(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 753 246**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **09.10.2013 E 13382397 (1)**

(97) Fecha y número de publicación de la concesión europea: **14.08.2019 EP 2860934**

(54) Título: **Un método implementado en ordenador para impedir ataques contra sistemas de autorización y productos de programas de ordenador del mismo**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.04.2020

(73) Titular/es:

TELEFONICA DIGITAL ESPAÑA, S.L.U. (100.0%)
Gran Via 28
28013 Madrid, ES

(72) Inventor/es:

ALONSO CEBRIÁN, JOSÉ MARÍA;
BARROSO BERRUETA, DAVID;
PALAZÓN ROMERO, JOSÉ MARÍA y
GUZMÁN SACRISTÁN, ANTONIO

(74) Agente/Representante:

ARIZTI ACHA, Monica

DESCRIPCIÓN

Un método implementado en ordenador para impedir ataques contra sistemas de autorización y productos de programas de ordenador del mismo

Campo de la técnica

La presente invención se dirige, en general, a sistemas de autenticación y autorización y, más particularmente, a un método implementado en ordenador y productos de programa de ordenador para impedir ataques contra los sistemas de autorización en los que se controlan el acceso a los diferentes recursos y las acciones definidas para un usuario, por ejemplo, por parte de un proveedor de servicios.

Antecedentes de la invención

En los últimos años, el mercado de la detección de fraudes en la red se ha incrementado considerablemente, de modo que la innovación en los procesos de autenticación y autorización ha llegado a tener gran importancia.

La creciente complejidad de las aplicaciones ha conducido a la adopción de muchas técnicas de seguridad crecientemente sofisticadas. Una de las clasificaciones que se puede proponer para el estudio de estas técnicas de seguridad permite la distinción entre soluciones de autenticación y soluciones de autorización. Las técnicas de autenticación están diseñadas para verificar que una persona es la que reivindica ser. Para añadir más fiabilidad en la verificación de que realmente la persona corresponde a la identidad que está siendo comprobada, se pueden tomar muchos esquemas de autenticación alternativos o se puede extender el número de factores para elaborar esta autenticación. Una vez que se identifica a un usuario, ha de determinarse a qué recursos puede acceder y cómo se puede realizar este acceso. Esta es la tarea de los modelos de autorización.

Hay muchas soluciones diseñadas para reforzar los procesos de autenticación y, por extensión, para fortificar los procesos de autorización. Hay esquemas de autorización que permiten flexibilidad y robustez en la asignación de permisos a los usuarios para asegurar un acceso seguro a los recursos del sistema. Sin embargo, hay amenazas tales como las técnicas denominadas de “Man in the Browser” (MitB) (“Persona en el navegador”) que no pueden ser desbaratadas aun adoptando cualquiera de los esquemas existentes para la autenticación/autorización, o la solución es demasiado cara para poder permitírselo. Estas amenazas afectan directamente a la forma en que se realiza el acceso a recursos específicos. Un método para acometer estas amenazas implica el diseño de mecanismos de seguridad completamente nuevos. Estos mecanismos deben garantizar que una vez que se ha verificado la identidad del usuario y se ha comprobado el nivel de autorización a un recurso para este usuario, las acciones realizadas por el usuario de ese recurso no son interceptadas y modificadas por cualquier atacante.

Dentro de la categoría de autorización, se incluyen diferentes técnicas que facilitan el acceso a varios recursos del sistema. La información del papel que juega (role) el usuario, los datos de control de acceso proporcionados cuando el usuario es autenticado, son ejemplos de información que se puede usar para determinar a quién dar acceso a qué recursos y cómo ha de garantizarse este acceso. Finalmente, la determinación de qué debería ser accedido por qué usuarios, se especificará para cada aplicación. Por esta razón, a veces será difícil proporcionar un esquema de autorización general. Será necesario definir una lógica específica de la aplicación para determinar qué usuarios pueden acceder y cómo realizan estos accesos. A partir de esta idea, hay muchas soluciones que proponen esquemas seguros y flexibles para la implementación de la autorización. En todas estas soluciones, la seguridad se debe garantizar mediante la selección correcta del mecanismo de autenticación y una implementación correcta del esquema de autorización seleccionado.

Algunas de las soluciones proporcionan la flexibilidad definiendo su propio SDK para fomentar el uso de sus esquemas para autenticación/autorización. Hoy en día, la mayor parte de los SDK se basan en conceptos introducidos por OAuth y no suponen un riesgo por sí mismos. Esto es aplicable al Microsoft Live Connect, Facebook PHP SDK y Windows 8 SDK Authentication Broker. Si existen, las amenazas deberían proceder de un uso eficiente de estos SDK. De hecho, independientemente de las amenazas derivadas de una pobre implementación del esquema elegido, la mayor parte de las amenazas que se pueden definir sobre un sistema de autorización coinciden con las amenazas definidas para los sistemas de autenticación. Esta coincidencia tiene que ver con el mal uso de las credenciales usadas para gestionar permisos que garanticen el acceso a los recursos [2], [5].

En [2] se definen cuatro niveles diferentes en términos de las consecuencias de errores de autenticación y autorización y mala utilización de las credenciales. El nivel 1 es el nivel más bajo (el más inseguro) y el nivel 4 es el más alto.

- Nivel 1 - Un atacante puede realizar intentos de registro repetidos suponiendo valores posibles de la autenticación de la prueba (token). Un atacante también es capaz de reproducir mensajes previamente capturados (entre un usuario legítimo y un verificador) para autenticarse como ese usuario al verificador. El

National Institute of Standard and Technology (NIST) recomendó el uso de una autenticación mono o multi-factor sin ninguna demostración de identidad para proporcionar una protección contra estos ataques de suposición y reproducción en línea.

- Nivel 2 - Un atacante puede escuchar pasivamente el protocolo de autenticación para capturar información que puede usar en un ataque activo posterior para enmascararse como el usuario. El NIST recomienda el uso de una autenticación mono o multi-factor para proporcionar protección contra estos ataques de escuchas a escondidas o espionaje y todos los ataques del nivel 1.
- Nivel 3 - El atacante se coloca entre el usuario y el verificador de modo que puede interceptar y alterar el contenido de los mensajes del protocolo de autenticación. El atacante típicamente imita al verificador para el usuario e imita simultáneamente al usuario para el verificador. La realización de un intercambio activo con ambas partes simultáneamente puede permitir al atacante usar los mensajes de autenticación enviados por una parte legítima para autenticarse con éxito ante la otra. El NIST recomienda el uso de una autenticación multi-factor y el amplio uso de OTP. También sugiere que un token usado para la autenticación sea desbloqueado por el usuario usando una palabra clave o biométrica. La adopción de estas soluciones proporciona protección contra los ataques de imitación del verificador, ataques MitM y ataques del nivel 2.
- Nivel 4 - Un atacante es capaz de situarse entre un usuario y un verificador posteriormente a un intercambio de autenticación con éxito entre estas dos últimas partes. El atacante es capaz de aparentar un usuario para el verificador, o viceversa, para controlar el intercambio de datos de la sesión. Por otro lado, el atacante puede comprometer o explotar en otra manera los tokens de autenticación y puede interceptar todas las comunicaciones de entrada o salida desde el dispositivo (ataques de Man-in-the-device (MitD) o “Persona en el dispositivo” o ataques de Man-in-the-Browser (MitB)). El atacante puede hacer esto infectando el sistema con software maligno. El NIST sugiere el empleo de autenticación multi-factor con hardware (tokens de hardware) resistente contra manipulaciones certificado por FIPS-140-2 [4] para obtener protección contra estos ataques de apropiación de la sesión y los ataques del nivel 3.

Para los tres primeros niveles, los ataques y las soluciones existentes se enfocan ambas en la forma de verificación de la identidad del usuario. En el nivel 4, el NIST propone el uso de soluciones contra la apropiación de la sesión y otros ataques sobre los procesos de autenticación. Esta apropiación de la sesión implica que un atacante se aprovecha del intercambio legítimo de credenciales que un usuario realiza para cumplir con el proceso de autenticación. Una vez que se lleva a cabo esta validación, el atacante se interpone entonces en la comunicación que tiene lugar. Este tipo de ataque se puede implementar de dos maneras: actuando activamente, apropiándose de la conexión y dejando fuera de ella al usuario legítimo, o permaneciendo oculto modificando el contenido de la comunicación transparentemente para el usuario. Cualquiera que sea la implementación de este ataque, es importante observar, que este es un ataque dirigido a la quiebra del sistema de autorización, dejando intacto, aunque inútil, el sistema de autenticación. Aunque hay alternativas para proteger activamente sistemas frente a esta amenaza, no hay una solución adecuada para mitigar los efectos del ataque una vez que el dispositivo desde el que se requiere el acceso a los recursos, se ha cometido.

El NIST sugiere el empleo de hardware (tokens de hardware) resistente contra manipulaciones certificado por FIPS-140-2 [4]. El uso de estos dispositivos proporciona a los usuarios la capacidad para generar una palabra clave de uso único (palabra clave de una vez, OTP de “one time password”) para probar su identidad en cada transacción. Además, hay implementaciones de hardware de esos tokens que pueden generar otras OTP codificadas para contener información sobre cómo concretar una transacción específica.

Se pueden definir diferentes criterios para establecer una comparación entre los esquemas de autenticación/autorización. En [1] los autores sugieren la necesidad de definir los criterios para realizar una comparación efectiva. Estos aspectos son: seguridad, capacidad de uso y complejidad de la implementación (capacidad de despliegue). Este documento presenta un estudio intensivo para instrumentar la comparación a través de la definición de las mediciones. La tabla a continuación resume las mediciones definidas para cada criterio.

Capacidad de uso	Memoria sin esfuerzo Escalable para los usuarios Nada que transportar Sin esfuerzo físico Fácil de aprender Eficiente en el uso Errores infrecuentes Fácil recuperación de una pérdida
Capacidad de despliegue	Accesible Coste por usuario despreciable Compatible con el servidor Compatible con navegador Maduro No propietario

Seguridad	Resistente a la observación física Resistente a la imitación dirigida Resistente a la suposición estrangulada Resistente a la suposición no estrangulada Resistente a la observación interna Resistente a fugas desde otros verificadores Resistente al phishing Resistente al robo Terceras partes no fiables Requiere consenso explícito Desagradable

En el caso del criterio de seguridad, el conjunto de mediciones propuesto resume todos los aspectos que se estiman normalmente en la definición de un modelo de amenaza. En la definición de estos modelos es necesario adoptar un cierto número de decisiones. Y estas decisiones definen el escenario de trabajo. Por ejemplo en el caso de OAuth 2.0 [5] los supuestos adoptados son los siguientes:

- El atacante tiene un acceso total a la red entre el cliente y los servidores de autorización del cliente y el servidor de recursos, respectivamente. El atacante puede escuchar a escondidas cualquier comunicación entre esas partes. No se supone que tiene acceso a la comunicación entre el servidor de autorización y el servidor de recursos.
- Un atacante tiene recursos ilimitados para organizar un ataque.
- Dos de las tres partes involucradas en el protocolo OAuth pueden conspirar para montar un ataque contra la tercera parte. Por ejemplo, el cliente y el servidor de autorización pueden estar bajo el control de un atacante y conspirar para engañar a un usuario para obtener acceso a los recursos.

Atendiendo a las mediciones introducidas anteriormente, es posible determinar qué soluciones correspondientes al nivel de seguridad más alto (nivel 4) tienen un pobre rendimiento en capacidad de despliegue de uso. Una vez que la evaluación del sistema permite determinar en qué nivel ha de ser desplegado su sistema de autenticación, es necesario evaluar si el usuario se ha autenticado con seguridad y correctamente. Aunque hay algunas herramientas que ayudan en esta tarea [3], [6], los despliegues en el nivel 4 son difíciles de evaluar correctamente. En términos de capacidad de uso, el uso de tokens de hardware resistentes a la manipulación va en contra de la adopción de estas soluciones por los usuarios, y se ha comprobado que esta situación conduce a una mala utilización del sistema de credenciales. Estos tokens son caros. Hay dispositivos independientes que el usuario debe custodiar y que pueden emplearse solamente con un proveedor de servicios. Si el usuario tiene que manejarse con más de un proveedor de servicios que haya adoptado estos tokens de hardware de resistencia a la manipulación, han de tener en custodia tantos tokens como proveedores de servicios tengan.

Adicionalmente, en términos de autorización, en [7] los autores explican que, junto a algunos problemas de seguridad de cada SDK, los desarrolladores que han elegido integrarse con uno de ellos realizan suposiciones que pueden conducir a problemas de seguridad. Esto es debido a que los SDK frecuentemente no están bien documentados y las roturas de la seguridad casi siempre proceden de atacantes que hallan formas de violar este sistema de suposiciones en el que confiaron los implementadores.

Junto a estas dificultades, se deben considerar otros problemas para comprender el incremento constante en el fraude que surge del robo de identidades digitales. Por ejemplo, no es posible medir un nivel de seguridad homogéneo en todas las cuentas digitales de usuarios. Es necesaria una solución que pueda igualar el nivel de seguridad de todas las cuentas digitales que un usuario posee. Esta solución debería extender esta seguridad no solamente a los procesos de autenticación sino también a los procesos de autorización de recursos y a todos los procedimientos en relación con tales cuentas. Adicionalmente, no hay una solución que pueda mitigar los efectos de los denominados ataques MitB o MitD sin que sean caros o afecten significativamente a la capacidad de uso.

El documento US2009183247 (A1) proporciona sistemas y métodos para asegurar el acceso a una red. El acceso a la red está asegurado mediante autenticación de factor múltiple, biometría, cifrado sólido y una variedad de estándares de redes inalámbricas. La biometría incluye huellas digitales, reconocimiento facial, exploración de retina, reconocimiento de voz y biometría que se usan en combinación con otros factores de autenticación para crear un esquema de autenticación de múltiples factores para un acceso de red altamente seguro. Las solicitudes que requieren acceso a recursos de red seguros pueden ser interceptadas y una página de portal cautiva puede ser devuelta para desafiar a un usuario. La información biométrica devuelta en respuesta a la página del portal se utiliza para autenticar al usuario y determinar los derechos de acceso a la red.

