(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** ***3 104 870***
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **19 14489**

(51) Int Cl[8] : ***H 04 L 9/30*** *(2019.12), H 04 L 9/08, G 16 Y 40/50*

(12) **BREVET D'INVENTION** **B1**

(54) Plateforme sécurisée, décentralisée, automatisée et multi-acteurs de gestion d'identités d'objets au travers de l'utilisation d'une technologie de chaîne de blocs.

(22) **Date de dépôt :** 16.12.19.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 18.06.21 Bulletin 21/24.

(45) **Date de la mise à disposition du public du brevet d'invention :** 02.09.22 Bulletin 22/35.

(56) **Liste des documents cités dans le rapport de recherche :**

Se reporter à la fin du présent fascicule

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

◯ **Demande(s) d'extension :**

(71) **Demandeur(s) :** *BULL SAS Société par actions simplifiée* — FR.

(72) **Inventeur(s) :** HÉBERT Guillaume et LEPORINI David.

(73) **Titulaire(s) :** BULL SAS Société par actions simplifiée.

(74) **Mandataire(s) :** IPAZ.

FR 3 104 870 - B1

Description

Titre de l'invention : Plateforme sécurisée, décentralisée, automatisée et multi-acteurs de gestion d'identités d'objets au travers de l'utilisation d'une technologie de chaîne de blocs.

Domaine technique de l'invention

[0001] La présente invention concerne de manière générale le domaine de la Gestion des Identités et des Accès, et plus particulièrement à l'accès automatisé par des objets, de manière sécurisée, à des services numériques, et la protection des échanges qui s'en suivent,

état de la technique antérieure

[0002] Nous sommes aujourd'hui dans un contexte de plein essor de l'internet des objets (IoT) et de sécurisation de ces objets. Une estimation du marché donne le chiffre de 30 milliards comme nombre d'objets connectés à l'IoT d'ici 2020. C'est pourquoi il est donc important de trouver des solutions IoT répondant au besoin de scalabilité pour répondre à la demande, mais également aux aspects de sécurité pour se prémunir des cyberattaques. Les besoins de sécurité associés aux communications des objets (confidentialité, intégrité, authentification et non répudiation) sont couverts par l'utilisation de mécanismes cryptographiques qui se basent sur des jeux de clés et d'identités numériques. Ce gestionnaire de clés et d'identités représente ainsi le cœur de la sécurité du système. Du point de vue des objets, c'est grâce à ce gestionnaire que l'objet est autorisé à émettre sur un réseau et d'accéder à un service applicatif (identification et authentification de l'objet), qu'il est capable d'émettre des messages chiffrés, intègres et authentifiés et qu'il est capable de déchiffrer les données reçues (cryptographie symétrique/asymétrique).

[0003] L'accès automatisé par des objets, de manière sécurisée, à des services numériques, et la protection des échanges qui s'en suivent, nécessitent la mise en place de processus d'enrôlement à la fois pour les fabricants d'objets et pour les objets eux-mêmes, ainsi que leur association aux services numériques en question (« service on-boarding »).

[0004] Ces processus doivent répondre aux problématiques telles que l'identification des objets avec une liste d'attributs associés (incluant notamment des identifiants de sécurité tels que des clés cryptographiques), et leur enregistrement dans un référentiel du Fabricant des objets; Le transfert de la propriété et/ou des droits d'exploitation d'un objet d'un Fabricant à un utilisateur de l'objet (par exemple un fournisseur de service utilisant l'objet) ; Le transfert de la propriété et/ou des droits d'exploitation d'un utilisateur à un autre (cas, par exemple, du besoin de réversibilité) ; La mise à jour des attributs liés à l'identité de l'objet par le propriétaire d'un objet et/ou l'entité en charge

de ses droits d'exploitation.

[0005] De plus, les plateformes qui répondent à ces processus doivent montrer une haute résilience aux pannes, une haute disponibilité et une forte sécurité.

[0006] Avec l'essor des objets connectés (IoT), et particulièrement des objets IoT de petite taille et de faible coût, de nouvelles contraintes, propres à ceux-ci, émergent, telle qu'une taille de mémoire réduite, une faible puissance de calcul, une basse consommation et un possible mode hors ligne ou une déconnexion de l'objet.

[0007] A toutes ces contraintes techniques s'ajoutent des contraintes légales grandissantes, telles que les nouvelles réglementations en vigueur sur la propriété des données (GDPR) et le Privacy by Design (PvD).

[0008] Il existe aujourd'hui plusieurs solutions pour répondre à ces problématiques, à voir les solutions de GIA (Gestion des Identités et des Access) plus communément appelées IAM (Identity Access Management). De nombreuses sociétés de cybersécurité offrent de telles solutions : Active Directory, IBM Security Identity and Access Assurance, Oracle Identity Cloud Service, Okta, Centrify, RSA SecurID Access, Keeper Security, SailPoint, OneLogin, Ping… Néanmoins les différents acteurs de cette liste proposent des solutions centralisées, avec un stockage de données interne qui peut avoir un caractère personnel donc sensible et ainsi ne plus respecter la réglementation GDPR.

[0009] Ces solutions proposent généralement un processus technique centralisé habituellement géré par le fournisseur de services ce qui ne permet pas une automatisation, et des accords bipartites préalables entre les fournisseurs de services et les fabricants d'objets, nécessaire pour permettre l'association des objets aux services du fournisseur.

[0010] L'objet est déjà enregistré et « appairé avec son Manufacturer / Owner ».

[0011] Enfin, ces solutions demandent des capacités de calcul et de stockage suffisamment importantes au niveau de l'objet pour gérer les besoins sécuritaires d'identification et d'authentification au moyen de clés cryptographiques publiques/certificats électroniques. Ces demandes en puissance de calcul, en espace de stockage et en cout énergétique peuvent ne pas être gérées par certains objets IoT qui ont une capacité de calcul et une batterie trop faible pour cela.

Exposé de l'invention

[0012] La présente invention a donc pour objet de proposer un procédé de communication pour la gestion sécurisée de clés et d'identités, permettant de palier au moins une partie des inconvénients de l'art antérieur.

[0013] Ce but est atteint par un procédé de communication pour la gestion sécurisée de clés et d'identités d'un Objet fabriqué par un Fabricant possédant une bi-clé clé publique Kp, clé privée ou secrète Ks de Fabricant (Ks_{man},Kp_{man}) et un client possédant une bi-clé Client (Ks_{client},Kp_{client}), caractérisé en ce que la gestion se fait au moins partiellement

sur une base de données décentralisée de chaine de blocs, et que le procédé comprend les étapes suivantes :

a) Génération par le Fabricant de deux clés symétriques diversifiées à partir de sa bi-clé et de diversifiants, par exemple sous forme de clés AES 128 bits, les deux clés symétriques étant composées d'une clé de confidentialité K0c et d'une clé d'Identité K0i, puis partage desdites clés avec l'objet .

b) Publication et enregistrement dans la base de données de chaine de blocs de l'identifiant décentralisé (decentralized Identifier, DID) de l'objet et préférentiellement du chiffrement des diversifiants utilisés pour obtenir les deux clés symétriques par une clé publique Kp_{man}: et association *du* couple identifiant de l'objet avec le chiffrement de la clé publique Kp_{man} et des diversifiants chiffrés pour former l'information DID – $Enc(Kp_{man},DIV_c||DIV\_ID)$

Et, lorsqu'un Client achète l'objet audit Fabricant, le procédé comprend les étapes d'initialisation suivantes :

c) Fourniture par le Fabricant de l'objet, de l'identifiant de l'objet DID, et des clés symétriques clé de confidentialité K0c et clé d'Identité K0i les clés symétriques étant chiffrées par la clé publique du client kp_{client},au client, préférentiellement par un mécanisme , en dehors de la chaine de blocs, dit « off-chain »;

d) Mise à jour de la chaine de blocs de la base de données par publication et *association dans ladite chaine* de blocs du couple identifiant de l'objet (DID) avec la clé publique du client Kp_{client} et le chiffrement de la clé publique client kp_{client} et des diversifiants chiffrés pour former l'information *DID*-kp_{client} *et* $Enc(Kp_{client},DIV_c||DIV\_ID)$ pour que le client puisse pouvoir recalculer les valeurs des clés de l'objet.

- Et, lorsque l'objet est allumé pour la première fois, l'objet s'auto-enrôle selon les étapes suivantes :

e) Génération de ses nouvelles clés symétriques clé de confidentialité K1c et clé d'Identité K1i par diversification de ses clés anciennes clés K0c, K0i. ;

f) Auto-enrôlement de l'objet est réalisé par un challenge cryptographique mettant en œuvre la clé d'identité

g) Envoi par l'objet au client des deux nouveaux diversifiants chiffrés avec la clé publique du client, l'envoi étant réalisé par un mécanisme en dehors de la chaine de blocs, dit « off-chain »

h) Publication et enregistrement desdits nouveaux diversifiants chiffré avec la clé publique du client dans la chaine de blocs.

[0014] Selon une particularité, le procédé comprend en outre une étape préalable à la génération de bi-clés de fabrication par le Fabricant, dans laquelle ledit Fabricant enregistre son identifiant de Fabricant dans la chaine de blocs et publie sa clé publique de Fabricant (Kp_{man}) en l'associant à son identifiant de Fabricant.

[0015] Selon une autre particularité, le générateur de bi-clés repose sur des portemonnaies de clés hiérarchiques (Hierarchical Key Wallets) pour fournir les bi-clés de fabrication uniques qui sont diversifiées à partir de la bi-clé du Fabricant.

[0016] Selon une autre particularité, les deux clés symétriques générées par le Fabricant sont issues du schéma IES (Integration Encryption Scheme, ou du schéma ECIES (Elliptic Curve Integrated Encryption Scheme), préférentiellement du schéma ECIES, et où le Fabricant génère une bi-clé temporaire dont il utilise la partie publique pour la dérivation desdites deux clés symétriques générées.

