

SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR,
TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés (*sauf indication contraire, pour tout titre de protection régionale disponible*) : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasién (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Publiée:

— avec rapport de recherche internationale (Art. 21(3))

PROCEDE DE PROTECTION D'UN TERMINAL DE PAIEMENT

DOMAINE DE L'INVENTION

- 5 La présente invention concerne un procédé de protection d'un terminal de paiement, notamment par carte bancaire. La présente invention concerne également un terminal de paiement sécurisé, notamment par carte bancaire.

ETAT DE LA TECHNIQUE

- 10 Les terminaux de paiement par carte bancaire sont dédiés au paiement (tel un terminal pour point de vente avec un clavier d'authentification par code confidentiel intégré ou séparé) ou à la distribution de produits (tels un guichet automatique ou un self-service de distribution d'essence).

- 15 Les terminaux de paiement par carte bancaire doivent être conformes aux standards de sécurité PCI PTS (pour « Payment Card Industry Pin Transaction Security » en anglais). La dernière version du standard « PCI PTS V5 » impose des normes de protection relatives à la sécurité physique active d'un terminal de paiement.

- 20 La sécurité physique active selon le standard PCI PTS consiste à protéger des clés de chiffrement (ainsi que d'autres données sensibles comme un numéro de carte, un numéro d'identification personnel du porteur, etc..) contenues dans le terminal de paiement contre entre autres :

- l'intrusion physique par perçage ou autre ;
- l'ouverture du terminal ;
- 25 - l'usage du terminal dans des zones de températures où celui-ci n'est plus qualifié ;
- la variation des fréquences des horloges pour tenter de faire fonctionner le terminal dans des situations où il n'est pas qualifié ; et
- le fonctionnement du terminal avec des tensions trop basses ou trop hautes.

- 30 En conséquence, dans le cas où la sécurité physique du terminal est compromise toutes les clés de chiffrement stockées dans le terminal doivent être effacées pour protéger les transactions, les identités, les applications...

- 35 Les méthodes actuelles pour réaliser la sécurité physique PCI PTS consistent à utiliser des microprocesseurs spécifiques développés précisément pour ce marché de sécurité. Ils

intègrent un circuit matériel capable de gérer et piloter les protections physiques demandées par le standard PCI PTS. Ces microprocesseurs de sécurité sont des microprocesseurs cryptographiques dédiés, spécialement conçus pour protéger les clés de chiffrement tout au long de leur cycle de vie.

5 Cependant, de tels microprocesseurs sécurisés, qui s'appuient sur des mécanismes matériels spécifiques, ont un coût important.

De plus, en cas de détection d'une anomalie de sécurité physique, le terminal nécessite un retour en maintenance pour être remis en fonctionnement, ce qui peut s'avérer dommageable dans le cas où l'anomalie ne correspond pas à une véritable attaque de sécurité
10 physique.

Il existe donc un besoin de fournir une solution de paiement bancaire moins onéreuse, tout en offrant un niveau de sécurité au moins équivalent aux solutions actuelles, permettant de sécuriser des clés cryptographiques et de fournir des services de chiffrement, de
15 déchiffrement, d'authentification et de signature électronique pour tous types d'applications.

Il existe également un besoin de fournir une solution permettant de différencier facilement des anomalies de fonctionnement d'une véritable attaque de sécurité physique.

EXPOSE DE L'INVENTION

20 La présente invention a pour but de pallier aux besoins décrits ci-dessus en proposant un procédé de protection logiciel d'un terminal de paiement traitant et conservant de manière sécurisée les clés de chiffrement dudit terminal.

Plus précisément, l'invention a pour objet un procédé de protection d'un terminal de paiement, ledit terminal de paiement comprenant :

- 25 - une clé de cryptage de données accédée pour le cryptage de données à sécuriser ;
 - un module de surveillance d'au moins un paramètre physique du terminal comprenant un moyen de mesure dudit paramètre physique ;
 - un microcontrôleur ;
 - une unité compteur du microcontrôleur ;
30 - Une horloge, l'unité compteur étant asservi sur ladite horloge pour incrémenter à intervalle régulier une valeur compteur de l'unité compteur ;
 ledit procédé comprenant les étapes suivantes :
 - mesure d'un paramètre physique par le moyen de mesure du dispositif de surveillance ;
 - comparaison de la valeur mesurée à une valeur seuil prédéterminée, correspondante à
35 une attaque physique dudit terminal par le dispositif de surveillance ;

- suppression de l'accès à la clé de cryptage de données par le microprocesseur si une des conditions suivantes est remplie :
 - au moins une valeur de paramètres physiques est significative d'une attaque physique dudit terminal ;
 - 5 ○ la valeur compteur est supérieure à une valeur seuil prédéfinie ;
 - réinitialisation de l'unité compteur par le dispositif de surveillance ; et dans lequel les étapes de mesure, de comparaison, et de réinitialisation sont exécutées périodiquement.
- 10 Avantageusement, mais facultativement, le système selon l'invention peut en outre comprendre au moins l'une des caractéristiques suivantes :
- la clé de cryptage est générée par la combinaison d'une pluralité de clés stockées dans au moins une mémoire du terminal ;
 - l'étape de suppression met en œuvre des méthodes de suppressions distinctes pour la
15 première clé stockée dans une zone de mémoire de type registre du microprocesseur, et la seconde clé stockée dans une zone de mémoire de type mémoire volatile du microprocesseur ;
 - la clé de cryptage est générée par la combinaison d'une première et d'une seconde clé, la première clé étant stockée dans une zone de mémoire de type registre du microprocesseur, la seconde clé étant stockée dans une zone de mémoire de type mémoire volatile du
20 microprocesseur, et dans lequel de suppression comporte la suppression d'au moins une clé de la zone de mémoire associée ;
 - la période d'exécution T1 étant aléatoirement comprise dans un intervalle de valeurs prédéfinies [T1a ; T1b] ;
 - le procédé (100) comporte également les étapes suivantes :
25 ○ vérification que la valeur du délai prédéfini T1 est comprise dans un intervalle de valeurs prédéfini, et si la valeur n'est pas comprise dans l'intervalle :
 - suppression d'au moins une clé de la pluralité de clés ;
 - le terminal de paiement comporte également une seconde horloge avec une fréquence prédéfinie pour piloter la période d'exécution T1, ladite horloge étant configurée pour
30 transmettre dans une étape une interruption au microcontrôleur pour l'exécution périodique des étapes de mesure, de comparaison, et de réinitialisation ;
 - le terminal comporte également une troisième horloge avec une fréquence prédéfinie et dans lequel le procédé comporte une étape de vérification de la fréquence de la seconde horloge comprenant :

