(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 105378774 A
(43)申请公布日 2016.03.02

(21)申请号 201480027094.X
(22)申请日 2014.03.12
(30)优先权数据
61/778122 2013.03.12 US
61/835069 2013.06.14 US
61/878195 2013.09.16 US
61/914212 2013.12.10 US
61/918506 2013.12.19 US
61/932927 2014.01.29 US
(85)PCT国际申请进入国家阶段日
2015.11.12
(86)PCT国际申请的申请数据
PCT/US2014/025085 2014.03.12
(87)PCT国际申请的公布数据
WO2014/165284 EN 2014.10.09
(71)申请人 英特托拉斯技术公司
地址 美国加利福尼亚州
(72)发明人 D.P.马赫 P.沙瓦纳 Y.纳高 M.曼宁特
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 徐红燕 陈岚
(51)Int.Cl.
G06Q 20/40(2006.01)

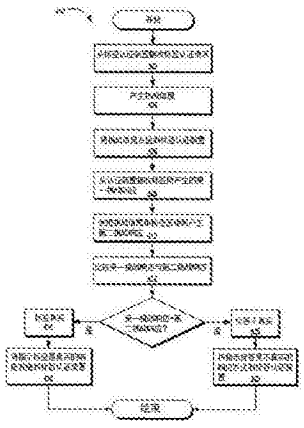
权利要求书1页 说明书32页 附图17页

(54)发明名称

安全交易系统和方法

(57)摘要

本发明描述结合各种交易而使用标签认证和存在验证技术的系统和方法。在某些实施例中，认证装置可通过确定安全标签是否存储由可信机构提供的秘密信息来验证所述安全标签的真实性。在一些实施例中，此认证过程可在不将所述秘密信息透露给所述认证装置的情况下执行，进而维持所述安全标签的完整性。在其它实施例中，使用了不安全标签和/或不包含秘密信息的标签。



CN 105378774 A

1. 一种由可信系统执行的方法，所述可信系统包括处理器和存储指令的非暂时性计算机可读存储介质，所述指令在被执行时使所述系统执行所述方法，所述方法包括：

在所述可信系统的接口处从认证装置接收由安全标签产生的第一挑战响应；

基于挑战信息和所述可信系统所存储的秘密信息而产生第二挑战响应；

比较所述第一挑战响应与所述第二挑战响应；

确定所述第一挑战响应与所述第二挑战响应匹配；以及

经由所述可信系统的所述接口而将认证所述安全标签的响应发送到所述认证装置。

2. 根据权利要求 1 所述的方法，其中所述方法进一步包括：

产生所述挑战信息；以及

经由所述可信系统的所述接口而将所述挑战信息发送到所述认证装置。

3. 根据权利要求 1 所述的方法，其中所述方法进一步包括：

在所述可信系统的接口处从所述认证装置接收所述挑战信息。

4. 根据权利要求 1 所述的方法，其中所述挑战信息包括随机产生的值。

5. 根据权利要求 1 所述的方法，其中所述挑战信息包括密码随机数。

6. 根据权利要求 1 所述的方法，其中所述安全标签包括安全近场通信（“NFC”）标签。

7. 根据权利要求 1 所述的方法，其中产生所述第二挑战响应包括：

基于所述挑战信息和所述可信系统所存储的所述秘密信息而计算密码函数的结果。

8. 根据权利要求 7 所述的方法，其中所述密码函数包括使用所述可信系统所存储的所述秘密信息来对所述挑战信息进行数字签名。

9. 根据权利要求 7 所述的方法，其中所述密码函数包括基于所述可信系统所存储的所述秘密信息来对所述挑战信息进行散列运算。

10. 根据权利要求 1 所述的方法，其中所述秘密信息包括秘密密钥。

11. 根据权利要求 1 所述的方法，其中产生所述第二挑战响应进一步包括：

使用所述第一挑战响应中所包含的与所述安全标签相关联的识别信息来检索所述可信系统所存储的所述秘密信息，

其中所述可信系统所存储的所述秘密信息与所述安全标签相关联。

12. 根据权利要求 1 所述的方法，其中认证所述安全标签的所述响应进一步包括与关联于所述安全标签的产品相关的信息。

13. 根据权利要求 12 所述的方法，其中由所述可信系统基于所述第一挑战响应中所包含的与所述安全标签相关联的识别信息来检索与所述产品相关的所述信息。

安全交易系统和方法

相关申请案

[0001] 本申请案根据35U.S.C.§119(e)主张2013年3月12日申请且标题为“物体识别系统和方法(OBJECT IDENTIFICATION SYSTEMS AND METHODS)”的第61/778,122号美国临时专利申请案、2013年6月14日申请且标题为“安全交易系统和方法(SECURE TRANSACTION SYSTEMS AND METHODS)”的第61/835,069号美国临时专利申请案、2013年9月16日申请且标题为“安全交易系统和方法(SECURE TRANSACTION SYSTEMS AND METHODS)”的第61/878,195号美国临时专利申请案、2013年12月10日申请且标题为“安全交易系统和方法(SECURE TRANSACTION SYSTEMS AND METHODS)”的第61/914,212号美国临时专利申请案、2013年12月19日申请且标题为“安全交易系统和方法(SECURE TRANSACTION SYSTEMS AND METHODS)”的第61/918,506号美国临时专利申请案以及2014年1月29日申请且标题为“文档执行系统和方法(DOCUMENT EXECUTION SYSTEMS AND METHODS)”的第61/932,927号美国临时专利申请案的优先权权益,所有这些美国临时专利申请案的全部内容以引用方式并入本文中。

版权授权

[0002] 本专利文件的公开内容的部分可含有受到版权保护的内容。版权所有人不反对任何人对专利文件或专利公开内容进行传真复制,如同其出现在美国专利商标局的专利文件或记录中一样,但另外,无论如何均保留全部版权权利。

技术领域

[0003] 本发明总的来说涉及用于进行各种安全交易的系统和方法。更具体来说,但不排他地,本发明涉及结合各种交易而使用电子标签和/或存在验证的系统和方法。

背景技术

[0004] 电子标签可用于各种有益应用中,包含产品库存控制、储值卡和/或回馈卡系统、个人识别系统等。然而,使用常规电子标签的系统可能不特别稳健。举例来说,在利用常规电子标签的储值卡和/或回馈卡系统中,卡余额可存储在标签中。如果这种卡失窃,用户可能至少暂时感到不便且可能几乎没有恢复与卡相关联的储值的追索权。利用电子标签的常规系统还可需要电子标签读取器和/或相关联的通信信道的显著安全性强化。与常规标签读取器中所包含的安全硬件相关联的成本可阻碍这些系统的广泛采用。此外,利用电子标签的现有系统在它们安全地证明标签的真实性和/或有效性和/或确定标签在适当时间处于特定场所的能力方面受到限制。在本文中描述了修正这些问题中的一些或全部的系统和方法。举例来说,但不加限制,在一些现有的基于电子标签的系统中,除非使用相对复杂和/或昂贵的技术,否则电子标签相对于容易复制。在本文所公开的系统和方法的一些实施例中,服务器侧方法用于端对端系统中,所述方法减轻或减少对标签和/或标签读取器中的安全性的需要。

发明内容

[0005] 本文所公开的系统和方法有助于电子标签和/或存在验证。在一些实施例中，使用虚拟标签而不是物理标签，所述虚拟标签可驻留在例如移动电话和平板计算机等消费型装置中。除非另外从上下文清楚，否则本文中对安全电子标签、电子标签、标签和/或类似物的参考打算涵盖任何适当的实施方案（例如，安全芯片、虚拟标签或存储在用户的装置中的值等）。在某些实施例中，所公开的系统和方法可使用安全电子标签，所述安全电子标签被配置成存储由可信机构提供的秘密信息。标签对这种秘密信息的了解可由可信机构验证以认证标签在标签认证装置附近的存在。所公开的系统和方法的实施例可结合各种安全交易来使用，这些安全交易需要电子标签在特定时间在物理上存在于标签认证装置附近的可信验证。

[0006] 为了认证安全电子标签，标签认证装置可经由任何适当通信方法来检测标签在认证装置附近的存在。在检测到标签的存在之后，认证装置可与关联于标签的可信机构通信，且请求可信机构对标签的认证。作为响应，可信机构可产生挑战信息且将挑战信息传达给认证装置。在某些实施例中，挑战信息可包括随机产生的值，但其它类型的挑战信息也可结合所公开的系统和方法来使用。认证装置可将挑战信息传达给电子标签，且请求标签基于所述挑战信息而产生响应。在某些实施例中，所请求的响应可包括由电子标签使用挑战信息和秘密信息（例如，数字签名、散列和/或使用秘密信息的挑战信息的经加密的版本等）而执行的计算的结果。

[0007] 标签可将响应传达给认证装置，而认证装置又可将响应转发给可信机构。在接收到响应之后，可信机构可基于可信机构存储和/或以其它方式拥有的与标签相关联的挑战信息和秘密信息而产生其自身的响应。如果由标签产生的响应与由可信机构产生的响应匹配，那么对标签所存储的秘密信息的知晓可由可信机构验证，且标签可被认证。如果响应不匹配，那么标签可不被可信机构验证。标签是否已由可信机构认证的指示可被传达给认证装置和/或一个或更多个服务提供商，以结合提供与标签相关联的服务来使用。

[0008] 本文所公开的认证系统和方法的某些实施例可实现标签与在标签、读取器和/或可信机构或其它可信服务之间的背景交互两者的认证。作为实例，在一些实施例中，除挑战响应之外，用于产生挑战响应的挑战信息可由标签传达给认证装置和/或可信机构。虽然挑战响应可指示标签对某秘密信息的拥有，然而，如果标签不能也将相关联的挑战信息传达给认证装置和/或可信机构，那么根据本文所公开的实施例的标签、认证装置和/或可信机构之间的适当交互可不被认证。举例来说，在这情形下，可怀疑，标签响应是在除根据本文所公开的实施例的指定标签、认证装置和/或可信机构交互之外的某一其它背景中生成和/或以其它方式产生。

[0009] 本文所公开的系统和方法的实施例可允许由标签和/或可信机构存储的秘密信息不透露给认证装置和/或相关服务提供商系统，和/或直接从标签或可信机构传达。在某些实施例中，这可降低认证装置和/或相关联的硬件、软件和/或通信信道的安全复杂性。本文所公开的系统和方法可结合利用安全电子标签的各种安全交易来使用，所述安全交易包含（但不限于）产品认证、库存和/或所有权服务、产品信息分发服务、储值卡和/或忠诚卡系统（例如，私有货币系统）、售票系统、电子支付系统、用户认证服务、文档签名服务、电子商务服务（例如，拍卖服务）和/或类似物。在一些实施例中，公开可用于建构安全地

维持标签与物理项目之间的一对一对应的服务的系统和方法，从而在到最终消费者的整个分销链中实现安全的项目跟踪和询问追查，进而帮助防止盗窃和诈骗。

附图说明

[0010] 结合附图，通过参考下文详细描述，将容易理解发明性工作主体，其中：

[0011] 图 1 说明根据本发明的实施例的电子标签的提供。

[0012] 图 2 说明根据本发明的实施例的电子标签的认证。

[0013] 图 3 说明根据本发明的实施例的由认证装置认证电子标签的示范性方法的流程图。

[0014] 图 4 说明根据本发明的实施例的由可信机构认证电子标签的示范性方法的流程图。

[0015] 图 5 说明根据本发明的实施例的包含安全电子标签的系列化产品的证实。

[0016] 图 6 说明根据本发明的实施例的与包含电子标签的产品相关的信息的分发。

[0017] 图 7A 说明根据本发明的实施例的包含电子标签的忠诚卡的提供。

[0018] 图 7B 说明根据本发明的实施例的忠诚卡认证过程。

[0019] 图 7C 说明根据本发明的实施例的忠诚卡兑换过程。

[0020] 图 8 说明根据本发明的实施例的储值卡认证和交易过程。

[0021] 图 9 说明根据本发明的实施例的交通卡的认证。

[0022] 图 10 说明根据本发明的实施例的可减轻重放攻击的安全标签认证过程。

[0023] 图 11 说明根据本发明的实施例的结合电子商务服务的产品证实。

[0024] 图 12 说明根据本发明的实施例的结合电子商务服务的另一产品证实过程。

[0025] 图 13 说明根据本发明的实施例的结合评论服务的存在证实。

[0026] 图 14 说明根据本发明的实施例的结合文档签名服务的用户的认证。

[0027] 图 15 说明根据本发明的实施例的结合文档签名服务的用户认证过程。

[0028] 图 16 说明根据本发明的实施例的基于装置的标签的初始化过程。

[0029] 图 17 说明根据本发明的实施例的基于装置的标签的认证过程。

[0030] 图 18 说明可用于实施根据本发明的系统和方法的某些实施例的系统。

具体实施方式

[0031] 下文提供根据本发明的实施例的系统和方法的详细描述。虽然描述了若干实施例，但应理解，本发明不限于任何一个实施例，而是实际上涵盖许多替代物、修改和等同物。此外，虽然在下文描述中阐述了许多具体细节以便全面理解本文所公开的实施例，但可在不存在这些细节中的一些或全部的情况下实践一些实施例。此外，为了清楚起见，未详细描述相关技术中已知的某些技术内容，以便避免不必要地混淆本发明。

[0032] 本发明的一些实施例可通过参照附图来理解，其中类似部分可由类似数字表示。如本文中附图大体上描述和说明，所公开的实施例的组件可按广泛各种不同配置来布置和设计。因此，某些说明性实施例的下文详细描述不希望限制所主张的本发明的范围，而是仅代表本发明的可能实施例。此外，除非另有规定，否则本文所公开的任何方法的步骤未必需要以任何具体次序或甚至依序执行，也不需要所述步骤仅执行一次。

[0033] 本文所公开的实施例实现电子标签的存在的安全验证。此验证可结合各种安全交易来使用。举例来说，系列化产品可与实施本文所公开的实施例的标签相关联。与标签认证装置通信的可信机构可验证标签的真实性，进而验证相关联的系列化产品的真实性。类似地，本文所公开的实施例可用于结合卡交易来验证储值卡（例如，私有货币卡，例如，出入通行卡、交通通行卡和/或类似物）或包含标签的其它类似装置的真实性和/或状态。所公开的实施例的这些实施方案可尤其减少未被授权的人对假冒产品和/或储值卡的生产和/或分销。

[0034] 所公开的实施例可允许结合安全标签认证而使用相对低成本的标签认证装置，例如，移动智能电话和/或平板计算装置。因为一些实施例允许结合标签认证而使用的秘密信息不透露给认证装置，所以可降低认证装置的硬件/软件安全性要求。通过降低标签认证装置的成本和/或复杂性，所公开的系统和方法可增加结合各种服务的安全标签和/或存在认证的采用。此外，所公开的实施例可允许各种服务提供商使用共同的可信机构来用于安全标签认证，进而有助于结合各种服务的标签授权和/或存在验证的较容易的集成。

[0035] 在某些实施例中，本文所述的系统和方法可（例如）结合以下各者来使用：数字版权管理（“DRM”）技术，例如在2006年10月18日申请且作为第2007/0180519 A1号美国公开案（“‘693申请案”）而公开的共同转让的、共同待决的第11/583,693号美国专利申请案“数字版权管理引擎系统和方法(Digital Rights Management Engine Systems and Methods)”中描述的数字版权管理（“DRM”）技术；服务编排和DRM技术，例如在共同转让的第8,234,387号美国专利（“‘387专利”）“用于对等服务编排的互操作系统和方法(Interoperable Systems and Methods for Peer-to-Peer Service Orchestration)”中描述的服务编排和DRM技术；数据收集和分析技术，例如在共同转让的、共同待决的第13/914,538号美国专利申请案（“‘538申请案”）中描述的数据收集和分析技术；信息定向技术，例如在共同转让的、共同待决的第13/946,750号美国专利申请案（“‘750申请案”）中描述的信息定向技术；和/或内容递送技术，例如在共同转让的、共同待决的第12/785,406号美国专利申请案（“‘406申请案”）中描述的内容递送技术（‘693申请案、‘387专利、‘538申请案、‘750申请案和‘406申请案的全部内容以引用方式并入本文中）；且本文所述的系统和方法还可用于其它背景中。

[0036] 安全标签提供

[0037] 图1说明根据本发明的实施例的安全电子标签100的提供。安全电子标签100可包括任何适当的电子硬件和/或软件，所述电子硬件和/或软件被配置成安全地存储所提供的信息104(例如，秘密信息）且响应于来自标签认证装置的询问基于所述信息而产生一个或更多个响应(例如，带签名的值、散列值、经加密的值和/或其它计算、推导或变换等)。除了存储信息104之外，安全标签100可被配置成存储结合本文所公开的实施例而使用的各种其它信息。安全电子标签100可被配置成使用任何适当的有线和/或无线通信协议而与标签认证装置和/或其它相关联的系统（例如，在标签提供过程期间的可信机构102)通信。虽然，为了易于解释，在本文中通常将参考安全标签，但应了解，在一些实施例中，与标签固有的安全性能力相反，标签安全性可从服务器的安全性能力得到。因此，标签可由于以下事实而被认为是安全的：标签是实现端对端系统的安全性的服务的可识别的部分。除非另外从上下文清楚，否则本文中对安全标签的参考打算至少涵盖这两种情形（例如，利用

强化/安全标签的系统和/或利用在系统所参与的服务的背景中从与远程服务器的交互得到安全性的标签的系统)。

[0038] 在某些实施例中,安全标签100可包括近场通信("NFC")标签、射频识别("RFID")标签、通用串行总线("USB")令牌、存储安全信息的具备Bluetooth®功能("BLE")的装置等。在其它实施例中,安全标签100可经由相关联的装置中所包含的硬件和/或软件来实施。举例来说,安全标签100可使用在装置(例如,智能电话)上执行的安全软件应用程序(或"app")来实施,和/或可包含在装置的安全硬件(例如,智能电话中所包含的安全硬件)中。应了解,各种其它类型的标签可结合本文所公开的标签认证和/或存在验证过程来使用,且任何类型的电子标签可结合所公开的实施例来使用。

[0039] 在某些实施例中,可信机构102可向标签100提供秘密信息104。秘密信息104可包括可结合本文所公开的实施例而使用的任何适当信息和/或值。在某些实施例中,秘密信息104可包括电子密钥、数字签名、用于计算散列值的信息、可信证书和/或类似物。在一些实施例中,由可信机构102提供的秘密信息104可为特定标签100特有的。在其它实施例中,标签不需要被提供秘密信息104,而是可(例如)存储经认证的信息、且用于认证的秘密可(例如)存储在服务器(例如,与可信机构102相关联的服务器)上。

[0040] 当由可信机构102提供秘密信息104时,标签100可持久地存储秘密信息104以结合所公开的标签认证和/或存在验证过程来使用。在其它实施例中,可信机构102和/或一个或更多个第三方(例如,第三方服务提供商)可提供其它信息以由标签100存储。举例来说,与标签100相关联的各种元数据和/或交易信息(例如,标签识别信息、相关联的产品和/或装置元数据信息、服务提供商信息和/或类似物)可被提供给安全标签100且由安全标签100存储以结合所公开的实施例来使用。此元数据和/或交易信息可取决于与所述信息和/或标签100相关联的安全性要求和/或偏好而由标签100安全地和/或不安全地存储。在其它实施例中,标签100可被提供系列化识别符,所述系列化识别符与将被跟踪和/或以其它方式询问追查的一组项目一对一对应。识别符自身可为与个别系列化项目一对一相关联的随机选择的值,进而使诈骗者难以预测这些值。

[0041] 安全标签认证

[0042] 图2说明根据本发明的实施例的电子标签100的认证。在标签100由可信机构102提供秘密和/或经认证的信息104之后,标签认证装置200可用于验证标签100的真实性。即,标签认证装置200可用于确定标签100是由可信机构102提供的真实标签和/或标签100在物理上位于认证装置200附近和/或在特定时间存在。如下文更详细地论述,此信息可结合各种安全交易中的任一者而用作标签100、标签认证装置200和/或相关联的项目(例如,产品、储值卡和/或忠诚卡、识别卡或项目等)的相对于彼此的存在的证据或接近。

[0043] 标签认证装置200、可信机构102和/或一个或更多个其它服务提供商(未示出)可包括被配置成实施本文所公开的系统和方法的实施例的任何适当计算系统或系统的组合。在某些实施例中,标签认证装置200、可信机构102和/或其它服务提供商可包括被配置成执行存储在相关联的非暂时性计算机可读存储介质上的指令的至少一个处理器系统。如下文更详细地论述,标签认证装置200、可信机构102和/或其它服务提供商可进一步包括被配置成执行敏感操作(例如,可信证书和/或密钥管理、安全策略管理和/或本文所

公开的系统和方法的其它方面）的安全处理单元（“SPU”）。标签认证装置200、可信机构102和/或其它服务提供商进一步包括可进一步包括被配置成经由一个或更多个相关联的网络连接（例如，网络202）来实现装置和/或系统102、200之间的信息的电子通信的软件和/或硬件。

[0044] 标签认证装置200可包括计算装置，所述计算装置执行被配置成实施本文所公开的系统和方法的实施例的一个或更多个应用程序。在某些实施例中，标签认证装置200可包括可结合所公开的系统和方法而使用的膝上型计算机系统、桌上型计算机系统、智能电话、平板计算机、标签认证终端系统和/或任何其它计算系统和/或装置。在某些实施例中，标签认证装置200可包括被配置成尤其确定安全标签100是由可信机构102提供的真实标签且安全标签100在物理上位于认证装置200附近和/或在特定时间存在的软件和/或硬件。在一些实施例中，此功能性可使用在与可信机构102和/或一个或更多个服务提供商相关联的标签认证装置200上执行的一个或更多个应用程序（例如，标签认证应用程序204）来实施。

[0045] 某些所公开的实施例可允许相对低成本的通用标签认证装置200结合安全标签认证和/或存在验证来使用。因为标签认证装置200可不透露给结合所公开的系统和方法而使用的信息104，所以在某些实施例中，认证装置200可不需要包含对于维持与此信息104相关联的任何安全性所需要的某些安全软件和/或硬件。举例来说，在某些实施例中，执行标签认证应用程序204（例如，由可信机构102和/或另一服务提供商提供的认证应用程序）的通用智能电话和/或平板计算装置可用于实施所公开的实施例的某些方面。在其它实施例中，标签认证装置200可包含结合所公开的系统和方法而使用的安全软件和/或硬件。

