Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2732247 C 2016/06/07

(11)(21) 2 732 247

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(86) Date de dépôt PCT/PCT Filing Date: 2008/07/28
(87) Date publication PCT/PCT Publication Date: 2010/02/04
(45) Date de délivrance/Issue Date: 2016/06/07
(85) Entrée phase nationale/National Entry: 2011/01/26
(86) N° demande PCT/PCT Application No.: IB 2008/053022
(87) N° publication PCT/PCT Publication No.: 2010/013090

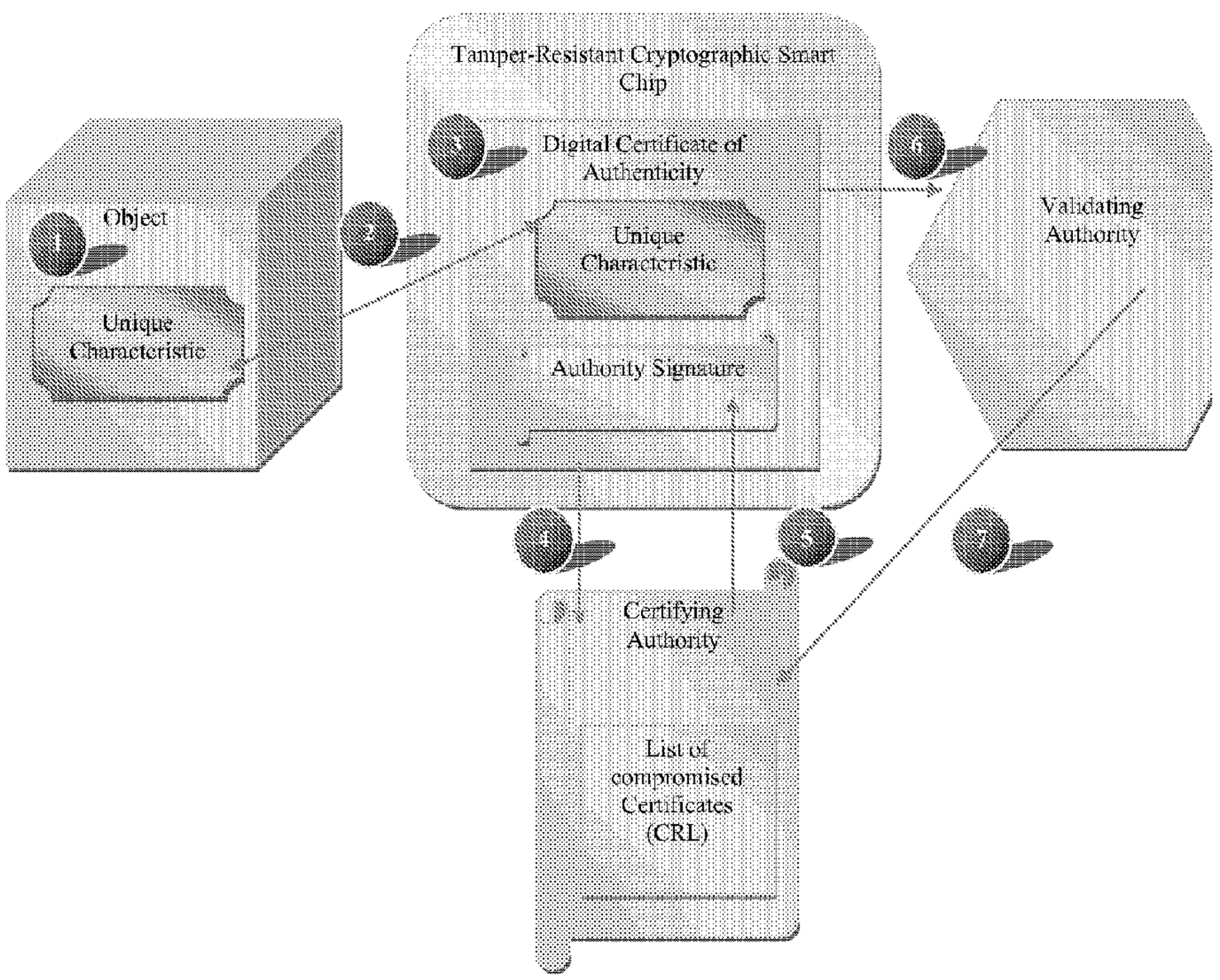
(51) Cl.Int./Int.Cl. *G06F 21/64* (2013.01)

(72) Inventeurs/Inventors:
DARBELLAY, JEROME, CH;
BLACKMAN, KEVIN, CH;
MORENO, CARLOS, CH;
CREUS MOREIRA, JUAN CARLOS, CH

(73) Propriétaire/Owner:
WISEKEY SA, CH

(74) Agent: BORDEN LADNER GERVAIS LLP

(54) Titre : PROCEDE ET MOYEN D'AUTHENTIFICATION NUMERIQUE DE MARCHANDISES DE VALEUR
(54) Title: METHOD AND MEANS FOR DIGITAL AUTHENTICATION OF VALUABLE GOODS



(57) Abrégé/Abstract:
The present invention is related to a method for digital certification of authenticity of a physical object, to corresponding computer program means and storage means, as well as to the use of the method for digital certification of authenticity of a physical object of value. The method comprises the steps of issuing (1, 2, 3, 4, 5) a storage means comprising a digital certificate of authenticity including encrypted information reflecting at least one characteristic unique to the physical object, checking (6, 7), whenever required, the validity of the digital certificate of authenticity by use of network computing means, the network computing means cooperating with said storage means and a validating and/or a certifying authority such as to output sensibly in real time the status of validity of said digital certificate of authenticity, and modifying the status of validity of said digital certificate of authenticity, whenever required.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 February 2010 (04.02.2010)

PCT

(10) International Publication Number
WO 2010/013090 A1

(51) **International Patent Classification**:
G06F 21/24 (2006.01)

(21) **International Application Number**:
PCT/IB2008/053022

(22) **International Filing Date**:
28 July 2008 (28.07.2008)

(25) **Filing Language**: English

(26) **Publication Language**: English

(71) **Applicant** *(for all designated States except US)*: **WISeKey SA** [CH/CH]; 29, route de Pré-Bois World Trade Center, CH-1217 Meyrin / Geneve (CH).

(72) **Inventor; and**
(75) **Inventor/Applicant** *(for US only)*: **DARBELLAY, Jérôme** [CH/CH]; 2, route François-Louis Duvillard, CH-1295 Tannay (CH).