- l'incrémentation d'une unité compteur à chaque signal d'horloge de la seconde horloge ;
 - la détermination d'une fréquence par le calcul du nombre d'incrémentations dans un cycle d'horloge de la troisième horloge ;
 - 5 ○ comparaison de la fréquence calculée avec un intervalle de fréquence prédéterminé ; et si la fréquence calculée n'est pas l'intervalle
 - suppression d'au moins une clé de la pluralité de clés ;
 - le terminal comporte également une étape de vérification de la fréquence de la troisième horloge comprenant :
 - 10 ○ l'incrémentation d'une unité compteur à chaque signal d'horloge de la troisième horloge ;
 - la détermination d'une fréquence par le calcul du nombre d'incrémentations dans un cycle d'horloge de la première horloge ;
 - comparaison de la fréquence calculée avec un intervalle de fréquence
 - 15 prédéterminé ; et si la fréquence calculée n'est pas l'intervalle
 - suppression d'au moins une clé de la pluralité de clés ;
 - le terminal comporte également un filtre passe-bande configuré pour filtrer une bande de fréquences prédéfinie et pour recevoir un signal d'horloge de la première horloge, et ledit procédé comporte également une étape comprenant la suppression d'au moins une clé de la
 - 20 pluralité de clés si aucun signal n'est présent en sortie du filtre ;
 - le dispositif de surveillance d'au moins un paramètre physique du terminal comporte un ou plusieurs moyens de mesure configuré pour :
 - mesurer la tension d'alimentation du terminal de paiement ;
 - mesurer la température de fonctionnement du terminal de paiement;
 - 25 ○ détecter l'ouverture du terminal de paiement; et
 - détecter le perçage du terminal de paiement.
 - le dispositif de surveillance est configuré pour émettre un signal de violation significatif d'une attaque physique dudit terminal ; et dans lequel
 - le microcontrôleur comporte au moins un port de réception dudit signal de violation; et dans
 - 30 lequel l'accès à la clé de cryptage de données est supprimé à la réception dudit signal sur ledit port de réception ;
 - le microprocesseur est également configuré pour, préalablement à la suppression de l'accès à la clé de cryptage de données, exécuter un algorithme de filtrage à la suite de la réception du signal de violation, ledit algorithme de filtrage détectant si le signal de violation

est significatif d'une attaque physique dudit terminal, et pour dans ce cas procéder à la suppression de l'accès à la clé de cryptage de données ;

Un tel procédé présente l'avantage d'utiliser une architecture de sécurité logicielle basée sur un microcontrôleur standard à usage général pour exécuter cette architecture. Le procédé étant conforme aux exigences de l'industrie des cartes de paiement, l'architecture logicielle fournit des protections contre les attaques physiques et les attaques logicielles pour garantir la confidentialité et l'authenticité des données. Ainsi, il est possible de construire un point de vente sans l'utilisation d'un "processeur sécurisé" rendant la solution proposée plus économique.

L'invention a également pour objet un produit programme d'ordinateur comprenant des instructions de code pour l'exécution d'un procédé de protection d'un terminal de paiement, tel que précédemment décrit, lorsque ce programme est exécuté par un processeur dudit terminal de paiement.

L'invention a également pour objet un terminal de paiement sécurisé comprenant :

- une clé de cryptage de données, ladite clé de cryptage étant accédée pour le cryptage de données à sécuriser ;
 - un dispositif de surveillance d'au moins un paramètre physique du terminal comprenant un moyen de mesure dudit paramètre physique ;
 - un microcontrôleur ;
 - une unité compteur du microcontrôleur,
 - une horloge, l'unité compteur étant asservi sur ladite horloge pour incrémenter à intervalle régulier une valeur compteur de l'unité compteur ;
- ledit dispositif de surveillance étant configuré pour périodiquement:
- mesurer un paramètre physique par le moyen de mesure ;
 - comparer de la valeur mesurée à une valeur seuil prédéterminée, correspondante à une attaque physique dudit terminal par le dispositif de surveillance ;
 - supprimer l'accès à la clé (MK) de cryptage de données si l'une des conditions suivantes est remplie :
 - o au moins une valeur de paramètres physiques est significative d'une attaque physique dudit terminal ;
 - o la valeur compteur est supérieure à une valeur seuil prédéfinie ; et
 - réinitialiser l'unité compteur .

Avantageusement, mais facultativement, le terminal de paiement sécurisé selon l'invention peut en outre être configuré pour la mise en œuvre d'un procédé selon l'une des caractéristiques précédemment décrites.

5 DESCRIPTION DES FIGURES

D'autres caractéristiques, buts et avantages de l'invention ressortiront de la description qui suit, qui est purement illustrative et non limitative, et qui doit être lue en regard des dessins annexés, sur lesquels :

- 10 - la figure 1 illustre une architecture matérielle d'un terminal sécurisé mettant en œuvre un procédé de protection dudit terminal selon l'invention ;
- la figure 2 illustre de façon plus détaillée l'architecture matérielle du terminal sécurisé selon l'invention ;
- la figure 3 illustre des étapes d'un procédé de protection du terminal selon l'invention.

15 DESCRIPTION DETAILLEE DE L'INVENTION

En référence à la **figure 1**, il est illustré un terminal de paiement 1.

Ledit terminal 1 comporte un microcontrôleur 10, par exemple reposant sur une architecture électronique basée sur un noyau ARM, tel qu'un microcontrôleur du type STM32 (microcontrôleur 32 bits). Celui-ci comporte de façon usuelle un processeur, des
20 mémoires (mémoire morte et mémoire vive), des unités périphériques et des interfaces d'entrées-sorties.

Le microcontrôleur 10 comporte également une horloge temps réel interne (terme parfois abrégé en HTR, dit RTC pour « Real-Time Clock » en anglais), permettant un décompte très
25 précis du temps, en vue de dater ou déclencher des événements selon l'heure. Cette horloge utilise par exemple un quartz piézoélectrique.

L'horloge temps réel nécessite un signal d'horloge ou un oscillateur à quartz pour garder le temps. Le microcontrôleur 10 comporte donc des moyens d'interactions avec une horloge externe 13 (dite LSE pour « Low Speed External » en anglais) utilisée pour piloter l'horloge
30 temps réel interne. Ladite horloge 13, comprise dans le terminal de paiement 1, fournit préférentiellement une fréquence d'horloge entre environ 30 et environ 34Khz, préférentiellement de 32.768 KHz.

Le microcontrôleur 10 comporte également des moyens d'alimentation 12, par exemple
35 par une batterie où des cellules fournissent l'alimentation électrique principale. Lorsque

l'alimentation principale est retirée, une alimentation de secours (comme une pile bouton interne) maintient le terminal 1 sous tension.

Avantageusement, le terminal de paiement est prévu pour fonctionner dans une gamme de tension prédéterminée.

5 Préférentiellement, la tension d'alimentation principale (Vcc) est régulée à 3,3 V pour alimenter l'ensemble du terminal de paiement 1.

Le microcontrôleur 10 comporte également des moyens d'interactions avec des composants matériels de sécurité (par exemple par des ports d'entrée/sortie, dit GPIO pour
10 General Purpose Input/Output en anglais) décrits plus en détail dans la suite de la description.

En référence à la **figure 2**, le microcontrôleur 10 est maintenant détaillé.

Le microcontrôleur 10 comporte deux horloges internes 161 et 162.

L'horloge interne 161 est de type HSI (« HiSpeed internal » en anglais). Elle est
15 configurée pour fournir une fréquence d'horloge d'environ 16 MHz.

L'horloge interne 162 est de type LSI (« LowSpeed internal » en anglais). Elle est configurée pour fournir une fréquence d'horloge entre environ 30 et environ 34 KHz, préférentiellement de 32.768 KHz.

Avantageusement, ces horloges internes (161,162) sont difficiles à attaquer (au sens de
20 perturbation) sans détruire le microcontrôleur 10, car elles sont localisées à l'intérieur de celui-ci.

Le microcontrôleur 10 comporte également une mémoire 151 comportant des registres. Un registre est un emplacement de mémoire interne à un processeur. Les registres se situent
25 au sommet de la hiérarchie mémoire, présentant un temps d'accès en lecture/écriture très rapide.

Le microcontrôleur 10 comporte en outre une mémoire 152 volatile : elle ne peut se passer d'alimentation sous peine de voir les informations stockées dans celle-ci, effacées
30 irrémédiablement.

La mémoire 152 est de préférence de type SRAM (pour l'anglais « Static Random Access Memory »), elle est particulièrement adaptée aux applications qui requièrent soit des temps d'accès courts, et/ou une faible consommation électrique.

