(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 750 151**

(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 13382398 (9)**

(97) Fecha y número de publicación de la concesión europea: **14.08.2019 EP 2860935**

(54) Título: **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:
25.03.2020

(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

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 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 procedimientos de autenticación y, por extensión, para fortificar los procedimientos 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 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 diversos recursos del sistema. La información del papel del 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 coincide 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 cuanto a 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 puede reproducir mensajes previamente capturados (entre un usuario legítimo y un verificador) para autenticarse como ese usuario al verificador. El Instituto Nacional de Estándares y Tecnología “*National Institute of Standard and Technology*” (NIST) recomienda 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 puede situarse entre un usuario y un verificador posteriormente a un intercambio de autenticación con éxito entre estas dos últimas partes. El atacante puede 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 de ataque, los ataques y las soluciones existentes se enfocan ambas en 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 procedimientos 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 procedimiento 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 éste 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 puede 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 cuanto a capacidad de uso, el uso de tokens de hardware resistentes a la manipulación va en contra la adopción de estas soluciones por los usuarios, y se han 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 cuanto a 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 la seguridad casi siempre se rompe procedente 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 procedimientos de autenticación sino también a los procedimientos de autorización de recursos y a todos los procedimientos relacionados con dichas cuentas.

Es necesario también reducir el riesgo asumido cuando se permiten algunos de los recursos y procedimientos asociados con las cuentas digitales a las que pueden acceder los usuarios después de una identificación inadecuada. Un ejemplo de esta situación es el fraude involucrado en los procedimientos que permiten la realización de una transacción (es decir pago) con un número de tarjeta de crédito, sin verificar que cualquiera que esté realizando la transacción es realmente el usuario legítimo (fraude de tarjeta no presente (CNP)). Las soluciones existentes para minimizar el riesgo relacionado con esta amenaza se basan en el uso de tokens de hardware proporcionadas por los primeros servidores (es decir los bancos). Sin embargo, estas soluciones presentan varias desventajas que han conducido a concluir que se necesita una mejor solución.

El documento US 2011/072507 A1 proporciona un sistema y método para establecer un túnel seguro entre un dispositivo cliente y un servidor remoto que utiliza múltiples identidades de usuario. En algunas realizaciones, también se proporciona una identidad de dispositivo cliente para autenticar el acceso al servidor remoto.

El documento US 2003/046551 A1 proporciona un método para lograr la autenticación de usuario de dos factores, que comprende proporcionar dos métodos de autenticación de usuario separados, permitiendo que un usuario comunique datos de autenticación para ambos métodos de autenticación a un primer sitio web usando Internet, y permitiendo la comunicación de al menos algunos de los datos de autenticación del primer sitio web a un segundo sitio web que también usa Internet. Por tanto, ambos sitios web participan en la autenticación del usuario utilizando los datos de autenticación.

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 el fraude CNP.

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 un método y un programa tal como se define en las reivindicaciones independientes 1 y 12. Las realizaciones particulares se definen en las reivindicaciones dependientes. La invención pretende impedir diversos ataques relacionados con los procedimientos de autenticación y autorización. Esta 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 procedimiento de autenticación/autorización bloqueando temporalmente el mecanismo de ejecución de la operación. 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 procedimientos de gestión de cuentas o incluso permitan al usuario activarla.

La solución propuesta usa una tecnología de comunicación de campo cercano (NFC, de “Near Field Communication”) para impedir dicho fraude CNP. El usuario puede usar un token NFC para eludir ataques que se basen en el robo de credenciales y se enfoquen en adquirir privilegios sobre operaciones críticas. Se pueden suponer dos escenarios diferentes. Una posibilidad puede ser que un primer servidor entregue una tarjeta NFC particular a sus usuarios y les permita enlazar esta tarjeta con la ejecución de algunas de las operaciones a través de dicho servidor. En este caso, se puede implementar un mecanismo criptográfico para evitar que una tarjeta pueda ser clonada o falsificada. Otra alternativa supone que es posible asociar cualquier tarjeta NFC que tenga el usuario. Este último caso se diseña para aplicaciones de seguridad más baja donde la duplicación del token es un riesgo aceptable. En ambos casos, el uso de esta clase de token supone un factor extra para mitigar el fraude CNP, debido a que, incluso en el caso de seguridad más baja, un atacante ha de haber robado tres factores (por ejemplo, el número de la tarjeta de crédito, nombre de usuario/palabra clave con el dicho segundo servidor y la tarjeta NFC asociada con el pago en Internet con tarjeta) para tener éxito en el ataque. En ambos casos, la presencia de un lector NFC se debería implementar dentro de un programa dedicado del usuario y se supone que dicho primer servidor instruye al usuario para usar apropiadamente esas tarjetas NFC.

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 ser registrado en un servicio en nombre de dicho usuario si dicho estado asociado se ha establecido como válido, o

- rechazo de dicha solicitud para ser registrado en un servicio si dicho estado asociado se ha establecido como inválido,

en el que, 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 en dicho primer servidor usando al menos una parte de los recursos de dicho primer servidor, el método comprende las siguientes etapas:

- coincidencia, por dicho primer servidor, si dicha solicitud de operación corresponde con una entrada en relación a un estado de entrada del esquema definido por el primer servidor para una cuenta del usuario;

- asociación, de al menos un token de hardware tal como una tarjeta de Comunicación en Campo Cercano (NFC) para dicha operación;

- solicitud, por dicho primer servidor a dicho segundo servidor de un estado asociado para dicha operación;

- inicialización de un intercambio de credenciales entre dicho primer servidor y dicho segundo servidor;

- evaluación, en dicho segundo servidor una información del estado de entrada del esquema de estado desde una raíz a dicha entrada;

- envío, por dicho segundo servidor, del resultado de dicha de la información de 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 generada dicho token de seguridad durante un procedimiento 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 de Corto (SMS) o un correo electrónico, 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 éste 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 niños (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, previa a dicha etapa de asociación del token de hardware, el primer servidor solicita al usuario la información necesaria para realizar dicha operación. Entonces el primer servidor realiza dicha solicitud del estado asociado a dicha operación tras la recepción de dicha información necesaria. De acuerdo con esta realización, el

segundo servidor, en dicha etapa de envío del resultado de la evaluación de la información de estado de la entrada del esquema al primer servidor, también envía, por medio del programa dedicado, una indicación acerca de un uso de una tarjeta que confirme una acción de presencia física de dicho usuario. Es decir, el primer servidor es informado si ha tenido lugar una CNP.

En caso de que haya sucedido u ocurrido el uso de una tarjeta confirmando la acción de presencia física del usuario, el segundo servidor solicita a dicho usuario, a través de dicho programa dedicado, el envío de dicho token de hardware; entonces el segundo servidor comprueba si dicho token de hardware recibida a través del programa dedicado coincide con dicho token de hardware asociada en relación con dicha operación; y establece el estado de dicha operación teniendo en cuenta el resultado de dicha comprobación.