El documento US2013247165 (A1) se refiere a un sistema informático que determina si el sistema informático es capaz de acceder a un servidor de autenticación. Si el sistema informático es capaz de acceder al servidor de autenticación, el sistema informático solicita un primer conjunto de credenciales de un usuario. Si el primer conjunto

de credenciales es válido, el sistema informático asigna al usuario un primer papel para realizar operaciones en el sistema informático en función del primer conjunto de credenciales. Si el sistema informático no es capaz de acceder al servidor de autenticación, el sistema informático solicita otro conjunto de credenciales del usuario. Si el otro conjunto de credenciales es válido, el sistema informático asigna al usuario otro papel para realizar operaciones en el sistema informático en función del otro conjunto de credenciales.

El documento US2004030932 divulga algunos protocolos de autenticación seguros, en particular bien adaptados para su uso en la autenticación de dispositivos de comunicaciones móviles con recursos computacionales limitados. En una realización ilustrativa, un sistema de comunicación basado en red incluye un dispositivo cliente y al menos dos servidores. Unas primeras y segundas partes se generan desde una primera contraseña asociada con el dispositivo cliente, y almacenada en respectivos primeros y segundos servidores. El dispositivo cliente envía información adicional asociada con ello a al menos uno de los primeros y segundos servidores. Cada una de las primeras y segundas partes tiene la propiedad de que es inviable determinar únicamente desde allí la correspondencia de la información adicional con la primera contraseña. Los primeros y segundos servidores utilizan entonces las respectivas primeras y segundas partes para determinar colectivamente dicha correspondencia de la información adicional con la primera contraseña. Ventajosamente, la determinación de correspondencia puede hacerse sin requerir más interacción entre el dispositivo cliente y uno o ambos servidores.

Por lo tanto, es necesario un enfoque diferente para mejorar la seguridad global en los sistemas de autenticación/autorización, cualquiera que sea el esquema o esquemas adoptados, minimizando el impacto en la capacidad de uso y despliegue de estos sistemas, y especialmente impidiendo amenazas de “Man in the Browser”.

Referencias:

[1] Bonneau, J., Herley, C., van Oorschot, P. C., y Stajano, F. (mayo de 2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In Security and Privacy (SP), 2012 IEEE Symposium on (págs. 553-567). IEEE.

[2] Burr, W. E., Dodson, D. F., y Polk, W. T. (2006). Electronic authentication guideline. NIST Special Publication, 800, 63.

[3] Dalton, M., Kozyrakis, C., y Zeldovich, N., Nemesis: Preventing Authentication & Access Control Vulnerabilities in Web Application, In Proceedings of the 18th conference on USENIX security symposium, (págs. 267-282) USENIX Association.

[4] Evans, D., Bond, P., Bement, A., Security Requirements for Cryptographic Modules, FIPS PUB 140-2 - FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION. Recurso en línea: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[5] McGloin M. y Hunt P. (2013, January) OAuth 2.0 Threat Model and Security Considerations. ISSN: 2070-1721. Recurso en línea: http://tools.ietf.org/pdf/rfc6819.pdf.

[6] Sun, F., Xu, L., y SU,Z. (2011,August) Static detection of Access control vulnerability in web applications. In Proceedings of the 20th USENIX conference on Security (págs. 11-11). USENIX.

[7] Wang, R., Zhou, Y., Chen, S., Qadeer, S., Evans, D., y Gurevich, Y. (2013). Explicating SDKs: Uncovering Assumptions Underlying Secure Authentication and Authorization (Vol. 37). Microsoft Research Technical Report MSR-TR-2013.

Descripción de la invención

Para conseguir lo anterior, la invención proporciona una solución para impedir diversos ataques relacionados con los procesos de autenticación y autorización. La solución comprende un método y un programa de ordenador como se define en las reivindicaciones independientes 1 y 14, respectivamente. Un número de realizaciones se definen en las reivindicaciones dependientes. La solución se diseña para limitar el tiempo en que un atacante puede desarrollar un ataque. Por lo tanto, supone un límite en los recursos disponibles para que un atacante se organice y ataque. Primero, la invención busca reducir el riesgo de un ataque dirigido a un proceso de autenticación/autorización bloqueando temporalmente el mecanismo de ejecución de operaciones. Disminuyendo por lo tanto el periodo de exposición de estos sistemas y, por lo tanto, disminuyendo las oportunidades de éxito de ataques sobre el sistema. Además, un primer servidor o proveedor de servicios puede forzar el uso de una segunda fase de autenticación (usando una infraestructura de OTP) para proveedores de servicios que no proporcionen esta opción en sus procesos de gestión de cuentas o incluso permitan al usuario activarla.

Además, la solución propuesta proporciona contramedidas contra MitB que dan también soporte para múltiples proveedores de servicios solamente con un dispositivo, en una forma barata y segura. Este ataque MitB supone que un atacante es capaz de insertarse a sí mismo entre un usuario y un primer servidor, con posterioridad a un intercambio de autenticación con éxito entre estas dos últimas partes. El atacante es capaz de hacerse pasar como el usuario para el primer servidor o viceversa para controlar el intercambio de datos de la sesión. Por otro lado, el atacante puede comprometer o explotar en otra forma los tokens de autenticación y puede interceptar todas las comunicaciones en clave salidas desde el dispositivo (por ejemplo un navegador o un ordenador). En este caso,

todas las acciones que se hayan invocado usando el dispositivo o la información que se haya mostrado a través de él, han de ser consideradas como sospechosas. Es necesario un canal seguro para asegurar la integridad de las operaciones.

De acuerdo con un primer aspecto se proporciona un método implementado en ordenador para impedir ataques contra sistemas de autorización, que comprende: la recepción por al menos un primer servidor de una solicitud en nombre de un usuario para ser registrado en un servicio de dicho primer servidor; y la autorización de dicha solicitud, por dicho primer servidor, verificando la información de identificación de usuario de dicho usuario.

Al contrario de las propuestas conocidas, y en una forma característica, para que dicha solicitud sea autorizada el método comprende adicionalmente:

- el envío, por dicho primer servidor a un segundo servidor en conexión con un dispositivo de ordenador del usuario con un programa dedicado, de una solicitud acerca de un estado asociado a dicho usuario;
- inicializar un intercambio de credenciales entre dicho primer y segundo servidores para proporcionar una autenticación mutua;
- verificación de dicho estado asociado que ha sido establecido previamente como válido o como inválido por dicho usuario y almacenado en una memoria de dicho segundo servidor;
- envío, en dicho segundo servidor, de dicho estado asociado a dicho primer servidor; y
- el uso por dicho primer servidor de dicho estado asociado recibido para:

    - autorización de dicha solicitud para dicho servicio en nombre de dicho usuario si dicho estado asociado se ha establecido como válido, o
    - rechazo de dicha solicitud para dicho servicio si dicho estado asociado se ha establecido como inválido,

en donde, en caso de que dicha solicitud a ser registrado en un servicio de dicho primer servidor sea autorizada y se realice una solicitud en nombre de dicho usuario para realizar una operación, pudiendo ser esta cualquier operación, en dicho primer servidor usando al menos una parte de los recursos de dicho primer servidor, el método comprende las siguientes etapas:

- realización, de una verificación del estado de la operación con protección de integridad asociada a dicho usuario por medio de:

    - verificación, por dicho primer servidor de que la solicitud para realizar una operación se autoriza por la coincidencia de la solicitud para realizar la operación con una entrada en relación a un estado de entrada del esquema definido por el primer servidor para una cuenta del usuario;
    - solicitud, del primer servidor de la información del usuario necesaria para realizar la operación;
    - envío, por el usuario, de al menos parte de dicha información necesaria al primer servidor y una parte de la información necesaria al segundo servidor;
    - con la recepción en dicho primer servidor de la información necesaria, solicitud al segundo servidor de un estado asociado para dicha operación;
    - inicialización de un intercambio de credenciales entre el primer servidor y el segundo servidor;
    - evaluación, por parte del segundo servidor del estado de entrada del esquema de estado desde una raíz a dicha entrada; y
    - envío, por el segundo servidor, del resultado de dicha evaluación del estado de entrada del esquema a dicho primer servidor; y

- el uso, por dicho primer servidor, del resultado de dicha evaluación para permitir o bloquear dicha solicitud en nombre de dicho usuario para realizar dicha operación.

La solicitud de estado asociada con el usuario comprende el envío de un token de seguridad, siendo generado dicho token de seguridad durante un proceso previo de vinculación de cuentas de usuario. Este token enlaza al usuario con el primer servidor sin desvelar ninguna información personal del usuario al segundo servidor de información. A continuación, el token se almacena con seguridad en una memoria del primer servidor y en una memoria del segundo servidor una vez que el usuario ha configurado la vinculación de la primera y segunda identificaciones de los servidores.

El intercambio de credenciales para asegurar la autenticación mutua entre el primer servidor y el segundo servidor, se realiza, preferiblemente, por medio de un procedimiento de autenticación estándar basado en el intercambio de certificados que define, como resultado, un canal seguro. El intercambio se realiza para verificar que tanto el primer servidor como el segundo servidor son quienes reivindican ser.

El segundo servidor puede mandar una notificación al usuario en caso de que dicha solicitud para ser registrado en un servicio del primer servidor se rechace. Por ejemplo, mediante el envío de un Servicio de Mensaje Corto (SMS) o

un e-mail, de o un mensaje mediante una aplicación de mensajería de teléfono inteligente, o solamente mediante el resalte o notificación en dicho programa dedicado de dicho dispositivo de ordenador del usuario.

El estado asociado se establece como válido (desbloqueado) o como inválido (bloqueado) un cierto período de tiempo y puede ser modificable por el usuario siempre que este último lo desee. Por ejemplo, el usuario puede planificar una política de bloqueo/desbloqueo para automatizar la gestión de sus cuentas mantenidas con diferentes servidores usando diferentes criterios: tiempo, geolocalización (diferentes políticas para hogar, trabajo, etc.). Otra posibilidad para la modificación de dicho estado asociado puede ser mediante la delegación del control que dicho usuario tiene sobre sus cuentas a otros usuarios. Esto se puede realizar considerando dos opciones diferentes. En la primera, se usa un mecanismo de control parental de modo que se delega el control de acceso de las cuentas de los hijos (original) al mecanismo de control del padre. En el segundo, una única cuenta permite múltiples bloqueos. En este último caso, la acción de desbloqueo requerirá que los usuarios desbloqueen sus bloqueos simultáneamente. En ambos casos, la delegación se realiza con seguridad manteniendo inalterada la privacidad de cada usuario.

La solicitud para ser registrado en un servicio y/o la solicitud para realizar una operación se puedan registrar para proporcionar estadísticas. De esta forma, el usuario puede obtener estadísticas de uso del sistema que reflejen la actividad del sistema y seguir los intentos de imitación. Estas estadísticas informan sobre cuándo alguien ha intentado acceder a un servicio con el nombre de usuario del usuario.

En una realización, la información completa necesaria para realizar la operación se envía por dicho usuario al primer servidor preferiblemente usando otro programa dedicado tal como un navegador. A continuación, dicho primer servidor (300) toma de la información completa recibida desde dicho usuario (100) la misma parte de la información que dicho usuario (100) ha enviado a dicho segundo servidor (200) y la engloba con dicha solicitud del estado de operación; y el segundo servidor previamente a realizar el envío del resultado de dicha entrada del esquema, comprueba si la información necesaria recibida desde el usuario coincide con la información necesaria recibida desde el primer servidor, siendo usadas ambas informaciones como tokens de integridad. Por lo tanto, todas estas etapas para la verificación de la integridad del estado de la operación se realizan en una forma síncrona.

En una realización, la verificación de la integridad de la ejecución de dicha operación se puede realizar también en una forma asíncrona. En este caso, el envío de información por el usuario al segundo servidor se envía después de que se realice la solicitud por este último a dicho programa dedicado, siendo realizada dicha solicitud al menos tras la recepción desde el primer servidor de la solicitud de estado de la operación. Por lo tanto, en este caso, el primer servidor espera hasta que el usuario confirma la operación, esto es, hasta que el usuario envía la integridad del token a través del programa dedicado. Esta confirmación podría no tener lugar nunca; en consecuencia se establece un plazo de espera asociado con el tiempo que el primer servidor ha de esperar.

En ambas realizaciones previas, la parte de información enviada al segundo servidor está dirigida a la realización de una validación.

Por el contrario, en una realización, esta información se puede usar también para completar la información de la operación. En este caso, la información necesaria para completar la operación se divide. De ese modo las dos partes son los dos elementos que completan la formación total necesaria. Un segmento se envía al primer servidor y el otro se envía a dicho segundo servidor. Por lo tanto, los dos servidores, primero y segundo, reciben una parte diferente de la información necesaria. El segundo servidor en este caso engloba la parte recibida de la información con el resultado de dicha evaluación del estado de entrada del esquema. Todas estas etapas se realizan en una forma síncrona.

Alternativamente, estas etapas se pueden realizar en una forma asíncrona, de acuerdo con otra realización más. En este caso, el segundo servidor, después de haber recibido la información necesaria del programa dedicado, ejecuta una llamada de retorno al primer servidor para comunicar los resultados del proceso de verificación de estado y envía la parte de información recibida al primer servidor.

