



(12) 发明专利

(10) 授权公告号 CN 1729476 B

(45) 授权公告日 2010.05.05

(21) 申请号 200380106976.7

(51) Int. Cl.

(22) 申请日 2003.10.17

G06Q 10/00(2006.01)

H04L 12/58(2006.01)

(30) 优先权数据

G06F 9/44(2006.01)

60/419,103 2002.10.18 US

60/494,625 2003.08.12 US

(85) PCT申请进入国家阶段日

(56) 对比文件

WO 02/35869 A1, 2002.05.02, 全文.

2005.06.20

US 2002/0147778 A1, 2002.10.10, 全文.

CN 1258363 A, 2000.06.28, 全文.

(86) PCT申请的申请数据

PCT/CA2003/001583 2003.10.17

审查员 解欣

(87) PCT申请的公布数据

W02004/036419 EN 2004.04.29

(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 尼尔·P·亚当斯 迈克尔·S·布朗

赫伯特·A·利特尔

安东尼·F·希安 迈克尔·K·布朗

(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

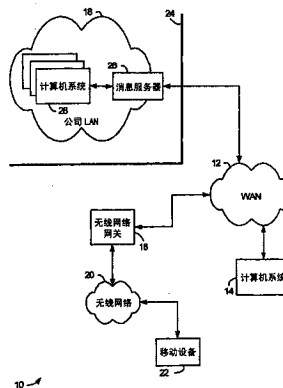
权利要求书 2 页 说明书 17 页 附图 6 页

(54) 发明名称

消息设置选择

(57) 摘要

提供了一种在消息传递客户程序上选择消息传递设置的系统和方法。当在所述消息传递客户程序上对输出消息进行编写时,被配置为与消息传递客户程序一同操作的显示屏显示包括消息部分和消息传递设置部分的编写屏幕。在所述编写屏幕的消息传递设置部分中显示被选为用于控制所述输出消息的消息特性的消息传递设置。



1. 一种在消息传递客户程序上选择消息传递设置的方法,所述方法包括步骤:
 - (a) 为编写输出消息提供消息编写接口,其中所述接口包括消息部分和消息传递设置部分;以及
 - (b) 从所述消息传递设置部分接收与正在所提供的消息编写接口中进行编写的所述输出消息相关联的消息传递设置。
2. 根据权利要求 1 的方法,进一步包括至少部分地基于已接收的消息传递设置来发送所述输出消息的步骤 (c)。
3. 根据权利要求 1 的方法,进一步包括在所提供接口的消息传递设置部分中显示所述已接收的消息传递设置的步骤 (c)。
4. 根据权利要求 3 的方法,进一步包括至少部分地基于已接收的消息传递设置来发送所述输出消息的步骤 (d)。
5. 根据权利要求 1 的方法,其中所接收的消息传递设置包括消息格式特性或消息保密特性。
6. 根据权利要求 5 的方法,其中所接收的消息传递设置包括用于加密的指示或者用于数字签名的指示。
7. 根据权利要求 1 的方法,进一步包括为多个消息传递设置重复步骤 (b) 的步骤 (c)。
8. 根据权利要求 7 的方法,其中所述多个消息传递设置中的每一个是消息格式特性或者消息保密特性。
9. 根据权利要求 1 的方法,其中用于所述输出消息的消息传递设置部分包括由用户修改的字段以指示在用于第一消息的消息设置中的变化,其中用于所述输出消息的已修改字段不会修改随后编写的输出消息的消息设置。
10. 根据权利要求 1 的方法,其中所述消息编写接口包括消息标题部分,其中所述消息标题部分包括 TO 字段和 SUBJECT 字段,其中所述消息标题部分包括所述消息传递设置部分。
11. 根据权利要求 10 的方法,进一步包括在所提供接口的消息编写部分的消息传递设置部分中显示所接收的消息传递设置的步骤 (c)。
12. 根据权利要求 1 的方法,其中所述消息部分包括用于允许用户输入消息的文本字段。
13. 根据权利要求 1 的方法,其中所述消息传递客户程序在桌上型电脑、笔记本电脑或移动计算设备上运行。
14. 一种在消息传递客户程序上用于选择消息传递设置的系统,所述系统包括:
 - (a) 用户输出设备适合于以终端用户可理解的方式来显示由系统处理器传递的数据;
 - (b) 用户输入设备适合于从终端用户接收数据,并且将所输入的数据传递到系统处理器;
 - (c) 系统处理器,其中所述系统处理器包括一个或多个处理元件,其中所述系统处理器与所述用户输入和输出设备进行通信,以及其中对所述一个或多个处理元件进行编程或其至少适合于:
 - (i) 使所述用户输出设备显示消息编写接口,其中所述接口包括消息部分和消息传递设置部分;

(ii) 经由所述用户输入设备接收消息传递设置；以及
(iii) 使所述用户输出设备在所述消息编写接口的消息传递设置部分中显示所接收的消息传递设置。

15. 根据权利要求 14 的系统,其中所述用户输出设备和所述用户输入设备是一个集成单元。

16. 根据权利要求 15 的系统,其中所述集成单元是一个触敏屏幕。

17. 根据权利要求 14 的系统,其中所述用户输出设备是可视显示屏、扬声器、触感显示屏或其组合。

18. 根据权利要求 17 的系统,其中所述用户输出设备包括液晶显示屏。

19. 根据权利要求 14 的系统,其中所述用户输入设备是触感输入设备、听觉输入设备或其组合。

20. 根据权利要求 19 的系统,其中所述用户输入设备是触敏垫、触敏屏幕、键盘、鼠标或其组合。

21. 根据权利要求 14 的系统,进一步包括 (d),无线收发信机与所述系统处理器进行通信,以及其中至少部分地基于所接收的消息传递设置,对所述系统处理器的一个或多个处理元件进一步进行编程或其至少适合于经由所述无线收发信机来发送输出消息。

22. 根据权利要求 14 的系统,进一步包括 (d),即数据存储器与所述系统处理器进行通信,以及其中对所述系统处理器的一个或多个处理元件进一步进行编程或其至少适合于 (iii) 将所接收的消息设置存储到所述数据存储器中。

消息设置选择

[0001] 相关申请的交叉引用

[0002] 按照 U. S. C35 条 § 119(e), 本申请要求于 2002 年 10 月 18 日提交的、标题为“MESSAGE SETTINGS SELECTION AND DISPLAY”的美国临时专利申请 No. 60/419103 的优先权, 并且要求于 2003 年 8 月 12 日提交的、标题为“MESSAGE SETTINGS SELECTION”的美国临时专利申请 No. 60/494625 的优先权, 作为参考的目的将上述申请引入到这里。

技术领域

[0003] 本申请一般涉及保密电子消息传递领域, 特别涉及在消息传递客户程序 (Messaging client) 上选择消息传递配置设置。

背景技术

[0004] 已知的保密消息传递软件客户程序 (诸如在桌上型计算机系统上运行的电子邮件软件应用程序) 一次仅使用一组消息传递设置 (Messagingsetting)。例如可以使用鼠标、键盘或者其它输入设备来建立消息传递设置, 以便配置在所有输出消息中出现的如格式、字体和通用文本这样的消息特性, 以及诸如消息签名和加密这样的保密消息传递特性。尽管用户可以建立多组设置, 但是在任何时候, 仅有一个预先选择的、作为当前或默认设置的组对消息传递客户程序的消息传递操作进行控制。为了对输出消息进行不同于当前设置中所建立的那些消息特性的配置, 必须覆盖当前的设置, 或必须选择另一组设置。这些操作可能很麻烦, 特别是在必须频繁地改变消息特性时, 例如在输出消息的收信人具有不同的消息传递能力时。

发明内容

[0005] 提供了一种在消息传递客户程序上为输出消息选择消息传递设置的方法。该方法包括步骤: 提供用于编写包含消息部分和消息传递设置部分的输出消息、以及接收用于控制一个或多个所述输出消息的消息特性的一个或多个消息传递设置。在某些情况下, 该方法还可以包括步骤: 在编写屏幕的消息传递设置部分中显示所接收的消息传递设置。该方法也可以包括步骤: 确定被寻址的所述输出消息接收者的记录是否存在于数据存储器中、并且基于在存有记录之处的记录来选择消息传递设置, 以控制所述输出消息的消息特性; 可以执行这些步骤来代替或附加接收一个或多个消息传递设置的步骤。该方法还可以包括至少部分地基于所接收的消息传递设置来发送所述输出消息。

[0006] 也提供了一种选择并显示消息传递设置的系统。该系统包括被配置以发送输出消息的消息传递客户程序, 所述每一个消息都具有消息特性; 以及被配置为与所述消息传递客户程序一同操作的显示屏。所述消息传递客户程序进一步被配置为: 当要在所述消息传递客户程序上编写输出消息时, 在所述显示屏上显示包含消息部分和消息传递设置部分的编写屏幕, 并且被配置为接收消息传递设置以控制所述输出消息的消息特性。某些这样的系统还可以包括用于存储包含一个或多个消息传递设置的记录的数据存储器。

附图说明

- [0007] 图 1 是消息传递系统的框图。
- [0008] 图 2 是示出了在消息传递系统中的保密电子邮件消息交换的框图。
- [0009] 图 3 是用于实现消息传递设置选择系统的无线移动通信设备的框图。
- [0010] 图 4 是示出了支持消息传递设置选择的系统和方法的一个实施例的编写屏幕的框图。
- [0011] 图 5-7 是示出了支持消息传递设置选择的系统和方法的另一个实施例的编写屏幕的框图。
- [0012] 图 8 是示出了编写屏幕和消息菜单的框图。
- [0013] 图 9 是示出了消息选项屏幕的框图。
- [0014] 图 10 是示出了在消息传递客户程序上选择消息传递设置的方法的流程图。
- [0015] 图 11 是无线移动通信设备的框图。

具体实施方式

[0016] 现在将详细描述各个实例。参考附图,整个说明书中同样的标号表示同样的部分。正如这里所使用的,“a”、“an”和“the”的意思包括多种参考(reference),除非上下文清楚地表明了其它的意思。同样,正如这里在说明书中所使用的,“in”的意思包括“in”和“on”,除非上下文清楚地表明了其它的意思。最后,正如在这里所使用的,“and”和“or”的意思都包括连接和转折而且可以交替使用,除非上下文清楚地表明了其它的意思;短语“exclusive or”可用于表明仅可以适用转折意思的情形。

[0017] 消息传递设置控制诸如用于不保密消息和保密消息的消息格式和字体这样的一般的消息特性。不保密消息例如包括通过因特网在消息传递客户程序之间进行交换的电子邮件消息。还通过建立消息设置来控制诸如消息签名和加密这样的保密消息特性。保密消息可以标有数字签名、可以被加密或者同时被签名和加密,而且还可以以其它方式、借助于消息发送者或者在消息发送者与接收所述保密消息的消息传递客户程序之间的中间系统对其进行处理。例如,保密消息包括根据安全多用途因特网邮件扩展(S/MIME)的变量,由消息发送者签名、加密而后签名、或者签名而后加密的消息。同样,可以在保密消息被签名和/或加密之前或之后对其进行编码、压缩或者其它的处理。所以,一组消息设置可以包括一般消息设置、保密消息设置或者二者都有。

[0018] 消息传递客户程序允许其所运行的系统接收并且还可能发送消息。消息传递客户程序在计算机系统、手持设备或者任何具有通信能力的其它系统或设备上运行。许多消息传递客户程序也具有附加的非消息传递功能。

