(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 794 087**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
H04W 12/04 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **10.04.2012 PCT/US2012/032840**

(87) Fecha y número de publicación internacional: **04.07.2013 WO13101286**

(96) Fecha de presentación y número de la solicitud europea: **10.04.2012 E 12862057 (2)**

(97) Fecha y número de publicación de la concesión europea: **08.04.2020 EP 2700003**

(54) Título: **Gestión de claves mediante arquitectura de autenticación cuasi fuera de banda**

(30) Prioridad:

19.04.2011 US 201113089430

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.11.2020

(73) Titular/es:

EARLY WARNING SERVICES, LLC (100.0%)
16552 N. 90th Street, Suite 100
Scottsdale, Arizona 85260, US

(72) Inventor/es:

RAVI, GANESAN

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Gestión de claves mediante arquitectura de autenticación cuasi fuera de banda

SOLICITUDES RELACIONADAS

[0001] Esta solicitud está relacionada con la solicitud pendiente n.º de serie 13/081,150, presentada el 6 de abril de 2011 y titulada "FLEXIBLE QUASI OUT OF BAND AUTHENTICATION ARCHETECTURE", que reivindica la prioridad basada en la solicitud provisional de EE. UU. n.º de serie 61/334,776, presentada el 14 de mayo de 2010. Esta solicitud también está relacionada con la solicitud pendiente n.º de serie 13/081,067, presentada el 6 de abril de 2011 y titulada "SECURE AND EFFICIENT LOGIN AND TRANSACTION AUTHENTICATION USING IPHONES™ AND OTHER SMART MOBILE COMMUNICATION DEVICES", que reivindica la prioridad basada en la solicitud provisional de EE. UU. n.º de serie 61/327,723, presentada el 26 de abril de 2010. Esta solicitud también está relacionada con la solicitud pendiente n.º de serie 12/938,161, presentada el 2 de noviembre de 2010 y titulada "A NEW METHOD FOR SECURE SITE AND USER AUTHENTICATION", que reivindica la prioridad basada en la solicitud provisional de EE. UU. n.º de serie 61/257,207, presentada el 2 se noviembre noviembre de 2009 y titulada "Project Seal". Esta solicitud también está relacionada con la solicitud pendiente n.º de serie 13/006,806, presentada el 14 de enero de 2011 y titulada "A NEW METHOD FOR SECURE USER AND SITE AUTHENTICATION", que es una continuación de la solicitud pendiente n.º de serie 12/938,161. Esta solicitud también está relacionada con la solicitud pendiente n.º de serie 13/011,587, presentada el 21 de enero de 2011, y titulada "A NEW METHOD FOR SECURE USER AND TRANSACTION AUTHENTICATION AND RISK MANAGEMENT", que reivindica la prioridad basada en la solicitud provisional de EE. UU. n.º de serie 61/298,551, presentada el 27 de enero de 2010 y titulada "Authentication-The Game Changer". Esta solicitud también está relacionada con la solicitud n.º de serie 13/011,739, presentada el 21 de enero de 2011, y titulada "A NEW METHOD FOR SECURE USER AND TRANSACTION AUTHENTICATION AND RISK MANAGEMENT", que es una continuación en parte de solicitud pendiente n.º de serie 13/011,587.

CAMPO TÉCNICO

[0002] Esta invención está relacionada con la seguridad y la privacidad. Más particularmente, se refiere al uso de la arquitectura de autenticación cuasi fuera de banda (QOOBA, *Quasi Out of Band Authentication Arquitecture*) para la gestión de claves.

ANTECEDENTES DE LA INVENCIÓN

[0003] La creciente sofisticación de los ataques específicos del sitio web basados en las técnicas *man-in-the-middle* (MITM) y *man-in-the-browser* (MITB) tiene profundas implicaciones para nuestras técnicas de autenticación actuales. Específicamente, la fuerza de la autenticación de inicio de sesión es cada vez menos relevante a medida que estos ataques manipulan las transacciones después de que el usuario legítimo haya proporcionado las credenciales iniciales para iniciar sesión. En reacción a esta tendencia, las principales organizaciones han empezado a desplegar sistemas de autenticación de transacción, tales como los autenticadores de *tokens* basados en EMV-CAP, o han estado usando técnicas de autenticación fuera de banda (OOBA, *Out of Band Authentication*) para asegurar que el usuario en realidad pretendía que la transacción se viera en el *back-end*. Sin embargo, tales enfoques no son intrínsecamente fáciles de usar y, en consecuencia, incluso cuando se despliegan, se usan generalmente solo para transacciones de alto riesgo o eventos ocasionales como cambios de perfil. Para la gran mayoría de transacciones, ninguna solución de autenticación actual proporciona un punto razonable en el intercambio "¿Cómo de fácil? ¿Cómo de seguro? ¿Cómo de caro?".

[0004] La US 6,223,287 B1 divulga un método para establecer un canal de comunicación asegurado entre un cliente y un servidor, donde un programa y un conjunto de información de encriptación para establecer el canal de comunicación asegurado se entregan del servidor al cliente. El conjunto de información de encriptación es compacto y se puede usar para cifrar y descifrar datos rápida y eficazmente. En particular, el cliente solicita un programa desde el servidor a través de un primer canal de comunicación asegurado que se puede establecer a través de un navegador web bajo el protocolo HTTPS (*Hypertext Transfer Protocol with SSL* o protocolo de transferencia de hipertexto con SLL). En respuesta, el servidor genera dinámicamente un conjunto de información de encriptación y un *token* que identifica este conjunto particular de información de encriptación. Esta información se envía posteriormente con el programa solicitado. Si bien el programa se puede escribir en cualquier lenguaje, el lenguaje de elección es un lenguaje independiente de la plataforma, como Java. Cuando el programa se ejecuta en el cliente y ejecuta sus tareas programadas, una de las tareas es establecer un canal de comunicación separado y asegurado con el servidor que usa la información de encriptación desde el servidor.

[0005] De la US 2007/0234061 A1 se conoce un sistema de red, que comprende una red de transacciones operativa para proporcionar una transacción con un usuario final; una fuente de confianza de un mecanismo de seguridad (por ejemplo, un módulo de disparo de arranque/paro, un módulo de bloqueo de aplicaciones, un módulo de control de red/archivo I/O, un administrador de controladores fiable, un controlador de generador de pulsaciones de teclas, un *hook* de eliminación de pulsaciones de teclas, y/o un administrador de red de transacciones VPN)

para proteger al menos parcialmente un dispositivo de usuario final del código malicioso operativo al respecto que intenta capturar datos confidenciales presentados durante la transacción, donde el mecanismo de seguridad es mantenido por una parte diferente del usuario final; y un agente para proporcionar el mecanismo de seguridad al dispositivo de usuario final para proteger el dispositivo de usuario final durante la transacción.

[0006] En la US 2009/0259848 A1 se revelan los sistemas y métodos para usar la autenticación fuera de banda para confirmar la identidad electrónica aseverada de un individuo y controlar la liberación de una clave criptográfica. Cuando se confirma a un nivel muy alto de confianza que la identidad electrónica aseverada es la registrada para el individuo, estos confirman que una persona que realiza una transacción es quien dice ser al confirmar, en primer lugar, algo que sabe, usando un nombre de usuario y contraseña (o solo un nombre de usuario) como un *token* de conocimiento compartido, y, al confirmar, en segundo lugar, algo que ella tiene, el artículo registrado para ella, y en tercer lugar, al confirmar el hecho de que ella tiene control sobre ese artículo. Una vez que se han establecido cada una de estas confirmaciones, una clave criptográfica puede ser liberada por el proceso de autenticación fuera de banda. La clave criptográfica liberada será específica para el individuo o será específica para el sistema que en realidad libera la clave. Si el sistema libera una clave que no es específica para el individuo, la asociación con el individuo que autenticó la liberación de la clave, por lo que se establece el no repudio de la clave, será proporcionada por la asociación de la transmisión específica de la clave del sistema con la transacción de autenticación única a través del registro auditable. La clave criptográfica liberada por la autenticación fuera de banda puede ser simétrica o asimétrica, es decir, se puede usar una clave para generar un código de autenticación de mensaje y para verificar el código, o dos claves relacionadas, una clave pública y una clave privada, se puede usar para la generación de firma y la verificación de firma, respectivamente.

