(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 810 148**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04L 29/06 (2006.01)
G06F 21/34 (2013.01)
G06F 21/62 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **09.07.2012 PCT/EP2012/063399**

(87) Fecha y número de publicación internacional: **17.01.2013 WO13007686**

(96) Fecha de presentación y número de la solicitud europea: **09.07.2012 E 12738071 (5)**

(97) Fecha y número de publicación de la concesión europea: **17.06.2020 EP 2730050**

(54) Título: **Procedimiento para la generación y verificación de una firma seudónima electrónica**

(30) Prioridad:

08.07.2011 DE 102011107501

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.03.2021

(73) Titular/es:

BUNDESREPUBLIK DEUTSCHLAND, VERTRETEN DURCH DAS BUNDESMINISTERIUM DES INNEREN, VERTRETEN DURCH DAS BUNDESAMT FÜR SICHERHEIT IN DER (100.0%)
Godesberger Allee 185-189
53175 Bonn, DE

(72) Inventor/es:

KÜGLER, DENNIS

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento para la generación y verificación de una firma seudónima electrónica

La invención se refiere a un procedimiento para el uso en la comunicación entre un generador y un receptor y a una tarjeta chip para la firma seudónima electrónica.

Las firmas electrónicas son ampliamente conocidas. Se basan en procedimientos criptográficos asimétricos. Para la generación de firma se usa una clave privada, la cual es conocida únicamente por el titular de la clave de firma. Para la verificación de firma sirve una clave pública correspondiente a la clave privada. La clave pública se autentifica por regla general por parte de una instancia fiable, la cual relaciona a través de un certificado la identidad del titular del par de claves con la clave pública. El certificado se incorpora entonces en directorios públicos, de modo que cada firma generada con la clave puede asignarse inequívocamente al titular de la clave y cualquiera con acceso al directorio puede comprobar la validez de la firma. Un ejemplo de una infraestructura de este tipo es la *"qualifizierte elektronische Signatur"* (firma electrónica cualificada) de acuerdo con la *Signaturgesetz* (ley de firmas) alemana.

De la *Technische Richtlinie* (directriz técnica) BSI TR-03110 se conoce un procedimiento para el intercambio de datos anónimo entre un generador (por ejemplo usuario de una tarjeta chip) y un receptor (por ejemplo proveedor de servicios). En el procedimiento se usa por parte del generador un seudónimo. Al generador hay asignadas una clave pública y una estática privada. Los pasos son:

- el generador obtiene la identidad del receptor,
- el generador calcula un seudónimo a partir de su clave privada y la identidad del receptor,
- el generador transmite el seudónimo al receptor,
- el receptor comprueba mediante el seudónimo si la tarjeta chip está registrada o bloqueada.

De acuerdo con la directriz se trata en el caso de las tarjetas chip de documentos soberanos, formando parte de los mismos un documento de identidad.

El procedimiento mencionado anteriormente se describe a continuación en detalle:

- en el caso del procedimiento no se trata de una firma electrónica. Un generador y un receptor de una firma por lo tanto no existen. Por esta razón se habla en lo sucesivo de un “usuario” en lugar del generador y de un “proveedor de servicios” en lugar del receptor.
- se genera un seudónimo inequívoco entre un proveedor de servicios, el cual ofrece un servicio electrónico, y un usuario, el cual usa o recurre a este servicio. Este seudónimo permite al proveedor de servicios asignar la tarjeta chip, es decir, el usuario, de forma inequívoca, también cuando no esté permitida la lectura o lo esté solo de unos pocos datos relativos a la persona a partir de la tarjeta chip. El proveedor de servicios puede comprobar además de ello a través de este seudónimo inequívoco si la tarjeta de chip ha sido notificada como bloqueada. El procedimiento asegura además de ello, que los proveedores de servicios no puedan vincular entre sí entre ellos los seudónimos. Dos o más proveedores de servicios no pueden comprobar mediante el seudónimo si han comunicado con la misma tarjeta chip. Esta es una de las características esenciales del uso de seudónimos.
- El usuario dispone por ejemplo como tarjeta chip, de un documento de identidad, en el cual hay memorizados datos relativos a la persona y una identificación específica de tarjeta, secreta. La tarjeta de chip dispone además de ello de un par de claves para la autentificación, así como de un certificado de autenticidad correspondiente, el cual fue expedido por el emisor de la tarjeta chip. A través de este certificado y la clave de autentificación privada correspondiente la tarjeta de chip puede identificarse con respecto a los proveedores de servicios como tarjeta de chip auténtica y establecer un canal seguro con el proveedor de servicios, de modo que los datos referidos a la persona pueden ser transmitidos de forma confidencial y auténtica.
- El proveedor de servicios obtiene igualmente un par de claves y un certificado de autorización correspondiente. El certificado de autorización indica qué datos referidos a la persona puede solicitar un proveedor de servicios a la tarjeta chip. El certificado de autorización comprende además de ello una identificación inequívoca, la cual es otorgada por el organismo de certificación.