(74) **Agents**: **SAMMER, Thomas** et al.; c/o BUGNION S.A., 10, route de Florissant P.O. Box 375, CH-1211 Geneve 12 (CH).

(81) **Designated States** *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

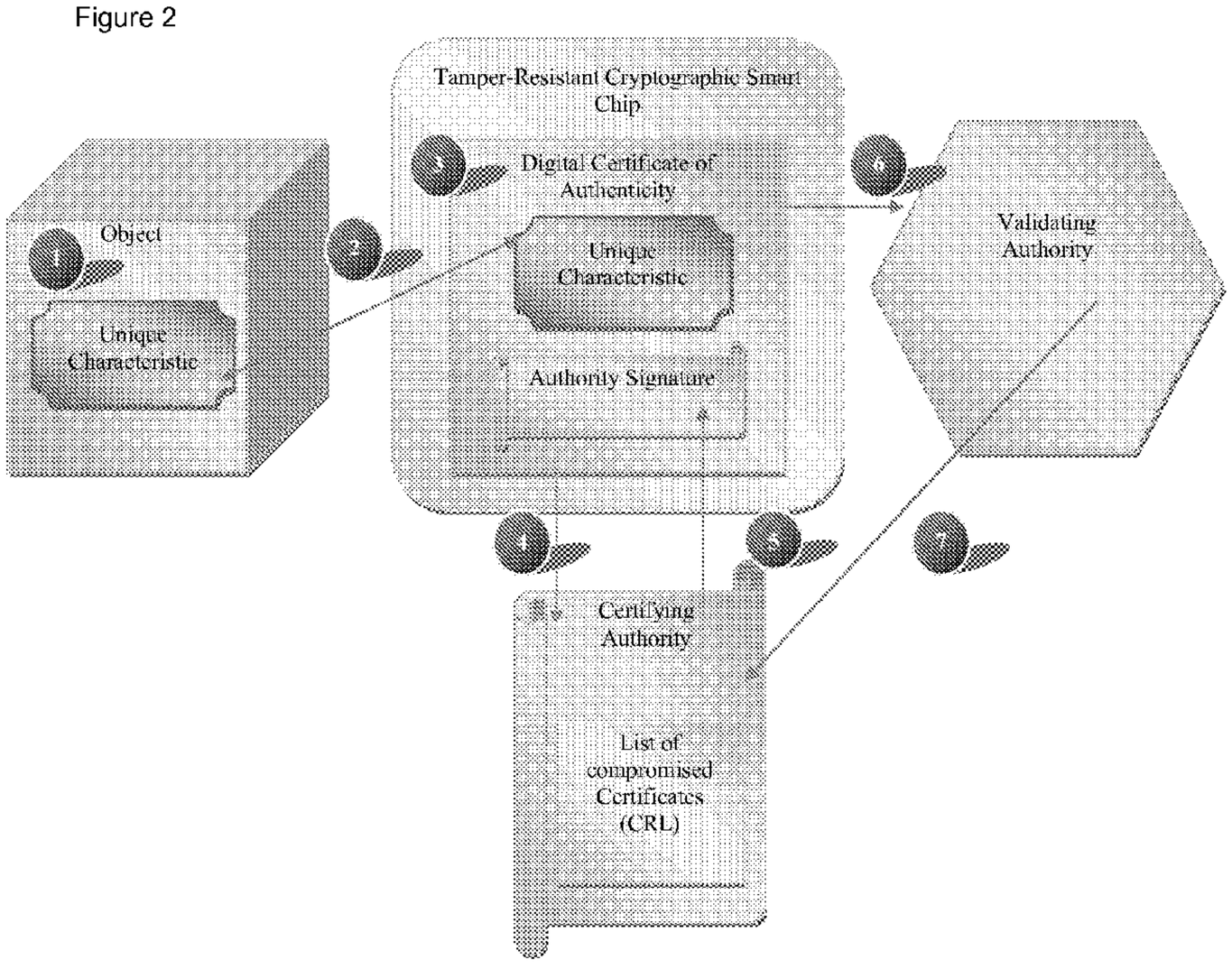
(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) Title: METHOD AND MEANS FOR DIGITAL AUTHENTICATION OF VALUABLE GOODS

Figure 2



(57) Abstract: The present invention is related to a method for digital certification of authenticity of a physical object, to corresponding computer program means and storage means, as well as to the use of the method for digital certification of authenticity of a physical object of value. The method comprises the steps of issuing (1, 2, 3, 4, 5) a storage means comprising a digital certificate of authenticity including encrypted information reflecting at least one characteristic unique to the physical object, checking (6, 7), whenever required, the validity of the digital certificate of authenticity by use of network computing means, the network computing means cooperating with said storage means and a validating and/or a certifying authority such as to output sensibly in real time the status of validity of said digital certificate of authenticity, and modifying the status of validity of said digital certificate of authenticity, whenever required.

WO 2010/013090 A1

Method and means for digital authentication of valuable goods

The present invention pertains to a method for digital certification of authenticity of a physical object of value, to corresponding computer program means and storage means, as well as to the use of the method for the digital certification of authenticity of a physical object of value.

In general, the present invention is situated in the context of protecting objects of a certain value, in particular luxury goods, against counterfeiting, which becomes more and more difficult in the present days. Nowadays, it is current practice that a manufacturer of luxury goods, such as e.g. watches or precious jewellery, issues a paper certificate of authenticity corresponding to the sold luxury product and handed out simultaneously with the product when the latter is acquired. Such paper certificates use the fact that luxury products of a certain value usually have a unique characteristic, such as e.g. a serial number, which, however, just as the object as a whole, usually is forgeable. Therefore, the producer of a forgeable, valuable object associates it with said paper certificate which reproduces the unique identifier. If the paper certificate is considered to be non-forgeable, authenticity of the valuable object can be established by requesting presentation of the certificate. Of course, the whole relies on that the paper certificate is produced by an authorized entity and cannot be faked. A typical example of the above said are e.g. watch brands selling high quality watches together with a paper certificate edited by the manufacturer or reseller and reproducing the serial number of an individual watch.

However, the above procedure inherently comprises several problems. First, the above mentioned solution relies on that it is technically impossible to fake the paper certificate. It is, however, known that such certificates based on secure

paper, watermarking, RFID or other conventional techniques do no longer offer the guarantee of not being forgeable, unless the technical complexity of the procedure applied is enormously high, which on the other hand complicates the production process and renders it very expensive. This led to the commonly known race between manufacturers of valuable goods and counterfeiters who also increase their technical capabilities not only of producing falsified goods but also of copying such certificates. Therefore, there is a need for producers of valuable goods to find a technical solution allowing them to produce effectively non-forgeable certificates of authenticity to be handed out simultaneously with the acquired good.

