

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.



[12] 发明专利说明书

专利号 ZL 200510095984.7

H04L 9/00 (2006.01)

G06F 21/00 (2006.01)

G06F 17/30 (2006.01)

[45] 授权公告日 2009 年 12 月 2 日

[11] 授权公告号 CN 100566236C

[22] 申请日 2005.8.30

[21] 申请号 200510095984.7

[30] 优先权

[32] 2004.9.1 [33] EP [31] 04104195.5

[73] 专利权人 捷讯研究有限公司

地址 加拿大安大略省

[72] 发明人 尼尔·P·亚当斯

迈克尔·S·布朗

赫伯特·A·利特尔

[56] 参考文献

CN1328675A 2001.12.26

WO03/079627A2 2003.9.25

CN1401172A 2003.3.5

BlackBerry Security with the S/MIME Support
Package. Research In Motion, BlackBerry, No. 1.
5. 2003

审查员 袁 敏

[74] 专利代理机构 中科专利商标代理有限责任公
司

代理人 王 玮

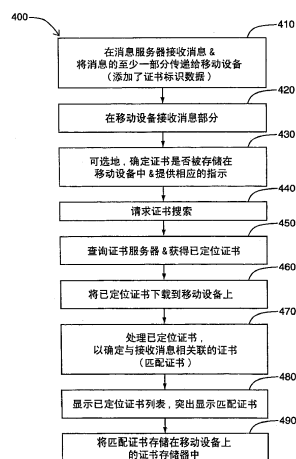
权利要求书 5 页 说明书 25 页 附图 8 页

[54] 发明名称

在系统中提供证书匹配以及用于搜索和获得
证书的方法

[57] 摘要

一种用于搜索和获得证书的系统和方法，其可以
用在对已解密消息的处理中。在一个更为广泛的
方案中，消息管理服务器根据消息，产生惟一地识
别了与所述消息相关联的证书的证书标识数据。然
后，可以使用所述证书标识数据来确定响应证书搜
索请求、从一个或多个证书服务器获得的给定已定
位证书是否是与所述消息相关联的证书。只需要证
书标识数据，有助于在用户计算设备(如移动设备
等)处的确定，缓解了用户为了进行确定而将整个
消息下载到计算设备上的需要。



1、 一种用于搜索和获得与从发送方的计算设备（262b）发送到用户的计算设备（100）的消息有关的证书的方法，所述消息包括用于识别与之相关联的发送方证书的数据，其中所述方法包括以下步骤：

在用户的计算设备（100）处通过消息管理服务器（272）接收来自发送方的计算设备（262b）的所述消息的至少一部分；

在用户的计算设备（100）处，接收由消息管理服务器（272）根据所述消息中用于识别发送方证书的数据而产生的发送方证书的证书标识数据，其中所述证书标识数据唯一地识别发送方证书；

执行搜索，以定位存储在所述用户的计算设备（100）上的证书；以及

利用所述证书标识数据，处理位于用户的计算设备（100）上的每个证书，以确定正在处理的位于用户的计算设备（100）上的证书是否是与所述消息相关联的发送方证书。

2、 根据权利要求1所述的方法，其特征在于还包括以下步骤：提供针对与发送方相关联的证书的证书搜索请求；

在一个或多个证书服务器（284）上进行搜索，其中向所述一个或多个证书服务器提交至少一个查询，以请求获得满足证书搜索请求的证书；

从所述一个或多个证书服务器获得满足证书搜索请求的至少一个证书；

利用证书标识数据，处理所获得的满足证书搜索请求的每个证书，以确定满足证书搜索请求的相应证书是否是与所述消息相关联的发送方证书；以及

如果确定满足证书搜索请求的相应证书是与所述消息相关联的发送方证书，则将满足证书搜索请求的相应证书存储在所述用户的计算设备上。

3、 根据权利要求1或2所述的方法，其特征在于所述用户的计

算设备包括移动设备（100）。

4、 根据权利要求 2 所述的方法，其特征在于所述用户的计算设备包括移动设备（100），并且在与所述移动设备（100）相连的第二计算设备（288）处执行在一个或多个证书服务器（284）上进行搜索的步骤和从所述一个或多个证书服务器获得满足证书搜索请求的至少一个证书的步骤。

5、 根据权利要求 4 所述的方法，其特征在于所述第二计算设备包括移动数据服务器（288）。

6、 根据权利要求 4 或 5 所述的方法，其特征在于也在第二计算设备处（288）执行利用证书标识数据处理所获得的满足证书搜索请求的每个证书，以确定满足证书搜索请求的相应证书是否是与所述消息相关联的发送方证书的步骤，以及所述方法还包括将被确定为与所述消息相关联的发送方证书的满足证书搜索请求的相应证书从第二计算设备下载到移动设备（100）的步骤。

7、 根据权利要求 4 或 5 所述的方法，其特征在于在移动设备（100）处执行利用证书标识数据处理所获得的满足证书搜索请求的每个证书，以确定满足证书搜索请求的相应证书是否是与所述消息相关联的发送方证书的步骤，以及所述方法还包括将从所述一个或多个证书服务器（284）获得的满足证书搜索请求的相应证书从第二计算设备（288）下载到移动设备（100）的步骤。

8、 根据权利要求 2、4 和 5 中的任一个所述的方法，其特征在于还包括在用户的计算设备（100）上显示在从所述一个或多个证书服务器（284）获得的满足证书搜索请求的至少一个证书的列表，其中所述列表表示如果存在，哪个满足证书搜索请求的证书被确定为与所述消息相关联的发送方证书。

9、 根据权利要求 8 所述的方法，其特征在于还包括接收用户对所述列表中的满足证书搜索请求的至少一个证书的一个或多个选择，并将一个或多个选择的满足证书搜索请求的至少一个证书存储在所述用户的计算设备（100）上的证书存储器中。

10、 根据权利要求 2、4 和 5 中的任一个所述的方法，其特征在

于还包括：在提供针对与发送方相关联的证书的证书搜索请求的步骤之前、执行利用证书标识数据处理位于用户的计算设备（100）上的每个证书，以确定位于用户的计算设备（100）上的证书是否是与所述消息相关联的发送方证书的步骤。

11、根据权利要求 1 或 2 所述的方法，其特征在于利用证书标识数据处理位于用户的计算设备（100）上的每个证书，以确定位于用户的计算设备（100）上的证书是否是与所述消息相关联的发送方证书的步骤包括以下步骤：

产生与位于所述用户的计算设备（100）上的每个证书相关联的证书标识数据；以及

将针对位于所述用户的计算设备（100）上的每个证书的已产生证书标识数据与在用户的计算设备（100）处接收的证书标识数据进行比较，以识别与发送方证书匹配的已存储证书。

12、根据权利要求 2、4 和 5 中任一个所述的方法，其特征在于：处理所获得的满足证书搜索请求的每个证书，以确定所获得的满足证书搜索请求的证书是否是与所述消息相关联的发送方证书的步骤包括：

产生与所获得的满足证书搜索请求的每个证书相关联的证书标识数据；以及

将针对所获得的满足证书搜索请求的每个证书的已产生证书标识数据与在用户的计算设备（100）处接收的证书标识数据进行比较，以识别与发送方证书匹配的所获得的满足证书搜索请求的证书。

13、根据权利要求 2、4 和 5 中任一个所述的方法，其特征在于针对发送方证书的证书标识数据包括针对发送方证书的序列号和颁发者数据；以及解析每个满足证书搜索请求的证书，以获得满足证书搜索请求的证书的相应序列号和颁发者数据，并将针对满足证书搜索请求的每个证书所获得的序列号和颁发者数据与针对发送方证书的证书标识数据进行比较。

14、根据权利要求 2、4 和 5 中任一个所述的方法，其特征在于针对发送方证书的证书标识数据包括发送方证书的至少一部分的散列

信息；以及满足证书搜索请求的每个证书具有应用于其的散列算法，以获得满足证书搜索请求的证书的相应散列信息，并将针对满足证书搜索请求的每个证书所获得的散列信息与针对发送方证书的证书标识数据进行比较。

15、根据权利要求 1 或 2 所述的方法，其特征在于针对发送方证书的证书标识数据包括针对发送方证书的序列号和颁发者数据；以及解析位于用户的计算设备（100）上的每个证书，以获得针对位于用户的计算设备（100）上的证书的相应序列号和颁发者数据，并将针对位于用户的计算设备（100）上的每个证书所获得的序列号和颁发者数据与针对发送方证书的证书标识数据进行比较。

16、根据权利要求 1 或 2 所述的方法，其特征在于针对发送方证书的证书标识数据包括发送方证书的至少一部分的散列信息；以及位于用户的计算设备（100）上的每个证书具有应用于其的散列算法，以获得位于用户的计算设备（100）上的证书的相应散列信息，并将针对位于用户的计算设备（100）上的每个证书所获得的散列信息与针对发送方证书的证书标识数据进行比较。

17、一种用于搜索和获得与由用户的计算设备（100）从发送方的计算设备（262b）接收到的消息有关的证书的系统，所述消息包括用于识别与之相关联的发送方证书的数据，所述系统包括：

消息管理服务器（272），用于根据所述消息，产生证书标识数据，其中所述证书标识数据唯一地识别发送方证书；

包括移动设备（100）的用户的计算设备，用于从消息管理服务器（272）接收所述消息的至少一部分和证书标识数据；以及

移动数据服务器（288），用于从用户的移动设备接收针对与发送方相关联的证书的搜索请求，通过针对满足搜索请求的已定位证书查询一个或多个证书服务器，在一个或多个证书服务器（284）上进行搜索，以及从所述一个或多个证书服务器获得已定位证书；

其中所述移动设备（100）和所述移动数据服务器（288）中的至少一个还用于处理在所述移动数据服务器（288）处获得的每个已定位证书，以利用证书标识数据，确定相应已定位证书是否为与所述消息

相关联的发送方证书；以及其中所述移动设备（100）提供一个或多个证书存储器，用于存储被确定为与所述消息相关联的发送方证书的已定位证书。

在系统中提供证书匹配以及用于搜索和获得证书的方法

技术领域

本发明大体上涉及如电子邮件消息等消息的处理，更具体地，涉及一种用于搜索和获得用在处理已编码消息中的系统和证书的方法。

背景技术

可以利用多种已知协议之一对电子邮件(“e-mail”)消息进行编码。如安全多用途因特网邮件扩展(“S/MIME”)等一些协议依赖于公用和私用加密密钥来提供保密性和完整性，以及依赖于公用密钥基础结构(PKI)来通信提供了验证和授权的信息。只能利用私用密钥/公用密钥对的公用密钥来解密利用该对的对应私用密钥进行了加密的数据，反之亦然。利用证书来确认用在消息编码中的公用密钥的真实性。具体地，如果计算设备的用户想要在将消息发送给特定的个体之前对消息进行解密，则该用户需要针对该个体的证书。所述证书典型地包括该个体的公用密钥以及其他标识相关信息。类似地，如果计算设备的用户希望验证已签名消息的发送方，该用户需要针对该发送方的证书。

如果所需证书并未存储在用户的计算设备上，则必须首先获得证书。搜索并获得特定的证书是涉及通过使用户在显示在计算设备上的搜索表格中手动输入要请求其证书的个体的姓名和/或电子邮件地址来查询证书服务器的处理。通常，随后将搜索中所定位的证书暂时下载到计算设备上，以便进行考虑，于是可以向用户显示已定位证书列表。然后，用户可以手动识别列表中的选定证书，从而存储在计算设备的非易失性存储器中，以便于可能的将来使用。

