

19 RÉPUBLIQUE FRANÇAISE
INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE
COURBEVOIE

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

3 147 921

21 N° d'enregistrement national : 23 03600

51 Int Cl⁸ : H 04 L 9/32 (2023.01), H 04 L 9/30, G 06 F 21/33, 21/34

12 DEMANDE DE BREVET D'INVENTION

A1

22 Date de dépôt : 11.04.23.

30 Priorité :

43 Date de mise à la disposition du public de la demande : 18.10.24 Bulletin 24/42.

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

60 Références à d'autres documents nationaux apparentés :

Demande(s) d'extension : Polynésie-Fr

71 Demandeur(s) : IMPRIMERIE NATIONALE SA Société anonyme — FR.

72 Inventeur(s) : FLEURY Thomas et LION Stéphanie.

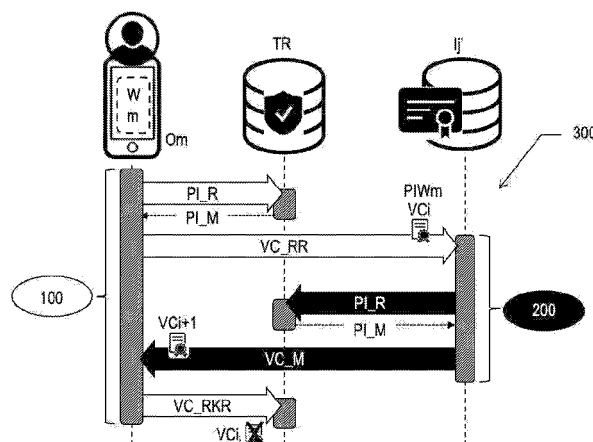
73 Titulaire(s) : IMPRIMERIE NATIONALE SA Société anonyme.

74 Mandataire(s) : MED'INVENT CONSULTING.

54 Procédé de renouvellement automatique d'un attribut vérifiable et système associé.

57 L'invention concerne un procédé (300) de renouvellement automatique d'un attribut vérifiable (VCi) mis en œuvre par un système de preuve en ligne comprenant un portefeuille (Wm) d'attributs vérifiables hébergé par un objet électronique (Om) et une entité émettrice d'attributs vérifiables. Un tel procédé (300) prévient la traçabilité de l'identité digitale du portefeuille et comporte deux sous-procédés (100, 200). Le premier (100) est mis en œuvre par ledit portefeuille (Wm) pour produire une nouvelle identité digitale (PIWm) et émettre une requête (VC_RR) en renouvellement d'un attribut vérifiable (VCi). Le second (200) est mis en œuvre par l'entité émettrice (Ij') pour produire un nouvel attribut vérifiable (VCi+1) en remplacement du précédent (VCi).

Figure à publier avec l'abrégié : Fig 3



FR 3 147 921 - A1



Description

Titre de l'invention : Procédé de renouvellement automatique d'un attribut vérifiable et système associé

- [0001] L'invention concerne le domaine de la vérification en ligne d'un attribut vérifiable, c'est-à-dire à force probatoire élevée, caractérisant une personne ou une entité. Plus précisément, l'invention adresse le problème de la preuve de majorité que toute personne se doit de présenter à un fournisseur de contenus numériques, de biens ou de services réservés aux adultes.
- [0002] L'invention sera décrite principalement, sans pour autant que cela engendre une quelconque limitation à la présente invention, dans le cadre de la preuve de majorité que doit fournir un sujet pour être autorisé à accéder à des contenus pour adulte. L'invention pourrait toutefois être exploitée pour attester de la véracité de tout autre attribut caractérisant une personne, comme une localité de résidence, l'obtention d'un niveau d'études sans qu'une souscription à un prestataire de biens ou de services exigeant une telle preuve oblige le souscripteur à une transmission d'éléments inutilement trop intimes ou précis.
- [0003] On peut en effet devoir prouver :
- que l'on est majeur sans nécessairement fournir sa date et son lieu de naissance ;
 - que l'on réside dans une ville ou région sans devoir communiquer son adresse complète ;
 - que l'on présente un certain niveau d'études sans pour autant préciser le ou les diplômes et années d'obtention de ceux-ci.
- [0004] En France, la Commission Nationale de l'Informatique et des Libertés, également connue sous l'acronyme « CNIL » préconise l'utilisation de systèmes qui ne soient pas facilement contournables sans pour autant que ces derniers ne soient trop intrusifs, afin qu'ils respectent la vie privée de chacune et chacun. La loi française, au même titre que d'autres règlements en vigueur dans le monde, soumet la fourniture de certains services ou biens à des conditions d'âge, obligeant les sites en ligne de fournisseurs de tels biens et services à une vérification de l'âge du client préalablement à toute fourniture. C'est par exemple le cas pour les sites de vente d'alcool, de jeux d'argent, de paris en ligne, de photos ou de vidéos pour adultes. Ladite CNIL préconise le recours à un tiers de confiance indépendant destiné à faire obstacle à la transmission directe de données identifiantes relatives à l'utilisateur à un site ou à une application proposant par exemple des contenus pornographiques. La CNIL, dans son avis du 3 juin 2021, recommande que le contrôle d'âge ou de majorité consiste en deux

opérations distinctes :

- l'émission d'une preuve de l'âge par un système sous la forme d'une entité informatique, que nous pourrions nommer par la suite « émetteur » ou « *Issuer* » selon une terminologie anglo-saxonne par mesure de simplification, ledit émetteur étant chargé de valider l'information sur l'âge de la personne et d'émettre une preuve d'âge (par exemple une preuve de majorité) assortie d'un niveau de confiance ;
- la transmission de ladite preuve de l'âge certifiée à un ou plusieurs fournisseurs de biens ou de services pour que ce dernier délivre ou refuse de délivrer lesdits biens ou services à l'internaute concerné par ladite preuve certifiée.

[0005] Pour préserver les données et la vie privée dudit internaute, une triple protection de la vie privée est exigée :

- l'émetteur d'une preuve de majorité connaît l'identité ou un pseudonyme de l'internaute concerné sans pour autant connaître le ou les fournisseurs de biens et de services exigeant une telle preuve de majorité certifiée ;
- la preuve de majorité est transmise audit fournisseur de biens et de services via ledit sujet ou internaute puis via une entité électronique dite « vérifieur » de preuve (« *verifier* » selon une expression anglo-saxonne), ci-après parfois nommée « vérifieur » par mesure de simplification ;
- le fournisseur de services ou de biens sollicité ne connaît pas l'identité de l'internaute mais seulement la majorité de celui-ci et le vérifieur de la preuve exigée.

[0006] L'exploitation d'un vérifieur indépendant est clairement recommandée par la CNIL pour protéger au mieux les données des personnes. De cette manière, les fournisseurs de biens ou de services soumis à une obligation de vérification d'âge ne réalisent pas eux-mêmes les opérations de vérification d'âge mais s'appuient sur un tiers de confiance chargé de ces opérations de vérification, reprenant ainsi le « triangle de la confiance » tel que défini dans l'approche connue sous l'appellation anglo-saxonne *Self-Sovereign Identity* ou SSI, popularisée avec l'émergence des technologies Web3, dont la blockchain.

[0007] La [Fig.1] illustre un exemple d'un système connu de vérification de la preuve de majorité d'un internaute désirant solliciter un fournisseur de contenus numériques réservés aux adultes (contenus pour adultes, jeux d'argent ou paris en ligne, par exemple).

[0008] Selon ladite [Fig.1], un système S comporte un objet électronique Om détenu par une personne Um désirant solliciter un fournisseur de biens ou de services SP, en l'espèce des contenus multimédia à caractère pornographique. Ledit objet électronique Om peut

consister en un téléphone mobile intelligent (« *smartphone* » selon une terminologie anglo-saxonne), une tablette électronique, un ordinateur personnel ou tout autre objet électronique adapté. Un tel fournisseur SP étant soumis à une vérification de la majorité de tout client, il s'appuie sur un vérifieur Vn pour attester ou non d'une telle majorité. Un tel vérifieur, sous la forme d'un serveur informatique, transmet une confirmation ou un rejet de la preuve de majorité au fournisseur SP par la transmission d'un message de vérification V_M. Pour ce faire, un tel vérifieur Vn exploite un ensemble structuré de données VC définissant un attribut certifié et vérifiable (« *verifiable credential* » selon une terminologie anglo-saxonne) véhiculé par un message de présentation PV_M (« *verifiable presentation* » selon une terminologie anglo-saxonne) émanant du dispositif électronique Om utilisé par la personne Um en réponse à une requête en présentation d'un tel attribut vérifiable VC_PR adressée par le vérifieur Vn à l'objet électronique Om.

[0009] Cette structure de données que nous nommerons « attribut vérifiable » VC comprend une pluralité d'informations en lien avec la personne concernée par la preuve, l'attribut attesté, l'entité émettrice Ij ayant constitué et émis ledit attribut vérifiable VC, voire des éléments contextuels d'exploitation Ctx, parmi lesquels une date de création ou d'émission CD, une date de fin de validité, EVD, etc. Un tel attribut vérifiable VC est généralement stocké dans la mémoire M de l'objet électronique Om. Il est administré par un portefeuille électronique Wm (« *wallet* » selon une terminologie anglo-saxonne) d'attributs vérifiables sous la forme d'une application ou, plus généralement, d'un programme d'ordinateur, dont les instructions de programme sont enregistrées dans la mémoire M de l'objet électronique Om. Par mesure de simplification, un tel portefeuille électronique Wm d'attributs vérifiables pourra être nommé « portefeuille » dans la suite de ce document. Ainsi, ledit portefeuille Wm peut décoder une requête en présentation VC_PR et émettre en réponse un message de présentation PV_M.

[0010] Un tel attribut vérifiable VC est généralement créé et émis par une entité électronique Ij, que nous pourrions nommer « émetteur » par mesure de simplification. Un tel émetteur Ij peut consister en un serveur informatique apte à recevoir une requête VC_CR en création d'un attribut vérifiable initiée par le portefeuille électronique Wm et transmise par l'objet électronique Om.

[0011] A réception d'une telle requête en création VC_CR, l'émetteur Ij sollicite un tiers ou autorité de confiance TA qui dispose d'une connaissance précise de l'utilisateur Um. Une telle autorité de confiance TA peut consister en un établissement bancaire, une administration publique ou privée, voire en un service opéré par un tel établissement ou administration. Nous pouvons par exemple citer le service « Live Identity » opéré par Orange Business Service. Un tel service est ouvert à tout opérateur de téléphonie mobile et permet de vérifier l'identité digitale d'un abonné. Une telle autorité de

confiance TA pourrait également consister en un serveur informatique opéré par un fournisseur d'énergie ayant connaissance de ses usagers. En réponse à une requête en création d'un attribut vérifiable, l'émetteur Ij sollicite une investigation CUI auprès d'un tel tiers ou autorité TA pour déterminer, par exemple, si ledit utilisateur Um est majeur ou bien s'il réside dans telle ou telle localité, selon l'attribut vérifiable concerné. En l'espèce, dans l'exemple décrit en liaison avec la [Fig.1], l'autorité TA sous la forme d'un serveur bancaire, connaissant la date de naissance de son client Um, peut remonter à l'émetteur une information confirmant ou réfutant la majorité de l'utilisateur Um. Dans l'affirmative, l'émetteur Ij élabore l'attribut vérifiable VC. Pour que l'autorité TA puisse répondre favorablement ou défavorablement audit émetteur Ij, l'investigation CUI peut consister en une requête véhiculant des informations publiques de l'identité digitale du sujet Um. Pour faire un lien entre le pseudonyme constitué par de telles informations publiques et un client ou abonné en tant que tel, l'autorité TA peut soumettre au portefeuille Wm, une requête en connaissance d'une information caractérisant le compte bancaire ou l'abonnement téléphonique du sujet utilisateur de l'objet électronique Om auprès de l'autorité TA ainsi que le consentement de l'utilisateur dudit objet électronique Om. En réponse à une telle requête, après sollicitation de l'utilisateur Um pour confirmer sa demande d'attribut vérifiable, ledit portefeuille Wm retourne l'information de compte bancaire ou d'abonnement signée à l'autorité TA qui peut en vérifier l'authenticité et élaborer la réponse à l'émetteur Ij qui ignore tout de ladite information caractérisant l'abonnement téléphonique ou le compte bancaire du porteur de l'objet Om. En variante, une telle requête en connaissance d'une information caractérisant le compte bancaire de l'utilisateur Um peut consister en une transaction bancaire d'un montant débité nul ou toute autre solution adaptée.

[0012] A titre d'exemple, comme l'indique la [Fig.1], un attribut vérifiable émis VC comporte des informations contextuelles Ctx, par exemple décrivant le schéma cryptographique exploité pour signer ledit attribut préalablement à son émission à destination du portefeuille Wm. Un tel attribut vérifiable VC peut également comporter des informations publiques d'identités digitales (identifiant unique, clé cryptographique publique, etc.) respectivement de l'utilisateur Um et de l'émetteur Ij, une date de création dudit attribut vérifiable, voire une date de fin de validité de ce dernier. Un tel attribut vérifiable VC pourrait contenir toute autre information nécessaire à la mise en œuvre du système de preuve en ligne S. L'émetteur Ij élabore et envoie un message VC_M pour transmettre ledit attribut vérifiable VC au portefeuille Wm via l'objet électronique Om.

[0013] Le système de preuve en ligne S peut comporter une pluralité d'émetteurs, de vérificateurs et de portefeuilles d'attributs vérifiables. Pour distinguer les entités élec-

troniques et informatiques les unes des autres, celles-ci sont associées à des informations d'identité digitales. Ainsi, le portefeuille W_m est associé à un identifiant unique IDW_m , l'émetteur I_j à un identifiant unique IDI_j et le vérifieur V_n à un identifiant unique IDV_n . Pour certifier que les messages ou contenus sont bien émis par une première entité à destination d'une deuxième entité, un système de preuve en ligne S s'appuie généralement sur un schéma cryptographique de signature/vérification asymétrique. Ainsi, chaque entité comporte un jeu de clés respectivement publique PK et privée SK . Les clés publiques sont symbolisées par des clés de couleur blanche sur la [Fig.1] et les clés privées sont symbolisées par des clés de couleur noire.