35

Le processeur μ du microcontrôleur 10 est configuré pour mettre en œuvre une bibliothèque cryptographique logicielle sécurisée protégée en écriture, et comporte un véritable générateur de nombres aléatoires, ainsi que des protections contre les attaques par canal latéral telles que les attaques par analyse de consommation électrique (par exemple par DPA et SPA) et les attaques de synchronisation d'horloges.

Le processeur μ du microcontrôleur 10 est également configuré pour mettre en œuvre des instructions pour l'exécution d'un procédé de protection logiciel.

Préférentiellement, les fonctionnalités matérielles et de sécurité sont rassemblées dans un noyau de système d'application sécurisé, qui est séparé des fonctions non liées à la sécurité, à un niveau d'exécution très bas en utilisant les capacités du microcontrôleur 10. En effet, ledit noyau dispose de privilèges pour accéder à l'ensemble des ressources matérielles du processeur μ (notamment les GPIO), et contrôle une partie du processeur qui gère la protection des accès à la mémoire (par exemple dit MPU pour Memory Protection Unit pour un processeur ARM). Ainsi, les données sensibles (telles que les clés cryptographiques) sont privées au noyau sécurisé, et chiffrées par une clé principale MK seulement connue (c'est-à-dire accessible) du noyau sécurisé.

La partie principale du procédé de protection logiciel comporte une « boucle sécurisée logicielle » exécutée par le processeur μ afin de protéger la clé principale MK. Ladite boucle permet de détecter les événements d'attaque de sécurité et déclencher l'effacement de la clé principale MK dans le cas d'un tel événement, rendant extrêmement difficile le vol de données ou le clonage du terminal de paiement 1.

Egalement, la boucle de sécurité peut permettre de collecter ces événements d'attaque de sécurité, pour éventuellement appliquer à ces événements un filtrage puis déclencher l'effacement de la clé principale MK.

La clé principale MK à protéger, répond à un standard de chiffrement, par exemple le standard AES128, AES (« Advanced Encryption Standard » en anglais) avec une clé de longueur 128, 192 ou 256 bits.

Préférentiellement, afin d'avoir une redondance sur l'effacement de la clé MK, celle-ci est générée à partir de la combinaison d'au moins deux clés K1 et K2, par exemple par la combinaison XOR de K1 et K2. Seules les clés K1 et K2 sont stockées en mémoire, la clé MK n'étant ainsi jamais stockée dans une mémoire persistante en clair. Les clés K1, K2 peuvent être stockées dans des zones mémoires distinctes.

Ainsi, la clé K1 est par exemple stockée dans un emplacement de mémoire interne d'un registre 151 du microprocesseur. Avantageusement, un tel emplacement mémoire permet d'obtenir un temps d'accès en lecture/écriture très rapide.

De surcroît, ces registres 151 peuvent être réinitialisés via une entrée GPIO extérieure
5 qui permet un effacement quasi instantané.

Quant à elle, la clé K2 est par exemple stockée dans une mémoire interne vive 152 statique ou dynamique de type RAM, SRAM ou FLASH. Facultativement, la clé K2 est stockée à une adresse déterminée aléatoirement.

De façon optionnelle, les registres 151 et la mémoire interne vive 152 utilisent des
10 mécanismes d'effacements différents, ce qui permet avantageusement d'augmenter la protection logicielle.

En référence également à la **figure 3**, il sera maintenant décrit un procédé 100 de protection du terminal de paiement 1, implémentant une boucle de sécurité BS.

15 Le procédé 100 permet de protéger le terminal de paiement 1 par la surveillance contre les attaques physiques et les attaques logicielles pour garantir la confidentialité et l'authenticité des données. Les attaques physiques considérées sont par exemple liées à l'altération de l'appareil, à la température, à l'horloge, à la sous ou surtension, aux impulsions électromagnétiques, au balayage fréquentiel.

20 Suite au démarrage (« **boot** ») ou au redémarrage suite à une réinitialisation (« **reset** ») du terminal de paiement 1, le procédé 100 comporte une étape **E0** d'initialisation du procédé 100. Au lancement, si les clés K1 et K2 ont déjà une valeur, elles sont supprimées, puis le générateur aléatoire est utilisé pour générer un aléa qui devient le nouveau jeu de clés K1, K2. La boucle de sécurité BS peut être exécutée en continu. Cependant, de façon préférentielle,
25 pour limiter la consommation, la boucle de sécurité BS est exécutée périodiquement, par exemple environ toutes les 100ms, ainsi le reste du temps le microcontrôleur 10 est dans un état de veille.

Ainsi, après l'étape d'initialisation E0, dans une étape **E1**, la boucle de sécurité BS est démarrée, mais mise dans un état de veille.

30 Une unité minuteur 111 permet d'activer l'exécution de la boucle BS périodiquement.

L'unité minuteur 111 est pilotée par exemple par l'horloge LSE. Ladite unité 111 génère périodiquement des interruptions à destination du processeur μ du microcontrôleur 10. Ces interruptions permettent l'arrêt temporaire de l'exécution normale d'un programme en tâche de fond du terminal de paiement 1, dans le but d'exécuter la boucle de sécurité BS.

Avantageusement, pour éviter qu'un attaquant se synchronise sur la boucle de sécurité BS, la valeur du temps entre deux itérations de la boucle est aléatoire entre environ 80ms et environ 100ms.

Dans ce but, l'unité minuteur 111 utilise le générateur aléatoire interne au microcontrôleur 10 pour générer une variation aléatoire inférieure à environ 20 ms.

Le microcontrôleur 10 s'assure en outre que ce nombre aléatoire n'est pas utilisé à d'autres fins.

Il est maintenant décrit plus en détail des attaques physiques dont le procédé 100 et le terminal de paiement sécurisé 1 ont pour responsabilité de surveiller.

Ouverture

Une attaque de sabotage par ouverture se produit lorsque le terminal de paiement 1 est ouvert ou qu'un composant inattendu entre dans une zone sécurisée dudit terminal 1. L'ouverture du terminal 1 est détectée grâce à une pluralité de commutateurs (Sw1, Sw2, ..., SwN) localisés en différents endroits d'un boîtier du terminal 1. Les commutateurs sont par exemple implémentés par des GPIO configurés en entrée du microcontrôleur 10, élevés par des résistances internes au microcontrôleur 10.

Lorsque le terminal 1 est fermé, ces signaux sont connectés à une phase à la masse du terminal de paiement 1.

Un module de surveillance d'ouverture 121 a pour fonction de détecter un état d'ouverture du terminal par la surveillance de la valeur de la pluralité des signaux transmis par les commutateurs (Sw1, Sw2, ..., SwN). Par exemple, dans un état non-ouvert du terminal, les commutateurs ont pour valeur une première valeur (par exemple égale à 0). Si le terminal est ouvert, au moins un des commutateurs, selon son emplacement, est à même de détecter cette ouverture, en prenant une seconde valeur (par exemple égale à 1). Le module de surveillance d'ouverture 121 a pour fonction de détecter un tel changement de valeur d'au moins un commutateur, et de transmettre un signal de violation S1 au microcontrôleur 10. Celui-ci peut être configuré pour comporter des moyens de réception dudit signal de violation S1, tels qu'un ou plusieurs ports spécifiques, sur lesquels la réception d'un signal audit microprocesseur 10 signifie la détection d'une attaque. Lesdits ports peuvent être spécifiques ou non à un type d'attaque.

