ROYAUME DU MAROC

OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
---

(19)

المملكة المغربية
المكتب المغربي للملكية الصناعية و التجارية

(12) BREVET D'INVENTION

(11) N° de publication :
MA 42027 B1

(51) Cl. internationale :
H04L 9/32; H04L 9/06

(43) Date de publication :
31.03.2020

(21) N° Dépôt :
42027

(22) Date de Dépôt :
19.02.2018

(71) Demandeur(s) :
Université Mohammed V - RABAT, Avenue des Nations Unies, Agdal, bp 8007 NU, Rabat, 10000 (MA)

(72) Inventeur(s) :
Echandouri Bouchra ; Omary Fouzia ; Hanin Charifa

(74) Mandataire :
Kartit Zaid

(54) Titre : **Méthode légère de génération d'une étiquette d'authentification d'objets (MAC-LM)**

(57) Abrégé : La présente invention concerne un procédé de génération de code d'authentification des étiquettes RFID. L'identification par radiofréquence (RFID) est l'un des piliers de base pour la réalisation de l'Internet des Objets (IoT). Ainsi, la protection de leur sécurité est d'une nécessité primordiale. Afin de contourner de nombreuses attaques potentielles, l'authentification permet de renier l'accès à des étiquettes malveillantes. Cependant, la cryptographie classique existante est inadaptable pour ce contexte de sécurité, puisque ces étiquettes RFID ont une puissance calculatoire faible. Ainsi, notre procédé d'authentification de message vient pour répondre aux exigences de la sécurité dans les étiquettes RFID. En plus, ce système a été prouvé robuste comparé aux autres systèmes existants.

Abrégé

La présente invention concerne un procédé de génération de code d'authentification des étiquettes RFID. L'identification par radiofréquence (RFID) est l'un des piliers de base pour la réalisation de l'Internet des Objets (IoT). Ainsi, la protection de leur sécurité est d'une nécessité primordiale. Afin de contourner de nombreuses attaques potentielles, l'authentification permet de renier l'accès à des étiquettes malveillantes. Cependant, la cryptographie classique existante est inadaptable pour ce contexte de sécurité, puisque ces étiquettes RFID ont une puissance calculatoire faible. Ainsi, notre procédé d'authentification de message vient pour répondre aux exigences de la sécurité dans les étiquettes RFID. En plus, ce système a été prouvé robuste comparé aux autres systèmes existants.

Titre : Méthode légère de génération d'une étiquette d'authentification d'objets (MAC-LM)

La présente invention concerne un système cryptographique, notamment un nouveau code d'authentification de message, par lequel un lecteur d'identification par radiofréquence (RFID) authentifie une étiquette RFID.

Puisqu'une étiquette d'identification par radiofréquence (RFID) est limitée en ressources de calcul, de mémoire et d'énergie. Ainsi, il est délicat d'utiliser une solution d'authentification cryptographique classique ; couteuse en mémoire et en énergie. Pour cela, notre procédé cryptographique approprié pour les étiquettes RFID a été développé, satisfaisant les différentes exigences de sécurité pour authentifier une étiquette RFID.

Les codes d'authentification de message (MACs) sont utilisés pour assurer à la fois l'intégrité et l'authentification. Il existe deux manières de les générer soit en utilisant une fonction de hachage à clé ou bien un système de chiffrement. Plus particulièrement, notre procédé est basé sur l'utilisation d'une fonction de hachage à clé légère.

En générale, en utilisant une clé secrète, un MAC génère une valeur, appelée empreinte, calculée à partir des données en entrée. L'émetteur prend ces données, les concatène à l'étiquette générée et les transmet dans un canal arbitraire. Lorsque le récepteur les reçoit, il génère l'étiquette, à partir des mêmes données reçu et en utilisant la même clé secrète, puis la compare avec celle reçu.

En 1995, les XOR-MAC, des codes d'authentification de message basés sur XOR, ont été proposés par Bellare et al. afin d'obtenir des Tags aléatoires. Leur construction décrite démontre l'utilisation d'une fonction Pseudo Random Function (PRF) en XOR sur l'ensemble des blocs générés (Bellare et al., 1995). Cette construction a été attaquée par Preneel.B et al en 1996.

