[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 29/06 (2006.01)

[12] 发明专利说明书

专利号 ZL 200380102818.4

[45] 授权公告日 2009 年 9 月 9 日

[11] 授权公告号 CN 100539581C

[22] 申请日 2003.10.24
[21] 申请号 200380102818.4
[30] 优先权
[32] 2002.11.6 [33] EP [31] 02405954.5
[86] 国际申请 PCT/IB2003/004720 2003.10.24
[87] 国际公布 WO2004/043037 英 2004.5.21
[85] 进入国家阶段日期 2005.5.8
[73] 专利权人 国际商业机器公司
地址 美国纽约阿芒克
[72] 发明人 迈克尔·贝恩奇 彼得·比勒
托马斯·艾里克 弗兰克·霍林
索尔斯坦·克兰普
马库斯·奥斯特赖克
迈克尔·奥斯本
托马斯·D·韦戈德
[56] 参考文献
CN1322076A 2001.11.14
CN1313576A 2001.9.19
US2002/0141588A1 2002.10.3
Handbook of Applied Cryptography. Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone, 全文, CRC press. 1997
审查员 封 展
[74] 专利代理机构 北京市柳沈律师事务所
代理人 郭定辉 黄小临

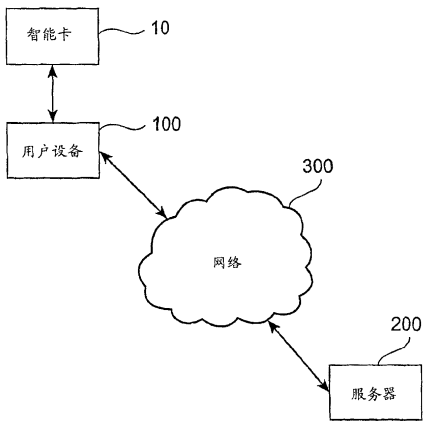
权利要求书 7 页 说明书 13 页 附图 7 页

[54] 发明名称

向用户设备提供一组访问码

[57] 摘要

向用户设备提供一组访问码的方法包括，在用户设备中，存储加密密钥和标识码，和通过通信网络将包含标识码的消息发送到服务器。 在服务器中，与存储在用户设备中的密钥相对应地存储加密密钥，一旦从用户设备接收到标识码就分配该组访问码。 根据在消息中接收的标识码执行查找功能以便从存储器中检索密钥。 利用检索的密钥加密该组访问码以生成加密组。 通过网络将包含加密组的消息发送到用户设备。 在用户设备中，利用存储器中的密钥解密从服务器接收的加密组，和存储解密组访问码供用户设备的用户使用。



1. 一种向用户设备提供一组访问码的方法，该方法包括:

在用户设备中，存储加密密钥和标识码，和通过通信网络将包含标识码的消息发送到服务器;

在服务器中，存储与存储在用户设备中的密钥相对应的加密密钥，一旦从用户设备接收到标识码就分配该组访问码，根据在消息中接收的标识码执行查找功能以便从存储器中检索密钥，利用检索的密钥加密该组访问码以生成加密组，和通过网络将包含加密组的消息发送到用户设备;

在用户设备中，利用存储器中的密钥解密从服务器接收的加密组，和存储解密组访问码供用户设备的用户使用;

一旦未用访问码的个数达到一预定阈值，就在服务器中通过网络将包含新组访问码的消息发送到用户设备; 和

在用户设备中，存储该新组供用户设备的用户使用。

2. 根据权利要求 1 所述的方法，进一步包括:

在用户设备中，跟踪用户使用的访问码，响应未用访问码的个数达到预定阈值生成一个请求，和将包含该请求的消息发送到服务器; 和

在服务器中，一旦接收到该请求就发送包含新组访问码的消息。

3. 根据权利要求 1 所述的方法，进一步包括:

在服务器中，跟踪用户使用的访问码，并响应未用访问码的个数达到预定阈值将包含新组访问码的消息发送到用户设备。

4. 根据权利要求 1 所述的方法，进一步包括:

在服务器中，生成新密钥，用旧密钥加密新密钥，和通过网络将包含加密新密钥的消息发送到用户设备; 和

在用户设备中，利用旧密钥解密从服务器接收的加密新密钥，和存储解密新密钥取代旧密钥。

5. 根据权利要求 4 所述的方法，进一步包括:

在服务器中，用新密钥加密新组访问码以生成新密钥加密组，和通过网络将包含新密钥加密组的消息发送到用户设备; 和

在用户设备中，用新密钥解密新密钥加密组，和存储解密新组供用户设备的用户使用。

6. 根据权利要求 1 所述的方法，进一步包括:

在用户设备中，生成公开/秘密密钥对，和通过网络将包含密钥对的公开密钥的消息发送到服务器;

在服务器中，生成会话密钥，用会话密钥加密该组访问码以生成会话密钥加密组，用公开密钥加密会话密钥以生成加密会话密钥，通过网络将包含会话密钥加密组和加密会话密钥的消息发送到用户设备; 和

在用户设备中，用密钥对的秘密密钥解密加密会话密钥以还原会话密钥，用还原会话密钥解密会话密钥加密组以还原该组，和存储解密组供用户设备的用户使用。

7. 根据权利要求 1-6 任意一项所述的方法，其中，访问码是一次性验证码。

8. 根据权利要求 1-6 任意一项所述的方法，其中，网络包括无线通信网络。

9. 根据权利要求 8 所述的方法，其中，用户设备包括移动电话、个人数字助理和智能卡。

10. 根据权利要求 8 所述的方法，其中，消息是 SMS 消息。

11. 一种向用户设备提供一组访问码的方法，该方法包括，在用户设备中:

存储加密密钥和标识码;

通过通信网络将包含标识码的消息发送到服务器;

从服务器接收包含用密钥加密的该组访问码的消息;

利用存储器中的密钥解密接收组访问码;

存储解密组访问码供用户设备的用户使用;

一旦未用访问码的个数达到一预定阈值，则从服务器接收包含新组访问码的消息; 和

在用户设备中，存储该新组供用户设备的用户使用。

12. 根据权利要求 11 所述的方法，进一步包括: 在用户设备中，跟踪用户使用的访问码，响应未用访问码的个数达到预定阈值生成一个请求，和将包含该请求的消息发送到服务器; 和在服务器中，一旦接收到该请求就发送包含新组访问码的消息。

13. 根据权利要求 11 所述的方法，进一步包括，在用户设备中:

