[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/00 (2006.01)
H04L 9/32 (2006.01)
H04K 1/00 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200510121789.7

[43] 公开日 2006 年 10 月 18 日

[11] 公开号 CN 1848723A

[22] 申请日 2005.10.18
[21] 申请号 200510121789.7
[30] 优先权
[32] 2004.10.18 [33] US [31] 10/967,669
[71] 申请人 因特鲁斯特有限公司
地址 加拿大安大略
[72] 发明人 克里斯·沃伊斯

[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
代理人 李春晖

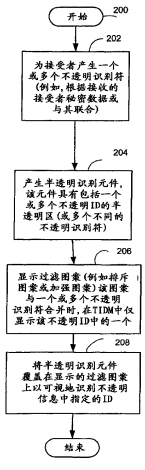
权利要求书 4 页 说明书 32 页 附图 23 页

[54] 发明名称

用于在发送单元和接受者之间提供相互认证的方法和设备

[57] 摘要

一种用于提供用户和发送单元(例如，目标源)之间的相互认证的方法和设备，在一个实施例中，包括为已被分配一个物品的用户确定，例如其上具有标记的卡片或其他适当物品，期望的发送者认证信息，该信息相对于嵌在该物品上的发送者认证信息。 通过使用发送单元提供的询问中的位置信息，可以将发送者认证信息定位在该物品上。 该方法包括为用户确定相关的物品标识信息，例如，被指定给该物品的序列号，或共享秘密，以及为用户发送询问，其中该询问至少包括位置信息，以允许用户标识定位在物品上的期望的发送者认证信息，以及发送物品标识信息。



1、一种用于提供用户和发送者之间的相互认证的方法，包括:

（a）为已经被分配物品的用户确定期望的发送者认证信息，该信息对应于嵌在该物品上的发送者认证信息，其中通过使用位置信息可以将该发送者认证信息定位在该物品上;

（b）为用户发送询问，该询问至少包括标识期望的发送者认证信息的位置信息;

（c）接收对于该发送询问的应答;

（d）确定接收的对于该询问的应答是否包括该期望的发送者认证信息，该信息被发送询问中的位置信息标识;

（e）如果接收的发送者认证信息不是该期望的发送者认证信息，那么为用户重新发送至少包括先前发送过的相同位置信息的同一询问；以及

（f）重复步骤（d）和（e）直到接收的应答包括该物品上的期望的发送者认证信息。

2、如权利要求1所述的方法，其中该物品至少包括交易卡、卡片、半透明卡或可视显示卡中的一个。

3、如权利要求1所述的方法，其中步骤（f）包括为每一个会话重复步骤（d）和（e），直到接收的应答中包括该物品上的期望的目标源认证信息。

4、如权利要求1所述的方法，其中在发送该询问之前，该方法包括:

从用户接收用户认证信息；以及

根据接收的用户认证信息认证该用户，并且如果该用户认证成功，那么根据该用户认证信息执行步骤（a）。

5、如权利要求1所述的方法，其中该位置信息包括用于在显示设备上显示的电子传输的数据。

6、如权利要求1所述的方法，其中发送给该用户的物品包含排列成行和列的发送者认证信息。

7、如权利要求4所述的方法，其中该用户认证信息包括用户名和密码。

8、一种用于提供用户和发送者之间的相互认证的方法，包括:

（a）为已经被分配物品的用户确定期望的发送者认证信息，该信息对应于

嵌在该物品上的发送者认证信息，其中通过使用位置信息能够将该发送者标识信息定位在该物品上;

（b）为同一用户确定对应的物品标识信息;

（c）为用户发送询问，该询问至少包括标识该期望的发送者认证信息的位置信息，并将该用于认证该发送者的物品标识信息发送给该用户；以及

（d）根据对于该询问的应答认证该用户，该应答包括根据位置信息从该物品获得的发送者认证信息。

9、如权利要求 8 所述的方法，其中在发送该询问以前，该方法包括:

接收用户的用户认证信息；以及

根据接收的用户认证信息认证该用户，如果该用户认证成功，那么根据该用户认证信息执行步骤（a）和（b）。

10、如权利要求 8 所述的方法，其中该物品标识信息至少包括用户和发送者知道的共享秘密和物品序列号中的一个。

11、一种用于提供用户和发送者之间的相互认证的方法包括:

提示用户输入第一级认证信息;

接收来自用户的第一级用户认证信息;

验证接收的第一级用户认证信息;

根据接收的第一级用户认证信息，为已经被分配物品的用户确定期望的发送者认证信息，该信息对应于嵌在物品上的发送者认证信息，该物品已被分配给该用户，其中可以通过使用位置信息将该发送者认证信息定位在该物品上;

为用户发送询问，该询问至少包括: 指定物品上的第一级用户认证信息的位置信息以及用于向用户认证发送者的物品标识信息;

根据该位置信息，相对于预期的第二级用户认证信息，验证接收的来自物品的第二级用户认证信息；以及

如果该第二级用户认证信息没有验证成功，那么继续为下一个用户会话发送同一电子询问和物品标识信息，该询问具有定位在该物品上的相同的指定的第二级用户认证信息和用于向用户认证发送者的物品认证信息，直到同一电子询问被成功验证。

12、如权利要求 11 所述的方法，其中该物品标识信息至少包括用户和发送者知道的共享秘密和物品序列号中的一个。

13、如权利要求 11 所述的方法，其中第一级用户认证信息包括用户密码信息和用户标识信息。

14、如权利要求 11 所述的方法，其中该位置信息和该物品标识信息包括用于显示在显示设备上的电子传输数据。

15、如权利要求 11 所述的方法，其中该发布给用户的物品包含排列成行和列的发送者认证信息。

16、一种用于提供用户相互认证的设备，包括:

一个或多个处理设备；以及

包含可执行指令的存储器，该指令使所述的一个或多个处理设备:

（a）为已经被分配物品的用户确定期望的发送者认证信息，该信息对应于嵌在该物品上的发送者认证信息，其中通过使用位置信息可以将该发送者标识信息定位在该物品上;

（b）为用户发送询问，该询问至少包括标识该期望的认证信息的位置信息;

（c）确定接收的对于该询问的应答是否包括在发送询问中位置信息标识期望的发送者认证信息;

（d）如果接收的目标认证信息不是该期望的发送者认证信息，那么为用户重新发送至少包括先前发送的相同位置信息的同一询问；以及

（e）重复操作（c）和（d），直到该接收的应答包括该物品上的期望的目标源认证信息。

17、如权利要求 16 所述的设备，其中该存储器包括指令使所述的一个或多个处理设备，在发送该询问之前，根据接收的用户认证信息认证该用户，并且如果用户认证成功，那么根据该用户认证信息执行操作（a）。

18、如权利要求 16 所述的设备，其中位置信息包括用于在显示设备上显示的电子传输数据。

19、如权利要求 16 所述的设备其中该用户认证信息包括用户名和密码。

20、一种用于提供用户相互认证的设备包括:

一个或多个处理设备；以及

包含可执行指令的存储器，该指令使所述的一个或多个处理设备:

（a）为已经被分配物品的用户确定期望的发送者认证信息，该信息对应于嵌在该物品上的发送者认证信息，其中通过使用位置信息可以将该发送者标识

信息定位在该物品上;

（b）为同一用户确定相关的物品标识信息;

（c）为用户发送询问，该询问至少包括标识用于认证发送者和用户的该期望的发送者认证信息的位置信息，并将该用于认证该发送者的物品标识信息发送给该用户；以及

（d）根据对于该询问的应答认证该用户，该询问包括根据位置信息从该物品获得的发送者认证信息。

21、如权利要求20所述的设备，其中该物品标识信息至少包括用户和发送者知道的共享秘密和物品序列号中的一个。

22、一种用于提供用户相互认证的设备包括:

一个或多个处理设备；以及

包含可执行指令的存储器，该指令使所述的一个或多个处理设备:

发送用户第一级认证信息提示请求;

验证响应该提示请求接受该信息接收的第一级用户认证信息;

根据接收的第一级用户认证信息，为已经被分配物品的用户确定期望的发送者认证信息，该信息对应于嵌在物品上在的发送者认证信息，该物品已被分配给该用户，其中通过使用位置信息可以将该发送者认证信息定位在该物品上;

为用户发送询问，该询问至少包括：指定物品上的第一级用户认证信息的位置信息以及用于向用户认证发送者的物品标识信息;

根据该位置信息相对于预期的第二级用户认证信息，验证接收的来自物品的第二级用户认证信息；以及

如果该第二级用户认证信息没有验证成功，那么继续为下一个用户会话发送同一电子询问和物品标识信息，该询问具有定位在该物品上的相同的指定的第二级用户认证信息和用于向用户认证发送者的物品认证信息，直到同一电子询问被成功验证。

用于在发送单元和接受者之间提供相互认证的方法和设备

相关未决申请

这是一美国专利申请的部分继续，该美国专利申请的发明名称为“METHOD AND APPRATUS FOR PROVIDING ELECTRONIC MESSAGE AUTHENTICATION”，序列号为 No.10/849402，申请日为 2004 年 5 月 19 日，发明人为 Voice 等并为直接受让人所有，其也是如下美国专利申请的部分继续，其中该美国专利申请的发明名称为“METHOD AND APPRATUS FOR SECURELY PROVIDING IDENTIFICATION INFORMATION USING TRANSLUCENT IDENTIFITCATION MEMBER”，序列号为 No.10/748523，申请日为 2003 年 11 月 30 日，发明人为 Chiviendacz 等并为直接受让人所有。

技术领域

本发明一般涉及用于在用户和目标源或信息发送实体之间提供认证的方法和设备，更具体的，涉及采用软令牌或硬令牌在用户和目标源之间提供相互认证的方法和设备。

背景技术

众所周知的相互认证系统和方法就是试图对信息用户或接收者进行认证，所述信息由内容服务提供商或其他目标源提供，也就是说，例如可以通过在线通信链接如互联网、内联网或其他合适的无线或非无线网络访问。该方法和设备试图阻止试图黑客或其他偷取用户身份的人的恶意使用。例如，恶意的实体可以使用合法银行的地址发送电子邮件并将接受者引导至“假网站”。接受者认为这是一个合法银行并且会被哄骗着提供信息例如帐号和密码，而恶意的实体会利用该信息访问接受者的在线帐户。这个问题在消费者世界是非常迫切的，因为传统的在线相互认证方法非常复杂，一般要求昂贵的硬件配置并且将用户的交互复杂化，使得这种相互认证技术非常不实用。因此，希望提供一种系统和方法，该系统和方法允许通过采用相对不那么昂贵但很安全的方式来认证正在访问预期的目标组织（例如发送实体）的用户或接受者。

现在所知的两要素认证技术就是，例如，使用第一认证要素来认证最终用

户的身份和用于认证的第二要素，该第二要素用于认证以补充一般用于第一要素认证的用户名和密码。第二要素的概念就是用户能够利用他们知道的（也就是他们的密码）和拥有的东西（也就是这个第二要素可以是，例如，硬令牌）进行认证。一般该第二要素机构是以硬件为基础的并被物理分配给最终用户。例如，我们知道的时间同步令牌有时也被认为是多要素认证技术。几种公知技术将在下文作进一步描述。

并且，我们知道与因特网应用有关的多种用于执行目标组织认证的方法包括，例如，安全套接字层服务器认证，该认证根据容纳给定的网络应用的组织的身份从受信第三方提供证书。然而，其能够要求用户执行双击屏幕图标并从头到尾读一遍信息的手工步骤。手工操作的要求经常使其不能连续执行，这样，会破坏该方法的有效性。此外，我们也知道客户安全插件应用，该应用包括最终用户下载和安装客户端软件，该软件提供用户何时与合法网站联系的可视指示。然而，下载和安装软件或通过几步人工操作来验证目标组织的身份对于最终用户来说是繁重的。

此外，用户和目标组织认证方法在扩展为其他通信信道时是不实用的，该信道例如为交互声音响应系统或通过可移动装置的通信，该可移动装置例如为便携式电话，个人数字助理，因特网设备，或其他可移动装置，因为它们可以依赖对于基于 web 的应用唯一的用户播放和输入方法。

保证已经发送的发送电子邮件信息或其他电子信息是由可以被信任的（也称为可靠的）的发送者发送的可帮助确保重要信息不被不择手段的用户组偷窃并能够帮助限制垃圾邮件和网页仿冒（phishing）。网页仿冒是一种因特网诈骗形式，通常包括看起来是合法组织发送的大量邮件，例如银行或其他金融机构或其他组织。这些电子邮件通常诱导接受者至欺诈网站或在该网站他或她被哄骗着泄漏个人或金融信息。一种网页仿冒欺诈的替换形式是不询问这样的信息但是一旦进入该 URL，就会执行一种能让欺诈者获得来自接受者机器的信息的按键登陆程序的下载。然后该信息被用于身份偷窃和诈骗。

因为网页仿冒攻击很昂贵并消耗公司的资源，所以例如大容量目标公司会遭遇大量攻击并且上亿的网页仿冒信息会通过过滤系统，这会降低电子邮件的传递，耗尽服务器的可用处理时间并最终导致重要的金融数据流失给不法方。

已经知道试图解决该问题的几种解决方案。因为网页仿冒攻击经常开始于

来自伪造发送地址的大量电子邮件，因此减少垃圾邮件的努力在某种程度上降低了网页仿冒攻击的数量。例如，一种被叫做是发件人策略框架的方法，信息始发者或始发者域以目录或其他适当形式出版合法的发送计算机地址，该地址可被接收消息传输代理验证。该消息传输代理通过DNS服务器（域名服务器）验证接收的消息。然而，该技术要求广泛采用SPF使能的消息传输代理，执行和调度该技术会很昂贵。

另一种被叫做协调垃圾邮件减少初始技术的技术再次要求始发者域中的始发者出版合法的发送计算机地址，该地址可被接收消息传输代理以如上所述的较相似的方法验证。

另一种技术要求域数字签名电子邮件，该签名被接收消息传输代理通过DNS服务器进行验证。此外，这要求广泛采用改进版本的消息传输代理。

另一种技术利用S/MIME协议，其中发送个人或域数字签名电子邮件，该邮件被接收输入的消息传输代理或用户电子邮件客户验证。这要求特殊电子邮件客户特征或接受者消息传输代理，这些特征和代理通常在基于电子邮件客户的网络中得不到支持。

另一种技术采用在发送者与接受者之间共享的秘密图像。如知道的那样，用户将个人图像发送给该认证服务器。该服务器存储接受者发送的图像。然后认证服务器可将个人图像连同电子邮件一起发送给接受者并且该用户看到的图像就是他发过的那个。另外，登陆到网站期间，该服务器在登陆页面中包含该图像以便当用户看到他们的个人图像（例如参见www.passmarksecurity.com）时相信该登陆页面。其他缺点之一就是，多次登陆时该系统利用同一图像直到改变该共享图像为止，同时要求接受者选择图像并将图像发送到发送服务器。

此外，我们知道其他系统尝试提供接受者认证，而不是发送者认证。例如，美国专利号5712627公开，在分配的卡上的可寻址的位置之一具有索引标记的已发行标识卡。该卡具有不同数目的行和列可被该行和列寻址的字母或符号。为了确定寻找访问数据的人是否被认证并获得其请求的访问，该标识卡被分配给被认证的人。寻找访问的请求人提供卡上一个或多个可寻址位置上的安全系统规定的标记。为了通知请求人输入或发回哪个标记，该系统选择特殊卡上显示的坐标标记。然后，接受者必须返回该定位在安全系统发送的地址上的该标记。如果该标记与分配给寻找访问的人的标记相匹配，则允许该访问。然而，

该系统不解决关于网页仿冒的问题，因为系统提供的是接受者认证而不是发送者，并要求寻找访问该系统的人标识他自己，并且该系统通过定位在安全卡上的用户信息要求进行输入和发送。

还知道已采用的其他认证系统，例如，在军事上，已采用使用发送者和接受者持有的卡片的数字密码／认证系统。例如通过使用一个询问和应答认证方案对传输进行认证。例如电子传输的发送者可使用该卡片并随机选择一组行和列并将该行列标识符作为一个询问进行传输。对于应答，可使用行列标识符查找字母表中的字母然后便返回通知。因而，该发送者能够确认该接受者持有卡片。然而，反之发送者发给接受者的认证可通过重复另外，的询问和应答实现，并且发送者和接受者都应该持相同的认证卡片以实现相互认证。

另一技术也使用在发送者和接受者两端均包含多个行和列信息的卡片，然而，该传输认证方案用于验证传输。例如在传输认证期间，传输认证作图器的多个列被定位在密码表的背部并用于认证一发送者。通过指定的代表例如单元指挥者产生列分配。该列分配很早就已被发送者和接受者所知。传输认证作图器只能使用一次。使用该已分配列中的第一未被使用的认证者并通过该认证者进行划线以预防其再一次被使用。因为事前知道该列信息，所以此方案不利用卡片上随机选择的信息以及不利用发送的坐标信息。因而，显然只传达该认证信息。如果发送者发送认证信息并且该信息是接受者所确定的有效信息，那么该接受者从卡片上划掉该认证信息。下次要求该认证时，会使用同一列中的下一个认证信息。因而，使用一种连续的和非随机的方法。然而，如果接受者的认证卡丢失或被不法方获得，因为他们知道列中的下一个认证信息，利用了非随机选择，以及卡片上已经标记，所以他们会充当一个发送者。该系统中，不发送坐标信息，因此发送者和接受者事先知道用于验证发送者的列信息。此外，如果接受者未收到发送者的传输，那么发送者和接受者之间的同步会丢失，这会导致接下来的认证尝试失败。

另外，，正如技术变得越来越完善那样，信息安全和用户身份安全变得越来越重要。例如，利用多因子认证方案试图阻挠电脑黑客或阻挠其他信息和用户身份的不正当利用。例如，双因子认证方案可使用接受者或用户熟知的信息，例如密码或个人身份号码（PIN）以及某种实际令牌如银行卡、信用卡、密码令牌或为了启动和完成在线交易而用户必须实际持有的其他实际令牌。认证的另

一等级可包括生物认证，该认证可包括扫描指纹、眼睛或其他生物特征以再次检验试图获取使用方法、装置、应用或其他权利的权利的用户是否为合适的用户。

熟知的交易卡可包括智能卡、磁条卡、以及其他便于银行交易、信用卡交易、或任何其他合适的交易的交易卡。正如本领域所熟知的那样，用户个人身份号码（PIN）通常要求与持有的银行卡一起以从自动取款机获得现金或另外执行一项在线交易。一种众所周知多因子认证技术是利用硬件令牌例如一种电池操作的智能卡的，并且在该智能卡的一部分显示周期性变化和表面上的随机数。当用户希望与该智能卡进行交易时，例如，该用户可以输入经常变化的看起来随机数。接收交易服务器将所接收的代码也就是该用户输入的智能卡上显示的代码与代码源生成器产生的相应数字进行比较。如果用户输入的代码与代码源生成器产生的数字相匹配，那么批准该交易并且该用户被授予特殊的权利例如访问银行帐户、购买商品、获取信息、有权使用网站或其他应用软件，或任何其他所描述的适当的权利。然而，该硬件令牌可能会非常昂贵并且是电池供电，因此需要更换电池，以及由于潮湿或任何其他问题产生的潜在电子故障会关系到电子的安全。

其他不采用这样的显示屏的智能卡需要读取资料例如磁条的读卡器。这可能是用户希望执行在线交易但却没有坐在包含或已访问到磁条读卡器的终端前的一个限制。

在一个明显不相关的领域中，我们熟知的半透明卡例如包含半透明图画或图案的塑料卡被可视地评估时并没有暗示任何特定信息。然而，当半透明标识卡被覆盖在具有相关的背景过滤图案的显示器上时，组合卡上的合并图案与显示屏幕上的背景图案以显示表面可标识的消息或单词如“对不起”或“你是胜利者”。这些是静态消息对任何用户来说不是唯一的并且典型地仅包括单个消息。该塑料卡可被用于例如观察持有者是否赢得奖金。例如该卡片可以电子邮件的形式邮寄给全体成员。然后接受者访问半透明卡上标识的或相反电子邮件信息中指定的网页，以观察他们是否赢得了奖金。然而，该塑料卡不提供多因子认证，不是用户特有的，不包括多个消息并典型地包括静态消息。

因此，需要一种解决上述一个或多个问题的方法和设备。

附图说明

图 1 是说明根据本发明一个实施例的用于安全提供标识信息的一个系统范例的结构图;

图 2 是说明根据本发明一个实施例中的用于安全提供标识信息的一种方法范例的流程图;

图 3 是说明图 2 所示方法的进一步分解图。

图 4 是说明根据本发明一个实施例的安全标识信息成员的一个范例图;

图 5 是用图解法说明根据本发明一个实施例的一种便于用户认证或用于安全提供标识信息的注册屏的一个范例图;