- [0014] Un couple de clés publique PK_x et privée SK_x d'une première entité électronique X est telle qu'une deuxième entité Y peut vérifier la signature de l'entité X en connaissant la clé publique PK_x si ladite signature a été élaborée par la première entité X à l'aide de la clé privée SK_x . En variante ou en complément, un message émis par l'entité X et adressé à l'entité Y peut également être chiffré de sorte que seule l'entité Y puisse lire ledit message. Dans ce cas, l'entité Y comporte également un couple de clés privée SK_y et publique PK_y . Connaissant la clé publique PK_y , l'entité X peut chiffrer le message à l'aide de ladite clé publique PK_y . Seule l'entité connaissant la clé privée SK_y (en l'espèce, l'entité Y) pourra décoder ledit message chiffré en exploitant ladite clé privée SK_y et obtenir le clair dudit message chiffré.
- [0015] En liaison avec la [Fig.1], l'identité digitale de chaque entité comporte, outre un identifiant unique, un tel jeu de clés publique et privée qui est propre à ladite entité. Sur la [Fig.1], l'identité digitale II_j de l'émetteur I_j comporte l'identifiant IDI_j , la clé publique PKI_j et la clé privée SKI_j . L'identité digitale IW_m du portefeuille W_m comporte l'identifiant IDW_m , la clé publique PKW_m et la clé privée SKW_m . L'identité digitale IV_n du vérifieur V_n comporte l'identifiant IDV_n , la clé publique PKV_n et la clé privée SKV_n .
- [0016] Ainsi, chaque entité électronique du système de preuve en ligne S dont fait partie le portefeuille W_m est associée à une identité digitale formée d'une identité digitale publique et d'une identité digitale privée, ladite identité digitale étant enregistrée dans une mémoire M de chaque entité électronique. Un message, une requête ou un contenu peut être signé par une première entité électronique à l'aide de son identité digitale privée, ladite signature pouvant être vérifiée par toute deuxième entité électronique en exploitant l'identité digitale publique de ladite première entité électronique. Éventuellement, ladite première entité peut chiffrer messages, requêtes ou contenus à l'aide de l'identité digitale publique d'une deuxième entité électronique déterminée, de sorte que cette dernière soit la seule entité électronique capable de déchiffrer lesdits messages, requêtes ou contenus à l'aide de sa propre identité digitale privée inconnue des autres entités électroniques.

- [0017] Ainsi, l'identité digitale IW_m du portefeuille W_m consiste en :
- une identité digitale publique PIW_m , en l'espèce un identifiant unique IDW_m et une clé publique PKW_m ;
 - une identité digitale privée, en l'espèce une clé privée SKW_m conjointement élaborée avec ladite clé publique PKW_m pour assurer un schéma cryptographique de signature asymétrique.
- [0018] L'identité digitale II_j de l'émetteur I_j de l'attribut VC_i , objet d'un renouvellement automatique consiste en :
- une identité digitale publique PII_j , en l'espèce un identifiant unique IDI_j et une clé publique PKI_j ;
 - une identité digitale privée, en l'espèce une clé privée SKI_j conjointement élaborée avec ladite clé publique PKI_j pour assurer un schéma cryptographique de signature asymétrique.
- [0019] Il en serait de même pour un deuxième émetteur I_j' (non représenté sur la [Fig.1]) distinct de l'émetteur I_j . Ainsi, l'identité digitale II_j' d'un tel émetteur I_j' consisterait en :
- une identité digitale publique PII_j' , en l'espèce un identifiant unique IDI_j' et une clé publique PKI_j' ;
 - une identité digitale privée, en l'espèce une clé privée SKI_j' conjointement élaborée avec ladite clé publique PKI_j' pour assurer un schéma cryptographique de signature asymétrique.
- [0020] Selon l'exemple de la [Fig.1], afin que les entités électroniques du système de preuve en ligne S puissent connaître les identités digitales publiques PI (i.e. les clés publiques PK , voire les identifiants ID desdites entités), ledit système S comporte un registre de confiance TR , sous la forme d'un serveur informatique associé lui-même à une identité digitale ITR dont l'identité digitale publique consiste en un identifiant unique $IDTR$ et une clé publique $PKTR$ et dont l'identité privée consiste en une clé privée $SKTR$. Ledit registre de confiance TR comporte une mémoire de données TRM comprenant un répertoire des identités digitales publiques des entités I_j , V_n , W_m dudit système S , voire celles de l'autorité TA et/ou du fournisseur de services SP . Toutes les entités électroniques du système de preuve en ligne S (notamment les émetteurs, vérificateurs et portefeuilles) peuvent ainsi solliciter ledit registre de confiance TR par des requêtes en consultation d'identités digitales publiques PI_R pour connaître en réponse, via un message de transmission PI_M une ou plusieurs identités digitales publiques (i.e. les valeurs des identifiants uniques IDV_n , IDI_j , IDW_m et/ou des clés publiques PKI_j , PKW_m , PKV_n) d'entités électroniques déterminées et ainsi pouvoir vérifier les signatures des requêtes VC_PR , VC_CR , PI_R et des messages VC_M , PV_M , voire pour chiffrer, si nécessaire, lesdites requêtes et lesdits messages. Le registre de

confiance TR est ainsi un référentiel, à date, des entités électroniques légitimes composant ledit système de preuve en ligne S. Une requête PI_R peut être signée à l'aide de l'identité digitale privée (en l'espèce une clé privée) de l'entité requérante. Ledit registre de confiance TR peut ainsi vérifier ladite signature en utilisant l'identité digitale publique (en l'espèce une clé publique) de l'entité requérante et s'assurer que celle-ci dispose bien d'une entrée dans son référentiel des entités électroniques légitimes du système S. Le message PI_M véhiculant le résultat d'une requête PI_R peut, à son tour, être signé par le registre de confiance TR en exploitant sa propre identité digitale privée (clé privée SKTR) avant émission.

- [0021] Une exploitation incontrôlée ou non maîtrisée d'identifiants uniques indépendants, tels qu'exprimés précédemment, généralement repris en clair dans des métadonnées, peut poser des problèmes de confidentialité et de traçabilité. De tels identifiants peuvent parfois même être monétisés pour des ciblage publicitaires par exemple. Aussi, le schéma cryptographique retenu pour produire les identités digitales (identifiants et clés cryptographiques) desdites entités et assurer les échanges entre celles-ci, peut être avantageusement choisi pour utiliser des identifiants sécurisés dits « identifiants décentralisés » ou DIDs (acronyme anglo-saxon de « *Decentralized Identifiers* ») en lieu et place d'identifiants uniques indépendants des clés publiques et privées. Les identités digitales des entités électroniques du système de preuve en ligne S peuvent alors s'exprimer sous la forme d'identifiants ID décentralisés et sécurisés (DIDs), créés par lesdites entités pour garantir leurs authentifications et signatures. Selon les algorithmes exploités pour générer de tels identifiants sécurisés, il est ainsi possible de réduire l'identité digitale publique à un tel identifiant décentralisé ou à la seule clé publique d'une entité électronique, une relation bijective existant entre ladite clé publique et un tel identifiant décentralisé. En quelque sorte, un identifiant décentralisé est hérité ou dérivé de la clé publique qui lui est associée. Ainsi, connaissant l'identifiant (sous la forme d'un DID) d'une première entité, une deuxième entité peut recouvrer la clé publique PK de ladite première entité à partir de l'identifiant décentralisé ou réciproquement. Le registre de confiance TR peut ainsi stocker dans la mémoire de données TRM, les seuls identifiants IDI_j, IDV_n, IDW_m, sous la forme d'identifiants décentralisés DIDs, ou bien les seules clés publiques PKI_j, PKV_n, PKW_m en lieu et place de couples [identifiants clairs et clés publiques] pour répertorier les identités digitales publiques des entités du système de preuve en ligne S. De la même manière, un attribut vérifiable VC peut ne comporter que l'identifiant IDI_j de l'émetteur I_j, lorsque ledit identifiant est un identifiant décentralisé ou en variante la seule clé publique PKI_j de ce dernier, lorsque ledit identifiant IDI_j est hérité de ladite clé publiques PKI_j. Il en est de même, pour l'identité digitale publique IWM=[IDW_m,PKW_m] du portefeuille W_m qui est incluse dans ledit attribut vérifiable

VC.

- [0022] Comme l'indique la [Fig.1], le système de preuve en ligne S comporte une pluralité d'entités électroniques en l'espèce des objets électroniques Om, des émetteurs Ij, des vérificateurs Vn, un registre de confiance TR, etc. De manière classique et comme l'illustre de manière simplifiée la [Fig.2], chacune desdites entités électroniques consiste en une instance d'un objet électronique ou d'un serveur informatique comportant une unité centrale de traitement 11 commandant, par des signaux acheminés par un bus de communication symbolisé sur la [Fig.2] par des doubles flèches en traits simples, des éléments électroniques dont une mémoire M. Cette dernière comprend une mémoire de données 12 et une mémoire de programmes 13, lesdites mémoires 12 et 13 pouvant ne former qu'une seule et même entité physique M.
- [0023] On entend par « mémoire » toute mémoire informatique qu'elle soit volatile ou non. Une mémoire non volatile est une mémoire informatique dont la technologie conserve ses données en l'absence d'une alimentation en énergie électrique. Elle peut contenir des données résultant de saisies, de calculs, de mesures et/ou des instructions de programmes. Les principales mémoires non volatiles actuellement disponibles sont inscriptibles électriquement telles que la technologie EPROM (« *Erasable Programmable Read-Only Memory* », selon une terminologie anglo-saxonne) ou encore inscriptibles et effaçables électriquement telles que les technologies EEPROM (« *Electrically-Erasable Programmable Read-Only Memory* », selon une terminologie anglo-saxonne), flash, SSD (« *Solid-State Drive* », selon une terminologie anglo-saxonne), etc. Les mémoires non volatiles se distinguent des mémoires dites « volatiles » dont les données sont perdues en l'absence d'une alimentation électrique. Les principales mémoires volatiles actuellement disponibles exploitent les technologies RAM (« *Random Access Memory* » selon une terminologie anglo-saxonne ou encore nommée « mémoire vive »), DRAM (mémoire vive dynamique, nécessitant une réactualisation régulière), SRAM (mémoire vive statique nécessitant une telle réactualisation lors d'une sous-alimentation électrique), DPRAM ou VRAM (particulièrement adaptées à la vidéo), etc.
- [0024] Selon la [Fig.2], une entité électronique d'un système de preuve en ligne comporte en outre des moyens de communication 14 avec le monde extérieur sous la forme d'une unité d'entrée et une unité de sortie. Lesdits moyens de communication 14 coopèrent avec l'unité de traitement 11 et assurent une communication de proximité sans fil ou filaire avec toute autre entité électronique dudit système S. Pour fonctionner, une telle entité électronique comporte généralement une source d'énergie électrique 15, externe ou interne sous la forme d'une ou plusieurs batteries par exemple. L'unité de traitement 11 peut également comporter des moyens de pilotage 16 d'une interface

homme-machine d'entrée et/ou de sortie 17. On entend par « interface homme-machine de sortie », tout dispositif, employé seul ou en combinaison, permettant de sortir ou délivrer une représentation graphique, haptique, sonore ou, plus généralement, perceptible par l'humain. Une telle interface homme-machine de sortie peut consister de manière non exhaustive en un ou plusieurs écrans, haut-parleurs ou autres moyens alternatifs adaptés. On entend par « interface homme-machine d'entrée », un clavier informatique, un dispositif de pointage, un écran tactile, un microphone ou, plus généralement, toute interface agencée pour traduire une gestuelle ou une consigne émise par un humain en données de commande ou de paramétrage. Avantageusement, les interfaces homme-machine d'entrée et de sortie peuvent ne constituer qu'une seule et même entité physique.

- [0025] Un tel système de preuve en ligne S peut être adapté en chargeant dans la mémoire de programmes 13 de chaque entité électronique un programme d'ordinateur P comportant des instructions pour provoquer, lors de leurs exécutions, la mise en œuvre d'un procédé idoine. Ce programme peut utiliser n'importe quel langage de programmation, et se présenter sous la forme de code source, code objet, ou de code intermédiaire entre code source et code objet, tel que dans une forme interprétée, partiellement ou entièrement compilée, ou sous n'importe quelle autre forme souhaitable.
- [0026] L'exploitation de pseudonymes (identifiants / clés publiques) en lieu et place d'informations identifiantes des internautes limite la traçabilité de ces dernières, notamment par l'emploi d'identifiants centralisés (DIDs). Toutefois, ces derniers demeurent traçables au gré des requêtes en présentations ou de créations d'attributs vérifiables.
- [0027] L'invention permet de résoudre les inconvénients précédemment exprimés. Parmi les nombreux avantages procurés par la mise en œuvre de l'invention, nous pouvons mentionner que :
- l'invention conserve l'anonymat du porteur ou utilisateur d'un objet électronique hébergeant un portefeuille d'attributs vérifiables et limite, voire prévient, toute traçabilité des identités digitales publiques de l'utilisateur et/ou de son objet électronique mettant en œuvre le portefeuille d'attributs vérifiables, sans que cela nécessite une action dudit utilisateur ou alourdisse la tâche de ce dernier ;
 - les attributs vérifiables émis ou réémis selon l'invention le sont par des émetteurs légitimes puisque connus du registre de confiance, limitant le risque que certains attributs vérifiables en cours de validité ne prospèrent alors qu'un émetteur d'attributs vérifiables a pu être révoqué ou supprimé du système de preuve en ligne ;
 - l'invention s'intègre parfaitement dans un système de preuve en ligne selon

l'état de l'art ([Fig.1]) offrant ainsi une garantie en matière d'interopérabilité ; la mise en œuvre de l'invention ne nécessite en effet qu'une mise à jour de portefeuilles d'attributs vérifiables et celle de certains émetteurs ou l'apport d'émetteurs spécifiques sans remettre en cause ou modifier le principe de la création d'attributs vérifiables, de présentations de ces derniers auprès d'entités vérifieurs en vue de l'obtention de contenus ou de biens et services.

