(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** ***3 085 815***

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **18 70826**

(51) Int Cl[8] : ***H 04 L 9/08*** *(2018.01)*

(12) BREVET D'INVENTION B1

(54) GOUVERNANCE DE SECURITE DU TRAITEMENT D'UNE REQUETE NUMERIQUE.

(22) **Date de dépôt :** 11.07.18.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 13.03.20 Bulletin 20/11.

(45) **Date de la mise à disposition du public du brevet d'invention :** 15.07.22 Bulletin 22/28.

(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 :** Polynésie-Fr

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

(72) **Inventeur(s) :** BACCA Nicolas et TOMAZ Olivier.

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

(74) **Mandataire(s) :** SELARL FWPA.

FR 3 085 815 - B1

Description

Titre de l'invention : Gouvernance de sécurité du traitement d'une requête numérique

[0001] L'invention est relative à la gouvernance de sécurité du traitement d'une requête numérique et a pour objet un procédé de validation d'une requête numérique par une entité demanderesse, un procédé de traitement d'une requête numérique mettant en œuvre ce procédé de validation d'une requête numérique, des applications de ce procédé de validation d'une requête numérique et un système pour la mise en œuvre de ce procédé de validation d'une requête numérique, incluant au moins deux processeurs de sécurité.

[0002] L'expression « gouvernance de sécurité du traitement d'une requête numérique » doit être considérée dans son acception la plus large et générique, de sorte à inclure, notamment mais non exclusivement, un procédé de gouvernance de signature électronique, un procédé de gouvernance de chiffrement ou déchiffrement de données, un procédé de vote électronique, un procédé de gouvernance de transactions bancaires ou monétiques.

[0003] Cette gouvernance de sécurité doit être comprise comme représentative des processus permettant de vérifier la conformité de la requête numérique d'une entité demanderesse au corpus de règles définies en commun par des entités coopérantes mettant en œuvre des processeurs de sécurité chargés d'une application. L'expression « entité coopérante » doit donc être comprise comme étant une personne ou un robot informatique apte à utiliser une application portée par un processeur de sécurité. L'expression « entité demanderesse » doit être comprise comme désignant l'entité qui fait la requête numérique. L'expression « requête numérique » doit être comprise comme signifiant un message adressé à un moyen électronique et informatique coopérant en vue d'un service et incluant un système pour la mise en œuvre de ce procédé de validation d'une requête numérique. Un tel service peut être, notamment mais non exclusivement, un chiffrement ou un déchiffrement de données, un vote électronique, une transaction bancaire ou monétique.

[0004] L'expression « processeur de sécurité » doit être comprise comme un dispositif électronique support pour des applications mettant en œuvre des données confidentielles, et comprenant une mémoire persistante, une mémoire volatile, un calculateur apte à réaliser des fonctions cryptographiques et notamment à authentifier tout ou partie du contenu de ses mémoires en fournissant ce que l'on dénomme ici une « attestation numérique ». Le processeur est qualifié de sécurité dans la mesure où le contenu des mémoires ne peut être modifié qu'avec une authentification auprès du dispositif.

[0005] Le terme « application » concernant l'application chargée dans une mémoire d'un tel processeur de sécurité doit être compris comme signifiant l'ensemble des règles exécutées avec des données confidentielles et des paramètres (incluant au moins un processus de création de secret).

[0006] Le document US 5 815 573 décrit un procédé de génération d'une clé cryptographique à utiliser par une paire de parties communicantes tout en prévoyant la récupération de ladite clé en utilisant une pluralité d'agents de récupération de clé coopérants, comprenant les étapes consistant à: générer une pluralité de parties clés partagées qui sont partagées avec les agents de récupération de clé respectifs; générer une partie clé non partagée qui n'est partagée avec aucun agent de récupération de clé; générer ladite clé en fonction desdites parties de clé partagées et de ladite partie de clé non partagée; et rendre disponibles les parties respectives desdites parties de clé partagées auxdits agents de récupération de clé pour faciliter ladite récupération de ladite clé en utilisant lesdits agents de récupération de clé.

[0007] Parmi d'autres, les documents WO 2017/064124, WO03077470 et WO9505712 décrivent des procédés pour générer un secret commun.

[0008] Le document WO 2017/145016 décrit un procédé et un système de détermination d'un secret commun pour deux nœuds. Chaque nœud possède une paire cryptographique asymétrique respective, chaque paire comprenant une clé privée maîtresse et une clé publique maîtresse. Des deuxièmes clés privées et publiques respectives peuvent être déterminées en fonction de la clé privée maîtresse, de la clé publique maîtresse et d'une clé déterministe. Un secret commun peut être déterminé au niveau de chacun des nœuds en fonction des deuxièmes clés privées et publiques. Dans un exemple, un nœud peut déterminer le secret commun en fonction : d'une deuxième clé privée fondée sur la propre clé privée maîtresse du nœud et la clé déterministe ; d'une deuxième clé publique fondée sur la clé publique maîtresse de l'autre nœud et de la clé déterministe. Ce procédé et ce système peuvent être adaptés à des portefeuilles numériques, des technologies à enchaînements de blocs et à la sécurité de dispositifs personnels. Avec ce procédé et ce système, il n'y a pas de partage d'un secret commun.

[0009] Le document W0 2017/145010 décrit un procédé mis en œuvre par ordinateur pour commander l'accès à une ressource informatique telle que, par exemple, un portefeuille numérique. Dans un ou plusieurs modes de réalisation, le portefeuille peut être mis en œuvre à l'aide d'une chaîne de blocs. La mise en œuvre du procédé durant la configuration initiale du portefeuille peut permettre à des opérations ultérieures, telles que des transactions de portefeuille, d'être gérées d'une manière sécurisée sur un canal non sécurisé, tel qu'Internet. Un procédé, selon un mode de réalisation peut comprendre les étapes consistant à diviser un élément de vérification (tel qu'une clé privée dans une paire de cryptographie asymétrique) en une pluralité de parts ; à dé-

terminer un secret partagé au niveau d'au moins deux nœuds dans un réseau ; et à utiliser le secret partagé pour transmettre au moins une part de l'élément de vérification entre lesdits deux nœuds. Les parts peuvent être divisées de telle sorte qu'aucune part toute seule n'est suffisante pour obtenir l'élément de vérification. Ceci signifie qu'aucune partie ne stocke toute la clé privée, ce qui offre une sécurité améliorée de la clé. Au moins deux parts sont nécessaires pour restaurer la clé. Les parts sont stockées à des emplacements séparés dont l'un est un emplacement de sauvegarde ou de stockage sécurisé indépendant. Si l'une des autres parts devient indisponible, la part peut être extraite de la sauvegarde pour garantir que la clé (et ainsi la ressource commandée) est toujours accessible. Pour garantir la transmission sécurisée desdites parts, le secret partagé est généré au niveau de deux nœuds différents indépendamment l'un de l'autre, puis utilisé pour générer une clé de chiffrement. La clé de chiffrement peut être utilisée pour chiffrer au moins une part de l'élément de vérification, ou un message la comprenant, pour garantir que lesdites parts sont transmises de manière sécurisée. Avec ce procédé, on ne fabrique pas un secret commun et on ne le partage pas. De plus, le processeur n'est pas de sécurité, comme cela a été précédemment défini.

[0010] Le document W0 2016/130030 décrit un procédé de protection de données à l'aide d'une cryptographie à seuil, dans lequel des données sont chiffrées à l'aide d'algorithmes cryptographiques et une clé cryptographique est divisée en parts. Le procédé de protection de données à l'aide d'une cryptographie à seuil est caractérisé en ce qu'un identificateur unique est affecté à des données chiffrées. Ensuite, au moins une part de la clé cryptographique est fusionnée avec des données chiffrées. Ensuite, les données chiffrées fusionnées avec certaines des parts de la clé sont divisées en fragments et un identificateur unique précédemment affecté aux données chiffrées est ajouté à chaque fragment. Le même identificateur unique est ajouté à la part de chaque clé qui n'a pas été fusionnée avec des données chiffrées. Les fragments obtenus de données sont déployés sur des dispositifs physiquement séparés comprenant au moins un processeur et une mémoire non volatile, et, pour chaque fragment, des informations concernant le dispositif sur lequel il est déployé sont sauvegardées. Les parts de la clé qui n'ont pas été fusionnées avec des données chiffrées sont placées sur des dispositifs physiquement séparés comprenant au moins un processeur et une mémoire non volatile, et, pour chaque part de la clé, des informations concernant le dispositif sur lequel elle est stockée sont sauvegardées. Ce brevet vise la confidentialité et non l'authentification.

[0011] Dans le document US 6 182 214, la cryptographie à seuil (partage secret) est utilisée pour échanger un secret entre un serveur et un client sur un réseau non fiable. Spécifiquement, un secret est divisé par calcul en N parts en utilisant un schéma de cryptage

à seuil tel que n'importe quel M des partages (M inférieur ou égal à N) peut être utilisé pour reconstruire le secret. Les N parts sont réparties sur un certain nombre de messages transmis, en supposant qu'un certain nombre de messages comprenant un total d'au moins M actions seront reçus par le client. Lors de la réception d'au moins M partages, le client utilise au moins M partages pour reconstruire le secret en utilisant le schéma de cryptage à seuil. Ce brevet vise la confidentialité pour le transfert d'un secret et non l'authentification.

[0012] On connaît une gouvernance de sécurité dans laquelle une entité demanderesse fait une requête auprès d'un système incluant un processeur de sécurité, dont l'exécution est conditionnée par le consentement in fine auprès dudit processeur de sécurité, de personnes ou robot informatiques, lesquels ont été préalablement habilités par une autorité extérieure jouant le rôle de tiers de confiance.

[0013] Une telle gouvernance a pour faiblesse la centralisation persistante des données confidentielles dans ledit processeur de sécurité. Et que les personnes ou robot informatiques ne peuvent attester sans tiers de confiance que les données confidentielles ne seront pas utilisées autrement que pour le consentement donné. Par ailleurs, une telle gouvernance a pour contrainte de devoir recourir à un tiers de confiance et à des processus d'habilitation rigides et complexes.

[0014] Tel est le contexte de l'invention et telle est l'interprétation qu'il convient de donner aux termes précédemment définis utilisés dans le texte.

[0015] Le problème à la base de l'invention est de valider une requête numérique d'une entité demanderesse et in fine de pouvoir traiter cette requête numérique, en la soumettant au consentement préalable de plusieurs entités, sans avoir à recourir à un tiers de confiance.

[0016] La solution apportée à ce problème consiste en ce que les entités coopérantes qui doivent consentir à l'exécution de la requête moyennant la mise en œuvre des technologies de la cryptographie à seuil, alors que ces entités coopérantes vont s'authentifier mutuellement en utilisant les attestations numériques délivrées par une pluralité de processeurs de sécurité.

[0017] Ci-après, un exposé de l'invention.

[0018] Selon un premier aspect, l'invention a pour objet un procédé de validation d'une requête numérique :

[0019] dans lequel une pluralité d'entités coopérantes sont aptes à mettre en œuvre chacune un processeur de sécurité chargé avec une même application nécessaire au traitement de ladite requête, application pour laquelle chaque processeur de sécurité délivre une attestation numérique d'intégrité sur demande,

[0020] qui comporte un processus de vérification d'intégrité de ladite application tel que, à partir des attestations numériques délivrées par chaque processeur de sécurité, chaque

entité de la pluralité d'entités coopérantes s'assure que chacune des autres entités de la pluralité d'entités met en œuvre une application identique à la sienne en vérifiant de façon cryptographique l'attestation numérique correspondante,

[0021] qui comporte un processus par lequel des entités coopérantes créent un secret commun et constituent ainsi un collège d'entités coopérantes créatrices,

[0022] qui comporte, moyennant la mise en œuvre du processus de vérification d'intégrité de ladite application, un processus par lequel des entités du collège d'entités coopérantes créatrices désignent les entités coopérantes signataires, constituant ainsi un collège d'entités coopérantes signataires, en sorte que ledit collège d'entités coopérantes signataires pris en tant que tel ait accès au secret commun,

[0023] de sorte que ladite requête est validée si et seulement si des entités coopérantes du collège d'entités coopérantes signataires mettent en œuvre ladite application moyennant le secret commun.