[0007] La US 2005/0071282 A1 enseña un sistema y un método para efectuar transacciones seguras a través de una red de ordenador diseñada de una manera para detener el robo de identidad perpetrado desde un ordenador no fiable. Una conexión desde un ordenador cliente a la red donde el ordenador cliente proporciona una interfaz de usuario para un usuario, una conexión desde un ordenador servidor a la red, y una conexión desde un dispositivo informático seguro portátil a la red proporciona una transmisión segura de información de usuario confidencial privada del usuario a un servidor. La información privada se transmite directamente del dispositivo informático seguro al servidor a través de la conexión segura sin posibilidad de capturarla en el ordenador con el cual el usuario está interactuando.

[0008] La US 7,861,077 B1 A enseña un sistema de autenticación de usuario seguro y operable a través de una red de comunicaciones cliente-servidor para autenticar a un usuario del sistema. El sistema incluye un servidor de aplicaciones, que incluye un sitio web que puede habilitarse, y un servidor de autenticación, que puede habilitar el sitio web del servidor de aplicaciones. El servidor de autenticación incluye una base de datos central, y recibe y almacena los datos que habilitan la autenticación del usuario en la base de datos central. El sistema incluye además un cliente y un programa cliente que puede actuar en el cliente. El programa cliente incluye los datos que habilitan la autenticación del usuario. Tras la activación, el programa cliente se conecta automática y directamente al servidor de autenticación y envía los datos que habilitan la autenticación del cliente al servidor de autenticación para la autenticación de usuario segura por parte del servidor de autenticación.

[0009] En los trabajos anteriores (véanse las solicitudes relacionadas identificadas anteriormente) describimos innovaciones que abordan algunos de los problemas con los sistemas de autenticación convencionales. Específicamente, introdujimos la noción de usar las técnicas de QOOBA para asegurar que el usuario pretendía realmente que la transacción se viera en el *back-end*. También describimos cómo estas técnicas se pueden usar para proporcionar a un usuario una contraseña de un solo uso (OTP, *One-Time Password*) para permitir el inicio de sesión en un sitio web (es decir, la autenticación del usuario en el sitio web), basada en un secreto compartido entre el sitio web y un servidor de seguridad de QOOBA. Por lo tanto, estas técnicas se pueden usar para proporcionar la seguridad de las contraseñas de un solo uso, pero no requieren un secreto compartido por el usuario que todos los sistemas de contraseñas de un solo uso previos han requerido.

[0010] También ampliamos nuestros trabajos anteriores para abordar el problema de proporcionar una solución de autenticación para la gran mayoría de transacciones en un punto razonable en la compensación "¿Cómo de fácil? ¿Cómo de seguro? ¿ Cómo de caro?".

[0011] En este documento ampliamos nuestros trabajos anteriores para considerar las soluciones al problema de gestión de claves que surge en varios contextos. Tres de muchos ejemplos potenciales incluyen los siguientes.

[0012] A continuación, describiremos varios ejemplos de cómo la gestión de claves se puede aplicar beneficiosamente a una arquitectura QOOBA. Nuestros primeros ejemplos se refieren a la firma digital. En las aplicaciones que requieren la firma digital, un usuario necesita estar provisto de una clave privada y un certificado digital, es decir, un enlace de la identidad y la clave publica del usuario como certificada por una autoridad de certificado. El uso de dicha clave privada, que no es conocida por ningún tercero, incluido el servidor de seguridad, proporciona un fuerte no repudio que es necesario para algunas aplicaciones. Seguimos la convención de la industria de referirse a las firmas creadas con criptografía de clave pública como "firmas digitales". Como entenderán los expertos en la técnica, las firmas basadas en criptografía simétrica subyacente con secretos

compartidos, como la que ya proporciona el sistema de QOOBA descrito anteriormente, se denominan normalmente "firmas electrónicas".

[0013] Nuestro segundo ejemplo se refiere a la entrega de documentos encriptados. Cuando un archivo encriptado se envía a un usuario, por ejemplo un PDF de una declaración de corretaje, el usuario necesita estar provisto de la clave con la que se encriptó el archivo.

[0014] Nuestro tercer ejemplo hace referencia a autenticadores de *tokens*. Cuando a los usuarios se les proporciona un autenticador de *tokens*, ya sea para un generador de contraseña de un solo uso o para un autenticador de transacciones, el *token* del usuario necesita estar provisto de una clave secreta compartida. Los expertos en la técnica reconocerán que, en este contexto, la clave secreta compartida se caracteriza a menudo como una "semilla".

[0015] En todos estos ejemplos, la gestión de claves se añade directamente al coste del sistema y afecta indirectamente a la seguridad. Las claves deben generarse, distribuirse y mantenerse en sincronización. Como las claves pueden perderse, dañarse o ser robadas, la gestión de claves es normalmente una fuente significativa de costes y un punto de vulnerabilidad en el sistema.

OBJETIVOS DE LA INVENCIÓN

[0016] Por consiguiente, un objetivo de la presente invención es proporcionar una forma innovadora de aprovechar el sistema de QOOBA para realizar la gestión de claves para la gestión de la firma digital, de la encriptación y de la semilla de *token*.

[0017] Los objetos, las ventajas y las nuevas características adicionales de la presente invención se harán evidentes para los expertos en la técnica a partir de esta divulgación, que incluye la siguiente descripción detallada, así como por la práctica de la invención. Si bien la invención se describe abajo con referencia a la(s) forma(s) de realización(s) preferida(s), debe entenderse que la invención no está limitada a la(s) misma(s). Los expertos en la técnica que tengan acceso a las instrucciones del presente documento reconocerán aplicaciones, modificaciones y formas de realización adicionales, así como otros campos de uso, que están dentro del alcance de la invención, como se describe y reivindica aquí y con respecto a los cuales la invención podrían ser de gran utilidad.

DIVULGACIÓN RESUMIDA DE LA INVENCIÓN

[0018] La presente invención está definida por las reivindicaciones independientes. Las formas de realización ventajosas se describen en las reivindicaciones dependientes, la siguiente descripción y los dibujos.

[0019] Conforme a determinados aspectos preferidos de la invención, se puede operar un servidor de seguridad para proporcionar la gestión de claves aplicada al sistema de autenticación cuasi fuera de banda. Una solicitud de activación de una ventana de interfaz de usuario para un usuario particular en un dispositivo de red, tal como un ordenador de sobremesa, asociada a ese usuario se recibe del dispositivo de red a través de un canal de comunicación. En este punto, el canal de comunicación no es seguro o lo que a veces se denomina "claro". Los expertos en la técnica reconocerán que tener un canal no seguro en este punto en un protocolo de comunicación no es inusual. Por ejemplo, cuando un usuario inicia comunicaciones con un sitio web protegido por SSL, inicialmente se establece una conexión TCP/IP insegura o clara, y solo más tarde se establece la seguridad SSL sobre la conexión TCP/IP no segura o clara.

[0020] Posteriormente, para autenticar al usuario en el servidor de seguridad, se transmite un PIN de activación (*Personal Identification Number* o número de identificación personal) a un sistema de autenticación fuera de banda (OOBA) para reenviarlo al teléfono del usuario mediante un mensaje de voz o texto. Por ejemplo, el sistema de OOBA puede realizar una llamada a la casa o al teléfono móvil del usuario, y trasmitir el PIN verbalmente al usuario, o puede enviar un mensaje de texto al teléfono inteligente del usuario, por ejemplo IPhone™ o Blackberry™ del usuario, y transmitir el PIN al usuario por escrito. En cualquier caso, el usuario debe introducir, es decir, copiar, el PIN transmitido en la ventana de la interfaz de usuario para que se devuelva al servidor de seguridad. De esta manera, el PIN transmitido previamente por el servidor de seguridad al sistema de OOBA es recibido de vuelta por el servidor de seguridad del dispositivo de red del usuario a través del canal de comunicación, y el usuario se autentica, o se rechaza la autenticación, en función del PIN devuelto.