图 6 是用图解法说明书根据本发明一个实施例的一种可显示的可视过滤图案的一个范例。

图 7 是用图解法说明根据本发明一个实施例的一种一个或多个定位在半透明标识元件上的不透明标识符中的视觉上可标识定义的标识符。

图 8 是根据本发明一个实施例的一种用于安全提供认证信息的系统范例图。

图 9 是详细说明根据本发明一个实施例的半透明认证成员发行者范例的结构图。

图 10 和 11 示出根据本发明一个实施例的一种用于安全提供认证信息的方法范例的流程图。

图 12 说明根据本发明一个实施例的一种包括包含一半透明标识元件部分的交易卡范例。

图 13 说明根据本发明一个实施例的一种包括半透明标识成员的交易卡的另一个范例。

图 14 说明本发明另一个实施例的一种安全标识信息成员的范例图。

图 15 用图解法说明根据本发明一个实施例的显示不透明标识符信息范例。

图 16 是说明根据本发明实施例的用于安全提供标识信息系统的另一个范例的结构图。

图 17 是说明根据本发明实施例的一种用于安全提供标识信息的方法范例的流程图。

图 18 是一项物品范例说明，例如卡片，该物品可被用于根据本发明一个实施例的用于提供电子消息认证的方法中。

图 19 说明根据本发明一个实施例的一种交易卡范例，该卡包括用于提供电子消息认证的发送者认证信息和位置坐标信息。

图 20 是说明根据本发明一个实施例的一种用于提供电子消息认证的方法范例的流程图。

图 21 是一个图解说明，其示出根据本发明一个实施例的一种具有附加发送者认证信息和位置坐标信息的消息范例。

图 22 是说明根据本发明实施例的用于提供电子消息认证的系统范例的结构图。

图 23 是说明根据本发明实施例的用于提供电子消息认证方法范例的流程图。

图 24 是说明根据本发明实施例的用于在用户和目标源之间提供相互认证的系统范例的结构图。

图 25 是说明根据本发明实施例的用于在用户和目标源之间提供相互认证的方法范例的流程图。

图 26 是说明根据本发明实施例的用于在用户和目标源之间提供相互认证的另一个方法实施例范例的流程图。

图 27 是说明根据本发明实施例的用于在用户和目标源之间提供相互认证的方法的另一范例的流程图。

图 28 以图解显示的形式说明根据本发明一个实施例的一种用于在用户和目标源之间提供相互认证的装置范例的结构图。

具体实施方式

简要地，一个实施例中的一种用于在用户和发送单元（例如目标源）之间提供相互认证的方法包括：确定用户渴望的发送者认证信息，该用户已被分配了一项物品，例如卡片或其他已标记的合适物品，该信息与嵌入在该物品上的实际发送者认证信息相应。通过使用在询问中的发送单元提供的定位信息，该发送者认证信息可被定位在该物品上。该方法包括为用户确定相应的物品标识信息，例如一系列指定在该物品上的数字，或共享秘密，并且为用户发送询问，该询问中至少包括了定位信息以允许用户标识定位在物品上的用户渴望的发送者认证信息。然后该用户接收定位信息和物品标识信息并且由于用户持有的物品还包括物品上的物品标识信息，因此可将该物品标识信息用作认证信息，以

指出发送者发送的信息是值得信任的。然后用户利用已发给用户装置的定位信息，例如通过目标源发送的行列信息，来确定例如相应的用户期望的发送者认证信息是否定位于该物品上，并将该询问的应答发送回上述目标源（例如，发送单元）。然后发送者根据该询问的应答认证该用户。该应答包括用户认证信息，该信息从所述物品获得，称为用户期望的发送者认证信息。如果根据定位信息，收到的发送者认证信息与用户期望的发送者认证信息相匹配，那么目标源准许适当访问该用户（例如，用户装置）。因而，发送者与定位信息一起发送物品标识信息后，例如，一级认证已被确认成功。第一级认证可包括，例如，在初始注册过程中用户将密码和用户 ID 发送到目标源，正如本领域所熟知的那样，随后根据成功的第一因子认证过程接着发送定位信息和物品标识符信息。

在另一个实施例中，一种用于提供相互认证的方法不需要将物品标识信息发送给用户，然而却仅需要发送定位信息以允许用户标识该物品上的相应认证信息，并且将用于验证的应答发回到目标源。然而，在该实施例中，如果应答不包括预期的目标源认证信息，正如发送单元发送的那样，那么该方法将包括重复对用户的另外，询问，该询问包括与先前发送的信息具有的相同定位信息。该过程重复再三，例如，每个连续对话，直到根据询问过程中发送的定位信息用户发送合适的来自于该物品的目标源认证信息。

此外，还公开了执行上述方法的相配合的装置。并且，使用了上述两种方法的组合以实现一种加强型相互认证过程。

还公开了一种用于提供电子消息认证的方法，该方法使用了物品（也可被认为是成员或令牌），例如卡片、标签、或任何其他适当的物品，该物品包括发送者认证信息和定位信息，例如行和列的首部。在一个实施例中，可将物品发布给每一个赶兴趣的接受者，该物品包括可被相应定位信息如行和列标识符标识的发送者认证信息。当电子消息的发送者希望将消息发送给赶兴趣的接受者时，发送者发送电子消息以及定位信息和被该定位信息标识的定位在地址上的用户期望的相应发送者认证信息。这包括表示该地址和认证信息的数据（例如定位信息和认证信息本身的索引、参考、或其它任何合适的表达式）。然后，在一个实施例中接受者可以观察物品上的相应地址并且查看该发送的用户期望的发送者认证信息是否与物品上的发送者认证信息（也称为期望的发送者认证信息相匹配）。如果匹配，那么接受者将信任发送者发送的消息。因而，简易卡或

其他物品可被用于认证发送者的消息以阻止网页仿冒或其他发送者认证问题。其他实施例将会被本领域内的普通技术人员所知晓。

此外，还公开了一种用于提供电子消息认证的系统，该系统执行上述方法，并且还公开了一种交易卡，卡上包含标签形式或作为卡本身的一部分的定位信息和用户认证信息。在另一个实施例中，该物品可以是半透明物品以允许光通过，因此可视过滤图象和发送者认证信息可与消息一起被发送者发送。用户可将该物品放在显示屏上并将起覆盖在发送者发送的可视过滤图象上。如果发送者认证信息结果与消息中发送的结果相匹配，那么接受者可以相信消息的发送者。

在另一个实施例中，一种用于安全提供标识信息的设备和方法可为接受者产生一个或多个不透明用户（例如，接受者）标识符，例如多个根据用户秘密数据如密码、个人身份号码或其他秘密或非秘密信息产生的标识符，或者不基于用户秘密数据的标识符，例如随机产生的随后与该用户相关的标识符。在这种情况下，不使用相关用户的信息，但该标识符仍然可以标识该用户。在另一个实施例中，可使用单个不透明标识符。

在一个实施例中，该方法和设备可产生半透明标识元件（TIDM），例如一部分或整个塑料卡、板、膜、或其他具有包括一个或多个不透明标识符的半透明区域的合适元件。如这里使用的那样，半透明区域也可以包含透明区域。例如，该半透明标识元件可由透明或透明板材制成，包括烟灰色塑料或其他墨水绘制的适当颜色的不透明标识符（包括非字母信息）或以其它方式放在上面或嵌在里面。所述一个或多个不透明标识符可以是如一次性的认证标识符，它对于半透明标识元件的接受者来说是唯一的。因而，该半透明标识元件或卡片包含可视随机图案的信息。

当用户想要使用该半透明标识元件时，还可以产生用于在显示装置上显示的相应可视过滤图案。例如，从直观上看该可视过滤图案也是随机的，但当将该半透明标识元件上的一个或多个不透明标识符真实地结合在一起时，该一个或多个不透明标识符中的被定义的那个可以真实地显示出来。在一个实施例中，用户可将该半透明标识元件覆盖在显示装置指定部分的表面或潜在显示装置指定部分中，以显示该可视过滤图案。组合半透明标识元件上的可视过滤图案与不同不透明标识符图案的合并图，以形成可视显示的单个标识符或来自该一个

或多个标识符的消息。因此，例如在一个实施例中，看起来的随机图案产生在屏幕上，并且有助于确保仅有单个标识符真实地显示给用户，其中该用户正在观察覆盖在正显示于显示装置的可视过滤图案上的半透明标识元件。

因此，如果想要，例如访问半透明标识元件发行人的安全官员可利用空白玻璃卡封装，该玻璃卡可用于将半透明标识元件连接本地打印机。该半透明标识元件可被打印出来并具有可充当一个或多个不透明标识符的半透明色图案，或具有其他用户看来半随机或不透明显示的适当标记。也可使用颜色或颜色背景防御光复印攻击。将会认识到可通过分配供应者和网络或服务网站提供半透明标识元件发行人的部分或全部功能。例如，接受者可通过网络连接访问 TIDM 发行服务并且本地打印该 TIDM 或通过电子邮件接收该 TIDM。而且，标识符可由组织提供并将其发送给另一组织用于打印和制造。正如所述的也可以利用其他分配操作。

一旦为用户显示可视地标识符，用户通过用户接口输入该可视显示的标识符，在此与预期标识符进行比较。如果输入的标识符与预期标识符相匹配，则表明认证正确并且接受者可被允许访问装置、应用、或处理过程或其他期望的权利（或接受提交的数据－例如投票）。此外，还可保留取消的半透明标识元件列表以避免由于被偷窃或丢失半透明标识元件造成的泄密。该列表可存储在任何适当的地方并被服务供应者、半透明标识元件发行者或任何适当的团体更新。由于该半透明标识元件不要求电子产生随机数，因此，此半透明标识元件的成本会非常低并且由于其对湿度或其他与智能卡典型相关的损害不敏感，因此其可靠性也会相当的高。

在替换的实施例中，智能卡或其他交易卡或非交易卡（例如，投票卡或其他适当的卡）如果期望的话可包括半透明标识元件。因此交易卡被解密并包括例如包含卡标识信息部分（例如交易卡号，其可被印在卡上例如通过提高复印或电子化或者通过任何其他适当的存储机构如磁条或任何其他适当机构），以及包含具有半透明区域的半透明标识元件部分，该半透明区域包括一个或多个不透明标识符。为了加强安全，因而如信用卡、银行卡或任何其他交易卡可包括窗口，该窗口包括该半透明标识元件，或者可具有交易标识号或其他贴在常规交易卡上的标识信息。

在另一个实施例中，半透明标识元件的角色与接受单元是相反的。例如，

在一个实施例中，该半透明标识元件包括可视过滤图案和显示至少一个不透明标识符的显示屏，该不透明标识符可以是如对用户来说是唯一的、表示用户认证的数据，或其他期望的数据。在显示不透明标识符的显示装置上覆盖半透明标识元件（可视过滤器）的合并，展现了（反模糊）屏幕上的至少一个不透明标识符。元件上的可视过滤图象保持相同，因为它印在该元件上，并且在每个对话期间或每隔其他适当的时间改变该显示的不透明标识符。

因此，会产生以下一个或多个优点。由于该半透明标识元件能被组织安全官员打印，因此无需制造成本并且能够为接受者在本地产生该元件。由于不需要电子设备，因此无需更换电池并且暴露在潮湿环境中也没有危险。不要求网络或无线连接例如使用磁条的装置典型需要上述连接。半透明标识元件可由任何其他适当厚度塑料或任何合适材料制成。由于可以在组织的本地生产，因此他们是耐用的并在被损害的情况下很容易替换。也可以在基本网络基础结构上进行投资以连续产生与屏幕上动态改变的代码相匹配的主代码，进而可不使用智能卡。

在一个实施例中，该被显示的可视过滤图象有选择性地照射半透明标识元件的一部分，以可视显示该一个或多个不透明标识符中的一个。该可视过滤图象可以随每个认证对话改变。一个或多个不透明标识符被打印并标记在半透明（或透明）卡上，并且该标记在用户的特定域内是唯一的。该一个或多个不透明标识符可通过很多适当技术如色彩发暗、字符调整、其组合或任何其他适当可视发暗技术而模糊。图 1 示出一个用于安全提供标识信息的系统 10 实施例，该系统包括操作产生安全标识元件的半透明标识元件发行者 12，半透明标识元件 14，可视过滤发生器 16，半透明标识元件认证模块 18，接收单元 20 以及存储器 22。在该实例中，可视过滤发生器 16 和半透明标识元件认证模块 18 是半透明标识元件确认者 24 的一部分，该确认者可作为一个或多个在计算单元例如个人电脑，工作站，服务器，手持装置，或任何其他适当装置或多网络装置上执行的软件模块来实现。在该实施例中，半透明标识元件确认者 24 有效连接至网络服务器，该服务器按顺序有效连接至网络如因特网 26 以促进基于网络的接收单元 20 与半透明标识元件确认者 24 之间的通信。因此该软件和处理装置形成多级电路。并且，正如这里所使用的，电路也可以指任何适当形式的任何适当的电子逻辑包括但不局限于硬件（微处理器，离散逻辑，状态机，数字信号

处理器等等），软件，固件或上述装置任何适当组合。

半透明标识元件发行者 12，可视过滤发生器 16，以及半透明标识元件认证模块 18 可由任何适当的方式实现，并且优选，但不限于，在一个或多个计算设备上执行的软件模块，该计算设备包括一个或多个执行存储在存储器中的指令的处理设备。

在一个实施例中，半透明标识元件发行者 12 将作为本地服务器进行描述，该服务器利用打印机或其他适当的机构产生半透明标识元件 14。半透明标识元件包括半透明区，其上包含一个或多个不透明标识符。然而，会认识到的是，该半透明标识元件发行者 12 可作为半透明标识元件确认者 24 的一部分，或定位在任何其他包括网络服务器的适当设备上，并且会被认识到的是这里描述的任何软件程序也可以合理定位在任何适当的设备上。

存储器 22 可以是任何适当的本地或分布式存储器并且如果想的话还可定位在网络服务器或在本地。存储器可以是 RAM，ROM 或任何适当的存储器工艺。接收单元 20 可以是任何适当的设备如膝上型电脑，台式电脑，手持设备或任何其他适当设备，这些设备包括显示器 30 和用户接口，并可包括一个或多个执行存储在任何适当存储器中指令的处理设备。接收设备包括必要的电路以通过网络浏览器或其他应用程序或操作系统提供一个或多个用户接口如图形用户接口，并可包括语言标识接口或其他适当的用户输入接口。因此，该单元包括显示电路，操作该电路以显示定义的可视过滤图象，这样当该可视过滤图象与半透明标识元件上的一个或多个不透明标识符真实合并时，被指定的一个或多个标识符中的一个被可视显示出来；以及输入接口，操作该接口以接收表示该可视显示标识符数据。在一个实例中，用户接口可被用于请求输入与半透明标识元件相关联的序列号；以及请求输入公开的标识符以确定是否将渴望的权利授权给接受者。

并且如果期望，接收单元能够接收用于在显示屏上显示的过滤器或不透明标识符并通过完全不同的设备（或通过完全不同的渠道）例如单元电话，SMS 消息，电子邮件消息或其他适当渠道和设备将应答发回。

并参考图 2 和 3，将描述一种用于安全提供标识信息的方法。如块 200 所示接受者通过因特网或任何其他适当的机构将请求发送给半透明标识元件发行者 12，并要求发布半透明标识元件 14。例如可通过具有用户提供数据如密码或

其他秘密信息的接受者登陆在线金融机构实现。这表示该半透明标识元件发行者 12 接收接受者特定信息 32。

如块 202 所示，该方法包括为用户产生一个或多个不透明标识符，其可基于例如接受者特定信息 32 和/或其他信息 34。该其他信息 34 可以是半透明标识元件系列号或其他想要的适当信息。例如，这可以由该半透明标识元件发行者 12 或任何其他适当的实体实现。如块 204 所示，该方法包括产生具有半透明区 36 的半透明标识元件 14，该半透明区中包括一个或多个不透明标识符 38。该一个或多个不透明标识符 38 在该实施例中由半透明标识元件发行者 12 产生并以数据库形式存储在存储器 22 中。该一个或多个不透明标识符存储在存储器 22 中，使得当有必要创建合适的可视图象 40 以显示该渴望的被显示标识符 700 时，或检查返回的可视图象 700 时，顺序地访问他们。

例如，半透明标识元件发行者 12 可控制打印机打印作为半透明标识元件 14 的其上印有一个或多个不透明标识符的单元电话卡。图 4 示出了半透明标识元件的一个实施例。半透明标识元件 14 可由任何适当的材料如塑料或任何其他适当材料制成，该材料提供某种透明度，以便当一个或多个不透明标识符的合并覆盖在发光显示器上时，允许显示器中的光能（或缺少光能）与该一个或多个不透明标识符进行组合，以真实指定半透明标识元件上的一个或多个标识符中的一个。半透明标识元件上的一个或多个标识符也可以是多个不同的不透明标识符。

半透明标识元件 14 可以是卡片，板，膜或其他元件，上述元件如果想要可包括任何合适的粘合剂或连接结构用来应用在交易卡或任何其他适当材料的窗口上。半透明标识元件还可连接至交易卡，例如，通过使用适当连接结构将半透明标识元件连接到交易卡的底端或侧面。打印在半透明标识元件 38 上的一个或多个不透明标识符 38，如上所述，可以是字符（例如 ，ASCII），符号，印刷图案，有色文本或任何其他适当标记。当被接受者浏览时上述一个或多个不透明标识符 38 表面上呈现模糊和看起来的随机。在其他实施例中，希望打印墨水图案，其不包含字符的但相反可视地隐藏一个消息或其他信息，以便当其覆盖在显示器上时，显示器产生的图案与该打印图案进行组合，以允许浏览者解密显示的标识符。

半透明区 36 包括表示一个或多个标识符的信息图案，标识符可以是可用于

一个或多个认证会话或其他目的的唯一标识信息。优选地，一个或多个不透明标识符表示的信息图案对于给定的用户定义域是唯一的，以减少同一用户获得具有相同不透明标识符的同一半透明标识元件的可能性。半透明区36被配置(例如，调整大小）以覆盖接收单元20上显示屏30的至少一部分。在一个实施例中，每一个上述一个或多个不透明标识符可充当半透明标识元件接受者的一次性认证标识符。注意如这里用到，标识信息包括任何直接或间接用于用户认证（例如，TIDM接受者）和其他有关处理过程的信息，或用于访问期望的与处理过程和设备相关的权利，或任何其他除了在实现交易的时刻外打算保密的适当信息。

制造TIDM的方法包括接收用户对一个或多个不透明用户标识符的请求，并且记录用户和与该一个或多个不透明用户标识符相关的标识信息之间的连接。该方法可包括提供一个或多个不透明用户标识符给用户，其中上述一个或多个不透明用户标识符在发送给用户的半透明标识元件上，该一个或多个不透明用户标识符被发送给第三用户并放置在用户半透明标识元件上，该一个或多个不透明用户标识符被发送给用户用于放置在半透明标识元件上，并且从存在的不透明用户标识符池中选择该一个或多个不透明用户标识符。用户请求可包括用户特定信息并且该特殊用户信息可用于创建一个或多个不透明标识符或与其他信息进行组合产生一个或多个不透明用户标识符。

如块206所示，一旦该半透明标识元件14被产生并提供给接受者，该可视过滤发生器16，或其他适当机构就产生可视过滤图案用于在接收装置30的显示器30上显示。当接收装置显示该可视过滤图案40时，该可视过滤图案与定位在半透明标识元件14上的一个或多个不透明标识符进行可视组合，以指定该一个或多个标识符中的一个。换句话说，该可视过滤图案滤除掉不希望的标识符以显示选择的一个或多个标识符中的一个。

如块208所示，该方法可包括，例如通过接受者或设备，将半透明标识元件14覆盖在显示的过滤图案40上，以可视标识半透明标识元件14上不透明标识符中的一个。然后接受者输入该可视地标识的标识符以便于交易或访问与任何处理过程或感兴趣的装置相关的特定的期望的权利。

再一次如图3所示，将详细描述图2中的步骤。如块300所示，产生一个或多个用于接受者的不透明标识符可通过例如半透明标识元件发行者12或任何

其他适当实体获得接受者特定信息，如秘密或公开数据或非用户相关信息来完成。该过程也可以通过使用非用户相关的或非用户提供的材料实现，在某种情况下，产生的一个或多个不透明标识符随后与用户进行关联。当使用接受者特定信息时，可以是个人标识码，密码，用户名，帐号或其他适当资源。这可被指定为接受者特定信息32。如块302所示接受者特定信息32被适当组合，例如通过适当的数学函数或算法，以产生一个或多个不透明标识符38。其他信息34可以是例如随机数发生器产生的输出，可打印在半透明标识元件14上或由半透明标识元件发行者12存储的实际半透明标识元件序列号44（或其他TIDM标识信息），或任何其他适当信息。如块204所示，半透明标识元件序列号，或用于标识该半透明标识元件的任何其他适当信息，被分配给该不透明的一个或多个标识符38。应该认识到的是依据初始请求或半透明标识元件发行者12产生的半透明标识元件可选择半透明标识元件序列号以及将其与接受者特定信息32相关联。可组合该信息以产生一个或多个不透明标识符38。该半透明标识元件序列号44可存储在存储器22中，然后由该半透明标识元件确认者24使用（利用半透明标识元件14认证接受者）。这里描述的关于任意方法的步骤的顺序根据期望的结果可被适当重排序。

如块306所示，产生该半透明标识元件14可包括在塑料膜，板或卡片上以期望的形式打印该不透明的不同标识符，以形成该半透明标识元件14。如块308所示，在显示器上显示过滤图案40可包括随机从不透明标识符中选择被选择的标识符以在显示器30上形成可视过滤图案40，当该半透明标识元件14覆盖在该可视过滤图案时，该显示器显示上述被选中的不透明标识符中的一个作为被显示的标识符。

如图4至7所示，为了进一步说明如图4所示的实施例，该半透明标识元件14上已被印刷半透明标识元件序列号44或其他标识信息，并且一个或多个不透明标识符30已印刷在半透明区36内。如上述注解这也可印刷在玻璃纸材料或其他材料并且由常规打印机进行迅速调整，如果希望，以降低制造成本。然而，可以使用任意的适当材料或制造过程。一旦接受者持有该半透明标识元件14，就可以利用该半透明标识元件14而被提供多因子认证。

