(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 609 407**

(51) Int. CI.:

G06F 21/42 (2013.01)
G06Q 20/40 (2012.01)
G06Q 20/42 (2012.01)
G06Q 30/06 (2012.01)
G07F 7/10 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **28.07.2006 E 06118042 (8)**

(97) Fecha y número de publicación de la concesión europea: **28.09.2016 EP 1755062**

(54) Título: **Métodos y sistemas para autentificación segura de usuario**

(30) Prioridad:

29.07.2005 US 703605 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.04.2017

(73) Titular/es:

CITICORP CREDIT SERVICES, INC. (USA) (100.0%)
701 East 60th Street, North
Sioux Falls, SD 57104, US

(72) Inventor/es:

GRANDCOLAS, MICHAEL;
KORYAKOVTSEVA, IRINA;
VOS, JENNIFER y
HERRIG, ROBERT A.

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Métodos y sistemas para autentificación segura de usuario

Campo de la invención

La presente invención está relacionada generalmente con el campo de comercio electrónico, y más particularmente con métodos y sistemas para autentificación segura de usuario en transacciones de comercio electrónico.

Antecedentes de la invención

Actualmente, el robo de credenciales es un substancial peligro en el mundo en línea, por ejemplo, mediante "*phishing*" (pesca de datos), registrador de teclas, software espía y ataques por desconocidos (*man-in-the middle attacks*), entre otros. Actualmente los reguladores y las instituciones financieras, tales como bancos, están presionando para que surjan técnicas de autentificación de dos factores por las que se mitigue la amenaza de robo de credencial simple, tal como robo de una contraseña, por ejemplo, por el hecho de que en la autentificación haya implicado algún factor distinto a una simple contraseña. Se han propuesto varias formas de identificación de dos factores que utilizan algo más además de una contraseña estándar, tal como la huella dactilar de usuario, o en un mundo físico, una tarjeta de cajero de un usuario.

Otro ejemplo del uso de algo más además de una contraseña estándar es lo que se denominan contraseñas de un solo uso, y específicamente símbolos o llaveros de contraseña de un solo uso. Estos símbolos de contraseña de un solo uso representan un tipo de manera estándar pero muy cara de proporcionar a un cliente un dispositivo que genere continuamente una contraseña de un solo uso basada en tiempo o basada en evento. Así, cuando un usuario se prepara para iniciar sesión, el usuario consulta el dispositivo, y el dispositivo muestra, por ejemplo, un número que el usuario teclea y que se puede usar únicamente una vez. Así, si una persona no autorizada intercepta el número particular, es demasiado tarde para que la persona no autorizada lo use.

Sin embargo, estos tipos de soluciones son extremadamente caros y no necesariamente fáciles de usar. Por ejemplo, típicamente se requiere que los clientes lleven con ellos sus símbolos, y si un cliente tiene relaciones, por ejemplo, con tres o cuatro bancos, se requiere que el cliente lleve tres o cuatro símbolos diferentes. Adicionalmente, los símbolos tienen una vida útil limitada tras la que se deben sustituir. Además, la tarea de distribuir los símbolos a usuarios crea asuntos de seguridad y gastos para las instituciones financieras, y de manera semejante se crean asuntos de seguridad y comodidad para que el cliente guarde sus múltiples símbolos.

Un aspecto particularmente problemático del robo de credenciales es el fraude electrónico en el que números crecientes de clientes desprevenidos de instituciones financieras, tales como bancos, reciben correos electrónicos de *phishing* (pesca de datos) para engañarles para que revelen sus nombres de usuario y contraseñas o PIN a una parte no autorizada. Típicamente, una parte no autorizada que tiene éxito capturando las credenciales de inicio de sesión de un cliente de banco por medio de pesca de datos por correo electrónico o quizá por medio de virus informáticos, reutiliza las credenciales del cliente para iniciar sesión en el sitio web de banca en línea del banco para realizar transacciones fraudulentas. Un tipo de transacción fraudulenta implica el uso de las credenciales robadas de inicio de sesión del cliente para mover dinero internacionalmente por transferencia bancaria, y otro tipo de fraude es una transacción conocida como transacción interurbana global que implica mover dinero, por ejemplo, de una cuenta bancaria en los Estados Unidos a una cuenta bancaria extranjera y la retirada del dinero.

El documento WO01/11450 describe una arquitectura de seguridad en la que se proporciona una única inscripción para múltiples recursos de información. Se asocian esquemas de autentificación con niveles de confianza y un servicio de inicio de sesión obtiene credenciales provistas de los requisitos de nivel de confianza.

Compendio de la invención

La invención está definida por el alcance de las reivindicaciones anexas.

Breve descripción de los dibujos

La figura 1 es un diagrama esquemático que ilustra un ejemplo de componentes clave y el flujo de información entre componentes clave de un sistema de autentificación segura de usuario para realizaciones de la invención;

La figura 2 es un diagrama de flujo que ilustra un ejemplo de un proceso de aspecto de contraseña de próxima-vez para realizaciones de la invención;

La figura 3 es un diagrama de flujo que ilustra un ejemplo de la fase de dejar pendiente de un proceso de aspecto de código de autentificación de un solo uso impuesto por proveedor de transacciones para realizaciones de la invención;

La figura 4 es un diagrama de flujo que ilustra un ejemplo de la fase de activación del proceso de aspecto de código de autentificación de un solo uso impuesto por proveedor de transacciones para realizaciones de la invención;

La figura 5 es un diagrama de flujo que ilustra un ejemplo de la fase de solicitud de código de acceso de un proceso de aspecto de código de autentificación impuesto por proveedor de navegación para realizaciones de la invención;

La figura 6 es un diagrama de flujo que ilustra un ejemplo de la fase de acceso permitido del proceso de aspecto de código de autentificación impuesto por proveedor de navegación para realizaciones de la invención;

La figura 7 es un diagrama de flujo que ilustra un ejemplo de la fase de solicitud de código de acceso de un proceso híbrido de aspecto de código de autentificación de menús de información impuesto por proveedor de navegación / impuesto por proveedor de transacciones para realizaciones de la invención;

La figura 8 es un diagrama de flujo que ilustra un ejemplo de la fase de acceso permitido del proceso híbrido para realizaciones de la invención;

La figura 9 es un ejemplo de pantalla de menú de GUI (interfaz gráfica de usuario) de pagos y transferencias para el aspecto de código de transacción segura de realizaciones de la invención;

La figura 10 es un ejemplo de pantalla de GUI de entrada de código de autorización de transferencia para el aspecto de código de transacción segura de realizaciones de la invención;

La figura 11 es un ejemplo de pantalla de GUI de confirmación de código de autorización de transferencia para el aspecto de código de transacción segura de realizaciones de la invención;

La figura 12 es un ejemplo de página de GUI de error de dirección de correo electrónico para el aspecto de código de transacción segura de realizaciones de la invención;

La figura 13 es un ejemplo de página de GUI de error de código de autorización para el aspecto de código de transacción segura de realizaciones de la invención;

La figura 14 es un ejemplo de mensaje de correo electrónico de código de autorización para el aspecto de código de transacción segura de realizaciones de la invención;

La figura 15 es un ejemplo de mensaje de notificación de cambio de correo electrónico para el aspecto de código de transacción segura de realizaciones de la invención;

La figura 16 es un ejemplo de página inicial que muestra la dirección de correo electrónico actual del cliente para el aspecto de código de transacción segura de realizaciones de la invención; y

La figura 17 es un ejemplo de página inicial que muestra la dirección de correo electrónico actual del cliente con una notificación de una dirección de correo electrónico cambiada recientemente para el aspecto de código de transacción segura de realizaciones de la invención.

Descripción detallada

Ahora se hará referencia en detalle a realizaciones de la invención, uno o más ejemplos de las cuales se ilustran en los dibujos adjuntos. Cada ejemplo se proporciona a modo de explicación de la invención y no como limitación de la invención. Para los expertos en la técnica será evidente que en la presente invención se pueden hacer diversas modificaciones y variaciones sin apartarse del alcance de la invención. Por ejemplo, rasgos ilustrados o descritos como parte de una realización se pueden usar en otra realización para producir una realización todavía adicional. Así, se pretende que la presente invención abarque dichas modificaciones y variaciones que se encuentren dentro del alcance de la invención.

Un aspecto de contraseña de próxima-vez de las realizaciones de la presente invención propone una forma diferente de contraseñas de una vez que mejora la tecnología existente. Una clave para una realización de contraseña de un solo uso es que se le da a un usuario por algún canal que es exterior a la manera con la que accede el usuario, por ejemplo, el servicio de internet del usuario. Como se ha indicado anteriormente, las soluciones actuales de contraseña de un solo uso requieren que el usuario lleve un dispositivo aparte que genera una contraseña de un solo uso basada en tiempo. Estos dispositivos son caros e incómodos, y ocupan espacio, por ejemplo, en un llavero. Sin embargo, casi todo el mundo tiene un teléfono móvil o una dirección de correo electrónico, y el uso del teléfono móvil está creciendo. En una realización de la invención, cada vez que un usuario, tal como un cliente de institución financiera, cierra sesión en el sitio de la institución financiera, se envía una contraseña de próxima-vez a la dirección de entrega prerregistrada del cliente, tal como el teléfono móvil del cliente o la dirección de correo electrónico u otro canal fuera de banda, por la institución financiera, por ejemplo, por medio de mensaje de texto.

La contraseña de próxima-vez para una realización de la invención es buena para un solo uso y opcionalmente también puede tener una fecha y/u hora de caducidad asociadas a ella, tras la cual la contraseña de próxima-vez ya no es válida. Se tiene que entender que si bien el presente ejemplo se refiere al envío de la contraseña de próxima-vez a un teléfono celular, un teléfono móvil o una dirección de correo electrónico, el canal para la entrega de la contraseña de próxima-vez puede ser cualquier otro canal de comunicación adecuado, tal como algún tipo de cuenta de correo electrónico o incluso un correo de voz al teléfono casero del cliente, que es fuera de banda o diferente del

canal de comunicación por el que el cliente se comunica con el sitio de la institución. Después de eso, cuando el cliente vuelve al sitio de la institución financiera, el cliente puede introducir las credenciales normales de inicio de sesión del cliente, tal como el nombre de usuario y la contraseña del cliente. Adicionalmente, el cliente puede consultar, por ejemplo, el teléfono móvil del cliente y encontrar la contraseña de próxima-vez que se almacenó en el teléfono móvil del cliente en mensajes guardados.

En el aspecto de contraseña de próxima-vez de realizaciones de la invención, si por alguna razón el cliente no tiene una contraseña de próxima-vez o no puede encontrar la contraseña de próxima-vez almacenada en el teléfono móvil del cliente, únicamente es necesario que el cliente introduzca nombre de usuario y contraseña para permitirle entrar al sitio de la institución financiera. Al mismo tiempo que el cliente entra al sitio, se envía inmediatamente una contraseña de próxima-vez al teléfono móvil u otro dispositivo de administración registrado del cliente. Entonces, al recibir la contraseña de próxima-vez en tiempo real o tiempo seudorreal, el cliente puede introducir la contraseña de próxima-vez y se le permite acceso completo al sitio entero.

La solución de contraseña de próxima-vez para realizaciones de la invención no requiere ningún software residente en el teléfono que genere un símbolo de contraseña de próxima-vez. Si bien se puede argumentar que un valor de símbolo constantemente cambiante puede ser ligeramente más seguro que la contraseña de próxima-vez, dado que la contraseña de próxima-vez es única para el cliente y se puede usar únicamente una vez, la oportunidad realista de que la contraseña de próxima-vez sea interceptada es extremadamente baja, y proporciona una contraseña de un solo uso muy eficaz. Además, una institución financiera típicamente puede tener la mayor parte de la infraestructura en el sitio para implementar la contraseña de próxima-vez para realizaciones de la invención.

Para un ejemplo de uso de la contraseña de próxima-vez para realizaciones de la invención, un cliente en un dispositivo informático con un navegador inicia sesión en un sitio web de banca en línea de la institución financiera al introducir su nombre de usuario y contraseña. Adicionalmente, el cliente localiza su contraseña de próxima-vez entre los mensajes guardados en el teléfono móvil del cliente e introduce la contraseña de próxima-vez. La contraseña de próxima-vez es válida únicamente para un solo uso y tan pronto como el cliente introduce la contraseña de próxima-vez, ya no es válida para ninguna finalidad. Después de eso, cuando el cliente cierra sesión, se envía otra contraseña de próxima-vez al dispositivo de comunicación registrado del cliente, tal como el teléfono móvil del cliente. Así, incluso si una parte no autorizada intercepta la contraseña de próxima-vez del cliente, lo más probable cualquier intercepción ocurrirá después de que la contraseña de próxima-vez ya haya sido usada. En otras palabras, si se intercepta la contraseña de próxima-vez por medio de un registrador de teclas, será demasiado tarde, porque la contraseña de próxima-vez ya ha sido usada cuando el cliente entra al sitio de la institución financiera y ya no es válida para ninguna finalidad.

Por consiguiente, la contraseña de próxima-vez para realizaciones de la invención tiene todas las características de una contraseña de un solo uso excepto que en lugar de ser generada constantemente, por ejemplo, cada pocos segundos, la contraseña de próxima-vez se envía al cliente cuando cierra sesión en un sitio para usarla cuando el cliente vuelva al sitio en un momento posterior. Además, si el cliente no puede encontrar su contraseña de próxima-vez cuando desea volver al sitio de la institución financiera, el cliente simplemente introduce su nombre de usuario y contraseña y entonces, por ejemplo, hace clic en un botón para decir que no tiene su contraseña de próxima-vez. En respuesta, la institución financiera envía inmediatamente una contraseña de próxima-vez al dispositivo registrado del cliente, que el cliente puede introducir entonces para acceso completo al sitio, por ejemplo, para banca en línea.

La figura 1 es un diagrama esquemático que ilustra un ejemplo de componentes clave y el flujo de información entre componentes clave de un sistema de autentificación segura de usuario para realizaciones de la invención. Haciendo referencia a la figura 1, el sistema para realizaciones de la invención incluye, por ejemplo, un dispositivo informático del cliente 10, tal como un PC, portátil o PDA del cliente, se conecta por una red 12, tal como internet u otra red global, a un servidor de portal 12 por la que un usuario, tal como un cliente, accede a un sitio web. El servidor de portal 12 puede ser el servidor de portal de cualquier entidad, incluida, por ejemplo, una institución financiera, tal como un banco. Adicionalmente, un servidor de mensajes de alerta 16 proporciona, por ejemplo, mensajes de correo electrónico al cliente en el dispositivo informático del cliente 10 por medio de la red 12 o el servidor de mensajes 16 puede proporcionar, por ejemplo, mensajes de texto al dispositivo de telecomunicación 18 del cliente, tal como un teléfono móvil o fijo, por medio de un sistema de telecomunicación 20. Además, el servidor de portal 14 también puede proporcionar acceso a uno o más servidores de transacciones 22, que pueden incluir una federación de dichos servidores.

