(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 372 128**

(51) Int. CI.:
H04L 29/06 (2006.01)
H04L 12/58 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08839248 .5**
(96) Fecha de presentación: **15.10.2008**
(97) Número de publicación de la solicitud: **2204033**
(97) Fecha de publicación de la solicitud: **07.07.2010**

(54) Título: **MÉTODO Y SISTEMA PARA FOMENTAR LAS COMUNICACIONES SEGURAS.**

(30) Prioridad:
15.10.2007 US 980018 P

(45) Fecha de publicación de la mención BOPI:
16.01.2012

(45) Fecha de la publicación del folleto de la patente:
16.01.2012

(73) Titular/es:
PENANGO, INC.
1215 K STREET NW
SACRAMENTO, CA 95814, US

(72) Inventor/es:
LEONARD, Sean

(74) Agente: **de Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Método y sistema para fomentar las comunicaciones seguras.

ANTECEDENTES

Campo

Esta invención se refiere a los sistemas de comunicaciones y mensajería electrónicas. En particular, las realizaciones de presente invención se refieren a los sistemas de mensajería segura, tales como los sistemas de mensajería cifrada y autentificada, y los procedimientos para fomentar el uso de la mensajería segura.

DESCRIPCIÓN DE LA TÉCNICA RELACIONADA

Hoy en día, las redes como Internet y las redes móviles permiten amplio acceso a las comunicaciones y la mensajería, tal como el correo electrónico, los mensajes de texto, los mensajes instantáneos, y similares. Sorprendentemente, no obstante, la mayoría de este tráfico de comunicaciones y mensajería no está asegurado o protegido. Por ejemplo, la abrumadora mayoría de los mensajes de correo electrónico se envían sin cifrar y sin firmar, de manera que cualquier espía en una sesión de comunicaciones sobre Internet puede leer y alterar tal correo electrónico mientras está en tránsito o en almacenamiento.

El envío y recepción de mensajes cifrados y firmados (por ejemplo, autentificados) es una capacidad bien conocida en la técnica. En un sistema típico, un usuario puede obtener un certificado gratis o por una tasa de una autoridad de certificación (CA). La CA verifica la identidad del usuario y la dirección de correo electrónico. El usuario puede entonces navegar al sitio web de la CA y completa una serie de acciones, tales como rellenar formularios, en el sitio web. Esto típicamente implica al usuario introducir datos personales, que incluyen una dirección de correo electrónico. Una pareja de claves pública-privada se genera entonces para el usuario. El usuario presenta una petición de certificación que contiene su clave pública junto con el resto de la información anteriormente mencionada durante el curso de la presentación de datos al sitio web. La clave privada se almacena en el ordenador del usuario. El sitio web de la CA entonces verifica la identidad del usuario mediante el envío de una confirmación, por ejemplo, a través de un correo electrónico al usuario. En la confirmación, se incluye un enlace, y cuando el usuario sigue manualmente el enlace, el sitio web de la CA provoca que un certificado expedido sea instalado en el navegador web del usuario y unido con la clave privada relacionada.

Desafortunadamente, el uso de estos mecanismos de seguridad no está ampliamente extendido. Por ejemplo, a pesar de la existencia de CA e infraestructura de claves públicas (PKI) bien establecidas, el uso de tecnologías tales como S/MIME y PGP no está muy ampliamente extendido. Una razón para la carencia de aceptación es que el proceso de establecimiento de estos mecanismos de seguridad requiere considerable interacción del usuario. Por ejemplo, los sistemas y los procesos conocidos para la obtención de un certificado digital y la clave privada supondrán típicamente al menos 20 pasos manuales por el usuario.

Además, otros obstáculos han ralentizado la aceptación de las comunicaciones de seguridad en línea. Por ejemplo, muchos clientes y programas informáticos de correo electrónico no pueden manejar los mensajes S/MIME. Los clientes de correo web son particularmente conocidos por no soportar S/MIME. S/MIME se considera actualmente poco adecuado para el uso a través de clientes de correo web por aquellos expertos en la técnica. Una razón es que algunas prácticas de seguridad requieren que la clave privada sea mantenida accesible al usuario, pero inaccesible desde el servidor de correo web. Esto complica una ventaja clave del correo web de proporcionar accesibilidad ubicua. Este problema con S/MIME y el correo web no es único. Por lo tanto, por estas y otras razones, la vasta mayoría de la mensajería permanece relativamente sin seguridad.

La US 2007/022162 describe un método para permitir a un usuario de correo electrónico crear una cuenta de correo de Infraestructura de Clave Pública (PKI) y a partir de entonces firmar digitalmente, enviar, verificar y recibir los correos electrónicos cifrados PKI sobre una red de ordenadores.

SUMARIO

En una realización, se proporciona un método de comunicaciones seguras, dicho método comprende: acceder a un servicio de mensajería; obtener la información de identificación que identifica un usuario del servicio; en respuesta al consentimiento por el usuario y sin interacción adicional con el usuario, obtener una pareja de claves que comprenden una clave pública y una clave privada, y presentar una petición de un certificado a una autoridad de certificación (CA) en base a la pareja de claves; recibir un código de verificación desde la CA; confirmar la recepción del código de verificación desde dicha CA; proporcionar una certificación para el usuario en base al código de verificación y la pareja de claves; y asegurar las comunicaciones desde el usuario en base al certificado.

En otra realización, un aparato comprende los medios configurados para realizar el método anterior.

En otra realización, un medio legible por ordenador comprende el código de programa ejecutable configurado para realizar el método anterior.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La FIG.1 muestra un sistema ejemplar consistente con las realizaciones de la presente invención.

La FIG. 2 muestra un navegador y la extensión ejemplares consistente con algunas realizaciones de la presente invención.

La FIG. 3 ilustra un flujo de proceso ejemplar para la configuración de un navegador de acuerdo con algunas realizaciones de la presente invención.

La FIG. 4 ilustra un flujo de proceso ejemplar para la obtención de un certificado digital consistente con algunas realizaciones de la presente invención.

La FIG. 5 muestra un extracto del material de las Extensiones Multipropósito de Correo de Internet (MIME) que incluye las cabeceras MIME cuando se varía el nombre de archivo por ciertas realizaciones de la invención.

La FIG. 6 muestra las muestras de mensajes que incluyen eslóganes y datos de firma digital visualizados usando las técnicas y realizaciones de la invención.

La FIG. 7 muestra cómo se pueden encadenar juntos una cascada de repositorios para construir conjuntos de preferencias, que la extensión usa en la determinación de su comportamiento, tal como el comportamiento por defecto y la selección UI para firmar los mensajes sometidos a composición.

DESCRIPCIÓN DETALLADA DE LAS REALIZACIONES

Las realizaciones de la presente invención permiten a un usuario participar en las comunicaciones seguras usando certificados digitales y otras tecnologías de cifrado de una forma fácil con un mínimo de interacción de distracción. Para los propósitos de ilustración, las realizaciones de la presente invención se describen con referencia a los mensajes de correo electrónico seguros. En particular, se revelan las realizaciones que proporcionan un planteamiento alternativo al correo web y que permiten a los usuarios obtener certificados S/MIME. Por supuesto, el correo web se proporciona como un ejemplo y otras formas de mensajería, tales como el correo electrónico a través de clientes basados en programas informáticos, mensajes de texto, SMS, mensajes instantáneos, están dentro del alcance de la presente revelación. Un experto en la técnica reconocerá que las realizaciones de la presente invención se pueden implementar para cualquier forma de mensajería, tal como mensajes de texto, mensajes instantáneos, etc.

Algunas realizaciones reducen drásticamente los pasos requeridos de la interacción del usuario, provocando una experiencia de usuario más placentera y por lo tanto un aumento en el número de usuarios que estarían deseando usar la tecnología de certificación digital para su mensajería. Al mismo tiempo, las realizaciones de la presente invención no requieren que ningún otro distinto del usuario tenga acceso a la clave privada. Ahora se hará referencia en detalle a las realizaciones ejemplares de la invención, las cuales se ilustran en los dibujos anexos. Donde sea posible, los mismos números de referencia se usarán en todos los dibujos para referirse a las mismas partes o similares.

En general, la FIG. 1 muestra un sistema ejemplar y la FIG. 2 muestra un navegador y extensión ejemplares. Las FIG. 3 y 4 entonces ilustran los flujos de proceso ejemplares. En particular, la FIG. 3 ilustra un flujo de proceso ejemplar para la configuración de un navegador. La FIG. 4 ilustra un flujo de proceso ejemplar para la obtención de un certificado digital. Las FIG. 5-7 también se proporcionan para ilustrar varios aspectos de las realizaciones. Por ejemplo, la FIG. 5 muestra un extracto del material de las Extensiones Multipropósito de Correo de Internet (MIME) que incluye las cabeceras MIME cuando se varía el nombre de archivo. La FIG. 6 muestra las muestras de mensajes que incluyen los eslóganes y los datos de firma digital visualizados usando las técnicas de las realizaciones de la invención. Y, la FIG. 7 muestra cómo se puede encadenar junta una cascada de repositorios para construir conjuntos de preferencias, que la extensión usa en la determinación de su comportamiento, tal como el comportamiento por defecto y la selección UI para firmar los mensajes sometidos a composición. Estas figuras se describirán además más adelante.

