

Traitement sécurisé de données

5 L'invention concerne le traitement sécurisé de données. Elle a plus précisément pour objet un processeur de sécurité du type comprenant une mémoire morte, une mémoire vive, un calculateur apte à réaliser des fonctions cryptographiques, et une unité de gestion de compteur monotone associée à au moins un compteur monotone, un ensemble de traitement sécurisé de données comprenant un tel processeur de sécurité et, avec des moyens de connexion, une mémoire extérieure, une infrastructure de traitement sécurisé de données comprenant plusieurs processeurs de sécurité, et enfin, un procédé de mise en œuvre d'un tel ensemble de traitement sécurisé de
10 données.

Dans le cadre de l'invention, la sécurisation s'entend du maintien et du contrôle de l'intégrité d'un programme composé d'instructions et du contexte y relatif, ainsi que de l'authentification des personnes donnant des ordres d'exécution des dits programme. Le terme « contexte » doit être compris comme un ensemble de paramètres,
15 d'instructions et de conditions, et plus largement tout ensemble d'instructions, de code ou données sous lesquels le programme peut être mis en œuvre. Le terme « administrateur » désigne d'une part l'administrateur enrôlé initial et d'autre part tout autre administrateur enrôlé ultérieur. Par « enrôlé », il faut comprendre enregistré, inscrit, ou, en d'autres termes, autorisé à donner des instructions. Par « authentification d'un administrateur enrôlé » on désigne le processus par lequel on vérifie qu'une personne donnant des instructions est un administrateur enrôlé et on
20 autorise l'exécution des instructions en question par le processeur de sécurité. Par « authentification des administrateurs enrôlés » on désigne un processus analogue appliqué de façon individuelle à plusieurs personnes et aux administrateurs enrôlés.

Le document FR2906380 décrit un système de sécurisation de données stockées sur un support physique et le
25 procédé de sa mise en œuvre. Le système de sécurisation de données est embarqué dans un dispositif comme un téléphone portable comprenant notamment un boîtier muni d'un clavier, d'un écran, d'un microphone, d'un haut-parleur, d'une carte électronique, d'un module pour l'émission et la réception de données, d'un module d'identification abonné et d'une batterie pour l'alimentation électrique. La carte électronique comprend au moins un microcontrôleur, une mémoire vive, une mémoire Flash, et un système de bus. L'exploitation du téléphone est gérée
30 par un système d'exploitation et un ensemble d'applications chargées par exemple dans une mémoire de ce téléphone. Le système de sécurisation comprend, formant un tout, une entité de calcul (comme un microprocesseur) avec le cas échéant des ressources système comme une mémoire vive, un compteur monotone (qui ne peut que s'incrémenter que d'une seule unité), une clé système (clé cryptographique accessible aux seules entités autorisées par le système), et un support physique de données assurant le stockage persistant de données
35 informatiques (comme un disque dur, une mémoire flash, etc.). Ce support physique de données comprend au moins un bloc de données et deux blocs maîtres, dont les tailles sont configurables. Le procédé de mise en œuvre utilise une clé d'authentification. Le système de sécurisation de données et le procédé de sa mise en œuvre du document FR2906380 visent à résoudre un problème de sécurisation contre, d'une part, le rejeu (accès frauduleux à des données par copie illicite du contenu antérieur d'un système de gestion de données) et, d'autre part, les
40 altérations ou modifications induites notamment par des interruptions brutales de service (comme une coupure du courant d'alimentation électrique ou un redémarrage intempestif du système). Ce document n'assure pas l'authentification des administrateurs.

Le document US 2004/0187006 concerne le domaine de la sécurité des données et plus particulièrement la
45 récupération fiable de données à partir d'une mémoire externe non sécurisée car étant située en dehors d'un environnement sécurisé. Le système de sécurisation de données comprend une entité de calcul et l'utilisation d'un compteur monotone pour déterminer, dans l'environnement sécurisé, si une requête vers la mémoire externe

renvoie les données les plus récentes. Le compteur monotone est incrémenté chaque fois qu'un élément principal est écrit dans la mémoire. Une entrée de contrôle enregistre l'heure de la dernière modification de l'élément lié à celui-ci. La valeur du compteur monotone reste la même jusqu'à la prochaine écriture de données dans la mémoire.

- 5 Si ce document fait état de la mise en œuvre d'un compteur monotone, il n'a pas pour but la sécurisation objet de l'invention.

