(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 602 054**

(51) Int. CI.:

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **25.03.2014 PCT/EP2014/055969**

(87) Fecha y número de publicación internacional: **02.10.2014 WO14154694**

(96) Fecha de presentación y número de la solicitud europea: **25.03.2014 E 14712007 (5)**

(97) Fecha y número de publicación de la concesión europea: **28.09.2016 EP 2891268**

(54) Título: **Firma de grupo utilizando un seudónimo**

(30) Prioridad:

25.03.2013 FR 1352650

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.02.2017

(73) Titular/es:

SAFRAN IDENTITY & SECURITY (100.0%)
11, boulevard Gallieni
92130 Issy-les-Moulineaux, FR

(72) Inventor/es:

PATEY, ALAIN;
CHABANNE, HERVÉ y
BRINGER, JULIEN

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Firma de grupo utilizando un seudónimo

Dominio de la invención

La presente invención concierne de forma general al dominio de las firmas numéricas.

La invención concierne más precisamente a un método novedoso de firma que combina una firma de grupo con la utilización de seudónimos, con fines de autentificación.

Ésta se aplica más particularmente a los documentos de identidad, en particular a los documentos de viaje legibles por máquinas (*Machine Readable Travel Document MRTD*) tales como los pasaportes o las tarjetas de identidad.

Estado de la técnica

Como se ilustra en la Figura 1, para que un titular de un documento de identidad DocId de tipo MRTD pueda acceder a un servicio propuesto por un proveedor de servicio SP, se establece una conexión entre el documento de identidad y un terminal T del proveedor de servicio y se ponen en práctica diversos mecanismos de seguridad. Entre estos mecanismos, el protocolo PACE (*Password Authenticated Connection Establishment*) permite establecer un canal seguro entre el documento de identidad y el terminal, y el protocolo EAC (*Extended Access Control*) permite realizar una autentificación mutua del documento de identidad y del proveedor de servicio y establecer otro canal seguro.

Además, el protocolo RI (*Restricted Identification*) permite generar un seudónimo específico a un documento de identidad para un dominio dado que reagrupa un conjunto de terminales del proveedor de servicio. Este seudónimo permite a dichos terminales identificar el documento de identidad. Por otra parte, este protocolo satisface la propiedad de "*cross – domain anonymity*": es imposible establecer un vínculo entre los seudónimos utilizados para dominios diferentes para un mismo documento de identidad.

Este protocolo puede entenderse como la utilización de seudónimos como tales para firmar numéricamente un mensaje. Una variante como tal de este protocolo se describe en la referencia *Bender, J., Dagdelen, O., Fischlin, M., Kugler, D.: Domain – specific pseudonymous signatures for the german identity card. In: Gollmann, D., Freiling, F.C (eds.) ISC. Lecture Notes in Computer Science, vol. 7483, pág. 104 – 119, Springer (2012)* y propone que cada usuario posea un elemento secreto, denominado clave de firma, generado por una autoridad de gestión de claves a partir de su propia clave secreta, y que este elemento secreto sea utilizado a la vez para firmar los mensajes emitidos y para generar el seudónimo utilizado por este usuario. Este protocolo permite garantizar que el usuario posee una clave de firma válida y no revocada, y que el seudónimo utilizado es legítimo.

Un protocolo como tal verifica las tres propiedades siguientes: "*unforgeability*", "*cross – domain anonimity*" y "*seclusiveness*".

La propiedad de "*unforgeability*" asegura que es imposible para cualquiera generar una firma en lugar del titular de un documento de identidad.

La propiedad de "*seclusiveness*" asegura que es imposible que se genere una firma válida utilizando un seudónimo no válido.

No obstante, este protocolo se basa en la hipótesis de que los usuarios no pueden recuperar su clave de firma, suponiéndose que esta clave está almacenada en un circuito integrado inviolable de un documento de identidad. En efecto, la puesta en común por al menos dos usuarios de sus claves de firma les permitiría recuperar la clave secreta de la autoridad de gestión de claves y, por lo tanto, generar nuevas claves válidas. Existe, por lo tanto, una necesidad de proponer un mecanismo de firma seguro incluso en caso de recuperación y de puesta en común de las claves de firma de varios usuarios.

Por otra parte, este protocolo supone igualmente que la autoridad de gestión de claves no memoriza las claves de firma generadas por los usuarios, una vez que éstas son entregadas. En efecto, el conocimiento de las calves por parte de la autoridad de gestión claves le permitiría utilizarlas para firmar un mensaje en lugar de cualquier usuario legítimo. Sin embargo, la ausencia de memorización de estas claves por la autoridad de gestión de claves es difícil de garantizar. Por lo tanto, existe igualmente una necesidad de proponer un mecanismo de firma que garantice que ninguna autoridad pueda firmar un mensaje en lugar de un usuario.

Por otra parte, otro mecanismo de firma conocido es el de la firma de grupo, tal como el descrito en la referencia *Bringer, J. Patey, A.: VLR group signatures – how to achieve both backward unlinkability and efficient revocation checks. In: SECRYPT*, pág. 215 – 220 (2012). Este permite a un miembro de un grupo firmar un mensaje de manera anónima en el nombre del grupo y probar la pertenencia de este miembro a este grupo.

Éste prevé asociar un secreto de grupo a los miembros de un grupo. Éste prevé igualmente asociar a cada miembro del grupo una clave secreta compuesta de una primera parte de clave generada por el miembro y una segunda parte de clave basada a la vez en la primera parte de clave y en el secreto de grupo. La firma de un mensaje o desafío por

parte de un miembro con su clave secreta le permite probar que él es miembro del grupo a la vez que permanece anónimo.

Sin embargo, un mecanismo como tal no permite que un miembro del grupo tenga una identidad dentro de ese grupo.

Las siguientes referencias describen igualmente mecanismos de firma de grupo: *David Chaum, Eugène van Heyst: Group Signatures. EUROCRYPT 1991:257 – 265* y *Dan Boneh, Hovav Shacham; Group signatures with verifier – local revocation. ACM Conference on Computer and Communications Security 2004: 168 – 177*.

Existe por lo tanto una necesidad de proponer un mecanismo de firma que permita a un miembro de un grupo firmar un mensaje en el nombre del grupo, a la vez que se tiene una identidad dentro del grupo, sin presentar los inconvenientes de los mecanismos de firma que utilizan seudónimos, citados anteriormente.

Resumen de la invención

Con este fin, la invención tiene por objetivo un procedimiento de firma de un mensaje m llevado a cabo por unos medios de tratamiento de un dispositivo usuario de un miembro M_i perteneciente a un grupo de miembros $\mathcal{G}$ generado por una autoridad de gestión de claves, poseyendo dicho dispositivo usuario una clave de firma secreta sk_i, que comprende una etapa de generación para el mensaje m de una firma de grupo σ que permite a dicho miembro M_i probar su pertenencia al grupo de miembros $\mathcal{G}$ y una etapa de generación de un seudónimo nym_{ij} que identifica al miembro M_i dentro de un dominio D_j de un proveedor de servicios SP_j, comprendiendo dicho dominio D_j un conjunto de terminales en comunicación con un servidor de dicho proveedor de servicios, estando dicha firma σ construida de manera tal que dicho miembro M_i puede probar al firmar el mensaje m su conocimiento de dicha clave de firma secreta sin divulgarla,

y caracterizado por que dicha firma de grupo está construida de manera tal que la pertenencia del miembro al grupo es verificable independientemente del seudónimo,

y por que la clave de firma secreta sk_i del miembro M_i comprende por lo menos una primera parte de clave f_i generada por los medios de tratamiento del dispositivo usuario de dicho miembro y desconocido por la autoridad de gestión de las claves,

y por que dicho seudónimo y dicha firma son función de una segunda parte x_i de dicha clave de firma secreta del miembro M_i, y están construidos de manera tal que prueban que el miembro identificado por el seudónimo es el firmante del mensaje m y por que dicho seudónimo nym_{ij} del miembro M_i es específico para el dominio D_j.

El mecanismo de firma objeto de la invención combina de este modo una firma de grupo y la utilización de seudónimos, y permite al firmante probar su pertenencia al grupo a la vez que tiene una identidad dentro de ese grupo.

Ventajosamente, dicha clave de firma secreta (sk_i) es almacenada dentro de un medio de almacenamiento seguro para impedir el acceso al mismo por un tercero.

En un modo de realización, previamente a dichas etapas de generación de una firma de grupo y de un seudónimo, dicho procedimiento puede comprender una etapa de generación de claves llevada a cabo por un servidor de gestión de claves de la autoridad de gestión de claves, en el transcurso de la cual los medios de tratamiento del servidor de gestión generan para el grupo de miembros $\mathcal{G}$ un conjunto de parámetros públicos gpk, determinan un parámetro de dominio dpk_j específico para el dominio D_j y transmiten este parámetro al proveedor de servicios SP_j.