Los pasos detallados del procedimiento son:

- el proveedor de servicios se autentifica con respecto a la tarjeta chip del usuario con su certificado de autorización y la clave privada correspondiente. La tarjeta chip comprueba la autentificación y valida el certificado de autorización del proveedor de servicios.

- La tarjeta chip se autentifica con respecto al proveedor de servicios como tarjeta chip auténtica y establece a este respecto una comunicación segura, es decir, codificada y asegurada en integridad. El proveedor de servicios comprueba la autentificación y valida el certificado de autenticidad de la tarjeta chip.

- La tarjeta chip extrae la identidad del proveedor de servicios del certificado de autorización y calcula junto con la identidad de tarjeta chip secreta el seudónimo y envía el mismo a través del canal seguro al proveedor de servicios.

- El proveedor de servicios puede comprobar mediante el seudónimo si la tarjeta chip está registrada en el proveedor de servicios y si la tarjeta chip está bloqueada. En caso de no estar aún registrada la tarjeta chip, el proveedor de servicios puede leer datos adicionales relativos a la persona en correspondencia con el permiso en el certificado de autorización y de este modo registrar la tarjeta chip con el seudónimo.

Dado que la *Technische Richtlinie* (directriz técnica) BSI TR-03110 no se refiere a ningún procedimiento de firma, tiene validez lo siguiente:

- la tarjeta chip genera el seudónimo sin probar que la generación es correcta. El cálculo correcto del seudónimo se presupone, dado que la tarjeta chip se ha autentificado anteriormente como tarjeta chip auténtica con respecto al proveedor de servicios. La tarjeta chip ha de autentificarse antes de la solicitud del seudónimo con respecto al proveedor de servicios como tarjeta chip auténtica y establecer un canal seguro. Sin este paso adicional no queda asegurado que el seudónimo realmente haya sido generado por la tarjeta chip. Una tarjeta chip manipulada podría hacerse pasar fácilmente por otra tarjeta chip y quedaría comprometida la seguridad del sistema. Esta autentificación adicional identifica la tarjeta chip o bien de forma inequívoca al usarse una clave de tarjeta chip individual. O bien, cuando una pluralidad de tarjetas chip usa la misma clave de autentificación, resulta el problema de la revocación de tarjetas de chip individuales al comprometerse la clave común.

- El seudónimo es únicamente una identificación específica de zona de la tarjeta chip. Falta la posibilidad de autentificar transacciones a través de la tarjeta chip. El seudónimo permite al proveedor de servicios reconocer la tarjeta chip, no permite sin embargo documentar de manera comprobable declaraciones de voluntades del usuario mediante la tarjeta con el seudónimo, por ejemplo la suposición de condiciones generales del proveedor de servicios, o la votación comprobable bajo el seudónimo en un sistema de votación.

De la bibliografía se conocen diferentes procedimientos para la generación de una firma electrónica. Son habituales firmas digitales, en cuyo caso a cada generador de firma se le asigna un par de claves individual, propio, consistente en una clave de firma privada estática y una clave de comprobación de firma pública estática. Mediante esta asignación inequívoca de la clave de comprobación de firma pública estática cada receptor de firmas puede comprobar que una firma ha sido generada por un determinado generador. También se conocen de la bibliografía firmas grupales, en cuyo caso hay asignada respectivamente a un grupo de generadores de firma la misma clave de firma pública estática (denominada clave grupal), pero cada uno de los firmantes tiene una clave de firma privada propia. En el caso de una firma grupal la firma se refiere únicamente al grupo, sin embargo no a un miembro del grupo determinado. Tampoco existe ninguna posibilidad de comprobar si dos firmas fueron generadas por el mismo miembro del grupo o por diferentes miembros del grupo.

Del documento WO-A-2010/034 507 se conoce un procedimiento para la firma electrónica, seudónima, entre un generador y un receptor, de tal modo que

- el generador presenta una tarjeta chip,

- el generador es un miembro de grupo,

- a cada miembro de grupo hay asignada una misma clave grupal pública,

- a cada miembro de grupo hay asignada una clave privada individual,

- el receptor de la firma presenta una identidad,

- el procedimiento presenta los siguientes pasos:

a) el generador recibe la identidad del receptor,

b) el generador calcula un seudónimo a partir de su clave privada propia y la identidad del receptor,

c) el generador calcula una firma para el seudónimo,

d) el generador transmite la firma al receptor,

e) el receptor comprueba el seudónimo con la firma y la clave grupal pública (y no la firma con la clave grupal pública y el seudónimo).

