

Contrôle d'intégrité d'un dispositif électronique

L'invention concerne le domaine du contrôle d'intégrité d'un dispositif électronique.

5

L'invention a plus précisément pour objet un procédé de contrôle d'intégrité d'un dispositif électronique, un tel dispositif électronique apte à mettre en œuvre ce procédé et des utilisations d'un tel dispositif électronique mettant en œuvre ce procédé. Par la suite, le dispositif électronique sera parfois dénommé par ellipse « dispositif ».

10

Un dispositif tel que celui de l'invention peut être un système de paiement par carte, cet exemple et cette application n'étant pas exclusifs d'autres. Par « système de paiement par carte », on entend la combinaison fonctionnelle d'un terminal de paiement et d'une carte à puce bancaire de paiement.

15

De façon connue, un dispositif du type de celui de l'invention comporte au moins :

- un processeur (communément dénommé MPU pour « micro-processor unit »),
- un élément sécurisé (qui peut être, en particulier, une carte à puce) 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 (tel qu'une mémoire).

20

Par ailleurs, il est également connu de pouvoir authentifier au préalable le contenu d'un moyen de stockage de manière que son intégrité puisse être vérifiée par une clé publique, correspondant à la clé privée ayant servi à cette authentification. Dans le contexte de la présente invention, cette clé publique peut être celle chargée dans la mémoire de l'élément sécurisé.

25

Dans le contexte de l'invention, on entend par « contrôle d'intégrité » la vérification que les données n'ont pas été modifiées ou détruites de façon non autorisée, conformément à la définition donnée par la norme Iso n° 7498-2.

30

De façon connue, dans une phase préalable à la mise à disposition de l'utilisateur, phase qui peut être au niveau de la fabrication du dispositif en question ou de son paramétrage par un fournisseur de produits ou de services, ses éléments constitutifs peuvent être authentifiés par une autorité de certification ad hoc, gouvernementale ou privée.

35

Dans une phase ultérieure déployée, il importe que le dispositif puisse être toujours mis en œuvre par l'utilisateur en toute confiance, c'est-à-dire avec la garantie de la conservation de son intégrité.

40 Tel est le but de l'invention.

On connaît la signature électronique qui permet de garantir l'intégrité d'un document électronique ou d'une information et d'en authentifier l'auteur. Toutefois, le mécanisme de la signature électronique ne permet pas à lui seul de garantir qu'un programme ayant fourni une
45 signature exécute de façon exacte ce qu'il prétend exécuter.

Dans les systèmes de paiement par carte bancaire, il est prévu une authentification par challenge-réponse carte bancaire / serveur d'authentification et terminal de paiement / serveur d'authentification ainsi qu'une validation que le terminal de paiement possède bien la clé privée
50 qu'il est sensé posséder pour la carte utilisée. Mais, l'utilisateur ne peut savoir, et donc n'a aucune certitude, quant à l'identité entre la transaction qu'il réalise au moyen du terminal de paiement et la transaction réellement réalisée par le terminal de paiement. Les certifications fournies par le groupement EMVCo® ou des organisations analogues n'empêchent pas l'utilisation d'un terminal de paiement contrefait ou cloné.

55

L'état de la technique est également illustré par les documents US 6 830 840 et US 5 721 781.

Le document US 6 839 840 décrit un procédé qui permet à une carte à mémoire et à un terminal de s'authentifier, dans lequel tous les calculs algorithmiques sont effectués par le terminal
60 auquel la carte à mémoire est connectée. Ces opérations relatives à l'authentification sont effectuées avant le début d'une transaction proprement dite et après la fin de cette transaction en vue de l'authentification au début de la transaction suivante.