[0046] 标签认证装置200可经由包括任何适当数量的网络和/或网络连接的网络202而与可信机构102和/或其它服务提供商通信。网络连接可包括各种网络通信装置和/或信道，且可使用促进所连接的装置与系统之间的通信的任何适当的通信协议和/或标准。举例来说，在一些实施例中，网络可包括利用一种或更多种电子通信技术和/或标准（例如，以太网和/或类似物）的因特网、局域网、虚拟专用网和/或任何其它通信网络。在一些实施例中，网络连接可包括例如个人通信系统（“PCS”）等无线载波系统和/或并有任何适当的通信标准和/或协议的任何其它适当的通信系统。在其它实施例中，网络连接可包括模拟移动通信网络和/或数字移动通信网络，其利用（例如）码分多址（“CDMA”）、全球移动通信系统（“GSM”）、频分多址（“FDMA”）和/或时分多址（“TDMA”）标准。在某些实施例中，网络连接可并有一个或更多个卫星通信链路。在又其它实施例中，网络连接可使用IEEE 802.11标准、Bluetooth®、超宽带（“UWB”）、Zigbee®和或任何其它适当的通信协议。

[0047] 标签认证装置200可被配置成经由任何适当类型的有线和/或无线通信协议而与安全标签100通信。在一些实施例中，标签认证装置200可使用NFC、RFID、TransferJet、Zigbee®、Bluetooth®、IEEE 802.11标准和/或包含本文所公开的通信协议中的任一者的其它适当无线通信协议而与安全标签100通信。在某些实施例中，标签认证装置200可将包含挑战信息208的一个或更多个询问传达给安全标签100和/或从安全标签100接

收一个或更多个响应 210 和 / 或其它信息。

[0048] 标签认证装置 200 可执行结合根据本文所公开的实施例的标签认证和 / 或存在验证过程而使用的标签认证应用程序 204。在某些实施例中，标签认证应用程序 204 可由可信机构 102 提供给标签认证装置 200 以执行标签认证和 / 或存在验证过程。在其它实施例中，标签认证应用程序 204 可由一个或更多个第三方（例如，包含利用本文所公开的标签认证和 / 或存在验证过程来提供服务的服务提供商）提供给标签认证装置 200。

[0049] 在某些实施例中，标签认证应用程序 204 可使用标签认证装置 200 来执行轮询过程，以经由任何适当的通信方法（例如，NFC、RFID 通信等）而检测位于附近的安全标签 100。然而，应了解，任何适当的标签检测过程可结合所公开的实施例来使用（例如，标签可将警告发送到标签认证装置等）。当标签认证应用程序 204 检测到位于附近的标签 100 时，标签认证应用程序 204 可产生请求标签 100 的认证的标签认证请求 206，且将标签认证请求 206 传达给可信机构 102。

[0050] 在一些实施例中，安全标签 100 可由标签认证装置 200 以各种其它方式检测，包含使用不涉及由标签认证应用程序 204 和 / 或认证装置 200 执行的轮询过程的方法。在一些实施例中，标签认证装置 200 可传输（例如，周期性地传输）当由位于附近的标签 100 接收时可使标签 100 产生响应的能量脉冲串和 / 或其它电磁信号（例如，无线电信号等）。或者，标签认证装置 200 可发射低能量电磁场。当标签 100 落入由标签认证装置 200 发射的场范围内时，所述场可按可由认证装置 200 检测到的某一方式改变，进而允许认证装置 200 识别位于附近的标签 100。

[0051] 在其它实施例中，标签 100 可主动将指示其存在的信号发射到位于附近的标签认证装置 200。举例来说，基于 NFC 的标签和 / 或使用智能电话应用程序而以电子方式实施的标签可发射指示其在标签认证装置 200 附近的存在的信号和 / 或信标。应了解，可使用各种其它适当标签检测过程，且可由标签 100 和 / 或认证装置 200 结合本文所公开的实施例实施任何适当类型的标签检测过程。举例来说，虽然某些实施例和 / 或实例在本文中被描述为使用轮询过程进行标签检测，但应了解，任何适当的标签检测过程（包含（不限于）本文所公开的任何标签检测过程）可结合所公开的实施例和 / 或实例来使用。

[0052] 在接收到标签认证请求 206 之后，可信机构 102 可使用在可信机构 102 上执行的挑战产生器 212 而产生挑战信息 208。在某些实施例中，挑战信息 208 可包括随机和 / 或伪随机地产生的值，例如，密码随机数，但其它类型的挑战信息也可结合所公开的系统和方法来使用。可信机构 102 可将所产生的挑战信息 208 传达给标签认证装置 200，而标签认证装置 200 又可将挑战信息 208 作为挑战询问的一部分而传达给标签 100。

[0053] 挑战询问可请求标签 100 至少部分基于挑战信息 208 而传回响应。在某些实施例中，所请求的响应可包括由标签 100 基于挑战信息 208 和标签 100 所存储的秘密信息 104 而执行的计算的结果。举例来说，所述计算可包括至少部分使用秘密信息 104 而计算挑战信息 208 中所包含的密码随机数的带数字签名的值、经加密的值、MAC 值和 / 或散列值。在某些实施例中，所述计算可传回单独基于挑战信息 208 而不可用于识别秘密信息 104 和 / 或可另外使结合所述计算而使用的秘密信息 104 模糊的结果。

[0054] 标签 100 可将响应于挑战询问而产生的挑战响应 210 传达给认证装置 200。在某些实施例中，挑战响应 210 可包括由标签 100 基于挑战信息 208 和秘密信息 104 而执行的

计算的结果。认证装置 200 可接着将挑战响应 210 转发给可信机构 102。在接收到挑战响应 210 之后，可信机构 102 可使用在可信机构 102 上执行的标签认证模块 214 而执行标签认证过程。作为标签认证过程的一部分，标签认证模块 214 可至少部分基于挑战信息 208 和可信机构 102 所存储的秘密信息而产生响应。举例来说，标签认证模块 214 可计算挑战信息 208 中所包含的密码随机数的带数字签名的值、经加密的值、MAC 值、散列值和 / 或其它推导或变换。在某些实施例中，由标签认证模块 214 执行的计算可与由标签 100 响应于挑战询问而执行的计算相同或类似。

[0055] 在产生响应之后，标签认证模块 214 可比较所产生的响应与由安全标签 100 产生的挑战响应 210。如果由标签认证模块 214 产生的响应与由安全标签 100 产生的挑战响应 210 匹配，那么标签认证模块 214 可验证安全标签 100 与可信机构 102 两者拥有相同的秘密信息 104，且因此安全标签 100 是真实安全标签 100。然而，如果响应不匹配，那么标签认证模块 214 可不验证安全标签 100 所拥有的秘密信息 104 的真实性和 / 或专有权。因此，在此情形下，标签认证模块 214 可确定安全标签 00 不真实。以这种方式，可确定安全标签 100 已由可信机构 102 提供秘密信息 104 且因此是真实的，或未被提供此信息且因此是不真实的。在其它实施例中，不对称密码技术可用于验证响应 210，借此标签认证模块 214 不需要具有知晓标签 100 所维持的信息，而是可改为拥有对应的不对称密码值（例如，对应于标签的私用密钥的公共密钥，或反之亦然）。

[0056] 认证响应 218 可基于由标签认证模块 214 执行的确定而传回到认证装置 200 和 / 或一个或更多个第三方服务（未示出）。举例来说，如果标签认证模块 214 确定安全标签 100 真实，那么认证响应 218 可包含安全标签 100 是真实的指示。类似地，如果标签认证模块 214 确定安全标签 100 不真实，那么认证响应 218 可包含安全标签 100 是不真实的指示。在某些实施例中，认证响应 218 中所包含的信息可显示在认证装置 200 上（例如，经由标签认证应用程序 204），从而允许认证装置 200 的用户接收安全标签 100 是否已由可信机构 102 结合各种安全交易而被认证的指示。在一些实施例中，认证装置 200 和 / 或可信机构 102 可将认证响应 218 转发给服务提供商，以使得服务提供商可确认存在的证据。

[0057] 在一些实施例中，如果标签认证模块 214 确定安全标签 100 是真实的，那么认证响应 218 进一步包括可进一步包括与安全标签 100 相关联的某标签元数据 216 和 / 或交易信息。举例来说，在某些实施例中，标签元数据 216 可包括标签认证信息、与相关联于安全标签 100 的产品和 / 或装置相关的信息，和 / 或可与安全标签 100 和 / 或将安全标签 100 用作认证手段的交易相关联的任何其它信息。认证响应 218 中所包含的元数据和 / 或其它信息可进一步向标签认证装置 200 的用户显示。举例来说，与经认证的安全标签 100 相关联的用户的照片可包含在认证响应 218 中且显示在认证装置 200 上，进而允许认证装置 200 的用户验证将安全标签 100 呈现给认证装置 200 的人与安全标签 100 相关联，如可信机构 102 所指示。

[0058] 本文所公开的系统和方法的实施例可允许由安全标签 100 和 / 或可信机构 102 存储的秘密信息 104 不透露给认证装置 200 和 / 或相关服务提供商系统，和 / 或直接从安全标签 100 或可信机构 102 传达。因为秘密信息 104 不透露给认证装置 200，所以认证装置 200 可不需要包含被设计成保护此秘密信息 104 的专有权的安全性经强化的软件和 / 或硬件组件，进而降低对于实施这些认证装置所需要的成本和复杂性。此外，在将秘密信息 104 最初

提供给标签 100 之后，秘密信息 104 不需要在标签 100 与各种其它系统和 / 或装置（例如，认证装置 200 和 / 或可信机构 102）之间传达。因此，这些通信信道可为相对不安全的通信信道。在一些实施例中，这可允许现有数据网络（包含（例如）开放移动装置数据网络、因特网和 / 或类似物）结合各种所公开的实施例来使用。

[0059] 在一些实施例中，标签 100 和 / 或可信机构 102 可经安全性强化（例如，使用基于安全软件和 / 或硬件的安全性技术），而认证装置 200 可未经安全性强化和 / 或经较小程度的安全性强化。在一些实施例中，认证装置 200 的可信度可由与装置 200 相关联的可信实体和 / 或起源控制机构基于认证装置 200 的发行而根据背景建立的。举例来说，认证装置 200 的所有人可基于用户对装置 200 的发行和 / 或拥有受既定的起源控制机构严格控制，而对装置 200 指定某一信赖度。

[0060] 在其它实施例中，本文所公开的系统和方法可使用相对不安全的标签 100 和 / 或认证装置 200（例如，相比可信机构 102 实施较少安全性强化的标签 100 和 / 或装置 200）来实施。可信机构 102 可实施较稳健的安全性措施（例如，使用基于安全软件和 / 或硬件的安全性技术、利用可信机构 102 的远程位置来限制对可信机构 102 上的数据和 / 或进程的访问，和 / 或类似物）。在某些实施例中，此配置可实现集中式安全性的利用、相对低成本的现有的标签认证装置 200 的使用（例如，执行标签认证应用程序 204 的移动智能电话和 / 或平板计算装置）和 / 或相对不安全的标签 100 的使用。举例来说，在一些实施例中，标签 100 可不存储秘密信息 104 和 / 或其它安全信息，而是存储标签 100 特有的所提供的识别符。可信机构 102 可结合认证装置 200 而基于标签 100 存储唯一识别符的确定来认证标签 100。如下文更详细地论述，结合产品证实，标签与相关联的项目之间的一对一对应可由可信机构 102 维持。基于此对应，可信机构 102 可能够检测伪造的标签 100 和 / 或项目（例如，通过识别具有复制的识别符的标签等）和 / 或响应于此而采取适当动作（例如，通知管理机构等）。

[0061] 应了解，可在本发明的范围内对结合图 2 而呈现的架构和关系进行许多变化。举例来说，但不加限制，在一些实施例中，由认证装置 200 执行的功能中的一些或全部可由可信机构 102 执行。类似地，由可信机构 102 执行的功能中的一些或全部可由认证装置 200 执行。如下文更详细地论述，图 2 所说明的安全标签认证和 / 或存在验证过程的某些方面可结合利用安全电子标签的各种安全交易来使用，包含（不限于）产品认证、库存管理和 / 或所有权服务、产品信息分发服务、储值卡和 / 或忠诚卡系统（例如，私有货币系统）、用户认证服务、文档签名服务、电子商务服务（例如，拍卖服务）、识别服务、电子货币服务和 / 或类似物。因此，应了解，是出于说明和解释的目的而不是出于限制的目的而提供图 2。

[0062] 图 3 说明根据本发明的实施例的由认证装置认证安全电子标签的示范性方法 300 的流程图。所说明的方法 300 可按各种方式来实施，包含使用软件、固件、硬件和 / 或其任何组合。在某些实施例中，方法 300 可至少部分由在如上所述的认证装置上执行的标签认证应用程序实施。

[0063] 在 302 中，可由装置检测位于标签认证装置附近的安全标签。在某些实施例中，可响应于由认证装置执行的轮询过程而检测安全标签。举例来说，认证装置可使用相关联的无线通信系统（例如，NFC、RFID 通信等）来执行轮询过程。在某些实施例中，无线通信系统可具有从认证装置扩展的特定范围。因此，当在无线通信系统的范围内检测安全标签时，可

确定安全标签位于标签认证装置附近。以这种方式，本文所公开的实施例可用于确定以下两种情况：安全标签是由可信机构提供的真实标签；以及真实标签位于认证装置附近（例如，存在验证）。

[0064] 在检测到安全标签之后，在 304 中，可将请求安全标签的认证的标签认证请求从标签认证装置传达给可信机构。在某些实施例中，标签认证请求可包含由认证装置从附近安全标签接收的信息，包含（例如）标签识别信息、交易信息，和 / 或类似物。在某些实施例中，此信息可由可信机构用于产生挑战信息，所述挑战信息稍后作为标签认证过程的一部分而传达给安全标签。

[0065] 在 306 中，标签认证装置可响应于标签认证请求而从可信机构接收挑战信息。在某些实施例中，挑战信息可包括随机和 / 或伪随机地产生的值，例如，密码随机数，但其它类型的挑战信息也可结合所公开的系统和方法来使用。在其它实施例中，标签认证装置和 / 或另一第三方服务可产生挑战信息且将其传达给标签和 / 或可信机构。

[0066] 在 308 中，标签认证装置可将挑战信息作为挑战询问的一部分而传达给位于附近的标签，所述挑战询问请求安全标签至少部分基于挑战信息而传回响应。在某些实施例中，所请求的响应可包括由安全标签基于挑战信息和安全标签所存储的秘密信息而执行的计算（例如，数字签名操作、散列计算等）的结果。

[0067] 在 310 中，由标签认证装置从位于附近的安全标签接收对挑战询问的响应，所述响应在 312 中继而被转发给可信机构以由可信机构认证。在 314 中，可从可信机构接收指示标签是否为由可信机构提供的真实安全标签的标签认证响应。基于此响应中所包含的信息，可将标签是否真实的指示提供给标签认证装置的用户。

[0068] 在其它实施例中，标签认证响应可包含额外的元数据（例如，与安全标签的登记用户相关联的用户信息）和 / 或其它交易信息（例如，与安全标签相关联的账户余额的指示）。应了解，与安全标签相关联的各种元数据和 / 或交易信息可包含在标签认证响应中，且可用于安全标签认证过程和 / 或涉及存在验证的交易中的任何适当类型的信息可结合本文所公开的实施例来使用。

[0069] 图 4 说明根据本发明的实施例的由可信机构认证安全电子标签的示范性方法 400 的流程图。所说明的方法 400 可按各种方式来实施，包含使用软件、固件、硬件和 / 或其任何组合。在某些实施例中，方法 400 可至少部分由在如上所述的认证装置上执行的挑战产生器和 / 或标签认证模块实施。

[0070] 在 402 中，可从已检测到位于附近的标签的标签认证装置接收标签认证请求。在某些实施例中，标签认证请求可包含由认证装置从附近标签接收的信息，包含（例如）标签识别信息、交易信息和 / 或类似物。在接收到标签认证请求之后，在 404 中，可信机构可产生挑战信息。标签信息可包括随机和 / 或伪随机地产生的值，例如，密码随机数。在其它实施例中，标签认证装置和 / 或另一第三方服务可产生挑战信息且将其传达给安全标签和 / 或可信机构。

[0071] 在 406 中，将所产生的挑战信息传达给标签认证装置。标签认证装置可将挑战信息作为挑战询问的一部分而传达给标签。在 408 中，可由可信机构从认证装置和 / 或标签接收由标签响应于挑战询问而产生的第一挑战响应。在 410 中，可信机构可使用在 404 中产生的挑战信息和可信机构所拥有的秘密信息而产生第二挑战响应。在某些实施例中，由

可信机构在 410 中使用的秘密信息可与特定安全标签相关联。在一些实施例中，可使用从标签认证装置传达的与安全标签相关联的标签识别信息而在秘密信息的多个例子之间识别由可信机构使用的秘密信息（例如，作为标签认证请求的一部分等）。

[0072] 在某些实施例中，第二挑战响应可包括由可信机构执行的计算的结果。举例来说，在一些实施例中，第二挑战响应可包括挑战信息中所包含的密码随机数的带数字签名的值和 / 或散列值。在某些实施例中，由可信机构执行的计算可为由安全标签响应于挑战询问而执行的相同计算。

[0073] 在 412 中，可比较从标签认证装置接收的第一挑战响应与可信机构所产生的第二挑战响应。如果第一挑战响应和第二挑战响应相同，那么在 414 中可确定标签是真实的（例如，标签拥有由可信机构提供的秘密信息）。在 416 中，可由可信机构将指示标签是真实的响应发送给标签认证装置。如果第一挑战响应和第二挑战响应不相同，那么在 418 中可确定标签是不真实的（例如，标签不拥有由可信机构提供的秘密信息）。在 420 中，可由可信机构将指示标签是不真实的响应发送给标签认证装置。

[0074] 虽然未具体说明，但如果在 414 中确定标签是真实的，那么在 416 中发送的响应可进一步包含与标签相关联的额外信息。举例来说，所发送的响应进一步包括可进一步包括与标签相关联的标签元数据和 / 或交易信息，包含（不限于）例如标签认证信息、与关联于安全标签的产品、装置和 / 或用户相关的信息、与标签相关联的交易信息（例如，账户余额等）、进行交易的授权和 / 或任何其它适当信息。在一些实施例中，作为响应而发送的数据 416 可由信任机构签名，以使得甚至当装置或信任机构将 416 转发给第三方（例如，服务提供商）时，第三方也可通过验证信任机构的签名来将 416 用作存在的证据。

[0075] 应了解，是出于说明的目的而不是出于限制的目的而提供图 4 ；且可对本文所说明的过程进行许多修改，而不偏离发明性工作主体的原理。举例来说，某些步骤可按不同次序执行、与其它步骤组合和 / 或类似物。举例来说，在一些实施例中，可信机构可产生所要的挑战响应，所述所要的挑战响应可使用（例如）密钥值来变换（例如，通过对所要的挑战响应进行加密）。当接着接收到挑战响应时，可简单地将挑战响应与最初选择的值进行比较（即，在此实施例中，将不需要在服务器处重新计算挑战响应）。因此，应了解，可使用任何一种或更多种适当的挑战 / 响应协议。

[0076] 系列化产品证实

[0077] 所公开的系统和方法的某些实施例可结合识别和 / 或检测各种产品和 / 或项目来使用。随着三维打印和使制造看起来类似于原件的物品的复制品更容易的其它技术的出现，伪造的项目（包含（例如）艺术品、设计师服装和配饰、原始设备制造商（“OEM”）部件、药品等）的检测可变得越来越困难。本文所公开的系统和方法可使用安全标签以及标签认证和 / 或存在验证以阻碍和 / 或以其它方式检测伪造行为。本文所公开的系统和方法的某些方面可集成到使用一个或更多个可执行应用程序的现有消费型装置中，从而允许消费者识别伪造的物品、通过使伪造的物品较容易识别来阻碍伪造，且辅助制造商和 / 或执法机构识别伪造行为的模式、采集证据和 / 或类似物。

[0078] 利用电子标签的某些常规系统可使用被称为线上到线下（“020”）协议的技术。在此系统中，标签可与物品相关联（例如，为产品或事件做广告的海报）。消费者可对着物品点击包含标签读取器的移动装置（例如，智能电话），且被引向提供关于产品或事件的额

外信息的网站（例如，对应于标签中所嵌入的URL的页面）。然而，在此系统中，标签可按一种方式被伪造，以使得消费者可对着标签点击其移动装置，但标签会将消费者引向伪造者以类似于用于恶意欺诈电子邮件活动中的“钓鱼”的方式选择的网站。

[0079] 本文所公开的系统和方法可用于通过使用安全电子标签来防止电子标签的伪造和/或减轻钓鱼行为。在一些实施例中，安全标签的制造商M可获得和/或以其它方式产生唯一秘密字符串S(M)或其它秘密信息和唯一识别符ID(M)。当制造商产生具有所嵌入的URL的标签时，制造商可使用密码函数H(...)（例如，单向散列函数）以计算H(S(M)，ID(M)，URL，...)（包含超出其选择的URL的任何信息（例如，元数据信息）），且可将计算的结果安全地嵌入到安全标签中。当安全标签由移动装置读取（例如，经由在移动装置上执行的标签认证应用程序）时，移动装置可通过作为也可计算密码函数的结果的可信机构而操作的可信服务提供商来检查密码函数计算的结果和制造商识别符。如果结果（例如，散列）不匹配，那么可信机构可告知移动装置和/或其用户怀疑是伪造的标签和/或钓鱼攻击。其它实施例可扩展上述方法以促进与安全标签相关联的物品自身是否已被伪造的检测。

[0080] 某些实施例可允许物理项目和/或产品的制造商将系列化安全标签与项目和/或产品的系列化复制品安全地相关联。在某些实施例中，安全标签可按一种方式与产品相关联，以使得将安全标签从产品移除将导致对安全标签和/或产品的损坏。举例来说，安全标签可与产品、产品的容器和/或类似物附着和/或以其它方式在物理上相关联（例如，经由包装）。可信服务提供商（例如，可信机构）T可证实合法的产品制造商M。可信服务提供商可将与制造商M相关联的唯一秘密字符串S(M)或其它秘密信息和唯一识别符ID(M)提供给制造商。当制造商制造具有序列号n的系列化产品P时（其中P(n)是对产品P的合法版本进行的序列号的指派），制造商M可产生存储与产品相关联的URL(URL(P))和/或与可信服务相关联的URL(URL(T))的系列化安全标签。

