(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 753 349**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **23.06.2014 PCT/EP2014/063189**

(87) Fecha y número de publicación internacional: **31.12.2014 WO14206946**

(96) Fecha de presentación y número de la solicitud europea: **23.06.2014 E 14732197 (0)**

(97) Fecha y número de publicación de la concesión europea: **07.08.2019 EP 3014836**

(54) Título: **Método, sistema de comunicación y producto de programa informático para autenticación biométrica y autorización**

(30) Prioridad:

24.06.2013 EP 13382237
09.10.2013 EP 13382396
09.10.2013 EP 13382397
09.10.2013 EP 13382398

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.04.2020

(73) Titular/es:

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

(72) Inventor/es:

PALAZÓN ROMERO, JOSÉ MARIA;
GUZMÁN SACRISTÁN, ANTONIO;
BARROSO BERRUETA, DAVID;
ALONSO CEBRIÁN, JOSÉ MARÍA y
KACHAKIL DIB, DANIEL

(74) Agente/Representante:

ARIZTI ACHA, Monica

DESCRIPCIÓN

Método, sistema de comunicación y producto de programa informático para autenticación biométrica y autorización

Campo de la técnica

La presente invención se refiere, en general, a los métodos y sistemas del campo de autenticación biométrica. En particular, la invención se refiere a un método implementado por ordenador, un sistema de comunicaciones y productos de programas informáticos para operaciones de aseguración en sistemas de autenticación y autorización usando información biométrica.

Antecedentes de la invención

En los últimos años, el mercado de la detección de fraude de web ha aumentado considerablemente, por lo que la innovación en procesos de autenticación y autorización se ha vuelto de gran importancia.

La complejidad creciente de las aplicaciones ha conducido a la adopción de muchas técnicas de seguridad cada vez más sofisticadas. Una de las clasificaciones que puede proponerse para el estudio de estas técnicas de seguridad permite distinguir entre soluciones de autenticación y soluciones de autorización. Las técnicas de autenticación se están diseñando para verificar que una persona es la que reivindica que es. Para añadir más fiabilidad al verificar que realmente una persona corresponde a la identidad que se está verificando, pueden tomarse muchos esquemas de autenticación alternativos o puede ampliarse el número de factores para crear esta autenticación.

Hay muchas soluciones diseñadas para fortalecer los procesos de autenticación y, por extensión para fortificar los procesos de autorización. Una vez que los usuarios se han identificado de manera segura, hay esquemas de autorización que permiten flexibilidad y robustez al asignar permisos a usuarios para asegurar acceso seguro a recursos de sistema. Sin embargo, hay amenazas que no pueden frustrarse adoptando cualesquiera de los esquemas existentes para la autenticación/autorización, o esta adopción es demasiado costosa para permitirla. Estas amenazas afectan directamente la manera que se realiza el acceso a recursos específicos. Un método para tratar estas amenazas implica el diseño de mecanismos de seguridad nuevos. Estos mecanismos deben garantizar que una vez que se ha verificado la identidad de un usuario y que se ha comprobado el nivel de autorización a un recurso para este usuario, las acciones tomadas por el usuario de ese recurso no se interceptan ni modifican por ningún atacante.

En cualquier modelo de autorización se incluyen diferentes técnicas que facilitan el acceso a diversos recursos de sistema. La información del papel de usuario, los datos de control de acceso proporcionados cuando se autentica el usuario, son ejemplos de información que puede usarse para determinar quién proporcionó acceso a qué recursos y cómo ha de garantizarse este acceso. Finalmente, determinar qué debería accederse por los usuarios, se especificará para cada aplicación. Por esta razón, en ocasiones será difícil proporcionar un esquema de autorización general. Será necesario definir una lógica específica de aplicación para determinar qué usuarios pueden acceder y cómo realizarían 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 debe garantizarse por la selección correcta del mecanismo de autenticación y una implementación correcta del esquema de autorización seleccionado.

Algunas de las soluciones proporcionan flexibilidad definiendo su propio SDK para fomentar el uso de sus esquemas para autenticación/autorización. Hoy en día, la mayoría de los SDK están basados en conceptos introducidos por OAuth y no suponen un riesgo por sí mismos. Esto se aplica a Microsoft Live Connect, Facebook PHP SDK y Broker de Autenticación de Windows 8 SDK. Si existen, las amenazas provienen de un uso deficiente de estos SDK. De hecho, independientemente de las amenazas derivadas por una implementación pobre del esquema elegido, la mayoría de las amenazas que pueden definirse en un sistema de autorización coinciden con amenazas definidas para sistemas de autenticación. Esta coincidencia tiene que hacerse con el uso incorrecto de las credenciales usadas para gestionar permisos que conceden acceso a recursos [2], [5].

En [2] se definen cuatro niveles diferentes en términos de las consecuencias de autenticación y errores de autorización y uso incorrecto de 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 inicio de sesión repetidos adivinando posibles valores del autenticador de testigo. Un atacante también puede reproducir mensajes previamente capturados (entre un usuario legítimo y un verificador) para autenticarse como ese usuario al verificador. NIST recomienda el uso de una única autenticación o de múltiples factores sin prueba de identidad para proporcionar protección contra estos ataques de adivinación en línea y de reproducción.
- Nivel 2- Un atacante puede escuchar de manera pasiva al protocolo de autenticación para capturar información

que puede usarse en un ataque activo posterior para enmascararse como el usuario. NIST recomienda el uso de autenticación única o de múltiples factores para proporcionar protección contra estos ataques de escucha clandestina y todos los ataques del nivel 1.

- Nivel 3- El atacante se sitúa a sí mismo o a sí misma entre el usuario y el verificador de modo que él o ella puede interceptar y modificar el contenido de los mensajes de protocolo de autenticación. El atacante típicamente suplanta el verificador al usuario y suplanta simultáneamente el usuario al verificador. Realizar un intercambio activo con ambas partes simultáneamente puede permitir que el atacante use mensajes de autenticación enviados por una parte legítima para autenticar satisfactoriamente la otra. NIST recomienda el uso de una autenticación de múltiples factores y el uso amplio de OTP. También sugiere un testigo usado para que se desbloquee la autenticación por el usuario usando una contraseña o biométricas. Adoptar estas soluciones proporciona protección contra ataques de suplantación del verificador, ataques de MitM y los ataques del nivel 2.
- Nivel 4- Un atacante puede insertarse a sí mismo o sí misma entre un usuario y un verificador posterior a un intercambio de autenticación satisfactorio entre las últimas dos partes. El atacante puede plantearse como un usuario al verificador, o viceversa, para controlar el intercambio de datos de sesión. Por otra parte, el atacante puede comprometer o aprovechar de otra manera los testigos de autenticación y puede interceptar todas las comunicaciones de entrada o salida del dispositivo (ataques de hombre en el dispositivo (MitD) o de hombre en el explorador (MitB)). El atacante puede hacer esto infectando el sistema con software maligno. NIST sugiere el uso de autenticación de múltiples factores con hardware resistente a manipulación certificado FIPS-140-2 (testigos de hardware) [4] para obtener protección contra estos ataques de secuestro de sesión y ataques del nivel 3.

Para los primeros tres niveles, los ataques y soluciones existentes ambos están centrados en la manera de verificación de la identidad del usuario. En el nivel 4, NIST propone el uso de soluciones contra secuestro de sesión y otros ataques a través de procesos de autenticación. Este secuestro de sesión implica que un atacante se aproveche del intercambio legítimo de credenciales que un usuario hace cumplir con el proceso de autenticación. Una vez que se consigue esta validación, el atacante a continuación interviene en la comunicación que tiene lugar. Este tipo de ataque puede implementarse de dos maneras: actuar de manera activa, secuestrando la conexión y dejando fuera al usuario legítimo, o, permanecer oculto y modificar el contenido de comunicación de manera transparente al usuario. Sea cual sea la implementación de este ataque, es importante observar que esto es un ataque que tiene como objetivo la ruptura del sistema de autorización, dejando intacto, aunque inútil, el sistema de autenticación. Aunque hay alternativas para proteger de manera proactiva sistemas de esta amenaza, no hay solución adecuada para mitigar los efectos del ataque una vez que se compromete el dispositivo a partir del cual se solicita acceso de recurso.

NIST sugiere emplear hardware resistente a la manipulación certificada FIPS-140-2 (testigos de hardware) [4]. Usar estos dispositivos proporciona a los usuarios la capacidad para generar una contraseña de único uso (contraseña de un solo uso, OTP) para probar su identidad a cada transacción. Además, hay implementaciones de hardware de estos testigos que pueden generar otras OTP codificadas para contener información sobre cómo completar una transacción específica.

Pueden definirse diferentes criterios para establecer la comparación entre esquemas de autenticación/autorización. En [1] los autores sugieren la necesidad de definir tres criterios para realizar una comparación eficaz. Estos aspectos son: seguridad, usabilidad y complejidad de implementación (capacidad de despliegue). Este artículo presenta un estudio intensivo para instrumentar la comparación a través de la definición de métricas. La siguiente tabla resume las métricas definidas para cada criterio.

Usabilidad	Sin esfuerzo de memoria Escalable-para usuarios Nada que llevar Sin esfuerzo físico Fácil de aprender Eficaz de usar Errores infrecuentes Recuperación fácil de pérdida
Capacidad de despliegue	Accesible Coste por usuario insignificante Compatible de servidor Compatible de explorador Maduro No propietario

(continuación)

Seguridad	Resistente a observación física Resistente a suplantación con objetivo Resistente a adivinación acelerada Resistente a adivinación no acelerada Resistente a observación interna Resistente a fugas de otros verificadores Resistente a suplantación de identidad Resistente a robo Sin terceros confiables Consentimiento explícito requerido Poco probable

En el caso de criterio de seguridad, el conjunto de métrica propuesta resume todos los aspectos que se estiman normalmente al definir un modelo de amenaza. En la definición de estos modelos es necesario adoptar un número de decisiones. Y estas decisiones definen el escenario de trabajo. Por ejemplo en el caso de OAuth 2.0 [5] las suposiciones adoptadas son como sigue:

- El atacante tiene acceso completo a la red entre el cliente y servidores de autorización y el cliente y el servidor de recurso, respectivamente. El atacante puede escuchar de manera clandestina cualesquiera comunicaciones entre estas partes. No se supone que él tiene acceso a comunicación entre el servidor de autorización y servidor de recurso.
- Un atacante tiene recursos ilimitados para organizar un ataque.
- Dos de las tres partes implicadas en el protocolo OAuth pueden confabularse para montar un ataque contra la tercera parte. Por ejemplo, el cliente y servidor de autorización pueden estar bajo el control de un atacante y colisionar para engañar a un usuario para conseguir acceso a recursos.

