(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 299 667**

(51) Int. Cl.:
G06Q 10/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **03077588 .6**
(86) Fecha de presentación : **08.11.2001**
(87) Número de publicación de la solicitud: **1365340**
(87) Fecha de publicación de la solicitud: **26.11.2003**

(54) Título: **Un sistema de gestión de la información.**

(30) Prioridad: **08.11.2000 GB 0027280**
07.08.2001 US 923704

(45) Fecha de publicación de la mención BOPI:
01.06.2008

(45) Fecha de la publicación del folleto de la patente:
01.06.2008

(73) Titular/es: **Orchestria Limited**
190 The Strand
London WC2R 1JN, GB

(72) Inventor/es: **Malcolm, Peter Bryan;**
Napier, John Anthony;
Stickler, Andrew Mark;
Tamblin, Nathan John;
Beadle, Paul James Owen y
Crocker, Jason Paul

(74) Agente: **Ungría López, Javier**

DESCRIPCIÓN

Un sistema de gestión de la información.

Antecedentes de la invención

Esta invención se refiere a la provisión de funcionalidad de gestión ampliada para aplicaciones de Internet, en particular en las zonas de seguridad de la información, auditoría e informes de transacción, política centralizada, y conectividad de aplicaciones.

El comercio electrónico ("eCommerce"), en particular entre empresas ("B2B"), pero también entre empresas y consumidores ("B2C"), es un mercado en rápido crecimiento donde compradores y vendedores se comunican usando Internet, una red mundial de sistemas informáticos conectados, en lugar de por los medios tradicionales tales como el correo, el teléfono y los encuentros personales. Los vendedores anuncian productos y servicios usando folletos y catálogos digitales, que se pueden ver o descargar mediante una conexión de Internet, a través de páginas en la web mundial, o mediante mercados electrónicos que negocian típicamente con los artículos y servicios de un sector mercantil concreto. Los compradores pueden encontrar proveedores, seleccionar artículos, obtener precios, realizar pedidos y hacer su seguimiento, e incluso hacer pagos de forma totalmente electrónica y en cualquier tiempo. El comercio electrónico promete una mayor flexibilidad, opción y eficiencia, con costos de adquisición drásticamente reducidos.

Hay dos medios universalmente aceptados de conectar los usuarios a Internet. El primero de estos es el 'Navegador Web' que permite a los usuarios ver páginas en la web mundial accediendo a sitios web individuales, cuyas direcciones se publican típicamente ampliamente o usando medios tradicionales, o son referenciadas en otro sitio de la web. El navegador web más ampliamente adoptado es "Internet Explorer" de Microsoft Corporation.

Los segundos medios de conexión son utilizar un programa de correo electrónico, con el que el usuario crea un mensaje, conocido como un correo electrónico, que posteriormente es dirigido electrónicamente a la dirección del receptor previsto por Internet. Los programas de correo electrónico conocidos incluyen "Lotus Notes" de IBM Corporation y "Outlook" de Microsoft Corporation.

En un escenario típico de comercio electrónico, un comprador podría identificar un producto concreto, juntamente con el precio e información de entrega, en el sitio web del vendedor. Entonces puede hacer un pedido, rellenando un formulario de pedido electrónico en el sitio web, o enviando un correo electrónico directamente al vendedor. El pedido incluiría típicamente un compromiso de pago, tal vez en forma de detalles de una tarjeta de crédito, o por algún medio de pago electrónico. El vendedor enviaría entonces típicamente un correo electrónico de retorno confirmando la aceptación del pedido.

Los navegadores web operan según normas reconocidas, en particular el Protocolo de Transferencia de Hipertexto ("HTTP"), descrito completamente en el documento de normas de Internet RFC2616. Los programas de correo electrónico operan según normas reconocidas, en particular Protocolo Simple de Transferencia de Correo ("SMTP"), descrito completamente en el documento de normas de Internet RFC0821 y Multipurpose Internet Mail Extensions ("MIME") descritas completamente en los documentos de normas de Internet RFC2045-2049.

Aunque el comercio electrónico proporciona enormes beneficios, su adopción plantea muchos problemas nuevos, que deben ser afrontados con el fin de asegurar su adopción continuada, en particular si ha de sustituir en último término a los métodos tradicionales. Uno de los problemas centrales es la seguridad.

Internet es una red de comunicaciones abiertas, que es por definición insegura, dado que cualquiera la puede usar. Se han proporcionado medios para asegurar el intercambio de información sensible por Internet (por ejemplo en una transacción de comercio electrónico) mediante la adopción de protocolos y mensajes de transmisión seguros. Los protocolos seguros de transmisión punto a punto, usados por ejemplo entre un servidor web y un navegador web, incluyen 'Secure Socket Layer' ("SSL"), definido por Netscape Communications Corporation, y su sucesor 'Transport Layer Security' ("TLS") definido en el documento de normas de Internet RFC2246. Las normas de mensajes por correo electrónico seguros incluyen 'Secure Multipurpose Internet Mail Extensions' ("S/MIME") descrito completamente en el documento de normas de Internet RFC2633 y "Pretty Good Privacy", un sistema de mensajes seguros de dominio público desarrollado por Philip Zimmerman.

Para controlar el acceso a información en servidores conectados a Internet, se ha adoptado ampliamente un sistema de nombres de usuario y contraseñas. Por ejemplo, el acceso a listas de precios con descuento en un servidor web concreto puede estar restringido a usuarios comerciales que previamente han dado un nombre de usuario y contraseña que les permiten acceder. Igualmente, los servicios de información en línea hacen típicamente amplio uso de nombres de usuario y contraseñas para restringir el acceso a quienes han pagado por el servicio. Proporcionando a cada usuario un único nombre de usuario y una contraseña cambiable, el servicio puede asegurar que solamente los abonados que hayan pagado puedan acceder al sistema, y que los usuarios puedan evitar el acceso por parte de otros a sus datos personales almacenados por el servicio.

En aplicaciones de comercio electrónico, un problema principal es la cuestión de identidad y confianza. Cuando un proveedor recibe un pedido mediante Internet es perfectamente posible, incluso probable, que no tenga conocimiento previo del cliente. El proveedor debe determinar que el cliente es a) quien dice ser, en otros términos que he no se está haciendo pasar por otra persona, y b) ha de ser de confianza y en último término pagar por los artículos o servicios a suministrar. Estas cuestiones han sido afrontadas en el mercado B2C principalmente por el uso de tarjetas de crédito. El cliente proporciona su número de tarjeta de crédito y dirección con el pedido, que el proveedor verifica posteriormente con la compañía de tarjetas de crédito, y obtiene autorización para el cargo. Todo el proceso se lleva a cabo típicamente en línea sin intervención humana. Este método es en gran parte efectivo donde un proveedor envía artículos a la dirección del tenedor de la tarjeta, dado que un robo potencial no solamente tendría que robar los detalles de los tenedores de las tarjetas, sino que también tendría que interceptar la entrega de los artículos. Es mucho menos efectivo en el caso de servicios que no implican entrega física.

Claramente, el uso de tarjetas de crédito en comercio electrónico, aunque está difundido, queda restringido a transacciones en pequeña escala que implican potencialmente cantidades, por ejemplo, de hasta $10.000. Para las transacciones superiores a dicha cantidad (que en términos monetarios agregados exceden con mucho de las inferiores a aquellas), hay que utilizar una tercera parte de confianza mutua para determinar la identidad y la confianza.

Esencial para determinar la identidad es el uso de certificados digitales. Al cliente se le puede conceder un certificado digital por una tercera parte de confianza, que entonces se utiliza para 'firmar' electrónicamente comunicaciones. A la recepción de un mensaje firmado, el receptor (en este caso el proveedor) puede determinar positivamente a) la identidad del emisor, b) que el mensaje no ha sido alterado, y c) que el emisor no puede negar posteriormente que envió el mensaje. Las normas reconocidas para certificados digitales se describen en el documento ITU X.509, y su uso en comunicaciones por Internet en los documentos de normas de Internet RFC2312, RFC2459, RFC2510, RFC2511, RFC2527, RFC2560, RFC2585 y RFC2632.

Se puede utilizar servicios cargables a terceros, tal como el proporcionado por Valicert Inc., para verificar que un certificado digital no ha sido revocado, por ejemplo después de que el certificado ha sido cuestionado de alguna forma.

Una vez determinada la autenticidad de los mensajes, el proveedor puede usar otra tercera parte para establecer confianza, o se puede utilizar la misma tercera parte para determinar tanto la autenticidad como la confianza. Por ejemplo "Identrus", un consorcio de los principales bancos mundiales, proporciona un sistema tal que cuando un proveedor recibe un mensaje firmado con un certificado digital concedido por Identrus, puede verificar independientemente que el cliente es un tenedor de cuenta válido de buena reputación con un banco reconocido. En último término, el sistema se ha de ampliar de tal manera que el banco garantice adicionalmente la transacción, garantizando por ello el pago al proveedor. Se apreciará que los términos 'cliente' y 'proveedor' se pueden aplicar a cualesquiera dos partes participantes en la comunicación por Internet.

Se puede ver que combinaciones apropiadas de los sistemas descritos proporcionan un fundamento seguro para uso de Internet y los servicios y funciones disponibles por su mediación. Sin embargo, hemos apreciado que la realización de comercio electrónico usando solamente estos sistemas tiene varios problemas. Estos problemas se explican a continuación.

En los protocolos y mensajes de transmisión seguros referidos anteriormente, los datos son encriptados generalmente antes de la transmisión y desencriptados por el receptor previsto antes de verlos. Así, si los datos fuesen interceptados durante la transmisión, estarían a salvo de que los viesen terceras partes no autorizadas a no ser que conozcan o puedan conocer la clave secreta encriptada del algoritmo encriptado.

El encriptado y desencriptado de datos en cada extremo de un enlace o mensaje seguros requiere significativa potencia de procesado. Además, las partes transmisora y receptora deben estar en posesión de la misma clave de encriptado del algoritmo encriptado, de la misma potencia criptográfica, para que el sistema opere satisfactoriamente. A menudo esto presenta un problema, por ejemplo donde las normas para la importación o exportación de datos a o de un sistema informático prohíben el uso de algoritmos de mayor fuerza, obligando a que el enlace o mensaje sea encriptado con una potencia criptográfica menor, o evitando por completo las comunicaciones seguras. En consecuencia, los enlaces y mensajes seguros se usan típicamente solamente cuando es necesario.

En el caso de comunicaciones por la web mundial, el requisito de asegurar las transmisiones lo determina e inicia el servidor web. Si, por ejemplo, el servidor está a punto de transmitir un formulario de pedido para terminación por el usuario, puede iniciar un enlace seguro de tal manera que la información del pedido sea encriptada cuando sea transmitida de nuevo al servidor. Igualmente, una vez completado el pedido, el servidor puede terminar el enlace seguro y volver a la comunicación no encriptada normal.

Típicamente, la única indicación que el usuario tiene de que un enlace es seguro es un icono (que ilustra generalmente un candado), que aparece en la ventana del navegador. Una vez que el icono ha aparecido, el usuario puede interrogar entonces típicamente al navegador para determinar la fuerza del algoritmo encriptado que se utiliza, y puede decidir si entrar o no, y posteriormente transmitir información sensible, tal como los detalles de su tarjeta de crédito y dirección.

Sin embargo, en la práctica, los usuarios frecuentemente no comprueban que el enlace sea seguro, y mucho menos que sea de la potencia criptográfica adecuada para proteger la información transmitida. Con el fin de resolver este problema, las aplicaciones de correo electrónico tales como "Outlook" de Microsoft Corporation proporcionan la capacidad de encriptar todos los correos electrónicos por defecto.

La amplia adopción de nombres de usuario y contraseñas ha creado un problema de gestión para muchos usuarios de Internet debido al simple número que tienen que recordar, en particular cuando la buena práctica de seguridad requiere el cambio frecuente de contraseñas. Igualmente, a menudo los usuarios tendrán que utilizar varios nombres de usuario diferentes dado que alguna otra persona puede haber tomado ya su 'favorito' en un sitio dado. Los navegadores web tal como 'Internet Explorer' de Microsoft Corporation, y las utilidades de 'ayuda' añadidas, como Gator.com's "Gator", ofrecen facilidades para recordar, y para completar automáticamente los campos del nombre de usuario y la contraseña en ocasiones posteriores. Estas facilidades mantienen típicamente un archivo de nombres de usuario, contraseñas y la página web a que se aplica cada uno. Estos archivos están encriptados para asegurar que solamente el usuario apropiado pueda acceder a ellos. Si se pierden dichos archivos de nombre de usuario y contraseña o no están disponibles, tal como cuando el usuario autorizado ha olvidado la clave encriptada o ya no puede ser contactado para proporcionarla, o cuando el archivo se pierde accidental o maliciosamente, se destruye, o corrompe, el acceso a cuentas y servicios de Internet se puede perder, y hay que acceder individualmente a cada sitio para sustituir o recuperar el nombre de usuario y/o la contraseña necesarios. Éste puede ser un problema muy caro para las compañías en términos de pérdida de acceso y tiempo de administración. Adicionalmente, tales nombres de usuario y contraseñas recordados solamente están disponibles para uso en la máquina en que se utilizaron originalmente. Si el usuario se pasa a otra máquina, o utiliza múltiples máquinas, los nombres de usuario y contraseñas almacenados no están disponibles para él desde las otras máquinas.

Todas las empresas, y muchos usuarios individuales, tienen la obligación legal de mantener registros exactos de las transacciones que realizan, pero para transacciones de comercio electrónico esto puede ser difícil de demostrar. Las empresas deben mantener registros a efectos de auditoría, por ejemplo, para demostrar los términos en los que se pidieron los artículos en caso de controversia. Tales registros son considerablemente más difíciles de mantener en un entorno de comercio electrónico, requiriendo que el usuario retenga, por ejemplo, copias de pedidos enviados por correo electrónico, o que imprima el resguardo de página web de una compra en un sitio web. Para el usuario, esto es laborioso y no garantiza que tales registros creados sean completos o fiables.

Una solución automatizada de mantener registros de transacciones de comercio electrónico la proporciona la aplicación "Max Manager" de Max Manager Corporation. Max Manager captura páginas de resguardo en páginas web conocidas, extrae información sobre transacciones de las páginas de recepción, y posteriormente guarda localmente la página de recepción y la información extraída sobre transacciones en la máquina en la que se ejecuta la aplicación. Sin embargo, con el fin de operar, a Max Manager se le debe suministrar la dirección y disposición exactas de la página de recepción. Max Manager determina que ha tenido lugar una transacción de comercio electrónico detectando la dirección de la página de recepción, o comparando la página actualmente visitada por un navegador con la disposición de la página de recepción que se le ha suministrado. Una vez identificada una página de recepción, los detalles relevantes de las transacciones son extraídos de la página de recepción usando la disposición conocido de la página como una plantilla a efectos de concordancia. Un inconveniente significativo de Max Manager es que solamente puede ser usado para extraer datos de las páginas de las que se le han suministrado detalles. Además, si se cambia la disposición de la página de recepción, Max Manager no puede extraer datos con sentido de la página hasta que reciba una nueva plantilla de la disposición cambiada. Dado que las páginas web cambian frecuentemente, Max Manager debe ser actualizado constantemente para tomar en cuenta tales cambios. Esto es inviable a gran escala y da lugar inevitablemente a que se pierdan transacciones o, lo que es peor, que se obtengan informes incorrectos.

También surgen problemas del hecho de que los terminales de ordenador están distribuidos, dando lugar a menudo a que los terminales y usuarios se encuentren en posiciones diferentes. En entornos multiusuario, las máquinas de usuario pueden estar físicamente conectadas una a otra, por ejemplo usando una red de área local ("LAN"), que proporciona una puerta de enlace para conexión a Internet. También pueden estar conectadas a servidores locales tales como el 'Exchange Server' de Microsoft Corporation, que actúa como un punto central de recogida y distribución de mensajes de correo electrónico, y el 'Proxy Server' de Microsoft Corporation, que actúa como una cache para mejorar el rendimiento de sitios web frecuentemente visitados, y como un filtro para evitar el acceso a ciertas páginas web que puedan haber sido calificadas de indeseables. Sin embargo, en lo que se refiere al intercambio de información, excepto en el caso de un mensaje enviado entre dos usuarios locales, cada usuario opera totalmente en aislamiento de otros en la misma posición. Esto presenta un problema significativo de gestión para organizaciones corporativas y otras, que no tienen medios de controlar en el centro la actividad de los empleados y no se pueden beneficiar de los significativos ahorros de costos que se podría obtener de compartir la información. Por ejemplo, dos usuarios en una organización pueden recibir independientemente mensajes de correo electrónico firmados digitalmente por el mismo emisor. Ambos receptores deben validar por separado el certificado digital, incurriendo en dos cargos por validación, de los que al menos uno era innecesario.

Un sistema y método para crear, editar y distribuir reglas para procesar mensajes electrónicos se conoce por la patente de Estados Unidos número US 5.917.489. Tales reglas son determinadas por los usuarios de estaciones de trabajo para ayudar a detectar, presentar y responder a sus mensajes.

US 6.073.142 describe un sistema y método para la posposición y revisión de mensajes de correo electrónico.

La presente invención proporciona funcionalidad adicional a los sistemas mencionados anteriormente con el fin de aliviar sus problemas inherentes y de proporcionar un solo sistema integrado para intercambio de información.

Resumen de la invención

La invención se expone en las reivindicaciones independientes a las que se hará referencia ahora. Características ventajosas de la invención se exponen en las reivindicaciones dependientes.

El sistema de gestión de información proporciona muchas ventajas en el entorno de comercio electrónico a compañías de comercio en línea, que se pueden beneficiar de ser capaces de regular las transacciones realizadas por su personal según sus instrucciones codificadas en los datos de política, mantener automáticamente registros de contraseñas y negocios realizados en línea, evitar el pago de comprobaciones innecesarias de la validez de certificados digitales, y asegurar que la transmisión de datos por su personal siempre se realice de forma segura.

Breve descripción de los dibujos

La realización preferida de la invención se describirá ahora con más detalle, a modo de ejemplo, y con referencia a los dibujos en los que:

La figura 1 es una ilustración esquemática de la presente disposición de sistemas y recursos que forman Internet según la técnica anterior.

La figura 2 es una ilustración esquemática de la realización preferida de la invención implementada en un entorno corporativo.

La figura 3 es una ilustración esquemática de la operación de un navegador web según la realización preferida de la invención.

La figura 4 es una ilustración de una ventana de entrada típica generada por un navegador web.

La figura 5 es una ilustración esquemática de la operación de un cliente de correo electrónico según la realización preferida de la invención.

La figura 6 es un diagrama de flujo que ilustra la operación de un módulo plug-in, según una realización preferida de la invención, para capturar valores de nombre de usuario y contraseña transmitidos por un usuario a un sitio web remoto.

La figura 7 es una ilustración de datos de política ejemplares especificando condiciones de control para registrar datos.

La figura 8 es un diagrama de flujo que ilustra la operación de un módulo plug-in, según una realización preferida de la invención, para reconocer números de tarjetas de crédito contenidos en datos transmitidos a o de un servidor web o cliente de correo electrónico.

La figura 9 es un diagrama de flujo que ilustra la operación de un módulo plug-in, según una realización preferida de la invención, para establecer la validez de un certificado digital recibido por un usuario.

La figura 10 es una ilustración de datos de política ejemplares para determinar si un certificado digital deberá ser verificado o no.

La figura 11 es un diagrama de flujo que ilustra cómo los datos de política ejemplares representados en la figura 10 se utilizan para determinar si se precisa una verificación de un certificado digital.

La figura 12 es un diagrama de flujo que ilustra la operación de un módulo plug-in, según una realización preferida de la invención, para identificar transmisiones de un usuario o a un usuario que incluyen parte de una transacción de comercio electrónico.

La figura 13 es una ilustración de datos de política ejemplares que se prevé usar con el proceso ilustrado en la figura 12 para identificar una transacción.

La figura 14 es un diagrama de flujo que ilustra la operación de un módulo plug-in, según una realización preferida de la invención, para registrar transmisiones identificadas como incluyendo parte de una sola transacción que forma por ello un registro de la transacción.

La figura 15 es un diagrama de flujo que ilustra la operación de un módulo plug-in, según una realización preferida de la invención, para aprobar o rechazar transacciones identificadas en base a un parámetro de política predeterminada.

La figura 16 es una ilustración de datos de política ejemplares para determinar si una transacción identificada requiere aprobación, y para identificar un aprobador apropiado.

La figura 17 es un diagrama de flujo que ilustra la operación de un módulo plug-in, según una realización preferida de la invención, para determinar un nivel apropiado de encriptado para una transmisión y permitir que la transmisión sea transmitida solamente si se proporciona dicho nivel.

La figura 18 es una ilustración de datos de política ejemplares especificando la intensidad de encriptado requerida para varios tipos de datos.

La figura 19 es una ilustración de datos de política ejemplares para controlar la redirección de mensajes de salida.

La figura 20 es un diagrama de flujo que ilustra la operación de un módulo plug-in, según una realización preferida de la invención, para redirigir mensajes de salida a una tercera parte para revisión antes de la transmisión, utilizando los datos de política representados en la figura 19.

La figura 21 es un diagrama de flujo que ilustra la operación de un módulo plug-in, según una realización preferida de la invención, para controlar la carga de información a un sitio externo a la compañía, utilizando los datos de política representados en la figura 19.

La figura 22 es una ilustración de datos de política ejemplares para controlar el envío de mensajes a receptores dentro o fuera de la compañía.

La figura 23 es un diagrama de flujo que ilustra la operación de un módulo plug-in, según una realización preferida de la invención, usando los datos de política representados en la figura 22.

La figura 24 es una ilustración de datos de política ejemplares para controlar si un mensaje de salida está firmado digitalmente.

Y la figura 25 es un diagrama de flujo que ilustra la operación de un módulo plug-in, según la realización preferida de la invención, utilizando los datos de política representados en la figura 24.

Descripción de la realización preferida

El sistema preferido proporciona a los usuarios de Internet una forma automática de gestionar el flujo de información en un sistema informático. Proporciona facilidades para gestionar el nivel de seguridad en el que tienen lugar las transmisiones, facilidades para registrar transacciones en línea y para referir a terceras partes para aprobación transacciones que están a punto de efectuarse, y medios para evitar que se produzcan transacciones si se deniega su aprobación; también proporciona facilidades para extraer y registrar datos pertinentes de cualesquiera transmisiones que sean recibidas o que estén a punto de ser transmitidas, y para gestionar inteligentemente la transmisión de correos electrónicos.

El sistema preferido proporciona soluciones para muchos de los problemas encontrados por compañías de comercio electrónico que comercian por Internet; en consecuencia la siguiente explicación ejemplar se referirá en su mayor parte a la implementación y al uso del sistema por una compañía de tamaño razonable para realizar al menos parte de su negocio por Internet. Sin embargo se apreciará que cualquier persona, incluyendo las compañías de cualquier tamaño o denominación e individuos privados, que usen Internet se pueden beneficiar de la funcionalidad que proporciona el sistema preferido.

La funcionalidad del sistema preferido se implementa a través de módulos de código que se "conectan" al navegador web o cliente de correo electrónico. Estos módulos 'plug-in' pueden ser usados para controlar y alterar el comportamiento del navegador web o cliente de correo electrónico en la operación.

Muchos navegadores web existentes y clientes de correo electrónico pueden estar ya fácilmente integrados con tales módulos plug-in. En el caso de Internet Explorer de Microsoft, el plug-in es conocido como un 'Browser Helper', y se describe de forma completa en el documento "Browser Helper Objects: The Navegador the Way You Want It" por Dino Esposito, publicado por Microsoft Corporation en Enero de 1999. En el caso de Outlook de Microsoft y Exchange e-mail Clients, el plug-in es conocido como una 'Extensión' y se describe de forma más completa en el documento "Microsoft Outlook and Exchange Client Extensions" por Sharon Lloyd, publicado por Microsoft Corporation en Marzo de 1998. El uso de los plug-ins 'Browser Helper Object' y 'Extension' realizado en el sistema preferido se describirán con más detalle más tarde.

El uso de módulos plug-in de navegador o cliente de correo electrónico para implementar la funcionalidad del sistema preferido tiene la ventaja adicional de que, dado que el encriptado de contenido de mensajes lo lleva a cabo generalmente el navegador o el cliente de correo electrónico propiamente dicho, el examen del contenido de la transmisión, para extraer información de contraseña o para determinar el nivel deseado de encriptado, por ejemplo, puede tener lugar antes de que el contenido haya sido encriptado como preparación para la transmisión, o de hecho después de haber sido recibido y desencriptado.

La figura 1 representa la relación entre proveedores de servicios, típicamente compañías que venden artículos y servicios por Internet 10, y usuarios que desean comprar tales artículos o servicios. Los usuarios provistos de los navegadores web 22, 24 y 26, pueden conectar mediante Internet y recuperar información de páginas web de servidores web 14 y 18. Alternativamente, usuarios con aplicaciones de correo electrónico 20, 30 y 32, pueden enviar y recibir mensajes de correo electrónico con abc.com y xyz.com mediante servidores de correo electrónico 12 y 16.

En un entorno corporativo, como el ilustrado en la esquina inferior derecha de la figura 1, los navegadores web 24 y 26 de un usuario corporativo están conectados a Internet mediante un servidor proxy 28. El servidor proxy 28 se usa para poner en cache páginas web y controlar el acceso a páginas web. Igualmente, la corporación tiene clientes de correo electrónico 30 y 32, conectados a Internet mediante el servidor de correo electrónico 34 que actúa como un punto central de recogida de correos electrónicos que entran a la corporación y que controla la distribución de los correos electrónicos a los usuarios individuales. Se apreciará que aunque la figura 1 describe abc.com y xyz.com como vendedores, una corporación puede ser comprador y vendedor, y como compradores abc.com y xyz.com se describirían como usuarios corporativos a los efectos de esta descripción.

En el caso de correos electrónicos enviados y recibidos por aplicación de correo electrónico personal 20, se deberá indicar que el correo será recogido y distribuido típicamente por un servidor remoto de correo electrónico proporcionado por el proveedor de servicio de conexión a Internet al que el usuario personal está abonado.

Aunque muchas de las características y funciones de este sistema proporcionan un beneficio considerable a un usuario individual, el sistema proporciona la ventaja máxima al operar en un entorno multiusuario donde se recoge información sobre transacciones de muchos usuarios. La figura 2 representa un diagrama esquemático de la configuración preferida del sistema en un entorno multiusuario. El sistema preferido incluye un servidor de gestión central 40 conectado a una base de datos 42 y consolas de operador 44. El servidor de gestión central 40 también está conectado a plug-ins de aplicación de servicios auxiliares incluyendo interfaces de aplicación 50, 52 e interface de programa de aplicación abierta 54, y a componentes de puerta de enlace 60, 62 y 64. El componente de puerta de enlace 62 se representa conectado a plug-ins de aplicación de usuario, situados en una o varias máquinas de usuario, incluyendo Internet Explorer Plug-in 70, Netscape Navigator Plug-in 72, Microsoft Outlook Plug-in 74, y Lotus Notes Plug-in 76. Estos plug-ins se usan para proporcionar la funcionalidad del sistema preferido en el programa de alojamiento en el que se integran. Se muestran cuatro programas de alojamiento posibles, Internet Explorer, Netscape Navigator, Microsoft Outlook y Lotus Notes, pero también se puede usar cualquier otro programa con la capacidad de conectar a Internet, a condición de que su comportamiento pueda ser modificado para implementar la funcionalidad del sistema preferido.

La conexión a Internet 10 se realiza mediante los plug-ins de aplicación de usuario y sus respectivos programas de alojamiento.

Los componentes de puerta de enlace 70, 72 y 74 son opcionales, pero se prefieren puesto que permiten escalar todo el sistema, almacenando y enviando información cada puerta de enlace, pudiendo conectar por ello cualquier número de usuarios.

La información de los múltiples plug-ins de aplicación 70, 72, 74 y 76 para las diferentes aplicaciones en múltiples máquinas de usuario es recogida por el servidor de gestión central 40 y almacenada en una base de datos asociada 42.

Los plug-ins de aplicación de servicios auxiliares 50, 52 y 54 permiten que el sistema conecte con aplicaciones de gestión de terceras partes tal como sistemas de procesado de pedidos y contabilidad. Esto permite que la información sobre transacciones sea introducida y procesada automáticamente por tales sistemas.

Las consolas de operador 44 se han previsto para fines administrativos, y en particular para la aprobación de transacciones. Aunque se ilustran lógicamente directamente unidas al servidor de gestión central en la figura 2, tales consolas se podrían ejecutar en cualquier máquina en red. Donde un plug-in de correo electrónico o navegador web determina que una transacción particular requiere aprobación, se envía una petición al servidor de gestión central y se pone en cola mientras está pendiente la aprobación por un operador autorizado.

La operación del sistema es controlada por datos de política, que guardan las normas de la corporación relativas a la seguridad, autorización, y las acciones que los usuarios pueden realizar, así como información operativa. Preferiblemente, los datos de política están almacenados en un archivo de política en el servidor de gestión central para acceso por cualquiera de las consolas de operador 44, plug-ins de aplicación de servicios auxiliares o plug-ins de aplicación de usuario. El administrador del sistema o supervisor de red puede definir una o más políticas o parámetros del archivo de política y puede asignar usuarios individuales o grupos de usuarios a diferentes políticas, controlando así la capacidad del usuario o incluso la capacidad de una estación de trabajo de interactuar con Internet sin la necesidad de establecer parámetros y controles directamente en cada máquina del usuario. Un usuario en el departamento de contabilidad de una compañía, por ejemplo, puede estar asignado a una “política de contabilidad”; cualquier cambio posterior en dicha política dará lugar automáticamente a un cambio en las capacidades de todos los usuarios asignados a dicha política.

Se prefiere que la capacidad de editar o establecer los datos de política esté restringida al supervisor de red u otra persona o personas autorizadas. Esto se puede lograr designando una o varias estaciones de trabajo supervisoras en la red habilitadas con acceso a editar los datos de política tales como las consolas de operador 44.

Preferiblemente, la política tiene una estructura en forma de árbol, permitiendo bajar los parámetros a los nodos de política individuales del árbol, y realizar rápidamente cambios globales, por ejemplo, si el CEO desea que todas sus compras requieran su aprobación si el flujo de dinero de la compañía fuese un problema. Tal sistema basado en política reduce en gran medida la latencia inherente tanto en sistemas de compra tradicionales como en entornos de compra de comercio electrónico corrientes.

Cada usuario de la red tendrá su propia representación de datos de política. Preferiblemente, solamente se guardan las ramas y hojas de cada política del usuario que difieren de una política de red maestro ya que esto permite ahorrar espacio en memoria. Aunque los datos de política se guardan preferiblemente en forma de archivo en el servidor de gestión central, no se ha previsto que el almacenamiento de los datos de política se restrinja a forma de archivo solamente. Se puede emplear cualquier otra representación o codificación de parámetros de política dentro del sistema preferido.

La implementación del sistema en un navegador web o en un cliente de correo electrónico se describirá ahora con más detalle.

Uso del sistema preferido en un navegador web

La figura 3 representa la operación simplificada de un navegador web. El navegador web se lanza en el paso S100 en respuesta a una petición de inicio del usuario o automáticamente del archivo de arranque del ordenador del usuario. El archivo de arranque contiene órdenes para ejecutar automáticamente programas especificados cuando el ordenador arranca. Después de que el navegador web ha arrancado, pide típicamente una 'página de inicio', la página web por defecto a ver, según una posición predeterminada. Esto se representa en el paso S102.

La petición es enviada al servidor web apropiado 90, cuya dirección de Internet exacta es determinada generalmente por Servicios de Nombres de Dominio; el servidor web 90 responde entonces con los datos apropiados que definen la página web. Este proceso se representa respectivamente como pasos S104 y S106 que dan lugar al paso S108.

Los datos que definen la página web constan de Script HTML, y otros tipos de datos posibles tales como XML o ActiveX, y Javascript que codifica programas ejecutables. El navegador interpreta estos datos, presentándolos y/o ejecutándolos según sea apropiado en el paso S110.

El navegador espera entonces típicamente una entrada de usuario en el paso S112. Tal entrada puede incluir rellenar campos visualizados, clicar en un hiperenlace, o introducir la dirección URL de una nueva página web. En último término, tales acciones dan lugar a que se envíe otra petición al servidor web 90 en el paso S114 y en el paso S116. La petición puede ser simplemente otra dirección de página web, o puede contener datos adicionales tales como los introducidos por teclado en campos visualizados por el usuario.

La figura 4 representa una pantalla de página web muestra, en la que se le presenta al usuario un GUI con el fin de recibir el nombre y la dirección de correo electrónico del usuario. Se verá por referencia a la figura 4 que el usuario ha introducido su nombre como 'Fred Smith' al campo de petición de nombre proporcionado, y su dirección de correo electrónico como 'fsmith@xyz.com' en el campo de dirección de correo electrónico.

