(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1968093 B
(45)授权公告日 2012.07.04

(21)申请号 200610141444.2
(22)申请日 2006.09.29
(30)优先权数据
11/163,010 2005.09.30 US
(73)专利权人 因特鲁斯特有限公司
地址 加拿大安大略
(72)发明人 克里斯·维埃斯 马克·史密斯
穆雷·麦库莱 罗伯特·朱克切拉托
(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 康建忠
(51)Int.Cl.
H04L 9/32(2006.01)
H04L 29/06(2006.01)
(56)对比文件
WO 2006/012538 A2,2006.02.02,
CN 1633776 A,2005.06.29,
US 2004/0187018 A1,2004.09.23,
审查员 冯玉学

权利要求书 5 页 说明书 29 页 附图 26 页

(54)发明名称

客户机/服务器验证系统中的离线验证方法

(57)摘要

一种用于当接收者单元离线时,提供接收者单元的用户验证的方法,包括基于与发送者单元的在线通信,存储与物品有关的一个或多个询问-应答集。每个询问-应答集包括至少一个询问-应答对,用于对于可通过接收者单元获得的特定资源进行用户的离线验证。当用户离线时,该方法包括选择多个存储的询问-应答集的至少一个,用于对于可通过接收者单元获得的特定资源进行用户的离线验证。

CN 1968093 B

1. 一种用于提供接收者单元的用户的验证的方法，包括：

基于与发送者单元的在线通信，存储与物品有关的至少一个询问－应答集，所述至少一个询问－应答集包括至少一个询问－应答对，用于对于可通过接收者单元获得的特定资源进行用户的离线验证；以及

由接收者单元选择至少一个存储的询问－应答集，用于对于可通过接收者单元获得的特定资源进行用户的离线验证。

2. 如权利要求 1 所述的方法，其中，存储至少一个询问－应答集包括：基于每个用户与发送者单元的在线通信，存储用于接收者单元的多个用户的每个用户的至少一个询问－应答集，其中，选择对应于每个用户的至少一个询问－应答集，用于可通过接收者单元获得的特定资源的每个用户的离线验证。

3. 如权利要求 1 所述的方法，其中，存储至少一个询问－应答集包括：将至少一个询问－应答集存储在高速缓冲存储器中。

4. 如权利要求 1 所述的方法，其中，所述接收者单元是无线通信设备。

5. 如权利要求 1 所述的方法，其中，所述询问－应答对基于成功的询问和应答。

6. 如权利要求 1 所述的方法，其中，所述询问基于发送者验证信息，可通过使用位置信息在物品上定位所述发送者验证信息，其中所述物品包括半透明或非半透明膜、不干胶贴纸、或卡。

7. 如权利要求6所述的方法，其中，存储的询问－应答集的数量小于可在物品上获得的所有可能的询问－应答集。

8. 如权利要求 6 所述的方法，其中，所述询问将位置信息识别为卡上的行和列信息。

9. 如权利要求 1 所述的方法，其中，除询问－应答对以外，存储的询问－应答集包括表示下述至少之一的数据：用户标识信息、物品标识信息、时间输入数据、指示是否已经离线使用存储的询问－应答集的标志、存储的询问－应答集已被离线使用的次数、以及在完成用户的成功验证后，用户可访问的接收者单元的特定资源的标识。

10. 如权利要求 1 所述的方法，其中，至少一个存储的询问－应答集基于密码变换。

11. 如权利要求 10 所述的方法，其中，所述密码变换基于散列函数。

12. 如权利要求 1 所述的方法，其中，存储至少一个询问－应答集包括：清除存储的询问－应答集，以及在从发送者单元接收到用户验证确认后，存储至少一个新的询问－应答集，所述用户验证确认具有不同于存储在接收者单元中的物品标识信息的物品标识信息。

13. 如权利要求1所述的方法，包括存储与物品有关的多个询问－应答集，其中，所述选择包括选择多个询问－应答集中的至少一个。

14. 如权利要求 13 所述的方法，其中，存储多个询问－应答集包括：当尝试将询问－应答集增加到已经具有预定最大数量询问－应答集的多个存储的询问－应答集时，替换存储的询问－应答集。

15. 如权利要求 13 所述的方法，其中，存储多个询问－应答集包括：基于下述至少之一来替换存储的询问－应答集：随机替换、替换最早的、替换最新的、替换最常使用的和替换最少使用的。

16. 如权利要求 13 所述的方法，其中，存储多个询问－应答集包括：从发送者单元请求询问－应答集组中的任何一个，以及响应接收到该组而存储该组。

17. 如权利要求 13 所述的方法，其中，存储多个询问 - 应答集包括 ：从发送者单元请求与物品有关的所有可能询问和相应应答，以及在从发送者单元接收到与物品有关的所有询问和相应应答后，存储与物品有关的所有询问和相应应答。

18. 如权利要求 13 所述的方法，其中，选择基于下述至少之一 ：随机选择、选择最早的、选择最新的、选择最常使用的、选择多个存储的询问 - 应答集中最少使用的至少一个。

19. 如权利要求 1 所述的方法，包括在选择至少一个存储的询问 - 应答集用于用户的第二级验证之前，提供第一级验证。

20. 一种用于提供接收者单元的用户的验证的方法，包括 ：

选择多个存储的询问 - 应答集的至少一个，用于可通过接收者单元获得的特定资源的用户离线验证 ；

对应于对于多个存储的询问 - 应答集的被选至少一个的每一个的发送询问，从用户接收应答 ；

比较接收的应答和存储的应答是否匹配 ；以及

对应于对于多个存储的询问 - 应答集的被选至少一个的每一个的发送询问，在接收的应答与存储的应答匹配后，认可用户的验证。

21. 如权利要求 20 所述的方法，其中，认可用户的验证包括 ：递增用于多个存储的询问 - 应答集的被选至少一个的每一个的使用计数器。

22. 如权利要求 20 所述的方法，其中，选择基于下述至少之一 ：随机选择、选择最早的、选择最新的、选择最常使用的、选择最少使用的多个存储的询问 - 应答集的至少一个。

23. 如权利要求 20 所述的方法，其中，所述询问基于发送者验证信息，可通过使用位置信息在物品上定位所述发送者验证信息，其中所述物品包括半透明或非半透明膜、不干胶贴纸、或卡。

24. 如权利要求 23 所述的方法，其中，存储的询问 - 应答集的数量小于可在物品上获得的所有可能的询问 - 应答集。

25. 如权利要求 23 所述的方法，其中，所述询问将位置信息识别为卡上的行和列信息。

26. 一种用于提供接收者单元的用户的验证的方法，包括 ：

当接收者单元与发送者单元在线时，在接收者单元存储用于验证用户的至少一个询问 - 应答集 ；以及

当接收者单元离线时，使用存储的询问 - 应答集来验证用户。

27. 如权利要求 26 所述的方法，其中，存储的询问 - 应答集基于成功的先前使用的询问 - 应答集。

28. 如权利要求 26 所述的方法，进一步包括 ：当接收者单元离线以及询问 - 应答验证尝试超出预定最大数时，使用保密口令短语来验证接收者单元的用户。

29. 如权利要求 26 所述的方法，其中，所述询问基于发送者验证信息，可通过使用位置信息在物品上定位所述发送者验证信息，其中所述物品包括半透明或非半透明膜、不干胶贴纸、或卡。

30. 如权利要求 29 所述的方法，其中，存储的询问 - 应答集的数量小于可在物品上获得的所有可能的询问 - 应答集。

31. 如权利要求 29 所述的方法，其中，所述询问将位置信息识别为卡上的行和列信息。

32. 一种用于提供接收者单元的用户的验证的设备，包括：

用于基于与发送者单元的在线通信，存储与物品有关的至少一个询问－应答集的部件，所述至少一个询问－应答集包括至少一个询问－应答对，用于对于可通过接收者单元获得的特定资源进行用户的离线验证；以及

由接收者单元选择至少一个存储的询问－应答集，用于对于可通过接收者单元获得的特定资源进行用户的离线验证的部件。

33. 如权利要求 32 所述的设备，其中，用于存储询问－应答集的部件包括：基于每个用户与发送者单元的在线通信，存储用于接收者单元的多个用户的每个用户的至少一个询问－应答集的部件，其中，选择对应于每个用户的至少一个询问－应答集，用于对于可通过接收者单元获得的特定资源进行每个用户的离线验证。

34. 如权利要求 32 所述的设备，其中，用于存储询问－应答集的部件包括：用于将至少一个询问－应答集存储在高速缓冲存储器中的部件。

35. 如权利要求 32 所述的设备，其中，所述接收者单元是无线通信设备。

36. 如权利要求 32 所述的设备，其中，所述询问－应答对基于成功的询问和应答。

37. 如权利要求 32 所述的设备，其中，所述询问基于发送者验证信息，可通过使用位置信息在物品上定位所述发送者验证信息。

38. 如权利要求 37 所述的设备，其中，存储的询问－应答集的数量小于可在物品上获得的所有可能的询问－应答集。

39. 如权利要求 37 所述的设备，其中，所述询问将位置信息识别为卡上的行和列信息。

40. 如权利要求 32 所述的设备，其中，除询问－应答对以外，存储的询问－应答集包括表示下述至少之一的数据：用户标识信息、物品标识信息、时间输入数据、表示是否已经离线使用存储的询问－应答集的标志、存储的询问－应答集已被离线使用的次数、以及在完成用户的成功验证之后，用户可访问的接收者单元的特定资源的标识。

41. 如权利要求 32 所述的设备，其中，所述至少一个存储的询问－应答集基于密码变换。

42. 如权利要求 41 所述的设备，其中，所述密码变换基于散列函数。

43. 如权利要求 32 所述的设备，其中，用于存储询问－应答集的部件包括：用于清除存储的询问－应答集，以及在从发送者单元接收到用户验证确认后，存储至少一个新的询问－应答集的部件，所述用户验证确认具有不同于存储在接收者单元中的物品标识信息的物品标识信息。

44. 如权利要求 32 所述的设备，其中，用于存储询问－应答集的部件包括用于存储与物品有关的多个询问－应答集的部件，其中，选择包括选择多个询问－应答集的至少一个。

45. 如权利要求 44 所述的设备，其中，所述用于存储与物品有关的多个询问－应答集的部件包括：用于当尝试将询问－应答集增加到已经具有预定最大数量询问－应答集的多个存储的询问－应答集时，替换存储的询问－应答集的部件。

46. 如权利要求 44 所述的设备，其中，所述用于存储与物品有关的多个询问－应答集的部件包括：用于基于下述至少之一来替换存储的询问－应答集的部件：随机替换、替换最早的、替换最新的、替换最常使用的和替换最少使用的。

47. 如权利要求 44 所述的设备，其中，所述用于存储与物品有关的多个询问－应答集的

部件包括：用于从发送者单元请求询问－应答集组的任何一个，以及响应接收到该组而存储该组的部件。

48. 如权利要求44所述的设备，其中，所述用于存储与物品有关的多个询问－应答集的部件包括：用于从发送者单元请求与物品有关的任何可能的询问和相应应答，以及在从发送者单元接收到与物品有关的所有询问和相应应答后，存储与物品有关的所有询问和相应应答的部件。

49. 如权利要求44所述的设备，其中，所述用于选择询问－应答集的部件的选择基于下述至少之一：随机选择、选择最早的、选择最新的、选择最常使用的、选择多个存储的询问－应答集中最少使用的至少一个。

50. 如权利要求32所述的设备，其中，在选择多个存储的询问－应答集的至少一个用于用户的第二级验证之前，提供第一级验证。

51. 一种用于提供接收者单元的用户的验证的设备，包括：

选择多个存储的询问－应答集的至少一个，用于可通过接收者单元获得的特定资源的用户离线验证的部件；

对应于对于多个存储的询问－应答集的被选至少一个的每一个的发送询问，从用户接收应答的部件；

比较接收的应答和存储的应答是否匹配的部件；以及

对应于对于多个存储的询问－应答集的被选至少一个的每一个的发送询问，在接收的应答与存储的应答匹配后，认可用户的验证的部件。

52. 如权利要求51所述的设备，其中，认可用户的验证的部件包括：用于递增用于多个存储的询问－应答集的被选至少一个的每一个的使用计数器的部件。

53. 如权利要求51所述的设备，其中，所述用于选择的部件的选择基于下述至少一个：随机选择、选择最早的、选择最新的、选择最常使用的、选择多个存储的询问－应答集最少使用的至少一个。

54. 一种用于提供接收者单元的用户的验证的设备，包括：

当接收者单元与发送者单元在线时，在接收者单元存储用于验证用户的至少一个询问－应答集的部件；以及

当接收者单元离线时，使用存储的询问－应答集来验证用户的部件。

55. 如权利要求54所述的设备，其中，当接收者单元离线以及询问－应答验证尝试超出预定最大数时，使用保密口令短语来验证接收者单元的用户。

56. 如权利要求54所述的设备，其中，所述询问基于发送者验证信息，可通过使用位置信息在物品上定位所述发送者验证信息。

57. 如权利要求56所述的设备，其中，所述询问将位置信息识别为卡上的行和列信息。

58. 一种用于提供接收者单元的用户验证的方法，包括：

从接收者单元接收对于至少一个询问－应答集的请求；以及

基于与接收者单元的在线通信，响应所述请求，将与物品相关的至少一个询问－应答集发送给接收者单元，发送的询问－应答集包括至少一个询问－应答对，用于对于可通过接收者单元获得的特定资源进行用户的离线验证。

59. 如权利要求58所述的方法，其中，所述请求是对于先前成功的在线询问应答集。

60. 如权利要求 58 所述的方法，其中，响应请求进行发送包括发送下述至少一个：

多个先前成功的询问 - 应答集；

所有可能的询问 - 应答集；以及

少于所有可能的询问 - 应答集。

61. 如权利要求 58 所述的方法，其中，所述询问基于发送者验证信息，可通过使用位置信息在物品上定位所述发送者验证信息。

62. 如权利要求 61 所述的方法，其中，存储的询问 - 应答集的数量小于可在物品上获得的所有可能的询问 - 应答集。

63. 如权利要求 61 所述的方法，其中，所述询问将位置信息识别为卡上的行和列信息。

64. 一种系统，包括：

发送者单元和由用户使用的接收者单元，所述发送者单元和接收者单元适合于相互通信，所述发送者单元用来响应于从接收者单元接收到请求，向接收者单元发送至少一个询问 - 应答集；以及

接收者单元，用来：

存储从发送者单元发送的至少一个询问 - 应答集，所述至少一个询问 - 应答集包括至少一个询问 - 应答对，用于对于可通过接收者单元获得的特定资源进行用户的离线验证；

从用户接收对应于至少一个存储的询问 - 应答集的发送询问的应答；

比较接收的应答与存储的应答是否匹配，以及

在接收的应答与对应于发送询问的存储的应答匹配后，认可用户的验证。

65. 如权利要求 64 所述的系统，其中，所述询问基于发送者验证信息，可通过使用位置信息在物品上定位所述发送者验证信息，其中所述物品包括半透明或非半透明膜、不干胶贴纸、或卡。

66. 如权利要求 65 所述的系统，其中，存储的询问 - 应答集的数量小于可在物品上获得的所有可能的询问 - 应答集。

67. 如权利要求 65 所述的系统，其中，所述询问将位置信息识别为卡上的行和列信息。

客户机／服务器验证系统中的离线验证方法

技术领域

[0001] 本发明通常涉及用于提供用户和目标资源或信息发送实体之间的验证的方法和装置，以及更具体地说，涉及采用软令牌或硬令牌来提供用户和目标资源或信息发送实体之间的相互验证的方法和装置。

背景技术

[0002] 已知相互验证系统和方法尝试验证由内容服务供应商或其它目标资源提供的信息的用户或接收者，所述目标资源例如可通过在线通信链路、诸如通过互联网、内联网或任何其它适当的无线或非无线网络来访问。这些方法和装置尝试阻止尝试窃取用户身份的黑客或其它人的恶意利用。例如，恶意实体可能使用合法银行的地址来发送邮件，并将接收者引向“假冒网站”。相信它是合法站点的接收者可以被欺骗提供能由恶意方使用来访问接收者在线帐户的诸如帐号和口令字的信息。这一问题可能在消费者人群中尤其严重，其中，传统的在线相互验证方法可能非常复杂，通常要求昂贵的硬件配置和复杂的用户交互，使得这种相互验证技术不实际。同样地，期望提供允许以相对低廉但安全的方式来确认正访问所需目标组织（即发送实体）的用户或接收者的系统和方法。

[0003] 已知双因素验证技术，例如使用第一验证因素来验证终端用户的身份，以及用于验证的第二因素补充通常用在第一因素验证中的用户名和口令字。第二因素的概念是，用户能使用他们知道的一些东西（即他们的口令字）以及他们具有的一些东西（即第二因素，可以是例如硬件令牌）来进行验证。典型地，第二因素机制是基于硬件的，并被物理分发给终端用户。例如，时间同步令牌是已知的并有时被称为多因素验证技术。下面进一步描述几种已知的技术。

[0004] 同时，已知用于结合互联网应用来执行目标组织验证的各种方法，包括例如基于主办给定 web 应用的组织的身份，由可信第三方来提供证明的安全套接字层服务器验证。然而，这会要求用户执行双击屏上图标并读完信息的手动步骤。要求手动动作通常会防碍一致执行，由此破坏该方法的有效性。另外，也已知客户机安全性插件应用，包含终端用户下载并安装提供用户何时与合法站点通信的可视表示的客户机端软件。然而，对终端用户来说，下载和安装软件或通过几个手动步骤来确认目标组织的身份是很麻烦的。

[0005] 另外，用户和目标组织验证方法当延伸到其它通信信道，诸如通过诸如便携式电话、个人数字助理、互联网设备的移动设备或其它移动设备的交互式语音响应系统或通信时也是不实际的，因为它们依赖于基于 web 的应用独特的用户显示和输入方法。

[0006] 确保已经由信任的也称为可信发送实体发送了发送电子邮件消息或其它电子消息有助于确保防止重要信息被恶意方窃取或能帮助限制垃圾邮件和网络钓鱼 (phishing)。网络钓鱼是互联网骗局的一种形式，通常包含好象来自合法组织，诸如银行或其它金融机构或其它组织的邮件的大规模发送。这些邮件通常将接收者引向欺骗网站或由此欺骗他或她泄露个人或金融信息。另一种网络钓鱼骗局可能不要求这些信息，但一旦输入 URL，则执行下载击键登录程序，该程序允许网络钓鱼者从接收者的机器获得信息。然后，该信息能用

于身份窃取或欺骗。

[0007] 网络钓鱼攻击会很昂贵且会消耗公司的资源，因为例如大量攻击会遇到大量目标公司以及数亿网络钓鱼消息通过过滤系统，会降低电子邮件递送，用光服务器的宝贵处理时间以及最终会导致重要金融数据流失到不道德方。

[0008] 已经尝试解决这一问题的几种解决方案。因为网络钓鱼攻击通常开始于从仿造的发送地址发送大量电子邮件，努力减少垃圾邮件在降低网络钓鱼攻击量方面相当有效。例如，一种方法被称为发送者策略架构，消息的发起人或发起人域在目录或其它适当的库中公布通过接收消息传送代理而验证的合法发送计算机地址。消息传送代理可以经 DNS 服务器（域名服务器）来校验接收的消息。然而，该技术会要求普遍采用实现和配置可能昂贵的 SPF 使能消息传送代理。

[0009] 被称为主动协同减少垃圾邮件的另一技术也要求发起人域中的发起人以如上所述比较类似的方式来公布由接收消息传送代理校验的合法发送计算机地址。

[0010] 另一技术要求域数字签名电子邮件，通过经 DNS 服务器接收消息传送代理来对其进行校验。同样地，这也要求普遍采用改进版本的消息传送代理。

[0011] 另一技术使用 S/MINE 协议，其中，发送个人或域数字签名电子邮件，通过接收呼入消息传送代理或用户电子邮件客户机对其进行校验。这要求在基于 web 的电子邮件客户机中当前不支持的特定电子邮件客户机特征或接收者消息传送代理。

[0012] 另一技术采用在发送者和接收者之间共享的保密图像。如所理解的，私人图像由用户发送到验证服务器。该服务器存储接收者发送的图像。验证服务器也可以通过电子邮件将私人图像发送到接收者，以及看到图像的用户认出这是他发送的那个。同时，在登录到站点期间，服务器可以将图像包括在登录页中，使得当用户看到他们的私人图像时，用户信任该登录页（见例如 www.passmarksecurity.com）。在其它缺点中，该系统似乎将同一图像用于多次登录直到改变共享图像为止，并会要求接收者选择并将该图像发送到发送服务器。

[0013] 另外，已知其它系统尝试提供接收者验证，而不是发送者验证。例如，US 专利 No.5,712,627 除别的以外，公开了一种发行的标识卡，在分配的卡上的一个可访问地址处具有标记。该卡可以具有可按行或列访问的不同数字、字母或符号的行和列。为了确定是否授权正试图访问数据的人获得所请求的访问，将标识卡分发给受权用户。尝试访问的请求人提供在如由安全系统指定的卡上的一个或多个可访问位置处的标记。为了告知输入和返回哪一标记，系统选择已知存在于特定卡上的同等标记。然后，接收者必须发回位于由安全系统发送的地址处的标记。如果该标记与指定给正试图访问的人的标记匹配，那么，准许访问。然而，这些系统未解决有关网络钓鱼的问题，因为该系统提供接收者而不是发送者的验证，以及请求正尝试访问的人向系统识别它们自己，以及该系统要求用户输入和发送位于安全卡上的信息。

[0014] 也已知其它验证系统，例如已经用在军事中，已经使用数字加密 / 验证系统，其采用由发送者和接收者持有的卡。例如通过使用询问和应答验证方案来验证传输。例如电子传输的发送者可以使用该卡并随机选择行和列，并传送行和列标识符作为询问。作为应答，使用行和列标识符来查找字母然后传送回。如此，发送者能确保接收者拥有卡。然而，通常通过颠倒地重复相同的询问和应答来完成发送者到接收者的验证，并且发送者和接收者都

必须拥有相同的验证卡来实现相互验证。

[0015] 另一技术也使用包括有关发送者和接收者的信息的行和列的卡，然而，该传输验证方案用来验证传输。例如，在传输验证期间，传输验证图的列位于密码表的后面并用来验证发送者。通过指定代表，诸如单元的命令者来进行列分配。发送者和接收者事先都知道列分配。传输验证图仅使用一次。使用指定列中的第一个未用验证码以及通过验证码画线以便防止其再用。这些方案不利用卡上的信息的随机选择以及不利用发送协同信息，因为事前已知列信息。如此，显然仅发送验证信息。如果发送者发送验证信息并由接收者确定其有效，则接收者从该卡划掉该验证信息。下次要求验证时，使用同一列中的下一个验证信息。如此，使用顺序和非随机方法。然而，如果接收者的验证卡丢失或由不道德方获得，则他们将知道如何充当发送者，因为他们知道哪一验证信息是列中的下一个，因为利用了非随机选择以及因为该卡在其上具有标记。在该系统中，由于用来验证发送者的信息列对于发送者和接收者来说事前已知，不发送协同信息。另外，如果接收者未收到发送者的传输，则将失去发送者和接收者之间的同步，这会导致后续验证尝试失败。

[0016] 同时，随着技术变得更成熟，信息安全和用户标识安全正变得日益重要。例如，试图使用多因素验证方案来挫败黑客或挫败信息和用户标识的其它不适当使用。例如，双因素验证方案可以使用接收者或用户已知的信息，诸如口令字或个人标识号 (PIN)，以及一些类型的物理令牌，诸如银行卡、信用卡、口令字令牌或用户必须实际拥有的其它物理令牌，以便启动或完成在线交易。另一验证级可以包括生物测定验证，可以包括指纹、眼睛或其它生物测定的扫描，以便再次校验试图访问过程、设备、应用或其它权利的用户事实上是适合的用户。

[0017] 已知交易卡可以包括例如智能卡、基于磁条的卡以及便于银行交易、信用卡交易或任何其它适当交易的其它交易卡。如本领域所公知的，除了拥有银行卡以外，通常要求用户个人标识号 (PIN) 以便从自动提款机获得现金或者执行在线交易。一种已知的多因素验证技术采用使用硬件令牌，诸如电池操作的智能卡，在智能卡的一部分上显示定期改变和表面上的随机数。当用户希望通过智能卡来执行交易时，例如，用户输入通常改变的表面上的随机数。接收交易服务器将如在智能卡上显示的由用户输入的接收码与由码源发生器生成的相应数进行比较。如果由用户输入的码与码源发生器所生成的数匹配，则准许交易并授予用户特定权利，诸如访问银行帐号、购买商品、获得信息、有权访问网站或其它软件应用，或所需要的任何其它适当权利。然而，这些硬件令牌会相当昂贵以及是电池供电的，因此要求更换电池，并存在由于与电子电路有关的潮湿问题或任何其它问题而电子误操作的可能。

[0018] 不采用这类屏幕的其它智能卡通常要求读取例如磁带的卡阅读器。这对用户希望执行在线交易但没有位于包含或有权访问磁带阅读器的地方是限制。

[0019] 在似乎不相关的领域中，已知半透明卡，诸如包含半透明图形或图案的塑料卡，当被可视地观察时，似乎不包含任何具体信息。然而，当该半透明卡被放在具有相应的背景过滤图案的显示器上时，卡上图案与显示屏上的背景图案的组合结合表示可视识别的消息或词，诸如词“对不起”或“你是胜利者”。这些是对任一用户不唯一的静态消息并通常仅包括单个消息。这些塑料卡可以用来例如查看拥有者是否已经赢得奖励。可以在邮件中将卡邮寄给会员。然后，那些参与者到半透明卡上所识别或邮寄信息中指示的网页来查看他们是

否赢得奖励。然而，这些塑料卡不提供多因素验证，不是用户专用的，不包括多个消息和通常包括静态消息。

[0020] 在某些环境中，当接收者单元相对于目标源离线时，当用户希望使用接收者单元的资源时，有必要验证用户接收者。例如，接收者单元可以是能登录到目标源，诸如服务器以便使用服务器的资源的膝上型电脑。当膝上型电脑与服务器处于在线通信时，用户可以使用已知验证方法的任何一个从膝上型电脑登录到服务器。然而，通过接收者单元和目标源之间的在线交互来提供用户的验证。当接收者单元离线，即，不与目标源通信时，系统管理员可能希望也提供用户的验证以便访问接收者单元的资源。除第一级验证外，当访问离线接收者时，管理员可能希望提供用户的第二级验证。例如上述膝上型电脑 / 服务器的例子，膝上型电脑的用户可能带膝上型电脑旅行，并且不能通过在线验证来访问服务器。然而，管理员可能希望当用户离线时，限制用户使用膝上型电脑，或当离线的同时使用膝上型电脑的资源时，提供用户的第二级验证。然而，没有正与目标源在线的接收者，通常不能第二级验证用户，因为通常在线验证期间从目标源向接收者传送第二级验证信息和用户的校验。

[0021] 上述问题的现有解决方案由用于 Microsoft ® Windows ®的 RSA 安全的 RSA 的 SecurID ®来提供，其是客户机验证客户机 / 服务器应用，允许使用 SecurID ®时间同步一次口令字令牌来验证 MicrosoftWindows 客户机。用于 Microsoft Windows 的 SecurID ®能离线完成验证过程。SecurID ®包括驻留在服务器上的 RSA 验证管理器，以及用于驻留在客户机上的 Microsoft Windows 的 RSA 代理。

[0022] SecurID 过程的第一步是在成功的在线验证之后，验证管理器通过预先计算将在预定多天内由客户机使用的一系列未来时间相关验证码，来定制用于离线验证的客户机系统。然后，验证管理器散列代码并发送它们，以便安全存储在客户机系统上。当用户尝试离线登录到他们的台式机时，用于 Microsoft Windows 的验证代理将识别出客户机未连接到服务器，将提示用户输入他们的 UserID 和密码。然后，验证代理将用户输入的信息与存储的代码进行比较，并将相应地准许或拒绝访问。用户下次通过与服务器的在线连接登录到桌面时，验证管理器将更新存储在客户机上的代码用于未来的离线访问。

