(19) CONFÉDÉRATION SUISSE
INSTITUT FÉDÉRAL DE LA PROPRIÉTÉ INTELLECTUELLE

(11) **CH 699 083 B1**

(51) Int. Cl.: ***G06K 19/10*** *(2006.01)*
G06F 19/00 *(2011.01)*

Brevet d'invention délivré pour la Suisse et le Liechtenstein
Traité sur les brevets, du 22 décembre 1978, entre la Suisse et le Liechtenstein

(12) FASCICULE DU BREVET

(21) Numéro de la demande: 01172/08

(22) Date de dépôt: 28.07.2008

(43) Demande publiée: 29.01.2010

(24) Brevet délivré: 15.10.2013

(45) Fascicule du brevet publié: 15.10.2013

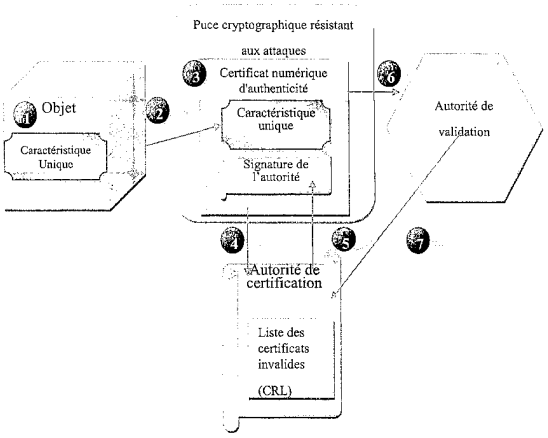
(73) Titulaire(s):
WISeKey SA, 29, route de Pré-Bois World Trade Center
1217 Meyrin/Genève (CH)

(72) Inventeur(s):
Jérôme Darbellay, 1003 Lausanne (CH)
Juan Carlos Creus Moreira, 1233 Bernex (CH)
Kevin Blackman, 1207 Genève (CH)
Carlos Moreno, 1213 Petit-Lancy 2 (CH)

(74) Mandataire:
per Mens Intellectual Property Consulting Sàrl,
Thomas Sammer Rue Agasse 54
1208 Genève (CH)

(54) Procédé pour la certification numérique d'authenticité d'un objet physique et support d'enregistrement pour la mise en œuvre d'un tel procédé

(57) La présente invention se réfère à un procédé pour la certification numérique d'un objet physique, aux moyens de programme d'ordinateur et aux supports d'enregistrement correspondants, ainsi qu'à l'application du procédé pour la certification numérique d'authenticité d'un objet physique de valeur. Le procédé comprend les étapes de délivrer (1, 2, 3, 4, 5) un support d'enregistrement comportant un certificat numérique d'authenticité comprenant des informations codées reflétant au moins une caractéristique unique de l'objet physique, de vérifier (6, 7), chaque fois que cela est voulu, la validité du certificat numérique d'authenticité par l'utilisation de moyens informatiques de réseau, ces moyens informatiques de réseau coopérant avec ledit support d'enregistrement et une autorité de validation et/ou de certification afin de sortir sensiblement en temps réel l'état de validité dudit certificat numérique d'authenticité, et de modifier, chaque fois que cela est voulu, l'état de validité dudit certificat numérique d'authenticité.



Description

[0001] La présente invention se rapporte à un procédé pour la certification numérique d'authenticité d'un objet physique de valeur, à un support d'enregistrement comprenant un programme d'ordinateur correspondant ainsi qu'à l'utilisation du procédé pour la certification numérique d'authenticité d'un objet physique de valeur.

[0002] En général, la présente invention se situe dans le contexte de la protection d'objets d'une certaine valeur, en particulier de produits de luxe, contre une falsification ce qui devient de plus en plus difficile de nos jours. De nos jours, il est pratique courante pour un fabricant de produits de luxe, par exemple de montres ou de joaillerie précieuse, d'émettre un certificat de l'authenticité sur papier correspondant au produit de luxe vendu et de le remettre au client simultanément avec le produit lors de l'achat de ce dernier. De tels certificats sur papier utilisent le fait que des produits de luxe d'une certaine valeur présentent usuellement une caractéristique unique, par exemple un numéro de série, qui est cependant, tout comme le produit entier, usuellement falsifiable. Pour cette raison, le fabricant d'un objet de valeur falsifiable l'associe au certificat sur papier qui reproduit l'identifiant unique. Si le certificat sur papier est considéré comme étant non falsifiable, l'authenticité de l'objet de valeur peut être établie en demandant la présentation du certificat. Naturellement, le tout se base sur le fait que le certificat sur papier est produit par une autorité compétente et ne peut pas être falsifié. Un exemple typique de ce qui vient d'être décrit sont par exemple des marques de montres vendant des montres de haute qualité conjointement à un certificat sur papier délivré par le fabricant ou le vendeur et reproduisant le numéro de série d'une montre individuelle.

[0003] Cependant, la procédure décrite ci-dessus de manière inhérente comporte plusieurs problèmes. Premièrement, la solution mentionnée ci-dessus se fonde sur le fait qu'il est techniquement impossible de falsifier le certificat sur papier. Il est cependant connu que de tels certificats basés sur du papier de sécurité, un filigrane, un RFID ou d'autres techniques conventionnelles n'offrent désormais plus la garantie d'être infalsifiables, sauf si la complexité technique de la procédure appliquée est énormément élevée ce qui, d'autre côté, complique le procédé de fabrication et le rend très coûteux. Cela a mené à la compétition bien connue entre les fabricants de produits de valeur et les contrefacteurs qui augmentent de leur côté également leurs possibilités techniques non seulement pour la production des produits falsifiés mais également en ce qui concerne la copie des certificats. Pour cette raison, il y a un besoin chez les fabricants de produits de valeur de trouver une solution technique qui leur permet de fabriquer des certificats d'authenticité effectivement infalsifiables qui sont destinés à être délivrés simultanément avec le produit acheté.