Finalmente, como una opción, la etapa de evaluación del estado de la entrada del esquema realizada por el segundo servidor puede incluir adicionalmente un segundo factor de autenticación que comprende, si dicho estado de entrada del esquema se establece como válido:

- el envío, por dicho segundo servidor de una OTP al primer servidor dentro del resultado de la solicitud del estado de operación;
- solicitud, por el primer servidor al usuario, de una OTP que el usuario va a usar como segundo factor temporal;
- el envío, por el segundo servidor de la misma OTP enviada al primer servidor al usuario a través de dicho otro programa de usuario dedicado;
- recuperación, por el usuario, de dicho segundo factor OTP temporal solicitado a través de dicho programa dedicado, introduciéndole en dicho otro programa dedicado del usuario y enviándolo adicionalmente a través de

dicho otro programa dedicado del usuario al primer servidor; y

- comprobación, por el primer servidor, si la OTP recibida desde el segundo servidor y el segundo factor OTP temporal recibido desde dicho otro programa dedicado de usuario coinciden, para permitir o bloquear esa solicitud en nombre de dicho usuario para realizar dicha operación.

La materia objetivo descrita en el presente documento se puede implementar en software en combinación con hardware y/o firmware, o una combinación adecuada de ellos. Por ejemplo, la materia objeto descrita en el presente documento se puede implementar en un software ejecutado por un procesador.

De acuerdo con otro aspecto se proporciona un programa de ordenador que comprende medios de código de programa de ordenador adaptados para realizar las etapas de acuerdo con el método de la reivindicación 1 cuando dicho programa se ejecuta en un ordenador, un procesador de señales digitales, puertas lógicas programables en campo (FPGA – Field Programable Gate Array), un circuito integrado de aplicación específica, un microprocesador, un microcontrolador, o cualquier otra forma de hardware programable.

Las realizaciones de la invención también engloban un producto de programa de ordenador que incluye medios de código de programas adaptados para realizar una segunda autenticación del factor de acuerdo con el método de la reivindicación 10.

Por lo tanto, la presente invención permite que el usuario active la mitigación de MitB usando el canal de comunicación seguro propuesto por la invención. Con las diferentes opciones proporcionadas para intercambiar información crítica relacionada con las operaciones se garantiza la integridad de su ejecución. Más aún, la invención también permite que el usuario: planee una política de bloqueo/desbloqueo para automatizar la gestión de cuentas mantenidas con diferentes servidores usando diferentes criterios: tiempo, geolocalización (diferentes políticas para hogar, trabajo, etc.); delegar el control de sus cuentas a otros usuarios del segundo servidor; permitir sistemas de supervisión que permita a los usuarios ser alertados de intentos de robo de la identidad o imitación del usuario no verdadero en solicitudes de ejecución de operaciones, proporcionando una vía de actuación para tomar una acción para controlar la identidad digital; establecer un segundo factor para la autenticación para verificadores que no lo estén proporcionando; establecer una cuenta a ser bloqueada o desbloqueada y cambiarla con efecto inmediato mediante el uso de un control de conmutación; establecer una planificación para validar/invalidar (bloquear/ desbloquear) una cuenta con dicha operación automáticamente en base a ajustes de tiempo y fecha. Una vez que se recibe la solicitud de comprobación de estado, el segundo servidor responde en base al estado actual del planificador; mejora el nivel de seguridad de una cuenta de dicha operación configurando un segundo factor de autenticación integrado con el segundo servidor; controla diferentes acciones asociadas con una cuenta, autorizando o prohibiendo la ejecución de las mismas en una forma compatible con el esquema de autorización establecido. Este control no se limita a una orden de bloqueo/desbloqueo. De hecho, se pueden aplicar los mismos conceptos introducidos para controlar el proceso de autenticación (planificación, segundo factor, etc.) y aprovechar la invención y hacer uso del certificado digital para ser autenticado por cualquier proveedor de servicios evitando la introducción de palabras clave.

La invención permite homogeneizar el nivel de seguridad para todas las diferentes cuentas que tiene un usuario. Permite ofrecer un nivel de seguridad comparable con el nivel 4 definido por el NIST. Esto se realiza para diferentes cuentas que pueden controlarse ahora solamente con un dispositivo e independientemente del esquema de autenticación/autorización definido por cada proveedor de servicios.

La invención no propone ningún esquema de autenticación/autorización nuevo. Realmente, la invención complementa los esquemas existentes para incrementar su seguridad añadiendo una capa de seguridad extra. Aunque esto puede limitar su capacidad de uso y despliegue, el diseño de la invención está orientado a minimizar el impacto sobre estos criterios. Como se ha establecido anteriormente, la elección del esquema de autenticación determina el riesgo de seguridad que se está asumiendo para un sistema de autorización. Lo que se propone en este caso es reducir el riesgo tomado con la elección de cualquier mecanismo de autenticación/autorización reduciendo el tiempo en el que este sistema está accesible para ser roto.

Suponiendo que haya una relación entre el éxito y el fallo de un ataque sobre el sistema de autorización y el tiempo en el que este sistema es accesible (tiempo de exposición) es posible la determinación, como probabilidad condicional (p (ataque con éxito | expuesto)), de que el riesgo relativo (RR) satisfaga la siguiente expresión:

$$RR = \frac{p(Ataque\,con\acute{e}xito \mid \text{expuesto})}{p(Ataque\,con\acute{e}xito \mid \text{sinexposición})} > 1 \qquad \text{Ec. 1}$$

En esta expresión, se asume que la probabilidad de éxito de un ataque se relaciona directamente con el tiempo de exposición. Es decir, la exposición continua de un sistema de ordenador, en este caso sistema de autenticación, incrementa la probabilidad de éxito de un ataque a diferencia de un escenario en el que la exposición se limite. De la

misma manera se puede evaluar la siguiente expresión:

$$\frac{\frac{p(Ataque\ con\ éxito \mid \text{expuesto})}{p(Ataque\ fallido \mid \text{expuesto})}}{\frac{p(Ataque\ con\ éxito \mid \text{no expuesto})}{p(Ataque\ fallido \mid \text{no expuesto})}} > 1 \qquad \text{Ec. 2}$$

Indicando que hay una mayor probabilidad de un ataque con éxito si existe una exposición continuada del sistema. Es posible también estimar la parte de todos los ataques con éxito que podrían haberse evitado si la exposición se hubiera evitado (ARP). Esto se calcula con la expresión 3.

$$ARP = \frac{RR - 1}{RR} \qquad \text{Ec. 3}$$

Esta expresión permite la evaluación de la inversión requerida para permitir una solución diseñada para reducir el tiempo que está accesible el proceso de autenticación. La experiencia profesional y el conocimiento técnico de las técnicas de ataque documentadas para romper los sistemas de autenticación/autorización confirman la suposición realizada anteriormente (RR > 1). Por lo tanto, se puede afirmar que ARP > 1 una vez que se adopta el bloqueador de cuentas.

Esta reducción en el tiempo de exposición permite la mitigación de los efectos de la mayor parte de las amenazas relacionadas con la fase de autenticación antes de que un usuario pueda acceder a algunos recursos privilegiados. La presente invención permite también la reducción de la exposición de acciones particulares que se pueden tomar después de que el proceso de registro se haya llevado a cabo. Por lo tanto, esta reducción de la exposición supone la limitación del tiempo en el que la acción se puede ejecutar y el establecimiento de un canal que permita el envío de información crítica para asegurar la integridad de esta ejecución de la acción.

La invención engloba las soluciones para las amenazas definidas por el NIST. Pero en este caso, estas soluciones se proporcionan a los usuarios a través de un programa dedicado diseñado para ser ejecutado en un dispositivo móvil, que facilite la integración con un segundo servidor. Además, este segundo servidor trae la privacidad de las comunicaciones con relación al control de las cuentas del usuario e incorpora toda la información de control que los usuarios han establecido alrededor de las acciones que los proveedores de servicio les han ofrecido. Proporciona también una solución para mitigar los ataques de “man in the browser” garantizando la integridad de la operación.

Breve descripción de los dibujos

Lo anterior y otras ventajas y características se comprenderán más profundamente a partir de la descripción detallada a continuación de las realizaciones, con referencia a los adjuntos, que se deberían considerar en una forma ilustrativa y no limitativa, en los que:

la Figura 1 es una ilustración de la arquitectura general de la presente invención.
La Figura 2 es un diagrama de flujo que ilustra una secuencia de vinculación de cuentas con autorización.
La Figura 3 es un diagrama de flujo que ilustra cómo se puede comprobar un estado de una cuenta de usuario para autenticación.
La Figura 4 es un diagrama de flujo que ilustra una generalización de la Figura 3 en relación con el proceso de verificación del estado de la operación.
La Figura 5 es un diagrama de flujo que ilustra una primera opción para la mitigación de los efectos del MitB, de acuerdo con una realización de la presente invención.
La Figura 6 es un diagrama de flujo que ilustra una segunda opción para la mitigación de los efectos del MitB, de acuerdo con una realización de la presente invención.
La Figura 7 es un diagrama de flujo que ilustra una tercera opción para la mitigación de los efectos del MitB, de acuerdo con una realización de la presente invención.
La Figura 8 es un diagrama de flujo que ilustra una cuarta opción para la mitigación de los efectos del MitB, de acuerdo con una realización de la presente invención.

Descripción detallada de varias realizaciones

Con referencia a la Figura 1, se muestra la arquitectura general de la presente invención. En relación con la Figura 1, se usa un dispositivo de computación 100 de usuario tal como un teléfono móvil, un teléfono inteligente, una tablet-PC o una PDA entre otros, por dicho usuario para registrarse en un programa dedicado 102 en comunicación con un segundo servidor 200 y para gestionar el estado de cada primer servidor 300 con el que un usuario desea solicitar un servicio.

Con esta nueva propuesta, dicho usuario 100 puede desbloquear dicha operación definida para una cuenta particular creada con dicho primer servidor 300. Tal como se establece a continuación, esta acción puede mejorar el control definido para esta cuenta por la decisión del primer servidor 300. En esta decisión, el primer servidor 300 puede elegir incorporar un nuevo control de seguridad más allá de la opción por defecto de bloqueo/desbloqueo o del segundo factor de autenticación. Este control de seguridad consiste en proporcionar un canal de comunicación desde el usuario 100 al primer servidor 300, a través del segundo servidor 200. El primer servidor 300 puede configurar el sistema para pedir al usuario 100 una información particular relativa a dicha operación a ser realizada. Esta información se puede usar por el segundo servidor 200 para verificar si el usuario 100 es quien realmente está solicitando dicha operación y para confirmar si la operación que ha llegado al primer servidor 300 es exactamente como la que el usuario 100 ha ordenado.

Suponiendo que el primer servidor 300 pudiera desear verificar la integridad de la operación, se puede seleccionar qué parámetros son críticos para asegurar la integridad de la operación. En este caso, es importante que la información solicitada corresponda de modo único con el parámetro crítico de la operación para identificarlo correctamente.

En esta arquitectura, el usuario 100, junto a tener una cuenta en el segundo servidor 200, puede tener múltiples cuentas con diferentes proveedores de servicios. Uno de estos proveedores de servicios es el primer servidor 300. Una vez que el usuario 100 completa el proceso de registro con estas cuentas tendrá acceso a múltiples operaciones específicas para cada proveedor de servicio. El segundo servidor 200 facilita cómo un primer servidor 300 puede integrar este control dentro de la lógica de sus aplicaciones.

Cuando el primer servidor 300 decide integrar sus servicios, proporcionará la capacidad de enlazar sus cuentas con las cuentas que el usuario 100 tiene en el segundo servidor 200. Cuando dicho usuario 100 decide establecer este enlace, comienza el proceso de vinculación que asegura una privacidad completa para el usuario 100. Una vez que el proceso de vinculación está completo, el usuario 100 puede acceder a la configuración de control de la cuenta con el primer servidor 300 desde un programa dedicado 102 (es decir una aplicación móvil).

Cada vez que los ajustes asociados con una cuenta se cambian en dicha aplicación móvil, esta modificación se propaga inmediatamente al segundo servidor 200 para cambiar el estado de la cuenta que puede ser accedida por el primer servidor 300.

El núcleo del segundo servidor implementa la función principal del segundo servidor 200: bloquear o desbloquear dicha cuenta de usuario con el primer servidor 300 y las operaciones proporcionadas por el primer servidor 300. Para hacer esto, el segundo servidor 200 acepta y procesa las solicitudes de comprobación de estado enviadas desde el primer servidor 300. Este segundo servidor 200 también gestiona todos los datos acerca de los enlaces con dicho primer servidor 300 definidos por el usuario 100 y las solicitudes para la vinculación de nuevos bloqueos. La clave es que el usuario 100 nunca es preguntado por cualquier información privada. Una vez que el usuario 100 crea su cuenta con el segundo servidor 200, puede establecer bloqueos con diferentes proveedores de servicios, como dicho primer servidor 300. Para activar estos bloqueos el segundo servidor 200, de acuerdo con una realización, genera un token. Son necesarios un token único y la definición de canales seguros para completar el proceso de vinculación entre el usuario 100 y el primer servidor 300. Como resultado de este proceso de vinculación, el token criptográfico se envía desde el segundo servidor 200 al primer servidor 300 que tiene que almacenar esta información con sus datos personales del usuario. Posteriormente, este token criptográfico se usará para solicitar el estado de bloqueo correspondiente. El usuario 100 puede modificar el estado de sus bloqueos, mediante la activación o configuración de las diferentes opciones que el segundo servidor 200 proporciona.

En caso de que el usuario 100 haya establecido un bloqueo con el segundo factor para autenticación sobre una cuenta o una acción particular, el segundo servidor 200 incorporará toda la lógica necesaria para la generación y comunicación de la OTP. Cuando el segundo servidor 200 recibe una solicitud desde el primer servidor 300 pidiendo el estado de la cuenta del usuario, se activa un segundo factor de autenticación. Se genera una OTP y se envía al usuario 100. Se envía la misma OTP al primer servidor 300 junto con el estado de la cuenta. Si el estado es ACTIVO y el usuario 100 tiene activado el segundo factor, el primer servidor 300 debería solicitar al usuario introducir la OTP para proseguir con la operación.