[0023] 然而，SecurID ®产品具有几个缺点。一个缺点是，由 SecurID ®提供的整个离线验证是时间相关的。SecurID ®要求离线客户机和验证服务器的系统时钟同步，否则验证尝试将失败，因为将相对于系统时钟来校验提交的代码。另一缺点是，离线验证机制不够灵活以便适应在不定时间周期离线的用户。如果离线周期长于离线验证所允许的预定时间周期，则系统将不再能够验证用户。一旦时间周期届满，用户信任和验证将不再同受验证机制控制。另一缺点是，预先计算的时间相关验证应答（即代码）存储在不具有相应询问的客户机上。因此，询问永不改变并应用于所有预先计算的应答。

[0024] 因此，需要克服上述一个或多个问题的方法和装置。

附图说明

[0025] 图 1 是示例说明根据本发明的一个实施例，用于安全地提供标识信息的系统的一个例子的框图；

[0026] 图 2 是示例说明根据本发明的一个实施例，用于安全地提供标识信息的方法的一个例子的流程图；

[0027] 图 3 是示例说明图 2 所示的方法的进一步分解的图；

[0028] 图 4 是示例说明根据本发明的一个实施例的安全标识信息构件的一个例子的图；

[0029] 图 5 是图示根据本发明的一个实施例，便于用户验证或用于安全地提供标识信息的登录屏的一个例子的图；

[0030] 图 6 图示地示例说明根据本发明的一个实施例，显示的可视过滤图案的一个例子；

[0031] 图 7 图示地示例说明根据本发明的一个实施例，从位于半透明标识构件上的一个或多个隐蔽的标识符可视识别的指定标识符的一个例子；

[0032] 图 8 是根据本发明的一个实施例，用于安全地提供标识信息的系统的图；

[0033] 图 9 是根据本发明的一个实施例，更详细地示例说明半透明标识构件发行器的一个例子的框图；

[0034] 图 10 和 11 示例说明了根据本发明的一个实施例，用于安全地提供标识信息的方法的一个例子的流程图；

[0035] 图 12 示例说明根据本发明的一个实施例，包括包含半透明标识构件的部分的交易卡的一个例子；

[0036] 图 13 示例说明根据本发明的一个实施例，包含半透明标识构件的交易卡的另一例子；

[0037] 图 14 是示例说明根据本发明的另一实施例，安全标识信息构件的一个例子的图；

[0038] 图 15 图示地示例说明根据本发明的一个实施例，显示的隐蔽标识符信息的一个例子；

[0039] 图 16 是示例说明根据本发明的一个实施例，用于安全地提供标识信息的系统的另一例子的框图；

[0040] 图 17 是示例说明根据本发明的一个实施例，用于安全地提供标识信息的方法的一个例子的流程图；

[0041] 图 18 是表示根据本发明的一个实施例，可以用在用于提供电子消息验证的方法中的物品，诸如卡的一个例子的图示；

[0042] 图 19 示例说明根据本发明的一个实施例，包括用在提供电子消息验证中的发送者验证信息和位置坐标信息的交易卡的一个例子；

[0043] 图 20 是示例说明根据本发明的一个实施例，用于提供电子消息验证的方法的一个例子的流程图；

[0044] 图 21 是表示根据本发明的一个实施例，具有附加的发送者验证信息和位置坐标信息的消息的一个例子的图示；

[0045] 图 22 是示例说明根据本发明的一个实施例，用于提供电子消息验证的系统的一个例子的框图；

[0046] 图 23 是示例说明根据本发明的一个实施例，用于提供电子消息验证的方法的一个例子的流程图；

[0047] 图 24 是示例说明根据本发明的一个实施例，用于提供用户和目标资源之间的相

互验证的系统的一个例子的框图；

[0048] 图 25 是示例说明根据本发明的一个实施例，用于提供用户和目标资源之间的相互验证的方法的一个例子的流程图；

[0049] 图 26 是示例说明根据本发明的一个实施例，用于提供用户和目标资源之间的相互验证的方法的另一实施例的例子的流程图；

[0050] 图 27 是示例说明根据本发明的一个实施例，用于提供用户和目标资源之间的相互验证的方法的另一例子的流程图；

[0051] 图 28 是示例说明根据本发明的一个实施例，用于以图示形式来提供用户和目标资源之间的相互验证的设备的一个例子的框图；

[0052] 图 29 是示例说明用于用户的离线验证的询问 - 应答集的在线存储的一个例子的框图；

[0053] 图 30 是示例说明当接收者单元与发送者单元在线时，用户的在线验证和询问 - 应答集的存储的例子的流程图；

[0054] 图 31 是示例说明当接收者单元与发送者单元离线时，用户的离线验证的例子的流程图；

[0055] 图 32 是示例说明基于在线验证期间的多个存储的询问应答集的离线验证尝试的例子的流程图；以及

[0056] 图 33 是示例说明用于用户的离线验证的询问 - 应答集的在线存储的一个例子的框图。

具体实施方式

[0057] 简单地说，公开了一种用于当接收者单元离线时，提供接收者单元的用户的验证的方法。该方法包括基于与发送者单元的在线通信，存储与物品有关的至少一个询问 - 应答集。该询问 - 应答集包括至少一个询问 - 应答对，用于对可通过接收者单元获得的特定资源进行用户的离线验证。当用户离线时，该方法包括对可通过接收者单元获得的特定资源，选择存储的询问 - 应答集用户的离线验证。该方法还包括存储与物品有关的多个询问 - 应答集，每个询问 - 应答集包括用于用户的离线验证的至少一个询问 - 应答对。因此，当用户离线时，该方法包括对接收者单元可获得的特定资源，选择多个询问 - 应答集中的至少一个用于用户的离线验证。

[0058] 在另一实施例中，用于提供用户和发送者单元（即目标资源）之间的相互验证的方法包括：对已经被分配物品（诸如其上具有标记的卡或其它适当物品）的用户，确定对应于嵌在物品上的实际发送者验证信息的所需发送者验证信息。通过使用由询问的发送者单元提供的位置信息，在物品上定位发送者验证信息。该方法包括为用户确定相应的物品标识信息，诸如已经分配给该物品的序列号或共享密钥，以及发送用于该用户的询问，其中，该询问至少包括位置信息，以便允许用户识别位于物品上的所需发送者验证信息并发送物品标识信息。然后，用户接收位置信息和物品标识信息，并将物品标识信息用作表示已经发送信息的发送者可信的验证信息，因为用户拥有的物品也包括其上的物品标识信息。然后，用户使用已经发送到用户设备的位置信息来确定例如位于物品上的相应所需发送者验证信息，诸如通过目标资源所发送的行和列信息，并将询问应答发送回目标资源（即发送者

单元）。然后，发送者基于询问应答来验证用户。应答包括从物品获得的用户验证信息，即所需发送者验证信息。如果由用户设备基于位置信息而发送（以及从物品获得）的所接收的发送者验证信息与所需发送者验证信息匹配，则目标资源准许用户（即用户设备）适当地访问。如此，在例如已经确定第一级验证成功之后，由发送者与位置信息一起发送物品标识信息。第一级验证可以包括例如在登录过程的初始阶段，用户将口令字和用户 ID 发送到目标资源，如本领域所公知的，在此之后，基于成功的第一因素验证处理，随后发送位置信息和物品标识信息。

[0059] 在另一例子中，用于提供相互验证的方法不要求将物品标识信息发送给用户，而是仅需要发送位置信息，以便允许用户识别物品上的相应验证信息，并将应答发送回目标资源以便验证。然而，在该实施例中，如果应答不包括发送者单元所期望的期望目标资源验证信息，那么该方法包括重复用于该用户的相同询问，包括先前发送的相同位置信息。例如在每一连续会话上重复该过程，直到用户发送基于在询问中发送的位置信息从物品获得的适当目标资源验证信息为止。

[0060] 另外，还公开了执行上述方法的适当设备。同时，采用两种方法的结合来实现一种增强的相互验证过程。

[0061] 还公开了一种用于电子消息验证的方法，采用物品（也称为构件或令牌），诸如卡、不干胶贴纸或任何其它的适当物品，所述物品包括发送者验证信息和位置信息（诸如行和列标题）。在一个例子中，向感兴趣的每一个接收者发行包含可通过相应位置信息（诸如列和行标识符）识别的发送者验证信息的物品。当电子消息的发送者希望将消息发送给感兴趣的接收者时，发送者发送电子消息和位置信息以及位于由位置信息识别的位置处的相应所需发送者验证信息。这包括表示位置和验证信息的数据（诸如索引、引用、位置信息或验证信息本身、或其任何适当表示）。然后，在一个实施例中，接收者在相应位置查看他们的物品（例如卡），并看发送的所需发送者验证信息是否与位于物品上的发送者验证信息（也称为期望的发送者验证信息）相匹配。如果出现匹配，那么接收者信任消息的发送者。接收者不需要向发送者发回任何信息。如此，可以使用简单卡或其它物品来验证消息的发送者以便防止网络钓鱼或其它发送者验证问题。将由本领域的普通技术人员识别其它例子。

[0062] 另外，还公开了一种用于提供电子消息验证的系统，执行上述方法，还公开了一种交易卡，以不干胶贴纸的形式或作为交易卡本身的一部分，在其上包括位置信息和发送者验证信息。在另一实施例中，物品可以是半透明物品以便允许光通过，使得可以由发送者与消息一起发送可视过滤图案和发送者验证信息。用户将物品举到显示屏并将其覆盖在由发送者发送的可视过滤图案上。如果最终发送者验证信息与消息中发送的结果匹配，则接收者可以信任消息的发送者。

[0063] 在另一实施例中，用于安全地提供标识信息的装置和方法生成用于接收者的一个或多个隐蔽用户（例如接收者）标识符，诸如基于用户保密数据（诸如口令字、个人标识号或其它保密或非保密信息）而生成的多个标识符，或不基于用户保密数据的标识符（诸如随机生成然后与用户相关联的标识符）。在这种情况下，使用非用户相关信息，但标识符仍然可以识别用户。在另一实施例中，可以使用单个隐蔽标识符。

[0064] 在一个实施例中，该方法和装置生成半透明标识构件（TIDM，translucent

identification member)，诸如塑料卡、片、膜的一部分或全部，或具有包括一个或多个隐蔽标识符的半透明区的其它适当构件。如在此所使用的，半透明区也能包括透明区。例如，半透明标识构件可以由透明或清晰片制成，包括具有用墨水打印或者置于其上或其中的隐蔽标识符（包括非字符信息）的烟熏塑料或其它适当色彩。一个或多个隐蔽标识符可以是例如对半透明标识构件的接收者唯一的一次性验证标识符。如此，半透明标识构件或卡包含视觉上看起来像是信息的随机图案。

[0065] 当用户期望使用半透明标识构件时，也生成相应的可视过滤图案用于在显示设备上显示。例如，从可视观点看，可视过滤图案也看起来是随机的，但当可视地结合半透明标识构件上的一个或多个隐蔽标识符时，可视地显示出一个或多个隐蔽标识符中的指定的一个。在一个实施例中，用户可以将半透明标识构件覆盖在显示设备的指定部分上，或显示可视过滤图案的显示器的指定部分中。可视过滤图案和半透明标识构件上的不同隐蔽标识符图案的结合从一个或多个标识符形成可视显示的单个标识符或消息。因此，例如在一个实施例中，在屏幕上生成似乎是随机的图案，其有助于确保向正在查看覆盖在正在显示器上显示的可视过滤图案上的半透明标识构件的用户可视地显露仅单个标识符。

[0066] 因此，如果期望，已经例如访问半透明标识构件发行器的安全人员可以使用空白玻璃纸卡的包装，用来在本地打印机上制作半透明标识构件。可以使半透明标识构件打印有充当一个或多个隐蔽标识符的半透明彩色图案，或具有看起来半随机或对用户隐蔽的其它适当标记。也可以使用彩色或彩色背景来阻止影印攻击。将意识到，可以通过供应商和网络的分布或通过基于 web 的服务来提供半透明标识构件发行器的部分或全部功能。例如，接收者可以通过 web 连接来访问 TIDM 发行服务以及本地打印 TIDM，或通过邮件接收 TIDM。而且，可以由一方来提供标识符并发送到另一方用于打印或制造。根据需要，也可以采用操作的其它分布。

[0067] 一旦向用户呈现了可视显示的标识符，用户通过用户界面输入可视显示的标识符，其中，将其与期望的标识符进行比较。如果输入的标识符与期望的标识符匹配，则表示适当的验证并准许接收者访问设备、应用或过程或其它所需权利（或接收所提交的数据—例如投票）。另外，也可以保持废除的半透明标识构件的列表，以便防止由于偷窃或丢失半透明标识构件而泄密。该列表可以存储在任何适当的位置并由服务供应商、半透明标识构件发行器或任何适当实体更新。由于半透明标识构件不要求生成随机数的电子设备，半透明标识构件的成本可能相当低，以及它们的可靠性也可以相对高，因为它们不易经受通常与智能卡有关的潮湿或其它损坏。

[0068] 在另一实施例中，如果需要的话，智能卡或其它交易卡或非交易卡（例如投票卡或其它适当卡）可以包括半透明标识构件。因此，公开了一种交易卡，包括例如包含卡标识信息的部分（诸如交易卡号，其可以印在其上，诸如通过凸起打印或电子或通过任何其它适当的存储机构，诸如磁带或任何其它适当的机构），以及包含具有包括一个或多个隐蔽标识符的半透明区的半透明标识构件。如此，交易卡，诸如信用卡、银行卡或任何其它交易卡可以包括包含半透明标识构件的窗口，或可以具有固定到传统交易卡上的交易标识号或其它标识信息以便增强安全性。

[0069] 在另一实施例中，半透明标识构件和接收者单元的作用被翻转。例如，在该实施例，半透明标识构件包含可视过滤图案，以及显示屏显示至少一个隐蔽的标识符，其可以是

例如表示对用户唯一的用户验证数据的数据，或如果需要，表示其它数据。将半透明标识构件（可视过滤器）覆盖在显示隐蔽标识符的显示器上的组合显示出（未隐蔽）屏幕上的至少一个隐蔽标识符。构件上的可视过滤图案保持相同，因为其被打印在构件上，以及在每一会话期间或以其它适当间隔改变所显示的隐蔽标识符。

[0070] 因此，可以产生一个或多个下述优点。由于可以由组织安全官员打印半透明标识构件，不需要招致制造成本，以及能本地生成它们用于接收者。由于不需要电子设备，不存在待替换的电池，以及不会发生由于暴露于潮湿的损坏。不需要网络或无线电连接，诸如由采用磁带的设备通常所需的。半透明标识构件可以由塑料或任何其它适当的材料制成并处于任何适当的厚度。它们耐用且在泄密的情况下易于替换，因为由组织本地生成它们。能避免连续地生成与屏幕上的动态变化码匹配的主代码的基本网络体系结构和智能卡的投资。

[0071] 在一个实施例中，显示的可视过滤图案有选择地照明半透明标识构件的一部分以便可视地显示一个或多个隐蔽标识符中的一个。可以每一验证会话改变可视过滤图案。所述一个或多个隐蔽标识符是半透明（或透明）卡上的打印标记并且在特定用户域内最好是唯一的。通过许多适当的技术，诸如色调发暗、字符排序、它们的组合或任何其它适当的可视模糊技术，使一个或多个隐蔽标识符可视地隐蔽。图 1 示例说明用于安全地提供标识信息的系统 10 的一个例子，包括 ：半透明标识构件发行器 12，用于生成安全标识构件，诸如半透明标识构件 14 ；可视过滤发生器 16 ；半透明标识构件验证模块 18 ；接收者单元 20 和存储器 22。在该例子中，可视过滤发生器 16 和半透明标识构件验证模块 18 包括为半透明标识构件验证器 24 的一部分，验证器 24 可以实现为在计算单元（诸如个人计算机、工作站、服务器、手持设备，或任何其它适当的设备或多个联网设备）上执行的一个或多个软件模块。半透明标识构件验证器 24 在该例子中可操作地耦合到 web 服务器，web 服务器再可操作地耦合到网络，诸如互联网 26 以便于接收者单元 20 和半透明标识构件验证器 24 之间的基于 web 的通信。如此，多个电路由软件和处理设备形成。同时，如在此所使用的，电路也被称为任何适当的形式的任何适当的电子逻辑，包括但不限于硬件（微处理器、离散逻辑、状态机、数字信号处理器等等）、软件、固件或它们的任何适当组合。

[0072] 半透明标识构件发行器 12、可视过滤发生器 16 和半透明标识构件验证模块 18 可以用任何适当的方式来实现，最好但不限于在一个或多个计算设备上执行的软件模块，所述计算设备包含执行存储在存储器中的指令的一个或多个处理设备。

[0073] 在该例子中，半透明标识构件发行器 12 将被描述为本地服务器，使用打印机或生成半透明标识构件 14 的其它适当的机器，来生成半透明标识构件 14。半透明标识构件包括半透明区，包括其上的一个或多个隐蔽标识符。然而，将意识到，半透明标识构件发行器 12 可以包括为半透明标识构件验证器 24 的一部分，或可以位于包括 web 服务器的任何其它适当设备上，以及将意识到，在此所述的任何软件程序也可以适当地位于任一适当设备或多个设备上。

[0074] 存储器 22 可以是任何适当的本地或分布式存储器，以及如果需要，可以位于 web 服务器或本地放置。存储器可以是 RAM、ROM 或任何适当的存储器技术。接收者单元 20 可以是任何适当的设备，诸如膝上型电脑、台式计算机、手持设备或包括显示器 30 和用户接口的任何其它适当设备，并可以包括执行存储在任何适当存储器中的指令的一个或多个处理设备。接收设备包括通过 web 浏览器或其它应用或操作系统，来提供一个或多个用户界

面（诸如图形用户界面）的必要电路，并可以包括语音识别接口或任何其它适当的用户接口。如此，这些单元包括：用来显示所定义的可视过滤图案的显示电路，以便当可视过滤图案与位于半透明标识构件上的一个或多个隐蔽标识符可视地结合时，可视地显示一个或多个标识符中指定的一个；以及用来接收表示可视显示的标识符的数据的输入接口。在一个例子中，使用用户接口来请求输入与半透明标识构件有关的序列号，以及请求输入所显示的标识符以便确定是否准许接收者所需的权利。

[0075] 同时，如果需要，接收者单元能接收过滤或隐蔽的标识符用于在显示屏上显示，以及通过完全不同的设备（或通过完全不同的信道），诸如蜂窝电话、通过SMS消息、电子邮件消息或其它适当的信道和/或设备，来发回响应。

[0076] 再参考图2和3，将描述用于安全地提供标识信息的方法。如块200所示，接收者通过互联网或通过任何其它适当的机构，将请求发送到半透明标识构件发行器12，以便请求发行半透明标识构件14。例如这可以通过接收者通过用户提供的数据，诸如口令字或其它保密信息与在线金融机构注册来完成。这表示为由半透明标识构件发行器12接收的接收者特定信息32。

[0077] 如块202所示，该方法包括生成用于接收者的一个或多个隐蔽标识符，其可以基于例如接收者特定信息32和/或其它信息34。其它信息34可以是半透明标识构件序列号，或如果需要，其它适当的信息。这可以例如由半透明标识构件发行器12或任何其它适当实体来完成。如块204所示，该方法包括生成具有包括一个或多个隐蔽标识符38的半透明区36的半透明标识构件14。在该例子中，由半透明标识构件发行器12来生成一个或多个隐蔽标识符38并以数据库形式存储在存储器22中。一个或多个隐蔽标识符存储在存储器22中，使得当需要创建适当的可视图案40以显示需要显示的标识符700时，或当校验返回的显示标识符700时，可以随后访问它们。

[0078] 例如，半透明标识构件发行器12可以控制打印机来打印玻璃纸卡作为在其上打印有一个或多个隐蔽标识符的半透明标识构件14。半透明标识构件的一个例子如图4所示。该半透明标识构件14可以由任何适当的材料，诸如塑料或提供一定透明级的任何其它适当的材料制成，使得当一个或多个隐蔽标识符覆盖在发光的显示器上时，允许来自显示器的光能（或缺少光能）与一个或多个隐蔽标识符组合，以便可视地指定半透明标识构件上的一个或多个标识符中的一个。半透明标识构件上的一个或多个标识符也可以是多个不同的隐蔽标识符。

[0079] 半透明标识构件14可以是卡、片、薄膜或其它构件，如果需要，可以包括任何适当的粘附或连接结构，以便应用于交易卡的窗口上，或任何其它适当的材料。半透明标识构件也可以连接到交易卡，诸如通过使用适当的连接结构将半透明标识构件连接到交易卡的末端或侧面。在半透明标识构件38上打印的一个或多个隐蔽标识符38，如上所述，可以是字母（例如ASCII）、符号、打印图案、颜色版本或任何其它的适当标记。一个或多个隐蔽标识符38看起来是视觉隐蔽的，并因此当由接收者查看时似乎是随机的。在其它实施例中，可以期望打印不隐含字母而是可视地隐蔽消息或其它信息的油墨图案，使得当覆盖在显示器的顶面时，由显示器生成的图案结合打印图像允许查看者可视地解密所显示出的标识符。

[0080] 半透明区36包括表示一个或多个标识符的信息图案，所述标识符可以是用于一个或多个验证会话或其它目的的唯一标识信息。由一个或多个隐蔽标识符表示的信息图案

最好对于指定用户域是唯一的，以便降低同一用户获得具有相同隐蔽标识符的相同半透明标识构件的可能性。构造（例如按尺寸制作）半透明区 36 以便覆盖接收者单元 20 上的显示屏 30 的至少一部分。在一个实施例中，一个或多个隐蔽标识符的每一个用作用于半透明标识构件的接收者的一次性验证标识符。注意到，如在此所使用的，标识信息包括用来直接或间接验证用户（例如 TIDM 接收者）或感兴趣的其它过程，或获得访问与过程或设备有关的所需权利的任何信息，或除实施交易之外意图保密的任何其它适当信息。

[0081] 为了制作 TIDM，该方法可以包括从用户接收对于一个或多个隐蔽用户标识符的请求，并记录用户和与一个或多个隐蔽用户标识符有关的标识信息之间的链接。该方法可以包括向用户提供一个或多个隐蔽用户标识符，其中，一个或多个隐蔽用户标识符在发送给用户的半透明标识构件上，一个或多个隐蔽用户标识符发送到第三方以便置于用户的半透明标识构件上，一个或多个隐蔽用户标识符发送到用户以便置于半透明标识构件上，以及从预先存在的隐蔽用户标识符库中选择一个或多个隐蔽用户标识符。来自用户的请求可以包括用户特定信息，以及用户特定信息可以用来创建一个或多个隐蔽标识符，以及可以与其它信息结合来产生一个或多个隐蔽用户标识符。

[0082] 如块 206 所示，一旦已经生成半透明标识构件 14 并提供给接收者，可视过滤发生器 16 或其它适当的机构生成可视过滤图案，用于在接收者设备的显示器 30 上显示。当由接收者设备显示可视过滤图案 40 时，可视过滤图案与位于半透明标识构件 14 上的一个或多个隐蔽标识符结合，以便指定一个或多个标识符中的一个。换句话说，可视过滤图案滤出不期望的标识符以便显示一个或多个标识符中的被选一个。

[0083] 如块 208 所示，该方法可以包括诸如由接收者或设备将半透明标识构件 14 覆盖在显示的过滤图案 40 上，以便可视地识别半透明标识构件 14 上的隐蔽标识符中的指定一个。然后，由接收者输入可视识别的标识符，以便于交易或获得访问与感兴趣的任何过程或设备有关的特定所需权利。

[0084] 如图 3 所示，更详细地表示图 2 的步骤。如块 300 所示，例如通过获得接收者特定信息，诸如保密或非保密数据或非用户相关信息，由半透明标识构件发行器 12 或任何其它适当实体来实现生成用于接收者的一个或隐蔽标识符。也可以通过使用非用户相关和非用户提供的材料来实现该过程，在任一情况下，将生成的一个或多个隐蔽标识符与用户后续相关。当使用接收者特定信息时，可以是由接收者通过接收者单元 20 提供或来自任何其它适当源的个人标识号、口令字、用户名、帐号或其它数据。这表示为接收者特定信息 32。如块 302 所示，诸如通过适当的数学函数或算法适当地组合接收者特定信息 32 以产生一个或多个隐蔽标识符 38。其它信息 34 可以是例如由随机数发生器生成的输出、可以打印在半透明标识构件 14 上或由半透明标识构件发行器 12 存储的实际半透明标识构件序列号 44（或其它 TIDM 标识信息）或任何其它适当信息。如块 204 所示，半透明标识构件序列号或用于识别半透明标识构件的任何其它适当信息分配给隐蔽的一个或多个标识符 38。将意识到，在初始请求或生成半透明标识构件后，半透明标识构件发行器 12 可以选择半透明标识构件序列号并与接收者特定信息 32 相关联。组合该信息以便生成一个或多个隐蔽标识符 38。半透明标识构件序列号 44 可以存储在存储器 22 中，用于由半透明标识构件验证器 24 以后使用（使用半透明标识构件 14 来验证接收者）。基于所需结果，可以适当地重排与在此所述的任一方法有关的步骤的顺序。

[0085] 如块 306 所示，生成半透明标识构件 14 可以包括在塑料膜、片或卡上以所需格式打印隐蔽的不同标识符以便产生半透明标识构件 14。如块 308 所示，在显示器上显示过滤图案 40 可以包括从隐蔽标识符中随机选择在显示器 30 上产生可视过滤图案 40 的被选标识符，作为当半透明标识构件 14 覆盖在可视过滤图案 40 上时将显示的标识符。

[0086] 如图 4-7 所示，以及进一步示例说明例子，如图 4 所示，半透明标识构件 14 在其上印有半透明标识构件序列号 44 或其它标识信息，以及印在半透明区 36 中的一个或多个隐蔽标识符。如上所述，这可以印在玻璃纸材料或传统打印机易于适应的其它材料上，如果需要，降低制作成本。然而，可以使用任何适当的材料或制造工艺。一旦接收者拥有半透明标识构件 14，使用半透明标识构件 14 来提供多因素验证。

[0087] 可以以任何适当的方式来生成过滤器。例如，可以从 TIDM 上位置被限定的存储的一个或多个隐蔽标识符中选择被选的隐蔽标识符。可视过滤图案生成器 16 基于 TIDM 的预定布局来生成过滤图案，以保证过滤器挡住适当的字符位置。也可以使用任何其它适当的技术。

[0088] 如图 5 所示，接收者设备 20 可以通过 web 浏览器或其它适当的用户界面来显示输入屏，如果使用 web 浏览器，则基于接收的 HTML 页，包含接收用户输入的字段，诸如用户标识符字段 500、口令字字段 502 和半透明标识构件序列号字段 44。用户通过适当的界面按钮 504 来提交输入的信息。然后，该信息经互联网发送到 web 服务器，以及如果需要，转发到半透明标识构件验证器 24。如该例子所示，在用户 ID 字段 500 或口令字字段 502 中输入的信息可以被视为当半透明标识构件发行器 12 初始生成半透明标识构件 14 时先前输入的接收者特定信息 32。

[0089] 图 6 示例说明在显示器 30 上显示以便于使用半透明标识构件 14 来安全地提供标识信息的图形用户界面（基于接收的 HTML 页生成）的一个例子。例如可以通过接收者单元上的 web 浏览器和适当的主处理器或任何其它适当的处理器来生成图形用户界面，并表示可以与显示器 30 上所显示的可视过滤图案 40 相同大小或不同大小的覆盖区 600。因此，响应于图 5 所示的登录屏，半透明标识构件验证器 24 提交包含图 6 所示的可视过滤图案 40 和响应界面屏的响应。接收者单元 20 显示可视过滤图案 40 和显露的标识符字段 602，以便允许输入来自一个或多个隐蔽标识符的一个显露的 ID。

