(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 969 879**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **10 61146**

(51) Int Cl[8] : ***H 04 L 9/32*** *(2012.01)*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 23.12.10.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 29.06.12 Bulletin 12/26.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *FRANCE TELECOM Société anonyme* — FR.

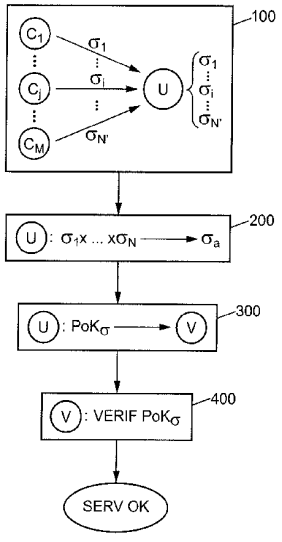
(72) **Inventeur(s) :** CANARD SEBASTIEN et LESCUYER ROCH.

(73) **Titulaire(s) :** FRANCE TELECOM Société anonyme.

(74) **Mandataire(s) :** CABINET PLASSERAUD.

(54) ACCES ANONYME A UN SERVICE AU MOYEN DE CERTIFICATS AGREGES.

(57) L'invention concerne un procédé d'accès anonyme à un service, comprenant l'attribution (100), par au moins une entité certificatrice (C_i), d'une pluralité de certificats (σ_1,$\sigma_{N'}$) à une entité utilisatrice (U), ces certificats étant calculés à partir d'au moins un attribut (m_k) associé à l'entité utilisatrice, le calcul (200), par l'entité utilisatrice (U), d'un certificat agrégé (σ_a) à partir d'une pluralité de certificats (σ_1,σ_N) parmi les certificats attribués à l'entité utilisatrice (U), le calcul (300), par l'entité utilisatrice (U), d'une preuve de connaissance (PoK_σ) du certificat agrégé (σ_a) et une vérification (400), effectuée par une entité vérificatrice (V), d'au moins un de ces certificats au moyen de ladite preuve de connaissance (PoK_σ), l'accès au service étant fourni par l'entité vérificatrice à l'entité utilisatrice en fonction du résultat de cette vérification. L'invention concerne en outre un programme d'ordinateur correspondant, les entités utilisatrices (U), vérificatrices (V) et certificatrices (Ci) correspondantes ainsi qu'un système d'accréditation anonyme (SAA) pour l'accès anonyme à un service comprenant ces différentes entités.



FR 2 969 879 - A1

Accès anonyme à un service au moyen de certificats agrégés

L'invention concerne le domaine des systèmes d'accréditation anonyme pour l'accès à des services, en particulier au moyen de l'attribution de certificats agrégés entre eux.

Dans un système d'accréditation courant, une organisation de confiance émet, pour certains utilisateurs, des accréditations certifiées portant sur un ou plusieurs attributs de cet utilisateur.

Une telle organisation peut être, par exemple, une mairie émettant des accréditations certifiées consistant en des cartes d'identité, lesquelles présentent un certain nombre d'attributs associés à l'utilisateur du type nom, prénom, date de naissance, adresse, etc. Cette organisation peut également être une université émettant des accréditations certifiées consistant en des cartes d'étudiant, lesquelles présentent certains attributs associés à un étudiant du type nom, prénom, numéro d'étudiant, études suivies, etc.

Lorsqu'il souhaite accéder à un service offert par un organisme tiers agissant en tant que fournisseur de services, l'utilisateur peut alors vouloir utiliser de telles accréditations certifiées de façon anonyme, c'est-à-dire en minimisant l'information qu'il fournit à ce fournisseur de service afin d'en obtenir le service désiré.

Par exemple, l'accès à certains services spécifiques peut être restreint aux habitants d'une ville. Dans un tel cas, l'utilisateur doit alors prouver qu'il habite bien la bonne ville, de façon certifiée par la mairie, mais il peut ne pas vouloir révéler les autres attributs le concernant sur sa carte d'identité, tels que son nom ou son adresse exacte.

Similairement, un étudiant peut vouloir bénéficier d'une ristourne sur un service offert par l'organisme tiers. L'étudiant doit alors prouver qu'il possède une accréditation provenant d'une université, mais peut ne pas vouloir révéler les autres attributs le concernant sur sa carte d'étudiant, tels que son nom ou les études qu'il suit.

Pour répondre à ce besoin d'anonymat, il est possible d'envisager des systèmes d'accréditation utilisant des techniques cryptographiques proches des signatures de groupe ou des signatures aveugles.

Dans le cas des signatures de groupe, l'organisation certificatrice signe, lors de la phase de création de l'accréditation, l'ensemble des attributs associés à l'utilisateur en ne produisant qu'une seule signature. Cette signature doit être telle que l'organisation certificatrice elle-même ne doit pas être capable d'utiliser cette accréditation afin de se faire passer pour l'utilisateur, ce qui est par exemple possible en utilisant des techniques liées aux schémas de signature de groupe. L'entité de confiance est l'organisation qui délivre des accréditations. Dans les exemples présentés ci-dessus, l'Entité de confiance est la mairie, ou l'université.

Une fois l'utilisateur en possession d'une telle accréditation, il peut révéler un ou plusieurs attributs qui lui sont associés, en fonction de la demande de l'organisme tiers agissant en tant que fournisseur de services auprès duquel il requiert un service, en générant, à l'instar des techniques de signature de groupe, une preuve de connaissance des attributs non révélés et une signature sur l'ensemble

des attributs, révélés ou non, sans divulguer ni les attributs non révélés ni la signature de l'organisation certificatrice. L'utilisateur préserve de ce fait son anonymat vis-à-vis du monde extérieur.

Dans ce cas de figure, il est nécessaire d'utiliser un schéma de signature permettant de signer plusieurs messages/attributs en une seule signature et où le possesseur de la signature est capable de faire une preuve de connaissance de la signature et des messages signés, sans révéler ni la signature, ni l'ensemble de ces messages/attributs qu'il souhaite cacher, tout en gardant la possibilité de donner en clair le ou les attributs qui lui sont demandés par l'organisme tiers.

Un tel schéma de signature est consommateur en temps de calcul puisqu'il nécessite de cacher explicitement les attributs non révélés. La taille de la preuve dépend donc du nombre d'attributs initialement certifiés par l'entité émettrice. Par ailleurs, sa mise en œuvre pratique nécessite l'utilisation de données cryptographiques de taille importante, comme cela est le cas dans la technologie Idemix proposée par IBM.

Dans les cas des signatures aveugles, l'idée consiste à faire signer de façon aveugle les attributs par l'organisation certificatrice. L'utilisation d'une telle signature aveugle rend le système d'accréditation plus efficace, au détriment cependant d'une traçabilité accrue de l'utilisateur. Un exemple de ce type de technique est repris dans la technologie UProve proposée par Microsoft.

La présente invention a pour objet de remédier aux inconvénients précités des solutions envisagées de l'art antérieur et de proposer une technique alternative d'accréditation anonyme, qui soit potentiellement plus efficace et moins gourmande en temps de calcul et en bande passante et qui permette une simplification des procédures lorsqu'un utilisateur doit faire appel à des accréditations provenant d'organisations différentes.

La présente invention propose à cet effet un procédé d'accès anonyme à un service comprenant :

l'attribution, par au moins une entité certificatrice, d'une pluralité de certificats à une entité utilisatrice, ces certificats étant calculés à partir d'au moins un attribut associé à l'entité utilisatrice ;

le calcul, par l'entité utilisatrice, d'un certificat agrégé à partir d'une pluralité de certificats parmi les certificats attribués à l'entité utilisatrice ;

le calcul, par l'entité utilisatrice, d'une preuve de connaissance du certificat agrégé ; et

une vérification, effectuée par une entité vérificatrice, d'au moins un de ces certificats au moyen de ladite preuve de connaissance, l'accès au service étant fourni par l'entité vérificatrice à l'entité utilisatrice en fonction du résultat de ladite vérification.

Dans un mode de réalisation, l'attribution de la pluralité de certificats à l'entité utilisatrice comprend, pour chacun des certificats attribués par une entité certificatrice, le calcul d'un certificat au moyen d'une donnée publique liée à une clé secrète de l'entité utilisatrice, d'au moins un attribut associé à l'entité utilisatrice et d'une clé secrète de l'entité certificatrice et la transmission du certificat à l'entité utilisatrice, ce qui permet de certifier que l'utilisateur présente bien l'attribut en question tout en ne révélant pas la clé secrète de l'utilisateur.

En particulier, le certificat peut être calculé dans le cadre des environnements bilinéaires munis de couplages selon la formule suivante :

$$\sigma_i = \left(C \cdot \prod_{k=1}^{l_j} H(g_1^{sk_{Cj}} \| g_2^{sk_{Cj}} \| m_k) \right)^{sk_{Cj}}$$

où σ_i représente le certificat, C représente la donnée publique liée à la clé secrète de l'entité utilisatrice, lj représente le nombre d'attributs signés par l'entité certificatrice C_j, H représente une fonction cryptographique de hachage, g_1 et g_2 représentent deux générateurs de groupe choisis aléatoirement et de manière uniforme respectivement dans deux groupes bilinéaires d'ordre p, où p est un nombre entier premier, sk_{Cj} représente la clé secrète de l'entité certificatrice, et m_k représente un attribut associé à l'entité utilisatrice.

Dans un mode de réalisation avantageux où le certificat calculé par l'entité certificatrice est un certificat provisoire, la donnée publique liée à la clé secrète de l'entité utilisatrice est un engagement sur la clé secrète de l'entité utilisatrice calculé dans l'entité utilisatrice au moyen d'une variable aléatoire avant d'être transmis à l'entité certificatrice et le certificat provisoire reçu par l'entité utilisatrice est démasqué au moyen de ladite variable aléatoire afin d'obtenir le certificat attribué à l'entité utilisatrice. Ceci permet d'empêcher l'entité certificatrice de générer des certificats qu'elle pourrait utiliser à la place de l'utilisateur.

En particulier, le démasquage du certificat provisoire comprend le calcul du certificat attribué à l'entité utilisatrice en multipliant le certificat reçu de l'entité certificatrice par la variable $(g_1^{sk_{Cj}})^{-s}$, où g_1 représente un générateur de groupe choisi aléatoirement et de manière uniforme dans un groupe d'ordre p, où p est un nombre entier premier, sk_{Cj} représente la clé secrète de l'entité certificatrice et s est une valeur aléatoirement choisie dans l'ensemble Z_p des entiers modulo p.

Avantageusement, le certificat attribué à l'entité utilisatrice est vérifié par l'entité utilisatrice après le démasquage du certificat provisoire, afin de pouvoir interrompre le protocole d'attribution avant de transmettre une quelconque de preuve de connaissance si ce protocole ne s'est pas bien déroulé.

Avantageusement, la donnée publique liée à la clé secrète de l'entité utilisatrice est vérifiée au moyen d'une preuve de connaissance de cette donnée publique, et le calcul du certificat n'est effectué que si le résultat de la vérification de l'engagement est positif, ce qui évite d'effectuer inutilement le calcul du certificat si l'utilisateur n'est pas habilité à obtenir un tel certificat et permet l'envoi d'un message d'erreur si le protocole ne s'est pas bien déroulé.

L'étape d'attribution peut comprendre en particulier le calcul, par l'entité utilisatrice, de la donnée publique liée à la clé secrète de l'entité utilisatrice, le calcul d'une première partie de la preuve de connaissance à partir de cette donnée publique liée à la clé secrète et le calcul d'une deuxième partie de la preuve de connaissance à partir d'une donnée aléatoire reçue de l'entité certificatrice.

Dans un mode de réalisation particulier, le calcul de l'engagement comprend le calcul d'une première partie de ladite donnée publique liée à la clé secrète de l'entité utilisatrice et le calcul d'une

deuxième partie de la donnée publique liée à la clé secrète de l'entité utilisatrice et à au moins un certificat attribué par une autre entité certificatrice.

Avantageusement, le calcul de la preuve de connaissance de la pluralité de certificats attribués à l'entité utilisatrice comprend le calcul d'un engagement sur le certificat agrégé, le calcul d'une première partie de la preuve de connaissance à partir de l'engagement sur le certificat agrégé et le calcul d'une deuxième partie de la preuve de connaissance à partir d'une donnée aléatoire reçue de l'entité vérificatrice, ce qui permet de ne pas révéler directement le certificat agrégé et donc de préserver au mieux l'anonymat.

La présente invention vise également un programme d'ordinateur comprenant des instructions pour la mise en œuvre de l'étape de calcul d'un certificat ci-avant lorsque ce programme d'ordinateur est exécuté par une unité de calcul située dans une entité certificatrice.

La présente invention vise par ailleurs un programme d'ordinateur comprenant des instructions pour la mise en œuvre de l'étape de génération d'une preuve de connaissance d'une pluralité de certificats attribués à une entité utilisatrice ci-avant lorsque ce programme d'ordinateur est exécuté par une unité de calcul située dans une entité utilisatrice.

La présente invention vise en outre un programme d'ordinateur comprenant des instructions pour la mise en œuvre de l'étape de vérification au moyen d'une preuve de connaissance d'une pluralité de certificats ci-avant, lorsque ce programme d'ordinateur est exécuté par une unité de calcul située dans une entité vérificatrice.

Au titre de la protection recherchée, les programmes d'ordinateur ci-avant sont à considérer comme des produits programme d'ordinateur.

La présente invention propose par ailleurs une entité certificatrice, apte à accréditer une entité utilisatrice, comprenant une unité de calcul apte à mettre en œuvre l'étape de calcul d'un certificat à partir d'au moins un attribut ci-avant, et une unité de communication apte à transmettre ce certificat calculé à l'entité utilisatrice.