[0081] 例如散列函数等密码函数H(...)可用于计算结果H(S(M)，ID(M)，URL(P)，URL(T)，P(n)，...)。结果可存储在每一安全标签中，从而导致系列化安全标签与系列化产品之间的1对1对应。安全标签的安全性可经由确保唯一秘密字符串S(M)或其它秘密信息不透露给其它各方而由安全标签的制造商维持。因为安全标签可用于识别相关联的产品的有效性和/或真实性，所以相关联的产品的固有值可捆绑到安全标签。

[0082] 所公开的系统和方法的实施例可用于结合购买交易来证实产品的真实性。作为购买交易的一部分，用户可使用智能电话或其它移动装置来读取与产品相关联的安全标签所存储的信息。移动装置上的应用程序可询问用户在购买新的还是使用过的产品。如果购买新的，那么系统和方法的实施例可用于查看产品的特定系列化版本先前是否已由另一方新购买。应用程序还可结合交易而收集与安全标签在哪里由移动装置读取的位置相关联的其它数据（例如，GPS位置信息等）。如果购买使用过的，那么系统和方法的实施例可进一步检查产品先前已在何时何处由何人购买。在一些实施例中，相关联的服务可使用此信息和/或由制造商获得的先前收集的信息（例如，关于使用和/或转售模式的信息）以确定产品是被授权的复制品的可能性。

[0083] 图5说明根据本发明的实施例的包含安全电子标签100的系列化产品500的证实。可信机构102和/或另一可信服务提供商可向安全标签100提供秘密信息104。在提

供之后，安全标签 100 可与产品 500 安全地相关联（例如，通过产品的制造商或另一第三方）。产品 500 可包含任何产品和 / 或项目，包含（不限于）艺术品、设计师服装和配饰、OEM 部件、车辆、药品、储值卡和 / 或回馈卡、移动装置和 / 或类似物。在某些实施例中，产品 500 可为唯一产品。在其它实施例中，产品 500 可为系列化产品 500。即，产品 500 可为产品的多个复制品中具有相关联的序列号或其它唯一识别符的一个复制品。

[0084] 在某些实施例中，安全标签 100 可与系列化产品 500 在物理上相关联。举例来说，安全标签 100 可按一种方式与产品 500 相关联，以使得将安全标签 100 从产品 500 移除将导致对安全标签 100 和 / 或产品 500 的损坏，和 / 或降低与安全标签 100 和 / 或产品 500 相关联的价值。在其它实施例中，安全标签 100 可按一种方式与产品 500 和 / 或关联于产品 500 的容器附着和 / 或在物理上相关联，以使得安全标签 100 的存在在产品 500 上可看不见或另外显而易见。

[0085] 用户可对获得关于产品 500 的信息感兴趣。在某些情形下，用户可对结合涉及产品 500 的交易（例如，购买）而获得关于产品 500 的信息感兴趣。举例来说，结合购买交易，用户可尤其希望证实产品 500 是来自其制造商的真实产品且不是伪造品，确认产品 500 是新产品或先前未作为新产品而出售过，获得关于产品 500 的所有权历史信息和 / 或类似物。根据本文所公开的实施例，用户可经由涉及与产品 500 相关联的安全标签 100 的认证过程而获得此信息。

[0086] 为了证实产品 500 和 / 或获得相关联的信息，用户可使用认证装置 200。认证装置 200 可尤其证实安全标签 100 是由可信机构 102 提供的真实标签，且通过扩展，证实与安全标签 100 相关联的产品 500 是位于认证装置 200 附近的真实和 / 或有效的产品 500。在某些实施例中，在认证装置 200 上执行的产品证实应用程序 502（例如，由可信机构 102、产品 500 的制造商和 / 或任何其它方提供的应用程序）可结合根据本文所公开的实施例的标签认证和 / 或存在验证过程来使用。

[0087] 在一些实施例中，产品证实应用程序 502 可使用标签认证装置 200 来执行轮询过程，以检测包含安全标签 100 的位于附近的产品 500。在其它实施例中，可使用其它标签检测技术。当产品证实应用程序 502 检测到包含安全标签 100 的位于附近的产品 500 时，产品证实应用程序 502 可产生请求证实产品 500 证实的产品证实请求 504，且将产品证实请求 504 传达给可信机构 102。

[0088] 类似于上文参照图 2 所述的标签认证过程，可信机构 102 可使用挑战产生器 212 而产生挑战信息 208，且将挑战信息 208 传达给产品 500 中所包含的安全标签 100。安全标签 100 可传达挑战响应 210，挑战响应 210 可包含由安全标签 100 使用挑战信息 208 和安全标签 100 所存储的秘密信息 104 而执行的计算（例如，散列计算等）的结果。挑战响应 210 可进一步包含与安全标签 100 相关联的其它信息，例如，与标签 100 和 / 或产品 500 相关联的序列号和 / 或其它识别信息。

[0089] 可信机构 102 可比较挑战响应 210 中所包含的结果与可信机构 102 使用标签认证模块 214 基于挑战信息 208 和可信机构 102 所拥有的秘密信息 104 而执行的类似计算的结果。如果结果匹配，或满足某一预定关系，那么可信机构 102 可确定安全标签 100 是由可信机构 102 提供的真实标签，且因此，相关联的产品 500 是有效的。如果结果不匹配，那么可信机构 102 可确定安全标签 100 不是由可信机构 102 提供的真实标签，且因此，相关联的产

品 500 不是有效的或已与伪造的标签相关联。。可信机构 102 可将指示产品 500 是否曾由可信机构证实的产品证实响应 506 传达给认证装置 200。基于证实响应 506 的内容，可在装置 200 上向认证装置 200 的用户呈现关于产品 500 是否有效的指示（例如，“产品有效”）。在其它实施例中，如果有效，那么关于产品 500 的额外信息（例如，由可信机构 102 和 / 或另一服务维持的产品元数据 508）可包含在证实响应 506 中，且呈现给认证装置 200 的用户

[0090] 根据本文所公开的实施例，安全标签 100 所存储的相关联的序列号或其它唯一识别符可被传达给可信机构 102。序列号或识别符可由安全标签 100 结合计算挑战响应 210 中所包含的结果来使用。类似地，序列号或识别符可进一步由可信机构 102 用于计算结果以用于与来自安全标签 100 的挑战响应 210 中所包含的结果进行比较。以这种方式，本文所公开的认证过程可使用与安全标签 100 和 / 或产品 500 相关联的唯一系列化信息。序列号或识别符还可由可信机构 102 用于从可信机构 102 所维持的产品元数据的数据库识别与安全标签 100 和 / 或产品 500 相关联的产品元数据 508 且且分发产品元数据 508。

[0091] 维持安全标签 100 与有效或合法产品 500 的 1 对 1 对应可加强所公开的系统和方法减轻伪造的能力。虽然系列化安全标签 100 可不容易被伪造者制造，但个别安全标签 100 可被复制（虽然不像产品自身一样容易），以致于可存在现存的给定系列化标签的一个以上复制品。因此，在一些实施例中，额外技术可用于减轻伪造行为。举例来说，在某些实施例中，可信机构 102 可充当制造商及其产品 500 的登记机构。

[0092] 在一些实施例中，可信机构 102 可通过核对合法制造商且提供产品证实服务而向消费者和制造商提供有价值的服务。此外，可信机构 102 可提供基于机器学习的模式检测服务以识别违法产品复制和 / 或销售的模式。可信机构 102 可在产品 500 的引入之前收集数据，且可在产品 500 已被引入之后从用户收据数据（例如，通过收集用户和后续用户的使用模式）。可通过可信机构 102 利用结合本文所公开的产品证实技术而识别的使用模式和 / 或 GPS 位置、时间、日期、所有权和 / 或产品分类信息来识别欺诈行为。

[0093] 失窃商品识别

[0094] 所公开的系统和方法的某些实施例可结合阻碍和 / 或检测盗窃来使用。在购买或以其它方式获得新的或使用过的项目之后，消费者和 / 或卖主可向可维持此信息的可信机构记录、登记和 / 或以其它方式主张所述项目的所有权。举例来说，可信机构可维持关于项目是新的还是先前已出售过的信息（例如，项目可向可信机构登记为“新的”、“使用过的”、“第一次出售”、“第二次出售”和 / 或类似物）。通过将用户识别符与每一所登记的交易相关联，与特定用户相关联的产品和 / 或产品的序列号的列表可由可信机构维持。以后，如果用户因盗窃而遭受到项目的损失，那么用户可从可信机构检索其项目的列表，且指示这些项目中的哪一个被盗和 / 或以其它方式丢失。

[0095] 将失窃项目报告给可信机构可由用户直接执行和 / 或由例如执法官员等另一方执行（例如，作为警察报告过程的一部分等）。举例来说，可给予执法官员与可信机构相关联的特殊账户，所述特殊账户可允许官员在由可信机构维持的项目数据库（例如，产品元数据数据库）中将项目报告和 / 或识别为被盗。项目可按一种方式来标记，以使得如果用户（例如）通过尝试认证（例如，扫描）项目的标签来询问项目的状态，主张项目的所有权，在认证装置附近经过和 / 或类似物，那么可将通知提供给可信机构、执法官员和 / 或其它关注方（例如，主张项目的所有权的另一用户）。

[0096] 通知可包含（不限于）通知将项目分类为失窃的机构、通知曾报告项目失窃的用户、通知接近所扫描的项目位置（例如，如通过认证装置的位置和/或其它位置识别手段（例如，蜂窝无线电三角测量、GPS、所报告的用户位置、IP地址跟踪等）来确定）的机构（例如，执法机构）和/或通知潜在买主（例如，尝试扫描或以其它方式认证项目的人）。在某些实施例中，通知可包含额外数据，例如，与认证请求相关联的用户账户、发生扫描的位置（例如，GPS位置）、对应于安全标签和/或认证装置的其它环境数据、项目被报告为失窃的日期和/或位置和/或类似物。通过使失窃商品的潜在客户能够在购买之前证实商品，执法的范围可大幅增大到商品的灰色市场内的许多出售点，进而帮助减小可能的窃贼的潜在转售市场且定位可能涉及到失窃财产的洗白的个人。

[0097] 产品信息分发

[0098] 图6说明根据本发明的实施例的与包含安全电子标签100的产品600相关的信息的分发。如上文所论述，安全标签100可由可信机构102和/或另一可信服务提供商提供秘密信息104，且与产品600安全地相关联（例如，通过产品的制造商或另一第三方）。虽然产品600被说明为车辆，但产品600可包括任何类型的项目和/或产品，包含下文详述的类型的项目和/或产品中的任一者。在其它实施例中，产品600可为用户可使用本文所公开的系统和方法来交互以接收与产品和/或服务相关的信息的项目，例如，广告和/或其它系统（例如，信息亭等）。

[0099] 消费者感兴趣的各种信息可与产品600相关联。举例来说，由于安全顾虑或其它，制造商可针对某些产品型号或给定型号的某些组特定序列号发出安全召回。当发生这种情形时，制造商可将某一形式的补偿给予消费者，以作为对消费者销毁或除去危险产品600和/或将产品带来维修的交换。在一些情形下，仅某些产品型号或序列号可在产品召回中受到影响且符合补偿条件，且因此安全地认证系列化产品600可结合服务产品召回来使用。

[0100] 所公开的系统和方法的实施例可通过以下方式来促进此类工作：提供便于采集和报告此产品信息和/或登记和/或以其它方式建立召回要求（例如，维修、更换等）的符合条件的机制。举例来说，在安全相关召回的状况下，可希望确保潜在危险产品600不转售给不知情的个人。通过将本文所公开的报告能力扩展到包含产品召回信息，潜在客户还可被警告对所述消费者可使用认证装置200而扫描的产品600的特定型号和/或序列号的召回。通过收集和/或审核此数据，可辅助制造商识别可能已正确实施召回的经授权分销商或零售商，或可能出于营利的目的而忽视召回的名声不佳的销售人员。

[0101] 用户可对获得关于产品600的信息感兴趣。举例来说，结合购买交易，用户可尤其希望证实：产品600不具有尚未解决的制造商召回；产品600已根据产品召回和/或维护时间表来维修；和/或接收与产品600相关的任何其它信息。根据本文所公开的实施例，用户可经由涉及与产品600相关联的安全标签100的认证过程而获得此信息。

[0102] 为了证实产品600和/或获得相关联的信息，用户可使用认证装置200。举例来说（非限制），在一些实施例中，认证装置200可为用户的智能电话或平板计算机，在所述智能电话或平板计算机上加载了如上所述的与可信机构102交互的应用程序。认证装置200可尤其证实：安全标签100是由可信机构102提供的真实标签；标签100在特定时间在物理上位于认证装置200附近；以及通过扩展，与安全标签100相关联的产品600是位于认证装置

200 附近的真实和 / 或有效的产品 600。在某些实施例中，在认证装置 200 上执行的产品信息应用程序 602（例如，由可信机构 102、产品 600 的制造商和 / 或任何其它方提供的应用程序）可结合根据本文所公开的实施例的标签认证和 / 或存在验证过程来使用。

[0103] 当产品信息应用程序 602 检测到包含安全标签 100 的位于附近的产品 600 时，产品信息应用程序 602 可产生请求产品 600 的证实的信息请求 604，且将信息请求 604 传达给可信机构 102。在某些实施例中，信息请求 604 可包括对关于产品 600 的信息（例如，召回信息、服务信息、所有权信息和 / 或与产品 600 相关的任何其它信息）的请求。

[0104] 类似于上文所述的标签认证过程，可信机构 102 可产生挑战信息 208，且将挑战信息 208 传达给产品 600 中所包含的安全标签 100。安全标签 100 可传达挑战响应 606，挑战响应 606 可包含由安全标签 100 使用挑战信息 208 和安全标签 100 所存储的秘密信息 104 而执行的计算（例如，散列计算等）的结果。挑战响应 606 可进一步包含与安全标签 100 相关联的其它信息，例如，与标签 100 和 / 或产品 600 相关联的序列号和 / 或其它识别信息（例如，产品识别符）。

[0105] 可信机构 102 可比较挑战响应 606 中所包含的结果与可信机构 102 使用标签认证模块 214 基于挑战信息 208 和可信机构 102 所拥有的存储在数据库 608 中的秘密信息而执行的类似计算的结果，数据库 608 将多个密码密钥（例如，秘密密钥、不对称密钥等）与多个产品识别符相关联。如果结果匹配，那么可信机构 102 可确定安全标签 100 是由可信机构 102 提供的真实标签，且因此，相关联的产品 600 是真实的。如果结果不匹配，那么可信机构 102 可确定安全标签 100 不是由可信机构 102 提供的真实标签，且因此，相关联的产品 600 是不真实的。

[0106] 在确定产品 600 是真实的之后，可信机构 102 可向认证装置 200 提供由可信机构和 / 或另一服务（例如，在产品元数据数据库 508 和 / 或类似物中）维持的与产品 600 相关联的信息 610。在某些实施例中，被提供给认证装置 200 的信息 610 可包括由认证装置 200 结合信息请求 604 而请求的信息。举例来说，信息 610 可包括与产品 600 相关联的任何制造商召回的指示、与产品 600 相关联的维修历史、与产品 600 相关联的规格和 / 或其它信息、与产品 600 相关联的广告内容、与产品 600 相关联的所有权信息（例如，产品是否失窃、所有权历史信息等）和 / 或与产品 600 相关联的任何其它信息。可在装置 200 上向认证装置 200 的用户呈现所接收的产品信息 610 的指示（例如，“产品被召回”）。产品信息 610 可进一步被提供给一个或更多个第三方，例如，执法部门、产品制造商和 / 或类似物。

[0107] 起源控制和产品登记

[0108] 本文所公开的系统和方法的某些实施例可用于更严格地控制和 / 或管理价值链和 / 或售后市场中的产品的登记所有人之间的换手。针对高价值项目，对于当前所有人来说，限制特定系列化项目的登记状态的改变和 / 或以相当程度的确定性维持项目的所有所有人的准确记录是有利的。举例来说，奢饰品的所有人可具有许多前来访问他或她的财产的客人，和 / 或奢饰品零售商可在实际客户购买产品之前有许多潜在客户查看产品。

[0109] 为了防止普通用户将商店中的新产品“主张”为已被购买或防止一居所处的客人“主张”其并不拥有的产品，这一项目的当前所有人可对可信机构和 / 或其它服务所维持的与所述所有人的项目相关联的数据（例如，产品元数据）中的一些或全部加锁。举例来说，在项目展示在商店中时，所管理的产品元数据中所包含的产品购买属性（例如，“新的”、“第

一次出售”等）和所有人属性（例如，当前所有人属性）可由当前所有人（例如，零售商）锁定。在购买交易期间，零售商或其它授权方可解锁且改变与项目相关联的购买属性（例如，改变为“已出售”），解锁所有人属性，且移除其姓名或其它识别符，或以其它方式将所有人属性改变为新的一方（例如，买方）。此时，买方可扫描与项目相关联的标签，且为自己主张所述项目。如果在以后，所述项目被再次出售，所述过程可重复，其中每一交易已由可信机构和 / 或其它可信服务记录且安全地存储。以这种方式，项目的起源可作为项目的固有部分进行跟踪和 / 或报告。在一些实施例中，项目可基于其利用本文所公开的系统和方法而管理的可验证的起源而获得价值（例如，著名棒球选手所拥有的第一根棒球球棒、著名演员所给出的设计师珠宝首饰等）。

[0110] 所公开的系统和方法的其它实施例可结合产品登记、质保管理、产品召回管理、产品生命末期管理和 / 或类似物来使用。举例来说，在购买项目（例如，新的项目或使用过的项目）之后，新的所有人可扫描附着到项目的相关联的安全标签以记录序列号和 / 或型号、购买日期和 / 或类似物，且将其自身的个人识别信息与项目相关联（例如，通过将此信息包含在产品元数据和 / 或由可信机构和 / 或其它可信服务管理的其它信息中）。如果特定项目和 / 或序列号遭受未来召回（例如，安全召回），那么制造商可访问产品的原始所有人和 / 或当前所有人的管理列表，以向相关各方告知召回。

[0111] 当使用根据本文所公开的实施例的认证装置来扫描与项目相关联的安全标签时，可向用户提供与项目相关联的各种信息。举例来说，可向用户提供关于与项目相关联的过去召回的信息、项目的序列号、安全考虑、可仍对项目有效的质保或保证、特定项目、型号和 / 或序列号的支持或服务寿命末期、用户可感兴趣的相关产品和 / 或报价，和 / 或与项目相关的任何其它相关信息。出于产品召回和 / 或质保的目的，本文所公开的系统和方法的实施例可帮助确保制造商不会错误地补偿伪造的项目的买主和 / 或如果消费者不拥有具有可验证的安全标签的真项目，那么可为制造商提供可验证的理由来拒绝客户补偿。

[0112] 在一些实施例中，可信机构和 / 或其它服务可管控哪方可改变由可信机构和 / 或服务管理的与项目相关联的各种属性和 / 或其它元数据或信息。举例来说，在一些实施例中，可信机构和 / 或服务可指定 ：仅制造商将能够改变特定系列化项目的召回状态 ；仅制造商将能够将项目的购买状态改变为“新”；仅制造商或经授权修理中心将能够根据工厂标准而将状态改变为“经过整修”或“经过修理”；仅经授权分销商将能够将购买状态改变为“第一次出售”；仅登记的所有人或主管机构将能够移除 / 改变所有权 ；仅登记的所有人可添加关于项目的断言且可仅在其拥有项目时添加断言（例如，“2020 世界系列赛中所使用的幸运球棒”）和 / 或类似物。这些策略可通过任何适当技术来实行，包含（不限于）常规密码认证、DRM 技术（例如，‘693 申请案中所描述的 DRM 技术）和 / 或类似物。

[0113] 储值卡、忠诚卡和识别卡交易

[0114] 私有货币和 / 或零售商点、奖励点和 / 或类似物可使用基于储值卡、忠诚卡和 / 或其它识别卡的系统来实施。举例来说，零售商（例如，咖啡店）可实施奖励点系统，其中客户可结合交易来累积忠诚奖励（例如，奖励点），且可兑换忠诚奖励以交换某些产品和 / 或服务（例如，免费咖啡等）。然而，因为常规系统通常使用许多元件（包含唯一客户识别发行、客户识别认证和后端服务）来使私有货币循环，所以可需要大量工作和投资来建立并维持这些私有货币系统的安全性。此外，可难以建立可由多个不同零售商使用的安全私有

货币系统。

[0115] 本文所公开的系统和方法的实施例可结合基于储值卡、忠诚卡和/或其它识别卡的私有货币系统来使用。具体来说，本文所公开的安全标签认证技术的实施例可结合各种安全交易结合确定包含安全标签的储值卡、忠诚卡和/或其它识别卡的存在证据来使用。尤其，通过在与交易相关联的位置处验证具备真实安全标签的真实的储值卡、忠诚卡和/或其它识别卡的存在，可确定相关联的用户实际上存在于所述位置处。

[0116] 图7A说明根据本发明的实施例的包含安全电子标签的忠诚卡的提供。在某些实施例中，零售商（例如，商店的所有者）700或对实施基于储值卡、忠诚卡和/或其它识别卡的私有货币系统感兴趣的其它方可与可信机构102或提供私有货币服务的其它可信服务提供商（例如，网络服务等）交互。在一些实施例中，可信机构102可对多方（例如，多家餐馆等）提供基于卡的私有货币服务。

[0117] 零售商700或其它方可使用可信机构102来建立账户。通过使用可信机构102来建立账户，零售所有者700可针对顾客而建立其由可信机构102服务的私有货币。在其它实施例中，零售商700可将其由可信机构102服务的私有货币的可用性扩展到一方或更多其它方。在又其它实施例（例如，与卡相关联的储值相对少的情形）中，不需要使用安全和/或秘密标签。而是改为使用（例如）用户拥有的简单条形码（例如，在卡上和/或在智能电话应用程序中）。

[0118] 根据本文所公开的实施例，零售商700可具备包含标签和/或储值的一张或更多张卡和/或一个或更多个其它装置（例如，钥匙扣装置等）。卡可由零售商700分发给希望使用通过经由可信机构102服务的零售商700提供的私有货币的一个或更多个客户。在其它实施例中，零售商70可不将卡分发给用户，而是将应用程序分发给使用存储在用户的装置上的储值（例如，在制造时充入的安全和/或秘密的储值（和/或由此产生的储值）、由可信机构102充入的值、非安全储值和/或类似物）而实施本文所述的技术的用户的智能电话或其它装置。虽然为了便于解释，本文所述的实例中的一些涉及基于卡的系统，但应了解，替代地或另外，这些系统可利用在用户的智能电话或其它装置上运行的应用程序（进而消除用户携带独立卡的需要）。