[0024] Selon les réalisations, un dit processeur de sécurité est apte à être mis en œuvre soit par une entité coopérante auquel cas ledit processeur de sécurité est propre à cette entité coopérante soit par plusieurs entités coopérantes auquel cas ledit processeur de sécurité est commun à ces entités coopérantes, le procédé impliquant la mise en œuvre d'au moins deux processeurs de sécurité.

[0025] Selon une caractéristique, pour que chaque processeur de sécurité délivre une attestation numérique d'intégrité sur demande :

on met en œuvre des processeurs de sécurité choisis de sorte qu'ils disposent chacun, en propre, d'une première paire de clés cryptographiques asymétriques,

à la demande d'une ou plusieurs entités coopérantes, chaque processeur de sécurité utilise la clé privée de ladite première paire de clés pour produire une signature électronique de tout ou partie du contenu de ses mémoires,

ladite signature électronique valant attestation numérique d'intégrité du contenu signé correspondant, et son authenticité peut être vérifiée en utilisant la partie publique de la dite première paire de clés.

[0026] Selon une caractéristique, en vue du processus de vérification d'intégrité de ladite application,

les entités coopérantes de ladite pluralité d'entités coopérantes conviennent ensemble d'une seconde paire de clés cryptographiques asymétriques,

la partie privée de ladite seconde paire de clés est mise en œuvre pour produire la signature électronique de la partie publique desdites premières paires de clés de chaque processeur de sécurité,

de sorte que lesdites entités coopérantes sont aptes à authentifier, en mettant en œuvre la partie publique de ladite seconde paire de clés, les attestations numériques d'intégrité délivrées par chacun des processeurs de sécurité.

[0027] Selon les réalisations, en vue de convenir de ladite seconde paire de clés cryptographiques asymétriques, les entités coopérantes utilisent une paire de clés cryptographiques asymétriques tirée aléatoirement et partagées entre elles ou bien ladite seconde paire de clés cryptographiques asymétriques est celle d'une autorité de certification externe.

[0028] Selon une caractéristique, pour créer un secret commun :

[0029] des entités coopérantes de la pluralité d'entités coopérantes mettent en commun des données confidentielles propres,

[0030] un traitement numérique est appliqué à l'ensemble desdites données confidentielles propres, créant ainsi ledit secret commun.

[0031] Selon les réalisations, les dites données confidentielles propres sont tirées aléatoirement par chacune des entités coopérantes, et/ou introduites par les entités coopérantes dans la mémoire des processeurs de sécurité associées, et/ou extraites de la mémoire des processeurs de sécurité associés.

[0032] Selon une caractéristique, moyennant un algorithme de découpage/reconstitution, le secret commun est apte à être découpé, en parties découpées de sorte à être reconstitué ultérieurement et/ou dans lequel au moins certaines des, ou toutes les, parties découpées sont aptes et suffisantes à reconstituer ultérieurement ledit secret commun.

[0033] Selon une réalisation :

[0034] ledit secret commun une fois créé est découpé en un nombre de parties découpées créatrices, égal au nombre d'entités coopérantes créatrices,

[0035] et lesdites parties découpées créatrices sont réparties entre les entités coopérantes créatrices, chacune des dites entités conservant l'une desdites parties découpées créatrices,

[0036] de sorte qu'ultérieurement, ledit secret commun puisse être reconstitué avec au moins certaines des, ou toutes les, dites parties découpées créatrices.

[0037] Selon une possibilité, ledit secret commun ne peut être utilisé que pour la validation d'une et une seule requête numérique et ne peut être stocké de manière persistante dans aucune des mémoires des processeurs de sécurité associés.

[0038] Selon une première réalisation possible, lors de la mise en œuvre du procédé de validation, il est prévu un processus de vérification d'intégrité de ladite application tel que, à partir des attestations numériques délivrées par chaque processeur de sécurité, chaque entité de la pluralité d'entités coopérantes s'assure directement que chacune des autres entités de la pluralité d'entités met en œuvre une application identique à la sienne en vérifiant de façon cryptographique l'attestation numérique correspondante.

[0039] Selon une seconde réalisation possible, lors de la mise en œuvre du procédé de validation, il est prévu un processus de vérification d'intégrité de ladite application tel que, à partir des attestations numériques délivrées par chaque processeur de sécurité,

chaque entité de la pluralité d'entités coopérantes s'assure que chacune des autres entités de la pluralité d'entités met en œuvre une application identique à la sienne en vérifiant de façon cryptographique l'attestation numérique correspondante, de façon indirecte et par transitivité, en s'assurant qu'une certaine entité de la pluralité d'entités met en œuvre une application identique à la sienne en vérifiant de façon cryptographique l'attestation numérique correspondante, cette certaine entité s'étant elle-même assurée que les autres entités de la pluralité d'entités mettent en œuvre la même application.

[0040] Selon une caractéristique, lesdites données confidentielles propres sont transmises de manière confidentielle, moyennant un algorithme de chiffrement et déchiffrement, entre les entités coopérantes créatrices en utilisant au moins une clé de session, ladite au moins une clé de session étant rendue inutilisable après la création d'un secret commun.

[0041] Selon une réalisation :

[0042] Les entités coopérantes créatrices comprennent une première entité créatrice pilote et les autres entités coopérantes créatrices,

[0043] il est utilisé une pluralité de clés de session, de sorte que chaque entité coopérante créatrice met en œuvre une clé propre pour communiquer de manière confidentielle, moyennant un algorithme de chiffrement et déchiffrement, avec ladite première entité créatrice pilote,

[0044] ladite application intègre un algorithme d'échange des clés de session,

[0045] ladite première entité créatrice pilote, initie ledit algorithme d'échange de clés de session avec chacune des autres entités coopérantes créatrices,

[0046] de sorte que lesdites autres entités coopérantes créatrices transmettent, de manière confidentielle en utilisant leur propre clé de session, moyennant un algorithme de chiffrement et déchiffrement, et non rejouable, leurs dites données confidentielles propres à ladite première entité créatrice pilote,

[0047] le procédé étant réitéré, chaque entité coopérante créatrice étant ladite première entité créatrice pilote,

[0048] de sorte que les entités coopérantes créatrices sont aptes à appliquer un traitement numérique à l'ensemble desdites données confidentielles propres, créant ainsi ledit secret commun.

[0049] Selon une réalisation :

[0050] les entités coopérantes créatrices comprennent une seconde entité créatrice pilote et les autres entités coopérantes créatrices,

[0051] il est utilisé une pluralité de clés de session, de sorte que chaque entité coopérante signataire met en œuvre une clé propre pour communiquer de manière confidentielle, moyennant un algorithme de chiffrement et déchiffrement, avec ladite seconde entité

créatrice pilote,

[0052] il est utilisé une pluralité de clés de session, de sorte que chaque entité coopérante créatrice met en œuvre une clé propre pour communiquer de manière confidentielle, moyennant un algorithme de chiffrement et déchiffrement, avec ladite seconde entité créatrice pilote,

[0053] ladite seconde entité créatrice pilote met en œuvre un processus de vérification d'intégrité de ladite application portée par le processeur de sécurité de chaque entité coopérante signataire, de sorte que ladite seconde entité créatrice pilote s'assure que chacune des entités coopérantes signataires met en œuvre une application identique à la sienne en vérifiant de façon cryptographique l'attestation numérique correspondante,

[0054] ladite application intègre un algorithme d'échange des clés de session,

[0055] est initié ledit algorithme d'échange de clés de session entre, d'une part, chacune des dites autres entités coopérantes créatrices et chacune des entités coopérantes signataires et, d'autre part, ladite seconde entité créatrice pilote,

[0056] de sorte que :

[0057]
- toutes les, ou au moins certaines des – en nombre suffisant à la reconstitution du secret commun –, dites autres entités coopérantes créatrices transmettent, de manière confidentielle en utilisant leur propre clé de session, moyennant un algorithme de chiffrement et déchiffrement, et non rejouable, leurs dites parties découpées créatrices issues d'un même découpage du secret commun à ladite seconde entité créatrice pilote,
- ladite seconde entité créatrice pilote reconstitue le secret commun,
- ladite seconde entité créatrice pilote découpe le secret commun en un nombre de parties découpées signataires égal au nombre d'entités coopérantes signataires,
- ladite seconde entité créatrice pilote transmet, de manière confidentielle en utilisant les clés de session, moyennant un algorithme de chiffrement et déchiffrement, et non rejouable, leurs dites parties découpées signataires du secret commun aux dites entités coopérantes signataires.

[0058] Selon une réalisation, des parties découpées issues d'un même découpage du secret commun sont transmises de manière confidentielle, moyennant un algorithme de chiffrement et déchiffrement, entre les entités coopérantes en utilisant au moins une clé de session, ladite au moins une clé de session étant rendue inutilisable après la reconstitution dudit secret commun.

[0059] Selon une réalisation :

[0060] les entités coopérantes comprennent une entité pilote et les autres entités coopérantes,

[0061] il est utilisé une pluralité de clés de session, de sorte que chaque entités coopérantes met en œuvre une clé propre pour communiquer de manière confidentielle, moyennant

un algorithme de chiffrement et déchiffrement, avec ladite entité pilote,

[0062] ladite application intègre un algorithme d'échange des clés de session,

[0063] ladite entité pilote, initie ledit algorithme d'échange de clés de session avec chacune des autres entités coopérantes,

[0064] de sorte que toutes les, ou au moins certaines des – en nombre suffisant à la reconstitution du secret commun -, dites autres entités coopérantes transmettent, de manière confidentielle en utilisant leur propre clé de session, moyennant un algorithme de chiffrement et déchiffrement, non rejouable, leurs dites parties découpées issues d'un même découpage du secret commun à ladite entité pilote.

[0065] Selon les cas, le collège d'entités coopérantes créatrices et le collège d'entités coopérantes signataires sont distincts ou bien le collège d'entités coopérantes créatrices et le collège d'entités coopérantes signataires sont au moins pour partie communs.

[0066] Selon un deuxième aspect, l'invention a pour objet un procédé de traitement d'une requête numérique d'une entité demanderesse, avec une pluralité d'entités coopérantes qui sont aptes à mettre en œuvre chacune un processeur de sécurité chargé avec une même application nécessaire au traitement de ladite requête, application pour laquelle chaque processeur de sécurité délivre une attestation numérique d'intégrité sur demande, qui met en œuvre le procédé de validation d'une requête numérique qui vient d'être décrit, de sorte que ladite requête est traitée si et seulement si des entités coopérantes du collège d'entités coopérantes signataires mettent en œuvre ladite application moyennant le secret commun.

[0067] Selon une caractéristique :

[0068] l'entité demanderesse transmet ladite requête numérique d'une part au collège d'entités coopérantes, d'autre part à un moyen électronique apte à exécuter ladite requête,

[0069] le collège d'entités coopérantes met en œuvre un procédé de validation, moyennant ledit secret commun, en vue de la validation de ladite requête numérique,

[0070] ledit moyen électronique exécute ladite requête numérique en fonction de ladite validation.

