(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 1672380 B
(45)授权公告日 2010.08.18

(21)申请号 03810928.X

(22)申请日 2003.03.20

(30)优先权数据
60/365,518 2002.03.20 US

(85)PCT申请进入国家阶段日
2004.11.15

(86)PCT申请的申请数据
PCT/CA2003/000403 2003.03.20

(87)PCT申请的公布数据
WO03/079626 EN 2003.09.25

(73)专利权人 捷讯研究有限公司
地址 加拿大安大略省沃特卢市

(72)发明人 赫伯特·A·利特尔
斯蒂芬·E·扬胡宁

(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 王玮

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)

(56)对比文件

US 2002/0184182 A1,2002.12.05, 图2,5,6A,6B、第2栏第61-65行,第3栏第5-15,45-49行,第8栏第24-34行.

EP 0942568 A2,1999.09.15, 全文.

EP 0869636 A2,1998.10.07, 图6,8、第9栏第4行至第10栏第29行,第10栏第37-55行.

CN 1202288 A,1998.12.16, 全文.

US 6219694 B1,2001.04.17, 全文.

US 2001/0002485 A1,2001.05.31, 图1A,图3A.

M. Myers.X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP.1-23.

审查员 王海荣

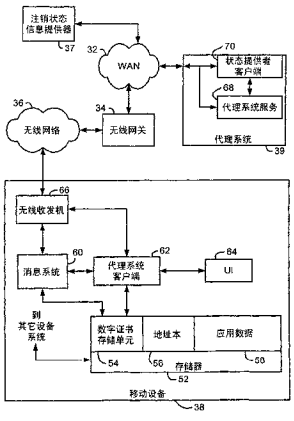
权利要求书 2 页 说明书 25 页 附图 11 页

(54)发明名称

用于检验数字证书状态的系统和方法

(57)摘要

提供了一种用于处理数字证书状态检验的方法和系统。在代理系统处,接收从客户端系统传送的数字证书状态请求数据。代理系统响应于数字证书状态请求数据的接收,产生针对数字证书状态的查询数据。将所述查询数据传送到状态提供器系统,并且在代理系统处,接收响应于查询数据来自状态提供器系统的状态数据。基于接收的状态数据的数字证书状态数据由代理系统产生并且传送到客户端系统。



CN 1672380 B

1. 一种根据存储在状态提供器系统中的状态数据来确定数字证书的状态的系统，包括：

客户端系统，包括客户端模块，该客户端模块配置用于产生和提供与针对数字证书的状态请求相对应的状态请求数据，用于从客户端系统发送，并且响应针对数字证书的状态请求，接收针对数字证书的数字证书状态数据；和

代理系统，包括代理模块，该代理模块配置用于接收从所述客户端系统传送的状态请求数据，并且对此进行响应，产生针对数字证书状态的查询数据，并且提供所述查询数据，用于按照状态提供器系统与代理系统之间的第一通信协议，从代理系统传送到状态提供器系统，以及还配置用于从所述状态提供器系统接收状态数据，根据接收的状态数据来产生所述数字证书状态数据，并且提供所述数字证书状态数据，用于按照客户端系统与代理系统之间的第二通信协议，传送到客户端系统。

2. 如权利要求 1 所述的系统，其特征在于所述客户端系统包括一个移动设备，该移动设备包括存储器子系统并且所述移动设备配置用于经无线网络与代理系统通信，经无线网络接收数据项，和在所述存储器子系统中存储所述数据项。

3. 如权利要求 2 所述的系统，其特征在于，所述数字证书状态数据包括从所述状态提供器系统接收的状态数据的子集。

4. 如权利要求 3 所述的系统，其特征在于，所述状态请求数据包括所述查询数据的子集。

5. 如权利要求 4 所述的系统，其特征在于，所述查询数据包括与在线证书状态协议查询相关的数据。

6. 如权利要求 2 所述的系统，其特征在于，从所述代理系统发送的所述数字证书状态数据包括：有效指示符、注销指示符、和未知指示符。

7. 如权利要求 2 所述的系统，其特征在于，所述数字证书状态数据包括指示数字证书的有效期的有效期数据，并且所述客户端模块进一步配置用于在数字证书的有效期内，周期性地产生和提供与状态请求相对应的状态请求数据，用于传送到代理系统。

8. 如权利要求 2 所述的系统，其特征在于，所述代理系统配置用于将数据项重定向到移动设备，并且所述代理模块进一步配置用于确定所述数据项是否包括数字证书，一旦确定所述数据项包括所述数字证书，产生和提供与针对数字证书的状态请求相对应的状态请求数据，用于传送到状态提供器系统，和响应针对数字证书的状态请求，接收针对数字证书的数字证书状态数据。

9. 如权利要求 3 所述的系统，其特征在于，所述数字证书包括数字证书的数字证书链，并且所述状态请求数据包括与所述数字证书链中的每个数字证书相对应的数据。

10. 一种处理客户端系统和代理系统之间的数字证书状态请求的方法，该方法包括步骤：

在所述代理系统，接收从所述客户端系统传送来的数字证书状态请求数据；

在所述代理系统处，响应所述数字证书状态请求数据的接收，产生针对所述数字证书状态的查询数据；

按照状态提供器系统与代理系统之间的第一通信协议，将所述查询数据从所述代理系统传送到状态提供器系统；

响应所述查询数据，在所述代理系统，从所述状态提供器系统接收状态数据；

在代理系统处，根据接收的所述状态数据，产生数字证书状态数据；和

按照客户端系统与代理系统之间的第二通信协议，将所述数字证书状态数据从所述代理系统传送到所述客户端系统。

11. 如权利要求 10 所述的方法，其特征在于，所述数字证书状态数据是从所述状态提供器接收的状态数据的子集。

12. 如权利要求 10 所述的方法，其特征在于，所述数字证书状态请求数据包括所述查询数据的子集。

13. 如权利要求 12 所述的方法，其特征在于，针对所述数字证书状态的所述查询数据包括与在线证书状态协议查询数据相关的数据。

用于检验数字证书状态的系统和方法

[0001] 本申请要求2002年3月20号提交的美国临时专利申请序列号为:60/365,518的权益,其全部公开通过引用包含于此。

技术领域

[0002] 本发明一般地涉及安全电子消息传送领域,并且特别涉及检验数字证书的状态。

背景技术

[0003] 包括例如运行在桌面计算机系统上的电子邮件软件应用的已知安全消息客户端保持数据存储器,或至少一个专用的数据存储区用于安全消息信息,诸如数字证书。数字证书通常包括一个实体的公钥及用一个或多个数字签名捆绑到公钥的标识信息。在安全多用途因特网邮件扩展(S/MIME)消息传送中,例如,使用公钥验证所接收的安全消息上的数字签名,并且加密用于加密要发送的消息的会话密钥。在其它安全消息方案中,可以使用公钥加密数据或消息。如果公钥当需要用于加密或数字签名验证时而在消息客户端中得不到时,那么在能够执行这些操作之前,数字证书被加载到消息客户端上。

[0004] 通常,针对证书注销表(CRL)检验数字证书,以确定是否数字证书已经被其发行者注销。当数字证书首先被接收到时,并且之后周期地,例如当接收到新CRL时,通常执行该检验。然而,CRL趋于相对庞大,这样CRL传送到消息客户端消耗相当大的通信资源,并且在消息客户端处的CRL的存储可能消耗有效的存储器空间。基于CRL的注销状态检验也是处理器集中式的和费时的。这些影响在运行于无线移动通信设备上的消息客户端中特别明显,这些消息客户端运行在有限带宽的无限通信网络内,并且可能具有有限的处理和存储器资源。此外,只有当分发新CRL时,在基于CRL的系统中更新注销状态。

[0005] 用于数字证书注销状态检验的另一方案涉及查询保持数字证书注销状态信息的远端系统。这种类型的方案需要传送较少的信息,减少了在消息客户端处执行的操作的复杂性,以检验数字证书的注销状态,并且还提供了与基于CRL方案有关更及时的数字证书注销状态信息。在线证书状态协议(OCSP)是这种方案的一个示例。然而,无线通信系统带宽限制和等待时间使得这些已知方案不适合于运行在无线移动通信设备上的安全消息客户端。

发明内容

[0006] 按照本发明的一个方面,一种根据存储在状态提供器系统中的状态数据来确定数字证书的状态的系统,包括:客户端系统,包括客户端模块,该客户端模块可操作用于产生和提供对应于数字证书状态请求的状态请求数据用于从客户端系统传输,并且响应于该状态请求,接收用于数字证书的数字证书状态数据;和代理系统,包括代理模块,该代理模块可操作用于接收从所述客户端系统传送的状态请求数据,并且响应于此,产生用于所述数字证书状态的查询数据,和提供所述查询数据用于从代理系统传送到状态提供器系统,和进一步可操作用于从所述状态提供器系统接收状态数据,基于接收的状态数据产生所述数

字证书状态数据，和提供所述数字证书状态数据用于传送到客户端系统。

[0007] 按照本发明的另一方面，一种用于处理用于客户端系统的数字证书状态检验服务的系统，包括：代理系统，包括代理模块，可操作用于从客户端系统接收针对数字证书的第一数字证书状态检验服务请求数据，并且响应于此，产生第二数字证书状态检验服务请求数据和提供所述第二数字证书状态检验服务请求数据，用于传送到数字证书状态检验服务提供器系统，并且进一步可操作用于从所述数字证书状态检验服务提供器系统接收第一数字证书状态检验服务数据，基于接收的所述第一数字证书状态检验服务数据，产生第二数字证书状态检验服务数据，和提供所述第二数字证书状态检验服务数据，用于传送到客户端系统，其中，所述第二数字证书状态检验服务数据包括从所述服务提供器系统接收的第一数字证书状态检验服务数据的子集。

[0008] 在本发明的另一个实施例中，一种用于处理用于数字证书的数字证书状态检验服务的系统，所述数字证书状态检验服务由数字证书状态检验服务提供器系统提供，该系统可操作用于接收用于数字证书状态检验服务请求的查询数据，该系统包括：客户端系统，该客户端系统包括客户端模块，可操作用于准备并且提供传输对应于数字证书的数字证书状态检验服务的第一数字证书状态检验服务请求数据，和响应于第一数字证书状态检验服务请求数据，接收第一数字证书状态检验服务数据，其中，所述第一数字证书状态检验服务请求数据包括针对数字证书状态检验服务请求的查询数据的子集。

[0009] 按照本发明的另一方面，一种用于处理用于数字证书的数字证书状态检验服务的方法，所述数字证书状态检验服务由数字证书状态检验服务提供器系统提供，该系统可操作用于接收针对数字证书状态检验服务请求的查询数据，所述方法包括步骤：接收数据项，确定是否所述数据项包括数字证书，如果所述数据项包括数字证书，产生包括所述查询数据的子集的数字证书状态检验服务请求数据，提供所述数字证书状态检验服务请求数据，用于传送到代理系统，和响应于所述数字证书状态检验服务请求数据，从所述代理系统接收数字证书状态检验服务数据。

[0010] 在本发明的另一个实施例中，一种处理客户端系统和代理系统之间的数字证书状态请求的方法，该方法包括步骤：在所述代理系统接收从所述客户端系统传送的数字证书状态请求数据，响应于接收所述数字证书状态请求数据，产生针对所述数字证书状态的查询数据，传送所述查询数据到状态提供器系统，响应于所述查询数据，在所述代理系统从所述状态提供器系统接收状态数据，基于接收的所述状态数据，产生数字证书状态数据，和传送所述数字证书状态数据到所述客户端系统。

[0011] 在上述系统和方法中，按照状态提供器系统与代理系统之间的第一通信协议，将所述查询数据从所述代理系统传送到状态提供器系统；按照客户端系统与代理系统之间的第二通信协议，将所述数字证书状态数据从所述代理系统传送到所述客户端系统。

[0012] **附图说明**

[0013] 图 1 是一个示例消息系统的方框图。

[0014] 图 2 是图示在消息系统中的安全电子邮件消息交换的方框图。

[0015] 图 3 是实现数字证书注销状态检验系统的一个系统的方框图。

[0016] 图 4A 是图示检验数字证书注销状态的方法的流程图。

[0017] 图 4B 是图示检验数字证书注销状态的另一方法的流程图。

[0018] 图 5 是实现具有多代理系统客户端模块的数字证书注销状态检验系统的系统的方框图。

[0019] 图 6 是无线移动通信设备的方框图。

[0020] 图 7 是图示数字证书状态请求的处理的功能方框图。

[0021] 图 8 是展示一个通信系统的方框图。

[0022] 图 9 是可选的通信系统的方框图。

[0023] 图 10 是另一可选的通信系统的方框图。

具体实施方式

[0024] 安全消息是由消息发送器或者可能由消息发送器和消息接收器之间的中间系统已经进行处理的消息，以保证一个或多个数据保密性，数据整体性和用户验证。安全消息传送的通用技术包括利用数字签名对消息进行签名，和 / 或加密消息。例如，安全消息可以是按照诸如安全多用途因特网邮件扩展 (S/MIME) 的各种变体的已签名、加密、先加密然后签名或先签名然后加密的消息。

[0025] 消息客户端 (messaging client) 允许它在其上运行的一个系统接收并且可能也发送消息。消息客户端可以运行在计算机系统、手持设备、或带有通信能力的任何其它系统或设备上。很多消息客户端还具有附加的非消息传送功能。

[0026] 图 1 是一个示例消息系统的方框图。系统 10 包括 :广域网络 (WAN)12 ;其连接到计算机系统 14 ;无线网络网关 16 和公司局域网络 (LAN)18。无线网络网关 16 还连接到无线通信网络 20，其中，配置无线移动通信设备 22(“移动设备”) 以进行操作。

[0027] 一个示例的移动设备 22 可以是在美国专利 6,278,442，标题为“HAND-HELD ELECTRONIC DEVICE WITH A KEYBOARD OPTIMIZED FOR USEWITH THE THUMBS”中公开的类型，其全部公开通过引用被包含于此。计算机系统 14 是被配置用于对 WAN 12 进行通信的桌上型或膝上型 PC。WAN 12 可以是大的网络，诸如因特网。PC 诸如计算机系统 14 通常通过因特网服务提供商 (ISP)，应用服务提供商 (ASP) 等访问因特网。

[0028] 公司 LAN 18 图示为位于安全防火墙 24 的后面的基于网络的消息客户端的例子。在公司 LAN 18 内，运行在防火墙 24 后的计算机上的消息服务器 26，作为主要接口，用于公司在 LAN18 内交换信息、和通过 WAN12 与其它外部消息客户端交换消息。两个所知的最普通的消息服务器 26 是 Microsoft™ Exchange Server 和 Lotus Domino™。这些服务器通常与路由和传递邮件的因特网邮件路由器一起使用。消息服务器 26 还可以提供附加功能，诸如用于涉及日历、to-do 表、任务表、电子邮件和文档的数据的动态数据库存储。

[0029] 消息服务器 26 向连接到 LAN18 的联网计算机系统 28 提供消息传送能力。典型的 LAN18 包括多个计算机系统 28，每个均实现一消息客户端，诸如 Microsoft Outlook™，Lotus Notes™ 等。在 LAN 18 内，消息由消息服务器 26 接收，分布给在接收的消息中所寻址的用户帐户的合适信箱，然后通过运行在计算机系统 28 上的消息客户端而由用户访问。

[0030] 无线网关 16 给无线网络 20 提供接口，通过该接口，可与移动设备 22 交换消息。移动设备 22 例如可以包括 :数据通信设备、语音通信设备、双模式通信设备 (诸如具有数据和语音通信功能的移动电话)、能够用于无线通信的个人数字助理 (PDA)、或与膝上或桌面型计算机系统或某些其它设备一起工作的无线调制解调器。前面已经描述了一个示例的移动

设备 22，下面参照图 6 进一步描述。

[0031] 这些功能，诸如移动设备 22 的寻址、用于无线传输的消息的编码或其它转换和任何其它需要的接口功能，可以由无线网络网关 16 来执行。可以配置无线网关 16，以便与多于一个的无线网络 20 操作，在该情况下，无线网关 16 也可以确定用于定位给定的用户的最可能的网络，并且当用户在国家或网络之间漫游时，可跟踪其移动设备。

[0032] 任何访问 WAN 12 的计算机系统可以通过无线网络网关 16 与移动设备 22 交换消息。或者，也可以实现专有无线网络网关，诸如无线虚拟专有网络 (VPN) 路由器，以给无线网络提供专有接口。例如，在 LAN 18 中实现的无线 VPN 可以通过无线网络 20，提供从 LAN 18 到一个或多个无线移动设备诸如 22 的专有接口。通过提供与消息服务器 26 操作的消息转发或重定向系统，这种通过无线网络网关 16 和 / 或无线网络 20 到无线设备的专有接口被有效地扩展到 LAN 18 外部的实体。在该类型的系统中，由消息服务器 26 接收并且寻址到与移动设备诸如 22 的用户相关的一个信箱或数据存储器的输入消息通过无线网络接口，例如无线 VPN 路由器、无线网络网关 16 或其它接口，发送到无线网络 20 及到用户移动设备 22。在消息服务器 26 上运行的示例重定向器系统可以具有在美国专利 6,219,694 中公开的类型，该专利标题为“SYSTEM AND METHODFOR PUSHING INFORMATION FROM A HOST SYSTEM TO A MOBILE DATACOMMUNICATION DEVICE HAVING A SHARED ELECTRONIC ADDRESS”，其全部公开通过引用包含在此。

[0033] 到消息服务器 26 上的用户信箱的另一可选接口是无线应用协议 (WAP) 网关。通过 WAP 网关，可以将在消息服务器 26 上的用户信箱中的消息列表、或可能每个消息或每个消息的一部分发送到移动设备 22。