Cuando el usuario pincha el botón "Presentar" dispuesto en la ventana de petición, los detalles que introdujo el usuario se incluyen en el pedido enviado al servidor web 90. Tal pedido podría ser:

http://www.sample.com/sample2.htm?UserID=Fred+Smith&email=fsmith@xyz.com&submit=submit

Se puede ver por lo anterior que el nombre del usuario se incorpora en la orden como el valor de una variable llamada 'UserID' y su dirección de correo electrónico se incorpora como el valor de una variable llamada 'correo electrónico'.

La orden se ensambla en el paso S114, y transmite al servidor web 90 en el paso S116 donde la información del nombre de usuario y de la dirección de correo electrónico puede ser usada, por ejemplo, para enviar información de productos al usuario mediante correo electrónico, o para acceder a otras páginas web.

El módulo plug-in proporcionado por la realización preferida de la invención en forma de un Browser Helper Object (BHO) proporciona funcionalidad adicional para aumentar la del navegador web estándar. El BHO se implementa con el fin de responder a un número de eventos significativos que tienen lugar cuando el navegador web es operado y dirigido por el usuario para interactuar con varias páginas y sitios web.

El BHO es implementado para supervisar peticiones de navegación y datos presentados al servidor web del navegador y para identificar datos que son exclusivos del usuario. Puede hacerlo buscando simplemente en los datos de salida corrientes la presencia de palabras o expresiones predeterminadas. En el caso antes representado en la figura 4, se pueden buscar las dos definiciones de las variables 'UserID' y 'email', y los datos que las siguen se pueden extraer y almacenar. Alternativamente, el BHO puede buscar el símbolo '?', que indica el final de la dirección URL con la que conecta e indica que lo que sigue son datos. El BHO también puede supervisar los datos de entrada corrientes recibidos del sitio web con el que conecta.

Además, el BHO puede ser implementado para supervisar la operación del navegador web propiamente dicho. Cuando opera el navegador web, genera 'eventos' a notificar a módulos de software codependientes u objetos que algo significativo acaba de producirse o que una acción acaba de finalizar. El nombre del evento suele ser descriptivo de lo que ha ocurrido; normalmente se dispone de datos adicionales que describen el evento con más detalle. El BHO se implementa con el fin de atrapar estos eventos y actuar dependiendo de ellos.

Un evento para cuya respuesta se implementa el BHO se llama 'BeforeNavigate2' que el navegador web dispara cuando el usuario pide al navegador que navegue a una nueva página. El evento es enviado y puede ser reconocido por el BHO antes de que se descargue la página pedida, permitiendo al BHO tomar cualquier acción pertinente antes del usuario vea la página. Tal acción podría ser registrar la página y los datos presentados en respuesta a dicha página en una base de datos. Otra acción podría ser identificar la URL de la página pedida a partir del evento y evitar que la página sea descargada.

Otro evento que el BHO atrapa es el evento 'DocumentComplete', que es disparado por el navegador web cuando una nueva página ha sido descargada desde la página web a memoria. La página es codificada en forma de un documento objeto, conforme al Document Object Model de Microsoft (DOM). El DOM proporciona acceso general a los datos incluyendo la página, permitiendo al BHO extraer elementos de datos que son de interés. Por ejemplo, el BHO puede pedir datos al DOM para determinar si la página forma parte de una transacción de comercio electrónico. Puede hacerlo buscando objetos en el DOM por términos como 'Recibo' o 'Número de cuenta'.

El BHO también puede utilizar el DOM para determinar los nombres de campo o tipos de campo de los datos pedidos en una página web. Los datos introducidos por el usuario en dichos campos pueden ser extraídos posteriormente del DOM y almacenados o se puede actuar en ellos. Los nombres de campo son típicamente descriptivos de lo que se guarda; las contraseñas, por ejemplo, se guardan a menudo en un campo llamado 'password' y así se pueden buscar en una página web. Los números de tarjetas de crédito se pueden buscar de forma similar. Generalmente, los campos de contraseña son de un tipo tal que los datos introducidos sean visualizados como asteriscos. Esto también se puede determinar a partir del análisis del DOM y usar para identificar datos pertinentes.

Los datos de usuario no estarían normalmente en una página web descargada de un sitio web, sino que serían introducidos por el usuario en forma HTML. Generalmente, los datos de usuario potencialmente sensibles son transmitidos al sitio web mediante el servidor web cuando el usuario selecciona un botón "Presentar". En esta etapa, el BHO puede atrapar el evento "Presentar" concedido por el navegador web, y acceder al DOM para extraer los datos de usuario, y, si es necesario, evitar que los datos sean transmitidos.

El encriptado y desencriptado en un enlace seguro tendrán lugar después del punto C y antes del punto A en la figura 3 respectivamente. Así, el BHO puede analizar los datos antes de que sean encriptados o después de que sean desencriptados. Esto es ventajoso dado que no se necesita el BHO para realizar ninguna codificación o decodificación de datos propiamente dicha. Esto no afecta a la capacidad de determinar si el enlace es seguro o no, dado que un enlace seguro puede ser identificado por el identificador de protocolo "https" al inicio del URL corriente. Se prefiere que el examen del contenido de la transmisión tenga lugar antes del encriptado o después del desencriptado.

Explicación de la operación de un cliente de correo electrónico

La operación de un cliente de correo electrónico típico, y la implementación de la realización preferida en un cliente de correo electrónico se describirá ahora con referencia a la figura 5 de los dibujos.

La figura 5 representa la operación simplificada de un cliente de correo electrónico. Las operaciones de Recibir y Enviar operan típicamente independientemente, y estas operaciones se representan por separado en lados opuestos de la figura 5, comenzando en los pasos S120 y los pasos S130, respectivamente.

En el paso S120 se inicia una operación de "recibir mensaje" del cliente de correo electrónico. Esto se puede hacer automáticamente a intervalos predeterminados con el fin de mantener al usuario informado de los nuevos mensajes que reciba, o se puede hacer en respuesta a que el usuario seleccione manualmente un icono "recibir mensajes". El inicio de esta operación hace que el cliente de correo electrónico interrogue al servidor de correo electrónico 95 y descargue los mensajes nuevos a la máquina del usuario. En el paso S122 el cliente de correo electrónico recibe un mensaje de correo electrónico. Típicamente, cuando se recibe un mensaje nuevo, se añade a un 'Buzón de entrada', disponiéndose en una lista las cabeceras de los mensajes recibidos (nombre del emisor, fecha y título, por ejemplo). El usuario clica entonces en la entrada apropiada de la lista para leer todo el mensaje visualizándolo en la pantalla del ordenador. El mensaje de correo electrónico se presenta en el paso S124.

En el caso de un correo electrónico de salida, el usuario selecciona una opción 'crear correo electrónico' como paso S130. En respuesta, el cliente de correo electrónico proporciona una interface incluyendo un editor de texto en el que el usuario puede introducir el texto del cuerpo del mensaje y otra información tal como dirección de destino, asunto, etc. El usuario crea el mensaje en el paso S132 y posteriormente opta por enviarlo, seleccionando un icono u opción de menú proporcionada por el cliente de correo electrónico para emitir una 'orden de enviar'. El correo electrónico es enviado al servidor de correo electrónico para transmisión al receptor en el paso S134. Si el cliente de correo electrónico aplica algún encriptado, se aplica en el paso S134 antes de la transmisión.

En la realización preferida, se proporciona funcionalidad adicional para el cliente de correo electrónico mediante un módulo plug-in. Preferiblemente, el cliente de correo electrónico es uno de los proporcionados por Microsoft, tal como el cliente de Exchange de Microsoft, o el cliente Outlook de Microsoft, y el módulo plug-in es codificado como una extensión de cliente de intercambio. Estos se describen en el documento "Microsoft Outlook y Exchange Client Extensions" por Sharon Lloyd, antes mencionados.

Una extensión de cliente de intercambio es un componente objeto que es conforme con el Component Object Model (COM) de Windows de Microsoft y que utiliza la interface de intercambio IExchExt. Esta interface proporciona un número de interfaces adicionales para modificar la operación del intercambio de cliente de correo electrónico, tal como la interface IExchExtCommands, que permite sustituir o modificar el comportamiento de cliente existente y añadir nuevas órdenes a los menús del cliente; y la interface IExchExtEvents que permite implementar el comportamiento personalizado para manejar 'eventos' de cliente tales como la llegada de nuevos mensajes, leer, escribir, enviar mensajes y leer y escribir archivos adjuntos. También se proporcionan los eventos IExchExtMessage, los eventos IExchExtSession y las interfaces IExchExtAttachmentEvents y proporcionan funcionalidad adicional para las tareas más específicas que cada uno de los nombres de interface sugieren.

En la realización preferida, la extensión de cliente de Exchange que forma el módulo plug-in se implementa con el fin de responder a 'eventos' de cliente disparados por el programa de cliente cuando realiza operaciones y completa acciones. Los 'eventos' en cuestión son proporcionados por las interfaces COM mencionadas anteriormente. Por lo tanto, la supervisión del cliente de correo electrónico por el módulo plug-in puede ser considerada análoga a la forma en que el módulo plug-in de BHO supervisa la operación del navegador web.

El módulo plug-in de cliente de correo electrónico se implementa con el fin de responder al evento 'OnDelivery', por ejemplo, que se dispara cuando se recibe un mensaje nuevo del sistema de administración de correo subyacente y antes de que sea visible para el usuario. El evento 'OnDelivery' contiene información para acceder a las partes diferentes del mensaje de correo electrónico que se han descargado y que se mantienen en memoria. La cabecera del mensaje, el cuerpo del mensaje y los anexos al mensaje se codifican en memoria como propiedades del objeto de mensaje al que se puede acceder por separado mediante llamadas de la Interface de Programa de Aplicación de Correo (MAPI).

Mediante la información suministrada como parte del evento 'OnDelivery', el módulo plug-in puede acceder a la cabecera del mensaje y extraer la identidad del emisor, por ejemplo. Además, el módulo plug-in puede utilizar información obtenida de llamadas MAPI para explorar el cuerpo de un mensaje recibido en busca de palabras clave o datos pertinentes. Puede buscar evidencia de una transacción de comercio electrónico, identificando palabras significativas tales como 'recepción' o 'número de cuenta'. El mensaje se puede guardar entonces a efectos de auditoría. En el caso de un emisor no aprobado, o un contenido nocivo del mensaje, el mensaje puede ser borrado sin verlo.

Por lo tanto, el análisis de un correo electrónico recibido tiene lugar en el punto A en la figura 5 antes de que lo vea el usuario. Preferiblemente el correo electrónico es examinado incluso antes de que el correo electrónico sea puesto en el Buzón de entrada. Donde un mensaje no es desencriptado automáticamente antes de ponerlo en el buzón de entrada, por ejemplo donde el usuario tiene que introducir una clave de desencriptado, el mensaje es examinado inmediatamente después del desencriptado, pero antes de verlo. Se puede incluir certificados digitales como anexos al correo electrónico y pueden ser examinados antes de verlo, pudiendo realizar las acciones apropiadas, tales como validación.

Otro evento de cliente significativo para cuya respuesta se implementa el módulo plug-in, es el evento 'OnWriteComplete' que es disparado cuando el usuario la seleccionado la 'orden de enviar' y pedido al cliente de correo electrónico que transmita un nuevo mensaje de correo electrónico al sistema de administración de correo. Este evento es disparado, en el punto B en la figura 5, antes de la transmisión y antes de que tenga lugar el encriptado. El nuevo mensaje que ha de ser transmitido es igualmente almacenado en memoria como un objeto al que pueden acceder las llamadas MAPI. El módulo plug-in puede usar las llamadas MAPI para explorar el contenido del correo electrónico de salida en busca de datos sensibles, tales como número de tarjeta de crédito, y en consecuencia hacer que el mensaje sea registrado o incluso bloqueado.

Operación del módulo plug-in

La implementación preferida de los módulos plug-in de navegador web y cliente de correo electrónico se ha descrito anteriormente con referencia a las figuras 3 y 5 anteriores. A continuación, la funcionalidad proporcionada por los módulos plug-in se describirá en detalle y con referencia a las figuras 6 a 18.

Identificación y registro de nombres de usuario, contraseñas y otra información

El sistema preferido proporciona medios para identificar, recoger y almacenar automáticamente datos contenidos en las transmisiones a y de una estación de trabajo del usuario, en particular, los nombres de usuario y las contraseñas introducidas por un usuario para acceder a páginas web, sitios de Protocolo de Transferencia de Archivos ('FTP') y otros lugares en Internet.

Los sistemas que proporcionan actualmente facilidades para registrar contraseñas, actualmente sólo lo hacen cuando un usuario clica en la opción 'recordar contraseña' proporcionada en el GUI. La contraseña se guarda en un archivo local protegido en la máquina del usuario que solamente se abre cuando el usuario es autenticado en dicha máquina, por ejemplo, introduciendo su nombre de usuario y contraseña al tiempo de arrancar. La opción recordar contraseña hace que el sistema recuerde la contraseña del usuario cuando realice las visitas siguientes, prellenando el campo de contraseña con dicha contraseña de modo que el usuario no tenga que introducirla cada vez que sea preciso. El inconveniente de que el archivo de contraseña se guarde localmente es que si el usuario pasa a otra máquina, no tiene acceso al archivo de contraseña guardado y tendrá que volver a introducir la contraseña.

El sistema preferido identifica contraseñas automáticamente, sin necesidad de instrucción del usuario, y guarda las contraseñas y nombres de usuario identificados en un depósito de datos. Preferiblemente ésta es la base central de datos 42. Esto permite que las contraseñas de cualquier usuario sean reclamadas independientemente del terminal en el que el usuario entre, a condición de que el terminal tenga acceso a la base de datos central.

Las contraseñas y los nombres de usuario identificados se almacenan en la base de datos junto con los nombres de campos en los que se almacenan en el sitio web original y la dirección de la página de Internet a la que fueron transmitidos y en la que se utilizan. La información de la página puede ser recuperada sencillamente puesto que se incluye en la petición HTTP que presenta la información de contraseña y nombre de usuario en dicha página, y en la representación de la página web mantenida en memoria.

Preferiblemente, por razones de seguridad, la información almacenada en la base de datos es encriptada, de modo que solamente un número seleccionado de personas, tal como los supervisores de red, administradores del sistema o directores de la compañía tengan acceso a ella. Pueden acceder a la base de datos a través de una estación de trabajo en la red, introduciendo un nombre de usuario o una contraseña para identificarse, o a través de una estación de trabajo supervisora, tal como las Consolas Operativas 44.

Este almacenamiento de nombres de usuario y contraseñas junto con detalles de dirección ofrece una ventaja significativa a las compañías que utilizan facilidades en línea. Con las tecnologías existentes, si un usuario olvida su contraseña de autenticación evitando el acceso al archivo protegido, o deja la compañía sin haberla revelado, no se puede acceder al servicio de Internet. Tiene lugar una situación similar si el archivo protegido se daña, borra o pierde de otro modo. Entonces hay que acceder a cada servicio de Internet con el fin de sustituir o recuperar la contraseña perdida, lo que puede ser caro tanto en términos de pérdida de acceso como de tiempo administrativo. Con el sistema preferido, la información de contraseña puede ser recuperada de la base de datos central, de modo que el acceso a páginas web no se pierde.

La figura 6 es un diagrama de flujo que ilustra esquemáticamente la operación de un módulo plug-in implementado para extraer información de nombre de usuario y contraseña de los datos a transmitir a un servidor web.

En el paso S150, el módulo plug-in comienza y analiza los datos a punto de ser transmitidos al servidor web desde el navegador. Esto tiene lugar en el punto 'C' en el proceso ilustrado en la figura 3. El control pasa entonces al paso S152 donde el módulo plug-in determina si los datos que han de ser transmitidos contienen información de nombre de usuario o contraseña.

Las contraseñas y nombres de usuario pueden ser identificados de la manera descrita anteriormente con referencia a las figuras 3, 4 y 5, identificando los nombres de campo en la orden presentada o usando el DOM, por ejemplo, para buscar nombres de campo, tipos de campo, o el método de visualización usado para identificar los datos en páginas web. También se pueden recuperar del HTML de páginas web, las ventanas emergentes o GUIs (interfaces gráficas de usuario) presentados por servidores remotos o proveedores en la web mundial o incluso explorando el contenido de mensajes de correo electrónico.

La identificación de contraseñas y nombres de usuario en las órdenes transmitidas o en el DOM de una página web a partir de sus nombres de campo se basa en los nombres de campo que describen su finalidad con etiquetas obvias, tal como 'contraseña' o 'nombre de usuario'. En los casos en que los nombres de campo no son significativos por sí mismos, la naturaleza de datos transmitidos se puede deducir del tipo de campo de los datos, que es 'cadena', 'entero', etc, o el método de visualización usado para introducir los datos. Los campos que deben recibir una contraseña pueden ser identificados a partir de la representación buscando un tipo de campo 'contraseña' en el DOM. Los recuadros de texto en una página web en los que se han de introducir datos de contraseña, por ejemplo, presentan típicamente cada carácter introducido como un asterisco; esta propiedad puede ser determinada a partir del DOM y usada para deducir que los datos introducidos en el recuadro de texto son una contraseña, aunque no haya otras indicaciones. Aunque la contraseña sea visualizada como una cadena de asteriscos, la representación en memoria todavía contiene la información de caracteres que introdujo el usuario. La contraseña puede ser recuperada entonces simplemente extrayendo la entrada del campo.

Alternativamente, las contraseñas y los nombres de usuario pueden ser identificados con referencia a los almacenados por otros programas tal como 'Internet Explorer' de Microsoft cuando el usuario selecciona la opción recordar contraseña. Tales contraseñas son almacenadas en un archivo local protegido en el ordenador del usuario. Este archivo es 'desbloqueado' cuando el usuario es autenticado en el ordenador, y así se puede acceder a él para obtener información de contraseña y nombre de usuario por el módulo plug-in del navegador del sistema preferido.

Si el módulo plug-in no detecta un nombre de usuario o una contraseña en los datos que se han de transmitir, el control pasa al paso S158, punto en el que el módulo sale y el control vuelve al punto 'C' en la figura 3. El navegador puede transmitir entonces los datos al servidor web. Sin embargo, si un nombre de usuario o una contraseña es detectado por el módulo plug-in en el paso S152, el control pasa al paso S154, donde se extraen los valores del nombre de usuario o contraseña identificados y la URL u otro identificador de la página web a la que se han de transmitir los datos. El control pasa entonces al paso S156 donde se almacenan estos valores y la URL u otro identificador en una base de datos predeterminada del sistema 42. Una vez que el almacenamiento tiene lugar, el control pasa entonces al paso S158, donde el módulo sale y el control vuelve al punto 'C' en la figura 3. El navegador puede transmitir entonces los datos al servidor web.

La realización preferida no se tiene que limitar solamente al almacenamiento de contraseñas o nombres de usuario que se han utilizado como un ejemplo a causa de la ventaja inmediata que proporciona su almacenamiento. Otros tipos de datos, en particular los relativos a transacciones de comercio electrónico, tales como información de tarjeta de crédito y certificado digital, también pueden ser extraídos de forma útil y almacenados para proporcionar una base de datos o registro. El sistema para extraer información de transmisiones también puede ser aplicado a sistemas de correo electrónico.

La información puede ser extraída de la manera descrita anteriormente, mediante el DOM o mediante llamadas MAPI a la representación COM de contenido de correo electrónico, o puede ser extraída del lenguaje en el que una página web está codificada. Las páginas web están codificadas típicamente en Lenguaje de Marcación de HiperTexto (HTML), un lenguaje basado en texto legible por humano en el que se puede buscar palabras clave conocidas o indicadores usando técnicas de concordancia de texto convencionales. En la realización preferida, el registro de los datos puede implicar registrar la información de contraseña y nombre de usuario, registrar la URL de una página web que se ve o de una cuenta de correo electrónico, registrar los datos presentados a los campos de una página web, y registrar el HTML de una página web, de modo que la página web pueda ser recuperada posteriormente y vista.

Los módulos plug-in proporcionados por el sistema preferido operan en unión con datos de política, que pueden ser registrados en un archivo, base de datos, o código de software, por ejemplo. Los datos de política permiten al usuario del sistema preferido ordenar la operación de cada uno de los módulos plug-in, controlando por ello su funcionalidad.

Una representación de muestra de los datos de política, ilustrados en la figura 7, representa cómo un usuario puede controlar la operación del módulo plug-in para registrar información de contraseña y nombre de usuario junto con otros tipos de datos.

La estructura en forma de árbol de los datos de política se ve claramente en la figura 7 que representa una bifurcación principal de los datos de política titulada 'Recording'. La bifurcación de registro se separa en dos bifurcaciones secundarias llamadas 'Navegator' y 'Email' que contienen instrucciones para la operación de los módulos plug-in de navegador web y cliente de correo electrónico, respectivamente.

La bifurcación de navegador contiene tres bifurcaciones secundarias llamadas 'DataToRecord', 'WhenToStartRecording' y 'WhenToStopRecording'. La bifurcación DataToRecord especifica el tipo de datos que se ha de extraer de transmisiones a o de la estación de trabajo del usuario y un servidor web. En la ilustración se hace referencia a cuatro tipos de datos, siendo estos la URL de la página web que se visita, EL HTML de la página web visitada, datos introducidos por un usuario en campos dispuestos en la página web y presentados a un sitio web, y las contraseñas y los nombres de usuario que son introducidos por el usuario. A estos se hace referencia en cuatro bifurcaciones secundarias distintas de la bifurcación DataToRecord, tituladas 'URL', 'HTML', 'SubmittedFields' y 'Passwords'. Un opción Sí/No en cada una de las bifurcaciones secundarias especifica si los datos indicados han de ser registrados o no.

La bifurcación WhenToStartRecording expone un número de condiciones que especifican el punto en el que los datos especificados en la bifurcación DataToRecord han de ser registrados. Se ilustran cinco condiciones en este ejemplo, cada una de las cuales se expone en una bifurcación separada y tituladas, respectivamente, 'WhenNavegatorIsOpened', 'IfCreditCard NumberSubmitted', 'IfPasswordSubmitted', 'IfKeywordsReceived' y 'IfKeywordsSenr'. Si estas condiciones se han de utilizar o no con el fin de determinar cuándo iniciar el registro se indica por marcadores Sí/No en cada bifurcación.

Igualmente, la bifurcación WhenToStopRecording enumera tres condiciones que pueden ser usadas para determinar el punto en el que el registro de los datos especificados en la bifurcación DataToRecord se ha de detener. Estas condiciones son 'WhenUserClosesNavegator', 'WhenUserChangesSite' y 'WhenUserChangesPage'. El estado Sí/No de cada una de las condiciones y para cada uno de los tipos de datos a registrar puede ser establecido fácilmente por un usuario del sistema preferido con el fin de controlar la operación del módulo plug-in.

La bifurcación correo electrónico de los datos de política se divide en una bifurcación DataToRecord y una bifurcación WhenToRecord. Cada una de estas bifurcaciones se subdivide en bifurcaciones que tratan de correo enviado y correo recibido. El tipo de datos que se puede registrar se expone en la bifurcación DataToRecord y para correo enviado puede ser el texto del mensaje, cualesquiera anexos al mensaje, y en el caso de mensajes firmados con una firma digital, una copia del certificado digital que acompaña a la firma. Las condiciones para registrar correo enviado

y correo recibido se exponen en la bifurcación WhenToRecord y se pueden basar en la identificación de un número de tarjeta de crédito, una palabra clave o un certificado digital en el correo enviado o recibido.

La estructura en forma de árbol descrita es la forma preferida para los datos de política dado que permite organizar y consultar fácilmente los datos. También permite que diferentes usuarios sean asignados a diferentes bifurcaciones del árbol con el fin de recibir políticas diferentes. Aunque se prefiere la estructura en forma de árbol, también son posibles otras disposiciones. Se ha previsto que las bifurcaciones representadas en este diagrama sean solamente ilustrativas.

Identificación de números de tarjetas de crédito

El sistema preferido también busca números de tarjetas de crédito u otra información de cuenta en los datos a transmitir al servidor web o cliente de correo electrónico buscando una cadena de dígitos numéricos, típicamente de entre 14 y 16 de longitud. Entonces determina si la cadena de dígitos pasa una de las pruebas universalmente usadas por las compañías de tarjetas de crédito para validar números de tarjeta. Si se halla un número de tarjeta de crédito en la transmisión, el sistema preferido puede realizar varias acciones dependiendo de los parámetros en el archivo de política, tal como referir la transmisión a una tercera parte para aprobación, renegociar un nivel más alto de encriptado para salvaguardar la transmisión si el número de tarjeta de crédito pertenece a la compañía, o evitar que tenga lugar la transmisión.

La prueba más común para identificar un número de tarjeta de crédito se define en la norma ANSI X4.13, y se conoce comúnmente como LUHN o Mod 10.

La fórmula Luhn se aplica a números de tarjetas de crédito con el fin de generar un dígito de comprobación, y así también se puede usar para validar tarjetas de crédito, en cuyo caso el dígito de comprobación se configura como parte de la fórmula. Para validar un número de tarjeta de crédito usando la fórmula de Luhn, el valor de cada segundo dígito después del primero, comenzando por el lado derecho del número y siguiendo hacia la izquierda, es multiplicado por dos; todos los dígitos, los que han sido multiplicados por dos y los que no lo han sido, se suman entonces conjuntamente; cualesquiera valores de dígito que tengan que ser mayores o iguales a diez como resultado de ser duplicados, se suman como si fuesen dos valores de un solo dígito, por ejemplo: ‘10’ cuenta como ‘1+0 = 1’, ‘18’ cuenta como ‘1+8 = 9’. Si el total de la suma es divisible por diez, entonces la tarjeta de crédito es un número válido de tarjeta de crédito.

La figura 8 es un diagrama de flujo que ilustra la operación de un módulo plug-in que detecta números de tarjetas de crédito, usando la fórmula de Luhn descrita anteriormente, en datos que están a punto de ser transmitidos. Si se identifica un número de tarjeta de crédito, el módulo plug-in implementa más comprobaciones basadas en política, en base a cuyo resultado el módulo plug-in puede determinar transmitir los datos conteniendo el número de tarjeta de crédito o evitar la transmisión.

El módulo comienza la operación en el paso S160, que sigue al punto ‘C’ en el proceso ilustrado en la figura 3 en el caso de la implementación de navegador, o el punto B en el proceso ilustrado en la figura 5 en el caso de una implementación de cliente de correo electrónico. El control pasa del paso S160 al paso S162 en el que el módulo explora los datos a punto de ser transmitidos al servidor web o servicio de correo electrónico y extrae de ellos una primera cadena de dígitos que probablemente será un número de tarjeta de crédito.

Esto se logra explorando los datos incluyendo la transmisión en busca de cadenas de dígitos sobre un número concreto de dígitos de longitud. Los números de tarjetas de crédito están formados generalmente por más de 12 dígitos, y no tienen generalmente más de 16 dígitos de longitud. Así cualesquiera cadenas de dígitos en este rango pueden ser identificadas como posibles números de tarjetas de crédito.

Después del paso de extracción S162 el control pasa al paso de decisión S164 donde se realiza una rutina de comprobación de fin de archivo. Si los datos no contienen ningún número de tarjeta de crédito candidato y se llega a la comprobación de fin del archivo antes de que se pueda hallar algún primer número candidato, entonces en el paso S164 el control se pasa al paso S178 donde la transmisión de los datos puede proseguir sin que se hagan otras verificaciones. El módulo sale entonces en el paso S180. El control se reanuda en la operación del navegador web representada en la figura 3 desde punto ‘C’ o en la operación de cliente de correo electrónico representada en la figura 5 desde el punto B.

Si se halla un primer número potencial de tarjeta de crédito en los datos en el paso S162, entonces se extrae y almacena en memoria. Todavía no se ha llegado al fin de archivo de modo que el control pasa del paso S162 al paso S164 y posteriormente a S166 donde se calcula una suma de verificación del número candidato almacenado usando la fórmula de Luhn. El control pasa entonces al paso de decisión S168, donde se consulta la suma de verificación.

Si la suma de verificación indica que el número candidato no es un número válido de tarjeta de crédito, entonces el control vuelve al paso S162 donde se extrae de los datos el número de tarjeta de crédito posible siguiente. Si no se halla un segundo número de tarjeta de crédito, entonces se llega al final del archivo y el control pasa al paso S178 donde la transmisión puede proseguir, y posteriormente al paso S180 donde el módulo sale.

Sin embargo, si la suma de verificación indica que el número candidato es un número válido de tarjeta de crédito, entonces el control pasa al paso de decisión S170 donde se consultan los parámetros de los datos de política en busca

de la acción apropiada a tomar. La acción puede ser determinada a partir de factores tales como el número propiamente dicho, la identidad del usuario que transmite el número y la dirección a la que ha de ser enviado. Los datos de política podrían especificar, por ejemplo, que no se han de transmitir tarjetas de crédito, o que se requiere una mayor intensidad de encriptado para la transmisión antes de poder proseguir.

Este paso de verificación de política permite controlar transacciones con tarjeta de crédito a un nivel más alto que el usuario que realiza la transacción. Así las decisiones financieras pueden ser implementadas rápida y fácilmente, y pueden ser realizadas automáticamente sin la necesidad de supervisión. Una organización puede desear, por ejemplo, restringir la capacidad de hacer transacciones con tarjeta de crédito en la cuenta de la organización a personas concretas autorizadas o puede desear restringir transacciones también en una cuenta concreta.

En el paso S170, el número de tarjeta de crédito, y otros detalles de la transacción son comparados con los parámetros en el archivo de política y se determina si la transmisión puede tener lugar o no. Si por alguna razón, con referencia a la comprobación de política, se determina que el número de tarjeta de crédito no deberá ser transmitido, el control pasa al paso S172 donde se detiene la transmisión de los datos, y posteriormente al paso S174 donde el módulo sale. En este punto el sistema podría notificar al usuario que la petición ha sido denegada por medio de un buzón de mensajes emergentes. El control entonces vuelve al punto A en la figura 3, en el caso de un navegador web, o al paso S132, 'crear correo' en la figura 5, en el caso de un cliente de correo electrónico.

Si se determina en el paso S172 que el número de tarjeta de crédito puede ser transmitido, el control pasa al paso S176 donde tiene lugar la transmisión de los datos, y posteriormente al paso S180 donde el módulo sale. En este caso, el control se reanuda desde el punto C en la operación del navegador web ilustrado en la figura 3, o desde el punto B en la operación de cliente de correo electrónico ilustrado en la figura 5.

Los números de tarjetas de crédito no tienen que ser identificados en el paso S162 únicamente explorando el contenido de la transmisión. En las implementaciones de navegador web el número de tarjeta de crédito puede ser identificado directamente, por ejemplo, con referencia a los nombres de campo de cualesquiera variables que hayan de ser transmitidas o también de la representación de la página web en memoria. La explicación anterior acerca de la identificación de contraseñas lo explica con más detalle.

El sistema preferido también puede estar configurado para buscar en las transmisiones de salida otros detalles financieros pertinentes, tal como números de cuenta. Los números de cuenta de una compañía de las que se pueden depositar fondos, pueden ser almacenados en un archivo separado. Entonces se puede extraer cualesquiera cadenas de caracteres o dígitos probables de los datos de salida de la manera descrita, y comparar con las entradas en el archivo de cuentas para determinar si es o no un número de cuenta válido. La transacción puede proseguir entonces o ser denegada de la manera descrita anteriormente. Aunque se ha hecho referencia a números de tarjetas de crédito, se apreciará que también se puede usar cualquier tipo de número de tarjeta para hacer pago, tal como números de tarjeta de débito.

Además, aunque la identificación de números de tarjetas de crédito se ha explicado con referencia a datos que han de ser transmitidos, se apreciará que se podría usar técnicas similares para identificar y extraer números de tarjetas de crédito a partir de las transmisiones recibidas.

Tenedor de validación y autenticación

Las transacciones en línea requieren típicamente alguna forma de autenticación de que el usuario es quien dice ser, y que es capaz de pagar los artículos pedidos. Estos requisitos los cumple generalmente el comprador que suministra al comerciante su número de tarjeta de crédito y la dirección del tenedor que entonces pueden ser verificados por el vendedor con el emisor de tarjetas. Sin embargo, el usuario une cada vez más a transmisiones electrónicas certificados digitales que, en unión con una firma digital, permiten al receptor verificar que la transmisión se originó en la persona designada como emisor. Los certificados digitales de algunas autoridades emisoras, como Identrus, también pueden actuar como una garantía de que el tenedor cumplirá su compromiso de pagar una cantidad especificada de dinero. Estos certificados son útiles en el comercio en línea.