[0004] Deuxièmement, les solutions connues à présent pour certifier l'authenticité d'un objet physique donné présentent l'inconvénient additionnel que, même si le certificat dans les mains d'un propriétaire d'un objet de valeur donné n'est pas falsifié, il est difficile et pénible pour le propriétaire, qui à priori ne sait pas cela, de vérifier le certificat. Par exemple, si le propriétaire d'un objet donné avec un tel certificat a des doutes concernant son authenticité, ou dans le cas où il songera à une acquisition autrement que chez un vendeur officiel, il serait normalement nécessaire d'envoyer le certificat par courrier au fabricant du produit ou à une autre autorité correspondante afin de procéder à la vérification. Il existe donc un besoin chez les fabricants de tels produits de trouver des solutions techniques afin de simplifier cette procédure.

[0005] De plus, les certificats d'authenticité conventionnels de produits de valeur qui utilisent par exemple du papier de sécurité, un filigrane ou un RFID ne mentionnent normalement que les propriétés principales du produit conjointement audit identifiant unique tel que le numéro de série du produit. Après la délivrance du certificat, il n'est plus possible d'ajouter facilement d'autres informations du produit ou de modifier facilement l'état de validité du certificat associé à un produit donné. Il existe donc encore un besoin chez les fabricants de tels produits de trouver une solution technique qui permet une utilisation et une modification plus flexibles des données figurant sur le certificat et se référant aux produits vendus.

[0006] La présente invention a pour objet de surmonter les difficultés mentionnées ci-dessus et de mettre en œuvre un procédé pour la certification de l'authenticité d'un objet physique ayant une certaine valeur, le procédé présentant le niveau de sécurité le plus élevé possible pour que le certificat d'authenticité ne puisse pas être falsifié. De plus, une vérification du certificat d'authenticité devrait devenir beaucoup plus facile par rapport aux solutions connues, et des données se rapportant à l'objet authentifié et/ou à son propriétaire devraient pouvoir être incorporées dans le certificat d'une façon plus flexible et plus facile.

[0007] A cet effet, la présente invention propose un procédé pour la certification numérique d'authenticité d'objets physiques, le procédé étant caractérisé par les caractéristiques énumérées dans la revendication 1 qui permettent d'atteindre les objectifs identifiés ci-dessus.

[0008] En particulier, le procédé pour la certification numérique d'authenticité selon la présente invention comprend les étapes de l'émission d'un certificat numérique d'authenticité stocké sur un support d'enregistrement et comportant des informations codées qui reflètent au moins une caractéristique unique de l'objet physique, de la vérification de la validité du certificat numérique à chaque fois que cela est voulu, et de la modification de l'état de validité dudit certificat également à chaque fois que cela est voulu, et se distingue du fait que l'étape d'émettre un certificat numérique d'authenticité comprend la génération d'une paire de clefs de cryptage asymétrique comprenant une clé publique et une clé privée sur ledit support d'enregistrement, ladite clé privée étant stockée de façon non-exportable sur le support d'enregistrement, et que l'étape de vérifier la validité du certificat numérique d'authenticité comprend l'utilisation d'une fonctionnalité d'authentification mutuelle, en particulier l'utilisation des protocoles TLS ou SSL, afin de sortir, sensiblement en temps réel, l'état de validité

dudit certificat numérique d'authenticité. Le fait que des certificats numériques délivrés et signés par des autorités de certification autorisées ainsi qu'enregistrés par exemple sur une puce cryptographique ne sont pas falsifiables fournit une solution au problème technique mentionné ci-dessus. De plus, la validité du certificat numérique peut être vérifiée facilement dans le monde entier en utilisant une communication sécurisée sur des réseaux à présent bien établis tel que l'internet. Ensuite, le certificat numérique peut facilement être doté d'informations additionnelles relatives aux produits authentifiés, ou l'état du certificat peut être modifié.

[0009] La présente invention propose également des supports d'enregistrement qui sont adaptés à la mise en œuvre dudit procédé; ces supports d'enregistrement se distinguent par les caractéristiques énumérées dans la revendication 9, ils sont en particulier adaptés pour loger ledit certificat numérique d'authenticité ainsi que pour pouvoir coopérer avec un moyen informatique de réseau et une autorité de validation et/ou de certification afin de vérifier la validité dudit certificat.

[0010] En particulier, la présente invention propose l'application du procédé selon la présente invention dans le contexte de l'authentification d'objets physiques ayant une grande valeur, par exemple de montres précieuses, des bijoux ou d'autres produits de luxe.

[0011] D'autres propriétés et avantages de la présente invention sont mentionnés dans les revendications dépendantes ainsi que dans la description qui illustre, dans ce qui suit, l'invention plus en détail en faisant référence aux figures.

[0012] Les figures ci-attachées illustrent les principes de la présente invention sous forme d'exemples et schématiquement.

La fig. 1	montre schématiquement le principe d'une certification d'authenticité utilisé dans l'état de la technique ainsi que dans la solution selon la présente invention.
La fig. 2	est une vue d'ensemble schématique des étapes du procédé pour une certification numérique d'authenticité d'un objet physique selon la présente invention.
Les fig. 3a et 3b	montrent un exemple d'une interface graphique d'un programme d'ordinateur correspondant au cours de la procédure de vérification de la validité du certificat numérique, à savoir au stade auquel la vérification est demandée et, respectivement, une fois la validité du certificat confirmée.

[0013] Dans la description qui suit, on décrira l'invention en détail en faisant référence aux figures mentionnées ci-dessus.