[0034] 无线网络通常通过无线网络中的基站和移动设备之间的 RF 传输，传递消息给移动设备或从移动设备传递消息。无线网络 20 例如可以是数据中心型无线网络、语音中心型无线网络、或通过相同的基础设施能够同时支持语音和数据通信的双模式网络。示出的无线网络包括 :码分多址 (CDMA) 网络，移动特别小组或全球移动通信系统 (GSM) 和通用分组无线业务 (GPRS)、以及诸如用于全球演进的增强型数据率 (EDGE) 和通用移动电信系统 (UMTS) 等第三代 (3G) 网络。GPRS 是在现有的 GSM 无线网络上的数据覆盖的数据中心型的。

[0035] 某些老的数据中心网络的例子，包括但不限于 :Mobitex™ 无线网络 (“Mobitex”)，和 DataTAC™ 无线网络 (“DataTAC”)。语音中心型数据网络的例子包括个人通信系统 (PCS) 网络，象 CDMA、GSM 和已经使用了多年的时分多址 (TDMA) 系统。

[0036] 也许当前使用的最普遍的消息是电子邮件。在标准的电子邮件系统中，电子邮件消息由电子邮件发送器发送，很可能通过消息服务器和 / 或服务提供者系统发送、并且典型地，经因特网路由到一个或多个消息接收器。电子邮件消息通常用明文发送，并且使用传统的简单邮件传递协议 (SMTP)、RFC822 报头和 MIME 主体部分，来定义电子邮件消息的格式。

[0037] 在近些年，安全消息技术已经得到发展，以保护消息诸如电子邮件消息的内容和完整性。S/MIME 和 Pretty Good Privacy™(PGp™) 是两个公钥安全电子邮件消息协议，用于加密和签名，从而保护消息的完整性，以及用于由消息接收器进行的发送器验证。安全消息除了被加密和 / 或签名之外，还可以被编码，压缩或另外处理。

[0038] 图 2 是图示在消息传送系统中安全电子邮件消息交换的方框图。系统包括连接到

WAN 32 和无线网关 34 的电子邮件发送者 30，其提供了 WAN 32 和无线网络 34 之间的接口。移动设备 38 适合于运行在无线网络 36 内。在图 2 还示出了数字证书注销状态信息提供器 37 和代理系统 39，二者连接到 WAN 32。

[0039] 电子邮件发送器 30 是 PC 诸如图 1 中的系统 14、或联网的计算机诸如图 1 中的计算机系统 28、或电子邮件消息 A 在其上构成和发送的另一移动设备。WAN32、无线网关 34、无线网络 36 和移动设备 38 实际上与图 1 中类似标记的组件相同。

[0040] 按照安全消息方案，诸如 S/MIME 和 PGP，使用由电子邮件发送器 30 选择的一次性会话密钥来加密消息。使用会话密钥加密消息体，然后使用消息将要被发送到的每个所寻址的消息接收器的公钥，进行自身加密。如在 40 示出的，用该方法加密的消息包括加密的消息体 44 和加密的会话密钥 46。在这种类型的消息加密方案中，消息发送器诸如电子邮件发送器 30 必须具有对加密的消息要发送到其的每个实体的公钥的访问能力。

[0041] 按照一个已知的数字签名方案，安全电子邮件发送器 30 通常通过获取消息的摘要并且使用发送器的私钥签名摘要，来对消息进行签名。例如可以通过对消息执行检验和、循环冗余检验 (CRC)、或某些其它优选的非可逆操作诸如散列，来产生摘要。然后，由发送器使用发送器私钥来签名该摘要。该私钥可用于对摘要执行加密或其它转换操作，以产生摘要签名。然后，将包括摘要和摘要签名的数字签名附加到输出消息。此外，发送器 30 的数字证书，其包括发送器公钥和利用一个或多个数字签名捆绑到公钥的发送器标识信息、及可能的任何链式数字证书、和与发送器数字证书及任何链式证书相关的 CRL，也可以被附加到安全消息上。

[0042] 由电子邮件发送者 30 发送的安全电子邮件消息 40 包括数字签名 42、以及均被签名的加密的消息体 44 和加密的会话密钥 46。发送器的数字证书、任何链式数字证书和一个或多个 CRL 也可以被包括在消息 40 中。在 S/MIME 安全消息技术中，数字证书、CRL 和数字签名通常被放置在消息的开始，并且在文件附件中包括消息体。由其它安全消息方案产生的消息可以以与所示的不同的顺序放置消息组件，或包括附加的和 / 或不同的组件。例如，安全消息诸如 40 可以包括寻址信息，诸如“To :(到 :)”和“From :(从 :)”电子邮件地址和其它报头信息。

[0043] 当从电子邮件发送器 30 发送安全电子邮件消息 40 时，它通过 WAN32 和无线网关 34 路由到无线网络 36 和移动设备 38。电子邮件发送者 30 和移动设备 38 之间的传输路径还可以包括附加的或与图 2 所示的不同的组件。例如，安全电子邮件消息 40 可以寻址到与消息服务器或数据服务器相关的信箱或数据存储器，所述消息服务器或数据服务器已经能够无线地转发或发送接收的消息和数据到移动设备 38。另外，中间系统也可以存储和 / 或路由安全消息到移动设备 38。如先前描述并且在美国专利 6,219,694 中公开的示例重定向系统是一个这种系统的例子。

[0044] 此外，消息可以通过其它传输机制而不是无线网关 34，路由或转发到移动设备 38。例如，路由到无线网络 36 可以利用以下方式来实现 :使用与电子邮件发送者 30 相关的无线 VPN 路由器、或在中间计算机系统处接收消息然后转发到移动设备 38 的情况下，与中间计算机系统或服务器相关的无线 VPN 路由器。

[0045] 无论签名的消息直接发送到移动设备 38 还是重定向到移动设备 38，当接收到签名的消息时，移动设备 38 通过产生消息体 44 和加密的会话密钥 46 的摘要，从数字签名 42

提取摘要(digest),比较产生的摘要与从数字签名42提取的摘要,和验证在数字签名42中的摘要签名,可以验证数字签名42。由安全消息接收者使用的摘要算法与由消息发送者使用的算法相同,并且例如可以在消息报头中或可能在数字签名42中被指定。一个通用的摘要算法是所说的安全散列算法1(SHA1),尽管也可以使用其它摘要算法,诸如消息摘要算法5(MD5)。

[0046] 为了验证数字签名42,消息接收器检索发送者公钥,并且通过对摘要签名执行逆向变换,对数字签名42中的摘要验证签名。例如,如果消息发送者通过使用发送者私钥加密摘要产生摘要签名,那么接收者使用发送者公钥解密摘要签名,以恢复原始摘要。如果安全消息包括发送者数字证书,或发送者数字证书已经存储在移动设备38处的数据存储器中,那么可以从接收的或存储的数字证书中提取发送者公钥。作为替代,如果从来自发送者的较早消息提取公钥并且存储在接收者本地存储器中的密钥存储单元中,则可以从本地存储单元获取发送者的公钥。或者,可以从公钥服务器(PKS)请求发送者数字证书。PKS是通常与证书授权(CA)相关的服务器,从证书授权中,可得到一个实体的数字证书,包括实体的公钥。PKS可驻留在公司LAN,诸如图1的LAN 18内,或在消息接收者可以通过其与PKS建立通信的WAN 32、因特网或其它网络或系统上的任何位置。可能地,还可以将发送者的数字证书从PC或其他计算机系统加载到移动设备39上。

[0047] 摘要算法最好是产生针对每个唯一输入的唯一输出的非可逆函数。因此,如果原始消息被改变或被破坏,那么由接收者产生的摘要将不同于从数字签名提取的摘要,因此签名验证失败。然而,因为摘要算法是公知的,实体可能会改变安全消息,产生被改变的消息的新摘要,和转发改变的消息到任何所寻址的消息接收者。在该情况下,基于改变的消息在接收器处产生的摘要将与由改变消息的实体添加的新摘要相匹配。摘要签名检验想要在这种情况下防止数字签名的验证。即使产生的和新摘要将会匹配,由于发送者使用其自己的私钥来签名原始摘要,改变消息的实体不能产生能够利用发送者公钥来验证的新摘要签名。因此,尽管在改变的消息中的摘要相匹配,但是,由于摘要签名验证将失败,将不验证所述数字签名。

[0048] 这些数学操作不防止任何人看到安全消息的内容,但是保证消息没有被篡改,因为它由发送者签名,并且保证消息由在消息的“From(来自)”字段中所指示的人签名。

[0049] 还应该理解,作为替代,可以使用其它数字签名产生和验证算法。上述的摘要和逆向转换方案是一个数字签名方案的例子。本发明决不限于此。

[0050] 当数字签名42已经被验证,或者某些时候,即使数字签名验证失败,那么在被显示或进一步由运行在图2中的移动设备38上的接收消息客户端处理之前,加密的消息主体44被解密。接收消息客户端使用其私钥来解密被加密的会话密钥46,然后使用解密会话密钥来解密被加密的消息主体44,并且由此恢复原始消息。

[0051] 被寻址到多于一个接收者的加密消息包括使用接收者的公钥加密的针对每个接收者的会话密钥的加密版本。每个接收者执行相同的数字签名验证操作,但是,使用其自己的私钥来解密不同的一个加密会话密钥。

[0052] 因此,在安全消息系统中,发送消息客户端应该能够访问加密消息将发送到其的任何接收者的公钥。接收消息客户端必须能够获得发送者的公钥,这可通过各种机制对消息客户端有效,以便验证签名消息中的数字签名。尽管移动设备38是安全消息40的接收

者，但是，移动设备 38 可以能够进行双向通信，并且因此可能需要用于消息发送和消息接收二个操作的公钥。

[0053] 公钥通常设置在数字证书中。如上所述，针对任何特定的实体的数字证书典型地包括：实体公钥和利用数字签名捆绑到公钥上的标识信息。几个类型的数字证书当前在被广泛使用，包括例如典型地用于 S/MIME 中的 X.509 数字证书。PGP 使用具有稍微不同格式的数字证书。在此公开的系统和方法可以结合这些类型的数字证书的任何一个、以及其它类型的数字证书、当前已知类型以及将来可以开发的其它类型来使用。

[0054] 数字证书中的数字签名由数字证书的发行者产生，并且能够由消息接收者检验。数字证书某些时候包括过期时间 (expiry time) 或有效期，根据其，消息客户端确定数字证书是否已经过期。数字证书的有效性的验证也可涉及通过数字证书链来跟踪认证路径，证书链包括用户的数字证书、和验证用户数字证书是可信的其它可能的数字证书。

[0055] 还可以检验数字证书以保证它还没有被注销。如上所述，可以通过查询 CRL 或通过请求来自数字证书注销状态信息源的数字证书状态信息，来检验数字证书注销状态。在图 2 的系统中，移动设备 38 的用户可以针对存储在移动设备 38 处的任何数字证书，向注销状态信息提供器 37 提交注销状态请求。然后，提供器 37 返回针对该数字证书的注销状态信息给移动设备 38。

[0056] OCSP 是提供用于不需要 CRL 而确定数字证书注销状态的一个方案。例如已经在 RFC 2560 和在因特网草案“在线数字证书状态协议，版本 2”（二者可从因特网工程任务组 (IETF) 得到）中定义了 OCSP 版本。OCSR 是最广泛使用的数字证书注销状态检验协议之一，因此，在此用作这些方案的一个示例。然而，在此描述的系统和方法也可以用于涉及从远端源中获取注销状态信息的其它类型的数字证书注销状态检验方案。

[0057] 按照 OCSP，提交请求给通常称为 OCSP 响应器的状态信息提供器。一旦接收到合适格式的请求，OCSP 响应器返回响应给请求器。OCSP 请求至少包括 OCSP 协议版本号、服务请求、和与该请求相关的目标数字证书的标识。

[0058] 版本号标识请求所遵从的 OCSP 的版本。服务请求指定正在被请求的服务的类型。对于 OCSP 版本 2，已经定义了在线注销状态 (ORS)、派遣路径有效 (DPV) 和派遣路径发现 (DPD) 服务。通过 ORS 服务，消息客户端获得数字证书的注销状态信息。DPV 和 DPD 服务有效地派遣数字证书有效路径相关的处理给远端系统。

[0059] 通常，使用数字证书发行者的区别名 (DN) 的散列、以及数字证书的序列号，在 OCSP 请求中识别目标数字证书。然而，由于多个数字证书发行者可以使用相同的 DN，以发行者公钥的散列的形式的另外的标识信息也包括在该请求中。因此，在 OCSP 请求中的目标数字证书信息包括散列算法标识符、使用散列算法产生的数字证书发行者的 DN 的散列、也是使用散列算法产生的发行者公钥的散列、和目标数字证书的序列号。

[0060] 该请求可以或可以不由请求器进行签名。另外可选的信息也可以包括在请求中，并且由 OCSP 响应器处理。

[0061] 当消息客户端操作在移动设备 22 上时，OCSP 可以是理想的，因为它相对于基于 CRL 的注销状态检验，减少了检验数字证书的注销状态需要的处理和存储器资源。然而，OCSP 请求可能会相对较长，并且由此消耗了移动设备上可用的通常有限的无线通信资源和电能。代理系统 39，连同适当能力的移动设备 38，用于优化 OCSP 和涉及移动设备的远端系

统的类似协议，这正如在下面进一步详细描述的。

[0062] 图 3 是实现数字证书注销状态检验系统的系统方框图。该移动设备 38 包括存储器 52、消息系统 60、代理系统客户端模块 62、用户接口 (UI)64 和无线收发器 66。存储器 52 最好包括用于数字证书存储单元 54 的存储区域，以及诸如其中存储消息联系信息的地址本 56 的可能的其它数据存储单元、和存储与安装在移动设备 38 上的软件应用相关的数据的应用数据存储单元 58。数据存储单元 56 和 58 是可以在移动设备 38 上的存储器 52 中实现的存储单元的示例。存储器 52 也可以由除了图 3 中所示的那些之外的其它设备系统来使用，以存储其它类型的数据。

[0063] 存储器 52 是示例的其它设备组件可以向其中写入数据的可写存储单元，诸如 RAM。数字证书存储单元 54 是专用于在移动设备 38 上存储数字证书的存储区。数字证书可以以它们被接收的格式，存储在数字证书存储单元 54 中，或者可选地，在写到存储单元 54 之前被解析或另外转换成存储格式。

[0064] 消息系统 60 连接到无线收发器 65，由此启动通过无线网络 36 的通信。在大多数实现中，消息系统 60 可以是以软件应用来实现的消息客户端。

[0065] 最好也作为软件应用或组件实现的代理系统客户模块 62 连接到消息系统 60、无线收发机 66、数字证书存储单元 54 和 UI 64。正如下面详细描述的，可以使用代理系统客户端模块 62 来检验针对存储在数字证书存储单元 54 中的任何数字证书的注销状态，以及由消息系统 60 接收但还没有存储在数字证书存储单元 54 中的数字证书的注销状态。

[0066] UI 64 可以包括如键盘或小键盘、显示器、或从移动设备 38 的用户接收输入或提供输出给移动设备 38 的用户的其它组件这样的 UI 组件。尽管在图 3 中示为单个方框，移动设备典型地包括多于一个 UI，和由此 UI 64 代表一个或多个用户接口。

[0067] 无线网络 36、无线网关 34、WAN 32 和注销状态信息提供器 37 基本上与图 2 中类似标出的组件相同。

[0068] 代理系统 39 包括代理系统服务模块 68 和状态提供器客户端模块 70。代理系统 39 图示包括连接到 WAN 32 和可操作用于从移动设备 38 或某些其它客户端系统接收加密项目状态请求的一个或多个计算机，并且代表移动设备 38，执行状态请求和伴随的处理步骤。在一个实施例中，代理系统 39 是代表移动设备 38 来执行状态请求的中间计算机。该中间计算机进一步可操作用于向移动设备的地址提供状态请求。在另一个实施例中，代理系统 39 包括代理服务器，该代理服务器除了代表移动设备 38 执行状态请求以外，也可以操作用于执行代理服务器功能，诸如提供安全、管理控制和高速缓存。

[0069] 配置代理系统服务模块 68，以便与代理系统客户端模块 62 交换信息，并且状态客户端模块 70 适合于与注销状态提供器 37 交换信息。这些组件的每一个，状态提供器客户端模块 70 和代理系统服务模块 68 最好是操作在代理系统 39 处的软件应用或模块。这些软件应用可以以单个计算机程序来实现，或可选地，可以是独立地执行分离程序。

[0070] 在运行中，如上所述，移动设备 38 上的消息系统 60 通过无线网络 36 接收和可能发送安全消息。当要对在接收的安全消息上的签名进行验证或要利用加密的会话密钥发送消息时，消息系统 60 可从数字证书中检索到针对实体（或接收到的消息的发送者或要发送的消息的接收者）的公钥。然而，在使用该公钥之前，消息系统 60 或其用户可能希望检验包含该公钥的数字证书是有效的并且还没有被注销。

[0071] 例如在以预定的或用户配置的间隔，或当通过 UI 64 由用户调用时，在利用安全消息接收数字证书的情况下，可以自动执行数字证书验证操作。

[0072] 不同类型的数字证书检验操作也可以取决于不同的控制。例如，当数字证书首先被加载进移动设备 38 上时，可以自动检验数字证书的有效性和注销状态，如果数字证书是有效的并且没有被注销，那么可以假定数字证书直到过期时间或在数字证书中指定的有效期内是有效的，而此后可以每星期一次，检验其注销状态以保证在其过期之前没有被注销。

[0073] 如上所述，对远端信息提供器诸如 37 的数字证书状态信息请求可能相对较长，并且因此对于在移动设备 38 或其它带宽受限的通信系统中的实现并不是最优的。代理系统客户端和服务模块 62 和 68 适合于减少从移动设备 38 发送以请求数字证书的状态信息的信息量。

