



- (51) Classification internationale des brevets :
H04L 9/32 (2006.01)
- (21) Numéro de la demande internationale :
PCT/FR20 12/052780
- (22) Date de dépôt international :
3 décembre 2012 (03.12.2012)
- (25) Langue de dépôt : français
- (26) Langue de publication : français
- (30) Données relatives à la priorité :
1161 737 15 décembre 2011 (15.12.2011) FR
- (71) Déposant : **FRANCE TELECOM** [FR/FR]; 78 rue Olivier de Serres, F-75015 Paris (FR).
- (72) Inventeurs : **CANARD, Sébastien**; 15 rue Alexandre Bigot, F-14000 Caen (FR). **LESCUYER, Roch**; 6 rue François Mitterrand, F-14123 Fleury sur Orne (FR).
- (74) Mandataire : **FRANCE TELECOM/OLNC/OLPS/IPL/PAT**; 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, BN, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, RW, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, 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, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— avec rapport de recherche internationale (Art. 21(3))

(54) Title : ANONYMOUS REGISTRATIONS

(54) Titre : ACCREDITATIONS ANONYMES

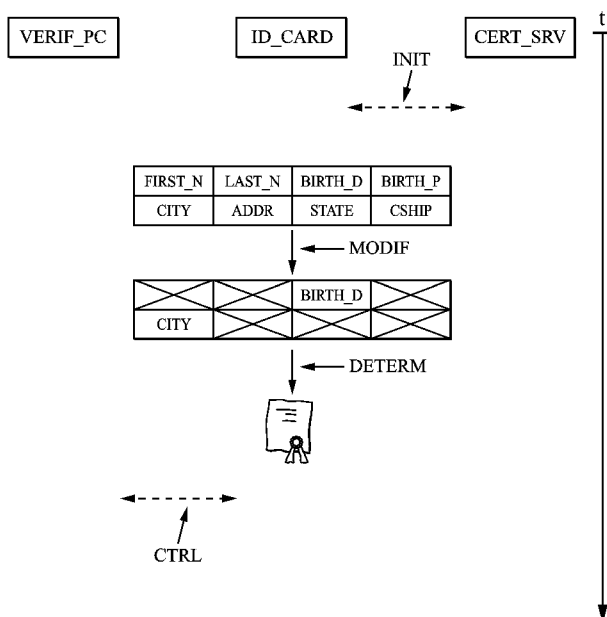


FIG. 1

(57) Abstract : The application relates in particular to a method for monitoring anonymous access to a service. An electronic user device (ID_CARD) stores a certified set of attributes (FIRST_N, LAST_N, BIRTH_D, BIRTH_P, ADDR, CITY, STATE, CSHIP) and a modification key (MOD_K). Said set is certified by an electronic certification device (CERT_SRV) by means of a sanitisable electronic signature fonction. Said fonction corresponds to a signature key (SIG_K) stored in the electronic certification device and to said modification key (MOD_K). The method includes the modification of the set of attributes by means of the electronic user device, said modification including the deletion of attributes other than the attributes (BIRTH_D, CITY) required for anonymous access to said service. The method also includes the détermination, by means of the electronic user device and the modification key, the signature of the modified set in order to make it possible to subsequently monitor, by means of an electronic verifying device (VERI_PC), the fact that the electronic signature of the modified set corresponds to a valid signature for the electronic certification device.

(57) Abrégé :

[Suite sur la page suivante]

La demande se rapporte notamment à un procédé de contrôle d'accès anonyme à un service. Un dispositif électronique utilisateur (ID_CARD) stocke un ensemble certifié d'attributs (FIRST_N, LAST_N, BIRTH_D, BIRTH_P, ADDR, CITY, STATE, CSHIP) et une clé de modification (MOD_K). Cet ensemble est certifié par un dispositif électronique certificateur (CERT_SRV) à l'aide d'une fonction de signature électronique sanitisable. Cette fonction est associée à une clé de signature (SIG_K) stockée dans le dispositif électronique certificateur ainsi qu'à ladite clé de modification (MOD_K). Le procédé comprend la modification, par le dispositif électronique utilisateur, de l'ensemble d'attributs, ladite modification comprenant l'effacement d'attributs autres que les attributs (BIRTH_D, CITY) requis pour l'accès anonyme audit service. Le procédé comprend également la détermination, par le dispositif électronique utilisateur, à l'aide de la clé de modification, de la signature de l'ensemble modifié, afin de permettre le contrôle ultérieur, par un dispositif électronique vérifieur (VERIF_PC), du fait que la signature électronique de l'ensemble modifié correspond à une signature valide du dispositif électronique certificateur.

Accréditations Anonymes

L'invention concerne le domaine des systèmes d'accréditation anonyme pour l'accès à des services.

Dans un système d'accréditation habituel, 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.

De façon similaire, un étudiant peut vouloir bénéficier d'une réduction sur un service offert par un organisme tiers. L'étudiant doit alors prouver qu'il possède une accréditation provenant (par exemple) 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. L'entité de confiance peut être notamment une mairie, ou encore une 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 connu 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 le 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, puisque l'organisation certificatrice est impliquée lors de chaque demande d'accès. Un exemple de ce type de technique est repris dans la technologie UProve proposée par Microsoft.

L'invention vise à améliorer la situation.

L'invention se rapporte notamment à un procédé de contrôle d'accès anonyme à un service, dans lequel, un dispositif électronique utilisateur stockant un ensemble certifié d'attributs et une clé de modification, ledit ensemble ayant été certifié par un dispositif électronique certificateur à l'aide d'une fonction de signature électronique sanitisable, ladite fonction étant associée à une clé de signature stockée dans ledit dispositif électronique certificateur ainsi qu'à ladite clé de modification, le procédé comprend:

/a1/ la modification, par le dispositif électronique utilisateur, de l'ensemble d'attributs, ladite modification comprenant l'effacement d'attributs autres que les attributs requis pour l'accès anonyme audit service,

/a2/ la détermination, par le dispositif électronique utilisateur, à l'aide de la clé de modification, de la signature de l'ensemble modifié, afin de permettre le contrôle ultérieur, par un dispositif électronique vérifieur, du fait que la signature électronique de l'ensemble modifié correspond à une signature valide du dispositif électronique certificateur.

Ce procédé est avantageux notamment en ce qu'il permet au dispositif électronique utilisateur de prouver au dispositif électronique vérifieur qu'il détient des attributs donnant accès à un service donné, sans pour autant avoir besoin de divulguer au dispositif électronique vérifieur des attributs autres (susceptibles de porter atteinte à la vie privée).

L'invention se rapporte également, notamment, à un dispositif électronique utilisateur agencé pour stocker une clé de modification ainsi qu'un ensemble certifié d'attributs, l'ensemble d'attributs stocké étant certifié par un dispositif électronique certificateur à l'aide d'une fonction de signature électronique sanitisable, ladite fonction étant associée à une clé de signature stockée dans ledit dispositif électronique certificateur ainsi qu'à ladite clé de modification, le dispositif électronique utilisateur étant agencé pour modifier l'ensemble d'attributs en effaçant des attributs autres que les attributs requis pour l'accès anonyme audit service, et pour déterminer, à l'aide de la clé de modification, la signature de l'ensemble d'attributs modifié, afin de permettre le contrôle ultérieur, par un dispositif électronique vérifieur, du fait que la signature électronique de l'ensemble modifié correspond à une signature valide du dispositif électronique certificateur.

Ce dispositif est avantageux notamment en ce qu'il est agencé pour prouver au dispositif électronique vérifieur qu'il détient des attributs donnant accès à un service donné, sans pour autant avoir besoin de divulguer au dispositif électronique vérifieur des attributs autres (susceptibles de porter atteinte à la vie privée).

L'invention se rapporte également, notamment, à un système de contrôle d'accès anonyme à un service, comprenant un dispositif électronique utilisateur selon un mode de réalisation de l'invention, et au moins l'un des deux dispositifs suivants:

- un dispositif électronique certificateur agencé pour certifier un ensemble d'attributs à l'aide d'une fonction de signature électronique sanitisable, ladite fonction étant associée à une clé de signature stockée dans le dispositif électronique certificateur ainsi qu'à une clé de modification, de manière à permettre au dispositif électronique utilisateur, lorsqu'il a préalablement stocké l'ensemble d'attributs certifié ainsi que la clé de modification, de modifier l'ensemble d'attributs en effaçant des attributs autres que les attributs requis pour l'accès anonyme audit service, et de déterminer, à l'aide de la clé de modification, la signature de l'ensemble modifié,
- un dispositif électronique vérifieur agencé pour recevoir du dispositif électronique utilisateur un ensemble certifié d'attributs, et pour contrôler que la signature électronique de l'ensemble reçu correspond à une signature valide d'un dispositif électronique certificateur.

L'invention se rapporte également, notamment, à un programme d'ordinateur agencé pour mettre en œuvre un procédé selon un mode de réalisation de l'invention lorsqu'il est exécuté par un processeur.

L'invention se rapporte également, notamment, à un support de stockage non transitoire lisible par ordinateur, stockant un programme d'ordinateur selon un mode de réalisation de l'invention.

D'autres aspects, buts et avantages de l'invention apparaîtront à la lecture de la description d'un de ses modes de réalisation.

L'invention sera également mieux comprise à l'aide des dessins, sur lesquels:

- la figure 1 illustre un procédé selon un mode de réalisation ;

- la figure 2 illustre l'architecture d'un dispositif électronique utilisateur selon un mode de réalisation ;

- la figure 3 illustre un système selon un mode de réalisation ;

La figure 1 illustre un procédé selon lequel, l'axe du temps t étant orienté du haut vers le bas, après une première étape d'initialisation INIT (indiquée en pointillés car elle ne fait en l'occurrence pas partie du procédé), le procédé modifie (lors d'une étape MODIF) un ensemble d'attributs FIRST_N, LAST_N, BIRTH_D, BIRTH_P, ADDR, CITY, STATE, CSHIP en effaçant les attributs FIRST_N, LAST_N, BIRTH_P, ADDR, STATE, CSHIP et en ne conservant que les attributs BIRTH_D, CITY. Le procédé détermine alors (durant une étape DETERM) une nouvelle signature de l'ensemble d'attributs dont on a effacé les attributs précités. Une première signature avait été préalablement calculée durant l'étape INIT, pendant laquelle un dispositif électronique certificateur CERT_SRV avait certifié les attributs pour le compte du dispositif électronique utilisateur ID_CARD. Le procédé peut être suivi d'une étape (indiquée en pointillés car elle ne fait en l'occurrence pas partie du procédé) de contrôle CTRL de la validité de la signature des attributs modifiés par un dispositif électronique vérifieur VERIF_PC.

La figure 2 illustre de façon symbolique l'architecture d'un dispositif électronique utilisateur selon un mode de réalisation de l'invention (en l'occurrence une carte à puce ID_CARD). Cette carte comporte un microcontrôleur, sous forme d'un seul composant (bien que les différents éléments soient représentés schématiquement comme s'ils étaient discrets). Le microcontrôleur intègre un processeur PROC, une mémoire vive RAM, et une mémoire morte ROM (pouvant mémoriser un système d'exploitation ainsi qu'un programme d'ordinateur adapté pour mettre en œuvre un procédé selon un mode de réalisation de l'invention lorsqu'il est exécuté par le processeur PROC). Le microcontrôleur intègre également une mémoire programmable EEPROM (il pourrait évidemment s'agir d'une autre technologie, telle que la mémoire Flash), mémorisant différentes informations, dont une clé de modification MOD_K et huit attributs FIRST_N, LAST_N, BIRTH_D, BIRTH_P, ADDR, CITY, STATE, CSHIP.

La figure 3 illustre un système selon un mode de réalisation possible de l'invention, comprenant un dispositif électronique de certification (en l'occurrence un serveur CERT_SRV), un dispositif électronique utilisateur (en l'occurrence une carte à puce ID_CARD), et un dispositif électronique vérifieur (en l'occurrence un ordinateur personnel VERIF_PC). Le serveur comprend un TPM (Trusted Platform Module), qui est un composant sécurisé, stockant une clé privée de signature SIG_K. L'ordinateur VERIF_PC est connecté à un lecteur NFC lui permettant de communiquer avec la carte ID_CARD. L'ordinateur est également connecté à une porte dont il est en mesure de commander l'ouverture en fonction de ses communications avec la carte ID_CARD.

