(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105052072 A
(43)申请公布日 2015.11.11

(21)申请号 201380073932.2
(22)申请日 2013.12.27
(30)优先权数据
61/746,892 2012.12.28 US
(85)PCT国际申请进入国家阶段日
2015.08.27
(86)PCT国际申请的申请数据
PCT/US2013/077961 2013.12.27
(87)PCT国际申请的公布数据
WO2014/106031 EN 2014.07.03
(71)申请人 威斯科数据安全国际有限公司
地址 瑞士格拉特布吕格
(72)发明人 迪尔克·马里恩 弗兰克·库利耶
弗兰克·霍尔内特
弗雷德里克·门内斯
(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 康建峰 李春晖
(51)Int.Cl.
H04L 9/32(2006.01)

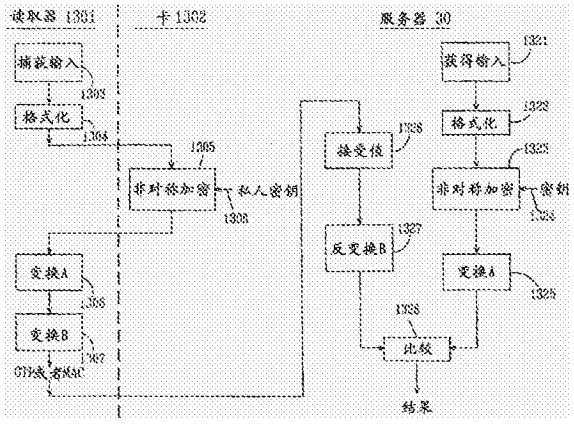
权利要求书7页 说明书49页 附图21页

(54)发明名称

远程认证和业务签名

(57)摘要

公开了一种用于生成动态凭证的认证设备和方法。认证设备包括用于与安全设备例如智能卡通信的通信接口。可以通过以下步骤来生成一次性口令(OTP)或消息认证代码(MAC):从服务器接收使用公共/私人密钥对的公共密钥利用非对称加密算法加密的经加密初始化种子;将经加密的初始化种子提交至安全设备;在所述安全设备处使用公共/私人密钥对的私人密钥对经加密的初始化种子进行解密;将经解密的初始化种子返回至认证设备;在认证设备处根据经解密的初始化种子来导出秘密凭证生成密钥;以及通过使用对称密码动态凭证生成算法将动态变量与秘密凭证生成密钥进行组合来生成动态凭证。



CN 105052072 A

1. 一种用于生成动态凭证的认证设备，包括：

存储器部件，所述存储器部件用于存储秘密凭证生成密钥；

用户输入接口，所述用户输入接口用于接收来自用户的输入；

通信接口，所述通信接口用于与所述用户的安全设备进行通信，所述安全设备存储与所述用户关联的第一公共/私人密钥对的第一私人密钥，并且所述安全设备适于利用所述第一私人密钥来执行非对称密码计算，其中，所述非对称密码计算至少包括非对称密码解密操作；

数据输入接口，所述数据输入接口用于接收包括初始化种子的初始化消息，所述初始化种子的至少第一部分利用所述第一公共/私人密钥对的第一公共密钥进行加密；以及

处理部件，所述处理部件适于使用将所述秘密凭证生成密钥与动态变量密码地组合的对称密码算法来生成动态凭证；

其中，所述认证设备适于：

从所述初始化消息中提取所述初始化种子的经加密的至少所述第一部分，

使用所述通信接口向所述用户的安全设备提交所述初始化种子的经加密的所述第一部分，以便所述安全设备使用所述私人密钥和所述非对称密码解密操作将所述初始化种子的经加密的所述第一部分进行解密，

使用所述通信接口从所述安全设备接收由所述安全设备解密的所述初始化种子的所述第一部分，以及

根据所述初始化种子的经解密的至少所述第一部分来导出所述秘密凭证生成密钥的值。

2. 根据权利要求 1 所述的认证设备，其中，所述初始化种子的经加密的所述第一部分包括整个所述初始化种子。

3. 根据权利要求 2 所述的认证设备，其中，所述初始化种子包括所述秘密凭证生成密钥。

4. 根据权利要求 1 所述的认证设备，还适于限制所述秘密凭证生成密钥的使用期限。

5. 根据权利要求 4 所述的认证设备，还适于确定是否已超过所述秘密凭证生成密钥的使用期限，并且在确定出已超过所述秘密凭证生成密钥的使用期限之后丢弃所述秘密凭证生成密钥。

6. 根据权利要求 5 所述的认证设备，其中，所述秘密凭证生成密钥的使用期限基于从特定事件开始所经过的时间，并且所述认证设备还适于在经过预定的时间段之后丢弃所述秘密凭证生成密钥。

7. 根据权利要求 6 所述的认证设备，其中，所述特定事件是所述秘密凭证生成密钥何时由所述认证设备导出。

8. 根据权利要求 5 所述的认证设备，其中，所述秘密凭证生成密钥的使用期限基于从所述秘密凭证生成密钥的当前值被所述认证设备导出开始所述秘密凭证生成密钥的当前值已经被用于生成动态凭证的次数。

9. 根据权利要求 8 所述的认证设备，还适于在所述认证设备获得所述秘密凭证生成密钥的当前值之后对所述认证设备已使用所述秘密凭证生成密钥的次数进行计数，并且当该次数超出某一固定阈值时丢弃该当前值。

10. 根据权利要求 9 所述的认证设备，还适于在所述秘密凭证生成密钥为生成动态凭证而被使用一次之后丢弃所述秘密凭证生成密钥。

11. 根据权利要求 5 所述的认证设备，其中，鉴于某些事件来限定所述秘密凭证生成密钥的使用期限。

12. 根据权利要求 11 所述的认证设备，还适于要求提供所述安全设备以生成动态凭证，并且当移除所述安全设备时丢弃所述秘密凭证生成密钥。

13. 根据权利要求 5 所述的认证设备，其中，丢弃所述秘密凭证生成密钥包括 ：从所述存储器部件擦除所述秘密凭证生成密钥的值。

14. 根据权利要求 5 所述的认证设备，还适于在所述秘密凭证生成密钥被丢弃之后再生所述秘密凭证生成密钥的值。

15. 根据权利要求 14 所述的认证设备，还适于在所述存储器部件中存储与所述秘密凭证生成密钥关联的包括第一再生值的数据集合 ；以及

其中，所述认证设备再生所述秘密凭证生成密钥的值包括 ：

所述认证设备向所述用户的安全设备提交所述第一再生值，以使所述用户的安全设备使用存储在所述用户的安全设备中的第二公共 / 私人密钥对的第二私人密钥利用非对称加密算法来处理所述第一再生值 ；

从所述用户的安全设备接收由所述用户的安全设备使用所述第二私人密钥对所述第一再生值进行所述处理的所得值 ；以及

根据所述第一所得值来导出所述秘密凭证生成密钥的值。

16. 根据权利要求 15 所述的认证设备，其中，所述第二公共 / 私人密钥对与所述第一公共 / 私人密钥对相同。

17. 根据权利要求 15 所述的认证设备，其中，所述第一再生值包括所述初始化种子的经加密的所述第一部分。

18. 根据权利要求 15 所述的认证设备，其中，所述第一再生值包括使用与所述第二私人密钥对应的所述第二公共密钥加密的所述秘密凭证生成密钥，以及再生所述秘密凭证生成密钥的值包括 ：所述认证设备向所述用户的安全设备提交经加密的所述秘密凭证生成密钥，以使所述用户的安全设备使用存储在所述用户的安全设备中的所述第二公共 / 私人密钥对的所述第二私人密钥对经加密的所述秘密凭证生成密钥进行解密。

19. 根据权利要求 14 所述的认证设备，其中，所述认证设备再生所述秘密凭证生成密钥的值包括 ：所述认证设备向所述用户的安全设备提交所述初始化种子的经加密的所述第一部分，以使所述用户的安全设备使用存储在所述用户的安全设备中的所述第一公共 / 私人密钥对的所述第一私人密钥对所述初始化种子的经加密的所述第一部分进行解密。

20. 根据权利要求 15 所述的认证设备，还适于在丢弃所述秘密凭证生成密钥之前确定所述第一再生值。

21. 根据权利要求 20 所述的认证设备，其中，确定所述第一再生值包括 ：

确定再生种子，

使用与所述第二私人密钥对应的所述第二公共密钥来加密所述再生种子，以及

将经加密的所述再生种子包括在所述第一再生值中 ；

以及

其中，再生所述秘密凭证生成密钥的值包括：

所述认证设备向所述用户的安全设备提交所述第一再生值，以使所述用户的安全设备使用所述第二私人密钥利用非对称解密算法对所述第一再生值进行解密，以及

根据经解密的所述第一再生值来导出所述秘密动态凭证生成密钥。

22. 根据权利要求 15 所述的认证设备，其中，与所述秘密凭证生成密钥关联的所述数据集还包括第二再生值，以及所述认证设备还适于使用所述第二再生值和由所述用户的安全设备对所述第一再生值进行所述处理的所述所得值来再生秘密凭证生成值。

23. 根据权利要求 22 所述的认证设备，其中，所述第二再生值包括使用对称加密算法利用再生加密密钥加密的再生种子。

24. 根据权利要求 23 所述的认证设备，其中，所述再生种子包括所述初始化种子。

25. 根据权利要求 23 所述的认证设备，其中，所述再生种子包括所述秘密凭证生成密钥。

26. 根据权利要求 23 所述的认证设备，其中，再生所述秘密凭证生成密钥包括：

所述认证设备向所述安全设备提交所述第一再生值，以使所述安全设备使用非对称签名算法和所述第二私人密钥来进行签名，

接收所得签名，

根据所述所得签名来导出所述再生加密密钥，

使用所导出的所述再生加密密钥来使用对称解密算法对所述第二再生值进行解密以获得所述再生种子，以及

根据经解密的所述再生种子来导出所述秘密凭证生成值。

27. 根据权利要求 23 所述的认证设备，还适于在丢弃所述秘密凭证生成密钥之前确定所述第一再生值和所述第二再生值。

28. 根据权利要求 27 所述的认证设备，其中，所述认证设备通过选择询问来确定所述第一再生值；以及通过确定再生种子和再生加密密钥并且利用所述再生加密密钥对所述再生种子进行加密以获得所述第二再生值来确定所述第二再生值；其中，所述认证设备通过以下步骤来确定所述再生加密密钥：向所述安全设备提交所述第一再生值以使所述安全设备使用非对称签名算法和所述第二私人密钥来签名，接收所得签名，根据所述所得签名来导出所述再生加密密钥，以及其中所述再生种子被确定为与所述秘密凭证生成密钥有关的值使得所述认证设备能够根据所述再生种子来导出所述秘密凭证生成密钥。

29. 根据权利要求 1 所述的认证设备，还适于捕获由所述用户的访问设备的人类输出接口输出或发射并且对所述初始化消息的表示进行编码的信号，并且所述认证设备还能够适于从所捕获的信号提取并解码所述初始化消息。

30. 根据权利要求 1 所述的认证设备，还包括：

相机；并且

所述认证设备还适于使用所述相机来拍摄对所述初始化消息进行编码并且在所述访问设备的显示器上显示的图像的照片；以及

所述认证设备还适于从使用所述相机拍摄的所述照片中提取所述图像并且对所述图像进行解码以获得在所述图像中被编码的所述消息。

31. 根据权利要求 1 所述的认证设备，还包括用于提供时间值的时钟，并且所述认证设

备还适于使用所述时间值来确定所述动态变量的值。

32. 根据权利要求 1 所述的认证设备，其中，所述动态值根据由所述认证设备存储和保持并且在某些事件下由所述认证设备更新的值而导出。

33. 根据权利要求 1 所述的认证设备，还适于根据在所述认证设备外部生成的并且由所述认证设备接收的询问来导出所述动态变量。

34. 根据权利要求 1 所述的认证设备，还适于根据表示所述用户想要提交至应用的业务并且由所述认证设备接收的业务数据来导出所述动态变量。

35. 根据权利要求 1 所述的认证设备，还包括用户输出接口，并且所述认证设备还适于使用所述用户输出接口将所生成的动态凭证送达至所述用户。

36. 一种使用用于生成动态凭证的秘密凭证生成密钥来初始化特定用户的根据权利要求 1 所述的特定认证设备的方法，所述方法包括以下步骤：

在所述认证设备处接收来自服务器的初始化消息，所述初始化消息包括初始化种子的经加密的至少第一部分和所述初始化种子的任何其他部分，其中，使用第一公共 / 私人密钥对的第一公共密钥利用第一非对称加密算法来加密所述初始化种子的所述第一部分；

在所述认证设备处从所接收的初始化消息提取所述初始化种子的经加密的第一部分和所述初始化种子的任何其他部分；

在所述认证设备处与所述用户的由所述用户提供给所述认证设备的安全设备进行通信；

由所述认证设备向所述安全设备提交所述初始化种子的经加密的第一部分；

在所述安全设备处使用所述第一公共 / 私人密钥对的第一私人密钥对所述初始化种子的经加密的第一部分进行解密，并且所述初始化种子的经解密的第一部分返回至所述认证设备，所述第一私人密钥存储在所述安全设备上；

在所述认证设备处接收所述初始化种子的经解密的第一部分；以及

在所述认证设备处根据所述初始化种子导出所述秘密凭证生成密钥。

37. 根据权利要求 36 所述的方法，还包括：

在所述服务器处确定所述秘密凭证生成密钥是所述初始化种子的函数；

在所述服务器处将所述秘密凭证生成密钥与所述特定用户进行关联；

在所述服务器处使用所述第一公共 / 私人密钥对的所述第一公共密钥利用所述第一非对称加密算法对所述初始化种子的至少第一部分进行加密；

在所述服务器处收集初始化消息，所述初始化消息包括所述初始化种子的所述加密的第一部分和所述初始化种子的任何其他部分；以及

将所述初始化消息发送至所述用户的所述认证设备。

38. 根据权利要求 36 所述的方法，包括以下另外的步骤：将所导出的所述秘密凭证生成密钥至少暂时存储在所述认证设备的存储器部件中。

39. 根据权利要求 37 所述的方法，包括以下另外的步骤：在所述服务器处使用与所述认证设备已知的解密密钥匹配的加密密钥对所述初始化种子的至少第二部分进行加密，以及在所述认证设备处使用所述解密密钥对所述初始化种子的所述第二部分进行解密。