En 1996, Bellare et al. a présenté un standard, nommé HMAC qui est une fonction de hachage à clé (Bellare, M., Canetti, R., & Krawczyk, H. (1996, August). Keying hash functions for message authentication. In Crypto (Vol. 96, pp. 1-15).). Prenant un message M, HMAC est généré comme suit :

H (K xor opad) || H ((K xor ipad) ||M))

où || est la concaténation, H est une fonction de hachage et K une clé secrète. Ici, opad et ipad sont des constantes prédéterminées. Déjà attaqué, ce standard proposé obtient presque toute sa sécurité à partir de la fonction de hachage utilisée.

En 2013, dans (Eiroa, S et al.), les auteurs ont décrit l'implémentation d'un autre HMAC basé sur la fonction de hachage légère PHOTON (Guo, J, et al.2011). Néanmoins, sa mise en œuvre n'est pas pratique pour les ressources à grande vitesse avec une puissance de calcul restreinte (Eiroa et Baturone, 2013).

De plus, dans (Shin, S. et al. 2012), les auteurs ont introduit un schéma d'authentification léger basé sur les automates cellulaires pour multiple-utilisateurs pour le contexte du Cloud Computing. Cependant, ce schéma n'assure que l'authentification et non pas l'intégrité. Si on se limite à l'authentification, une entité malveillante peut altérer les données transmises.

Par ceci, il existe une nécessité en procédé d'authentification à utiliser avec une étiquette RFID, capable d'exécuter une authentification robuste sans faire appel à un une ressource puissante.

Brève description des figures

Fig. 1 : une illustration du procédé de génération du code d'authentification des messages (LCAHASHMAC).

Fig.2 : procédé de vérification

Description détaillée

Description détaillé

La robustesse d'un code d'authentification de message repose généralement sur la robustesse de la fonction de hachage utilisée dans son processus. Cependant, la plupart des fonctions de hachages connues sont déjà attaquées et cassées.

Pour assurer l'authenticité, ce nouveau système est basé sur une fonction de hachage légère. Sa conception repose sur l'utilisation des automates cellulaires, connu par leur légèreté, une simplicité et facilité d'implémentation. Il comporte trois procédés. Un pour génération de clé secrète, un pour générer l'empreinte et un pour la vérification.

Lors du premier procédé de génération de clé, un générateur pseudo

aléatoire est utilisé pour générer les deux clés sk1 et sk2 de longueur 256 bits. Skp est un nombre secret qui est premier avec une longueur supérieur à 13 bits. Enfin, Skindex est un index secret choisi aléatoirement de [0, n], où n est le nombre de blocs possibles.

Dans la fig. 1-1, prenons un identifiant ID, à authentifier, avec une longueur fini arbitraire L, le procédé commence tout d'abord par faire un découpage en blocs (Mi) de taille fixe de 256 bits. Il faut ajouter un padding de '10000….0', si nécessaire pour compléter le dernier bloc (Mpad). Ensuite, dans la fig. 1-2 on XOR sk1 avec le bloc d'indice skindex (Mskindex) . Par la suite, dans la fig. 1-3 on calcule le résidu Ri résultant de l'opération modulo de chaque bloc Mi avec skp, pour obtenir un message compressé M'. Ce dernier, est la concaténation de tous les résidus Ri (fig. 1-4), qui est lui aussi découpé en blocs d'une longueur fixe de 256 bits. Ensuite, si la taille de M' est supérieure à 256 bit une opération 'XOR' est appliquée entre tous les M'i avec la deuxième sous-clé Sk2 (fig. 1-5). Sinon, si la longueur du M' est inférieure à 256 bits, M' est concaténé avec une partie de la deuxième sous-clé sk2 (fig. 1-6)..

Dans la fig. 1-7, dénoté M'', le bloc de bits obtenu représente l'automate cellulaire et l'entrée à la règle globale : $\{0,1\}^{256} \rightarrow \{0,1\}^{256}$, qui renvoie la configuration globale de l'automate. Où chaque cellule évolue selon l'une des règles ; à savoir la règle 150 et la règle 101. La sortie est l'étiquette (fig.1-8).

Dans la figure 2, le procédé de vérification prend en entrée l'identifiant ID, les même sous clés secrètes et l'empreinte (empreinte 0), pour reproduire une autre étiquette (empreinte 1) en utilisant le procédé de génération d'étiquette. Si les deux étiquettes sont égales, celle reproduite et celle reçue, alors l'authenticité du message est garantie.

La capacité de stockage d'informations ainsi que la capacité à transférer des informations via des moyens sans contact directe des étiquettes d'identification par radiofréquence (RFID) se traduisent par un avantage significatif par rapport aux codes-barres. Cependant, les problèmes de coût et de protection de la vie privée sont des obstacles majeurs. Pour ce fait, ce procédé vient pour résoudre l'un de ces problèmes, en particulier ceux qui se rapportent à l'authenticité des étiquettes RFID.