[0090] 图 7 图示地示例说明半透明标识构件 14 覆盖在可视过滤图案 40 的上面以便显露一个或多个隐蔽标识符中的一个的情形。用户放置半透明标识构件 14，并因此将一个或多个打印隐蔽标识符 38 放在可视过滤图案 40 上，以及可视过滤图案 40 和打印的不同隐蔽标识符 38 的组合在该例子中显露出标识符 700，该标识符 700 然后由接收者输入显露的标识符字段 602 中。然后，用户将显露的标识符 700 提交给半透明标识构件验证器 24，以便验证特定交易的用户或访问特定权利。因此，半透明标识构件验证器 24 接收表示响应于用户或其它实体将半透明标识构件 14 覆盖在显示器 30 上而显露的标识符 70 的数据。半透明标识构件验证模块 18 将接收的显露的标识符 700 与相应的期望标识符 702（见图 1）进行比较以便确定接收者的适当验证是否合适。半透明标识构件验证模块 18 从存储器 22 获得相应的期望标识符 702，或已知可视过滤图案并访问隐蔽标识符 38 而临时生成期望标识符，或可以以任何其它适当方式来获得期望标识符 702。

[0091] 参考图 8 和 9，通过示例性实施例，更详细地描述半透明标识构件 14 的发行。为了

获得半透明标识构件 14，接收者使用接收者特定信息 32，诸如帐号或由注册请求 800 表示的其它信息，与在线银行或其它机构进行注册。然后，将该请求传递到 web 服务器 802。web 服务器 802 然后与银行服务器 804 通信，银行服务器 804 包括例如客户机管理系统和半透明标识构件请求器 806，如果需要的话，半透明标识构件请求器 806 可以是在处理设备上执行的适当软件应用程序或任何其它适当结构。然后，银行服务器 804 可以生成至半透明标识构件发行器 12 的半透明标识构件发行请求 808，半透明标识构件发行器 12 可以包括在适当的服务器 809 中或与服务器 809 分离。半透明标识构件发行请求 808 包括由用户输入的接收者特定信息 32。作为响应，半透明标识构件发行器 12 在响应消息 810 中提供隐蔽标识符 38，并连同将出现在用于请求接收者的半透明 ID 构件 14 上的相关隐蔽标识符 38，生成半透明标识构件序列号 44 并记录在存储器 22 中。在该例子中，银行服务器 804 将接收者帐号与半透明标识构件序列号 44 链接，然后，将链接的信息存储在数据库 810 中以便以后使用。然后，银行服务器 804 例如通过格式化隐蔽标识符 38 以便打印，并向打印机 814 或其它设备发送信息，然后打印机 814 或其它设备打印出或制造半透明标识构件 14，来生成半透明标识构件 14。因此，半透明标识构件序列号 44 由半透明标识构件发行器 12 分配并与一个或多个隐蔽标识符 38 相关联（例如链接），以及与数据库中的存储器 22 中的用户相关联。

[0092] 半透明标识构件发行器 12 可以包括信息随机发生器 900 和半透明标识构件格式器 902。信息随机发生器 900 可以使用半透明标识构件序列号 44 作为将与接收者特定信息 32 结合以便生成一个或多个隐蔽标识符 38 的其它信息 34。这可以使用散列算法或所需的其它适当编码技术来完成，以便生成一个或多个隐蔽标识符 38。半透明标识构件格式器 902 可以是在适当处理设备或多个设备上执行的另一软件应用程序，用于格式化输出到打印机或其它制造设备的信息。

[0093] 图 10 和 11 示例说明在发生半透明标识构件的发行之后，系统的操作的另一实施例。如块 1000 所示，该方法包括请求并获得接收者特定信息 32，诸如参考图 5 所述。一旦已经打印或制造半透明标识构件 14，则人工或通过邮寄或任何其它适当技术将其提供给接收者，如块 1002 所示。如块 1004 所示，银行的银行服务器确定接收者是否已经请求验证，诸如登录请求。如果已经接收到请求，则可以发送 web 页，请求输入接收者信息 32，包括口令字和半透明标识构件序列号 44 作为多因素验证过程的第一级，如块 1006 所示。这例如可以通过图 5 所示的屏幕来完成。如块 206 所示，银行服务器例如通过将信息传递到半透明标识构件验证器 24，来确定输入的接收者特定信息 32 和口令字以及半透明标识构件序列号 44 是否正确。如果第一验证级通过，那么如块 1010 所示，该方法包括显示可视过滤图案 44，该可视过滤图案当与半透明标识构件 14 上的一个或多个隐蔽标识符 38 可视结合时，显露出一个或多个隐蔽标识符中的仅一个作为将被输入用于当前会话或交易的适当标识符。然后，银行服务器通过 web 服务器，通过提供如图 6 所示的屏幕，请求输入如通过在显示器上显示的过滤图案而有选择地显露出的标识符 700。这在块 1010 中示出。响应请求，半透明标识构件验证器 24 接收显露出的一次使用标识符 700，并将接收的标识符与例如由可视过滤发生器或验证器 24 确定的相应的期望 ID 进行比较。这如块 1012 所示。给定“过滤器”、用户数据数据和有关那个用户的存储信息，验证器可以验证用户是否输入了正确数据（在本身上或传递到“服务器”）。如果在从用户请求它之前生成了所需标识符，那么该系统

也生成显露预定标识符的正确过滤器（均在之前显示给用户）。另外，如果为用户提供图案（过滤器），然后，系统通过从该图案获得的标识符来验证用户输入的标识符，则不需要提前拾取所需标识符和“过滤生成器”，因此不要求任何其它知识。也可以使用除显示可视过滤图案的设备以外的设备来接收表示可视显露的标识符的数据（例如数据本身、加密形式或其它适当数据）。例如，标识符可以显露在一个设备的屏幕上，以及可以使用手持设备或非手持设备来输入并向校验是否匹配的另一设备或系统发送可视显露的标识符。

[0094] 如块 1014 所示，如果匹配不存在，则向接收者发送错误并请求重输显露的标识符。系统可以改为使用不同标识符用于重试。同时，在一定数量的失败尝试之后，系统可以锁住用户。然而，如块 1016 所示，如果匹配出现，则可以确定第二因素验证成功并授予用户所需权利。

[0095] 图 12 和 13 示例说明采用半透明标识构件 14（包括图 14 所示的类型）的交易卡的例子。该交易卡可以是智能卡或非智能卡，并具有与信用卡、支付卡或任何其它适当交易卡相关的传统信息，并另外包括半透明标识构件 14。半透明标识构件出现在交易卡的一部分上。交易卡的一个部分包括帐户信息，诸如帐号、信用卡号或任何其它适当标识符 1300，以及如果需要，其它用户标识符，诸如用户名 1402。在图 12 所示的例子中，交易卡包括开口 1306，该开口 1306 可以例如在塑料交易卡中切出或者在塑料卡中提供，以及具有粘合剂的半透明标识构件 14 可被置于所述开口上，或可以在其中整体模塑，或者附着，诸如但不限于被构造成在交易卡中容纳或保持 TIDM 的连接结构，使得交易卡的大小与传统交易卡相同，或所需的任何其它适当大小。如果使用，连接结构可以是扣合结构、滑入结构、基于粘合剂的连接或所需的任何适当连接结构。

[0096] 图 13 示例说明不同的例子，其中，半透明标识构件 14 附着到传统交易卡的侧面或任何其它表面。半透明标识构件 14 可以沿折叠线 1400 折叠，或如果需要，可以是一种非折叠并形成为交易卡的一部分的厚度。也预期用于将半透明标识构件与交易卡附着的任何其它适当机构。

[0097] 图 14 和 15 示例说明基本上颠倒半透明标识构件和接收者单元的作用的另一实施例。在该实施例中，半透明标识符 14 包含可视过滤或增强图案 40，以及显示屏显示至少一个隐蔽标识符，其可以是例如表示根据需要，对用户唯一或不唯一的用户验证数据的数据（见图 15）。关于在前实施例，将半透明标识构件（可视过滤器）覆盖在显示隐蔽标识符的显示器上的组合显露出（不隐匿）或增强屏幕上的至少一个隐蔽标识符。然后，可以将显露的用户验证数据输入到适当的交易设备中作为口令字或其它用户验证信息。而且，当半透明区附着或包含在传统交易卡中时，如图 12 和 13 所示，交易卡包括例如包含交易卡号的第一部分和包含半透明标识号或其它识别信息的第二部分，其具有包括可视过滤图案的半透明区。

[0098] 图 16 示例说明采用图 14 的 TIDM 14 的系统 1600 的一个例子。在该例子中，TIDM 验证器 24 包括与用来生成参考图 1 所述的一个或多个标识符的类型类似的隐蔽标识符生成器 1602。隐蔽标识符生成器 1602 在从用户收到接收者特定信息，诸如用户名、TIDM 序列号或其它适当信息之后，生成隐蔽标识符，以保证向那个用户显示适当的隐蔽标识符。作为注册过程的一部分，用户已经提供了相同的用户特定信息，以及隐蔽标识符生成器 1602 可以已经生成隐蔽标识符并将它们存储在存储器 22 中。

[0099] 在该例子中，半透明标识构件发行器 12 生成 TIDM 14，该 TIDM14 具有在其上具有可视过滤图案 40 的半透明区，该可视过滤图案 40 被构造成可视地过滤显示的隐蔽用户标识符 38，并被构造成覆盖显示屏的至少一部分。可以期望用户输入用户特定信息来启动会话，其中，在半透明标识构件上打印相同的过滤图案用于多个用户。期望知道 TIDM 的持有者是适当用户而非偷取 TIDM 的小偷。验证器或其它源将生成的隐蔽标识符发送到接收者设备。接收者设备显示至少一个视觉上隐蔽的标识符作为用户验证数据，并接收表示基于其上具有过滤图案的半透明标识构件而显露的用户验证数据（诸如显露的 ID 本身或其表示）的数据。例如，当在显示器上保持其上具有过滤图案的半透明标识构件时，过滤器显露出用户标识符。如果需要，半透明标识符序列号可分配给每一 TIDM，即使在一个以上的 TIDM 上打印相同的过滤图案。如此，几个用户可以拥有具有相同过滤图案的半透明标识构件

[0100] 半透明标识构件发行器 12 用来生成具有半透明区的半透明标识构件 14，在所述半透明区上包括可视过滤图案 40，该可视过滤图案 40 被构造成可视地过滤显示的隐蔽用户标识符，并被构造成覆盖显示屏的至少一部分。隐蔽标识符生成器 1602 响应接收的用户信息，诸如用户特定信息，生成至少一个视觉上隐蔽的标识符用于在显示器上显示。在显示器上覆盖过滤图案之后，如上所述，半透明标识构件验证器 18，在该例子中，诸如通过用户通过用户界面输入信息，而接收表示显露的标识符的数据，半透明标识构件验证器将接收的显露标识符与相应的期望标识符进行比较（因为它由隐蔽标识符生成器生成），以便确定接收者的适当验证是否适合。另外，半透明标识构件验证器可以将接收的显露标识符发送到执行比较并将消息发送回验证器或接收者单元的第三方。根据需要，可以使用任何其它适当的操作划分。然后，响应与相应的期望标识符匹配的接收数据，半透明标识构件验证器或第三方将授权信息发送到接收者单元。

[0101] 图 17 示例说明用于安全地提供标识信息的方法的一个例子，包括基于例如接收的接收者保密数据或非保密数据或无关数据或从接收者接收的数据，生成用于接收者的至少一个隐蔽标识符。这如块 1700 所示。如块 1702 所示，该方法包括生成在其上具有可视过滤图案 40 的半透明标识构件 14。在已经制成 TIDM 后，该方法包括接收用户标识信息，诸如 PIN 或其它数据，作为用户验证的第一因素。如块 1704 所示，该方法包括将一个或多个隐蔽标识符发送到接收者，并显示至少一个视觉上隐蔽的标识符作为第二因素用户验证数据，当与半透明标识构件上的可视过滤图案 40 可视地结合时，显露出用于用户的隐蔽标识符。如块 1706 所示，该方法包括用户例如将半透明标识构件覆盖在显示器上，以便通过过滤器可视地识别隐蔽标识符。该方法还包括接收表示基于其上具有过滤图案的半透明标识构件而显露的用户验证数据的数据。该方法还包括诸如在显示隐蔽标识符之前，接收用户特定信息，以便确定将在显示器上显示的视觉上隐蔽的标识符。例如，由于每一用户最好具有不同的标识符，系统需要确定显示哪一隐蔽标识符。这可以通过例如让用户通过接收者单元中的用户界面输入用户特定信息，诸如口令字或其它保密或所需的非保密信息来确定。

[0102] 换言之，该方法包括诸如由 TIDM 验证器、服务供应商或其它适当的实体接收用户标识信息作为用户的第一验证因素，使用这些用户标识信息来识别包含已知与该用户有关的特定可视过滤图案的存储器中的半透明标识构件。该方法包括生成将被用作用于与接收

的用户标识信息有关的用户的第二验证因素的期望标识符，以及生成包含期望标识符的隐蔽用户标识符的图案，使得当隐蔽用户标识符的图案与该用户有关的识别的半透明标识构件上的可视过滤图案结合时，将显露出期望标识符。该方法包括将隐蔽用户标识符的图案传送到显示器（例如显示 GUI），并请求输入显露的标识符；以及接收表示显露的标识符的数据。如上所述，例如 TIDM 验证器、或任何适当数量的服务器或设备充当执行上述操作的电路。

[0103] 可以通过由能易于集成到当前体系结构中的一个或多个处理设备执行的应用编程接口 (API)，来提供公开的装置、方法和系统的主要功能。另外，在一个实施例中的每一半透明标识构件不同，并具有似乎不同的随机信息，因为似乎随机信息典型地但不一定是由接收者唯一的信息（诸如口令字、用户名、个人标识号）或任何其它信息生成的。在每一实施例中，能预先制造半透明标识构件和 / 或可视过滤器和 / 或隐蔽标识符，随后与用户相关联。另外，能预先生成隐蔽标识符和 / 或过滤图案，随后应用于半透明标识构件。可以由过滤图案或隐蔽标识符的创建者完成到半透明标识构件的这种后续应用，或可以由提供服务的实体或服务供应商的第三方立约人来完成。由于能通过非常简单的材料，诸如透明塑料来完成半透明标识构件的制造，因此，对服务供应商来说，也可以将隐蔽标识符或可视图案发送给用户，然后，用户自己将过滤图案或隐蔽标识符应用于半透明标识构件。

[0104] 同一半透明标识构件可以重复使用多次，因为在其上有多个不同的隐蔽标识符，其中，每次请求验证时，通过可视过滤图案来暴露隐蔽标识符的不同的一个。因此，如果需要，半透明标识构件上的可视显露标识符可在每次验证会话期间改变。在此所述的半透明标识构件可以用于用户验证、激活软件应用或用于任何其它适当目的。不同的隐蔽标识符可以是字母、图像或任何其它适当信息。

[0105] 图 18 示例说明物品 1800（例如构件）的一个例子，诸如半透明或非半透明膜、不干胶贴纸、卡或任何其它适当材料或物品。将意识到，物品 1800 上所示的信息仅示为一个例子，以及将意识到，可以使用任何适当的信息。在该例子中，物品 1800 包括位置信息 1802 和 1804（示为行和列标记）以及数字形式的发送验证信息 1806，该发送验证信息 1806 可通过坐标位置信息（例如行和列信息）来寻址或定位。另外，物品 1800 包括可选的物品标识符 1808，诸如由物品 1800 的发行器生成（例如分配）的序列号。

[0106] 一般来说，如果需要，可以如上所述相对于半透明标识构件来生成物品 1800，以便生成例如发送者验证信息。然而，另外，在一个实施例中，还需要添加位置信息 1802 和 1804。另外，将意识到，半透明标识构件 14 也可以用作发送者验证物品，以及隐蔽标识符 38 也可以用作发送者验证信息。

[0107] 另外，在该实施例中，如果系统不需要，则不需要接收者特定信息，因为如果期望，发送者验证信息可以独立于或基于接收者特定信息来生成。这可以在接收者签约服务时进行。另外，如在此所使用的，位置信息包括例如与消息一起发送或由发送者发送的表示接收者将校验物品 1800 上的哪一发送者验证信息的消息索引的信息。例如，位置信息不需要是行和列信息，而可以仅是术语，诸如“左上角”、“左下角”、“从右起第三”或任何其它适当的信息，来告知接收者物品上的哪一发送者验证信息将用作用于指定会话、交易或其它通信的验证信息。另外，发送者验证信息可以是指向包含发送者验证信息的位置的指针，诸如例如指向用于指定会话、交易或其它通信的发送者验证信息的统一资源定位符 (URL)。另外，

位置信息可以是指向包含实际位置信息的位置的指针，实际位置信息再表示在物品上的何处查看用于指定会话、交易或其它通信的发送者验证信息。在另一实施例中，位置信息是可视过滤图案。

[0108] 图 19 示例说明交易卡 1900，其可以包括例如磁条 1902 或可以提供帐户信息或消息发送者信息的任何其它适当信息。交易卡 1900 可以是例如上述银行卡、信用卡、借记卡或任何其它适当的交易卡，以及可以包括交易卡标识符信息，诸如卡号等。该交易卡 1900 不同于传统的交易卡，因为它还包括在其上、在其中或以任何适当方式固定到它的物品 1800（或构件）。如此，例如在图 13 中，示例说明了交易卡 1900 的变形。在一个例子中，如果需要，构件 1800，诸如胶衬纸或任何其它适当的构件被固定到传统的交易卡上。还将意识到，如上所述，可以通过任何适当的方式（包括但不限于胶粘）或任何其它适当的机构来固定或适当地粘贴所述构件或物品。构件 1800 还可以被发送到接收者作为财务报表、帐单报表等的撕掉部分。最好，尺寸化它以便安放在交易卡上。

[0109] 图 20 示例说明用于提供可以由任何适当的元件执行的电子消息验证的方法的一个例子。在该例子中，可以由服务器或多个服务器或在一个或多个处理设备上执行的其它适当的应用程序来执行它。如块 2000 所示，该方法包括例如当发送者（诸如银行服务器或其它消息发送者）希望将消息发送给接收者时，确定所需位置信息（诸如还存在于特定接收者物品上的行和列信息）和相应的所需发送者验证信息，相应的所需发送者验证信息被发送并与位于物品上并根据发送的位置信息来定位的发送者验证信息进行匹配。这可以例如通过访问一个数据库来完成，该数据库将例如接收者电子邮件地址链接到表示例如发行给那个接收者的物品的内容的相应数据库字段。如块 2002 所示，该方法包括向接收者发送电子消息以及所需位置信息及相应的所需发送者验证信息，其中，基于发送的所需位置信息，可在物品上定位所需发送者验证信息。如此，例如，发送者或发送者单元可以将行和列信息与应当出现在物品上的那些位置的相应发送者验证信息相关联（例如追加、预先计划、插入或者附加），作为到接收者的电子消息的一部分。然后，接收者可以基于接收的列和行号来定位由（代表）发送者发行给他们的物品上的发送者验证信息，并确认发送的所需发送者验证信息是否与由发送者单元所发送的发送位置信息表示的位置上的相同信息相匹配。如果出现匹配，那么接收者信任该信息的发送者。将意识到，发送的位置信息和发送者验证信息可以是数据本身、位置信息和发送者验证信息中的任一个的索引、函数、引用或任何其它适当表示。

[0110] 例如，位置坐标信息和相应的发送者验证信息可以包括电子传送的数据，用于在显示设备上显示，诸如可视过滤图案和发送者验证信息。在该实施例中，物品可以是透明物品，以允许用户将物品放在显示屏区域上。发送的消息将包括可视过滤图案以及所需发送者验证信息，当用户在显示屏上覆盖所述物品时，所需发送者验证信息应当可视地呈现给用户。如果接收者可视地识别出或看到通过屏幕上的可视过滤图案显露出的发送者验证信息，以及发送的所需发送者验证信息并且匹配，那么用户能信任该消息的发送者。如此，可以部分使用之前所述的用于接收者验证的半透明标识构件的可视过滤技术来验证发送者。

[0111] 还参考图 21，消息以及相关的发送者验证信息和位置信息的具体例子示为 2100。在特定实施例中，也参考图 18，所述消息被追加发送者验证信息（具体是数字“98413”）以及坐标信息“A2，E4，F1，H4，J2”。如此，发送者单元发送电子消息，连同所需的发送者验证

信息和所需位置信息，如图所示。然后，用户使用物品 1800 并查看例如坐标位置 A2 并看到数字 9，查看位置坐标 E2 并看到数字 8，查看坐标位置 F1 并看到数字 4，查看坐标位置 H4 并看到数字 1，以及查看坐标位置 J2 并看到数字 3。如果用户在物品 1800 上看到与发送者单元发送的相同发送者验证信息，那么，接收者将该发送者信任为可信消息发送者。在该例子中，发送者验证信息可视地表示可由行和列形式的位置坐标信息识别的发送者验证信息。然而，将意识到，不需要使用行和列格式，以及不需要采用所示的单元。例如，如果使用物体而非字母和数字，则物体可以位于物品和发送者验证信息的左上、右上、中间或任何其它适当的位置，其可以是可被发送的物体，诸如图形形式或其它适当的物体，以及坐标位置信息实际上可以是读取“左上角”的单词。也可以使用任何其它适当的坐标位置信息或发送者验证信息。

[0112] 上面提到的物品 1800 可以是例如纸、塑料卡、透明塑料卡、能贴在现有塑料卡或任何其它适当物品上的不干胶贴纸。在该例子中，每一电子邮件接收者具有带有其自己随机（或似乎随机）生成的内容的物品。当发送电子邮件时，发起人的消息传送代理或其它服务器部件使用 URL 或其它适当引用、坐标或用于定位一个或多个卡单元或位置的其它方向，诸如通过链接，直接或间接地将每一出站电子邮件与 HTML 页相关联。而且，追加、预先计划、插入或者附加到电子邮件的是那些位置处的内容。在接收后，用户使用他们个人的发送者验证物品来确认查找结果，诸如阅读电子邮件中列出的坐标并在他们自己的发送者验证物品上查找它们。在使用验证物品的半透明版本的情况下，验证物品可以放在电子邮件提供的可视过滤图案上，以及由接收者将显露出的发送者验证信息与电子邮件中提供的所需发送者验证信息进行比较。如果字母或其它信息不匹配，那么验证失败。

[0113] 图 23 更详细地示例说明用于提供电子消息验证的方法，其中，该方法包括如块 2300 所示，生成例如将放在物品上的随机发送者验证信息，如果需要，生成也可以放在物品的位置信息，并将两者与被选接收者链接。随机包括伪随机信息或信息的任何适当随机化等级。这可以如之前相对于半透明标识构件所述通过一个或多个服务器计算机或任何其它适当设备上的适当接口来实现。如块 2302 所示，该信息存储为适当数据库中的验证信息和相应的位置信息。如块 2304 所示，该方法包括创建物品（诸如物品 1800），其包含位置坐标信息和相应的发送者验证信息，如果需要，包含物品标识符 1808，诸如发行给指定接收者的序列号。这可以例如以基本上与上述类似的方式来实现。例如，可以印刷卡，可以适当地形成交易卡，或可以生成能粘贴到任何适当物品上的不干胶贴纸。然后，将该物品通过邮寄或任何其它适当的渠道发送给接收者。

[0114] 在另一实施例中，代替使用硬令牌类型（例如物品），可以使用软令牌，其中，在每次会话期间或一次性地，将例如卡的表示（可以不是实际图像）或物品的表示电子地发送给用户，用于经显示屏显示或用于该用户的其它电子访问，以及用户可以将电子发送者验证物品存储在文件中，并当需要时访问它。如此，可以通过软件应用来访问物品的电子表示，以便向接收者提供位于由发送的位置信息识别的位置处的发送者验证信息。

[0115] 如块 2306 所示，该方法还包括例如参考图 20 所示，诸如由发送者确定位置信息和相应的发送者验证信息的至少一个所需项，以便追加、预先计划、插入或者附加到当前消息。可以用任何适当的方式，诸如随机或以所需的任何其它适当方式来实现位置信息和验证信息的选择。如虚线块 2308 所示，在另一实施例中，以可视过滤图案的形式，有效地传送

位置信息和发送者验证信息，如果需要，可视过滤图案可以覆盖所有行和列标题，当物品被覆盖时，仅允许可视地显示发送者验证信息。如此，该方法可以包括将用于显示的可视过滤图案发送给接收者，以便允许接收者可视地确定发送者是否可信。接收者可以将物品上的发送者验证信息的至少一部分放在显示屏上显示的可视过滤图案上，以便确定随消息发送的发送者验证信息是否与通过可视过滤图案可见的发送者验证信息相匹配。

[0116] 在一个例子中，该方法包括将位置信息和相应的发送者验证信息的至少一个所需项追加到用于接收者的电子消息。发送者验证信息可视地表示可由位置坐标信息识别的验证信息。如此，可以将消息本身追加、预先计划、插入或者附加到信息上，或可以包含信息的引用，诸如网站或任何其它适当链接或发送者验证信息和位置坐标信息的任何其它适当表示。

[0117] 如块 2310 所示，该方法包括将电子消息和表示位置坐标信息和相应的发送者验证信息的数据发送给接收者。然后，接收者可以查看物品上的信息，并看它是否与由发送者单元所发送的信息匹配。

[0118] 还将意识到，可以动态地实现基于位置信息和相应的发送者验证信息来确定至少一个位置坐标，而不是查找存储在数据库中的信息。例如，可以通过函数来简单地编程发送者（例如消息发送者单元），以便生成发送者验证信息来发送，而不是查找预先存储的信息。

[0119] 而且如果需要，发送者验证信息可以是例如诸如银行报表上的期末结余、发送者先前已经发送给接收者的可以包含发送者验证信息的帐单报表或帐户报表中的任何适当信息。位置信息可以是特定报表的日期，以及发送者验证信息可以是信用卡帐户上的当前余额。也可以使用任何其它报表或可以使用接收者拥有的已知或发送者单元提供的任何其它信息。

[0120] 图 22 示例说明用于提供电子消息验证的系统的一个例子，如果需要，可以执行参考图 23 所述的步骤。例如，发送者单元 2200（诸如任何服务器计算机、多个服务器、移动设备或任何其它适当的结构）可以包括发送者验证物品发行器 2202，或根据需要，第三方可以发行发送者验证物品。例如，发送者验证物品发行器 2202 可以生成随机发送者验证信息和相应的位置坐标信息，并将它与接收者链接，并将该信息存储在数据库 2204 中。然后，可以将物品 1800 邮寄给接收者，或在软令牌的情况下，电子发送给接收者。在该示例中（图 22），示出了半透明物品。如此，接收者 20 包括显示器 30，以及与可视过滤图案和发送的发送者验证信息一起，在显示器上显示消息 2100。然后，使用该可视过滤图案来显露期望的发送者验证信息，然后，由接收者与在消息 2100 中发送的信息进行匹配。在该实施例中，发送者验证物品是半透明型，由于接收者将发送者验证物品覆盖在显示器上的结果将导致在物品中的特定位置处可视显露的发送者验证信息，由发送者单元发送的可视过滤图案体现位置信息。如此，可视过滤图案包括位置信息，另外，将意识到，术语“信息”指任何适当的标记。

[0121] 可以是网络、节点或任何其它适当设备中的适当服务器的发送者单元 2200 包括一个或多个电路，所述电路可以是执行存储在存储器中的软件指令的一个或多个处理设备的形式，或可以使用分立逻辑来实现，或是执行在此所述的操作的硬件、软件或固件的任何适当组合。如此，发送者单元 2200 包括用来执行上述步骤的电路。

[0122] 在另一实施例中，可以例如与上述相对于半透明标识构件的系统结合使用发送者验证物品，使得半透明标识构件在其上包括位置信息和发送者验证信息。例如，如果需要，隐蔽标识符也可以用作发送者验证信息，或在另一实施例中，半透明标识构件可以具有包括隐蔽标识符的部分和包括位置信息和发送者验证信息的另一部分。在任一情况下，使用如此所述为半透明的单个物品或构件能提供多级验证。例如，对于发送者验证，可以采用参考图 18-22 所述的方法来确认发送者可信。一旦例如使接收者确信电子邮件的发送者是可信的，则接收者可以点击在电子邮件消息中发送然后以适当的 HTML 形式呈现的 URL，以便输入帐户信息或其它保密信息。然而，在输入该保密信息之前，可以采用半透明标识构件和隐蔽标识符来执行第二级验证，使得在该会话或交易阶段，发送者单元可以验证接收者。还将意识到，也可以采用任何其它适当的操作顺序或验证方案的组合。

