

Revendications

1. Procédé de contrôle d'intégrité d'un dispositif électronique (DE), notamment un système de
445 paiement par carte, comportant au moins :

- un processeur (MPU),
- un élément sécurisé (SE) apte à stocker et gérer des données et dans lequel a été chargé une clé publique (KP) destinée à vérifier une signature électronique, et
- un moyen de stockage de données (MEM), dont le contenu a été préalablement
450 authentifié et dont l'intégrité peut être vérifiée par la clé publique,

tel qu'une commande de contrôle d'intégrité entraîne l'exécution des étapes suivantes :

- l'élément sécurisé (SE) exécute, par l'intermédiaire du processeur (MPU), sur le contenu reçu de la mémoire du moyen de stockage de données (MEM) une vérification d'authenticité, afin de vérifier grâce à la clé publique (KP) que son contenu n'a pu être
455 modifié depuis son authentification initiale,

- lorsque la vérification d'authenticité a réussi, le dispositif est considéré comme intègre.
caractérisé en ce qu'une commande de contrôle d'intégrité entraîne l'exécution des étapes successives suivantes :

- le processeur (MPU) du dispositif sollicite l'élément sécurisé (SE),
- 460 - en réponse, l'élément sécurisé (SE) adresse, par l'intermédiaire du processeur (MPU), au moyen de stockage de données (MEM) une requête en vue de se faire adresser le contenu intégral de sa mémoire,
- l'élément sécurisé (SE) exécute ensuite ladite vérification d'authenticité.

465 2. Procédé de contrôle d'intégrité d'un dispositif électronique (DE) selon la revendication 1, dans lequel lorsque le dispositif est considéré comme intègre, ce dispositif est apte à fonctionner selon le comportement nominal qui lui a été attribué,

3. Procédé de contrôle d'intégrité d'un dispositif électronique (DE) selon l'une des
470 revendications 1 et 2, dans lequel lorsque la vérification d'authenticité ne réussit pas, le dispositif est programmé pour fonctionner selon un mode adapté tenant compte de l'échec de la vérification.

4. Procédé de contrôle d'intégrité selon l'une des revendications 1 à 3, qui comporte, outre les
475 étapes exécutées à chaque fois qu'une commande de contrôle d'intégrité est adressée au dispositif, une phase préalable de paramétrage du dispositif électronique (DE), dans lequel le

contenu initial de la mémoire du moyen de stockage de données (MEM) est validé grâce à un moyen d'authentification numérique tel que notamment un système de signature électronique utilisant la clé privée correspondante à la clé publique (KP) chargée dans l'élément sécurisé (SE).

5. Procédé de contrôle d'intégrité d'un dispositif électronique (DE) selon la revendication 4, dans lequel la signature électronique réalisée initialement lors de la phase préalable de paramétrage du dispositif électronique (DE) est chargée soit dans le moyen de stockage de données (MEM), soit dans la mémoire de l'élément sécurisé (SE).

6. Procédé de contrôle d'intégrité d'un dispositif électronique (DE) selon l'une des revendications 1 à 5, dans lequel une commande de contrôle d'intégrité est effectuée soit lors d'un démarrage du dispositif, soit lors d'une sollicitation de son utilisateur requérant le contrôle de son intégrité.

7. Procédé de contrôle d'intégrité selon l'une des revendications 1 à 6, dans lequel après au moins un ou un nombre déterminé d'exécution des étapes de contrôle d'intégrité n'ayant pas abouti à confirmer l'intégrité de la mémoire par rapport à son état initial, l'échec de la vérification d'authenticité du contenu de la mémoire entraîne l'une ou plusieurs des modalités de fonctionnement dégradé suivantes :

- notification de l'échec de vérification d'intégrité à l'utilisateur,
- blocage d'accès aux données chargées dans l'élément sécurisé (SE),
- blocage d'accès au dispositif électronique (DE),
- effacement de tout ou partie des données stockées dans le dispositif électronique (DE) et les éléments qui le composent.