La FIG. 1 muestra un sistema ejemplar consistente con las realizaciones de la presente invención. La FIG. 1 se entiende como un ejemplo, y no como una limitación arquitectónica para las realizaciones descritas. Como se muestra, un sistema 100 puede comprender una red 102, un ordenador de usuario 104, un servidor de mensajería 106, y un servidor de CA 108. Estos componentes se describirán ahora además más adelante. El sistema 100 puede incluir, no obstante, servidores adicionales, clientes, y otros dispositivos no mostrados.

La red 102 sirve como una infraestructura de comunicación para soportar las comunicaciones entre los otros componentes del sistema 100, tal como el usuario 104, el servidor de mensajería 106, y el servidor de CA 108. Tales redes son bien conocidas por aquellos expertos en la técnica incluyendo las redes de área local, las redes de área metropolitana, las redes de área extensa, las redes de comunicaciones móviles (tales como las redes 3G), las redes WiFi, y similares. En algunas realizaciones, la red 102 puede comprender una o más redes de Internet.

El ordenador del usuario (o simplemente “usuario”) 104 proporciona los componentes físicos y los componentes lógicos para que un usuario utilice los métodos y sistemas de las realizaciones. El ordenador del usuario 104 se puede implementar en dispositivos bien conocidos, tales como, ordenadores personales, ordenadores en red, teléfonos móviles, ordenadores portátiles, y similares. En el ejemplo representado, el ordenador del usuario 104 puede comprender componentes físicos, componentes lógicos y datos (no se muestran), tales como procesadores, memoria, sistemas de almacenamiento, archivos de arranque, imágenes del sistema operativo, y aplicaciones (como un navegador o extensión de navegador). Adicionalmente, el ordenador de usuario 104 puede emplear el conjunto de protocolos Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP) para comunicar con los otros componentes del sistema 100.

El servidor de mensajería 106 proporciona los servicios, por ejemplo, al usuario 104 relacionados con la mensajería. Por ejemplo, el servidor de mensajería 106 puede ser uno o más servidores web que implementan una aplicación de correo web. Tales servidores son bien conocidos por aquellos expertos en la técnica. Por supuesto, el servidor de mensajería 106 puede proporcionar otros servicios, tales como la gestión de cuentas, u otras formas de mensajería. En algunas realizaciones, el servidor de mensajería 106 puede referirse a los servicios de correo web bien conocidos, tales como el Correo de Yahoo!, Gmail, y similares.

En el ejemplo representado, el servidor de mensajería 106 puede comprender componentes físicos, componentes lógicos y datos (no se muestran), tales como procesadores, memoria, sistemas de almacenamiento, archivos de arranque, imágenes del sistema operativo, y aplicaciones (como un servidor web). Adicionalmente, el servidor de mensajería 106 puede emplear el conjunto de protocolos TCP/IP para comunicar con los otros componentes del sistema 100.

El servidor de CA 108 sirve como un intermediario de confianza tanto para el ordenador del usuario 104 como el servidor de mensajería 108. En general, el servidor de CA 108 confirma que cada ordenador es de hecho quién dice ser y entonces proporciona las claves públicas de cada ordenador al otro. En algunas realizaciones, el servidor de CA 108 proporciona los certificados digitales y un sistema de PKI que permite al ordenador del usuario 104 y al servidor de mensajería 106 asegurar su mensajería. Por ejemplo, en algunas realizaciones, los servicios del servidor de CA 108 pueden permitir el uso de S/MIME por el usuario 104 con una aplicación de correo web proporcionada por el servidor de mensajería 106.

En el ejemplo representado, el servidor de CA 108 puede comprender componentes físicos, componentes lógicos y datos (no se muestran), tales como procesadores, memoria, sistemas de almacenamiento, archivos de arranque, imágenes del sistema operativo, y aplicaciones (como un servidor web). Adicionalmente, el servidor de CA 108 puede emplear el conjunto de protocolos TCP/IP para comunicar con los otros componentes del sistema 100.

La FIG. 2 muestra un navegador y extensión ejemplares consistentes con algunas realizaciones de la presente invención. Como se muestra, el ordenador del usuario 104 se puede configurar para ejecutar un navegador 200 y una extensión de navegador 202. Además, para varios rasgos de las realizaciones, el navegador 200 y la extensión 202 pueden acceder a un repositorio 204. Estos componentes y ciertos aspectos de su funcionamiento se describirán además ahora.

El navegador 200 sirve como un interfaz de usuario que se ejecuta en el ordenador del usuario 104. Tales navegadores son bien conocidos por aquellos expertos en la técnica. A través del navegador 200, el usuario 104 puede acceder de esta manera a sus servicios de mensajería, tales como el correo web. Por supuesto, las realizaciones se pueden implementar usando otros tipos de aplicaciones cliente de mensajería. Por ejemplo, los clientes de correo electrónico como Microsoft Outlook y Thunderbird se pueden usar en las realizaciones.

La extensión 202 asiste al navegador 200 en proporcionar varios rasgos de las realizaciones. En una realización de la presente invención, un usuario instala, o hace que se instale, una parte de los componentes lógicos en dicha máquina de usuario. El usuario puede consumar esto, por ejemplo, mediante la descarga de la extensión 202 en el navegador web del usuario 200. La extensión 202 puede ser cualquier programa informático que modifique el comportamiento del navegador. Ejemplos de extensiones del navegador que se pueden emplear en las realizaciones incluyen, pero no se limitan a, los “Objetos Auxiliares de Navegación” para Internet Explorer de Microsoft y las “Extensiones” para Mozilla Firefox. Gmail S/MIME 0.2.4 por ejemplo, es un tipo de extensión de navegación que se puede emplear en las realizaciones.

El repositorio 204 mantiene los datos preferentes, que cuando se combinan juntos forman un caso de conjunto de preferencias que gobierna cómo se comportará la extensión 202. Por ejemplo, un servidor de políticas (no se muestra) puede encargar que todos los mensajes salientes sean firmados, y la preferencia del usuario almacenada dentro del navegador puede indicar el mismo, pero ningún repositorio puede tener un certificado digital y la clave privada adecuados para un mensaje particular sometido a composición. El comportamiento resultante bajo esta política sería para que el mensaje sea enviado no firmado, pero que un aviso sea expedido al usuario antes de enviar el mensaje no firmado.

Las realizaciones de la invención pueden almacenar la preferencia en uno o más repositorios de preferencias 204. Tales preferencias pueden incluir: el(los) certificado(s) digital(es) del usuario y la(s) clave(s) privada(s); las

preferencias del usuario para la visualización y cifrado de ciertos mensajes, tales como intentar firmar o cifrar automáticamente todos los mensajes por defecto; los certificados digitales de los destinatarios; y una historia acumulada de las interacciones y preferencias con respecto a los destinatarios de los certificados de los destinatarios.

El repositorio 204 se puede situar en varios emplazamientos, tales como, dentro del navegador, dentro del sistema operativo, en disco como una estructura de datos de extensión específica, un servidor de políticas central, o un servidor globalmente disponible. El repositorio 204 también se puede distribuir a través de una red de igual a igual, almacenar en un servidor de correo web como datos especiales o cifrados, almacenar en la ubicación en Internet definida por el usuario, tal como un sitio web o un sitio de FTP, o en o a través de una red de sincronización, tal como Plaxo.

Además, las preferencias de repositorio se pueden conectar en cascada. Por ejemplo, el repositorio 204 se puede conectar en cascada de acuerdo con la siguiente lista ejemplo: 1. por defecto (almacenado internamente en la extensión) 2. global (a través de un servidor global) 3. por tipo de servicio de mensajería (por ejemplo, por vendedor de los programas informáticos de servicio de correo web) 4. por sub-URI (por ejemplo, por dominio) 5. por URI (es decir, por servicio de correo web particular) 6. por Remitente (por ejemplo, por identidad o papel indicado en una dirección De:) 7. por tipo de destinatario (por ejemplo, por papel) 8. por destinatario (por ejemplo, por identidad) 9. por certificado 10. por dirección de correo electrónico.