[0017] Selon une autre particularité, l'objet est transféré d'un propriétaire à un autre en reprenant les étapes d, g, h, préférentiellement les étapes d à h.

[0018] Selon une autre particularité, le partage ou gestion des droits sur l'objet est opéré par le propriétaire de l'objet au moyen de titres vérifiables (Verifiable Credentials), préférentiellement demandés par les fournisseurs de service (Service Providers) et validés par le propriétaire.

[0019] Selon une autre particularité, un système de preuve à divulgation nulle de connaissance, en anglais (ZKP, Zero Knowledge Proof) est mis en place au sein d'un contrat intelligent, en anglais Smart Contract, pour donner des informations sans en dévoiler les valeurs.

[0020] La présente invention concerne aussi un système de gestion d'identités sécurisées basé sur une chaine de bloc apte à réaliser les étapes d'un processus réalisant :

- L'identification des objets avec une liste d'attributs associés, incluant notamment des identifiants de sécurité tels que des clés cryptographiques, et leur enregistrement dans un référentiel du Fabricant ;
- Le transfert de la propriété et/ou des droits d'exploitation d'un objet d'un Fabricant à un utilisateur de l'objet, par exemple un fournisseur de service utilisant l'objet, par l'enregistrement des nouvelles identités associées à l'objet;
- Le transfert de la propriété et/ou des droits d'exploitation d'un utilisateur à un autre, par l'enregistrement des nouvelles identités associées à l'objet ;
- La mise à jour des attributs liés à l'identité de l'objet par le propriétaire d'un objet et/ou l'entité en charge de ses droits d'exploitation.

[0021] La présente invention concerne aussi une base de donnée, utilisée par le système de gestion d'identités sécurisées basé sur une chaine de bloc, implémenté sur une plateforme sécurisée, décentralisée, automatisée et multi-acteurs de gestion d'identités d'objets au travers de l'utilisation de la technologie de chaîne de blocs mise en œuvre sur plusieurs nœuds du système avec lesquels la plateforme communique , les nœuds étant responsables du maintien de la chaine de blocs et permettent aux acteurs (et aux objets) de consulter l'état de cette chaine et d'interagir avec cette chaine par l'intermédiaire d'un référentiel (ou registre) commun partagé , chaque nœud ayant

accès à un module cryptographique, de préférence physique, en charge du stockage sécurisé de sa clé privée et de l'accès au registre partagé caractérisée en ce que la base de données constitue un référentiel pour chaque fabricant contenant une liste d'attributs associés, incluant notamment des identifiants de sécurité tels que des clés cryptographiques, et soit réalisant leur enregistrement dans le référentiel du Fabricant, soit réalisant la mise à jour des attributs liés à l'identité de l'objet par le propriétaire d'un objet et/ou l'entité en charge de ses droits d'exploitation.

[0022] La présente invention concerne aussi une plateforme sécurisée, décentralisée, automatisée et multi-acteurs de gestion d'identités d'objets utilisant une base de données, caractérisée en ce qu'elle gère :

- Le transfert de la propriété et/ou des droits d'exploitation d'un objet ;
- L'enregistrement de preuves de possession d'objet dans le référentiel partagé ;
- L'activation / réactivation d'objets ;

[0023] Selon une particularité, la technologie de la chaine de bloc utilisée ne doit pas être d'un type précis et comprend au moins :

- un système de permission, pour identifier et authentifier fortement un acteur ;
- un système de contrôle d'accès, basé sur les identités des utilisateurs ;
- un mécanisme d'anti-rejeu ,

chaque nœud maintenant la chaîne de blocs devant se trouver dans un environnement sécurisé, et l'identité publique de chaque nœud doit être mise à disposition des autres nœuds et acteurs au sein du registre partagé; l'exécution de Smart Contract et de fonctions sur la chaine de blocs étant effectuée dans cette sphère sécurisée, l'enregistrement ayant pour finalité de créer un lien, accessible par tout le monde dans la chaine de blocs, pour permettre de faire correspondre l'acteur et son identité digitale par une bi-clé (clé publique et clé privée) ou par un certificat éventuellement signé par un organisme certifié de gestion d'identités.

[0024] La présente invention concerne aussi un système de gestion d'identités sécurisées basé sur une chaine de bloc et apte à réaliser les étapes d'un procédé de communication pour la gestion sécurisée de clés et d'identités, le système comprenant au moins :

un Fabricant, utilisant un système de diversification de clé à partir de diversifiants générés par un générateur de diversifiants, un système de connexion à chaine de blocs, un système d'attribution, à chaque objet sorti de fabrication, d'un identifiant, et un arrangement matériel et logiciel pour envoyer au serveur de chaine de blocs un message de publication et d'enregistrement de l'*association* DID – $Enc(Kp_{man}, DIV_c || DIV\_ID)$.

[0025] La présente invention concerne aussi un système de gestion d'identités sécurisées basé sur une chaine de bloc et apte à réaliser les étapes d'un procédé de communication pour la gestion sécurisée de clés et d'identités, le système comprenant au

moins

Un objet pourvu de moyens de calcul et de moyens de mémorisation d'un programme et de données suffisants pour réaliser les opérations suivantes : lorsque l'objet est allumé pour la première fois, l'objet s'enrôle selon les étapes suivantes :

- Génération de ses nouvelles clés symétriques clé de confidentialité K1c et clé d'Identité K1i par diversification de ses clés anciennes clés K0c, K0i
- Auto-enrôlement par un challenge cryptographique mettant en œuvre la clé d'identité K0i
- Envoi par l'objet au client des deux nouveaux diversifiants chiffré avec la clé publique du client, l'envoi étant réalisé par un mécanisme, en dehors de la base de données de chaines de blocs,
- Publication et enregistrement desdits nouveaux diversifiants chiffré avec la clé publique du client dans la base de données de chaines de blocs

[0026] Selon une autre particularité, un système de partage de clés de confidentialité est mis en place « off-chain », afin que les opérateurs de service aient accès à l'objet, et donc aux informations relatives.

[0027] La présente invention concerne aussi un système de gestion d'identités d'un fournisseur de service d'identité (ID service provider) mettant en œuvre une chaîne de blocs « block-chain » et utilisant les objets enregistrés sur un réseau pour remplir des services applicatifs (SA) dans lesquels les informations fournies par les objets sont utilisées, chaque nœud du réseau du fournisseur de service d'identité a accès à un module cryptographique en charge du stockage sécurisé de sa clé privée, les nœuds possédant des client appelés Acteurs ayant chacun leur propre identité ID_{act} enregistrée dans la chaine de bloc, chaque fabricant d'objet est enregistré dans la chaîne de blocs « block-chain » du fournisseur de service d'identité et leur clé publique sont connues de tous, pour chaque objet vendu ou transféré chaque fabricant fournit l'identifiant de l'objet et le chiffrement des diversifiants utilisé par le fabricant pour le calcul des clés symétriques de chaque objet par publication dans la chaîne de bloc « block-chain », seules les clés symétriques restent stockées en dehors de la chaîne, en l'occurrence dans l'objet ;

Chaque objet étant pourvu de moyens de calcul et de moyens de mémorisation d'un programme et de données suffisants pour exécuter les opérations suivantes : lorsque l'objet est allumé pour la première fois, l'objet s'enrôle auprès du fournisseur de service d'identité en réalisant les étapes suivantes :

- Génération dans l'objet de ses nouvelles clés symétriques clé de confidentialité K1c et clé d'Identité K1i par diversification de ses clés anciennes clés K0c, K0i,
- Auto-enrôlement par un challenge cryptographique mettant en œuvre la clé

d'identité.

- Envoi par l'objet au client des deux nouveaux diversifiants chiffrés avec la clé publique du client, l'envoi étant réalisé par un mécanisme, en dehors de la chaine de blocs,
- Publication et enregistrement desdits nouveaux diversifiants chiffrés avec la clé publique du client dans la chaine de blocs.

[0028] La présente invention concerne aussi un objet pourvu de moyens de calcul et de moyens de mémorisation d'un programme et de données suffisants pour exécuter les opérations suivantes : lorsque l'objet est allumé pour la première fois, l'objet s'enrôle auprès du fournisseur de service d'identité en réalisant les étapes suivantes :

- Génération dans l'objet de ses nouvelles clés symétriques clé de confidentialité K1c et clé d'Identité K1i par diversification de ses clés anciennes clés K0c, K0i,
- Auto-enrôlement par un challenge cryptographique mettant en œuvre la clé d'identité.
- Envoi par l'objet au client des deux nouveaux diversifiants chiffrés avec la clé publique du client, l'envoi étant réalisé par un mécanisme, en dehors de la chaine de blocs,
- Publication et enregistrement desdits nouveaux diversifiants chiffrés avec la clé publique du client dans la chaine de blocs.

Brève description des figures

[0029] D'autres caractéristiques, détails et avantages de l'invention ressortiront à la lecture de la description qui suit en référence aux figures annexées, qui illustre :

- [Fig. 1], représente un mode de réalisation du procédé de façon schématique.
- [Fig. 2], représente les étapes a) et b) du procédé selon certains modes de réalisation,
- [Fig. 3], représente les étapes c) et d) du procédé selon certains modes de réalisation,
- [Fig. 4], représente, les étapes e), f), g) et h) du procédé selon certains modes de réalisation,

description detaillee de l'invention

[0030] De nombreuses combinaisons peuvent être envisagées sans sortir du cadre de l'invention ; l'homme de métier choisira l'une ou l'autre en fonction des contraintes économiques, ergonomiques, dimensionnelles ou autres qu'il devra respecter.