考虑用户的计算设备是移动设备的实施方式。当在消息服务器接收到消息并且可用于下载到移动设备时，通常只是在预定大小的连续

数据块中将消息传输到移动设备，以便保留带宽。更具体地，将消息的第一块（例如 2KB 的数据）下载到移动设备，如果用户想要接收更多的消息，用户可以请求将其他块下载到移动设备，直到已经将整个消息下载到移动设备或者直到达到消息下载的一些预定限制为止。

例如，如果所接收到的消息是已签名 S/MIME 消息，为了验证消息的完整性和验证发送方的身份，需要发送方的证书。在一些情况下，所需证书可以伴随所述消息，典型地将证书附加到消息的末尾。或者，所需证书可以不伴随所述消息，而是提供识别用在签名中的证书的一个或多个证书标识符，通常也位于消息的末尾。然后，如果该证书已经被存储在移动设备的证书存储器中，则从中获得所识别的证书，或者可以从能够如上所述地从中下载证书的证书服务器中获得所识别的证书。

为了获得针对消息的证书或证书标识符，典型地必须将整个消息下载到移动设备。不幸地，只是为了简单地获得证书信息而下载整个消息是耗时和昂贵的任务（例如，对于带宽而言）。另一方面，如果只将消息的一小部分下载到移动设备上，或者如果消息太长而由于所设置的限制不能将其下载到移动设备上，则不能识别以一些确定的事实验证接收消息的完整性和验证发送方身份所需的证书。

发明内容

本发明的实施例大体上涉及一种用于更有效地搜索和获得证书的系统和方法，其中可以识别所需证书，而无需将发送方的消息完整地下载到用户的计算设备（如移动设备等）上。具体地，所述系统和方法有助于从搜索一个或多个证书服务器中而定位的证书中确定所需的证书。

在本发明的一个更为广泛的方案中，提出了一种用于搜索和获得与用户从发送方接收到的消息有关的证书的方法，所述消息包括用于识别与之相关联的发送方证书的数据，其中可以根据所述消息，产生惟一地识别了发送方证书的证书标识数据，所述方法包括以下步骤：在计算设备处接收所述消息的至少一部分和证书标识数据；提供针对

与发送方相关联的证书的证书搜索请求；在一个或多个证书服务器上进行搜索，其中向所述一个或多个证书服务器提交至少一个查询，以请求获得满足证书搜索请求的已定位证书；从所述一个或多个证书服务器获得至少一个已定位证书；利用证书标识数据，处理所获得的每个已定位证书，以确定各个已定位证书是否是与所述消息相关联的发送方证书；以及如果在确定步骤确定已定位证书是与所述消息相关联的发送方证书，则将已定位证书存储在所述计算设备上。

在另一更为广泛的方案中，所产生的证书标识数据包括针对发送方证书的序列号和颁发者数据；以及所述处理步骤包括解析所获得的每个已定位证书，以获得各自的序列号和颁发者数据，并将各自的序列号和颁发者数据与证书标识数据进行比较。

在另一更为广泛的方案中，所产生的证书标识数据包括发送方证书的至少一部分的散列信息；以及所述处理步骤包括将散列算法应用于所获得的每个已定位证书，以获得各自的散列信息，并将各自的散列信息与证书标识数据进行比较。

在本发明的另一更为广泛的方案中，提出了一种用于搜索和获得与用户从发送方接收到的消息有关的证书的系统，所述消息包括用于识别与之相关联的发送方证书的数据，所述系统包括：消息管理服务器，用于根据所述消息，产生证书标识数据，其中所述证书标识数据唯一地识别发送方证书；移动设备，用于从消息管理服务器接收所述消息的至少一部分和证书标识数据；以及移动数据服务器，用于从移动设备接收针对与发送方相关联的证书的证书搜索请求，通过针对满足搜索请求的已定位证书查询一个或多个证书服务器，在一个或多个证书服务器上进行搜索，以及从所述一个或多个证书服务器获得已定位证书；其中所述移动设备和所述移动数据服务器中的至少一个还用于处理在所述移动数据服务器处获得的每个已定位证书，以利用证书标识数据，确定各个已定位证书是否是与所述消息相关联的发送方证书；以及其中所述移动设备提供一个或多个证书存储器，用于存储被确定为与所述消息相关联的发送方证书的证书。

在另一更为广泛的方案中，提出了一种用于搜索和获得与用户从

发送方接收到的消息有关的证书的方法，所述消息包括用于识别与之相关联的发送方证书的数据，其中所述方法包括以下步骤：根据所接收到的消息中的数据，产生针对发送方证书的证书标识数据，用于识别发送方证书，其中所述证书标识数据惟一地识别发送方证书；在计算设备处接收证书标识数据；以及通过产生与存储在计算设备上的多个证书中的每一个相关联的证书标识数据，以及将针对所述多个已存储证书中的每一个的已产生证书标识数据与针对发送方证书而产生的证书标识数据进行比较，以识别与发送方证书匹配的已存储证书，来确定发送方证书是否被存储在计算设备上。

附图说明

为了更好地理解本发明的实施例，以及更为清楚地示出其如何实现所述效果，以下将参照附图，作为示例，对其进行描述，其中：

图 1 是一个示例实施方式中的移动设备的方框图；

图 2 是图 1 所示移动设备的通信子系统组件的方框图；

图 3 是无线网络的节点的方框图；

图 4 是示出了一个示例结构中的主机系统的组件的方框图；

图 5 是示出了证书链的示例的方框图；

图 6 是示出了已编码消息的示例的组件的方框图；

图 7A 是示出了本发明一个实施例中的搜索和获得证书的方法中的步骤的流程图；以及

图 7B 是示出了本发明另一实施例中的搜索和获得证书的方法中的步骤的流程图。

具体实施方式

本发明的一些实施例使用移动台。移动台是具有高级数据通信能力的双向通信设备，具有与其他计算机系统进行通信的能力，并且以下被统称为移动设备。移动设备还可以包括语音通信能力。根据移动设备所提供的功能，可以将其称为数据消息收发设备、双向寻呼机、具有数据消息收发能力的蜂窝电话、无线因特网设备或数据通信设备

(具有或不具有电话功能)。移动设备通过收发机站网络与其他设备进行通信。

为了帮助读者理解移动设备的结构及其如何与其他设备进行通信,将参照图 1 到 3。

首先,参考图 1,将一个示例实施方式中的移动设备的方框图总体表示为 100。移动设备 100 包括多个组件,控制组件是微处理器 102。微处理器 102 控制移动设备 100 的总体操作。通过通信子系统 104 执行包括数据和语音通信在内的通信功能。通信子系统 104 从和向无线网络 200 接收和发送消息。在移动设备 100 的示例实施方式中,根据全球移动通信系统(GSM)和通用分组无线业务(GPRS)标准来配置通信子系统 104。GSM/GPRS 无线网络得到了广泛的使用,并且预期这些标准将被全球发展增进型数据比率(EDGE)和通用移动通信系统(UMTS)所取代。仍在定义新标准,但可以确信其将具有与这里所描述的网络行为的类似性,并且本领域普通技术人员应当理解的是本发明倾向于使用未来开发的任何适当的标准。连接通信子系统 104 和网络 200 的无线链路表示一个或多个不同的射频(RF)信道,根据针对 GSM/GPRS 通信而规定的已定义协议进行操作。利用更新的网络协议,这些信道能够支持电路交换语音通信和分组交换数据通信。

尽管在移动设备 100 的一个典型实施方式中,与移动设备 100 相关联的无线网络是 GSM/GPRS 无线网络,在变体实施方式中,其他无线网络也可以与移动设备 100 相关联。例如,可以采用的不同类型的无线网络包括:数据中心型无线网络、语音中心型无线网络和通过相同的物理基站能够支持语音和数据通信的双模式网络。组合双模式网络包括但不限于码分多址(CDMA)或 CDMA2000 网络、GSM/GPRS 网络(如上所述)和将来第三代(3G)网络,如 EDGE 和 UMTS。数据中心网络的一些较早示例包括 Mobitex™ 无线网络和 DataTAC™ 无线网络。较早的语音中心型数据网络的示例包括个人通信系统(PCS)网络,如 GSM 和时分多址(TDMA)系统。

微处理器 102 还与其他子系统进行交互,如随机存取存储器(RAM) 106、闪速存储器 108、显示器 110、辅助输入/输出(I/O)子系统 112、

串行端口 114、键盘 116、扬声器 118、麦克风 120、短距离通信子系统 122 和其他设备 124。

移动设备 100 的一些子系统执行通信相关的功能，而其他子系统可提供“驻留”或设备内置功能。作为示例，显示器 110 和键盘 116 可以用于如输入用于通过网络 200 传送的文本消息等通信相关功能以及如计算器或任务表等设备驻留功能。通常将微处理器 102 使用的操作系统软件存储在如闪速处理器 108 等永久存储器中，或者可以是只读存储器（ROM）或类似的存储元件（未示出）。本领域普通技术人员应当清楚的是可以将操作系统、设备专用应用程序或其一部分暂时加载到如 RAM 106 等易失性存储器中。

在已经完成所需的网络登记或激活程序之后，移动设备 100 可以在网络 200 上发送和接收通信信号。网络接入与移动设备 100 的订户或用户相关联。为了识别订户，移动设备 100 需要将订户身份模块或“SIM”卡 126 插入 SIM 接口 128 中，以便与网络进行通信。特别地，SIM 126 是用于识别移动设备 100 的订户和使移动设备 100 个性化的一类传统“智能卡”。没有 SIM 126，移动设备 100 不能完全操作与网络 200 的通信。通过将 SIM 126 插入 SIM 接口 128，订户可以访问全部已订阅服务。服务可以包括：网络浏览和消息收发，如电子邮件、语音邮件、短消息服务（SMS）和多媒体消息服务（MMS）。更多的高级服务可以包括：销售点、现场服务和销售力量自动控制（sales force automation）。SIM 126 包括处理器和用于存储信息的存储器。一旦将 SIM 126 插入 SIM 接口 128 中，其与微处理器 102 相连。为了识别订户，SIM 126 包含一些用户参数，如国际移动订户身份（IMSI）等。使用 SIM 126 的优点是用户不必与任何单一的物理移动设备绑定。SIM 126 也可以存储针对移动设备的额外订户信息，包括记事册（或日历）信息和最近呼叫信息。

移动设备 100 是电池供电的设备，并包括电池接口 132，用于容纳一个或多个可充电电池 130。电池接口 132 与稳压器（未示出）相连，其辅助电池 130 将电源 V+ 提供给移动设备 100。尽管目前的技术使用电池，但如微型燃料电池等未来的技术也可以为移动设备 100 提

供能量。

除了其操作系统功能外，微处理器 102 能够在移动设备 100 上执行软件应用程序。通常在制造期间，将控制基本设备操作的应用程序组（包括数据和语音通信应用程序）安装到移动设备 100 上。可以加载到移动设备 100 上的其他应用程序是个人信息管理器（PIM）。PIM 具有组合和管理用户所关心的数据项的功能，例如但不限于电子邮件、日历事件、语音邮件、约会和任务项。PIM 应用程序具有通过无线网络 200 发送和接收数据项的能力。PIM 数据项可以通过无线网络 200 与所存储的和/或与主计算机系统相关的、移动设备订户的相应数据项无缝集成、同步和更新。此功能在移动设备 100 上创建了针对这些数据项的镜像主机。这在主计算机系统是移动设备订户的办公室计算机系统的情况下尤为有利。

