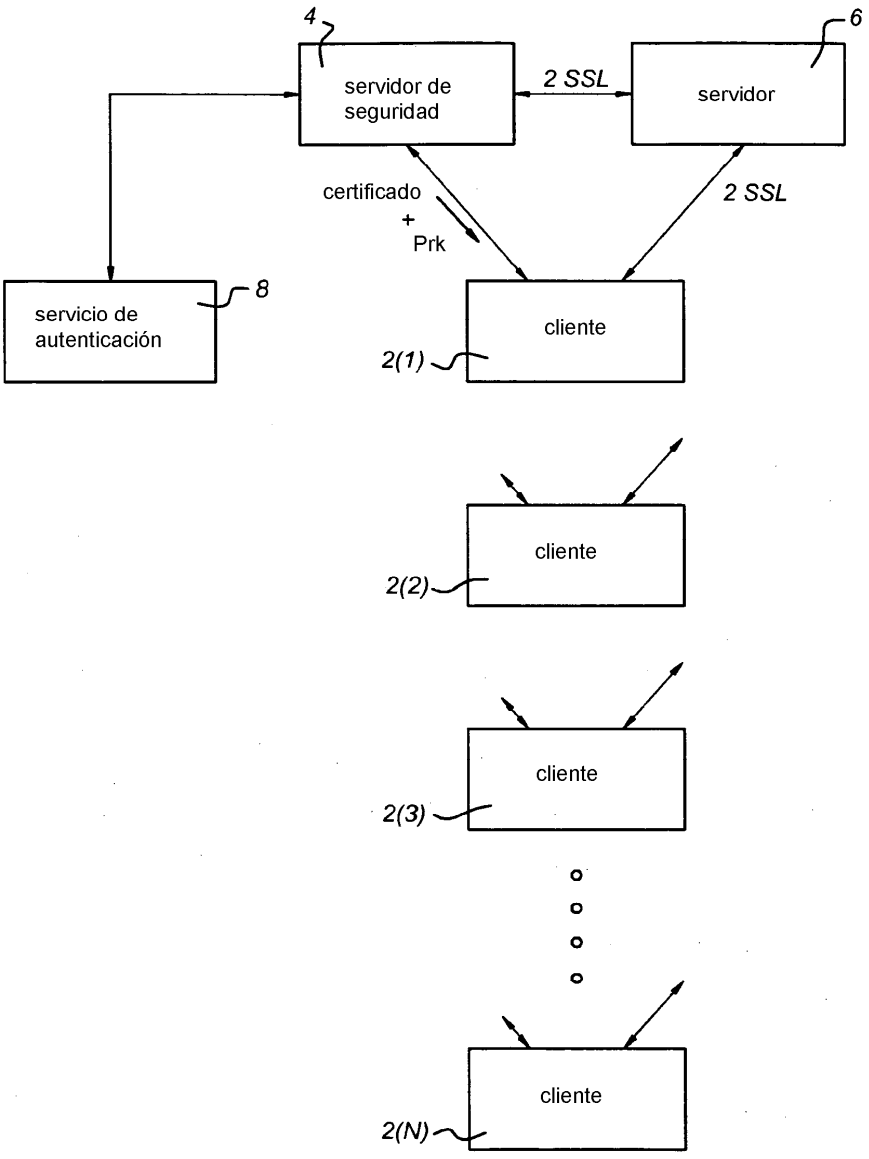

4
servidor de seguridad
2 SSL
6
servidor
certificado
+
Prk
2 SSL
8
servicio de autenticación
cliente
2(1)
cliente
2(2)
cliente
2(3)
cliente
2(N)