Revendications

1- Un système d'authentification d'objet à partir de son identificateur (ID) caractérisé en ce qu'il utilise un procédé pour générer une étiquette légère ; ledit procédé vérifier également l'authenticité dudit objet.

2- Le système selon la revendication 1 est caractérisé en ce que le dit objet peut être physique ou virtuel (message) ; ledit identificateur est de longueur fini arbitraire L.

3- Le système selon les revendications 1 et 2 caractérisé en ce que ledit procédé comprend les étapes suivantes :

a- Une étape d'initialisation consiste à :

- Générer les deux clés S_{k1} et S_{k2} d'une taille de 256 bits, à partir d'un pseudo aléatoire ;
- Générer une clé secret S_{kp} d'une taille minimale de 13 bits.
- Découper le message initial M en n blocs M_i de taille 256 bits chacun,
- Compléter le dernier bloc par un padding sous forme 100…..00.
- Choisir un index secret Sk_{index} entre 0-n

b- Une étape de prétraitement consiste à :

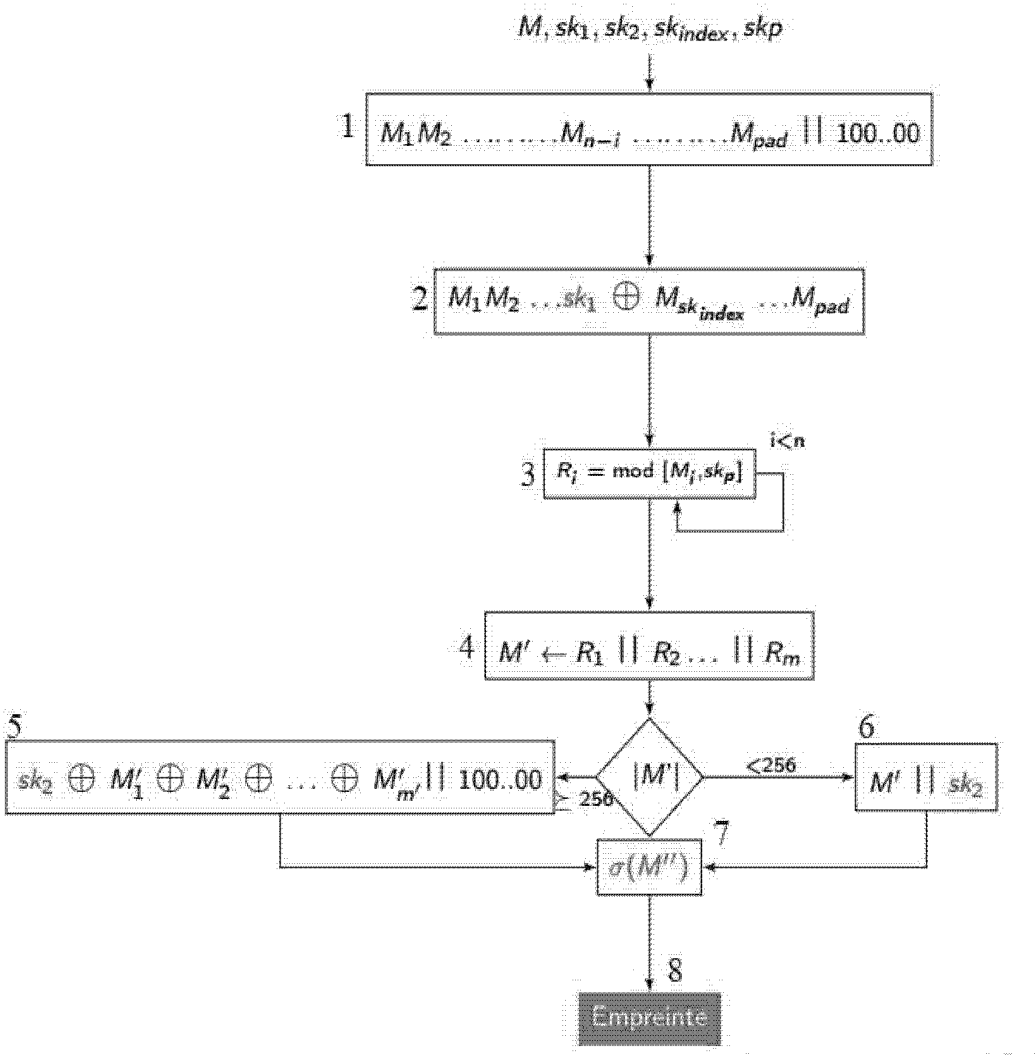
- Effectuer une opération xor entre S_{k1} et ledit MSk_{index} (2).
- Calculer les résidus Ri résultant de l'opération modulo de chaque bloc Mi avec Skp (3).
- Concaténer les dites R_i pour former le message M'(4)