[0019] 图 1 是消息传递系统的框图。系统 10 包括与计算机系统 14 相耦合的广域网(WAN) 12、无线网络网关 16 以及公司局域网(LAN) 18。无线网络网关 16 也与无线通信网络 20 相耦合,其中将无线移动通信设备 22 (“移动设备”)配置为可操作。

[0020] 计算机系统 14 是桌上型或者膝上型个人计算机(PC),其被配置为与 WAN12 进行通信,在大多数实现方案中,WAN12 是因特网。诸如计算机系统 14 这样的 PC 通常通过因特网服务提供商(ISP)、应用服务提供商(ASP)等接入因特网。

[0021] 公司 LAN18 是基于网络的消息传递客户端。其通常放置在安全防火墙 24 的后面。在公司 LAN18 内,在防火墙 24 后面的计算机上运行的消息服务器 26 为公司充当在 LAN18 内、以及经由 WAN12 与其它外部消息传递客户程序交换消息的主要接口。两种已知的消息服务器 26 是 Microsoft™ 交换服务器和 Lotus Domino™ 服务器。这些服务器 26 通常与路由并递送邮件消息的因特网邮件服务器一同使用。诸如消息服务器 26 这样的服务器还典型地提供附加功能,诸如用于日历、待办事项 (Todolist)、任务列表、电子邮件、电子文档等的动态数据库存储。

[0022] 消息服务器 26 具有将消息传递到与 LAN18 耦合的公司网络的计算机系统 28 的能力。典型的 LAN18 包括多个计算机系统 28,其中的每一个都运行消息传递客户程序,诸如 Microsoft Outlook™、Lotus Notes 等。在 LAN18 内,通过消息服务器 26 来接收消息,这些消息被分布到合适的邮箱,这些邮箱用于在已接收的消息中写明了地址的用户帐单,然后用户通过以消息传递客户程序来运行的计算机系统 28 对消息进行访问。

[0023] 无线网关 16 提供到无线网络 20 的一个接口,通过该接口与移动设备 22 交换消息。通过无线网关 16 来执行像移动设备 22 的寻址、对无线传输的消息进行编码或其它变换、以及任何其它所需的接口功能这样的功能。尽管在图 1 中,无线网关 16 与单一的无线网络 20 一同工作,但在可替换实施例中,可以将无线网关配置为与多个无线网络一同工作,在这种情况下,无线网关也可以确定用于定位一给定移动设备用户的最可能的网络,也可以当用户在地域或者网络间漫游时对其进行跟踪。

[0024] 可以使用 WAN12 的任何计算机系统 14、28 可以通过无线网络网关 16 与移动设备 22 交换消息。作为选择,诸如无线虚拟专用网 (VPN) 路由器这样的专用无线网络网关可实现用于向无线网络提供专用接口。例如,在 LAN18 中运行的无线 VPN 路由器将通过无线网络 20 提供从 LAN18 到诸如移动设备 22 这样的—个或多个移动设备的专用接口。通过提供与消息服务器 26 一同工作的消息转送或者重寄 (redirection) 系统,可以有效地将无线 VPN 路由器和其它类型的到移动设备 22 的专用接口扩展为 LAN18 之外的实体。这样一种重寄系统在美国专利 No. 6219694 中公开,其在此引入仅作参考。在这种类型的重寄系统中,通过无线网络接口、无线 VPN 路由器、无线网关 16、或者其它接口将由消息服务器 26 接收的并且寻址到移动设备 22 的用户的输入消息发送到无线网络 20 且发送到用户移动设备 22。另一个在消息服务器 26 上的到用户邮箱的可选接口是无线应用协议 (WAP) 网关,通过该网关,可以将消息服务器 26 上的用户邮箱中的一列消息、和各个可能的消息或者各个消息的一部分发送到移动设备 22。

[0025] 诸如无线网关 20 这样的无线网络通常经由基站和移动设备之间的 RF 传输将消息递送到移动设备 / 或者从移动设备递送消息。无线网络 20 例如可以是以数据为中心的无线网络、以语音为中心的无线网络、或者能够在相同的基础结构上支持语音和数据通信的双模网络。已知的以数据为中心的网络包括 Mobitex™ 无线网络 (“Mobitex”),以及 DataTAC™ 无线网络 (“DataTAC”)。已知的以语音为中心的数据网络的例子包括个人通信系统 (PCS) 网络,诸如全球移动数字通信系统 (GSM) 和时分多址 (TDMA) 系统。双模无线网络包括码分多址 (CDMA) 网络、通用分组无线业务 (GPRS) 网络、以及所谓的第三代 (3G) 网络,诸如当前正在开发中的全球演进增强型数据速率 (EDGE) 和通用移动通信系统 (UMTS)。

[0026] 移动设备 22 是数据通信设备、语音通信设备或者能够进行语音、数据和其它类型

通信的多模设备。下面将更加详细地描述一种示例性移动设备 22。

[0027] 当前使用的最普通的消息传递类型可能就是电子邮件。在标准电子邮件系统中,可能通过消息服务器和 / 或者服务提供商系统、由电子邮件发送者来发送电子邮件消息,然后在必要时,通过因特网路由到一个或者多个消息接收者。通常用一般的文字来发送电子邮件消息,而且所述电子邮件消息典型地使用简单邮件传输协议 (SMTP) 标题和多用途网际邮件扩充协议 (MIME) 实体部分来定义电子邮件消息的格式。

[0028] 近年来,已经开发了保密消息传递技术来保护诸如电子邮件消息这样的消息的内容和完整性。S/MIME 和 Pretty Good Privacy™ (PGP™) 是两种公共密钥保密电子邮件消息传递协议,其提供用于保护数据内容的加密和保护消息完整性、并且为发送者提供由消息接收者进行验证的签名。除了利用数字签名和可能的加密之外,还可以或可替换地对保密消息进行编码、压缩或者其它的处理。

[0029] 图 2 是示出了在消息传递系统中的保密电子邮件消息交换的框图。该系统包括与 WAN32 相耦合的电子邮件发送者 30,和无线网关 34,其提供 WAN32 与无线网络 36 之间的接口。移动设备 38 适合于在无线网络 36 内进行操作。

[0030] 电子邮件发送者 30 是诸如图 1 中的系统 14 这样的一台 PC,诸如图 1 中的计算机 28 这样的与网络连接的计算机;或者移动设备,消息传递客户程序在该移动设备上进行操作以使得能够编写并发送电子邮件消息。WAN32、无线网关 34、无线网络 36 以及移动设备 38 实际上与图 1 中类似标记的元件相同。

[0031] 在该示例性数字签名方案中,保密电子邮件消息发送者 30 通过采用消息摘要对消息进行签名,并且使用发送者的专用密钥对该摘要进行签名。例如可以通过执行较验和、循环冗余较验 (CRC)、散列 (hash) 或者某些其它对所述消息进行的不可逆操作来产生摘要。然后,由发送者使用所述发送者的专用密钥对所述摘要进行数字化签名。该专用密钥用于执行对所述摘要的加密或者某种其它的变换操作以产生数字签名。然后,将包括所述摘要和所述数字签名的数字签名附加到输出消息上。另外,发送者的数字认证 (Cert) 包括发送者的公共密钥、和必定作为具有一个或多个数字签名的公共密钥的发送者识别信息,并且所述输出消息通常还包括任何可能的链接 Certs 以及与该 Cert 和任何被链接的 Certs 相关联的认证撤销列表 (CRL)。

[0032] 由电子邮件发送者 30 发送的保密电子邮件消息 40 包括包含发送者 Cert、Cert 链接 (chain)、CRL 和数字签名的成分 42 以及被签名的消息体 44。在 S/MIME 保密消息传递技术中,Cert、CRL 和数字签名通常放置在图 2 所示消息的开始处,而消息体则包括在附件中。由其它保密消息传递方案产生的消息可以以不同于所示出的顺序来放置消息成分,或者包括附加的和 / 或不同的成分。例如,被签名的消息 40 可以包括寻址信息,诸如“To : ”和“From : ”电子邮件地址,以及图 2 中未示出的其它标题信息。

[0033] 当从电子邮件发送者 30 发送保密电子邮件消息 40 时,通过 WAN32 将所述电子邮件消息路由到无线网关 34,然后,通过无线网络 36 路由到移动设备 38。如上所述,电子邮件消息发送者可以选择性地将消息直接发送到无线网关、与移动设备相关联的计算机系统,或者发送到无线 VPN 路由器或者用于递送到移动设备的其它接口。

[0034] 被签名消息 40 的接收者,即移动设备 38 典型地通过产生消息体 44 的摘要、从所述数字签名 42 中提取被发送的摘要、将所产生的摘要与从数字签名 42 中提取的摘要相比

较、然后验证数字签名中的数字签名,对所述保密消息 40 中的数字签名 42 进行验证。由保密消息接收者使用的、用于产生已生成摘要的摘要算法与消息发送者使用的算法相同,而且通常在消息标题中、或者可能在所述保密消息的数字签名中进行规定。通常使用的摘要算法包括保密散列算法 1(Hash Algorithm)(SHA1)和消息摘要算法 5(MD5),尽管其它的摘要算法也可以使用。

[0035] 为了验证数字签名,接收者 38 通常通过从消息 40 上附带的发送者的 Cert42 中提取公共密钥来检索发送者 30 的公共密钥,然后通过对数字签名执行逆变换来验证所述数字签名中的关于摘要的签名。例如,如果消息发送者 30 通过使用其专用密钥对所述摘要进行加密来产生数字签名,则接收者 38 使用发送者的公共密钥来解密所述数字签名以恢复最初的摘要。图 2 中示出的保密消息 40 包括发送者的 Cert42,可以从中提取发送者的公共密钥。如果从较早的来自发送者 30 的消息中提取发送者的公共密钥,且将其存储到接收者本地存储器中的密钥存储器中,则可以改为从所述本地存储器中检索发送者的公共密钥。作为选择,可以从本地存储器中存储的发送者的 Cert 中、或者从公共密钥服务器(PKS)中检索公共密钥。PKS 是一个通常与认证授权(CA)相关联的服务器,从中可以得到包括实体公共密钥的实体的 Cert。PKS 可以驻留到公司的 LAN(诸如图 1 的 18)中,或者 WAN32、因特网或者消息接收者可以与 PKS 建立通信的其它网络或者系统上的任何位置。

[0036] 由接收者使用 Cert、Cert 链接和 CRL42,以确保发送者的 Cert 有效,即该 Cert 没有取消也没有过期,而且是可置信的。Cert 通常是 Cert 链接的一部分,其包括用户的 Cert 以及用于验证用户的 Cert 真实性的其它 Cert。例如,用于任何特定实体的 Cert 典型地包括实体的公共密钥和必定作为具有数字签名的公共密钥的识别信息。例如,当前使用的若干种 Cert 类型包括 X.509Cert,其典型地在 S/MIME 中使用,以及 PGP Cert,其格式稍微有些不同。通过 Cert 发行方来产生 Cert 中的数字签名,并且如上所述通过消息接收者对其进行较验。Cert 可以包括到期时间或者有效周期,消息传递客户程序根据该到期时间或者有效周期来确定所述 Cert 是否过期。当 CRL 有效时,针对该 CRL 来较验所述 Cert,以确保该 Cert 没有被撤销。