[0123] 另外，要求术语的使用包括其任何表示。例如，术语“发送者验证信息”包括数据本身、数据的任何索引、数据的任何引用或指针，或其任何其它表示。

[0124] 除其它优点，不需要对接收者的消息传送代理或电子邮件客户机做任何修改。而且如果期望，不需要注册接收者计算机，允许如果需要，由任何计算机执行验证。该系统也可以适用于移动设备，其中，可以在小的显示屏上容易地显示查找坐标。其它验证目的可以包括 web 验证、交互式语音响应验证或任何验证情形。另外，与要求智能卡、令牌或公钥体系结构的更复杂技术相比，该系统和方法提供廉价机构类型，诸如能分发的验证卡。本领域的普通技术人员将意识到其它优点。

[0125] 图 24 示例说明提供用户（例如接收者单元）和发送者单元（也称为目标源）之间的相互验证的系统 2400 的一个例子。如参考图 18-23 以及别处所述，在该例子中，物品 1800 用作分配给每个终端用户的验证卡，并包括例如仅由发送者单元（例如目标源）和终端用户已知的随机和 / 或唯一标记。通过向接收者提供那一知识的证据，发送者单元能证明其身份，以及通过终端用户使接收者单元返回位于验证卡中的信息，终端用户能将他 / 她的身份证明为适当终端用户。

[0126] 如上所述，系统 2400 可以包括发送者验证构件发行器 2202，其基于例如可以是但不限于例如口令字和 / 或用户 ID 的接收者特定信息 32（即用户验证信息）而产生物品 1800，系统 2400 还包括发送者单元 2402，其可以是服务器或如前所述的任何适当设备，以及也可以包括如前所述，执行在此所述的操作的一组服务器或电路。系统 2400 还包括与在前所述的数据库类似的数据库 2404，在该例子中，也存储允许执行第一级用户验证操作的用户验证信息 32。另外，如上所述，数据库 2404 还存储位于物品上的发送者验证信息和物品标识符，使得发送者单元 2402 可以提供第二级验证过程，如在此所述。

[0127] 发送者单元 2402 还包括例如存储器，其包含当由一个或多个处理设备执行时，作为第一级用户验证器 2406 和第二级验证器 2408 操作的可执行指令。如上所述，然而，将意识到，可以由可通过互联网、内联网或任何适当的网络定位或访问的分离服务器或其它计算单元来执行这些操作。也将意识到，可以无线地传送在此所述的通信，其中，接收者单元 20 是无线手持设备或其它适当的便携式无线设备。

[0128] 还参考图 24，描述用于提供用户和发送者单元（诸如目标源）之间的相互验证的方法。如上所述的物品可以包括交易卡、不具有任何交易信息的卡、半透明卡、电子卡（例如可视显示卡），所述电子卡可以例如存储在接收者单元或任何其它适当单元上的存储器

中，然后在用户请求后显示给用户，或响应询问的接收而自动显示给用户，或物品可以采用任何其它适当形式。而且，在询问中发送的位置信息包括例如电子传送的数据，用于在显示设备中显示。如上所述，这可以采用行和列信息或任何其它适当信息的形式，所述信息可以被电子地传送并例如在显示器 30 上显示给用户或可听地呈现。将假定对于该实施例，用户已经收到发送者验证物品 1800，以及在该例子中，这不是半透明物品，因此在该例子中，不需要使用可视过滤器。然而，将意识到，可以对于任何适当的物品，包括半透明卡或物品，适当地执行在此所述的操作。例如，可以通过图 24 所示的系统，或通过任何适当系统或结构来执行该方法。在该例子中，物品标识信息不需要由发送者单元 2402 发送到接收者单元。然而，如果需要也可以发送。在该例子中，发送者单元 2402 重复地校验以便查看对于发送的询问的应答是否包括与期望的（例如发送者期望的）发送者验证信息匹配的、由发送的询问中的位置信息识别的发送者验证信息。如果没有，在会话期间或在多个会话上重复发送多次询问，直到由发送单元接收的所需发送者验证信息与期望的验证信息匹配为止。

[0129] 尽管图 25 中未示出，可以初始地执行第一级验证过程。例如，这可以包括从接收者单元 20，由此从用户接收用户验证信息 2410，用户验证信息可以包括例如用户口令字和用户 ID。这可以例如由第一级用户验证器 2406 接收。然后，第一级用户验证器 2406 通过使用例如从数据库 2402 获得的用户验证信息 32，基于接收的用户验证信息 2410 来验证用户。如果它们匹配，则用户验证成功。然后，将“是”表示 2412 发送到第二级验证器 2408，表示可以执行第二验证过程。最好例如在第一级验证过程期间，实现锁定机制，诸如限制在第一级验证过程期间验证尝试的次数，防止强力攻击。在成功完成第一验证步骤之后，提示用户通过物品特定信息来验证，如下所述。

[0130] 如块 2500 所示，该方法包括对于已被分配物品 1800 的用户，确定对应于物品上所包含的发送者验证信息的所需发送者验证信息。这可以由第二级验证器 2408 来完成，所述第二级验证器 2408 例如基于用户验证信息 32，从位于物品 1800 上的数据库 2404 中适当地选择发送者验证信息。如上所述，由发送者验证构件发行器 2202 将物品上的标记存储在数据库 2404 中。由用户通过使用位置信息，诸如行和列标识符，或如上所述的任何其它适当的位置信息，将发送者验证信息定位于物品 1800 上。

[0131] 如块 2502 所示，该方法包括诸如由发送者单元 2402 发送对于用户的询问，所述询问至少包括识别能位于物品 1800 上的所需发送者验证信息的位置信息。所述询问可以包括例如一个或多个坐标集，例如经显示器 30 显示给用户。所述询问对于每一用户最好是特定的，以及必须基于来自第一级用户验证过程的身份或用户验证信息被检索。这确保了用户被呈现同一询问直到成功验证完成为止。重复同一询问能防止攻击者基于例如可以使用各种潜在攻击机制获得的仅少量用户卡内容的知识来安装强力攻击。然后，一旦用户已经通过第二级验证过程成功地验证，则执行并存储随机生成的询问。询问 2414 可以以任何适当的方式发送，并可以采用适当的方式，包括但不限于 SSL 通信或如果需要，不保密通信。如块 2504 所示，该方法包括接收对于发送的询问的应答。在该例子中，从接收者单元 20 接收表示为 2416 的应答，所述应答是在用户的控制下，例如使用在询问 2414 中发送以便确定位于卡上的发送者验证信息的位置信息，诸如行和列 ID 由接收者单元生成的。响应询问，用户通过适当的用户界面输入该信息。如此，根据图 24-28 的实施例，所述应答包括从物品获得的期望（发送者单元所期望）的发送者验证信息。该应答信息（尽管被称为“发送者

验证信息”）实际上用来由发送者单元或其它实体来验证用户，因为该应答包含仅可由验证卡的持有者获得的信息。

[0132] 如块 2506 所示，该方法包括诸如由发送者单元 2402 确定接收的对于询问的应答是否包括由询问中所发送的位置信息识别的所需发送者验证信息。如块 2508 所示，如果应答中接收的发送者验证信息不是通过位置信息在询问中识别的所需发送者验证信息，那么，在该例子中，发送者单元 2402 将包含先前发送的相同位置信息的相同询问重新发送给接收者单元 20。如块 2510 所示，该方法包括重复分析接收的应答，以及如果所述应答不包括基于询问中发送的位置信息的所需发送者验证信息，则发送者单元在同一会话期间传送同一询问，直到收到的应答包括物品上的所需发送者验证信息为止，或直到已经尝试由例如发送者单元设置的适当尝试次数为止的步骤。重复询问直到应答包括所期望的所需发送者验证信息为止。

[0133] 图 26 示例说明用于在用户和发送者之间提供相互验证的另一方法，以及可以例如由图 24 的系统 2400 或任何其它适当系统或设备来执行。在该例子中，不执行重复发送同一询问直到接收适当应答为止。在该实施例中，除询问中的位置信息外，还将物品标识信息，诸如位于物品上的序列号或任何其它的适当物品标识发送给用户。如块 2600 所示，该方法包括诸如由发送者单元 2402 确定对应于物品上所包含的发送者验证信息的所需发送者验证信息，以及还确定用于同一用户的相应物品标识信息，诸如物品上的序列号或共享保密或任何其它适当标识信息。如块 2602 所示，该方法包括向用户发送对用户的询问，包括用于验证发送者单元的确定的位置信息和物品标识信息。

[0134] 如块 2604 所示，该方法包括基于对询问的应答来验证用户，其中，该应答包括基于位置信息从物品获得的发送者验证信息。在该例子中，用户例如不输入或发送对询问的应答，除非用户校验出在询问中发送的物品标识信息与在物品本身上的物品标识信息相匹配。如此，用户可以基于物品标识信息来验证发送者单元。同样地，在该例子中，除位置信息外，所述询问包括物品标识信息。所述应答包括由位置信息限定的、位于物品上的发送者验证信息。如果询问中的物品标识符与用户所拥有的物品上的物品标识符相匹配，那么用户信任发送者单元。如块 2606 所示，该方法包括基于对询问的应答来验证用户。在该例子中，最好再次执行基于用户口令字和 / 或用户 ID 的先前所述的第一级验证。如果该级验证成功，那么可以适当地执行图 26 所示的方法。如所提到的，物品标识信息可以包括用户和发送者已知的共享秘密，或可以是物品序列号或任何其它适当信息。

[0135] 图 27 示例说明有效地结合图 25 和 26 所示的一些操作的提供用户和发送者之间的相互验证的另一方法。如块 2700 所示，该方法包括诸如通过提示输入第一级用户验证信息来执行第一验证过程。这可以包括例如发送者单元发送请求或向用户提供输入口令字或用户 ID 的提示。作为响应，发送者单元接收第一级用户验证信息，诸如口令字，以及校验存储的用户验证信息 32（例如接收口令字的散列），以确保接收的第一级用户验证信息正确。如块 2702 所示，如果第一级验证成功，该方法包括确定用于用户的对应于物品上所包含的发送者验证信息的所需发送者验证信息，以及例如，确定可位于物品上的物品标识信息。如此，在该例子中，在询问中发送位置信息和物品标识信息。然后执行先前参考图 25 和 26 所述的步骤，以便例如重复地发送询问，其中，询问是同一个询问，直到在应答中接收到正确的发送者验证信息为止。同样地，用户确认来自询问的物品标识符的显示与他们卡上的标

识符匹配。这将发送者单元或目标组织验证为只有它和终端用户知道该标识符的知识。用户通过查看在询问中发送的位置信息处的卡内容，来输入对询问的适当响应。发送者单元能校验所述应答，以及仅当具有该卡的终端用户能正确地响应询问时，才验证用户。将意识到，在例如互联网的环境中描述操作，但这些操作同样地适用于通信的其它信道，诸如交互式语音响应或任何其它适当的通信系统。例如，当使用交互式语音响应时，通过经由无线或有线电话网来自例如自动化系统的语音来提供用户提示。经按钮音键盘代替例如通过 web 形式输入来提供用户响应。也可以使用任何其它适当的通信系统。

[0136] 除其它优点，所述装置、系统和方法提供了终端用户和发送者单元或目标组织之间的安全验证，以及与更复杂的技术，诸如智能卡、硬件令牌或公钥体系结构相比，可以相对容易地使用和相对廉价地生产和分发这些验证卡。另外，使用跨越用于移动设备、非移动设备、语音激活设备或任何其它适当设备的多个通信信道的 web 客户机，可以易于实现该系统。

[0137] 图 28 图示地表示上述操作。例如，如通过通信 2800 所示，向用户提供传统的用户名和口令字登录屏，以及用户输入他们的用户名和口令字，并将它作为登录响应 2800 发送给发送者单元 2402，然后，如本领域所公知的，通过将接收的口令字和用户 ID 与例如口令字数据库 2802 中所存储的那些进行比较来执行验证过程。如果确认成功，发送者单元 2402 将询问 2414 发送给接收者单元，询问具有例如用户卡标识符，以及询问包括位置信息以便用户能定位卡上的特定标记。该询问例如在接收者单元上显示给用户。用户确认接收的卡标识符和用户拥有的验证卡上的卡标识符，并通过将应答 2416 发送回发送者单元 2402 来回答询问。然后，由发送者单元验证该应答以便验证用户以便结束相互验证。然而，如果第二级验证不成功，发送者单元将重复地发送同一询问，即，将相同的位置信息返回给接收者单元，直到接收到正确的应答为止。

[0138] 在图 29 中，示出了用于当用户离线时，验证接收者单元的用户的另一方法。当用户通过接收者单元 2915 与发送者单元 2920 在线时，能将一个或多个询问 - 应答集 2975 存储在接收者单元 2915 的存储器 2960 中。存储器 2960 可以是能存储询问 - 应答集 2975 的任何类型的存储设备。例如，存储器 2960 可以包括一个或多个磁性或光学存储设备或任何其它适当的存储设备。可以用任何适当的方式来构造存储器 2960，诸如高速缓存或非高速缓存存储器。基于接收者单元 2915 与发送者单元 2920 以前的在线通信，将每一个询问 - 应答集 2975 与物品 1800 相关联。每一个询问 - 应答集 2975 至少包括询问 - 应答对 2965 和 2970，在用户的在线验证期间存储在接收者单元 2915 的存储器 2960 中，以便接收者单元 2915 上的特定资源可以用于用户。当用户离线以及如果仅有一个询问 - 应答集 2975 存储在存储器 2960 中时，选择该存储的询问 - 应答集 2975，用于用户对可通过接收者单元 2915 获得的特定资源的离线验证。当用户离线以及多个询问 - 应答集 2975 存储在存储器 2960 中时，选择多个存储的询问 - 应答集 2975 中的至少一个，用于用户对可通过接收者单元 2915 获得的特定资源的离线验证。

[0139] 用户可以用来对发送者单元 2920 的询问进行应答的物品 1800 可以是相对于当前公开的各个实施例，如上所述的验证物品中的任何一个。例如，参考图 18，物品 1800 可以是半透明或非半透明膜、不干胶贴纸、卡或任何其它适当的物品。将意识到，物品 1800 上所示的信息仅示为一个例子，以及将意识到，可以使用任何适当的信息。在图 18 所示的例子

中，物品 1800 包括位置信息 1802 和 1804（被示为行和列标记），以及以可通过坐标位置信息（例如行和列信息）寻址或定位的数字形式的发送者验证信息 1806。另外，物品 1800 包括可选的物品标识符 1808，诸如由物品 1800 的发行器生成（例如指定）的序列号。然而，本领域的普通技术人员将意识到，物品 1800 可以是根据当前公开的各个实施例所述的验证物品中的任何一种，或可以采用任何适当的形状或形式。

[0140] 可以是网络、节点或任何其它适当设备中的适当服务器的发送者单元 2920 可以包括一个或多个电路，所述一个或多个电路是执行存储在存储器中的软件指令的一个或多个处理设备的形式，或可以使用分立逻辑或硬件、软件或固件的任何适当组合来实现，以执行在此所述的操作。同样地，发送者单元 2920 包括用来执行如上和下文所述的步骤的电路。发送者单元 2920 可以直接与接收者单元 2915 通信。另外，发送者单元 2920 也可以包括网络接口，用于直接或通过互联网 26、内联网或任何适当网络与接收者单元 2915 通信。网络接口可以可操作地耦合到发送者单元 2920 的处理设备。

[0141] 发送者单元 2920 也可以包括存储器，该存储器包含当由一个或多个处理设备执行时，作为第一级用户验证器 2905 和第二级验证器 2920 操作的可执行指令。如上所述，然而，将意识到，可以由单独的服务器或位于或可通过互联网 26、内联网或任何适当网络访问的其它计算单元来执行这些操作。还将意识到，可以例如无线地传送在此所述的通信，其中，接收者单元 2915 是无线手持设备或其它适当的便携式无线设备。

[0142] 可以是网络中的适当服务器、节点或任何其它适当设备的接收者单元 2915 可以包括一个或多个电路，所述一个或多个电路可以是执行存储在存储器中的软件指令的一个或多个处理设备的形式，或可以使用分立逻辑或执行在此所述的操作的硬件、软件或固件的任何适当组合来实现。同样地，接收者单元 2915 包括用来执行上文和下文所述的步骤的电路。接收者单元 2915 可以直接与发送者单元 2920 通信。另外，接收者单元 2915 可以包括用于直接或通过互联网 26、内联网或任何适当网络与发送者单元 2920 通信的网络接口。网络接口可以操作地耦合到接收者单元 2915 的处理设备。

[0143] 接收者单元 2915 也可以包括存储器，所述存储器包含当由一个或多个处理设备执行时，作为第一级用户验证器 2406 和第二级验证器 2408 操作的可执行指令。如上所提到的，然而，将意识到，可以由位于或通过互联网、内联网或任何适当网络访问的单独服务器或其它计算单元来执行这些操作。还将意识到，可以例如无线地传送在此所述的通信，其中，接收者单元 20 是无线手持设备或其它适当的便携式无线设备。

[0144] 参考图 29，当用户希望登录到接收者单元 2915 以便使用接收者单元 2915 的一个或多个资源时（所述资源诸如但不限于在有权访问前要求用户验证的软件应用、设备过程、外围设备、文件、其它存储数据或任何实体），可以初始地执行第一级验证过程。例如，这可以包括从接收者单元 2915 由此从用户接收用户验证信息 2935，所述用户验证信息可以包括例如用户口令字和用户 ID。这可以例如由第一级用户验证服务器 2905 接收。然后，第一级用户验证服务器 2905 通过使用例如从数据库 2910 获得的用户验证信息，基于接收的用户验证信息 2930 来验证用户。如果它们匹配，则用户验证成功，并可以执行用户的第二级验证。

[0145] 在第二级验证过程期间，可以向用户提供多个询问 2945，用户能通过包含在物品 1800 上的信息，对此提供应答 2950。对于已经被分配物品 1800 的用户，可以从发送者单元

290 请求询问。该询问可以是发送者验证询问，响应在询问中发送的位置信息，可以要求包含能在物品 1800 上找到的信息的应答。例如，通过使用位置信息，诸如行和列标识符，或如上所述的任何其它适当的位置信息，由用户在物品 1800 上定位发送者验证信息。

[0146] 询问 - 应答集 2975 可以包括如上文详细所述的第二级用户验证，诸如用于用户的询问，其至少包括识别可以位于物品 1800 上的所需发送者验证信息的位置信息。询问 2945 可以包括例如一个或多个坐标集，例如经接收者单元 2915 显示给用户。询问 2945 对每一用户可以是特定的，以及必须基于来自第一级用户验证过程的身份或用户验证信息来检索。然后，一旦用户已经成功地通过第二级验证过程的验证，则执行随机生成的询问并存储在接收者单元 2915 的存储器 2960 中。因此，当用户在线时，存储一个或多个询问 - 应答集 2975，即，存储在接收者单元 2915 的存储器 2960 上。询问 2945 可以以任何适当的方式发送，以及可以采用任何适当的形式，包括但不限于 SSL 通信，或如果需要，包括非保密通信。询问 2945 也可以在发送给用户之前基于加密信息。例如，加密信息可以基于散列函数。

[0147] 除一个或多个询问 - 应答对外，每一个询问 - 应答集可以包括用户标识信息、物品 1800 的标识信息、时间录入数据、表示是否离线使用存储的询问 - 应答集的标记、已经离线使用存储的询问 - 应答集的次数、和 / 或在完成用户的成功验证后，可由用户访问的接收者单元的特定资源的标识。

[0148] 图 30 示例说明用于提供接收者单元 2915 和发送者单元 2920（诸如目标资源）之间的相互验证的上述方法，其中，将一个或多个询问应答集存储在接收者单元 2915 中。所公开的方法在块 3015 确定用户是否在线。如果用户在线，接收者单元 2915 向发送者单元 2920 请求询问。然后，在块 3025，将询问发送给用户。如上文详细所述，用户应答该询问。在块 3030，将应答发送给发送者单元 2920。在块 3035，接收者单元 2915 从发送者单元 2920 接收验证的确认。在块 3040，接收者单元 2915 将询问 - 应答集 2975 的副本存储在存储器 2960 中，用于离线再用。

[0149] 当将多个询问 - 应答集 2975 存储在存储器 2960 中时，每次接收者单元 2915 尝试与发送者单元 2920 成功登录并完成成功询问 - 应答集时，接收者单元 2915 可以在其存储器 2960 中存储成功的询问 - 应答集 2975。当仅将一个询问 - 应答集 2975 存储在存储器 2960 中时，每次接收者单元 2915 尝试与发送者单元 2920 成功登录并完成成功询问 - 应答集时，接收者单元 2915 能将该询问 - 应答集 2975 存储在存储器中。询问 - 应答集 2975 的存储可能需要覆盖存储器 2960 中先前的询问 - 应答集 2975。

[0150] 然而，另外，在存储器 2960 中存储的询问 - 应答集 2975 可以不基于成功登录尝试。每次用户登录到接收者单元 2915 以及接收者单元 2915 与发送者单元 2920 在线时，发送者单元 2920 可以向接收者单元 2915 发送不是基于用户的成功登录而存储在存储器 2960 中的询问 - 应答集。例如，当用户登录到发送者单元 2920 时，一个或多个询问和基于物品 1800 的相应应答可以被存储在存储器 2960 中，其不一定是任何用户的成功询问 - 应答集的副本。

[0151] 可以由接收者单元 2915 或发送者单元 2920 的用户来预定或限制可以存储在存储器 2960 中的询问 - 应答集 2975 的数量。例如，如前所述，可以将仅一个询问 - 应答集 2975 存储在存储器 2960 中用于离线使用。因此，向用户提供仅一个到接收者单元 2915 的离线登录。例如，如果将存储多个询问 - 应答集 2975，则可以在接收者单元 2915 的存储器

2960 中，仅存储最多十个成功的询问 - 应答集 2975。当在接收者单元 2915 的存储器 2960 中存储的询问 - 应答集 2975 的数量为预定最大值时，接收者单元 2915 可以停止将另外的询问 - 应答集 2975 存储在存储器 2960 中，或通过覆盖当前存储的询问 - 应答集 2975 来继续将成功的询问 - 应答集 2975 存储在存储器 2960 中，以便不超出可以在存储器 2960 中存储的预定最大多个询问 - 应答集 2975。然而，数量可以不预定，以及可以通过来自接收者单元 2915 的 GUI 界面由用户选择。

[0152] 在图 31 中描述了当用户离线时，向用户提供可通过接收者单元 2915 获得的特定资源的方法。在块 3110，接收者单元 2915 确定用户离线还是在线。如果用户在线，则在块 3010，接收者单元 2915 将按照图 30 所示的流程图。如上所述，当多个询问 - 应答集 2975 存储在存储器 2960 中时，当用户离线时，可以将接收者单元 2915 的用户限定到仅预定多次登录到发送者单元 2920。因此，如果接收者单元离线，该方法将进入块 3113，其中，接收者单元 2930 确定询问 - 应答验证尝试是否大于或等于预定容许最大上限。如果询问 - 应答验证尝试大于或等于预定容许最大上限，该方法将进入图 32 的块 3155。如果询问 - 应答验证尝试不大于或等于预定容许最大上限，该方法将进入图 31 的块 3115，其中，接收者单元将选择存储在其存储器 2960 中的成功的询问 - 应答集 2975 中的一个。如果在存储器 2960 中仅存储一个询问 - 应答集 2975，则该方法可以跳过块 3113，并直接从块 3110 进入块 3115，其中，接收者单元将选择存储在存储器 2960 中的存储的询问 - 应答集 2975。然后，该接收者单元 2915 允许用户基于存储器 2960 中存储的询问 - 应答集 2975 中的一个，登录到接收者单元 2915。

[0153] 如块 3120 所示，接收者单元 2915 向用户提供来自存储器的被选询问信息。可以在接收者单元 2915 的显示器上可视地和 / 或可听地向用户提供询问信息。用户通过传送应答来响应该询问，如块 3125 所示。在块 3130，将用户的应答与对应于用户响应的询问的存储的应答进行比较。如由判定块 3135 所示，如果用户对询问的应答与存储的应答相同，那么授权用户访问接收者单元 2915 的资源，如块 3145 所示。因为用户已经使用成功的询问 - 应答集 2975，在块 3140，接收者单元递增使用计数器，即，使用询问 - 应答集 2975 的次数，以表示使用了询问 - 应答集 2975 并授权。可以将最大预定离线验证尝试次数分配给一个标记，即变量。如果询问 - 应答验证尝试大于预定容许最大上限，即，计数器大于所述标记，则在块 3115，由接收者单元 2915 通知用户采取其它动作。其它动作可以简单需要用户联系发送者单元 2920 的管理员，以便接收访问接收者单元 2915 的资源的口令短语，如下文所述。

[0154] 当用户成功地完成在线验证时，由发送者单元 2920 生成一个随机的保密口令短语，可选地，加密保护（例如散列）并由发送者单元 20 自动发送并存储在接收者单元 2915 的存储器 2960 中，而用户不知道。该口令短语也在用户标识信息下保存在发送者单元 2920 中，连同成功验证后也在其上存储该口令短语的接收者单元 2915 的身份。如果用户需要访问接收者单元 2915 的资源但已经超出容许的离线验证尝试次数，则用户可以与发送者单元 2920 的管理员联系以便接收该口令短语。然后，在由发送者单元 2920 的管理员提供给用户的口令短语和存储在接收者单元 2915 中的口令短语匹配之后，用户能使用该口令短语来访问接收者单元 2915。

[0155] 参考图 33，示出了当用户离线时，提供接收者单元 2915 的用户的验证的另一方

法。在图 33 所示的方法中，每次用户与发送者单元 2920 在线时，接收者单元 2915 可以不将成功的询问 - 应答集 2975 存储在存储器 2916 中。在图 33 所示的方法中，仅当用户请求将询问 - 应答集 2975 存储在接收者单元 2915 的存储器 2960 中时，才将成功的询问 - 应答集 2975 存储在接收者单元 2915 中。例如，如果用户在进入离线之前，知道他将使用接收者单元 2915 而不是与发送者单元 2920 在线，则用户可以请求将一组询问 - 应答集 2975 存储在接收者单元 2915 的存储器 2960 中，如图 33 的块 3315 所示。将这种请求发送到发送者单元 2920 并由发送者单元 2920 接收，如块 3330 所示。发送者单元 2920 通过向接收者单元发送用于存储到存储器 2960 中的一组询问 - 应答集 2975，来响应该请求。如块 3320 所示，接收者单元 3305 接收询问 - 应答集 2975 并将询问 - 应答集 2975 存储在存储器 2960 中。一旦将询问 - 应答集 2975 存储在存储器 2960 中，接收者单元 3305 可以离线，以及允许用户通过响应存储在存储器 2960 中的询问 - 应答集 2975，在离线的同时，访问接收者单元 2915 的资源，如上文详细所述。每次由接收考单元 2915 的特定用户进行这种请求时，发送者单元 2920 根据在块 3345 实现的用于这种接收和响应请求的存储规则，触发接收请求和响应请求过程的在线刷新，如块 3330 和 3340 所示。

[0156] 接收者单元 2915 可以由单个用户使用来访问发送者单元 2920。接收者单元 2915 可以是诸如当用户正旅行并且不能执行在线验证时可离线使用的任何适当设备，诸如但不限于膝上型电脑、移动电话、PDA 或电子邮件设备。当用户与发送者单元 2920 在线时，在接收者单元 2915 将多个询问 - 应答集 2975 存储在接收者单元 2915 的存储器 2960 之前，接收者单元 2915 清除（例如覆盖或删除数据）已经存储来自先前用户的多个询问 - 应答集 2975 的接收者单元 2915 的存储器 2960 的一部分。因此，每次新用户与发送者单元 2920 在线时，接收者单元 2915 可以在存储用于接收者单元 2915 的当前用户的多个询问 - 应答集 2975 之前，清除存储器 2960。

