(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 989 547**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **12 53381**

(51) Int Cl[8] : ***H 04 L 9/32*** *(2013.01)*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 12.04.12.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 18.10.13 Bulletin 13/42.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *THIBAUDEAU EMMANUEL* — FR.

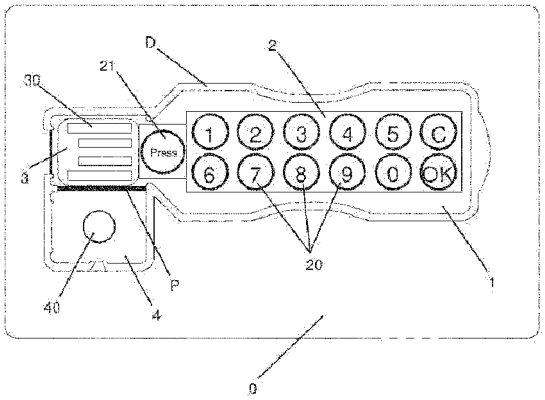
(72) **Inventeur(s) :** THIBAUDEAU EMMANUEL.

(73) **Titulaire(s) :** THIBAUDEAU EMMANUEL.

(74) **Mandataire(s) :** CABINET YVES DEBAY.

(54) SYSTEME DE SECURISATION DES TRANSACTIONS, PROCEDE DE MISE EN OEUVRE ET SERVEUR D'AUTHENTIFICATION DUDIT SYSTEME.

(57) L'invention concerne un système de sécurisation des transactions formant un objet portable caractérisé en ce qu'il est de type USB, le système comprenant au moins un microcontrôleur, un espace mémoire sécurisé non volatile et des moyens de connexions de type USB, le système étant connectable pour être rendu opérationnel dans un port USB sans ajout de matériel de lecture spécifique et assimilable à une interface homme/machine, le système comprenant en outre un clavier numérique intégré et électriquement relié au microcontrôleur de l'objet portable, alimenté via la connexion de type USB réalisée avec un terminal relié à un réseau étendu, le système étant adapté pour générer un message d'authentification envoyé à un serveur d'authentification relié au réseau étendu, permettant audit serveur d'identifier un système de sécurisation des transactions associé à un utilisateur et d'autoriser ou non la transaction.



FR 2 989 547 - A1

Système de sécurisation des transactions, procédé de mise en œuvre et serveur d'authentification dudit système

DOMAINE TECHNIQUE DE L'INVENTION

La présente invention se rapporte au domaine de la sécurisation des transactions en ligne, par exemple bancaires. Plus précisément, l'invention se rapporte à un système associé à une unique carte de transactions, et offrant la possibilité de chiffrer des données sensibles utiles à la sécurisation des transactions en ligne.

ARRIERE-PLAN TECHNOLOGIQUE DE L'INVENTION

De façon connue en soi, de nombreuses sociétés proposent de réaliser des transactions bancaires de manière virtuelle par le biais d'un réseau étendu type internet. Pour l'utilisateur souhaitant réaliser un paiement par carte bancaire sur un terminal de paiement électronique virtuel (ou TPE virtuel), il est proposé par le serveur de la société commerçante une connexion vers une page de paiement hébergée par le serveur de la banque gestionnaire des transactions. L'utilisateur est alors invité à saisir ses coordonnées bancaires et envoie ces informations, chiffrées au préalable par un algorithme de chiffrement ou condensées par une fonction de hachage. L'organisme bancaire vérifie en ligne les coordonnées bancaires saisies, et autorise la transaction le cas échéant.

Cependant, ce type de transaction présente plusieurs inconvénients, notamment l'absence de saisie d'un code d'identification et/ou d'informations chiffrées supplémentaires qui sécuriseraient davantage la transaction. En effet, il est devenu notoire que les transactions bancaires réalisées via des TPE virtuels sont beaucoup plus sensibles à la fraude que les transactions effectuées à l'aide d'un terminal de paiement électronique physique. A titre d'exemple, l'UFC-Que choisir affirme qu'en 2010 le taux de fraude avoisine les 0.276 % lors des transactions sur internet, ce qui est 23 fois plus élevé que le taux de fraude observé pour les transactions réalisées à l'aide d'un terminal de paiement électronique physique. De plus, le nombre de cartes bancaires en

circulation progressant régulièrement, la recherche de modèles de paiement en ligne au moins aussi sécurisés que les modèles de paiement physique est primordiale.

Il est également connu que certains organismes bancaires associent le numéro de carte avec le numéro de téléphone mobile de l'utilisateur, et utilise ce numéro pour envoyer par le réseau de téléphonie mobile un message texte (SMS, de l'anglais Short Message Service) contenant un code qui s'affiche sur le téléphone. Si l'utilisateur de la carte remplit la case code du formulaire avec celui reçu par SMS sur le téléphone mobile, alors la banque autorise la transaction car l'utilisateur est authentifié.

Toutefois, le réseau de téléphonie mobile ne permet pas de recevoir des SMS partout. Il demeure dans tous les pays des zones géographiques non desservies par le réseau de téléphonie mobile et où ce mode de sécurisation des transactions ne peut être mis en œuvre. D'autre part, la batterie du téléphone portable peut être déchargée, empêchant le fonctionnement du téléphone mobile ce qui au final fait échouer la transaction.

DESCRIPTION GENERALE DE L'INVENTION

Le problème technique est donc de permettre de sécuriser les transactions quelque soit le lieu en utilisant de préférence le réseau commuté là où le réseau sans fil n'est pas disponible, ou de permettre la transaction en ligne même si on ne dispose pas d'un téléphone mobile. La présente invention a donc pour objet de pallier un ou plusieurs des inconvénients de l'art antérieur, en proposant un organe informatique simple d'utilisation, pouvant jouer le rôle de système physique de sécurisation des transactions en ligne.

A cet effet, l'invention concerne un système de sécurisation des transactions formant un objet portable caractérisé en ce qu'il est de type USB, le système comprenant au moins un microcontrôleur, un espace mémoire sécurisé non volatile et des moyens de connexions de type USB, le système étant connectable pour être rendu opérationnel dans un port USB sans ajout de matériel de lecture spécifique et assimilable à une interface homme/machine, le système comprenant en outre un clavier numérique intégré et électriquement

relié au microcontrôleur de l'objet portable, alimenté via la connexion de type USB réalisée avec un terminal relié à un réseau étendu, le système étant adapté pour générer un message d'authentification envoyé à un serveur d'authentification relié au réseau étendu, permettant audit serveur d'identifier un système de sécurisation des transactions associé à un utilisateur et d'autoriser ou non la transaction.

le système de sécurisation des transactions est caractérisé en ce que les informations saisies par l'utilisateur sur le clavier sous forme d'un code utilisateur et transmises au microcontrôleur de l'objet portable sont chiffrées par ledit microcontrôleur au moyen d'un algorithme et d'une clef de chiffrement enregistrés dans l'espace mémoire, un identifiant caractérisant le système étant enregistré dans ladite mémoire, les informations saisies puis chiffrées par le microcontrôleur de l'objet portable autorisant l'envoi de l'identifiant du système avec un code secret chiffré enregistré dans l'espace mémoire du système à un serveur d'authentification relié au réseau étendu, autorisant ou non la poursuite de la transaction auprès d'un serveur de transactions.

Selon une autre particularité, le système de sécurisation des transactions est caractérisé en ce que le code utilisateur saisi est chiffré par le microcontrôleur du système et comparé avec le code confidentiel chiffré dans la mémoire dudit système, suivi du chiffrement de l'identifiant du système par le microcontrôleur dudit système, l'identifiant chiffré étant envoyé avec le nom de l'utilisateur à un serveur d'authentification relié au réseau étendu, autorisant ou non la poursuite de la transaction.