[0119] 图7B说明根据本发明的实施例的忠诚卡702认证过程。在将忠诚卡702分发给希望使用零售商的私有货币的一个或更多客户之后，客户可使用忠诚卡702来认证其在利用认证装置200的零售商位置处的实际存在。举例来说，每当消费者购买一杯咖啡时，零售商就可以基于点的私有货币奖励客户某数量的点。当客户访问零售商时，客户可通过使用在零售商的认证装置200上执行的私有货币应用程序来认证其忠诚卡702（例如，通过“签到”）而证实其物理存在。在某些实施例中，通过认证客户的忠诚卡702在认证装置200附近的存在来证实客户的存在可利用本文所公开的安全标签认证技术的实施例来执行。如上文所论述，认证装置200可包括被配置成执行可用于实施所公开的安全标签认证技术的应用程序的任何适当装置（例如，智能电话、平板计算系统等）。在证实其存在之后，指示签到过程的结果的消息（例如，与客户相关联的私有货币账户的点的奖励）可显示在认证装置200上。

[0120] 图7C说明根据本发明的实施例的忠诚卡702兑换过程。在某些实施例中，客户可在访问零售商位置时兑换累积的点/货币。举例来说，客户可希望使用累积的点/货币从

零售商购买一杯咖啡。为了兑换累积的点 / 货币，客户可通过认证其忠诚卡 702 在与零售商的位置相关联的认证装置 200 附近的存在而证实其存在。在某些实施例中，零售商可使用在认证 200 上执行的私有货币应用程序以向实施私有货币服务的可信机构请求点 / 货币兑换过程（例如，通过指定正兑换点 / 货币的量等）。作为忠诚卡 702 认证过程的一部分，可信机构可使用私有货币应用程序而以零售商所指定的量将关联于忠诚卡 702 的账户计入借方，且可将指示成功账户借入的指示提供给认证装置 200。

[0121] 虽然上文结合忠诚卡系统来论述，但应了解，类似过程可结合基于储值卡、识别卡和 / 或任何其它卡的私有货币系统来公开。在某些实施例中，与卡相关联的账户余额可由执行本文所公开的安全标签认证操作的可信机构维持和 / 或以其它方式管理。在其它实施例中，可信机构可用于执行某些所公开的安全标签认证应用程序，且提供私有货币的单独第三方服务可用于维持和 / 或以其它方式管理账户余额。

[0122] 私有货币交易

[0123] 图 8 说明根据本发明的实施例的储值卡 800 认证和交易过程。在所说明的实施例中，可信机构 102 可结合认证装置 200 而用于使用本文所公开的安全标签认证过程的实施例来认证储值卡 800，且私有货币服务 802 可用于维持和 / 或以其它方式管理与储值卡 800 相关联的账户余额 804。虽然被说明为单独系统，但应了解，在其它实施例中，认证装置 200、可信机构 102 和 / 或私有货币服务 802 的某些功能可由单一系统和 / 或系统的任何适当组合执行。

[0124] 储值卡 800 可包含由可信机构 102 和 / 或另一可信服务提供秘密信息的安全标签。可信机构 102 可维持数据库，所述数据库尤其将安全标签的识别信息（例如，标签 ID）、对应的所提供的秘密信息（例如，安全密钥等）和 / 或与安全标签相关联的客户的账户信息（例如，账户 ID）相关联。在一些实施例中，储值卡 800（和 / 或智能电话应用程序和 / 或类似物）不需要包含安全标签，而是改为包含账号，且如果接收到（例如）将与卡相关联的储值计入借方的请求，那么某额外形式的认证（例如，输入到装置 200 上的密码）可用于证实所述请求被授权。

[0125] 在标签认证装置 200 上执行的私有货币应用程序可根据本文所公开的实施例检测包含标签或值的位于附近的储值卡 800（例如，响应于轮询过程等）。在检测到位于附近的储值卡 800 之后，标签认证装置 200 可产生挑战信息 R，且将其传达给储值卡 800 中所包含的安全标签。在某些实施例中，挑战信息可包括随机和 / 或伪随机地产生的值，例如，密码随机数（为易于解释，本文中对“随机”值的参考希望涵盖真随机值、伪随机值和 / 或类似物），但其它类型的挑战信息也可结合所公开的系统和方法来使用。在其它实施例中，挑战信息可由可信机构 102 和 / 或另一可信服务产生且传达给安全标签（例如，响应于来自认证装置 200 的认证请求等）。

[0126] 在接收到挑战信息 R 之后，储值卡 800 的安全标签可至少部分基于由安全标签存储的秘密信息而产生 MAC 和 / 或其它计算结果。在其它实施例中，MAC 可进一步基于其它数据（例如，任意消息数据 Msg）而产生。MAC、标签识别信息、挑战信息和 / 或其它数据可从储值卡 800 的安全标签传达给位于附近的认证装置 200，位于附近的认证装置 200 又可将所述信息传达给可信机构 102。

[0127] 可信机构 102 可基于所接收的信息（即，标签 ID、R、MAC、Msg 等）而执行根据本

文所公开的实施例的标签认证过程。举例来说，可信机构 102 可基于所接收的标签识别信息而检索与储值卡 800 的安全标签相关联的安全密钥。所检索的安全密钥可结合基于安全密钥以及挑战信息和 / 或从认证装置 200 接收的其它信息（例如，Msg）计算 MAC 和 / 或其它计算结果来使用。一旦计算出，可信机构 102 可比较所计算的 MAC 与储值卡 800 的安全标签所产生的从认证装置 200 接收的 MAC。如果两个 MAC 值匹配，那么可信机构 102 可将指示安全标签（且通过扩展，储值卡 800）是真实的且位于认证装置 200 附近的认证结果传回到认证装置 200。如果两个 MAC 值不匹配，那么可信机构 102 可将指示安全标签和 / 或储值卡 800 是不真实的认证结果传回到认证装置 200。

[0128] 如果所接收的认证结果指示安全标签和 / 或储值卡 800 是真实的，那么认证装置 200 可将结果转发给与储值卡 800 相关联的私有货币服务 802。如上文所论述，私有货币服务 802 可尤其用于维持和 / 或以其它方式管理与储值卡 800 相关联的账户余额 804 和涉及储值卡 800 的交易。除认证结果之外，认证装置 200 还可将与储值卡 800 的用户希望执行的交易相关的交易信息传达给私有货币服务 802。举例来说，交易信息可请求与储值卡 800 相关联的账户余额 804 中所包含的点的某一量被减去和 / 或加上和 / 或转移到另一账户（例如，与认证装置 200 的用户相关联的账户等）。使用此信息，私有货币服务 802 可执行相关联的交易过程。

[0129] 在执行账户交易过程之后，私有货币服务 802 可将交易成功的确认传达给认证装置 200。认证装置 200 的用户可使用此确认来认证交易被执行，且可进行实行交易的其它方面的动作（例如，向储值卡 800 的用户提供购买的产品等）。

[0130] 在其它实施例中，与用户和 / 或储值卡 800 相关联的账户识别可由储值卡 800 和 / 或认证装置 200 传达给私有货币服务 802。在认证此账户信息之后，私有货币服务 802 可尤其将可用于确定与储值卡 800 和 / 或其用户相关联的可用余额的账户余额信息传达给储值卡 800 和 / 或认证装置 200。虽然未具体说明，但在某些实施例中，认证过程可在认证装置 200 与私有货币服务 802 之间执行，以认证认证装置 200 的用户被授权使用由私有货币服务 802 提供的私有货币。

[0131] 出入卡证实

[0132] 本文所公开的系统和方法的实施例可用于验证出入卡（例如，出入通行卡、交通通行卡和 / 或类似物）的真实性和 / 或状态。所公开的系统和方法可尤其用于验证包含安全标签的出入卡是由可信机构提供的真实卡。此外，所公开的系统和方法可用于确定与所认证的出入卡相关联的账户是活动的和 / 或具有足以用于特定交易的余额。举例来说，所公开的系统和方法的实施例可用于确定由交通管理局发行的真实出入卡（例如，交通卡）已被呈现给相关联的认证装置，且与所呈现的出入卡相关联的账户是活动的和 / 或具有可用于特定行程的充足资金。

[0133] 图 9 说明根据本发明的实施例的交通卡 900 的认证。如上文所论述，可信机构 102 和 / 或另一可信服务提供商可向安全标签 100 提供秘密信息 104，且与卡 900 或关联于消费者的其它装置安全地相关联。虽然卡 900 被说明为交通卡（例如，公共汽车卡、铁路卡和 / 或类似物），但卡 900 可包括任何类型的出入卡（包含（例如）大楼出入卡、滑雪通行卡和 / 或类似物）。

[0134] 交通管理局可希望结合其收费系统来使用交通卡 900。结合收费交易，交通管理局

可希望证实：由用户呈现的交通卡900是由交通管理局或另一可信方发行的真实卡，且不是伪造品；交通卡900在物理上存在于交易的终端处；及交通卡900具有活动状态和/或足以支付特定费用的相关联的余额。所公开的系统和方法的实施例可由交通管理局使用以结合收费交易来执行这些动作。

[0135] 根据本文所公开的实施例，交通管理局可在其希望允许用户进行收费交易的位置处分发执行卡证实应用程序902的多个认证装置200。举例来说，可将认证装置200分发在交通管理局的公共汽车、火车车厢、交通枢纽和/或类似物上。因为本文所公开的实施例允许结合安全标签认证和/或存在验证而使用相对低成本的通用标签认证装置200(例如，智能电话或平板计算装置)，所以根据所公开的实施例，交通管理局可按通常比常规收费交易系统低的成本实施收费交易。

[0136] 为了起始收费交易，用户可将包含具备秘密信息104的安全标签100的交通卡900呈现给位于附近的认证装置200。在一些实施例中，卡证实应用程序902可使用标签认证装置200来执行轮询或其它过程，以检测包含安全标签100的位于附近的交通卡900。当卡证实应用程序902检测到包含安全标签100的位于附近的交通卡900时，卡证实应用程序902可产生请求交通卡904的证实的卡证实请求904，且将卡证实请求904传达给可信机构102。

[0137] 根据本文所公开的标签认证过程，与交通管理局相关联的可信机构102可产生挑战信息208，且将挑战信息208传达给交通卡900中所包含的安全标签100(例如，经由认证装置200)。在其它实施例中，挑战信息208可由认证装置200产生，且传达给交通卡900和可信机构102。安全标签100可产生挑战响应906，挑战响应906可包含由安全标签100使用挑战信息208和安全标签100所存储的秘密信息104而执行的计算(例如，散列计算等)的结果。挑战响应906可进一步包含与交通卡900和/或安全标签100相关联的识别符。挑战响应906可被传达给认证装置200且可被转发给可信机构102以进行认证。

[0138] 可信机构102可比较挑战响应906中所包含的结果与可信机构102使用标签认证模块214基于挑战信息208和存储在数据库908中的可信机构102所拥有的秘密信息而执行的类似计算的结果。在一些实施例中，与特定安全标签100相关联的存储在数据库908中的秘密信息可由可信机构102使用包含在挑战信息906中的与交通卡900和/或安全标签100相关联的识别符来识别。如果挑战响应906中所包含的结果匹配由可信机构产生的结果，那么可信机构102可确定安全标签100是由可信机构102提供的真实标签，且因此相关联的交通卡900是真实的且不是伪造品。如果结果不匹配，那么可信机构102可确定安全标签100不是由可信机构102提供的真实标签，且因此，相关联的交通卡900是不真实的。

[0139] 如果确定交通卡900不真实，那么可信机构102可将指示卡900不真实的卡证实响应916传达给认证装置200。在其它实施例中，一个或更多个其它方(例如，执法官员等)可被通知交通卡900由可信机构102识别为不真实，因而，确定可为伪造活动的指示。

[0140] 如果确定交通卡900是真实的，那么可信机构102和/或另一系统可结合收费交易而确定交通卡900是否与具有活动状态(例如，如所管理的卡状态数据库912等中所识别)的账户相关联，从而允许卡900的持有者进入交通系统。在其它实施例中，可信机构102和/或另一系统可结合收费交易而确定与交通卡900相关联的账户是否具有足以用于特定费用的余额(例如，如所管理的卡储值数据库914中所反映)。交通卡900的用户可与

可信机构 102 交互以通过对与交通卡 900 相关联的账户投入资金（例如，经由由可信机构、相关服务提供商（例如，交通管理局）和 / 或类似物提供的网站接口）而管理其卡状态和 / 或卡储值。

[0141] 如果可信机构 102 确定与交通卡 900 相关联的账户具有足够余额和 / 或活动状态，那么发送到认证装置 200 的卡证实响应 916 可包含收费交易成功的指示。如果可信机构 102 确定与交通卡 900 相关联的账户具有不足余额和 / 或非活动状态，那么发送到认证装置 200 的卡证实响应 916 可包含收费交易不成功的指示。可在装置 200 上向认证装置 200 的用户呈现所接收的卡证实响应 916 的内容的指示（例如，“卡有效”等）。

[0142] 与交通卡 900 相关联的状态和 / 或账户余额可由可信机构 102 根据收费交易来更新。举例来说，与交通卡 900 相关联的账户可被计入借方等。类似地，与交通卡 900 相关联的状态可结合收费交易来改变。

[0143] 在一些实施例中，可信机构 102 在卡元数据数据库 910 中存储的与交通卡 900 相关联的元数据可包含在由可信机构 102 传达到认证装置 200 的卡证实响应 916 中。举例来说，与交通卡相关联的用户的照片、密码和 / 或其它联系人信息可结合卡确定响应 916 由可信机构 102 传输到认证装置 200。卡元数据尤其可由认证装置 200 的用户用于不仅确定交通卡 900 是具有足够账户余额和 / 或有效的相关联的状态的真实卡，而且结合收费交易确定呈现交通卡 900 的个人被授权使用和 / 或以其它方式与所述卡相关联。

[0144] 重放攻击的减轻

[0145] 图 10 说明根据本发明的实施例的可减轻重放攻击的安全标签认证过程。在所说明的实施例中，可信机构 102 可结合认证装置 200 和商店服务 1000 来使用，以使用本文所公开的标签认证过程的实施例来认证安全标签 100。虽然被说明为单独系统，但应了解，在其它实施例中，认证装置 200、可信机构 102 和 / 或商店服务 1000 的某些功能可由单一系统和 / 或系统的任何适当组合执行。

[0146] 可信机构 102 和 / 或另一可信服务可向安全标签 100 提供秘密信息。在认证装置 200（例如，与商店或其它零售店相关联的认证装置）上执行的标签认证应用程序可按任何适当方式检测位于附近的安全标签 100。

[0147] 在检测到位于附近的安全标签 100 时，服务应用程序（例如，与商店相关联的服务）可在认证装置 200 上启动。在一些实施例中，服务应用程序可登录到由商店服务 1000 提供的远程服务。商店服务 1000 可产生挑战信息，且经由认证装置 200 而将挑战信息传达给安全标签 100。在某些实施例中，挑战信息可包括随机和 / 或伪随机地产生的值，例如，密码随机数，但其它类型的挑战信息也可结合所公开的系统和方法来使用。在其它实施例中，挑战信息可由可信机构 102 和 / 或认证装置 200 产生，且传达给安全标签 100。

[0148] 在接收到挑战信息之后，安全标签可至少部分基于由安全标签存储的秘密信息而产生 MAC 和 / 或其它计算结果。在其它实施例中，MAC 可进一步基于其它数据而产生。MAC、标签识别信息、挑战信息和 / 或其它数据可从安全标签 100 传达给位于附近的认证装置 200，位于附近的认证装置 200 又可将所述信息传达给可信机构 102。

[0149] 可信机构 102 可基于所接收的信息（例如，标签 ID、随机数、MAC 等）而执行根据本文所公开的实施例的标签认证过程。举例来说，可信机构 102 可基于所接收的标签识别信息而检索与安全标签 100 相关联的安全密钥。所检索的安全密钥可结合基于安全密钥以

及挑战信息和/或从认证装置200接收的其它信息计算MAC和/或其它计算结果来使用。一旦计算出，可信机构102可比较所计算的MAC与安全标签100所产生的从认证装置200接收的MAC。如果两个MAC值匹配，那么可信机构102可将指示安全标签100是真实的且位于认证装置200附近的认证结果（例如，状态）传回到认证装置200。如果两个MAC值不匹配，那么可信机构102可将指示安全标签100不真实的认证结果（例如，状态）传回到认证装置200。

[0150] 在某些实施例中，除状态（例如，“真实”或“不真实”）之外，传回到认证装置200的认证结果可进一步包含由可信服务102签名的挑战信息、认证时间和标签识别信息。认证装置200可将带签名的挑战信息、认证时间和标签识别信息转发给商店服务1000。在某些实施例中，商店服务1000可奖励忠诚点和/或执行与安全标签100的成功认证的任何其它功能。

[0151] 商店服务1000可检查认证时间处于特定时段内。也就是说，商店服务1000可检查带签名的认证时间是“新近的”。商店服务1000可还检查带签名的挑战信息的“新近性”以确定带签名的挑战信息是在特定时间段内发出。如果这些值不处于特定时间段内（即，不新近），那么商店服务1000可确定其不应奖励忠诚点或执行与安全标签100的认证相关联的其它功能，这是因为带签名的认证时间和/或挑战信息的年龄段可指示可能的重放攻击。在某些实施例中，因为认证时间和/或挑战信息可由可信机构102签名，所以此机制可不依赖于认证装置200的安全性，进而提高所公开的实施例防止潜在重放攻击的可能性。

[0152] 标签证实和存在确认服务

[0153] 本文所公开的系统和方法的某些实施例可结合例如消费者对消费者（“C2C”）业务（例如，在线拍卖服务、分类广告服务等）等电子商务服务来使用。举例来说，在在线拍卖服务中，投标人和/或服务可难以确保在在线拍卖服务上出售的产品的真实性，这是因为投标人可仅能够访问卖主选择发布的关于产品的有限信息（例如，图片和/或描述）。根据本文所公开的实施例，安全标签可与产品相关联，进而实现以可信机构和/或其它服务提供商使用安全标签进行的产品的认证。当产品由可信机构认证时，可将指示提供给电子商务服务，进而允许所述服务验证卖主已具有给定产品的实际确实的拥有、确定结合项目从卖主提供的产品信息是否匹配来自制造商的产品信息和/或类似物。

[0154] 图11说明根据本发明的实施例的结合电子商务服务1100的产品证实。在某些实施例中，电子商务服务1100可包括C2C服务，例如，在线拍卖服务、分类广告服务和/或类似物。应了解，各种其它类型的电子商务服务可使用本文所公开的标签认证和/或存在验证过程，且任何适当类型的电子商务或其它服务可实施所公开的实施例。

[0155] 结合使用电子商务服务1100的购买交易，用户可尤其希望：证实由卖主提供以出售的产品500是来自其制造商的真实产品且不是伪造品；确认产品500是新的或先前未作为新的而出售过；获得关于产品500的所有权历史信息和/或类似物。根据本文所公开的实施例，此信息可经由涉及与产品500相关联的安全标签100、认证装置200和/或可信机构102的认证过程来获得。此信息可进一步结合由电子商务服务1100提供的接口1102呈现给预期买主。

[0156] 证实产品500的真实性可使用认证装置200和/或可信机构102来执行，如上文结合图5而详述。举例来说，当卖主希望提供产品500以在由电子商务服务1100管理的在

线拍卖中出售时，用户可选择使用电子商务服务 1100 来证实产品 500 的真实性。在某些实施例中，使用电子商务服务 1100 来证实产品 500 可尤其由于其证实而导致预期买主将更多价值归于产品 500。

[0157] 为了证实产品 500，卖主可使用在认证装置 200（例如，智能电话或平板计算装置）上执行的产品认证应用程序 502。如上所述，利用安全标签 100、认证装置 200 和 / 或可信机构 102 的证实过程可被执行，从而导致证实响应 506 由可信机构 102 发出且传达给认证装置 200。在某些实施例中，证实响应 506 可进一步被传达给电子商务服务 1100。在接收到证实响应 506 之后，电子商务服务 1100 可经由相关联的接口 1102 结合相关联的产品 500 而将证实信息呈现给预期买主。在其它实施例中，证实响应 506 可进一步包含可由电子商务服务 1100 经由接口 1102 而呈现给预期买主的关于产品 500 的额外信息（例如，由可信机构 102 和 / 或另一服务维持的产品元数据 508）。

[0158] 图 12 说明根据本发明的实施例的结合电子商务服务 1100 的另一产品证实过程。在所说明的实施例中，可信机构 102 可结合认证装置 200 和电子商务服务 1100 来使用，以用于使用本文所公开的标签认证过程的实施例来认证包含安全标签的产品。虽然被说明为单独系统，但应了解，在其它实施例中，认证装置 200、可信机构 102 和 / 或电子商务服务 1100 的某些功能可由单一系统和 / 或系统的任何适当组合执行。

[0159] 可信机构 102 和 / 或另一可信服务可向与产品相关联的安全标签 100 提供秘密信息。在与卖主相关联的认证装置 200 上执行的产品证实应用程序（例如，由电子商务服务 1100 提供的应用程序）可根据本文所公开的实施例来检测位于附近的安全标签 100。

[0160] 在检测到位于附近的安全标签 100 之后，应用程序可在可登录到由电子商务服务 1100 提供的服务的装置 200 上启动。电子商务服务 1100 可产生挑战信息，且经由认证装置 200 而将挑战信息传达给安全标签 100。在某些实施例中，挑战信息可包括随机和 / 或伪随机地产生的值，例如，密码随机数，但其它类型的挑战信息也可结合所公开的系统和方法来使用。在其它实施例中，挑战信息可由可信机构 102 和 / 或认证装置 200 产生，且传达给安全标签 100。

[0161] 在接收到挑战信息之后，安全标签 100 可至少部分基于由安全标签存储的秘密信息而产生 MAC、散列和 / 或其它计算结果。在其它实施例中，所述计算可进一步基于其它数据而产生。计算结果、标签识别信息、挑战信息和 / 或其它数据可从安全标签 100 传达给位于附近的认证装置 200，位于附近的认证装置 200 又可将所述信息传达给可信机构 102。