Secondly, the presently known solutions for certifying authenticity of a given physical object do have the further disadvantage that, even if the certificate in the hands of the owner of a given valuable object is not faked, it is difficult and painful for the owner, who does not know this beforehand, to verify it. For example, should the owner of a given object with such a certificate doubt its authenticity, or should he contemplate its acquisition without passing by an official reseller, it would traditionally be necessary to send the certificate by mail to the manufacturer of the goods or another corresponding entity for verification. Therefore, there is a need for producers of such goods to find technical solutions simplifying this process.

Furthermore, conventional certificates of authenticity of valuable goods using e.g. secure paper, watermarking or RFID usually do only mention the main properties of the product together with said unique identifier like the serial number of the product. Once the certificate has been issued, it is no longer possible to flexibly add further information on the product or to easily modify the status of validity of the certificate associated to a given good. Therefore, there is also a need for the producer of such goods to find a technical solution allowing more flexible use and modification of the data contained in the certificate and relating to the goods sold.

It is the object of the present invention to overcome the above mentioned difficulties and to realize a method for certification of authenticity of a physical object of a certain value, the method providing highest possible level of security that the certificate of the authenticity cannot be faked. Furthermore, a verification of the certificate of authenticity should be much easier as compared to the known solutions and data relating to the authenticated object and/or its owner should be able to be included in the certificate in a more flexible and easier way.

To this effect, the present invention proposes a method for digital certification of authenticity of physical objects as further described herein.

In particular, the method for digital certification of authenticity according to the present invention is characterized by the fact that the method comprises the steps of issuing a storage means comprising a digital certificate of authenticity including encrypted information reflecting at least one characteristic unique to the physical object, checking, whenever required, the validity of the digital certificate, and modifying the status of validity of said certificate, also whenever required. The fact that digital certificates issued and signed by authorized certifying authorities and stored e.g. on a cryptographic chip are not forgeable provides a solution to the above mentioned technical problem. Moreover, the validity of the digital certificate may be easily verified all over the world by using secure communication on nowadays common networks like the Internet. Furthermore, the digital certificate may flexibly be provided with additional information related to the authenticated goods or its status be changed.

The invention also relates to corresponding computer program means implementing the method of digital certification of authenticity according to the present invention.

Also, the present invention proposes storage means adapted for the implementation of said method, the storage means is described in greater detail below and, in particular being adapted to host said digital certificate of authenticity as well as to cooperate with a computing network means and a validating and/or a certifying authority to verify the validity of said certificate.

In particular, the present invention proposes the use of the method according to the present invention in the context of authenticating physical objects of great value, like e.g. precious watches, jewellery or other luxury goods.

Other features and advantages of the present invention are mentioned in the description disclosing in the following, with reference to the figures, the invention in more detail.

The attached figures exemplarily and schematically illustrate the principles of the present invention.

Figure 1 schematically illustrates the principle of certification of authenticity used both in prior art as in the solution according to the present invention.

Figure 2 is a schematic overview of the steps of the method for digital certification of authenticity of a physical object according to the present invention.

Figures 3a and 3b show an example of a graphical interface of a corresponding computer program during the process of checking the validity of the

digital certificate, this at the stage of requesting the check respectively once the validity of the certificate has been confirmed.

In the following, the invention shall be described in detail with reference to the above mentioned figures.

Figure 1 illustrates the principle used both in conventional certificates of authenticity based on secure paper, watermarking or other traditional technologies as well as in the context of the present invention. The forgeable object like e.g. a watch or another luxury product presented on the left side of figure 1 comprises a unique characteristic like e.g. a serial number. The certificate of authenticity edited by an authorized entity and considered to be non-forgeable reproduces this unique characteristic and is symbolically illustrated on the right side of figure 1. Whereas the non-forgeability of traditional certificates is no longer valid as soon as counterfeiters reach the corresponding level of technology required to copy these certificates, duplicating digital certificates of authenticity according to the present invention is much more difficult, as the following description will clarify.

Figure 2 schematically illustrates the different steps during a process of digital certification of authenticity of a physical object according to the present invention. Of course, a physical object like a luxury product first has to be provided, after its production, with a unique identifier such as an alphanumerical serial number, this being indicated symbolically by reference number 1 in figure 2. The serial number may for example be engraved on the luxury product or the latter may comprise any other unique identifier adapted for this purpose.

As a first step of the method according to the invention, a digital certificate of authenticity corresponding to said luxury product has to be created. To this effect, a storage means comprising a digital certificate of authenticity including

digitally signed information that reflects at least the above mentioned unique characteristic is issued. Storage means adapted for the purposes of the present invention typically consist in cryptographic smart chips comprising computer program means allowing to create cryptographic information on-board and - at least partially - in non-exportable manner. Such smart chips are usually integrated into a cryptographic smart card. The terms “cryptographic smart chip” respectively “cryptographic smart card” will be used in the following description widely synonymously to the term “storage means”. Such cryptographic smart chips are adapted to host digital certificates of authenticity according to the present invention, which then may be verified by external computing means.

Issuing a digital certificate according to the present invention therefore comprises providing such a cryptographic smart chip. The chip is then inserted into reading and processing means such as smart card reader in an ordinary PC used as input and output means during issuing the digital certificate. Afterwards, as it is indicated by reference number 2 in figure 2, a request for issue of said digital certificate of authenticity of the luxury product is formulated. The request file for the digital certificate reproduces said at least one characteristic unique to the luxury product by including encrypted information reflecting said at least one unique characteristic. The unique characteristic like an engraved serial number may e.g. be placed in the common name field of the certificate. The request file may be formulated based on the X.509 certificate issuance standard known to the person skilled in the art.

For issuing a digital certificate, the present invention uses asymmetric encryption, this method being the best solution for such purposes according to present knowledge. Therefore, formulating said request for issue of the digital certificate of authenticity to be created on said storage means comprises, such as indicated symbolically by reference number 3 in figure 2, generating an

asymmetric encryption key pair comprising a public and a private key. The generation of said asymmetric encryption key pair takes place on-board on said storage means and in such a manner that the private key is non-exportable. This involves the above mentioned computer program means on the cryptographic smart chip allowing to create cryptographic information on-board and at least partially in a non-exportable manner, such programs also being called “smart chip middleware “ or “drivers”. Alternatively, the generation of the asymmetric encryption key pair is not performed on-board, but by secure means external to the card, and will be saved after generation on the chip such that the private is non-exportable as well as, of course, unique. Preferably, generating the asymmetric encryption key pair, either on-board the cryptographic smart chip or by said secure means, is done by using public key cryptographic algorithms such as the Rivest-Shamir-Adleman (RSA) cryptographic algorithm or elliptic curve cryptography (ECC), this also being known to a person skilled in the art. The private key of the digital certificate of authenticity being generated in secure and unique manner, on the cryptographic smart chip or by said secure means, and in any case being stored thereon in a non-exportable manner, this provides for ideal non-duplicability of the certificate respectively the chip, rendering it tamper–resistant and non-forgeable in a very effective manner.