Selon une autre particularité, le système de sécurisation des transactions est caractérisé en ce que le code saisi par l'utilisateur sur le clavier intégré est comparé au code confidentiel enregistré dans l'espace mémoire par le microcontrôleur, ce code confidentiel n'étant jamais transmis au terminal, au serveur d'authentification ou au serveur de transaction.

Selon une autre particularité, le système de sécurisation des transactions est caractérisé en ce que le système est une partie détachable d'une carte dont les dimensions sont compatibles avec la norme ISO 7816.

Selon une autre particularité, le système de sécurisation des transactions est caractérisé en ce que la clef de chiffrement enregistrée dans une zone mémoire du système n'est jamais transmise au serveur d'authentification ou à un serveur de transactions via le réseau étendu.

Selon une autre particularité, le système de sécurisation des transactions est caractérisé en ce que les clefs de chiffrement peuvent être symétriques ou asymétriques.

Selon une autre particularité, le système de sécurisation des transactions est caractérisé en ce qu'une fonction de hachage permettant de créer un condensat de l'identifiant du système de sécurisation des transactions, est comprise dans la mémoire du système et mise en œuvre par au moins un microcontrôleur.

Selon une autre particularité, le système de sécurisation des transactions est caractérisé en ce qu'il comprend deux microcontrôleurs, le premier étant alimenté par un port de type USB par le biais duquel le système de sécurisation est connecté à un terminal, ledit premier microcontrôleur alimentant le deuxième microcontrôleur réalisant l'opération de chiffrement des données.

Selon une autre particularité, le système de sécurisation des transactions est caractérisé en ce qu'une fois connecté à un terminal via une interface de type USB, le système est assimilable à une interface homme/machine type clavier de saisie

Un objectif supplémentaire de l'invention est de proposer un procédé de sécurisation des transactions. Le procédé mis en œuvre par le système de sécurisation des transactions est caractérisé en ce qu'il comprend :

a. une étape d'envoi au serveur d'authentification, suite à l'établissement d'une connexion sécurisée, de l'identifiant de la

carte de transactions de l'utilisateur, saisi depuis un terminal relié au réseau étendu,

b. une étape d'envoi, depuis le serveur d'authentification, d'une requête de saisie d'un code confidentiel caractérisant le système de sécurisation des transactions associé à la carte de transactions de l'utilisateur, vers le terminal sur lequel est connecté le système de sécurisation,

c. une étape de saisie du code confidentiel à l'aide du clavier intégré au système de sécurisation,

d. une étape de comparaison par le microcontrôleur du système de sécurisation des transactions du code confidentiel saisi par l'utilisateur avec le code confidentiel enregistré dans l'espace mémoire,

e. une étape de chiffrement de l'identifiant et d'un code secret, enregistré dans l'espace mémoire, par le microcontrôleur du système de sécurisation des transactions, via un algorithme de chiffrement et une clef de chiffrement,

f. une étape d'envoi des informations chiffrées depuis le terminal vers le serveur d'authentification, ces informations chiffrées contenant au moins l'identifiant du système de sécurisation, ainsi que le code secret,

g. une étape de déchiffrage du code secret et de l'identifiant chiffré par les moyens de traitement du serveur d'authentification, un algorithme de déchiffrement associé à une clef étant enregistrés dans un espace mémoire du serveur d'authentification,

h. une étape de comparaison, par les moyens de traitement des donnés du serveur d'authentification, du code secret et de l'identifiant du système de sécurisation enregistrés dans une zone mémoire du serveur, avec le code secret et l'identifiant du système de sécurisation reçu à l'étape f et déchiffré à l'étape g,

i. une étape d'envoi de l'autorisation de transaction depuis le serveur d'authentification vers le serveur de transactions.

Selon une autre particularité, le procédé de sécurisation est caractérisé en ce qu'il comprend :

a. une étape d'envoi au serveur d'authentification, suite à l'établissement d'une connexion sécurisée, de l'identifiant de la carte de transactions de l'utilisateur, saisi depuis un terminal relié au réseau étendu,

b. une étape d'envoi, depuis le serveur d'authentification, d'une requête de saisie d'un code confidentiel caractérisant le système de sécurisation des transactions associé à la carte de transactions de l'utilisateur, vers le terminal sur lequel est connecté le système de sécurisation,

c. une étape de saisie du code utilisateur à l'aide du clavier intégré au système de sécurisation,

d. une étape de chiffrement par le microcontrôleur du système de sécurisation du code d'utilisateur, et du code confidentiel enregistré dans la mémoire du système de sécurisation via un algorithme de chiffrement et une clef de chiffrement, le code utilisateur chiffré étant affiché en parallèle sur les moyens d'affichage du terminal relié au réseau étendu,

e. une étape de comparaison par le microcontrôleur du système des codes utilisateur et confidentiel chiffrés,

f. une étape de chiffrement de l'identifiant du système de sécurisation des transactions par le microcontrôleur dudit système,

g. une étape d'envoi des informations chiffrées depuis le terminal vers le serveur d'authentification, ces informations chiffrées

contenant au moins l'identifiant du système de sécurisation, ainsi que le nom de l'utilisateur,

h. étape de déchiffrage de l'identifiant chiffré par les moyens de traitement du serveur d'authentification, un algorithme de déchiffrement associé à une clef étant enregistrés dans un espace mémoire du serveur d'authentification,

i. une étape de comparaison, par les moyens de traitement des donnés du serveur d'authentification, de l'identifiant du système de sécurisation associé au nom de l'utilisateur enregistrés dans une zone mémoire du serveur, avec le nom de l'utilisateur et l'identifiant du système de sécurisation reçus à l'étape g et déchiffré à l'étape h,

j. une étape d'envoi de l'autorisation de transaction depuis le serveur d'authentification vers le serveur de transactions.

Selon une autre particularité, le procédé de sécurisation est caractérisé en ce qu'il comprend une étape de hachage de l'identifiant du système de sécurisation des transactions, ladite étape étant située avant l'étape de chiffrement de l'identifiant du système.

Selon une autre particularité, le procédé de sécurisation est caractérisé en ce que le serveur d'authentification envoie une information aléatoire à destination du système de sécurisation, ladite information faisant partie des données chiffrées par le microcontrôleur du système de sécurisation et envoyées au serveur d'authentification.

Selon une autre particularité, le procédé de sécurisation est caractérisé en ce que le serveur de transactions envoie une information aléatoire à destination du système de sécurisation et du serveur d'authentification, ladite information faisant partie des données chiffrées par le microcontrôleur du système de sécurisation et envoyées au serveur d'authentification.

Selon une autre particularité, le procédé de sécurisation est caractérisé en ce que l'algorithme de déchiffrement et la clef associée sont enregistrés

dans une zone mémoire du serveur d'authentification et du serveur de transactions.

Selon une autre particularité, le procédé de sécurisation est caractérisé en ce que les clefs de chiffrement peuvent être symétriques ou asymétriques.

Selon une autre particularité, le procédé de sécurisation est caractérisé en ce que la connexion sécurisé réalisée entre le terminal et le serveur d'authentification est chiffrée à l'aide d'un protocole de type SSL ou TLS.

