ROYAUME DU MAROC

OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
---

(19)

المملكة المغربية
المكتب المغربي للملكية الصناعية و التجارية

(12) DEMANDE DE BREVET D'INVENTION

(11) N° de publication :
MA 38733 A1

(51) Cl. internationale :
H04L 9/00

(43) Date de publication :
31.10.2017

(21) N° Dépôt :
38733

(22) Date de Dépôt :
29.12.2015

(71) Demandeur(s) :
UNIVERSITÉ MOHAMMED V DE RABAT, Angle avenue Allal El Fassi et Mfadel Cherkaoui, Alirfane 8007.N.U, Rabat Rabat-Chellah (MA)

(72) Inventeur(s) :
Abdelltif Kobbane ; Mohamed Senhadji

(74) Mandataire :
KARTIT ZAID

(54) Titre : **Dispositif de mot de passe embarqué dans un smart card sans contact**

(57) Abrégé : La plupart des systèmes existants utilisent un simple mot de passe ou un code PIN pour authentifier l'utilisateur. Malgré l'omniprésence des systèmes à mot de passe, l'accès aux applications pose beaucoup de problèmes. Un mot de passe idéal doit être facile à retenir par l'utilisateur. Cependant, pour que les mots de passe soient sécurisés, ils devraient être longs et difficile à déchiffrer, en contradiction avec la première exigence. Cette situation devient excessive par la prolifération des mots de passe pour la multitude d'applications qu'un utilisateur utilise généralement, pour laquelle les meilleures pratiques de sécurité recommandent l'utilisation de différents mots de passe. D'autant plus que le mot de passe transite via le réseau pour être contrôlé par le serveur d'application. Afm de faciliter l'authentification forte, il est souvent souhaitable d'utiliser un mécanisme qui utilise ou combine deux facteurs différents, par exemple «quelque chose que vous avez" (tels que, une carte à puce) et «quelque chose que vous savez" (tels que, un mot de passe).

Abrégé

La plupart des systèmes existants utilisent un simple mot de passe ou un code PIN pour authentifier l'utilisateur. Malgré l'omniprésence des systèmes à mot de passe, l'accès aux applications pose beaucoup de problèmes. Un mot de passe idéal doit être facile à retenir par l'utilisateur. Cependant, pour que les mots de passe soient sécurisés, ils devraient être longs et difficile à déchiffrer, en contradiction avec la première exigence. Cette situation devient excessive par la prolifération des mots de passe pour la multitude d'applications qu'un utilisateur utilise généralement, pour laquelle les meilleures pratiques de sécurité recommandent l'utilisation de différents mots de passe. D'autant plus que le mot de passe transite via le réseau pour être contrôlé par le serveur d'application.

Afin de faciliter l'authentification forte, il est souvent souhaitable d'utiliser un mécanisme qui utilise ou combine deux facteurs différents, par exemple «quelque chose que vous avez" (tels que, une carte à puce) et «quelque chose que vous savez" (tels que, un mot de passe).

Titre : Dispositif de mot de passe embarqué dans une smart card sans contact

Description

La présente invention concerne des dispositifs d'authentification et d'autorisation d'accès à des applications logicielles sensibles ou à des ressources informatiques ou dans le domaine du contrôle d'accès physique à des zones très sensibles.

La plupart des systèmes existants utilisent un simple mot de passe ou un code PIN pour authentifier l'utilisateur. Malgré l'omniprésence des systèmes à mot de passe, l'accès aux applications pose beaucoup de problèmes. Un mot de passe idéal doit être facile à retenir par l'utilisateur. Cependant, pour que les mots de passe soient sécurisés, ils devraient être longs et difficile à déchiffrer, en contradiction avec la première exigence. Cette situation devient excessive par la prolifération des mots de passe pour la multitude d'applications qu'un utilisateur utilise généralement, pour laquelle les meilleures pratiques de sécurité recommandent l'utilisation de différents mots de passe. D'autant plus que le mot de passe transite via le réseau pour être contrôlé par le serveur d'application.

Afin de faciliter l'authentification forte, il est souvent souhaitable d'utiliser un mécanisme qui utilise ou combine deux facteurs différents, par exemple «quelque chose que vous avez" (tels que, une carte à puce) et «quelque chose que vous savez" (tels que, un mot de passe).