Un mode de réalisation de l'invention se rapporte à un procédé de contrôle d'accès anonyme à un service. Le service peut être un service de toute nature. Il peut s'agir par exemple d'un service consistant à commander l'ouverture d'un tourniquet, d'un sas, ou encore d'une porte, en commandant l'arrêt de l'alimentation électrique d'un électro-aimant retenant une porte en position fermée (ou encore commandant la rotation d'un moteur électrique contrôlant le désengagement d'un pêne de la gâche d'une serrure), donnant ainsi accès à un espace particulier dont l'accès est restreint. Le service peut plus simplement consister à commander l'allumage d'un indicateur particulier (par exemple une ampoule verte ou une ampoule rouge selon que l'accès est ou non autorisé, ou même l'affichage d'un message explicite sous forme de texte sur un écran d'ordinateur), permettant à un contrôleur humain de décider de laisser ou de ne pas laisser passer un autre humain, détenteur d'un dispositif électronique utilisateur.

Un dispositif électronique utilisateur ID_CARD (tel qu'une carte d'identité électronique, une carte d'étudiant électronique, ou encore un téléphone portable NFC) stocke (par exemple lors d'une étape d'initialisation préalable audit procédé, ou encore durant ledit procédé) un ensemble certifié d'attributs.

Le fait que les attributs sont certifiés signifie qu'ils sont associés à une (ou plusieurs) signature(s) d'une (ou plusieurs) autorité(s). Cette (ou ces) signature est stockée avec les attributs, afin de pouvoir vérifier que ces attributs sont effectivement correctement certifiés. L'autorité peut être par exemple une mairie, habilitée à certifier lesdits attributs.

Les attributs peuvent comprendre, à titre d'exemple non limitatif, un prénom FIRST_N, un nom de famille LAST_N, une date de naissance BIRTH_D, un lieu de naissance BIRTH_P, une adresse postale ADDR, une ville de résidence CITY, un Etat de résidence STATE, et/ou encore une nationalité/citoyenneté CSHIP.

Ledit ensemble est certifié (par exemple lors d'une étape d'initialisation préalable au procédé, ou encore pendant ledit procédé) par un dispositif électronique certificateur CERT_SRV. Ce dispositif électronique certificateur est typiquement un serveur (mais peut également être tout type d'ordinateur ou de matériel électronique dédié approprié). Il peut comprendre des éléments de sécurité (tels qu'un HSM - hardware security module - pour la gestion de clés). Le dispositif électronique certificateur peut être opéré par exemple par la dite autorité ou encore sous son contrôle (il est possible que le dispositif électronique certificateur soit par exemple opéré par un prestataire de service spécialisé pour le compte d'une mairie).

L'ensemble est certifié à l'aide d'une fonction de signature électronique sanitisable. Une fonction de signature électronique est une fonction mise en œuvre par un dispositif électronique, prenant en entrée un message (pouvant être représenté par une suite de bits) et produisant, à l'aide du message et d'une clé privée de signature, une signature de ce message (signature pouvant elle-même être représentée par une suite de bit). La signature est liée au message et au détenteur de la clé privée de signature (changer le message change la signature, et une clé de signature différente produit une signature différente). La signature peut également faire intervenir des paramètres additionnels (tels qu'un aléa pouvant être concaténé au message, permettant ainsi de produire deux signatures différentes lors de deux signatures

d'un même message avec la même clé privée de signature). Il est mathématiquement très difficile (en pratique impossible) de déterminer la signature sans la clé privée de signature. Une fonction de signature électronique sanitisable est une variante d'une fonction de signature électronique conventionnelle, selon laquelle on peut modifier a posteriori un couple message/signature de manière prédéfinie et contrôlée par l'entité détentrice de la clé privée de signature (c'est-à-dire l'entité habilitée à signer, à savoir dans le cas général l'autorité précitée ou son prestataire), mais sans interaction avec cette entité. Cette possibilité de modification constitue la seule exception au principe selon lequel il est mathématiquement très difficile (en pratique impossible) de déterminer la signature d'un message sans connaître la clé privée de signature. Plus précisément, le message est modifié, et la signature du message modifié est recalculée en fonction notamment de la modification apportée au message et de la précédente signature. La signature est modifiée (c'est-à-dire recalculée) de sorte à ce qu'une fois modifiée, elle constitue une signature valide du nouveau message (le message modifié). La « sanitisation » peut être publique (tout le monde pouvant alors modifier le couple message/signature a posteriori, dans la limite des modifications autorisées) ou ne se faire que par un (ou un groupe de) « sanitiseur(s) » désigné. Dans le contexte de ce mode de réalisation, le message n'est modifiable que dans les limites définies comme étant admissibles par l'entité détentrice de la clé de signature. Ces limites peuvent comprendre non seulement les modifications possibles (typiquement l'autorisation d'effacer un attribut mais pas celle de le remplacer par un attribut valide différent), mais également les entités habilitées à apporter ces modifications. Le contrôle de l'admissibilité d'une modification de message est opéré à l'aide d'une clé de modification générée par exemple sous le contrôle de l'autorité (mais pas nécessairement détenue par elle). Autrement dit, seul un détenteur de la clé de modification peut apporter des modifications et recalculer une signature légitime. Les signatures sanitisables donnent ainsi les moyens à un signataire de déléguer à une autre entité le pouvoir de modifier un message signé, de telle sorte que le message modifié est toujours considéré comme ayant été signé par le signataire initial (puisqu'il est associé à une signature valide recalculée). Des constructions possibles de fonctions de signature sanitisable peuvent utiliser un schéma de signature standard avec utilisation d'une fonction de hachage. Pour obtenir la propriété de sanitisation, une étape préliminaire à l'utilisation de la fonction de hachage peut consister à diviser le message à signer en plusieurs parties (pouvant chacune correspondre à un attribut), selon ce qui est modifiable ou non par le dispositif électronique utilisateur, puis à utiliser une fonction de hachage caméléon sur les parties modifiables. Une fonction de hachage cryptographique standard peut ensuite être appliquée au résultat ainsi obtenu, puis une fonction de signature électronique conventionnelle peut être utilisée. La clé de modification (ou « trappe de sanitisation ») utilisée par le dispositif électronique utilisateur peut alors correspondre à la trappe de la fonction de hachage caméléon. De telles fonctions de hachage sont décrites notamment dans l'article « Chameleon Hashing and Signatures » de Hugo Krawczyk et Tal Rabin (octobre 1997), dont le contenu est incorporé par référence. Une fonction de hachage est habituellement dénuée de collisions prévisibles, c'est-à-dire qu'il n'est pas possible en pratique de trouver deux messages différents sur lesquels l'application d'une fonction de hachage donne le même résultat. Une fonction de hachage caméléon permet, à l'aide d'une trappe (une clé secrète appropriée) de construire de telles

collisions. Pour cela, la sortie de la fonction de hachage est associée à une valeur dite 'aléatoire' qui va varier en fonction du message haché (et pour une collision donnée).

Le dispositif électronique utilisateur stocke également une clé de modification afin de pouvoir recalculer la signature du message une fois le message modifié. Le dispositif électronique utilisateur peut être la seule entité détentrice de cette clé de modification.

Ladite fonction de signature électronique sanitisable est associée à une clé de signature stockée dans ledit dispositif électronique certificateur (si elle n'est stockée nulle part ailleurs, la non-répudiation de la signature peut s'en trouver améliorée).

Ladite fonction est également associée à ladite clé de modification (précitée). Cette clé peut n'être stockée que dans le dispositif électronique utilisateur.

Le procédé comprend:

/a1/ la modification, par le dispositif électronique utilisateur, de l'ensemble d'attributs, ladite modification comprenant l'effacement d'attributs autres que les attributs (par exemple des attributs de date de naissance BIRTH_D et de ville de résidence CITY) requis pour l'accès anonyme audit service,

/a2/ la détermination, par le dispositif électronique utilisateur, à l'aide de la clé de modification, de la signature de l'ensemble modifié, afin de permettre le contrôle ultérieur (soit dans le cadre du procédé selon le présent mode de réalisation, soit dans le cadre d'un autre procédé), par un dispositif électronique vérifieur VERIF_PC, du fait que la signature électronique de l'ensemble modifié correspond à une signature valide du dispositif électronique certificateur.

Un étudiant peut ainsi prouver, en entrant dans un cinéma, qu'il a plus de seize ans (le film qu'il souhaite voir étant interdit aux moins de seize ans) à l'aide d'un dispositif électronique utilisateur tel que sa carte (à puce) d'étudiant, et qu'il habite la ville du cinéma considéré (ce qui le cas échéant lui donne droit à une réduction) sans pour autant divulguer son adresse précise, ses noms et prénoms, ni aucune autre information personnelle non requise pour voir le film et bénéficier d'un tarif préférentiel.

Selon un mode de réalisation possible, la détermination de la signature de l'ensemble modifié par le dispositif électronique utilisateur, à l'aide de la clé de modification, est effectuée sans qu'il ne soit nécessaire que le dispositif électronique utilisateur communique avec le dispositif électronique certificateur (il peut le cas échéant exister des communications entre ces dispositifs, mais elles n'ont besoin de révéler aucune information sur les attributs stockés dans le dispositif utilisateur). De même, selon un mode de réalisation, le contrôle ultérieur par le dispositif électronique vérifieur du fait que la signature électronique de l'ensemble modifié correspond à une signature valide du dispositif électronique certificateur ne nécessite pas que le dispositif électronique vérifieur communique avec le dispositif électronique certificateur. Ainsi, le dispositif électronique certificateur, même s'il est amené à communiquer avec le dispositif électronique vérifieur, n'acquiert aucune information sur les attributs. Par exemple, la mairie n'est pas informée (et ne peut déduire des informations collectées) que telle ou telle personne est allée au cinéma à telle ou telle date et à telle ou telle heure. Selon un mode de réalisation possible, le procédé empêche la mairie de récupérer (par exemple via son dispositif électronique certificateur) des informations susceptibles d'identifier l'utilisateur, non seulement par l'absence de

communication entre le dispositif électronique certificateur et d'une part le dispositif électronique utilisateur, d'autre part le dispositif électronique vérifieur, mais également par le protocole mis en œuvre par le procédé. Ce protocole peut empêcher le dispositif électronique certificateur d'établir un lien entre une demande d'autorisation d'accès par un dispositif électronique utilisateur (et/ou le traitement de cette
5 demande d'accès par un dispositif électronique vérifieur) et des informations identifiant un dispositif électronique utilisateur particulier. Selon une variante possible, le dispositif électronique certificateur peut être amené à intervenir lors de la requête d'accès par le dispositif électronique utilisateur et de son traitement par le dispositif électronique vérifieur. Le protocole mis en œuvre peut alors empêcher le dispositif électronique certificateur de déduire, à partir des informations auxquelles il est amené à
10 accéder, des informations d'identification de l'utilisateur. En particulier, selon un mode de réalisation, le procédé met en œuvre un protocole empêchant d'établir un lien entre la signature émise par le dispositif électronique certificateur et celle qui est déterminée par le dispositif électronique utilisateur à partir de cette précédente signature.

Ce procédé est avantageux en ce qu'il permet de préserver l'anonymat (en ne divulguant pas tous
15 les attributs mais seulement ceux qui sont nécessaires), tout en préservant l'authentification (le dispositif électronique utilisateur prouve qu'il détient bien les attributs critiques pour l'accès au service). Ce procédé est également avantageux en ce qu'il permet d'empêcher le dispositif électronique utilisateur de modifier les attributs protégés autrement qu'en les effaçant (ainsi, il ne peut pas, par exemple, remplacer un nom de famille par un autre), et en ce que le dispositif électronique utilisateur ne peut effacer que les
20 attributs autorisés (il peut lui être interdit d'effacer certains attributs). Le procédé permet également d'empêcher un dispositif électronique utilisateur de partager ses attributs avec d'autres. A cette fin, il peut être prévu que la clé de modification ne puisse pas être extraite du dispositif électronique utilisateur. Par exemple, dans le cas où ledit dispositif est une carte à puce conforme au standard ISO 7816-4, la clé de modification peut être stockée dans un fichier tel qu'un fichier de type EF (elementary file au sens de la
25 norme ISO précitée). Ce fichier EF peut être protégé en lecture, mais accessible à l'OS (système d'exploitation) de la carte à puce (ou à une application telle qu'un softmask ou une applet javacard). Ainsi, la clé de modification peut être utilisée par le dispositif électronique utilisateur lui-même (à l'aide par exemple des fonctions prédéfinies qu'il embarque dans son système d'exploitation sécurisé), mais pas extrait (une commande de type READ_BINARY définie par l'ISO renvoyant un code d'erreur puisque
30 l'accès en lecture est interdit). A l'aide de dispositions de ce type, un dispositif électronique utilisateur ne peut donc pas être frauduleusement combiné avec d'autres, afin de reconstituer une fausse identité (par exemple en combinant l'attribut FIRST_N d'un premier dispositif avec l'attribut LAST_N d'un deuxième dispositif et l'attribut BIRTH_D d'un troisième dispositif).