Le document US 5 721 781 décrit un procédé pour authentifier une transaction entre un
65 dispositif d'information portable et un terminal, le dispositif d'information portable stockant un certificat lié à un dispositif unique au dispositif et le terminal mémorisant un certificat lié au terminal unique au terminal qui inclut des informations concernant un type de terminal. Le procédé comprenant les étapes suivantes: échanger les certificats liés au terminal et liés au terminal entre le dispositif d'informations portable et le terminal pendant une transaction;
70 authentifier le dispositif d'informations portable et le terminal l'un par l'autre en utilisant les certificats liés au dispositif et au terminal échangés; déterminer, sur le dispositif d'information

portable, un niveau de sécurité pour le terminal sur la base des informations de type terminal
contenues dans le certificat lié au terminal reçu du terminal, le niveau de sécurité ayant une
valeur limite associée pour une valeur de la transaction effectuée pendant la transaction; et
75 restreindre la valeur de la transaction à la limite de valeur associée au niveau de sécurité
déterminé.

Le document US 2002/023032 concerne un procédé pour permettre à une transaction financière
d'être effectuée à l'aide d'un système électronique, consistant à interroger un terminal de
80 transaction électronique avec un dispositif de sécurité électronique afin d'obtenir une métrique
d'intégrité pour le terminal de transaction financière ; à déterminer si le terminal de transaction
est un terminal de confiance sur la base de la métrique d'intégrité; à permettre aux données de
transaction financière d'être entrées dans le terminal de transaction si le terminal de transaction
est identifié en tant que terminal de confiance. Le document US 2002/023032 concerne
85 également un système de transaction financière comprenant un terminal financier électronique;
un dispositif de sécurité électronique ayant un moyen d'interrogation pour interroger le terminal
de transaction financière électronique afin d'obtenir une métrique d'intégrité pour le terminal de
transaction financière électronique, un moyen de détermination pour déterminer si le terminal
de transaction est un terminal de confiance sur la base de la métrique d'intégrité, un moyen pour
90 autoriser des données de transaction financière à entrer dans le terminal de transaction si le
terminal de transaction est identifié comme un terminal de confiance. Le procédé et le système
décrits dans le document US 2002/023032 ne prévient pas que la totalité de la mémoire du
terminal de transaction soit soumise au hachage par l'élément sécurisé. Or, ne soumettre au
hachage qu'un certificat et une somme de contrôle implique qu'ils peuvent avoir été falsifiés.
95 Le procédé et le système décrits dans le document US 2002/023032 ne permettent pas d'ajuster
le niveau de fonctionnalité de l'élément sécurisé en fonction de la métrique d'intégrité.

Le document US 9 177 152 concerne un procédé d'authentification et de déchiffrement d'un
fichier programme crypté destiné à être exécuté par un élément sécurisé, qui consiste à recevoir
100 le fichier programme et un certificat numérique associé au fichier programme à partir d'un
dispositif externe. Le procédé stocke le fichier de programme et le certificat associé dans une
mémoire vive sécurisée disposée dans l'élément sécurisé et hache le fichier de programme pour
obtenir un hachage. La méthode authentifie le fichier de programme en comparant le hachage
obtenu à une somme de contrôle stockée dans le certificat. De plus, le procédé écrit les
105 informations de configuration d'exécution stockées dans le certificat dans les registres de
configuration correspondants disposés dans l'élément sécurisé. ; le procédé génère en outre une

clé de chiffrement en utilisant une valeur de départ stockée dans le certificat et un identifiant unique disposé dans l'élément sécurisé et déchiffre le fichier de programme en utilisant la clé de chiffrement générée. Le procédé selon le document US 9 177 152 ne permet pas à l'élément
110 sécurisé de hacher un programme qui ne serait pas stockable dans sa mémoire vive sécurisée. De plus, ce document ne prévoit pas d'autoriser ou non l'exécution du programme par un autre microprocesseur.

Les procédés et systèmes décrits dans les documents US 2002/023032 et US 9 177 152 sont
115 tels que l'élément sécurisé se voit soumettre une somme de contrôle ou un contenu complet mais relativement petit dont il vérifie l'intégrité.

Tout au contraire, dans l'esprit de l'invention, il est souhaité que ce soit l'élément sécurisé qui décide des fonctionnalités qu'il pourra remplir en fonction du résultat du contrôle d'intégrité
120 du reste de la plateforme, ce qui implique de contrôler l'ensemble de la mémoire du reste des microprocesseurs.