[0031] De manière générale, la présente invention comporte un procédé de communication pour la gestion sécurisée de clés et d'identités d'un Objet fabriqué par un Fabricant possédant une bi-clé clé publique Kp, clé privée ou secrète Ks de Fabricant (Ks_{man},Kp

$_{man}$) et un client possédant une bi-clé Client (Ks_{client},Kp_{client}), caractérisé en ce que la gestion se fait au moins partiellement sur une base de données décentralisée de chaine de blocs, et que le procédé comprend les étapes suivantes :

a) Génération par le Fabricant de deux clés symétriques diversifiées à partir de sa bi-clé et de diversifiants, par exemple sous forme de clés AES 128 bits, les deux clés symétriques étant composées d'une clé de confidentialité K0c et d'une clé d'Identité K0i, puis partage desdites clés avec l'objet .

b) Publication et enregistrement dans la base de données de chaine de blocs de l'identifiant décentralisé (decentralized Identifier, DID) de l'objet et préférentiellement du chiffrement des diversifiants utilisés pour obtenir les deux clés symétriques par une clé publique Kp_{man}: et association du couple identifiant de l'objet avec le chiffrement de la clé publique Kp_{man} et des diversifiants chiffrés pour former l'information DID – $Enc(Kp_{man},DIV_c||DIV\_ID)$

Et, lorsqu'un Client achète l'objet audit Fabricant, le procédé comprend les étapes d'initialisation suivantes :

c) Fourniture par le Fabricant de l'objet, de l'identifiant de l'objet DID, et des clés symétriques clé de confidentialité K0c et clé d'Identité K0i les clés symétriques étant chiffrées par la clé publique du client kp_{client},au client, par un mécanisme , en dehors de la chaine de blocs, dit « off-chain »;

d) Mise à jour de la chaine de blocs de la base de données par publication et association dans ladite chaine de blocs du couple identifiant de l'objet (DID) avec la clé publique du client Kp_{client} et le chiffrement de la clé publique client kp_{client} et des diversifiants chiffrés pour former l'information *DID*-kp_{client} *et* $Enc(Kp_{client},DIV_c||DIV\_ID)$ pour que le client puisse pouvoir recalculer les valeurs des clés de l'objet.

[0032] Dans certains modes de réalisation, dans le procédé, lorsque l'objet est allumé pour la première fois l'objet s'auto-enrôle selon les étapes suivantes :

e) Génération de ses nouvelles clés symétriques clé de confidentialité K1c et clé d'Identité K1i par diversification de ses clés anciennes clés K0c, K0i. ;

f) Auto-enrôlement de l'objet est réalisé par un challenge cryptographique mettant en œuvre la clé d'identité

g) Envoi par l'objet au client des deux nouveaux diversifiants chiffrés avec la clé publique du client, l'envoi étant réalisé par un mécanisme en dehors de la chaine de blocs, dit « off-chain »

h) Publication et enregistrement desdits nouveaux diversifiants chiffré avec la clé publique du client dans la chaine de blocs.

[0033] Avantageusement, La première clé, clé de confidentialité K0c, étant nécessaire pour le chiffrement des données, et la seconde clé, clé d'Identité K0i, étant nécessaire pour l'authentification sur la chaine de blocs.

[0034] Ces clés peuvent être issues du schéma IES (Integrated Encryption Scheme), où l'on préfèrera utiliser le schéma ECIES (Elliptic Curve Integrated Encryption Scheme) plus adapté à l'IoT que le schéma DLIES (Discrete Logarithm Integrated Encryption Scheme). Dans ce cas de figure, le Fabricant est obligé de générer une bi-clé temporaire et d'utiliser la partie publique pour la dérivation. Ces deux clés symétriques sont calculées par une fonction de dérivation de clé qui prend en argument la clé publique temporaire gt générée par le Fabricant et dérivée à partir de la bi-clé du *Fabricant* (g^f, f) par un diversifiant.

[0035] En d'autres termes, dans ce mode de réalisation, une clé publique temporaire est générée par le fabricant de manière aléatoire. Elle est dérivée à partir de deux objets : la bi-clé du fabricant et un diversifiant. Le résultat de la dérivation avec un premier diversifiant est un nouvel objet : une clé symétrique K de confidentialité. Le résultat de la dérivation avec un second diversifiant est un nouvel objet : une clé symétrique K d'identité.

[0036] Dans certains modes de réalisation, chaque publication dans la chaine de blocs équivaut à au moins une transaction dans celle-ci

[0037] Le diversifiant DIV pourrait ne pas être publié dans la Blockchain, mais par mesure de sécurité il l'est. En effet cela permet au Fabricant de ne pas stocker la Bi-clé de fabrication, et d'être ainsi obligé de la recalculer au besoin.

[0038] Il existe une relation qui permet de faire l'association entre le DID et le DIV. Ainsi, n'importe quel acteur est ainsi capable de retrouver le DIV s'il connait le DID. Le DIV est nécessaire puisqu'il permet au fabricant de recalculer la clé : DIV pour diversifiant. Une clé diversifiée s'obtient à partir d'une clé et d'un diversifiant : la clé est connue du fabricant et le diversifiant est stockée dans la blockchain.

[0039] Dans certains modes de réalisation, le chiffrement des diversifiants est réalisé avec la clé publique du fabricant (seul le fabricant porteur de la clé privée peut ainsi déchiffrer)

[0040] La preuve d'appartenance de l'objet se fait intrinsèquement car le propriétaire/ fabricant est le seul à posséder la clé privée associée à la clé publique référencée.

[0041] Avantageusement, l'objet est capable de s'auto-enrôler et signe le message d'enrôlement avec la clé de fabrication (Ks_{fab}) qu'il est le seul à posséder.

[0042] Dans certains modes de réalisation, la fourniture des données, notamment de l'identifiant de l'objet DID, et des clés symétriques clé de confidentialité K0c et clé d'Identité K0i chiffrées, est réalisée par une transmission off-chain.

[0043] L'objectif de la fourniture de cette clé par le fabricant au client acquéreur de l'objet est double. Cela permet à l'acquéreur d'identifier l'objet (même si le DID l'identifie également). Cela permet également à l'acquéreur de vérifier que l'objet appartenait bien au fabricant car seul le fabricant possède lesdites clés pertinentes.

[0044] On entend par une fourniture ou un envoi de données « off-chain », une fourniture ou envoi de données par un mécanisme extérieur à la chaine de blocs, de façon à améliorer la sécurité et la confidentialité de données particulièrement sensibles. On entend par là par exemple un envoi sécurisé par mail, la mise à disposition sur un serveur de stockage sécurisé, l'envoi d'une clé USB avec les données sécurisées, ou encore d'autres moyens possibles envisageables par l'Homme du métier qui répondent à la problématique donnée.

[0045] De manière alternative, il serait possible, mais moins sûr, d'envoyer les nouveaux diversifiants lors de l'étape e) directement au Smart Contract qui les chiffre avec la clé publique du client.

[0046] Le mécanisme devra impérativement sécuriser ces diversifiants : chiffrement de la donnée par l'émetteur avec la clé publique du destinataire par exemple.

[0047] Avantageusement, le chiffrement des clés symétriques est réalisé par le Fabricant.

[0048] Avantageusement, le remplacement (mise à jour), c'est-à-dire la publication et enregistrement dans la chaine de blocs est réalisée par une mise à jour de la chaine de blocs (Blockchain) via une transaction. La Blockchain est comme un registre d'état : mis à jour de l'état d'une valeur, donc remplacement via une transaction. L'ancien état est gardé (paradigme blockchain) mais n'est plus à jour.

[0049] Dans certains modes de réalisation, l'objet accède au registre partagé via le nœud de son Fabricant, avec sa clé d'Identité K0i qui lui donne les droits nécessaires pour faire le processus d'enrôlement. Cette clé symétrique est connue uniquement du Fabricant, de l'objet et du Client, l'objet est authentifié par la Blockchain : la vérification est faite par le Smart Contract, via un challenge uniquement réalisable par les seuls porteurs de la clé d'identité K0i (p.ex., en utilisant un mécanisme de type HMAC).

[0050] Un challenge cryptographique est un mécanisme d'authentification qui met en œuvre un secret, ici une clé. La fonction HMAC citée permet d'authentifier l'émetteur d'une donnée et d'assurer l'intégrité de la donnée.

[0051] On comprend par base de données décentralisée « blockchain », ou « chaine de de blocs », une base de données décentralisée comprenant un réseau de chaines de blocs, avec des nœuds comprenant tout ou partie du registre de chaine de blocs. Avantageusement, pour garder une trace de toutes les transactions, le réseau de chaines de blocs utilise le registre à chaînes multiples qui est répliqué sur tous les nœuds homologues du réseau de chaines de blocs. La blockchain est une liste de blocs, chacun contenant plusieurs transactions. Chaque bloc a un pointeur sur le bloc précédent et l'ordre et le contenu des blocs sont protégés par des signatures de hachage. Les nœuds d'exploitation de bitcoins construisent de nouveaux blocs à partir des transactions entrantes. Cette construction est rendue difficile à réaliser et nécessite des calculs par minage considérables, la preuve du travail. Les efforts déployés rendent tout aussi

difficile de changer des blocs déjà inclus dans la chaine de blocs (blockchain), d'autant plus que changer un bloc au milieu de la chaîne nécessiterait la recréation de tous les blocs suivants. Ainsi, le registre de la chaine de blocs est bien protégé des modifications et peut être considéré comme un enregistrement permanent des transactions. Afin d'inciter à l'effort de minage, les mineurs sont récompensés par les bitcoins nouvellement créés lors de la création d'un bloc. Ils reçoivent également tous les frais de transaction des transactions incluses dans le nouveau bloc.

[0052] La technologie de chaîne de blocs est utilisée comme un référentiel partagé et distribué d'identités incluant une liste d'attributs publics associés. Ces identités peuvent, à titre d'illustration, utilisées le format DID défini dans la spécification « Decentralized Identifiers (DIDs) »

[0053] Le système ne repose préférentiellement par sur une blockchain publique, et pas sur une blockchain avec un proof of work, qui nécessite de la puissance de calcul et de l'énergie dans un cas d'usage IoT (des objets présentant des contraintes de basse consommation et de faible puissance de calcul). Au contraire, la solution se base préférentiellement sur une blockchain de consortium / blockchain d'entreprise / blockchain à permission /blockchain POK (Proof of Knowledge, preuve de connaissance en français).