[0037] 如果验证了消息发送者的 Cert 中的数字签名,则该 Cert 没有过期也没有被撤销,并且通过消息接收者来确认 Cert 的发行方,然后通过消息接收者来确认该消息的数字签名。如果 Cert 的发行方没有被确认,则消息接收者通过 Cert 链接来跟踪验证路径,以较验在所述链接中的各个 Cert 通过其发行方进行签名(其 Cert 是该 Cert 链接中的下一个),直到发现由来自置信源(诸如大的 PKS)的根 Cert 签名的 Cert 为止。一旦发现了该根 Cert,就可以确认一个签名,因为发送者和接收者都确认了该根 Cert 的源。

[0038] 如果在签名之后由消息发送者对保密消息进行加密或者其它的处理,则在执行签名较验之前,各个接收者首先对所述消息进行解密或者执行其它的逆处理操作。然而,如果在签名之前执行加密或者其它的处理,则在签名较验之后执行诸如解密这样的逆处理。加密和解密包括将加密密钥和密码算法应用于要被加密或解密的信息。找到加密和 Cert,然后可以确认一个签名,因为发送者和接收者二者都对根 Cert 的源进行确认。

[0039] 如果在签名之后由消息发送者对保密消息进行加密或者进行其它的处理,则在执行签名较验之前,各个接收机首先对所述消息执行解密或者执行其它的逆处理操作。然而,如果在签名之前执行加密或者其它的处理,则在签名较验之后执行诸如解密这样的逆处

理。加密和解密包括将加密密钥和密码算法应用于要被加密或解密的信息。加密和解密使用可相同也可不同的相应密码算法、和要么相同要么不同的加密密钥。在公共密钥体系中，不同的密钥被用于加密和解密，而在“共享保密”型操作中，相同的密钥，即发送者和接收者之间共享的保密被用于加密和解密二者。

[0040] 在电子邮件发送者 30 处，由消息传递设置对保密消息传递特性和消息 40 中的消息签名进行控制。这些设置可以是默认消息传递设置，也可以是由用户或者由覆盖默认、或者当前消息传递设置建立的消息传递设置的当前选择的组。在已知的系统中，当从消息传递客户程序发送具有不同于在消息设置的当前组中规定的消息特性的消息时，必须选择消息传递设置的不同的组，或者必须覆盖当前的设置。

[0041] 频繁地改变消息传递设置不仅令人讨厌而且消耗时间，同时也容易出错。例如，将某些保密消息传递客户程序配置为与其它消息传递客户程序交换保密或者不保密消息。但是，没有为保密消息传递配置的消息传递客户程序不能处理所接收的保密消息。如上所述，已知的消息传递客户程序在任何时候仅允许一个消息传递设置组是有效的。因此，当保密消息传递客户程序与不保密消息传递客户程序相当频繁地交换消息时，保密消息传递客户程序的用户通常只将一般的消息传递设置选择为默认消息传递设置，以确保可以通过不保密消息传递客户程序来处理发送的消息。然后，当将保密消息发送到保密消息传递客户程序时，选择不同的设置组或者覆盖当前一般的消息传递设置，以便发送保密消息。当用户忘记选择保密消息传递设置或者忘记覆盖一般的消息传递设置时，就以不保密的方式来发送旨在保密发送的消息。例如，当这种消息包括机密信息时，就特别不希望出现这种情况。同样，在消息被发送到不保密消息设置客户程序的情况下将保密消息传递设置用作默认设置并且不被覆盖时，该不保密消息传递客户程序就不能处理保密消息，而且发送者必须以不保密的格式来重新发送消息。

[0042] 尽管某些已知消息传递客户程序通过在发送输出消息时提供多种消息发送选择来简化消息传递设置选择，但是消息传递设置选择仍然使用户容易出错。在这种消息传递客户程序中，通过用户来编写输出消息并且寻址到一个或者多个接收者。当从该消息传递客户程序发送输出消息时，用户选择一组消息传递设置来控制输出消息的消息特性，并且将所述消息发送到接收者，即使用户作出错误的或者不希望的消息传递设置选择。

[0043] 图 3 是运行消息传递设置选择系统的无线移动通信设备的框图。

[0044] 移动设备 38 包括存储器 52、消息传递客户程序 60、用户接口 (UI) 62、显示屏 63 和无线收发信机 64。

[0045] 存储器 52 是一种其它设备元件和系统将数据写入其中的、诸如 RAM 这样的可写入存储器，并且包括用于 Cert 存储器 54 的存储区域、其中存储消息传递联系信息的地址簿 56、存储与移动设备 38 上的软件应用程序相关联的数据的应用数据存储区域 58、以及存储消息传递设置的设置存储器 59。数据存储 54、56、58 和 59 是在移动设备 38 的存储器 52 中实现的存储器的示例性实例。除了图 3 示出的这些之外，存储器 52 还典型地由其它设备系统用于存储其它类型的数据。

[0046] 消息传递系统 60 与无线收发信机 64 相连，从而能够经由无线网络进行通信。

[0047] UI62 可以包括诸如键盘或者小键盘这样的 UI 元件，或者从移动设备 38 的用户接收输入、或者将输出提供给移动设备 38 的用户的其它元件。移动设备 38 典型地包括多个

UI, 因此 UI62 表示一个或者多个用户接口。

[0048] 在移动设备 38 中, 显示屏 63 典型地是液晶显示屏 (LCD), 尽管可以在移动设备中改为使用其它类型的显示屏。显示屏 63 也是用户接口, 但在图 3 中将其单独示出。

[0049] 消息传递客户程序 60 将所接收的 Cert 存储到 Cert 存储器 54 中, 并且从该 Cert 存储器 54 中检索被存储的 Cert。Cert 通常以其被接收的格式存储到 Cert 存储器 54 中, 但作为选择, 可以对其进行分析或以别的方式将其转化为在被写入 Cert 存储器 54 之前的存储格式。Cert 可以利用保密消息来接收, 从诸如 PKS 这样的 Cert 源经由无线收发信机 64 进行请求, 或者从例如 PC 这样的类似配置的外部系统通过诸如串行接口、通用串行总线 (USB) 端口、红外数据相关 (IrDA) 端口、或 Bluetooth™ 模块这样的通信接口将其加载到移动设备 38 上。如上所述, 可以请求 Cert 中的公共密钥来发送或接收保密消息。本领域的普通技术人员将理解, 能够用于保密通信的移动设备除了 Cert 存储器之外, 还可以包括用于存储加密密钥的单独的密钥存储器。

[0050] 地址簿 56 存储联系信息, 其中的至少某些在消息传递操作中由消息传递客户程序 60 使用。地址簿 56 中的条目典型地用于对在消息传递客户程序 60 上编写的消息进行寻址。当在显示屏 63 上将发送者接收的消息显示给移动设备 38 的用户时, 地址簿条目也可以用于以个人或亲属的名字来代替诸如电子邮件地址这样的寻址信息, 所述发送者存在于地址簿 56 的地址簿条目中。通常, 例如通过输入联系信息或者使用 UI62 从所接收的消息中选择一个地址来手动地创建地址簿条目, 或者通过在从没有条目存在于地址簿 56 的发送者接收消息时、对消息传递客户程序 60 进行配置以存储联系信息这样的方式来自动地创建地址簿条目。如上所述, 在所附的标题为“Certificate Information Storage System And Method”的美国专利申请序列 No. 60/356516 中, 在将新的 Cert 存储到 Cert 存储器 54 中时, 也可以提取联系信息并且将其存储到地址簿 56 中, 该申请已转让给本申请的受让人, 在此引用仅作参考。

[0051] 设置存储器 59 存储用于控制从移动设备 38 发送的输出消息特性的消息传递设置。在可替换的实施例中, 设置存储器 59 存储消息特性、或者设置和特性组合的指示符。尽管在已知系统中, 任何时候仅有一组先前选择的设置有效, 但设置存储器 59 也可以存储多组消息传递设置。已知的消息传递客户程序确定哪一组消息传递设置先前被选择, 并且使用那组设置来控制输出消息的消息特性。其它已知的消息传递客户程序要求用户在已经编写了输出消息并且准备发送时选择消息传递设置, 如上所述, 这容易使用户出错。

[0052] 然而, 将消息传递客户程序 60 配置为: 在要编写输出消息时, 为各个输出消息提供消息传递设置选择。在一个实施例中, 借助于用于输出消息的、包括消息部分和消息传递设置部分的编写屏幕能够显示附加的设置特性。

[0053] 图 4 是示出了支持消息传递设置选择的系统和方法的一个实施例的编写屏幕的框图。图 4 的框图同样支持对显示进行设置, 其是一个可选特性。编写屏幕 70 包括消息部分 74 和消息传递设置部分 72。编写屏幕 70 还包括“To :”行 80 和“Subject :”行 78。76 表示光标位置。

[0054] 消息部分 74 用于编写输出消息的消息文本。当用户在消息区域 74 中编写输出消息的消息文本时, 光标位于 76 所示的位置处。由用户输入的信息 (诸如通过使用键盘或者小键盘键入的字符) 例如被显示到编写屏幕 70 的当前光标位置处。类似地, 通过将光标放

置到“To:”行 80 和“Subject:”行 78 来分别输入接收者的地址和消息的主题。正如下面进一步详细描述,也可以从地址簿中检索输出消息的接收者地址。当正在编写的输入消息是与先前的消息相关的回复或者转发消息时,“To:”行 80、“Subject:”行 78 和消息部分 74 典型地预先填充有来自先前消息的相应信息。

[0055] 消息传递设置部分 72 显示当前选择的用于控制所述输出消息的消息特性的消息传递设置、或者一组消息传递设置的名称或其它标识符。在编写屏幕 70 上,当前选择一组称为“Home (S/MIME)”的消息传递设置。由于在编写屏幕 70 上显示了当前消息传递设置,所以用户就知道已为当前正在编写的输出消息选择的消息传递设置,因此不太可能发送不具有所希望消息特性的输出消息。如果当前选择的消息传递设置与所希望的消息特性不一致,则可能在发送输出消息之前或者发送输出消息之时为输出消息选择新的消息传递设置。

[0056] 参考图 3 和 4,可以使用诸如键盘和显示屏 63 这样的 UI62 在移动设置 38 上编写输出消息。将显示屏 63 配置为与消息传递客户程序 60 一同工作。将消息传递客户程序 60 配置为当准备编写输出消息时在显示屏 63 上显示编写屏幕 70。例如,用户可以从菜单选择“编写”、“转发消息”或者“回复消息”功能,并且将类似的命令发送到消息传递客户程序 60 以激活编写消息操作。

[0057] 如上所述,当正在编写的输出消息是转发或回复消息时,编写屏幕 70 中的至少“To:”行 80、消息部分 74 以及可能是“Subject:”行 78 包括来自先前消息的信息。对于最初的输出消息来说,“To:”行 80、“Subject:”行 78 和消息部分 74 是空白的。

[0058] 根据消息传递客户程序 60 的配置和能力,有若干种不同的方案可能用于选择消息传递设置。在一个实施例中,基于用于接收消息的消息传递设置来选择与先前接收的消息相关的任何消息的消息传递设置,并当接收消息被接收时存储在设置存储器中。例如,回复消息和转发消息是与已接收的消息相关的消息。例如,在一个移动设备支持的消息传递帐户(account)或者业务中接收消息的情况下,为与已接收消息相关的输出消息选择相同的消息传递帐目或者业务、以及可能用于已接收消息的其它消息传递设置。