Un objectif supplémentaire de l'invention est de proposer un serveur d'authentification d'un système de sécurisation des transactions. Le serveur d'authentification comprend des moyens de traitement des données, au moins un espace mémoire, des moyens de connexion à un réseau étendu, et est caractérisé en ce qu'il comprend en outre :

- au moins une base de données comprenant les identifiants, au moins une clef permettant de retrouver la clef de chiffrement de chaque système de sécurisation des transactions et un code secret de chaque système de sécurisation des transactions,

- au moins une base de données comprenant les identifiants, au moins une clef permettant de retrouver la clef de chiffrement de chaque système de sécurisation et un code confidentiel de chaque système de sécurisation des transactions,

- un algorithme de déchiffrement inverse de celui enregistré dans la mémoire du système de sécurisation des transactions, pour déchiffrer les données reçues grâce à une clef de chiffrement, et comparant le résultat du déchiffrement soit à l'identifiant, soit au code secret pour réaliser l'authentification en cas de coïncidence avec au moins un des deux,

le serveur d'authentification étant connecté d'une part à un terminal d'un utilisateur réalisant une transaction en ligne à l'aide de sa carte de transactions et du système de sécurisation associé, et d'autre part au serveur de transactions correspondant, le serveur d'authentification la transaction auprès du serveur de transactions une fois l'authentification combinée des identifiants de la carte de transactions et du système de sécurisation réalisée.

Selon une autre particularité, le serveur d'authentification d'un système de sécurisation des transactions est caractérisé en ce qu'il envoie au terminal de l'utilisateur via les moyens de connexion au réseau étendu, un nombre généré aléatoirement utilisé dans le chiffrement de l'identifiant et du code secret du système de sécurisation des transactions relié au terminal de l'utilisateur.

L'invention, avec ses caractéristiques et avantages, ressortira plus clairement à la lecture de la description faite en référence aux dessins annexés dans lesquels :

La figure 1a illustre l'invention dans un mode de réalisation préférentiel.

La figure 1b illustre le recto de la partie comprenant les moyens de connexion USB et le microcontrôleur.

La figure 1c illustre le verso de la partie comprenant les moyens de connexion USB et le microcontrôleur.

La figure 2 illustre un schéma de réalisation d'une transaction utilisant l'invention, le terminal utilisateur, le serveur d'authentification et le serveur de transactions.

DESCRIPTION DES MODES DE REALISATION PREFERES DE L'INVENTION

En référence aux figures 1a à 1c, le système de sécurisation des transactions (1) va maintenant être décrit. Dans certains modes de réalisation, le système de sécurisation des transactions (1) est compris dans une carte (0) comprenant un corps en matériau synthétique classique, par exemple en ABS (Acrylonitrile Butadiène Styrène) ou en PVC (Polychlorure de Vinyle). Selon une

variante de réalisation, le corps de la carte (0) peut être réalisé en matière biodégradable. La carte (0) comprend une partie détachable prédécoupée destinée à former un objet informatique (1), cet objet étant dans des modes de réalisation le système de sécurisation des transactions (1).

La partie détachable de la carte (0) est délimitée par un évidemment linéaire (D), et est accrochée au reste du corps de la carte grâce à des moyens de liaison frangible interrompant donc l'évidemment linéaire.

Dans certains modes de réalisation, l'objet informatique (1) comprend des moyens matérialisant une ligne de pliage (P). Dans l'exemple représenté à la figure 1a, la ligne de pliage (P) est matérialisée par un amincissement localisé du corps de la carte (0). Cet amincissement pourra, par exemple et de façon non restrictive, être réalisé par poinçonnage, par fraisage, par découpe laser ou tout autre moyen d'usinage.

On notera que la ligne de pliage (P) sépare deux zones appelées respectivement dormant (3) et abattant (4).

Après découpage de l'objet informatique (1) et pliage par rabattement de l'abattant (3) sur le dormant (4), l'abattant et le dormant étant solidarisés grâce à des moyens d'encliquetage (40), la partie présente sous le connecteur a maintenant une épaisseur compatible avec les dimensions d'un connecteur USB femelle. Dans cette configuration, le système de sécurisation des transactions (1) peut être connecté à un hôte informatique, par exemple et de façon non limitative un terminal (5) d'un utilisateur.

Dans un mode de réalisation préférentiel, la carte (0) est réalisée dans des dimensions respectant le format de la norme ISO 7816, notamment la norme ISO 7816-1 relative aux caractéristiques physiques de cartes à puce.

Le système de sécurisation des transactions (1) comprend notamment un dispositif électronique (31) solidarisé au corps de l'objet informatique (1) par exemple à l'aide d'un adhésif classique pendant une étape d'intégration du dispositif électronique. Le dispositif électronique (31) comprend des moyens de connexion (30) de type bus informatique à transmission série. Dans certains

modes de réalisation, le dispositif électronique (31) est une puce électronique reliée électriquement selon la norme USB (de l'anglais, Universal Serial Bus) à une vignette à plages de contact électriquement disjointes, fabriqué selon un procédé connu de l'homme du métier : la puce électronique (31) est placé sous la vignettes à plages de contact, puis les contacts électriques de la puce sont ensuite reliés aux plages de contact de ladite vignette.

La puce électronique (31) peut comprendre, par exemple et de façon non limitative, au moins un microcontrôleur, comme par exemple et de façon non limitative un microprocesseur comprenant une mémoire volatile, un contrôleur USB, un ou plusieurs espaces mémoires, par exemple des mémoires sécurisées non volatiles intégrées ou non dans le microcontrôleur. Contrairement au cas des puces réalisées selon la norme ISO 7816, les signaux d'horloge, des périphériques de type USB, ne sont pas transmis par le connecteur USB, la puce (31) comportera donc son circuit d'horloge intégré ou non dans un microcontrôleur. Ce circuit d'horloge pourra, par exemple et de façon non restrictive, comporter un résonateur ou un quartz.

Dans un mode de réalisation, les plages de contact (30) sont réalisées par une vignette à huit contacts. Contrairement aux vignettes au format ISO 7816 classiquement utilisées sur une carte à puce, les plages de contact (30) correspondant aux contacts ISO C1 à C4 ont été rallongées de façon à faire correspondre les dimensions des plages de contact (30) de la vignette avec ceux d'un connecteur USB tout en respectant la norme 7816-2 relative aux dimensions et emplacement des contacts. Pour cela, la longueur des plages de contact (30) correspondant aux contacts ISO C5 à C8 a été raccourcie. Un connecteur USB ne comprenant que quatre pistes, les plages de contact (30) correspondant aux contacts ISO C5 à C8 ne seront donc pas utilisées. Suivant un premier mode de réalisation, ces plages de contact (30) seront chacune isolées entre elles mais ne seront pas câblées au microcircuit. Suivant un autre mode de réalisation, les plages de contact correspondant aux contacts ISO C5 à C8 pourront être isolées des contacts ISO C2 à C4 mais ne seront pas isolées entre elles et seront reliées au contact ISO C1 de façon à ne former qu'une seule plage de contact.

Ainsi, le système de sécurisation des transactions (1) forme un organe informatique connectable selon la norme USB, un microcontrôleur de la puce électronique (31) étant programmé par des moyens de programmation de telle sorte que ledit organe informatique (1) se comporte comme une interface homme/machine une fois connecté, par exemple à un terminal (5). En effet, au moins un espace mémoire intégré dans la puce électronique (31) comprend au moins un identifiant destiné à identifier l'organe informatique (1) de type USB connecté comme étant une interface homme/machine. Dans des modes de réalisation préférentiels, l'organe informatique (1) est reconnu, par le terminal (5) auquel il est connecté, comme étant un clavier.