[0014] La fig. 1 illustre le principe utilisé dans les certificats d'authenticité conventionnels fondés sur le papier de sécurité, les filigranes ou d'autres technologies traditionnelles ainsi que selon le contexte de la présente invention. L'objet falsifiable, par exemple une montre ou un autre produit de luxe, présenté à gauche dans la fig. 1, comprend une caractéristique unique telle qu'un numéro de série par exemple. Le certificat d'authenticité, émis par une entité autorisée et considéré comme étant infalsifiable, reproduit cette caractéristique unique et est illustré symboliquement à droite sur la fig. 1. Tandis que la supposition que les certificats traditionnels ne sont pas falsifiables n'est plus valable dès que les contrefacteurs atteignent le niveau correspondant de technologie pour copier ces certificats, la duplication des certificats numériques d'authenticité selon la présente invention est beaucoup plus difficile comme il sera démontré dans la description qui suit.

[0015] La fig. 2 montre schématiquement les différentes étapes d'un procédé de certification numérique d'authenticité d'un objet physique selon la présente invention. Un objet physique, par exemple un produit de luxe, doit normalement d'abord être pourvu après sa fabrication d'un identifiant unique tel qu'un numéro de série alphanumérique ce qui est symboliquement indiqué par le numéro de référence 1 dans la fig. 2. Le numéro de série peut être par exemple gravé sur le produit de luxe, ou ce dernier peut comprendre tout autre identifiant unique adapté à ce but.

[0016] Comme première étape du procédé selon l'invention, un certificat numérique d'authenticité correspondant audit produit de luxe doit d'abord être créé. A cet effet, un support d'enregistrement comprenant un certificat numérique d'authenticité comportant des informations signées numériquement qui reflètent au moins la caractéristique unique mentionnée ci-dessus, est délivré. Des supports d'enregistrement de la présente invention adaptés à ce but consistent typiquement en des puces cryptographiques comprenant un programme d'ordinateur permettant de créer des informations cryptographiques in situ et, au moins partiellement, d'une manière non exportable. De telles puces sont normalement intégrées dans une carte à puce cryptographique. Les notions «puce cryptographiques» et, respectivement, «carte à puce cryptographique» sont utilisées dans la description qui suit largement à titre de synonyme du terme «support d'enregistrement». De telles puces cryptographiques sont adaptées pour loger les certificats numériques d'authenticité selon la présente invention qui peuvent ensuite être vérifiés par des moyens informatiques externes.

[0017] La délivrance d'un certificat numérique selon la présente invention comprend donc la fourniture d'une telle puce cryptographique. La puce est ensuite insérée dans un moyen de lecture et de traitement tel qu'un lecteur de carte à puce dans un ordinateur personnel normal, utilisé comme moyen d'entrée et de sortie au cours de la délivrance du certificat numérique. Ensuite, comme il est indiqué par le numéro de référence 2 à la fig. 2, une requête pour délivrer ledit certificat numérique d'authenticité du produit de luxe est formulée. Le fichier de requête du certificat numérique reproduit ladite au moins une caractéristique unique du produit de luxe en incorporant des informations codées représentant ladite au moins une caractéristique unique. La caractéristique unique peut par exemple être placée, comme un numéro de série

gravé, dans le champ du nom commun du certificat. Le fichier de requête peut être formulé basé sur la norme X.509 de délivrance de certificat, connue de l'homme du métier.

[0018] Pour la création d'un certificat numérique, la présente invention utilise un cryptage asymétrique, cette méthode étant la meilleure solution pour des tels buts selon la connaissance actuelle. Par conséquent, la formulation de ladite requête pour délivrer le certificat numérique d'authenticité devant être crée sur ledit support d'enregistrement comprend, comme il est indiqué symboliquement par le numéro de référence 3 à la fig. 2, la génération d'une paire de clés de cryptage asymétrique comprenant une clé publique et une clé privée. La génération de la paire de clés de cryptage asymétrique s'effectue directement (on-board) sur ledit support d'enregistrement et de façon à ce que la clé privée ne puisse pas être exportée. Cela demande que le programme d'ordinateur mentionné ci-dessus sur la puce cryptographique permet de créer l'information cryptographique sur site et au moins partiellement d'une manière non exportable, de tels programmes étant également appelés «smart chip middleware» ou «pilotes». De manière alternative, la génération de la paire de clés de cryptage asymétrique n'est pas effectuée directement sur la puce mais par un moyen sécurisé externe par rapport à la carte et sera mémorisée après génération sur la puce de telle façon que la clé privée ne soit pas exportable ainsi que, bien évidemment, unique. De préférence, la génération de la paire de clés de cryptage asymétrique, ou bien sur le site de la puce cryptographique ou bien par ledit moyen sécurisé, est effectuée en utilisant des algorithmes cryptographiques de clés publiques tels que l'algorithme cryptographique Rivest-Shamir-Adlemon (RSA), ou bien la cryptographie de courbe elliptique (ECC), ces algorithmes étant également bien connus de l'homme du métier. La clé privée du certificat numérique d'authenticité étant générée d'une manière sécurisée et unique, ou bien sur la puce cryptographique ou bien par ledit moyen sécurisé, et en tout cas enregistrée sur la puce d'une manière non exportable, une propriété de non-duplicabilité idéale du certificat voire de la puce est obtenue, les rendant résistants aux attaques et infalsifiables d'une façon très efficace.