Le document US2014/0137178 se rapporte à un procédé comprenant les étapes consistant à réceptionner, par un module de plate-forme sécurisé TPM d'un dispositif informatique, une demande émanant d'un programme du
10 dispositif informatique pour accéder à des informations contenues dans un objet protégé; déterminer si des conditions permettant au programme d'accéder à l'information sont remplies; permettre au programme d'accéder aux informations en réponse aux conditions remplies; refuser au programme l'accès à l'information en réponse aux conditions non remplies; et verrouiller, en réponse à une condition non remplie pour un nombre seuil de demandes provenant du programme, les informations pendant une durée indéterminée pour empêcher le programme
15 d'accéder aux informations. Des objets sont maintenus par un module de plateforme sécurisé. Chacun des objets stocke des informations et est associé à une politique identifiant les conditions auxquelles un programme doit satisfaire pour que le programme puisse accéder aux informations. Pour chacun des objets, le module de plate-forme sécurisée gère un compteur monotone associé à l'objet. Le compteur monotone est utilisé pour déterminer si un nombre seuil de demandes d'accès aux informations de l'objet sont effectuées qui ne satisfont pas aux
20 conditions de la stratégie associée à l'objet. Le module de plateforme sécurisée fournit un stockage sécurisé et / ou une fonctionnalité de traitement sécurisé au dispositif informatique. Le stockage sécurisé fait référence à une mémoire non volatile qui est protégée par des fonctions particulières ou d'autres composants du module de plate-forme sécurisé et n'est accessible que par celle-ci. Les informations sont stockées dans une structure de données ou un objet désigné sous le nom d'objet protégé par le module et peuvent prendre diverses formes, telles qu'une
25 clé cryptographique. L'accès aux informations peut prendre différentes formes, telles que la lecture des informations, leur écriture ou leur modification, etc. La mémoire non volatile comprend un ou plusieurs compteurs monotones et un ou plusieurs objets protégés (voir figure 1 du document).

Le document « Key Management with Trusted Platform Modules » de Andreas Nilsson, publié chez KTH CSC se
30 rapporte à un concept qui vise à rendre les plates-formes informatiques plus fiables. Il repose sur une puce appelée Trusted Platform Module (TPM). Le TPM est une puce qui fournit des fonctionnalités cryptographiques telles que le cryptage RSA et le stockage sécurisé des clés. Chaque module TPM dispose d'une paire de clés unique appelée clé de validation, créée en interne par le TPM, après fabrication mais avant expédition aux clients. La paire de clés identifie de manière unique le TPM et ne peut jamais être changé. La partie privée ne quitte jamais le TPM et la
35 partie publique est utilisée dans un certificat d'authentification. Il est prévu une mémoire non volatile et une mémoire volatile. La mémoire non volatile est utilisée pour stocker des données d'identité et d'état persistantes et les clés internes. Avec l'autorisation du propriétaire, il est possible d'écrire et de lire des données persistantes et opaques (auxquelles le TPM n'a pas accès ou qu'il ne peut utiliser) vers et depuis le TPM. La mémoire volatile est principalement utilisée en interne par le TPM.

40 Le document « Virtual Monotonic Counters and Count-Limited Objects using a TPM without a trusted OS » de Luis F.G. Sarmenta et al expose un développement des compteurs monotones virtuels avec des machines non de confiance avec un module de plateforme sécurisée TPM.

45 Le problème à la base de l'invention est, s'agissant d'un processeur de sécurité comprenant une mémoire morte une mémoire vive, un calculateur apte à réaliser des fonctions cryptographiques, et une unité de gestion de compteur monotone associée à au moins un compteur monotone, d'assurer la sécurisation de son utilisation, à

savoir le maintien et le contrôle de l'intégrité des programmes qu'il exécute et des contextes qui y sont relatifs, ainsi que de l'authentification des administrateurs enrôlés donnant ordre d'exécuter les dits programmes.

- 5 L'invention apporte une solution à ce problème, notamment en prévoyant que le processeur ne comprend aucune autre mémoire de stockage, de sorte qu'il ne stocke aucun programme ou données extérieures. Ainsi, le stockage est « externalisé » par rapport au processeur, le système d'exécution étant séparé et isolé des données à exécuter, de manière à conserver une parfaite intégrité.

- 10 Ci-après, un exposé de l'invention.

Selon un premier aspect, l'invention a pour objet un processeur de sécurité comprenant au moins une mémoire morte, une mémoire vive, un calculateur apte à réaliser des fonctions cryptographiques et une unité de gestion de compteur monotone associée à au moins un compteur monotone. Ce processeur de sécurité est tel que :

- 15 - il ne comprend aucune autre mémoire de stockage, de sorte qu'il ne stocke aucun programme, contexte - instructions, code, données - ou données extérieures,
- une clé publique permettant d'authentifier au moins un administrateur enrôlé initial est stockée avant sa première utilisation dans la mémoire morte,
- la mémoire vive est apte à charger un ensemble de données, tel qu'un contexte, et d'instructions pouvant être
20 authentifié par un module cryptographique à clé publique,
- l'exécution par le calculateur, après leur authentification par l'administrateur enrôlé initial, de certaines instructions incrémente l'un des compteurs monotones.

