(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102112993 A
(43)申请公布日 2011.06.29

(21)申请号 200880130551.2
(22)申请日 2008.07.28
(85)PCT申请进入国家阶段日
2011.01.28
(86)PCT申请的申请数据
PCT/IB2008/053022 2008.07.28
(87)PCT申请的公布数据
WO2010/013090 EN 2010.02.04
(71)申请人 维思电钥股份有限公司
地址 瑞士日内瓦
(72)发明人 J·达尔贝莱
J·C·克罗伊斯莫雷拉
K·布莱克曼 C·莫雷诺
(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 曲瑞
(51)Int.Cl.
G06F 21/24(2006.01)

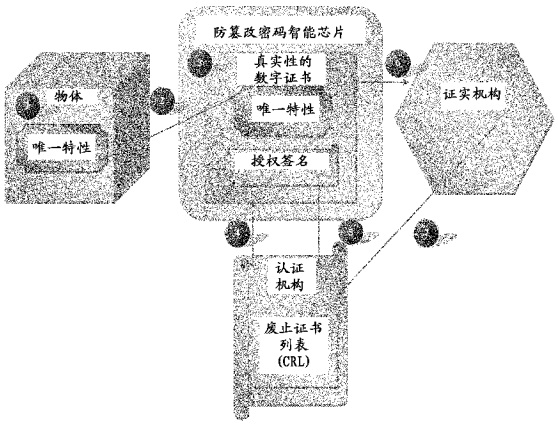
权利要求书 2 页 说明书 6 页 附图 2 页

(54)发明名称

用于贵重物品的数字验证的方法和装置

(57)摘要

本发明涉及一种用于物理物体的真实性的数字认证的方法、相应的计算机程序装置和存储装置以及用于具有一定价值的物理物体的真实性的数字认证的方法的使用。该方法包括下述步骤：颁发(1,2,3,4,5)包括真实性的数字证书的存储装置，该数字证书包括反映对于该物理物体唯一的至少一个特性的加密信息，在所需要的任何时间通过使用网络计算装置检查(6,7)真实性的数字证书的有效性，所述网络计算装置与所述存储装置和证实机构和/或认证机构协作以灵敏地实时输出所述真实性的数字证书的有效性的状态，在所需要的任何时间修改所述真实性的数字证书的有效性的状态。



CN 102112993 A

1. 一种用于物理物体的真实性的数字认证的方法，其特征在于，该方法包括下述步骤：

- 颁发 (1,2,3,4,5) 包括真实性的数字证书的存储装置，该真实性的数字证书包括反映对于该物理物体唯一的至少一个特性的以数字方式签署的信息，

- 在所需要的任何时间，通过使用网络计算装置检查 (6,7) 真实性的数字证书的有效性，所述网络计算装置与所述存储装置和证实机构和 / 或认证机构协作以灵敏地实时输出所述真实性的数字证书的有效性的状态，

- 在所需要的任何时间，修改所述真实性的数字证书的有效性的状态。

2. 如前一权利要求所述的方法，其特征在于，颁发所述存储装置包括下述步骤：

- 形成 (2,3) 对将要在所述存储装置上创建的所述真实性的数字证书的颁发的请求，该请求包括反映所述至少一个唯一特性的信息，

- 把所述请求发送 (4) 给认证机构以得到批准，

- 进行核查，如果核查通过，则由所述认证机构以数字方式签署所述请求，

- 把签署的请求发送 (5) 给存储装置，

- 通过与包括认证机构的批准的所述签署的请求的相互作用完成所述存储装置上真实性的数字证书的创建。

3. 如前面权利要求之一所述的方法，其特征在于，形成对将要在所述存储装置上创建的所述真实性的数字证书的颁发的请求包括：在所述存储装置上产生 (3) 包括公钥和私钥的不对称加密密钥对，关于该产生对于所述私钥是以不可输出的方式进行的。