[0021] En función de que el usuario sea autenticado por el servidor de seguridad, se establece un canal de comunicación seguro, independiente y encriptado entre la ventana de interfaz de usuario y el servidor de seguridad sobre el canal de comunicación originalmente establecido. Con este canal seguro establecido, entre la ventana de interfaz de usuario y el servidor de seguridad se puede generar y/o transmitir, de manera segura, el material de clave y/o el material de certificado para operaciones basadas en criptografía de clave pública y/o clave simétrica. Quizás valga la pena señalar aquí que el material de clave y el material de certificado son términos bien entendidos en la técnica. Por ejemplo, el material de clave a menudo incluye claves simétricas o claves asimétricas y el material de certificado a menudo incluye la identidad del usuario y el enlace de clave pública.

[0022] En implementaciones que implican la generación y la transmisión de material de certificado para criptografía de clave pública, el servidor de seguridad recibe preferiblemente una clave pública Pu de un par de claves privada/pública Du/Pu asociado al usuario y generado previamente por la ventana de interfaz de usuario. La clave pública Pu se recibe de la ventana de interfaz de usuario a través del canal de comunicación seguro, independiente y encriptado. En respuesta, el servidor de seguridad transmite un certificado firmado, que asocia al usuario con la clave pública Pu recibida y las instrucciones para el almacenamiento del certificado, y ambos van a la ventana de interfaz de usuario a través del canal seguro.

[0023] El certificado puede ser firmado por el propio servidor de seguridad o por una autoridad de autenticación externa, como una autoridad de certificado de terceros. Si el servidor de seguridad actúa como una autoridad de certificado intermedia o raíz, el servidor de seguridad preferiblemente genera y firma el certificado usando material de clave de la autoridad de certificado almacenado localmente. Si, por otro lado, el certificado es firmado por una autoridad de certificado externa, el servidor de seguridad envía preferiblemente un certificado sin firmar a la autoridad de certificado externa y recibe el certificado firmado de la autoridad de certificado. En tal caso, este es el certificado firmado por la autoridad de certificado externa que es transmitida por el servidor de seguridad a la ventana de interfaz de usuario.

[0024] La instrucción de almacenamiento transmitida puede requerir, dependiendo de la implementación, el almacenamiento de la clave privada Du y el certificado firmado del usuario en la memoria del dispositivo de red del usuario o en el almacenamiento de claves de un sistema operativo, tal como el sistema operativo Windows™, del dispositivo de red, o ambos. Alternativamente, la instrucción de almacenamiento transmitida puede dejar explícita o implícitamente la decisión de almacenamiento a la ventana de interfaz de usuario. Por ejemplo, si no se proporciona ninguna instrucción de almacenamiento, la ventana de interfaz de usuario puede considerar que es una instrucción implícita de que corresponde a la ventana de interfaz de usuario decidir dónde almacenar la clave privada Du y el certificado del usuario. El almacenamiento puede ser solo para el beneficio de la ventana de interfaz de usuario o también puede ser para el beneficio de otras aplicaciones locales, que pueden incluir la aplicación del navegador.

[0025] En implementaciones que implican la generación y transmisión por parte del servidor de seguridad de material de clave para operaciones de criptografía de clave simétrica, el servidor de seguridad recibe, de manera beneficiosa, una solicitud autenticada que contiene información de identificación única asociada al usuario o a un archivo, es decir, un documento, tal como un archivo o documento de Adobe™ o WinZip™. Esta información se puede recibir de la ventana de interfaz de usuario o de un sitio de red de terceros, tal como un sitio web comercial o bancario. Independientemente de la entidad de la cual se recibe la solicitud, el servidor de seguridad genera una única clave simétrica K. La clave K se genera usando una función unidireccional, y el valor de la clave se deriva de la información de identificación única recibida y de un secreto conocido solo por el servidor de seguridad. El servidor de seguridad transmite la clave simétrica K al solicitante, es decir, a la ventana de interfaz de usuario o al sitio de red de terceros.

[0026] En implementaciones que involucran al servidor de seguridad que realiza operaciones de criptografía de clave pública para obtener una firma digital en una transacción, el servidor de seguridad recibe ventajosamente la transacción y una solicitud de firma digital de la transacción de un sitio de red de terceros, tal como un sitio web comercial o banquero. El servidor de seguridad transmite la transacción y una solicitud de una firma digital a la ventana de interfaz de usuario a través del canal seguro. En respuesta, el servidor de seguridad recibe, de la ventana de interfaz de usuario, un *hash* de la transacción transmitido y firmado digitalmente con la clave privada Du del usuario a través del canal seguro. El servidor de seguridad transmite posteriormente el *hash* de la transacción recibido y firmado digitalmente y un certificado para el sitio de red de terceros. El servidor de seguridad también transmite instrucciones para que el sitio de red de terceros verifique la firma digital recalculando el *hash* y comparándolo con el *hash* que se puede recuperar del *hash* transmitido y firmado digitalmente al aplicar la clave pública Pu del usuario incluida en el certificado transmitido al *hash* transmitido y firmado digitalmente. Esta instrucción puede ser explícita o implícita. Por ejemplo, el servidor de seguridad no puede proporcionar ninguna instrucción con respecto a la verificación y esto puede ser considerado por el sitio de red de terceros como una instrucción implícita para realizar la verificación de la manera descrita al respecto.

[0027] Incluso si se requiere una firma digital, puede ser deseable obtener también la firma electrónica del usuario en la transacción. Si es así, el servidor de seguridad puede transmitir, a la ventana de interfaz de usuario para su presentación al usuario, un número de identificación personal (PIN) con el que firmar electrónicamente la transacción presentada en una ventana de navegador visualizada en el dispositivo de red del usuario. El PIN se transmite mediante el canal de comunicación seguro, independiente y encriptado. El usuario introduce el PIN transmitido, presentado en la ventana de interfaz de usuario, en una ventana de navegador, que se está comunicando con el sitio de red de terceros con el que el usuario está realizando la transacción comercial, para firmar electrónicamente la transacción. Es bastante preferible que el PIN corresponda a un secreto compartido por el servidor de seguridad y por el sitio de red de terceros, pero no por el usuario.

[0028] La transacción transmitida puede incluir o no una instrucción para presentar la transacción al usuario en la ventana de interfaz de usuario y/o para obtener la aprobación del usuario antes de firmar digitalmente la transacción. Aquí nuevamente, la instrucción puede ser explícita o implícita. Por ejemplo, en el caso de aprobación, la aprobación del usuario de la transacción puede requerir que el usuario haga clic en un botón aprobado presentado en la ventana de interfaz de usuario, antes de que la ventana de interfaz de usuario firme digitalmente la transacción. Alternativamente, la aprobación puede ser señalada por el usuario al no rechazar la transacción presentada en la ventana de interfaz de usuario dentro de un periodo de tiempo predefinido después de que la transacción se presente por primera vez en la ventana de interfaz de usuario.

[0029] En el caso de firmas digitales, la ventana de interfaz de usuario puede administrar el almacenamiento de la clave privada Du del usuario y del certificado firmado en la memoria o en el almacenamiento de claves de un sistema operativo del dispositivo de red, o en ambos, en beneficio de otras aplicaciones locales. El servidor de seguridad también puede verificar la firma digital antes de transmitir el *hash* de la transacción recibido y firmado digitalmente y el certificado para el sitio de red de terceros. Para verificar la firma, el servidor de seguridad recalcula el *hash* de la transacción y lo compara con el *hash* recuperado del *hash* recibido y firmado digitalmente al aplicar la clave pública Pu del usuario incluida en el certificado recibido para el *hash* de la transacción recibido y firmado digitalmente.

[0030] En implementaciones que involucran al servidor de seguridad que realiza operaciones basadas en criptografía de clave simétrica que incluyen compartir claves de encriptación, el servidor de seguridad recibe una solicitud de una o más claves de encriptación asociadas a combinaciones particulares de identificación del emisor, identificación del receptor e identificación del documento, que se denominan colectivamente DocumentID, de un sitio de red de terceros, por ejemplo un comerciante, un banco, el gobierno de EE.UU., etc.