Atendiendo a las métricas anteriormente introducidas, es posible determinar que las soluciones que corresponden al nivel de seguridad superior (nivel 4) tienen rendimiento pobre en capacidad de despliegue y usabilidad. Una vez que la determinación de un sistema permite determinar en qué nivel ha de desplegarse su sistema de autenticación, es necesario evaluar si los usuarios están autenticados de manera segura y correcta. Aunque hay algunas herramientas que ayudan en esta tarea [3], [6], los despliegues en el nivel 4 son difíciles de evaluar de manera correcta. En términos de usabilidad, el uso de testigos de hardware resistentes a manipulación va contra la adopción de estas soluciones por los usuarios, y ha sido probado que esta situación conduce a un uso incorrecto de los sistemas de credenciales. Estos testigos son costosos. Son dispositivos independientes que el usuario tiene que custodiar y que pueden emplearse con un proveedor de servicio únicamente. Si los usuarios tienen que tratar con más de un proveedor de servicio que ha adoptado estos testigos de hardware resistentes a manipulación, tienen que tener en custodia tantos testigos como proveedores de servicio tengan.

Adicionalmente, en términos de autorización, en [7] los autores explican que, aparte de algunos problemas de seguridad de cada SDK, los desarrolladores que eligen integrar con uno de ellos hacen suposiciones que conducen a problemas de seguridad. Esto es debido a que los SDK a menudo no están bien documentados y las vulnerabilidades de seguridad casi siempre provienen de atacantes que hallan maneras para violar estas suposiciones en las que se basan los implementadores de sistemas.

Junto con estas dificultades, deben considerarse otros problemas para entender el aumento constante en fraude que surge del robo de identidades digitales. Por ejemplo, no es posible medir un nivel de seguridad homogénea en todas las cuentas digitales de los usuarios. Es necesaria una solución que puede igualar el nivel de seguridad de todas las cuentas digitales que posee un usuario. Esta solución debería extender esta seguridad no únicamente a los procesos de autenticación sino también a los procesos de autorización de recursos y todos los procedimientos relacionados con tales cuentas.

Además, están en uso numerosas técnicas de identificación y autenticación biométrica hoy en día para asegurar y acceder a aplicaciones de control. Estas técnicas biométricas incluyen identificación de huella digital, reconocimiento facial, exploración retinal, exploración de iris, reconocimiento de mano y análisis de voz o de firma. Sin embargo, aunque hay muchas ventajas de autenticación biométrica, varios factores han limitado su propagación debido a algunos de los procesos pueden ser muy intrusivos, incómodos y/o costosos.

El documento US 2009/183247 A1 desvela sistemas y métodos de acceso de aseguración a una red. El acceso a la red se asegura usando autenticación de múltiples factores, biométricas, encriptación intensa y una diversidad de normas de interconexión en red inalámbrica. Las biométricas incluyen huellas digitales, reconocimiento facial, exploración retinal, reconocimiento de voz y biométricas que pueden usarse en combinación con otros factores de autenticación para crear un esquema de autenticación de múltiples factores para acceso de red altamente seguro. Las solicitudes que requieren acceso a recursos de red asegurados pueden interceptarse y una página de portal

cautiva devolverse a un desafío de un usuario. La información biométrica devuelta en respuesta a la página de portal se usa para autenticar el usuario y determinar derechos de acceso a la red.

El documento WO 02/095554 A2 se refiere a autenticación usando biométricas. Un alias para un individuo está asociado con un conjunto de datos biométricos de referencia del individuo y, en una localización separada del conjunto de referencia de datos biométricos, se almacena información que asocia al individuo con el alias. La invención puede operar en una solicitud de autenticación que solicita autenticación de un usuario identificado por el alias, junto con un conjunto candidato de datos biométricos del usuario y que confirma autenticación del usuario como el individuo registrado; la autenticación se concede si el conjunto candidato de datos biométricos coincide de manera suficiente con el conjunto de referencia de datos biométricos.

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. Online Resource: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[5] McGloin M. y Hunt P. (enero de 2013) OAuth 2.0 Threat Model and Security Considerations. ISSN: 2070-1721. Online resource: http://tools.ietf.org/pdf/rfc6819.pdf.

[6] Sun, F., Xu, L., y SU,Z. (agosto de 2011) 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.

[8] DAILEY, Matthew D. Authentication Schemes based on Physically Unclonable Functions. 2009. Tesis Doctoral. WORCESTER POLYTECHNIC INSTITUTE.

[9] DODIS, Yevgeniy; REYZIN, Leonid; SMITH, Adam. Fuzzy extractors: How to generate strong keys from biometrics y other noisy data. En Advances in cryptology-Eurocrypt 2004. Springer Berlin Heidelberg, 2004. págs. 523-540.

Sumario de la invención

La presente invención proporciona un método para asegurar operaciones en sistemas de autenticación y autorización usando información biométrica, como se define en la reivindicación independiente 1. Las reivindicaciones independientes 10 y 11 definen un sistema correspondiente y producto de programa informático, respectivamente. Se definen realizaciones particulares en las reivindicaciones dependientes.

El método implementado por ordenador proporcionado se caracteriza por el uso de un segundo servidor, en conexión con el dispositivo informático de usuario que tiene instalado en el mismo un programa especializado o aplicación móvil, para recibir, del primer servidor, una primera solicitud acerca de un estado asociado a dicho usuario para ayudar al primer servidor a autorizar o rechazar el registro del servicio solicitado. En caso de que esté autorizado al servicio solicitado, y se haga otra solicitud por el usuario para realizar una operación en el primer servidor, el segundo servidor también: recibe una segunda solicitud del primer servidor acerca de un estado que ha establecido el usuario para dicha operación; evalúa el estado de operación para comprobar si el primer servidor está permitido a acceder a la configuración de usuario para dicha operación y envía el resultado del estado de operación al primer servidor.

A continuación, si dicho resultado se establece como válido, se usa un mecanismo de factor de autenticación adicional que incluye una verificación de identidad biométrica de información biométrica del usuario, de modo que se permite que el segundo servidor confirme la autenticación del usuario, y que el segundo servidor incluya una contraseña de un solo uso en el envío del resultado de estado de operación al primer servidor.

La información biométrica puede incluir una huella digital, una exploración de voz, una exploración facial, una exploración de iris, una exploración de la palma entre otras.

De acuerdo con la invención, la primera solicitud realizada por el primer servidor comprende: un intercambio de credencial entre el primer servidor y el segundo servidor para proporcionar autenticación mutua; la verificación, por el

segundo servidor, de dicho estado asociado del usuario, dicho estado asociado se ha establecido previamente como válido o como inválido por dicho usuario y se ha almacenado en una memoria del segundo servidor; y el envío, por el segundo servidor, del estado asociado del usuario al primer servidor.

Se realiza el intercambio de credenciales para autenticación mutua segura entre el primer servidor y el segundo servidor, preferentemente, mediante un procedimiento de autenticación convencional basado en intercambio de certificados que define, como resultado, un canal asegurado. El intercambio se realiza para verificar que tanto el primer servidor como el segundo servidor son quien reivindican que son.

El segundo servidor puede notificar al usuario en caso de que se rechace dicha solicitud para iniciar sesión en un servicio del primer servidor. Por ejemplo, mediante el envío de un Servicio de Mensajes Cortos (SMS), de un correo electrónico, de o un mensaje por una aplicación de mensajería de teléfono inteligente, o solo resaltando o insistiendo en dicho programa especializado de dicho dispositivo informático de usuario.

El estado asociado se establece como válido (desbloqueado) o como inválido (bloqueado) un cierto periodo de tiempo y puede modificarse por el usuario cada vez que lo desee el último. Por ejemplo, el usuario puede planear 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 modificar dicho estado asociado puede ser delegando el control que dicho usuario tiene de sus cuentas a otros usuarios. Esto puede hacerse considerando dos opciones diferentes. En la primera, se usa un mecanismo de control parental para que el control de acceso de las cuentas de los niños (originales) se delegue al mecanismo de control parental. En la segunda, una única cuenta permite múltiples bloqueos. En este último caso, la acción de desbloqueo requerirá que múltiples usuarios desbloqueen sus bloqueos de manera concurrente. En ambos casos, la delegación se realiza manteniendo de manera segura la privacidad de cada usuario sin variar.

Además, la solicitud para iniciar sesión en un servicio y/o la solicitud para realizar una operación pueden registrarse para proporcionar estadísticas. De esta manera, el usuario puede obtener estadísticas de uso de sistema que reflejan la actividad del sistema y rastrean los intentos de suplantación. Estas estadísticas informan acerca de lo que alguien ha intentado acceder a un servicio con nombre de usuario del usuario.

De acuerdo con una realización, el mecanismo de factor de autenticación adicional que incluye la verificación de identidad biométrica de información biométrica del usuario y la generación de testigos que pueden usarse como contraseñas de un solo uso (OTP) se realiza por el segundo servidor:

recuperando una firma biométrica previamente almacenada del usuario y un vector de pesos de la misma;
seleccionando un conjunto de coeficientes de dicha firma biométrica almacenada para usarse como clave criptográfica, realizando la función de troceo del conjunto seleccionado de coeficientes para producir una clave válida, y generar una cadena auxiliar; y
cifrando la OTP con la clave válida producida y enviando la OTP cifrada junto con al menos la clave auxiliar generada al programa especializado.

Después de eso, el programa especializado captura una firma biométrica del usuario, capturándose dicha firma biométrica capturada empleando la misma técnica biométrica que dicha firma biométrica almacenada; y usa la cadena auxiliar recibida para determinar el conjunto de coeficientes a usarse al menos para dicha firma biométrica capturada del usuario y realiza la función de troceo del conjunto de coeficientes para producir la clave válida para descifrar la OTP recibida.

Preferentemente, la firma biométrica del usuario y el vector de pesos se almacenan en el segundo servidor después de tener que ejecutar el programa especializado un procedimiento de entrenamiento. El procedimiento de entrenamiento incluye la captura de diferentes medidas biométricas del usuario de acuerdo con patrones predefinidos generados por el segundo servidor y el procesamiento de las medidas biométricas para realizar el cálculo de la firma biométrica y del vector de pesos.

Como una mejora de la invención, puede emplearse también un número aleatorio, como una sal criptográfica, para aumentar la entropía de la clave criptográfica y para evitar ataques de reproducción en la generación de la cadena auxiliar.

En un segundo aspecto la invención propone un sistema de comunicaciones para asegurar operaciones en sistemas de autenticación y autorización usando información biométrica, en el que un primer servidor está configurado para recibir de un usuario que tiene un dispositivo informático, una solicitud para registrarse en un servicio en la misma y para autenticar información de credenciales de dicho usuario para autorizar dicha solicitud de servicio.