可以用任意适当方法产生过滤器。例如，从存储的一个或多个不透明标识符中选择一个被选中的不透明标识符，上述存储的标识符在TIDM上的位置已

被定义。可视过滤图案发生器16在预定义的TIDM版样上产生过滤图案，以确保该过滤器阻塞该合适的字符位置。任何其他适当技术也会用到。

如图5所示，接收装置20可通过网络浏览器或其他适当用户接口，输入屏，如果网络浏览器正在使用中可根据接收的HTML进行显示，该装置包括接收用户输入的区域，例如用户标识区500，密码区502，以及半透明标识元件序列号区44。用户通过适当的用户接口按钮504提交输入的信息。然后通过因特网将该信息发送到网络服务器并且如果想要还可以将其发送到半透明标识元件确认者24。如该实施例所示输入到用户ID区500或密码区502的信息可被认为是接受者特定信息，该信息在半透明标识元件发行者12初始生成该半透明标识元件14时被事先输入。

图6说明一个在显示器30上显示（根据接收的HTML网页产生）图形用户接口的实施例，便于利用半透明标识元件14安全提供标识信息。该图形用户接口可通过如网络浏览器和接收单元上的适当主处理器或任何其他适当处理器产生，并且定义可与显示器30上显示的可视过滤图案40相同或不同大小的覆盖区600。因此，响应图5中的注册屏幕，该半透明标识元件确认者24提交包含该可视过滤图案40以及图6中的应答接口屏幕的应答。接收单元20显示该可视过滤图案40与显示标识符区602，以允许输入一个或多个不透明标识符中的被显示标识符的ID。

图7以图形的形式说明了该半透明标识元件14覆盖在可视过滤图案40上以显示一个或多个不透明标识符中一个的情况。用户定位该半透明标识元件14，并因此该可视过滤图案40上的一个或多个印刷的不透明标识符38，以及可视过滤图案40，以及印刷的不同不透明标识符38的合并显示被显示的标识符700，其是由接受者在显示标识符区602输入的。然后用户将显示的标识符700提交给半透明标识元件确认者24，以认证特殊交易或访问特殊权利的用户。因此，响应用户或其他实体将半透明标识元件14覆盖在显示器30上，半透明标识元件确认者24接收表示被显示的标识符700的数据。该半透明标识元件确认模块18比较接收的被显示标识符700与相应的预期标识符702（参见图1），以确定接受者的适当认证是否是合适的。半透明标识元件认证模块18包括存储器22中的相应预期的标识符702，或在了解该可视过滤图案以及访问该不透明标识符3中产生该预期标识符，或可包括以任何其他适当方法的预期标识符702。

参考图 8 和 9 半透明标识元件 14 的发行将作为一个范例进行详细描述。为获得半透明标识元件 14，接受者利用接受者特定信息 32 例如如注册请求 800 指示的帐号或其他信息向在线银行或其他机构登记。然后该请求被传给网络服务器 802。然后该网络服务器 802 与银行服务器 804 进行通信，该银行服务器包括如客户管理系统和半透明标识元件请求程序 806，该程序可以是处理装置或任何其他适当机构上执行的适当应用软件。然后银行服务器 804 向半透明标识元件发行者 12 产生半透明标识元件发行请求 808，该发行者可以包含在适当服务器 810 中或与其分开。半透明标识元件发行请求 808 包括用户输入的接受者特定信息 12。作为响应，半透明标识元件发行者 12 在应答消息 808 中提供不透明标识符 38，并为用户产生和记录存储器 22 中的半透明元件序列号 44 和显示在半透明 ID 元件 14 上的相关不透明标识符。在该实施例中，银行服务器 804 将接受者帐号与半透明标识元件序列号 44 链接，然后在数据库 810 中存储该链接信息以备后用。然后银行服务器 804 产生半透明标识元件 14 通过，例如，格式化该不透明标识符 38 用于印刷和发送到打印机 814 或其他设备然后打印出或制造该半透明标识元件 14。因此，半透明标识元件序列号 44 被该半透明标识元件发行者 12 指定并与一个或多个不透明标识符 38 和存储器 22 数据库中的用户进行关联（例如，链接）。

半透明标识元件发行者 12 可包括信息随机发生器 900 和半透明标识元件格式程序 902。该信息随机发生器 900 可利用半透明标识元件序列号 44 如其他与接受者特定信息组合的信息产生一个或多个不透明标识符 38。可利用散列算法或所描述的其他适当编码技术产生一个或多个不透标识符 38 实现。半透明标识元件格式程序 902 可以是另一种在适当处理设备或格式化输出到打印机或其他制造设备中的信息的设备上的应用软件。

图 10 和 11 说明半透明标识元件发行出现后系统操作的另一个实施例。如块 1000 所示，该方法包括请求和获得接受者特定信息 32 如参考图 5 的先前描述。一旦打印出或制造出该半透明标识元件 14，那么被提供给接受者通过块 1002 中所示的手工或通过电子邮件或任何其他技术。如块 1004 所示，银行服务器确定接受者是否请求了认证，例如注册请求。如块 1006 所示，如果收到请求，发送网页要求输入包括密码和半透明标识元件序列号 44 作为多因子认证处理向第一级接受者信息 32。例如可通过图 5 所示的屏幕实现。如块 206 所示，银行服

务器确定输入的接受者特定信息 32 和密码和半透明标识元件序列号 44 是否正确，例如通过将信息传递给半透明标识元件确认者 24。如果第一认证级通过，该方法包括，如块 1010 所示，显示该可视过滤图案 44 当其与一个或多个半透明标识元件 14 上的不透明标识符真实组合时，仅显示一个或多个不透明标识符中的一个作为当前会话或交易输入合适的标识符。然后银行服务器通过网络服务器，通过提供图 6 所示的屏幕请求输入可显示的标识符 700，作为通过显示器显示的过滤图案选择的可显示的标识符。上述内容已被块 1010 示出。响应该请求，半透明标识元件确认者 24 接收一次性使用的被显示标识符 700 并将收到的标识符与该可视过滤发生器或确认者 24 确定的相应的预期 ID 进行比较。该内容在块 1012 中示出。给定该"过滤器"，用户输入数据和有关用户的存储的信息，该鉴别器能够验证用户是否输入正确数据（或者通过自身或将其传递到"服务器"）。如果向用户请求之前产生渴望的标识符，系统也会产生正确的过滤器并显示预先确定的标识符（显示给用户前的所有）。换句话说，如果用户被提供一个图案（过滤器）然后该系统该图案本应产生的标识符，验证用户输入的标识符，不需要提前选择渴望的标识符并且过滤器发生器因此不要求任何其他知识。利用不同于显示可视过滤图案设备的设备也可以接收表示可视显示标识符的数据（例如，数据本身，加密形成的数据或其他适当的数据）。例如，一个屏幕上显示标识符，手持装置或非手持装置可在可被用于将该可视显示的标识符输入和发送到其他装置或系统的某装置，以检查是否存在相匹配的标识符。

如块 1014 所示如果不存在匹配，会发送错误信息给接受者并要求重新输入显示的标识符。系统会改变以利用不同标识符进行重新尝试。并且，一定次数的尝试失败后系统会锁定用户。然而如块 1016 所示，如果匹配，第二因子认证被确定成功并且用户被授予其所要的权利。

图 12 和图 13 说明利用半透明标识元件 14（包括图 14 所示的类型）的交易卡的实施例。该交易卡可以是智能卡或非智能卡并具有与信用卡、借记卡或任何其他适当交易卡相关的常规信息，并且还包括半透明标识元件 14。该半透明标识元件 14 出现在该交易卡上的一部分。交易卡的一部分包括帐户信息如帐号、信用卡号、或任何其他适当标识符 1300 以及如果希望还包括其他的用户标识符如用户名 1402。在图 12 所示的实施例中，该交易卡包括开口 1306 例如可在塑料卡中剪出或以其它方式在塑料卡上提供该开口，以及具有黏合剂的半透

明标识元件14可被放置在该开口上或被整个模压在交易卡中或还可以例如但不局限于被贴在连接结构上，该机构被配置为接收并保存该TIDM在交易卡中或将该TIDM固定到交易卡上，使得该交易卡的尺寸与常规交易卡的尺寸相同或其他所描述的适当尺寸。如果使用，该连接结构可以是紧扣配合机构、滑入机构、基于附接的连接或任何所述的连接结构。

图13说明了不同的实施例，在该实施例中半透明标识元件14被贴在交易卡的侧面或任何其他面上。半透明标识元件14可沿折叠线1400折叠或如果希望可以是厚的非折叠的而且作为交易卡的一部分。任何其他用于适合将半透明标识元件粘贴在交易卡上的适当机构也会被注视。

图14和15说明了基本颠倒了半透明标识元件和接收单元的角色的替换实施例。在该实施例中，半透明标识符14包括可视过滤或加强图案40和显示屏，该显示屏显示至少一个可以是表示用户认证数据的数据，其按照需要对用户是唯一的或非唯一的数据的不透明标识符（参见图15）。如同以前的实施例一样，将半透明标识元件（可视过滤器）覆盖在显示不透明标识符的显示器上的组合，显示（无遮掩）和加强了屏幕上的至少一个不透明标识符。然后将显示的用户认证数据如密码或其他认证信息输入到适当交易设备中。而且，当半透明区被贴在或合并在常规交易卡上时，该交易卡包括如图12和13所示的实施例，第一部分包括交易卡号以及第二部分包括半透明标识号或具有包括可视过滤图案半透明区的其他标识信息。

图16说明应用图14中的TIDM14的系统1600的实施例。在该实施例中，TIDM确认者24包括与参考图1所述的用于产生一个或多个标识符的类似类型的不透明标识符发生器1602。不透明标识符发生器1602从用户接收接受者特定信息如用户名、TIDM序列号、或其他适当信息后产生不透明标识符，以确保为用户显示正确的不透明标识符。作为注册处理过程的一部分，用户准备提供相同的用户特定信息并且该不透明标识符发生器1602准备产生该不透明标识符并被将其存储在存储器22中。

半透明标识元件发行者12，在该实施例中产生具有半透明区的TIDM14，在该半透明区具有被配置为真实过滤该被显示的不透明用户标识符38并被配置为覆盖显示屏的至少一部分的可视过滤图案40。会希望具有用户特定信息的用户输入以初始化会话，其中同一个过滤图案被复制在半透明标识元件上用于多

个用户。希望知道的是，该 TIDM 的持有者是正确的用户而不是偷窃该 TIDM 的贼。该确认者，或其他资源，将产生的不透明标识符发送给接收设备。该接收设备显示至少一个作为用户认证数据的表面上不透明的标识符，以及根据具有直观图案的半透明标识元件接收表示显示的用户认证数据（例如显示的 ID 本身或其表达式）的数据。例如当该具有直观图案的半透明标识元件留在显示器上时，过滤器显示用户标识符。如果希望，半透明标识序列号能够分配给每个 TIDM，尽管同一个过滤图案会被复印在不止一个 TIDM 上。因而，几个用户会拥有具有相同过滤图案的半透明标识元件。

半透明标识元件发行者 12 被操作产生具有被配置为真实过滤该被显示的不透明用户标识符 38 并被配置为覆盖显示屏的至少一部分的可视过滤图案 40 的半透明区的半透明标识元件 14。响应接收的用户信息如用户特定信息，不透明标识符发生器 1602 产生用于在显示器显示的至少一个表面上不透明的标识符。半透明标识元件认证 18，在该实施例中接收表示显示的标识符数据，例如在过滤图案被覆盖在显示器上后通过用户通过用户接口输入信息，并如前所述半透明标识元件确认者将收到的显示标识符与相应的预期标识符进行比较（由于其由不透明标识符发生器产生），以确定接受者的适当认证是否是合适的。替换地，半透明标识元件确认者可以将收到的显示标识符发送给执行该比较的第三实体并将消息发回到确认者或接收单元。如所述任何其他适当的操作会话也可以被使用。然后，响应接收的与相应预期标识符相匹配的数据，半透明标识元件确认者或第三实体将授权信息发送给接收单元。

图 17 说明用于安全提供认证信息的方法，该方法包括根据例如收到的接受者秘密数据或公开数据或与接受者无关或不是来自接受者的数据，为接受者产生至少一个不透明标识符，如块 1700 所示。如块 1702 所示，该方法包括产生其上具有可视过滤图案 40 的半透明标识元件 14。产生 TIDM 后，该方法包括接收用户标识信息，例如 PIN: 或其他作为用户认证第一因子的数据。如块 1704 所示，该方法包括将一个或多个不透明标识符发送给接受者并显示至少一个作为用户认证数据第二因子的表面上不透明的标识符，并当在半透明标识元件上表面上与可视过滤图案 40 组合时，为用户显示一个不透明标识符。如块 1706 所示，该方法包括，例如用户将半透明标识元件覆盖在显示器上以通过过滤器可视地标识该不透明标识符。该方法还包括根据其上具有过滤图案的半透明标

识元件接收表示被显示的用户认证数据的数据。该方法还包括接收用户特定信息，例如先于该显示不透明标识符的步骤，以确定要显示在显示器上的该视觉上不透明的标识符显示在显示器上。例如，由于每个用户优先拥有一个不同的标识符，该系统需要确定显示哪一个不透明的标识符。这可由例如让用户通过接收单元中的用户接口输入用户特定信息，例如密码或其他所述的秘密或公开信息来确定。

叙述另一种方法，该方法包括接收作为用户认证的第一因子的用户标识信息并通过例如 TIDM 确认者，服务提供者或其他适当实体使用该用户标识信息，以标识存储器中的包含与该用户相关的特殊可视过滤图案的半透明标识元件。该方法包括产生包含预期标识符的不透明用户标识符图案，以便当不透明用户标识符图案与被标识的与用户相关的半透明标识元件上的可视过滤图案进行合并时，该预期标识符将被显示出来。该方法包括将不透明标识符图案传递给显示器（例如显示的 GUI）并要求输入被显示的标识符；并接收表示该被显示的标识符的数据。如上所述，TIDM 确认者例如，或任何适当数目的服务器或设备作为电路执行上述操作。

公开的设备、方法和系统的主要功能可通过一个或多个处理设备执行的应用程序接口（API）提供，该处理设备能够很容易被集成到当前的基础结构中。此外，实施例中的每个半透明标识元件是不同的并拥有不同的看起来的随机信息，由于该看起来的随机信息是典型的，但不是必要的，根据对接受者来说是唯一的信息产生，所述信息例如为密码，用户名，个人身份号码，或任何其他信息。在每个实施例中，半透明标识元件，和/或可视过滤器和/或不透明标识符能够提前被制造并接着与用户相关。此外，该不透明标识符和/或过滤图案能够被提前产生并接着被应用到半透明标识元件。该随后的半透明标识元件上的应用可由该过滤图案或不透明标识符的创建者来实现，或由提供该服务的实体实现，或由该服务提供者的第三实体承包者来实现。由于该半透明标识元件的制造可由非常简单的材料完成例如透明塑料，对于服务提供者来说将不透明标识符或直观图案发送给用户，然后该用户自己将过滤图案或不透明标识符应用到半透明标识元件是可能的。

同一半透明标识元件可重复使用几次，由于其上有多个不同的不透明标识符，其中每次认证要求通过该可视过滤图案公开的不透明标识符中的不同的一

个。因此，如果希望，在每个认证对话期间，该可视地显示在半透明标识元件上的标识符能够改变。这里所述的半透明标识元件可用于用户认证，激活应用程序或用于任何其他适当用途。不同的不透明标识符可以是字母，图象，或任何其他适当信息。

图 18 说明物品 1800（例如，元件）的一个实施例，例如半透明或非半透明薄膜、标签、卡、或其他任何适当材料和物品。会认识到是，项目 1800 所示的信息仅表明一个实施例并且会认识到的是可以使用任何适当信息。在实施例中，项目 1800 包括各自的位置信息 1802 和 1804（被表明是行列标记）以及数字形式的发送者认证信息 1806，该信息被坐标位置信息（例如行列信息）寻址或定位。 此外， 物品 1800 包括选择项目标识符 1808 例如物品 1800 发行者产生（例如分配）的序列号。

一般来说，如果希望可相对于如上所述的半透明标识元件产生该物品 1800，以产生例如发送者认证信息。然而，此外该位置信息 1802 和 1804 也需要加入到实施例中。此外，会认识到的是，半透明标识元件 14 也可以用作发送者认证项目并且该不透明标识符 38 也可以作为发送者认证信息。

此外，由于发送者认证信息如果希望可独立于或基于接受者特定信息，在该实施例中如果系统没有要求则不需要接受者特定信息。这会出现在接受者签字参加该服务的时候。此外，如这里所用的，位置信息包括与消息一起发送的信息或发送者发送的消息指向的信息，该信息指出接受者将验证哪一个物品 1800 上的发送者认证信息。例如，位置信息不必是行列信息，但仅可以是术语例如“左上角”，“左下角”“右边第三个”，或任何其他适当信息，以通知接受者物品上的发送者信息被作为该给出的会话，交易或其他通信的认证信息。替换地，该发送者认证信息可以是包含发送者认证信息的地址指针，例如，指向给出的会话，交易或其他通信的发送者认证信息的一般信息位置（URL）。此外，位置信息能够是包含实际位置信息的位置指针，其按顺序指出观看给出的会话，交易或其他通信的发送者认证信息的物品地址。在另一个实施例中，该位置信息是可视过滤图案。

图 19 说明包含例如磁条 1902 或任何其他可提供帐户信息或可通知发送者信息的适当信息的交易卡 1900。交易卡 1900 可以是例如银行卡，信用卡，借记卡或任何其他如上所述的适当卡并可包含交易卡标识信息如卡号等等，如上所

述。交易卡1900与常规卡不同是因为除了别的以外，其上包括物品1800（或元件），以任何适当的方法制造在其中或秘密放入其中。因而，在图13中说明了各种各样的交易卡1900。在一个实施例中，元件1800，例如一张背面带有标签的纸或任何其他适当元件，如果希望可被常规交易卡保护。如上所述也会认识到的是，以任何适当方法可保护或适当附加该元件或物品，该方法包括但不限于粘贴，或任何其他适当机构。元件1800也可以作为财务报表，帐单报表的撕开部分发送给接受者。优选地其尺寸可以安装在交易卡上。

图20说明用于提供电子消息认证方法的实施例，该方法可被任何适当单元执行。在该实施例中，它可被例如服务器或多个服务器或其他在一个或多个处理设备上执行的适当程序实现。如块2000所示，该方法包括，例如，当发送者如银行服务器或其他消息发送者希望将消息发送给接受者、确定渴望的位置信息时，例如也存在于特殊接受者的物品上的行和列，并且响应发送的渴望的发送者认证信息并与物品上的发送者认证信息进行匹配，并根据发送的位置信息进行定位。这可以例如通过访问连接接受者电子邮件地址的数据库例如，以响应为接受者展现例如发行的物品内容的数据库区域。如块2002所示，该方法包括将电子消息和期望的位置信息以及相应的期望的发送者认证信息发送给接受者，其中该期望的发送者认证信息根据该发送的期望的位置信息被定位在物品上。因而，例如，该发送者或发送单元可联合（例如，添加，前置，插入或不同的贴附方式）行和列信息和相应的发送者认证信息，该信息将物品上的那些位置作为电子消息的一部分呈现给接受者。然后，接受者可根据接收的行列数，物品上的通过（或代表）发送者发布的发送者认证信息，定位并确认该发送的期望的发送者认证信息与发送单元发送的该发送的位置信息指定的该地址中的相同信息相匹配。如果匹配，那么接受者信任消息的发送者。会认识到的是该发送的位置信息和发送者认证信息可以是数据本身，索引，函数，引用，或任何其他适当位置信息和发送者认证信息二者中的任何一个的表达式。

例如，地址坐标信息和相应的发送者认证信息包括用于在显示器上显示的电子传输的数据，例如可视过滤图案和发送者认证信息。在该实施例中，该物品会是透明物品以允许用户将该物品放置在显示屏幕区内。该发送的消息可包括可视过滤图案和期望的发送者认证信息，当用户将物品覆盖在显示屏上时，该信息将会真实地显示给用户。如果接受者真实地认识到或看到该发送者认证

信息，该信息通过屏幕上的可视过滤图案和与其匹配的发送的期望的发送者认证信息被显示，然后用户能相信该消息的发送者。因而，如前所述的关于接受者的半透明标识元件的可视过滤技术可部分用于认证该发送者。

再参考图 21，如 2100 所示的一个消息和相关发送者认证信息和位置信息的特殊实施例。在一个特殊的实施例中，再参考图 18，该消息被添加发送者认证信息和特别数字“98413”以及坐标信息“A2，E4，F1，H4，J2”。因而，该发送单元一起发送该电子消息和所示的该期望的发送者认证信息和期望的位置信息。然后用户使用物品 1800 并观察例如坐标地址 A2 并看到数字 9，观察坐标地址 E4 看到数字 8，观察坐标地址 F1 看到数字 4，观察坐标地址 H4 看到数字 1，并观察坐标地址 J2 看到数字 3。如果该用户得到的物品 1800 上的发送者认证信息与发送单元发送的相同，那么该接受者相信该发送者是真正的消息发送者。在该实施例中，发送者认证信息可视地呈现行列形式地址坐标信息标识的发送者认证信息。然而，会认识到的是不必使用行列格式并且不必使用如所示的该单元。例如，如果使用的对象与字母和数字相反，该对象可定位在该物品的左上，右上，中间或任何其他适当位置，并且该发送认证信息可以是能够以图象形式或其他适当对象被发送的对象，并且该坐标位置信息实际上可以是词组可读作“左上角”。任何其他适当坐标位置信息或发送者认证信息也可以被使用。