利用旧密钥解密从服务器接收的加密新密钥；和

存储解码新密钥取代旧密钥。

14. 根据权利要求 13 所述的方法，进一步包括，在用户设备中：

通过网络从服务器接收包含新密钥加密组访问码的消息；

用新密钥解码新密钥加密组；和

存储解密新组供用户设备的用户使用。

15. 根据权利要求 11 所述的方法，包括，在用户设备中：

生成公开/秘密密钥对；

通过网络将包含密钥对的公开密钥的消息发送到服务器；

通过网络从服务器接收包含会话密钥加密组访问码和公开密钥加密会话密钥的消息；

用密钥对的秘密密钥解密公开密钥加密会话密钥以还原会话密钥加密组和相应会话密钥；

用还原会话密钥解密会话密钥加密组以还原该组；和

存储解密组供用户设备的用户使用。

16. 根据权利要求 11-15 任意一项所述的方法，其中，访问码是一次性验证码。

17. 根据权利要求 11-15 任意一项所述的方法，其中，网络包括无线通信网络。

18. 根据权利要求 17 所述的方法，其中，用户设备包括移动电话、个人数字助理和智能卡。

19. 根据权利要求 17 所述的方法，其中，消息是 SMS 消息。

20. 一种向用户设备提供一组访问码的方法，该方法包括，在通过网络与用户设备通信的服务器中：

存储与存储在用户设备中的加密密钥相对应的加密密钥；

一旦通过网络从用户设备接收到包含标识码的消息就将该组访问码分配给用户设备；

根据在消息中接收的标识码执行查找功能以便从存储器中检索密钥；

利用检索的密钥加密该组访问码以生成加密组；

通过网络将包含加密组的消息发送到用户设备；和

一旦未用访问码的个数达到一预定阈值，就通过网络将包含新组访问码

的消息发送到用户设备。

21. 根据权利要求 20 所述的方法，进一步包括，在服务器中：

生成新密钥，用旧密钥加密新密钥；和

通过网络将包含加密新密钥的消息发送到用户设备。

22. 根据权利要求 21 所述的方法，进一步包括，在服务器中：

用新密钥加密新组访问码以生成新密钥加密组；和

通过网络将包含新密钥加密组的消息发送到用户设备。

23. 根据权利要求 20 所述的方法，进一步包括，在服务器中：

从用户设备接收包含公开/秘密密钥对的公开密钥的消息；

生成会话密钥；

用会话密钥加密该组访问码以生成会话密钥加密组；

用公开密钥加密会话密钥以生成公开密钥加密会话密钥；和

通过网络将包含会话密钥加密组和公开密钥加密会话密钥的消息发送到用户设备。

24. 根据权利要求 20-23 任意一项所述的方法，其中，访问码是一次性验证码。

25. 根据权利要求 20-23 任意一项所述的方法，其中，网络包括无线通信网络。

26. 根据权利要求 25 所述的方法，其中，用户设备包括移动电话、个人数字助理和智能卡。

27. 根据权利要求 25 所述的方法，其中，消息是 SMS 消息。

28. 一种向用户设备提供一组访问码的设备，该设备包括：用户设备；和通过通信网络与用户设备通信的服务器，该用户设备包括存储加密密钥和标识码的装置和通过网络将包含标识码的消息发送到服务器的装置；该服务器包括存储与存储在用户设备中的密钥相对应的加密密钥的装置、一旦从用户设备接收到标识码就分配该组访问码的装置、根据在消息中接收的标识码执行查找功能以便从存储器中检索密钥的装置、利用检索的密钥加密该组访问码以生成加密组的装置和通过网络将包含加密组的消息发送到用户设备并当未用访问码的个数达到一预定阈值时通过网络将包含新组访问码的消息发送到用户设备的装置；和该用户设备进一步包括存储该新组供用户设备的用户使用的装置、利用存储在用户设备中的密钥解密从服务器接收的加密组的

装置、和存储解密组访问码供用户使用的装置。

29. 根据权利要求 28 所述的设备，其中，服务器进一步包括生成新密钥的装置、用旧密钥加密新密钥的装置、和通过网络将包含加密新密钥的消息发送到用户设备的装置，和其中，用户设备进一步包括利用旧密钥解密从服务器接收的加密新密钥的装置、和存储解密新密钥取代旧密钥的装置。

30. 根据权利要求 29 所述的设备，其中，服务器进一步包括用新密钥加密新组访问码以生成新密钥加密组的装置、和通过网络将包含新密钥加密组的消息发送到用户设备的装置，和其中，用户设备进一步包括用新密钥解密新密钥加密组的装置、和存储解密新组供用户设备的用户使用的装置。

31. 根据权利要求 28 所述的设备，进一步包括：在服务器中，通过网络将包含新组访问码的消息发送到用户设备的装置；和在用户设备中，存储该新组供用户设备的用户使用的装置。

32. 根据权利要求 31 所述的设备，进一步包括：在用户设备中，跟踪用户使用的访问码的装置、响应未用访问码的个数达到预定阈值生成一个请求的装置、和将包含该请求的消息发送到服务器的装置；和在服务器中，一旦接收到该请求就发送包含新组访问码的消息的装置。

33. 根据权利要求 31 所述的设备，进一步包括：在服务器中，跟踪用户使用的访问码的装置、和响应未用访问码的个数达到预定阈值，将包含新组访问码的消息发送到用户设备的装置。

34. 根据权利要求 31 所述的设备，进一步包括：在用户设备中，响应来自用户的人工输入，生成一个请求的装置、和将包含该请求的消息发送到服务器的装置；和在服务器中，一旦接收到该请求就发送包含新组访问码的消息的装置。

35. 根据权利要求 28 所述的设备，其中，用户设备进一步包括生成公开/秘密密钥对的装置、和通过网络将包含密钥对的公开密钥的消息发送到服务器的装置；其中，服务器进一步包括生成会话密钥的装置、用会话密钥加密该组访问码以生成会话密钥加密组的装置、用公开密钥加密会话密钥以生成公开密钥加密会话密钥的装置、和通过网络将包含会话密钥加密组和公开密钥加密会话密钥的消息发送到用户设备的装置；和其中，用户设备进一步包括用密钥对的秘密密钥解密公开密钥加密会话密钥以还原会话密钥的装置、用还原会话密钥解密会话密钥加密组以还原该组的装置、和存储解密组供用

户设备的用户使用的装置。

36. 根据权利要求 28 到 35 的任何一项所述的设备，其中，访问码是一次性验证码。

37. 根据权利要求 28 到 34 的任何一项所述的设备，其中，网络包括无线通信网络。

38. 根据权利要求 37 所述的设备，其中，用户设备包括移动电话、个人数字助理和智能卡。

39. 根据权利要求 37 所述的设备，其中，消息是 SMS 消息。

40. 一种通过通信网络从服务器接收一组访问码的用户设备，该设备包括：存储加密密钥和标识码的装置；通过通信网络将包含标识码的消息发送到服务器的装置；从服务器接收包含用密钥加密的该组访问码的消息的装置；利用存储器中的密钥解密接收组访问码的装置；存储解密组访问码供用户设备的用户使用的装置；以及当未用访问码的个数达到一预定阈值时通过网络从服务器中接收包含新密钥加密组访问码的消息的装置。

41. 根据权利要求 40 所述的用户设备，进一步包括：用旧密钥解密从服务器接收的加密新密钥的装置；和存储解密新密钥取代旧密钥的装置。

42. 根据权利要求 41 所述的用户设备，进一步包括：通过网络从服务器接收包括新密钥加密组访问码的消息的装置；利用新密钥解密新密钥加密组的装置；和存储解码新组供用户设备的用户使用的装置。

43. 根据权利要求 41 所述的用户设备，进一步包括：生成公开/秘密密钥对的装置；通过网络将包含密钥对的公开密钥的消息发送到服务器的装置；通过网络从服务器接收包含会话密钥加密组访问码和公开密钥加密会话密钥的消息的装置；用密钥对的秘密密钥解密公开密钥加密会话密钥以还原会话密钥的装置；用还原会话密钥解码会话密钥加密组以还原该组的装置；和存储解密组供用户设备的用户使用的装置。

44. 一种通过通信网络向用户设备提供一组访问码的服务器，该服务器包括：存储与存储在用户设备中的加密密钥相对应的加密密钥的装置；一旦通过网络从用户设备接收到包含标识码的消息就将该组访问码分配给用户设备的装置；根据在消息中接收的标识码执行查找功能以便从存储器中检索密钥的装置；利用检索的密钥加密该组访问码以生成加密组的装置；通过网络将包含加密组的消息发送到用户设备的装置；以及当未用访问码的个数达到

一预定阈值时通过网络将包含新密钥加密组访问码的消息发送到用户设备的装置。

45. 根据权利要求 44 所述的服务器，进一步包括：生成新密钥的装置；用旧密钥加密新密钥的装置；和通过网络将包含加密新密钥的消息发送到用户设备的装置。

46. 根据权利要求 45 所述的服务器，进一步包括：用新密钥加密新组访问码以生成新密钥加密组的装置；和通过网络将包含新密钥加密组的消息发送到用户设备的装置。

47. 根据权利要求 44 所述的服务器，进一步包括：从用户设备接收包含公开/秘密密钥对的公开密钥的消息的装置；生成会话密钥的装置；用会话密钥加密该组访问码以生成会话密钥加密组的装置；用公开密钥加密会话密钥以生成公开密钥加密会话密钥的装置；和通过网络将包含会话密钥加密组和公开密钥加密会话密钥的消息发送到用户设备的装置。

向用户设备提供一组访问码

本发明一般涉及通过诸如无线通信网络之类的数据通信网络向用户设备提供诸如一次性验证码之类的一组访问码。

在联机交易的领域中，一次性验证码（OTAC）以及交易验证号（TAN）或一次性信用卡号的纸质暂存表越来越流行。允许安全地存储和分配 OTAC 是人们所希望的。无论何时何地需要都允许方便地访问 OTAC 同样也是人们所希望的。不幸的是，相对而言，纸质暂存表既不安全也不便于访问。通常，暂存表是通过平信从诸如银行的服务操作者传送给客户的。邮寄的暂存表在邮寄给客户的途中可能被截获和复制。另外，许多客户不能信赖将暂存表存放在像保险箱那样的安全地方。定期使用暂存表的情况尤其如此。定期使用的暂存表可能被遗忘在公开的地方，例如，桌子上。这向其它人提供了访问暂存表的机会。如果客户将暂存表带在身边，它可以被丢失或被偷。暂存表上的 OTAC 通常是不加密的。一般与 OTAC 结合在一起实现交易的客户帐号普遍认为是公知的。对于许多客户来说，人为关注哪些 OTAC 已经使用过是不便的。当从一张暂存表过渡到另一张暂存表时，客户需要暂时保存或携带两张暂存表。这增加了安全风险。此外，发行服务提供者及时印刷和邮寄纸质暂存表也很麻烦。