Ahora, si el usuario 100 ha establecido un bloqueo sobre una de dichas operaciones con un factor de integridad para verificar que los parámetros de la operación no se han modificado, dicho segundo servidor 200 incorpora la lógica necesaria para obtener la información crítica del usuario 100 y desde el primer servidor 300 y para comprobar si ambas son iguales. El segundo servidor 200 envía el resultado de la comprobación como el estado de la cuenta al primer servidor 300. En caso de falta de coincidencia, el primer servidor 300 puede concluir que un intruso puede estar interceptando la información desde el usuario 100. El primer servidor 300 puede construir entonces mecanismos para eludir el fraude y para elevar alertas de seguridad.

Con referencia a la Figura 2, se ilustra un proceso de vinculación de la cuenta del usuario 100 del segundo servidor 200 con diferentes cuentas para diferentes primeros servidores 300. En la Figura 2, una vez que un usuario 100, usando por ejemplo el programa dedicado 101 tal como un navegador, ha completado el proceso de registro (A-B) con un primer servidor 300 (en este caso particular un banco en línea, una red social, proveedores de tarjetas de créditos, etc.), el usuario 100 decide realizar dicho proceso de vinculación de cuentas. El usuario 100 solicita la vinculación al primer servidor 300 (C) usando el navegador 101. Como respuesta, el primer servidor 300 solicita un token de vinculación (D). El usuario 100 usa entonces el programa dedicado 102 (D') para obtener este token de vinculación desde el segundo servidor 200, después de un proceso de registro previo. El segundo servidor 200 genera un token (por ejemplo como una OTP) (E) y lo envía al programa dedicado del usuario 102 (F). Este token se puede usar para varios procesos de vinculación siempre que sea válido. El usuario obtiene el token (OTP) desde el programa dedicado 102 y lo introduce en la página web visualizada en el navegador 101 por el primer servidor 300 (G-G'). El primer servidor 300 envía entonces el token recibido al segundo servidor 200, después de un intercambio previo de credenciales (H). Si la identidad del primer servidor 300 es validada, el segundo servidor 200 almacena el enlace entre el usuario 100 y el primer servidor 300 y genera un nuevo token que identifica este enlace. Este token (ID de cuenta) se envía al primer servidor 300 (I) y allí se almacena para comunicaciones futuras (J). Finalmente, se envía un acuse de recibo de la vinculación al navegador del usuario 101 (K).

Con referencia ahora a la Figura 3 se ilustra cómo se puede comprobar un estado de la cuenta de usuario para autenticación. En la Figura 3, un usuario 100, usando por ejemplo un navegador 101, solicita ser registrado en un servicio (A) de un primer servidor 300 de modo que una vez que se haya validado (B) la existencia del usuario por dicho primer servidor 300, este último solicitará al segundo servidor 200 el estado de cuentas del usuario (C). Entonces el segundo servidor 200 inicializa el intercambio de credenciales antes de que se envíe el resultado de la información del estado de cuentas (D). Con el estado del resultado, el primer servidor 300 toma la decisión de permitir o bloquear el acceso del usuario (E).

En una realización, si el estado de la cuenta es desbloqueada o válida pero el segundo factor de autenticación está activo, dentro de la respuesta de la solicitud de estado, el segundo servidor 200 envía una OTP al primer servidor 300 que ha de emplear para completar la autenticación. El primer servidor 300 solicita entonces al usuario 100 la OTP que va a ser un segundo factor temporal (F). Entonces el segundo servidor 200 envía la misma OTP al programa dedicado del usuario 102 (G). El usuario 100 recupera la OTP desde el programa dedicado 102 y la introduce en el navegador 101 (H) y la envía al primer servidor 300 (I). El primer servidor 300 puede comprobar si la OTP enviada a través del navegador 101 coincide con la recibida con el estado de la cuenta (J). Dependiendo de los resultados de esta verificación, el primer servidor realiza el proceso de autenticación (K) y comunica el resultado al usuario a través de 101.

Cuando un primer servidor 300 envía una Solicitud de estado (Status_Request), el segundo servidor 200 comprende que alguien, con la información de identificación del servicio apropiada (es decir ID y palabra clave), está tratando de acceder al servicio. Si el estado de la cuenta se establece como bloqueada, o si esta solicitud ha llegado en un momento que no está incluido en el intervalo definido por el usuario 100, el segundo servidor 200 registra este evento como un intento falso. El segundo servidor 200 podría enviar, de acuerdo con una realización, una alerta de este evento al usuario si dicho usuario lo ha configurado así (por ejemplo mediante el envío de un Servicio de Mensaje Corto (SMS), un e-mail, un mensaje mediante una aplicación de mensajería de teléfono inteligente, mediante un resaltado o realzado en dicho programa dedicado 102 de dicho dispositivo de computación del usuario 100, etc.) o solamente actualizar las estadísticas para una revisión posterior. Entonces el segundo servidor 200 vuelve al estado asociado con la cuenta como bloqueada.

Con la intención de mejorar la seguridad de cualquier sistema de autorización, el uso del segundo servidor 200 se propone como una nueva capa que da a los usuarios la oportunidad de controlar el acceso a los recursos y procedimientos asociados con sus cuentas definidas con cualquier primer servidor. Estos recursos y procedimientos se envían con operaciones que dependen de las acciones principales definidas para una cuenta (es decir proceso de registro). Esta dependencia se establece con una jerarquía en la que los cambios en las entradas raíz se propagan a sus hijos.

La Figura 4 ilustra el proceso de verificación del estado de la operación de una operación solicitada por el usuario 100. Esta operación es propuesta por el primer servidor 300 adjunto a la gestión de cuenta. El usuario 100, usando por ejemplo un navegador 101, solicita, de acuerdo con una realización, ejecutar una operación relacionada con una cuenta (A) en el primer servidor 300. Esta operación puede ser el registro en un servicio particular o ejecutar alguna operación relacionada con los servicios proporcionados por el primer servidor 300 (por ejemplo pago por Internet con una tarjeta de crédito). De ese modo una vez que ha sido validada la existencia del usuario (B) por dicho primer servidor 300, este último realiza la correspondencia de la operación solicitada con la entrada de esquema en la jerarquía definida por esta cuenta de usuario (D) y solicita al segundo servidor 200 este estado de entrada (E).

Entonces el segundo servidor 200 inicializa el intercambio de credenciales antes de evaluar el estado de entrada del esquema desde la raíz a la entrada (F). El estado de la cuenta del usuario se recupera y si está desbloqueada se

realiza la misma evaluación con cada etapa hallada hasta alcanzar la entrada del esquema. La información del estado de la entrada del esquema se envía (G) y, con esta información, el primer servidor 300 toma la decisión de permitir o bloquear el acceso del usuario a la operación.

El segundo factor de autenticación se puede activar si el estado de entrada del esquema es válido o desbloqueado para reforzar el proceso. El segundo servidor 200 envía una OTP al primer servidor 300 dentro de la respuesta de la solicitud de estado. Este primer servidor 300 ha de emplearla para completar la autenticación. El primer servidor 300 solicita al usuario 100 la OTP que va a ser el segundo factor temporal (H). El segundo servidor 200 envía la misma OTP al programa dedicado del usuario 102 (I). El usuario 100 recupera la OTP desde el programa dedicado 102 y la introduce en el navegador 101 (J) y la envía al primer servidor 300 (K). El primer servidor 300 puede comprobar si la OTP enviada a través del navegador 101 coincide con la recibida con el estado de la cuenta (L). El primer servidor 300 deniega la operación de ejecución si las OTP no se ajustan.

A continuación, para mitigar los efectos del MitB, la presente invención propone cuatro opciones o realizaciones diferentes. Las diferencias entre estas opciones permiten definir cuatro escenarios en los que la implementación final se puede diseñar para ser síncrona o asíncrona. Se puede decidir verificar la información relacionada con las operaciones y recibirla través de un canal no seguro, usando el canal seguro definido por dicho segundo servidor para enviar un factor de integridad. Es posible también dividir la información crítica y enviar al menos una de las partes resultantes usando el canal seguro definido por dicho segundo servidor.

La Figura 5 ilustra la primera opción propuesta por la invención para la mitigación de dicho efecto. Para esta realización, se supone que el primer servidor 300 instruye al usuario 100 para introducir parte de la información (por ejemplo el segmento A como se ilustra en la figura) usado para completar la operación solicitada en el programa dedicado 102 antes de completar la información de la operación como por ejemplo, en el navegador 101. Todas estas etapas se realizan de una forma síncrona.

En la Figura 5 se muestra el proceso de verificación del estado de la operación con la protección de integridad de la operación. Esta operación se propone por el primer servidor adjunto a la gestión de cuentas. El usuario 100, usando por ejemplo el navegador 101, solicita, de acuerdo con una realización, ejecutar una operación relacionada con una cuenta (A) de un primer servidor 300. Esta operación puede ser registrada en un servicio particular o ejecutar alguna otra acción relacionada con los servicios proporcionados por el primer servidor (por ejemplo pago en Internet con una tarjeta de crédito). De ese modo una vez que se ha validado la existencia del usuario 100 (B) mediante dicho primer servidor 300, este último realiza la correspondencia de la operación solicitada con la entrada del esquema en la jerarquía definida por esta cuenta del usuario (D) y solicita al navegador 101 la información necesaria para realizar la operación (E). Si el usuario 100 ha sido instruido en el uso de su programa dedicado 102 para realizar la verificación de integridad, el usuario 100 envía entonces el segmento A al segundo servidor 200 (F) y, en este caso, la información de la operación completa necesaria para el primer servidor 300 (G). El segundo servidor 200 registra la información recibida como parte del contenido con la configuración del usuario. Si se espera esa entrega pero el usuario 100 no la realiza se podría enviar un mensaje de error. Una vez que se recibe la información de la operación, el primer servidor 300 solicita el estado de esta operación al segundo servidor 200 (H). Englobado dentro de esta solicitud el segmento A de la información recibida desde el usuario 100 se envía al segundo servidor 200.

Entonces el segundo servidor 200 inicializa el intercambio de credenciales antes de la evaluación del estado de entrada del esquema desde la raíz a la entrada. El estado de la cuenta del usuario se recupera y si está desbloqueada se realiza la misma evaluación con cada etapa hallada hasta alcanzar la entrada del esquema. El segundo servidor 200 comprueba también los dos segmentos A recibidos y asociados con esta operación (I). Si los dos segmentos son iguales y el estado se establece en activo, la respuesta será desbloqueada. En otro caso, si el proceso de comprobación del segmento devuelve una no coincidencia de segmentos la respuesta será bloqueada. La información del estado de entrada del esquema se envía (J) y, con esta información, el primer servidor 300 toma la decisión de permitir o bloquear el acceso del usuario a la operación.

Opcionalmente, si el estado de entrada del esquema es válido (desbloqueado) y se activa el segundo factor de autenticación, el segundo servidor 200 puede enviar una OTP al primer servidor 300 dentro de la respuesta de la solicitud de estado. Este primer servidor 300 la emplea para completar la autenticación. El primer servidor 300 solicita al usuario la OTP que va a ser un segundo factor temporal (N). El segundo servidor 200 envía la misma OTP al programa dedicado del usuario 102 (O). El usuario 100 recupera la OTP desde el programa dedicado 102 y la introduce en el navegador 101 (P) y la envía al primer servidor 300 (Q). Los primeros servidores pueden comprobar si la OTP enviada a través del navegador 101 coincide con la recibida con el estado de la cuenta (R). El primer servidor 300 deniega la ejecución de la operación si las OTP no se ajustan.

La Figura 6 ilustra la segunda opción propuesta por la invención para la mitigación de dicho efecto MitB. Para esta realización, se supone de nuevo que el primer servidor 300 instruye al usuario 100 para introducir parte de la información (por ejemplo el segmento A como se ilustra en la figura) usado para completar la operación solicitada en el programa dedicado 102 antes de completar la información de la operación, por ejemplo, en el navegador 101. Sin

embargo, a diferencia de la primera opción, la verificación de la integridad de la ejecución de la operación se realiza en una forma asíncrona. El flujo parece más intuitivo que tener que “arrancar” la operación en dos extremos, el programa dedicado 102 y el primer servidor 300. Sin embargo en este caso el primer servidor 300 necesita esperar hasta que el usuario 100 confirma la operación. Esto podría no ocurrir nunca dejando la operación sin acabar, de modo que, para evitar eso, se define un tiempo de espera asociado con el tiempo que el primer servidor 300 ha de esperar a la llamada de retorno identificada en la figura 6 como S.

De nuevo, en esta realización, se muestra el proceso de verificación del estado de la operación con protección de integridad de la operación. Esta operación se propone por el primer servidor 300 adjunto a la gestión de la cuenta. El usuario 100, usando, por ejemplo, el navegador 101, solicita, de acuerdo con una realización, ejecutar una operación relacionada con una cuenta (A) del primer servidor 300. Esta operación puede ser registrarse en un servicio particular o ejecutar alguna otra acción relacionada con los servicios proporcionados por el primer servidor 300 (por ejemplo pago por Internet con una tarjeta de crédito). Así, una vez que la existencia del usuario ha sido validada (B) por dicho primer servidor 300, este último realiza la correspondencia de la operación solicitada con la entrada del esquema en la jerarquía definida por esta cuenta del usuario (D) y solicita al navegador 101 la información necesaria para realizar la operación (E). El usuario envía la información de la operación necesaria al primer servidor (G) (como se ilustra en la figura, segmentos A y B). Una vez que se recibe la información de la operación, el primer servidor 300 solicita el estado para esta operación al segundo servidor 200 (G). Englobada con esta solicitud se envía el segmento A de la información recibida desde el usuario 100 al segundo servidor 200 y espera a recibir la llamada de retorno que informa sobre el resultado de la verificación de la integridad.

