

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
5 janvier 2012 (05.01.2012)

PCT

(10) Numéro de publication internationale
WO 2012/001272 A1

(51) Classification internationale des brevets :
H04L 29/06 (2006.01) H04L 9/32 (2006.01)

(21) Numéro de la demande internationale :
PCT/FR20 11/05 1441

(22) Date de dépôt international :
23 juin 2011 (23.06.2011)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1002784 30 juin 2010 (30.06.2010) FR

(71) Déposant (pour tous les États désignés sauf US) :
FRANCE TELECOM [FR/FR]; 6 place d'Alleray,
F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants (pour US seulement) : CANARD,
Sébastien [FR/FR]; 15 rue Alexandre Bigot, F-14000
Caen (FR). TRAORE, Jacques [FR/FR]; 23 avenue de la
Suisse Normande, F-61 100 Saint Georges Des Groseillers
(FR).

(74) Mandataire : FRANCE TELECOM
R&D/PIV/BREVETS; RENARD Béatrice, 38-40 rue du
Général Leclerc, F-92794 Issy Moulineaux Cedex 9 (FR).

(81) États désignés (sauf indication contraire, pour tout titre
de protection nationale disponible) : AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ,
CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO,
DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP,
KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD,
ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI,
NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD,
SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR,
TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés (sauf indication contraire, pour tout titre
de protection régionale disponible) : ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG,
ZM, ZW), eurasién (AM, AZ, BY, KG, KZ, MD, RU, TJ,
TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK,
EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU,
LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,

[Suite sur la page suivante]

(54) Title : AUTHENTICATION METHOD THAT STRENGTHENS ANONYMITY BETWEEN AN IDENTITY PROVIDER AND A SERVICE PROVIDER

(54) Titre : PROCÉDE D'AUTHENTIFICATION PERMETTANT DE RENFORCER L'ANONYMAT ENTRE UN FOURNISSEUR D'IDENTITÉS ET UN FOURNISSEUR DE SERVICES

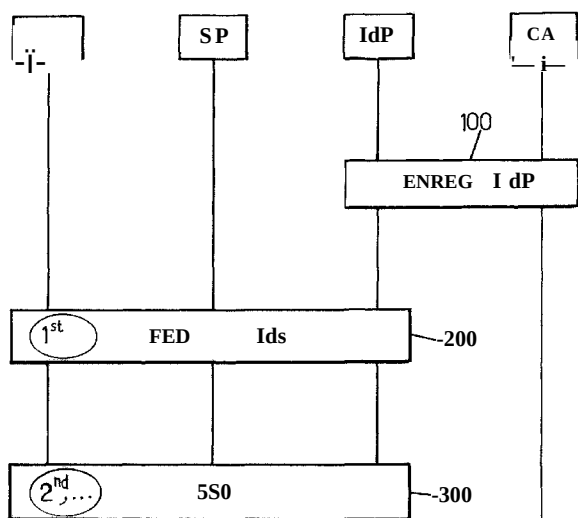


FIG.1 .

(57) Abstract : The invention relates to a method for authenticating a user (U) in relation to at least one service provider (SP), said method comprising the following steps in which: the user sends (223) the service provider a first proof of knowledge (W) of a validity certificate (k) of a public key (t) associated with a secret key (y) used by an identity provider (IdP) in order to sign a first user authentication request; and the service provider verifies (225) said proof of knowledge. The invention also relates to a System for carrying out said method and to a corresponding computer program.

(57) Abrégé : L'invention concerne un procédé d'authentification d'un utilisateur (U) auprès d'au moins un fournisseur de services (SP), ledit procédé comprenant 1 envoi (223), par l'utilisateur au fournisseur de services, d'une première preuve de connaissance (W) d'un certificat de validité (κ) d'une clé publique (t) associée à une clé secrète (y) utilisée par un fournisseur d'identités (IdP) pour signer une première requête d'authentification de l'utilisateur et la vérification (225) de cette preuve de connaissance par le fournisseur de services. L'invention concerne également un système apte à mettre en œuvre un tel procédé ainsi qu'un programme d'ordinateur correspondant.

SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG). **Publiée :**

Déclarations en vertu de la règle 4.17 :

— relative à la qualité d'inventeur (règle 4.1 7.iv)

- avec rapport de recherche internationale (Art. 21(3))
- avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues (règle 48.2.h))

**Procédé d'authentification permettant de renforcer l'anonymat entre un fournisseur
d'identités et un fournisseur de services**

5 La présente invention concerne le domaine de l'authentification, en particulier celui de l'authentification unique d'un utilisateur par un fournisseur d'identités lorsque cet utilisateur requiert l'accès à un fournisseur de services.

10 L'invention trouve une application particulièrement avantageuse dans le domaine des systèmes à authentification unique permettant à un utilisateur disposant de plusieurs identités auprès de plusieurs fournisseurs de service de fédérer ses identités, c'est-à-dire d'établir des liens logiques entre elles, et de bénéficier d'un service d'authentification unique, autrement appelé SSO (pour "Single Sign-On" en anglais) pour accéder aux divers fournisseurs de service sans avoir à s'authentifier plusieurs fois.

15 Les mécanismes d'authentification classiques sur lesquels s'appuie la présente invention supposent que l'utilisateur a préalablement ouvert, auprès du fournisseur d'identités et respectivement auprès des fournisseurs de services, un compte identifié par une identité locale (user@idp, respectivement user@sp) en s'enregistrant sur la base de noms d'utilisateur respectifs, chacun de ces noms d'utilisateur pouvant être, selon la politique respective du fournisseur d'identités et de chaque fournisseur de services, soit le patronyme civil (certifié) de l'utilisateur, 20 soit un pseudonyme.

 L'authentification auprès d'un fournisseur d'identités ou d'un fournisseur de services consiste, pour l'utilisateur, à prouver qu'il est bien l'entité correspondant au nom d'utilisateur sur la base duquel il a ouvert un compte, et pour le fournisseur d'identités ou le fournisseur de services, à se référer, après vérification, à l'identité locale associée à cet utilisateur.

25 Dans l'état de la technique, plusieurs systèmes offrant des fonctionnalités de fédération d'identités ont été initialement proposés, mettant en œuvre un mécanisme consistant pour un utilisateur à s'authentifier une première fois auprès d'un fournisseur d'identités IdP ("Identity Provider" en anglais) et à accéder ensuite à des fournisseurs de services SP ("Service Provider" en anglais) sans devoir s'authentifier à nouveau.

30 Une première famille de solutions de première génération d'authentification unique consiste à mettre en œuvre une identité locale unique partagée par le fournisseur d'identités et les différents fournisseurs de services. Des systèmes d'authentification unique tels que Tivoli Access Manager d'IBM s'appuient sur ce type d'approche. Un inconvénient de ces systèmes est que le fournisseur d'identités et les différents fournisseurs de services, qui disposent de l'identité unique de 35 l'utilisateur, peuvent alors croiser leurs bases de données clients et donc porter atteinte à la vie privée des utilisateurs.

Une seconde famille de solutions de première génération d'authentification unique consiste à mettre en œuvre une fédération d'identités. L'utilisateur a des identités différentes (autrement appelées alias) chez le fournisseur d'identités et les différents fournisseurs de services, et l'utilisateur établit des liens logiques entre ces différentes identités de sorte que l'ensemble constitue
5 in fine une identité logiquement unique mais physiquement distribuée.

Des standards tels que Liberty de l'Alliance Liberty ou SAML de l'OASIS définissent des mécanismes de fédération d'identités et d'authentification unique entre services s'appuyant sur une telle fédération d'identités.

Les mécanismes spécifiés par l'Alliance Liberty ou l'OASIS permettent aux utilisateurs de
10 fédérer leurs identités dynamiquement et en ligne. Ils permettent également à un fournisseur de services de bénéficier d'une identité certifiée et délivrée par un fournisseur d'identités et donc d'affranchir l'utilisateur souhaitant consommer un service d'une nouvelle phase d'authentification.

Lorsqu'un utilisateur se connecte pour la première fois à un fournisseur de services pour s'authentifier auprès de ce fournisseur de services, il se voit offrir la possibilité de fédérer son
15 identité chez le fournisseur de services avec son identité chez un fournisseur d'identités.

Contrairement à l'approche adoptée par des produits de la première famille de solutions ci-avant (Tivoli Access Manager d'IBM par exemple), les standards Liberty et SAML n'imposent pas aux fournisseurs d'identités de fournir l'identité locale d'un utilisateur. Au contraire, les fournisseurs d'identités peuvent, à la place, fournir une référence, appelée « alias de fédération »,
20 associée à cet utilisateur, l'alias de fédération fourni par le fournisseur d'identités pour un utilisateur étant différent pour chaque fournisseur de services.

Dans une fédération d'identités, chaque entité, que ce soit le fournisseur d'identités ou les fournisseurs de services, crée pour chaque utilisateur une table de correspondance entre l'identité locale de l'utilisateur et les alias respectifs utilisés par chacune des autres entités. L'authentification
25 unique est alors possible une fois que les identités d'un utilisateur chez le fournisseur d'identités et chaque fournisseur de services sont fédérées.

Du point de vue de l'utilisateur, l'authentification unique est réalisée quand l'utilisateur s'authentifie auprès d'un fournisseur d'identités et accède à plusieurs fournisseurs de services affiliés sans avoir à s'authentifier à nouveau. Cet avantage est obtenu après avoir fédéré les
30 identités locales de l'utilisateur entre le fournisseur d'identités et les divers fournisseurs de services.

Les standards de Liberty et de l'OASIS offrent donc un mécanisme de SSO garantissant un premier niveau de respect de la vie privée. En effet, dans le mécanisme de fédération d'identités qu'ils proposent, un fournisseur d'identités fournit un alias de fédération différent pour chaque fournisseur de services. Les fournisseurs de services ne peuvent donc pas utiliser ces alias pour
35 croiser leurs bases de données clients afin d'obtenir des informations sur les pratiques et les habitudes des utilisateurs en termes d'accès à des services.