Los repositorios 204 sujetos a manipulación, tales como aquéllos que residen en un servidor de correo web 106 o un servidor globalmente público, se pueden firmar (por el usuario o por otra entidad de confianza, tal como la organización del usuario o por los autores de la extensión) para asegurar la integridad, y se pueden cifrar para asegurar la confidencialidad si la información en el repositorio 204 se considera privada.

Una ventaja de firmar el repositorio 204 por un proveedor de almacenamiento, tal como el servidor de correo web 106, es que pudiera apreciar la información del repositorio 204 (tal como la lista de certificados del destinatario) para varios propósitos que incluyen hacer el seguimiento del uso de la tecnología de certificación digital. Una ventaja adicional de firmar es que el servidor de mensajería 106 ya conoce las direcciones de correo electrónico del destinatario en virtud de las cabeceras y otra información de encaminamiento en todos los mensajes de correo electrónico.

En las realizaciones adicionales, los repositorios 204 pueden sincronizarse entre sí de manera que el usuario puede acceder a su información del repositorio, tal como la información del libro de direcciones y los certificados correspondientes, desde cualquier cuenta de mensajería, tal como cualquier cuenta de correo web. En ausencia de usar un servidor central, en una realización la extensión envía actualizaciones periódicas (tales como por elemento cambiado en el repositorio, a continuación de la finalización de sesión, o cada pocos minutos) a otras cuentas conocidas en forma de mensajes de correo electrónico (firmados o cifrados opcionalmente). Cuando se reciben los mensajes, opcionalmente se filtran a través de las reglas de servidor a una carpeta especial. Cuando el usuario se registra en el servicio de mensajería 106 mientras que usa la extensión 202 en cualquier instalación, la extensión 202 descarga y procesa las actualizaciones pendientes al repositorio de correo web correspondiente 204, sincronizando de esta manera cada repositorio de correo web 204 con un estado consistente. La existencia de dichas cuentas se puede registrar directamente en un repositorio 204, de manera que el usuario 104 no tenga que poner en marcha una lista de tales cuentas en cada repositorio de navegador almacenado en los navegadores 200 que el usuario usa.

En una realización adicional, el repositorio 204 se almacena en una red igual a igual. Aún en otra realización, un repositorio primario se almacena en un servidor de usuario especificado, donde cada servicio de correo web contiene un repositorio con bastante información para identificar dicho servidor de usuario especificado. Tal realización se puede usar para evitar la complejidad de las actualizaciones distribuidas mientas que se conservan al menos dos rasgos. Primero, esta realización conserva la conveniencia de localizar el servidor de usuario especificado sin requerir que el usuario lo especifique constantemente en cada cliente local. Y segundo, se conserva el sentido de seguridad con respecto al repositorio principal en el servidor de usuario especificado, dado que el repositorio no necesita residir en un servidor global sometido al control de los autores de extensión u otra tercera parte.

La FIG. 3 ilustra un flujo de proceso ejemplar para obtener un certificado digital consistente con algunas realizaciones de la presente invención. Como se señaló anteriormente, las realizaciones de la invención pueden fomentar la instalación de la extensión 202 y el uso de la tecnología de certificación digital más ampliamente, tal como, a través de las siguientes técnicas. En una realización, el usuario es inducido a obtener la extensión 202 mediante la visualización prominentemente de los mensajes de información o eslóganes.

Los mensajes enviados desde el remitente pueden estar en una de tres formas: en blanco, firmado, o cifrado. Las partes cifradas o firmadas se pueden encapsular en mensajes firmados o cifrados, que forman un mensaje firmado y cifrado compuesto.

En algunas realizaciones, siempre que el usuario envía mensajes, la extensión puede 202 inyectar selectivamente

eslóganes en los mensajes antes de firmar o cifrar el mensaje. Por ejemplo, tales mensajes se pueden enviar selectivamente solamente a aquellos destinatarios que el remitente no sabe que tienen certificados digitales, pero que de otro modo tienen la capacidad para procesar tales mensajes si se usa la extensión. Los eslóganes pueden invitar al destinatario a: verificar la autenticidad del mensaje o mensajes en general con la extensión; preguntar si el mensaje u otros mensajes son auténticos; asegurar los mensajes entre el remitente u otros remitentes en general con la extensión; preguntar si el mensaje u otros mensajes son privados; sugerir al destinatario que pregunte al remitente más sobre la extensión; y aumentar el conocimiento de la extensión.

Los eslóganes pueden indicar al usuario que el mensaje puede no ser de confianza, sino que meramente sugieren incertidumbre. Tales eslóganes también pueden mostrar alguna conexión con el remitente, en quién el destinatario implícitamente confía. Es de señalar, que muchos estándares, tales como aquéllos aplicables a S/MIME específicamente desalientan el uso de eslóganes tales como aquéllos descritos anteriormente. No obstante, los eslóganes de las realizaciones pueden ser útiles sin embargo a pesar de esta recomendación del estándar S/MIME.

Estos mensajes se podrían situar en cualquier sitio en el mensaje. Por ejemplo, los eslóganes pueden aparecer en la parte superior del mensaje. Los eslóganes también se pueden emplear para ciertos destinatarios en base a criterios. Por ejemplo, para fomentar los rasgos de cifrado de la invención, los eslóganes pueden indicar al usuario que con el programa informático, pueden enviar y recibir mensajes cifrados, sellados, o privados, usando palabrería que tipos particulares de grupos demográficos de usuarios entenderían. Algunos destinatarios pueden responder negativamente a los eslóganes en los mensajes que sugieren a un destinatario visitar un sitio web desconocido hasta ahora, a pesar de una relación de confianza existente con el remitente del mensaje. Más que enviar destinatarios a un sitio web desconocido hasta ahora, se sugiere al destinatario preguntar al remitente, con quien el remitente ya tiene una relación de confianza, más acerca de la extensión. Presumiblemente en virtud del uso continuado de la extensión, el remitente está dispuesto a tratar los rasgos de la extensión para el beneficio del uso expandido de la extensión. De esta manera, el destinatario puede percibir que la información con respecto a la extensión es de valor mayor porque se proporciona desde alguien con quien el destinatario tiene un nivel de confianza preestablecido.

Con respecto a la firma digital agregada, el mensaje firmado opaco, o el texto cifrado, en algunas realizaciones, los agentes de correo incompatibles con S/MIME, tales como la mayoría de los sistemas de correo web, visualizan tales elementos como adjuntos simples. En algunas realizaciones, el nombre de archivo del adjunto puede variar. Las cabeceras que ilustran estas realizaciones se dan en la FIG. 5, y muestras de tales mensajes en los agentes de correo se dan en la FIG. 6.

Una ventaja de las realizaciones es que el nombre de archivo puede comunicar más información informativa sobre el adjunto que su asociación con la S/MIME. En una realización, el adjunto porta una descripción y un origen, tal como “Firma Digital de tipo Extensión”. Tal convenio de nombre de archivo puede resultar útil para poner la marca del origen o fuente del material criptográfico. En otra realización, el adjunto porta un eslogan o mensaje de recomendación como, “Usar la Extensión Cada Día”. Es posible una innumerable cantidad de otras realizaciones. Por ejemplo, una realización ejemplar varía la base del nombre de archivo, pero conserva la extensión de fichero correspondiente. De esta manera, si un usuario intenta descargar o abrir el adjunto, el adjunto se comportaría en el curso normal de abrir archivos con similares extensiones de fichero.

Con referencia ahora al proceso ilustrado en la FIG. 3 en una realización de la presente invención, un usuario instala, o hace que se instale, una parte de programa informático en dicha máquina del usuario. El usuario puede consumar esto, por ejemplo, mediante la descarga de la extensión 202 en el navegador web del usuario 200. La extensión 202 puede ser cualquier programa informático que modifique el comportamiento del navegador. Como se señaló, ejemplos de las extensiones del navegador que se pueden emplear en las realizaciones incluyen, pero no se limitan a, los “Objetos Auxiliares del Navegador” para Internet Explorer de Microsoft y las “Extensiones” para Mozilla Firefox.

En general, cuando un usuario navega a una página web en el servidor de mensajería 106, el servidor de mensajería 106 puede determinar el entorno en el ordenador de usuario 104. Por ejemplo, el servidor de mensajería 106 puede detectar el navegador 200, el sistema operativo en el ordenador del usuario 104, y otros parámetros del cliente del ordenador del usuario 104 que usa las cabeceras HTTP, la dirección IP del cliente, y otros métodos.

A continuación, el servidor de mensajería 106 entonces sirve una sugerencia de página web al usuario para descargar la extensión automáticamente, por ejemplo, usando la tecnología ActiveX en Internet Explorer, los archivos XPI de Desencadenamiento Instalados en Mozilla Firefox, y similares. En algunas realizaciones, se puede sugerir al usuario que acepte la extensión 202.