La présente invention propose également une entité vérificatrice, apte à vérifier une entité utilisatrice, comprenant une unité de communication apte à recevoir une preuve de connaissance d'une pluralité de certificats attribués à l'entité utilisatrice et une unité de calcul apte à mettre en œuvre l'étape de vérification ci-avant au moyen de cette preuve de connaissance, afin de démarrer la fourniture d'un service à l'entité utilisatrice en fonction du résultat de la vérification.

La présente invention propose en outre une entité utilisatrice, apte à requérir un service par l'intermédiaire d'une entité vérificatrice, au moyen d'une preuve de connaissance d'une pluralité de certificats attribués à l'entité utilisatrice par au moins une entité certificatrice, cette entité utilisatrice comprenant une unité de communication apte à recevoir une pluralité de certificats provenant d'au moins une entité certificatrice et une unité de calcul apte à mettre en œuvre l'étape de calcul d'une preuve de connaissance ci-avant à partir de la pluralité de certificats reçus, l'unité de communication étant apte, en outre, à transmettre la preuve de connaissance à une entité vérificatrice afin de requérir un service.

La présente invention vise enfin un système d'accréditation anonyme, pour l'accès anonyme à un service, comprenant au moins une entité certificatrice telle que décrite ci-avant, une entité vérificatrice telle que décrite ci-avant et une entité utilisatrice telle que décrite ci-avant.

D'autres caractéristiques et avantages de l'invention apparaîtront à l'examen de la description détaillée ci-après, et des dessins annexés sur lesquels :

- la figure 1 illustre les étapes principales d'un procédé d'accès anonyme à un service selon la présente invention ;
- la figure 2 illustre en particulier l'étape d'attribution d'un certificat employée par le procédé d'accès anonyme à un service selon la présente invention ;
- la figure 3 illustre en particulier les étapes de calcul d'un certificat agrégé à partir des certificats attribués à l'entité utilisatrice, de calcul d'une preuve de connaissance de ces certificats et de vérification de cette preuve de connaissance employées par le procédé d'accès anonyme à un service selon la présente invention ;
- la figure 4 illustre plus particulièrement l'étape d'attribution d'un certificat employée par le procédé d'accès anonyme à un service selon un deuxième mode de réalisation de l'invention ;
- la figure 5 illustre plus particulièrement l'étape d'attribution d'un certificat employée par le procédé d'accès anonyme à un service selon un troisième mode de réalisation de l'invention ; et
- la figure 6 représente schématiquement un système d'accréditation anonyme pour l'accès anonyme à un service, dans lequel est mis en œuvre le procédé d'accès anonyme à un service selon la présente invention.

On se réfère tout d'abord à la **figure 1** sur laquelle sont illustrées les étapes principales d'un procédé d'accès anonyme à un service selon la présente invention.

Ce procédé d'accès anonyme débute par l'attribution préalable (étape 100) d'une pluralité de certificats $\sigma_{1,\ldots},\sigma_{i,\ldots},\sigma_{N'}$ à une entité utilisatrice U. Ces certificats sont attribués par au moins une entité certificatrice C_j, voire par une pluralité d'entités certificatrices $C_1,\ldots, C_j,\ldots,C_M$, de sorte qu'une même entité certificatrice C_j peut attribuer plusieurs certificats à l'entité utilisatrice U.

On entend ici par « entité utilisatrice » tout dispositif pouvant être utilisé par un utilisateur et disposant au moins d'une unité de communication, pour communiquer avec d'autres entités, et d'une unité de calcul permettant d'effectuer des calculs sur des données échangées avec ces autres entités, comme cela sera expliqué par la suite.

Similairement, on entend ici par « entité certificatrice » tout dispositif disposant au moins d'une unité de communication, pour pouvoir communiquer avec des entités utilisatrices, et d'une unité de calcul permettant d'effectuer des calculs sur des données échangées avec ces entités utilisatrices afin de leur attribuer un certificat, un tel certificat pouvant être agrégés avec d'autres certificats comme cela sera expliqué par la suite.

Enfin, on entend ici par « certificat » une ou plusieurs donnée(s), sous forme numérique, permettant à l'entité utilisatrice et son utilisateur de s'authentifier auprès d'un organisme tiers fournissant un service (lequel peut être distinct de l'entité certificatrice) sans lui révéler plus d'information que ce qui est nécessaire pour valider l'accès à ce service et donc en préservant leur anonymat. On peut parler ici également d'accréditation anonyme, auquel cas l'entité certificatrice peut être vue comme étant une entité d'accréditation.

Dans la présente invention, un certificat σ_i est généré au moyen d'un ou plusieurs attribut(s) $m_1,\ldots,m_k$ associé(s) à l'entité utilisatrice U.

De tels attributs $m_1,\ldots,m_k$ peuvent être en particulier certains attributs de l'utilisateur utilisant cette entité utilisatrice U. Ainsi, pour reprendre l'exemple illustratif d'une entité certificatrice appartenant à une université et d'une entité utilisatrice appartenant à un étudiant, de tels attributs peuvent correspondre au nom de l'étudiant, à son prénom, son numéro d'étudiant, les différents types d'études qu'il suit dans cette université, etc. Dans l'autre exemple illustratif déjà évoqué où l'entité certificatrice appartient cette fois à une mairie émettant des cartes d'identité, ces attributs peuvent correspondre au nom de l'administré, à son prénom, sa date de naissance, son adresse, etc.

Ainsi, comme chacun des certificats σ_i est généré à partir de tels attributs, l'utilisateur de l'entité utilisatrice peut se servir de tels certificats σ_i pour s'authentifier auprès d'un organisme sollicitant la preuve de la certification de tels attributs par une entité certificatrice, au moyen de son entité utilisatrice U, sans révéler plus d'informations pour autant.

Une fois qu'un certain nombre de certificats $\sigma_{1,\ldots},\sigma_{i,\ldots},\sigma_{N'}$ ont été attribués à l'entité utilisatrice U, un certificat agrégé σ_a est calculé (étape 200) par l'entité utilisatrice U à partir d'une pluralité de certificats $\sigma_{1,\ldots},\sigma_{i,\ldots},\sigma_N$ (où $N \leq N'$) parmi les certificats attribués à l'entité utilisatrice (U), par exemple en les multipliant entre eux. Cette étape 200 d'agrégation peut, par exemple, être effectuée à la volée lorsque l'utilisateur entame la procédure de requête d'un service auprès d'une entité vérificatrice V.

Ainsi, lorsque l'entité utilisatrice U désire s'authentifier auprès d'une entité vérificatrice V requérant l'authentification sur la base d'un certain nombre d'attributs de l'utilisateur, l'entité utilisatrice U peut choisir les σ_i correspondant à ces attributs nécessaires à l'authentification parmi les N' certificats dont elle dispose.

Le procédé d'accès anonyme se poursuit par le calcul (étape 300), par l'entité utilisatrice U, d'une preuve de connaissance PoK_σ du certificat agrégé σ_a.

On entend ici par « preuve de connaissance des certificats σ_a» des données, sous forme numérique, calculées à partir de ce certificat agrégé et permettant de prouver que l'utilisateur a la connaissance de ce certificat agrégé, donc des certificats individuels $\sigma_{1,\ldots},\sigma_{i,\ldots},\sigma_N$, qui le composent, et donc que ces certificats ont bien été attribués à l'entité utilisatrice U par une entité certificatrice, sans pour autant dévoiler ces certificats eux-mêmes.

Ici, dans la mesure où chaque certificat σ_i a lui-même été obtenu à partir d'attributs associés à l'entité utilisatrice, la preuve de connaissance PoK_σ ainsi générée correspond indirectement à une preuve de connaissance du fait que l'utilisateur de l'entité utilisatrice U présente bien ces attributs qui lui sont associés, ce qui permet à l'organisme tiers d'être renseigné à ce sujet sans qu'il n'ait directement accès ni à l'identité de l'utilisateur, ni aux autres attributs préalablement certifiés. Sa seule certitude est que les attributs qu'il obtient appartiennent effectivement à cette entité utilisatrice et qu'ils ont effectivement été certifiés par une entité certificatrice C_j.

Ce calcul de la preuve de connaissance PoK_σ, effectuée dans l'entité utilisatrice U, se termine par la transmission de cette preuve de connaissance PoK_σ vers une entité vérificatrice V afin d'en obtenir un service.

Ainsi, on entend ici par « entité vérificatrice » tout dispositif disposant au moins d'une unité de communication pour pouvoir communiquer avec des entités utilisatrices requérant un service au moyen d'une preuve de connaissance des certificats, d'une unité de calcul pour effectuer des calculs sur des données échangées avec ces entités utilisatrices, afin de vérifier ces données avant de déclencher la fourniture du service. Le service peut alors être soit fourni directement par l'entité vérificatrice, soit fourni par une entité tiers distincte de l'entité vérificatrice auquel cas l'entité vérificatrice est apte à requérir la fourniture du service auprès de cette entité de tiers après avoir vérifié les données.

Suite à la réception de la preuve de connaissance PoK_σ par cette entité vérificatrice V, une vérification (étape 400) est alors effectuée par cette entité vérificatrice V au moyen de cette preuve de connaissance PoK_σ portant sur les certificats $\sigma_{1,\ldots,}\sigma_{i,\ldots,}\sigma_N$ attribués préalablement à l'entité utilisatrice U.

L'entité vérificatrice V fournit alors l'accès au service requis à l'entité utilisatrice U en fonction du résultat de cette vérification, c'est-à-dire seulement si cette vérification donne un résultat positif.

Dans la présente invention, les certificats $\sigma_{1,\ldots,}\sigma_{i,\ldots,}\sigma_N$ sont agrégeables, c'est-à-dire qu'un certificat agrégé σ_a peut être obtenu dans l'entité utilisatrice U à partir de l'agrégation de différents certificats $\sigma_1,\ldots,\sigma_N$ attribués par une ou plusieurs entités certificatrices $C_1,\ldots C_j,\ldots,C_M$, par exemple en multipliant ces certificats.

Afin d'obtenir de tels certificats agrégeables, un schéma de signature agrégeable peut être avantageusement employé par l'entité certificatrice C_j pour générer un certificat agrégeable σ_i, en procédant à une signature d'un ou plusieurs attribut(s) $m_1,\ldots,m_k$ avec une clé secrète sk_{Cj} attribuée préalablement à l'entité certificatrice C_j, et potentiellement certifiée dans le cadre par exemple d'un système PKI classique.

L'intérêt d'utiliser des certificats $\sigma_1,\ldots,\sigma_N$ agrégeables est de permettre d'obtenir un seul certificat agrégé σ_a, conçu à partir de plusieurs certificats agrégeables. Ce certificat agrégé σ_a peut ensuite être vérifié par différentes entités vérificatrices au moyen d'une preuve de connaissance PoK_σ d'un tel certificat agrégé. Dans la présente invention, une nouvelle preuve de connaissance PoK_σ du certificat agrégé σ_a est générée, de façon distincte, à chaque requête d'accès de l'entité utilisatrice U auprès d'une entité vérificatrice V afin d'empêcher la traçabilité de l'utilisateur.

L'invention se traduit également par un gain potentiel en bande passante et en simplicité d'utilisation dans la mesure où seule une preuve de connaissance d'un certificat agrégé est transmise aux entités vérificatrices V au lieu d'une multitude de certificats distincts et dans la mesure où l'accès à un service tiers ne nécessite pas de preuve dont la quantité de calcul dépendrait du nombre d'attributs initialement certifiés par l'entité émettrice.

En particulier, dans un petit dispositif embarqué, le fait de transmettre des données consomme plus de batterie que de faire un calcul. Pour cette raison, l'agrégation de certificats par l'entité utilisatrice U videra moins la batterie que leur transmission.

La présente invention permet en outre une simplification des procédures lorsqu'un utilisateur doit faire appel à des accréditations provenant d'organisations différentes, puisqu'un seul certificat agrégé est utilisé.

On se réfère maintenant à la **figure 2** qui illustre plus particulièrement l'étape 100 d'attribution d'un certificat σ_i telle qu'employée par le procédé d'accès anonyme à un service selon la présente invention.

Sur cette figure 2 sont représentées, à gauche, les sous-étapes effectuées par l'entité utilisatrice U et, à droite, les sous-étapes effectuées par l'entité certificatrice C_j, ainsi que les différentes données échangées entre ces entités au moyen de leur unité de communication respective.

L'entité utilisatrice U et l'entité certificatrice C_j disposent avantageusement d'une paire de clés privée et publique respective (sk_U,pk_U) et (sk_{Ci},pk_{Ci}), par exemple de paires de clés asymétriques conformément à un schéma de cryptographie à clé publique. Ces clés privées et publiques peuvent être obtenues de la façon suivante :

a) une procédure d'initialisation *SETUP* est d'abord exécutée, au cours de laquelle :

- Un environnement bilinéaire (p, G_1, G_2, e) est choisi où p est un nombre premier, G_1 et G_2 deux groupes d'ordre p et e un couplage bilinéaire applicable à $G_1 \times G_2$. Dans la suite, Z_p désigne l'ensemble des entiers modulo p ;
- une fonction cryptographique de hachage résistante aux collisions $H : \{0,1\}^* \rightarrow G_1$ est choisie ;
- deux générateurs de groupe g_1 et u sont choisis aléatoirement de manière uniforme dans G_1 ; et
- un générateur de groupe g_2 est choisi aléatoirement de manière uniforme dans G_2.

A l'issue de cette procédure d'initialisation, les paramètres globaux $(p,G_1,G_2,e,g_1,g_2,u,H)$ sont disponibles.

b) une procédure de génération de clés *KEY.GEN* est ensuite exécutée, au cours de laquelle :

- Pour l'entité utilisatrice U :

- une variable x est choisie aléatoirement de manière uniforme dans Z_p, laquelle correspond à la clé privée sk_U de l'entité utilisatrice U, i.e. $sk_U = x$;

- la variable $X = g_1^x$ est calculée, laquelle correspond à la clé publique pk_U de l'entité utilisatrice U, i.e. $pk_U = X$.