Ventajosamente, el parámetro de dominio (dpk_j) es igual a g_1^{rj}, siendo r_j un entero y g1 un generador de un grupo G1, siendo g1 un parámetro que es parte del conjunto de parámetros públicos (gpk). En un modo de realización, el entero r_j es determinado por la autoridad de gestión de claves.

De manera preferente, dicho seudónimo nym_{ij} del miembro M_i dentro del dominio D_j es función del parámetro de dominio dpk_j específico del dominio D_j determinado por dicho servidor de gestión.

En particular, el seudónimo nym_{ij} puede ser igual a dpk_j^{xi} siendo x_i dicha segunda parte de la clave de firma secreta del miembro M_i y siendo dpk_j dicho parámetro de dominio.

De este modo, el seudónimo de un miembro es diferente en cada dominio y no revela la parte de clave secreta utilizada para generarlo, lo cual permite garantizar que no se puedan vincular los seudónimos del mismo miembro en dos dominios diferentes.

Por otra parte, dicha firma σ puede comprender un valor K, diferente del seudónimo, de la forma B^x_i, siendo B un elemento de un grupo G1 y x_i dicha segunda parte de clave de firma secreta del miembro M_i.

Según una variante, los medios de tratamiento del dispositivo usuario llevan a cabo un algoritmo de prueba de divulgación nula de conocimiento en el cual dicha firma es generada de forma tal que se prueba que el miembro

identificado por el seudónimo (nym_{ij}) es el firmante del mensaje. La utilización de un algoritmo de divulgación nula de conocimiento permite al firmante aportar la prueba de su identidad sin, sin embargo, divulgar su clave secreta.

La invención tiene igualmente como objetivo un procedimiento de control de una firma de un mensaje m y de un seudónimo, llevado a cabo por unos medios de tratamiento de un servidor de control, siendo generados dicha firma σ y dicho seudónimo nym_{ij} según el procedimiento de firma descrito anteriormente, comprendiendo una etapa de verificación, a partir de la firma σ y del seudónimo nym_{ij}, del conocimiento por parte del miembro M_i de la clave de firma secreta sk_i, y de que dicho seudónimo y dicha firma del miembro M_i son función de una segunda parte xi de dicha clave de firma secreta, con el fin de probar que el miembro identificado por el seudónimo es el firmante del mensaje m y que éste pertenece al grupo de miembros $\mathcal{G}$.

Según una variante, dicha etapa de verificación comprende una etapa de verificación de prueba, en el transcurso de la cual los medios de tratamiento del servidor de control verifican que una prueba de divulgación nula de conocimiento que prueba que el miembro identificado por el seudónimo es el firmante del mensaje (m) es correcta. Dicha etapa de verificación de prueba puede verificar la igualdad de los logaritmos discretos del valor K en base B y del seudónimo nym_{ij} en base dpk_j. Una etapa como tal prueba de este modo que el miembro identificado por el seudónimo es con certeza el firmante del mensaje m sin tener que calcular dichos logaritmos discretos y sin revelar ninguna parte de la clave de firma secreta del miembro M_i.

Según un modo de realización, dicha etapa de verificación comprende una verificación de dicha firma para probar la pertenencia del miembro (M_i) al grupo y dicha etapa de verificación de prueba es realizada en el transcurso de la verificación de dicha firma. De este modo, la verificación de la firma permite a la vez probar la pertenencia del firmante al grupo y probar que el miembro identificado por el seudónimo es con certeza el firmante del mensaje.

El procedimiento de control puede igualmente comprender una etapa de verificación de la revocación del miembro M_i del grupo de miembros $\mathcal{G}$.

Para hacer esto, los medios de tratamiento del servidor de control pueden verificar en una base de datos que el seudónimo nym_{ij} del miembro M_i no pertenece a una lista de revocación RL_j para el dominio D_j, estando construida dicha lista de revocación a partir de los seudónimos nym_{ij} de los miembros del grupo $\mathcal{G}$ revocados por la autoridad de gestión.

La autoridad de gestión que desea revocar del grupo de miembros $\mathcal{G}$ a un miembro M_i, transmite dicha segunda parte de clave secreta x_i del miembro M_i al proveedor de servicios SP_j. La lista de revocación RL_j para el dominio D_j almacenado en una base de datos, es construida por el proveedor de servicios SP_j, añadiendo a la lista de revocación RL_j el seudónimo nym_{ij} del miembro M_i calculado a partir de dicha segunda parte de clave secreta recibida.

La invención tiene igualmente como objetivo un programa de ordenador que comprende instrucciones de código de programa para la ejecución de las etapas de los procedimientos de firma y de control de firma definidos anteriormente cuando dicho programa es ejecutado en un ordenador, comprendiendo un dispositivo usuario y un servidor de control por lo menos un medio de almacenamiento, un medio de tratamiento y una interfaz de comunicación configurados para llevar a cabo respectivamente un procedimiento de firma y un procedimiento de control de firma tales como los definidos anteriormente, así como un sistema que comprende por lo menos un dispositivo usuario como tal y por lo menos un servidor de control como tal.

Descripción de las figuras

Otras características y ventajas se harán aún evidentes a partir de la descripción siguiente, la cual es puramente ilustrativa y no limitativa, y debe ser leída en relación con las figuras anexas, entre las cuales:

La Figura 1 ilustra mecanismos de seguridad avanzados para MRTD.

La Figura 2 es una representación esquemática de un ejemplo de sistema para la puesta en marcha de los procedimientos según la invención.

La Figura 3 representa un ordinograma que ilustra las etapas genéricas de un procedimiento de firma según un modo de realización de la invención.

La Figura 4 representa un ordinograma que ilustra las etapas de un procedimiento de generación de parámetros públicos según un modo de realización de la invención.

La Figura 5 representa un ordinograma que ilustra las etapas de un procedimiento de adhesión a un grupo según un modo de realización de la invención.

La Figura 6 representa un ordinograma que ilustra las etapas de un procedimiento de firma de un mensaje según un modo de realización de la invención.

La Figura 7 representa un ordinograma que ilustra las etapas genéricas de un procedimiento de firma y de control de firma según un modo de realización de la invención.

La Figura 8 representa un ordinograma que ilustra las etapas de un procedimiento control de firma según un modo de realización de la invención.

Descripción detallada de por lo menos un modo de realización

La Figura 2 representa un ejemplo de sistema para la implementación de los procedimientos según la invención.

Un sistema como tal comprende un conjunto de dispositivos usuarios 201 en posesión cada uno por parte de un miembro M_i (i entero) que forma parte de un conjunto de miembros que constituye un grupo de miembros $\mathcal{G}$, unos terminales de lectura 202, una autoridad de gestión de claves 203, unos proveedores de servicios 204 y unos verificadores 205, pudiendo ser los verificadores, proveedores de servicio.

El conjunto de los dispositivos usuarios, los terminales de lectura, la autoridad de gestión de claves, los proveedores de servicios y los verificadores están interconectados por medio de una red informática 206. Un conjunto de terminales de esta red en comunicación con un proveedor de servicio constituye un dominio.

La autoridad de gestión de claves, los proveedores de servicio y los verificadores pueden estar conectados a esta red mediante servidores respectivos que comprenden una memoria viva y medios de almacenamiento tales como una memoria no volátil regrabable (memoria flash o memoria EEPROM) que puede almacenar una base de datos, medios de tratamiento que comprenden un procesador, unidades criptográficas para generar en particular números aleatorios, etc., y medios de interfaz que les permiten comunicarse con otras entidades en la red y estar conectados a bases de datos. Servidores como tales pueden comprender igualmente medios de introducción de datos y de interfaz de usuario que permiten su administración. Los servidores de las entidades mencionadas se denominan respectivamente servidor de gestión de claves 203s, servidor de proveedor de servicio 204s y servidor de control 205s en lo que sigue de la descripción.

Ventajosamente, por lo menos dos de estos servidores pueden estar reunidos en el seno de un mismo dispositivo informático, asegurando conjuntamente las funciones de dichos servidores.

El dispositivo usuario de un miembro M_i puede comprender un dispositivo electrónico portátil apto para almacenar datos seguros legibles por un terminal de lectura.

Un dispositivo electrónico portátil puede ser un documento de identidad que comprende un circuito integrado en el cual se almacenan datos seguros, por ejemplo, un documento de viaje legible por una máquina *(Machine Readable Travel Document, MRTD)* tal como un pasaporte o un documento de identidad, un dispositivo de almacenamiento con memoria flash dotado de una interfaz de comunicación USB, denominado clave USB *("Universal Serial Bus")*, una tarjeta con circuito integrado, etc. El dispositivo electrónico portátil puede comprender una memoria viva y medios de almacenamiento tales como una memoria no volátil regrabable (memoria flash o memoria EEPROM), medios de tratamiento que comprenden un procesador, unidades criptográficas para generar en particular números aleatorios, etc. El dispositivo electrónico portátil puede comprender igualmente una interfaz de comunicación sin contacto tal como una interfaz RFID o NFC, o bien, una interfaz de comunicación inalámbrica tal como una interfaz *Bluetooth* o *WiFi*.