Las firmas digitales son un medio ampliamente usado de establecer la identidad de una persona en línea al transmitir información o al realizar una transacción. También proporcionan una garantía al receptor de cualquier información o detalles de transmisión transmitidos de que los detalles y la información no han sido manipulados en el camino por terceros no autorizados.

Los certificados digitales son concedidos a individuos, organizaciones o compañías por autoridades de certificación independientes, tales como Verisign Inc. Una organización también puede actuar como su propia autoridad de certificación que emite sus propios certificados digitales que pueden derivar o no de un certificado "raíz" concedido por otra autoridad de certificación. Un certificado digital contiene típicamente el nombre del tenedor, un número de serie, una fecha de caducidad, una copia de la clave pública del tenedor del certificado y la firma digital de la autoridad emisora del certificado. También se concede una clave privada al tenedor del certificado que no deberá revelar a nadie.

Los certificados son únicos para cada tenedor y pueden ser revocados por el emisor si el tenedor ya no es viable; alternativamente, un tenedor puede pedir que se revoque si su clave privada está en peligro.

Las claves pública y privada pueden ser usadas en tándem para encriptar o desencriptar un mensaje. Cualquiera puede usar una clave pública del tenedor del certificado para encriptar un mensaje de modo que solamente pueda ser leído por el tenedor del certificado después de desencriptar el mensaje con su clave privada.

Los mensajes también pueden ser firmados digitalmente usando software que convierte el contenido del mensaje en un resumen matemático, llamado un hash. El hash es encriptado entonces usando la clave privada del remitente. El hash encriptado puede ser utilizado entonces como una firma digital para el mensaje que se transmite. El mensaje original, la firma digital y el certificado digital del transmisor son enviados a un receptor que, con el fin de confirmar que el mensaje que ha recibido está completo y no ha sido alterado con respecto a su forma original, puede producir entonces un hash para el mensaje recibido. Si el hash recibido, que ha sido desencriptado con la clave pública del tenedor, corresponde al hash producido por el receptor, entonces el receptor puede confiar en que el mensaje ha sido enviado por la persona a quien se le concedió el certificado, y que el mensaje no ha sido alterado en ruta con respecto a su forma original. Por lo tanto, los certificados digitales son de importancia considerable y creciente para que las compañías realicen operaciones comerciales en Internet.

En los casos en que un comerciante en línea utiliza certificados digitales para asegurar la identidad de sus clientes, hay que comprobar con el emisor que el certificado todavía es válido antes de autorizar una transacción. Tales comprobaciones se pueden llevar a cabo en línea usando un servicio de verificación independiente tal como el proporcionado por Valicert, Inc. Generalmente se carga una tarifa por tales servicios.

Puede ser que empleados individuales de una organización reciban correos electrónicos de un solo cliente, cada uno firmado con su certificado digital, en ocasiones separadas. Actualmente, no hay forma de que la información acerca de los certificados recibidos por un empleado sea compartida con otro empleado a no ser que la compartan manualmente, y como resultado, los empleados individuales podrían pedir que se validase el mismo certificado cada vez que lo reciban. Sin embargo, esto es inútil dado que una vez que un certificado ha sido revocado por su emisor, nunca se reinstaura de nuevo, de modo que los cargos por validación gastados en un certificado ya revocado son innecesarios. Adicionalmente, tal vez desee el receptor realizar una estimación comercial de si un certificado previamente validado deberá ser comprobado de nuevo o no. Por ejemplo, si un día se recibe un pedido firmado digitalmente de $1 M en artículos, y el certificado es validado satisfactoriamente, y al día siguiente se recibe otro pedido de $50, firmado con el mismo certificado, la organización puede considerar que la segunda comprobación de validación es innecesaria, ahorrando por ello el cargo por validación.

El sistema preferido proporciona medios para registrar información acerca de los certificados digitales que han sido recibidos, el estado del certificado en la última comprobación así como, donde sea aplicable, información sobre transacciones, tales como cliente, cantidad, fecha, artículos, etc. Esta información se almacena en una base de datos central a la que todos los usuarios del sistema tienen acceso. El sistema preferido también proporciona medios para utilizar la información almacenada con el fin de decidir si es deseable o no una comprobación de validación, y aceptar o rechazar transmisiones dependiendo del estado del certificado digital. Así, los usuarios del sistema pueden recibir y revisar transmisiones sin necesidad de establecer su autenticidad por sí mismos.

La figura 9 ilustra la operación de un módulo plug-in del sistema preferido implementado para extraer certificados digitales de transmisiones recibidas por empleados de una compañía y registrarlos en una base de datos junto con su estado de validez y detalles de las transacciones asociadas, tal como fecha, cantidad, artículos, etc. El módulo realiza primero una comprobación para determinar si el certificado no es obviamente válido, y que el mensaje ha sido firmado correctamente por él. Obviamente, el certificado no es válido, por ejemplo, si ha superado la fecha de caducidad, o si contiene una 'huella digital' no válida. Tal huella digital puede ser una suma de verificación para el certificado propiamente dicho, por ejemplo. El mensaje no ha sido firmado correctamente si la firma no puede ser verificada a partir de la información contenida dentro del certificado. Los detalles de la validación de certificados y firma de mensajes se describen de forma más completa en los documentos ITU y RFC previamente referenciados. El módulo realiza entonces una comprobación para determinar si el certificado ya ha sido almacenado en la base de datos y solamente registra los que no lo han sido. Cuando ya se ha almacenado una copia del certificado, el módulo comprueba el registro de la base de datos para determinar si ha sido previamente identificado como revocado, en cuyo caso la transmisión es rechazada inmediatamente. De otro modo, el módulo determina entonces, según la política que define las normas comerciales, si validar o no el certificado. Teniendo en cuenta los resultados de cualquier validación, determina posteriormente si el certificado merece confianza, y por lo tanto si la transmisión firmada por el certificado digital deberá ser rechazada o aceptada. El módulo se inicia en el paso S190, después de la recepción de datos conteniendo un certificado digital. Los certificados digitales se transmiten típicamente como anexos a mensajes y pueden ser identificados examinando los primeros pocos bytes en la cabecera del anexo. Estos bytes identifican el tipo de archivo unido y por ello indicarán si un anexo es un certificado digital o no.

El paso de inicialización S190 tiene lugar después del punto A en la figura 3 si el módulo se implementa en un navegador web, y después del punto A en la figura 5 si el módulo se implementa en un cliente de correo electrónico. Después de la inicialización, el módulo pasa al paso S191 en el que se verifica la fecha de caducidad del certificado, y se confirma la firma digital que ha firmado el mensaje. Si el certificado ha expirado, o el mensaje está firmado incorrectamente, el módulo pasa al paso S198 y rechaza la transmisión. De otro modo, el módulo pasa al paso S192 en el que se busca en la base de datos una copia previamente recibida del certificado digital. El control pasa entonces al paso de decisión S194. Si se halla una copia del certificado en la base de datos, entonces el control pasa al paso de decisión S196 donde el módulo determina si el certificado ha sido marcado previamente como revocado. Esto se

habrá producido si una previa comprobación de validez reveló que un certificado digital había sido revocado. Si el certificado ya no está en la base de datos, el control pasa del paso S194 al paso S202 donde el nuevo certificado y la fecha en que se recibió se guardan en la base de datos, juntamente con detalles adicionales, tal como la dirección desde la que se envió y detalles de cualquier transacción asociada con la transmisión tal como valor monetario, número de cuenta, etc. Si el certificado ya ha sido marcado como revocado en el paso S196, entonces el control pasa directamente al paso S198 en el que la transmisión incluyendo el certificado digital es rechazada automáticamente. Esto puede implicar, por ejemplo, transmitir un mensaje generado automáticamente al iniciador de la transmisión cuyo certificado se ha considerado no válido para explicar el rechazo, y evitar que el receptor del certificado digital lleve a cabo pasos adicionales en conexión con la transmisión rehusada. El módulo sale entonces en el paso S200.

Sin embargo, si el certificado no ha sido marcado previamente como revocado en el paso S196, entonces el control pasa al paso S204 en el que la historia de las transmisiones firmadas por el certificado, por otros certificados de la misma compañía, o usadas para realizar transacciones en la misma cuenta se considera con datos de política para determinar si es necesaria una comprobación de validez en línea del certificado. El control también pasa al paso S204 después de añadir un nuevo certificado digital a la base de datos en el paso S202.

Los datos de política contienen instrucciones que, cuando se consideran en unión con la historia de las transmisiones firmadas previamente recibidas y las comprobaciones de revocación previamente realizadas indican si el certificado usado para firmar una transmisión deberá ser verificado o no en esta ocasión. Se ilustran datos de política ejemplares en la figura 10 a la que se deberá hacer referencia ahora.

Los datos de política se guardan en la bifurcación AcceptanceConfidenceRating en la bifurcación DigitalCertificates de la representación de datos de política. La bifurcación AcceptanceConfidenceRating se subdivide en dos bifurcaciones separadas que tratan individualmente de certificados digitales 'monetarios', donde un certificado ha sido usado para firmar una transmisión que implica una transacción con el receptor por una cantidad de dinero, y certificados digitales de 'identidad' que no implican una transacción monetaria con el receptor de la transmisión. Algunos certificados se conceden solamente para uso en unión con transacciones monetarias. Por ejemplo, el 'certificado de garantía' concedido por algunas organizaciones bancarias en línea, tal como Identrus, como una garantía para el receptor de la transmisión firmada. Tales certificados de garantía testifican que el emisor de la transmisión es un cliente de un banco miembro de Identrus, y que si no efectúa el pago, el banco aceptará la responsabilidad.

Organizaciones que emiten diferentes tipos o clases de certificados digitales, marcan cada certificado según su clase. Identificar un certificado como de una clase particular es entonces cuestión de conocer cómo clasifican las diferentes organizaciones sus certificados y buscar el indicador apropiado en el certificado recibido.

Los emisores de certificados digitales pueden proporcionar muchas clases diferentes de certificados adecuados para fines diferentes. Estos pueden ser tratados por separado por los datos de política por las correspondientes bifurcaciones secundarias del árbol de datos de política.

En el ejemplo de política, la primera bifurcación titulada 'IdentityCertificates' se ocupa de transmisiones que no implican una transacción monetaria. La bifurcación incluye cuatro bifurcaciones secundarias separadas. La primera de ellas, titulada 'AlwaysAcceptFrom', contiene una referencia a una tabla, 'tabla a', que enumera los nombres de individuos y organizaciones que se consideran fiables. Los nombres enumerados en esta tabla serán los conocidos e implícitamente los de confianza de la compañía, para quienes no se considera necesario determinar si un certificado digital ha sido revocado por su emisor.

La segunda bifurcación titulada 'AlwaysCheckFrom' contiene una referencia a una tabla separada, tabla b, en la que se guardan los nombres de organizaciones e individuos cuyos certificados digitales siempre deberán ser verificados. Es claro que el contenido de tabla a y de la tabla b dependerá de la experiencia del usuario del sistema preferido y quedará pendiente hasta que el usuario lo introduzca.

La tercera bifurcación titulada 'CheckIfDaysSince CertificateReceivedFromCompany' especifica un período de tiempo después de la recepción de un certificado digital válido de una compañía, dentro del que no se consideran necesarias las comprobaciones de certificados digitales adicionales recibidos de dicha compañía. En este caso, el período de tiempo es de 10 días.

La cuarta bifurcación titulada 'CheckIfDaysSince LastReceivedThisCertificate' especifica un período de tiempo similar en el caso de un certificado digital individual. En el ejemplo representado, los datos de política especifican que las comprobaciones de validación de cualquier certificado digital dado solamente se tienen que efectuar cada 30 días. De nuevo, el número de días especificado en estas dos bifurcaciones se deja a la decisión del usuario del sistema preferido. La cantidad de tiempo transcurrido desde la recepción de un certificado digital válido puede ser determinada con referencia a certificados digitales y datos asociados almacenados en la base de datos. La verificación de certificados digitales periódicamente, más bien que cada vez que se reciben, permite ahorrar dinero gastado en la realización de comprobaciones.

La bifurcación MonetaryCertificates también contiene una bifurcación AlwaysAcceptFrom y otra AlwaysCheckFrom que hacen referencia a las tablas x e y, respectivamente. La tabla x enumera todas las organizaciones e individuos para quienes no es preciso comprobar el estado de un certificado digital; la tabla y enumera todos aquellos para quienes siempre hay que efectuar una comprobación. La bifurcación MonetaryCertificate también contiene una bifurcación

CheckIfAmountExceeds que especifica una cantidad umbral de transacción por encima de la que todos los certificados digitales deben ser verificados, y por último una bifurcación IfRecentlyChecked que establece dos condiciones para realizar comprobaciones en un certificado digital que ha sido recibido y validado recientemente. La bifurcación IfRecentlyChecked permite al usuario especificar que los certificados digitales recibidos para transacciones para una pequeña cantidad, en este caso $5000, recibidos dentro de un tiempo especificado, en este caso 30 días, de una comprobación de revocación anterior, no tienen que ser validados.

La figura 11 ilustra el proceso del módulo plug-in que interactúa con los datos de política representados en la figura 9. Este proceso es un subproceso del representado en la figura 8 y tiene lugar en el paso S204 que conduce al paso de decisión S206 en el que el módulo plug-in determina si realizar o no una comprobación en línea del estado del certificado digital recibido. El subproceso comienza en el paso S220 del que el control pasa al paso de decisión S222 en el que se determina si la transmisión es monetaria de la clase del certificado digital usado para firmar el mensaje. Si la transmisión es monetaria, entonces el control fluye al paso de decisión S232, que es el primero de una cadena de pasos de decisión correspondientes a las bifurcaciones en la bifurcación MonetaryCertificates de la bifurcación AcceptanceConfidenceRating de los datos de política.

Si se determina en el paso S222 que la transmisión no es monetaria, el control pasa al paso de decisión S224, que es el primer paso de decisión de una cadena de pasos de decisión correspondientes a las bifurcaciones IdentityCertificates de la bifurcación AcceptanceConfidenceRating de los datos de política. En cada uno de los pasos de decisión de la cadena se realiza una simple comprobación para ver si se cumplen las condiciones especificadas en cada bifurcación secundaria de la bifurcación IdentityCertificates de los datos de política. Dependiendo de los resultados de dicha comprobación, el control fluye al paso S242, en el que se establece confianza en el certificado digital y no se considera necesaria la comprobación en línea del estado del certificado digital, o al paso S244, en el que no se establece confianza y se considera necesaria la comprobación en línea, o al paso de decisión siguiente de la cadena.

Así, en el paso de decisión S224, en el que se determina si el emisor del certificado digital se enumera en la tabla a, que es la tabla 'AlwaysAcceptFrom', si el emisor del certificado digital se enumera en la tabla a, entonces el control fluye del paso de decisión S224 al paso S242 donde se establece confianza en el certificado y el subproceso termina volviendo al paso S208 en la figura 8. Si el emisor no se enumera en la tabla a, entonces el control fluye del paso S224 al paso de decisión siguiente en el paso de la serie S226 en el que se determina si el emisor del certificado digital se enumera en la tabla b, que es la tabla 'AlwaysCheckFrom'. Igualmente, si el emisor se enumera en esta tabla, el control fluye al paso S244 en el que se considera necesaria una comprobación en línea del estado del certificado digital. El control vuelve del paso S244 en el subproceso al paso S210 en la figura 8.

Si el emisor del certificado digital no se enumera en la tabla b, entonces el control fluye del paso de decisión S226 al paso de decisión siguiente en la cadena que representa la condición siguiente enumerada como una bifurcación secundaria enumerada en los datos de política. Así, en el paso de decisión S228 se comprueba si este certificado digital ha sido validado en los últimos 30 días. Esto implicará buscar el certificado digital en la base de datos de certificados digitales almacenados y extraer de la información almacenada la fecha en que el certificado digital fue verificado por última vez. Si el estado del certificado digital ha sido verificado en los últimos 30 días, el control fluye al paso S242 donde se establece confianza. Si la información en la base de datos de certificados digitales almacenados indica que el certificado digital no ha sido verificado en los últimos 30 días, entonces el control fluye del paso S228 al paso de decisión S230 en el que se comprueba si se ha recibido otro certificado digital de la misma compañía y si dicho certificado digital ha sido verificado dentro de los últimos 10 días. Esta determinación implica de nuevo verificar la base de datos de certificados digitales almacenados y la información relativa a los certificados digitales. Si el otro certificado digital ha sido verificado en los últimos 10 días, entonces el control fluye al paso S242 donde se establece confianza en el certificado digital recibido. En caso negativo, el control fluye al paso S244.

En el caso de una transmisión monetaria, las condiciones expuestas en los datos de política son escalonadas desde los pasos de decisión S232 al paso de decisión S240. Si en el paso de decisión S232 el emisor del certificado digital se encuentra enumerado en la tabla x, que contiene los nombres de compañías y organizaciones para las que no se considera necesaria la comprobación del estado del certificado digital, entonces se establece confianza y el control pasa al paso S242. De otro modo, el control pasa al paso de decisión siguiente en la cadena que es el paso de decisión S234. En el paso de decisión S234, si el emisor del certificado digital está enumerado en la tabla b, que es la tabla 'AlwaysCheckFrom', entonces no se establece confianza y el control pasa a S244. De otro modo, el control pasa al paso de decisión S236, donde se determina si la cantidad de la transacción excede de $10.000. Esta determinación se realiza con referencia a los datos de transacción firmados que contendrán la cantidad monetaria o de manera predeterminada por el emisor del certificado, o contenidos dentro del correo electrónico o correos electrónicos asociados que forman la transacción o transmisiones. Si se halla que la transacción es por una cantidad superior a $10.000, o si la cantidad de la transacción no puede ser determinada con una referencia a los datos transmitidos, entonces no se establece confianza y el control pasa al paso S244. De otro modo, el control pasa al paso de decisión S238 en el que se determina si el certificado digital ha sido verificado dentro de los últimos 30 días. De nuevo, esta determinación se realiza con referencia a la base de datos de certificados digitales almacenados y datos relativos a certificados digitales. Si el certificado no ha sido verificado dentro de los últimos 30 días, entonces no se establece confianza y el control pasa al paso S244. Si ha sido verificado, entonces el control pasa al paso de decisión S240 donde, si la cantidad previamente determinada de la transacción se considera que es superior a $5.000, entonces no se establece confianza y el control pasa al paso S244. Si la cantidad de la transacción es inferior a $5.000, entonces se clasifica como riesgo aceptable de confianza en el certificado digital, se establece confianza y el control pasa al paso S242.

Estas dos últimas condiciones permiten que el sistema determine si comprobar el estado del certificado en base a la historia comercial reciente. Por ejemplo, si una parte va a realizar una transacción por una suma modesta, es decir, inferior a $5000, y la búsqueda de los detalles registrados de la transacción y del certificado describe que en fecha bastante reciente la misma parte realizó una transacción y entonces su certificado digital se confirmó como válido, entonces se puede afirmar que no es necesario verificar la validez del certificado de dicha parte de nuevo con tan poco espacio de tiempo del primero, y es preferible confiar en la parte más bien que pagar la tarifa de validación por segunda vez.

Se apreciará que se puede hacer que las instrucciones contenidas en el archivo de política reflejen el nivel de confianza que la compañía tiene en sus clientes o proveedores, en base a la experiencia de individuos dentro de la compañía, las cantidades de transacciones consideradas permisibles sin riesgo significativo, etc. El archivo de política también se puede crear con el fin de implementar políticas más generales que se hayan de usar en unión con un registro de detalles de transacción para el tenedor de dicho certificado digital. Por ejemplo, cualquier transacción ofrecida por el tenedor puede ser comparado con el registro de las que efectuó antes con el fin de ver si la cantidad y los artículos y servicios pedidos concuerdan con su historia comercial. Si no concuerdan, entonces puede ser deseable comprobar la validez del certificado para confirmar que todavía es válido y garantizar la identidad del emisor. Si ha sido revocado, entonces una tercera parte puede haber adquirido la clave privada del tenedor original y estar intentando hacer transacciones fraudulentas.

Habiendo verificado los datos de política en el paso S204, se habrá establecido confianza en el certificado digital o no. En el paso de decisión S206, si se estableció confianza, entonces el control pasa al paso S208 en el que se acepta la transmisión conteniendo la transacción. El control pasa entonces al paso S200 donde el módulo sale y el control vuelve al punto A en la figura 3 en el caso de un navegador web, o al punto A en la figura 5 en el caso de un cliente de correo electrónico.

Si en el paso S206 no se estableció confianza en el certificado digital, entonces el control pasa al paso S210, donde se lleva a cabo una comprobación de validación en línea del certificado digital. Esto puede implicar verificar si el certificado digital ha sido revocado, o si, en el caso de una transacción de comercio electrónico, el emisor del certificado digital confirmará una garantía de la cantidad prometida en la transacción. El control pasa después al paso S212, en el que se actualiza el estado de validez almacenado en la base de datos de dicho certificado. El control pasa entonces al paso de decisión S214 en el que, si el certificado se consideró no válido, el control pasa al paso S198 donde la transmisión es rechazada, o al paso S208 donde la transmisión es aceptada. El rechazo de la transmisión puede significar que se borre del buzón de receptores antes de que se abra, o que la transmisión se marque con la palabra 'rechazado' o algún otro indicador. Después de los pasos S198 o S208, el control pasa al paso S200 donde el módulo sale. Siempre que se permite que una transacción prosiga, la base de datos es actualizada de tal manera que incluya información acerca de la transacción, tal como fecha y cantidad, para que la información pueda ser usada al determinar la necesidad de futuras comprobaciones de validación.

Registro de información

El sistema preferido también proporciona una forma automática en la que registrar información sobre transacciones relativa a transacciones realizadas en línea. En este contexto, se ha previsto que la palabra 'transacción' y 'transacción de comercio electrónico' signifiquen un acuerdo que prometa dinero o valor en dinero realizado entre dos partes por Internet, o incluso en la misma red de una compañía. Normalmente, el usuario es responsable de mantener información sobre transacciones haciendo copias en papel de los registros electrónicos relevantes o guardando activamente copias de registros electrónicos en los archivos de su ordenador. Depender de métodos manuales para asegurar el mantenimiento de estos registros es claramente poco fiable y necesita mucho trabajo.

Por otra parte, el sistema preferido explora la información contenida de todas las comunicaciones procesadas por el sistema en busca de indicaciones de que una transacción ha comenzado o está teniendo lugar. Tales indicaciones son numerosas. La más sencilla es si el enlace es seguro o no puesto que muchas páginas web negocian un enlace seguro antes de realizar una transacción y cierran dicho enlace posteriormente. Determinar si un enlace es seguro se logra examinando la URL de la página web destino. Un enlace seguro se indica con una 's' después del prefijo 'http'. Así, un modo de operación del sistema preferido es registrar todos los datos transmitidos a una página web mientras un enlace es seguro. El sistema preferido también mantiene un registro de páginas web que negocian enlaces seguros, pero que no son sitios de comercio electrónico, es decir, los que están conectados a otro distinto de hacer compras, y no registran datos transmitidos a estas páginas. Tal página web podría ser la página web Hotmail de Microsoft que proporciona un servicio de correo electrónico.

Otra indicación podría ser simplemente la URL del sitio. En este caso el sistema preferido puede estar configurado para registrar todos los datos transmitidos a una página web que ha sido identificado como la de una compañía comercial en línea. Otras indicaciones podrían ser un número de tarjeta de crédito identificado, un resguardo electrónico, un reconocimiento por correo electrónico de la venta, la utilización de un certificado digital, en particular un certificado de garantía digital, o un código de compra.

Una vez que una transacción ha sido identificada como una transacción que está teniendo lugar, el sistema preferido puede registrar los detalles de la transacción almacenando en su totalidad cada comunicación entre un usuario y el comerciante identificado, o explorando las transmisiones y extrayendo detalles particulares, tales como la fecha, la cantidad, el tipo de artículos, la cantidad, etc.

El registro de datos de transacción puede ser parado cuando se identifica el final de la transacción o después de producirse un número predefinido de transmisiones entre el comprador y el comerciante. Igualmente, una vez que una transacción ha sido identificada, el sistema preferido puede registrar en la base de datos un número predefinido de transmisiones en cache producidas inmediatamente antes de la primera transmisión reconocida de la transacción.

Esto será útil cuando, por ejemplo, la primera indicación de que una transmisión está teniendo lugar es la detección de un número de tarjeta de crédito o un resguardo electrónico, dado que estos se recibirán probablemente al final de una transacción. Las transmisiones anteriores pueden constar, por ejemplo, de páginas web conteniendo información acerca de los artículos o servicios comprados, o un intercambio de correos electrónicos donde se acuerdan las especificaciones o los términos de entrega. Obsérvese que es perfectamente posible que las transmisiones anteriores sean del mismo tipo que aquella en la que se detectó la transacción, de un tipo diferente, o una mezcla de tipos. Por ejemplo un usuario podría visitar un sitio web www.abc.com, obtener detalles de artículos, y posteriormente pedirlas en un correo electrónico enviado a orders@ abc.com.

El sistema preferido registra los detalles de transacción en una base de datos común centralizada 42. Adicionalmente, la base de datos puede ser un archivo local o un servicio en una red. La información almacenada en la base de datos puede ser encriptada usando técnicas de encriptado conocidas de modo que solamente pueda acceder una persona con la autorización necesaria.

La figura 12 es una ilustración de la operación de una implementación ejemplar de un módulo para identificar cuándo se está realizando una transacción electrónica en línea. La figura 14 ilustra el proceso por el que el sistema preferido registra una transacción identificada en la base de datos, y la figura 15 ilustra cómo el sistema preferido permite que una transacción identificada sea aprobada o rechazada en base a una política de aprobaciones predeterminada.

Con referencia a la figura 12, a continuación se describirá la operación de un módulo para identificar cuándo está teniendo lugar una transacción en línea.

El módulo comienza la operación en el paso S250 en respuesta a recibir datos o en respuesta a que un usuario inicia una transmisión de datos a un sitio remoto. En el caso de una implementación de navegador web, será después del punto A o después del punto C, respectivamente, como se representa en la figura 3; en el caso de implementación en un cliente de correo electrónico será después del punto A o B, respectivamente, como se representa en la figura 5.

El control pasa entonces al paso de decisión S252 en el que se determina si, en el caso de un navegador web, se ha negociado un enlace seguro entre el sitio que transmite datos y el sitio que recibe datos. Esto se puede lograr consultando la dirección URL con la que se ha conectado, como se ha mencionado anteriormente, o interrogando el navegador web para ver si se está empleando encriptado. En el caso de un mensaje de correo electrónico este paso se omite y el control pasa directamente al paso S260. Dado que las transacciones por navegador web en línea implican generalmente la transmisión de información personal, como el nombre y la dirección, el número de tarjeta de crédito u otra información de identificación de cuenta, es natural que se negocien generalmente enlaces seguros. Así, la presencia de un enlace seguro solo es una buena indicación de que está teniendo lugar una transacción. Sin embargo, se puede negociar conexiones seguras por razones distintas de la transmisión de detalles de transacción. Así, si en el paso S252 se determina que la conexión es segura, el control pasa al paso S254, en el que la dirección del sitio remoto con la que se ha establecido la conexión, es verificada contra una lista de sitios conocidos que no proporcionan facilidades para realizar transacciones en línea, sino que establecen conexiones seguras. Los sitios de correo electrónico basados en navegador tales como el sitio Hotmail de Microsoft, es un ejemplo. El control pasa entonces al paso de decisión S256 donde se realiza una determinación en base a la comprobación previa. Si la dirección del sitio es identificada como un sitio no de comercio electrónico, que es uno que no facilita la realización de una transacción, entonces se determina que una transacción puede estar teniendo lugar o no, y el control pasa al paso de decisión S260 para hacer más comprobaciones en el contenido de la transmisión. Si en el paso S256 la dirección del sitio no es identificada como un sitio no de comercio electrónico conocido, entonces se supone que está teniendo lugar una transacción en línea, y el módulo sale en el paso S258.

Si se halla en el paso S252 que no se ha establecido una conexión segura, o si se ha establecido una conexión segura, pero con un sitio no de comercio electrónico conocido, determinado en el paso S256, o la transmisión es un correo electrónico, entonces el control pasa al paso de decisión S260. En el paso de decisión S260, se realiza la primera de varias comprobaciones del contenido de la transmisión con el fin de determinar si es parte de una transacción. En el paso S260, la transmisión es explorada para ver si contiene un número de tarjeta de crédito. El método para hacerlo se ha descrito con referencia a la figura 8. Si se halla un número de tarjeta de crédito en la transmisión, entonces se supone que una transacción debe estar teniendo lugar y el control pasa al paso S258 en el que el módulo sale. Si no se halla ningún número de tarjeta de crédito, entonces el control pasa en cambio al paso de decisión S262 donde se explora la transmisión para ver si contiene un código de cuenta. Los códigos de cuenta pueden estar almacenados (por ejemplo) en un archivo separado al que accede el módulo al realizar este paso o alternativamente un código de cuenta puede ser identificado a partir de datos descriptivos en la transmisión tal como un nombre de campo como “Account Number” o caracteres similares que aparecen en el texto de un mensaje.

Si en el paso de decisión S262 se halla un código de cuenta, entonces se supone que la transmisión constituye parte de una transacción y el control pasa al paso S258 donde el módulo sale. Si no se halla ningún código de cuenta, entonces el control pasa al paso S264 donde, en el caso de un navegador web, la URL es comparada con una lista de

URLs de comercio electrónico conocidas almacenadas en un archivo o en una base de datos. En el paso de decisión S266, se realiza una determinación sobre dicha comparación. Si se halla que la URL está en una página comercio electrónico conocida, o dentro de un conjunto conocido de páginas comercio electrónico, entonces se determina que está teniendo lugar una transacción de comercio electrónico y el control pasa al paso S258 donde el módulo sale. Igualmente, en el caso de un correo electrónico, la dirección de destino puede ser comparada contra una lista de direcciones de correo electrónico de comercio electrónico conocidas, por ejemplo 'orders@abc.com', y si se halla concordancia, entonces se determina que está teniendo lugar una transacción de comercio electrónico y el control pasa al paso S258 donde el módulo sale.

Las comprobaciones descritas son solamente representativas de las posibles comprobaciones que se podría hacer para determinar si es probable que una transmisión sea parte de una transacción de comercio electrónico, y no se pretende ser exhaustivos. Además, el orden en el que se han ilustrado las comprobaciones, no tiene significado especial. El orden depende simplemente de la estructura de los datos de política como se verá con referencia a la figura 13.

En el paso S268, se ilustra una comprobación general que representa más comprobaciones para una indicación de una transacción, además de las descritas anteriormente, que una compañía considera deseable emplear, tal como buscar códigos de compra o códigos embebidos colocados en los datos, por ejemplo. Se prefiere que el navegador web o cliente de correo electrónico usado en el sistema preferido permita al usuario marcar las transmisiones con un código embebido para indicar que la transmisión es parte de una transacción y deberá ser registrada. Además, el código embebido se podría poner en los datos por el sitio web o el cliente de correo electrónico que transmite algunos datos de transacción a la estación de trabajo del usuario.

El control pasa a este paso después del paso S266, si el lugar no es reconocido como un sitio de comercio electrónico conocido, y si se halla dicho indicador de transacción en el paso S268, entonces se considera que está teniendo lugar una transacción y el control pasa al paso S258 donde el módulo sale. Si en el paso S268, no se halla dicho indicador, entonces se considera que no está teniendo lugar ninguna transacción y el módulo sale en el paso S258. Después de la salida, los datos pueden ser transmitidos, después de los puntos C y B en las figuras 3 y 5, respectivamente, o ser procesados después a partir de su recepción en el punto A en las figuras 3 y 5.

En el ejemplo descrito, la finalidad es empezar a registrar transmisiones y posibles detalles de transacción si se sospecha que está teniendo lugar una transacción. Se supone que registrar datos que no son parte de una transacción es preferible a no registrar una transacción. La figura 13 es una ilustración de los datos de política usados para identificar que está teniendo lugar una transacción de comercio electrónico y para controlar la forma en que se registran los datos de transacción. Los datos de política se representan por una bifurcación de transacciones del árbol de datos de política que se subdivide en dos bifurcaciones secundarias separadas llamadas 'Identification' y 'Termination'. La bifurcación de identificación se divide en cinco bifurcaciones secundarias que corresponden a las determinaciones realizadas en el proceso ilustrado en la figura 12. La primera de estas bifurcaciones secundarias titulada 'IfConnectionGoesSecure' permite a un usuario especificar si el registro deberá empezar cuando el módulo plug-in detecte que la conexión al servidor web es segura. La condición especificada en esta bifurcación secundaria corresponde al paso de decisión S252 representado en la figura 12. Se apreciará con referencia a las figuras 12 y 13 que el flujo de control representado en la figura 12 corresponde a la disposición de las condiciones especificadas en las bifurcaciones del árbol de datos de política representado en la figura 13. La bifurcación ExcludedSites de la bifurcación IfConnectionGoesSecure contiene una referencia a la tabla q en la que se enumeran los sitios web de los que se sabe que negocian sitios seguros, pero que se sabe que no son sitios web comercio electrónico. A la tabla q se hace referencia en el paso S256 del proceso representado en la figura 12.