En revanche, le fournisseur d'identités dispose, quant à lui, de tous les alias de fédération, et donc des informations nécessaires et suffisantes pour pouvoir recouper les bases clients. Cette opération de recoupement frauduleuse peut être réalisée à l'initiative du fournisseur d'identités lui-même ou d'un tiers ayant réussi à accéder aux données détenues par le fournisseur d'identités.

5

Afin de répondre à cet inconvénient, une deuxième génération de solutions a été proposée par la suite permettant de garantir un deuxième niveau, plus élevé, de protection de la vie privée. Une telle solution est décrite dans la demande PCT WO 2008/113951. Cette deuxième génération de solutions consiste à permettre aux utilisateurs de fédérer leurs identités sans que ni les fournisseurs d'identités, ni les fournisseurs de services, n'aient les informations leur permettant de croiser leurs bases de données client.

10

Cette deuxième génération de solutions s'appuie sur le concept de signature aveugle introduit par Chaum à la conférence Crypto'83. Un schéma de signature aveugle est un protocole mettant en jeu deux entités : un utilisateur et un signataire. Il permet à l'utilisateur d'obtenir du signataire la signature d'un message donné, sans que ce dernier n'apprenne quoi que ce soit à propos du message.

15

Dans le contexte de l'authentification unique, l'utilisation d'un schéma de signature aveugle permet de gérer et de contrôler la table de fédération d'identités du côté client, tout en maintenant le mécanisme d'authentification du côté réseau, par un fournisseur d'identités.

20

Cependant, avec cette deuxième génération de solutions, le fournisseur d'identités dispose d'une parfaite connaissance de l'identité des fournisseurs de services auxquels accède un utilisateur et peut donc ainsi corréler tous les centres d'intérêt d'un utilisateur en particulier. De même, le fournisseur de services connaît le fournisseur d'identités.

Il manque donc aux mécanismes de gestion de l'identité décrits ci-avant un mécanisme de fédération d'identités et de SSO dans lequel la vie privée de l'utilisateur est totalement sauvegardée en renforçant l'anonymat réciproque entre un fournisseur de services et un fournisseur d'identités utilisés par un utilisateur lors d'une authentification unique.

25

La présente invention a pour objet d'améliorer la situation.

30

Elle propose à cette effet un procédé d'authentification d'un utilisateur auprès d'au moins un fournisseur de services, ledit procédé comprenant l'envoi, par l'utilisateur au fournisseur de services, d'une première preuve de connaissance d'un certificat de validité d'une clé publique associée à une clé secrète utilisée par un fournisseur d'identités pour signer une première requête d'authentification de l'utilisateur et la vérification de cette preuve de connaissance par le fournisseur de services.

35

Grâce à l'envoi d'une telle preuve de connaissance, au lieu de l'envoi de la signature ou de la clé publique qui révéleraient l'identité du fournisseur d'identités, il est possible de garantir l'anonymat de ce fournisseur d'identités auprès du fournisseur de services, et de renforcer ainsi l'anonymat réciproque entre ces deux fournisseurs.

Avantageusement, l'envoi et la vérification de la première preuve de connaissance ont lieu durant une étape de fédération d'identités qui comprend, en outre :

- l'envoi au fournisseur d'identités d'un alias aveuglé calculé à partir d'un alias de l'utilisateur ;

- le calcul par l'utilisateur de la première preuve de connaissance à partir d'une signature partielle calculée par le fournisseur d'identités à partir de l'alias aveuglé et de la clé secrète ;

- l'envoi au fournisseur de services de l'alias de l'utilisateur avec la première preuve de connaissance.

Une telle étape de fédération d'identités permet alors d'obtenir un procédé d'authentification unique.

Avantageusement, la première preuve de connaissance est calculée en outre à partir de la clé publique et d'au moins une partie du certificat de validité.

De façon particulièrement avantageuse, la première preuve de connaissance comprend au moins une première valeur masquée calculée à partir de la clé publique, une deuxième valeur masquée calculée à partir d'au moins une partie du certificat de validité et une troisième valeur masquée calculée à partir de la signature partielle.

Dans un mode de réalisation avantageux, le procédé comprend une étape préliminaire d'enregistrement, préalable à la fédération d'identités, du fournisseur d'identités auprès d'une autorité de certification comprenant l'envoi par l'autorité de certification au fournisseur d'identités du certificat de validité calculé à partir d'au moins un engagement envoyé par le fournisseur d'identités. Ceci permet de certifier la validité de la signature effectuée par le fournisseur d'identités par le biais d'une autorité tiers.

Avantageusement, l'engagement envoyé par le fournisseur d'identités est un engagement sur un premier élément choisi aléatoirement par le fournisseur d'identités.

De manière particulièrement avantageuse, la clé secrète utilisée par le fournisseur d'identités comprend le premier élément choisi aléatoirement par le fournisseur d'identités ainsi qu'un deuxième élément choisi aléatoirement par l'autorité de certification.

Avantageusement, lors de l'étape de fédération d'identités, la requête d'authentification comprend au moins une partie aveuglée par l'utilisateur, une desdites au moins une partie aveuglée comprenant l'identité du fournisseur de services.

Dans un mode de réalisation avantageux où le procédé comprend au moins une étape ultérieure d'authentification, chaque étape ultérieure d'authentification comprend l'envoi d'une nouvelle preuve de connaissance obtenue à partir d'une signature partielle calculée par le

fournisseur d'identités à partir d'un nouvel alias aveuglé et de la clé secrète, suivi de la vérification de ladite nouvelle preuve de connaissance par le fournisseur de services.

De manière avantageuse, pour chaque étape ultérieure d'authentification, la nouvelle preuve de connaissance est calculée de sorte à être différente de la première preuve de connaissance calculée lors de la fédération d'identités et, si le procédé comprend plusieurs étapes ultérieures d'authentification, des nouvelles preuves de connaissance calculées lors des autres étapes ultérieures d'authentification.

Avantageusement, la première preuve de connaissance est calculée en fonction d'une première et une deuxième variables aléatoires et la nouvelle preuve de connaissance est calculée en fonction d'une première et une deuxième variables aléatoires ultérieures, lesdites première et deuxième variables aléatoires ultérieures étant choisies pour être différentes desdites première et deuxième variables aléatoires et, si le procédé comprend plusieurs étapes ultérieures d'authentification, des première et deuxième variables aléatoires ultérieures (r_i^*) choisies lors des autres étapes ultérieures d'authentification.

Avantageusement, un message d'authentification comprenant un alias aveuglé de l'utilisateur est envoyé au fournisseur de services à chaque étape ultérieure d'authentification, et chaque étape ultérieure d'authentification comprend l'aveuglement de l'alias de l'utilisateur de sorte que l'alias aveuglé obtenu soit différent de l'alias aveuglé obtenu lors de l'étape de fédération d'identités et, si le procédé comprend plusieurs étapes ultérieures d'authentification, des autres alias aveuglés obtenus lors des autres étapes ultérieures d'authentification.

Avantageusement, l'alias aveuglé obtenu lors de l'étape de fédération d'identités est calculé en fonction de l'alias de l'utilisateur et d'une variable aléatoire, et l'alias aveuglé obtenu lors d'une étape ultérieure d'authentification est calculé en fonction de l'alias de l'utilisateur et d'une variable aléatoire ultérieure, ladite variable aléatoire ultérieure étant choisie pour être différente de ladite variable aléatoires et, si le procédé comprend plusieurs étapes ultérieures d'authentification, des variables aléatoires ultérieures choisies lors des autres étapes ultérieures d'authentification.

La présente invention propose en outre un système d'authentification à anonymat renforcé comprenant au moins un utilisateur, au moins un fournisseur de services, un fournisseur d'identités et une autorité de certification, ce système étant apte à mettre en œuvre le procédé d'authentification ci-avant lorsqu'un desdits au moins un utilisateur requiert un service auprès d'un desdits au moins un fournisseur de services.

La présente invention propose également un programme d'ordinateur, téléchargeable via un réseau de télécommunication et/ou stocké dans une mémoire d'une unité centrale et/ou stocké sur un support mémoire destiné à coopérer avec une unité centrale, ce programme d'ordinateur étant apte à mettre en œuvre le procédé d'authentification ci-avant.

Le procédé d'authentification, objet de l'invention, sera mieux compris à la lecture de la description et à l'observation des dessins ci-après dans lesquels :

- la figure 1 illustre les étapes d'un procédé d'authentification permettant un anonymat renforcé entre un fournisseur d'identités et un fournisseur de services selon la présente invention ;

5 - la figure 2 illustre un mode de réalisation des sous-étapes composant une étape préliminaire d'enregistrement selon la présente invention ; et

- la figure 3 illustre les sous-étapes d'une étape de fédération d'identité 200 selon la présente invention.

10 On se réfère tout d'abord à la **figure 1** sur laquelle sont illustrées les étapes d'un procédé d'authentification permettant de renforcer l'anonymat entre un fournisseur d'identités et un fournisseur de services.

 Ce procédé d'authentification se déroule dans un système d'authentification à anonymat renforcé comprenant au moins un utilisateur U, au moins un fournisseur de services SP, un fournisseur d'identités IdP ainsi qu'une autorité de certification CA. A titre purement illustratif, un
15 seul utilisateur U et un seul fournisseur de services sont indiqués sur la figure 1, bien qu'un nombre quelconque d'utilisateurs et/ou de fournisseurs de services puisse être concerné par le procédé de la présente invention.

 Dans ce procédé, une étape préliminaire d'enregistrement d'un fournisseur d'identités est
20 tout d'abord effectuée (étape 100). Une telle étape préliminaire peut intervenir lors de l'initialisation du système d'authentification, lorsqu'une entité souhaite devenir un fournisseur d'identités IdP ou lorsqu'un fournisseur d'identités IdP souhaite fournir à l'un de ses clients un service de protection de la vie privée.