WO98/37524 描述了利用移动设备的交易方法。这种方法应用国际信贷用户标识（IDUI）号来标识各个帐户。IDUI 类似于客户银行帐号。具体地说，将 IDUI 预装到信用/信贷卡中。在操作过程中，销售点（POS）终端从信用/信贷卡中读取 IDUI 和显示要从识别帐户中扣除的数目。客户通过按下 POS 终端的 OK 按钮完成交易。POS 终端将交易接受凭证发送到负责帐户的银行。WO98 /37524 建议将 IDUI 预存在像用在 GSM（全球能）移动电话网络中那样的用户标识模块（SIM）智能卡上，而不是预存在磁条或存储卡上。然后，终端以非接触方式从智能卡中读取 IDUI。将交易接受凭证发送到服务器，以便通过 SMS（短消息服务）消息加以核实。这种方案只讨论了通过非接触方式将 IDUI 用于与 POS 终端的交易和交换用于交易核实的 SMS 消息。该方案

不适用于 OTAC 交付。这是因为 IDUI 对于每个帐户是固定的。但 OTAC 却不是这样。在 EP1 176 844、WO99/16029、WO00/495585、WO01/09851、WO02/21464、和 WO01/93528 中描述了类似的电子支付系统。

按照本发明，现在提供向用户设备提供一组访问码的方法，该方法包括：在用户设备中，存储加密密钥和标识码，和通过通信网络将包含标识码的消息发送到服务器；在服务器中，存储与存储在用户设备中的密钥相对应的加密密钥，一旦从用户设备接收到标识码就分配该组访问码，根据在消息中接收的标识码执行查找功能以便从存储器中检索密钥，利用检索的密钥加密该组访问码以生成加密组，和通过网络将包含加密组的消息发送到用户设备；和在用户设备中，利用存储器中的密钥解密从服务器接收的加密组，和存储解密组访问码供用户设备的用户使用。

这样有利地提供了以既方便又安全的方式向客户提供诸如 OTAC 之类的访问码的方案。

最好，该方法进一步包括：在服务器中，生成新密钥，用旧密钥加密新密钥，和通过网络将包含加密新密钥的消息发送到用户设备；和在用户设备中，利用旧密钥解密从服务器接收的新密钥，和存储解密新密钥取代旧密钥。

这样通过促进应用的密钥得到安全更新，有利地提供了附加安全。

该方法还可以推广到，在服务器中，用新密钥加密新组访问码以生成新密钥加密组，和通过网络将包含新密钥加密组的消息发送到用户设备；和在用户设备中，用新密钥解密新密钥加密组，和存储解密新组供用户设备的用户使用。

这样有利地保证了访问码以方便的方式得到安全更新。

最好，该方法进一步包括：在服务器中，通过网络将包含新组访问码的消息发送到用户设备；和在用户设备中，存储该新组供用户设备的用户使用。该方法可以进一步包括：在用户设备中，跟踪用户使用的访问码，响应未用访问码的个数达到预定阈值生成一个请求，和将包含该请求的消息发送到服务器；和在服务器中，一旦接收到该请求就发送包含新组访问码的消息。可替代地，该方法可以包括：在服务器中，跟踪用户使用的访问码，和响应未用访问码的个数达到预定阈值，将包含新组访问码的消息发送到用户设备。在另一个替代中，该方法可以包括：在用户设备中，响应来自用户的人工输

入，生成一个请求，和将包含该请求的消息发送到服务器；和在服务器中，一旦接收到该请求就发送包含新组访问码的消息。

在本发明的一个优选实施例中，该方法进一步包括：在用户设备中，生成公开/秘密密钥对，和通过网络将包含密钥对的公开密钥的消息发送到服务器；在服务器中，生成会话密钥，用会话密钥加密该组访问码以生成会话密钥加密组，用公开密钥加密会话密钥以生成加密会话密钥，通过网络将包含会话密钥加密组和加密会话密钥的消息发送到用户设备；和在用户设备中，用密钥对的秘密密钥解密加密会话密钥以还原会话密钥，用还原会话密钥解密会话密钥加密组以还原该组，和存储解密组供用户设备的用户使用。

这样通过多次密钥加密提供了进一步的安全。

从另一个方面来观看本发明，现在提供了向用户设备提供一组访问码的方法，该方法包括，在用户设备中：存储加密密钥和标识码，通过通信网络将包含标识码的消息发送到服务器；从服务器接收包含用密钥加密的该组访问码的消息；利用存储器中的密钥解密接收组访问码；和存储解密组访问码供用户设备的用户使用。本发明也可推广到包括当被装入用户设备的处理器中时，将处理器配置成执行在本段中所述的方法的计算机程序代码模块的计算机程序单元。

从又一个方面来观看本发明，现在提供了向用户设备提供一组访问码的方法，该方法包括，在通过网络与用户设备通信的服务器中：存储与存储在用户设备中的加密密钥相对应的加密密钥；一旦通过网络从用户设备接收到包含标识码的消息就将该组访问码分配给用户设备；根据在消息中接收的标识码执行查找功能以便从存储器中检索密钥；利用检索的密钥加密该组访问码以生成加密组；和通过网络将包含加密组的消息发送到用户设备。本发明也可推广到包括当被装入服务器计算机系统的处理器中时，将处理器配置成执行在本段中所述的方法的计算机程序代码模块的计算机程序单元。

在本发明的一个特定优选实施例中，访问码是一次性验证码。类似地，在本发明的一个优选实施例中，网络包括无线通信网络。用户设备可以包括移动电话。类似地，用户设备可以包括智能卡。在本发明的一个特定优选实施例中，消息是 SMS 消息。

从再一个方面来观看本发明，现在提供了向用户设备提供一组访问码的设备，该设备包括：用户设备；和通过通信网络与用户设备通信的服务器；

该用户设备包括存储加密密钥和标识码的装置、和通过网络将包含标识码的消息发送到服务器的装置；服务器包括存储与存储在用户设备中的密钥相对应的加密密钥的装置、一旦从用户设备接收到标识码就分配该组访问码的装置、根据在消息中接收的标识码执行查找功能以便从存储器中检索密钥的装置、利用检索的密钥加密该组访问码以生成加密组的装置、和通过网络将包含加密组的消息发送到用户设备的装置；和用户设备进一步包括利用存储器中的密钥解密从服务器接收的加密组的装置、和存储解密组访问码供用户设备的用户使用的装置。

本发明进一步推广到通过通信网络从服务器接收一组访问码的用户设备，该设备包括：存储加密密钥和标识码的装置；通过通信网络将包含标识码的消息发送到服务器的装置；从服务器接收包含用密钥加密的该组访问码的消息的装置；利用存储器中的密钥解密接收组访问码的装置；和存储解密组访问码供用户设备的用户使用的装置。

另外，本发明推广到通过通信网络向用户设备提供一组访问码的服务器，该服务器包括：存储与存储在用户设备中的加密密钥相对应的加密密钥的装置；一旦通过网络从用户设备接收到包含标识码的消息就将该组访问码分配给用户设备的装置；根据在消息中接收的标识码执行查找功能以便从存储器中检索密钥的装置；利用检索的密钥加密该组访问码以生成加密组的装置；和通过网络将包含加密组的消息发送到用户设备的装置。

在本发明的一个优选实施例中，提供了与传统方案相比，对于客户和例如，金融服务提供者两者来说既更加安全又更加方便的安全交易方案。本发明的特定优选实施例包括：以抗篡改方式存储一个或多个暂存表的智能卡；方便地访问存储在智能卡上的暂存表的移动设备；和为了更加存储在智能卡上的暂存表，在移动设备和服务器计算机之间的无线通信信道上进行加密消息传送。有利的是，不需要作出与无线通信信道的安全或加密能力有关的假设。移动设备可以是移动电话、和个人数字助理（PDA）等。智能卡可以是插入移动电话等中的 SIM 模块。无线通信信道可以是 GSM 信道中的短消息服务（SMS）等。

在马上要描述的本发明的一个优选实施例中，移动设备通过移动电话来实现；智能卡通过 SIM 模块来实现；和无线通信信道通过 GSM 网络中的 SMS 信道来实现。在这个实施例中，客户配有含有 SIM 模块的移动电话。SIM 模