El sistema de comunicaciones está caracterizado por incluir un segundo servidor, en conexión con dicho dispositivo informático de usuario que tiene instalado en el mismo un programa especializado, que está configurado para:

- recibir, del primer servidor, una primera solicitud acerca de un estado asociado a dicho usuario para ayudar al primer servidor a autorizar o rechazar el registro de servicio solicitado;
- recibir, del primer servidor, y en caso de que se autorice dicho registro de servicio solicitado y se haga una solicitud por el usuario para realizar una operación en el primer servidor, una segunda solicitud acerca de un estado que el usuario ha establecido para dicha operación;
- evaluar el estado de operación para comprobar si el primer servidor está permitido a acceder a la configuración de usuario para dicha operación; y
- enviar el resultado del estado de operación al primer servidor que incluye una contraseña de un solo uso (OTP), en caso de que el resultado se haya establecido como válido y se usa un mecanismo de factor de autenticación adicional que incluye una verificación de identidad biométrica de información biométrica del usuario.

En el sistema de comunicación para realizar el mecanismo de factor de autenticación adicional que incluye la verificación de identidad biométrica de información biométrica del usuario, el segundo servidor incluye preferentemente una pluralidad de módulos que están configurados adicionalmente para:

- recuperar, por un módulo biométrico de servidor, una firma biométrica previamente almacenada del usuario y un vector de pesos de la misma;
- seleccionar, por un módulo de generación, un conjunto de coeficientes de dicha firma biométrica almacenada para usarse como clave criptográfica, realizar la función de troceo del conjunto seleccionado de coeficientes para producir una clave válida, y generar una cadena auxiliar; y
- cifrar, por un módulo de cifrado, la OTP generada con la clave válida producida y enviar, por un módulo emisor, la OTP cifrada junto con al menos la clave auxiliar generada al programa especializado.

Además, el programa especializado preferentemente también incluye una pluralidad de módulos que están configurados para:

- capturar, por un módulo biométrico, una firma biométrica del usuario;
- recibir, por un módulo receptor, la OTP cifrada enviada junto con la cadena auxiliar generada y la firma biométrica capturada del usuario;
- determinar, por un módulo de reproducción usando al menos la clave auxiliar generada, el conjunto de coeficientes a usarse para dicha firma biométrica capturada del usuario y para realizar la función de troceo del conjunto de coeficientes para producir la clave válida; y
- descifrar, por un módulo de descifrado, la OTP recibida usando la clave válida producida.

La materia objeto descrita en el presente documento puede implementarse 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 puede implementarse en software ejecutado por un procesador.

De acuerdo con un tercer aspecto la invención proporciona un programa informático que comprende medios de código de programa informático adaptados para realizar las etapas de acuerdo con el método implementado por ordenador del primer aspecto de la invención cuando dicho programa se ejecuta en un ordenador, un procesador de señales digitales, un campo de matriz de puertas programables, un circuito integrado específico de la aplicación, un micro-procesador, un micro-controlador, o cualquier otra forma de hardware programable.

Las realizaciones de la invención también comprenden un producto de programa informático que incluye medios de código de programa adaptados para realizar otras realizaciones de la invención de acuerdo con los métodos de las reivindicaciones 3 o 5.

Breve descripción de los dibujos

Las anteriores y otras ventajas y características se entenderán más en profundidad a partir de la siguiente descripción detallada de las realizaciones, con referencia a lo adjunto, que deben considerarse de una manera ilustrativa y no limitante, en las 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 emparejamiento de cuenta con autorización.
La Figura 3 es un diagrama de flujo que ilustra cómo un estado de una cuenta de usuario puede comprobarse para autenticación.
La Figura 4 ilustra la estructura general del mecanismo propuesto para reforzar el mecanismo de factor de autenticación adicional incluyendo una verificación de identidad biométrica de información biométrica del usuario.
La Figura 5 ilustra la estructura propuesta para el procedimiento de generación (Gen) propuesto.
La Figura 6 ilustra la estructura propuesta para el procedimiento de reproducción *(Rep)* propuesto.
La Figura 7 es el diagrama de flujo que ilustra la realización en la que el factor de autenticación adicional

propuesto se refuerza con información biométrica del usuario.
La Figura 8 es el diagrama de flujo que ilustra el proceso de entrenamiento propuesto por la invención.

Descripción detallada de la invención y de varias realizaciones

En referencia a la Figura 1 se muestra la arquitectura general de la presente invención. Con respecto a la Figura 1, un dispositivo informático de usuario 100 tal como un teléfono móvil, un teléfono inteligente, un PC de tableta o un PDA entre otros, se usa por dicho usuario para iniciar sesión en un programa especializado 102 en comunicación con un segundo servidor 200 y para gestionar el estado para 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. 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 del bloqueo/desbloqueo de la opción por defecto o el segundo factor de autenticación. Este control de seguridad consiste en proporcionar un canal de comunicación del usuario 100 al primer servidor 300, a través del segundo servidor 200. El primer servidor 300 puede configurar el sistema para solicitar al usuario 100 una información particular relacionada con dicha operación a realizarse. Esta información puede usarse por el segundo servidor 200 para verificar si el usuario 100 es quien realmente está demandando dicha operación y para confirmar si la operación que ha llegado al primer servidor 300 es exactamente como la que ha ordenado el usuario 100.

Suponiendo que el primer servidor 300 podría desear verificar la integridad de la operación, puede seleccionarse qué parámetros son críticos para asegurar la integridad de operación. En este caso, es importante que la información solicitada corresponda de manera unívoca con el parámetro crítico de operación para identificarlo correctamente.

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

Cuando un primer servidor 300 decide integrar sus servicios, proporcionará la capacidad para vincular sus cuentas con las cuentas que tiene el usuario 100 en el segundo servidor 200. Cuando dicho usuario 100 decide establecer este enlace, él o ella inicia un proceso de emparejamiento que asegura privacidad completa al usuario 100. Una vez que se completa el proceso de emparejamiento, el usuario 100 puede acceder a la configuración del control de la cuenta con el primer servidor 300 de un programa especializado 102 (es decir una aplicación móvil).

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

El segundo núcleo de 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 eso, el segundo servidor 200 acepta y procesa las solicitudes de comprobación-estado enviadas del 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 el emparejamiento de nuevos bloqueos. La clave es que nunca se solicita al usuario 100 por información privada alguna. Una vez que el usuario 100 crea su cuenta con el segundo servidor 200, él puede establecer bloqueos con diferentes proveedores de servicio, como dicho primer servidor 300. Para activar estos bloqueos el segundo servidor 200, de acuerdo con una realización, genera un testigo. Son necesarios un testigo único y la definición de canales asegurados para completar el proceso de emparejamiento entre el usuario 100 y el primer servidor 300. Como resultado de este proceso de emparejamiento, el testigo criptográfico se envía del segundo servidor 200 al primer servidor 300 que tiene que almacenar esta información con sus datos personales del usuario. Más tarde, este testigo criptográfico se usará para solicitar el correspondiente estado de bloqueo. El usuario 100 puede modificar el estado de sus bloqueos, por la activación o configuración de las diferentes opciones que proporciona el segundo servidor 200.

En caso de que el usuario 100 haya establecido un bloqueo con un segundo factor para autenticación a través de 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 del primer servidor 300 que solicita el estado de la cuenta de usuario, se activa un segundo factor de autenticación. Se genera una OTP y se envía al usuario 100. La misma OTP se envía al primer servidor 300 junto con el estado de la cuenta. Si el estado está ACTIVADO y el usuario 100 ha activado el segundo factor, el primer servidor 300 debería solicitar que el usuario introduzca la OTP para continuar con la operación.

Ahora, si el usuario 100 ha de establecer un bloqueo a través de dicha operación con un factor de integridad para verificar que los parámetros de operación no se hayan modificado, dicho segundo servidor 200 incorpora la lógica necesaria para obtener la información crítica del usuario 100 y del primer servidor 300 y para comprobar si ambos 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 desajuste, el primer servidor 300 puede concluir que un intruso puede estar interceptando la información del usuario 100. El primer servidor 300 puede a continuación crear mecanismos para eludir el fraude y para generar alertas de seguridad.

En referencia a la Figura 2 se ilustra un proceso de emparejamiento 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 especializado 101 tal como un explorador, ha completado el proceso de inicio de sesión (A-B) con un primer servidor 300 (en este caso particular un banco en línea, una red social, unos proveedores de tarjeta de crédito, etc.), el usuario 100 decide realizar dicho proceso de emparejamiento de las cuentas. El usuario 100 solicita el emparejamiento al primer servidor 300 (C) usando el explorador 101. Como respuesta, el primer servidor 300 solicita un testigo de emparejamiento (D). El usuario 100 a continuación usa el programa especializado 102 (D') para obtener este testigo de emparejamiento del segundo servidor 200, después de un proceso de inicio de sesión anterior. El segundo servidor 200 genera un testigo (por ejemplo como una OTP) (E) y lo envía al programa especializado del usuario 102 (F). Este testigo puede usarse para varios procesos de emparejamiento mientras que sea válido. El usuario obtiene el testigo (OTP) del programa especializado 102 y lo introduce en la página web visualizada en el explorador 101 por el primer servidor 300 (G-G'). El primer servidor 300 a continuación envía el testigo recibido al segundo servidor 200, después de un intercambio de credenciales previo (H). Si se valida la identidad del primer servidor 300, el segundo servidor 200 almacena el enlace entre el usuario 100 y el primer servidor 300 y genera un nuevo testigo que identifica este enlace. Este testigo (accountID) se envía al primer servidor 300 (I) y queda almacenado para comunicaciones futuras (J). Al final, se envía unos acuses de recibo de emparejamiento al explorador del usuario 101 (K).

En referencia ahora a la Figura 3, se ilustra cómo un estado de una cuenta de usuario puede comprobarse para autenticación. En la Figura 3, un usuario 100, usando, por ejemplo, un explorador 101, solicita iniciar sesión en un servicio (A) de un primer servidor 300 por lo que una vez que se ha validado la existencia del usuario (B) por dicho primer servidor 300, el último demanda al segundo servidor 200 el estado de la cuenta de usuario (C). A continuación el segundo servidor 200 inicializa el intercambio de credenciales antes de que se envíe el resultado de la información de estado de cuenta (D). Con el estado de resultado, el primer servidor 300 hace la decisión de permitir o bloquear el acceso de usuario (E).

En una realización, si el estado de la cuenta está bloqueado o es válido pero el segundo factor de autenticación está activado, en la respuesta de la solicitud de estado, el segundo servidor 200 envía una OTP al primer servidor 300 que tiene que emplear para completar la autenticación. El primer servidor 300 a continuación solicita al usuario 100 la OTP que va a ser un segundo factor temporal (F). A continuación el segundo servidor 200 envía la misma OTP al programa especializado del usuario 102 (G). El usuario 100 recupera la OTP del programa especializado 102 y la introduce en el explorador 101 (H) y la envía al primer servidor 300 (I). El primer servidor 300 puede comprobar si la OTP enviada a través del explorador 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 mediante 101.