 Cette étape préliminaire d'enregistrement comprend un certain nombre d'interactions entre
25 un fournisseur d'identités IdP, dont le rôle est d'authentifier l'utilisateur U lorsque celui-ci cherche à accéder au fournisseur de services SP, et une autorité de certification CA dont le rôle est de certifier la validité d'une signature calculée par le fournisseur d'identités IdP à partir d'un message d'authentification reçu de l'utilisateur et destiné au fournisseur de services.

 A l'issue de cette étape préliminaire d'enregistrement, le fournisseur d'identités IdP reçoit de
30 l'autorité de certification CA un certificat de validité κ d'une clé publique t associée à une clé secrète y utilisée par le fournisseur d'identités IdP pour signer les messages de l'utilisateur U.

 Par la suite, une étape de fédération d'identité (étape 200) a lieu, durant laquelle le fournisseur d'identités IdP utilise sa clé secrète y pour signer un message d'authentification de l'utilisateur.

35 Durant cette étape de fédération d'identités, après l'obtention de la signature du message d'authentification de l'utilisateur par le fournisseur d'identités, l'utilisateur U calcule une preuve de connaissance W du certificat de validité κ de la clé publique t associée à la clé secrète y utilisée par

le fournisseur d'identités IdP pour signer le message d'authentification de l'utilisateur U. L'utilisateur U l'envoie ensuite au fournisseur de services SP avec le message d'authentification, afin que celui-ci puisse authentifier l'utilisateur U en vérifiant ladite preuve de connaissance.

Le fournisseur de services SP n'a ainsi pas accès directement à l'identité du fournisseur d'identités IdP, dont l'anonymat est préservé. En effet, la preuve de connaissance calculée par l'utilisateur prouve que la signature du message d'authentification provient d'un fournisseur d'identités valide sans pour autant révéler d'éléments de cette signature.

Une fois les identités fédérées, lorsque l'utilisateur cherche à nouveau à accéder au fournisseur de services, une étape ultérieure d'authentification (étape 300) est alors effectuée, sur la base d'une nouvelle requête d'authentification, cette étape se déroulant toujours sans que le fournisseur de services SP n'ait directement accès à l'identité du fournisseur d'identités IdP, dont l'anonymat est toujours préservé. Bien qu'une seule étape ultérieure d'authentification soit illustrée sur la figure 1, un nombre quelconque d'étapes ultérieures d'authentification successives peuvent avoir lieu.

On se réfère maintenant à la **figure 2**, qui illustre un mode de réalisation des sous-étapes de l'étape préliminaire d'enregistrement 100.

Comme indiqué précédemment, cette étape préliminaire d'enregistrement comprend un certain nombre d'interactions entre un fournisseur d'identités IdP et une autorité de certification CA.

L'autorité de certification CA dispose d'une paire de clés publique/secrète (capk, cask) pour un algorithme de signature, par exemple un algorithme de signature avec extensions tel que décrit dans l'article « Signature schemes and anonymous credentials from bilinear maps. », de Camenisch et Lysyanskaya.

On peut par exemple choisir la clé secrète cask telle que $cask = \gamma \in Z_p^*$, où p est un nombre premier et la clé publique capk telle que $capk = g_2^\gamma$ où g_2 est un générateur d'un groupe G d'ordre p. Des générateurs g_1 et h de ce groupe G peuvent également être choisis.

Dans cette étape préliminaire d'enregistrement, un schéma de signature avec extensions va être employé afin de permettre à un signataire, en l'espèce le fournisseur d'identités IdP, de signer des valeurs qui lui parviennent sous une forme engagée.

Cette étape préliminaire d'enregistrement peut alors se dérouler de la façon suivante :

1) Le fournisseur d'identités IdP choisit aléatoirement, dans Z_p^* , un élément y' et calcule un engagement C sur cet élément tel que $C = h^{y'}$ dans le groupe G (sous-étape 101).

2) Le fournisseur d'identités IdP calcule une preuve PoK de connaissance du logarithme discret y' de l'engagement C en base y' (sous-étape 103).

5 3) Le fournisseur d'identités IdP envoie à l'autorité de certification CA l'engagement C et la preuve PoK. Cet envoi peut s'accompagner, de façon avantageuse, d'une authentification forte auprès de l'autorité de certification CA, par exemple une authentification à base de défi réponse mise en œuvre au moyen d'un certificat d'authentification octroyé au fournisseur d'identités IdP dans le cadre d'une infrastructure à clés publiques, ou PKI (sous-étape 105).

10 4) L'autorité de certification CA choisit aléatoirement, dans Z_p^* , un élément y'' et calcule un deuxième engagement C sur cet élément y'' tel que $C = C'h^{y''}$ dans le groupe G (sous-étape 107). Ce deuxième engagement se trouve être finalement un engagement sur un élément $y = y' + y''$, qui se trouve être ainsi calculé conjointement par le fournisseur d'identités IdP et l'autorité de certification CA, mais n'est connu que par le fournisseur d'identités IdP. L'élément y servira à celui-ci de clé secrète de signature.

5) L'autorité de certification CA calcule la signature κ de l'engagement C au moyen de la procédure SIGN de signature avec extensions de cet engagement, en utilisant la clé secrète ask .

20 Ceci peut être fait, par exemple, en choisissant aléatoirement, dans Z_p^* , un premier élément a et en calculant un deuxième élément A tel que $A = (g^a)^{\frac{1}{\gamma+\alpha}}$ (sous-étape 109).

La signature κ correspond alors à la paire d'éléments (A, a) .

Cette signature κ correspond à un certificat de validité de la clé publique t de signature du fournisseur d'identités IdP, délivré par l'autorité de certification CA et peut servir à prouver à des tiers la validité de cette clé publique t .

6) L'autorité de certification CA envoie alors au fournisseur d'identités l'élément y'' et la signature $\kappa = (A, a)$ (sous-étape 111).

30 7) Le fournisseur d'identités IdP calcule alors la clé privée de signature $y = y' + y'' \pmod{p}$ (sous-étape 113).

8) Le fournisseur d'identités IdP vérifie au moyen de la clé publique $capk$ que la signature κ est bien la signature de l'élément y (sous-étape 115).

Cette vérification peut se faire, par exemple, au moyen de l'équation suivante :

$$(1) \quad e(A, \text{capk} \cdot g_2^\alpha) = e(g_1, g_2) \cdot e(h, g_2)^y$$

où e est une application bilinéaire de $G \times G \rightarrow G_T$, avec G_T un groupe d'ordre p .

5 A l'issue de ces sous-étapes, le fournisseur d'identités IdP dispose d'une clé secrète de signature y et d'une clé publique t de vérification de signature telle que $t = h^y$.

Cette clé publique t est associée à un certificat de validité $\kappa = (A, a)$ calculé par l'autorité de certification CA.

10 Le couple (t, K) , qui vérifie la formule $\kappa = \text{SIGN}_{CA}(t)$ est public et accessible à tous, au même titre que l'ensemble des autres couples d'éléments des fournisseurs d'identités préalablement enregistrés.

On se réfère maintenant à la **figure 3**, qui illustre les sous-étapes de l'étape de fédération d'identités 200.

15 Lorsqu'un utilisateur U souhaite accéder à un service proposé par un fournisseur de services SP, il souhaite mettre en œuvre un processus d'authentification unique à l'aide de son fournisseur d'identités IdP préalablement enregistré auprès d'une autorité de certification comme décrit précédemment.

20 Conformément à un schéma d'authentification unique, lorsque l'utilisateur U souhaite accéder pour la première fois à un service du fournisseur de services SP, une étape de fédération d'identités 200 a lieu afin que l'utilisateur U puisse fédérer dans un premier temps ses identités chez le fournisseur de services SP et chez le fournisseur d'identités IdP.

25 Dans la présente invention, à la différence de ce qui a été décrit dans l'état de la technique précédemment discuté, le fournisseur de services SP ne prend pas connaissance de l'identité du fournisseur d'identités IdP lors de cette étape de fédération d'identités. Le fournisseur de services SP est simplement convaincu, au moyen d'une preuve, qu'un fournisseur d'identités IdP, dont l'identité a été certifiée par l'autorité de certification CA, a bien authentifié l'utilisateur U conformément aux besoins de l'authentification unique.

30 On utilise ici un schéma de signature aveugle, mis en œuvre par le fournisseur d'identités IdP, d'un message d'authentification msg divisé en trois parties M , m et m^* .

Cette étape 200 de fédération d'identités peut alors se dérouler de la façon suivante :

1) L'utilisateur U requiert l'accès à un service du fournisseur de services SP, au moyen d'une première requête d'accès $\text{REQ}(\text{SERV})$ (sous-étape 201 d'envoi d'une requête d'accès).

2) Suite à la réception de cette première requête d'accès REQ(SERV), le fournisseur de services SP envoie une requête d'authentification REQ(AUTH) signée afin que l'utilisateur U entame les démarches pour s'authentifier (sous-étape 203 d'envoi d'une requête d'authentification).

5

3) Après réception de cette requête d'authentification, l'utilisateur U construit un message d'authentification msg lors d'une sous-étape 204 de construction de message d'authentification.

Ce message d'authentification msg comprend :

- une première partie M rassemblant des éléments non-aveuglés, comme par exemple des balises SAML, l'identité du fournisseur de services SP, le nom de l'algorithme de signature, ou d'autres champs et/ou attributs d'une requête SAML qui ne permettent pas de relier la requête finale à la requête d'authentification,

- une deuxième partie m rassemblant des éléments aveuglés variables d'un accès à un autre, telles que la date de la requête ou l'identifiant de requête, et

- une troisième partie m* comprenant les éléments aveuglés invariants d'un accès à un autre, à savoir l'alias de l'utilisateur, e.g. $m^*=h^s$.