40. 根据权利要求 39 所述的方法，其中，所述解密密钥的值对于所述特定认证设备是唯一的。

41. 根据权利要求 39 所述的方法，其中，所述特定认证设备与至少一个其他认证设备共享所述解密密钥的值。

42. 根据权利要求 37 所述的方法，其中：

将所述初始化消息发送至所述用户的所述认证设备的步骤包括：所述服务器将所述初始化消息发送至所述用户的访问设备；以及所述访问设备通过所述访问设备的人类输出接口发出编码有所述初始化消息的表示的信号，以及

在所述认证设备处接收所述初始化消息的步骤包括：所述认证设备捕获所述信号并且将所述信号解码以获得所述初始化消息的表示。

43. 根据权利要求 42 所述的方法，其中，所述认证设备包括相机，所述访问设备包括显示器，所述初始化消息的表示包括二维图像，并且所述方法包括以下另外的步骤：所述访问设备在所述访问设备的显示器上显示所述二维图像，以及所述认证设备拍摄所述图像的照片，从所述照片提取所述二维图像，并且将所述图像解码以获得所述初始化消息。

44. 一种用于由特定用户的认证设备和安全设备来生成第一动态凭证的方法，所述方法包括以下步骤：

根据权利要求 36 所述的方法来初始化所述特定用户的所述认证设备；

所述认证设备获得动态变量的值；以及

所述认证设备将所述第一动态凭证确定为使用对称密码动态凭证生成算法将所述动态变量的值与所述秘密凭证生成密钥密码地组合的结果。

45. 根据权利要求 44 所述的方法，所述方法包括以下另外的步骤：

所述认证设备生成能够提供给所述用户的所生成的所述动态凭证的表示，以及

所述认证设备借助于所述认证设备的人类输出接口将所述表示提供给所述用户。

46. 根据权利要求 44 所述的方法，所述方法包括以下另外的步骤：

所述认证设备对照一组标来准验证所述秘密凭证生成密钥的使用期限是否已经过期，并且如果所述使用期限已经过期，则所述认证设备丢弃所述秘密凭证生成密钥。

47. 根据权利要求 46 所述的方法，其中，在所述生成所述第一动态凭证之后丢弃所述秘密凭证生成密钥。

48. 根据权利要求 46 所述的方法，其中，所述丢弃包括所述认证设备将所述秘密凭证生成密钥从所述认证设备的存储器部件中擦除。

49. 根据权利要求 46 所述的方法，其中，所述丢弃包括所述认证设备使存储在所述认证设备的存储器部件中的所述秘密凭证生成密钥无效。

50. 根据权利要求 46 所述的方法，包括以下另外的步骤：所述认证设备在使用所述秘密凭证生成密钥来生成第二动态凭证之前再生所述秘密凭证生成密钥。

51. 根据权利要求 50 所述的方法，其中，再生所述秘密凭证生成密钥包括：

所述认证设备要求提供所述用户的安全设备并且与所述安全设备通信，

所述认证设备将第一再生值提交至所述安全设备，

所述安全设备接收所述第一再生值，并且将所接收的所述第一再生值用作由与所述用户关联的第二公共 / 私人密钥对的存储在所述安全设备上的第二私人密钥参数化的第二非对称密码操作的输入，

所述安全设备将由所述安全设备进行的所述第二非对称密码操作的结果返回至所述

认证设备，并且所述认证设备使用所述结果。

52. 根据权利要求 51 所述的方法，其中，所述认证设备使用所述结果包括：所述认证设备验证所述结果。

53. 根据权利要求 52 所述的方法，其中：

由所述安全设备进行的所述第二非对称密码操作包括：使用由所述第二私人密钥参数化的非对称密码签名算法来对所接收的第一再生值生成签名，

所述结果包括所述签名，

以及所述认证设备对所述结果的所述验证包括：验证包含在所述结果中的所述签名。

54. 根据权利要求 53 所述的方法，其中，所述第一再生值包括

由所述认证设备生成的随机询问。

55. 根据权利要求 52 所述的方法，其中，所述认证设备丢弃所述秘密凭证生成密钥包括：所述认证设备使存储在所述认证设备的存储器部件中的所述秘密凭证生成密钥无效，以及所述认证设备使用所述安全设备进行的所述非对称密码操作的所述结果包括：在对所述结果的所述验证成功的情况下重新激活存储在所述认证设备的存储器部件中的所述秘密凭证生成密钥。

56. 根据权利要求 51 所述的方法，其中，所述认证设备在丢弃所述秘密凭证生成密钥之前确定中间值，以及所述第一再生值包括使用由与所述第二公共 / 私人密钥对的所述第二私人密钥对应的第二公共密钥参数化的第二非对称加密算法来加密的所述中间值。

57. 根据权利要求 56 所述的方法，其中，由所述安全设备进行的所述第二非对称密码操作包括：使用由所述第二私人密钥参数化的第二非对称解密算法对所接收的第一再生值进行解密，所述结果包括经解密的中间值，以及所述认证设备使用所述结果包括：所述认证设备使用经解密的中间值以获得所述秘密凭证生成密钥的值。

58. 根据权利要求 57 所述的方法，其中，所述中间值包括所述秘密凭证生成密钥。

59. 根据权利要求 57 所述的方法，其中，所述中间值包括初始化密钥。

60. 根据权利要求 51 所述的方法，其中，所述认证设备在丢弃所述秘密凭证生成密钥之前确定第二再生值，以及所述认证设备使用由所述安全设备进行的所述第二非对称密码操作的所述结果包括：所述认证设备将所述第二再生值与所述结果数学地或密码地组合以确定所述秘密凭证生成密钥的值。

61. 根据权利要求 60 所述的方法，其中，所述确定所述第二再生值包括：确定中间再生种子并且使用中间加密密钥将所述中间再生种子加密，所述第二再生值包括使用所述中间加密密钥加密的所述中间再生种子，以及所述认证设备使用由所述安全设备进行的所述第二非对称密码操作的所述结果包括：根据所述结果导出与所述中间加密密钥匹配的中间解密密钥，对经加密的所述中间再生种子进行解密，并且根据经解密的中间再生种子来导出所述秘密凭证生成密钥的值。

62. 根据权利要求 61 所述的方法，其中，所述中间再生种子包括所述秘密凭证生成密钥。

63. 根据权利要求 61 所述的方法，其中，所述中间再生种子包括初始化种子。

64. 根据权利要求 61 所述的方法，其中，所述认证设备确定所述中间解密密钥的值，并且通过使用所述第二公共密钥将所述中间解密密钥加密来确定所述第一再生值，以及所述

认证设备通过将所述第一再生值提交至所述安全设备以由所述第二私人密钥进行解密来重新获得所述中间解密密钥。

65. 根据权利要求 61 所述的方法，其中，所述认证设备确定所述第一再生值，并且在首次时通过将所述第一再生值提交至所述安全设备以由所述第二私人密钥进行签名并且根据所得签名来导出所述中间加密密钥来确定所述中间加密密钥的值，所述认证设备通过使用如上所述的所述中间加密密钥对所述中间再生种子进行加密而使用所述中间加密密钥来确定所述第二再生值，存储所述第一再生值和所述第二再生值，以及如上所述通过以下步骤来再生所述秘密凭证生成密钥：通过将所述第一再生值重新提交至所述安全设备以由所述第二私人密钥进行签名并且根据所得签名重新导出所述中间加密密钥来再生所述中间加密密钥，以及使用再生的中间加密密钥对所述第二再生值进行解密以获得所述中间再生种子的值，以及根据所获得的中间再生种子的值来导出所述密码凭证生成密钥。

66. 一种用于使用用户的认证设备来保障所述用户与远程服务器之间的交互的方法，所述方法包括以下步骤：

在应用服务器处接收所述用户的请求；

应所述用户的所述请求在所述认证设备处生成根据权利要求 44 所述的方法的动态凭证；

使验证服务器能够获得与所述用户关联的秘密动态凭证生成密钥；

在所述验证服务器处接收所生成的动态凭证；

在所述验证服务器处使用所述秘密动态凭证生成密钥来验证所接收的动态凭证的有效性；以及

如果所接收的动态凭证被验证为有效，则在远程应用服务器处批准所述请求。

远程认证和业务签名

相关申请的交叉引用

本申请要求于2012年12月28日提交的名称为“Remote Authentication and Transaction Signatures”的序号为61/746,892的美国临时申请的优先权,其全部内容通过引用被合并在本文中。

背景技术

随着计算机系统和应用的远程访问的繁荣发展,通过公共网络如因特网来远程访问的业务(transaction)数目和种类已经急剧增加。该繁荣特别地凸显了对安全性的需要。

a. 如何确保正在远程地访问应用的人正是他们所声称的人以及如何确保正在远程地进行的业务由合法个体发起。该主题被称为认证。

b. 如何确保业务数据在被应用服务器接收到之前未被更改。这被称为数据完整性。

c. 如何保证个体一旦已经参与业务就不能够否认。这被称为不可否认。

应用提供者过去一直依赖于静态口令来为远程应用提供安全性。在最近几年中已经变得明显的是,静态口令还不够并且需要更高级的安全技术。

PKI 智能卡

解决与通过公共网络对计算机系统和应用进行远程访问相关联的安全问题的一种方式由公共密钥基础设施(Public Key Infrastructure)来提供。在公共密钥基础设施中,将公共-私人密钥对与各用户相关联。密钥对与将该公共-私人密钥对绑定到特定用户的证书(由受信任的证书颁发机构签发)相关联。借助非对称密码,该公共-私人密钥对可以用来:

a. 认证用户,

b. 对业务、文档、电子邮件签名(以便防止否认),以及

c. 建立加密的通信信道。

为了保证足够的安全等级,强制各用户的私人密钥保持秘密并且仅能由与该密钥相关联的合法用户访问(以例如创建签名)。通常依赖于智能卡来存储公共-私人密钥对和证书,并且进行涉及私人密钥的密码计算。通过卡来使用私人密钥于是通常是受PIN保护的。

具有PKI功能的智能卡正在并且已经由:

a. 公司签发给它们的雇员或者客户,以保障对它们的计算机网络的登录或者对它们的应用的远程访问;

b. 银行签发给它们的客户,以保障例如网上银行应用;以及

c. 政府签发给它们的公民作为电子ID卡,以创建依法绑定的电子签名。

除了优点之外,也存在与PKI以及携带PKI密钥和证书的智能卡相关联的一些缺点:

a. 在与竞争的安全技术比较时,构建公共密钥基础设施一般很复杂并且因此昂贵。

b.PKI固有地限于在客户端与服务器之间有数字连接的环境和应用。换言之,它并不适于电话银行或者在一方面是PKI证书和私人密钥的容器与另一方面是应用服务器之间无法提供数字连接的其他传送信道。

c.PKI 智能卡没有电源或者用户接口。PKI 智能卡因此依赖于接口设备的存在，该接口设备向该卡提供电力，能够以数字方式与该卡交换数据，并且能够与用户接口（例如捕获卡的PIN并且提供应当被签名的数据）。在大多数情况下，使用具有所连接的透明的智能卡读取器的PC。这减少了用户的灵活性（许多PC未配备智能卡读取器）。它也带来了安全问题：在本身不安全的PC上完成所有用户交互（比如批准签名或者捕获卡的PIN）。

强认证令牌

一种关于认证能力和业务签名能力的可选技术由称为“强认证令牌设备”的设备提供。强认证令牌的典型示例是由Vasco Data Security公司提供的任一数字通(Digipass)令牌，参见网站Vasco.com。

强认证令牌是小型自主电池供电的设备，该设备具有其自己的显示器和键盘。在一些情况下，键盘简化为单个按钮或者甚至完全被省略。强认证令牌的主要目的在于生成所谓的“一次性口令(One-Time Password)”(OTP)。在一些情况下，强认证令牌也能够对在令牌的键盘上已经输入的数据生成电子签名或者消息认证代码(MAC,Message Authentication Code)。如果令牌具有键盘，则对令牌的使用常常由PIN保护。为了能够生成OTP或者MAC，强认证令牌能够基于用秘密值或者密钥参数化的对称密码算法来完成密码计算。用秘密值或者密钥参数化的这种对称密码算法的典型例子是对称加密/解密算法（比如3DES或者AES）和/或带密钥(keyed)的单向散列函数（比如符合OATH的令牌中的MD5或者SHA-1）。在本文的其余部分中，这样的算法的输出有时会称为‘对称密码’。术语‘对称密码’因此应当不仅理解为对称加密算法的输出，而且还理解为对称解密算法或者带密钥散列函数的输出。用假设为对于每个个别令牌而言不同的一个或更多个秘密密钥将强认证令牌个性化。为了生成一次性口令或者签名，令牌通常执行以下步骤（参照图1）：

a. 步骤10：令牌取得一个或更多个输入值（这可以包括由服务器生成的并且由用户在键盘上键入的询问、和/或令牌的内部实时时钟的值、和/或由令牌管理的内部计数器的值、和/或由用户在令牌的键盘上键入的业务数据）。

b. 步骤11：令牌将一个或更多个输入值表达成指定格式。

c. 步骤12：然后令牌将一个或更多个输入值与安全地存储于令牌中的个性化秘密密钥15密码地组合。在典型的强认证令牌中，令牌将一个或更多个输入值提交至由安全地存储于令牌中的个性化秘密密钥15参数化的对称加密/解密算法和/或单向散列函数。结果是密码或者散列值。

d. 步骤13：令牌使作为该加密/解密或者单向散列的结果的密码或者散列值（或更一般地，一些其他密码组合）变换成实际的OTP或者MAC，即密码或者散列通常被截取、以人类可读格式转换（例如通过十进制换算）以及在显示器上可视化。用户可以将该值提交至应用服务器。

在本文的其余部分中，如上所述由强认证令牌生成的一次性口令或电子签名可以被称为动态认证凭证或仅称为动态凭证。在本文的其余部分中，在步骤10中提到的输入值可以被称为动态变量。动态变量——其值来自在强认证令牌的外部的源——可以被称为外部动态变量。外部动态变量的示例可以包括例如可由用户在令牌的键盘上键入而提供给令牌的询问或业务数据。动态变量——其值来自在强认证令牌的内部的源——可以被称为内部动态变量。内部动态变量的示例可包括由令牌的实时时钟或存储在令牌的存储器中并且由令

牌的处理器更新的计数器所提供的时间值。由“OATH-开放认证的倡议者”所公布的算法是用于生成动态凭证的标准化算法的示例。

在大多数情况下，强认证令牌是物理设备，然而在一些情况下，这些强认证令牌生成OTP签名或者MAC签名的功能由在PC、工作站、移动电话、个人管理器、PDA等上运行的软件模仿。后者称为“软令牌”。