Perçage

Le perçage du terminal 1 est détecté grâce à au moins un treillis métallique. Celui-ci est implémenté par exemple par un maillage connecté aux moyens d'interface du microcontrôleur. Par exemple, un maillage est un couple (A, B) de GPIO. Au moins deux mailles M1, M2 sont ainsi nécessaires pour protéger l'appareil du perçage. GPIO A est configuré en entrée et GPIO B en sortie.

Un module de surveillance de perçage 122 écrit une séquence aléatoire, par exemple de 16 bits, vers la sortie (le débit étant choisi en fonction des contraintes matérielles, en effet, le temps de montée et de descente dépend de la longueur du maillage). La même séquence doit être lue sur l'entrée GPIO. Ensuite, GPIO B est défini comme entrée et A comme sortie et la même vérification est appliquée.

La séquence aléatoire de bits appliquée est choisie au hasard parmi un ensemble de séquences possibles (par exemple au moins 20). La séquence aléatoire est générée par le générateur aléatoire réel interne du microcontrôleur 10. En outre, celui-ci s'assure que la séquence aléatoire n'est pas utilisée à d'autres fins.

En conséquence, dans le cas où la séquence réceptionnée ne correspond pas à la séquence prédéfinie, le module de surveillance 122 est configuré pour transmettre un signal de violation S1 au microprocesseur 10.

Température

Une attaque de température est détectée lorsque la température courante du terminal de paiement 1 est supérieure ou inférieure à une plage de température attendue. Par exemple, la plage de température de fonctionnement normale est d'environ [-30 °C ; + 85 °C].

Le microcontrôleur 10 comporte par exemple au moins un capteur de température intégré pour mettre en œuvre la surveillance de la température.

Un module de surveillance température 123 a pour fonction de mesurer les températures, via le(s) capteur(s) de température, de détecter un état anormal de la température si la température mesurée n'est pas dans la zone de fonctionnement normal prévue, et dans ce cas de transmettre un signal de violation S1 au microprocesseur 10.

Fréquence d'horloge

Les fonctions de surveillance exécutées par les différents modules de surveillance 121 à 123 permettent donc d'effectuer une surveillance sécurisée chargée de détecter une variété d'attaques physiques.

Un module de sécurité 120 regroupe les modules de surveillance 121 à 123 et les fonctions de surveillance associées. Ledit module 120 de sécurité est configuré pour effectuer

une surveillance sécurisée et de détecter des attaques de sécurité sur le terminal de paiement 1 en implémentant la boucle de sécurité BS (qui exécute les fonctions du module de sécurité 120) décrite précédemment.

5 Ainsi, dans une étape **E10a**, il est procédé à la mesure des différents paramètres physiques à surveiller par les moyens de mesure du module de sécurité 120.

Dans une étape **E10b**, il est ensuite procédé à la comparaison des valeurs mesurées à des valeurs seuils prédéterminées, correspondantes à des attaques physiques du terminal 1. Dans le cas où une comparaison est significative d'une attaque physique du terminal 1, un signal de violation S1 est transmis à un port de réception du microprocesseur 10

10

Pour assurer que la boucle de sécurité BS est systématiquement exécutée malgré les attaques, la fréquence de l'horloge qui pilote l'unité minuteur 111, l'horloge LSE (Low Speed External Clock), est vérifiée par un compteur piloté par la HSI (High Speed Internal Clock).

15 Dans ce but, dans une étape **E10c**, le module de sécurité 120 fait dans la boucle de sécurité BS, un premier comptage du nombre de « coups » (tel un front montant ou descendant d'un signal d'horloge) de l'horloge HSI dans un cycle de l'horloge LSI pour vérifier que la fréquence de l'horloge HSI est dans un intervalle de fréquence acceptable (par exemple dans la gamme de fonctionnement normal [+/- 30 KHz]). Dans le cas où cette condition ne serait pas vérifiée un signal de violation S1 est transmis à un port de réception du microprocesseur 10

20 Puis, dans une étape **E10d**, le module de sécurité 120 fait dans la boucle de sécurité BS, un second comptage du nombre de coups de l'horloge LSE dans un cycle de l'horloge HSI pour vérifier que la fréquence de l'horloge LSE est dans un intervalle de fréquence acceptable (par exemple dans la gamme de fonctionnement normal [30 KHz - 34 KHz]). Dans le cas où cette condition ne serait pas vérifiée un signal de violation S1 est transmis à un port de réception du microprocesseur 10

25

Le procédé 100 comporte également un autre mécanisme pour s'assurer que la boucle BS est régulièrement exécutée.

30 Ainsi le procédé 100 comporte un mécanisme dit « chien de garde » implémenté par un module 126 de surveillance de boucle BS, par exemple configuré pour mettre en œuvre un compteur qui est régulièrement remis à zéro. Si le compteur dépasse une valeur donnée (timeout) alors il est procédé à un redémarrage (reset) du terminal de paiement 1.

35 Plus précisément, le module 126 de surveillance de boucle BS est démarré au démarrage du terminal de paiement 1 et ne peut jamais être arrêté tant que ce dernier est en fonctionnement. Si le compteur atteint une valeur prédéfinie, le terminal 1 est réinitialisé.

Seule la boucle sécurisée BS "actualise" le compteur du module 126 de surveillance de boucle dans une étape **E13**, en effet, préférentiellement seule la boucle sécurisée BS dispose de l'accès au compteur 126. L'opération de rafraîchissement est effectuée une seule fois pendant le cycle de surveillance (c'est-à-dire que le chien de garde est actualisé dans le processus de boucle sécurisée périodique lorsque toutes les surveillances ont été traitées dans un laps de temps donné).

Le module 126 de surveillance de boucle, compare le compteur avec une valeur limite prédéfinie pour surveiller si la boucle de sécurité BS n'est pas exécutée dans le temps prédéfini.

Ainsi, si cette situation se présente, le compteur du chien de garde atteindra la valeur limite prédéfinie, et dans une étape **E50**, le module 126 de surveillance de boucle transmet un signal S2 de redémarrage au microprocesseur 10.

Avantageusement, ce mécanisme de chien de garde permet d'assurer que tout le code lié à la sécurité est exécuté dans le temps.

Préférentiellement, le délai d'expiration du chien de garde est environ égal à "Période de surveillance périodique + 50 ms".

Le compteur du module 126 de surveillance de boucle est piloté par l'horloge LSI, pour être incrémenté à chaque coup d'horloge (réception d'un front montant ou descendant du signal d'horloge). La fréquence de l'horloge LSI est donc également surveillée pour vérifier qu'il n'y a pas d'attaque du terminal de paiement 1 par manipulation de la fréquence de ladite horloge LSI dans une zone de fréquence anormale, dans le but d'entraîner un dysfonctionnement du terminal de paiement 1.

Ainsi, la vérification de la fréquence de la LSI (par exemple dans la gamme de fonctionnement normal [30 KHz - 34 KHz]) est réalisée dans une étape **E30** par un module 131 de vérification de fréquence, implémenté par exemple par un circuit passe-bande externe associé à un transistor dont la sortie pilote la transmission d'un signal de violation S1 à un port de réception du microprocesseur 10.

Tension d'alimentation

Une attaque de sécurité est considérée lorsque la tension d'alimentation du microcontrôleur 10 est inférieure ou supérieure à des valeurs seuils.

La tension Vcc du microcontrôleur 10 est fournie par l'alimentation principale lorsque la batterie est branchée et par l'alimentation de secours lorsque la batterie est retirée. Le système étant ainsi normalement toujours alimenté, la perte de Vcc est considérée comme une attaque de sécurité.