[0162] 可信机构 102 可基于所接收的信息（例如，标签 ID、随机数、MAC 等）而执行根据本文所公开的实施例的标签认证过程。举例来说，可信机构 102 可基于所接收的标签识别信息而检索与安全标签 100 相关联的安全密钥。所检索的安全密钥可结合基于安全密钥以及挑战信息和 / 或从认证装置 200 接收的其它信息计算 MAC、散列和 / 或其它计算结果来使用。一旦计算出，可信机构 102 可比较所计算的结果与从认证装置 200 接收且由安全标签 100 产生的所计算的结果。如果两个值匹配，那么可信机构 102 可将指示安全标签 100 是真实的认证结果（例如，状态）传回到认证装置 200。如果两个值不匹配，那么可信机构 102 可将指示安全标签 100 是不真实的认证结果（例如，状态）传回到认证装置 200。

[0163] 在某些实施例中，除状态（例如，“真实”或“不真实”）之外，传回到认证装置 200 的认证结果可进一步包含由可信服务 102 签名的挑战信息、认证时间和 / 或标签识别信

息。认证装置 200 可将带签名的挑战信息、认证时间和标签识别信息转发给电子商务服务 1100。在一些实施例中，电子商务服务 1100 可进一步检查用于确认卖主曾执行认证的带签名的挑战信息、用于确认卖主何时执行认证的带签名的认证时间和用于确认卖主认证哪一产品的带签名的标签识别信息。在其它实施例中，电子商务服务 1100 可将产品的证实的指示提供给预期买主和 / 或执行与安全标签 100 的成功认证相关联的任何其它功能。

[0164] 评论服务存在确认

[0165] 本文所公开的某些实施例可用于增强结合在线评论服务而发布的特定产品和 / 或企业的个人的评注、意见和 / 或评论的特性。举例来说，如果可认证评论者实际上访问过餐馆，那么个人关于所述餐馆而发布到在线评论服务的评论可被视为比评论服务的用户有价值。类似地，结合产品评论向产品评论服务的用户提供如下指示可为有益的 :产品评论者在其发布评论时实际上拥有所评论的产品。

[0166] 本文所公开的系统和方法的实施例可实现在特定时间特定位置的真实电子标签的存在的安全验证。评论系统的用户可具备卡、智能电话应用程序或其它装置，所有这些包含当结合企业的位置处的认证装置使用时可用于验证用户在所述位置处的存在的安全电子标签和 / 或秘密值。此验证可用于（例如）结合所发布的评论验证企业和 / 或产品评论者实际上访问过企业和 / 或拥有过产品。对评论者在所评论的位置处的存在和 / 或所评论的产品的拥有的验证可提高评论服务的用户区分基于企业和 / 或产品的第一手了解的评论与较不可靠的评论的能力。

[0167] 图 13 说明根据本发明的实施例的结合评论服务 1300 的存在证实。结合产品评论服务 1300，产品评论者 1302 可希望尤其证实他们实际上拥有真实的所评论的产品。类似地，结合企业评论服务 1300，企业评论者 1302 可希望尤其证实他们实际上访问过所评论的企业。本文所公开的安全标签认证技术的实施例可用于结合各种评论服务 1300 确定与评论者相关的产品和 / 或企业的存在证据。

[0168] 证实评论者 1302 拥有真实产品和 / 或在物理上存在于特定企业处可使用认证装置 200 和 / 或可信机构 102 使用本文所公开的安全标签授权和 / 或存在验证技术来执行。举例来说，当评论者 1302 希望结合评论 1304 来验证他们实际上访问过餐馆时，评论者可选择使用可信机构 102 来证实他们在餐馆处的存在。为了证实他们的存在，评论者 1302 可将与评论者 1302 相关联的安全标签 100 呈现给在认证装置 200（例如，位于入口处或附近的装置等）上执行的与餐馆的位置相关联的签到应用程序 1306。如上文结合其它实施例所论述，利用安全标签 100、认证装置 200 和 / 或可信机构 102 的证实过程可被执行，从而导致证实响应 218 由可信机构 102 发出且传达给认证装置 200，从而证实安全标签 100 在装置 200 附近的存在。在一些实施例中，标签可置于餐馆中（例如，密封在餐馆中的餐桌中），且当评论者使用认证装置 200 从可信机构 102 获得标签认证响应 218 时，装置 200 或可信机构 102 可将标签认证响应 218 作为存在证据转发给评论服务 1300。

[0169] 在某些实施例中，认证响应 218 可进一步被传达给评论服务 1300。在接收到认证响应 218 之后，评论服务 1300 可结合所发布的评论 1304 而呈现指示评论者 1302 实际上访问过所评论的餐馆的证实信息（例如，“经过验证的用户评论”等）。应了解，类似实施例可结合产品评论服务 1300 来使用，其中产品评论者 1302 可使用认证装置 200 通过可信机构 102 证实他们拥有所评论的产品，且将此证实传达给产品评论服务 1300 以结合产品的评论

来呈现。

[0170] 如上文所论述，在替代实施例中，评论者 1302 可拥有执行签到应用程序 1306 的认证装置 200。可认证标签 100 可与餐馆的位置相关联（例如，位于入口处或附近，位于餐桌中或餐桌上和 / 或类似物的标签）。评论者 1302 可利用认证装置 200、安全标签 100 和 / 或可信机构 102 来执行证实过程，从而导致证实响应 218 由可信机构 102 发出且传达给用户的认证装置 200，从而证实安全标签 100 在装置 200 附近的存在。此响应 218 可用作评论者 1302 在餐馆的位置处的存在证据。

[0171] 在其它实施例中，响应 218 可从可信机构 102 传达给评论服务 1300。在一些实施例中，响应 218 可从认证装置 200 传达给评论服务 1300。评论服务 1300 可将所接收的响应用作评论者 1302 在餐馆的位置处的存在证据，从而结合所发布的评论 1304 而呈现指示评论者 1302 实际上访问过所评论的餐馆的信息（例如，“经过验证的用户评论”等）。

[0172] 文档签名服务

[0173] 本文所公开的系统和方法可进一步结合可信文档签名服务来使用。在某些权限中，可需要将签名、图章和 / 或印章应用到文档，以使文档具有法律效力。当应用到文档时，签名、图章和 / 或印章可表示包括任何适当字符、图像和 / 或其组合的唯一标记（例如，图形标记）。在某些实施例中，签名、图章和 / 或印章可与组织相关联，且当应用到文档时，表示组织对文档的核准、文档的内容的认证、文档的签名人的权力（例如，代表组织行动的权力）和 / 或类似物。

[0174] 所公开的可信文档签名服务的实施例可尤其确保应用电子签名、图章和 / 或印章的一方有权如此。在某些实施例中，使用所公开的实施例的电子签名、图章和 / 或印章可涉及用户在他们可执行文档之前表明拥有秘密信息。在某些实施例中，秘密信息的拥有可经由表明拥有安全标签或存储秘密信息的其它相关联的项目（例如，物理图章、印章、授权卡等）来表明。通过表明拥有安全标签，用户可使用文档签名服务来认证他们应用电子签名、图章和 / 或印章的授权。

[0175] 图 14 说明根据本发明的实施例的结合文档签名服务 1402 的用户的认证。在某些实施例中，认证可涉及确定用户是否拥有存储在安全标签 100 中的某秘密信息 104，且通过扩展，确定是否被授权以电子方式将签名、图章和 / 或印章应用到文档。在一些实施例中，安全标签 100 可通过用户应用相关联的签名、图章和 / 或印章的权力而包含在用户拥有的物理项目（例如，物理图章、印章 1400、笔、授权卡、移动装置和 / 或类似物）中。应了解，各种其它类型的项目可结合本文所公开的过程来使用，且包含安全标签 100 的任何类型的项目（或，例如，运行安全应用程序的智能电话，所述安全应用程序利用存储在智能电话的存储器中的秘密值）可用于所公开的实施例中。

[0176] 证实用户拥有包含存储所提供的秘密信息 104 的安全标签 100 的印章 1400 可使用实施本文所公开的安全标签授权和 / 或存在验证技术的认证装置 200 和 / 或可信机构 102 来执行。举例来说，当用户希望将电子签名、图章和 / 或印章应用到文档时，用户可选择使用可信机构 102 来证实用户拥有印章 1400。为了证实用户拥有印章 1400，用户可将印章 1400 呈现给在认证装置 200（例如，与用户和 / 或文档签名服务 1402 相关联的装置）上执行的印章认证应用程序 1404。类似于上文结合其它实施例而论述的过程，印章认证请求 1406 可从认证装置 200 传达给可信机构 102，从而起始利用安全标签 100、认证装置 200 和

/或可信机构102的认证过程。认证过程可导致印章认证响应1408由可信机构102发出且传达给认证装置200，从而证实安全标签100在装置200附近的存在。在某些实施例中，印章认证响应1408可进一步作为应用相关联的签名、图章和/或印章的用户授权的证据而传达给文档签名服务1402。

[0177] 图15说明根据本发明的实施例的结合文档签名服务1402的用户认证过程。在与文档签名服务1402交互的过程中，用户可希望尤其通过表明拥有指示此授权的项目（例如，物理印章1400）而认证用户被授权以电子方式将签名、图章和/或印章应用到文档。本文所公开的安全标签认证技术的实施例可用于认证用户拥有此印章1400。

[0178] 认证用户拥有表明他们应用签名、图章和/或印章的授权的物理印章1400可使用利用本文所公开的安全标签授权和/或存在验证技术的物理印章1400、认证装置200和/或可信机构102来执行。虽然被说明为单独系统，但应了解，在其它实施例中，认证装置200、可信机构102和/或文档签名服务1402的某些功能可由单一系统和/或系统的任何适当组合执行。

[0179] 当向文档签名服务1402表明用户应用签名、图章和/或印章的授权时，用户可使用可信机构102来证实他们拥有物理印章1400。可信机构102和/或另一可信服务可向物理印章1400提供包含在安全标签100中的秘密信息104。用户可首先在认证装置200上启动与文档签名服务1402相关联的应用程序（例如，印章认证应用程序）。印章认证应用程序可根据本文所公开的实施例来检测位于附近的安全标签100（例如，响应于轮询过程等）。认证装置200可接着登录到由文档签名服务1402提供的签名服务。

[0180] 文档签名服务1402可将例如密码随机数等挑战信息发出到认证装置200，且可将挑战信息与用户请求认证相关联。或者，认证装置200、可信服务102和/或另一可信服务可产生挑战信息。认证装置200可将挑战信息传达给安全标签100，作为相应，安全标签100可传回基于挑战信息而计算的标签识别符和MAC。认证装置200可接着将标签识别符、MAC和挑战信息发送给可信机构102。使用此信息，可信机构102可使用所接收的标签识别符和挑战信息而导出MAC。

[0181] 如果传达给可信机构102和由可信机构102导出的MAC匹配，那么可信机构102可将匹配的证据传回到认证装置200。在某些实施例中，此证据可包括带签名的数据，包含挑战信息、标签识别符和时戳。认证装置200可将此证据转发给文档签名服务1402。文档签名服务1402可验证证据的签名以进行认证。文档签名服务1402可使用标签识别以检索签名、图章和/或印章数据以供所认证的用户使用。在某些实施例中，所应用的签名、图章和/或印章可与所传回的时戳所指示的日期和/或时间相关联。

[0182] 基于装置的安全电子标签

[0183] 在某些实施例中，安全标签可为基于装置的和/或另外集成到任何适当装置中，包含本文所公开的装置中的任一者。基于装置的标签可用于各种情形中。举例来说，安保公司可使用基于装置的安全标签来确认安保人员巡逻访问某些指定检查点。所述公司可将认证装置置于巡逻检查点处，且安保人员可使用基于装置的安全电子标签而在每一巡逻检查点处提供存在证据。安保公司可将此存在证据用作安保巡逻的记录。

[0184] 类似地，公司可希望管理进出工作场所的员工。所述公司可将认证装置置于签到点处，且员工可使用基于装置的安全电子标签而提供其签进和签出工作场所的存在证据。

所述公司可将此存在证据用作每一员工工作时间的记录。虽然结合基于装置的安全电子标签来论述，但应了解，前述实例还可使用本文所公开的任何其它类型的标签（例如，基于卡的标签、非安全标签等）。

[0185] 图 16 说明根据本发明的实施例的基于装置的安全标签的初始化过程。在某些实施例中，可向 BLE 装置 1602（例如，智能电话等）和 / 或任何其它适当装置提供安全嵌入的秘密信息（例如，唯一密钥）。在某些实施例中，所述信息可经由安全硬件、软件和 / 或其组合而安全嵌入到 BLE 装置 1602 中。在一些实施例中，提供可由初始化装置 1600 初始化，初始化装置 1600 可向 BLE 装置 1602 提供唯一密钥。与 BLE 装置 1602 相关联的唯一密钥和 / 或识别信息可被分发到可信机构 102，可信机构 102 被配置成执行根据所公开的实施例的安全标签认证和 / 或存在验证过程。应了解，可对所说明的初始化过程进行许多变化。举例来说，在一些实施例中，BLE 装置 1602 可由可信机构 102 初始化，而不使用离散的初始化装置 1600。

[0186] 图 17 说明根据本发明的实施例的基于装置的安全标签的认证过程。如上文所论述，在某些实施例中，基于装置的安全标签可使用所提供的 BLE 装置 1602 来实施。在某些实施例中，所说明的认证过程可用于使用可信机构 102 而在与认证装置 200 相关联的物理位置处验证 BLE 装置 1602 的存在。如果经过验证，那么 BLE 装置 1602 的存在证据可传达给利用存在验证实施服务的应用程序服务 1700。虽然被说明为单独系统，但应了解，在其它实施例中，BLE 装置 1602、认证装置 200、可信机构 102 和 / 或应用程序服务 1700 的某些功能可由单一系统和 / 或系统的任何适当组合执行。

[0187] 认证装置 200 可参与 BLE 装置发现过程以定位附近的 BLE 装置 1602。在检测到位于附近的 BLE 装置 1602 之后，认证装置 200 可产生挑战信息（例如，随机数）且将其传达给 BLE 装置 1602。在某些实施例中，挑战信息可包括随机和 / 或伪随机地产生的值，例如，密码随机数，但其它类型的挑战信息也可结合所公开的系统和方法来使用。在其它实施例中，挑战信息可由可信机构 102 产生，且传达给 BLE 装置 1602。

[0188] 在接收到挑战信息之后，BLE 装置 1602 可至少部分基于由 BLE 装置 1602 存储的所提供的秘密信息而产生 MAC 和 / 或其它计算结果。在其它实施例中，MAC 可进一步基于其它数据而产生。与 BLE 装置 1602 相关联的 MAC 和识别信息可传达给认证装置 200。认证装置 200 可转而将此信息与发出到 BLE 装置 1602 的挑战信息一起传达给可信机构 102。

[0189] 可信机构 102 可基于所接收的信息（即，装置 ID、随机数、MAC 等）而执行根据本文所公开的实施例的标签认证过程。举例来说，可信机构可基于所接收的装置识别信息而检索可信机构拥有的与 BLE 装置 1602 相关联的安全密钥。所检索的秘密信息可结合基于秘密信息以及挑战信息和 / 或从认证装置 200 接收的其它信息计算 MAC 和 / 或其它计算结果来使用。一旦计算出，可信机构 102 可比较所计算的 MAC 与 BLE 装置 1602 所产生的从认证装置 200 接收的 MAC。如果两个 MAC 值匹配，那么可信机构 102 可传回认证 BLE 装置在认证装置 200 处的存在的存在证据。如果两个 MAC 值不匹配，那么可信机构 102 将不传回存在证据。在某些实施例中，存在证据可从可信机构 102 和 / 或认证装置 200 传达给应用程序服务 1700，应用程序服务 1700 可结合各种基于存在验证的服务来使用所述信息。

[0190] 用户认证过程

[0191] 在某些实施例中，除本文所公开的安全标签认证技术之外，还可使用用户认证技

术。举例来说，除所公开的安全标签认证技术之外，还可使用用户名和 / 或密码认证、生物计量认证、个人识别号认证和 / 或任何其它适当类型的使用过的认证技术。在某些实施例中，实施除安全标签认证之外的用户认证可有助于确定不仅安全标签是由可信机构提供的真实安全标签，而且确定结合安全交易而呈现安全标签的个人被授权使用安全标签和 / 或以其它方式与安全标签相关联。

[0192] 在某些实施例中，用户认证可为主动的，其中安全标签的用户可通过表明知晓和 / 或拥有某秘密信息（例如，唯一密码、识别号和 / 或生物计量信息）而使用可信机构和 / 或其它服务来认证他们的身份。在一些实施例中，此信息可结合安全标签认证过程和 / 或与交易相关联的一个或更多个其它装置和 / 或服务而提供给认证装置。在其它实施例中，用户认证可为被动的，其中信息可结合安全标签认证过程而提供给认证装置，所述安全标签认证过程可由装置的用户使用以确认呈现安全标签的个人与所述安全标签相关联。举例来说，与井认证的安全标签的授权用户相关联的照片和 / 或其它个人信息（例如，高度、重量，发色等）可显示在认证装置上。认证装置的用户可使用此信息以确认结合交易而呈现安全标签的人与相关联的信息匹配。

[0193] 在某些实施例中，用户认证可使用认证装置来执行。在其它实施例中，一个或更多个其它系统可结合用户认证来使用，包含（不限于）可信机构和 / 或一个或更多个其它可信服务。

[0194] 个性化广告和信息服务

[0195] 在其它实施例中，所公开的安全标签认证技术可用于促进消费型产品推销和品牌管理。本文所公开的实施例可允许用户使用认证装置来认证产品中所包含的安全标签，且接收关于产品的有用信息。这些实施例可向消费者提供产品真实性的保证，以及来自可信源的丰富的产品信息。

[0196] 某些技术（包含‘406 申请案、‘538 申请案和‘750 申请案中所述的技术）可结合所公开的实施例来使用以向产品推销员和品牌管理员提供如下保证：正当的消费者在隐私保护下接收到其信息（例如，定向到其个人简档），且他们将能够检索关于购买其产品和 / 或考虑购买其产品的消费者的特性的详细且及时的分析报告。品牌管理员还可了解真实性的保证、伪造品和 / 或失窃项目的检测、经由未被授权的渠道（例如，根据位置报告）而进行的出售的识别，和 / 或可由所公开的系统和方法提供的售后支持和 / 或销售的产品登记。

[0197] 所公开的系统和方法的实施例可与可信机构一起经由使用可从消费者的移动装置读取的低廉的安全标签而提供前述能力，如此确保：品牌和消息未被他人截获；适用于给定消费者的消息被提供；及适用于零售商（例如，商店职员、出售人员等）的消息被提供给这些方，而不是消费者。根据本文所公开的实施例的可信服务可帮助阻止伪造品和 / 或通过位置来识别未被授权的销售渠道。

[0198] 某些实施例可允许将丰富的反向渠道信息提供给产品管理员，而不侵犯消费者隐私。举例来说，所公开的系统和方法可经由分销链而实现产品的跟踪和 / 或追查。这可尤其向消费者提供关于产品的真实性和伪造产品及其位置的检测的保证（进而阻碍伪造）、促进失窃产品的检测和 / 或定位、通过地理学、人口统计学和 / 或消费者权益而实现消费者出售的便利的隐私保护的跟踪、在出售点提供隐私受保护的客户承诺，和 / 或促进隐私受保护的售后支持和定向。

[0199] 当安全标签被认证时，可将信息提供给消费者和/或零售商。举例来说，当使用消费者认证装置的个人认证安全标签时，可提供消费者导向信息。此信息可与消费者的个人特征匹配和/或通过消费者的个人特征来区分优先级，而不侵犯消费者的隐私。在一些实施例中，信息可呈各种格式，包含（不限于）视频、音频、文字等。

[0200] 举例来说，当使用零售商认证装置的零售商认证安全标签时，可提供零售商导向信息。零售商信息可包含关于产品的零售商特定信息，例如，可让消费者迷惑或不知所措但可在产品的出售中帮助零售商的信息。类似地，更具体的信息可被提供给具有认证安全标签的特殊需要和/或要求的用户。举例来说，具有特殊需要的消费者、合法地转售使用过的项目的个人、执行库存的店员和/或类似物可在他们认证安全标签时被提供关于其需要的具体信息。

[0201] 在某些实施例中，可使用确保适当信息在特定情形下被提供给正当的人的可信基础结构。在某些实施例中，所述基础结构可为可缩放的且有效的，从而支持各种装置和/或应用。这尤其可确保使用在认证装置上执行的适当授权的应用程序的消费者可进入任何零售渠道、使用他们的装置来认证包含安全标签的产品，且从可信源可靠地接收真实性和产品信息。此外，产品制造商可保证：消费者将接收到关于其产品的正当消息和/或信息；关于消费者与他们的产品的交互而收集的信息由被授权实体传达和访问。

[0202] 在一些实施例中，可提供互操作性，进而实现在各种品牌和/或产品之间的成本的分布，且确保消费者可仅依赖于一个或几个被授权应用程序，而不是从用于不同零售商和/或产品的许多应用程序中选择。在其它实施例中，本文所述的系统和方法可被部署成支持单一品牌、产品、企业或服务，或支持其闭合子集。在一些实施例中，可提供登记机构，所述登记机构确保拥有和/或控制品牌的那些人是被授权提供关于品牌产品的信息的仅有的人。

[0203] 作为具有品牌产品的公司可如何实施所公开的系统和方法的实施例的实例，公司可首先识别兼容的安全标签供应商（例如，经由可信机构等）。公司可向可信机构登记，从而提供相关联系人信息、品牌信息和/或类似物。公司可从供应商获得安全标签且将所述安全标签与他们的产品相关联（例如，通过将所述安全标签集成到其产品和/或其产品包装中）。公司可将每一产品的标签信息（例如，如果产品是系列化的，则为系列化标签识别信息）上传到可信机构。此外，公司可上传产品信息和/或媒体或产品信息的链接，以提供给消费者、零售商和/或安全地认证与他们的产品相关联的标签的其它方。在某些实施例中，公司可基于消费者属性、零售环境、位置等来指定如何显示此信息。

[0204] 在实施之后，公司可登录到可信机构以管理他们的信息（例如，经由仪表板等）。公司可查看与其产品相关的各种信息。举例来说，公司可查看关于消费者与公司的产品的交互的报告（例如，实时报告）（例如，消费者简档、购买/忽视比率，位置信息等），且可收集消费者登记、评注和/或类似物。公司可访问由可信机构提供的诈骗管理服务以获得关于可能的伪造、未经许可的产品分销、未被授权的出售的位置和/或类似物的信息。

[0205] 消费者可按各种方式与根据本文所公开的实施例的具备安全标签的产品交互。举例来说，消费者可能够将购物应用程序下载到他们的移动装置，以收集且观看关于包含他们认证的安全标签的任何产品的信息。通过认证安全标签，消费者可接收到产品真实性和/或关于产品的个性化信息的保证。在一些实施例中，消费者可能够将关于产品的信息和/