[0019] Après avoir formulé la requête de délivrer un certificat numérique de la façon décrite ci-dessus, la requête est envoyée à une autorité de certification pour approbation, ce qui est indiqué symboliquement par le numéro de référence 4 à la fig. 2. L'autorité de certification doit être contrôlée et mise en œuvre par des personnes autorisées, ou bien au moyen de procédés automatiques, et cette autorité peut par exemple être identique au fabricant du produit de luxe dont l'authenticité doit être certifiée, ou elle peut correspondre à une entité désignée par ce fabricant. Sur réception de ladite requête par l'autorité de certification, l'intégrité du certificat et/ou l'unicité de la requête sera vérifiée par rapport à plusieurs paramètres, par exemple aux autorisations de l'opérateur. Si l'étape de vérification est couronnée de succès, l'autorité de certification signe le fichier de requête pour un certificat numérique de manière numérique avec son propre certificat, à savoir le certificat de l'autorité certifiante, et envoie le fichier de requête avec signature numérique en retour au support d'enregistrement inséré dans le moyen de lecture et de traitement. Cette étape est indiquée à la fig. 2 par le numéro de référence 5. Sur réception de la requête signée par la puce cryptographique, le logiciel mentionné ci-dessus («middleware») finalise la création du certificat d'authenticité numérique par l'interaction avec la requête signée comprenant l'approbation de l'autorité de certification. Plusieurs aspects de cette procédure peuvent être accomplis selon la procédure standard pour la délivrance d'un certificat X.509; cela n'est cependant pas absolument nécessaire si des alternatives techniquement équivalentes sont ou deviennent disponibles.

[0020] Après la délivrance d'un certificat numérique d'authenticité sur une carte à puce cryptographique selon le procédé décrit ci-dessus, et après la vente d'un produit de luxe conjointement à sa carte d'authenticité correspondante, la validité du certificat numérique et donc l'authenticité du produit de luxe correspondant peuvent être vérifiées par le propriétaire du produit quand et où il l'estime nécessaire, et ce par l'utilisation d'un moyen informatique de réseau. A cet effet, le moyen informatique de réseau coopère avec ledit support d'enregistrement et avec l'autorité de validation et/ou de certification, de manière à ce qu'on obtient effectivement en temps réel l'état de validité du certificat numérique d'authenticité. Dans ce contexte, il est à noter que l'autorité de validation peut être identique avec l'autorité de certification, mais cela n'est pas nécessairement le cas car la première peut également être composée par une ou plusieurs entités correspondantes.

[0021] En effet, pour vérifier la validité du certificat numérique d'authenticité, il suffit d'insérer la carte à puce cryptographique qui comprend le certificat numérique d'authenticité dans n'importe quel moyen de lecture et de traitement, à savoir dans un ordinateur qui est équipé d'un lecteur de cartes à puce et qui est configuré en conséquence. Ensuite, la validité du certificat sur la carte à puce peut être vérifiée en faisant appel à un serveur web qui est également configuré à cet effet, cette opération faisant également usage du logiciel («middleware») sur la carte à puce. A cet effet, la puce comprenant le certificat numérique d'authenticité se connecte via les moyens informatiques de réseau à l'autorité de validation et/ou à l'autorité de certification ce qui est illustré symboliquement par le numéro de référence 6 à la fig. 2. L'autorité de validation consiste typiquement en le serveur web mentionné ci-dessus qui est configuré pour être adapté à l'utilisation de protocoles de communication cryptographique tels que TLS (Transport Layer Security) ou SSL (Secours Socket Layer), de préférence TLS, et comprenant encore une fonctionnalité d'établissement de liaison («handshake») afin de fournir une authentification mutuelle au cours du procédé de communication; des moyens de communication de sécurité alternatifs fournissant une fonctionnalité adéquate peuvent également être adaptés à une utilisation pour ce but. Les termes techniques mentionnés ci-dessus sont également connus de l'homme du métier et ne demandent pas d'explications plus détaillées.

[0022] L'autorité de validation vérifie la période de validité du certificat ainsi que s'il a été annulé, ceci en faisant appel à l'autorité de certification qui utilise pour ce but par exemple une liste d'annulation de certificats (Certificate Revocation List/ CRL) se trouvant généralement au sein de l'autorité de certification ou bien un protocole d'état de certificat online (Online

Certificate Status Protocol/OCSP) ce qui est indiqué symboliquement par le numéro de référence 7 à la fig. 2. Chacun des deux répertoires est une espèce de liste comprenant des informations sur les certificats délivrés, en particulier une entrée correspondante dans le cas où des certificats individuels ont été compromis. Cette étape comprend donc une interaction du moyen informatique de réseau avec le support d'enregistrement ainsi que l'autorité de validation et/ou de certification afin de permettre l'accès par ladite autorité de validation et/ou de certification au certificat numérique d'authenticité. En effet, la validité du certificat est vérifiée par un échange de la clé publique entre l'autorité de validation et la carte à puce ce qui est connu de l'homme du métier, et par une vérification croisée du certificat avec les listes mentionnées ci-dessus (CRL ou OCSP). Cette étape comprend usuellement la vérification de la validité du certificat par l'autorité de certification ce qui est connu à l'homme du métier comme validation du certificat en chaîne («certificate chain validation»). Ensuite, la sortie sous forme de l'état de validité du certificat est effectuée sensiblement en temps réel via le moyen informatique de réseau. La sortie peut par exemple consister en le fait que le certificat d'authenticité est valide, à savoir que le produit de luxe est authentique ce qui est illustré par l'exemple de l'interface graphique du programme d'ordinateur mettant en œuvre le procédé décrit ci-dessus et démontré à la fig. 3b. Afin de faciliter l'utilisation du procédé par le propriétaire du produit, la sortie sur l'interface graphique donnerait visuellement encore quelques informations additionnelles, par exemple la désignation de la série et/ou du modèle du produit ainsi que, naturellement, le numéro de série ou bien la caractéristique unique sélectionnée pour le but du certificat, et des informations concernant le fabricant. Ces informations, ou une partie de celles-ci, peuvent également être imprimées sur la surface de la carte à puce. La fig. 3a représente un exemple d'une interface graphique correspondante selon la présente invention d'une page de requête permettant de valider les certificats numériques d'authenticité, cette page étant destinée à apparaître juste avant la page représentée par la fig. 3b. Cela souligne que la présente invention fournit une solution technique convenable au problème de la fourniture d'un certificat d'authenticité infalsifiable dont la validité peut être vérifiée de manière simple, à tout moment et quasiment à tout endroit.