Cuando un primer servidor 300 envía una Solicitud_estado, el segundo servidor 200 entiende que alguien, con la información de identificación de servicio apropiada (es decir ID y contraseña), está intentando acceder al servicio. Si el estado de la cuenta se establece como bloqueado, o si esta solicitud ha provenido 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 la ha configurado así (por ejemplo enviando un Servicio de Mensajes Cortos (SMS), un correo electrónico, un mensaje por una aplicación de mensajería de teléfono inteligente, resaltando o insistiendo en dicho programa especializado 102 de dicho dispositivo informático de usuario 100, etc.) o solamente actualizar las estadísticas para una revisión posterior. A continuación el segundo servidor 200 devuelve el estado asociado con la cuenta como bloqueada.

Con el objetivo de mejorar la seguridad de cualquier sistema de autorización, el uso de dicho segundo servidor 200 se propone como una nueva capa que proporciona a los usuarios la posibilidad de controlar el acceso a los recursos y procedimientos asociados con sus cuentas definidas con cualesquiera primeros servidores. Estos recursos y procedimientos se observan como operaciones que dependen de las acciones principales definidas para una cuenta (es decir proceso de inicio de sesión). Esta dependencia se establece como una jerarquía donde los cambios en las entradas de raíz se propagan a sus hijos.

Además de eso, el uso de canales "fuera de banda" permite proporcionar una solución segura para comunicar los

usuarios y los proveedores de servicio. Hasta ahora, la invención ha creado un intercambio de OTP usando este canal seguro para aumentar el nivel de autenticación. Ahora, el primer servidor puede determinar si el usuario 100 desea que una operación tenga un estado particular (bloqueado o desbloqueado) y puede comprobar si este usuario 100 está en posesión de las credenciales de su cuenta con el segundo servidor 200 para recibir el testigo usado como segundo factor de autenticación. Esto es únicamente un uso particular que puede desplegarse usando este canal seguro adicional tal como está también, por ejemplo, el uso de este canal por los proveedores de servicio para alertar a los usuarios acerca de información de su interés particular (por ejemplo anomalías detectadas con sus credenciales). En este punto, la invención también aumenta el nivel de autenticación de la solución que refuerza el segundo factor previamente descrito. Este refuerzo se basa en información de biometría para permitir que el segundo servidor 200 compruebe si el que está en posesión de las credenciales necesarias para interactuar con el sistema es, de hecho, el mismo/a usuario/a. El objetivo final es proteger el sistema contra el robo de las credenciales del usuario. Es importante señalar que esta solución no significa protección alguna si el dispositivo donde los usuarios introducen sus credenciales está comprometido (hombre en el dispositivo).

La invención considera que el programa especializado 102 puede capturar y procesar los datos biométricos del usuario 100 para producir una clave que puede usarse para cifrar y descifrar la información enviada del segundo servidor 200 o por el primer servidor 300 a través del segundo servidor 200. La fuente de la información no afecta el mismo procedimiento. El hecho es que el primer servidor 300 puede basarse en que la persona que recibe esta información es quien se espera que sea, puesto que el segundo servidor 200 realiza una verificación biométrica. En consecuencia, se requiere el mismo proceso para el segundo servidor 200 pero el primer servidor 300 no necesita integrar estos procedimientos. Los esfuerzos realizados por el primer servidor 300 únicamente están relacionados con el proceso de la información (por ejemplo procesar la OTP recibida).

Adicionalmente, en la invención, para gestionar el segundo factor de autenticación, el testigo que va a usarse como OTP no prueba únicamente que el usuario 100 que está solicitando una operación tiene las credenciales del usuario legítimo del segundo servidor 200 sino que también demuestra que este usuario 100 es quien reivindica ser. Por lo tanto se aumenta la protección para hacer frente al robo de las credenciales del dispositivo o del segundo servidor del usuario teniendo en cuenta estos datos biométricos.

La idea principal es poder generar una clave criptográfica a partir de las características biométricas previamente registradas para un usuario particular por el segundo servidor 200 durante una fase de entrenamiento. Esta fase de entrenamiento supone que cuando el usuario 100 decide operar con un mecanismo de factor de autenticación adicional reforzado, o es el proveedor de servicio (primer servidor 300) que configura sus operaciones de esta manera, el programa especializado 102 instalado en el dispositivo del usuario ejecuta un procedimiento de entrenamiento. Este procedimiento requiere que el usuario 100 facilite diferentes medidas biométricas de acuerdo con plantillas prefijadas. Esto se hace varias veces con cambios menores en los patrones posteriores. Cada vez que el usuario 100 completa una medición, el programa especializado 102 procesa los datos biométricos obtenidos y calcula la firma biométrica que identifica al usuario 100. Típicamente, esta firma puede observarse como una secuencia de coeficientes: $C = (C_0, C_1, C_{2,\ldots,} C_N)$, donde N es el número máximo de coeficientes que depende de la técnica biométrica empleada.

Uno de los asuntos que no puede evitarse cuando se emplea cualquier técnica biométrica es la necesidad de hacer frente a cierto nivel de incertidumbre en este cálculo de coeficientes de firma biométrica. Es decir, puesto que la fuente de información a procesarse es una característica humana que debe medirse, la naturaleza variable intrínseca de estas características o los problemas relacionados con el proceso de medición, normalmente hacen menos probable obtener exactamente los mismos coeficientes para la misma persona para cada proceso de medición. Por esa razón, en la invención el objetivo final de esta fase es perfilar cada usuario 100 con dos vectores usando una colección prefijada de patrones: un vector cuyos coeficientes son el coeficiente biométrico devuelto por la técnica biométrica (C), y otro vector con la incertidumbre asociada con cada uno de estos coeficientes (σ).

Basándose en la información dada por el vector σ es posible determinar qué coeficientes biométricos definen al correspondiente usuario con menos incertidumbre. Sin embargo, esto es agnóstico del significado de los coeficientes. Dependiendo de la técnica biométrica aplicada, el significado en términos de potencia discriminatoria de los coeficientes no necesita que sea homogéneo. Algunos de estos coeficientes pueden ser más valiosos que otros en la verificación de identidad de un interlocutor dado (usuario), de modo que puede definirse un vector de pesos W: $W=\left(\frac{\tau_0}{\sigma_0}, \frac{\tau_1}{\sigma_1}, \frac{\tau_2}{\sigma_2}, \ldots, \frac{\tau_N}{\sigma_N}\right)$, donde τ_i y σ_i representan el significado del coeficiente i en una verificación de interlocutor particular y la incertidumbre de este coeficiente medido durante la fase de entrenamiento respectivamente. Cada componente $W_i = \frac{\tau_i}{\sigma_i}$ del vector W determinaría la efectividad de la contribución del coeficiente i en el proceso de reconocimiento de usuario global.

Para la fase de entrenamiento, se han diseñado dos modos de operación para ganar en flexibilidad: el primer modo implica enviar todos los datos asociados con el proceso realizado en cada palabra al segundo servidor 200 una vez que se han completado todas las repeticiones. Más tarde, en el segundo servidor 200, una vez que se han recibido

todas las repeticiones, es posible seleccionar qué método aplicar para determinar el nivel de incertidumbre asociada con un interlocutor particular y obtener el nivel de incertidumbre relacionada con cada coeficiente de su firma biométrica. El segundo modo se aprovecha de aquellos dispositivos móviles de alta capacidad de cálculo que pueden asumir el coste de rendimiento de ejecución de todos los procedimientos expuestos antes. Por lo tanto, este modo consigue una transmisión que contiene los coeficientes promedio y el vector de tolerancia calculado relacionado con un usuario particular y su nivel asociado de incertidumbre.

Con referencia a la Figura 4, esta figura ilustra la arquitectura global para reforzar el mecanismo de factor de autenticación adicional con una verificación de identidad biométrica del usuario 100. El procedimiento ejecutado para obtener una clave criptográfica de la biométrica propuesta está basado en el uso de un extractor difuso creado a partir de bocetos seguros [8] [9]. Por definición, un extractor difuso es un par de procedimientos aleatorizados: generación *(Gen)* 202 y reproducción *(Rep)* 105. Dados los coeficientes derivados de la técnica biométrica empleada (*C*), el procedimiento Gen produce una cadena *K* y una cadena auxiliar *P* como salida. Ambas dependen de las técnicas incluidas en la definición de extractor difuso. En la invención, una vez que se han producido, la cadena K es la clave criptográfica que puede usare para cifrar el mensaje en un módulo de cifrado 204 (es decir el testigo usado como OTP) y la cadena P puede usarse para hacer frente a la variabilidad relacionada con el uso de técnicas biométricas. El procedimiento *Rep* toma como entradas los coeficientes biométricos calculados por un módulo biométrico 103 del programa especializado 102 a partir de una señal de audio (*C'*) y la cadena auxiliar *P* y, si *C'* está lo suficientemente cerca de *C*, emite la cadena *K* que puede usarse para descifrar 106 el mensaje. Por lo que, desde un punto de vista general, para hacer frente a la incertidumbre relacionada con las técnicas biométricas es necesario agrupar el mensaje cifrado (por ejemplo $E_K[OTP]$) con la cadena auxiliar P.

El proceso comienza cuando se selecciona un patrón particular para un usuario específico (UserID). Este patrón depende de la técnica biométrica empleada y se propone ampliar el espacio definido por las características que esta técnica puede extraer de un usuario. Por ejemplo, si la técnica biométrica usada está basada en la voz del usuario este patrón puede ser un subconjunto de las palabras usadas durante el entrenamiento del sistema (por ejemplo en el caso de técnicas basadas en texto prefijado) o un filtro sintético usado en el caso de técnicas en un texto prefijado. En esta figura aparecen dos módulos - módulo emisor 205 y módulo receptor 104 - que modelan cualquier esquema de comunicación seguro basándose en criptografía de clave pública (K_P)/privada(K_{PR}) (por ejemplo SSL).

Como se ha indicado antes, la invención ofrece protección contra fuga de credenciales o robo de dispositivo. Por lo tanto, la invención está diseñada para ser resistente frente a ataques de reproducción o ataques de fuerza bruta desplegados una vez que las credenciales están comprometidas. Adicionalmente, el diseño propuesto tiene en cuenta que parte de la solución se ejecutará en un dispositivo informático de bajo rendimiento tal como un teléfono inteligente, etc. Para hacer frente a estos asuntos, la alternativa empleada en esta invención significa proponer un diseño particular de estos procedimientos Gen y *Rep*. Algo de la modificación puede observarse en la Figura 4 donde el módulo de generación 202 no recibe únicamente el vector de coeficiente biométrico sino también recibe información relacionada con la precisión de cualquiera de estos coeficientes (*W*).