Dans certains modes de réalisation, la puce (31) comprise dans le système de sécurisation des transactions (1) est programmée de manière à stocker dans l'espace mémoire de la puce des informations caractéristiques du système de sécurisation des transactions (1), par exemple et de façon non limitative un identifiant unique du système permettant d'identifier l'utilisateur, un code confidentiel ne devant jamais être transmis à un quelconque système informatique, par exemple et de façon non limitative un serveur ou un terminal utilisateur, auquel le système de sécurisation des transactions est relié et/ou connecté, un code secret différent du code confidentiel et servant par exemple été de façon non restrictive à l'authentification du système de sécurisation des transactions (1) auprès d'un terminal utilisateur (5) et/ou d'un serveur distant, au moins un programme de fonctionnement du ou des microcontrôleur(s). Dans certains modes de réalisation, un microcontrôleur du système de sécurisation des transactions (1) fonctionne selon un algorithme de chiffrement enregistré en mémoire, une clef de chiffrement étant également enregistrée en mémoire. Le microcontrôleur exécutant un tel algorithme permet par exemple et de façon non limitative de chiffrer les informations enregistrées dans l'espace mémoire du système de sécurisation (1). Ainsi, un système de sécurisation des transactions (1) connecté à un terminal (5) relié à un réseau étendu (en anglais, wide area network ou WAN) est en mesure de générer un message chiffré par le microcontrôleur alimenté via la connexion de type USB, et de l'envoyer

depuis le terminal (5) de l'utilisateur vers un serveur d'authentification (SA) relié au réseau étendu, ce message chiffré permettant audit serveur d'authentification (SA) d'identifier le système de sécurisation des transactions (1), et de l'associer à l'utilisateur. Suivant le résultat, le serveur d'authentification (SA) autorise ou non la transaction, initiée par l'utilisateur, par exemple avec un serveur de transactions (ST) connecté au réseau étendu. On appelle réseau étendu un réseau couvrant une large zone géographique. Par exemple et de façon non limitative, le réseau téléphonique commuté, les réseaux GSM, 2G, 3G et/ou 4G sont des réseaux étendus. Dans certains modes de réalisation, le système de sécurisation des transactions (1) comprend deux microcontrôleurs, le premier étant alimenté par le port de type USB par le biais duquel le système de sécurisation (1) est connecté à un terminal (5), ledit premier microcontrôleur alimentant le deuxième microcontrôleur réalisant l'opération de chiffrement des données.

Dans certains modes de réalisation, le serveur d'authentification (SA) comprend des moyens de traitement des données, au moins un espace mémoire, des moyens de connexion à un réseau étendu, au moins une base de données comprenant les identifiants, au moins une clef permettant de retrouver la clef de chiffrement de chaque système de sécurisation (1) et un code secret de chaque système de sécurisation des transactions (1), au moins une base de données comprenant les noms d'utilisateur associés à chaque système de sécurisation des transactions (1), et un algorithme de déchiffrement inverse de celui enregistré dans la mémoire du système de sécurisation des transactions (1), pour déchiffrer les données reçues grâce à une clef de chiffrement, et comparant le résultat du déchiffrement soit à l'identifiant, soit au code secret pour réaliser l'authentification en cas de coïncidence avec au moins un des deux.

Le serveur d'authentification (SA) est connecté d'une part à un terminal (5) d'un utilisateur réalisant une transaction en ligne à l'aide de sa carte de transactions et du système de sécurisation (1) associé, et d'autre part au serveur de transactions (ST) correspondant, le serveur d'authentification (SA)

autorisant la transaction auprès du serveur de transactions (ST) une fois l'authentification combinée des identifiants de la carte de transactions et du système de sécurisation (1) réalisée.

Dans certains modes de réalisation, la clef de chiffrement présente en mémoire est une clef symétrique. Ainsi, seul un algorithme de déchiffrement utilisant cette même clef sera en mesure de déchiffrer les données chiffrées par le microcontrôleur du système de sécurisation des transactions (1).

Dans d'autres modes de réalisation, la clef de chiffrement présente en mémoire est une clef asymétrique. Ainsi, les données présentes dans la mémoire du système de sécurisation (1) et chiffrées par le microcontrôleur à l'aide d'une première clef, pourront être déchiffrées à l'aide d'un algorithme utilisant une clef complémentaire. Ces mécanismes de chiffrement symétriques et asymétriques sont bien connus de l'homme du métier.

Dans certains modes de réalisation, toutes ces clefs de chiffrement sont présentes dans l'espace mémoire du système de sécurisation des transactions (ST), ainsi que dans l'espace mémoire des serveurs d'authentification (SA) et de transactions (ST), mais elles ne sont jamais transmises, pour des raisons de sécurité, via le réseau étendu.

Dans certains modes de réalisation, une fonction de hachage et sa clef de chiffrement sont enregistrées dans un espace mémoire du système de sécurisation des transactions (1). Ce type de fonctions, bien connu de l'homme du métier, permet de réaliser une empreinte, ou condensat, de l'identifiant du système de sécurisation des transactions (1). Cette fonction permet notamment de renforcer le processus d'authentification.

Suivant un exemple de réalisation, nullement restrictif, la puce (31) de la carte n'est programmable qu'une seule fois et ne peut pas être reprogrammée. Une fois les données entrées (identifiants, programme de fonctionnement du microcontrôleur...) celles-ci ne pourront plus être modifiées. De même, il n'est pas possible de rajouter des informations après programmation complète de la puce (31).

Suivant un autre mode de réalisation, la puce (31) est reprogrammable. Ainsi, certaines informations présentes dans l'espace mémoire du système (1) pourront être reprogrammées, par exemple et de façon non limitative le code confidentiel enregistré en mémoire.

De façon préférentielle, la programmation des objets portables est réalisée avec les mêmes outils de fabrication et de programmation utilisés dans le domaine de la carte à puce classique, comme par exemple et de façon non limitative, celui des cartes bancaires. Afin de pouvoir être programmée dans de telles machines, les objets portables (1) sont dotés d'un connecteur formé par une vignette, selon la norme ISO 7816.

Dans certains modes de réalisation, le système de sécurisation des transactions (1) comprend un clavier numérique intégré (2), électriquement relié au microcontrôleur du système de sécurisation des transactions. Par exemple et de façon non limitative, ce clavier (2) comporte treize touches (20) : une pour chaque chiffre de zéro à neuf, une touche (20) permettant d'effacer au moins un caractère que l'utilisateur vient de taper, par exemple en cas d'erreur, une touche de validation, et une touche supplémentaire (21) dont la fonction peut être programmée. Ce clavier numérique (2) permet donc à l'utilisateur de taper un code utilisateur nécessaire à l'authentification du système de sécurisation des transactions (1). Le clavier étant relié au microcontrôleur, les données saisies par l'utilisateur sont chiffrées dans certains modes de réalisation, par ledit microcontrôleur, par exemple et de façon non limitative via un algorithme de chiffrement.

En référence à la figure 2, le procédé de sécurisation des transactions mis en œuvre par le système de sécurisation des transactions (1) va maintenant être décrit.