En una realización, en la etapa de asociación de dicho token de hardware, dicho token de hardware se puede asociar mediante la introducción del usuario en dicho segundo servidor y validado por el segundo servidor. Se puede usar un segundo factor de autenticación dentro de la respuesta de dicho estado de entrada del esquema. Involucrando este segundo factor de autenticación:

- el envío, por dicho segundo servidor de una OTP al primer servidor dentro de la respuesta a la solicitud;

- 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, una puertas lógicas programables en campo (FPGA), 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 6.

Por lo tanto, la presente invención permite que el usuario use el token de hardware asociado con las operaciones para probar que el usuario legítimo conoce que han sido solicitadas las operaciones. El usuario puede mitigar el fraude relacionado con las operaciones proporcionadas por diferentes proveedores de servicios cuando estas operaciones se realizan en base a que el usuario es el propietario legítimo de la información particular necesaria para la operación pero sin la oportunidad de verificar este hecho (es decir operaciones de tarjeta no presente).

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 bloqueo/desbloqueo. De hecho, se pueden aplicar los mismos conceptos introducidos para controlar el procedimiento 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)) el riesgo relativo (RR) satisfaga la siguiente expresión:

$$RR = \frac{p(Ataque\,con\,éxito \mid \text{expuesto})}{p(Ataque\,con\,éxito \mid \text{sin exposición})} > 1 \qquad \text{Ec. 1}$$

En esta expresión, se asume que la probabilidad de éxito de un ataque se relaciona directamente con el tiempo de exposición. Esto es, 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:

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

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 procedimiento de autenticación. La experiencia profesional y el conocimiento técnico de las técnicas de ataque documentadas para romper los sistemas de autorización confirman la suposición realizada anteriormente (RR > 1). Por lo tanto, se puede afirmar que ARP > 1 una vez que se adopta la invención.

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 procedimiento 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.

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 al procedimiento de verificación del estado de la operación.

La figura 5 es un diagrama de flujo que ilustra una primera opción para mitigar el fraude CNP, de acuerdo con una primera realización de la presente invención.

La figura 6 es un diagrama de flujo que ilustra el procedimiento completo seguido por la presente invención para mitigar el fraude CNP, de acuerdo con una segunda 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 a la figura 1, se usa un dispositivo 100 de cálculo tal como un teléfono móvil, un teléfono inteligente, una tablet-PC o una PDA entre otros, por dicho usuario para registrarse en un programa 102 dedicado en comunicación con un segundo 200 servidor y para gestionar el estado de cada primer 300 servidor 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 300 servidor. Tal como se establece a continuación, esta acción puede mejorar el control definido para esta cuenta por la decisión del primer 300 servidor. En esta decisión, el primer 300 servidor 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 300 servidor, a través del segundo 200 servidor. El primer 300 servidor 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 200 servidor para verificar si el usuario 100 es quien realmente está solicitando dicha operación y para confirmar si la operación que ha llegado al primer 300 servidor es exactamente como la que el usuario 100 ha ordenado.

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

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

El núcleo del segundo servidor implementa la función principal del segundo 200 servidor: bloquear o desbloquear dicha cuenta de usuario con el primer 300 servidor y las operaciones proporcionadas por el primer 300 servidor. Para hacer esto, el segundo 200 servidor acepta y procesa las solicitudes de comprobación de estado enviadas

desde el primer 300 servidor. Este segundo 200 servidor también gestiona todos los datos acerca de los enlaces con dicho primer 300 servidor 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 200 servidor, puede establecer bloqueos con diferentes proveedores de servicios, como dicho primer 300 servidor. Para activar estos bloqueos el segundo 200 servidor, de acuerdo con una realización, genera un token. Son necesarios un token único y la definición de canales seguros para completar el procedimiento de vinculación entre el usuario 100 y el primer 300 servidor. Como resultado de este procedimiento de vinculación, el token criptográfico se envía desde el segundo 200 servidor al primer 300 servidor 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 200 servidor 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 200 servidor incorporará toda la lógica necesaria para la generación y comunicación de la OTP. Cuando el segundo 200 servidor recibe una solicitud desde el primer 300 servidor 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 300 servidor junto con el estado de la cuenta. Si el estado es ACTIVO y el usuario 100 tiene activado el segundo factor, el primer 300 servidor 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 200 servidor incorpora la lógica necesaria para obtener la información crítica del usuario 100 y desde el primer 300 servidor y para comprobar si ambas son iguales. El segundo 200 servidor envía el resultado de la comprobación como el estado de la cuenta al primer 300 servidor. En caso de falta de coincidencia, el primer 300 servidor puede concluir que un intruso puede estar interceptando la información desde el usuario 100. El primer 300 servidor puede construir entonces mecanismos para eludir el fraude y para elevar alertas de seguridad.

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

Cuando un primer 300 servidor envía una Solicitud de estado (Status_Request), el segundo 200 servidor 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 200 servidor registra este evento como un intento falso. El segundo 200 servidor 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 correo electrónico, un mensaje mediante una aplicación de mensajería de teléfono inteligente, mediante un resaltado o notificación en dicho programa 102 dedicado de dicho dispositivo 100 de cálculo del usuario, etc.) o solamente actualizar las estadísticas para una revisión posterior. Entonces el segundo 200 servidor 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 200 servidor 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 procedimiento de registro). Esta dependencia se establece con una jerarquía en la que los cambios en las entradas raíz se propagan a sus niños.

La figura 4 ilustra el procedimiento de verificación del estado de la operación de una operación solicitada por el usuario 100. Esta operación es propuesta por el primer 300 servidor 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 300 servidor. Esta operación puede ser el registro en un servicio particular o ejecutar alguna operación relacionada con los servicios proporcionados por el primer 300 servidor (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 300 servidor, 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 200 servidor este estado de entrada (E).

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

A continuación, para mitigar los efectos del fraude CNP, la invención propone dos opciones o realizaciones diferentes. Como se ha dicho anteriormente, se puede usar un token NFC, en este caso por el usuario 100, para evitar ataques.

La figura 5 ilustra una primera realización propuesta por la invención. En esta realización, se muestra el procedimiento de verificación del estado de la operación con protección contra fraude NCP, en base a tarjetas NFC. Esta operación se propone por el primer 300 servidor adjunto a la gestión de cuentas. El usuario 100, usando por ejemplo el navegador 101, solicita ejecutar una operación relacionada con una cuenta (A) del primer 300 servidor. Esta operación puede incluir 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 ese modo una vez que se ha validado la existencia del usuario (B) por dicho primer 300 servidor, 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 100 envía la información de la operación al primer 300 servidor. Una vez que se recibe la información de la operación, el primer 300 servidor solicita el estado para esta operación al segundo 200 servidor (G).