La bifurcación secundaria siguiente de la bifurcación de identificación se titula 'IfCreditCardNumberPresent' y permite al usuario especificar si la detección de un número de tarjeta de crédito deberá ser usada para iniciar el registro de datos que están siendo transmitidos o recibidos. Esta bifurcación secundaria corresponde al paso de decisión S260. La bifurcación secundaria PreviousPages de la bifurcación IfCreditCardNumberPresent enumera el número de páginas web, antes de la página web en la que se detectó el número de tarjeta de crédito, que también se deberá registrar. Dado que los números de tarjetas de crédito son presentados normalmente al final de la transacción, la provisión de esta bifurcación secundaria permite recuperar y almacenar páginas web anteriores que probablemente contienen los detalles y petición de la transacción. Estas páginas web se ponen en cache de forma continua por el sistema preferido de modo que si se identificase una transacción, puedan ser recuperadas de la cache y almacenadas en la base de datos. Esto se explicará con más detalle con referencia a la figura 14.

La bifurcación secundaria siguiente del árbol de bifurcaciones de identificación se titula 'IfAccountsCodePresent' y permite al usuario especificar si la detección de un código de cuenta en los datos transmitidos o recibidos ha de ser tomada como un indicador para iniciar el registro de los datos. Los códigos de cuentas son identificados en el paso S262 representado en la figura 12 por referencia a la tabla r. La referencia a esta tabla se contiene en la bifurcación secundaria AccountCodes de la bifurcación IfAccountCodePresent. Obsérvese que esta tabla también representa el número de páginas anteriores a registrar, de manera similar a la descrita anteriormente para la identificación de tarjetas de crédito; sin embargo, en este caso el número de páginas anteriores a registrar se guarda en la tabla r que permite especificar un número diferente de páginas para cada código de cuenta detectado.

La bifurcación IfKnownECommerceSite permite al usuario especificar una lista de URLs correspondientes a sitios, partes de sitios, o incluso sólo páginas, donde se sabe que tienen lugar transacciones de comercio electrónico.

EL URL de la página actual se coteja con entradas de esta lista para determinar si una transacción está teniendo lugar. La bifurcación secundaria KnownSites contiene una referencia a la tabla s en la que se guardan las URLs de sitios de comercio electrónico conocidos. La determinación de si la URL del sitio web es un sitio de comercio electrónico conocido se realiza en el paso de decisión S266 después del paso S264 de la figura 12. Por último, la bifurcación IfOtherIndicatorPresent proporciona una forma de que el usuario especifique si la determinación de otros indicadores deberá ser usada o no como un punto de inicio para el registro de datos. Dos bifurcaciones secundarias de esta bifurcación tituladas Keywords y PreviousPages especifican posibles indicadores que pueden ser detectados, en este caso las palabras clave enumeradas en la tabla t, y también el número de páginas anteriores que hay que almacenar si se detectan palabras clave.

La bifurcación Termination de la bifurcación Transactions se divide en cuatro bifurcaciones secundarias que especifican condiciones que se usan para finalizar el registro de datos transmitidos o recibidos. Cada bifurcación secundaria establece una condición por la que el final de la transacción puede ser definido. La primera bifurcación titulada 'IfConnectionGoesInsecure' permite al usuario especificar que el abandono de una conexión segura por el navegador web indica el final de una transacción de modo que el registro se deberá parar. Las otras bifurcaciones secundarias especifican que, cuando cambie el sitio web, se deberá parar el registro, si se recibe un resguardo digital se deberá parar el registro, y el registro deberá parar después de la recepción de 20 páginas web después de la identificación de que está teniendo lugar una transacción.

Se debe recalcar que los datos de política representados en este diagrama en particular, pero también en los otros diagramas, son únicos para cada usuario. No solamente puede el usuario especificar si se ha de actuar o no en condiciones concretas estableciendo consiguientemente la variable Sí o No, o cambiando el número de páginas que se han de registrar, por ejemplo, sino también la estructura y disposición de las bifurcaciones, y las condiciones especificadas en las bifurcaciones pueden ser diferentes de un usuario a otro. Se apreciará que aunque la política del ejemplo describe el registro de transacciones en un entorno de navegador web, una política similar controlaría el entorno de correo electrónico, omitiendo la opción de conexión segura, pero permitiendo definir la política para registrar correos electrónicos a la detección de números de tarjetas de crédito, códigos de cuenta u otra información identificable dentro de ellos, o donde los correos electrónicos son enviados a direcciones de comercio electrónico conocidas.

El pleno beneficio del método de identificar una transacción se obtiene cuando el método se utiliza junto con medios para registrar transmisiones entre un usuario del sistema preferido y un sitio remoto. Esto permite llevar y mantener automáticamente un registro de todas las transacciones realizadas por un usuario. Los registros se pueden mantener actualizados sin la necesidad de hacer copias en papel de cada transmisión recibida o enviada. Así, el mantenimiento de registros de una compañía se hace considerablemente más fácil y más exacto.

La figura 14 ilustra la operación de un módulo para registrar transmisiones que incluyen una transacción. El módulo se inicia en el paso S270.

Si el módulo se implementa como parte de un navegador web, el paso S270 se inicia en el punto A en la figura 3 después de la recepción de datos o después del punto C en la figura 3 directamente antes de la transmisión de datos al sitio remoto. Si el módulo se implementa como parte de un cliente de correo electrónico, el paso S270 tiene lugar después del punto A en la figura 5 después de haber recibido un correo electrónico o después del punto B en la figura 5 justo antes de que un correo electrónico creado por el usuario sea enviado a un receptor.

Después del paso S270, el control pasa al paso S272, en el que se realiza la prueba de identificar una transacción, descrita anteriormente con referencia a la figura 9, y se determina si está teniendo lugar una transacción de comercio electrónico. El control pasa entonces al paso de decisión S274 donde, si se determina que no está teniendo lugar ninguna transacción, el control pasa directamente al paso S276 donde el módulo sale.

Sin embargo, si se determina que una transacción está teniendo lugar, el control pasa al paso S278 en el que la política es consultada con respecto a uno o más medios de detección, la identidad del emisor, la cantidad de la transacción, u otros parámetros para determinar que las transmisiones anteriores, si hay alguna, deberán ser almacenadas con la transmisión identificada, y con cuánto detalle se deberá registrar la transmisión. La política podría requerir, por ejemplo, que una transacción que implique una suma grande de dinero, sea registrada con más detalle que una transacción de una suma pequeña. Un ejemplo de esto en la práctica podría ser el registro de cada página web a la que se accede durante la formación de una transacción en un sitio web de un comerciante en línea para transacciones que implican grandes sumas de dinero, pero solamente registrar la transmisión conteniendo un resguardo electrónico de transacciones de cantidades más pequeñas.

Además de determinar la cantidad de datos a almacenar, el archivo de política también puede determinar la naturaleza de los datos a registrar. Toda la transmisión o página web puede ser registrada como una serie de instantáneas de la transacción, de la misma forma que las páginas web se almacenan en memorias cache, por ejemplo, o alternativamente, elementos individuales de datos, tal como la fecha, la identidad del comerciante, la cantidad, etc, pueden ser extraídos de la transmisión o página web, y almacenarse solos o conjuntamente con los datos de instantánea.

De esta forma, la memoria para almacenamiento puede ser usada muy efectivamente con el fin de asegurar que las transacciones más importantes tengan suficiente espacio para ser registradas. La cantidad de datos de transacción a

registrar también puede depender de la identidad del comerciante, la posición geográfica, la historia comercial con la compañía del usuario, y los artículos y servicios que ofrece.

En la figura 13, los datos de política ejemplares muestran un escenario sencillo en el que la cantidad de datos a registrar se especifica en términos del número de páginas web que se han de recuperar de las páginas en memoria cache. El número difiere dependiendo de si se identifica un número de tarjeta de crédito, un código de cuenta o una palabra clave. Además, la tabla r representa que con el reconocimiento de diferentes códigos de cuenta, el número de páginas web anteriores a almacenar podría ser diferente, reflejando la importancia relativa de la cuenta.

La ampliación de este caso sencillo a otro más sofisticado se puede lograr proporcionando un nivel más alto de detalle en los datos de política. Bifurcaciones adicionales del árbol de datos de política podrían especificar nombres de una compañía o persona, o palabras clave específicas relativas a artículos y/o servicios; la cantidad de datos a registrar dependiendo de estas palabras clave así como los nombres.

Además, las tablas podrían expandirse para hacer referencia a la cantidad de diferentes tipos de datos que deberán ser almacenados. Datos como el nombre de la compañía, qué se vende, la cantidad, etc, podrían ser extraídos de texto de correo electrónico, del texto HTML que define la página web, o de la representación DOM de la página web, y almacenarse en la base de datos.

Todas las páginas web o la información almacenada en la cache pueden ser recuperadas, o alternativamente el sistema puede recuperar solamente páginas que tengan detalles en común con la página inicialmente identificada como parte de una transacción.

Alternativamente, se puede presentar al usuario una lista de todos los mensajes almacenados para que el usuario seleccione manualmente las transmisiones que se refieran a la transacción identificada.

Después de la determinación de cuántos datos registrar, el control pasa al paso de decisión S280. En el paso S280, si se ha de almacenar transmisiones anteriores, el control pasa al paso S282 donde se recuperan las transmisiones almacenadas en la cache local. En el caso de un navegador web, esto puede ser un número determinado de páginas anteriores, como se ha descrito anteriormente. Donde la transacción se detectó en un navegador web, la política también puede indicar que se busque en la cache mensajes de correo electrónico anteriores relativos a la transacción, por ejemplo enviados o recibidos de la misma organización. Esto se puede determinar cotejando porciones del navegador URL con porciones de las direcciones de correo electrónico. Igualmente, las transacciones detectadas en mensajes de correo electrónico pueden hacer que se recuperen de la cache correos electrónicos anteriores y páginas web anteriores. El control pasa entonces al paso S284 en el que la transacción identificada y las transmisiones anteriores recuperadas son almacenadas en la base de datos 42 del sistema.

En el paso S280, si no se requieren transmisiones anteriores, el control pasa directamente al paso S284 donde la transmisión identificada como una transacción es registrada en la base de datos del sistema. Al mismo tiempo que las transmisiones son almacenadas en el paso S284, datos relacionados, como la identidad del usuario, la cantidad y la otra parte de la transacción, también pueden ser registrados en la base de datos del sistema con el fin de formar un registro completo, aunque esto dependerá de las instrucciones de los datos de política. El control pasa entonces al S286 y el módulo sale.

A partir del paso S276 después de la salida del módulo, los datos pueden ser transmitidos, después del punto A en las figuras 3 y 5, o ser procesados después de ser recibidos en los puntos C y B en las figuras 3 y 5, respectivamente.

Una vez que una transmisión ha sido identificada como una transmisión que está teniendo lugar, todas las transmisiones entre el usuario y la otra parte pueden ser registradas hasta que el sistema detecte que la transacción ha terminado. La detección del punto de terminación de una transacción y la parada del registro se pueden hacer de manera similar a la descrita anteriormente para identificar si una transacción está teniendo lugar. La implementación más simple es registrar información de transmisión hasta que se reciba un resguardo electrónico u orden de envío. Alternativamente, el registro de transmisiones se puede parar después haberse producido un número predeterminado de transmisiones entre el usuario y la otra parte, o si ha pasado una cierta cantidad de tiempo desde que se identificó la transacción.

Las transmisiones se pueden hacer más sencillas si cada vez que el usuario cambia de sitio web se vacía la cache. Esto hace que sea poca la memoria requerida para la memoria cache, además de reducir el número de transmisiones previas que hay que buscar si se han de emplear técnicas de búsqueda.

Se apreciará que los métodos descritos anteriormente también se pueden usar para registrar transmisiones asociadas que tienen lugar después de que una transacción ha sido detectada y registrada. Por ejemplo, una transacción realizada usando un navegador web irá seguida típicamente de un correo electrónico de confirmación enviado por el vendedor al comprador. Este correo electrónico puede ser detectado como parte de la transacción, dado que contendrá características comunes, tales como el número de pedido, el número de cuenta, la descripción de artículos, el precio etc. También puede ser enviado desde una dirección similar a la dirección del sitio web, por ejemplo 'customerservices@abc.com' cuando el sitio web original usado para hacer la compra sea 'abc.com'. Se utiliza preferiblemente un

elemento de tiempo de tal manera que solamente las transmisiones posteriores que se produzcan dentro de un período de tiempo dado sean consideradas asociadas con la transacción original.

Además de registrar información sobre transacciones, puede ser ventajoso registrar otra información que proporcione a la gestión la capacidad de analizar el comportamiento de sus usuarios, por ejemplo, para asegurar que la organización está obteniendo de hecho un beneficio de productividad real de su adopción del comercio electrónico. Tal información no se limita a la productividad del usuario, sino al proceso general, permitiendo, por ejemplo, una comparación de sitios web de compra para determinar cuáles son los más eficientes en términos del proceso de compra, y por lo tanto cuáles serán más beneficiosos al reducir los costos de compra. El sistema preferido permite registrar información adicional, tal como la cantidad de tiempo que se tarda en una compra, el número de pulsaciones de teclas y clics de ratón requeridos para completar una compra, la cantidad de tiempo 'muerto' mientras el usuario espera a que se descarguen páginas o a recibir respuestas. Esta información puede ser registrada con el registro de transacción en la base de datos, pudiendo realizar un análisis estadístico de un rango de transacciones.

El tiempo que se tarda en una transacción puede ser determinado asociando un sello de tiempo con cada una de las transmisiones recibidas. Cuando se determina que la transacción ha terminado, el sello de tiempo asociado con la primera transmisión (que puede haber sido recuperada de la cache en el paso S282) se resta del sello de tiempo asociado con la última transmisión, y el resultado, que será la duración general de la transacción, se guarda en la base de datos en el paso S284. Alternativamente, se podrían registrar los sellos de tiempo primero y último en la base de datos y calcular más tarde la duración de la transacción. El número de pulsaciones de teclas y clics de ratón se puede determinar en un sistema basado en Windows de Microsoft usando "ganchos" de Windows estándar al sistema operativo. Tales técnicas se describen más plenamente en el documento "Win 32 Hooks" por Kyle Marsh del Microsoft Developer Network Technology Group, de 29 de julio de 1993, disponible en el sitio web de Microsoft Corporation (http://msdn.microsoft.com/library/default.asp?url./library/enus/dnmgmt/html/msdn_hooks32.asp).

El sistema preferido mantiene contadores del número de pulsaciones de teclas (usando el gancho WH_ KEYBOARD) y clics de ratón (usando el gancho WH_MOUSE) que se producen entre cada transmisión recibida, y asocia estos totales con la transmisión recibida. Se ignoran las pulsaciones de teclas y clics de ratón que se producen mientras otra aplicación constituye el centro de atención (por ejemplo, si el usuario pasa temporalmente a otra aplicación). Cuando se determina que la transacción ha terminado, los totales de pulsaciones de teclas y clics de ratón producidos entre la primera transmisión (que puede haberse recuperado de la cache en el paso S282) y la última transmisión se suman, y el resultado, que será el número total de pulsaciones de teclas y clics de ratón durante la transacción general, se guarda en la base de datos en el paso S284. Igualmente, el tiempo de respuesta de transacción del sitio web se puede medir anotando el tiempo en que se envía cada petición de transmisión de salida, y restándolo posteriormente del tiempo en que se recibe la transmisión de respuesta. Sumando los tiempos de respuesta entre el inicio y el final de la transacción se obtendrá el tiempo total que el usuario pasó esperando al sitio web. Igualmente el sistema preferido también cuenta el tiempo de respuesta del usuario, que es el tiempo entre la recepción de una transmisión, y el tiempo de transmisión de una respuesta.

El sistema preferido también calcula cuánto tiempo de respuesta del usuario se emplea en introducir datos, y por lo tanto permite determinar el tiempo requerido para que el usuario 'absorba' la transmisión entrante (que es la diferencia). El tiempo empleado introduciendo datos se determina manteniendo un 'cronómetro'. El cronómetro se resetea cada vez que se recibe una transmisión nueva, y se reinicia inmediatamente siempre que el usuario pulsa una tecla o clica el ratón. Si el usuario no introdujese ninguna pulsación de tecla o clicase el ratón durante un período de tiempo predeterminado, por ejemplo 5 segundos, el sistema asume que el usuario está entonces absorbiendo detalles de la transmisión anterior y para el reloj. El reloj también se para cuando la pulsación de tecla o clic del ratón hace que se envíe una transmisión de salida. Sumando el tiempo empleado en introducir datos entre el inicio y el final de la transacción se obtendrá el tiempo total que el usuario pasó introduciendo datos en el sitio web. Los tiempos sumados pueden ser almacenados en la base de datos en el paso S284 para análisis posterior.

El sistema preferido también proporciona medios para supervisar transacciones que se están realizando y referir automáticamente la transacción para aprobación si se considera necesario. Este proceso permite a una compañía grande supervisar y controlar las transacciones realizadas por sus empleados usando un solo conjunto de criterios expuestos en los datos de política. Los datos de política pueden ser consultados cada vez que se identifica una transacción con el fin de determinar si el usuario está autorizado para realizar dicha transacción o si tiene que pedir autorización de personas de nivel superior en la compañía. El proceso se ilustra en la figura 15 a la que ahora se hará referencia.

El módulo que realiza este proceso se inicia en el paso S290. Esta iniciación tiene lugar preferiblemente tan pronto como se han determinado todos los detalles relevantes de la transacción que hay que considerar, y antes de comprometer la transacción. En el caso de una transacción por correo electrónico, los detalles como los artículos y el precio se encuentran típicamente dentro de un solo correo electrónico y pueden ser considerados anteriores a la transmisión de dicho correo electrónico. En el caso de una transacción por navegador web, la existencia de transacción puede ser detectada antes de que se conozcan todos los detalles, en cuyo caso la iniciación no tiene lugar hasta que se conozcan. Esto no presenta normalmente ningún problema puesto que el compromiso final no tiene lugar hasta el final del proceso de transacción, después de conocer todos los detalles relevantes. La detección de la transacción y los detalles relevantes pueden ser determinados de la manera descrita anteriormente con referencia a la figura 12. Con referencia brevemente a las figuras 3 y 5, se observará que el paso S290 tiene lugar después del punto C en la figura 3

en el caso de implementación de navegador web, o después de punto A en la figura 5 en el caso de implementación de cliente de correo electrónico, una vez conocidos los detalles necesarios.

El control pasa del paso S290 al paso de decisión S292 en el que los detalles de la transacción son comparados con los parámetros de la política para determinar si se precisa aprobación. La determinación se puede basar en la identidad o el puesto del empleado que efectúa la transacción, la cantidad de la transacción, o la otra parte de la transacción. En algunos casos, la aprobación podría ser necesaria siempre, tal como si el director financiero de una compañía desea revisar cada transacción antes de que se realice.

La figura 16 es una ilustración de datos de política ejemplares que pueden ser usados para determinar si una transacción requiere aprobación de una tercera parte y también para determinar la identidad de un aprobador apropiado que se ha de utilizar. En este caso, las condiciones que figuran en los datos de política estipulan si se precisa aprobación dependiendo de la cantidad de la transacción, y la dirección URL de la otra parte de la transacción.

Los datos de política relevantes se exponen en la bifurcación Transactions Approval del árbol de datos de política. Esta bifurcación se subdivide en cuatro bifurcaciones secundarias. La primera bifurcación se denomina 'MaximumUnapproved TransactionAmount' y define una cantidad umbral de las transacciones. Las transacciones relativas a cantidades superiores al umbral deben ser aprobadas por un aprobador antes de que se lleven a cabo.

La segunda bifurcación secundaria titulada 'MaximumUnapproved MonthlyAmount' define una cantidad máxima para transacciones que un usuario puede efectuar en un mes. En este caso, cualquier transacción realizada por el usuario que haga que el total mensual exceda de $2.500 requerirá aprobación de una tercera parte, así como las transacciones adicionales realizadas después de alcanzar dicho umbral.

La tercera bifurcación titulada 'ExcludedSites' se refiere a una tabla conteniendo direcciones de sitios web y correo electrónico de todos los sitios que siempre requieren aprobación de una tercera parte antes de poder llevar a cabo una transacción. Finalmente, la última bifurcación titulada 'Approvers' se refiere a una tabla en la que se enumeran los nombres de posibles terceros aprobadores. Al lado de cada nombre figura la cantidad máxima de la transacción para la que dicho aprobador tiene autoridad, y una lista de sitios excluidos para los que dicho aprobador no puede aprobar una transacción. En el caso más simple, los aprobadores serán otros usuarios de ordenador registrados en la misma red que el usuario que realiza la transacción, tal como administradores de departamento o supervisores. Los aprobadores, por la naturaleza de su función, serán miembros de la compañía comercial que asuman y tengan la autoridad de asumir responsabilidad de las transacciones financieras que realice la compañía. También es posible que los aprobadores pertenezcan a un grupo de personas que realicen primariamente esta función, como las personas del departamento financiero solamente.

Si las condiciones de las tres primeras bifurcaciones secundarias de la bifurcación de transacción indican que se precisa aprobación, se puede buscar un aprobador apropiado explorando la tabla de aprobadores hasta que se encuentre un aprobador cuyo límite de transacción sea igual o mayor que el de la transacción propuesta y que no tenga prohibida la aprobación de transacciones con el sitio relevante.

Se apreciará que los datos de política ejemplares representados en la figura 16 son datos de política específicos de un solo usuario de ordenador, o grupo de usuarios, en la red. Otros usuarios, o grupos, pueden tener parámetros diferentes y una lista diferente de aprobadores.

Se apreciará que las condiciones para determinar un aprobador apropiado se pueden introducir creando nuevas bifurcaciones secundarias del árbol de datos de política.

La operación del proceso de aprobación se podría extender, por ejemplo, a cualquier tipo de transmisión, no solamente a las que incluyen una transacción de comercio electrónico. Tal operación puede ser implementada haciendo que las condiciones definidas o las bifurcaciones secundarias de los datos de política especifiquen nombres de usuario, direcciones o palabras clave, por ejemplo, que hayan de ser identificadas en la transmisión y en las que haya que actuar. Así, se puede hacer que todas las transmisiones por correo electrónico a una compañía concreta o individuo requieran aprobación, o que todos los correos electrónicos conteniendo información predeterminada sean reconocidos mediante identificación de palabras clave.

Si se determina en el paso S292 que no se requiere aprobación, el control pasa directamente al paso S294 en que el módulo sale. Después del paso S294, se permite la transmisión de la transacción y la transacción puede proseguir. El control vuelve del paso S294 al punto C en la figura 3 o al punto B en la figura 5.

Sin embargo, si en el paso S292, después de consultar los parámetros de la política, se determina que se precisa aprobación de la transacción, el control pasa al paso S296 en el que los detalles de la transacción se utilizan para determinar un aprobador apropiado para la transacción. El aprobador puede ser un empleado de la compañía registrado en su estación de trabajo, o en una estación de trabajo con función dedicada de aprobador tal como consolas de operador 44, como se representa en la figura 2, o puede incluso ser un proceso automatizado. En el caso de una compañía grande con varios departamentos, puede ser ventajoso tener un grupo de aprobadores por cada departamento, supervisando cada grupo las cuentas del departamento. Esto permite rechazar transacciones antes de realizarlas, por ejemplo, si el jefe del departamento decide que desea suspender temporalmente las compras o las compras de una clase concreta.

El control pasa del paso S296 después de la determinación de un aprobador apropiado al paso S298 donde se transmite una petición de aprobación al aprobador designado mediante la cola de aprobaciones del sistema 100. Después del paso S298 el control pasa al paso de decisión S300 donde se determina si se ha recibido una respuesta del aprobador. Un temporizador se pone en marcha en el momento en que se presenta una petición de aprobación. Si no se recibe una respuesta en el paso S300, el control pasa al paso S302 donde se determina a partir del temporizador si ha transcurrido el tiempo. A condición de que el período no haya transcurrido, el control vuelve del paso S302 a S300 donde el sistema sigue esperando una respuesta del aprobador. Así, los pasos de decisión S300 y S302 forman un bucle en el que el sistema espera hasta que se reciba una respuesta o hasta que expire el tiempo. En el paso de decisión S300 una vez recibida una respuesta, el control pasa al paso S304 en el que se actúa dependiendo de si la transacción fue aprobada o rechazada.

Si se aprobó la transacción, el control pasa del paso S304 al paso S294 en el que el módulo sale y la transmisión puede proseguir. Sin embargo, si la transmisión no es aprobada, entonces el control pasa del paso S300 al paso S306 en el que el módulo sale. Sin embargo, la salida en el paso S306 evita que tenga lugar la transmisión de la transacción y vuelve el usuario al punto A en la figura 3 en el caso de implementación de navegador web o al paso S132 “crear correo electrónico” en la figura 5 en el caso de implementación de cliente de correo electrónico.

Además, si se considera en el paso S302 que ha expirado el ‘tiempo’ sin que se haya recibido una respuesta del aprobador, entonces el control pasa directamente al paso S306 en el que el módulo sale.

El lado derecho de la figura 15 muestra los pasos implicados para el proceso de aprobación. El proceso de aprobación se inicia en el paso S310, del que el control pasa al paso S312 en el que la máquina del aprobador consulta en la cola de aprobaciones del sistema si hay nuevas peticiones de aprobación. El control pasa entonces al paso de decisión S314. En el paso S314, si no hay pendiente ninguna petición, el control vuelve al paso S312, donde la cola del sistema es interrogada de nuevo. Estos pasos se repiten hasta que se reciba una petición de aprobación o hasta que el aprobador desactive el proceso de aprobación.

En el paso S314, si se recibe una petición de aprobación, el control pasa al paso S316 en el que la petición de aprobación es descargada de la cola del sistema y el aprobador decide si aprobar la petición o denegarla. El control pasa entonces al paso S318 en el que la respuesta del aprobador es transmitida de nuevo a la cola de aprobaciones del sistema y de allí vuelve a la estación de trabajo de los usuarios.

El control vuelve del paso S318 al paso S312 en el que se consulta la cola de aprobaciones del sistema para ver si hay nuevas peticiones de aprobación. Se apreciará que el proceso de aprobación podría ser totalmente automatizado en algunas circunstancias. Por ejemplo, las transacciones puede ser rechazadas automáticamente si la compañía no tiene fondos suficientes, si harían que se superasen las cantidades presupuestadas, o si superasen simplemente una cantidad máxima. Tal automatización se podría prever alternativamente como parte del proceso de usuario, de tal manera que ni siquiera se haga una petición de aprobación.

Al determinar si aprobar una transacción dada, lo ideal es que el aprobador sea capaz de tener una visión completa, por ejemplo, de manera que pueda ver exactamente qué se está comprando, en vez de tener simplemente una información resumida, como el precio total y el proveedor. El sistema preferido lo permite combinando las características de registrar transmisiones descritas anteriormente con la característica de aprobaciones. La petición de aprobación presentada en el paso S298 se complementa con una referencia a la posición en la base de datos de la información sobre transacciones almacenada en el paso S284. El aprobador recibe los detalles de posición en el paso S316 y el sistema recupera las transmisiones que constituyen la transacción de la base de datos, presentándolas adecuadamente de tal manera que el aprobador pueda considerarlas al hacer su determinación de aprobación. La operación continúa entonces normalmente en el paso S318. Es claro que es importante que el paso de registro S284 tenga lugar antes de realizar la petición de aprobación en el paso S298, de otro modo la información registrada todavía no estará disponible. Dado que en el paso S284 la transacción habrá sido identificada, pero no completada todavía (dado que todavía no ha sido aprobada), es necesario que el registro de la base de datos realizado en el paso S284 contenga un señalizador que identifique la transacción como “pendiente”. Este señalizador puede ser actualizado posteriormente en el paso S316 para mostrar que la transacción ha sido aprobada o denegada, o alternativamente, si se deniega la aprobación, el registro y la base de datos se pueden borrar dado que la transacción no tuvo lugar.

Seguridad

El sistema preferido proporciona medios para asignar un nivel de seguridad apropiado a la transmisión dependiendo de la naturaleza identificada de los datos transmitidos. El nivel de seguridad asignado lo puede poner el usuario del sistema usando los datos de política para reflejar sus necesidades.

La implementación más simple de los datos de política en este caso es una lista conteniendo en una primera columna los posibles tipos de datos, tal como contraseñas de empleados, contraseñas de empresarios, números de tarjetas de crédito, detalles bancarios, etc, y conteniendo en una segunda columna la intensidad de encriptado deseada (en bits clave, por ejemplo) que se considera apropiada para cada tipo de datos. Se apreciará que también se puede emplear dentro del alcance de la invención otras formas de asignar niveles de seguridad en dependencia de la naturaleza determinada de los datos.

La figura 17 representa una ilustración ejemplar de datos de política que definen las intensidades de encriptado apropiadas para varios tipos de datos. Los datos de política asumen la forma de un número de pares de clave-valor dispuestos en bifurcaciones separadas del árbol de datos de política. La clave especifica el tipo de datos que se están transmitiendo, tales como contraseñas, números de tarjetas de crédito, palabras clave presentadas y una clave general para otros datos presentados. Los valores que corresponden a estas claves son la intensidad de encriptado en bits que se considera apropiada para la transmisión de los datos especificados en la clave. Los pares de clave-valor están dispuestos en varias bifurcaciones de la bifurcación RequiredEncryptionLevel de la bifurcación TransmittedDataSecurity del árbol de datos de política. Así, en el ejemplo, se puede ver que las contraseñas tienen una intensidad de encriptado deseada de 40 bits, los números de tarjetas de crédito de la compañía y los números de tarjetas de crédito personales tienen una intensidad de encriptado deseada de 128 bits, las palabras clave presentadas tienen una intensidad de encriptado deseada de 40 bits y otros datos presentados no requieren encriptado.

La bifurcación SubmittedKeywords se refiere a palabras concretas o cadenas o texto que han sido designados como sensibles y requieren alguna forma de encriptado. Pueden ser nombres de usuario, información de dirección, información financiera o palabras preseleccionadas tales como 'Confidencial' o 'Secreto'. Las palabras clave presentadas pueden ser detectadas con referencia a una tabla o archivo donde se guardan.

Además, cada bifurcación de los datos de política puede hacer referencia, en lugar de indicar una intensidad general de encriptado, a una tabla en la que las diferentes contraseñas o números de tarjetas de crédito, por ejemplo, se enumeran junto con las intensidades de encriptado correspondientes específicas de cada contraseña o número.

Una vez asignado un nivel de seguridad, el módulo plug-in interroga el navegador web para determinar la seguridad del enlace que ha sido establecido por el navegador web con el servidor web para transmisión de dicha información, o en el caso de una transmisión por correo electrónico, se aplicarán al mensaje los parámetros de encriptado que el usuario o la aplicación hayan determinado. Típicamente, serán la potencia criptográfica del algoritmo de encriptado usado para codificar los datos para transmisión. Tales detalles de transmisión son recibidos por el navegador web como parte de la 'conexión electrónica' del proveedor de servicios web.

Un enlace seguro se indica en general en una ventana del navegador por la presencia de un icono de candado cerrado en la esquina inferior derecha. Un usuario puede clicar en el icono para interrogar el nivel de seguridad proporcionado por el establecimiento de conexión. Al hacerlo, puede recibir una notificación de la forma ASSL segura (128 bit). La primera parte de la notificación describe el tipo del encriptado usado, mientras que la segunda parte describe la intensidad de encriptado. El módulo plug-in es implementado para obtener automáticamente estos datos del navegador de modo que pueda ser usado para determinar si el nivel de seguridad es adecuado para una transmisión propuesta. Igualmente, en el caso de un mensaje de correo electrónico, el módulo plug-in determina los parámetros de encriptado especificados por el usuario o la aplicación que se han de utilizar antes de la transmisión del mensaje.