Le procédé peut être mis en œuvre à l'aide d'une suite d'instructions constituant un programme
35 d'ordinateur exécuté par un processeur du dispositif électronique utilisateur. Mais il peut également être mis en œuvre à l'aide d'un circuit électronique dédié intégré au dispositif électronique utilisateur, tel qu'un ASIC, un FPGA (ou les variantes PAL, EPLD, PLD, CPLD, PLA, etc.) convenablement configuré (par exemple en VHDL), voire de l'électronique dédiée conçue sur mesure.

Selon un mode de réalisation, un procédé de contrôle d'accès est mis en œuvre de façon à ce que la détermination de la signature de l'ensemble modifié soit opérée sans que le dispositif électronique utilisateur ne communique avec le dispositif électronique certificateur, afin de permettre le contrôle ultérieur, par le dispositif électronique vérifieur, sans que le dispositif électronique vérifieur ne communique avec le dispositif électronique certificateur, du fait que la signature électronique de l'ensemble modifié correspond à une signature valide du dispositif électronique certificateur.

On évite ainsi toute communication avec le dispositif électronique certificateur lors de la tentative d'accès au service, ce qui élimine de facto tout risque de récupération d'informations par le dispositif électronique certificateur durant cette tentative d'accès.

Selon un mode de réalisation, l'effacement d'attributs mis en œuvre par le procédé de contrôle d'accès comprend le retrait des attributs à effacer de l'ensemble d'attributs.

Ainsi, on peut par exemple recalculer que signature des seuls attributs date de naissance BIRTH_D et ville de résidence CITY, à l'exclusion des autres attributs. Si ces deux attributs occupent 20 octets chacun, on recalcule ainsi la signature d'un message de 40 octets seulement (à l'exclusion des octets alloués aux autres attributs).

Selon un mode de réalisation, l'effacement d'attributs mis en œuvre par le procédé de contrôle d'accès comprend le remplacement des attributs à effacer par des informations anonymes.

Par exemple, le procédé peut remplacer les attributs à effacer par des caractères distingués (sans corrélation avec l'attribut à remplacer). Ainsi, l'attribut de nom de famille LAST_N, qui peut par exemple contenir la chaîne de caractères « DUCHESNES », peut-il être remplacé par l'une des chaînes « XXXXXXXXX », « » (chaîne constituée de caractères d'espacement), « _____ », « ##### », ou encore « ??????? », qui ne sont évidemment indiquées qu'à titre purement indicatif et non limitatif. Les attributs de remplacement peuvent avoir la même taille que les attributs d'origine (en nombre de bits). Dans cette hypothèse, les attributs peuvent avoir une taille prédéfinie indépendamment de leur contenu. Par exemple un attribut de nom de famille peut faire 35 caractères, indépendamment du nom de famille enregistré dans cet attribut (les noms sont alors supposés de longueur égale ou inférieure à 35 caractères, dans le cas contraire ils peuvent être tronqués à 35 caractères, ou à toute autre taille jugée opportune pour l'attribut considéré). Le nom de famille peut alors être enregistré indifféremment au début, au milieu, à la fin, ou en toute position du champ de 35 caractères réservés pour le nom de famille, les caractères non utilisés du champ pouvant être définis de façon conventionnelle (par exemple il peut s'agir de caractères d'espacement, tels que le caractère de code ASCII 32, soit 0x20).

Alternativement, il est possible de transformer le contenu d'un attribut (par exemple une chaîne de caractères ASCII) en une série de bits (ne possédant pas nécessairement de représentation visuelle selon un jeu de caractères standard, tel que l'ASCII), la valeur des bits de la série de bits étant calculée afin de ne pas modifier le résultat d'une fonction de hachage caméléon appliquée à l'ensemble d'attributs.

Selon un mode de réalisation, la fonction de signature électronique sanitisable du procédé de contrôle d'accès est une fonction de signature caviardable, ou une fonction de signature électronique couplée à une fonction de hachage caméléon, ou encore une fonction de signature électronique couplée à une fonction de noircissage.

Les fonctions de signature caviardable sont des fonctions de signature électronique permettant de cacher certaines parties d'un message signé tout en gardant la signature valide. Elles peuvent s'appuyer sur la construction de certificats (sortes de cartes d'identité numérique) ayant des propriétés de caviardage (terme typographique désignant le fait d'ôter certaines parties d'un texte). Ainsi, par exemple, un étudiant peut cacher certains attributs de sa carte d'identité numérique sans la rendre inutilisable. Les fonctions de signature caviardable peuvent être une version simple des signatures sanitisables. Les fonctions de signature caviardable peuvent s'appuyer notamment sur un schéma de signature caméléon. Les fonctions de signature caviardable mises en œuvre dans le procédé peuvent noircir les attributs à cacher (tous les attributs sauf les attributs requis pour l'accès au service) en les remplaçant par des caractères distingués, mais elles peuvent également être des fonctions de signature dite supprimable (de l'anglais deletable), où l'on supprime (retire) les attributs à cacher, sans les remplacer par quoi que ce soit (même des caractères distingués). Elles permettent seulement à une entité possédant la bonne trappe, de noircir ou supprimer certaines parties bien définies d'un message, de telle sorte qu'il ne soit en pratique pas possible de déterminer ces parties à partir des parties noircies (ou supprimées - il est clair que l'on ne peut pas déterminer une information à partir de rien). Noircir une information sensible signifie remplacer cette information (telle qu'un attribut que l'on n'est pas tenu de divulguer), par des informations non corrélées, ne divulguant aucune information sensible (par exemple des caractères distingués, tels que la chaîne de caractères « ##### »).

En faisant signer un ensemble d'attributs par un dispositif électronique certificateur à l'aide d'une signature caviardable (éventuellement supprimable), et en donnant la trappe (la clé de modification) au dispositif électronique utilisateur, le dispositif électronique utilisateur est donc en mesure de noircir (ou de supprimer, suivant la technique utilisée) les attributs qu'il ne souhaite pas révéler, puis de modifier la signature de telle sorte qu'elle semble avoir été produite par le dispositif électronique certificateur. Le dispositif électronique utilisateur est ainsi, lors d'une demande d'accès à un service, anonyme vis-à-vis de l'extérieur (que ce soit vis-à-vis du dispositif électronique vérifieur, du dispositif électronique certificateur, ou de toute autre entité) et ne révèle au dispositif électronique vérifieur que les attributs demandés. Par ailleurs, dispositif électronique utilisateur n'est pas en mesure de modifier les attributs initialement signés par le dispositif électronique certificateur autrement qu'en les supprimant ou en les remplaçant par des informations « neutres » (ne correspondant à aucun attribut légitime du même type, tel que le nom d'une autre ville pour un attribut indiquant une ville) et ne peut donc pas tricher en se faisant passer pour un dispositif électronique utilisateur détenant des attributs différents.

Selon un mode de réalisation, les attributs (par exemple les attributs BIRTH_D et CITY) requis pour l'accès anonyme au service dépendent dudit service, et le procédé comprend une détermination desdits attributs requis en fonction dudit service. Par exemple, le même dispositif électronique utilisateur peut permettre à son détenteur humain d'accéder à un cinéma mais également d'accéder à une piscine municipale. L'accès au cinéma avec un tarif réduit peut être subordonné à la présentation d'un attribut CITY autorisé. L'accès au cinéma pour voir des films réservés aux plus de 16 ans peut être subordonné à l'attribut BIRTH_D. Ces deux attributs peuvent donc constituer l'ensemble des attributs potentiellement modifiables. Selon un mode de réalisation, pour un accès à un cinéma, le dispositif électronique peut déterminer que seuls les attributs CITY et BIRTH_D sont susceptibles d'être requis. Le dispositif électronique utilisateur peut automatiquement effacer tous les attributs autres. Il peut alternativement laisser à l'utilisateur humain du dispositif électronique utilisateur l'opportunité d'effacer les attributs de son choix (les attributs peuvent correspondre à des attributs de l'utilisateur humain lui-même). Il peut être interdit à l'utilisateur humain d'effacer certains attributs, par exemple l'attribut BIRTH_D. Dans ce cas, la non-présentation (par effacement) de l'attribut CITY entraîne par exemple simplement l'absence de réduction, mais il n'est pas possible de ne pas présenter son âge (ceci n'est évidemment qu'un exemple, il serait possible que l'âge soit également effaçable). Selon un mode de réalisation, pour un accès à une piscine, les attributs peuvent être différents de ceux requis pour un accès au cinéma. Il peut par exemple y avoir un attribut indiquant la date du dernier certificat médical d'aptitude à la natation dûment présenté à une autorité habilitée, et il peut être prévu que seul un détenteur authentifié d'un attribut indiquant une date de moins d'un an a le droit d'entrer dans la piscine.

L'entité qui accède au service à l'aide du dispositif électronique utilisateur (par exemple une carte d'identité électronique) peut être un utilisateur humain du dispositif électronique utilisateur. Par exemple en entrant dans un cinéma, un utilisateur humain peut présenter sa carte d'identité à un lecteur NFC pour valider qu'il a le droit de voir un film en fonction des attributs de la carte d'identité. Cependant, le service peut également être fourni au dispositif électronique utilisateur. L'utilisateur humain peut alors accéder au service par l'intermédiaire du dispositif électronique. Par exemple, le dispositif électronique utilisateur peut être un téléphone portable, et le service peut être un service de vidéo à la demande, dans ce cas la vidéo est envoyée au téléphone portable (le service est donc fourni au dispositif électronique utilisateur), et l'utilisateur humain peut visualiser la vidéo sur son téléphone portable.

Pour certains services, l'utilisateur humain peut être amené à laisser son dispositif électronique utilisateur (carte d'identité, carte d'étudiant, etc.) à l'entrée, et à ne le récupérer qu'à la sortie (club de tir, bibliothèque réservée aux chercheurs et donnant accès à des ouvrages d'une valeur inestimable, visite d'un site classé confidentiel défense, etc.). Le dispositif électronique utilisateur pouvant également être un téléphone portable stockant les données personnelles requises pour l'accès (les attributs), l'accès peut être autorisé par le téléphone portable mais son utilisateur humain peut être obligé de laisser le téléphone portable à l'entrée ou de l'éteindre. Ce type de situations est également envisageable pour des dispositifs électroniques utilisateurs autres que des téléphones portables.

Le dispositif électronique utilisateur peut contenir des informations personnelles imprimées (par exemple dans le cas d'une carte d'identité). Le dispositif électronique utilisateur peut contenir des informations imprimées se rapportant à des caractéristiques différentes des caractéristiques faisant l'objet des attributs stockés. Par exemple, la photo, les initiales, et le département dans lequel travaille un étudiant chercheur peuvent être imprimés sur sa carte d'étudiant, mais son nom complet, son adresse personnelle et sa date de naissance peuvent n'être disponibles que sous forme d'attributs enregistrés dans la puce de sa carte d'étudiant. Ceci est avantageux notamment dans le cas où le dispositif électronique utilisateur doit être laissé à l'entrée. Alternativement, le dispositif électronique utilisateur peut comprendre les mêmes informations sous forme d'attributs stockés et de données imprimées, mais peut être remis dans une consigne fermée en échange de la clé unique d'un cadenas de la consigne, ou encore, dans le cas d'une carte, être avalé par un lecteur de carte (à la manière d'un distributeur de billet), stocké à l'intérieur, et restitué sur présentation d'un identifiant et d'un code PIN de la carte (sans que personne d'autre que le titulaire n'ait l'opportunité de voir ce qui est imprimé sur la carte), après délivrance du service à l'utilisateur humain.

Selon un mode de réalisation, le procédé de contrôle d'accès comprend la certification, par le dispositif électronique certificateur, de l'ensemble d'attributs à l'aide de la fonction de signature électronique sanitisable.

Selon un mode de réalisation, le procédé de contrôle d'accès comprend le contrôle, par le dispositif électronique vérifieur, du fait que la signature électronique de l'ensemble modifié correspond à une signature valide du dispositif électronique certificateur.

Selon un mode de réalisation, un dispositif électronique utilisateur ID_CARD est agencé pour stocker une clé de modification MOD_K ainsi qu'un ensemble certifié d'attributs FIRST_N, LAST_N, BIRTH_D, BIRTH_P, ADDR, CITY, STATE, CSHIP.