Le microcontrôleur 10 comporte un module de surveillance de tension basse 141 pour mesurer la tension et détecter lorsque la tension est inférieure à une valeur seuil, par exemple lorsque la tension chute en dessous d'environ 2.2V.

Le module de surveillance de tension basse 141 est par exemple implémenté par un
5 circuit de réinitialisation de baisse de tension interne au microprocesseur 10, ledit circuit étant configuré pour transmettre un signal de réinitialisation S2 au microprocesseur 10.

La réinitialisation a pour effet de supprimer les données de la mémoire vive, et donc la suppression de la clé K2. Préférentiellement, la réinitialisation est détectée "instantanément" (c'est-à-dire qu'il s'agit d'un circuit uniquement matériel). Pour optimiser le délai de suppression
10 de la clé K2, celle-ci peut être placée dans une zone d'adresse en début de mémoire 152

Une attaque de sécurité est considérée lorsque Vcc est par exemple au-dessus de 3.7V.

Un module de surveillance de tension haute 132 est responsable de la surveillance haute tension, par exemple sous la forme d'un contrôleur externe de surveillance de très faible puissance. Celui-ci est configuré pour, dans une étape **E40**, détecter lorsque la tension est
15 supérieure à une valeur seuil par exemple 3,7V, et si cette condition est vérifiée, transmettre un signal de violation S1 à un port de réception du microprocesseur 10.

Le microcontrôleur 10 comporte des ports dédiés à la réception d'un signal de violation S1.

20 Ainsi, dans une étape **E11**, à la réception d'un signal sur un de ces ports, le microcontrôleur 10 procède à la suppression de la clé K1 stockée dans une mémoire de registre 151. Ce traitement permet d'avoir un temps de suppression le plus court possible, l'exécution de la commande de suppression ne dépendant pas d'un signal d'horloge. En outre, la commande peut être exécutée même si les différentes horloges ne sont pas fonctionnelles.

25 En parallèle, il est également procédé à l'effacement de la zone mémoire 152 dans lequel la clé K2 est stockée.

Le microcontrôleur 10 comporte également des ports dédiés à la réception d'un signal de réinitialisation S2.

30 Ainsi, à la réception d'un signal sur un de ces ports, le microcontrôleur 10 procède à la suppression de la clé K2 stockée dans une mémoire volatile dans une étape de **Reset**.

A titre d'exemple, le temps d'effacement pour un mot de 32 bits dans une mémoire de type SRAM2 est de 1 cycle d'horloge (c'est-à-dire 250 ns). Le temps d'effacement SRAM2 complet est $8192 * 250 = 2.048$ ms

35

Egalement, dans une étape **E12**, le module de sécurité peut enregistrer les types d'alarmes et la « date » à laquelle chaque alarme est vue. Avantageusement, les données enregistrées peuvent être analysées lorsque le terminal entre en maintenance suite à une attaque de sécurité.

5

Dans un mode de réalisation alternatif, le terminal de paiement 1 peut comprendre également un module de filtrage (non représenté).

10 Ainsi, dans une étape **E12'**, quand le module de sécurité détecte une anomalie, le module de filtrage est configuré pour traiter l'alarme et pour ensuite exécuter un algorithme de filtrage/détection pour une ou plusieurs itérations de la boucle de sécurité BS. Ledit algorithme permet de déclarer si l'alarme est significative d'une véritable situation de piratage du terminal pour dans ce cas procéder à la suppression d'une ou plusieurs clés stockées.

15 Dans un mode de réalisation particulier, un algorithme de filtrage/détection est tel qu'à la réception d'un ou de plusieurs signaux de violation S1 dans un premier délai déterminé, le microcontrôleur 10 procède à la suppression de la clé K1 dans le cas où un signal de violation S1 est reçu dans un second délai déterminé (par exemple environ une seconde). Un tel algorithme permet de réaliser un filtrage sur les événements d'origine mécanique (ouverture, perçage...). Ainsi, si plusieurs événements mécaniques sont détectés simultanément et s'arrêtent avant le délai déterminé, la clé MK n'est pas supprimée, puisque ceci est par exemple
20 la signature d'un modèle d'une chute du terminal 1.

Pour éviter que des hackers, après avoir eu accès à cet algorithme, utilisent ce filtrage pour attaquer plus facilement le terminal, le système de filtrage ne peut pas être activé pendant un délai (dont une composante est aléatoire) à la suite d'une séquence de filtrage d'un même événement. Ceci n'a pas d'effet dans le cadre d'une utilisation normale puisque par exemple
25 dans le cas d'un événement de chute, il est peu probable de faire tomber deux fois de suite en moins de quelques secondes le même terminal.

Par ailleurs, avantageusement, le terminal 1 peut être configuré avec des modèles d'attaque physique, en utilisant des événements d'attaques collectés sur plusieurs types de chute, lors de phase de conception ou de test du terminal. Ce modèle est ainsi utilisé pour
30 filtrer les attaques pendant la vie du produit.

Avantageusement, ceci permet d'éviter de déclarer une attaque alors que la détection d'une attaque ne correspond qu'à un parasite passager.

En outre, les données enregistrées (alarme(s) et date(s)) par le terminal de paiement 1, ou par une pluralité de terminaux de paiement 1, peuvent être analysées pour affiner
35 l'algorithme de filtrage/détection

REVENDICATIONS

- 5 1. Procédé (100) de protection d'un terminal (1) de paiement, ledit terminal (1) de paiement comprenant :
- 10 - une clé (MK) de cryptage de données accédée pour le cryptage de données à sécuriser ;
- un module (120) de surveillance d'au moins un paramètre physique du terminal comprenant un moyen de mesure dudit paramètre physique;
- un microcontrôleur (10);
- une unité compteur du microcontrôleur,
- une horloge (LSI), l'unité compteur étant asservi sur ladite horloge pour incrémenter à intervalle régulier une valeur compteur de l'unité compteur ;
- 15 ledit procédé comprenant les étapes suivantes :
- (E10a) mesure d'un paramètre physique par le moyen de mesure du dispositif de surveillance ;
- (E10b) comparaison de la valeur mesurée à une valeur seuil prédéterminée, correspondante à une attaque physique dudit terminal par le dispositif de
- 20 surveillance ;
- (E11) suppression de l'accès à la clé (MK) de cryptage de données par le microprocesseur (10) si une des conditions suivantes est remplie :
- au moins une valeur de paramètres physiques est significative d'une attaque physique dudit terminal ;
- 25 ○ la valeur compteur est supérieure à une valeur seuil prédéfinie ;
- (E13) réinitialisation de l'unité compteur par le dispositif de surveillance ; et dans lequel les étapes de mesure (E10a), de comparaison (E10b), et de réinitialisation (E13) sont exécutées périodiquement.
- 30 2. Procédé (100) de protection d'un terminal (1) de paiement, selon la revendication 1 dans lequel la clé (MK) de cryptage est générée par la combinaison d'une pluralité de clés (K1, K2) stockées dans au moins une mémoire (151, 152) du terminal (1).