Los datos seguros almacenados en el dispositivo electrónico portátil pueden ser datos biométricos. En este caso, el dispositivo portátil puede estar provisto de sensores que permiten capturar los datos biométricos de un miembro M_i, tales como sus huellas digitales, palmares o retinianas.

Un dispositivo electrónico portátil y un terminal de lectura pueden comunicarse por medio de comunicaciones inalámbricas o sin contacto tales como las mencionadas anteriormente. Éstos pueden igualmente comunicarse por medio de un interfaz USB, *Firewire* o cualquier otra interfaz de comunicación con cable. Éstos pueden igualmente comunicarse por medio de una interfaz de contacto de tarjeta con circuito integrado de tipo ISO 7816.

Un terminal de lectura puede igualmente comprender una interfaz de comunicación con cable o inalámbrica, adaptada para la conexión del terminal a la red informática, tal como una interfaz *Ethernet*, *WiFi* o 3G, y una interfaz de usuario que permita al miembro M_i controlar su funcionamiento.

Según una variante, un dispositivo electrónico portátil y un terminal de lectura pueden estar reunidos en el seno de un mismo dispositivo electrónico que comprende medios de interfaz de comunicación y de interfaz de usuario similares a los descritos anteriormente.

La red que une los miembros M_i y los servidores consiste, a título de ejemplo, en una red local *Ethernet*, una red local inalámbrica, la red *Internet*, una red de telefonía móvil, etc. Ventajosamente, las comunicaciones sobre esta red son seguras, en particular mediante el cifrado de los datos intercambiados.

La figura 3 representa un ordinograma que ilustra las etapas genéricas del procedimiento de firma en un modo de realización de la invención.

El mecanismo de firma objeto de la invención combina una firma de grupo y la utilización de seudónimos.

En un modo de realización preferencial y detallado a continuación, el mecanismo de firma de grupo presentado está basado en un mecanismo de firma de grupo VLR *("Verifier Local Revocation")* tal como el descrito en la referencia *Bringer, J. Patey, A.: VLR group signatures – how to achieve both backward unlinkability and efficient revocation checks. In: SECRYPT*, pág 215 – 220 (2012).

El procedimiento de firma según la invención puede comprender una etapa E100 de generación de una clave, una etapa E200 de adhesión al grupo y una etapa E300 de firma, descritos en los parágrafos siguientes.

Se denota con:

G_1, G_2, G_T unos grupos bilineales de primer orden p (estando codificado p sobre k bits) tal que (p – 1)/2 sea un número primo,

q, un número primo,

e, un acoplamiento de G_1 x G_2 en G_T, es decir, una forma bilineal y no degenerada de G_1 x G_2 en G_T,

g_1 y g_2, generadores de G_1 y G_2

Por otra parte, la notación "||" representa la operación de concatenación.

El procedimiento de firma puede comprender una primera etapa E100 de generación de clave llevada a cabo por el servidor de gestión de claves 203s, representada en la Figura 4. Según un modo de realización, en el transcurso de una etapa E101 los medios de tratamiento del servidor de gestión generan para el grupo un conjunto de parámetros públicos gpk y un secreto de grupo γ. En el transcurso de una etapa E102, el servidor de gestión determina de manera aleatoria un parámetro de dominio dpk_j y lo transmite en el transcurso de una etapa E103 a través de sus medios de interfaz al servidor del proveedor de servicio SP_j 204 perteneciente a un dominio Dj. Los parámetros públicos gpk se hacen públicos en el transcurso de una etapa E104. Según una variante, el parámetro de dominio dpk_j se hace público igualmente.

Más precisamente, en un modo de realización de la invención, en el transcurso de esta etapa E100, los medios de tratamiento del servidor de gestión de claves:

- determinan los grupos bilineales de primer orden G_1, G_2, G_T, el número primo q y el acoplamiento e;
- determinan una función de control H de {0, 1}* hacia Z_p;
- determinan $\check{g}_1$, $\hat{g}_1$, pertenecientes a G_1,
- determinan el secreto de grupo γ perteneciente a Z_p*,
- calculan $w = g_2^{\gamma}$,
- calculan $T_1 = e(g_1, g_2)$, $T_2 = e(\check{g}_1, g_2)$, $T_3 = e(\hat{g}_1, g_2)$ y $T_4 = e(\hat{g}_1, w)$

A partir de estos elementos, el servidor de gestión de claves puede generar el conjunto de parámetros públicos $gpk = (G_1, G_2, G_T, e, p, g_1, g_2, \check{g}_1, \hat{g}_1, w, H, T_1, T_2, T_3, T_4)$.

El secreto de grupo no forma parte, de este modo, de los parámetros públicos gpk, y no es poseído más que por la autoridad de gestión. La dificultad de llevar a cabo el algoritmo del logaritmo discreto para un grupo G_2 bien elegido permite garantizar la imposibilidad práctica de recuperar el secreto de grupo γ a partir de w. De este modo, la difusión de w en el conjunto de parámetros públicos gpk no genera ningún problema de seguridad del mecanismo de firma y w será utilizado para verificar la pertenencia al grupo del firmante de un mensaje.

En el transcurso de la etapa E102, para cada proveedor de servicio SPj, el servidor de gestión de claves genera un parámetro de dominio dpk_j específico para el dominio D_j. Este parámetro puede ser función de un número entero r_j. A título de ejemplo, este parámetro puede ser igual a g_1^{rj}. El entero r_j puede ser generado ventajosamente de manera aleatoria por el servidor de gestión con la ayuda de su unidad criptográfica. El servidor de gestión transmite a continuación este parámetro mediante sus medios de interfaz al servidor del proveedor de servicio SP_j.

Los parámetros públicos gpk y, llegado el caso, el parámetro de dominio dpk_j, pueden hacerse públicos de diversas maneras. Éstos pueden ser enviados a los dispositivos usuarios 201 y a los servidores de control 205s por los proveedores de servicio o publicados en un sitio de proveedores de servicio.

El procedimiento de firma puede comprender igualmente, según un modo de realización de la invención, una segunda etapa E200 denominada de adhesión al grupo, consistente en crear una clave de firma secreta para un nuevo miembro que se adhiere al grupo, descrito en la Figura 5. Esta etapa puede ser llevada a cabo cuando un propietario

de un dispositivo usuario 201 desea hacerse miembro Mi, siendo i entero, del grupo $\mathbb{G}$ generado por la autoridad de gestión de claves 203 que juega el papel de gestor de grupo.

Según un modo de realización, este miembro puede generar, en el transcurso de una etapa E201, con la ayuda de medios de tratamiento de sus dispositivo electrónico portátil, una primera parte de clave desconocida por la autoridad de gestión de claves, transmitir en el transcurso de una etapa E203 un dato de identidad, calculado en el transcurso de una etapa E202 por esos medios de tratamiento a partir de esta primera parte de clave, al servidor de gestión de claves 203s y probar a la autoridad de gestión de claves, con la ayuda de este dato de identidad, que él posee la primera parte de clave mediante un algoritmo de prueba de divulgación nula de conocimiento *("Zero knowledge proof")*. El servidor de gestión de claves genera entonces, en el transcurso de una etapa E204 y transmite a continuación al miembro Mi en el transcurso de una etapa E205, la parte de clave que hace falta, formando con la primera parte de la clave, la clave de firma del miembro Mi.

Más precisamente, en un modo de realización de la invención, en el transcurso de esta etapa E200:

- El servidor de gestión de claves transmite al dispositivo usuario del miembro M_i a través de sus medios de interfaz, un número n_i determinado aleatoriamente, perteneciente a $\{0, 1\}^k$.
- Los medios de tratamiento del dispositivo usuario del miembro M_i determinan una primera parte de clave f_i perteneciente a Z_p y calculan los datos de identidad $F_i = \breve{g}_1^{fi}$.
- Los medios de tratamiento del dispositivo usuario del miembro M_i determinan aleatoriamente un número r_f perteneciente a Z_p y calculan $R = \breve{g}_1^{rf}$, $c = H(gpk \,||\, F_i \,||\, R \,||\, n_i)$ y después $s_f = r_f + c\, f_i$.
- El dispositivo usuario del miembro M_i transmite F_i, c y s_f al servidor de gestión de claves.
- Los medios de tratamiento del servidor de gestión de claves calculan $R' = \breve{g}_1^{sf}, x\, F_i^{-c}$ comparan c y $H(gpk \,||\, F_i \,||\, R' \,||\, n_i)$ y verifican que s_f pertenece a Z_p. Si esta comparación es positiva, el miembro M_i ha aportado bien a la autoridad de gestión la prueba de que éste posee la primera parte de la clave f_i. sin divulgarla.
- Si la comparación es positiva, los medios de tratamiento del servidor de gestión de claves determinan una segunda parte de clave x_i perteneciente a Z_p y calculan una tercera parte de clave $A_i = (g_1 F_i)^{1/(xi+\gamma)}$.
- Los medios de interfaz del servidor de gestión de claves transmiten las partes segunda y tercera de clave, x_i y A_i al miembro M_i utilizando un canal, con preferencia, seguro.
- De manera opcional, M_i verifica que $e(A_i, w g_2^{xi}) = e(g_1 \hat{g}_1^{fi}, g_2)$ en el transcurso de una etapa E206.