如上所述的物品 1800 可以是例如一张纸，一个塑料卡，透明塑料卡，能够贴在现有塑料卡或任何其他适当物品的标签。在该实施例中，每个电子邮件接受者被提供具有其自己随机（或看起来随机）产生内容的物品。当发送电子邮件时，发出者的消息传输代理或其他服务器组件通过利用 URL 或其他适当引用，坐标或用于定位一个或多个卡的单元格或位置的其他方向到 HTML 网页的直接或间接的链接，与外发的电子邮件相关联。另外添加，前置，插入或以其它方式贴附该电子邮件的是在那些位置的内容。接收后，用户利用他们自身的发送者认证物品确认该查找结果，例如阅读电子邮件列表中的坐标并在他们自己的发送者认证物品中查找他们。在该实施例中其中认证物品的半透明会话被使用，该认证物品可被放置在该电子邮件提供的可视过滤图案上并且接受者将显示的发送者认证信息与该电子邮件中提供的所渴望的发送者认证信息进行比较。如果字符或其他信息不匹配，那么认证失败。

图23详细说明了用于提供电子消息认证方法，其中该方法包括，如块2300所示，产生例如放置在物品上的随机发送者认证信息并且如果希望，位置信息也可以被放置在该物品上并用选择的接受者链接上述两者。随机包括伪随机信息或任何适当级别的随机信息。如上所述的关于该半透明标识元件这可以通过一个或多个服务器计算机或任何其他适当设备上的适当接口实现。如块2302所示，该信息作为认证信息和相关的位置信息存储在适当的数据库中。图块2304所示，该方法包括创建物品，例如物品1800包括地址坐标信息和相应的发送者认证信息，以及如果希望，创建物品标识符1808，例如发布给特殊接受者的序列号。这基本上由如上所述的方法完成。例如，复制卡片，适当地产生交易卡，或产生标签并能够粘贴到任何适当物品上。然后，该物品通过电子邮件或任何其他适当渠道被发送给接受者。

在一个替换的实施例中，使用软令牌代替硬令牌（例如，物品）的使用，其中卡的表示（可以不是实际图像）或物品表示在每个会话期间或只一次通过显示屏被电子发送给用户用于显示或该用户用于其他的电子访问，并且该用户可存储文件中的电子发送者认证物品并必要时访问该物品。因而该物品的电子表示能够通过软件被访问，以便为接受者提供发送者认证信息，该信息被定位在发送的位置信息标识的地址上。

如块2306所示，该方法还包括，例如如上述图20所述，例如通过发送确定至少一个期望的位置信息条目以及相关的发送者认证信息，以添加，前置，插入或其他贴附当前消息。位置信息和认证信息的选择可由任何适当方法实现，例如随机地或以期望的任何其他适当形式。如虚块2308所示，在一个替换的实施例中，位置信息和发送者认证信息以可视过滤图案的方式被有效地组合，该图案，如果希望，可掩盖所有行和列的首部并且当该物品被覆盖时刚好允许该发送者认证信息真实呈现。因而，该方法可包括将用于可视过滤图案发送给接受者，以允许该接受者真实确定该发送者是否被认证。该接受者可将物品上的发送者认证信息的至少一部分放置在显示在显示屏上的可视过滤图案上，以确定该发送的带有消息的发送者认证信息是否与该可视过滤图案再现的发送者认证信息相匹配。

在一个实施例中，该方法包括添加至少一个期望的位置信息条目和相关的认证信息到接受者的电子消息中。该发送者认证信息真实呈现该地址坐标信息

标识的认证信息。因而，消息本身可被添加，前置，插入或其他贴附到该信息中，或该消息可包括参考信息例如网站或任何其他适当链接，或该发送者认证信息和地址坐标信息的任何其他适当表示。

如块2310所示，该方法包括将电子信息以及表示地址坐标信息与对应的的发送者认证信息二者的数据发送给接受者。然后该接受者查看物品上的该信息并查看其是否匹配发送单元发送的信息。

也会认识到的是可实现根据该位置信息和对应的发送者认证信息确定至少一个地址坐标，例如，动态地完成而不是查找存储在数据库中的信息。例如，该发送者（例如，消息发送单元）可被简单编程并具有要发送的发送者认证信息的函数，而不是查找预先存储的信息。

并且如果希望，发送者认证信息可以是例如银行对帐单上的结余，帐单报表或帐户报表上的任何适当信息，上述信息已经被发送者发送给接受者并包含发送者认证信息。位置信息可以是特殊报表的日期以及该发送者认证信息可以是信用卡帐户上的当前结余。也可以使用任何其他的报表或任何其他的所知道的信息，或由接受者持有的发送单元提供。

图22说明用于提供电子消息认证的系统的实施例，其可执行参考图23所描述的步骤。例如，发送单元2200，例如任何服务器计算机，多个服务器，移动设备或任何其他包括发送者认证物品发行者2202的适当结构，或第三组织可发行所述的发送者认证物品。例如，该发送者认证物品发行者2202可产生随机的发送者认证信息和对应的地址坐标信息，并将该发行者链接到接受者并存储上述信息到数据库2204中。然后该物品1800可被邮寄到接受者或在软令牌的情况下，电子发送给接受者。在该说明中（图22），示出了半透明物品。因而，接受者20包括显示器30并且消息2100与可视过滤图案和发送的发送者认证信息一起显示在显示器上。然后该可视过滤图案被用于显示预期发送者认证信息并且然后接受者将该信息与消息2100中发送的信息进行匹配。在该实施例中，其中该发送者认证物品是半透明型的，发送单元发送的可视过滤图案具体化位置信息，因为接受者将发送者认证物品覆盖在显示屏上的结果会导致可视显示物品中特殊位置上的发送者认证信息。因而，该可视过滤图案包括该位置信息。此外，会认识到的是条目信息指的是任何适当标记。

发送单元2200可以是网络、节点、或任何其他适当设备中的适当服务器，

包括一个或多个电路其可以是一个或多个执行存储在存储器中的软件指令的处理设备的形式，或可利用离散数学实现，或硬件，软件或固件的任何适当组合来执行这里所述的操作。因而，发送单元2200包括被操作而执行如上所述步骤的电路。

在另一个实施例中，使用该发送者验证物品可与上述关于半透明标识元件的系统相组合，该半透明标识元件上包括位置信息和发送者认证信息。例如如果希望，该不透明标识符也可以用作该发送者认证信息或在一个替换的实施例中该半透明标识元件可具有包含该不透明标识符的部分以及包含该位置信息和发送者认证信息的另一部分。无论如何，使用单个物品或这里所述的半透明元件能够提供多级认证。例如，对于发送者认证，可使用图18－22所述的上述方法验证发送者是可信的。一旦例如接受者确信发送者的电子邮件是可信的，然后该接受者点击发送的电子邮件消息中的URL接着出现一个合适的HTML网页以输入帐户信息或其他机密信息。然而，输入这些秘密信息之前会利用该半透明标识元件和不透明标识符执行第二级认证，以便该发送单元能够认证当前的会话或交易。也会认识到的是也可以使用该认证方案的任何其他适当的操作顺序和组合。

此外权利要求使用的术语包括它的任何表示。例如该术语发送者认证信息包括数据本身，任何该数据的索引，该数据的任何参考和指针，或其任何其它表示。

除了其他的优点，不必对消息传输代理或接受者的电子邮件客户作出任何修改。而且如果希望，不必注册接受者计算机，允许执行来自任何计算机的认证。该系统也可适用于移动设备其中检查坐标能够很容易地显示在小型显示屏幕上。其他认证目的可包括网络认证，语音响应相互认证或任何认证方案。此外，该系统和方法提供一款便宜的机构例如认证卡，该卡能够被分配较复杂的技术其要求智能卡，令牌，或公共密钥基础结构。其他优点本领域普通技术人员会认识到。

图24说明在用户（例如，接收单元）与发送单元也可以作为目标源间提供相互认证的系统2400的一个实施例。例如如图18－23和其他地方所述的。在该实施例中，物品1800用作认证卡并分配给每个终端用户，包括例如仅由发送单元（例如，目标源）与终端用户知道的随机和／或唯一的标记。通过将该信

息的证明提供给接受者，发送单元能够证明它的身份并通过终端用户使接收单元返回信息并定位在该交易卡上，该终端用户作为正确的终端用户证明他／她的身份。

如上所述，系统 2400 可包括发送者认证元件发行者 2202，基于例如，接受者特定信息 32（即用户认证信息），产生物品 1800，所述信息可以是但不局限于密码和／或用户 ID。系统 2400 还包括发送单元 2402，其可以是一个服务器或如前所述的任何适当的设备，并还可包括，如上所述，一组服务器或执行这里所述操作的电路。系统 2400 还包括前面所述数据库相似的数据库 2404，在该实施例中，该数据库也存储用户认证信息 32 以允许第一级用户认证操作执行。此外，如上所述，数据库 2404 也存储位于物品上的发送者认证信息和物品标识符，以便发送单元 2402 可提供这里所述的第二级认证处理过程。

发送单元 2402 还包括，例如，包含可执行指令的存储器，当这些指令被一个或多个处理设备执行时，该存储器作为第一级用户确认者 2406 和第二级用户确认者进行操作。如上所述，然而会认识到的是这些操作由单独的服务器或其他定位或可访问的计算单元通过因特网，内联网或任何适当网络执行。也会认识到的是这里所述的组合可以是无线组合例如其中的接收单元 20 是无线手持设备或其他适当无线便携式设备。

再参考图 25，描述了用于在用户和发送单元间例如目标源提供相互认证的方法。上述的物品可包括交易卡，不具有任何交易信息的卡片，半透明卡，电子卡（例如，可视的被显示卡），上述卡片可以存储在接收单元或任何其他适当单元的存储器中，然后根据用户的请求或自动响应接收的询问而显示给用户，或者该物品可采取任何其他适当的形式。而且，在询问中发送的位置信息包括，例如，显示设备上显示的电子传输的数据。如上所述，这可采取行列信息或任何其他适当信息的形式，其中该信息可被电子传输并在显示器 30 被显示给用户或被清楚呈现。在该实施例中假定已经收到该发送者认证物品 1800 并该实施例中不是半透明物品，因此在该实施例中不必使用可视过滤器。然而，会认识到的是对于任何包括半透明卡或物品的适当物品来说这里所述的操作可被适当执行。该方法可被例如图 24 所示的系统或任何适当系统或机构执行。在该实施例中，发送单元 2402 不必将物品标识信息发送给接受者。然而，如果希望，可能会。在该实施例中，发送单元 2402 重复检查以发现发送的询问的应答是否与预

期的（例如，发送者希望的）发送者认证信息相匹配，该询问包括发送的询问中的位置信息标识的发送者认证信息。如果不匹配，在会话期间或通过多个会话多次重复发送该询问，直到接收单元接收的期望的发送者认证信息与预期的认证信息相匹配。

尽管在图 25 中没有示出，一开始可以执行第一级认证处理过程。例如，这可包括从接收单元 20 接收用户认证信息 2410，该信息可包括例如用户密码和用户 ID，以及该用户。这通过第一级用户确认者 2406 接收。然后第一级用户确认者 2406 通过使用从数据库 2403 获得的用户认证信息 32 并根据接收的用户认证信息 2410 认证该用户。如果两信息匹配，用户认证成功。然后一"是"指示 2412 被发送到第二级确认者 2408 以指示第二级认证处理过程可被执行。优选地，例如仍然在第一级认证处理期间，利用封锁机构，例如限制第一级认证处理期间尝试认证的数量以阻止强制攻击。由于第一部认证成功完成，该用户被提示认证如下所述的物品特定信息。

如块 2500 所示，该方法包括为已被分配物品 18 的用户确定期望的与具体化在物品上的发送者认证信息相关的发送者认证信息。这可通过第二级确认者 2408 根据用户认证信息 32 从数据库 2404 选择定位在物品 18 上的发送者认证信息来实现。如上所述，发送者认证元件发行者 2202 将物品上的标记存储到数据库 2404 中。通过使用该位置信息如行列标识符，或任何其他如上所述的适当位置信息，用户能够将发送者认证信息定位在物品 1800 上。

如块 2502 所示，该方法包括为用户发送询问，例如通过发送单元 2402，该询问至少包括标识能定位在物品 18 上的期望的发送者认证信息的位置信息。该询问可包括，例如，一个或多个例如通过显示器 30 显示给用户的坐标集合。优选地，该询问为每个用户所特有并必须根据第一级用户认证处理中的标识符或用户认证信息被检索。这表明向用户提出相同的询问直到认证成功完成。相同询问的重复可阻止攻击者根据用户卡上很少的内容信息安装强制攻击，例如，利用各种潜在攻击机制获得上述信息。然后一旦该用户通过第二级认证处理认证成功则执行并存储随机产生的询问。询问 2414 可以任何一种方法发送并可采取任何适当的形式如果希望包括，但不限制于，SSL 通信或非安全通信。如块 2504 所示，该方法包括接收发送的询问的应答。在该实施例中，从接收单元 20 接收被指定为 2416 的应答，并且该应答在用户的控制下由接收单元产生，例如，

利用发送的询问 2414 中的位置信息如行列 ID 以确定卡上的发送者确认信息。响应该询问该用户通过适当用户接口输入信息。因而，对于图 24-28 的实施例，该应答包括期望的（发送单元期望的）从物品上获得的发送者认证信息。该应答信息，尽管被认为是"发送者认证信息"，实际被发送单元或其他实体用来认证该用户，因为该应答仅包括该认证卡持有者可获得的信息。

如块 3506 所示，该方法包括确定，例如通过发送单元 2402，接收的该询问的应答是否包括期望的发送者认证信息，该信息被发送的询问中的位置信息所标识。如块 2508 所示，如果应答中的接收的发送者认证信息不是询问中的位置信息标识的期望的发送者认证信息，发送单元 2402，在该实施例中，然后将包含与先前发送的具有相同位置信息的同一询问重新发送给接收单元 20。如块 2510 所示，该方法包括重复以下步骤：根据发送的询问中的位置信息分析接收的应答并且如果该应答不包括预期的发送者认证信息，在同一会话期间发送单元发送相同的询问，直到接收的应答包括期望的物品上的发送者认证信息为止或例如直到发送单元作出了适当次尝试为止。重复询问直到该应答包括该预期的期望的发送者认证信息。

图 26 说明用于在用户和发送者之间提供相互认证的另一个方法，并且该方法可由例如图 24 所示的系统或任何其他适当系统或设备实现。在该实施例中，不执行重复发送相同的询问直到收到正确的应答为止。在该实施例中，物品标识信息，如物品上的序列号或任何其他适当的物品信息加上询问中的位置信息也被发送给该用户。如块 2600 所示，该方法包括确定，例如通过发送单元 2402，与物品上的发送者认证信息相关的期望的发送者认证信息，也为同一用户确定相关的物品标识信息，如物品上的序列号或共享秘密或任何其他适当的标识信息。如块 2602 所示，该方法包括将包括确定的位置信息和物品标识信息的用于认证该发送单元的用户询问发送给用户。

如块 2604 所示，该方法包括根据询问的应答认证该用户，其中包括根据该位置信息从物品中获得的发送者认证信息。在该实施例中，例如用户不输入或发送应答给该询问，除非该用户核实发送的询问中的物品标识信息与该物品本身上的物品标识信息相匹配。因而，用户可以根据该物品标识信息认证该发送单元。因而，在该实施例中，该询问包括附加位置信息的物品标识信息。该应答包括位置信息定义的定位在物品上的发送者认证信息。如果询问中的物品标

识符与用户持有的物品上的物品标识符相匹配，那么该用户相信该发送单元。如块 2606 所示，该方法包括根据该询问的应答认证该用户。在该实施例中，优选地根据用户秘密和／或用户 ID 再一次执行如前所述的第一级认证。如果该级别的认证成功，则可执行图 26 中的方法。如所述，物品标识信息可包括用户和发送者知道的共享秘密或可以是物品序列号，或任何其他适当信息。

图 27 说明用于在用户和发送者间提供相互认证的另一种方法，该方法是图 25 和 26 中操作的有效组合。如块 2700 所示，该方法包括执行第一认证处理如通过提示第一级用户认证信息。可包括，例如，发送单元发送请求或为用户提供提示以输入密码和用户 ID。作为响应，该发送单元接收第一级用户认证信息如密码或并且验证存储的用户认证信息 32（例如，接收的散列密码）以确保接收的第一级用户认证信息是正确的。如块 2702 所示，如果第一级认证信息成功，该方法包括为用户确定与具体化在物品上的发送者认证信息一致的期望的发送者认证信息，并确定例如能够定位在物品上的物品标识信息。因而，在该实施例中，位置信息和物品标识信息都被发送到询问中。然后执行先前所述的图 25 和 26 所示的步骤，例如，重复发送询问，其中该询问是相同的询问，直到应答中接收到该正确的发送者认证信息为止。因而，用户确认所显示的询问中的物品标识符与卡上的标识符相匹配。这认证了发送单元和目标组织是唯一的并且最终用户拥有了该标识符的信息。通过观察卡上发送的询问中的位置信息内容该用户输入该询问的适当应答。发送单元能够验证该应答并且验证作为唯一的持有该卡片的最终用户的用户能够正确响应该询问。会认识到的是因特网的上下文已经描述了该操作但是该操作被同等应用于其他通信通道中，例如交互语音响应或任何其他适当通信系统。例如，其中使用交互语音响应的地方，利用无线或有线电话网络形式通过语音提供用户提示，例如，自动化系统。相反，利用网络形式的输入通过按键明暗提供用户应答。也可以使用任何其他适当的通信系统。

其他的优点中，所述的设备系统和方法提供最终用户和发送单元或目标组织的安全认证，并且使用起来相对简单且制造起来相对便宜，并可被配置相对复杂技术的认证卡例如智能卡，硬件令牌或公共密钥机制。此外，利用网络客户通过多个通信通道如移动设备，非移动设备，声音触发设备，或任何其他适当设备可使该系统的实现变得简单。

图 28 用图解法表示了上述操作。例如，如通信 2800 所示，将具有常规用户名和密码的登陆屏幕呈现给用户并输入其用户名和密码，并且用户将其作为登陆响应 2800 发送给发送单元 2402，然后执行认证处理，如本领域熟知的那样例如通过将接收到的密码和用户 ID 与存储在密码数据库 2802 中的那些信息进行比较。如果验证成功，则发送单元 2402 发送询问 2414 给接收单元，例如，该接收单元具有用户卡标识符，以及询问包括位置信息以便该用户能够在卡上定位该特殊标记。例如，为用户在接收单元上显示该询问。用户利用用户持有的认证卡上的卡标识符确认接收的卡标识符并通过将应答 2416 发回到发送单元 2402 回答该询问。然后，发送单元验证该应答以证实该用户完成了相互认证。然而，第二级认证没有成功，发送单元会重复发送相同的询问即相同的位置信息到该接收单元直到接收到正确的应答。

上述本发明的详细描述以及这里所述的实施例已被给用于说明和详细叙述，以及本领域技术人员会认识到其他变更。例如，会认识到的是这里所述的各种操作可分布在网络或非网络配置中。例如，确认者，发送单元或 TIDM 发行者的不同操作或其他操作可被一个或多个第三实体网络服务器或其他实体或装置执行。用于发送者认证设备和方法的其他变更也会被认识到。

因此，任何和全部覆盖本发明的修改，变更或等价物将落在上述和这里所要求的基本原理的精神和范围内。

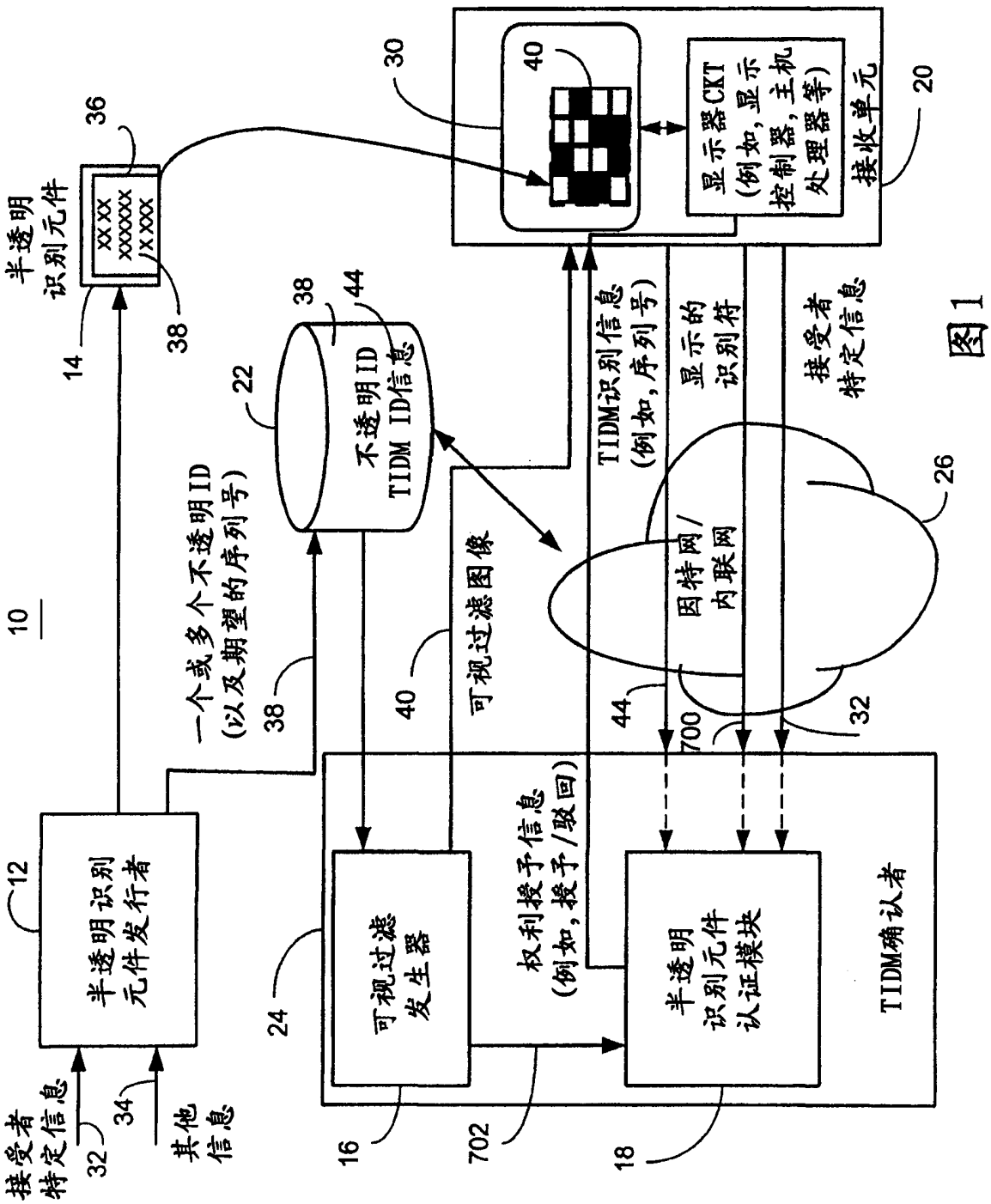

半透明识别元件
XX XX
XXXXXX
XXXX
36
38
14
10
半透明识别元件发行者
12
接受者特定信息
32
34
其他信息
一个或多个不透明ID
(以及期望的序列号)
38
22
不透明ID
TIDM ID信息
38
44
可视过滤图像
40
24
可视过滤发生器
16
权利授予信息
(例如,授予/驳回)
702
半透明识别元件认证模块
18
TIDM确认者
TIDM识别信息
(例如,序列号)
显示的识别符
接受者特定信息
因特网/内联网
26
44
700
32
30
40
显示器CKT
(例如,显示控制器,主机处理器等)
接收单元
20