Ce message d'authentification msg peut ainsi consister en la concaténation de ces trois parties telles que $msg = M \parallel m \parallel m^*$.

20

4) Lors d'une sous-étape 205 d'aveuglement, l'utilisateur U aveugle alors la deuxième partie m en calculant un premier élément aveuglé c tel que $c = h_1^{H(m)} h_4^r$ et aveugle la troisième partie m* en calculant un deuxième élément aveuglé c* tel que $c^* = h^s h_4^{r^*}$.

Ces deux éléments aveuglés vont permettre la signature par le fournisseur d'identités IdP sans que celui-ci n'ait accès aux deux parties m et m*.

25

5) Ensuite, lors d'une sous-étape 207 de calcul de preuves de connaissance, l'utilisateur U calcule une première preuve V de connaissance de la représentation $(H(m), r)$ du premier élément aveuglé c en bases (h_1, h_4) . L'utilisateur calcule également une deuxième preuve V* de connaissance de la représentation (s, r^*) du deuxième élément aveuglé c* en bases (h, h_4) .

30

6) Une fois tous ces éléments obtenus, l'utilisateur U envoie au fournisseur d'identités IdP la première partie M du message msg, les premier et deuxième éléments aveuglés c et c*, ainsi que leurs preuves respectives de connaissance V et V* (sous-étape d'envoi 209).

35

Cet envoi peut avantageusement s'accompagner de l'authentification de l'utilisateur auprès du fournisseur d'identités IdP, selon une méthode choisie par ce dernier, pour les besoins de la

signature aveugle aussi bien que pour la fédération d'identités, dans la mesure où le fournisseur d'identités IdP a pour rôle d'authentifier l'utilisateur U.

A l'issue de cette étape, le fournisseur d'identités IdP peut associer, dans sa base de
5 fédération, l'alias aveuglé c^* de l'utilisateur U chez le fournisseur de services SP à un compte local $user@idp$ de l'utilisateur chez le fournisseur d'identités IdP.

7) Après réception des éléments M, c, c^*, V et V^* , le fournisseur d'identités IdP calcule une
10 valeur d'engagement C'' contenant des engagements sur M, m, m^* ainsi qu'une valeur dite de randomisation r^*+r . Pour ce faire, le fournisseur d'identités IdP choisit aléatoirement une valeur w et calcule la valeur d'engagement C'' telle que $C'' = cc^* h_2^{H(m)} h_3^w$ dans G (sous-étape de calcul 211). Il est avantageux d'utiliser ici une valeur aléatoire w afin de renforcer la sécurité du processus.

8) Une fois la valeur d'engagement C'' calculée, une sous-étape 213 d'obtention d'une
15 signature partielle S sur cette valeur d'engagement C'' a lieu. Cette signature partielle S est obtenue en utilisant un processus de signature $SIGN$ avec extensions de l'engagement C'' telle que décrit, par exemple, dans « A client-side approach for privacy-preserving identity fédération » de S. Canard et al.

20 Par exemple, cette signature S peut être calculée telle que $S = (g_1 C)^{\frac{1}{r^*+r}}$, avec k choisi aléatoirement dans Z_p^* .

La signature de l'engagement C'' correspond alors au triplet (S, w, k) .

9) Une fois la signature (S, w, k) de l'engagement C'' obtenue, le fournisseur d'identités IdP
25 envoie cette signature (S, w, k) de l'engagement C'' à l'utilisateur U lors d'une sous-étape 215 d'envoi de signature d'engagement.

10) Après réception de cette signature (S, w, k) de l'engagement C'' , l'utilisateur U peut
30 composer une signature σ telle que $\sigma = (S, w, k, r^*+r)$ (sous-étape 217 d'obtention de la signature σ).

11) Peut alors s'ensuivre une sous-étape 219 de vérification de cette signature finale.

Une telle vérification peut être faite en vérifiant que la relation
 $C = m^* h_1^{fl(m)} h_2^{H(m)} h_3^w h_4^{r^*+r}$ est vérifiée.

Cette vérification peut en outre comporter la vérification de l'équation suivante :

$$(2) \quad e(S, t \cdot g_2^k) = e(g_1, g_2) \cdot e(m^*, g_2) \cdot e(h_1, g_2)^{H(m)} \cdot e(h_2, g_2)^{H(m)} \cdot e(h_3, g_2)^w \cdot e(h_1, g_2)^{r^*+r}$$

12) A l'issue de cette étape 219, l'utilisateur U dispose donc d'une signature σ telle que $\sigma = (S, w, k, r^*+r)$ de son message msg tel que msg = (M, m, m*), ainsi que de ce message msg en tant que tel.

Il ne peut cependant pas transmettre au fournisseur de services SP la signature σ en tant que telle sans révéler l'identité du fournisseur d'identités IdP. Il ne peut pas non plus lui envoyer la clé publique t, pourtant nécessaire à la vérification de cette signature, car cela reviendrait également à révéler l'identité du fournisseur d'identités IdP.

13) Afin de conserver l'anonymat du fournisseur d'identités IdP, l'utilisateur U produit alors une preuve W de connaissance de la signature σ , sans révéler les éléments (S, w, k, r*+r) de cette signature proprement dite, tout en révélant le message msg = (M, m, m*).

Cette preuve W de connaissance sert également à prouver la connaissance de la clé publique t et du certificat de validité de la signature κ , sans révéler ces deux valeurs.

La preuve W de connaissance peut ainsi être calculée telle que :

$$W = \text{POK}(r, t, \sigma : \kappa = \text{SIGN}_{AC}(t) \wedge \sigma = \text{SIGN}_{IdP}(m^* || m || M))$$

Le calcul de cette preuve W de connaissance peut se dérouler de la façon suivante (sous-étape de calcul 221) :

- une première variable masquée associée à la clé publique t est calculée à partir de la clé publique t comme suit :

$$C_t = t z^{v_t} \text{ et } \tilde{C}_t = g^{v_t} z^{w_t}, \text{ où } v_t \text{ et } w_t \text{ sont des valeurs aléatoires ;}$$

- une deuxième variable masquée associée à l'élément A du certificat κ est calculée à partir de cet élément A comme suit :

$$C_A = A z^{v_A} \text{ et } \tilde{C}_A = g^{v_A} z^{w_A}, \text{ où } v_A \text{ et } w_A \text{ sont des valeurs aléatoires ;}$$

- une troisième variable masquée associée à la signature partielle S appartenant à la signature σ est calculée à partir de cette signature partielle S comme suit :

$$C_s = S z^{v_s} \text{ et } \tilde{C}_s = g^{v_s} z^{w_s}, \text{ où } v_s \text{ et } w_s \text{ sont des valeurs aléatoires ;}$$

- les trois autres variables masquées suivantes sont également calculées :

$$\tilde{C}_A^\alpha = g^{v_A^\alpha} z^{w_A^\alpha}$$

$$\tilde{C}_s^k = g^{v_s^k} z^{w_s^k}$$

$$\tilde{C}_s^{v_t} = g^{v_s^{v_t}} z^{w_s^{v_t}}$$

Parmi ces trois variables masquées supplémentaires, la quatrième variable masquée $\tilde{C}_A''$ est associée à la variable A du certificat κ (et dépend de celle-ci), et la cinquième variable masquée $\tilde{C}_g^k$ ainsi que la sixième variable masquée $\tilde{C}_g^{v_i}$ sont associées à la signature partielle S (et dépendent de celles-ci).

5 La preuve de connaissance W comprend alors au moins les six variables masquées $C_t, C_s, C_A, \tilde{C}_A'', \tilde{C}_g^k, \tilde{C}_g^{v_i}$ telles que calculées précédemment.

14) Une fois calculée, la preuve W de connaissance est alors envoyée par l'utilisateur U au fournisseur de services SP, lors d'une étape 223 de transmission de preuve de connaissance.

10 Ainsi, le fournisseur de services SP ne reçoit pas directement la clé publique t, le certificat κ et la signature σ , ce qui ne lui permet pas de retrouver l'identité du fournisseur d'identités IdP. Cependant, les variables masquées reçues, associées à l'un de ces trois éléments, permettent de vérifier la connaissance de ces trois éléments par l'utilisateur.

L'envoi de cette preuve de connaissance W s'accompagne de l'envoi du message d'authentification msg. La partie m^* de ce message, à savoir l'alias de l'utilisateur U, peut alors être associé à un compte local user@sp dans une base de clients du fournisseur de services, ce qui permet la fédération d'identités entre les comptes locaux du fournisseur d'identités IdP et du fournisseur de services SP. La fédération est gérée par l'utilisateur U afin de préserver l'anonymat de celui-ci auprès de ces deux entités.

20

15) Ainsi, suite à la réception de la preuve W de connaissance, la vérification de la preuve de connaissance W est effectuée, lors d'une sous-étape 225 de vérification, par le fournisseur de services.

25 Cette vérification de la preuve de connaissance peut comprendre la vérification des équations (1) et (2) telles que définies précédemment.