De este modo, A_i que constituye la tercera parte de la clave, es función del secreto de grupo.

Además, en un modo de realización como tal, el miembro M_i es el único que conoce la integridad de su clave de firma constituida por las primera, segunda y tercera partes de la clave. Nadie, ni siquiera la autoridad de gestión de claves puede, de este modo, firmar un mensaje en lugar de un miembro.

La última verificación opcional permite al miembro verificar que el par de partes segunda y tercera (A_i, x_i) que le han sido transmitidos no se ha corrompido y es válido, es decir, verifica la ecuación $A_i = (g_1 F_i)^{1/(xi+\gamma)}$.

La clave de firma del miembro M_i puede ser almacenada en medios de almacenamiento seguros del dispositivo usuario perteneciente al miembro M_i, ventajosamente en la memoria no volátil del dispositivo electrónico portátil correspondiente.

Del mismo modo, las segunda y tercera partes de la clave pueden ser almacenadas por el servidor de gestión de claves, ventajosamente en el seno de una base de datos registrada en los medios de almacenamiento del servidor de gestión de claves, o bien, conectada a ésta.

Según una variante de la invención, la primera parte de la clave f_i se calcula a partir de un dato biométrico del miembro M_i capturado por los sensores del dispositivo electrónico portátil, o bien, memorizado por éste. La primera parte de clave f_i puede igualmente ser el resultado de la aplicación, por parte de los medios de tratamiento del dispositivo electrónico portátil, de una función de control a un dato biométrico como tal.

De forma opcional, en el transcurso de la ejecución de esta etapa de adhesión a un grupo, la autoridad de gestión envía el resultado del acoplamiento $e(A_i, g_2)$ al miembro M_i para evitar que éste tenga que hacerse cargo del cálculo de un acoplamiento posterior en el transcurso de la firma.

El procedimiento de firma comprende una tercera etapa E300 de firma de un mensaje m, descrito en la Figura 6. El mensaje m puede ser un desafío ("reto") transmitido previamente por un servidor de control 205s al miembro M_i, o bien, cualquier tipo de mensaje a firmar por el miembro M_i. Ventajosamente, se transmite igualmente al miembro M_i el parámetro de dominio dpk_j, si éste no se ha hecho público o ya no es conocido por dicho miembro.

Esta etapa permite generar, en el transcurso de una etapa E301 para el mensaje m, una firma de grupo que permite probar la pertenencia del miembro al grupo de manera anónima y de asociarle, en el transcurso de una etapa E302, un seudónimo nym_{ij} que identifica al miembro M_i. Dicho seudónimo y dicha firma son función de una parte de dicha clave de firma secreta del miembro M_i, y son construidos de manera que prueben que el miembro identificado por el seudónimo es el firmante del mensaje m. Además, dicho seudónimo nym_{ij} del miembro M_i es específico para el dominio D_j.

Ventajosamente, los medios de tratamiento del dispositivo usuario llevan a cabo un algoritmo de prueba de divulgación nula de conocimiento en el cual la firma es generada de manera tal que prueba que el miembro identificado por el seudónimo nym_{ij} es el firmante del mensaje m.

Más precisamente, en un primer modo de realización de la invención, en el transcurso de esta etapa E300, los medios de tratamiento del dispositivo usuario 201 del miembro M_i:

- Determinan B perteneciente a G_1 y calculan $J = B^{fi}$, $K = B^{xi}$.
- Determinan a perteneciente a Z_p y calculan $b = a\, x_i$ y $T = A_i\, \hat{g}_1^{a}$
- Determinan r_f, r_x, r_a, r_b, r_{x2}, pertenecientes a Z_p.
- Calculan $R_1 = B^{rf}$, $R_2 = B^{rx}$, $R_4 = K^{ra}B^{-rb}$, $R_3 = e(T, g_2)^{-rx}\, T_2^{rf}\, T_3^{rb}\, T_4^{ra}$, $R_5 = dpk_j^{rx2}$, $R_6 = B^{rx2}$.
- Calculan $c = H(gpk \,||\, B \,||\, J \,||\, K \,||\, T \,||\, R_1 \,||\, R_2 \,||\, R_3 \,||\, R_4 \,||\, m)$ y $d = H(gpk \,||\, B \,||\, K \,||\, dpk_j \,||\, nym_{ij} \,||\, R_5 \,||\, R_6)$.
- Calculan $s_f = r_f + c\, f_i$, $s_x = r_x + c\, x_i$, $s_a = r_a + c\, a$, $s_b = r_b + c\, b$, $s_{x2} = r_{x2} + d\, x_i$.

El miembro M_i posee entonces la firma del mensaje $\sigma = (B, J, K, T, c, s_f, s_x, s_a, s_b, d, s_{x2})$ y un seudónimo $nym_{ij} = dpk_j^{xi}$. Los elementos B, J, K, T, c, s_f, s_x, s_a y s_b de la firma pueden ser utilizados para verificar la pertenencia del miembro al grupo independientemente del seudónimo. La firma puede, por lo tanto, ser utilizada de manera anónima. Por otra parte, el seudónimo y los elementos B, K, d y s_{x2} de la firma pueden ser utilizados para probar que la misma clave secreta ha sido utilizada para generar el seudónimo y la firma, y así probar que el miembro identificado por el seudónimo nym_{ij} es el firmante del mensaje m.

En un segundo modo de realización, en el transcurso de esta etapa E300, los medios de tratamiento del dispositivo usuario 201 del miembro M_i:

- Determinan B perteneciente a G_1 y calculan $J = B^{fi}$, $K = B^{xi}$.
- Determinan a perteneciente a Z_p y calculan $b = a\, x_i$ y $T = A_i\, \hat{g}_1^{a}$
- Determinan r_f, r_x, r_a, r_b, pertenecientes a Z_p.
- Calculan $R_1 = B^{rf}$, $R_2 = B^{rx}$, $R_4 = K^{ra}B^{-rb}$, $R_3 = e(T, g_2^{)-rx}\, T_2^{rf}\, T_3^{rb}\, T_4^{ra}$, $R_5 = dpk_j^{rx}$.
- Calculan $c = H(gpk \,||\, B \,||\, J \,||\, K \,||\, T \,||\, R_1 \,||\, R_2 \,||\, R_3 \,||\, R_4 \,||\, R_5 \,||\, m)$.
- Calculan $s_f = r_f + c\, f_i$, $s_x = r_x + c\, x_i$, $s_a = r_a + c\, a$, $s_b = r_b + c\, b$.

El miembro M_i posee entonces la firma del mensaje $\sigma = (B, J, K, T, c, s_f, s_x, s_a, s_b)$ y un seudónimo $nym_{ij} = dpk_j^{xi}$ que le permiten identificarse dentro del grupo. La firma σ y el elemento R_5 pueden ser utilizados para verificar la pertenencia del miembro al grupo independientemente del seudónimo y, por lo tanto, de manera anónima. Por otra parte, la firma y el seudónimo pueden ser utilizados para probar que el miembro identificado por el seudónimo nym_{ij} es el firmante del mensaje m. De forma alternativa, la firma y el seudónimo pueden ser utilizados para probar en una sola operación de verificación la pertenencia del miembro al grupo y que el miembro identificado por el seudónimo nym_{ij} es el firmante del mensaje m, como se detalló anteriormente.

Estando formado el seudónimo del miembro M_i dentro del dominio D_j a partir del parámetro de dominio dpk_j específico del dominio D_j, el miembro M_i tendrá seudónimos diferentes dentro de dominios distintos. Por lo tanto, es imposible para los proveedores de servicio 204 o para los verificadores 205 determinar si dos mensajes de dos dominios distintos que presentan firmas y seudónimos diferentes han sido generados por el mismo miembro *("cross – domain unlinkability")*.

Sin embargo, para preservar la propiedad de *unlinkability*, los proveedores de servicio y verificadores no deben tener conocimiento de los r_j. En efecto, a partir de r_j y de un seudónimo $nym_{ij} = dpk_j^{xi}$ con $dpk_j = g_1^{rj}$, g_1^{xi} puede ser recuperado. De este modo, conociendo dos r_j utilizados para generar los parámetros de dominio de dos dominios distintos, un proveedor de servicio o un verificador podría determinar si dos seudónimos dentro de estos dominios corresponden al mismo miembro.

La firma σ está construida de manera tal que el miembro M_i pueda probar, firmando un mensaje o desafío, que él tiene conocimiento de la clave de firma secreta ski = (f_i, x_i, A_i) sin divulgarla, ventajosamente por un algoritmo de prueba de divulgación nula de conocimiento y, por lo tanto, probar su pertenencia al grupo.