[0031] El servidor de seguridad genera entonces una o más claves de encriptación simétricas para cada DocumentID. Las claves de encriptación simétricas se generan en base a una función unidireccional, la DocumentID aplicable, un secreto conocido solo por el servidor de seguridad y, si se desea, otra información comúnmente usada para generar claves criptográficas simétricas y bien conocidas por los expertos en la técnica. El servidor de seguridad transmite las claves de encriptación generadas al sitio de red de terceros, con instrucciones para encriptar el documento representado por la DocumentID aplicable con la(s) clave(s) apropiada(s) y para transmitir el documento encriptado al usuario. Aquí de nuevo, las instrucciones pueden ser explícitas o implícitas.

[0032] El servidor de seguridad recibe posteriormente una solicitud de la una o más claves de encriptación simétricas requeridas para desencriptar un documento representado por una DocumentID particular aplicable. La solicitud incluye la DocumentID aplicable y se recibe del *software*, que no sea la ventana de interfaz de usuario, que está funcionando en el dispositivo de red y se está usando para abrir un documento encriptado representado por una DocumentID aplicable. Por ejemplo, la solicitud se puede recibir de Adobe™ o WinZip™ o del *software* del navegador. En determinados casos, puede ser preferible recibir la solicitud directamente del *software*. Sin embargo, en otros casos puede ser preferible recibir la solicitud del *software* a través de un sitio de red que está en comunicación con el *software* que intenta abrir el documento.

[0033] El servidor de seguridad recalcula o recibe la una o más claves de encriptación simétricas aplicables. Este luego transmite la(s) clave(s) de encriptación aplicable(s) recalculada(s) o recibida(s) a la ventana de interfaz de usuario. Se transmiten con la(s) clave(s) aplicable(s) las instrucciones para presentar la(s) clave(s) aplicable(s) al usuario para copiarlas, es decir introducirlas, en el *software* para desencriptar el documento representado por la DocumentID aplicable. Aquí nuevamente, las instrucciones para la ventana de interfaz de usuario pueden ser explícitas o implícitas.

[0034] Si se recibe(n), la(s) clave(s) de encriptación simétricas aplicables se recibe(n) de un sitio de red en comunicación con el *software* que intenta abrir el documento, y la(s) clave(s) transmitida(s) a la ventana de interfaz de usuario son la(s) clave(s) recibida(s) por el servidor de seguridad del sitio de red. Si se recalcula(n), el servidor de seguridad recalcula la(s) clave(s) aplicable(s) basadas en la función unidireccional, la DocumentID aplicable, el secreto conocido solo por el servidor de seguridad y la otra información, y la(s) clave(s) transmitida(s) a la ventana de interfaz de usuario es(son) la(s) clave(s) recalculada(s).

[0035] En implementaciones que involucran al servidor de seguridad que realiza operaciones basadas en criptografía de clave simétrica para proporcionar una semilla para *hardware* o *software* del autenticador de *tokens*, el servidor de seguridad recibe una solicitud de una semilla de *token* de la ventana de interfaz de usuario. Junto con la solicitud de semilla de *token*, este también recibe un identificador de usuario y/o un identificador de *token* para el que se solicita la semilla.

[0036] El servidor de seguridad genera la semilla, en base a una función unidireccional, el identificador o los identificadores, un secreto conocido solo por el servidor de seguridad y otra información bien conocida por los expertos en la técnica. Este luego transmite, a la ventana de interfaz de usuario, la semilla generada con instrucciones explícitas o implícitas para presentar la semilla transmitida al usuario en la pantalla de ventana de

interfaz de usuario para que el usuario la introduzca en una interfaz de semilla del *token* o para introducir la semilla transmitida en la interfaz de semillas del *token* directamente sin intervención del usuario. Esta transmisión se realiza a la ventana de interfaz de usuario mediante el canal de comunicación seguro, independiente y encriptado. En determinadas aplicaciones, la semilla transmitida puede ser beneficiosamente una semilla intermedia, que será procesada por el *software* de *token* para generar la semilla final.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0037]

La figura 1 representa los componentes principales de la arquitectura de autenticación flexible cuasi fuera de banda, conforme a la presente invención.
La figura 2 muestra la arquitectura de autenticación flexible cuasi fuera de banda con la funcionalidad de gestión de claves aplicada a ella, conforme a la presente invención.

FORMA(S) DE REALIZACIÓN PREFERIDA(S) DE LA INVENCIÓN

Descripción general de los trabajos anteriores relacionados con la QOOBA

[0038] En los trabajos anteriores hemos descrito cómo la introducción de un servidor de seguridad basado en la red, que tiene un canal independiente de una ventana visualizada en un dispositivo de usuario, se puede usar junto con un navegador, un *software* de ordenador o un teléfono inteligente u otra aplicación del dispositivo de comunicación móvil del usuario, y el sitio web que están visitando para proporcionar la autenticación del usuario para el inicio de sesión o la autorización de transacciones a través de uno o más dispositivos de red del usuario.

[0039] La QOOBA es un enfoque innovador para crear una solución que se pueda usar para autenticar cada transacción de una manera que los usuarios sientan natural. La idea central es crear una pequeña ventana segura, la ventana de QOOBA, que tiene un canal encriptado independiente para un servidor seguro (el servidor de QOOBA). La ventana de QOOBA se puede implementar como una ventana emergente del navegador de descarga cero (la ventana emergente de QOOBA), como una pequeña aplicación de escritorio (la ventana de *software* de QOOBA) o como una aplicación en un teléfono inteligente (la ventana de teléfono de QOOBA). Un aspecto importante de la innovación es que, a diferencia de con los *tokens* blandos, la ventana de QOOBA no requiere ningún almacenamiento seguro de secretos a largo plazo. En su lugar, se "activa" durante el inicio de sesión usando la autenticación fuera de banda. A medida que un usuario realiza transacciones en un sitio web (por ejemplo, un sitio web comercial o bancario), que sea parte de la red de QOOBA, las transacciones que el sitio web cree que el usuario intenta realizar las envía de forma segura a través del navegador del usuario al servidor de QOOBA, que muestra la transacción en la ventana de QOOBA. Al usuario también se le muestra opcionalmente una firma de transacción que el usuario puede cortar y pegar de la ventana de QOOBA a su navegador para autenticar al sitio web para fines de inicio de sesión o de autorización de transacciones.

Descripción de trabajos anteriores acerca de una arquitectura QOOBA flexible

[0040] La solución de QOOBA tiene los siguientes beneficios en cuanto a facilidad de uso, coste total de propiedad y, de particular interés aquí, seguridad.

[0041] En primer lugar, con respecto a la facilidad de uso, el usuario no tiene dispositivo un nuevo para llevar o una contraseña para recordar, más allá de tener acceso al teléfono usado para la autenticación fuera de banda. El usuario no tiene que ingresar ningún código de transacción críptico en un dispositivo y escribir el resultado en el navegador. En cambio, el usuario ve toda la transacción en su ventana de QOOBA y puede copiar y pegar la firma de transacción con unos pocos clics.

[0042] En segundo lugar, con respecto al coste de total de propiedad, la arquitectura QOOBA reduce significativamente los costes totales del ciclo de vida. Esto no requiere ningún *hardware* nuevo y, a diferencia de un *token* blando, no requiere aprovisionamiento ni gestión de secretos por usuario. Además, como todas las comunicaciones entre el sitio web y el servidor de QOOBA se pueden realizar a través del navegador, los requisitos de integración en el sitio web son extremadamente leves. Los costes generales de la solución de QOOBA están diseñados para ser significativamente menores que un despliegue de *tokens* blandos equivalente, y mucho menores que los de un *token* físico.

[0043] Finalmente, en términos de seguridad, como también se explicará más adelante, el nivel de garantía depende del factor de forma de la ventana de QOOBA que se use. La ventana de QOOBA basada en el teléfono inteligente, es decir, la ventana de teléfono de QOOBA, proporciona la máxima garantía, pero incluso la ventana emergente de descarga cero, es decir, la ventana emergente de QOOBA, eleva significativamente la barra para un atacante. Es probable que la ventana de QOOBA de *software*, es decir, la ventana de *software* de QOOBA, sea satisfactoria para casi todos los niveles de riesgo.