[0059] 根据另一种消息传递设置选择方案,将消息传递客户程序 60 配置为保持用于先前已发送消息的消息传递设置的记录。在将消息传递客户程序 60 也配置为接收消息的情况下,可以类似地对用于已接收消息的消息传递设置进行记录。这种记录由消息接收者或消息发送者来标引,例如,将这种记录存储到地址簿 56、设置存储器 59 或者移动设备 38 上的其它存储器中。然后,在消息传递客户程序 60 为输出消息选择一组消息传递设置之前,协商该消息传递设置的记录。如上所述,尽管这里描述了存储的消息传递设置,但是对于输出消息来说,在选择消息传递设置中也可以或者改为记录和使用消息特性、或者可选择的特性。

[0060] 在通过消息接收者来标引消息传递设置的记录的情况下,消息传递客户程序 60 存储该消息接收者的标识符,诸如电子邮件地址、以及用于控制各个被发送消息的消息特性的消息传递设置或者一组消息传递设置的标识符。然后,基于被寻址的输出消息接收者来选择输出消息的消息传递设置,其中已在消息传递设置记录中存储了用于该接收者的一个条目。当要编写输出消息时,用户在编写屏幕 70 的“To:”行 80 中输入接收者信息。消息传递客户程序典型地支持若干种用于接收者信息输入的机制,包括使用键盘、小键盘或

者其它输入设备进行的手动地址输入,或者从地址簿 56 中选择接收者。地址传递客户程序 60 还可以允许用户输入名字或其它标识符,然后通过搜索地址簿 56、或者可能通过查询远端数据库将该名字或标识符转换为地址。通常在编写屏幕显示之后执行输出消息寻址操作,但也可能改为在编写屏幕显示之前,诸如在激活消息编写功能时通过提示用户接收者的信息来执行输出消息寻址操作。当在编写屏幕显示之前执行寻址操作、或者正在编写的输出消息是回复或者转发消息时,在首先显示编写屏幕 70 时在“To:”行 80 中显示接收地址或者名字至少其中之一。

[0061] 一旦将输出消息寻址到接收者,接收者的地址就在“To:”行 80 中显示。在编写屏幕 70 中,“To:”行 80 显示接收者的地址 user@domain.com。本领域的普通技术人员将理解,“To:”行可以改为显示与接收者地址相关联的亲属的名字,特别是当从地址簿 56 选择接收者地址、或者对应于接收者名字或地址的条目在地址簿 56 中被存储时。然后,消息传递客户程序 60 协商消息传递设置记录,以确定该记录是否包括用于先前发送到接收者的消息的一个条目。如果该记录包括用于先前发送到接收者的消息的一个条目,则为正在编写且在编写屏幕 70 的消息传递设置部分 72 中显示的输出消息选择消息传递设置记录条目中的消息传递设置。

[0062] 当消息传递客户程序在移动设备上运行时,如图 3 所示,存储器资源典型地受到限制。至少对于这些消息传递客户程序来说,为了确保存储器资源不被大量的消息传递设置记录所耗尽,希望建立最大尺寸和数量的用于消息传递设置记录的条目。尽管运行消息传递客户程序的桌上型和膝上型计算机系统实际上趋向于具有比移动设备更多的存储器资源,但是对于这些系统来说,消息传递设置记录尺寸的上限对于保存存储器资源是有利的。随着消息传递设置记录尺寸的增加,搜索时间也会增加。例如,已经发现在消息传递设置记录中的 128 个条目的限制提供了有效的消息传递设置选择操作,尽管可以改为使用其它的限制。

[0063] 对于具有限定尺寸的消息传递设置记录来说,仅保持确定数目 x 个条目。因此,这种消息传递设置记录不包括先前发送到输出消息接收者的消息的条目,除非所述先前发送的消息是最后发送的 x 个消息其中之一。当然,消息传递设置记录(不考虑其尺寸是否受限)不包括先前未将消息发送到接收者的一个接收者的条目。

[0064] 选择并在消息传递设置部分 72 中显示默认消息传递设置(即最近选择的消息传递设置)、或者在用于其它消息接收者的消息传递设置记录中出现的消息传递设置,该其它的消息接收者具有与正在编写的输出消息的接收者相同的域名(即图 4 中的“domain.com”),其中消息传递设置记录不包括先前被发送到所述接收者的消息的一个条目。作为选择,可以将消息传递客户程序 60 配置为:促使用户选择要用于在这种情况下的输出消息的消息传递设置,然后将所选的消息传递设置或其指示显示在消息传递设置部分 72 中。

[0065] 如图 4 所示,已经为输出消息选择了称为“Home(S/MIME)”的消息传递设置。在该实例中,“Home”表示将消息传递客户程序 60 和移动设备 38 配置为以其进行操作的消息传递帐目或者业务,而“S/MIME”表示应用于该输出消息的编码类型。因此,将使用 S/MIME 的变量、经由“Home”消息传递业务来发送图 4 中示出的测试消息。当消息传递客户程序 60 和移动设备 38 能够与多个消息传递帐目或者业务进行操作时,这种类型的命名协定特别有用,正如下面进一步详细描述,尽管其它的命名协定也是可能的。

[0066] 在正在编写输出消息的同时在编写屏幕 70 的消息传递设置部分 72 中显示消息传递设置的情况下,消息传递客户程序 60 的用户注意到在将输出消息发送到接收者时用于控制该输出消息的消息特性的该消息传递设置。将该消息传递设置显示给用户,同时对输出消息进行编写,这为用户提供了用于确定所述消息传递设置是否将为该输出消息产生所希望的消息传递特性的机会。如果由消息传递客户程序 60 选择的消息传递设置导致在发送该输出消息时、该输出消息具有所希望的消息特性,则用户仅需要激活发送功能或命令,而不必首先选择消息传递设置。

[0067] 与已发送和 / 或接收的消息相关的消息设置或特性的存储或高速缓存提供了一种用于跟踪和使用信息的装置,该信息是与用户进行通信的人们的信息。例如,用户可能希望能够跟踪其它人优选使用的加密算法,而不管这些人是否正常地对它们的消息或者其它相关的信息进行了签名。数据存储器保持对不同接收者、发送者或者二者的相关设置或者特性进行跟踪。然后,消息传递客户程序使用已存储的信息对默认的、以及允许将来与特定的人进行通信的行为做出选择。

[0068] 优选地,数据存储器存储加密算法的优先选择。例如在 S/MIME 中,要求 TripleDES 和 RC2 的支持。然而,输出消息的接收者也可以支持 AES,其是一种更强的算法。在该实例中,能够通过确定发送者的 S/MIME 能力、根据所接收的消息来选择 AES。然后存储该信息,用户下次将该消息发送到那个发送者(作为用于发送消息的接收者),询问数据存储器。如果那个接收者支持 AES,则该消息传递客户程序默认使用该算法。

[0069] 另一种被优选存储的设置或者特性是:接收者是否在它们的保密电子邮件中支持压缩。如上所述,实际上用于加密的算法可以实现这个目的。

[0070] 数据存储器或者高速缓存最好也跟踪来自各个接收者的最后通信的“式样”。如果从输出消息接收者接收的最后通信使用 PGP,则将其存储。对于接下来寻址到该接收者的输出消息来说,可以选择 PGP。可以以类似的方式对接收者最后使用的“动作”进行跟踪。如果对从接收者接收的最后的电子邮件进行签名和加密,则接收者也将优选地对随后的电子邮件进行签名和加密。

[0071] 如上所述,优选地根据先前使用的消息传递设置或默认消息传递设置来选择消息传递设置。然而,对于输出消息来说,可以按照顺序要求不同的消息传递设置,以便在发送输出消息时具有所希望的消息特性。同样如上所述,根据消息传递客户程序 60 的配置,可以在发送输出消息时选择不同的消息传递设置。对于其它消息传递客户程序来说,典型地,用户必须中断或中止编写操作、或者保存正在编写的消息同时终止编写操作,以便选择不同的消息传递设置。然后,将新的消息传递设置显示在编写屏幕 70 的消息传递设置部分 72 中,并且将其用于控制输出消息的消息特性。

[0072] 图 5-7 是示出了支持消息传递设置选择的系统和方法的另一个实施例的编写屏幕的框图。图 5-7 中的编写屏幕 71 类似于图 4 中的编写屏幕 70,并且包括其中显示已选消息传递设置的消息传递设置部分 73、和用于编写输出消息的消息文本的消息部分 75。然而,在编写屏幕 71 中,消息传递设置部分 73 包括消息传递设置选择字段 82。

[0073] 使用编写屏幕 71 的编写消息操作实际上与上述编写屏幕 70 一样。当用户使用消息传递客户程序(图 3)激活编写消息特性或功能时,编写屏幕 71 在显示屏 63 上显示。通过将光标定位到编写屏幕 71 上的合适位置,来输入或选择信息并且将其显示在“To:”行、

“Subject:”行和消息部分 75 中。也可以根据上述任何一种技术来选择用于在编写屏幕 71 的消息传递设置部分 73 中显示的最初的消息传递设置。

[0074] 在为了产生正在编写的输出消息所希望的消息特性、而必须改变在消息传递设置部分 73 中显示的所选消息传递设置时,消息传递设置选择字段 82 简化不同消息传递设置的选择。必要时,使用消息传递设置选择字段 82 从编写屏幕 71 中选择新的消息传递设置。如图 5 所示,无论用户何时确定要求不同的消息传递设置,用户都将光标定位到消息传递设置选择字段 82 中。

[0075] 一旦将光标定位到消息传递设置选择字段 82 中,用户就输入或选择新的消息传递设置。在一个实施例中,当光标被定位到消息传递设置选择字段 82 中时,操作诸如功能键或指轮这样的输入设备来显示有效消息传递设置的一个菜单,如图 6 中的 84 所示。然后,通过将光标定位到菜单条目并且操作输入设备来选择消息传递设置。例如,可以通过滚动指轮将光标定位到消息传递设置选择字段 82,通过按压该指轮可以显示菜单 84,然后通过滚动该指轮以将光标移到菜单 84 的一个特定条目、同时按压该指轮来选择消息传递设置。

[0076] 在图 6 中,在菜单 84 中列出了多个消息传递设置。如上所述,名称“Home (S/MIME)”表示:将消息传递客户程序 60 和移动设备 38 配置为以其进行操作的消息传递帐目或者业务,以及 S/MIME 编码方案。根据消息传递客户程序 60 的类型和能力,多种类型的编码方案可能对消息传递帐目或业务是有效的。对于“Home”消息传递业务来说,S/MIME、PGP 以及不保密或者原文编码是有效的。例如,可以与商业或者工作邮件帐目相关联的“Desktop”消息传递业务也支持不保密的、PGP 及 S/MIME 编码。对本领域的普通技术人员显而易见的是,菜单 84 和消息传递设置选择字段 82 在输出消息被编辑的同时彻底地简化了新的消息传递设置的选择。