El módulo compara la intensidad de encriptado especificada con la del enlace o mensaje, y dependiendo del resultado de la comparación, realiza una de las acciones siguientes:

a) si la seguridad del enlace es apropiada para la naturaleza de la información que se transmite, el módulo permite que la información sea transmitida;

b) si la seguridad del enlace es mayor que la requerida para la transmisión de la información, el módulo puede permitir que la información sea transmitida en dicho nivel de seguridad, renegociar automáticamente con el servidor web y el navegador web un nuevo nivel de seguridad apropiado y transmitir la información en dicho nivel, o indicar al usuario que el nivel de seguridad presente es innecesario e invitarle a realizar alguna acción.

c) si la seguridad del enlace no es suficiente para la naturaleza de la información que se transmite, el módulo puede evitar que se produzca la transmisión y avisar al usuario, renegociar automáticamente con el servidor web y el navegador web un nuevo nivel de seguridad apropiado y transmitir posteriormente la información en dicho nivel, o en el caso de un correo electrónico aumentar automáticamente el valor de la intensidad de encriptado, o indicar al usuario que el nivel de seguridad presente no es suficiente e invitarle a confirmar que sigue deseando que se produzca la transmisión.

Se apreciará que el módulo plug-in podría estar configurado para responder a una diferencia en el nivel de seguridad deseable determinado y que se dispone de varias formas y que las acciones esbozadas anteriormente son solamente ilustrativas.

Otras acciones que puede llevar a cabo el sistema podrían incluir pedir la descarga de una página web diferente a la máquina del usuario o modificar los datos de campo presentados de tal manera que no se transmita información sensible.

La operación de un módulo plug-in de navegador o correo electrónico para supervisar los datos transmitidos por un usuario del sistema preferido se ilustra en la figura 18, a la que se hará referencia. El módulo inicia la operación en el paso S320 en el punto C en la figura 3, justo antes de la transmisión de los datos a un servidor web, o en el punto B en la figura 5 justo antes de la transmisión de un correo electrónico. El control pasa entonces al paso S322, en el que

el módulo analiza los datos a punto de ser transmitidos y busca números de tarjetas de crédito. Un posible método de hacerlo se describió anteriormente con referencia a la figura 8. Si no se detecta ningún número de tarjeta de crédito en los datos, el control pasa al paso S314 en el que el módulo busca contraseñas en los datos a punto de ser transmitidos. Un método de hacerlo se ha descrito anteriormente, con referencia a la figura 6. Si no se halla ninguna contraseña en los datos, el control pasa al paso S316 en el que el módulo busca una cuenta de la compañía o códigos de compra en los datos. El reconocimiento de la cuenta o de los códigos de compra se puede lograr almacenando los códigos de la compañía en un archivo e intentando cotejar estos códigos con cadenas de dígitos halladas en los datos de salida. Si no se halla ningún código de cuenta, el control pasa al paso S318, donde el módulo busca indicaciones de otros datos sensibles en los datos a transmitir. Tales indicaciones se habrán tenido que definir con anterioridad preferiblemente en un archivo separado usado para detección, y dependerán de los requisitos de los usuarios del sistema preferido. Los ejemplos podrían ser palabras clave especificadas con relación a proyectos que la compañía esté realizando, los títulos de los proyectos, detalles personales, dirección del receptor de los datos, o del emisor, o incluso la palabra 'confidencial' o 'privado' incluida en los datos propiamente dichos.

Si no se hallan dichas indicaciones de que los datos son sensibles y requieren una mayor protección antes de ser transmitidos, la transmisión puede proseguir al nivel de encriptado corriente. Esto puede significar que la transmisión tiene lugar sin que se aplique ningún encriptado.

Sin embargo, si algunas de las comprobaciones realizadas en los pasos S322 a S328 ponen de manifiesto datos que se consideran sensibles, el control pasa al paso S332 en el que se asigna un nivel de seguridad a los datos detectados. Esto se logra comparando los datos detectados con entradas predeterminadas en los datos de política.

Cada entrada en la bifurcación de los datos de política tiene un nivel de encriptado preasignado que es el nivel mínimo que se puede utilizar para la transmisión de dichos datos. Las entradas en la tabla y el nivel de encriptado asignado, como con todos los parámetros de la política, son decididos por la compañía usando el sistema preferido dependiendo de sus requisitos. Entonces, asignar un nivel de seguridad es simplemente cuestión de buscar una contraseña, un número de tarjeta de crédito u otros datos en los datos de política y leer el nivel correspondiente. Se puede utilizar referencias a tablas en una bifurcación secundaria de los datos de política para asignar diferentes intensidades de encriptado a diferentes contraseñas, números de tarjetas de crédito, etc.

Una vez que el nivel de seguridad apropiado ha sido determinado en el paso S332, el control pasa al paso S334 en el que el módulo determina el nivel de encriptado que ha sido negociado con el servidor web al que se están transmitiendo los datos, o que ha de ser utilizado por la aplicación de correo electrónico antes de transmitir el mensaje. Esto se puede lograr interrogando al navegador web o aplicación de correo electrónico, o estableciendo variables de intensidad de encriptado al tiempo que se establece el enlace o determinan los requisitos de encriptado de correo electrónico, que tendrán lugar antes de la transmisión.

El control pasa entonces al paso de decisión S336 en que el nivel deseado de seguridad, es decir la intensidad de encriptado, se compara con el determinado en el paso anterior. Si el nivel deseado de encriptado es inferior o igual al determinado en el paso S334, se considera que hay suficiente protección de los datos a transmitir, y el control pasa al paso final S330, donde el módulo sale. Después del paso S330, el control vuelve al punto C en la figura 3 o al punto B en la figura 5 dependiendo de si el módulo se implementa en un navegador web o un cliente de correo electrónico. La transmisión de los datos puede proseguir entonces de forma usual.

Sin embargo, si en el paso S336 el nivel deseado de encriptado es superior al actualmente establecido, el módulo no permite que la transmisión siga adelante hasta que se haya negociado el nivel de encriptado apropiado. El control pasa al paso de decisión S338 en el que el módulo determina si es capaz de aumentar la intensidad de encriptado, y si es así, pasa el control al paso S340 donde se negocia un nuevo enlace encriptado más intenso, o en el caso de un correo electrónico una mayor intensidad de encriptado.

El nivel más alto de encriptado disponible depende del software usado por el servidor web y el navegador web, o en el caso de un correo electrónico por las aplicaciones de envío y recepción de correo electrónico. Puede haber casos en los que el nivel apropiado de encriptado no esté disponible, por una parte, y la transmisión de los datos nunca pueda proseguir. Además, a algunos tipos de datos se les puede dar un nivel de seguridad que indica que ningún nivel de encriptado será suficientemente alto para protegerlos, es decir, evitar que los datos sean transmitidos.

Habiendo intentado restablecer el enlace, o cambiar los parámetros de encriptado de correo electrónico, a una mayor intensidad de encriptado, el control vuelve al paso S334 para asegurar que el enlace o los parámetros tengan ahora una intensidad adecuada. Si no se puede renegociar el nivel de encriptado apropiado en el paso S338 o no tiene éxito un intento de aumentar la intensidad de encriptado en el paso S340, se considera inseguro transmitir los datos, y el control pasa al paso final S342 donde el módulo sale. Después de la salida en el paso S342, el control vuelve al punto A en la figura 3, o al paso S132 en la figura 5 'crear correo electrónico', para que el usuario reconsidere y edite o interrumpa la transmisión. También se puede presentar al usuario un mensaje adecuado para explicar las razones por las que se evita la transmisión.

Por lo tanto, el sistema preferido proporciona una forma de asegurar que la transmisión de datos sea lo más segura posible. Excluye la posibilidad de que un usuario olvide asegurar una transmisión, y negocia un nivel de seguridad más apropiado si el usado no es suficiente.

Los navegadores web pueden proporcionar similares facilidades para avisar al usuario de que los datos introducidos por el usuario están a punto de ser enviados por un enlace inseguro o proporcionar facilidades para encriptar todos los mensajes por defecto. Sin embargo, el sistema preferido proporciona la capacidad de examinar el contenido de datos a transmitir para determinar la seguridad que precisan, con el fin de permitir o evitar la transmisión en base a dichos requisitos de seguridad, y al nivel de seguridad determinado del enlace (intensidad de encriptado). Se apreciará que el sistema preferido proporciona un sistema significativamente mejorado de asegurar la transmisión, el cual reduce la posibilidad de error humano.

Supervisión de información sensible en los correos electrónicos de salida

Además del problema de que los datos sensibles sean interceptados por terceros entre el emisor y el receptor, las organizaciones corren un riesgo considerable de que sus usuarios revelen deliberadamente información sensible. Por ejemplo, la práctica de robar "electrónicamente" copias de documentos confidenciales, tales como listas de clientes, antes de dejar el empleo en una organización se lleva a cabo fácilmente, virtualmente sin dejar rastro, y en consecuencia está difundida. Todo lo que se precisa es que el usuario envíe el documento a su propia dirección privada de correo electrónico para recuperación posterior. El documento ni siquiera tiene que ser enviado mediante el propio sistema de correo electrónico de la organización, dado que se puede utilizar un servicio de correo por Internet, tal como "Hotmail", haciendo virtualmente imposible por los medios actuales el seguimiento de la "fuga" no autorizada.

Además de proporcionar medios para asegurar que se aplique a los mensajes un nivel apropiado de encriptado, el sistema preferido permite que los mensajes identificados como potencialmente sensibles sean redirigidos automáticamente o copiados a otro destino sin el conocimiento del usuario. Al determinar si redirigir tales mensajes, el sistema preferido tiene en cuenta varios factores incluyendo la identidad del emisor, la identidad del receptor previsto, la naturaleza de la dirección de los receptores previstos, la naturaleza del mensaje contenido, la naturaleza y la existencia de anexos al mensaje, los medios por los que está previsto que el mensaje sea transmitido, y si el mensaje y/o los anexos están encriptados.

La naturaleza del mensaje se puede determinar explorando una o más palabras clave, o combinaciones de palabras clave, o usando técnicas estándar de 'búsqueda en lenguaje natural'. La naturaleza de la dirección de los receptores previstos puede ser determinada por referencia a una lista de dominios conocidos de servicio de correo por Internet. Por ejemplo "hotmail.com", "yahoo.com" y "aol.com" son utilizados predominantemente por individuos, no por corporaciones. Igualmente, la dirección puede ser examinada en busca de semejanzas con el nombre del remitente, por ejemplo un correo electrónico del que se sabe que será enviado por Fred Smith a la dirección "smith900©; aol.com" podría ser considerado sospechoso por la inclusión de "smith" y "aol.com" en la dirección del receptor. El examen adicional del mensaje puede corroborar la probabilidad de que sea una revelación no autorizada de datos confidenciales, por ejemplo si el mensaje consta solamente de archivos anexos con el texto del mensaje y asunto en blanco, un indicio importante dado que es menos probable que el emisor teclee texto que solamente él leerá. Los medios por los que el mensaje está siendo transmitido es un factor importante, por ejemplo una transmisión enviada usando un servicio de correo por Internet, tal como hotmail, puede ser considerada mucho más sospechosa que otra enviada a través del sistema de correo electrónico corporativo usual.

De hecho, la 'carga' de archivos a un servicio de correo por Internet es potencialmente tan sospechosa que la realización preferida proporciona medios para prohibir la carga de archivos a dichos servicios.

Al redirigir correo, el sistema preferido añade texto adicional al inicio del correo, por ejemplo "----Correo redirigido----", juntamente con las direcciones de los receptores originalmente previstos, de tal manera que el nuevo receptor pueda determinar quién le redirigió el mensaje y a quién fue enviado originalmente.

Si el mensaje enviado ha de ser encriptado, el sistema preferido puede redirigir el mensaje encriptado o no encriptado a terceros. Preferiblemente, la clave encriptada del remitente es transmitida con el mensaje y se han previsto medios para que la tercera parte desencripte el mensaje, si ya ha sido encriptado, y encripte el mensaje con la clave encriptada del remitente original para transmisión.

El sistema preferido también identifica el correo entrante que ha sido redirigido (es decir, enviado a un usuario que no es el receptor previsto originalmente), buscando el texto "----Correo redirigido----". Tal correo puede ser señalizado para llamar la atención del nuevo receptor, por ejemplo, usando iconos especiales, o creando un buzón de mensajes para notificárselo. También se pueden prever medios para permitir que el nuevo receptor 'apruebe' fácilmente el mensaje y lo envíe al (a los) receptor(es) originalmente previstos. Esto se puede lograr, por ejemplo, proporcionando un botón "Aprobar". Si se pincha este botón, entonces el sistema preferido crea un nuevo mensaje de la misma manera que si el usuario hubiese pinchado el botón normal "Enviar". Sin embargo, en lugar de añadir texto al mensaje para indicar que ha sido enviado, en el caso del botón "Aprobar", el sistema extrae del mensaje la lista de receptores previstos originalmente, y posteriormente extrae los detalles de redirección para dejar el mensaje en su estado original. Los campos de destino "A", "Cc" y "Bcc" se rellenan entonces automáticamente con las direcciones extraídas de los receptores originales, y el campo "De" (que existe para cada mensaje aunque no se visualice normalmente) se rellena con el nombre/dirección del remitente original. El campo fecha/hora también puede ser ajustado a la fecha/hora del mensaje original. El mensaje es enviado entonces automáticamente o cuando el usuario pinche el botón 'Enviar'. De esta forma, pinchando solamente uno o dos botones, el correo redirigido puede ser aprobado y enviado, y cuando sea distribuido, parecerá venir del receptor original como si la redirección nunca hubiese tenido lugar.

Los datos de política de muestra para controlar la operación de un módulo plug-in implementado para redirigir correo se representan en la figura 19 y una ilustración esquemática de la operación de tal módulo plug-in se representa en la figura 20. La figura 19 es un árbol de datos de política que tiene varias bifurcaciones que corresponden a los pasos de decisión de la figura 20.

El módulo plug-in se inicia en el paso S350 que corresponde al punto B en la ilustración de la operación del cliente de correo electrónico en la figura 5. Una vez iniciado, el módulo plug-in recorre seis pasos para determinar diferentes detalles del mensaje de correo electrónico de salida. En primer lugar, en el paso S351 se verifica la identidad de la persona que envía el correo electrónico contra entradas en una lista predeterminada de nombres o direcciones. Se considera que los correos electrónicos de usuarios de esta lista tienen la autoridad de transmitir correos electrónicos directamente a los receptores previstos independientemente del contenido del mensaje e independientemente del receptor. Cualquier persona, no incluida en la lista, puede hacer que su correo electrónico sea redirigido o no dependiendo de su contenido. Así, en el paso de decisión S351, si el nombre o la dirección del usuario se encuentran en la lista, entonces el control pasa al paso S364 donde el correo electrónico puede ser transmitido sin más interacción. Sin embargo, si el usuario no está en la lista, el control pasa al paso S253 para comprobaciones adicionales. En el paso S352 el receptor del mensaje de correo electrónico de salida es verificado contra tablas de consulta, especificadas en la bifurcación Recipients de los datos de política representados en la figura 19. En el paso de decisión siguiente S354, el texto incluyendo el mensaje de correo electrónico, y los anexos unidos al mensaje de correo electrónico, es comparado con entradas de una tabla de consulta t. A la tabla t se hace referencia en la bifurcación Keywords de los datos de política y contiene palabras que indican que la naturaleza del mensaje de correo electrónico podría ser sensible a la compañía. En el paso siguiente S356, el mensaje de correo electrónico es verificado para ver si ha de ser encriptado o no. Se recordará que el encriptado no tiene lugar hasta el momento en que el correo electrónico sea transmitido, de modo que en esta etapa el correo electrónico solamente se señalizará para encriptado. En el paso de decisión siguiente S358, se determina si el mensaje de correo electrónico contiene anexos, y en el paso de decisión siguiente S360 si el mensaje de correo electrónico contiene texto acompañando a los anexos, es decir, si el texto del cuerpo del mensaje de correo electrónico está en blanco.

En cualquiera de los pasos de decisión S352, S354 o S362 donde se consulta una tabla de consulta, la concordancia entre una entrada en la tabla de consulta y una entrada en el correo electrónico indica que el correo electrónico deberá ser redirigido a una tercera parte para verificación antes de ser enviado por la compañía. Por ejemplo, si en el paso S354, se halla que el correo electrónico contiene las palabras 'confidencial' o 'secreto', que serán suficientes para garantizar que el correo electrónico sea verificado por una tercera parte antes de ser enviado a su receptor previsto. Esto asegura que la compañía no envíe información sensible sin que la compañía sea consciente de ello. Por lo tanto, el control fluye desde estos pasos al paso S364 donde se añade al mensaje texto que indica que el correo electrónico ha sido redirigido, y la dirección del receptor se cambia a la de la parte verificadora a quien el mensaje redirigido deberá ser transmitido. El control pasa entonces al paso S366 donde el correo electrónico es transmitido. Si el mensaje de correo electrónico ha sido marcado para redirección, en el paso S336 será transmitido naturalmente a la parte verificadora para revisión más bien que al el receptor original del mensaje.

En el paso de decisión S356, si se detecta encriptado del mensaje, entonces se considera suficiente garantizar la redirección del mensaje a una tercera parte para revisión. Consiguientemente, si el mensaje ha de ser encriptado, el control pasa del paso S356 al paso S364 donde el mensaje es modificado para redirección. En el caso de un mensaje señalizado para encriptado, se borra preferiblemente el señalizador de encriptado, de tal manera que el mensaje sea redirigido sin ser encriptado, permitiendo que el nuevo receptor lo lea. El texto de redirección, añadido al mensaje, también incluye preferiblemente la clave encriptada (que es generalmente la clave pública del receptor previsto, y por lo tanto no sensible) de modo que el mensaje pueda ser reencriptado antes de la transmisión.

Alternativamente, todo el certificado digital del receptor previsto podría ser incluido con el mensaje redirigido. La clave pública, o el certificado, según sea el caso, se quitarían entonces mediante el proceso automatizado de aprobación descrito anteriormente.

Si, en el paso S358, el correo electrónico no contiene anexos, entonces se considera que es improbable que el correo electrónico contenga documentos o archivos de información potencialmente sensible, y el correo electrónico puede ser transmitido así sin más intervención en el paso S364. Si el correo electrónico contiene anexos, y en el paso S360 se determina que el correo electrónico no contiene texto introducido en el cuerpo o el asunto del mensaje, entonces el mensaje es considerado un mensaje que probablemente está siendo enviado a una cuenta diferente del emisor. El correo electrónico es enviado entonces en el paso S362 y S364 a una tercera parte para verificación.

La figura 21 representa la operación del módulo plug-in para bloquear la carga de información del sistema informático de la compañía a un sitio externo. Se utiliza una comprobación simple en dos etapas, incluyendo una comprobación de la dirección del sitio externo en S372, después de la iniciación en el paso S370, y una comprobación de palabras clave sensibles en la información cargada en el paso S374. A condición de que no se halle que la dirección del sitio externo es un sitio prohibido en el paso S372, y que no se detecten palabras clave sensibles en el paso S374, la carga puede proseguir en el paso S376. De otro modo, la carga es bloqueada en el paso S378.

Los datos de política para controlar la operación del módulo plug-in para bloquear selectivamente la carga de información son sencillos, y se representan en la parte inferior de la figura 19.

De esta forma, las transmisiones de salida conteniendo información sensible que están siendo transmitidas por razones que no son del interés de la compañía, pueden ser verificadas antes de la transmisión, y la transmisión se puede evitar si es necesario.

Gestión del envío de correos electrónicos

Las aplicaciones de correo electrónico proporcionan medios para "Enviar" correo entrante a uno o más usuarios. El usuario típicamente pincha un botón "Enviar", que hace que una copia del correo entrante sea introducida automáticamente en la ventana de creación de correo, como si el usuario la hubiese tecleado. Todo lo que entonces tiene que hacer el usuario es introducir los nombres de los receptores previstos del correo enviado y pinchar el botón "Enviar". Ésta es una característica útil que permite al usuario compartir fácilmente con otros el contenido de un correo electrónico recibido.

Sin embargo, puede surgir un problema en el caso de que el correo contenga información sensible, en particular si la naturaleza sensible del correo no es inmediatamente evidente, por ejemplo si la información sensible aparece más abajo en el correo, de modo que el usuario tenga que bajar por la ventana de visión para leerla. Los usuarios envían frecuentemente correos electrónicos después de repasar solamente las primeras líneas, o en algunos casos solamente la línea de asunto, en particular cuando tienen grandes cantidades de correos electrónicos que procesar. Como consecuencia, a menudo se revela involuntariamente información sensible tanto dentro de la organización como fuera de ella, lo que es más peligroso. Ha habido casos donde se han perdido sumas considerables como resultado de ello.

Por lo tanto, el sistema preferido proporciona medios de controlar el envío de correos electrónicos. Tales controles incluyen proporcionar avisos al usuario antes de que un correo electrónico enviado sea transmitido y evitar que el correo electrónico sea enviado. También se podría facilitar medios para aprobar el correo electrónico antes de la transmisión, o para redirigirlo a otro usuario, como se ha descrito anteriormente.

Preferiblemente, el envío tiene lugar según el contenido del correo electrónico, y las direcciones de los receptores a quien ya haya sido enviado. Por ejemplo, la naturaleza sensible del correo electrónico puede ser determinada por varios métodos incluyendo la búsqueda de palabras clave tales como "confidencial", o verificando si el atributo de sensibilidad se ha puesto a "Personal", "Privado" o "Confidencial". También se pueden prever medios para que el creador original del mensaje lo marque como inadecuado para envío futuro insertando series de caracteres predefinidos, tales como "<NOFORWARD>" (evitar todo envío), o "<NOFORWARDEXTERNAL>" (evitar el envío fuera de la organización). Tales medios se podrían prever también en forma de un atributo adicional del mensaje.

Además de los factores basados en el contenido, el sistema preferido consulta la lista de receptores anteriores del mensaje. Si el correo electrónico ya ha sido enviado desde la organización por el creador original, entonces se puede considerar, por ejemplo, que es seguro permitir que sea enviado a más direcciones externas. Igualmente, si el correo electrónico original solamente fue enviado a un solo receptor, entonces se puede determinar que el creador original no quería que circulase ampliamente y se podría dar un aviso apropiado. El desarrollo de la acción en respuesta a los factores descritos puede ser determinado según la política.

El hecho de que un correo electrónico que está a punto de ser transmitido es un correo electrónico enviado, se puede determinar fácilmente buscando en el correo electrónico cadenas de caracteres tales como "Mensaje original" que el programa de correo electrónico añade automáticamente al inicio del correo original. Igualmente, la lista de receptores anteriores puede ser determinada buscando la serie de caracteres "Para:" y "CC:" que siguen a la cadena del mensaje original. La lista de receptores se encuentra inmediatamente después de estas series de caracteres. Los receptores internos y externos se pueden distinguir fácilmente por referencia al nombre de dominio (si lo hay). Por ejemplo, el nombre de un receptor representado como "Fred Smith" es típicamente interno, mientras que "fsmith@xyz.com" es típicamente externo.

Los datos de política para ordenar la operación de un módulo plug-in implementado para controlar el envío de mensajes de correo electrónico se representan en la figura 22, y la operación de tal módulo se muestra en la figura 23.

El árbol de datos de política contiene varias bifurcaciones secundarias especificando parámetros contra los que se pueden poner valores de órdenes. Por ejemplo, la primera bifurcación secundaria "PreventAll" cuando se pone a 'SÍ' ordena al módulo que evite que todos los correos electrónicos sean enviados. La bifurcación secundaria siguiente WarnAll cuando se pone a SÍ, exige al módulo que avise al usuario cliente de correo electrónico siempre que un correo electrónico esté a punto de ser enviado. Las dos bifurcaciones secundarias siguientes PreventExternal y WarnExternal contienen parámetros correspondientes para correos electrónicos externos solamente y permitir al usuario del cliente de correo electrónico distinguir entre reglas que afectan al envío de correos electrónicos dentro de la compañía y al envío de correos electrónicos a personas fuera de la compañía. La bifurcación "PreventKeywords" especifica una tabla de consulta en la que se guardan palabras clave indicativas de información sensible. Tales palabras clave pueden ser cadenas clave predefinidas tales como <NOFORWARD> o <NOFORWARDEXTERNAL>, o una o varias palabras predeterminadas.

El correo electrónico es explorado antes de la transmisión, y si se halla dicha palabra clave en el texto del correo electrónico o en cualquier anexo del correo electrónico, el correo electrónico no podrá ser enviado. Las últimas dos

bifurcaciones secundarias PreventIfNotSentExternally cuando estén puestas a SÍ, inhibirán la transmisión del correo electrónico enviado fuera de la compañía si antes no ha sido transmitido fuera de la compañía. En la práctica, el correo electrónico enviado puede ser transmitido a todos los receptores internos de la compañía, borrándose simplemente los receptores externos de la lista de receptores o alternativamente, antes de la transmisión, se le puede exigir al usuario que modifique la lista de direcciones de modo que no contenga receptores externos.

Finalmente, el parámetro puesto en la bifurcación PreventIfSingleRecipient cuando se pone a SÍ, evita el envío de mensajes de correo electrónico si el receptor original del mensaje era una sola persona.

La operación del módulo plug-in se ilustra en la figura 23. El módulo plug-in se inicia en el paso S380, de nuevo en el punto B en la figura 5. En el paso de decisión S382, el correo electrónico es objeto de una exploración preliminar para ver si contiene la cadena "----Mensaje original----", dado que el programa de correo electrónico añade automáticamente esta cadena clave al inicio del correo original al generar un mensaje para enviarlo. Si el mensaje de correo electrónico no contiene esta cadena, entonces se puede deducir que el mensaje de correo electrónico es un mensaje original y no está siendo enviado y el mensaje puede ser transmitido en el paso S384. Sin embargo, si se halla en el paso S382 que el mensaje contiene la cadena clave "----Mensaje original----", entonces el mensaje de correo electrónico es claramente un mensaje enviado, y el módulo lleva a cabo pasos adicionales para determinar si permitir que el mensaje enviado sea transmitido. El control fluye entonces al paso S386 en el que se verifican los receptores del mensaje enviado para ver si alguno es externo a la compañía en línea. Si hay un receptor externo, entonces el módulo plug-in explora en el paso S388 el mensaje de correo electrónico para ver si el correo electrónico ha sido enviado anteriormente a un receptor fuera de la compañía. En caso negativo, se evita que el mensaje de correo electrónico sea enviado en el paso S390 y se le notifica al usuario del cliente de correo electrónico. Sin embargo, si el mensaje de correo electrónico ha sido enviado fuera de la compañía con anterioridad, entonces se le notifica al usuario en el paso S392, después de lo que el mensaje de correo electrónico puede ser transmitido por el usuario o puede ser devuelto al usuario para que revise los receptores previstos.

Si en el paso S386 el mensaje enviado no ha de ser enviado a una dirección fuera de la compañía, entonces el control pasa al paso S394, en el que se determina si el usuario era el único receptor del mensaje original. Si lo era, entonces puede ser que el creador original del mensaje no pretendía que fuese transmitido a una audiencia grande. Consiguientemente, el control fluye al paso S390 donde se bloquea la transmisión del mensaje enviado de correo electrónico. Esto se lleva a cabo según los datos de política representados en la figura 22, que especifican la realización de dicha acción. Alternativamente, se puede avisar al usuario que intenta enviar el mensaje.

La última comprobación se realiza en el paso de decisión S396 en el que el contenido del mensaje y los anexos son comparados con entradas en una tabla de palabras clave. Si se halla alguna concordancia entre entradas del correo electrónico y de la tabla, entonces se considera que el mensaje contiene información sensible y no es enviado. El módulo termina entonces en el paso S390. Si no se encuentran palabras clave sensibles, entonces el correo electrónico puede ser enviado en el paso S384.

Gestionar la firma de transmisiones de salida

La capacidad de usar un certificado digital para firmar un mensaje es claramente valioso para el receptor del mensaje al establecer la identidad del emisor, y para ambas partes al asegurar que el mensaje no ha sido manipulado. Sin embargo, el emisor del mensaje deberá ser consciente de que un mensaje firmado digitalmente constituye potencialmente un contrato vinculante, que no puede ser negado o revocado una vez enviado. Por lo tanto, hay que tener cuidado al firmar digitalmente un documento, lo mismo que al firmar un documento en papel. Las aplicaciones de correo electrónico, tales como "Outlook" de Microsoft Corporation proporcionan medios para firmar digitalmente mensajes automáticamente, y aunque esto puede ser valioso al confirmar la identidad del emisor ante el receptor, por las razones descritas anteriormente, también es potencialmente peligroso, requiriendo que el usuario tenga sumo cuidado con el contenido del mensaje.

El sistema preferido proporciona medios para controlar la firma de mensajes de salida, según los datos de política. Se muestran datos de política de muestra en la figura 24. Tales controles incluyen:

obligar a que un mensaje sea firmado;

indicar al usuario que firme un mensaje;

indicar al usuario que un mensaje no deberá ser firmado; y

evitar que un mensaje sea firmado.

Al determinar el desarrollo de la acción a tomar, el sistema preferido tiene en cuenta varios factores, incluyendo la naturaleza del contenido del mensaje (incluyendo los anexos), la identidad del receptor previsto y/o su organización, la identidad del emisor, la naturaleza del certificado digital usado (si el mensaje ya ha sido señalizado para firma), y la naturaleza del (de los) certificado(s) digital(es) disponibles para firmar el mensaje.

La naturaleza del mensaje puede ser determinada buscando una o más palabras clave, o combinaciones de palabras clave, o usando técnicas estándar 'de búsqueda en lenguaje natural'. Igualmente, la naturaleza de los certificados digitales previstos o disponibles puede ser determinada por referencia al emisor y al tipo de certificado.

La figura 25 ilustra la operación de un módulo plug-in para asegurar que un correo electrónico sea firmado digitalmente de forma apropiada o no. El módulo se inicia en el paso S400, en el punto B en la operación del cliente de correo electrónico ilustrado en la figura 5. El control pasa entonces al paso de decisión S402 en el que el correo electrónico de salida es explorado para ver si ya ha sido marcado para firma. La 'firma' real del mensaje no se producirá hasta directamente antes de la transmisión. Si no está marcado para firma, el control pasa a S404 donde el módulo consulta una tabla de consulta de receptores (tabla f) para determinar si el receptor del correo electrónico de salida ha sido identificado como uno cuyos correos electrónicos siempre deberán ser firmados digitalmente. Si el receptor figura en la tabla f, el control pasa al paso S406 donde al usuario del cliente de correo electrónico se le notifica que el correo electrónico no será enviado a no ser que esté firmado digitalmente. Alternativamente, el módulo plug-in puede firmar digitalmente de forma automática el correo electrónico usando el certificado digital del autor del correo electrónico.

Si en el paso S404, el receptor del correo electrónico de salida no se encuentra en la tabla de consulta, el control pasa al paso de decisión S408 donde se consulta la KeywordsTable en la bifurcación EnforceSigning del árbol de política. Si se hallase alguna de las palabras clave de la tabla g en el texto del correo electrónico o en alguno de los anexos del correo electrónico, se requerirá la firma digital del correo electrónico, y el control pasará al paso S406 como antes. Se apreciará que los pasos de decisión S404 y S406 corresponden a órdenes de búsqueda para consultar las tablas Recipients y Keywords en la bifurcación EnforceSigning de los datos de política.

Tales palabras clave pueden ser palabras predeterminadas como "Confidencial", "Secreto", "Contrato", "Precio", "Pedido", etc, como se ilustra en la figura 24.

Si los receptores del correo electrónico no se encuentran en la tabla f, y el correo electrónico no contiene palabras clave especificadas en la tabla g, el control pasa al paso de decisión S410, correspondiente a una orden de consulta en la bifurcación SuggestSigning de los datos de política de muestra. En el paso de decisión S410 la dirección del receptor es verificada contra las de la tabla de consulta h para determinar si se aconseja la firma del correo electrónico. Si el nombre del receptor se halla en la tabla h, entonces el control pasa al paso S412, donde al usuario del cliente de correo electrónico se le notifica la conveniencia de firmar digitalmente el mensaje de correo electrónico de salida. Sin embargo, al usuario del cliente de correo electrónico no se le exige que firme digitalmente el mensaje de correo electrónico y por lo tanto el correo electrónico puede ser transmitido sin firma, si el usuario opta por ello. Después del paso de decisión S410, si el nombre del receptor no se encuentra en la tabla h, el control pasa al paso de decisión S414, donde, como antes, se busca en el texto del correo electrónico un número de palabras clave que podría indicar que contiene datos sensibles y requiere una firma digital. Dependiendo de si correo electrónico contiene tales palabras clave sensibles, al usuario del cliente de correo electrónico se le notifica en el paso S412 la conveniencia de firmar digitalmente el mensaje, o alternativamente, el mensaje de correo electrónico es transmitido sin firma en el paso S416.