4. 如前一权利要求所述的方法，其特征在于，通过使用公钥密码算法完成在所述存储装置上产生 (3) 不对称加密密钥对的步骤。

5. 如前面权利要求之一所述的方法，其特征在于，检查所述真实性的数字证书的有效性包括下述步骤：

- 经由网络计算装置把包括真实性的数字证书的存储装置连接 (6) 到证实机构和 / 或认证机构，

- 网络计算装置与存储装置和证实机构和 / 或认证机构相互作用 (7)，以允许由所述证实机构和 / 或认证机构访问真实性的数字证书和 / 或访问反映对于物理物体唯一的至少一个特性的信息，

- 经由网络计算装置灵敏地实时输出所述真实性的数字证书的有效性的状态。

6. 如前一权利要求所述的方法，其特征在于，经由网络计算装置把存储装置连接 (6) 到证实机构和 / 或认证机构以及网络计算装置与存储装置和证实机构和 / 或认证机构相互作用 (7) 包括：使用密码通信协议，特别地使用 TLS 或 SSL 协议，以及使用相互验证功能。

7. 如前面权利要求之一所述的方法，其特征在于，修改存储装置上的所述真实性的数字证书的有效性的状态包括下述步骤：

- 由认证机构接收关于物理物体的状态的信息，

- 在数据库中创建与物理物体的状态信息对应的条目，每当检查存储装置上的真实性的数字证书的有效性时该条目由证实机构读取。

8. 如前面权利要求之一所述的方法，其特征在于，该方法还包括下述步骤：

- 由认证机构接收补充信息，所述补充信息反映物理物体的一个或多个其它特性或与

该物体相关和 / 或与该物体的所有者和 / 或生产者相关的任何其它信息，

- 根据需要经由网络计算装置输出所述补充信息的任何部分。

9. 一种存储在计算机可读介质中的计算机程序装置，用于实现根据前面权利要求之一的方法。

10. 一种用于实现如前面权利要求 1 至 8 之一所述的方法的存储装置，其特征在于，它包括包含反映物理物体的至少一个特性的以数字方式签署的信息的真实性的数字证书，并且它与网络计算装置和 / 或证实机构和 / 或认证机构协作以允许后者输出所述真实性的数字证书的有效性的状态。

11. 如前一权利要求所述的存储装置，其特征在于，它包括密码智能芯片，所述密码智能芯片包括允许存储至少部分地以不可输出的方式在板上创建的或通过安全装置输入到该芯片的信息的计算机程序装置和 / 或电子装置。

12. 如前一权利要求所述的存储装置，其特征在于，所述密码智能芯片包括允许在板上创建密码信息的计算机程序装置。

13. 如前面权利要求 11 至 12 之一所述的存储装置，其特征在于，所述智能芯片集成到密码智能卡中。

14. 如前面权利要求 1 至 8 之一所述的用于具有一定价值的物理物体的真实性的数字认证的方法的使用。

15. 如前一权利要求所述的使用，其特征在于，所述具有一定价值的物体包括奢侈品，尤其是昂贵的表、珠宝。

用于贵重物品的数字验证的方法和装置

技术领域

[0001] 本发明涉及一种用于具有一定价值的物理物体的真实性的数字认证的方法、相应的计算机程序装置和存储装置以及对用于具有一定价值的物理物体的真实性的数字认证的方法的使用。

背景技术

[0002] 通常，在保护具有一定价值的物体（特别地，奢侈品）以使其免于假冒（当前，防止假冒已变得越来越难）的情况下应用本发明。现今，实际情况是，奢侈品（诸如，表或昂贵珠宝）的制造商颁发真实性的纸质证书，所述纸质证书对应于销售的奢侈产品并在获得奢侈产品时随该产品同时分发。这种纸质证书利用这样的事实，即具有一定价值的奢侈产品通常具有唯一特性（诸如，序列号），然而所述唯一特性作为整体的目标通常是可伪造的。因此，可伪造的贵重物体的生产者把它与再现唯一标识符的所述纸质证书关联。如果该纸质证书视为不可伪造，则通过请求提供该证书能够确定贵重物体的真实性。当然，所有这些依赖于这样的情况：纸质证书由授权实体生产并且不能被赝造。上述情况的典型例子是，例如，销售高质量表的表品牌以及由制造商或经销商编辑并再现各表的序列号的纸质证书。