c- Une étape de génération de l'empreinte consiste à calculer la valeur absolu de M' ; dans le cas où ladite valeur est inférieur à 256, on concatène M'avec S_{k2} (6) ; Sinon on découpe M'en des blocs de 256 avec un padding éventuel et on effectue un xor entre les M'_i et S_{k2} pour avoir M'' (5) et on applique l'automate cellulaire sur M'' pour générer le tag $\sigma(M'')$ (7).

b- Une étape de vérification qui consiste à :

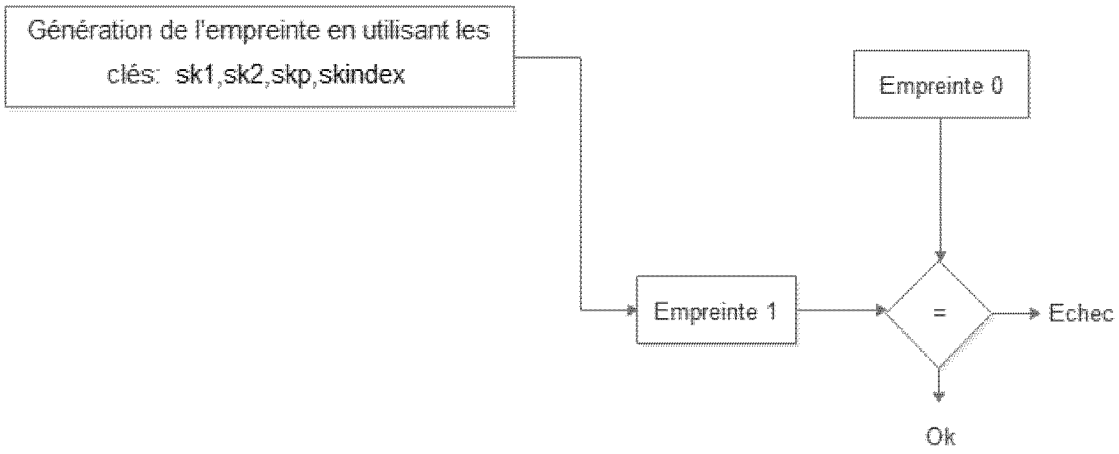
- Reproduire une étiquette (empreinte 1) en appliquant les mêmes étapes précédentes sur l'identifiant ID de l'objet reçu en utilisant les clés secrètes Sk1,Sk2, Skp et Skindex ;
- Comparer l'étiquète reçu (empreinte 0) et celle reproduite (empreinte 1), en cas d'égalité l'objet est authentifié.

Fig.1


$M, sk_1, sk_2, sk_{index}, skp$
1
$M_1 M_2 \ldots\ldots M_{n-i} \ldots\ldots M_{pad} \,||\, 100..00$
2
$M_1 M_2 \ldots sk_1 \oplus M_{sk_{index}} \ldots M_{pad}$
3
$R_i = \text{mod}\,[M_i, sk_p]$
i<n
4
$M' \leftarrow R_1 \,||\, R_2 \ldots \,||\, R_m$
5
$sk_2 \oplus M'_1 \oplus M'_2 \oplus \ldots \oplus M'_{m'} \,||\, 100..00$
$|M'|$
≥ 256
<256
6
$M' \,||\, sk_2$
7
$\sigma(M'')$
8
Empreinte

25

Fig. 2


Génération de l'empreinte en utilisant les clés: sk1,sk2,skp,skindex
Empreinte 0
Empreinte 1
=
Echec
Ok

MA 42027B1

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

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 : 42027	Date de dépôt : 19/02/2018
Déposant : Université Mohammed V - RABAT	
Intitulé de l'invention : Méthode légère de génération d'une étiquette d'authentification d'objets (MAC-LM)	

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** : 21/09/2018
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
  3 Pages
- Revendications
  3
- Planches de dessin
  2 Pages

Partie 2 : Rapport de recherche

Classement de l'objet de la demande :