块包括中央处理单元和内存。在内存中存储着 Java（Sun Microsystems 公司的商标）兼容操作平台软件和 Java 工具箱小应用程序软件。操作平台软件配置执行工具箱的 CPU。工具箱有助于 OTAC 的管理。可以在为客户定制 SIM 期间将工具箱装入内存中。可替代地，如果 GSM 网络服务提供者允许，可以通过 GSM 网络动态地将工具箱装入内存中和更新工具箱。访问内存中的工具箱受客户通过移动电话设置的个人识别号（PIN）保护。

在本发明的一个特定优选实施例中，银行通过传统邮递系统向客户发送启动纸邮件。启动纸邮件包含：诸如 16 字节 DES（数据加密标准）密钥之类的客户专用对称密钥 K；客户标识（ID）码 N；和银行上的 SMS 兼容服务器的电话号码。ID 码 N 由银行用于识别客户。ID 码 N 无需是客户帐号，而是可以通过唯一随机信息来实现。

一旦客户开始激活，工具箱请求客户通过移动电话的小键盘输入密钥 K、信息 N、和服务器的电话号码。然后，工具箱将包含标识码 N 的初始化 SMS 消息发送到服务器。初始化消息指示允许使用工具箱。服务器通过向客户发送包含用密钥 K 加密的 OTAC 列表的 SMS 回答消息，对初始化消息的接收作出响应。取决于要传送的数据量，OTAC 列表可以涵盖一系列 SMS 消息。工具箱利用密钥 K 解密接收的 OTAC 列表。然后，初始化即告完成。当客户需要 OTAC 时，为了在，例如，因特网上进行联机金融交易，客户再次将 PIN 输入移动电话中以解锁工具箱，和取决于银行的 OTAC 分配系统，从工具箱中请求下一个 OTAC 或特定 OTAC。工具箱关注发放的 OTAC。当工具箱存储的所有 OTAC 都已发放时，从服务器获取新 OTAC 列表。正如前面所述的那样，通过 SMS 信道再次传送新列表。服务器还无时无刻关注每个客户使用了多少和哪些 OTAC，并且，在需要时自动开始更新。注意，这种方案只涉及到服务器和客户 SIM 模块中的工具箱之间的端到端加密。不需要作出与介入无线信道的安全有关的假设。

在本发明的另一个优选实施例中，通过无线信道将用密钥 K 加密的新密钥 K'从服务器发送到工具箱，可以按需更新密钥 K。此后，工具箱只接受用新密钥 K'加密的消息。新密钥 K'的分配可以与新 OTAC 列表的分配一起完成。可替代地，新密钥 K'的分配可以与新 OTAC 列表的分配无关地完成。

在本发明的又一个优选实施例中，服务器可以通过无线信道将用密钥 K 加密的另一个密钥 S 发送到工具箱。其它密钥 S 可以用于，例如，签名核实。

然后，在用密钥K加密之前，用签名密钥S签名来自服务器的进一步消息。然后，工具箱可以据此核实签名。

在本发明的进一步实施例中，取代如上所述的对称密码术，应用非对称密码术。在这种情况下，客户无需人工输入起始对称密钥 K。取而代之，在SIM模块上，工具箱生成诸如1024位RSA（里韦斯特-沙米尔-阿德莱曼）密钥对的公开/秘密密钥对。然后，工具箱通过通信信道将公开密钥E与ID码N 一起发送到服务器来启动自己。对于到工具箱的每个消息，服务器现在生成对称会话密钥。在每种情况下，服务器都用会话密钥加密消息，用公开密钥E加密会话密钥，和通过通信信道将加密消息与加密会话密钥一起发送到工具箱。工具箱用它的秘密密钥D解密会话密钥。然后，工具箱利用解密会话密钥解密每个消息以还原OTAC列表。

服务器还可以将公开/秘密密钥应用于签名生成和核实，将它的公开密钥发送到工具箱供进一步核实动作之用。注意，服务器可以将用于签名核实的同一公开密钥发放给可能由拥有预存在智能卡上的公开密钥的可信第三方证书管理机构签名的所有工具箱。

在本发明的进一步实施例中，移动设备和智能卡的至少一个包括诸如红外线或感应接口之类的非接触接口。该接口允许通过数据终端访问智能卡上的工具箱。一旦客户通过数据终端发出请求，就可以通过该接口读取OTAC。这样的请求可以通过，例如，数据终端的键盘发出。可替代地，无需要求这样的人工请求，也可以通过该接口读取 OTAC。在智能卡和数据终端之间可以应用各种各样问答式方案。例如，数据终端本身可能不访问 OTAC。取而代之，数据终端可以将问题发送到工具箱。接着，工具箱根据OTAC生成问题的答案。例如，如果OTAC有效地包括诸如3 DES密钥之类的密码式密钥，工具箱可以数字签名和/或用OTAC加密该问题。如此计算的答案可以用于验证或启动交易。

应该认识到，本发明的优点是多方面的。本发明的一个优点是提供了将OTAC 分配给用户设备的安全技术。这样用户设备的例子包括配有抗篡改智能卡技术的移动设备，从而无论何时何地需要都不会妨碍方便地访问OTAC。这样的访问可以人工启动，也可以通过无线信道自动启动。本发明尤其对金融应用有吸引力，因为不要求对过去应用在银行中的典型计算机基础设施作任何改变。使OTAC列表的分配更便宜、更简单、和更安全。此外，利用现

有基础设施意味着，无需将另外 OTAC 专用移动设备和/或智能卡发放给已经拥有带有允许下载和执行工具箱小应用程序的 SIM 卡的移动电话的客户。

现在参照附图，只通过举例的方式描述本发明的优选实施例，在附图中：

图 1 是数据处理网络的方块图；

图 2 是网络的智能卡的方块图；

图 3 是网络的移动设备的方块图；

图 4 是网络的服务器计算机系统的方块图；

图 5 是与智能卡相联系的流程图；

图 6 是智能卡的内存的方块图；

图 7 是与服务器相联系的流程图；

图 8 是与智能卡相联系的另一个流程图；

图 9 是智能卡内存的另一个方块图；

图 10 是与智能卡相联系的又一个流程图；

图 11 是与存储在智能卡的内存中的 OTAC 的更新相联系的另一个流程图；

图 12 是与服务器相联系的另一个流程图；

图 13 是与智能卡相联系的进一步流程图；

图 14 是与智能卡相联系的再一个流程图；

图 15 是与服务器相联系的进一步流程图；

图 16 也是与智能卡相联系的流程图；和

图 17 是使本发明具体化的数据处理系统的方块图。

首先参照图 1，使本发明具体化的数据处理网络包括以移动电话形式出现的用户设备 100，用户设备 100 可通过含有以 GSM 访问网络形式出现的无线访问网络的通信网络基础设施 300 与服务器计算机系统 200 连接。以 SIM 卡形式出现的智能卡 10 也可通过用户设备 100 与网络连接。

现在参照图 2，智能卡 10 包括均通过总线子系统 50 互连的内存 20、中央处理单元（CPU）30、加密引擎 90、和输入/输出（I/O）子系统 40，在内存 20 中存储着 CPU 30 可执行的计算机程序代码。计算机程序代码包括以 Java 兼容操作平台形式出现的操作系统 60 和以 Java 小应用程序形式出现的工具

箱 70 应用软件。内存 20 还有助于以抗篡改方式存储暂存表 80。暂存表 80 包括数个 OTAC。操作系统 60 将 CPU 30 配置成执行工具箱 70。工具箱 70 有助于管理暂存表 80 中的 OTAC。马上将详细描述工具箱 70 的功能的一些方面。加密引擎 80 包括加密和解密从智能卡 10 发送的和由智能卡 10 接收的数据的密码处理逻辑单元。密码处理逻辑单元可以用硬件、软件、或硬件和软件的组合来实现。

参照图 3，用户设备 100 包括均通过总线子系统 120 互连的含有 RF 天线 170 的射频（RF）级 110、控制逻辑单元 130、视频显示器 140、和小键盘 160。智能卡 10 可移动地插入用户设备 100 中和智能卡 10 的 I/O 子系统 40 可释放地与用户设备 100 的总线子系统 40 连接。在操作过程中，RF 级 110 和 RF 天线有助于用户设备 100 和与网络 300 连接的其它设备之间的无线通信视频显示器 140 为诸如准备消息和读取消息之类的功能提供用户和用户设备之间的图形用户界面。小键盘 160 为诸如数据输入和呼叫管理之类的功能向用户提供用户设备 10 的小键盘控制。控制逻辑单元 130 根据从，例如，小键盘 160 接收的输入，控制诸如呼叫管理之类用户设备 100 的功能。来自用户设备 100 的输出，譬如，视频显示单元 140 上的数据显示或通过 RF 级 110 的呼出，也受控制逻辑单元 130 控制。类似地，控制逻辑单元 130 协调来自智能卡 10 和用户设备 100 的其它单元的数据通过总线子系统 120 的传送。控制逻辑单元 130 可以用专用硬件、编程 CPU、或专用硬件和编程 CPU 的组合来实现。

