SPF Economie, PME, Classes
Moyennes & Energie
Office de la Propriété intellectuelle

(11) 1026342 B9

(47) Date de délivrance : 14/01/2020

(12) BREVET D'INVENTION BELGE

(47) Date de publication : 14/01/2020

(48) Date d'édition : 04/02/2020

(21) Numéro de demande : BE2018/5368

(22) Date de dépôt : 04/06/2018

(62) Divisé de la demande de base :

(62) Date de dépôt demande de base :

(51) Classification internationale : G06F 21/31, G06Q 20/32, G06Q 20/38, G06Q 20/40

(30) Données de priorité :

(73) Titulaire(s) :

WORLDLINE SA

1130, BRUXELLES (HAREN)
Belgique

(72) Inventeur(s) :

YOUSSEF Mohamed Amine
1831 MACHELEN
Belgique

CAVIGNEAUX Christophe
1360 ORBAIS
Belgique

BAESENS Pierrot
1600 SINT-PIETERS-LEEUW
Belgique

LESIRE Philippe
2550 KONTICH
Belgique

(54) DISPOSITIF ET PROCEDE POUR L'IDENTIFICATION SECURISEE D'UN UTILISATEUR

(57) L'invention concerne un terminal portable de paiement ou de point de vente avec un connecteur jack et un procédé pour l'identification sécurisée d'un titulaire de carte, le terminal comprenant un ensemble de dispositifs et un agencement pour mettre en œuvre ledit procédé, qui comprend au moins: détecter si ledit titulaire de carte a un dispositif mobile, configurer le terminal pour le lancement d'un mode d'accessibilité sur le dispositif mobile du titulaire de carte; transmettre une demande au dispositif mobile pour l'envoi d'un code PIN au terminal ; et, lors de la réception d'une communication du dispositif mobile comprenant des informations, déchiffrer lesdites informations pour obtenir le code PIN et valider la transaction.

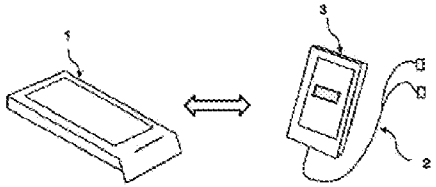

Figure 4

BE2018/5368

Dispositif et procédé pour l'identification sécurisée d'un utilisateur

DOMAINE TECHNIQUE DE L'INVENTION

La présente invention concerne le domaine de l'authentification et/ou du contrôle de l'identité d'un utilisateur qui demande un service ou qui procède à une transaction, plus précisément l'invention concerne un dispositif et un procédé pour identifier une personne et qui convient également aux personnes malvoyantes.

ARRIERE-PLAN TECHNOLOGIQUE DE L'INVENTION

L'objet de l'invention consiste à augmenter la sécurité lorsqu'un utilisateur entre un code d'identification tel que, par exemple, un code PIN, sur un écran tactile.

Généralement, l'écran affiche un clavier d'identification personnelle avec une valeur numérique ou autre pour chaque touche et l'utilisateur sélectionne chaque touche correspondant à chaque valeur de chaque chiffre du code PIN.

Pendant cette opération, n'importe quel tiers peut observer et mémoriser jusqu'à 12 chiffres (généralement 4 ou 6 chiffres) du code PIN, ce qui permet ensuite à un tiers frauduleux de combiner ces informations avec d'autres pour effectuer un retrait frauduleux sur le compte.

Un exemple de l'inconvénient de cette solution est représenté par le document EP 2 791 845.

Jusqu'à présent, les fabricants de terminaux équipaient la partie affichée d'une protection contre la possibilité d'observer les valeurs des touches. Cette solution n'est pas complètement efficace et présente l'inconvénient d'augmenter le volume du terminal.

Une autre tentative pour résoudre ce problème consistait, conformément au document US 8 392 846, à afficher un clavier d'identification personnelle virtuel à des emplacements variables sur un écran tactile afin d'empêcher la fraude ou l'interception de l'identification personnelle. Cependant, une caméra pourrait néanmoins observer chaque étape et, en revoyant les images, un tiers frauduleux pourrait accéder aux informations. La solution de la présente invention est capable de pallier cet inconvénient.

DESCRIPTION GENERALE DE L'INVENTION

La présente invention a pour but de pallier certains inconvénients de l'art antérieur en proposant des moyens pour l'authentification ou le contrôle sécurisé de l'identité de personnes, y compris de personnes mal voyantes.

Cet but est atteint par un terminal portable de paiement ou de point de vente avec un connecteur jack pour une transaction sécurisée comprenant au moins :

- une première mémoire pour mémoriser un ensemble de programmes ou une séquence d'instructions à exécuter sur un processeur dudit terminal et au moins un ensemble de clés pour l'authentification et/ou le chiffrement ne pouvant pas être lu à partir de l'extérieur du terminal ;
- un dispositif de détection de moyens de communication filaire ou sans fil pour détecter si un titulaire de carte utilise un dispositif mobile ;

le terminal (1) étant caractérisé en ce qu'il comprend au moins un module de gestion de transaction comprenant un agencement pour configurer le terminal (1) de manière à :

- lancer un mode d'accessibilité sur le dispositif mobile du titulaire de carte ;

- transmettre une demande au dispositif mobile pour envoyer un code PIN au terminal ; et
- lors de la réception d'une communication du dispositif mobile comprenant des informations, déchiffrer lesdites informations pour obtenir le code PIN, au moyen de l'ensemble de clés pour l'authentification et/ou le chiffrement et valider la transaction.

Selon une autre caractéristique, lors du lancement du mode d'accessibilité sur le dispositif mobile, le terminal comprend au moins un programme pour vérifier si une application propriétaire de mode d'accessibilité est installée sur le dispositif mobile, ladite application étant téléchargée à partir d'un portail de téléchargement d'applications, et exécuter une authentification de ladite application de mode d'accessibilité installée au moyen de l'ensemble de clés pour l'authentification et/ou le chiffrement mémorisé dans la première mémoire.

Selon une autre caractéristique, le terminal comprend au moins un système d'exploitation (OS) pour la création d'une machine virtuelle, si, lors du lancement du mode d'accessibilité sur le dispositif mobile, le terminal détermine qu'aucune application de mode d'accessibilité n'est installée sur ledit dispositif mobile, ladite machine virtuelle étant transmise au dispositif mobile de titulaire de carte, lorsque ledit dispositif mobile est détecté au moyen du dispositif de détection de moyens de communication filaire/sans fil du terminal, de manière à être installée sur ledit dispositif mobile.

Selon une autre caractéristique, le terminal comprend au moins une application instantanée qui est poussée à partir du terminal dans la machine virtuelle s'exécutant sur le dispositif mobile, pour exécuter le mode d'accessibilité sur le dispositif mobile de titulaire de carte.

Selon une autre caractéristique, le terminal comprend :

- une application de mode d'accessibilité mémorisée dans la première mémoire et mettant en œuvre la séquence entière du mode d'accessibilité du terminal pour permettre au titulaire de carte de valider une transaction sur l'écran du terminal ;
- un agencement d'authentification pour mettre en œuvre un processus d'authentification pour les titulaires de carte en entrant un code PIN ou une séquence de nombres et de lettres (SNL) ;
- un capteur de proximité pour détecter la présence d'un titulaire de carte ;
- un premier dispositif de détection pour détecter la présence, dans le connecteur, d'une fiche enfichée pour connecter un casque de titulaire de carte et comprenant un agencement pour produire un signal électrique pour déclencher l'exécution du mode d'accessibilité ;
- un deuxième dispositif de détection pour détecter la position du doigt sur l'écran chaque fois qu'un doigt du propriétaire du casque touche l'écran.

Selon une autre caractéristique, le module de gestion de transaction comprend un agencement pour au moins configurer ledit terminal pour exécuter, si le dispositif mobile de titulaire de carte n'est pas détecté par le dispositif de détection de moyens de communication filaire/sans fil, un mode d'accessibilité, dans lequel, au moins, le terminal :

- demande, à l'aide de moyens de notification, la connexion d'un casque dans le connecteur jack dudit terminal ;

- exécute la première application de mode d'accessibilité, après la détection, au moyen du premier dispositif de détection, d'une fiche enfichée pour connecter un casque de titulaire de carte, l'écran du terminal étant brouillé et maintenu en noir pendant la séquence entière du mode d'accessibilité ;
- configure, au moyen d'un ensemble d'agencements, l'écran pour détecter la position du doigt du titulaire de carte lorsque ledit titulaire de carte déplace son doigt sur ledit écran pour sélectionner chaque chiffre de son code PIN en déplaçant son doigt sur ledit écran ;
- envoie, par l'intermédiaire du casque, de signaux audio préenregistrés correspondant à chaque position du doigt pour aider le titulaire de carte à choisir les chiffres de son code PIN.

Selon une autre caractéristique, le terminal comprend au moins un moyen de notification qui consiste en un agencement audio pour émettre un message vocal par l'intermédiaire d'un haut–parleur, inclus dans ledit terminal, et/ou envoyer ledit message vocal au dispositif mobile de titulaire de carte.

Selon une autre caractéristique, le terminal comprend au moins un moyen de notification qui consiste en un module de messages textuels pour afficher des informations sur l'écran dudit terminal ou envoyer lesdites informations sur l'écran du dispositif mobile de titulaire de carte.

Selon une autre caractéristique, le terminal comprend à la fois un module de messages textuels et un agencement audio pour envoyer des informations au titulaire de carte par l'intermédiaire dudit terminal ou dudit dispositif mobile de titulaire de carte.

Selon une autre caractéristique, le terminal comprend un ensemble de clés mémorisé dans une sixième mémoire, incluse dans le terminal, ledit ensemble de clés ne pouvant pas être lu à partir de l'extérieur du terminal et correspondant à l'ensemble de clés mémorisé dans la première mémoire, l'ensemble de clés mémorisé dans la sixième mémoire étant poussé avec l'application instantanée sur la machine virtuelle s'exécutant sur le dispositif mobile de titulaire de carte, ledit ensemble de clés de la sixième mémoire étant utilisé pour l'échange sécurisé de données et/ou d'informations entre le terminal et le dispositif mobile de titulaire de carte et enregistré dans une mémoire du dispositif mobile de titulaire de carte où il ne peut pas être lu à partir de l'extérieur.

Selon une autre caractéristique, le terminal comprend au moins un ensemble de programmes envoyé au dispositif mobile du titulaire de carte pour supprimer la machine virtuelle et/ou l'application instantanée s'exécutant sur ladite machine virtuelle, dudit dispositif mobile après la validation de la transaction.

Selon une autre caractéristique, la machine virtuelle comprend au moins un ensemble de programmes pour simuler chaque composant du terminal de paiement et leur connexion de manière à mettre en œuvre, lors de l'exécution de l'application instantanée, un mode d'accessibilité comprenant au moins le mode d'accessibilité tel qu'exécuté par ledit terminal.

Selon une autre caractéristique, l'application instantanée comprend un ensemble de programmes pour simuler les fonctionnalités de chaque composant du terminal de paiement et sa connexion de manière à mettre en

œuvre un mode d'accessibilité comprenant au moins le mode d'accessibilité tel qu'exécuté par ledit terminal.

Selon une autre caractéristique, l'application instantanée lancée par le terminal sur le dispositif mobile de titulaire de carte comprend au moins un programme dont l'exécution sur le dispositif mobile de titulaire de carte permet de répondre à la demande d'authentification et/ou de code PIN envoyée par le terminal.

Selon une autre caractéristique, l'application instantanée lancée par le terminal sur le dispositif mobile de titulaire de carte comprend au moins un programme dont l'exécution sur le dispositif mobile de titulaire de carte récupère, dans la mémoire dudit dispositif mobile de titulaire de carte, l'ensemble de clés enregistré, permettant audit dispositif mobile de répondre à la demande d'authentification et/ou de code PIN envoyée par le terminal.

Selon une autre caractéristique, le terminal comprend une mémoire dans laquelle les informations de transaction relatives au moins au montant de la transaction et/ou au marchand sont enregistrées, lesdites informations étant transmises avec la demande de code PIN au dispositif mobile de titulaire de carte.

Selon une autre caractéristique, l'application instantanée s'exécutant sur le dispositif mobile de titulaire de carte comprend au moins un ensemble de programmes pour configurer le dispositif mobile de titulaire de carte, lorsqu'au moins une demande d'entrée de code PIN a été envoyée par ledit terminal, de manière à :

- vérifier si un casque est enfiché ou non dans le connecteur jack audio dudit dispositif mobile ;

- demander, à l'aide d'un moyen de notification, la connexion d'un casque au dispositif mobile, si aucun casque n'est enfiché ;
- lancer le mode d'accessibilité pour l'entrée du code PIN une fois qu'un casque est enfiché.