[0003] 然而，以上过程固有地包括几个问题。首先，上述方案依赖于这样的情况：在技术上无法赝造纸质证书。然而，已知这种基于防伪纸、水印、RFID 或其它常规技术的证书不再提供不被伪造的保证，除非应用的过程的技术复杂性非常高，而这在另一方面使生产过程变复杂并且使生产过程非常昂贵。这导致了通常已知的贵重物品的制造商和假冒者之间的竞争，所述假冒者也不仅增加他们生产伪造物品的技术能力还增加复制这种证书的技术能力。因此，贵重物品的生产者需要寻找一种允许他们有效地生产随获得的物品同时分发的不可伪造的真实性的证书。

[0004] 其次，当前已知的用于认证给定物理物体的真实性的方案具有另外的缺点：即使给定贵重物品的所有者手中的证书不是赝造的，对于事先不知道这种情况的所有者而言核查该证书也是困难而棘手的。例如，如果具有这种证书的给定物体的所有者怀疑它的真实性或者如果他认为该证书的获得未经过正式经销商，则通常必须通过邮件把该证书发送给物品的制造商或另一相应实体进行核查。因此，这种物品的生产者需要寻找简化这个过程的技术方案。

[0005] 另外，使用例如防伪纸、水印或 RFID 的贵重物品的真实性的常规证书通常仅提到产品的主要性质以及所述唯一标识符（像产品的序列号）。一旦已颁发证书，则不再可以灵活地增加关于产品的另外的信息或者容易地修改与给定物品关联的证书的有效性的状态。因此，这种物品的生产者还需要寻找一种允许证书中包含的与销售的物品相关的数据的更灵活的使用和修改的技术方案。

发明内容

[0006] 本发明的目的在于克服上述困难并实现一种用于具有一定价值的物理物体的真

实性的验证的方法，该方法提供真实性的证书不能被赝造的最高可能水平的安全性。另外，与已知方案相比，真实性的证书的核查应该容易得多，并且与验证的物体和 / 或它的所有者相关的数据应该能够以更加灵活和容易的方式被包括在证书中。

[0007] 为此，本发明提出一种用于物理物体的真实性的数字认证的方法，其特征在于权利要求 1 中列举的特征并允许实现上述目的。

[0008] 特别地，根据本发明的用于真实性的数字认证的方法的特征在于，该方法包括下述步骤 :颁发包括真实性的数字证书的存储装置，该数字证书包括反映对于该物理物体唯一的至少一个特性的加密信息，在所需要的任何时间检查数字证书的有效性，还在所需要的任何时间修改所述证书的有效性的状态。由授权认证机构颁发并签署并且存储在例如密码芯片上的数字证书不可伪造的事实为上述技术问题提供了方案。此外，通过在现今的公共网络（像因特网）上使用安全通信可以在全世界容易地核查数字证书的有效性。另外，可以灵活地为数字证书提供与验证的物品相关的附加信息或者改变它的状态。

[0009] 本发明还涉及实现根据根据本发明的用于真实性的数字认证的方法的相应计算机程序装置。

[0010] 此外，本发明提出用于实现所述方法的存储装置，该存储装置的特征在于权利要求 10 中列举的特征，特别地，该存储装置保存所述真实性的数字证书并与计算网络装置和证实和 / 或认证机构协作以核查所述证书的有效性。