[0054] L'invention porte sur un système ou une plateforme sécurisée, décentralisée, automatisée et multi-acteurs de gestion d'identités d'objets au travers de l'utilisation d'une technologie de chaîne de blocs. En d'autres termes, sur un système de chaine de blocs afin de bénéficier de ses avantages : scalabilité, réplication, résilience aux pannes/attaques tout en ajoutant une couche supplémentaire pour l'IAM et la GIA lié à l'identité des entités.

[0055] Ces modes de réalisations n'ont donc pas besoin d'acteurs supplémentaires, de serveurs annexes, seulement les acteurs directs (Fabricant, Client, Objet), d'une base de données décentralisée blockchain, et potentiellement d'un fournisseur de service. Avantageusement, les nœuds de la chaine de blocs ne sont utilisés que pour stocker des données et les mettre à jour via des transactions effectuées sur ladite chaine de blocs.

[0056] Certaines solutions prévoient la présence d'un DM (device Manager), tandis que dans le présent système, l'enregistrement est déjà fait et l'enrôlement sur le réseau est à l'initiative de l'objet. L'objet autonome grâce au DID.

[0057] Dans certains modes de réalisation, le procédé comprend en outre une étape préalable à la génération de bi-clés de fabrication par le Fabricant, dans laquelle ledit Fabricant enregistre son identifiant de Fabricant dans la chaine de blocs et publie sa clé publique de Fabricant (Kp_{man}) en l'asssociant à son identifiant de Fabricant.

[0058] Dans certains modes de réalisation, le générateur de bi-clés repose sur des porte-monnaies de clé hiérarchiques (Hierarchical Key Wallets) pour fournir les bi-clés de

fabrication uniques qui sont diversifiées à partir de la bi-clé du Fabricant.

[0059] Dans certains modes de réalisation, les deux clés symétriques générées par le Fabricant sont issues du schéma IES (Integration Encryption Scheme, ou du schéma ECIES (Elliptic Curve Integrated Encryption Scheme), préférentiellement du schéma ECIES, et où le Fabricant génère une bi-clé temporaire dont il utilise la partie publique pour la dérivation desdites deux clés symétriques générées.

[0060] Dans certains modes de réalisation, l'objet est transféré d'un propriétaire à un autre en reprenant les étapes d, g, h, préférentiellement les étapes d à h.

[0061] Dans un tel cas (second transfert de propriétaire, ou ultérieur), l'étape e) (génération d'une nouvelle paire de clés Kc et Ki) peut être rendue optionnelle, et être effectuée ou non par le nouveau propriétaire. En effet, seul l'objet a connaissance de sa clé privée, ce qui en théorie ne l'oblige pas à faire ce changement. La génération de cette nouvelle double clé et le changement associé est cependant préféré pour diverses raisons sécuritaires.

[0062] Dans certains modes de réalisation, le partage ou gestion des droits sur l'objet est opéré par le propriétaire de l'objet au moyen de titres vérifiables (Verifiable Credentials), préférentiellement demandés par les fournisseurs de service (Service Providers) et validés par le propriétaire.

[0063] Les Verifiable Credentials et les DID Documents (Decentralized IDentifiers) seront utilisés respectivement comme moyen de contrôle d'accès et de format de stockage des informations liés à l'objet sur la chaine de blocs. Le premier permettant de donner les accès en lecture aux informations de l'objet en fonction de l'identité du pair.

[0064] Dans certains modes de réalisation, dans le procédé, un système de Preuve à divulgation nulle de connaissance, en anglais (ZKP, Zero Knowledge Proof) est mis en place au sein d'un contrat intelligent, en anglais Smart Contract, pour donner des informations sans en dévoiler les valeurs.

[0065] Le ZPK est une méthode qui permet à une entité de prouver à une autre qu'une proposition est vraie sans en dévoiler la valeur. Cela permet, dans un souci de préservation des données, de répondre à une question sans dévoiler la valeur. Par exemple, un service peut demander à un objet si sa température est inférieure ou supérieure à 0°C sans que l'objet n'ait à dévoiler la valeur de sa température. Cela permet ainsi une optimisation sur l'utilisation du service, et non dans les étapes.

[0066] On entend par Smart Contract ou contrat intelligent un protocole/programme digitale unique et répliqué qui permet d'effectuer des opérations sur la blockchain, et que cela se fasse en respectant des règles bien définies.

[0067] Ainsi, toutes les inscriptions/publications dans la chaine de blocs passent par des Smart Contract. Les règles d'accès sont aussi régies par des Smart Contracts.

[0068] Divers modes de réalisations décrits portent aussi sur un système de gestion

d'identités sécurisées basé sur une chaine de bloc.

[0069] Ainsi, dans certains modes de réalisation, un système de gestion d'identités sécurisées basé sur une chaine de blocs est apte à réaliser les étapes d'un processus réalisant :

- L'identification des objets avec une liste d'attributs associés, incluant notamment des identifiants de sécurité tels que des clés cryptographiques, et leur enregistrement dans un référentiel du Fabricant ;
- Le transfert de la propriété et/ou des droits d'exploitation d'un objet d'un Fabricant à un utilisateur de l'objet, par exemple un fournisseur de service utilisant l'objet, par l'enregistrement des nouvelles identités associées à l'objet;
- Le transfert de la propriété et/ou des droits d'exploitation d'un utilisateur à un autre, par l'enregistrement des nouvelles identités associées à l'objet ;
- La mise à jour des attributs liés à l'identité de l'objet par le propriétaire d'un objet et/ou l'entité en charge de ses droits d'exploitation.

[0070] Ainsi, il peut être mis en place un système, ou une plateforme sécurisée, décentralisée, automatisée et multi-acteurs de gestion d'identités d'objets au travers de l'utilisation d'une technologie de chaîne de blocs, permettant l'accès automatisé par des objets, de manière sécurisée, à des services numériques, et l'assurance d'une protection des échanges qui s'en suivent.

[0071] Divers modes de réalisations décrits portent aussi sur une base de données, utilisée par le système de gestion d'identités sécurisées basé sur une chaine de bloc.

[0072] Ainsi, certains modes de réalisation portent sur une base de données, utilisée par le système de gestion d'identités sécurisées basé sur une chaine de bloc, implémenté sur une plateforme sécurisée, décentralisée, automatisée et multi-acteurs de gestion d'identités d'objets au travers de l'utilisation de la technologie de chaîne de blocs mise en œuvre sur plusieurs nœuds du système avec lesquels la plateforme communique, les nœuds étant responsables du maintien de la chaine de blocs et permettent aux acteurs (et aux objets) de consulter l'état de cette chaine et d'interagir avec cette chaine par l'intermédiaire d'un référentiel (ou registre) commun partagé , chaque nœud ayant accès à un module cryptographique, de préférence physique, en charge du stockage sécurisé de sa clé privée et de l'accès au registre partagé caractérisée en ce que la base de données constitue un référentiel pour chaque fabricant contenant une liste d'attributs associés, incluant notamment des identifiants de sécurité tels que des clés cryptographiques, et soit réalisant leur enregistrement dans le référentiel du Fabricant, soit réalisant la mise à jour des attributs liés à l'identité de l'objet par le propriétaire d'un objet et/ou l'entité en charge de ses droits d'exploitation.

[0073] Divers modes de réalisations décrits portent aussi sur une plateforme sécurisée, décentralisée, automatisée et multi-acteurs de gestion d'identités d'objets utilisant une

base de données décentralisée.

[0074] Dans certains modes de réalisation, une plateforme sécurisée, décentralisée, automatisée et multi-acteurs de gestion d'identités d'objets utilisant une base de données décentralisée gère :

- Le transfert de la propriété et/ou des droits d'exploitation d'un objet ;
- L'enregistrement de preuves de possession d'objet dans le référentiel partagé ;
- L'activation / réactivation d'objets ;

[0075] Dans certains modes de réalisation, la technologie de la chaine de bloc utilisée ne doit pas être d'un type précis. Dans certains modes de réalisation, la technologie de la chaine de bloc utilisée comprend au moins :

- un système de permission, pour identifier et authentifier fortement un acteur ; - un système de contrôle d'accès, basé sur les identités des utilisateurs ;
- un mécanisme d'anti-rejeu ,

Chaque nœud maintenant la chaîne de blocs devant se trouver dans un environnement sécurisé, et l'identité publique de chaque nœud doit être mise à disposition des autres nœuds et acteurs au sein du registre partagé; l'exécution de Smart Contract et de fonctions sur la chaine de blocs étant effectuée dans cette sphère sécurisée, l'enregistrement ayant pour finalité de créer un lien, accessible par tout le monde dans la chaine de blocs, pour permettre de faire correspondre l'acteur et son identité digitale par une bi-clé, clé publique et clé privée, ou par un certificat éventuellement signé par un organisme certifié de gestion d'identités.

[0076] Une attaque par rejeu (en anglais, replay attack ou playback attack) est une forme d'attaque réseau dans laquelle une transmission est malicieusement répétée par un attaquant qui a intercepté la transmission. Il s'agit d'un type d'usurpation d'identité.

[0077] Dans certains modes de réalisation, le système comprend au moins :

un Fabricant, utilisant un système de diversification de clé à partir de diversifiants générés par un générateur de diversifiants, un système de connexion à chaine de blocs, un système d'attribution, à chaque objet sorti de fabrication, d'un identifiant, et un arrangement matériel et logiciel pour envoyer au serveur de chaine de blocs un message de publication et d'enregistrement de l'*association* DID – $Enc(Kp_{man}, DIV_c||DIV\_ID)$.

le système apte à demander à un fournisseur de service la mise à jour de la chaine de blocs dans la base de données par publication et *association dans ladite chaine de blocs du couple identifiant de l'objet (DID) avec* la clé publique du client Kp_{client}*et le chiffrement de la clé publique client* kp_{client} et des diversifiants chiffrés pour former l'information *DID*-kp_{client} *et* $Enc(Kp_{client}, DIV_c||DIV\_ID)$ l'*association DID-DIV et Kp* $_{client}$ ..