Debido a que la comprobación del seudónimo únicamente se verifica a través de la corrección de la firma, resulta en el procedimiento conocido la desventaja de que una tarjeta chip manipulada pueda calcular un seudónimo falso.

La invención se basa en la tarea de lograr un procedimiento para la generación y verificación de una firma seudónima electrónica para el intercambio de datos (en particular anónimo) entre un generador (por ejemplo un usuario de una tarjeta chip) y un receptor (por ejemplo un proveedor de servicios), que sea sencillo y seguro y pueda usarse polifacéticamente.

La solución a esta tarea resulta de las características de las reivindicaciones 1 a 11 adjuntas.

Para la solución de esta tarea se propone con la invención un procedimiento para la generación y verificación de una firma seudónima electrónica para el uso en la comunicación entre un generador y un receptor, siendo el generador miembro de un grupo de generadores, de los cuales a cada uno hay asignada una clave grupal (y) pública estática igual y una clave (x_1, x_2) privada estática propia y presentando el receptor una identidad (R) y donde en el procedimiento

- el generador recibe del receptor su identidad (R),
- el generador calcula a partir tanto de su clave (x_1, x_2) privada propia o una parte de ella, como también de la identidad (R) del receptor, al menos un seudónimo (I_R),
- el generador calcula mediante el uso del seudónimo (I_R) una firma seudónima electrónica (I_R, c, s_1, s_2),
- el generador transmite la firma seudónima electrónica (I_R, c, s_1, s_2) al receptor y
- el receptor verifica la firma seudónima electrónica (I_R, c, s_1, s_2) del generador mediante su clave grupal (y) pública, así como su propia identidad (R) (lo cual significa que la verificación de firma falla cuando el seudónimo es incorrecto).

Es un aspecto esencial de la invención que el seudónimo se genera de forma verificable a partir de la misma clave privada, así como la firma y con ello el seudónimo y firma están unidos entre sí de forma inseparable. De ello resulta la ventaja de que la verificación de firma solo tiene éxito cuando el seudónimo fue generado correctamente.

Las ventajas de la invención se basan en que en lugar del cálculo único de un seudónimo se presenta un procedimiento de firma nuevo.

- En este procedimiento de firma hay asignada a cada miembro de grupo una misma clave grupal pública. Hay asignada además de ello a cada miembro de grupo una clave privada propia. Además de ello las firmas generadas por los miembros de grupo son con respecto al receptor (de firma) fijado, seudónimas. Esto significa que cada receptor (de firma) puede comprobar si una firma fue generada por el mismo miembro de grupo. Un encadenamiento de seudónimos, los cuales fueron dados a dos diferentes receptores (de firma), queda sin embargo excluido.
- Debido a la firma adicional el receptor (por ejemplo proveedor de servicios), puede comprobar por ejemplo a través de un procedimiento de reto/respuesta, que el seudónimo fue generado realmente por el generador (por ejemplo la tarjeta chip) usando la clave privada correspondiente. Una autentificación previa del generador (de la tarjeta chip) mismo puede de este modo suprimirse. Dado que cada generador (cada tarjeta chip) dispone de su propia clave privada, un compromiso de esta una clave tiene efectos menores.
- El generador (por ejemplo usuario de la tarjeta chip) puede entregar además de ello a través de la firma una declaración de voluntades bajo el seudónimo y autentificar de este modo una transacción frente al proveedor de servicios.

Es desconocida hasta ahora una firma seudónima, tal como se propone de acuerdo con la invención, es decir, un procedimiento de firma, que ha de emplazarse entre una firma digital individual y una firma grupal. Análogamente a la firma grupal se representa en el caso de la firma seudónima de acuerdo con la invención, el grupo de los firmantes (el decir, el generador) mediante una clave grupal estática común. Además de ello, cada miembro del grupo dispone de una clave estática privada individual. Adicionalmente se asigna a cada receptor una identidad inequívoca. Durante la generación de firma se calcula a partir de la clave privada individual del firmante y de la identidad del receptor de la firma, un seudónimo inequívoco como componente de la firma, de manera que durante la verificación de firma por parte del receptor de firma autorizado puede comprobarse la corrección de la firma incluido el seudónimo con la ayuda de la clave grupal. Debido a ello resulta la ventaja de que el firmante puede ser reconocido inequívocamente a través del seudónimo. Como consecuencia de ello el receptor de la firma puede comprobar si dos firmas fueron generadas por el mismo generador o por diferentes generadores. Dos diferentes receptores de firma no pueden sin embargo comprobar si dos firmas fueron generadas por el mismo generador, dado que la formación de seudónimo es dependiente de la identidad del receptor. Una ventaja particular resulta de la generación

de firma con el seudónimo de acuerdo con la invención, en cuanto que mediante el proceso de firma se asegura que tanto seudónimo, como también firma, fueron generados con la misma clave de firma privada. Debido a ello el receptor de firma puede asegurar tras comprobación de la firma con la clave grupal y el seudónimo, que el seudónimo se generó correctamente. De otro modo la firma no sería verificable.