Además, por construcción, xi, que constituye una segunda parte de la clave de firma secreta, es utilizada a la vez para el cálculo de la firma del mensaje m y para generar el seudónimo utilizado por el miembro M_i. Esto permite vincularlos y, de este modo, poder probar a partir de la firma y del seudónimo que el miembro M_i conoce la segunda parte de la clave x_i sin desvelar esta última y que el miembro identificado por el seudónimo construido a partir de esta segunda parte de clave x_i es con certeza el firmante legítimo del mensaje m.

Con el fin de limitar la utilización de los recursos del dispositivo usuario del miembro M_i, la autoridad de gestión 203 puede enviar, durante la ejecución de la etapa de adhesión al grupo E200, el resultado del acoplamiento $e(A_i, g_2)$ al miembro M_i con el fin de que éste no tenga que hacerse cargo del cálculo de R_3. En efecto, $e(T_2, g_2) = e(A_i, g_2)\, e(\hat{g}_1, g_2)^a$. Conociendo $e(A_i, g_2)$ y $e(\hat{g}_1, g_2)$, el miembro M_i no tiene más que, de este modo, exponentes y multiplicaciones a calcular.

Del mismo modo, ventajosamente, todos los cálculos efectuados en el transcurso de esta etapa de firma pueden ser realizados fuera de línea antes de la recepción del mensaje m a firmar, con la excepción del cálculo de control y de los exponentes de R_5 y nym_{ij}. Esto permite limitar el tiempo de firma de un mensaje y los recursos necesarios para ésta. Según una variante, es igualmente posible calcular con anterioridad R_5 y nym_{ij} para cada uno de los proveedores de servicio si los parámetros de dominio dpk_j han sido previamente obtenidos por el miembro M_i y si la memoria necesaria para almacenar los resultados de estos cálculos está disponible.

Al final de esta etapa de firma, el dispositivo usuario 201 del miembro M_i transmite, en el transcurso de una etapa E303 por sus medios de interfaz de comunicación, la firma σ obtenida, el seudónimo correspondiente al miembro M_i, y el elemento R_5 en el segundo modo de realización, al servidor de control 205s que le ha enviado el desafío a firmar, o bien, al destinatario del mensaje m al cual éste envía igualmente el mensaje m.

La invención concierne igualmente a un procedimiento de firma y de control de firma, del cual un modo de realización se describe en la Figura 7 y que puede comprenden etapas de creación de una base de datos de revocación E400, una etapa E500 de implementación del procedimiento de firma ilustrado en la Figura 3 y una etapa E600 de control de firma, estando descritas las etapas E400 y E600 a continuación.

Pudiendo unos miembros adherirse al grupo o quitarse en instantes diferentes, o bien, pudiendo unos miembros perder su capacidad de firma, se puede situar un mecanismo de revocación en el transcurso de la etapa E400. Se puede establecer una lista de revocación para cada dominio y poner al día por la autoridad de gestión 203. Para hacer esto, se construye una lista de revocación RL_j para el dominio D_j a partir de los seudónimos nym_{ij} de los miembros del grupo revocados y se almacena en una base de datos de revocación BD_j. Según un modo de realización de la invención, cuando la autoridad de gestión desea revocar a un miembro M_i del grupo, el servidor de gestión 203s transmite a cada servidor 204s del proveedor de servicio SP_j la segunda parte de la clave secreta x_i del miembro, y cada servidor del proveedor de servicio SP_j calcula los seudónimos nym_{ij} correspondientes y los añade en la lista de revocación RL_j de la base de datos de revocación BD_j.

Como se ilustra en la Figura 8, el procedimiento de control de firma E600 comprende una primera etapa E601 de verificación consistente en controlar, a partir de la firma σ y del seudónimo nym_{ij}, que el miembro M_i tiene conocimiento de la clave de firma secreta sk_i = (f_i, x_i, A_i), es decir que él es un miembro legítimo del grupo, y que el seudónimo y la firma del miembro M_i están vinculados, es decir que dicho seudónimo y dicha firma del miembro M_i son función de una parte de dicha clave de firma secreta. Si esta verificación es positiva, el seudónimo recibido con la clave es con certeza la del firmante.

Según un modo de realización, dicha etapa de verificación comprende un etapa de verificación de prueba en el transcurso de la cual los medios de tratamiento del servidor de control verifican que una prueba de divulgación nula de conocimiento que prueba que el miembro identificado por el seudónimo es el firmante del mensaje (m) es correcta.

Ventajosamente, dicha etapa de verificación de prueba verifica la igualdad de los logaritmos discretos del valor $K = B^{xi}$ en base B y del seudónimo $nym_{ij} = dpk_j^{xi}$ en base dpk_j.

La pertenencia del firmante al grupo es verificable independientemente del seudónimo, y la verificación de que la prueba de que el miembro identificado por el seudónimo es el firmante del mensaje es correcta, es realizada por operaciones distintas a partir de la firma y del seudónimo.

Según una variante del segundo modo de realización, dicha etapa de verificación puede comprender una operación de verificación de dicha firma que permite probar a la vez la pertenencia del miembro (M_i) al grupo y que el miembro identificado por el seudónimo es el firmante del mensaje.

El procedimiento de control E600 puede igualmente comprender una segunda etapa E602 de verificación de revocación consistente en verificar que el miembro M_i no ha sido revocado del grupo.

Más precisamente, en el primer modo de realización de la invención, en el transcurso de la etapa E601, los medios de tratamiento de un servidor de control 205s:

- Verifican que B, J, K, T pertenecen a G_1 y que s_f, s_x, s_a, s_b, s_{x2}, pertenecen a Z_p.
- Calculan $R'_2 = B^{sx}K^{-c}$, $R'_3 = e(T, g_2)^{-sx}\ T_2^{sf}\ T_3^{sb}\ T_4^{sa}\ T_1^{c}\ e(T, w)^{-c}$, $R'_4 = K^{sa}B^{-sb}$, $R'_1 = B^{sf}J^{c}$, $R'_5 = dpk_j^{sx2}nym_{ij}^{-d}$ y $R'_6 = B^{sx2}K^{d}$.
- Verifican que c = H (gpk || B || J || K || T || R'_1 || R'_2 || R'_3 || R'_4 || m) y que d = H (gpk || B || K || dpk_j || nym_{ij} || R'_5 || R'_6).

En este modo de realización, la verificación de la igualdad entre c y H (gpk || B || J || K || T || R'_1 || R'_2 || R'_3 || R'_4 || m) permite probar la pertenencia del miembro al grupo independientemente del seudónimo. Por otra parte, la verificación de la igualdad entre d y H (gpk || B || K || dpk_j || nym_{ij} || R'_5 || R'_6) permite probar que la misma clave secreta ha sido utilizada para generar el seudónimo y la firma.

En el segundo modo de realización de la invención, en el transcurso de la etapa E601, los medios de tratamiento de un servidor de control 205 s:

- Verifican que B, J, K, T pertenecen a G_1 y que s_f, s_x, s_a, s_b, pertenecen a Z_p.
- Calculan $R'_2 = B^{sx}K^{-c}$, $R'_3 = e(T, g_2)^{-sx}\ T_2^{sf}\ T_3^{sb}\ T_4^{sa}\ T_1^{c}\ e(T, w)^{-c}$, y $R'_4 = K^{sa}B^{-sb}$, $R'_1 = B^{sf}J^{c}$.
- Verifican que c = H (gpk || B || J || K || T || R'_1 || R'_2 || R'_3 || R'_4 || R_5 || m).

En este modo de realización, la verificación de la igualdad entre c y H (gpk || B || J || K || T || R'_1 || R'_2 || R'_3 || R'_4 || R_5 || m) permite probar la pertenencia del miembro al grupo independientemente del seudónimo.

A partir del seudónimo, los medios de tratamiento de un servidor de control 205s calculan a continuación $R'_5 = dpk_j^{sx}nym_{ij}^{-c}$ y verifican que c = H (gpk || B || J || K || T || R'_1 || R'_2 || R'_3 || R'_4 || R'_5 || m). Esta verificación permite probar que la misma clave secreta ha sido utilizada para generar el seudónimo y la firma, y por lo tanto, que el miembro identificado por el seudónimo es con certeza el firmante del mensaje.

Según una variante de este segundo modo de realización de la invención, en el transcurso de la etapa E601, los medios de tratamiento de un servidor de control 205s:

- Verifican que B, J, K, T pertenecen a G_1 y que s_f, s_x, s_a, s_b, pertenecen a Z_p.
- Calculan $R'_2 = B^{sx}K^{-c}$, $R'_3 = e(T, g_2)^{-sx}\ T_2^{sf}\ T_3^{sb}\ T_4^{sa}\ T_1^{c}\ e(T, w)^{-c}$, $R'_4 = K^{sa}B^{-sb}$, $R'_1 = B^{sf}J^{c}$ y $R'_5 = dpk_j^{sx}nym_{ij}^{-c}$.
- Verifican que c = H (gpk || B || J || K || T || R'_1 || R'_2 || R'_3 || R'_4 || R'_5 || m).