附加的应用程序也可以通过网络 200、通过辅助 I/O 子系统 112、通过串行端口 114、通过短距离通信子系统 122 或通过任何其他合适的子系统 124 加载到移动设备 100 上。这种在应用程序安装方面的灵活性增加了移动设备 100 的功能，并且能够提供增强的设备内置功能、通信相关功能或这二者。例如，安全通信应用程序可以使得电子商务功能和其他财务交易能够使用移动设备 100 执行。

通过提供除了通过无线通信网络以外到移动设备 100 的信息或软件下载，串行端口 114 使订户能够通过外部设备或软件应用程序来设置偏好，并扩展移动设备 100 的能力。例如，可选的下载路径可以用于通过直接、从而可靠、可信的连接，将加密密钥加载到移动设备 100 上，以提供安全设备通信。

短距离通信子系统 122 用于移动设备 100 和不同系统或设备之间的通信，无需使用网络 200。例如，子系统 122 可以包括红外设备以及用于短距离通信的相关电路和组件。短距离通信的示例将包括由红外数据协会（IrDA）、蓝牙开发的标准和由 IEEE 开发的 802.11 标准族。

在使用中，通信子系统 104 将处理如文本消息、电子邮件消息或网页下载等接收信号，并输入微处理器 102。然后，微处理器 102 处

理接收信号，以便输出到显示器 110 或者代替地输出到辅助 I/O 子系统 112。订户也可以构造数据项，如电子邮件消息等，例如，与显示器 110 和可能的辅助 I/O 子系统 112 相结合地使用键盘 116。辅助子系统 112 可以包括以下设备：触摸屏、鼠标、轨迹球、红外指纹检测器或具有动态按钮按下能力的滚轮。键盘 116 是字母数字键盘和/或电话型小键盘。可以通过通信子系统 104、在网络 200 上传输所构造的数据项。

对于语音通信，移动设备 100 的总体操作实质上是类似的，除了将接收到的信号输出到扬声器 118 和用于传输的语音信号由麦克风 120 产生之外。可选的语音或音频 I/O 子系统，如语音消息记录子系统，也可以在移动设备 100 上实现。尽管语音或音频信号输出主要通过扬声器 118 完成，也可以使用显示器 110 提供如呼叫方身份、语音呼叫的持续时间或其他语音呼叫相关信息等附加信息。

现在参照图 2，示出了图 1 所示的通信子系统组件 104 的方框图。通信子系统 104 包括接收机 150、发射机 152、一个或多个嵌入式或内部天线元件 154、156、本地振荡器 (LO) 158 和如数字信号处理器 (DSP) 160 等处理模块。

通信子系统 104 的详细设计取决于移动设备 100 将运行其中的网络 200，因此应当理解的是图 2 所示的涉及只用作一个示例。将天线 154 通过网络 200 接收的信号输入接收机 150，接收机 150 可以进行如信号放大、频率下转换、滤波、信道选择和模拟到数字 (A/D) 转换等普通接收机功能。接收信号的 A/D 转换允许更复杂的通信功能，如要在 DSP 160 中执行的数字解调和解码。以类似方式，处理要发射的信号，包括 DSP 160 执行的调制和编码。将这些 DSP 处理后的信号输入发射机 152，进行数字模拟 (D/A) 转换、频率上变换、滤波、放大和经天线 156 在网络 200 上传输。DSP 160 不仅处理通信信号，还提供接收机和发射机控制。例如，可以通过在 DSP 160 中实现的自动增益控制算法，自适应控制施加到接收机 150 和发射机 152 中的通信信号的增益。

移动设备 100 和网络 200 之间的无线链路可以包含一个或多个不

同的信道（典型地是不同的 RF 信道）以及用在移动设备 100 和网络 200 之间的相关协议。典型地，由于移动设备 100 的总体带宽和有限电池功率，RF 信道是有限的资源，必须加以保留。

当移动设备 100 可完全操作时，发射机 152 通常只在其向网络 200 进行发送时接通，而在其他时刻关闭，以保留资源。类似地，在指定的时间段内，接收机 150 周期性地关闭，以保留电力，直到其需要接收信号或信息为止。

现在参照图 3，将无线网络的节点的方框图表示为 202。具体地，网络 200 包括一个或多个节点 202。移动设备 100 与无线网络 200 中的节点 202 进行通信。在图 3 所示的示例实施方式中，根据通用分组无线业务（GPRS）和全球移动通信系统（GSM）技术来配置节点 202。节点 202 包括与塔站 206 相关联的基站控制器（BSC）204、添加了对 GSM 中的 GPRS 支持的分组控制单元（PCU）208、移动交换中心（MSC）210、归属位置寄存器（HLR）212、拜访位置寄存器（VLR）214、服务 GPRS 支持节点（SGSN）216、网关 GPRS 支持节点（GGSN）218 和动态主机配置协议（DHCP）220。此组件列表并不表示 GSM/GPRS 网络中的每个节点 202 的穷尽组件列表，而是通常用在通过网络 200 的通信中的组件列表。

在 GSM 网络中，MSC 210 与 BSC 204 和陆上传输网络（如公用交换电话网络（PTSN）222 等）相连，以满足电路交换的需求。通过 PCU 208、SGSN 216 和 GGSN 218 到公用或专用网络（因特网）224（也统称为共享网络基础结构）的连接表示针对 GPRS 使能移动设备的数据路径。在以 GPRS 能力加以扩展的 GSM 网络中，BSC 204 还包含与 SGSN 216 相连的分组控制单元（PCU）208，用于控制分段、无线电信道分频，以及满足分组交换需要。为了跟踪移动设备位置和可用性，以便进行电路交换和分组交换管理，在 MSC 210 和 SGSN 216 之间共享 HLR 212。对 VLR 214 的访问由 MSC 210 控制。

站点 206 是固定收发机站。站点 206 和 BSC 204 一起形成了固定收发机设备。固定收发机设备提供针对通常被称作“小区”的特定覆盖区域的无线网络覆盖。固定收发机设备通过站点 206 向和从其小区

内的移动设备发射和接收通信信号。固定收发机设备通常在其控制器的控制下，根据特定、通常是预定的通信协议和参数，执行对要发送到移动设备的信号的调制和可能的编码和/或加密等处理。固定收发机设备类似地解调和可能地解码和解密（如果需要的话）从其小区内的移动设备 100 接收到的任意通信信号。通信协议和参数可以在不同的节点间不同。例如，一个节点可以采用不同的调制方案，并在与其他节点不同的频率进行操作。

对于与特定网络进行登记的全部移动设备 100，将如用户简档表等永久配置数据存储在 HLR 212 中。HLR 212 还包含针对每个已登记移动设备的位置信息，并且可以被查询，以确定移动设备的当前位置。MSC 210 负责一组位置区域，并将当前位于其负责区域内的移动设备的数据存储在 VLR 214 中。其他 VLR 214 也包含与拜访其他网络的移动设备有关的信息。VLR 214 中的信息包括从 HLR 212 传送到 VLR 214 的部分永久移动设备数据，以便进行更快的访问。通过将额外的信息从远程 HLR 212 节点移动到 VLR 214，可以减少这些节点间的业务量，从而能够以更快的响应时间提供语音和数据服务，并且同时需要较少地使用计算资源。

SGSN 216 和 GGSN 218 为添加了对 GPRS 的支持的元件；即在 GSM 内支持分组交换数据。SGSN 216 和 MSC 210 在无线网络 200 内具有类似的职责，保持对每个移动设备 100 的位置的跟踪。SGSN 216 还执行安全功能和对网络 200 上的数据业务的访问控制。GGSN 218 提供与外部分组交换网络的联网连接，并通过在网络 200 内进行操作的因特网协议（IP）骨干网与一个或多个 SGSN 216 相连。在正常操作期间，给定的移动设备 100 必须执行“GPRS 附属”以获取 IP 地址并访问数据服务。由于将集成服务数字网络（ISDN）地址用于路由呼入和呼出呼叫，这一要求并不出现在电路交换语音信道中。目前，所有 GPRS 使能网络使用专用、动态分配 IP 地址，因而需要与 GGSN 218 相连的 DHCP 服务器 220。存在多种针对动态 IP 分配的机制，包括使用远程验证拨入用户服务（RADIUS）服务器和 DHCP 服务器的组合。一旦 GPRS 附属完成，则建立从移动设备 100 通过 PCU 208 和 SGSN 216 到 GGSN 218

内的接入点节点 (APN) 的逻辑连接。APN 表示能够访问直接因特网兼容服务或专用网络连接的 IP 隧道的逻辑端点。在每个移动设备 100 必须被分配给一个或多个 APN, 并且如果未执行对以授权其使用的 APN 的 GPRS 附属, 移动设备 100 不能交换数据这一点上, APN 还表示针对网络 200 的安全机制。可以认为 APN 与如 “myconnection.wireless.com” 等因特网域名相似。

一旦 GPRS 附属完成, 则创建了隧道, 并利用 IP 分组中能够支持的任何协议, 在标准 IP 分组内交换所有业务。这包括如在与虚拟专用网络 (VPN) 一起使用的一些 IP 安全 (IPsec) 连接的情况下的 IP over IP 等隧道方法。这些隧道也被称为分组数据协议 (PDP) 上下文, 并且在网络 200 中存在有限的可用数量。为了最大化对 PDP 上下文的使用, 网络 200 将运行针对每个 PDP 上下文的空闲定时器, 以确定是否缺乏活动性。当移动设备 100 并未使用其 PDP 上下文时, 可以取消对 PDP 上下文的分配, 并将 IP 地址返回给由 DHCP 服务器 220 管理的 IP 地址库。

现在参照图 4, 示出了一个示例结构中的主机系统的组件的方框图。主机系统 250 将典型地是公司办公室或其他局域网 (LAN), 但也可以是家庭办公室计算机或一些其他私有系统, 例如在变体实施方式中。在图 4 所示的示例中, 将主机系统 250 图示为移动设备 100 的用户所属的组织的 LAN。

LAN 250 包括通过 LAN 连接 260 彼此相连的多个网络组件。例如, 具有用于用户移动设备 100 的附属底座 264 的用户桌面计算机 262a 适用于 LAN 250 上。例如, 针对移动设备 100 的底座 264 可以通过串行或通用串行总线 (USB) 连接与计算机 262a 相连。其他用户计算机 262b 也适用于 LAN 250, 并且每个计算机可以配备有或不配备有针对移动设备的附属底座 264。底座 264 有利于信息 (例如 PIM 数据、有利于移动设备 100 和 LAN 250 之间的安全通信的私用对称密钥等) 从用户计算机 262a 到移动设备 100 的加载, 并且对于通常在初始化移动设备 100 以便使用时执行的批量信息更新尤为有用。下载到移动设备 100 上的信息可以包括用在消息交换中的证书。本领域普通技术人员

应当理解,用户计算机 262a、262b 还将典型地与图 4 未示出的其他外围设备相连。

本发明的实施例大体上涉及消息的处理,如电子邮件消息等,以及一些实施例大体上涉及这种消息到和从移动设备 100 的通信。因此,为了便于公开,图 4 只示出了 LAN 250 的网络组件的子集,并且本领域普通技术人员应当理解的是,对于此示例结构,LAN 250 将包括图 4 中未详尽示出的额外组件。更一般地,LAN 250 可以表示所述组织的较大网络[未示出]的一小部分,并且可以包括与图 4 所示的示例不同的组件和/或按照与图 4 所示的示例不同的拓扑进行排列。