Entonces el segundo servidor 200 inicializa el intercambio de credenciales antes de la evaluación del estado de entrada del esquema desde la raíz a la entrada. Se recupera el estado de la cuenta del usuario y si está desbloqueada se realiza la misma operación con cada etapa hallada hasta alcanzar la entrada del esquema. Esta información de estado de la entrada del esquema se envía (I) y, con esta información, el primer servidor 300 toma la decisión de permitir o bloquear el acceso del usuario a la operación. El primer servidor 300 es informado de si la verificación de la integridad está pendiente de la autenticación del usuario.

Opcionalmente, si el estado de entrada del esquema es válido (desbloqueado) y el segundo factor de autenticación está activado, el segundo servidor 200 puede enviar una OTP al primer servidor 300 dentro de la respuesta de la solicitud de estado. Este primer servidor 300 ha de emplearla para completar la autenticación. El primer servidor 300 solicita al usuario 100 la OTP que va a ser un segundo factor temporal (J). El segundo servidor 200 envía la misma OTP al programa dedicado del usuario 102 (K). El usuario 100 recupera la OTP desde el programa dedicado 102 y la introduce en el navegador 101 (L) y la envía al primer servidor 300 (M). El primer servidor 300 puede comprobar si la OTP enviada a través del navegador 101 coincide con la recibida con el estado de la cuenta (N).

En caso de que la operación esté pendiente de la autenticación del usuario para verificar su integridad, el primer servidor 300 informa al usuario 100 de que la operación está pendiente de autenticación (O). Asíncronamente, el segundo servidor 200 solicita al usuario 100 a través del programa dedicado 102 el segmento A de la información de la operación (A). Una vez que el usuario 100 envía este segmento A usando el programa dedicado 102 (Q), el segundo servidor 200 puede comprobar si los dos segmentos A recibidos coinciden (R). Entonces el segundo servidor 200 retorna la llamada al primer servidor 300 para comunicar los resultados de su proceso de verificación (S).

La Figura 7 ilustra la tercera opción propuesta por la invención para la mitigación de dicho efecto MitB. Para esta realización, de nuevo se supone que el primer servidor 300 instruye al usuario 100 para introducir parte de la información (el segmento A como se ilustra en la figura) usado para completar la operación solicitada del programa dedicado 102 antes de completar la información de la operación, por ejemplo, en el navegador 101. Todas estas etapas siguientes se realizan en una forma síncrona. Es casi la misma que la primera y segunda opciones pero, en este caso, la información necesaria (segmento A) no se introduce en el programa dedicado 102 del usuario para validación. Ahora el segmento A se envía usando el programa dedicado 102 del usuario para ser usado para completar la información de la operación.

De nuevo, se muestra el proceso de verificación del estado de la operación con protección de la integridad de la operación. Esta operación se propone por el primer servidor 300 adjunto a la gestión de la cuenta. El usuario 100, usando por ejemplo el navegador 101, solicita, de acuerdo con una realización, ejecutar una operación relacionada con una cuenta (A) del primer servidor 300. Esta operación puede ser registrarse en un servicio particular o ejecutar alguna otra acción relacionada con los servicios proporcionados por el primer servidor (por ejemplo pago por Internet con una tarjeta de crédito). Así, una vez que la existencia del usuario ha sido validada (B) por dicho primer servidor 300, este último toma la correspondencia de la operación solicitada con la entrada del esquema en la jerarquía definida por esta cuenta del usuario (D) y solicita al navegador 101 la información necesaria para realizar la operación (E). Si el usuario ha sido instruido en el uso de su programa dedicado 102 para realizar la verificación de la integridad, el usuario 100 envía entonces el segmento A al segundo servidor 200 (F) y un segmento diferente necesario de la información de la operación (por ejemplo el segmento B) al primer servidor 300 (G). El segundo

servidor 200 registra la información recibida como parte del contenido con la configuración del usuario. Si se espera esta entrega y el usuario no la realiza, se envía un mensaje de error. Una vez que se recibe la información de la operación, el primer servidor 300 solicita el estado para esta operación al segundo servidor 200 (H).

A continuación el segundo servidor 200 inicializa el intercambio de credenciales antes de la evaluación del estado de la entrada del esquema desde la raíz a la entrada. Se recupera el estado de la cuenta del usuario y si está bloqueada se realiza la misma evaluación con cada etapa hallada hasta alcanzar la entrada del esquema. Se envía la información del estado de entrada del esquema (I). Englobado con la respuesta del estado está el segmento A que se recibe por el primer servidor 300. Ahora el primer servidor 300 puede completar la información de la operación, necesaria para realizar la acción solicitada (J). Con esta información, el primer servidor 300 toma la decisión de permitir o bloquear el acceso del usuario a la operación.

Opcionalmente, si el estado de entrada del esquema es válido (desbloqueado) y se activa el segundo factor de autenticación, el segundo servidor 200 puede enviar una OTP al primer servidor 300 dentro de la respuesta de la solicitud de estado. El primer servidor 300 ha de emplearla para completar la autenticación. El primer servidor 300 solicita al usuario 100 la OTP que va a ser el segundo factor temporal (N). El segundo servidor 200 envía la misma OTP al programa dedicado del usuario 102 (O). El usuario 100 recupera la OTP desde el programa dedicado 102 y la introduce en el navegador 101 (P) y la envía al primer servidor 300 (Q). Los primeros servidores pueden comprobar si la OTP enviada a través del navegador 101 coincide con la recibida con el estado de la cuenta (R). El primer servidor 300 deniega la ejecución de la operación si las OTP no se ajustan.

La Figura 8 ilustra la cuarta opción propuesta por la invención para la mitigación de dicho efecto MitB. Para esta realización, se supone que el primer servidor 300 instruye al usuario 100 para introducir parte de la información (el segmento A como se ilustra en la figura) usado para completar la operación solicitada en el programa dedicado del usuario (102) antes de completar la información de la operación. Todas estas etapas siguientes se realizan en una forma asíncrona.

De nuevo, se muestra el proceso de verificación del estado de la operación con protección de integridad de la operación. Esta operación se propone por el primer servidor 300 adjunto a la gestión de cuentas. El usuario 100, usando por ejemplo el navegador 101, solicita, de acuerdo con una realización, ejecutar una operación relacionada con una cuenta (A) del primer servidor 300. Esta operación puede ser registrarse en un servicio particular o ejecutar alguna otra acción relacionada con los servicios proporcionados por el primer servidor (por ejemplo pago por Internet con una tarjeta de crédito). De modo que una vez se haya validado la existencia del usuario (B) por dicho primer servidor 300, este último realiza la correspondencia de la operación solicitada con la entrada del esquema en la jerarquía definida por esta cuenta del usuario (D) y demanda del navegador 101 la información necesaria para realizar la operación (E). El usuario envía la información de la operación necesaria (segmento B) al primer servidor 300 (G). Una vez que se recibe la información de la operación, el primer servidor 300 solicita el estado para esta operación al segundo servidor 200 (G). El primer servidor 300 espera recibir la llamada de retorno que informa sobre el resultado de la verificación de integridad.

A continuación el segundo servidor 200 inicializa el intercambio de credenciales antes de la evaluación del estado de la entrada del esquema desde la raíz a la entrada. Se recupera el estado de la cuenta del usuario y si está desbloqueada se realiza la misma evaluación con cada etapa hallada hasta alcanzar la entrada del esquema. Se envía la información del estado de entrada del esquema (I) y, con esta información, el primer servidor 300 toma la decisión de permitir o bloquear el acceso del usuario a la operación.

Opcionalmente, si el estado de entrada del esquema es válido (desbloqueado) y se activa el segundo factor de autenticación, el segundo servidor 200 puede enviar una OTP al primer servidor 300 dentro de la respuesta de la solicitud de estado. El primer servidor 300 ha de emplearla para completar la autenticación. El primer servidor 300 solicita al usuario 100 la OTP que va a ser el segundo factor temporal (J). El segundo servidor 200 envía la misma OTP al programa dedicado del usuario 102 (K). El usuario 100 recupera la OTP desde el programa dedicado 102 y la introduce en el navegador 101 (L) y la envía al primer servidor 300 (M). Los primeros servidores pueden comprobar si la OTP enviada a través del navegador 101 coincide con la recibida con el estado de la cuenta (N).

Si el estado de entrada del esquema revela que la verificación de integridad está activa, el primer servidor 300 informa al usuario 100 de que la operación está pendiente de autenticación (O). Asíncronamente, el segundo servidor solicita al usuario, a través del programa dedicado 102, el segmento A de la información de la operación (P). Una vez que el usuario 100 envía este segmento A usando el programa dedicado 102 (Q), el segundo servidor 200 ejecuta la llamada de retorno al primer servidor 300 para comunicar los resultados de este proceso de verificación (S) y envía el segmento recibido desde el usuario al primer servidor 300. El primer servidor 300 puede completar entonces la información de la operación necesaria para realizar la acción solicitada (T).

En alcance de la presente invención se define en el siguiente conjunto de reivindicaciones.

REIVINDICACIONES

1. Un método implementado en ordenador para impedir ataques contra sistemas de autorización, en donde un segundo servidor (200), en conexión con un dispositivo informático de un usuario (100), a través de un segundo programa dedicado (102) instalado en dicho dispositivo informático, se usa para administrar un estado de las cuentas que el usuario (100) tiene en un primer servidor (300) y un estado de las operaciones definidas para una cuenta particular, configurándose dicho estado de cuenta y dicho estado de operación, cuando el usuario (100) quiera, como válido o no válido por el usuario (100) a través del segundo programa dedicado (102) y almacenados en una memoria del segundo servidor (200), y configurándose dicho estado de cuenta y dicho estado de operación por el usuario (100) una vez que un proceso de vinculación con el segundo servidor (200) se ha completado, asegurando dicho proceso de vinculación la privacidad del usuario (100), comprendiendo el método:

- recibir, por dicho primer servidor (300), del usuario (100) a través de un primer programa dedicado (101) que incluye un navegador, una solicitud para ser registrado en un servicio de dicho primer servidor (300), incluyendo dicha solicitud la provisión de información de identificación que valida la identidad del usuario (100) en el primer servidor (300);
- una vez que se ha validado la existencia del usuario por el primer servidor (300), recibir, por dicho segundo servidor (200), del primer servidor (300), una solicitud sobre un estado referente a una cuenta del usuario (100) en el primer servidor (300);
- en respuesta a recibir la solicitud, inicializar un primer intercambio de credenciales entre dicho primer (300) y segundo (200) servidores para proporcionar una autenticación mutua, realizándose el intercambio de credenciales mediante un procedimiento de autenticación en función del intercambio de certificados;
- verificación de dicho estado de cuenta por dicho segundo servidor (200);
- envío, por dicho segundo servidor (200), de dicho estado de cuenta a dicho primer servidor (300); y
- el uso por dicho primer servidor (300) de dicho estado de cuenta recibido para:

  o autorización de dicha solicitud para ser registrado en dicho servicio si dicho estado de cuenta se ha establecido como válido, o
  o rechazo de dicha solicitud para ser registrado en dicho servicio si dicho estado de cuenta se ha establecido como inválido,

en donde, en respuesta a la autorización de dicha solicitud para ser registrado en el servicio, se realiza una solicitud adicional por el usuario (100) mediante el primer programa dedicado (101) para realizar una operación relacionada con dicha cuenta del usuario (100) en dicho primer servidor (300), el método comprende además las siguientes etapas:

- realización de una verificación del estado de la operación por medio de:

  o determinación, por dicho primer servidor (300) de qué entrada en un esquema de una jerarquía definida por dicha cuenta corresponde a dicha operación solicitada;
  o solicitud, por dicho primer servidor (300) a dicho usuario (100) de la información necesaria para realizar dicha operación;
  o en respuesta a recibir la solicitud, envío, por dicho usuario (100), de al menos parte de dicha información necesaria a dicho primer servidor (300) y una parte de dicha información necesaria a dicho segundo servidor (200) para completar la operación solicitada;
  o con la recepción en dicho primer servidor (300) de dicha información necesaria, solicitud a dicho segundo servidor (200) del estado de operación definido por el usuario (100) sobre dicha entrada y registrando el segundo servidor (200) la parte recibida de información en su interior como parte de la configuración de usuario;
  o inicialización de un segundo intercambio de credenciales entre dicho primer servidor (300) y dicho segundo servidor (200);
  o evaluación, por parte de dicho segundo servidor (200) de información de estado de entrada de esquema desde una raíz de dicho esquema jerárquico a dicha entrada; y
  o envío, por dicho segundo servidor (200), del resultado de dicha evaluación de información de estado de entrada del esquema a dicho primer servidor (300); y

- el uso, por dicho primer servidor (300), del resultado de dicha evaluación para permitir o bloquear dicha operación solicitada.

2. Un método implementado en ordenador de acuerdo con la reivindicación 1, en donde:

- se envía la información completa necesaria para realizar dicha operación, por parte de dicho usuario (100), a través del primer programa dedicado (101) a dicho primer servidor (300);
- tomar, por dicho primer servidor (300), de la información completa recibida desde dicho usuario (100), la misma

parte de información que dicho usuario (100) ha enviado a dicho segundo servidor (200) y engloba dicha misma parte de información necesaria con dicha solicitud del estado de operación; y
- dicho segundo servidor (200) previamente a realizar dicho envío del resultado de dicha información de estado de entrada del esquema comprende la comprobación de si dicha información necesaria recibida desde el usuario (100) a través de dicho segundo programa dedicado (102) coincide con dicha información necesaria recibida desde el primer servidor (300), siendo usadas ambas informaciones como tokens de integridad.