Selon une autre caractéristique, l'application instantanée s'exécutant sur le dispositif mobile de titulaire de carte comprend au moins un programme pour récupérer l'ensemble de clés dans la mémoire dudit dispositif mobile de manière à chiffrer le code PIN entré par le titulaire de carte avant son envoi au terminal pour la validation de la transaction.

Selon une autre caractéristique, l'application instantanée s'exécutant sur le dispositif mobile de titulaire de carte comprend au moins un programme pour brouiller et maintenir en noir l'écran du dispositif mobile de titulaire de carte pendant la séquence entière du mode d'accessibilité.

Selon une autre caractéristique, l'application instantanée comprend au moins un programme configurant l'écran du dispositif mobile de titulaire de carte pour détecter la position du doigt du titulaire de carte lorsque ledit titulaire de carte déplace son doigt sur ledit écran pour sélectionner chaque chiffre de son code PIN en déplaçant son doigt sur ledit écran.

Selon une autre caractéristique, l'application instantanée comprend au moins un programme configurant le dispositif mobile de titulaire de carte pour envoyer, par l'intermédiaire du casque, les signaux audio préenregistrés correspondant à chaque position du doigt pour aider le titulaire de carte à choisir les chiffres de son code PIN, lesdits signaux audio étant transmis au

dispositif mobile de titulaire de carte avec les informations de transaction et le code PIN demandés par le terminal.

Selon une autre caractéristique, l'application instantanée comprend au moins un programme pour configurer le dispositif mobile de titulaire de carte de manière à permettre au titulaire de carte d'entrer son code PIN au moyen d'une application tiers autorisée.

Un autre but de la présente invention consiste à proposer un processus pour l'authentification sécurisée d'un utilisateur.

Cet but est atteint au moyen d'un procédé pour l'identification sécurisée d'un titulaire de carte avec un terminal portable de paiement ou de point de vente tel que décrit dans la présente demande et/ou un dispositif mobile de titulaire de carte, ledit procédé comprenant au moins l'étape :

- de détection de moyens de communication filaire/sans fil d'un dispositif mobile ;

le procédé étant caractérisé en ce que, si le dispositif mobile de titulaire de carte est détecté, il comprend au moins l'étape de configuration du terminal pour :

- lancer un mode d'accessibilité sur le dispositif mobile du titulaire de carte ;
- transmettre une demande au dispositif mobile pour envoyer un code PIN au terminal ; et
- lors de la réception d'une communication du dispositif mobile comprenant des informations, déchiffrer lesdites informations pour obtenir le code PIN et valider la transaction.

Selon une autre caractéristique, le procédé pour l'identification sécurisée comprend au moins, lors du lancement du mode d'accessibilité, les étapes :

- de vérification si une application propriétaire de mode d'accessibilité est installée sur le dispositif mobile ;
- d'exécution d'une authentification de ladite application de mode d'accessibilité installée.

Selon une autre caractéristique, le procédé pour l'identification sécurisée comprend au moins les étapes :

- de création d'une machine virtuelle si, lors du lancement du mode d'accessibilité sur le dispositif mobile, le terminal détermine qu'aucune application de mode d'accessibilité n'est installée sur ledit dispositif mobile ;
- de transmission de ladite machine virtuelle au dispositif mobile de titulaire de carte ;
- de poussée d'une application instantanée sur ladite machine virtuelle pour exécuter le mode d'accessibilité sur le dispositif mobile (3).

Selon une autre caractéristique, le procédé pour l'identification sécurisée comprend au moins l'étape de chiffrement au moins du code PIN ou d'une partie du code PIN sur le dispositif mobile de titulaire de carte avant sa transmission au terminal pour validation.

Selon une autre caractéristique, si le dispositif mobile n'est pas détecté, le procédé pour l'identification sécurisée comprend au moins les étapes :

- de demande, au moyen d'une notification, sur l'écran du terminal, de la connexion d'un casque dans le connecteur de fiche dudit terminal ;
- de détection de la présence d'une fiche enfichée dans le connecteur du terminal pour la connexion d'un casque de titulaire de carte ;
- de déclenchement de l'exécution d'un premier mode d'accessibilité permettant au titulaire de carte de s'identifier ;
- de brouillage et de maintien de l'écran en noir pendant la séquence du mode d'accessibilité ;
- de configuration de l'écran pour détecter la position du doigt du titulaire de carte lorsque ledit titulaire de carte déplace son doigt sur ledit écran pour sélectionner chaque chiffre de son code PIN en déplaçant son doigt sur ledit écran ;
- d'envoi, par l'intermédiaire du casque, de signaux audio préenregistrés correspondant à chaque position du doigt pour aider le titulaire de carte à choisir les chiffres de son code PIN.

Selon une autre caractéristique, l'étape d'exécution du mode d'accessibilité sur le dispositif mobile de titulaire de carte comprend les étapes :

- de contrôle si un casque est enfiché ou non dans le connecteur jack audio dudit dispositif mobile ;
- de demande de la connexion d'un casque au dispositif mobile, si aucun casque n'est enfiché ;
- de lancement du mode d'accessibilité pour l'entrée du code PIN une fois qu'un casque est enfiché.

DESCRIPTION DES FIGURES ILLUSTRATIVES

D'autres particularités et avantages de la présente invention apparaîtront plus clairement à la lecture de la description ci-après, faite en référence aux dessins annexés, dans lesquels :

– les figures 1A, 1B sont respectivement des représentations schématiques des composants du terminal portable de paiement ou de point de vente et du contrôleur, selon un mode de réalisation ;

– les figures 2A, 2B sont des représentations schématiques de l'entrée d'un code PIN sur un écran brouillé en noir, selon un mode de réalisation ;

– les figures 3A, 3B et 3C sont respectivement des représentations schématiques du processus d'authentification, de l'étape dudit processus d'authentification sur le terminal portable de paiement ou de point de vente et de l'étape dudit processus d'authentification sur le dispositif mobile de titulaire de carte (3), composant dudit processus d'authentification ;

– la figure 4 est une représentation schématique du terminal échangeant avec le dispositif mobile de titulaire de carte pendant la connexion du terminal portable de paiement ou de point de vente et du contrôleur, selon un mode de réalisation.

DESCRIPTION DES MODES DE REALISATION PREFERES DE L'INVENTION

La présente invention concerne un terminal portable de paiement ou de point de vente (1) pour l'identification sécurisée d'un utilisateur, y compris un utilisateur malvoyant, pendant une transaction.

Dans certains modes de réalisation, le terminal portable de paiement ou de point de vente (1, figures 1A, 4) avec un connecteur jackpour une transaction sécurisée comprend au moins :

- une première mémoire (13) pour mémoriser un ensemble de programmes ou une séquence d'instructions à exécuter sur un

processeur dudit terminal et au moins un ensemble de clés pour l'authentification et/ou le chiffrement ne pouvant pas être lu à partir de l'extérieur du terminal ;

- un dispositif de détection de moyens de communication filaire ou sans fil (USB, Wifi, Bluethooth, ...) pour détecter si un titulaire de carte utilise un dispositif mobile (3, figure 4) ;

le terminal (1) étant caractérisé en ce qu'il comprend au moins un module de gestion de transaction comprenant un agencement pour configurer le terminal de manière à :

- lancer un mode d'accessibilité sur le dispositif mobile (3) du titulaire de carte ;
- transmettre une demande au dispositif mobile pour envoyer un code PIN au terminal ; et
- lors de la réception d'une communication du dispositif mobile comprenant des informations, déchiffrer lesdites informations pour obtenir le code PIN, au moyen de l'ensemble de clés pour l'authentification et/ou le chiffrement et valider la transaction.

Dans certains modes de réalisation, lors du lancement du mode d'accessibilité sur le dispositif mobile (3), le terminal comprend au moins un programme pour vérifier si une application propriétaire de mode d'accessibilité est installée sur le dispositif mobile, ladite application étant téléchargée à partir d'un portail de téléchargement d'applications, tel que, par exemple, Google playstore ou Applestore, et exécuter une authentification de ladite application de mode d'accessibilité installée au moyen de l'ensemble de clés pour l'authentification et/ou le chiffrement mémorisé dans la première mémoire. Dans ce cas, l'application de mode d'accessibilité peut comprendre un ensemble de clés pour l'authentification et/ou le chiffrement de données,

lesdites clés correspondant à l'ensemble de clés mémorisé dans la première mémoire du terminal.

Dans certains modes de réalisation, le terminal portable de paiement ou de point de vente comprend au moins un système d'exploitation (OS) pour la création d'une machine virtuelle, si, lors du lancement du mode d'accessibilité sur le dispositif mobile (3), le terminal détermine qu'aucune application de mode d'accessibilité n'est installée sur ledit dispositif mobile, ladite machine virtuelle étant transmise au dispositif mobile (3) du titulaire de carte, lorsque ledit dispositif mobile (3) est détecté au moyen du dispositif de détection de moyens de communication filaire/sans fil du terminal, de manière à être installée sur ledit dispositif mobile (3).

Dans certains modes de réalisation, le terminal portable de paiement ou de point de vente comprend au moins une application instantanée qui est poussée à partir du terminal dans la machine virtuelle s'exécutant sur le dispositif mobile (3), pour exécuter le mode d'accessibilité sur le dispositif mobile (3) du titulaire de carte.

Par « application instantanée », nous entendons une application qui peut être exécutée instantanément sur le dispositif mobile sans nécessiter une installation sur ledit dispositif mobile (3).

Dans certains modes de réalisation, le terminal (1) comprend :

- une application de mode d'accessibilité mémorisée dans la première mémoire et mettant en œuvre la séquence entière du mode d'accessibilité du terminal pour permettre au titulaire de carte de valider une transaction sur l'écran (14) du terminal ;
- un agencement d'authentification (12, figures 1A, 1B) pour mettre en œuvre un processus d'authentification pour les

titulaires de carte en entrant un code PIN ou une séquence de nombres et de lettres (SNL) ;

- un capteur de proximité pour détecter la présence d'un titulaire de carte (non montré) ;
- un premier dispositif de détection (11) pour détecter la présence, dans le connecteur, d'une fiche enfichée pour connecter un casque de titulaire de carte (2, figure 4) et comprenant un agencement pour produire un signal électrique pour déclencher l'exécution du mode d'accessibilité ;
- un deuxième dispositif de détection (101) pour détecter la position du doigt sur l'écran (14), chaque fois qu'un doigt du propriétaire du casque (2) touche l'écran (14).

Dans certains modes de réalisation, le module de gestion de transaction comprend un agencement pour au moins configurer ledit terminal pour exécuter, si le dispositif mobile (3) du titulaire de carte n'est pas détecté par le dispositif de détection de moyens de communication filaire/sans fil, un mode d'accessibilité dans lequel, au moins, le terminal :

- demande, à l'aide de moyens de notification, la connexion d'un casque (2) dans le connecteur jack dudit terminal ;
- exécute la première application de mode d'accessibilité, après la détection, au moyen du premier dispositif de détection, d'une fiche enfichée pour connecter un casque de titulaire de carte (2), l'écran du terminal étant brouillé et maintenu en noir pendant la séquence entière du mode d'accessibilité ;
- configure, au moyen d'un ensemble d'agencements, l'écran pour détecter la position du doigt du titulaire de carte lorsque ledit titulaire de carte déplace son doigt sur ledit écran pour

sélectionner chaque chiffre de son code PIN en déplaçant son doigt sur ledit écran ;

- envoie, par l'intermédiaire du casque (2), de signaux audio préenregistrés correspondant à chaque position du doigt pour aider le titulaire de carte à choisir les chiffres de son code PIN.

Le terminal (1), tel qu'illustré sur la figure 1A, comprend un agencement connecté à l'agencement d'authentification (12) pour brouiller et maintenir l'écran (14) en noir pendant la séquence entière du mode d'accessibilité.

L'agencement d'authentification (12) peut comprendre un programme pour générer, à chaque fois que le mode d'accessibilité est actif, au moins un ensemble de « chaîne de touches » (figures 2A, 2B) mémorisé dans un « fichier de chaînes » du terminal (1), pour l'entrée du PIN/de la SNL, chaque « chaîne de touches » comprenant un ensemble de touches (20), lesdites touches (20) étant réparties de manière aléatoire dans ladite « chaîne de touches ».

Le deuxième dispositif de détection (101) comprend un agencement pour détecter la longueur, d, ou l'orientation du déplacement du doigt sur l'écran et est connecté à l'agencement d'authentification (12) de manière à transmettre un signal correspondant à la longueur d ou à l'angle d'orientation pour indiquer qu'un déplacement a lieu ou non en fonction de la valeur de ladite longueur d ou dudit angle d'orientation comparée à une valeur de seuil mémorisée.