[0074] 当移动设备 38 的用户希望检验数字证书的注销状态时，通过在 UI64 诸如象键盘上输入合适的命令，可以调用代理系统客户端模块 62 或可能协同代理系统客户端模块 62 一起操作的软件应用。用户也可以例如使用数字证书的序列号或主题名，指定要检验的特定数字证书。或者，代理系统客户端模块 62 可以访问数字证书存储单元 54，以显示给用户当前存储的数字证书的列表，从该表中，用户可以选择一个或多个要检验的数字证书。

[0075] 然后，代理系统客户端模块 62 最好或者从所选择的数字证书中提取、或者通过 UI 64 从用户中获得由代理系统服务模块 68 进行数字证书注销状态检验所需的任何信息。因为代理系统 39 提供移动设备 38 和状态信息提供器 37 之间的接口，代理系统客户端模块 62 和代理系统服务模块 68 之间的请求和响应不需要遵循在状态提供器客户端模块 70 和状态信息提供器 37 之间使用的协议。因此，尽管状态提供器 37 和状态提供器客户端模块 70 可以支持 OCSP 或类似协议，但是，代理系统服务模块 68 和客户端模块 62 最好支持涉及较少数据交换诸如较小请求的、更为无线友好的协议。

[0076] 由代理系统客户端模块 62 提取或获得的特定信息依赖于在代理系统客户端模块 62 和代理系统服务模块 68 之间实现的通信协议。代理系统客户端模块 62 最好从数字证书存储单元 54 中的数字证书中提取数字证书主题名、序列号、发行者名字、和其它数字证书信息。如果数字证书首先被解析，然后将解析的数据存储在数字证书存储单元 54 中，那么这种信息可以由代理系统客户端模块 62 从数字证书存储单元 54 中的解析数据中提取。如果需要另外的信息，用户可被提示以输入数据。

[0077] 当所有需要的信息已经被提取或者另外由代理系统客户端模块 62 获得时，格式化请求并且发送到代理系统服务模块 68。该请求的内容还取决于在代理系统服务模块 68 和客户端模块 62 之间使用的通信协议。如果支持多于一个类型的服务，那么该请求可以指定请求哪个类型的服务。在某些实现中，仅有单一服务可被支持，这样，没有服务类型需要被指定。

[0078] 由代理系统服务模块 68 接收的信息最好传递到状态提供器客户端模块 70。然后，由状态提供器客户端模块 70 使用该信息以格式化对状态信息提供器 37 的请求。如果注销状态信息提供器 37 和状态提供器客户端模块 70 例如支持 OCSP，则将由代理系统服务模块 68 提供的信息以及任何进一步需要的信息格式化成 OCSP 请求。在某些情况下，由代理系统服务模块 68 提供的信息包括所有需要的信息，而在其它情况下，可以从其它源中提取进一步的信息。例如，在配置代理系统 39 以存储保持数字证书发行者与序列号和 / 或主题名之

间的对应关系的映射表等元素的情况下，那么，状态提供者客户端模块 70 可以只基于从代理系统客户端模块 62 由代理系统服务模块 68 接收的序列号或主题名，格式化针对正确的注销状态信息提供器 37 的状态请求。

[0079] 在图 3 中，假定注销状态信息提供器 37 支持 ORS 等服务。一旦接收到请求，当提供器 37 及客户端模块 70 支持 OCSP 时作为 OCSP 响应器的注销状态信息提供器 37 检验该请求，以保证对适当地格式化、所请求的服务是被配置而提供的服务、并且该请求包括所请求的服务需要的所有信息。如果这些条件不满足，那么提供器 37 返回一个差错消息给客户端模块 70。然后，客户端模块 70 执行差错处理，提供任何丢失的需要的信息，并且可能通过代理系统服务模块 68 从移动设备 38 中请求丢失的信息，或返回差错消息给代理系统服务模块 68，代理系统服务模块 68 然后格式化并且发送差错消息给代理系统客户端模块 62，作为对其初始服务请求的响应。其它条件，诸如当提供器 37 接收到未签名的请求但被配置为期望签名的请求时，或当提供器服务不能响应时，可能导致被返回到提供器客户端模块 70 的差错消息。

[0080] 如果所述请求满足上述条件，那么确定的响应返回到提供器客户端模块 70。确定的响应可以包括多个状态指示之一，诸如，当目标数字证书还没有注销时“有效”等指示，当目标数字证书已经被注销时的“注销”指示，或如果状态提供器 37 没有目标数字证书的记录或不知道目标数字证书时的“未知”指示。

[0081] 此外，还可以操作代理系统客户端模块 62，当发送请求后等待数字证书的状态时，将数字证书划分为“等待 (pending)”。然后，在代理系统客户端模块 62 从代理系统 39 接收到相应的状态指示之后，数字证书的状态从等待改变到有效、注销或未知之一。如果数据项目包括带有等待、注销或未知状态的数字签名，还可以配置代理系统客户端模块 62，以便通过在移动设备 38 上的 I/O 设备提醒用户确认要对该数据项目执行的动作。

[0082] 将由状态信息提供器 37 返回到状态提供器客户端模块 70 的响应传递到代理系统服务模块 68，其准备并发送响应到代理系统客户端模块 62。当来自提供器 37 的响应被签名，并且代理系统客户端模块 62 或移动设备 38 上的另一组件被配置来验证状态响应签名时，那么来自状态提供器 37 的整个响应或可能其签名的部分，最好实质上未改变地转发到代理系统客户端模块 62。然而，如果代理系统服务模块 68 或状态提供器客户端模块 70 代表移动设备 38 检验状态响应签名，那么仅响应的一部分，例如状态指示和数字证书序列号或主题名，最好由代理系统服务模块 68 提取，并且格式化成响应，然后将其发送到代理系统客户端模块 62。然后，来自代理系统服务模块 68 的响应由代理系统客户端模块 62 处理，以确定是否该数字证书已经被注销。

[0083] 代理系统客户端模块 62 的存在最好不排除按照已知技术的数字证书有效性和注销状态检验。这样，涉及远端系统诸如状态信息提供器 37 的数字证书状态检验是对移动设备 38 能够进行的其它状态检验操作的补充。

[0084] 尽管图 3 的实施例将无线网关 34、代理系统 39 和注销状态提供器 37 作为在 WAN 32 上作为分离的系统的通信进行了描述，但是，这些系统也可以被组合。例如，在可选的实施例中，包括代理系统服务模块 68 和状态提供器客户端模块 70 的软件应用在无线网关 34 上存储并且执行。

[0085] 在另一个实施例中，包括代理系统服务模块 68 和状态提供器客户端模块 70 的软

件应用在注销状态提供器 37 上存储并且执行。在另一个实施例中，包括代理系统服务模块 68 和状态提供器客户端模块 70 的软件应用在消息服务器 26（图 1）上存储并且执行。当然，也可以使用能够实现在此公开的客户端 / 代理数字证书状态系统的功能的、针对分布在一个或多个网络上的计算机系统的其它配置和通信路径。

[0086] 在另一个可选实施例中，无线网关 34 是可操作的，以确定是否数据项，诸如要发送到移动设备 38 的 S/MIME 消息，利用数字签名进行签名或包括数字证书。如果这样，那么，无线网关 34 事先查询注销状态提供器 37，以获得用于 S/MIME 消息的签名者的数字证书状态。

[0087] 在 S/MIME 消息发送到移动设备 38 之前，最好获得数字证书状态，在该情况下，在无线网关 34 处存储 S/MIME 消息。如果数字证书不有效或过期，无线网关 34 可以进一步可操作用于丢弃 S/MIME 消息，或可选地，可以利用数字证书不是有效的或过期的通知，发送 S/MIME 消息给移动设备 38。

[0088] 图 4A 提供了图示检验数字证书注销状态的方法的流程图。在步骤 80，标识要执行状态检验的任何数字证书。如上所述，该步骤能够自动执行或数字证书能够由用户选择。然后在步骤 82，准备初始请求并且发送到代理系统。在步骤 84，代理系统准备和发送服务请求给状态信息提供器诸如 OCSP 响应器。然后，状态信息提供器检验该请求，以保证它被合适地格式化、在该例中为数字证书注销状态的所请求的服务得到提供器支持、并且所有需要的信息包括在请求中。这些检验在步骤 86 被执行。

[0089] 如果请求不满足这些条件，那么在步骤 88，向代理系统返回差错消息。在步骤 90，也可以返回给移动设备一个差错消息。或者在步骤 90 可以执行差错处理，例如，当该请求不包括所有需要的信息时，获得进一步的信息，之后，在步骤 84 可以准备新的服务请求和发送到提供器。

[0090] 当在步骤 86 中该请求满足所述条件时，在步骤 94，状态信息提供器返回状态指示给代理系统，以响应来自代理系统的服务请求。然后，在步骤 96，代理系统返回来自状态信息提供器的整个响应、或至少响应的一部分给移动设备，作为对来自移动设备的初始服务请求的响应。

[0091] 尽管上述的系统和方法涉及数字证书注销状态检验，数字证书有效性检验的示例，按照 OCSP 的 DPV 和 DPD 服务或其它协议，例如，可以通过代理系统客户端模块和服务模块，类似地优化用于移动设备和其他类型的处理受限、存储器受限或通信资源受限的系统。也可以使得代理系统 39 能够提供其代理服务给多个移动设备。

[0092] 图 4B 提供了图示检验数字证书注销状态的另一方法的流程图。在该方法中，无线网关 34（图 3）执行先前描述的代理程序，并且进一步可操作用于确定要传送到移动设备 38 的数据项诸如 S/MIME 消息是否包括数字证书。如果是这样，无线网关 34 事先查询注销状态信息提供器 37。

[0093] 在步骤 200，无线网关 34 接收要发送到移动设备 38 的数据项。在步骤 202，无线网关确定是否所述数据项包括数字证书。如果该数据项不包括数字证书，那么如在步骤 216 所示的，发送数据项到移动设备 38。

[0094] 然而，如果数据项包括数字证书，那么如在步骤 204 中所示的，则无线网关 34 存储数据项和准备发送到状态提供器的服务请求。

[0095] 在步骤206中接收状态信息，并且在步骤208，无线网关34确定是否该数字证书状态是有效的、被注销的、还是未知的。如果数字证书是有效的，那么如在步骤210和216中所示的，无线网关34将有效指示符附加到该数据项，然后该数据项重定向给移动设备38。如果数字证书被注销，那么如在步骤212和216中所示的，无线网关34将注销指示符附加到该数据项，然后该数据项发送给移动设备38。如果数字证书是未知的，那么在步骤214和216中，无线网关34将未知指示符附加到该数据项，然后该数据项发送给移动设备38。

[0096] 这样，一旦接收到包括数字证书的数据项，移动设备通过参考附加到数据项的有效、注销或未知指示符，立即确定数字证书的状态。

[0097] 在一个可选的实施例中，无线网关34事先查询注销状态信息提供器，但是用一个指示符例如指示数字证书状态已经被查询的“等待”指示符，转发所述接收的数据项给移动设备。然后，当从状态信息提供器接收到状态指示时，将证书状态的进一步指示发送给移动设备。

[0098] 在另一个实施例中，消息服务器26(图1)还包括如上所述的重定向系统。重定向系统执行代理程序，并且进一步可操作用于确定是否要发送到移动设备38的数据项包括数字证书。如果是这样，重定向系统事先查询注销状态提供器37以获得数字证书状态，和执行如参照无线网关34和图4B描述的类似处理步骤。

[0099] 在另一个实施例中，移动设备和代理系统包括多个客户端和服务模块。图5是实现具有多个代理系统客户端模块的数字证书注销状态检验系统的系统方框图。在图5中，存储器102、数据存储单元104、106和108、消息系统110、UI 114、无线收发器116、无线网络118、无线网关120和WAN 122基本上与在图3中类似标出的组件相同。

[0100] 移动设备100包括含有代理系统客户端模块N 113和代理系统客户端模块A 111和可能其它代理系统客户端模块的客户端模块112。代理系统128包括相应的代理系统服务模块A和N、132和136。代理系统128还包括状态提供器客户端模块A和N、130和134，所述模块被配置用于分别与状态信息提供器A 124和状态信息提供器N 126通信。

[0101] 图5所示的系统基本上如上所述操作。当一个或多个数字证书的状态诸如注销状态要被检验时，每个代理系统客户端模块111和113最好提取或另外获得在对其各代理系统服务模块132和136的服务请求中需要的信息。然后，状态提供器客户端模块130和134使用来自移动设备38的服务请求的信息、和可能在代理系统128处可得到的信息，以准备对状态信息提供器124和126的服务请求。然后，由状态信息提供器124和126返回的响应、或至少其一部分，如果需要，被重新格式化，并且返回到在移动设备100处的代理系统客户端模块111和113。

[0102] 每个代理系统客户端模块111和113可以适合于收集请求信息并且处理用于不同的远端数字证书状态检验协议的响应信息。然而，由代理系统客户端模块111和113收集的信息可以被组合成对代理系统128的单个服务请求。然后，每个代理系统服务模块132和136从对其相关的状态信息提供器124和126的服务请求所需要的服务请求中提取信息。由状态提供器系统124和126返回到状态提供器客户端模块130和134的响应或者分开地或者以单个响应，返回到代理系统客户端模块111和113。例如，当状态信息提供器124和126的一个或两个签名其响应时，配置代理系统客户端模块132和136验证响应签名，然后分开的响应按照它们各自的协议最好返回到代理系统客户端模块111和113。然而如果响

应没有被签名，响应可以被组合成单个响应。

[0103] 图5中所示的多客户端模块系统当用户希望检验整个数字证书链的有效性和/或注销状态时，特别有用，所述数字证书链包括从不同的状态信息提供器得到状态信息的数字证书。在已知系统中，在所述链中对每个数字证书的分开的请求，必须被发送到状态信息提供者。然而，在图5的系统中，只有单个请求需要从移动设备100发送，以从任何数目的状态信息提供器获得状态信息。此外，由所有代理系统客户端模块和服务模块请求的公共信息需要仅在发送到代理系统128的初始服务请求中包括一次，由此减少了在初始服务请求中的冗余。

[0104] 图6是无线移动通信设备的方框图。移动设备600最好是至少具有语音和数据通信能力的双向通信设备。移动设备600最好具有与因特网上的其它计算机系统通信的能力。根据移动设备提供的功能，移动设备可称为数据消息传送设备、双向寻呼机、带有数据消息传送能力的移动电话、无线因特网设备或数据通信设备（带有或不带有电话功能）。如上所述，这种设备在此简单统称为移动设备。

[0105] 移动设备600包括收发器611、微处理器638、显示器622、快闪存储器624、随机存取存储器(RAM)626、辅助输入/输出(I/O)设备628、串行口630、键盘632、扬声器634、麦克风636和短距离无线通信子系统640、以及其它设备子系统642。收发器611包括发送和接收天线616、618、接收器(Rx)612、发送器(Tx)614、一个或多个本地振荡器(LO)613、和数字信号处理器(DSP)620。在快闪存储器624内，移动设备600包括多个可由微处理器638(和/或DSP 620)执行的软件模块624A-624N，包括语音通信模块624A、数据通信模块624B和多个用于执行多个其它功能的其它操作模块624N。

[0106] 移动设备600最好是具有语音和数据通信能力的双向通信设备。于是，例如，移动设备600可以在语音网络诸如任何模拟或数字蜂窝网络上的任一个上进行通信，也可以在数据网络上通信。语音和数据网络在图6中由通信塔619表示。这些语音和数据网络可以是使用分离的基础设施诸如基站、网络控制器等的分离的通信网络，或它们可以集成为一个单个的无线网络。因此对网络619的引用应解释为包括单个语音和数据网络和分离的网络。

[0107] 通信子系统611用于与网络619的通信。DSP 620用于向和从发送器614和从接收器612发送和接收通信信号，并且也可以与发送器614和接收器612交换控制信息。如果语音和数据通信发生在单个频率上，或近间隔的频率组上，那么单个LO 613可以与发送器614和接收器612一起使用。或者，如果不同频率用于语音和数据通信，那么能够使用多个LO产生对应于网络619的多个频率。尽管在图6中示出了两个天线616、618，移动设备600能够使用单天线结构。包括语音和数据信息二者的信息，经DSP 620和微处理器638之间的链路与通信模块611交互通信。

[0108] 通信子系统611的详细设计诸如频带、分量选择和功率电平等取决于移动设备600将运行其中的通信网络619。例如，打算运行于北美市场的移动设备600可包括通信子系统611，该子系统设计运行于Mobitex或DataTAC移动数据通信网络，并且也设计运行于各种语音通信网络诸如AMPS，TDMA，CDMA，PCS等，而打算用在欧洲的移动设备600可被配置运行于GPRS数据通信网络和GSM语音通信网络。其它类型的数据和语音网络，分离的和集成的，也可以用于移动设备600。

[0109] 根据网络 619 的类型，对于移动设备 600 的访问需要也可改变。例如，在 Mobitex 和 DataTAC 数据网络中，移动设备使用与每个设备相关的唯一标识号注册在网络上。然而，在 GPRS 数据网络中，网络访问与移动设备 600 的订户或用户相关。GPRS 设备典型地需要用户标识模块（“SIM”），需要它，以便移动设备 500 运行于 GPRS 网络上。没有 SIM，本地或非网络通信功能（如果有）可能是可运行的，但是移动设备 600 将不能执行涉及在网络 619 上通信的任何功能，除了任何合法需要的操作诸如‘911’紧急呼叫之外。