3. Procédé (100) de protection d'un terminal (1) de paiement, selon la revendication 2 dans lequel la clé (MK) de cryptage est générée par la combinaison d'une première (K1) et d'une seconde (K2) clé, la première clé (K1) étant stockée dans une zone de mémoire (151) de type registre du microprocesseur (10), la seconde clé (K2) étant stockée dans une zone de mémoire (152) de type mémoire volatile du microprocesseur (10), et dans lequel l'étape (E11) de suppression comporte la suppression d'au moins une clé de la zone de mémoire associée.
4. Procédé (100) de protection d'un terminal (1) de paiement, selon la revendication 3 dans lequel l'étape (E11) de suppression met en œuvre des méthodes de suppressions distinctes pour la première clé (K1) stockée dans une zone de mémoire (151) de type registre du microprocesseur (10), et la seconde clé (K2) stockée dans une zone de mémoire (152) de type mémoire volatile du microprocesseur (10).
5. Procédé (100) de protection d'un terminal (1) de paiement selon l'une des revendications précédentes dans lequel la période d'exécution T1 étant aléatoirement comprise dans un intervalle de valeurs prédéfinies [T1a ; T1b].
6. Procédé (100) de protection d'un terminal (1) de paiement, selon la revendication précédente dans lequel le procédé (100) comporte également les étapes suivantes :
- vérification que la valeur du délai prédéfini T1 est comprise dans un intervalle de valeurs prédéfini, et si la valeur n'est pas comprise dans l'intervalle :
 - suppression d'au moins une clé de la pluralité de clés.
7. Procédé (100) de protection d'un terminal (1) de paiement selon l'une des revendications 5 à 6 dans lequel le terminal (1) de paiement comporte également une seconde horloge (LSE) avec une fréquence prédéfinie pour piloter la période d'exécution T1, ladite horloge (LSE) étant configurée pour transmettre dans une étape (E0) une interruption au microcontrôleur pour l'exécution périodique des étapes de mesure (E10a), de comparaison (E10b), et de réinitialisation (E13).

- 5 8. Procédé (100) de protection d'un terminal (1) de paiement selon la revendication précédente dans lequel le terminal (1) comporte également une troisième horloge (HSI) avec une fréquence prédéfinie et dans lequel le procédé (100) comporte une étape (E50) de vérification de la fréquence de la seconde horloge (LSE) comprenant :
- l'incréméntation d'une unité compteur à chaque signal d'horloge de la seconde horloge ;
 - la détermination d'une fréquence par le calcul du nombre d'incrémentations dans un cycle d'horloge de la troisième horloge ;
 - 10 - comparaison de la fréquence calculée avec un intervalle de fréquence prédéterminé ; et si la fréquence calculée n'est pas l'intervalle
 - suppression d'au moins une clé de la pluralité de clés.
- 15 9. Procédé (100) de protection d'un terminal (1) de paiement, selon la revendication précédente dans lequel le terminal comporte également une étape (E30) de vérification de la fréquence de la troisième horloge (HSI) comprenant :
- l'incréméntation d'une unité compteur à chaque signal d'horloge de la troisième horloge (HSI);
 - la détermination d'une fréquence par le calcul du nombre d'incrémentations dans un cycle d'horloge de la première horloge (LSI) ;
 - 20 - comparaison de la fréquence calculée avec un intervalle de fréquence prédéterminé ; et si la fréquence calculée n'est pas l'intervalle
 - suppression d'au moins une clé de la pluralité de clés.
- 25 10. Procédé (100) de protection d'un terminal (1) de paiement selon l'une des revendications précédentes dans lequel le terminal (1) comporte également un filtre passe-bande configuré pour filtrer une bande de fréquences prédéfinie et pour recevoir un signal d'horloge de la première horloge (LSI), et ledit procédé (100) comporte également une étape comprenant la suppression d'au moins une
- 30 clé de la pluralité de clés si aucun signal n'est présent en sortie du filtre.
11. Procédé (100) de protection d'un terminal (1) de paiement, selon l'une des revendications précédentes dans lequel le dispositif (120) de surveillance d'au

moins un paramètre physique du terminal (1) comporte un ou plusieurs moyens de mesure configuré pour :

- mesurer la tension d'alimentation du terminal (1) de paiement ;
- mesurer la température de fonctionnement du terminal (1) de paiement;
- 5 - détecter l'ouverture du terminal (1) de paiement; et
- détecter le perçage du terminal (1) de paiement.

12. Procédé (100) de protection d'un terminal (1) de paiement, selon l'une des revendications précédentes dans lequel
10 le dispositif (120) de surveillance est configuré pour émettre un signal de violation (S1) significatif d'une attaque physique dudit terminal ; et dans lequel
 le microcontrôleur (10) comporte au moins un port de réception dudit signal de violation (S1); et dans lequel l'accès à la clé (MK) de cryptage de données est
 supprimé à la réception dudit signal (S1) sur ledit port de réception.

15 13. Procédé (100) de protection d'un terminal (1) de paiement, selon la revendication précédente dans lequel le microprocesseur (10) est également configuré pour,
 préalablement à la suppression de l'accès à la clé (MK) de cryptage de données, exécuter un algorithme de filtrage à la suite de la réception du signal de violation
20 (S1), ledit algorithme de filtrage détectant si le signal de violation (S1) est significatif d'une attaque physique dudit terminal, et pour dans ce cas procéder à
 la (E11) suppression de l'accès à la clé (MK) de cryptage de données.

25 14. Terminal (1) de paiement sécurisé comprenant :
 - une clé (MK) de cryptage de données, ladite clé (MK) de cryptage étant accédée pour le cryptage de données à sécuriser ;
 - un dispositif (120) de surveillance d'au moins un paramètre physique du terminal comprenant un moyen de mesure dudit paramètre physique;
30 - un microcontrôleur (10) ;
 - une unité compteur du microcontrôleur (10),
 - une horloge (LSI), l'unité compteur étant asservi sur ladite horloge (LSI) pour incrémenter à intervalle régulier une valeur compteur de l'unité compteur ;
 - ledit dispositif (120) de surveillance étant configuré pour périodiquement :
35 - (E10a) mesurer un paramètre physique par le moyen de mesure ;

- (E10b) comparer de la valeur mesurée à une valeur seuil prédéterminée, correspondante à une attaque physique dudit terminal par le dispositif (120) de surveillance ;
 - (E11) supprimer l'accès à la clé (MK) de cryptage de données si l'une des conditions suivantes est remplie :
 - au moins une valeur de paramètres physiques est significative d'une attaque physique dudit terminal ;
 - la valeur compteur est supérieure à une valeur seuil prédéfinie ;
 - et ;
 - (E13) réinitialiser l'unité compteur.
15. Produit programme d'ordinateur comprenant des instructions de code pour l'exécution d'un procédé (100) de protection d'un terminal (1) de paiement selon l'une quelconque des revendications 1 à 13 lorsque ce programme est exécuté par un processeur.