[0023] Le procédé pour la certification numérique d'authenticité de produits de luxe selon la présente invention comprend également l'étape de modification de l'état de validité dudit certificat numérique quand cela est voulu. Par exemple, il peut arriver que le produit de luxe et/ou la carte à puce cryptographique délivrée conjointement au produit de luxe au propriétaire du produit soient volés, perdus, demandent une réparation ou ont subis toute autre modification qui exige une mise à jour correspondante du certificat numérique. Le procédé proposé ici permet alors la modification de l'état du certificat numérique en permettant la réception des informations sur l'état de l'objet physique par l'autorité de certification. Une entrée correspondante dans les informations concernant l'état de l'objet physique, par exemple qu'il a été volé, est alors générée dans une base de données, par exemple sous forme de la liste de certificats problématiques (CRL) mentionnée ci-dessus et illustrée par exemple à la fig. 2. L'entrée dans la base de données est adaptée pour être lue, normalement par l'autorité de validation, et éventuellement également par l'autorité de certification, lorsque la validité du certificat numérique d'authenticité sur le support d'enregistrement est vérifiée.

[0024] De plus, le procédé selon la présente invention permet également de fournir des informations supplémentaires qui peuvent être intéressantes par rapport au produit de luxe en question. Hormis des informations mentionnées ci-dessus que le produit a été volé ou perdu par exemple, ces informations supplémentaires peuvent par exemple consister en d'autres caractéristiques de l'objet physique ou en toute autre information relative à l'objet, ou en des informations concernant le propriétaire ou le fabricant du produit. En utilisant le moyen informatique de réseau tel qu'expliqué ci-dessus, toute autre partie d'informations supplémentaires peut être fournie par le moyen informatique de réseau et l'interface graphique correspondante. Il est par exemple possible de fournir de cette façon des informations concernant la vente qui peuvent être maintenues online, par exemple dans le but de présenter une garantie numérique du produit. En outre, si la vérification ci-dessus du certificat numérique d'authenticité est en principe anonyme grâce au fait que la carte à puce ne concerne que le produit en question, on peut prévoir une possibilité par un programme d'ordinateur correspondant selon la présente invention pour permettre un enregistrement personnel du propriétaire du produit. Un tel propriétaire certifié pourrait alors obtenir l'accès, en utilisant un tel programme d'ordinateur, à plusieurs fonctions en rapport par exemple au produit qu'il a acheté ou à un club de propriétaires réunissant d'autres personnes ayant acquis des produits similaires. La puce cryptographique pourrait également comprendre des certificats numériques de conformité afin d'établir la conformité du procédé de la fabrication du produit avec un jeu prédéfini de règles, par exemple pour obtenir le label de conformité «Swiss made» ou tout autre label similaire. De tels labels sont délivrés par une autorité de contrôle correspondante et peuvent conférer une valeur additionnelle au procédé proposé pour la certification d'authenticité de produits de luxe, étant donné qu'il est facile d'ajouter un certificat numérique de conformité correspondant à la puce cryptographique comprenant un certificat numérique d'authenticité. Dans ce contexte, il doit être mentionné que le procédé selon la présente invention peut également permettre à la personne qui effectue la validation du certificat numérique d'authenticité de vérifier via le moyen informatique de réseau le cadre technique et opérationnel de l'autorité de certification ayant délivré le certificat. En particulier, cela concerne la police de certification (Certificate Policy/CP) et le protocole de la pratique de certification (Certificate Practice Statement/CPS).

[0025] Après avoir décrit ci-dessus le procédé pour la certification numérique d'authenticité de produits de luxe selon la présente invention, il est clair que l'invention concerne également un moyen de programme d'ordinateur enregistré dans un milieu accessible par ordinateur («computer readable médium») et qui est adapté pour la mise en œuvre du procédé. En particulier, un programme d'ordinateur correspondant fournit la fonctionnalité correspondante et l'interface graphique afin de mettre en œuvre les autorités de certification et de validation mentionnées ci-dessus qui sont habilitées à délivrer

le certificat numérique d'authenticité ou, respectivement, à vérifier sa validité, de tels programmes d'ordinateur pouvant facilement être réalisés par l'homme du métier ayant pris note des instructions contenues dans la présente description.

[0026] Comme mentionné ci-dessus, la présente invention se réfère également au support d'enregistrement correspondant, respectivement aux puces cryptographiques, afin de mettre en œuvre le procédé selon la présente invention. De telles puces comportent un certificat numérique d'authenticité comprenant des informations cryptées reflétant au moins une caractéristique d'un objet physique, et elles sont adaptées pour coopérer avec Ides moyens informatiques de réseau et une autorité de validation et/ou de certification afin de permettre à cette dernière de fournir l'état de validité du certificat numérique. De telles puces cryptographiques adaptées aux buts de la présente invention comprennent un logiciel («middle-ware») permettant de créer des informations cryptographiques in situ et au moins partiellement d'une manière non exportable.

[0027] Finalement, la présente invention se réfère également à l'utilisation du procédé proposé à la certification numérique d'authenticité dans le domaine de la protection d'objets physiques de valeur contre les contrefaçons. Des exemples de tels objets de valeur sont tous types de produits de luxe comme par exemple les montres précieuses ou la bijouterie.