Le dispositif électronique utilisateur peut être une carte à puce, ce qui est avantageux pour la sécurité. Il peut s'agir d'une carte à puce quelconque, notamment d'une carte à contact (par exemple au standard ISO 7816-2), d'une carte sans contact (par exemple une carte au standard MiFare, au standard ISO 14443, ou encore comprenant une interface NFC quelconque), d'une carte mixte à contact et sans contact avec une puce commune aux deux interfaces ou bien avec une puce distincte pour chaque interface contact et sans contact, etc. La carte peut être au format ID-1 de l'ISO-7810, au format ID-000 de cette même norme (format dit « plug-in »), au format microSIM, ou à tout autre format adapté (il peut s'agir d'un document d'identité en papier au format d'un passeport conventionnel, etc.). La carte peut comprendre une puce de carte bancaire, de carte SIM (l'acronyme SIM, de l'anglais Subscriber Identity Module, désigne de façon générique toutes les variantes CSIM, USIM, UICC etc.), de carte PKI, de carte d'accès, de carte de santé, de carte de transport, de carte d'identité, de passeport, de chronotachygraphe, etc.

En particulier, le dispositif électronique utilisateur peut être une carte SIM équipée d'un circuit électronique capable de gérer des communications sans fil de type NFC. Comme le format de petite taille d'une carte SIM rend difficile l'intégration d'une antenne, la carte SIM peut comprendre un contact conforme au standard SWP (Single Wire Protocol) permettant à la SIM de se raccorder à une antenne intégrée au téléphone portable et de fonctionner de façon autonome. Autrement dit, la carte peut fonctionner indépendamment du fait que le portable soit allumé ou éteint et que la batterie du téléphone portable soit chargée ou vide. La carte peut en effet être alimentée par le champ électromagnétique généré à cet effet par le lecteur NFC avec lequel elle entre en communication (un lecteur NFC intégré au dispositif électronique vérifieur, ou communiquant avec lui), via l'antenne NFC du téléphone portable. Ceci permet de mettre en place un environnement mieux contrôlé et plus sécurisé que celui du téléphone portable qui est souvent beaucoup plus complexe et ouvert (permettant le chargement d'applications tierces, et éventuellement de virus).

Le dispositif électronique utilisateur peut également être une carte mémoire dotée d'un processeur (de type secureMMC, etc.), une clé USB, etc. Le dispositif électronique utilisateur peut également être un ordinateur quelconque.

L'ensemble d'attributs stocké dans le dispositif électronique utilisateur est certifié par un dispositif électronique certificateur CERT_SRV à l'aide d'une fonction de signature électronique sanitisable. Ladite fonction est associée à une clé de signature SIG_K stockée dans ledit dispositif électronique certificateur ainsi qu'à ladite clé de modification MOD_K. Le dispositif électronique utilisateur est agencé pour modifier l'ensemble d'attributs en effaçant des attributs autres que les attributs BIRTH_D et CITY requis pour l'accès anonyme audit service, et pour déterminer, à l'aide de la clé de modification, la signature de l'ensemble d'attributs modifié. Ceci permet le contrôle ultérieur, par un dispositif électronique vérifieur VERIF_PC (qui peut être un ordinateur de type PC, un serveur, un lecteur NFC comprenant un circuit pour communiquer avec le dispositif électronique utilisateur, etc.), du fait que la signature électronique de l'ensemble modifié correspond à une signature valide du dispositif électronique certificateur.

Selon un mode de réalisation, un dispositif électronique utilisateur est agencé pour déterminer la signature de l'ensemble d'attributs modifié sans communiquer avec le dispositif électronique certificateur. Ceci permet le contrôle ultérieur, par le dispositif électronique vérifieur, sans que ce dispositif électronique vérifieur ne communique lui non plus avec le dispositif électronique certificateur, du fait que la signature électronique de l'ensemble modifié correspond à une signature valide du dispositif électronique certificateur. Le dispositif électronique certificateur n'étant à aucun moment impliqué dans la requête d'accès par le dispositif électronique utilisateur ni le traitement de cette requête par le dispositif électronique vérifieur, ce dispositif électronique certificateur ne peut matériellement collecter aucune information sur le dispositif électronique utilisateur (et sur son détenteur humain) à l'occasion de cette transaction (et ce que la transaction aboutisse ou non à une approbation de l'accès).

Selon un mode de réalisation, un dispositif électronique utilisateur est agencé pour effacer les attributs autres que les attributs requis pour l'accès anonyme audit service en retirant lesdits attributs à effacer de l'ensemble d'attributs.

5 Selon un mode de réalisation, un dispositif électronique utilisateur est agencé pour effacer les attributs autres que les attributs requis pour l'accès anonyme audit service en remplaçant lesdits attributs à effacer par des informations anonymes.

10 Selon un mode de réalisation, la fonction de signature électronique sanitisable d'un dispositif électronique utilisateur est de l'un des types suivants: une fonction de signature caviardable, ou une fonction de signature électronique conventionnelle couplée à une fonction de hachage caméléon, ou encore une fonction de signature électronique conventionnelle couplée à une fonction de noircissage.

15 Selon un mode de réalisation, les attributs (par exemple BIRTH_D et CITY) requis pour l'accès anonyme au service dépendent dudit service, le dispositif électronique utilisateur étant agencé pour déterminer lesdits attributs requis en fonction dudit service.

20 Selon un mode de réalisation, un système de contrôle d'accès anonyme à un service comprend un dispositif électronique utilisateur selon un mode de réalisation, et au moins l'un des deux dispositifs suivants:

- un dispositif électronique certificateur CERT_SRV agencé pour certifier un ensemble d'attributs FIRST_N, LAST_N, BIRTH_D, BIRTH_P, ADDR, CITY, STATE et CSHIP à l'aide d'une fonction de signature électronique sanitisable, ladite fonction étant associée à une clé de signature stockée dans le dispositif électronique certificateur ainsi qu'à une clé de modification, de manière à permettre au
25 dispositif électronique utilisateur, lorsqu'il a préalablement stocké l'ensemble d'attributs certifié ainsi que la clé de modification, de modifier l'ensemble d'attributs en effaçant des attributs autres que les attributs BIRTH_D et CITY requis pour l'accès anonyme audit service, et de déterminer, à l'aide de la clé de modification, la signature de l'ensemble modifié,
- un dispositif électronique vérifieur VERIF_PC agencé pour recevoir du dispositif électronique
30 utilisateur un ensemble certifié d'attributs BIRTH_D, CITY, et pour contrôler que la signature électronique de l'ensemble reçu correspond à une signature valide d'un dispositif électronique certificateur CERT_SRV.

35 Le dispositif électronique utilisateur peut être agencé pour communiquer avec le dispositif électronique certificateur via un réseau filaire ou sans fil (par exemple de type Ethernet, WiFi, ATM, ADSL, satellite, Wimax, réseaux cellulaires 1G, 2G, 3G, 4G etc.), éventuellement par l'intermédiaire d'un hôte (par exemple un ordinateur personnel ou un téléphone portable auquel on connecte le dispositif électronique utilisateur). Le dispositif électronique vérifieur peut également être agencé pour communiquer avec le dispositif électronique certificateur via un réseau filaire ou sans fil (par exemple de

type Ethernet, Wi-Fi, ATM, ADSL, satellite, Wimax, réseaux cellulaires 1G, 2G, 3G, 4G etc.). Cependant, dans le cadre d'une transaction d'autorisation d'accès, le dispositif électronique utilisateur et le dispositif électronique vérifieur peuvent être agencés pour ne communiquer ni l'un ni l'autre avec le dispositif électronique certificateur. Le dispositif électronique utilisateur et le dispositif électronique vérifieur peuvent être agencés pour communiquer entre eux à l'aide de protocoles filaires ou sans fil qui peuvent être des protocoles à courte portée (ZigBee, Bluetooth, infrarouge tel que l'irDA, connexion USB, connexion FireWire - IEEE 1394, connexion SATA ou eSata, connexion CPL, connexion Wireless USB, connexion propriétaire, ISO 7816, ISO 14443A ou ISO 14443B, Wi-Fi, etc.).

Le dispositif électronique certificateur peut comprendre des éléments de redondance, par exemple des disques durs ou des mémoires protégées selon une technique RAID (pour redundant array of independent disks) bien connue, protégeant ainsi contre la perte de la clé de signature sans pour autant imposer de stockage de cette clé hors du dispositif électronique certificateur.

Selon un mode de réalisation, un programme d'ordinateur est agencé pour mettre en œuvre un procédé selon un mode de réalisation lorsqu'il est exécuté par un processeur. Le processeur peut être un processeur du dispositif électronique utilisateur, ou un processeur d'un module de sécurité inséré dans un tel dispositif (par exemple un processeur de carte à puce SIM insérée dans un téléphone portable). Le programme d'ordinateur peut être écrit en langage C, en Java, en C++, en C#, en Basic (et ses multiples variantes), en assembleur, ou en tout langage approprié. Le programme d'ordinateur peut comprendre des instructions adaptées pour tirer partie d'un support matériel dédié du processeur, tel qu'un cryptoprocèsseur permettant d'accélérer certains calculs (tels que des exponentiations modulaires) qui sinon peuvent être plus lents à mettre en œuvre sur la seule base d'un jeu d'instruction standard de processeur conventionnel.

Selon un mode de réalisation, un support de stockage non transitoire lisible par ordinateur stocke un programme selon un mode de réalisation possible. Le support de stockage peut être par exemple une carte à puce, une clé USB, un microcontrôleur doté d'une mémoire non volatile (EEPROM, Flash, ROM, etc.), une puce mémoire, une carte mémoire, un support de stockage magnétique (disque dur, bande magnétique, disquette, etc.), ou tout autre forme de stockage adaptée.

Des modes de réalisation spécifiques particulièrement avantageux sont décrits plus précisément ci-après.

Les participants d'un système d'accréditation anonyme sont des organisations (disposant de dispositifs électroniques certificateurs), des utilisateurs (disposant de dispositifs électroniques certificateurs), et des vérificateurs (disposant de dispositifs électroniques vérificateurs). Les organisations délivrent des accréditations (par exemple des attributs certifiés) aux utilisateurs, qui peuvent les utiliser de manière anonymes auprès de vérificateurs (par exemple des fournisseurs de services). Un système d'accréditation anonyme peut mettre en œuvre les fonctions suivantes.

AC:Setup :

La fonction AC:Setup a pour but de générer les paramètres du système. Elle prend en entrée un paramètre de sécurité λ (qui peut correspondre à la taille des éléments cryptographiques à manipuler) et retourne les paramètres param (éléments d'un groupe et scalaires qui sont publics).

5 AC:OrgKeyGen, AC:UserKeyGen :

Les fonctions OrgKeyGen et UserKeyGen génèrent des clefs (secrètes et/ou publiques) pour, respectivement, les organisations et les utilisateurs.

AC:Obtain $\leftrightarrow$ AC:Issue.

10 Ces deux fonctions forment un protocole exécuté entre un utilisateur souhaitant obtenir une accréditation et une organisation délivrant des accréditations. La fonction Obtain, exécutée par l'utilisateur, prend en entrée une clef secrète sk_U et une clef publique d'organisation pk_O . La fonction Issue, exécutée par l'organisation, prend en entrée une clef secrète d'organisation sk_O , une donnée publique utilisateur pk_U et une liste d'attributs (nom, date de naissance, étude, etc.) qu'elle souhaite certifier à l'utilisateur $\{m_n\}_{n=1}^N := \{m_1, m_2, \dots, m_N\}$.

15 A la fin du protocole, l'utilisateur U a obtenu une accréditation C (ou bien un message d'erreur $\perp$ a été généré).

$$C \leftarrow \text{OBTAIN}(sk_U, pk_O) \leftrightarrow \text{ISSUE}(sk_O, pk_U, \{m_n\}_{n=1}^N)$$

La double flèche $\leftrightarrow$ symbolise les interactions entre les différents programmes qui s'exécutent et les flèches $\leftarrow$ et $\rightarrow$ indiquent les sorties des fonctions.

20 AC:Show $\leftrightarrow$ AC:Verify. Ces deux fonctions forment un protocole exécuté entre un utilisateur souhaitant justifier la possession d'une accréditation et un vérifieur souhaitant vérifier cette possession.

La fonction Show, exécutée par l'utilisateur, prend en entrée une clef secrète sk_U , une clef publique pk_O , une liste de messages $\{m_n\}_{n=1}^N$ et une accréditation C. La fonction Verify, exécutée par le vérifieur, prend en entrée une clef publique pk_O et une liste M de messages telle que $M \subseteq \{m_n\}_{n=1}^N$.

25 A la fin du protocole, la fonction Verify retourne un bit $b \in \{0, 1\}$ indiquant s'il accepte la preuve de possession de l'utilisateur.

$$\text{SHOW}(sk_U, pk_O, \{m_n\}_{n=1}^N, C) \leftrightarrow \text{VERIFY}(pk_O, M) \rightarrow b$$

Le protocole de vérification est public: il ne nécessite pas de clef secrète pour être exécuté.