- 25 Un tel processeur de sécurité permet, dans le cadre d'un ensemble de traitement sécurisé de données comprenant un tel processeur de sécurité et une mémoire extérieure, d'exécuter automatiquement une séquence d'opérations de manière sécurisée.

Dans une réalisation, le processeur de sécurité est émulé comme une machine virtuelle.

- 30 Selon un deuxième aspect, l'invention a pour objet un ensemble de traitement sécurisé de données comprenant un processeur de sécurité tel qu'il vient d'être décrit et, en outre, au moins une mémoire extérieure à ce processeur de sécurité et au moins un moyen de connexion apte à relier cette au moins une mémoire extérieure au processeur de sécurité, tel que notamment par l'intermédiaire un réseau de communication électronique.

- 35 Selon une caractéristique et une réalisation, pour des raisons de sécurité, l'ensemble de traitement sécurisé de données comprend une pluralité soit au moins deux mémoires extérieures reliées au processeur de sécurité.

Selon une caractéristique, la au moins une mémoire extérieure de l'ensemble de traitement sécurisé de données est authentifiée vis-à-vis du processeur de sécurité.

- 40 Selon une réalisation, la mémoire extérieure de l'ensemble de traitement sécurisé de données est configurée pour être apte et spécialement destinée à :

- stocker au moins un programme et au moins un contexte - instructions, code, données -, destiné à être chargé dans la mémoire vive du processeur de sécurité,
45 - et à pouvoir recevoir et stocker tout fichier authentifié résultant de l'exécution par le processeur de sécurité du au moins un programme et du au moins un contexte qui a été chargé temporairement dans la mémoire vive du processeur de sécurité,

alors que l'au moins un contexte peut comprendre une valeur de référence apte à permettre au processeur de sécurité de vérifier la synchronisation du au moins un contexte avec le dernier état d'un compteur monotone.

- 5 Selon un troisième aspect, l'invention a pour objet une infrastructure de traitement sécurisé de données qui comprend une pluralité soit au moins deux processeurs de sécurité tels que ceux précédemment décrits et au moins une mémoire extérieure telle que celle précédemment décrite en relation avec l'ensemble de traitement sécurisé de données, l'infrastructure étant telle que chaque processeur de sécurité de la pluralité de processeurs de sécurité est relié à au moins une mémoire extérieure.

10

Selon une réalisation, l'infrastructure de traitement sécurisé de données comprend une pluralité soit au moins deux mémoires extérieures, chaque processeur de sécurité de la pluralité de processeurs de sécurité étant relié à au moins une mémoire extérieure de la pluralité de mémoires extérieures.

- 15 Selon une réalisation possible, l'infrastructure de traitement sécurisé de données comprend une pluralité soit au moins deux mémoires extérieures synchronisées entre elles, chacun des processeurs de sécurité de la pluralité de processeurs de sécurité pouvant utiliser de façon indifférenciée l'une ou l'autre des mémoires extérieures de la pluralité de mémoires extérieures.

- 20 Selon une réalisation possible, l'infrastructure de traitement sécurisé de données comprend plusieurs paires, trios, quatuors ou plus de mémoires extérieures, chacun des processeurs de sécurité étant associé à une paire, un trio, un quatuor ou plus de mémoires extérieures synchronisées entre elles.

- Ainsi, le processeur de sécurité en tant que tel ne comprend autre mémoire de stockage. Une ou plusieurs telles
25 mémoires de stockage sont extérieures au processeur de sécurité pour former un ensemble de traitement sécurisé de données ou une infrastructure de traitement sécurisé de données.

Selon un quatrième aspect, l'invention a pour objet un procédé d'exécution sécurisée d'une séquence d'opérations par un ensemble de traitement sécurisé de données qui comprend au moins l'exécution des étapes suivantes :

- 30 - A : un administrateur disposant d'une mémoire extérieure relié au processeur de sécurité active le processeur de sécurité,
- B : le processeur de sécurité une fois activé récupère une clé publique dans une mémoire extérieure afin de pouvoir l'authentifier par un module cryptographique à clé publique,
- C : si le processeur de sécurité authentifie l'administrateur qui l'a activé comme administrateur enrôlé ultérieur, il
35 charge un ensemble de données et d'instructions authentifié par cet administrateur enrôlé ultérieur et l'exécute,
- D : cette exécution par le processeur de sécurité produit un ensemble de données dont certaines peuvent être authentifiées, et cet ensemble de données une fois produit par le processeur de sécurité est stocké dans la mémoire extérieure utilisée par l'administrateur enrôlé ultérieur.

- 40 Selon une caractéristique et une réalisation, pour des raisons de sécurité, le procédé qui vient d'être décrit est exécuté avec deux administrateurs enrôlés ultérieurs, et plus généralement une pluralité d'au moins deux administrateurs enrôlés ultérieurs, chacun disposant d'une mémoire extérieure.