[0028] A la lumière de la description ci-dessus de la présente invention, ses avantages sont évidents. Premièrement, un certificat numérique d'authenticité selon la présente invention est beaucoup plus sûr contre des essais de le copier grâce au fait que la clé privée est générée et enregistrée d'une manière non exportable sur la puce cryptographique. Par conséquent, le fait que le certificat n'est pas falsifiable n'est pas basé, comme dans les solutions conventionnelles de tels certificats, sur la complexité technique mais sur le principe décrit de la non-exportabilité de données à l'intérieur de la puce, et renforcé par la complexité des algorithmes mathématiques utilisés pour le cryptage ainsi que par l'électronique correspondante de la puce cryptographique. Donc, même si la substitution d'un seul produit authentique par une contrefaçon ayant le même identifiant mais qui est falsifié, accompagnée d'un certificat valide fourni par exemple par un voleur, ne peut pas être évitée par le présent procédé, celui-ci fournit quand même une solution technique pour une protection efficace contre une contrefaçon industrielle massive de produits d'une certaine valeur qui justifie l'utilisation de la procédure décrite ci-dessus, et ce en raison du fait que le certificat numérique lui-même ne peut pas être copié industriellement par des contrefacteurs. De plus, la validation du certificat numérique d'authenticité du produit peut être effectuée n'importe quand et n'importe où si voulu. L'état des certificats de validité peut également être modifié tel que désiré. Des informations additionnelles peuvent être introduites dans les certificats, respectivement dans les puces également tel que désiré. Ces certificats numériques d'authenticité ne changent pas le procédé de fabrication existant des produits et peuvent être délivrés par le fabricant ainsi que par tout autre distributeur ou revendeur autorisé des produits et peuvent être délivrés pour n'importe quel produit même si sa fabrication date de plusieurs années déjà.

Revendications

1. Procédé pour la certification numérique d'authenticité d'un objet physique, le procédé comprenant les étapes de
   – émettre (1, 2, 3, 4, 5) un certificat numérique d'authenticité stocké sur un support d'enregistrement et comprenant des informations signées numériquement qui reflètent au moins une caractéristique unique de l'objet physique,
   – vérifier (6, 7), à chaque fois que cela est voulu, la validité du certificat numérique d'authenticité par l'utilisation de moyens informatiques de réseau, ces, moyens informatiques de réseau coopérant avec ledit support d'enregistrement et une autorité de validation et/ou l'autorité de certification, et
   – modifier, à chaque fois que cela est voulu, l'état de validité dudit certificat numérique d'authenticité, caractérisé par le fait que
   – l'étape d'émettre (1, 2, 3, 4, 5) un certificat numérique d'authenticité comprend la génération (3) d'une paire de clés de cryptage asymétrique comprenant une clé publique et une clé privée sur ledit support d'enregistrement, ladite clé privée étant stockée de façon non-exportable sur le support d'enregistrement, et que
   – l'étape de vérifier (6, 7) la validité du certificat numérique d'authenticité comprend l'utilisation d'une fonctionnalité d'authentification mutuelle, en particulier l'utilisation des protocoles TLS ou SSL, afin de sortir, sensiblement en temps réel, l'état de validité dudit certificat numérique d'authenticité.
2. Procédé selon la revendication précédente, caractérisé par le fait que l'émission dudit certificat numérique d'authenticité stocké sur ledit support d'enregistrement comprend les étapes de
   – formuler (2, 3) une requête pour délivrer ledit certificat numérique d'authenticité destiné à être créé sur ledit support d'enregistrement, la requête comprenant des informations reflétant ladite au moins une caractéristique unique,
   – transmettre (4) ladite requête à l'autorité de certification pour approbation,
   – vérifier et, dans le cas d'une vérification positive, signer numériquement ladite requête par ladite autorité de certification,
   – transmettre (5) la requête signée au support d'enregistrement, et
   – finaliser la création du certificat numérique d'authenticité sur ledit support d'enregistrement par interaction avec ladite requête signée comprenant l'approbation de l'autorité de certification.
3. Procédé selon l'une des revendications 1 à 2, caractérisé par le fait que la formulation d'une requête pour délivrer ledit certificat numérique d'authenticité destiné à être créé sur ledit support d'enregistrement comprend la génération

(3) d'une paire de clés de cryptage asymétrique comprenant une clé publique et une clé privée sur ledit support d'enregistrement, ladite génération s'effectuant d'une façon non exportable par rapport à ladite clé privée.

4. Procédé selon la revendication précédente, caractérisé par le fait que la génération (3) de la paire de clés de cryptage asymétrique sur ledit support d'enregistrement est effectuée en utilisant des algorithmes cryptographiques de clés publiques.

5. Procédé selon l'une des revendications 1 à 4, caractérisé par le fait que la vérification de la validité du certificat numérique d'authenticité comprend les étapes de
– connecter (6) le support d'enregistrement comprenant le certificat numérique d'authenticité, par des moyens informatiques de réseau, à l'autorité de validation et/ou à l'autorité de certification,
– l'interaction (7) des moyens informatiques de réseau avec le support d'enregistrement et l'autorité de validation et/ou l'autorité de certification afin de permettre à l'autorité de validation et/ou l'autorité de certification l'accès au certificat numérique d'authenticité et/ou aux informations reflétant ladite au moins une caractéristique unique de l'objet physique, et
– sortir, sensiblement en temps réel, l'état de validité dudit certificat numérique d'authenticité par les moyens informatiques de réseau.

6. Procédé selon la revendication 5, caractérisé par le fait que la connexion (6) du support d'enregistrement via les moyens informatiques de réseau à l'autorité de validation et/ou de certification, et l'interaction (7) des moyens informatiques de réseau avec le support d'enregistrement et l'autorité de validation et/ou de certification comprend l'utilisation de protocoles de communication cryptographiques, en particulier l'utilisation des protocoles TLS ou SSL, et l'utilisation d'une fonctionnalité d'authentification mutuelle.