Entonces el segundo 200 servidor inicializa el intercambio de credenciales antes de la evaluación del estado de entrada del esquema desde la raíz a la entrada (H). 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 entrada del esquema se envía (I) y, con esta información, el primer 300 servidor toma la decisión de permitir o bloquear el acceso del usuario a la operación. En este punto, el primer servidor es informado de si la presencia de CNP está pendiente de una acción del usuario. Si se confirma esta presencia entonces el

primer servidor espera a recibir la llamada de retorno que informa sobre el resultado de la verificación de la integridad.

Opcionalmente, si el estado de entrada del esquema es válido (desbloqueado) y el segundo factor de autenticación está activado, el segundo 200 servidor puede enviar una OTP al primer 300 servidor dentro de la respuesta de la solicitud de estado. Este primer 300 servidor ha de emplearla para completar la autenticación. El primer 300 servidor solicita al usuario 100 la OTP que va a ser un segundo factor temporal (K). El segundo 200 servidor envía la misma OTP al programa 102 dedicado del usuario (J). El usuario 100 recupera la OTP desde el programa 102 dedicado y la introduce en el navegador 101 (L) y la envía al primer 300 servidor (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 la operación esté pendiente de la autenticación del usuario a través de la presencia del token NFC, el primer 300 servidor, que está esperando a una llamada de retorno desde el segundo 200 servidor, informa al usuario 100 de que la operación está pendiente de autenticación (O). Asíncronamente, el segundo 200 servidor solicita al usuario 100 a través del programa 102 dedicado probar la posesión del token NFC (Q). Una vez que el usuario 100 presente este token A usando el programa 102 dedicado (R), el segundo 200 servidor comprueba si la información relacionada con el token NFC recibido coincide (S) con la información previamente registrada sobre el token asociado con esta operación. A continuación, el segundo 200 servidor puede realizar la llamada de retorno al primer 300 servidor para comunicar los resultados de este procedimiento de verificación (T). El primer 300 servidor puede completar la información de la operación necesaria para realizar la acción solicitada (U).

La figura 6 ilustra una segunda realización propuesta por la invención para la mitigación del fraude CNP. En este caso la figura ilustra el procedimiento completo seguido por la invención. Se muestra una alternativa a la protección contra fraude CNP basada en el uso de tarjetas NFC. El objetivo de esta protección es incrementar el nivel de seguridad en algunas operaciones particulares. Esta operación se propone por el primer servidor 100 adjunto a la gestión de la cuenta.

Un ejemplo para ilustrar cómo esta opción difiere de la realización descrita en la figura 5, es considerar a un usuario 100 que va a realizar una transacción a través de una página web usando su tarjeta de crédito en un navegador 101 web. Cuando la página web solicita el número de la tarjeta para completar la transacción, el usuario 100 puede desbloquear la operación de transacción por Internet definida para la tarjeta de crédito del usuario, con sólo registrándose en el programa 102 dedicado del usuario y presentando ahí el token NFC asociado con la operación. Este cambio de estado puede establecerse para que sea temporal (es decir sólo unos pocos minutos). Dicha figura 6 ilustra cómo en un solicitud de cooperación realizada por usuario 100 se puede colocar la interacción NFC. Sin embargo, esta integración es asíncrona de modo que se puede realizar en cualquier momento antes de que el primer 300 servidor solicite el estado de la operación a dicho segundo 200 servidor.

Una vez que un usuario 100 desea ejecutar una de estas operaciones, se registra en dicho segundo 200 servidor (A, B) y presenta la tarjeta NFC. Previamente, el token NFC contenido en la tarjeta NFC se asoció con dicha operación. Esto supone que cuando quiera que se envíe el token NFC a dicho segundo 200 servidor (C), y después de un procedimiento de validación (E), todos las operaciones asociadas con el token NFC se convierten en activas (E). Cuando expira un tiempo prefijado el segundo 200 servidor devuelve todas estas operaciones a sus estados previos

El usuario 100, usando por ejemplo un navegador 101, solicita, de acuerdo con una realización, ejecutar una operación asociada con un servicio (F) de un primer 300 servidor. Una vez que la existencia del usuario ha sido validada (G) por dicho primer 300 servidor, este último resuelve la correspondencia de esta operación con una de las entradas incluidas en el esquema de autorización (I) y solicita al segundo 200 servidor el estado la cuenta del usuario (J). Entonces el segundo 200 servidor inicializa el intercambio de credenciales antes de que se envíe la información de estado de la cuenta (L). Con esta información, el primer 300 servidor toma la decisión de permitir o bloquear el acceso del usuario.

Opcionalmente, si el estado de entrada del esquema es válido (desbloqueado) y se activa el segundo factor de autenticación, dentro de la respuesta de la solicitud, el segundo 200 servidor envía una OTP al primer 300 servidor que ha de emplear para completar la autenticación. El primer 300 servidor solicita al usuario 100 la OTP que va a ser el segundo factor temporal (M). Entonces el segundo 200 servidor envía la misma OTP al programa 102 dedicado del usuario (N). El usuario 100 recupera la OTP desde el programa 102 dedicado y la introduce en el navegador 101 (O) y la envía al primer 300 servidor (P). El primer 300 servidor puede comprobar si la OTP enviada usando el navegador 101 coincide con la recibida con el estado de la cuenta (Q). Dependiendo de los resultados de esta verificación, el primer 300 servidor realiza el procedimiento de autorización (R) y comunica el resultado al usuario a través del navegador 101 (S).

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

REIVINDICACIONES

1. Método implementado en ordenador para impedir ataques contra sistemas de autorización, en el que un segundo (200) servidor en conexión con un dispositivo de cálculo de un usuario (100), a través de un segundo (102) programa dedicado instalado en dicho dispositivo de cálculo, se usa para gestionar un estado de las cuentas, el usuario (100) tiene un primer (300) servidor y un estado de las operaciones definido para una cuenta particular, estableciendo dicho estado de la cuenta y dicho estado de la operación, siempre que el usuario (100) quiere, como válido o como inválido por el usuario (100) a través del segundo (102) programa dedicado y almacenado en una memoria del segundo (200) servidor, y estableciendo dicho estado de la cuenta y dicho estado de la operación por el usuario (100) una vez que se completa un procedimiento de emparejamiento con el segundo (200) servidor, garantizando dicho procedimiento de emparejamiento la privacidad del usuario (100), comprendiendo el método:

- recibir, por dicho primer (300) servidor, del usuario (100) usando un primer programa dedicado que incluye un navegador (101), una solicitud para estar registrado en un servicio de dicho primer (300) servidor, incluyendo dicha solicitud la provisión de información de identificación que valida la identidad del usuario (100) en el primer (300) servidor;

- una vez que la existencia del usuario ha sido validada por el primer (300) servidor, que recibe, por dicho segundo (200) servidor, de dicho primer (300) servidor, una solicitud sobre un estado con respecto a una cuenta del usuario (100) en el primer (300) servidor;