[0077] 由消息传递客户程序 60 根据移动设备 38 的配置对菜单 84 进行填充。消息传递客户程序 60 确定将移动电话 38 配置为以其进行操作的消息传递业务。在图 6 中,“Home”和“Desktop”消息传递业务是有效的,并且在消息传递设置菜单中示出。消息传递客户程序 60 还通过确定哪一个编码器对于移动设备 38 是有效的,来确定支持消息传递业务的编码类型,并且将各个编码器都配置为以该消息传递业务中的一个进行操作。例如,当编码方案是基于公共密钥的保密消息传递方案时,消息传递客户程序 60 要为消息传递业务确定已经将专用密钥加载到移动设备 38 的密钥存储器中。如果不同的身份或者消息传递地址与各个消息传递业务相关联,如通常的情况是,使用这种业务的保密消息传递一般就需要不同的专用加密和签名密钥。只有当这种编码实际上对于那种业务有效时,才优选地在用于消息传递业务的消息传递设置菜单中列出这种类型的编码。换句话说,用户可以选择不能使用的消息传递业务和编码组合。

[0078] 如果消息传递业务允许或支持例如用于不保密消息传递的明文编码 (plaintext encoding),则如图 6 所示,该服务的名称将显示到菜单 84 中。各种业务的名称可以与该业务名称后面的括号中标识的、该业务支持的其它编码类型的编码方法一起显示在菜单 84 中。在图 6 中,“Desktop”和“Home”这两种业务支持 PGP 和 S/MIME。本领域的普通技术人员将理解,特殊的显示方案或者命名协定可以不同于图 6 中出于示例性目的而给出的(方案)。还可以使用例如由移动设备 38 的生产商控制的、消息传递客户程序 60 的开发人员建

立的、或者可能由移动设备 38 的用户配置的其它菜单和显示格式。

[0079] 图 7 示出了具有消息菜单 88 的编写屏幕 71。可以在编写输出消息的同时、或者已经编写完输出消息并将其发送之后由用户来显示消息菜单 88。例如,用户可以通过操作功能键或者输入设备来显示消息菜单 88。在指轮作为输入设备的上述例子中,可以通过滚动指轮将光标定位到编写屏幕 71 的消息部分 75、“To:”行或者“Subject:”行中、而后按压该指轮来显示消息菜单 88。正如所示出的,消息菜单 88 包括多项功能,包括用于关闭消息菜单 88 的“Hide Menu”功能、使用户高亮显示消息中的文本的“Select”功能、发送消息的“Send”功能、在不发送消息的情况下将消息保存到存储器中的“Save Draft”功能、将“To:”、“Cc:”和“Bcc.”地址加到消息中的“Add”功能、将地址簿中的地址附加到消息上的“AttachAddress”功能、当显示消息菜单 88 时用于清除光标位置处区域的内容(即图 7 中的消息部分 75)的“Clear Field”功能、用于显示消息选项的“Options”功能 88、以及用于取消编写操作的“Cancel”功能。本领域的普通技术人员将理解,仅仅出于示例性目的而给出消息菜单 88,此外,也可以在消息菜单或类似的菜单中得到较少的、或者不同的功能。

[0080] 如上所述,消息传递设置选择字段 82 使用户在编写消息的同时能够选择消息传递设置,所以仅有一个“Send”功能需要包括在消息菜单 88 中。如图 4 所示,如果消息传递客户程序实现了用于选择消息传递设置、并在编写屏幕 70 的消息传递设置部分 80 中显示所选消息传递设置的消息传递选择和显示系统,则可以在消息菜单中包括多个“Send”功能、和用于各个有效的消息传递业务和编码类型的功能,以允许用户在消息发送之前选择新的消息管理设置。当激活“Send”功能时,消息传递客户程序 60 处理并经由无线收发信机 64、无线网络和可能的其它通信链路及网络将输出消息发送到所寻址的输出消息的接收者。消息传递客户程序 60 例如在发送输出消息之前,根据所选的消息传递设置执行处理操作,诸如加密和数字签名。消息传递客户程序 60 也可以执行诸如数据压缩、或将输出消息重新装配为电子封装这样的操作,以便通过与运行消息传递客户 60 的移动设备 80 相关联的主机系统将所述电子封装传送到消息接收者。

[0081] 也可以通过使用消息菜单 88 上的“选项”功能选择消息选项来选择或控制某些用于输出消息的消息特性。图 8 是示出了编写屏幕和消息菜单的框图。与图 7 中一样,在图 8 中,消息菜单 88 包括多项功能。例如,通过将光标定位到菜单中的特定条目然后选择该条目、通过滚动然后按压指轮来激活各项功能。在图 8 中,如 92 所示选择“Options”功能。

[0082] 图 9 示出了消息选项屏幕的框图。当在消息菜单 88 上选择“options”功能时,显示消息选项屏幕 94。正如所示出的,当前正在编写的输出消息具有“Normal”重要性级别,将使用具有“S/MIME”编码的“Home”消息传递业务对其进行发送,并将仅在发送之前对其进行加密。由于当前的“Home(S/MIME)”消息传递设置规定了将对消息进行加密,所以消息选项屏幕 94 还将显示加密选项。当不对正在编写的输出消息进行加密时,可以或者不必显示这些选项。但同样或者改为对输出消息进行数字化签名时,类似地可以在消息选项屏幕中显示签名选项。

[0083] 在消息选项屏幕 94 中,至少可以选择重要性级别。因此,显示重要性级别的消息选项屏幕 94 部分优选地包括用于选择重要性级别的消息重要性级别选项字段。例如,可以从重要性级别菜单中选择重要性级别。如上所述,实际上可以在光标定位到重要性级别选择字段时通过操作功能键或其它输入设备来显示重要性级别菜单。在多个用于特定消息传

递业务或编码类型的这种动作有效的情况下,还可以以类似的方式来选择除了用于特定消息传递业务或编码类型的默认动作之外的其它动作。在 S/MIME 编码的例子中,仅加密、仅签名、加密而后签名以及签名而后加密,都是可以对输出消息有效的 S/MIME 的变量。消息选项屏幕 94 的编码动作显示部分可以包括一个选择字段,通过该选择字段可以指定或选择编码动作。

[0084] 另外,或者作为替代,可以从消息选项屏幕 84 中选择消息传递设置。最后,在图 9 中的“Using”行中的消息选项屏幕 94 的消息传递设置部分优选地包括消息设置选择字段 96。从而不仅通过消息设置选择字段 96 来显示消息传递设置,而且该消息传递设置还是可选择的。优选地,从消息设置选择字段 96 中选择消息传递设置实际上与上述消息传递设置选择字段 82 中的一样。可以从编写屏幕 71 的消息传递设置部分中的消息传递设置字段 82(图 5)、或者从消息选项屏幕 94 中的消息传递设置字段 96 中激活消息传递设置菜单 84。例如在设置或者类似的数据存储器中不存在消息接收者的记录时,使用以这种方式选择的消息传递设置。

[0085] 图 10 是示出了在消息传递客户程序上选择并显示消息传递设置的方法的流程图。与显示所选消息传递设置相关联的操作是可选择的。

[0086] 在步骤 100 和 102,用户开始编写消息操作并且对正在编写的输出消息进行寻址。如上所述,可以在开始编写消息操作之前或者编写消息的同时将输出消息寻址到消息接收者。从地址簿中选择的、或者当该消息是回复消息时自动选择的的消息接收者典型地由用户手动输入。当准备编写消息时,显示包括消息传递设置部分和消息部分的编写屏幕。

[0087] 为了选择用于输出消息的最初的消息传递设置,消息传递客户程序在步骤 104 优选地确定先前消息的记录是否包括与消息接收者相关联的一个条目,所述先前消息至少包括已接收的消息和可能发送的消息。如果所述记录不包括与任何消息接收者相关联的条目,则在步骤 106 选择默认消息传递设置,同时在步骤 108 处,在编写屏幕的消息传递设置部分中显示该默认消息传递设置。

[0088] 如果所述记录包括与消息接收者相关联的一个条目,则最初的消息传递设置选择优选地以该条目为基础,或者如果发现了多个条目,则以这些条目的其中一个为基础。在步骤 110,消息传递客户程序确定是否存在设置冲突。在步骤 104,如果在消息记录中仅发现了一个条目,则不存在冲突,在步骤 112,从该记录中选择先前的消息传递设置,并且在步骤 108,在编写屏幕的消息传递设置部分中对其进行显示。

[0089] 例如,如果在消息传递设置记录中发现多条与不同的消息传递设置相关联的条目,则存在设置冲突。不同的消息传递设置可能对应于不同寻址的消息接收者,或者对应于被发送到相同寻址的接收者、或从该相同寻址的接收者接收的可能不同的消息。替代,或者另外,步骤 114 中的冲突解决方案例如包括:从被寻址接收者的消息传递设置记录中发现的条目中选择一组最安全的消息传递设置,从所发现的条目中选择一组最近使用的消息传递设置,从所发现的条目中选择一组最常使用的消息传递设置,提示用户从所发现的条目中选择消息传递设置,或者选择与首先被寻址的消息接收者相关联的消息传递设置。其它的冲突解决方案也是可能的。

[0090] 在步骤 108 处,在编写屏幕的消息传递设置部分中显示所选的消息传递设置。然后用户开始编写输出消息,并且可以在编写该消息的同时选择新的消息传递设置。如上所

述,这可以包括退出所述编写屏幕,以便重新设置消息选项或者选择新的消息传递设置。然而,优选地,该消息传递客户程序支持在编写屏幕、消息选项屏幕或者这二者中的至少一个消息传递设置选择字段。如步骤 120 所确定的,如果在完成编写操作之前选择新的消息传递设置,如果这样来启动消息传递客户程序,则在步骤 122 处,在编写屏幕的消息设置部分、以及消息选项屏幕中显示新的消息传递设置。当完成编写操作时(步骤 116),根据所选的消息传递设置在步骤 118 准备并发送输出消息。

[0091] 如连续的步骤 116 和 120 所示,应当理解,在完成输出消息或准备选择新的消息传递设置时,优选地由用户来激活完成编写操作以及选择新设置的检测。如上所述,消息传递客户程序典型地检测预先确定的输入或者菜单选择,以确定应当发送消息或者已经选择了新的消息传递设置。

[0092] 同样应当理解,编写操作可以包括比图 10 中示出的步骤更多或者更少的方法步骤。例如,消息传递客户程序通过从如上所述的消息菜单中选择“Cancel”功能,典型地支持诸如编写操作这样的操作的取消。

[0093] 另外,图 10 示出了基于消息传递设置记录或者默认的消息传递设置的最初消息传递设置选择的一个实施例。可以将上述消息传递设置选择方案的任意组合用于为输出消息选择消息传递设置。

[0094] 图 11 是无线移动通信设备的框图。移动设置 600 优选地是一种至少具有语音和数据通信能力的双向通信设备。移动设置 600 优选地具有基于因特网与其它计算机系统通信的能力。根据该设备提供的功能,可以将该设备称为数据消息传递设备、双向寻呼机、具有数据消息传递能力的蜂窝电话、无线因特网设备或者数据通信设备(具有或不具有电话能力)。

[0095] 移动设备 600 包括收发信机 611,微处理器 638、显示屏 622、非易失性存储器 624、RAM626、辅助输入/输出(I/O)设备 628、串行接口 630、键盘 632、扬声器 634、麦克风 636、近距离无线通信子系统 640 以及其它的设备子系统 642。收发信机 611 包括发射和接收天线 616、618、接收机(Rx)612、发射机(Tx)614、一个或多个本地振荡器(L0)613 以及数字信号处理器(DSP)620。在非易失性存储器 624 内,移动设备 600 包括可以由微处理器 638(和/或 DSP620)执行的多个软件模块 624A-624N,这些软件模块包括语音通信模块 624A、数据通信模块 624B 以及用于执行多项其它功能的多个其它的操作模块 624N。