或备忘录存储在他们的移动装置上。

[0206] 如果消费者决定购买具备安全标签的产品，那么消费者可使用所公开的系统和方法向可信机构登记他们的购买，和/或接收与产品相关的额外信息（例如，质保信息、附加信息、用户指南等）。消费者可选择与产品制造商所提供的产品网站交互。在某些实施例中，购物应用程序可维持与消费者的购买相关的信息，且稍后如果消费者需要辅助或想要购买额外货物和/或服务，就将消费者连接到适当的资源。在某些实施例中，消费者的此财产目录可尤其用于保险目的、重获失窃的货物，和/或导出偏好干扰和/或属性以较好地提供个性化产品匹配和/或推荐服务。

[0207] 系统和装置架构

[0208] 图18说明可用于实施根据本发明的系统和方法的某些实施例的系统1800。系统1800可包括被配置成实施本文所述的系统和方法的蜂窝式电话、PDA、智能电话、便携式音频或视频播放器、平板计算机系统、服务器计算机系统和/或任何其它系统。在某些实施例中，系统1800可执行与本文所公开的认证装置、可信机构和/或另一相关服务相关联的某些功能。

[0209] 如图18中所说明，系统1800可包含：处理器1802；系统存储器1804，其可包含用于存储由处理器1802使用和执行的程序和其它数据的高速RAM、非易失性存储器和/或一个或更多个大容量非易失性计算机可读存储介质（例如，硬盘、快闪存储器等）；接口1816（例如，输入/输出接口），其可包含显示器和/或一个或更多个输入装置，例如，触摸屏、键盘、鼠标、触控板等；端口1806，其用于与可装卸存储器1808介接，可装卸存储器1808可包含一个或更多个磁盘、光学存储介质和/或其它计算机可读存储介质（例如，快闪存储器、拇指驱动器、USB适配器、压缩盘、DVD等）；网络接口1810，其用于使用一种或更多种通信技术经由网络1812而与其它系统通信；一个或更多个传感器1818，其可包括包含本文所公开的传感器系统中的任一者的一个或更多个位置传感器、安全电子标签传感器和/或任何其它传感器系统；以及一个或更多个总线1832，其用于通信地耦合前述元件。

[0210] 在某些实施例中，网络1832可包括利用一种或更多种电子通信技术和/或标准（例如，以太网等）的因特网、局域网、虚拟专用网和/或任何其它通信网络。在一些实施例中，网络接口1810和/或网络1832可为无线载波系统（例如，PCS）和/或并有任何适当的通信标准和/或协议的任何其它适当通信系统的一部分。在其它实施例中，网络接口1810和/或网络1832可为模拟移动通信网络和/或数字移动通信网络的一部分，其利用（例如）CDMA、GSM、FDMA和/或TDMA标准。在又其它实施例中，网络接口1810和/或网络1832可并有一个或更多个卫星通信链路和/或使用IEEE 802.11标准、近场通信、Bluetooth®、UWB、Zigbee®和/或任何其它一种或更多种适当的标准。

[0211] 在一些实施例中，替代地或另外，系统1800可包含SPU 1814，SPU 1814由系统1800的用户或其它实体通过利用安全的物理和/或虚拟的安全性技术而受到保护而不会篡改。SPU 1814可帮助增强和/或促进敏感操作（例如，秘密或其它安全信息的私人管理）以及本文所公开的系统和方法的其它方面的安全性。在某些实施例中，SPU 1814可在逻辑上安全的处理域中操作，且被配置成保护秘密信息且对秘密信息操作。在一些实施例中，SPU 1814可包含内部存储器，所述内部存储器存储被配置成使SPU1814能够执行安全操作

的可执行指令或程序。

[0212] 系统 1800 的操作可总体上由处理器 1802 控制，处理器 1802 通过执行存储在系统存储器 1804（和 / 或其它计算机可读介质，例如，可装卸存储器 1808）中的软件指令和程序来操作。系统存储器 1804 可存储用于控制系统 1800 的操作的各种可执行程序或模块。举例来说，系统存储器 1804 可包含 :操作系统（“OS”）1820，其可至少部分管理和协调系统硬件资源并提供用于各种应用程序的执行的公共服务 ;以及信任和隐私管理系统 1822，其用于实施包含对秘密信息的保护和 / 或管理的信任和隐私管理功能性。系统存储器 1804 可进一步包含（不限于）:通信软件 1824，其被配置成部分实现与系统 1800 的通信和系统 1800 进行的通信 ;应用程序 1826（例如，标签和 / 或产品证实应用程序）;标签认证模块 1828 ;挑战产生器 1830 ;和 / 或被配置成实施本文所公开的系统和方法的实施例的任何其它信息和 / 或应用程序。

[0213] 所属领域的技术人员应了解，本文所述的系统和方法可通过与图 18 中所说明的计算装置类似或等同的计算装置或实际上通过任何其它适当的计算装置（包含不拥有图 18 所示的组件中的一些的计算装置和 / 或拥有未示出的其它组件的计算装置）来实践。因此，应了解，是出于说明的目的而不是出于限制的目的而提供图 18。

[0214] 本文所公开的系统和方法不与任何特定计算机、电子控制单元或其它设备固有地相关，且可通过硬件、软件和 / 或固件的适当组合来实施。软件实施方案可包含一个或更多个计算机程序，所述计算机程序包括可执行代码 / 指令，所述可执行代码 / 指令在由处理器执行时可使处理器执行至少部分由可执行指令界定的方法。计算机程序可用任何形式的编程语言（包含编译或解译语言）来编写，且可按任何形式部署，包含部署为独立程序或部署为适用于计算环境中的模块、组件、子例程或其它单元。此外，计算机程序可被部署成在一个场所处的一个计算机或多个计算机上执行或跨越多个场所而分布且由通信网络互连。软件实施例可实施为包括非暂时性存储介质的计算机程序产品，所述非暂时性存储介质被配置成存储计算机程序和指令，所述计算机程序和指令在由处理器执行时被配置成使处理器根据指令而执行一种方法。在某些实施例中，非暂时性存储介质可采用能够在非暂时性存储介质上存储处理器可读指令的任何形式。非暂时性存储介质可通过压缩盘、数字视频盘、磁带、磁盘、快闪存储器、集成电路或任何其它非暂时性数字处理设备存储器装置来体现。

[0215] 虽然已为了清楚起见而有点详细地描述了前述内容，但应明白，可进行某些改变和修改，而不偏离其原理。应注意，存在实施本文所述的系统和方法两者的许多替代方式。因此，本发明的实施例将被视为说明性的，而不是限制性的，且本发明不限于本文给出的细节，而是可在随附权利要求书的范围和等同物内修改。

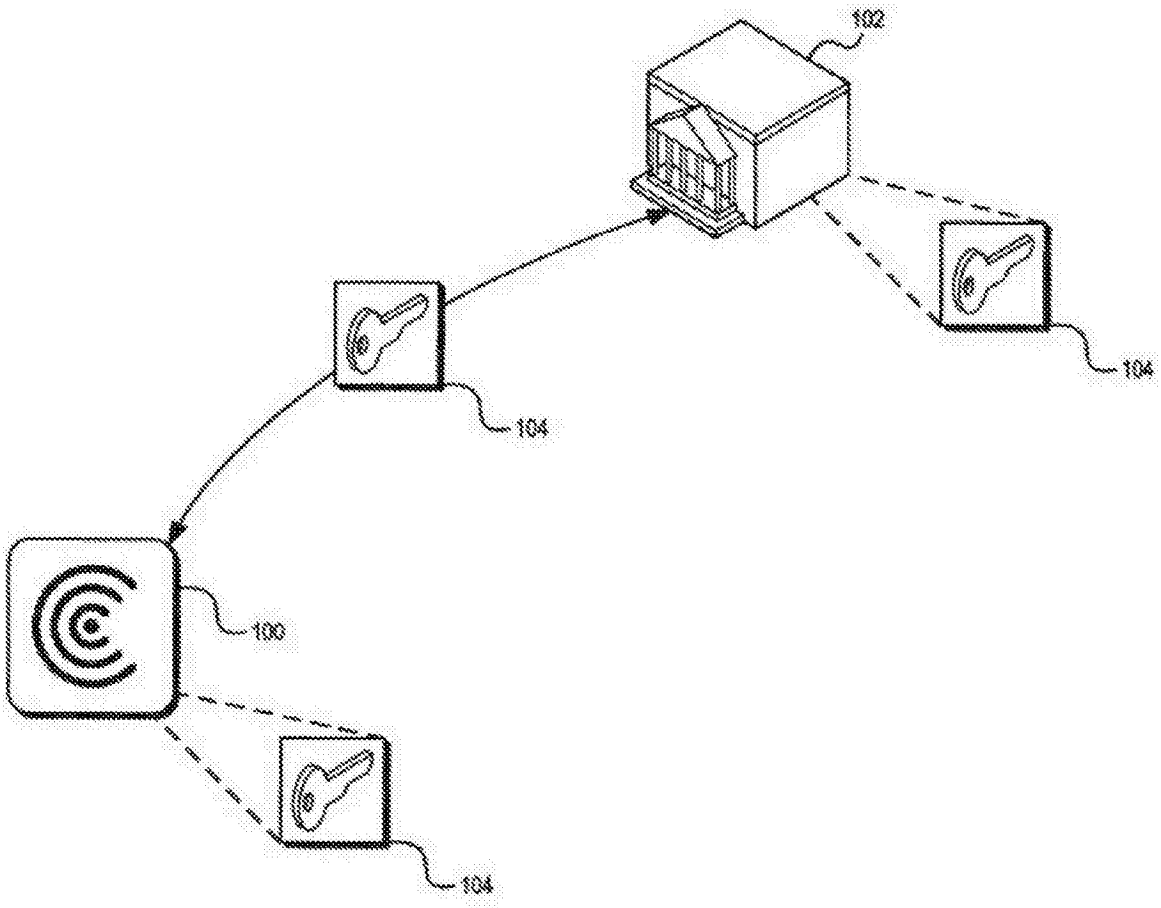


图 1

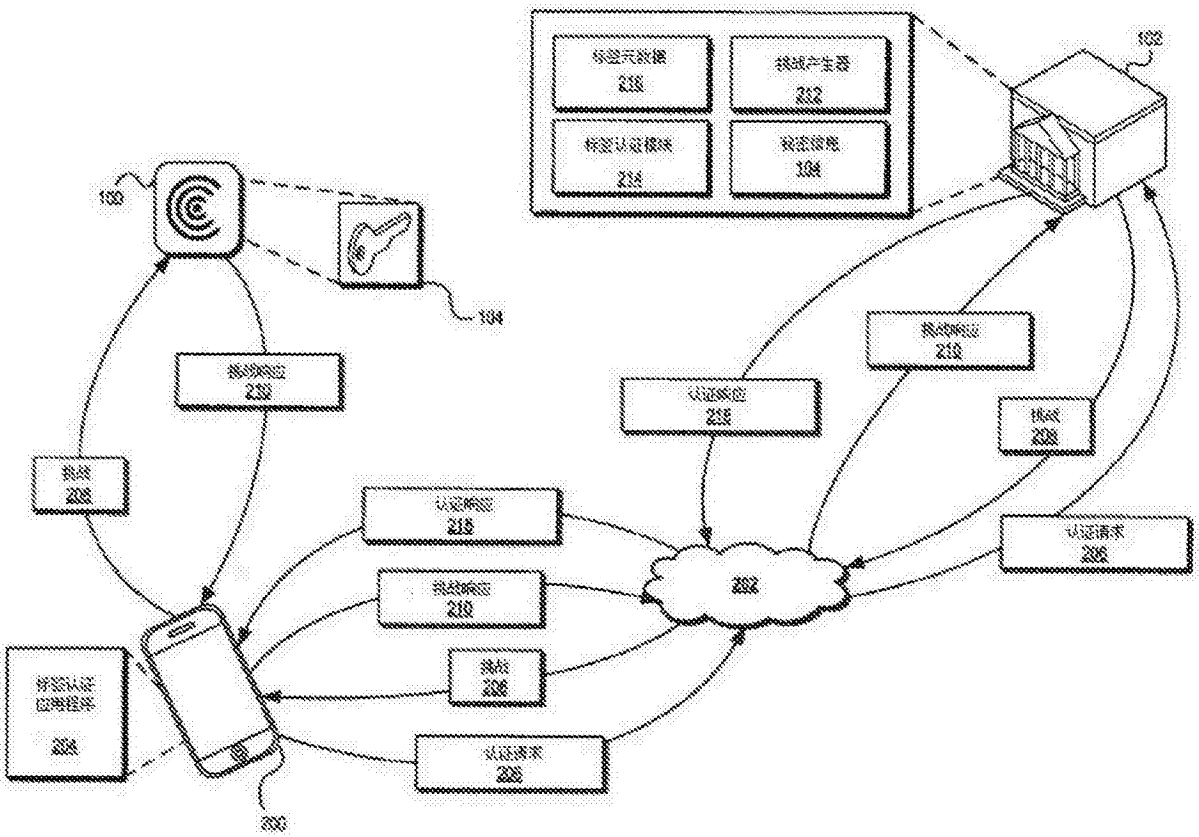


图 2

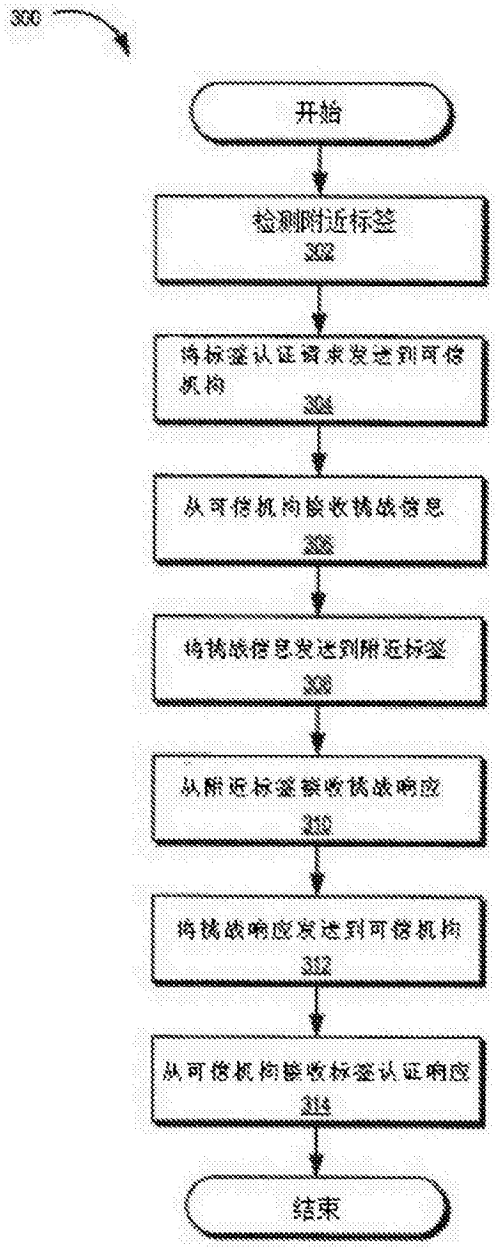

300
开始
检测附近标签
302
将标签认证请求发送到可信机构
304
从可信机构接收挑战信息
306
将挑战信息发送到附近标签
308
从附近标签接收挑战响应
310
将挑战响应发送到可信机构
312
从可信机构接收标签认证响应
314
结束

图 3

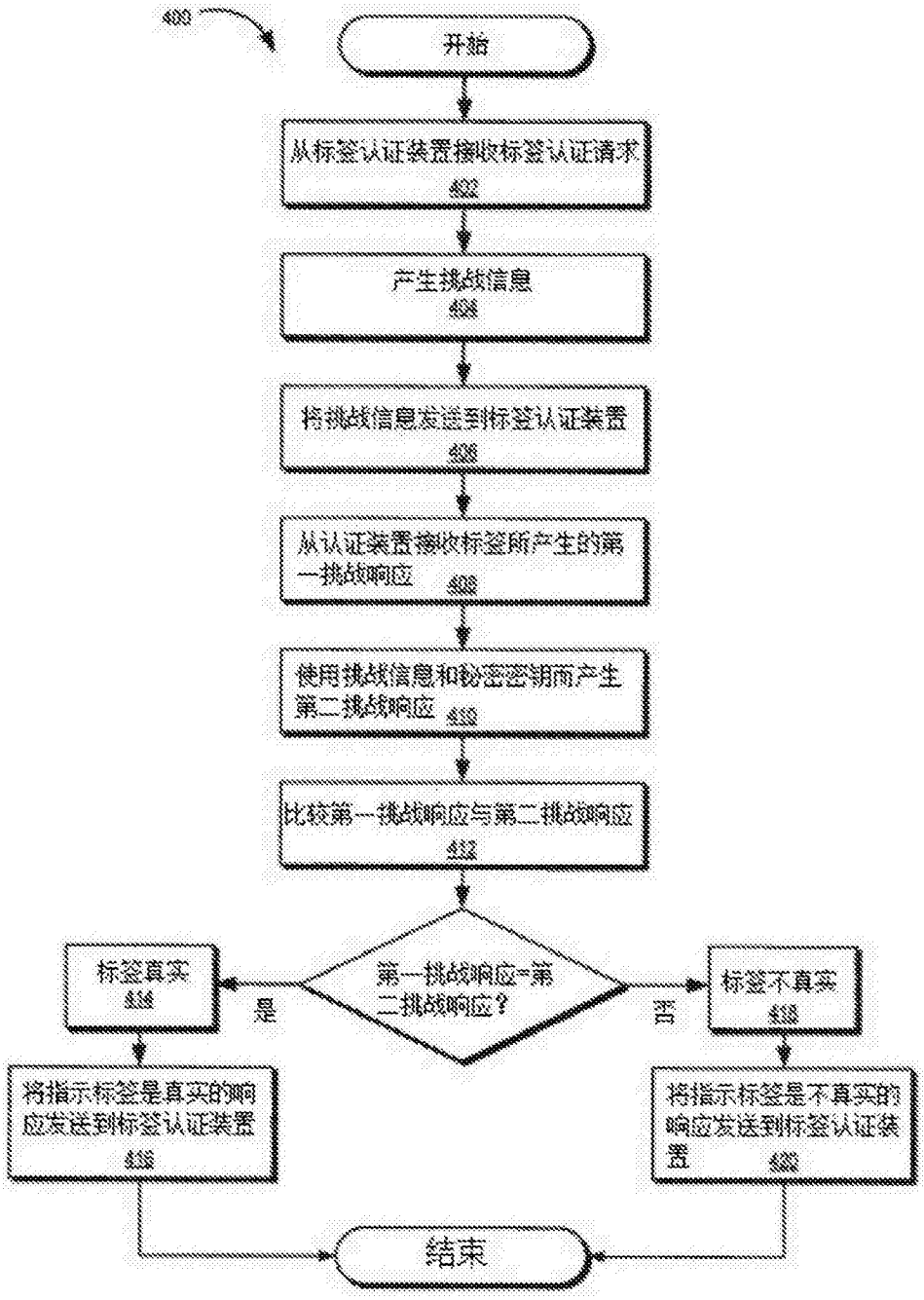

400
开始
从标签认证装置接收标签认证请求
402
产生挑战信息
404
将挑战信息发送到标签认证装置
406
从认证装置接收标签所产生的第一挑战响应
408
使用挑战信息和秘密密钥而产生第二挑战响应
410
比较第一挑战响应与第二挑战响应
412
第一挑战响应=第二挑战响应？
是
否
标签真实
414
标签不真实
416
将指示标签是真实的响应发送到标签认证装置
418
将指示标签是不真实的响应发送到标签认证装置
420
结束