- en respuesta a la recepción de la solicitud, inicializando un primer intercambio de credenciales entre dicho primer (300) servidor y dicho segundo (200) servidor para proporcionar autenticación mutua, realizándose el primer intercambio de credenciales a través de un procedimiento de autenticación basado en el intercambio de certificados;

- verificar, por el segundo (200) servidor, dicho estado de la cuenta;

- enviar, por dicho segundo (200) servidor, dicho estado de la cuenta a dicho primer (300) servidor; y

- usar, por dicho primer (300) servidor, dicho estado de la cuenta recibido para:

    - autorizar dicha solicitud para ser registrado en el servicio si dicho estado de la cuenta se ha establecido como válido, o

    - rechazar dicha solicitud para ser registrado en el servicio si dicho estado de la cuenta se ha establecido como inválido,

en el que, en respuesta a dicha solicitud para ser registrado en el servicio que se autoriza, el usuario (100) realiza una solicitud adicional a través del primer (101) programa dedicado para realizar una operación relacionada con dicha cuenta del usuario (100) en el primer (300) servidor, comprendiendo además el método las siguientes etapas:

- determinar, por el primer (300) servidor, qué entrada en un esquema de una jerarquía definida por dicha cuenta corresponde con dicha operación solicitada;

- asociar, o bien por el primer (300) servidor o bien por el usuario (100) a través del segundo programa (102) dedicado, en al menos un token de hardware tal como una tarjeta de comunicación de campo cercano, NFC, a dicha operación solicitada para evitar fraude de tarjeta no presente, CNP;

- solicitar, por dicho primer (300) servidor, a dicho segundo (200) servidor, el estado de la operación definido por el usuario (100) sobre dicha entrada;

- inicializar un segundo intercambio de credenciales entre el primer (300) servidor y el segundo (200) servidor;

- evaluar, por el segundo (200) servidor, una información de estado de entrada de esquema desde una raíz de dicho esquema de jerarquía a dicha entrada;

- enviar, por el segundo (200) servidor, el resultado de dicha evaluación de información de estado de entrada de esquema al primero (300) servidor, y

- usar, por el primer (300) servidor, el resultado de dicha evaluación para permitir o bloquear dicha

operación solicitada.

2. Método implementado en ordenador de acuerdo con la reivindicación 1, que comprende previamente a dicha etapa de asociación del token de hardware, la petición, de dicho primer (300) servidor a dicho usuario (100), de la información necesaria para realizar dicha operación y la realización de dicha solicitud del estado de la operación tras la recepción por dicho primer (300) servidor de dicha información necesaria.

3. Método implementado en ordenador de acuerdo con las reivindicaciones previas, en el que en dicha etapa de envío, por el segundo (200) servidor, del resultado de dicha información del estado de entrada del esquema, se envía también una indicación sobre el uso de una tarjeta que confirme una acción de presencia física de dicho usuario (100) usando el segundo (102) programa dedicado.

4. Método implementado en ordenador de acuerdo con la reivindicación 3, en el que si dicho uso de una tarjeta confirmando una acción de presencia física del usuario ha sido indicada como sucediendo, dicho segundo (200) servidor comprende:

- la solicitud a dicho usuario (100) a través de dicho segundo (102) programa dedicado para el envío de dicho token de hardware;

- la comprobación de si dicho token de hardware recibida a través del segundo (102) programa dedicado coincide con dicho token de hardware asociada en relación con dicha operación, y

- establecimiento del estado de dicha operación teniendo en cuenta el resultado de dicha comprobación.

5. Método implementado en ordenador de acuerdo con la reivindicación 1, en el que en dicha etapa de asociación de dicho token de hardware, dicho token de hardware se asocia mediante la introducción del usuario (100) en dicho segundo (200) servidor y validado por el segundo (200) servidor.

6. Método implementado en ordenador de acuerdo con las reivindicaciones previas, que comprende además el uso de un segundo factor de autenticación, si dicho estado de entrada del esquema se establece como válido, comprendiendo dicho segundo factor de autenticación:

- el envío, por dicho segundo (200) servidor de una OTP al primer (300) servidor dentro de la respuesta de la solicitud;

- solicitud, por el primer (300) servidor al usuario (100), de una OTP que el usuario (100) va a usar como segundo factor temporal;

- el envío, por el segundo (200) servidor de la misma OTP enviada al primer (300) servidor al usuario a través de dicho primer programa (101) dedicado;

- recuperación, por el usuario (100), de dicho segundo factor temporal solicitado de OTP a través de dicho programa dedicado (102), introduciéndola en el primer programa (101) dedicado y enviando adicionalmente el factor segundo temporal solicitado de OTP a través de dicho primer programa (101) dedicado al primer (300) servidor; y

- comprobación, por el primer (300) servidor, si la OTP recibida desde el segundo (200) servidor y el segundo factor OTP temporal recibido desde dicho primer programa (101) dedicado coinciden, con el fin de permitir o bloquear dicha operación solicitada.

7. Método implementado en ordenador de acuerdo con la reivindicación 1, en el que dicha etapa de evaluación se realiza para cada etapa hallada hasta alcanzar la entrada del esquema.

8. Método implementado en ordenador de acuerdo con la reivindicación 1, que comprende la notificación, por dicho segundo (200) servidor, el usuario (100) en caso de que dicha solicitud para ser registrado en un servicio del primer servidor se rechace.

9. Método implementado en ordenador de acuerdo con la reivindicación 8, en el que dicha notificación comprende una de un envío de un Servicio de Mensajes Cortos (SMS), un envío de un correo electrónico, un envío de un mensaje mediante una aplicación de mensajería de teléfono inteligente, un resalte o notificación en dicho programa (102) dedicado de dicho dispositivo de cálculo de usuario.

10. Método implementado en ordenador de acuerdo con la reivindicación 1, en el que dicho estado de la cuenta se establece como válido o como inválido un cierto período de tiempo.

11. Método implementado en ordenador de acuerdo con la reivindicación 1, en el que dicha solicitud para ser registrado en un servicio y/o dicha solicitud para realizar una operación se registran con el fin de proporcionar estadísticas.

12. 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.

13. Programa de ordenador de acuerdo con la reivindicación 12, que comprende además medios de código de programa adaptados para realizar un segundo factor de autenticación de acuerdo con el método de la reivindicación 6.