CIB : H04L9/06, H04L9/32, G06F21/31
CPC : H04L9/0643, H04L9/3271

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 A	WO2007068519A3 ; IbmIbm FranceFrederic BauchotJean-Yves ClementGerard MarmigerePierre Secondo 21-06-2007	1-2 3
X A	CN105391544A ; BEIJING INSTITUTE PETROCHEMICAL TECHNOLOGY ; 09-03-2016	1-2 3
X	WO2001072107A3 ; Int Paper Co ; 29-08-2002	1
X A	CN104115442A ; UNIV NORTH CHINA ELEC POWER ; 02-08-2017	1-2 3
X A	https://www.iacr.org/archive/ches2008/51540279/51540279.pdf	1-2 3

***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

La demande ne satisfait pas aux exigences de l'art. 35 de la loi 17-97 telle que modifiée et complétée par la loi 23-13, les revendications 1-3 manquent de clarté et de concision, et ce pour les raisons suivantes :

- Les revendications de système sont considérées comme des revendications de dispositif, et non pas comme des revendications de méthode ou de procédé. Les caractéristiques énoncées dans les revendications 1-3 portent sur un procédé, au lieu de définir clairement ce dispositif en termes de caractéristiques techniques. Les limitations visées ne ressortent donc pas clairement de ces revendications. Par ailleurs, lesdites revendications du système ont été interprétées comme étant des revendications du procédé.

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

Nouveauté (N)	Revendications 3 Revendications 1-2	Oui Non
Activité inventive (AI)	Revendications 3 Revendications 1-2	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 : WO2007068519A3

1. Nouveauté (N) :

Le document D1 divulgue un système et son procédé d'authentification d'objet à partir de son identificateur ID ledit identificateur est de longueur fini arbitraire L. ledit procédé vérifie l'authenticité dudit objet et génère une étiquette. Par conséquent, l'objet des revendications 1-2 n'est pas nouveau au sens de l'art. 26 de la loi 17-97 telle que modifiée et complétée par la loi 23-13.

Aucun des documents cités ci-dessus ne divulgue l'ensemble des caractéristiques techniques énoncées dans la revendication 3. Par conséquent, l'objet de ladite revendication est nouveau au sens de l'art. 26 de la loi 17-97 telle que modifiée et complétée par la loi 23-13.

2. Activité inventive (AI) :

Le document D1, qui est considéré comme l'état de la technique le plus proche de l'objet de la revendication 1, divulgue (voir abrégé) un procédé permettant d'authentifier un objet comprenant une identification par radio fréquence (RFID) possédant une mémoire afin de stocker un identificateur et une clé secrète et une fonction de hachage intégrée. La sortie de l'identification RFID de l'objet à authentifier est comparée à la sortie de l'identification RFID d'un objet authentique ; un nombre aléatoire est transmis à l'objet à authentifier avec zéro comme paramètres ; l'identificateur de l'identification RFID, le nombre aléatoire et la clé secrète sont concaténés et utilisés comme entrée dans la fonction de hachage intégrée

dont la sortie est obtenue au moyen de l'identificateur de RFID ; Celui-ci et le nombre aléatoire sont ensuite transmis à l'identification RFID de l'objet authentique retournant son identificateur et la sortie de la fonction de hachage intégrée calculée au moyen de l'identificateur de l'identification RFID de l'objet à authentifier, du nombre aléatoire et de la clé secrète ; Si les résultats des deux fonctions de hachage intégrés sont identiques, l'objet est authentifié, sinon l'objet est une contrefaçon.

Par conséquent, l'objet de la revendication 3 diffère de ce procédé connu en ce que il contient des étapes d'initialisation, de prétraitement, de génération d'empreinte et de vérification différentes que ceux divulgués dans D1.

Le problème que la présente invention se propose de résoudre peut donc être considéré comme celui d'améliorer la robustesse du procédé d'authentification d'objets.

La solution à ce problème proposée dans la revendication indépendante de la présente demande est considérée comme impliquant une activité inventive. En effet, l'homme du métier ne serait pas parvenu d'une manière évidente à reproduire l'invention revendiquée en partant de D1. Aussi, aucun enseignement n'a été trouvé dans le reste de l'état de la technique disponible qui aurait incité la personne du métier, en partant du document D1, à atteindre le résultat recherché.

Par conséquent, l'objet de la revendication 3 implique une activité inventive au sens de l'article 28 de la loi 17-97 telle que modifiée et complétée par la loi 23-13.

3. 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.