La FIG. 4 ilustra un flujo de proceso ejemplar para la obtención de un certificado digital y que usa S/MIME con su servicio de mensajería de acuerdo con algunas realizaciones de la presente invención. Desde la perspectiva del usuario, el proceso puede parecer muy simple y requerir poca o ninguna interacción. En particular, la experiencia del usuario del proceso generalmente comprendería: registrarse en su servicio de mensajería 106, tal como correo web (no obstante, el registro en proceso se puede desviar, por ejemplo, con el uso de códigos gratuitos recibidos por Internet); la vista de un diálogo acerca de los certificados y la gestión de identidad; opcionalmente pulsar para

aceptar (o esperar a la cuenta atrás automática); y entonces usar el correo web del servicio de mensajería 106 en su forma acostumbrada. Incluso si el usuario necesita instalar una extensión 202 u otro programa informático, la experiencia del usuario del proceso requerirá poca o ninguna interacción y generalmente puede comprender: la instalación de la extensión 202 u otro programa informático y opcionalmente pulsar para aceptar la instalación; si el navegador 200 fue reiniciado, registrarse en el correo web del servidor de mensajería 106 (no obstante, el registro en proceso se puede desviar, por ejemplo, con el uso de códigos gratuitos recibidos por Internet); la vista de un diálogo sobre los certificados y la gestión de identidad; esperar a la cuenta atrás automática u opcionalmente editar las entradas y pulsar aceptar; y usar el correo web del servicio de mensajería 106 en su forma acostumbrada. Por lo tanto, en ambas circunstancias, el usuario puede obtener y comenzar usando un certificado digital expedido por la CA de confianza en una pulsación o menos.

Aunque las realizaciones se pueden configurar de manera general para requerir poca o ninguna interacción con el usuario para simplificar la experiencia del usuario, se puede sugerir al usuario en varios momentos según se desee por el servicio de mensajería, la CA, etc. Requerir al menos una pulsación u otro reconocimiento positivo del usuario siguiendo la presentación de las opciones, se puede emplear por una o más razones. Por ejemplo, cuando se almacena una clave privada en el servidor de correo web 106 o cualquier otra ubicación accesible de terceras partes, se puede evitar al usuario argumentar que la clave se ha perdido. Sin embargo, se puede proporcionar al usuario la opción de almacenar la clave y recuperar la clave desde una ubicación de servidor no de terceras partes. De esta manera, para algunas realizaciones, se puede emplear las ventajas de presentar opciones alternativas durante la creación y recuperación de la clave privada, requiriendo alguna interacción positiva del usuario.

En otra realización, este proceso se repite no solo después de la primera instalación de la extensión 202, sino en cualquier momento después de que un usuario se registra en un servicio de mensajería y cuando la extensión 202 falla al detectar un certificado digital adecuado correspondiente a través de sus repositorios de preferencia clasificados 204.

Los pasos y acciones subyacentes de una realización para obtener y usar un certificado digital se describirán ahora además más adelante. Después de que se ha instalado la extensión, el usuario se registra en el servidor de mensajería 106, se registró en, o está registrado automáticamente en el servidor de mensajería 106, tal como su servicio de correo web, en su forma acostumbrada. Alternativamente, donde el usuario está empleando un cliente de correo electrónico (tal como Outlook), el usuario puede acceder al servidor de mensajería 106 automáticamente según se inicia el cliente de correo electrónico en el ordenador del usuario 104.

A continuación, sin ninguna acción adicional, o con solamente una pequeña cantidad de interacción del usuario (tal como una única pulsación para los propósitos de confirmación), la extensión del navegador obtiene un certificado digital firmado por una autoridad de certificación de manera que el usuario puede iniciar el envío de los mensajes firmados a través de su servicio de correo web. En algunas realizaciones, se puede incluir una cantidad nominal de interacción del usuario como parte de esta fase. La aceptación del usuario se puede indicar por diversos medios, se puede ser implícita a través de otras acciones del usuario, o puede ser implícita por la aceptación pasiva de ciertos procesos automáticos usados por algunas realizaciones.

En la fase 402, la extensión comprueba la presencia de las combinaciones del certificado y la clave privada existentes aseguradas para el usuario. En las realizaciones, se proporciona a un usuario uno o más repositorios de preferencia. Estos repositorios se tratan además más adelante, pero a modo de ejemplo, podrían incluir a) el almacenamiento del certificado local del navegador, y b) el servicio de correo web en sí mismo. En el caso de b), la extensión busca el servidor de tales datos en un lugar predeterminado, tal como el almacén de mensajes (como un mensaje denominado especialmente), o como los datos adjuntos a una entrada del libro de direcciones. Tales datos se pueden cifrar mediante el uso de otra clave privada para impedir a los administradores o atacantes que tienen acceso al sistema de correo web usar la clave privada del usuario para descifrar los mensajes y hacerse pasar por el usuario.

El uso de los repositorios por las realizaciones puede tener varios beneficios. Con el uso de los repositorios por algunas realizaciones, la clave privada se puede almacenar de manera segura en el servidor de correo web de manera que el usuario puede recuperar la clave desde cualquier navegador web equipado con la extensión. Aún otra ventaja de los repositorios 204 es que el usuario disminuirá drásticamente el riesgo de perder la clave debido a medios defectuosos o perdidos, tales como un impacto del disco duro, un desastre natural, o simplemente la caída de un disco flexible o una barra de memoria rápida.

Adicionalmente, si la extensión almacena la clave usando técnicas taquigráficas en el servidor de mensajería, los repositorios se pueden ocultar entre otros patrones del correo electrónico, tal como en el cuerpo o los preámbulos MIME de los mensajes seleccionados. Por facilidad de uso, la contraseña del usuario (o frases de paso) se podría teclear para identificar tales mensajes o subpartes de los mensajes. Los usuarios se pueden entrenar para evitar reutilizar sus contraseñas de registro para sus contraseñas de cifrado, y la extensión podría comprobarlo dado que la extensión puede observar las contraseñas de los usuarios en el registro inicial. Verdaderamente, en una realización, la extensión 202 puede fomentar que un usuario escoja una frase de paso de recuperación deliberadamente larga, complicada, y obtusa, y entonces anotarla y almacenarla en un lugar privado. Tal estrategia

puede proporcionar autenticación automática de dos factores, dado que para recuperar la clave el usuario necesita producir su contraseña de registro (que “conoce”) y su frase de paso.

En una realización, cuando el usuario obtiene su clave privada y desea cargarla al repositorio 204, la extensión 202 puede generar una clave de recuperación, tal como una clave simétrica de 128 bit. La extensión 202 entonces puede proporcionar la clave de recuperación al usuario, la cual el usuario puede almacenar en una lugar seguro, tal como en un disco o incluso en forma escrita. En ciertos casos, el usuario entonces puede utilizar esta clave de recuperación para reiniciar o recuperar su clave privada. La clave de recuperación se puede usar para cifrar un bloque de recuperación que incluye una pregunta de seguridad. El usuario puede usar entonces la clave de recuperación para acceder a su cuenta en el servidor de mensajería 106 para recuperar su clave privada en base al bloque de recuperación descifrado y la pregunta de seguridad. La respuesta a la pregunta de seguridad se puede usar para recuperar su clave privada.

Se puede desanimar o impedir al usuario usar preguntas de seguridad fáciles, tal como “dónde creciste”, o “a qué colegio fuiste”. Verdaderamente, el sistema 100 puede monitorizar varios sitios web y bases de datos que indican cuáles de las preguntas de seguridad son probablemente inseguras.

En la fase 404, si un certificado digital adecuado no se encuentra o no se selecciona, la extensión extrae otra información, tal como, información personal como la(s) dirección(direcciones) de correo electrónico del usuario y otra información a ser incluida en el certificado digital, tal como el nombre del usuario del servicio de mensajería. La extensión puede extraer esta información a través de las técnicas de raspado de páginas o mediante el envío de un tipo predeterminado de petición al servidor de mensajería para recuperar los datos de las preferencias almacenadas del usuario en el servidor. Alternativamente, en la fase 406, si se encuentra un certificado digital pero no se selecciona, la extensión opcionalmente puede extraer información a partir del certificado digital más que de o además de la información encontrada en el servicio de mensajería.