La figura 2 es un diagrama de flujo que ilustra un ejemplo de un proceso de aspecto de contraseña de próxima-vez para realizaciones de la invención. Haciendo referencia a la figura 2, en S1, cada vez que el cliente cierra sesión, por ejemplo, el sitio web 14 de la institución financiera, la institución financiera envía una contraseña de próxima-vez única para el cliente que se puede usar únicamente una vez (y opcionalmente puede tener una fecha y/u hora de caducidad) al cliente por medio de un canal de comunicación fuera de banda, tal como a la dirección de correo electrónico o teléfono móvil 18 prerregistrados del cliente, por ejemplo, por medio de mensaje de texto. En S2, cuando el cliente vuelve al sitio web 14 en una ocasión siguiente, el cliente inicia sesión introduciendo las credenciales normales de inicio de sesión del cliente, tales como el nombre de usuario y la contraseña del cliente, y, adicionalmente, el cliente consulta, por ejemplo, los mensajes almacenados en el teléfono móvil 18 o correo electrónico del cliente en el dispositivo informático 10 del cliente para encontrar la contraseña de próxima-vez que se

recibió cuando el cliente cerró sesión en el sitio web 14 en la ocasión anterior y se almacenó en el teléfono móvil del cliente en mensajes guardados o en la carpeta de correo electrónico del cliente, y el cliente introduce la contraseña de próxima-vez para acceso completo al sitio entero.

Haciendo referencia de nuevo a la figura 2, en S3, si por alguna razón el cliente no tiene o no puede encontrar la contraseña de próxima-vez almacenada o guardada, el cliente puede introducir su nombre de usuario y contraseña y se permite iniciar sesión en el sitio de la institución financiera 14, y al mismo tiempo o sustancialmente al mismo tiempo que el cliente inicia sesión en el sitio, se envía inmediatamente una contraseña de próxima-vez fuera de banda al teléfono móvil 18 u otro dispositivo registrado del cliente, y al recibir la contraseña de próxima-vez, el cliente puede introducir la contraseña de próxima-vez y se le permite acceso completo al sitio entero. Después de eso, en S4, cuando el cliente cierra sesión, se envía fuera de banda otra contraseña de próxima-vez al dispositivo de comunicación registrado del cliente, tal como el teléfono móvil 18 del cliente.

Si bien el ejemplo anterior se refiere a acceso a un sitio web en línea de institución financiera o banca, el uso de la contraseña de próxima-vez para realizaciones de la invención no se limita de ninguna manera al sitio de un banco u otro tipo de institución financiera. Ni el uso de la contraseña de próxima-vez se limita a acceder a un sitio web. Por ejemplo, la contraseña de próxima-vez también se puede emplear en un sistema de cajero automático (ATM), así como en cualquier otra operación en la que se requiera que un cliente introduzca información de autentificación. Adicionalmente, si bien se ha mencionado previamente, la solución de contraseña de próxima-vez para realizaciones de la invención no requiere software residente en el teléfono para generar la contraseña de próxima-vez, realizaciones alternativas de la invención implican, por ejemplo, proporcionar al cliente una aplicación simple residente en el teléfono que haga más fácil y más cómodo para el cliente guardar y ver el símbolo de contraseña de próxima-vez que se le envió al teléfono móvil 18. Otro aspecto alternativo para realizaciones de la invención implica, por ejemplo, una aplicación residente en el teléfono que genera el símbolo de contraseña de próxima-vez.

Una característica clave del aspecto de contraseña de próxima-vez para realizaciones de la invención es que cada vez que un cliente cierra sesión el sitio de la institución financiera 14, se envía una contraseña de próxima-vez al dispositivo registrado del cliente, tal como el teléfono móvil 18 del cliente, y la próxima vez que el cliente inicia sesión, además de introducir su nombre de usuario y contraseña, el cliente simplemente consulta mensajes almacenados en su teléfono móvil 18, que típicamente está en la posesión inmediata del cliente, y encuentra e introduce la contraseña de próxima-vez previamente proporcionada. Así, no se requiere que el cliente lleve nada que no lleve típicamente.

Se tiene que entender que si bien la solución de contraseña de próxima-vez para realizaciones de la invención puede ser implementada por cualquier número de tipos diferentes de entidades, incluidas sin limitación, instituciones financieras, tales como bancos, así como otros tipos de instituciones financieras, la utilidad de la contraseña de próxima-vez no se limita a instituciones financieras, y también se puede implementar para iniciar sesión en otros tipos de sitios. El aspecto de contraseña de próxima-vez de realizaciones de la invención combina elementos para proporcionar una contraseña de un solo uso en forma de contraseña de próxima-vez que, si bien no cambia constantemente, cambia suficientemente a menudo y se entrega de una manera que es suficientemente segura para que sean extremadamente bajas las oportunidades de intercepción y robo, especialmente robo masivo. Además, la implementación y uso de la solución de contraseña de próxima-vez para realizaciones de la invención es extremadamente económica y no requiere la compra ni distribución de dispositivos de símbolo caros. Ni es dependiente de diferentes versiones de teléfonos y funcionará virtualmente con cualquier teléfono que sea compatible, por ejemplo, con mensajes de texto.

El aspecto de código de transacción segura para realizaciones de la invención proporciona un planteamiento para proteger a los clientes de un banco frente a transacciones fraudulentas incluso si roban sus credenciales principales de inicio de sesión. En el aspecto de código de transacción segura, sigue sin cambios el procedimiento en el que un cliente usa las credenciales de inicio de sesión del cliente para iniciar sesión en el sistema de un banco, pero si el cliente intenta realizar ciertos tipos predefinidos de transacciones considerados por el banco como funciones sensibles, tales como transferencias bancarias o transferencias interurbanas globales, el cliente debe responder un valor de un solo uso, es decir, el código de transacción segura, con el fin de ejecutar la transacción sensible. En el aspecto de código de transacción segura, el valor de un solo uso que es el código de transacción segura se envía de manera semejante al cliente fuera de banda del canal de internet a la dirección de entrega prerregistrada del cliente, tal como la dirección de correo electrónico o teléfono móvil 18 del cliente. Como en el aspecto de contraseña de próxima-vez, el cliente debe haber registrado previamente una dirección de destino de entrega, como una dirección de correo electrónico o un número de teléfono móvil como vehículo de entrega para el código de transacción segura del cliente. Cuando el cliente recibe el código de transacción segura en la dirección de correo electrónico o teléfono móvil 18 del cliente, el cliente ve el valor y responde con él en el sitio web 12 y entonces se le permite proceder y ejecutar la transacción considerada por el banco como función sensible.

Un rasgo del aspecto de código de transacción segura para realizaciones de la invención está relacionado con una manera adicional de proteger el acceso a un sitio web del banco. Como potencialmente hay una multitud de diferentes clases de funciones que pueden ser protegidas por el código de transacción segura, una realización de la invención implementa la protección de entrada principal en la navegación del propio sitio. Así, cuando un cliente intenta hacer clic en una función o un enlace de navegación que llevaría al cliente a una función sensible, se le pide

al cliente que introduzca un código de transacción segura. Si el cliente al que se ha pedido que introduzca un código de transacción segura no tiene uno, el cliente puede responder por medio de la GUI del sitio web 12 que no tiene un código de transacción segura. Tras eso, el aspecto de navegación del sitio 12 que trabaja con un componente de seguridad del sitio 12 genera un código de transacción segura y provoca que sea entregado, por ejemplo, a la dirección de correo electrónico o teléfono móvil 18 del cliente. Al recibir el código de transacción segura, incluso dentro de la misma sesión, el cliente puede introducir el valor que representa el código de transacción segura y se le permite continuar.

Un rasgo adicional del aspecto de código de transacción segura de realizaciones de la invención está relacionado con proporcionar protección para funciones que están tanto en el propio sitio primario 14 del banco como en cualquiera de varios sitios federados que también son parte de la funcionalidad de banca en línea del banco, incluidos por ejemplo, sitios para una funcionalidad que es el ejecutor para transferencias interurbanas globales y una funcionalidad que es el sistema de ejecución para transferencias bancarias. Proporcionar esta protección implica, por ejemplo, asignar una tarea a un indicador para un único mecanismo de inicio de sesión del banco a los sitios federados 22 para que diga a los sitios federados 22 que el cliente ha solicitado una función segura y advierte a los sitios federados 22 si el cliente ha introducido un código de transacción segura.

El aspecto de código de transacción segura para realizaciones de la invención se ve como una forma de contraseña de un solo uso, lo que significa que únicamente se puede introducir una vez, y una vez se ha introducido, nunca se puede usar de nuevo. Así, si roban el código de transacción segura, no tiene valor. El código de transacción segura también puede tener un periodo de tiempo durante el que permanece válido, que puede ser cualquier longitud adecuada de tiempo, tal como de unos pocos minutos hasta varios días. Así, cuando se emite un código de transacción segura, se notifica al cliente que es válido únicamente durante la cantidad predeterminada de tiempo, tras la que caduca. Sin embargo, también se hace que el cliente sea consciente de que puede recibir un nuevo código de transacción segura por adelantado a la siguiente ocasión en la que desee realizar una de las funciones sensibles, y el código de transacción segura también se puede usar para realizar múltiples transacciones sensibles dentro de una única sesión de cliente una vez que el cliente introduce el código de transacción segura.

Haciendo referencia a la figura 1, en un ejemplo del aspecto de código de transacción segura para realizaciones de la invención, cuando el cliente selecciona un enlace en un portal 14 de institución financiera para una transacción sensible, se muestra una página de autorización que explica la necesidad de un código de autorización para acceder a la función particular. Por ejemplo, cuando el cliente hace clic en un enlace de una función que la institución financiera considera como una transacción sensible, tal como transferencia bancaria, dentro de una página de menú, el enlace expone la página de autorización. Si el portal 14 de institución financiera detecta que el cliente no tiene una dirección de correo electrónico en el perfil almacenado del cliente, se expone una versión modificada de la página de autorización. El portal 14 confirma si el cliente tiene derecho o no a la funcionalidad de transferencia bancaria y si es así el portal 14 recupera la dirección de correo electrónico prerregistrada del cliente y la fecha cuando se modificó por última vez en el registro de perfil almacenado del cliente. El portal 14 provoca que se emita un código secreto aleatorio (es decir, código de transacción segura) para el cliente y que se almacene en el registro de perfil del cliente, así como la fecha de emisión del código secreto. Adicionalmente, el portal 14 provoca que se envíe un correo electrónico fuera de banda al cliente con el código secreto. Cuando el cliente introduce el código secreto en la página de autorización, el código secreto introducido por el cliente es comparado por el portal 14 con el código secreto almacenado y su fecha de caducidad.

En realizaciones del aspecto de código de transacción segura de la invención, se envían alertas a clientes cuando se cambia la dirección de correo electrónico en el perfil del cliente. Por ejemplo, el portal 14 puede enviar uno o más mensajes al cliente por medio de servicio postal sobre la dirección de correo electrónico cambiada. Adicionalmente, la dirección de correo electrónico del perfil de cliente se puede mostrar en la página inicial de inicio de sesión del cliente, junto con un enlace para editar la dirección. Además, cuando se hace un cambio de dirección de correo electrónico, en la página inicial de inicio de sesión del cliente se puede mostrar una notificación de que se ha cambiado la dirección. Si el cliente introduce el código secreto después de que haya caducado, se muestra un mensaje que advierte al cliente para que pida un código secreto nuevo y se dirige al cliente a una pantalla de petición de nuevo código. Si el código se introduce correctamente y no ha caducado, se dirige al cliente a la pantalla apropiada para la transacción sensible requerida. Si el código introducido es incorrecto, se muestra una pantalla de error y se aumenta un contador de intentos.

Realizaciones del aspecto de código de transacción segura proporcionan, por ejemplo, un proceso de código de autentificación de un solo uso impuesto por proveedor de transacciones con una fase de dejar pendiente y una fase de activación; un proceso de código de autentificación impuesto por proveedor de navegación con una fase de solicitud de código de acceso y una fase de acceso permitido; y/o un proceso híbrido de código de autentificación de menús de información impuesto por proveedor de navegación / impuesto por proveedor de transacciones, de manera semejante con una fase de solicitud de código de acceso y una fase de acceso permitido. La figura 3 es un diagrama de flujo que ilustra un ejemplo de la fase de dejar pendiente del proceso de aspecto de código de autentificación de un solo uso impuesto por proveedor de transacciones para realizaciones de la invención. En el proceso impuesto por proveedor de transacciones, el proveedor de transacciones es responsable de la imposición de autentificación adicional y soporta la fase de dejar pendiente o de configuración, así como la activación de la fase de ejecución.

Haciendo referencia a la figura 3, en S11, el cliente inicia sesión en un dispositivo informático 10 con un navegador, por ejemplo, el servidor de portal 14 de banca en casa de la institución financiera y selecciona una tarea de transacción sensible, tal como una transferencia bancaria, es redirigido a un servidor de transacciones 22 de institución financiera, introduce información para establecer la transacción, y es informado de que se enviará al cliente por correo electrónico un código de activación de un solo uso (es decir, código de transacción segura). Haciendo referencia además a la figura 3, en S12, el servidor de transacciones 22 mantiene un dialogo con el cliente para establecer la transferencia bancaria y deja pendiente la transacción en una base de datos. En S13, el servidor de transacciones 22 genera, almacena y envía el código de activación de un solo uso al servidor de mensajes de alerta 16 de institución financiera para la entrega a la dirección de correo electrónico del cliente. En S14, el servidor de mensajes de alerta 16 envía el código de un solo uso a la dirección de correo electrónico del cliente si la dirección de correo electrónico no ha cambiado recientemente. En S15, el cliente, en el dispositivo informático 10 del cliente, recibe el correo electrónico con el código de un solo uso.