[0078] L'inscription, aussi appelée personnalisation, est faite une seule et unique fois par le fabricant. L'objet se met à jour de lui-même dans les étapes suivant la fabrication, en

l'occurrence notamment lorsqu'il est acheté/cédé.

[0079] Le diversifiant DIV pourrait ne pas être publié dans la Blockchain, mais par mesure de sécurité il l'est. En effet cela permet au Fabricant de ne pas stocker la Bi-clé de fabrication, et d'être ainsi obligé de la recalculer au besoin.

[0080] Dans certains modes de réalisation, l'objet, une fois acheté, est apte à demander à un fournisseur de service la mise à jour de la chaine de blocs dans la base de données par publication et association dans ladite chaine de blocs du couple identifiant de l'objet (DID) avec la clé publique du client Kp_{client} et le chiffrement de la clé publique client kp_{client} et des diversifiants chiffrés pour former l'information *DID*-kp_{client} *et* Enc(*Kp client* ,DIV_c||DIV_ID) l'*association DID-DIV et Kp client* .

[0081] Dans certains modes de réalisation, le système comprend au moins :

Un objet pourvu de moyens de calcul et de moyens de mémorisation d'un programme et de données suffisants pour réaliser les opérations suivantes : lorsque l'objet est allumé pour la première fois, l'objet s'enrôle selon les étapes suivantes :

- Génération de ses nouvelles clés symétriques clé de confidentialité K1c et clé d'Identité K1i par diversification de ses clés anciennes clés K0c, K0i
- Auto-enrôlement par un challenge cryptographique mettant en œuvre la clé d'identité K0i
- Envoi par l'objet au client des deux nouveaux diversifiants chiffré avec la clé publique du client, l'envoi étant réalisé par un mécanisme, en dehors de la base de données de chaines de blocs,
- Publication et enregistrement desdits nouveaux diversifiants chiffré avec la clé publique du client dans la base de données de chaines de blocs.

[0082] Dans certains modes de réalisation, un système de partage de clés de confidentialité est mis en place « off-chain », afin que les opérateurs de service aient accès à l'objet, et donc aux informations relatives.

[0083] Dans certains modes de réalisation, un système de gestion d'identités d'un fournisseur de service d'identité (ID service provider) met en œuvre une chaîne de blocs « block-chain » et utilise les objets enregistrés sur un réseau pour remplir des services applicatifs (SA) dans lesquels les informations fournies par les objets sont utilisées, chaque nœud du réseau du fournisseur de service d'identité a accès à un module cryptographique en charge du stockage sécurisé de la clé privée dudit nœud, les nœuds possédant des client appelés Acteurs ayant chacun leur propre identité ID_{act} enregistrée dans la chaine de bloc, chaque fabricant d'objet est enregistré dans la chaîne de blocs « block-chain » du fournisseur de service d'identité et les clés publiques de fabrication des fabricants sont connues de tous, pour chaque objet vendu ou transféré, chaque fabricant fournit l'identifiant de l'objet et un diversifiant utilisé par le fabricant (DID, DIV) pour le calcul des bi-clés de fabrication de chaque objet

par le fabricant, et seul l'identifiant de l'objet et la clé publique de fabrication sont publiés dans la chaîne de bloc « block-chain », seule la clé privée de fabrication reste stockée en dehors de la chaîne, en l'occurrence dans l'objet ;
Chaque objet étant pourvu de moyens de calcul et de moyens de mémorisation d'un programme et de données suffisants pour exécuter les opérations suivantes : lorsque l'objet est allumé pour la première fois, l'objet s'enrôle auprès du fournisseur de service d'identité en réalisant les étapes suivantes :

- Génération dans l'objet de ses nouvelles clés symétriques clé de confidentialité K1c et clé d'Identité K1i par diversification de ses clés anciennes clés K0c, K0i,
- Auto-enrôlement par un challenge cryptographique mettant en œuvre la clé d'identité.
- Envoi par l'objet au client des deux nouveaux diversifiants chiffrés avec la clé publique du client, l'envoi étant réalisé par un mécanisme, en dehors de la chaine de blocs,
- Publication et enregistrement desdits nouveaux diversifiants chiffrés avec la clé publique du client dans la chaine de blocs.

[0084] Dans certains modes de réalisation, un objet pourvu de moyens de calcul et de moyens de mémorisation d'un programme et de données suffisants pour exécuter les opérations suivantes : lorsque l'objet est allumé pour la première fois, l'objet s'enrôle auprès du fournisseur de service d'identité en réalisant les étapes suivantes :

- Génération dans l'objet de ses nouvelles clés symétriques clé de confidentialité K1c et clé d'Identité K1i par diversification de ses clés anciennes clés K0c, K0i,
- Auto-enrôlement par un challenge cryptographique mettant en œuvre la clé d'identité.
- Envoi par l'objet au client des deux nouveaux diversifiants chiffrés avec la clé publique du client, l'envoi étant réalisé par un mécanisme, en dehors de la chaine de blocs,
- Publication et enregistrement desdits nouveaux diversifiants chiffrés avec la clé publique du client dans la chaine de blocs.

[0085] Le système comprend ainsi un gestionnaire d'identités sécurisées basé sur une chaine de blocs dans laquelle sont publiées les identités ou le processus permettant de retrouver ces identités. Les nœuds du registre partagé maintiennent ainsi une chaine de blocs et, par extrapolation, le gestionnaire d'identités.

[0086] Ainsi, il peut être mis en place un système, ou une plateforme sécurisée, décentralisée, automatisée et multi-acteurs de gestion d'identités d'objets au travers de l'utilisation d'une technologie de chaîne de blocs, permettant l'accès automatisé par

des objets, de manière sécurisée, à des services numériques, et l'assurance d'une protection des échanges qui s'en suivent.

[0087] Ce système peut être mis en place pour des Objets IoT présentant une faible capacité de calcul, une faible capacité de stockage et/ou des contraintes de faible consommation d'énergie.

[0088] Dans certains modes de réalisation, et en résumé, les fabricants sont enregistrés dans la Blockchain, et leurs clés publiques respectives sont connues de tous. Ils fabriquent et personnalisent des Objets avec des identifiants et des clés de symétriques uniques. Pour chaque objet, ils publient dans la Blockchain l'identifiant de l'objet, et le chiffré des diversifiants utilisés pour la génération. Les objets IoT sont susceptibles de ne pouvoir utiliser que des mécanismes de cryptographie symétrique. Pour s'identifier, ils doivent utiliser des challenges cryptographiques qui impliquent des clés secrètes. Le Client opère l'Objet et doit donc avoir connaissance des clés secrètes, afin de pouvoir communiquer avec l'Objet et gérer les droits d'accès. La [fig.1] illustre ainsi cela à titre d'exemple et de manière non limitative en récapitulant les différentes étapes clés de certains modes de réalisation.

[0089] Plus particulièrement, la [fig.2] illustre un exemple de mode de réalisation non limitatif de la présente invention, dans lequel sont représentées les étapes a) et b). L'étape a) concerne la génération des deux clés symétriques par le Fabricant, qque celui-ci partagera avec l'objet, les deux clés symétriques étant diversifiées à partir de la bi-clé du Fabricant et de diversifiants, par exemple sous forme de clés AES 128 bits, les deux clés symétriques étant composées d'une clé de confidentialité K0c et d'une clé d'Identité K0i (Etape I-1), et l'initialisation de l'objet avec ces clés symétriques (Etape I-2). L'étape b) concerne la publication et enregistrement dans la chaine de blocs du DID et du chiffrement des diversifiants utilisés pour obtenir les deux clés symétriques pour former l'information DID – Enc(kpman,DIVc||DIV_ID) (Etape II). Ainsi le script avec une double signature permet de différencier le propriétaire de l'objet de celui qui a créé l'objet. Cela permet également de contrôler que celui qui écrit cette transaction est bel et bien celui qui a créé l'objet.

[0090] Par simplification, la bi-clé temporaire g^t qui est un des mécanismes possibles pour la génération de ces clés secrètes, n'apparait pas volontairement dans les schémas et les explications. Il en est de même pour les clés symétriques qui sont des « clés maîtres ». Tous les mécanismes de signature et de chiffrement les impliquant, nécessitent qu'elles soient diversifiées par leurs diversifiants associés.

[0091] La [fig.3] illustre un exemple de mode de réalisation non limitatif de la présente invention, dans lequel sont représentées les étapes c) et d) correspondant aux étapes réalisées lorsqu'un Client achète l'objet audit Fabricant (Etape III-1). La fourniture des données par le Fabricant au client par un mécanisme « off-chain » n'est pas représenté.

La preuve d'appartenance de l'objet se fait intrinsèquement car le propriétaire est le seul à posséder la clé privée associée à la clé publique référencée. Lors de l'échange entre le Client et le Fabricant, le client prouve qu'il est bien le propriétaire de la clé publique en insérant sa signature (Etape III-2). Le Fabricant met à jour le référentiel commun en publiant la clé publique associée au Client Kpclient et le chiffrement de la clé publique client kpclient et des diversifiants chiffrés pour former l'information DID-kpclient et Enc(Kpclient,DIVc||DIV_ID) pour que le client puisse pouvoir recalculer les valeurs des clés de l'objet (Etape III-3).

[0092] Enfin, la [fig.4] illustre un exemple de mode de réalisation non limitatif de la présente invention, dans lequel sont représentées les étapes e), f), g) et h), correspondant aux étapes réalisées lorsque l'objet est allumé pour la première fois, et s'auto-enrôle. En effet, une fois allumé, l'objet réalise la génération de nouvelles clés symétriques (Etape IV-1). L'objet s''auto-enrôle ensuite par un challenge cryptographique mettant en œuvre la clé d'identité K0i (Etape IV-2). L'envoi par l'objet au client des deux nouveaux diversifiants chiffrés avec la clé publique du client, réalisé par un mécanisme en dehors de la chaine de blocs, dit « off-chain », n'est pas représenté sur la figure. Enfin, la publication (Etape IV-3) pour mise à jour de la chaine de blocs desdits nouveaux diversifiants chiffré avec la clé publique du client.