En esta variante, la verificación de la igualdad entre c y H (gpk || B || J || K || T || R'_1 || R'_2 || R'_3 || R'_4 || R'_5 || m) permite a la vez probar la pertenencia del miembro al grupo y probar que la misma clave secreta ha sido utilizada para generar el seudónimo y la firma.

De este modo, en todos los modos de realización descritos, un verificador puede controlar la pertenencia del firmante del mensaje al grupo sin conocer el secreto de grupo e identificar el firmante por su seudónimo. El verificador puede igualmente controlar que el seudónimo proporcionado con la firma identifica con certeza al firmante.

En un modo de realización de la invención, en el transcurso de la etapa E602, los medios de tratamiento del servidor de control verifican en la base de datos de revocación BD_j que el seudónimo nym_{ij} no pertenece a la lista de revocación RL_j.

Si las dos etapas de verificación E601 y E602 son positivas, entonces la firma y el seudónimo con considerados como válidos.

Para verificar la firma de un mensaje m y el seudónimo del miembro Mi, el servidor de control no tiene necesidad de conocer esta firma y este seudónimo así como los parámetros de dominio dpkj y los parámetros públicos gpk. El servidor de control no tiene, en particular, conocimiento de la clave de firma secreta del miembro Mi. Ningún servidor de control puede, de este modo, firmar un mensaje en lugar del miembro, ni conocer el seudónimo del miembro Mi en diversos dominios y vincular las firmas y seudónimos de este miembro para diferentes dominios. Por lo tanto, y debido a la construcción de los seudónimos: cuando se observan dos seudónimos para dos dominios diferentes, es imposible, gracias a hipótesis de complejidad de ciertos problemas matemáticos, decir si éstos corresponden o no al mismo miembro.

Por otra parte, la lista de revocación no se tiene en cuenta en el transcurso de la firma. Esto permite no tener que renovar las claves de los miembros válidas después de una revocación de un miembro y no implica cálculos suplementarios para el firmante.

Además, en el transcurso de la segunda etapa de verificación, los medios de tratamiento del servidor de control no tienen más que realizar un test de pertenencia a una lista y no un número lineal de operaciones aritméticas como en los mecanismos de firma de grupo conocidos.

Según una variante de la invención, se utilizan listas de miembros válidas en lugar de listas de revocación. En el transcurso de la segunda etapa de verificación, el servidor de control debe entonces verificar que el seudónimo que él verifica pertenece con certeza a la lista de miembros válidos.

Ventajosamente, las bases de datos de almacenamiento de estas listas son almacenadas en los servidores de los proveedores de servicio. Según una variante, las listas son memorizadas en una base de datos común almacenada en el servidor de gestión de claves.

De este modo, el objeto de la invención permite construir firmas utilizando seudónimos y permitiendo a un miembro de un grupo firmar un mensaje en el nombre del grupo, a la vez que tiene una identidad dentro del grupo, sin presentar los inconvenientes de los mecanismos de firma que utilizan seudónimos.

En efecto, este mecanismo de firma es seguro incluso en caso de recuperación y de puesta en común de claves de firma por parte de los miembros del grupo y puede garantizar igualmente que nadie, ni la autoridad de gestión de claves puede firmar un mensaje en lugar de un miembro del grupo.

El mecanismo de firma objeto de la invención puede ser aplicado para realizar, por ejemplo, autentificaciones biométricas anónimas tales como las descritas en la referencia *Bringer, J. Chabanne, H. Pointcheval, D. Zimmer, S. An application of the Boneh and Shacham group signature scheme to biometric authentication. In: Matsuura, K., Fujisaki. E. (eds.) IWSEC. Lecture Notes in Computer Science, vol 5312, pág 219 – 230. Springer (2008)* y puede estar fundada en las firmas de grupo de tipo *"Backward Unlinkability"* como se describe en la referencia *Bringer, J. Patey, A.: VLR group signatures – how to achieve both backward unlinkability and efficient revocation checks. In: SECRYPT*, pág. 215 – 220 (2012) y en la referencia *Nakanishi, T., Funabiki, N.: A short verifier – local revocation group signature scheme with backward unlinkability. In: Yoshiura, H., Sakurai, K., Rannenberg, K.; Murayama, Y., Ichi Kamamura, S. (eds.) IWSEC. Lecture Notes in Computer Science, vol. 4266, pág 17 – 32. Springer (2006)*.

REIVINDICACIONES

1. Un procedimiento de firma de un mensaje (m) llevado a cabo por unos medios de tratamiento de un dispositivo usuario de un miembro (M_i) perteneciente a un grupo de miembros ($\mathcal{G}$) generado por una autoridad de gestión de claves, poseyendo dicho dispositivo usuario una clave de firma secreta (sk_i),

que comprende una etapa de generación (E301) para el mensaje (m) de una firma de grupo (σ) que permite a dicho miembro (M_i) probar su pertenencia al grupo de miembros ($\mathcal{G}$) y una etapa de generación (E302) de un seudónimo (nym_{ij}) que identifica al miembro (M_i) dentro de un dominio (D_j) de un proveedor de servicios (SP_j), comprendiendo dicho dominio un conjunto de terminales en comunicación con un servidor de dicho proveedor de servicios,

estando dicha firma de grupo (σ) construida de manera tal que dicho miembro (M_i) puede probar al firmar el mensaje (m) su conocimiento de dicha clave de firma secreta sin divulgarla,

y caracterizado por que dicha firma de grupo (σ) está construida de manera tal que la pertenencia del miembro (M_l) al grupo es verificable independientemente del seudónimo (nym_{ij}),

y por que la clave de firma secreta (sk_i) del miembro (M_i) comprende por lo menos una primera parte de clave (f_i) generada por los medios de tratamiento del dispositivo usuario de dicho miembro y desconocido por la autoridad de gestión de las claves,

y por que dicho seudónimo y dicha firma son función de una segunda parte (x_i) de dicha clave de firma secreta del miembro (M_i), y están construidos de manera tal que prueban que el miembro identificado por el seudónimo es el firmante del mensaje (m) y por que dicho seudónimo (nym_{ij}) del miembro (M_i) es específico para el dominio (D_j).

2. Procedimiento de firma según la reivindicación anterior caracterizado por que dicha clave de firma secreta (sk_i) es almacenada dentro de un medio de almacenamiento seguro.

3. Procedimiento de firma según una cualquiera de las reivindicaciones anteriores, caracterizado por que previamente a dichas etapas de generación de una firma de grupo y de un seudónimo, dicho procedimiento comprende una etapa (E100) de generación de claves llevada a cabo por un servidor de gestión de claves de la autoridad de gestión de claves, en el transcurso de la cual, unos medios de tratamiento del servidor de gestión:

- generan para el grupo de miembros ($\mathcal{G}$) un conjunto de parámetros públicos (gpk) (E101),

- determinan un parámetro de dominio (dpk_j) específico para el dominio (D_j) (E102) y,

- transmiten este parámetro al proveedor de servicios (SP_j) (E103).

4. Procedimiento de firma según la reivindicación 3 caracterizado por que el parámetro de dominio (dpk_j) es igual a g_1^{rj} siendo r_j un entero y g1 un generador de un grupo G1, siendo g1 un parámetro que es parte del conjunto de parámetros públicos (gpk).

5. Procedimiento de firma según la reivindicación 4 caracterizado por que el entero r_j es determinado por la autoridad de gestión de claves.

6. Procedimiento de firma según una cualquiera de las reivindicaciones 3 a 5 caracterizado por que dicho seudónimo (nym_{ij}) del miembro (M_i) dentro del dominio (D_j) es función del parámetro de dominio (dpk_j) específico del dominio (D_j) determinado por dicho servidor de gestión.

7. Procedimiento de control de una firma de un mensaje (m) y de un seudónimo llevado a cabo por unos medios de tratamiento de un servidor de control, siendo generados (E500) dicha firma (σ) y dicho seudónimo (nym_{ij}) según el procedimiento de una cualquiera de las reivindicaciones anteriores,

comprendiendo una etapa de verificación (E601), a partir de la firma (σ) y del seudónimo (nym_{ij}), del conocimiento por parte del miembro (M_i) de la clave de firma secreta (sk_i) y de que dicho seudónimo y dicha firma del miembro M_i) son función de una segunda parte (xi) de dicha clave de firma secreta, con el fin de probar que el miembro identificado por el seudónimo es el firmante del mensaje (m) y que éste pertenece al grupo de miembros ($\mathcal{G}$).

8. Procedimiento de control según la reivindicación 7, caracterizado por que dicha etapa de verificación comprende una etapa de verificación de prueba, en el transcurso de la cual los medios de tratamiento del servidor de control verifican que una prueba de divulgación nula de conocimiento que prueba que el miembro identificado por el seudónimo es el firmante del mensaje (m) es correcta.