在此示例中,移动设备 100 通过无线网络 200 的节点 202 和如服务提供商网络或公用因特网等共享网络基础结构 224 与 LAN 250 进行通信。可以通过一个或多个路由器[未示出]提供对 LAN 250 的接入,并且 LAN 250 的计算设备可以在防火墙或代理服务器 266 的后面进行操作。

在变体实施方式中,LAN 250 包括无线 VPN 路由器[未示出],便于 LAN 250 和移动设备 100 之间的数据交换。无线 VPN 路由器的概念在无线产业中是新的,并且意味着可以通过特定的无线网络直接建立对移动设备 100 的 VPN 连接。使用无线 VPN 路由器的可能性在最近才成为可能,并且可以在新的因特网协议(IP)版本 6(IPv6)出现在基于 IP 的无线网络中时使用。这种新协议将提供足够的 IP 地址,从而使 IP 地址专用于每个移动设备,使其能够在任意时刻将信息推入移动设备。使用无线 VPN 路由器的优点是其可以是不需要使用分离的无线网关和分离的无线基础设施的现成的 VPN 组件。优选地,在此变体实施方式中,VPN 连接可以是传输控制协议(TCP)/IP 或用户数据报协议(UDP)/IP 连接,直接将消息传递到移动设备 100。

最初,由 LAN 250 的消息服务器 268 接收针对移动设备 100 的用户的消息。这些消息可以来自于多个源中的任意一个。例如,可以由发送方从 LAN 250 内的移动设备 262b、从与无线网络 200 或不同无线网络相连的不同移动设备[未示出]、或从不同的计算设备或能够发送消息的其他设备,通过共享网络基础结构 224,并可能通过应用服务

提供商（ASP）或因特网服务提供商（ISP），发送消息。

消息服务器 268 典型地作为交换消息的主要接口，尤其是电子邮件消息，在所述组织内部，在共享网络基础结构 224 上。已经建立用于发送和接收消息的组织中的每个用户典型地与由消息服务器 268 管理的用户帐户相关联。消息服务器 268 的一个示例是 Microsoft Exchange™ 服务器。在一些实施方式中，LAN 250 可以包括多个消息服务器 268。消息服务器 268 也可以适用于提供除消息管理以外的附加功能，例如，包括与日历和任务列表相关的数据的管理等。

当消息服务器 268 接收到消息时，通常将其存储在消息存储器[未详尽示出]中，随后可以从中检索消息并传递给用户。例如，在用户计算机 262a 上操作的电子邮件客户端应用程序可以请求与存储在消息服务器 268 上的用户帐户相关联的电子邮件消息。然后，从消息服务器 268 获得这些消息，并本地存储在计算机 262a 上。

当操作移动设备 100 时，用户可能希望将所获得的电子邮件消息传递到手持设备上。在移动设备 100 上进行操作的电子邮件客户端应用程序也可以向消息服务器 268 请求与用户帐户相关联的消息。可以配置电子邮件客户端（由用户或管理员进行，可能根据组织的信息技术（IT）策略），以某些预定的时间间隔或者在一些预定时间发生时，使此请求指向该用户。在一些实施方式中，向移动设备 100 分配其自身的电子邮件地址，并在消息服务器 268 接收到专门寻址于移动设备 100 的消息时，将其自动重新定向到移动设备 100。

为了有利于移动设备 100 和 LAN 250 的组件之间的消息和消息相关数据的无线通信，可以设置多个无线通信支持组件 270。例如，在此示例实施方式中，无线通信支持组件 270 包括消息管理服务器 272。消息管理服务器 272 专门用于提供对消息管理的支持，如电子邮件消息等将由移动设备处理的消息。通常，在消息仍被存储在消息服务器 268 上时，消息服务器 272 可以用于控制何时、是否以及如何将消息发送给移动设备 100。消息管理服务器 272 还有利于处理在移动设备 100 上构成的消息，该消息被发送到消息服务器 268，以便进行随后的传递。

例如，消息管理服务器 272 可以：针对新电子邮件消息，监视用户的“邮箱”（例如消息服务器 268 上、与用户帐户相关联的消息存储器）；将用户定义过滤器应用于新消息，以确定是否和如何将消息中继到用户的移动设备 100；压缩并加密新消息（例如，使用如数据加密标准（DES）或三重 DES 等加密技术），并通过共享网络基础结构 224 和无线网络 200 将其推入移动设备 100；以及接收在移动设备 100 上构成的消息（例如利用三重 DES 进行加密），解密并解压缩所构成的消息，如果需要，对所构成的消息重新格式化，从而使其看上去来自用户的计算机 262a，并将所构成的消息重新路由到消息服务器 268，以便进行传递。

消息管理服务器 272 可以定义（由管理员根据 IT 策略）和强化与要从和/或要由移动设备 100 发送和/或接收的消息相关联的特定属性或约束。可以包括移动设备 100 是否可以接收已加密和/或已签名消息、最小加密密钥尺寸、是否必须加密和/或签名输出消息、以及是否要向预定副本地址发送从移动设备 100 发送的全部安全消息的副本等。

消息管理服务器 272 也可以用于提供其他控制功能，例如，只将存储在消息服务器 268 上的特定消息信息或消息的预定部分（如“块”）推入移动设备 100。例如，当移动设备 100 最初从消息服务器 268 检索消息时，消息管理服务器 272 用于只将消息的第一部分推入移动设备 100，该部分具有预定尺寸（如 2KB）。然后，用户可以请求消息管理服务器 272 将更多的消息按照类似的尺寸传递给移动设备 100，可能直到最大预定消息尺寸。

因此，消息管理服务器 272 有利于更好地控制与移动设备 100 进行通信的数据类型和数据量，并有助于最小化带宽或其他资源的潜在浪费。

本领域普通技术人员应当理解的是不必将消息管理服务器 272 实现在 LAN 250 或其他网络中的分离物理服务器上。例如，可以将与消息管理服务器 272 相关联的一些或全部功能与消息服务器 268 或 LAN 250 中的一些其他服务器集成。此外，LAN 250 可以包括多个消息管理

服务器 272，尤其是在需要支持大量移动设备的变体实施方式中。

本发明的实施例大体上涉及对已编码消息的处理，如已加密和/或已签名的电子邮件消息。在简单邮件传送协议（SMTP）、RFC 822 报头和多用途因特网邮件扩展（MIME）体部分可以用于定义不需要编码的典型电子邮件消息的格式时，可以在通信已编码消息时（即在安全消息收发应用程序中），使用安全/MIME（S/MIME），MIME 协议的一种版本。S/MIME 实现了端到端验证和保密性，并且从消息的发起者发送消息的时刻开始直到消息接收方解码并使其可用为止，保护数据完整性和私密性。也可以采用其他已知的标准和协议，以有助于安全消息通信，如 Pretty Good Privacy™（PGP）、OpenPGP 或其他已知技术。

如 S/MIME 等安全消息收发协议依赖于公用和私用加密密钥来提供保密性和完整性，并依赖于公用密钥基础结构（PKI）来通信提供了验证和授权的信息。只能利用私用密钥/公用密钥对的公用密钥来解密利用该对的对应私用密钥进行了加密的数据，反之亦然。私用密钥信息永不公开，而公用密钥信息是共享的。

例如，如果发送方希望以加密形式向接收方发送消息，利用接收方的公用密钥来加密消息，之后将只能利用接收方的私用密钥进行解密。或者，在一些编码技术中，产生一次性的会话密钥，并用于加密消息体，典型地利用对称加密技术（如三重 DES 等）。然后，利用接收方的公用密钥对会话密钥进行加密（例如，利用如 RSA 等公用密钥加密算法），之后将只能利用接收方的私用密钥进行解密。然后，利用解密后的会话密钥来解密消息体。消息报头可以用于规定必须用于解密消息的特定解密方案。在变体实施方式中，可以使用基于公用密钥加密法的其他加密技术。但是，在每种情况下，只有接收方的私用密钥可以用于有利于消息的解密，并且按照这种方式，可以保持消息的保密性。

作为另一示例，发送方可以利用数字签名来签名消息。数字签名是利用发送方的私用密钥进行加密的消息的摘要（例如消息的散列信息），然后将其附加到输出消息上。为了在接收时验证消息的签名，

接收方使用与发送方相同的技术（例如，使用相同的标准散列算法），以获得接收消息的摘要。接收方还使用发送方的公用密钥来解密数字签名，以便获得什么是接收消息的匹配摘要。如果接收消息的摘要不匹配，这意味着在传送期间消息内容被改变和/或所述消息并非来自将其公用密钥用于验证的发送方。通过按照这种方式验证数字签名，可以保持发送方的验证和消息完整性。

可以加密、签名、既加密又签名已编码消息。利用证书来确保用在这些操作中的公用密钥的真实性。证书是由证书权威机构（CA）颁发的数字文档。证书用于验证用户及其公用密钥之间的关联性，实质上提供了用户公用密钥的真实性的可信程度。证书包含与证书持有者有关的信息，典型地根据已接受标准（如 X.509）来格式化证书内容。

考虑图 5，其中示出了示例证书链 300。颁发给“John Smith”的证书 310 是颁发给个人的证书的示例，可以将其称为终端实体证书。终端实体证书 310 典型地识别证书持有者（即此示例中的 John Smith）和证书的颁发者 314，并包括颁发者的数字签名 316 和证书持有者的公用密钥 318。证书 310 还将典型地包括识别证书持有者的其他信息和属性（如电子邮件地址、组织名称、组织单位名称、地点等）。当个人构建要发送给接收方的消息时，通常将个人的证书 310 包括在消息内。

对于可信的公用密钥，其颁发组织必须是可信的。可以通过一系列相关证书来表示可信 CA 和用户的公用密钥之间的关系，也被称作证书链。可以跟踪证书链，以确定证书的有效性。

例如，在图 5 所示的示例证书链 300 中，声称由 John Smith 发送的消息的接收方可能希望验证附属于接收消息的证书 310 的可信状态。例如，为了在接收方计算设备（例如图 4 的计算机 262a）上验证证书 310 的可信状态，获得颁发者 ABC 的证书 320，并用于验证证书 310 确实是由颁发者 ABC 签名的。证书 320 可能已经被存储在计算设备上的证书存储器中，或者可能需要从证书源（例如图 4 的 LDAP 服务器 284 或一些其他公用或专用 LDAP 服务器）获得。如果证书 320 已经被存储在接收方的计算设备中，则接收方将该证书指定为可信的，并

认为证书 310 是可信的，因为其链接到已存储的可信证书上。

但是，在图 5 所示的示例中，还需要证书 330 来验证证书 310 的可信度。证书 330 是自签名的，并被称作“根证书”。因此，可以将证书 320 称为证书链 300 中的“中间证书”；假设可以针对特定的终端实体证书确定到达根证书的链，到达根证书的任意给定证书链可以包含零个、一个或多个中间证书。如果证书 330 是由可信源（来自较大的证书权威机构，如 Verisign 或 Entrust）颁发的根证书，则可以认为证书 310 是可信的，因为其链接到可信证书。这意味着消息的发送方和接收方都信任根证书 330 的源。如果证书不能链接到可信证书，则认为证书是“不可信的”。

证书服务器存储与证书有关的信息和用于识别已经被调用的证书的列表。可以访问这些证书服务器，以获得证书，并验证证书真实性和撤消状态。例如，轻载目录访问协议（LDAP）服务器可以用于获得证书，以及在线证书状态协议（OCSP）服务器可以用于验证证书撤消状态。