Avec les variables masquées appartenant à la preuve de connaissance reçue par le fournisseur de services SP, les équations (1) et (2) précédentes peuvent être reformulées respectivement sous la forme des équations (3) et (4) suivantes :

30 (3) $e(C_A, \text{capk} \cdot g_2^\alpha) = e(\wedge_1, g_2) \cdot e(C_t, g_2) \cdot e(z^{\wedge_2})^{-v_i} \cdot e(z, \text{capk})^{v_A} \cdot e(z, g_2)^{m_A}$

(4) $e(S, t \cdot g_2^k) = e(C_s, C_t) \cdot e(C_s, g_2)^{2k} \cdot e(C_s, z)^{-v_i} \cdot e(z, Ct)^{-v_s} \cdot e(z^{\wedge_2})^{-2v_s k} \cdot e(z, \zeta)^{v_{A'}}$

La vérification de la preuve de connaissance consiste alors à vérifier l'équation (5) suivante :

$$\begin{aligned}
W &= \text{POK}(v_t, w_t, v_A, w_A, av_A, aw_A, v_s, w_s, v_s k, w_s k, v_s v_t, w_s v_t, a, w, r^{*+r}, k) : \\
\tilde{C}_t &= g^{v_t} z^{w_t} A \tilde{C}_a = g^{v_{At}} z^{w_{At}} \wedge \tilde{C}_s = g^{v_s} z^{w_s} \wedge \\
\tilde{C}_A^\alpha &= g^{v_A^\alpha} z^{w_A^\alpha} \wedge g_S^k = g^{v_s k} z^{w_s k} \wedge g_S^{v_t} = g^{v_s v_t} z^{w_s v_t} \wedge \\
(5) \quad e(C_A, \text{capk}) e(C_A - g_2)^\alpha &= e(g_1, g_2) e(C_t, g_2) e(z, g_2)^{-v_t} e(z, \text{capk})^{v_A} e(z, g_2)^{\alpha v_A} \wedge \\
e(g_1, g_2) - e(m^*, g_2) - e(h_1, g_2)^{H(m)} &\cdot e(h_2, g_2)^{H(m)} - e(h_3, g_2)^w - e(h_1, g_2)^{r^*+r} = \\
e(C_s, C_t) e(C_s, g_2)^{2k} e(C_s, z)^{-v_t} &e(z, C_t)^{-v_s} e(z, g_2)^{-2} e(z, z)^{-v_s v_t}
\end{aligned}$$

16) Si cette preuve de connaissance est bien vérifiée, le fournisseur de services SP donne alors accès (sous-étape 227 d'accès au service) à l'utilisateur au service requis.

5

La fédération d'identités 200 précédemment décrite se déroule lors du premier accès de l'utilisateur au fournisseur de services SP, c'est-à-dire lors de l'envoi d'une première requête d'accès de l'utilisateur au fournisseur de services SP.

10

Lorsque le même utilisateur soumet ultérieurement une nouvelle requête d'accès au même fournisseur de services SP, son identité aura déjà été fédérée et une étape ultérieure d'authentification 300 aura alors lieu, pour chaque envoi d'une nouvelle requête d'accès au fournisseur de services, au moyen des alias déjà fédérés.

15

Une telle étape ultérieure d'authentification est relativement similaire à la fédération d'identités décrite ci-avant.

Elle diffère cependant de celle-ci en ce que l'utilisateur U doit envoyer au fournisseur de services SP, pendant chaque étape ultérieure d'authentification, le même alias m^* que celui qui a été validé pendant la fédération d'identités, afin de permettre au fournisseur de services SP de retrouver l'identité de l'utilisateur U associée à cet alias m^* dans sa base de clients

20

Ici, l'utilisateur U n'a pas besoin de prouver qu'il utilise, au cours de la génération de la preuve de connaissance, le même alias m^* que dans l'étape préliminaire de fédération d'identités. En effet, si l'utilisateur U ne suit pas le protocole d'authentification décrit ci-avant, par exemple en utilisant un alias différent de m^* , il ne pourra pas être authentifié par le fournisseur de services SP puisque ce dernier ne reconnaîtra pas l'alias qu'il avait précédemment reçu.

25

Dans un mode de réalisation avantageux, une nouvelle preuve de connaissance W est calculée à chaque étape ultérieure d'authentification de l'utilisateur U auprès du fournisseur de services SP. Cette nouvelle preuve de connaissance est différente des preuves de connaissance calculée(s) lors de l'étape de fédération d'identités 200 et des étapes précédentes d'authentification 300, afin d'assurer l'intraçabilité du fournisseur de services SP par le fournisseur d'identités IdP.

30

En effet, si la même preuve de connaissance est utilisée lors de plusieurs phases d'authentification ultérieures, le fournisseur d'identités IdP peut faire le lien avec les informations

recueillies lors de l'étape préliminaire de fédération d'identités. Pour obtenir une preuve de connaissance différente à chaque étape ultérieure d'authentification 300, les valeurs aléatoires r et r^* (voire les deux) peuvent être choisies pour être différentes.

La **figure 4** illustre les sous-étapes constituant une telle étape d'authentification ultérieure 300. Sur cette figure 4 sont illustrées les sous-étapes 301 à 327, respectivement similaires aux sous-étapes 201 à 227 de l'étape de fédération d'identités 200 décrite précédemment. Une telle étape d'authentification ultérieure 300 se déroule de la façon suivante :

1) L'utilisateur U requiert l'accès à un service du fournisseur de services SP , au moyen d'une requête d'accès $REQ_i(SERV)$ (sous-étape 301 d'envoi d'une requête d'accès).

2) Suite à la réception de cette requête d'accès $REQ_i(SERV)$, le fournisseur de services SP envoie une requête d'authentification ultérieure $REQ_i(AUTH)$ signée afin que l'utilisateur U entame les démarches pour s'authentifier à nouveau (sous-étape 303 d'envoi d'une requête d'authentification).

3) Après réception de cette requête d'authentification, l'utilisateur U construit un message d'authentification ultérieure msg_i (sous-étape 304 de construction de message d'authentification) comprenant une première partie M_i rassemblant des éléments non-aveuglés, une deuxième partie m_i rassemblant des éléments aveuglés variables d'un accès à un autre, et une troisième partie m^* comprenant les éléments aveuglés invariants d'un accès à un autre, à savoir l'alias de l'utilisateur.

Ce message d'authentification ultérieure msg_i peut ainsi consister en la concaténation de ces trois parties telles que $msg_i = M_i \parallel m_i \parallel m^*$.

4) Lors d'une sous-étape 305 d'aveuglement, l'utilisateur U aveugle alors la deuxième partie m_i en calculant un premier élément aveuglé c_i tel que $c_i = h_1^{H(m)} h_4^{r_i}$ et aveugle la troisième partie m^* en calculant un deuxième élément aveuglé c_i^* tel que $c_i^* = h^s h_4^{r_i^*}$.

Ces deux éléments aveuglés vont permettre la signature par le fournisseur d'identités IdP sans que celui-ci n'ait accès aux deux parties m et m^* .

Les valeurs aléatoires r_i et r_i^* sont ici avantageusement choisies pour être différentes respectivement des valeurs aléatoires r et r^* choisies durant la fédération d'identités ainsi que des valeurs aléatoires r_i et r_i^* qui ont pu être choisies lors d'éventuelles étapes d'authentification précédentes, dans le but de conserver l'intraçabilité du fournisseur de services SP .

5) Ensuite, lors d'une sous-étape 307 de calcul de preuves de connaissance, l'utilisateur U calcule une première preuve V_i de connaissance du premier élément aveuglé c_i en bases (h_1, h_4) , ainsi qu'une deuxième preuve V_i^* de connaissance du deuxième élément aveuglé c^* en bases (h, h_4) , similairement à ce qui est fait à l'étape 207.

5

6) Une fois tous ces éléments obtenus, l'utilisateur U envoie au fournisseur d'identités IdP la première partie M_i du message msg_i , les premier et deuxième éléments aveuglés c_i et c_i^* , ainsi que leurs preuves respectives de connaissance V_i et V_i^* (sous-étape d'envoi 309).

10

7) Après réception des éléments M_i, c_i, c_i^*, V_i et V_i^* , le fournisseur d'identités IdP calcule une valeur d'engagement C_i'' contenant des engagements sur $M_i, \eta_{3/4}, m^*$ ainsi qu'une valeur dite de randomisation $r_i^* + r_i$, similairement à l'étape 211 (sous-étape de calcul 311).

15

8) Une fois la valeur d'engagement C_i'' calculée, une sous-étape 313 d'obtention d'une signature partielle S_i sur cette valeur d'engagement C_i'' a lieu, similairement à l'étape 213. La signature de l'engagement C_i'' ainsi obtenue correspond alors au triplet (S_i, w_j, κ) .

20

9) Une fois la signature (S_i, w_j, κ) de l'engagement C_i'' obtenue, le fournisseur d'identités IdP envoie cette signature (S_i, w_j, κ) à l'utilisateur U lors d'une sous-étape 315 d'envoi de signature d'engagement.

25

10) Après réception de cette signature (S_i, w_j, κ) de l'engagement C_i'' , l'utilisateur U peut composer une nouvelle signature σ_i telle que $\sigma_i = (S_i, w_j, \kappa, r_i^* + r_i)$ (sous-étape 317 d'obtention de la signature σ).

11) Peut alors s'ensuivre une sous-étape 319 de vérification de cette nouvelle signature σ_i , similaire à l'étape 219 de la fédération d'identités.

12) A l'issue de cette étape 319, l'utilisateur U dispose donc d'une nouvelle signature σ_i telle que $\sigma_i = (S_i, w_j, \kappa, r_i^* + r_i)$ de son message msg_i tel que $msg_i = (M_i, \eta_{3/4}, m^*)$, ainsi que de ce message msg_i en tant que tel.

13) Afin de conserver l'anonymat du fournisseur d'identités IdP, l'utilisateur U produit alors une nouvelle preuve W_i de connaissance de la signature κ sans révéler les éléments $(S_i, w_j, \kappa, r_i^* + r_i)$ de cette nouvelle signature proprement dite, tout en révélant le message $msg_i = (M_i, \eta_{3/4}, m^*)$.

35

Cette nouvelle preuve W_i de connaissance sert également à prouver la connaissance de la clé publique t et du certificat de validité de la signature κ , sans révéler ces deux valeurs.

La nouvelle preuve W_i de connaissance est calculée similairement à l'étape 221 de la fédération d'identités (sous-étape de calcul 321) :

5 14) Une fois calculée, la nouvelle preuve W_i de connaissance est alors envoyée par l'utilisateur U au fournisseur de services SP, lors d'une étape 323 de transmission de nouvelle preuve de connaissance.