DESCRIPTION DE L'INVENTION : Dans les implémentations existantes, il n'y a pas de connexion entre l'ordinateur accédant au réseau et les services applicatifs dans la mesure où l'entité responsable de l'accès au réseau, telles que la passerelle VPN, diffère de l'entité régissant l'accès aux applications. Par conséquent les solutions existantes emploient généralement deux méthodes d'authentification. Parmi celles-ci, la première peut être utilisée pour authentifier l'ordinateur à la passerelle VPN, tandis que la seconde peut être utilisée pour l'authentification vers le serveur d'applications. Afin de faciliter l'authentification forte, il est souhaitable d'utiliser un lecteur de carte RFID. La plupart des ordinateurs offrent plusieurs possibilités pour connecter des périphériques externes,

Le résultat final est que la plupart des développeurs d'applications choisissent d'utiliser

uniquement un mot de passe, et opter pour l'utilisation d'une paire nom d'utilisateur / mot de passe uniquement. Cette situation empêche l'utilisation efficace de mécanismes d'authentification plus efficace par conséquent plus complexes tels que ceux utilisant des cartes à puce et / ou PKI pour sécuriser les deux facteurs d'authentification.

Cela crée une situation malheureuse dans laquelle chaque application doit gérer son propre système d'authentification, ce qui complique la gestion de l'authentification pour des applications multiples.

La présente invention concerne un procédé et un système d'authentification d'un utilisateur à une application ou ressource informatique accessible via un poste client utilisant un jeton de sécurité portable (par exemple une carte à puce sans contact), avec un secret que l'utilisateur peut facilement se rappeler (par exemple un code PIN). Ce secret fournit un second facteur de sécurité qui doit être de préférence indépendant pour protéger l'accès à l'application ou la ressource informatique, même si le jeton de sécurité portable est perdu ou volé. La meilleure façon pour protéger des données et l'accès sécurisé aux applications et données stockées accessibles en utilisant une communication en champ proche (NFC) matériel ou jeton RFID à courte portée.

L'Authentification sécurisée d'un utilisateur par l'intermédiaire d'un dispositif portable devient très importante dans deux situations différentes, d'une part pour l'authentification de l'accès utilisateur à une application ou une ressource d'ordinateur sur le poste client et d'autre part sur un serveur distant.

Une façon de fournir un niveau de sécurité supplémentaire aux utilisateurs d'applications est en exigeant que l'utilisateur soit muni également d'un jeton physique portable qui communique avec l'appareil à l'aide d'un système de communication RFID (lecteur RFID). Le lecteur RFID test en permanence la présence du jeton. Ce jeton, quand il est présent dans une plage de quelques centimètres du lecteur, vérifie constamment que l'utilisateur est bien présent. Lorsque l'utilisateur écarte le jeton du lecteur il perd le contact.

En dépit d'être chiffré, en raison des nombreux événements d'authentification transitoires

qui ont lieu entre le jeton et le dispositif, un hacker dispose de nombreuses possibilités de cryptanalyse les messages d'authentification, ainsi que pour effectuer des analyses de trafic sans même avoir à tenter une attaque cryptanalyse.

Même si un voleur qui vole le lecteur RFID et le jeton de sécurité porté par le propriétaire de l'appareil ne sera pas en mesure d'accéder aux ressources de l'appareil. Un Hacker qui veut déchiffrer le mot de passe logé dans la carte RFID en utilisation un brute force se verra avec la carte bloquée après trois tentatives, en effet le mot de passe est protégé par un nombre limité de tentatives, une foie ce nombre dépassé la carte sera inutilisable.

L'intérêt d'utilisation d'une carte RFID ISO 14443A est le fait de loger le mot de passe dans un bloc de mémoire de la carte. L'accès à ce bloque de mémoire est sécurisé par des clés de sécurité A & B.

Aussi avec cette invention, l'utilisateur peut stocker une clé cryptographique de 48 bits pour le Mifare classique figures 1 et 2 (128 bits pour le Mifare Plus & Mifare DESFire) sur le jeton de sécurité portable. Cette clé est utilisée pour générer directement la clé de session de cryptage de données d'une application ou d'un long et complexe mot de passe, à partir de laquelle une clé suffisamment longue et avec un chiffrement sécurisé peut être dérivée. Cela permet à l'utilisateur de protéger les données stockées sur le jeton avec une clé de chiffrement très forte. Si l'appareil est volé, il est alors impossible pour n'importe quel agresseur potentiel de déchiffrer les données cryptées sur elle sans le jeton associé.