[0096] 如上所述,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。因此,该移动设备 600 例如可以基于诸如任何模拟或数字蜂窝网络这样的语音网络进行通信,也可以基于数据网络进行通信。在图 11 中借助于通信塔 619 描绘了语音和数据网络。这些语音和数据网络可以是使用诸如基站、网络控制器等这样的独立基础设施的独立通信网络,或者可以将这些独立基础设施整合到一个无线网络中。

[0097] 通信子系统 611 用于与网络 619 进行通信。DSP620 用于将通信信号发送到发射机 614 和接收机 612、或者从发射机 614 和接收机 612 接收通信信号,也可以与发射机 614 和接收机 612 交换控制信息。如果语音和数据通信在单频率、或者空间上非常靠近的频率集上出现,则单 L0613 可以与发射机 614 和接收机 612 一同使用。作为选择,如果针对语音通信和数据通信使用不同的频率,则可以使用多个 L0613 来产生对应于网络 619 的多个频率。尽管图 11 中描绘了两个天线 616、618,但该移动设备 600 也可以使用单天线结构。经

由 DSP620 和微处理器 638 之间的链路将包括语音和数据信息的信息发送到通信模块 611，或者从通信模块 611 进行接收。

[0098] 诸如频带、元件选择、功率电平等这样的通信子系统 611 的详细设计将取决于规定了移动设备 600 旨在其中进行操作的通信网络 619。例如，打算在北美市场进行操作的移动设备 600 可以包括通信子系统 611，该子系统 611 被设计为利用 Mobitex 或 DataTAC 移动数据通信网络进行操作，并且还将其设计为与诸如 AMPS、TDMA、CDMA、PCS 等多种语音通信网络中的任何一个进行操作，而可以将打算在欧洲使用的移动设备 600 配置为利用 GPRS 数据通信网络和 GSM 语音通信网络进行操作。该移动设备 600 还可以使用其它类型的独立和整合的数据和语音网络。

[0099] 根据网络 619 的类型，双模移动设备 600 的接入需求也可以变化。例如，在 Mobitex 或 DataTAC 数据网络中，使用与各个设备相关联的唯一识别号将移动设备登记到该网络上。但是在 GPRS 数据网络中，网络接入与移动设备 600 的用户相关联。GPRS 设备典型地需要用户识别模块（“SIM”），需要该模块以便在 GPRS 网络上操作该移动设备 600。在没有 SIM 的情况下，可以操作本地或非网络通信功能（若有的话），但该移动设备 600 不能在网络 619 上执行除了诸如“911”紧急呼叫这样的规定操作之外的任何涉及通信的功能。

[0100] 在完成任何所需的网络登记或激活程序之后，移动设备 600 可以基于网络 619 发送和接收通信信号，这些通信信号优选地包括语音和数据信号。将通过天线 616 从通信网络 619 接收的信号路由到接收机 612，该接收机 612 提供信号放大、频率下变换、滤波、信道选择等，而且也提供模拟到数字的转换。已接收信号的模拟到数字转换提供了更加复杂的通信功能，诸如使用 DSP620 来执行数字解调和解码。例如以类似的方式，通过 DSP620 对要发送到网络 619 的信号进行包括调制和编码的处理，然后经由天线 618 提供给用于数模转换、频率上变换、滤波、放大并发送到通信网络 619 的发射机 614。尽管图 11 中示出了用于语音和数据通信的单收发信机 611，但移动设备 600 还可以包括两个截然不同的收发信机，第一个收发信机用于发射和接收语音信号，而第二个收发信机用于发射和接收数据信号。

[0101] 除了处理通信信号之外，DSP620 还提供接收机和发射机控制。例如，可以通过在 DSP620 中执行的自动增益控制算法来自适应地控制施加给接收机 614 和发射机 614 中的通信信号的增益电平。为了提供对收发信机 611 更加高级的控制，也可以在 DSP620 中执行其它的收发信机控制算法。

[0102] 优选地，微处理器 638 管理并控制移动设备 600 的整个操作。多种类型的微处理器或微控制器可以用于该部分，或者作为选择，单 DSP620 可用于执行微处理器 638 的功能。通过收发信机 611 中的 DSP620 来执行至少包括数据和语音通信的低级通信功能。另外，可以将由微处理器 638 执行的诸如语音通信应用 624A 和数据通信应用 624B 这样的高级通信应用存储到非易失性存储器 624 中。例如，语音通信模块 624A 可以提供经由网络 619 在移动设备 600 和多个其它语音设备之间可操作地发送和接收语音呼叫的高级用户接口。同样，数据通信模块 624B 可以提供经由网络 619 在移动设备 600 和多个其它数据设备之间可操作地发送和接收诸如电子邮件消息、文件、管理器信息、短文本消息等的数据的高级用户接口。

[0103] 微处理器 638 也可以与其它设备子系统相互作用，该其它设备子系统诸如是显示屏 622、非易失性存储器 624、随机接入存储器 (RAM) 626、辅助输入 / 输出 (I/O) 子系统 628、

串行接口 630、键盘 632、扬声器 634、麦克风 636、近距离通信子系统 640 以及一般由 642 指明的其它设备子系统。部件 628、632、634 和 636 是可以以 UI62(图 3)来提供的子系统类型的实例。通过微处理器 638 来执行模块 624A-N,而且模块 624A-N 还提供移动设备用户和移动设备之间的高级接口。该接口典型地包括通过显示屏 622 提供的图形组件,以及通过辅助 I/O628、键盘 632、扬声器 634 或者麦克风 636 提供的输入/输出组件。

[0104] 图 11 中示出的某些子系统执行与通信相关的功能,而其它子系统可以提供“驻留”或设备上(on-device)的功能。值得注意的是,诸如键盘 632 和显示屏 622 这样的某些子系统既可以用于与通信相关的功能(诸如输入用于在数据通信网络上进行传输的文本消息),也可以用于设备驻留功能(诸如日历或者任务列表或者其它 PDA 类型功能)。

[0105] 优选地,将由微处理器 638 使用的操作系统软件存储到诸如非易失性存储器 624 这样的持久存储器中。除了操作系统和通信模块 624A-N 之外,该非易失性存储器 624 还可以包括用于存储数据的文件系统。优选地,在非易失性存储器 624 中提供用于存储公共密钥、专用密钥和其它保密消息传递所需信息的存储区域。为了较快地进行操作,可以将操作系统、特定设备应用程序或模块,或其部分临时加载到诸如 RAM626 这样的易失性存储器中。此外,在永久地将所接收的通信信号写到位于非易失性存储器 624 中的文件系统之前,还可以将所接收的通信信号临时存储到 RAM626 中。本领域的普通技术人员将理解,非易失性存储器 624 例如可以实现为闪存部件或电池供电(battery backed-up)的 RAM。

[0106] 可以加载到移动设备 600 上的示例性应用程序模块 624N 是具有诸如日历事件、约会和任务项目这样的 PDA 功能的个人信息管理器(PIM)应用程序。该模块 624N 也可以与用于管理电话呼叫、语音邮件等的语音通信模块 624A 相互作用,并且还可以与用于管理电子邮件通信和其它数据传输的数据通信模块 624B 相互作用。作为选择,语音通信模块 624A 和数据通信模块 624B 的所有功能都可以被整合到 PIM 模块中。

[0107] 优选地,非易失性存储器 624 提供文件系统以方便在设备上存储 PIM 数据项。优选地,PIM 应用程序包括经由无线网络 619 单独地、或者与语音和数据通信模块 624A、624B 一同来发送和接收数据项的能力。优选地,利用所存储的或与主机系统相关联的一组相应的数据项、经由无线网络 619 对 PIM 数据项进行无缝地整合、同步和更新,从而为与特定用户相关联的数据项创建一个镜像系统。

[0108] 通过将移动设备 600 放到接口支架中,也可以手动地将该移动设备 600 与主系统同步,该接口支架将移动设备 600 的串行接口 630 耦合到主系统的串行接口。串行接口 630 还可以用于通过外部设备或软件应用程序使用户建立消息传递设置,以下载用于安装的其他应用程序模块 624N,并且将 Cert、密钥和其它信息加载到设备上。可以使用这种有线下载路径将加密密钥加载到移动设备 600 上,这是一种比经由无线网络 619 交换加密信息更加安全的方法。

[0109] 可以将附加的应用程序模块 624N 通过网络 619、通过辅助 I/O 子系统 628、通过串行接口 630、通过近距离通信子系统 640 或者通过任何其它合适的子系统 642 加载到移动设备 600 上,并且由用户安装到非易失性存储器 624 或者 RAM626 中。这种应用程序安装中的灵活性增强了移动设备 600 的功能,并且可以提供增强的设备上(on-device)的功能、与通信相关的功能或者这两种功能。例如,保密通信应用可以使得通过使用移动设备 600 来执行电子商务功能和其它的这种金融交易。

[0110] 当移动设备 600 在数据通信模式中运行时,通过收发信机 611 来处理诸如文本消息或网页下载这样的接收信号,并且提供给微处理器 638,优选地,该微处理器 638 进一步处理用于输出到显示屏 622、或作为选择输出到辅助 I/O 设备 628 的已接收信号。移动设备 600 的用户也可以使用键盘 632 来编写诸如电子邮件消息这样的数据项,优选地,该键盘 632 是以 QWERTY 式样来布置的完整的字母数字键盘,尽管也可以使用诸如已知 DVORAK 式样的其它式样的完整字母数字键盘。利用多个辅助 I/O 设备 628 来进一步增强到移动设备 600 的用户输入,这些辅助 I/O 设备 628 可以包括指轮输入设备、触摸屏、各种开关、摇杆输入开关等。然后,可以准备用户输入的已编写数据项,作为规定在已选消息传递设置中,并经收发信机 611 传输过通信网络 619。

[0111] 当移动设备 600 在语音通信模式中进行操作时,移动设备 600 的整个操作实际上类似于数据模式,除了优选地将所接收的信号输出到扬声器 634、以及通过麦克风 636 来产生用于传输的语音信号之外。还可以在移动设备 600 上实现诸如语音消息记录子系统这样的可选语音或音频 I/O 子系统。优选地,尽管主要是通过扬声器 634 来实现语音或音频信号输出,但是也可以使用显示屏 622 来提供呼叫方身份、语音呼叫持续时间或者其它与语音呼叫相关的信息的指示。例如,麦克风 638 结合语音通信模块 624A 和操作系统软件可以检测输入语音呼叫的呼叫者标识信息,并且将其显示在显示屏 622 上。

[0112] 可以将近距离通信子系统 640 也包括在移动设备 600 中。例如,该子系统 640 可以包括红外设备和相关的电路及元件、或者近距离无线通信模块,诸如 Bluetooth™(蓝牙)通信模块或者用于提供与类似激活的系统和设备进行通信的 802.11 模块。本领域的普通技术人员将理解,“蓝牙”和“802.11”是指可从电子和电气工程师协会(IEEE)得到的规范集,分别与无线个人区域网和无线 LAN 相关联。

[0113] 上面的描述涉及一个或多个实例。许多在本申请范围内的各种变型对本领域的普通技术人员将是显而易见的。

[0114] 例如,尽管在图 11 中示出了无线移动通信设备,并且作为一种可以在其上运行消息传递客户程序的可能的系统进行了描述,但是也可以在其它消息传递客户程序中实现消息传递设置选择系统和方法,该其它消息传递客户程序包括被配置为用于在桌上型计算机、膝上型计算机或成为网络的计算机系统上运行的消息传递客户程序。