当产生了OTP或者MAC时，就在认证用户或者消息时将其传达至实体，在所述实体处可以验证该值，参见图2。该实体通常是应用服务器。应用服务器为各令牌存储数据，该数据包括已经用哪一个或者哪些个秘密密钥将令牌个性化以及与令牌相关联的用户的身份。为了证实一次性口令或者签名，服务器检索秘密密钥(115)(它是在令牌中的个性化的密钥的副本)，取得与令牌所用的输入相同的输入，并且进行本质上与令牌相同的算法112。然后，服务器将其获得的结果与服务器接收的值进行比较120。(在实践中，如果强认证算法是基于时间的或者基于计数器的，则由于同步问题使对OTP或者MAC的证实往往在一定程度上更复杂。)由于强认证令牌生成的一次性口令或者签名是令牌的个别秘密密钥和输入令牌算法的总是不同的(多个)输入值的函数，所以证实一次性口令或者签名的正确性向应用服务器给予了关于提交一次性口令或者签名的个人拥有正确令牌并且知道其PIN(如果令牌受PIN保护)的很高的置信度，这又给予了关于该个人确实是与该令牌设备相关联的合法用户的高置信度。

由于OTP验证服务器和OTP令牌本质上用相同密钥来执行相同算法，所以OTP生成算法可以是单向或者不可逆函数。这意味着实际OTP可以比用来导出实际OTP的密码或者散列值更短。这允许OTP长度或者MAC长度充分短，从而用户将OTP值或者MAC值从令牌显示器手动复制到PC上不会太不便。因而得到的强认证令牌并不要求在令牌与验证服务器之间的数字连接。

强认证令牌在与PKI卡比较时的主要优点在于：

a)它们为全自治的(令牌具有其自己的电源和其自己的用户接口)；

b)它们独立于传送信道或者通信介质(令牌并不要求与任何其他设备的任何数字或者电子连接；所有数据输入和输出由用户经由令牌的显示器和键盘来完成)；以及

c)它们提供很高安全等级(所有用户交互(比如捕获PIN或者提供要签名的业务数据)都经由令牌自己的安全用户接口来完成)。

在已经签发智能卡的一些情况下，想要回避与智能卡相关联的缺点和限制，并且实现强认证令牌提供的相同优点，即全自治、独立于传送信道和安全的用户接口。

一种可选方式是将智能卡与未连接的由电池供电的智能卡读取器组合，该读取器具有其自己的显示器和键盘。想法是智能卡与未连接的智能卡读取器的组合模仿强认证令牌。强认证令牌通常提供的功能于是在智能卡与未连接的读取器上划分。未连接的读取器负责所有用户接口，而其他令牌功能的全部或者部分交给该卡。

通常，所有个性化的秘密和对安全性敏感的数据由卡存储和管理(例如PIN由卡来存储和验证，秘密密钥存储于卡上，而涉及到这些密钥的所有密码操作由卡完成，用作令牌算法的输入的计数器由卡存储和管理)。令牌功能的敏感性较低的部分(例如截取和转换生成的散列或者密码)常常发生在读取器中。下文讨论该组合的示例。

该原理常常由银行使用，这些银行将其签发的银行卡(用于在自动取款机或者销

售点终端使用）与未连接的读取器进行组合以保护其远程银行应用（比如网上银行或者电话银行）。这一点的适合例子是万事达卡（Mastercard）芯片认证方案（CAP，Chip Authentication Programme），该CAP指定EMV智能卡可以如何与未连接的智能卡读取器组合使用以生成一次性口令和电子业务数字签名。

该技术依赖于智能卡，该智能卡能够完成对称密码计算并且已经用要用于对称密码操作的秘密密钥来个性化。然而，具有PKI功能的智能卡被设计成存储非对称密钥并且完成非对称密码操作。许多具有PKI功能的智能卡并不支持对称密码操作或者（如果它们支持则）从未用个别对称秘密密钥来个性化。

传统PKI签名

用PKI智能卡创建电子签名的常用方式是输入数据（输入数据通常包括想进行签名的实际业务数据的散列）由卡的私人密钥进行加密。

证实这样的签名的常用方式是证实实体用公共密钥来对接收的签名进行解密。如果签名的解密获得与假设已经由私人密钥加密的输入数据相同的值，则成功地证实该签名。注意由于该非对称特性，该证实实体从不需要访问该卡的私人密钥。这允许私人密钥对签名方以外的任一方、甚至对任何验证方秘密，由此提供真正的不可否认性。

这只有在该证实实体可获得整个签名本身的情况下才可以成功完成。对不完整签名的解密将仅获得与假设已经签名的输入数据无法比较的无意义数据。

在实践中，当使用未连接的小型手持智能卡读取器时，不能满足该条件：假如典型PKI签名大小为100字节数量级，那么这些读取器的显示器太小到而无法显示整个签名，并且在任何情况下期望用户将100字节的值从读取器的显示器手动传送到PC而不犯一个错误完全不切实际。100字节的典型PKI签名应当与传统强认证令牌的典型6到8数位或者3到4字节的OTP或者MAC比较。这的确是非对称密码和私人密钥尚未用来例如通过强认证令牌生成OTP和MAC的原因。

发明人确定需要以下方法和装置：

a）允许使用存储PKI私人密钥的设备（比如具有PKI功能的智能卡或者USB棒）来认证用户并且对业务进行签名，

b）如果没有必要，任何用户应用无需与包含私人密钥的设备具有某种直接或者间接数字连接、特别是将允许用户应用将数据提交到卡以便由卡的私人密钥来签名并且将允许从卡检索作为结果的整个签名的数字连接，

c）无需包含私人密钥的具有PKI功能的设备（例如PKI智能卡或者USB棒）：

1）支持对称密码操作；或者

2）用可以由适当读取器读取的一些秘密或者机密数据元素来个性化。

发明内容

本申请提供了对满足上述要求的方法和装置的描述。具体地，本申请描述了多种实施例，这些实施例使用公共-私人密钥对中的私人密钥（意在用于非对称密码例如RSA算法的密钥）来（经由生成OTP）认证用户或者（经由生成MAC）对数据进行签名。

这里描述的实施例与传统上使用私人密钥来认证用户和对数据进行签名（如上所述）的不同之处在于：

a) 使用相同密码密钥来生成和验证 OTP 和 MAC ;并且

b)OTP 值和 MAC 值的位长度可以安全地显著少于私人密钥生成的密码的位长度。

所有实施例的共同之处在于 :

a) 它们都借助于使用验证服务器也知道或者可获得的秘密的密码算法,使用一个或更多个可变输入来计算动态值。

b) 这些可变输入可以是例如以下输入中的任何输入 :

1) 时间值,或者

2) 计数器值,或者

3) 询问值,或者

4) 业务数据,或者

5) 上述输入的任何组合。

c) 然后动态值被变换成 OTP 或者 MAC。

d) 在开发 OTP 或者 MAC 的过程中的某一点,执行使用私人密钥的非对称密码操作 (即加密 / 解密或者签名)。

e) 将动态值变换成 OPT 或者 MAC,使得 OTP 或者 MAC 的长度或者大小小于使用私人密钥通过非对称密码操作生成的密码的大小。

利用私人密钥的非对称密码操作在生成 OTP 或者 MAC 的整个处理中的确切作用可以因实施例不同而不同。

在一些实施例中,每当不得不生成 OTP 或者 MAC 时执行使用私人密钥的非对称密码操作。在其他实施例中,可以结合使用私人密钥的单个非对称密码操作来生成多于一个 OTP 或者 MAC。在后一种情况下,能够确定当需要生成新 OTP 或者 MAC 时是否需要使用私人密钥的新非对称密码操作的标准可以包括 :

a) 从上次非对称密码操作开始已经过去的时间。

b) 已经生成的 OTP 和 / 或 MAC 的数目。

c) 在包含私人密钥的设备与捕获输入并且使 OTP 可用的设备之间的通信会话是否未中断 (例如 PKI 智能卡是否尚未从智能卡读取器移除)。

d)OTP 或者 MAC 的类型。例如,MAC 的生成可能总是需要新的非对称密码操作,但是 OTP 的生成则不需要新的非对称密码操作。

在典型的实施例中,使用仅一个私人密钥,并且用该私人密钥进行仅一个非对称密码操作。然而,一些实施例可以用单个私人密钥或者用多个私人密钥执行多个密码操作。例如 :

a) 如果 OTP 是私人密钥对可变输入的加密的结果的函数,则变型可以是 :OTP 是多于一个的密码的函数,或者可变输入由多于一个的私人密钥加密以生成 OTP。

b) 如果 OTP 的生成仅在通过检查由卡的私人密钥对询问进行的加密的结果来验证特定智能卡的存在之后发生,则变体可以是 :将多于一个的询问提交到卡以由卡的私人密钥来加密。

c) 在许多情况下,PKI 卡包含所谓实用私人密钥和签名私人密钥。在该情况下,如果生成 OTP 则可以使用实用密钥,而如果生成 MAC 则可以使用签名密钥。

在优选的实施例中,可以生成用于认证用户的 OTP 和用于对数字进行签名的 MAC 二者。

然而，可选实施例可以限于仅能够生成 OTP 或者仅能够生成 MAC 签名。

在典型的实施例中，使用私人密钥的非对称密码算法将是 RSA 算法。然而，其他实施例可以使用其他非对称算法，只要它们能够通过使用私人密钥来实现对功能的加密或者解密或者签名即可。这样的算法的例子包括：RSA、渐缩算法（比如 Merkle-Hellman 或者 Chor-Rivest、Pohlig-Hellman、Diffie-Hellman、ElGamal、Schnorr、Rabin）、椭圆曲线密码系统、有限自动机公共密钥密码系统、数字签名算法（DAS、DSS）。

在典型的实施例中，包含私人密钥的部件以及生成 OTP 和 MAC 值的部件是两个不同部件，各部件是两个不同设备的一部分。然而，可以容易地设想这两个部件是同一设备的部分或者甚至是同一部件。

在典型的实施例中，私人密钥存储于智能卡上。在优选的实施例中，涉及到私人密钥的密码计算由该智能卡进行。在典型的实施例中，OTP 和 / 或 MAC 值由如下设备生成，该设备配备有或者连接到可以与包含私人密钥的智能卡通信的部件或者设备。

在优选的实施例中，卡读取设备是未连接的智能卡读取器，该读取器具有其自己的电源，并且运行适当软件以与已经插入该智能卡读取器中的 PKI 智能卡通信，以生成 OTP 或者 MAC。

在另一实施例中，卡读取设备是一些计算设备如 PC、PDA、蜂窝电话等的组合，这些计算设备配备有智能卡读取器，并且运行适当软件以生成 OTP 或者 MAC。

在典型的实施例中，在智能卡与智能卡读取器设备之间的通信的物理方面、电气方面和协议方面与 ISO 7816 标准中描述的方面相同或者相似。其他实施例可以使用其他通信接口，比如 ISO 14443 中描述的非接触式智能卡接口。

可选的形式因素可用于私人密钥包含设备，并且可选的形式因素可用于 OTP 或者 MAC 生成设备，而且可选的装置可用于在一方面是私人密钥包含部件或者设备与另一方面是 OTP 和 MAC 生成部件或者设备之间的通信。这些可选的因素和装置处在如本文所描述的本发明的范围内。

在一个实施例中，OTP 值或者 MAC 值可视化于卡读取设备的显示器上。OTP 可以例如由一连串符号构成。在典型的实施例中，这些符号是十进制数位。在其他实施例中，这些符号可以例如包括：

a) 十六进制数位，或者

b) 基本 64 数位，或者

c) 来自书写系统如字母表的字符，或者

d) 象形文字。

在一个实施例中，生成的 OTP 或者 MAC 借助可听信号送达到用户。例如，OTP 可以是数位或者字符或者字词的串，各数位或者字符或者字词具有特性关联音调或者由文字到语音的转换器读取。

在一个实施例中，生成的 OTP 或者 MAC 通过某种电子有线或者无线通信机制直接送达到应用程序。该机制可以包括 USB 连接或者红外线连接或者近场通信连接或者 RF 连接或者蓝牙连接。

可以提供用于 OTP 或者 MAC 的其他输出机制。在一些实施例中，基于私人密钥的功能受 PIN 保护。

以下说明更详细地描述了基本实施例。在一些实施例中，在生成 OTP 或者 MAC 时直接或者间接使用卡的基于私人密钥的功能。

a) 涉及到卡的私人密钥的非对称密码操作是将可变输入变换成 OTP 或者 MAC（以对称方式使用非对称算法）的这一变换的整个阶段或者部分阶段，或者

b) 卡的基于私人密钥的功能更间接用来提供种子值，该种子值用来导出 OTP 或者 MAC 生成算法所用的秘密对称密钥（使用非对称密码作为种子以导出秘密密钥）。

在一些实施例中，OTP 和 / 或 MAC 的值是卡的私人密钥的实际值的函数。在另外一些实施例中，卡的基于私人密钥的函数用来在读取器中对 OTP 或者 MAC 生成算法进行解锁：

a) 卡链接到已经个性化的读取器，并且基于存储的询问 - 响应对来进行识别，或者

b) 卡通过传统的基于 PKI 证书的验证由读取器认证。

在前一段落中描述的实施例中，生成的 OTP 和 / 或 MAC 的值不是卡的私人密钥的实际值的函数。

因此，在一个方面中，本发明提供了一种用于生成包括一次性口令 (OTP) 或者消息认证代码签名 (MAC) 的安全值的方法，该方法包括：

获得使用一个或更多个可变输入和采用至少一个秘密的密码算法来创建的中间动态值；

将所述动态值变换成所述安全值，

其中，执行利用私人密钥的非对称密码操作以产生密码，以便变换所述动态值，并且

所述变换包括产生大小比由所述非对称密码操作生成的密码的大小更小的所述安全值。

在另一方面中，本发明提供一种使用上文刚描述的方法来生成包括一次性口令 (OTP) 或者消息认证代码签名 (MAC) 的安全值的设备。

在另一方面中，本发明提供一种证实用户提供的安全值以便认证用户或者与用户关联的数据的方法，所述安全值包括一次性口令或者包括包含消息认证代码的签名；所述方法包括：

使用与可信用户的 PKI 私人密钥有关的服务器密钥，使用应用于一个或更多个参考输入的参考密码算法来创建参考密码，该参考密码算法和一个或更多个参考输入被选择为与可信用户在创建安全值时所用的对应要素相同；