L'agencement d'authentification peut également comprendre un module de tri pour récupérer, lors de la réception d'un signal indiquant un déplacement, dans le « fichier de chaînes » mémorisé, une « chaîne de touches » de manière à attribuer une valeur de touche correspondant à la longueur d ou à l'angle d'orientation du déplacement du doigt, et est connecté à un agencement audio (17) du terminal (1) où les signaux audio préenregistrés correspondant à chaque touche de la « chaîne de touches »

sont mémorisés, de manière à sélectionner le son correspondant à la touche attribuée au déplacement et à l'émettre par l'intermédiaire du connecteur jack vers le casque (2) du titulaire de carte.

Le terminal peut comprendre un programme pour réitérer ces actions jusqu'à ce que l'utilisateur écoutant la valeur d'un chiffre ou d'un caractère d'un PIN/d'une SNL retire son doigt de l'écran (14), la dernière valeur, indiquée en tant que retour, est ensuite mémorisée dans la deuxième mémoire (15), incluse dans le terminal (1), en tant que chiffre du PIN/de la SNL.

L'expression « chaîne de touches » signifie ici un nombre de chiffres ou de caractères successifs donné.

La « chaîne de touches » peut comprendre au moins des touches (20) avec des valeurs de 0 à 9 ou des lettres de A à Z, ou les deux. Par exemple, et de manière non limitative, une chaîne générée peut être « 3241569807 ».

A chaque fois que l'utilisateur touche l'écran après un choix d'un chiffre de son code PIN/code, le terminal récupère une nouvelle « chaîne de touches » dans le « fichier de chaînes ».

Une fois qu'une valeur de touche (20) est choisie par l'utilisateur, un geste de double frappe du doigt permet de valider ledit choix.

Il est ainsi évident que le terminal décrit dans la présente demande fournit une manière sécurisée de valider une transaction, étant donné qu'il n'y a pas de touche ou de clavier affiché sur l'écran (14).

De plus, étant donné que l'écran est maintenu en noir et que l'utilisateur doit seulement déplacer son doigt sur l'écran pour sélectionner une touche (20) ou un chiffre, le terminal peut être utilisé à la fois pour des utilisateurs normaux et malvoyants.

Par « transaction », nous entendons le paiement d'un produit ou d'un service par exemple.

Le dispositif mobile (3) du titulaire de carte (téléphone intelligent ou tablette, par exemple) peut comprendre un ensemble de moyens de communication, tels qu'un câble USB, le Wifi, la NFC (Near Field Communication), le Bluetooth, la VLC (Visual Light Communication) ... pour se connecter au terminal.

Le terminal de paiement peut également comprendre un ensemble de moyens de communication, tels qu'un câble USB, le Wifi, la NFC (Near Field Communication), le Bluetooth, la VLC (Visual Light Communication)...pour établir une communication avec le dispositif mobile (3) du titulaire de carte.

La deuxième application de mode d'accessibilité est utilisée en tant qu'application miroir du terminal. En lançant ladite application, le titulaire de carte (personne normale ou mal voyante) est maintenant capable d'entrer le code PIN sur son propre dispositif. Cette solution a pour avantage, en particulier pour une personne malvoyante, de ne pas nécessiter l'apprentissage de la manière d'utiliser un nouveau dispositif pour effectuer une transaction, étant donné que ladite personne mal voyante sait maintenant comment utiliser son propre dispositif mobile (3) (téléphone intelligent, tablette, ...).

Dans certains modes de réalisation, le terminal (1) comprend un moyen de notification qui peut être un agencement audio pour émettre un message vocal par l'intermédiaire d'un haut–parleur, inclus dans ledit terminal, et/ou envoyer ledit message vocal au dispositif mobile (3) du titulaire de carte.

Dans certains modes de réalisation, le terminal (1) comprend un moyen de notification qui peut être un module de messages textuels pour afficher des informations sur l'écran dudit terminal ou envoyer lesdites informations sur l'écran du dispositif mobile (3) du titulaire de carte.

Dans certains modes de réalisation, le terminal de paiement comprend à la fois un module de messages textuels et un agencement audio pour envoyer des informations au titulaire de carte par l'intermédiaire dudit terminal ou dudit dispositif mobile (3) du titulaire de carte.

Dans certains modes de réalisation, le deuxième dispositif de détection (101) comprend un agencement pour mesurer le déplacement ou le mouvement du doigt sur l'écran à partir d'une position ou d'une orientation initiale donnée, la longueur du déplacement ou du mouvement étant caractérisée par la valeur d ou l'angle d'orientation. La longueur d ou l'angle d'orientation est comparé à une valeur de seuil mémorisée dans ledit deuxième dispositif de détection (101). Si la longueur d ou l'angle d'orientation est supérieur à la valeur de seuil, un signal est transmis à l'agencement d'authentification pour indiquer qu'il y a un déplacement du doigt. Si, au contraire, la longueur d ou l'angle d'orientation est inférieur à la valeur de seuil, le deuxième dispositif de détection (101) considère qu'aucun déplacement du doigt n'a lieu, et un signal est transmis à l'agencement d'authentification indiquant qu'il n'y a pas de déplacement du doigt.

Dans certains modes de réalisation, le terminal portable de paiement ou de point de vente (1) peut comprendre un contrôleur (10) comprenant au moins :

- le deuxième dispositif de détection (101) qui est connecté à l'écran (14) du terminal (1) de manière à capturer et enregistrer, dans une troisième mémoire (104), les données liées aux positions du doigt lorsque ledit écran (14) est touché ;
- un dispositif de génération de positions (102), comprenant un agencement pour générer des données correspondant à diverses positions sur l'écran (14), lesdites diverses positions étant enregistrées dans une quatrième mémoire (105) ;

- un processeur (100) et une cinquième mémoire (103) comprenant un ensemble de programmes exécutés sur ledit processeur (100) de manière à éviter que l'écran tactile (14) affiche une « chaîne de touches » avec les positions de touches (20) déterminées par les données générées par le dispositif de génération de positions (102) ;

l'ensemble de programmes de la cinquième mémoire dudit contrôleur (10) comprenant au moins :

- un algorithme de comparaison pour comparer les données correspondant aux régions touchées, enregistrées dans la troisième mémoire, avec les données représentatives de chaque emplacement de l'écran générées par le dispositif de génération de positions et enregistrées dans la quatrième mémoire ;
- un algorithme audio pour produire, dans un casque (2) connecté à la fiche, un signal audible correspondant à la valeur de la touche (20) ;
- un premier algorithme d'itération pour réitérer l'algorithme de comparaison et l'algorithme audio jusqu'à ce que l'utilisateur écoutant la valeur qu'il attend retire le doigt de l'écran (14), cette action déclenchant dans la mémoire la mémorisation de ladite valeur en tant que premier chiffre ;
- un deuxième algorithme d'itération pour réitérer en outre le premier algorithme d'itération à chaque fois que l'agencement d'authentification reçoit un nouveau signal de détection de contact et tant que la valeur du nombre de chiffres mémorisée est inférieure à la valeur maximum des nombres de chiffres contenus par le code PIN ou le code d'identification.

Dans certains modes de réalisation, le premier dispositif de détection (11) est connecté au contrôleur (10) de manière à transmettre le signal électrique pour déclencher le mode d'accessibilité.

Dans certains modes de réalisation, le processeur du contrôleur est connecté à la première mémoire pour télécharger et exécuter une séquence d'instructions représentant le mode d'accessibilité lors de la réception dudit signal électrique.

Dans certains modes de réalisation, le contrôleur (10) est connecté à l'agencement d'authentification (12) de manière à lui transmettre un signal d'activation lorsque le mode d'accessibilité est actif, l'agencement d'authentification (12) générant les « chaînes de touches » pour l'identification du titulaire de carte après la réception dudit signal d'activation.

Dans certains modes de réalisation, le contrôleur (10) transmet un ensemble de données, comprenant au moins les valeurs de position générées par le dispositif de génération de positions (102), à l'agencement d'authentification (12), ledit agencement d'authentification (12) générant la « chaîne de touches » à un emplacement de l'écran (14) sur la base dudit ensemble de données.

Dans certains modes de réalisation, l'agencement d'authentification est connecté au deuxième dispositif de détection de manière à récupérer une « chaîne de touches » dans le « fichier de chaînes » lorsque ledit deuxième dispositif de détection (101) détecte le doigt sur l'écran. Lorsque le deuxième dispositif de détection détecte un déplacement ou un mouvement du doigt sur l'écran, ledit agencement d'authentification attribue à la position du doigt une valeur d'une touche (20) de la « chaîne de touches ». Par exemple et

sans limitation, lorsque le premier déplacement ou mouvement du doigt est détecté sur l'écran, l'agencement d'authentification attribue la valeur de la première touche (20) de la « chaîne de touches », par exemple « 2 », à la position du doigt et un son ou un signal audio préenregistré correspondant à la touche « 2 » est récupéré dans l'agencement audio et émis par l'intermédiaire du casque de l'utilisateur indiquant la valeur de la touche (20). Lorsque le deuxième dispositif de détection détecte un deuxième déplacement ou mouvement du doigt, à partir de la dernière position, l'agencement d'authentification attribue la valeur de la deuxième touche (20) de la « chaîne de touches », par exemple « 7 », à la position du doigt et un son ou un signal audio préenregistré correspondant à la touche « 7 » est récupéré dans l'agencement audio et est émis par l'intermédiaire du casque (2) de l'utilisateur indiquant la valeur de la touche (20), et ainsi de suite jusqu'à ce que l'utilisateur choisisse et valide une valeur donnée.

Dans certains modes de réalisation, l'agencement d'authentification comprend un module de désignation de touches (106) qui génère une liste de touches comprenant des informations concernant chaque touche (20) de la « chaîne de touches » et la position associée, ladite liste de touches étant réutilisée par ledit agencement d'authentification si l'utilisateur déplaçant son doigt dans une direction ou une orientation donnée retourne à une position précédente ou dans une autre direction de manière à corriger ou changer un choix de touche (20).

Dans certains modes de réalisation, l'agencement d'authentification comprend un programme qui détermine, en temps réel, à partir des informations contenues dans la liste de touches, la direction du doigt se déplaçant sur l'écran de manière à contrôler si l'utilisateur déplace ledit doigt en avant ou en arrière ou dans n'importe quelle orientation.

Dans certains modes de réalisation, le terminal portable de paiement ou de point de vente (1) comprend un dispositif de comptage (16) connecté à l'agencement d'authentification (12) et à la deuxième mémoire (15) du terminal (1), ledit dispositif de comptage (16) comptant le nombre de chiffres mémorisés dans la deuxième mémoire (15) et, lorsque ledit nombre de comptage correspond à une valeur prédéterminée enregistrée et représentant le nombre de chiffres du PIN/de la SNL, émettant un signal vers ledit agencement d'authentification (12) de manière à exécuter le processus d'authentification.

Dans certains modes de réalisation, le premier dispositif de détection est un commutateur électromécanique.

Dans certains modes de réalisation, le premier dispositif de détection est un capteur.

Dans certains modes de réalisation, le terminal (1) peut comprendre un ensemble de clés mémorisé dans une sixième mémoire, incluse dans le terminal, ledit ensemble de clés ne pouvant pas être lu à partir de l'extérieur du terminal et correspondant à l'ensemble de clés mémorisé dans la première mémoire, ledit ensemble de clés mémorisé dans la sixième mémoire étant poussé avec l'application instantanée sur la machine virtuelle s'exécutant sur le dispositif mobile (3) de titulaire de carte, ledit ensemble de clés de la sixième mémoire étant utilisé pour l'échange sécurisé de données et/ou d'informations entre le terminal et le dispositif mobile (3) de titulaire de carte et enregistré dans une mémoire du dispositif mobile (3) de titulaire de carte où il ne peut pas être lu à partir de l'extérieur.

Dans certains modes de réalisation, le terminal (1) comprend au moins un ensemble de programmes envoyé au dispositif mobile (3) du titulaire de carte pour supprimer la machine virtuelle et/ou l'application instantanée s'exécutant sur ladite machine virtuelle, dudit dispositif mobile (3) après la validation de la transaction.

Dans certains modes de réalisation, la machine virtuelle comprend au moins un ensemble de programmes pour simuler chaque composant du terminal de paiement et leur connexion de manière à mettre en œuvre, lors de l'exécution de l'application instantanée, un mode d'accessibilité comprenant au moins le mode d'accessibilité tel qu'exécuté par ledit terminal.

Dans certains modes de réalisation, l'application de mode d'accessibilité installée ou l'application instantanée peut comprendre un ensemble de programmes pour simuler les fonctionnalités de chaque composant du terminal de paiement et leur connexion de manière à mettre en œuvre un mode d'accessibilité comprenant au moins le mode d'accessibilité tel qu'exécuté par ledit terminal.