La figura 4 es un diagrama de flujo que ilustra un ejemplo de la fase de activación del proceso de aspecto de código de autentificación de un solo uso impuesto por proveedor de transacciones para realizaciones de la invención. Haciendo referencia a la figura 4 en S16 el cliente, en el dispositivo informático 10 con el navegador, inicia sesión en el servidor de portal 14 de banca en casa de la institución financiera, introduce una selección para la tarea de transacción sensible, es redirigido al servidor de transacciones 22, e introduce el código de un solo uso cuando se lo pide el servidor de transacciones 22. En S17, el servidor de transacciones determina si el código de un solo uso es válido o no, y si es válido, activa la transacción y envía una respuesta que confirma la activación de la transacción al cliente.

La figura 5 es un diagrama de flujo que ilustra un ejemplo de la fase de solicitud de código de acceso del aspecto de código de autentificación impuesto por proveedor de navegación para realizaciones de la invención. En el proceso impuesto por proveedor de navegador, el proveedor de navegador proporciona imposición por tarea de navegación en la que, por ejemplo, no se permite que un cliente entre a una tarea de navegación sin un código de acceso de autentificación. Se tiene que entender que el código de acceso de autentificación puede ser cualquiera de un código de un solo uso, o un código multiuso con una hora o fecha de caducidad, o código con número de usos. Haciendo referencia a la figura 5, en S21, el cliente, en el dispositivo informático 10 con un navegador, inicia sesión en el servidor de portal 14 de banca en casa de la institución financiera y selecciona una tarea de transacción sensible, tal como una transferencia bancaria, el servidor de portal 14 le pide que introduzca el código de acceso de autentificación del cliente (es decir, código de acceso seguro), y si el cliente responde que no tiene un código de acceso de autentificación, el servidor de portal 14 le informa de que se enviará por correo electrónico al cliente un código de acceso de autentificación. En S22, el servidor de portal 14 genera un código de acceso para el uso por parte del cliente para la transacción sensible particular y envía el acceso a la dirección de correo electrónico del cliente por medio de un servidor de mensajes de alerta 16 de institución financiera. En S23, el servidor de mensajes de alerta 16 envía el código de acceso a la dirección de correo electrónico del cliente si la dirección de correo electrónico no se ha cambiado recientemente. En S24, el cliente, en el dispositivo informático 10 del cliente, recibe el correo electrónico con el código de un solo uso.

La figura 6 es un diagrama de flujo que ilustra un ejemplo de la fase de acceso permitido del proceso de aspecto de código de autentificación impuesto por proveedor de navegación para realizaciones de la invención. Haciendo referencia a la figura 6, en S25, el cliente, en el dispositivo informático 10 con el navegador, inicia sesión en el servidor de portal 14 de banca en casa de la institución financiera, introduce una selección para la tarea de transacción sensible, e introduce el código de acceso. En S26, el servidor de portal 14 determina si el código de acceso es válido o no para la tarea particular, y si es válido, permite la entrada a la tarea, por ejemplo, redirigiendo el navegador del cliente al servidor de transacciones 22. Cabe señalar que en el proceso impuesto por proveedor de navegación, el proveedor o proveedores de transacciones son transparentes para el proceso de autentificación. Cabe señalar además que el cliente puede realizar más de una transacción sensible durante una sesión y que no hay necesidad de dejar pendientes transacciones.

La figura 7 es un diagrama de flujo que ilustra un ejemplo de la fase de solicitud de código de acceso del proceso híbrido de aspecto de código de autentificación de menús de información impuesto por proveedor de navegación / impuesto por proveedor de transacciones para realizaciones de la invención. En el proceso híbrido, el proveedor de navegador proporciona de manera semejante imposición por tarea de navegación en la que, por ejemplo, no se permite a un cliente entrar a una tarea de navegación sin un código de acceso de autentificación (es decir, código de acceso seguro). De manera semejante, se tiene que entender que el código de acceso de autentificación puede ser cualquiera de un código de un solo uso, o un código multiuso con una hora o fecha de caducidad, o código con número de usos. Haciendo referencia a la figura 7, en S31, el cliente, en un dispositivo informático 10 con un navegador, inicia sesión en el servidor de portal 14 de banca en casa de la institución financiera y selecciona una tarea de transacción sensible, tal como una transferencia bancaria, el servidor de portal 14 le pide que introduzca el código de acceso de autentificación del cliente, y si el cliente responde que no tiene un código de acceso de autentificación, el servidor de portal 14 le informa de que se enviará por correo electrónico al cliente un código de acceso de autentificación. En S32, el servidor de portal 14 genera un código de acceso para el uso por parte del cliente para la transacción sensible particular y envía el código de acceso a la dirección de correo electrónico del cliente por medio de un servidor de mensajes de alerta 16 de institución financiera. En S33, el servidor de mensajes de alerta 16 envía el código de acceso a la dirección de correo electrónico del cliente si la dirección de correo

electrónico no se ha cambiado recientemente. En S34, el cliente, en el dispositivo informático 10 del cliente, recibe el correo electrónico con el código de un solo uso.

La figura 8 es un diagrama de flujo que ilustra un ejemplo de la fase de acceso permitido del proceso híbrido para realizaciones de la invención. Haciendo referencia a la figura 8, en S35, el cliente, en el dispositivo informático 10 con el navegador, inicia sesión en el servidor de portal 14 de banca en casa de la institución financiera, introduce una selección para la tarea de transacción sensible, e introduce el código de acceso. En S26, el servidor de portal 14 determina si el código de acceso es válido o no para la tarea particular, y, si es válido, permite la entrada a la tarea, por ejemplo, redirigiendo el navegador del cliente al servidor de transacciones 22 con una marca que indica que el cliente tiene derecho a transacciones sensibles, en cuyo caso se permite al cliente realizar todas las transacciones. De otro modo, sin la marca de derechos, al cliente únicamente se le permite realizar transacciones no sensibles. Cabe señalar que en el proceso híbrido, el proveedor o proveedores de transacciones son transparentes para el proceso de autentificación. Cabe señalar además que el cliente puede realizar más de una transacción sensible durante una sesión y que no hay necesidad de dejar pendientes transacciones.

El código de transacción segura para realizaciones de la invención proporciona un nivel de protección adicional para transacciones sumamente sensibles, tales como transferencias bancarias u otras transacciones de alto riesgo, solicitando a un cliente que use un código de autorización de transacción (es decir, código de acceso seguro) para hacer cada transacción de este tipo. Entonces, cuando el cliente selecciona un enlace a una transacción sensible, al cliente se le muestra una página de autorización que explica la necesidad de un código de autorización para acceder a la función. La página también presenta opciones para que el cliente introduzca un código, para solicitar un código, o para acceder a una función no sensible. Clientes que ya poseen un código pueden ejercer la primera opción e introducir un código en un campo de entrada. Clientes que todavía no poseen un código pueden ejercer la segunda opción para solicitar un código y se les enviará un código generado aleatoriamente por medio de correo electrónico usando la dirección de correo electrónico del cliente en el perfil de usuario. El cliente que ha iniciado sesión en la misma sesión o una posterior proporciona entonces el código de transacción para autorizar la función sensible solicitada o posiblemente autorizar alguna otra función sensible. El código de transacción caduca un tiempo predeterminado después de la emisión, tal como una semana.

En realizaciones de la invención, cuando un cliente cambia la dirección de correo electrónico del perfil del cliente, se establece una marca en el perfil almacenado que prohíbe el envío de un código de transacción al cliente en la dirección de correo electrónico del cliente. La marca también se puede establecer para que caduque tras un periodo predeterminado, tal como una semana. Durante ese periodo de tiempo, si el cliente solicita que el envíen un código de transacción por medio de correo electrónico, se presenta una página de error que advierte al cliente que no se puede enviar un código de transacción, y que si el cliente necesita realizar mientras tanto una transacción sensible, tal como una transferencia bancaria, la transacción se puede realizar en persona en una oficina de institución financiera. Como alternativa, la página de error puede dirigir al cliente para que llame a un número de atención al cliente, por ejemplo, para autentificación manual por parte de un representante de atención al cliente. Al autentificar manualmente al cliente, el representante de atención al cliente puede proporcionar un código de transacción aleatorio para el cliente o borrar la marca de correo electrónico, con lo que el cliente puede solicitar el código en línea y recibirlo en la nueva dirección de correo electrónico del cliente. A los clientes que ejercen la tercera opción para acceder a funciones no sensibles se les proporciona únicamente información. Por ejemplo, en el caso de transferencias bancarias, se le presenta al cliente un menú con opciones para que vea información acerca de transferencias bancarias que están planificadas, pasadas o entrantes.

En realizaciones de la invención, cuando se cambia la dirección de correo electrónico en el perfil de usuario almacenado del cliente, se envía una alerta por correo electrónico a la nueva dirección de correo electrónico y a la dirección de correo electrónico cambiada. Además, la dirección de correo electrónico de perfil de usuario actual del cliente se muestra en la página inicial de inicio de sesión del cliente, junto con un enlace para editar la dirección. Adicionalmente, si se hace un cambio de dirección de correo electrónico, se muestra una notificación para el cliente de que se ha cambiado la dirección de correo electrónico.

Realizaciones de la invención emplean diversas pantallas de GUI. Se tiene que entender que si bien el ejemplo de flujo y pantallas descritos en esta memoria están relacionados con transacciones sensibles, tales como transferencias bancarias, el mismo proceso de autentificación de transacción para realizaciones de la invención es igualmente útil y fácilmente portátil a otros tipos de transacciones sensibles. La figura 9 es un ejemplo de pantalla de menú de GUI 40 de pagos y transferencias para el aspecto de código de transacción segura de realizaciones de la invención. Haciendo referencia a la figura 9, si un cliente selecciona una función sensible, tal como "Transfer to an Account in the U.S." (Transferencia a una cuenta en los EE. UU.) 42 o "Transfer to an Account Abroad" (Transferencia a una cuenta en el extranjero) 44, un enlace expone una pantalla de entrada de autorización de transacción.

La figura 10 es un ejemplo de pantalla de GUI 46 de entrada de código de autorización de transferencia para el aspecto de código de transacción segura de realizaciones de la invención. Haciendo referencia a la figura 10, al cliente se le presentan opciones de solicitar un código de autorización 48, introducir un código de autorización proporcionado previamente al cliente 50, o seleccionar una función no sensible (informativa) 52. Si el cliente introduce un código de transacción de autorización y el código de autorización es autentificado, al cliente se le

presenta un menú apropiado de transacciones sensibles. Si no se autentifica el código de autorización, al cliente se le presenta una pantalla de error de código de autorización. Adicionalmente, el cliente puede seleccionar "Cancelar" 54 y volver al menú de pagos y transferencias 40. Haciendo referencia además a la figura 10, si el cliente introduce una selección que solicita que se envíe un código al cliente 48, si no se establece marca de autorización en la dirección de correo electrónico de perfil del cliente, al cliente se le muestra una pantalla de GUI de confirmación de código de autorización de transferencia. Sin embargo, si se establece una marca de autorización en la dirección de correo electrónico de perfil del cliente, se muestra una página de error que informa al cliente de que el código no se puede enviar por correo electrónico. Un enlace de actualizar dirección 56 permite al cliente actualizar la dirección de correo electrónico del cliente. Si el cliente introduce una selección para ver información acerca de actividad reciente 52, se ofrece al cliente opciones adicionales para ver información acerca de transferencias bancarias planificadas, transferencias bancarias pasadas y transferencias bancarias entrantes

La figura 11 es un ejemplo de pantalla de GUI 58 de confirmación de código de autorización de transferencia para el aspecto de código de transacción segura de realizaciones de la invención. Haciendo referencia a la figura 11, la página de GUI 58 de confirmación de código de autorización de transferencia notifica al cliente de que se ha enviado un código y advierte al cliente cómo usar el código de autorización de transferencia. Cuando el cliente hace clic en "Continue" (continuar) 60, se devuelve al cliente a la página 40 de entrada de código de autorización de transferencia. La figura 12 es un ejemplo de página de GUI 62 de error de dirección de correo electrónico para el aspecto de código de transacción segura de realizaciones de la invención. Haciendo referencia a la figura 12, cuando el cliente ha cambiado la dirección de correo electrónico de perfil del cliente dentro de un periodo de tiempo anterior predeterminado, tal como en la semana pasada, se presenta la página de error 62 al cliente para advertir al cliente de la situación. La figura 13 es un ejemplo de página de GUI 64 de error de código de autorización para el aspecto de código de transacción segura de realizaciones de la invención. Haciendo referencia a la figura 13, cuando un código de autorización no es autorizado por el sistema, en la página 64 de error de código de autorización se presenta al cliente un mensaje de error "Information Not Recognized" (Información no reconocida) 66. Tras un número predeterminado de intentos sin éxito, tal como tres intentos, para que coincida el código de autorización, se bloquea el número de identificación personal del cliente, tal como un PIN o CIN.

La figura 14 es un ejemplo de mensaje 68 de correo electrónico de código de autorización para el aspecto de código de transacción segura de realizaciones de la invención. Cuando un cliente solicita un código de autorización, se envía un correo electrónico similar al ejemplo de mensaje de correo electrónico 68 ilustrado en la figura 14 a la dirección de correo electrónico asociada con el perfil de usuario del cliente. La figura 15 es un ejemplo de mensaje 70 de notificación de cambio de correo electrónico para el aspecto de código de transacción segura de realizaciones de la invención. Cuando un cliente cambia la dirección de correo electrónico de perfil de usuario del cliente, se envía un correo electrónico similar al ejemplo de mensaje de correo electrónico 70 ilustrado en la figura 15 a la nueva dirección de correo electrónico según el perfil de usuario del cliente y a la antigua dirección de correo electrónico según el perfil de usuario del cliente.

La figura 16 es un ejemplo de página inicial 72 que muestra la dirección de correo electrónico actual 74 del cliente para el aspecto de código de transacción segura de realizaciones de la invención. Haciendo referencia a la figura 16, la página inicial 72 del cliente muestra la dirección de correo electrónico actual 74 del cliente y también proporciona un enlace a una función de edición 76 para actualizar la dirección de correo electrónico del cliente en el perfil de usuario del cliente. Adicionalmente, cambios de dirección de correo electrónico se destacan en la página inicial 72 mostrando la dirección de correo electrónico del cliente durante un periodo predeterminado, tal como una semana. La figura 17 es un ejemplo de página inicial 72 que la muestra dirección de correo electrónico actual del cliente con una notificación de una dirección de correo electrónico cambiada recientemente 78 para el aspecto de código de transacción segura de realizaciones de la invención.