标准电子邮件安全协议典型地有利于非移动计算设备（如图 4 所示的计算机 262a、262b；远程桌面设备）之间的安全消息传输。再次参照图 4，为了能够从移动设备 100 读取从发送方接收到的已签名消息以及要发送到这些发送方的已加密消息，移动设备 100 用于存储证书和其他个体的关联公用密钥。例如，存储在用户的计算机 262a 上的证书通常是从计算机 262a 通过底座 264 下载到移动设备 100 上的。

存储在计算机 262a 上并被下载到移动设备 100 上的证书并不局限于与个人相关的证书，还可以包括如由 CA 颁发的证书等。存储在计算机 262a 和移动设备 100 上的特定证书也可以被用户明确地指定为“可信的”。因此，当用户在移动设备 100 上接收到证书时，其可以通过将所述证书与存储在移动设备 100 上并被指定为可信的证书或者被确定为链接到可信证书的证书进行匹配，在移动设备 100 上进行验证。

移动设备 100 还可以用于存储与用户相关联的公用密钥/私用密钥对的私用密钥，从而移动设备 100 的用户可以签名在移动设备 100

上构成的输出消息，并解密以用户的公用密钥加密的、发送到用户的消息。例如，私用密钥可以从用户的计算机 262a 通过底座 264 下载到移动设备 100 上。优选地，在计算机 262a 和移动设备 100 之间交换私用密钥，从而使用户可以共享用于访问消息的一个身份和一种方法。

用户计算机 262a、262b 可以获得来自多个源的证书，以便存储在计算机 262a、262b 和/或移动设备（如移动设备 100）上。例如，这些证书源可以是私用的（例如，专用于组织内部的用户）或公用的，可以位于本地或远程，并且可以从组织的专用网络内部或通过因特网进行访问。在图 4 所示的示例中，与所述组织相关联的多个 PKI 服务器 280 位于 LAN 250 上。PKI 服务器 280 包括用于颁发证书的 CA 服务器 282、用于搜索和下载证书（例如，针对组织内部的个人）的 LDAP 服务器 284、和用于验证证书的撤消状态的 OCSP 服务器 286。

例如，用户计算机 262a 可以从 LDAP 服务器 284 中检索证书，以便通过底座 264 下载到移动设备 100。但是，在变体实施方式中，移动设备 100 也可以直接访问 LDAP 服务器 284（即，在这种情况下，“在空中”），以及移动设备 100 可以通过移动数据服务器 288 搜索并获得个人证书。类似地，移动数据服务器 288 可以用于允许移动设备 100 直接查询 OCSP 服务器 286，以验证证书的撤消状态。

本领域普通技术人员应当理解的是移动数据服务器 288 不必物理上位于与 LAN 250 的其他组件分离的计算设备上，在变体实施方式中，可以将移动数据服务器 288 设置在与 LAN 250 的另一组件相同的计算设备上。此外，在变体实施方式中，可以将移动数据服务器 288 的功能与 LAN 250 中的另一组件（如消息管理服务器 272）的功能进行集成。

在变体实施方式中，只允许选定的 PKI 服务器 280 访问移动设备（例如，只允许从用户的计算机 262a、262b 下载证书，同时允许从移动设备 100 检查证书的撤消状态）。

在变体实施方式中，例如，只允许特定的 PKI 服务器 280 访问登记给特定用户的移动设备，由 IT 管理员规定，并可能根据 IT 策略来规定。

例如，其他证书源[未示出]可以包括 Windows 证书源、位于 LAN 250 上或之外的另一安全证书存储器、以及智能卡等。

现在参照图 6，将示出了可以由消息服务器（例如图 4 的消息服务器 268）接收的已编码消息示例的组件的方框图总体表示为 350。已编码消息 350 典型地包括以下的一个或多个部分：报头部分 352、已编码体部分 354、可选的一个或多个已编码附件 356、一个或多个加密会话密钥 358、以及签名和签名相关信息 360。例如，报头部分 352 典型地包括地址信息，如“到”、“来自”和“抄送”地址等，也可以包括消息长度指示符以及发送方加密和签名方案标识符等。实际消息内容通常包括消息体或数据部分 354 和可能的一个或多个附件 356，可以由发送方利用会话密钥进行加密。如果使用了会话密钥，利用每个接收方的相应公用密钥，针对每个预期的接收方，对会话密钥进行加密，并且包括在消息 358 中。如果签名消息，则还包括签名和签名相关信息 360。例如，这可以包括发送方的证书。

图 6 所示的已编码消息的格式只是作为示例，本领域普通技术人员应当理解本发明的实施例可以应用于其他形式的已编码消息。根据所使用的特定消息收发方案，已编码消息的组件可以表现出与图 6 所示不同的次序，并且已编码消息可以包括更少、更多或不同的组件，可以依赖于是否对已编码消息进行了加密、签名或这二种操作。

本发明的实施例大体上涉及一种用于搜索和获得证书的系统和方法。在一个实施例中，对驻留在移动设备上并在移动设备（例如，图 4 所示的移动设备 100）上执行的证书搜索应用程序进行编程，以便在一个或多个证书服务器（例如，图 4 所示的 LDAP 服务器 284）上发起证书搜索。在此实施例中，移动设备通过中间计算设备（例如，图 4 所示的移动数据服务器 288）从证书服务器中搜索并获得证书。

参考图 4，考虑其中移动设备 100 上的证书搜索应用程序通过移动数据服务器 288 从 LDAP 服务器 284 中搜索并获得个人证书的示例实施方式。证书搜索应用程序接收搜索请求，典型地从用户处接收，用户提供了用户想要定位证书的个人的名、姓和电子邮件地址。也可以更为广泛地进行特定的搜索请求，例如，通过构成只输入姓名的较少

字母将返回以包含这些字母作为前缀的姓名颁发的全部证书的搜索查询，或者通过在输入字段中使用通配符或空白条目来扩展搜索。然后，将搜索请求从移动设备 100 通信到移动数据服务器 288，然后，移动数据 288 针对所请求的证书查询 LDAP 服务器 284。在此示例实施方式中，由移动数据服务器 288 获得已定位证书，并将与每个所获得的证书有关的特定搜索结果数据（如向其颁发了相应证书的个人（或实体）的通用名称和电子邮件地址）通信到移动设备 100，从而可以根据搜索结果产生列表，并将其显示给用户。然后，用户可以从所述列表中选择特定的证书进行下载并存储到移动设备 100 上。然后，将所述选择通信给移动数据服务器 288，根据该选择，将选定的证书下载到移动设备 100 上。

当移动设备 100 的用户从发送方接收到已签名消息时，需要发送方的证书，以便验证消息的完整性，并验证发送方的身份。在本说明书和权利要求中，还将此证书称作“发送方证书”或“发送方的证书”。考虑之间接收消息的一部分下载到移动设备 100 上以使用户通过在移动设备 100 上执行并驻留在移动设备 100 上的消息收发应用程序进行查看的情形。所述接收消息的一部分可能包括报头信息（例如，图 6 所示的报头 352），典型地从所述报头信息中至少能够获得发送方的电子邮件地址。但是，移动设备 100 所接收的所述消息部分可能不包括发送方的证书和能够用于识别所需证书的标识，由于这些签名相关信息典型地被附加在消息的末尾附近（例如参见图 6 所示的签名和签名相关信息）。

可以激活移动设备 100 上的证书搜索应用程序（例如，用户选择在查看消息时可访问的适当菜单选项），来下载发送方的证书。由于可以从下载报头信息中获得发送方的电子邮件地址，证书搜索应用程序可以通过移动数据服务器 288、在一个或多个证书服务器（如 LDAP 服务器 284 等）上、自动发起针对具有匹配电子邮件地址的证书的搜索。具体地，在消息并未伴随有发送方的证书的情况下，需要证书搜索应用程序从证书服务器获得证书。

但是，可能会通过搜索定位与所规定的电子邮件地址匹配的多个

证书。在现有系统中，如果未将包含用于正确识别与该消息相关的所需证书的必要信息的消息部分下载到移动设备 100 上，则用户不能肯定地从用于识别在搜索中定位的多个证书的列表中选择正确的证书。于是，用户将不得不猜测正确的证书，或者下载全部已定位证书，存储在移动设备上，将消耗时间和带宽。在从消息中获得除电子邮件以外的其他数据并将其用于进行证书搜索时，可能会产生类似的问题。

因此，本发明的实施例大体上涉及能够有助于从在一个或多个证书服务器的搜索中所定位的多个证书中确定与消息相关的证书的方法，即使是在未将消息完整地下载到用户计算设备（例如移动设备）的情况下。

参照图 7A，将示出了本发明一个实施例中的用于搜索和获得证书的方法的步骤的流程图总体表示为 400。

在步骤 410，在消息服务器（例如如图 4 所示的消息服务器 268）处接收到寻址于移动设备（例如如图 4 所示的移动设备 100）的用户的消息。在一个示例实施方式中，消息管理器服务器（例如如图 4 所示的消息管理服务器 272）将存储在消息服务器上的接收消息的第一部分推入移动设备。消息管理服务器可以根据用户的请求传递接收消息的其他部分，可能到最大的预定消息尺寸。传递给移动设备的信息部分通常包括报头信息（例如如图 6 所示的报头 352），典型地设置在消息的开头。

在本发明的实施例中，消息管理服务器将证书标识数据添加到要传递的消息部分上（例如添加到消息的报头上）。如果证书伴随着所接收到的消息，则消息管理服务器可以处理证书，以产生证书标识数据。在一个实施例中，消息管理服务器应用散列算法，对证书的至少一部分进行散列运算。然后，将散列信息用作要添加到即将传递给移动设备的信息部分（例如报头）上的证书标识数据。在一个实施例中，对整个证书进行散列运算，以产生散列信息。但是，在变体实施例中，可以对证书的一个或多个特定部分或字段进行散列运算，以产生散列信息，尽管根据散列部分或字段，散列信息惟一且正确地识别相同证书的可能性会有所降低。

在另一实施例中，消息管理服务器通过解析证书以识别证书的序列号和颁发者，处理伴随这接收消息的证书。然后，将此序列号和颁发者数据用作要添加到即将传递给移动设备的消息部分（例如报头）上的证书标识数据。

类似地，在发送方的证书并未伴随着接收消息的情况下，消息管理服务器可以解析消息中的签名相关信息，以获得用于识别与消息相关联的发送方证书的数据，如用于签名消息的证书的序列号和颁发者。然后，将此数据用作要添加到即将传递给移动设备的消息部分（例如报头）上的证书标识数据。

在一些应用中，与使用实际证书（可以参照图 5 对该证书进行确认）的散列信息相比，使用来自证书的序列号和颁发者数据作为证书标识数据可能不那么安全，因为序列号和颁发者数据更容易被遗忘。但是，根据所需的安全等级，使用任何一种证书标识数据在变体实施方式中都是有用的。

可以使用所产生的证书标识数据来惟一地识别与接收消息相关联的发送方证书。在未将接收消息的实际签名和签名相关信息（例如，图 6 所示的签名和签名相关信息 360）传递到移动设备时，这样做尤为有用。

在步骤 420，驻留在移动设备上并在移动设备上执行的消息收发应用程序从消息管理服务器接收所述接收消息的一个或多个部分，包括证书标识数据。可以响应用户的请求，从消息管理服务器获得接收消息的额外部分。