Fig 2

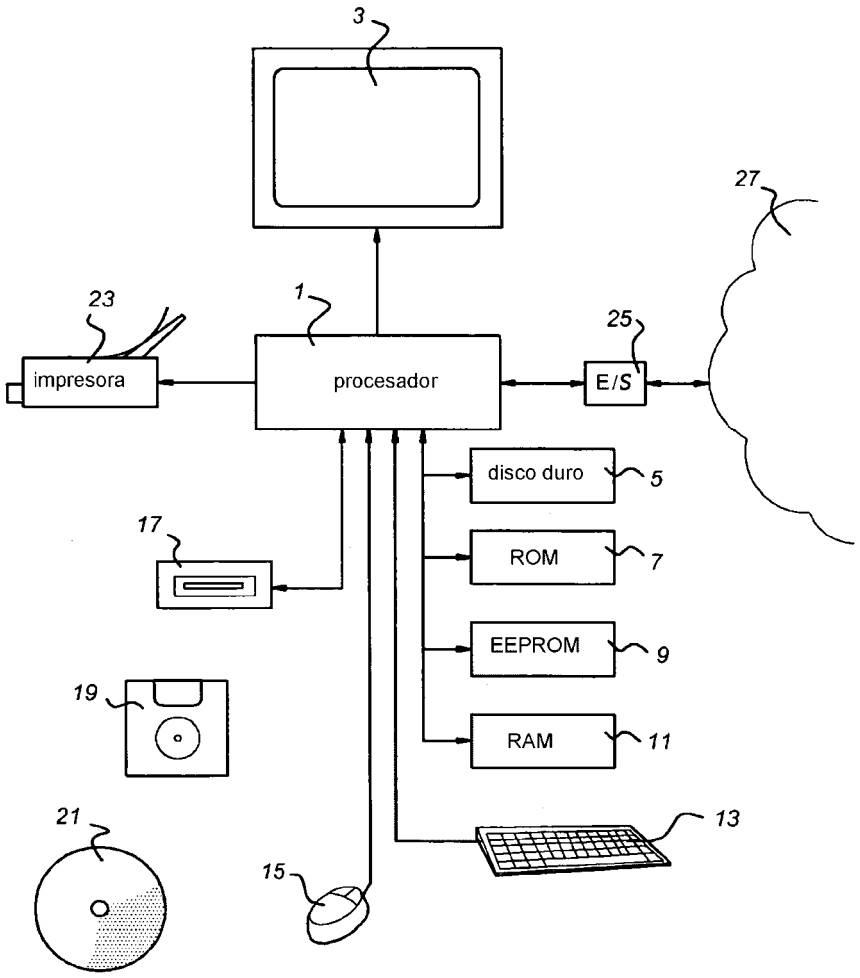
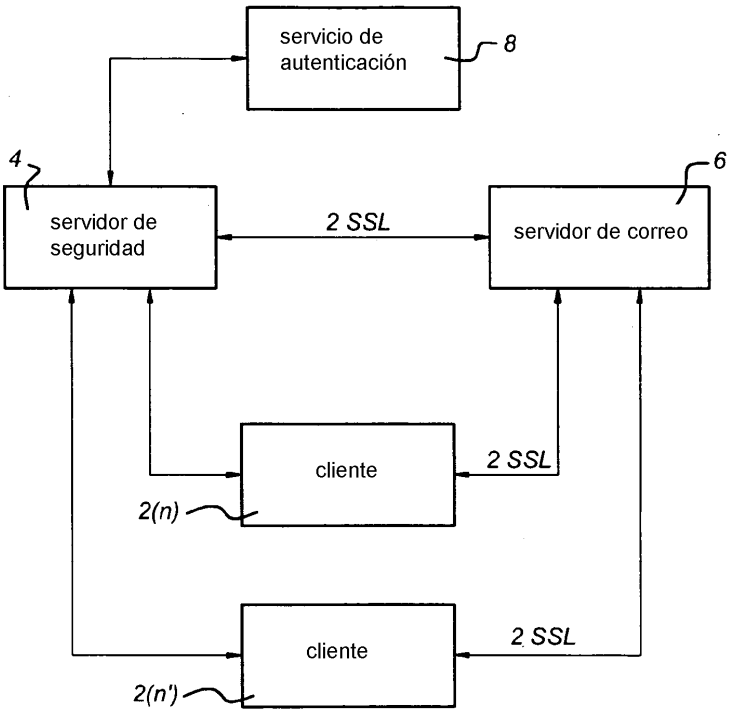

3
27
23
1
25
impresora
procesador
E/S
disco duro
5
17
ROM
7
EEPROM
9
19
RAM
11
21
13
15

Fig 3


servicio de autenticación
8
4
6
servidor de seguridad
2 SSL
servidor de correo
cliente
2 SSL
2(n)
cliente
2 SSL
2(n')