[0115] 在下面权利要求中使用的数字或字母标记完全是出于方便和参考的目的。这些标记并不旨在限制权利要求的范围或规定特定限制的特定顺序。此外,实际上权利要求中所述的限制可以以任何合适的顺序出现,也可以对其进行重新排列或组合或其它的整合而不脱离权利要求的范围。

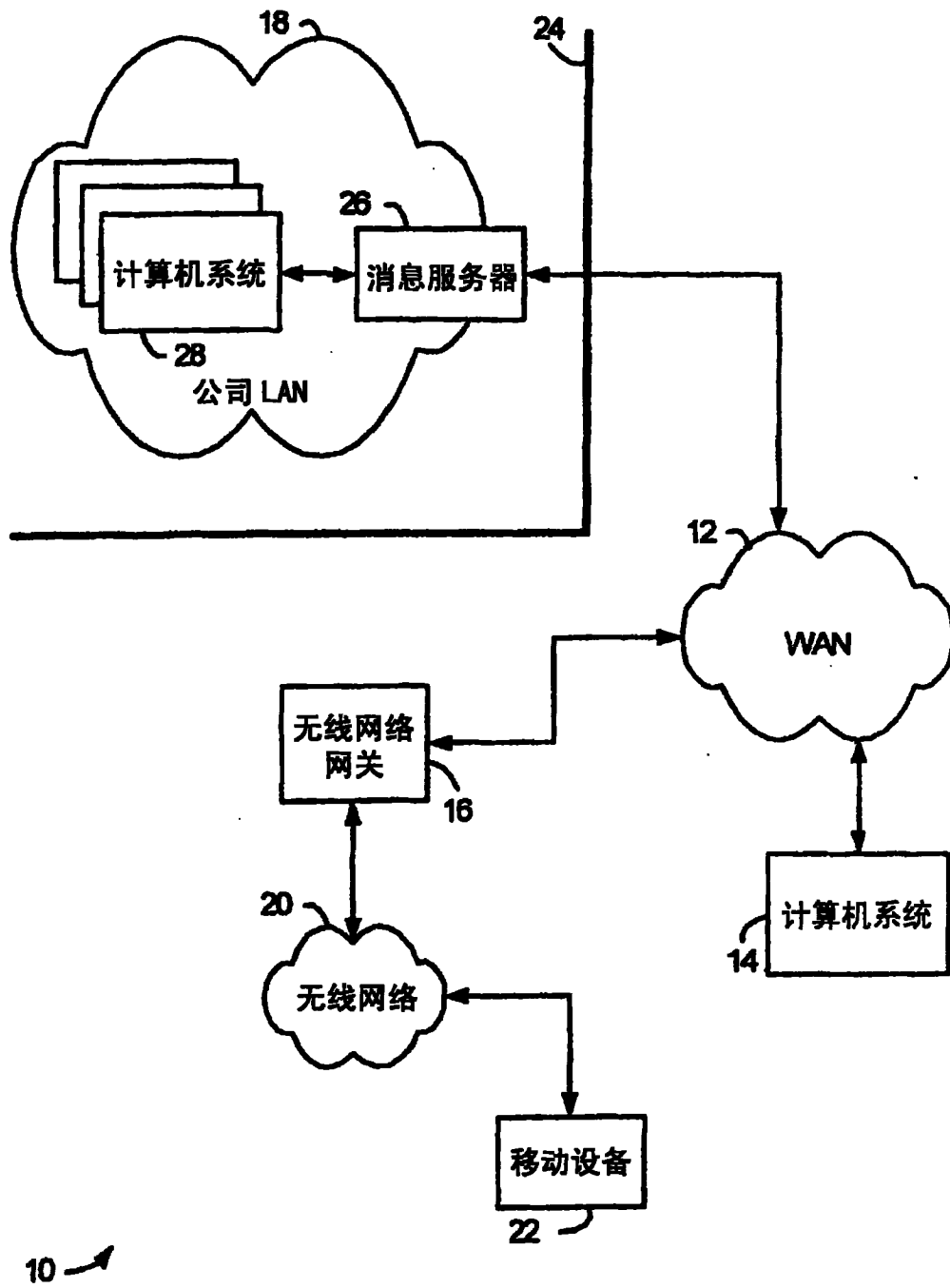


图 1

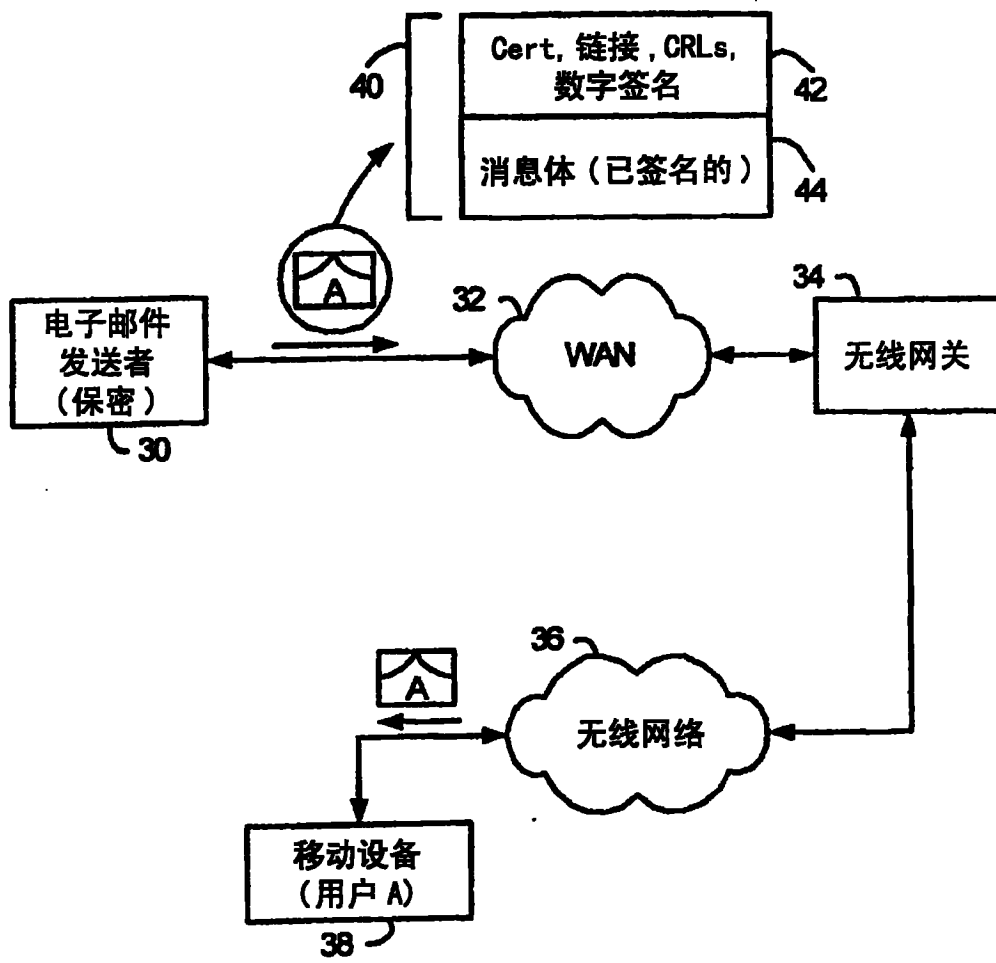


图 2

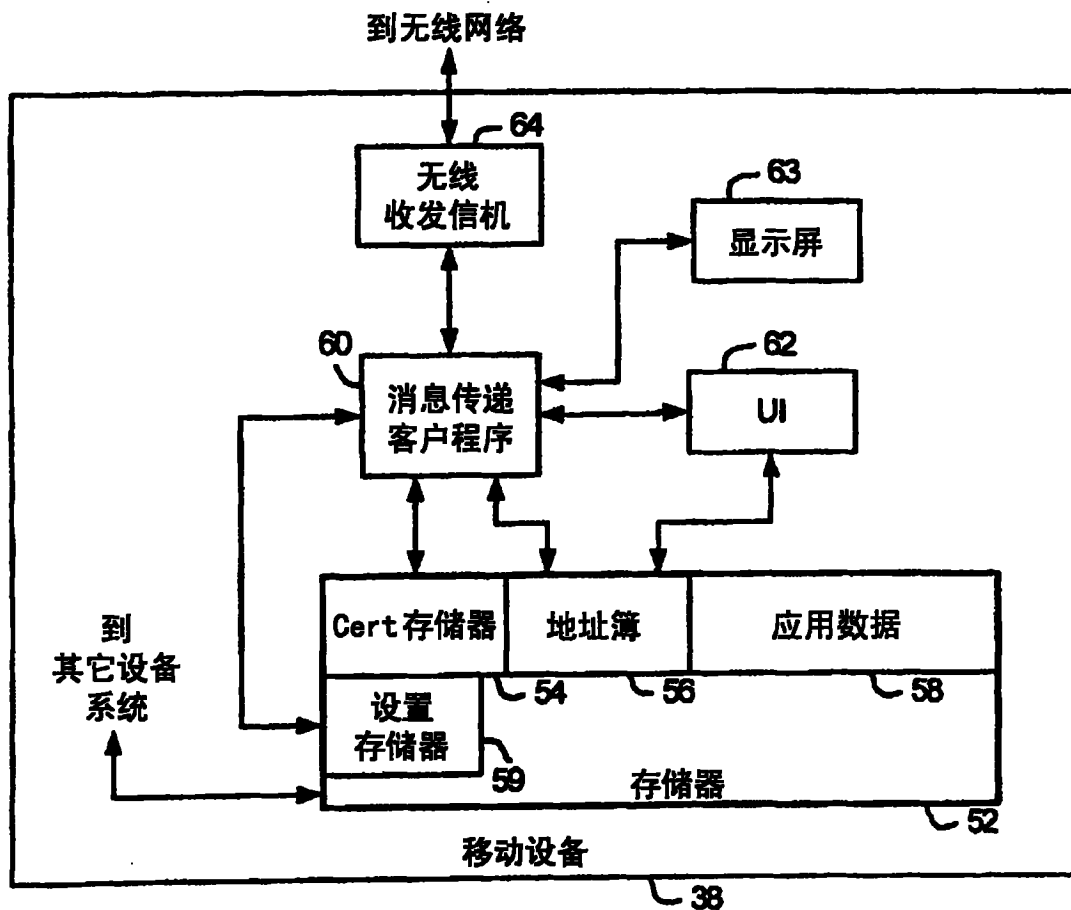


图 3

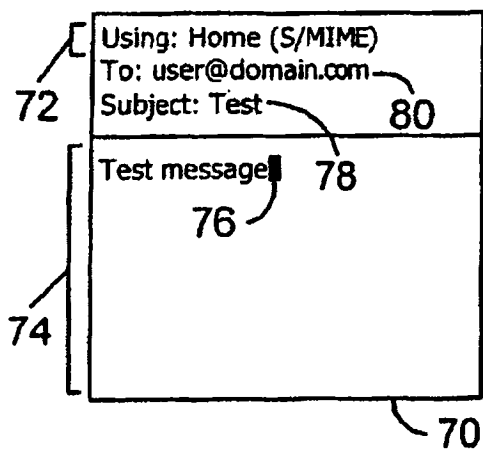


图 4