参照图 4，服务器 200 包括均通过总线子系统 240 互连的内存 210、CPU 220、和 I/O 子系统 230。在内存 210 中存储着可由 CPU 220 执行的计算机程序代码。计算机程序代码包括操作系统 250 和 OTAC 服务应用软件 260。操作系统 250 将 CPU 220 配置成执行 OTAC 服务 260。OTAC 服务 260 有助于管理用户设备 100 中的 OTAC。马上将详细描述 OTAC 服务 260 的功能的一些方面。

在操作过程中，在用户设备 100 和服务器 200 之间建立以 SMS 信道形式出现的无线通信信道。SMS 信道有助于暂存表 80 从服务器 200 中的 OTAC 服务 260 通过用户设备 100 到智能卡 10 的安全传送。可以在为用户配置智能卡 10 期间将工具箱 70 装入用户设备 100 的内存 20 中。可替代地，如果网络基础设施 300 允许，可以通过网络基础设施 300 动态地将工具箱 70 装入内存

20 中和更新工具箱 70。访问内存 20 中的工具箱 70 受用户通过移动设备 100 设置的 PIN 保护。小键盘 160 可以用于这个目的。可替代地，如果用户设备 100 拥有语音识别功能，可以口头设置和重新设置 PIN。其它设备可以支持数据输入的更进一步装置。

在本发明的特定优选应用中，服务器 200 放在银行和用户设备 100 的用户是银行的客户。最初，银行将纸邮件供应给用户。纸邮件可以通过，例如，传统邮递系统供应。纸邮件包含：诸如 16 字节 DES 密钥之类的客户专用对称密钥 K；客户标识（ID）码 N；通过基础设施 300 访问服务器 200 的电话号码。银行利用 ID 码 N 来识别用户。ID 码 N 无需是用户的客户帐号，而是可以通过唯一随机信息来实现。

现在参照图 5，对于第一次激活工具箱 70，用户通过小键盘 160 输入 PIN。参见步骤 400。一旦接收到 PIN，工具箱 70 请求用户通过小键盘 160 输入密钥 K、ID 码 N、和服务器 200 的电话号码。参见步骤 410。此外，如果用户设备 100 拥有语音识别功能，可以口头输入这个数据。但是，应该认识到，由于有人可能偷听用户朗读数据，这是一种较不安全的输入技术。一旦接收上面列出的用户输入，工具箱 70 就将包含标识码 N 的初始化 SMS 消息发送到服务器 200 上的 OTAC 服务 260。参见步骤 420。初始化消息向 OTAC 服务 260 指示工具箱 70 已经被启动。参照图 6，智能卡上的内存 20 现在包含 PIN、密钥 K、和 ID 码 N。

参照图 7，在服务器 200 上一旦接收到初始化消息，OTAC 服务 260 就根据 ID 码 N 查找用户和检索发放给用户的密钥 K。参见步骤 430。然后，OTAC 服务 260 利用密钥 K 为用户加密 OTAC 的新暂存表。参见步骤 440。然后，OTAC 服务 260 将包含加密列表的 SMS 回答消息发送到工具箱 70。取决于要发送的数据量，该列表可以涵盖一系列 SMS 消息。

转到图 8，在用户设备 200 上一旦接收到回答消息，工具箱 70 就提取加密列表。参见步骤 460。工具箱 70 使用加密引擎 90 来利用密钥 K 解密列表。参见步骤 470。然后，工具箱 70 将解密列表存储在内存 60 中。参见步骤 480。然后，初始化即告完成。参照图 9，内存 20 现在包含密钥 K、PIN、ID 码 N、和 OTAC 的列表。

现在参照图 10，当用户需要 OTAC 时，为了在，例如，因特网上进行金融交易，用户再次通过小键盘 160 输入 PIN 以解锁工具箱 70。参见步骤 500。

然后，用户向工具箱 70 请求 OTAC。参见步骤 510，取决于银行应用的 OTAC 分配系统，OTAC 可以是列表中的下一个 OTAC 或特定 OTAC。工具箱 70 跟踪发放的 OTAC。参见步骤 520。

为了更新存储在内存 20 中的 OTAC 的列表 80，可以应用许多方法。例如，在本发明的一个优选实施例中，OTAC 的列表 80 的更新由工具箱 70 自动触发。具体地说，参照图 11，每当在步骤 530 中使用 OTAC 时，工具箱 70 进行测试，以确定保留在列表 80 中的未用 OTAC 的个数是否小于预定阈值。参见步骤 540。在未用 OTAC 的个数大于预定阈值的情况下，工具箱 70 等待下一个 OTAC 被使用。但是，在达到阈值的情况下，工具箱 70 自动生成消息和通过网络 300 将消息发送到服务器 200，以请求 OTAC 的新列表。ID 码 N 包括在前面参照图 5 所述的请求消息中，以便服务器 200 中的 OTAC 服务 260 可以查找适合加密 OTAC 新列表的密钥。具体地说，正如前面参照图 7 所述的那样，通过信道将新列表传送给智能卡 10。在本发明的另一个实施例中，存储在内存 20 中的 OTAC 的列表 80 由服务器 200 上的 OTAC 服务 260 自动更新。具体地说，再次参照图 11，服务器 200 上的 OTAC 服务 260 现在无时无刻关注每个客户已经使用了多少和哪些 OTAC。参见步骤 530。每当 OTAC 被使用时，OTAC 服务 260 就确定保留在列表中的未用 OTAC 的个数是否小于预定阈值。参见步骤 540。如果不是，OTAC 服务 260 等待下一个 OTAC 被使用。如果是，正如前面参照图 7 所述的那样，OTAC 服务 260 自动将用密钥 K 加密的新列表发送到工具箱 70。可以将前面所述的阈值设置成当所有以前发放的 OTAC 都用完时发放新列表 80。可替代地，可以将阈值设置成当旧列表中只剩下预置个 OTAC 未使用时发放新列表 80。在本发明的又一个实施例中，存储在内存 20 中的 OTAC 的列表 80 的更新可以由用户人工触发。具体地说，响应到用户设备 100 的人工输入，工具箱 70 生成消息和通过网络 300 将消息发送到服务器 200，以请求 OTAC 的新列表。ID 码 N 包括在前面参照图 5 所述的请求消息中，以便服务器 200 中的 OTAC 服务 260 可以查找适合加密 OTAC 新列表的密钥。此外，正如前面参照图 7 所述的那样，通过信道将新列表传送给智能卡 10。注意，这些更新方案只涉及到 OTAC 服务 260 和工具箱 70 之间的端到端加密。不需要作出与介入网络基础设施 300 的安全有关的假设。

在前面参照图 5－11 所述的本发明的优选实施例的一个变体中，可以按

需更新存储在内存 20 中的密钥 K。具体地说，参照图 12，OTAC 服务 260 生成新密钥 K'。参见步骤 550。OTAC 服务 260 用现有密钥 K 加密新密钥 K'。参见步骤 560。然后，OTAC 服务 260 通过网络基础设施 300 将包含用现有密钥 K 加密的新密钥 K'的 SMS 消息发送到工具箱 70。

参照图 13，工具箱 70 接收加密新密钥 K'。参见步骤 600。工具箱 70 利用存储在内存 20 中的现有密钥 K，通过加密引擎 280 解密新密钥 K'。参见步骤 610。然后，工具箱 70 用新密钥 K'取代内存 20 中的现有密钥 K。此后，工具箱 70 只接受用新密钥 K'加密的消息。新密钥 K'的分配可以与新列表的分配一起由服务器完成。可替代地，新密钥 K'的分配可以与新列表的分配无关地完成。

在前面参照图 5－11 所述的本发明的优选实施例的另一个变体中，OTAC 服务 260 通过网络基础设施 300 将用密钥 K 加密的另一个密钥 S 发送到工具箱 70。其它密钥 S 可以用于，例如，签名核实。然后，在用密钥 K 加密之前，用签名密钥 S 签名来自 OTAC 服务 260 的进一步消息。然后，工具箱 70 可以据此核实签名。密钥 K 和 S 未必不同。