Si en el paso S402 después de la iniciación del módulo plug-in se halla que el correo electrónico ha sido marcado para firma, entonces el control pasa al paso de decisión S418. En el paso de decisión S418 el módulo plug-in consulta la tabla de consulta m en la bifurcación DenySigning especificada debajo de la bifurcación DenySigning de los datos de política. La tabla m es especificada en la bifurcación CertificatesUsed debajo de la bifurcación DenySigning, y especifica el emisor, el tipo, el número de certificado o clave de firma de certificados digitales que se consideran de interés. Si el certificado digital o clave de firma que se ha de usar para firmar el correo electrónico de salida se encuentra en la tabla m, entonces se harán más comprobaciones relativas al receptor y la naturaleza del correo electrónico de salida con el fin de determinar si es apropiado firmar el mensaje o no. El control pasa al paso S420, donde el receptor del correo electrónico de salida es verificado contra la tabla de receptores n y posteriormente al paso de decisión S422 donde el texto del correo electrónico y los anexos son explorados en busca de varias palabras clave. Si en alguno de los pasos de decisión S420 o S422, el receptor o algún texto del mensaje coinciden con las tablas de consulta, el control pasa al paso S424 donde se bloquea la transmisión del correo electrónico. El usuario del cliente de correo electrónico puede volver entonces a la etapa de entrada de texto del correo electrónico, y se le puede exigir que retransmita el mensaje sin firma digital.

Si en alguno de los pasos S418 o S422 se halla que el certificado o clave de firma no es de interés, y que el texto del correo electrónico no contiene palabras sensibles, el control pasa al paso S426 que corresponde a la primera bifurcación secundaria en la bifurcación SuggestNotSigning del árbol de datos de política. Como para la bifurcación DenySigning del árbol de datos de política, los tres pasos de decisión S426, S428 y S430 corresponden a las órdenes de consulta para verificar el certificado digital o la clave de firma usada con el correo electrónico, el receptor del correo electrónico de salida y el texto del correo electrónico de salida contra entradas sensibles predeterminadas en las tablas de consulta j, k y l, respectivamente. Si se halla en el paso S426 que el certificado usado para firmar el correo electrónico de salida es de interés, y se halla en alguno de los pasos S428 o S430 que el receptor o el texto del correo electrónico de salida coincide con entradas en las tablas de consulta especificadas, el control pasará al paso S432 en el que al usuario del cliente de correo electrónico se le notificará la conveniencia de no firmar digitalmente el mensaje de correo electrónico de salida. Sin embargo, el usuario todavía es libre de enviar el mensaje de correo electrónico firmado, si así lo desea.

Si no se halla coincidencia en ninguno de los pasos de decisión S426, S428 y S430, entonces el correo electrónico es enviado normalmente en el paso S416.

Aplicaciones de telefonía y mensajería instantánea

Además de la actividad de navegador y correo electrónico, en situaciones comerciales son populares ahora aplicaciones adicionales como mensajes instantáneos (también conocidos como 'chat') y aplicaciones de telefonía digital, tal como "Voice over IP"). Las normas sobre mensajería instantánea se definen en 2778 y 2779 de RFC y por el grupo de trabajo IETF SIMPLE. Las normas de Voz por IP se definen en ITU-T Recomendación H.323 (1998). Muchos aspectos de la presente invención pueden ser aplicados a los datos transmitidos y recibidos por tales aplicaciones. La mensajería instantánea es conceptualmente similar a una serie de correos electrónicos enviados y recibidos, excepto que la 'conversación' se lleva a cabo 'en vivo', estando presentes ambas partes durante toda ella. Sin embargo, a los efectos de la presente invención, los procedimientos son idénticos. La figura 5 de los dibujos puede representar mensajería instantánea sustituyendo la palabra "Correo electrónico" en los pasos S122, S124, S132 y S134 por la palabra "Mensaje". La descripción de "servidor de correo electrónico" 95 se sustituye por "Envío de mensaje". La realización preferida se ha dispuesto para interceptación en los puntos A y B como antes, proporcionando un plug-in a la aplicación de mensajes por Internet, o desarrollando una aplicación de mensajería instantánea que contenga la funcionalidad plug-in. Alternativamente, se apreciará que la intercepción podría tener lugar al nivel de protocolo, interceptando paquetes en red antes de que salgan de la máquina del usuario, o cuando lleguen a la máquina del usuario.

El protocolo de voz por Internet (VOIP) es conceptualmente similar a la mensajería instantánea, a excepción de que el contenido del mensaje consiste en voz digitalizada, que es codificada y transmitida inmediatamente. El análisis del contenido de los mensajes es inviable; sin embargo, los medios para registrar el mensaje y establecer controles al nivel de 'llamada' son viables y se implementan de manera similar, o como un plug-in en la aplicación de mensajes de voz, o al nivel de protocolo de red, o dentro de la máquina del usuario.

Aunque la implementación del sistema preferido se ha descrito con referencia a módulos plug-in para aplicaciones existentes, la invención se puede implementar proporcionando los navegadores web, clientes de correo electrónico, aplicaciones de mensajería instantánea o aplicaciones de voz por IP en los que la funcionalidad de los módulos plug-in aquí descritos ya está codificada desde el principio.

REIVINDICACIONES

1. Un sistema de gestión de información incluyendo:

una pluralidad de estaciones de trabajo adaptadas para conexión a una red de ordenadores, teniendo cada estación de trabajo una memoria;

una aplicación almacenada en dicha memoria de cada estación de trabajo para transmitir mensajes de salida a dicha red y recibir mensajes de entrada de dicha red; y

un analizador, integrado en la aplicación, pudiendo operar dicho analizador en unión con datos de política para determinar uno o más detalles completados del mensaje de salida cuando se inicia la transmisión del mensaje de salida, y para redirigir selectivamente el mensaje de salida a una tercera parte en lugar del receptor previsto originalmente;

donde los datos de política están definidos en el centro para la pluralidad de estaciones de trabajo y contienen reglas para determinar uno o más detalles completados del mensaje de salida, y para controlar la transmisión de dicho mensaje de salida en dependencia de los detalles.

2. El sistema de la reivindicación 1, donde el analizador puede operar para redirigir el mensaje de salida a dicha tercera parte si el mensaje ha de ser enviado a uno o más de una lista predeterminada de receptores o direcciones.

3. El sistema de la reivindicación 1 o 2, donde dichos datos de política incluyen una lista de nombres de empleados de compañía que pueden usar dicha aplicación para enviar mensajes de salida de y recibir mensajes de entrada en una dirección de la compañía, y donde el analizador puede operar para redirigir el mensaje de salida de cualquiera de dichos empleados a dicha tercera parte, si determina que la dirección prevista del mensaje de salida contiene uno de una lista predeterminada de nombres de dominio, y si la dirección de la compañía incluye al menos uno del apellido, primeros nombres o iniciales del empleado en dicha lista de nombres.

4. El sistema de cualquier reivindicación precedente, donde el analizador puede operar para redirigir el mensaje de salida a dicha tercera parte si el mensaje contiene una o más palabras clave predeterminadas o combinación de palabras clave.

5. El sistema de cualquier reivindicación precedente, donde el analizador puede operar para redirigir el mensaje de salida a dicha tercera parte si el mensaje o anexos al mensaje han de ser encriptados antes de la transmisión.

6. El sistema de la reivindicación 5, donde el analizador puede operar para redirigir el mensaje con su clave original encriptada a la tercera parte, y donde la tercera parte tiene medios para aprobar el mensaje para transmisión al receptor previsto originalmente y volver a encriptar el mensaje con la clave original.

7. El sistema de la reivindicación 5 o 6, donde el analizador puede operar para añadir texto al mensaje antes de que sea redirigido indicando que es un mensaje redirigido.

8. El sistema de cualquier reivindicación precedente, donde el analizador puede operar para redirigir el mensaje de salida a dicha tercera parte si el mensaje contiene anexos, o tipos particulares de anexos.

9. El sistema de cualquier reivindicación precedente, donde el analizador puede operar para redirigir el mensaje de salida a dicha tercera parte si el mensaje contiene anexos y si el cuerpo o el asunto del mensaje contiene menos de una cantidad predeterminada de texto.

10. El sistema de cualquier reivindicación precedente, donde el analizador puede operar para redirigir el mensaje de salida a dicha tercera parte en dependencia de la identidad del autor del mensaje.

11. El sistema de cualquier reivindicación precedente, donde se han previsto medios en el mensaje redirigido recibido por la tercera parte para que la tercera parte apruebe el mensaje para transmisión al receptor previsto originalmente.

12. El sistema de cualquier reivindicación precedente, donde dicha aplicación es un navegador web.

13. El sistema de la reivindicación 12, donde dicho analizador es un módulo plug-in (70, 72) de dicho navegador web.

14. El sistema de la reivindicación 13, donde dicho navegador web es Internet Explorer de Microsoft y dicho analizador es un Browser Helper Object.

15. El sistema de cualquiera de las reivindicaciones 1 a 11, donde dicha aplicación es un cliente de correo electrónico.

16. El sistema de la reivindicación 15, donde dicho analizador es un módulo plug-in (74) de dicho cliente de correo electrónico.

17. El sistema de la reivindicación 16, donde dicho cliente de correo electrónico es cliente de correo electrónico Outlook de Microsoft y dicho analizador es una extensión de cliente de Exchange de Microsoft.

18. El sistema de cualquiera de las reivindicaciones 1 a 11, donde dicha aplicación es una aplicación de mensajería instantánea.

19. El sistema de la reivindicación 18, donde dicho analizador es un módulo plug-in de dicha aplicación de mensajería instantánea.

20. El sistema de cualquiera de las reivindicaciones 1 a 11, donde dicha aplicación es una aplicación de mensajes de voz.

21. El sistema de la reivindicación 20, donde dicho analizador es un módulo plug-in de dicha aplicación de mensajes de voz.

22. El sistema de cualquier reivindicación precedente donde los datos de política definen una o más políticas para usuarios individuales o grupos de usuarios de las estaciones de trabajo.

23. El sistema de cualquier reivindicación precedente incluyendo un servidor central en el que los datos de política están almacenados.

24. Un método de gestionar información incluyendo los pasos de:

proporcionar una pluralidad de estaciones de trabajo adaptadas para conexión a una red de ordenadores, teniendo cada estación de trabajo una memoria;

proporcionar una aplicación almacenada en la memoria de cada estación de trabajo para transmitir mensajes de salida a dicha red y recibir mensajes de entrada de dicha red;

analizar por medio de un analizador integrado en la aplicación, dicho mensaje de salida cuando se inicia la transmisión del mensaje para determinar, en unión con dichos datos de política, uno o más detalles completados del mensaje de salida; y

redirigir selectivamente el mensaje de salida a una tercera parte en lugar del receptor previsto originalmente dependiendo de dicho uno o más detalles;

donde los datos de política están definidos en el centro para la pluralidad de estaciones de trabajo y contienen reglas para determinar uno o más detalles del mensaje de salida, y para controlar la transmisión de dicho mensaje de salida en dependencia de los detalles.

25. El método de la reivindicación 24, donde el mensaje de salida es redirigido a dicha tercera parte si el mensaje ha de ser enviado a uno o más de una lista predeterminada de receptores o direcciones.

26. El método de la reivindicación 24 a 25, donde dichos datos de política incluyen una lista de nombres de empleados de compañía que pueden usar dicha aplicación para enviar mensajes de salida de y recibir mensajes de entrada en una dirección de la compañía, y donde el mensaje de salida de cualquiera de dichos empleados es redirigido a dicha tercera parte, si se determina en el paso de análisis que la dirección prevista del mensaje de salida contiene uno de una lista predeterminada de nombres de dominio, y si la dirección de la compañía incluye al menos uno del apellido, primeros nombres o iniciales de un empleado en dicha lista de nombres.

27. El método de cualquiera de las reivindicaciones 24 a 26, donde el mensaje de salida es redirigido a dicha tercera parte si el mensaje contiene una o más palabras clave predeterminadas o combinación de palabras clave.

28. El método de cualquiera de las reivindicaciones 24 a 27, donde el mensaje de salida es redirigido a dicha tercera parte si el mensaje o anexos al mensaje han de ser encriptados antes de la transmisión.

29. El método de la reivindicación 28, incluyendo los pasos de:

redirigir el mensaje de salida con su clave original encriptada a la tercera parte, y proporcionar medios para que la tercera parte apruebe el mensaje para transmisión al receptor previsto originalmente y reencripte el mensaje con la clave original.

30. El método de las reivindicaciones 28 a 29, incluyendo añadir texto al mensaje antes de que sea redirigido indicando que es un mensaje redirigido.

31. El método de cualquiera de las reivindicaciones 24 a 30, donde el mensaje de salida es redirigido a dicha tercera parte si el mensaje contiene anexos, o tipos particulares de anexos.

32. El método de cualquiera de las reivindicaciones 24 a 31, donde el mensaje de salida es redirigido a dicha tercera parte si el mensaje contiene anexos y si el cuerpo o el asunto del mensaje contiene menos de una cantidad predeterminada de texto.

33. El método de cualquiera de las reivindicaciones 24 a 32, donde el mensaje de salida es redirigido a dicha tercera parte en dependencia de la identidad del autor del mensaje.

34. El método de cualquiera de las reivindicaciones 24 a 33, incluyendo proporcionar medios para que la tercera parte apruebe el mensaje para transmisión al receptor previsto originalmente.

35. El método de cualquiera de las reivindicaciones 24 a 34, donde dicha aplicación es un navegador web.

36. El método de la reivindicación 35, donde dicho paso de análisis es realizado por un módulo plug-in (70, 72) de dicho navegador web.

37. El método de la reivindicación 36, donde dicho navegador web es Internet Explorer de Microsoft y dicho módulo plug-in es un Browser Helper Object.

38. El método de cualquiera de las reivindicaciones 24 a 34, donde dicha aplicación es un cliente de correo electrónico.

39. El método de la reivindicación 38, donde dicho paso de análisis es realizado por un módulo plug-in (74) de dicho cliente de correo electrónico.

40. El método de la reivindicación 39, donde dicho cliente de correo electrónico es cliente de correo electrónico Outlook de Microsoft y dicho módulo plug-in es una extensión de cliente de Exchange de Microsoft.

41. El método de cualquiera de las reivindicaciones 24 a 34, donde dicha aplicación es una aplicación de mensajería instantánea.

42. El método de la reivindicación 41, donde dicho paso de análisis es realizado por un módulo plug-in de dicha aplicación de mensajería instantánea.

43. El método de cualquiera de las reivindicaciones 24 a 34, donde dicha aplicación es una aplicación de mensajes de voz.

44. El método de la reivindicación 43, donde dicho paso de análisis es realizado por un módulo plug-in de dicha aplicación de mensajes de voz.

45. El método de cualquiera de las reivindicaciones 24 a 44, donde los datos de política definen una o más políticas para usuarios individuales o grupos de usuarios de las estaciones de trabajo.

46. El método de cualquiera de las reivindicaciones 24 a 45, incluyendo proporcionar un servidor central y almacenar los datos de política en el servidor central.

47. Un producto de software informático, para controlar un ordenador en una pluralidad de estaciones de trabajo para gestionar información, estando conectado dicho ordenador a una red y teniendo acceso a datos de política de definición central para la pluralidad de estaciones de trabajo conteniendo reglas para controlar la transmisión de datos de salida a la red, incluyendo un medio de registro legible por el ordenador, en el que se ha registrado un código de programa que, cuando es ejecutado en dicho ordenador, configura el ordenador para:

> analizar, por medio de un analizador integrado en una aplicación que se ejecuta en dicho ordenador y que puede operar para transmitir mensajes de salida a dicha red y recibir mensajes de entrada de dicha red, dichos mensajes de salida cuando se inicia la transmisión del mensaje de salida para determinar, en unión con dichas reglas de dichos datos de política, uno o más detalles completados de dicho mensaje de salida; y
>
> redirigir selectivamente el mensaje de salida a una tercera parte en lugar del receptor previsto originalmente en dependencia de dicho uno o más detalles.

48. El producto de software informático de la reivindicación 47, donde el código de programa puede operar para redirigir el mensaje de salida a dicha tercera parte si el mensaje ha de ser enviado a uno o más de una lista predeterminada de receptores o direcciones.

49. El producto de software informático de la reivindicación 47 o 48, donde dichos datos de política incluyen una lista de nombres de empleados de compañía que pueden usar dicha aplicación para enviar mensajes de salida de y recibir mensajes de entrada en una dirección de la compañía, y donde el código de programa puede operar para redirigir el mensaje de salida de cualquiera de dichos empleados a dicha tercera parte, si determina que la dirección de la compañía del mensaje de salida contiene uno de una lista predeterminada de nombres de dominio, y si la dirección prevista incluye al menos uno del apellido, primeros nombres, o iniciales de un empleado en dicha lista de nombres.

50. El producto de software informático de cualquiera de las reivindicaciones 47 a 49, donde el código de programa puede operar para redirigir el mensaje de salida a dicha tercera parte si el mensaje contiene una o más palabras clave predeterminadas o combinación de palabras clave.

51. El producto de software informático de cualquiera de las reivindicaciones 47 a 50, donde el código de programa puede operar para redirigir el mensaje de salida a dicha tercera parte si el mensaje o anexos al mensaje han de ser encriptados antes de la transmisión.

52. El producto de software informático de la reivindicación 51 donde el código de programa puede operar para redirigir el mensaje con su clave original encriptada a la tercera parte, y donde se han previsto medios en el mensaje redirigido recibido por la tercera parte para que la tercera parte apruebe el mensaje para transmisión al receptor previsto originalmente y reencripte el mensaje con la clave original.

53. El producto de software informático de la reivindicación 52, donde el código de programa puede operar para añadir texto al mensaje antes de que sea redirigido indicando que es un mensaje redirigido.

54. El producto de software informático de cualquiera de las reivindicaciones 47 a 53, donde el código de programa puede operar para redirigir el mensaje de salida a dicha tercera parte si el mensaje contiene anexos, o tipos particulares de anexos.

55. El producto de software informático de cualquiera de las reivindicaciones 47 a 54, donde el código de programa puede operar para redirigir el mensaje de salida a dicha tercera parte si el mensaje contiene anexos y si el cuerpo o el asunto del mensaje contiene menos de una cantidad predeterminada de texto.

56. El producto de software informático de cualquiera de las reivindicaciones 47 a 55, donde el código de programa puede operar para redirigir el mensaje de salida a dicha tercera parte en dependencia de la identidad del autor del mensaje.

57. El producto de software informático de cualquiera de las reivindicaciones 47 a 56, donde se han previsto medios en el mensaje redirigido recibido por la tercera parte para que la tercera parte apruebe el mensaje para transmisión al receptor previsto originalmente.

58. El producto de programa informático de cualquiera de las reivindicaciones 47 a 57, donde dicha aplicación es un navegador web.

59. El producto de programa informático de la reivindicación 58, donde dicho código de programa cuando es ejecutado en dicho ordenador es un módulo plug-in (70, 72) de dicho navegador web.

60. El producto de programa informático de la reivindicación 59, donde dicho navegador web es Internet Explorer de Microsoft y dicho módulo plug-in es un Browser Helper Object.

61. El producto de programa informático de cualquiera de las reivindicaciones 47 a 57, donde dicha aplicación es un cliente de correo electrónico.

62. El producto de programa informático de la reivindicación 61, donde dicho código de programa cuando es ejecutado en dicho ordenador es un módulo plug-in (74) de dicho cliente de correo electrónico.

63. El producto de programa informático de la reivindicación 62, donde dicho cliente de correo electrónico es cliente de correo electrónico Outlook de Microsoft y dicho módulo plug-in es una extensión de cliente de Exchange de Microsoft.

64. El producto de software informático de cualquiera de las reivindicaciones 47 a 57, donde dicha aplicación es una aplicación de mensajería instantánea.

65. El producto de software informático de la reivindicación 64, donde dicho código de programa cuando es ejecutado en dicho ordenador es un módulo plug-in de dicha aplicación de mensajería instantánea.

66. El producto de software informático de cualquiera de las reivindicaciones 47 a 57, donde dicha aplicación es una aplicación de mensajes de voz.

67. El producto de software informático de la reivindicación 66, donde dicho código de programa cuando es ejecutado en dicho ordenador es un módulo plug-in de dicha aplicación de mensajes de voz.

68. El producto de software informático de cualquiera de las reivindicaciones 47 a 67, donde los datos de política definen una o más políticas para usuarios individuales o grupos de usuarios de las estaciones de trabajo.

69. El producto de software informático de cualquiera de las reivindicaciones 47 a 68, donde los datos de política están almacenados en un servidor central.

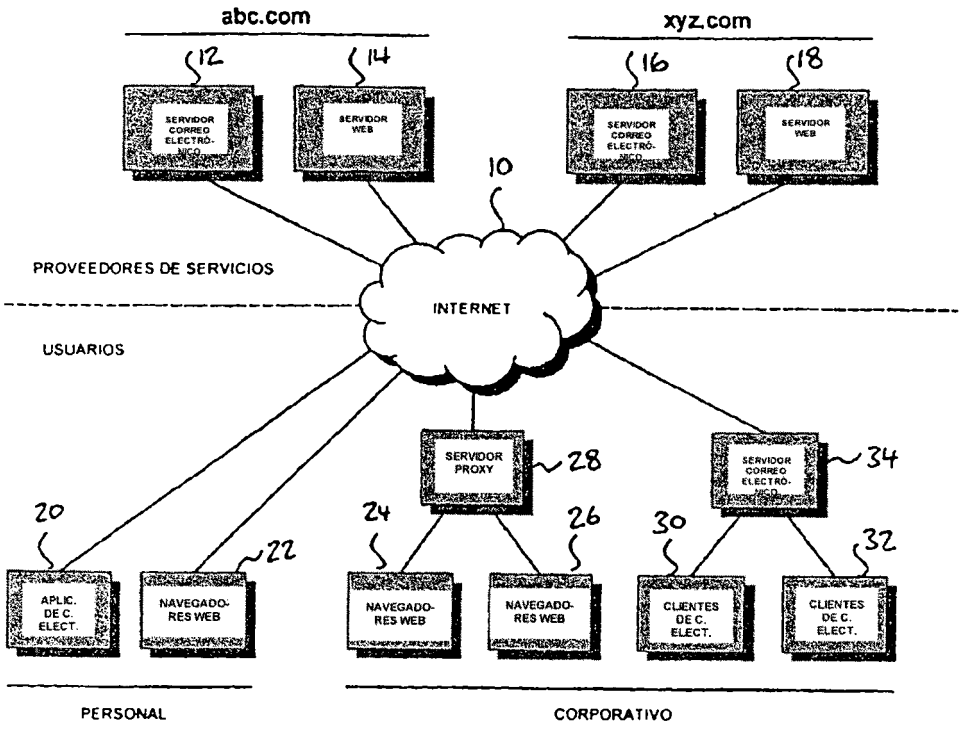
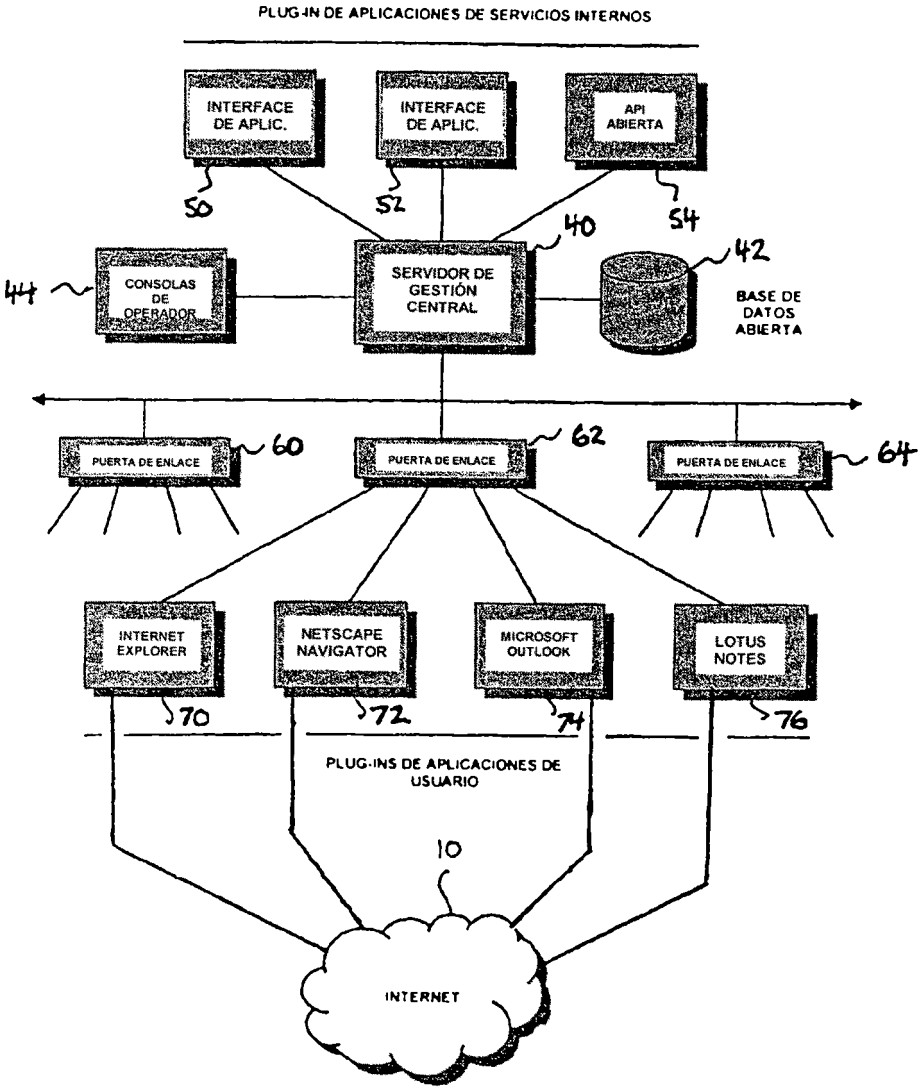

abc.com
xyz.com
12
14
16
18
SERVIDOR CORREO ELECTRÓNICO
SERVIDOR WEB
SERVIDOR CORREO ELECTRÓNICO
SERVIDOR WEB
10
PROVEEDORES DE SERVICIOS
INTERNET
USUARIOS
SERVIDOR PROXY
28
SERVIDOR CORREO ELECTRÓNICO
34
20
24
26
30
32
22
APLIC. DE C. ELECT.
NAVEGADORES WEB
NAVEGADORES WEB
NAVEGADORES WEB
CLIENTES DE C. ELECT.
CLIENTES DE C. ELECT.
PERSONAL
CORPORATIVO

Fig. 1

Fig. 2


PLUG-IN DE APLICACIONES DE SERVICIOS INTERNOS
INTERFACE DE APLIC.
INTERFACE DE APLIC.
API ABIERTA
50
52
54
40
42
44
CONSOLAS DE OPERADOR
SERVIDOR DE GESTIÓN CENTRAL
BASE DE DATOS ABIERTA
PUERTA DE ENLACE
60
PUERTA DE ENLACE
62
PUERTA DE ENLACE
64
INTERNET EXPLORER
NETSCAPE NAVIGATOR
MICROSOFT OUTLOOK
LOTUS NOTES
70
72
74
76
PLUG-INS DE APLICACIONES DE USUARIO
10
INTERNET

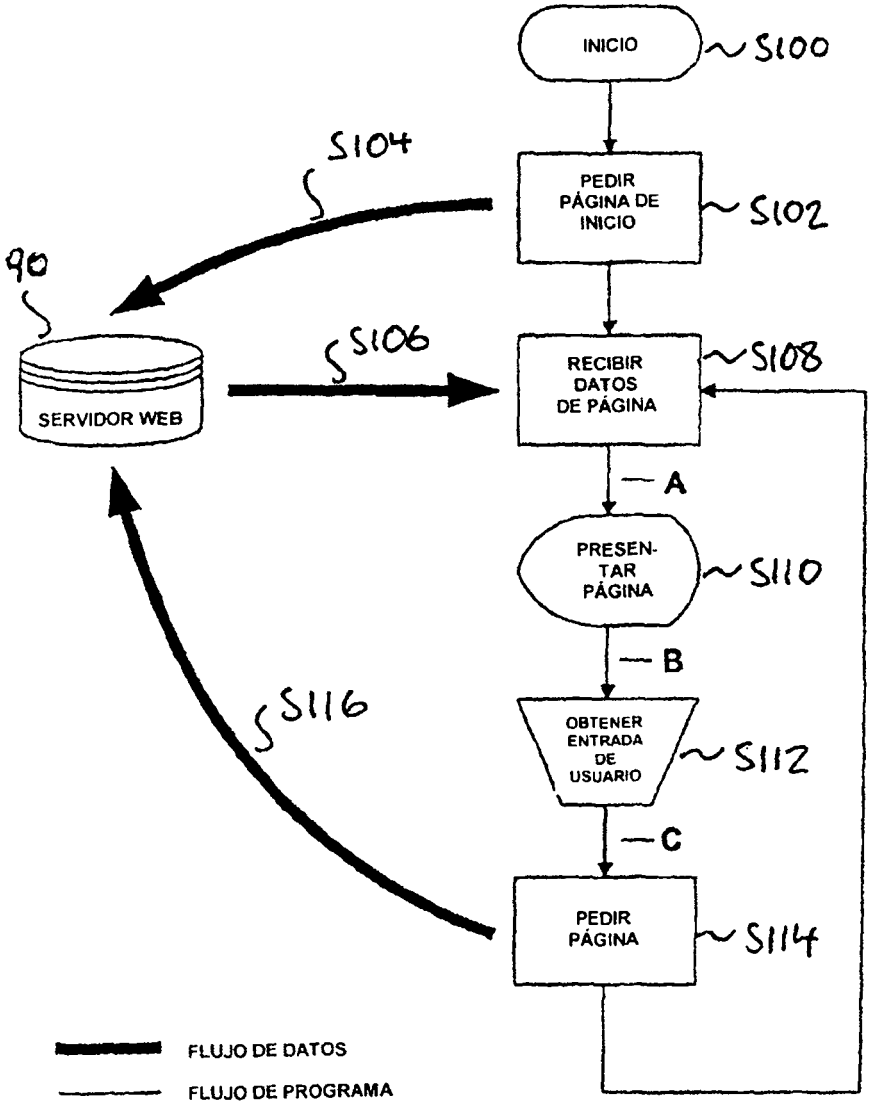

INICIO
S100
PEDIR PÁGINA DE INICIO
S102
S104
90
SERVIDOR WEB
S106
RECIBIR DATOS DE PÁGINA
S108
A
PRESEN-TAR PÁGINA
S110
B
OBTENER ENTRADA DE USUARIO
S112
C
PEDIR PÁGINA
S114
S116
FLUJO DE DATOS
FLUJO DE PROGRAMA

Fig. 3

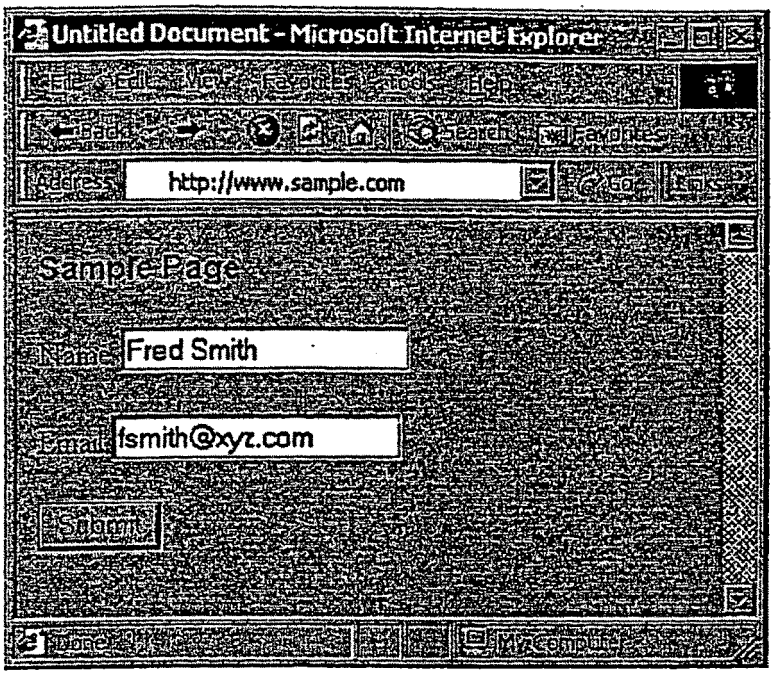

Untitled Document - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.sample.com
Go Links
Sample Page
Name: Fred Smith
Email: fsmith@xyz.com
Submit
Done
My Computer

