(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 403 280**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **11.05.2009 E 09776598 (6)**

(97) Fecha y número de publicación de la concesión europea: **23.01.2013 EP 2359525**

(54) Título: **Método para rehabilitar la limitación del acceso de servicio**

(30) Prioridad:

10.09.2008 EP 08015967

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.05.2013

(73) Titular/es:

NEC CORPORATION (100.0%)
7-1, Shiba 5-chome Minato-ku
Tokyo 108-8001, JP

(72) Inventor/es:

PASHALIDIS, ANDREAS

(74) Agente/Representante:

ROEB DÍAZ-ÁLVAREZ, María

DESCRIPCIÓN

Método para habilitar la limitación del acceso de servicio

La presente invención se refiere a un método para habilitar la limitación del acceso de servicio.

En las redes de comunicación de hoy, existen muchos tipos diferentes de servicios y los emplean un número constantemente creciente de usuarios. Normalmente, estos servicios los ofrecen proveedores de servicio con los cuales los usuarios se pueden registrar con el fin de obtener acceso a los servicios solicitados. En general, el registro de un usuario con un proveedor de servicio es un proceso anónimo en un cierto sentido, es decir, el registro se basa en la identidad digital de un usuario, mientras que la identidad real del usuario sigue siendo desconocida para el proveedor de servicio.

Para muchas aplicaciones en el mundo digital, tales como por ejemplo el voto electrónico, el dinero electrónico, los cupones electrónicos o la navegación de prueba de contenido, es una tarea crucial imponer un límite estricto en el número de identidades digitales diferentes con las cuales un usuario puede invocar o registrarse en un servicio. Por ejemplo, en el caso del voto electrónico es esencial garantizar de manera fiable que cada usuario pueda votar sólo una vez. En el caso de la navegación de prueba de contenido, los proveedores normalmente quieren asegurarse de que a un usuario específico le esté permitido buscar contenido tal como películas o música libremente sólo por un número limitado de veces, p. ej. el proveedor de servicio puede permitir al usuario que descargue dos películas o diez canciones. Después de la fase de prueba, el proveedor del servicio quiere que el usuario pague el servicio.

De acuerdo con el estado de la técnica, hay soluciones para habilitar una limitación del acceso de servicio que se basan en la criptografía asimétrica. No obstante, estos métodos conocidos a partir de la técnica anterior son bastante desventajosos ya que las técnicas asimétricas empleadas requieren costosas computaciones y procedimientos de gestión clave complejos que resultan en un gasto general computacional elevado. Debido a su complejidad computacional, estos métodos no son adecuados para muchas aplicaciones.

Además, imponer un límite en el número de identidades digitales diferentes con las cuales un usuario puede invocar o registrarse en un servicio normalmente requiere que el proveedor del servicio obtenga cierta información sobre un usuario registrado. Esto vincula la identidad digital del usuario empleada para acceder al proveedor del servicio al menos de algún modo con la identidad real del usuario. Un vínculo tal puede ser fundamental con respecto a la preservación de la privacidad de un usuario.

Como una técnica convencional para habilitar la limitación del acceso de servicio, se conoce un mecanismo revelado en WO 2005/069295 A1, el cual se dirige a la detección de terminales no autorizados por medio de un servidor de autenticación. En la invención revelada en este documento, un terminal de DVD solicita al servidor de autenticación que envíe subcontenido. En respuesta, el servidor de autenticación genera y transmite al terminal de DVD un número aleatorio R. El terminal de DVD lee una tecla del terminal y un ID de terminal que se almacenan en una unidad de memoria de información de terminal, descifra el número aleatorio recibido R mediante el uso de una tecla del terminal SK_X y lo envía junto con el ID de terminal (ID_X) al servidor de autenticación. A continuación, el servidor de autenticación verifica el número aleatorio encriptado R y el ID de terminal recibidos del terminal de DVD y juzga si el terminal de DVD es el terminal autenticado o no.

Además, GB 2 371 957 A revela una técnica de autenticación entre servidores en un protocolo de red de terceros incluyendo un servidor de acceso a la red (NAS) en comunicación con un servidor de autenticación remoto (RAS) acoplado a la red.

En US 6,487,659 B1, se revelan un dispositivo y un método para la autenticación condicional con uso de información de soporte de prueba, la cual se destina a imponer una limitación en cuanto a la utilización y a hacer posible el procesamiento de alta velocidad.

WO 2005/008399 A2 revela sistemas y métodos para habilitar transacciones en arquitectura, en las que se presenta el concepto de personalidad, el cual es un conjunto de datos sobre un individuo que se puede acercar de forma segura a una transacción. Una interfaz garantiza el acceso a la personalidad basado en una biometría presentada por un usuario en una transacción.

Es por tanto un objeto de la presente invención mejorar y desarrollar además un método para habilitar la limitación del acceso de servicio de una forma tal que se garantice una elevada fiabilidad con respecto a la imposición de la limitación. Además, la privacidad de los usuarios “honestos”, es decir, los usuarios que no intentan exceder un número máximo de accesos de servicio admisibles, se debe preservar, empleando de este modo mecanismos que se van a implementar inmediatamente y que implican una complejidad computacional reducida.

De acuerdo con la invención, el objeto anteriormente mencionado se logra por un método que comprende las características de la reivindicación 1. De acuerdo con esta reivindicación, se revela un método para habilitar la limitación del acceso de servicio, en el cual un proveedor de servicio ofrece al menos un servicio y en el que un

usuario posee múltiples identidades digitales diferentes I_i, que se pueden usar para invocar o registrarse en el servicio. El acceso al servicio requiere una cuenta en una entidad de terceros, en la que el usuario registra sus identidades digitales I_i con la cuenta y en la que el usuario acuerda un secreto S con la entidad de terceros. El método comprende los pasos de

el usuario asignando a sus identidades digitales diferentes I_i valores de contador únicos $k_{i,SR}$,

el usuario solicitando el servicio empleando una identidad digital específica I_i y calculando un valor de verificación – primer valor de verificación v_1 – mediante la aplicación de un algoritmo de codificación H en el secreto S y el valor de contador $k_{i,SR}$ asignado a la identidad digital I_i empleada para la solicitud del servicio, recibiendo dicha entidad de terceros el primer valor de verificación v_1, aplicando el algoritmo de codificación H para reconstruir el valor de contador empleado $k_{i,SR}$ y proporcionando información de si el valor de contador reconstruido $k_{i,SR}$ excede un límite lim_{SR},

en el que dicho proveedor de servicio mantiene una lista V_{SR}, en la cual se incluyen los primeros valores de verificación v_1 recibidos del usuario, y

en la que dicho proveedor de servicio aborta el registro del usuario con dicho servicio en caso de que una comprobación demuestre que dicho primer valor de verificación reconstruido correctamente v_1 ya es un elemento de dicha lista V_{SR}.

De acuerdo con la invención, se ha organizado primero que, en el contexto de habilitar la limitación del acceso de servicio, los mecanismos existentes que usan primitivas de clave pública son bastante complejos y, por consiguiente, no se pueden aplicar en varias situaciones. Además, se ha reconocido que debido al hecho de que la criptografía asimétrica requiere un gasto general computacional muy elevado, en particular en el caso en el que el número de registros admisible es amplio, los mecanismos existentes no son eficientes.