[0110] 在已经完成任何需要的网络注册或激活过程之后，移动设备 600 可经网络 619 发送和接收通信信号，最好包括语音和数据两种信号。由天线 616 从通信网络 619 接收的信号被路由到接收器 612，该接收器设有信号放大、降频转换、滤波、信道选择和模拟到数字转换的操作。接收信号的模拟到数字转换允许更复杂的通信功能，诸如将使用 DSP 620 执行的数字解调和解码。以类似方式，处理将发送到网络 619 的信号，包括例如由 DSP 620 执行的调制和编码，然后提供给发送器 614 用于数字模拟转换、升频变换、滤波、放大和经天线 618 发送给通信网络 619。尽管图 6 中所示的单个接收器 611 用于语音和数据二种通信，移动设备 611 能够包括两个不同的收发器，用于发送和接收语音信号的第一收发器和用于发送和接收数据信号的第二收发器。也可以在移动设备中提供多个收发器，该移动设备用于操作于多于一个通信网络或多个频带内。

[0111] 除了处理通信信号之外，DSP 620 还可设有接收器和发送器控制。例如，应用到接收器 612 和发送器 614 中的通信信号的增益电平也可以通过在 DSP 620 中实现的自动增益控制算法得到自适应控制。其它收发器控制算法也能够在 DSP 620 中实现，以便提供更复杂的收发器 611 的控制。

[0112] 微处理器 638 最好管理和控制移动设备 600 的整个操作。这里，可以使用很多类型的微处理器或微控制器，或者，可选地，能够使用单个 DSP 620 执行微处理器 638 的功能。低级通信功能，包括至少数据和语音通信，通过收发器 611 中的 DSP 620 执行。其它高级通信功能，诸如语音通信应用 624A 和数据通信应用 624B，也可以存储在快闪存储器 624 中，用于由微处理器 638 执行。例如，语音通信模块 624A 可提供高级用户接口，该接口可操作用于经网络 619 在移动设备 600 和多个其它语音设备之间发送和接收语音呼叫。类似地，数据通信模块 624B 可提供高级用户接口，可操作用于经网络 619 在移动设备 600 和多个其它数据设备之间发送和接收数据，诸如电子邮件消息、文件、组织者信息、短文本消息等。在移动设备 600 上，安全消息软件应用，例如包含对应于消息系统 60 和代理系统客户端模块 62 或客户端模块 113 和 111 的软件模块，可与数据通信模块 624B 一起运行，以实现上述的技术。

[0113] 微处理器 638 还与其它设备子系统交互，这些子系统诸如是显示器 622、快闪存储器 624、RAM 626、辅助输入 / 输出 (I/O) 子系统 628、串行口 630、键盘 632、扬声器 634、麦克风 636、短距离通信子系统 640 和统一表示为 642 的任何其它设备子系统。例如，模块 624A-N 由微处理器 638 执行，并且可提供用户和移动设备 600 之间的高级接口。该接口典型包括通过显示器 622 提供的图形组件和通过辅助 I/O 628、键盘 632、扬声器 634 或麦克风 636 提供的输入 / 输出组件。这些接口在图 3 和 5 中总的表示为 UI 64 和 114。

[0114] 图 6 中所示的某些子系统执行与通信相关的功能，而其它子系统可提供“驻留”或设备内置功能。明显的是，某些子系统诸如键盘 632 和显示器 622 可以用于通信相关功能，

诸如输入文本消息用于经数据通信网络传送，以及设备驻留功能，诸如计算器或任务列表或其它 PDA 型功能。

[0115] 微处理器 638 使用的操作系统软件最好存储在非易失存储器诸如快闪存储器 624 中。除了操作系统和通信模块 624A-N 之外，快闪存储器 624 还可以包括用于存储数据的文件系统。最好还在快闪存储器 624 中提供存储区域以存储数字证书，地址本条目，和消息通信需要的其它可能的信息，如图 3 和 5 中的数据存储单元 54，56 和 58。操作系统、特定的设备应用或模块或其部分，可以临时加载到易失存储器诸如 RAM626 用于较快操作。此外，在永久将它们写到位于快闪存储器 624 中的文件系统之前，接收的通信信号也可以临时存储到 RAM 626。

[0116] 可以加载到双模式设备 600 的示例应用模块 624N 是个人信息管理器 (PIM) 应用，其提供 PDA 功能，诸如日历事件、约会和任务项。该模块 624N 还能与语音通信模块 624A 交互，用于管理电话呼叫，语音邮件等，也可以与数据通信模块 624B 交互，用于管理电子邮件通信和其它数据传输。或者，语音通信模块 624A 和数据通信模块 624B 的所有功能可以集成到 PIM 模块中。

[0117] 快闪存储器 624 最好提供文件系统，以方便在该设备上 PIM 数据项的存储。PIM 应用最好包括经无线网络 619，或者通过其自身或者结合语音和数据通信模块 624A 和 624B 来发送和接收数据项的能力。PIM 数据项通过无线网络 619，最好与所存储的或与主计算机系统相关的相应的数据项集合无缝地集成、同步和更新，由此，为与特定的用户相关的数据项建立镜像系统。

[0118] 尽管示为快闪存储器 624，本领域技术人员将理解除了闪存储器 624 之外或代替快闪存储器 624，可以使用其它类型的非易失存储器，诸如电池支持 RAM。

[0119] 通过将移动设备 600 放置在连接移动设备 600 的串行口 630 到主系统的串行口的接口底座中，移动设备 600 还能与计算机系统人工同步。串行口 630 还可以用于使用户能够通过外部设备或软件应用程序设定优选项，以下载其它应用模块 624N 用于安装，并且可能加载数字证书到设备上。可以使用该有线下载路径，以将加密密钥加载到设备上，这个是比通过无线网络 619 交换加密信息更安全的方法。

[0120] 附加的应用模块 624N 可通过网络 619、通过辅助 I/O 子系统 628、通过串行口 630、通过短距离通信子系统 640 或通过任何其它合适的子系统 642 被加载到移动设备 600 上，并且由用户安装在快闪存储器 624 或 RAM 626 中。这种在应用安装方面的灵活性增加了移动设备 600 的功能，并且能够提供增强的设备内置功能、通信相关功能或二者。例如，安全通信应用可以使得电子商务功能和其它金融交易能够使用移动设备 600 执行。

[0121] 当移动设备 600 运行于数据通信模式时，接收的信号诸如文本消息或网页下载，由收发器 611 处理并且提供给微处理器 638，其最好进一步处理接收的信号用于输出到显示器 622，或可选地输出到辅助 I/O 设备 628。由收发器 611 接收的数字证书，例如响应对一 PKS 的请求或附加到一安全消息上的，将按如上所述进行处理，以将其加到快闪存储器 624 中的数字证书存储单元（如果它还没有被存储）。这样的数字证书的有效性和 / 或注销状态也可以如上所述被检验。移动设备 600 的用户也可以使用键盘 632 编辑数据项，诸如电子邮件信息，键盘 632 最好是 QWERTY 型的完整字母数字键盘布局，尽管也能使用其它类型的完整字母数字键盘诸如已知的 DVORAK 型。对移动设备 600 的用户输入利用多个辅助 I/

0 设备 628 而得到进一步增强，该辅助设备可包括指轮输入设备、触板、各种开关、摇杆输入开关等。然后用户输入的编辑的数据项可经收发器 611 在通信网络 619 上被发送。

[0122] 当移动设备 600 操作在语音通信模式中时，移动设备 600 的整个操作基本上类似于数据模式，除了接收的信号最好输出到扬声器 634 和用于发送的语音信号由麦克风 636 产生之外。此外，上述的安全消息技术可以不一定必须应用于语音通信。可选的语音或音频 I/O 子系统诸如语音消息记录子系统，也可以在移动设备 600 上实现。尽管语音或音频信号输出最好基本通过扬声器 634 完成，也可以使用显示器 622 提供呼叫方标识的指示、语音呼叫的持续时间或其它语音呼叫相关的功能。例如，微处理器 638 结合语音通信模块 624A 和操作系统软件，可以检测输入的语音呼叫的呼叫方标识信息并且将其显示在显示器 622 上。

[0123] 短距离通信子系统 640 可以包括红外设备及相关电路和组件或诸如蓝牙模块或 802.11 模块的短距离无线通信模块，以提供与类似能力的系统和设备的通信。本领域技术人员将理解，“蓝牙”和“802.11”指从电气和电子工程师协会得到的规范组，分别涉及无线个人区域网络和无线 LAN。

[0124] 上述描述仅以示例方式涉及优选实施例，可以实现其它实施例。例如，尽管数字证书状态检验主要结合无线移动通信设备进行了描述。在此公开的系统和方法也可以应用到运行在其它平台上的消息客户端，包括那些运行在桌面和膝上型计算机系统的、联网的计算机工作站和可希望涉及远端系统的数字证书检验的其它类型的消息客户端。

[0125] 尽管上述描述也主要涉及 OCSP，通过结合远端系统和代理系统客户端模块运行的中间系统，可以类似优化其它协议。这些其它协议不限于数字证书状态检验协议。可以配置代理系统和代理系统客户端模块提供除了数字证书状态检验服务之外的其它服务。

[0126] 图 7 提供了图示数字证书状态请求的处理的功能性方框图 500。尽管数字证书状态请求的处理示于图 7 中，其它类型的状态请求也可以按照图 7 描述的被处理。客户端系统具有要由外部系统，诸如运行实现一个或多个代理系统服务模块和状态提供器客户端模块的代理系统程序 504 的代理系统，来提供服务的状态信息需求 502。

[0127] 将数字证书状态请求发送到运行在代理系统上的代理系统程序 504。发送到代理系统程序 504 的数字证书状态请求遵循客户端 / 代理协议。正如参照代理系统服务模块 68 和状态提供器客户端模块 70 描述的，代理系统程序 504 可操作用于代表客户端系统来接收数字证书状态请求和执行状态请求和后续处理步骤。客户端 / 代理协议可以遵循已知的通信协议或可替换为一个专有协议。

[0128] 然后，代理系统程序 504 准备数字证书状态请求，例如在映射表 514 中，包括在来自客户端系统的请求中的信息和在代理系统处可得到的可能信息，该数字证书状态请求要按照状态查询协议发送到运行状态提供器程序 506 的状态提供器系统。状态查询协议可以遵循一个已知的状态协议，诸如 OCSP，或取而代之可以是一个专有协议。在一个实施例中，客户端 / 代理协议是第一协议诸如专有协议，和状态查询协议是第二协议，诸如 OCSP。

[0129] 然后，状态提供器程序 506 处理该查询和状态提供器系统提供数字证书状态数据给代理系统程序 504。数字证书状态数据示例地包括一个数字证书状态指示符。如果数字证书包括一个数字证书链，那么相应数目的数字证书状态指示符被提供给代理系统程序 504。此外，状态提供器程序 506 可能需要来自代理系统程序 504 的附加信息，这样，代理系统程

序 504 和状态提供器程序 506 之间的多通信可能发生。相应地，多通信 508 和 510 表示在代理系统程序 504 和状态提供器程序 506 之间。

[0130] 一旦完成数字证书状态请求，代理系统程序 504 准备用于传送回到客户端系统的数字证书状态数据。在一个实施例中，代理系统程序 504 选择要发送到客户端系统的、从状态提供器程序 506 接收的整组状态答复数据。在另一个实施例中，代理系统程序只选择将发送到客户端系统的单状态指示符，诸如有效、无效、未知或注销。例如，如果在数字证书链中的一个数字证书由状态提供器程序 506 发现是无效的，那么代理系统程序 504 可以只选择要发送到客户端系统的无效状态指示符。或者，代理系统程序 504 可以选择要发送到客户端系统的无效状态指示符、并且还选择指定在数字证书链中哪个数字证书是无效的数据。也可以推导出要发送回到客户端系统的其它数据组合。

[0131] 客户端系统和代理系统存储保持数字证书发行者和序列号和 / 或主题名之间的对应关系的相应映射表 512 和 514 等元素。然后客户端系统可以只提供用于相应的数字证书的唯一指示符，诸如序列号或主题名。然后代理系统程序 504 可以只基于从客户端系统接收的序列号或主题名，按照用于运行状态提供器程序 506 的状态提供器系统的状态查询协议，格式化数字证书状态请求。类似地，如果需要，由代理系统返回到客户端系统的唯一标识符由客户端系统使用映射表 512 进行解析。这样，如果客户端系统包括可操作经无线网络与代理系统通信的移动设备，映射表 512 和 514 保持了 RF 网络相对有限的带宽。

[0132] 在图 8-10 示出了在此公开的系统和方法的宽范围的其它例子。图 8-10 描述了不同的示例通信系统内的系统和方法的另外应用。

[0133] 图 8 是展示通信系统的方框图。在图 8 中，示出了计算机系统 802、WAN 804、安全防火墙 808 之后的公司 LAN 806、无线基础设施 810、无线网络 812 和 814、和移动设备 816 和 818。公司 LAN 806 包括消息服务器 820、无线连接器系统 828、包括至少多个信箱 819 的数据存储单元 817、桌面计算机系统 822(具有直接到移动设备的通信链路，诸如通过物理连接 824 到接口或连接器 826)、和无线 VAN 路由器 832。下面将参考消息 833、834 和 836 描述图 8 中的系统的操作。

[0134] 计算机系统 802 例如可以是被配置连接到 WAN 804 的膝上、桌面或掌上型计算机系统。这样的计算机系统可以通过 ISP 或 ASP 连接到 WAN804。或者，计算机系统 802 可以是联网的计算机系统，例如计算机系统 822，其通过 LAN 或其它网络访问 WAN 804。很多现代的移动设备能够通过各种基础设施和网关配置连接到 WAN，这样计算机系统 802 也可以是一移动设备。

[0135] 公司 LAN 806 是已经能够用于无线通信的、中央型、基于服务器的消息系统的例子。公司 LAN 806 可以称为“主系统”，因为它主持带有用于消息的信箱 819 的数据存储单元 817，及可能地用于可以发送到移动设备 816 和 818 或从移动设备 816 和 818 接收的其它数据项的另外的数据存储单元 (未示出)，和无线连接器系统 828，无线 VAN 路由器 832，或能够进行公司 LAN 806 和一个或多个移动设备 816 和 818 之间的通信的其它可能的组件。用更通用的术语，主系统可以是无线连接器系统在其上运行或与无线连接器系统一起运行或相关运行的一个或多个计算机。公司 LAN 806 是主系统的一个优选实施例，其中主系统是在至少一个安全通信防火墙 808 之后操作并且由其保护的公司网络环境内运行的服务器计算机。其它可能的中央主系统包括 ISP、ASP 和其它服务提供商或邮件系统。尽管桌面

计算机系统 824 和接口 / 连接器 826 可以位于这些主系统之外，无线通信操作可以类似于下面描述的那些。

[0136] 公司 LAN 806 将无线连接器系统 828 作为相关无线通信功能组件实现，其将通常是软件程序、软件应用或建立与至少一个消息服务器 820 工作的软件组件。使用无线连接器系统 828，通过一个或多个无线网络 812 和 814 发送用户选择的信息到一个或多个移动设备 816 和 818，并且从这些移动设备接收信息。无线连接器系统 828 可以是消息系统的分离的组件，如图 8 所示，或者可以是部分或全部包含于其它通信系统组件中。例如，消息服务器 820 可以包含实现无线连接器系统 828、无线连接器系统 828 的一部分、或某些功能或全部功能的软件程序、应用或组件。

[0137] 运行在防火墙 808 后面的计算机上的消息服务器 820 充当主接口，用于公司与诸如因特网的 WAN 804 交换消息，该消息包括例如电子邮件、日历数据、语音邮件、电子文档和其它 PIM 数据。具体中间的操作和计算机将取决于经其交换消息的消息传递机制和网络的特定类型，因此没有在图 8 中示出。消息服务器 820 的功能可以扩展到超过消息发送和接收，如上所述，提供诸如动态数据库存储，用于数据如日历、to-do 表、任务表、电子邮件和文档这些特征。

[0138] 消息服务器诸如 820 通常在一个或多个数据存储单元诸如 817 中，保持多个信箱 819，用于在服务器上具有帐户的每个用户。数据存储单元 817 包括信箱 819，用于多个（“n 个”）用户帐户。标识用户、用户帐号、信箱或与用户、帐号或信箱 819 相关的其它可能的地址作为消息接收者的、由消息服务器 820 接收的消息，通常被存储在相应的信箱 819 内。如果将消息寻址到多个接收者或分布表，那么相同消息的复制件可被存储在多于一个信箱 819 内。或者，消息服务器 820 可以在一数据存储单元中存储该消息的单个复制件，该数据存储单元对于具有在消息服务器 820 上的帐户的所有用户是可访问的，并且在每个接收者的信箱 819 中存储指针或其它标识符。在典型的消息系统中，每个用户于是可以使用通常运行于连接在 LAN 806 内的 PC 诸如桌面计算机系统 822 上的消息客户端（诸如 Microsoft Outlook 或 Lotus Notes），访问他或她的信箱 819 和其内容。尽管在图 8 中仅示出了一个桌面计算机系统 822，本领域技术人员应理解 LAN 将通常包含很多桌面、笔记本和膝上计算机系统。每个消息客户通常通过消息服务器 820 访问信箱 819，尽管在某些系统中，消息客户能够直接访问由桌面计算机系统 822 在其上进行存储的信箱 819 和数据存储单元 817。消息也可以从数据存储单元 817 下载到桌面计算机系统 822 上的本地数据存储单元（未示出）中。

[0139] 在公司 LAN 806 内，无线连接器系统 828 结合消息服务器 820 操作。无线连接器系统 828 可驻留在与消息服务器 820 相同的计算机系统上，或作为替代，可以在不同的计算机系统上实现。实现无线连接器系统 828 的软件也可以部分或全部地与消息服务器 820 集成。最好设计无线连接器系统 828 和消息服务器 820 合作并且交互操作，以允许将信息推到移动设备 816、818。在这样的安装中，最好配置无线连接器系统 828，将存储在一个或多个与公司 LAN 806 相关的数据存储单元中的信息通过公司防火墙 808 和经 WAN 804 和无线网络 812，814 之一，发送到一个或多个移动设备 816、818。例如，在数据存储单元 817 中具有一个帐户和相关信箱 819 的用户也可以具有移动设备诸如 816。如上所述，标识用户、帐号或信箱 819 的由消息服务器 820 接收的消息由消息服务器 820 存储到相应的信箱 819。如