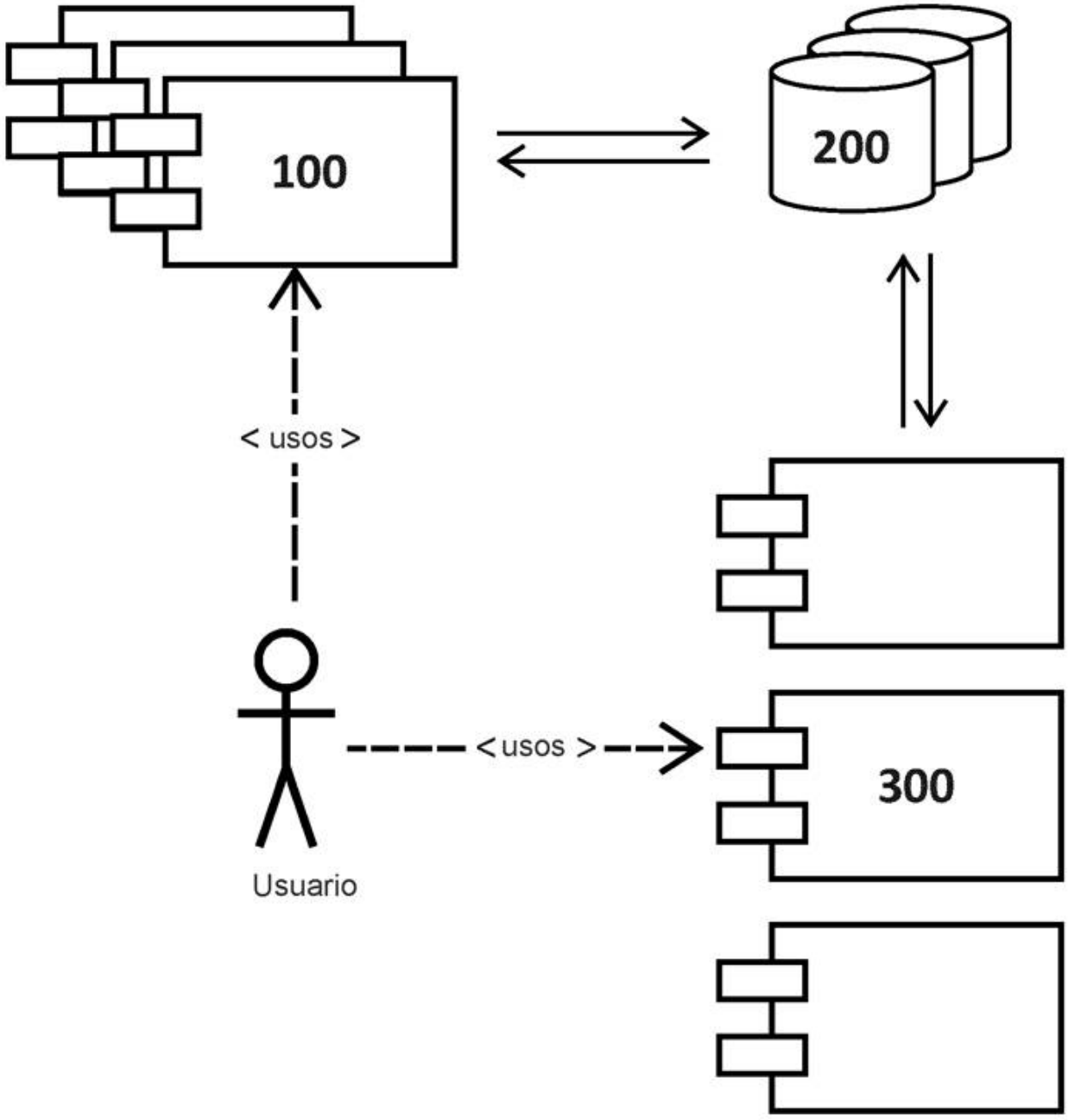

FIG. 1

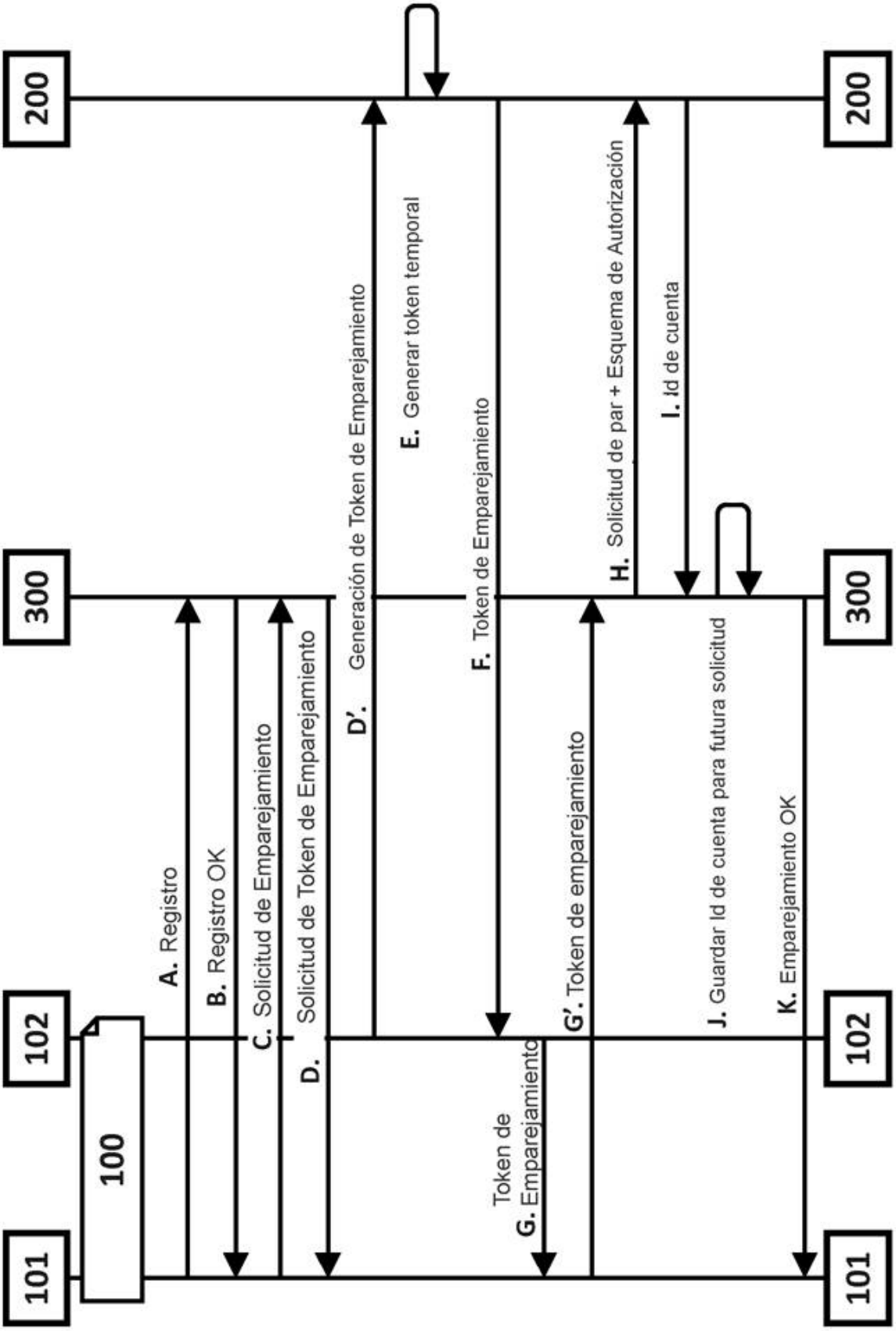
200
300
102
101
100
A. Registro
B. Registro OK
C. Solicitud de Emparejamiento
D. Solicitud de Token de Emparejamiento
D'. Generación de Token de Emparejamiento
E. Generar token temporal
F. Token de Emparejamiento
G. Token de Emparejamiento
G'. Token de emparejamiento
H. Solicitud de par + Esquema de Autorización
I. Id de cuenta
J. Guardar Id de cuenta para futura solicitud
K. Emparejamiento OK
200
300
102
101