FIG. 1

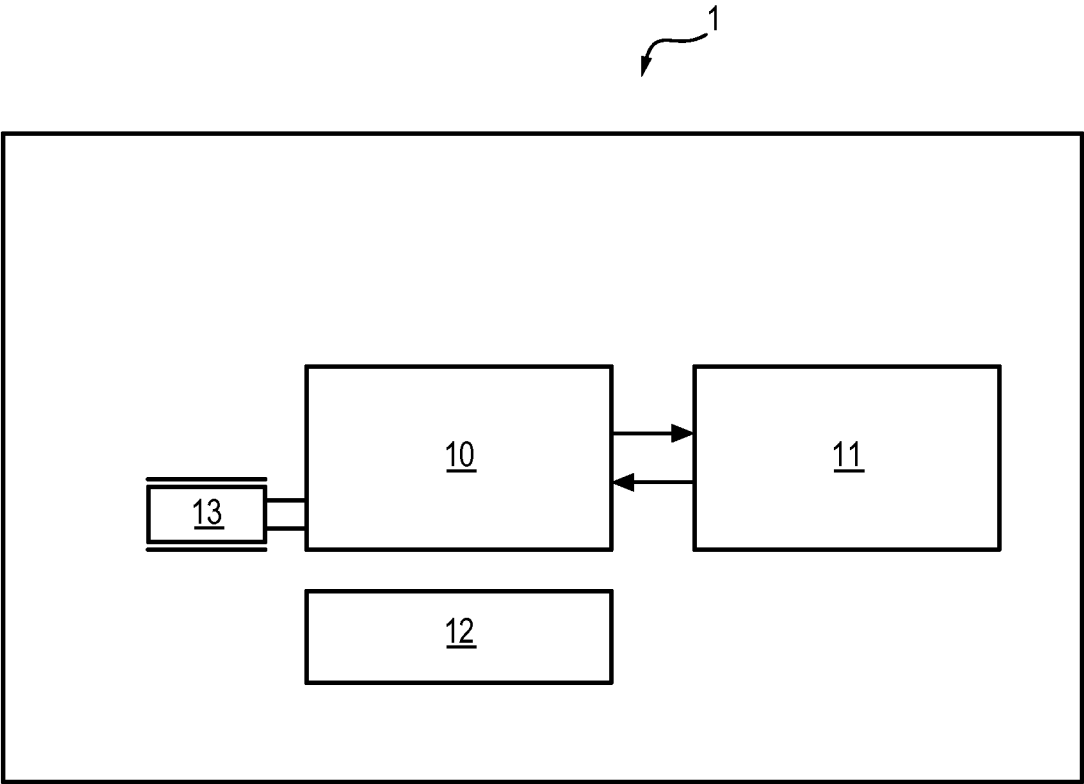
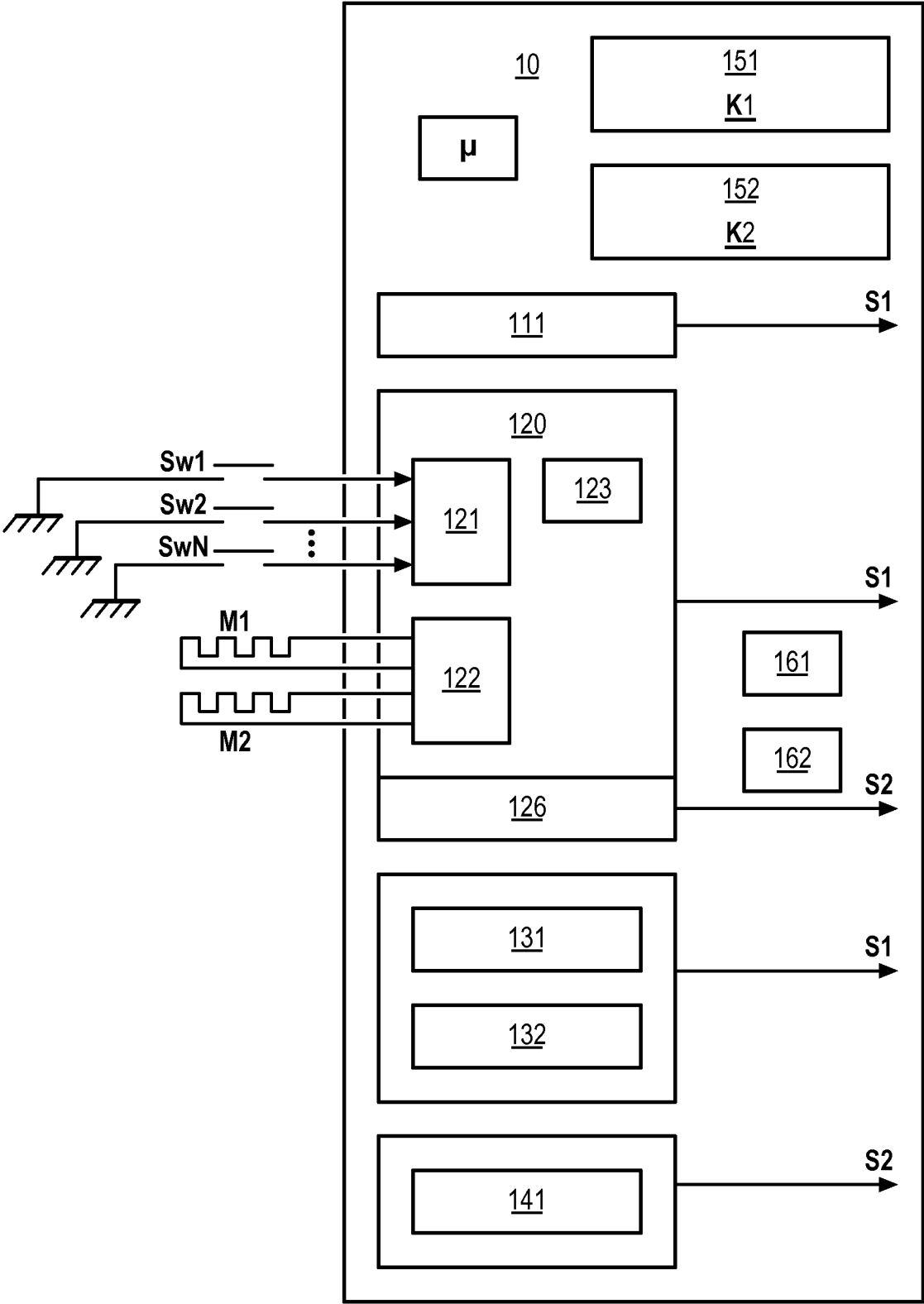
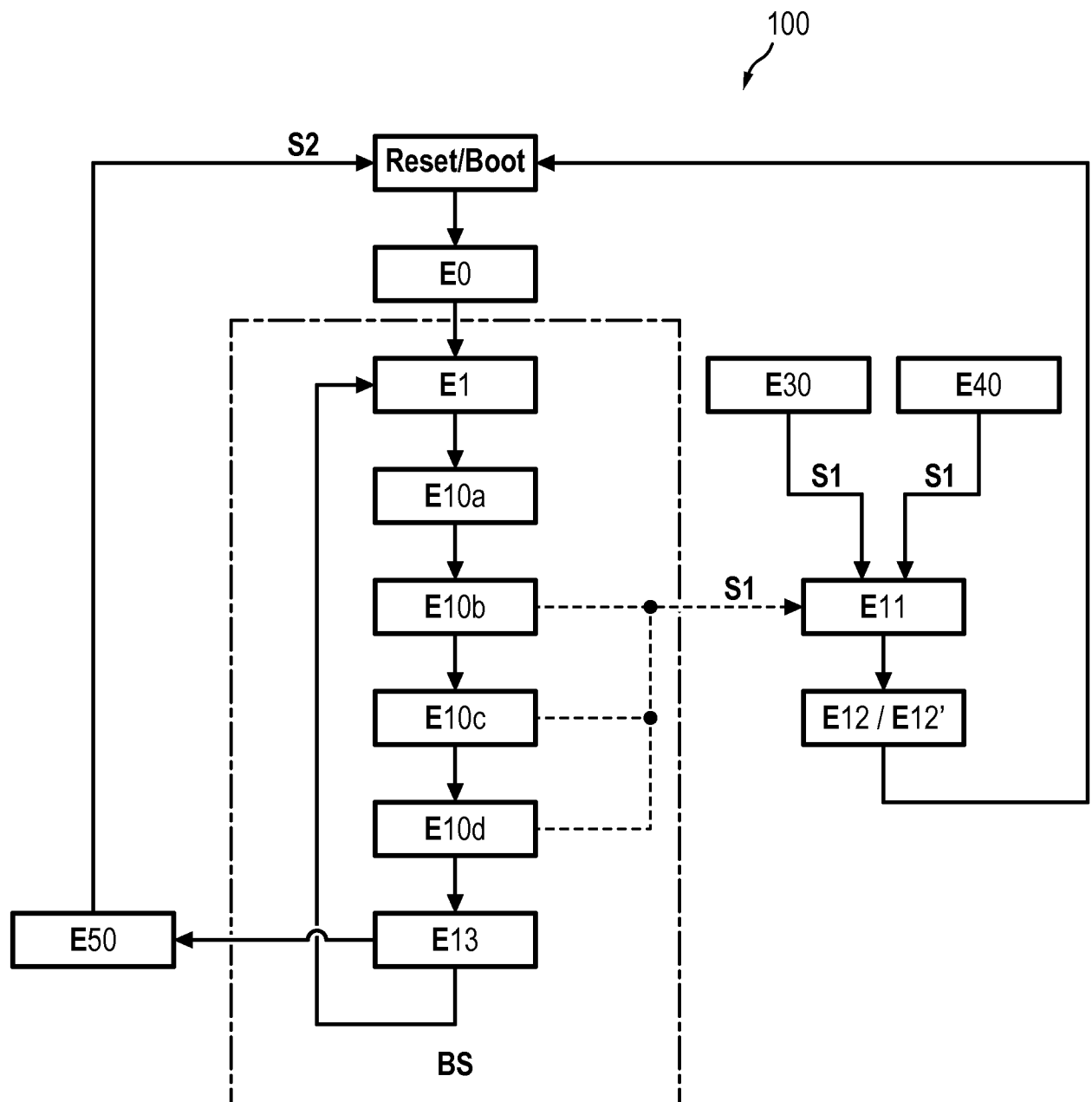