果用户具有移动设备，诸如 816，由消息服务器 820 接收并且存储到用户信箱 819 的消息最好由无线连接器系统 828 检验，并且发送到用户的移动设备 816。该类型的功能代表“推”消息发送技术。作为替代，无线连接器系统 828 可以采用“拉”技术，其中，存储在信箱 819 中的项目响应使用移动设备进行的请求或访问操作，被发送到移动设备 816、818，或这两种技术的某些组合。

[0140] 因此，无线连接器 828 的使用使得包括消息服务器 820 的消息系统能够被扩展，这样每个用户的移动设备 816，818 具有对消息服务器 820 的存储消息的访问能力。尽管在此描述的系统和方法不仅限于基于推的技术，但是，基于推消息传送的更详细描述可被发现于上述被引用参考的美国专利和申请中。该推技术使用无线友好编码、压缩和加密技术，以将所有信息传递到移动设备，于是，有效地扩展了公司防火墙 808 以使其包括移动设备 816 和 818。

[0141] 如图 8 所示，有多个路径用于从公司 LAN 806 与移动设备 816，818 交换信息。一个可能的信息传送路径是使用接口或连接器 826，通过物理连接 824，诸如串行口。该路径能够是有用的，例如用于在移动设备 816，818 初始化上经常执行的、或当移动设备 816，818 的用户工作于 LAN 806 上的计算机系统诸如计算机系统 822 时周期执行的庞大信息更新。例如，如上所述，PIM 数据通常通过这样的连接，例如连接到一个移动设备 816，818 可以放入或放上的底座的串行口，被进行交换。物理连接 824 也可以用于从桌面计算机系统 822 到移动设备 816，818 传送其它信息，包括私有安全密钥（私钥），诸如与桌面计算机系统 822 相关的私有加密或数字签名密钥、或其它诸如数字证书和 CRL 等相对较大的信息。

[0142] 使用物理连接 824 和连接器或接口 826 的私钥交换允许用户的桌面计算机系统 822 和移动设备 816 或 818 共享至少一个标识，用于访问所有加密和 / 或签名的邮件。用户的桌面计算机系统 822 和移动设备 816 或 818 由此也能够用于共享私钥，这样主系统 822 或移动设备 816 或 818 能够处理寻址到消息服务器 820 上的用户信箱或帐户的安全消息。需要经过这种物理连接传送证书和 CRL，因为它们代表 S/MIME、PGP 和其它公钥安全方法需要的大量数据。用户自己的数字证书、用于验证用户数字证书的一连串证书和 CRL、及用于其它用户的数字证书、数字证书链和 CRL 可以从用户桌面计算机系统 822 加载到移动设备 816、818 上。该其它用户数字证书和 CRL 到移动设备 816，818 的加载允许移动设备用户选择其它的实体或用户（这些实体或用户可能与移动设备用户正在交换安全消息），并且通过物理连接（代替无线）将大信息预加载到移动设备上，于是，节省了当从这些其它用户接收到安全消息或安全消息发送到这些用户时，或当数字证书的状态将被基于一个或多个 CRL 确定时的时间和无线带宽。在采用在此描述的系统和方法的情况下，也能避免基于 CRL 的状态检验。

[0143] 在已知的“同步”型无线消息系统中，物理路径也已经用来从与消息服务器 820 相关的信箱 819 到移动设备 816 和 818 传送消息。

[0144] 用于与移动设备 816、818 数据交换的另一方法是通过无线方式，通过无线连接器系统 828 和使用无线网络 812、814。如图 8 所示，这能够涉及无线 VPN 路由器 832（如果在网络 806 中存在的话），或可选地，涉及到无线基础设施 810 的传统 WAN 连接，其提供到一个或多个无线网络诸如 814 的接口。无线 VPN 路由器 832 用于创建直接通过特定无线网络 812 到无线设备 816 的 VPN 连接。这种无线 VPN 路由器 832 可以与静态寻址方案一起使用。

例如，如果无线网络 812 是基于 IP 的无线网络。那么 IPV6 将提供足够的 IP 地址以分配一个 IP 地址给被配置操作在网络 812 内的每个移动设备 816，由此能够在任何时间，将信息推到移动设备 816。使用无线 VPN 路由器 832 的主要优点是它是不需要无线基础设施 810 的现成的 VPN 组件。VPN 连接可以使用 TCP/IP 或 UDP/IP 连接，直接传递消息到移动设备 816 和从移动设备 816 传递信息。

[0145] 如果无线 VPN 路由器 832 不是可用的，那么与 WAN 804（通常是一因特网）的连接，是可由无线连接器系统 828 使用的常使用的连接机制。为了处理移动设备 816 的寻址和任何其它需要的接口功能，最好使用无线基础设施 810。无线基础设施 810 也可以确定用于定位一个给定的用户的最可能的无线网络，并且当用户在国家或网络之间漫游时跟踪用户。在无线网络诸如 812 和 814 中，消息通常经基站和移动设备之间的 RF 传输，传递到移动设备或从该移动设备传递。

[0146] 可以提供到无线网络 812 和 814 的多个连接，包括例如利用在整个因特网中使用的 TCP/IP 协议的 ISDN、帧中继或 T1 连接。无线网络 812 和 814 能够表示清楚的、唯一的和不相关的网络，或它们能够表示不同国家中的相同网络，并且可以是下列不同类型的网络的任何一个，这些网络包括但不限于：数据为核心的无线网络、语音为核心的无线网络、和能够支持经相同或类似基础设施诸如上述描述的那些中的语音和数据通信的双模式网络。

[0147] 在某些实现中，可以在公司 LAN 806 中提供多于一个无线信息交换机制。例如，在图 8 例子中，配置与用户相关的移动设备 816、818，以使其运行在不同的无线网络 812 和 814 中，所述用户具有与消息服务器 820 上的用户帐户相关的信箱 819。如果无线网络 812 支持 IPv6 寻址，那么无线 VPN 路由器 832 可由无线连接器 828 使用，以与运行在无线网络 812 内的任何移动设备 816 交换数据。然而，无线网络 814 可以是不同类型的无线网络，诸如 Mobitex 网络，在该情况下，作为替代，信息可经到 WAN 804 和无线基础设施 810 的连接，与运行于无线网络 814 内的移动设备 818 交换。

[0148] 现在，使用从计算机系统 802 发送并且寻址到具有帐号和信箱 819 或与消息服务器 820 和移动设备 816 或 818 相关的数据存储单元的至少一个接收者的电子邮件消息 833 的例子，描述图 8 中的系统的操作。然而，电子邮件消息 833 仅用于示例。公司 LAN 806 之间的其它类型信息的交换最好也能由无线连接器系统 828 进行。

[0149] 从计算机系统 802 经 WAN 804 发送的电子邮件消息 833 根据使用的具体消息传送方案，可以是明文的或用数字签名进行签名的和 / 或被加密的。例如，如果使用 S/MIME 使得计算机系统 802 能够用于安全消息传送，那么电子邮件消息 833 可以被签名、加密、或签名并加密。

[0150] 电子邮件消息诸如 833 通常使用传统 SMTP，RFC822 报头和 MIME 主体部分以定义电子邮件消息的格式。这些技术对于本领域技术人员全部公知的。电子邮件消息 833 到达消息服务器 820，其确定电子邮件消息 833 应该存储进哪个信箱 819。如上所述，消息诸如电子邮件消息 833 可以包括用户名、用户帐户、信箱标识符或可由消息服务器 820 映射到特定的帐户或相关信箱 819 的其它类型的标识符。对于电子邮件消息 833，接收者通常使用对应于用户帐户和由此的一个信箱 819 的电子邮件地址被识别。

[0151] 无线连接器系统 828 最好一旦检测到已经发生了一个或多个触发事件，通过无线网络 812 或 814，从公司 LAN 806 到用户移动设备 816 或 818 发送或镜像某些用户选择的数

据项或数据项的一部分。触发事件包括但不限于下列情况的一个或多个：在用户联网的计算机系统 822 上的屏幕保护程序的激活；用户移动设备 816 或 818 从接口 826 断开；或接收从移动设备 816 或 818 发送到主系统以开始发送存储在主系统上的一个或多个消息的命令。这样，无线连接器系统 828 可以检测与消息服务器 820 相关的触发事件，诸如命令的接收，或与一个或多个联网的计算机系统 822 相关的触发事件，包括上述的屏幕保护程序和断开事件。当在 LAN 806 已经激活针对移动设备 816 或 818 的公司数据的无线访问时，例如，当无线连接器系统 828 检测到对于移动设备用户发生了触发事件时，由用户选择的数据项最好发送到用户移动设备。在电子邮件消息 833 的例子中，假定一旦已经检测到触发事件，由无线连接器系统 828 检测在消息服务器 820 处消息 833 的到达。这个例如可以通过监视或询问与消息服务器 820 相关的信箱 819 完成，或者如果消息服务器 820 是微软交换服务器 (Microsoft Exchange server)，那么，无线连接器系统 828 可以登记由微软消息应用编程接口 (MAPI) 提供的建议同步，由此当新消息存储到信箱 819 时接收通知。

[0152] 当一数据项诸如电子邮件消息 833 将要发送到移动设备 816 或 818 时，无线连接器系统 828 最好以对移动设备 816 或 818 透明的方式重新打包数据项，这样，发送到移动设备 816 或 818 或由移动设备 816 或 818 接收的信息类似于存储在主系统、并且在主系统处 (图 8 中的 LAN 806) 可访问的信息。一个优选的重新打包的方法包括：在对应于消息将发送到其的移动设备 816 或 818 的无线网络地址的电子信封中，打包将通过无线网络 812 或 814 发送的所接收的消息。或者，可以使用其它重新打包的方法，诸如专用 TCP/IP 打包技术。这种重新打包的方法最好还导致从移动设备 816 或 818 发送的电子邮件消息，似乎来自一个相应的主系统帐户或信箱 819，即使它们从移动设备编写并且发送。因此，移动设备 816 或 818 的用户最好在主系统帐户或信箱 819 和移动设备之间，可以有效地共享单个电子邮件地址。

[0153] 电子邮件消息 833 的重新打包在 834 和 836 处指示。重新打包技术对于任何可用的传送路径可以是类似的，或可以取决于具体的传送路径，无线基础设施 810 或无线 VPN 路由器 832。例如，电子邮件消息 833 最好被压缩和加密，在 834 处被重新打包之前或之后，由此，有效地提供到移动设备 818 的安全传送。压缩减少了发送消息需要的带宽，而加密保证了发送到移动设备 816 和 818 的任何消息或其它信息的保密性。相反，经 VPN 路由器 832 传送的消息可能仅被压缩，但不加密，因为由 VPN 路由器 832 建立的 VPN 连接是固有安全的。由此，经在无线连接器系统 828 处的加密，例如可被考虑一非标准的 VPN 隧道或类 VPN 连接，或者经 VPN 路由器 832，消息安全发送到移动设备 816 和 818。由此，使用移动设备 816 或 818 访问消息与使用桌面计算机系统 822 访问 LAN 806 处信箱同样安全。

[0154] 当重新打包的消息 834 或 836 经无线基础设施 810 或经无线 VPN 路由器 832 到达移动设备 816 或 818 时，移动设备 816 或 818 从重新打包的消息 834 或 836 移去外面的电子信封，并且执行任何需要的解压缩和解密操作。从移动设备 816 或 818 发送并且寻址到一个或多个接收者的消息最好被类似重新打包，并且可能压缩和加密，和发送到主系统诸如 LAN806。然后，主系统从重新打包的消息移去电子信封，如果需要，解密和解压缩消息，并且将消息路由到被寻址的接收者。

[0155] 使用外部信封的另一目的是至少保持在原始电子邮件消息 833 中的某些寻址信息。尽管用来路由信息到移动设备 816、818 的外部信封使用一个或多个移动设备的网络地

址而被寻址，外部信封最好将整个原始的电子邮件消息 833，包括至少一个地址字段，可能以压缩和 / 或加密的形式，进行封装。这使得当外部信封被去除并且消息显示在移动设备 816 或 818 上时，电子邮件消息 833 的原始的“To（到）”“From（从）”和“CC（抄送）”地址得到显示。当从移动设备发送的重新打包的输出消息的外部信封由无线连接器系统 828 移去时，重新打包也使得利用反映主系统上移动设备用户帐户或信箱的地址的“From”字段，将答复消息传递到所寻址的接收者。使用来自移动设备 816 或 818 的用户帐户或信箱地址使得从移动设备发送的消息仿佛是来自主系统上用户信箱 819 或帐户的消息，而不是来自移动设备。

[0156] 图 9 是可选的通信系统例子的方框图，其中无线通信由与无线网络的运营者相关的组件启动。如图 9 所示，该系统包括：计算机系统 802、WAN 804、位于安全防火墙 808 后面的公司 LAN 807、网络运营者基础设施 840、无线网络 811、和移动设备 813 和 815。计算机系统 802、WAN 804、安全防火墙 808、消息服务器 820、数据存储单元 817、信箱 819 和 VPN 路由器 835 实际上与图 8 中相同标记的组件相同。然而，由于 VPN 路由器 835 与网络运营者基础设施 840 通信，它不必一定是图 9 的系统中的无线 VPN 路由器。网络运营者基础设施 840 能够实现分别与计算机系统 842 和 852 相关并且配置运行在无线网络 811 中的 LAN 807 和移动设备 813、815 之间的无线信息交换。在 LAN 807 中，示出了多个桌面计算机系统 842、852，每个具有到接口或连接器 848 或 858 的物理连接 846 或 856。无线连接器系统 844 或 854 运行在每个计算机系统 842 和 852 上或与每个计算机系统 842 和 852 一起工作。

[0157] 无线连接器系统 844 和 854 类似于上述的无线连接器系统 828，因为它使得数据项诸如电子邮件消息和存储在信箱 819 中的其它项、以及可能存储在本地或网络数据存储单元中的数据项，能够从 LAN 807 发送到一个或多个移动设备 813、815。然而在图 9 中，网络运营者基础设施 840 提供移动设备 813 和 815 和 LAN 807 之间的接口。如同上面，下面将以电子邮件消息作为可以发送到移动设备 813 和 815 的数据项的例子，描述图 9 所示的系统的操作。

[0158] 当由消息服务器 820 接收寻址到具有消息服务器 820 上的帐户的一个或多个接收者的电子邮件消息 833 时，消息或可能是存储在中央信箱或数据存储单元中的消息的单个复制件的指针，被存储在每个这种接收者的信箱 819 中。一旦电子邮件消息 833 或指针已经存储在信箱 819 中，它最好能够使用移动设备 813 或 815 被访问。在图 9 示出的例子中，电子邮件消息 833 已经被寻址到与桌面计算机系统 842 和 852 以及由此与相应的移动设备 813 和 815 相关的信箱 819。

[0159] 正如本领域技术人员理解的，通常用在有线网络诸如 LAN 807 和 / 或 WAN 804 中的通信网络协议不适合于或不匹配在无线网络诸如 811 中使用的无线网络通信协议。例如，在无线网络通信中主要关心的通信带宽、协议开销和网络等待时间，在有线网络中不重要，有线网络比无线网络典型地具有更高容量和速度。因此，移动设备 813 和 815 通常不能直接访问数据存储单元 817。网络运营者基础设施 840 提供无线网络 811 和 LAN 807 之间的桥接。

[0160] 网络运营者基础设施 840 使得移动设备 813 或 815 能够通过 WAN 804 建立到 LAN 807 的连接，并且例如可以由无线网络 811 的运营者或为移动设备 813 和 815 提供无线通信服务的服务提供商来操作。在基于拉的系统中，使用无线网络匹配通信方案，当信息应该保

持保密时最好使用安全方案诸如无线传输层安全 (WTLS)、和无线网络浏览器诸如无线应用协议 (WAP) 浏览器，移动设备 813 或 815 可以建立与网络运营者基础设施 840 的通信会话。然后，用户可以请求（通过人工选择或驻留在移动设备里的软件中的预选择缺省）存储在 LAN 807 处的数据存储单元 817 中的信箱 819 中的任何或所有信息或例如仅仅新信息。然后如果没有会话已经建立，例如使用安全超文本传输协议 (HTTPS)，网络运营者基础设施 840 建立与无线连接器系统 844 或 854 的连接或会话。如上所述，可以经典型的 WAN 连接或通过 VPN 路由器 835（如果有的话）进行网络运营者基础设施 840 和无线连接器系统 844 或 854 之间的会话。当接收来自移动设备 813 或 815 的请求和传递所请求的信息回到设备之间的时间延迟将被最小化时，可以配置网络运营者基础设施 840 和无线连接器系统 844 和 854，使得通信连接一旦被建立保持开通。

[0161] 在图 9 的系统中，来自移动设备 A 813 和 B 815 的请求将分别发送到无线连接器系统 844 和 854。一旦接收到来自网络运营者基础设施 840 的信息请求，无线连接器系统 844 或 854 从数据存储单元中获得所请求的信息。对于电子邮件信息 833，无线连接器系统 844 或 854 通常通过结合计算机系统 842 或 852 操作的消息客户端（或者经消息服务器 820 或者直接可访问信箱 819），从适当的信箱 819 获取电子邮件消息 833。或者，可以配置无线连接器系统 844 或 854，直接或通过消息服务器 820 访问信箱 819 本身。此外，其它数据存储单元，类似于数据存储单元 817 的网络数据存储单元和与每个计算机系统 842，852 相关的本地数据存储单元，对于无线连接器系统 844、854 来说可以访问，并且由此对于移动设备 813，815 可以访问。