Ainsi, le fournisseur de services SP ne reçoit pas directement la clé publique t , le certificat κ et la signature σ , ce qui ne lui permet pas de retrouver l'identité du fournisseur d'identités IdP.

10 En outre, le fournisseur de services SP reçoit une nouvelle preuve W_i de connaissance, différente de la preuve W de connaissance utilisée lors de la fédération d'identités ainsi que des preuves de connaissance $W_1, \dots, W_n$ utilisées lors des éventuelles étapes précédentes d'authentification, ce qui garantit l'intraçabilité du fournisseur de services SP.

15 15) Suite à la réception de la nouvelle preuve W_i de connaissance, la vérification de cette nouvelle preuve W_i de connaissance est alors effectuée, lors d'une sous-étape 325 de vérification similaire à l'étape 225 décrite ci-avant.

20 Dans un mode de réalisation avantageux, il n'est pas nécessaire d'avoir recours au fournisseur d'identités IdP pendant l'étape ultérieure d'authentification. L'authentification de l'utilisateur U peut être rendue possible par la connaissance du logarithme discret s de l'alias m' dans la base h .

Dans ce mode de réalisation avantageux, l'utilisateur U complète la nouvelle preuve de connaissance W_i avec la preuve de connaissance du logarithme discret s vérifiant $m^* = h^s$.

25 Ceci peut être fait en remplaçant l'élément $e(m^*, g_2)$ par $e(h, g_2)^s$ dans l'équation (5).

Le fournisseur de services SP vérifie alors cette preuve de connaissance du logarithme discret s par l'utilisateur U et donne l'accès à ses services si cette vérification est positive.

30 Avec les modes de réalisation décrits précédemment, l'anonymat du fournisseur d'identités IdP auprès du fournisseur de services SP est garanti, ce qui permet de renforcer l'anonymat entre ces deux entités.

Cependant, l'inverse n'est pas forcément vrai dans la mesure où, dans l'exemple de message d'authentification décrit précédemment au cours de la fédération d'identités, l'identité du fournisseur de services SP est comprise dans la partie M non aveuglé du message d'authentification. Le fournisseur d'identités IdP a donc accès à l'identité du fournisseur de services SP et peut obtenir ainsi à partir de sa base clients (ou base de fédération) une information
35 sur les centres d'intérêt de l'utilisateur U.

Aussi, dans un mode de réalisation particulièrement avantageux, l'identité du fournisseur de services SP est placée dans la partie aveuglée variable m du message d'authentification, au cours de l'étape 200 de fédération d'identités ainsi qu'au cours des éventuelles étapes 300 d'authentification ultérieures, afin de garantir l'anonymat du fournisseur de services SP auprès du fournisseur d'identités IdP, ce qui permet de renforcer encore plus l'anonymat entre ces deux entités.

Dans ce mode de réalisation particulièrement avantageux, le fournisseur de services SP signe la requête d'authentification avec une signature de groupe avant d'envoyer cette requête à l'utilisateur U, lors des sous-étapes 203 et 303, afin de rester anonyme vis-à-vis du fournisseur d'identités IdP.

Une telle signature de groupe est décrite par exemple dans les articles « A practical and provably secure coalition-resistant group signature scheme » de Ateniese et al., et « Short group signatures » de Boneh et al.

Dans la mesure où il peut être plus avantageux que l'utilisateur U prouve que la même identité SP est utilisée à chaque fois, un mode particulier de réalisation peut alors consister à ce que l'identité du fournisseur de services SP soit placée dans la partie aveuglée invariante m* (en supplément de l'alias de l'utilisateur) plutôt que dans la partie aveuglée variable m du message d'authentification.

Bien entendu, l'invention n'est pas limitée aux exemples de réalisation ci-dessus décrits et représentés, à partir desquels on pourra prévoir d'autres modes et d'autres formes de réalisation, sans pour autant sortir du cadre de l'invention.

Ainsi, les termes « utilisateur », « fournisseur de services », « fournisseur d'identités » et « autorité de certification » employés précédemment recouvrent les entités matérielles utilisées respectivement par un utilisateur, un fournisseur de services, un fournisseur d'identités et une autorité de certification.

De telles entités matérielles peuvent prendre la forme d'un ordinateur ou d'un serveur aptes à effectuer les opérations décrites précédemment, que ce soit en termes de calcul ou de génération de données aléatoires.

Lorsque l'envoi (respectivement la réception) d'un message ou d'une requête par l'une de ces entités matérielles est indiqué ci-avant, cela signifie que cette entité matérielle dispose d'une interface matérielle de transmission (respectivement de réception) utilisant des moyens classiques de transfert de données, par câble ou sans fil par exemple, qui ne seront pas décrits plus en détail ici mais qui sont connus de l'art.

Revendications

1. Procédé d'authentification d'un utilisateur (U) auprès d'au moins un fournisseur de services (SP), ledit procédé comprenant l'envoi (223), par l'utilisateur au fournisseur de services, d'une première preuve de connaissance (W) d'un certificat de validité (κ) d'une clé publique (t) associée à une clé secrète (y) utilisée par un fournisseur d'identités (IdP) pour signer une première requête d'authentification de l'utilisateur et la vérification (225) de cette preuve de connaissance par le fournisseur de services.

2. Procédé d'authentification selon la revendication 1, caractérisé en ce que l'envoi (223) et la vérification (225) de la première preuve de connaissance (W) ont lieu durant une étape de fédération d'identités (200) qui comprend, en outre :

- l'envoi (209) au fournisseur d'identités (IdP) d'un alias aveuglé (c^*) calculé (205) à partir d'un alias (m^*) de l'utilisateur (U) ;

- le calcul (221) par l'utilisateur (U) de la première preuve de connaissance (W) à partir d'une signature partielle (S) calculée (213) par le fournisseur d'identités (IdP) à partir de l'alias aveuglé (c^*) et de la clé secrète (y);

- l'envoi (223) au fournisseur de services (SP) de l'alias (m^*) de l'utilisateur avec la première preuve de connaissance (W).

3. Procédé d'authentification selon la revendication 2, caractérisé en ce que ladite première preuve de connaissance (W) est calculée en outre à partir de la clé publique (t) et d'au moins une partie du certificat de validité (κ).

4. Procédé d'authentification selon la revendication 3, caractérisé en ce que ladite première preuve de connaissance (W) comprend au moins une première valeur masquée (C_t) calculée à partir de la clé publique (t), une deuxième valeur masquée (C_A) calculée à partir d'au moins une partie du certificat de validité (κ) et une troisième valeur masquée (C_s) calculée à partir de la signature partielle (S).

5. Procédé d'authentification selon l'une des revendications 1 à 4, caractérisé par une étape préliminaire d'enregistrement (100), préalable à la fédération d'identités, du fournisseur d'identités auprès d'une autorité de certification (CA) comprenant l'envoi (111) par l'autorité de certification au fournisseur d'identités du certificat de validité (κ) calculé (109) à partir d'au moins un engagement (C) envoyé (105) par le fournisseur d'identités.

6. Procédé d'authentification selon la revendication 5, caractérisé en ce que l'engagement (C) envoyé par le fournisseur d'identités est un engagement sur un premier élément (y') choisi aléatoirement par le fournisseur d'identités.

5 7. Procédé d'authentification selon la revendication 6, caractérisé en ce que la clé secrète (y) utilisée par le fournisseur d'identités comprend le premier élément (y') choisi aléatoirement par le fournisseur d'identités (IdP) ainsi qu'un deuxième élément (y'') choisi aléatoirement par l'autorité de certification (CA).

10 8. Procédé d'authentification selon l'une des revendications précédentes, caractérisé en ce que, lors de l'étape de fédération d'identités (200), la requête d'authentification comprend au moins une partie aveuglée (m, m*) par l'utilisateur (U), une desdites au moins une partie aveuglée comprenant l'identité du fournisseur de services (SP).

15 9. Procédé d'authentification selon l'une des revendications précédentes, ledit procédé comprenant au moins une étape ultérieure d'authentification (300) et étant caractérisé en ce que chaque étape ultérieure d'authentification comprend l'envoi (323) d'une nouvelle preuve de connaissance (W_i) obtenue (321) à partir d'une signature partielle (S_i) calculée (313) par le fournisseur d'identités (IdP) à partir d'un nouvel alias aveuglé (c_i^*) et de la clé secrète (y), suivi de
20 la vérification (325) de ladite nouvelle preuve de connaissance par le fournisseur de services.

10. Procédé d'authentification selon la revendication précédente, caractérisé en ce que, pour chaque étape ultérieure d'authentification (300), la nouvelle preuve de connaissance (W_i) est calculée (321) de sorte à être différente de la première preuve de connaissance (W) calculée lors de
25 la fédération d'identités et, si le procédé comprend plusieurs étapes ultérieures d'authentification (300), des nouvelles preuves de connaissance (W_i) calculées lors des autres étapes ultérieures d'authentification.

11. Procédé d'authentification selon la revendication précédente, caractérisé en ce que la
30 première preuve de connaissance (W) est calculée (221) en fonction d'une première et une deuxième variables aléatoires (r, r^*) et la nouvelle preuve de connaissance (W_i) est calculée (321) en fonction d'une première et une deuxième variables aléatoires ultérieures (r_i, r_i^*), lesdites première et deuxième variables aléatoires ultérieures (r_i, r_i^*) étant choisies pour être différentes desdites première et deuxième variables aléatoires (r, r^*) et, si le procédé comprend plusieurs étapes
35 ultérieures d'authentification (300), des première et deuxième variables aléatoires ultérieures (r_i, r_i^*) choisies lors des autres étapes ultérieures d'authentification.