Dans certains modes de réalisation, l'application de mode d'accessibilité installée ou l'application instantanée lancée par le terminal sur le dispositif mobile (3) du titulaire de carte comprend au moins un programme dont l'exécution sur le dispositif mobile (3) du titulaire de carte permet de répondre à la demande d'authentification et/ou de code PIN envoyée par le terminal.

Dans certains modes de réalisation, l'application de mode d'accessibilité installée ou l'application instantanée lancée par le terminal sur

le dispositif mobile (3) du titulaire de carte comprend au moins un programme dont l'exécution sur le dispositif mobile (3) du titulaire de carte récupère, dans la mémoire dudit dispositif mobile (3) du titulaire de carte, l'ensemble de clés enregistré, permettant audit dispositif mobile (3) de répondre à la demande d'authentification et/ou de code PIN envoyée par le terminal.

Dans certains modes de réalisation, le terminal comprend une mémoire dans laquelle les informations de transaction relatives au moins au montant de la transaction et/ou au marchand sont enregistrées, lesdites informations étant transmises avec la demande de code PIN au dispositif mobile (3) du titulaire de carte.

Dans certains modes de réalisation, l'application de mode d'accessibilité installée ou l'application instantanée s'exécutant sur le dispositif mobile (3) du titulaire de carte comprend au moins un ensemble de programmes pour configurer le dispositif mobile (3) de titulaire de carte, lorsqu'au moins une demande d'entrée de code PIN a été envoyée par ledit terminal, de manière à :

- vérifier si un casque (2) est enfiché ou non dans le connecteur jack audio dudit dispositif mobile (3) ;
- demander, à l'aide d'un moyen de notification, la connexion d'un casque (2) au dispositif mobile (3), si aucun casque (2) n'est enfiché ;
- lancer le mode d'accessibilité pour l'entrée du code PIN une fois qu'un casque (2) est enfiché.

Dans certains modes de réalisation, l'application instantanée ou l'application de mode d'accessibilité installée s'exécutant sur le dispositif

mobile (3) du titulaire de carte comprend au moins un programme pour récupérer l'ensemble de clés dans la mémoire dudit dispositif mobile (3) de manière à chiffrer le code PIN entré par le titulaire de carte avant son envoi au terminal pour la validation de la transaction.

Dans certains modes de réalisation, l'application instantanée ou l'application de mode d'accessibilité installée sur le dispositif mobile (3) du titulaire de carte peut comprendre au moins un programme pour brouiller et maintenir en noir l'écran du dispositif mobile (3) du titulaire de carte pendant la séquence entière du mode d'accessibilité.

Dans certains modes de réalisation, l'application instantanée ou l'application de mode d'accessibilité installée peut comprendre au moins un programme configurant l'écran du dispositif mobile (3) du titulaire de carte pour détecter la position du doigt du titulaire de carte lorsque ledit titulaire de carte déplace son doigt sur ledit écran pour sélectionner chaque chiffre de son code PIN en déplaçant son doigt sur ledit écran.

Dans certains modes de réalisation, l'application instantanée ou l'application de mode d'accessibilité installée comprend au moins un programme configurant le dispositif mobile (3) du titulaire de carte pour envoyer, par l'intermédiaire du casque (2), les signaux audio préenregistrés correspondant à chaque position du doigt pour aider le titulaire de carte à choisir les chiffres de son code PIN. Dans certains modes de réalisation, les signaux audio sont transmis au dispositif mobile (3) du titulaire de carte avec les informations de transaction et le code PIN demandés par le terminal.

Dans certains modes de réalisation, l'application instantanée ou l'application de mode d'accessibilité installée comprend au moins un

programme pour configurer le dispositif mobile (3) du titulaire de carte de manière à permettre au titulaire de carte d'entrer son code PIN au moyen d'une application tiers autorisée. Par exemple, le titulaire de carte peut utiliser une application telle que « itsme ».

« Itsme » est une application qui permet à un utilisateur de confirmer son identité en utilisant son dispositif mobile (3) tel qu'un téléphone intelligent. « Itsme » utilise les données de la carte d'identité électronique (eID), de la carte SIM de son téléphone intelligent et de son téléphone intelligent pour créer une ID (identité) unique associée à un code PIN.

Dans certains modes de réalisation, l'application instantanée ou l'application de mode d'accessibilité installée comprend au moins un programme pour configurer le dispositif mobile (3) du titulaire de carte de manière à permettre au titulaire de carte de valider la transaction en utilisant des moyens de reconnaissance d'empreinte digitale ou faciale inclus dans ledit dispositif mobile (3) du titulaire de carte.

La présente invention concerne également un procédé pour l'identification sécurisée d'un titulaire de carte (personne normale ou mal voyante) avec un terminal portable de paiement ou de point de vente (1) tel que décrit ci–dessus (dans la présente demande) et/ou ledit dispositif mobile (3) de titulaire de carte.

Dans certains modes de réalisation, le procédé pour l'identification sécurisée (voir les figures 3A, 3B et 3C) d'un titulaire de carte comprend au moins l'étape :

- de détection de moyens de communication filaire/sans fil d'un dispositif mobile (3) ;

le procédé étant caractérisé en ce que, si le dispositif mobile (3) du titulaire de carte est détecté, il comprend au moins l'étape de configuration du terminal (1) pour :

- lancer un mode d'accessibilité sur le dispositif mobile (3) du titulaire de carte ;
- transmettre une demande au dispositif mobile pour envoyer un code PIN au terminal (1) ; et
- lors de la réception d'une communication du dispositif mobile comprenant des informations, déchiffrer lesdites informations pour obtenir le code PIN et valider la transaction.

Dans certains modes de réalisation, le procédé pour l'identification sécurisée comprend au moins, lors du lancement du mode d'accessibilité, les étapes :

- de vérification si une application propriétaire de mode d'accessibilité est installée sur le dispositif mobile ;
- d'exécution d'une authentification de ladite application de mode d'accessibilité installée.

Dans certains modes de réalisation, le procédé pour l'identification sécurisée comprend au moins les étapes :

- de création d'une machine virtuelle si, lors du lancement du mode d'accessibilité sur le dispositif mobile (3), le terminal détermine qu'aucune application de mode d'accessibilité n'est installée sur ledit dispositif mobile ;
- de transmission de ladite machine virtuelle au dispositif mobile (3) du titulaire de carte;

- de poussée d'une application instantanée sur ladite machine virtuelle pour exécuter le mode d'accessibilité sur le dispositif mobile (3).

Dans certains modes de réalisation, le procédé pour l'identification sécurisée d'un titulaire de carte peut comprendre l'étape de chiffrement au moins du code PIN ou d'une partie du code PIN sur le dispositif mobile (3) de titulaire de carte avant sa transmission au terminal pour la validation.

Dans certains modes de réalisation, si le dispositif mobile (3) n'est pas détecté, le procédé pour l'identification sécurisée comprend au moins les étapes :

- de demande, au moyen d'une notification, sur l'écran du terminal, de la connexion d'un casque (2) dans le connecteur de fiche dudit terminal ;
- de détection de la présence d'une fiche enfichée dans le connecteur du terminal (1) pour la connexion d'un casque (2) de titulaire de carte;
- de déclenchement de l'exécution d'un premier mode d'accessibilité permettant au titulaire de carte de s'identifier ;
- de brouillage et de maintien de l'écran en noir pendant la séquence du mode d'accessibilité ;
- de configuration de l'écran pour détecter la position du doigt du titulaire de carte lorsque ledit titulaire de carte déplace son doigt sur ledit écran pour sélectionner chaque chiffre de son code PIN en déplaçant son doigt sur ledit écran ;

- d'envoi, par l'intermédiaire du casque (2), de signaux audio préenregistrés correspondant à chaque position du doigt pour aider le titulaire de carte à choisir les chiffres de son code PIN.

Dans certains modes de réalisation, l'étape d'exécution du mode d'accessibilité sur le dispositif mobile (3) du titulaire de carte peut comprendre les étapes :

- de contrôle si un casque (2) est enfiché ou non dans le connecteur jack audio dudit dispositif mobile (3) ;
- de demande de la connexion d'un casque (2) au dispositif mobile (3), si aucun casque (2) n'est enfiché ;
- de lancement du mode d'accessibilité pour l'entrée du code PIN une fois qu'un casque (2) est enfiché.

Dans certains modes de réalisation, le procédé pour l'identification sécurisée d'un titulaire de carte comprend au moins les étapes :

- de génération d'une « chaîne de touches » comprenant un ensemble de touches (20) ne devant pas être affichées à des positions sur l'écran (14) du terminal (1) pour l'entrée du PIN/de la SNL ;
- de détection de la longueur ou de l'orientation du déplacement du doigt sur l'écran et de transmission d'un signal correspondant à la longueur d ou à l'angle d'orientation pour indiquer qu'un déplacement a lieu ou non en fonction de la valeur de ladite longueur d ou dudit angle d'orientation comparée à une valeur de seuil mémorisée ;
- de récupération, lors de la réception d'un signal indiquant un déplacement, dans le « fichier de chaînes » mémorisé, d'une

« chaîne de touches » de manière à attribuer une valeur de touche correspondant à la longueur d ou à l'angle d'orientation du déplacement du doigt, et de sélection, parmi les signaux audio préenregistrés correspondant à chaque touche de la « chaîne de touches », du son correspondant à la touche attribuée au déplacement et d'émission de celui–ci par l'intermédiaire du connecteur de fiche vers le casque de titulaire de carte (2) ;

- de réitération des étapes de détection et de récupération jusqu'à ce que le doigt soit retiré de l'écran (14) ;
- de mémorisation de la dernière valeur lors du retrait du doigt en tant que chiffre du PIN/de la SNL.

Dans certains modes de réalisation, le procédé pour l'identification sécurisée comprend également au moins les étapes :

- de génération d'un ensemble de données correspondant à diverses positions sur l'écran (14) ;
- de génération de la « chaîne de touches » à un emplacement de l'écran sur la base d'un sous–ensemble de l'ensemble de données de diverses positions généré.

La présente demande décrit diverses caractéristiques techniques et divers avantages avec référence aux figures et/ou aux divers modes de réalisation. Les hommes du métier comprendront que les caractéristiques

techniques d'un mode de réalisation donné peuvent en fait être combinées avec des caractéristiques d'un autre mode de réalisation, sauf spécification contraire, ou sauf si la combinaison ne fournit pas une solution à au moins l'un des problèmes techniques mentionnés dans la présente demande. De plus, les caractéristiques techniques décrites dans un mode de réalisation donné peuvent être isolées des autres caractéristiques techniques de ce mode de réalisation, sauf spécification contraire.

Il doit être évident aux hommes du métier que la présente invention permet la réalisation de modes de réalisation en de nombreuses formes spécifiques sans s'écarter du domaine d'application de l'invention telle que revendiquée. Par conséquent, les présents modes de réalisation doivent être considérés à titre d'illustration, mais peuvent être modifiés dans le domaine défini par la protection demandée, et l'invention ne doit pas être limitée aux détails donnés ci–dessus.

REVENDICATIONS

1. Terminal portable de paiement ou de point de vente avec un connecteur jack pour une transaction sécurisée comprenant au moins :

- une première mémoire pour mémoriser un ensemble de programmes ou une séquence d'instructions à exécuter sur un processeur dudit terminal et au moins un ensemble de clés pour l'authentification et/ou le chiffrement ne pouvant pas être lu à partir de l'extérieur du terminal ;
- un dispositif de détection de moyens de communication filaire ou sans fil pour détecter si un titulaire de carte utilise un dispositif mobile (3) ;

le terminal (1) étant caractérisé en ce qu'il comprend au moins un module de gestion de transaction comprenant un agencement pour configurer le terminal (1) de manière à :

- lancer l'exécution d'un mode d'accessibilité sur le dispositif mobile (3) du titulaire de carte ;
- transmettre une demande au dispositif mobile pour envoyer un code PIN au terminal (1) ; et
- lors de la réception d'une communication du dispositif mobile (3) comprenant des informations, déchiffrer lesdites informations pour obtenir le code PIN, au moyen de l'ensemble de clés pour l'authentification et/ou le chiffrement et valider la transaction.

2. Terminal portable de paiement ou de point de vente pour une transaction sécurisée selon la revendication 1, caractérisé en ce que, lors du lancement du mode d'accessibilité sur le dispositif mobile (3), le terminal

comprend au moins un programme pour vérifier si une application propriétaire de mode d'accessibilité est installée sur le dispositif mobile, ladite application étant téléchargée à partir d'un portail de téléchargement d'applications, et exécuter une authentification de ladite application de mode d'accessibilité installée au moyen de l'ensemble de clés pour l'authentification et/ou le chiffrement mémorisé dans la première mémoire.