9. Procedimiento de control según la reivindicación 8, caracterizado por que el seudónimo (nym_{ij}) es igual a dpk_j^{xi} siendo x_i dicha segunda parte de la clave de firma secreta del miembro (M_i) y siendo (dpk_j) un parámetro de dominio específico del dominio, y por que dicha firma (σ) comprende un valor K, diferente del seudónimo (nym_{ij}), de la forma B^x_i, siendo B un elemento de un grupo G1 y x_i dicha segunda parte de clave de firma secreta del miembro

(M_i), y por que en dicha etapa de verificación de prueba se verificar la igualdad de los logaritmos discretos del valor K en base B y del seudónimo nym_{ij} en base dpk_j.

10. Procedimiento de control según una cualquiera de las reivindicaciones 8 a 9, caracterizado por que dicha etapa de verificación comprende una verificación de dicha firma para probar la pertenencia del miembro (M_i) al grupo y por que dicha etapa de verificación de prueba es realizada en el transcurso de la verificación de dicha firma.

11. Programa de ordenador que comprende instrucciones de código de programa para la ejecución de las etapas del procedimiento según una cualquiera de las reivindicaciones anteriores, cuando dicho programa es ejecutado en un ordenador.

12. Dispositivo usuario (201) que comprende por lo menos un medio de almacenamiento, un medio de tratamiento y una interfaz de comunicación, caracterizado por que éste está configurado para llevar a cabo un procedimiento según una cualquiera de las reivindicaciones 1 a 6.

13. Servidor de control (205s) que comprende por lo menos un medio de almacenamiento, un medio de tratamiento y una interfaz de comunicación, caracterizado por que éste está configurado para llevar a cabo un procedimiento según una cualquiera de las reivindicaciones 7 a 10.

14. Sistema caracterizado por que éste comprende por lo menos un dispositivo usuario (201) según la reivindicación 12 y por lo menos un servidor de control (205s) según la reivindicación 13.