- Le procédé comprend également l'exécution d'étapes initiales dans lesquelles un administrateur enrôlé initial
45 dispose d'un ensemble de traitement sécurisé de données et enrôle un administrateur enrôlé ultérieur.

Le procédé comprend alors l'exécution des étapes d'enrôlement suivantes :

- A' : un premier ensemble de données et d'instructions authentifié et vérifié grâce à la clé publique stockée dans la mémoire morte est chargé dans la mémoire vive du processeur de sécurité afin de lui permettre d'exécuter un programme d'habilitation d'un administrateur enrôlé ultérieurs et à charger un autre ensemble de données et d'instructions et à le faire exécuter par le processeur de sécurité,
- B' : l'exécution par le processeur de sécurité du premier ensemble de données et d'instructions engendre un fichier chiffré et signé comprenant les éléments d'authentification de l'administrateur enrôlé ultérieur et qui est sauvegardé et stocké sur une mémoire extérieure au processeur de sécurité par l'administrateur enrôlé ultérieur,
- C' : l'exécution par le processeur de sécurité du premier ensemble de données et d'instructions entraîne en même temps l'incrémentation d'un compteur monotone.

Selon une caractéristique et une réalisation, pour des raisons de sécurité, les étapes d'enrôlement qui viennent d'être décrites sont telles qu'un administrateur enrôlé initial enrôle au moins deux administrateurs enrôlés ultérieurs, et plus généralement une pluralité d'au moins deux administrateurs enrôlés ultérieurs.

Selon une réalisation, les trois étapes A', B' et C,' précédemment décrites peuvent être répétées à plusieurs reprises de manière à permettre d'enrôler différents groupes d'administrateurs enrôlés ultérieurs, à charger et à faire s'exécuter différents ensembles de données et d'instructions, le tout en vue de pouvoir faire exécuter par le processeur de sécurité et transmettre à tout dispositif électronique ou réseau externe une séquence d'opérations.

Le procédé est également caractérisé en ce qu'il comprend l'exécution des étapes postérieures suivantes :

- les administrateurs enrôlés ultérieurs, enrôlés lors d'étapes d'enrôlement précédentes, s'authentifient auprès du processeur de sécurité au regard du contexte d'exécution en l'état, par un procédé fiable de contrôle d'accès, tel qu'une signature électronique, avant de pouvoir charger dans la mémoire vive du processeur de sécurité un ensemble de données et d'instructions,
- l'exécution par le processeur de sécurité de l'ensemble de données et d'instructions engendre un second fichier chiffré et signé comprenant des données liées à l'exécution du code et qui est sauvegardé et stocké uniquement par chacun de ces administrateurs enrôlés ultérieurs à l'extérieur du processeur de sécurité, dans la mémoire extérieure, et qui peut engendrer l'incrémentation d'un ou de plusieurs compteurs monotones.

Pour des raisons de sécurité, il peut être prévu que l'ensemble de données et d'instructions, une fois chargé dans la mémoire vive du processeur de sécurité, ne peut être exécuté qu'après que le processeur de sécurité a validé l'authentification de tous les administrateurs enrôlés ultérieurs par le précédent ensemble de données et d'instructions.

On décrit maintenant brièvement les figures des dessins.

La figure 1 représente de façon schématique les différents composants constitutifs d'un processeur de sécurité élémentaire selon l'invention. Cette figure illustre que le processeur de sécurité ne comprend qu'une mémoire morte, une mémoire vive, un calculateur, une unité de gestion de compteur monotone associée à un compteur monotone et qu'il ne comprend aucune autre mémoire de stockage, de sorte qu'il ne stocke aucun programme ou données extérieures.

La figure 2 représente de façon schématique les différents composants constitutifs d'un ensemble de traitement sécurisé de données élémentaire selon l'invention, comprenant un processeur de sécurité tel que celui de la figure 1, une mémoire extérieure au processeur de sécurité, et des moyens de connexion aptes à relier ce processeur de sécurité et cette mémoire extérieure à lui, comme par l'intermédiaire un réseau de communication électronique.

Les figures 3 et 4 représentent de façon schématique les différents composants constitutifs de deux infrastructures de traitement sécurisé de données selon l'invention. Dans le cas de la figure 3, l'infrastructure comprend deux processeurs de sécurité tels que ceux des figures 1 et 2 et trois mémoires extérieures telles que celle de la figure 2, synchronisées entre elles, chacun des processeurs de sécurité pouvant utiliser de façon indifférenciée l'une des trois mémoires extérieures. Dans le cas de la figure 4, l'infrastructure comprend deux processeurs de sécurité tels que ceux des figures 1 et 2 et deux paires de mémoires extérieures telles que celle de la figure 2, chacun des processeurs de sécurité étant associé à une paire de mémoires extérieures, synchronisées entre elles.