Opcionalmente, la extensión puede proporcionar un elemento de interfaz, tal como una ventana desplegable o una forma, para poner en marcha la extensión con la información y los controles de entrada para ver el usuario. Los controles de entrada se pueden rellenar previamente con información personal obtenida previamente, de manera que el usuario puede modificar la información. Opcionalmente, el interfaz puede impedir al usuario modificar la dirección de correo electrónico asociada con el registro al servicio, o puede permitir que múltiples correos electrónicos sean asociados con un certificado (dentro de las restricciones de la política de la CA). Además, el interfaz puede presentar la información a enseñar al usuario sobre la tecnología de certificación digital. El interfaz de usuario puede presentar información al usuario para importar o de otro modo reutilizar un certificado y la clave privada existentes en lugar de generar uno nueva. El interfaz del usuario puede presentar de manera virtual todas estas opciones como opciones avanzadas. Se puede acceder a estas opciones avanzadas, por ejemplo, a través de una pulsación adicional o confirmación para desvelar tales opciones.

Durante la operación, el usuario acepta que extensión requerirá, asociada, o reutilizará un certificado digital y la clave privada en el nombre del usuario. Esta aceptación se puede indicar de varias formas. Si el usuario elige reutilizar un certificado y la clave privada existentes, la extensión almacena esa asociación en sus preferencias y permitirá al usuario usar el correo web por la vía normal. De otro modo, la extensión provoca que sea generada una pareja de clave pública-privada, u obtenga la pareja de clave pública-privada a partir de otra fuente. Tal fuente pudiera incluir una tarjeta inteligente, un archivo en disco, u otro certificado, tal como un certificado o clave privada vencidos, aún no comprometidos.

En la fase 408, la extensión puede reunir la clave pública y otra información en una petición de certificación al servidor de CA. Varias implementaciones de petición de certificación son conocidas en la técnica, una de las cuales se conoce como una petición de firma de certificado. Esta petición se puede consumar mediante la realización del equivalente automático de presentar un formulario en línea, o mediante la llamada de interfaces de programación de aplicaciones remotas especiales. En una realización, esta petición se puede consumar mediante la realización del equivalente automático de presentar un formulario en línea, o mediante la llamada de interfaces de programación de aplicaciones remotas especiales a lado de un canal de comunicación.

En la fase 410, el servidor de CA, tras la recepción de la petición, opcionalmente recoge y registra la información adicional acerca de la petición, tal como la dirección IP de origen y el cliente (navegador y extensión) evidente que hizo la petición. El servidor de CA entonces puede enviar una respuesta usando varios canales de comunicaciones, tales como un correo electrónico, mensaje de texto, mensaje instantáneo, mensaje de teléfono, fax, etc.

La extensión recibe la respuesta y determina si la petición de la CA fue aceptada en base a la respuesta de verificación desde el servidor de CA. Como se señala, esta respuesta se puede esperar a través de uno o más canales de comunicación, tales como un correo electrónico, mensaje de texto, llamada o comunicación telefónica, fax, y similares. En particular, las realizaciones se pueden basar en las garantías de seguridad y autentificación que proporcionan múltiples canales. Por ejemplo, una verificación de la dirección de correo electrónico verifica la dirección de correo electrónico de uno (suponiendo que el sistema de correo electrónico no está comprometido); la verificación de la tarjeta de crédito verifica la información asociada con la tarjeta de crédito, tal como el nombre y la dirección de facturación (suponiendo que el sistema de la tarjeta de crédito no está comprometido). En algunas

realizaciones, el sistema proporciona la verificación de múltiples partes de información a través de múltiples canales con pocas o ningunas interacciones del usuario.

En una realización, el sistema verifica múltiples direcciones de correo electrónico asociadas con un registro particular. Una práctica común, por ejemplo, es que el usuario tenga múltiples direcciones de correo electrónico (user@example.com, user@webmail.com, user@school.edu) y reenviar todos los mensajes a una cuenta de correo web designada. En una realización ejemplar, el usuario inscribe cada dirección separadamente, por ejemplo, mediante: a) la sugerencia automática cuando la extensión detecta una nueva dirección De que el usuario está usando, mediante el análisis del interfaz de correo web, o b) manualmente a través de la indicación del usuario, tal como pulsando un botón en un interfaz.

En algunos casos, el usuario puede emplear múltiples certificados, por ejemplo, uno por dirección, pero si se desea, el usuario también puede ser capaz de reutilizar una clave privada usada previamente. En la realización en cuestión, el usuario puede indicar que múltiples direcciones de correo electrónico van a estar presentes en el certificado. Siguiendo los pasos, la extensión repite de esta manera su procesamiento para cada dirección de correo electrónico y cada mensaje recibido, hasta que se verifican todas las direcciones de correo electrónico. Entonces la autoridad de certificación expide el certificado digital por el procedimiento anteriormente mencionado.

Alternativamente, el usuario puede mantener múltiples direcciones de correo electrónico que no reenvían automáticamente a una cuenta. En tal caso: la extensión puede monitorizar múltiples cuentas a las que el usuario está registrado en esas cuentas o que la extensión obtiene las credenciales de registro del usuario. Como otra alternativa, la extensión puede proporcionar un interfaz de usuario para la introducción de códigos de verificación, los cuales el usuario puede introducir en cualquier momento. Esta realización alternativa proporciona casos en los que la extensión no tiene control programable sobre ciertos canales de verificación, tales como el correo postal o la llamada de teléfono.

Las realizaciones multicanal anteriormente mencionadas pueden presentar tales códigos de verificación a la CA de una manera serie según se reciben y por ello pueden presentar al usuario indicios, tales como una marca de los siguientes códigos de código, que indica que la CA aceptó el código, o puede amontonar todos o los subconjuntos seleccionados de los códigos de verificación a la CA en tan sólo un paso.

En el caso de una respuesta inmediata, tal como por correo electrónico o mensaje instantáneo, la extensión puede presentar un interfaz de usuario opcional que indica que la petición está siendo procesada y debería llegar en breve. Para respuestas más largas, tales como un correo electrónico, mensaje instantáneo o correo postal retardados, la extensión puede notificar al usuario que el proceso se completará tras la recepción de instrucciones o información adicional.

En algunas realizaciones, la extensión del navegador se configura para detectar la respuesta, tal como un correo electrónico. Es decir, la extensión del navegador puede monitorizar los correos electrónicos recibidos por el usuario hasta que llega el mensaje de verificación deseado y entonces puede actuar tras el mensaje automáticamente con o sin la interacción del usuario. Tras la recepción de un mensaje de verificación, el cual opcionalmente está firmado para impedir un ataque de suplantación de identidad basado en temporización, la extensión sigue un enlace integrado u otra información integrada (por ejemplo, los códigos de verificación) a una ubicación de recogida, tal como una URL, en el servidor de CA.

En otra realización, el servidor de CA puede incluir el certificado digital firmado por la CA dentro de su respuesta en forma de un mensaje de verificación. En esta realización, se pueden usar las técnicas conocidas en la técnica, tales como la vinculación a un sitio de verificación de la CA a través de SSL (HTTPS). El navegador y la extensión pueden presentar un número aleatorio a usar una sola vez, tal como uno formado en base a la URL u otra información integrada con el servidor de CA autentificado. Esta técnica puede ser útil, por ejemplo, para evitar vulnerabilidades de estancamiento y de hombre en el medio.

La CA puede incluir cualquier información en el certificado que la CA desea afirmar, consistente con las políticas de la CA. Por ejemplo, la verificación de la dirección de correo electrónico puede ligar la petición, por ejemplo, sobre HTTP con una dirección de correo electrónico. Las direcciones IP grabadas durante la secuencia de petición y la secuencia de recogida de verificación posterior se pueden introducir en los atributos incluyendo el DN, los atributos firmados, u otras estructuras del certificado digital. Aunque la dirección IP puede no identificar únicamente al usuario, la grabación de las direcciones IP puede hacer más fácil el seguimiento de los usuarios maliciosos de dichos certificados. Adicionalmente, el almacenamiento de las direcciones IP en los certificados expedidos puede servir a una función de aviso público. Tal inclusión pública además desanimaría a los usuarios maliciosos de enviar, por ejemplo, correo basura debido a que se podría hacer un seguimiento de su adquisición de certificados a las direcciones IP particulares en momentos particulares y desde esa dirección IP en particular.

En la fase 412, tras recoger el certificado digital, la extensión provoca que el certificado digital y la clave privada sean unidos y entonces se puedan usar por el usuario en su mensajería. Opcionalmente, la extensión puede presentar una indicación al usuario de que la operación se completó con éxito, que el usuario puede iniciar usando la tecnología de certificación digital, y que el usuario puede indicar que le gustaría aprender más acerca de tal

tecnología.

Los distintos destinatarios de mensajes pueden usar los agentes de mensajería con capacidades que varían ampliamente. Por ejemplo, algunos clientes de mensajería no pueden soportar la transmisión o presentación adecuada de mensajes firmados o cifrados. Varias realizaciones de la invención pueden de esta manera reunir, grabar, y actuar en las propiedades de los mensajes observados en el tiempo durante la comunicación entre las partes.