之后，

通过将所述参考密码变换成参考安全值来单独对所述参考密码进行操作包括产生大小比参考密码的大小更小的所述参考安全值，并且实现所述参考安全值与所述安全值的比较，或者

对所述参考密码和所述安全值两者进行操作，以产生修改的参考密码和修改的安全值，对所述参考密码进行的所述操作与为了创建所述安全值而执行的操作部分地相同，并且实现修改的所述参考密码与修改的所述安全值的比较，并且

根据所述比较的结果确定所述安全值的有效性。

在又一方面中，本发明包括一种支持指令序列的计算机可读介质，这些指令在执行时实现一种生成包括一次性口令 (OTP) 或者消息认证代码签名 (MAC) 的安全值的方法，所述方法包括：

获得使用一个或更多个可变输入和采用至少一个秘密的密码算法来创建的中间动态值；

将所述动态值变换成所述安全值，

其中执行利用私人密钥产生密码的非对称密码操作，以便变换所述动态值，并且

所述变换包括产生大小比所述非对称密码操作生成的密码的大小更小的所述安全值。

最后在又一方面中，本发明包括包含指令序列的信息承载信号，这些指令在处理器中执行时实现一种生成包括一次性口令 (OTP) 或者消息认证代码签名 (MAC) 的安全值的方法，所述方法包括：

获得使用一个或者多个可变输入和采用至少一个秘密的密码算法来创建的中间动态值；

将所述动态值变换成所述安全值，

其中执行利用私人密钥产生密码的非对称密码操作，以便变换所述动态值，并且所述变换包括产生大小比所述非对称密码操作生成的密码的大小更小的所述安全值。

附图说明

现在在说明书的以下部分中结合附图进一步描述本发明的若干实施例：

图 1 是现有技术的强认证令牌在生成 MAC 的 OTP 时的操作的流程图；

图 2 是现有技术的服务器在认证由强认证令牌生成的 OTP 或者 MAC 时的操作的流程图及其与 OTP 或者 MAC 生成的关系；

图 3 是依赖于使用 PKI 私人密钥来创建从中生成 OTP 或者 MAC 的密码的非对称密码操作的本发明一个实施例的流程图；

图 4 是示出了在客户端的 OTP/MAC 生成（例如如图 3 中那样）和在服务器的有关认证的本发明一个实施例的流程图；

图 5 是使用非对称密码作为种子以导出在创建代表 OTP 或者 MAC 的密码时所用密钥的本发明另一个实施例的流程图；

图 6 和图 7 是其中智能卡用来向读取器认证用户的本发明又一实施例的流程图，该读取器又产生从中导出 OTP 或者 MAC 的密码，在这一实施例中，在初始操作中将用户的智能卡绑定到读取器（图 6），而在图 7 中表示了随后的操作；

图 8 和图 9 是其中包括 PKI 证书的智能卡用来向读取器认证用户的本发明又一实施例的流程图，该读取器又产生从中导出 OTP 或者 MAC 的密码，在这一实施例中可以认证随机用户；

图 10 和图 11 图示了为了捕获允许本发明各种实施例操作的信息而在初始会话中进行的动作；

图 12 图示了本发明实施例进行操作的背景；

图 13 是第一证实过程的图示；并且

图 14 是另一证实过程的图示；

图 15 是 PKI 设备的一个实施例的示图；

图 16 是读取器的实施例的示图；

图 17 表示根据本发明的实施例的在用于生成动态认证凭证的协议中采用的数据；

图 18 图示了根据本发明的实施例的用于验证动态凭证的服务器侧部件的架构；

图 19 图示了根据本发明的实施例的用于保障应用的方法；

图 20A 和图 20B 图示了根据本发明的实施例的用于登记或启用用户的私人密钥的方法；

图 21 图示了根据本发明的实施例的用于生成动态凭证的方法；

图 22 图示了根据本发明的实施例的用于验证动态凭证的方法；

图 23 是根据本发明的一些方面的接纳安全设备的认证设备的图示；

图 24 是根据本发明的一些方面的用于使用认证设备和安全设备来生成用于认证用户和 / 或业务的 OTP 和 / 或 MAC 的步骤的流程图。

具体实施方式

本发明的实施例的重要部件在图 12 中被图示为包括智能卡读取器 20（或者简称为读取器）和认证服务器 30（或者简称为服务器）。

读取器 20 至少包括接口 28 以接受智能卡和电源 27。一些读取器还包括在图 12 中由键盘 25 代表的一个或更多个用户可操作按钮或者键。如本文所使用的那样，用户将智能卡插入智能卡接口 28 中。由于读取器 20 进行的某一操作，信息由读取器生成。该信息可以是一次性口令 (OTP)。如果业务数据输入到读取器，则生成的信息可以包括签名，比如 MAC。输出信息可以提供于显示器如显示器 26 上。可选地，读取器可以用数字方式连接到网络。在该情况下，信息可以提供给也连接到网络的另一实体，而显示器 26 可能是不必要的。通常，读取器 20 生成的信息用来认证个人或者消息。可以通过使用智能卡（证明拥有该卡）和一些其他信息（比如 PIN 或者其他用户数据）来认证个人。读取器接受智能卡和其他信息并且创建 OTP。OTP 被送达至服务器 30。可选地，消息由读取器 20 签名从而产生 MAC，而该 MAC 被送达至服务器 30。

服务器 30 通常被实施为具有处理能力和数据库 35 的计算机。读取器生成的信息经由数据路径 40 送达至服务器 30。数据路径 40 可以采用各种形式。通常，用户将信息从显示器 26 手动传送至连接至服务器 30 的客户端设备。可选地，数据路径 40 可以包括允许信息从读取器 20 送达至服务器 30 的数字路径。作为另一选择，数据路径可以运送音频信息，比如运送用户的语音的电话电路，该用户念出在显示器 26 上向用户提供的信息；其中该信息可以是 OTP 或者 MAC。数据路径 40 可以运送代表在读取器 20 生成的信息的光学信号。一般而言，数据路径 40 是可以用来将信息从读取器 20 送达至服务器 30 的任何路径。服务器 30 接受 OTP 或者 MAC，并且借助数据库 35 中的数据在证实用户的身份 (OTP) 或者消息的可信性 (MAC) 时确定是接受还是拒绝该信息。下文更具体地描述了由服务器 30 使用的数据和具体过程。服务器 30 的一个输出端选择接受或者拒绝状态 36，从而反映在证实用户的身份声明的可信性时对 OTP 的接受，或者反映在认证相关联的消息时对 MAC 的证实。

以对称的方式使用非对称算法

在该实施例（参见图 3）中，智能卡 100 与智能卡读取器 105 配合。智能卡 100 存储在非对称密码操作中使用的 PKI 私人密钥 301。该卡的基于私人密钥的功能（即涉及到卡的私人密钥的非对称密码操作，比如签名或者解密）是产生 OTP 或者 MAC 的过程的整体阶段或者一部分。

OTP 和 / 或 MAC 的生成以如下方式发生 :

步骤 99 :捕获将在以后步骤中使用的输入值。

步骤 101 :用于 OTP 或者 MAC 生成算法的 (多个) 输入被变换或者格式化成初始值。

步骤 102 :初始值由卡的私人密钥 301 进行签名或者加密 / 解密。

步骤 103 :将所得密码变换成 OTP 或者 MAC。

在图 3 的例子中, OTP 或者 MAC 仅为非对称密码操作的结果的函数。然而在其他实施例中,OTP 或者 MAC 也可以是包括多个值的其他数据元素的函数,所述多个值是可变输入的函数,但不是私人密钥 301 的函数。

在典型的实施例中,对 OTP 或者 MAC 生成算法的输入与在传统强认证令牌中使用的 (多个) 强认证算法的输入相同或者相似。换言之,这些输入例如可以选择为 :

时间值,或者

询问 (通常由服务器提供),或者

计数器值,或者

业务数据,或者

上述输入的任何组合。

在一些实施例中,对 OTP/MAC 生成算法的 (多个) 附加输入或者 (多个) 参数例如可以包括 :

标识设备的数据 (例如读取器序列号),或者

存储于设备中的秘密,或者

用户标识数据,或者

用户提供的秘密代码或者秘密值。

为了将这些 (多个) 输入格式化成初始值,步骤 101 例如可以包括以下操作 :

并置 (concatenation),或者

散列,或者

利用对称密码算法 (例如使用设备中存储的或者用户提供的秘密密钥) 的加密 / 解密。

为了将所得密码变换成最终 OTP 或者 MAC 值,步骤 103 例如可以包括以下操作 :

散列 (可能是使用读取器 105 中存储的或者用户提供的秘密密钥的带密钥散列),或者

利用对称密码算法 (例如使用读取器 105 中存储的或者用户提供的秘密密钥) 的加密 / 解密,或者

截取,或者

选择某些位、半字节 (nibble) 或者字节,或者

十进制换算。后者可以实现如下 :

将要十进制转换的位串解释为对数的大的二进制表示,或者按位组划分要十进制转换的位串,并且将各位组映射到十进制数位。典型例子是将位串划分成半字节,并且根据以下规则将各半字节映射到十进制数位。如果半字节的十六进制值为 0x0 到 0x9,则取得具有相同值的十进制数位 ;如果半字节的十六进制值为 0xA 到 0xF,则减去常数 (在 0x6 与 0xA 之间),然后取得值与相减的结果相同的十进制数位,或者本领域技术人员已知的许多其他十进制换算算法。

现在描述证实阶段。在该实施例中，证实服务器具有用来生成 OTP 或者 MAC 值的私人密钥 301 的副本，并且使用该副本来进行与用于生成 OTP 或者 MAC 值的算法本质上相同的算法。证实服务器：

（参见图 4）以某种方式获得或者重构或者猜测在生成 OTP 或者 MAC 时用作对 OTP 或者 MAC 生成算法的（多个）输入的数据元素的（多个）值：

在时间值的情况下，证实服务器可以具有其自己的与用于生成 OTP 或者 MAC 的时钟同步的时钟，

在询问的情况下，询问可以由证实服务器本身生成，或者可以与接收的 OTP 或者 MAC 一起由应用传递至证实服务器，

在计数器的情况下，证实服务器可以维护其自己的与用于生成 OTP 或者 MAC 的计数器值同步的计数器值，

在业务数据的情况下，这些数据可以与接收的 OTP 或者 MAC 一起由应用传递至证实服务器；

将用于 OTP 或者 MAC 生成算法的（多个）输入变换成初始值。

随后使用由证实服务器保持的私人密钥 301 的副本对初始值进行签名或者加密 / 解密 (402)。然后，证实服务器将所得参考密码与接收的 OTP 或者 MAC 值进行比较 (403)。如果所得参考密码与接收的 OTP 或者 MAC 值匹配，则成功地证实了签名。可以用以下多种方式完成该比较：

证实服务器在一些实施例中可以将参考密码变换成参考 OTP 或者 MAC 值，并且将参考 OTP 或者 MAC 值与接收的 OTP 或者 MAC 值进行比较（例如通过检验它们是否相同），或者

证实服务器可以根据接收的 OTP 或者 MAC 值来重构由私人密钥生成的原密码的一部分，并且将这一部分密码与参考密码的对应（多个）部分进行比较，或者

证实服务器可以将参考密码变换成第一中间证实值，并且将接收的 OTP 或者 MAC 变换成第二中间证实值，并且将第一中间证实值与第二中间证实值进行比较。

这可以由以下例子说明（参见图 14）。在该例子中，基于如下密码来产生 OTP 或者 MAC，该密码是使用私人密钥 1308 的非对称加密的结果。服务器产生如下参考密码，该参考密码也是使用密钥 1324 的非对称加密的结果，密钥 1324 是私人密钥 1308 的副本。如图 14 中所示：

- 读取器 1350 通过以下操作根据所述原密码来计算 OTP 或者 MAC：

○选择所述所得密码的每个字节的每个第一位 (1355)，并且

○将选择的所述位并置成位串 (1356)，并且

○将所述位串解释为数的二进制说明，并且通过取得所述数的十进制表示来获得 OTP 或者 MAC(1357)

- 证实服务器使该 OTP 或者 MAC 证实如下：

○服务器通过将每个字节的除了每个第一位之外的所有位设置成 1 来修改参考密码 (1364)，并且

○服务器将接收的 OTP 或者 MAC 解释为数的十进制表示，并且通过取得该数的二进制表示来获得位串 (1359)，并且

○服务器通过将所述位串的每一位替换成如下字节来扩展所述位串 (1360)，该字节由

附加以七个 1 位来扩展的位构成，并且

○服务器将扩展的所述位串与修改的所述参考密码进行比较 (1365)。

该过程的参数（选择每个字节的一位）为说明性的。本领域技术人员将能够选择适当参数以适合他们的需要和背景。具体而言，典型 RSA 密码约为 100 字节。选择各字节的一位将产生 100 位。这在每十进制数位约为 3 位时将产生用于 OTP 或者 MAC 的约 30 个十进制数位，这比 300 个十进制数位更实用，但是仍然可能被认为难以使用。在该情况下可以选择每 40 位中的一位，从而共计 20 位或者约 6 个十进制数位。也可以在使用对称密钥而不是非对称密钥的情况下，使用用于根据密码来生成 OTP 或者 MAC（通过选择密码的一些位但是并非所有位来变换）的相同过程。典型对称密码包括约 100 位。在该情况下，每八位选择一位将带来约 12 位或者 4 个十进制数位。这可能被认为是太小以至于无法免受攻击的数目。为了避免该问题，仅使用每 4 位中的一位（而不是每 8 位中的一位）以带来约 25 位或者约 8 个十进制数位。

在图 13 中图示了一种可选证实过程。图 13 的过程在产生客户端侧的密码（操作 1305）和服务器侧的参考密码（操作 1323）方面与图 14 的过程相同。如图 13 中所示：

密码通过首先是变换 A(1306)、然后是变换 B(1307) 这两个变换的序列来变换成 OTP 或者 MAC

证实服务器使参考密码经历操作 1325 以产生修改的参考密码，操作 1325 与变换 A 的操作相同，

证实服务器也使 OTP 或者 MAC 经历操作 (1327)，该操作是用于产生修改的 OTP 或者 MAC 的变换 B 的逆变换，

证实取决于修改的 OTP 或者 MAC 与修改的参考密码的比较 (1328)。

如针对图 14 的证实过程的情况那样，无论是用对称密钥还是用非对称密钥来产生密码都可以使用图 13 的技术。

与传统 PKI 签名验证相比，图 3 的方法并不要求服务器可获得整个签名（如结合图 13 或者图 14 示范的那样）。即使在不使用私人密钥之外的附加秘密代码或者密钥（由用户提供或者存储于设备中）的情况下，该解决方案仍然可以提供很高的安全等级。