[0011] 特别地，本发明提出在验证具有很大价值的物理物体（例如，昂贵的表、珠宝或其它奢侈品）的情况下根据本发明的方法的使用。

[0012] 在从属权利要求中以及在下面参照附图更详细地公开本发明的描述中提到了本发明的其它特征和优点。

附图说明

[0013] 附图示例性地并且示意性地表示本发明的原理。

[0014] 图 1 示意性地表示在现有技术中以及在根据本发明的方案中都使用的真实性的认证的原理。

[0015] 图 2 是根据本发明的用于物理物体的真实性的数字认证的方法的步骤的示意性总体示图。

[0016] 图 3a 和 3b 分别显示在请求检查或者一旦已确认证书的有效性的阶段在检查数字证书的有效性的过程期间相应计算机程序的图形界面的例子。

具体实施方式

[0017] 在下面，将参照上述附图详细描述本发明。

[0018] 图 1 表示在基于防伪纸、水印或其它传统技术的真实性的常规证书中以及在本发明的情况下都使用的原理。在图 1 的左侧呈现的可伪造的物体（例如，表或其他奢侈产品）包括唯一特性，例如序列号。由授权实体编辑并视为不可伪造的真实性的证书再现这个唯一特性并且象征性地表示在图 1 的右侧。鉴于假冒者一达到复制这些证书所需的相应技术水平，传统证书的不可伪造性就不再有效，复制根据本发明的真实性的数字证书难得多，从下面的描述将会清楚这一点。

[0019] 图 2 示意性地表示在根据本发明的物理物体的真实性的数字认证的过程期间的不同步骤。当然，在物理物体（像奢侈产品）的生产之后必须首先为该物理物体提供唯一标识符（诸如，字母数字序列号），这个唯一标识符在图 2 中由附图标记附图标记 1 象征性地指示。该序列号可以例如雕刻在奢侈产品上或者奢侈产品可包括用于这种目的的任何其它唯一标识符。

[0020] 作为根据本发明的方法的第一步骤，必须创建与所述奢侈产品对应的真实性的数字证书。为此，颁发包括真实性的数字证书的存储装置，该数字证书包括至少反映上述唯一特性的以数字方式签署的信息。用于本发明的目的的存储装置通常由密码智能芯片构成，所述密码智能芯片包括允许在板上并且至少部分地以不可输出的方式创建密码信息的计算机程序装置。这种智能芯片通常集成于密码智能卡。术语“密码智能芯片”和“密码智能卡”将按照与术语“存储装置”同义的方式在下面的描述中广泛使用。这种密码智能芯片用于保存 (host) 根据本发明的真实性的数字证书，该数字证书随后可以由外部计算装置核查。

[0021] 因此，颁发根据本发明的数字证书包括提供这种密码智能芯片。该芯片随后在颁发数字证书期间插入到用作输入和输出装置的普通 PC 中的读取和处理装置（诸如，智能卡读取器）。然后，如图 2 中附图标记 2 所指示，制订 (formulate) 对奢侈产品的所述真实性的数字证书的颁发的请求。数字证书的请求文件通过包括反映所述至少一个唯一特性的加密信息再现对于奢侈产品唯一的至少一个特性。所述唯一特性（像雕刻的序列号）可以例如放置在证书的普通名称字段。可基于本领域技术人员已知的 X.509 证书颁发标准制订所述请求文件。

[0022] 为了颁发数字证书，本发明使用不对称加密，这种方法是根据当前知识用于这种目的的最佳方案。因此，制订对将要在所述存储装置上创建的真实性的数字证书的颁发的所述请求包括产生包括公钥和私钥的不对称加密密钥对（如图 2 中的附图标记 3 象征性所示）。所述不对称加密密钥对的产生在存储装置上在板上发生并且以私钥不可输出的方式发生。这涉及允许在板上并且至少部分地以不可输出的方式创建密码信息的密码智能芯片上的上述计算机程序装置，这种程序也称为“智能芯片中间件”或“驱动程序”。可替代地，不对称加密密钥对的产生不在板上执行而是由智能卡外部的安全装置执行并且将会在产生之后被保存在所述芯片上从而私钥不可输出并且当然地是唯一的。优选地，通过使用本领域技术人员也已知的公钥密码算法（诸如，Rivest-Shamir-Adleman(RSA) 密码算法或椭圆曲线密码术 (ECC)）完成在密码智能芯片上或通过所述安全装置产生不对称加密密钥对的操作。真实性的数字证书的私钥以安全和唯一的方式在密码智能芯片上或通过所述安全装置产生并且在任何情况下以不可输出的方式存储在密码智能芯片上，这为芯片提供了证书的理想的不可复制性，从而以非常有效的方式使得证书防篡改并且不可伪造。