可选地，在步骤 430，消息收发应用程序可以使用从消息管理服务器接收到的证书标识数据，在移动设备的一个或多个指定证书存储器中，确定与接收消息相关联的证书是否已经被存储在移动设备上。可以将证书是否已经被存储的相应指示提供给正在显示的消息部分，或者例如，显示在用于在由用户接收到的消息列表中识别消息的条目侧面。

例如，在证书识别数据包括散列信息的实施例中，在步骤 430，消息收发应用程序针对存储在移动设备上、一个或多个指定证书存储

器中的每个证书，产生散列信息，并将每个所产生的散列信息与作为证书标识数据提供的散列信息进行比较，以便确定所述证书是否已经被存储在移动设备上。将与步骤 410 所采用的相同的散列算法应用于此步骤（如果未对整个证书进行散列运算，则将散列算法应用于已存储证书的相同部分或字段），以产生已存储证书的散列信息。因此，如果给定已存储证书的所产生的散列信息与从消息管理服务器接收到的散列信息匹配，则认为已经确定了匹配。

或者，在证书标识数据包括序列号和颁发者数据的实施例，在步骤 430，消息收发应用程序将与存储在移动设备上、一个或多个指定证书存储器中的每个证书相关联的序列号和颁发者数据与作为证书标识数据提供的序列号和颁发者数据进行比较，以便确定所述证书是否已经被存储在移动设备上。

在变体实施方式中，可以由除消息收发应用程序以外的其他驻留在移动设备上并在移动设备上执行的应用程序（如证书搜索应用程序等）执行步骤 430。

在步骤 440，驻留在移动设备上并在移动设备上执行的证书搜索应用程序做出对证书的搜索请求。例如，搜索请求可以由用户发起，其选择由消息收发应用程序提供的菜单选项，以激活证书搜索应用程序。或者，消息收发应用程序或移动设备上的一些其他应用程序可以自动的激活证书搜索应用程序，例如，在接收到消息时，以及可能在步骤 430 处确定证书未被存储在移动设备上之后。

在一个示例实施方式中，在步骤 440 请求证书搜索时，证书搜索应用程序将搜索请求通过移动数据服务器（例如图 4 所示的移动数据服务器 288）传送给至少一个证书服务器（例如图 4 所示的 LDAP 服务器 284）。搜索请求包括以下数据，典型地包括电子邮件地址、以及可能的至少一个与接收消息的发送方相关联的姓名。但是，本领域普通技术人员应当理解的是，可以构建多种搜索查询，而不偏离本发明的范围。

在步骤 450，移动数据服务器针对满足移动设备的证书搜索应用程序在步骤 440 做出的搜索请求的证书，查询至少一个证书服务器。

移动数据服务器从至少一个证书服务器获得作为搜索查询的结果而定位的证书。

在步骤 460, 将已定位证书从移动数据服务器下载到移动设备上。典型地, 将所下载的证书暂时存储在移动设备上, 以便进行进一步的处理。

在步骤 470, 证书搜索应用程序对在步骤 460 下载到移动设备的已定位证书进行处理, 以确定哪一个已定位证书匹配由伴随接收消息的证书标识数据识别的、与接收消息相关联的证书。

在证书标识数据包括散列信息的实施例, 证书搜索应用程序产生针对每个已定位证书的散列信息, 并将每个所产生的散列信息与作为证书标识数据提供的散列信息进行比较, 以便确定适当的匹配。将与步骤 410 所采用的相同的散列算法应用于此步骤 (如果未对整个证书进行散列运算, 则将散列算法应用于已存储证书的相同部分或字段), 以产生已存储证书的散列信息。因此, 如果给定已存储证书的所产生的散列信息与从消息管理服务器接收到的散列信息匹配, 则认为已经确定了匹配。

或者, 在证书标识数据包括序列号和颁发者数据的实施例, 证书搜索应用程序将与每个已定位证书相关联的序列号和颁发者数据与作为证书标识数据提供的序列号和颁发者数据进行比较, 以便确定适当的匹配。

可选地, 在步骤 480, 可以向用户显示在步骤 460 下载的用于识别已定位证书的列表, 使用指示符或其他突出显示技术来识别此列表中的匹配证书。然后, 可以提示用户选择匹配证书 (以及可能的其他已定位证书) 存储在移动设备上的证书存储器中, 以便稍后使用。

在步骤 490, 将匹配证书存储在移动设备上的证书存储器中。在一个实施例中, 证书搜索应用程序可以自动地执行此步骤, 而不在步骤 480 提示用户进行选择。

例如, 在变体实施例中, 还可以使匹配证书生效 [未示出该步骤], 以便在存储前后, 验证其可信状态。

现在参照图 7B, 将示出了本发明另一实施例中的用于搜索和获得

证书的方法的步骤的流程图总体表示为 400b。方法 400b 类似于方法 400,除了证书搜索应用程序可以将证书标识数据传递给移动数据服务器(例如,与搜索请求一起)以外,从而移动数据服务器只将匹配证书返回给移动设备,而不是将搜索中定位的全部证书。

具体地,在本发明的这个实施例中,在步骤 440,将最初在移动设备处从消息管理服务器接收到的证书标识数据与搜索请求一起转发给移动数据服务器。

在步骤 460b,移动数据服务器处理已定位证书,以确定哪一个已定位证书匹配由在步骤 440、在移动数据服务器处、从移动设备接收到的证书标识数据识别的、与接收消息相关联的证书。然后,在此步骤,只将匹配证书下载到移动设备上,以便随后在步骤 490 存储在移动设备上的证书存储器中。可以在存储之前,提示用户允许保存匹配证书[未示出此步骤]。