[0071] Selon un troisième aspect, l'invention a pour objet l'application du procédé de validation d'une requête numérique qui vient d'être décrit, à un procédé de traitement d'une requête numérique d'une entité demanderesse comme précédemment décrit ou bien, notamment, notamment un procédé de gouvernance de signature électronique, un procédé de gouvernance de chiffrement ou déchiffrement de données, un procédé de vote électronique, un procédé de gouvernance de transactions bancaires ou monétiques.

[0072] Selon un quatrième aspect, l'invention a pour objet un système pour la mise en œuvre du procédé de validation d'une requête numérique qui vient d'être décrit, qui comporte :

[0073] - au moins deux processeurs de sécurité support d'une application nécessaire au traitement de ladite requête, mettant en œuvre des données confidentielles, et comprenant une mémoire persistante, une mémoire volatile, un calculateur apte à réaliser des fonctions cryptographiques et notamment à authentifier tout ou partie du contenu de ses mémoires en fournissant une attestation numérique d'intégrité sur demande, de sorte qu'une pluralité d'entités coopérantes sont aptes à mettre en œuvre chacune un dit processeur de sécurité, et dont le contenu des mémoires ne peut être modifié qu'avec une authentification,

[0074] - un moyen apte à créer un secret commun,

[0075] - un algorithme d'attestation numérique,

[0076] - un algorithme de chiffrement et déchiffrement,

[0077] - un algorithme de découpage / reconstitution de secret commun,

[0078] - un algorithme d'échange de clés de session,

[0079] - des moyens de communication entre les processeurs de sécurité et les entités.

[0080] On décrit maintenant brièvement les figures des dessins.

[0081] La figure 1 [Fig. 1] est un schéma simplifié illustrant un exemple de réalisation possible d'un procédé de traitement d'une requête numérique mettant en œuvre un procédé de validation de la requête. Sur cette figure sont symbolisés une entité demanderesse, trois entités coopérantes, trois processeurs de sécurité, et un moyen électronique et informatique apte et destiné à exécuter la requête. Les flèches symbolisent les opérations effectuées.

[0082] La figure 2 [Fig. 2] est un schéma simplifié qui illustre deux exemples de réalisation possible en ce qui concerne les processeurs de sécurité et les entités coopérantes, à savoir une réalisation dans laquelle le processeur de sécurité est propre à une entité coopérante et une réalisation dans laquelle le processeur de sécurité est commun à plusieurs entités coopérantes.

[0083] La figure 3 [Fig. 3] est un schéma simplifié illustrant un exemple de réalisation d'un processus de vérification d'intégrité de l'application mise en œuvre, moyennant un processus cryptographique à clés cryptographiques asymétriques.

[0084] En complément, la figure 4 [Fig. 4] est un schéma simplifié correspondant à un exemple de réalisation avec une seconde paire de clés cryptographiques asymétriques.

[0085] Les figures 5 [Fig. 5] et 6 [Fig. 6] sont deux schémas simplifiés illustrant deux exemples de réalisation afin que les entités coopérantes conviennent d'une seconde paire de clés cryptographiques asymétriques, à savoir une réalisation avec tirage aléatoire et une réalisation impliquant une autorité de certification externe.

[0086] La figure 7 [Fig. 7] est un schéma simplifié illustrant que des entités coopérantes mettent en commun des données confidentielles propres et qu'un traitement numérique est appliqué à l'ensemble de celles-ci afin de créer un secret commun.

[0087] La figure 8a [Fig. 8a] est un schéma simplifié illustrant une réalisation dans laquelle les données confidentielles propres sont tirées aléatoirement par chacune des entités coopérantes.

[0088] La figure 8b [Fig. 8b] est un schéma illustrant une autre réalisation dans laquelle les données confidentielles propres sont introduites par les entités coopérantes dans la mémoire des processeurs de sécurité associés.

[0089] La figure 9 [Fig. 9] est un schéma simplifié illustrant que, moyennant un algorithme de découpage/reconstitution, le secret commun est découpé en parties découpées puis reconstitué ultérieurement.

[0090] La figure 10 [Fig. 10] est un schéma simplifié illustrant la mise en commun des données confidentielles propres et leur le traitement numérique afin de créer un secret commun, puis son découpage au moyen d'un algorithme de découpage et sa répartition entre entités coopérantes, puis sa reconstitution au moyen d'un algorithme de reconstitution.

[0091] Les figures 11 [Fig. 11] et 12 [Fig. 12] sont deux schémas simplifiés illustrant deux exemples de réalisation possible en ce qui concerne le processus de vérification d'intégrité de l'application, à savoir une vérification directe (figure 11 [Fig. 11]) et une vérification indirecte par transitivité (figure 12 [Fig. 12]).

[0092] Ci-après un exposé détaillé de modes d'exécution de l'invention et de différentes réalisations, assorti d'exemples et de référence aux figures. Cet exposé doit être compris dans le contexte de l'invention et avec l'interprétation des termes, comme il a été présenté précédemment.

[0093] Dans une application possible, un procédé de validation d'une requête numérique RN, selon l'invention, est appliqué à un procédé de traitement d'une requête numérique RN d'une entité demanderesse ED.

[0094] Comme il a été exposé, la gouvernance de sécurité du traitement d'une requête numérique RN doit être considérée dans son acception la plus large et générique, de sorte à inclure, notamment mais non exclusivement, un procédé de gouvernance de signature électronique, un procédé de gouvernance de chiffrement ou déchiffrement de données, un procédé de vote électronique, un procédé de gouvernance de transactions bancaires ou monétiques.

[0095] L'entité demanderesse ED est une personne ou un robot informatique qui est apte à faire ou à procéder à la requête numérique RN et qui, concrètement fait ou procède à cette requête numérique RN.

[0096] La requête numérique RN est un message adressé à un moyen électronique et informatique MEI approprié. Dans des réalisations possibles, une telle requête numérique RN et un tel moyen électronique et informatique MEI sont un formulaire Internet porté par un serveur, rempli par l'entité demanderesse ED.

[0097] Dans la suite du texte, le procédé de validation d'une requête numérique RN est parfois appelé, par ellipse, procédé de validation et, par analogie, le procédé de traitement d'une requête numérique RN est parfois appelé, par ellipse, procédé de traitement.

[0098] Le procédé de validation met en œuvre un système de validation SV qui comporte au moins deux processeurs de sécurité PS, support d'une application AP nécessaire au traitement de la requête RN, par suite appropriée à cette fin, et mettant en œuvre des données confidentielles DC. Un tel processeur de sécurité PS comprend une mémoire persistante, une mémoire volatile, un calculateur apte à réaliser des fonctions cryptographiques et notamment à authentifier tout ou partie du contenu de ses mémoires en fournissant une attestation numérique d'intégrité AN sur demande. L'application AP est chargée dans une mémoire d'un tel processeur de sécurité PS et exprime l'ensemble des règles exécutées avec des données confidentielles DC et des paramètres. En l'espèce, l'application AP inclut au moins un processus de création de secret commun SC.

[0099] Dans le procédé de validation, il est prévu une pluralité (au moins deux) d'entités coopérantes EC, lesquelles sont aptes et destinées à mettre en œuvre chacune un processeur de sécurité PS.

[0100] Le contenu des mémoires des processeurs de sécurité PS ne peut être modifié qu'avec une authentification, ce qui permet de qualifier les processeurs PS comme étant « de sécurité ».

[0101] Le système de validation SV comporte en outre un moyen apte et destiné à créer un secret commun SC, un algorithme d'attestation numérique, un algorithme de chiffrement et déchiffrement ALCD, un algorithme de découpage / reconstitution de secret commun SC, ALDE/ALRE, un algorithme d'échange de clés de session ALEC, des moyens de communication entre les processeurs de sécurité PS et les entités EC, ED.

[0102] Les moyens constitutifs du système de validation SV, dont sont exposés par la suite les fonctions remplies et les résultats procurés, peuvent faire l'objet de différentes réalisations, connues ou à la portée de l'homme du métier, ainsi que de réalisations équivalentes pour assurer les mêmes fonctions et procurer des résultats identiques ou analogues.

[0103] Dans une réalisation possible, un processeur de sécurité PS est par exemple une carte à puce.

[0104] Dans des réalisations possibles, un moyen apte et destiné à créer un secret commun SC est fondé sur une fonction OU exclusif (souvent appelée XOR) ; un algorithme d'attestation numérique est un algorithme ECDSA (pour Elliptic Curve Digital Signature Algorithm) ; un algorithme de chiffrement et déchiffrement est un al-

gorithme AES (pour Advanced Encryption Starndard) ; un algorithme de découpage / reconstitution de secret commun SC est un algorithme SSS (pour Shamir's Secret Sharing) ; un algorithme d'échange de clés de session est un algorithme SCDH (pour Elliptic Curve Diffie-Hellman), des moyens de communication entre les processeurs de sécurité PS et les entités EC, ED sont des liaisons télématiques.

[0105] Ces réalisations sont données à titre purement exemplatif. Elles ne sont pas limitatives.

[0106] Le procédé de traitement met en œuvre le procédé de validation dont il a été question précédemment, de sorte que la requête RN est traitée si et seulement si des entités coopérantes EC d'un collège d'entités coopérantes signataires COECS dont il est question par la suite, mettent en œuvre l'application AP moyennant un secret commun SC dont il est également question par la suite. Pour ce faire, l'entité demanderesse ED transmet la requête RN d'une part au collège d'entités coopérantes COEC, d'autre part à un le moyen électronique et informatique MEI, conçu et choisi de sorte à être apte et destiné à exécuter la requête RN. Le collège d'entités coopérantes COEC met en œuvre le procédé de validation, moyennant le secret commun SC, en vue de la validation de la requête RN. Le moyen électronique et informatique MEI exécute alors la requête RN en fonction de la validation.

[0107] Par « collège d'entités » on entend plusieurs entités (au moins deux) ayant pour caractéristique commune de concourir à un même processus donné, comme notamment un processus de vérification d'intégrité ou un processus de création de secret commun, dont il est question par la suite.

[0108] Le moyen électronique et informatique MEI peut faire l'objet de différentes réalisations, connues ou à la portée de l'homme du métier, en fonction de la requête RN, du service correspondant et de l'environnement dans lequel se déroule le procédé de traitement de la requête RN.

[0109] Dans des réalisations possibles, un moyen électronique et informatique MEI est un ordinateur, quel qu'en soit la forme.

[0110] Le procédé de validation permet d'assurer une gouvernance de sécurité, dans la mesure où cela conduit à vérifier la conformité de la requête numérique RN au corpus de règles définies en commun par les entités coopérantes EC, et cela en mettant en œuvre les processeurs de sécurité PS chargés de l'application AP.

[0111] Les entités coopérantes EC sont, chacune, une personne ou un robot informatique apte à utiliser l'application AP.

[0112] Le procédé de traitement incluant le procédé de validation est illustré de façon simplifiée par la figure 1 [Fig. 1] représentant de façon schématique, l'entité demanderesse ED, une pluralité d'entités coopérantes EC comprenant ici trois entités, trois processeurs de sécurité PS, un par entité coopérante EC, les trois entités co-

opérantes EC et les trois processeurs de sécurité PS formant une sorte de « bloc » comprenant un collège d'entités coopérantes signataires COECS et leurs processeurs de sécurité PS associés, et le moyen électronique et informatique MEI apte et destiné à exécuter la requête RN. La flèche de référence a symbolise la demande de validation de la requête RN par l'entité demanderesse ED au « bloc ». Les flèches de référence b symbolisent le processus de validation de la requête RN de l'entité demanderesse ED au sein du « bloc », moyennant un processus de reconstitution de secret commun SC. La flèche de référence c symbolise le résultat de la validation transmise par le « bloc » à l'entité demanderesse ED et la référence d symbolise la requête validée transmise au le moyen électronique et informatique MEI.