[0023] 在已如上所述制订对数字证书的颁发的请求之后，该请求被发送给认证机构以得到批准，如图 2 中的附图标记 4 象征性所示。该认证机构必须由授权人员最终通过自动化过程控制和操作，并且可例如与将要关于真实性进行认证的奢侈产品的生产者相同或者可对应于由所述生产者指定的实体。当由认证机构接收到所述请求时，将针对几个参数（诸如，操作者权限）核查证书的完整性和 / 或所述请求的唯一性。如果核查步骤成功，则认证机构利用它自己的证书（认证机构证书）以数字方式签署数字证书的请求文件并把以数字

方式签署的请求文件发回到插入在读取和处理装置中的存储装置。这个步骤在图 2 中由附图标记 5 指示。当在密码智能芯片中接收到签署的请求时，上述中间件通过与包括认证机构的批准的签署的请求的相互作用完成真实性的数字证书的创建。这个过程的几个方面可根据 X.509 证书颁发的标准过程来完成，然而在技术上等同的替换方案变为可用或者将要变为可用的情况下这不是绝对必需的。

[0024] 一旦根据上述方法已在密码智能卡上颁发真实性的数字证书以及一旦已销售了奢侈产品及其相应的真实性卡，在所需要的任何时间和任何地点，通过使用网络计算装置可以由该奢侈产品的所有者检查数字证书的有效性并因此检查相应奢侈产品的真实性。为此，网络计算装置与所述存储装置和证实和 / 或认证机构协作以灵敏地实时输出所述真实性的数字证书的有效性的状态。在这种情况下，应该注意的是，证实机构可以与认证机构相同，但这不是必需的情况，因为前者也可以由一个或多个相应实体构成。

[0025] 实际上，为了检查真实性的数字证书的有效性，可以把包括真实性的数字证书的密码智能卡插入到任何读取和处理装置，即插入到装备了智能卡读取器并相应地构造的任何计算机。然后，能够针对也为此目的构造的网络服务器检查智能卡上的证书的有效性，该操作再次涉及智能芯片上的中间件。为此，包括真实性的数字证书的智能芯片经由网络计算装置连接到证实机构和 / 或认证机构，如图 2 中的附图标记 6 象征性所示。证实机构通常由构造为使用密码通信协议（诸如 TLS（传输层安全）或 SSL（安全套接层），优选 TLS）并包括握手功能的上述网络服务器构成以便在通信过程期间提供相互验证，提供足够功能的另外的保密通信装置也用于这个目的。上述技术术语对于本领域技术人员而言是已知的并且不需要在这里进行任何进一步的解释。

[0026] 证实机构检查证书的有效期限以及它是否已被撤销，使用例如通常保存在认证机构的证书撤销列表 (CRL) 或者在线证书状态协议 (OCSP) 针对认证机构检查证书是否已被撤销，如图 2 中的附图标记 7 象征性所示。这二者都是一种包括关于颁发的证书的信息的列表（特别地，在个体证书废止的情况下的相应条目）。因此，这个步骤包括网络计算装置与存储装置和证实和 / 或认证机构的相互作用以允许由所述证实和 / 或认证机构访问真实性的数字证书。实际上，通过本领域技术人员已知的证实机构和智能芯片之间的公钥交换以及通过利用上述 CRL 或 OCSP 的证书的交叉检查来检查证书的有效性。这个步骤通常包括核查本领域技术人员已知的认证机构的证书的有效性作为证书链验证。然后，经由网络计算装置灵敏地实时执行以证书的有效性的状态的形式的输出。该输出可例如包括这样的事实 :真实性的证书有效，即奢侈产品是真实的，如图 3b 中显示的实现上述方法的计算机程序装置的图形界面的例子所示。通常，为了方便由产品的所有者使用该方法，图形界面上的输出也会给出一些附加信息，例如产品的系列和 / 或型号的名称，当然也例如是序列号（为证书的目的而选择的相应的唯一特性）和关于生产者的信息。为了方便，这种信息或它的一部分可以顺便打印在智能卡的表面上。图 3a 表示关于允许证实真实性的数字证书的请求页的根据本发明的相应图形界面的例子，这一页应该就出现在图 3b 中显示的页之前。这表明 :针对提供可以容易地在任何时间以及几乎在任何地点质疑其有效性的不可伪造的真实性的证书的问题，本发明提供了一种方便的技术方案。