La figure 5 présente une vue générale des étapes d'exécution d'un ensemble de traitement sécurisé de données selon l'invention.

La figure 6 présente les différentes étapes d'enrôlement de deux administrateurs enrôlés ultérieurs.

Un processeur de sécurité PS selon l'invention comprend (figure 1) une mémoire morte ROM, une mémoire vive RAM, un calculateur UE apte à réaliser des fonctions cryptographiques, une unité de gestion UG de compteur monotone associée à au moins un compteur monotone CM.

Une clé publique CP permettant d'authentifier au moins un administrateur enrôlé initial AI est stockée avant sa première utilisation dans la mémoire morte ROM. La mémoire vive RAM est apte à charger un ensemble de données - tel qu'un contexte - et d'instructions, pouvant être authentifié par un module cryptographique MC à clé publique que comprend le processeur de sécurité PS.

L'exécution par le calculateur UE, après leur authentification, de certaines instructions peut incrémenter un compteur monotone CM.

Dans une réalisation, le processeur de sécurité PS est émulé comme une machine virtuelle.

Selon une caractéristique du processeur de sécurité PS, celui-ci ne comprend aucune autre mémoire de stockage, permanente de sorte que le processeur de sécurité PS ne stocke de façon permanente aucun programme, contexte - instructions, code, données - ou données extérieures.

Ainsi, le processeur de sécurité PS est constitué de la mémoire morte ROM, de la mémoire vive RAM, du calculateur UE, de l'unité de gestion UG, du au moins un compteur monotone CM et du module cryptographique MC.

Pour autant, il est prévu pour le traitement sécurisé de données, au moins une telle mémoire de stockage ME, mais celle-ci est extérieure au processeur de sécurité PS et non partie de lui et intégrée physiquement à lui.

C'est ainsi que l'on forme avec un tel processeur de sécurité PS et au moins une telle mémoire de stockage ME, ainsi que des moyens de communication appropriés, un ensemble ETS de traitement sécurisé de données ou une infrastructure ITS de traitement sécurisé de données (figures 2, 3 et 4).

Le processeur de sécurité PS peut, dans un tel ensemble ETS de traitement sécurisé de données ou dans une telle infrastructure ITS de traitement sécurisé de données, exécuter automatiquement une séquence d'opérations de manière sécurisée. On entend par là que l'on assure le maintien et le contrôle de l'intégrité du programme et du contexte y relatif, ainsi que de l'authentification des administrateurs enrôlés, au sens où cela a été précédemment défini.

Par mémoire de stockage « extérieure » au processeur de sécurité », il faut comprendre une mémoire qui n'est pas incluse dans l'unité physique que constitue le processeur PS. Pour cette raison, cette mémoire est dénommée « mémoire extérieure » et référencée ME.

La caractéristique que la mémoire ME est extérieure au processeur de sécurité PS a pour fonction d'externaliser le stockage par rapport au processeur PS, ou en d'autres termes, de séparer et d'isoler le système d'exécution (le processeur PS) des données.

- 5 La caractéristique que la mémoire ME est extérieure au processeur de sécurité PS a pour résultat, d'une part, de ne pas limiter la capacité de traitement de données du processeur PS, d'autre part, de garantir l'immuabilité, et donc l'intégrité, du traitement du processeur, car la mémoire extérieure, permanente, n'a pas d'effet ou d'influence sur le processeur de sécurité PS en tant que tel.

- 10 L'invention vise également tous autres moyens différents d'une mémoire de stockage extérieures ME comme il vient d'être décrit, mais qui remplissent la même fonction et procurent un résultat analogue que ce qui vient d'être exposé.

- 15 Un ensemble ETS de traitement sécurisé de données comprend (figure 2) un processeur de sécurité PS tel qu'il a été décrit et, en outre, une mémoire extérieure ME, au sens où cela a été précédemment défini. L'ensemble ETS comprend également au moins un moyen de connexion CO, apte à relier la mémoire extérieure ME au processeur de sécurité PS, tel que notamment par l'intermédiaire d'un réseau de communication électronique.

- L'ensemble ETS de traitement sécurisé de données peut ne comprendre qu'une seule mémoire extérieure ME. Mais, si l'on souhaite, pour des raisons de sécurité, qu'aucune décision applicative ne puisse être exécutée par une personne unique, on prévoit que l'ensemble ETS de traitement sécurisé de données comprenne au moins deux
20 mémoires extérieures ME pour au moins deux administrateurs enrôlés ultérieurs AU.

- La description qui suit est faite en relation avec une réalisation à deux mémoires extérieures ME. Toutefois, cette caractéristique du nombre de mémoires extérieures ME n'est pas limitative. En particulier, il peut être prévu plus de deux mémoires extérieures ME. C'est pourquoi l'on peut se référer à une pluralité soit au moins deux mémoires
25 extérieures ME (le nombre de mémoires extérieures ME pouvant être plus important) et à une pluralité soit au moins deux administrateurs enrôlés ultérieurs AU (le nombre d'administrateurs enrôlés ultérieurs AU pouvant être plus important).