[0113] Plus précisément, le procédé de validation est tel qu'une pluralité (au moins deux) d'entités coopérantes EC sont aptes à mettre en œuvre chacune un processeur de sécurité PS chargé avec la même application AP, pour laquelle chaque processeur de sécurité PS délivre une attestation numérique AN d'intégrité sur demande.

[0114] Ainsi, la requête numérique RN est validée et in fine traitée en la soumettant au consentement préalable de plusieurs entités, sans avoir à recourir à un tiers de confiance. En effet, les entités coopérantes EC consentent à l'exécution de la requête numérique RN, moyennant la mise en œuvre des technologies de la cryptographie à seuil, alors que ces entités coopérantes EC vont s'authentifier mutuellement en utilisant les attestations numériques AN délivrées par les processeurs de sécurité PS.

[0115] On se réfère maintenant à la figure 2 [Fig. 2] qui reprend une partie de la figure 1 [Fig. 1] et illustre deux réalisations possibles en ce qui concerne les processeurs de sécurité PS et les entités coopérantes EC. Dans une première réalisation (partie droite de la figure 2 [Fig. 2]), le processeur de sécurité PS est propre à une entité coopérante EC. Dans une seconde réalisation (partie gauche de la figure 2 [Fig. 2]), le processeur de sécurité PS est commun à plusieurs entités coopérantes. Dans tous les cas, le procédé de validation implique la mise en œuvre d'au moins deux processeurs de sécurité PS.

[0116] Le procédé de validation comporte un processus de vérification d'intégrité de l'application AP tel que, à partir des attestations numériques AN délivrées par chaque processeur de sécurité PS, chaque entité EC de la pluralité d'entités coopérantes EC s'assure que chacune des autres entités EC de la pluralité d'entités EC met en œuvre une application AP identique à la sienne en vérifiant de façon cryptographique l'attestation numérique correspondante AN.

[0117] A cet effet, et dans une réalisation (voir schéma de la figure 3 [Fig. 3]), moyennant la mise en œuvre d'un processus cryptographique PCR, on met en œuvre des processeurs de sécurité PS choisis de sorte qu'ils disposent chacun, en propre, d'une première paire de clés cryptographiques asymétriques CC1. A la demande d'une ou plusieurs entités

coopérantes EC, chaque processeur de sécurité PS utilise la clé privée CPR1 de la première paire de clés CC1 pour produire (ce qui est symbolisé par la flèche de référence a de la figure 3 [Fig. 3]) une signature électronique de tout ou partie du contenu de ses mémoires COMEM. Cette signature électronique vaut attestation numérique AN d'intégrité du contenu signé correspondant, et son authenticité peut être vérifiée en utilisant la clé publique CPU1 de la première paire de clés CC1.

[0118] De plus, (voir schéma de la figure 4 [Fig. 4]), les entités coopérantes EC conviennent ensemble d'une seconde paire de clés cryptographiques asymétriques CC2. Puis, la clé privée CPR2 de la seconde paire de clés CC2 est mise en œuvre pour produire la signature électronique de la clé publique CPU1 des premières paires de clés CC1 de chaque processeur de sécurité PS, précédemment mentionnées. Ainsi, les entités coopérantes EC sont aptes à authentifier, en mettant en œuvre la clé publique CPU2 de la seconde paire de clés CC2, les attestations numériques AN d'intégrité délivrées par chacun des processeurs de sécurité PS. Sur la figure 4 [Fig. 4], la flèche de référence a symbolise l'extraction de la clé publique CPU1 de la première paire de clés CC1 et la flèche de référence b symbolise la signature, par la clé privée CPR2 de la seconde paire de clés CC2, de la clé publique CPU1 de la première paire de clés CC1.

[0119] On peut envisager deux réalisations afin que les entités coopérantes EC conviennent d'une seconde paire de clés cryptographiques asymétriques CC2. Dans une réalisation (voir schéma de la figure 5 [Fig. 5]), les entités coopérantes EC utilisent une paire de clés cryptographiques asymétriques tirée aléatoirement et partagées entre elles. Dans une autre réalisation (voir schéma de la figure 6 [Fig. 6]), la seconde paire de clés cryptographiques asymétriques CC2 est celle d'une autorité de certification externe. Ces deux réalisations ne sont pas exclusives d'autres, différentes, connues ou à la portée de l'homme du métier, procurant un résultat analogue.

[0120] Sur la figure 5 [Fig. 5], la flèche de référence a symbolise le tirage aléatoire et le partage de la clé privée CPR2 de la seconde paire de clés CC2 et la flèche de référence b symbolise la mise en œuvre de la clé privée CPR2 de la seconde paire de clés CC2 pour fournir la signature électronique de la clé publique CPR1 de la première paire de clés CC1.

[0121] Sur la figure 6 [Fig. 6] , la flèche de référence a symbolise la fourniture de la clé publique CPU1 de la première paire de clés CC1 à l'autorité de certification externe ACE, la flèche de référence b symbolise la mise en œuvre de la clé privée CPR2 de la seconde paire de clé CC2 de l'autorité de certification externe ACE pour signer la clé publique CPU1 de la première paire de clés CC1 (création d'attestation numérique AN), et la flèche de référence c symbolise le retour de la signature électronique de la clé publique CPU1 de la première paire de clés CC1 par la clé privée CPR2 de la

seconde paire de clés CC2, en vue de son stockage dans le processeur de sécurité PS.

[0122] Outre le processus de vérification d'intégrité de l'application AP, le procédé de validation comporte également un processus par lequel des entités coopérantes EC créent un secret commun SC et constituent ainsi un collège d'entités coopérantes créatrices COECC.

[0123] A cet effet, et dans une réalisation (voir schéma de la figure 7 [Fig. 7]), des entités coopérantes EC mettent en commun des données confidentielles propres DC et un traitement numérique TN est appliqué à l'ensemble de ces données confidentielles propres DC afin de créer le secret commun SC.

[0124] On peut envisager plusieurs réalisations concernant les données confidentielles DC. Dans une réalisation

[0125] (voir figure 8a [Fig. 8a]), la flèche de référence b de cette figure symbolise les données confidentielles propres DC qui sont tirées aléatoirement par chacune des entités coopérantes EC. Dans une autre réalisation (voir figure 8b [Fig. 8b]), la flèche de référence a de cette figure symbolise les données confidentielles propres DC qui sont introduites par les entités coopérantes EC dans la mémoire des processeurs de sécurité PS associés. Dans une autre réalisation, les données confidentielles propres DC sont extraites de la mémoire des processeurs de sécurité PS associés. Ces réalisations peuvent éventuellement être combinées. Les différentes réalisations ne sont pas exclusives d'autres, différentes, connues ou à la portée de l'homme du métier, procurant un résultat analogue.

[0126] Comme il est illustré par la figure 9 [Fig. 9], il est prévu que, moyennant un algorithme de découpage/reconstitution ALDE/ALRE, le secret commun SC est apte à être découpé, en parties découpées PDE de sorte à être reconstitué ultérieurement.

[0127] Sur la figure 9 [Fig. 9], la flèche de référence a symbolise un tel découpage et la flèche de référence b symbolise une telle reconstitution.

[0128] Selon la réalisation représentée sur la figure 9 [Fig. 9], la reconstitution du secret commun SC peut être réalisée à partir, non de toutes les parties découpées PDE, mais seulement de certaines d'entre elles, lesquelles sont alors aptes et suffisantes à reconstituer ultérieurement dit secret commun SC. Selon une autre réalisation, toutes les parties découpées PDE sont nécessaires afin de reconstituer ultérieurement le secret commun SC.

[0129] Selon une réalisation, il est procédé à plusieurs découpages successifs du secret commun SC en parties découpées PDE. Dans ce cas, selon une réalisation, et à des fins de sécurité, le secret commun SC ne peut ensuite être reconstitué qu'à partir des parties découpées PDE issues d'un même découpage et non à partir de parties découpées PDE issues de plusieurs découpages.

[0130] Selon la réalisation représentée sur la figure 10 [Fig. 10], des entités coopérantes EC

mettent en commun des données confidentielles propres DC (ce qui est symbolisé par la flèche de référence a de la figure 10 [Fig. 10]), le traitement numérique TN appliqué à l'ensemble de ces données confidentielles propres DC afin de créer le secret commun SC, comme il a été précédemment exposé. Puis, le secret commun SC ainsi créé est découpé en un nombre de parties découpées créatrices PDEC qui est égal au nombre d'entités coopérantes créatrices ECC constituant un collège COECC, au moyen d'un algorithme de découpage ALDE (ce qui est symbolisé par la flèche de référence b de la figure 10 [Fig. 10]). Les parties découpées créatrices PDEC sont alors réparties entre les entités coopérantes créatrices ECC, chacune d'elles conservant l'une des parties découpées créatrices PDEC (ce qui est symbolisé par la flèche de référence c de la figure 10 [Fig. 10]). Puis, au moyen d'un algorithme de reconstitution ALRE, le secret commun SC est reconstitué avec au moins certaines des (deux sur trois dans le cas de la figure 10 [Fig. 10]) parties découpées créatrices PDEC. Ou bien, dans une réalisation, le secret commun SC est reconstitué avec toutes les parties découpées créatrices PDEC.

[0131] Selon une possibilité visant à davantage de sécurité, le secret commun SC ne peut être utilisé que pour la validation d'une et une seule requête numérique RN et il ne peut être stocké de manière persistante dans aucune des mémoires des processeurs de sécurité PS associés.

[0132] Deux réalisations possibles peuvent être envisagées en ce qui concerne le processus de vérification d'intégrité de l'application AP tel que, à partir des attestations numériques AN délivrées par chaque processeur de sécurité PS, chaque entité coopérante EC s'assure que chacune des autres entités coopérantes EC met en œuvre une application AP identique à la sienne en vérifiant de façon cryptographique l'attestation numérique correspondante AN.

[0133] Selon une première réalisation possible illustrée par la figure 11 [Fig. 11] , chaque entité coopérante EC s'en assure directement. Sur la figure 11 [Fig. 11] sont représentées trois entités coopérantes EC, trois processeurs de sécurité PS avec les applications AP. Les deux flèches de référence a de la figure 11 [Fig. 11] symbolisent la délivrance par deux entités coopérantes EC à la troisième entité coopérante EC des attestations AN de leur application AP propre. La flèche de référence b de la figure 11 [Fig. 11] symbolise la vérification par la troisième entité coopérante EC que les applications des deux premières entités coopérantes EC sont identiques à la sienne. La vérification est donc directe.

[0134] Selon une seconde réalisation possible illustrée par la figure 12 [Fig. 12] , chaque entité coopérante EC s'assure que chacune des autres entités coopérantes EC met en œuvre une application AP identique à la sienne en vérifiant de façon cryptographique l'attestation numérique AN correspondante, non pas de façon directe comme dans la

première réalisation, mais de façon indirecte et par transitivité, en s'assurant qu'une certaine entité coopérante ECT met en œuvre une application AP identique à la sienne en vérifiant de façon cryptographique l'attestation numérique AN correspondante, cette certaine entité coopérante ECT s'étant elle-même assurée que les autres entités coopérantes EC mettent en œuvre la même application AP. Sur la figure 12 [Fig. 12] sont représentées quatre entités coopérantes EC, dont la certaine entité ECT, quatre processeurs de sécurité PS avec les applications AP. Les deux flèches de référence a de la figure 12 [Fig. 12] symbolisent la délivrance par deux entités coopérantes EC à la certaine entité coopérante ECT, des attestations AN de leur application AP propre. La flèche de référence b de la figure 12 [Fig. 12] symbolise la vérification par cette la certaine entité coopérante ECT que les applications AP des deux premières entités coopérantes EC sont identiques à la sienne. La flèche de référence c de la figure 12 [Fig. 12] symbolise la délivrance par la certaine entité coopérante ECT à la quatrième entité coopérante EC d'une attestation AN de son application AP propre, laquelle est identique à celle des deux premières entités coopérantes EC. Et, enfin, la flèche de référence d de la figure 12 [Fig. 12] symbolise la vérification par cette quatrième entité coopérante EC que l'application AP de la certaine entité coopérante ECT et donc aussi de manière transitive l'application AP des deux premières entités coopérantes EC sont identiques à la sienne. La vérification est donc ici indirecte.