12. Procédé d'authentification selon l'une des revendications 9 à 11, dans lequel un message d'authentification comprenant un alias aveuglé (c_i^*) de l'utilisateur est envoyé au fournisseur de services à chaque étape ultérieure d'authentification (300), caractérisé en ce que chaque étape ultérieure d'authentification (300) comprend l'aveuglement (305) de l'alias (m^*) de l'utilisateur de sorte que l'alias aveuglé obtenu (q^*) soit différent de l'alias aveuglé (c^*) obtenu lors de l'étape de fédération d'identités (200) et, si le procédé comprend plusieurs étapes ultérieures d'authentification (300), des autres alias aveuglés (c_i^*) obtenus lors des autres étapes ultérieures d'authentification.

13. Procédé d'authentification selon la revendication précédente, caractérisé en ce que l'alias aveuglé (c^*) obtenu lors de l'étape de fédération d'identités (200) est calculé (205) en fonction de l'alias (m^*) de l'utilisateur et d'une variable aléatoire (r^*) et l'alias aveuglé (c_i^*) obtenu lors d'une étape ultérieure d'authentification (300) est calculé (305) en fonction de l'alias (m^*) de l'utilisateur et d'une variable aléatoire ultérieure (r_i^*), ladite variable aléatoire ultérieure (r_i^*) étant choisie pour être différente de ladite variable aléatoires (r^*) et, si le procédé comprend plusieurs étapes ultérieures d'authentification (300), des variables aléatoires ultérieures (r_i^*) choisies lors des autres étapes ultérieures d'authentification.

14. Système d'authentification à anonymat renforcé comprenant au moins un utilisateur (U), au moins un fournisseur de services (SP), un fournisseur d'identités (IdP) et une autorité de certification (CA), caractérisé en ce que le système est apte à mettre en œuvre le procédé d'authentification selon l'une des revendications 1 à 13 lorsqu'un desdits au moins un utilisateur requiert un service auprès d'un desdits au moins un fournisseur de services.

15. Programme d'ordinateur, téléchargeable via un réseau de télécommunication et/ou stocké dans une mémoire d'une unité centrale et/ou stocké sur un support mémoire destiné à coopérer avec une unité centrale, caractérisé pour mettre en œuvre un procédé selon l'une quelconque des revendications 1 à 13.

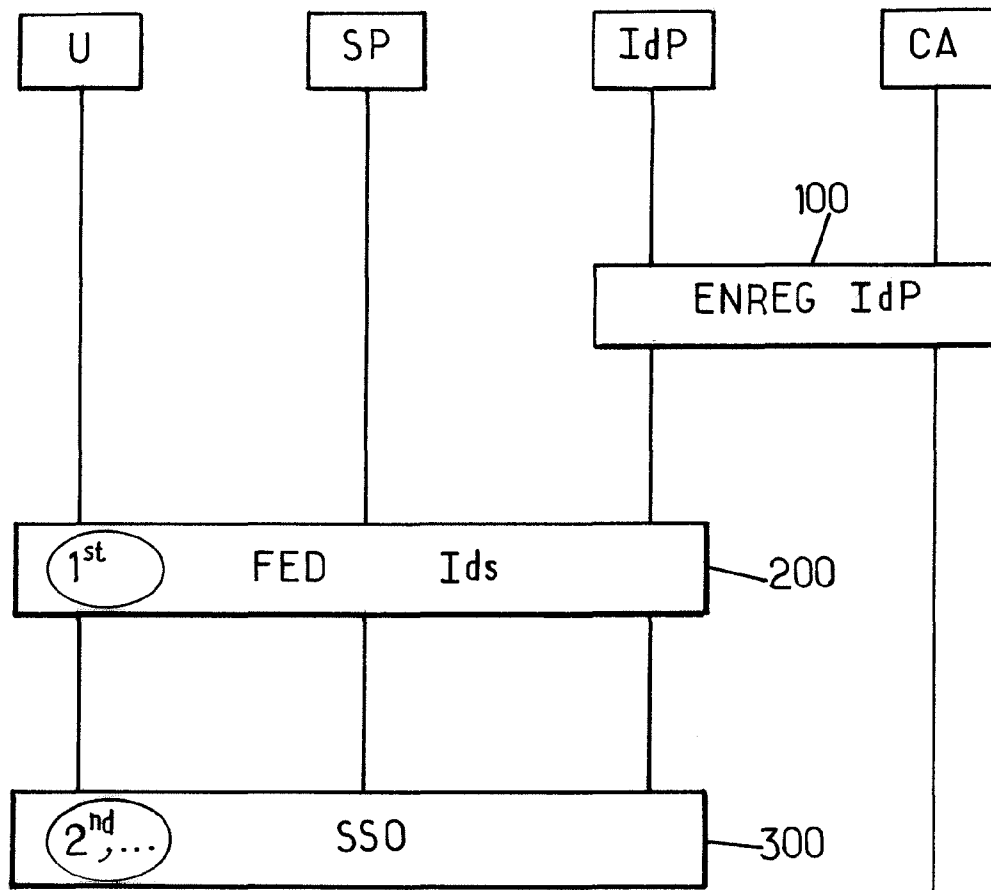
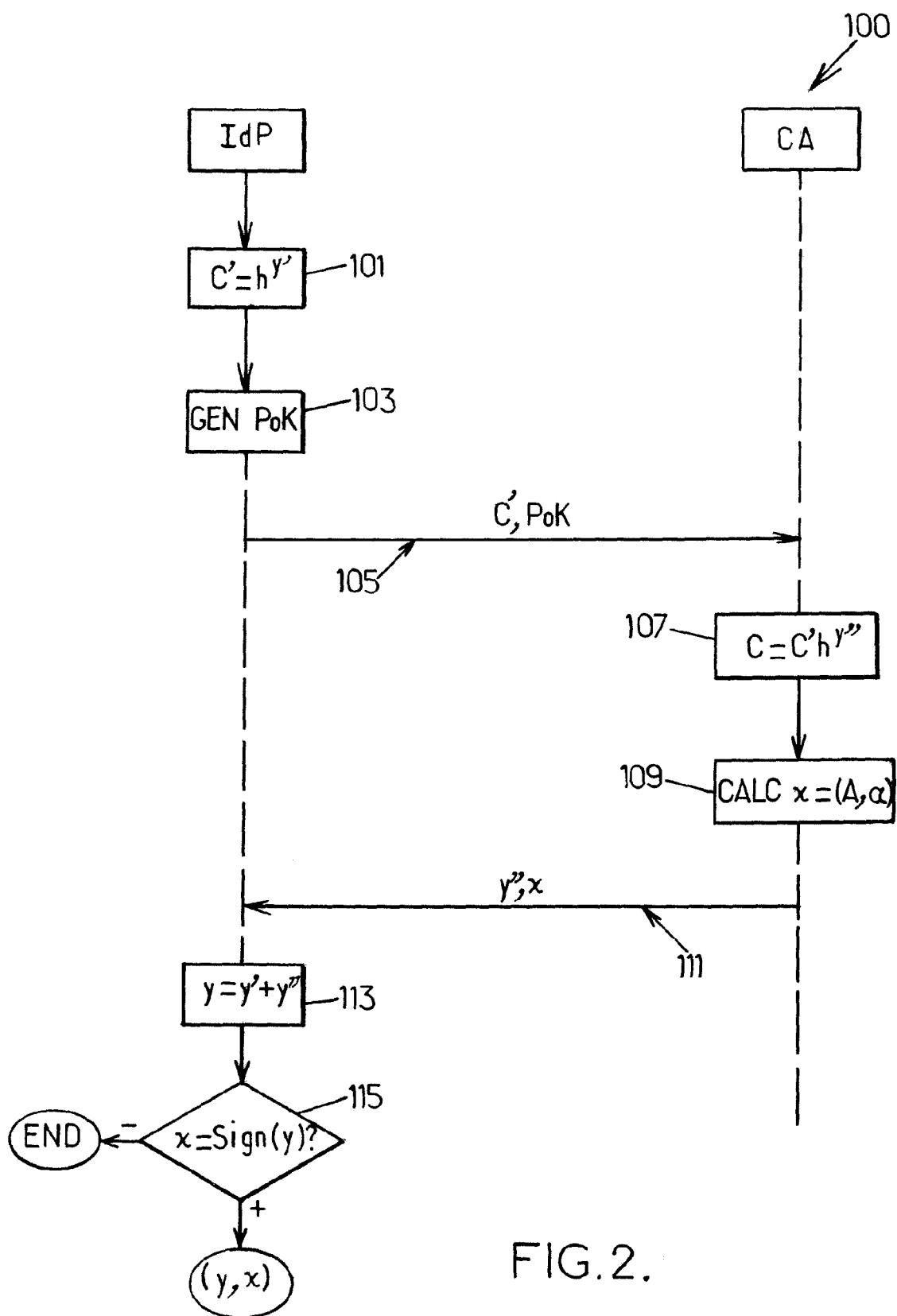
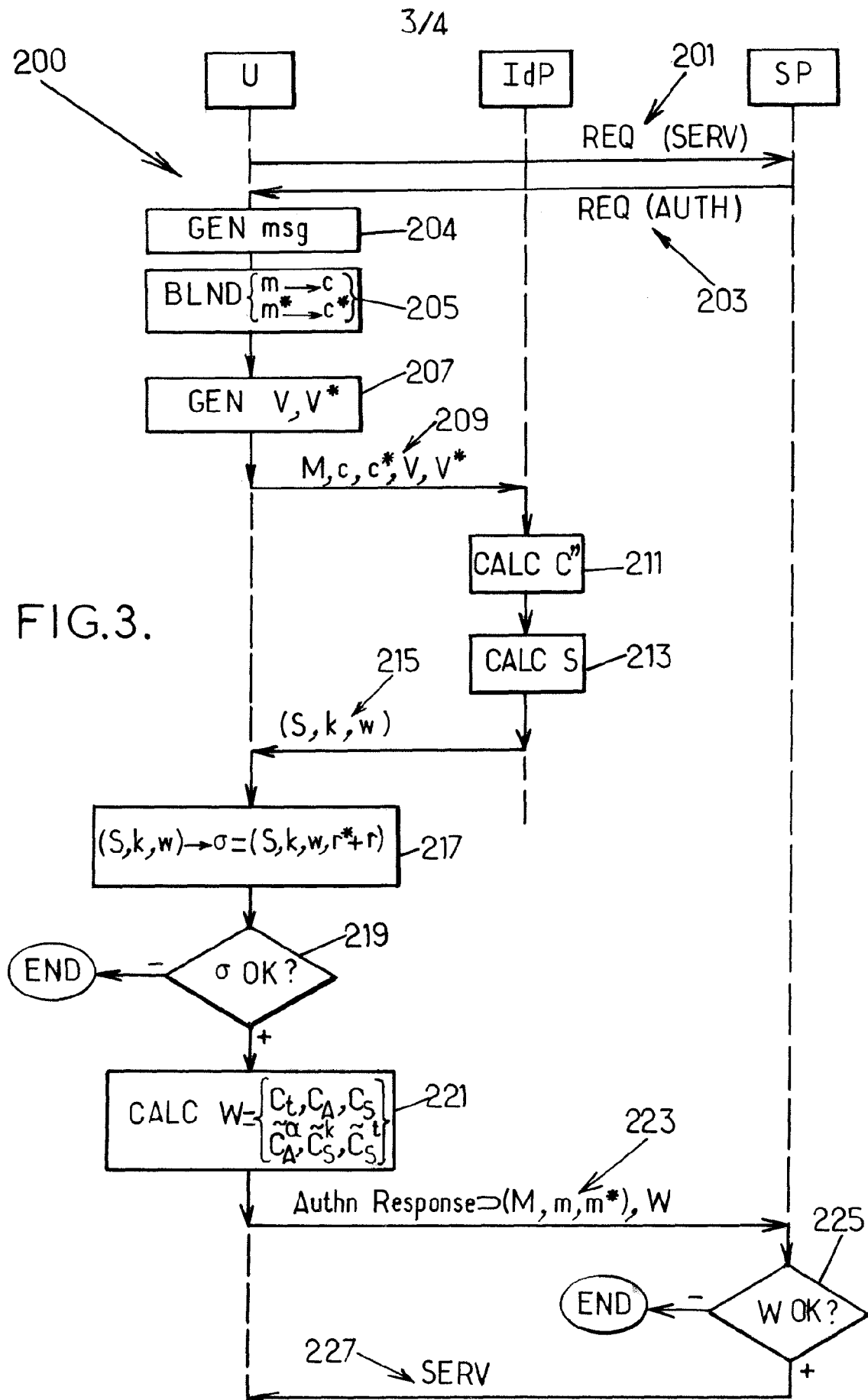