Se ha reconocido además que, mediante la implicación de una entidad de terceros de una forma adecuada, es posible realizar una imposición de límite de registro eficiente que se basa exclusivamente en primitivas de criptografía simétricas. Confiando solamente en técnicas simétricas, se obtienen como resultado gastos generales computacionales muy bajos y gestión de clave relativamente simple.

De acuerdo con la presente invención, se garantiza que el valor de contador no exceda el límite lim_{SR}. La entidad de terceros puede proporcionar un mensaje de error en caso de que no se haya encontrado un primer valor de verificación correcto v_1 y puede proporcionar un mensaje satisfactorio en caso de que se haya encontrado el primer valor de verificación correcto v_1. Dependiendo del resultado de la reconstrucción, el proveedor del servicio puede cumplir diferentes decisiones en lo que se refiere al manejo de la solicitud de servicio del usuario. Por ejemplo, se puede prever que el proveedor del servicio rechace la solicitud del servicio en caso de recibir un mensaje de error de la entidad de terceros.

Por otro lado, en el caso de recibir un mensaje satisfactorio de la entidad de terceros, es preferible no conceder automáticamente al usuario el acceso al servicio. De acuerdo con la presente invención, en este caso se lleva a cabo una comprobación adicional en el proveedor del servicio con el fin de evitar que se reutilicen los valores de contador. Con este fin, el proveedor del servicio SP mantiene una lista V_{SR} de valores de verificación v_1, es decir, una lista en la cual se almacenan todos los primeros valores de verificación v_1 recibidos del usuario. Cuando el proveedor del servicio recibe un mensaje satisfactorio de la entidad de terceros, puede comprobar si el primer valor de verificación correspondiente v_1 ya se ha incluido en su lista V_{SR}. Si es así, esto se puede interpretar como una fuerte evidencia de que el usuario intenta acceder al servicio más veces de las que se permiten y el proveedor del servicio puede rechazar la solicitud. Si no es así, el proveedor del servicio puede conceder al usuario el acceso y puede añadir los primeros valores de verificación recibidos v_1 a la lista V_{SR}.

Una ventaja adicional de la presente invención es que el método se puede usar en una diversa gama de dominios de aplicación con el fin de evitar una superación del límite. De acuerdo con la invención, se hace cumplir el límite de una forma que habilite el anonimato de los usuarios para que se revoque si es necesario y al mismo tiempo respeta la privacidad de los usuarios “honestos”, es decir, los usuarios que no intentan exceder el límite. En otras palabras, el método, de acuerdo con la invención tiene la habilidad inherente de revocar el anonimato de los usuarios.

En una forma de realización específica, el servicio tiene asociado un identificador de servicio único I_{SR} para la identificación del servicio en la entidad de terceros. Especialmente en el caso de los proveedores del servicio que ofrecen una multitud de servicios, se puede emplear un identificador de servicio único I_{SR} para distinguir cada uno de los servicios. Esto es importante ya que un proveedor de servicio puede querer aplicar diferentes políticas para sus servicios, es decir, por ejemplo el número de accesos admisibles para un usuario puede variar de un servicio a otro.

De acuerdo con una forma de realización preferible, el identificador del servicio I_{SR} puede acompañarse con información adicional que se asocia únicamente con el servicio. Con este fin el identificador del servicio I_{SR} se contiene preferiblemente en una cadena de bits. La cadena de bits puede extenderse entonces incluyendo más

información relacionada con el servicio, como p. ej. el localizador de recursos uniforme (URL) del servicio, el límite lim_{SR} del número de accesos admisibles definidos para el servicio, un identificador para el ejemplo de servicio concreto, un valor de marca de tiempo (p. ej. indicando la realidad del servicio) y/o un certificado de clave pública o cadena de certificado para el proveedor del servicio y/o el servicio.

De forma ventajosa, la entidad de terceros es una autoridad de registro. La autoridad de registro puede asistir al proveedor del servicio haciendo cumplir el límite y también puede actuar como una autoridad de revocación de anonimato. La autoridad de registro llega a conocer la asignación de las identidades de usuario a los usuarios; por tanto, se confía en que la autoridad de registro no va a revelar esta asignación a menos que sea requerido para fines de revocación de anonimato. En lo que prueba que es beneficioso si la autoridad de registro es una entidad de confianza, por ejemplo una administración gubernamental o al menos una autoridad oficial.

De acuerdo con una forma de realización preferible, la entidad de terceros puede garantizar que a cada usuario individual le esté permitido crear solamente un número de cuentas bastante limitado. Esto se puede conseguir requiriendo al usuario que produzca un documento que de alguna manera se asigna a su persona y que el usuario posee en la práctica normalmente sólo en un número limitado. Ejemplos característicos de tales documentos serían pasaportes, permisos de conducir o tarjetas de crédito.

En una forma de realización particularmente preferible, la entidad de terceros garantiza que cada usuario individual no pueda tener más de una única cuenta. Con sólo una única cuenta en la entidad de terceros, es posible el estricto control del número de accesos de un usuario en el proveedor del servicio. La prevención de la creación de múltiples cuentas por usuario se puede conseguir requiriendo a un usuario que muestre alguna identificación biométrica única antes de crear la cuenta en la entidad de terceros.

De forma ventajosa, el algoritmo de codificación H es una función unidireccional determinista. La presente invención no impone el uso de ninguna función unidireccional particular para H, siempre que sea determinista. Es decir, se requiere que $a = b => H(a) = H(b)$. Los ejemplos de funciones unidireccionales que se pueden usar con la invención son (sugeridos) generadores de número pseudoaleatorios, esquemas de codificación simétrica, esquemas de código de autenticación de mensaje (MAC) y funciones de troceo. Se recomienda usar una función de troceo criptográfica que tenga un resultado que sea indistinguible del resultado de un oráculo aleatorio.

De acuerdo con una forma de realización preferible, el secreto acordado entre el usuario y la entidad de terceros en el momento de la creación de la cuenta en la entidad de terceros se puede generar aleatoriamente como un valor de secreto único. Desde el punto de vista de generación del secreto, sirve como un secreto que sólo conoce el usuario y la entidad de terceros. Aunque puede derivarse de una contraseña o frase de contraseña, preferiblemente se genera uniformemente de manera aleatoria a partir de un amplio espacio. Con el fin de garantizar una alta fiabilidad, el secreto debería tener la suficiente longitud. La longitud recomendada para el secreto es igual a la longitud del resultado del algoritmo de codificación empleado H.

En cuanto a una codificación eficiente, se puede prever que el usuario, en el contexto de acceder a un servicio, calcule un valor p mediante la aplicación del algoritmo de codificación H en el secreto acordado con la entidad de terceros y el identificador único I_{SR} del servicio solicitado. Esto se puede realizar generando primero una concatenación del secreto y el identificador y aplicando a continuación el algoritmo de codificación H en el valor concatenado. Alternativamente, el secreto y el identificador de servicio se pueden emplear como dos parámetros de entrada independientes para el algoritmo de codificación H. No obstante, en ambos casos el orden de los parámetros es de importancia desde el momento en que las otras partes respectivas deben mantener el orden.