8. Procédé de contrôle d'intégrité d'un dispositif électronique (DE) selon l'une des revendications 1 à 7, dans lequel l'élément sécurisé (SE) dispose en mémoire d'un intervalle de temps T de référence qui est choisi pour être inférieur au temps maximal nécessaire pour que cet élément sécurisé (SE) récupère la totalité du contenu de la mémoire à authentifier, et dans lequel, chaque commande de contrôle d'intégrité adressée au dispositif entraîne l'exécution des étapes successives suivantes :

- l'élément sécurisé (SE) adresse une requête au moyen de stockage de données (MEM) afin qu'elle lui adresse une ou plusieurs séquences de données extraites de sa mémoire,

- l'élément sécurisé (SE) identifie le délai qui s'écoule entre l'envoi de la requête et la réception du ou des séquences demandées et le compare à l'intervalle de temps T de référence,
- si le délai écoulé est supérieur à l'intervalle T, l'élément sécurisé (SE) refuse l'authentification du contenu de mémoire du moyen de stockage de données (MEM) et interrompt l'exécution des étapes suivantes du procédé de contrôle d'intégrité.

9. Procédé de contrôle d'intégrité d'un dispositif électronique (DE) selon la revendication 8, dans lequel lorsque le délai écoulé entre l'envoi de la requête par l'élément sécurisé (SE) et la réception du ou des séquences demandées est inférieur à l'intervalle T, l'élément sécurisé (SE) exécute les étapes du procédé de contrôle d'intégrité, tout en vérifiant l'intégrité des séquences reçues par rapport à l'authenticité du contenu de la mémoire qu'il doit valider.

10. Procédé de contrôle d'intégrité d'un dispositif électronique (DE) selon l'une des revendications 1 à 9, dans lequel la fonction du processeur (MPU) est assurée par un microcontrôleur.

11. Dispositif électronique (DE), notamment un terminal de paiement, comportant au moins :
- un processeur (MPU),
 - un élément sécurisé (SE) apte à stocker et gérer des données et dans lequel a été chargé une clé publique destinée à vérifier une signature électronique, et
 - un moyen de stockage de données (MEM), dont le contenu a été préalablement authentifié et dont l'intégrité peut être vérifiée par la clé publique,
- caractérisé en ce qu'il est apte et destiné à mettre en œuvre un procédé de contrôle d'intégrité selon l'une des revendications 1 à 9, en ce qu'une commande de contrôle d'intégrité entraîne l'exécution des étapes successives suivantes :
- le processeur (MPU) sollicite l'élément sécurisé (SE),
 - en réponse, l'élément sécurisé (SE) adresse, par l'intermédiaire du processeur (MPU), au moyen de stockage de données (MEM) une requête en vue de se faire adresser le contenu intégral de sa mémoire,
 - l'élément sécurisé (SE) exécute ensuite, par l'intermédiaire du processeur (MPU), sur le contenu reçu de la mémoire du moyen de stockage de données (MEM) une vérification d'authenticité, afin de vérifier grâce à la clé publique (KP) que son contenu n'a pu être modifié depuis son authentification initiale,
 - lorsque la vérification d'authenticité a réussi, le dispositif est considéré comme intègre.

12. Dispositif électronique (DE) selon la revendication 11, qui comporte un microcontrôleur dont la mémoire comporte tout ou partie du moyen de stockage de données (MEM) et dont le
550 processeur assure la fonction du processeur (MPU).

13. Dispositif électronique (DE) selon l'une des revendications 11 et 12, caractérisé en ce qu'il comporte également l'un ou/et l'autre des moyens complémentaires suivants :

- une interface homme-machine, notamment un clavier ou un écran,
- 555 - une interface de communication avec des dispositifs numériques externes, notamment un ordinateur, un réseau de communication ou un serveur distant.

14. Utilisation d'un dispositif électronique (DE) selon l'une des revendications 11 à 13, moyennant la mise en œuvre du procédé de contrôle d'intégrité de ce dispositif selon l'une des
560 revendications 1 à 10, pour la mise en œuvre de fonctions de sécurité, telles que notamment l'authentification, le chiffrement ou l'échange sécurisé à distance, de données stockées soit à l'intérieur même du dispositif soit à distance et accessibles à travers un réseau de communication.

565 15. Utilisation d'un dispositif électronique (DE) selon l'une des revendications 11 et 13, moyennant la mise en œuvre du procédé de contrôle d'intégrité de ce dispositif selon l'une des revendications 1 à 10, pour l'exécution de transactions, notamment financières.

570