Dans certains modes de réalisation non restrictifs, lorsque l'utilisateur réalise une transaction à l'aide de sa carte de transactions, par exemple et de façon non limitative une carte bancaire, ce dernier connecte au préalable son système de sécurisation des transactions (1) personnel, le système (1) étant

associé à l'utilisateur d'une carte de transactions. Dans une première étape, l'utilisateur saisie depuis le terminal (5), grâce à des moyens de saisie relié audit terminal (50), l'identifiant de la carte de transactions vers le serveur d'authentification (SA), par le biais d'une page chiffrée par exemple et de façon non limitative suivant le protocole SSL ou TSL. Dans une deuxième étape, le serveur d'authentification (SA) ayant reçu l'identifiant de la carte de transaction grâce au réseau étendu, envoie vers le terminal (5) de l'utilisateur une requête de saisie d'un code confidentiel caractérisant le système de sécurisation (1) associé à l'utilisateur. Dans une troisième étape, l'utilisateur saisie son code confidentiel sur le clavier intégré (2) au système de sécurisation des transactions (1). Au cours de la quatrième étape, et simultanément à la saisie du code par l'utilisateur, le microcontrôleur du système de sécurisation des transactions (1) réalise la comparaison du code confidentiel saisi par l'utilisateur avec le code confidentiel enregistré dans un espace mémoire du dispositif de sécurisation des transactions (1). Il est important de noté que ce code confidentiel enregistré dans l'espace mémoire n'est jamais transmis à un quelconque système informatique connecté et/ou relié au système de sécurisation des transactions (1), par exemple le terminal utilisateur (5), le serveur d'authentification (SA) ou le serveur de transactions (ST). Une fois la comparaison entre le code confidentiel enregistré en mémoire et le code confidentiel saisi réalisée au sein du microcontrôleur, toute trace de ce code confidentiel est effacée de la mémoire volatile dudit microcontrôleur. Ainsi, il est impossible que ce code confidentiel soit intercepté : le système de sécurisation des transactions (1) est inviolable et reste impossible à utiliser sans saisie manuelle du code confidentiel. Dans certains modes de réalisation, des caractères spéciaux sont affichées (52) sur les moyens d'affichage (51) du terminal (5) à mesure que l'utilisateur tape les caractères du code confidentiel via le clavier intégré (2) au système de sécurisation des transactions (1). Cet affichage (52) permet, par exemple et de façon non limitative, à l'utilisateur de s'assurer qu'il a bien tapé le nombre correct de caractères du code confidentiel Au cours de la cinquième étape, le microcontrôleur réalise le chiffrement de l'identifiant et d'un code secret enregistré dans un espace mémoire et différent

du code confidentiel saisi par l'utilisateur sur le clavier intégré (2), par le biais d'un algorithme de chiffrement associé à une clef de chiffrement. Au cours de la sixième étape, les informations contenant le code secret et l'identifiant chiffrés du système de sécurisation des transactions (1) sont transmises au terminal (5) via la connexion USB, puis envoyées grâce au réseau étendu du terminal (5) de l'utilisateur vers le serveur d'authentification (SA). Dans une septième étape, le programme de traitement du serveur d'authentification (SA) déchiffre, via un algorithme de déchiffrement et la clef associée, les informations chiffrées reçues du terminal (5) de l'utilisateur. Au cours de la huitième étape, les moyens de traitement du serveur d'authentification (SA) comparent le code secret et l'identifiant déchiffrés du système de sécurisation des transactions (1), avec le code secret et l'identifiant du système de sécurisation (1) enregistrés dans une zone mémoire du serveur d'authentification (SA). Si le résultat de la comparaison renvoie des résultats identiques, alors le serveur d'authentification (SA) autorise la poursuite de la transaction, par exemple au niveau du serveur de transactions (ST). Dans certains modes de réalisation, les algorithmes de déchiffrement et les clefs associées sont enregistrées dans un espace mémoire du serveur de transactions (ST).

Dans des modes de réalisation alternatifs, une étape de hachage de l'identifiant du système de sécurisation des transactions (1) est réalisée avant la quatrième étape par un microcontrôleur du système de sécurisation des transactions (1), et ce afin de créer une empreinte ou un condensat de l'identifiant du système de sécurisation des transactions (1). Afin de déchiffrer ce condensat, le serveur d'authentification (SA) comprend dans une zone mémoire la même fonction de hachage ayant servi à la création du condensat, et la clef permettant le déchiffrage.

Dans des modes de réalisation alternatifs, un nombre aléatoire est d'une part envoyé par les moyens de traitement du serveur d'authentification (SA) vers le système de sécurisation des transactions (1) par le biais du réseau étendu et du terminal (5) de l'utilisateur, et d'autre part enregistré dans la mémoire du serveur d'authentification (SA). Ce nombre aléatoire est chiffré par

le microcontrôleur du système de sécurisation en même temps que le code secret et l'identifiant du système de sécurisation des transactions (1), via l'algorithme de chiffrement. Ainsi, le système de sécurisation des transactions (1) renvoie ces données chiffrées au serveur d'authentification (SA), qui seront déchiffrées par les moyens de traitement dudit serveur (SA). Les moyens de traitement du serveur d'authentification (SA) comparent le code secret, le nombre aléatoire et l'identifiant déchiffrés du système de sécurisation des transactions (1), avec le code secret, le nombre aléatoire et l'identifiant du système de sécurisation (1) enregistrés dans une zone mémoire du serveur d'authentification (SA). Si le résultat de la comparaison renvoie des résultats identiques, alors le serveur d'authentification (SA) autorise la poursuite de la transaction par exemple au niveau du serveur de transactions (ST). Cette méthode de chiffrement, bien connu de l'homme du métier, renforce la confidentialité des données chiffrées.

Dans un mode de réalisation alternatif, c'est le serveur de transactions (ST) qui envoie au serveur d'authentification (SA) et au système de sécurisation des transactions (1), par le biais du réseau étendu et le cas échéant du terminal (5) de l'utilisateur, le nombre aléatoire qui sera enregistré dans l'espace mémoire de chaque serveur (SA, ST), et chiffré par le microcontrôleur du système de sécurisation (1) en même temps que le code secret et l'identifiant du système de sécurisation des transactions (1), via l'algorithme de chiffrement.

Dans certains modes de réalisation, le système de sécurisation des transactions (1) peut jouer le rôle d'un terminal de paiement électronique. Le procédé de sécurisation des transactions mis en œuvre par le système de sécurisation des transactions (1) s'en trouve légèrement modifié. Après les deux premières étapes du procédé, explicitées plus haut dans la description, l'utilisateur saisie son code confidentiel sur le clavier intégré (2) au système de sécurisation des transactions (1). Au cours de la quatrième étape, le microcontrôleur du système de sécurisation (1) chiffre d'une part le code confidentiel saisi par l'utilisateur, et d'autre part le code confidentiel enregistré dans une zone mémoire du système de sécurisation des transactions (1), via

l'algorithme de chiffrement. Au cours de la cinquième étape, le microcontrôleur du système de sécurisation des transactions (1) compare les deux codes chiffrés. Si les codes sont identiques, alors le microcontrôleur du système de sécurisation des transactions (1) réalise le chiffrement de l'identifiant et du nom de l'utilisateur, par le biais d'un algorithme de chiffrement associé à une clef de chiffrement. Au cours de la septième étape, les informations contenant le nom de l'utilisateur et l'identifiant chiffrés du système de sécurisation des transactions (1) sont transmises au terminal (5) via la connexion USB, puis envoyées grâce au réseau étendu du terminal (5) de l'utilisateur vers le serveur d'authentification (SA). Dans une huitième étape, le programme de traitement du serveur d'authentification (SA) déchiffre, via un algorithme de déchiffrement et la clef associée, les informations chiffrées reçues du terminal (5) de l'utilisateur. Au cours de la neuvième étape, les moyens de traitement du serveur d'authentification (SA) comparent le nom d'utilisateur et l'identifiant déchiffrés du système de sécurisation des transactions (1), avec le nom d'utilisateur et l'identifiant du système de sécurisation (1) enregistrés dans une zone mémoire du serveur d'authentification (SA). Si le résultat de la comparaison renvoie des résultats identiques, alors le serveur d'authentification (SA) autorise la poursuite de la transaction au niveau du serveur de transactions (ST).