[0028] A cette fin, l'invention prévoit un procédé de renouvellement automatique d'un attribut d'un utilisateur vérifiable par une entité électronique vérificatrice d'un système de preuve en ligne, un tel système comportant une pluralité d'entités électroniques respectivement agencées pour communiquer les unes avec les autres au sein dudit système dont, outre ladite entité électronique vérificatrice, un portefeuille d'attributs vérifiables mis en œuvre par une unité de traitement d'un objet électronique détenu par un utilisateur, une entité électronique émettrice d'attributs vérifiables, tout attribut vérifiable émis ayant été préalablement élaboré et transmis par une entité électronique émettrice dudit système de preuve en ligne en réponse à une requête en création d'attribut vérifiable initiée par un portefeuille d'attributs vérifiables dudit système. Pour préserver l'anonymat et prévenir la traçabilité de l'identité digitale publique de l'utilisateur, un tel procédé de renouvellement automatique comporte :

- un premier sous-procédé, mis en œuvre par un portefeuille d'attributs vérifiables, comprenant :
 - une étape de détection d'un événement déclencheur d'un renouvellement d'un attribut vérifiable d'ores et déjà émis ;
 - une étape d'élaboration et de déclenchement de l'émission d'une requête en renouvellement d'un attribut vérifiable d'ores et déjà émis, à destination d'une entité électronique émettrice du système de preuve en ligne ;
 - une étape de gestion d'un nouvel attribut vérifiable fruit d'une telle requête en renouvellement et transmis par ladite entité émettrice ;
- un deuxième sous-procédé mis en œuvre par une unité de traitement d'une entité émettrice comprenant :
 - une étape de traitement d'une requête en renouvellement d'un attribut vérifiable d'ores et déjà émis, transmise par un portefeuille d'attributs vérifiables ;
 - une étape de renouvellement d'un tel attribut vérifiable d'ores et déjà émis et de transmission d'un nouvel attribut vérifiable à destination du portefeuille d'attributs vérifiables requérant ledit renouvellement d'attribut vérifiable d'ores et déjà émis.

[0029] Un tel système de preuve en ligne pouvant comporter de nombreuses entités élec-

troniques, chaque entité électronique dudit système de preuve en ligne peut avantageusement être associée à une identité digitale formée d'une partie publique, dite « identité digitale publique » et d'une partie privée), dite « identité digitale privée », ladite identité digitale étant enregistrée dans une mémoire de données de ladite chaque entité électronique. Ledit système de preuve en ligne comprend alors un registre de confiance agencé pour :

- enregistrer, dans une mémoire de données, les identités digitales publiques respectives des entités électroniques dudit système de preuve en ligne ;
- recevoir une requête en consultation d'identités digitales publiques émanant d'une entité électronique dudit système ;
- élaborer un message de transmission véhiculant une ou plusieurs identités digitales publiques et émettre un tel message à destination de l'entité électronique émettrice de ladite requête en consultation d'identités digitales publiques.

[0030] Le premier sous-procédé d'un procédé conforme à l'invention peut alors être agencé de sorte que :

- l'étape de gestion d'un nouvel attribut vérifiable fruit d'une telle requête en renouvellement comporte :
 - une étape de vérification de la signature du nouvel attribut vérifiable par l'entité émettrice de ce dernier, à l'aide de l'identité digitale publique de ladite entité électronique émettrice ;
 - une étape d'enregistrement du nouvel attribut vérifiable, dans une mémoire de données accessible en lecture et en écriture par le portefeuille d'attributs vérifiables, en remplacement de l'attribut vérifiable renouvelé si et seulement si ladite étape de vérification de la signature du nouvel attribut vérifiable confirme l'authenticité de ladite signature ;

[0031] Le deuxième sous-procédé peut, quant à lui, être agencé de sorte que :

- l'étape de traitement d'une requête en renouvellement d'un attribut vérifiable d'ores et déjà émis comporte :
 - une étape de réception d'une telle requête en renouvellement et de lecture des informations véhiculées par cette dernière parmi lesquelles l'attribut vérifiable d'ores et déjà émis et l'identité digitale publique du portefeuille d'attributs vérifiables, respectivement objet et émetteur de ladite requête en renouvellement ;
 - une étape de vérification de la signature de l'attribut vérifiable à renouveler par l'entité électronique émettrice de ce dernier, à l'aide de l'identité digitale publique de cette dernière ;

- l'étape de renouvellement d'un attribut vérifiable d'ores et déjà émis et de transmission d'un nouvel attribut vérifiable :
 - n'est mise œuvre que si ladite étape de vérification de la signature de l'attribut vérifiable à renouveler confirme l'authenticité de cette dernière ;
 - comporte une étape :
 - d'élaboration du nouvel attribut vérifiable consistant en la copie de l'intégralité des informations contenues dans l'attribut vérifiable à renouveler exception faite des informations en lien avec l'élaboration en tant que telle de ce dernier ;
 - de signature dudit nouvel attribut vérifiable à l'aide de l'identité digitale privée de l'entité émettrice dudit nouvel attribut vérifiable ;
 - comporte une étape pour provoquer l'émission du nouvel attribut vérifiable à destination du portefeuille d'attributs vérifiables requérant le renouvellement.

[0032] De manière avantageuse, le premier sous-procédé d'un procédé de renouvellement automatique selon l'invention peut être agencé de sorte que l'étape d'élaboration et de déclenchement de l'émission d'une requête en renouvellement puisse comporter une étape de signature de ladite requête en renouvellement à l'aide de l'identité digitale privée du portefeuille d'attributs vérifiables. Dans ce cas, le deuxième sous-procédé peut être agencé de sorte que :

- l'étape de traitement d'une requête en renouvellement d'un attribut vérifiable d'ores et déjà émis comporte une étape de vérification de la signature de ladite requête en renouvellement par le portefeuille d'attributs vérifiables, à l'aide de l'identité digitale publique de ce dernier ;
- l'étape de renouvellement d'un attribut vérifiable d'ores et déjà émis et de transmission d'un nouvel attribut vérifiable n'est mise œuvre que si ladite étape de signature de la requête en renouvellement confirme l'authenticité de ladite signature.

[0033] Pour provoquer à bon escient et de manière automatique une mise en œuvre d'un procédé de renouvellement automatique d'un attribut conforme à l'invention, le premier sous-procédé de ce dernier peut être agencé de sorte que l'étape de détection d'un événement déclencheur d'un renouvellement automatique d'un attribut vérifiable puisse consister en :

- une lecture, dans une mémoire de données accessible en lecture et écriture par le portefeuille d'attributs vérifiables, la valeur d'un compteur de messages de

présentation véhiculant l'attribut vérifiable adressés à une entité électronique vérificatrice du système de preuve en ligne ;

- une comparaison de la valeur courante dudit compteur à un seuil maximal prédéterminé et une conclusion quant à la détection d'un événement déclencheur d'un renouvellement automatique si ladite valeur dudit compteur atteint ledit seuil prédéterminé.

[0034] Dans ce cas, ledit premier sous-procédé peut en outre être agencé de sorte que l'étape de gestion d'un nouvel attribut vérifiable fruit d'une requête en renouvellement puisse également consister en une initialisation de la valeur d'un compteur de messages de présentation véhiculant ledit nouvel attribut vérifiable dans une mémoire de données accessible en lecture et en écriture par le portefeuille d'attributs vérifiables.

[0035] Selon un mode de réalisation avantageux, lorsque le système de preuve en ligne comporte un registre de confiance, l'étape d'élaboration et de déclenchement de l'émission d'une requête en renouvellement d'un attribut vérifiable d'ores et déjà émis du premier sous-procédé peut comporter :

- une étape d'élaboration d'une requête en consultation d'identités digitales publiques d'entités émettrices du système de preuve en ligne et de déclenchement de l'émission de ladite requête à destination du registre de confiance ;
- une étape de réception d'un message de transmission émanant dudit registre de confiance et de lecture au sein de celui-ci d'une identité digitale publique d'entité émettrice véhiculée par ledit message ;
- une étape de production d'une nouvelle identité digitale du portefeuille d'attributs vérifiables en remplacement de la précédente ;
- une étape d'élaboration de la requête en renouvellement de l'attribut vérifiable d'ores et déjà émis à destination de l'entité émettrice dont l'identité digitale publique a été lue dans le message de transmission émanant dudit registre de confiance, ladite requête en renouvellement comportant l'attribut vérifiable à renouveler et la nouvelle identité digitale publique du portefeuille d'attributs vérifiables.

[0036] Selon ce mode de réalisation avantageux, afin de rendre accessible une telle nouvelle identité digitale publique du portefeuille d'attributs vérifiables aux autres entités électroniques du système de preuve en ligne, l'étape de production d'une nouvelle identité digitale du portefeuille d'attributs vérifiables peut consister en outre à élaborer une requête en mise à jour d'identité digitale publique à destination du registre de confiance, ladite requête véhiculant la nouvelle identité digitale publique issue de la nouvelle identité digitale signée à l'aide de la précédente identité digitale privée dudit portefeuille d'attributs vérifiables.

- [0037] Pour prévenir toute constitution, par une entité électronique émettrice malveillante ou susceptible d'être la cible d'une attaque malveillante à dessein, d'un historique d'émissions d'attributs vérifiables d'un portefeuille d'attributs vérifiables, et donc *in fine* de l'internaute porteur de l'objet électronique qui héberge ledit portefeuille, l'étape de réception d'un message de transmission émanant du registre de confiance et de lecture au sein de celui-ci d'une identité digitale publique d'entité électronique émettrice véhiculée par ledit message peut consister en la sélection d'une identité digitale publique d'entité émettrice distincte de celle de l'entité électronique émettrice ayant émis l'attribut vérifiable à renouveler.
- [0038] L'invention permet de prévenir toute exploitation future d'une instance antérieure d'un attribut vérifiable qui a fait l'objet d'un renouvellement, ladite instance antérieure pouvant faire l'objet d'une révocation publique au sein du système de preuve en ligne. Pour cela :
- le registre de confiance peut être agencé pour mémoriser tout attribut vérifiable révoqué ou une information caractéristique d'un tel attribut vérifiable révoqué en réponse à la réception d'une requête en révocation d'attribut vérifiable ;
 - l'étape de gestion d'un nouvel attribut vérifiable fruit d'une requête en renouvellement peut comporter une étape d'élaboration d'une telle requête en révocation d'attribut vérifiable véhiculant l'attribut vérifiable ayant fait l'objet d'un renouvellement à destination du registre de confiance ou une information caractéristique de ce dernier.
- [0039] Selon ce dernier mode de réalisation avantageux, afin de prévenir toute révocation illégitime, l'étape d'élaboration d'une telle requête en révocation peut consister en outre à signer ladite requête à l'aide de l'identité digitale privée dudit portefeuille d'attributs vérifiables.
- [0040] Selon un mode de réalisation avantageux, l'étape de vérification de la signature de l'attribut vérifiable à renouveler du deuxième sous-procédé peut à son tour être précédée :
- d'une étape d'élaboration d'une requête en consultation d'identités digitales publiques d'entités électroniques du système de preuve en ligne et de déclenchement de l'émission de ladite requête à destination du registre de confiance ;
 - d'une étape de réception d'un message de transmission émanant dudit registre de confiance et de recherche, au sein de celui-ci, de l'identité digitale publique de l'entité électronique émettrice de l'attribut vérifiable à renouveler.
- [0041] De la même manière, l'étape de vérification de la signature de la requête en renouvellement par le portefeuille d'attributs vérifiables du deuxième sous-procédé peut être

avantageusement précédée :

- d'une étape d'élaboration d'une requête en consultation d'identités digitales publiques d'entités électroniques du système de preuve en ligne et de déclenchement de l'émission de ladite requête à destination du registre de confiance ;
- d'une étape de réception d'un message de transmission émanant dudit registre de confiance et de recherche, au sein de celui-ci, de l'identité digitale publique du portefeuille d'attributs vérifiables.

[0042] Selon un mode d'application préféré, l'attribut vérifiable pouvant faire l'objet d'un processus de renouvellement selon l'invention peut caractériser la majorité de l'utilisateur de l'objet électronique hébergeant le portefeuille d'attributs vérifiables.

[0043] Selon un mode de réalisation préféré, pour chaque entité électronique d'un système de preuve en ligne adapté selon l'invention :

- l'identité digitale publique peut consister en une clé publique et un identifiant ;
- l'identité digitale privée consiste en une clé privée produite conjointement avec ladite clé publique, par la mise en œuvre d'un algorithme cryptographique asymétrique.

[0044] Pour chaque entité électronique d'un tel système, l'identifiant peut être un identifiant décentralisé dérivé de ladite clé publique par la mise en œuvre d'un algorithme cryptographique réversible, ladite identité digitale publique se réduisant ainsi en ledit identifiant décentralisé ou en ladite clé publique.

[0045] Pour adapter un système de preuve en ligne connu de sorte qu'il préserve l'anonymat des utilisateurs et préserve toute traçabilité des activités respectives de ces derniers, l'invention concerne en outre un premier produit programme d'ordinateur comportant une ou plusieurs instructions de programme exécutables par une unité de traitement d'un objet électronique hébergeant un portefeuille d'attributs vérifiables d'un système de preuve en ligne, lesdites instructions de programme étant :

- chargeables dans une mémoire dudit objet électronique hébergeant un portefeuille d'attributs vérifiables ;
- conçues de sorte que leur exécution par ladite unité de traitement provoque la mise en œuvre par ledit portefeuille d'attributs vérifiables d'un premier sous-procédé d'un procédé de renouvellement automatique d'un attribut vérifiable selon l'invention.

[0046] L'invention concerne alors également :

- un support de mémorisation lisible par un ordinateur comportant les instructions d'un tel premier produit programme d'ordinateur ;
- un objet électronique comportant une unité de traitement, des moyens de com-

munication avec le monde extérieur et une mémoire enregistrant les instructions de programme d'un tel premier produit programme d'ordinateur.

[0047] Pour adapter un système de preuve en ligne connu de sorte qu'il préserve l'anonymat des utilisateurs et préserve toute traçabilité des activités respectives de ces derniers, l'invention concerne en outre un deuxième produit programme d'ordinateur comportant une ou plusieurs instructions de programme exécutables par une unité de traitement d'une entité électronique émettrice d'attributs vérifiables d'un système de preuve en ligne, lesdites instructions de programme étant :

- chargeables dans une mémoire de ladite entité électronique émettrice ;
- conçues de sorte que leur exécution par ladite unité de traitement provoque la mise en œuvre d'un deuxième sous-procédé d'un procédé de renouvellement automatique d'un attribut vérifiable selon l'invention.

[0048] L'invention concerne alors également :

- un support de mémorisation lisible par un ordinateur comportant les instructions d'un tel deuxième produit programme d'ordinateur ;
- une entité électronique émettrice d'attributs vérifiables comportant une unité de traitement, des moyens de communication avec le monde extérieur et une mémoire enregistrant les instructions de programme d'un tel deuxième produit programme d'ordinateur.

[0049] Enfin, l'invention concerne tout système de preuve en ligne comportant une pluralité d'entités électroniques respectivement agencées pour communiquer les unes avec les autres au sein dudit système dont :

- une entité électronique vérificatrice d'attributs vérifiables ;
- un portefeuille d'attributs vérifiables mis en œuvre par une unité de traitement d'un objet électronique détenu par un utilisateur, ledit objet électronique étant agencé selon l'invention et tel qu'exprimé précédemment ;
- une entité électronique émettrice d'attributs vérifiables agencée selon l'invention et tel qu'exprimé précédemment.