然而，证实服务器在其必须证实 OTP 或者 MAC 时仅在具有卡的私人密钥的副本的情况下，才可以使用图 3 的技术。PKI 的全部要点正是在于为了保障真正的不可否认性，私人密钥决不可以被与该密钥相关联的用户之外的任何人访问。在许多情况下，在不可能从卡提取私人密钥的情况下通过生成机载私人和公共密钥对的卡来保障这一点。在其他情况下，密钥对在外部生成，然后注入卡中，但是这些过程通常会确保卡个性化系统中的私人密钥在注入卡中之后立即被破坏，并且在卡外不允许存在私人密钥的副本。换言之，该方法在许多情况下不是适合的解决方案。

使用非对称密码作为种子以导出秘密密钥（图 5）

在以下实施例中，并不要求证实服务器在证实时访问私人密钥的副本。在该实施例中，以与传统强认证令牌相同的方式生成 OTP/MAC。该算法的所有步骤（捕获输入、将输入格式化、对格式化的输入进行加密或者散列、将所得散列的密码变换成 OTP/MAC）由读取器 505 进行。在该实施例中，本发明与常规实践不同之处在于读取器 505 如何获得对称秘密强认证密钥。为了获得该秘密对称认证密钥，读取器 505 依赖于涉及到卡 500 的私人密钥 520

的对卡 500 的操作。该方法的基本实施例的主要步骤如下：

1. 如果需要（即卡通过 PIN 保护私人密钥的使用），则读取器要求用户输入 PIN 并且将该 PIN 提交到卡。

2. 假设卡 500 接受 PIN，未连接的卡读取器将固定值提交到卡以由私人密钥签名。该固定值也称为‘读取器到卡的询问’。

3. 卡使用其私人密钥对给定询问进行签名并且将所得密码返回到读取器。该所得密码也称为‘卡到读取器的签名响应’。

4. 读取器使用所得密码作为种子以导出对称秘密密钥。该密钥也称为‘导出的强认证秘密密钥’。

读取器用导出的强认证秘密密钥将强认证算法动态地个性化（完全由读取器进行）。换言之，读取器使用导出的强认证秘密密钥来执行强认证令牌算法。

图 5 图示了适当的实施例，该实施例示出了读取器 505 与卡 500 的交互。该处理可以要求用户输入 PIN 510 以便将卡 500 解锁。这一步骤是可选的，但是如果执行该步骤，则用户在 510 输入的 PIN 被送达 511 到待测试的卡 500。卡接受或者拒绝该 PIN。测试卡 500 的响应 (512)，并且仅在接受的情况下处理才继续。随后功能 513 捕获来自读取器、用户或者卡中的一些或者全部的输入值。功能 514 可以将一些或者所有输入值格式化。这些值中的一些或者所有值或者其他值可以形成向卡 500 发送（功能 515）的读取器到卡的询问 515a。卡 500 通过用卡的私人密钥 510 进行密码操作来使用询问 515a。卡到读取器的签名响应 516a 这一所得密码被回送到读取器（功能 516）。然后，将响应 516a 用作种子以经由功能 517 创建秘密值或者密钥 517a。密钥 517a 称为导出的秘密强认证密钥。然后，在功能 518 处将密钥 517a 与由功能 514 提供的格式化的值一起用在密码操作中。最后在功能 519 处变换所得的密码以产生 OTP 或者 MAC。

‘读取器到卡的询问’515a 可以是任何以下值：

1. 对于某个批次的所有读取器而言相同的固定值。

2. 对于给定读取器而言固定的、但是对于各读取器而言具有不同值的固定值。

3. 对于给定用户而言是恒定的、但是对于不同用户而言可以不同并且被用户输入读取器中至少一次的固定值。在实践中很有可能的是，每当使用卡时将输入该值，或者仅在首次将给定卡与某一读取器一起使用时输入该值，并且然后读取器将记住该值。

4. 存储于卡上可以由读取器读取的静态数据（例如公共密钥和证书或者卡序列号）

5. 上述值的任何组合。

6. 根据任何上述值导出的值。该导出可选地包括使用某一读取器秘密。

用于根据‘卡到读取器的签名响应’来导出强认证秘密密钥的算法可以利用以下技术（以及其他技术）：

1. 提取一些数据元素的位

2. 并置一些数据元素的一些部分

3. 对称加密 / 解密算法（例如 DES、AES、…）

4. 散列算法（例如 SHA-1）

用于根据‘卡到读取器的签名响应’516a 来导出强认证秘密密钥 517a 的算法除了‘卡到读取器的签名响应’516a 之外还可以利用以下额外数据元素：

1. 对于某个批次的所有读取器而言相同的固定值。

2. 对于给定读取器而言固定的、但是对于各读取器而言具有不同值的固定值。

3. 对于给定用户而言恒定的、但是对于不同用户而言可以不同并且用户在读取器中输入至少一次的固定值。

4. 存储于卡上、可以由读取器读取的静态数据（例如与私人密钥相关联的数据，比如公共密钥和证书或者卡序列号）。

5. 上述值的任何组合。

该描述仅提及对智能卡的单个私人密钥的使用和与该密钥相关联的单个操作；如果卡包含多于一个私人密钥，则读取器可以将‘读取器到卡的询问’515a 提交至这些卡私人密钥中的每个私人密钥，并且在导出‘导出的强认证秘密密钥’517a 时组合所得的‘卡到读取器的签名响应’516a。

类似地，读取器也可以将不同的‘读取器到卡的询问’值 515a 提交到卡，并且在导出‘导出的强认证秘密密钥’517a 时组合所得的‘卡到读取器的签名响应’516a。

在又一实施例中，读取器并不依赖于单个‘读取器到卡的询问’515a 以及对应的‘卡到读取器的签名响应’516a 和‘导出的强认证秘密密钥’517a，而代之以使用一组‘读取器到卡的询问’515a 以及对应的‘卡到读取器的签名响应’516a 和‘导出的强认证秘密密钥’517a。为了获得‘导出的强认证秘密密钥’577a，读取器选择这些‘读取器到卡的 515a 询问’之一并且将其提交至卡。选择哪个‘读取器到卡的询问’515a 确定了对应的‘卡到读取器的签名响应’516a 和‘导出的强认证秘密密钥’517a。该选择因此必须以对于证实服务器而言可预测的方式发生。读取器可以例如按固定顺序遍历这组‘读取器到卡的询问’515a，或者可以根据对强认证令牌算法的（多个）输入值来选择‘读取器到卡的询问’515a。后一种方法的简单例子是强认证令牌算法在询问 - 响应模式下工作，并且询问的一个特定数位（例如末位）表明要使用的‘读取器到卡的询问’的索引。

由于私人密钥对于各卡而言不同，所以导出的秘密密钥对于给定询问而言将为给定卡所特有。换言之，在读取器中的强认证算法中使用的秘密密钥是卡（或者更精确地为该卡中的私人密钥 510）的函数。这意味着原则上需要访问正确的卡以能够生成正确的 OTP。

在大多数情况下，私人密钥受 PIN 保护，从而除了访问正确的卡之外也需要知道卡的 PIN 以能够生成正确的 OTP。

如果读取器向卡提交的要由私人密钥签名的固定值对于不同读取器而言可以不同，则除了其他要素（例如访问正确的卡和知道卡的 PIN）之外也需要正确的读取器。注意：对于不同读取器而言不同的值的这样的使用将读取器有效地‘绑定’到卡。

为了使证实服务器能够证实以该方式生成的强认证 OTP 和 / 或 MAC，证实服务器必须知道导出的强认证秘密密钥 517a 的值。服务器因此必须知道卡的签名响应 516a。针对给定卡询问的卡签名响应由卡的私人密钥 510 确定，并且在没有访问私人密钥 510 的情况下不能加以计算。这样做的一个后果是，服务器必须（直接或者间接地）访问卡的私人密钥 510 至少一次。

如果在卡上内部生成密钥对，则这意味着服务器需要访问卡至少一次，从而服务器可以向卡提交将适用于该用户的（多个）卡询问，并且检索和存储对（多个）询问的（多个）卡响应（间接访问私人密钥）。如果密钥对在外部生成、然后注入卡中，则服务器可以直接

使用私人密钥，从而在位于卡外的私人密钥被破坏之前对（多个）询问加密。

服务器仅这时才能够根据加密的卡询问来计算对应的导出的强认证密钥。这一点的缺点在于，在实践中，用户将不得不在一种登记阶段期间向服务器授予对他／她的卡的访问权，或者（在外部密钥生成的情况下）必须允许服务器在该私人密钥值被破坏之前用该私人密钥值对询问加密。

另一后果是，在实践中对于某一用户而言，导出的强认证秘密密钥必须保持不变。由于根据对某一卡询问进行响应的卡的签名来导出该导出的强认证秘密密钥，所以该卡询问和对应的‘卡到读取器的签名响应’对于给定用户必须保持固定。这一点的缺点在于，如果攻击者获得某个用户的‘卡到读取器的签名响应’的值，则该攻击者可能潜在地伪造如下卡，这些卡在插入读取器中时总是返回所记录的“卡到读取器的签名响应”值。

在生成‘读取器到卡的询问’和／或根据‘卡到读取器的签名响应’来导出‘导出的强认证秘密密钥’时包括读取器特有或者用户特有的数据元素可以使攻击者更难以获得正确的‘卡到读取器的签名响应’的值或者更难以将该值与读取器一起用来以欺诈方式生成正确的 OTP 或者 MAC。

使攻击者更难以获得正确的‘卡到读取器的签名响应’的另一方式并不如上文说明的那样依赖于单个‘读取器到卡的询问’以及对应的‘卡到读取器的签名响应’和‘导出的强认证秘密密钥’，而代之以使用一组‘读取器到卡的询问’以及对应的‘卡到读取器的签名响应’和‘导出的强认证秘密密钥’。

在以下实施例中，使服务器访问卡至少一次以进行私人密钥操作的要求被完全消除。

在该实施例中，对称秘密认证密钥的值并不（直接或者间接地）取决于卡的私人密钥的值。并未借助涉及到卡的私人密钥的非对称密码操作根据由卡生成的种子来导出对称秘密认证密钥。代之以用对称秘密认证密钥或者用读取器可以从中动态地导出对称秘密认证密钥的秘密数据来将读取器个性化。利用该对称秘密认证密钥，读取器可以生成恰如传统强认证令牌一样的 OTP 或者 MAC。通过将用户的卡逻辑地绑定到读取器来使读取器的使用受到保护并且为合法用户而保留。一旦用户的卡绑定到读取器，仅在用户插入绑定到读取器的卡的情况下读取器才会生成 OTP 或者 MAC。卡因此用作用于将个性化的读取器解锁的访问密钥。

在首次使用时，读取器将请求插入用户的卡。在插入卡时，读取器以如下方式将自身逻辑地绑定到插入的卡。读取器确定和记住该卡的一些特有个别特征。这些特征可以包括：

○卡序列号

○卡的公共密钥和／或证书

○卡对给定询问的响应（其中将响应定义为用卡的私人密钥对询问的加密。注意：这通常会要求用户提交 PIN 以将私人密钥解锁）。该询问和对应的卡的响应必须由读取器记住。询问可以是：

■固定总询问（对于所有卡和所有读取器而言相同）

■每读取器的固定询问

■每卡的固定询问（例如在首次提供卡时由读取器随机生成、然后被读取器记住）

■用户提供的询问

■上述询问的任何组合

在图 6 中图示了该操作的例子。读取器 600 等待接收卡数据（功能 616）。卡将一些卡数据 611 提供给读取器（功能 610）。当读取器接收到卡数据 611 时存储该数据（功能 617）。

如果用户想要生成动态口令或者签名（参见图 7），则读取器请求绑定到该读取器的卡。读取器检验提供的卡是否确实为期望的卡。即读取器将检索提供的卡的特征（功能 710），并且将这些特征与绑定到读取器的卡的存储的特征进行比较（功能 711）。该步骤可以包括：

■读取卡的序列号

■读取卡的公共密钥和 / 或证书

■将（存储的）询问提交到卡，以便由卡的私人密钥加密（可以要求用户提供 PIN 以将私人密钥解锁），并且接收卡的响应。

一旦提供的卡被成功证实，读取器继续执行如普通强认证令牌那样的强认证算法。

为了加强安全性，许多变化是可能的。读取器可以根据以下各项来导出对称秘密认证密钥：

○在读取器中预先个性化的数据元素

○和 / 或用户向读取器提供的数据元素

○和 / 或读取器从卡读取的数据元素

优选地，这些数据元素是秘密的。代替总是使用在卡绑定到读取器时使用和获得的相同询问和对应的卡响应，读取器可以使用多对询问和对应的响应。按照该原理的变化包括：

○当卡绑定到读取器时，读取器生成多于一个的询问并将所述询问提交至卡并且记住对应的卡响应。当读取器以后需要证实该卡时，其可以将这些询问的任何子集提交到卡，并且检验卡的响应是否与存储的响应匹配。

○当读取器已经成功证实插入的卡时，它可以生成新询问并且从卡获得对应的响应。然后，该新询问 - 响应对可以由读取器记住，作为先前已知的（多个）询问 - 响应对的替代对或者附加对。

○可以组合这两种变化。

又一实施例（图 8 和图 9）的原理如下。读取器代表服务器借助于基于传统证书的对用户的 PKI 卡的认证在本地认证用户。

如果用户由读取器成功认证，则读取器生成可以由证实服务器证实的 OTP 或者 MAC（使用传统强认证令牌算法）。然后，用户可以将该 OTP 或者 MAC 提交到服务器作为他已经由读取器成功认证的证据。

读取器借助于用户的插入的 PKI 卡并且使用传统 PKI 技术来本地认证用户。在典型的实施例中这可以进行如下（参见图 8）：

1. 读取器 800 证实卡的证书 806（或者证书链）。

a. 注意：这假设读取器具有对（根）证书颁发机构的受信任公共密钥的访问权。这可以通过在读取器中存储（根）证书颁发机构的受信任公共密钥来完成。

b. 注意：读取器 800 无需每当在读取器中插入卡时都完成从（根）CA 公共密钥开始对整个证书（链）的显式验证。替代地，读取器 800 可以在卡 805 首次插入读取器中时进行