De la même manière, dans certains modes de réalisation, un nombre aléatoire est d'une part envoyé par les moyens de traitement du serveur d'authentification (SA) vers le système de sécurisation des transactions (1) par le biais du réseau étendu et du terminal (5) de l'utilisateur, et d'autre part enregistré dans la mémoire du serveur d'authentification (SA), afin de renforcer la confidentialité des données chiffrées. Dans un mode de réalisation alternatif, c'est le serveur de transactions (ST) qui envoie au serveur d'authentification (SA) et au système de sécurisation des transactions (1), par le biais du réseau étendu et le cas échéant du terminal (5) de l'utilisateur, le nombre aléatoire qui sera enregistré dans l'espace mémoire de chaque serveur (SA, ST), et chiffré par le microcontrôleur du système de sécurisation (1) en même temps que le

code confidentiel et l'identifiant du système de sécurisation des transactions (1), via l'algorithme de chiffrement.

La présente demande décrit diverses caractéristiques techniques et avantages en référence aux figures et/ou à divers modes de réalisation. L'homme de métier comprendra que les caractéristiques techniques d'un mode de réalisation donné peuvent en fait être combinées avec des caractéristiques d'un autre mode de réalisation à moins que l'inverse ne soit explicitement mentionné ou qu'il ne soit évident que ces caractéristiques sont incompatibles. De plus, les caractéristiques techniques décrites dans un mode de réalisation donné peuvent être isolées des autres caractéristiques de ce mode à moins que l'inverse ne soit explicitement mentionné.

Il doit être évident pour les personnes versées dans l'art que la présente invention permet des modes de réalisation sous de nombreuses autres formes spécifiques sans l'éloigner du domaine d'application de l'invention comme revendiqué. Par conséquent, les présents modes de réalisation doivent être considérés à titre d'illustration, mais peuvent être modifiés dans le domaine défini par la portée des revendications jointes, et l'invention ne doit pas être limitée aux détails donnés ci-dessus.

REVENDICATIONS

1. Système de sécurisation des transactions formant un objet portable (1) caractérisé en ce qu'il est de type USB, le système comprenant au moins un microcontrôleur, un espace mémoire sécurisé non volatile et des moyens de connexions de type USB (30), le système étant connectable pour être rendu opérationnel dans un port USB sans ajout de matériel de lecture spécifique et assimilable à une interface homme/machine, le système comprenant en outre un clavier numérique (2) intégré et électriquement relié au microcontrôleur de l'objet portable (1), alimenté via la connexion de type USB réalisée avec un terminal (5) relié à un réseau étendu, le système étant adapté pour générer un message d'authentification envoyé à un serveur d'authentification (SA) relié au réseau étendu, permettant audit serveur d'identifier un système de sécurisation des transactions (1) associé à un utilisateur et d'autoriser ou non la transaction.

2. Système de sécurisation des transactions selon la revendication précédente, caractérisé en ce que les informations saisies par l'utilisateur sur le clavier (2) sous forme d'un code utilisateur et transmises au microcontrôleur de l'objet portable sont chiffrées par ledit microcontrôleur au moyen d'un algorithme et d'une clef de chiffrement enregistrés dans l'espace mémoire, un identifiant caractérisant le système étant enregistré dans ladite mémoire, les informations saisies puis chiffrées par le microcontrôleur de l'objet portable (1) autorisant l'envoi de l'identifiant du système avec un code secret chiffré enregistré dans l'espace mémoire du système (1) à un serveur d'authentification (SA) relié au réseau étendu, autorisant ou non la poursuite de la transaction auprès d'un serveur de transactions (ST).

3. Système de sécurisation des transactions selon la revendication 1, caractérisé en ce que le code utilisateur saisi est chiffré par le microcontrôleur du système (1) et comparé avec le code confidentiel chiffré dans la mémoire dudit système, suivi du chiffrement de l'identifiant du système par le microcontrôleur dudit système, l'identifiant chiffré étant envoyé avec le nom de

l'utilisateur à un serveur d'authentification (SA) relié au réseau étendu, autorisant ou non la poursuite de la transaction.

4. Système de sécurisation des transactions selon les revendications précédentes, caractérisé en ce que le code saisi par l'utilisateur sur le clavier intégré (2) est comparé au code confidentiel enregistré dans l'espace mémoire par le microcontrôleur, ce code confidentiel n'étant jamais être transmis au terminal (5), au serveur d'authentification (SA) ou au serveur de transaction (ST).

5. Système de sécurisation des transactions selon la revendication précédente, caractérisé en ce que le système (1) est une partie détachable d'une carte (0) dont les dimensions sont compatibles avec la norme ISO 7816.

6. Système de sécurisation des transactions selon une des revendications précédentes, caractérisé en ce que la clef de chiffrement enregistrée dans une zone mémoire du système (1) n'est jamais transmise au serveur d'authentification (SA) ou à un serveur de transactions (ST) via le réseau étendu.

7. Système de sécurisation des transactions selon une des revendications précédentes, caractérisé en ce que les clefs de chiffrement peuvent être symétriques ou asymétriques.

8. Système de sécurisation des transactions selon les revendications précédentes, caractérisé en ce qu'une fonction de hachage permettant de créer un condensat de l'identifiant du système de sécurisation des transactions (1), est comprise dans la mémoire du système et mise en œuvre par au moins un microcontrôleur.

9. Système de sécurisation des transactions selon les revendications précédentes, caractérisé en ce qu'il comprend deux microcontrôleurs, le premier étant alimenté par un port de type USB par le biais duquel le système de sécurisation (1) est connecté à un terminal (5), ledit premier microcontrôleur alimentant le deuxième microcontrôleur réalisant l'opération de chiffrement des données.

10. Système de sécurisation des transactions selon la revendication 1, caractérisé en ce qu'une fois connecté à un terminal (5) via une interface de type USB, le système (1) est assimilable à une interface homme/machine type clavier de saisie.

11. Procédé de sécurisation des transactions mis en œuvre par le système de sécurisation selon la revendication 1, caractérisé en ce qu'il comprend :

a. Une étape d'envoi au serveur d'authentification (SA), suite à l'établissement d'une connexion sécurisée, de l'identifiant de la carte de transactions de l'utilisateur, saisi depuis un terminal (5) relié au réseau étendu,

b. Une étape d'envoi, depuis le serveur d'authentification (SA), d'une requête de saisie d'un code confidentiel caractérisant le système de sécurisation des transactions (1) associé à la carte de transactions de l'utilisateur, vers le terminal (5) sur lequel est connecté le système de sécurisation (1),

c. Une étape de saisie du code confidentiel à l'aide du clavier intégré (2) au système de sécurisation (1),

d. Une étape de comparaison par le microcontrôleur du système de sécurisation des transactions (1) du code confidentiel saisi par l'utilisateur avec le code confidentiel enregistré dans l'espace mémoire,

e. Une étape de chiffrement de l'identifiant et d'un code secret, enregistré dans l'espace mémoire, par le microcontrôleur du système de sécurisation des transactions (1), via un algorithme de chiffrement et une clef de chiffrement,

f. Une étape d'envoi des informations chiffrées depuis le terminal (5) vers le serveur d'authentification (SA), ces informations chiffrées contenant au moins l'identifiant du système de sécurisation (1), ainsi que le code secret,

g. Une étape de déchiffrage du code secret et de l'identifiant chiffré par les moyens de traitement du serveur d'authentification (SA), un algorithme de déchiffrement associé à une clef étant enregistrés dans un espace mémoire du serveur d'authentification (SA),

h. Une étape de comparaison, par les moyens de traitement des donnés du serveur d'authentification (SA), du code secret et de l'identifiant du système de sécurisation enregistrés dans une zone mémoire du serveur (SA), avec le code secret et l'identifiant du système de sécurisation reçu à l'étape f et déchiffré à l'étape g.

i. Une étape d'envoi de l'autorisation de transaction depuis le serveur d'authentification (SA) vers le serveur de transactions (ST).