[0162] 如果电子邮件消息 833 寻址到与计算机系统 842 和 852 及设备 813 和 815 两者相关的消息服务器帐户或信箱 819，那么电子邮件消息 833 可发送到网络运营者基础设施 840，如在 860 和 862 示出的那样，然后发送电子邮件消息的复制件到每个移动设备 813 和 815，如在 864 和 866 指示的。信息经到 WAN 804 的连接或 VPN 路由器 835，在无线连接器系统 844 和 854 和网络运营者基础设施 840 之间传送。当网络运营者基础设施 840 经不同的协议与无线连接器系统 844、854 和移动设备 813，815 通信时，可由网络运营者基础设施 840 执行转换操作。重新打包技术也可以在无线连接器系统 844、854 和网络运营者基础设施 840 之间、以及每个移动设备 813 和 815 和网络运营者基础设施 840 之间使用。

[0163] 要从移动设备 813 或 815 发送的消息或其它信息能够以类似方式得到处理，这些信息首先从移动设备 813 或 815 传送到网络运营者基础设施 840。然后，网络运营者基础设施 840 发送信息到无线连接器系统 844 或 854，用于存储在信箱 819 中，并且例如通过消息服务器 820 传递到任何所寻址的接收者，或者可选地将信息传递到寻址的接收者。

[0164] 图 9 中的系统的上述描述涉及基于拉的操作。作为替代，无线连接器系统 844 和 854 和网络运营者基础设施可配置为将数据项推到移动设备 813 和 815。也能够是一组合的推 / 拉系统。例如，当前存储在 LAN807 处的数据存储单元中的数据项列表或新消息的通知可以推到移动设备 813、815，然后可以用来经网络运营者基础设施 840，从 LAN 807 请求消息或数据项。

[0165] 如果与 LAN 807 上的用户帐户相关的移动设备被配置操作于不同的无线网络内，然后，每个无线网络可以具有类似于 840 的相关无线网络基础设施组件。

[0166] 尽管在图 9 的系统中，为每个计算机系统 842 和 852 示出了分离的专用的无线连

接器系统 844 和 854。最好配置一个或多个无线连接器系统 844 和 854，以与多于一个计算机系统 842 和 852 一起操作，或访问与多于一个计算机系统相关的数据存储单元或信箱 819。例如，无线连接器系统 844 可被授权访问与计算机系统 842 和计算机系统 852 二者相关的信箱 819。然后，来自移动设备 A 813 或 B 815 对数据项的请求可以由无线连接器系统 844 处理。该配置可用于启动 LAN 807 和移动设备 813 和 815 之间的通信，不需要针对每个移动设备用户运行桌面计算机系统 842 和 852。作为替换，无线连接器系统可以与消息服务器 820 一起实现，以能够进行无线通信。

[0167] 图 10 是另一个可选的通信系统的方框图。该系统包括：计算机系统 802、WAN 804、位于安全防火墙 808 后面的公司 LAN 809、访问网关 880、数据存储单元 882、无线网络 884 和 886、和移动设备 888 和 890。计算机系统 802、WAN 804、安全防火墙 808、消息服务器 820、数据存储单元 817、信箱 819、桌上型计算机系统 822、物理连接 824、接口或连接器 826 和 VPN 路由器 835 实质上与上述相应的组件相同。访问网关 880 和数据存储单元 882 给移动设备 888 和 890 提供对存储在 LAN 809 处的数据项的访问。在图 10 中，无线连接器系统 878 运行于消息服务器 820 上或与消息服务器 820 一起操作，尽管作为替换，无线连接器系统可以运行于 LAN 809 中的一个或多个桌面计算机系统上或与 LAN 809 中的一个或多个桌面计算机系统一起工作。

[0168] 无线连接器系统 878 用于存储在 LAN 809 上的数据项到一个或多个移动设备 888 和 890 的传送。这些数据项最好包括，存储在数据存储单元 817 上的信箱 819 中的电子邮件消息、以及存储在数据存储单元 817 或另一网络数据存储单元或计算机系统诸如 822 的本地数据存储单元中的可能的其它数据项。

[0169] 如上所述，寻址到具有消息服务器 820 上的帐户的一个或多个接收者并且由消息服务器 820 接收的电子邮件消息 833 可以存储到每个这样的接收者的信箱 819 中。在图 10 的系统中，外部数据存储单元 882 最好具有与数据存储单元 817 类似的结构，并且保持与数据存储单元 817 同步。存储在数据存储单元 882 中的 PIM 信息或数据最好可独立修改存储在主系统上的 PIM 信息或数据。在该种具体配置中，在外部数据存储单元 882 处独立可修改的信息可保持与用户相关的多个数据存储单元（例如移动设备上的数据、家中个人计算机上的数据、公司 LAN 上的数据）的同步。该同步可按照如下方式完成：例如，可通过以一定的时间间隔、每次数据存储单元 817 中的一项被添加或改变时、在一天的某些时候、或当在 LAN 809 启动时，由无线连接器系统 878 发送到数据存储单元 882 的更新，通过消息服务器 820 或计算机系统 822，在数据存储单元 882 处，或可能通过移动设备 888，890 经由访问网关 880。

[0170] 在电子邮件消息 833 的清况下，接收电子邮件消息 833 之后的某时间发送到数据存储单元 882 的更新指示消息 833 已经存储在存储单元 817 中的某一信箱 819 中，并且电子邮件消息的复制件将被存储到数据存储单元 882 中的相应的存储区域中。当电子邮件消息 833 已经存储在对应于移动设备 888 和 890 的信箱 819 中时，在图 10 中以 892 和 894 指示的电子邮件消息的一个或多个复制件将被发送到并且存储到数据存储单元 882 中的相应的存储区域或信箱中。正如示出的，在数据存储单元 817 中存储信息的更新或复制可通过到 WAN 804 的连接或 VPN 路由器 835 的连接发送到数据存储单元 882。例如，无线连接器系统 878 可经 HTTP 投寄请求，投寄更新或存储的信息到数据存储单元 882 中的资源。或

者，可以使用安全协议，诸如HTTPS或安全套接字层(SSL)。本领域技术人员将理解，存储在LAN 809处的数据存储单元中多于一个位置的数据项的单个复制件可以被替换为发送到数据存储单元882。然后，数据项的该复制件，利用存储在数据存储单元882中的每个相应位置中的所存储数据项的指针或其它标识符，能够存储在数据存储单元882中多于一个相应的位置，或者单个复制件可存储在数据存储单元882中。

[0171] 访问网关880是一个有效的访问平台，因为它为移动设备888和890提供了对数据存储单元882的访问。数据存储单元882可以配置为在WAN 804上可访问的资源，并且访问网关880可以是ISP系统或WAP网关，通过其，移动设备888和890可以连接到WAN 804。然后，与无线网络884和886兼容的WAP浏览器或其它浏览器可被用于访问与数据存储单元817同步的数据存储单元882，并且或者自动地或者响应于来自移动设备888或890的请求，下载存储的数据项。如在896和898示出的，存储在数据存储单元817中的电子邮件消息833的复制件，可发送到移动设备888和890。由此，在每个移动设备888，890上的数据存储单元（未示处）可以与公司LAN 809上的数据存储单元817的一部分诸如信箱819同步。移动设备数据存储单元的变化可类似地反映在数据存储单元882和817中。

[0172] 在此描述的实施例是具有对应于在权利要求中列举的发明单元的组件的系统和方法。该书面说明书可以使得本领域普通技术人员能够制造和使用具有同样对应于权利要求中列举的发明单元的可选组件的实施例。由此本发明的打算范围包括不同于权利要求的文字语言的其它结构、系统或方法，并且进一步包括具有与权利要求的文字语言无实质区别的其它结构，系统或方法。

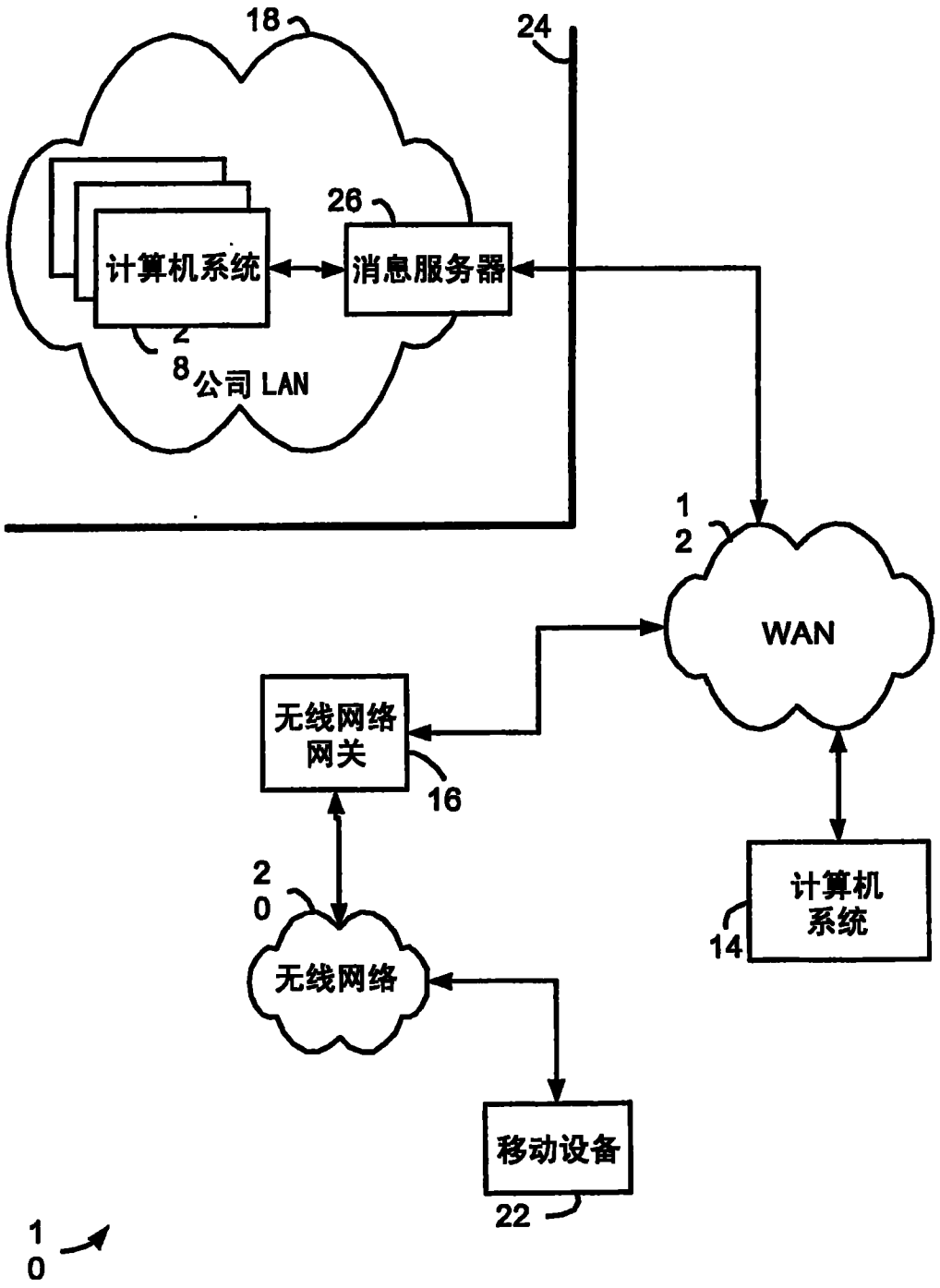

18
24
26
计算机系统
消息服务器
28
公司 LAN
12
WAN
无线网络
网关
16
20
无线网络
计算机
系统
14
移动设备
22
10

图 1

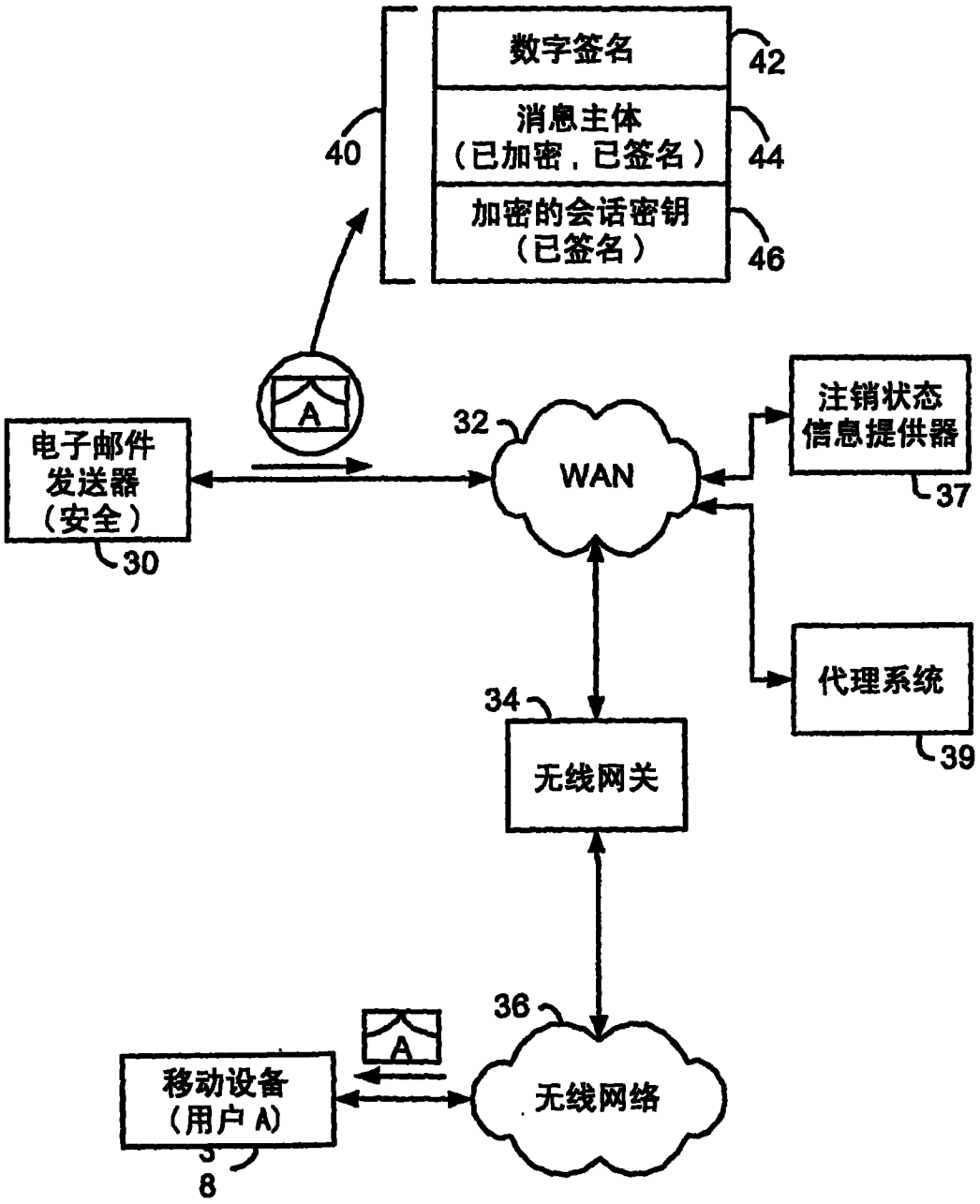

数字签名
42
消息主体
（已加密，已签名）
44
加密的会话密钥
（已签名）
46
40
A
电子邮件
发送器
（安全）
30
32
WAN
注销状态
信息提供器
37
代理系统
39
34
无线网关
36
A
移动设备
（用户 A）
无线网络