整个验证。然后，读取器可以存储经验证的证书或证书的公共密钥或者从验证的证书或者公共密钥导出的参考值（例如证书或者公共密钥的散列）。然后，如果在以后插入卡 805，则读取器 800 不再需要进行与证书证实相关联的所有计算，而是可以仅将卡上的证书与存储于读取器中的证书或者参考值相比较。

2. 读取器 800 进行对卡的私人密钥的询问 - 响应认证：

a. 读取器 (810) 生成询问 811，例如通常为例如使用读取器中存储的某一秘密借助密码算法根据时间值或者计数器值而导出的随机数或者某一其他非可预测值。

b. 用户提供对卡的私人密钥进行保护的 PIN。

c. 读取器 800 将 PIN 提交至卡。

d. 读取器 800 将随机询问 811 提交至卡以由卡的私人密钥来加密。

e. 卡用其私人密钥对读取器签名 (815) 并且返回响应（＝加密的询问 816）。

f. 读取器 800 用（来自证书的）卡的公共密钥对卡的响应进行解密。

g. 读取器将经解密的卡的响应与原来生成的询问进行比较 820。如果解密的卡响应与原来生成的询问相同，则卡的私人密钥被认证，并且因此用户被认证。

本质上，读取器以与传统强认证算法相同的方式生成 (825)OTP/MAC。该算法的所有步骤（捕获输入、将输入格式化、对格式化的输入进行加密或者散列、将散列的所得密码变换成 OTP/MAC) 以与传统强认证令牌本质上相同的方式由读取器 800 完成。在一个实施例中，用对称秘密强认证密钥将读取器个性化。在该情况下，读取器 800 也通常被配置成期望特定的卡。读取器借助卡的数据元素的某一特性值来识别该卡。通常，卡的证书用作这样的数据元素。在其他实施例（参见图 9）中，为了避免不得不对读取器进行个性化和配置，读取器 800 根据以下数据元素来为对称秘密强认证密钥导出 (835) 卡特有的值：

○最好与卡的证书或者公共密钥有关的公共卡数据（例如卡序列号、证书序列号、公共密钥等）

○存储于读取器中并且为服务器所知的主密钥 846。这一主密钥可以是：

■用于所有读取器的相同值

■用于各个别读取器的特定 / 唯一值。这要求以某种方式向用户分配读取器和在服务器登记该分配。

○（可选）额外导出数据元素可以是用户向读取器提供的（秘密）数据元素。用户必须显式地提供该数据元素：

■每当以该方式使用读取器和卡时，或者

■仅当该卡首次与该读取器一起使用时（此后读取器将记住所提供的用于该卡的数据元素的值）

读取器 800 在对称强认证算法（例如，数字通算法或 OATH) 中使用导出的卡特有对称认证密钥 836 以生成 (845)（基于询问 - 应答和 / 或时间和 / 或事件）的动态口令或者生成 (845) 在某些业务数据上的电子签名（可选地包括时间和 / 或时间计数器信息）。

[0121] 服务器使生成的动态口令或者签名证实如下：

■服务器导出与读取器相同的卡特有对称强认证密钥。这假设服务器具有将用户链接到以下数据的数据库（或者检索所需信息的替代方式）：

○公共卡数据，

○用户提供的数据元素（如果适用）

○以及读取器的主密钥

注意：代替每当必须执行证实时就执行这一导出，也可以执行一次导出，并且所得的导出密钥可以存储于数据库中以供将来使用。

■服务器以与它针对传统强认证令牌进行证实的方式相同的方式来证实动态口令或者签名。

[0122] 一个典型的实施例操作如下（图 10-11）：

在招募阶段中，银行客户 1001 前往银行支行 1003。客户使用其全国电子身份卡 (e-id 卡 1002) 与银行支行终端 (BBT，Bank Branch Terminal) 一起来对电子银行合同 1004 进行电子签名。

[0123] 在客户的 e-id 卡插入 BBT 中时 (1010)，BBT：

○捕获客户的证书 (1011)，

○生成随机种子询问 (1012)，

○将随机种子询问提交到 e-id 卡 (1002) 以由卡的私人密钥加密 (1013)，

○捕获在该询问上的卡密码 (1014)。

[0124] 最后，BBT 将客户的证书、生成的种子询问和种子询问上的卡密码发送到服务器 (1015)。服务器将这一数据存储于链接至客户的数据库中。银行然后将未连接的智能卡读取器传送给客户。这一读取器包含秘密主密钥。银行还向客户发送 PIN 邮包，该 PIN 邮包具有 BBT 生成和使用的种子询问的值。也向认证服务器通知秘密主密钥的值。

[0125] 当客户首次使用读取器时：

○读取器要求插入客户的 e-id 卡。

○读取器还请求 PIN 邮包的种子询问并且将它存储于存储器中。

○读取器读取卡的证书并且还将它存储于存储器中。

○读取器生成随机读取器询问，并且将它提交至卡，以由卡的私人密钥加密。读取器存储读取器询问和由卡生成的对应密码。

[0126] 如果客户想要生成 OTP（或者 MAC 或者响应或者…），则读取器完成以下步骤：

○读取器要求插入客户的 e-id 卡。

○读取器证实卡：

■读取器读取卡的证书并且将它与存储的证书相比较。

■如果检查成功，则读取器将存储的读取器询问提交至卡进行签名，并且将卡的密码与存储的密码相比较。

○如果读取器已经成功地证实卡，则读取器生成秘密认证密钥：

■读取器将存储的 PIN 邮包种子询问提交至卡以便由卡加密。

■读取器现在根据以下各项来导出秘密认证密钥：

■读取器中的秘密主密钥，

■ PIN 邮包种子询问，

■该 PIN 的邮包种子询问上的卡密码，

■卡的证书。

○读取器现在在强认证算法中使用生成的秘密认证密钥（以例如生成 OTP 或者 MAC）。

认证服务器能够验证所得的 OTP(或者 MAC),因为它具有对生成秘密认证密钥所必需的所有数据的访问权 :

○读取器的秘密主密钥,

○卡的证书,

○ PIN 邮包询问,

○ PIN 邮包询问上的卡密码。

使用生成的秘密认证密钥,认证服务器可以用与它证实由传统强认证令牌生成的 OTP 或者 MAC 的方式相同的方式来证实 OTP 或者 MAC。

代替地,认证服务器可以使用用于证实操作的在图 13 或者图 14 中所示的任一过程。

结合图 13 的过程,假设使用变换 A(1306) 和变换 B(1307) 这一序列来变换由读取器产生的密码。出于证实目的,服务器使 OTP 或者 MAC 经历反变换 B(1327) 以产生修改的 OTP 或者 MAC,然后使参考密码经历变换 A(1325) 以产生修改的参考密码。最后,服务器将修改的参考密码与修改的 OTP 或者 MAC 进行比较。

结合图 14 的过程,假设如图 14 中所示使用位选择 (1355)、并置 (1356) 和位串变换 (1357) 这一序列来变换由读取器产生的密码以产生 OTP 或者 MAC。出于证实目的,服务器使 OTP 或者 MAC 经历图 14 的位流处理 1359 和扩展处理 1360 以产生修改的 OTP 或者 MAC。服务器使参考密码经历操作 1364 以产生修改的参考密码。最后,服务器将修改的参考密码与修改的 OTP 或者 MAC 进行比较 (1365) 以进行证实。

图 15 至图 22 图示了本发明的实施例的特定集合的各个方面。以下装置和数据元素在这些实施例中起作用 :

装置

PKI 装置

在这一组实施例的环境中,图 15 中图示的 PKI 装置 1500 是包括下述器件的设备 :存储器 1520,其用于存储公共 - 私人密钥对中的至少一个私人密钥 ;以及数据处理装置 1510,其包括使用该私人密钥进行非对称密码操作的一个或更多个数据处理部件 (例如,Infineon(英飞凌)SLE66CLxxx 微型控制器)。PKI 装置 1500 还可以包括存储另外的私人密钥和 / 或与这些一个或更多个私人密钥相关联的一个或更多个公共秘钥和 / 或与这些一个或更多个公共秘钥相关联的一个或更多个证书。非对称密码计算通常包括生成数字签名。PKI 装置 1500 还能够进行其他类型的密码操作。PKI 装置 1500 还可以存储包括用户相关数据例如用户名称或者与用户有关的唯一号码的其他类型的数据。在典型的实施例中,PKI 装置 1500 还包括用于与特定读取器装置进行电子通信和交换数据的通信接口 1530,电子通信和交换数据包括 :接收来自这样的读取器装置的数据 ;接收来自读取器装置的指令以使用在 PKI 装置上存储的非对称私人密钥对由读取器装置提供的特定数据进行非对称密码操作 ;以及返回该非对称密码操作的结果。在典型的实施例中,这包括使用私人密钥对由读取器装置提供特定数据进行数字签名以及返回得到的签名。在一些实施例中,通信接口 1530 可以包括 USB 接口。在其他实施例中,通信接口可以包括智能卡接口。在典型的实施例中,智能卡接口根据 ISO/IEC 标准集合。在一些实施例中,PKI 装置可以包括 USB 令牌。在其他实施例中,PKI 装置可以包括智能卡。在一些实施例中,PKI 装置可以由政府机构发放给至少一些公民。PKI 装置可以例如包括电子全国身份卡。在其他实施例中,PKI 装置可

以由金融机制发放给例如其客户。在再一些实施例中，PKI 装置可以由提供电信服务的公司发放。在一些情况下，PKI 装置可以包括 SIM（用户身份模块）卡。在一些实施例中，由 PIN 码来保护涉及使用 PKI 装置的私人密钥的操作。在典型的实施例中，存储在 PKI 装置中的私人密钥对于 PKI 装置是已知的，并且不能从 PKI 装置读出。在特定实施例中，PKI 装置包括具有至少一个公共 - 私人密钥对的 PKI 智能卡，至少一个公共 - 私人密钥对具有能够使用私人密钥生成数字签名从而由 PIN 码保护私人密钥的使用的关联证书。

读取器装置

在这一组实施例的环境中，图 16 所示的读取器装置 1600 是包括与特定 PKI 装置进行电子通信和交换数据的电子通信接口 1630 的设备。在典型的实施例中，这包括 ：将特定数据提供至 PKI 装置 ；指示 PKI 装置使用在 PKI 装置上存储的非对称私人密钥对提供至 PKI 装置的数据进行非对称密码操作 ；以及从 PKI 装置接收该非对称密码操作的结果。在典型的实施例中，这可以包括指示 PKI 装置使用在 PKI 装置上存储的私人密钥对由读取器装置提供的特定数据进行数字签名并且接收所得到的签名。在一些实施例中，读取器装置的电子通信接口 1630 可以包括与包括智能卡的 PKI 装置进行交互的智能卡读取器 1635。在典型的实施例中，智能卡读取器 1635 符合 ISO/IEC 标准集。智能卡读取器的智能卡接口还可以符合由 EMVco（参见 www.emvco.com）发布的 EMV 规范。在其他实施例中，读取器装置的电子通信接口 1630 可以包括例如与包括 USB 令牌的 PKI 装置进行交互的 USB 接口。

读取器装置 1600 还包括处理装置 1620，处理装置 1620 包括适于进行对称密码操作的一个或更多个数据处理部件。数据处理部件可以例如包括适当地编程的微型处理器、微型控制器、FPGA（现场可编程门阵列）或 ASIC（专用集成电路）。数据处理部件可以例如包括德州仪器 (Texas Instruments) MSP430 微型控制器。这些对称密码操作包括生成动态认证凭证例如 OTP 或电子签名，从而读取器装置的处理装置使用对称密码算法来将至少一个或多个对称秘密值与一个或更多个动态变量进行组合，从而根据该组合的结果导出动态认证凭证。在典型的实施例（参见图 17）中，对称密码算法 1621 通过将至少一个或多个秘密秘钥（1661、1662 等）与一个或更多个动态变量（1671、1672 等）以及还与作为存储在 PKI 装置中的私人密钥的函数的数据元素（私人密钥相关输入参数（1681）：参见下文）进行组合来生成一个或更多个动态凭证 (1691)。在另一实施例中，对称密码算法通过将一个或更多个动态变量与作为私人密钥相关输入参数或者根据私人密钥相关输入参数导出的对称秘密值进行组合来生成（多个）动态凭证。在一些实施例中，生成动态凭证的对称密码算法可以包括动态加密或解密算法例如 DES 或 AES。在典型的实施例中，生成动态认证凭证包括使用对称加密或解密算法利用秘密对称秘钥对至少一个或多个动态变量与私人密钥相关输入参数的组合进行加密或解密。在一些其他实施例中，对称密码算法可以包括键入 - 散列 (keyed-hash) 算法。在典型的实施例中，生成动态认证凭证包括使得秘密值、动态值和私人密钥相关输入参数的组合散列。动态变量可以包括时间相关值、计数值、由一些应用提供的询问、业务相关数据或者前述的组合。在特定实施例中，对称密码算法包括生成 OTP 或电子签名的已知的或标准的对称算法，该算法将对称秘密与第一外部动态变量和第二内部或外部动态变量进行组合，从而读取器装置将私人密钥相关输入参数的值分配至第一外部动态变量。生成 OTP 或电子签名的已知的或标准的对称算法可以包括 OATH 或 DIGIASS 询问响应或业务数字签名算法。

读取器装置 1600 可以包括用于提供时间相关值的实时时钟 1650。读取器装置 1600 还可以包括用于存储计数值的存储器 1610。读取器装置 1600 还可以包括用于存储一个或更多个秘密密钥或秘密值的存储器 1610。读取器装置 1600 还可以包括用于存储数据例如 PKI 装置专用或私人密钥专用的询问或者与 PKI 装置或 PKI 装置上的私人密钥有关的允许读取器装置随后识别 PKI 装置或 PKI 装置上的私人密钥的数据。

读取器装置 1600 还包括用于输出至少一个或更多个动态认证凭证的一个或更多个输出部件 1660。在典型的实施例中，读取器装置还可以使用输出部件来输出私人密钥码（参见另外描述）。在一些实施例中，输出部件 1660 包括显示器。可以使用不同类型的显示器。显示器可以包括例如 CRT（阴极射线管）、LED（发光二极管）或 LCD（液晶显示）显示器。输出部件还可以包括显示器或 LCD 控制器。在其他实施例中，输出部件 1660 例如电磁扬声器以声音的形式生成输出。在其他特定实施例中，这些输出部件适于生成和输出合成语音。