Un rasgo único del aspecto de código de transacción segura para realizaciones de la invención es que, a diferencia de la mayoría de mecanismos de contraseña de un solo uso, no hay requisito de que el cliente tenga ningún tipo de dispositivo físico que genere un valor único de un solo uso. En cambio, en el aspecto de código de transacción segura, el banco en el lado de servidor genera el valor y lo comunica al cliente fuera de banda, y cuando el cliente lo recibe, únicamente es necesario que el cliente introduzca el valor. Así, el código de transacción segura logra aspectos seguros de una contraseña de un solo uso sin el gasto, incomodidad y complicaciones de usar llaveros de contraseña de un solo uso o tipos similares de dispositivos generadores de contraseña de un solo uso.

REIVINDICACIONES

1. Un método implementado en ordenador para autentificación segura de usuario en comercio electrónico, que comprende:

mantener información electrónica que tiene un primer aspecto y un segundo aspecto, dicho primer aspecto es accesible por un usuario por un primer canal electrónico de comunicación en respuesta a la entrada de una primera credencial conocida por el usuario y dicho segundo aspecto es accesible por el usuario por el primer canal electrónico de comunicación en respuesta a la entrada de una segunda credencial proporcionada al usuario;

pre-registrar una dirección de entrega en un segundo canal electrónico de comunicación que es diferente del primer canal electrónico de comunicación para proporcionar la segunda credencial al usuario;

permitir a un usuario una sesión actual de acceso al primer aspecto de la información electrónica en respuesta a la entrada de la primera credencial y proporcionar la segunda credencial al usuario en la dirección de entrega prerregistrada por medio del segundo canal electrónico de comunicación en respuesta a la entrada de una selección predeterminada de usuario durante dicha sesión de acceso de usuario al primer aspecto, en donde un cambio en la dirección de entrega del usuario en dicho segundo canal electrónico de comunicación tiene como resultado que se establece una marca en un perfil almacenado que prohíbe proporcionar la segunda credencial al usuario, en donde dicha marca se establece para que caduque tras un periodo de tiempo predeterminado, y permitir al usuario una sesión de acceso al segundo aspecto de la información electrónica por medio del primer canal electrónico de comunicación en respuesta a la entrada de la segunda credencial durante una de dicha sesión actual de acceso de usuario al primer aspecto y una sesión exitosa de acceso de usuario al primer aspecto.

2. El método de la reivindicación 1, en donde dicho primer aspecto comprende además aspectos de transacción preseleccionados no sensibles de la información electrónica y dicho segundo aspecto comprende además aspectos de transacción preseleccionados sensibles de la información electrónica.

3. El método de la reivindicación 1, en donde dicho primer canal electrónico de comunicación comprende además un dispositivo informático conectado por una red global a un servidor de sitios web.

4. El método de la reivindicación 3, en donde dicho primer canal electrónico de comunicación comprende además el dispositivo informático conectado por la red global a un servidor de transacciones por medio del servidor de sitios web.

5. El método de la reivindicación 1, en donde dicho primer canal electrónico de comunicación comprende además un terminal de transacciones financieras de autoservicio conectado por red de transacciones financieras de autoservicio a un servidor anfitrión.

6. El método de la reivindicación 1, en donde dicha primera credencial comprende además una contraseña seleccionada por el usuario para identificar al usuario.

7. El método de la reivindicación 1, en donde dicha segunda credencial comprende además un código secreto generado aleatoriamente para identificar al usuario que se proporciona al usuario.

8. El método de la reivindicación 1, en donde dicha segunda credencial se proporciona al usuario para una única sesión de acceso al segundo aspecto de la información electrónica.

9. El método de la reivindicación 1, en donde dicha segunda credencial tiene una caducidad predeterminada, tras la cual la segunda credencial de identificación ya no es válida para acceder el segundo aspecto de la información electrónica.

10. El método de la reivindicación 1, en donde prerregistrar dicha dirección de entrega en el segundo canal electrónico de comunicación comprende además prerregistrar una de una dirección de dispositivo de telecomunicación móvil y una dirección de correo electrónico para proporcionar al usuario la segunda credencial.

11. El método de la reivindicación 1, en donde proporcionar dicha segunda credencial al usuario por medio del segundo canal electrónico de comunicación comprende además proporcionar la segunda credencial al usuario mediante mensaje de texto.

12. El método de la reivindicación 1, en donde proporcionar dicha segunda credencial al usuario en respuesta a la selección de usuario comprende además proporcionar la segunda credencial de identificación al usuario en respuesta a un cierre de sesión de usuario a la conclusión de dicha sesión actual de acceso de usuario al primer aspecto.

13. El método de la reivindicación 12, en donde proporcionar dicha segunda credencial al usuario en respuesta al cierre de sesión de usuario comprende además proporcionar la segunda credencial al usuario para uso durante una sesión exitosa de acceso de usuario al primer aspecto.

14. El método de la reivindicación 1, en donde proporcionar dicha segunda credencial al usuario en respuesta a la selección de usuario comprende además proporcionar la segunda credencial al usuario en respuesta a una solicitud de usuario por la segunda credencial durante dicha sesión actual de acceso de usuario al primer aspecto.

15. El método de la reivindicación 1, en donde proporcionar dicha segunda credencial al usuario en respuesta a la selección de usuario comprende además proporcionar la segunda credencial al usuario en respuesta a un intento de usuario para acceder al segundo aspecto de la información electrónica durante dicha sesión actual de acceso de usuario al primer aspecto.

16. El método de la reivindicación 15, en donde proporcionar dicha segunda credencial al usuario en respuesta al intento de usuario para acceder al segundo aspecto de la información electrónica comprende además proporcionar la segunda credencial al usuario en respuesta a un intento de usuario para acceder a aspectos de transacción preseleccionados sensibles de la información electrónica.

17. El método de la reivindicación 16, en donde proporcionar dicha segunda credencial al usuario en respuesta al intento de usuario para acceder a aspectos de transacción preseleccionados sensibles de la información electrónica comprende además proporcionar la segunda credencial al usuario en respuesta a recibir una indicación del intento del usuario para navegar a los aspectos de transacción preseleccionados sensibles de la información electrónica.

18. Un sistema informático para autentificación segura de usuario en comercio electrónico, que comprende:

medios de almacenamiento de datos que almacenan información electrónica que tiene un primer aspecto y un segundo aspecto;

primeros medios de canal electrónico de comunicación por los que dicho primer aspecto es accesible por un usuario en respuesta a la entrada de una primera credencial conocida por un usuario y por los que dicho segundo aspecto es accesible por el usuario en respuesta a la entrada de una segunda credencial proporcionada al usuario;

segundos medios de canal electrónico de comunicación que son diferentes de los primeros medios de canal electrónico de comunicación para proporcionar la segunda credencial al usuario en una dirección de entrega prerregistrada;

dichos primeros medios de canal electrónico de comunicación están adaptados para permitir al usuario una sesión actual de acceso al primer aspecto de la información electrónica en respuesta a la entrada de la primera credencial y para proporcionar la segunda credencial al usuario en la dirección prerregistrada de entrega por medio del segundo canal electrónico de comunicación en respuesta a la entrada de una selección predeterminada de usuario durante dicha sesión de acceso de usuario al primer aspecto, en donde un cambio en la dirección de entrega del usuario en dicho segundo canal electrónico de comunicación tiene como resultado que se establece una marca en un perfil almacenado que prohíbe proporcionar la segunda credencial al usuario, en donde dicha marca se establece para que caduque tras un periodo de tiempo predeterminado, y dichos primeros medios de canal electrónico de comunicación están adaptados además para permitir al usuario una sesión de acceso al segundo aspecto de la información electrónica por medio del primer canal electrónico de comunicación en respuesta a la entrada de la segunda credencial durante una de dicha sesión actual de acceso de usuario al primer aspecto y una sesión exitosa de acceso de usuario al primer aspecto.

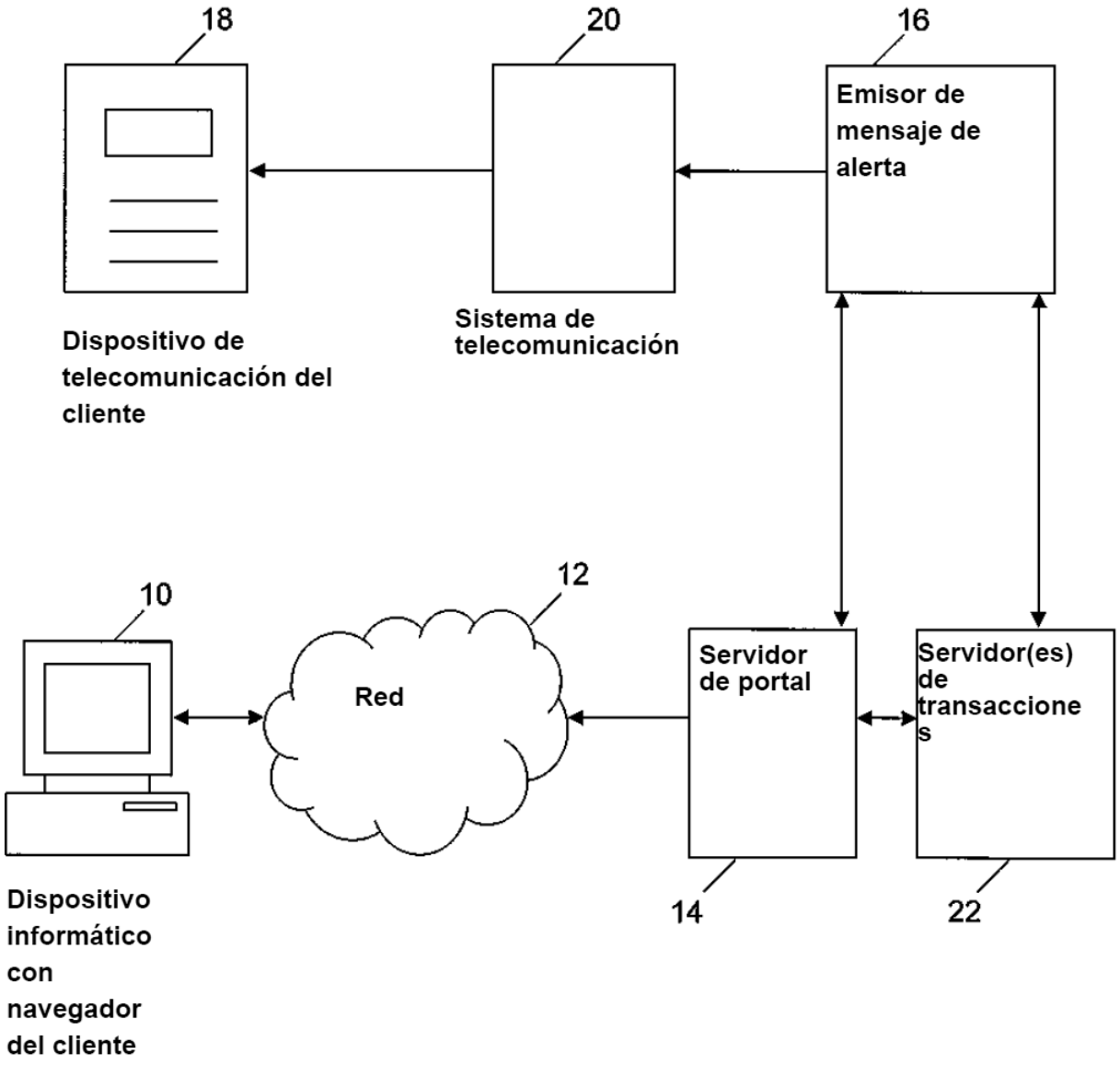
18
20
16
Emisor de mensaje de alerta
Dispositivo de telecomunicación del cliente
Sistema de telecomunicación
12
10
Red
Servidor de portal
Servidor(es) de transacciones
Dispositivo informático con navegador del cliente
14
22