After having formulated the request for issue of a digital certificate such as described above, the request is sent to a certifying authority for approval, such as indicated symbolically by reference number 4 in figure 2. The certifying authority must be controlled and operated by authorized persons, eventually by means of automated processes, and may for example be identical to the producer of the luxury product to be certified for authenticity, or may correspond to an entity designed by said producer. Upon receipt of said request by the certifying authority, the integrity of the certificate and/or the uniqueness of the request will be verified with respect to several parameters, such as operator rights. If the verification step

succeeds, the certifying authority digitally signs the request file for a digital certificate with its own certificate, the certifying authority certificate, and sends the digitally signed request file back to the storage means inserted into the reading and processing means. This step is indicated in figure 2 by reference number 5. Upon receipt of the signed request in the cryptographic smart chip, the above mentioned middleware completes creation of the digital certificate of authenticity by interaction with the signed request comprising approval of the certifying authority. Several aspects of this procedure may be done according to the standard procedure for X.509 certificate issuance, this is however not absolutely necessary insofar as technically equivalent alternatives are or will become available.

Once a digital certificate of authenticity has been issued on a cryptographic smart card according to the above described method, and once a luxury product has been sold in combination with its corresponding authenticity card, validity of the digital certificate and therefore authenticity of the corresponding luxury product may be checked by the owner of the product, whenever and wherever required, by use of network computing means. To this effect, the network computing means cooperates with said storage means and the a validating and/or the certifying authority such as to output sensibly in real time the status of validity of said digital certificate of authenticity. In this context, it is to be noted that the validating authority may be identical to the certifying authority, but this is not necessarily the case, as the former may also consist in one or several corresponding entities.

Actually, for checking the validity of the digital certificate of authenticity, one may insert the cryptographic smart card comprising the digital certificate of authenticity to any reading and processing means, i.e. to any computer being equipped with a smart card reader and being configured correspondingly. Then, validity of the certificate on the smart card can be checked against a web server

also configured for this purpose, this operation involving again the middleware on the smart chip. To this effect, the smart chip comprising the digital certificate of authenticity connects via network computing means to the validating authority and/or the certifying authority, such as illustrated symbolically by reference number 6 in figure 2. The validating authority consists typically in the above mentioned web server which is configured to be adapted to use cryptographic communication protocols such as TLS (Transport Layer Security) or SSL (Secure Socket Layer), preferably TLS, and including handshake functionality in order to provide for mutual authentication during the communication process, alternative secure communication means providing adequate functionality also being adapted to be used for this purpose. The above mentioned technical terms are known to the person skilled in the art and do not need any further explanation here.

The validating authority checks the validity period of the certificate as well as whether it has been revoked, the latter against the certifying authority using e.g. a certificate revocation list (CRL) generally hosted at the certifying authority or an online certificate status protocol (OCSP), such as indicated symbolically by reference number 7 in figure 2. Both of these are a kind of list comprising information on issued certificates, in particular a corresponding entry in case individual certificates were compromised. Thus, this step comprises interaction of the network computing means with both the storage means and the validating and/or the certifying authority such as to allow access by said validating and/or certifying authority to the digital certificate of authority. Actually, the validity of the certificate is checked by public key exchange between the validating authority and the smart chip such as known to the person skilled in the art, and by crosscheck of the certificate with the above mentioned CRL or OCSP. This step usually involves verifying the validity of the certificate of the certifying authority known to the person skilled in the art as certificate chain validation. Then, the output in the form of the status of validity of the certificate is performed sensibly in real time via the network

computing means. The output may e.g. consist in the fact that the certificate of authenticity is valid, i.e. that the luxury product is authentic, such as illustrated in the example of a graphical interface of computer program means implementing the above described method shown in figure 3b. Usually, in order to facilitate use of the method by the owner of the product, the output on the graphical interface would also give some additional information, like for example the name of the series and/or of the model of the product as well as, of course, the serial number respectively the unique characteristic chosen for the purpose of the certificate, and information relative to the producer. For reasons of convenience, this information or parts of it may by the way be printed on the surface of the smart card. Figure 3a represents an example of a corresponding graphical interface according to the present invention for a request page allowing to validate digital certificates of authenticity, this page being supposed to appear just before the one shown in figure 3b. This underlines that the present invention provides for a convenient technical solution to the problem of providing a non-forgeable certificate of authenticity which may easily, whenever as well as almost wherever be challenged for its validity.

The method for digital certification of authenticity of luxury goods according to the present invention also includes the step of modifying the status of validity of said digital certificate whenever required. It might e.g. happen that the luxury product and/or the cryptographic smart card handed out together with the luxury product to the owner of the product are stolen, lost, or need repair, or suffer any other modification which would require corresponding update of the digital certificate. Therefore, the presently proposed method allows modifying the status of the digital certificate by allowing to receive information on the status of the physical object by the certifying authority. An entry corresponding to the status information of the physical object, e.g. that it has been stolen, is then created in a database, for example in the form of the above mentioned list of compromised

certificates (CRL) illustrated exemplarily in figure 2. The entry in the database is adapted to be read, usually by the validating authority, eventually also by the certifying authority, whenever checking the validity of the digital certificate of authenticity on the storage means occurs.