3. Terminal portable de paiement ou de point de vente pour une transaction sécurisée selon les revendications 1 et 2, caractérisé en ce qu'il comprend au moins un système d'exploitation (OS) pour la création d'une machine virtuelle, si, lors du lancement du mode d'accessibilité sur le dispositif mobile (3), le terminal détermine qu'aucune application de mode d'accessibilité n'est installée sur ledit dispositif mobile, ladite machine virtuelle étant transmise au dispositif mobile (3) du titulaire de carte, lorsque ledit dispositif mobile (3) est détecté au moyen du dispositif de détection de moyens de communication filaire/sans fil du terminal, de manière à être installée sur ledit dispositif mobile (3).

4. Terminal portable de paiement ou de point de vente pour une transaction sécurisée selon la revendication 3, caractérisé en ce qu'il comprend au moins une application instantanée qui est poussée à partir du terminal dans la machine virtuelle s'exécutant sur le dispositif mobile (3), pour exécuter le mode d'accessibilité sur le dispositif mobile (3) du titulaire de carte.

5. Terminal portable de paiement pour une transaction sécurisée selon la revendication 1, caractérisé en ce qu'il comprend :

- une application de mode d'accessibilité mémorisée dans la première mémoire et mettant en œuvre la séquence entière du mode d'accessibilité du terminal pour permettre au titulaire de carte de valider une transaction sur l'écran (14) du terminal ;
- un agencement d'authentification pour mettre en œuvre un processus d'authentification pour les titulaires de carte en

entrant un code PIN ou une séquence de nombres et de lettres (SNL) ;

- un capteur de proximité pour détecter la présence d'un titulaire de carte ;
- un premier dispositif de détection (11) pour détecter la présence, dans le connecteur, d'une fiche enfichée pour connecter un casque de titulaire de carte et comprenant un agencement pour produire un signal électrique pour déclencher l'exécution du mode d'accessibilité ;
- un deuxième dispositif de détection (101) pour détecter la position du doigt sur l'écran (14), chaque fois qu'un doigt du propriétaire du casque (2) touche l'écran (14).

6. Terminal portable de paiement pour une transaction sécurisée selon la revendication 1, caractérisé en ce que le module de gestion de transaction comprend un agencement pour au moins configurer ledit terminal pour exécuter, si le dispositif mobile (3) de titulaire de carte n'est pas détecté par le dispositif de détection de moyens de communication filaire/sans fil, un mode d'accessibilité, dans lequel, au moins, le terminal :

- demande, à l'aide de moyens de notification, la connexion d'un casque (2) dans le connecteur jack dudit terminal ;
- exécute la première application de mode d'accessibilité, après la détection, au moyen du premier dispositif de détection, d'une fiche enfichée pour connecter un casque de titulaire de carte (2), l'écran du terminal étant brouillé et maintenu en noir pendant la séquence entière du mode d'accessibilité ;
- configure, au moyen d'un ensemble d'agencements, l'écran pour détecter la position du doigt du titulaire de carte lorsque ledit titulaire de carte déplace son doigt sur ledit écran pour

sélectionner chaque chiffre de son code PIN en déplaçant son doigt sur ledit écran ;

- envoie, par l'intermédiaire du casque (2), de signaux audio préenregistrés correspondant à chaque position du doigt pour aider le titulaire de carte à choisir les chiffres de son code PIN.

7. Terminal portable de paiement pour une transaction sécurisée selon les revendications 1 à 6, caractérisé en ce qu'il comprend au moins un moyen de notification qui est un agencement audio pour émettre un message vocal par l'intermédiaire d'un haut–parleur, inclus dans ledit terminal, et/ou envoyer ledit message vocal au dispositif mobile (3) du titulaire de carte.

8. Terminal portable de paiement pour une transaction sécurisée selon les revendications 1 à 6, caractérisé en ce qu'il comprend un moyen de notification qui est un module de messages textuels pour afficher des informations sur l'écran (14) dudit terminal ou envoyer lesdites informations sur l'écran du dispositif mobile (3) du titulaire de carte.

9. Terminal portable de paiement pour une transaction sécurisée selon les revendications 7 et 8, caractérisé en ce qu'il comprend à la fois un module de messages textuels et un agencement audio pour envoyer des informations au titulaire de carte par l'intermédiaire dudit terminal ou dudit dispositif mobile (3) du titulaire de carte.

10. Terminal portable de paiement ou de point de vente pour une transaction sécurisée selon les revendications 3 et 4, caractérisé en ce qu'il comprend un ensemble de clés mémorisé dans une sixième mémoire, incluse dans le terminal (1), ledit ensemble de clés ne pouvant pas être lu à partir de l'extérieur du terminal et correspondant à l'ensemble de clés mémorisé dans la première mémoire, l'ensemble de clés mémorisé dans la sixième mémoire étant poussé avec l'application instantanée sur la machine virtuelle s'exécutant sur le dispositif mobile (3) du titulaire de carte, ledit ensemble de clés de la sixième mémoire étant utilisé pour l'échange sécurisé de données et/ou d'informations entre le terminal et le dispositif mobile (3) du

titulaire de carte et enregistré dans une mémoire du dispositif mobile (3) du titulaire de carte où il ne peut pas être lu à partir de l'extérieur.

11. Terminal portable de paiement ou de point de vente pour une transaction sécurisée selon la revendication 10, caractérisé en ce qu'il comprend au moins un ensemble de programmes envoyé au dispositif mobile (3) du titulaire de carte pour supprimer la machine virtuelle et/ou l'application instantanée s'exécutant sur ladite machine virtuelle, dudit dispositif mobile (3) après la validation de la transaction.

12. Terminal portable de paiement ou de point de vente pour une transaction sécurisée selon la revendication 3, caractérisé en ce que la machine virtuelle comprend au moins un ensemble de programmes pour simuler chaque composant du terminal de paiement (1) et leur connexion de manière à mettre en œuvre, lors de l'exécution de l'application instantanée, un mode d'accessibilité comprenant au moins le mode d'accessibilité tel qu'exécuté par ledit terminal (1).

13. Terminal portable de paiement ou de point de vente pour une transaction sécurisée selon l'une des revendications 4, 10, 11 ou 12, caractérisé en ce que l'application instantanée comprend un ensemble de programmes pour simuler les fonctionnalités de chaque composant du terminal de paiement (1) et sa connexion de manière à mettre en œuvre un mode d'accessibilité comprenant au moins le mode d'accessibilité tel qu'exécuté par ledit terminal (1).

14. Terminal portable de paiement ou de point de vente pour une transaction sécurisée selon l'une des revendications 4, 10, 11, 12 ou 13, caractérisé en ce que l'application instantanée lancée par le terminal sur le dispositif mobile (3) du titulaire de carte comprend au moins un programme dont l'exécution sur le dispositif mobile (3) du titulaire de carte permet de répondre à la demande d'authentification et/ou de code PIN envoyée par le terminal.

15. Terminal portable de paiement ou de point de vente pour une transaction sécurisée selon l'une des revendications 4, 10, 11, 12, 13 ou 14, caractérisé en ce que l'application instantanée lancée par le terminal sur le dispositif mobile (3) du titulaire de carte comprend au moins un programme dont l'exécution sur le dispositif mobile (3) du titulaire de carte récupère, dans la mémoire dudit dispositif mobile (3) du titulaire de carte, l'ensemble de clés enregistré, permettant audit dispositif mobile (3) de répondre à la demande d'authentification et/ou de code PIN envoyée par le terminal.

16. Terminal portable de paiement ou de point de vente pour une transaction sécurisée selon les revendications 1 à 15, caractérisé en ce qu'il comprend une mémoire dans laquelle les informations de transaction relatives au moins au montant de la transaction et/ou au marchand sont enregistrées, lesdites informations étant transmises avec la demande de code PIN au dispositif mobile (3) du titulaire de carte.

17. Terminal portable de paiement pour une transaction sécurisée selon l'une des revendications 4, 10 à 15, caractérisé en ce que l'application instantanée s'exécutant sur le dispositif mobile (3) du titulaire de carte comprend au moins un ensemble de programmes pour configurer le dispositif mobile (3) du titulaire de carte, lorsqu'au moins une demande d'entrée de code PIN a été envoyée par ledit terminal, de manière à :

- vérifier si un casque (2) est enfiché ou non dans le connecteur jack audio dudit dispositif mobile (3) ;
- demander, à l'aide d'un moyen de notification, la connexion d'un casque (2) au dispositif mobile (3), si aucun casque (2) n'est enfiché ;
- lancer le mode d'accessibilité pour l'entrée du code PIN une fois qu'un casque (2) est enfiché.

18. Terminal portable de paiement pour une transaction sécurisée selon l'une des revendications 4, 10 à 17, caractérisé en ce que l'application instantanée s'exécutant sur le dispositif (3) mobile du titulaire de carte

comprend au moins un programme pour récupérer l'ensemble de clés dans la mémoire dudit dispositif mobile (3) de manière à chiffrer le code PIN entré par le titulaire de carte avant son envoi au terminal pour la validation de la transaction.

19. Terminal portable de paiement pour une transaction sécurisée selon l'une des revendications 4, 10 à 18, caractérisé en ce que l'application instantanée s'exécutant sur le dispositif (3) mobile du titulaire de carte comprend au moins un programme pour brouiller et maintenir en noir l'écran du dispositif mobile (3) du titulaire de carte pendant la séquence entière du mode d'accessibilité.

20. Terminal portable de paiement pour une transaction sécurisée selon l'une des revendications 4, 10 à 19, caractérisé en ce que l'application instantanée comprend au moins un programme configurant l'écran du dispositif mobile (3) du titulaire de carte pour détecter la position du doigt du titulaire de carte lorsque ledit titulaire de carte déplace son doigt sur ledit écran pour sélectionner chaque chiffre de son code PIN en déplaçant son doigt sur ledit écran.

21. Terminal portable de paiement pour une transaction sécurisée selon l'une des revendications 4, 10 à 20, caractérisé en ce que l'application instantanée comprend au moins un programme configurant le dispositif mobile (3) du titulaire de carte pour envoyer, par l'intermédiaire du casque (2), les signaux audio préenregistrés correspondant à chaque position du doigt pour aider le titulaire de carte à choisir les chiffres de son code PIN, lesdits signaux audio étant transmis au dispositif mobile (3) du titulaire de carte avec les informations de transaction et le code PIN demandés par le terminal (1).

22. Terminal portable de paiement pour une transaction sécurisée selon l'une des revendications 4, 10 à 21, caractérisé en ce que l'application instantanée comprend au moins un programme pour configurer le dispositif

mobile (3) du titulaire de carte de manière à permettre au titulaire de carte d'entrer son code PIN au moyen d'une application tiers autorisée.

23. Procédé pour l'identification sécurisée d'un titulaire de carte avec un terminal portable de paiement ou de point de vente (1) selon la revendication 1, ledit procédé comprenant au moins les étapes :

- de détection de moyens de communication filaire/sans fil d'un dispositif mobile (3) ;

le procédé étant caractérisé en ce que, si le dispositif mobile de titulaire de carte (3) est détecté, il comprend au moins l'étape de configuration du terminal (1) pour :

- lancer un mode d'accessibilité sur le dispositif mobile (3) du titulaire de carte ;
- transmettre une demande au dispositif mobile pour envoyer un code PIN au terminal (1) ; et
- lors de la réception d'une communication du dispositif mobile comprenant des informations, déchiffrer lesdites informations pour obtenir le code PIN et valider la transaction.

24. Procédé pour l'identification sécurisée d'un titulaire de carte selon la revendication 23, caractérisé en ce qu'il comprend au moins, lors du lancement du mode d'accessibilité, les étapes :

- de vérification si une application propriétaire de mode d'accessibilité de est installée sur le dispositif mobile ;
- d'exécution d'une authentification de ladite application de mode d'accessibilité installée.

25. Procédé pour l'identification sécurisée d'un titulaire de carte selon la revendication 23, caractérisé en ce qu'il comprend au moins les étapes :

- de création d'une machine virtuelle si, lors du lancement du mode d'accessibilité sur le dispositif mobile (3), le terminal détermine qu'aucune application de mode d'accessibilité n'est installée sur ledit dispositif mobile ;
- de transmission de ladite machine virtuelle au dispositif mobile (3) du titulaire de carte;
- de poussée d'une application instantanée sur ladite machine virtuelle pour exécuter le mode d'accessibilité sur le dispositif mobile (3).