FIG. 1

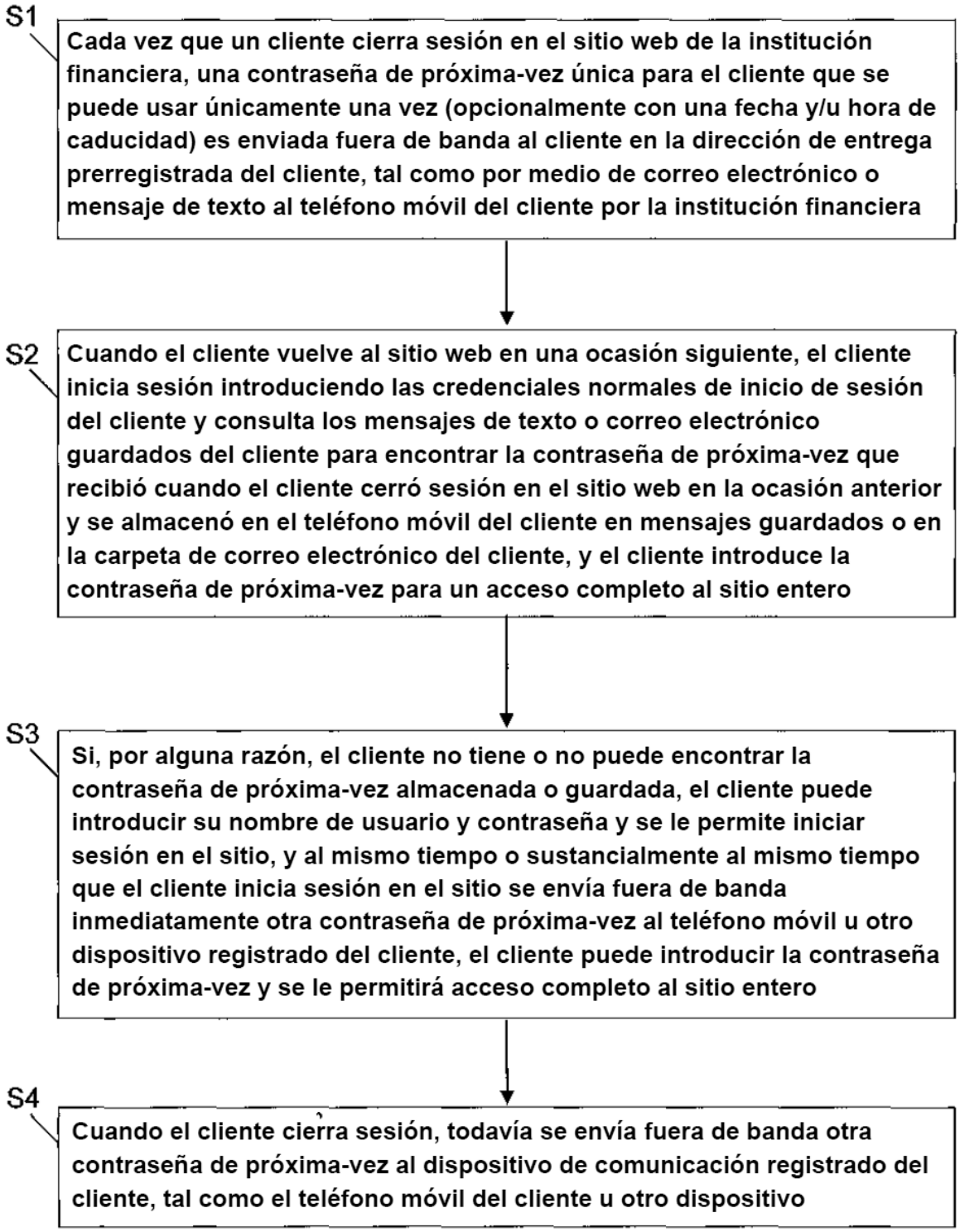
S1
Cada vez que un cliente cierra sesión en el sitio web de la institución financiera, una contraseña de próxima-vez única para el cliente que se puede usar únicamente una vez (opcionalmente con una fecha y/u hora de caducidad) es enviada fuera de banda al cliente en la dirección de entrega prerregistrada del cliente, tal como por medio de correo electrónico o mensaje de texto al teléfono móvil del cliente por la institución financiera
S2
Cuando el cliente vuelve al sitio web en una ocasión siguiente, el cliente inicia sesión introduciendo las credenciales normales de inicio de sesión del cliente y consulta los mensajes de texto o correo electrónico guardados del cliente para encontrar la contraseña de próxima-vez que recibió cuando el cliente cerró sesión en el sitio web en la ocasión anterior y se almacenó en el teléfono móvil del cliente en mensajes guardados o en la carpeta de correo electrónico del cliente, y el cliente introduce la contraseña de próxima-vez para un acceso completo al sitio entero
S3
Si, por alguna razón, el cliente no tiene o no puede encontrar la contraseña de próxima-vez almacenada o guardada, el cliente puede introducir su nombre de usuario y contraseña y se le permite iniciar sesión en el sitio, y al mismo tiempo o sustancialmente al mismo tiempo que el cliente inicia sesión en el sitio se envía fuera de banda inmediatamente otra contraseña de próxima-vez al teléfono móvil u otro dispositivo registrado del cliente, el cliente puede introducir la contraseña de próxima-vez y se le permitirá acceso completo al sitio entero
S4
Cuando el cliente cierra sesión, todavía se envía fuera de banda otra contraseña de próxima-vez al dispositivo de comunicación registrado del cliente, tal como el teléfono móvil del cliente u otro dispositivo

FIG. 2

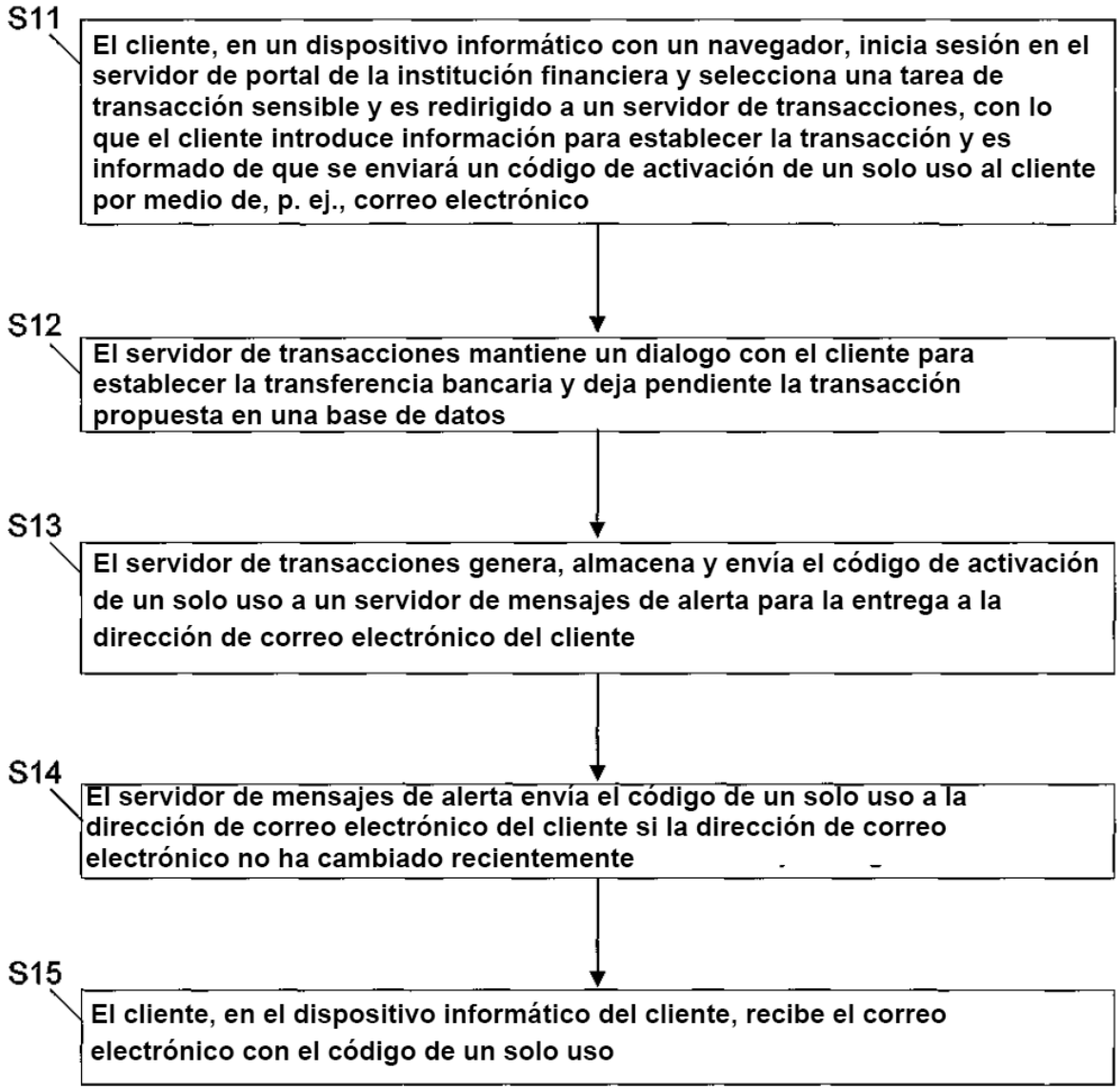
S11
El cliente, en un dispositivo informático con un navegador, inicia sesión en el servidor de portal de la institución financiera y selecciona una tarea de transacción sensible y es redirigido a un servidor de transacciones, con lo que el cliente introduce información para establecer la transacción y es informado de que se enviará un código de activación de un solo uso al cliente por medio de, p. ej., correo electrónico
S12
El servidor de transacciones mantiene un dialogo con el cliente para establecer la transferencia bancaria y deja pendiente la transacción propuesta en una base de datos
S13
El servidor de transacciones genera, almacena y envía el código de activación de un solo uso a un servidor de mensajes de alerta para la entrega a la dirección de correo electrónico del cliente
S14
El servidor de mensajes de alerta envía el código de un solo uso a la dirección de correo electrónico del cliente si la dirección de correo electrónico no ha cambiado recientemente
S15
El cliente, en el dispositivo informático del cliente, recibe el correo electrónico con el código de un solo uso

FIG. 3

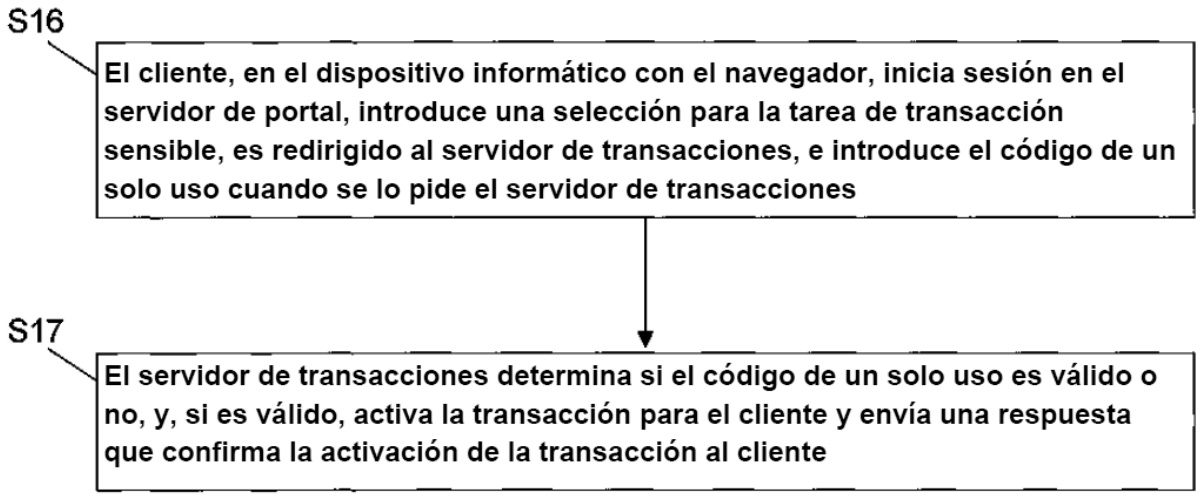
S16
El cliente, en el dispositivo informático con el navegador, inicia sesión en el servidor de portal, introduce una selección para la tarea de transacción sensible, es redirigido al servidor de transacciones, e introduce el código de un solo uso cuando se lo pide el servidor de transacciones
S17
El servidor de transacciones determina si el código de un solo uso es válido o no, y, si es válido, activa la transacción para el cliente y envía una respuesta que confirma la activación de la transacción al cliente

FIG. 4

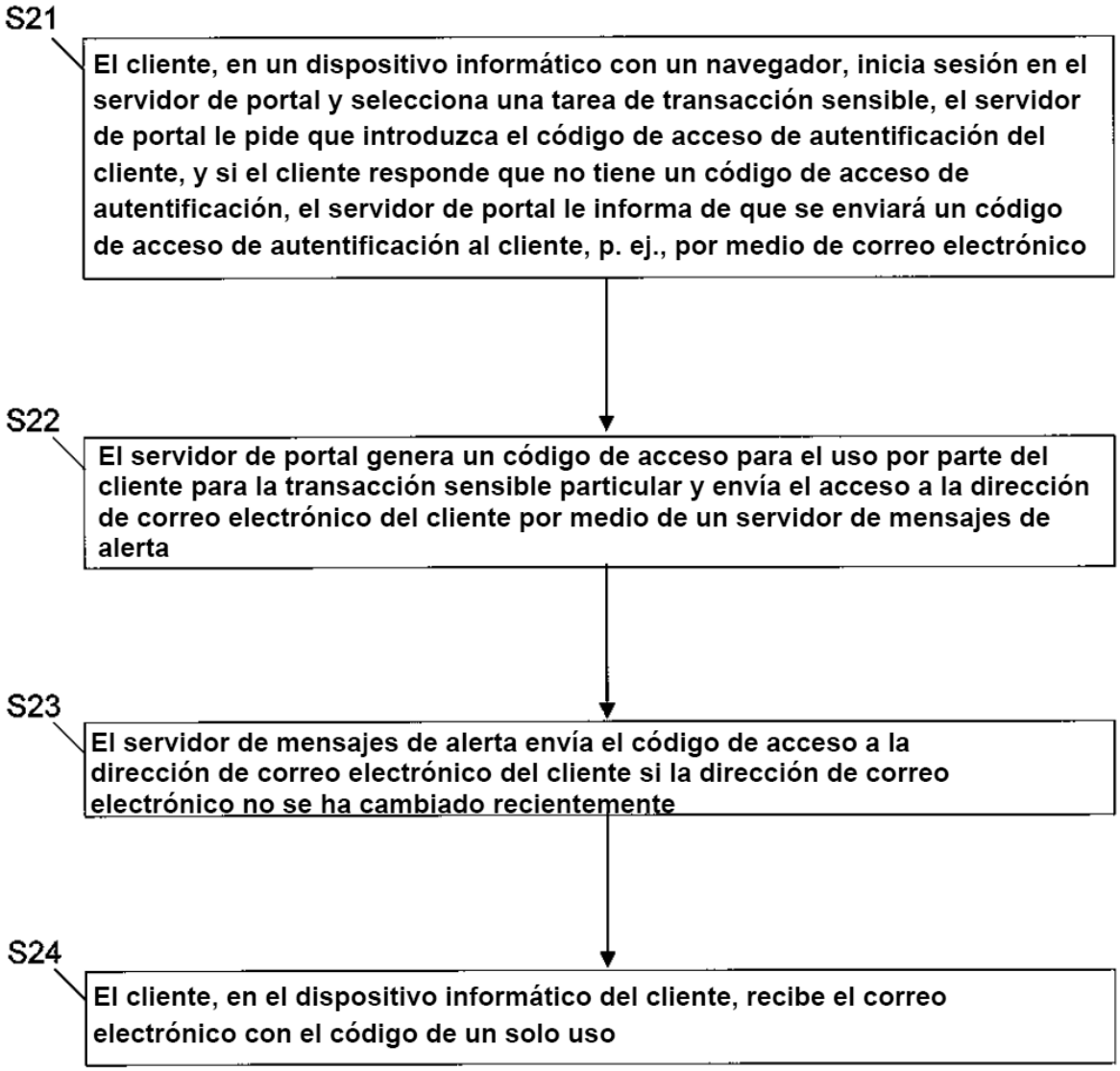
S21
El cliente, en un dispositivo informático con un navegador, inicia sesión en el servidor de portal y selecciona una tarea de transacción sensible, el servidor de portal le pide que introduzca el código de acceso de autentificación del cliente, y si el cliente responde que no tiene un código de acceso de autentificación, el servidor de portal le informa de que se enviará un código de acceso de autentificación al cliente, p. ej., por medio de correo electrónico
S22
El servidor de portal genera un código de acceso para el uso por parte del cliente para la transacción sensible particular y envía el acceso a la dirección de correo electrónico del cliente por medio de un servidor de mensajes de alerta
S23
El servidor de mensajes de alerta envía el código de acceso a la dirección de correo electrónico del cliente si la dirección de correo electrónico no se ha cambiado recientemente
S24
El cliente, en el dispositivo informático del cliente, recibe el correo electrónico con el código de un solo uso