[0027] 根据本发明的奢侈品的真实性的数字认证的方法还包括 :在所需的任何时间修改所述数字证书的有效性的状态。例如，可能发生这样的情况 :奢侈产品和 / 或随奢侈产品一

起分发给该产品的所有者的密码智能卡失窃、丢失或需要修理或者经受需要数字证书的相应更新的任何其它修改。因此，通过允许由认证机构接收关于物理物体的状态的信息，现在提出的方法允许修改数字证书的状态。然后，例如以图 2 中示例性地表示的上述废止证书列表 (CRL) 的形式在数据库中创建与物理物体的状态信息对应的条目 (例如，该物体已失窃)。每当检查存储装置上的真实性的数字证书的有效性时，数据库中的条目通常由证实机构读取，最终也由认证机构读取。

[0028] 另外，根据本发明的方法还允许提供关于所讨论的奢侈产品的可能有趣的补充信息。除了上述例如产品失窃或丢失的信息之外，这种补充信息可例如包括物理物体的其它特性或任何其它与物体相关的信息或者与所有者或产品的生产者相关的信息。通过使用如上解释的网络计算装置，可以经由网络计算装置和相应的图形界面输出 (putout) 这种补充信息的任何部分。例如，可以以这种方法提供销售相关信息，该销售相关信息可以在线保持，例如旨在为产品提供数字保证。另外，如果由于智能卡仅与所讨论的产品相关的事实导致真实性的数字证书的以上核查原则上是匿名的，则可以由根据本发明的相应计算机程序装置提供用于允许产品的所有者的个人注册的设施。例如，这种认证的所有者将会随后通过使用这种计算机程序访问与例如他获得的产品或者已获得类似物品的其他人的所有者俱乐部相关的几个功能。此外，密码智能芯片可另外包括一致性的数字证书以便建立给定产品的制造过程与预设的一组规则的一致性，例如获得标签“瑞士制造”或任何其它类似标签。这种标签由相应控制实体颁发并且可以对提出的认证奢侈品的真实性的方法给予附加值，该方法可以容易地在包括真实性的数字证书的密码智能芯片上增加相应的一致性的数字证书。在这种情况下应该提及的是，根据本发明的方法也可以允许执行真实性的数字证书的证实的人经由网络计算装置检查已颁发所述证书的认证机构的技术和操作框架。特别地，这涉及证书策略 (CP) 和认证业务规则 (CPS)。

[0029] 在以上讨论了根据本发明的奢侈品的真实性的数字认证的方法之后，很清楚的是，本发明也涉及用于实现这种方法的计算机可读介质中存储的计算机程序装置。特别地，相应的计算机程序提供相应功能和图形界面以便实现授权颁发或检查真实性的数字证书的有效性的上述认证和证实机构。这种计算机程序装置可以由理解了本发明中的教导的本领域技术人员容易地实现。

[0030] 如上所述，本发明还涉及用于实现根据本发明的方法的相应存储装置 (相应的密码智能芯片)。这种芯片包括包含反映物理物体的至少一个特性的加密信息的真实性的数字证书，并与网络计算装置和证实和 / 或认证机构协作以允许后者输出数字证书的有效性的状态。这种用于本发明目的的密码智能芯片包括允许在板上并且至少部分地以不可输出的方式创建密码信息的中间件。