FIG. 1

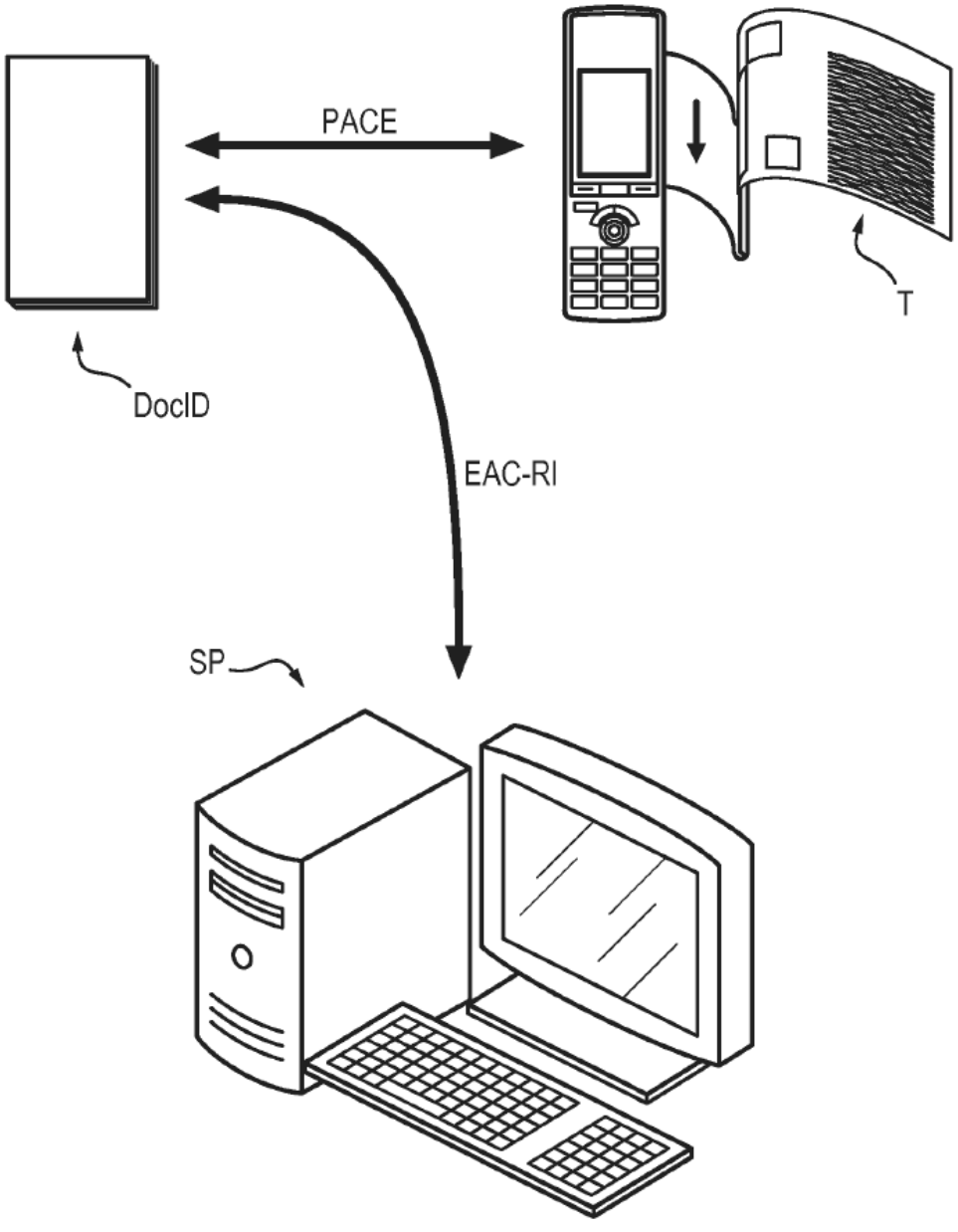


FIG. 2

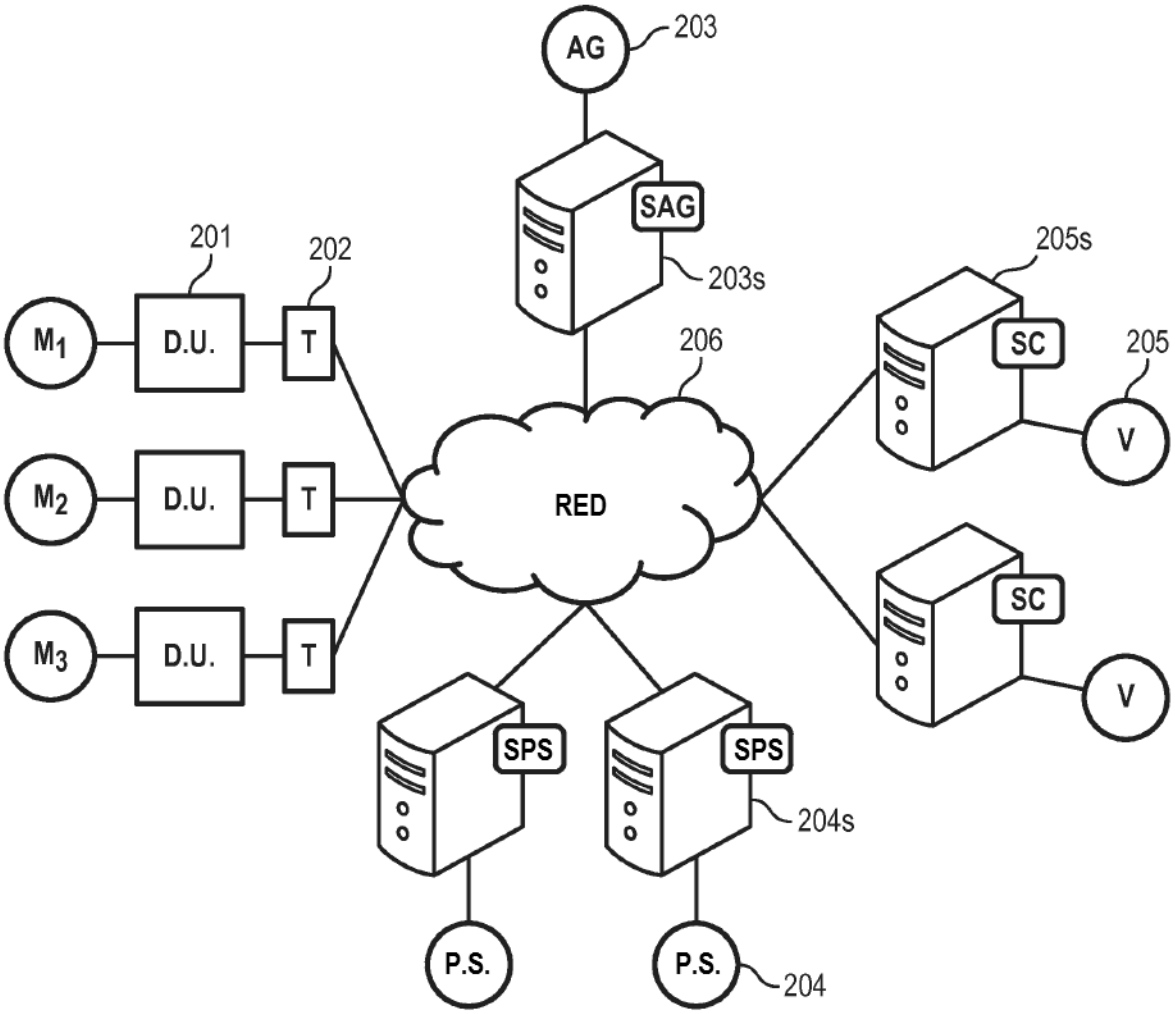

AG
203
SAG
203s
201
202
205s
M1
D.U.
T
206
SC
205
V
M2
D.U.
T
RED
SC
M3
D.U.
T
V
SPS
SPS
204s
P.S.
P.S.
204

FIG. 3

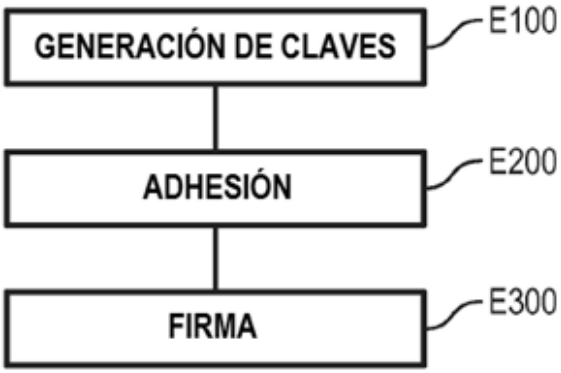

GENERACIÓN DE CLAVES
E100
ADHESIÓN
E200
FIRMA
E300

FIG. 4

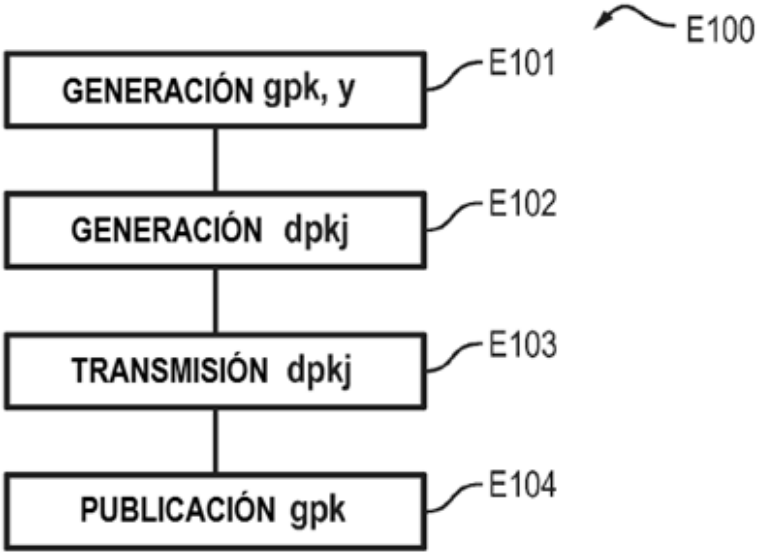

E100
GENERACIÓN gpk, y
E101
GENERACIÓN dpkj
E102
TRANSMISIÓN dpkj
E103
PUBLICACIÓN gpk
E104

FIG. 5

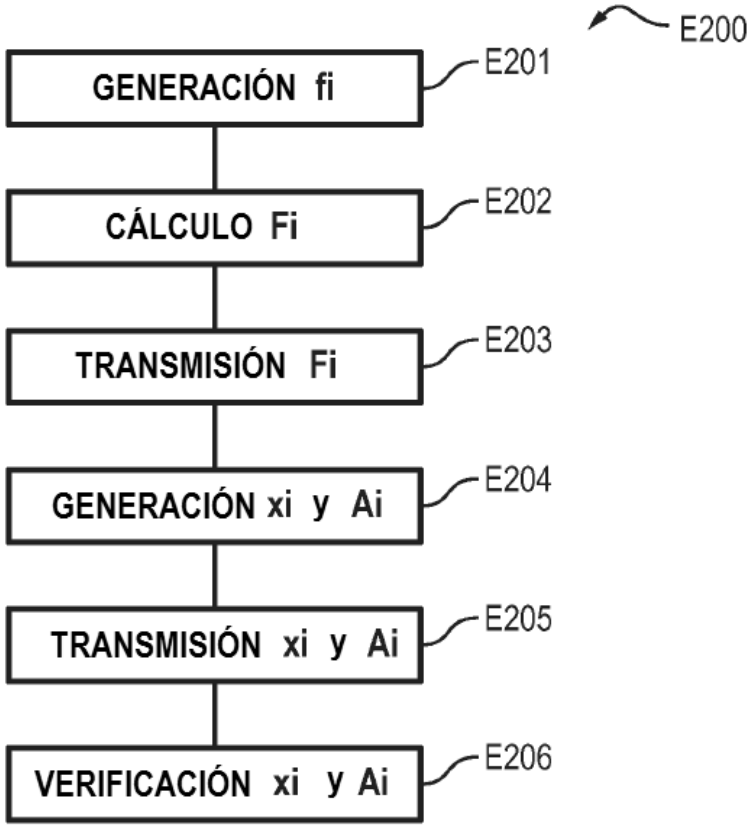

E200
GENERACIÓN fi
E201
CÁLCULO Fi
E202
TRANSMISIÓN Fi
E203
GENERACIÓN xi y Ai
E204
TRANSMISIÓN xi y Ai
E205
VERIFICACIÓN xi y Ai
E206

FIG. 6

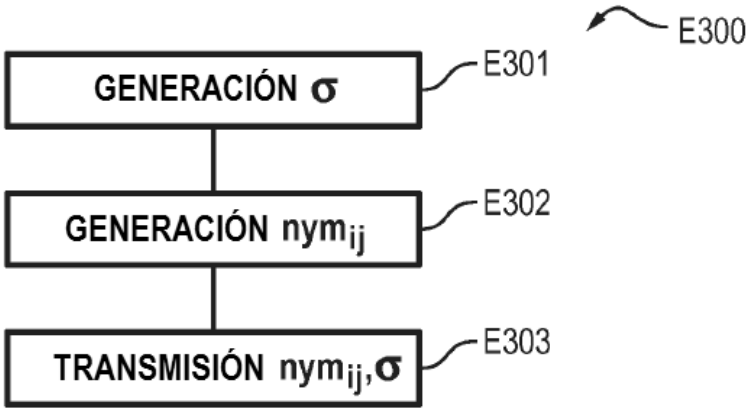

E300
GENERACIÓN σ
E301
GENERACIÓN nym$_{ij}$
E302
TRANSMISIÓN nym$_{ij}$,σ
E303

FIG. 7

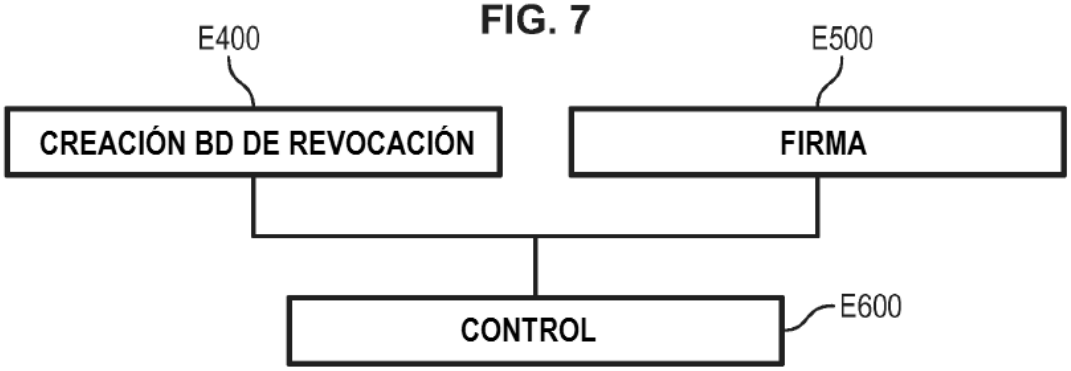
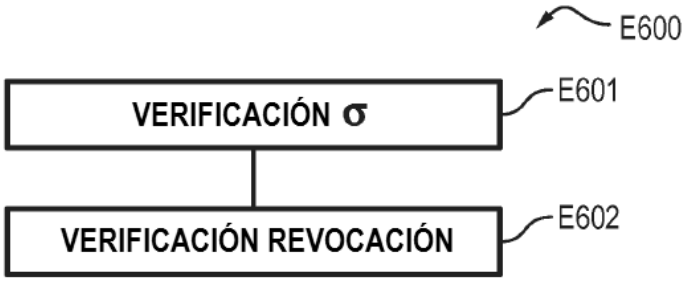

E400
E500
CREACIÓN BD DE REVOCACIÓN
FIRMA
CONTROL
E600

FIG. 8


E600
VERIFICACIÓN σ
E601
VERIFICACIÓN REVOCACIÓN
E602