3. Un método implementado en ordenador de acuerdo con la reivindicación 1, en donde:

- dicha al menos parte de la información necesaria enviada a dicho primer servidor (300) es diferente de dicha parte de información necesaria enviada a dicho segundo servidor (200), siendo enviada dicha información necesaria por el primer servidor (300) a través del primer programa dedicado (101); y
- dicho segundo servidor (200) comprende el englobar con los resultados de dicha evaluación de información de estado de entrada de esquema la parte de información necesaria recibida desde dicho usuario (100).

4. Un método implementado en ordenador de acuerdo con las reivindicaciones 2 o 3, que comprende la notificación, por dicho segundo servidor (200) a dicho usuario (100) en caso de que dicha información necesaria no llegue.

5. Un método implementado en ordenador de acuerdo con la reivindicación 1, en donde dicho envío de dicha parte de información necesaria a dicho segundo servidor (200) se realiza después de que se realice una solicitud por dicho segundo servidor (200) a dicho segundo programa dedicado (102), siendo realizada dicha solicitud al menos tras la recepción desde el primer servidor (300) de dicha solicitud del estado de la operación.

6. Un método implementado en ordenador de acuerdo con la reivindicación 5, en donde:

- la información completa necesaria para realizar dicha operación se envía, por dicho usuario (100), a través del primer programa dedicado (101) a dicho primer servidor (300);
- dicho primer servidor (300) comprende el englobar con dicha solicitud del estado de la operación la información necesaria recibida desde dicho usuario (100); y
- dicho segundo servidor (200) previamente a la realización de dicho envío del resultado de dicha evaluación información de estado de entrada del esquema comprende la comprobación de si dicha información necesaria recibida desde el segundo programa dedicado (102) coincide con dicha información necesaria recibida desde el primer servidor (300), siendo usadas ambas informaciones como tokens de integridad.

7. Un método implementado en ordenador de acuerdo con la reivindicación 5, en donde:

- dicha al menos parte de la información necesaria para dicho primer servidor (300) es diferente a dicha parte de la información necesaria enviada a dicho segundo servidor (200), siendo enviada dicha información necesaria por el primer servidor (300) a través del primer programa dedicado (101) que incluye un navegador; y
- dicho segundo servidor (200) comprende el envío de dicha información necesaria recibida desde el segundo programa dedicado (102) a dicho primer servidor (300).

8. Un método implementado en ordenador de acuerdo con las reivindicaciones 6 o 7, en donde dicho primer servidor (300) antes de usar el resultado de dicha evaluación para permitir o bloquear dicha operación solicitada comprende el esperar hasta la confirmación de dicho usuario (100).

9. Un método implementado en ordenador de acuerdo con la reivindicación 8, en donde el tiempo para la realización de dicha confirmación está limitado.

10. Un método implementado en ordenador de acuerdo con las reivindicaciones previas, que comprende adicionalmente el uso de un segundo factor de autenticación, si dicha información de estado de entrada del esquema se establece como válida:

- el envío, por dicho segundo servidor (200) de una OTP al primer servidor (300) dentro de la respuesta de la solicitud del estado de operación;
- solicitud, por el primer servidor (300) al usuario (100), de una OTP que el usuario (100) va a usar como segundo factor temporal;
- el envío, por el segundo servidor (200) de la misma OTP enviada al primer servidor (300) al usuario (100) a través de dicho primer programa de usuario dedicado (101);
- recuperación, por el usuario (100), de dicho segundo factor temporal solicitado de OTP a través de dicho segundo programa dedicado (102), introduciéndola en dicho primer programa dedicado (101) del usuario y enviando adicionalmente el segundo factor temporal solicitado de OTP a través de dicho primer programa dedicado (101) del usuario al primer servidor (300); y
- comprobación, por el primer servidor (300), de si la OTP recibida desde el segundo servidor (200) y el segundo

factor OTP temporal recibido desde dicho primer programa dedicado (101) de usuario coinciden, para permitir o bloquear dicha operación solicitada.

11. Un método implementado en ordenador de acuerdo con la reivindicación 1, que comprende la notificación, por dicho segundo servidor (200) al usuario (100) en caso de que dicha solicitud para ser registrado en un servicio se rechace, comprendiendo dicha notificación al menos una de entre un envío de un Servicio de Mensajes Cortos (SMS), un envío de un e-mail, un envío del mensaje mediante una aplicación de mensajería de teléfono inteligente, un resalte o notificación en dicho segundo programa dedicado (102) de dicho dispositivo de computación de usuario.

12. Un método implementado en ordenador de acuerdo con la reivindicación 1, en donde dicho estado de cuenta se establece como válido o como inválido un cierto período de tiempo.

13. Un método implementado en ordenador de acuerdo con la reivindicación 1, en donde dicha solicitud para ser registrado en un servicio y/o dicha solicitud para realizar una operación se registran para proporcionar estadísticas.

14. Un programa de ordenador que comprende medios de código de programa de ordenador adaptados para realizar las etapas de acuerdo con el método de la reivindicación 1 cuando dicho programa se ejecuta en un ordenador, un procesador de señales digitales, una puerta lógica programable en campo (FPGA), un circuito integrado de aplicación específica, un microprocesador, un microcontrolador o cualquier otra forma de hardware programable.

15. Un programa de ordenador de acuerdo con la reivindicación 14, que comprende adicionalmente medios de código de programa adaptados para realizar un segundo factor de autenticación de acuerdo con el método de la reivindicación 10.

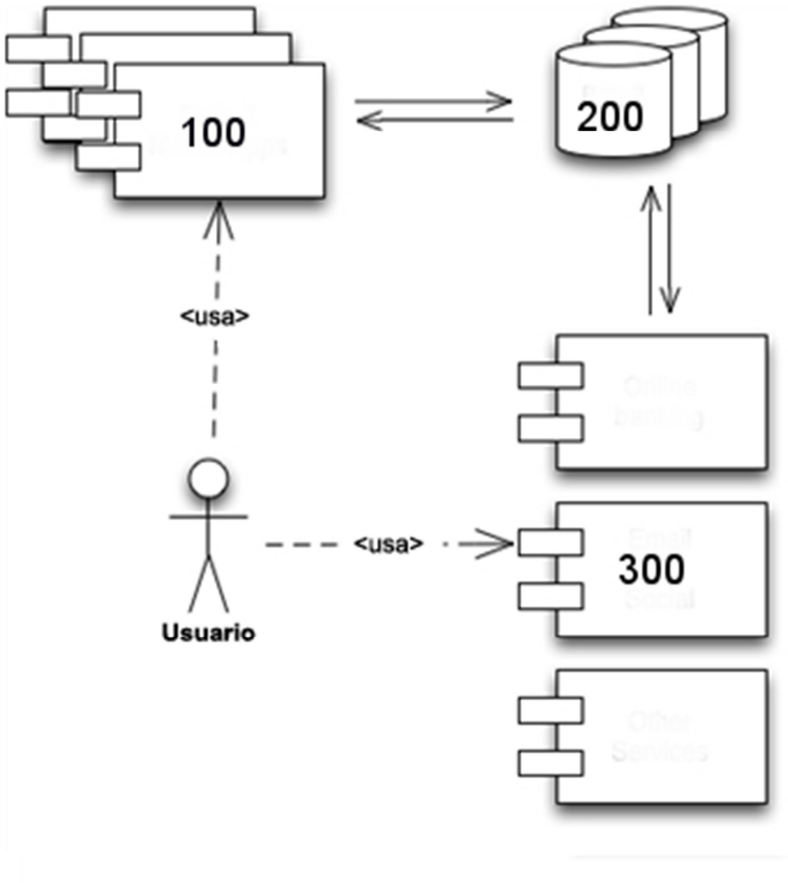

Figura 1

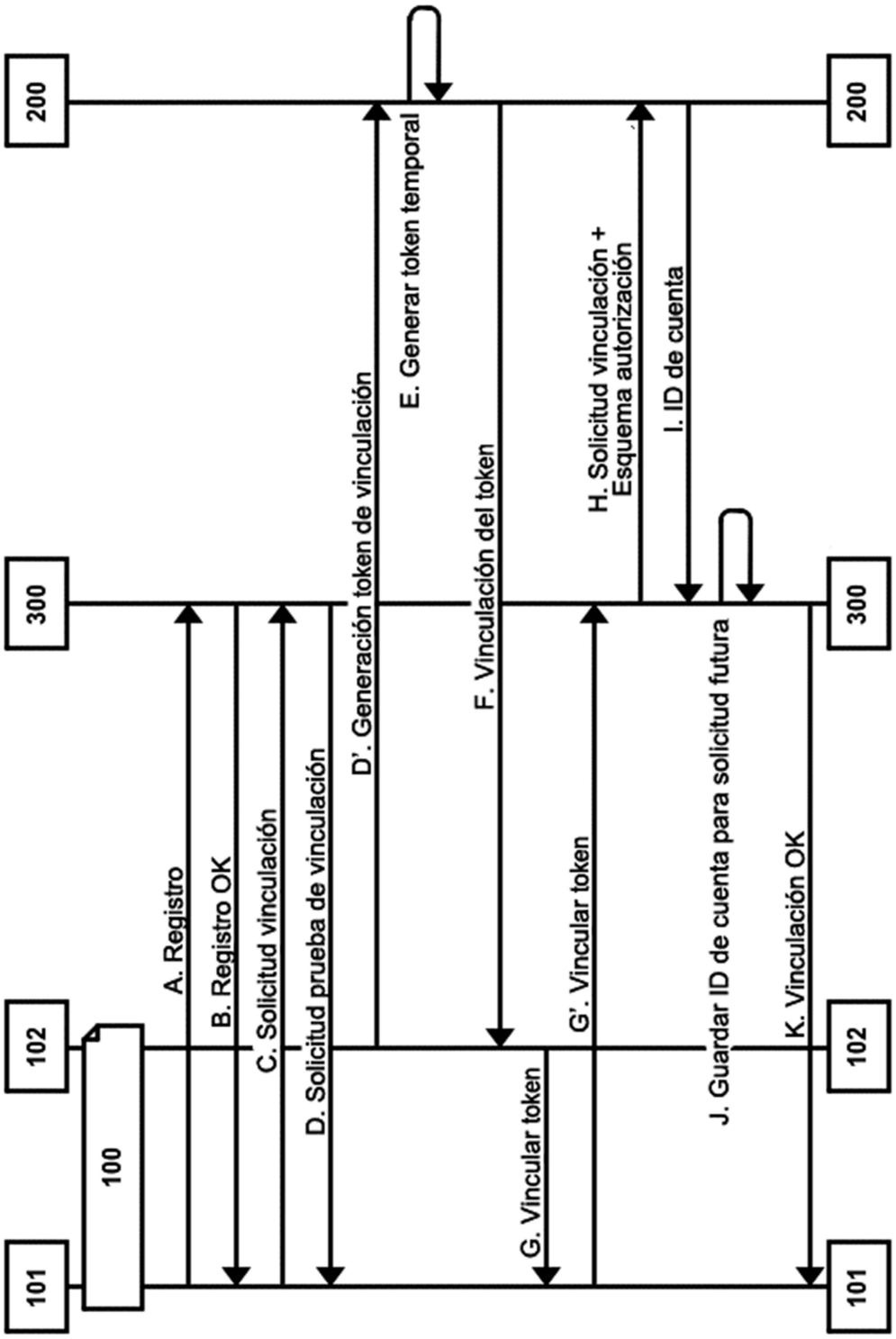
200
200
E. Generar token temporal
D'. Generación token de vinculación
F. Vinculación del token
H. Solicitud vinculación + Esquema autorización
I. ID de cuenta
300
300
A. Registro
B. Registro OK
C. Solicitud vinculación
D. Solicitud prueba de vinculación
G'. Vincular token
J. Guardar ID de cuenta para solicitud futura
K. Vinculación OK
102
102
100
G. Vincular token
101
101