La Figura 5 ilustra el procedimiento Gen propuesto 202 reforzado con el uso de funciones de troceo y valores aleatorios, y la Figura 6 ilustra el correspondiente procedimiento *Rep* 105. Una vez que el procedimiento Gen recibe el vector (*W*) cuyos coeficientes proporcionan información acerca de la incertidumbre de cualesquiera estimadores biométricos, se define un subconjunto (ω) de estos estimadores. La selección de estimadores de este subconjunto depende de dos aspectos: rendimiento y seguridad. El número de elementos contenido en ω impacta en el rendimiento del procedimiento *Rep*. Debido a que *Rep* debe ejecutarse por el programa especializado 102 en un dispositivo informático de bajo rendimiento el número de elementos en ω puede parametrizarse y ajustarse más tarde de acuerdo con la potencia de cálculo estimada para cada usuario.

Existe, sin embargo, un límite bajo en el número de elementos. El número de elementos en ω determina cuántos coeficientes biométricos se usan para producir una clave criptográfica. Dejando aparte que la complejidad de la clave se aumenta por el uso de una función de troceo, la información única relacionada con el usuario 100 se expresa en términos de estos coeficientes, por lo que es necesario un número mínimo de ellos. De hecho, para aumentar la entropía de esta clave criptográfica, se añade un número aleatorio (*x*) en el cálculo de la clave como una sal criptográfica. A continuación, el subconjunto ω se emplea entonces para determinar qué coeficientes biométricos usar para generar una clave criptográfica y se añade un número aleatorio *x* para evitar que el mismo subconjunto de coeficientes biométricos (*c*) produzca la misma clave en cualquier momento que se seleccione. Esta *x* evita que los atacantes creen fácilmente una lista de valores de troceo para claves comunes y evita que los esfuerzos de rotura de claves escalen a través de muchas comunicaciones.

Con los vectores ω y *C* es posible determinar el subconjunto (*c*) de coeficientes empleados para generar una clave criptográfica. Para poder hacer frente a la variabilidad de técnicas biométricas, se propone un boceto seguro (SS) para producir la información (*s*) que garantiza la recuperación de datos biométricos de una C' lo suficiente similar a *C.* Estos bocetos seguros permiten una construcción fácil del extractor difuso con la flexibilidad en términos de la capacidad de corrección de error. Para evitar cualquier fuga de información se emplea de nuevo un número aleatorio

(x) para evitar la adivinación de esta s y producir la cadena auxiliar *P* que se enviará al programa especializado 102.

Una vez que el programa especializado 102 recibe el patrón puede medir a continuación datos biométricos del usuario 100 y obtener una *C*'. Al mismo tiempo, el programa 102 recupera la cadena *P* donde puede hallar la información s para asegurar que *C* puede determinarse a partir de *C'*. Los datos contenidos en la cadena *P* también facilitan el cálculo de la clave criptográfica *K,* una vez que se recupera *C*.

En referencia a la Figura 7 se muestra el estado del proceso de verificación de operación que incluye el mecanismo de factor de autenticación adicional propuesto reforzado con información biométrica del usuario 100. Esta operación se propone por el primer servidor 300 fijado a la gestión de cuenta. El usuario 100, una vez que se ha registrado correctamente en el primer servidor 300 como se ha explicado anteriormente, solicita ejecutar usando, por ejemplo, un explorador 101 una operación relacionada con una cuenta (A) del primer servidor 300. Esta operación puede ser, por ejemplo, ejecutar alguna acción relacionada con los servicios proporcionados por el primer servidor 300 (por ejemplo pago de Internet con una tarjeta de crédito). Por lo que una vez que se ha validado (B) la existencia de usuario por dicho primer servidor 300, lo último hace la correspondencia de la operación solicitada con la entrada en la jerarquía definida por esta cuenta del usuario (D) y demanda al segundo servidor 200 este estado de entrada (E).

A continuación el segundo servidor 200 inicializa el intercambio de credenciales antes de evaluar el estado de entrada de esquema de la raíz a la entrada (F). Se recupera el estado de la cuenta de usuario y si está desbloqueado se realiza la misma evaluación con cada etapa fundada hasta que alcance la entrada de esquema. La información de estado de entrada de esquema se envía (G) y, con esta información, el primer servidor 300 hace la decisión de permitir o bloquear el acceso de usuario a la operación. Si el estado de la entrada de esquema está desbloqueado y se activa el segundo factor de autenticación, el segundo servidor 200 envía una OTP al primer servidor 300 dentro de la respuesta de la solicitud de estado de operación. Este primer servidor 300 tiene que emplearla para completar la autenticación. El primer servidor 300 solicita al usuario 100 la OTP que va a ser un segundo factor temporal (S)

Si el estado de la entrada de esquema está desbloqueado y el segundo factor de autenticación se refuerza con la verificación de identidad biométrica a continuación el segundo servidor 200 tiene que recuperar la firma biométrica y el vector de pesos del almacenamiento para el usuario 100 en particular (H). Usando estos vectores, tiene que seleccionar un subconjunto de coeficientes a usarse como la semilla de una clave criptográfica robusta (I). A continuación el sistema implementado en el segundo servidor 200 puede realizar la función de troceo de estos coeficientes para producir una clave válida (J) y generar una clave auxiliar *P* que permite hacer frente a la variabilidad inherente de enfoques biométricos (K). Con la clave criptográfica cifra el testigo usado como OTP (L) y la salida de este proceso se agrupa con la cadena auxiliar *P* y toda la información necesaria para facilitar la tarea de descifrar esta información al programa especializado 102 manejado por el usuario 100 (patrón, indicaciones de tiempo, etc.).

El segundo servidor 200 envía toda esta información al programa especializado del usuario 102 (M) que recibe la información y solicita que el usuario 100 genere una firma biométrica válida basándose en el patrón recibido (N). Una vez que se captura una nueva firma biométrica el sistema usa la cadena auxiliar *P* para determinar el subconjunto de coeficientes a usarse como la semilla de la clave criptográfica esperada (O). Y a continuación realiza la función de troceo de este subconjunto con otras partes de la cadena auxiliar *P* para producir la clave criptográfica (P) y la usa para descifrar la OTP (Q) solicitada por el primer servidor 300 (S). El usuario 100 recupera la OTP del programa especializado 102 y la introduce en el explorador 101 (T) y la envía al primer servidor 300 (U). El primer servidor 300 puede comprobar si la OTP enviada a través del explorador 101 coincide con la recibida con el estado de la cuenta (V). El primer servidor 300 deniega la ejecución de la operación si las OTP no se ajustan.

La Figura 8 ilustra el proceso definido para obtener información biométrica del usuario para realizar el reconocimiento de usuario posterior. Una vez que el usuario 100 intenta iniciar una sesión con el segundo servidor 200 usando el programa especializado 102 instalado en su dispositivo móvil, debe proporcionar credenciales válidas (A) que el segundo servidor 200 comprobará (B) antes de confirmar el inicio de sesión (D). Cuando el segundo servidor 200 verifica la corrección de las credenciales también recupera la información de perfil para conocer si hay información biométrica fijada en él y si esta información debe existir (C). Si el usuario 100 tuviera que añadir información biométrica proporcionada para interactuar con el primer servidor 300, debe almacenarse una firma biométrica válida y un vector con la información de la tolerancia de cualesquiera de los coeficientes incluidos en esa firma (E).

En el caso de que esta firma se requiriera pero no exista en el sistema, es necesario solicitar que el usuario 100 participe en un proceso de entrenamiento. Antes del proceso de entrenamiento, se genera un conjunto de patrones por el segundo servidor 200 (F) y se envía al programa especializado 102 (G). Una vez que se recibe este conjunto en el programa especializado 102, los patrones se usan uno a uno para presentarse al usuario 100 para calcular la correspondiente firma biométrica (H). En el caso mostrado en la Figura 8 es el programa especializado 102 el que se encarga de calcular la firma biométrica promedio de todas las muestras precalculadas. Durante este cálculo, es

posible determinar la tolerancia asociada a cada coeficiente (I). Como se ha explicado antes, esta tolerancia proporciona información acerca de cómo de discriminatorio es un coeficiente en el deber de reconocer este usuario particular 100. Sin embargo, en algunas circunstancias, puede ser necesario configurar el programa especializado 102 para enviar los datos obtenidos del usuario 100 al segundo servidor 200 sin procesarlos. En este caso, los procedimientos biométricos se calcularán en el segundo servidor 200. Una vez que se determinan la firma promedio y el vector de tolerancia, se envían al segundo servidor 200 (J) que los almacena en el perfil del usuario 100 (K), listos para usarse cuando se recibirá una solicitud de estado de operación y están configurados con este mecanismo de factor de autenticación adicional reforzado.

La invención propuesta puede implementarse en hardware, software, firmware, o cualquier combinación de los mismos. Si se implementan en software, las funciones pueden almacenarse en o codificarse como una o más instrucciones o código en un medio legible por ordenador.

Medio legible por ordenador incluye medio de almacenamiento informático. Medio de almacenamiento puede ser cualquier medio disponible que pueda accederse por un ordenador. A modo de ejemplo, y no como limitación, tal medio legible por ordenador puede comprender RAM, ROM, EEPROM, CD-ROM u otro almacenamiento de disco óptico, almacenamiento de disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio que pueda usarse para llevar o almacenar código de programa deseado en forma de instrucciones o estructuras de datos y que puede accederse por un ordenador. Disco magnético y disco óptico, como se usan en el presente documento, incluyen disco compacto (CD), laser disc, disco óptico, disco versátil digital (DVD), disco flexible y disco Blu-ray donde los discos magnéticos normalmente reproducen datos magnéticamente, mientras que los discos ópticos reproducen datos ópticamente con láseres. Combinaciones de lo anterior deberían incluirse también dentro del alcance de medio legible por ordenador. Cualquier procesador y el medio de almacenamiento pueden residir en un ASIC. El ASIC puede residir en un terminal de usuario. Como alternativa, el procesador y el medio de almacenamiento pueden residir como componentes discretos en un terminal de usuario.

Como se usa en el presente documento, productos de programa informático que comprenden medio legible por ordenador incluyen todas las formas de medio legible por ordenador excepto, en la medida en que dichos medios se consideran señales de propagación transitorias no reglamentarias.