La invención presenta la gran ventaja de que los esfuerzos de cálculo para la generación y la verificación de una firma seudónima son esencialmente menores que en el caso de una firma grupal, dado que el paso, en el cual el generador calcula una firma con el seudónimo, se produce como prueba simultánea del conocimiento de la clave privada propia.

Las diferencias de la invención con respecto a los procedimientos conocidos de acuerdo con WO-A-2010/034 507 son las siguientes:

- el generador calcula una firma con el seudónimo y no, tal como en el procedimiento conocido, una firma para el seudónimo. Mediante la generación de firma de acuerdo con la invención con seudónimo, resulta una ventaja particular debido a que mediante el procedimiento de firma se asegura que tanto el seudónimo, como también la firma, fueron generados con la misma clave de firma privada. A diferencia de ello se genera en el procedimiento conocido un seudónimo por parte del firmante y se autentifica mediante una firma (grupal). Mediante la separación de formación de seudónimo y firma, tal como es el caso en el procedimiento conocido, las manipulaciones por parte del firmante no pueden ni excluirse ni reconocerse.

- En la invención el receptor comprueba la firma con la clave grupal pública y el seudónimo, y no como en el caso del procedimiento conocido, el seudónimo con la firma y la clave grupal pública. Debido a ello resulta la ventaja particular de que el receptor de la firma tras comprobación de la firma con la clave grupal puede asegurar que el seudónimo fue generado correctamente o expresado de otro modo: la comprobación de la firma da error cuando el seudónimo no se generó correctamente. De lo contrario la firma no sería verificable. A diferencia de ello se determina en el procedimiento conocido un seudónimo solo por parte del firmante y se autentifica mediante una firma (grupal).

- El paso, en el cual el generador calcula una firma con el seudónimo, se produce como prueba simultánea del conocimiento de la clave privada propia. Esta característica no encuentra modelo en el procedimiento conocido. Con el procedimiento de acuerdo con la invención se da lugar a una implementación eficiente. El cálculo de una firma seudónima puede producirse de manera particularmente eficiente cuando la generación de firma no comprende solo la generación del seudónimo, sino que incluye (simultáneamente) la comprobación de la corrección del seudónimo. En comparación con el procedimiento conocido es posible de este modo un claro aumento de la eficiencia. En el procedimiento conocido se requiere una firma grupal para la anonimización del firmante, que conlleva esfuerzos de cálculo notables.

De manera conveniente se establece la firma seudónima electrónica (I_R, c, s_1, s_2) basándose en el cálculo de una firma Schnorr.

Puede estar previsto además de ello adicionalmente que el receptor se autentifique con respecto al generador mediante un certificado de autorización certificado por una tercera parte, que comprende la identidad (R) del receptor y que el generador compruebe la autentificación, así como el certificado de autorización y extraiga del certificado de autorización la identidad (R) del receptor.

Se indica que el generador presenta por ejemplo una tarjeta chip o un servidor y/o que el receptor es por ejemplo un proveedor de servicios.

En otra configuración ventajosa de la invención se usa para la generación de la firma seudónima electrónica un grupo matemático criptográficamente seguro, por ejemplo escrito multiplicativa o aditivamente, con entre otros un generador criptográfico (g_1) y una función Hash.

Otro aspecto de la invención se refiere al caso de que cada receptor de una firma seudónima electrónica compara los seudónimos generados por un generador de un grupo con introducciones de seudónimo de una lista negra o lista blanca, para comprobar si el generador está autorizado para generar una firma seudónima electrónica usando su clave estática privada y la clave grupal estática pública. Este aspecto de la invención tiene importancia independiente. Es decir, que estos pasos de procedimiento forman independientemente de los otros pasos de procedimiento descritos aquí y en lo sucesivo, un aspecto inventivo autónomo.

En el caso del aspecto descrito anteriormente puede estar previsto en particular que para cualquier posible receptor se alisten todos los seudónimos válidos en una lista blanca y que un receptor de este tipo compruebe antes de la verificación de la firma seudónima electrónica que el seudónimo está contenido en la lista blanca.

Es concebible además de ello, que para cada posible receptor se alisten todos los seudónimos bloqueados en una lista negra y que un receptor de este tipo compruebe antes de la verificación de la firma seudónima que el seudónimo no está contenido en la lista negra.