En un paso siguiente, se puede prever que el usuario calcule el primer valor de verificación denotado v_1 mediante la aplicación del algoritmo de codificación H en el valor previamente calculado p y el valor de contador respectivo $k_{i,SR}$. El valor de contador respectivo $k_{i,SR}$ es el valor de contador asociado a la entidad digital I_i empleada por el usuario al intentar acceder al servicio SR. De nuevo, los dos valores se pueden concatenar antes de aplicar H o se pueden introducir como dos parámetros independientes.

De acuerdo con una forma de realización preferible, se puede prever que el valor de verificación v_1 se remita al proveedor del servicio por parte del usuario U directamente. El proveedor del servicio puede entonces remitir además el valor de verificación v_1 a la entidad de terceros desencadenando de ese modo el proceso de reconstrucción del valor de contador respectivo $k_{i,SR}$ tal como se describe con mayor detalle a continuación. Además, el proveedor del servicio puede transmitir el identificador de servicio único I_{SR} a la entidad de terceros de tal forma que el servicio se pueda identificar fácilmente. Se debe tener en cuenta que el reenvío de los valores por parte del proveedor del servicio será la situación de aplicación más importante ya que normalmente el proveedor del servicio estará interesado en hacer cumplir un límite en cuanto al acceso del servicio. No obstante, hay aplicaciones, como el voto electrónico por ejemplo, en las cuales otra entidad u otra persona o grupo de personas o incluso el público tengan un interés en limitar el uso del servicio, por ejemplo para garantizar que ninguna persona haya dado más de un voto. En tanto, también es posible que los valores mencionados más arriba, en particular el primer valor de verificación v_1 sea remitido a la entidad de terceros por una entidad externa.

En la entidad de terceros, después de haber recibido el valor de verificación v_1, el valor de contador $k_{i,SR}$ (asignado a la identidad digital I_i empleada para la solicitud del servicio del usuario) se puede reconstruir del siguiente modo: la entidad de terceros calcula un valor $\overline{p}$ mediante la aplicación del algoritmo de codificación H en el secreto S y el identificador de servicio único I_{SR} de la misma forma que lo hizo el usuario U. No obstante, el problema es que la entidad de terceros, cuando solamente recibe el valor de verificación v_1 y, como puede ser el caso, el identificador de servicio I_{SR}, no disponen de ninguna información de la cual se pudiera deducir el secreto correcto S del usuario. De este modo, se recomienda que la entidad de terceros guarde una lista V_s en la cual se contienen los secretos S_n de todos los usuarios que tienen una cuenta en la entidad de terceros. La entidad de terceros puede iniciar entonces su cálculo mediante (a) la selección de un primer secreto S_1 de la lista V_8 y (b) la aplicación del algoritmo de codificación H tal como se describe dando como resultado un valor $\overline{p}_1$.

En un paso siguiente, la entidad de terceros intenta reconstruir el valor de verificación v_1 mediante la aplicación del algoritmo de codificación H en el valor $\overline{p}_1$ y un valor λ de la misma forma que el usuario U ha aplicado el algoritmo H en los valores p y $k_{i,SR}$ anteriormente. λ denota un valor entre 1 y el límite lim_{SR}. El cálculo se puede iniciar con $\lambda = 1$ y el valor de λ se puede incrementar sucesivamente hasta que se encuentre el primer valor de verificación correcto v_1. Si la entidad de terceros no consigue reproducir el primer valor de verificación correcto v_1, se tomará otro secreto, p. ej. S_2 de la lista V_s y el cálculo se repetirá tal como se describe más arriba. Si la entidad de terceros tiene éxito al reconstruir el primer valor de verificación correcto v_1, esto significa que el usuario ha empleado una identidad digital admisible y que no ha excedido el número tolerable máximo de los accesos del servicio. Por otro lado, un error en la reconstrucción del primer valor de verificación correcto v_1 significa que el usuario ya ha aprovechado completamente el número de accesos concedido y que ahora va a exceder el límite lim_{SR}.

De acuerdo con una forma de realización preferible, el proveedor del servicio SP, además del primer valor de verificación v_1, remite la identidad digital I_i empleada por el usuario a la entidad de terceros. Por estos medios, se puede lograr una reducción significativa del esfuerzo computacional por parte de la entidad de terceros, ya que el secreto correcto se puede derivar directamente debido a la asignación entre las identidades digitales registradas en la entidad de terceros para el usuario y el secreto acordado. Por consiguiente, los cálculos para la reconstrucción del valor de contador $k_{i,SR}$ (asignado a la identidad digital I_i empleada para la solicitud del servicio del usuario) se deben llevar a cabo solamente para un secreto específico.

De forma ventajosa, después de haber recibido el primer valor de verificación junto con la identidad digital I_i, la reconstrucción del valor de contador $k_{i,SR}$ en la entidad de terceros puede comprender los siguientes pasos: en un primer paso, se busca el secreto S correspondiente a la identidad digital I_i. En un segundo paso, se calcula un valor $\overline{p}$ mediante la aplicación del algoritmo de codificación H en el secreto S y el identificador de servicio único I_{SR} de la misma forma que lo hizo el usuario. En un tercer paso, el primer valor de verificación v_1 se calcula mediante la aplicación del algoritmo de codificación H en el valor $\overline{p}$ y λ, siendo λ de nuevo un valor entre 1 y el límite lim_{SR}. El cálculo se puede iniciar con $\lambda = 1$ y el valor de λ se puede incrementar sucesivamente hasta que se encuentre la primera verificación correcta v_1 o hasta que se alcance el límite lim_{SR}.

En caso de que el proveedor del servicio remita la identidad digital I_i empleada por el usuario a la entidad de terceros, se puede presentar un segundo valor de verificación v_2 que esté destinado a reforzar más la privacidad del usuario. Más específicamente, se puede prever que el usuario calcule el segundo valor de verificación v_2 mediante la aplicación del algoritmo de codificación H en el valor p, la identidad digital I_i y el primer valor de verificación v_1. Tal como ya se ha descrito más arriba, los tres valores se pueden concatenar primero y el algoritmo de codificación H se puede aplicar en el valor concatenado. De nuevo, el usuario U puede remitir el segundo valor de verificación v_2 al proveedor del servicio directamente. El proveedor del servicio puede entonces proporcionar el segundo valor de verificación v_2 a la entidad de terceros.

Después de haber reconstruido correctamente el valor de contador $k_{i,SR}$ (asignado a la identidad digital I_i empleada para la solicitud de servicio del usuario) mediante la búsqueda del primer valor de verificación correcto v_1, se puede prever que la entidad de terceros empiece a aplicar dicho algoritmo de codificación H en dicho valor $\overline{p}$, dicha identidad digital I_i y dicho primer valor de verificación v_1 de la misma forma que lo hizo el usuario U, para reconstruir el segundo valor de verificación v_2.