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

REIVINDICACIONES

1. Un método implementado por ordenador para asegurar operaciones en sistemas de autenticación y autorización usando información biométrica, en el que se usa un segundo servidor (200), en conexión con un dispositivo informático de un usuario (100), mediante un segundo programa especializado (102) instalado en dicho dispositivo informático, para gestionar un estado de las cuentas que tiene el usuario (100) en un primer servidor (300) y un estado de las operaciones definidas para una cuenta particular, estableciéndose dicho estado de cuenta y dicho estado de operación, cada vez que el usuario (100) desea, como válido o inválido por el usuario (100) mediante el segundo programa especializado (102) y almacenado en una memoria del segundo servidor (200), y estableciéndose dicho estado de cuenta y dicho estado de operación por el usuario (100) una vez que se completa un proceso de emparejamiento con el segundo servidor (200), asegurando dicho proceso de emparejamiento privacidad para el usuario (100), comprendiendo el método:

- recibir, por dicho primer servidor (300), del usuario (100) mediante un primer programa especializado (101) que incluye un explorador, una solicitud para iniciarse sesión en un servicio de dicho primer servidor (300), incluyendo dicha solicitud el suministro de información de identificación que valida la identidad del usuario (100) en el primer servidor (300);
- autenticar, por dicho primer servidor (300), dicha información de identificación del usuario (100) para autorizar dicha solicitud de inicio de sesión de servicio;
- solicitar, por el usuario (100), mediante el primer programa especializado (101), una vez que se ha autenticado la solicitud de inicio de sesión de servicio por el primer servidor (300), para realizar una operación en el primer servidor (300) asociada con el servicio solicitado;
- recibir, por el segundo servidor (200), del primer servidor (300), una solicitud acerca de un estado de operación asociado con lo que el usuario (100) ha establecido para dicha operación solicitada para ayudar al primer servidor (300) a autorizar o rechazar la operación solicitada;
- verificar, por el segundo servidor (200), dicho estado de operación previamente establecido por el usuario (100) para dicha operación solicitada, y si el resultado de dicho estado de operación se ha establecido como válido por el usuario (100), generar, por el segundo servidor (200), un mecanismo de factor de autenticación adicional que comprende las siguientes etapas:

  recuperar, por el segundo servidor (200), una firma biométrica previamente almacenada del usuario (100) (*C*) y un vector de pesos (*W*) de la misma;
  seleccionar, por el segundo servidor (200), un conjunto de coeficientes ($C_0, C_1, C_2,..., C_N$) de dicha firma biométrica almacenada (*C*) para usarse como clave criptográfica, realizar la función de troceo del conjunto seleccionado de coeficientes (C_0, C_1, C_2, C_N) para producir una clave válida (*K*), y generar una cadena auxiliar (*P*);
  cifrar, por el segundo servidor (200), una contraseña de un solo uso, OTP, con la clave válida producida (*K*) y enviar la OTP cifrada junto con al menos la clave auxiliar generada (*P*) al segundo programa especializado (102);
  capturar, por el segundo programa especializado (102), una firma biométrica del usuario (100) (*C*'), capturándose dicha firma biométrica capturada (*C*') empleando la misma técnica biométrica que dicha firma biométrica almacenada (*C*); y
  usar, por el segundo programa especializado (102), la cadena auxiliar recibida (*P*) para determinar el conjunto de coeficientes (C_0, C_1, C_2,...,C_N) a usarse al menos para dicha firma biométrica capturada del usuario (100) (*C'*) y realizar la función de troceo del conjunto de coeficientes (C_0, C_1, C_2,...,C_N) para producir la clave válida para descifrar la OTP cifrada; y

- enviar, por el segundo servidor (200), dicha OTP en el envío de dicho resultado del estado de operación al primer servidor (300) para que el último emplee la OTP recibida para continuar con la operación solicitada.

2. El método implementado por ordenador de la reivindicación 1, en el que dicha solicitud hecha por el primer servidor (300) al segundo servidor (200) comprende un intercambio de credencial entre el primer servidor (300) y el segundo servidor (200) para proporcionar autenticación mutua.

3. El método implementado por ordenador de la reivindicación 1, en el que la firma biométrica del usuario (100) (*C*) y el vector de pesos (*W*) están almacenados en el segundo servidor (200) después de que el segundo programa especializado (102) haya ejecutado un procedimiento de entrenamiento.

4. El método implementado por ordenador de la reivindicación 3, en el que el procedimiento de entrenamiento incluye la captura de diferentes medidas biométricas del usuario (100) de acuerdo con patrones predefinidos generados por el segundo servidor (200), y el procesamiento de las medidas biométricas para cálculo adicional de dicha biométrica (*C*) y dicho vector de pesos (*W*).

5. El método implementado por ordenador de la reivindicación 1, que comprende adicionalmente emplear un número

aleatorio *(x),* como una sal criptográfica, para aumentar la entropía de la clave criptográfica y para evitar ataques de reproducción en la generación de la cadena auxiliar *(P).*

6. El método implementado por ordenador de reivindicaciones anteriores, en el que la información biométrica incluye al menos una de una huella digital, una exploración de voz, una exploración facial o una exploración de iris.

7. El método implementado por ordenador de la reivindicación 1, en el que el segundo servidor (200) notifica al usuario (100) si se rechaza la solicitud para iniciarse sesión en un servicio de dicho primer servidor (300), comprendiendo dicha notificación uno de un envío de un Servicio de Mensajes Cortos (SMS), un envío de un correo electrónico, un envío de un mensaje por una aplicación de mensajería de teléfono inteligente, y/o resaltando o destacando en dicho segundo programa especializado (102) de dicho dispositivo informático de usuario.

8. El método implementado por ordenador de la reivindicación 2, en el que dicho estado de operación se establece como válido o como inválido un cierto periodo de tiempo.

9. El método implementado por ordenador de la reivindicación 1, en el que se registran la solicitud para iniciarse sesión en un servicio del primer servidor (300) y/o la solicitud para realizar una operación en el primer servidor (300) para proporcionar estadísticas.

10. Un sistema de comunicaciones para asegurar operaciones en sistemas de autenticación y autorización usando información biométrica, que comprende un primer servidor (300) configurado para recibir, de un usuario (100) mediante un primer programa especializado (101) que incluye un explorador, una solicitud para iniciarse sesión en un servicio en el mismo y para autenticar información de identificación de dicho usuario (100) en el primer servidor (300) para autorizar dicha solicitud de inicio de sesión de servicio,
caracterizado porque comprende adicionalmente un segundo servidor (200), en conexión con un dispositivo informático del usuario (100) que tiene instalado en el mismo un segundo programa especializado (102), configurado para:

- recibir, del segundo programa especializado (102), cada vez que el usuario (100) desee, los ajustes que el usuario desea para las operaciones proporcionadas por el primer servidor (300), comprendiendo dichos ajustes una indicación de que se permite una operación, o establecida como válida, por el usuario (100) o que una operación no está permitida, o establecida como inválida, por el usuario (100), y estableciéndose los ajustes una vez que se completa un proceso de emparejamiento entre el segundo servidor (200) y el usuario (100), asegurando el proceso de emparejamiento privacidad para el usuario (100);
- recibir, del primer servidor (300), una solicitud acerca de un estado de operación asociado con lo que dicho usuario (100) ha establecido para dicha operación solicitada para ayudar al primer servidor (300) a autorizar o rechazar la operación solicitada;
- verificar dicho estado de operación previamente establecido por el usuario (100) para dicha operación solicitada;
- generar, en caso de que el resultado de dicho estado de operación se establezca como válido por el usuario (100), un mecanismo de factor de autenticación adicional por el segundo servidor (200) que incluye una pluralidad de módulos configurados para:

  recuperar, por un módulo biométrico de servidor (201), una firma biométrica previamente almacenada del usuario (100) (C) y un vector de pesos (*W*) de la misma;
  seleccionar, por un módulo de generación (202), un conjunto de coeficientes (C_0, C_1, C_2,..., C_N) de dicha firma biométrica almacenada *(C)* para usarse como clave criptográfica, realizar la función de troceo del conjunto seleccionado de coeficientes (C_0, C_1, C_2,...,C_N) para producir una clave válida (*K*), y generar una cadena auxiliar (*P*); y
  cifrar, por un módulo de cifrado (204), la OTP generada con la clave válida producida (*K*) y enviar, por un módulo emisor (205), la OTP cifrada junto con al menos la clave auxiliar generada (*P*) al segundo programa especializado (102);

e incluyendo el segundo programa especializado (102) una pluralidad de módulos configurados para:

  capturar, por un módulo biométrico (103), una firma biométrica del usuario (100) (*C'*);
  recibir, por un módulo receptor (104) la OTP cifrada enviada junto con la cadena auxiliar generada (*P*) y la firma biométrica capturada del usuario (100) (*C'*);
  determinar, por un módulo de reproducción (105), usando al menos la clave auxiliar generada (*P*), el conjunto de coeficientes (C_0, C_1, C_2,..., C_N) a usarse para dicha firma biométrica capturada del usuario (100) (C') y para realizar la función de troceo del conjunto de coeficientes (C_0, C_1, C_2,..., C_N) para producir la clave válida; y
  descifrar, por un módulo de descifrado (106), la OTP recibida usando la clave válida producida; y

- enviar el resultado del estado de operación y dicha OTP al primer servidor (300) para que el primer servidor

(300) emplee la OTP para continuar con la operación solicitada.

11. Un producto de programa informático, que incluye instrucciones de código de programa informático que cuando se ejecutan en un ordenador realizan las etapas del método para asegurar operaciones usando información biométrica de acuerdo con la reivindicación 1.

12. El producto de programa informático de la reivindicación 11, que incluye adicionalmente instrucciones de código de programa informático que cuando se ejecutan en un ordenador implementan las etapas del método de acuerdo con la reivindicación 4.