26. Procédé pour l'identification sécurisée d'un titulaire de carte selon la revendication 23, caractérisé en ce qu'il comprend au moins l'étape de chiffrement au moins du code PIN ou d'une partie du code PIN sur le dispositif mobile (3) du titulaire de carte avant sa transmission au terminal pour validation.

27. Procédé pour l'identification sécurisée d'un titulaire de carte selon la revendication 23, caractérisé en ce que, si le dispositif mobile (3) n'est pas détecté, il comprend au moins les étapes :

- de demande, au moyen d'une notification, sur l'écran du terminal, de la connexion d'un casque (2) dans le connecteur de fiche dudit terminal ;
- de détection de la présence d'une fiche enfichée dans le connecteur du terminal (1) pour la connexion d'un casque (2) du titulaire de carte;
- de déclenchement de l'exécution d'un premier mode d'accessibilité permettant au titulaire de carte de s'identifier ;
- de brouillage et de maintien de l'écran en noir pendant la séquence du mode d'accessibilité ;
- de configuration de l'écran pour détecter la position du doigt du titulaire de carte lorsque ledit titulaire de carte déplace son doigt

sur ledit écran pour sélectionner chaque chiffre de son code PIN en déplaçant son doigt sur ledit écran ;

- d'envoi, par l'intermédiaire du casque (2), de signaux audio préenregistrés correspondant à chaque position du doigt pour aider le titulaire de carte à choisir les chiffres de son code PIN.

28. Procédé pour l'identification sécurisée d'un titulaire de carte selon la revendication 23, caractérisé en ce que l'étape d'exécution du mode d'accessibilité sur le dispositif mobile (3) du titulaire de carte comprend les étapes :

- de contrôle si un casque (2) est enfiché ou non dans le connecteur jack audio dudit dispositif mobile (3) ;
- de demande de la connexion d'un casque (2) au dispositif mobile (3), si aucun casque (2) n'est enfiché ;
- de lancement du mode d'accessibilité pour l'entrée du code PIN une fois qu'un casque (2) est enfiché.

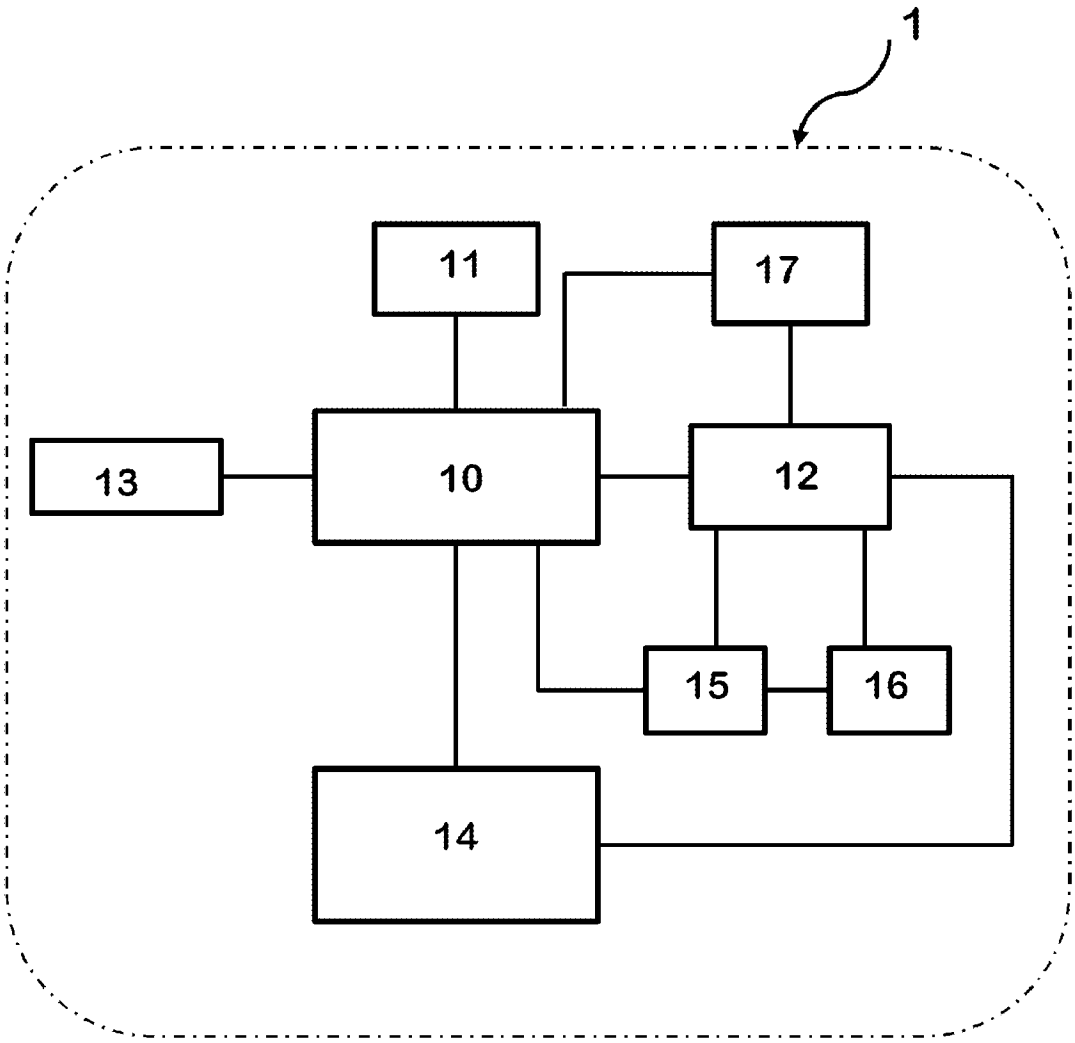

Figure 1A

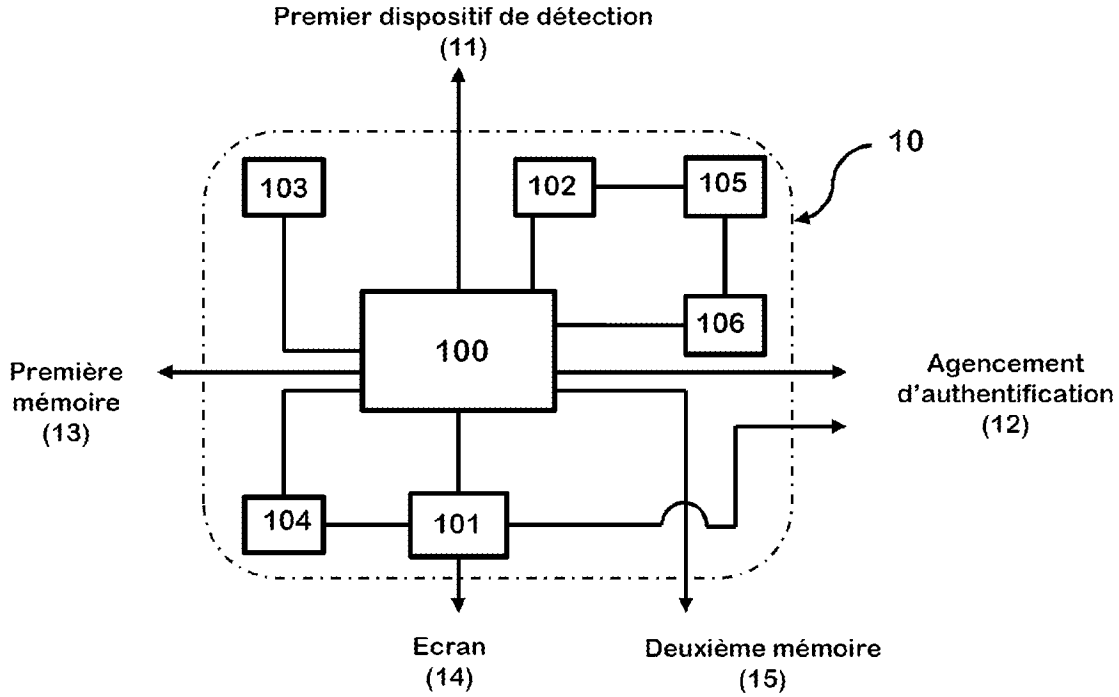
Premier dispositif de détection
(11)
10
103
102
105
106
100
Première
mémoire
(13)
Agencement
d'authentification
(12)
104
101
Ecran
(14)
Deuxième mémoire
(15)

Figure 1B

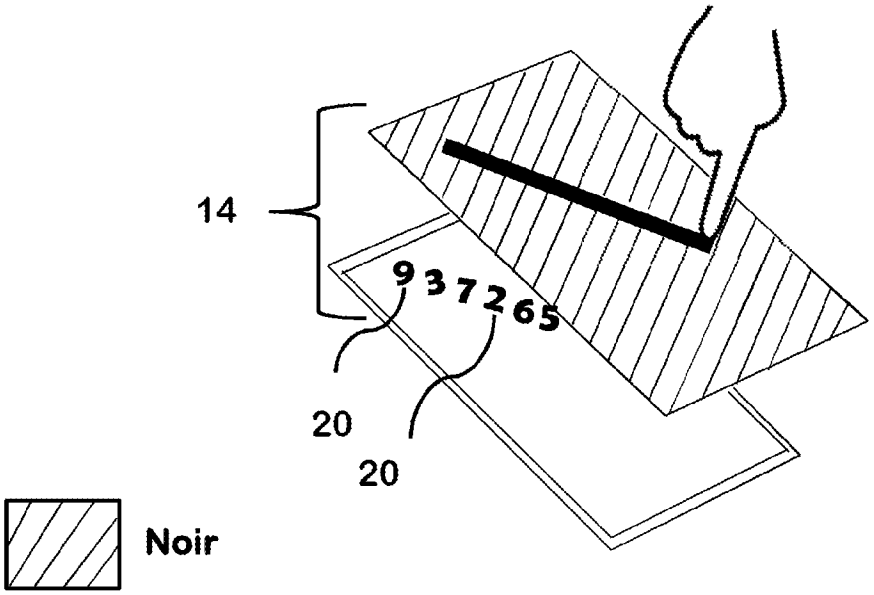

Figure 2a

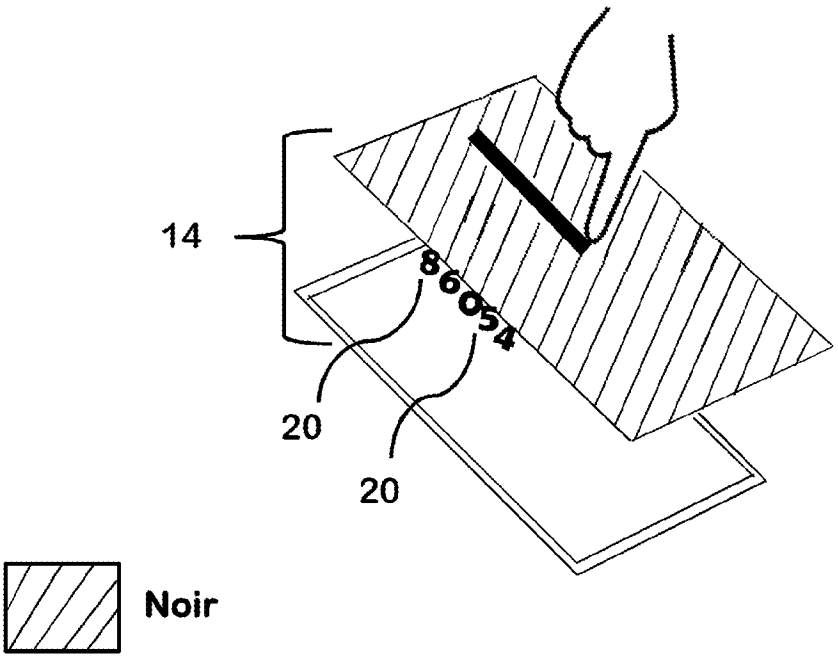

Figure 2b

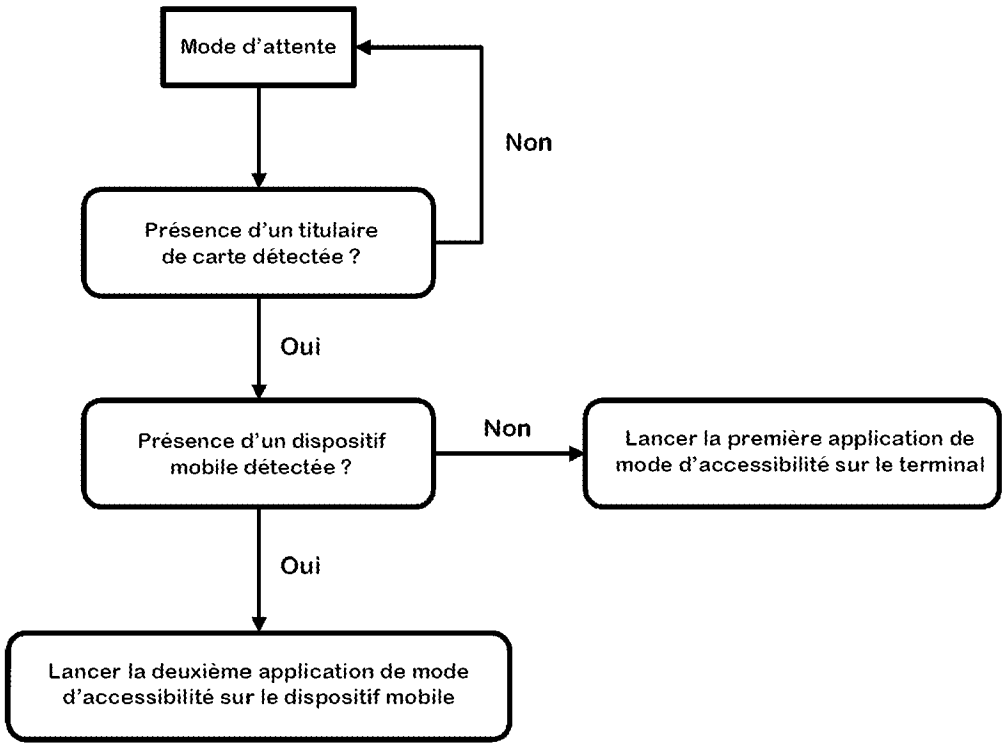
Mode d'attente
Non
Présence d'un titulaire de carte détectée ?
Oui
Présence d'un dispositif mobile détectée ?
Non
Lancer la première application de mode d'accessibilité sur le terminal
Oui
Lancer la deuxième application de mode d'accessibilité sur le dispositif mobile