在前面所述的本发明的优选实施例中，应用了对称密码术。但是，在本发明的另一个实施例中，应用非对称密码术。在这个实施例中，用户无需人工输入起始对称密钥 K。参照图 14，工具箱 70 通过加密引擎 280，取而代之生成诸如 1024 位 RSA 密钥对的公开/秘密密钥对。参见步骤 630。然后，工具箱 70 通过通信基础设施 300 将密钥对的公开密钥 E 与 ID 码 N 一起发送到 OTAC 服务 260。参见步骤 640。现在工具箱 70 已被启动。

现在参照图 15，OTAC 服务 260 现在生成对称安全会话密钥 P。参见步骤 650。OTAC 服务 260 生成包含 OTAC 列表的消息。参见步骤 660。OTAC 服务 260 现在用会话密钥 P 加密消息。参见步骤 670。OTAC 服务 260 还用公开密钥 E 加密会话密钥 P。参见步骤 680。然后，OTAC 服务 260 通过通信基础设施 300 将加密消息与加密会话密钥 P 一起发送到工具箱 70。参见步骤 690。参照图 16，工具箱 70 通过加密引擎 280，用它的秘密密钥 D 解密会话密钥 P。参见步骤 700。然后，工具箱 70 通过加密引擎 280，用解密会话密钥解密消息。参见步骤 710。然后，工具箱 70 从解密消息中还原列表。参见步骤 720。

在本发明的一个优选实施例中，OTAC 服务 260 还将公开/秘密密钥对应

用于签名生成和核实。OTAC服务260将它的公开密钥发送到工具箱70供将来核实动作之用。注意，OTAC服务260可以将用于签名核实的同一公开密钥发放给可能由拥有预存在智能卡上的公开密钥的可信第三方证书管理机构签名的、它服务的所有工具箱70。

参照图17，在本发明的另一个实施例中，用户设备100包括诸如红外线或感应接口之类的非接触接口800。该接口800允许通过数据终端810访问智能卡10上的工具箱70。数据终端810也包括与用户设备100的接口800通信的非接触接口880。数据终端800进一步包括与接口880一起都通过总线子系统820互连的小键盘830、显示器840、和I/O子系统850。I/O子系统850通过介入数据网络860与远程交易处理计算机系统870连接。

在操作过程中，数据终端810可以响应客户通过数据终端810的小键盘830发出的请求，从驻留在用户设备10中的智能卡10中读取OTAC。可替代地，无需要求这样的人工请求，数据终端810也可以通过接口800读取OTAC。在智能卡10和数据终端810之间可以应用各种各样问答式方案。例如，在本发明的一个优选实施例中，数据终端80不访问OTAC。取而代之，数据终端810将问题发送到智能卡10中的工具箱70。接着，工具箱70根据OTAC生成问题的答案。例如，如果OTAC有效地包括诸如3 DES密钥之类的密码式密钥，工具箱70可以数字签名和用OTAC加密该问题。如此计算的答案可以用于验证或启动交易。在本发明的其它实施例中，非接触接口800可以与智能卡800合并在一起，而不是与用户设备100合并在一起。

在前面所述的本发明的优选实施例中，用户设备100以移动电话的形式出现。但是，在本发明的其它实施例中，用户设备10可以具有不同形式，譬如，PDA、便携式计算机、膝上型计算机等。类似地，在前面所述的本发明的优选实施例中，无线网络用于实现用户设备100和服务器200之间的连接。但是，在本发明的其它实施例中，有线网络或无线网络和有线网络的组合可以用于实现用户设备100和服务器200之间的连接。另外，在前面所述的本发明的优选实施例中，通过SMS信道实现用户设备100和服务器200之间的无线通信。但是，在本发明的其它实施例中，可以应用不同形式的消息传送服务。并且，在前面所述的本发明的优选实施例中，智能卡10以SIM模块的形式出现。但是，在本发明的其它实施例中，智能卡10可以具有不同形式，譬如，信用卡或收费卡形式。其它类似形式的专用处理器系统也可以用于取

代智能卡 10。在本发明的实施例中，Java 兼容操作系统 60 用在智能卡 10 中，以便执行以 Java 小应用程序形式出现的工具箱 70。但是，在本发明的其它实施例中，可以应用不同形式的智能卡操作系统和相应不同形式的工具箱应用软件。更进一步，在本发明的优选实施例中，访问码以一次性标识码的形式出现。但是，应该认识到，本发明同样可应用于传送其它类型的访问码，譬如，访问，例如，受限区的进入码。本发明的许多其它应用是显而易见的。

总而言之，本文通过本发明的例子描述了向用户设备提供一组访问码的方法，该方法包括：在用户设备中，存储加密密钥和标识码，和通过通信网络将包含标识码的消息发送到服务器。在服务器中，与存储在用户设备中的密钥相对应地存储加密密钥，一旦从用户设备接收到标识码就分配该组访问码。根据在消息中接收的标识码执行查找功能以便从存储器中检索密钥。利用检索的密钥加密该组访问码以生成加密组。通过网络将包含加密组的消息发送到用户设备。在用户设备中，利用存储器中的密钥解密从服务器接收的加密组，和存储解密组访问码供用户设备的用户使用。