[0135] Selon une possibilité visant à davantage de sécurité, les données confidentielles propres DC sont transmises de manière confidentielle, moyennant un algorithme de chiffrement et déchiffrement, entre les entités coopérantes créatrices ECC, en utilisant au moins une clé de session, laquelle clé de session est rendue inutilisable après la création d'un secret commun SC.

[0136] De même, des parties découpées PDE issues d'un même découpage du secret commun SC sont transmises de manière confidentielle, moyennant un algorithme de chiffrement et déchiffrement, entre les entités coopérantes EC en utilisant au moins une clé de session, la clé de session étant rendue inutilisable après la reconstitution dudit secret commun SC.

[0137] Selon une réalisation possible, les entités coopérantes créatrices ECC comprennent une première entité créatrice pilote ECCP1 et les autres entités coopérantes créatrices ECCA1.

[0138] Il est utilisé une pluralité de clés de session, de sorte que chaque entité coopérante créatrice ECC met en œuvre une clé propre pour communiquer de manière confidentielle, moyennant un algorithme de chiffrement et déchiffrement ALCD, avec la première entité créatrice pilote ECCP1. L'application AP intègre un algorithme d'échange des clés de session, ALEC. Et, la première entité créatrice pilote ECCP1 initie l'algorithme d'échange de clés de session ALEC avec chacune des autres entités

coopérantes créatrices ECCA1.

[0139] Ce faisant, les autres entités coopérantes créatrices ECCA1 transmettent, de manière confidentielle en utilisant leur propre clé de session, moyennant un algorithme de chiffrement et déchiffrement ALCD, et non rejouable, leurs données confidentielles propres DC à la première entité créatrice pilote ECCP1.

[0140] Le procédé est ensuite réitéré, chaque entité coopérante créatrice ECC devenant la première entité créatrice pilote ECCP1.

[0141] Ainsi, les entités coopérantes créatrices ECC sont aptes à appliquer un traitement numérique à l'ensemble des données confidentielles propres DC, créant ainsi le secret commun SC.

[0142] Selon une autre réalisation possible, les entités coopérantes créatrices ECC comprennent une seconde entité créatrice pilote ECCP2 et les autres entités coopérantes créatricesECCA2.

[0143] Il est utilisé une pluralité de clés de session, de sorte que chaque entité coopérante signataire ECS met en œuvre une clé propre pour communiquer de manière confidentielle, moyennant un algorithme de chiffrement et déchiffrement ALCD, avec la seconde entité créatrice pilote ECCP2.

[0144] Il est aussi utilisé une pluralité de clés de session, de sorte que chaque entité coopérante créatrice ECC met en œuvre une clé propre pour communiquer de manière confidentielle, moyennant un algorithme de chiffrement et déchiffrement ALCD, avec la seconde entité créatrice pilote ECCP2.

[0145] La seconde entité créatrice pilote ECCP2 met en œuvre un processus de vérification d'intégrité de l'application AP portée par le processeur de sécurité PS de chaque entité coopérante signataire ECS, de sorte que la seconde entité créatrice pilote ECCP2 s'assure que chacune des entités coopérantes signataires ECS met en œuvre une application AP identique à la sienne en vérifiant de façon cryptographique l'attestation numérique AN correspondante.

[0146] L'application AP intègre un algorithme d'échange des clés de session ALEC. Puis, est initié l'algorithme d'échange de clés de session ALEC entre, d'une part, chacune des autres entités coopérantes créatrices ECCA2 et chacune des entités coopérantes signataires ECS et, d'autre part, la seconde entité créatrice pilote ECCP2.

[0147] Ainsi, toutes les, ou au moins certaines des (en nombre suffisant à la reconstitution du secret commun SC) autres entités coopérantes créatrices ECCA2 transmettent, de manière confidentielle en utilisant leur propre clé de session, moyennant un algorithme de chiffrement et déchiffrement ALCD, et non rejouable, leurs parties découpées créatrices PDEC issues d'un même découpage du secret commun SC à la seconde entité créatrice pilote ECCP2.

[0148] La seconde entité créatrice pilote ECCP2 reconstitue le secret commun SC.

[0149] La seconde entité créatrice pilote ECCP2 découpe le secret commun SC en un nombre de parties découpées signataires PDES égal au nombre d'entités coopérantes signataires ES.

[0150] La seconde entité créatrice pilote ECCP2 transmet, de manière confidentielle en utilisant les clés de session, moyennant un algorithme de chiffrement et déchiffrement ALCD, et non rejouable, leurs parties découpées signataires PDES du secret commun SC aux entités coopérantes signataires ECS.

[0151] Selon une réalisation possible, les entités coopérantes EC comprennent une entité pilote ECP et les autres entités coopérantes ECA. Il est utilisé une pluralité de clés de session, de sorte que chaque entités coopérantes EC met en œuvre une clé propre pour communiquer de manière confidentielle, moyennant un algorithme de chiffrement et déchiffrement ALCD, avec l'entité pilote ECP. L'application AP intègre un algorithme d'échange des clés de session ALEC. L'entité pilote ECP initie l'algorithme d'échange de clés de session ALEC avec chacune des autres entités coopérantes EC. Ainsi, toutes les, ou au moins certaines des (en nombre suffisant à la reconstitution du secret commun SC) autres entités coopérantes ECA transmettent, de manière confidentielle en utilisant leur propre clé de session, moyennant un algorithme de chiffrement et déchiffrement ALCD, non rejouable, leurs parties découpées PDE issues d'un même découpage du secret commun SC à l'entité pilote ECP.

[0152] Comme il résulte de l'exposé qui précède, le procédé de validation comporte, moyennant la mise en œuvre du processus de vérification d'intégrité de l'application AP, un processus par lequel des entités ECC du collège d'entités coopérantes créatrices COECC désignent les entités coopérantes signataires ES, constituant ainsi un collège d'entités coopérantes signataires COECS. Ce collège d'entités coopérantes signataires COES, pris en tant que tel, a accès au secret commun SC.

[0153] Finalement, la requête RN est validée si et seulement si des entités coopérantes ECS du collège d'entités coopérantes signataires COECS mettent en œuvre l'application AP moyennant le secret commun SC. Selon les cas, il s'agit de toutes les entités coopérantes signataires ou seulement d'un quorum du collège d'entités coopérantes signataires COECS.

[0154] Selon les cas, le collège d'entités coopérantes créatrices COECC et le collège d'entités coopérantes signataires COECS sont distincts ou bien le collège d'entités coopérantes créatrices COECC et le collège d'entités coopérantes signataires COECS sont au moins pour partie communs.

Revendications

[Revendication 1] Procédé de validation d'une requête numérique (RN) :

- dans lequel une pluralité d'entités coopérantes (EC) sont aptes à mettre en œuvre chacune un processeur de sécurité (PS) chargé avec une même application (APP) nécessaire au traitement de ladite requête (RN), application (APP) pour laquelle chaque processeur de sécurité (PS) délivre une attestation numérique (AN) d'intégrité sur demande, ledit processeur de sécurité (PS) étant apte à être mis en œuvre soit par une entité coopérante (EC) auquel cas ledit processeur de sécurité (PS) est propre à cette entité coopérante (EC) soit par plusieurs entités coopérantes (EC) auquel cas ledit processeur de sécurité (PS) est commun à ces entités coopérantes (EC), le procédé impliquant la mise en œuvre d'au moins deux processeurs de sécurité (PS).
- qui comporte un processus de vérification d'intégrité de ladite application (APP) tel que, à partir des attestations numériques (AN) délivrées par chaque processeur de sécurité (PS), chaque entité (EC) de la pluralité d'entités coopérantes (EC) s'assure que chacune des autres entités (EC) de la pluralité d'entités (EC) met en œuvre une application (APP) identique à la sienne en vérifiant de façon cryptographique l'attestation numérique (AN) correspondante,
- qui comporte un processus par lequel des entités coopérantes (ECC) créent un secret commun (SC) et constituent ainsi un collège d'entités coopérantes créatrices (COECC),
- qui comporte, moyennant la mise en œuvre du processus de vérification d'intégrité de ladite application (APP), un processus par lequel des entités (ECC) du collège d'entités coopérantes créatrices (COECC) désignent les entités coopérantes signataires (ECS), constituant ainsi un collège d'entités coopérantes signataires (COECS), en sorte que ledit collège d'entités coopérantes signataires (COECS) pris en tant que tel ait accès au secret commun (SC),

de sorte que ladite requête (RN) est validée si et seulement si des entités

coopérantes (ECS) du collège d'entités coopérantes signataires (COECS) mettent en œuvre ladite application (APP) moyennant le secret commun (SC).

[Revendication 2] Procédé de validation d'une requête numérique (RN) selon la revendication 1, dans lequel pour que chaque processeur de sécurité (PS) délivre une attestation numérique (AN) d'intégrité sur demande :

- on met en œuvre des processeurs de sécurité (PS) choisis de sorte qu'ils disposent chacun, en propre, d'une première paire de clés cryptographiques asymétriques (CC1),
- à la demande d'une ou plusieurs entités coopérantes (EC), chaque processeur de sécurité (PS) utilise la clé privée (CPR1) de ladite première paire de clés (CC1) pour produire une signature électronique de tout ou partie du contenu de ses mémoires,
- ladite signature électronique valant attestation numérique (AN) d'intégrité du contenu signé correspondant, et son authenticité peut être vérifiée en utilisant la partie publique (CPU1) de la dite première paire de clés (CC1).

[Revendication 3] Procédé de validation d'une requête numérique (RN) selon l'une des revendications 1 et 2, dans lequel, en outre, en vue du processus de vérification d'intégrité de ladite application (APP),

- les entités coopérantes (EC) de ladite pluralité d'entités coopérantes (COEC) conviennent ensemble d'une seconde paire de clés cryptographiques asymétriques (CC2),
- la partie privée (CPR2) de ladite seconde paire de clés (CC2) est mise en œuvre pour produire la signature électronique de la partie publique (CPU1) desdites premières paires de clés (CC1) de chaque processeur de sécurité (PS),
- de sorte que lesdites entités coopérantes (EC) sont aptes à authentifier, en mettant en œuvre la partie publique (CPU2) de ladite seconde paire de clés (CC2), les attestations numériques (AN) d'intégrité délivrées par chacun des processeurs de sécurité (PS).

[Revendication 4] Procédé de validation d'une requête numérique (RN) selon la reven-

dication 3, dans lequel, en vue de convenir de ladite seconde paire de clés cryptographiques asymétriques (CC2°, les entités coopérantes (EC) utilisent une paire de clés cryptographiques asymétriques tirée aléatoirement et partagées entre elles.

[Revendication 5] Procédé de validation d'une requête numérique (RN) selon la revendication 3, dans lequel, ladite seconde paire de clés cryptographiques asymétriques (CC2) est celle d'une autorité de certification externe (ACE).

[Revendication 6] Procédé de validation d'une requête numérique (RN) selon l'une des revendications 1 à 5, dans lequel, pour créer un secret commun (SC) :

- des entités coopérantes (EC) de la pluralité d'entités coopérantes (EC) mettent en commun des données confidentielles propres (DC),
- un traitement numérique (TN) est appliqué à l'ensemble desdites données confidentielles propres (DC), créant ainsi ledit secret commun (SC).