Un tel souhait se heurte à deux obstacles. D'une part, le contrôle de l'intégrité d'une grande quantité d'information de manière sûre passe par le fait que le contenu doit être envoyé et haché
125 par l'élément sécurisé, ce qui constitue un goulot d'étranglement des performances de cette opération de contrôle d'intégrité. D'autre part, le fait que l'autre microprocesseur soit encore en fonctionnement lors de la transmission du contenu intégral de sa mémoire impose de s'assurer qu'il n'a pas modifié à la volée les données transmises afin de masquer une éventuelle modification par un tiers malveillant souhaitant compromettre le système.

130 Ces deux obstacles expliquent pourquoi les solutions existantes aujourd'hui ne procèdent pas dans ce sens mais procèdent plutôt à une vérification du contenu soit avant leur exécution, soit via une simple somme d'intégrité et un certificat associé.

135 Pourtant, les solutions à ces deux obstacles, comme présentées par l'invention, permettent d'ajouter des fonctionnalités avancées au système. Par exemple, le fait que suivant le niveau d'intégrité constaté, l'élément sécurisé ne soit pas réduit au choix binaire de délivrer ou de non délivrer le service, mais à un gradient de fonctionnalités.

140 Ainsi, il existe le problème général de permettre à un utilisateur de contrôler l'intégrité d'un dispositif de validation des transactions, à savoir l'intégrité d'un couple carte à puce / terminal

de paiement (tenant compte de l'hétérogénéité du parc de ceux-ci) et le problème particulier de surmonter les deux obstacles qui viennent d'être énoncés.

145 L'invention vise à apporter une solution à ces problèmes en tirant partie de l'élément sécurisé. Ainsi, dans la phase ultérieure déployée du dispositif, celui-ci peut toujours mis en œuvre par l'utilisateur en toute confiance.

A cette fin, on met en œuvre dans la phase ultérieure déployée, la paire de clés clé publique /
150 clé privée ayant été utilisées dans la phase préalable (de fabrication ou de paramétrage). Les deux phases sont donc interdépendantes.

Ci-après, un exposé de l'invention.

155 Selon un premier aspect, l'invention a pour objet un procédé de contrôle d'intégrité d'un dispositif électronique, notamment un système de paiement par carte, comportant au moins :

- un processeur,
- un élément sécurisé apte à stocker et gérer des données et dans lequel a été chargé une clé publique destinée à vérifier une signature électronique, et
- 160 - un moyen de stockage de données, dont le contenu a été préalablement 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 exécute, par l'intermédiaire du processeur, sur le contenu reçu de la mémoire du moyen de stockage de données une vérification d'authenticité, afin de
165 vérifier grâce à la clé publique 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.

Le procédé est tel qu'une commande de contrôle d'intégrité entraîne l'exécution des étapes
170 successives suivantes :

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

Selon une réalisation, lorsque le dispositif est considéré comme intègre, ce dispositif est apte à fonctionner selon le comportement nominal qui lui a été attribué,

180 Selon une réalisation, 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.

Selon une réalisation, le procédé comporte, outre les étapes exécutées à chaque fois qu'une commande de contrôle d'intégrité est adressée au dispositif, une phase préalable de paramétrage
185 du dispositif électronique, dans lequel le contenu initial de la mémoire du moyen de stockage de données 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 chargée dans l'élément sécurisé. En particulier, la signature électronique réalisée initialement lors de la phase préalable de fabrication ou de paramétrage du dispositif électronique est chargée
190 soit dans le moyen de stockage de données soit dans la mémoire de l'élément sécurisé.

Selon une réalisation, 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.

195

Selon une réalisation, 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 :

- 200
- notification de l'échec de vérification d'intégrité à l'utilisateur,
 - blocage d'accès aux données chargées dans l'élément sécurisé,
 - blocage d'accès au dispositif électronique,
 - effacement de tout ou partie des données stockées dans le dispositif électronique et les éléments qui le composent.