Les informations d'identification sont stockées sur le jeton. Et ne transitent pas via le réseau.

Selon un premier aspect, un procédé d'authentification d'une application une Smarccard comprend:

- Installation du Kir Embeded Pass
- Le stockage d'un du Login & mot de passe dans la Smartcard;
- Lancer le lien d'accès à l'application;

- Demander à l'utilisateur de s'authentifier en saisissant son login et mot de passe sur le poste client;

- Transmission de la demande cryptée a la Smartcard ;

- Sur la Smartcard décryptage du MDP & comparaison par rapport au MDP saisi;

- Si la comparaison est valide, une autorisation de déverrouillage est fournie, sinon accès verrouillé ;

- Le changement du mot de passe se fait via le kit Embeded Pass. La présente invention réside dans un dispositif de lecture de carte à puce. Le lecteur peut en outre être couplé à divers dispositifs de plug-in ou biométrique pour obtenir jusqu'à cinq niveaux d'authentification, à savoir, (1) la carte à puce sans contact ISO 14443 A; (2) le lecteur de carte RFID; (3) le mot de passe ou PIN code; (4) la cryptographie à clé privée (PKI) et (5) un lecteur biométrique (en option). Ces niveaux de sécurité représentent une authentification extrêmement forte applicables aux réseaux publics sur les ordinateurs publics / privés, les applications logicielles, les serveurs et même pour le contrôle d'accès physique. Les transactions peuvent être effectuées sans risque d'émulation, de l'altération de la communication, d'erreur d'authentification ou de vol d'identité.

Figure1 : Processus d'accès via des cartes MIFARE, RFID

Figure 2 : Scénario puce sans contact

REVENDICATIONS

1. Dispositif de mot de passe d'authentification et d'autorisation d'accès à des applications logicielles sensibles ou à des ressources informatiques ou dans le domaine du contrôle d'accès physique à des zones très sensibles , caractérisé en ce que le mot de passe ne transite pas via le réseau ce qui lui octroie une sécurité
2. Dispositif de mot de passe selon la revendication 1 caractérisé en ce que les échanges entre le lecteur et la Smartcard sont crypté entant que renfort de la sécurisé dans les transactions
3. Dispositif de mot de passe selon la revendication 1 et 2 caractérisé en ce que le lecteur, la Smartcard et le mot de passe sont associés pour l'accès à l'application , le dispositif comporte le lecteur biométrique.