图 2

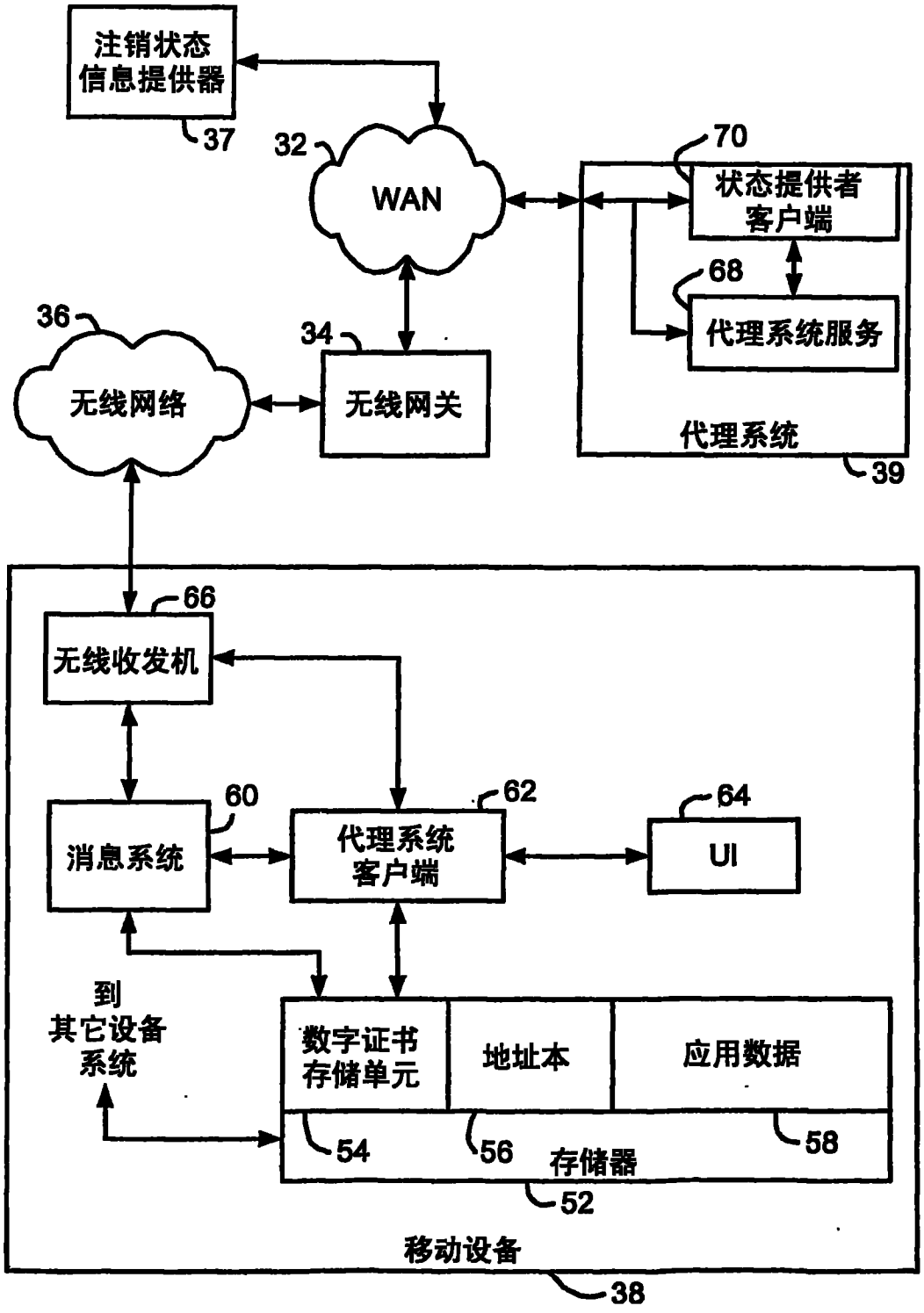

注销状态信息提供器
37
32
WAN
70
状态提供者客户端
68
代理系统服务
代理系统
39
36
无线网络
34
无线网关
66
无线收发机
60
消息系统
62
代理系统客户端
64
UI
到其它设备系统
数字证书存储单元
地址本
应用数据
54
56
存储器
58
52
移动设备
38

图 3

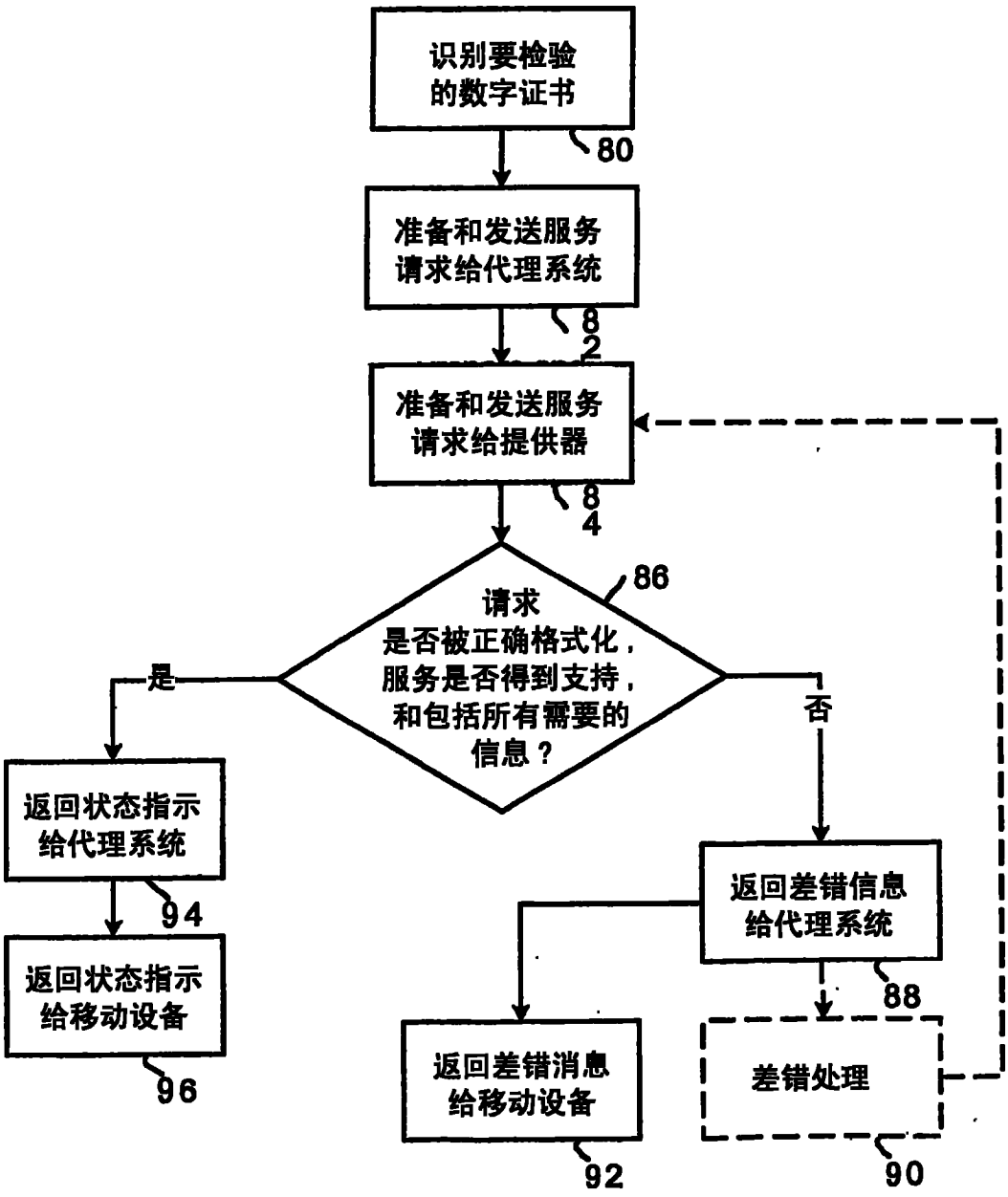

识别要检验的数字证书
80
准备和发送服务请求给代理系统
82
准备和发送服务请求给提供器
84
请求是否被正确格式化，服务是否得到支持，和包括所有需要的信息？
86
是
否
返回状态指示给代理系统
94
返回状态指示给移动设备
96
返回差错信息给代理系统
88
返回差错消息给移动设备
92
差错处理
90

图 4A

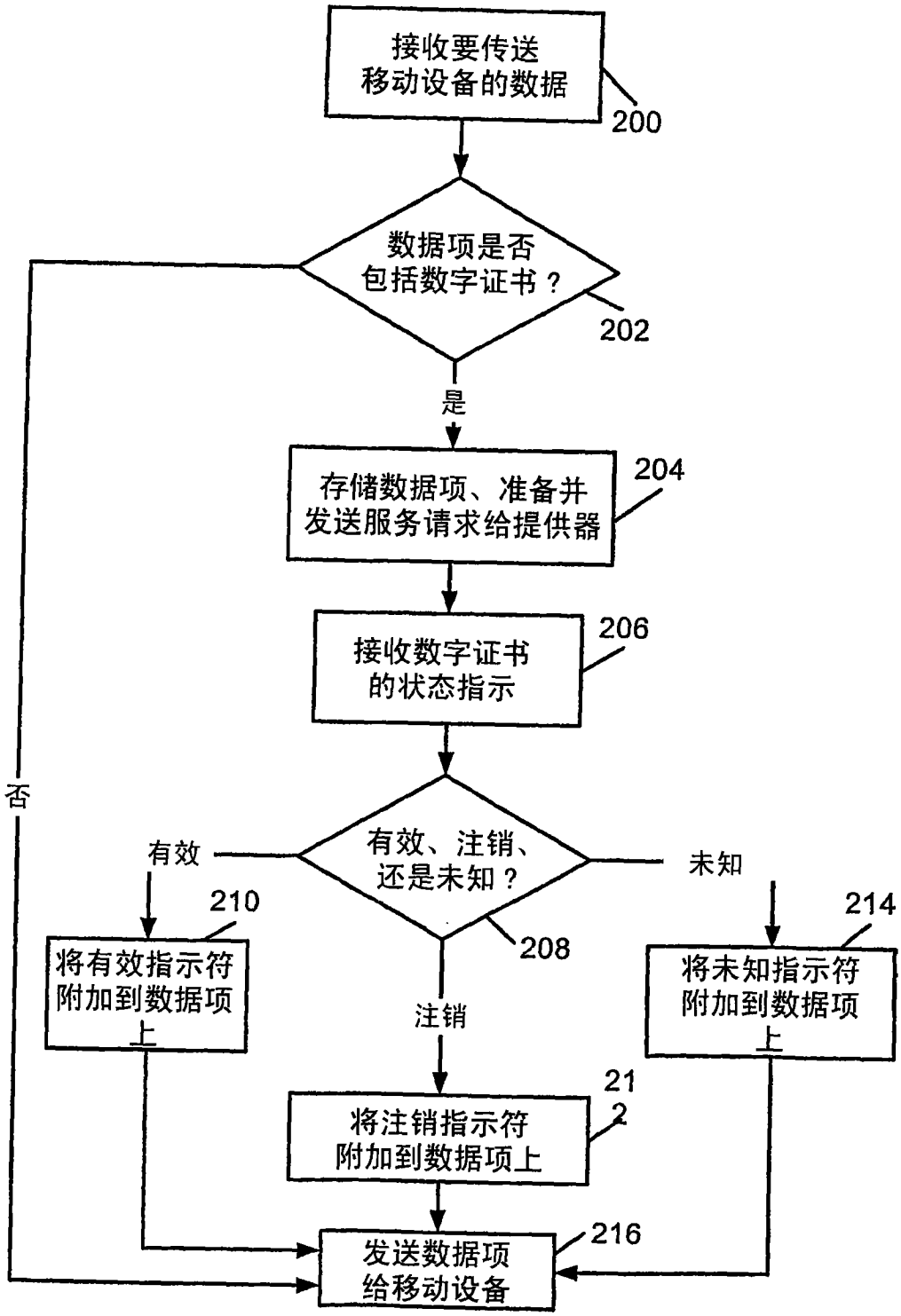

接收要传送移动设备的数据
200
数据项是否包括数字证书？
202
否
是
存储数据项、准备并发送服务请求给提供器
204
接收数字证书的状态指示
206
有效、注销、还是未知？
208
有效
未知
注销
210
将有效指示符附加到数据项上
214
将未知指示符附加到数据项上
212
将注销指示符附加到数据项上
216
发送数据项给移动设备

图 4B

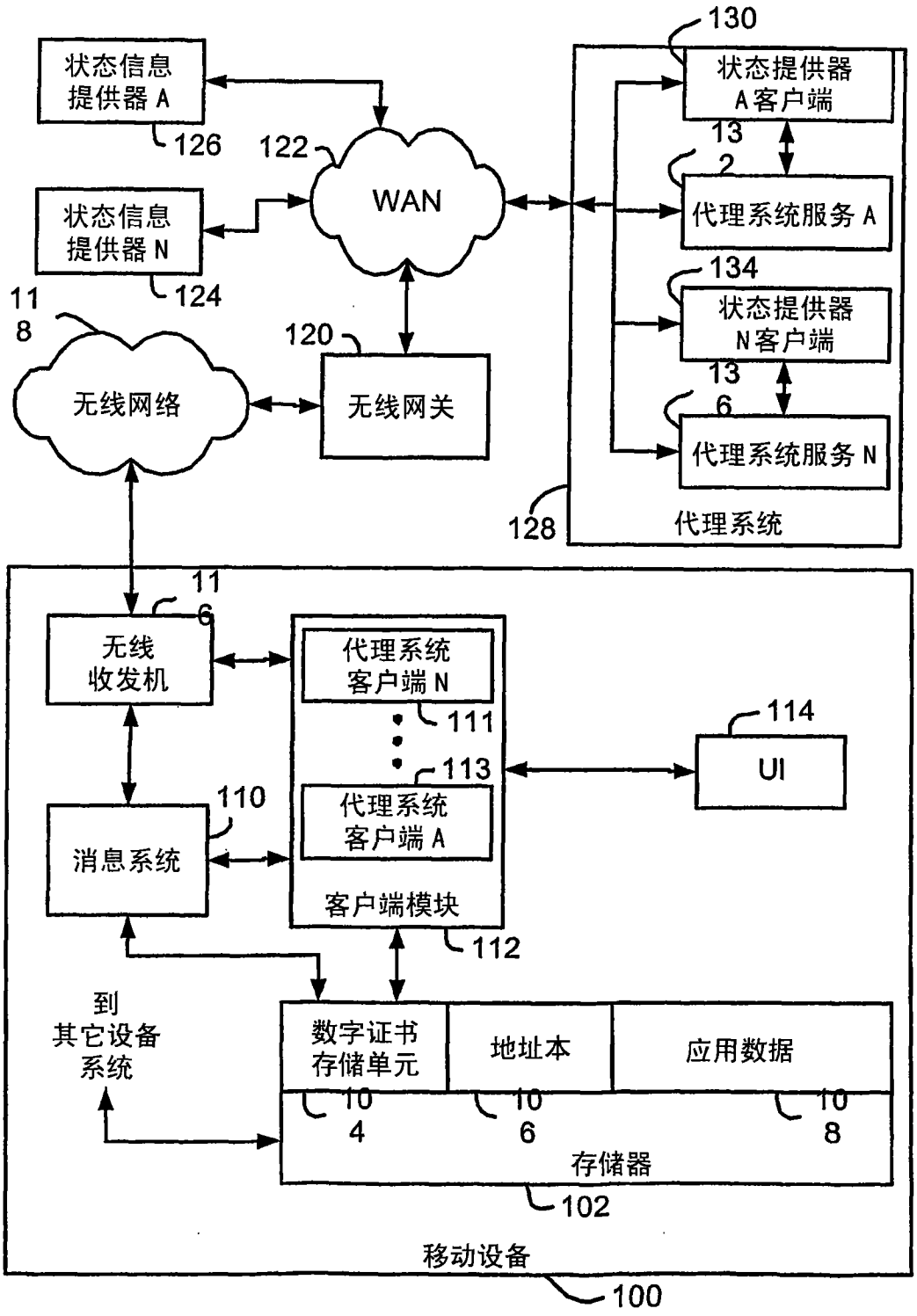

状态信息提供器 A
126
122
WAN
状态信息提供器 N
124
130
状态提供器 A客户端
132
代理系统服务 A
134
状态提供器 N客户端
136
代理系统服务 N
128
代理系统
118
无线网络
120
无线网关
116
无线收发机
代理系统客户端 N
111
113
代理系统客户端 A
客户端模块
112
114
UI
110
消息系统
到其它设备系统
数字证书存储单元
104
地址本
106
应用数据
108
存储器
102
移动设备
100

图 5

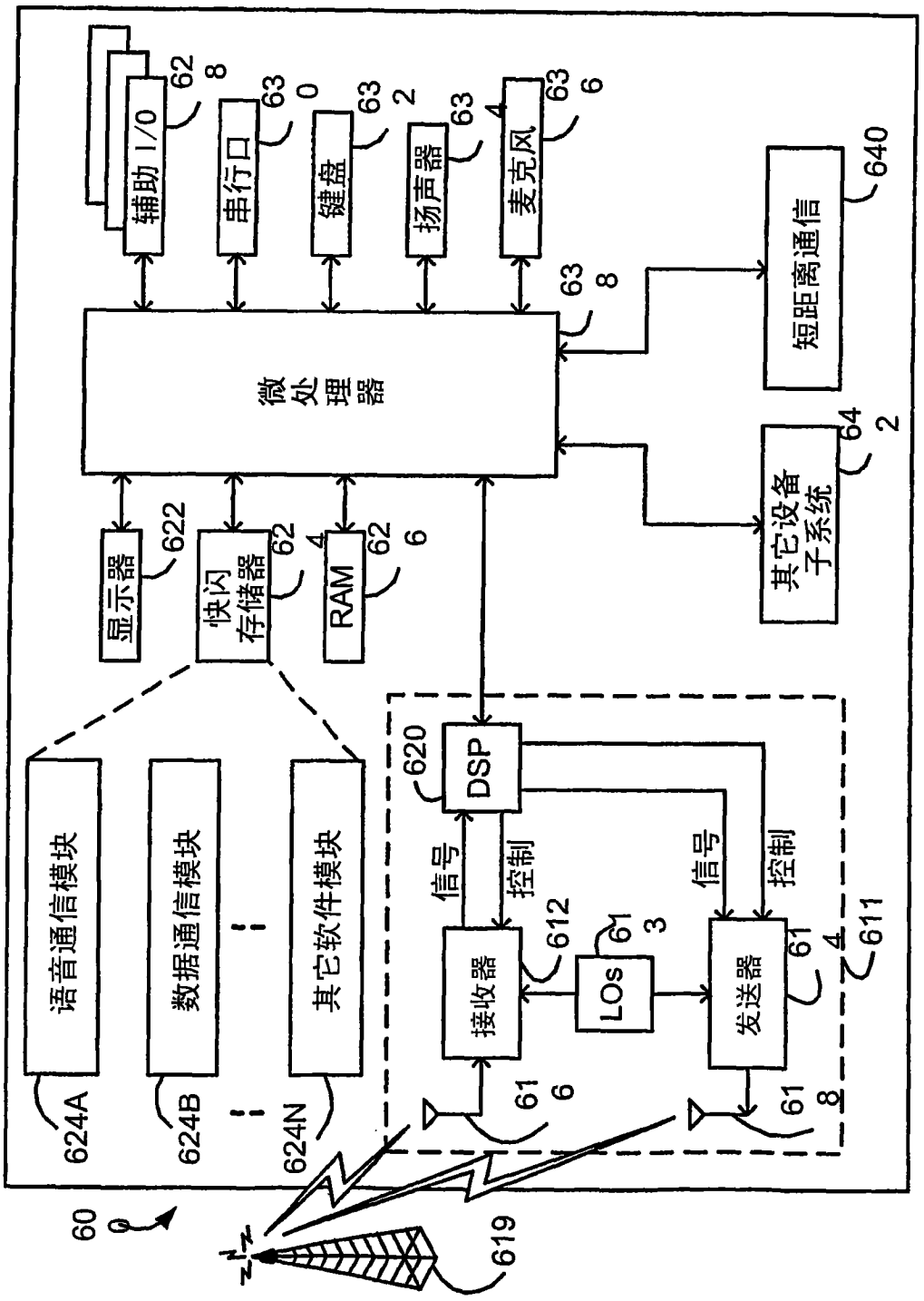

辅助 I/O
628
串行口
630
键盘
632
扬声器
634
麦克风
636
微处理器
638
短距离通信
640
其它设备子系统
642
显示器
622
快闪存储器
624
RAM
626
语音通信模块
624A
数据通信模块
624B
其它软件模块
624N
DSP
620
信号
控制
接收器
612
LOs
613
发送器
614
611
616
618
619
60