Additionally, the method according to the present invention also allows to provide for supplementary information which may be interesting with respect to the luxury product in question. Apart from the above mentioned information that the product was e.g. stolen or lost, such supplementary information may inter alia consist in other characteristics of the physical object or any other information related to the object or information related to the owner or to the producer of the product. By using the network computing means such as explained above, any part of such supplementary information may be put out via the network computing means and the corresponding graphical interface. It is e.g. possible in this way to provide for sales related information which may be maintained online, e.g. aiming at presenting a digital guarantee for the product. Furthermore, if the above verification of the digital certificate of authenticity is in principle anonymous due to the fact that the smart card is only related to the product in question, a facility may be provided by corresponding computer program means according to the present invention to allow personal registration of the owner of the product. Such a certified owner would then e.g. have access by using such computer program to several functions related for example to the product he acquired or to an owners' club of other persons having acquired similar goods. Also, the cryptographic smart chip may additionally include digital certificates of compliance in order to establish the compliance of the manufacturing process of the given product with a predefined set of rules, such as e.g. to obtain the label "Swiss made" or any other similar label. Such labels are issued by the corresponding controlling entity and may give additional value to the proposed method for certifying authenticity of luxury goods, it being easy to add a corresponding digital certificate of compliance

on the cryptographic smart chip comprising the digital certificate of authenticity. It should be mentioned in this context that the method according to the invention may also allow the person performing the validation of the digital certificate of authenticity to check via the network computing means the technical and operational framework of the certifying authority having issued the certificate. In particular, this concerns the certificate policy (CP) and the certificate practice statement (CPS).

After having disclosed above the method of digital certification of authenticity of luxury goods according to the present invention, it is clear that the invention also concerns computer program means stored in a computer readable medium which is adapted to implement this method. Especially, a corresponding computer program provides the corresponding functionality and the graphical interface in order to implement the above mentioned certifying and validating authorities which are entitled to issue respectively to check the validity of the digital certificate of authenticity. Such computer program means may readily be realized by a person skilled in the art having taken note of the teaching in the present disclosure.

As already mentioned above, the present invention is also related to corresponding storage means, respectively cryptographic smart chips, for the implementation of the method according to the present invention. Such chips comprise a digital certificate of authenticity including encrypted information reflecting at least one characteristic of a physical object and are adapted to cooperate with network computing means and a validating and/or certifying authority such as to allow the latter to output the status of validity of the digital certificate. Such cryptographic smart chips adapted to the purposes of the present invention comprise middleware allowing to create cryptographic information on-board and at least partially in non-exportable manner.

Finally, the present invention is also related to the use of the proposed method for digital certification of authenticity in the field of protecting physical objects of value against counterfeiting. Examples of such objects of value are any type of luxury goods like e.g. precious watches or jewellery.

In light of the above description of the present invention, its advantages are clear. Primarily, a digital certificate of authenticity according to the present invention is much safer against attempts to duplicate it due to the fact that the private key is generated and stored in a non-exportable manner on the cryptographic smart chip. Therefore, non-forgeability of the certificate does not rely, such as in conventional solutions for such certificates, on technical complexity, but on said principle of non-exportability of data inside the chip, further enhanced by the complexity of the mathematical algorithms used for encryption as well as corresponding electronics of the cryptographic smart chip. Thus, even if substitution of a single authentic product by a counterfeited item showing the same, but falsified unique identifier together with a valid certificate acquired e.g. by theft cannot be avoided by the present method, it nevertheless provides for a technical solution for an efficient protection against massive, industrial counterfeiting of products having a value which justifies deployment of the above described procedure, due to the fact that the digital certificate itself cannot be duplicated industrially by counterfeiters. Moreover, validation of the digital certificate of authenticity of the product may be performed wherever and whenever required. Also, the status of the certificates of validity may be modified such as desired. Additional information may be included into the certificate respectively the smart chips also such as desired. Such digital certificates of authenticity do not alter the existing manufacturing process of the goods and may be issued by the manufacturer as well as by any authorized distributor or reseller of the goods, and may be issued for any product, even if its production dates back years ago.

CLAIMS:

1. A method for digital certification of authenticity of a physical object, the method comprising:

issuing a storage device comprising a digital certificate of authenticity including digitally signed information reflecting at least one characteristic unique to the physical object, the physical object being an article of manufacture, and the digital certificate of authenticity comprising the at least one characteristic unique to the physical object;

checking, whenever required, validity of the digital certificate of authenticity by use of a network computer, the network computer cooperating with said storage device and a validating authority or a certifying authority; and

modifying a status of validity of said digital certificate of authenticity, whenever required, by updating a certificate revocation list hosted at the validating authority or certifying authority,

wherein, the step of issuing a storage device comprises generating an asymmetric encryption key pair comprising a public key and a private key on said storage device, said private key being stored in non-exportable manner on said storage device, and the step of checking the validity of the digital certificate of authenticity comprises use of mutual authentication functionality in a form of the Transport Layer Security (TLS) or Secure Socket Layer (SSL) protocols, enabling an output in real time of the status of validity of said digital certificate of authenticity.

2. The method according to claim 1, wherein issuing said storage device includes:

formulating a request for issuance of said digital certificate of authenticity to be created on said storage device, the request including information reflecting said at least one unique characteristic;

sending said request to the certifying authority for approval;

verifying and, if positively verified, digitally signing said request by said certifying authority;

sending the signed request to the storage device; and

completing creation of the digital certificate of authenticity on said storage device by interaction with said signed request comprising approval of the certifying authority.

3. The method according to claim 1, wherein generating the asymmetric encryption key pair on said storage device is done by using public key cryptographic algorithms.

4. The method according to claim 1, wherein checking the validity of the digital certificate of authenticity comprises:

connecting the storage device comprising the digital certificate of authenticity via the network computer to the validating authority or the certifying authority;

interaction of the network computer with the storage device and the validating authority or the certifying authority allow enabling access by said validating authority or certifying authority to the digital certificate of authenticity or to the information reflecting at least one characteristic unique to the physical object;

outputting in real time the status of validity of said digital certificate of authenticity via the network computer.

5. The method according to claim 1, wherein modifying the status of validity of said digital certificate of authenticity on the storage device comprises:

receiving information on the status of the physical object by the certifying authority; and

creating an entry corresponding to the status information of the physical object in a database, the entry being adapted to be read by the validating

authority whenever checking of the validity of the digital certificate of authenticity on the storage device occurs.

6. The method according to claim 1, wherein the method further comprises:

receiving supplementary information reflecting one or more other characteristics of the physical object or any other information related to that object or to the owner or the producer of that object by the certifying authority; and

outputting, on demand, any part of said supplementary information via the network computer.

7. The method according to claim 1 for digital certification of authenticity of a physical object of value.

8. The method according to claim 7, wherein the physical object of value consists of luxury goods.

9. The method according to claim 8, wherein the luxury goods comprise a watch.

10. The method according to claim 8, wherein the luxury goods comprise jewelry.

11. The method according to claim 1, wherein checking the validity of the digital certificate of authenticity comprises accessing the private key for the mutual authentication functionality without entering any identification information.