- Pour chaque entité certificatrice C_j impliquée :

- une variable γ est choisie aléatoirement de manière uniforme dans Z_p, laquelle correspond à la clé privée sk_{Cj} de l'entité certificatrice U, i.e. $sk_{Cj} = \gamma$;

- les variables $\Gamma_{j,1} = g_1^{\gamma}$ et $\Gamma_{j,2} = g_2^{\gamma}$ sont calculées, afin d'obtenir la clé publique pk_{Cj} de l'entité certificatrice C_j, telle que $pk_{Cj} = (\Gamma_{j,1}, \Gamma_{j,2})$.

Une fois ces différents paramètres obtenus au préalable, l'étape 100 d'attribution peut débuter par le calcul (étape 110), par l'entité utilisatrice U, d'une donnée publique C liée à la clé secrète sk_U de l'entité utilisatrice U, cette donnée publique C permettant de masquer la clé secrète sk_U tout en autorisant des calculs impliquant cette clé secrète.

A titre d'exemple, dans un premier mode de réalisation, cette donnée publique liée à la clé secrète sk_U peut être calculée selon la formule suivante :

(1) $$C = u^{sk_U}$$

Une fois la donnée publique C calculée, une première partie R d'une preuve de connaissance PoK_C de cette donnée publique C peut être calculée par l'entité utilisatrice, lors d'une étape 120 de calcul d'une partie au moins de la preuve de connaissance.

Similairement à la donnée publique C, toujours dans un premier mode de réalisation, cette première partie R de la preuve de connaissance PoK_C de la donnée publique C peut être calculée à partir d'une donnée r_x, choisie aléatoirement dans Z_p^*, selon la formule suivante :

(2) $$R = u^{r_x}$$

La donnée publique C et la première partie R de la preuve de connaissance PoK_C de cette donnée publique C sont alors transmises, sous forme de donnée numérique, à l'entité certificatrice C_j (étape 123).

Cette entité certificatrice C_j renvoie en retour un nombre aléatoire c à l'entité utilisatrice U (étape 127), afin de permettre la génération d'une deuxième partie S de la preuve de connaissance PoK_C au moyen de cette variable aléatoire c, ce qui est effectué lors de l'étape 130 de calcul d'une deuxième partie S de la preuve de connaissance PoK_C de la donnée publique C par l'entité utilisatrice U.

Dans un premier mode de réalisation, cette deuxième partie S de la preuve de connaissance PoK_C de la donnée publique C peut ainsi être calculé la formule suivante :

(3) $$S = r_x + c \cdot sk_U$$

Cette deuxième partie S de la preuve de connaissance PoK_C est alors transmise vers l'entité certificatrice C_j (étape 135).

Une fois en possession de la donnée publique C et de la preuve de connaissance PoK_C de cette donnée publique C, l'entité certificatrice C_j peut procéder alors au calcul (étape 150) d'un certificat σ_i au moyen de la donnée publique C liée à la clé secrète sk_U de l'entité utilisatrice U, d'un ou plusieurs attribut(s) $m_1,\ldots, m_{l_j}$ associé(s) à l'entité utilisatrice U et de la clé secrète sk_{Cj} de l'entité certificatrice C_j.

En d'autres termes, cette étape 150 de calcul correspond à la signature, par l'entité certificatrice C_j, d'un ou plusieurs attribut(s) $m_1,\ldots, m_k,\ldots, m_{l_j}$ (où $l_j \geq 1$ est le nombre d'attributs signés par l'entité certificatrice C_j) associé(s) à l'entité utilisatrice U au moyen de sa clé secrète sk_{Cj} en appliquant un schéma de signature agrégeable permettant d'obtenir une signature agrégeable correspondant au certificat σ_j.

A titre d'exemple, dans le premier mode de réalisation introduit précédemment, le certificat σ_i peut être calculé ici selon la formule suivante :

(4) $$\sigma_i = \left(C \cdot \prod_{k=1}^{l_j} H(g_1^{sk_{C_j}} \| g_2^{sk_{C_j}} \| m_k) \right)^{sk_{C_j}} = C^{sk_{C_j}} \cdot \prod_{k=1}^{l_j} \sigma_k'$$

où $\sigma_k' = H(g_1^{sk_{C_j}} \| g_2^{sk_{C_j}} \| m_k)^{sk_{C_j}}$

Ainsi, dans le cas particulier où un seul attribut m_1 est certifié par l'entité certificatrice C_j, c'est-à-dire où $l_j=1$, cette formule (4) devient alors la formule suivante :

(5) $$\sigma_i = \left(C \cdot H(g_1^{sk_{C_j}} \| g_2^{sk_{C_j}} \| m_1) \right)^{sk_{C_j}}$$

Il est avantageux de conditionner ce calcul au résultat d'une étape de vérification de la donnée publique C, afin d'éviter d'attribuer un certificat à un utilisateur non habilité.

Pour ce faire, une fois en possession de la donnée publique C et de la preuve de connaissance PoK_C de cette donnée publique C, et avant tout calcul de certificat, l'entité certificatrice C_j procède à la vérification (étape 140) de la donnée publique C liée à la clé secrète sk_U de l'entité utilisatrice U, au moyen de la preuve de connaissance PoK_C, c'est-à-dire au moyen des première et deuxième parties R et S de la preuve de connaissance PoK_C.

Ainsi, dans le cas du premier mode de réalisation introduit précédemment, cette vérification peut consister à vérifier si l'égalité suivante est bien respectée :

(6) $$u^{s_x} = R \cdot C^c$$

Si le résultat de cette vérification est positif, c'est-à-dire si l'égalité (4) est bien vérifiée, l'entité certificatrice C_j peut alors procéder au calcul du certificat σ_i tel que décrit précédemment. Si ce résultat est négatif, une donnée d'erreur (par exemple une donnée « 0 ») peut être émise et le procédé s'arrête à ce stade.

Une fois calculé, le certificat σ_i est ensuite transmis (étape 155) à l'entité utilisatrice U où il peut être directement utilisé pour obtenir le certificat agrégé σ_a.

Dans un mode particulier de réalisation, une ou plusieurs variable(s) auxiliaires d'information σ_k' telle(s) que $\sigma_k' = H(g_1^{sk_{C_j}} \| g_2^{sk_{C_j}} \| m_k)^{sk_{C_j}}$ peuvent également être transmises à l'entité utilisatrice U à ce stade, et ce pour chaque attribut m_k appartenant à un sous-ensemble M' d'attributs inclus dans l'ensemble de tous les attributs $\{m_k\}_{1 \le k \le l_j}$ signés lors de l'étape 150 de calcul. Ces variables auxiliaires d'information σ_k' peuvent être employées, lors de l'étape 300 d'authentification anonyme auprès d'une entité vérificatrice V, pour cacher certains attributs comme cela est expliqué plus loin.

Une fois reçu par l'entité utilisatrice, il peut être avantageux de vérifier (étape 170) le certificat σ_i dans l'entité utilisatrice, avant de s'en servir pour générer une quelconque preuve de connaissance.

Cette vérification peut être effectuée au moyen de la vérification d'une relation entre le certificat σ_i, les attributs $m_1,\ldots, m_{l_j}$ utilisés lors de la génération de ce certificat σ_i et de la clé secrète sk_U de l'entité utilisatrice U.

Pour reprendre le premier mode de réalisation évoqué précédemment, cette vérification peut consister à vérifier l'égalité suivante :

$$e(\sigma_i, g_2) = e(u, \Gamma_{j,2})^{sk_U} \prod_{k=1}^{l_j} e(H(\Gamma_{j,1} \| \Gamma_{j,2} \| m_k), \Gamma_{j,2}) \quad (7)$$

Si cette relation (7) n'est pas respectée, le résultat de la vérification 170 est négatif, ce qui se traduit par l'émission d'un message d'erreur (par exemple une donnée « 0 ») et la non-validation du certificat σ_i dans l'entité utilisatrice U.

Si cette relation (7) est vérifiée, le résultat de cette vérification est positif : le certificat σ_i est validé et peut être utilisé ultérieurement pour construire un certificat agrégé σ_a permettant de requérir un service impliquant les attributs $m_1,\ldots,m_l$ auprès d'une entité vérificatrice, en combinaison éventuellement avec d'autres attributs certifiés par d'autres entités certificatrices.

Ce certificat σ_j peut être mémorisé à cet effet dans l'entité utilisatrice U, éventuellement conjointement avec les variables auxiliaires d'information σ_k' qui ont été avantageusement reçues de l'entité certificatrice C_j.

Cette étape 100 d'attribution, qui aboutit à l'attribution par une entité certificatrice C_j d'un certain nombre de (au moins un) certificats σ_j, à l'entité utilisatrice U peut être répétée pour chacune des M entités certificatrices d'un ensemble d'entités certificatrices $\{C_j\}_{1 \le j \le M}$, ce qui aboutit à l'attribution à l'entité utilisatrice U d'un ensemble de N certificats $\{\sigma_i\}_{1 \le i \le N}$ délivrés par ces M entités certificatrices, et portant sur un ensemble d'attributs.

On se réfère maintenant à la **figure 3**, laquelle illustre en particulier les étapes de calcul d'un certificat agrégé à partir des certificats attribués à l'entité utilisatrice, de calcul d'une preuve de

connaissance de ces certificats et de vérification de cette preuve de connaissance employées par le procédé d'accès anonyme à un service selon la présente invention.

Sur cette figure 3 sont représentées, à gauche, les sous-étapes effectuées par l'entité utilisatrice U et, à droite, les sous-étapes effectuées par l'entité vérificatrice V, ainsi que les différentes données échangées entre ces entités au moyen de leur unité de communication respectif.

On se place ici dans la situation où, lors de l'étape préalable 100 d'attribution, l'entité utilisatrice a reçu plusieurs certificats $\sigma_1,\ldots,\sigma_i,\ldots,\sigma_N$ attribués respectivement par M entités certificatrices $C_1,\ldots,C_j,\ldots,C_M$.

On procède alors au calcul (étape 200) d'un certificat agrégé σ_a à partir d'un sous-ensemble des certificats $\sigma_1,\ldots,\sigma_i,\ldots,\sigma_k$ préalablement obtenus, par exemple en multipliant ces certificats de sorte que $\sigma_a = \sigma_1 * \ldots * \sigma_i * \ldots * \sigma_N$.

Cette étape 200 d'agrégation peut être effectuée à la volée par l'utilisateur, lorsque celui souhaite requérir un service par l'intermédiaire d'une entité vérificatrice V.

Une fois ce certificat agrégé σ_a obtenu, l'entité utilisatrice U procède au calcul (étape 300) d'une preuve de connaissance PoK_σ des certificats attribués à l'entité utilisatrice au moyen de ce certificat agrégé σ_a.

L'étape 300 de calcul de cette preuve de connaissance PoK_σ peut se décomposer de la façon suivante :

- Un engagement D sur le certificat agrégé σ_a est d'abord calculé (sous-étape 310) au moyen de ce certificat agrégé σ_a et de la clé secrète sk_U de l'entité utilisatrice U, par exemple selon la procédure suivante :

a) on choisit une variable aléatoire r dans Z_p^* ;

b) une première partie d'engagement D_1 est calculée à partir de cette variable aléatoire r, telle que $D_1 = g_1^r$

c) une deuxième partie d'engagement D_2 est calculée à partir de la clé secrète sk_U de l'entité utilisatrice U et du certificat agrégé σ_a, selon la formule $D_2 = \sigma_a^{\frac{1}{sk_U}} \cdot u^r$

L'engagement D sur le certificat agrégé σ_a correspond alors à la paire (D1,D2).

- Une fois cet engagement D calculé par l'entité utilisatrice U, la preuve de connaissance PoK_σ peut être calculée à partir au moins de cet engagement D, de la façon suivante :

a) une première partie P de cette preuve de connaissance PoK_σ peut être calculée par l'entité utilisatrice U, à partir d'une partie au moins de l'engagement D, lors d'une étape 320 de calcul, selon la procédure suivante :

- on choisit trois variables aléatoires r_x, r_r et r_δ dans Z_p^* ;

- on calcule les deux variables $P_1 = g_1^{r_r}$, $P_2 = D_1^{r_x} g_1^{-r_\delta}$

- on calcule également $P_3 = e(D_2, g_2)^{r_x} \cdot e(u, g_2)^{-r_\delta} \cdot e(u, \prod_{j=1}^{N} \Gamma_{j,2})^{-r_x}$;

La première partie P de la preuve de connaissance PoK_σ correspond alors au triplet (P_1,P_2,P_3).

b) L'engagement D et la première partie $P=(P_1,P_2,P_3)$ de la preuve de connaissance PoK_σ sont alors transmis à l'entité vérificatrice V (étape 325), laquelle, suite à la réception de ces données, procède à la sélection d'une valeur aléatoire d dans Z_p^* (étape 330) et envoie en retour cette variable aléatoire d à l'entité utilisatrice U (étape 335).

c) Une fois cette variable d reçue, l'entité utilisatrice U procède alors au calcul d'une deuxième partie T de la preuve de connaissance PoK_σ (étape 340) à partir de cette variable aléatoire d, par exemple selon la procédure suivante :

- une variable s_x est calculée telle que $t_x = r_x + d \cdot sk_u$;

- une variable s_r est calculée telle que $t_r = r_r + d \cdot r$; et

- une variable s_δ est calculée telle que $t_\delta = r_\delta + d \cdot r \cdot sk_u$.

La deuxième partie T de la preuve de connaissance PoK_σ correspond alors au triplet de ces variables, i.e. $T=(t_x,t_r,t_\delta)$.

A l'issue de cette étape 340, la deuxième partie T de la preuve de connaissance PoK_σ est transmise (étape 345) à l'entité vérificatrice V, qui dispose alors de l'engagement D sur le certificat agrégé σ_a , de la valeur aléatoire d et des deux parties P et T de la preuve de connaissance PoK_σ de ce certificat agrégé σ_a.