[0031] 最后，本发明还涉及所提出的用于真实性的数字认证的方法在保护具有一定价值的物理物体免于被假冒的领域中的使用。这种具有一定价值的物体的例子是任何类型的奢侈品，例如昂贵的表或珠宝。

[0032] 根据本发明的以上描述，它的优点很清楚。首先，由于私钥以不可输出的方式产生并存储在密码智能芯片中的事实，所以根据本发明的真实性的数字证书在防止对它的复制方面安全得多。因此，证书的不可伪造性不像这种证书的常规方案中那样依赖于技术复杂性，而是依赖于芯片里面的数据的不可输出性的所述原理，并且通过用于加密的数学算法

的复杂性以及密码智能芯片的相应电子系统得到进一步增强证书。因此，即使由看起来相同的假冒物品替换单个真实的产品，但根据本方法不能避免伪造的唯一标识符以及例如通过偷窃获得的有效证书，尽管如此，这提供了用于有效防止具有一定价值的产品的大规模工业假冒的技术方案，由于假冒者不能以工业方式复制数字证书自身的事实，所以这种情况证明应该采用上述过程。此外，可以在所需要的任何地点和任何时间执行产品的真实性的数字证书的证实。此外，可以根据需要修改有效性的证书的状态。也可以根据需要把另外的信息包括在证书（相应的智能芯片）中。这种真实性的数字证书不改变物品的现有制造过程，可由制造商以及由物品的任何授权销售者或经销商颁发，并且可以针对任何产品颁发，即使其生产日期为几年以前。