图 6

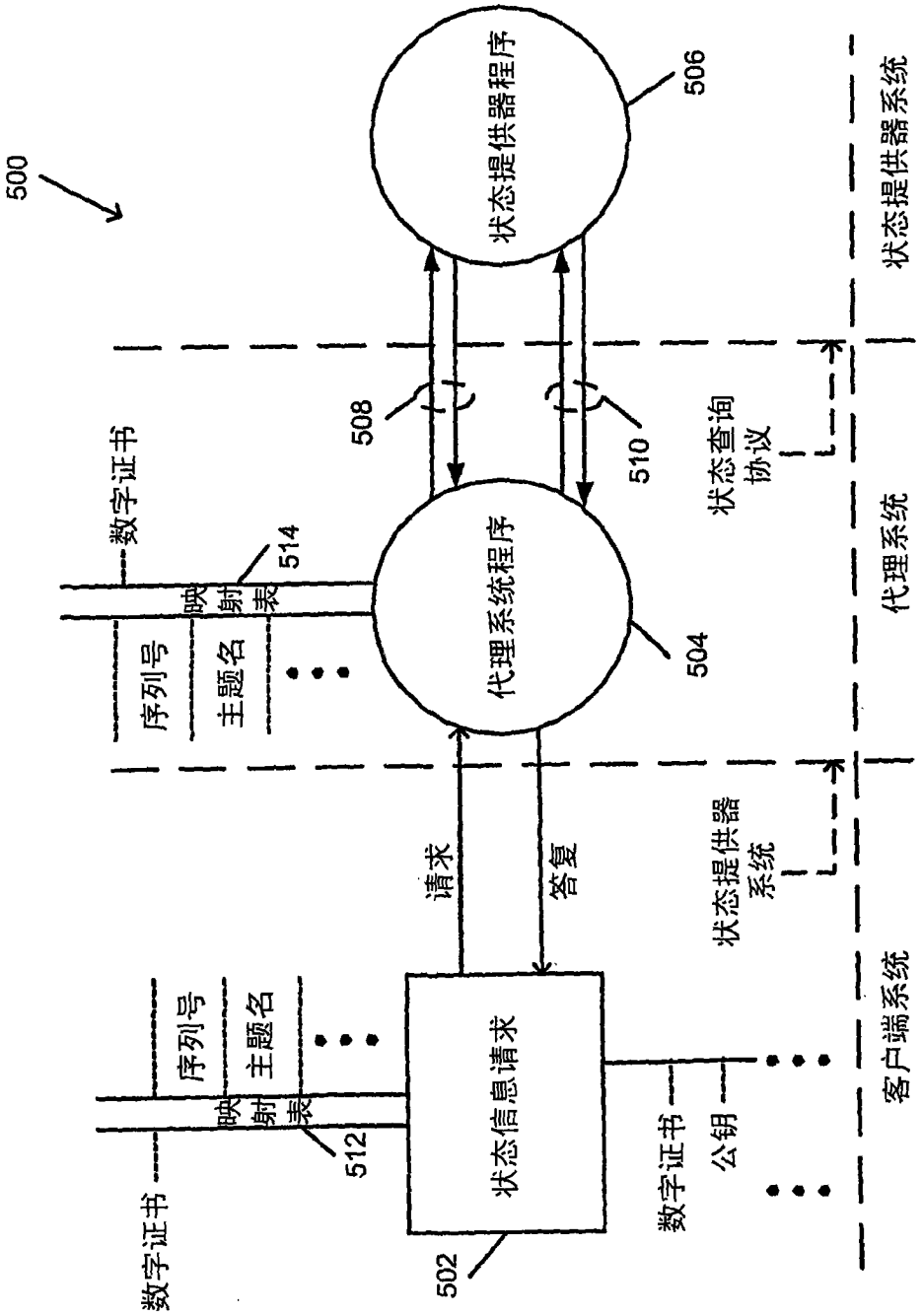

500
状态提供器程序
506
状态提供器系统
数字证书
508
510
状态查询协议
序列号
主题名
映射表
514
代理系统程序
504
代理系统
请求
答复
状态提供器系统
状态信息请求
512
数字证书
公钥
数字证书
502
客户端系统

图 7

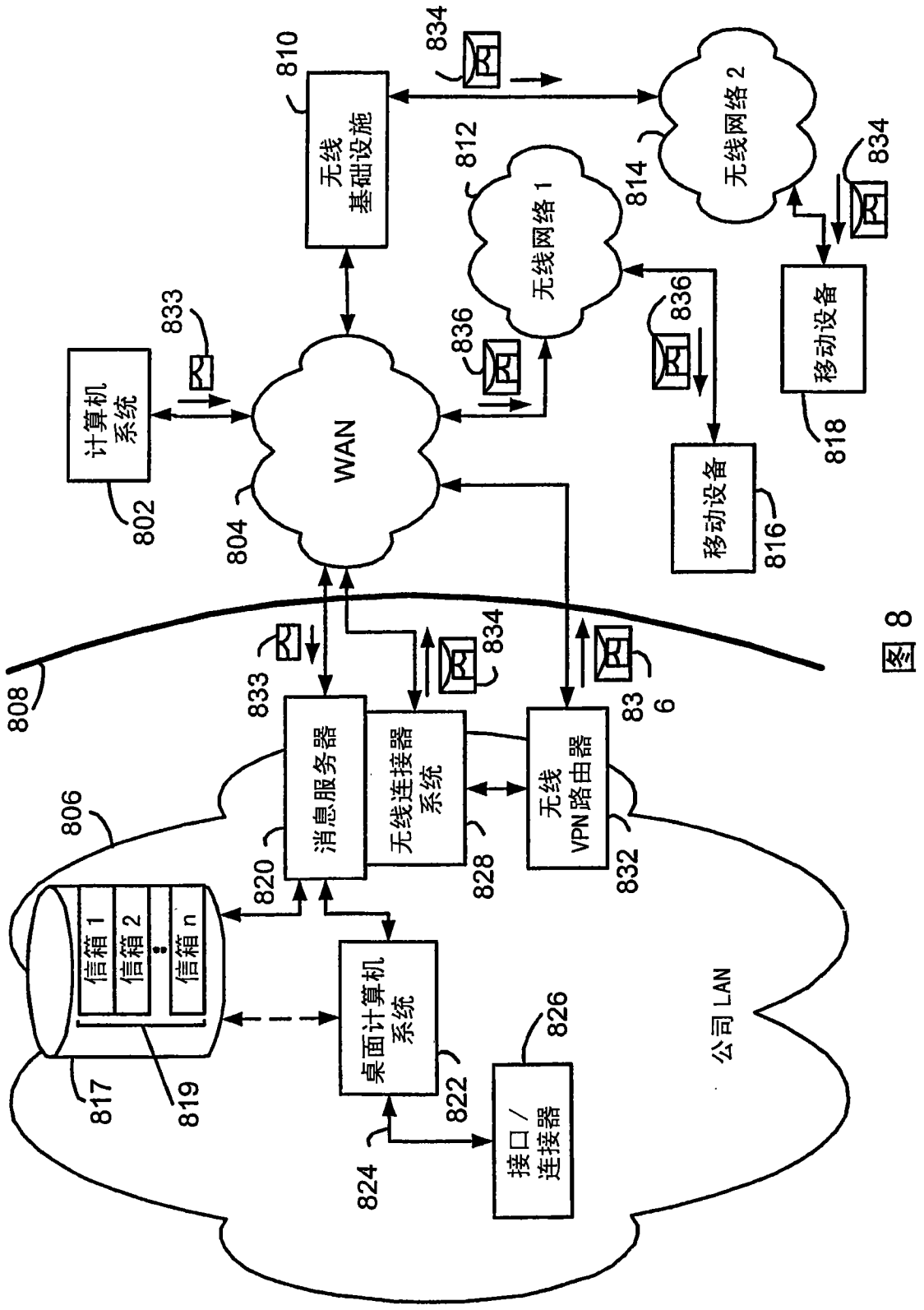

无线基础设施
810
834
无线网络 2
814
812
无线网络 1
836
833
计算机系统
802
WAN
804
移动设备
818
移动设备
816
808
消息服务器
820
无线连接器系统
828
无线 VPN 路由器
832
806
信箱 1
信箱 2
信箱 n
817
819
桌面计算机系统
822
824
接口 / 连接器
826
公司 LAN

图 8

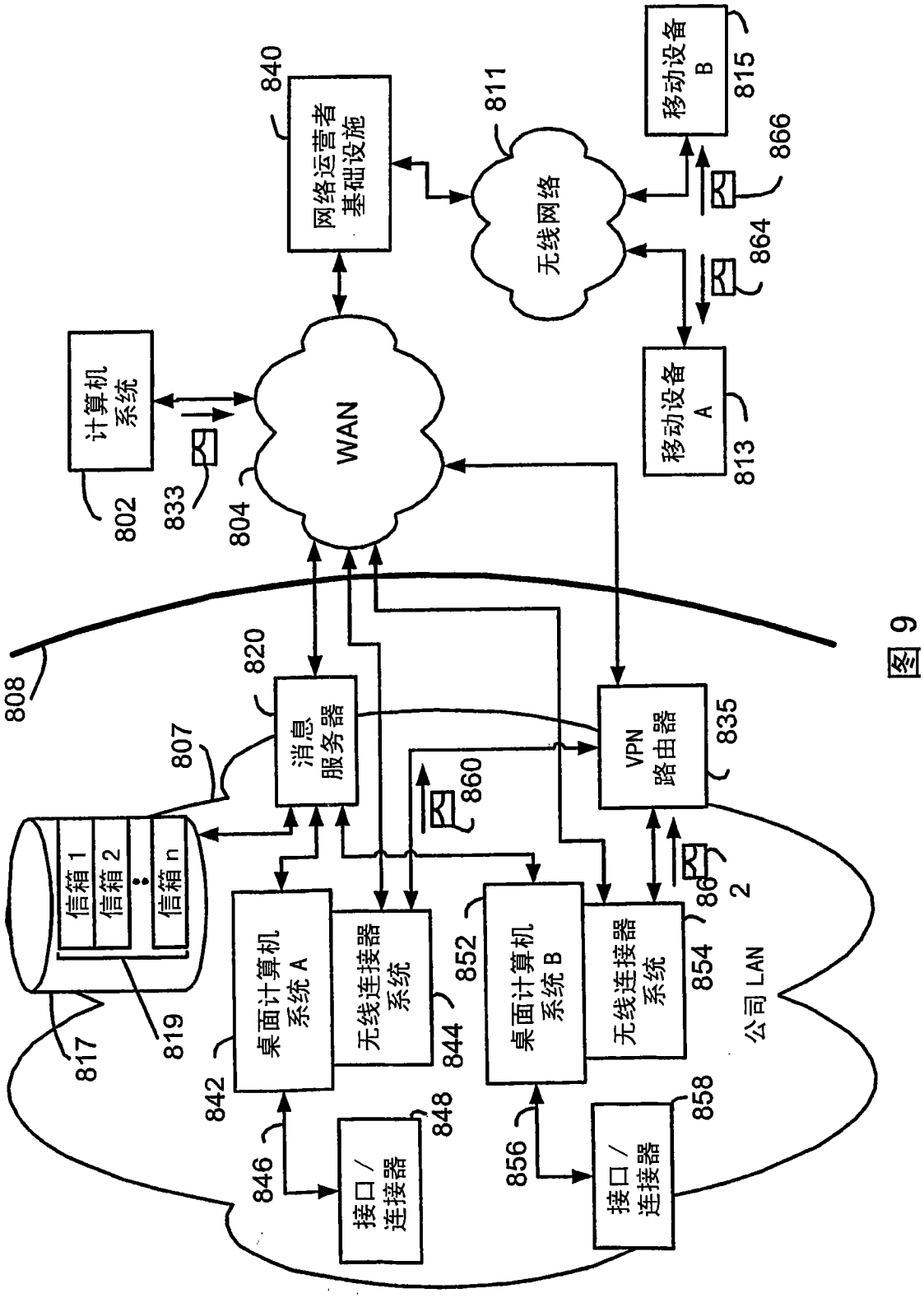

840
网络运营者基础设施
811
无线网络
移动设备 B
815
866
864
计算机系统
802
833
804
WAN
移动设备 A
813
808
820
消息服务器
807
VPN 路由器
835
860
862
信箱 1
信箱 2
信箱 n
817
819
桌面计算机系统 A
842
无线连接器系统
844
852
桌面计算机系统 B
854
无线连接器系统
公司 LAN
846
接口 / 连接器
848
856
接口 / 连接器
858

图 9

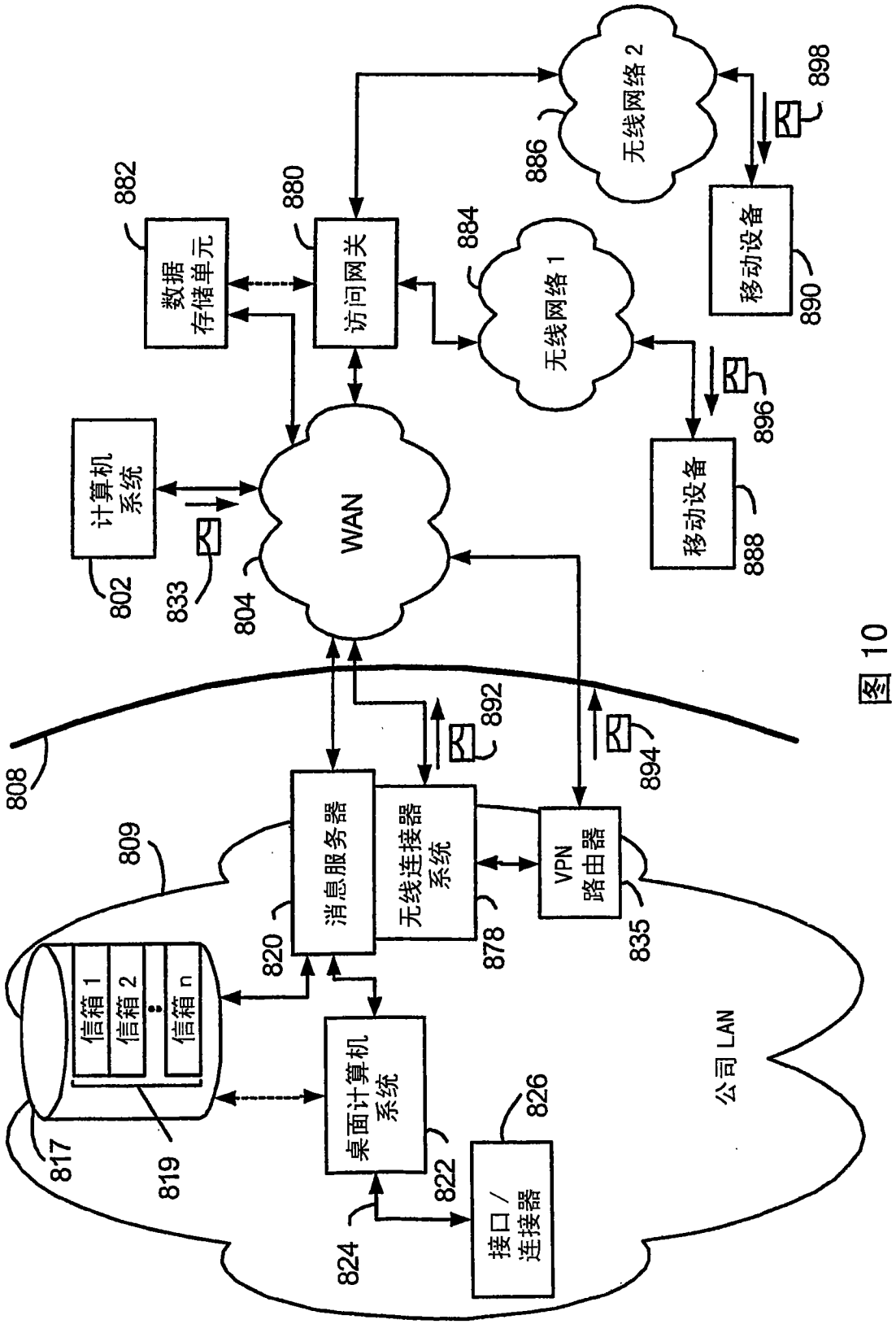

无线网络 2
886
898
882
880
884
数据存储单元
访问网关
无线网络 1
移动设备
890
896
计算机系统
WAN
移动设备
802
833
804
888
808
892
894
809
消息服务器
无线连接器系统
VPN 路由器
820
878
835
信箱 1
信箱 2
信箱 n
桌面计算机系统
公司 LAN
817
819
822
826
824
接口 / 连接器

图 10