Il est alors possible d'effectuer une vérification 400, dans l'entité vérificatrice V, de cette preuve de connaissance PoK_σ.

Une telle vérification peut être réalisée en vérifiant si les trois relations suivantes (8)-(10) sont bien respectées :

(8) $$g_1^{t_r} = P_1 \cdot D_1^{d}$$

(9) $$D_1^{t_x} g_1^{-t_\delta} = P_2$$

(10) $$e(D_2, g_2)^{t_x} e(h_1, g_2)^{-t_\delta} e(u, \prod_{j=1}^{N} \Gamma_{j,2})^{-t_x} = P_3 \left(\prod_{j=1}^{N} e\left(\prod_{k=1}^{l_j} H(\Gamma_{j,1} \| \Gamma_{j,2} \| m_k), \Gamma_{j,2} \right) \right)^{d}$$

Si l'une de ces relations (8) à (10) n'est pas respectée, le résultat de la vérification 300 est négatif, ce qui se traduit par l'émission d'un message d'erreur (par exemple une donnée « 0 ») et la non-

attribution du service requis par l'entité utilisatrice U auprès de l'entité vérificatrice. Le procédé d'accès anonyme à ce service s'arrête alors à ce stade.

Par contre, si toutes les relations (8) à (10) sont respectées, le résultat de la vérification 300 est positif et le service requis par l'entité utilisatrice U auprès de l'entité vérificatrice peut être fourni à cette entité utilisatrice U, par exemple en envoyant un message d'autorisation (étape 405) à l'entité utilisatrice U, ce message pouvant comprendre des données correspondant au service requis lui-même.

Dans un mode de réalisation particulier où l'utilisateur souhaite cacher certains des attributs m_k, attribués par l'entité certificatrice C_j et ayant un indice k appartenant à l'ensemble M_j' inclus dans $M_j=\{1,\ldots,l_j\}$, et pour lesquels il a reçu des variables d'information auxiliaires σ_k' telles que $\sigma_k' = H(g_1^{sk_{C_j}} \| g_2^{sk_{C_j}} \| m_k)^{sk_{C_j}}$ lors de l'étape 155 de transmission, le certificat agrégé σ_a peut être modifié à l'issue de l'étape 200 d'agrégation en utilisant ces variables d'information auxiliaires σ_k'.

En particulier, si l'utilisateur souhaite cacher les attributs m_k dont les indices k appartiennent à un sous-ensemble M_j'' inclus dans l'ensemble M_j' ci-avant, l'opération suivante est effectuée sur le certificat agrégé après l'étape 200 d'agrégation, pour le(s) valeur(s) de k appartenant à l'ensemble M_j'' :

$$\sigma_a * \sigma_k'^{-1} \rightarrow \sigma_a$$

Cette transformation du certificat agrégé σ_a au moyen d'une ou plusieurs variable(s) auxiliaire(s) σ_k' calculée pour un ou plusieurs attribut(s) m_k à cacher permet de cacher cet ou ces attribut(s) m_k à l'entité vérificatrice V lors du processus d'authentification de l'entité utilisatrice U.

Dans ce mode particulier de réalisation, la relation (10) à vérifier devient alors la relation modifiée (10') suivante :

$$(10') \qquad e(D_2, g_2)^{t_x} e(h_1, g_2)^{-t_\delta} e(u, \prod_{j=1}^{N} \Gamma_{j,2})^{-t_x} = P_3 \left(\prod_{j=1}^{N} e\left(\prod_{k \in M_j / M_j''} H(\Gamma_{j,1} \| \Gamma_{j,2} \| m_k), \Gamma_{j,2} \right) \right)^d$$

En d'autres termes, cette relation modifiée (10') revient à vérifier une accréditation agrégée sur le sous-ensemble M_j / M_j'' valide sous les clefs publiques Γ_j des entités certificatrices.

On se réfère maintenant à la **figure 4**, laquelle illustre en particulier l'étape d'attribution 100' d'un certificat employée par le procédé d'accès anonyme à un service selon un deuxième mode de réalisation de l'invention.

En effet, il est avantageux de masquer la donnée publique liée à la clé secrète sk_U de l'entité utilisatrice U et la première partie de preuve de connaissance de cette donnée publique générée lors de l'étape d'attribution, afin de mieux protéger l'utilisateur en empêchant l'entité certificatrice C_j de générer des certificats qu'elle pourrait délivrer à la place de l'utilisateur.

Pour ce faire, dans ce deuxième mode de réalisation, la donnée publique correspond à un engagement sur la clé secrète sk_U. Le terme d'« engagement » sur une valeur est entendu ici dans son sens cryptographique et correspond à une donnée (sous forme numérique), non-modifiable et liée à cette valeur, qui permet de garder cette valeur cachée dans un premier temps mais peut être employée

ultérieurement pour révéler cette valeur. Un tel engagement permet de masquer la clé secrète sk_U, tout en garantissant son intraçabilité.

Ainsi, dans le deuxième mode de réalisation illustré sur cette figure 4, l'étape 100' d'attribution peut débuter par le calcul (étape 110'), par l'entité utilisatrice U, d'un engagement C' sur la clé secrète sk_U de l'entité utilisatrice U.

Ce calcul consiste à choisir une variable aléatoire s dans Z_p^* et à calculer l'engagement C' selon la formule modifiée (11) suivante, laquelle remplace alors la formule (1) évoquée précédemment en relation avec l'étape 110 du premier mode de réalisation :

(11) $$C' = u^{sk_u} g_1^{\ s}$$

Une fois cet engagement C' calculé, la première partie R' de la preuve de connaissance PoK_C de cet engagement peut être calculée par l'entité utilisatrice, lors d'une étape 120' de calcul, en choisissant deux variables aléatoires r_x et r_s dans Z_p^* et en calculant la valeur R' selon la formule modifiée (12) suivante, laquelle remplace alors la formule (2) évoquée précédemment en relation avec l'étape 120 du premier mode de réalisation :

(12) $$R' = u^{r_x} g_1^{\ r_s}$$

L'engagement C' et la première partie R' de la preuve de connaissance $PoK_{C'}$ de cet engagement C' sont alors transmises à l'entité certificatrice C_j (étape 123').

Suite à la réception de ces données, l'entité certificatrice C_j procède à la sélection d'une variable aléatoire c' dans Z_p^* (étape 125') et envoie en retour cette variable aléatoire c' à l'entité utilisatrice U (étape 127').

Une fois cette variable c' reçue, l'entité utilisatrice U procède alors au calcul d'une deuxième partie S' de la preuve de connaissance $PoK_{C'}$ de l'engagement C' (étape 130'), cette deuxième partie S' correspondant à la paire de variables (s_x, s_s) calculées selon les formules modifiées (13) et (14) suivantes, lesquelles remplacent ainsi la formule (3) évoquée précédemment en relation avec l'étape 130 du premier mode de réalisation :, selon la procédure suivante :

(13) $$s_x = r_x + c' \cdot sk_u$$

(14) $$s_s = r_s + c' \cdot s\,.$$

La deuxième partie S' de la preuve de connaissance $PoK_{C'}$ telle que $S'=(s_x, s_s)$ est alors transmise vers l'entité certificatrice C_j (étape 135').

Une fois en possession de l'engagement C', de la première partie R' de la preuve de connaissance $PoK_{C'}$ et de la deuxième partie $S'=(s_x, s_s)$ de cette preuve de connaissance $PoK_{C'}$, l'entité certificatrice C_i peut procéder à la vérification (étape 140') de l'engagement C' en vérifiant si la relation modifiée (15)

suivante, correspondant à la relation (6) évoquée en relation avec l'étape 140 du premier mode de réalisation, est bien respectée :

(15) $$u^{s_x} g_1^{s_s} = R' \cdot C'^{c'}$$

Si cette relation modifiée (5') n'est pas respectée, le résultat de la vérification 140' est négatif, ce qui se traduit par l'émission d'un message d'erreur et la non-attribution d'un certificat à l'entité utilisatrice U. L'étape 100' d'attribution du certificat s'arrête alors à ce stade.

Si, par contre, la relation modifiée (15) est respectée, le résultat de la vérification 140' est positif et l'étape 100' d'attribution peut se poursuivre par le calcul (étape 150') d'un certificat σ_i selon la formule (16) suivante, laquelle correspond à la formule (4) employée lors de l'étape 150 de calcul du premier mode de réalisation :

(16) $$\sigma_i = \left(C' \cdot \prod_{k=1}^{l} H(g_1^{sk_{Cj}} \| g_2^{sk_{Cj}} \| m_k) \right)^{sk_{Cj}}$$

Le certificat σ_i ainsi obtenu correspond au certificat obtenu par la formule (5) dans le premier mode de réalisation multiplié par la variable $g_1^{s \cdot sk_{Cj}}$ et est donc masqué par une telle variable. Ce certificat σ_i n'est alors pas agrégeable en tant que tel et ne peut donc pas être utilisé directement par l'entité utilisatrice U lors de l'étape 200 d'agrégation. A ce titre, ce certificat σ_i est un certificat provisoire qui est alors transmis (étape 155') par l'entité certificatrice C_j à l'entité utilisatrice U.

Afin de rendre son caractère agrégeable à ce certificat provisoire σ_i reçu de l'entité certificatrice C_j, ce certificat provisoire σ_i est ensuite démasqué (étape 160') par l'entité utilisatrice U, selon la formule (17) suivante :

(17) $$\sigma_i \cdot \Gamma_{j,1}^{-s} = \sigma_i \cdot \left(g_1^{sk_{Cj}} \right)^{-s} \rightarrow \sigma_i$$

Cette opération de démasquage permet d'obtenir un certificat définitif σ_i respectant la relation de la formule (4) (i.e. où $\sigma_i = \left(C \cdot \prod_{k=1}^{l} H(g_1^{sk_{Cj}} \| g_2^{sk_{Cj}} \| m_k) \right)^{sk_{Cj}}$) et donc agrégeable avec d'autres certificats agrégeables.

Ce certificat définitif σ_i est ensuite avantageusement vérifié (étape 170') au moyen de la relation (7) évoquée en relation avec l'étape 170 du premier mode de réalisation.

Comme pour le premier mode de réalisation, cette étape 100' d'attribution selon un deuxième mode de réalisation, qui aboutit à l'attribution par une entité certificatrice C_j d'un certificat provisoire

démasqué en un certificat définitif σ_i par l'entité utilisatrice U, peut être répétée pour chacune des M entités certificatrices C_j d'un ensemble d'entités certificatrices $\{C_j\}_{1\leq j\leq M}$, ce qui aboutit à l'attribution à l'entité utilisatrice U d'un ensemble de N certificats $\{\sigma_i\}_{1\leq i\leq N}$, délivrés respectivement par chacune des M entités certificatrices $C_1,\ldots,C_j,\ldots,C_M$.

Dans ce deuxième mode de réalisation de l'étape d'attribution, la quantité de données fournies par l'utilisateur de l'entité utilisatrice U à l'entité vérificatrice V, sous forme d'attributs associés à cet utilisateur, est minimisé.

On se réfère maintenant à la **figure 5**, laquelle illustre également l'étape 100'' d'attribution d'un certificat, telle qu'employée par le procédé d'accès anonyme à un service, selon un troisième mode de réalisation de l'invention.

Ce troisième mode de réalisation s'applique au cas où l'entité utilisatrice U possède déjà N certificats $\sigma_1,\ldots, \sigma_N$, obtenus auprès de différentes entités certificatrices $C_1,\ldots,C_j,\ldots,C_M$ et sollicite l'attribution d'un nouveau certificat σ_{N+1} auprès d'une nouvelle entité certificatrice C_{j+1}, tout en cherchant à minimiser les données fournies à cette nouvelle entité certificatrice C_{j+1}.

Pour illustrer ce troisième mode de réalisation, on se place dans la situation où l'entité utilisatrice a calculé un certificat agrégé σ_a à partir des N certificats $\sigma_1,\ldots, \sigma_N$, déjà attribués, c'est-à-dire dans le cas où : $\sigma_a = \prod_{i=1}^{N} \sigma_i$

Dans ce troisième mode de réalisation tel qu'illustré sur cette figure 5, l'étape 100'' d'attribution débute également par le calcul (étape 110''), par l'entité utilisatrice U, d'une donnée publique C'' liée à la clé secrète sk_U de l'entité utilisatrice U.

Cette donnée publique C'' comprend une première partie de donnée publique C_0'' liée à la clé secrète sk_U, par exemple calculée selon la procédure suivante dans laquelle cette première partie de donnée publique correspond à un engagement sur cette clé secrète sk_U, similairement à ce qui a été précédemment décrit pour l'étape 110' :

a) on choisit une variable aléatoire s dans Z_p^* ;

b) on calcule $C_0'' = u^{sk_u} g_1^{\ s}$

Outre cette première partie de donnée publique C_0'', une deuxième partie de donnée publique C_1'' est calculée selon la procédure suivante :

a) on choisit une variable aléatoire r dans Z_p^* ;

b) on calcule $C_1'' = g_1^{\ r}$

Enfin, une troisième partie de donnée publique C_2'' liée à la clé secrète sk_U et au certificat agrégé σ_a est calculée à partir de la clé secrète sk_U de l'entité utilisatrice U et du certificat agrégé σ_a, par exemple selon la formule (18) suivante où cette troisième partie de donnée publique C_2'' correspond à un engagement sur la clé secrète sk_U de l'entité utilisatrice U et le certificat agrégé σ_a:

(18) $$C_2'' = \sigma_a^{\frac{1}{sk_U}} \cdot u^r$$

Ainsi la donnée publique C'' correspond au triplet de données publiques (C_0'',C_1'',C_2'') et porte aussi bien sur la clé secrète sk_U de l'entité utilisatrice U que sur le certificat agrégé σ_a possédé par l'entité utilisatrice U.