FIG. 2

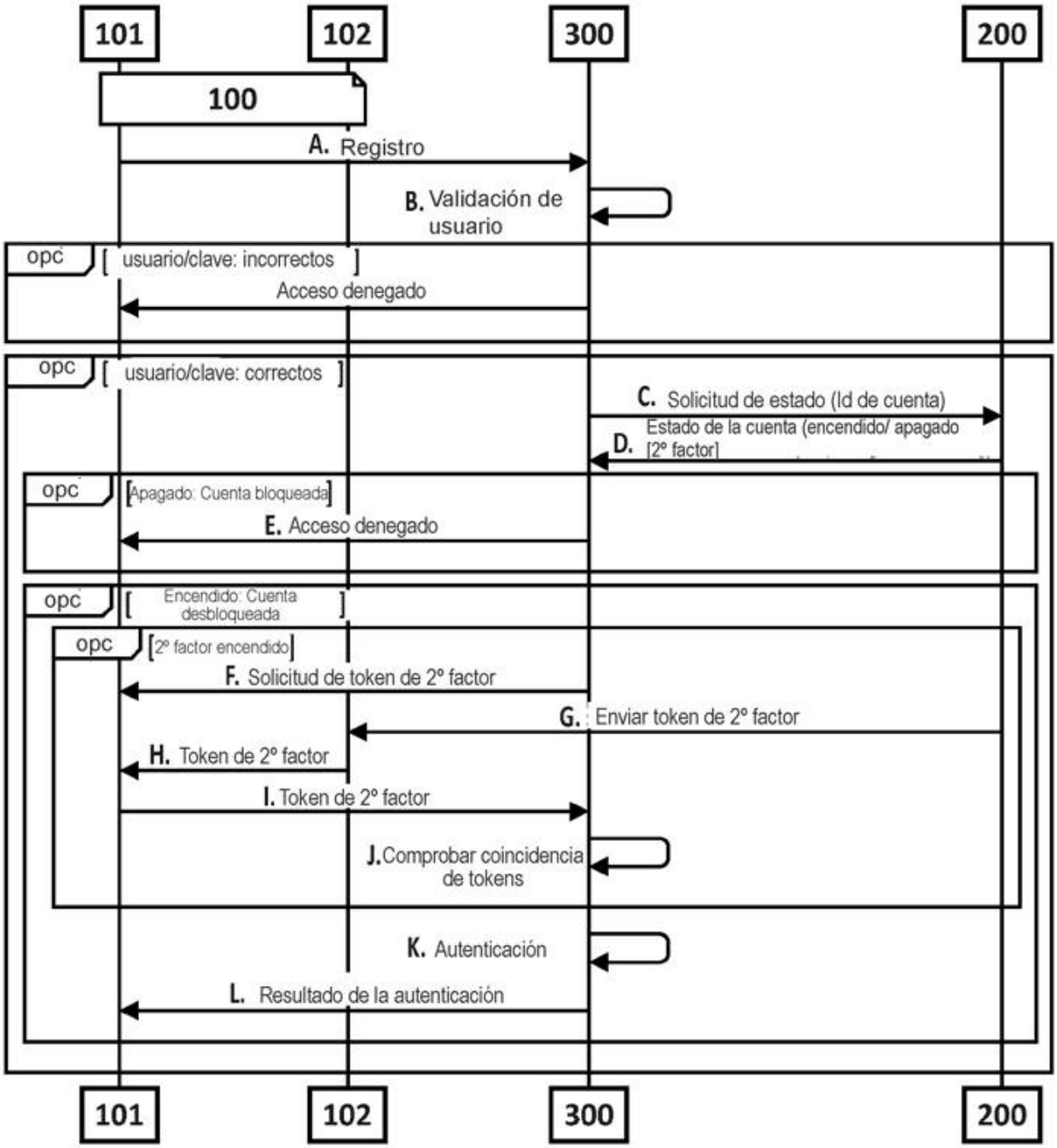
101
102
300
200
100
A. Registro
B. Validación de usuario
opc
[usuario/clave: incorrectos]
Acceso denegado
opc
[usuario/clave: correctos]
C. Solicitud de estado (Id de cuenta)
Estado de la cuenta (encendido/ apagado
D. [2º factor]
opc
[Apagado: Cuenta bloqueada]
E. Acceso denegado
opc
[Encendido: Cuenta desbloqueada]
opc
[2º factor encendido]
F. Solicitud de token de 2º factor
G. Enviar token de 2º factor
H. Token de 2º factor
I. Token de 2º factor
J. Comprobar coincidencia de tokens
K. Autenticación
L. Resultado de la autenticación
101
102
300
200