12. Procédé de sécurisation selon la revendication précédente, caractérisé en ce qu'il comprend :

a. Une étape d'envoi au serveur d'authentification (SA), suite à l'établissement d'une connexion sécurisée, de l'identifiant de la carte de transactions de l'utilisateur, saisi depuis un terminal (5) relié au réseau étendu,

b. Une étape d'envoi, depuis le serveur d'authentification (SA), d'une requête de saisie d'un code confidentiel caractérisant le système de sécurisation des transactions (1) associé à la carte de transactions de l'utilisateur, vers le terminal (5) sur lequel est connecté le système de sécurisation (1),

c. Une étape de saisie du code utilisateur à l'aide du clavier intégré au système de sécurisation (1),

d. Une étape de chiffrement par le microcontrôleur du système de sécurisation (1) du code d'utilisateur, et du code confidentiel enregistré dans la mémoire du système de sécurisation (1) via un algorithme de chiffrement et une clef de chiffrement, le code utilisateur chiffré étant affiché en parallèle (52) sur les moyens d'affichage (51) du terminal (5) relié au réseau étendu,

e. Une étape de comparaison par le microcontrôleur du système (1) des codes utilisateur et confidentiel chiffrés,

f. Une étape de chiffrement de l'identifiant du système de sécurisation des transactions (1) par le microcontrôleur dudit système,

g. Une étape d'envoi des informations chiffrées depuis le terminal (5) vers le serveur d'authentification (SA), ces informations chiffrées contenant au moins l'identifiant du système de sécurisation (1), ainsi que le nom de l'utilisateur,

h. Une étape de déchiffrage de l'identifiant chiffré par les moyens de traitement du serveur d'authentification (SA), un algorithme de déchiffrement associé à une clef étant enregistrés dans un espace mémoire du serveur d'authentification (SA),

i. Une étape de comparaison, par les moyens de traitement des donnés du serveur d'authentification (SA), de l'identifiant du système de sécurisation (1) associé au nom de l'utilisateur enregistrés dans une zone mémoire du serveur (SA), avec le nom de l'utilisateur et l'identifiant du système de sécurisation (1) reçus à l'étape g et déchiffré à l'étape h,

j. Une étape d'envoi de l'autorisation de transaction depuis le serveur d'authentification (SA) vers le serveur de transactions (ST).

13. Procédé de sécurisation selon la revendication 11 ou 12, caractérisé en ce qu'il comprend une étape de hachage de l'identifiant du système de sécurisation des transactions (1), ladite étape étant située avant l'étape de chiffrement de l'identifiant du système.

14. Procédé de sécurisation selon les revendications 11 à 13, caractérisé en ce que le serveur d'authentification (SA) envoie une information aléatoire à destination du système de sécurisation (1), ladite information faisant partie des données chiffrées par le microcontrôleur du système de sécurisation (1) et envoyées au serveur d'authentification (SA).

15. Procédé de sécurisation selon les revendications 11 à 13, caractérisé en ce que le serveur de transactions (ST) envoie une information aléatoire à destination du système de sécurisation (1) et du serveur d'authentification (SA), ladite information faisant partie des données chiffrées par le microcontrôleur du système de sécurisation (1) et envoyées au serveur d'authentification (SA).

16. Procédé de sécurisation selon les revendications 11 à 15, caractérisé en ce que l'algorithme de déchiffrement et la clef associée sont enregistrés dans une zone mémoire du serveur d'authentification (SA) et du serveur de transactions (ST).

17. Procédé de sécurisation selon les revendications 11 à 16, caractérisé en ce que les clefs de chiffrement peuvent être symétriques ou asymétriques.

18. Procédé de sécurisation selon les revendications 11 à 17, caractérisé en ce que la connexion sécurisé réalisée entre le terminal (5) et le serveur d'authentification (SA) est chiffrée à l'aide d'un protocole de type SSL ou TLS.

19. Serveur d'authentification (SA) d'un système de sécurisation des transactions (1), comprenant des moyens de traitement des données, au moins un espace mémoire, des moyens de connexion à un réseau étendu, caractérisé en ce qu'il comprend en outre :

- au moins une base de données comprenant les identifiants, au moins une clef permettant de retrouver la clef de chiffrement de chaque système de sécurisation des transactions (1) et un code secret de chaque système de sécurisation des transactions (1),

- au moins une base de données comprenant les noms d'utilisateur associés à chaque système de sécurisation des transactions (1),

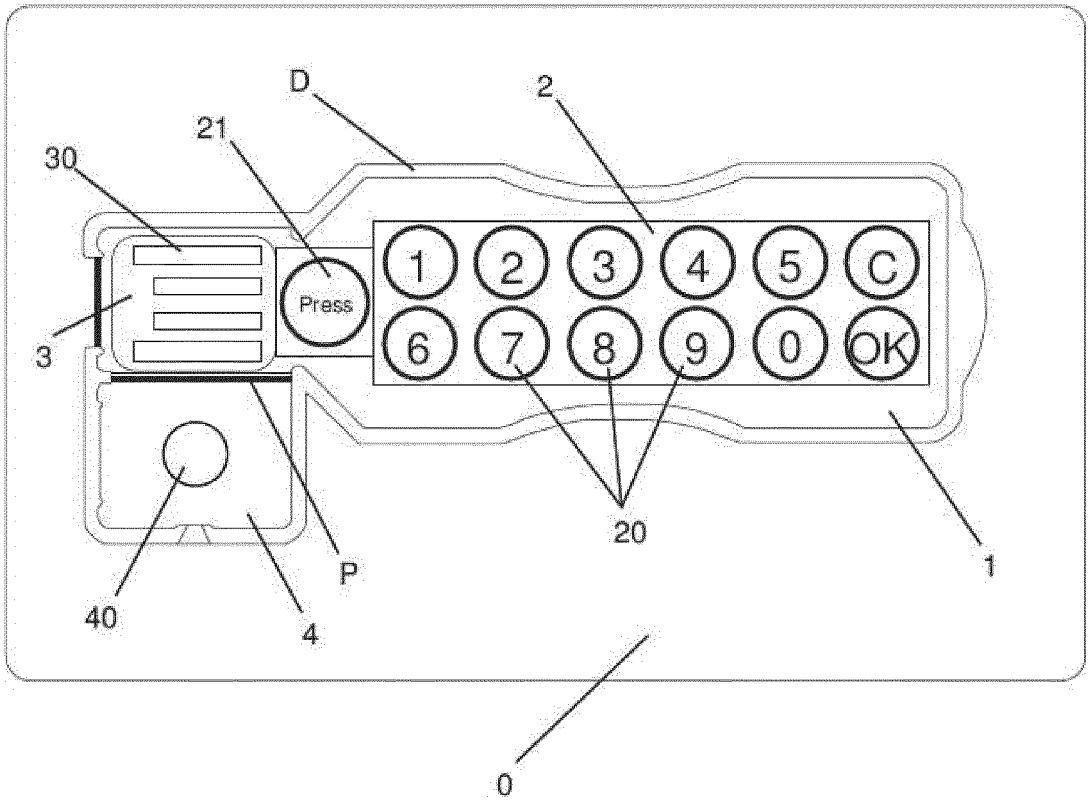
- un algorithme de déchiffrement inverse de celui enregistré dans la mémoire du système de sécurisation des transactions (1), pour déchiffrer les données reçues grâce à une clef de chiffrement, et comparant le résultat du

déchiffrement soit à l'identifiant, soit au code secret pour réaliser l'authentification en cas de coïncidence avec au moins un des deux,

le serveur d'authentification (SA) étant connecté d'une part à un terminal (5) d'un utilisateur réalisant une transaction en ligne à l'aide de sa carte de transactions et du système de sécurisation (1) associé, et d'autre part au serveur de transactions (ST) correspondant, le serveur d'authentification (SA) autorisant la transaction auprès du serveur de transactions (ST) une fois l'authentification combinée des identifiants de la carte de transactions et du système de sécurisation (1) réalisée.