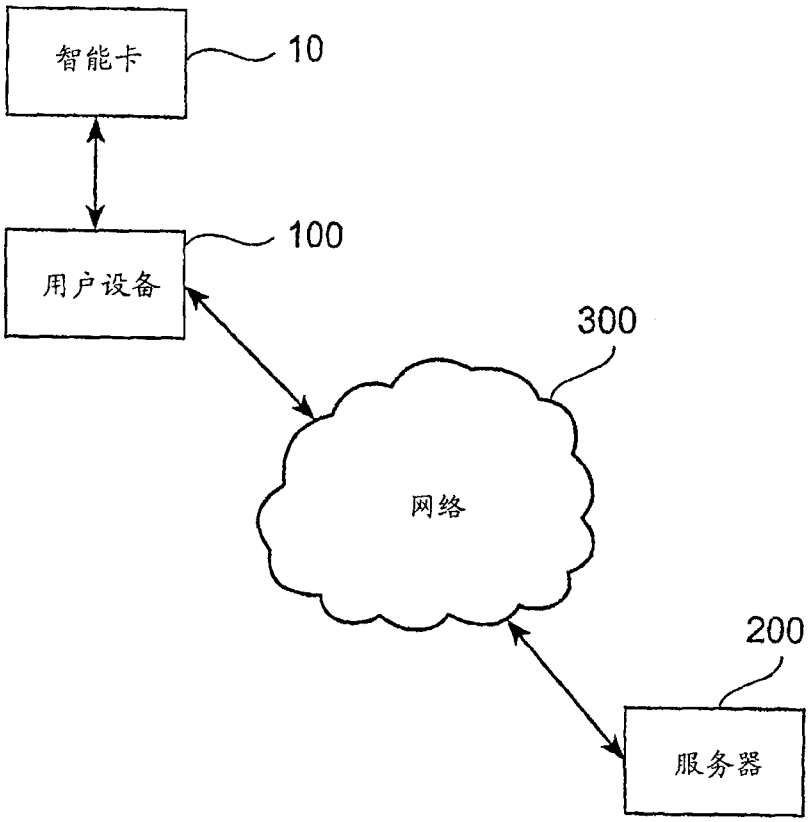


图 1

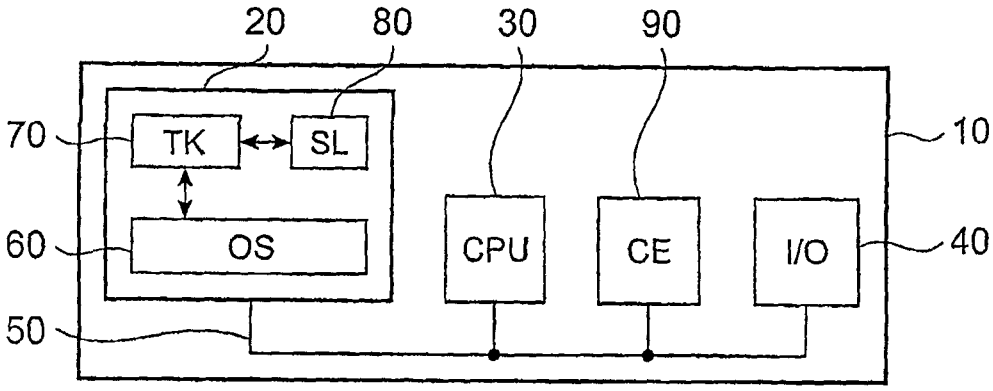

20
80
30
90
70
TK
SL
10
60
OS
CPU
CE
I/O
40
50

图 2

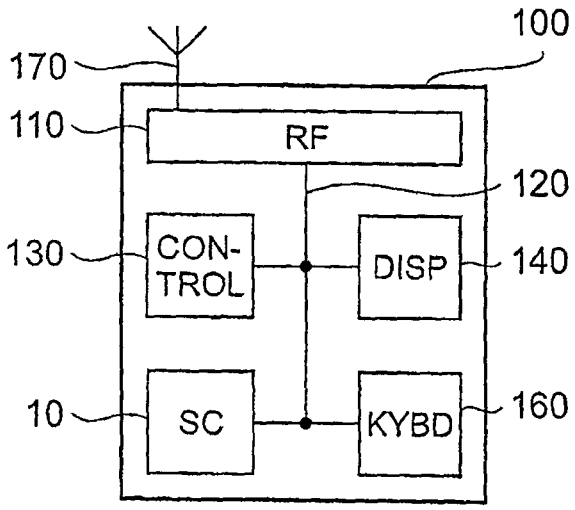

100
170
110
RF
120
130
CON-
TROL
DISP
140
10
SC
KYBD
160

图 3

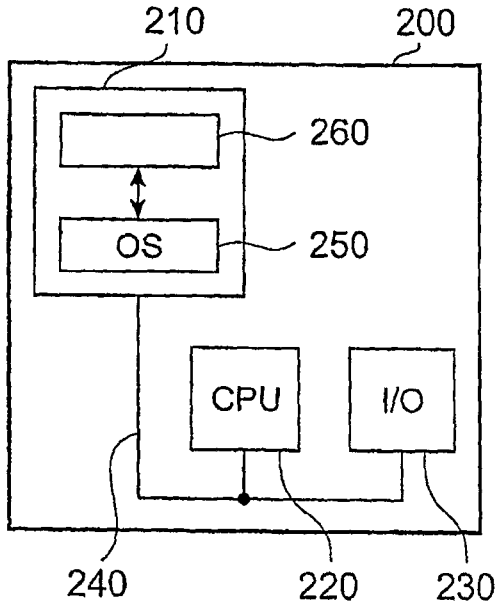

210
200
260
OS
250
CPU
I/O
240
220
230

图 4

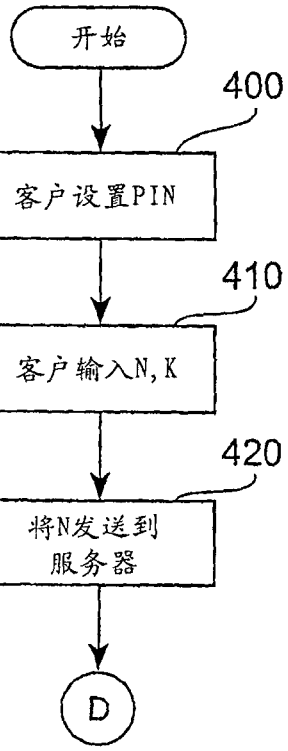

开始
400
客户设置PIN
410
客户输入N,K
420
将N发送到
服务器
D

图 5

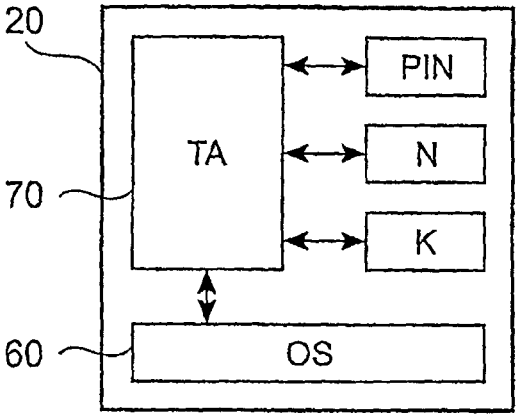

20
TA
PIN
N
K
70
60
OS

图 6

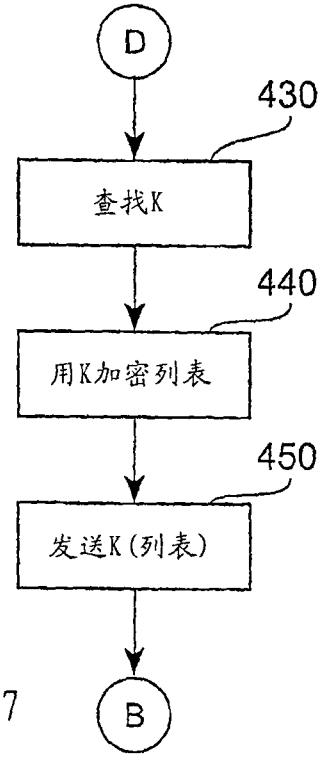

D
430
查找K
440
用K加密列表
450
发送K(列表)
B

图 7

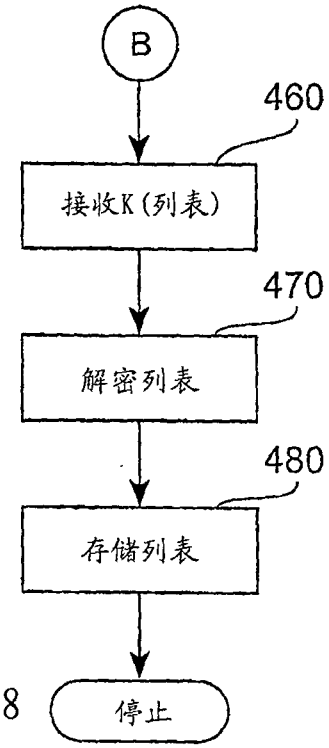

B
460
接收K(列表)
470
解密列表
480
存储列表
停止

图 8

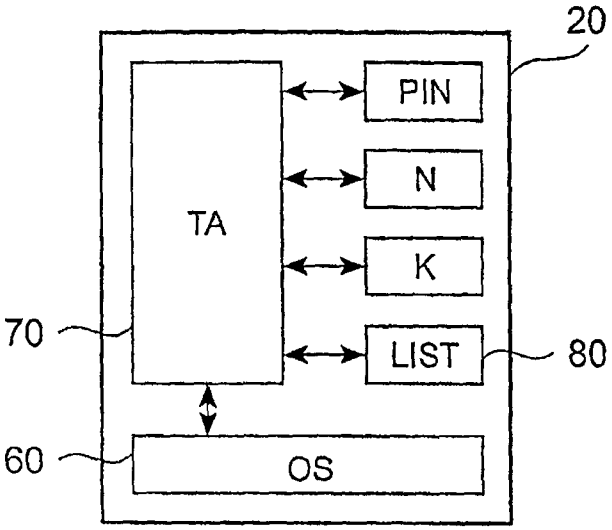

20
PIN
N
K
LIST
TA
70
80
60
OS

图 9

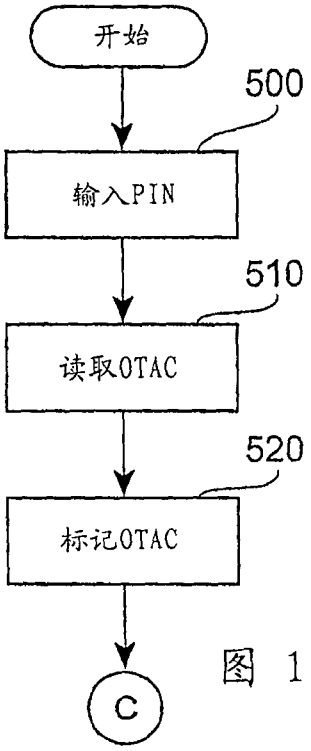