[0044] En nuestros trabajos anteriores hemos descrito cómo, al implementar la solución de QOOBA usando una arquitectura QOOBA flexible, los sitios web en la red de QOOBA pueden solicitar o seleccionar el factor de forma y un tipo de aprobación de transacciones apropiado para la transacción. Por ejemplo, un usuario puede tener simultáneamente una ventana de QOOBA en su teléfono inteligente, así como en su escritorio. Mientras que la mayoría de transacciones se pueden enviar a la ventana de *software* de QOOBA de su escritorio (que es mucho más conveniente), las transacciones de mayor riesgo se pueden enviar a la ventana de teléfono de QOOBA de su teléfono inteligente. Se le puede pedir a un usuario que apruebe la mayoría de transacciones simplemente haciendo clic en un botón de aprobación, pero se le permite aprobar otras transacciones simplemente sin realizar ninguna acción y además otras transacciones colocando una firma electrónica segura en la transacción.

Superposición de gestión de claves en la arquitectura QOOBA

[0045] Ahora describimos cómo superponemos componentes para la gestión de claves en la arquitectura QOOBA.

El sistema de QOOBA

[0046] Con referencia ahora a la figura 1, de acuerdo con la presente invención, el sistema de QOOBA consiste en un dispositivo informático personal de escritorio 100 que tiene la ventana de QOOBA 110 y una ventana de navegador 112 que se ejecutan y se visualizan en el mismo, un servidor 125 y un servicio de web 150, que tiene la interfaz de programación de aplicaciones (API, *Application Programming Interface*) de QOOBA 155 operable en el mismo. Se debe entender que en una implementación práctica normalmente habría múltiples sitios web. También se incluye en el sistema, como se muestra, un servicio de OOBA 165, que es usado por el servidor de QOOBA 125 para iniciar la autenticación de *bootstrap* de usuario que usa el teléfono 175 del usuario, que puede ser un teléfono fijo, un teléfono móvil o un teléfono inteligente.

[0047] Como se describe con más detalle en las aplicaciones relacionadas a las que se hizo referencia anteriormente, el usuario activa la ventana de QOOBA 110, usando generalmente la autenticación fuera de banda a través del servicio de OOBA 165, y establece una sesión con el servidor de QOOBA 125. El servicio web 150 participa en la red de QOOBA y pasa por un único proceso de configuración para establecer un secreto compartido con el servidor de QOOBA 125, que no es compartido ni conocido por el usuario. Cuando el usuario tiene una sesión activa con el servidor de QOOBA 125 a través del canal de comunicación 450 y también se encuentra en el sitio web 150 a través del canal de comunicación 400, el sitio web puede usar la API de QOOBA 155 para solicitar, a través del canal de comunicación de *back-end* 500, la autenticación de transacciones enviando la transacción directamente al servidor de QOOBA 125. El servidor de QOOBA 125 muestra posteriormente la transacción al usuario en la ventana de QOOBA aplicable, que se muestra en la figura 1 como la ventana 110.

Las ventanas de QOOBA

[0048] El servidor de QOOBA 125 puede presentar diversa información al usuario en la ventana de QOOBA 110 visualizada. Por ejemplo, como hemos descrito en nuestros trabajos anteriores, el servidor de QOOBA 125 puede mostrar una transacción al usuario en la ventana de QOOBA 110, y si se solicita, mostrar también en la ventana de QOOBA 110 una transacción, es decir, una firma electrónica derivada de la transacción, el secreto compartido entre el servidor de QOOBA 125 y el sitio web 150, y otra información. Esto se logra a través del canal de comunicación 600. El usuario tiene la opción de aceptar o rechazar la transacción. La aceptación se puede señalar pasivamente al no realizar ninguna acción al hacer clic en ACEPTAR dentro de la ventana de QOOBA 110 y enviar una señal a través del canal de comunicación 600 de vuelta al servidor de QOOBA 125, o al copiar y pegar la firma de transacción de la ventana de QOOBA 110 a la aplicación web visualizada en la ventana de navegador 112 y luego enviada de vuelta al servicio web 150 a través del canal de comunicación 400. Si la firma de transacción de la ventana de QOOBA 110 se pega en la aplicación web visualizada en la ventana de navegador 112, el sitio web 150 puede verificar la firma usando la transacción, el secreto compartido entre el servidor de QOOBA 125 y el servicio web 150, y otra información.

[0049] Por lo tanto, un tipo aprobación se puede caracterizar como "INFORMAR". La transacción se muestra simplemente al usuario y no se requiere ninguna confirmación. Este es como un "flujo de actividad" y puede tranquilizar al usuario cauto. Otro tipo de aprobación se puede caracterizar como "CONFIRMAR". Se le pide al usuario que confirme o rechace la transacción dentro de la ventana de QOOBA 110 y esta respuesta se envía de vuelta al servicio web 150 a través del servidor de QOOBA 125. Otro tipo de aprobación más se puede caracterizar como "FIRMAR". El servidor de QOOBA 125 genera un número de identificación personal (PIN), que servirá como "firma de transacción", y se lo muestra al usuario dentro de la ventana de QOOBA 110 o de una ventana de QOOBA (no mostrada) en el teléfono inteligente. El usuario copia esta firma de transacción en su ventana de navegador 112 y la envía al servicio web 150. Como el PIN se deriva a partir de un secreto compartido entre el servidor de QOOBA 125 y el servicio web 150 (y nunca revelado al usuario), el servicio web 150 puede recalcular la firma de transacción de manera independiente y confirmar, de esta manera, la transacción. Se observará que esto logra el mismo efecto de seguridad de un sistema de autenticador de transacciones, pero no hay aprovisionamiento de secretos por usuario.

[0050] La interfaz de usuario al servidor de QOOBA 125 permanece en gran medida constante, independientemente del navegador y/o del sistema operativo (SO) que se utilice y el factor de forma de la ventana de QOOBA 110. El único caso de uso en el que la experiencia del usuario se desvía es cuando el usuario está navegando en un teléfono inteligente, donde la experiencia de QOOBA está optimizada para el dispositivo.

[0051] Como se ha indicado anteriormente, la ventana de QOOBA 110 se puede implementar en uno o al menos tres factores de forma, una ventana emergente del navegador, que comúnmente denominamos la ventana emergente de QOOBA, no requiere ninguna descarga de *software*, una aplicación pequeña que se instala en el escritorio, a lo que comúnmente llamamos la ventana de *software* de QOOBA, o una aplicación de teléfono inteligente, a lo que comúnmente llamamos la ventana de teléfono de QOOBA.

[0052] El mismo usuario podría estar usando diferentes factores de forma en diferentes momentos. Por ejemplo, un usuario que tiene la ventana de QOOBA de *software* instalada, y la usa la mayor parte del tiempo, podría usar la ventana de QOOBA emergente del navegador mientras está en algún otro escritorio (itinerancia). Para determinadas transacciones de alto riesgo, el sitio web podría requerir mostrar la transacción en la ventana de QOOBA del teléfono inteligente, mientras que la mayoría de transacciones se muestran en la ventana del escritorio. La apariencia de la ventana de QOOBA 110 puede ser personalizada completamente por la red de QOOBA particular. Una implementación para un banco destinada exclusivamente para sus propios sitios webs podría tener un aspecto muy diferente al de una implementación para un servicio de pago que ofrece autenticación en varios servicios web de comercio electrónico, como el servicio web 150. Aunque se describen numerosos elementos, se debe entender que la mayor parte de estos son opcionales.

Gestión de claves mediante la arquitectura QOOBA

[0053] Volviendo a la figura 2, en el centro del sistema de QOOBA se encuentra el establecimiento de un canal seguro, encriptado e independiente 600 entre la ventana de QOOBA en un escritorio 100 del usuario o la ventana de QOOBA en el teléfono inteligente 175 del usuario (no mostrado) y el servidor de seguridad de QOOBA 125. Como se ha descrito anteriormente, la ventana de QOOBA se utiliza para mostrar las transacciones de usuario y proporcionarles la oportunidad de confirmar, es decir, aprobar, la transacción.

[0054] Ahora presentamos en la arquitectura, como se muestra en la figura 1, la lógica-cliente de gestión de claves de QOOBA (KMLC) 610 en el escritorio 300 del usuario, la lógica-servidor de gestión de claves de QOOBA (KMLS) 620 en el servidor de seguridad de QOOBA 325, la lógica-API de gestión de claves de QOOBA (KMLAPI) 630 en el servicio web 350 y la posibilidad de un *software* de escritorio o de teléfono inteligente "sin navegador" (por ejemplo, Acrobat Reader) 314. Las KMLC 610 y KMLS 620 se comunican a través del canal seguro de QOOBA 600 entre la ventana de QOOBA 310 y el servidor de seguridad de QOOBA 325. Las KMLS 620 y KMLAPI 630 se comunican a través del canal de comunicación de *back-end* 500 entre el servidor de seguridad de QOOBA 325 y el servicio web 350.