De acuerdo con una forma de realización preferible, la entidad de terceros proporciona un mensaje satisfactorio, en caso de que el segundo valor de verificación correcto v_2 se pudiera reconstruir. Por otro lado, en caso de que las reconstrucciones no se realicen correctamente, la entidad de terceros puede proporcionar un mensaje de error. Hay que tener en cuenta que un error de reconstrucción para un segundo valor de verificación v_2 (habiendo sido reconstruido correctamente un primer valor de verificación v_1) significa que el valor v_1 y el valor v_2 no coinciden y que

el proveedor del servicio ha manipulado su solicitud en la entidad de terceros. Por ejemplo, el proveedor del servicio puede haber amalgamado una identidad de usuario digital I_i recibida en una solicitud de servicio con un primer valor de verificación v_1 recibido con otra solicitud de servicio con el fin de saber si ambas solicitudes del servicio las originó el mismo usuario. Mediante la comprobación del valor v_2 además del valor v_1 en la entidad de terceros, este tipo de uso inapropiado, que puede ser inadmisible, en ciertas aplicaciones, se puede observar y se puede inhabilitar proporcionando un mensaje de error al proveedor del servicio.

De acuerdo con una forma de realización preferible, la entidad de terceros está en línea durante el protocolo. Como consecuencia, es posible *evitar* realmente que los usuarios excedan el límite; algunos de los sistemas existentes detectan simplemente que un usuario ha excedido el límite *después del hecho*, es decir, después de la prestación del servicio. No obstante, puede haber aplicaciones que no requieran que la entidad de terceros esté en línea todo el tiempo; en algunas configuraciones puede bastar con que la entidad de terceros esté en línea periódicamente. En particular, en ocasiones puede no ser necesario para un proveedor de servicio *evitar* que un usuario exceda el límite; puede bastar en su lugar con “limpiar” la base de datos de cuentas duplicadas (o, más generalmente, cuentas que excedan el límite) en intervalos periódicos; en este caso, el proveedor del servicio puede guardar el primer y el segundo valor de verificación v_1, v_2 que recibe de los usuarios y validar sus cuentas con la ayuda de la entidad de terceros en intervalos periódicos.

De acuerdo con una forma de realización preferible, el límite lim_{SR} lo predefine o bien el proveedor del servicio SP en sí mismo o cualquier instancia externa. Por ejemplo, en el caso de las aplicaciones de voto electrónico, una autoridad de confianza puede especificar de forma ventajosa el límite lim_{SR}. De acuerdo con una forma de realización preferible adicional, el límite lim_{SR} se puede cambiar de forma dinámica, por ejemplo dependiendo de los parámetros del servicio.

Hay varias formas sobre cómo diseñar y desarrollar además la enseñanza de la presente invención de una forma ventajosa. Con este fin, se hace referencia a las reivindicaciones de la patente supeditadas a la reivindicación 1 de la patente por un lado y a la siguiente explicación de los ejemplos de las formas de realización preferibles de la invención, ilustrados por el dibujo por otro lado. En conexión con la explicación de las formas de realización preferibles de la invención con ayuda del dibujo, se explicarán en los dibujos las formas de realización generalmente preferibles y los desarrollos adicionales de la enseñanza

Fig. 1 es una vista esquemática de una implementación de un método para habilitar la limitación del acceso de servicio de acuerdo con una forma de realización de la presente invención,

Fig. 2 ilustra una primera forma de realización del algoritmo usado para la implementación del protocolo de imposición de límite de registro de acuerdo con una forma de realización de la presente invención,

Fig. 3 ilustra una segunda forma de realización del algoritmo usado para la implementación del protocolo de imposición de límite de registro de acuerdo con una forma de realización de la presente invención,

Fig. 4 ilustra una tercera forma de realización del algoritmo usado para la implementación del protocolo de imposición de límite de registro de acuerdo con una forma de realización de la presente invención.

La Fig. 1 ilustra, esquemáticamente, los principios básicos de un método de acuerdo con la presente invención para habilitar la limitación del acceso de servicio. La Fig. 1 está relacionada con una situación en la cual un proveedor de servicio SP ofrece un servicio SR (entre servicios adicionales, como puede ser el caso) y en la que un usuario U intenta registrarse en el servicio SR con el fin de usar el servicio SR. El usuario U posee múltiples identidades digitales I_i que se pueden usar para invocar o registrarse en el servicio SR.

Para acceder al servicio SR, se requiere al usuario U que tenga una cuenta en una entidad de terceros, a la cual se hace referencia en el ejemplo específico tratado como autoridad de registro RA. El usuario U registra sus identidades digitales I_i con la cuenta en la autoridad de registro RA y acuerda un secreto S con la RA. En la Fig. 1, no se muestra la creación de la cuenta del usuario U con la autoridad de registro RA, más bien se supone que la cuenta ya se ha creado en el período previo a la primera solicitud de registro del usuario U con el proveedor del servicio SP.

La autoridad de registro RA garantiza que el usuario U pueda tener solamente una única cuenta o que el usuario U posea al menos solamente un número muy restringido de cuentas. La autorización de solamente una única cuenta se puede realizar requiriendo al usuario U que muestre algún identificador biométrico único al crear la cuenta en la autoridad de registro RA.

Después de la solicitud de registro del usuario U, el proveedor de servicio SP empieza a llevar a cabo un método para habilitar la limitación de acceso de servicio de acuerdo con la presente invención. Más específicamente, el proveedor de servicio SP activa un protocolo con el usuario U al que en lo sucesivo se hará referencia como “protocolo de imposición de límite de registro” y que se describirá con más detalle en conexión con las Figs. 2, 3 y 4. En la Fig. 1 el protocolo de imposición de límite de registro se indica con líneas de puntos. Básicamente, en la forma

de realización específica tratada, el protocolo hace participar al usuario U enviando un mensaje al proveedor de servicio SP y el proveedor de servicio SP involucrándose en un intercambio de mensaje único con la autoridad de registro RA.

Finalmente, dependiendo del resultado del protocolo, el proveedor de servicio SP puede conceder al usuario U el acceso al servicio solicitado (éxito) o el proveedor de servicio SP puede denegar el acceso (error). El proveedor de servicio SP denegará el acceso si resulta que ya se le ha concedido acceso al usuario para un número máximo admisible de veces (el cual se puede especificar basado en las políticas del proveedor de servicio SP).

La Fig. 2 ilustra una primera forma de realización del protocolo de imposición de límite de registro con más detalle. De nuevo se asume que el usuario U posee un número de n identidades digitales diferentes, denotado I_i (con i = 1, …n, con n $\in$ N). Además se asume que el proveedor de servicio SP ofrece un servicio SR al que el usuario U desea registrarse, en el que el proveedor de servicio SP impone un límite lim_{SR} en el servicio SR con respecto al número de identidades diferentes I_i con las cuales un usuario puede invocar o registrarse en el servicio SR. Además se asume que el usuario U ya tiene una cuenta en la autoridad de registro RA con un secreto S y que el usuario U tiene sus identidades digitales I_i registradas con su cuenta de RA. Por consiguiente, la autoridad de registro RA se habilitará para asignar la identidad digital de un usuario I_i a la “identidad real” del usuario o al menos al secreto acordado S.