在一些实施例中，读取器装置 1600 还可以包括输入部件 1670，该输入部件 1670 用于接收数据例如外部动态变量值（例如，询问或业务数据）或者例如要提交至 PKI 装置的 PIN 值或者激活码。在一些实施例中，输入部件可以包括键盘或键区。在其他实施例中，输入部件可以包括具有多个光传感器的光学接口。

在典型的实施例中，读取器装置具有自主电源例如一个或更多个电池。在一些实施例中，这些电池可以更换。

服务器侧部件

以上描述的读取器装置通常由用户与用于生成动态凭证以确保一些计算机管理的应用的用户的 PKI 装置结合使用。在典型的实施例中，计算机管理的应用与用于验证从应用的用户接收的动态凭证的一个或更多个认证部件进行交互或者包括用于验证从应用的用户接收的动态凭证的一个或更多个认证部件。其他服务器侧部件可以包括一个或更多个数据库，一个或更多个数据库用于存储链接至特定用户的数据，例如与特定用户相关联的读取器装置的读取器装置识别数据元素或者与特定用户相关联的私人密钥相关输入参数的值和 / 或链接至特定读取器装置的数据例如一个或更多个秘密秘钥。

应用服务器

计算机管理的应用通常由用户可以经由网络访问的应用服务器来管理。在通常情况下，应用是基于网络的，应用服务器为网络服务器，网络为因特网，并且用户可以借助于能够上网的客户端装置上的浏览器来访问应用。在其他实施例中，应用可以具有 IVR（交互语音响应，Interactive Voice Response）接口并且用户可以经由电话网络来访问应用。在又一些实施例中，应用可以存在于用户直接访问的本地计算机装置上。在所有这些情况下（包括随后的情况），将应用及其关联部件称为服务器侧和服务器侧部件。

认证软件 / 服务器 / 应用

一个或更多个认证部件可以包括集成进应用软件并且对应用提供动态凭证验证功能的认证软件库。在其他实施例中，一个或更多个认证部件可以包括使用用于验证所接收的一个或更多个动态凭证的一些认证协议的独立式认证服务器。在一些实施例中，一个或更多个认证部件可以包括认证应用。在典型的实施例中，如图 18 所示，在一个或更多个认证部件中可以分为两级或两层。

第一（内或芯）层 1801 包括用于使用现有或标准动态凭证验证算法来验证一个或更

多个动态凭证的一个或更多个部件，现有或标准动态凭证验证算法将至少一个对称秘密密钥与至少第一外部动态变量（例如询问或业务相关数据）和第二内部或外部动态变量（例如，计数器或基于时间的变量）以密码的形式进行组合。在一些实施例中，验证算法还可以使用另外的外部或内部动态变量。该内层或芯层的接口至少包括用于验证动态凭证从而期望调用部件传递动态凭证和至少第一外部动态变量的值以及如果适用则还有另外的外部变量的值的功能或功能性。在一些实施例中，调用部件还通过接口来传递对称秘密秘钥。在其他实施例中，调用部件传递与用户身份有关的数据元素或者读取器标识符，并且内层包括使用所接收的与用户身份或读取器标识符有关的数据元来确定对称秘密密钥的值的一个或更多个部件。确定对称密钥的值可以包括使用所接收的与用户身份或读取器标识符有关的数据元作为搜索密钥来进行数据库搜索。

第二（外层）1802 包括具有用于验证动态认证凭证的功能或功能性的接口，该动态认证凭证由在上面结合对读取器装置的描述（图 16）而描述的读取器装置（1600）生成。外层的接口允许调用应用将要验证的动态认证凭证与和应该已提交动态凭证的用户的身份或者应该已生成动态凭证的读取器的标识符有关的值一起传递，并且可选地，还允许传递一个或更多个外部动态变量例如询问或业务数据。外层包括使用所接收的用户身份相关值或读取器标识符来确定或检索私人密钥相关输入参数的值的一个或更多个部件。确定或检索私人密钥相关输入参数的值可以包括使用所接收的用户身份相关值或读取器标识符（或者与读取器标识符相关的数据）作为搜索密钥来进行数据库搜索。为了验证所接收的动态凭证，在内层传递所接收的动态凭证时，外层调用所接收的要验证的动态凭证和私人密钥相关输入参数的被分配至内层期望的第一外部动态变量的获得值。如果可应用，则外层还将另外的外部动态变量（例如，询问或业务数据）的值传递至内层。在一些实施例中，即，在内层期望通过接口传递对称秘密密钥的值的情况下，外层包括使用其从调用应用接收的与用户身份或读取器标识符有关的数据元素来确定对称秘密密钥的值的一个或更多个部件。确定对称密钥的值可以包括将所接收的与用户身份或读取器标识符有关的数据元素用作搜索密钥来进行数据库搜索。在其他实施例中，外层将内层确定一个或更多个对称秘密密钥的值可以使用的与用户身份或读取器标识符有关的数据元素传递至内层。

在一些实施例中，除了使用其他数据元素（对称读取器密钥、PKRIP、动态变量）之外，还可以使用用户身份码（参见以下详细描述）来生成动态凭证。为了验证所接收的动态凭证，服务器侧的认证部件还确定用户身份码值并且然后在验证计算中使用该值。在一个实施例中，外层确定用户身份码并且将其作为内层期望的外部动态变量值传递至内层（与以上针对私人密钥相关输入参数的描述相似）。

在这种方式下，可以通过将用于验证动态凭证的没有被设计成实现本文中所公开的本发明的实施例的一个或更多个现有部件用作内芯并且仅添加包括根据本文中所公开的发明的实施例的一个或更多个部件的外层来产生本发明的实施例。

数据元素

用户 ID

在一组典型的实施例中，用户与应用或计算机系统进行交互并且借助于用户 ID 将其自身标识到应用或计算机系统。在优选的实施例中，该用户 ID 包括唯一地识别每个单独的用户的代码。在一些情况下，用户 ID 可以包括与用户关联的名称。在其他情况下，用户 ID

可以包括账号。在一些情况下，用户 ID 可以包括号码，而在其他情况下，用户 ID 可以包括字母串。在一些实施例中，用户 ID 可以由应用提供者选定，而在其他实施例中，用户 ID 可以由用户选定。

私人密钥代码和私人密钥相关输入参数

私人密钥相关输入参数(PKRIP，Private Key Related Input Parameter)为由读取器装置 1600 用于生成动态认证凭证以及由服务器侧用于验证由读取器装置生成的认证凭证的数据元素。私人密钥代码为在登记时最初生成并且由读取器装置 1600 使能并传送至服务器侧并且服务器侧可以根据其来计算 PKRIP 的数据元素。私人密钥代码和 PKRIP 均为来自用户的PKI装置的用户私人密钥的数学函数。读取器1600根据密码在数学上导出PKRIP，该密码由用户的 PKI 装置 1500 响应于来自读取器装置的询问（另外也称为 PKRIP 询问）使用非对称密码操作利用用户的私人密钥而生成。例如，可以由用户的 PKI 装置响应于来自读取器装置 1600 的询问使用用户的私人密钥和非对称密码算法根据非对称密码操作的结果例如加密或签名在数学上导出 PKRIP。在一些实施例中，导出可以包括散列和 / 或截取操作。在其他实施例中，导出还可以包括将秘密与和私人密钥数学上有关的数据——或者具体地，由用户的 PKI 装置响应于来自读取器装置的询问使用非对称密码操作利用用户的私人密钥得到的解密或签名的结果——以密码的形式进行组合。在又一些实施例中，导出还可以包括将其他类型的数据与和私人密钥数学上有关的数据——或者更具体地，由用户的 PKI 装置响应于来自读取器装置的询问使用非对称密码操作利用用户的私人密钥得到的解密或签名的结果——进行组合。在一些实施例中，这些其他类型的数据可以包括读取器装置专用的数据例如读取器装置序列号或者用户专用的数据例如在一些实施例中可以由用户提供给读取器装置的用户名称或者用户标识符，或者 PKI 装置专用的数据例如序列号，或者私人密钥专用的数据例如来自与私人密钥相关联的公共密钥或证书或者和与私人密钥相关联的公共密钥或证书有关的数据，或者在一些实施例中可以由用户提供给读取器装置的应用提供者专用的数据。用于导出 PKRIP 的算法可以使用以下额外数据元素：

1. 针对特定批次的所有的读取器装置相同的固定值。

2. 针对给定读取器装置固定但是针对每个读取器具有不同值的固定值。

3. 针对给定用户是恒定的、但是针对不同用户可以不同并且被用户输入读取器装置至少一次的固定值。

4. 存储在 PKI 装置上的可以由读取器装置读取的静态数据（例如，与私人密钥关联的数据，例如公共密钥和证书，或者 PKI 装置的序列号）。

5. 以上数据元素中的任何数据元素的组合。

在典型的实施例中，PKRIP 询问为由读取器装置以如下方式确定或计算的值：读取器装置随后可以针对相同的 PKI 装置或者 PKI 装置上的相同的私人密钥重新确定或重新计算 PKRIP 询问的相同的值。在典型的实施例中，PKRIP 询问包括秘密或者不可预测值。在一些实施例中，PKRIP 询问为常数或者根据存储在读取器装置中的常数导出。在特定实施例中，该常数对于多个读取器装置而言相同。在另一特定实施例中，该常数是单独的读取器装置专用的。在一些典型的实施例中，该常数是秘密。在其他实施例中，PKRIP 询问为随机或伪随机值或者根据随机或伪随机值导出。在一些实施例中，在生成 PKRIP 询问之后，读取器装置将允许重新确定或重新计算 PKRIP 询问的值存储在持久性存储器中以供随后使用。在

一个实施例中，该存储的值可以为PKRIP询问本身。在一些实施例中，该值与和PKI装置或PKI装置上的私人密钥有关的允许读取器装置识别PKI装置或PKI装置上的私人密钥的信息一起存储。该信息可以包括PKI装置的序列号或者来自PKI装置上的私人密钥或与PKI装置上的私人密钥有关的数据。在一些实施例中，PKRIP询问例如包括以下中任何一个或者可以根据以下中任何一个导出：

1. 针对特定批次的所有的读取器装置相同的固定值。

2. 针对给定读取器装置固定但是针对每个读取器具有不同值的固定值。

3. 针对给定用户是恒定的、但是针对不同用户可以不同并且被用户输入读取器装置至少一次的固定值。实际中，很可能，或者在每次使用PKI装置时输入该值，或者仅在首次使用给定PKI装置时使用读取器装置输入该值，并且然后由读取器装置记录该值。

4. 存储在PKI装置上的可以由读取器装置读取的静态数据（例如，公共密钥或证书，或者PKI装置序列号）。

5. 在一些实施例中可以由用户提供给读取器装置的特定应用提供者专用的数据。

6. 以上中的任何的组合。

7. 根据以上中的任何一个导出的值。该导出可选地包括使用一些读取器装置秘密。

私人密钥代码由读取器装置生成并且与PKRIP在数学上相关。在典型的实施例中，生成私人密钥代码，使得服务器侧可以根据私人密钥代码值来计算PKRIP的值。在一些实施例中，服务器侧还使用服务器侧对其具有访问权的另外的数据元素以根据私人密钥代码值来计算PKRIP。在一些实施例中，这些另外的数据元素可以包括读取器装置已知的秘密数据或者与可访问服务器侧的用户有关的数据例如用户名称或用户ID，或者与读取器装置有关并且服务器侧可访问的数据例如读取器装置序列号（在一些实施例中，读取器装置序列号可以由用户在登记时提供给服务器侧），或者与PKI装置有关的数据例如序列号，或者与在服务器侧可访问的PKI装置上存储的私人密钥有关的数据（在一些实施例中，这可以包括例如数据库中的来自与私人密钥相关联的公共密钥或证书或者和与私人密钥相关联的公共密钥或证书相关并且服务器侧可访问的数据）。在一些实施例中，私人密钥代码为在生成PKRIP时由读取器装置生成的中间数据元素。在其他实施例中，读取器装置在其已经生成PKRIP之后根据PKRIP在数学上导出私人密钥代码。在特定实施例中，私人密钥代码与PKRIP相同。在典型实施例中，私人密钥代码由读取器生成并且在登记时被传输至服务器侧以使得服务器侧能够计算或获得读取器装置已经计算的PKRIP的值。

激活密钥或激活代码

激活密钥(Activation Key)为在一些实施例中在登记和使能用户的PKI装置时使用的对称密钥，或者更具体地，存储在PKI装置上的用于生成PKRIP的私人密钥。在典型实施例中，激活密钥在登记时用于确保将由读取器装置生成的私人密钥代码传输至服务器侧。在一个实施例中，激活密钥对读取器装置是已知的或者由读取器装置在登记时计算。在一个实施例中，激活密钥由读取器装置用于对私人密钥代码进行加密，然后私人密钥代码以加密的形式从读取器装置被传输至服务器侧。在一个实施例中，激活密钥对服务器侧也是已知的或者由服务器侧在登记时计算。在一个实施例中，服务器侧接收加密的私人密钥代码并且使用其激活密钥的副本对加密的私人密钥代码进行解密。

在一些实施例中，根据读取器装置和服务器侧二者均已知的对称秘密来导出激活密

钥。在一个实施例中，激活密钥为读取器装置和服务器侧二者均已知的对称秘密。在另一特定实施例中，根据动态变量例如时间相关变量或询问与对称秘密的密码组合来导出激活密钥。

在一些实施例中，根据在对用户分配读取器装置之前已经存在于读取器装置中的对称秘密来导出激活密钥。在一个实施例中，激活密钥为在对用户分配读取器装置之前已经存在于读取器装置中的对称密钥。在特定实施例中，激活密钥作为产生步骤的一部分被加载至读取器装置中并且在对用户的PKI装置或者更具体地被存储在该PKI装置中的用于生成PKRIP的私人密钥进行登记之前被传输至服务器侧。

在一些实施例中，根据在服务器侧生成并且在生成之后被提供至读取器装置的数据元素来导出激活密钥。该数据元素还称为激活代码。在典型实施例中，激活代码被用户提供至读取器装置。在一些实施例中，用户可以在读取器装置的键盘上输入激活代码。在一些实施例中，用户经由被认为提供足够高的安全等级的传递信道来接收激活代码。在一个实施例中，当用户使用较老的认证技术（例如，使用静态口令）登录时，将激活代码传递至用户。在另一实施例中，激活代码通过邮件（例如，挂号邮件）被发送至用户。在又一实施例中，用户例如在已经插入银行卡并且已经输入与银行卡关联的PIN之后可以经由ATM（自动取款机）机获得激活代码。在再一实施例中，激活代码经由文本信息或SMS（短信服务）消息被发送至被认为在用户的控制下的移动电话。在再一实施例中，激活代码经由电子邮件被发送至被认为在用户的控制下的电子邮件账户。