Figura 2

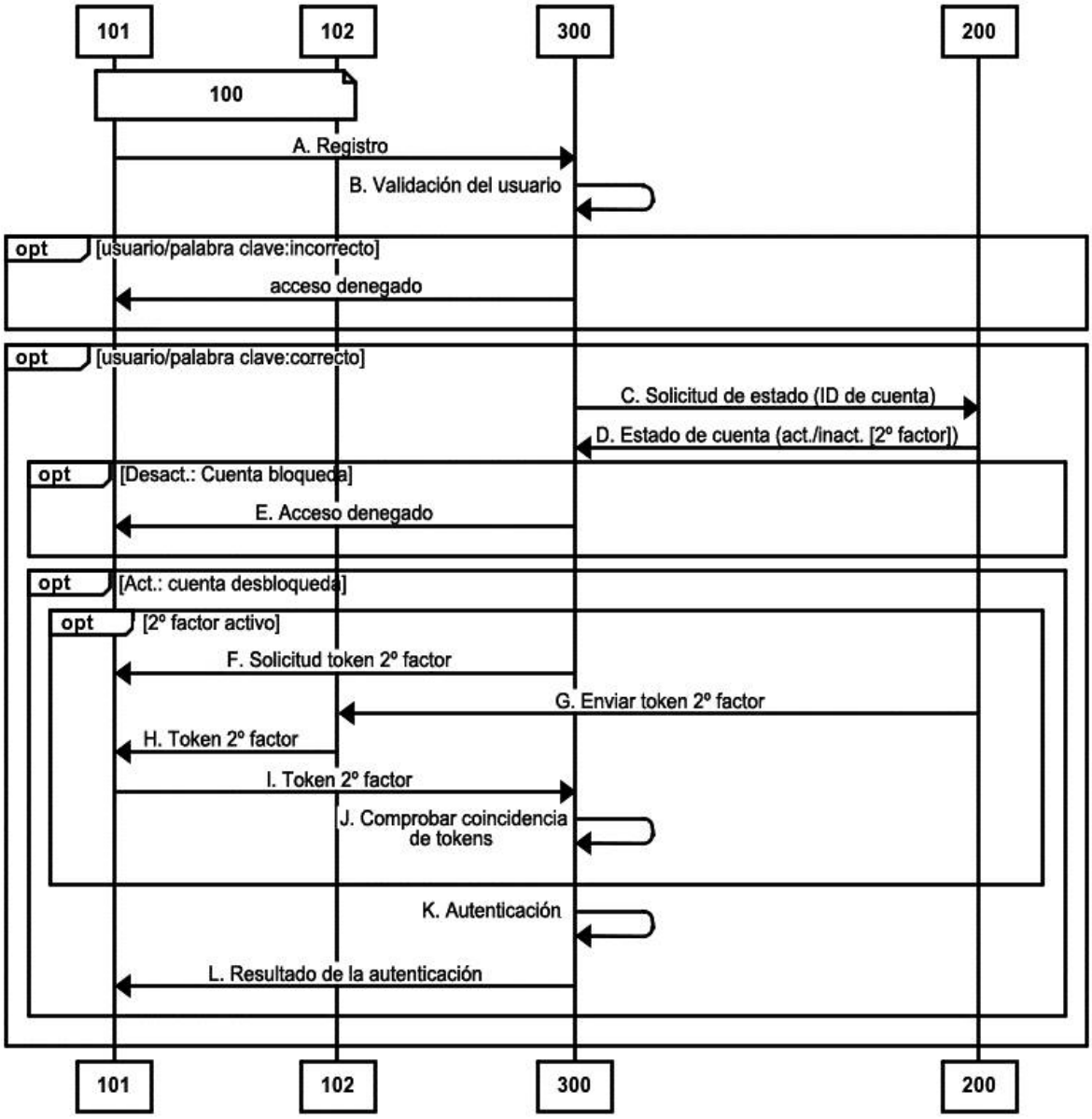
101
102
300
200
100
A. Registro
B. Validación del usuario
opt
[usuario/palabra clave:incorrecto]
acceso denegado
opt
[usuario/palabra clave:correcto]
C. Solicitud de estado (ID de cuenta)
D. Estado de cuenta (act./inact. [2º factor])
opt
[Desact.: Cuenta bloqueda]
E. Acceso denegado
opt
[Act.: cuenta desbloqueda]
opt
[2º factor activo]
F. Solicitud token 2º factor
G. Enviar token 2º factor
H. Token 2º factor
I. Token 2º factor
J. Comprobar coincidencia de tokens
K. Autenticación
L. Resultado de la autenticación
101
102
300
200

Figura 3

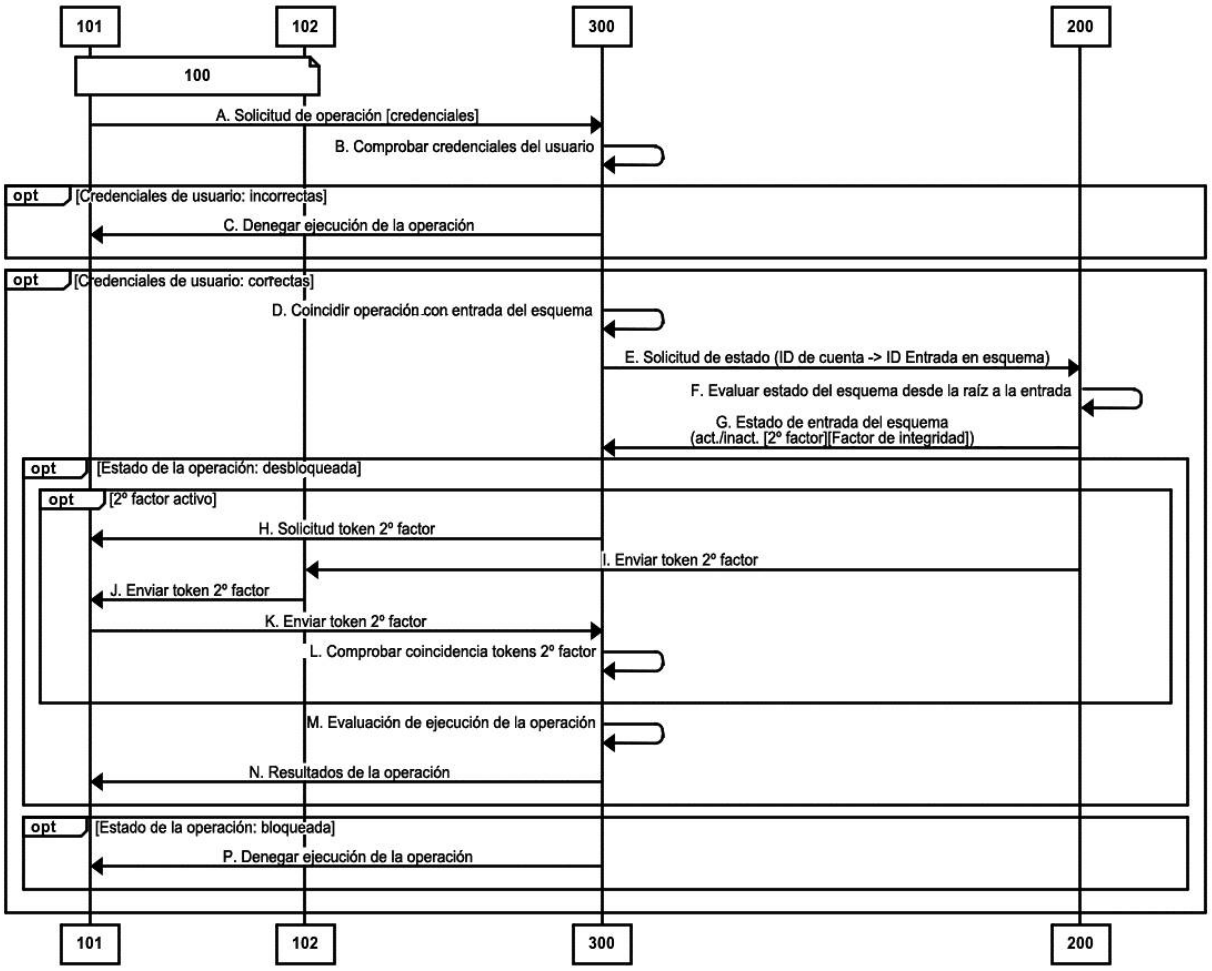
101
102
300
200
100
A. Solicitud de operación [credenciales]
B. Comprobar credenciales del usuario
opt
[Credenciales de usuario: incorrectas]
C. Denegar ejecución de la operación
opt
[Credenciales de usuario: correctas]
D. Coincidir operación con entrada del esquema
E. Solicitud de estado (ID de cuenta -> ID Entrada en esquema)
F. Evaluar estado del esquema desde la raíz a la entrada
G. Estado de entrada del esquema
(act./inact. [2º factor][Factor de integridad])
opt
[Estado de la operación: desbloqueada]
opt
[2º factor activo]
H. Solicitud token 2º factor
I. Enviar token 2º factor
J. Enviar token 2º factor
K. Enviar token 2º factor
L. Comprobar coincidencia tokens 2º factor
M. Evaluación de ejecución de la operación
N. Resultados de la operación
opt
[Estado de la operación: bloqueada]
P. Denegar ejecución de la operación
101
102
300
200

Figura 4

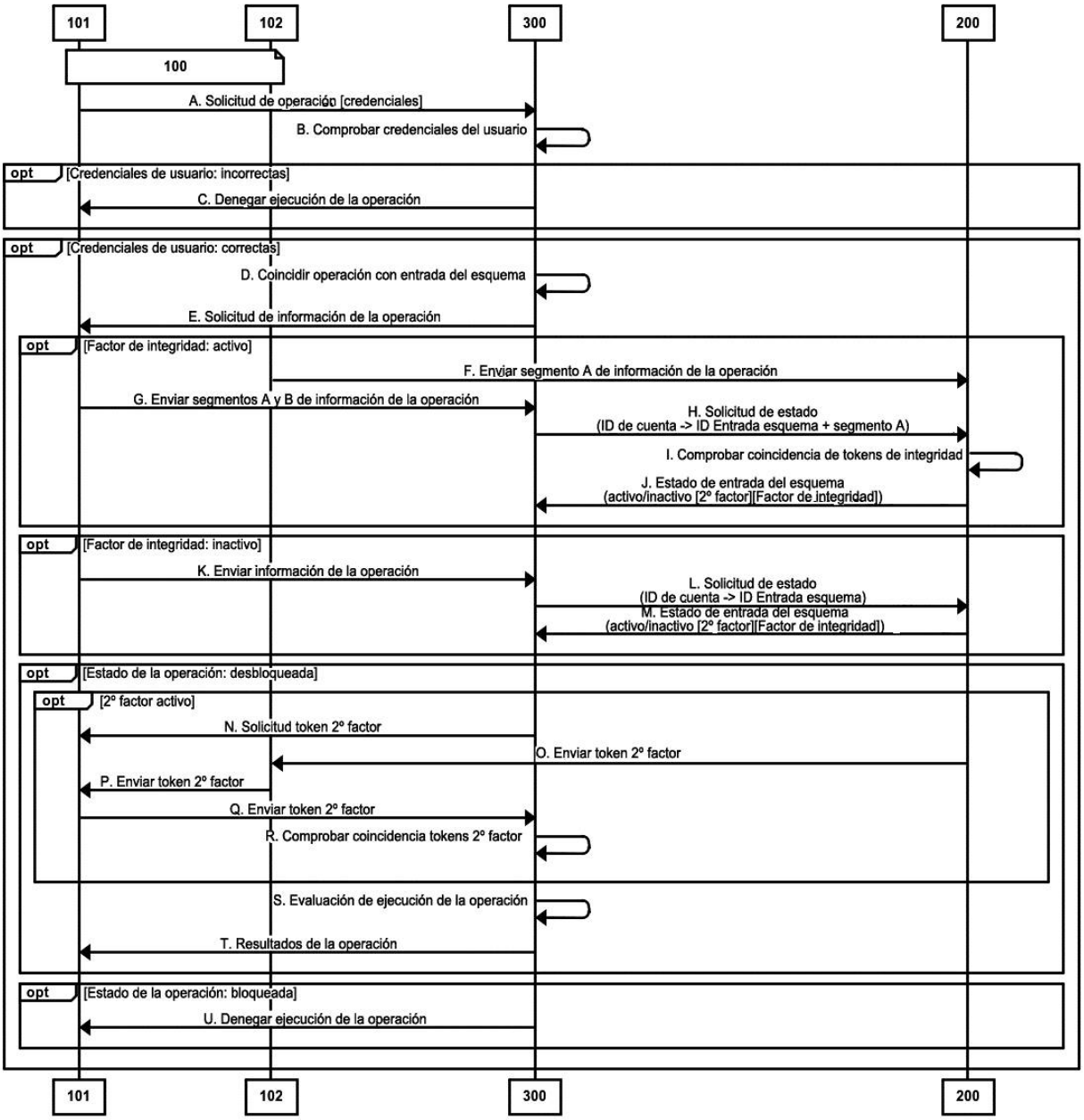
101
102
300
200
100
A. Solicitud de operación [credenciales]
B. Comprobar credenciales del usuario
opt
[Credenciales de usuario: incorrectas]
C. Denegar ejecución de la operación
opt
[Credenciales de usuario: correctas]
D. Coincidir operación con entrada del esquema
E. Solicitud de información de la operación
opt
[Factor de integridad: activo]
F. Enviar segmento A de información de la operación
G. Enviar segmentos A y B de información de la operación
H. Solicitud de estado
(ID de cuenta -> ID Entrada esquema + segmento A)
I. Comprobar coincidencia de tokens de integridad
J. Estado de entrada del esquema
(activo/inactivo [2º factor][Factor de integridad])
opt
[Factor de integridad: inactivo]
K. Enviar información de la operación
L. Solicitud de estado
(ID de cuenta -> ID Entrada esquema)
M. Estado de entrada del esquema
(activo/inactivo [2º factor][Factor de integridad])
opt
[Estado de la operación: desbloqueada]
opt
[2º factor activo]
N. Solicitud token 2º factor
O. Enviar token 2º factor
P. Enviar token 2º factor
Q. Enviar token 2º factor
R. Comprobar coincidencia tokens 2º factor
S. Evaluación de ejecución de la operación
T. Resultados de la operación
opt
[Estado de la operación: bloqueada]
U. Denegar ejecución de la operación
101
102
300
200