[0055] Con referencia adicional a la figura 2, dentro del marco descrito anteriormente, la generación de claves procede de la siguiente manera. En algún momento, después de que se active la ventana de QOOBA 310, la KMLC 610 genera un par de claves privada/pública, por ejemplo, Du/Pu, y almacena la clave privada Du de forma segura (generalmente en la memoria). La KMLC 610 envía la clave pública Pu al servidor de QOOBA 325, donde la solicitud es interceptada por la KMLS 620. La KMLS 620 prepara un certificado digital ("Cert"), que incluye la clave pública Pu del usuario, y ocurre una de las dos cosas.

[0056] Si la KMLS 620 es capaz de actuar como una autoridad de certificado intermedia o raíz, esta firma el certificado y devuelve el certificado firmado a la KMLC 610, que lo mantiene localmente (preferiblemente en la memoria). Por ejemplo, la KMLS 620 podría firmar el Cert con la clave privada Ds de su par de claves privada/pública Ds/Ps, de manera que [Cert]Ds se devuelve a la KMLC 610.

[0057] Por otro lado, si la KMLS 620 actúa como una "autoridad de registro", esta reenvía la solicitud de certificado a una autoridad de certificado externa 900, que crea el certificado y lo devuelve a la KMLS 620, que a su vez reenvía el certificado de vuelta a 610, que lo mantiene localmente (preferiblemente en la memoria). En tal caso, el Cert será firmado por la autoridad de certificado con la clave privada Dca de su par de claves privada/pública Dca/Pca, de manera que [Cert]Dca se devuelve a la KMLS 620. La KMLS 620 reenvía posteriormente el Cert recibido firmado, es decir, [Cert]Dca, a la KMLC 610.

[0058] En cualquier caso, es preferible que el Cert expedido tenga una vida relativamente corta, es decir, temporal, y coincida con la vida de su propia sesión de QOOBA. Al hacer que sea simple la coincidencia de la generación de claves con la activación, se evita la necesidad de memorizar certificados digitales y claves privadas localmente durante un periodo prolongado.

[0059] En algunas situaciones, como se explicará con más detalle posteriormente, otras aplicaciones, por ejemplo, navegadores 312 o procesadores de documento 314, pueden necesitar la clave privada y el certificado en el mismo escritorio (o dispositivo móvil). Si el sistema operativo subyacente admite depósitos de claves estándar, como lo

hacen MS Windows™o Apple MacOS™, entonces se le puede asignar a la KMLC 610 que encargue las claves al almacenamiento de claves y las borre cuando sea apropiado.

[0060] Además de la generación de claves, descrita anteriormente, adecuada para la criptografía de clave pública, es decir claves asimétricas, el sistema de gestión de claves también puede generar y distribuir claves simétricas. En el centro de esto se encuentra una función *Shared_Secret_Generator()*, incorporada dentro de la KMLS 620, que toma como entrada tales factores como la UserID (quizás la línea dura del usuario o el número de teléfono móvil), un secreto de larga vida conocido solo por el servidor de QOOBA 325, y otros parámetros misceláneos, y produce como salida la *shared_secret* K. Es importante tener en cuenta que para un conjunto dado de entradas, el mismo secreto compartido se calculará de manera determinista. Las diferentes entidades autenticadas pueden solicitar a la KMLS 620 que les proporcione la clave simétrica apropiada al proporcionarle a la KMLS 620 los parámetros de entrada aplicables.

[0061] Tenga en cuenta que, dependiendo de la aplicación, la lógica de gestión de claves de QOOBA puede hacer uso de una o ambas capacidades de criptografía de clave asimétrica (es decir, pública) o de criptografía de clave simétrica anteriormente descritas. Ahora hemos descrito el sistema de gestión de claves, incluidas sus capacidades de generación de claves, y centramos nuestra atención en tres aplicaciones de ejemplo que hacen uso de estas capacidades.

Uso de gestión de claves de QOOBA para firma digital

[0062] Como se describe anteriormente, para determinadas aplicaciones, la firma digital que usa criptografía de clave pública se considera más apropiada que la firma de transacción electrónica. La firma digital se realiza siguiendo los pasos descritos a continuación.

[0063] El usuario final navega en la ventana de navegador 312 y ejecuta una transacción en un servicio web 350. El servicio web 350 usa la KMLAPI 630 para realizar una solicitud de firma de transacción con la "firma digital" requerida. Esta solicitud se envía a través del canal de comunicación seguro de *back-end* 500 a la KMLS 620. La solicitud se envía posteriormente de la KMLS 620 a la KMLC 610 a través del canal seguro 600, con una indicación de que se requiere una firma digital. El PIN de la firma de transacción de QOOBA es generado opcionalmente por el servidor de QOOBA 325 y enviado junto con la solicitud de firma digital. Se debe entender que, como se ha descrito anteriormente, el PIN podría, si se desea, ser enviado por el servidor de QOOBA 325 a una ventana de QOOBA, similar a la ventana de QOOBA 310, visualizada en el teléfono inteligente del usuario (no mostrado), a través de una conexión persistente similar a la conexión 600, en vez de a la ventana de QOOBA 310 visualizada en el escritorio 300, como se muestra.

[0064] La ventana de QOOBA 310 muestra al usuario la transacción como de costumbre y opcionalmente requiere que el usuario copie el PIN de la firma de transacción, es decir, la firma electrónica, en la ventana de navegador 312. En paralelo, la KMLC 610 calcula un *hash* en la transacción ("HashTran") y calcula una firma digital usando la clave privada Du del usuario, que se almacenó previamente en la memoria y el resultado fue [HashTran]Du. Este proceso podría ocurrir detrás de escena o al solicitarle al usuario que acepte firmar la transacción. En cualquier caso, la firma digital Du se aplica a la transacción *hash* [HashTran]. El *hash* firmado digitalmente de la transacción [HashTran]Du se envía posteriormente, a través del canal seguro 600, de la KMLC 610 a la KMLS 620, junto con el certificado digital [Cert]Ds o [Cert]Dca.

[0065] La KMLS 620 puede realizar opcionalmente una validación de la firma al aplicar la clave pública Pu del usuario a la firma digital [HashTran]Du para obtener HashTran, y compararla con una HashTran generada de manera independiente. Si se realiza o no una validación, la KMLS 620 reenvía la firma a la KMLAPI 630 a través del canal seguro 500.

[0066] La KMLAPI 630 puede recalcular la HashTran *hash* y verificar la firma que usa la clave pública Pu del usuario incluida en el certificado digital, Cert. Por lo tanto, la KMLAPI 630 aplica la clave pública Ps de KMLS 620 a [Cert]Ds, o la clave pública de autoridad de certificado Pca a [Cert]Dca, para recuperar Pu. Luego aplica la Pu recuperada a [HashTran]Du para recuperar HashTran y la compara con una HashTran, generada de manera independiente, para verificar la firma.

[0067] Tenga en cuenta que en la descripción anterior el *hash* se crea en la KMLC 610. Sin embargo, podría crearse fácilmente en KMLAPI 630 o la KMLS 620, aunque es posible que cada entidad lo recalcule para asegurar su autenticidad.

[0068] En este ejemplo, la transacción completa llega a la ventana de QOOBA 310. Si, por otro lado, es necesario firmar un documento usando este enfoque, entonces es posible extender la funcionalidad para que la KMLC confirme la clave privada y la clave pública en los almacenes de claves disponibles en el escritorio 300 del usuario, lo que haría que las claves estén disponibles para otras aplicaciones, por ejemplo, navegadores 312 o aplicaciones sin navegador 314. La KMLC sería responsable de eliminar las claves de usuario del almacenamiento de claves en el tiempo apropiado.