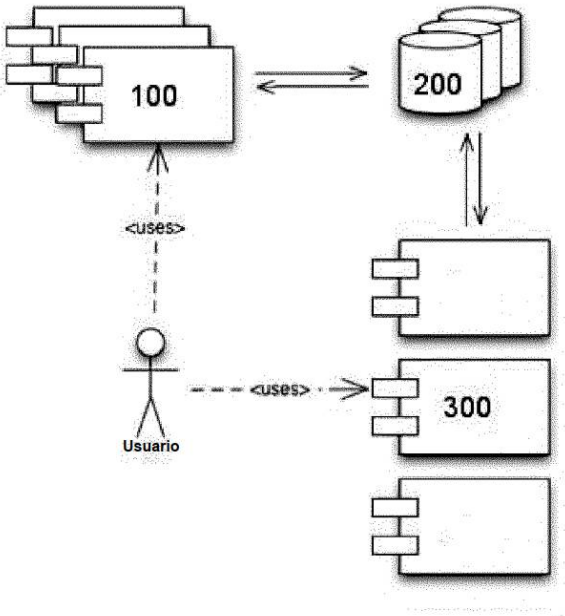
100
200
<uses>
<uses>
300
Usuario

Fig. 1

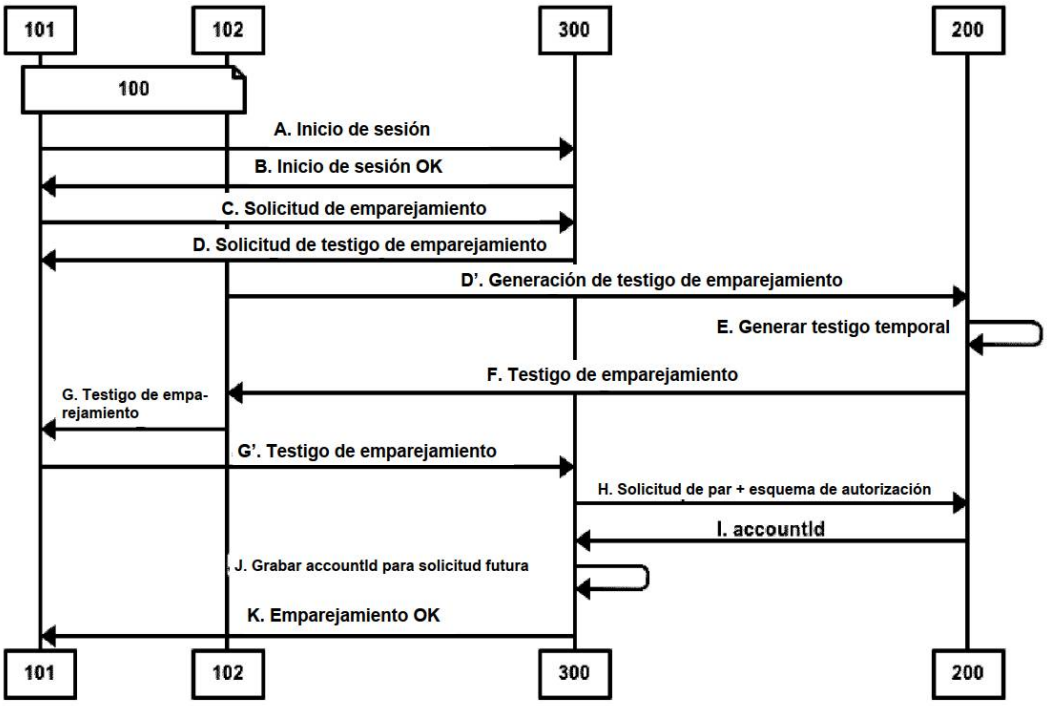
101
102
300
200
100
A. Inicio de sesión
B. Inicio de sesión OK
C. Solicitud de emparejamiento
D. Solicitud de testigo de emparejamiento
D'. Generación de testigo de emparejamiento
E. Generar testigo temporal
F. Testigo de emparejamiento
G. Testigo de empa-
rejamiento
G'. Testigo de emparejamiento
H. Solicitud de par + esquema de autorización
I. accountId
J. Grabar accountId para solicitud futura
K. Emparejamiento OK
101
102
300
200

Fig. 2

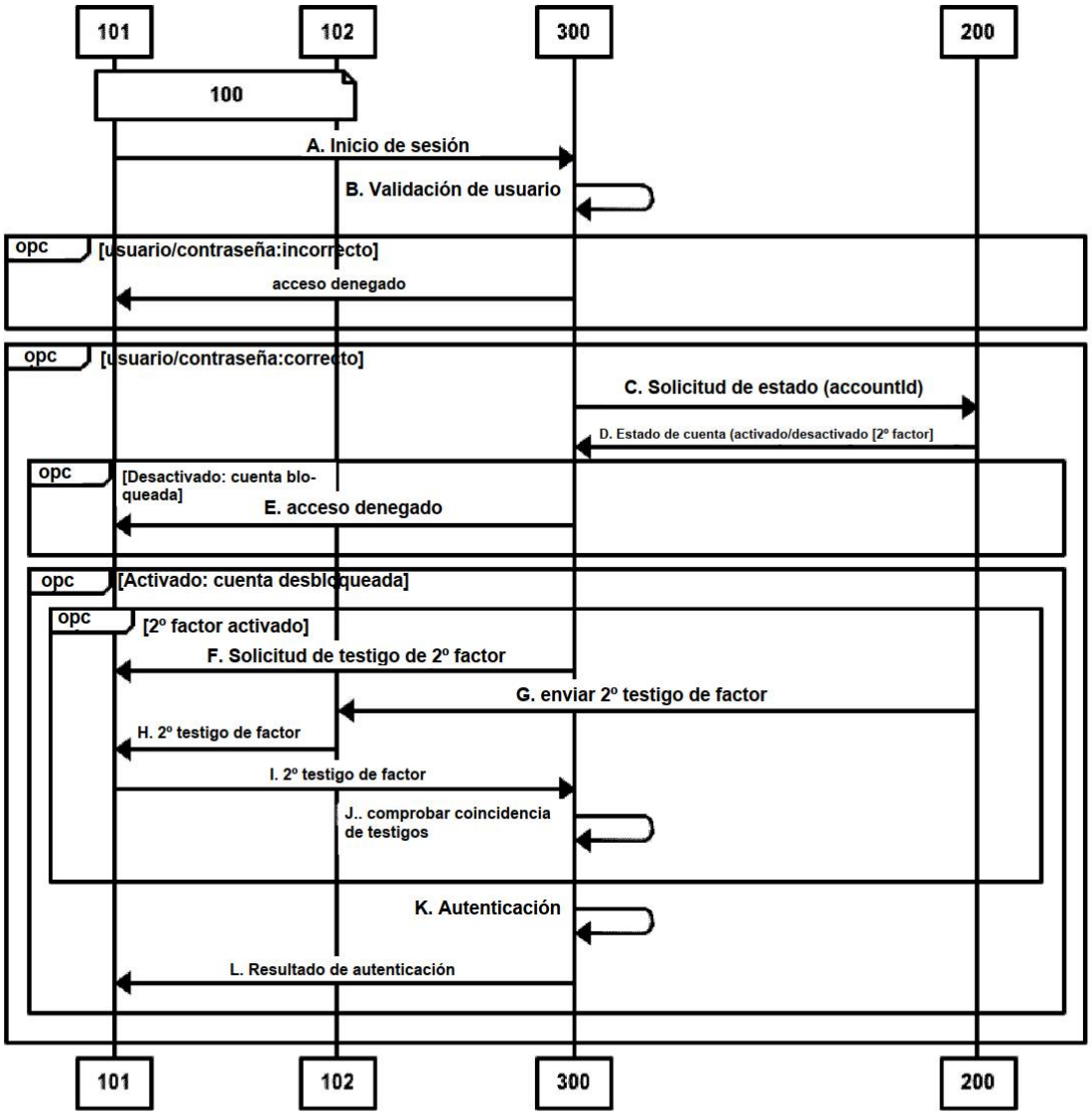
101
102
300
200
100
A. Inicio de sesión
B. Validación de usuario
opc
[usuario/contraseña:incorrecto]
acceso denegado
opc
[usuario/contraseña:correcto]
C. Solicitud de estado (accountId)
D. Estado de cuenta (activado/desactivado [2º factor]
opc
[Desactivado: cuenta bloqueada]
E. acceso denegado
opc
[Activado: cuenta desbloqueada]
opc
[2º factor activado]
F. Solicitud de testigo de 2º factor
G. enviar 2º testigo de factor
H. 2º testigo de factor
I. 2º testigo de factor
J.. comprobar coincidencia de testigos
K. Autenticación
L. Resultado de autenticación
101
102
300
200

Fig. 3

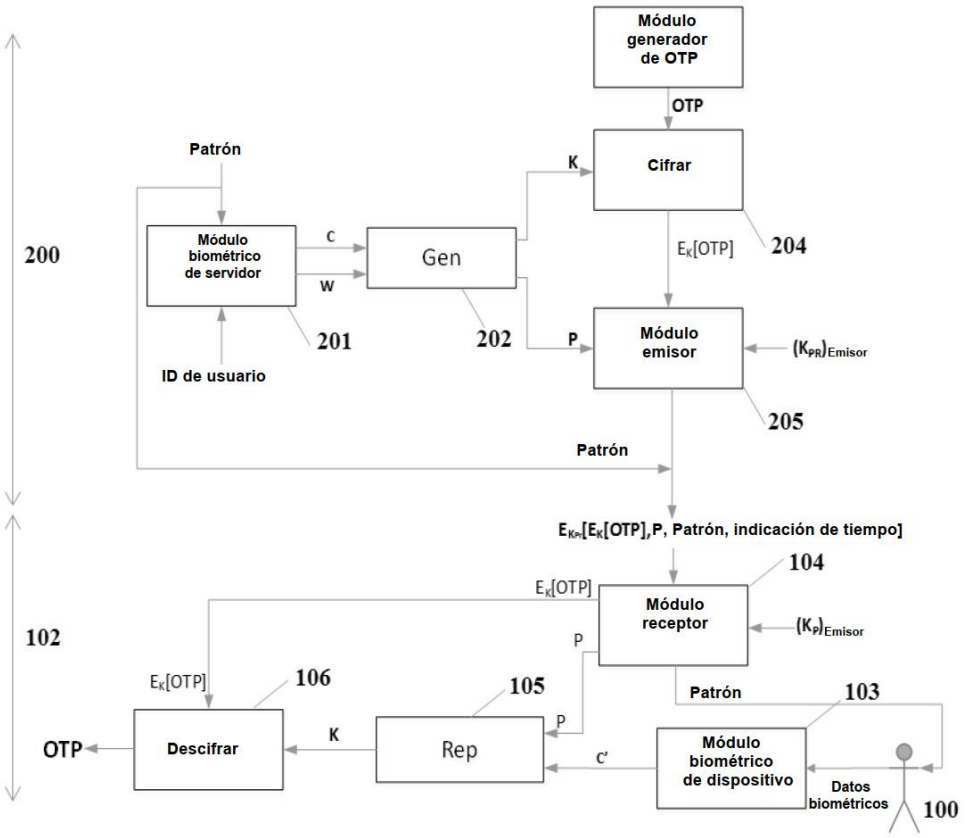
Módulo generador de OTP
OTP
Patrón
K
Cifrar
Módulo biométrico de servidor
c
W
Gen
E_K[OTP]
204
200
201
202
P
Módulo emisor
$(K_{PR})_{Emisor}$
ID de usuario
205
Patrón
$E_{K_P}[E_K[OTP], P, Patrón, indicación de tiempo]$
104
E_K[OTP]
Módulo receptor
$(K_P)_{Emisor}$
102
P
E_K[OTP]
106
105
Patrón
103
OTP
Descifrar
K
Rep
P
c'
Módulo biométrico de dispositivo
Datos biométricos
100

Fig. 4

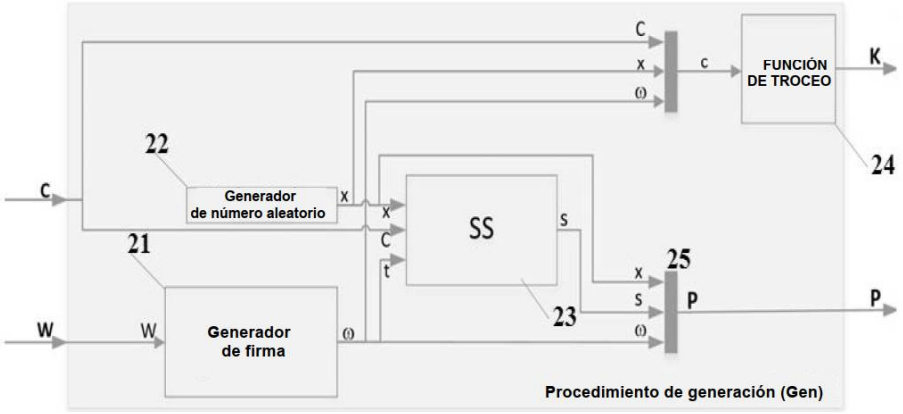
C
x
ω
c
FUNCIÓN DE TROCEO
K
22
24
C
Generador de número aleatorio
x
x
SS
s
C
21
t
25
x
s
P
P
W
W
Generador de firma
ω
23
ω
Procedimiento de generación (Gen)