Une fois cette donnée publique C'' calculée, la première partie R'' de la preuve de connaissance $PoK_{C''}$ de cette donnée publique C'' peut être calculée par l'entité utilisatrice U, lors d'une étape 120'' de calcul, selon la procédure suivante :

a) on choisit quatre variables aléatoires r_x, r_s, r_r et r_δ dans Z_p^* ;

b) on calcule $R_0 = u^{r_x} g_1^{r_s}$, $R_1 = g_1^{r_r}$, $R_2 = (C_1'')^{r_x} g_1^{-r_\delta}$

c) on calcule $R_3 = e(C_2'', g_2)^{r_x} \cdot e(u, g_2)^{-r_\delta} \cdot e(u, \prod_{j=1}^{N} \Gamma_{j,2})^{-r_x}$;

La donnée publique C''=(C_0'',C_1'',C_2'') et la première partie R'=(R_0,R_1,R_2,R_3) de la preuve de connaissance $PoK_{C''}$ de cette donnée publique C'' sont alors transmises à l'entité certificatrice C_{N+1} (étape 123''), laquelle, suite à la réception de ces données, procède à la sélection d'une variable aléatoire c'' dans Z_p (étape 125'') et renvoie en retour cette variable aléatoire c'' à l'entité utilisatrice U (étape 127'').

Une fois cette variable c'' reçue, l'entité utilisatrice U procède alors au calcul d'une deuxième partie S'' de la preuve de connaissance $PoK_{C''}$ de cette donnée publique C'' (étape 130'') selon la procédure suivante :

a) une variable s_x est calculée telle que $s_x = r_x + c'' \cdot sk_u$;

b) une variable s_s est calculée telle que $s_s = r_s + c'' \cdot s$;

c) une variable s_r est calculée telle que $s_r = r_r + c'' \cdot r$; et

d) une variable s_δ est calculée telle que $s_\delta = r_\delta + c'' \cdot r \cdot sk_u$.

La deuxième partie S'' de la preuve de connaissance $PoK_{C''}$ correspond alors au quadruplet de variables $(s_x,s_s,,s_r,s_\delta)$, qui est alors transmis vers l'entité certificatrice C_j (étape 135'').

Une fois en possession de la donnée publique C'', de la première partie R'' de la preuve de connaissance $PoK_{C''}$ et de la deuxième partie S'' de cette preuve de connaissance $PoK_{C''}$, l'entité certificatrice C_{j+1} procède alors avantageusement à la vérification (étape 140'') de la donnée publique C'', en vérifiant si les quatre relations suivantes (19)-(22) sont bien respectées :

(19) $$u^{s_x} g_1^{s_s} = R_0 \cdot (C_0'')^{c''}$$

(20) $$g_1^{s_r} = R_1 \cdot (C_1'')^{c''}$$

(21) $$(C_1'')^{s_x} g_1^{-s_\delta} = R_2$$

(22) $$e(C_2'', g_2)^{s_x} e(h_1, g_2)^{-s_\delta} e(u, \prod_{j=1}^{N} \Gamma_{j,2})^{-s_x} = R_3 \left(\prod_{j=1}^{N} e\left(\prod_{i=1}^{l_j} H(\Gamma_{j,1} \| \Gamma_{j,2} \| m_{j,i}), \Gamma_{j,2} \right) \right)^{c''}$$

Si l'une de ces relations (19) à (22) n'est pas respectée, le résultat de la vérification 140'' est négatif, ce qui se traduit par l'émission d'un message d'erreur (par exemple une donnée « 0 ») et la non-attribution d'un certificat σ_{N+1} à l'entité utilisatrice U. L'étape 100'' d'attribution du certificat s'arrête alors à ce stade.

Par contre, si toutes les relations (19) à (22) sont respectées, le résultat de la vérification 140'' est positif et l'étape 100'' d'attribution peut se poursuivre par le calcul (étape 150'') du certificat σ_{N+1} selon la formule (23) suivante :

(23) $$\sigma_{N+1} = \left(C_0'' \cdot \prod_{k=1}^{l} H(g_1^{sk_{Cj}} \| g_2^{sk_{Cj}} \| m_k) \right)^{sk_{Cj}}$$

Ce certificat σ_{N+1}, lequel est un certificat provisoire au sens où il n'est pas agrégeable en tant que tel, est alors transmis (étape 155'') par l'entité certificatrice C_{j+1} à l'entité utilisatrice U, où il peut être ensuite transformé en un certificat démasqué (i.e. agrégeable) σ_{N+1} par l'entité utilisatrice U (étape 160''), selon la formule (24) suivante :

(24) $$\sigma_{N+1} \cdot \Gamma_{j+1,1}^{-s} = \sigma_{N+1} \cdot \left(g_1^{sk_{C_{j+1}}} \right)^{-s} \rightarrow \sigma_{N+1}$$

Ce nouveau certificat σ_{N+1} est ensuite avantageusement vérifié (étape 170'') au moyen de la relation (25) suivante :

(25) $$e(\sigma_{N+1}, g_2) = e(u, \Gamma_{j+1,2})^{sk_U} \prod_{k=1}^{l} e(H(\Gamma_{j+1,1} \| \Gamma_{j+1,2} \| m_l), \Gamma_{j+1,2})$$

Si cette relation (25) n'est pas respectée, le résultat de la vérification 170'' est négatif, ce qui se traduit par l'émission d'un message d'erreur (par exemple une donnée « 0 ») et la non-validation du certificat σ_{N+1} dans l'entité utilisatrice U.

Par contre, si la relation (25) est respectée, le résultat de la vérification 170'' est positif et le certificat σ_{N+1} est validé. Il peut alors être mémorisé par l'entité utilisatrice U afin d'être utilisé ultérieurement pour requérir anonymement un service impliquant un des attributs $m_1,\ldots,m_l$ auprès d'une entité vérificatrice V.

On notera ici qu'à la différence des certificats σ_i individuellement attribués dans les premier et deuxième modes de réalisation de l'étape d'attribution du procédé, le certificat σ_{N+1} obtenu dans le troisième mode est un certificat obtenu sur présentation d'un certain nombre de certificats précédemment attribués. Il est ainsi possible de reproduire cette étape 100'' d'attribution avec une nouvelle entité certificatrice C_{N+2}, ce qui aboutira à l'attribution d'un nouveau certificat σ_{N+2}, et ainsi de suite, de façon itérative.

On se réfère enfin à la **figure 6** qui représente schématiquement un système d'accréditation anonyme SAA pour l'accès anonyme à un service, dans lequel est mis en œuvre le procédé d'accès anonyme à un service décrit précédemment.

Ce système d'accréditation anonyme SAA comprend :

- une entité utilisatrice U, utilisée par un utilisateur pour requérir anonymement un service auprès d'une entité vérificatrice grâce à au moins un ou plusieurs certificat(s) anonyme(s) σ_j attribué(s) par au moins une entité certificatrice C_j ;
- au moins une entité certificatrice C_j, apte à accréditer anonymement une entité utilisatrice U, en lui attribuant un ou plusieurs certificat(s) anonyme(s) σ_j ; et
- au moins une entité vérificatrice V, apte à vérifier anonymement l'entité utilisatrice U et à lui fournir un service SERV après vérification d'une preuve de connaissance PoK_σ portant sur un ou plusieurs certificat(s) anonyme(s).

Sur la figure 6 sont illustrées M entités certificatrices distinctes $C_1,\ldots,C_j,\ldots,C_M$, ce nombre M pouvant être n'importe quel nombre entier supérieur ou égal à 1. Seule l'entité certificatrice C_j est décrite en détail, les autres entités certificatrices étant similaires à cette entité C_j.

Cette entité certificatrice C_j peut être un dispositif informatique de type serveur appartenant à une organisation certificatrice telle qu'une mairie, une université, une préfecture, etc.

Cette entité certificatrice C_j comprend en particulier une unité de calcul $CALC_{Cj}$ arrangée pour mettre en œuvre l'étape 100 d'attribution d'un certificat A_i à l'entité utilisatrice U telle que décrite ci-

avant. Une telle unité de calcul $CALC_{Cj}$ peut consister en un processeur, un micro-processeur, ou bien un ordinateur personnel ou un serveur comprenant un tel processeur.

Cette entité certificatrice C_i comprend en outre une unité de communication COM_{Cj} adaptée pour transmettre le certificat provisoire A_i généré par l'unité de calcul $CALC_{Cj}$ à l'entité utilisatrice U auquel il est attribué. Cette unité de communication COM_{Cj} peut être implémentée avec des dispositifs de transmission de type radiofréquence, sans-fil ou optique, ou filaires, capables de transmettre des données numériques correspondant à un certificat provisoire A_i vers l'entité utilisatrice U, aussi bien que de recevoir de celle-ci des données numériques correspondant à un engagement C et une preuve de connaissance PoK_C de cet engagement C.

Cette entité certificatrice C_j peut comprendre en outre une unité de mémorisation MEM_{Cj}, connectée à l'unité de calcul $CALC_{Cj}$ et capable de mémoriser les attributs $m_1,\ldots,m_l$ associés à l'utilisateur de l'entité utilisatrice U afin de pouvoir les fournir ultérieurement à l'unité de calcul $CALC_{Cj}$ lorsque celle-ci est amenée à générer un certificat A_i . Cette unité de mémorisation MEM_{Ci} comprend en outre une partie sécurisée capable de stocker la clé secrète sk_{Cj} attribuée à l'entité certificatrice C_j.

L'entité vérificatrice V, quant à elle, peut être un dispositif informatique de type serveur appartenant à un organisme tiers apte à délivrer un service, tel que des transports publics, un organisme vendant des billets de concert ou de musée, délivrant des tickets restaurant pour des étudiants, ou donnant accès à des équipements de type bibliothèque ou piscine, entre autres.

Cette entité vérificatrice V comprend une unité de communication COM_V capable de recevoir une preuve de connaissance PoK_σ d'une pluralité de certificats $\sigma_1,\ldots,\sigma_i,\ldots,\sigma_N$ attribués à l'entité utilisatrice. Cette unité de communication COM_V peut être implémentée similairement à l'unité de communication COM_{Ci} décrite ci-avant.

Cette entité vérificatrice V comprend en outre une unité de calcul $CALC_V$ capable d'appliquer l'étape de vérification 400 décrite ci-avant à une preuve de connaissance PoK_σ reçue de l'entité utilisatrice U et à déclencher la fourniture d'un service SERV à cette entité utilisatrice U en fonction du résultat de cette vérification. Cette unité de calcul $CALC_V$ peut être implémentée similairement à l'unité de communication $CALC_{Cj}$ décrite ci-avant.

Dans un mode de réalisation, l'entité vérificatrice V correspond à l'entité fournissant un service, auquel cas l'entité vérificatrice V comprend une unité de fourniture de service, qui peut être l'unité de calcul $CALC_V$ elle-même lorsqu'il s'agit de calculer une réduction en fonction de l'âge d'un utilisateur, par exemple. Dans un autre mode de réalisation, l'entité vérificatrice V n'est pas elle-même l'entité fournissant un service, mais prend le rôle d'intermédiaire vérificateur. Dans ce cas, l'unité de communication COM_V est apte, en outre, à communiquer avec l'entité fournissant le service requis par l'entité utilisatrice U, afin de déclencher la fourniture du service après que l'unité de calcul $CALC_V$ ait vérifié la preuve de connaissance PoK_σ reçue de l'entité utilisatrice U.

L'entité utilisatrice U, pour sa part, peut prendre la forme d'un dispositif informatique de type ordinateur personnel ou d'un smartphone, voire d'une carte à puce ou d'une étiquette RFID, et comprend une unité de communication COM_U, similaire aux unités COM_V et COM_C décrite précédemment, capable de recevoir au moins un certificat A_i calculé par une entité certificatrice C_i et de transmettre une preuve de connaissance PoK_σ construite à partir des certificats A_i reçus de différentes entité certificatrices à l'entité vérificatrice V afin de requérir un service SERV.

L'entité utilisatrice U comprend en outre une unité de calcul $CALC_U$ capable de mettre en œuvre l'étape 300 de calcul de la preuve de connaissance PoK_σ d'une pluralité de certificats $\sigma_1,\ldots,\sigma_i,\ldots,\sigma_N$ attribués à l'entité utilisatrice, telle que décrite ci-avant. Une telle unité de calcul $CALC_U$ peut être implémentée similairement aux unités de calcul $CALC_{Cj}$ et $CALC_V$ décrites ci-avant.

Cette entité utilisatrice U peut comprendre en outre une unité de mémorisation MEM_U, connectée à l'unité de calcul $CALC_U$ et capable de mémoriser les différents certificats $A_1,\ldots,A_i,\ldots,A_N$ reçus des entités certificatrices, les certificats $\sigma_1,\ldots,\sigma_i,\ldots,\sigma_N$ avantageusement obtenus respectivement par démasquage de ces certificats $A_1,\ldots,A_i,\ldots,A_N$ lorsque ces derniers sont des certificats provisoires, ainsi que le certificat agrégé σ_a obtenu à partir de ces certificats. Cette unité de mémorisation MEM_U comprend en outre une partie sécurisée capable de stocker la clé secrète sk_U attribuée à l'entité utilisatrice U.

La présente invention vise en outre un programme d'ordinateur comprenant des instructions pour la mise en œuvre de l'étape de génération d'un certificat A_i au moyen d'au moins un attribut m_k ci-avant, lorsque ce programme d'ordinateur est exécuté par l'unité de calcul $CALC_{Cj}$ située dans l'entité certificatrice C_j décrite ci-avant.

La présente invention vise aussi un programme d'ordinateur comprenant des instructions pour la mise en œuvre de l'étape 300 de génération d'une preuve de connaissance PoK_σ d'une pluralité de certificats attribués à une entité utilisatrice U lorsque ce programme d'ordinateur est exécuté par l'unité de calcul $CALC_U$ située dans l'entité utilisatrice U décrite ci-avant.