Fig. 4

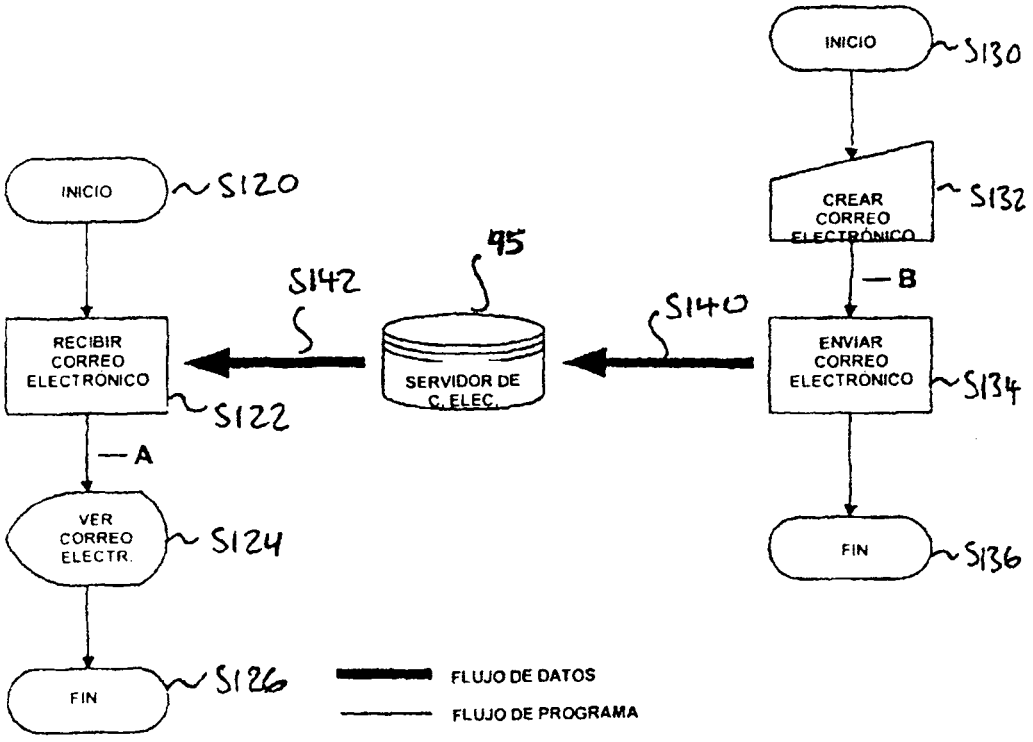

INICIO
S130
CREAR CORREO ELECTRÓNICO
S132
B
ENVIAR CORREO ELECTRÓNICO
S134
FIN
S136
S140
95
SERVIDOR DE C. ELEC.
S142
INICIO
S120
RECIBIR CORREO ELECTRÓNICO
S122
A
VER CORREO ELECTR.
S124
FIN
S126
FLUJO DE DATOS
FLUJO DE PROGRAMA

Fig. 5

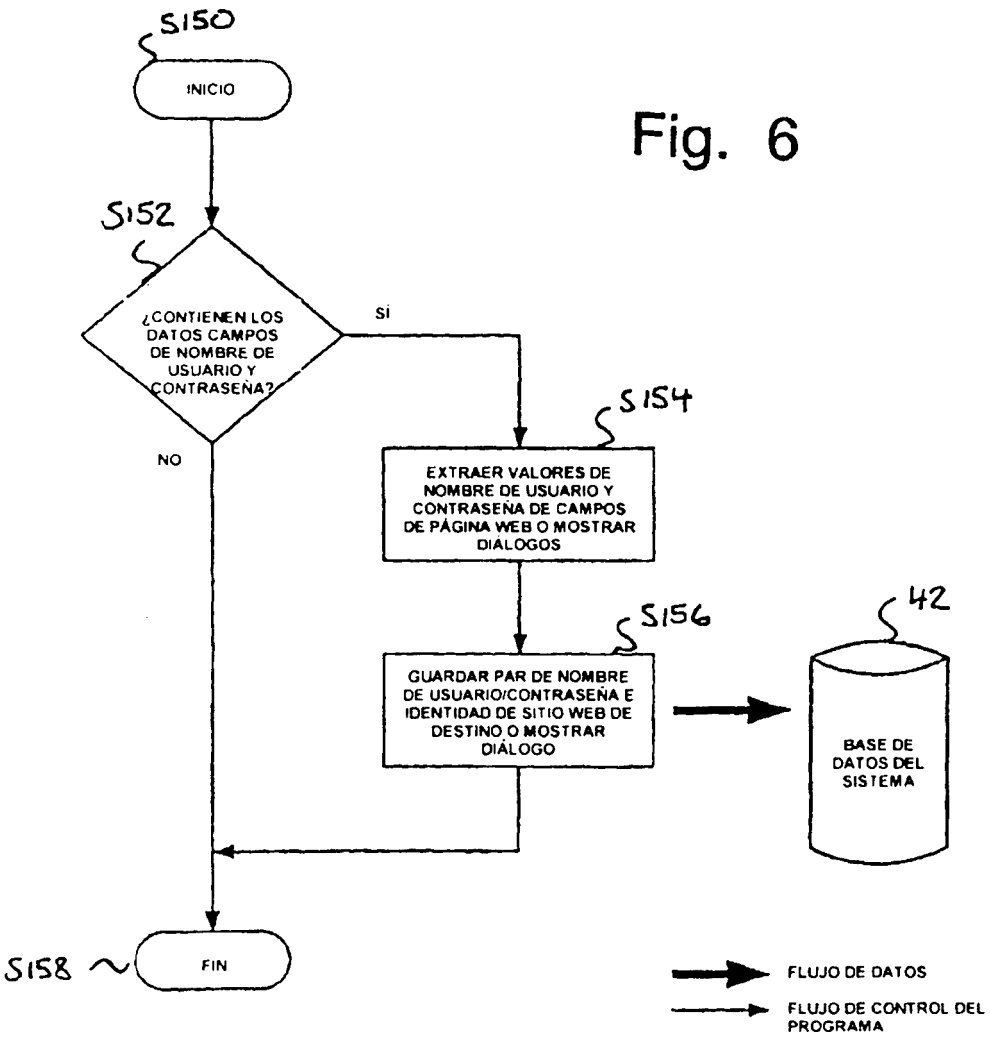

S150
INICIO
S152
¿CONTIENEN LOS DATOS CAMPOS DE NOMBRE DE USUARIO Y CONTRASEÑA?
SÍ
NO
S154
EXTRAER VALORES DE NOMBRE DE USUARIO Y CONTRASEÑA DE CAMPOS DE PÁGINA WEB O MOSTRAR DIÁLOGOS
S156
GUARDAR PAR DE NOMBRE DE USUARIO/CONTRASEÑA E IDENTIDAD DE SITIO WEB DE DESTINO O MOSTRAR DIÁLOGO
42
BASE DE DATOS DEL SISTEMA
S158
FIN
FLUJO DE DATOS
FLUJO DE CONTROL DEL PROGRAMA

Fig. 6

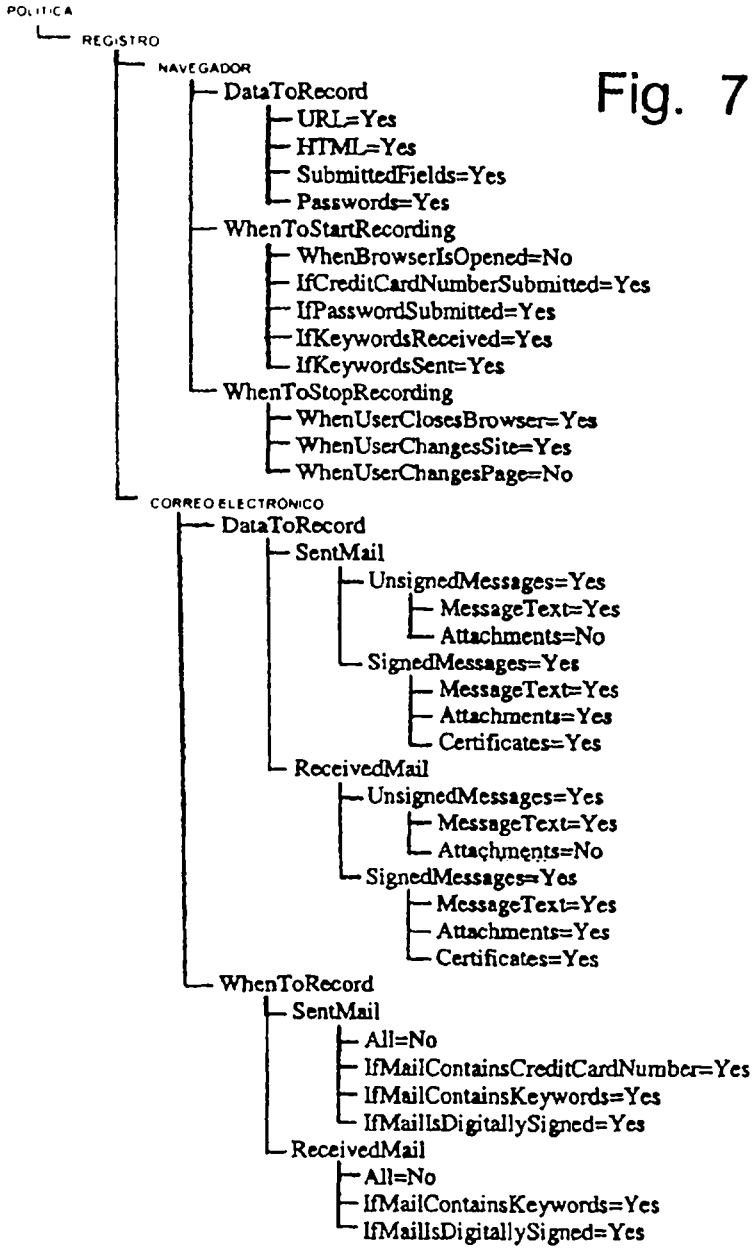

POLITICA
REGISTRO
NAVEGADOR
DataToRecord
URL=Yes
HTML=Yes
SubmittedFields=Yes
Passwords=Yes
WhenToStartRecording
WhenBrowserIsOpened=No
IfCreditCardNumberSubmitted=Yes
IfPasswordSubmitted=Yes
IfKeywordsReceived=Yes
IfKeywordsSent=Yes
WhenToStopRecording
WhenUserClosesBrowser=Yes
WhenUserChangesSite=Yes
WhenUserChangesPage=No
CORREO ELECTRONICO
DataToRecord
SentMail
UnsignedMessages=Yes
MessageText=Yes
Attachments=No
SignedMessages=Yes
MessageText=Yes
Attachments=Yes
Certificates=Yes
ReceivedMail
UnsignedMessages=Yes
MessageText=Yes
Attachments=No
SignedMessages=Yes
MessageText=Yes
Attachments=Yes
Certificates=Yes
WhenToRecord
SentMail
All=No
IfMailContainsCreditCardNumber=Yes
IfMailContainsKeywords=Yes
IfMailIsDigitallySigned=Yes
ReceivedMail
All=No
IfMailContainsKeywords=Yes
IfMailIsDigitallySigned=Yes

Fig. 7

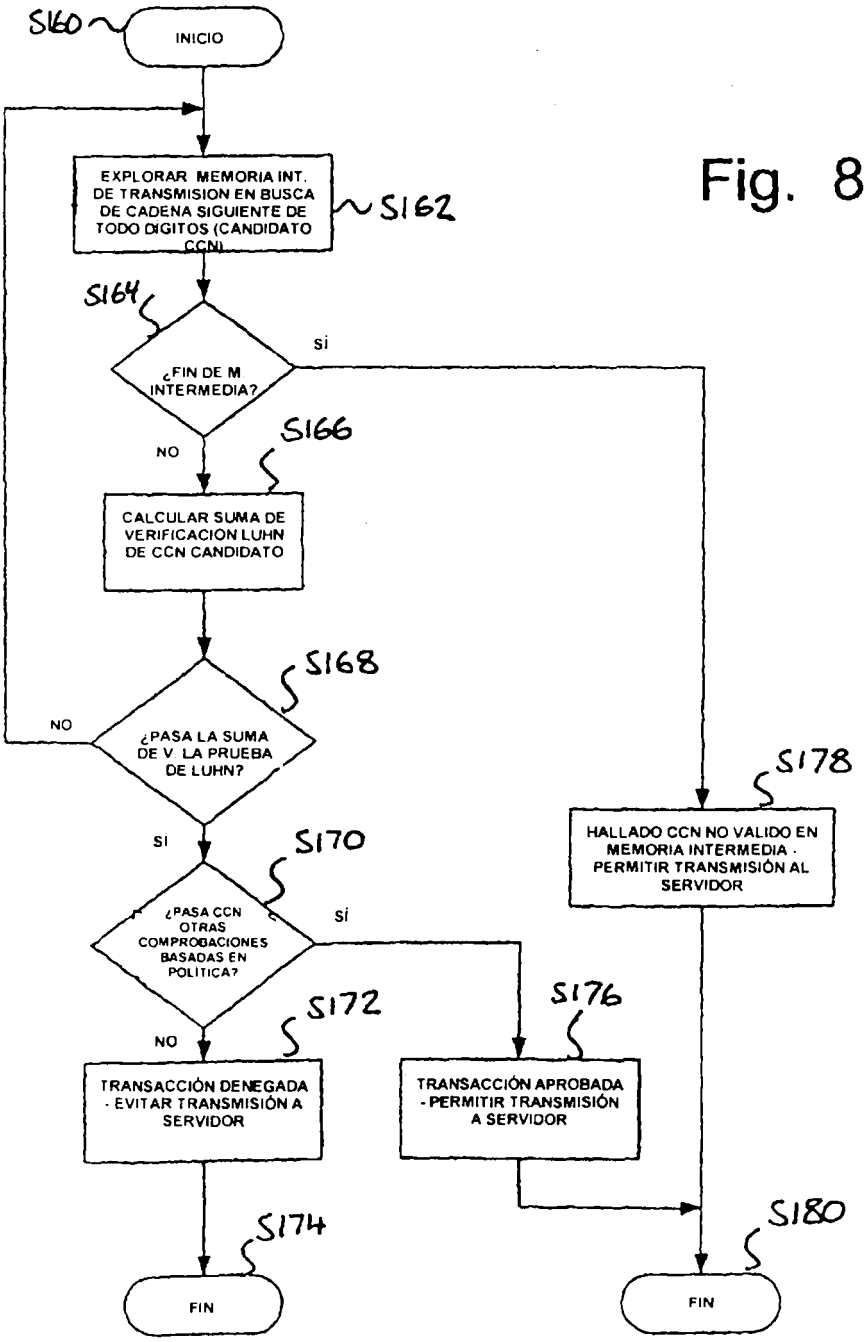

S160
INICIO
EXPLORAR MEMORIA INT. DE TRANSMISION EN BUSCA DE CADENA SIGUIENTE DE TODO DIGITOS (CANDIDATO CCN)
S162
S164
¿FIN DE M INTERMEDIA?
SÍ
NO
S166
CALCULAR SUMA DE VERIFICACION LUHN DE CCN CANDIDATO
S168
¿PASA LA SUMA DE V LA PRUEBA DE LUHN?
NO
SI
S170
¿PASA CCN OTRAS COMPROBACIONES BASADAS EN POLITICA?
SÍ
NO
S172
TRANSACCIÓN DENEGADA - EVITAR TRANSMISIÓN A SERVIDOR
S174
FIN
S176
TRANSACCIÓN APROBADA - PERMITIR TRANSMISIÓN A SERVIDOR
S178
HALLADO CCN NO VALIDO EN MEMORIA INTERMEDIA - PERMITIR TRANSMISIÓN AL SERVIDOR
S180
FIN

Fig. 8

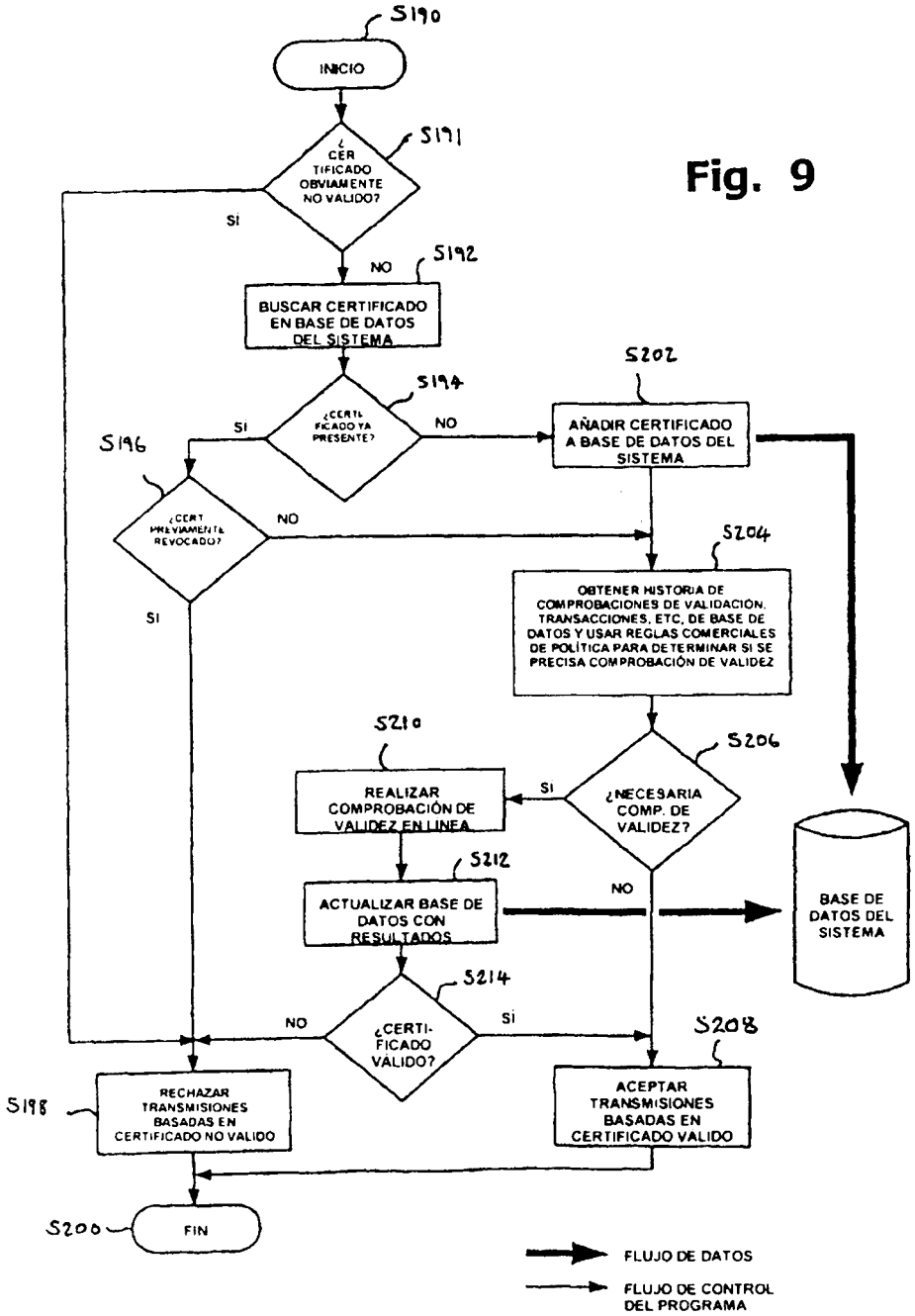

S190
INICIO
S191
¿CERTIFICADO OBVIAMENTE NO VALIDO?
SI
NO
S192
BUSCAR CERTIFICADO EN BASE DE DATOS DEL SISTEMA
S194
¿CERTIFICADO YA PRESENTE?
SI
NO
S196
¿CERT. PREVIAMENTE REVOCADO?
NO
SI
S202
AÑADIR CERTIFICADO A BASE DE DATOS DEL SISTEMA
S204
OBTENER HISTORIA DE COMPROBACIONES DE VALIDACIÓN, TRANSACCIONES, ETC. DE BASE DE DATOS Y USAR REGLAS COMERCIALES DE POLÍTICA PARA DETERMINAR SI SE PRECISA COMPROBACIÓN DE VALIDEZ
S206
¿NECESARIA COMP. DE VALIDEZ?
SI
NO
S210
REALIZAR COMPROBACIÓN DE VALIDEZ EN LINEA
S212
ACTUALIZAR BASE DE DATOS CON RESULTADOS
S214
¿CERTIFICADO VALIDO?
NO
SI
S208
ACEPTAR TRANSMISIONES BASADAS EN CERTIFICADO VALIDO
S198
RECHAZAR TRANSMISIONES BASADAS EN CERTIFICADO NO VALIDO
S200
FIN
BASE DE DATOS DEL SISTEMA
FLUJO DE DATOS
FLUJO DE CONTROL DEL PROGRAMA

Fig. 9

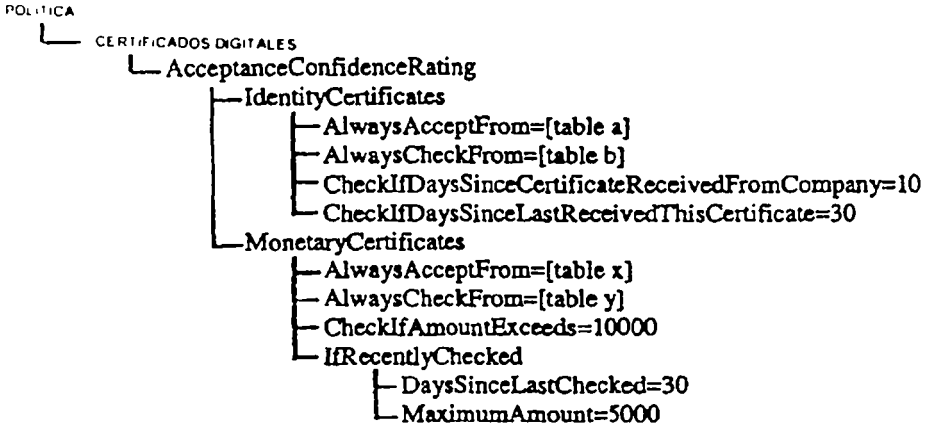
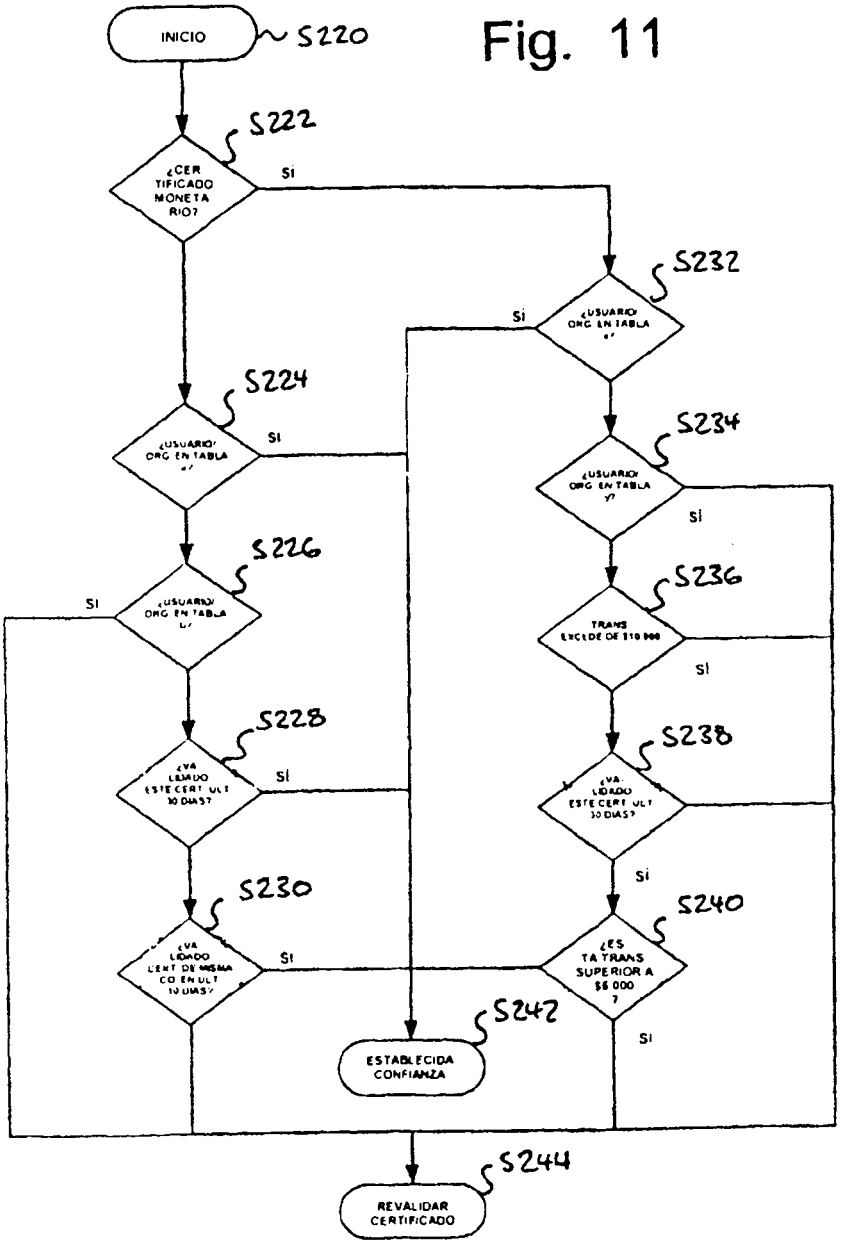

POLÍTICA
CERTIFICADOS DIGITALES
AcceptanceConfidenceRating
IdentityCertificates
AlwaysAcceptFrom=[table a]
AlwaysCheckFrom=[table b]
CheckIfDaysSinceCertificateReceivedFromCompany=10
CheckIfDaysSinceLastReceivedThisCertificate=30
MonetaryCertificates
AlwaysAcceptFrom=[table x]
AlwaysCheckFrom=[table y]
CheckIfAmountExceeds=10000
IfRecentlyChecked
DaysSinceLastChecked=30
MaximumAmount=5000

Fig. 10

Fig. 11


INICIO
S220
S222
¿CERTIFICADO MONETARIO?
Si
S224
¿USUARIO ORG EN TABLA
Si
S226
¿USUARIO ORG EN TABLA
Si
S228
¿VA LEIDO ESTE CERT ULT 10 DIAS?
Si
S230
¿VA LEIDO CERT DE MISMA CO EN ULT 10 DIAS?
Si
S232
¿USUARIO ORG EN TABLA
Si
S234
¿USUARIO ORG EN TABLA
Si
S236
TRANS EXCEDE DE $10 000
Si
S238
¿VA LEIDO ESTE CERT ULT 10 DIAS?
Si
S240
¿ES TA TRANS SUPERIOR A $5 000 ?
Si
S242
ESTABLECIDA CONFIANZA
S244
REVALIDAR CERTIFICADO

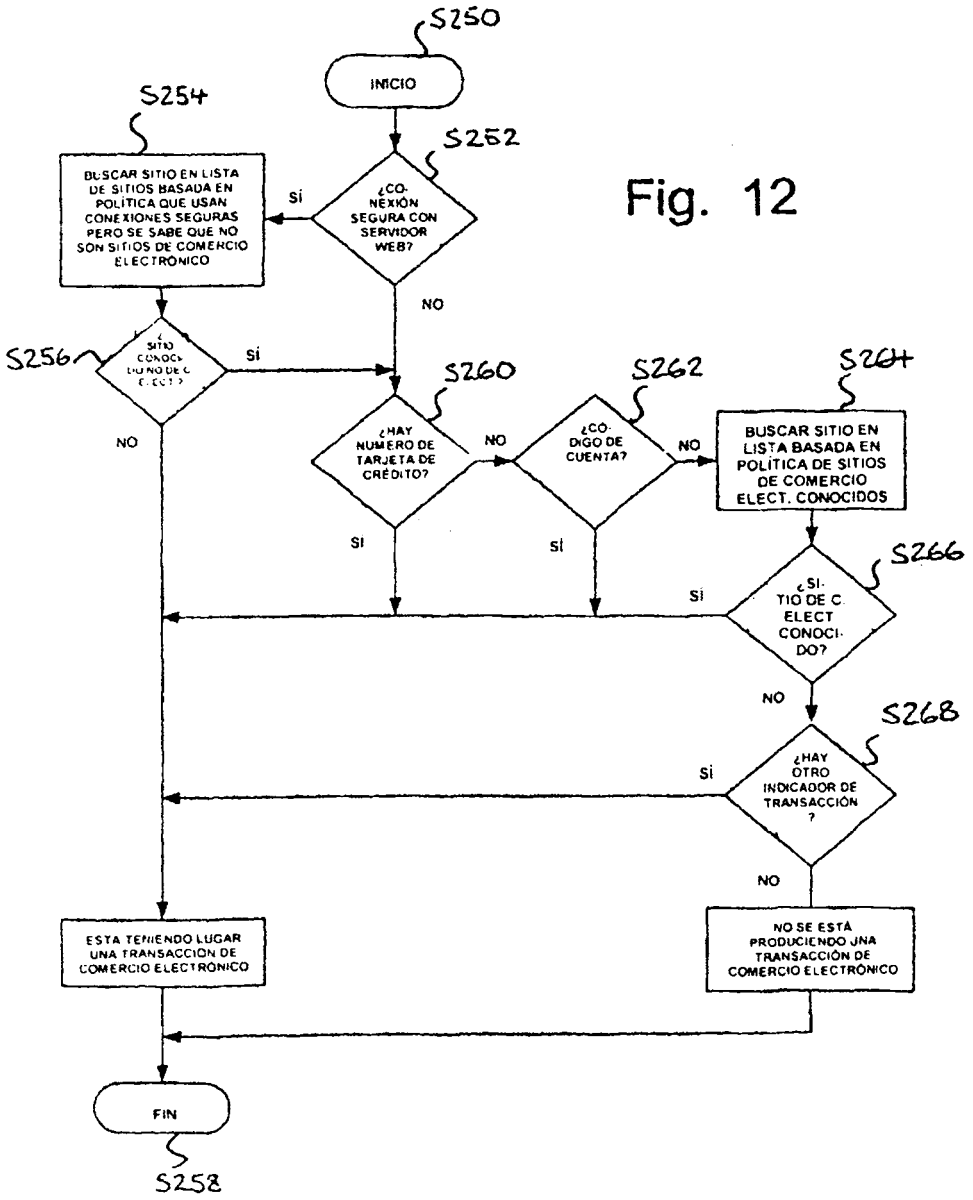

S250
INICIO
S252
¿CONEXIÓN SEGURA CON SERVIDOR WEB?
SÍ
S254
BUSCAR SITIO EN LISTA DE SITIOS BASADA EN POLÍTICA QUE USAN CONEXIONES SEGURAS PERO SE SABE QUE NO SON SITIOS DE COMERCIO ELECTRÓNICO
NO
S256
¿SITIO CONOCIDO DE C. ELECT.?
SÍ
NO
S260
¿HAY NÚMERO DE TARJETA DE CRÉDITO?
NO
SÍ
S262
¿CÓDIGO DE CUENTA?
NO
SÍ
S264
BUSCAR SITIO EN LISTA BASADA EN POLÍTICA DE SITIOS DE COMERCIO ELECT. CONOCIDOS
S266
¿SITIO DE C. ELECT CONOCIDO?
SÍ
NO
S268
¿HAY OTRO INDICADOR DE TRANSACCIÓN ?
SÍ
NO
ESTÁ TENIENDO LUGAR UNA TRANSACCIÓN DE COMERCIO ELECTRÓNICO
NO SE ESTÁ PRODUCIENDO UNA TRANSACCIÓN DE COMERCIO ELECTRÓNICO
FIN
S258

Fig. 12

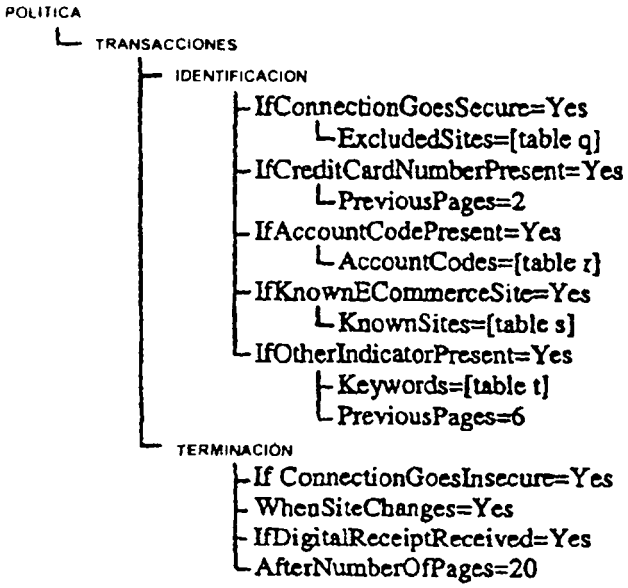


TABLA q: SITIOS EXCLUIDOS
www.hotmail.com
www.passport.com
ibankon.barclays.co.uk
www.nwolb.co.uk

TABLA r: CODIGOS DE CUENTA	
Código de cuenta	Páginas anteriores a registrar
21321234	2
ORCH01	6
58734	1
PETER304	0