12. A non-transitory computer readable medium storing a computer program to cause a computer to implement a method for digital certification of authenticity of a physical object, the method comprising:

issuing a storage device comprising a digital certificate of authenticity including digitally signed information reflecting at least one characteristic unique to the physical object, the physical object being an article of manufacture, and the digital certificate of authenticity comprising the at least one characteristic unique to the physical object;

checking, whenever required, validity of the digital certificate of authenticity by use of a network computer, the network computer cooperating with said storage device and a validating authority or a certifying authority; and

modifying a status of validity of said digital certificate of authenticity, whenever required, by updating a certificate revocation list hosted at the validating authority or certifying authority,

wherein, the step of issuing a storage device comprises generating an asymmetric encryption key pair comprising a public key and a private key on said storage device, said private key being stored in non-exportable manner on said storage device, and the step of checking the validity of the digital certificate of authenticity comprises use of mutual authentication functionality in a form of the Transport Layer Security (TLS) or Secure Socket Layer (SSL) protocols, enabling an output in real time of the status of validity of said digital certificate of authenticity.

Figure 1

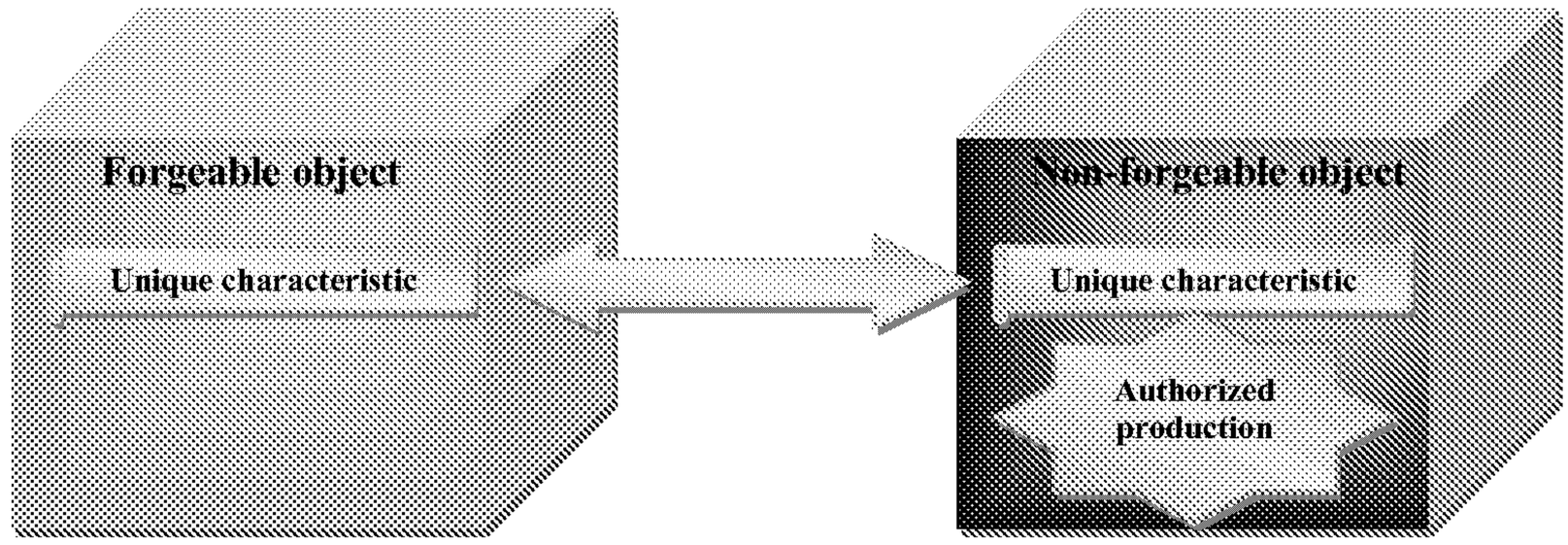


Figure 2

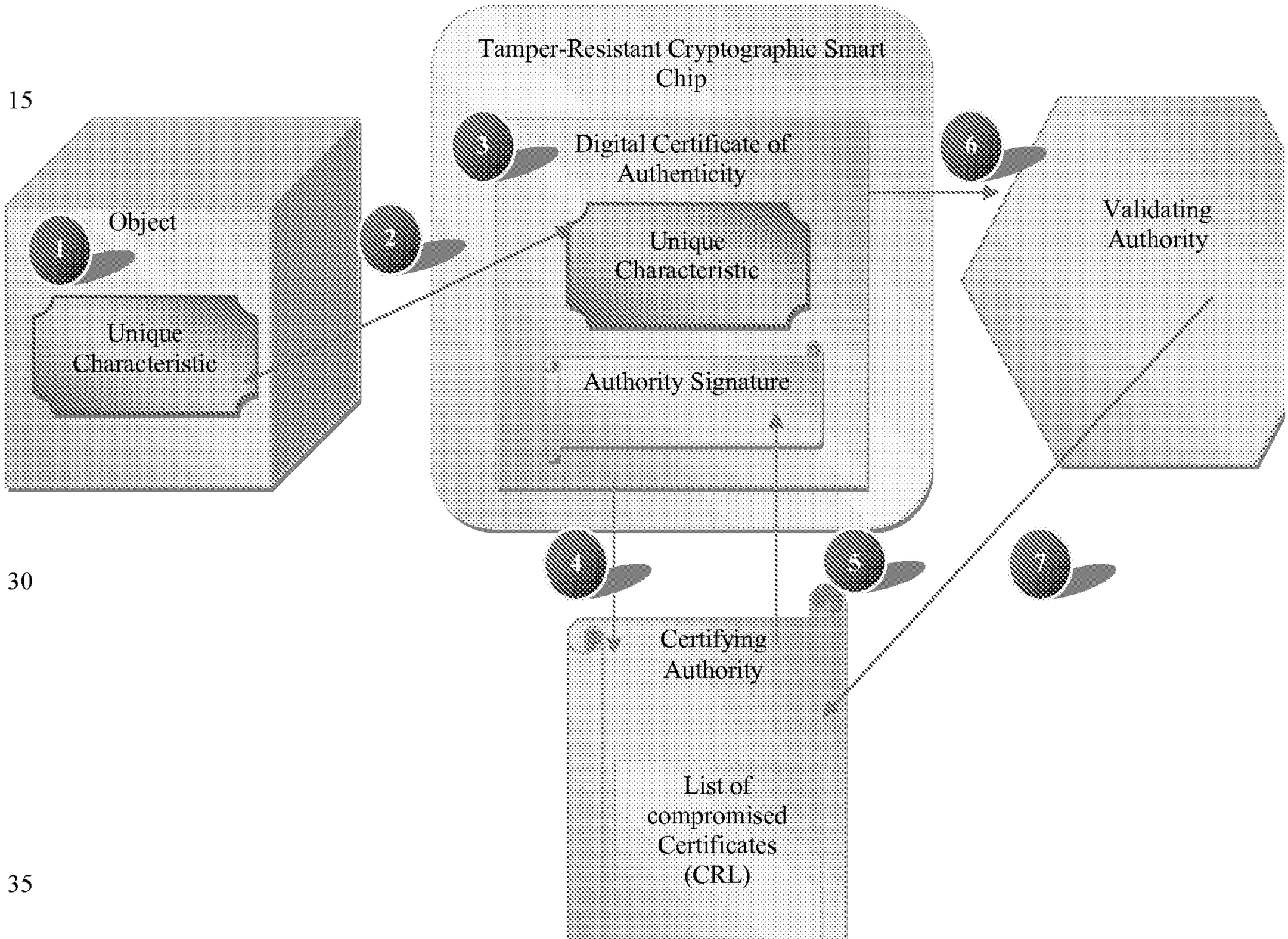


Figure 3a

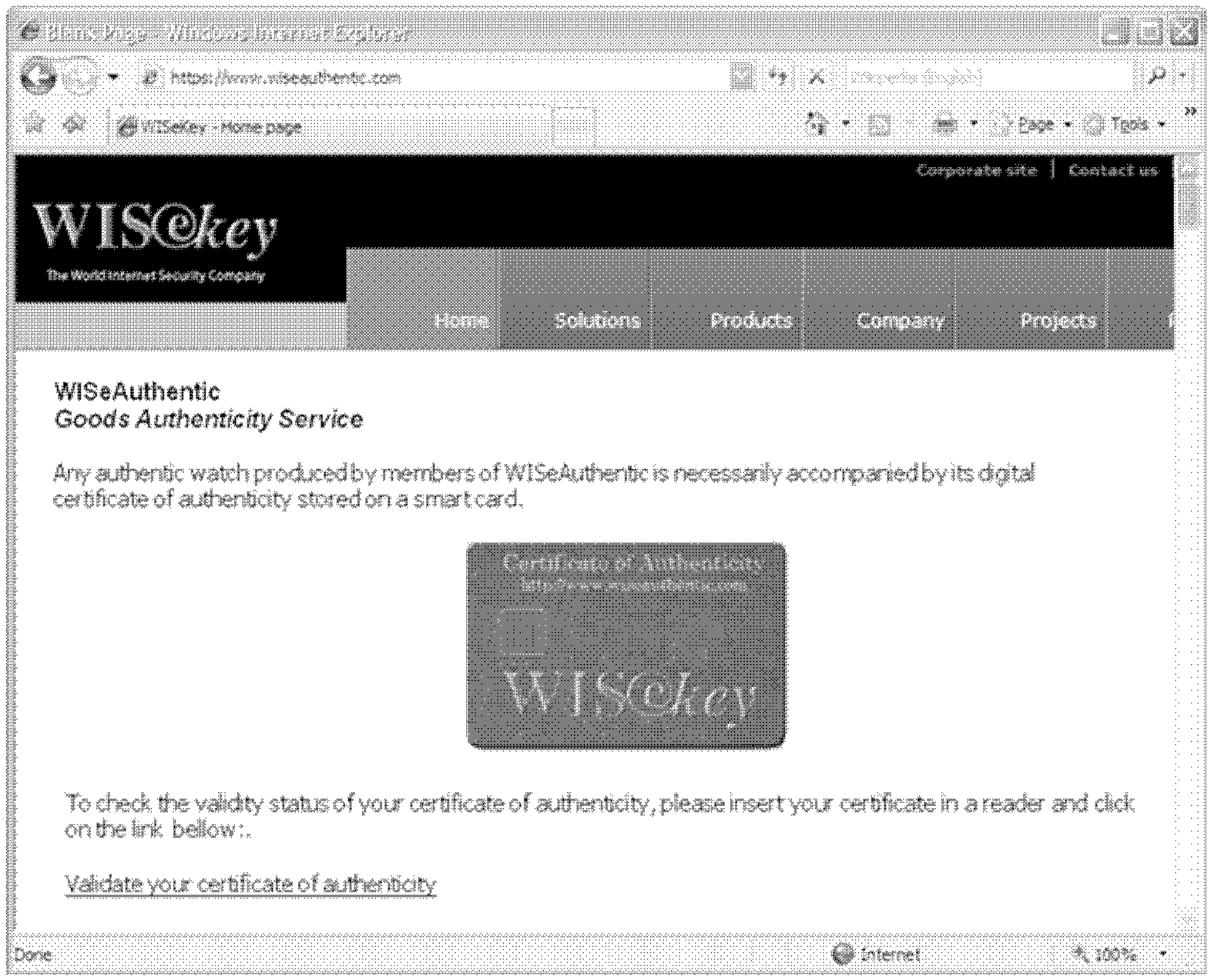
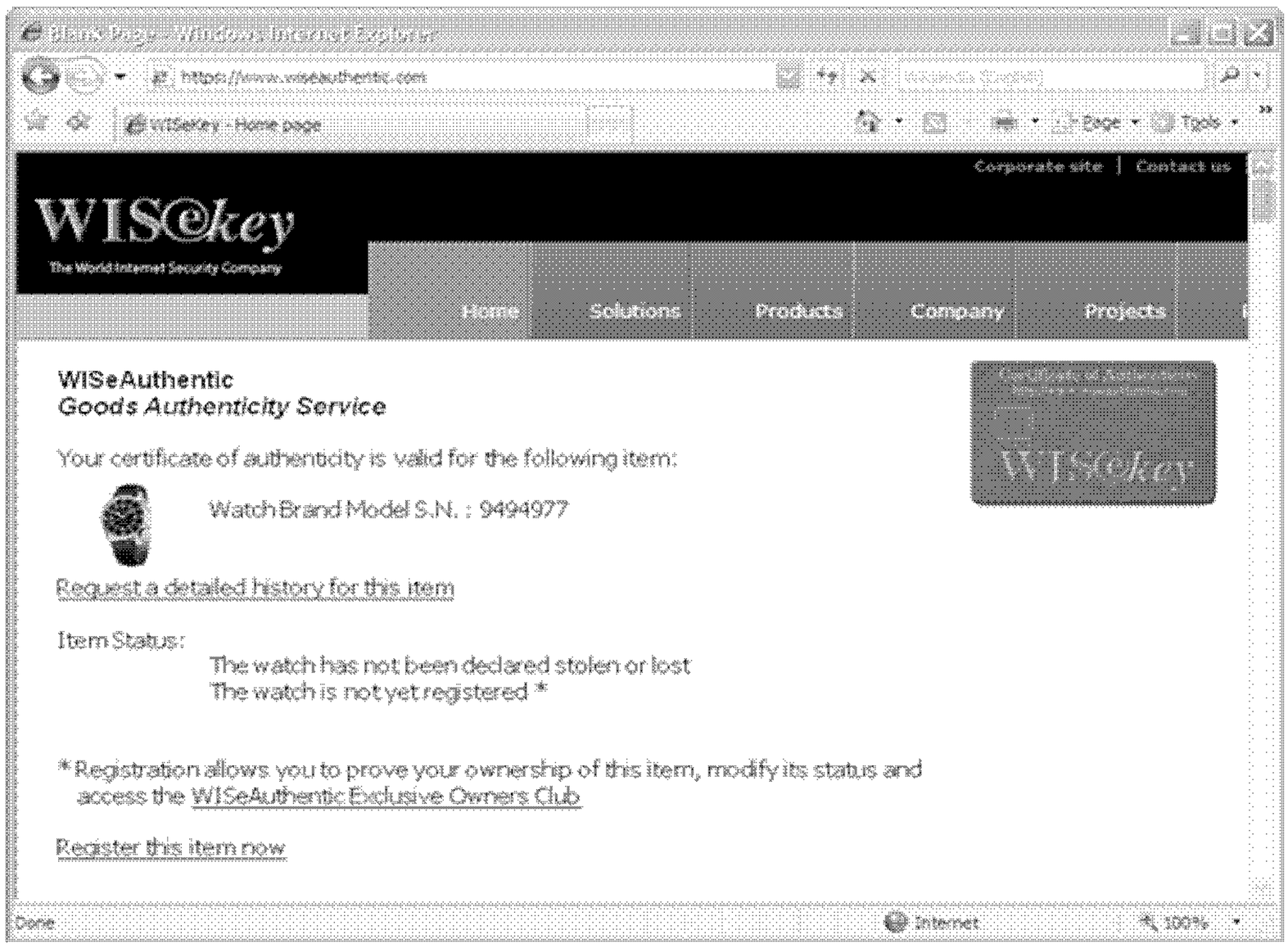
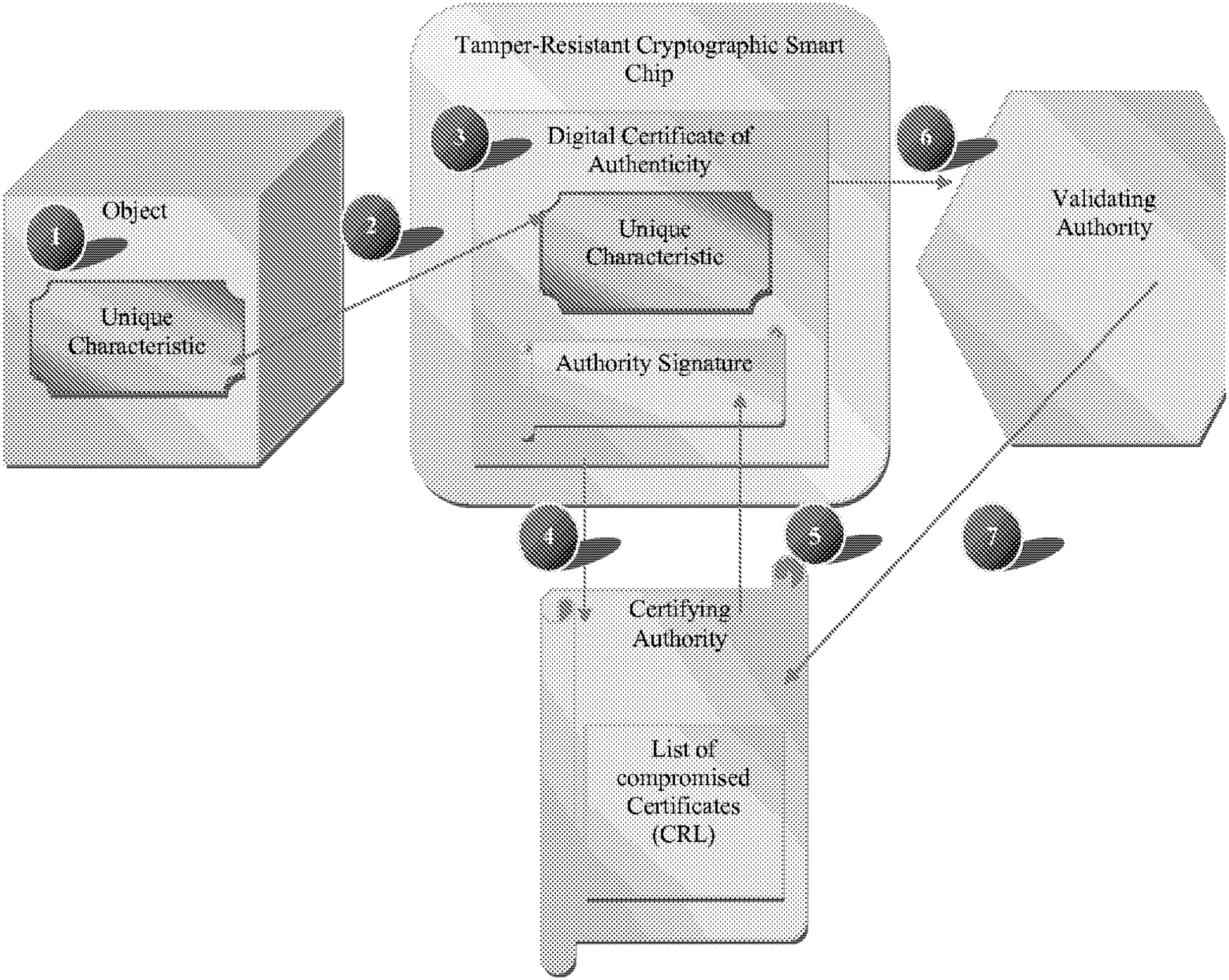


Figure 3b




Tamper-Resistant Cryptographic Smart Chip
Object
Unique Characteristic
Digital Certificate of Authenticity
Unique Characteristic
Authority Signature
Validating Authority
Certifying Authority
List of compromised Certificates (CRL)
1
2
3
4
5
6
7