

Revendications

- 5 1. Processeur de sécurité (PS) comprenant au moins
- 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),
- 10 caractérisé en ce que :
- le processeur de sécurité (PS) ne comprend aucune autre mémoire de stockage, de sorte que le processeur de sécurité (PS) ne stocke aucun programme, contexte – instructions, code, données - ou données extérieures,
 - 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),
- 15 - 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,
- l'exécution par le calculateur (UE), après leur authentification par l'administrateur enrôlé initial (AI), de certaines instructions incrémente l'un des compteurs monotones (CM),
- de sorte à pouvoir exécuter automatiquement une séquence d'opérations de manière sécurisée dans le cadre d'un
- 20 ensemble de traitement sécurisé de données comprenant un tel processeur de sécurité.
2. Processeur de sécurité (PS) selon la revendication 1 caractérisé en ce qu'il est émulé comme une machine virtuelle.
- 25 3. Ensemble (ETS) de traitement sécurisé de données, comprenant un processeur de sécurité (PS) selon l'une des revendications 1 et 2, caractérisé en ce qu'il comprend en outre au moins une mémoire (ME) extérieure à ce processeur de sécurité (PS) et au moins un moyen de connexion (CO) apte à relier cette au moins une mémoire extérieure (ME) au processeur de sécurité (PS), tel que notamment par l'intermédiaire un réseau de communication électronique.
- 30 4. Ensemble (ETS) de traitement sécurisé de données selon la revendication 3, caractérisé en ce qu'il comprend une pluralité soit au moins deux mémoires extérieures (ME) reliées au processeur de sécurité (PS).
5. Ensemble (ETS) de traitement sécurisé de données selon l'une des revendications 3 et 4, caractérisé en ce
- 35 que la au moins une mémoire extérieure (ME) qu'il comprend est authentifiée vis-à-vis du processeur de sécurité (PS).
6. Ensemble (ETS) de traitement sécurisé de données selon l'une des revendications 4 à 5, caractérisé en ce que la mémoire extérieure (ME) est configurée pour être apte et spécialement destinée à :
- 40 - 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 fichier authentifié résultant de l'exécution par le processeur de sécurité (PS) du au moins un programme et du au moins un contexte chargé temporairement dans la mémoire vive (RAM) du processeur de sécurité (PS),
- 45 et en ce que l'au moins un contexte peut comprendre une valeur de référence apte à permettre au processeur de sécurité (PS) de vérifier la synchronisation du au moins un contexte avec le dernier état d'un compteur monotone (CM).