[0093] L'auto-enrôlement de l'objet se fait par une passerelle mise à disposition par le fabricant, c'est la seule information connue de l'objet lors de sa mise en route.

[0094] On comprendra aisément à la lecture de la présente demande que les particularités de la présente invention, comme généralement décrits et illustrés dans les figures, puissent être arrangés et conçus selon une grande variété de configurations différentes. Ainsi, la description de la présente invention et les figures afférentes ne sont pas prévues pour limiter la portée de l'invention mais représentent simplement des modes de réalisation choisis.

[0095] L'homme de métier comprendra que les caractéristiques techniques d'un mode de réalisation donné peuvent en fait être combinées avec des caractéristiques d'un autre mode de réalisation à moins que l'inverse ne soit explicitement mentionné ou qu'il ne soit évident que ces caractéristiques sont incompatibles. De plus, les caractéristiques techniques décrites dans un mode de réalisation donné peuvent être isolées des autres caractéristiques de ce mode à moins que l'inverse ne soit explicitement mentionné.

[0096] Il doit être évident pour les personnes versées dans l'art que la présente invention permet des modes de réalisation sous de nombreuses autres formes spécifiques sans l'éloigner du domaine défini par la portée des revendications jointes, ils doivent être considérés à titre d'illustration et l'invention ne doit pas être limitée aux détails donnés ci-dessus.

Revendications

[Revendication 1] Procédé de communication pour la gestion sécurisée de clés et d'identités d'un Objet fabriqué par un Fabricant possédant une bi-clé clé publique Kp, clé privée ou secrète Ks de Fabricant (Ks_{man},Kp_{man}) et un client possédant une bi-clé Client (Ks_{client},Kp_{client}), caractérisé en ce que la gestion se fait au moins partiellement sur une base de données décentralisée de chaine de blocs, et que le procédé comprend les étapes suivantes :

a) Génération par le Fabricant de deux clés symétriques diversifiées à partir de sa bi-clé et de diversifiants, par exemple sous forme de clés AES 128 bits, les deux clés symétriques étant composées d'une clé de confidentialité K0c et d'une clé d'Identité K0i, puis partage desdites clés avec l'objet .

b) Publication et enregistrement dans la base de données de chaine de blocs de l'identifiant décentralisé (decentralized Identifier, DID) de l'objet et préférentiellement du chiffrement des diversifiants utilisés pour obtenir les deux clés symétriques par une clé publique Kp_{man}: et association du couple identifiant de l'objet avec le chiffrement de la clé publique Kp_{man} et des diversifiants chiffrés pour former l'information DID – Enc(Kp_{man},DIV_c||DIV_ID)

Et, lorsqu'un Client achète l'objet audit Fabricant, le procédé comprend les étapes d'initialisation suivantes :

c) Fourniture par le Fabricant de l'objet, de l'identifiant de l'objet DID, et des clés symétriques clé de confidentialité K0c et clé d'Identité K0i les clés symétriques étant chiffrées par la clé publique du client kp_{client},au client, par un mécanisme , en dehors de la chaine de blocs, dit « off-chain »;

d) Mise à jour de la chaine de blocs de la base de données par publication et association dans ladite chaine de blocs du couple identifiant de l'objet *(DID) avec* la clé publique du client Kp_{client} et le chiffrement de la clé publique client kp_{client} et des diversifiants chiffrés pour former l'information DID-kp_{client} *et* Enc(Kp_{client} ,DIV_c||DIV_ID),

- Et, lorsque l'objet est allumé pour la première fois, l'objet s'auto-enrôle selon les étapes suivantes :

e) Génération de ses nouvelles clés symétriques clé de confidentialité K1c et clé d'Identité K1i par diversification de ses clés anciennes clés K0c, K0i ;

f) Auto-enrôlement de l'objet est réalisé par un challenge cryptographique mettant en œuvre la clé d'identité

g) Envoi par l'objet au client des deux nouveaux diversifiants chiffrés avec la clé publique du client, l'envoi étant réalisé par un mécanisme en dehors de la chaine de blocs, dit « off-chain »

h) Publication et enregistrement desdits nouveaux diversifiants chiffré avec la clé publique du client dans la chaine de blocs.

[Revendication 2] Procédé de communication selon la revendication 1, qui comprend en outre une étape préalable à la génération de bi-clés de fabrication par le Fabricant, dans laquelle ledit Fabricant enregistre son identifiant de Fabricant dans la chaine de blocs et publie sa clé publique de Fabricant (Kp_{man}) en l'asssociant à son identifiant de Fabricant.

[Revendication 3] Procédé de communication selon l'une quelconque des revendications précédentes, dans lequel le générateur de bi-clés repose sur des porte-monnaies de clé hiérarchiques (Hierarchical Key Wallets) pour fournir les bi-clés du Fabricant et du Client.

[Revendication 4] Procédé de communication selon l'une quelconque des revendications précédentes, dans lequel les deux clés symétriques générées par le Fabricant sont issues du schéma IES (Integration Encryption Scheme, ou du schéma ECIES (Elliptic Curve Integrated Encryption Scheme), préférentiellement du schéma ECIES, et où le Fabricant génère une bi-clé temporaire dont il utilise la partie publique pour la dérivation desdites deux clés symétriques générées.

[Revendication 5] Procédé de communication selon l'une quelconque des revendications précédentes, dans lequel l'objet est transféré d'un propriétaire à un autre en reprenant les étapes d, g, h, préférentiellement les étapes d à h.

[Revendication 6] Procédé de communication selon l'une quelconque des revendications précédentes, dans lequel le partage ou gestion des droits sur l'objet est opéré par le propriétaire de l'objet au moyen de titres vérifiables (Verifiable Credentials), préférentiellement demandés par les fournisseurs de service (Service Providers) et validés par le propriétaire.

[Revendication 7] Procédé de communication selon l'une quelconque des revendications précédentes, dans lequel un système de Preuve à divulgation nulle de connaissance, en anglais (ZKP, Zero Knowledge Proof) est mis en place au sein d'un contrat intelligent, en anglais Smart Contract, pour donner des informations sans en dévoiler les valeurs.

[Revendication 8] Système de gestion d'identités sécurisées basé sur une chaine de bloc apte à réaliser les étapes d'un processus réalisant :

- L'identification des objets avec une liste d'attributs associés, incluant notamment des identifiants de sécurité tels que des clés cryptographiques, et leur enregistrement dans un référentiel du Fabricant ;
- Le transfert de la propriété et/ou des droits d'exploitation d'un objet d'un Fabricant à un utilisateur de l'objet, par exemple un fournisseur de service utilisant l'objet, par l'enregistrement des nouvelles identités associées à l'objet;
- Le transfert de la propriété et/ou des droits d'exploitation d'un utilisateur à un autre, par l'enregistrement des nouvelles identités associées à l'objet ;
- La mise à jour des attributs liés à l'identité de l'objet par le propriétaire d'un objet et/ou l'entité en charge de ses droits d'exploitation.

[Revendication 9] Base de donnée, utilisée par le système de gestion d'identités sécurisées basé sur une chaine de bloc, implémenté sur une plateforme sécurisée, décentralisée, automatisée et multi-acteurs de gestion d'identités d'objets au travers de l'utilisation de la technologie de chaîne de blocs mise en œuvre sur plusieurs nœuds du système avec lesquels la plateforme communique , les nœuds étant responsables du maintien de la chaine de blocs et permettent aux acteurs, et aux objets, de consulter l'état de cette chaine et d'interagir avec cette chaine par l'intermédiaire d'un référentiel (ou registre) commun partagé , chaque nœud ayant accès à un module cryptographique, de préférence physique, en charge du stockage sécurisé de sa clé privée et de l'accès au registre partagé caractérisée en ce que la base de données constitue un référentiel pour chaque fabricant contenant une liste d'attributs associés, incluant notamment des identifiants de sécurité tels que des clés cryptographiques, et soit réalisant leur enregistrement dans le référentiel du Fabricant, soit réalisant la mise à jour des attributs liés à l'identité de l'objet par le propriétaire d'un objet et/ou l'entité en charge de ses droits d'exploitation.

[Revendication 10] Plateforme sécurisée, décentralisée, automatisée et multi-acteurs de gestion d'identités d'objets utilisant une base de données selon la revendication 9, caractérisée en ce qu'elle gère :
- Le transfert de la propriété et/ou des droits d'exploitation d'un objet ;
- L'enregistrement de preuves de possession d'objet dans le référentiel partagé ;
- L'activation / réactivation d'objets ;

[Revendication 11] Plateforme sécurisée, décentralisée, automatisée et multi-acteurs de

gestion d'identités d'objets selon la revendication 10 caractérisée en ce que la technologie de la chaine de bloc utilisée ne doit pas être d'un type précis et comprend au moins :
- un système de permission, pour identifier et authentifier fortement un acteur ;
- un système de contrôle d'accès, basé sur les identités des utilisateurs ;
- un mécanisme d'anti-rejeu ,
chaque nœud maintenant la chaîne de blocs devant se trouver dans un environnement sécurisé, et l'identité publique de chaque nœud doit être mise à disposition des autres nœuds et acteurs au sein du registre partagé; l'exécution de Smart Contract et de fonctions sur la chaine de blocs étant effectuée dans cette sphère sécurisée, l'enregistrement ayant pour finalité de créer un lien, accessible par tout le monde dans la chaine de blocs, pour permettre de faire correspondre l'acteur et son identité digitale par une bi-clé (clé publique et clé privée) ou par un certificat éventuellement signé par un organisme certifié de gestion d'identités.