[0050] D'autres caractéristiques et avantages apparaîtront plus clairement à la lecture de la description qui suit et à l'examen des figures qui l'accompagnent parmi lesquelles :

[0051] [Fig.1], d'ores et déjà décrite, illustre un exemple d'un système de preuve en ligne d'attributs vérifiables selon l'état de l'art ;

[0052] [Fig.2], d'ores et déjà décrite, illustre un exemple d'architecture fonctionnelle de toute entité électronique formant ledit système de preuve en ligne selon la [Fig.1] ;

[0053] [Fig.3] illustre un exemple d'un procédé de renouvellement automatique d'attributs vérifiables conforme à l'invention et mis en œuvre par un système de preuve en ligne d'attributs vérifiables ;

[0054] [Fig.4] illustre un organigramme fonctionnel d'un premier sous-procédé d'un

procédé de renouvellement automatique d'attributs vérifiables conforme à l'invention et décrit par la [Fig.3], ledit premier sous-procédé étant destiné à être mis en œuvre par un portefeuille d'attributs vérifiables d'un système de preuve en ligne tel que celui illustré par la [Fig.1] ;

[0055] [Fig.5] illustre un organigramme fonctionnel d'un deuxième sous-procédé d'un procédé de renouvellement automatique d'attributs vérifiables conforme à l'invention et décrit par la [Fig.3], ledit deuxième sous-procédé étant destiné à être mis en œuvre par une entité électronique émettrice d'attributs vérifiables d'un système de preuve en ligne illustré par la [Fig.1].

[0056] La [Fig.3] illustre ainsi un procédé 300 de renouvellement automatique d'un attribut vérifiable VCi, destiné à être vérifié par un vérifieur Vn d'un système de preuve en ligne S selon la [Fig.1]. Un tel vérifieur Vn n'est pas impliqué dans le procédé 300 et n'apparaît donc pas sur la [Fig.3]. En effet, un attribut vérifiable obtenu après la mise en œuvre d'un procédé de renouvellement 300 conforme à l'invention est similaire à tout autre attribut vérifiable obtenu après la mise en œuvre d'un processus connu par un émetteur Ij en réponse à une requête en création VC_CR selon l'état de l'art.

[0057] Un tel procédé 300 selon l'invention est principalement agencé sous la forme de deux sous-procédés, respectivement référencés 100 et 200 sur la [Fig.3]. Ces deux sous-procédés 100 et 200 seront détaillés ultérieurement, respectivement en liaison avec les figures 4 et 5.

[0058] Le premier sous-procédé 100 est agencé pour être mis en œuvre par un portefeuille Wm hébergé par un objet électronique Om, sous la forme avantageuse d'un téléphone mobile intelligent selon l'exemple non limitatif illustré par la [Fig.3], ledit portefeuille Wm étant agencé sous la forme d'une application logicielle (programme d'ordinateur adapté aux systèmes d'exploitation de tels téléphones). Plus précisément, un tel sous-procédé 100 peut être conçu, sous la forme d'un sous-programme d'ordinateur ou bien être intégré au programme d'ordinateur P installé dans la mémoire de programmes M, 13, de l'objet électronique Om et dont les instructions de programme, lors de leur exécution par l'unité de traitement 11 dudit objet Om, provoquent la mise en œuvre du portefeuille Wm par ledit objet électronique Om.

[0059] Le deuxième sous-procédé 200 est, quant à lui, agencé pour être mis en œuvre sous la forme d'un programme ou sous-programme d'ordinateur P, par une unité de traitement d'une entité électronique émettrice d'attributs vérifiables ou émetteur Ij'.

[0060] Pour sa mise en œuvre, l'invention ne requiert ainsi que l'adaptation ou la conception de portefeuilles et d'émetteurs d'un système de preuve en ligne S. Comme l'indique la [Fig.3], ledit procédé 300 peut en outre mettre en scène un registre de confiance TR enregistrant les identités digitales publiques des entités électroniques du système S, parmi lesquelles notamment celles du portefeuille Wm et de l'émetteur Ij' ainsi

adaptés. En effet, ledit registre de confiance TR peut être avantageusement sollicité durant la mise en œuvre du procédé 300 au moyen de requêtes classiques et connues PI_R en consultation d'identités digitales publiques émanant de toute entité électronique d'un système de preuve en ligne S tel que celui décrit en lien avec la [Fig.1]. Ainsi, un tel registre de confiance TR peut, selon l'état de l'art, élaborer un message de transmission PI_M véhiculant une ou plusieurs identités digitales publiques et émettre un tel message à destination de l'entité électronique à l'initiative de ladite requête PI_R en consultation d'identités digitales publiques.

[0061] Pour illustrer un tel procédé 300 conforme à l'invention, supposons qu'un attribut vérifiable VC atteste de la majorité du porteur Um de l'objet électronique Om. Une instance de cet attribut, référencée VCi en [Fig.3], a été créée et émise en réponse à une requête en création d'un attribut vérifiable, ladite requête en création VC_CR étant conforme à l'état actuel de la technique et ayant été adressée par le portefeuille Wm à un premier émetteur Ij tel que celui d'ores et déjà décrit en lien avec le système de preuve en ligne S selon la [Fig.1]. Ledit émetteur Ij n'est pas représenté sur la [Fig.3] car ladite étape de création et de transmission dudit attribut vérifiable VCi ne fait pas partie de l'invention. Supposons également que ledit attribut vérifiable VCi, à l'instar de l'état actuel de la technique, comporte les informations suivantes :

- des données de contexte Ctx propres à la mise en œuvre du système de preuve en ligne S ;
- l'identité digitale publique PIWm (identifiant IDWm et/ou clé publique PKWm) de l'utilisateur Um ou, plus précisément, celle du portefeuille Wm mis en œuvre par l'objet Om détenu par ledit utilisateur Um ;
- l'attribut attesté, en l'espèce « l'utilisateur est majeur » - cet attribut pourrait être facultatif dans le cadre d'un système de preuve de majorité en ligne dédié à ce seul attribut ;
- l'identité digitale de l'émetteur Ij ayant élaboré et émis ledit attribut vérifiable VCi ;
- une date de création ou d'émission CD dudit attribut vérifiable VCi ;
- une date de fin de validité EVD au-delà de laquelle, toute demande de présentation CV_PR dudit attribut vérifiable VCi serait rejetée par tout vérifieur Vn dudit système S ;
- une signature dudit attribut vérifiable VCi par l'émetteur Ij réalisée par ce dernier à l'aide de son identité digitale privée (clé privée SKIj).

[0062] Un tel attribut vérifiable peut être exploité par le portefeuille Wm pour répondre à toute requête en présentation VC_PR émanant de vérificateurs Vn. Bien qu'exploitant éventuellement un pseudonyme sous la forme d'un identifiant décentralisé IDWm, ce dernier peut être tracé par lesdits vérificateurs Vn. Il est donc possible de consister un

historique des messages de présentation PV_M, historique pouvant être préjudiciable pour l'internaute, certains vérificateurs ou émetteurs pouvant croiser et partager leurs informations en lien avec l'exploitation dudit attribut vérifiable. Il n'existe pas à cette heure de solution permettant de prévenir ce risque.

[0063] Le procédé 300 illustré par la [Fig.3] résout cette difficulté de manière élégante et transparente pour l'internaute. Ainsi, principalement par la mise en œuvre du sous-procédé 100, un portefeuille Wm peut décider, selon différents critères, de provoquer un renouvellement conjoint de l'identité digitale du portefeuille Wm et d'attributs vérifiables d'ores et déjà légitimement émis, sans nécessiter d'itérer une procédure de création VC_CR d'attributs vérifiables. Ledit sous-procédé 100 est agencé pour adresser une requête innovante en renouvellement d'un attribut vérifiable d'ores et déjà émis VC_RR à tout émetteur Ij' du système de preuve en ligne S qui aurait été adapté ou agencé pour mettre en œuvre le sous-procédé 200. Une telle requête VC_RR véhicule principalement l'attribut VCi d'ores et déjà émis par l'émetteur Ij et la nouvelle identité digitale publique du portefeuille Wm. En réponse à une telle requête en renouvellement VC_RR, puisqu'un tel attribut vérifiable VCi a été mis par un émetteur Ij légitime au sein du système S, l'émetteur Ij' crée une copie de l'attribut vérifiable VCi sous la forme d'un nouvel attribut vérifiable VCi+1 conservant tout ou partie de la teneur de l'attribut VCi, c'est-à-dire, en l'espèce :

- les données de contexte Ctx propres à la mise en œuvre du système de preuve en ligne S ;
- l'attribut attesté, en l'espèce « l'utilisateur est majeur » - cet attribut pouvant être facultatif dans le cadre d'un système de preuve de majorité en ligne dédié à ce seul attribut ;
- la date de fin de validité EVD au-delà de laquelle, toute demande de présentation CV_PR dudit nouvel attribut vérifiable VCi+1 serait rejetée par tout vérificateur Vn dudit système S.

[0064] Le nouvel attribut vérifiable VCi+1, quasi-clone de l'attribut vérifiable VCi, diffère uniquement dans son contenu en ce que :

- l'identité digitale publique PIWm (identifiant IDWm et/ou clé publique PKWm) de l'utilisateur Um ou plus précisément celle du portefeuille Wm requérant le renouvellement et mis en œuvre par l'objet Om détenu par ledit utilisateur Um ;
- une signature dudit nouvel attribut vérifiable VCi+1 par l'émetteur Ij' réalisée par ce dernier à l'aide de son identité digitale privée (clé privée SKIj') remplace la signature de l'émetteur Ij de l'attribut vérifiable VCi ;
- l'identité digitale publique de l'émetteur Ij' ayant élaboré et émis ledit nouvel attribut vérifiable VCi+1 remplace celle de l'émetteur Ij de l'attribut VCi ;

- une date de création ou d'émission CD dudit nouvel attribut vérifiable VC_{i+1} en lieu et place de la date de création de l'attribut vérifiable VC_i .
- [0065] Il est à noter que lorsque l'attribut vérifiable à renouveler VC_i comporte une date de fin de validité EVD au-delà de laquelle toute demande de présentation CV_PR dudit nouvel attribut vérifiable VC_i serait rejetée par tout vérifieur V_n dudit système S , le nouvel attribut vérifiable VC_{i+1} issu du processus de renouvellement reproduit la même date de fin de validité EVD que l'attribut vérifiable initial VC_i .
- [0066] Par la mise en œuvre du sous-procédé 200 après avoir créé ledit nouvel attribut vérifiable VC_{i+1} , sans déclencher une quelconque investigation CUI auprès d'une entité ou autorité TA , l'émetteur I_j transmet ledit nouvel attribut vérifiable VC_{i+1} , par un message de transmission VC_M , au portefeuille W_m qui remplace, dans la mémoire de donnée M , 12 de l'objet électronique O_m , l'attribut vérifiable VC_i par l'attribut vérifiable VC_{i+1} .
- [0067] Un tel procédé 300 peut être itéré autant que nécessaire, de sorte que ledit nouvel attribut vérifiable VC_{i+1} puisse faire, à son tour, l'objet d'une requête en renouvellement auprès d'un émetteur du système S pour donner naissance à un nouvel attribut vérifiable VC_{i+n} , à l'instar de l'attribut vérifiable initial VC_i . Par la mise en œuvre de l'invention, le traçage à des fins de constitution d'historique est limité. Il devient totalement impossible dans le cas où les demandes de renouvellement d'un attribut vérifiable sont adressées à des émetteurs distincts au sein du système de preuve en ligne S . En effet, un émetteur sollicité pour un renouvellement ne disposerait plus de la capacité d'enrichir une chaîne de renouvellements, si l'attribut vérifiable à renouveler l'a été par un deuxième émetteur, sauf à créer des coalitions avec ses pairs. L'invention prévoit ainsi un mode de réalisation avantageux d'un procédé 300 selon lequel un émetteur sollicité pour un renouvellement d'un attribut vérifiable soit systématiquement ou aléatoirement différent de celui qui a été à l'origine de l'émission (création ou renouvellement) de l'attribut vérifiable faisant l'objet du renouvellement.
- [0068] La [Fig.3] illustre également que les sous-procédés 100 et 200 peuvent solliciter le registre de confiance TR du système de preuve en ligne au moyen de requêtes PI_R en consultation d'identités digitales publiques, ledit registre TR communiquant, en réponse, de telles identités digitales publiques par des messages de transmission PI_M . Cette variante avantageuse d'un procédé 300 selon l'invention permet au portefeuille W_m et à l'émetteur I_j sollicité pour un renouvellement d'attribut vérifiable de s'assurer mutuellement de la légitimité des requêtes et messages échangés ainsi que de l'authenticité de l'attribut vérifiable à renouveler. En effet, préalablement à l'émission d'une requête en renouvellement VC_RR , le portefeuille W_m peut consulter le registre de confiance pour sélectionner un émetteur légitime et satisfaisant certaines contraintes, comme celle évoquée précédemment pour prévenir un suivi des renou-

vellements par un émetteur malveillant ou cible d'une attaque. De son côté, pour donner une suite favorable à une requête en renouvellement adressée par un portefeuille Wm, un émetteur destinataire de ladite requête peut solliciter ledit registre de confiance TR pour disposer des identités digitales publiques respectives dudit portefeuille et de l'émetteur dont l'identité digitale publique est consignée dans l'attribut vérifiable objet d'un renouvellement. Ledit émetteur destinataire de la requête en renouvellement peut ainsi vérifier, d'une part, la signature du portefeuille Wm si celui-ci a signé la requête en renouvellement à l'aide de sa propre identité digitale privée et, d'autre part, la signature de l'émetteur de l'attribut vérifiable concerné par le renouvellement, si ce dernier comporte une telle signature élaborée à partir de l'identité digitale privée de son émetteur.

[0069] Enfin, la [Fig.3] illustre un procédé 300 de renouvellement automatique d'un attribut vérifiable pour lequel le sous-procédé 100 permet une élaboration d'une requête en révocation VC_RKR d'un attribut vérifiable renouvelé VCi, c'est-à-dire celui sur lequel portait une requête en renouvellement VC_RR, à l'issue de la production d'un nouvel attribut vérifiable VCi+1. Une telle requête en révocation est agencée pour être interprétée par le registre de confiance TR ou tout autre registre dédié à cet effet, pour enregistrer les attributs vérifiables ainsi révoqués après renouvellement ou, en lieu et place de tels attributs vérifiables révoqués, enregistrer des informations caractéristiques de ces derniers, à l'instar du résultat d'une fonction cryptographique de hachage d'un tel attribut vérifiable par exemple. Selon cette variante, un émetteur Ij' destinataire d'une requête en renouvellement d'un attribut vérifiable peut en outre vérifier, en sollicitant ledit registre, que l'attribut vérifiable objet d'un renouvellement n'est pas un attribut vérifiable révoqué. Dans la négative, le sous-procédé 200 ne procède pas au renouvellement et peut retourner un message d'erreur au portefeuille requérant le renouvellement.