Uso de gestión de claves de QOOBA para compartir claves de encriptación

[0069] Con frecuencia ocurre que los datos se encriptan y se reenvían al receptor en un sistema de almacenamiento y reenvío, tal como el correo electrónico. Por ejemplo, las regulaciones requieren que los documentos, tales como las declaraciones financieras o los registros de salud, deban ser enviados encriptados si se envían como archivos adjuntos de correo electrónico. Muchas aplicaciones, por ejemplo, WinZip™ y Acrobat Reader™, han incorporado capacidades de encriptación basadas en contraseña. Entonces surge la pregunta de cómo se envía la contraseña de desencriptación al usuario. Un enfoque es acordar a priori una contraseña compartida. Los inconvenientes de este enfoque son que se puede utilizar una contraseña comprometida para desencriptar muchos documentos, y también es difícil requerir contraseñas complejas, ya que es probable que el usuario olvide la contraseña. A continuación se describen tres métodos para utilizar el sistema de gestión de claves de QOOBA para resolver este problema.

Enfoque 1

[0070] Un documento identificado de forma exclusiva, por ejemplo, por una DocumentID única, se encripta con una clave derivada de un PIN, por ejemplo, un PIN alfanumérico de ocho caracteres, por un servicio web 350 y luego se envía a un usuario, por ejemplo, por correo electrónico. Para los propósitos de esta discusión, una DocumentID es un valor único asociado a combinaciones particulares de identificación del emisor, identificación del receptor e identificación del documento. Cuando el usuario abre el documento usando alguna aplicación 314, típicamente una aplicación de *software*, en su escritorio, por ejemplo, WinZip™ y Acrobat Reader™, el programa envía una señal al servicio web 350 indicando que el usuario está intentando leer el documento particular. Aunque la aplicación 314 podría ser el navegador, para los propósitos de este análisis, como se muestra en la figura 2, se supone que es otro *software* de escritorio.

[0071] El servicio web 350 recupera el PIN con el que ese documento referenciado por la DocumentID se encriptó inicialmente, y luego usa la KMLAPI 630 para enviar el PIN al servidor de QOOBA 325. El servidor de QOOBA 325, usando la KMLS 620, transmite el PIN a la KMLC 610 y luego el PIN se muestra al usuario dentro de la ventana de QOOBA 310.

[0072] El usuario copia el PIN en la aplicación 314 y la desencriptación continúa normalmente. Debe observarse que, en general, no se requiere ningún cambio en la aplicación 314. La capacidad de activar un mensaje en el servicio web 350 cuando se abre es una funcionalidad que ya está integrada en muchas aplicaciones (por ejemplo, Acrobat Reader).

Enfoque 2

[0073] Un inconveniente del enfoque anterior es que el servicio web 350 tiene que mantener una lista de DocumentIDs y PINs. Una forma de resolver este problema es tener la clave con la que cada documento se encripta como resultado de una función, que toma como entrada la DocumentID y un secreto a largo plazo conocido solo por el servicio web 350. De esta forma, la clave se puede generar dinámicamente después de que el usuario intente abrir el documento como se describe en el enfoque 1.

Enfoque 3

[0074] Un inconveniente de lo anterior es que se supone que el servicio web 350 está disponible y en línea cuando se abre el documento. Dado que algunos de los sistemas que generan y distribuyen documentos son sistemas por lotes de *back-end*, esta suposición puede no ser siempre aplicable. La capacidad de generación de secretos compartidos de la gestión de claves de QOOBA se puede usar para resolver el problema de la siguiente manera.

[0075] El servicio web 350 envía al servidor de QOOBA 325, de uno en uno, o más pobablemente en un archivo por lotes, las DocumentIDs que quiere encriptar. Para los fines de este análisis, se supondrá que el archivo contiene información de envolvente, tal como las IDs del emisor y del receptor. La KMLS 620 usa la Shared_Secret_Generator() anteriormente descrita para calcular claves de encriptación para cada DocumentID. Por ejemplo, la clave K1 para una DocumentID, la K2 para otra DocumentID, la K3 para otra DocumentID, etc. Estas claves son devueltas posteriormente por la KMLS 620 al servicio web 350. El servicio web 350 luego encripta cada documento respectivo con la clave aplicable y envía el documento encriptado, por ejemplo, por correo electrónico, a los respectivos usuarios aplicables.

[0076] El usuario aplicable usa el otro *software* de escritorio 314 para abrir el documento, lo que desencadena una solicitud de una clave directamente al servidor de QOOBA 325 a través de una conexión web segura 750, que es otro canal de comunicación. Cabe señalar que esta es una conexión directa 750 del *software* sin navegador 314 al servidor de QOOBA 325 y no a través de la ventana de QOOBA 310.

[0077] Esta acción provoca que la KMLS 620 use la Shared_Secret_Generator() para recalcular la clave de encriptación aplicable, por ejemplo, K1, K2, K3, etc. La clave aplicable se envía posteriormente a la KMLC 610 y se muestra al usuario en la ventana de QOOBA 310 para copiarla en la ventana sin navegador 314, como se describe anteriormente.

[0078] Si bien hemos descrito lo anterior usando un *software* sin navegador (por ejemplo, Acrobat Reader) como nuestro ejemplo, se puede utilizar la misma funcionalidad para aplicaciones web basadas en navegador.

Uso de la gestión de claves de QOOBA para "sembrar" contraseñas de un solo uso (OTPs) y *tokens* de autenticación de transacciones

[0079] Todos los autenticadores de token de contraseñas de un solo uso (OTPs) y de autenticación de transacciones, por ejemplo, *hardware*, *software*, aplicaciones de teléfono inteligente, etc., requieren una clave que se almacena en el *token* y también se almacena en el sistema de *back-end*. La administración de estas claves (que comúnmente se conocen como "semillas") ocasiona costes y complejidad. El sistema de gestión de claves de QOOBA se puede usar para simplificar enormemente este proceso.

[0080] Para los propósitos de esta discusión, se supone que un autenticador de *tokens* (no mostrado) se implementa como *hardware*, *software* o como una aplicación de teléfono móvil. El *token* comienza en un estado inactivo sin ninguna semilla (o se requiere una actualización de semillas). El usuario realiza una solicitud directamente dentro de la ventana de QOOBA 310 o directamente del *token* al servidor de QOOBA 325 o a un servicio de web externo 350 que solicite un evento de semillas. Al servidor de QOOBA 325 se le proporciona algún identificador único que identifica a la UserID.

[0081] La KMLS 620 dentro del servidor de QOOBA 325 usa la única UserID y otra información, incluido el secreto a largo plazo conocido solo por la KMLS 620, como entradas a la Shared_Secret_Generator() para generar una semilla única para ese usuario. Esta semilla se envía de vuelta a la KMLC 610 a través del canal seguro 600, y luego se muestra al usuario en la ventana de QOOBA 310. El usuario inserta la semilla en el *token* de la aplicación del *software* o del teléfono inteligente. Nos damos cuenta que la semilla real puede ser generada por una función que transforma la semilla que el usuario inserta. Se reconocerá que para el *hardware* esto solo funcionará si el *token* tiene un teclado que la mayoría de autenticadores de transacciones sí tienen.

[0082] Como una variante de lo anterior, observe que el autenticador de transacciones se puede integrar directamente en la ventana de QOOBA 310 como parte de la funcionalidad. Mientras que a primera vista la razón fundamental para esto puede no ser obvia, la compatibilidad con sistemas existentes, tales como EMV/CAP, proporciona la razón fundamental para este enfoque. Esta siembra a petición de los autenticadores de transacción simplifica enormemente los costes de aprovisionamiento.