[Revendication 12] Système de gestion d'identités sécurisées basé sur une chaine de blocs apte à réaliser les étapes du procédé selon une quelconque des revendications 1 à 7, le système comprenant au moins :
un Fabricant, utilisant un système de diversification de clé à partir de diversifiants générés par un générateur de diversifiants, un système de connexion à chaine de blocs, un système d'attribution, à chaque objet sorti de fabrication, d'un identifiant, et un arrangement matériel et logiciel pour envoyer au serveur de chaine de blocs un message de publication et d'enregistrement de l'*association* DID – Enc(Kp_{man},DIV_c ||DIV_ID) .

[Revendication 13] Système de gestion d'identités sécurisées basé sur une chaine de blocs et apte à réaliser les étapes du procédé selon une quelconque des revendications 1 à 7, le système comprenant au moins
Un objet pourvu de moyens de calcul et de moyens de mémorisation d'un programme et de données suffisants pour réaliser les opérations suivantes : lorsque l'objet est allumé pour la première fois, l'objet s'enrôle selon les étapes suivantes :

- Génération de ses nouvelles clés symétriques clé de confidentialité K1c et clé d'Identité K1i par diversification de ses clés anciennes clés K0c, K0i
- Auto-enrôlement par un challenge cryptographique mettant en

œuvre la clé d'identité K0i

- Envoi par l'objet au client des deux nouveaux diversifiants chiffré avec la clé publique du client, l'envoi étant réalisé par un mécanisme, en dehors de la base de données de chaines de blocs,
- Publication et enregistrement desdits nouveaux diversifiants chiffré avec la clé publique du client dans la base de données de chaines de blocs,

[Revendication 14] Système de gestion d'identités selon la revendication 12 ou 13, dans lequel un système de partage de clés de confidentialité est mis en place « off-chain », afin que les opérateurs de service aient accès à l'objet, et donc aux informations relatives.

[Revendication 15] Système de gestion d'identités d'un fournisseur de service d'identité (ID service provider) mettant en œuvre une chaîne de blocs « block-chain » et utilisant les objets enregistrés sur un réseau pour remplir des services applicatifs (SA) dans lesquels les informations fournies par les objets sont utilisées, chaque nœud du réseau du fournisseur de service d'identité a accès à un module cryptographique en charge du stockage sécurisé de sa clé privée, les nœuds possédant des client appelés Acteurs ayant chacun leur propre identité ID_{act} enregistrée dans la chaine de bloc, chaque fabricant d'objet est enregistré dans la chaîne de blocs « block-chain » du fournisseur de service d'identité et leur clé publique sont connues de tous, pour chaque objet vendu ou transféré chaque fabricant fournit l'identifiant de l'objet et le chiffrement des diversifiants utilisé par le fabricant pour le calcul des clés symétriques de chaque objet par publication dans la chaîne de bloc « block-chain », seules les clés symétriques restent stockées en dehors de la chaîne, en l'occurrence dans l'objet ;

Chaque objet étant pourvu de moyens de calcul et de moyens de mémorisation d'un programme et de données suffisants pour exécuter les opérations suivantes : lorsque l'objet est allumé pour la première fois, l'objet s'enrôle auprès du fournisseur de service d'identité en réalisant les étapes suivantes :

- Génération dans l'objet de ses nouvelles clés symétriques clé de confidentialité K1c et clé d'Identité K1i par diversification de ses clés anciennes clés K0c, K0i,

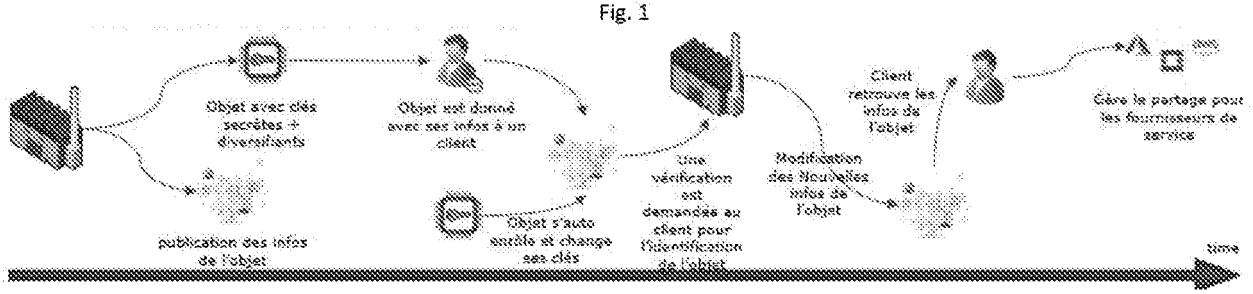
- Auto-enrôlement par un challenge cryptographique mettant en œuvre la clé d'identité.
- Envoi par l'objet au client des deux nouveaux diversifiants chiffrés avec la clé publique du client, l'envoi étant réalisé par un mécanisme, en dehors de la chaine de blocs,
- Publication et enregistrement desdits nouveaux diversifiants chiffrés avec la clé publique du client dans la chaine de blocs.

[Revendication 16] Un objet étant pourvu de moyens de calcul et de moyens de mémorisation d'un programme et de données suffisants pour exécuter les opérations suivantes : lorsque l'objet est allumé pour la première fois, l'objet s'enrôle auprès du fournisseur de service d'identité en réalisant les étapes suivantes :

- Génération dans l'objet de ses nouvelles clés symétriques clé de confidentialité K1c et clé d'Identité K1i par diversification de ses clés anciennes clés K0c, K0i,
- Auto-enrôlement par un challenge cryptographique mettant en œuvre la clé d'identité.
- Envoi par l'objet au client des deux nouveaux diversifiants chiffrés avec la clé publique du client, l'envoi étant réalisé par un mécanisme, en dehors de la chaine de blocs,
- Publication et enregistrement desdits nouveaux diversifiants chiffrés avec la clé publique du client dans la chaine de blocs.

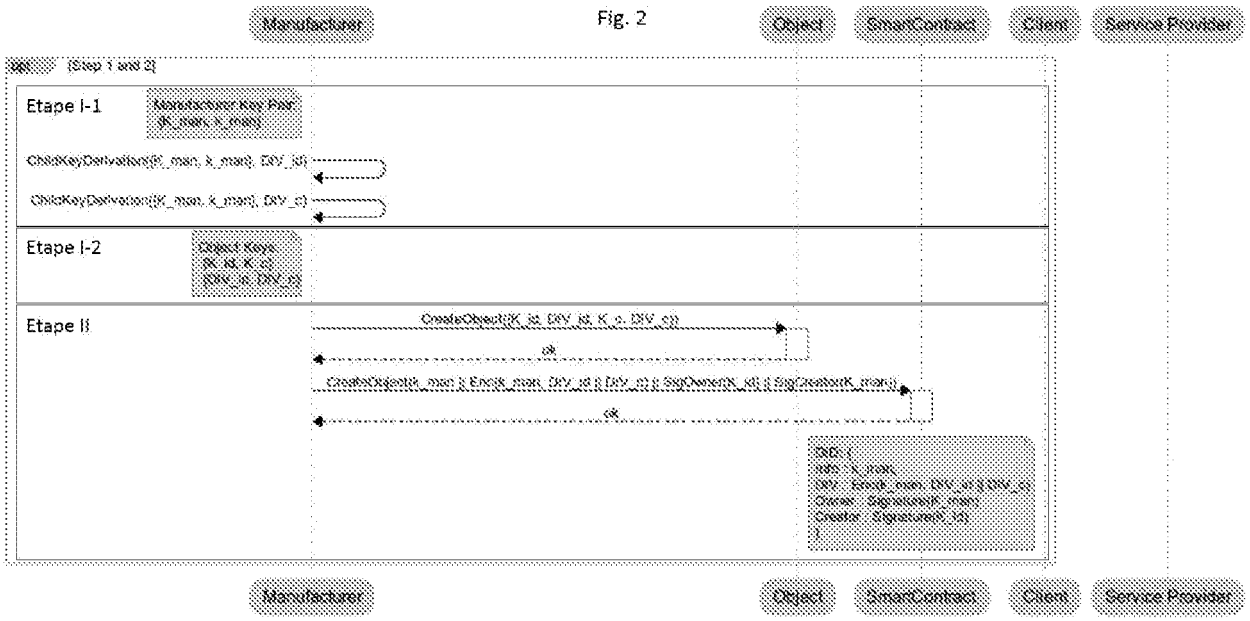
[Fig. 1]