Les notations suivantes sont utilisées.

Un message m est, génériquement, une chaîne de bits de longueur $m \in \{0, 1\}^*$ (c'est-à-dire une suite de bits 0 ou 1, de longueur arbitraire comme l'indique l'étoile $*$). On sépare les messages en blocs $m := m_1 \parallel \dots \parallel m_N$, où N est le nombre de blocs et $\parallel$ un symbole de concaténation.

Les portions de message que l'utilisateur pourra modifier, ou supprimer selon les cas, sont désignées par un sous-ensemble d'indice $\text{ADM} \subseteq \{1, \dots, N\}$.

La partie fixe m_{FIX} d'un message $m = m_1 \parallel \dots \parallel m_N$ d'après un ensemble de portions admissibles ADM est donnée par la fonction $\text{FIX}_{\text{ADM}} : m \mapsto m_{i_1} \parallel \dots \parallel m_{i_n}$ où $\{i_1, \dots, i_n\} := \{1, \dots, N\} \setminus \text{ADM}$.

Les instructions de modification MOD , étant donnée une assignation de portions (ou blocs) admissibles (c'est-à-dire modifiables) ADM pour un message $m = m_1 \parallel \dots \parallel m_N$, sont données par une liste de paires d'indices et de messages $\text{MOD} := \{(j, m'_j)\}_{j \in \text{ADM}}$ où $|m_j| = |m'_j|$ (c'est-à-dire que le bloc modifié m'_j a la même taille, en nombre de bits, que le bloc m_j d'origine), pour tout $j \in \text{ADM}$. Ces instructions dénotent le fait que le $j^{\text{ème}}$ bloc de message m doit être remplacé par le nouveau bloc m'_j .

Dans le cas des signatures caviardables, une instruction de modification (j, m'_j) devient $(j, \perp)$, le symbole $\perp$ (« bot », de l'anglais bottom) indiquant que le $j^{\text{ème}}$ bloc de message doit être noirci ou supprimé.

La notation $\text{MOD} \subseteq \text{ADM}$ indique que les instructions de modification MOD sont compatibles avec les portions admissibles ADM . C'est-à-dire que ces instructions ne demandent pas de modifier un bloc qui n'a pas été désigné comme modifiable.

On note $m' := \text{MOD}(m)$ le message m' résultant de la sanitisation du message m selon les instructions de modification MOD .

Soit ADM des portions admissibles et (m_0, MOD_0) et (m_1, MOD_1) deux messages accompagnés d'instructions de modification. Si les messages sont identiques une fois que la sanitisation a été appliquée, alors on note $(m_0, \text{MOD}_0, \text{ADM}) \equiv (m_1, \text{MOD}_1, \text{ADM})$.

La notation $\{m'_{n'}\}_{n'=1}^{N'} \subseteq \{m_n\}_{n=1}^N$ indique qu'il existe un sous-ensemble d'indices $\{j_{n'}\}_{n'=1}^{N'} \subseteq \{1, \dots, N\}$ tel que $m'_{n'} = m_{j_{n'}}$ pour tout $n' \in \{1, \dots, N'\}$.

Dans un schéma de signature sanitisable, noté SAN , deux types de participants sont présents: les signeurs et les sanitiseurs. Un schéma de signature sanitisable est donné par les cinq fonctions suivantes.

SAN:Setup .

La fonction Setup génère les paramètres du système. Elle prend en entrée un paramètre de sécurité λ (qui correspond à la taille des éléments cryptographiques à manipuler) et retourne les paramètres param (éléments d'un groupe et scalaires qui sont publics).

SAN:SigKeyGen, SAN:SanKeyGen.

5 Les fonctions SigKeyGen et SanKeyGen génèrent des clefs pour, respectivement, les signeurs et les sanitiseurs.

SAN:Sign.

La fonction de signature Sign prend en entrée une clef secrète sk_{sig} , un sanitiseur i désigné par l'indice i à qui il souhaite déléguer le droit de modifier le message, un message m et des portions admissibles ADM. Il génère une signature σ (ou un message d'erreur $\perp$, utilisant la même notation que pour la fonction de noircissage / suppression mais il s'agit ici d'une notion différente).

$$\sigma \leftarrow \text{SIGN}(sk_{sig}, i, m, \text{ADM})$$

SAN:Sanitize.

La fonction de sanitisation Sanitize prend en entrée une clef secrète de sanitiseur sk_{san} , la clef publique du signeur pk_{sig} , le message m , la signature σ et des modifications d'instructions MOD. Elle génère un message m' et une signature σ' sur ce message (ou un message d'erreur $\perp$).

$$(m', \sigma') \leftarrow \text{SANITIZE}(sk_{san}, pk_{sig}, m, \sigma, \text{MOD})$$

SAN:Verify.

La fonction de vérification Verify prend en entrée la clef publique du signeur pk_{sig} , le message m et la signature σ . Elle retourne un bit d'acceptation $b \in \{0, 1\}$ indiquant si la signature est valide ou non.

La procédure de vérification est publique: elle ne nécessite pas de clef secrète pour être exécutée.

Il existe différentes versions de signatures sanitisables. Les propriétés fonctionnelles et de sécurité de ces différentes versions varient selon les versions. Dans le cadre des modes réalisations décrits ci-dessous, le procédé s'appuie sur des signatures sanitisables remplissant les conditions suivantes. D'autres propriétés pourraient être ajoutées, mais ne sont pas indispensables. Il s'agit de conditions nécessaires pour obtenir les propriétés recherchées pour les accréditations anonymes dans le cadre de ces modes de réalisation (bien sûr, d'autres modes de réalisation moins sécurisés sont envisageables).

P1A

La vérification d'une signature ne doit pas nécessiter la clé publique du sanitiseur qui a le droit de modifier le couple message/signature que l'on a. Ceci nous permet d'obtenir l'anonymat du sanitiseur (et donc de l'utilisateur dans notre système d'accréditations). En effet, même si la clé publique n'était pas liée à un individu formellement identifié, le simple fait qu'elle existe permettrait au minimum de suivre les

transactions de l'utilisateur associé à cette clé publique, et pour peu que l'une des transactions révèle son identité, il serait éventuellement possible de lui associer toutes les transactions correspondantes.

P1B

5 Alternativement, la clé du sanitiseur est nécessaire, mais elle est cachée au moment de la vérification. A cette fin, le procédé s'appuie sur une preuve à divulgation nulle de connaissance (preuve dite « zero-knowledge ») pour cacher la clé du sanitiseur, tout en prouvant que la signature obtenue est valide.

10 P2

L'utilisateur/sanitiseur ne doit pas être capable de remplacer l'un de ses attributs par quelque chose qui l'arrange (par exemple remplacer sa véritable ville de résidence par celle dont il souhaite profiter des services). En pratique, le sanitiseur ne doit pas être capable de remplacer une partie admissible d'un message signé par ce qu'il veut. Il faut par conséquent un système qui limite les
15 modifications que peut apporter le sanitiseur.

P3

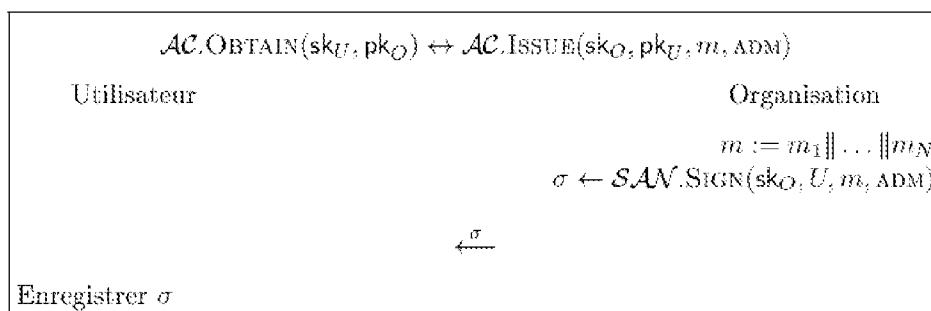
Si un message initialement signé est modifié deux fois de la même façon par le même sanitiseur, cela doit être fait de façon non traçable: on ne doit pas savoir qu'il s'agit de la même entité.

20

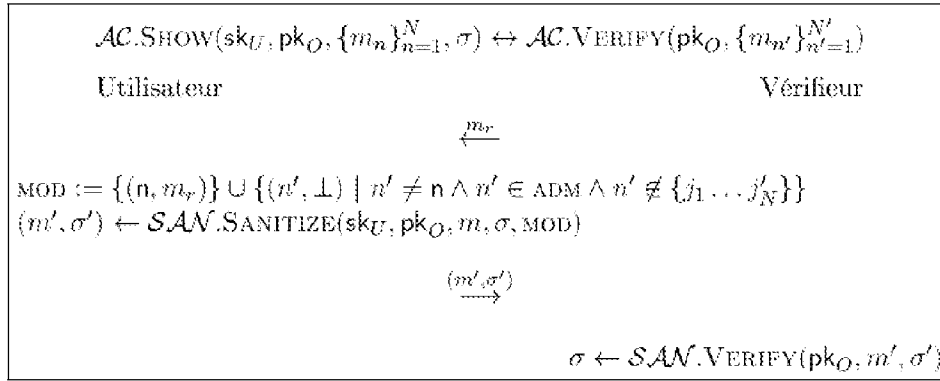
P4

Le jeu d'une signature sanitisée doit être infaisable. Cette phase doit contenir un aléa maîtrisé à la fois par le sanitiseur et le vérifieur.

25 L'obtention d'une accréditation peut s'effectuer selon le schéma suivant :



L'utilisation d'une accréditation peut, quant à elle, obéir au schéma suivant :



Un système d'accréditation anonyme AC selon un mode de réalisation s'appuie sur un schéma de signature sanitisable SAN respectant les propriétés PIA ou PIB, ainsi que P2 à P4, énoncées ci-dessus.

5 La procédure AC:Setup de génération des paramètres du système d'accréditation anonyme est la procédure SAN:Setup de génération des paramètres du schéma de signature sanitisable.

La procédure AC:UserKeyGen de génération des clefs des utilisateurs du système d'accréditation anonyme est la procédure SAN:SanKeyGen de génération des clefs des sanitiseurs du schéma de signature sanitisable.

10 La procédure AC:OrgKeyGen de génération des clefs des organisations du système d'accréditation anonyme est la procédure SAN:SigKeyGen de génération des clefs des signeurs du schéma de signature sanitisable.

Le protocole AC:Obtain $\leftrightarrow$ AC:Issue d'obtention d'une accréditation anonyme par un utilisateur est exécuté de la manière suivante.

15 Supposons que le document à signer $m \in \{0, 1\}^*$ soit de longueur t (t bits), l'organisation O sépare m en N blocs de longueurs respectives $\{t_n\}_{n=1}^N$ et spécifie un sous-ensemble d'indices $\text{ADM} \subseteq \{1, \dots, N\}$ à sa convenance. Un champ spécifique, d'indice n , est choisi. L'organisation O génère alors une signature $\sigma := \text{SAN:Sign}(\text{sk}_O; \text{pk}_U; m; \text{ADM})$ à l'aide de la clef publique pk_U de l'utilisateur U et envoie la signature à U. L'utilisateur U enregistre σ comme une accréditation de O sur le message m .

20 Le document à accréditer peut correspondre à une concaténation des noms (ou identifiants) des champs (par exemple LAST_N, ADDR, etc.) et à la valeur de chacun de ces champs dans le cas d'espèce considéré (par exemple « Lescuyer », « Caen », etc.). Les parties admissibles peuvent correspondre aux valeurs des champs, et exclure les identifiants des champs (dans cette hypothèse, l'utilisateur ne doit pas pouvoir modifier LAST_N mais doit pouvoir modifier « Lescuyer », du moins il doit pouvoir le modifier d'une manière autorisée). La clé publique de l'utilisateur qui obtient l'accréditation correspond à sa clé publique de sanitiseur.

25 Le protocole AC:Show $\leftrightarrow$ AC:Verify d'utilisation d'une accréditation par un utilisateur U auprès d'un vérifieur V peut être exécuté de la manière suivante.

Supposons qu'un vérifieur V souhaite vérifier qu'un utilisateur U possède une accréditation certifiant la possession d'un ensemble d'attributs M. Supposons que l'utilisateur U possède une accréditation σ sur un document $m = m_1 \parallel \dots \parallel m_N$ tel que $\mathbf{M} \subseteq \{m_n\}_{n=1}^N$ (c'est-à-dire que le document m possède les attributs demandés).