图1

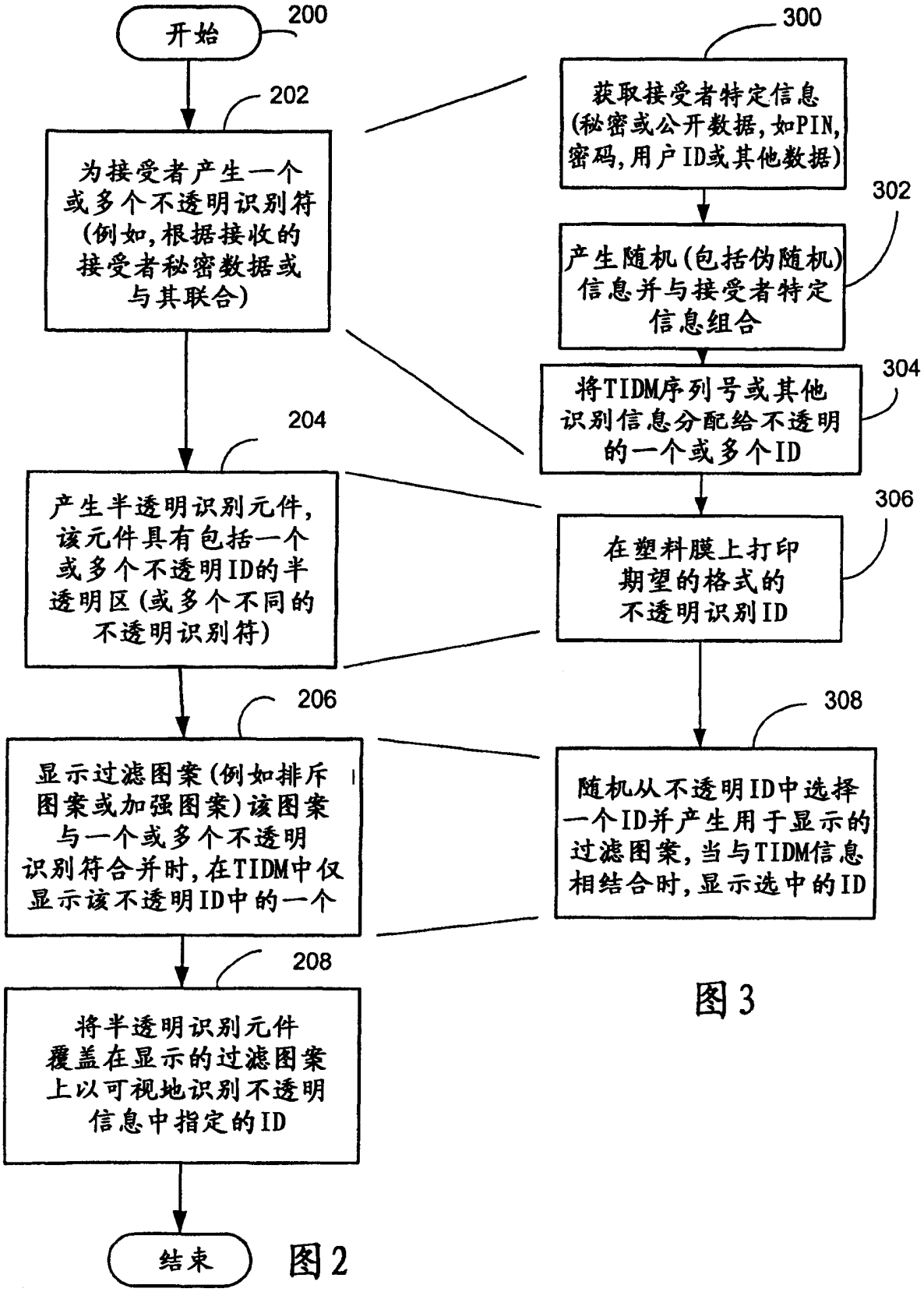

开始
200
202
为接受者产生一个或多个不透明识别符(例如,根据接收的接受者秘密数据或与其联合)
204
产生半透明识别元件,该元件具有包括一个或多个不透明ID的半透明区(或多个不同的不透明识别符)
206
显示过滤图案(例如排斥图案或加强图案)该图案与一个或多个不透明识别符合并时,在TIDM中仅显示该不透明ID中的一个
208
将半透明识别元件覆盖在显示的过滤图案上以可视地识别不透明信息中指定的ID
结束
300
获取接受者特定信息(秘密或公开数据,如PIN,密码,用户ID或其他数据)
302
产生随机(包括伪随机)信息并与接受者特定信息组合
304
将TIDM序列号或其他识别信息分配给不透明的一个或多个ID
306
在塑料膜上打印期望的格式的不透明识别ID
308
随机从不透明ID中选择一个ID并产生用于显示的过滤图案,当与TIDM信息相结合时,显示选中的ID

图2

图3

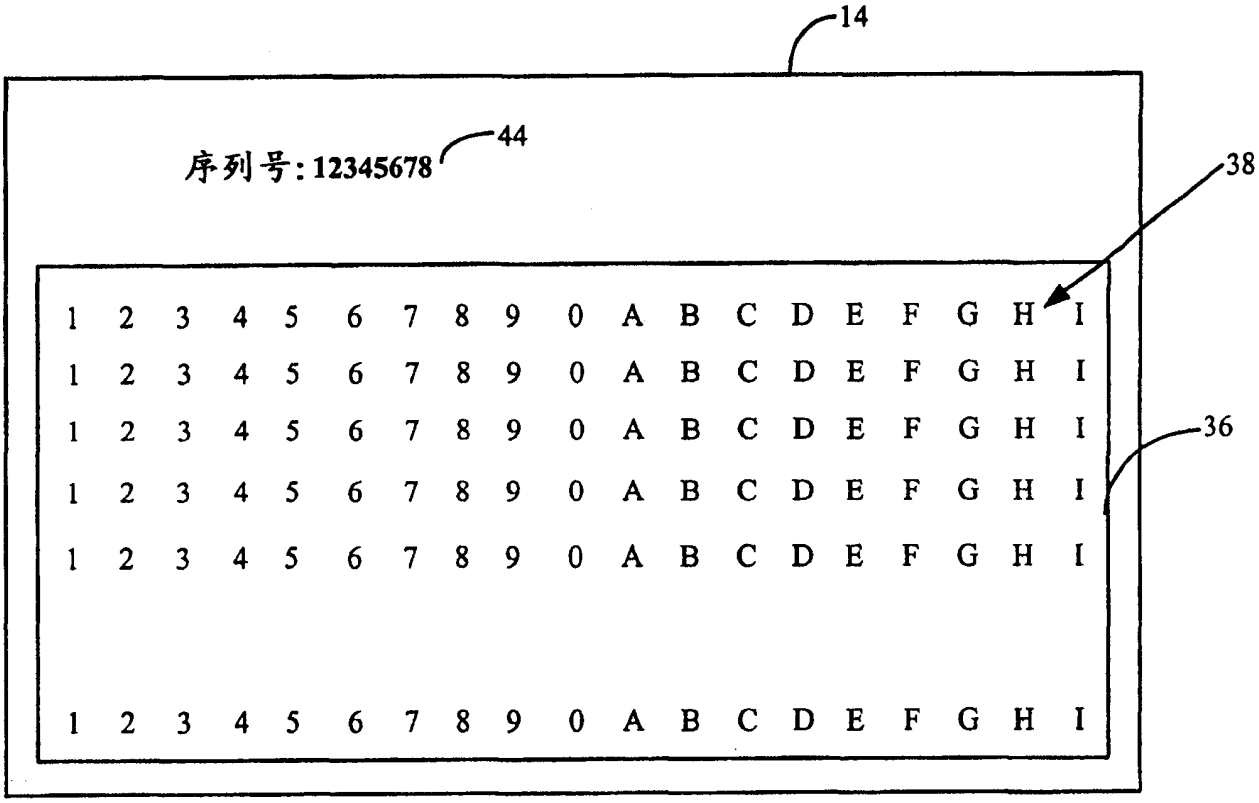

14
序列号:12345678
44
38
36
1 2 3 4 5 6 7 8 9 0 A B C D E F G H I
1 2 3 4 5 6 7 8 9 0 A B C D E F G H I
1 2 3 4 5 6 7 8 9 0 A B C D E F G H I
1 2 3 4 5 6 7 8 9 0 A B C D E F G H I
1 2 3 4 5 6 7 8 9 0 A B C D E F G H I
1 2 3 4 5 6 7 8 9 0 A B C D E F G H I

图4

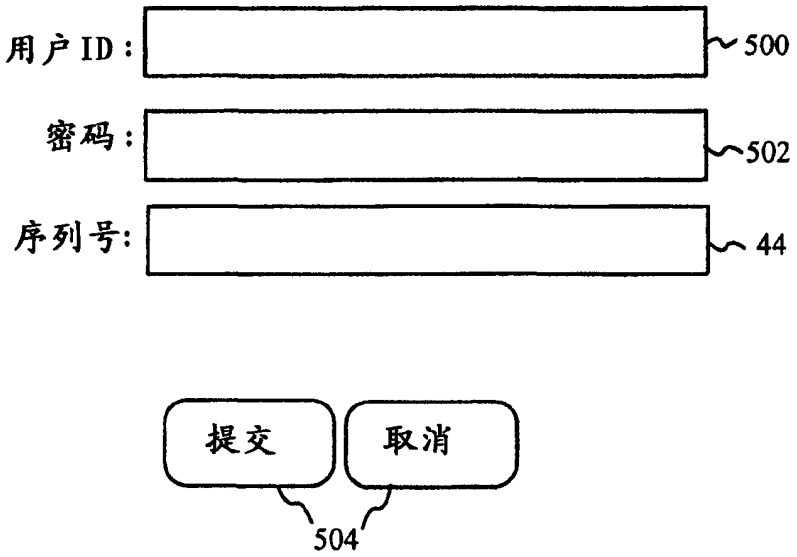


图5

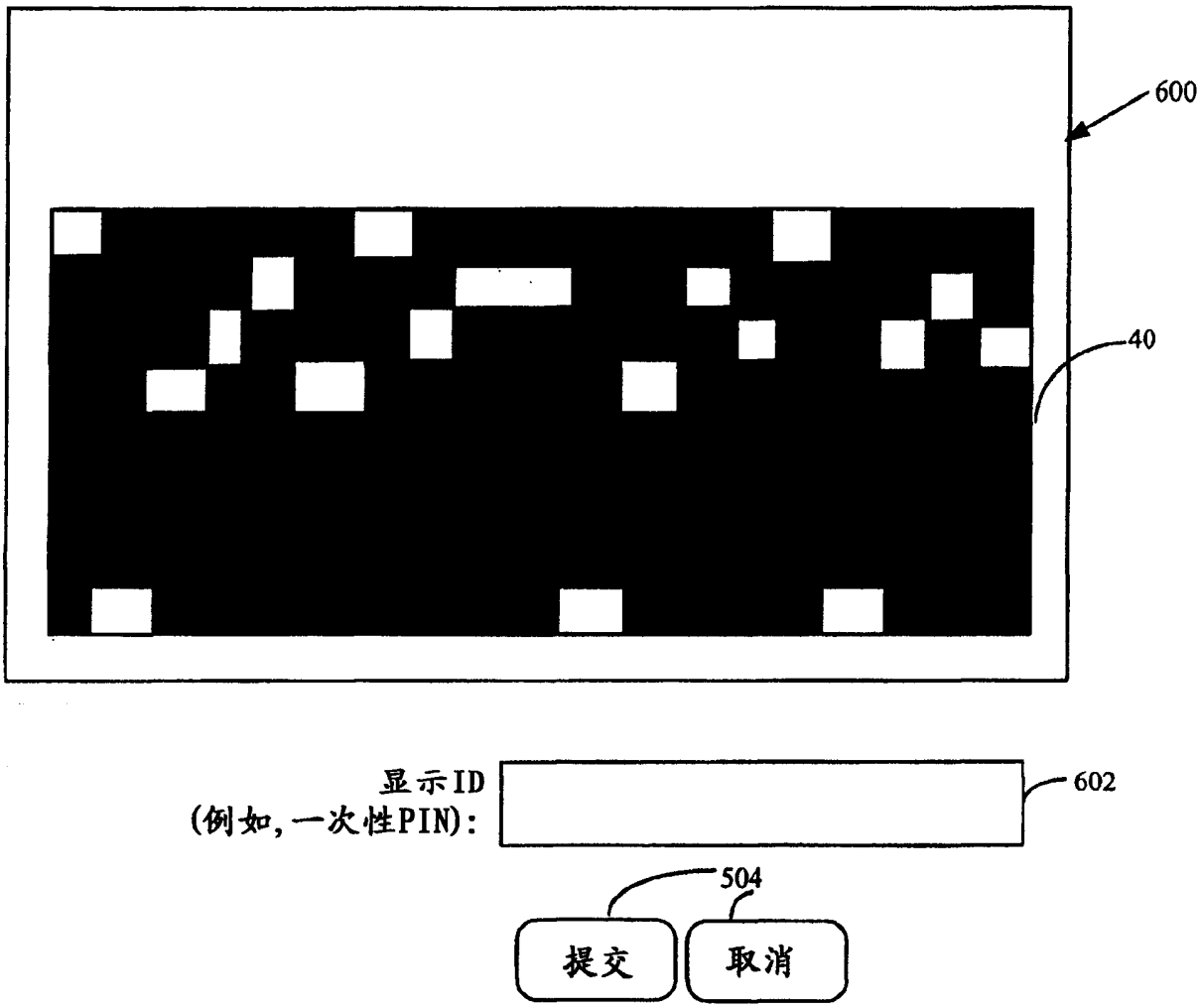


图6

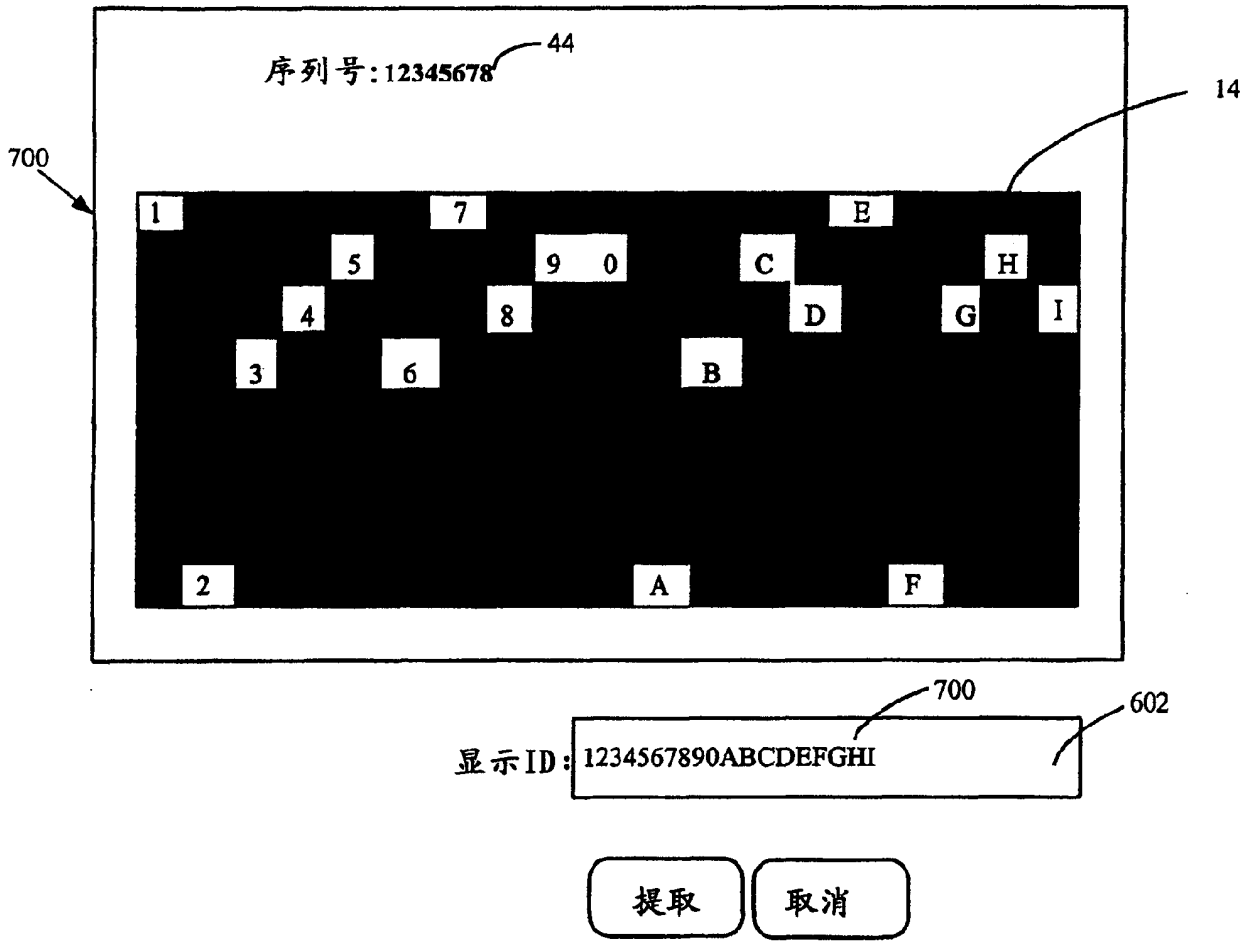

序列号:12345678
44
14
700
1
7
E
5
9
0
C
H
4
8
D
G
I
3
6
B
2
A
F
700
602
显示ID:
1234567890ABCDEFGHI
提取
取消

图7

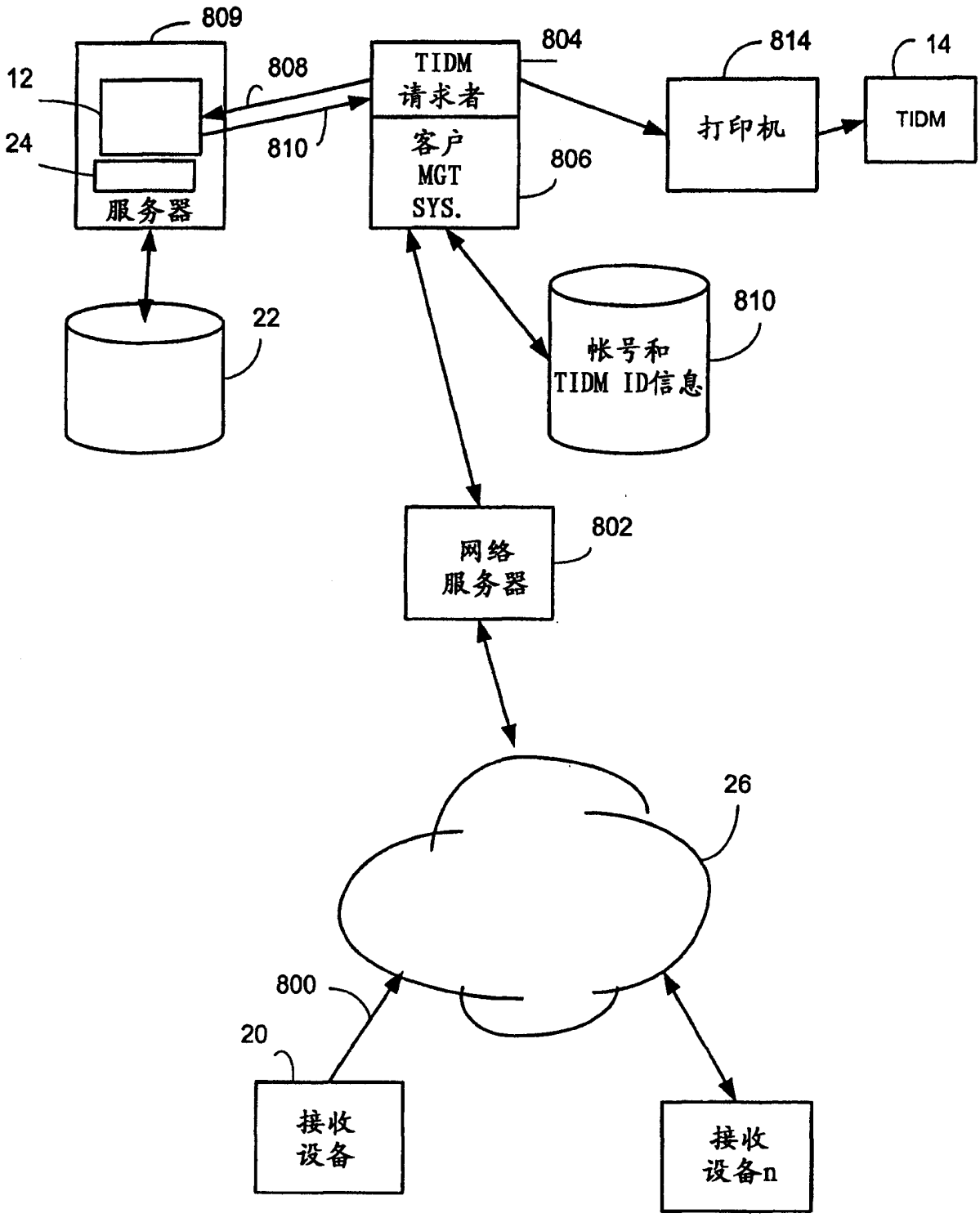

809
12
24
服务器
808
810
TIDM
请求者
804
客户
MGT
SYS.
806
814
打印机
14
TIDM
22
帐号和
TIDM ID信息
810
网络
服务器
802
26
800
20
接收
设备
接收
设备n