De acuerdo con una configuración de la invención el paso, en el cual el generador calcula una firma con el seudónimo, se produce como prueba simultánea del conocimiento de la clave privada propia. Mediante esta prueba se comprueba simultáneamente que la clave privada propia se usó tanto para la generación del seudónimo, como también para la generación de la firma seudónima. Debido a ello las dos operaciones están unidas entre sí de forma no separable y la firma está ligada el seudónimo, de manera que éstos no pueden separarse entre sí. Mediante la prueba simultánea resulta además de ello también una implementación eficiente, dado que la generación correcta del seudónimo no ha de probarse por separado.

De acuerdo con otra configuración de la invención el receptor comprueba con la ayuda del seudónimo mediante una lista negra o lista blanca si la tarjeta chip es válida. Una lista negra contiene seudónimos bloqueados, siendo todos los demás seudónimos válidos. Una lista blanca contiene los seudónimos válidos, todos los demás seudónimos están bloqueados. Cual de los dos tipos de lista se usa puede depender de cuantos seudónimos estén bloqueados. A través de una comprobación de lista blanca, incluso en caso de compromiso de la clave grupal pública igual para todos los miembros del grupo, puede mantenerse la seguridad del procedimiento.

Un ejemplo de realización de la invención se explica a continuación con mayor detalle mediante el dibujo. El dibujo ilustra un procedimiento para la generación y verificación de una firma seudónima electrónica para la comunicación en particular anónima entre un generador y un receptor.

En el dibujo se representa en primer lugar una tarjeta chip. Esta tarjeta chip está asignada a un generador de una firma. El generador de la firma es una persona y la tarjeta chip es un documento de identidad. En esta tarjeta chip está memorizada una clave privada (x_1, x_2) propia para la generación de firmas y seudónimos. La clave privada (x_1, x_2) propia es una tupla. La tarjeta chip pertenece a una generación de tarjetas chip, las cuales presentan todas una clave grupal y pública común. La clave grupal y pública se usa para la verificación de firmas y seudónimos. Una generación de tarjetas chip pueden ser aquellas tarjetas chip, las cuales se producen en un espacio temporal de tres meses. En este caso las tarjetas chip de una generación son los miembros del grupo.

El receptor de una firma es un proveedor de servicios. El proveedor de servicios es en el ejemplo de realización un centro electoral. El receptor tiene una identidad, la cual está contenida en un certificado de autorización. Un mensaje a firmar puede ser por ejemplo una papeleta de votación electrónica.

La tarjeta chip comprende un microordenador con una memoria de microordenador. En la memoria de microordenador hay memorizado un primer programa de ordenador, el cual está configurado de tal modo que puede llevarse a cabo un procedimiento para la firma seudónima en relación con el generador. La implementación del primer programa de ordenador en la memoria de microordenador se produjo mediante el uso de un primer producto de programa de ordenador.

Al receptor hay asignado un computador con una memoria de computador. En la memoria de computador hay memorizado un segundo programa de ordenador, el cual está configurado de tal modo que puede llevarse a cabo el procedimiento en relación con el generador. La implementación del segundo programa de ordenador en la memoria de computador se produjo mediante el uso de un segundo producto de programa de ordenador.

La tarjeta chip del generador se lee en un lector de tarjetas y está en contacto a través de Internet con el computador del receptor.

Instalación

En el dibujo se indica un emisor de la tarjeta chip. El emisor de la tarjeta chip selecciona parámetros adecuados para el procedimiento matemático de base, de acuerdo con el cual se genera la firma electrónica, es decir, por ejemplo una curva elíptica o un cuerpo primario. Los parámetros consisten al menos en el generador (generador criptográfico) g_1, la magnitud q (denominado también orden) del grupo matemático generado de este modo (denominado en lo sucesivo también estructura), así como en una descripción de la operación que puede llevarse a cabo en él (multiplicación o adición, en el ejemplo de realización se usa la multiplicación). El emisor selecciona un número aleatorio $z \in_R Z_q$ secreto y determina un generador adicional (generador criptográfico) $g_2 = g_1^z$. Los parámetros del grupo criptográfico y del generador adicional g_2 se publican, el valor z es mantenido en secreto por el emisor de la tarjeta chip.