En una realización, los repositorios interactúan para definir los conjuntos de preferencias según se elaboraron anteriormente. Los conjuntos de preferencias definen, por categoría de información del destinatario identificado en la lista del párrafo anterior, los siguientes rasgos inclusivos en una forma por mensaje (o alternativamente o además, en forma por fecha y hora): las direcciones de correo electrónico; los certificados; si y a qué extensión les gustaría a los destinatarios recibir los eslóganes y mensajes solamente firmados, en base a las respuestas observadas; los clientes de correo electrónico que el destinatario usa; las pasarelas intermedias y los filtros de correo; otras cabeceras de correo electrónico; otra información de encaminamiento del correo electrónico; las preferencias expresadas de los destinatarios (es decir, aquéllas de quienes el usuario está recibiendo mensajes y a quienes el usuario enviará mensajes); y las preferencias de conducta explícitas independientes de o como consecuencia de los rasgos observados.

Para cada mensaje que se recibe, la extensión puede grabar alguna información dada anteriormente en un repositorio adecuado. Estos registros se pueden amontonar y transmitir a los repositorios remotos en el tiempo, para minimizar el consumo de ancho de banda de esta manera, los repositorios o partes de los repositorios se pueden almacenar en caché. La conveniencia de un repositorio dado también es una función del conjunto de preferencias, pero en una realización preferente, ciertos repositorios serían solamente de lectura, tal como aquéllos en los servidores centrales de políticas o el repositorio por defecto del sistema.

Para los propósitos de eficiencia, una realización puede resumir los rasgos observados en preferencias pre calculadas. Tal cálculo previo puede ahorrar ancho de banda de acceso y tiempo de procesamiento. Por ejemplo, después de la observación un mes del correo electrónico, la extensión puede calcular “para el destinatario r@x.com, siempre enviar los correos electrónicos firmados,” porque el 95% de los correos electrónicos observados demuestran el uso de un cliente de correo electrónico compatible. A partir de entonces, con el uso de esta preferencia, la extensión no necesita integrar continuamente los resultados del mes previo para ese usuario.

En una realización, la extensión puede automáticamente o en la dirección del usuario presentar los resultados agregados de ciertas clases de destinatarios, tales como, los resultados de si unos clientes de correo de los destinatarios del dominio entero pueden interpretar los mensajes firmados para los autores de la extensión para la integración en los repositorios globales o de otro modo ampliamente disponibles. En otra realización, en la primera instalación, activación, o tras detectar que cierta información del repositorio está indisponible y sin inicializar, la extensión puede indexar los mensajes para grabar las capacidades en evolución de los clientes de correo de los destinatarios en el tiempo.

Cuando se compone un mensaje, la extensión se puede basar en el conjunto de preferencias en la determinación de si firmar por defecto (o bien firmar claro o firmar opaco), o cifrar el mensaje dado para un conjunto dado de destinatarios. La extensión puede permitir opcionalmente al usuario modificar aquellas preferencias para el mensaje sometido a composición.

Las preferencias no está limitadas a si se firma o cifra un mensaje: las preferencias podrían incluir adicionalmente los siguientes rasgos: si almacenar una copia indexable y texto en claro del mensaje en el servidor de mensajería para que lo lea el usuario; si producir un cuerpo cifrado único para entregar a todos los destinatarios que incluye la capacidad de cualquier destinatario de descifrar los datos enviados a cualquier otro destinatario, o si producir múltiples cuerpos cifrados, donde cada destinatario recibe los datos que solamente puede descifrar el destinatario; si el cuerpo o cuerpos cifrados también se pueden descifrar por el remitente, y en caso afirmativo, mediante qué claves privadas del remitente; si cifrar para entidades adicionales, tales como una entidad de recuperación o de conformidad en el caso de litigio u otra necesidad; con qué algoritmos firmar y cifrar; si los destinatarios soportan codificaciones MIME particulares tales como de 8 bites o binaria; y qué estándares de mensajería segura (tal como S/MIME v3) usar.

Una muestra de cómo interactúan los repositorios para definir los conjuntos de preferencias y las selecciones UI por defecto se ilustra en la FIG. 7. Con referencia ahora a la FIG. 7, el conjunto de preferencias efectivo se usa para calcular más que dictar la selección UI por defecto. Para el Ordenador 2, ninguno de los correos electrónicos para los destinatarios enumerados se firma jamás por defecto porque no hay clave privada con la que firmar, a pesar del hecho que el conjunto de preferencias sugiere que se deberían firmar algunos correos electrónicos.

Se pretende que la especificación y los ejemplos sean considerados como ejemplares solamente. Por ejemplo, son posibles muchas otras variaciones. El navegador y la extensión se pueden combinar en una parte funcional del programa informático. La extensión puede estar dando los permisos y la confianza adecuados y se puede integrar mediante JavaScript, enchufables, controles binarios, u otros elementos que residen en un contexto de seguridad de

página. Además, las realizaciones de la presente invención pueden ser aplicables a aplicaciones distintas de un navegador, tales como un cliente de correo electrónico, un cliente de mensajería, una aplicación en un teléfono móvil, o similares. El alcance verdadero de la invención se indica por las siguientes reivindicaciones.

REIVINDICACIONES

1. Un método de asegurar comunicaciones, dicho método que comprende:

acceder a un servicio de mensajería (106);

obtener la información de identificación que identifica un usuario del servicio (106);

en respuesta al consentimiento por el usuario y sin interacción adicional con el usuario, obtener una pareja de claves que comprende una clave pública y una clave privada, y presentar una petición de un certificado a una autoridad de certificación (CA) en base a la pareja de claves;

recibir un código de verificación desde la CA;

confirmar la recepción del código de verificación de dicha CA;

proporcionar un certificado para el usuario en base al código de verificación y la pareja de claves; y

asegurar las comunicaciones desde el usuario en base al certificado.

2. El método de la reivindicación 1, en el que el consentimiento por el usuario comprende una acción única por el usuario, el método que además comprende en respuesta a la acción única por el usuario y sin interacción adicional con el usuario, detectar un certificado preexistente y una clave privada preexistente.

3. El método de la reivindicación 1, en el que la recepción del código de verificación desde la CA se dirige en respuesta a una acción única por el usuario y sin interacción adicional con el usuario.

4. El método de la reivindicación 1, en el que la confirmación de recepción del código de verificación comprende seguir un enlace automáticamente a un sitio web designado por la CA.

5. El método de la reivindicación 1, en el que proporcionar un certificado para el usuario en base al código de verificación y la pareja de claves se dirige en respuesta a la acción única por el usuario y sin interacción adicional con el usuario.

6. El método de la reivindicación 1, en el que la confirmación de recepción del código de verificación de dicha CA comprende la monitorización de los mensajes recibidos que tienen información relacionada con la petición del certificado.

7. El método de la reivindicación 1, que además comprende la presentación de un interfaz a un usuario para una oportunidad de confirmar el código de verificación.

8. El método de la reivindicación 1, en el que el consentimiento por el usuario es una aceptación pasiva de un proceso automatizado.

9. El método de la reivindicación 1, en el que el consentimiento por el usuario es un consentimiento anterior al funcionamiento del método.

10. El método de la reivindicación 9, en el que el consentimiento anterior es al menos uno de instalar un producto y la ejecución del producto configurado para realizar el método.

11. El método de la reivindicación 1, que además comprende:

proporcionar una clave de recuperación para un usuario para reinicializar o recuperar la clave privada del usuario.

12. El método de la reivindicación 1, que además comprende:

componer una estructura de datos que contiene una versión cifrada de la clave privada, donde la clave de cifrado para la estructura de datos se deriva en parte de la información derivada de al menos una de una clave de recuperación proporcionada al usuario, y la información secreta conocida por el usuario; y

cargar la estructura de datos a al menos uno del servicio de mensajería y una ubicación accesible por el usuario para la recuperación futura.

13. El método de la reivindicación 1, que además comprende:

permitir a un usuario proporcionar una frase de paso de recuperación para la recuperación de la clave privada del usuario.

14. Un aparato que comprende los medios configurados para realizar el método de cualquier reivindicación

precedente.

15. Un medio legible por ordenador que comprende el código de programa ejecutable configurado para realizar el método de cualquiera de las reivindicaciones 1 a 13.