[Revendication 7] Procédé de validation d'une requête numérique (RN) selon la revendication 6 dans lequel les dites données confidentielles propres (DC) sont tirées aléatoirement par chacune des entités coopérantes (EC), et/ou introduites par les entités coopérantes (EC) dans la mémoire des processeurs de sécurité (PS) associées, et/ou extraites de la mémoire des processeurs de sécurité (PS) associés.

[Revendication 8] Procédé de validation d'une requête numérique (RN) selon l'une des revendications 1 à 7, dans lequel moyennant un algorithme de découpage/reconstitution (ALDE/ARE), le secret commun (SC) est apte à être découpé, en parties découpées (PDE) de sorte à être reconstitué ultérieurement et/ou dans lequel au moins certaines des, ou toutes les, parties découpées (PDE) sont aptes et suffisantes à reconstituer ultérieurement ledit secret commun (SC).

[Revendication 9] Procédé de validation d'une requête numérique (RN) selon la revendication 8, dans lequel :

- ledit secret commun (SC) une fois créé est découpé en un nombre de parties découpées créatrices (PDEC), égal au nombre d'entités coopérantes créatrices (ECC),
- et lesdites parties découpées créatrices (PDEC) sont réparties entre les entités coopérantes créatrices (ECC), chacune des

dites entités (ECC) conservant l'une desdites parties découpées créatrices (PDEC),

– de sorte qu'ultérieurement, ledit secret commun (SC) puisse être reconstitué avec au moins certaines des, ou toutes les, dites parties découpées créatrices (PDEC).

[Revendication 10] Procédé de validation d'une requête numérique (RN) selon l'une des revendications 1 à 9, dans lequel ledit secret commun (SC) ne peut être utilisé que pour la validation d'une et une seule requête numérique (RN) et ne peut être stocké de manière persistante dans aucune des mémoires des processeurs de sécurité (PS) associés.

[Revendication 11] Procédé de validation d'une requête numérique (RN) selon l'une des revendications 1 à 10, dans lequel lors de sa mise en œuvre, un processus de vérification d'intégrité de ladite application (APP) tel que, à partir des attestations numériques (AN) délivrées par chaque processeur de sécurité (PS), chaque entité (EC) de la pluralité d'entités coopérantes (EC) s'assure directement que chacune des autres entités (EC) de la pluralité d'entités (EC) met en œuvre une application (APP) identique à la sienne en vérifiant de façon cryptographique l'attestation numérique (AN) correspondante.

[Revendication 12] Procédé de validation d'une requête numérique (RN) selon l'une des revendications 1 à 10 dans lequel lors de sa mise en œuvre, un processus de vérification d'intégrité de ladite application (APP) tel que, à partir des attestations numériques (AN) délivrées par chaque processeur de sécurité (PS), chaque entité (EC) de la pluralité d'entités coopérantes (EC) s'assure que chacune des autres entités (EC) de la pluralité d'entités (EC) met en œuvre une application (APP) identique à la sienne en vérifiant de façon cryptographique l'attestation numérique (AN) correspondante, de façon indirecte et par transitivité, en s'assurant qu'une certaine entité (ECT) de la pluralité d'entités met en œuvre une application (APP) identique à la sienne en vérifiant de façon cryptographique l'attestation numérique (AN) correspondante, cette certaine entité (ECT) s'étant elle-même assurée que les autres entités (EC) de la pluralité d'entités (EC) mettent en œuvre la même application (APP).

[Revendication 13] Procédé de validation d'une requête numérique (RN) selon l'une des revendications 6 à 12 en ce qu'elles dépendent de la revendication 7, dans lequel lesdites données confidentielles propres (DC) sont transmises de

manière confidentielle, moyennant un algorithme de chiffrement et déchiffrement (ALCD), entre les entités coopérantes créatrices (ECC) en utilisant au moins une clé de session, ladite au moins une clé de session étant rendue inutilisable après la création d'un secret commun (SC).

[Revendication 14] Procédé de validation d'une requête numérique (RN) selon l'une des revendications 6 à 13 en ce qu'elles dépendent de la revendication 7, dans lequel :

- Les entités coopérantes créatrices (ECC) comprennent une première entité créatrice pilote (ECCP1) et les autres entités coopérantes créatrices (ECCA),
- il est utilisé une pluralité de clés de session, de sorte que chaque entité coopérante créatrice (ECC) met en œuvre une clé propre pour communiquer de manière confidentielle, moyennant un algorithme de chiffrement et déchiffrement (ALCD), avec ladite première entité créatrice pilote (ECCP1),
- ladite application (APP) intègre un algorithme d'échange des clés de session (ALEC),
- ladite première entité créatrice pilote (ECCP1), initie ledit algorithme d'échange de clés de session (ALEC) avec chacune des autres entités coopérantes créatrices (ECCA),
- de sorte que lesdites autres entités coopérantes créatrices (ECCA) transmettent, de manière confidentielle en utilisant leur propre clé de session, moyennant un algorithme de chiffrement et déchiffrement (ALCD), et non rejouable, leurs dites données confidentielles propres (DC) à ladite première entité créatrice pilote (ECCP1),
- le procédé étant réitéré, chaque entité coopérante créatrice (ECC) étant ladite première entité créatrice pilote (ECCP1),

de sorte que les entités coopérantes créatrices (ECC) sont aptes à appliquer un traitement numérique (TN) à l'ensemble desdites données confidentielles propres (DC), créant ainsi ledit secret commun (SC).

[Revendication 15] Procédé de validation d'une requête numérique (RN) selon l'une des revendications 8 à 14, en ce qu'elles dépendent de la revendication 9, dans lequel :

- les entités coopérantes créatrices (ECC) comprennent une seconde entité créatrice pilote (ECCP2) et les autres entités co-

opérantes créatrices (ECCA),

- il est utilisé une pluralité de clés de session, de sorte que chaque entité coopérante signataire (ECS) met en œuvre une clé propre pour communiquer de manière confidentielle, moyennant un algorithme de chiffrement et déchiffrement (ALCD), avec ladite seconde entité créatrice pilote (ECCP2),
- il est utilisé une pluralité de clés de session, de sorte que chaque entité coopérante créatrice (EC) met en œuvre une clé propre pour communiquer de manière confidentielle, moyennant un algorithme de chiffrement et déchiffrement (ALCD), avec ladite seconde entité créatrice pilote (ECCP2),
- ladite seconde entité créatrice pilote (ECCP2) met en œuvre un processus de vérification d'intégrité de ladite application (APP) portée par le processeur de sécurité (PS) de chaque entité coopérante signataire (ECS), de sorte que ladite seconde entité créatrice pilote (ECCP2) s'assure que chacune des entités coopérantes signataires (ECS) met en œuvre une application (APP) identique à la sienne en vérifiant de façon cryptographique l'attestation numérique (AN) correspondante,
- ladite application (APP) intègre un algorithme d'échange des clés de session (ALEC),
- est initié ledit algorithme d'échange de clés de session (ALEC) entre, d'une part, chacune des dites autres entités coopérantes créatrices (ECCA) et chacune des entités coopérantes signataires (ECS) et, d'autre part, ladite seconde entité créatrice pilote (ECCP2),
- de sorte que :
  - toutes les, ou au moins certaines des – en nombre suffisant à la reconstitution du secret commun (SC) -, dites autres entités coopérantes créatrices (ECC) transmettent, de manière confidentielle en utilisant leur propre clé de session, moyennant un algorithme de chiffrement et déchiffrement (ALCD), et non rejouable, leurs dites parties découpées créatrices (PDEC) issues d'un même découpage du secret commun (SC) à ladite seconde entité créatrice pilote (ECCP2),
  - ladite seconde entité créatrice pilote (ECCP2) re-

constitue le secret commun (SC),

- ladite seconde entité créatrice pilote (ECCP2) découpe le secret commun (SC) en un nombre de parties découpées (PDE) signataires égal au nombre d'entités coopérantes signataires (ECS),
- ladite seconde entité créatrice pilote (ECCP2) transmet, de manière confidentielle en utilisant les clés de session, moyennant un algorithme de chiffrement et déchiffrement (ALCD), et non rejouable, leurs dites parties découpées (PDE) signataires du secret commun (SC) aux dites entités coopérantes signataires (ECS).

[Revendication 16] Procédé de validation d'une requête numérique (RN) selon l'une des revendications 13 à 15 en ce qu'elle dépend de la revendication 8, dans lequel des parties découpées (PDE) issues d'un même découpage du secret commun (SC) sont transmises de manière confidentielle, moyennant un algorithme de chiffrement et déchiffrement (ALCD), entre les entités coopérantes (EC) en utilisant au moins une clé de session, ladite au moins une clé de session étant rendue inutilisable après la reconstitution dudit secret commun (SC).

[Revendication 17] Procédé de validation d'une requête numérique (RN) selon l'une des revendications 13 à 15 en ce qu'elle dépend de la revendication 8, dans lequel :

- les entités coopérantes (EC) comprennent une entité pilote (ECP) et les autres entités coopérantes (ECA),
- il est utilisé une pluralité de clés de session, de sorte que chaque entités coopérantes (EC) met en œuvre une clé propre pour communiquer de manière confidentielle, moyennant un algorithme de chiffrement et déchiffrement (ALCD), avec ladite entité pilote (ECP),
- ladite application (APP) intègre un algorithme d'échange des clés de session (ALEC),
- ladite entité pilote (ECP), initie ledit algorithme d'échange de clés de session (ALEC) avec chacune des autres entités coopérantes (EC),

de sorte que toutes les, ou au moins certaines des – en nombre suffisant à la reconstitution du secret commun (SC) -, dites autres entités coopérantes (EC) transmettent, de manière confidentielle en utilisant leur propre clé de session, moyennant un algorithme de chiffrement et déchiffrement (ALCD), non rejouable, leurs dites parties découpées (PDE) issues d'un même découpage du secret commun (SC) à ladite entité pilote (ECP).

[Revendication 18] Procédé de validation d'une requête numérique (RN) selon l'une des revendications 1 à 17, dans lequel le collège d'entités coopérantes créatrices (COECC) et le collège d'entités coopérantes signataires (COECS) sont distincts.

[Revendication 19] Procédé de validation d'une requête numérique (RN) selon l'une des revendications 1 à 17, dans lequel le collège d'entités coopérantes créatrices (COECC) et le collège d'entités coopérantes signataires (COECS) sont au moins pour partie communs.

[Revendication 20] Procédé de traitement d'une requête numérique (RN) d'une entité demanderesse (ED), avec une pluralité d'entités coopérantes (EC) qui sont aptes à mettre en œuvre chacune un processeur de sécurité (PS) chargé avec une même application (APP) nécessaire au traitement de ladite requête (RN), application (APP) pour laquelle chaque processeur de sécurité (PS) délivre une attestation numérique (AN) d'intégrité sur demande, qui met en œuvre le procédé de validation d'une requête numérique (RN) selon l'une des revendications 1 à 19, de sorte que ladite requête (RN) est traitée si et seulement si des entités coopérantes (ECS) du collège d'entités coopérantes signataires (COECS) mettent en œuvre ladite application (APP) moyennant le secret commun (SC).

[Revendication 21] Procédé de traitement d'une requête numérique (RN) d'une entité demanderesse (ED) selon la revendication 20, dans lequel :

- l'entité demanderesse (ED) transmet ladite requête numérique (RN) d'une part au collège d'entités coopérantes (COEC), d'autre part à un moyen électronique informatique (MEI) apte à exécuter ladite requête (RN),
- le collège d'entités coopérantes (EC) met en œuvre un procédé de validation, moyennant ledit secret commun (SC), en vue de la validation de ladite requête numérique (RN),

ledit moyen électronique informatique (MEI) exécute ladite requête

numérique (RN) en fonction de ladite validation.