Generación de clave para miembros de grupo

A cada miembro de grupo hay asignado un par de claves, consistente en una clave grupal pública igual $y = g_1^{x_1} \cdot g_2^{x_2}$ y en una clave privada propia (x_1, x_2). La cantidad de las claves privadas posibles se determina a partir de la magnitud de la estructura matemática seleccionada. Por esta razón existe en el caso de una estructura con una magnitud q también q diferentes claves. Normalmente g es un número primo con al menos una longitud de 200 bits. Para la generación de varias claves privadas, el emisor de la tarjeta chip selecciona en primer lugar un par de claves fijo (x, $y = g_1^z$). A continuación se genera para cada miembro del grupo una clave privada propia de la siguiente manera: el valor $x_2 \in_R Z_q$ es seleccionado aleatoriamente por parte del emisor de la tarjeta chip para cada tarjeta chip y a continuación se calcula el valor $x_1 = x - z \cdot x_2$. Dado que $x = x_1 + z \cdot x_2$, puede calcularse a partir de

respectivamente dos claves privadas diferentes (x_1, x_2) y (x'_1, x'_2) el número aleatorio $z = \frac{x_1 - x_1'}{x_2 - x_2'}$ secreto. Por esta razón han de memorizarse las claves privadas de forma segura en la tarjeta chip. El emisor de la tarjeta chip calcula además de ello la identidad de bloqueo $S = g_1^{x_1}$ del miembro de grupo y conduce al mismo al servicio de bloqueo. El servicio de bloqueo es en el ejemplo de realización también el emisor de la tarjeta chip.

Registro de receptores

Cada proveedor de servicios registrado se caracteriza por una identidad inequívoca $R = g_1^{x_R}$. Las identidades de receptor son calculadas por el emisor de la tarjeta chip. Las identidades de receptor *R* se publican. Los valores x_R correspondientes han de continuar desconocidos para los receptores y se transmiten al servicio de bloqueo.

Procedimiento para la firma seudónima electrónica

Las siguientes variables se usan para la firma y la generación de seudónimo:

- la clave grupal *y* pública del generador,
- la clave privada (x_1, x_2) propia correspondiente, del generador,
- el mensaje *m* a firmar,
- la identidad *R* del receptor.

La firma y la generación de seudónimo se produce en los siguientes pasos a) hasta e):

a) el generador recibe la identidad y opcionalmente el mensaje a firmar del receptor. El receptor se autentifica frente al generador con un certificado de autorización, el cual contiene su identidad *R*. El generador comprueba la autentificación y el certificado de autorización y extrae entonces la identidad *R* del certificado.

b) el generador calcula un seudónimo a partir de su clave privada propia y de la identidad del receptor. El generador calcula el seudónimo como $I_R = R^{x_1}$.

c) el generador calcula una firma con el seudónimo. Este paso se produce como prueba simultánea del conocimiento de la clave privada propia (x_1, x_2). La generación de firma se produce en los siguientes pasos:

- genera una clave efímera (r_1, r_2) con $r_1 \in_R Z_q$ y $r_2 \in_R Z_q$.

- Calcula a partir de ello una clave efímera pública $a_1 = g_1^{r_1} \cdot g_2^{r_2}$ y $a_2 = R^{r_1}$.

- Calcula Hash $c = H([R,I_R,]a_1,a_2,m)$.

- Sea $s_1 = r_1 - c \cdot x_1$ y $s_2 = r_2 - c \cdot x_2$.

d) el generador transmite el seudónimo y la firma al receptor.

El seudónimo I_R y la firma (c, s_1, s_2) se envían al receptor.

e) el receptor comprueba la firma con la clave grupal pública y el seudónimo.

Los pasos son:

- calcula $a_1 = y^c \cdot g_1^{s_1} \cdot g_2^{s_2}$ y $a_2 = I_R^c \cdot R^{s_1}$

- la firma es válida precisamente cuando $H([R,I_R,]a_1,a_2,m)$.

Opciones

Los valores *R* e I_R pueden incorporarse durante la generación de firma opcionalmente en la firma, para ligar la firma adicionalmente de forma explícita a seudónimo e identidad de receptor.

La firma puede ampliarse opcionalmente a dos seudónimos $I_{R_1} = R^{x_1}$ e $I_{R_2} = R^{x_2}$.

Comprobación de la validez de la tarjeta chip con una lista negra o lista blanca

El receptor comprueba adicionalmente si la tarjeta chip es válida. Para ello el receptor comprueba el seudónimo con el seudónimo de una lista negra. La lista negra es gestionada por un servicio de bloqueo, que en el presente ejemplo es también el emisor de la tarjeta chip. Una comprobación de lista negra se usa para retirar una clave privada propia de un miembro de grupo cuando por ejemplo el miembro de grupo abandona el grupo. Para cada receptor registrado ha de generarse una lista negra propia, en la cual se alistan los seudónimos bloqueados.