TABLA s: SITIOS DE C. EL. CONOCIDOS
ecomm.us.dell.com/dellstore
buy.supersaver.co.uk
www.booksforall.com/basket

TABLA t: PALABRAS CLAVE
"receipt"
"thank you for your order"
"order confirmation"

Fig. 13

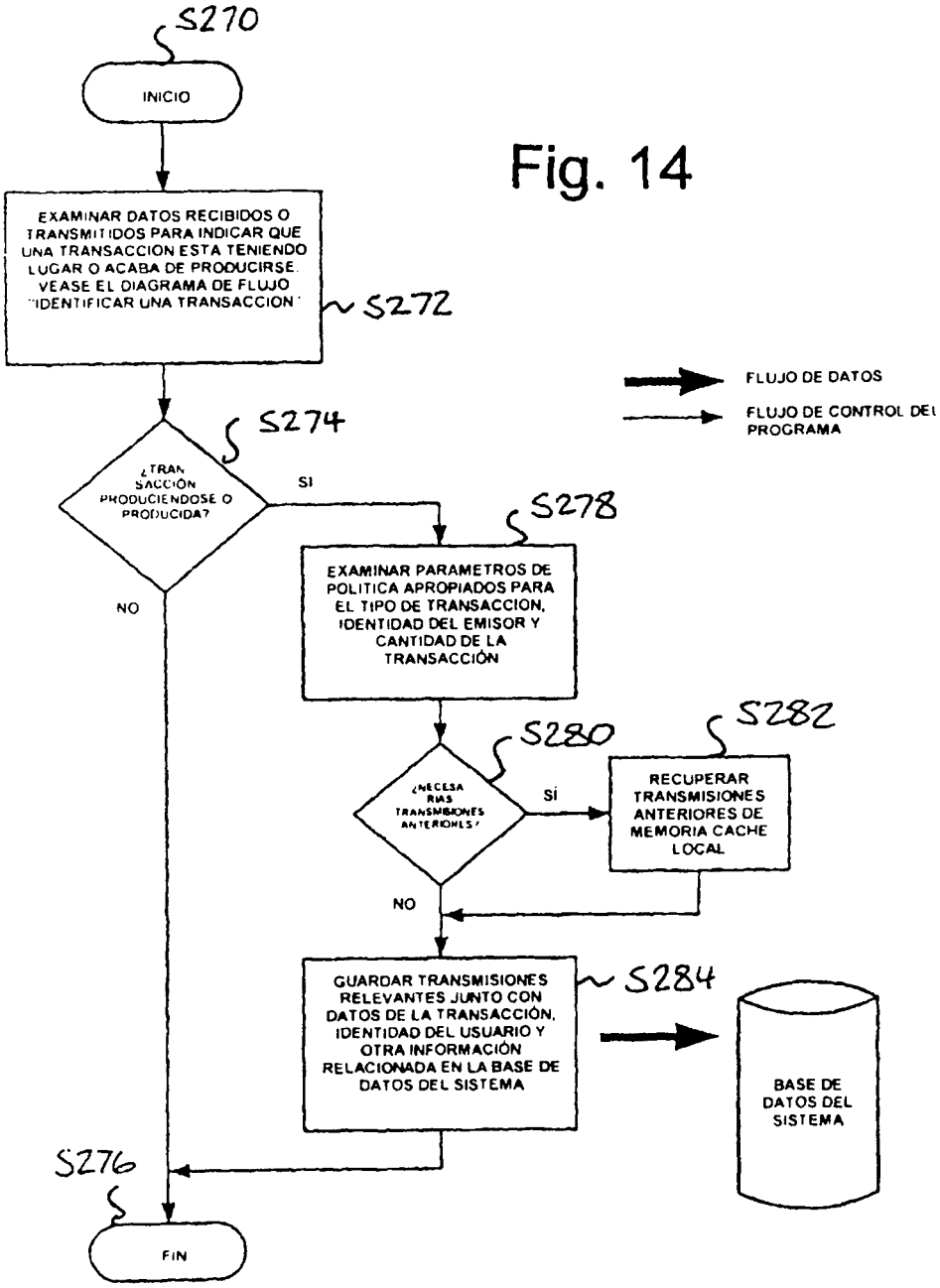
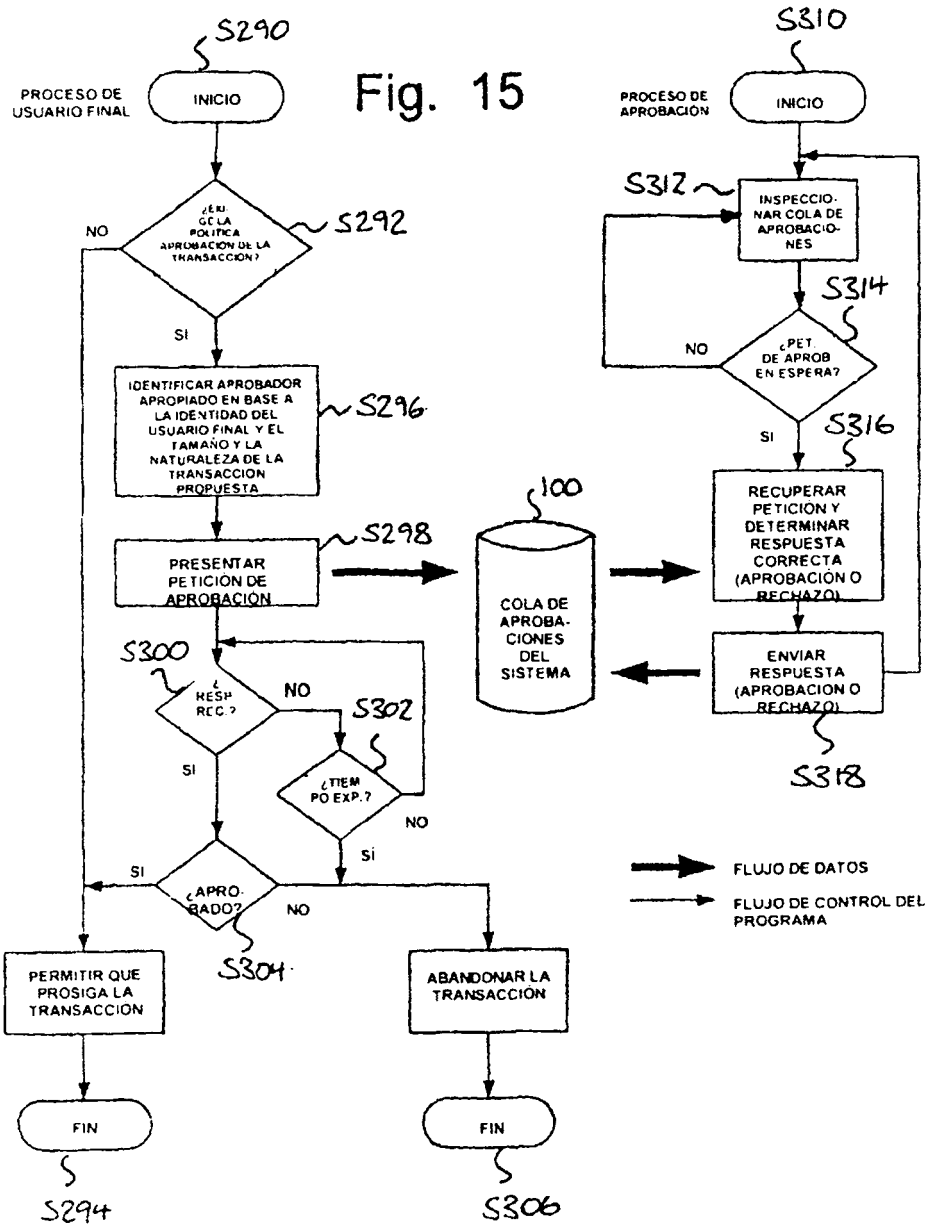

S270
INICIO
EXAMINAR DATOS RECIBIDOS O TRANSMITIDOS PARA INDICAR QUE UNA TRANSACCION ESTA TENIENDO LUGAR O ACABA DE PRODUCIRSE. VEASE EL DIAGRAMA DE FLUJO "IDENTIFICAR UNA TRANSACCION"
S272
FLUJO DE DATOS
FLUJO DE CONTROL DEL PROGRAMA
S274
¿TRANSACCIÓN PRODUCIENDOSE O PRODUCIDA?
SI
NO
S278
EXAMINAR PARAMETROS DE POLITICA APROPIADOS PARA EL TIPO DE TRANSACCION, IDENTIDAD DEL EMISOR Y CANTIDAD DE LA TRANSACCIÓN
S280
¿NECESARIAS TRANSMISIONES ANTERIORES?
SÍ
S282
RECUPERAR TRANSMISIONES ANTERIORES DE MEMORIA CACHE LOCAL
NO
GUARDAR TRANSMISIONES RELEVANTES JUNTO CON DATOS DE LA TRANSACCIÓN, IDENTIDAD DEL USUARIO Y OTRA INFORMACIÓN RELACIONADA EN LA BASE DE DATOS DEL SISTEMA
S284
BASE DE DATOS DEL SISTEMA
S276
FIN

Fig. 14

Fig. 15


S290
PROCESO DE USUARIO FINAL
INICIO
¿EXISTE LA POLITICA APROBACION DE LA TRANSACCION?
S292
NO
SI
IDENTIFICAR APROBADOR APROPIADO EN BASE A LA IDENTIDAD DEL USUARIO FINAL Y EL TAMAÑO Y LA NATURALEZA DE LA TRANSACCION PROPUESTA
S296
PRESENTAR PETICION DE APROBACION
S298
S300
¿RESP REC.?
NO
SI
S302
¿TIEMPO EXP.?
NO
SI
¿APROBADO?
SI
NO
S304
PERMITIR QUE PROSIGA LA TRANSACCION
ABANDONAR LA TRANSACCION
FIN
S294
FIN
S306
100
COLA DE APROBACIONES DEL SISTEMA
S310
PROCESO DE APROBACION
INICIO
S312
INSPECCIONAR COLA DE APROBACIONES
S314
¿PET. DE APROB EN ESPERA?
NO
SI
S316
RECUPERAR PETICION Y DETERMINAR RESPUESTA CORRECTA (APROBACION O RECHAZO)
ENVIAR RESPUESTA (APROBACION O RECHAZO)
S318
FLUJO DE DATOS
FLUJO DE CONTROL DEL PROGRAMA

POLÍTICA
- TransactionApproval
  - MaximumUnapprovedTransactionAmount = 500
  - MaximumUnapprovedMonthlyAmount = 2500
  - ExcludedSites = [table e]
  - Approvers = [table f]

TABLA f: APROBADORES		
NOMBRE	LÍMITE	SITIOS EXCLUIDOS
F Smith	$500	www.dell.com
R Jones	$1000	www.dell.com; www.officemax.com
F Healy	ILIMITADO	NINGUNO

Fig. 16

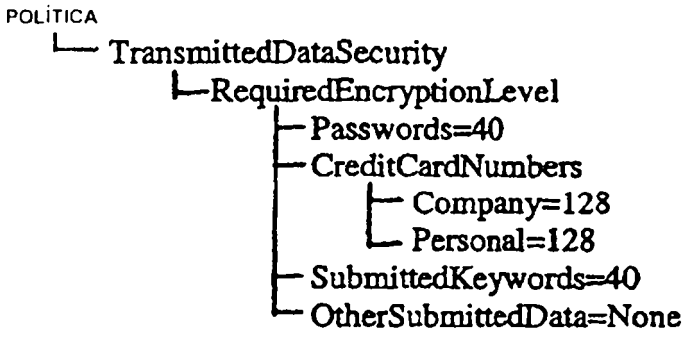
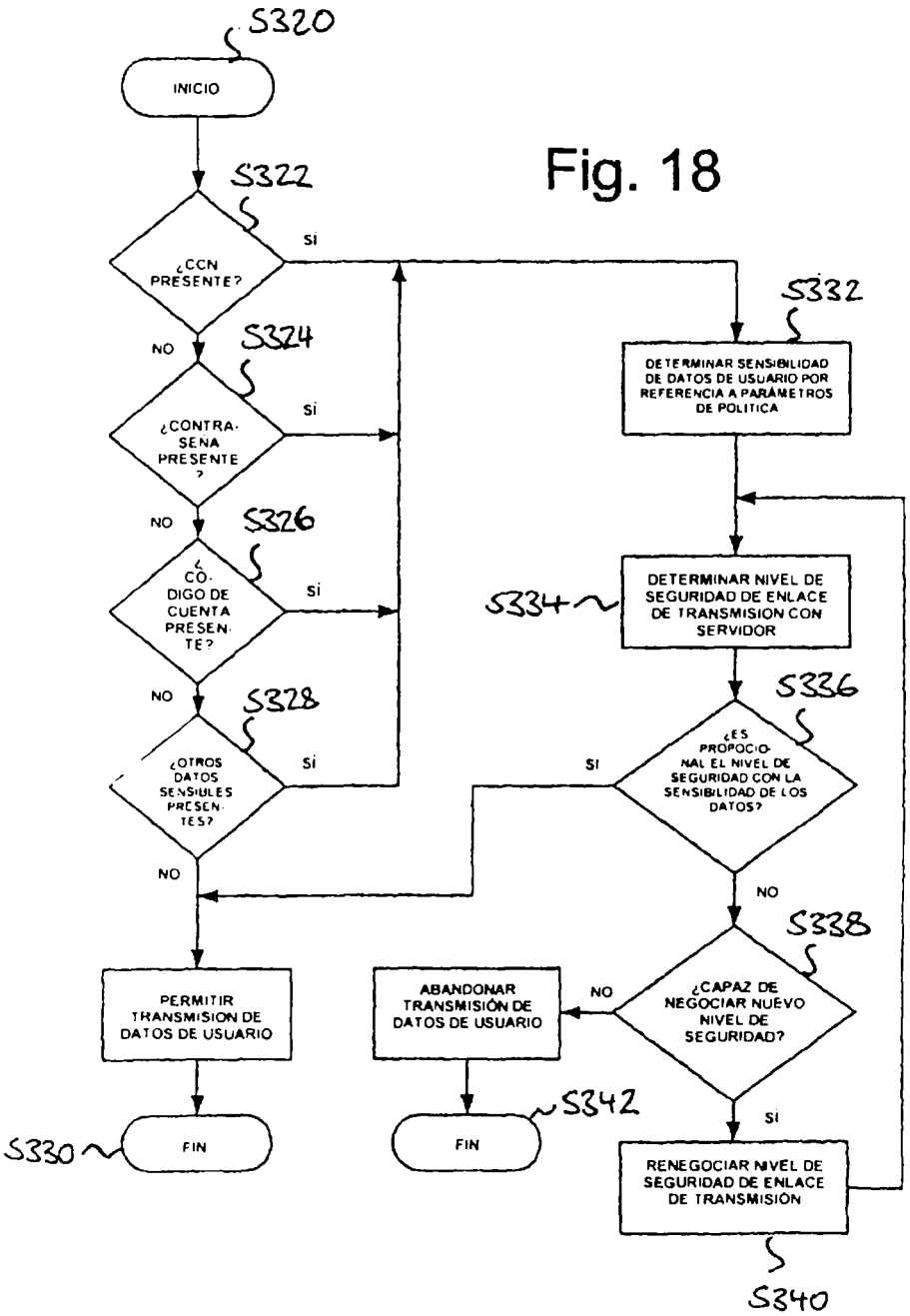
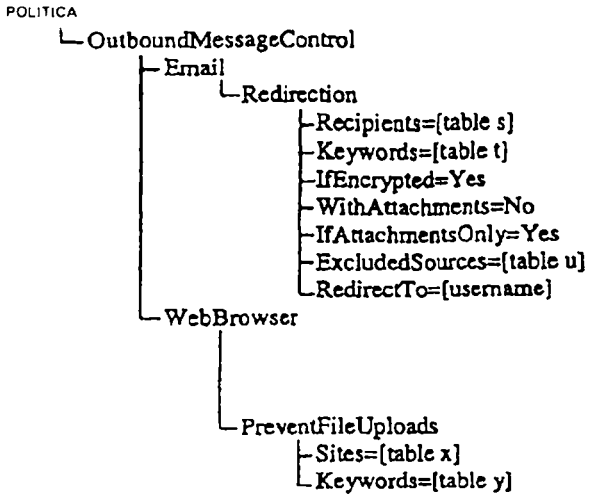

POLÍTICA
TransmittedDataSecurity
RequiredEncryptionLevel
Passwords=40
CreditCardNumbers
Company=128
Personal=128
SubmittedKeywords=40
OtherSubmittedData=None

Fig. 17

Fig. 18


S320
INICIO
S322
¿CCN PRESENTE?
SI
NO
S324
¿CONTRASEÑA PRESENTE?
SI
NO
S326
¿CÓDIGO DE CUENTA PRESENTE?
SI
NO
S328
¿OTROS DATOS SENSIBLES PRESENTES?
SI
NO
PERMITIR TRANSMISION DE DATOS DE USUARIO
S330
FIN
S332
DETERMINAR SENSIBILIDAD DE DATOS DE USUARIO POR REFERENCIA A PARÁMETROS DE POLITICA
S334
DETERMINAR NIVEL DE SEGURIDAD DE ENLACE DE TRANSMISION CON SERVIDOR
S336
¿ES PROPORCIONAL EL NIVEL DE SEGURIDAD CON LA SENSIBILIDAD DE LOS DATOS?
SI
NO
S338
¿CAPAZ DE NEGOCIAR NUEVO NIVEL DE SEGURIDAD?
NO
ABANDONAR TRANSMISIÓN DE DATOS DE USUARIO
S342
FIN
SI
RENEGOCIAR NIVEL DE SEGURIDAD DE ENLACE DE TRANSMISIÓN
S340



EJEMPLO DE TABLA s
*@microsoft.com
fred.smith@xyz.com
jjones@hotmail.com

EJEMPLO DE TABLAS x
* @ hotmail.com
*@ aol.com
username

EJEMPLO DE TABLAS t, y
CONFIDENCIAL
SECRETO
CONTRATO
PRECIOS
PEDIDO
PROYECTO X

EJEMPLO DE TABLA u
A.N. Authoriseduser
T.H.E. Boss

Fig. 19

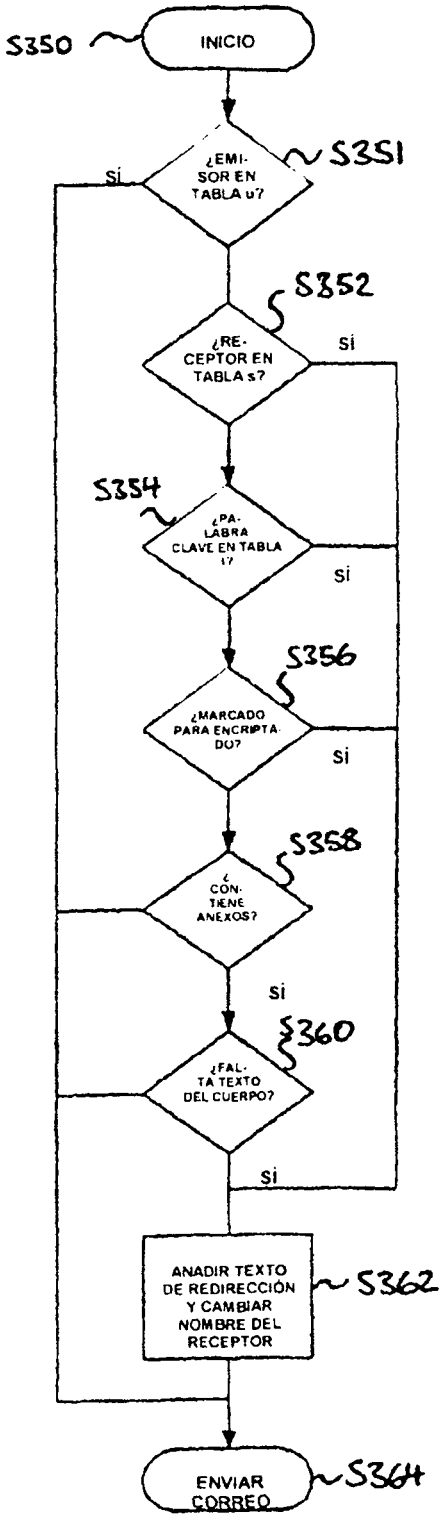

S350
INICIO
S351
¿EMISOR EN TABLA u?
Sí
S352
¿RECEPTOR EN TABLA s?
Sí
S354
¿PALABRA CLAVE EN TABLA t?
Sí
S356
¿MARCADO PARA ENCRIPTADO?
Sí
S358
¿CONTIENE ANEXOS?
Sí
S360
¿FALTA TEXTO DEL CUERPO?
Sí
ANADIR TEXTO DE REDIRECCIÓN Y CAMBIAR NOMBRE DEL RECEPTOR
S362
ENVIAR CORREO
S364

Fig. 20

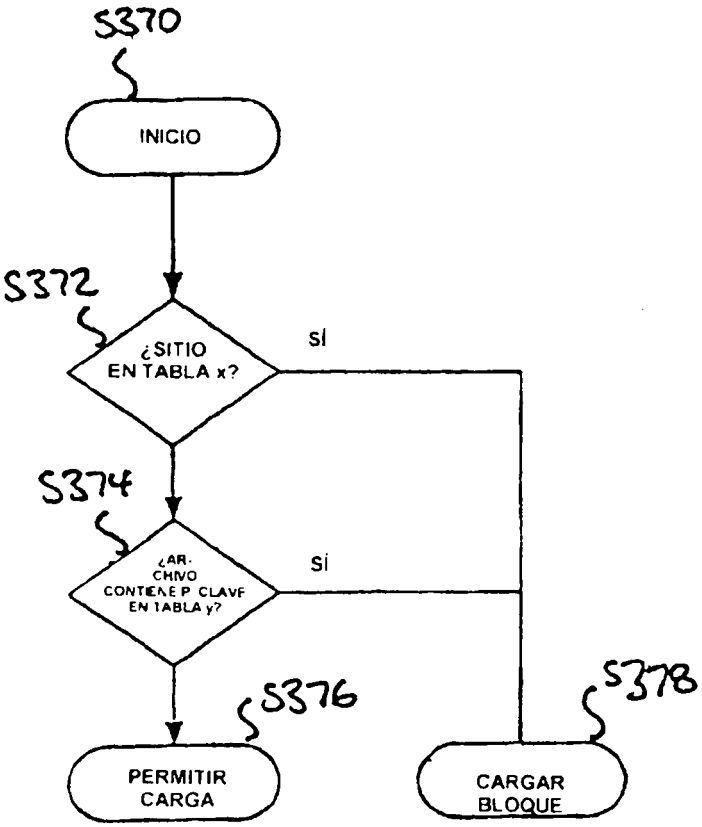

S370
INICIO
S372
¿SITIO EN TABLA x?
SÍ
S374
¿ARCHIVO CONTIENE P CLAVE EN TABLA y?
SÍ
S376
PERMITIR CARGA
S378
CARGAR BLOQUE

Fig. 21

POLÍTICA

- EmailForwarding
  - PreventAll=No
  - WarnAll=No
  - PreventExternal=No
  - WarnExternal=Yes
  - PreventKeywords=[table j]
  - PreventIfNotSentExternally=Yes
  - PreventIfSingleRecipient=Yes

EJEMPLO DE TABLAS j
CONFIDENCIAL
SECRETO
CONTRATO
PRECIOS
PEDIDO
PROYECTO X

Fig. 22

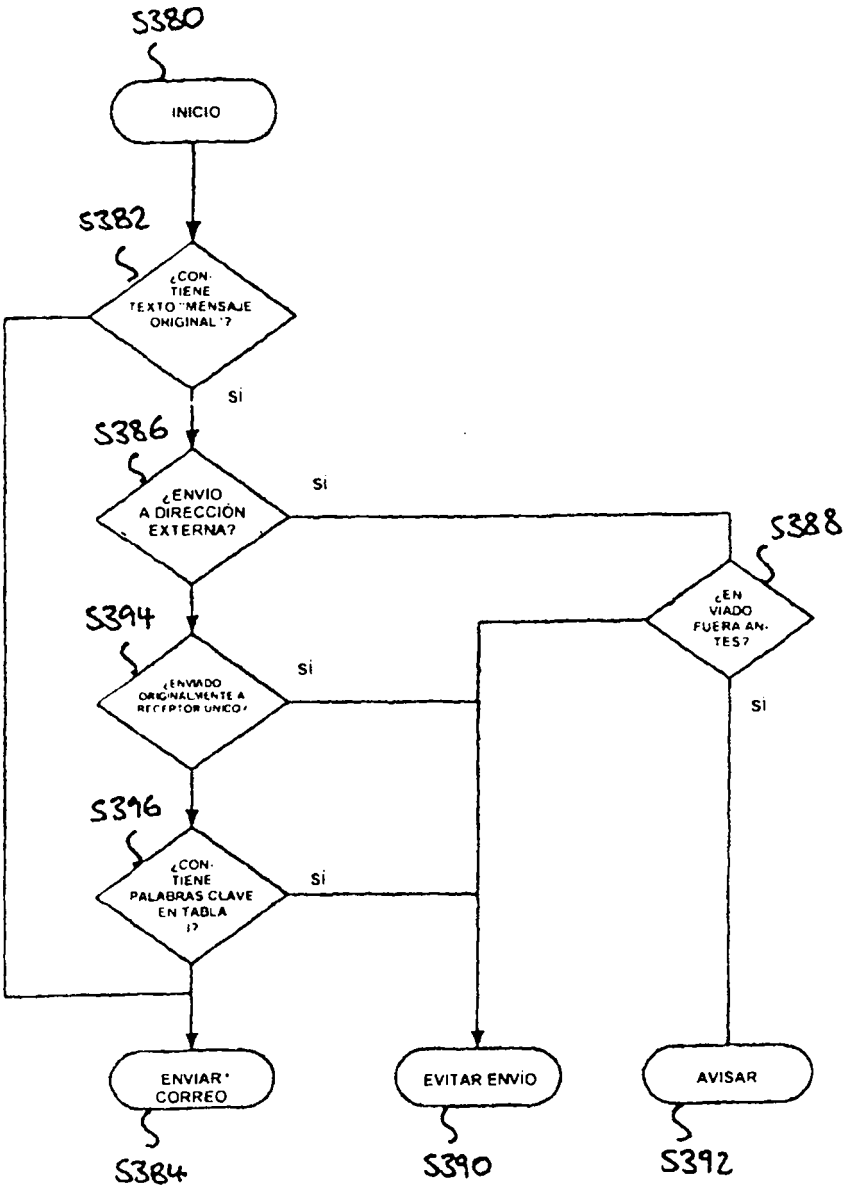
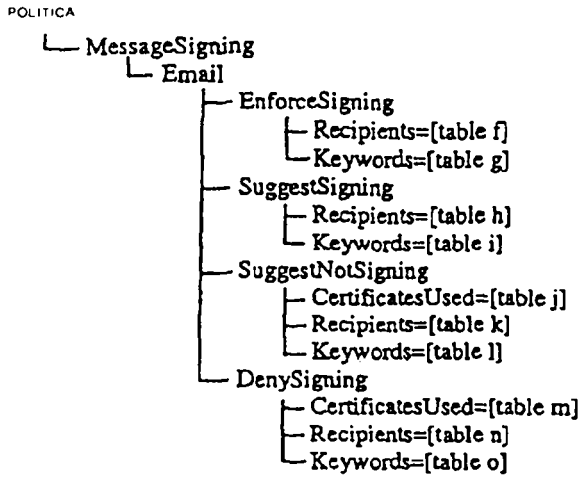

S380
INICIO
S382
¿CONTIENE TEXTO "MENSAJE ORIGINAL"?
SI
S386
¿ENVIO A DIRECCIÓN EXTERNA?
SI
S388
¿ENVIADO FUERA ANTES?
S394
¿ENVIADO ORIGINALMENTE A RECEPTOR UNICO?
SI
SI
S396
¿CONTIENE PALABRAS CLAVE EN TABLA ?
SI
ENVIAR CORREO
S384
EVITAR ENVIO
S390
AVISAR
S392

Fig. 23



EJEMPLO DE TABLAS f, h, k, n
*@microsoft.com
fred.smith@xyz.com
'jjones@hotmail.com

EJEMPLO DE TABLAS j, m
Issuer = "Identrus", Type = Waranty
Issuer = "MyCompany", Type = Any
Key = 1234567890

EJEMPLO DE TABLAS g, i, l, o
CONFIDENCIAL
SECRETO
CONTRATO
PRECIOS
PEDIDO
PROYECTO X

Fig. 24

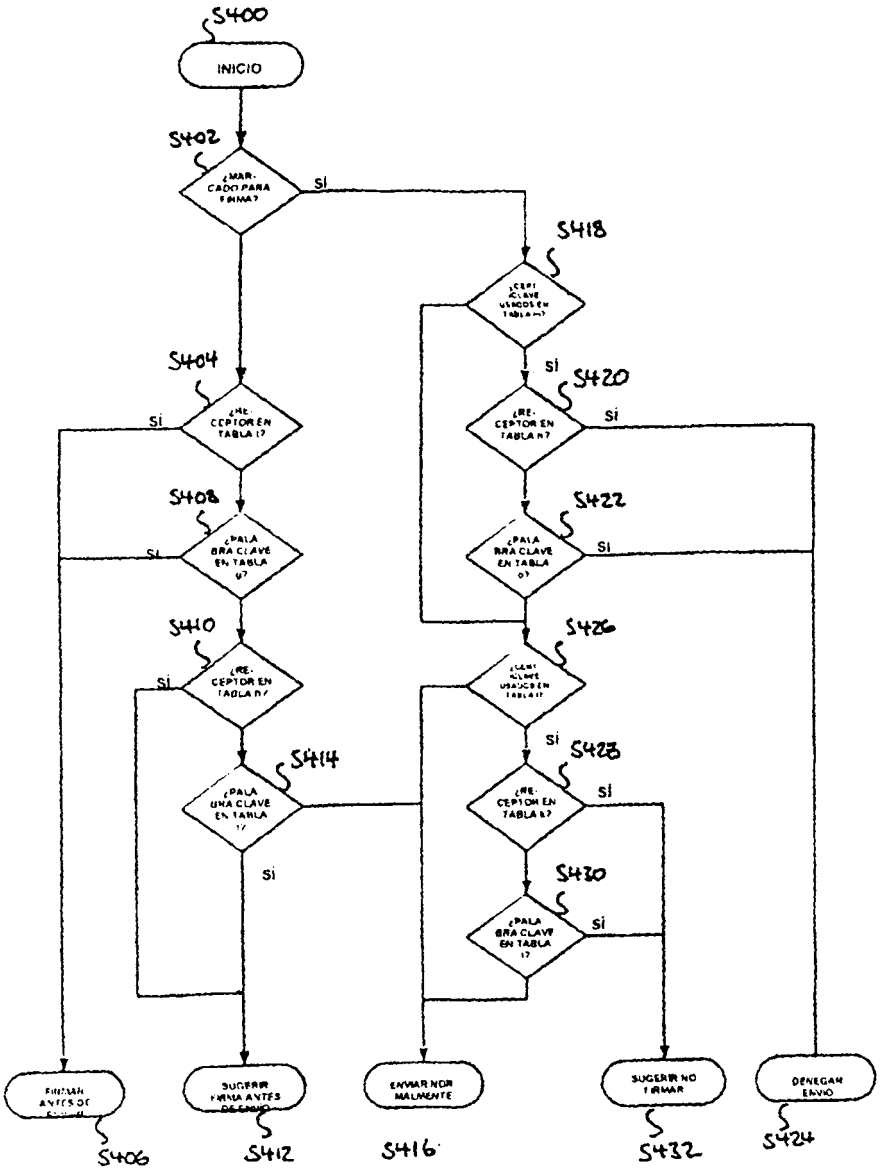

S400
INICIO
S402
¿MARCADO PARA FIRMA?
SÍ
S418
S404
¿RECEPTOR EN TABLA 1?
SÍ
S420
¿RECEPTOR EN TABLA N?
SÍ
S408
¿PALABRA CLAVE EN TABLA 0?
SÍ
S422
¿PALABRA CLAVE EN TABLA 0?
SÍ
S410
¿RECEPTOR EN TABLA N?
SÍ
S426
SÍ
S414
¿PALABRA CLAVE EN TABLA 1?
SÍ
S428
¿RECEPTOR EN TABLA 0?
SÍ
S430
¿PALABRA CLAVE EN TABLA 1?
SÍ
SUGERIR FIRMA ANTES DE ENVIO
ENVIAR NORMALMENTE
SUGERIR NO FIRMAR
DENEGAR ENVIO
S406
S412
S416
S432
S424

Fig. 25