Antes de iniciar el protocolo, el usuario U tiene que asignar un valor de contador único a cada identidad diferente con la cual intente registrarse con el servicio SR. Los valores de contador se denotan por $k_{i,SR}$. El usuario U debe realizar un seguimiento de las identidades que intenta registrar con el servicio SR. Por ejemplo, el usuario U puede tener las identidades digitales $\{I_1, I_2, I_3, I_4, I_5\}$. Si el usuario U se registra con el servicio SR usando primero I_2, a continuación usando I_4 y, a continuación, usando I_1, a continuación los valores de contador $k_{i,SR}$ pueden tomar los valores $k_{2,SR}$ = 1, $k_{4,SR}$ = 2 y $k_{1,SR}$ = 3. El usuario U (o más precisamente el dispositivo del usuario U empleado para acceder al servicio SR) se requiere para recordar estos valores de contador. Es decir, si el usuario U decide registrarse con (o invocar) el servicio SR de nuevo en el futuro, entonces deberá usar el mismo valor de contador en el protocolo.

Cuando el usuario U envía una solicitud de registro para el servicio SR al proveedor de servicio SP empleando una identidad digital específica I_1. Se recomienda que el usuario U y el proveedor de servicio SP se autentiquen mutuamente ellos mismos antes de inicializar el protocolo de imposición de límite. El mecanismo de autenticación se acopla preferiblemente al identificador de servicio único I_{SR} y la identidad digital empleada I_i. Es decir, se recomienda que el usuario U autentique el identificador de servicio I_{SR} y que el proveedor de servicio SP autentique la identidad digital I_i.

Además, se recomienda que el proveedor de servicio SP y la autoridad de registro RA se autentiquen mutuamente cada una antes de intercambiar los mensajes del protocolo de imposición de límite. En particular, se recomienda que la autoridad de registro RA garantice que ciertamente se comunica con el proveedor de servicio SP que está proporcionando el servicio identificado por el identificador de servicio I_{SR}.

El protocolo de imposición de límite se inicia con el usuario calculando un valor p mediante la aplicación de un algoritmo de codificación H sobre el secreto S y el identificador de servicio único I_{SR}. Con este fin, el secreto S y el identificador I_{SR} se concatenan primero y H se aplica entonces en el resultado concatenado. En el ejemplo específico ilustrado en la Fig. 2, el algoritmo de codificación H es una función de troceo. Posteriormente, el usuario U calcula un valor de verificación v_1 mediante la aplicación del algoritmo de codificación H en el valor p y el valor de contador $k_{i,SR}$ asignado a la identidad digital I_i empleada para la solicitud de servicio, de nuevo concatenando ambos parámetros primero y aplicando H en el resultado concatenado.

El usuario U remite el valor de verificación v_1 al proveedor de servicio SP, junto con la solicitud de registro o en un mensaje independiente, por ejemplo después de la autenticación mutua. El proveedor de servicio SP a su vez proporciona el valor de verificación v_1 – y opcionalmente (tal como se indica entre corchetes) el identificador de servicio único I_{SR} – a la autoridad de registro RA. El identificador único I_{SR} se envía, por ejemplo, en casos en los cuales la autenticación del proveedor de servicio SP con respecto a la autoridad de registro RA no deja claro para qué servicio particular SR está destinada la ejecución del protocolo.

Después de haber recibido el valor de verificación v_1, la reconstrucción del valor de contador $k_{i,SR}$ asignado a la identidad digital I_i empleado para la solicitud de servicio del usuario U en la autoridad de registro RA puede comprender cuatro pasos:

1.) La autoridad de registro RA selecciona un secreto S_n de una lista V_s en la cual se almacenan los secretos de todos los usuarios que tienen una cuenta en la autoridad de registro RA.

2.) La autoridad de registro RA calcula un valor $\overline{p_n}$ mediante la aplicación del algoritmo de codificación H en el secreto escogido S_n y el identificador de servicio único I_{SR} de la misma forma que el usuario U lo hizo anteriormente. En este contexto, se asume que el usuario U y la autoridad de registro RA son conscientes de qué algoritmo específico H se va a aplicar y de cómo se va a aplicar el algoritmo (es decir, cómo introducir los parámetros). Por

ejemplo, es posible que el usuario U posea la información respectiva al crear su cuenta con la autoridad de registro RA.

3.) La autoridad de registro RA intenta reconstruir el valor de verificación v_1 mediante la aplicación del algoritmo de codificación H en el valor $\overline{p_n}$ y un valor λ de la misma forma que el usuario U lo hizo anteriormente, en el que λ es un valor entre 1 y el límite lim_{SR} definido para el servicio SR. La autoridad de registro RA inicia el cálculo con λ=1 e incrementa sucesivamente el valor de λ hasta que se encuentre el valor de verificación correcto v_1 o se alcance el límite lim_{SR}.

4.) En caso de que la autoridad de registro RA no consiga reconstruir correctamente el valor de verificación v_1, se llevarán a cabo repetidamente los pasos de 1.) a 3.) con secretos adicionales S_n tomados de la lista V_s.

Después de haber terminado los cálculos de reconstrucción, la autoridad de registro RA proporciona un mensaje de error en caso de que no se haya encontrado el primer valor de verificación correcto v_1 y proporciona un mensaje satisfactorio en caso de que se haya encontrado v_1. El error de la reconstrucción del valor de verificación v_1 significa que el usuario ha empleado una identidad digital inadmisible I_i cuyo valor de contador asociado $k_{i,SR}$ excede el límite lim_{SR} especificado para el servicio SR. De este modo, tras la recepción del mensaje de error, el proveedor de servicio SP aborta el registro del usuario U y deniega el acceso.

El proveedor de servicio SP mantiene una lista V_{SR} de valores de verificación v_1 que ya se han usado antes con fines de registro. En caso de recibir un mensaje satisfactorio de la autoridad de registro RA, el proveedor de servicio SP comprueba si el valor de verificación v_1 ya es un elemento de la lista V_{SR}. Si el valor v_1 aún no se incluye en la lista V_{SR}, el proveedor de servicio SP añadirá el valor v a la lista V_{SR}. Por otro lado, si el valor de verificación v_1 ya se incluye en V_{SR}, el proveedor de servicio SP sabrá que el usuario U ya se ha registrado antes en el servicio SR con la identidad digital correspondiente. Por consiguiente, el proveedor de servicio SP rechaza la solicitud de registro del usuario U.

Se debe observar que es posible usar el protocolo descrito en conexión con la Fig. 2 como un mecanismo para credenciales anónimas de uso de k. A este respecto, el secreto S se puede derivar en la autoridad de registro RA de una forma casi iterativa tal como se ha descrito más arriba. Alternativamente, se puede emplear cualquier otro mecanismo para recuperar el S correcto.

La Fig. 3 ilustra una segunda forma de realización del protocolo de imposición de límite de registro. El protocolo es bastante similar al protocolo descrito en conexión con la forma de realización mostrada en la Fig. 2. Se denotan los mismos elementos y los mismos parámetros con numerales parecidos. La siguiente descripción se centra en las diferencias con respecto a la forma de realización de la Fig. 2.

