

Revendications

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,

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).

2. Procédé de validation d'une requête numérique (RN) selon la revendication 1, dans lequel un dit processeur de sécurité (PS) est 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).

3. Procédé de validation d'une requête numérique (RN) selon l'une des revendications 1 et 2, 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).

4. Procédé de validation d'une requête numérique (RN) selon l'une des revendications 1 à 3, 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).
5. Procédé de validation d'une requête numérique (RN) selon la revendication 4, 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.
6. Procédé de validation d'une requête numérique (RN) selon la revendication 4, dans lequel, ladite seconde paire de clés cryptographiques asymétriques (CC2) est celle d'une autorité de certification externe (ACE).
7. Procédé de validation d'une requête numérique (RN) selon l'une des revendications 1 à 6, 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).
8. Procédé de validation d'une requête numérique (RN) selon la revendication 7 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.
9. Procédé de validation d'une requête numérique (RN) selon l'une des revendications 1 à 8, 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).
10. Procédé de validation d'une requête numérique (RN) selon la revendication 9, 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).

11. Procédé de validation d'une requête numérique (RN) selon l'une des revendications 1 à 10, 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.
12. Procédé de validation d'une requête numérique (RN) selon l'une des revendications 1 à 11, 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.
13. Procédé de validation d'une requête numérique (RN) selon l'une des revendications 1 à 11 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).
14. Procédé de validation d'une requête numérique (RN) selon l'une des revendications 7 à 13 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).
15. Procédé de validation d'une requête numérique (RN) selon l'une des revendications 7 à 14 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).

16. Procédé de validation d'une requête numérique (RN) selon l'une des revendications 9 à 15, 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 coopérantes 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) reconstitue 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).

17. Procédé de validation d'une requête numérique (RN) selon l'une des revendications 14 à 16 en ce qu'elle dépend de la revendication 9, 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).

18. Procédé de validation d'une requête numérique (RN) selon l'une des revendications 14 à 16 en ce qu'elle dépend de la revendication 9, 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).

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

20. Procédé de validation d'une requête numérique (RN) selon l'une des revendications 1 à 18, dans lequel le collège d'entités coopérantes créatrices (COECC) et le collège d'entités coopérantes signataires (COECS) sont au moins pour partie communs.

21. 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 20, 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).
22. Procédé de traitement d'une requête numérique (RN) d'une entité demanderesse (ED) selon la revendication 21, 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.
23. Application du procédé de validation d'une requête numérique (RN) selon l'une des revendications 1 à 20, 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.
24. 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 20, 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.