- 30 Les moyens de connexion CO peuvent permettre dans le sens processeur de sécurité PS vers la mémoire extérieure ME, un stockage chiffré et dans le sens mémoire extérieure ME vers processeur de sécurité PS, une récupération chiffrée.

Le contenu de la ou des mémoires extérieures ME de l'ensemble ETS de traitement sécurisé de données est authentifié vis-à-vis du processeur de sécurité PS.

- 35 Une mémoire extérieure ME est configurée pour être apte et spécialement destinée à stocker au moins un programme et au moins un contexte - instructions, code, données -, destiné à être chargé dans la mémoire vive RAM du processeur de sécurité PS, et à pouvoir recevoir et stocker tout ensemble de données authentifié résultant de l'exécution par le processeur de sécurité PS d'un tel programme et d'un tel contexte qui a été chargé temporairement dans la mémoire vive RAM, comme il vient d'être exposé.

- 40 Un contexte (ensemble de paramètres et de conditions sous lesquels le programme peut être mis en œuvre) peut comprendre une valeur de référence apte à permettre au processeur de sécurité PS de vérifier la synchronisation du contexte avec le dernier état d'un compteur monotone CM.

- 45 Une infrastructure ITS de traitement sécurisé de données comprend (figures 3 et 4) une pluralité soit au moins deux processeurs de sécurité PS tels qu'il vient d'être décrit, par exemple PS1 et PS2, et, en outre, au moins une mémoire extérieure ME, telle qu'il vient d'être décrit.

Mais, comme pour l'ensemble ETS de traitement sécurisé de données, il peut être prévu que l'infrastructure ITS de traitement sécurisé de données comprenne une pluralité soit au moins deux (ou un plus grand nombre), de mémoires extérieures ME.

- 5 L'infrastructure ITS comprend également, comme l'ensemble ETS, au moins un moyen de connexion CO, apte à relier une mémoire extérieure ME à un processeur de sécurité PS.

- 10 La structure d'une telle infrastructure ITS de traitement sécurisé de données peut faire l'objet de nombre de réalisations, chacune de ces réalisations étant telle que chacun des processeurs de sécurité PS est relié à au moins une mémoire extérieure ME. Ainsi, selon les cas, un processeur de sécurité PS est relié à une seule mémoire extérieure ME ou au contraire à plusieurs mémoires extérieures ME et, une mémoire extérieure ME est reliée à un seul processeur de sécurité PS ou au contraire à plusieurs processeurs de sécurité PS.

- 15 Ainsi, une infrastructure ITS de traitement sécurisé de données peut être vue comme la structuration de plusieurs ensembles ETS de traitement sécurisé de données, combinés entre eux, le cas échéant ayant en commun un ou plusieurs processeurs de sécurité PS et/ou une ou plusieurs mémoires extérieures ME.

- 20 Dans une réalisation possible (figure 3), l'infrastructure ITS de traitement sécurisé de données comprend plusieurs processeurs de sécurité PS1, PS2 et plusieurs mémoires extérieures ME1, ME2, ME3, synchronisées entre elles, de sorte que chacun des processeurs de sécurité PS1, PS2, peut utiliser de façon indifférenciée l'une ou l'autre des mémoires extérieures ME1, ME2, ME3.

Une telle structure a pour avantage de présenter une résistance aux fautes élevées.

- 25 Dans une autre réalisation possible (figure 4), l'infrastructure ITS de traitement sécurisé de données comprend plusieurs processeurs de sécurité PS1, PS2 et plusieurs paires, par exemple ME1a et ME1b, d'une part, ME2a et ME2b, d'autre part, ou bien plusieurs trios, quatuors ou plus de mémoires extérieures ME, de sorte que chacun des processeurs de sécurité PS1, PS2, est associé à une paire, un trio, un quatuor... de mémoires extérieures ME, synchronisées entre elles.

- 30 Une telle structure a pour avantage d'améliorer les performances du système en créant des groupes de données, par un partitionnement.

On décrit maintenant des procédés de mise en œuvre d'un ensemble ETS de traitement sécurisé de données tel qu'il vient d'être décrit, lesquels procédés comprennent l'exécution d'étapes successives.

- 35 Dans le cadre des procédés selon l'invention, l'on est amené à se référer à un ou à des administrateurs enrôlés AI, AU, qui mettent en œuvre ces procédés. Ces administrateurs sont l'administrateur enrôlé initial AI et tout autre administrateur enrôlé ultérieur AU.