Figure 3A

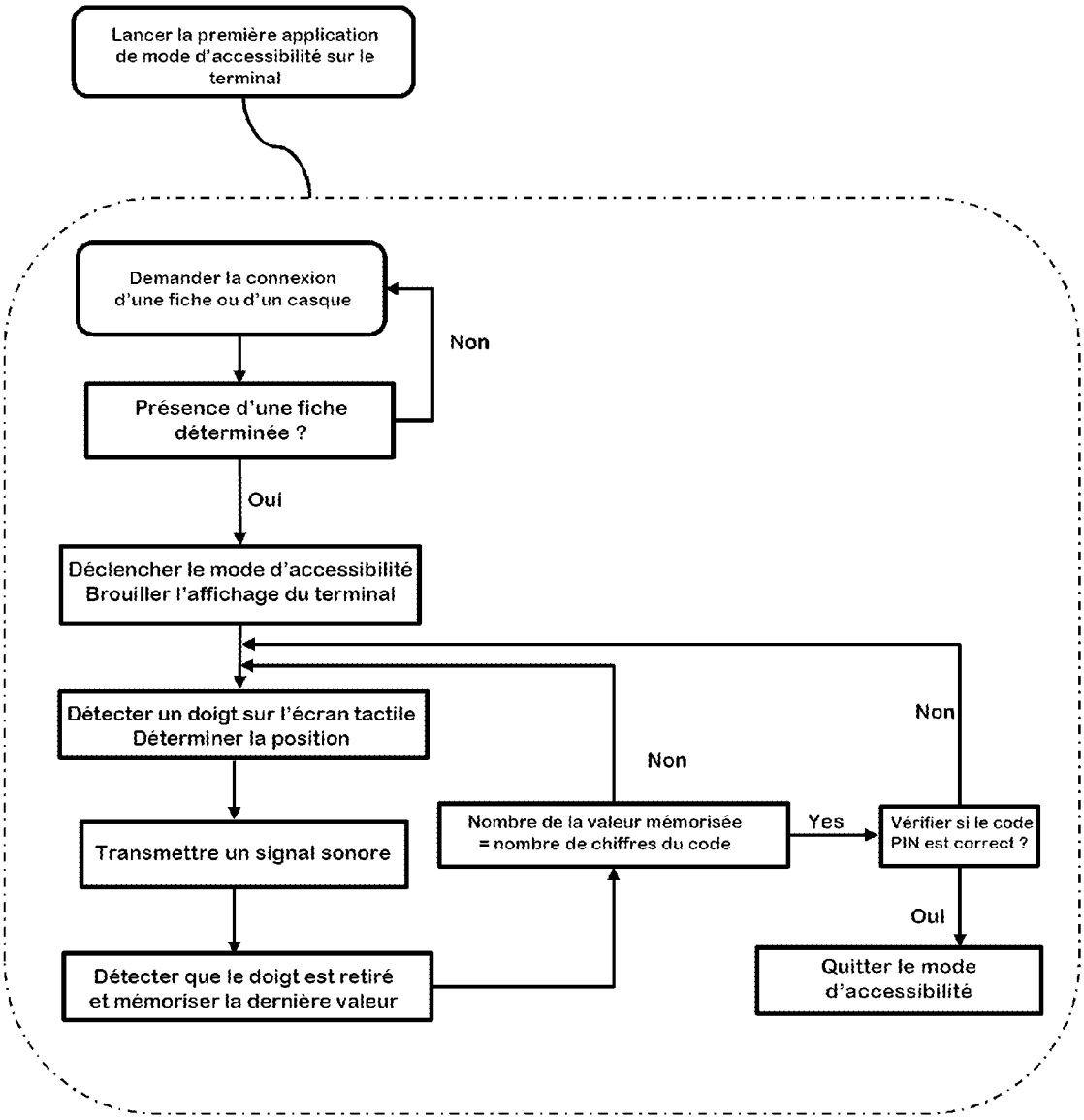
Lancer la première application de mode d'accessibilité sur le terminal
Demander la connexion d'une fiche ou d'un casque
Non
Présence d'une fiche déterminée ?
Oui
Déclencher le mode d'accessibilité
Brouiller l'affichage du terminal
Détecter un doigt sur l'écran tactile
Déterminer la position
Transmettre un signal sonore
Détecter que le doigt est retiré et mémoriser la dernière valeur
Non
Nombre de la valeur mémorisée = nombre de chiffres du code
Yes
Vérifier si le code PIN est correct ?
Non
Oui
Quitter le mode d'accessibilité

Figure 3B

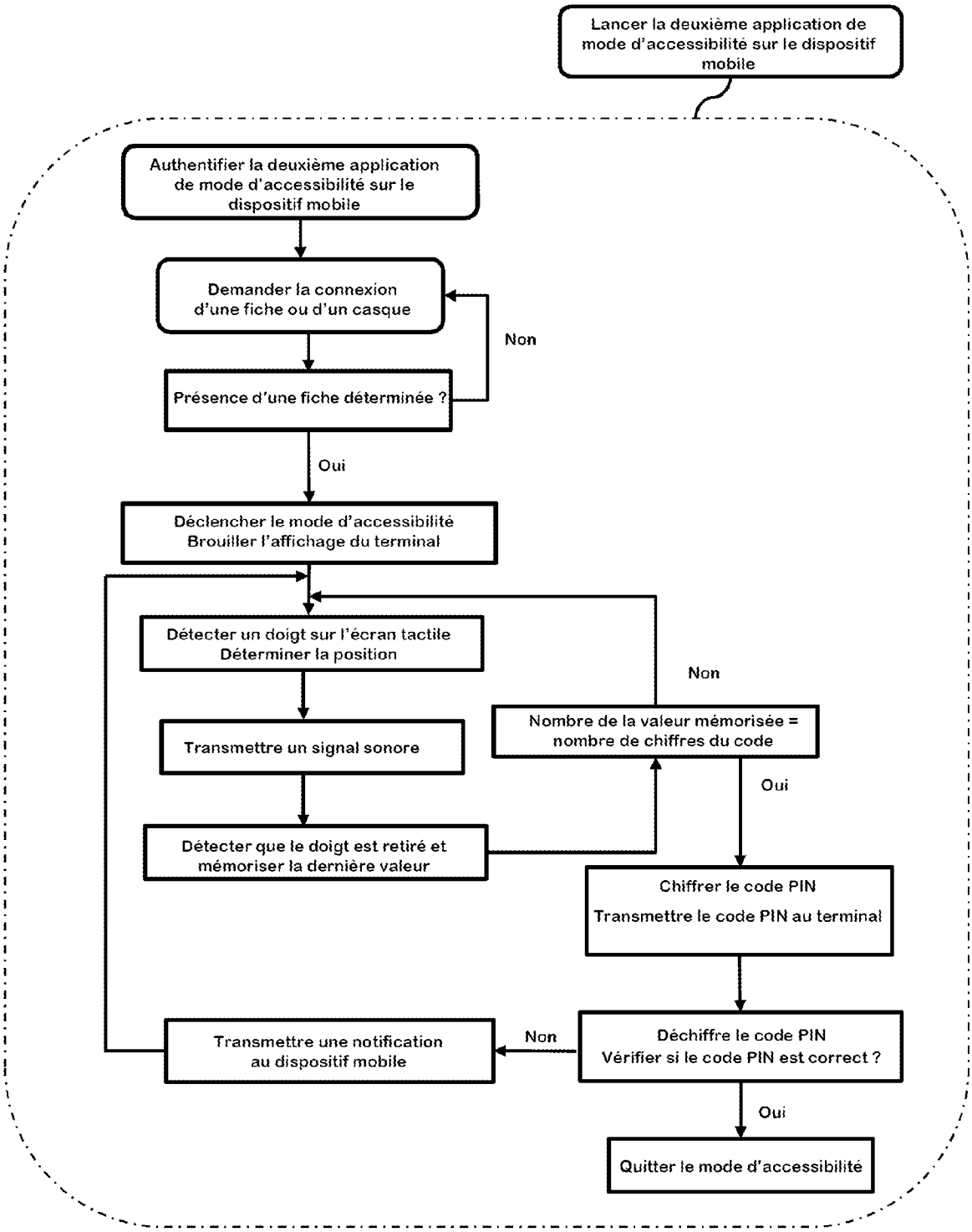
Lancer la deuxième application de mode d'accessibilité sur le dispositif mobile
Authentifier la deuxième application de mode d'accessibilité sur le dispositif mobile
Demander la connexion d'une fiche ou d'un casque
Non
Présence d'une fiche déterminée ?
Oui
Déclencher le mode d'accessibilité
Brouiller l'affichage du terminal
Détecter un doigt sur l'écran tactile
Déterminer la position
Non
Nombre de la valeur mémorisée = nombre de chiffres du code
Transmettre un signal sonore
Oui
Détecter que le doigt est retiré et mémoriser la dernière valeur
Chiffrer le code PIN
Transmettre le code PIN au terminal
Transmettre une notification au dispositif mobile
Non
Déchiffre le code PIN
Vérifier si le code PIN est correct ?
Oui
Quitter le mode d'accessibilité

Figure 3C

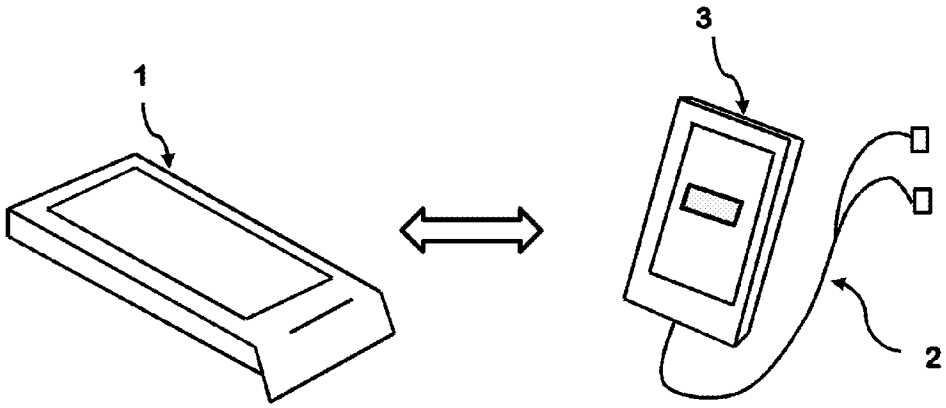

Figure 4

TRAITE DE COOPERATION EN MATIERE DE BREVETS

RAPPORT DE RECHERCHE DE TYPE INTERNATIONAL ÉTABLI EN VERTU DE L'ARTICLE XI.23., §10 DU CODE DE DROIT ÉCONOMIQUE BELGE

IDENTIFICATION DE LA DEMANDE INTERNATIONALE	REFERENCE DU DEPOSANT OU DU MANDATAIRE
	WORLDLINE/19/BE
Demande nationale belge n° **201805368**	Date du dépôt **04-06-2018**
	Date de priorité revendiquée
Déposant (Nom) **WORLDINE SA**	
Date de la requête d'une recherche de type international **21-07-2018**	Numéro attribué par l'administration chargée de la recherche internationale à la requête d'une recherche de type international **SN71643**