205

Selon une réalisation, l'élément sécurisé 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 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
210 successives suivantes :

- l'élément sécurisé adresse, par l'intermédiaire du processeur, une requête au moyen de stockage de données afin qu'elle lui adresse une ou plusieurs séquences de données extraites de sa mémoire,
- 215 - l'élément sécurisé identifie le délai qui s'écoule entre l'envoi de la requête et la réception, par l'intermédiaire du processeur, 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 refuse l'authentification du contenu de mémoire du moyen de stockage de données et interrompt l'exécution des étapes suivantes du procédé de contrôle d'intégrité.

220

Selon une réalisation, lorsque le délai écoulé entre l'envoi de la requête par l'élément sécurisé et la réception du ou des séquences demandées est inférieur à l'intervalle T, l'élément sécurisé exécute les étapes 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.

225

Selon une réalisation, la fonction du processeur est assurée par un microcontrôleur.

Selon un deuxième aspect, l'invention a pour objet un dispositif électronique, notamment un terminal de paiement, comportant au moins :

- 230 - un processeur,
- un élément sécurisé 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, dont le contenu a été préalablement authentifié et dont l'intégrité peut être vérifiée par la clé publique,

235 apte et destiné à mettre en œuvre un procédé de contrôle d'intégrité tel qu'il a été précédemment décrit, en ce qu'une commande de contrôle d'intégrité entraîne l'exécution des étapes successives suivantes :

- le processeur sollicite l'élément sécurisé,
- en réponse, l'élément sécurisé adresse, par l'intermédiaire du processeur, au moyen de 240 stockage de données une requête en vue de se faire adresser le contenu intégral de sa mémoire,
- l'élément sécurisé exécute ensuite, par l'intermédiaire du processeur, sur le contenu reçu de la mémoire du moyen de stockage de données une vérification d'authenticité, afin de vérifier grâce à la clé publique que son contenu n'a pu être modifié depuis son 245 authentification initiale,

- lorsque la vérification d'authenticité a réussi, le dispositif est considéré comme intègre.

Plus généralement, le dispositif met en œuvre les autres étapes et/ou caractéristiques du procédé précédemment décrites.

250

Selon une réalisation, le dispositif comporte un microcontrôleur dont la mémoire comporte tout ou partie du moyen de stockage de données et dont le processeur assure la fonction du processeur.

255 Selon les cas, le dispositif comporte également l'un ou/et l'autre des moyens complémentaires suivants :

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

260

Selon un troisième aspect, l'invention a pour objet des utilisations d'un tel dispositif électronique mettant en œuvre un tel procédé de contrôle d'intégrité.

Ces utilisations sont 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, ou encore l'exécution de transactions, notamment financières.

265

On décrit maintenant brièvement les figures des dessins.

270 La figure 1 est un schéma illustrant le dispositif électronique selon l'invention.

La figure 2 est un schéma illustrant la phase préalable de fabrication ou de paramétrage du dispositif en question.

La figure 3 est un diagramme de séquences illustrant les étapes de la phase déployée du procédé de contrôle d'intégrité du dispositif en question.

275

L'invention a pour objet un procédé de contrôle d'intégrité d'un dispositif électronique DE. Comme indiqué, le dispositif électronique DE sera parfois dénommé par ellipse « dispositif ». Elle a aussi pour objet un dispositif électronique DE apte et destiné à mettre en œuvre ce procédé de contrôle d'intégrité.

280 Elle a également pour objet des utilisations du dispositif électronique DE en ce qu'il met en œuvre le procédé de contrôle d'intégrité.

Le dispositif DE peut être un système de paiement par carte, c'est-à-dire la combinaison fonctionnelle d'un terminal de paiement et d'une carte à puce bancaire de paiement.

285

Toutefois, cet exemple et cette application ne sont pas exclusifs d'autres.

De façon connue, un dispositif DE comporte au moins :

- un processeur MPU,
- 290 - 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 authentifié et dont l'intégrité peut être vérifiée par la clé publique KP. Ce moyen de stockage de données MEM comprend tout ou partie de la mémoire interne d'un microcontrôleur.

295

Le dispositif DE peut comporter également une interface homme-machine, notamment un clavier ou un écran. Il peut comporter également une interface de communication avec des dispositifs numériques externes, notamment un ordinateur, un réseau de communication ou un serveur distant.