[0157] 当接收者单元 2915 离线时，可以由多个用户使用接收者单元 2915 来访问发送者单元 2920。当每一用户与发送者单元 2920 在线时，接收者单元 2915 将用于那个特定用户的多个询问 - 应答集 2975 存储在存储器 2960 的段中。相应地，用于那个用户的询问 - 应答集 2975 存储在分配给那个用户的存储器 2960 段中。因此，存储器 2960 的每一段不能由另一用户的询问 - 应答集 2975 覆盖。接收者单元 2915 也可以包括多个存储器 2960 以便将每一存储器 2960 分配给每一用户。当每一用户希望离线使用接收者单元 2915 的资源时，访问用于那个用户的存储器 2960 段，并如在此所述，执行该用户的第二因素验证。发送者单元 2920 的管理员可以选择由单个用户还是由多个用户离线使用接收者单元 2920。

[0158] 如上文所述，询问 - 应答集 2975 可以用新的询问 - 应答集 2975 覆盖。例如当存储的询问 - 应答集 2975 的数量是最大容许上限时，这会发生，并且任何另外的询问 - 应答集覆盖存储的询问 - 应答集 2975。当接收者单元 2915 由于上文所述的原因而覆盖存储的询问 - 应答集 2975 时，存储的询问 - 应答集 2975 的替换可以基于随机替换存储器 2960 中的询问 - 应答集 2975、替换最早的询问 - 应答集 2975、替换最新的询问 - 应答集 2975、替换最常使用的询问 - 应答集 2975 和 / 或替换最少使用的询问 - 应答集 2975。

[0159] 当验证用户以便离线使用接收者单元 2915 时，可以将存储在接收者单元 2915 的存储器 2960 中的一个或多个存储的询问 - 应答集 2975 用于验证。本公开内容提供了基于随机选择、选择最早、选择最新、选择最常使用和 / 或选择最少使用的存储询问 - 应答集

2975，来选择用于离线验证的询问－应答集 2975。

[0160] 为了提供接收者单元 2915 用于用户的离线验证的上述描述功能，可以将可执行指令集或软件程序存储在接收者单元 2915 上，当执行所述指令集或软件程序时，提供上述功能。由软件程序提供的功能的示例性如下：当用户在线时提供与发送者单元 2920 的连接性，以便接收用于离线验证的询问－应答集 2975，通过递增当尝试离线验证时可变的标记，跟踪用户尝试离线验证的次数，基于上述方法中的任何一个，选择存储的询问－应答集 2975 用于离线验证，和／或通过接收者单元 2920，管理不同用户离线和在线验证。

[0161] 存储器 2960 中存储的询问－应答集 2975 的数量通常小于来自物品 1800 的所有可能的询问－应答集 2975。在某些情况下，当接收者单元离线时，发送者单元 2920 的管理员可能希望允许接收者单元 2915 的用户与所需的次数一样多地访问接收者单元。因此，可在接收者单元 2915 的存储器中获得的询问－应答集 2975 的数量可以不限于预定多个询问－应答集 2975。在这种情况下，当接收者单元登录到发送者单元 2920 中时，来自物品 1800 的所有可能询问－应答集 2975 或其子集可以存储在接收者单元 2915 的存储器 2960 中。当接收者单元 2915 离线时，当用户尝试使用接收者单元 2915 的资源时，基于物品 1800 的询问－应答集 2975 的所有可能组合中的一个，来生成用于接收者单元 2915 的用户的询问－应答集 2975。因此，接收者单元 2915 的上述软件程序可以提供如上文所述的在线询问和应答过程，以便基于来自物品 1800 的所有存储的询问－应答集 2975 来验证用户。然而，当另一用户使用接收者单元 2915 并登录到发送者单元 2920，并通过网络或通过与发送者单元 2920 通信而与发送者单元 2920 在线时，将由接收者单元 2915 自动地删除（例如清除或覆盖）存储在接收者单元 2915 的存储器 2960 中的所有询问－应答集 2975，以便能将基于新用户的物品 1800 的所有少于用于该新用户的所有询问－应答集 2975 存储在存储器 2960 中。

[0162] 发送者单元 2920 可以包括图形用户界面 (GUI)，其允许发送者单元 2920 的管理员在每一用户或组的基础上确定所需的离线验证安全方案。例如，GUI 可以包括下拉菜单，以便允许发送者单元 2920 的管理员响应来自接收者单元 2915 的请求，选择多个离线验证安全方案中的一个发送到接收者单元 2915。可以由发送者单元 2920 的管理员选择的安全方案可以包括可存储在接收者单元 2915 的存储器 2960 上的询问－应答集 2975 的数量。另外，可由发送者单元 2920 的管理员选择的安全方案可以包括可存储在接收者单元 2915 的存储器 2960 上的询问－应答集 2975 的类型。例如，发送者单元 2920 的 GUI 可以包括下拉菜单，通过该菜单，发送者单元 2920 的管理员可以选择安全方案以便发送到接收者单元 2915。可选择的安全方案可以包括接收者单元 2915 存储在线先前成功的询问－应答集 2975、向接收者单元发送预定数目询问－应答集 2975，所有可能的询问－应答集 2975 可以在物品 1800 上获得，或少于所有可能的询问－应答集 2975 可以在物品 1800 上获得。

[0163] 如上所述，当接收者单元 2915 相对于发送者单元 2920 离线时，该方法和装置提供用于接收者单元 2915 的第二因素验证。当接收者单元 2915 未连接到网络并且不能访问验证服务器 2905 时，该方法和装置允许接收者单元 2915 响应由发送者单元 2920 发出的唯一、一次性验证询问，所述发送者单元 2920 可以是验证服务器 2905。

[0164] 当发送者单元 2920 不可用于接收者单元 2915 时，该方法和装置使用动态一次性询问－应答集 2975 来提供离线验证的安全方法。该方法和装置不具有基于时间的固有期

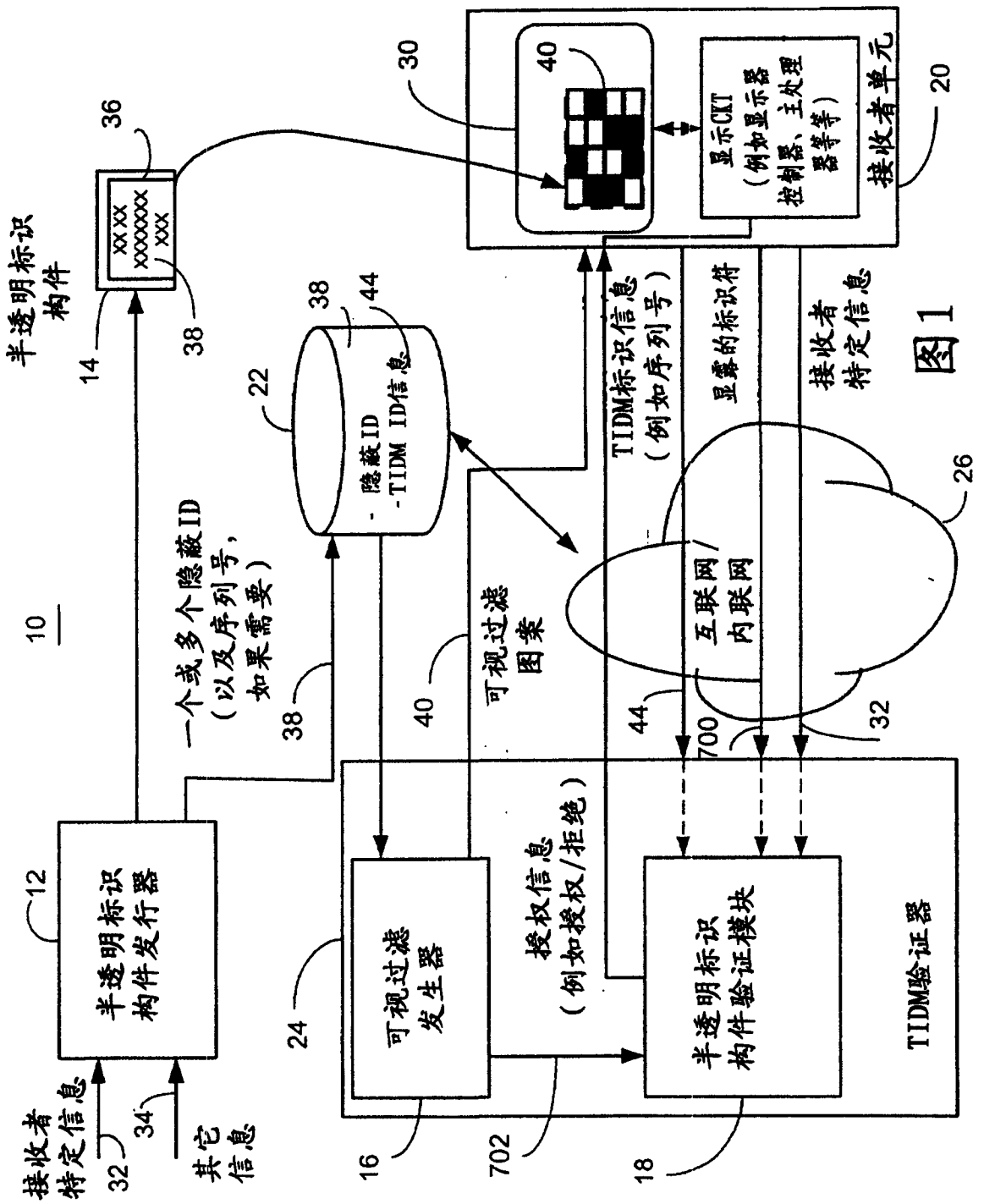
限。用户能保持离线达不定时间周期，而仍然允许验证方法起作用。另外，接收者单元 2915 能自动地采取所有必要的步骤来准备离线验证。因此，由于网络故障或其它原因而发送者单元 2920 非有意离线时，该离线验证方法允许用户继续使用第二因素来验证。即使发送者单元 2920 变为离线，仍然加强采用本方法和系统的组织的安全策略，以及在接收者单元 2915 上保持双因素验证。本领域的普通技术人员将意识到其它优点。

[0165] 因此，期望本发明覆盖落在在此公开和其中所要求的基本原理的精神和范围内的任何和所有改变、变形或等效。例如，该方法不需要通过两级验证使用，而可以充当单级验证。

[0166] 本领域的技术人员将意识到尽管结合某些实施例，示例说明本发明的教导，不打算将本发明限定到这些实施例。相反，本申请的意图是覆盖完全落在本发明的教导的范围内的所有改变和实施例。

[0167] 相关申请

[0168] 这是发明人为 Voice 等人并由本受让人拥有的 2004 年 5 月 19 日提交的序列号为 10/849,402、名称为“METHOD AND APPARATUSFOR PROVIDING ELECTRONIC MESSAGE AUTHENTICATION”的 U.S. 专利申请的继续申请，该 U.S. 专利申请是发明人为 Chiviendacz 等人并由本受让人拥有的 2003 年 12 月 30 日提交的序列号 10/748,523、名称为“METHOD AND APPARATUS FOR SECURELYPROVIDING IDENTIFICATION INFORMATION USINGTRANSLUCENT IDENTIFICATION MEMBER”的 U.S. 专利申请的继续申请。


半透明标识构件
XX XX
XXXXXXX
XXX
36
14
38
30
40
显示CKT
(例如显示器控制器、主处理器等等)
接收者单元
20
22
38
44
- 隐蔽ID
-TIDM ID信息
TIDM标识信息
(例如序列号)
显露的标识符
接收者特定信息
图 1
10
一个或多个隐蔽ID
(以及序列号,
如果需要)
38
40
可视过滤图案
互联网/
内联网
26
44
700
32
12
半透明标识构件发行器
24
可视过滤发生器
授权信息
(例如授权/拒绝)
半透明标识构件验证模块
TIDM验证器
接收者特定信息
32
34
其它信息
16
702
18

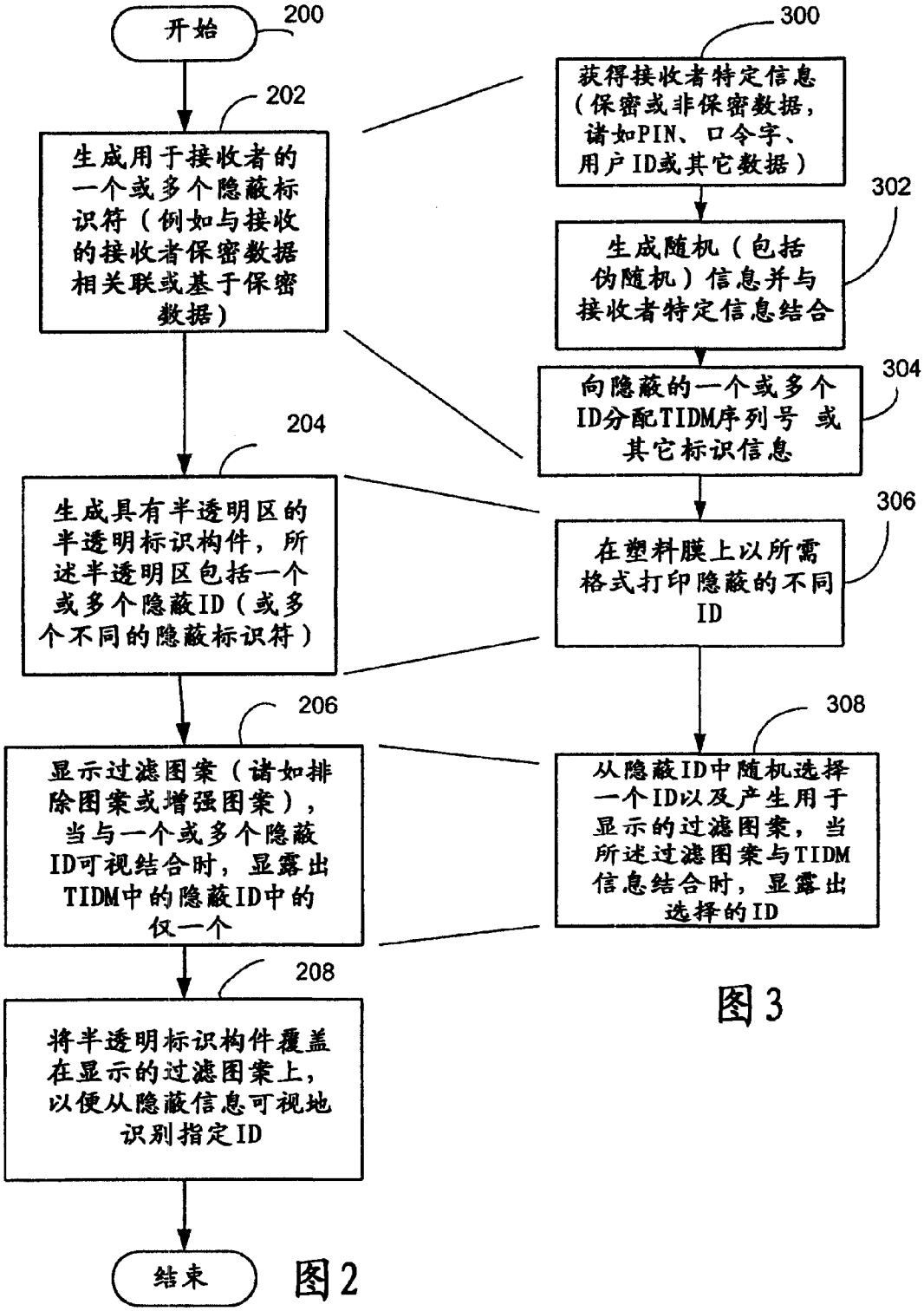

开始
200
202
生成用于接收者的一个或多个隐蔽标识符（例如与接收的接收者保密数据相关联或基于保密数据）
204
生成具有半透明区的半透明标识构件，所述半透明区包括一个或多个隐蔽ID（或多个不同的隐蔽标识符）
206
显示过滤图案（诸如排除图案或增强图案），当与一个或多个隐蔽ID可视结合时，显露出TIDM中的隐蔽ID中的仅一个
208
将半透明标识构件覆盖在显示的过滤图案上，以便从隐蔽信息可视地识别指定ID
结束
300
获得接收者特定信息（保密或非保密数据，诸如PIN、口令字、用户ID或其它数据）
302
生成随机（包括伪随机）信息并与接收者特定信息结合
304
向隐蔽的一个或多个ID分配TIDM序列号 或其它标识信息
306
在塑料膜上以所需格式打印隐蔽的不同ID
308
从隐蔽ID中随机选择一个ID以及产生用于显示的过滤图案，当所述过滤图案与TIDM信息结合时，显露出选择的ID

图2

图3

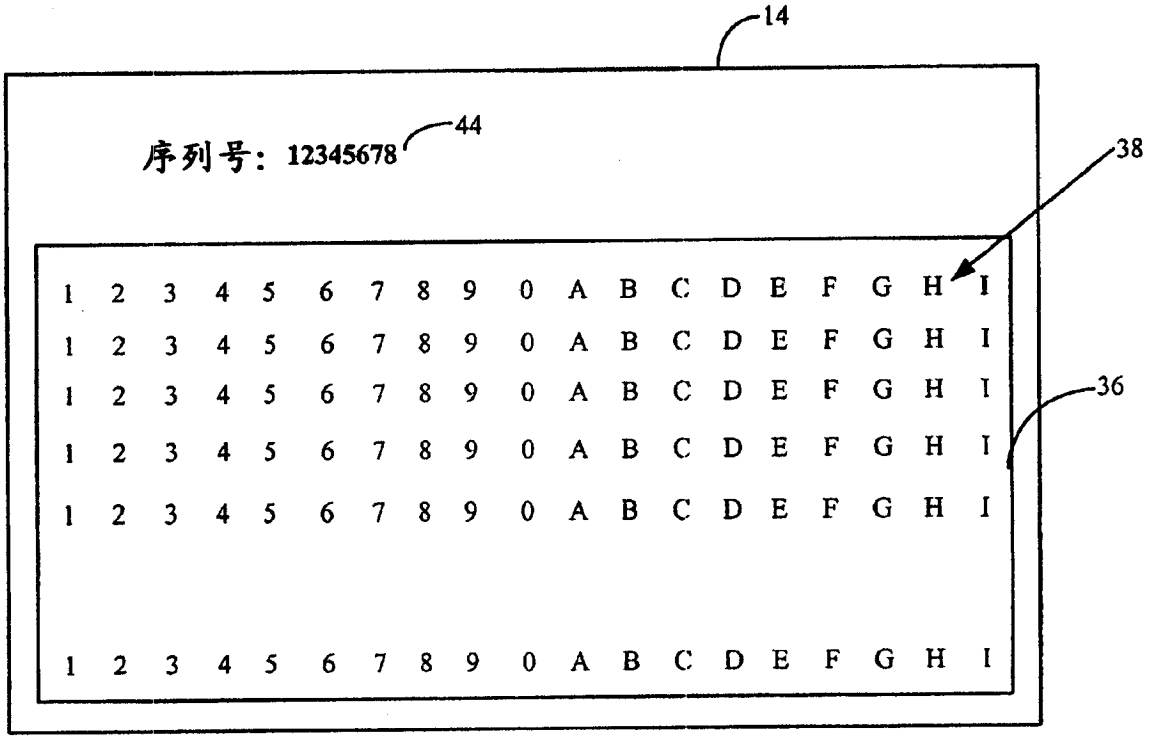

14
序列号：12345678
44
38
36
1 2 3 4 5 6 7 8 9 0 A B C D E F G H I
1 2 3 4 5 6 7 8 9 0 A B C D E F G H I
1 2 3 4 5 6 7 8 9 0 A B C D E F G H I
1 2 3 4 5 6 7 8 9 0 A B C D E F G H I
1 2 3 4 5 6 7 8 9 0 A B C D E F G H I
1 2 3 4 5 6 7 8 9 0 A B C D E F G H I

图 4

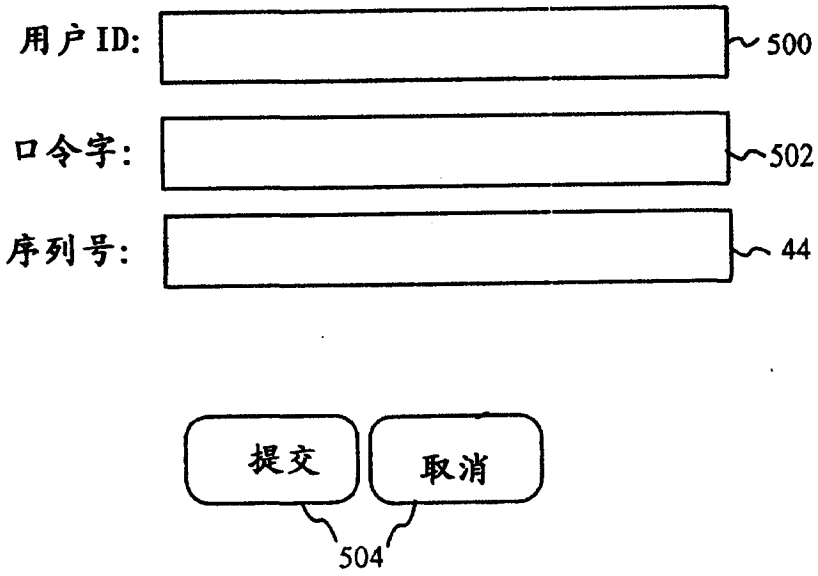

用户 ID:
500
口令字:
502
序列号:
44
提交
取消
504

图 5

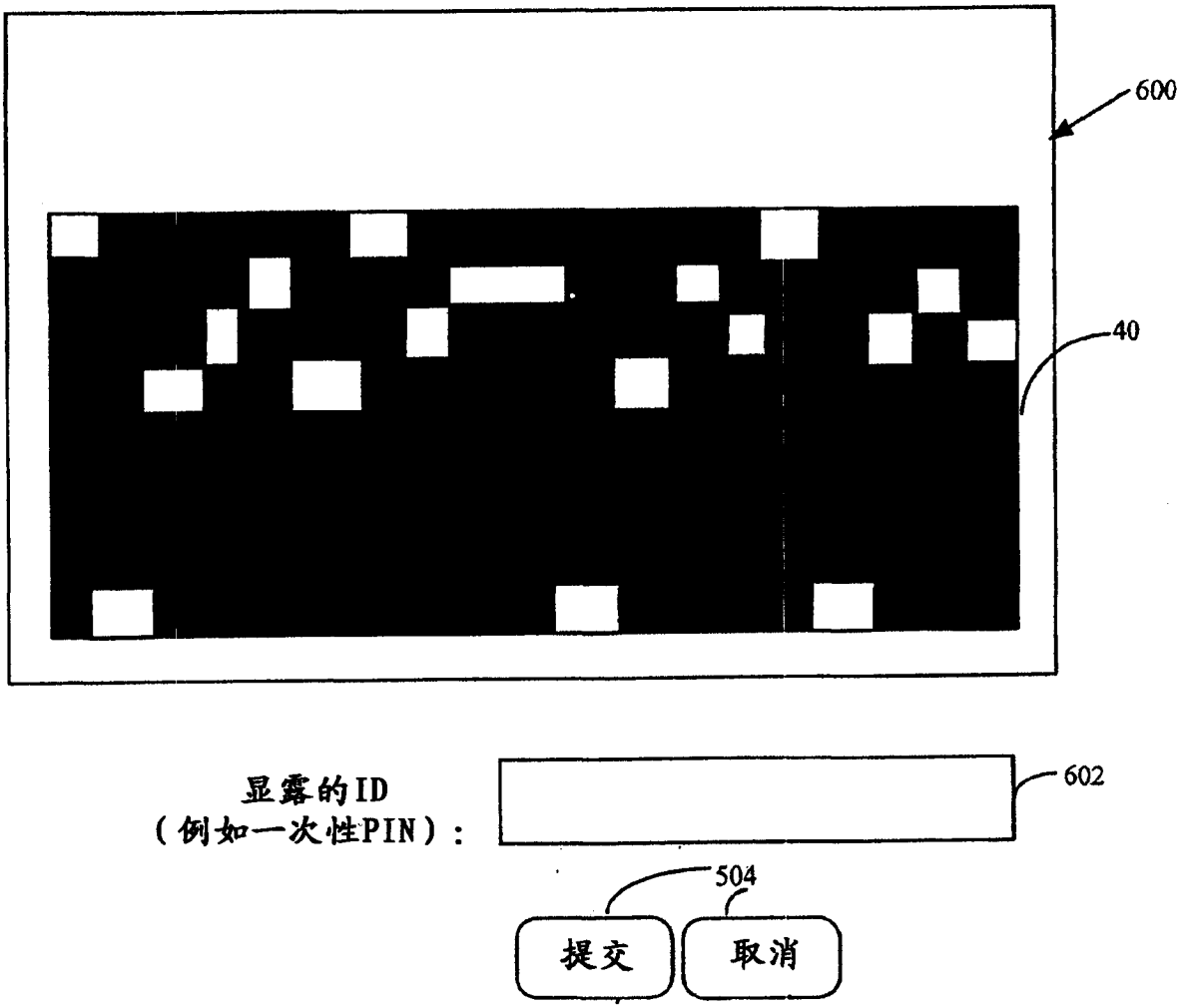


图 6

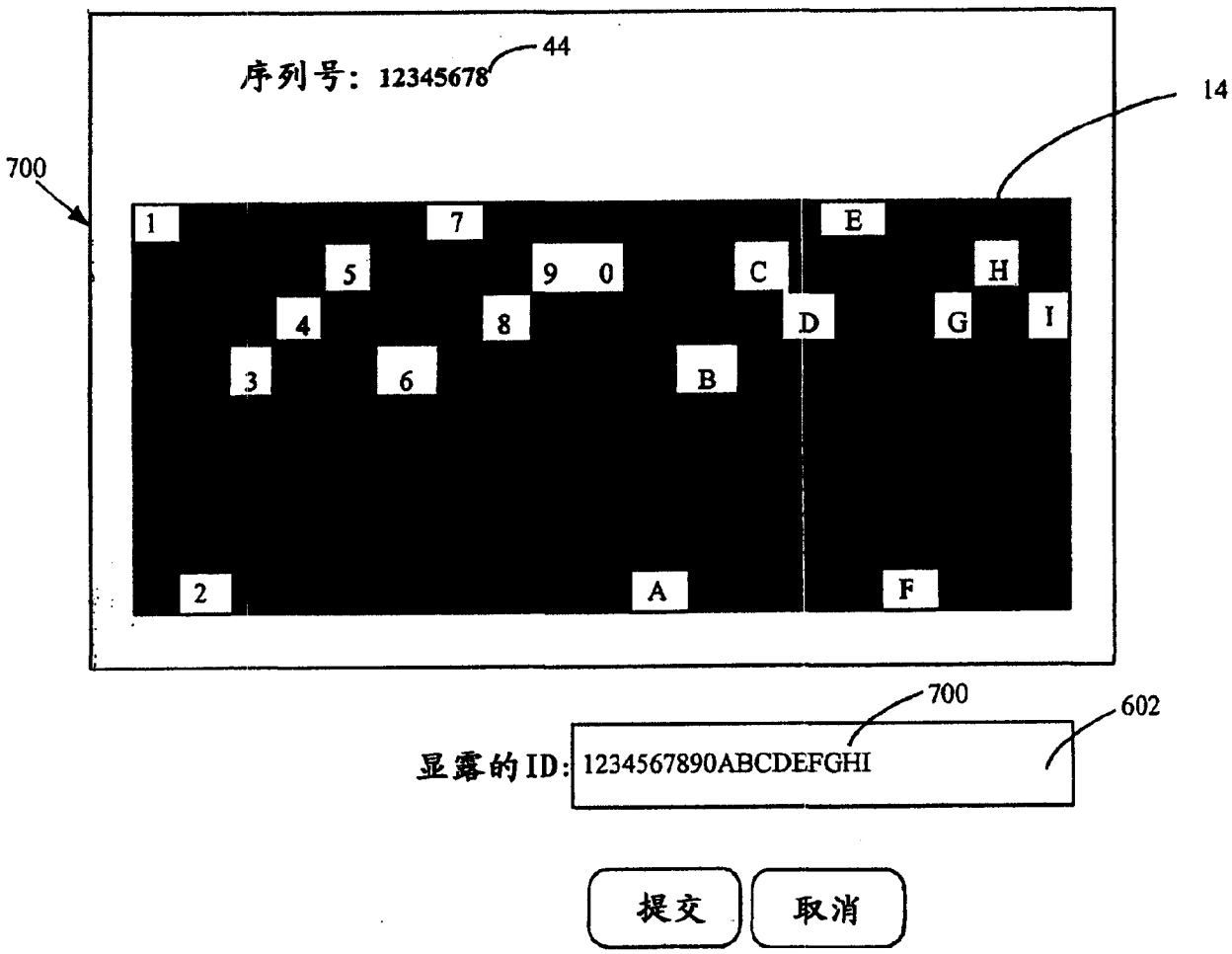

序列号：12345678
44
14
700
1
7
E
5
9
0
C
H
4
8
D
G
I
3
6
B
2
A
F
700
602
显露的ID：1234567890ABCDEFGHI
提交
取消