[0070] La [Fig.4] illustre en détail des modes de réalisation avantageux d'un sous-procédé 100 d'un procédé de renouvellement automatique d'attributs vérifiables selon l'invention. Comme indiqué précédemment, un tel sous-procédé 100 est agencé pour être mis en œuvre, ou faire partie, d'un portefeuille Wm adapté en conséquence et appartenant à un système de preuve en ligne S dont au moins un émetteur Ij' est adapté pour mettre en œuvre un sous-procédé 200 exploitant une requête en renouvellement d'un attribut vérifiable.

[0071] Un tel sous-procédé 100 consiste en trois grandes étapes distinctes référencées 110, 120, 130 sur la [Fig.4], lesdites étapes étant dédiées respectivement à :

- la détection 110 d'un événement déclencheur d'un renouvellement d'un attribut vérifiable VCi, c'est-à-dire un attribut vérifiable d'ores et déjà émis légitimement (simplement créé ou précédemment renouvelé) par

- l'émetteur Ij (non représenté sur la [Fig.4]) ;
 - l'élaboration et le déclenchement 120 de l'émission d'une requête VC_RR en renouvellement d'un tel attribut vérifiable VCi à destination d'un émetteur Ij' du système de preuve en ligne S ;
 - la gestion 130 d'un nouvel attribut vérifiable VCi+1 fruit d'une telle requête en renouvellement VC_RR et transmis par ledit émetteur Ij' par un message de transmission VC_M.
- [0072] Selon la [Fig.4], chaque entité électronique du système de preuve en ligne dont fait partie le portefeuille Wm est associée à une identité digitale formée d'une identité digitale publique et d'une identité digitale privée, ladite identité digitale étant enregistrée dans une mémoire de données 12 de chaque entité électronique. Un message, une requête ou un contenu peut être signé par une première entité électronique à l'aide de son identité digitale privée, ladite signature pouvant être vérifiée par toute deuxième entité électronique en exploitant l'identité digitale publique de ladite première entité électronique. Éventuellement, ladite première entité peut chiffrer messages, requêtes ou contenus à l'aide de l'identité digitale publique d'une deuxième entité électronique déterminée, de sorte que cette dernière soit la seule entité électronique capable de déchiffrer lesdits messages, requêtes ou contenus à l'aide de sa propre identité digitale privée inconnue des autres entités électroniques.
- [0073] Ainsi, l'identité digitale IWm du portefeuille Wm consiste en :
- une identité digitale publique PIWm, en l'espèce un identifiant unique IDWm (éventuellement décentralisé) et une clé publique PKWm ;
 - une identité digitale privée, en l'espèce une clé privée SKWm conjointement élaborée avec ladite clé publique PKWm pour assurer un schéma cryptographique de signature et/ou de chiffrement asymétrique.
- [0074] L'identité digitale IIj de l'émetteur Ij de l'attribut VCi, objet d'un renouvellement automatique consiste en :
- une identité digitale publique PIIj, en l'espèce un identifiant unique IDIj (éventuellement décentralisé) et une clé publique PKIj ;
 - une identité digitale privée, en l'espèce une clé privée SKIj conjointement élaborée avec ladite clé publique PKIj pour assurer un schéma cryptographique de signature et/ou de chiffrement asymétrique.
- [0075] Il en est de même pour l'émetteur Ij' destinataire d'une requête en renouvellement de l'attribut vérifiable VCi, éventuellement ou avantageusement distinct de l'émetteur Ij. Ainsi, l'identité digitale IIj' de l'émetteur Ij' consiste en :
- une identité digitale publique PIIj', en l'espèce un identifiant unique IDIj' (éventuellement décentralisé) et une clé publique PKIj' ;
 - une identité digitale privée, en l'espèce une clé privée SKIj' conjointement

élaborée avec ladite clé publique PKIj' pour assurer un schéma cryptographique de signature et/ou de chiffrement asymétrique.

- [0076] Le système de preuve en ligne S, dont fait partie le portefeuille Wm et les émetteurs Ij et Ij', comprend un registre de confiance TR agencé pour enregistrer, dans une mémoire de données TRM qui lui est propre les identités digitales publiques PIWm, PIIj, PIIj', respectives des entités électroniques Wm, Ij, et Ij' dudit système de preuve en ligne S. Ledit registre est apte à recevoir une requête PI_R en consultation d'identités digitales publiques émanant d'une entité électronique dudit système S et élaborer, en réponse à une telle requête PI_R, un message de transmission PI_M véhiculant une ou plusieurs identités digitales publiques à destination de l'entité électronique émettrice de ladite requête PI_R en consultation d'identités digitales publiques.
- [0077] Le sous-procédé 100 comporte donc une première étape de détection 110 d'un événement déclencheur d'un renouvellement d'un attribut vérifiable, en l'espèce l'attribut vérifiable VCi émis au préalable par l'émetteur Ij.
- [0078] Un tel événement peut être de différentes natures. L'invention prévoit en effet qu'un renouvellement d'un attribut vérifiable puisse être déclenché automatiquement à la suite d'un nombre prédéterminé de réponses à des requêtes en présentation VC_PR d'un tel attribut vérifiable émanant de vérificateurs du système de preuve en ligne tel que le vérificateur Vn décrit en lien avec la [Fig.1]. Un tel renouvellement d'attribut vérifiable pourrait également intervenir automatiquement après une certaine durée s'écoulant à compter de la date de création CD d'un tel attribut vérifiable, que ladite création découle d'une requête en création VC_CR selon l'état de l'art ou d'une requête en renouvellement CV_RR propre à l'invention. Un tel renouvellement d'attribut vérifiable pourrait en outre être déclenché automatiquement et de manière aléatoire par la mise en œuvre d'un algorithme exploitant tout ou partie du contenu dudit attribut vérifiable en qualité d'une graine pour la production d'un aléa comparé *in fine* à un seuil, etc. L'invention prévoit que la détection d'un événement déclencheur ne se réduise à ces seuls exemples pris seuls ou en combinaison.
- [0079] A titre d'exemple, la [Fig.4] décrit un mode de réalisation selon lequel le portefeuille Wm associe à chaque attribut vérifiable VCi dont il assure la gestion, un compteur nPV d'émission de messages en présentation PV_M véhiculant ledit attribut vérifiable VCi en réponse à des requêtes en présentation VC_PR émanant de vérificateurs. Selon cet exemple de réalisation, chaque attribut vérifiable VCi est donc associé à un tel compteur conjointement enregistré en mémoire de données 12 de l'objet électronique hébergeant ledit portefeuille Wm. L'étape 110 peut alors consister tout d'abord en une lecture 111, dans une telle mémoire de données 12 accessible en lecture et écriture par le portefeuille Wm, de la valeur courante d'un compteur nPV de messages de pré-

sensation PV_M véhiculant l'attribut vérifiable VCi adressés à un vérifieur du système de preuve en ligne S. Ladite étape 110 peut alors consister en la comparaison 112 de la valeur courante dudit compteur nPV à un seuil maximal de présentations prédéterminé, par exemple compris entre deux et dix, préférentiellement égal à cinq de manière à ne pas trop fréquemment engendrer des renouvellements tout en préservant l'effet technique de non traçabilité recherché. Enfin, ladite étape 110 conclut en la détection d'un événement déclencheur d'un renouvellement automatique si ladite valeur dudit compteur nPV atteint ledit seuil prédéterminé. Une telle situation est représentée par le lien 112-y sur la [Fig.4]. Tant que ledit compteur nPV demeure en deçà dudit seuil, aucun renouvellement de l'attribut vérifiable n'est déclenché (situation représentée par le lien 112-n sur la [Fig.4]).

[0080] Un tel renouvellement d'attribut vérifiable VCi est détaillé à présent en lien avec l'étape 120 du sous-procédé 100. Un tel traitement 120 comporte principalement une étape 125 d'élaboration d'une requête en renouvellement VC_RR à adresser à un émetteur du système de preuve en ligne. Pour cela, au préalable, afin de prévenir la traçabilité de l'identité digitale publique du portefeuille et, par voie de conséquence, celle de l'internaute Um porteur de l'objet Om hébergeant ledit portefeuille Wm, le traitement 120 peut comporter une étape 121 de production d'une nouvelle identité digitale IWm du portefeuille d'attributs vérifiables Wm en remplacement de l'identité digitale courante, à l'instar d'une création d'une telle identité digitale lors de l'installation de l'application « portefeuille d'attributs vérifiables » dans l'objet électronique Om. Cette étape consiste en une production d'un nouveau jeu de clés publique PKVm et privée SKWm, par exemple en dérivant une clé mère et une graine aléatoire. De la même manière, une telle étape 121 consiste en outre en une production d'un nouvel identifiant IDWm, soit de toute pièce par exemple via la génération d'un aléa ou bien en le dérivant de la clé publique PKWm s'il s'agit d'un identifiant décentralisé. Les identités digitales publique PIWm et privée SKWm formant la nouvelle identité digitale IWm du portefeuille Wm, sont ainsi recrées. Lorsque le registre de confiance TR mémorise l'identité digitale publique dudit portefeuille Wm, l'invention prévoit que ladite étape 121 puisse consister en outre à élaborer une requête PI_U en mise à jour d'identité digitale publique à destination du registre de confiance TR. Une telle requête PI_U est agencée par le portefeuille Wm pour véhiculer la nouvelle identité digitale publique PIWm issue de la nouvelle identité digitale IWm et être signée à l'aide de la précédente identité digitale privée SKm dudit portefeuille Wm. Le registre de confiance TR peut alors, en réponse à une telle requête en mise à jour, vérifier ladite signature en exploitant la future ancienne identité digitale publique dudit portefeuille Wm et accepter, dans l'affirmative, ladite mise à jour de l'identité publique du portefeuille Wm. Ladite étape 121 de production d'une nouvelle identité digitale IWm

demeure toutefois avantageuse mais optionnelle. L'invention prévoit en effet qu'un portefeuille Wm puisse conserver une même identité digitale IWm pour mettre en œuvre une pluralité de requêtes en renouvellement VC_RR. En variante, une mise en œuvre de l'étape 121 peut être déclenchée, de manière asynchrone, au regard de la mise en œuvre de l'étape de détection 110 d'un événement déclencheur d'un renouvellement d'un attribut vérifiable VC. Une mise en œuvre de l'étape 121 pourrait être déclenchée, selon tout critère, tel que, à titre d'exemples non limitatifs, un comptage, comparé à un seuil, de requêtes en renouvellement VC_RR d'un attribut vérifiable déterminé ou encore un déclenchement aléatoire. L'invention prévoit en effet, qu'un portefeuille Wm puisse comporter une pluralité d'identités digitales IWm respectivement associées à des attributs vérifiables VC distincts gérés par ledit portefeuille Wm.

- [0081] Pour que le portefeuille Wm puisse élaborer la requête en renouvellement VC_RR à l'étape 125, celle-ci étant agencée pour véhiculer l'attribut vérifiable VCi, objet du renouvellement, ainsi que la nouvelle identité publique du portefeuille Wm, il est nécessaire de sélectionner un émetteur à qui adresser ladite requête en renouvellement VC_RR.
- [0082] Pour cela, l'invention prévoit différents modes de réalisation pour sélectionner l'émetteur futur destinataire de la requête en renouvellement VC_RR.
- [0083] Selon un premier mode de réalisation, le traitement 120 comporte une étape 122 pour lire, au sein de l'attribut vérifiable VCi (objet d'un renouvellement et inscrit dans la mémoire de données 12), l'identité digitale publique PIIj de l'émetteur Ij dudit attribut vérifiable VCi, afin d'adresser ladite requête en renouvellement VC_RR, à l'étape 125, à destination dudit émetteur Ij précédemment en charge de la création (ou d'un précédent renouvellement) dudit attribut vérifiable VCi.
- [0084] En variante, l'invention prévoit que le portefeuille Wm dispose, dans la mémoire de données 12, d'une table des identités digitales publiques des émetteurs connus dudit portefeuille Wm. A chaque itération dudit traitement 120, la sélection de l'identité digitale publique de l'émetteur destinataire de la requête en renouvellement VC_RR peut être réalisée selon une lecture aléatoire ou cyclique selon un pas déterminé de ladite table.
- [0085] Selon une alternative préférée, pour effectuer une telle sélection parmi une liste d'identités digitales publiques d'émetteurs, le traitement 120 comporte une étape 123 d'élaboration d'une requête PI_R en consultation d'identités digitales publiques d'entités émettrices du système de preuve en ligne S et de déclenchement de l'émission de ladite requête PI_R à destination du registre de confiance TR. Ledit traitement 120 comporte alors une étape 124, subséquente à l'étape 123, de réception d'un message de transmission PI_M émanant dudit registre de confiance TR et de lecture au sein de

celui-ci d'une ou plusieurs identités digitales publiques d'émetteurs véhiculées par ledit message PI_M. Une telle sollicitation systématique du registre de confiance TR pour constituer une liste d'émetteurs permet au portefeuille Wm de connaître, à date, les émetteurs disponibles et aptes à réaliser un tel renouvellement d'attributs vérifiables. La sélection finale dudit émetteur destinataire de la requête en renouvellement VC_RR peut également être réalisée de manière aléatoire au sein de ladite liste obtenue ou bien de manière dirigée pour s'interdire d'émettre ladite requête CV_RR à destination de l'émetteur Ij de l'attribut vérifiable VCi objet du renouvellement. Dans ce cas, la sélection du destinataire s'effectue en choisissant une identité digitale publique distincte de celle de l'émetteur Ij.

[0086] L'étape 125 du traitement 120 consiste alors en une élaboration de la requête VC_RR en renouvellement de l'attribut vérifiable VCi, puis à en provoquer l'émission, à destination de l'entité émettrice Ij' dont l'identité digitale publique PIIj' a été sélectionnée, ladite requête en renouvellement comportant l'attribut vérifiable VCi à renouveler et la nouvelle identité digitale publique PIWm du portefeuille Wm.

[0087] Enfin, ladite étape 125 peut avantageusement consister à signer ladite requête VC_RR, préalablement à l'émission de cette dernière, à l'aide de l'identité digitale privée SKWm du portefeuille Wm. De cette manière, l'émetteur Ij' destinataire pourra en vérifier la légitimité, comme il sera expliqué en lien avec la [Fig.5]. De la même manière, ladite étape 125 pourrait consister, en variante ou en complément de ladite signature, à chiffrer le contenu de ladite requête VC_RR, préalablement à son émission, à l'aide de l'identité digitale publique PIIj' (plus précisément de la clé publique PKIj' issue de celle-ci) de sorte que ledit émetteur Ij' puisse être le seul à déchiffrer ladite requête en renouvellement.