- 40 Comme il a été exposé précédemment, si l'on souhaite, pour des raisons de sécurité, qu'aucune décision applicative ne puisse être exécutée par une personne unique, on prévoit au moins deux administrateurs enrôlés ultérieurs AU.

- La description des procédés qui suit est faite en relation avec une réalisation à deux administrateurs enrôlés ultérieurs AU, respectivement AU1 et AU2. Toutefois, cette caractéristique du nombre administrateurs enrôlés ultérieurs AU n'est pas limitative. En particulier, il peut être prévu plus de deux administrateurs enrôlés ultérieurs AU.

45

On se réfère maintenant à la figure 5 pour exposer de façon générale l'exécution d'un ensemble ETS de traitement sécurisé de données dans le cas de deux administrateurs enrôlés ultérieurs AU1 et AU2.

Dans une étape A, les deux administrateurs enrôlés ultérieurs AU1 et AU2, disposant chacun d'une mémoire extérieure ME reliée au processeur de sécurité PS, activent le dit processeur de sécurité PS. Cette étape A comprend donc les opérations suivantes :

- A1 : récupération du contexte de l'administrateur enrôlé AU1,
- A2 : récupération du contexte de l'administrateur enrôlé AU2
- A3 : activation par l'administrateur enrôlé AU1 du processeur de sécurité PS,
- A4 : activation par l'administrateur enrôlé AU2 du processeur de sécurité PS.

10

Dans une étape B, le processeur de sécurité PS une fois activé récupère une clé publique CP dans une mémoire afin de pouvoir les authentifier par le module cryptographique MC mettant en œuvre un algorithme à clé publique.

Dans une étape C, si le processeur de sécurité PS authentifie les administrateurs enrôlés AU1 et AU2, il charge un ensemble de données et d'instructions authentifié par ces administrateurs enrôlés AU1 et AU2 (opérations C1 et C2 pour les administrateurs enrôlés AU1 et AU2) et l'exécute (opération C3).

Dans une étape D, cette exécution (opération C3) par le processeur de sécurité PS produit un ensemble de données dont certaines peuvent être authentifiées. Cet ensemble de données une fois produit par le processeur de sécurité PS est stocké dans la ou les mémoires extérieures ME utilisés par le ou les administrateurs enrôlés AU1, AU2. Cette étape D comprend donc les opérations suivantes :

- D1 : récupération de données liées à l'administrateur enrôlé AU1,
- D2 : récupération de données liées à l'administrateur enrôlé AU2,
- D3 : stockage de données liées à l'administrateur enrôlé AU1 dans la mémoire extérieure ME,
- D4 : stockage de données liées à l'administrateur enrôlé AU2 dans la mémoire extérieure ME.

Le procédé comprend également les étapes initiales suivantes d'enrôlement, dans lesquelles un administrateur enrôlé initial AI dispose d'un ensemble ETS de traitement sécurisé de données et enrôle au moins un administrateur enrôlé ultérieur AU. Comme il a été exposé précédemment, si l'on souhaite pour des raisons de sécurité qu'aucune décision applicative ne puisse être exécutée par une personne unique, un administrateur enrôlé initial AI enrôle deux ou au moins deux administrateurs enrôlés ultérieurs AU, respectivement AU1 et AU2 pour deux administrateurs enrôlés ultérieurs. La description du procédé d'enrôlement est faite en relation avec une réalisation à deux administrateurs enrôlés ultérieurs AU1 et AU2. Toutefois, comme il a été indiqué, cette caractéristique du nombre d'administrateurs enrôlés ultérieur n'est pas limitative. Aussi, plus généralement, un administrateur enrôlé initial AI peut enrôler une pluralité d'au moins deux administrateurs enrôlés ultérieurs (AU).

L'enrôlement de ces deux administrateurs enrôlés ultérieurs AU, respectivement AU1 et AU2, constitue un premier ensemble participant à la définition d'un premier contexte d'authentification utilisé pour les exécutions ultérieures.

L'administrateur enrôlé initial AI peut, ultérieurement, changer tel ou tel administrateur enrôlé ultérieur AU qui avait été précédemment enrôlé. Il peut ajouter un ou plusieurs administrateurs enrôlés ultérieurs AU. Il peut supprimer un ou plusieurs administrateurs enrôlés ultérieurs AU. Il peut modifier les droits d'un ou plusieurs administrateurs enrôlés ultérieurs AU. En cas de changement ultérieur de tel ou tel administrateur enrôlé ultérieur AU qui avait été précédemment enrôlé, l'administrateur enrôlé initial AI met en œuvre le procédé correspondant d'adaptation. On récupère alors le contexte mis à jour et le ou les compteurs monotones incrémentés.