FIG. 3

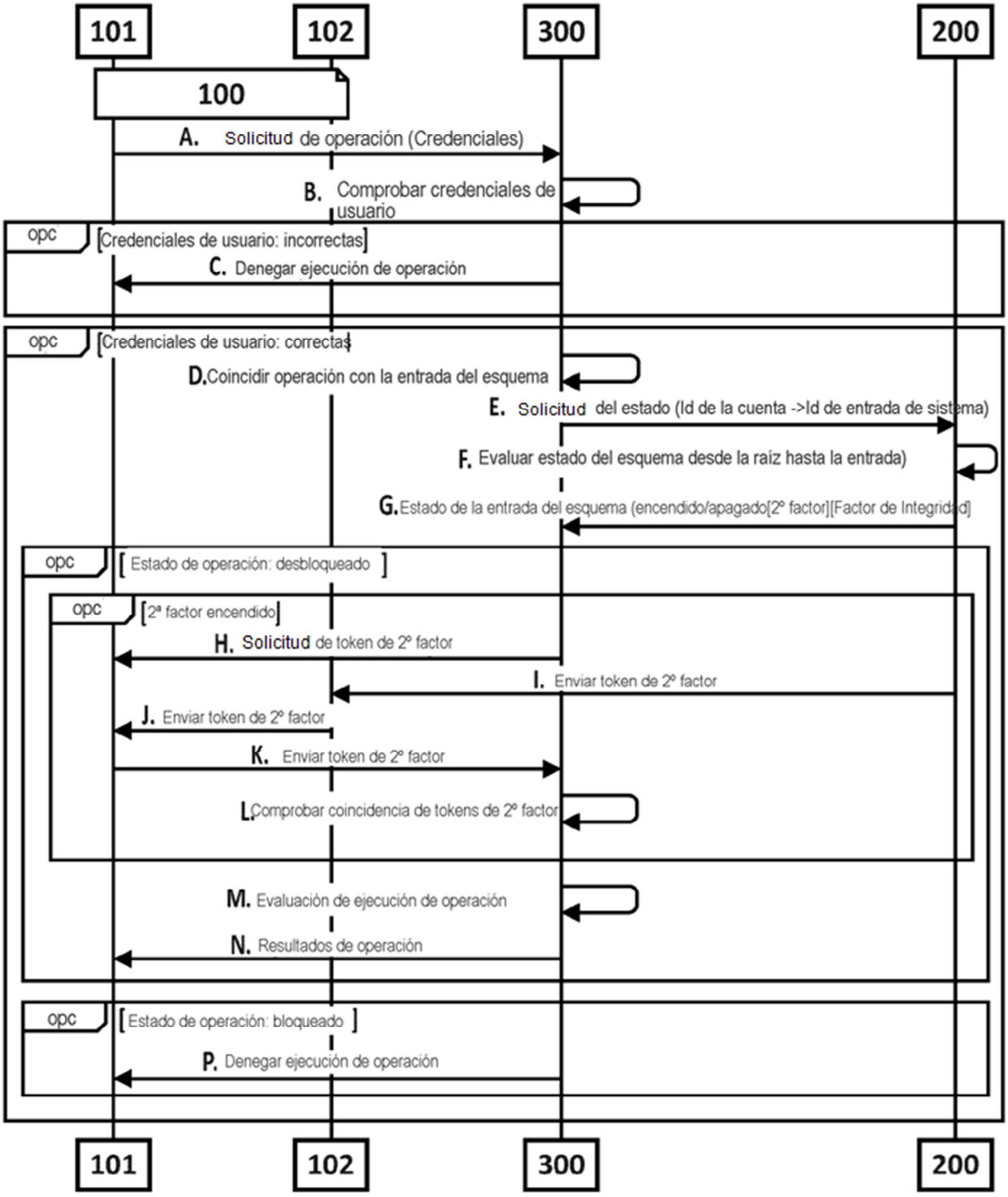
101
102
300
200
100
A. Solicitud de operación (Credenciales)
B. Comprobar credenciales de usuario
opc
[Credenciales de usuario: incorrectas]
C. Denegar ejecución de operación
opc
[Credenciales de usuario: correctas]
D. Coincidir operación con la entrada del esquema
E. Solicitud del estado (Id de la cuenta ->Id de entrada de sistema)
F. Evaluar estado del esquema desde la raíz hasta la entrada)
G. Estado de la entrada del esquema (encendido/apagado[2º factor][Factor de Integridad]
opc
[Estado de operación: desbloqueado]
opc
[2ª factor encendido]
H. Solicitud de token de 2º factor
I. Enviar token de 2º factor
J. Enviar token de 2º factor
K. Enviar token de 2º factor
L. Comprobar coincidencia de tokens de 2º factor
M. Evaluación de ejecución de operación
N. Resultados de operación
opc
[Estado de operación: bloqueado]
P. Denegar ejecución de operación
101
102
300
200

FIG. 4

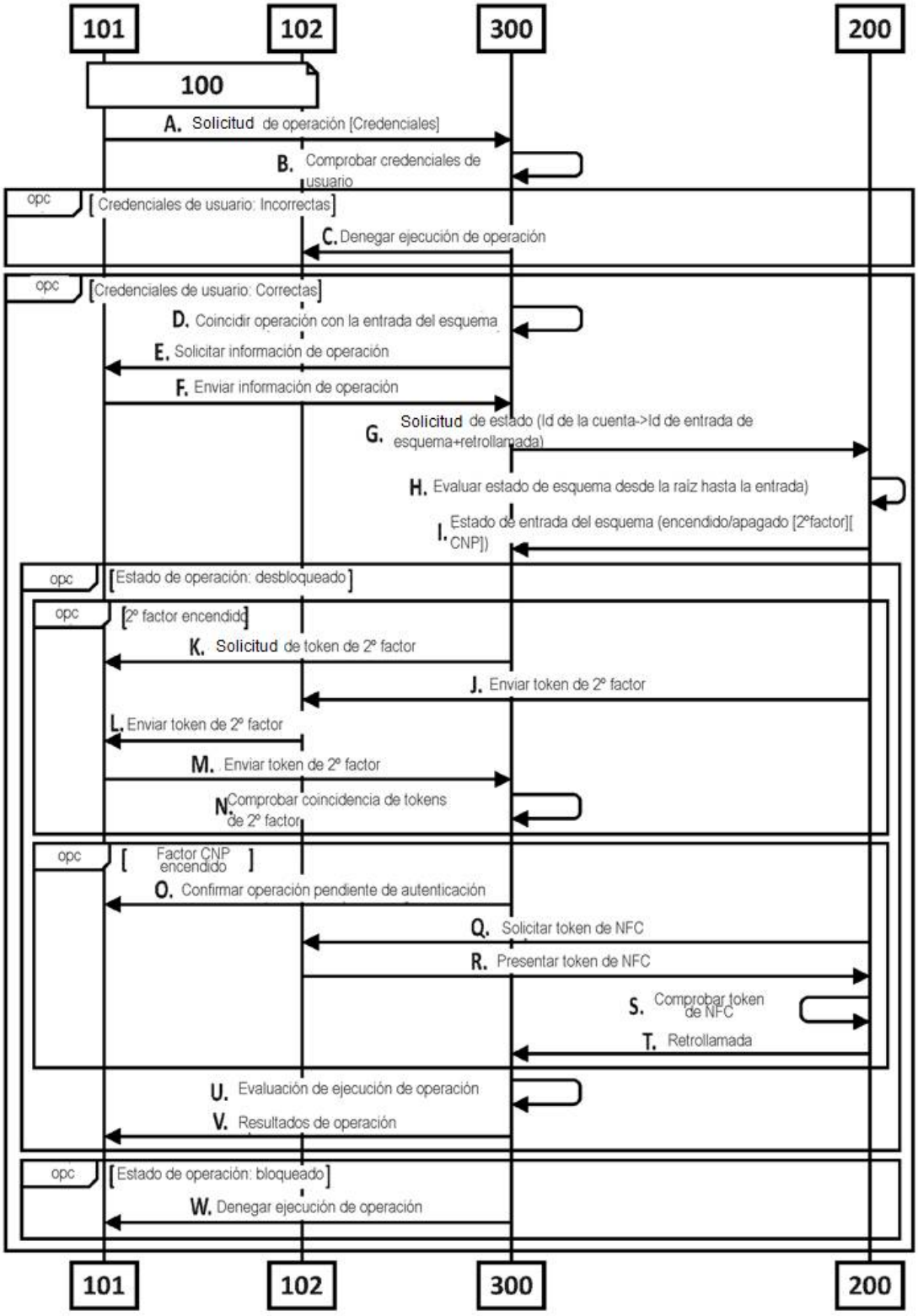
101
102
300
200
100
A. Solicitud de operación [Credenciales]
B. Comprobar credenciales de usuario
opc
[Credenciales de usuario: Incorrectas]
C. Denegar ejecución de operación
opc
[Credenciales de usuario: Correctas]
D. Coincidir operación con la entrada del esquema
E. Solicitar información de operación
F. Enviar información de operación
G. Solicitud de estado (Id de la cuenta->Id de entrada de esquema+retrollamada)
H. Evaluar estado de esquema desde la raíz hasta la entrada)
I. Estado de entrada del esquema (encendido/apagado [2ºfactor][CNP])
opc
[Estado de operación: desbloqueado]
opc
[2º factor encendido]
K. Solicitud de token de 2º factor
J. Enviar token de 2º factor
L. Enviar token de 2º factor
M. Enviar token de 2º factor
N. Comprobar coincidencia de tokens de 2º factor
opc
[Factor CNP encendido]
O. Confirmar operación pendiente de autenticación
Q. Solicitar token de NFC
R. Presentar token de NFC
S. Comprobar token de NFC
T. Retrollamada
U. Evaluación de ejecución de operación
V. Resultados de operación
opc
[Estado de operación: bloqueado]
W. Denegar ejecución de operación
101
102
300
200