图8

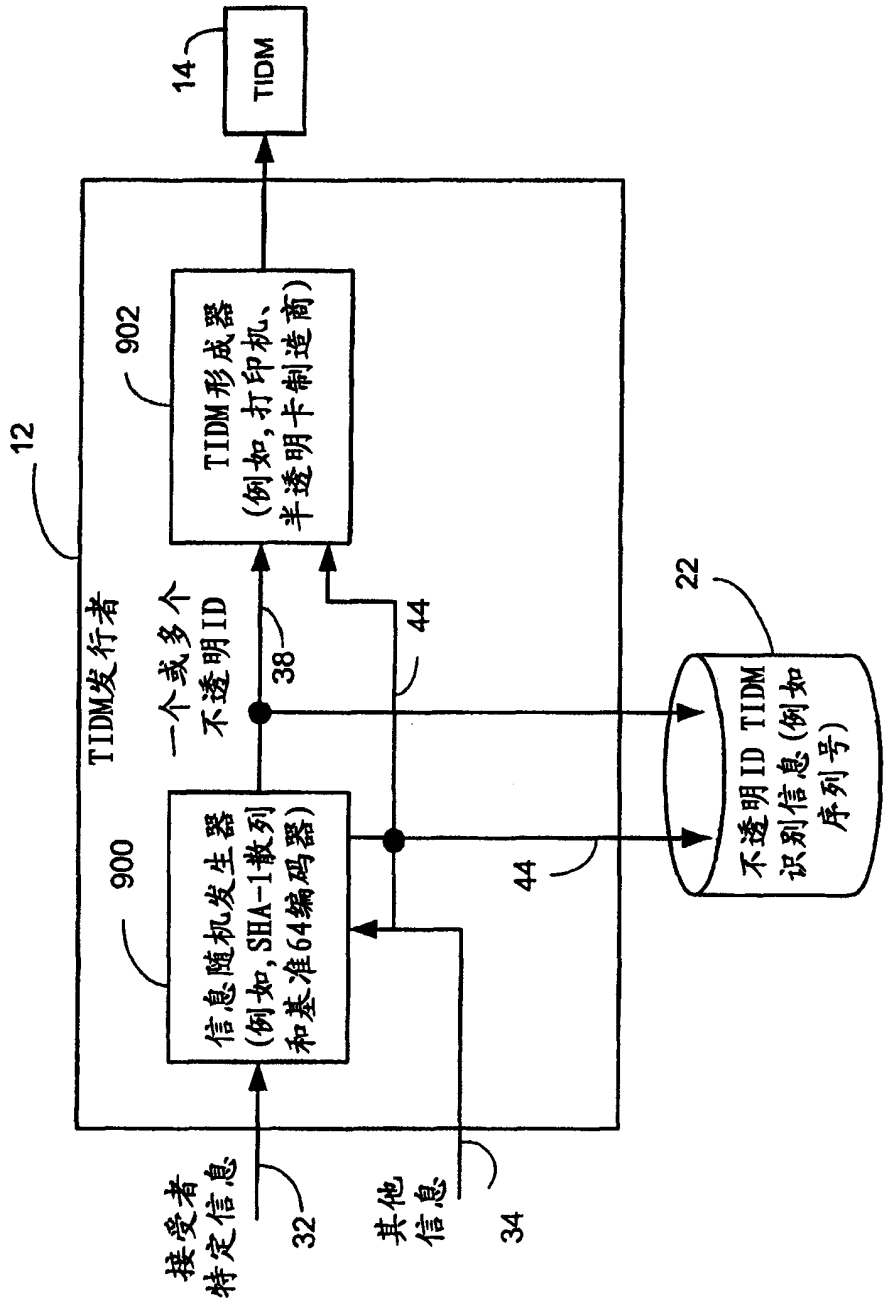

14
TIDM
12
TIDM发行者
902
TIDM形成器
(例如,打印机、
半透明卡制造商)
一个或多个
不透明ID
38
44
22
900
信息随机发生器
(例如,SHA-1散列
和基准64编码器)
44
不透明ID TIDM
识别信息(例如
序列号)
接受者
特定信息
32
其他
信息
34

图 9

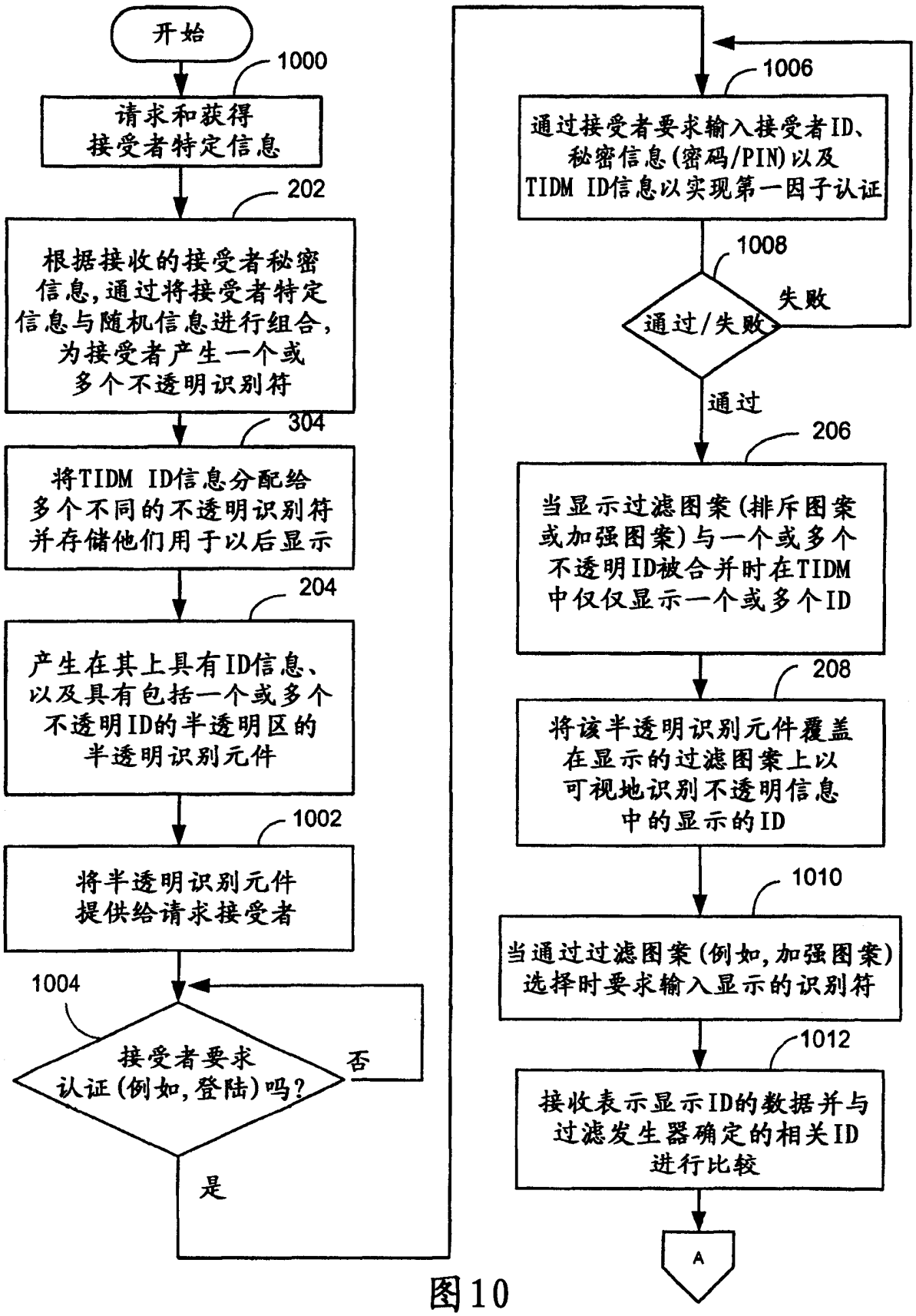

开始
1000
请求和获得
接受者特定信息
202
根据接收的接受者秘密
信息,通过将接受者特定
信息与随机信息进行组合,
为接受者产生一个或
多个不透明识别符
304
将TIDM ID信息分配给
多个不同的不透明识别符
并存储他们用于以后显示
204
产生在其上具有ID信息、
以及具有包括一个或多个
不透明ID的半透明区的
半透明识别元件
1002
将半透明识别元件
提供给请求接受者
1004
接受者要求
认证(例如,登陆)吗?
否
是
1006
通过接受者要求输入接受者ID、
秘密信息(密码/PIN)以及
TIDM ID信息以实现第一因子认证
1008
通过/失败
失败
通过
206
当显示过滤图案(排斥图案
或加强图案)与一个或多个
不透明ID被合并时在TIDM
中仅仅显示一个或多个ID
208
将该半透明识别元件覆盖
在显示的过滤图案上以
可视地识别不透明信息
中的显示的ID
1010
当通过过滤图案(例如,加强图案)
选择时要求输入显示的识别符
1012
接收表示显示ID的数据并与
过滤发生器确定的相关ID
进行比较
A

图10

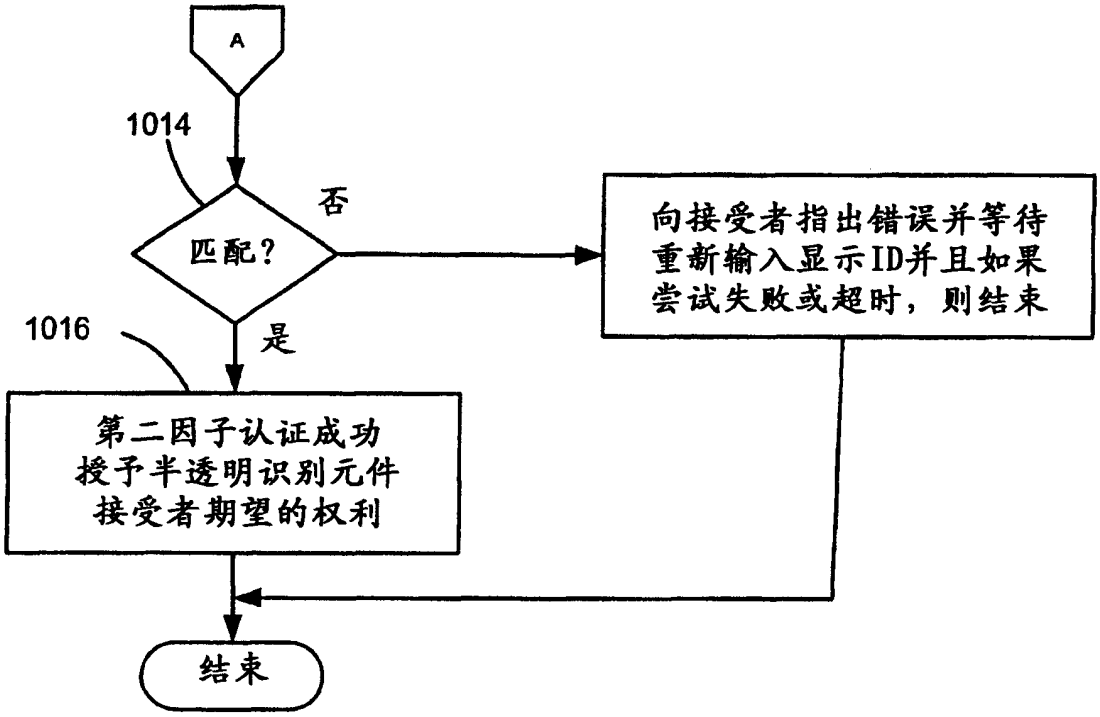

A
1014
匹配?
否
是
向接受者指出错误并等待
重新输入显示ID并且如果
尝试失败或超时，则结束
1016
第二因子认证成功
授予半透明识别元件
接受者期望的权利
结束

图11

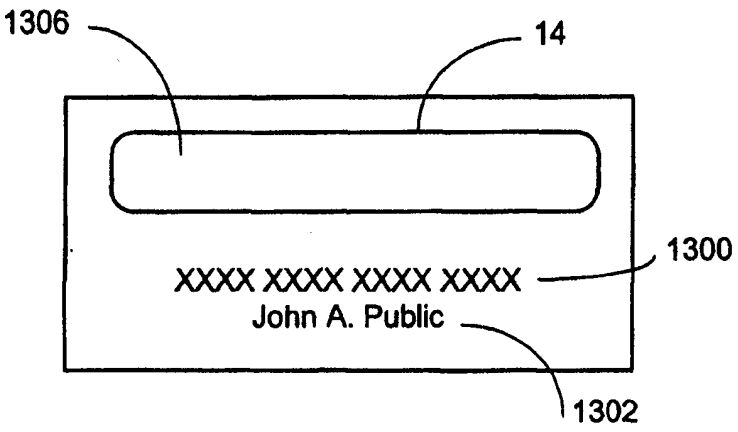

1306
14
1300
XXXX XXXX XXXX XXXX
John A. Public
1302

图12

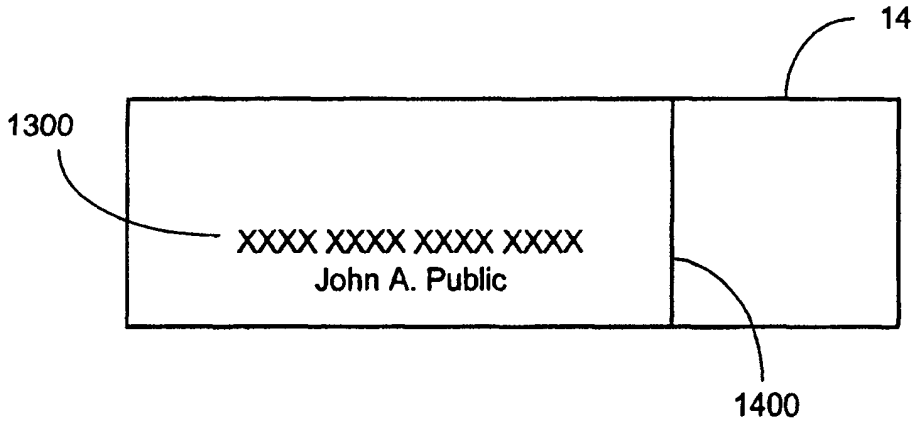

14
1300
XXXX XXXX XXXX XXXX
John A. Public
1400

图13

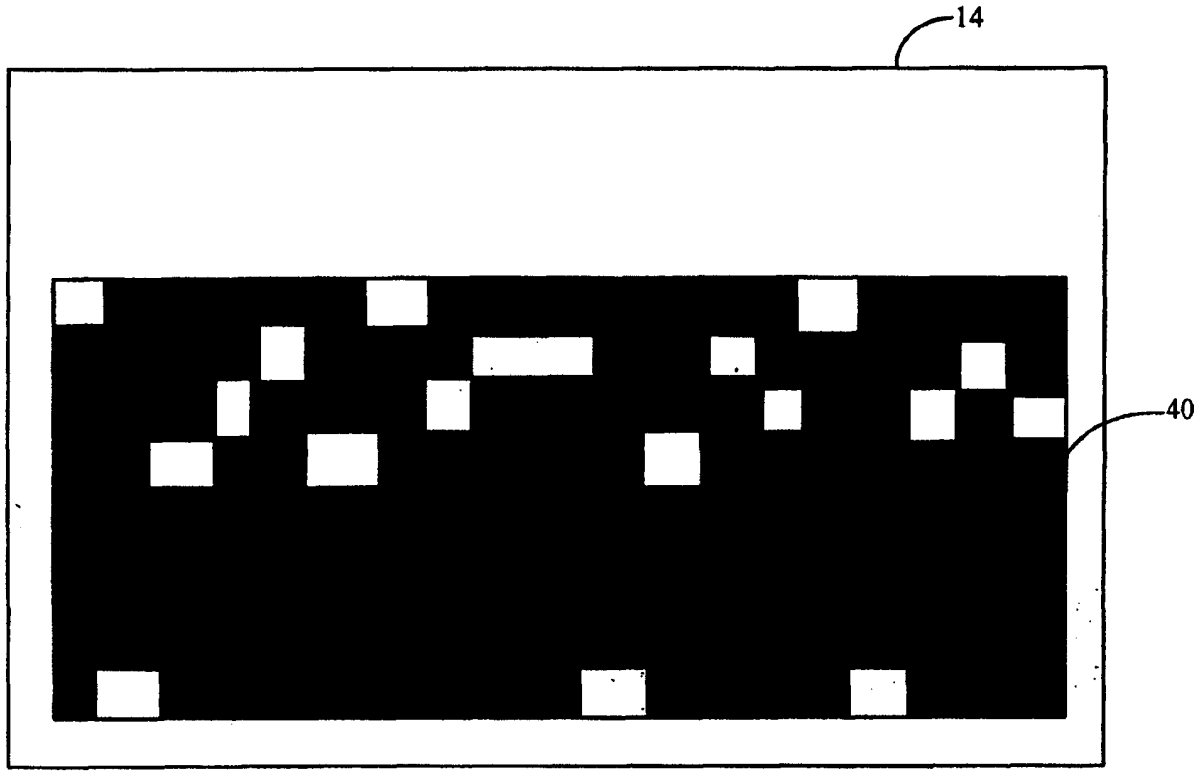


图14

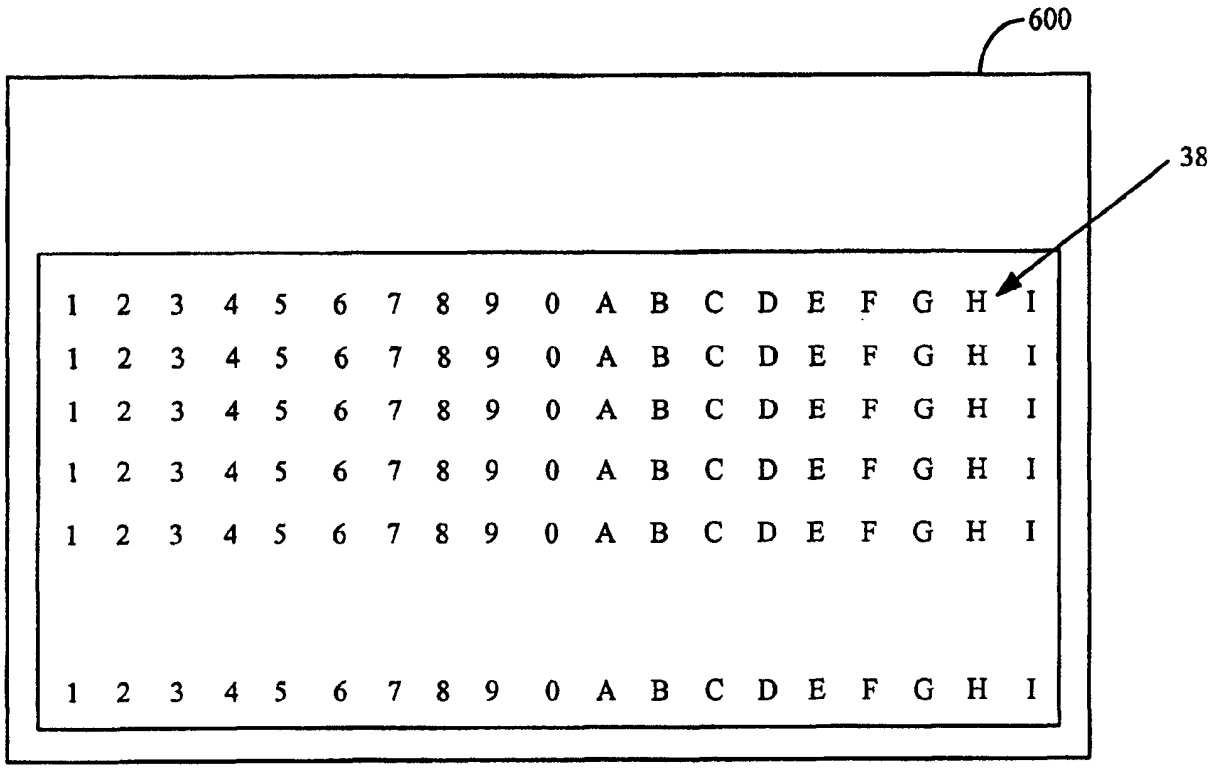

600
38
1 2 3 4 5 6 7 8 9 0 A B C D E F G H I
1 2 3 4 5 6 7 8 9 0 A B C D E F G H I
1 2 3 4 5 6 7 8 9 0 A B C D E F G H I
1 2 3 4 5 6 7 8 9 0 A B C D E F G H I
1 2 3 4 5 6 7 8 9 0 A B C D E F G H I
1 2 3 4 5 6 7 8 9 0 A B C D E F G H I