[Revendication 22] Application du procédé de validation d'une requête numérique (RN) selon l'une des revendications 1 à 19, à un procédé de traitement d'une requête numérique (RN) d'une entité demanderesse (ED), notamment un procédé de gouvernance de signature électronique, un procédé de gouvernance de chiffrement ou déchiffrement de données, un procédé de vote électronique, un procédé de gouvernance de transactions bancaires ou monétiques.

[Revendication 23] Système pour la mise en œuvre du procédé de validation d'une requête numérique (RN) par une entité demanderesse (ED), selon l'une des revendications 1 à 19, qui comporte :

- au moins deux processeurs de sécurité (PS) support d'une application (APP) nécessaire au traitement de ladite requête (RN), mettant en œuvre des données confidentielles (DC), et comprenant une mémoire persistante, une mémoire volatile, un calculateur apte à réaliser des fonctions cryptographiques et notamment à authentifier tout ou partie du contenu de ses mémoires en fournissant une attestation numérique (AN) d'intégrité sur demande, de sorte qu'une pluralité d'entités coopérantes (EC) sont aptes à mettre en œuvre chacune un dit processeur de sécurité (PS), et dont le contenu des mémoires ne peut être modifié qu'avec une authentification,
- un moyen apte à créer un secret commun (SC),
- un algorithme d'attestation numérique (AN),
- un algorithme de chiffrement et déchiffrement (ALCD)
- un algorithme de découpage / reconstitution (ALDE/ALRE) de secret commun (SC),
- un algorithme d'échange de clés de session (ALEC),
- des moyens de communication entre les processeurs de sécurité (PS) et les entités.

FIGURE 1 [Fig. 1]

Figure 1

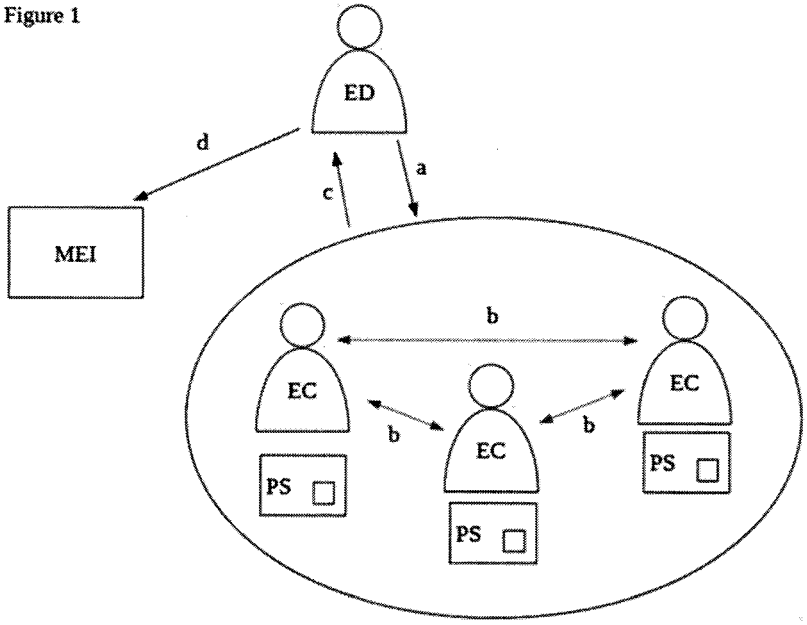


FIGURE 2 [Fig. 2]

Figure 2

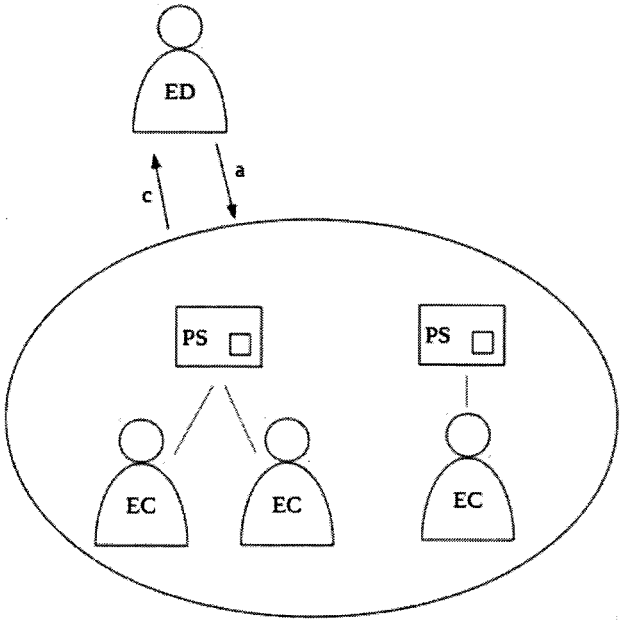


FIGURE 3 [Fig. 3]

Figure 3

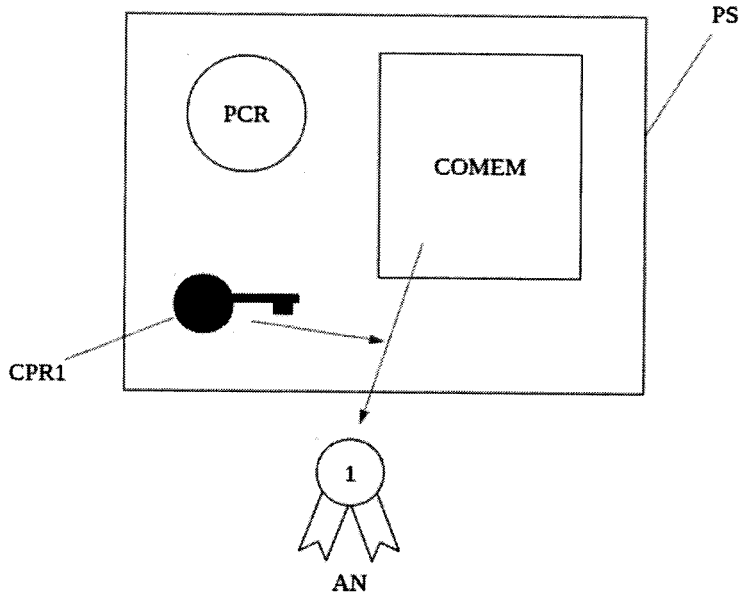


FIGURE 4 [Fig. 4]

Figure 4

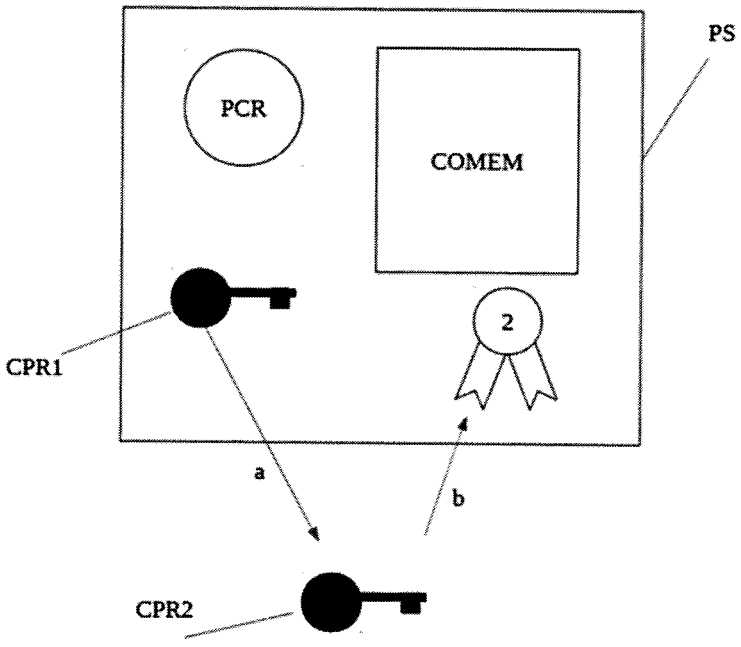


FIGURE 5 [Fig. 5]

Figure 5

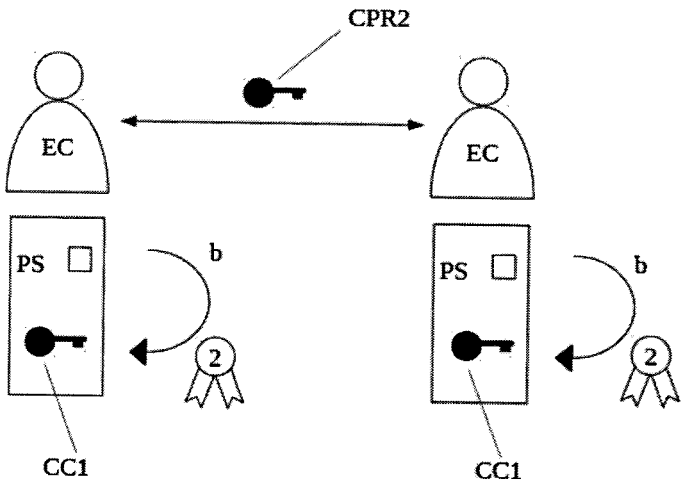


FIGURE 6 [Fig. 6]

Figure 6

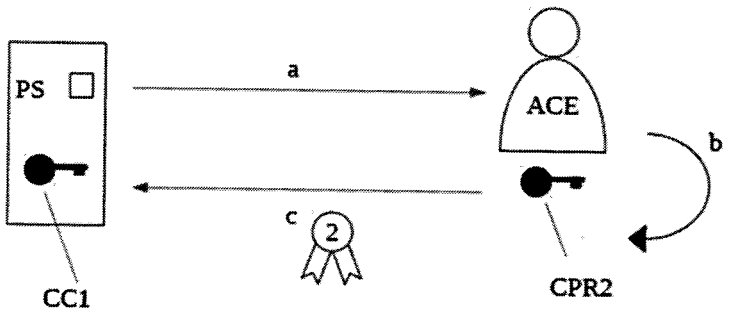


FIGURE 7 [Fig. 7]

Figure 7

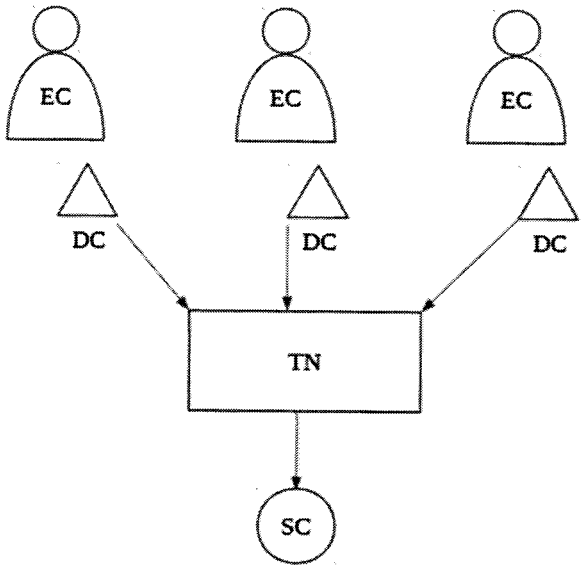


FIGURE 8b [Fig. 8b]

Figure 8b

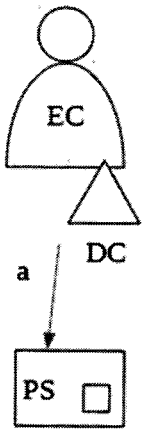


FIGURE 8 a [Fig. 8a]