De acuerdo con la forma de realización de la Fig. 3, el proveedor de servicio SP proporciona alguna información más a la autoridad de registro RA. Más específicamente, además del valor de verificación v_1, el proveedor de servicio SP remite la identidad digital I_i empleada por el usuario U en conexión con su solicitud de servicio a la autoridad de registro RA. Proporcionando esta información suplementaria, el esfuerzo computacional por parte de la autoridad de registro RA se reduce drásticamente. Debido a la asignación entre las identidades digitales I_i registradas en la autoridad de registro RA para el usuario y el secreto acordado S, la autoridad de registro RA puede derivar directamente el secreto correcto S. En otras palabras, la autoridad de registro RA usa la identidad digital I_i como un índice con el fin de encontrar el secreto S. Por consiguiente, los cálculos para reconstruir el valor de contador $k_{i,SR}$ (asignado a la identidad digital I_i empleada para la solicitud de servicio del usuario) se deben llevar a cabo para un secreto específico solamente. En detalle, la autoridad de registro RA lleva a cabo los siguientes pasos:

1.) La autoridad de registro RA busca el secreto S correspondiente a la identidad digital I_i del usuario U.

2.) La autoridad de registro RA calcula un valor $\overline{p}$ mediante la aplicación del algoritmo de codificación H en el secreto S y el identificador de servicio único I_{SR} de la misma forma que el usuario U lo hizo anteriormente.

3.) La autoridad de registro RA intenta reconstruir el valor de verificación v_1 mediante la aplicación del algoritmo de de codificación H en el valor $\overline{p}$ y un valor λ de la misma forma que el usuario U lo hizo anteriormente, en el que λ es un valor entre 1 y el límite lim_{SR} definido para el servicio SR. La autoridad de registro RA inicia el cálculo con λ=1 e incrementa sucesivamente el valor de λ hasta que se encuentre el valor de verificación correcto v_1 o se alcance el límite lim_{SR}.

El protocolo de acuerdo con la Fig.3 impone una ausencia de seguridad en la que los cálculos por parte de la autoridad de registro RA se basan en dos parámetros – valor de verificación v_1 e identidad digital I_i – que se reciben del proveedor de servicio sin ninguna supervisión. Puede ocurrir que el proveedor de servicio SP intente hacer un

uso incorrecto del protocolo. Por ejemplo, el proveedor de servicio SP puede combinar una identidad de usuario digital I_i recibida en una solicitud de servicio con un valor de verificación v_1 recibido en otra solicitud de servicio con el fin de descubrir si ambas solicitudes de servicio fueron originadas por el mismo usuario. Tal información amenaza la privacidad del usuario U.

La Fig. 4 ilustra una forma de realización del protocolo que es una mejora del protocolo descrito en conexión con la Fig. 3 y el cual elimina la amenaza de privacidad mencionada anteriormente. En esta forma de realización, el usuario U calcula un segundo valor de verificación v_2 mediante la aplicación del algoritmo de codificación H en el valor p, la identidad digital I_i y el primer valor de verificación v_1. Posteriormente, el usuario U remite el segundo valor de verificación v_2 junto con el primer valor de verificación v_1 al proveedor de servicio SP. Posteriormente, el proveedor de servicio SP proporciona el segundo valor de verificación v_2 junto con el primer valor de verificación v_1 y la identidad digital I_i – y opcionalmente la identidad de servicio única I_{SR} – a la autoridad de registro RA.

Después de haber reconstruido correctamente el primer valor de verificación v_1 (correspondiente a una determinación de la validez del valor de contador respectivo $k_{i,SR}$) en la autoridad de registro RA, el segundo valor de verificación v_2 se calcula mediante la aplicación del algoritmo de codificación H en el valor reconstruido p, la identidad digital recibida I_i y el primer valor de verificación recibido v_1 de la misma forma que el usuario U lo hizo anteriormente. Por medio de la comprobación del valor v_2 además del valor v_1 en la autoridad de registro RA, el uso incorrecto mencionado anteriormente del protocolo por parte del proveedor de servicio SP se hace evidente. Proporcionando un mensaje de error al proveedor de servicio SP en caso de que no se haya encontrado un segundo valor de verificación correcto v_2, la autoridad de registro RA puede inhabilitar el abuso del proveedor de servicio SP. No obstante, en caso de que se haya encontrado el segundo valor de verificación correcto v_2, es decir, el primer valor de verificación v_1 y la identidad digital I_i coinciden, la autoridad de registro RA proporciona un mensaje satisfactorio.

Muchas modificaciones y otras formas de realización de la invención establecidas en este documento vendrán a la mente del experto en la materia al cual pertenece la invención teniendo el beneficio de las enseñanzas presentadas en la descripción anterior y los dibujos asociados. Por tanto, ha de entenderse que la invención no se limita a las formas de realización específicas reveladas y que las modificaciones y otras formas de realización están destinadas a incluirse dentro del ámbito de las reivindicaciones anexas. Aunque se han empleado términos específicos en este documento, se usan solamente en un sentido genérico y descriptivo y no con fines de limitación.

REIVINDICACIONES

1. Método para habilitar la limitación de acceso de servicio, en el que un proveedor de servicio (SP) ofrece al menos un servicio (SR) y en el que un usuario (U) posee múltiples identidades digitales diferentes I_i que se pueden usar para invocar o registrarse con dicho servicio (SR),

acceder a dicho servicio (SR) requiriendo una cuenta en una entidad de terceros, en la que el usuario (U) registra sus identidades digitales I_i con dicha cuenta y en la que el usuario (U) acuerda un secreto S con dicha entidad de terceros, comprendiendo el método los pasos de:

el usuario (U) asignando a sus identidades digitales diferentes I_i valores de contador únicos $k_{i,SR}$,

el usuario (U) solicitando dicho servicio (SR) empleando una identidad digital específica I_i y calculando un valor de verificación – primer valor de verificación v_1 – mediante la aplicación de un algoritmo de codificación H en dicho secreto S y dicho valor de contador $k_{i,SR}$ asignado a la identidad digital I_i empleada para dicha solicitud de servicio,

dicha entidad de terceros recibiendo dicho primer valor de verificación v_1, aplicando dicho algoritmo de codificación H para reconstruir dicho valor de contador empleado $k_{i,SR}$ y proporcionando información de si el valor de contador reconstruido $k_{i,SR}$ excede un límite lim_{SR},

en el que dicho proveedor de servicio (SP) mantiene una lista V_{SR}, en la cual los primeros valores de verificación v_1 recibidos del usuario (U) se incluyen y en la que dicho proveedor de servicio (SP) aborta el registro del usuario (U) con dicho servicio (SR) en caso de que una comprobación revele que dicho primer valor de verificación reconstruido correctamente v_1 ya es un elemento de dicha lista V_{SR}.

2. Método de acuerdo con la reivindicación 1, en el que dicho servicio (SR) ha asociado un identificador de servicio único I_{SR} para la identificación de dicho servicio (SR) en dicha entidad de terceros.

3. Método de acuerdo con la reivindicación 2, en el que dicho identificador de servicio I_{SR} se incluye en una cadena de bits que incluye adicionalmente la URL (Localizador de Recursos Uniforme) de dicho servicio (SR) y/o dicho límite lim_{SR} y/o un identificador para el ejemplo de servicio concreto y/o un valor de marca de tiempo y/o un certificado de clave pública o cadena de certificado para dicho proveedor de servicio (SP) y/o dicho servicio (SR).