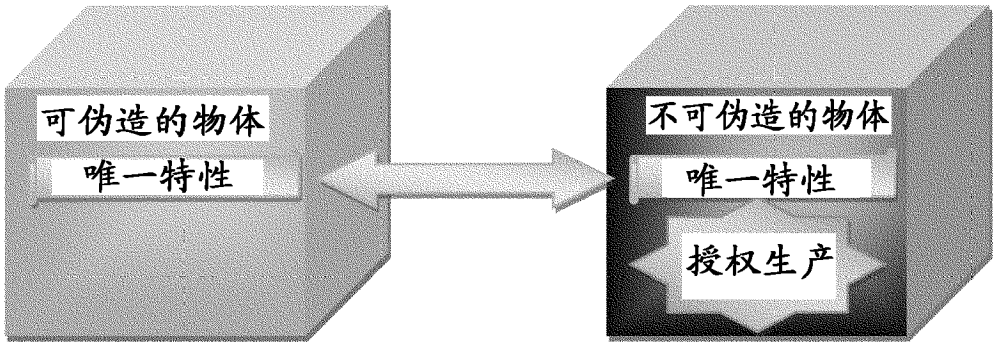

可伪造的物体
唯一特性
不可伪造的物体
唯一特性
授权生产

图 1

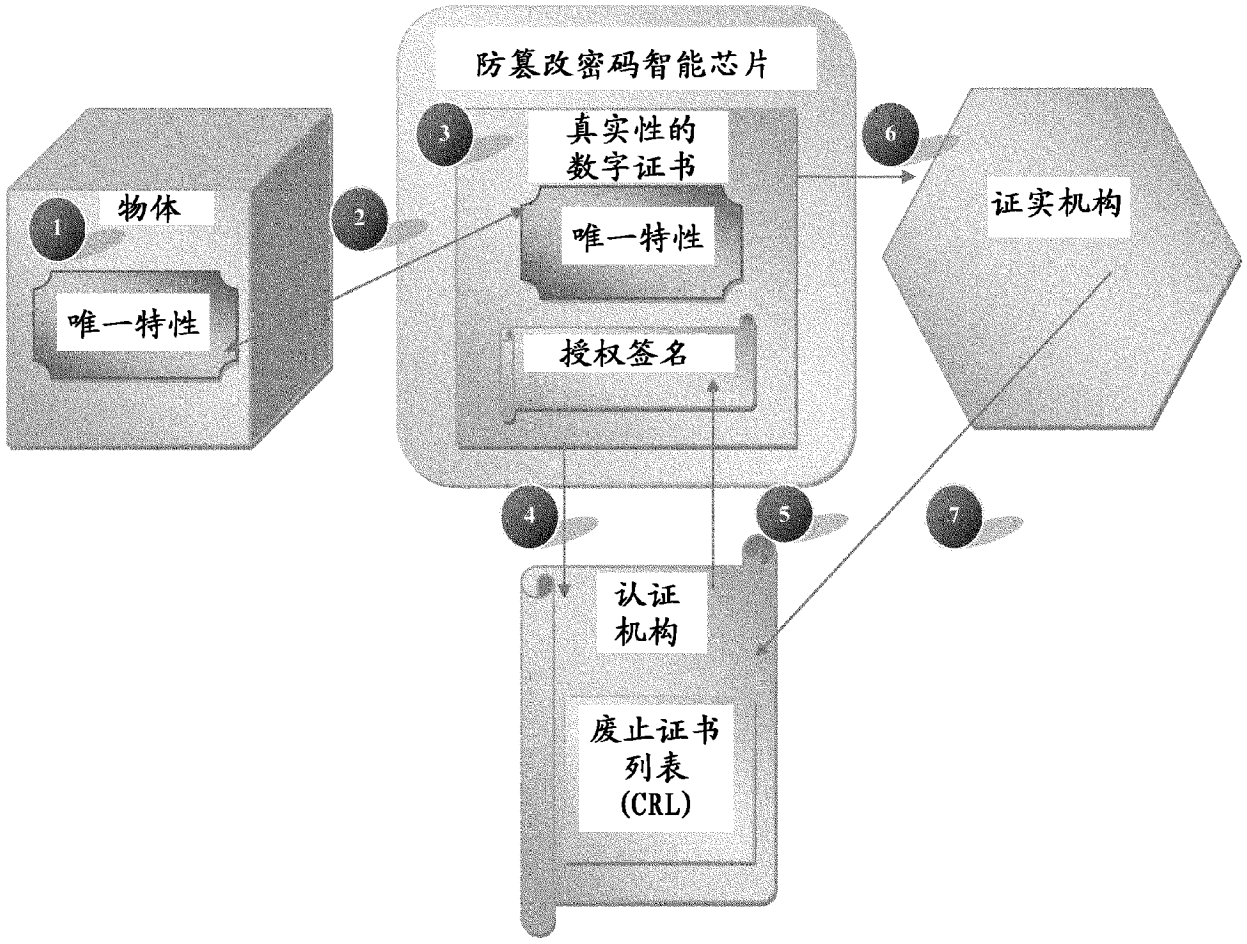

防篡改密码智能芯片
1
物体
唯一特性
2
3
真实性的
数字证书
唯一特性
授权签名
6
证实机构
4
5
7
认证
机构
废止证书
列表
(CRL)

图 2


Blank Page - Windows Internet Explorer
https://www.wiseauthentic.com
WISeKey - Home page
Corporate site | Contact us
WISeKey
The World Internet Security Company
Home
Solutions
Products
Company
Projects
WISeAuthentic
物品真实性服务
由WISeAuthentic的成员生产的任何真实表必须附有
其存储在智能卡上的真实性的数字证书
为了检查您的真实性的证书的有效性状态，请把您的
证书插入读取器并点击以下连接:
证实您的真实性的证书
Done
Internet
100%

图 3a


Blank Page - Windows Internet Explorer
https://www.wiseauthentic.com
WISeKey - Home page
Corporate site | Contact us
WISeKey
The World Internet Security Company
Home
Solutions
Products
Company
Projects
WISeAuthentic
物品真实性服务
您的真实性的证书对下列物品有效:
表品牌型号 S.N.:9494977
请求这项物品的详细历史
物品状态:
该表未被声明失窃或丢失
该表还未注册
*注册允许您证明您对这项物品的所有权，修改它的状态
并访问WISeAuthentic专有所有人俱乐部
现在注册这项物品
Done
Internet
100%

图 3b