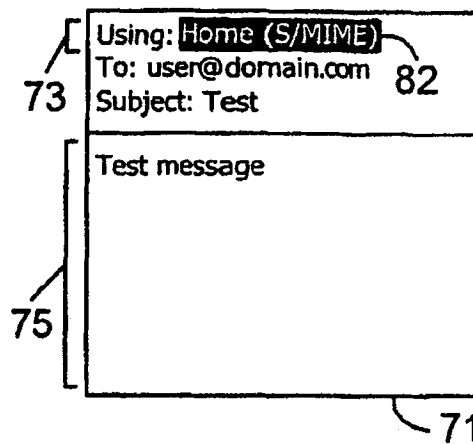


图 5

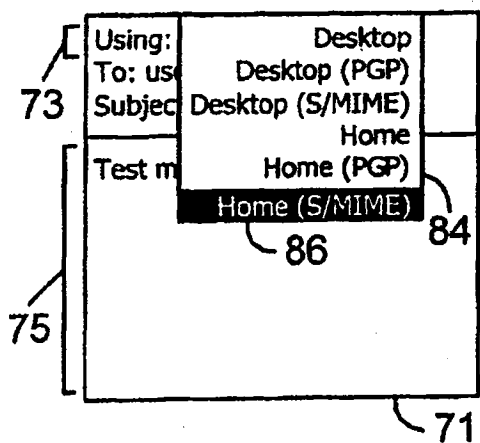


图 6

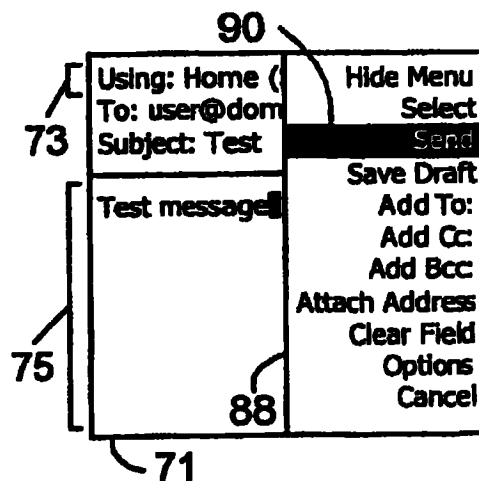


图 7

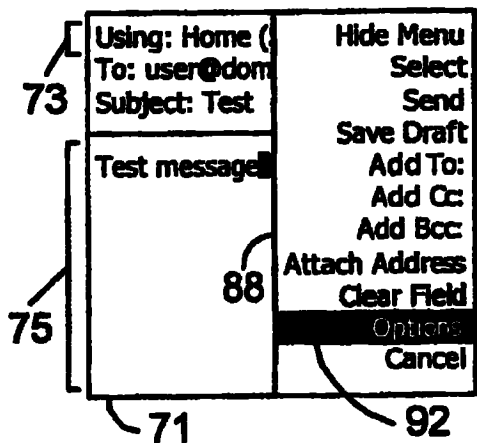


图 8

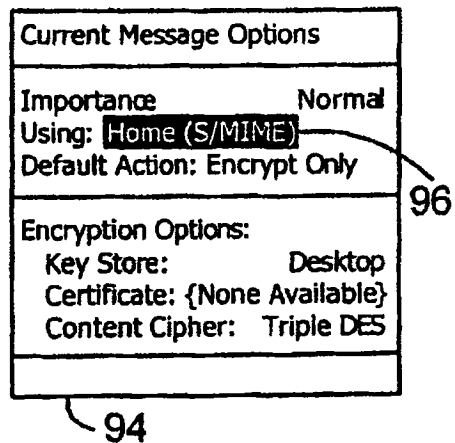


图 9

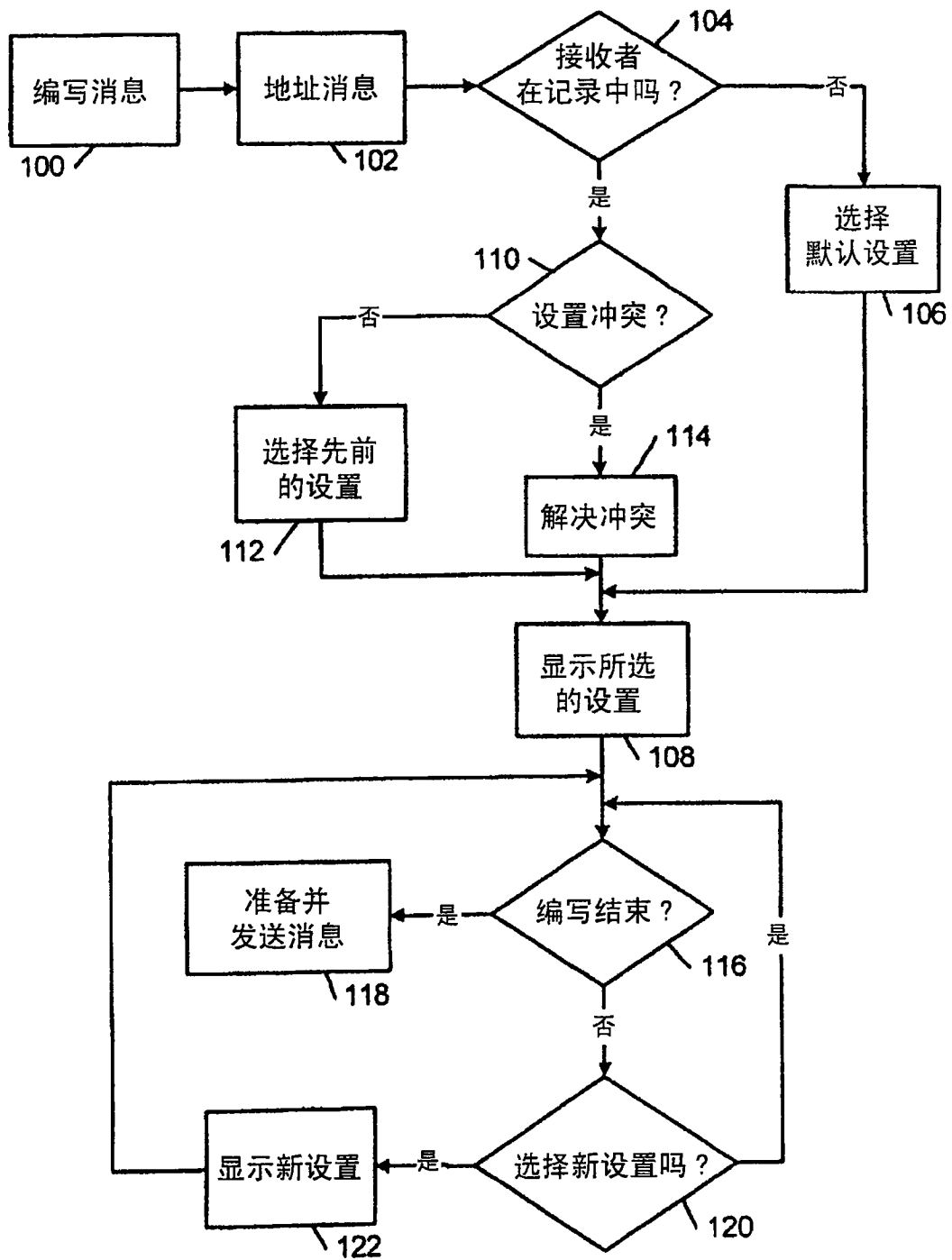


图 10

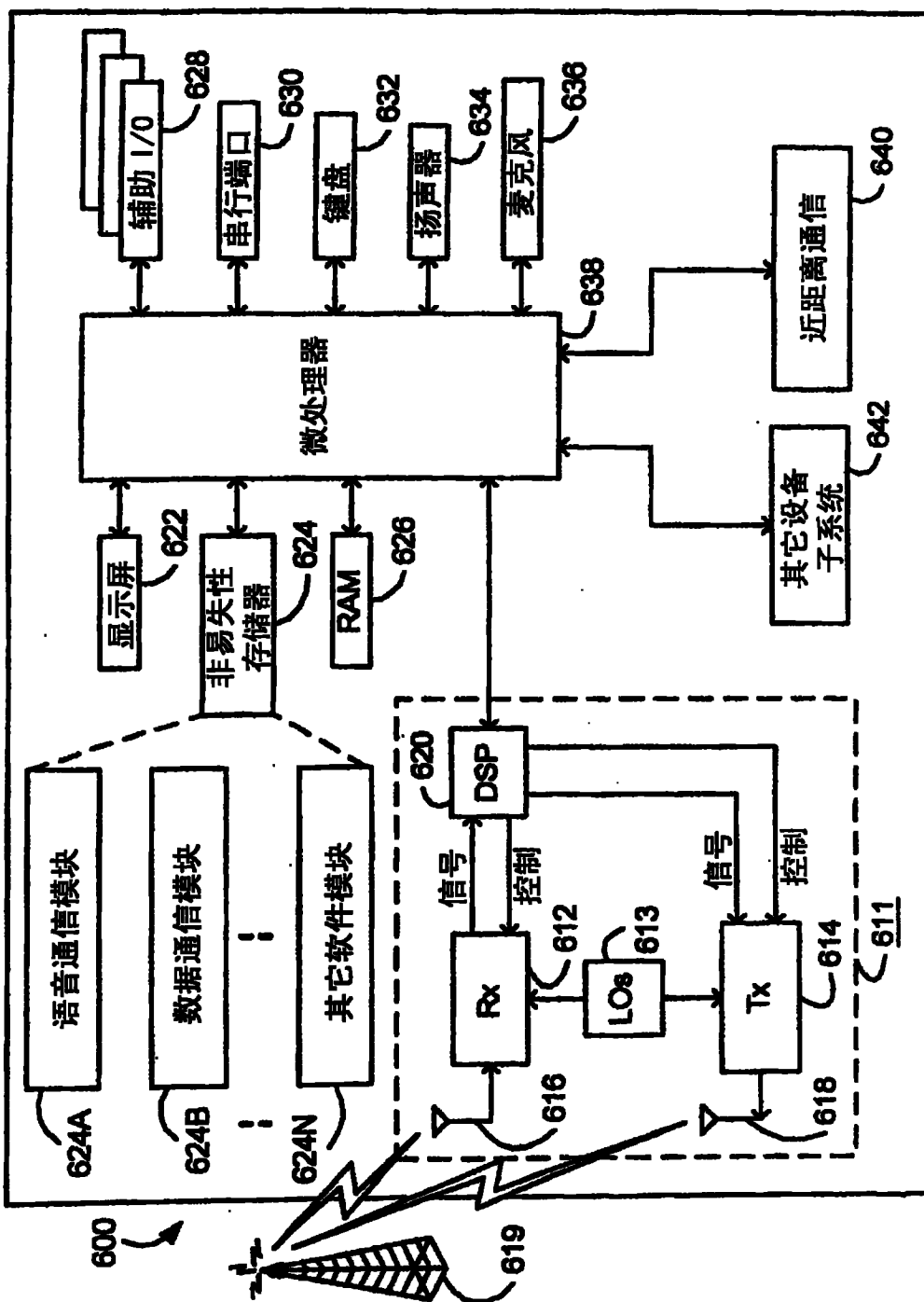


图 11