与图 7B 所示的其余步骤有关的详细描述参照图 7A。

在本发明的变体实施例中,可以将用于惟一识别证书的其他数据用作证书标识数据。

在本发明的变体实施例中,可以从一个或多个证书服务器获得已定位证书,并将其下载到移动设备,而无需通过移动数据服务器或其他中间计算设备进行传输。

上面已经参照移动设备对本发明的实施例进行了描述。但是,一些实施例也可以应用于除移动设备以外适合接收已编码消息的其他设备。

本发明实施例中用于搜索和获得证书的方法的步骤可以作为存储在计算机可读介质上的可执行软件指令来提供,所述计算机可读介质包括传输型介质。

已经针对多个实施例对本发明进行了描述。但是,本领域普通技术人员应当理解的是,在不偏离由所附权利要求所限定的本发明的范围的前提下,可以进行多种变化和修改。

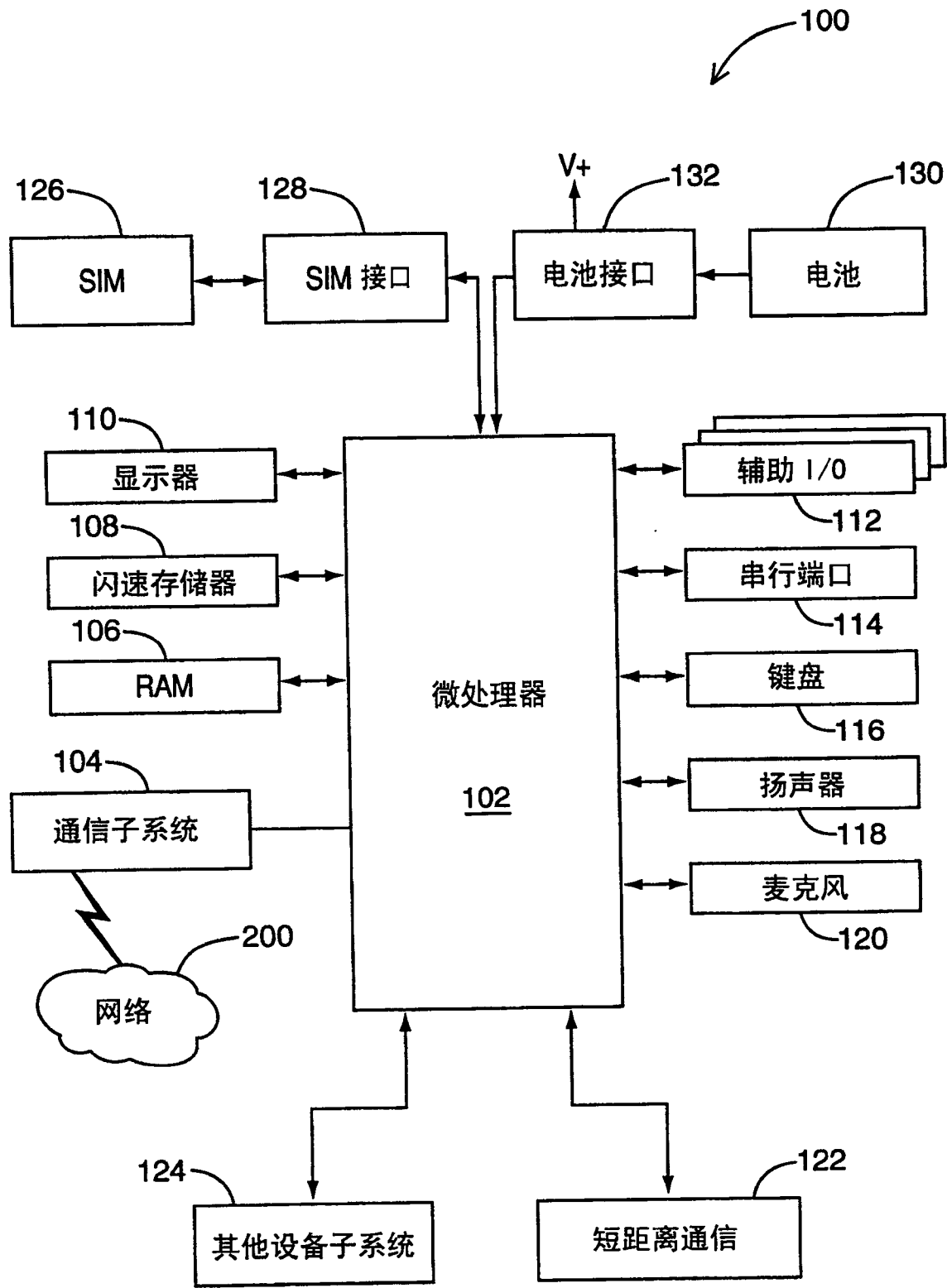


图 1

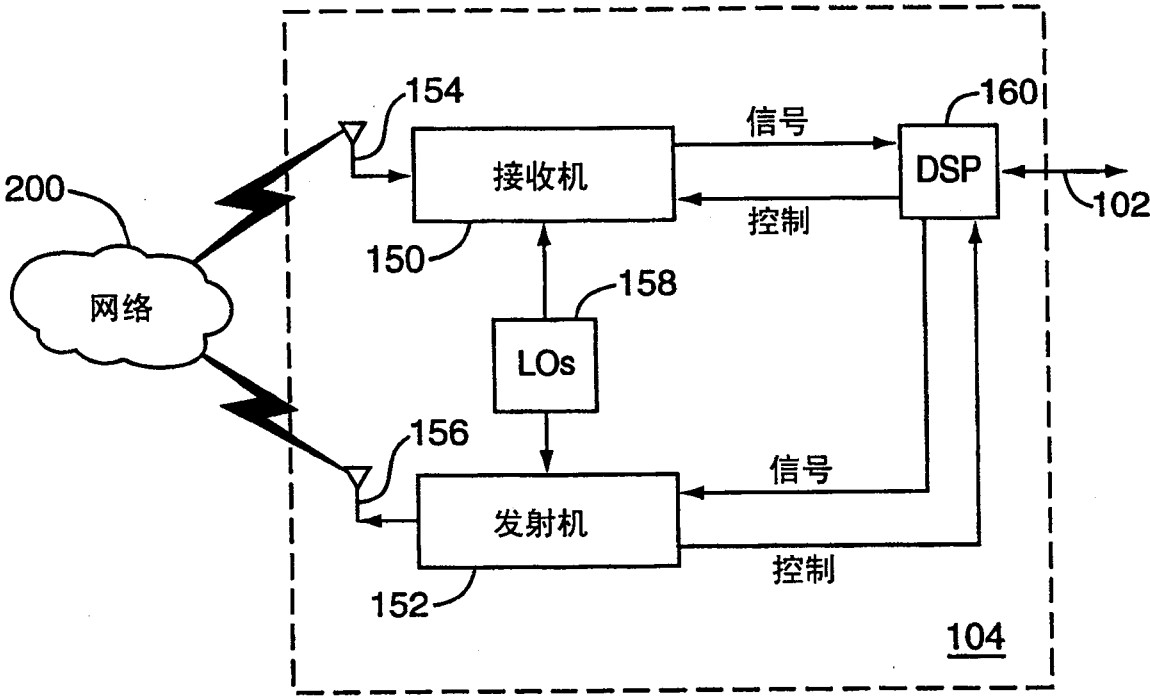


图 2

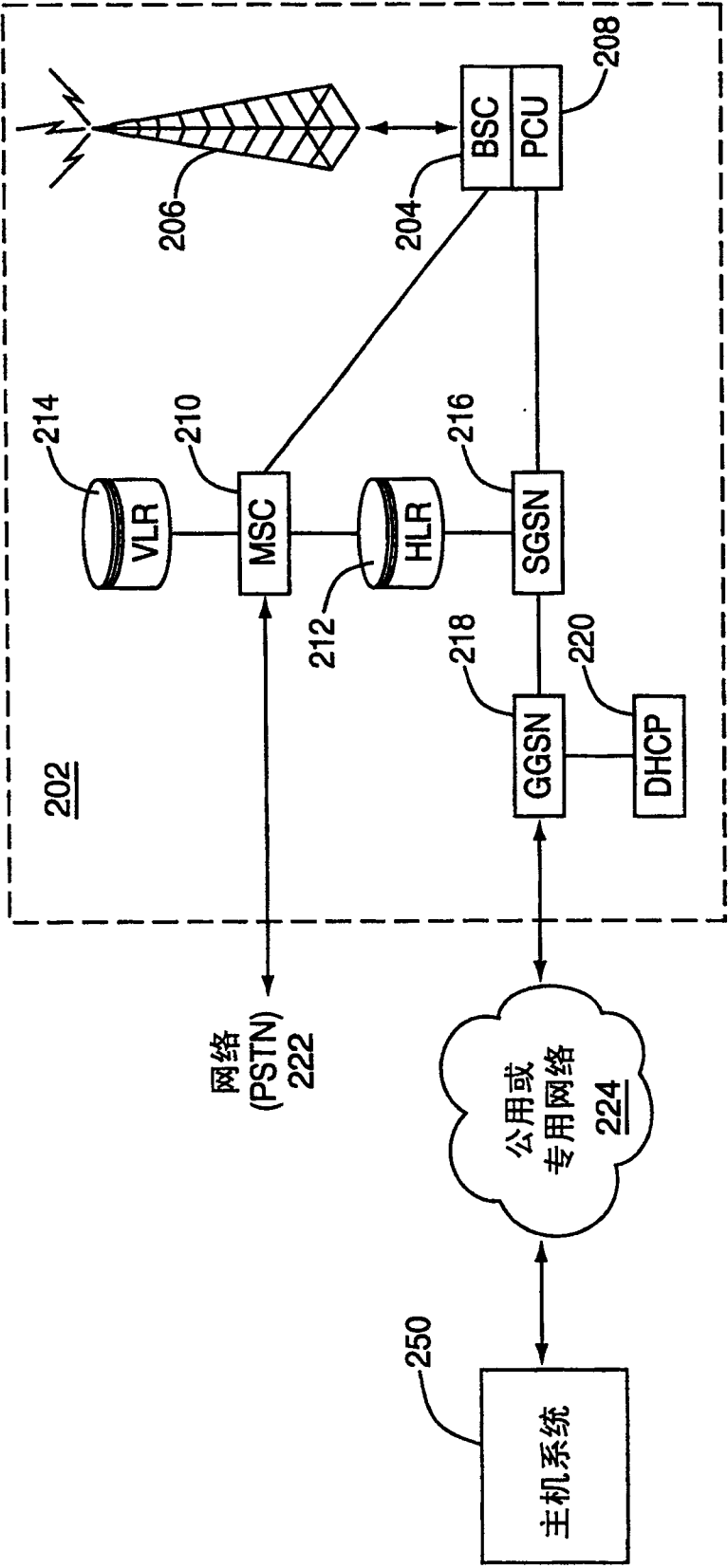


图 3

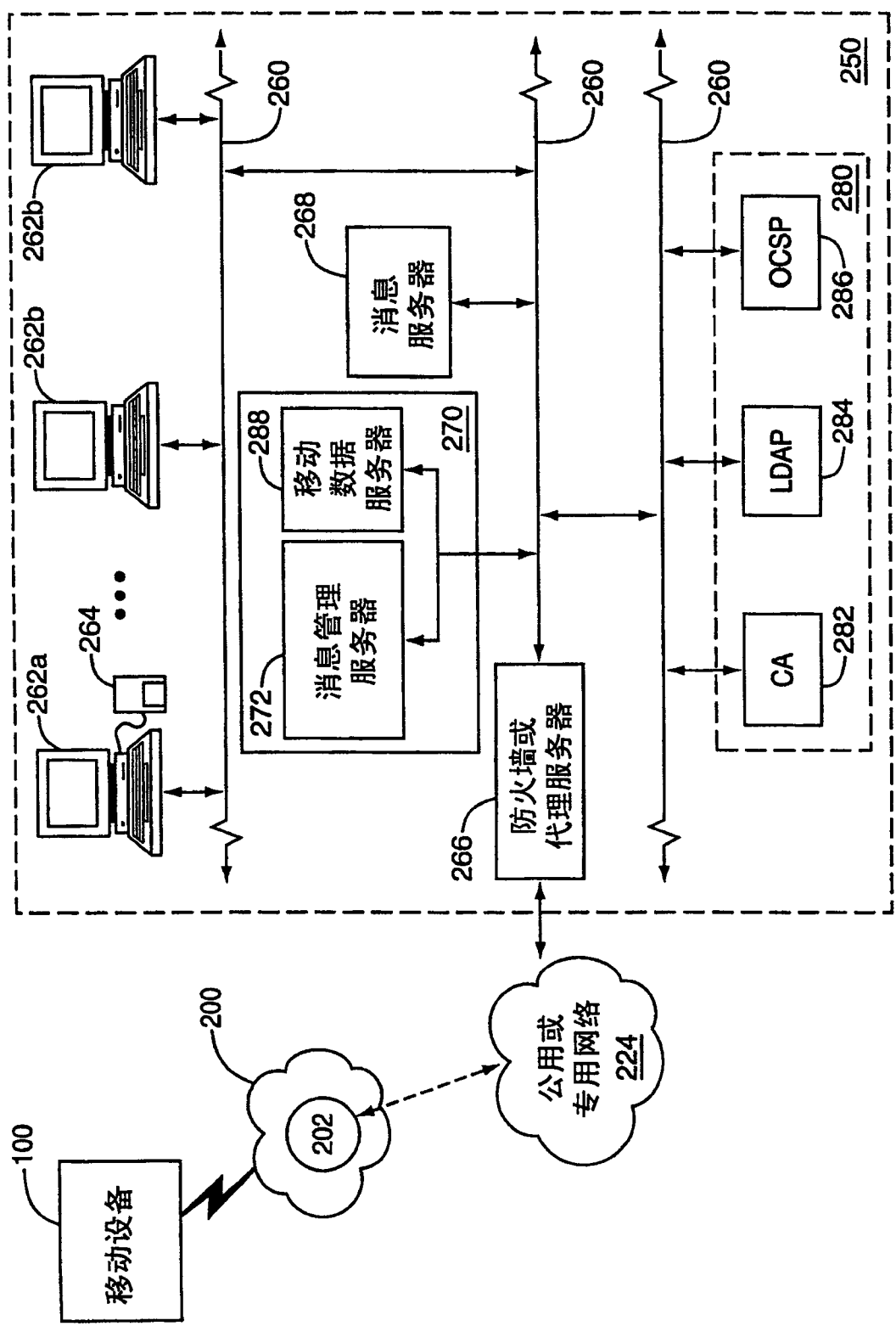


图 4

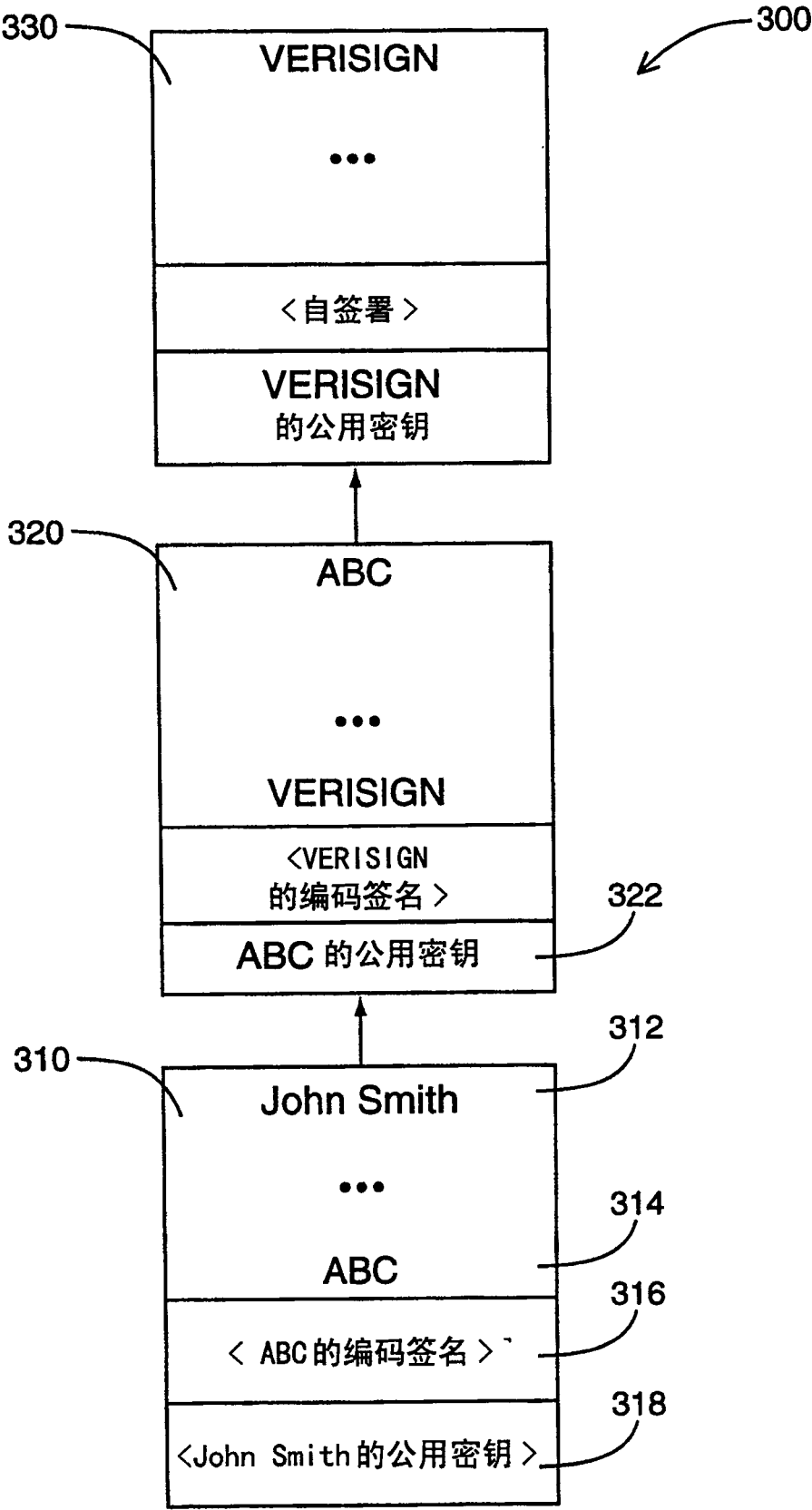


图 5

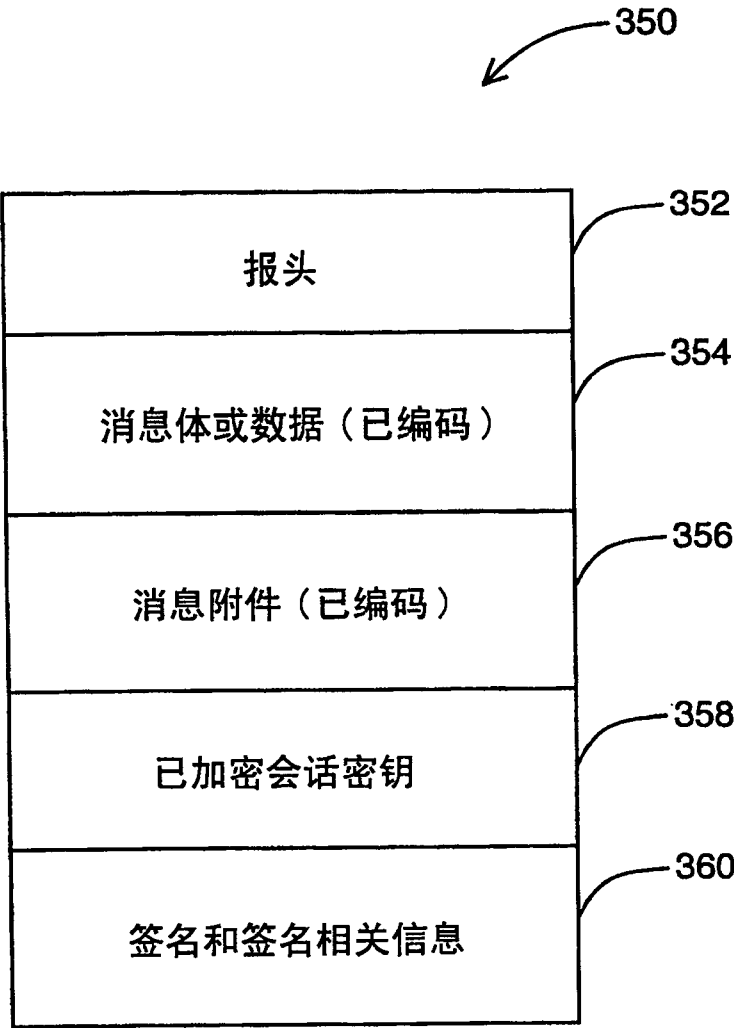


图 6

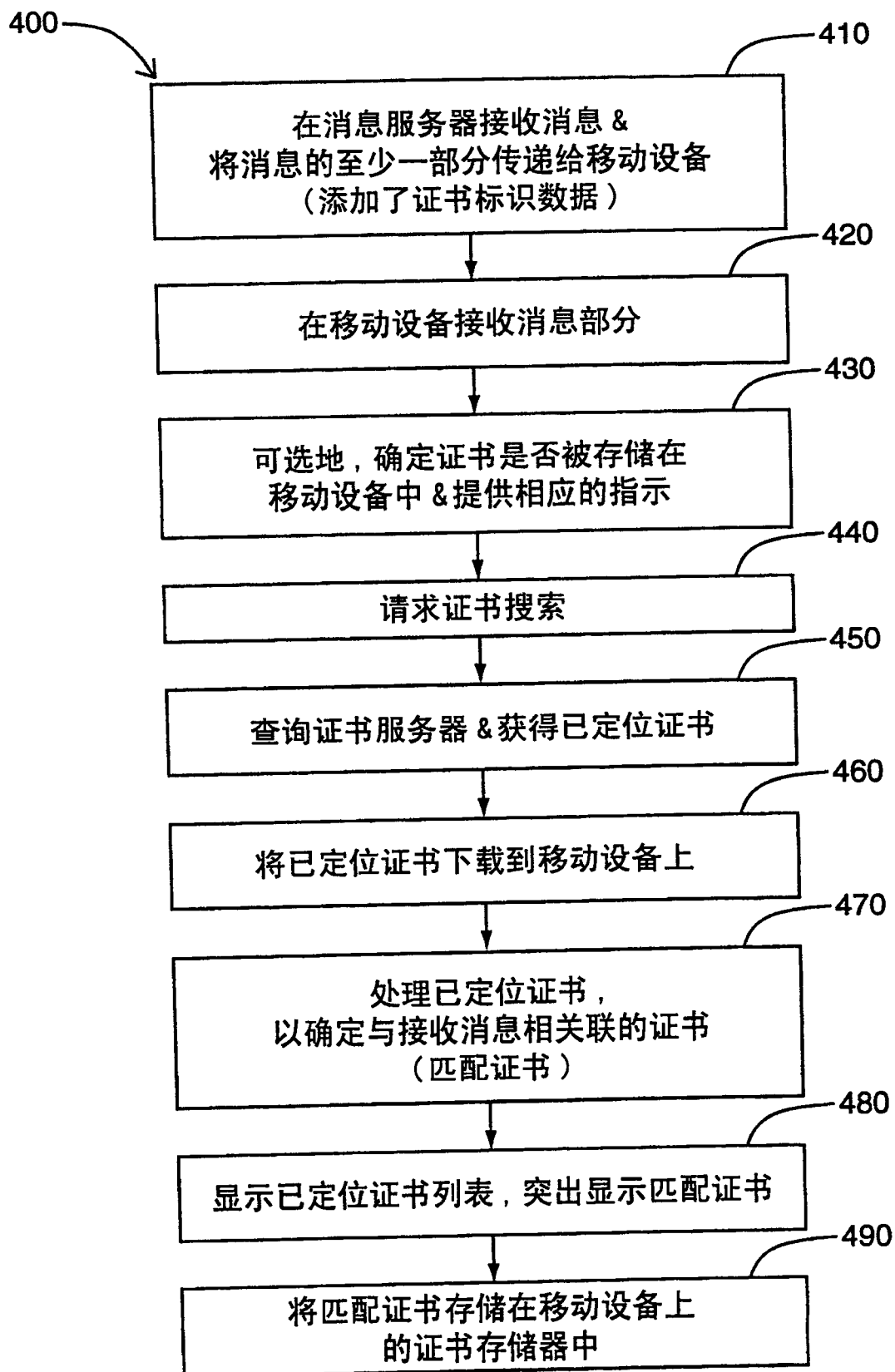


图 7A

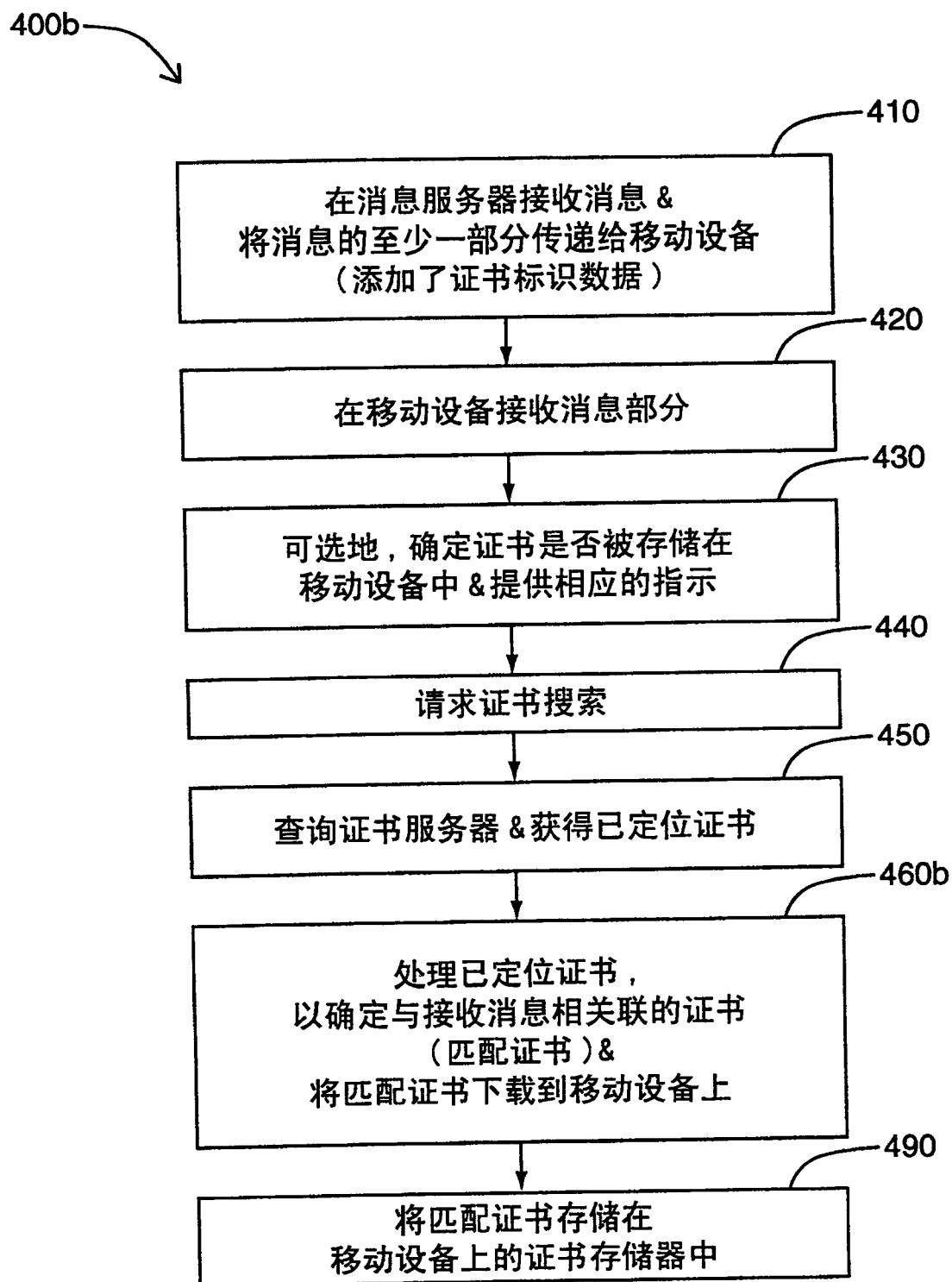


图 7B