Dans un premier temps, le vérifieur envoie une valeur aléatoire r à l'utilisateur U. Cette valeur r peut être par exemple la concaténation de données propres à la vérification et à l'heure courante. Dans un second temps, l'utilisateur U sanitise le document selon les instructions de modification suivantes

$$\text{MOD} := \{(n, r)\} \cup \{(n', \perp) \mid n' \neq n \wedge n' \in \text{ADM} \wedge n' \notin \{j_1 \dots j_N'\}\}$$

et calcule

$$(m', \sigma') \leftarrow \text{SAN.SANITIZE}(\text{sk}_U, \text{pk}_O, m, \sigma, \text{MOD})$$

L'utilisateur envoie (m', σ') au vérifieur. Le vérifieur vérifie que la signature σ' est une signature valide de message m' grâce à la clef publique de l'organisation O. Il renvoie 1 si c'est le cas et 0 sinon.

Un mode de réalisation est décrit plus précisément ci-dessous dans le cas d'une fonction de sanitisation particulièrement avantageuse.

Ce mode de réalisation s'applique à des documents quelconques. Un document peut être défini comme une chaîne quelconque de bits. L'espace des messages est donc $\mathcal{M} := \{0, 1\}^*$. Cependant, tous les documents à signer comportent un champ réservé de longueur fixe l_n .

Ce mode de réalisation s'appuie sur une fonction de hachage qui permet de hacher uniformément dans $\{0, 1\}^{l_n}$.

Selon ce mode de réalisation, les blocs de messages à noircir sont noircis d'une façon unique. Un bloc m_n de longueur $|m_n|$ est toujours remplacé par un bloc de même taille. Le noircissage d'un bloc m_n peut par exemple consister en un remplacement de ce bloc par une suite de bits 0 de même longueur que ce bloc.

Ce mode de réalisation se place dans le cadre d'un environnement bilinéaire symétrique $(p, \mathbb{G}, \mathbb{G}_T, e)$ pour effectuer les calculs.

Dans $(p, \mathbb{G}, \mathbb{G}_T, e)$, p est un nombre premier, $\mathbb{G}$ et $\mathbb{G}_T$ sont des groupes algébriques d'ordre p, et e est une application bilinéaire $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$. Il existe de nombreux algorithmes bien connus pour générer de tels environnements de calcul.

Les actions suivantes sont mises en œuvre afin de créer un environnement de calcul global pour le système :

1. Générer un environnement bilinéaire symétrique $(p, \mathbb{G}, \mathbb{G}_T, e)$
 2. Choisir des générateurs $g, g_2, u_1, u_2, v, h \xleftarrow{\$} \mathbb{G}$ (le signe \$ au dessus de la flèche désignant un choix opéré de façon aléatoire)
 3. Choisir deux fonctions de hachage $\mathcal{H}_1 : \{0, 1\}^* \rightarrow \mathbb{Z}_p$ et $\mathcal{H}_2 : \{0, 1\}^* \rightarrow \mathbb{Z}_p$
 4. Retourner les paramètres du système
- $\text{param} := (p, \mathbb{G}, \mathbb{G}_T, e, g, g_2, u_1, u_2, v, h, \mathcal{H}_1, \mathcal{H}_2)$

Le signeur génère ses clefs en mettant en œuvre les actions suivantes:

1. Choisir deux aléas $\gamma, \delta \xleftarrow{\$} \mathbb{Z}_p$
2. Calculer $X := g^\gamma, Y := g_2^\gamma$ et $\Delta := g^\delta$
3. Choisir une clef pour une fonction pseudo-aléatoire $k := \text{PRF.KEYGEN}()$
4. Retourner la paire de clefs $(\text{pk}_{\text{sig}}, \text{sk}_{\text{sig}}) := ((X, Y, \Delta), (\gamma, \delta, k))$

Le sanitiseur s'enregistre auprès d'un signeur, en mettant en œuvre les actions suivantes:

1. Générer deux aléas $y, r \xleftarrow{\$} \mathbb{Z}_p$ (dans le cas où le signeur est une carte à puce, la génération peut faire appel à un générateur aléatoire matériel, fournissant des aléas d'une qualité généralement supérieure à celle des générateurs purement algorithmiques, et s'appuyant par exemple sur un échantillonnage d'un bruit analogique mesuré au sein de la puce, traité éventuellement par un cryptoprocasseur)
2. Calculer $A := (g \cdot u_1^y)^{\frac{1}{\delta+r}}$
3. Donner (A, y, r) au sanitiseur.

Chacune des parties (le signeur et le sanitiseur), enregistre alors ces données en tant que certificat d'appartenance au système cert_{san}

Le protocole d'obtention d'une accréditation entre un utilisateur, déjà enregistré, et une organisation, est mis en œuvre de la façon suivante.

Le protocole rassemble les données utilisateurs en un document $m \in \{0, 1\}^*$ de longueur t (en bits). L'organisation sépare le document m en N blocs de longueurs respectives $\{t_n\}_{n=1}^N$ et spécifie un sous-ensemble d'indices $M \subseteq \{1, \dots, N\}$ désignant les portions de messages que l'utilisateur pourra cacher. Le protocole choisit un champ spécifique (champ réservé), d'indice $n \notin M$ et de longueur $t_n = l_n$. Le protocole définit $\text{ADM} := \{(n, \top)\} \cup \{(n, \perp) \mid n \in M\}$, ce qui signifie que le champ réservé m_n

peut être modifié à loisir par l'utilisateur tandis que les autres blocs modifiables ne peuvent être que noircis. La clef secrète sk_{sig} est (γ, δ, k) . Le sanitiseur i est représenté par son certificat $cert_{san,i} = (A_i, y_i, r_i)$. Ces différentes étapes (rassembler, séparer, spécifier, choisir, définir, représenter) peuvent être mises en œuvre par un dispositif distinct du dispositif électronique certificateur, également sous le contrôle de l'organisation, ou par le dispositif électronique certificateur lui-même.

Le signeur met en œuvre les actions suivantes.

1. Générer deux aléas r' et s' grâce à la fonction pseudo-aléatoire :

$$r' \leftarrow \mathcal{PRF.PRF}(k, 0 \| \Delta \| m_{FIX} \| ADM) \text{ et } s' \leftarrow \mathcal{PRF.PRF}(k, 1 \| \Delta \| m_{FIX} \| ADM)$$

2. Générer $|M| + 6$ aléas $t, t_0, t_1, \dots, t_{|M|}, r_y, r_r, r_t, r_b \xleftarrow{\$} \mathbb{Z}_p$

3. Hacher le message $c_1 \leftarrow \mathcal{H}_1(m_{FIX} \| ADM \| \Delta)$

4. Pour tout $n \in M$, exécuter les actions suivantes:

(a) Hacher $h_n \leftarrow \mathcal{H}_1(X \| Y \| \Delta \| m_{FIX} \| ADM \| n \| m_n)$

(b) Calculer $G_n := (g \cdot u_1^{y_i})^{\frac{1}{(\gamma + h_n)}}$; $B_{n,1} := g^{-t_n}$; $B_{n,2} := G_n \cdot h^{t_n}$

5. Calculer :

(a) $S := (g \cdot u_1^{y_i} \cdot u_2^{c_1} \cdot v^{s'})^{\frac{1}{(\gamma + r')}} ; B_{0,1} := g^{-t_0} ; B_{0,2} := S \cdot h^{t_0}$

(b) $T_1 := g^{-t} ; T_2 := A_i \cdot h^t$

(c) $R_1 := e(u_1, g)^{r_y} ; R_2 := g^{-r_r} ; R_3 := T_1^{r_r} \cdot g^{r_b}$

(d) $R_4 := e(T_2, g)^{r_r} \cdot e(h, \Delta)^{r_t} \cdot e(h, g)^{r_b} \cdot e(u_1, g)^{-r_y}$

6. Hacher le message :

$$c_2 \leftarrow \mathcal{H}_2(B_{0,1} \| B_{0,2} \| \prod_{n \in M} (B_{n,1} \cdot B_{n,2}) \| r' \| s' \| T_1 \| T_2 \| R_1 \| R_2 \| R_3 \| R_4 \| m \| X \| Y)$$

7. Calculer :

$$s_y := y_i \cdot c_2 + r_y ; s_r := r_i \cdot c_2 + r_r ; s_t := t \cdot c_2 + r_t ; s_b := r_i \cdot t \cdot c_2 + r_b$$

8. Poser :

$$\sigma := (B_{0,1}, B_{0,2}, \{(B_{n,1}, B_{n,2}) \mid n \in M\}, r', s', T_1, T_2, R_1, R_2, R_3, R_4, s_y, s_r, s_t, s_b, ADM)$$

Après avoir exécuté ces calculs (par exemple avec le dispositif électronique certificateur), l'organisation donne σ à l'utilisateur. Celui-ci enregistre σ comme accréditation sur le message m .

Le protocole permettant à l'utilisateur d'utiliser une accréditation afin d'obtenir un accès à un service auprès d'un fournisseur de service que l'on appellera le vérifieur est décrit ci-dessous. L'accréditation σ peut avoir été délivrée sur un message m par l'organisation identifiée par $pk_{sig} = (X, Y, \Delta)$ selon les modalités précitées. L'utilisateur possède un certificat $cert_{san} = (A_i, y_i, r_i)$. La signature σ est de la forme :

$$\sigma := (B_{0:1}, B_{0:2}, \{(B_{n:1}, B_{n:2}) \mid n \in M\}, r', s', T_1, T_2, R_1, R_2, R_3, R_4, s_y, s_r, s_t, s_b, \text{ADM})$$

L'utilisateur souhaite cacher un sous-ensemble d'attributs $\mathbf{M} \subseteq M$ du document m , où M est le sous-ensemble d'indices des blocs de messages que l'utilisateur a le droit de noircir.

On désigne par m' le document m dans lequel chaque portion m_j pour $j \in \mathbf{M}$ a été noircie.

5 Dans un premier temps, le vérifieur envoie à l'utilisateur une valeur aléatoire m_r (pour laquelle un champ réservé est prévu). On peut, par exemple, hacher dans $\{0,1\}^{l_0}$ la concaténation de données liées au fournisseur de service et la date courante.

Dans un second temps, l'utilisateur exécute les actions suivantes :

1. Générer $|M| - |\mathbf{M}| + 6$ aléas $t', t'_0, \{t'_n\}_{n \in M \setminus \mathbf{M}}, r_y, r_r, r_t, r_b \xleftarrow{\$} \mathbb{Z}_p$

10 2. Hacher le message $c_1 \leftarrow \mathcal{H}_1(m_{\text{FIX}} \parallel \text{ADM} \parallel \Delta)$

3. Pour tout $n \in M \setminus \mathbf{M}$, exécuter les actions suivantes :

(a) Hacher $h_n \leftarrow \mathcal{H}_1(X \parallel Y \parallel \Delta \parallel m_{\text{FIX}} \parallel \text{ADM} \parallel n \parallel m_n)$

(b) Calculer $B'_{n:1} := B_{n:1} \cdot g^{-t'_n}$; $B'_{n:2} := B'_{n:1} \cdot h^{t'_n}$

4. Calculer :

(a) $B'_{0:1} := B_{0:1} \cdot g^{-t'_0}$; $B'_{0:2} := B_{0:2} \cdot h^{t'_0}$

(b) $T'_1 := g^{-t'}$; $T'_2 := A_i \cdot h^{t'}$

(c) $R'_1 := e(u_1, g)^{r_y}$; $R'_2 := g^{-r_r}$; $R'_3 := T'^{r_r}_1 \cdot g^{r_b}$

15 (d) $R'_4 := e(T'_2, g)^{r_r} \cdot e(h, \Delta)^{r_t} \cdot e(h, g)^{r_b} \cdot e(u_1, g)^{-r_y}$

5. Hacher le message :

$$c_2 \leftarrow \mathcal{H}_2(B'_{0:1} \parallel B'_{0:2} \parallel \prod_{n \in M \setminus \mathbf{M}} (B'_{n:1} \cdot B'_{n:2}) \parallel r' \parallel s' \parallel T'_1 \parallel T'_2 \parallel R'_1 \parallel R'_2 \parallel R'_3 \parallel R'_4 \parallel m' \parallel X \parallel Y)$$

6. Calculer :

$$s_y := y_i \cdot c_2 + r_y ; \quad s_r := r_i \cdot c_2 + r_r ; \quad s_t := t \cdot c_2 + r_t ; \quad s_b := r_i \cdot t \cdot c_2 + r_b$$

20 7. Poser :

$$\sigma' := (B'_{0:1}, B'_{0:2}, \{(B'_{n:1}, B'_{n:2}) \mid n \in M \setminus \mathbf{M}\}, r', s', T'_1, T'_2, R'_1, R'_2, R'_3, R'_4, s'_y, s'_r, s'_t, s'_b, \text{ADM})$$

L'utilisateur envoie alors m' et σ' au vérifieur.