图15

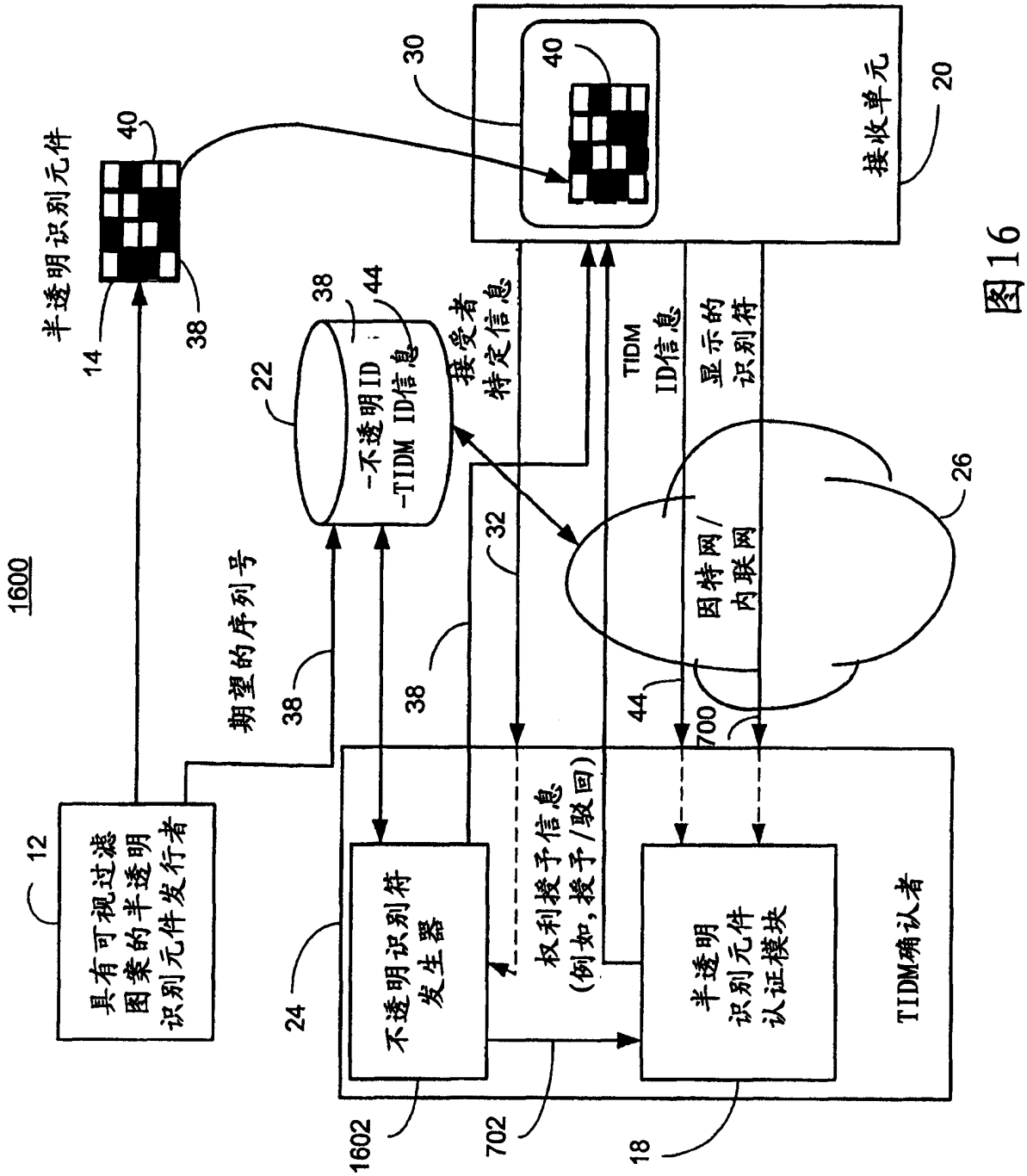

1600
具有可视过滤图案的半透明识别元件发行者
12
半透明识别元件
14
40
38
期望的序列号
38
22
-不透明ID
-TIDM ID信息
38
44
32
38
接受者特定信息
30
40
接收单元
20
TIDM ID信息
显示的识别符
因特网/内联网
26
44
700
24
不透明识别符发生器
权利授予信息(例如,授予/驳回)
半透明识别元件认证模块
TIDM确认者
1602
702
18

图16

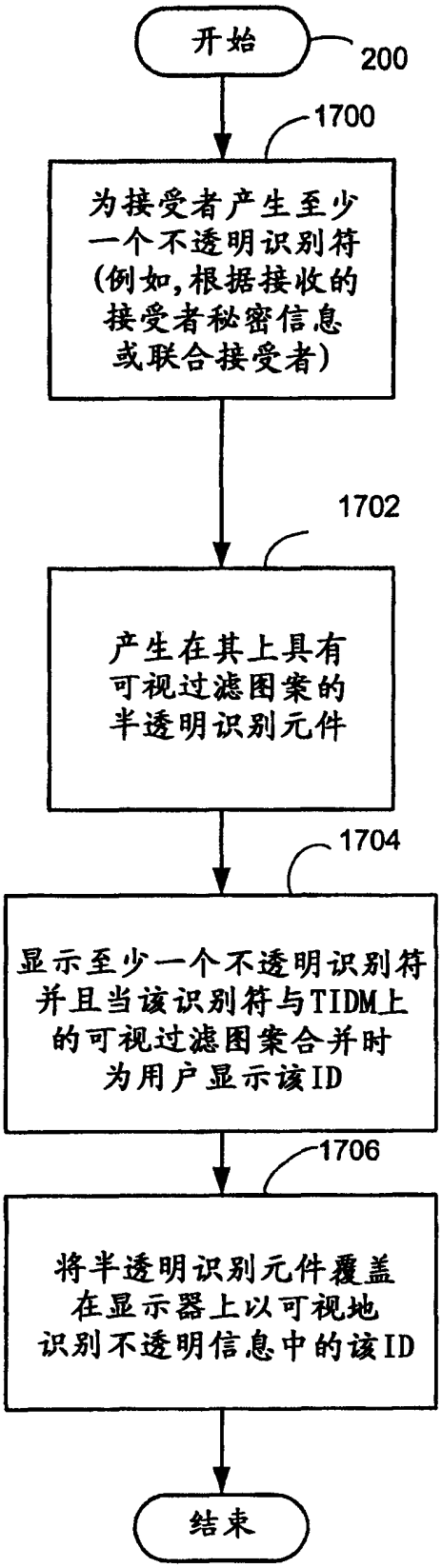

开始
200
1700
为接受者产生至少一个不透明识别符(例如,根据接收的接受者秘密信息或联合接受者)
1702
产生在其上具有可视过滤图案的半透明识别元件
1704
显示至少一个不透明识别符并且当该识别符与TIDM上的可视过滤图案合并时为用户显示该ID
1706
将半透明识别元件覆盖在显示器上以可视地识别不透明信息中的该ID
结束

图17

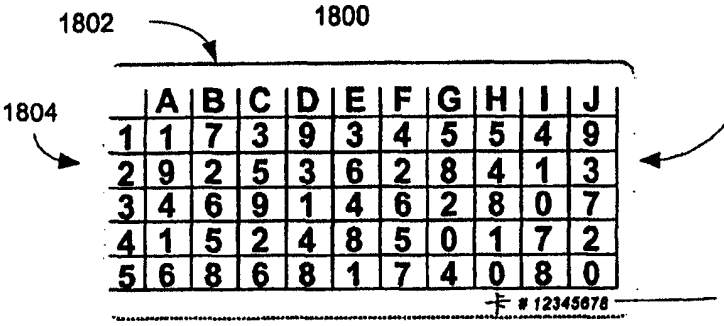

1802
1800
1806
1804
A B C D E F G H I J
1 1 7 3 9 3 4 5 5 4 9
2 9 2 5 3 6 2 8 4 1 3
3 4 6 9 1 4 6 2 8 0 7
4 1 5 2 4 8 5 0 1 7 2
5 6 8 6 8 1 7 4 0 8 0
卡 # 12345678
1808

图18

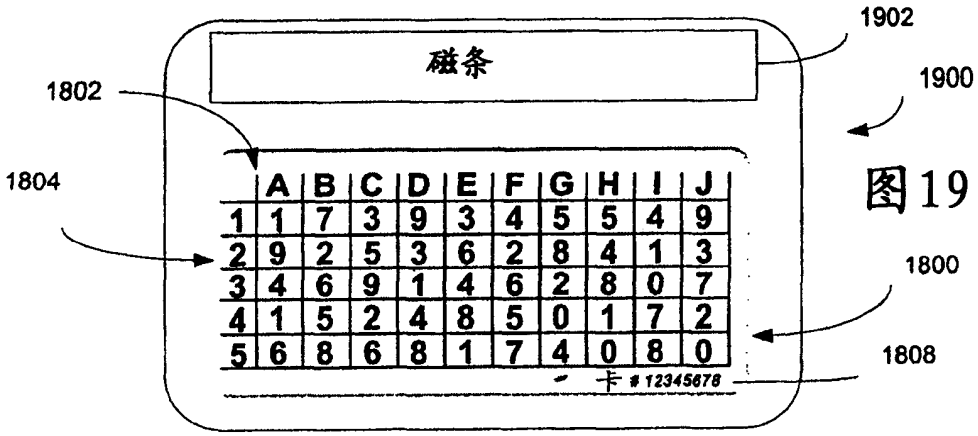

1902
磁条
1900
1802
1804
A B C D E F G H I J
1 1 7 3 9 3 4 5 5 4 9
2 9 2 5 3 6 2 8 4 1 3
3 4 6 9 1 4 6 2 8 0 7
4 1 5 2 4 8 5 0 1 7 2
5 6 8 6 8 1 7 4 0 8 0
卡 # 12345678
1800
1808

图19

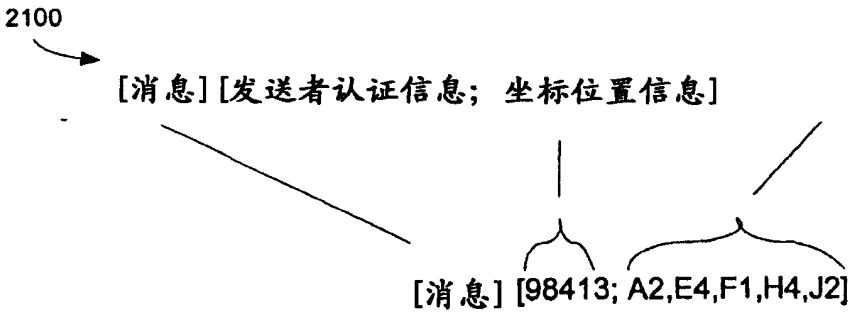

2100
[消息][发送者认证信息；坐标位置信息]
[消息] [98413; A2,E4,F1,H4,J2]

图21

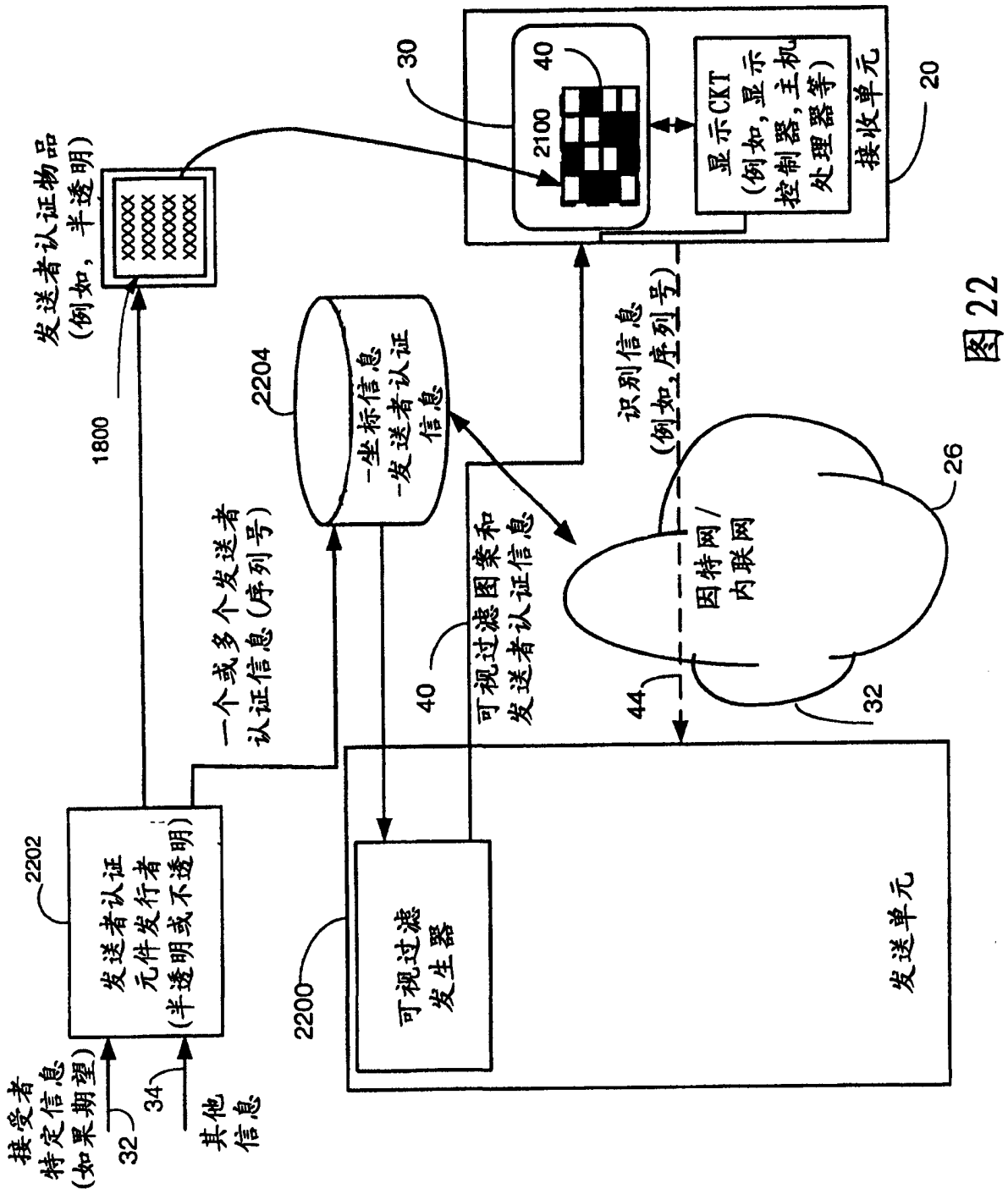

发送者认证物品
(例如，半透明)
1800
XXXXXX
XXXXXX
XXXXXX
XXXXXX
30
2100
40
显示CKT
(例如，显示
控制器，主机
处理器等)
接收单元
20
2204
-坐标信息
-发送者认证
信息
识别信息
(例如，序列号)
一个或多个发送者
认证信息(序列号)
可视过滤图案和
发送者认证信息
40
因特网/
内联网
26
44
32
2202
发送者认证
元件发行者
(半透明或不透明)
2200
可视过滤
发生器
发送单元
接受者
特定信息
(如果期望)
32
34
其他
信息

图 22

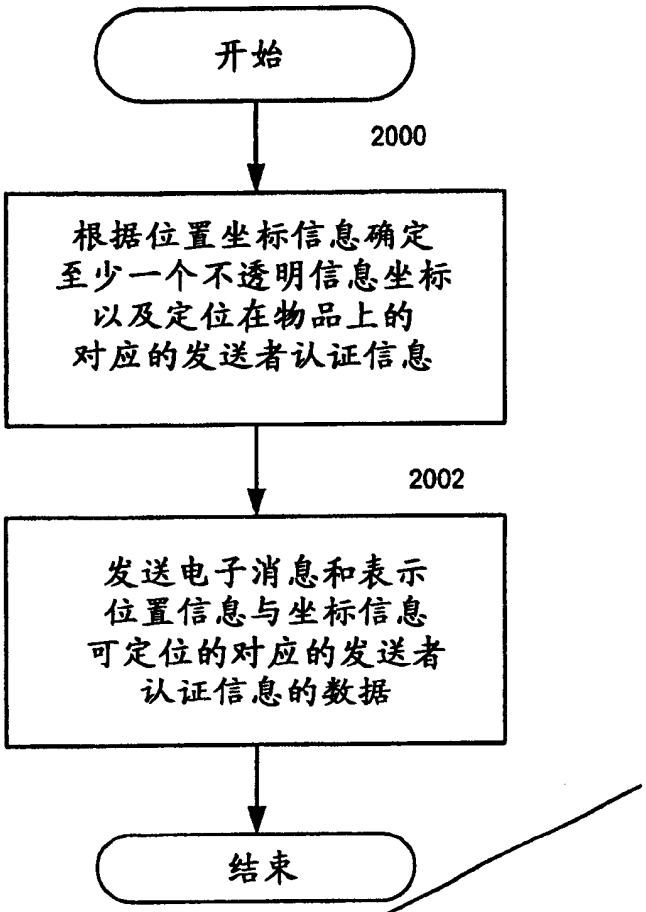
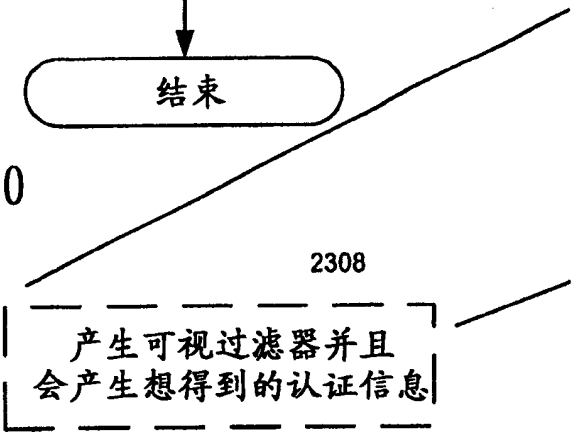

开始
2000
根据位置坐标信息确定至少一个不透明信息坐标以及定位在物品上的对应的发送者认证信息
2002
发送电子消息和表示位置信息与坐标信息可定位的对应的发送者认证信息的数据
结束

图20


2308
产生可视过滤器并且会产生想得到的认证信息

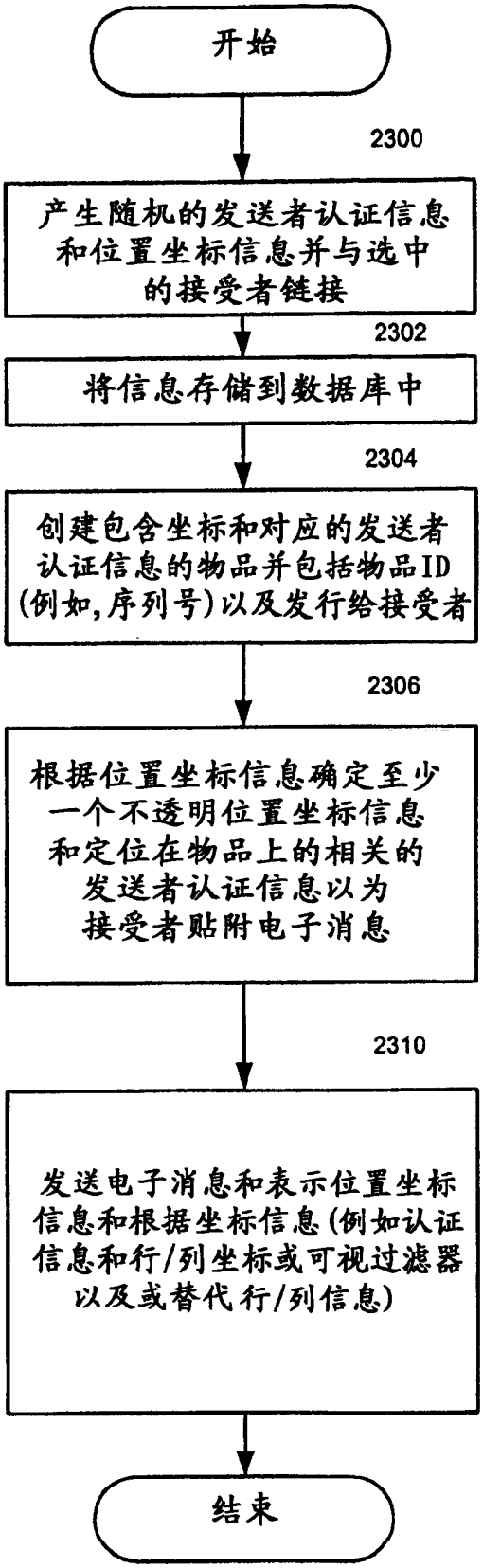

开始
2300
产生随机的发送者认证信息和位置坐标信息并与选中的接受者链接
2302
将信息存储到数据库中
2304
创建包含坐标和对应的发送者认证信息的物品并包括物品ID(例如,序列号)以及发行给接受者
2306
根据位置坐标信息确定至少一个不透明位置坐标信息和定位在物品上的相关的发送者认证信息以为接受者贴附电子消息
2310
发送电子消息和表示位置坐标信息和根据坐标信息(例如认证信息和行/列坐标或可视过滤器以及或替代行/列信息)
结束