FIG. 5

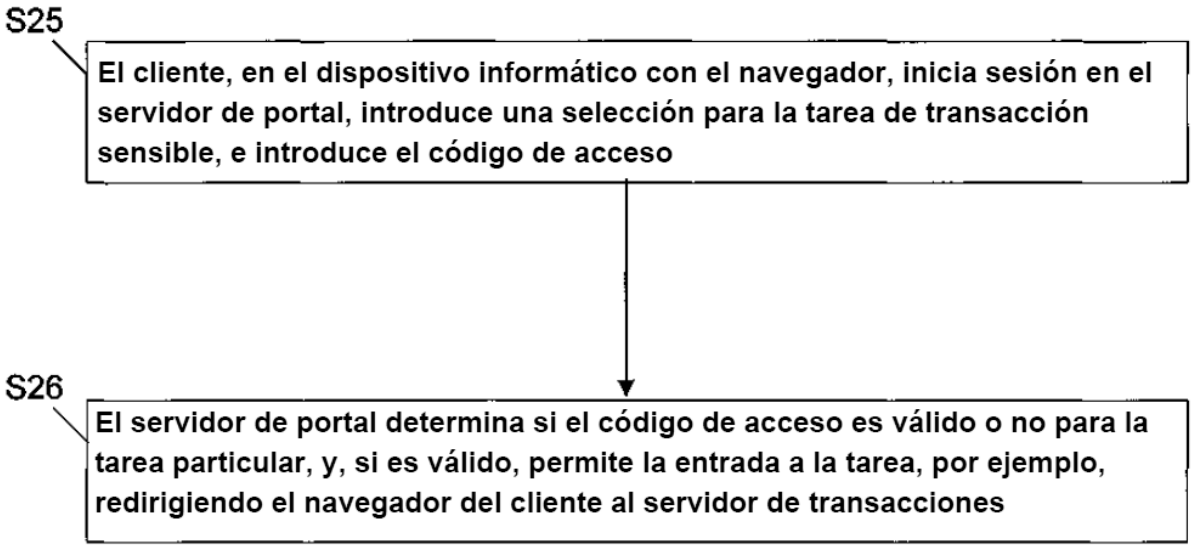
S25
El cliente, en el dispositivo informático con el navegador, inicia sesión en el servidor de portal, introduce una selección para la tarea de transacción sensible, e introduce el código de acceso
S26
El servidor de portal determina si el código de acceso es válido o no para la tarea particular, y, si es válido, permite la entrada a la tarea, por ejemplo, redirigiendo el navegador del cliente al servidor de transacciones

FIG. 6

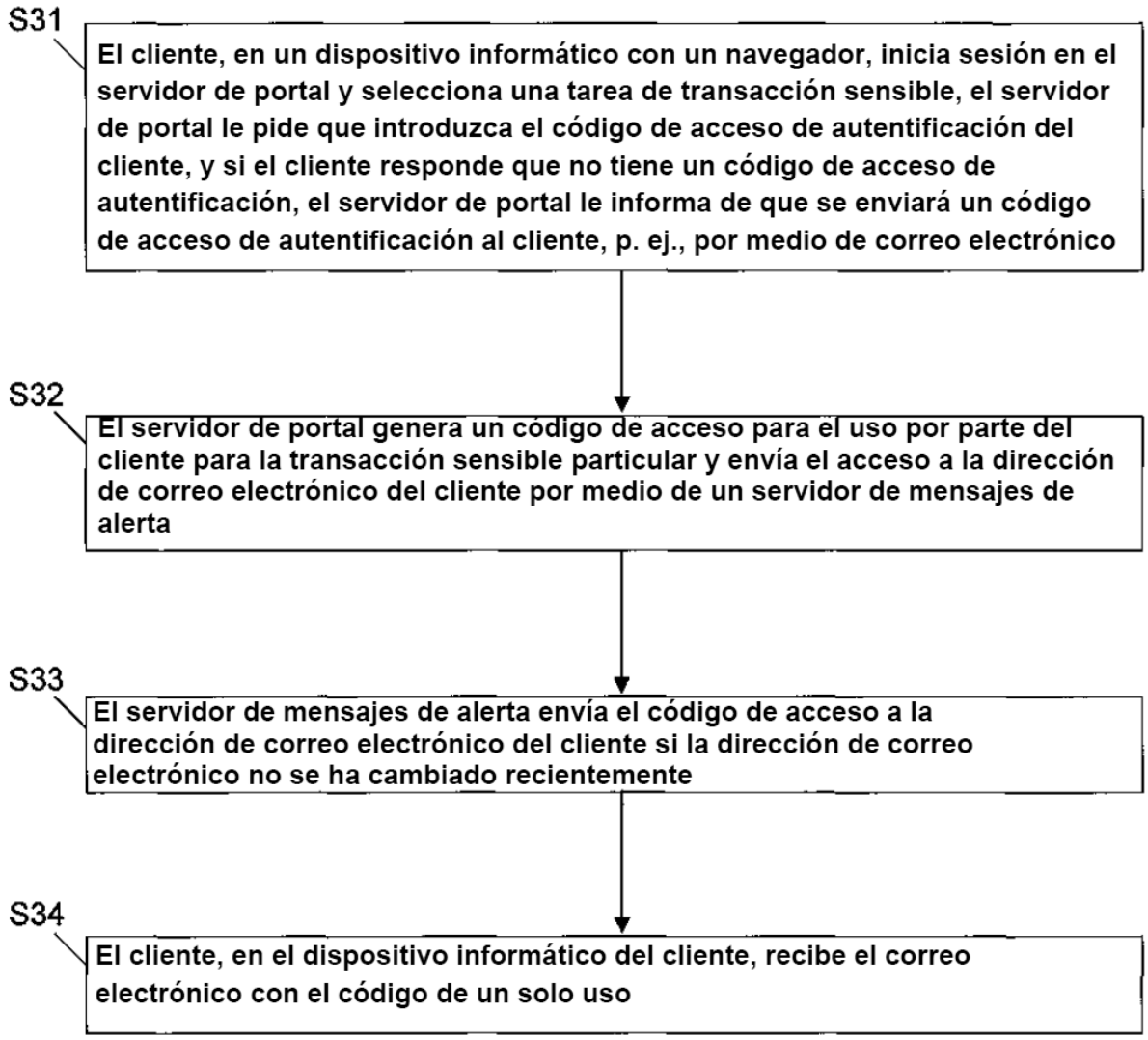
S31
El cliente, en un dispositivo informático con un navegador, inicia sesión en el servidor de portal y selecciona una tarea de transacción sensible, el servidor de portal le pide que introduzca el código de acceso de autentificación del cliente, y si el cliente responde que no tiene un código de acceso de autentificación, el servidor de portal le informa de que se enviará un código de acceso de autentificación al cliente, p. ej., por medio de correo electrónico
S32
El servidor de portal genera un código de acceso para el uso por parte del cliente para la transacción sensible particular y envía el acceso a la dirección de correo electrónico del cliente por medio de un servidor de mensajes de alerta
S33
El servidor de mensajes de alerta envía el código de acceso a la dirección de correo electrónico del cliente si la dirección de correo electrónico no se ha cambiado recientemente
S34
El cliente, en el dispositivo informático del cliente, recibe el correo electrónico con el código de un solo uso

FIG. 7

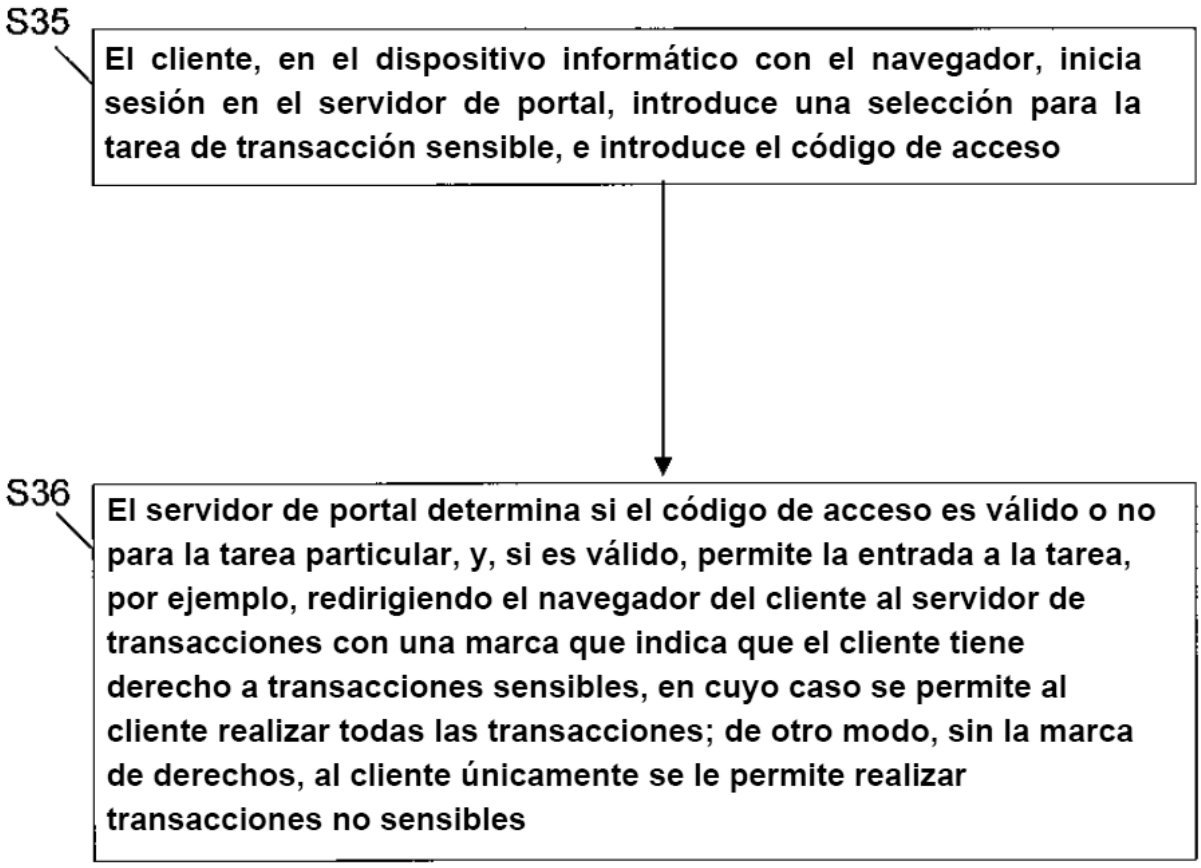
S35
El cliente, en el dispositivo informático con el navegador, inicia sesión en el servidor de portal, introduce una selección para la tarea de transacción sensible, e introduce el código de acceso
S36
El servidor de portal determina si el código de acceso es válido o no para la tarea particular, y, si es válido, permite la entrada a la tarea, por ejemplo, redirigiendo el navegador del cliente al servidor de transacciones con una marca que indica que el cliente tiene derecho a transacciones sensibles, en cuyo caso se permite al cliente realizar todas las transacciones; de otro modo, sin la marca de derechos, al cliente únicamente se le permite realizar transacciones no sensibles

FIG. 8

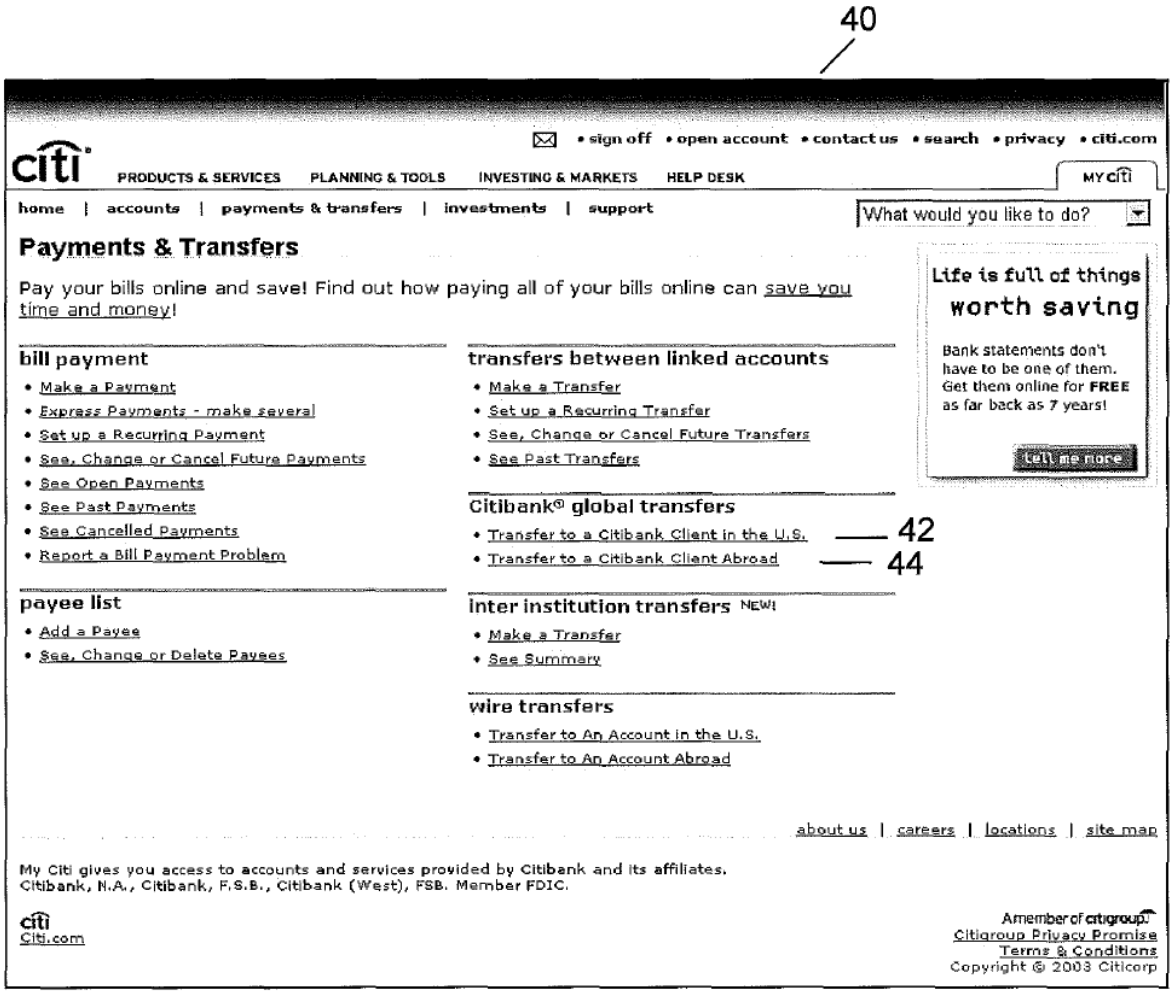
40
• sign off • open account • contact us • search • privacy • citi.com
citi
PRODUCTS & SERVICES
PLANNING & TOOLS
INVESTING & MARKETS
HELP DESK
MY citi
home | accounts | payments & transfers | investments | support
What would you like to do?
Payments & Transfers
Pay your bills online and save! Find out how paying all of your bills online can save you time and money!
bill payment
• Make a Payment
• Express Payments - make several
• Set up a Recurring Payment
• See, Change or Cancel Future Payments
• See Open Payments
• See Past Payments
• See Cancelled Payments
• Report a Bill Payment Problem
payee list
• Add a Payee
• See, Change or Delete Payees
transfers between linked accounts
• Make a Transfer
• Set up a Recurring Transfer
• See, Change or Cancel Future Transfers
• See Past Transfers
Citibank® global transfers
• Transfer to a Citibank Client in the U.S.
• Transfer to a Citibank Client Abroad
42
44
inter institution transfers NEW!
• Make a Transfer
• See Summary
wire transfers
• Transfer to An Account in the U.S.
• Transfer to An Account Abroad
Life is full of things worth saving
Bank statements don't have to be one of them. Get them online for FREE as far back as 7 years!
Tell me more
about us | careers | locations | site map
My Citi gives you access to accounts and services provided by Citibank and its affiliates.
Citibank, N.A., Citibank, F.S.B., Citibank (West), FSB. Member FDIC.
citi
Citi.com
A member of citigroup
Citigroup Privacy Promise
Terms & Conditions
Copyright © 2003 Citicorp