20. Serveur d'authentification (SA) selon la revendication précédente, caractérisé en ce qu'il envoie au terminal (5) de l'utilisateur via les moyens de connexion au réseau étendu, un nombre généré aléatoirement utilisé dans le chiffrement de l'identifiant et du code secret du système de sécurisation des transactions (1) relié au terminal (5) de l'utilisateur.

FIGURE 1a



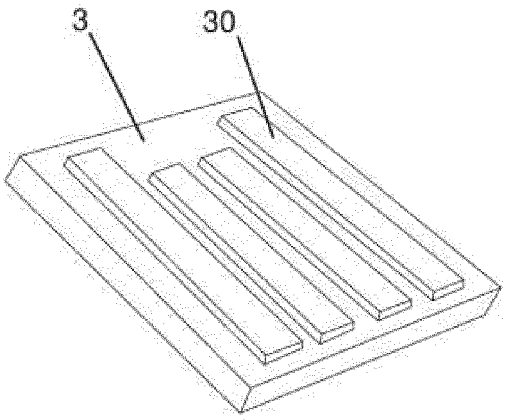


FIGURE 1b

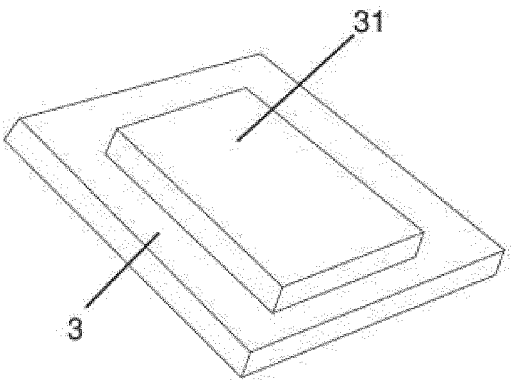
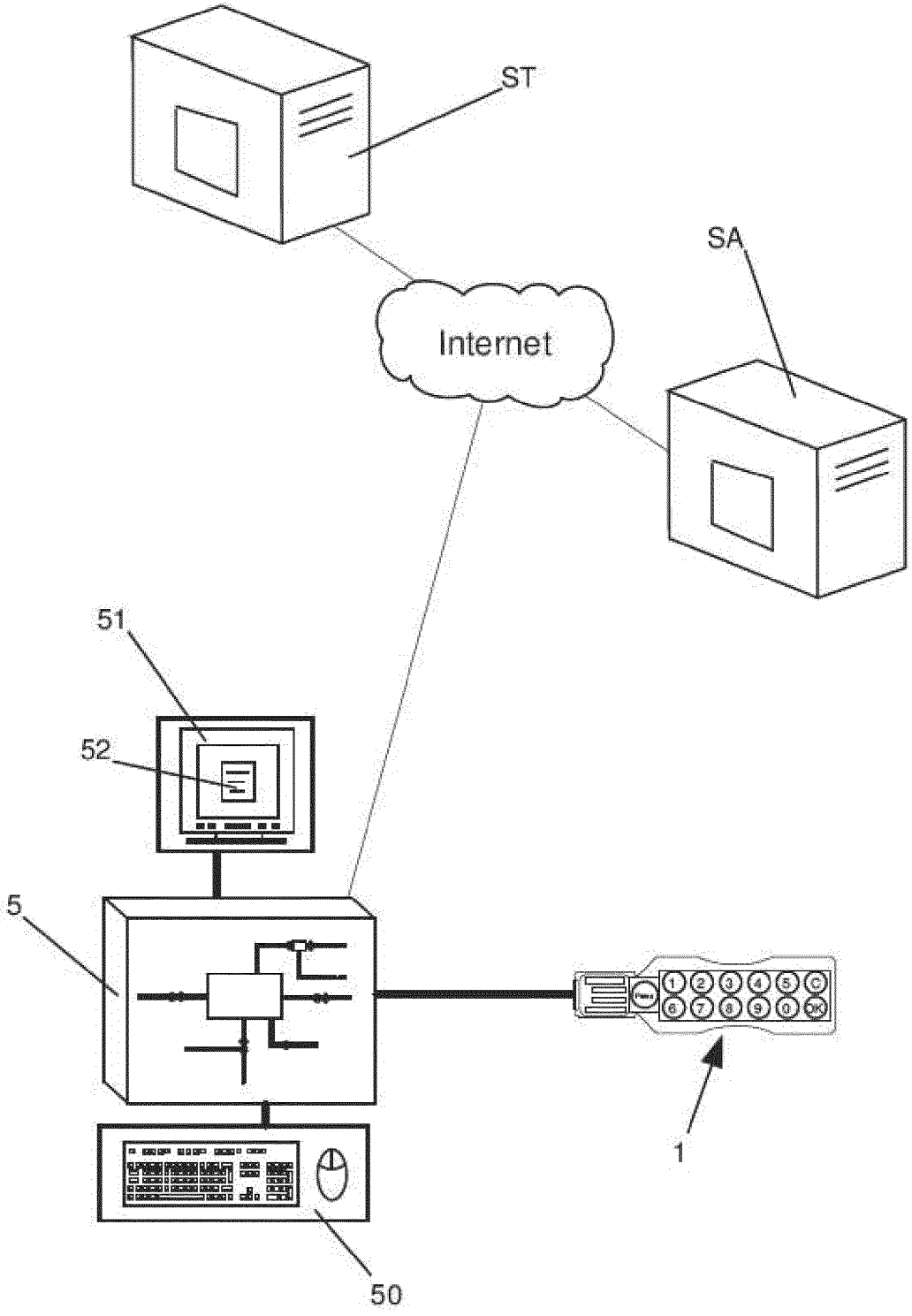


FIGURE 1c

FIGURE 2



RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 768012
FR 1253381

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	US 2007/143828 A1 (JEAL DAVID [GB] ET AL) 21 juin 2007 (2007-06-21) * abrégé * * alinéa [0040] - alinéa [0142]; revendications 1, 25; figures 1-4, 6-7C * -----	1-20	H04L9/32
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			G06F

Date d'achèvement de la recherche	Examinateur
20 décembre 2012	Savvides, George

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons
.....
& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1253381 FA 768012

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 20-12-2012
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2007143828 A1	21-06-2007	EP 1671198 A1	21-06-2006
		EP 2469374 A1	27-06-2012
		GB 2406925 A	13-04-2005
		GB 2406928 A	13-04-2005
		JP 2007513396 A	24-05-2007
		US 2007143828 A1	21-06-2007
		WO 2005043357 A1	12-05-2005

EPO FORM P0465