Fig. 5

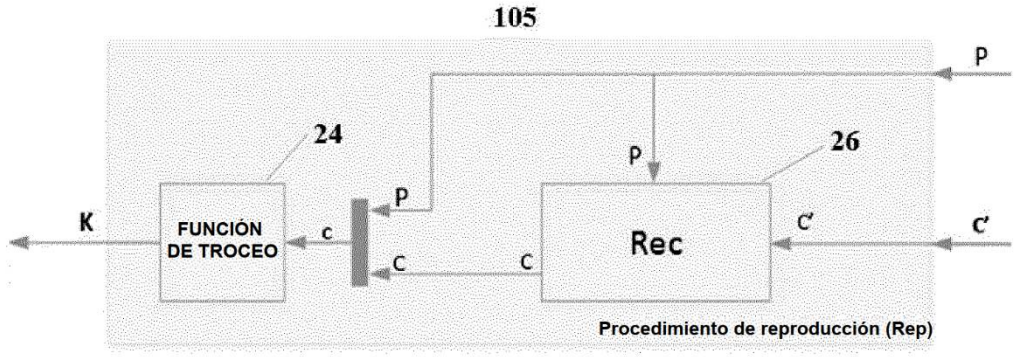
105
P
24
26
P
P
K
FUNCIÓN DE TROCEO
c
C
C
Rec
C'
C'
Procedimiento de reproducción (Rep)

Fig. 6

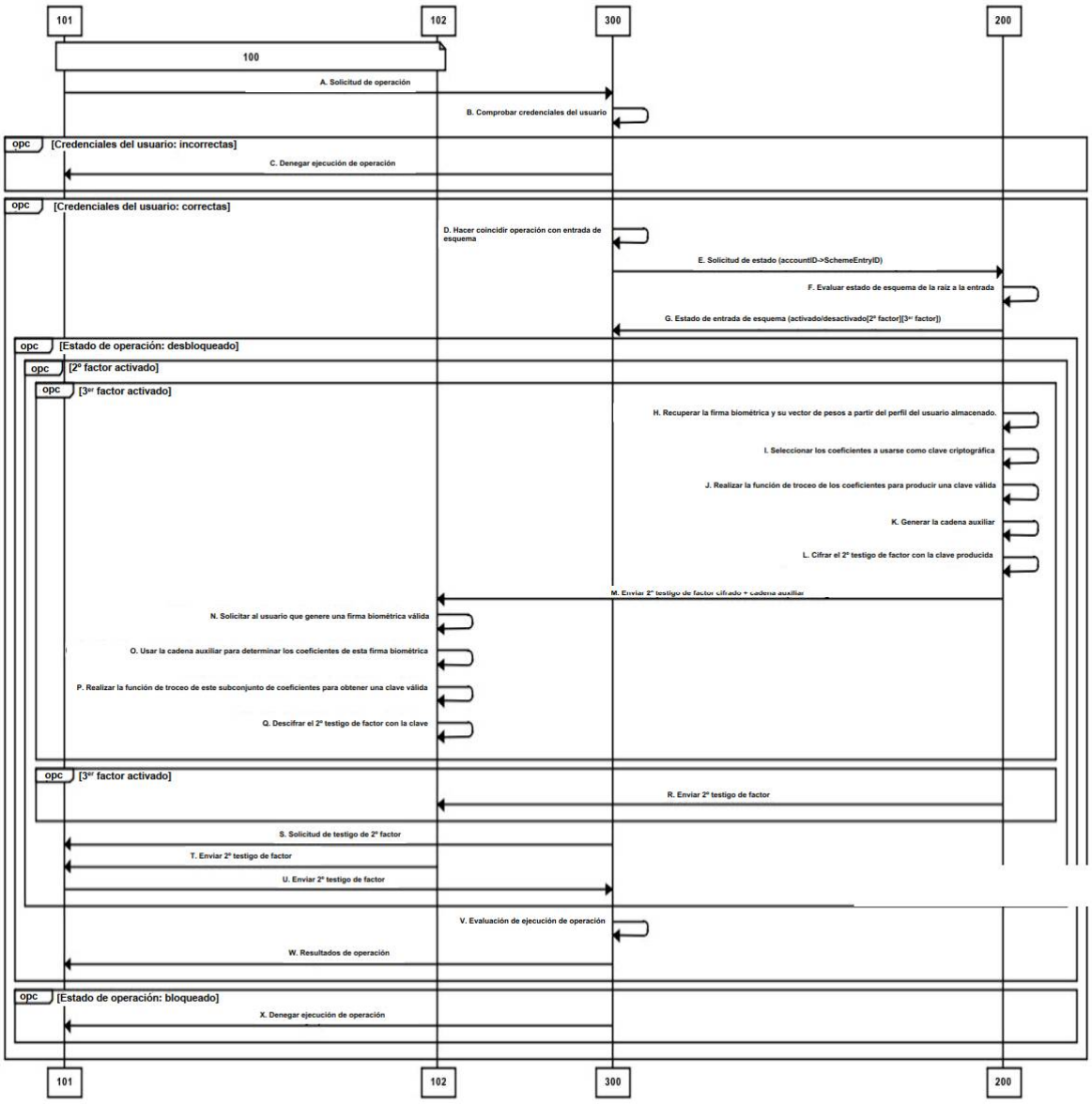
101
102
300
200
100
A. Solicitud de operación
B. Comprobar credenciales del usuario
opc
[Credenciales del usuario: incorrectas]
C. Denegar ejecución de operación
opc
[Credenciales del usuario: correctas]
D. Hacer coincidir operación con entrada de esquema
E. Solicitud de estado (accountID->SchemeEntryID)
F. Evaluar estado de esquema de la raiz a la entrada
G. Estado de entrada de esquema (activado/desactivado[2º factor][3er factor])
opc
[Estado de operación: desbloqueado]
opc
[2º factor activado]
opc
[3er factor activado]
H. Recuperar la firma biométrica y su vector de pesos a partir del perfil del usuario almacenado.
I. Seleccionar los coeficientes a usarse como clave criptográfica
J. Realizar la función de troceo de los coeficientes para producir una clave válida
K. Generar la cadena auxiliar
L. Cifrar el 2º testigo de factor con la clave producida
M. Enviar 2º testigo de factor cifrado + cadena auxiliar
N. Solicitar al usuario que genere una firma biométrica válida
O. Usar la cadena auxiliar para determinar los coeficientes de esta firma biométrica
P. Realizar la función de troceo de este subconjunto de coeficientes para obtener una clave válida
Q. Descifrar el 2º testigo de factor con la clave
opc
[3er factor activado]
R. Enviar 2º testigo de factor
S. Solicitud de testigo de 2º factor
T. Enviar 2º testigo de factor
U. Enviar 2º testigo de factor
V. Evaluación de ejecución de operación
W. Resultados de operación
opc
[Estado de operación: bloqueado]
X. Denegar ejecución de operación
101
102
300
200

Fig. 7

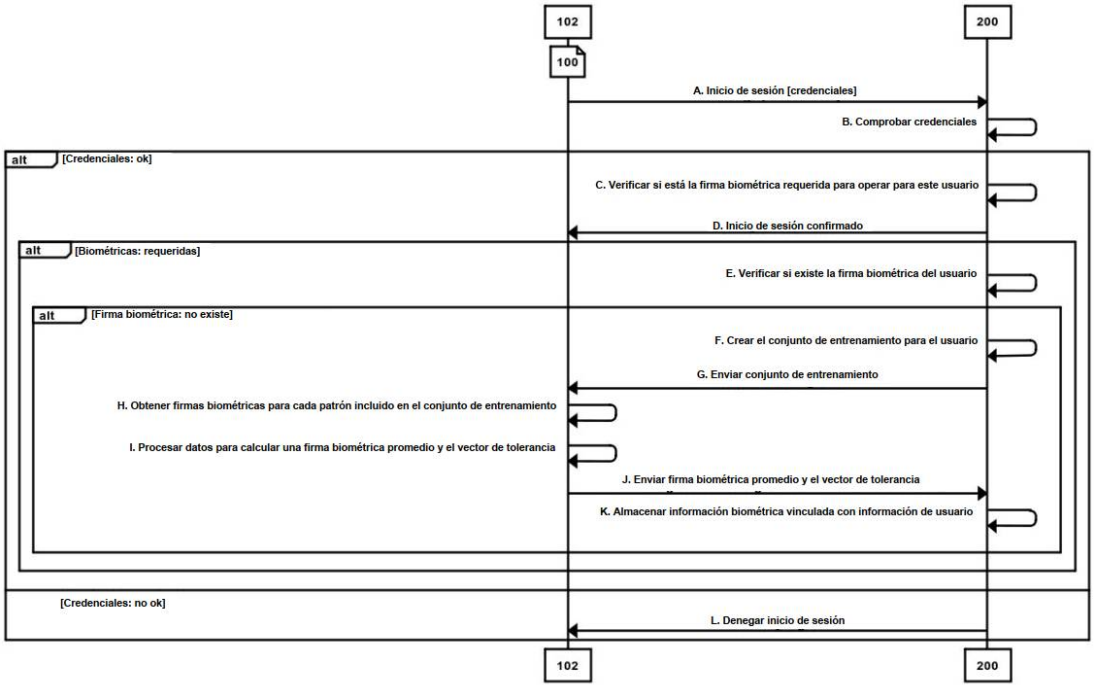
102
100
200
A. Inicio de sesión [credenciales]
B. Comprobar credenciales
alt
[Credenciales: ok]
C. Verificar si está la firma biométrica requerida para operar para este usuario
D. Inicio de sesión confirmado
alt
[Biométricas: requeridas]
E. Verificar si existe la firma biométrica del usuario
alt
[Firma biométrica: no existe]
F. Crear el conjunto de entrenamiento para el usuario
G. Enviar conjunto de entrenamiento
H. Obtener firmas biométricas para cada patrón incluido en el conjunto de entrenamiento
I. Procesar datos para calcular una firma biométrica promedio y el vector de tolerancia
J. Enviar firma biométrica promedio y el vector de tolerancia
K. Almacenar información biométrica vinculada con información de usuario
[Credenciales: no ok]
L. Denegar inicio de sesión
102
200

Fig. 8