La présente invention vise en outre un programme d'ordinateur comprenant des instructions pour la mise en œuvre de l'étape 400 de vérification, au moyen d'une telle preuve de connaissance PoK_σ, d'au moins un certificat attribué à une entité utilisatrice U lorsque ce programme d'ordinateur est exécuté par l'unité de calcul $CALC_V$ située dans l'entité vérificatrice V décrite ci-avant.

Ces programmes peuvent utiliser n'importe quel langage de programmation, et être sous la forme d'un code source, code objet, ou de code intermédiaire entre code source et code objet, tel que dans une forme provisoirement compilée, ou dans n'importe quelle autre forme souhaitable.

L'invention vise aussi un support d'informations lisible par un ordinateur ou processeur de données, et comportant les instructions d'un des programmes mentionnés ci-dessus. Un tel support d'informations peut être n'importe quelle entité ou dispositif capable de stocker le programme. Par exemple, le support peut comporter un moyen de stockage, tel qu'une ROM, par exemple un CD-ROM

ou une ROM de circuit microélectronique, ou encore un moyen d'enregistrement magnétique, par exemple une disquette ou un disque dur.

Ce support d'informations peut aussi être un support transmissible tel qu'un signal électrique ou optique, qui peut être acheminé via un câble électrique ou optique, par radio ou par d'autres moyens. Le programme selon l'invention peut être en particulier téléchargé sur un réseau de type Internet. Alternativement, le support d'informations peut être un circuit intégré dans lequel le programme est incorporé, le circuit étant adapté pour exécuter ou pour être utilisé dans l'exécution du procédé en question.

La présente invention peut trouver application dans tous les domaines dans lesquels des services sont fournis à des utilisateurs en fonction de la fourniture d'informations personnelles concernant ces utilisateurs.

La présente invention est notamment particulièrement avantageuse lorsqu'un organisme tiers ne fournit un service que sur la base du croisement d'informations personnelles d'un utilisateur certifiées par une ou (avantageusement) plusieurs organisations certificatrices distinctes, ce qui amène habituellement l'utilisateur à révéler des informations personnelles, non nécessaires en elles-mêmes à l'obtention de ce service mais fournies conjointement avec les informations nécessaires à l'obtention de ce service dans les certificats, à cet organisme tiers.

A titre d'exemple, un premier certificat peut être délivré par une mairie sur la base d'un attribut d'un utilisateur prouvant qu'il habite une ville bien précise, parmi d'autres attributs personnels. Un deuxième certificat peut être délivré par une université sur la base d'un attribut de cet utilisateur prouvant qu'il est bien étudiant dans cette université, parmi d'autres attributs personnels comme son âge.

Avec la présente invention, l'utilisateur peut alors agréger ces deux certificats afin de requérir une réduction auprès d'un service de transport public qui n'accorde de telles réductions qu'aux habitants de cette ville précise qui sont étudiants. En utilisant le procédé d'accès anonyme de la présente invention, l'utilisateur peut alors obtenir cette réduction spécifique aux seuls étudiants de cette ville, sans avoir besoin de dévoiler d'autres informations personnelles.

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.

La présente invention peut ainsi s'appliquer au cas où un seul attribut m_1 est certifié, ce qui correspond au cas où une entité certificatrice émet des certificats sur ce seul attribut m_1. Un schéma simple et efficace est ainsi obtenu. Dans ce cas, l'entité certificatrice signe l'attribut m_1, qui peut se présenter sous la forme d'un document, lequel peut être en l'occurrence n'importe quelle suite de bits, courte ou longue.

La présente invention peut également s'appliquer au cas où plusieurs attributs $m_{1,}\ldots, m_{l_j}$ sont certifiés, avec $l_j>1$. Dans ce cas, un document m à signer peut être séparé en plusieurs sous-documents

$m_{I_1}, \ldots, m_{I_j}$, ce qui permet de laisser la liberté à l'utilisateur de cacher certains sous-documents lorsqu'il montre ses accréditations, tout en lui interdisant de cacher d'autres sous-documents.

Par ailleurs, un mode de réalisation particulier de preuve de connaissance a été décrit dans le mode de réalisation illustré à la figure 3 en ce qui concerne la preuve de connaissance PoK_σ du certificat agrégé σ_a envoyée à l'entité vérificatrice V lors de la phase d'authentification correspondant aux étapes 300 et 400.

Il est cependant évident que la présente invention ne se limite à ce seul mode de réalisation et que la preuve de connaissance PoK_σ du certificat agrégé σ_a envoyée à l'entité vérificatrice V peut consister en une autre forme de donnée publique construite à partir de ce certificat agrégé et permettant de prouver que l'entité utilisatrice U a la connaissance de ce certificat agrégé σ_a et que les certificats composant ce certificat agrégé ont bien été attribués à l'entité utilisatrice U par une ou plusieurs entité(s) certificatrice(s), sans pour autant dévoiler ces certificats eux-mêmes, ni le certificat agrégé, à l'entité vérificatrice V.

Revendications

1. Procédé d'accès anonyme à un service, caractérisé par :

l'attribution (100), par au moins une entité certificatrice (C_j), d'une pluralité de certificats (σ_1,$\sigma_{N'}$) à une entité utilisatrice (U), lesdits certificats étant calculés à partir d'au moins un attribut (m_k) associé à l'entité utilisatrice ;

le calcul (200), par l'entité utilisatrice (U), d'un certificat agrégé (σ_a) à partir d'une pluralité de certificats (σ_1,σ_N) parmi les certificats attribués à l'entité utilisatrice (U) ;

le calcul (300), par l'entité utilisatrice (U), d'une preuve de connaissance (PoK_σ) du certificat agrégé (σ_a) ; et

une vérification (400), effectuée par une entité vérificatrice (V), d'au moins un desdits certificats au moyen de ladite preuve de connaissance (PoK_σ), l'accès au service étant fourni par l'entité vérificatrice à l'entité utilisatrice en fonction du résultat de ladite vérification.

2. Procédé d'accès anonyme à un service selon la revendication 1, caractérisé en ce que l'attribution (100) de la pluralité de certificats à l'entité utilisatrice comprend, pour chacun des certificats attribués par une entité certificatrice (C_j) :

le calcul (150) d'un certificat (σ_i) au moyen d'une donnée publique (C) liée à une clé secrète (sk_U) de l'entité utilisatrice, d'au moins un attribut (m_k) associé à l'entité utilisatrice et d'une clé secrète (sk_{Cj}) de l'entité certificatrice; et

la transmission (155) du certificat (σ_i) à l'entité utilisatrice (U).

3. Procédé d'accès anonyme à un service selon la revendication 2, caractérisé en ce que le certificat (σ_i) est calculé dans le cadre des environnements bilinéaires munis de couplages selon la formule suivante :

$$\sigma_i = \left(C \cdot \prod_{k=1}^{l_j} H(g_1^{sk_{Cj}} \| g_2^{sk_{Cj}} \| m_k) \right)^{sk_{Cj}}$$

où σ_i représente le certificat, C représente la donnée publique C liée à la clé secrète de l'entité utilisatrice, lj représente le nombre d'attributs signés par l'entité certificatrice C_j, H représente une fonction cryptographique de hachage, g_1 et g_2 représentent deux générateurs de groupe choisis aléatoirement et de manière uniforme respectivement dans deux groupes d'ordre p, où p est un nombre entier premier, sk_{Cj} représente la clé secrète de l'entité certificatrice, et m_k représente un attribut associé à l'entité utilisatrice.

4. Procédé d'accès anonyme à un service selon l'une des revendications 2 ou 3, dans lequel le certificat (σ_i) calculé par l'entité certificatrice (C_j) est un certificat provisoire, l'étape d'attribution (100') étant caractérisée en ce que :

la donnée publique liée à la clé secrète (sk_U) de l'entité utilisatrice est un engagement (C') sur la clé secrète (sk_U) de l'entité utilisatrice calculé (110'') dans l'entité utilisatrice (U) au moyen d'une variable aléatoire (s) avant d'être transmis (123') à l'entité certificatrice (C_j);

le certificat provisoire reçu par l'entité utilisatrice (U) est démasqué (160') au moyen de ladite variable aléatoire (s) afin d'obtenir le certificat (σ_i) attribué à l'entité utilisatrice (U).

5. Procédé d'accès anonyme à un service selon la revendication 4, caractérisé en ce que le démasquage (160) du certificat provisoire (A_i) comprend le calcul du certificat (σ_i) attribué à l'entité utilisatrice (U) en multipliant le certificat reçu de l'entité certificatrice par la variable $(g_1^{sk_{Cj}})^{-s}$, où g_1 représente un générateur de groupe choisi aléatoirement et de manière uniforme dans un groupe d'ordre p, où p est un nombre entier premier, sk_{Cj} représente la clé secrète de l'entité certificatrice et s est une valeur aléatoirement choisie dans l'ensemble Z_p des entiers modulo p.

6. Procédé d'accès anonyme à un service selon la revendication 4 ou 5, caractérisé en ce que le certificat (σ_i) attribué à l'entité utilisatrice (U) est vérifié (170) par l'entité utilisatrice après le démasquage (160) du certificat provisoire.

7. Procédé d'accès anonyme à un service selon l'une des revendications 2 à 6, l'étape d'attribution (100) étant caractérisée en ce que :

la donnée publique (C) liée à la clé secrète (sk_U) de l'entité utilisatrice est vérifiée (140) au moyen d'une preuve de connaissance (R,S) de ladite donnée publique (C) ; et

le calcul (150) du certificat (A_i) n'est effectué que si le résultat de la vérification (140) de l'engagement est positif.

8. Procédé d'accès anonyme à un service selon l'une des revendications 2 à 7, l'étape d'attribution (100) étant caractérisée par :

le calcul (110,110''), par l'entité utilisatrice, d'une donnée publique (C) liée à la clé secrète (sk_U) de l'entité utilisatrice ;

le calcul (120) d'une première partie (R) de la preuve de connaissance à partir de la donnée publique (C) liée à la clé secrète (sk_U); et

le calcul (130) d'une deuxième partie (S) de la preuve de connaissance à partir d'une donnée aléatoire (c) reçue de l'entité certificatrice.

9. Procédé d'accès anonyme à un service selon la revendication 8, caractérisé en ce que le calcul (110'') de la donnée publique (C'') comprend :

le calcul d'une première partie (C_0'') de ladite donnée publique liée à la clé secrète (sk_U) de l'entité utilisatrice ; et

le calcul d'une deuxième partie (C_2'') de la donnée publique liée à la clé secrète (sk_U) de l'entité utilisatrice et à au moins un certificat attribué par une autre entité certificatrice.

10. Procédé d'accès anonyme à un service selon l'une des revendications 1 à 9, caractérisé en ce que le calcul (300) de la preuve de connaissance (PoK_σ) de la pluralité de certificats (σ_i) attribués à l'entité utilisatrice comprend :

le calcul (310) d'un engagement (D) sur le certificat agrégé (σ_a) ;

le calcul (320) d'une première partie (P) de la preuve de connaissance (PoK_σ) à partir de l'engagement (D) sur le certificat agrégé (σ_a) ;

le calcul (340) d'une deuxième partie (T) de la preuve de connaissance (PoK_σ) à partir d'une donnée aléatoire (d) reçue de l'entité vérificatrice (V).

11. Programme d'ordinateur comprenant des instructions pour la mise en œuvre respectivement de l'étape de calcul d'un certificat (σ_i), l'étape de génération d'une preuve de connaissance d'une pluralité de certificats attribués à une entité utilisatrice et l'étape de vérification au moyen de ladite preuve de connaissance d'une pluralité de certificats selon l'une des revendications 1 à 10, lorsque ce programme d'ordinateur est exécuté par une unité de calcul située respectivement dans une entité certificatrice (C_j), une entité utilisatrice (U) et une entité vérificatrice (V).

12. Entité certificatrice (C_j) apte à accréditer une entité utilisatrice (U), caractérisée en ce qu'elle comprend :

une unité de calcul ($CALC_{Cj}$) apte à mettre en œuvre l'étape de calcul d'un certificat (σ_i) à partir d'au moins un attribut (m_k) du procédé d'accès anonyme selon l'une des revendications 1 à 10; et

une unité de communication (COM_{Cj}) apte à transmettre ledit certificat (σ_i) à l'entité utilisatrice (U).

13. Entité vérificatrice (V) apte à vérifier une entité utilisatrice (U), caractérisée en ce qu'elle comprend :

une unité de communication (COM_V) apte à recevoir une preuve de connaissance (PoK_σ) d'une pluralité de certificats attribués à l'entité utilisatrice ; et

une unité de calcul ($CALC_V$) apte à mettre en œuvre l'étape de vérification (400) du procédé d'accès anonyme selon l'une des revendications 1 à 10 au moyen de ladite preuve de connaissance, afin de démarrer la fourniture d'un service à l'entité utilisatrice en fonction du résultat de la vérification.

14. Entité utilisatrice (U) apte à requérir un service par l'intermédiaire d'une entité vérificatrice (V) au moyen d'une preuve de connaissance (PoK_σ) d'une pluralité de certificats attribués à l'entité utilisatrice par au moins une entité certificatrice (C_j), l'entité utilisatrice (U) étant caractérisée en ce qu'elle comprend :

une unité de communication (COM_U) apte à recevoir une pluralité de certificats (σ_i) provenant d'au moins une entité certificatrice (C_j) ; et

une unité de calcul ($CALC_U$) apte à mettre en œuvre l'étape (300) de calcul d'une preuve de connaissance (PoK_σ) du procédé d'accès anonyme selon l'une des revendications 1 à 10 à partir de la pluralité de certificats (σ_i) reçus,

l'unité de communication (COM_U) étant apte, en outre, à transmettre la preuve de connaissance (PoK_σ) à l'entité vérificatrice (V) afin de requérir un service.