En el marco de la generación de clave para un miembro del grupo el servicio de bloqueo ha obtenido la identidad de bloqueo $S = g_1^{x_1}$ del miembro del grupo y entonces la ha memorizado. Para bloquear un miembro del grupo con una clave privada propia (x_1, x_2), ha de calcularse para cada receptor *R* registrado el correspondiente seudónimo $I_R = R^{x_1}$ y memorizarse en la lista negra del receptor. Para ello el servicio de bloqueo calcula respectivamente a partir de la identificación privada x_R del receptor *R* y de la identidad de bloqueo $S = g_1^{x_1}$ del miembro del grupo el seudónimo $I_R = S^{x_R} = g_1^{x_1 \cdot x_R} = R^{x_1}$.

Los seudónimos calculados se ajustan en una lista negra específica de receptor.

El receptor puede comprobar también con la ayuda del seudónimo mediante una lista blanca de un servicio de bloqueo si la tarjeta chip es válida. Cuando la clave grupal y está comprometida, ésta ha de retirarse. En este caso pueden calcularse a través de una comprobación de lista blanca todos los seudónimos aún válidos. El cálculo de los seudónimos se produce de manera análoga a la comprobación de lista negra.

Para declarar como aún válido un miembro de grupo con una clave privada propia (x_1, x_2), ha de calcularse para cada receptor R registrado el correspondiente seudónimo $I_R = R^{x_1}$ y memorizarse en la lista blanca del receptor. Para ello el servicio de bloqueo calcula respectivamente a partir de la identificación privada x_R del receptor *R* y de la identidad de bloqueo $S = g_1^{x_1}$ del miembro del grupo el seudónimo $I_R = S^{x_R} = g_1^{x_1 \cdot x_R} = R^{x_1}$. Los seudónimos calculados se ajustan a una lista blanca específica de receptor. Suponiendo que existen esencialmente menos miembros de grupo que *q*, un atacante producirá mediante selección aleatoria o cálculo de una clave privada con alta probabilidad una clave, para la cual la identidad de bloqueo correspondiente no está contenida en la lista blanca.

REIVINDICACIONES

1. Procedimiento para la generación y verificación de una firma seudónima electrónica para el uso en la comunicación entre un generador y un receptor, siendo el generador miembro de un grupo de generadores, de los cuales a cada uno hay asignada una clave grupal (y) estática pública igual y una clave (x_1, x_2) estática privada propia y presentando el receptor una identidad (R), en donde en el procedimiento

- el generador recibe del receptor su identidad (R),

- el generador calcula a partir tanto de su clave (x_1, x_2) privada propia o una parte de ella, como también de la identidad (R) del receptor, al menos un seudónimo (I_R),

- el generador calcula mediante el uso del seudónimo (I_R) y su clave (x_1, x_2) privada propia una firma seudónima electrónica (I_R, c, s_1, s_2),

- el generador transmite la firma seudónima electrónica (I_R, c, s_1, s_2) al receptor y

- el receptor verifica mediante su propia identidad (R) y la clave grupal (y) pública la firma seudónima electrónica (I_R, c, s_1, s_2) incluida la generación correcta del seudónimo (I_R) obtenido del generador.

2. Procedimiento según la reivindicación 1, caracterizado por que la firma seudónima electrónica (I_R, c, s_1, s_2) se genera basándose en el cálculo de una firma Okamoto-Schnorr.

3. Procedimiento según una de las reivindicaciones 1 o 2, caracterizado por que el receptor se autentifica frente al generador mediante un certificado de autorización certificado por una tercera parte, que comprende la identidad (R) del receptor y que el generador verifica la autentificación, así como el certificado de autorización y extrae del certificado de autorización la identidad (R) del receptor.

4. Procedimiento según la reivindicación 1 a 3, caracterizado por que el generador presenta una tarjeta chip o un servidor y/o que el receptor es un proveedor de servicios.

5. Procedimiento según la reivindicación 1 a 4, caracterizado por que para la generación de la firma seudónima electrónica se usan un grupo matemático criptográficamente seguro, por ejemplo escrito multiplicativa o aditivamente, con, entre otros, un generador criptográfico (g_1) y una función Hash.

6. Procedimiento según una de las reivindicaciones 1 a 5, caracterizado por que para cada posible receptor se alistan todos los seudónimos válidos (I_R) en una lista blanca y que un receptor de este tipo comprueba antes de la verificación de la firma seudónima electrónica (I_R, c, s_1, s_2) que el seudónimo (I_R) está contenido en la lista blanca.

7. Procedimiento según una de las reivindicaciones 1 a 6, caracterizado por que para cada posible receptor se alistan todos los seudónimos bloqueados (I_R) en una lista negra y que un receptor de este tipo comprueba antes de la verificación de la firma seudónima (I_R, c, s_1, s_2) que el seudónimo (I_R) no está contenido en la lista negra.