图 7

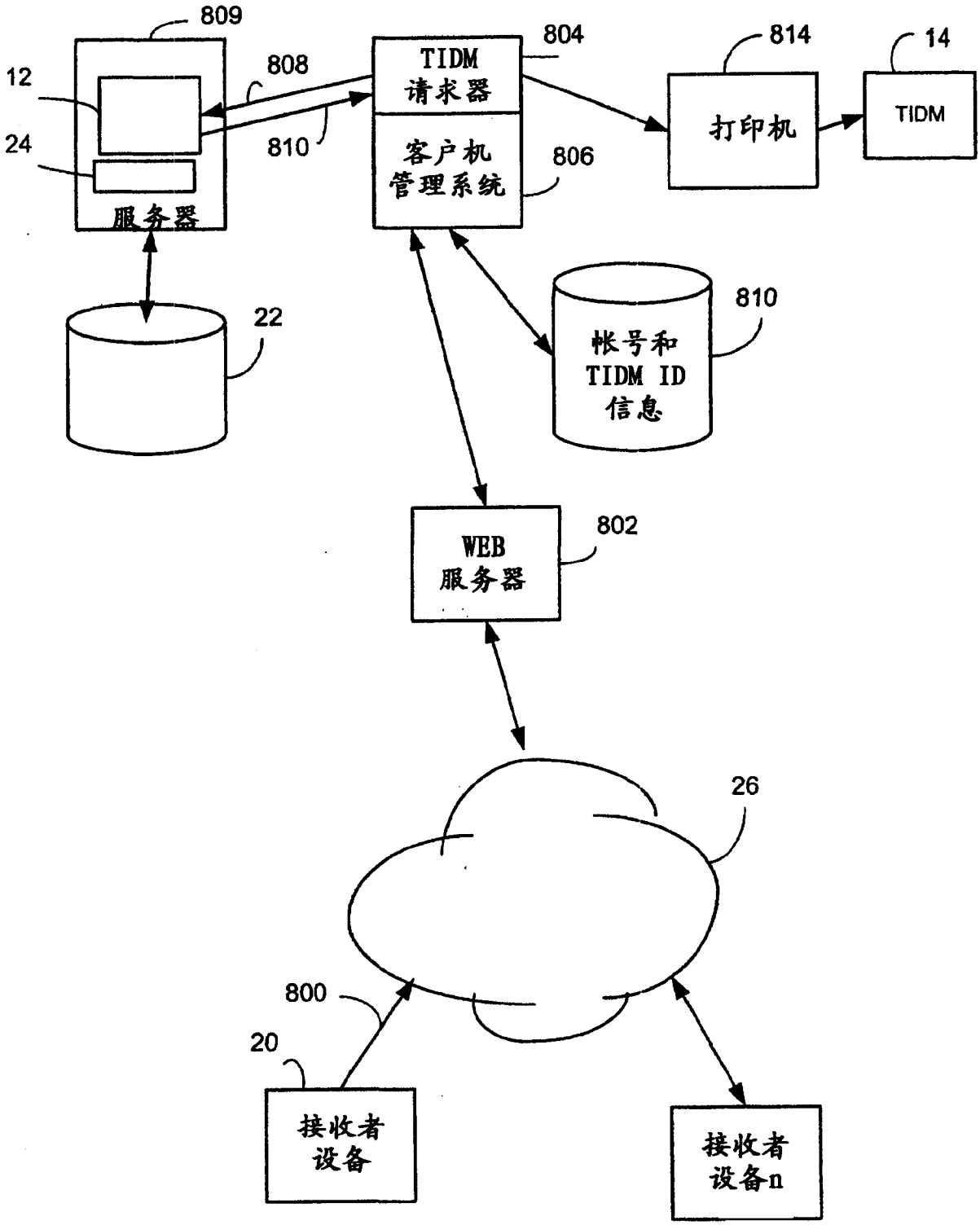

809
12
24
服务器
808
810
TIDM
请求器
804
客户机
管理系统
806
814
打印机
14
TIDM
22
帐号和
TIDM ID
信息
810
WEB
服务器
802
26
800
20
接收者
设备
接收者
设备n

图 8

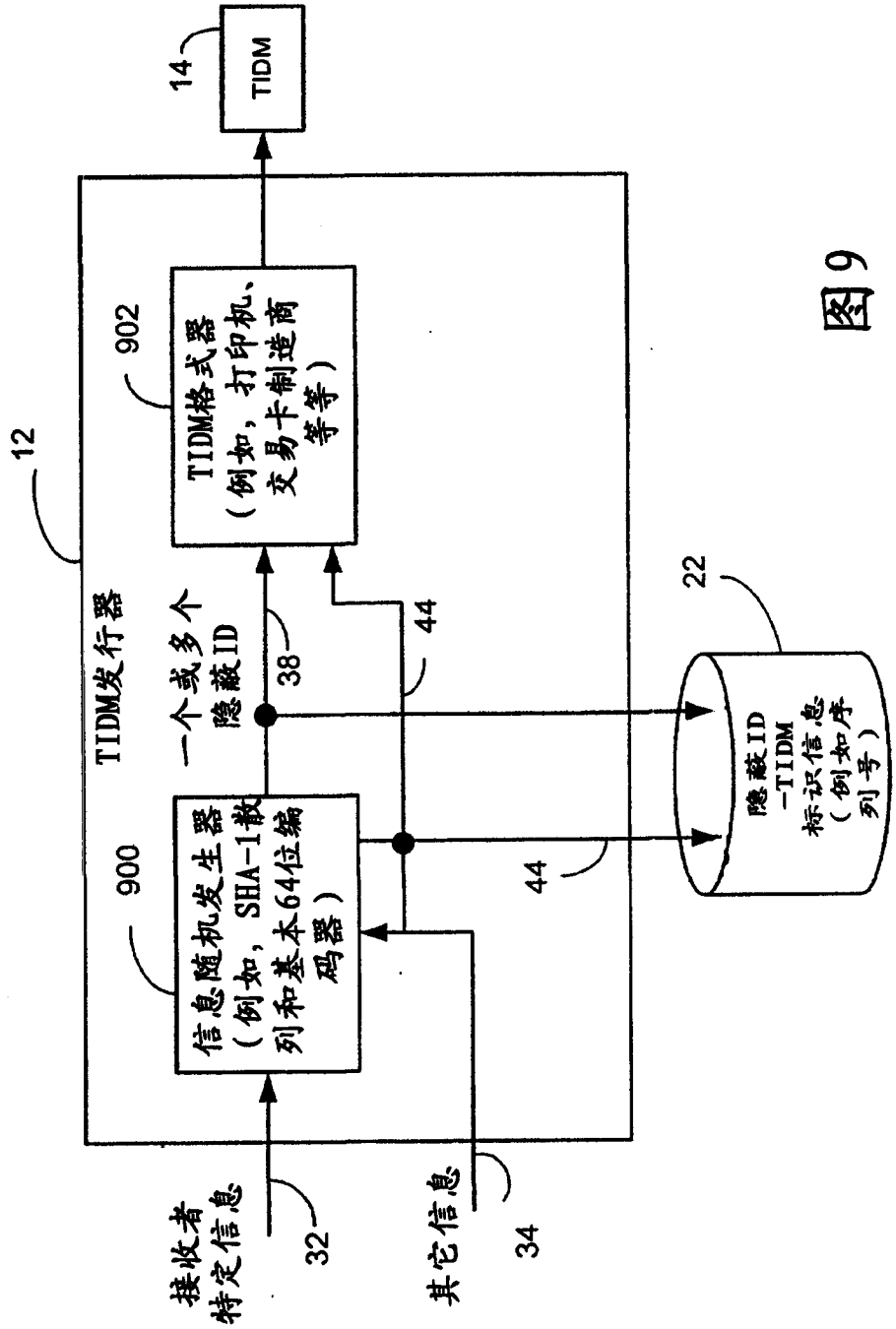

14
TIDM
902
TIDM格式器
（例如，打印机、
交易卡制造商
等等）
12
TIDM发行器
一个或多个
隐藏ID
38
44
22
隐藏ID
-TIDM
标识信息
（例如序
列号）
900
信息随机发生器
（例如，SHA-1散
列和基本64位编
码器）
44
接收者
特定信息
32
其它信息
34

图9

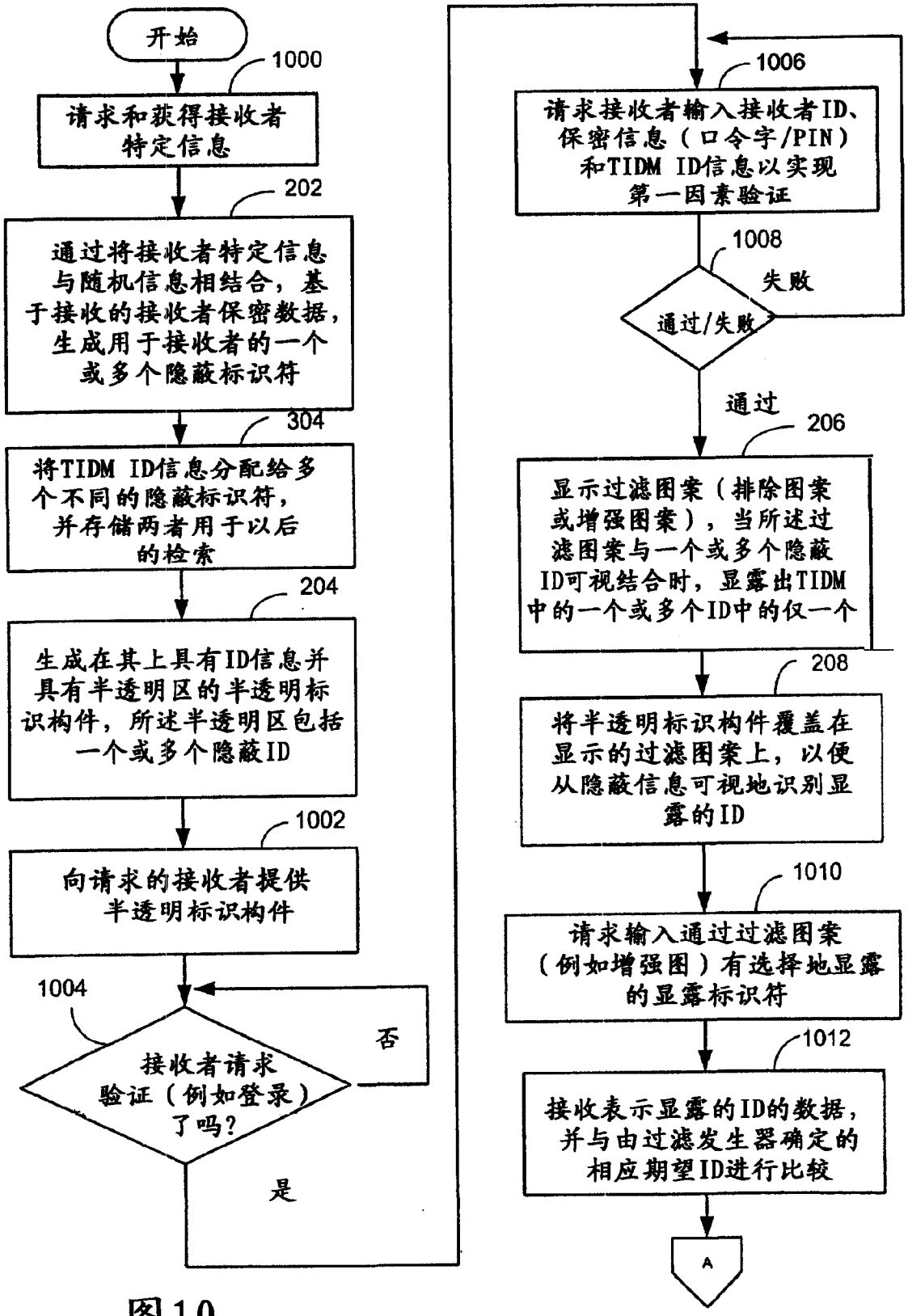

开始
1000
请求和获得接收者特定信息
202
通过将接收者特定信息与随机信息相结合，基于接收的接收者保密数据，生成用于接收者的一个或多个隐蔽标识符
304
将TIDM ID信息分配给多个不同的隐蔽标识符，并存储两者用于以后的检索
204
生成在其上具有ID信息并具有半透明区的半透明标识构件，所述半透明区包括一个或多个隐蔽ID
1002
向请求的接收者提供半透明标识构件
1004
接收者请求验证（例如登录）了吗？
否
是
1006
请求接收者输入接收者ID、保密信息（口令字/PIN）和TIDM ID信息以实现第一因素验证
1008
失败
通过/失败
通过
206
显示过滤图案（排除图案或增强图案），当所述过滤图案与一个或多个隐蔽ID可视结合时，显露出TIDM中的一个或多个ID中的仅一个
208
将半透明标识构件覆盖在显示的过滤图案上，以便从隐蔽信息可视地识别显露的ID
1010
请求输入通过过滤图案（例如增强图）有选择地显露的显露标识符
1012
接收表示显露的ID的数据，并与由过滤发生器确定的相应期望ID进行比较
A

图10

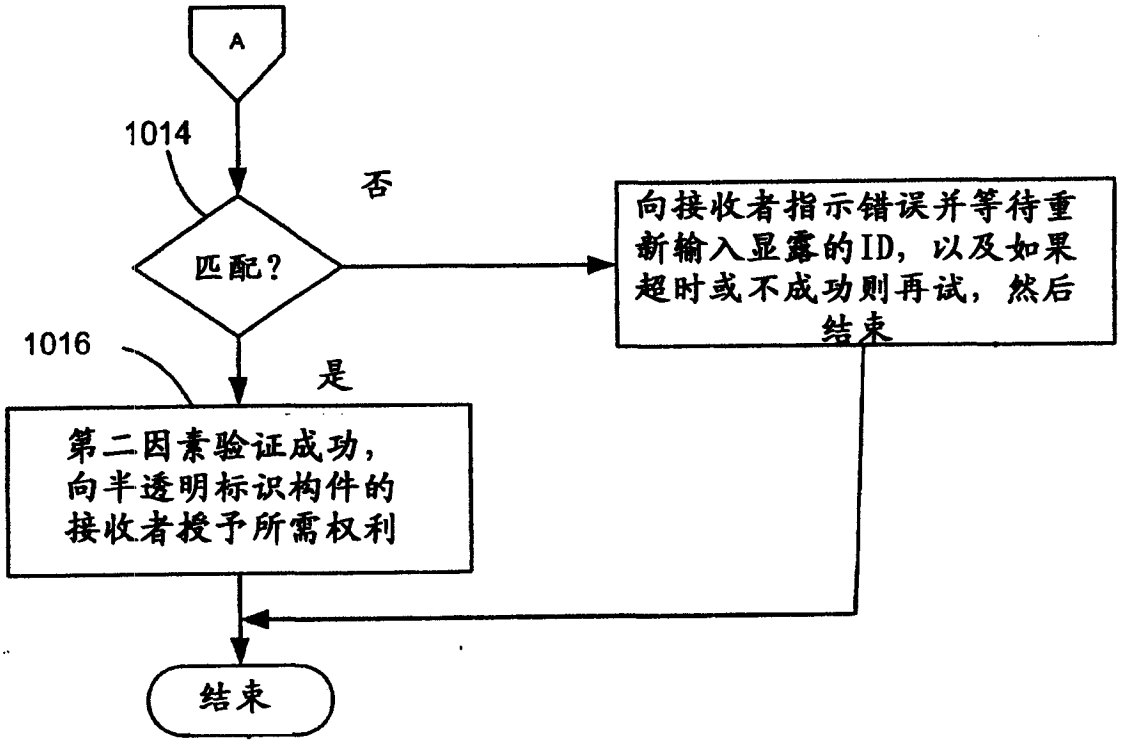

A
1014
否
匹配?
向接收者指示错误并等待重新输入显露的ID，以及如果超时或不成功则再试，然后结束
1016
是
第二因素验证成功，向半透明标识构件的接收者授予所需权利
结束

图 11

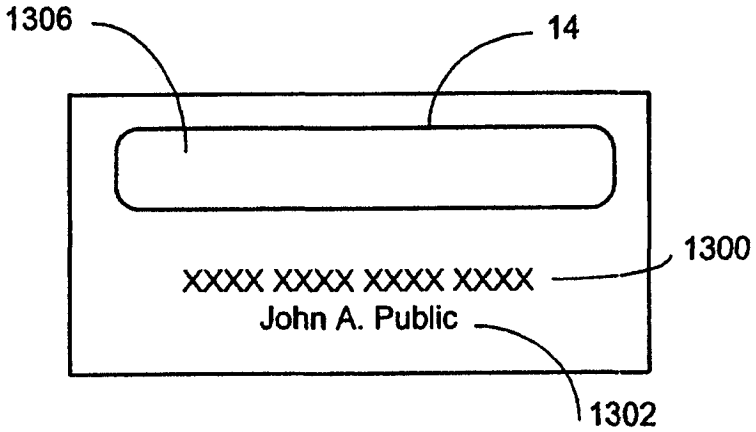

1306
14
1300
XXXX XXXX XXXX XXXX
John A. Public
1302

图 12

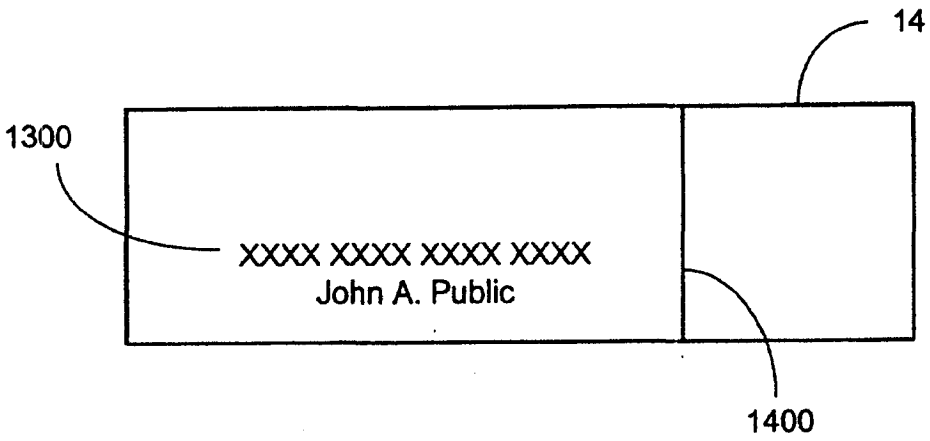


图 13

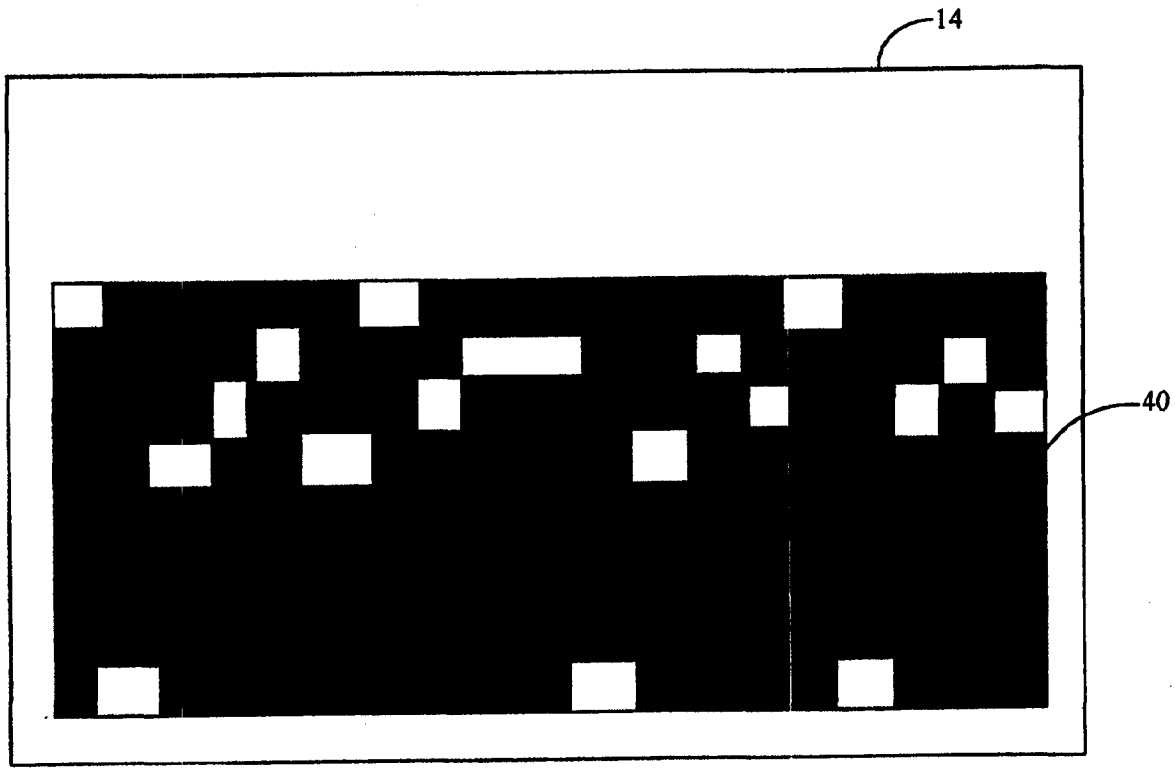


图 14

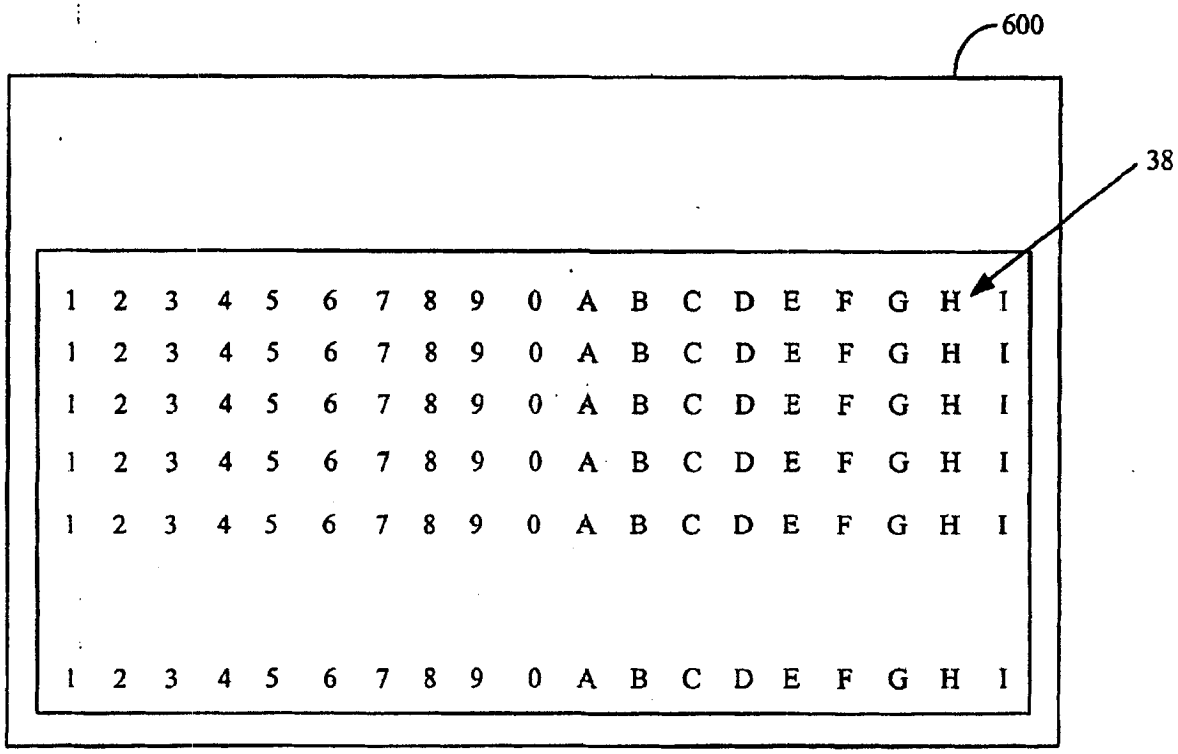

600
38
1 2 3 4 5 6 7 8 9 0 A B C D E F G H I
1 2 3 4 5 6 7 8 9 0 A B C D E F G H I
1 2 3 4 5 6 7 8 9 0 A B C D E F G H I
1 2 3 4 5 6 7 8 9 0 A B C D E F G H I
1 2 3 4 5 6 7 8 9 0 A B C D E F G H I
1 2 3 4 5 6 7 8 9 0 A B C D E F G H I

图 15

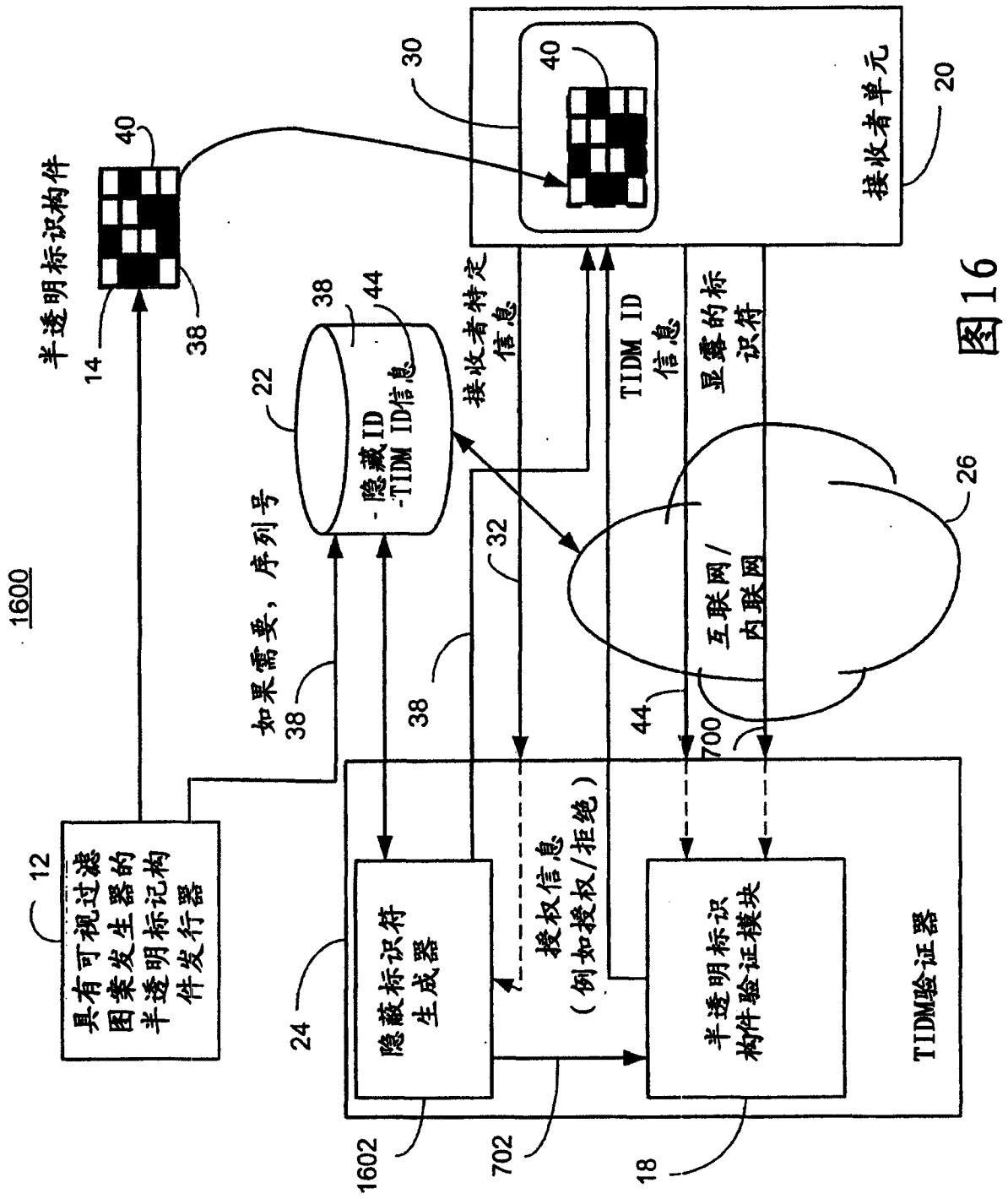

1600
具有可视过滤图案发生器的半透明标记构件发行器
12
半透明标识构件
14
40
38
隐藏ID
-TIDM ID信息
22
44
如果需要，序列号
38
38
32
38
接收者特定信息
TIDM ID信息
显露的标识符
44
700
互联网/内联网
26
接收者单元
20
30
40
隐蔽标识符生成器
24
授权信息
（例如授权/拒绝）
半透明标识构件验证模块
TIDM验证器
1602
702
18