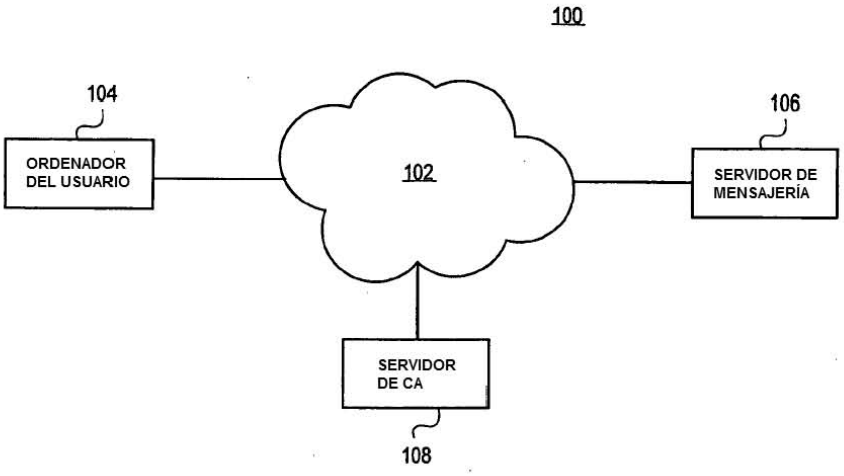
100
104
ORDENADOR DEL USUARIO
102
106
SERVIDOR DE MENSAJERÍA
SERVIDOR DE CA
108

FIG. 1

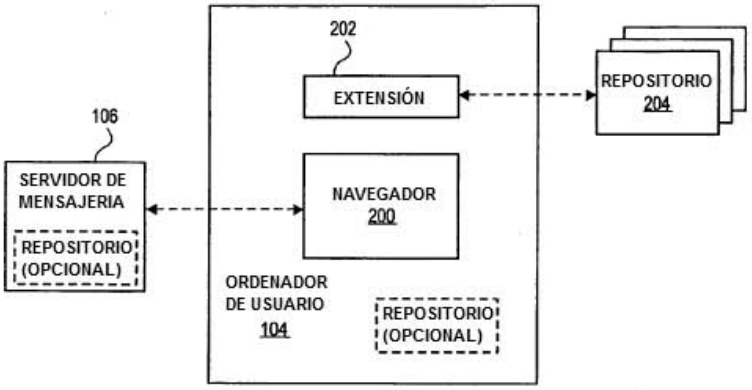
202
EXTENSIÓN
REPOSITORIO
204
106
SERVIDOR DE
MENSAJERIA
REPOSITORIO
(OPCIONAL)
NAVEGADOR
200
ORDENADOR
DE USUARIO
104
REPOSITORIO
(OPCIONAL)

FIG. 2

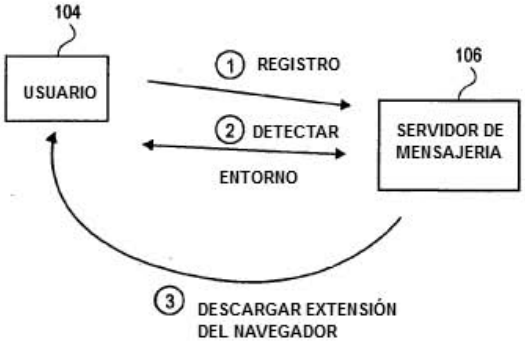
104
USUARIO
1 REGISTRO
106
2 DETECTAR
ENTORNO
SERVIDOR DE
MENSAJERIA
3 DESCARGAR EXTENSIÓN
DEL NAVEGADOR

FIG. 3

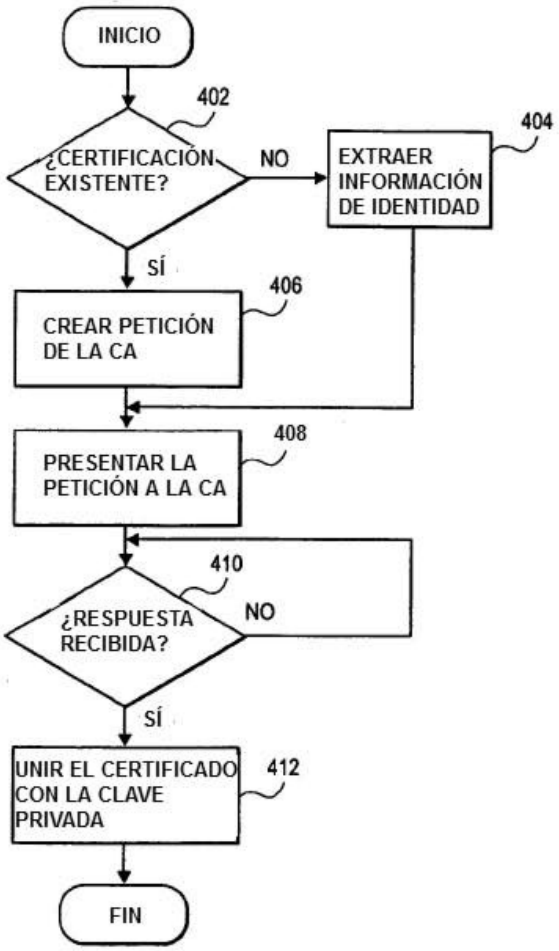
INICIO
402
¿CERTIFICACIÓN EXISTENTE?
NO
404
EXTRAER INFORMACIÓN DE IDENTIDAD
SÍ
406
CREAR PETICIÓN DE LA CA
408
PRESENTAR LA PETICIÓN A LA CA
410
¿RESPUESTA RECIBIDA?
NO
SÍ
412
UNIR EL CERTIFICADO CON LA CLAVE PRIVADA
FIN

FIG. 4

```
--gmsm0.2.4eqf7saj8hvzwe2kjh9ys2
Content-Type: application/pkcs7-signature; name="Ext Digital Signature.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="Ext Digital Signature.p7s"
Content-Description: S/MIME Cryptographic Signature

MIIJ0QYJKoZIhvcNAQcCoIIJwjCCCb4CAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3
```

FIG. 5

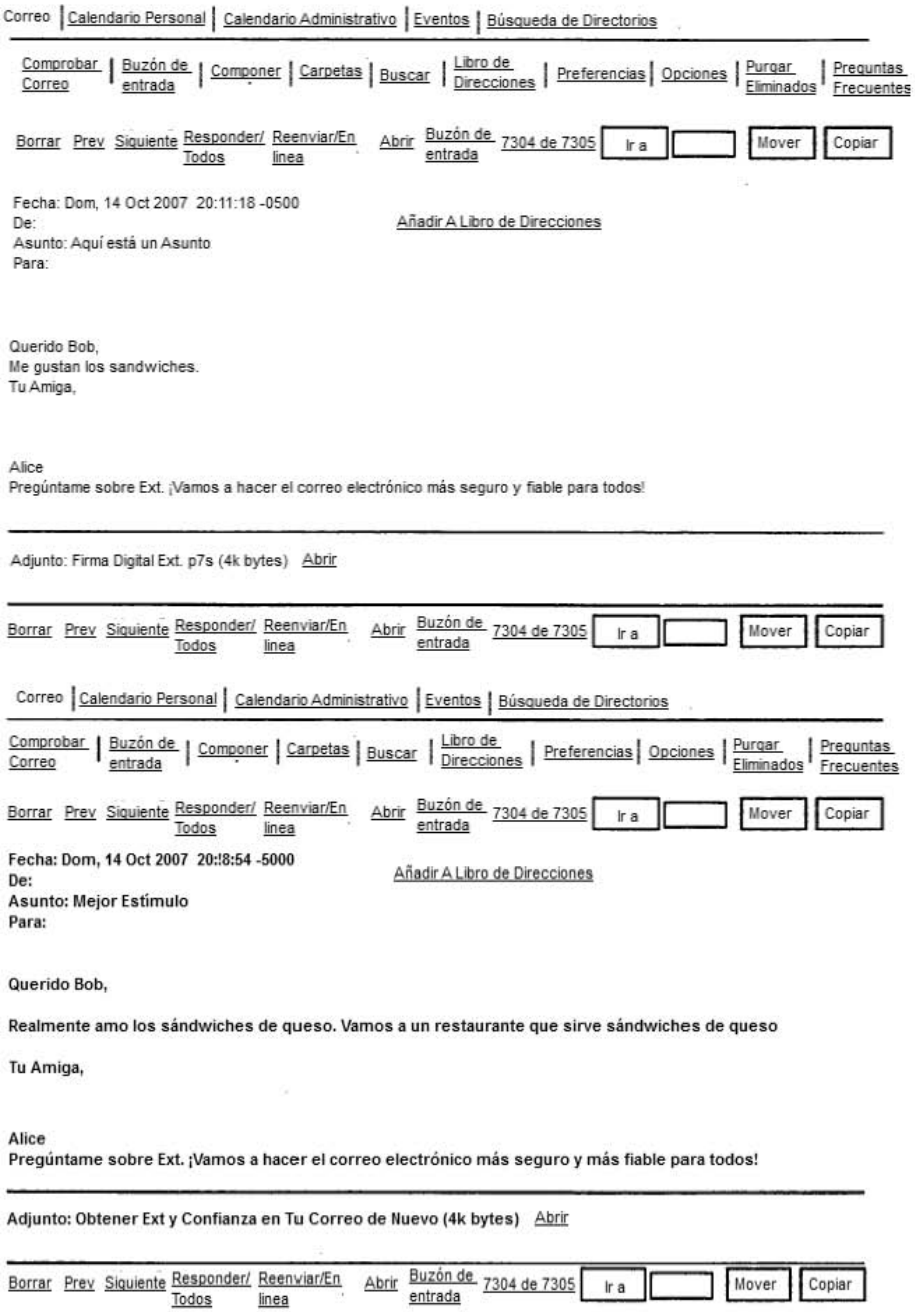
Correo | Calendario Personal | Calendario Administrativo | Eventos | Búsqueda de Directorios
Comprobar Correo | Buzón de entrada | Componer | Carpetas | Buscar | Libro de Direcciones | Preferencias | Opciones | Purgar Eliminados | Preguntas Frecuentes
Borrar Prev Siguiente Responder/ Todos Reenviar/En línea Abrir Buzón de entrada 7304 de 7305 Ir a Mover Copiar
Fecha: Dom, 14 Oct 2007 20:11:18 -0500
De:
Asunto: Aquí está un Asunto
Para:
Añadir A Libro de Direcciones
Querido Bob,
Me gustan los sandwiches.
Tu Amiga,
Alice
Pregúntame sobre Ext. ¡Vamos a hacer el correo electrónico más seguro y fiable para todos!
Adjunto: Firma Digital Ext. p7s (4k bytes) Abrir
Borrar Prev Siguiente Responder/ Todos Reenviar/En línea Abrir Buzón de entrada 7304 de 7305 Ir a Mover Copiar
Correo | Calendario Personal | Calendario Administrativo | Eventos | Búsqueda de Directorios
Comprobar Correo | Buzón de entrada | Componer | Carpetas | Buscar | Libro de Direcciones | Preferencias | Opciones | Purgar Eliminados | Preguntas Frecuentes
Borrar Prev Siguiente Responder/ Todos Reenviar/En línea Abrir Buzón de entrada 7304 de 7305 Ir a Mover Copiar
Fecha: Dom, 14 Oct 2007 20:!8:54 -5000
De:
Asunto: Mejor Estímulo
Para:
Añadir A Libro de Direcciones
Querido Bob,
Realmente amo los sándwiches de queso. Vamos a un restaurante que sirve sándwiches de queso
Tu Amiga,
Alice
Pregúntame sobre Ext. ¡Vamos a hacer el correo electrónico más seguro y más fiable para todos!
Adjunto: Obtener Ext y Confianza en Tu Correo de Nuevo (4k bytes) Abrir
Borrar Prev Siguiente Responder/ Todos Reenviar/En línea Abrir Buzón de entrada 7304 de 7305 Ir a Mover Copiar