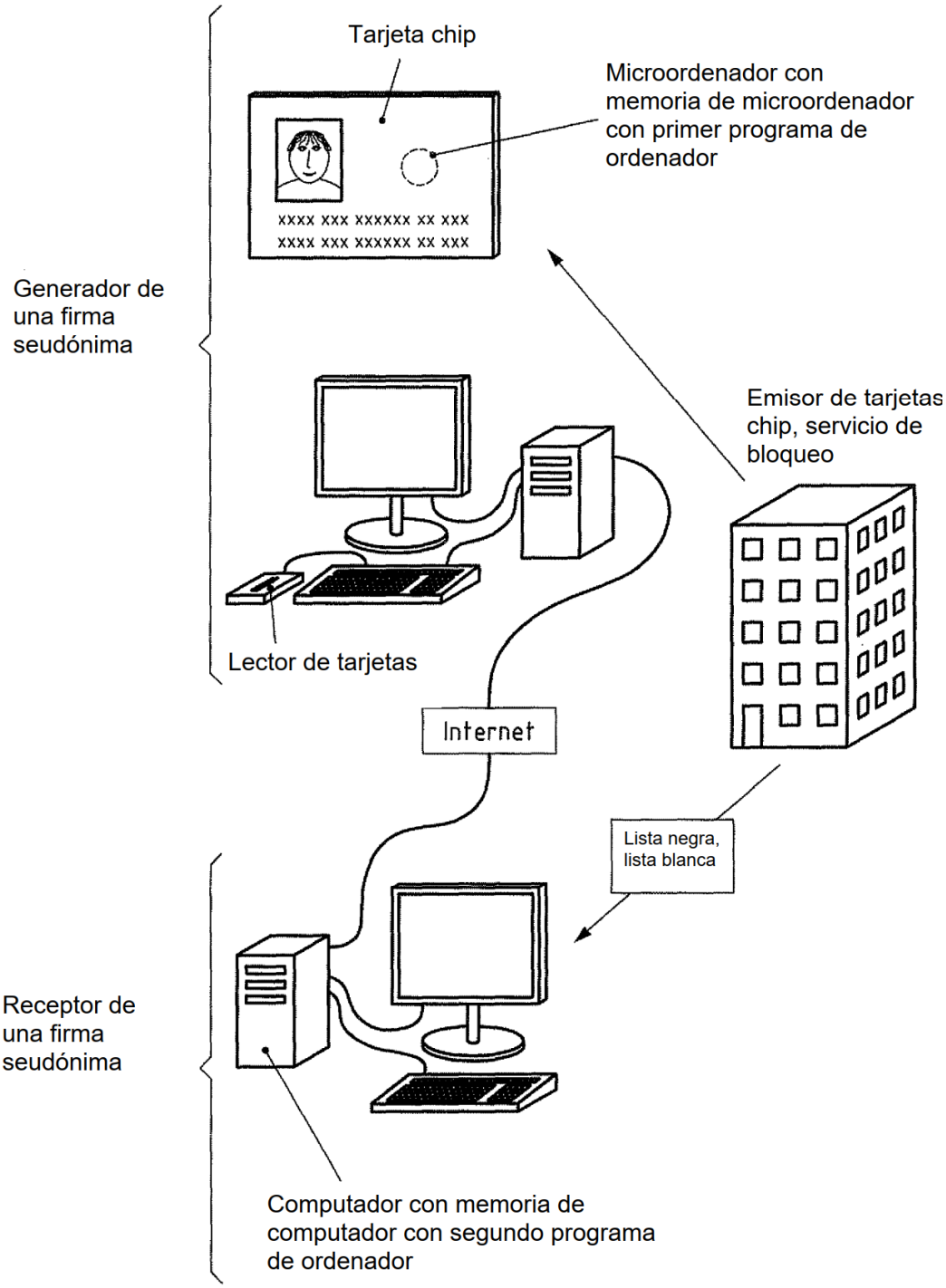
8. Uso del procedimiento según una de las reivindicaciones anteriores para el intercambio de datos anónimo entre dos participantes en la comunicación.

9. Procedimiento para la comunicación autentificada entre dos participantes en la comunicación usándose el procedimiento según una de las reivindicaciones 1 a 7.

10. Tarjeta chip, la cual está configurada para llevar a cabo el procedimiento según una de las reivindicaciones 1 a 7 en relación con el generador.

11. Computador, el cual está configurado para llevar a cabo el procedimiento según una de las reivindicaciones 1 a 7 en relación con el receptor.

Fig.


Tarjeta chip
Microordenador con memoria de microordenador con primer programa de ordenador
xxxx xxx xxxxxx xx xxx
xxxx xxx xxxxxx xx xxx
Generador de una firma seudónima
Emisor de tarjetas chip, servicio de bloqueo
Lector de tarjetas
Internet
Lista negra, lista blanca
Receptor de una firma seudónima
Computador con memoria de computador con segundo programa de ordenador