Annexes

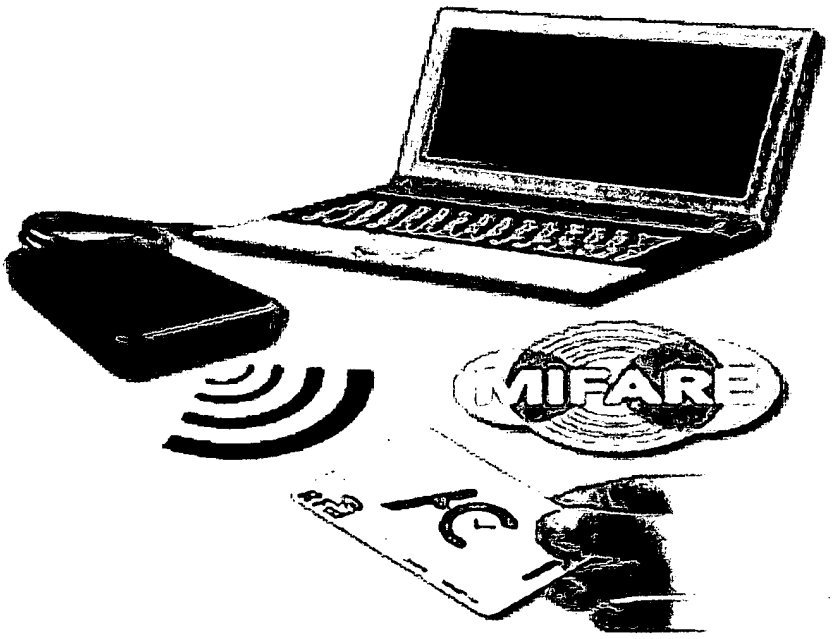

Figure1

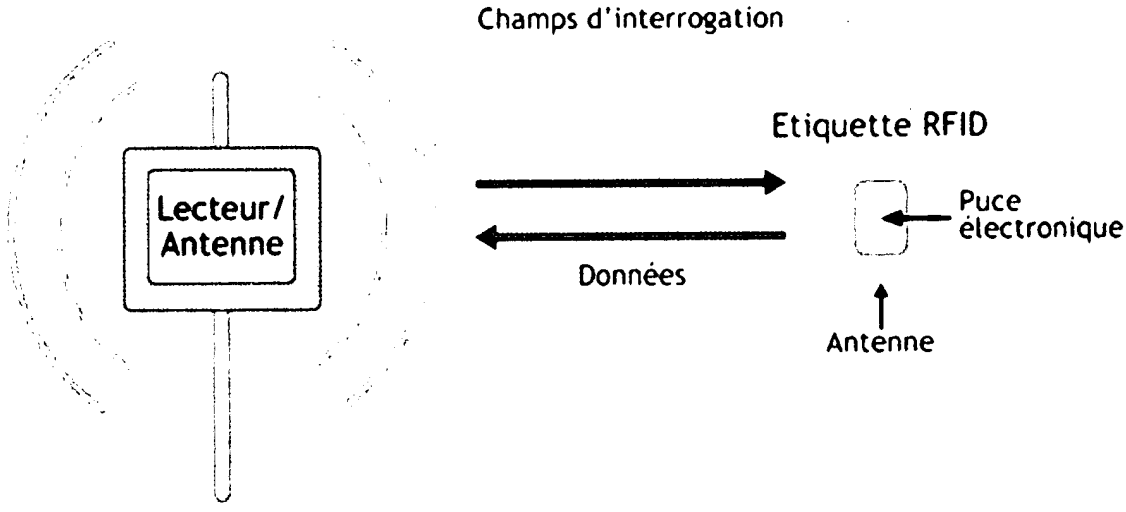

Figure 2

MA 38733A1

ROYAUME DU MAROC
****
OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
****

OMPIC

المملكة المغربية
المكتب المغربي للملكية الصناعية و التجارية

RAPPORT DE RECHERCHE AVEC OPINION SUR LA BREVETABILITE

(Conformément aux articles 43 et 43.2 de la loi 17-97 relative à la protection de la propriété industrielle telle que modifiée et complétée par la loi 23-13)

Renseignements relatifs à la demande	
N° de la demande : 38733	Date de dépôt : 29/12/2015
Déposant : UNIVERSITÉ MOHAMMED V DE RABAT	
Intitulé de l'invention : Dispositif de mot de passe embarqué dans un smart card sans contact	

Le présent document est le rapport de recherche avec opinion sur la brevetabilité établi par l'OMPIC conformément aux articles 43 et 43.2, et notifié au déposant conformément à l'article 43.1 de la loi 17-97 relative à la protection de la propriété industrielle telle que modifiée et complétée par la loi 23-13.

Les documents brevets cités dans le rapport de recherche sont téléchargeables à partir du site http://worldwide.espacenet.com, et les documents non brevets sont joints au présent document, s'il y en a lieu.

Le présent rapport contient des indications relatives aux éléments suivants :

Partie 1 : Considérations générales
- ☒ Cadre 1 : Base du présent rapport
- ☐ Cadre 2 : Priorité
- ☐ Cadre 3 : Titre et/ou Abrégé tel qu'ils sont définitivement arrêtés

Partie 2 : Rapport de recherche

Partie 3 : Opinion sur la brevetabilité
- ☐ Cadre 4 : Remarques de clarté
- ☒ Cadre 5 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle
- ☐ Cadre 6 : Observations à propos de certaines revendications dont aucune recherche significative n'a pu être effectuée
- ☐ Cadre 7 : Défaut d'unité d'invention

Examinateur: I. Oubiyi	**Date d'établissement du rapport** : 01/11/2017
Téléphone: 212 5 22 58 64 14/00	