[0088] Le sous-procédé 100, outre le traitement 110 pour détecter un événement déclencheur d'un renouvellement d'un attribut vérifiable VCi et le traitement 120 pour produire et émettre une requête en renouvellement VC_RR de ce dernier, comporte un traitement ou étape de gestion 130 d'un nouvel attribut vérifiable VCi+1 fruit d'une telle requête en renouvellement VC_RR et transmis par un message de transmission VC_M élaboré par l'émetteur Ij' destinataire de ladite requête en renouvellement VC_RR.

[0089] Un tel traitement 130 comporte une étape 131 de réception et de lecture d'un message de transmission d'un nouvel attribut vérifiable VCi+1 émanant de l'émetteur Ij' destinataire de la requête en renouvellement VC_RR élaborée au traitement 120. Une telle étape 131 peut en outre consister en la vérification de la signature du nouvel attribut vérifiable VCi+1 par l'entité émettrice Ij' de ce dernier, à l'aide de l'identité digitale publique PIIj' de ladite entité émettrice Ij', si ledit nouvel attribut a été signé par cette dernière. Le nouvel attribut vérifiable VCi+1 est rejeté si la vérification de la

signature échoue et une nouvelle itération du traitement 120 est mise en œuvre, avantageusement en sélectionnant un émetteur I_j' distinct de la précédente itération pour lui adresser une requête en renouvellement VC_RR .

[0090] Lorsque ledit nouvel attribut vérifiable paraît légitime, le traitement 130 comporte une étape 132 d'enregistrement du nouvel attribut vérifiable VC_{i+1} , dans la mémoire de données 12, M, accessible en lecture et en écriture par le portefeuille W_m . Cet enregistrement du nouvel attribut vérifiable VC_{i+1} est réalisé en écrasant l'attribut vérifiable VC_i ainsi renouvelé ou bien suivi par l'effacement de ce dernier.

[0091] Lorsque le sous-procédé 100 prévoit l'exploitation d'un compteur de présentations nPV, ladite étape 132 peut en outre consister en l'initialisation de la valeur d'un tel compteur nPV de messages de présentation PV_M véhiculant ledit nouvel attribut vérifiable VC_{i+1} dans une mémoire de données 12 de l'objet électronique O_m hébergeant le portefeuille W_m , ladite mémoire étant accessible en lecture et en écriture par ledit portefeuille W_m .

[0092] Comme évoqué précédemment en lien avec la [Fig.3], le sous-procédé 100 peut prévoir une élaboration d'une requête en révocation VC_RKR d'un attribut vérifiable renouvelé VC_i , c'est-à-dire celui sur lequel portait une requête en renouvellement VC_RR , à l'issue de la production d'un nouvel attribut vérifiable VC_{i+1} . Selon ce mode de réalisation avantageux, le traitement 130 comporte en amont de la destruction (par écrasement ou effacement) d'un attribut vérifiable renouvelé VC_i , une étape pour élaborer une telle requête en révocation VC_RKR agencée pour être interprétée par le registre de confiance TR ou tout autre registre dédié à cet effet. Ladite requête VC_RKR comporte l'attribut vérifiable VC_i renouvelé et ainsi révoqué ou une information caractéristique de celui-ci, par exemple le résultat de la mise en œuvre d'une fonction cryptographique de hachage dudit attribut vérifiable VC_i . Une telle requête VC_RKR peut être signée par le portefeuille W_m à l'étape 133 à l'aide de l'identité digitale privée SKW_m du portefeuille W_m , voire être chiffrée à l'aide de l'identité digitale publique du registre destinataire de la requête en révocation. De cette manière, ledit registre peut lire, accepter ou rejeter ladite révocation après confirmation de la vérification de la signature dudit portefeuille W_m à l'aide de l'identité digitale publique PIW_m de ce dernier.

[0093] Un procédé 300 de renouvellement automatique d'un attribut vérifiable VC_i conforme à l'invention consiste en outre en un deuxième sous-procédé 200 agencé pour être mis en œuvre par une unité de traitement 11 d'émetteur I_j' d'un système de preuve en ligne S tel que celui I_j illustré par la [Fig.1]. Pour adapter le fonctionnement d'un tel émetteur I_j' , ledit sous-procédé 200 comprend principalement deux étapes ou traitements référencés 210 et 200 sur la [Fig.5] :

- la première étape 210 permet le traitement d'une requête en renouvellement

VC_RR d'un attribut vérifiable d'ores et déjà légitiment émis VCI, ladite requête étant transmise par un portefeuille Wm adapté pour mettre en œuvre le sous-procédé 100 ;

- la deuxième étape 220 consiste en la mise en œuvre du renouvellement d'un tel attribut vérifiable VCI en tant que tel ainsi qu'en la communication, par un message de transmission VC_M, d'un nouvel attribut vérifiable VCI+1 au portefeuille Wm requérant ledit renouvellement d'attribut vérifiable.

[0094] Le traitement 210 d'une requête en renouvellement VC_RR d'un attribut vérifiable VCI comporte une première étape de réception 211 d'une telle requête en renouvellement et de lecture des informations véhiculées par cette dernière parmi lesquelles l'attribut vérifiable VCI à renouveler et l'identité digitale publique PIWm du portefeuille Wm, respectivement objet et émetteur de ladite requête en renouvellement VC_RR.

[0095] Ledit traitement 210 comporte en outre une étape 214 de vérification :

- de la signature de ladite requête en renouvellement VC_RR par le portefeuille Wm, à l'aide de l'identité digitale publique PIWm de ce dernier ;
- de la signature de l'attribut vérifiable à renouveler VCI par l'entité électronique émettrice Ij de ce dernier, à l'aide l'identité digitale publique PIJj de cette dernière.

[0096] La vérification 214 de la signature de ladite requête en renouvellement VC_RR par le portefeuille Wm peut être optionnelle. En effet, une telle signature constitue une variante préférée mais non essentielle du sous-procédé 100. En revanche, la vérification 214 de la signature de l'attribut vérifiable à renouveler VCI par l'entité électronique émettrice Ij de ce dernier est davantage intéressante pour la mise en œuvre de l'invention puisque que la légitimité d'un tel attribut vérifiable VCI permet de déroger à la sollicitation de l'autorité de confiance TA. Ainsi, la deuxième étape 220, consistant en la mise en œuvre du renouvellement en tant que tel d'un attribut vérifiable, n'est mise œuvre que si ladite étape 214 de l'attribut vérifiable VCI à renouveler confirme l'authenticité de ladite signature dudit attribut vérifiable VCI (situation illustrée par le lien 214-y sur la [Fig.5]).

[0097] Lorsque la vérification 214 de la signature de ladite requête VC_RR par le portefeuille Wm est prévue, alors la mise en œuvre de la deuxième étape 220 consistant en tant que telle en le renouvellement d'un attribut vérifiable est également conditionnée à la confirmation de l'authenticité de ladite signature de ladite requête VC_RR (situation illustrée par le lien 214-y sur la [Fig.5]).

[0098] Si l'étape 214 conclut à une non-authenticité de signature(s), situation symbolisée par le lien 214-n sur la [Fig.5], l'invention prévoit que ladite étape 214 puisse en outre consister en l'élaboration d'un message de transmission VC_M véhiculant un contenu

caractérisant une erreur (symbolisée par le vocable anglo-saxon « error » sur la [Fig.5]) à destination du portefeuille Wm requérant un renouvellement avorté. Un tel message VC_M peut être signé à l'aide de l'identité digitale privée SKIj' de l'émetteur Ij' mettant en œuvre la présente instance du sous-procédé 200.

[0099] Pour pouvoir vérifier la ou lesdites signatures de l'attribut vérifiable à renouveler VCi et/ou de la requête en renouvellement VC_RR en tant que telles, à l'instar de ce que prévoit le premier sous-procédé 100 aux étapes optionnelles 123 et 124, l'étape 214 de vérification du traitement 210 du deuxième sous-procédé 200, peut être avantageusement précédée :

- d'une étape 212 d'élaboration d'une requête PI_R en consultation d'identités digitales publiques d'entités électroniques du système de preuve en ligne S et de déclenchement de l'émission de ladite requête à destination du registre de confiance TR ;
- d'une étape 213 de réception d'un message de transmission PI_M émanant dudit registre de confiance TR et de recherche, au sein de celui-ci, de l'identité digitale publique PIIj de l'entité électronique émettrice Ij de l'attribut vérifiable VCi à renouveler, voire de celle PIWm du portefeuille Wm émetteur de la requête en renouvellement VC_RR.

[0100] La deuxième étape 220 du deuxième sous-procédé 200 consistant en la mise en œuvre du renouvellement en tant que tel d'un attribut vérifiable légitimement d'ores et déjà émis ainsi qu'en la communication, par un message de transmission VC_M, d'un nouvel attribut vérifiable VCi+1 au portefeuille Wm requérant ledit renouvellement d'attribut vérifiable, comporte une étape 221 d'élaboration du nouvel attribut vérifiable VCi+1 consistant à copier l'intégralité des informations contenues dans l'attribut vérifiable VCi à renouveler exception faite des informations en lien avec l'élaboration en tant que telle de ce dernier, comme évoqué précédemment en lien avec la [Fig.3].

[0101] Ladite étape 221 consiste en outre en une élaboration d'une signature du nouvel attribut vérifiable VCi+1 à l'aide de l'identité digitale privée SKIj' de l'entité émettrice Ij' dudit nouvel attribut vérifiable de sorte que celui-ci soit légitimement émis, à l'instar de l'attribut vérifiable renouvelé VCi. Une telle signature fait partie intégrante du contenu du nouvel attribut vérifiable VCi+1.

[0102] La deuxième étape 220 du deuxième sous-procédé 200 comporte une sous-étape 222 pour provoquer l'émission du nouvel attribut vérifiable VCi+1 à destination du portefeuille Wm requérant le renouvellement de l'attribut vérifiable VCi.

[0103] L'invention a été décrite au travers de différentes configurations d'un système de preuve en ligne S, afin qu'un internaute Um puisse solliciter un fournisseur de biens ou de services SP. L'invention ne saurait être limitée à ce seul exemple de système de preuve en ligne et trouverait une pleine application dans un système de preuve de

majorité ou de tout autre attribut vérifiable auprès d'un fournisseur de biens et de services dans le monde physique (tel qu'un distributeur de boissons alcoolisées, de tabac ou un opérateur d'un lieu de jeux d'argent) et non uniquement digital. Il suffit pour cela, que ledit fournisseur SP puisse établir une connexion avec un vérifieur V_n d'un tel système de preuve en ligne S.

Revendications

[Revendication 1]

Procédé (300) de renouvellement automatique d'un attribut d'un utilisateur (U_m) vérifiable (VC , VC_i , VC_{i+1}) par une entité électronique vérificatrice (V_n) d'un système de preuve en ligne (S),

- ledit système (S) comportant une pluralité d'entités électroniques (V_n , W_m , I_j , I_j') respectivement agencées pour communiquer les unes avec les autres au sein dudit système (S) dont, outre ladite entité électronique vérificatrice (V_n), un portefeuille (W_m) d'attributs vérifiables mis en œuvre par une unité de traitement (11) d'un objet électronique (O_m) détenu par un utilisateur (U_m), une entité électronique émettrice (I_j , I_j') d'attributs vérifiables,
- tout attribut vérifiable (VC , VC_i , VC_{i+1}) émis ayant été préalablement élaboré et transmis par une entité électronique émettrice (I_j , I_j') dudit système de preuve en ligne (S) en réponse à une requête (VC_CR) en création d'attribut vérifiable initiée par un portefeuille (W_m) d'attributs vérifiables dudit système (S),

ledit procédé (100, 200) de renouvellement automatique étant caractérisé en ce qu'il comporte :

- un premier sous-procédé (100), mis en œuvre par un portefeuille (W_m) d'attributs vérifiables, comprenant :
 - une étape (110) de détection d'un événement déclencheur d'un renouvellement d'un attribut vérifiable (VC_i) d'ores et déjà émis ;
 - une étape (120) d'élaboration et de déclenchement de l'émission d'une requête (VC_RR) en renouvellement d'un attribut vérifiable (VC_i) d'ores et déjà émis, à destination d'une entité électronique émettrice (I_j') du système de preuve en ligne (S) ;
 - une étape de gestion (130) d'un nouvel attribut vérifiable (VC_{i+1}) fruit d'une telle requête en renouvellement (VC_RR) et transmis (VC_M) par ladite entité émettrice (I_j') ;
- un deuxième sous-procédé (200) mis en œuvre par une unité

de traitement (11) d'une entité émettrice (Ij') comprenant :

- une étape (210) de traitement d'une requête en renouvellement d'un attribut vérifiable d'ores et déjà émis transmise par un portefeuille (Wm) d'attributs vérifiables ;
- une étape (220) de renouvellement d'un tel attribut vérifiable d'ores et déjà émis et de transmission (VC_M) d'un nouvel attribut vérifiable à destination du portefeuille (Wm) d'attributs vérifiables requérant ledit renouvellement d'attribut vérifiable d'ores et déjà émis.