FIG. 9

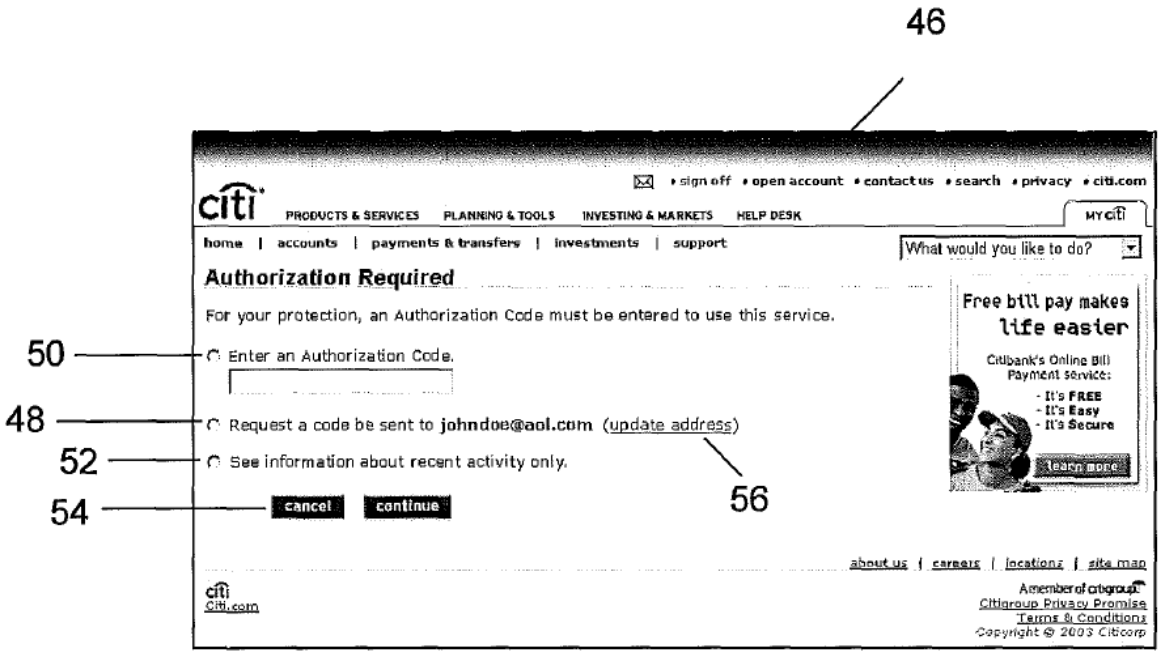
46
sign off
open account
contact us
search
privacy
citi.com
citi
PRODUCTS & SERVICES
PLANNING & TOOLS
INVESTING & MARKETS
HELP DESK
MY citi
home | accounts | payments & transfers | investments | support
What would you like to do?
Authorization Required
For your protection, an Authorization Code must be entered to use this service.
50
Enter an Authorization Code.
48
Request a code be sent to johndoe@aol.com (update address)
52
See information about recent activity only.
54
cancel
continue
56
Free bill pay makes life easier
Citibank's Online Bill Payment service:
- It's FREE
- It's Easy
- It's Secure
learn more
about us | careers | locations | site map
citi
Citi.com
A member of citigroup
Citigroup Privacy Promise
Terms & Conditions
Copyright © 2003 Citicorp

FIG. 10

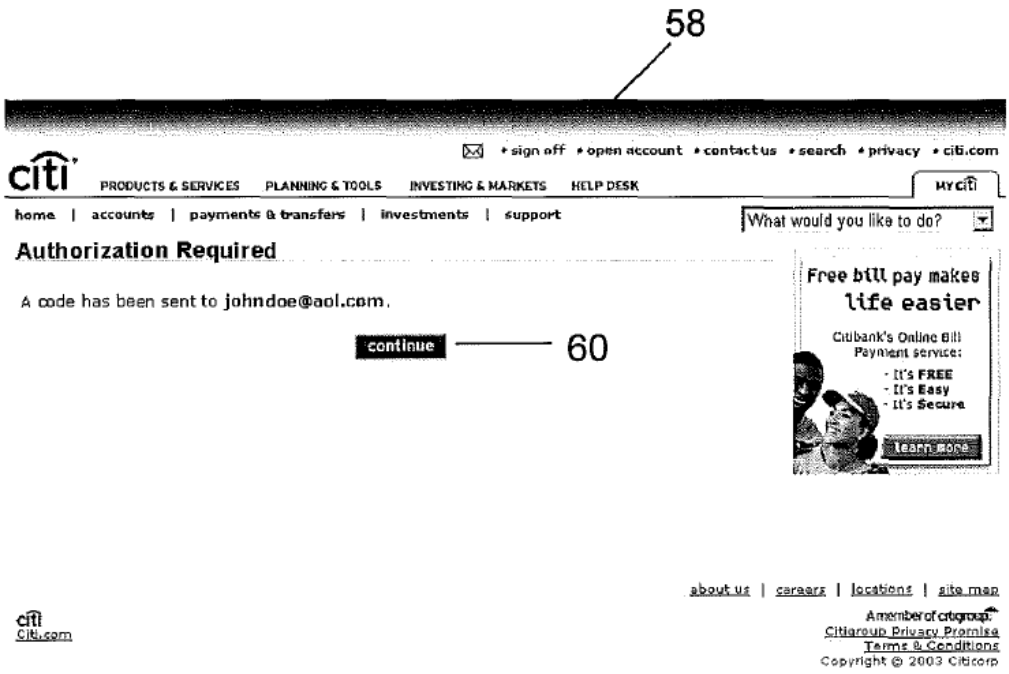
58
sign off
open account
contact us
search
privacy
citi.com
citi
PRODUCTS & SERVICES
PLANNING & TOOLS
INVESTING & MARKETS
HELP DESK
MY citi
home | accounts | payments & transfers | investments | support
What would you like to do?
Authorization Required
A code has been sent to johndoe@aol.com.
continue
60
Free bill pay makes life easier
Citibank's Online Bill Payment service:
- It's FREE
- It's Easy
- It's Secure
learn more
about us | careers | locations | site map
citi
Citi.com
A member of citigroup
Citigroup Privacy Promise
Terms & Conditions
Copyright © 2003 Citicorp

FIG. 11

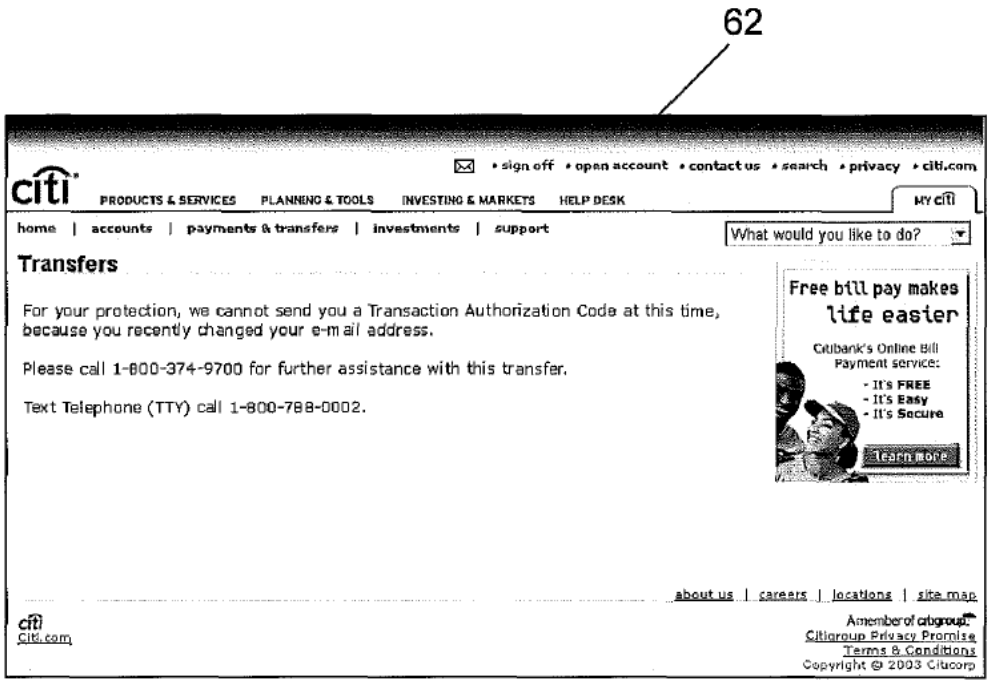
62
citi
• sign off • open account • contact us • search • privacy • citi.com
PRODUCTS & SERVICES
PLANNING & TOOLS
INVESTING & MARKETS
HELP DESK
MY citi
home | accounts | payments & transfers | investments | support
What would you like to do?
Transfers
For your protection, we cannot send you a Transaction Authorization Code at this time, because you recently changed your e-mail address.
Please call 1-800-374-9700 for further assistance with this transfer.
Text Telephone (TTY) call 1-800-788-0002.
Free bill pay makes life easier
Citibank's Online Bill Payment service:
- It's FREE
- It's Easy
- It's Secure
learn more
about us | careers | locations | site map
citi
Citi.com
A member of citigroup
Citigroup Privacy Promise
Terms & Conditions
Copyright © 2003 Citicorp

FIG. 12

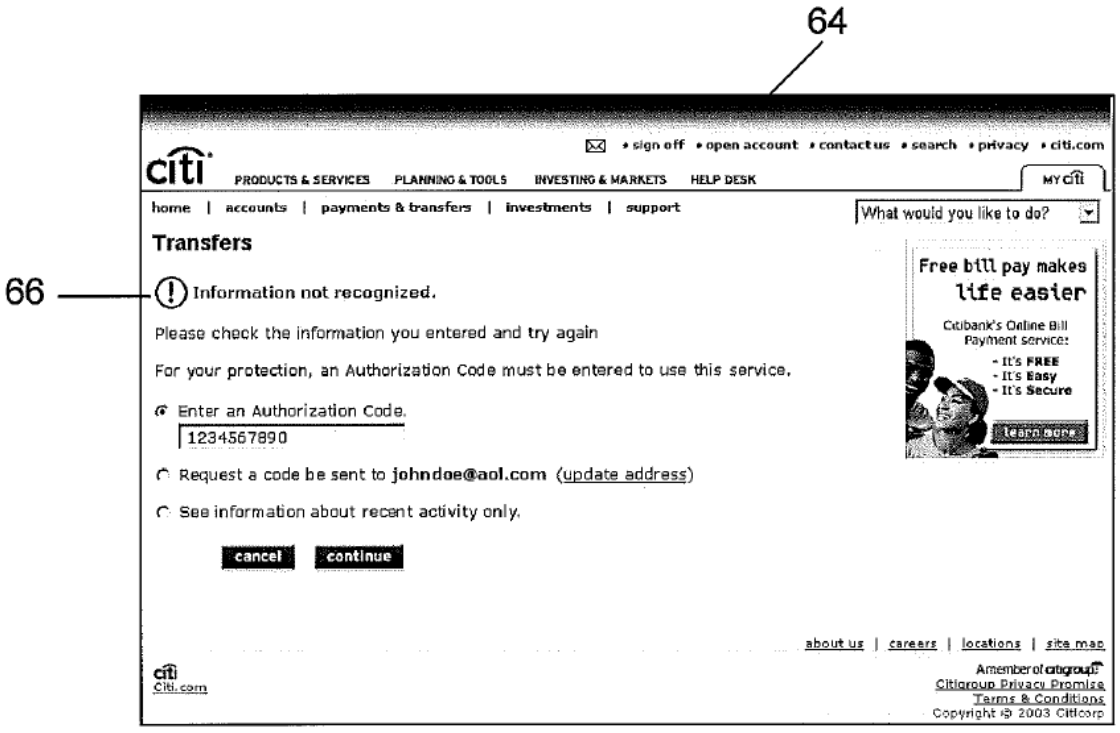
64
66
sign off
open account
contact us
search
privacy
citi.com
citi
PRODUCTS & SERVICES
PLANNING & TOOLS
INVESTING & MARKETS
HELP DESK
MY citi
home | accounts | payments & transfers | investments | support
What would you like to do?
Transfers
Information not recognized.
Please check the information you entered and try again
For your protection, an Authorization Code must be entered to use this service.
Enter an Authorization Code.
1234567890
Request a code be sent to johndoe@aol.com (update address)
See information about recent activity only.
cancel
continue
Free bill pay makes life easier
Citibank's Online Bill Payment service:
- It's FREE
- It's Easy
- It's Secure
learn more
about us | careers | locations | site map
citi
Citi.com
A member of citigroup
Citigroup Privacy Promise
Terms & Conditions
Copyright © 2003 Citicorp