15. Système d'accréditation anonyme (SAA) pour l'accès anonyme à un service, caractérisé en ce que le système comprend :

au moins une entité certificatrice (C_j) selon la revendication 12 ;

une entité vérificatrice (V) selon la revendication 13 ; et

une entité utilisatrice (U) selon la revendication 14.

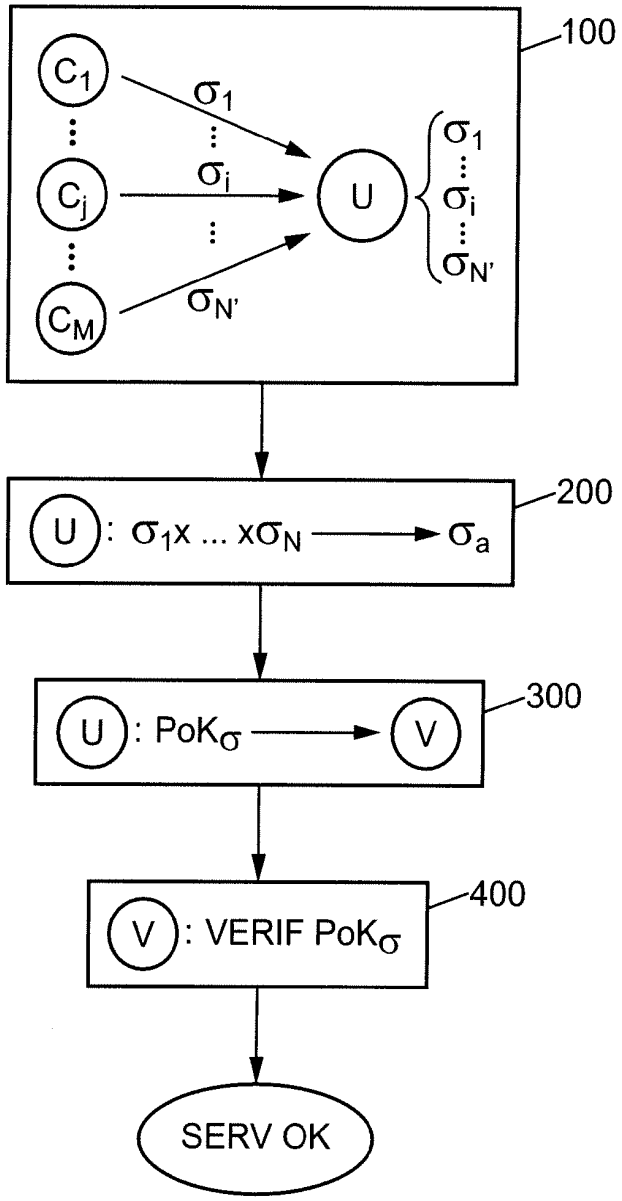

100
C1
σ1
Cj
σi
CM
σN'
U
σ1
σi
σN'
200
U : σ1x ... xσN
σa
300
U : PoKσ
V
400
V : VERIF PoKσ
SERV OK

FIG. 1

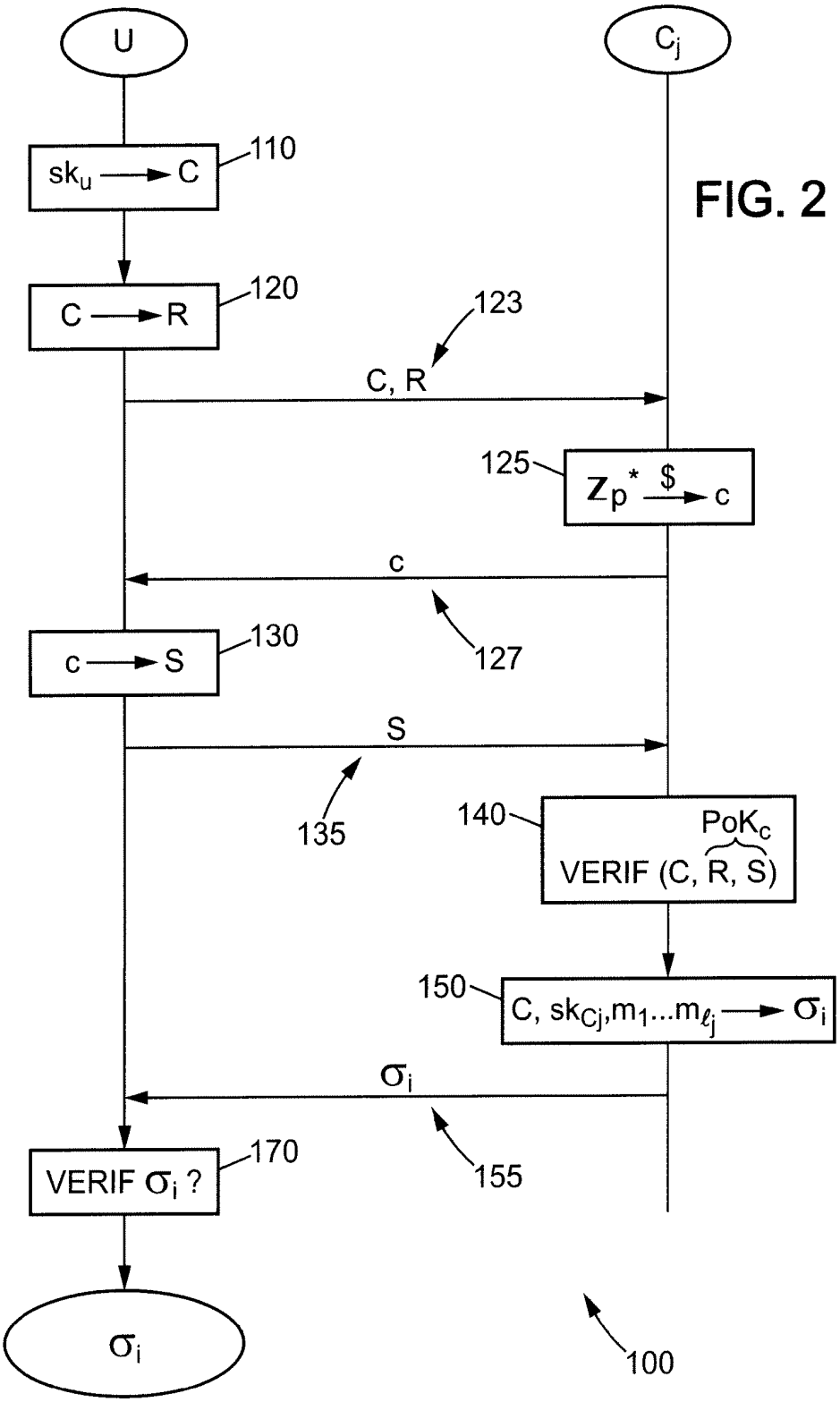

U
C_j
$sk_u \rightarrow C$
110
C → R
120
123
C, R
125
$Z_p^* \xrightarrow{\$} c$
c
127
c → S
130
S
135
140
PoK_c
VERIF (C, R, S)
150
C, sk_{Cj},m_1...m_{ℓ_j} → σ_i
σ_i
155
VERIF σ_i ?
170
σ_i
100

FIG. 2

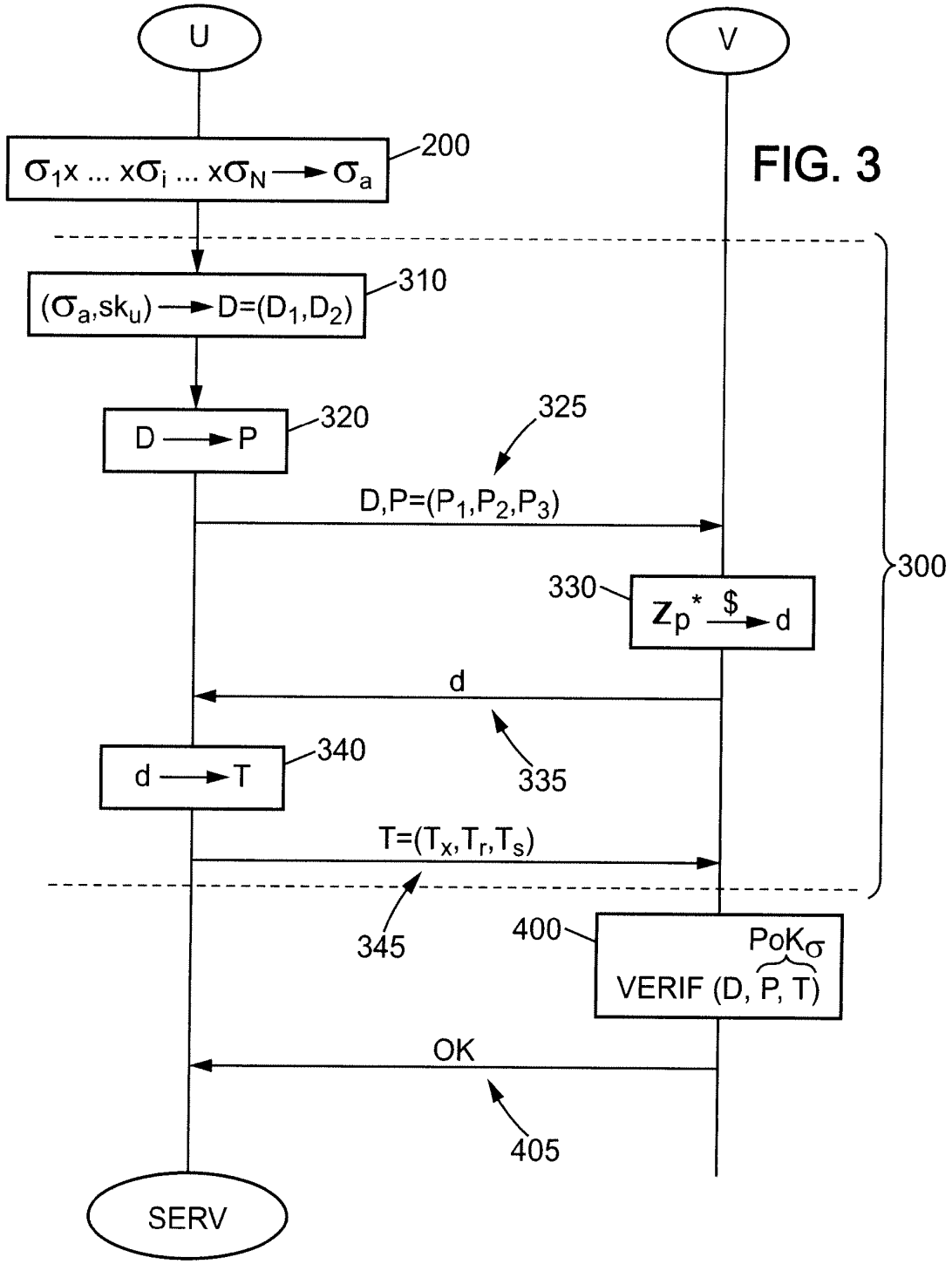

U
V
σ1x ... xσi ... xσN → σa
200
(σa,sku) → D=(D1,D2)
310
D → P
320
325
D,P=(P1,P2,P3)
300
330
Zp* $ → d
d
335
d → T
340
T=(Tx,Tr,Ts)
345
400
PoKσ
VERIF (D, P, T)
OK
405
SERV