Dans un troisième temps, le vérifieur, ayant reçu des données de la forme :

$$(m', (B'_{0:1}, B'_{0:2}, \mathcal{B}, r', s', T'_1, T'_2, R'_1, R'_2, R'_3, R'_4, s'_y, s'_r, s'_t, s'_b, \text{ADM})),$$

25 exécute les actions suivantes:

1. Hacher le message $c_1 \leftarrow \mathcal{H}_1(m_{\text{FIX}} \parallel \text{ADM} \parallel \Delta)$

2. Hacher le message :

$$c_2 \leftarrow \mathcal{H}_2(B'_{0:1} \parallel B'_{0:2} \parallel B' \parallel r' \parallel s' \parallel T'_1 \parallel T'_2 \parallel R'_1 \parallel R'_2 \parallel R'_3 \parallel R'_4 \parallel m' \parallel X \parallel Y)$$

$$\text{où } B' := \prod_{(B'_{n:1}, B'_{n:2}) \in \mathcal{B}} (B'_{n:1} \cdot B'_{n:2})$$

3. Récupérer $\bar{M}$ présent dans ADM et poser $\bar{M}' := \{\}$ puis, pour tout $n \in \bar{M}$, mettre en œuvre les actions suivantes:

(a) Si la portion m_n est différente de la partie noire, alors

5 i. Si $(B_{n:1}, B_{n:2}) \notin \mathcal{B}$, arrêter l'algorithme et retourner 0, sinon, continuer.

ii. Mettre à jour $\bar{M}' := \bar{M}' \cup \{n\}$

iii. Hacher $h_n \leftarrow \mathcal{H}_1(X \| Y \| \Delta \| m_{\text{FIX}} \| \text{ADM} \| n \| m_n)$

4. Tester les équations suivantes :

$$(a) \ e(u_1, g)^{s'_y} = \left(\frac{e(B'_{0:2}, g^{r'} \cdot X) \cdot e(g_2^{r'} \cdot Y, B'_{0:1})}{e(g \cdot u_2^{c_1} \cdot v^{s'}, g)} \right)^{c_2} \cdot R'_1$$

$$(b) \ \text{Pour tout } n \in \bar{M}', \ e(u_1, g)^{s'_y} = \left(\frac{e(B'_{n:2}, g^{r'} \cdot X) \cdot e(g_2^{r'} \cdot Y, B'_{n:1})}{e(g, g)} \right)^{h_n} \cdot R'_1$$

$$(c) \ g^{-s'_t} = T_1^{c_2} \cdot R'_2$$

$$(d) \ T_1^{s'_r} \cdot g^{s'_b} = R'_3$$

$$(e) \ e(T'_2, g)^{s'_r} \cdot e(h, \Delta)^{s'_t} \cdot e(h, g)^{s'_b} \cdot e(u_1, g)^{-s'_y} = \left(\frac{e(g, g)}{e(T'_2, \Delta)} \right)^{c_2} \cdot R'_4$$

10 Si toutes ces équations sont vérifiées, le vérifieur retourne 1, sinon, il retourne 0.

Bien entendu, les exemples donnés ci-dessus ne sont nullement limitatifs.

Les modes de réalisation concernant les procédés peuvent être transposés aux dispositifs, et réciproquement.

Revendications

- 5 1. Procédé de contrôle d'accès anonyme à un service, dans lequel, un dispositif électronique utilisateur (ID_CARD) stockant un ensemble certifié d'attributs (FIRST_N, LAST_N, BIRTH_D, BIRTH_P, ADDR, CITY, STATE, CSHIP) et une clé de modification (MOD_K), ledit ensemble ayant été certifié par un dispositif électronique certificateur (CERT_SRV) à l'aide d'une fonction de signature électronique sanitisable, ladite fonction étant associée à une clé de signature (SIG_K) stockée dans ledit
- 10 dispositif électronique certificateur ainsi qu'à ladite clé de modification (MOD_K), le procédé comprend :
- /a1/ la modification, par le dispositif électronique utilisateur, de l'ensemble d'attributs, ladite modification comprenant l'effacement d'attributs autres que les attributs (BIRTH_D, CITY) requis pour l'accès anonyme audit service,
- /a2/ la détermination, par le dispositif électronique utilisateur, à l'aide de la clé de modification, de la
- 15 signature de l'ensemble modifié, afin de permettre le contrôle ultérieur, par un dispositif électronique vérifieur (VERIF_PC), du fait que la signature électronique de l'ensemble modifié correspond à une signature valide du dispositif électronique certificateur.
2. Procédé de contrôle d'accès selon la revendication 1, dans lequel la détermination de la signature
- 20 de l'ensemble modifié est opérée sans que le dispositif électronique utilisateur ne communique avec le dispositif électronique certificateur, afin de permettre le contrôle ultérieur, par le dispositif électronique vérifieur, sans que le dispositif électronique vérifieur ne communique avec le dispositif électronique certificateur, du fait que la signature électronique de l'ensemble modifié correspond à une signature valide du dispositif électronique certificateur.
- 25 3. Procédé de contrôle d'accès selon la revendication 1, dans lequel l'effacement d'attributs comprend le retrait des attributs à effacer de l'ensemble d'attributs.
4. Procédé de contrôle d'accès selon la revendication 1, dans lequel l'effacement d'attributs
- 30 comprend le remplacement des attributs à effacer par des informations anonymes.
5. Procédé de contrôle d'accès selon la revendication 1, dans lequel la fonction de signature électronique sanitisable est une fonction de signature caviardable, ou une fonction de signature électronique couplée à une fonction de hachage caméléon, ou encore une fonction de signature
- 35 électronique couplée à une fonction de noircissage.

6. Procédé de contrôle d'accès selon la revendication 1, dans lequel les attributs (BIRTH_D, CITY) requis pour l'accès anonyme audit service dépendent dudit service, et dans lequel le procédé comprend une détermination desdits attributs requis en fonction dudit service.

7. Procédé de contrôle d'accès selon la revendication 1, comprenant :

/a0/ la certification, par le dispositif électronique certificateur (CERT_SRV), de l'ensemble d'attributs (FIRST_N, LAST_N, BIRTH_D, BIRTH_P, ADDR, CITY, STATE, CSHIP) à l'aide de ladite fonction de signature électronique sanitisable.

8. Procédé de contrôle d'accès selon la revendication 1, comprenant :

/a3/ le contrôle, par le dispositif électronique vérifieur (VERIF_PC), du fait que la signature électronique de l'ensemble modifié correspond à une signature valide du dispositif électronique certificateur.

9. Dispositif électronique utilisateur (ID_CARD) agencé pour stocker une clé de modification (MOD_K) ainsi qu'un ensemble certifié d'attributs (FIRST_N, LAST_N, BIRTH_D, BIRTH_P, ADDR, CITY, STATE, CSHIP), l'ensemble d'attributs stocké étant certifié par un dispositif électronique certificateur (CERT_SRV) à l'aide d'une fonction de signature électronique sanitisable, ladite fonction étant associée à une clé de signature (SIG_K) stockée dans ledit dispositif électronique certificateur ainsi qu'à ladite clé de modification (MOD_K), le dispositif électronique utilisateur étant agencé pour modifier l'ensemble d'attributs en effaçant des attributs autres que les attributs (BIRTH_D, CITY) requis pour l'accès anonyme audit service, et pour déterminer, à l'aide de la clé de modification, la signature de l'ensemble d'attributs modifié, afin de permettre le contrôle ultérieur, par un dispositif électronique vérifieur (VERIF_PC), du fait que la signature électronique de l'ensemble modifié correspond à une signature valide du dispositif électronique certificateur.

10. Dispositif électronique utilisateur selon la revendication 9, le dispositif électronique utilisateur étant agencé pour déterminer la signature de l'ensemble d'attributs modifié sans communiquer avec le dispositif électronique certificateur, afin de permettre le contrôle ultérieur, par le dispositif électronique vérifieur, sans que ce dispositif électronique vérifieur ne communique avec le dispositif électronique certificateur, du fait que la signature électronique de l'ensemble modifié correspond à une signature valide du dispositif électronique certificateur.

11. Dispositif électronique utilisateur selon la revendication 9, agencé pour effacer les attributs autres que les attributs requis pour l'accès anonyme audit service en retirant lesdits attributs à effacer de l'ensemble d'attributs.

12. Dispositif électronique utilisateur selon la revendication 9, agencé pour effacer les attributs autres que les attributs requis pour l'accès anonyme audit service en remplaçant lesdits attributs à effacer par des informations anonymes.

5

13. Dispositif électronique utilisateur selon la revendication 9, dans lequel la fonction de signature électronique sanitisable est de l'un des types suivants : une fonction de signature caviardable, ou une fonction de signature électronique conventionnelle couplée à une fonction de hachage caméléon, ou encore une fonction de signature électronique conventionnelle couplée à une fonction de noircissage.

10

14. Dispositif électronique utilisateur selon la revendication 9, dans lequel, les attributs (BIRTH_D, CITY) requis pour l'accès anonyme audit service dépendant dudit service, le dispositif électronique utilisateur est agencé pour déterminer lesdits attributs requis en fonction dudit service.

15

15. Système de contrôle d'accès anonyme à un service, comprenant un dispositif électronique utilisateur selon la revendication 9, et au moins l'un des deux dispositifs suivants :

- un dispositif électronique certificateur (CERT_SRV) agencé pour certifier un ensemble d'attributs (FIRST_N, LAST_N, BIRTH_D, BIRTH_P, ADDR, CITY, STATE, CSHIP) à l'aide d'une fonction de signature électronique sanitisable, ladite fonction étant associée à une clé de signature stockée dans le dispositif électronique certificateur ainsi qu'à une clé de modification, de manière à permettre au dispositif électronique utilisateur, lorsqu'il a préalablement stocké l'ensemble d'attributs certifié ainsi que la clé de modification, de modifier l'ensemble d'attributs en effaçant des attributs autres que les attributs (BIRTH_D, CITY) requis pour l'accès anonyme audit service, et de déterminer, à l'aide de la clé de modification, la signature de l'ensemble modifié,

20

- un dispositif électronique vérifieur (VERIF_PC) agencé pour recevoir du dispositif électronique utilisateur un ensemble certifié d'attributs (BIRTH_D, CITY), et pour contrôler que la signature électronique de l'ensemble reçu correspond à une signature valide d'un dispositif électronique certificateur (CERT_SRV).

25

30

16. Programme d'ordinateur agencé pour mettre en œuvre le procédé selon la revendication 1 lorsqu'il est exécuté par un processeur.