FIG. 13

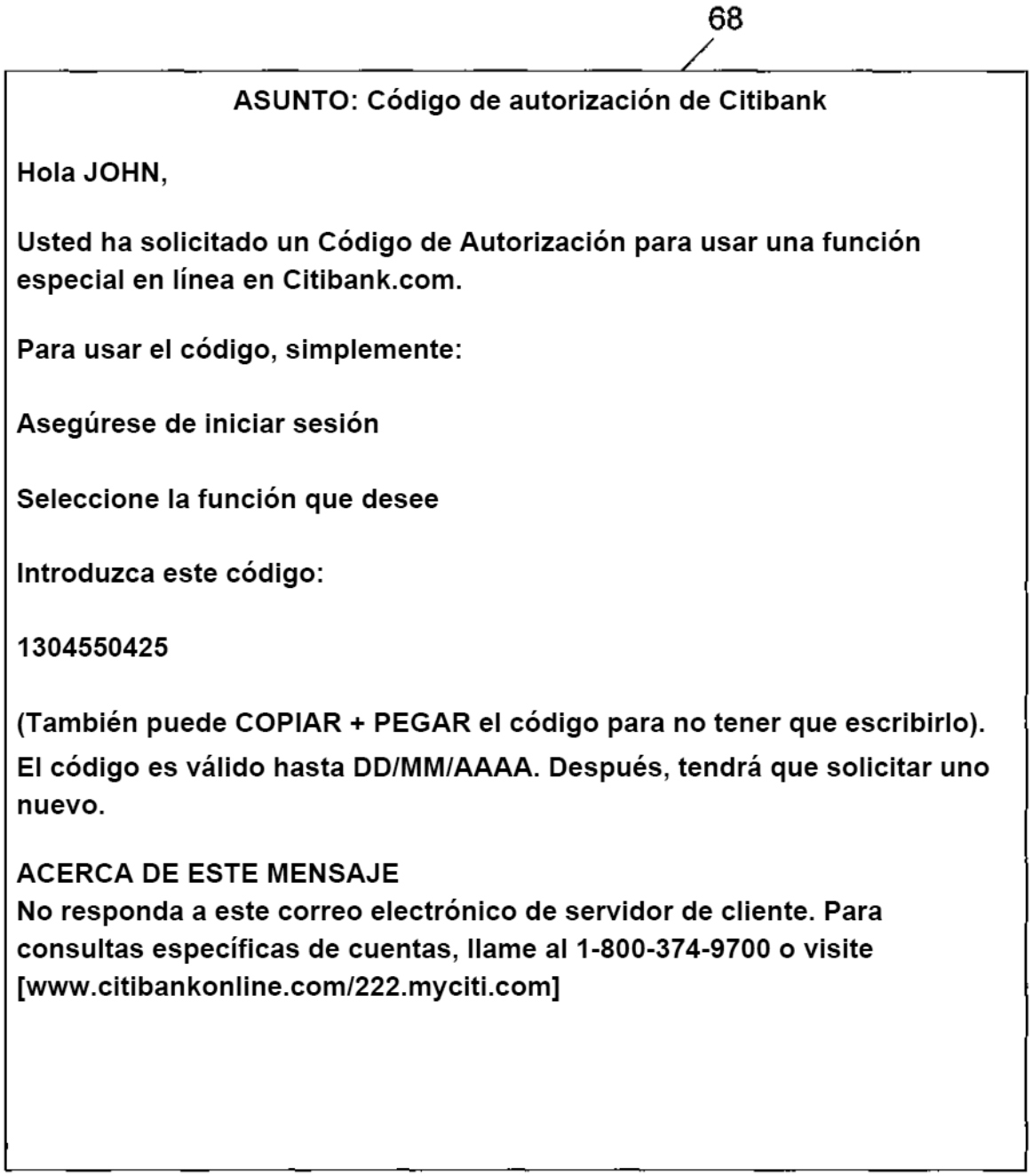
68
ASUNTO: Código de autorización de Citibank
Hola JOHN,
Usted ha solicitado un Código de Autorización para usar una función especial en línea en Citibank.com.
Para usar el código, simplemente:
Asegúrese de iniciar sesión
Seleccione la función que desee
Introduzca este código:
1304550425
(También puede COPIAR + PEGAR el código para no tener que escribirlo).
El código es válido hasta DD/MM/AAAA. Después, tendrá que solicitar uno nuevo.
ACERCA DE ESTE MENSAJE
No responda a este correo electrónico de servidor de cliente. Para consultas específicas de cuentas, llame al 1-800-374-9700 o visite [www.citibankonline.com/222.myciti.com]

FIG. 14

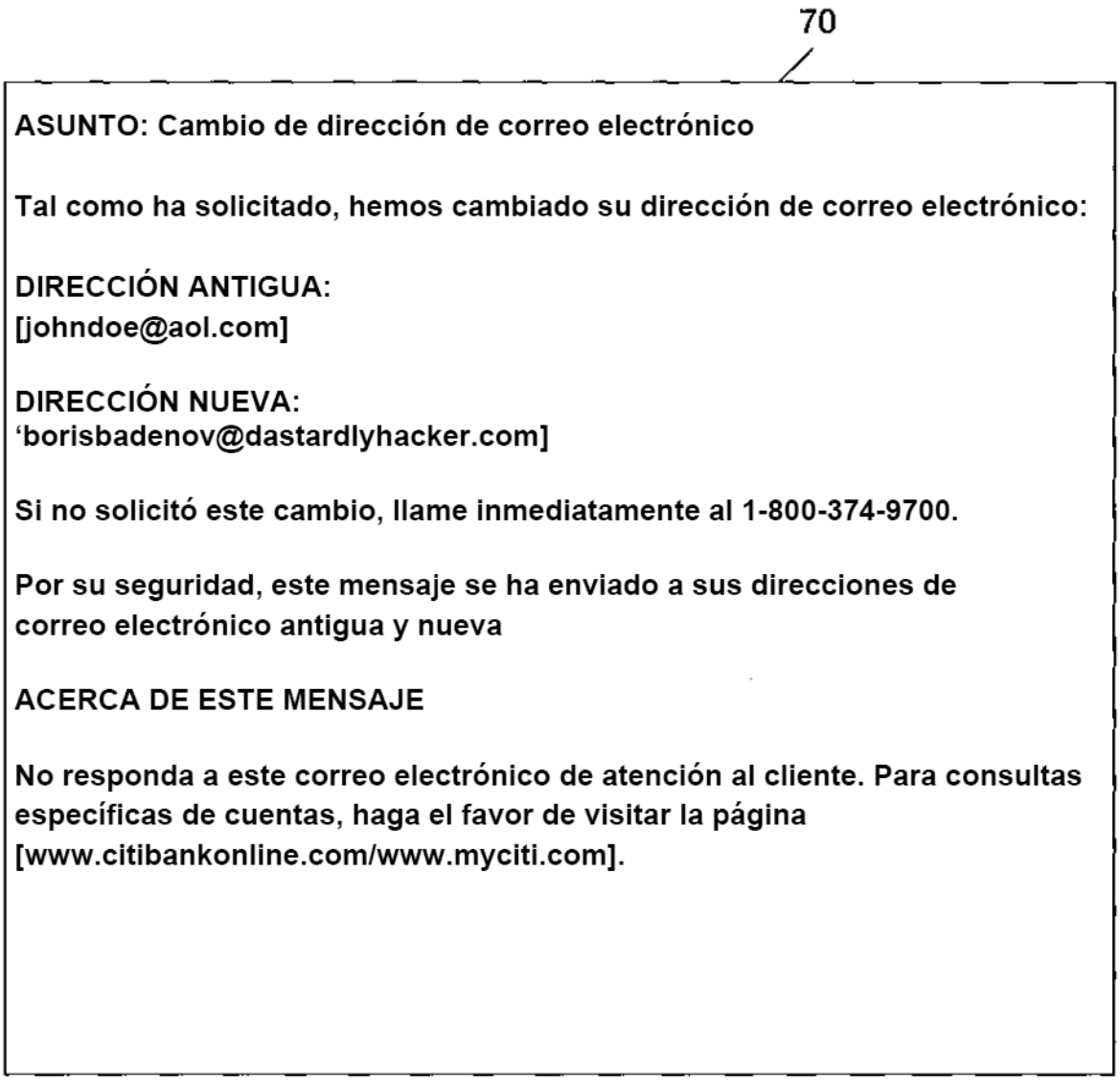
70
ASUNTO: Cambio de dirección de correo electrónico
Tal como ha solicitado, hemos cambiado su dirección de correo electrónico:
DIRECCIÓN ANTIGUA:
[johndoe@aol.com]
DIRECCIÓN NUEVA:
'borisbadenov@dastardlyhacker.com]
Si no solicitó este cambio, llame inmediatamente al 1-800-374-9700.
Por su seguridad, este mensaje se ha enviado a sus direcciones de correo electrónico antigua y nueva
ACERCA DE ESTE MENSAJE
No responda a este correo electrónico de atención al cliente. Para consultas específicas de cuentas, haga el favor de visitar la página [www.citibankonline.com/www.myciti.com].

FIG. 15

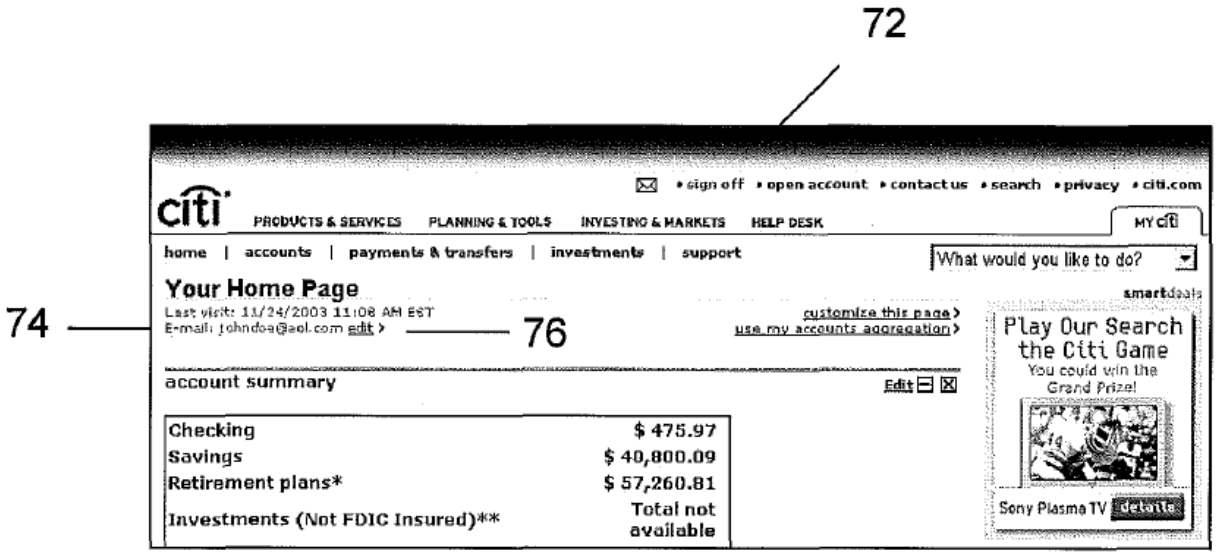
72
74
76
citi
sign off
open account
contact us
search
privacy
citi.com
PRODUCTS & SERVICES
PLANNING & TOOLS
INVESTING & MARKETS
HELP DESK
MY citi
home | accounts | payments & transfers | investments | support
What would you like to do?
Your Home Page
Last visit: 11/24/2003 11:08 AM EST
E-mail: johndoe@aol.com edit
customize this page
use my accounts aggregation
smartdeals
Play Our Search the Citi Game
You could win the Grand Prize!
Sony Plasma TV
Details
account summary
Edit
Checking $ 475.97
Savings $ 40,800.09
Retirement plans* $ 57,260.81
Investments (Not FDIC Insured)** Total not available

FIG. 16

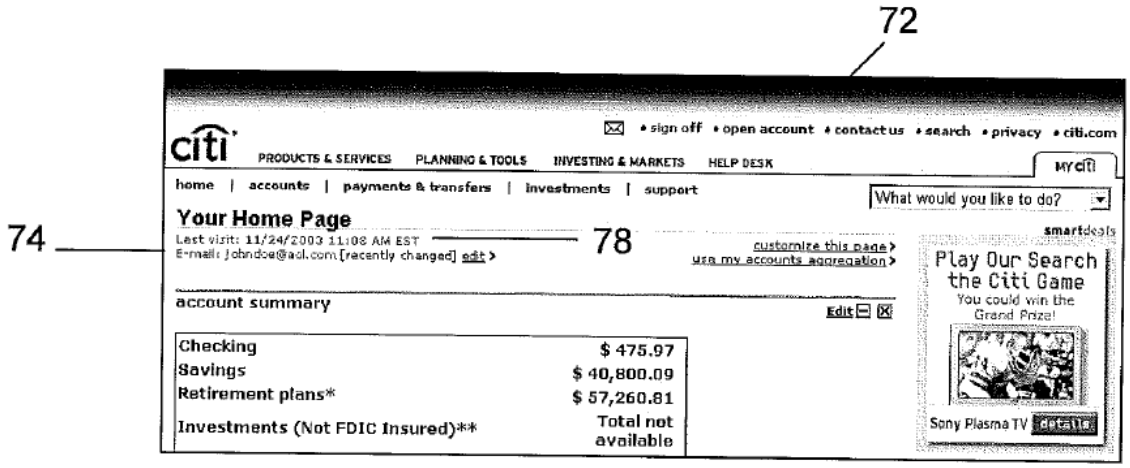
72
74
78
citi
• sign off • open account • contact us • search • privacy • citi.com
PRODUCTS & SERVICES
PLANNING & TOOLS
INVESTING & MARKETS
HELP DESK
MYciti
home | accounts | payments & transfers | investments | support
What would you like to do?
Your Home Page
Last visit: 11/24/2003 11:08 AM EST
E-mail: johndoe@aol.com [recently changed] edit >
customize this page >
use my accounts aggregation >
account summary
Edit
Checking $ 475.97
Savings $ 40,800.09
Retirement plans* $ 57,260.81
Investments (Not FDIC Insured)** Total not available
smartdeals
Play Our Search the Citi Game
You could win the Grand Prize!
Sony Plasma TV details

FIG. 17