7. Procédé selon l'une des revendications 1 à 6, caractérisé par le fait que la modification de l'état de validité dudit certificat numérique d'authenticité sur le support d'enregistrement comprend les étapes de
– recevoir des informations sur l'état de l'objet physique par l'autorité de certification,
– créer une entrée correspondante aux informations d'état de l'objet physique dans une banque de données, cette entrée pouvant être lue par l'autorité de validation lorsqu'elle vérifie la validité du certificat numérique d'authenticité sur le support d'enregistrement.

8. Procédé selon l'une des revendications 1 à 7, caractérisé par le fait que le procédé comprend de plus les étapes de
– recevoir des informations supplémentaires reflétant une ou plusieurs autres caractéristiques de l'objet physique ou toute autre information relative à cet objet et/ou au propriétaire et/ou au fabricant de l'objet par l'autorité de certification,
– sortir, sur demande, toute partie desdites informations supplémentaires par les moyens informatique de réseau.

9. Support d'enregistrement pour la mise en œuvre du procédé selon l'une des revendications 1 à 8, caractérisé par le fait qu'il comporte ledit certificat numérique d'authenticité comprenant des informations signées numériquement reflétant ladite au moins une caractéristique de l'objet physique, et par le fait qu'il est adapté à coopérer avec les moyens informatiques de réseau et ladite autorité de validation et/ou de certification de telle façon que cette dernière puisse sortir l'état de validité dudit certificat numérique d'authenticité.

10. Support d'enregistrement selon la revendication 9, caractérisé par le fait qu'il est constitué d'une puce cryptographique comprenant des moyens de programmation d'ordinateur et/ou des moyens électroniques permettant l'enregistrement d'informations créés sur site ou importés dans la puce par des moyens sécurisés au moins partiellement d'une manière non exportable.

11. Support d'enregistrement selon la revendication 10, caractérisé par le fait que la puce cryptographique comprend des moyens de programmation d'ordinateur permettant la génération sur site des informations cryptographiques.

12. Support d'enregistrement selon l'une des revendications 10 à 11, caractérisé par le fait que la puce est intégrée dans une carte à puce cryptographique.

13. Application du procédé selon l'une des revendications 1 à 8 pour la certification numérique d'authenticité d'un objet physique de valeur.

14. Application selon la revendication 13, caractérisée par le fait que l'objet de valeur est constitué par des produits de luxe, en particulier des montres précieuses ainsi que des bijoux.