300

Le dispositif DE peut se présenter sous la forme d'un boîtier plat et peu épais, de quelques centimètres de côté ou bien sous la forme d'une clé USB.

Un tel dispositif DE peut, moyennant la mise en œuvre du procédé de contrôle d'intégrité, être
305 mis en œuvre pour des 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 DE soit à distance et accessibles à travers un réseau de communication. Le dispositif DE peut donc être mis en œuvre de façon autonome, ou moyennant une communication avec d'autres moyens électroniques. Une utilisation typique du dispositif DE est l'exécution de
310 transactions, notamment financières et y compris pour des cryptomonnaies, de façon sécurisée.

Dans le contexte de l'invention, on entend par « contrôle d'intégrité » la vérification que les données n'ont pas été modifiées ou détruites de façon non autorisée conformément à la définition donnée par la norme Iso n° 7498-2.

315

Dans une phase préalable de fabrication ou de paramétrage FAB du dispositif DE, ses éléments constitutifs sont authentifiés par une autorité ad hoc, gouvernementale ou privée. Le dispositif DE est ainsi paramétré pour la mise en œuvre du procédé, grâce à cette authentification initiale.

320 Dans une phase ultérieure déployée USE, il est mis en œuvre le procédé de contrôle d'intégrité de l'invention.

On décrit maintenant plusieurs modes possibles de réalisation de l'invention.

325 On décrit maintenant plus spécialement la phase préalable de fabrication ou de paramétrage FAB du dispositif DE, en référence à la figure 2. Cette phase intervient au moment même de la fabrication physique du dispositif DE, ou bien ultérieurement, mais avant la phase ultérieure déployée USE. Cette transition de la phase préalable de fabrication ou de paramétrage FAB vers la phase déployée USE est définitive. Dans cette phase préalable de paramétrage du
330 dispositif électronique, le contenu initial CO 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 Kd correspondant à la clé publique KP chargée dans l'élément sécurisé SE. Selon les cas, la signature électronique SIGN est chargée soit dans le moyen de stockage de données MEM (comme illustré par la figure 3), soit dans la mémoire
335 de l'élément sécurisé SE.

On décrit maintenant plus spécialement le procédé de contrôle d'intégrité du dispositif électronique DE dans la phase ultérieure déployée USE en référence à la figure 3. Ce procédé de contrôle d'intégrité est tel qu'une commande de contrôle d'intégrité A entraîne l'exécution
340 des étapes et opérations successives décrites ci-après (chaque étape est illustrée sur la figure 3 par une flèche comportant une référence qui identifie l'étape).

D'abord, le processeur MPU du dispositif sollicite l'élément sécurisé SE (flèche B).

345 En réponse, l'élément sécurisé SE adresse, par l'intermédiaire du processeur MPU (flèche C), au moyen de stockage de données MEM une requête (flèche D) en vue de se faire adresser le contenu intégral de sa mémoire flèche E.

L'invention présente les avantages de permettre un contrôle complet et sans compromission des
350 mémoires des divers microprocesseurs du système.

L'élément sécurisé doit déléguer au processeur MPU des opérations d'affichage et d'interaction
utilisateur, et pour cela, il a besoin du concours d'un code validé s'exécutant sur le processeur
MPU. Dès lors, le processeur MPU doit exécuter un code intègre afin d'éviter à l'utilisateur
355 une inadéquation entre les informations affichées et réellement manipulées par l'élément
sécurisé SE.

Grace au fait que l'entièreté de la mémoire du processeur MPU collaborant avec l'élément
sécurisé SE est contrôlée, l'effet de sécurité est total, le processeur MPU n'ayant pas de marge
360 de manœuvre pour opérer des procédures non intègres, et le niveau de fonctionnalité de
l'élément sécurisé SE est adapté.