Figure 8a

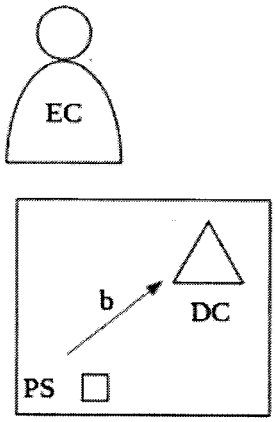


FIGURE 9 [Fig. 9]

Figure 9

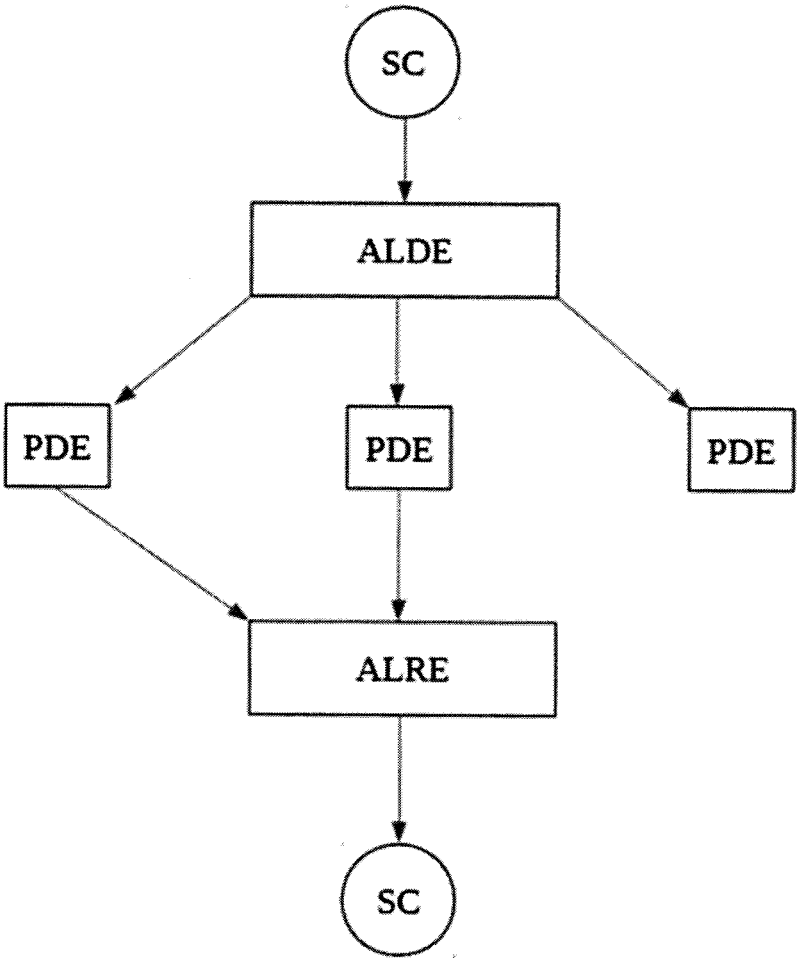


FIGURE 10 [Fig. 10]

Figure 10

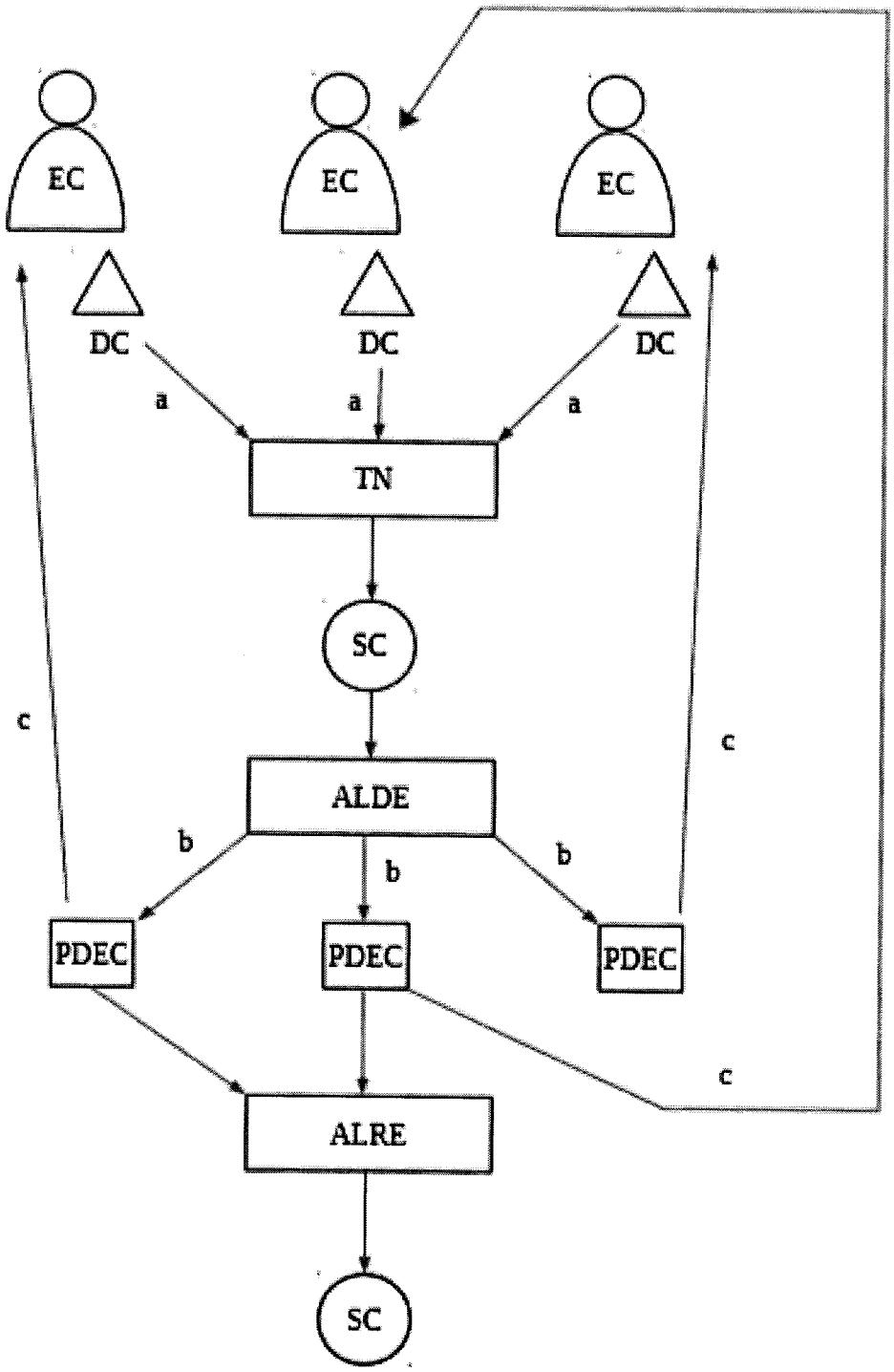


FIGURE 11 [Fig. 11]

Figure 11

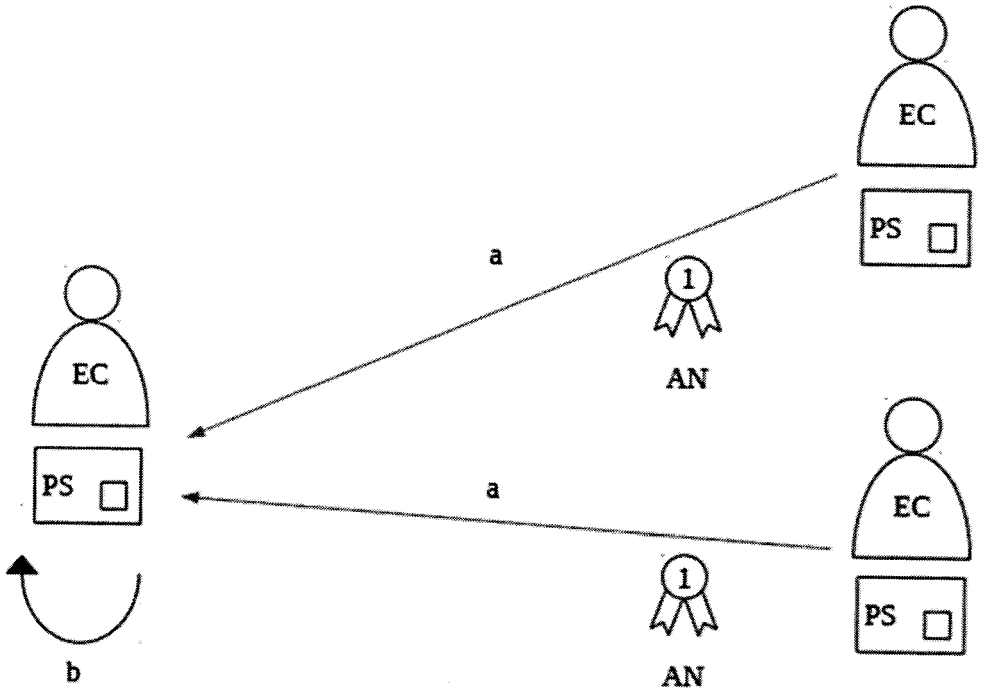
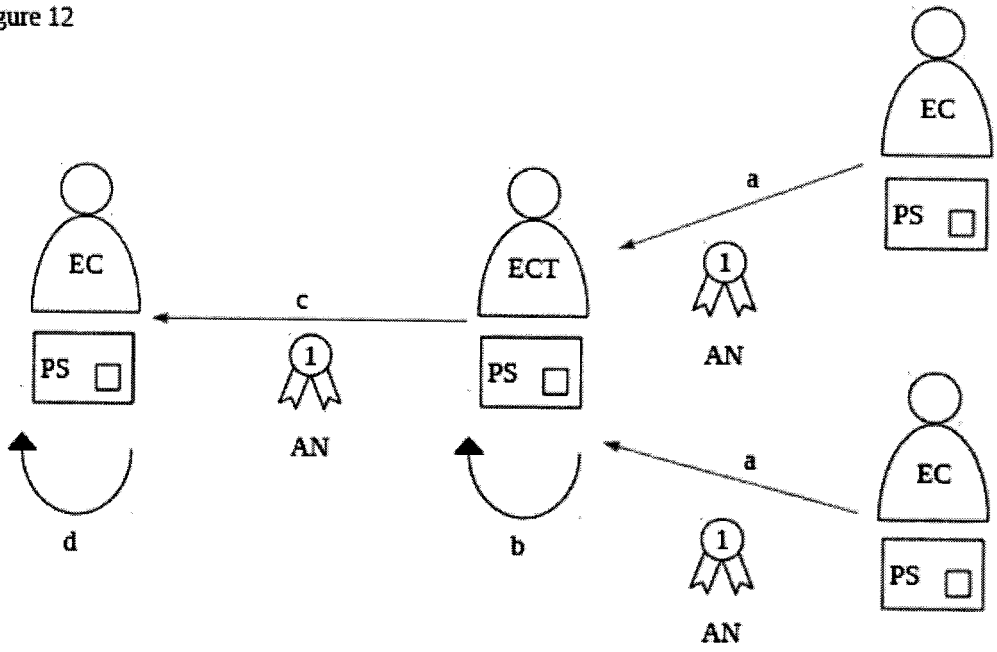


FIGURE 12 [Fig. 12]

Figure 12



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.

[x] 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

WO 2015/118160 A1 (THOMSON LICENSING [FR])
13 août 2015 (2015-08-13)

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

US 2015/229480 A1 (JOYE MARC [FR] ET AL)
13 août 2015 (2015-08-13)

WO 2015/160839 A1 (HRL LAB LLC [US]; EL DEFRAWY KARIM [US]; LAMPKINS JOSHUA D [US]) 22 octobre 2015 (2015-10-22)

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

NEANT