FIG. 3

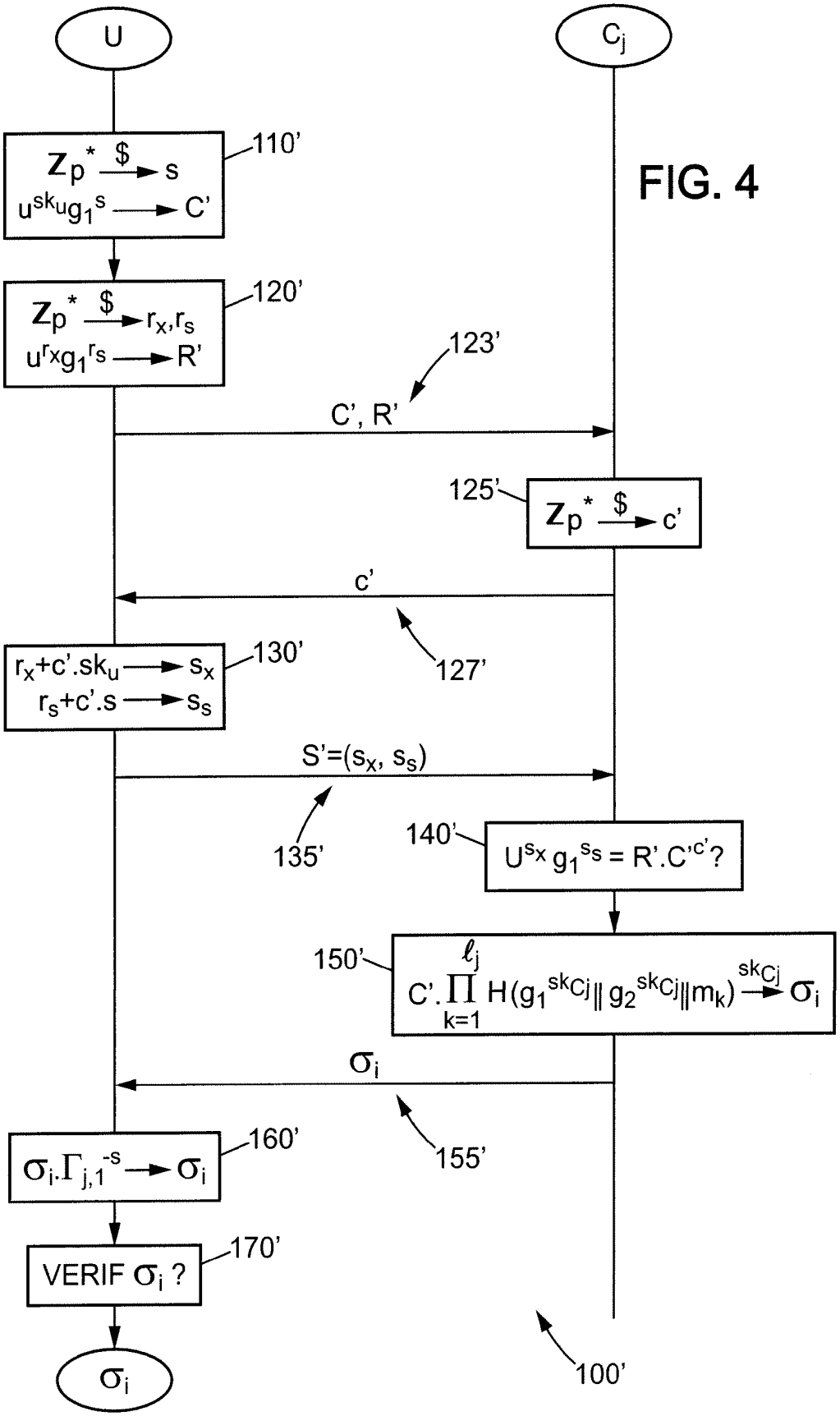

U
C_j
$Z_p^* \xrightarrow{\$} s$
$u^{sk_u} g_1^{s} \rightarrow C'$
110'
$Z_p^* \xrightarrow{\$} r_x, r_s$
$u^{r_x} g_1^{r_s} \rightarrow R'$
120'
123'
C', R'
125'
$Z_p^* \xrightarrow{\$} c'$
c'
127'
$r_x + c'.sk_u \rightarrow s_x$
$r_s + c'.s \rightarrow s_s$
130'
S'=(s_x, s_s)
135'
140'
$U^{s_x} g_1^{s_s} = R'.C'^{c'}$?
150'
$C'.\prod_{k=1}^{\ell_j} H(g_1^{sk_{Cj}} \| g_2^{sk_{Cj}} \| m_k) \xrightarrow{sk_{Cj}} \sigma_i$
σ_i
155'
$\sigma_i.\Gamma_{j,1}^{-s} \rightarrow \sigma_i$
160'
VERIF σ_i ?
170'
σ_i
100'

FIG. 4

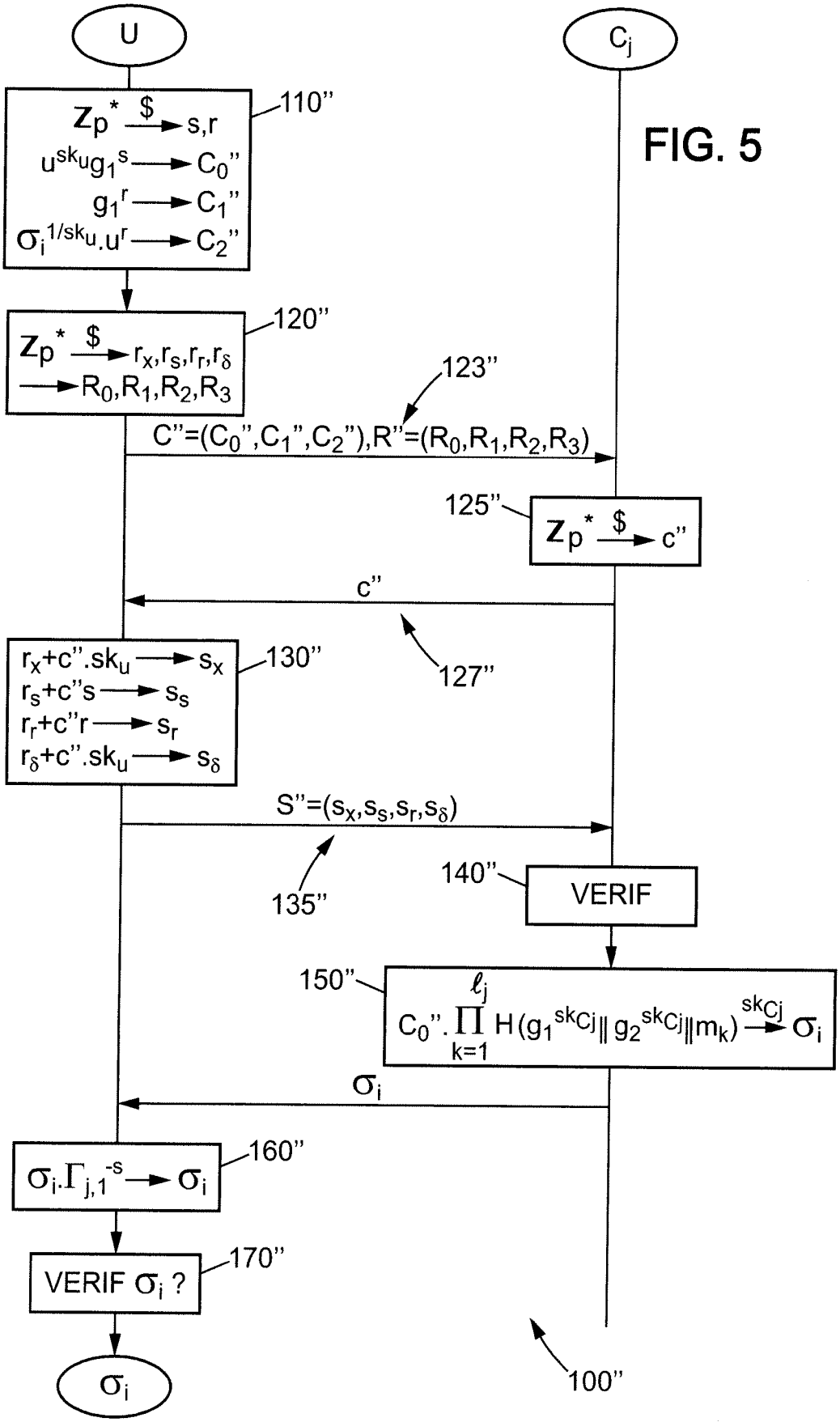

U
C_j
$Z_p^* \xrightarrow{\$} s,r$
$u^{sk_u} g_1^s \rightarrow C_0''$
$g_1^r \rightarrow C_1''$
$\sigma_i^{1/sk_u}.u^r \rightarrow C_2''$
110''
$Z_p^* \xrightarrow{\$} r_x,r_s,r_r,r_\delta$
$\rightarrow R_0,R_1,R_2,R_3$
120''
123''
$C''=(C_0'',C_1'',C_2''),R''=(R_0,R_1,R_2,R_3)$
125''
$Z_p^* \xrightarrow{\$} c''$
c''
127''
$r_x+c''.sk_u \rightarrow s_x$
$r_s+c''s \rightarrow s_s$
$r_r+c''r \rightarrow s_r$
$r_\delta+c''.sk_u \rightarrow s_\delta$
130''
$S''=(s_x,s_s,s_r,s_\delta)$
135''
140''
VERIF
150''
$C_0''.\prod_{k=1}^{\ell_j} H(g_1^{sk_{Cj}} \| g_2^{sk_{Cj}} \| m_k) \xrightarrow{sk_{Cj}} \sigma_i$
σ_i
$\sigma_i.\Gamma_{j,1}^{-s} \rightarrow \sigma_i$
160''
VERIF σ_i ?
170''
σ_i
100''

FIG. 5

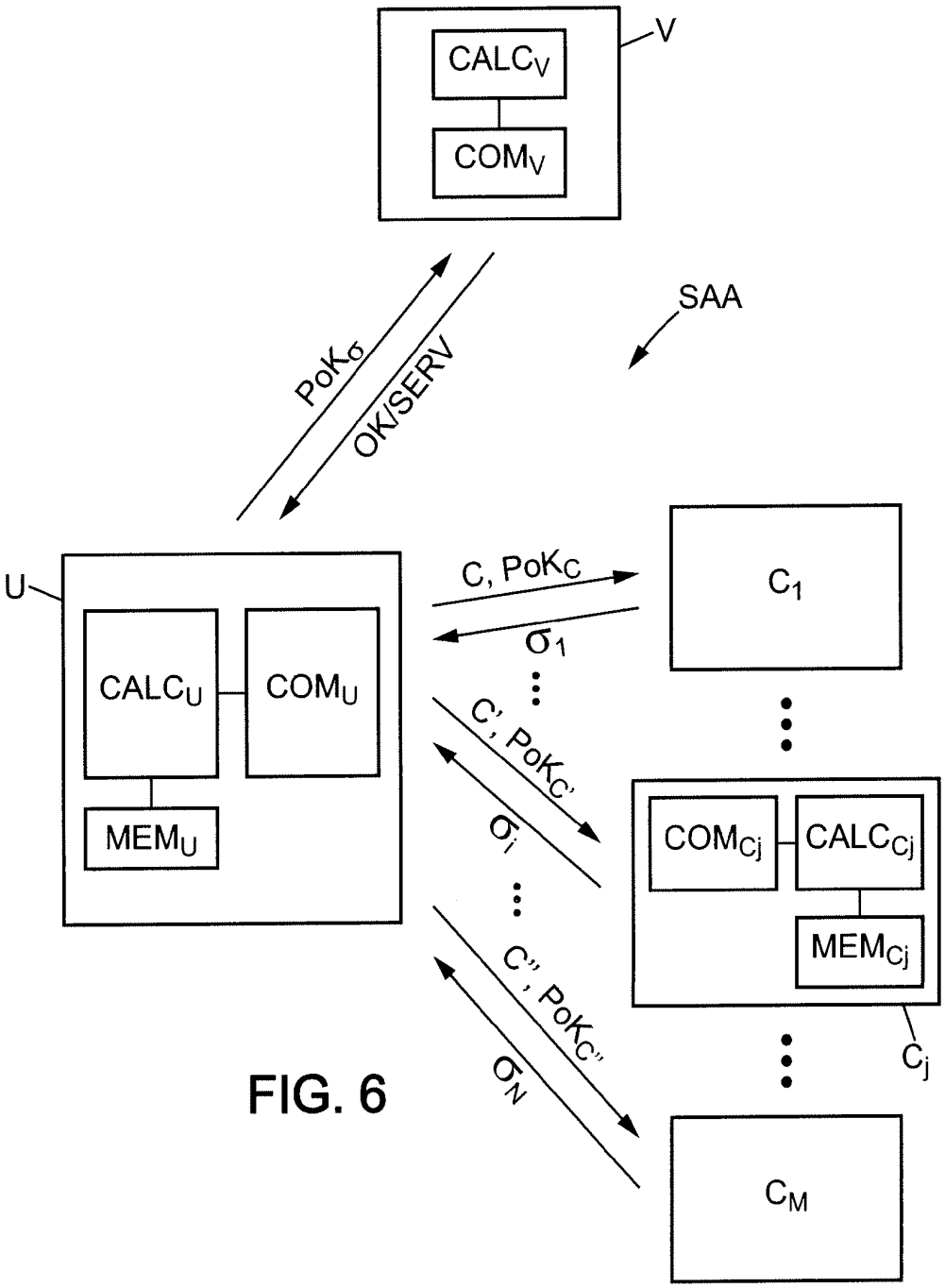

V
CALC$_V$
COM$_V$
SAA
PoK$_\sigma$
OK/SERV
U
CALC$_U$
COM$_U$
MEM$_U$
C, PoK$_C$
σ_1
C$_1$
C', PoK$_{C'}$
σ_i
COM$_{Cj}$
CALC$_{Cj}$
MEM$_{Cj}$
C$_j$
C'', PoK$_{C''}$
σ_N
C$_M$

FIG. 6

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 745689
FR 1061146

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	FEDERICA PACI ET AL: "VeryIDX - A Digital Identity Management System for Pervasive Computing Environments", 1 octobre 2008 (2008-10-01), SOFTWARE TECHNOLOGIES FOR EMBEDDED AND UBIQUITOUS SYSTEMS; [LECTURE NOTES IN COMPUTER SCIENCE], SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, PAGE(S) 268 - 279, XP019107200, ISBN: 978-3-540-87784-4	1,10-15	H04L9/32
A	* pages 271-274 *	2-9	

X	ABHILASHA BHARGAV-SPANTZEL ET AL: "Multifactor Identity Verification Using Aggregated Proof of Knowledge", IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: PART C:APPLICATIONS AND REVIEWS, IEEE SERVICE CENTER, PISCATAWAY, NJ, US, vol. 40, no. 4, 1 juillet 2010 (2010-07-01), pages 372-383, XP011307487, ISSN: 1094-6977	1,10-15	DOMAINES TECHNIQUES RECHERCHÉS (IPC)
A	* pages 375-378 *	2-9	H04L

T	CAMENISCH J ET AL: "EFFICIENT GROUP SIGNATURE SCHEMES FOR LARGE GROUPS", ADVANCES IN CRYPTOLOGY - CRYPTO '97. SANTA BARBARA, AUG. 17 - 21, 1997; [PROCEEDINGS OF THE ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE (CRYPTO)], BERLIN, SPRINGER, DE, vol. CONF. 17, 17 août 1997 (1997-08-17), pages 410-424, XP000767547, ISBN: 978-3-540-63384-6 * section 3.3 *		

	-/--		

Date d'achèvement de la recherche	Examinateur
12 août 2011	Billet, Olivier

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

2

EPO FORM 1503 12.99 (P04C14)

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 745689
FR 1061146

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	Stefan Brands: "A Technical Overview of Digital Credentials", , 20 février 2002 (2002-02-20), XP55004420, Extrait de l'Internet: URL:http://www.credentica.com/overview.pdf [extrait le 2011-08-09] * le document en entier * -----	1-15	

DOMAINES TECHNIQUES RECHERCHÉS (IPC)

Date d'achèvement de la recherche	Examinateur
12 août 2011	Billet, Olivier

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

.....

& : membre de la même famille, document correspondant

2

EPO FORM 1503 12.99 (P04C14)