图 4

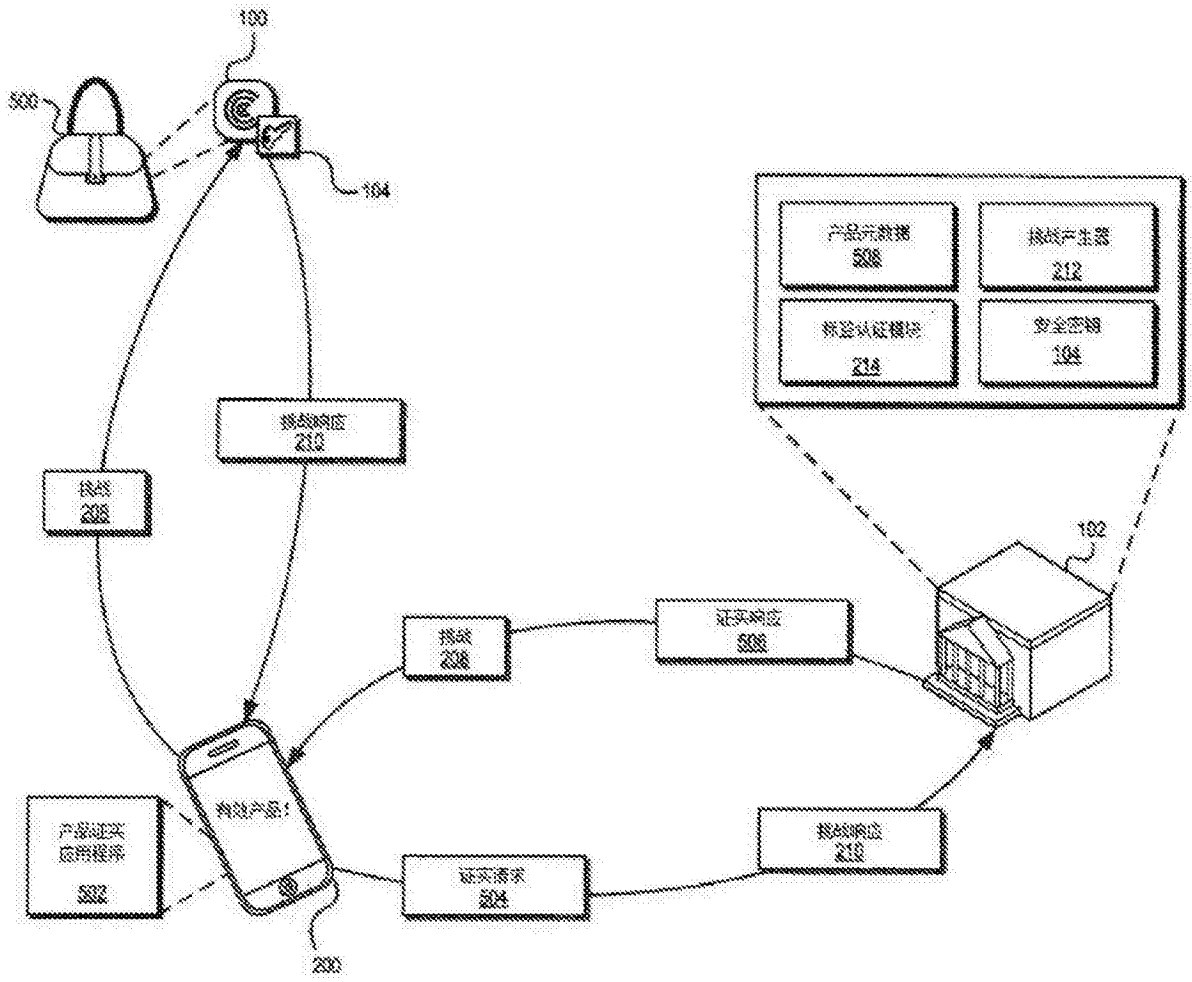


图 5

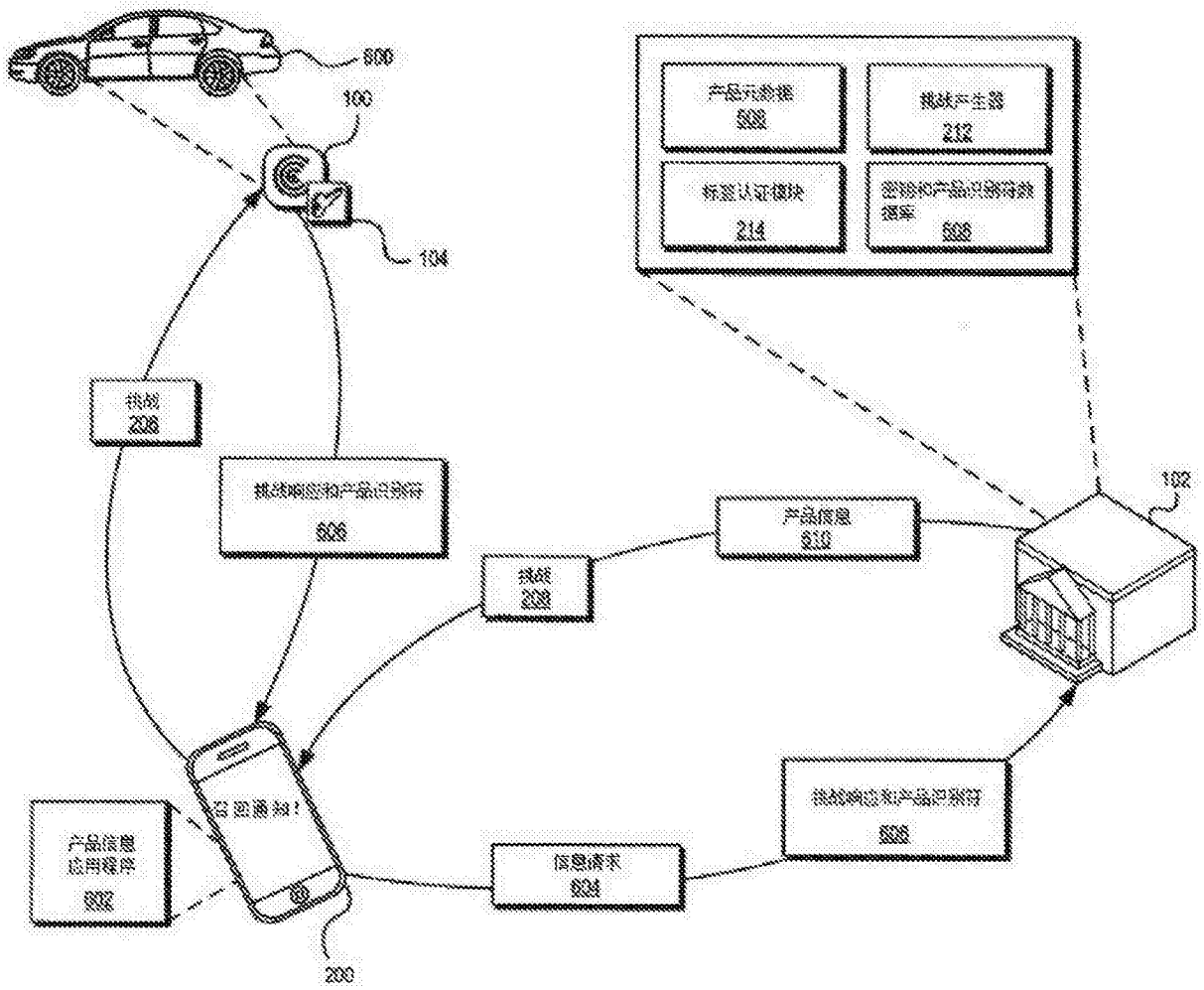


图 6

图 7A

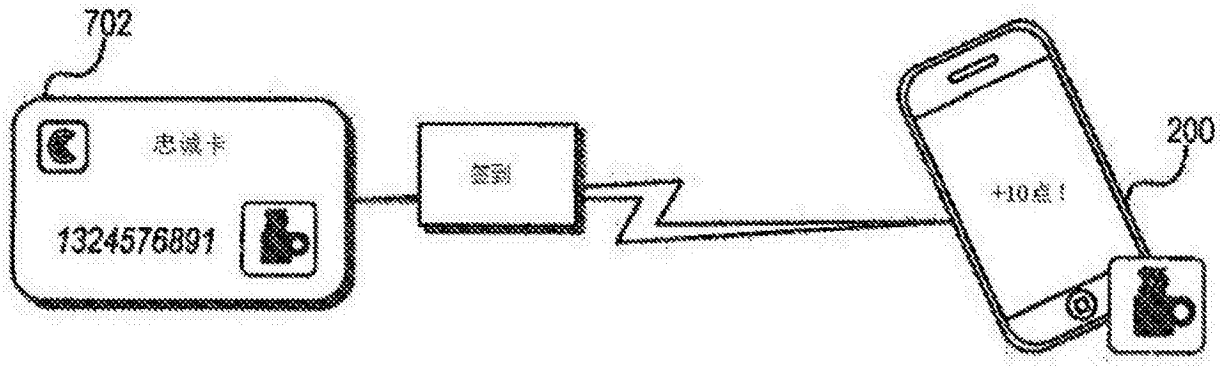

702
忠诚卡
1324576891
签到
+10点！
200

图 7B

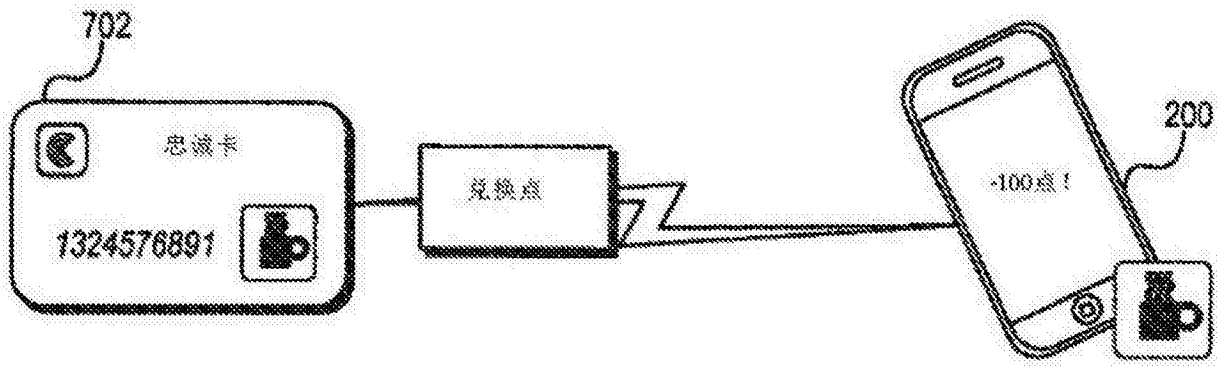

702
忠诚卡
1324576891
兑换点
+100点！
200

图 7C

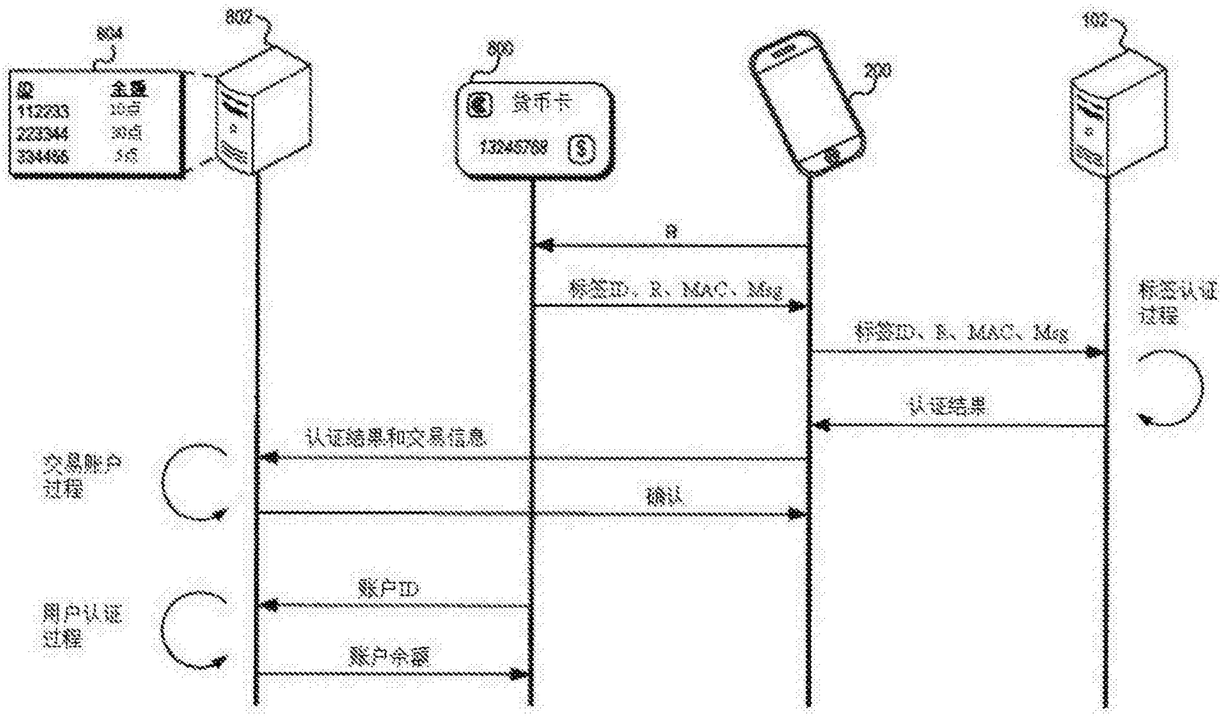

804
802
800
200
102
金额
112233
223344
334455
货币卡
R
标签ID、R、MAC、Msg
标签ID、R、MAC、Msg
标签认证过程
认证结果
认证结果和交易信息
交易账户过程
确认
账户ID
用户认证过程
账户余额

图 8

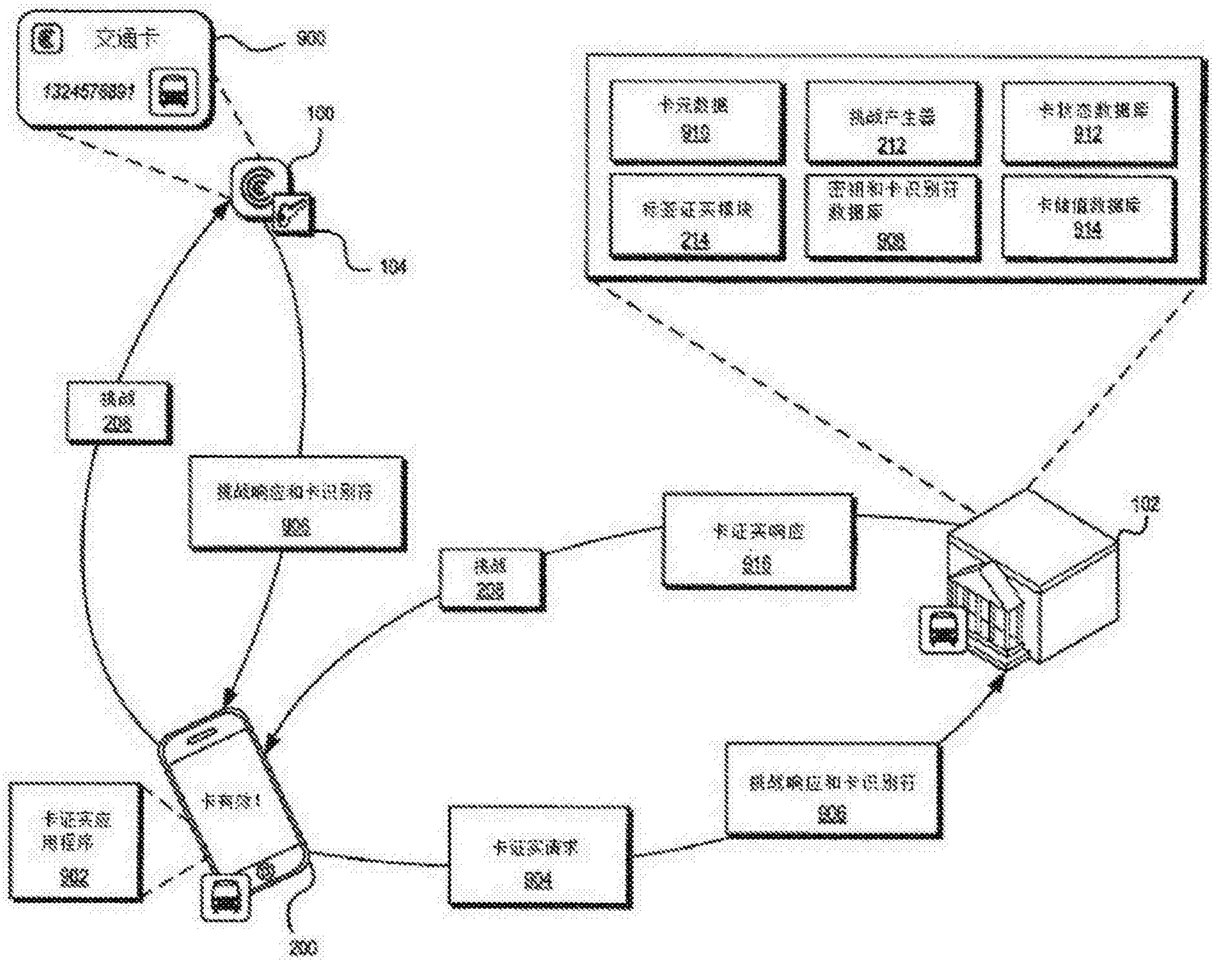

交通卡
900
100
104
挑战产生器
212
214
挑战
208
挑战响应和卡识别符
906
卡证实响应
916
102
卡证实请求
904
200

图 9

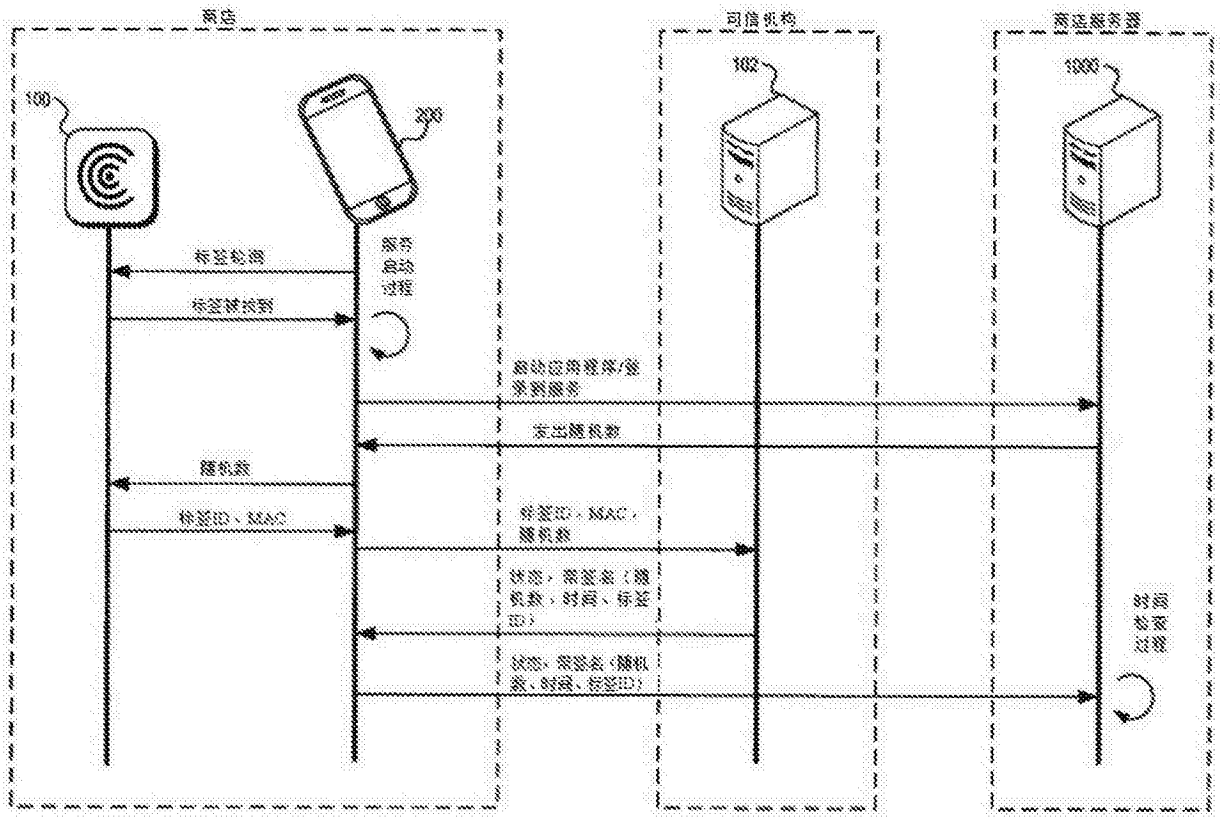

终端
可信机构
商业服务器
100
300
102
1000
标签检测
标签被检测到
服务启动过程
启动应用程序/登录到服务
发出随机数
随机数
标签ID、MAC
标签ID、MAC、随机数
状态、票签数（随机数、时间、标签ID）
状态、票签数（随机数、时间、标签ID）
时间标签过程

图 10

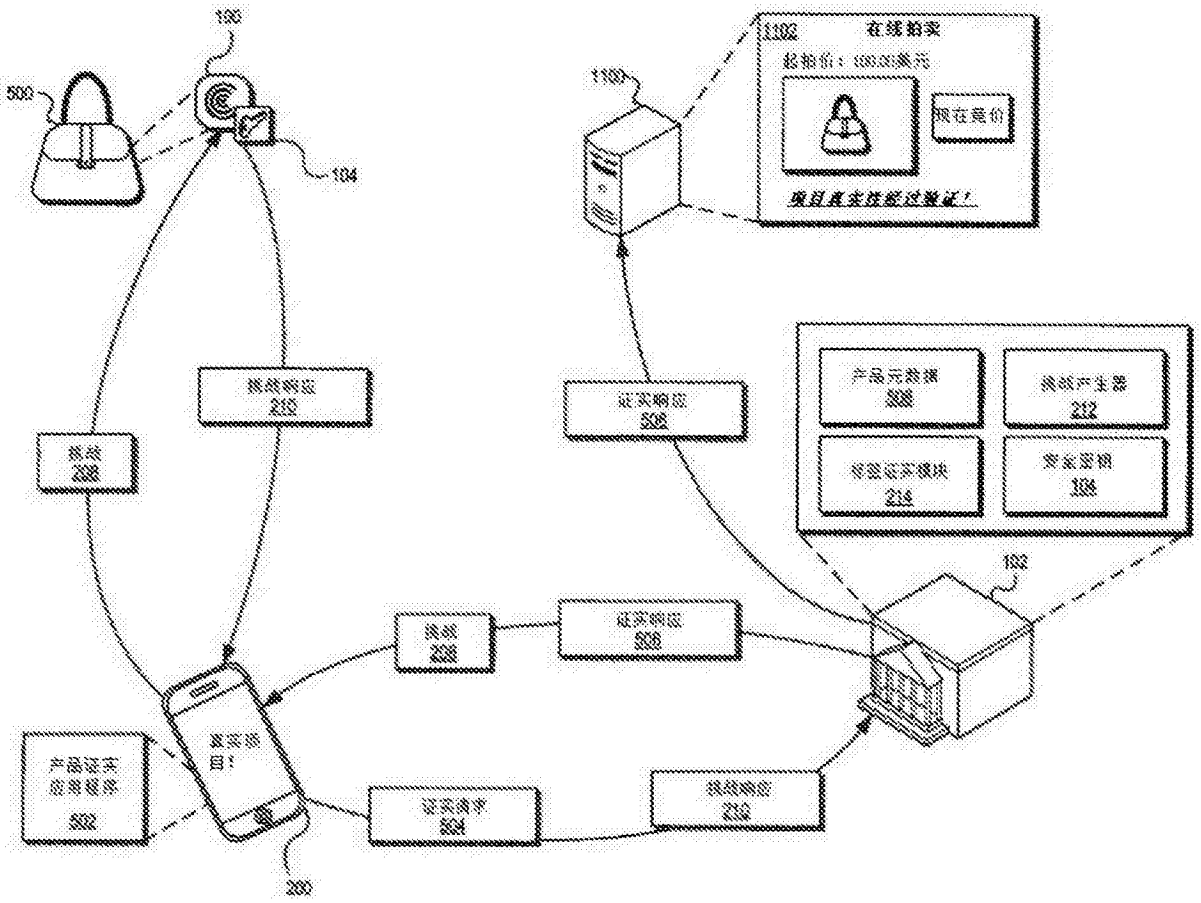


图 11

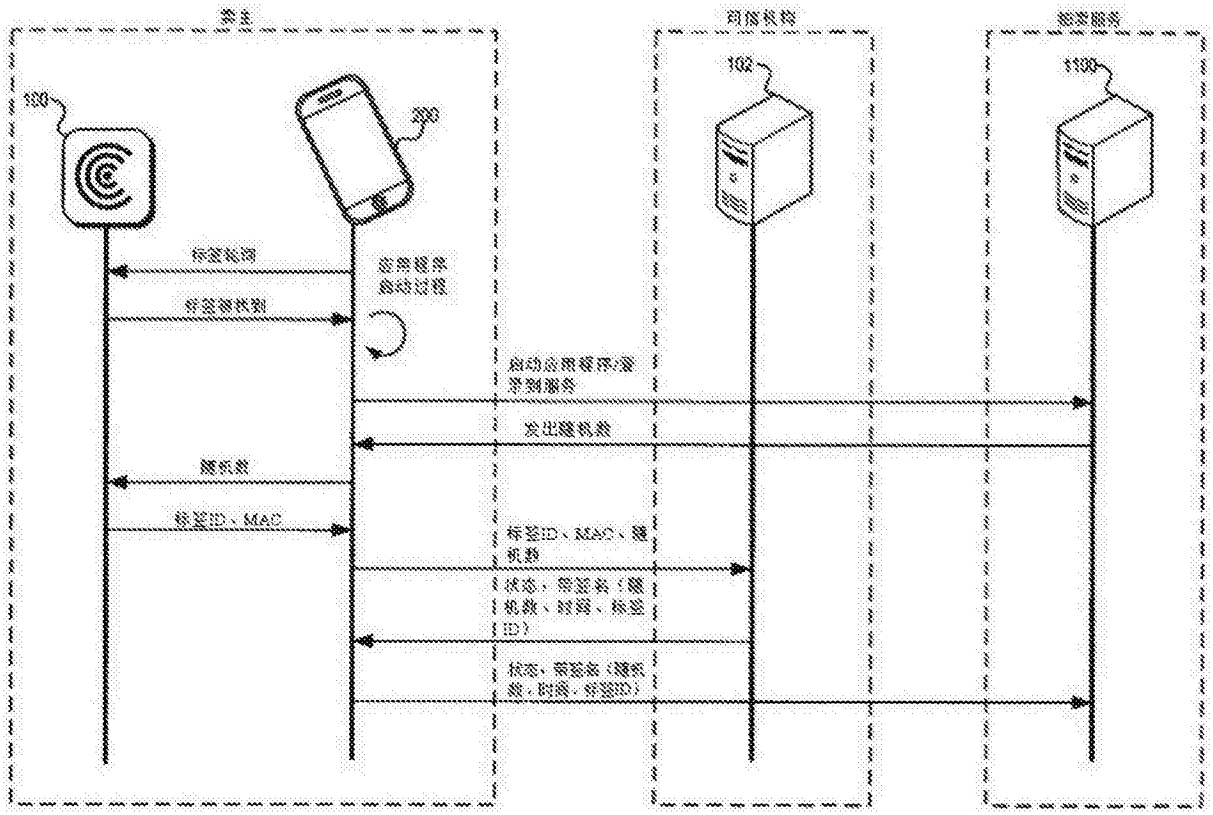

用户
可信机构
标签服务
100
200
102
110
标签检测
标签被检测
应用程序自动运行
自动应用程序/登录到服务
发出随机数
随机数
标签ID、MAC
标签ID、MAC、随机数
状态，带签名（随机数、时间、标签ID）
状态，带签名（随机数，时间，标签ID）