17. Support de stockage non transitoire lisible par ordinateur, stockant un programme selon la revendication 16.

35

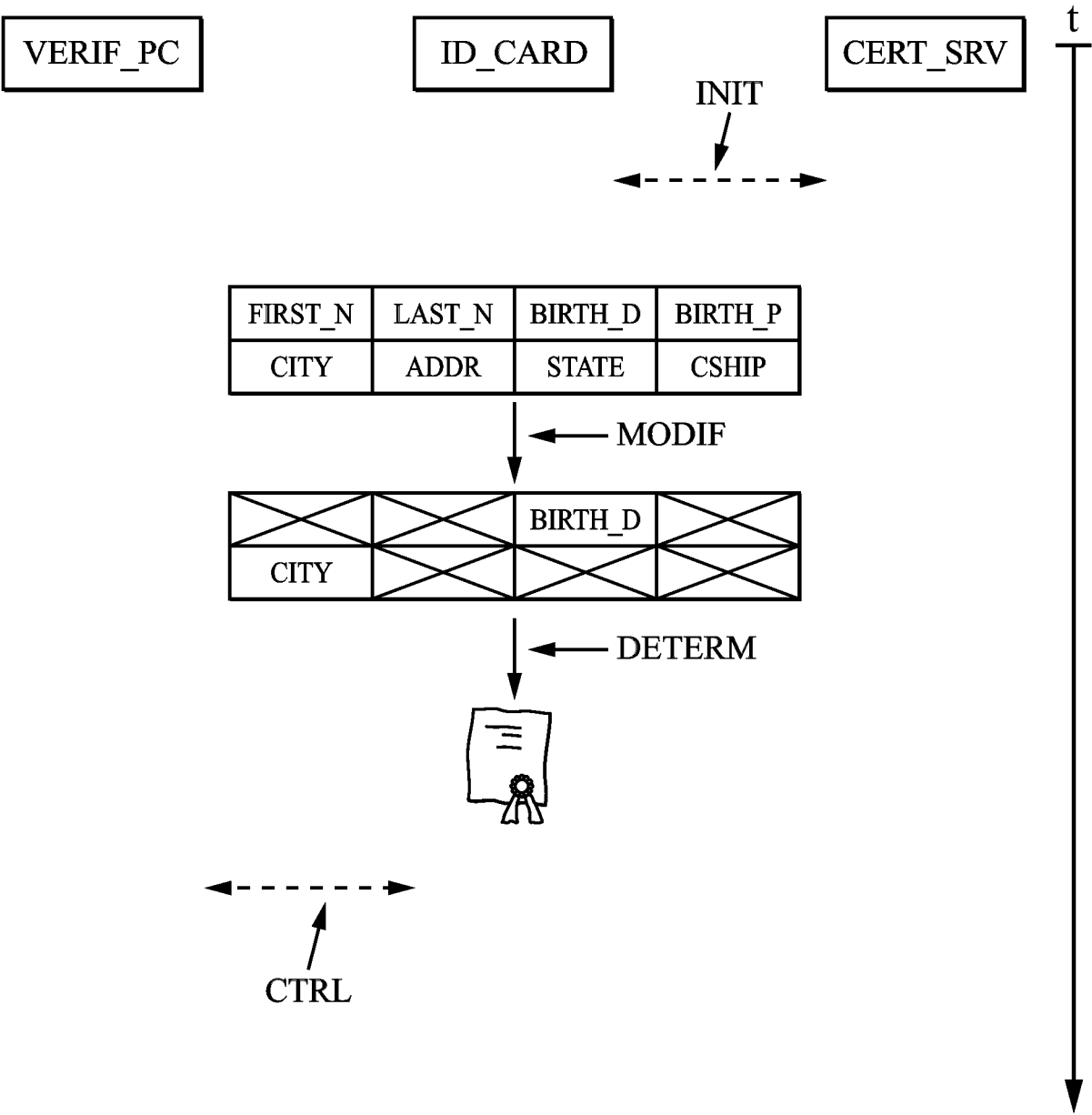


FIG. 1

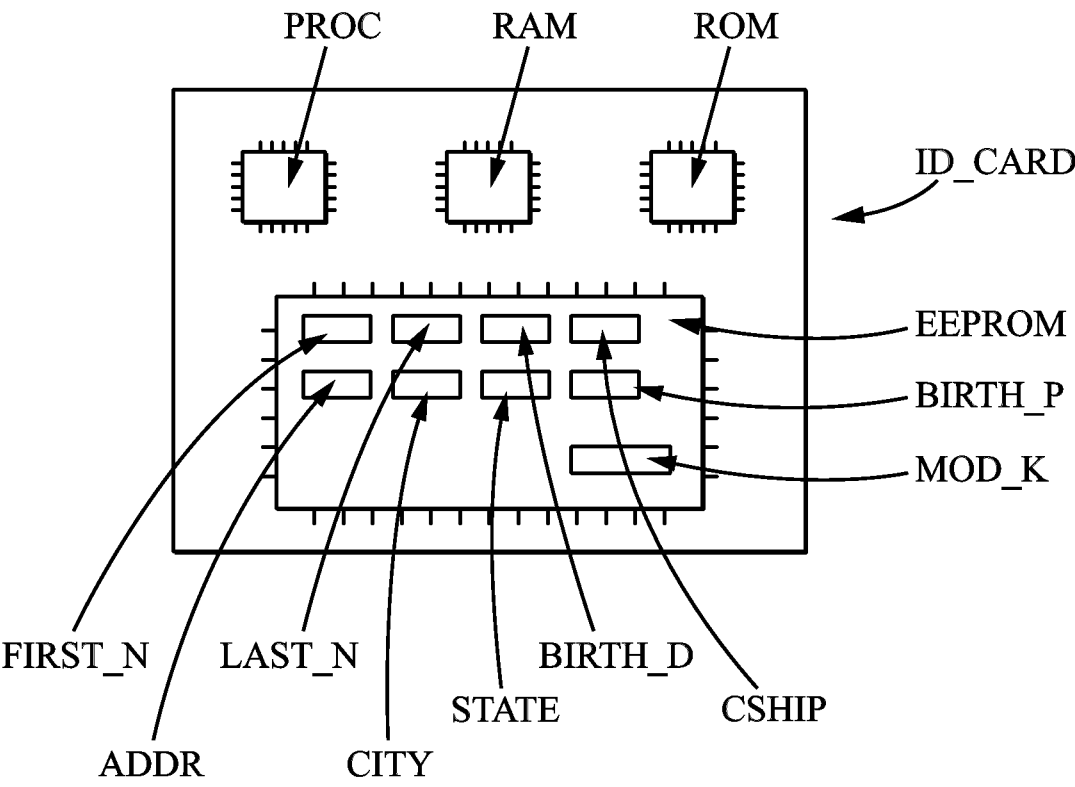


FIG. 2

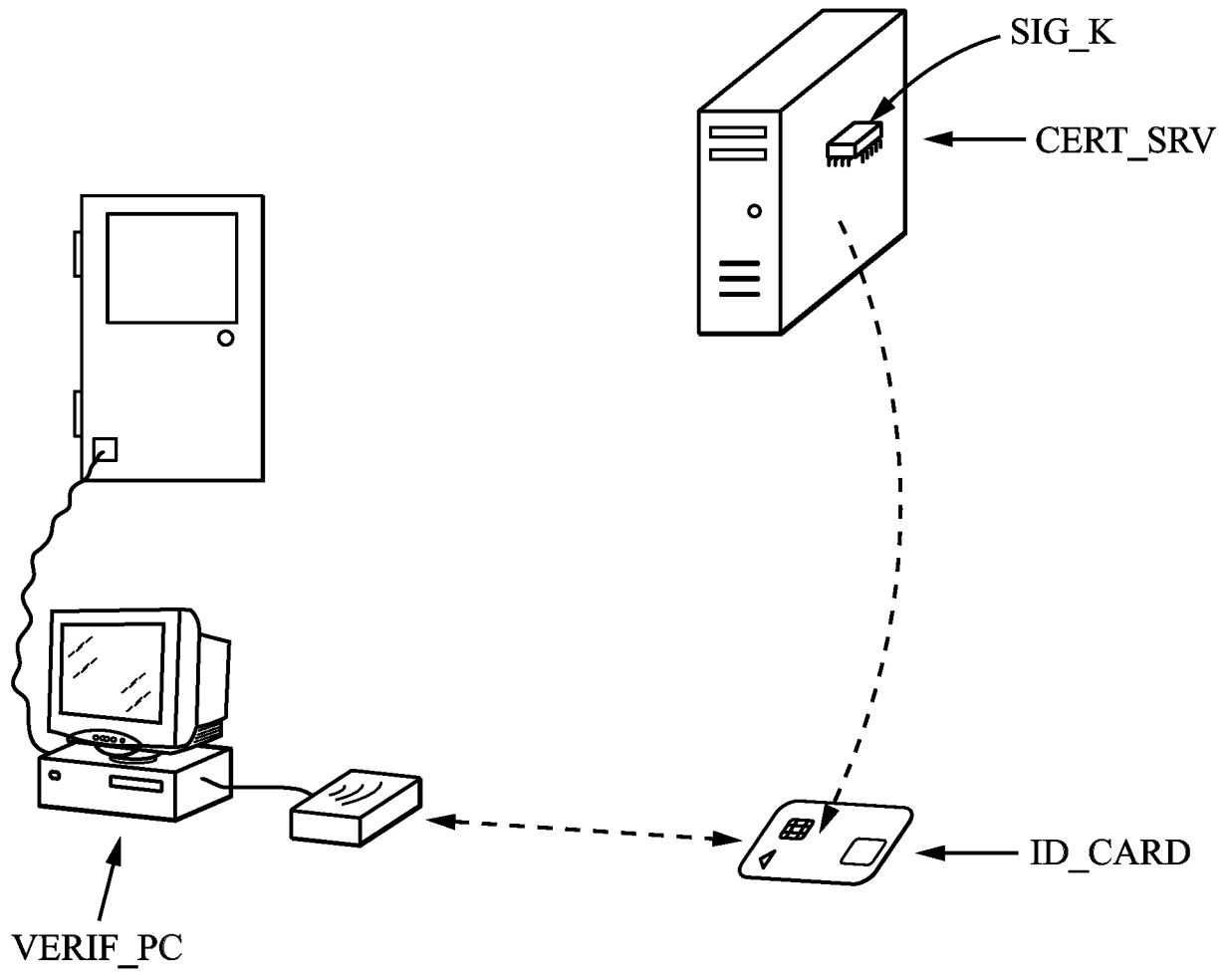


FIG. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2012/052780

A. CLASSIFICATION OF SUBJECT MATTER
INV. 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 practicable, search terms used)

EPO-Internal , WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Camei sch J. and Neven G. : "Savi ng On-Li ne Pri vacy" In: Bezzi et al . : "Pri vacy and Identi ty Management for Li fe" , 11 September 2009 (2009-09-11) , Spri nger, XP009162615 , secti ons 1 and 2 -----	1-17
T	GIUSEPPE ATENIESE ET AL: "Sani t i zabl e Signatures" , 1 January 2005 (2005-01-01) , COMPUTER SECURITY - ESORICS 2005 LECTURE NOTES IN COMPUTER SCI ENCE; ; LNCS, SPRINGER, BERLIN , DE, PAGE(S) 159 - 177 , XP019019069 , ISBN : 978-3-540-28963-0 ----- -/- .	



Further documents are listed in the continuation of Box C.



See patent family annex.

* Spécial catégories of cited documents :

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

"E" earlier application or patent 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 spécial 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

30 January 2013

Date of mailing of the international search report

06/02/2013

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

Bi l l e t, O l i v i e r

INTERNATIONAL SEARCH REPORT

International application No

PCT/FR2012/052780

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	MAREK KLONOWSKI ET AL: "Extended Sanitizable Signatures" , 1 January 2006 (2006-01-01) , INFORMATION SECURITY AND CRYPTOLOGY 4296/2006; ICISC 2006 LECTURE NOTES IN COMPUTER SCIENCE; ; LNCS, SPRINGER, BERLIN , DE, PAGE(S) 343 - 355 , XP019051336, ISBN: 978-3-540-49112-5 sections 1-5 -----	1-17
A	MIYAZAKI K ET AL: "Invisibly sanitizable digital signature scheme" , IEEE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS, COMMUNICATIONS AND COMPUTER SCIENCES, ENGINEERING SCIENCES SOCIETY, TOKYO, JP, vol . E91A, no. 1, 1 January 2008 (2008-01-01) , pages 392-402 , XP001510014, ISSN: 0916-8508, DOI : 10.1093/IETFEC/E91-A. 1.392 sections 1-3 -----	1-17

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°

PCT/FR2012/052780

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. 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 , 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
X	Camei sch J. and Neven G. : "Savi ng On-Li ne Pri vacy" In: Bezzi et al. : "Pri vacy and Identi ty Management for Li fe" , 11 septembre 2009 (2009-09-11) , Spri nger, XP009162615 , secti ons 1 and 2	1-17
T	GIUSEPPE ATENIESE ET AL: "Sani t i zabl e Signatures" , 1 janvi er 2005 (2005-01-01) , COMPUTER SECURITY - ESORICS 2005 LECTURE NOTES IN COMPUTER SCI ENCE; ; LNCS, SPRINGER, BERLIN , DE, PAGE(S) 159 - 177 , XP019019069 , ISBN : 978-3-540-28963-0	



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

30 janvi er 2013

Date d'expédition du présent rapport de recherche internationale

06/02/2013

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

Bi l l et, ol i vi er

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	MAREK KLONOWSKI ET AL: "Extended Sanitizable Signatures" , 1 janvier 2006 (2006-01-01) , INFORMATION SECURITY AND CRYPTOLOGY 4296/2006; ICISC 2006 LECTURE NOTES IN COMPUTER SCIENCE; ; LNCS, SPRINGER, BERLIN , DE, PAGE(S) 343 - 355 , XP019051336, ISBN : 978-3-540-49112-5 sections 1-5 -----	1-17
A	MIYAZAKI K ET AL: "Invisibly sanitizable digital signature scheme" , IEEE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS, COMMUNICATIONS AND COMPUTER SCIENCES, ENGINEERING SCIENCES SOCIETY, TOKYO, JP, vol . E91A, no. 1, 1 janvier 2008 (2008-01-01) , pages 392-402 , XP001510014, ISSN : 0916-8508, DOI : 10.1093/IETFEC/E91-A. 1.392 sections 1-3 -----	1-17