7. Infrastructure (ITS) de traitement sécurisé de données, caractérisée en ce qu'elle comprend une pluralité soit au moins deux processeurs de sécurité (PS) selon l'une des revendications 1 et 2, et au moins une mémoire extérieure (ME), et en ce que chaque processeur de sécurité (PS) de la pluralité de processeurs de sécurité (PS) est relié à au moins une mémoire extérieure (ME).
8. Infrastructure (ITS) de traitement sécurisé de données selon la revendication 7, caractérisée en ce qu'elle comprend une pluralité soit au moins deux mémoires extérieures (ME), chaque processeur de sécurité (PS) de la pluralité de processeurs de sécurité (PS) étant relié à au moins une mémoire extérieure (ME) de la pluralité de mémoires extérieures (ME).
9. Infrastructure ITS de traitement sécurisé de données selon l'une des revendications 7 et 8, qui comprend une pluralité soit au moins deux mémoires extérieures (ME) synchronisées entre elles, chacun des processeurs de sécurité (PS) de la pluralité de processeurs de sécurité (PS) pouvant utiliser de façon indifférenciée l'une ou l'autre des mémoires extérieures (ME) de la pluralité de mémoires extérieures (ME).
10. Infrastructure ITS de traitement sécurisé de données selon l'une des revendications 7 et 8, qui comprend plusieurs paires, trios, quatuors ou plus de mémoires extérieures (ME), chacun des processeurs de sécurité (PS) étant associé à une paire, un trio, un quatuor ou plus de mémoires extérieures (ME), synchronisées entre elles.
11. Procédé d'exécution sécurisée d'une séquence d'opérations par un ensemble (ETS) de traitement sécurisé de données selon l'une des revendications 3 à 6, caractérisé en ce qu'il comprend au moins l'exécution des étapes suivantes :
- A : un administrateur disposant d'une mémoire extérieure (ME) relié au processeur de sécurité (PS) active le processeur de sécurité (PS),
 - B : le processeur de sécurité (PS) une fois activé récupère une clé publique (CP) dans une mémoire extérieure (ME) afin de pouvoir l'authentifier par un module cryptographique (MC) à clé publique,
 - C : si le processeur de sécurité (PS) authentifie l'administrateur qui l'a activé comme administrateur enrôlé ultérieur (AU), il charge un ensemble de données et d'instructions authentifié par cet administrateur enrôlé ultérieur (AU) et l'exécute,
 - D : cette exécution par le processeur de sécurité (PS) produit un ensemble de données dont certaines peuvent être authentifiées, et le dit ensemble de données une fois produit par le processeur de sécurité (PS) est stocké dans la mémoire extérieure (ME) utilisée par l'administrateur enrôlé ultérieur (AU).
12. Procédé d'exécution sécurisée d'une séquence d'opérations, selon la revendication 11, avec deux administrateurs enrôlés ultérieurs (AU), et plus généralement une pluralité d'au moins deux administrateurs enrôlés ultérieurs (AU), chacun disposant d'une mémoire extérieure (ME).
13. Procédé d'exécution sécurisée d'une séquence d'opérations, selon l'une des revendications 11 et 12, caractérisé en ce qu'il comprend également l'exécution des étapes initiales dans lesquelles un administrateur enrôlé initial (AI) dispose d'un ensemble (ETS) de traitement sécurisé de données selon l'une des revendications 3 à 6 et enrôle un administrateur enrôlé ultérieur (AU).
14. Procédé d'exécution sécurisée d'une séquence d'opérations, selon la revendication 13, caractérisé en ce qu'il comprend l'exécution des étapes d'enrôlement suivantes :

- 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 du processeur de sécurité (PS) afin de lui permettre d'exécuter un programme d'habilitation d'un administrateur enrôlé ultérieurs (AU) et à charger un autre ensemble de données et d'instructions et à le faire exécuter par le processeur de sécurité (PS),
- 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 de l'administrateur enrôlé ultérieur (AU) et qui est sauvegardé et stocké sur une mémoire extérieure (ME) au processeur de sécurité (PS) par l'administrateur enrôlé ultérieur (AU),
- C' : l'exécution par le processeur de sécurité (PS) du premier ensemble de données et d'instructions entraîne en même temps l'incrémementation d'un compteur monotone (CM).

15. Procédé d'exécution sécurisée d'une séquence d'opérations, selon l'une des revendications 13 et 14, caractérisé par l'exécution d'étapes initiales dans lesquelles un administrateur enrôlé initial (AI) enrôle au moins deux administrateurs enrôlés ultérieurs (AU), et plus généralement une pluralité d'au moins deux administrateurs enrôlés ultérieurs (AU).

16. Procédé d'exécution sécurisée d'une séquence d'opérations, selon l'une des revendications 14 et 15, caractérisé en ce que les trois étapes A', B' et C' peuvent être répétées à plusieurs reprises de manière à permettre d'enrôler 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.

17. Procédé d'exécution sécurisée d'une séquence d'opérations, selon l'une des revendications 11 à 16, caractérisé en ce qu'il comprend l'exécution des étapes postérieures suivantes :

- les administrateurs enrôlés ultérieurs (AU), enrôlés lors d'étapes d'enrôlement précédentes, 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,
- l'exécution par le processeur de sécurité (PS) de l'ensemble de données et d'instructions engendre un nouveau 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 (AU) à l'extérieur du processeur de sécurité (PS), dans la mémoire extérieure (ME), et qui peut engendrer l'incrémementation d'un ou de plusieurs compteurs monotones (CM).

18. Procédé d'exécution sécurisée d'une séquence d'opérations, selon l'a revendication 17, caractérisé en ce que l'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 de tous les administrateurs enrôlés ultérieurs (AU) par le précédent ensemble de données et d'instructions.