On se réfère maintenant à la figure 6 pour exposer les différentes étapes d'enrôlement de deux administrateurs enrôlés ultérieurs AU1 et AU2. Ces étapes d'enrôlement sont, s'agissant des deux premiers administrateurs enrôlés désignés AU1 et AU2, des étapes initiales qui précèdent les étapes d'exécution décrites et représentées sur la figure 5. En cas de changement ultérieur de tel ou tel des premiers administrateurs enrôlés AU1 et AU2, ou en cas de changement de tel ou tel administrateur ultérieur AU précédemment enrôlé, les étapes d'enrôlement interviennent lors du changement d'administrateur, alors que l'ensemble ETS de traitement sécurisé de données a pu exécuter des instructions précédemment, avec d'autres administrateurs, dans le cadre d'un contexte précédent.

10 Dans une étape A', un premier ensemble de données et d'instructions, authentifié et vérifié grâce à la clé publique CP stockée dans la mémoire morte ROM, est chargé dans la mémoire vive RAM du processeur de sécurité PS, afin de lui permettre d'exécuter un programme d'habilitation des deux administrateurs enrôlés ultérieurs AU1 et AU2, à charger d'autres ensembles de données et d'instructions et à les faire exécuter par le processeur de sécurité PS.

15 Cette étape A' comprend donc les opérations suivantes :

- A'1 : récupération du programme d'habilitation par l'administrateur initial AI, depuis la mémoire extérieure ME,
- A'2 : récupération des éléments d'authentification de l'administrateur ultérieur AU1,
- A'3 : de manière analogue, récupération des éléments d'authentification de de l'administrateur ultérieur AU2,
- A'4 : transmission du programme d'habilitation et des éléments d'authentification au processeur de sécurité PS.

20

Dans une étape B', l'exécution par le processeur de sécurité PS du premier ensemble de données et d'instructions, engendre un fichier chiffré et signé comprenant les éléments d'authentification des administrateurs enrôlés ultérieurs AU1 et AU2, qui est sauvegardé et stocké sur une mémoire extérieure ME au processeur de sécurité PS par chacun des dits administrateurs enrôlés ultérieurs AU1, AU2.

25 Cette étape B' comprend donc les opérations suivantes :

- B'1 : exécution par le processeur de sécurité de sécurité PS du premier ensemble de données et d'instructions, en même temps que l'étape C dont il sera question par la suite,
- B'2 : transmission des données chiffrées et signées liées à l'administrateur ultérieur AU1,
- B'3 : stockage par l'administrateur ultérieur AU1 de ces données dans la mémoire extérieure ME,
- B'4 : de manière analogue, transmission des données chiffrées et signées liées à l'administrateur ultérieur AU2,
- B'5 : et, de manière analogue, stockage par l'administrateur ultérieur AU2 de ces données dans la mémoire extérieure ME.

30

35 Dans une étape C', l'exécution par le processeur de sécurité PS du premier ensemble de données et d'instructions (opération B'1) entraîne, en même temps, l'incrémentement d'un compteur monotone CM.

40 Les trois étapes A', B' et C', précédemment décrites peuvent être répétées à plusieurs reprises de manière à permettre d'habiller différents groupes d'administrateurs enrôlés ultérieurs AU, à charger et à faire s'exécuter différents ensembles de données et d'instructions, le tout en vue de pouvoir faire exécuter par le processeur de sécurité PS et transmettre à tout dispositif électronique ou réseau externe une séquence d'opérations.

Une fois les deux administrateurs ultérieurs AU1 et AU2 enrôlés, ceux-ci peuvent procéder à l'exécution des étapes postérieures suivantes, comme il a été précédemment décrit en référence à la figure 5.

45 Les administrateurs enrôlés ultérieurs AU1 et AU2, enrôlés lors des étapes précédentes d'enrôlement, s'authentifient auprès du processeur de sécurité PS au regard du contexte d'exécution en l'état, par un procédé

fiable de contrôle d'accès, tel qu'une signature électronique, avant de pouvoir charger dans la mémoire vive RAM du processeur de sécurité PS, un ensemble de données et d'instructions.

- 5 Cet ensemble de données et d'instructions, une fois chargé dans la mémoire vive RAM du processeur de sécurité PS, ne peut être exécuté qu'après que le processeur de sécurité PS a validé l'authentification des deux administrateurs enrôlés ultérieurs AU1 et AU2 par le précédent ensemble de données et d'instructions. Cette étape n'est pas obligatoire, mais seulement optionnelle. Elle vise à assurer une double sécurité. Si l'on souhaite doubler la sécurité, on réalise cette étape.

10

L'exécution par le processeur de sécurité PS de l'ensemble de données et d'instructions engendre un second fichier chiffré et signé comprenant des données liées à l'exécution du code et qui est sauvegardé et stocké uniquement par chacun de ces administrateurs enrôlés ultérieurs AU1 et AU2, à l'extérieur du processeur de sécurité PS, dans la mémoire extérieure ME, et qui peut engendrer l'incrémentation d'un ou de plusieurs compteurs monotones CM.

15