[Revendication 2]

Procédé (300) selon la revendication 1, pour lequel :

- chaque entité électronique (Ij, Ij', Vn, Wm) dudit système de preuve en ligne (S) est associée à une identité digitale (IIj, IIj', IVn, IWm) formée d'une partie publique (PIIj, PIIj', PIVn, PIWm), dite « identité digitale publique » et d'une partie privée (SKIj, SKIj', SKVn, SKWm), dite « identité digitale privée », ladite identité digitale étant enregistrée dans une mémoire de données (M, 12) de ladite chaque entité électronique ;
- ledit système de preuve en ligne (S) comprend un registre de confiance (TR) agencé pour :
 - enregistrer, dans une mémoire de données (TRM, 12), les identités digitales publiques (PIIj, PIIj', PIVn, PIWm) respectives des entités électroniques (Ij, Ij', Vn, Wm) dudit système de preuve en ligne (S) ;
 - recevoir une requête (PI_R) en consultation d'identités digitales publiques émanant d'une entité électronique dudit système (S) ;
 - élaborer un message de transmission (PI_M) véhiculant une ou plusieurs identités digitales publiques (PIIj, PIIj', PIVn, PIWm) et émettre un tel message à destination de l'entité électronique (Ij, Ij', Vn, Wm) émettrice de ladite requête (PI_R) en consultation d'identités digitales publiques ;
- le premier sous-procédé (100) est agencé de sorte que :

- l'étape de gestion (130) d'un nouvel attribut vérifiable (VC_{i+1}) fruit d'une telle requête en renouvellement (VC_RR) comporte :
 - une étape (131) de vérification de la signature du nouvel attribut vérifiable (VC_{i+1}) par l'entité émettrice (I_j') de ce dernier (VC_{i+1}), à l'aide de l'identité digitale publique (PII_j') de ladite entité émettrice (I_j') ;
 - une étape (132) d'enregistrement du nouvel attribut vérifiable (VC_{i+1}), dans une mémoire de données (M , 12) accessible en lecture et en écriture par le portefeuille (W_m) d'attributs vérifiables, en remplacement de l'attribut vérifiable (VC_i) renouvelé si, et seulement si, ladite étape (131) de vérification de la signature du nouvel attribut vérifiable (VC_{i+1}) confirme l'authenticité de ladite signature ;
- le deuxième procédé (200) est agencé de sorte que :
 - l'étape (210) de traitement d'une requête en renouvellement d'un attribut vérifiable d'ores et déjà émis comporte :
 - une étape de réception (211) d'une telle requête en renouvellement (VC_RR) et de lecture des informations véhiculées par cette dernière parmi lesquelles l'attribut vérifiable (VC_i) d'ores et déjà émis et l'identité digitale publique (PIW_m) du portefeuille (W_m) d'attributs vérifiables, respectivement objet et émetteur de ladite requête en renouvellement (VC_RR) ;
 - une étape (214) de vérification de la signature de l'attribut vérifiable à renouveler par l'entité électronique émettrice de ce dernier, à l'aide de l'identité digitale publique (PII_j) de cette dernière ;
 - l'étape (220) de renouvellement d'un attribut vé-

rifiable d'ores et déjà émis et de transmission
(VC_M) d'un nouvel attribut vérifiable :

- n'est mise œuvre que si ladite étape (214) de vérification de la signature de l'attribut vérifiable (VCi) à renouveler confirme l'authenticité de cette dernière ;
- comporte une étape (221) :
 - d'élaboration du nouvel attribut vérifiable (VCi+1) consistant à copier l'intégralité des informations contenues dans l'attribut vérifiable (VCi) à renouveler exception faite des informations en lien avec l'élaboration en tant que telle de ce dernier ;
 - de signature dudit nouvel attribut vérifiable (VCi+1) à l'aide de l'identité digitale privée (SKIj') de l'entité émettrice (Ij') dudit nouvel attribut vérifiable ;
- comporte une étape (222) pour provoquer l'émission du nouvel attribut vérifiable (VCi+1) à destination du portefeuille (Wm) d'attributs vérifiables requérant le renouvellement.

[Revendication 3] Procédé (300) selon la revendication 2, pour lequel :

- le premier sous-procédé (100) est agencé de sorte que l'étape (120) d'élaboration et de déclenchement de l'émission d'une requête en renouvellement (VC_RR) comporte une étape (125) de signature de ladite requête en renouvellement (VC_RR) à l'aide de l'identité digitale privée (SKWm) du portefeuille (Wm) d'attributs vérifiables ;
- le deuxième procédé (200) est agencé de sorte que :
 - l'étape (210) de traitement d'une requête en renouvellement d'un attribut vérifiable d'ores et déjà émis comporte une étape (214) de vérification de la

signature de ladite requête en renouvellement par le portefeuille (Wm) d'attributs vérifiables, à l'aide de l'identité digitale publique (PIWm) de ce dernier ;

- l'étape (220) de renouvellement d'un attribut vérifiable d'ores et déjà émis et de transmission (VC_M) d'un nouvel attribut vérifiable n'est mise œuvre que si ladite étape (214) de la signature de la requête en renouvellement (VC_RR) confirme l'authenticité de ladite signature.

[Revendication 4] Procédé (300) selon l'une quelconque des revendications 1 à 3, pour lequel :

- l'étape (110) de détection d'un événement déclencheur d'un renouvellement automatique d'un attribut vérifiable (VCi) d'ores et déjà émis, consiste en :
 - une lecture (111), dans une mémoire de données (M, 12) accessible en lecture et écriture par le portefeuille (Wm) d'attributs vérifiables, de la valeur d'un compteur (nPv) de messages de présentation (PV_M) véhiculant l'attribut vérifiable (VCi) adressés à une entité électronique vérificatrice (Vn) du système de preuve en ligne (S) ;
 - une comparaison (112) de la valeur courante dudit compteur à un seuil maximal prédéterminé et une conclusion quant à la détection d'un événement déclencheur d'un renouvellement automatique si (112-y) ladite valeur dudit compteur (nPv) atteint ledit seuil prédéterminé ;
- l'étape de gestion (130) d'un nouvel attribut vérifiable (VCi+1) fruit d'une requête en renouvellement (VC_RR), consiste en outre en une initialisation (132) de la valeur d'un compteur (nPv) de messages de présentation (PV_M) véhiculant ledit nouvel attribut vérifiable (VCi+1) dans une mémoire de données (M) accessible en lecture et en écriture par le portefeuille (Wm) d'attributs vérifiables.

- [Revendication 5] Procédé (300) selon l'une quelconque des revendications 2 à 4, pour lequel l'étape (120) d'élaboration et de déclenchement de l'émission d'une requête (VC_RR) en renouvellement d'un attribut vérifiable (VCi) d'ores et déjà émis du premier sous-procédé (100) comporte :
- une étape (123) d'élaboration d'une requête (PI_R) en consultation d'identités digitales publiques (PIIj') d'entités émettrices (Ij') du système de preuve en ligne (S) et de déclenchement de l'émission de ladite requête à destination du registre de confiance (TR) ;
 - une étape (124) de réception d'un message de transmission (PI_M) émanant dudit registre de confiance (TR) et de lecture au sein de celui-ci d'une identité digitale publique (PIIj') d'entité émettrice (Ij') véhiculée par ledit message (PI_M) ;
 - une étape (121) de production d'une nouvelle identité digitale (IWm) du portefeuille d'attributs vérifiables (Wm) en remplacement de la précédente ;
 - une étape (125) d'élaboration de la requête (VC_RR) en renouvellement de l'attribut vérifiable (VCi) d'ores et déjà émis à destination de l'entité émettrice (Ij') dont l'identité digitale publique (PIIj') a été lue dans le message de transmission (PI_M) émanant dudit registre de confiance (TR), ladite requête en renouvellement comportant l'attribut vérifiable (VCi) à renouveler et la nouvelle identité digitale publique (PIWm) du portefeuille (Wm) d'attributs vérifiables.
- [Revendication 6] Procédé (300) selon la revendication précédente, pour lequel l'étape (121) de production d'une nouvelle identité digitale (IWm) du portefeuille d'attributs vérifiables (Wm) consiste en outre en une élaboration d'une requête (PI_U) en mise à jour d'identité digitale publique à destination du registre de confiance (TR), ladite requête véhiculant la nouvelle identité digitale publique (PIWm) issue de la nouvelle identité digitale (IWm) signée à l'aide de la précédente identité digitale privée (SKm) dudit portefeuille d'attributs vérifiables (Wm).
- [Revendication 7] Procédé (100, 200) selon la revendication 5 ou 6, pour lequel l'étape (124) de réception d'un message de transmission (PI_M) émanant dudit registre de confiance (TR) et de lecture au sein de celui-ci d'une identité digitale publique (PIIj') d'entité électronique émettrice (Ij') véhiculée

par ledit message (PI_M) consiste en une sélection d'une identité digitale publique (PIIj') d'entité émettrice (Ij') distincte de celle de l'entité électronique émettrice (Ij) ayant émis l'attribut vérifiable (VCi) à renouveler.

- [Revendication 8] Procédé (300) selon l'une quelconque des revendication 2 à 7, pour lequel :
- le registre de confiance (TR) est agencé pour mémoriser (TRM) tout attribut vérifiable révoqué (VCi) ou une information caractéristique d'un tel attribut vérifiable révoqué (VCi) en réponse à la réception d'une requête en révocation (VC_RKR) d'attribut vérifiable ;
 - l'étape de gestion (130) d'un nouvel attribut vérifiable (VCi+1) fruit d'une requête en renouvellement (VC_RR) comporte une étape (133) d'élaboration d'une telle requête en révocation (VC_RKR) d'attribut vérifiable véhiculant l'attribut vérifiable (VCi) ayant fait l'objet d'un renouvellement à destination du registre de confiance (TR).
- [Revendication 9] Procédé (300) selon la revendication précédente, pour lequel l'étape (133) d'élaboration d'une requête en révocation (VC_RKR) consiste en outre en l'élaboration d'une signature de ladite requête (VC_RKR) à l'aide de l'identité digitale privée (SKWm) dudit portefeuille d'attributs vérifiables (Wm).
- [Revendication 10] Procédé (300) selon l'une quelconque des revendications 2 à 9, pour lequel l'étape (214) de vérification de la signature de l'attribut vérifiable à renouveler du deuxième sous-procédé (200) est précédée :
- d'une étape (212) d'élaboration d'une requête (PI_R) en consultation d'identités digitales publiques (PIWm, PIIj, PIIj') d'entités électroniques (Wm, Iij, Ij') du système de preuve en ligne (S) et de déclenchement de l'émission de ladite requête à destination du registre de confiance (TR) ;
 - d'une étape (213) de réception d'un message de transmission (PI_M) émanant dudit registre de confiance (TR) et de recherche, au sein de celui-ci, de l'identité digitale publique (PIIj) de l'entité électronique émettrice Ij de l'attribut vé-

rifiable à renouveler (VCi).

- [Revendication 11] Procédé (300) selon la revendication 3, pour lequel l'étape (214) de vérification de la signature de la requête en renouvellement par le portefeuille (Wm) d'attributs vérifiables du deuxième sous-procédé (200) est précédée :
- d'une étape (212) d'élaboration d'une requête (PI_R) en consultation d'identités digitales publiques (PIWm, PIIj, PIIj') d'entités électroniques (Wm, IIj, Ij') du système de preuve en ligne (S) et de déclenchement de l'émission de ladite requête à destination du registre de confiance (TR) ;
 - d'une étape (213) de réception d'un message de transmission (PI_M) émanant dudit registre de confiance (TR) et de recherche, au sein de celui-ci, de l'identité digitale publique (PIWm) du portefeuille d'attributs vérifiables (Wm).
- [Revendication 12] Procédé (300) selon l'une quelconque des revendications précédentes, pour lequel l'attribut vérifiable (VC, VCi, VCi+1) caractérise la majorité de l'utilisateur de l'objet électronique (Om) hébergeant le portefeuille (Wm) d'attributs vérifiables.
- [Revendication 13] Procédé (300) selon l'une quelconque des revendications précédentes, pour lequel et pour chaque entité électronique du système de preuve (S) :
- l'identité digitale publique (PIIj, PIIj', PIVn, PIWm) consiste en une clé publique (PKIj, PKIj', PKVn, PKWm) et un identifiant (IDIj, IDIj', IDVn, IDWm) ;
 - l'identité digitale privée consiste en une clé privée (SPKIj, SKIj', SKVn, SKWm) produite conjointement avec ladite clé publique, (PKIj, PKIj', PKVn, PKWm) par la mise en œuvre d'un algorithme cryptographique asymétrique.
- [Revendication 14] Procédé (300) selon la revendication précédente, pour lequel, et pour chaque entité électronique du système de preuve en ligne (S), l'identifiant (IDIj, IDIj', IDVn, IDWm) est un identifiant dé-

centralisé dérivé de ladite clé publique (PKIj, PKIj', PKVn, PKWm) par la mise en œuvre d'un algorithme cryptographique réversible, ladite identité digitale publique (PIIj, PIIj', PIVn, PIWm) se réduisant ainsi en ledit identifiant décentralisé (IDIj, IDIj', IDVn, IDWm) ou en ladite clé publique (PKIj, PKIj', PKVn, PKWm).

[Revendication 15] Produit programme d'ordinateur (P) comportant une ou plusieurs instructions de programme exécutables par une unité de traitement (11) d'un objet électronique hébergeant un portefeuille (Wm) d'attributs vérifiables d'un système de preuve en ligne (S), lesdites instructions de programme étant :

- chargeables dans une mémoire (M, 13) dudit objet électronique (Om) hébergeant un portefeuille (Wm) d'attributs vérifiables ;
- conçues de sorte que leur exécution par ladite unité de traitement (11) provoque la mise en œuvre par ledit portefeuille (Wm) d'attributs vérifiables d'un premier sous-procédé (100) d'un procédé (300) de renouvellement automatique d'un attribut vérifiable (VC, VCi, VCi+1) selon l'une quelconque des revendications 1 à 14.