图16

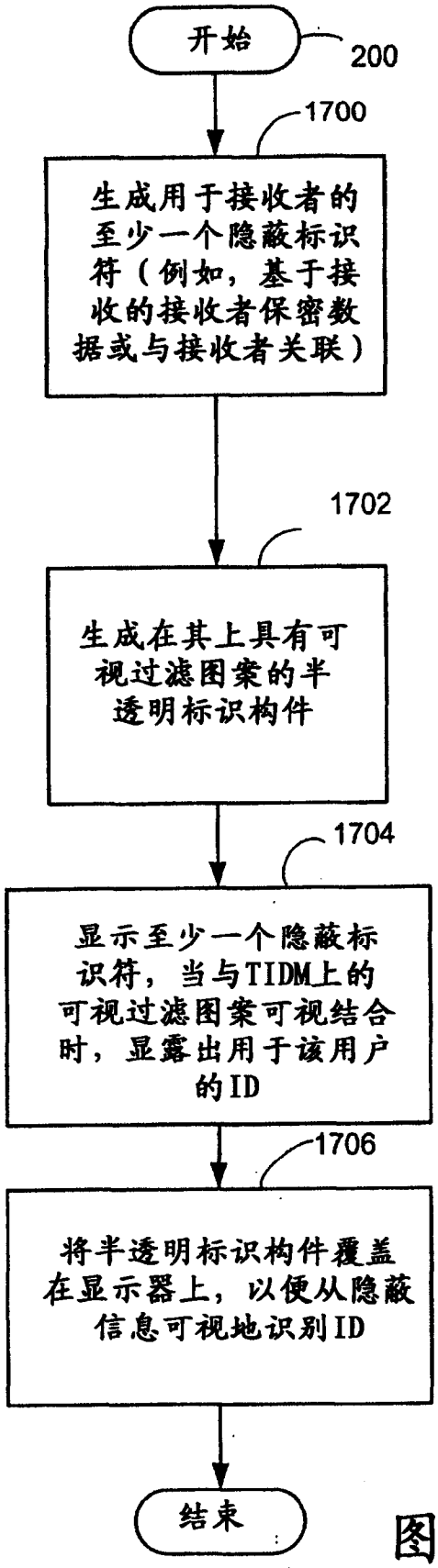

开始
200
1700
生成用于接收者的至少一个隐蔽标识符（例如，基于接收的接收者保密数据或与接收者关联）
1702
生成在其上具有可视过滤图案的半透明标识构件
1704
显示至少一个隐蔽标识符，当与TIDM上的可视过滤图案可视结合时，显露出用于该用户的ID
1706
将半透明标识构件覆盖在显示器上，以便从隐蔽信息可视地识别ID
结束

图17

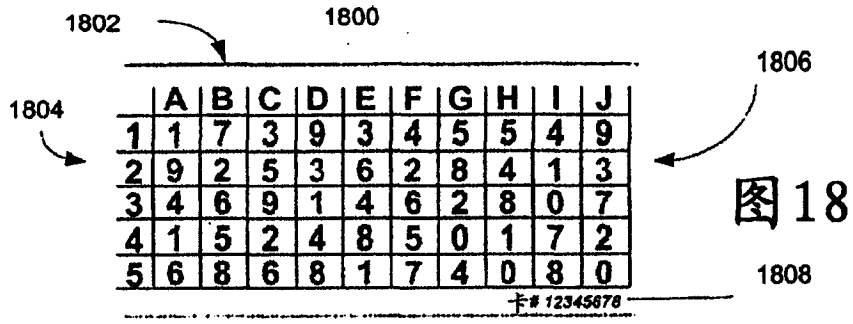

1802
1800
1806
1804
A B C D E F G H I J
1 1 7 3 9 3 4 5 5 4 9
2 9 2 5 3 6 2 8 4 1 3
3 4 6 9 1 4 6 2 8 0 7
4 1 5 2 4 8 5 0 1 7 2
5 6 8 6 8 1 7 4 0 8 0
卡# 12345678
1808

图18

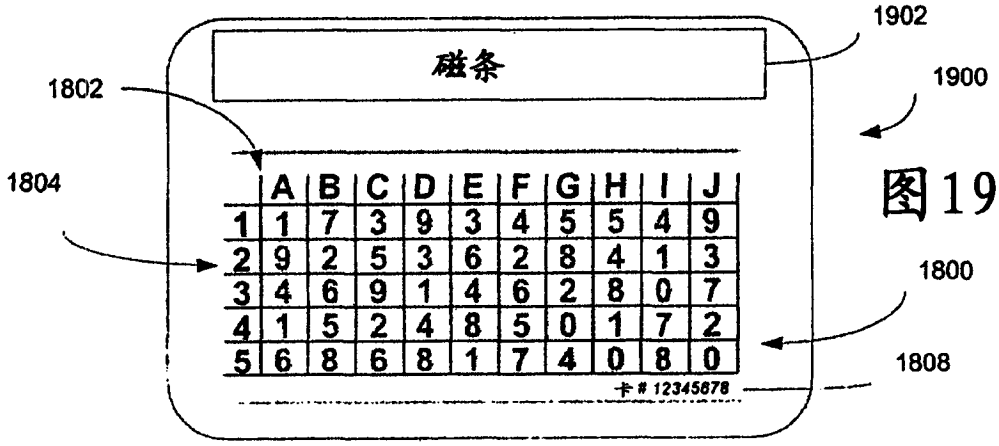

1902
磁条
1900
1802
1804
A B C D E F G H I J
1 1 7 3 9 3 4 5 5 4 9
2 9 2 5 3 6 2 8 4 1 3
3 4 6 9 1 4 6 2 8 0 7
4 1 5 2 4 8 5 0 1 7 2
5 6 8 6 8 1 7 4 0 8 0
卡# 12345678
1800
1808

图19

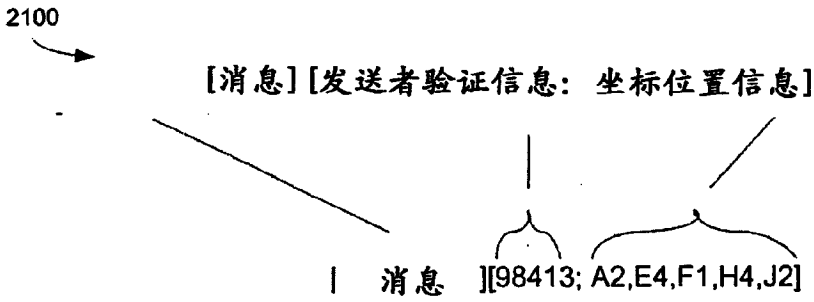

2100
[消息][发送者验证信息: 坐标位置信息]
| 消息][98413; A2,E4,F1,H4,J2]

图 21

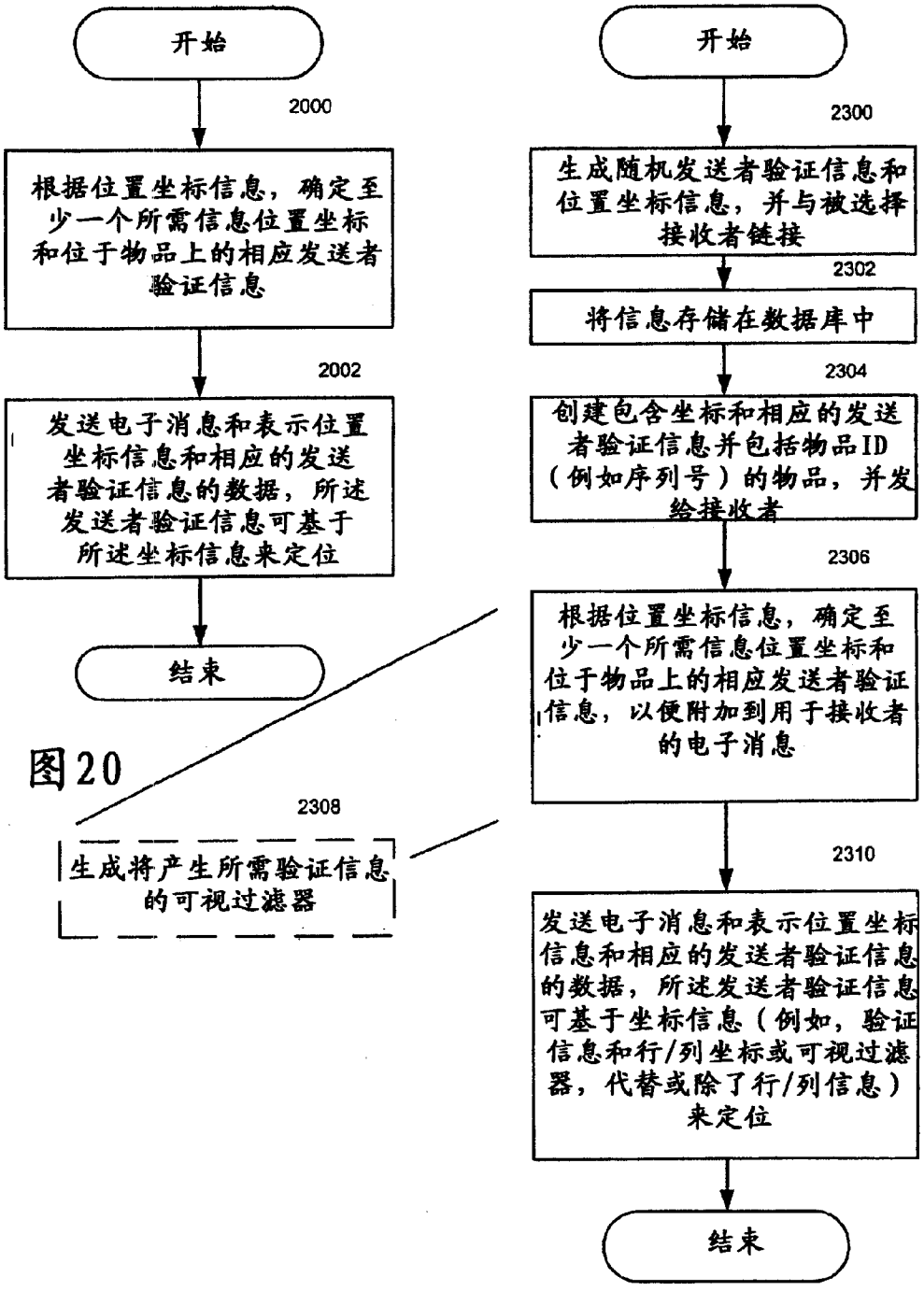

开始
2000
根据位置坐标信息，确定至少一个所需信息位置坐标和位于物品上的相应发送者验证信息
2002
发送电子消息和表示位置坐标信息和相应的发送者验证信息的数据，所述发送者验证信息可基于所述坐标信息来定位
结束
开始
2300
生成随机发送者验证信息和位置坐标信息，并与被选择接收者链接
2302
将信息存储在数据库中
2304
创建包含坐标和相应的发送者验证信息并包括物品ID（例如序列号）的物品，并发给接收者
2306
根据位置坐标信息，确定至少一个所需信息位置坐标和位于物品上的相应发送者验证信息，以便附加到用于接收者的电子消息
2308
生成将产生所需验证信息的可视过滤器
2310
发送电子消息和表示位置坐标信息和相应的发送者验证信息的数据，所述发送者验证信息可基于坐标信息（例如，验证信息和行/列坐标或可视过滤器，代替或除了行/列信息）来定位
结束

图20

图23

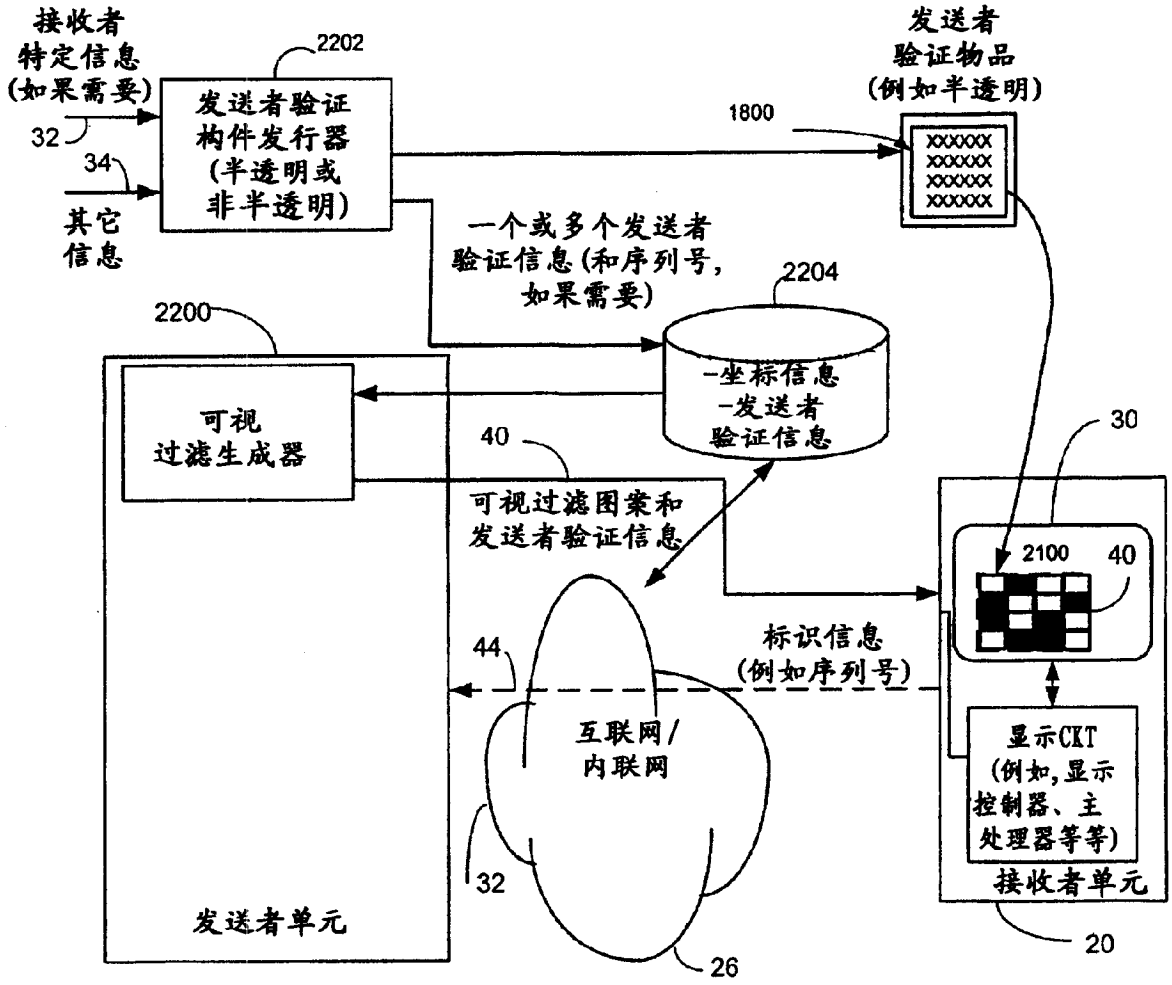

接收者
特定信息
(如果需要)
32
34
其它
信息
2202
发送者验证
构件发行器
(半透明或
非半透明)
1800
发送者
验证物品
(例如半透明)
XXXXX
XXXXX
XXXXX
XXXXX
一个或多个发送者
验证信息(和序列号,
如果需要)
2204
2200
-坐标信息
-发送者
验证信息
可视
过滤生成器
40
可视过滤图案和
发送者验证信息
30
2100
40
标识信息
(例如序列号)
44
互联网/
内联网
显示CKT
(例如,显示
控制器、主
处理器等等)
接收者单元
20
32
发送者单元
26

图 22

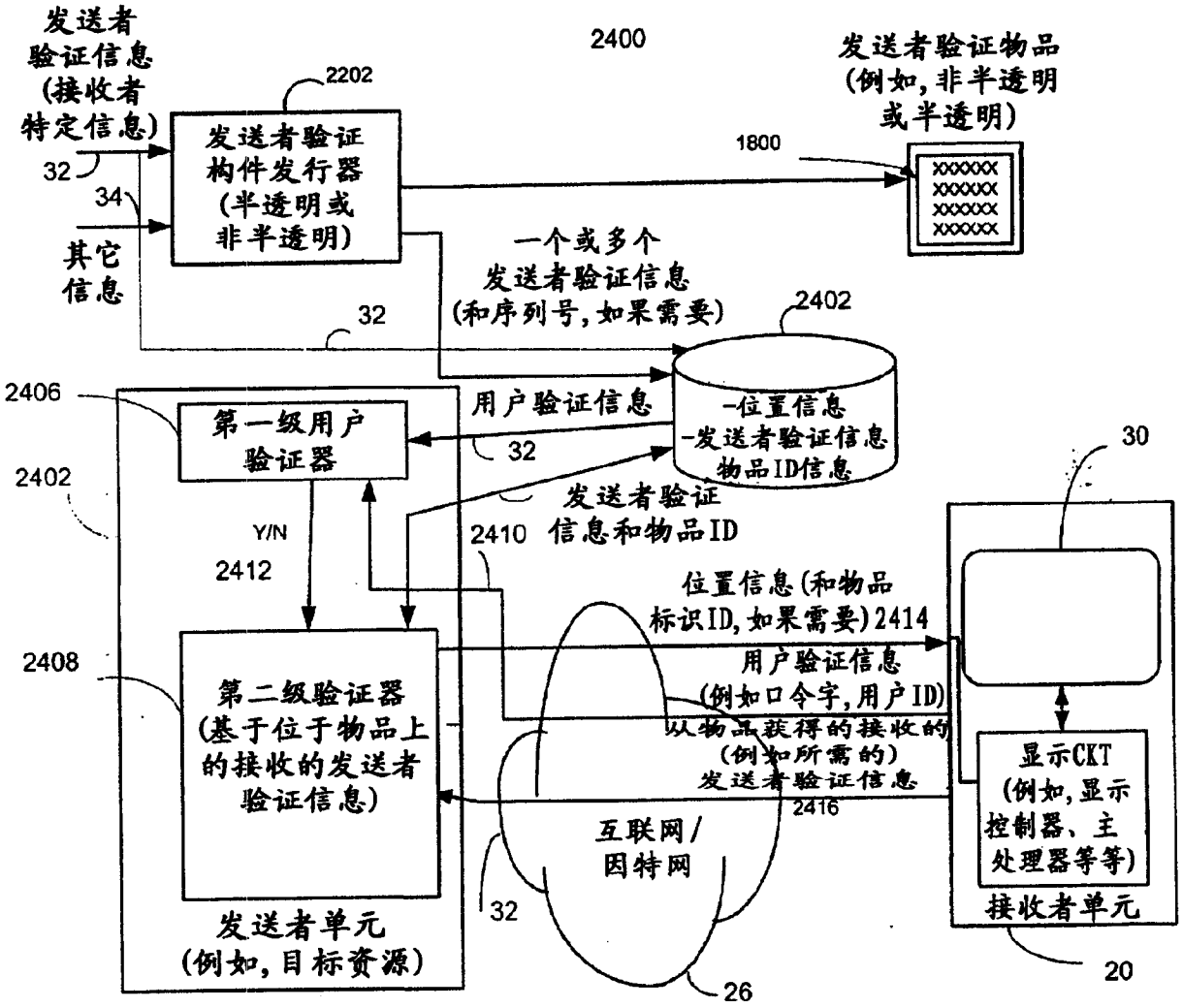

发送者
验证信息
(接收者
特定信息)
32
34
其它
信息
2202
发送者验证
构件发行器
(半透明或
非半透明)
2400
发送者验证物品
(例如,非半透明
或半透明)
1800
XXXXXX
XXXXXX
XXXXXX
XXXXXX
一个或多个
发送者验证信息
(和序列号,如果需要)
32
2402
-位置信息
-发送者验证信息
物品ID信息
2406
第一级用户
验证器
用户验证信息
32
2402
Y/N
2412
发送者验证
信息和物品ID
2410
位置信息(和物品
标识ID,如果需要)2414
2408
第二级验证器
(基于位于物品上
的接收的发送者
验证信息)
用户验证信息
(例如口令字,用户ID)
从物品获得的接收的
(例如所需的)
发送者验证信息
2416
互联网/
因特网
32
发送者单元
(例如,目标资源)
26
30
显示CKT
(例如,显示
控制器、主
处理器等等)
接收者单元
20

图 24

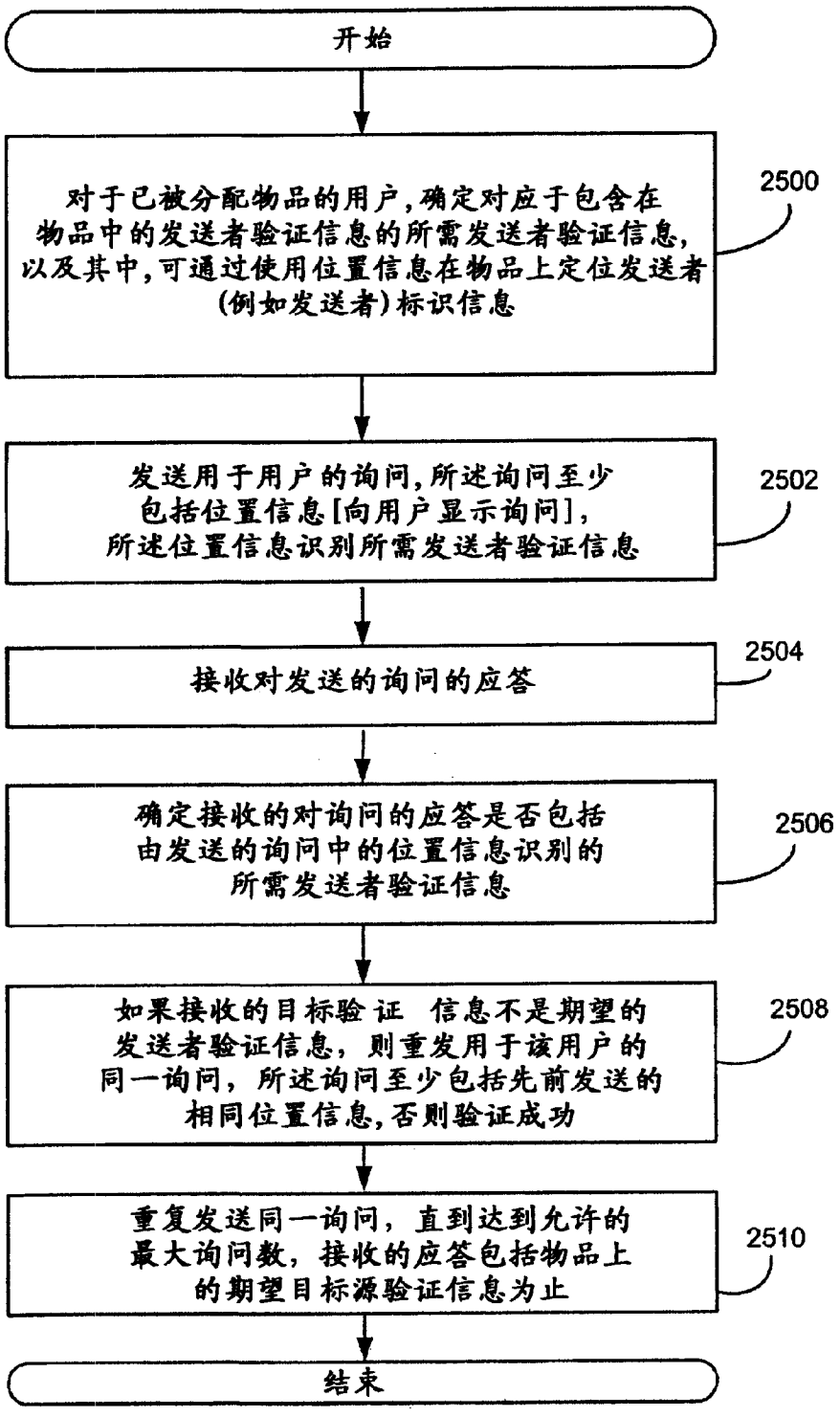

开始
对于已被分配物品的用户，确定对应于包含在物品中的发送者验证信息的所需发送者验证信息，以及其中，可通过使用位置信息在物品上定位发送者(例如发送者)标识信息
2500
发送用于用户的询问，所述询问至少包括位置信息[向用户显示询问]，所述位置信息识别所需发送者验证信息
2502
接收对发送的询问的应答
2504
确定接收的对询问的应答是否包括由发送的询问中的位置信息识别的所需发送者验证信息
2506
如果接收的目标验证 信息不是期望的发送者验证信息，则重发用于该用户的同一询问，所述询问至少包括先前发送的相同位置信息，否则验证成功
2508
重复发送同一询问，直到达到允许的最大询问数，接收的应答包括物品上的期望目标源验证信息为止
2510
结束