4. Método de acuerdo con cualquiera de las reivindicaciones de 1 a 3, en el que dicha entidad de terceros es una autoridad de registro (RA).

5. Método de acuerdo con cualquiera de las reivindicaciones de 1 a 4, en el que dicha entidad de terceros garantiza que dicho usuario (U) posee solamente un número limitado de cuentas o en el que dicha entidad de terceros garantiza que dicho usuario (U) no puede tener más de una cuenta, preferiblemente requiriendo a dicho usuario (U) que muestre alguna identificación biométrica única antes de crear dicha cuenta en dicha entidad de terceros.

6. Método de acuerdo con cualquiera de las reivindicaciones de 1 a 5, en el que dicho algoritmo de codificación H es una función unidireccional determinista, y/o en el que dicho algoritmo de codificación H es una función de troceo.

7. Método de acuerdo con cualquiera de las reivindicaciones de 1 a 6, en el que dicho secreto S se genera aleatoriamente.

8. Método de acuerdo con cualquiera de las reivindicaciones de 1 a 7, en el que dicho usuario (U), en el contexto de acceder a dicho servicio (SR), calcula un valor p mediante la aplicación del algoritmo de codificación H en dicho secreto S y dicho identificador de servicio I_{SR}, en el que dicho usuario (U) puede calcular dicho primer valor de verificación v_1 mediante la aplicación del algoritmo de codificación H en dicho valor p y dicho valor de contador $k_{i,SR}$.

9. Método de acuerdo con cualquiera de las reivindicaciones de 1 a 8, en el que dicho usuario (U) remite dicho primer valor de verificación v_1 a dicho proveedor de servicio (SP), y/o en el que dicho proveedor de servicio (SP) proporciona dicho primer valor de verificación v_1 preferiblemente junto con dicho identificador de servicio I_{SR} a dicha entidad de terceros.

10. Método de acuerdo con la reivindicación 8 ó 9, en el que dicha entidad de terceros, tras la recepción de dicho valor de verificación v_1, empieza a reconstruir el valor de contador $k_{i,SR}$ asignado a la identidad digital I_i que dicho usuario (U) ha empleado para dicha solicitud de servicio, llevando a cabo los pasos de:

selección de un secreto S_n de una lista V_s de secretos asignada por dicha entidad de terceros,

cálculo de un valor $\overline{p_n}$ mediante la aplicación de dicho algoritmo de codificación H en dicho secreto escogido S_n y dicho identificador de servicio I_{SR} de la misma forma que lo hizo el usuario (U),

selección de un número entero λ entre 1 y dicho límite lim_{SR}, aplicando dicho algoritmo de codificación H en dicho valor $\overline{p_n}$ y dicho λ de la misma forma que lo hizo dicho usuario (U),

variación sucesivamente de dicho número escogido λ y dicho secreto escogido S_n hasta que el resultado se corresponda con el primer valor de verificación recibido v_1.

11. Método de acuerdo con cualquiera de las reivindicaciones de 8 a 10, en el que dicha entidad de terceros, después de la recepción tanto del valor de verificación v_1 como de la identidad digital I_i, inicia la reconstrucción del valor de contador $k_{i,SR}$ asignado a la identidad digital I_i que dicho usuario (U) ha empleado para dicha solicitud de servicio, llevando a cabo los pasos de:

búsqueda de dicho secreto S correspondiente a dicha identidad digital I_i,

cálculo de un valor $\overline{p}$ mediante la aplicación de dicho algoritmo de codificación H en dicho secreto S y dicho identificador de servicio I_{SR} de la misma forma que lo hizo dicho usuario (U), escogiendo un número entero λ entre 1 y dicho límite lim_{SR}, aplicando dicho algoritmo de codificación H en dicho valor $\overline{p}$ y dicho λ de la misma forma que lo hizo dicho usuario (U),

variación sucesivamente de dicho número escogido λ hasta que el resultado se corresponda con el primer valor de verificación recibido v_1.

12. Método de acuerdo con cualquiera de las reivindicaciones de 8 a 11, en el que dicho usuario (U) calcula un valor de verificación adicional – segundo valor de verificación v_2 – mediante la aplicación de dicho algoritmo de codificación H en dicho valor p, dicha identidad digital empleada I_i y dicho primer valor de verificación v_1, en el que dicho usuario (U) puede remitir dicho segundo valor de verificación v_2 a dicho proveedor de servicio (SP) y/o en el que dicho proveedor de servicio (SP) puede proporcionar dicho segundo valor de verificación v_2 a dicha entidad de terceros.

13. Método de acuerdo con la reivindicación 12, en el que dicha entidad de terceros, después de haber reconstruido correctamente dicho valor de contador $k_{i,SR}$ mediante la búsqueda del primer valor de verificación correcto v_1, comienza aplicando dicho algoritmo de codificación H en dicho valor $\overline{p}$, dicha identidad digital I_i y dicho primer valor de verificación v_1 de la misma forma que lo hizo dicho usuario (U), para reconstruir dicho segundo valor de verificación v_2,
en el que dicha entidad de terceros puede proporcionar un mensaje satisfactorio en caso de que se haya encontrado el segundo valor de verificación correcto v_2 y puede proporcionar un mensaje de error en caso de que no se haya encontrado ningún segundo valor de verificación correcto v_2.

14. Método de acuerdo con cualquiera de las reivindicaciones de 1 a 13, en el que dicha entidad de terceros está en línea solamente por un tiempo limitado.

15. Método de acuerdo con cualquiera de las reivindicaciones de 1 a 14, en el que dicho límite lim_{SR} lo predefine el proveedor de servicio (SP) en sí mismo o cualquier instancia externa y/o

en el que dicho límite lim_{SR} está sujeto a variaciones dependiendo de los parámetros dinámicos.

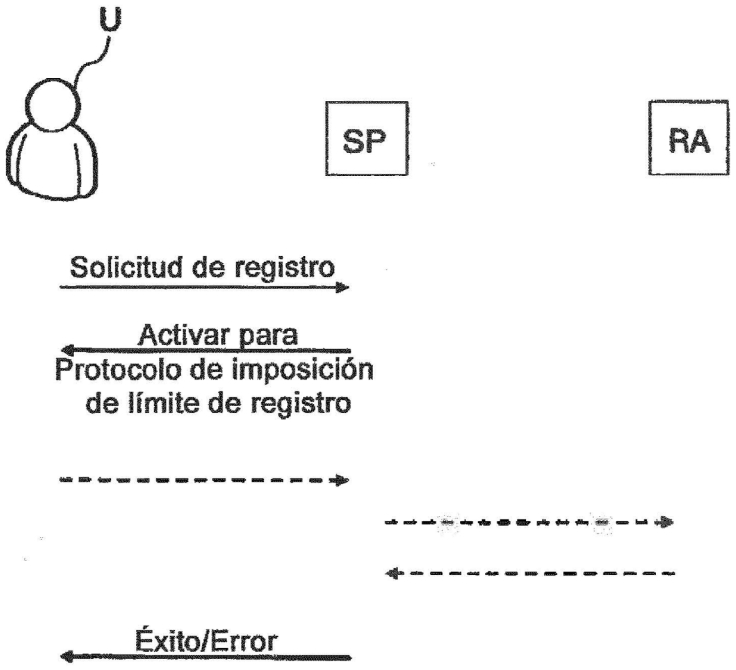
U
SP
RA
Solicitud de registro
Activar para
Protocolo de imposición
de límite de registro
Éxito/Error