ROYAUME DU MAROC OFFICE MAROCAIN de la PROPRIETE INDUSTRIELLE et COMMERCIALE CASABLANCA

Partie 1 : Considérations générales

Cadre 1 : base du présent rapport

Les pièces suivantes de la demande servent de base à l'établissement du présent rapport :

- Description
  4 Pages
- Revendications
  3
- Planches de dessin
  1 Page

Partie 2 : Rapport de recherche

Classement de l'objet de la demande :

CIB : H04L9/00
CPC : H04L2209/805 , H04L9/3234 , H04L63/0853

Bases de données électroniques consultées au cours de la recherche :

EPOQUE, Orbit

Catégorie*	Documents cités avec, le cas échéant, l'indication des passages pertinents	N° des revendications visées
X	US20060136717 A1 ; 22-06-2006 ; Mark Buer , Ed Frank	1-3
X	US8232862 B2 ; 31-07-2012 ; Assa Abloy Ab	1-3
X	US20020005774 A1 ; 17 janv. 2002 ; Rudolph Richard F., Rich Kirkham	1
X	US8214651 B2 ; 3 juil. 2012 ; International Business Machines Corporation	1
X	US20130214899 A1; 22-08-2013; Identive Group, Inc.	1

***Catégories spéciales de documents cités :**

-« **X** » document particulièrement pertinent ; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
-« **Y** » document particulièrement pertinent ; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
-« **A** » document définissant l'état général de la technique, non considéré comme particulièrement pertinent
-« **P** » documents intercalaires ; Les documents dont la date de publication est située entre la date de dépôt de la demande examinée et la date de priorité revendiquée ou la priorité la plus ancienne s'il y en a plusieurs
-« **E** » Éventuelles demandes de brevet interférentes. Tout document de brevet ayant une date de dépôt ou de priorité antérieure à la date de dépôt de la demande faisant l'objet de la recherche (et non à la date de priorité), mais publié postérieurement à cette date et dont le contenu constituerait un état de la technique pertinent pour la nouveauté

Partie 3 : Opinion sur la brevetabilité

Cadre 4 : Remarques de clarté

Les revendications 1 et 3 ne satisfait pas à l'exigence de clarté, car l'objet de la protection demandée n'est pas clairement défini. Les revendications tentent de définir l'objet par le résultat recherché, ce qui revient simplement à énoncer le problème sous-jacent, sans indiquer les caractéristiques techniques nécessaires pour parvenir à ce résultat.

Cadre 5 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle

Nouveauté (N)	Revendications aucune Revendications 1-3	Oui Non
Activité inventive (AI)	Revendications aucune Revendications 1-3	Oui Non
Possibilité d'application Industrielle (PAI)	Revendications 1-3 Revendications aucune	Oui Non

Il est fait référence aux documents suivants. Les numéros d'ordre qui leur sont attribués ci-après seront utilisés dans toute la suite de la procédure

D1 : US20060136717 A1

1. **Nouveauté (N) et Activité inventive (AI) :**

Le document D1 divulgue (§ [021], [0112] et fig. 7) un dispositif de mot de passe d'identification et d'autorisation d'accès à des applications logicielles, à des ressources informatiques ou dans le domaine d'accès physique à des zones très sensibles, caractérisé en ce que le mot de passe ne transite pas via le réseau. Par conséquent, l'objet de la revendication 1 n'est pas nouveau au sens de l'article 26 de la loi 17-97 telle que modifiée et complétée par la loi 23-13.

Les revendications dépendantes 2-3 ne semblent pas contenir des caractéristiques supplémentaires, en matière de nouveauté, en étant combinées avec les caractéristiques techniques de la revendication indépendante 1 auxquelles lesdites revendications dépendantes sont liées. Par conséquent, l'objet desdites revendications n'est pas nouveau et n'implique pas une activité inventive au sens des articles 26 et 28 de la loi 17-97 telle que modifiée et complétée par la loi 23-13.

2. **Possibilité d'application industrielle (PAI) :**

L'objet de la présente invention est susceptible d'application industrielle au sens de l'article 29 de la loi 17-97 telle que modifiée et complétée par la loi 23-13, parce qu'il présente une utilité déterminée, probante et crédible.