图 25

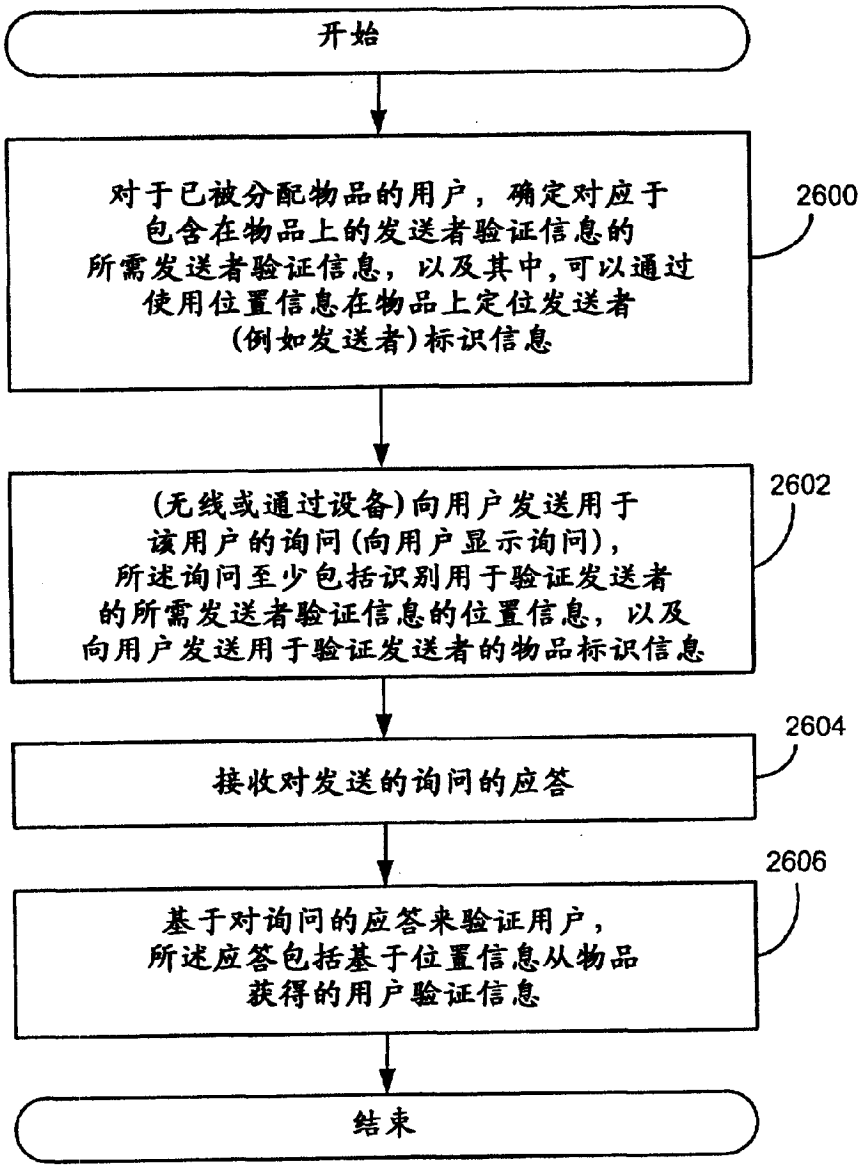

开始
对于已被分配物品的用户，确定对应于包含在物品上的发送者验证信息的所需发送者验证信息，以及其中，可以通过使用位置信息在物品上定位发送者(例如发送者)标识信息
2600
(无线或通过设备)向用户发送用于该用户的询问(向用户显示询问)，所述询问至少包括识别用于验证发送者的所需发送者验证信息的位置信息，以及向用户发送用于验证发送者的物品标识信息
2602
接收对发送的询问的应答
2604
基于对询问的应答来验证用户，所述应答包括基于位置信息从物品获得的用户验证信息
2606
结束

图 26

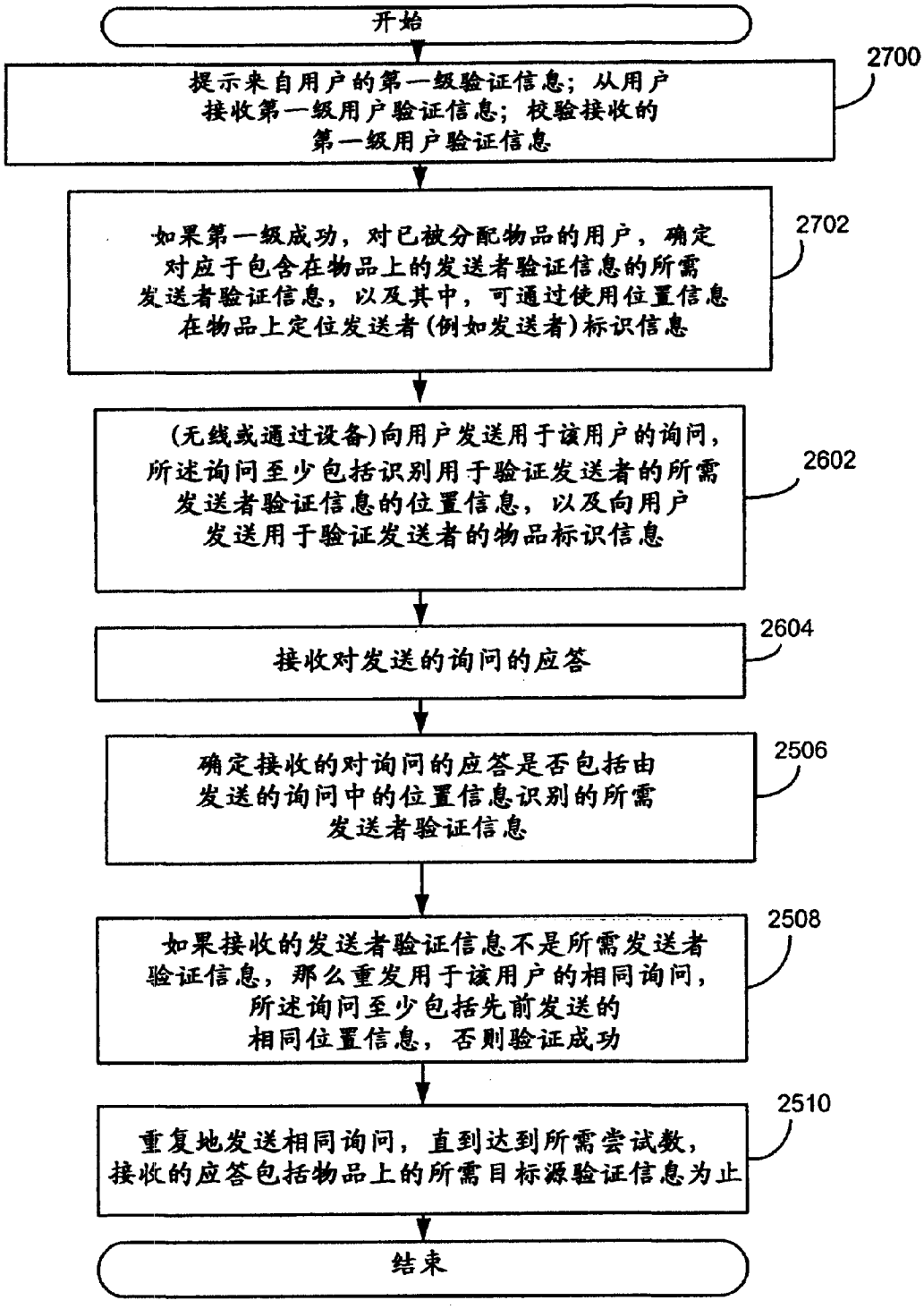

开始
提示来自用户的第一级验证信息；从用户接收第一级用户验证信息；校验接收的第一级用户验证信息
2700
如果第一级成功，对已被分配物品的用户，确定对应于包含在物品上的发送者验证信息的所需发送者验证信息，以及其中，可通过使用位置信息在物品上定位发送者(例如发送者)标识信息
2702
(无线或通过设备)向用户发送用于该用户的询问，所述询问至少包括识别用于验证发送者的所需发送者验证信息的位置信息，以及向用户发送用于验证发送者的物品标识信息
2602
接收对发送的询问的应答
2604
确定接收的对询问的应答是否包括由发送的询问中的位置信息识别的所需发送者验证信息
2506
如果接收的发送者验证信息不是所需发送者验证信息，那么重发用于该用户的相同询问，所述询问至少包括先前发送的相同位置信息，否则验证成功
2508
重复地发送相同询问，直到达到所需尝试数，接收的应答包括物品上的所需目标源验证信息为止
2510
结束

图 27

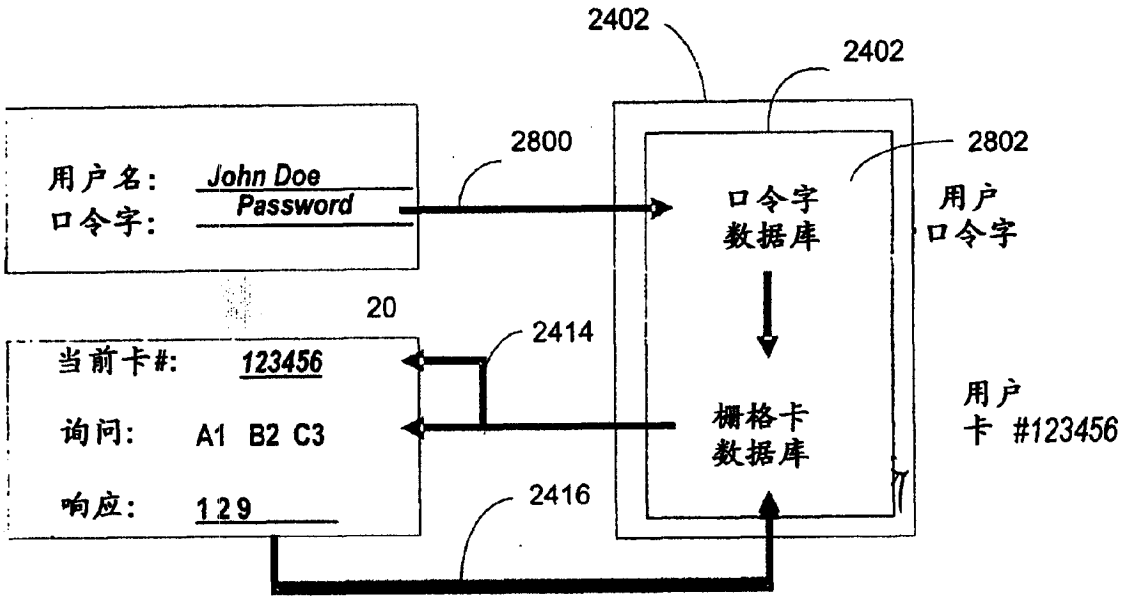

2402
2402
用户名: John Doe
口令字: Password
2800
2802
口令字
数据库
用户
口令字
20
2414
当前卡#: 123456
询问: A1 B2 C3
响应: 129
栅格卡
数据库
用户
卡 #123456
2416

图 28

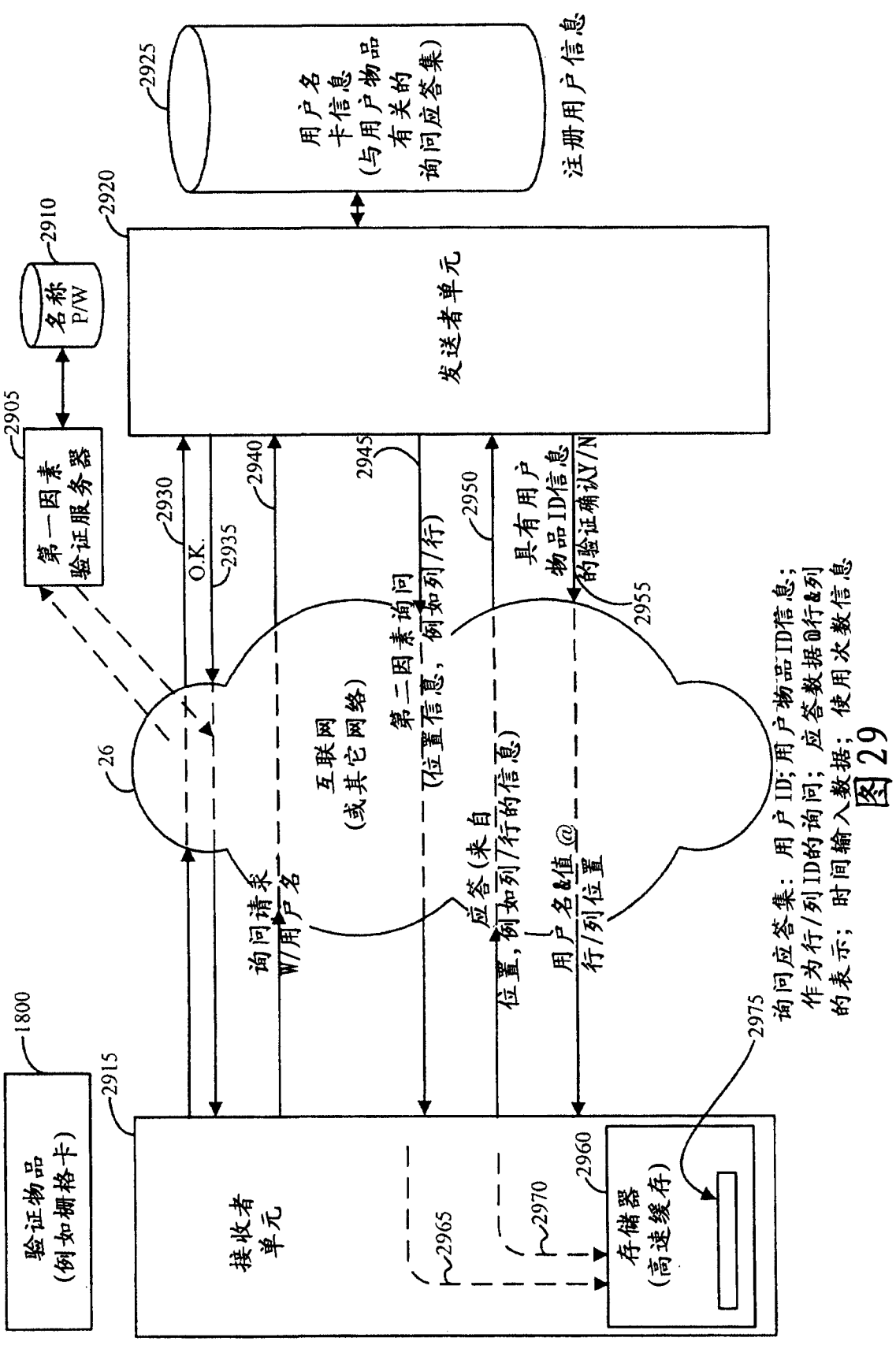

2925
用户名
卡信息
(与用户物品
有关的
询问应答集)
注册用户信息
2920
发送者单元
2910
名称
P/W
2905
第一因素
验证服务器
2930
O.K.
2935
2940
2945
2950
具有用户
物品ID信息
的验证确认Y/N
2955
26
互联网
(或其它网络)
第二因素询问
(位置信息，例如列/行)
询问请求
W/用户名
应答(来自
位置，例如列/行的信息)
用户名&值@
行/列位置
1800
验证物品
(例如栅格卡)
2915
接收者
单元
2965
2970
2960
存储器
(高速缓存)
2975
询问应答集：用户ID;用户物品ID信息;
作为行/列ID的询问；应答数据@行&列
的表示；时间输入数据；使用次数信息

图 29

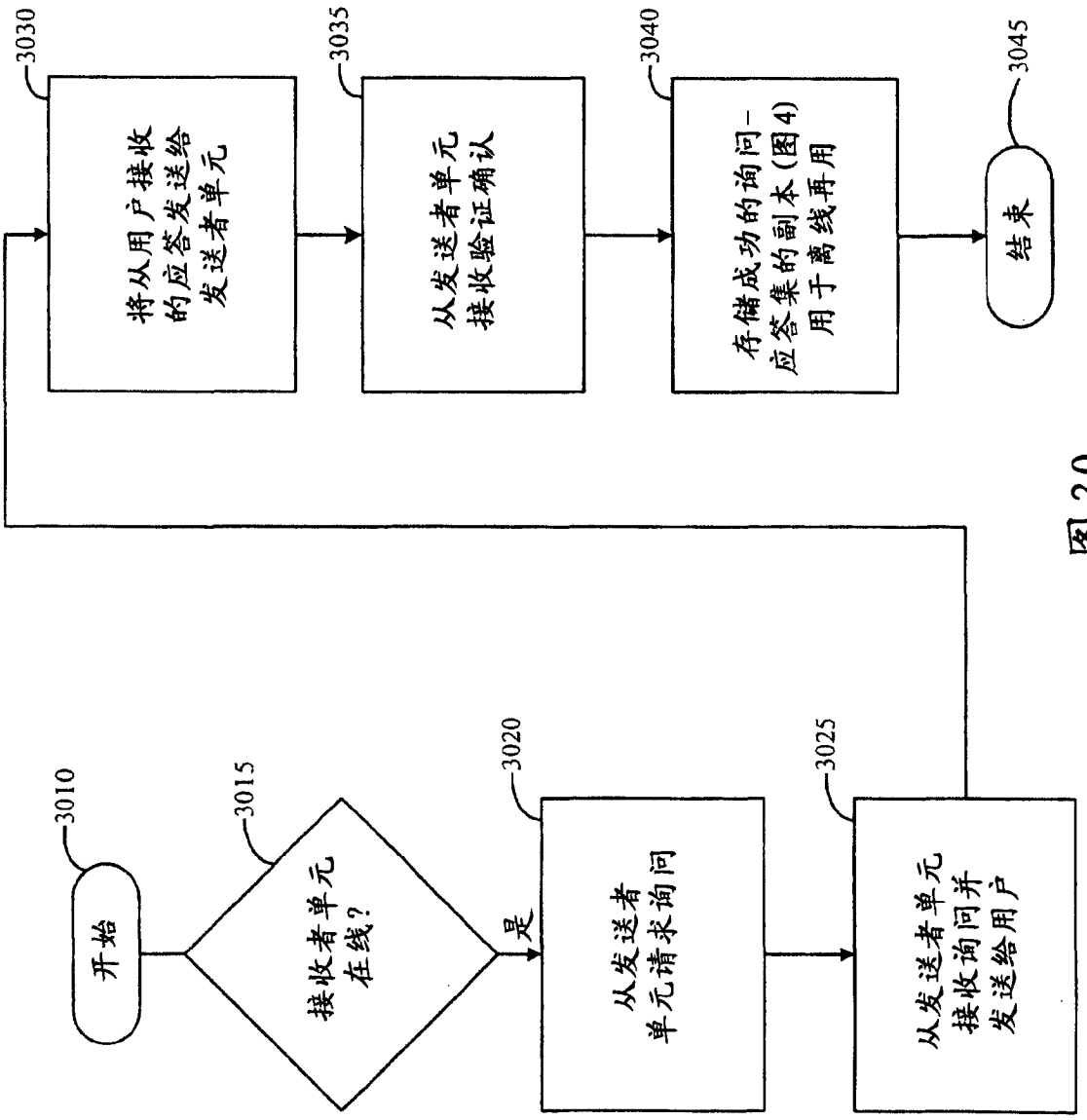

开始
3010
接收者单元在线?
3015
是
从发送者单元请求询问
3020
从发送者单元接收询问并发送给用户
3025
将从用户接收的应答发送给发送者单元
3030
从发送者单元接收验证确认
3035
存储成功的询问-应答集的副本(图4)用于离线再用
3040
结束
3045

图 30

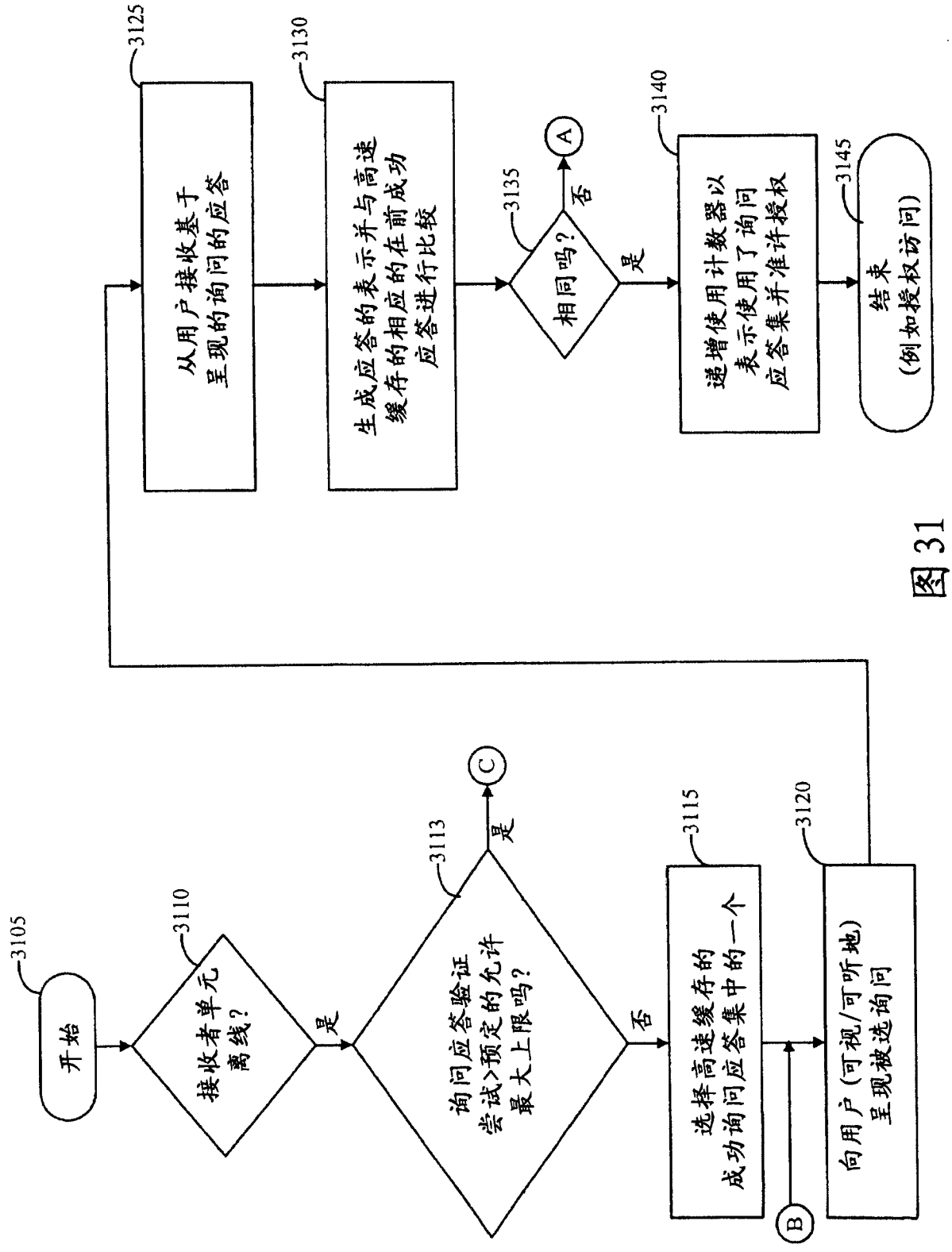

开始
3105
接收者单元离线?
3110
是
询问应答验证尝试>预定的允许最大上限吗?
3113
是
C
否
选择高速缓存的成功询问应答集中的一个
3115
B
向用户(可视/可听地)呈现被选询问
3120
从用户接收基于呈现的询问的应答
3125
生成应答的表示并与高速缓存的相应的在前成功应答进行比较
3130
相同吗?
3135
否
A
是
递增使用计数器以表示使用了询问应答集并准许授权
3140
结束(例如授权访问)
3145

图 31

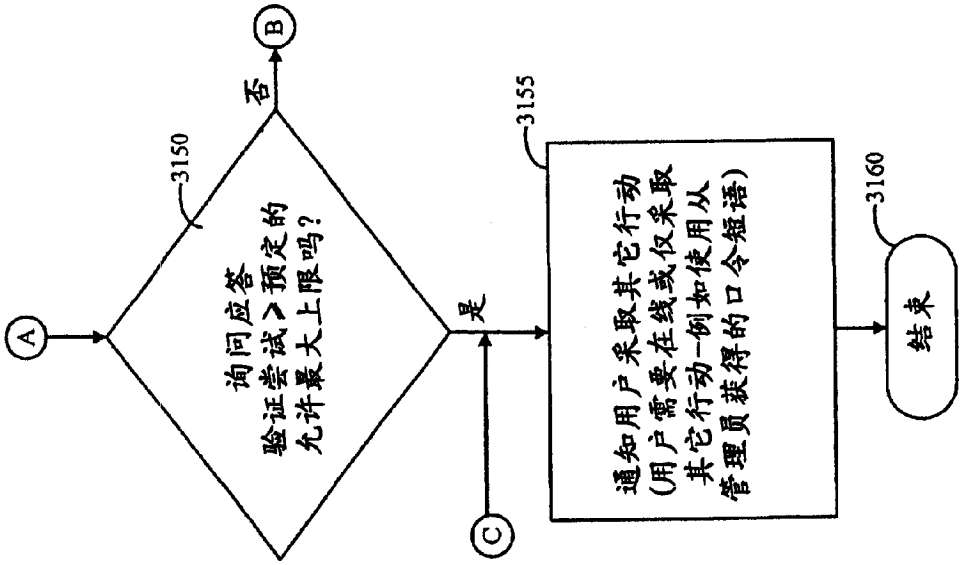

A
询问应答
验证尝试>预定的
允许最大上限吗?
3150
否
B
是
C
3155
通知用户采取其它行动
(用户需要在线或仅采取
其它行动-例如使用从
管理员获得的口令短语)
3160
结束

图 32

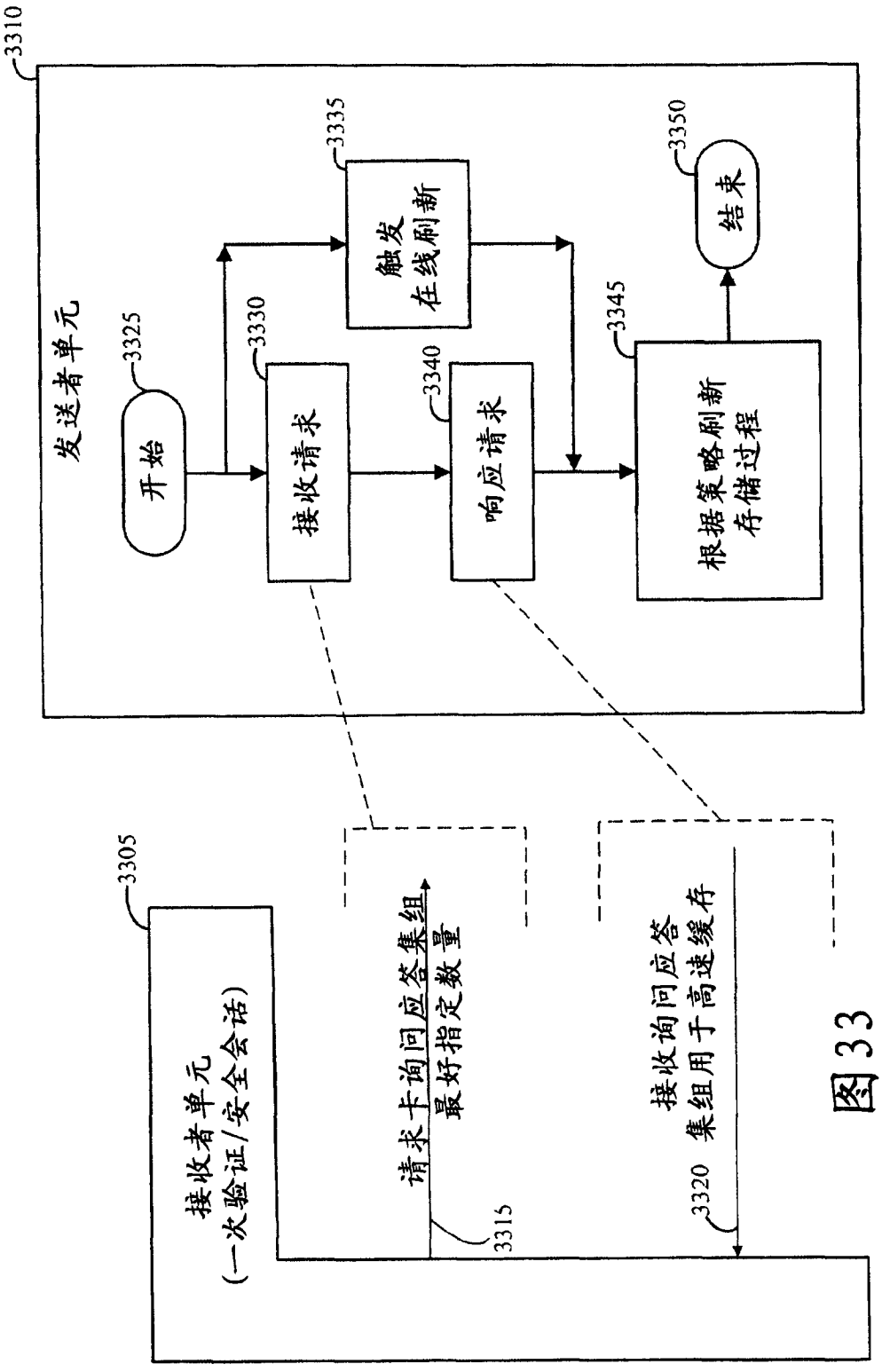

3310
发送者单元
开始
3325
接收请求
3330
触发在线刷新
3335
响应请求
3340
根据策略刷新存储过程
3345
结束
3350
3305
接收者单元
(一次验证/安全会话)
请求卡询问应答集组最好指定数量
3315
接收询问应答集组用于高速缓存
3320

图 33