Fig. 1

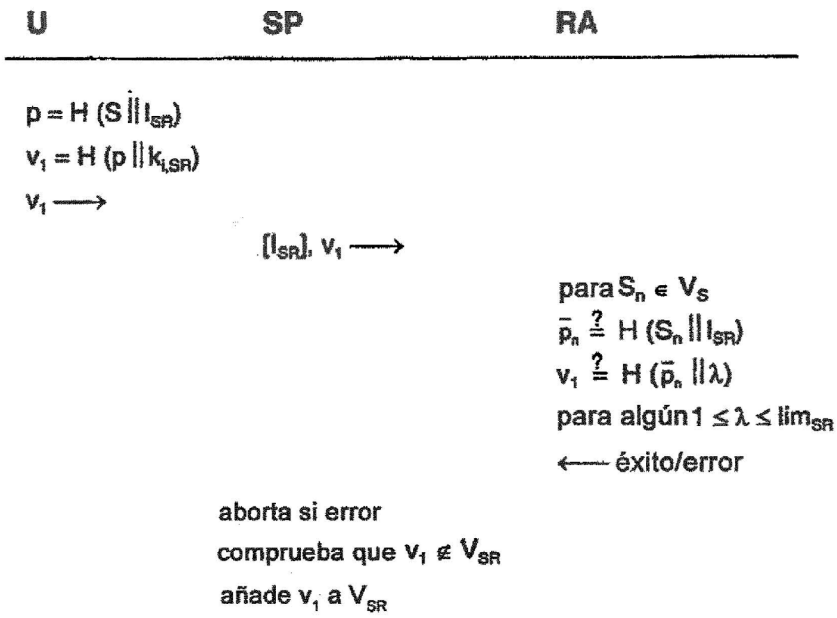
U
SP
RA
p = H (S || I_SR)
v_1 = H (p || k_i,SR)
v_1 ⟶
[I_SR], v_1 ⟶
para S_n ∈ V_S
p̄_n ≟ H (S_n || I_SR)
v_1 ≟ H (p̄_n || λ)
para algún 1 ≤ λ ≤ lim_SR
⟵ éxito/error
aborta si error
comprueba que v_1 ∉ V_SR
añade v_1 a V_SR

Fig. 2

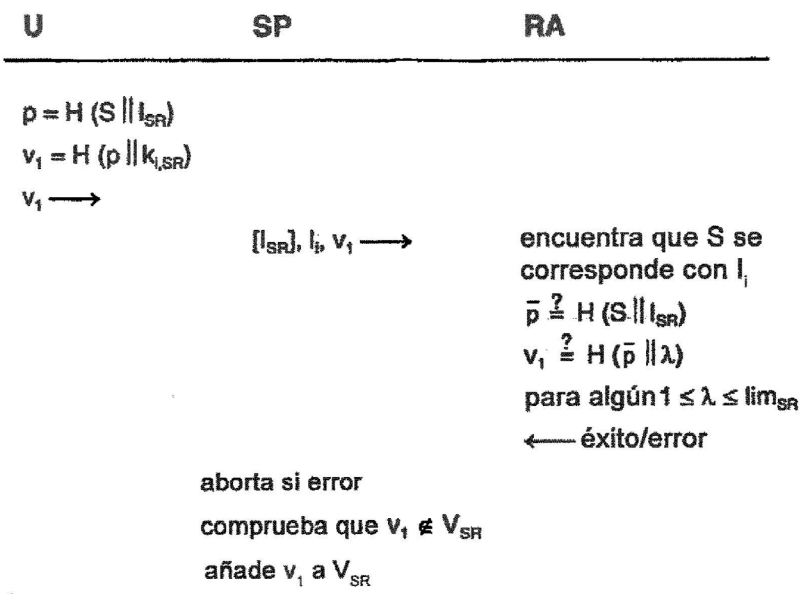
U
SP
RA
p = H (S || I_{SR})
v_1 = H (p || $k_{i,SR}$)
v_1 ⟶
[I_{SR}], I_i, v_1 ⟶
encuentra que S se corresponde con I_i
$\bar{p} \stackrel{?}{=}$ H (S || I_{SR})
$v_1 \stackrel{?}{=}$ H ($\bar{p}$ || λ)
para algún 1 ≤ λ ≤ lim_{SR}
⟵ éxito/error
aborta si error
comprueba que $v_1 \notin V_{SR}$
añade v_1 a V_{SR}

Fig. 3

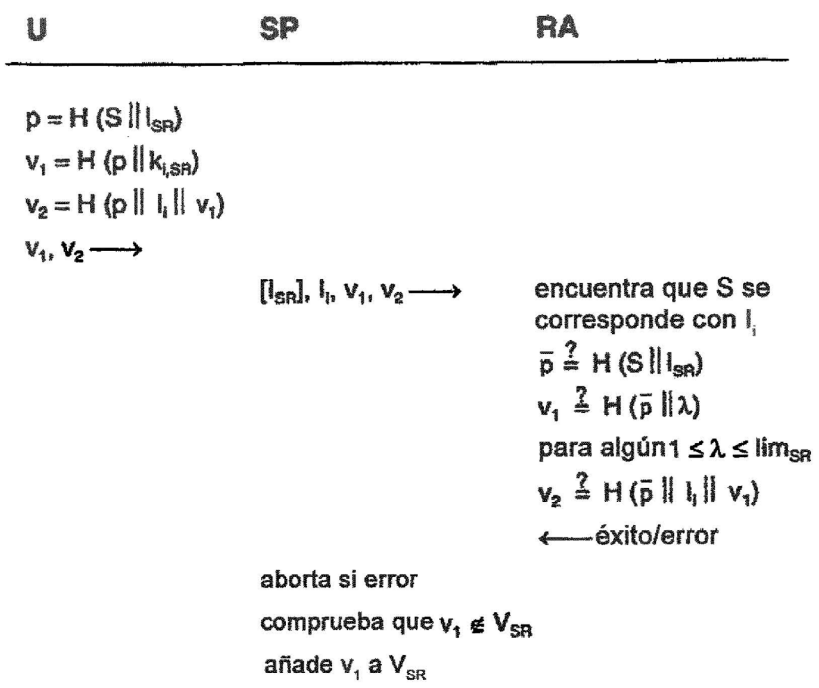
U
SP
RA
p = H (S || I_SR)
v_1 = H (p || k_i,SR)
v_2 = H (p || I_i || v_1)
v_1, v_2 ⟶
[I_SR], I_i, v_1, v_2 ⟶
encuentra que S se corresponde con I_i
p̄ ≟ H (S || I_SR)
v_1 ≟ H (p̄ || λ)
para algún 1 ≤ λ ≤ lim_SR
v_2 ≟ H (p̄ || I_i || v_1)
⟵ éxito/error
aborta si error
comprueba que v_1 ∉ V_SR
añade v_1 a V_SR

Fig. 4