图 12

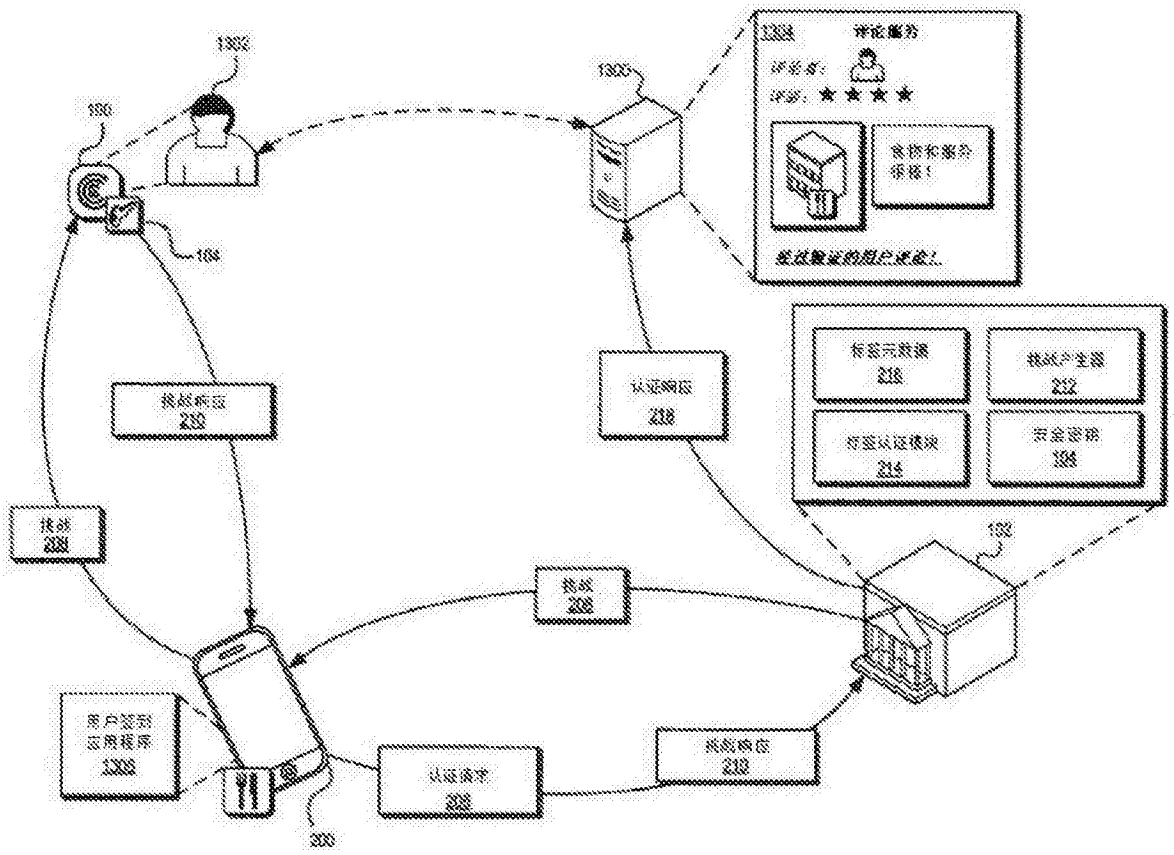


图 13

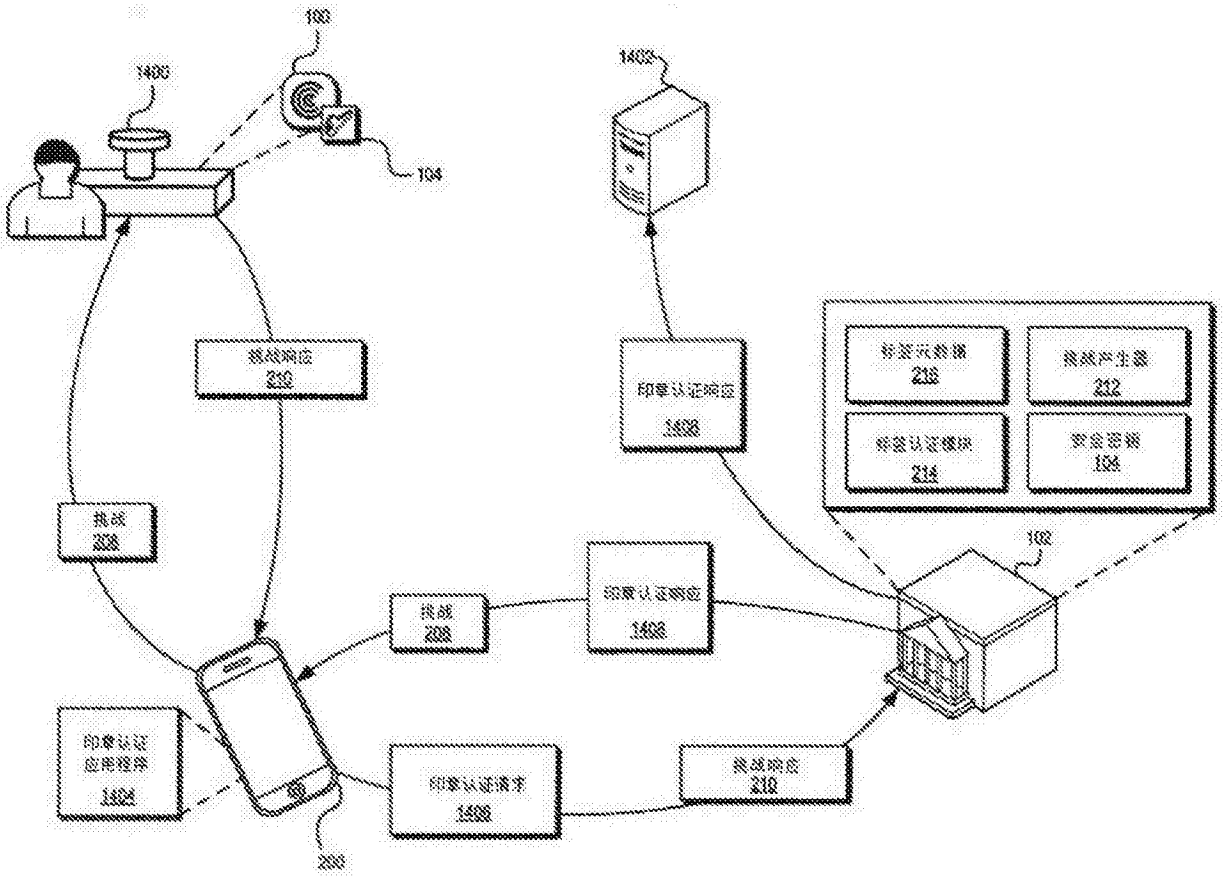


图 14

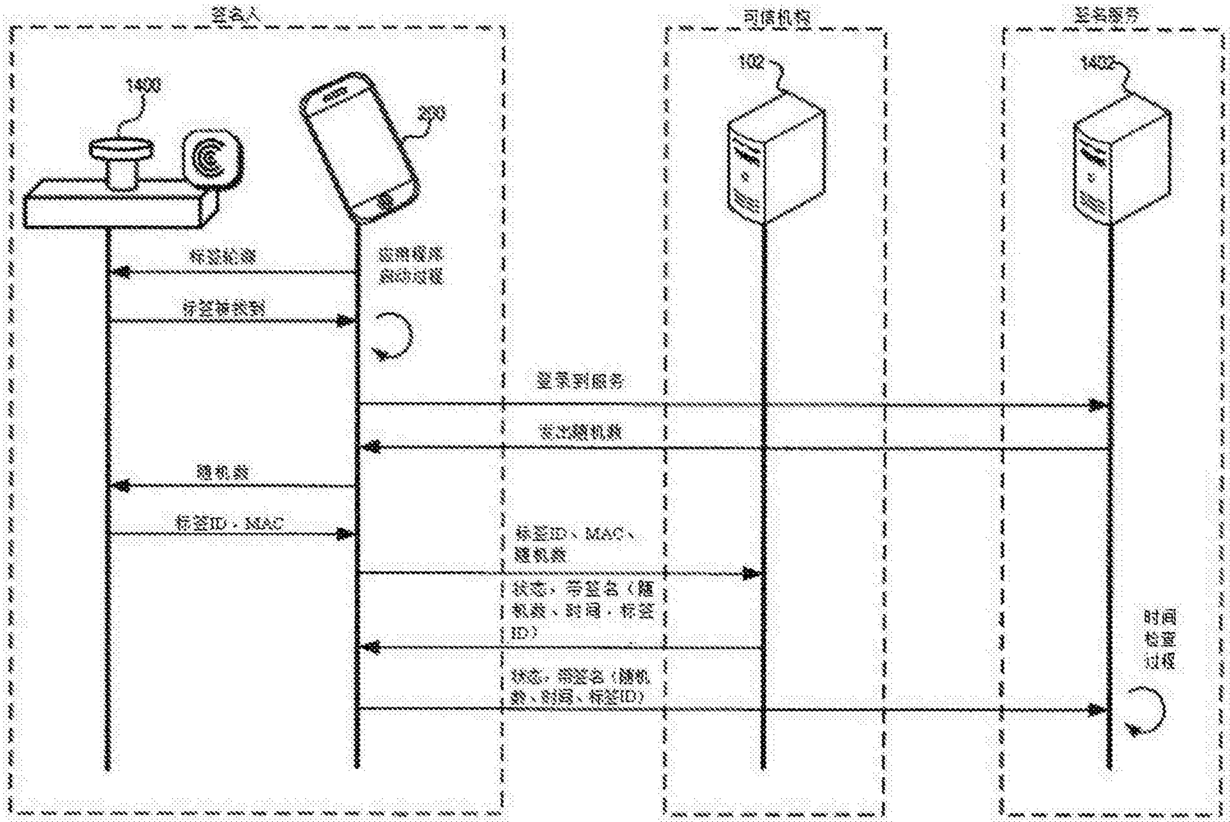

签名人
可信机构
签名服务
1400
300
102
1402
标签轮询
随机数
标签ID、MAC
标签ID、MAC、
随机数
状态，带签名（随机数、时间，标签ID）
时间
检查
过程

图 15

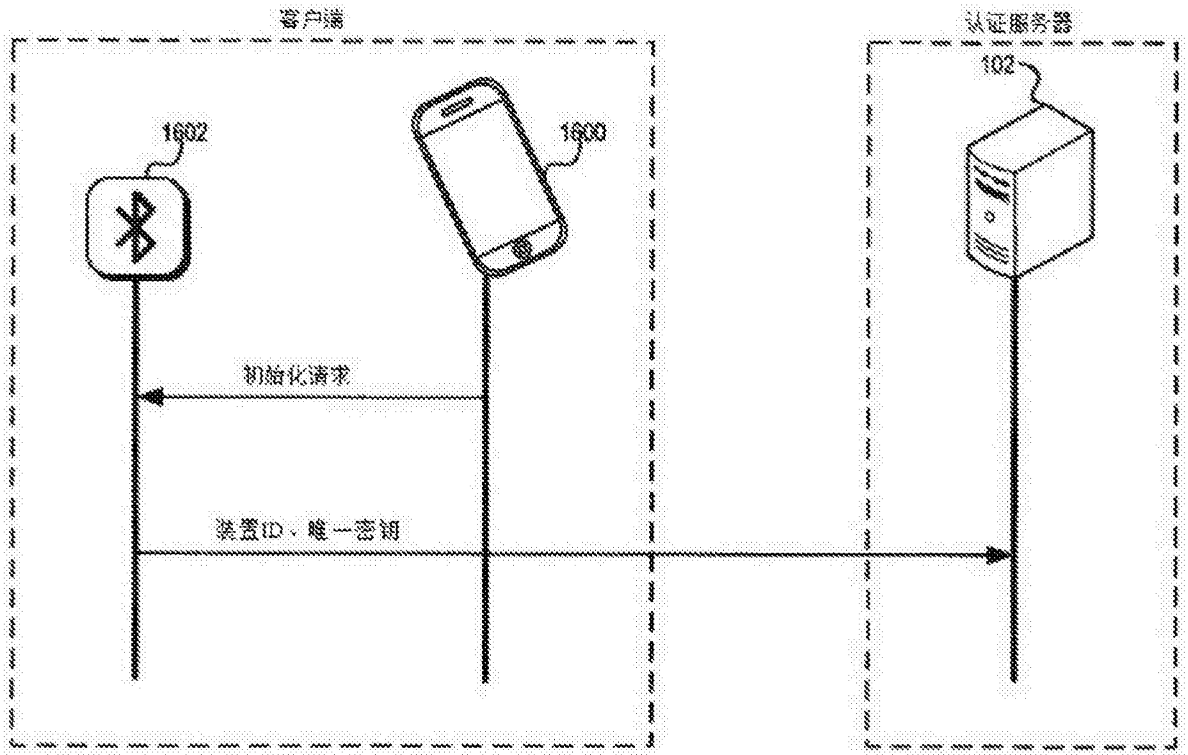

客户端
认证服务器
102
1602
1600
初始化请求
装置ID、唯一密钥

图 16

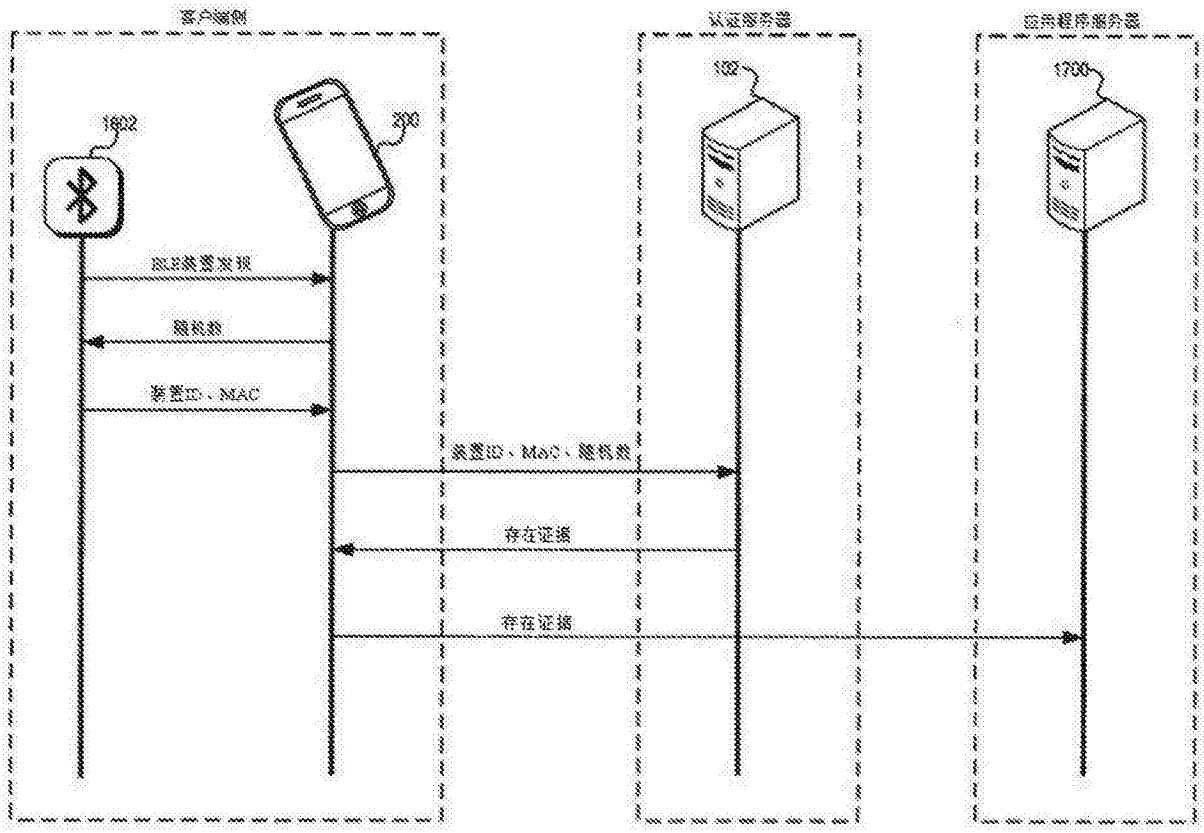

客户端侧
认证服务器
应用程序服务器
1602
300
102
1700
验证装置发现
服务器
装置ID、MAC
装置ID、MAC、服务器
存在证据
存在证据

图 17

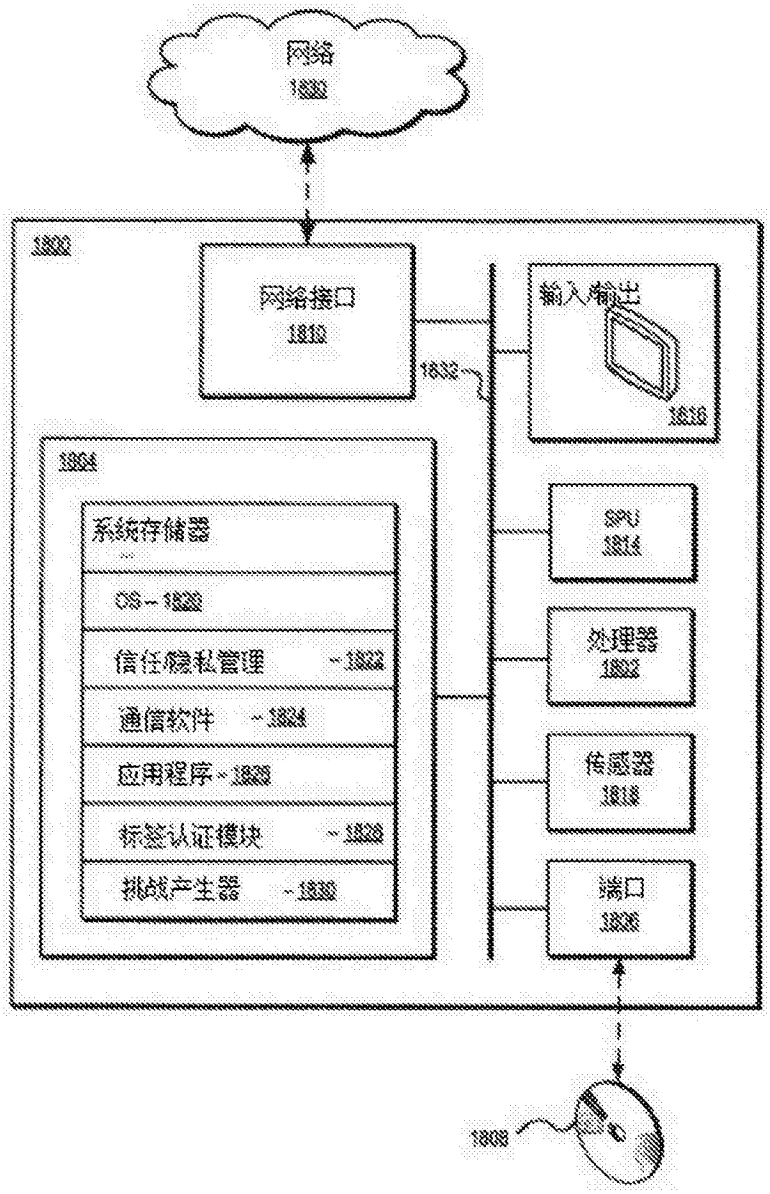

网络
1802
1800
网络接口
1810
1812
输入/输出
1816
1804
系统存储器
操作系统 - 1822
信任/隐私管理 - 1824
通信软件 - 1826
应用程序 - 1828
标签认证模块 - 1830
挑战产生器 - 1832
SPU
1814
处理器
1822
传感器
1818
端口
1820
1808

图 18