I. CLASSEMENT DE L'OBJET DE LA DEMANDE (en cas de plusieurs symboles de la classification, les indiquer tous)

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

G06F21/31;G06Q20/32;G06Q20/38;G06Q20/40

II. DOMAINES RECHERCHES

Documentation minimale consultée

Système de classification	Symboles de la classification
IPC	**G06F;G06Q**

Documentation consultée autre que la documentation minimale dans la mesure où ces documents fort partie des domaines consultés

III. ☐ **IL A ETE ESTIME QUE CERTAINES REVENDICATIONS NE POUVAIENT FAIRE L'OBJET D'UNE RECHERCHE** (Observations sur la feuille supplémentaire)

IV. ☐ **ABSENCE D'UNITE DE L'INVENTION ET/OU CONSTATATION RELATIVE A L'ETENDUE DE LA RECHERCHE** (Observations sur la feuille supplémentaire)

RAPPORT DE RECHERCHE DE TYPE INTERNATIONAL

Demande de recherche No
BE 201805368

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06F21/31 G06Q20/32 G06Q20/38 G06Q20/40
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 G06Q

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 réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 2013/328801 A1 (QUIGLEY OLIVER S C [US] ET AL) 12 décembre 2013 (2013-12-12) * abrégé * * alinéas [0003] - [0004], [0006], [0008] - [0010], [0012], [0014], [0017] - [0031], [0045], [0065], [0074] - [0087] * -----	1-28
X	US 7 146 577 B2 (NCR CORP [US]) 5 décembre 2006 (2006-12-05) * colonne 1, ligne 66 - colonne 2, ligne 12 * * colonne 2, ligne 66 - colonne 12, ligne 7 * * colonne 14, lignes 36-43 * ----- -/--	1-28

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] 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 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, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt ou la date de priorité et n'appartenenant 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 isolement

"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 de type international a été effectivement achevée	Date d'expédition du rapport de recherche de type international
7 septembre 2018	

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Thareau-Berthet, N

1

Formulaire PCT/ISA/201 (deuxième feuille) (Janvier 2004)

C.(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 2017/286938 A1 (BROWN JEREMY T [US] ET AL) 5 octobre 2017 (2017-10-05) * alinéas [0005] - [0008], [0022] - [0171] * -----	1-28
X	US 2016/224113 A1 (DAY PHILIP N [GB] ET AL) 4 août 2016 (2016-08-04) * alinéas [0033], [0044] * -----	21

1

RAPPORT DE RECHERCHE DE TYPE INTERNATIONAL

Renseignements relatifs aux membres de familles de brevets

Demande de recherche n
BE 201805368

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2013328801	A1 12-12-2013	CA 2876364 A1	19-12-2013
		EP 2859492 A2	15-04-2015
		EP 3296908 A1	21-03-2018
		US 2013328801 A1	12-12-2013
		US 2013332360 A1	12-12-2013
		US 2013332367 A1	12-12-2013
		US 2013333011 A1	12-12-2013
		US 2016275515 A1	22-09-2016
		WO 2013188599 A2	19-12-2013
US 7146577	B2 05-12-2006	AUCUN	
US 2017286938	A1 05-10-2017	CN 106233314 A	14-12-2016
		EP 3149679 A1	05-04-2017
		KR 20160137640 A	30-11-2016
		KR 20180021223 A	28-02-2018
		US 2015348009 A1	03-12-2015
		US 2016300211 A1	13-10-2016
		US 2017286938 A1	05-10-2017
		WO 2015183412 A1	03-12-2015
US 2016224113	A1 04-08-2016	AUCUN	

OPINION ÉCRITE

Dossier N°	Date du dépot *(jour/mois/année)*	Date de priorité *(jour/mois/année)*	Demande n°
SN71643	04.06.2018		BE201805368

Classification internationale des brevets (CIB)
INV. G06F21/31 G06Q20/32 G06Q20/38 G06Q20/40

Déposant
WORLDINE SA

La présente opinion contient des indications et les pages correspondantes relatives aux points suivants :

- ☒ Cadre n° I Base de l'opinion
- ☐ Cadre n° II Priorité
- ☐ Cadre n° III Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
- ☐ Cadre n° IV Absence d'unité de l'invention
- ☒ Cadre n° V Déclaration motivée quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
- ☐ Cadre n° VI Certains documents cités
- ☐ Cadre n° VII Irrégularités dans la demande
- ☐ Cadre n° VIII Observations relatives à la demande

Examinateur
Thareau-Berthet, N

Demande n°

OPINION ÉCRITE

BE201805368

Cadre n° I Base de l'opinion

1. Cette opinion a été établie sur la base des revendications déposées avant le commencement de la recherche.

2. En ce qui concerne **la ou les séquences de nucléotides ou d'acides aminés** divulguées dans la demande, le cas échéant, cette opinion a été effectuée sur la base des éléments suivants :

   a. Nature de l'élément:

   ☐ un listage de la ou des séquences

   ☐ un ou des tableaux relatifs au listage de la ou des séquences

   b. Type de support:

   ☐ sur papier

   ☐ sous forme électronique

   c. Moment du dépôt ou de la remise:

   ☐ contenu(s) dans la demande telle que déposée

   ☐ déposé(s) avec la demande, sous forme électronique

   ☐ remis ultérieurement

3. ☐ De plus, lorsque plus d'une version ou d'une copie d'un listage des séquences ou d'un ou plusieurs tableaux y relatifs a été déposée, les déclarations requises selon lesquelles les informations fournies ultérieurement ou au titre de copies supplémentaires sont identiques à celles initialement fournies et ne vont pas au-delà de la divulgation faite dans la demande internationale telle que déposée initialement, selon le cas, ont été remises.

4. Commentaires complémentaires :

Demande n°

OPINION ÉCRITE

BE201805368

Cadre n° V Opinion motivée quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui :	Revendications	1-28
	Non :	Revendications	
Activité inventive	Oui :	Revendications	
	Non :	Revendications	1-28
Possibilité d'application industrielle	Oui :	Revendications	1-28
	Non :	Revendications	

2. Citations et explications

voir feuille séparée

Ad point V

Déclaration motivée quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle ; citations et explications à l'appui de cette déclaration

1 Il est fait référence aux documents suivants :

D1 US 2013/328801 A1 (QUIGLEY OLIVER S C [US] ET AL) 12 décembre 2013 (2013-12-12)

D2 US 7 146 577 B2 (NCR CORP [US]) 5 décembre 2006 (2006-12-05)

D3 US 2017/286938 A1 (BROWN JEREMY T [US] ET AL) 5 octobre 2017 (2017-10-05)

D4 US 2016/224113 A1 (DAY PHILIP N [GB] ET AL) 4 août 2016 (2016-08-04)

2 La présente demande ne remplit pas les conditions de brevetabilité, pour les raisons suivantes:

2.1 Le document D1, qui est considéré comme l'état de la technique le plus proche de l'objet de la revendication 1, divulgue un terminal portable de paiement ou de point de vente ("card reader", par. 3-4, 6, 8-10, 12, 14, 17-31), avec un connecteur jack ("audio port", audio jack", par. 45, 47) pour une transaction sécurisée comprenant au moins :

• une première mémoire ("chip on the card", par. 45, 65) pour mémoriser un ensemble de programmes ou une séquence d'instructions à exécuter sur un processeur dudit terminal ("receiving verification from the chip that the passcode matches the embedded PIN values on the card", par. 45, 65) et au moins un ensemble de clés pour l'authentification et/ou le chiffrement ne pouvant pas être lu à partir de l'extérieur du terminal ("cryptographic key", "public key", "private key", par. 16-30, 74-87);

• un dispositif ~~de détection~~ de moyens de communication filaire ou sans fil ("Bluetooth technology or a WiFi hotspot", par. 45) pour ~~détecter si un titulaire de carte utilise~~ un dispositif mobile ("mobile computing device", "mobile device", par. 45);

le terminal étant caractérisé en ce qu'il comprend au moins un module de gestion de transaction comprenant un agencement pour configurer le terminal de manière à :

• ~~lancer un mode d'accessibilité sur le dispositif mobile du titulaire de carte~~ ;

• transmettre une demande au dispositif mobile pour envoyer un code PIN au terminal ("The card reader 110 sends a PIN request to the mobile device 102", par. 45); et

• lors de la réception d'une communication du dispositif mobile comprenant des informations, déchiffrer lesdites informations pour obtenir le code PIN, au moyen de l'ensemble de clés pour l'authentification et/ou le chiffrement et valider la transaction ("The mobile device receives a PIN from the user, e.g., entered through a user interface of the mobile device, e.g., a touch-screen display, and sends the PIN to the card reader for confirmation", "The card reader can read, on the card, a chip that contains an embedded PIN. The card reader compares the entered PIN to the embedded PIN.If the PINs match, the card reader sends a confirmation to the mobile device", par. 45).

L'objet de la revendication 1 diffère du système de D1 en ce que :
(i) le terminal comprends un moyen de détection pour détecter si le titulaire utilise un dispositif mobile; et
(ii) le terminal lance un mode d'accessibilité sur le dispositif mobile du titulaire.

Les caractéristiques (i) et (ii) étant simplement juxtaposées et n'ayant aucun effet synergétique, leurs contributions respectives à une activité inventive peuvent donc être analysées séparément.

Il est considéré comme faisant partie de la la connaissance générale informatique de déterminer la présence d'un dispositif mobile (voir, par exemple D3, par. 78, "RF interface 408 can implement a Bluetooth LE (Low energy) proximity sensor 409 that supports proximity detection through an estimation of signal strength and/or other protocols for determining proximity to another electronic device"). Cette différence correspond ainsi à un choix d'implémentation évident que la personne du métier considérerait sans qu'une activité inventive soit impliquée.

Lancer un mode d'accessibilité quand un dispositif mobile du titulaire de carte est détecté correspond à une caractéristique administrative non-technique qui est donc non pertinente pour l'évaluation de l'étape inventive.

Par conséquent, l'objet de la revendication 1 n'implique pas une activité inventive.

2.2 L'objet de la revendication indépendante 23 correspond à un procédé correspondant au dispositif de la revendication 1. L'objection de manque d'activité inventive s'applique donc de manière similaire à l'objet de la revendication indépendante 23 qui n'implique pas une activité inventive non plus.

2.3 Les revendications dépendantes 2-22 et 24-28 ne contiennent aucune caractéristique technique qui, en combinaison avec celles de l'une quelconque des revendications à laquelle elles se réfèrent, définisse un objet qui satisfasse aux exigences de l'activité inventive car elles correspondent à des caractéristiques déjà connues de D1 (i.e.détection d'un doigt sur l'écran, sélection du code PIN par déplacement du doigt sur l'écran, application permettant de répondre à la demande l'authentification et/ou de code PIN envoyée par le terminal, récupération des clés enregistrées pour permettre de répondre à la demande d'authentification et/ou de code PIN, récupération des clés enregistrées pour permettre de chiffrer le code PIN entré, par. 65, 78-79, 84-87),
ou à des caractéristiques bien connues de l'état de la technique (i.e. capteur de proximité, voir par exemple D3, par. 78, envoyer des signaux audio préenregistrés pour aider le titulaire à choisir son code PIN, voir par exemple, voir par exemple D2, col. 14, l. 36-43, ou D4, par. 33, 44),
ou des détails de design, des possibilités évidentes et des détails d'implémentation que la personne du métier choisirait, selon le cas d'espèce, sans qu'une activité inventive soit impliquée (i.e. vérification que l'application de mode accessibilité est installée, téléchargement depuis un portail, authentification de l'application, système d'exploitation pour la création de machine virtuelle, application transmise sous forme de machine virtuelle, détection d'une fiche enfichée pour connecter un casque, émission d'un message vocal par un haut parleur, messages textuels sur l'écran du terminal ou du dispositif mobile, clés mémorisées dans une sixième mémoire sécurisée, suppression du programme après validation de la transaction, simulation de chaque composant du terminal de paiement),
ou à des caractéristiques administratives non-technique non pertinences pour évaluer l'activité inventive (e.g. agencement d'authentification pour les titulaires de carte en entrant un code PIN ou une séquence de nombres et lettres (SNL), demander la connexion d'un casque, écran du terminal brouillé et maintenu en noir durant la saisie en mode d'accessibilité, enregistrement et transmission des informations de transaction comprenant au moins le montant de la transaction dans le terminal de paiement, lancer le mode d'accessibilité quand un casque est enfiché).

Par conséquent, l'objet des revendications dépendantes 2-22 et 24-28 n'implique pas une activité inventive.