Figura 5

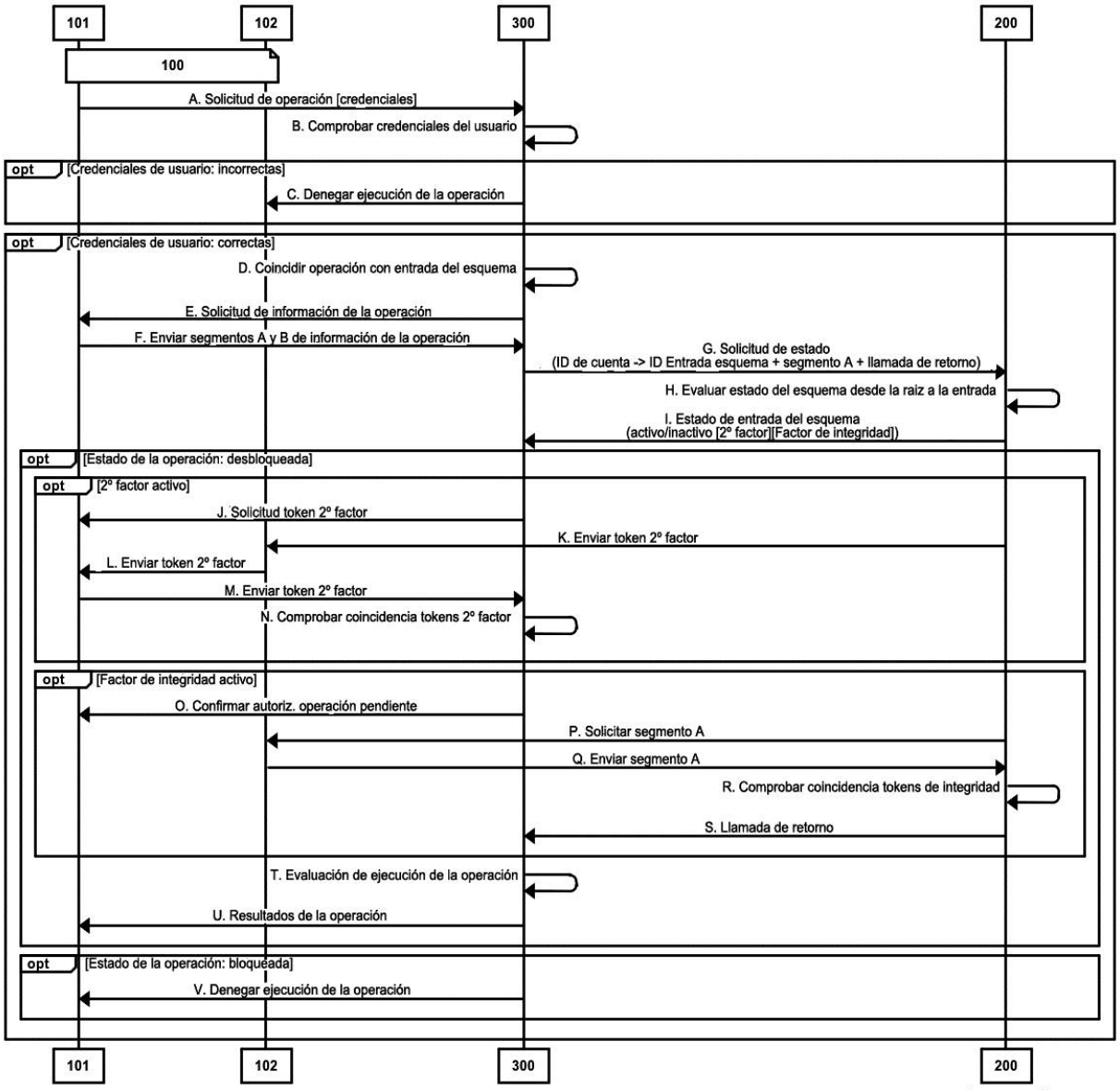
101
102
300
200
100
A. Solicitud de operación [credenciales]
B. Comprobar credenciales del usuario
opt
[Credenciales de usuario: incorrectas]
C. Denegar ejecución de la operación
opt
[Credenciales de usuario: correctas]
D. Coincidir operación con entrada del esquema
E. Solicitud de información de la operación
F. Enviar segmentos A y B de información de la operación
G. Solicitud de estado
(ID de cuenta -> ID Entrada esquema + segmento A + llamada de retorno)
H. Evaluar estado del esquema desde la raiz a la entrada
I. Estado de entrada del esquema
(activo/inactivo [2º factor][Factor de integridad])
opt
[Estado de la operación: desbloqueada]
opt
[2º factor activo]
J. Solicitud token 2º factor
K. Enviar token 2º factor
L. Enviar token 2º factor
M. Enviar token 2º factor
N. Comprobar coincidencia tokens 2º factor
opt
[Factor de integridad activo]
O. Confirmar autoriz. operación pendiente
P. Solicitar segmento A
Q. Enviar segmento A
R. Comprobar coincidencia tokens de integridad
S. Llamada de retorno
T. Evaluación de ejecución de la operación
U. Resultados de la operación
opt
[Estado de la operación: bloqueada]
V. Denegar ejecución de la operación
101
102
300
200

Figura 6

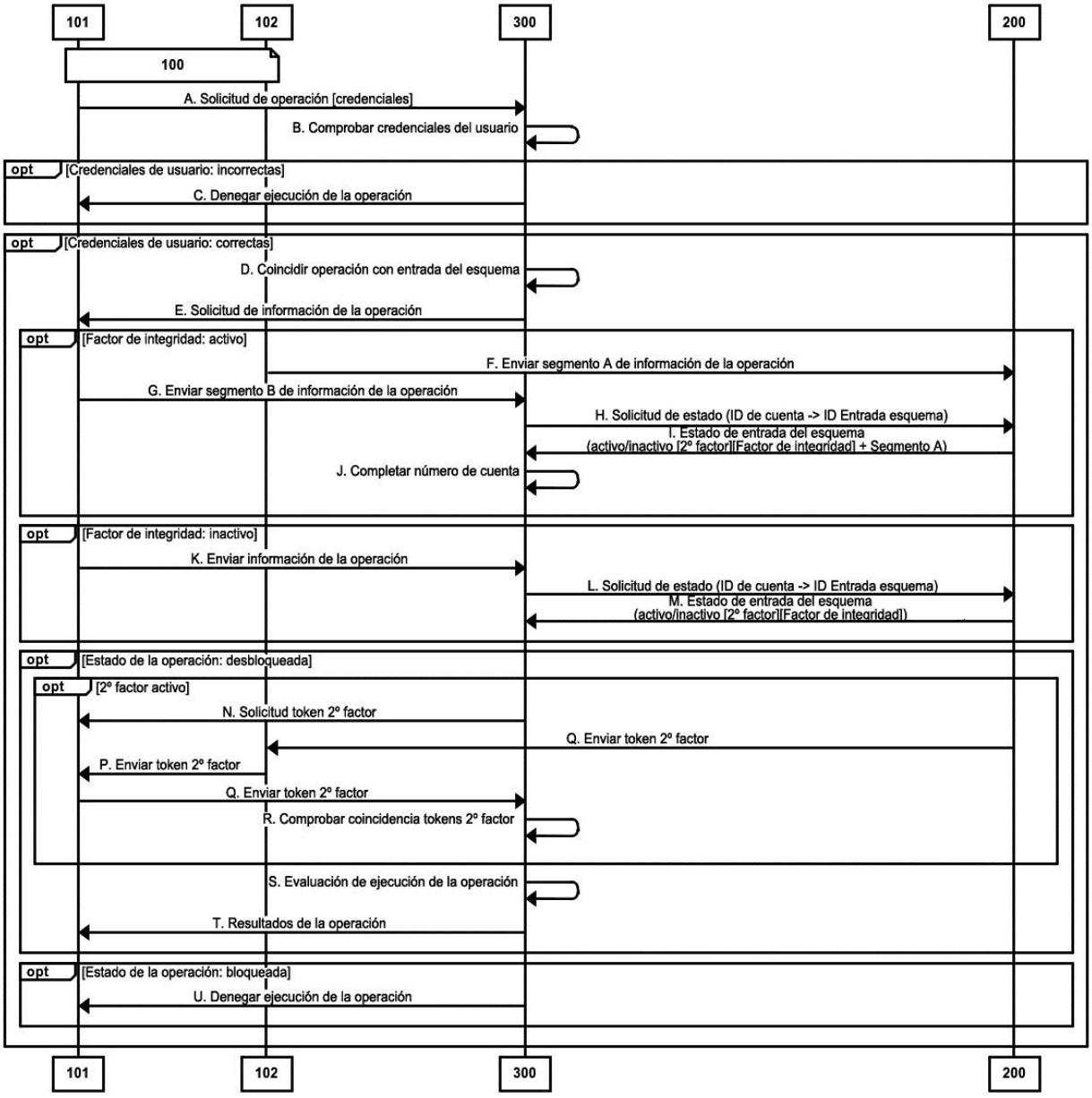
101
102
300
200
100
A. Solicitud de operación [credenciales]
B. Comprobar credenciales del usuario
opt
[Credenciales de usuario: incorrectas]
C. Denegar ejecución de la operación
opt
[Credenciales de usuario: correctas]
D. Coincidir operación con entrada del esquema
E. Solicitud de información de la operación
opt
[Factor de integridad: activo]
F. Enviar segmento A de información de la operación
G. Enviar segmento B de información de la operación
H. Solicitud de estado (ID de cuenta -> ID Entrada esquema)
I. Estado de entrada del esquema
(activo/inactivo [2º factor][Factor de integridad] + Segmento A)
J. Completar número de cuenta
opt
[Factor de integridad: inactivo]
K. Enviar información de la operación
L. Solicitud de estado (ID de cuenta -> ID Entrada esquema)
M. Estado de entrada del esquema
(activo/inactivo [2º factor][Factor de integridad])
opt
[Estado de la operación: desbloqueada]
opt
[2º factor activo]
N. Solicitud token 2º factor
Q. Enviar token 2º factor
P. Enviar token 2º factor
Q. Enviar token 2º factor
R. Comprobar coincidencia tokens 2º factor
S. Evaluación de ejecución de la operación
T. Resultados de la operación
opt
[Estado de la operación: bloqueada]
U. Denegar ejecución de la operación
101
102
300
200

Figura 7

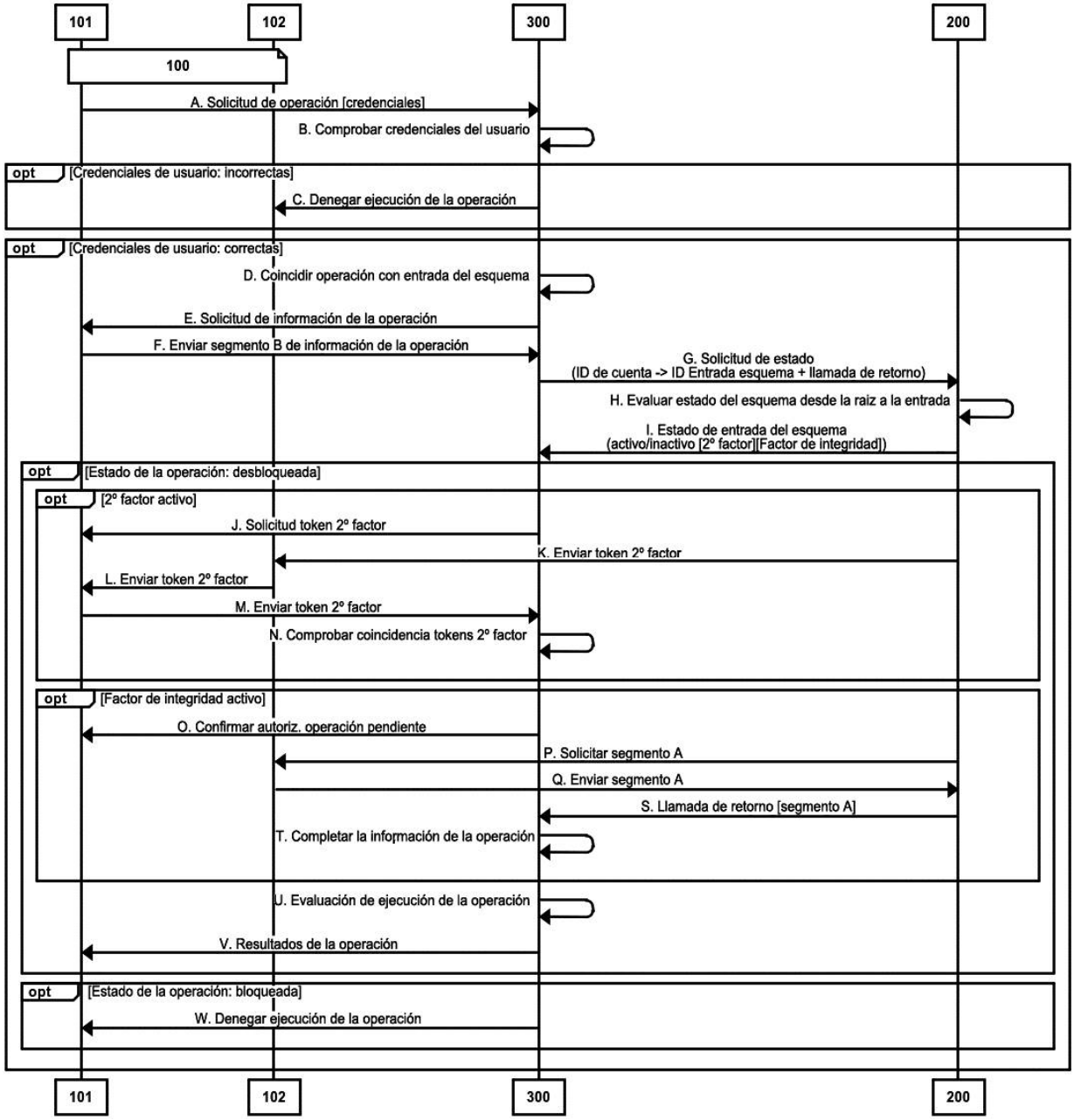
101
102
300
200
100
A. Solicitud de operación [credenciales]
B. Comprobar credenciales del usuario
opt
[Credenciales de usuario: incorrectas]
C. Denegar ejecución de la operación
opt
[Credenciales de usuario: correctas]
D. Coincidir operación con entrada del esquema
E. Solicitud de información de la operación
F. Enviar segmento B de información de la operación
G. Solicitud de estado
(ID de cuenta -> ID Entrada esquema + llamada de retorno)
H. Evaluar estado del esquema desde la raiz a la entrada
I. Estado de entrada del esquema
(activo/inactivo [2º factor][Factor de integridad])
opt
[Estado de la operación: desbloqueada]
opt
[2º factor activo]
J. Solicitud token 2º factor
K. Enviar token 2º factor
L. Enviar token 2º factor
M. Enviar token 2º factor
N. Comprobar coincidencia tokens 2º factor
opt
[Factor de integridad activo]
O. Confirmar autoriz. operación pendiente
P. Solicitar segmento A
Q. Enviar segmento A
S. Llamada de retorno [segmento A]
T. Completar la información de la operación
U. Evaluación de ejecución de la operación
V. Resultados de la operación
opt
[Estado de la operación: bloqueada]
W. Denegar ejecución de la operación
101
102
300
200

Figura 8