REIVINDICACIONES

1. Método de funcionamiento de un servidor de seguridad (125, 325) para proporcionar una gestión de claves aplicada en un sistema de autenticación cuasi fuera de banda, que comprende:

recibir, a través de un canal de comunicación (450, 750) de un dispositivo de red (100, 300) asociado a un usuario, una solicitud de activación de una ventana de interfaz de usuario (110, 310) para ese usuario particular en el dispositivo de red;
transmitir, a un sistema de autenticación fuera de banda, un número de identificación personal, PIN, de activación para reenviarlo a un teléfono (175) del usuario mediante un mensaje de voz o texto;
recibir, a través del canal de comunicación del dispositivo de red, el PIN de activación previamente transmitido;
autenticar al usuario en función del PIN de activación recibido;
establecer, sobre el canal de comunicación, después de la autenticación del usuario, un canal de comunicación seguro, independiente y encriptado (600) entre la ventana de interfaz de usuario y el servidor de seguridad; y
al menos uno de (i) generar y transmitir a la ventana de interfaz de usuario a través del canal de comunicación seguro, independiente y encriptado, uno o más (a) del material de certificado para operaciones basadas en criptografía de clave pública y (b) del material de clave para operaciones basadas en criptografía de clave simétrica y (ii) recibir de la ventana de interfaz de usuario, a través del canal de comunicación seguro, independiente y encriptado, material de clave para operaciones basadas en criptografía de clave pública;
donde el material de certificado para criptografía de clave pública se genera y transmite a la ventana de interfaz de usuario a través del canal de comunicación seguro, independiente y encriptado (600), y que comprende además:

recibir, de la ventana de interfaz de usuario (110, 310), a través del canal de comunicación seguro, independiente y encriptado, una clave pública Pu de un par de claves privada/pública Du/Pu asociado al usuario y previamente generado en la ventana de interfaz de usuario; y
donde el material de certificado transmitido a la ventana de interfaz de usuario a través del canal de comunicación seguro, independiente y encriptado, incluye un certificado, que está firmado por el servidor de seguridad (125, 325) o por una autoridad de certificado externa (900), y asocia al usuario la clave pública Pu recibida y las instrucciones para el almacenamiento del certificado;
donde el certificado está firmado por una autoridad de certificado externa (900), y además que comprende:

transmitir un certificado sin firmar a la autoridad de certificado externa; y
recibir el certificado firmado de la autoridad de certificado externa antes de transmitir el certificado firmado a la ventana de interfaz de usuario.

2. Método según la reivindicación 1, donde la instrucción de almacenamiento transmitida requiere el almacenamiento de la clave privada Du del usuario y el certificado firmado (i) en la memoria, o (ii) en el almacenamiento de claves de un sistema operativo del dispositivo de red, o (iii) en ambos.

3. Método según la reivindicación 1, donde la instrucción de almacenamiento transmitida deja explícitamente la decisión de almacenamiento a la ventana de interfaz de usuario.

4. Método según la reivindicación 1, donde el material de clave para operaciones de criptografía de clave simétrica es generado y transmitido por el servidor de seguridad (125, 325) a la ventana de interfaz de usuario a través del canal de comunicación seguro, independiente y encriptado (600), y que comprende además:

recibir, de la ventana de interfaz de usuario (110, 310) o de un sitio de red de terceros, una solicitud autenticada que contiene información de identificación única asociada al usuario o a un archivo;
generar, usando una función unidireccional, una única clave simétrica K, donde el valor de la clave K se deriva de la información de identificación recibida única y de un secreto conocido solo por el servidor de seguridad; y;
transmitir, al solicitante, la clave simétrica K generada.

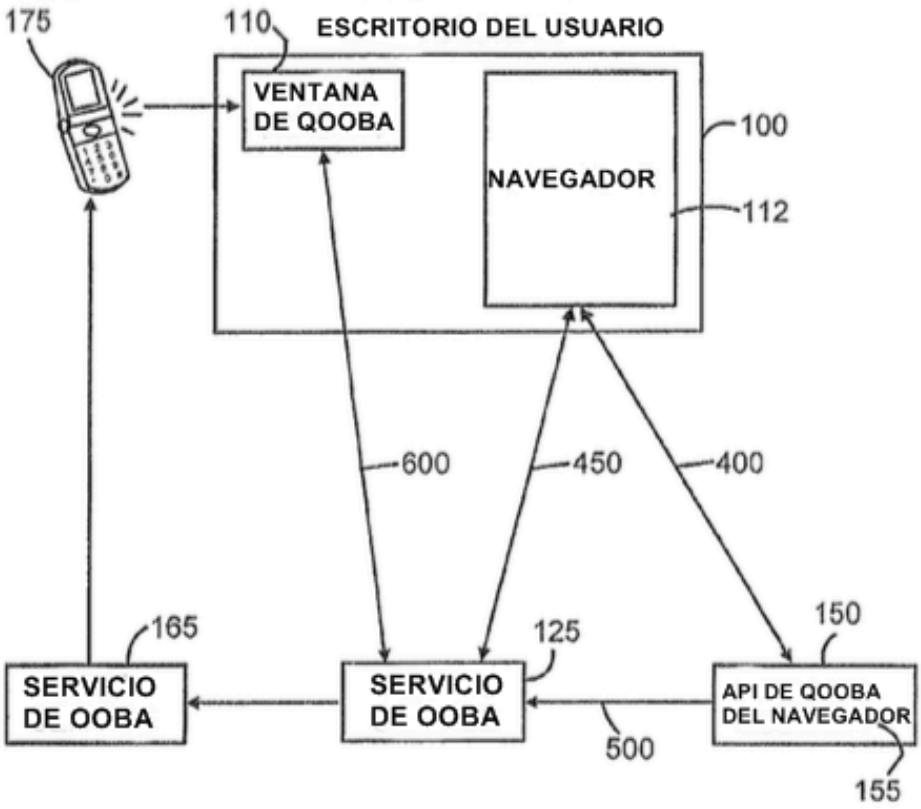
175
110
ESCRITORIO DEL USUARIO
VENTANA DE QOOBA
NAVEGADOR
100
112
600
450
400
165
125
150
SERVICIO DE OOBA
SERVICIO DE OOBA
API DE QOOBA DEL NAVEGADOR
500
155

Figura 1

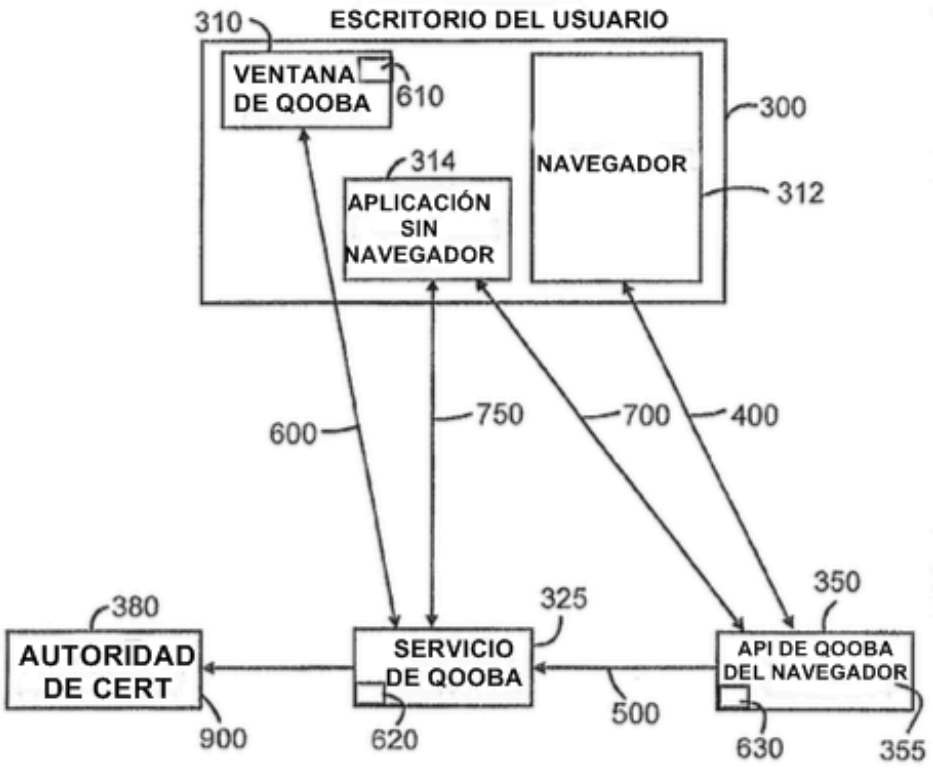
310
ESCRITORIO DEL USUARIO
VENTANA DE QOOBA
610
300
NAVEGADOR
312
314
APLICACIÓN SIN NAVEGADOR
600
750
700
400
350
380
325
AUTORIDAD DE CERT
SERVICIO DE QOOBA
API DE QOOBA DEL NAVEGADOR
500
900
620
630
355

Figura 2