FIG. 6

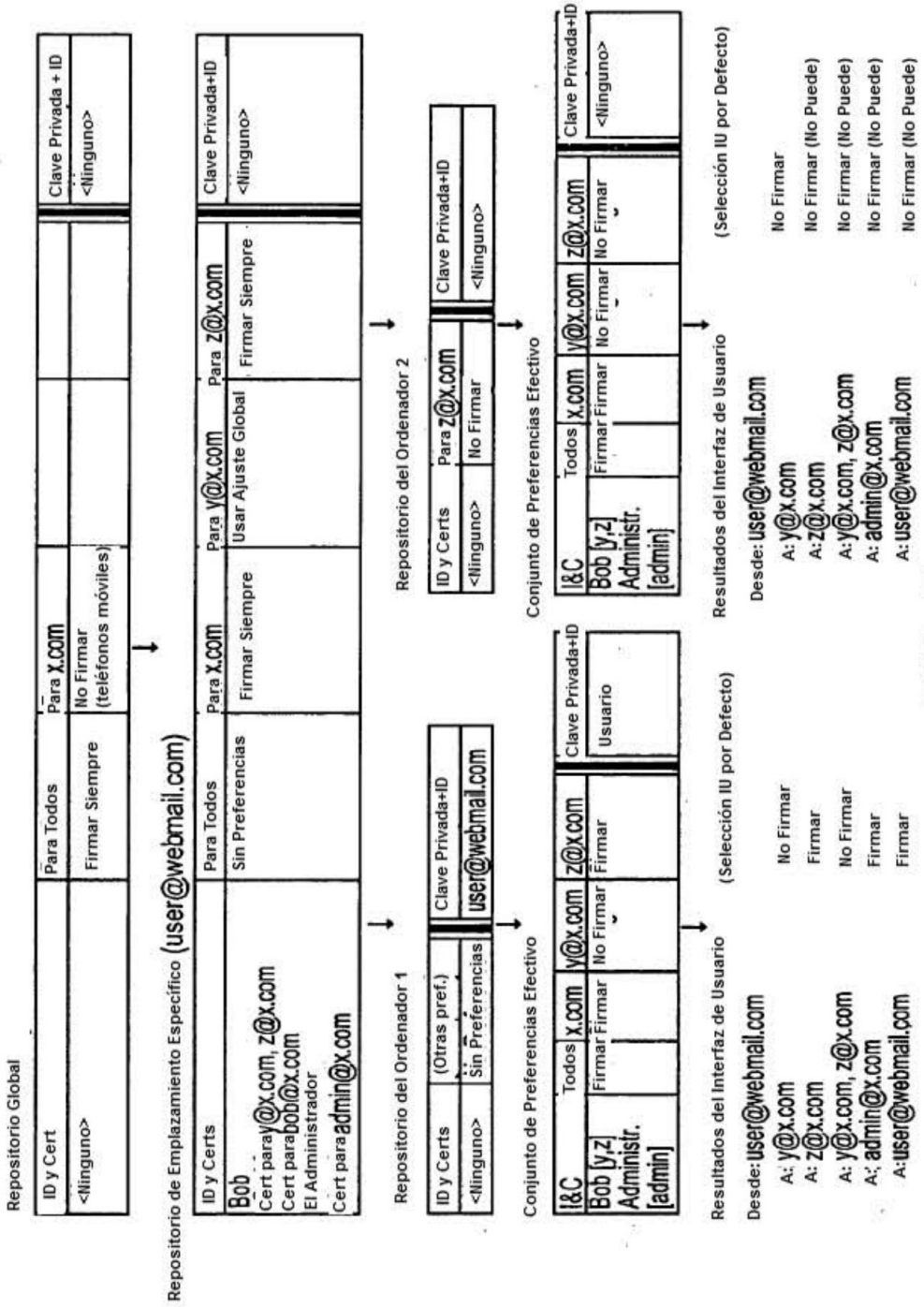
Repositorio Global
ID y Cert
Para Todos
Para x.com
Clave Privada + ID
<Ninguno>
Firmar Siempre
No Firmar (teléfonos móviles)
Repositorio de Emplazamiento Específico (user@webmail.com)
ID y Certs
Para Todos
Para x.com
Para y@x.com
Para z@x.com
Clave Privada+ID
Bob
Cert para y@x.com, z@x.com
Cert para bob@x.com
El Administrador
Cert para admin@x.com
Sin Preferencias
Firmar Siempre
Usar Ajuste Global
Firmar Siempre
<Ninguno>
Repositorio del Ordenador 1
ID y Certs
(Otras pref.)
Clave Privada+ID
<Ninguno>
Sin Preferencias
user@webmail.com
Repositorio del Ordenador 2
ID y Certs
Para z@x.com
Clave Privada+ID
<Ninguno>
No Firmar
<Ninguno>
Conjunto de Preferencias Efectivo
I&C
Todos
x.com
y@x.com
z@x.com
Clave Privada+ID
Bob [y,z] Administr. [admin]
Firmar Firmar
No Firmar
Firmar
Usuario
Conjunto de Preferencias Efectivo
I&C
Todos
x.com
y@x.com
z@x.com
Clave Privada+ID
Bob [y,z] Administr. [admin]
Firmar Firmar
No Firmar
No Firmar
<Ninguno>
Resultados del Interfaz de Usuario
(Selección IU por Defecto)
Desde: user@webmail.com
A: y@x.com
No Firmar
A: z@x.com
Firmar
A: y@x.com, z@x.com
No Firmar
A: admin@x.com
Firmar
A: user@webmail.com
Firmar
Resultados del Interfaz de Usuario
(Selección IU por Defecto)
Desde: user@webmail.com
A: y@x.com
No Firmar
A: z@x.com
No Firmar (No Puede)
A: y@x.com, z@x.com
No Firmar (No Puede)
A: admin@x.com
No Firmar (No Puede)
A: user@webmail.com
No Firmar (No Puede)

FIG. 7