图23

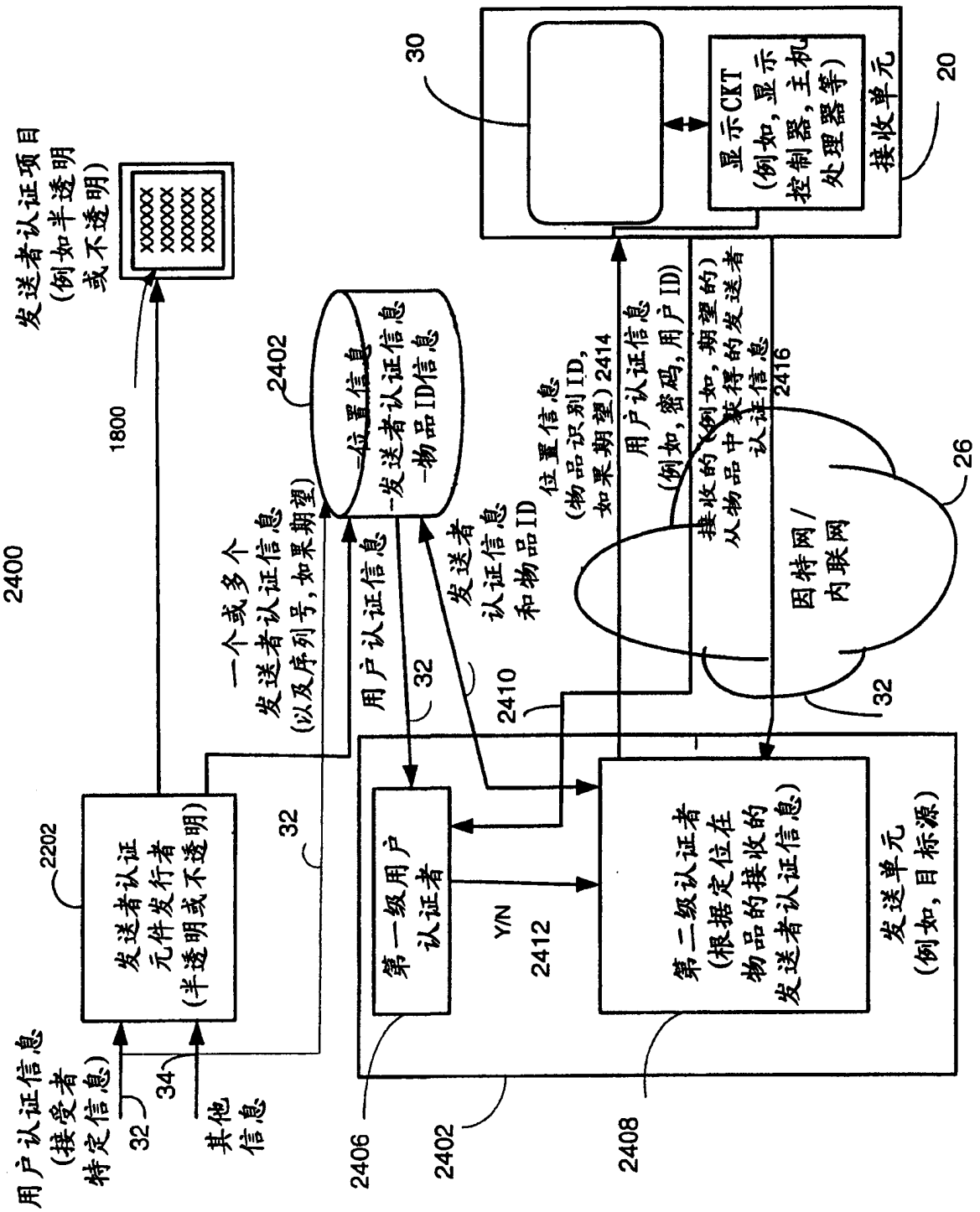

2400
发送者认证项目
(例如半透明
或不透明)
1800
XXXXXX
XXXXXX
XXXXXX
XXXXXX
30
显示CRT
(例如,显示
控制器,主机
处理器等)
接收单元
20
2402
-位置信息
-发送者认证信息
-物品ID信息
一个或多个
发送者认证信息
(以及序列号,如果期望)
位置信息
(物品识别ID,
如果期望)2414
用户认证信息
(例如,密码,用户ID)
接收的(例如,期望的)
从物品中获得的发送者
认证信息
2416
26
因特网/
内联网
用户认证信息
(接受者
特定信息)
32
34
其他
信息
2202
发送者认证
元件发行者
(半透明或不透明)
32
用户认证信息
32
发送者
认证信息
和物品ID
2410
第一级用户
认证者
Y/N
2412
第二级认证者
(根据定位在
物品的接收的
发送者认证信息)
发送单元
(例如,目标源)
2406
2402
2408
32

图24

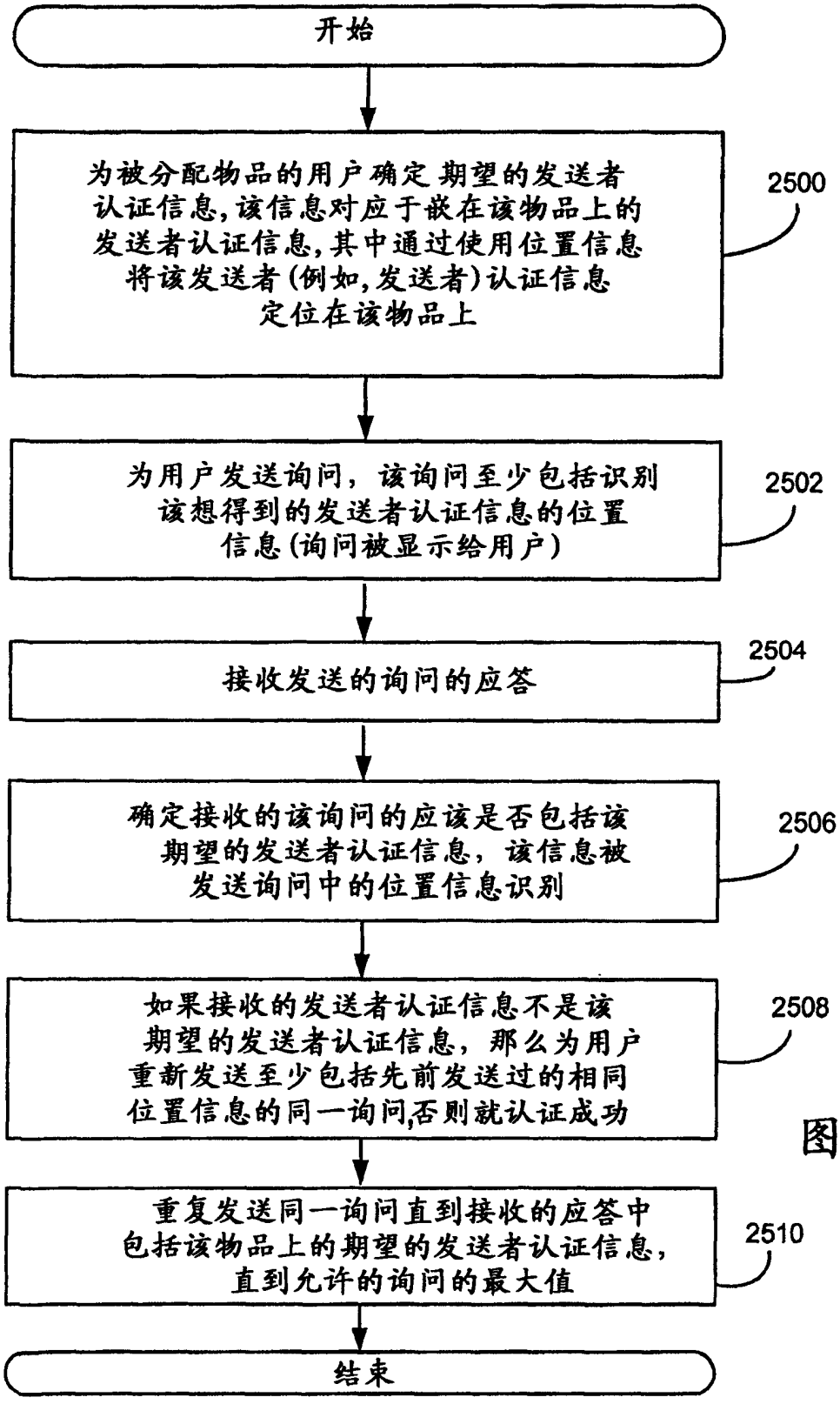

开始
为被分配物品的用户确定期望的发送者认证信息,该信息对应于嵌在该物品上的发送者认证信息,其中通过使用位置信息将该发送者(例如,发送者)认证信息定位在该物品上
2500
为用户发送询问,该询问至少包括识别该想得到的发送者认证信息的位置信息(询问被显示给用户)
2502
接收发送的询问的应答
2504
确定接收的该询问的应该是否包括该期望的发送者认证信息,该信息被发送询问中的位置信息识别
2506
如果接收的发送者认证信息不是该期望的发送者认证信息,那么为用户重新发送至少包括先前发送过的相同位置信息的同一询问,否则就认证成功
2508
重复发送同一询问直到接收的应答中包括该物品上的期望的发送者认证信息,直到允许的询问的最大值
2510
结束

图25

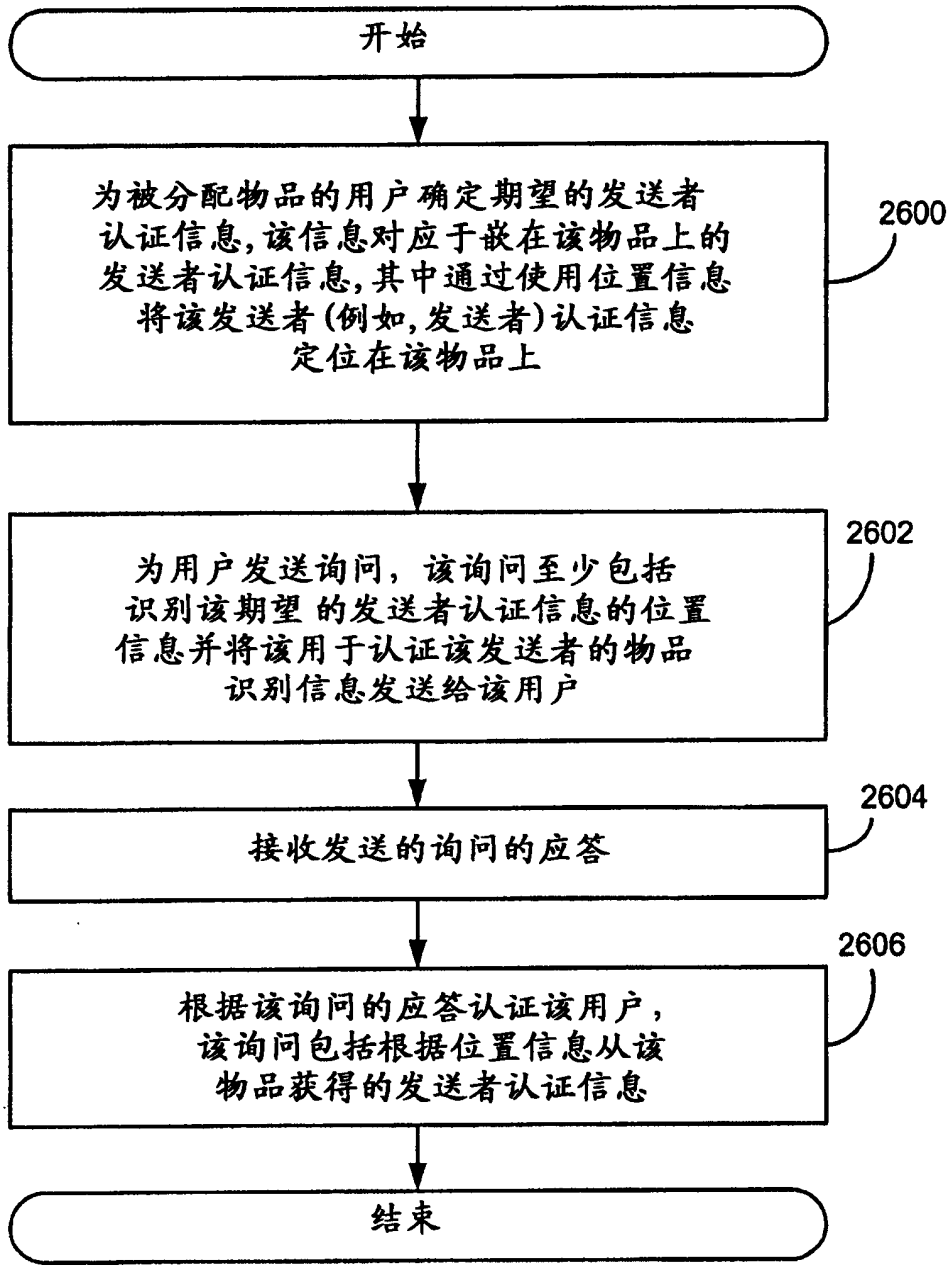

开始
为被分配物品的用户确定期望的发送者认证信息，该信息对应于嵌在该物品上的发送者认证信息，其中通过使用位置信息将该发送者（例如，发送者）认证信息定位在该物品上
2600
为用户发送询问，该询问至少包括识别该期望 的发送者认证信息的位置信息并将该用于认证该发送者的物品识别信息发送给该用户
2602
接收发送的询问的应答
2604
根据该询问的应答认证该用户，该询问包括根据位置信息从该物品获得的发送者认证信息
2606
结束

图26

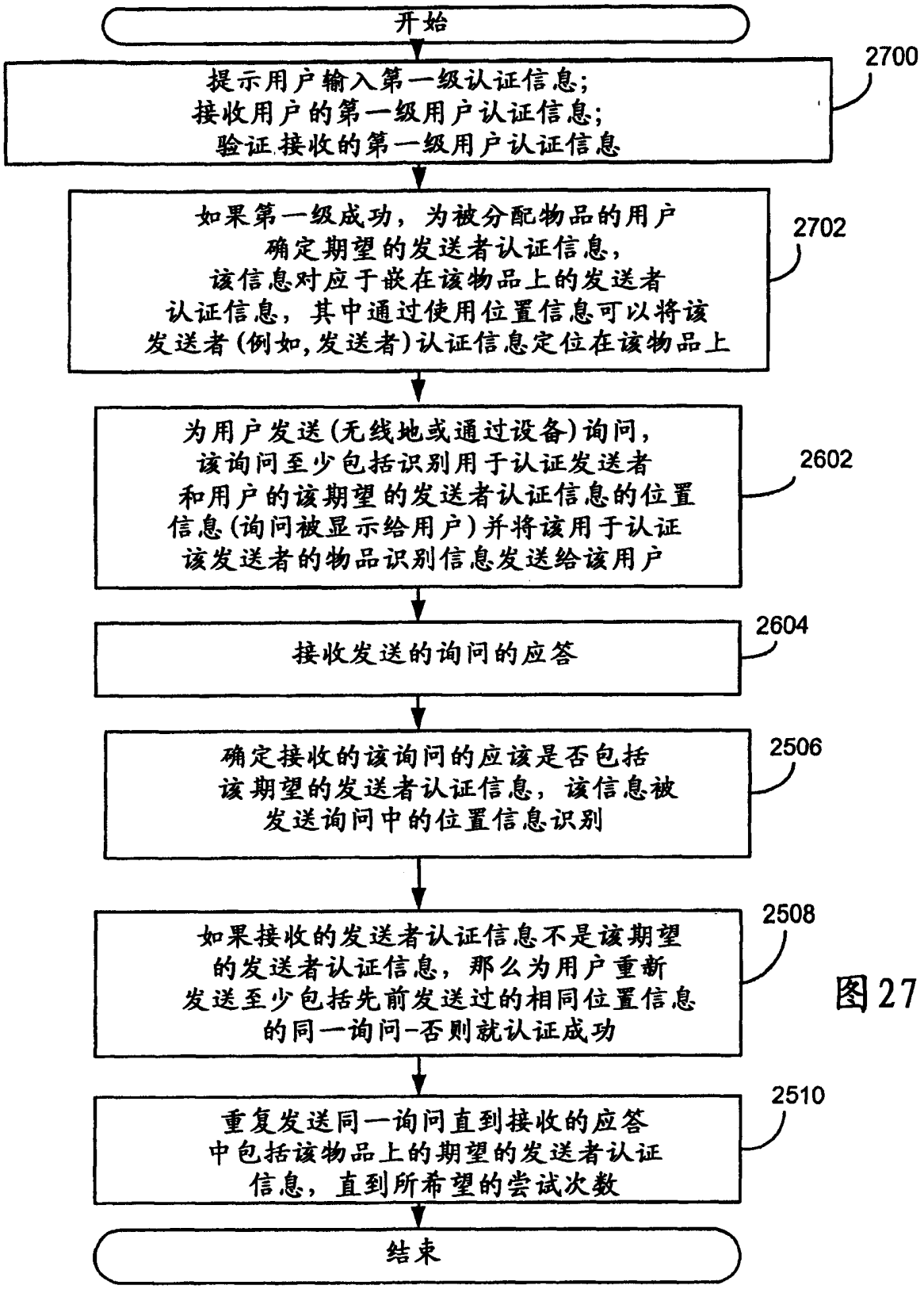
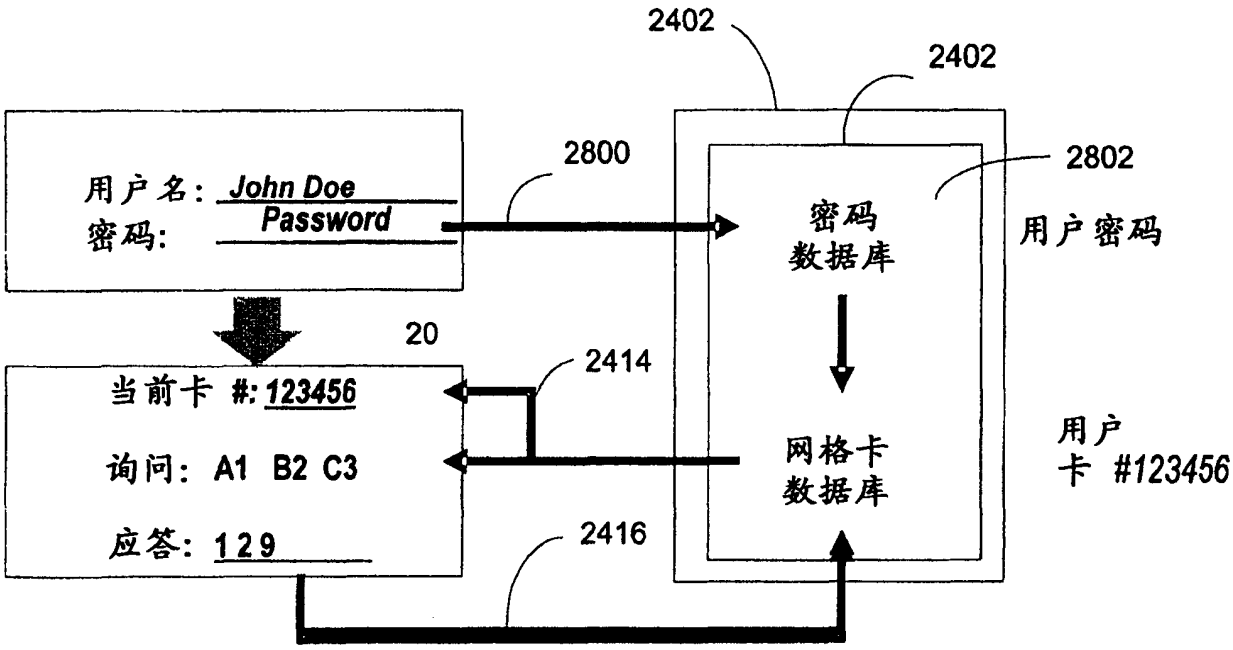

开始
提示用户输入第一级认证信息；
接收用户的第一级用户认证信息；
验证接收的第一级用户认证信息
2700
如果第一级成功，为被分配物品的用户
确定期望的发送者认证信息，
该信息对应于嵌在该物品上的发送者
认证信息，其中通过使用位置信息可以将该
发送者(例如,发送者)认证信息定位在该物品上
2702
为用户发送(无线地或通过设备)询问，
该询问至少包括识别用于认证发送者
和用户的该期望的发送者认证信息的位置
信息(询问被显示给用户)并将该用于认证
该发送者的物品识别信息发送给该用户
2602
接收发送的询问的应答
2604
确定接收的该询问的应该是否包括
该期望的发送者认证信息，该信息被
发送询问中的位置信息识别
2506
如果接收的发送者认证信息不是该期望
的发送者认证信息，那么为用户重新
发送至少包括先前发送过的相同位置信息
的同一询问-否则就认证成功
2508
重复发送同一询问直到接收的应答
中包括该物品上的期望的发送者认证
信息，直到所希望的尝试次数
2510
结束

图27

图28


2402
2402
用户名: John Doe
密码: Password
2800
2802
密码
数据库
用户密码
20
2414
当前卡 #: 123456
询问: A1 B2 C3
应答: 1 2 9
网格卡
数据库
用户
卡 #123456
2416