开始
500
输入PIN
510
读取OTAC
520
标记OTAC
C

图 10

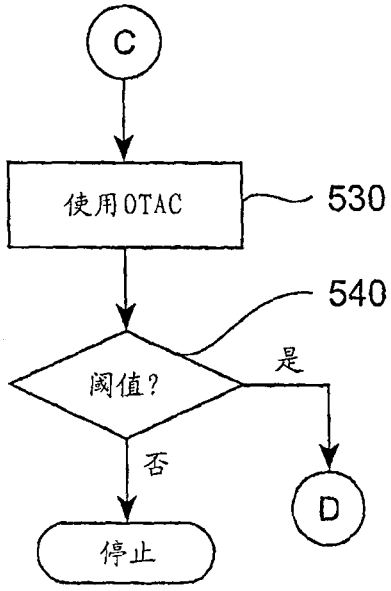

C
使用OTAC
530
540
阈值?
是
否
D
停止

图 11

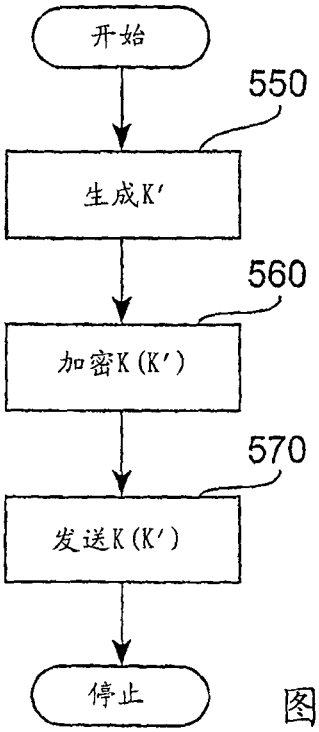

开始
550
生成K′
560
加密K(K′)
570
发送K(K′)
停止

图 12

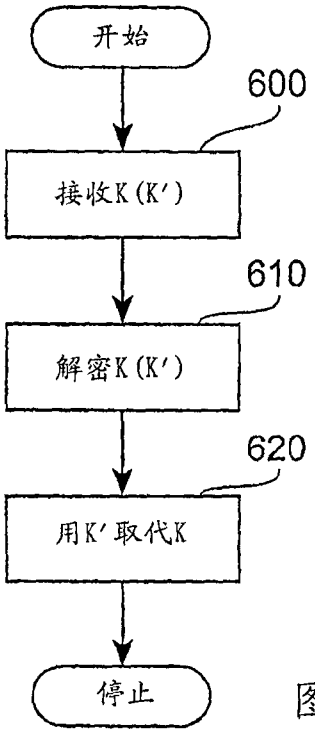

开始
600
接收K(K′)
610
解密K(K′)
620
用K′取代K
停止

图 13

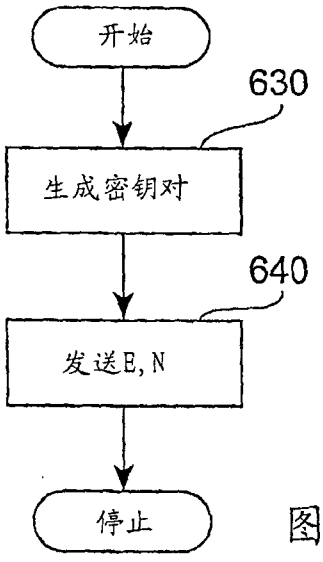

开始
630
生成密钥对
640
发送E,N
停止

图 14

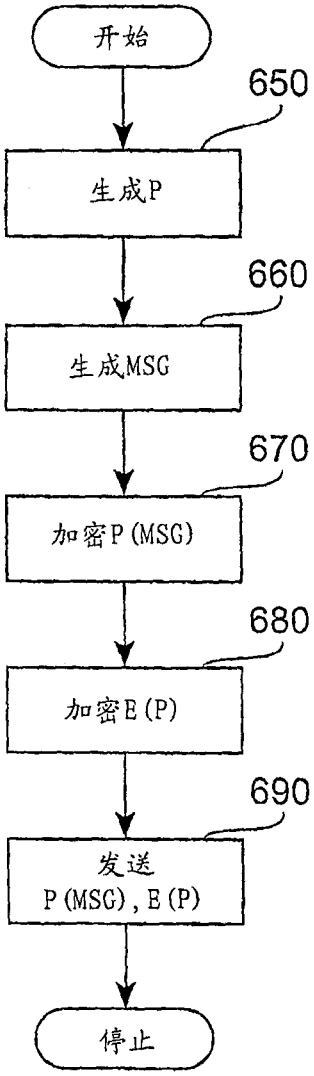

开始
650
生成P
660
生成MSG
670
加密P(MSG)
680
加密E(P)
690
发送
P(MSG),E(P)
停止

图 15

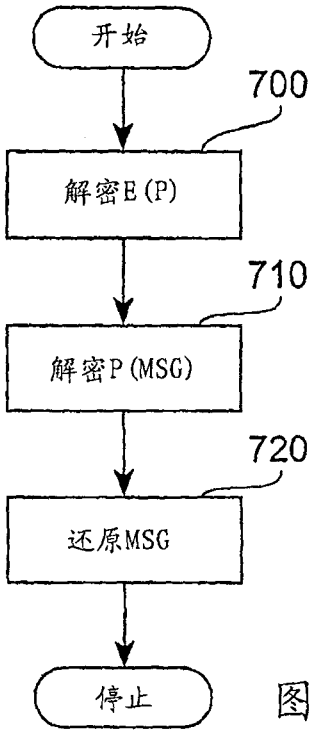

开始
700
解密E(P)
710
解密P(MSG)
720
还原MSG
停止

图 16

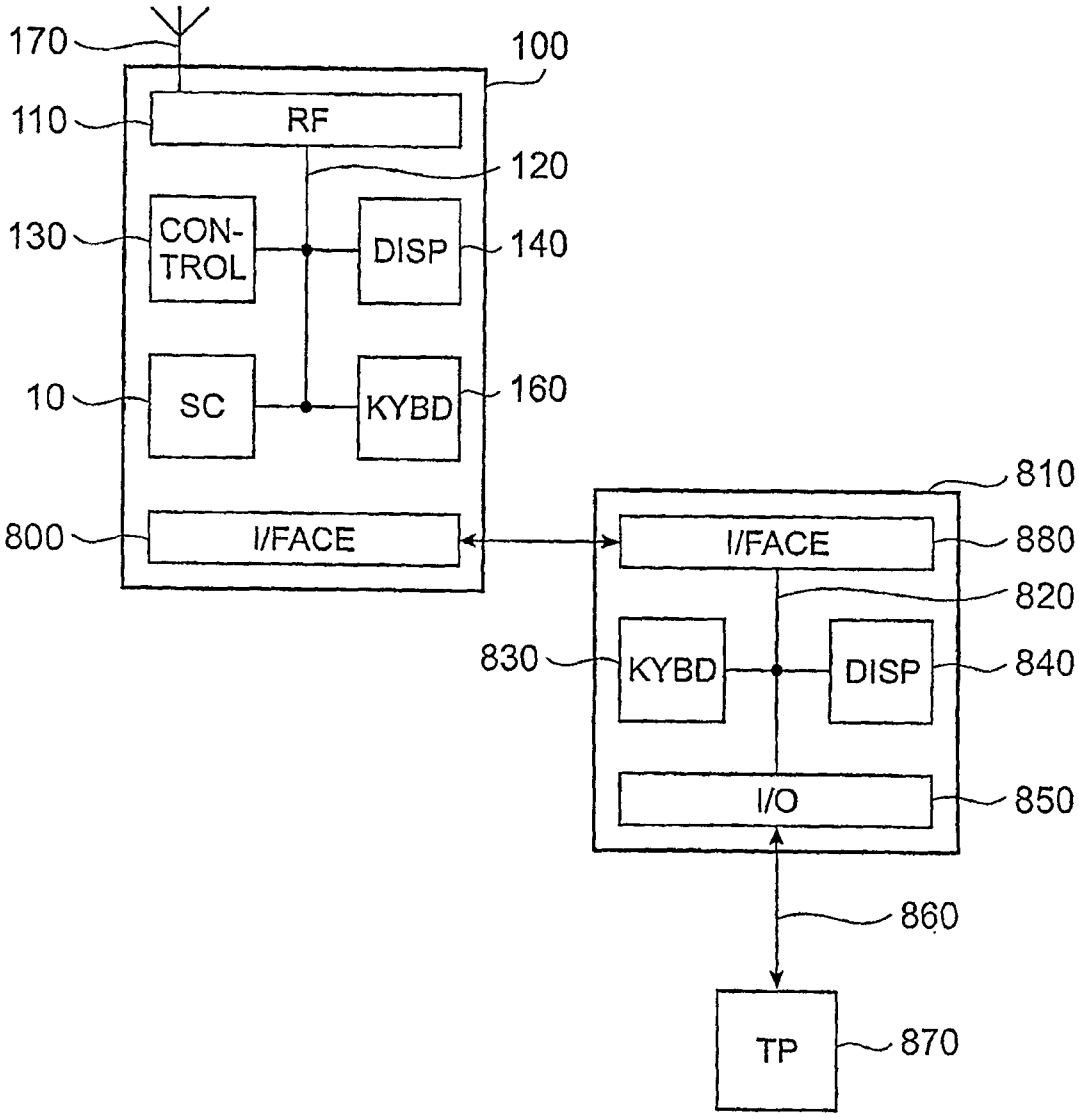

170
100
110
RF
120
130
CON-
TROL
DISP
140
10
SC
KYBD
160
800
I/FACE
810
I/FACE
880
820
830
KYBD
DISP
840
I/O
850
860
TP
870

图 17