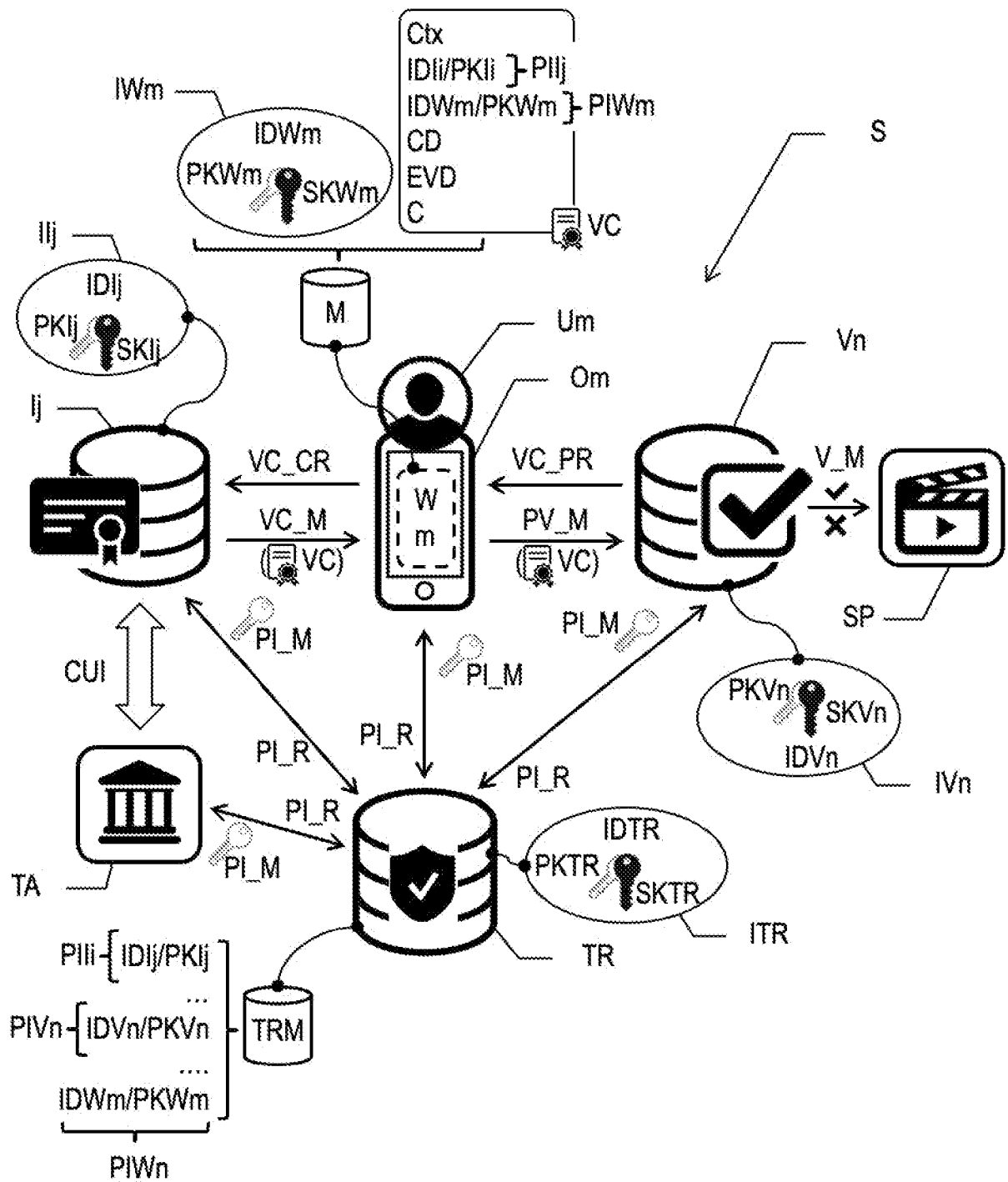
[Revendication 16] Support de mémorisation lisible par un ordinateur comportant les instructions d'un produit programme d'ordinateur selon la revendication précédente.

[Revendication 17] Produit programme d'ordinateur (P) comportant une ou plusieurs instructions de programme exécutables par une unité de traitement (11) d'une entité électronique émettrice (Ij, Ij') d'attributs vérifiables d'un système de preuve en ligne (S), lesdites instructions de programme étant :

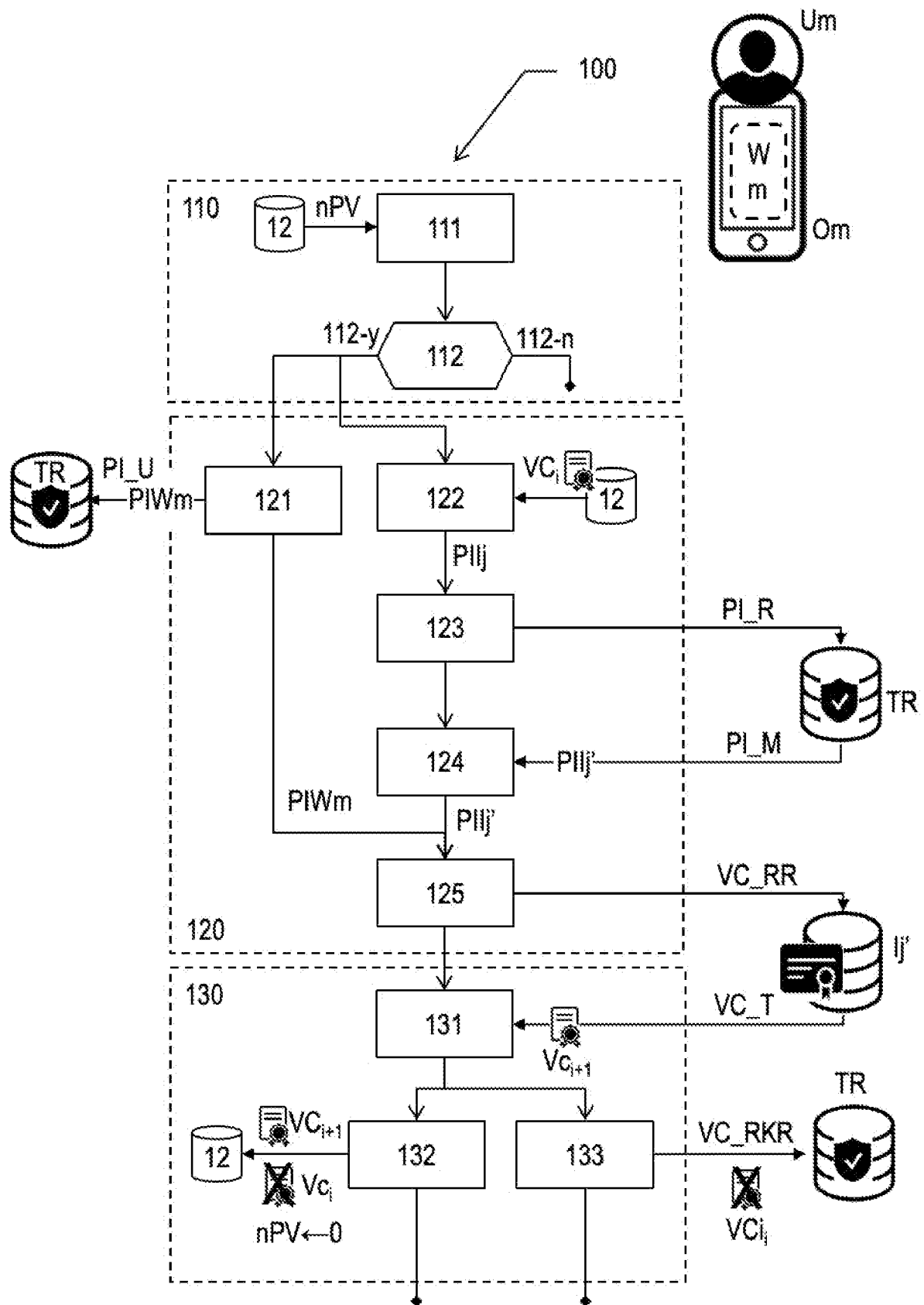
- chargeables dans une mémoire (M, 13) de ladite entité électronique émettrice (Ij, Ij') ;
- conçues de sorte que leur exécution par ladite unité de traitement (11) provoque la mise en œuvre d'un deuxième sous-procédé (200) d'un procédé (300) de renouvellement automatique d'un attribut vérifiable (VC, VCi, VCi+1) selon l'une quelconque des revendications 1 à 14.

- [Revendication 18] Support de mémorisation lisible par un ordinateur comportant les instructions d'un produit programme d'ordinateur selon la revendication précédente.
- [Revendication 19] Objet électronique (Om) comportant une unité de traitement (11), des moyens de communication (14) avec le monde extérieur et une mémoire (M, 13) enregistrant les instructions de programme d'un produit programme d'ordinateur selon la revendication 15.
- [Revendication 20] Entité électronique émettrice (Ij, Ij') d'attributs vérifiables comportant une unité de traitement (11), des moyens de communication (14) avec le monde extérieur et une mémoire (M, 13) enregistrant les instructions de programme d'un produit programme d'ordinateur selon la revendication 17.
- [Revendication 21] Système de preuve en ligne (S) comportant une pluralité d'entités électroniques (Vn, Wm, Ij, Ij') respectivement agencées pour communiquer les unes avec les autres au sein dudit système (S) dont :
- une entité électronique vérificatrice (Vn) d'attributs vérifiables ;
 - un portefeuille (Wm) d'attributs vérifiables mis en œuvre par une unité de traitement (11) d'un objet électronique (Om) détenu par un utilisateur (Um), ledit objet électronique étant agencé selon la revendication 19 ;
 - une entité électronique émettrice (Ij, Ij') d'attributs vérifiables agencée selon la revendication 20.

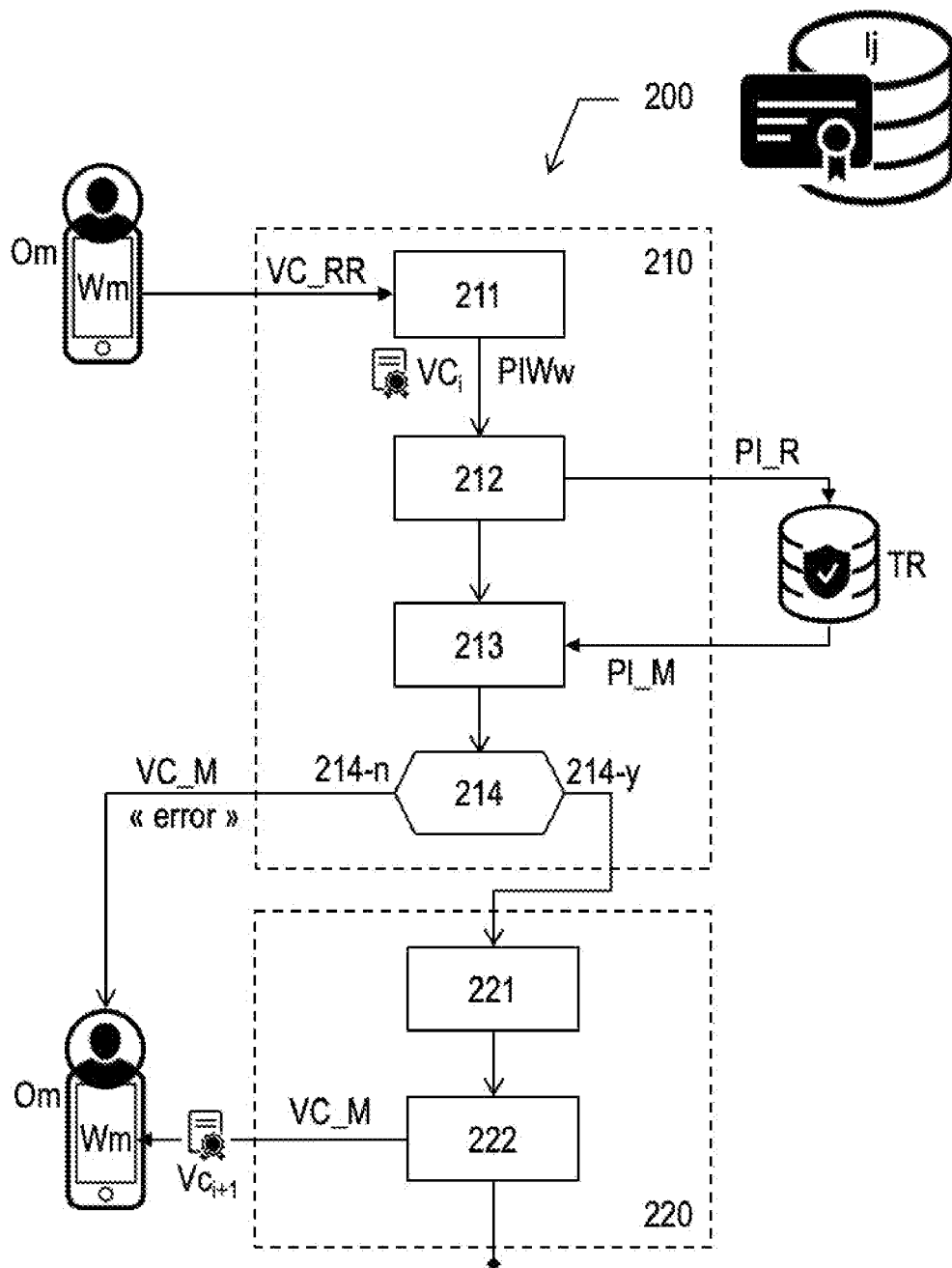
[Fig. 1]



[Fig. 4]



[Fig. 5]



RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement
national

FA 919569
FR 2303600

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	Sporny Manu ET AL: "Verifiable Credentials Data Model v1.1", W3C Recommendation, 3 mars 2022 (2022-03-03), pages 1-122, XP093110283, Extrait de l'Internet: URL:https://www.w3.org/TR/2022/REC-vc-data-model-20220303/ [extrait le 2023-12-08] * section 5.5; pages 8,13; figure 1 * -----	1-21	G06F 21/33 G06F 21/34 H04L 9/30 H04L 9/32
X	US 2020/220726 A1 (LOUGHEED III CHARLES [US] ET AL) 9 juillet 2020 (2020-07-09) * alinéas [0081] - [0085], [0097]; figure 6 * -----	1-21	
X	"Electronic Signatures and Infrastructures (ESI); Policy and Security requirements for Attribute Attestation Services", ETSI DRAFT SPECIFICATION; ESI-0019471V004.DOCX, EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE (ETSI), 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS ; FRANCE no. V0.0.4 3 octobre 2022 (2022-10-03), pages 1-25, XP014444164, Extrait de l'Internet: URL:ftp://docbox.etsi.org/ESI/ESI/70-Drafts/0019471/ESI-0019471v004.docx [extrait le 2022-10-03] * section 4.3.3; pages 9, 10 * ----- -/--	1,15-21	DOMAINES TECHNIQUES RECHERCHÉS (IPC) H04L
Date d'achèvement de la recherche		Examineur	
8 décembre 2023		Manet, Pascal	
CATÉGORIE DES DOCUMENTS CITÉS X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : arrière-plan technologique O : divulgation non-écrite P : document intercalaire T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant			

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement
national

FA 919569
FR 2303600

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	US 2022/385477 A1 (KRAVITZ DAVID WILLIAM [US] ET AL) 1 décembre 2022 (2022-12-01) * alinéas [0059] - [0060] * -----	1, 15-21	
X	US 2022/005047 A1 (MAHESHWARI RAJAT [SG] ET AL) 6 janvier 2022 (2022-01-06) * alinéas [0010], [0018] - [0025]; figure 1 * -----	1, 12, 15-21	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
Date d'achèvement de la recherche		Examineur	
8 décembre 2023		Manet, Pascal	
CATÉGORIE DES DOCUMENTS CITÉS X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : arrière-plan technologique O : divulgation non-écrite P : document intercalaire T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant			

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE **RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 2303600 FA 919569**

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
 Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du **08-12-2023**
 Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche		Date de publication		Membre(s) de la famille de brevet(s)		Date de publication
US 2020220726 A1		09-07-2020	CA	3125621 A1		09-07-2020
			EP	3906512 A1		10-11-2021
			US	2020220726 A1		09-07-2020
			WO	2020142772 A1		09-07-2020

US 2022385477 A1		01-12-2022	US	2022385477 A1		01-12-2022
			WO	2022256181 A1		08-12-2022

US 2022005047 A1		06-01-2022	AUCUN			