L'élément sécurisé SE peut par exemple, décider d'un ensemble de niveau de sécurité suivant :

- complet : la mémoire du processeur MPU est reconnue intègre et les contremesures pour
365 détecter un processeur MPU falsifié n'ont pas de résultats positifs.
- partiel (fonction d'authentification uniquement) : la mémoire du processeur MPU est
reconnue intègre, mais certaines contremesures de détection d'un processeur MPU
falsifié ont des résultats positifs, l'élément sécurisé SE n'acceptera que des requêtes
d'authentification de contenu via les secrets de l'utilisateur, mais rejettera toute autre
370 demande.
- nul : la mémoire du processeur MPU n'est pas reconnue comme intègre. Dans ce cas,
l'élément sécurisé SE n'accèdera à aucune demande faisant appel aux secrets de
l'utilisateur, mais autorisera néanmoins la réalisation d'autres opérations
cryptographique (importation de secrets externes, manipulation de ceux-ci). Dans ce
375 cas, optionnellement, l'élément sécurisé SE peut décider d'effacer les secrets de
l'utilisateur pour plus de confidentialité.

De ces niveaux de sécurité, il apparaît que l'élément sécurisé SE n'est pas seulement asservi
par le système qui lui soumet des requêtes, mais peut décider, en fonction de celles-ci, des
380 réponses à ses propres requêtes au système et du niveau de fonctionnalités qu'il sera en mesure
de délivrer.

Ensuite l'élément sécurisé SE exécute sur le contenu reçu (flèche F) de la mémoire du moyen de stockage de données MEM une vérification d'authenticité (flèche G), afin de vérifier grâce
385 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 DE est considéré comme intègre.

Selon les cas, en fonction des capacités des éléments constitutifs du dispositif DE, les étapes et
390 opérations correspondant aux flèches C, D, E et F portent soit sur l'entier contenu de la mémoire du moyen de stockage de données MEM soit sur des parties de ce contenu, auquel cas ces étapes et opérations correspondant aux flèches C, D, E et F sont répétées jusqu'à ce que l'entier contenu ait été reçu par l'élément sécurisé SE, afin qu'il puisse alors exécuter la vérification d'intégrité (flèche G).

395

Selon les cas, une commande de contrôle d'intégrité A est effectuée soit lors d'un démarrage du dispositif DE, soit lors d'une sollicitation de son utilisateur requérant le contrôle de son intégrité.

400 Lorsque le dispositif DE est considéré comme intègre, il est apte à fonctionner selon le comportement nominal qui lui a été attribué.

Lorsque, en revanche, la vérification d'authenticité ne réussit pas, le dispositif DE est programmé pour fonctionner selon un mode adapté tenant compte de l'échec de la vérification.

405 Un tel mode adapté peut, par exemple, comprendre un processus d'alerte de l'utilisateur impliquant une action positive de sa part de poursuivre malgré tout la mise en œuvre du dispositif DE ou bien au contraire de ne pas la poursuivre.

Dans une réalisation, il est prévu qu'après au moins un, ou un nombre déterminé d'exécution
410 des étapes de contrôle d'intégrité n'ayant pas abouti à confirmer l'intégrité de la mémoire du moyen de stockage de données MEM par rapport à son état initial, l'échec de la vérification d'authenticité du contenu de la mémoire du moyen de stockage de données MEM entraîne l'une ou plusieurs des modalités de fonctionnement dégradé suivantes :

- notification de l'échec de vérification d'intégrité à l'utilisateur,
- 415 - blocage d'accès aux données chargées dans l'élément sécurisé SE,
- blocage d'accès au dispositif DE,

- effacement de tout ou partie des données stockées dans le dispositif DE et les éléments qui le composent.

420 Dans une réalisation (voir figure 3), il est prévu que 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 l'exécution d'une séquence des étapes correspondant aux flèches C, D, E et F, et dans lequel, chaque commande de contrôle d'intégrité adressée au dispositif DE entraîne l'exécution des étapes successives suivantes :

- 425 - l'élément sécurisé SE adresse, par l'intermédiaire du processeur MPU, une requête au moyen de stockage de données MEM afin qu'il 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, par l'intermédiaire du processeur (MPU), du ou des séquences demandées et
430 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.

435 Lorsque le délai écoulé entre l'envoi de la requête par l'élément sécurisé SE et la réception de la 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.

440