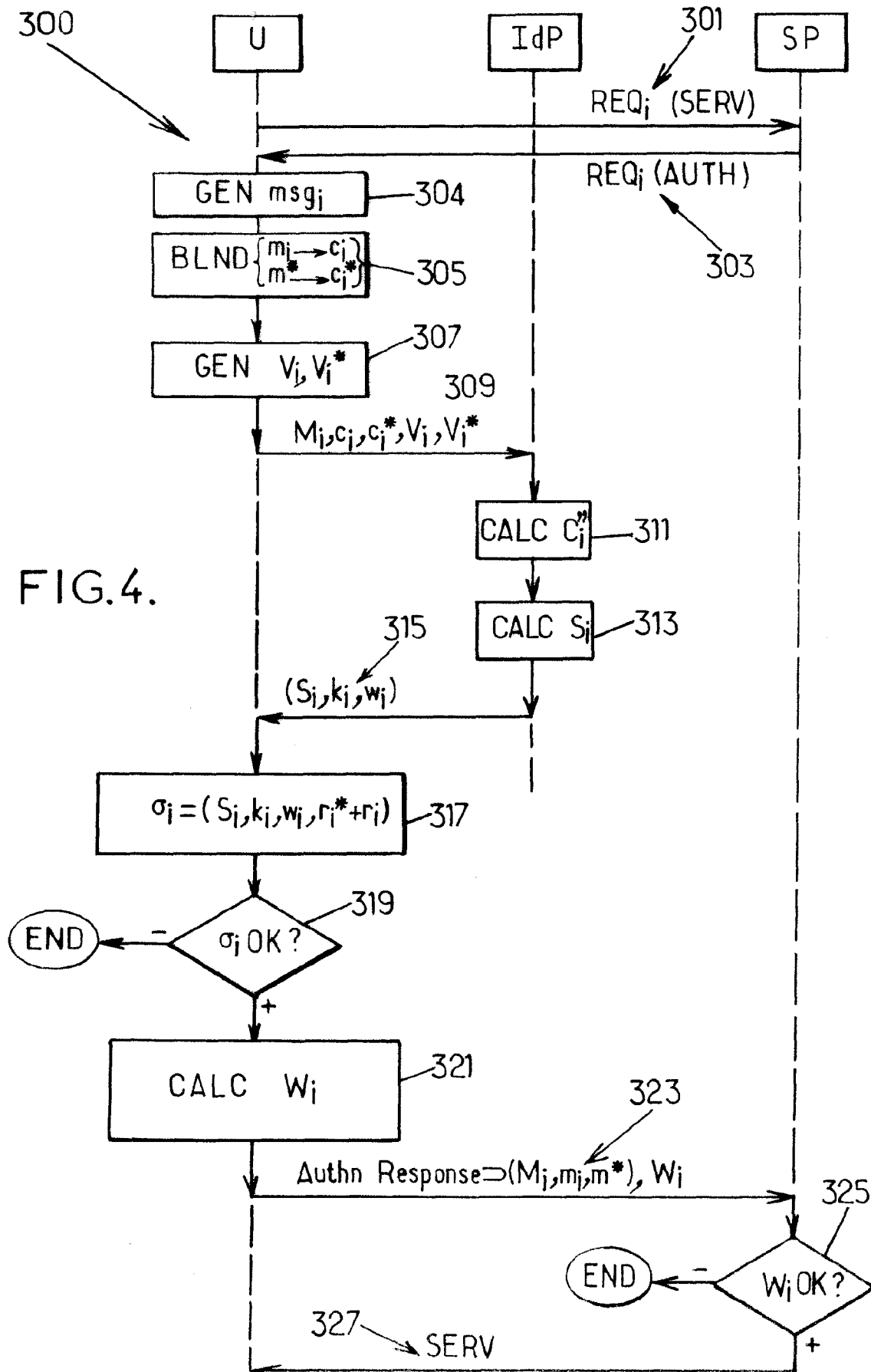
FIG.1.

2/4





4/4



INTERNATIONAL SEARCH REPORT

International application No

PCT/FR2011/051441

A. CLASSIFICATION OF SUBJECT MATTER
 INV. H04L29/06 H04L9/32
 ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification System followed by classification symbols)
 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal , INSPEC, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Wo 2008/113951 A2 (FRANCE TELECOM [FR] ; CANARD SEBASTIEN [FR] ; MALVILLE ERIC [FR] ; TRAORE) 25 September 2008 (2008-09-25) cited in the application page 4, line 16 - page 17, line 21; figures 2-5 -----	1-15
A	Canard, Sébastien et al: "A client-si de approach for privacy-preserving identity federation", Springer Netherlands, 1 December 2009 (2009-12-01) , pages 269-295 , XP002617625 , DOI : 10.1007/S12394-009-0024-4 Retrievd from the Internet: URL: http://dx.doi.org/10.1007/s12394-009-0024-4 [retrieved on 2011-01-18] the whole document -----	1-15



Further documents are listed in the continuation of Box C.



See patent family annex.

* Spécial catégories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

20 October 2011

Date of mailing of the international search report

28/10/2011

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040,
 Fax: (+31-70) 340-3016

Authorized officer

Raposo Pires , João

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/FR2011/051441

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
Wo 2008113951 A2	25-09-2008	EP 2116000 A2 US 2010275009 AI	11-11-2009 28-10-2010

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°

PCT/FR2011/051441

A. CLASSEMENT DE L'OBJET DE LA DEMANDE INV. H04L29/06 H04L9/32 ADD.		
Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB		
B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE Documentation minimale consultée (système de classification suivi des symboles de classement) H04L		
Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche		
Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés) EPO-Internal , INSPEC, WPI Data		
C. DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	Wo 2008/113951 A2 (FRANCE TELECOM [FR] ; CANARD SEBASTIEN [FR] ; MALVILLE ERIC [FR] ; TRAORE) 25 septembre 2008 (2008-09-25) cité dans la demande page 4, ligne 16 - page 17, ligne 21; figures 2-5 -----	1-15
A	Canard, Sébastien et al: "A client-side approach for privacy-preserving identity federation", Springer Netherlands, 1 décembre 2009 (2009-12-01) , pages 269-295 , XP002617625 , DOI : 10.1007/S12394-009-0024-4 Extrait de l'Internet: URL: http://dx.doi.org/10.1007/s12394-009-0024-4 [extrait le 2011-01-18] le document entier -----	1-15
☐ Voir la suite du cadre C pour la fin de la liste des documents ☒ Les documents de familles de brevets sont indiqués en annexe		
* Catégories spéciales de documents cités:		
"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent "E" document antérieur, mais publié à la date de dépôt international ou après cette date "L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée) "O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens "P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée "T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention "X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément "Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier "&" document qui fait partie de la même famille de brevets		
Date à laquelle la recherche internationale a été effectivement achevée 20 octobre 2011		Date d'expédition du présent rapport de recherche internationale 28/10/2011
Nom et adresse postale de l'administration chargée de la recherche internationale Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Fonctionnaire autorisé Raposo Pires , João

Renseignements relatifs aux membres de familles de brevets

PCT/FR2011/051441

Formulaire PCT/ISA/210 (annexe familles de brevets) (avril 2005)