Fig. 1



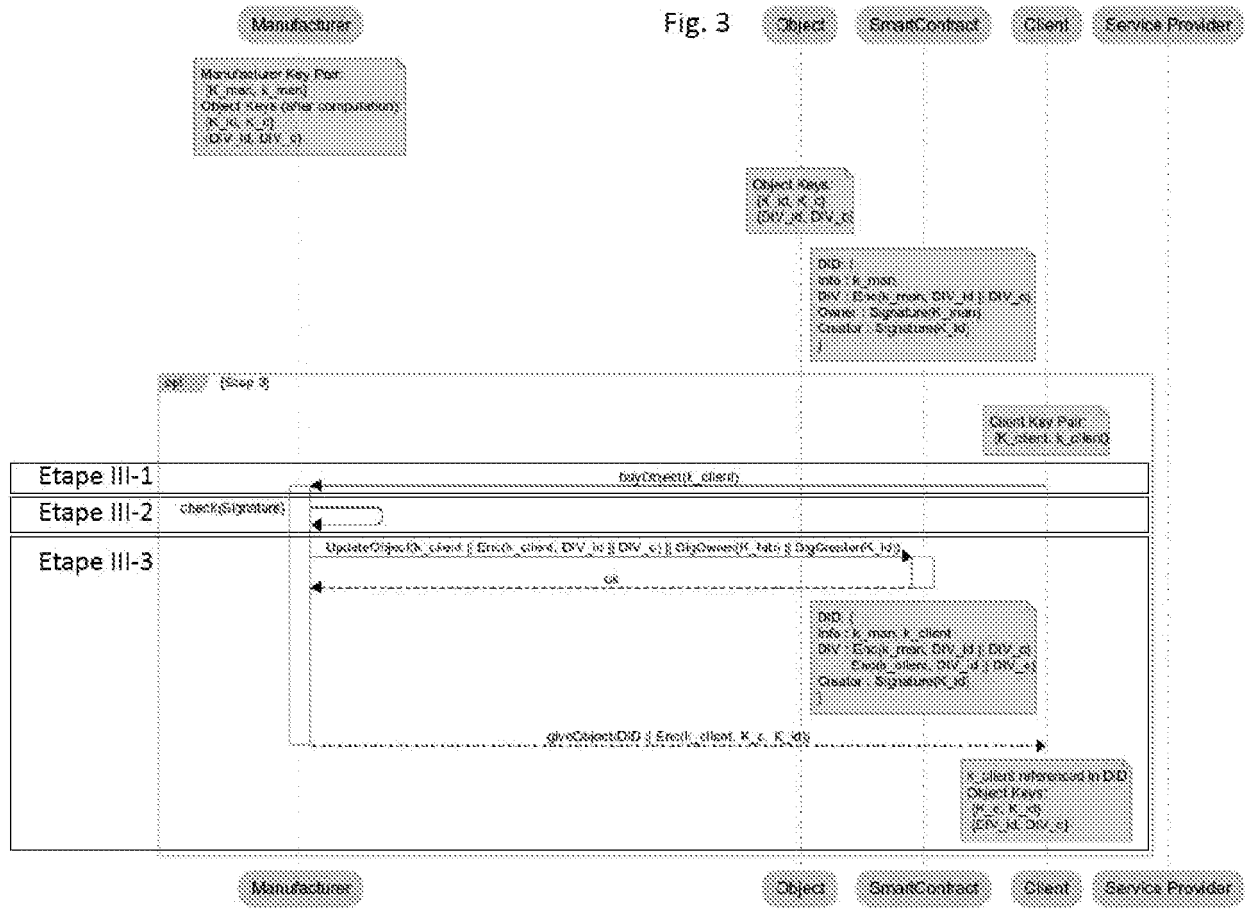
[Fig. 2]

Fig. 2



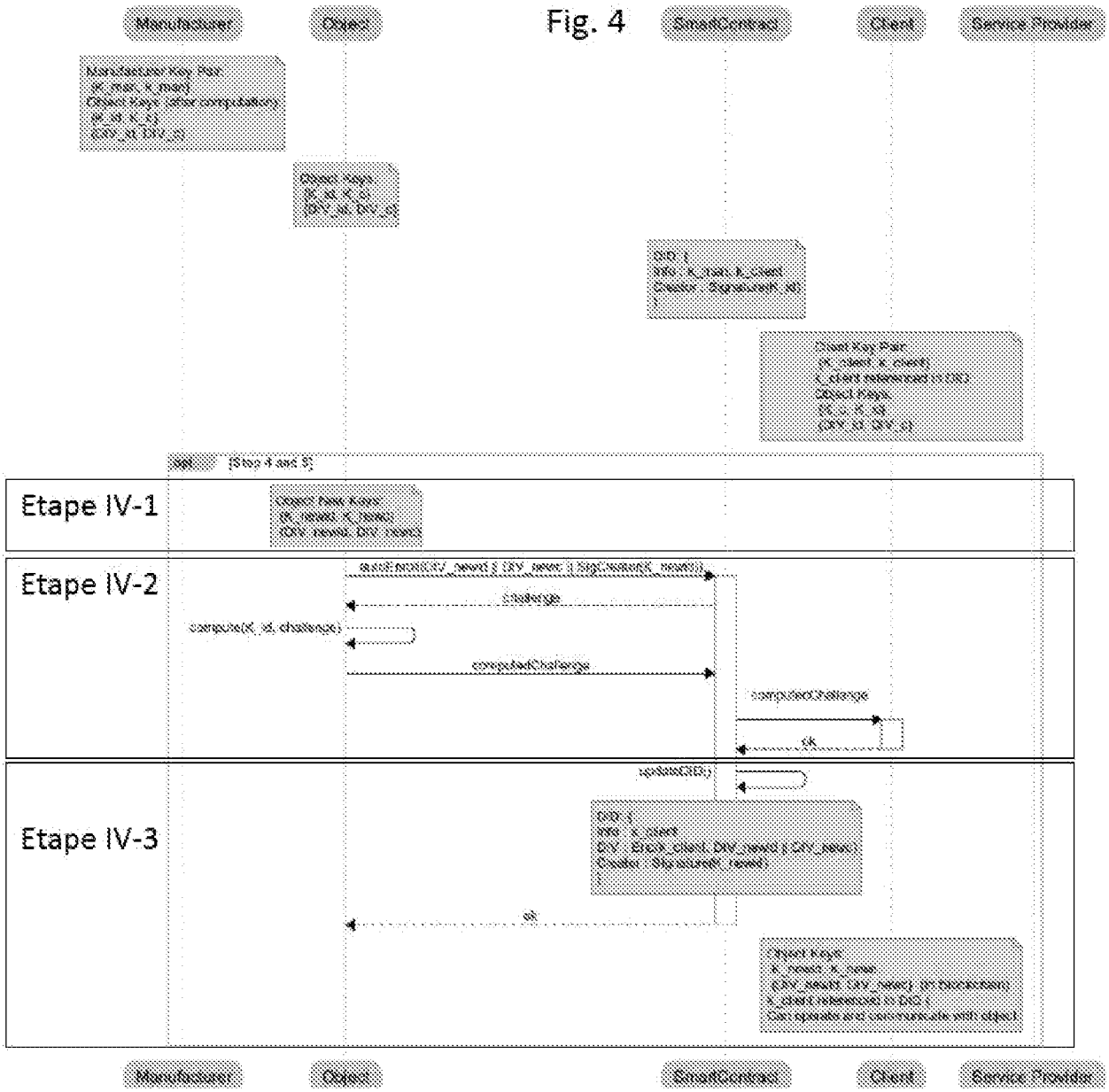
[Fig. 3]

Fig. 3



[Fig. 4]

Fig. 4


Manufacturer
Object
SmartContract
Client
Service Provider
Etape IV-1
Etape IV-2
Etape IV-3
challenge
computedChallenge
ok
Manufacturer
Object
SmartContract
Client
Service Provider

RAPPORT DE RECHERCHE

articles L.612-14, L.612-53 à 69 du code de la propriété intellectuelle

OBJET DU RAPPORT DE RECHERCHE

L'I.N.P.I. annexe à chaque brevet un "RAPPORT DE RECHERCHE" citant les éléments de l'état de la technique qui peuvent être pris en considération pour apprécier la brevetabilité de l'invention, au sens des articles L. 611-11 (nouveauté) et L. 611-14 (activité inventive) du code de la propriété intellectuelle. Ce rapport porte sur les revendications du brevet qui définissent l'objet de l'invention et délimitent l'étendue de la protection.
Après délivrance, l'I.N.P.I. peut, à la requête de toute personne intéressée, formuler un "AVIS DOCUMENTAIRE" sur la base des documents cités dans ce rapport de recherche et de tout autre document que le requérant souhaite voir prendre en considération.

CONDITIONS D'ETABLISSEMENT DU PRESENT RAPPORT DE RECHERCHE

[x] Le demandeur a présenté des observations en réponse au rapport de recherche préliminaire.

☐ Le demandeur a maintenu les revendications.

[x] Le demandeur a modifié les revendications.

☐ Le demandeur a modifié la description pour en éliminer les éléments qui n'étaient plus en concordance avec les nouvelles revendications.

☐ Les tiers ont présenté des observations après publication du rapport de recherche préliminaire.

☐ Un rapport de recherche préliminaire complémentaire a été établi.

DOCUMENTS CITES DANS LE PRESENT RAPPORT DE RECHERCHE

La répartition des documents entre les rubriques 1, 2 et 3 tient compte, le cas échéant, des revendications déposées en dernier lieu et/ou des observations présentées.

☐ Les documents énumérés à la rubrique 1 ci-après sont susceptibles d'être pris en considération pour apprécier la brevetabilité de l'invention.

[x] Les documents énumérés à la rubrique 2 ci-après illustrent l'arrière-plan technologique général.

☐ Les documents énumérés à la rubrique 3 ci-après ont été cités en cours de procédure, mais leur pertinence dépend de la validité des priorités revendiquées.

☐ Aucun document n'a été cité en cours de procédure.

1. ELEMENTS DE L'ETAT DE LA TECHNIQUE SUSCEPTIBLES D'ETRE PRIS EN CONSIDERATION POUR APPRECIER LA BREVETABILITE DE L'INVENTION

NEANT

2. ELEMENTS DE L'ETAT DE LA TECHNIQUE ILLUSTRANT L'ARRIERE-PLAN TECHNOLOGIQUE GENERAL

WON JONGHO ET AL: "Decentralized Public Key Infrastructure for Internet-of-Things", MILCOM 2018 - 2018 IEEE MILITARY COMMUNICATIONS CONFERENCE (MILCOM), IEEE, 29 octobre 2018 (2018-10-29), pages 907-913, XP033489288, DOI: 10.1109/MILCOM.2018.8599710 [extrait le 2019-01-02]

"Chapter 12: Key Establishment Protocols ED - Menezes A J; Van Oorschot P C; Vanstone S A", HANDBOOK OF APPLIED CRYPTOGRAPHY; [CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS], CRC PRESS, BOCA RATON, FL, US, PAGE(S) 489 - 541 , 1 octobre 1996 (1996-10-01), XP001525012, ISBN: 978-0-8493-8523-0 Extrait de l'Internet: URL:http://www.cacr.math.uwaterloo.ca/hac/

3. ELEMENTS DE L'ETAT DE LA TECHNIQUE DONT LA PERTINENCE DEPEND DE LA VALIDITE DES PRIORITES

NEANT