FIG. 2



3/3

FIG. 3



INTERNATIONAL SEARCH REPORT

International application No.

PCT/EP2019/067471

A. CLASSIFICATION OF SUBJECT MATTER G06F 21/55(2013.01)i; G06F 21/86(2013.01)i; G07F 19/00(2006.01)i According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) G06F Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) EPO-Internal		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2017017943 A1 (BILHAN ERKAN [US] ET AL) 19 January 2017 (2017-01-19) paragraph [0022] - paragraph [0027] paragraph [0030] - paragraph [0038] claims 1,3,4,7,11-15 figure 1	1-15
A	RA?L JIM?NEZ-NAHARRO ET AL. "Design and Implementation of a New Real-Time Frequency Sensor Used as Hardware Countermeasure" SENSORS, CH, Vol. 13, No. 9, 01 January 2013 (2013-01-01), pages 11709-11727 DOI: 10.3390/s130911709 ISSN: 1424-8220, XP055441735 page 11710, line 12 - page 11710, line 31 page 11712, line 4 - page 11712, line 9 page 11722, line 14 - page 11722, line 25 page 11725, line 7 - page 11726, line 15	1-15
☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search		Date of mailing of the international search report
16 July 2019		24 July 2019
Name and mailing address of the ISA/EP		Authorized officer
European Patent Office p.b. 5818, Patentlaan 2, 2280 HV Rijswijk Netherlands Telephone No. (+31-70)340-2040 Facsimile No. (+31-70)340-3016		Sauzon, Guillaume Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/EP2019/067471

C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0965902 A2 (NAT SEMICONDUCTOR CORP [US]) 22 December 1999 (1999-12-22) paragraph [0010] - paragraph [0019] paragraph [0052] - paragraph [0062] paragraph [0073] - paragraph [0074] paragraph [0083] - paragraph [0087] paragraph [0112] - paragraph [0115] paragraph [0126] - paragraph [0136] claims 1,4,6,8,9,10 figures 1,9,14a,14b,20a,20b	1-15
X A	FR 2871905 A1 (INNOVA CARD SARL [FR]) 23 December 2005 (2005-12-23) page 3, line 10 - page 3, line 30 claims 1,6 figure 1	1,5-15 2-4

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/EP2019/067471

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
US	2017017943	A1	19 January 2017	CN	106355096	A	25 January 2017
				US	2017017943	A1	19 January 2017
EP	0965902	A2	22 December 1999	DE	69519662	D1	25 January 2001
				DE	69519662	T2	23 May 2001
				EP	0715733	A1	12 June 1996
				EP	0965902	A2	22 December 1999
				KR	960705284	A	09 October 1996
				US	5533123	A	02 July 1996
				WO	9600953	A2	11 January 1996
FR	2871905	A1	23 December 2005	FR	2871905	A1	23 December 2005
				WO	2006008382	A1	26 January 2006

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°

PCT/EP2019/067471

A. CLASSEMENT DE L'OBJET DE LA DEMANDE INV. G06F21/55 G06F21/86 G07F19/00 ADD.		
Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB		
B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE Documentation minimale consultée (système de classification suivi des symboles de classement) G06F		
Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche		
Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés) EPO-Internal		
C. DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 2017/017943 A1 (BILHAN ERKAN [US] ET AL) 19 janvier 2017 (2017-01-19) alinéa [0022] - alinéa [0027] alinéa [0030] - alinéa [0038] revendications 1,3,4,7,11-15 figure 1 ----- -/--	1-15
☒ Voir la suite du cadre C pour la fin de la liste des documents ☒ Les documents de familles de brevets sont indiqués en annexe		
* Catégories spéciales de documents cités: "A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent "E" document antérieur, mais publié à la date de dépôt international ou après cette date "L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée) "O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens "P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée "T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention "X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément "Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier "&" document qui fait partie de la même famille de brevets		
Date à laquelle la recherche internationale a été effectivement achevée 16 juillet 2019		Date d'expédition du présent rapport de recherche internationale 24/07/2019
Nom et adresse postale de l'administration chargée de la recherche internationale Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Fonctionnaire autorisé Sauzon, Guillaume

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	RA?L JIM?NEZ-NAHARRO ET AL: "Design and Implementation of a New Real-Time Frequency Sensor Used as Hardware Countermeasure", SENSORS, vol. 13, no. 9, 1 janvier 2013 (2013-01-01), pages 11709-11727, XP055441735, CH ISSN: 1424-8220, DOI: 10.3390/s130911709 page 11710, ligne 12 - page 11710, ligne 31 page 11712, ligne 4 - page 11712, ligne 9 page 11722, ligne 14 - page 11722, ligne 25 page 11725, ligne 7 - page 11726, ligne 15 -----	1-15
X	EP 0 965 902 A2 (NAT SEMICONDUCTOR CORP [US]) 22 décembre 1999 (1999-12-22) alinéa [0010] - alinéa [0019] alinéa [0052] - alinéa [0062] alinéa [0073] - alinéa [0074] alinéa [0083] - alinéa [0087] alinéa [0112] - alinéa [0115] alinéa [0126] - alinéa [0136] revendications 1,4,6,8,9,10 figures 1,9,14a,14b,20a,20b -----	1-15
X	FR 2 871 905 A1 (INNOVA CARD SARL [FR]) 23 décembre 2005 (2005-12-23)	1,5-15
A	page 3, ligne 10 - page 3, ligne 30 revendications 1,6 figure 1 -----	2-4

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°

PCT/EP2019/067471

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2017017943	A1	19-01-2017	CN 106355096 A	25-01-2017
			US 2017017943 A1	19-01-2017

EP 0965902	A2	22-12-1999	DE 69519662 D1	25-01-2001
			DE 69519662 T2	23-05-2001
			EP 0715733 A1	12-06-1996
			EP 0965902 A2	22-12-1999
			KR 960705284 A	09-10-1996
			US 5533123 A	02-07-1996
			WO 9600953 A2	11-01-1996

FR 2871905	A1	23-12-2005	FR 2871905 A1	23-12-2005
			WO 2006008382 A1	26-01-2006