FIG. 5

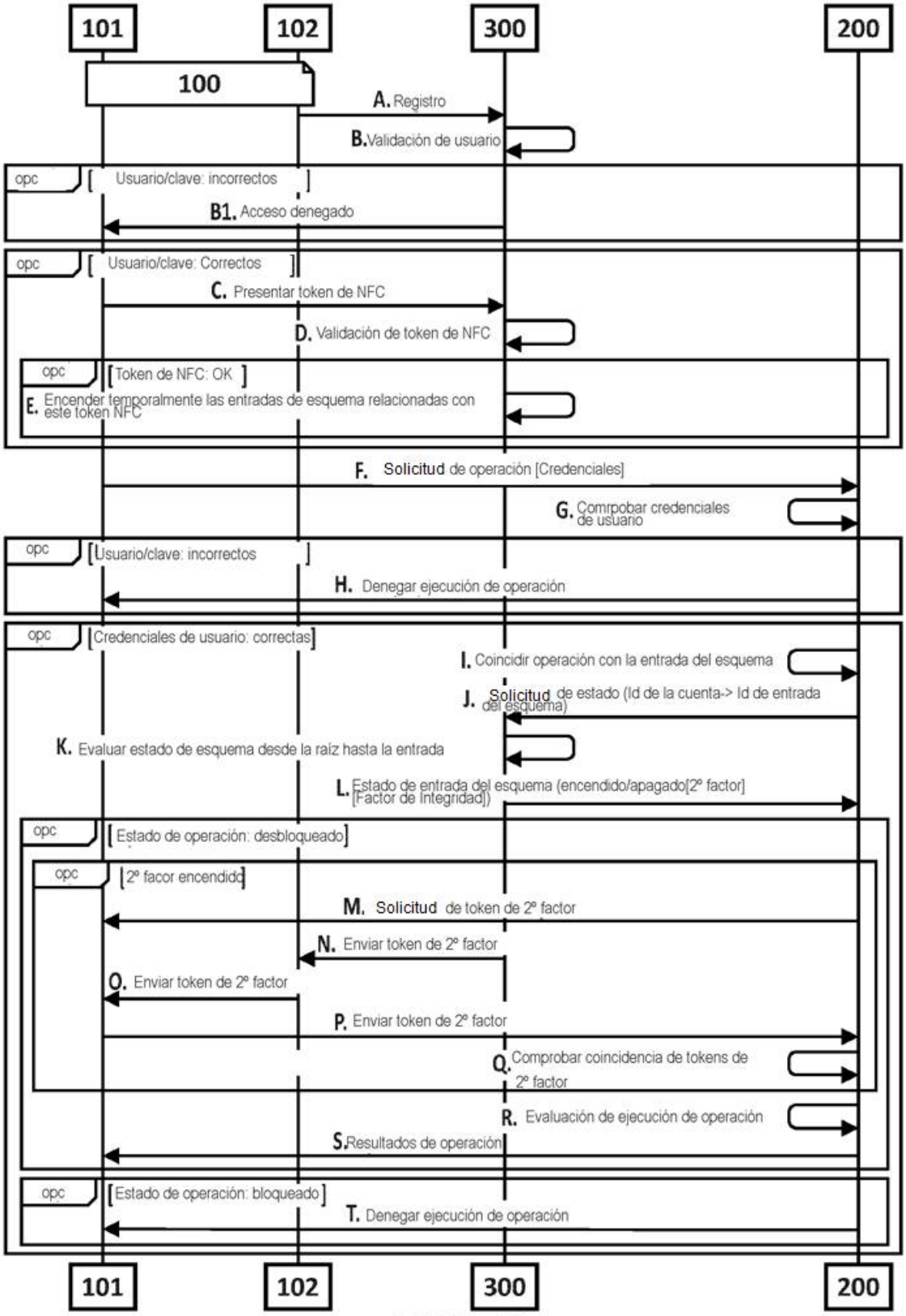
101
102
300
200
100
A. Registro
B. Validación de usuario
opc
Usuario/clave: incorrectos
B1. Acceso denegado
opc
Usuario/clave: Correctos
C. Presentar token de NFC
D. Validación de token de NFC
opc
Token de NFC: OK
E. Encender temporalmente las entradas de esquema relacionadas con este token NFC
F. Solicitud de operación [Credenciales]
G. Comrpobar credenciales de usuario
opc
Usuario/clave: incorrectos
H. Denegar ejecución de operación
opc
Credenciales de usuario: correctas
I. Coincidir operación con la entrada del esquema
J. Solicitud de estado (Id de la cuenta-> Id de entrada del esquema)
K. Evaluar estado de esquema desde la raíz hasta la entrada
L. Estado de entrada del esquema (encendido/apagado[2º factor] [Factor de integridad])
opc
Estado de operación: desbloqueado
opc
2º facor encendido
M. Solicitud de token de 2º factor
N. Enviar token de 2º factor
O. Enviar token de 2º factor
P. Enviar token de 2º factor
Q. Comprobar coincidencia de tokens de 2º factor
R. Evaluación de ejecución de operación
S. Resultados de operación
opc
Estado de operación: bloqueado
T. Denegar ejecución de operación
101
102
300
200

FIG. 6