Figure.1

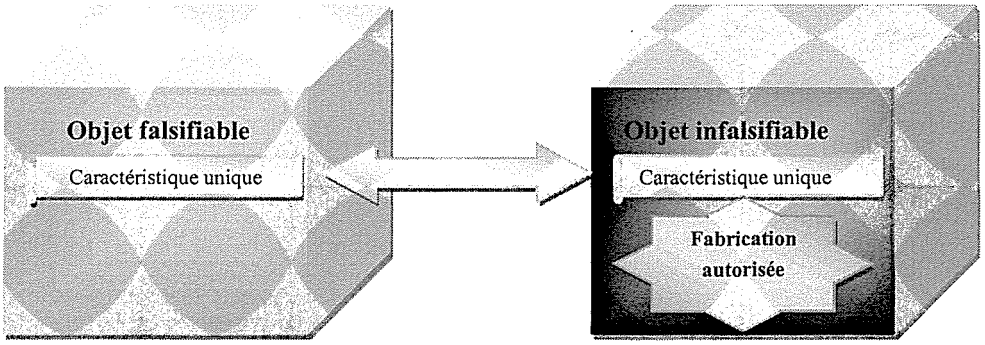


Figure.2

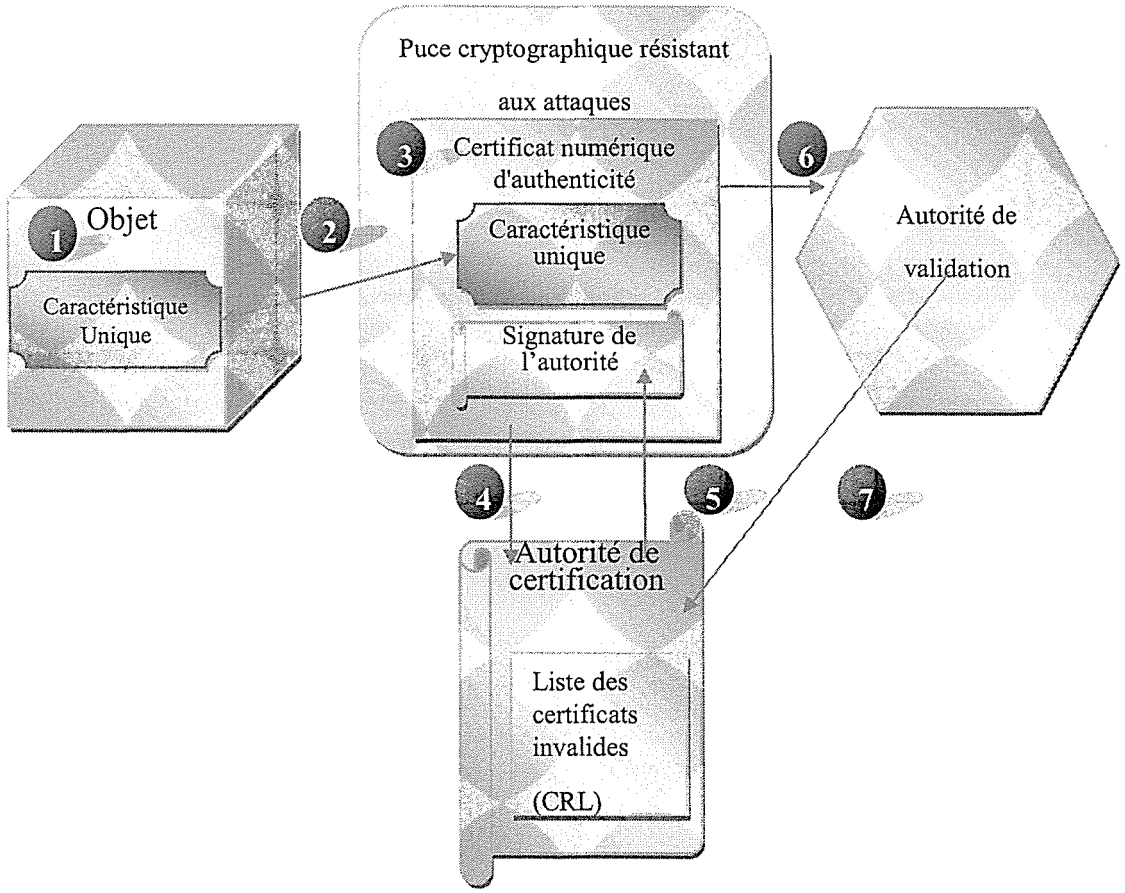
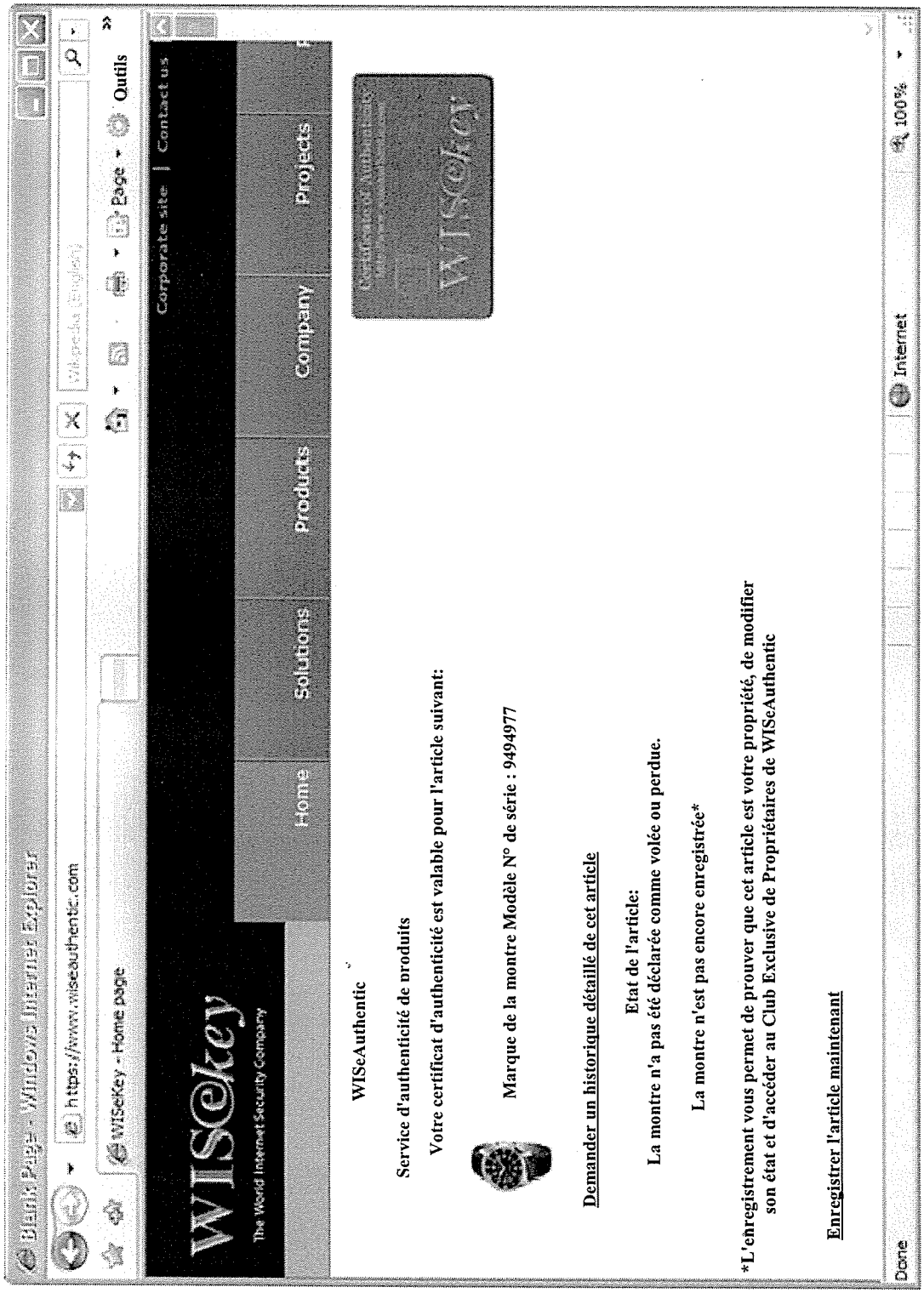


Figure.3a

CH 699 083 B1

Figure.3b


Blank Page - Windows Internet Explorer
https://www.wiseauthentic.com
WISeKey - Home page
Page
Outils
Corporate site | Contact us
WISeKey
The World Internet Security Company
Home
Solutions
Products
Company
Projects
WISeAuthentic
Service d'authenticité de nroduits
Votre certificat d'authenticité est valable pour l'article suivant:
Marque de la montre Modèle N° de série : 9494977
Demander un historique détaillé de cet article
Etat de l'article:
La montre n'a pas été déclarée comme volée ou perdue.
La montre n'est pas encore enregistrée*
*L'enregistrement vous permet de prouver que cet article est votre propriété, de modifier son état et d'accéder au Club Exclusive de Propriétaires de WISeAuthentic
Enregistrer l'article maintenant
Done
Internet
100%