在一些实施例中，激活密钥的导出使用读取器装置专用的数据元素例如读取器装置序列号或者用户专用的数据元素例如在一些实施例中可以由用户提供给读取器装置的用户名称或用户标识符。

用户身份代码

在一些实施例中，用户身份代码为下述数据元素：读取器装置可以从存储在PKI装置上的数据元素导出、并且读取器装置可以访问、并且表示或者链接至PKI装置的合法持有者的身份、并且还可以在给定PKI装置的合法持有者的身份的情况下服务器侧例如通过访问公共数据库可访问的数据元素。这样的数据元素的示例可以包括PKI装置持有者的名称或者PKI装置持有者的地址或者（例如，在PKI装置包括全国ID卡的情况下）对于每个PKI装置持有者唯一的PKI装置持有者的全国号码，或者（例如，在PKI装置由金融机制发布的情况下）PKI装置持有者的账户。在一些实施例中，该数据元素可以包括在与PKI装置持有者的在PKI装置上的私人密钥相关联的证书中。在一些其他实施例中，服务器侧可以具有对包括与用户的私人密钥相关联的证书或公共密钥的数据库的访问权。然后，根据其导出用户身份代码的数据元素可以包括与PKI装置上的用户私人密钥相关联的证书或公共密钥的一部分。用户身份代码可以使得服务器能够检查用户声称的身份与用户正在使用的PKI装置的合法持有者的身份是否一致。

在一个实施例中，用户身份代码由读取器装置在登记阶段根据用户正在使用的PKI装置上的数据元素导出，并且然后被传输至服务器侧。为了验证用户声称的身份与用户正在使用的PKI装置的合法持有者的身份对应，服务器侧可以根据与PKI装置上的数据元素对应的数据元素来生成相似的值，服务器侧可访问该值并且可以基于用户声称的身份来检索该值。然后，服务器侧可以将所接收的身份代码与其自身计算的值进行比较。如果用户所

声称的身份对应于用户正在使用的 PKI 装置的合法持有者的身份，则然后该比较应当给出肯定的结果。

在另一实施例中，用户身份代码由读取器装置在生成动态凭证时导出并且与其他数据元素（对称读取器密钥、PKRIP、动态变量）以密码的形式进行组合，从而生成动态凭证。当验证动态凭证时，服务器侧基于用户声称具有的身份来确定用户身份代码的值。如果用户声称具有的身份不同于用户正在使用的 PKI 装置的合法持有者的身份，则由读取器装置导出的用户身份代码与由服务器侧确定的用户身份代码将会不同，并且可以预期服务器侧对动态凭证的验证会产生否定的结果。这提供了服务器侧用于验证用户声称的身份对应于用户正在使用的 PKI 装置的合法持有者的身份的隐式方法。

方法

确保应用

在一些实施例中，图 19 所图示的用于确保用户访问基于计算机的应用和 / 或与基于计算机的应用交互的方法可以包括以下步骤：

•针对多个用户确保每个用户具有对链接至用户的 PKI 装置的访问权 (1905)；所述 PKI 装置存储私人密钥并且适于使用该私人密钥进行非对称密码操作，并且所述 PKI 装置具有用于与兼容读取器装置进行电子通信并且与兼容读取器装置交换数据的通信接口，与兼容读取器装置进行电子通信和与兼容读取器装置交换数据包括：从这样的读取器装置接收数据、从读取器装置接收指令以使用存储在 PKI 装置上的非对称私人密钥对由读取器装置提供的特定数据进行非对称密码操作；以及返回该非对称密码操作的结果。在一些实施例中，PKI 装置可以包括智能卡或 USB 令牌。在一些实施例中，例如在可以默认假设用户具有可用的 PKI 装置的情况下，该步骤可以是可选的或隐含的。例如，这可以是在所有公民获得具有 PKI 功能的全国 ID 卡的国家中的情况。在其他实施例中，例如，在金融机构发布 PKI 装置的情况下，该步骤可以包括确保针对每个用户在 PKI 装置上生成并且存储公共 - 私人密钥对，该密钥对的公共密钥被认证并且链接至合适的用户，PKI 装置被提供至合适的用户，并且（可选地）PIN 邮包被发送至合适的用户。

• 针对多个用户确保每个用户获得如上所述的读取器装置 (1908)；所述读取器装置适于处理激活密钥和激活代码并且适于生成如以上和以下所述的私人密钥代码、私人密钥相关输入参数和动态认证凭证。

•针对多个用户中的每个用户在与每个用户相关联的 PKI 装置上登记 (1910) 私人密钥（参见以下对登记步骤的描述）。

• 从多个用户接收 (1915) 由这些用户使用其 PKI 装置和读取器装置生成的动态凭证（参见以下对动态凭证的生成的描述）。

• 验证 (1925) 所接收的动态凭证（参见以下对动态凭证的验证的描述）。

• 根据验证步骤的结果采取合适的动作。例如，在一些实施例中，用户可以在成功验证 OTP(1935) 之后获得对应用的访问权并且在对 OTP 的验证不成功的 (1945) 的情况下被拒绝访问。在其他实施例中，由用户接收指令或业务可以在成功验证在指令和业务上的 OTP 或电子签名之后被执行，或者在对 OTP 或电子签名的验证不成功的情况下被拒绝。

在一些实施例中，要确保的应用包括金融应用例如网络银行应用。在其他实施例中，要确保的应用包括电子政务例如电子提交税收声明。在另一些实施例中，要确保的应用包括

社会保险或健康护理相关应用例如与医疗保险的交互。在另一些实施例中，要确保的应用包括彩票应用。

私人密钥的登记 / 使能

如图 20A 和图 20B 所图示，在典型实施例中，在用户的 PKI 装置上登记用户的私人密钥的步骤包括以下步骤：

• 在一些实施例中，将激活代码提供至用户 (2005)。

• 用户采用他 / 她的读取器装置和 PKI 装置并且使它们进行以下步骤。

• 读取器装置获得 PKRIP 和私人密钥代码，这又包括以下步骤：

i. 生成如上所述的 PKRIP 询问 (2006)。

ii. 将 PKRIP 询问发送至 PKI 装置并且命令 PKI 装置使用存储在 PKI 装置中的私人密钥对该 PKRIP 询问进行非对称密码操作并且从 PKI 装置接收该操作的结果 (2009)。

iii. 根据该操作的结果导出称为私人密钥代码的第一值以及（可选地）称为 PKRIP 的第二值 (2010)。

• 读取器装置获得激活密钥并且使用所获得的激活密钥对生成的私人密钥代码进行加密 (2011)。在一些实施例中，读取器装置首先获得激活代码并且根据所获得的激活代码导出激活密钥。在典型的实施例中，用户（例如，通过在读取器装置的键盘上输入激活代码）将激活代码提供至读取器装置。在另一典型的实施例中，激活代码为激活密钥的表示。

• 在一些实施例中，读取器装置还从 PKI 装置获得链接至用户的身份的并且还可以由服务器侧获得的数据元素，并且根据该数据元产生用户身份代码。

• 在一些实施例中，读取器装置还使用 PKRIP 生成动态凭证。

• 加密的私人密钥代码并且如果适用，用户的标识代码和 / 或所生成的动态凭证也被传输至服务器侧 (2014)。在一些实施例中，使得服务器侧识别用户的读取器装置的值（例如，读取器装置的序列号）也被传输至服务器侧。在典型的实施例中，从读取器装置向服务器侧传输这些数据元由用户例如通过从读取器装置的显示器读取这些数据元素并且将这些数据元素复制在服务器侧的网页上来完成。

• 服务器侧接收加密的私人密钥代码，并且如果适用，接收用户身份代码和 / 或所生成的动态凭证和 / 或读取器装置识别的数据元素 (2016)。

•服务器侧还获得激活密钥的副本。在一些实施例中，服务器侧获得已经被提供至用户的激活代码的副本并且根据该激活代码的副本导出激活密钥。在其他一些实施例中，服务器侧从数据库获得可以根据其导出激活密钥的值。在一些实施例中，服务器侧从数据库获得激活密钥自身的值。

• 服务器侧对所接收的加密私人密钥代码进行解密 (2018)。

•服务器侧根据私人密钥代码来导出允许服务器侧计算对应的 PKRIP 的值 (2019) 并且将链接至用户的那个值存储在例如数据库中 (2020)。在一些实施例中，该值可以为私人密钥代码。在其他实施例中，该值可以为 PKRIP 本身。

• 如果适用，服务器侧使用读取器装置识别元素来检索在由服务器侧计算或验证由读取器装置所生成的数据元素时所使用的读取器装置专用数据元（例如，读取器装置专用配置参数或密钥）。由读取器装置生成并且还由服务器侧计算或验证的数据元素可以包括由读取器装置生成的激活密钥、PKRIP、用户身份代码和 / 或任何动态凭证（例如，OTP 或电子

签名）。如果适用，服务器侧可以存储链接至用户的读取器装置识别元以供以后使用。在典型实施例中，读取器装置在生成动态凭证时使用一个或更多个读取器装置专用秘密，并且服务器侧将读取器装置识别元素存储在链接至用户的数据库中并且在验证由用户提供的动态凭证时使用所存储的读取器装置识别元素来从另一数据库（存储链接至读取器装置识别元的一个或更多个读取器装置专用密钥）检索一个或更多个读取器装置专用秘密。

• 如果适用，则服务器侧可以导出其自己的用户身份代码副本并且将其与所接收的用户身份代码进行比较。在一些实施例中，如果该比较失败，则登记失败或被拒绝。

• 如果适用，则服务器侧可以验证所接收的动态凭证。在一些实施例中，如果该验证失败，则登记失败或被拒绝。

动态凭证的生成

在典型实施例中，根据图 21 所图示的方法，读取器装置生成动态凭证 (2120)，该方法包括以下步骤：

• 读取器装置获得 PKRIP(2110)。

• 读取器装置使用对称密码算法将该 PKRIP 与一个或更多个动态变量以密码的形式进行组合 (2115)。

• 在一些实施例中，该组合还涉及一个或更多个对称读取器秘密。

• 在一些实施例中，该组合还涉及用户身份代码。

在一些实施例中，获得 PKRIP 包括：生成 PKRIP 询问；将该 PKRIP 询问发送至 PKI 装置；命令 PKI 装置使用存储在 PKI 装置上的私人密钥对 PKRIP 询问进行非对称密码操作；从 PKI 装置接收该非对称操作的结果；以及根据所接收的非对称操作的结果在数学上导出 PKRIP。在一些实施例中，所述非对称操作包括使用存储在 PKI 装置上的私人密钥生成数字签名并且非对称操作的所述结果包括得到的数字签名。在一些实施例中，根据所接收的非对称操作的结果导出 PKRIP 包括将非对称操作的结果与存储在读取器装置中的数据进行组合。在一些实施例中，存储在读取器装置中的这些数据可以包括单独的读取器装置专用的数据。在其他实施例中，存储在读取器装置中的这些数据可以包括一个或更多个秘密值或密钥。

在一些实施例中，使用对称密码算法将 PKRIP 与一个或更多个动态变量以密码的形式进行组合包括使用对称密码算法将 PKRIP 和一个或更多个动态变量与存储在读取器装置中的一个或更多个秘密值进行组合。在一些实施例中，这些一个或更多个秘密值包括多个读取器装置共用的秘密值。在其他一些实施例中，这些一个或更多个秘密值包括单独的读取器装置专用的秘密值。

在一些实施例中，读取器装置可以导出如上所述的用户身份代码，并且使用对称密码算法将 PKRIP 与一个或更多个动态变量以密码的形式进行组合包括将 PKRIP 和一个或更多个动态变量与所导出的用户身份代码进行组合。在一些实施例中，使用对称密码算法将 PKRIP 与一个或更多个动态变量以密码的形式进行组合包括使用对称密码算法将 PKRIP 和一个或更多个动态变量和所导出的用户身份代码与存储在读取器装置中的一个或更多个秘密值进行组合。

在特定实施例中，使用对称密码算法将 PKRIP 与一个或更多个动态变量以密码的形式进行组合包括将已知的或标准对称算法应用于存储在读取器装置中的 PKRIP、一个或更多

个动态变量以及一个或更多个对称秘密值，从而产生将对称秘密与第一外部动态变量和至少第二内部或外部动态变量进行组合的 OTP 或电子签名，从而读取器装置将私人密钥相关输入参数的值分配至第一外部动态变量，将存储在读取器装置中的对称秘密值分配至对称秘密并且将一个或更多个动态变量分配至至少第二内部或外部动态变量。

动态证书的验证

在典型实施例中，根据图 22 所图示的方法在服务器侧验证已经接收的动态证书 (2220)，该方法包括以下步骤：

• 服务器侧获得 PKRIP(2205)。

• 服务器侧使用对称密码算法将该 PKRIP 与一个或更多个动态变量以密码的形式进行组合，从而获得参考值 (2210)。

• 服务器侧将参考值与所接收的动态证书进行比较 (2215)。

在一些实施例中，获得 PKRIP 包括从数据库中检索链接至用户并且允许服务器侧计算对应的 PKRIP 的数据元素。在一些实施例中，该值可以为私人密钥代码。在其他实施例中，该值可以为 PKRIP 本身。在一些实施例中，服务器侧将该数据元素与其他数据元进行组合。在一些实施例中，这些其他数据元素可以包括可以链接至读取器或者链接至用户从而计算 PKRIP 的数据元素。在一些实施例中，这些其他数据元素可以包括一个或更多个秘密密钥。

在一些实施例中，使用对称密码算法将 PKRIP 与一个或更多个动态变量以密码的形式进行组合包括使用对称密码算法将 PKRIP 和一个或更多个动态变量与存储在读取器装置中的一个或更多个秘密值的服务器侧副本进行组合。在一些实施例中，这些一个或更多个秘密值包括多个读取器装置共用的秘密值。在其他一些实施例中，这些一个或更多个秘密值包括单独的读取器装置专用的秘密值。在一些实施例中，服务器侧从存储链接至用户识别数据元素或链接至读取器装置识别数据元素的这些值的数据库中检索一个或更多个秘密值。

在特定实施例中，使用对称密码算法将 PKRIP 与一个或更多个动态变量以密码的形式进行组合包括将已知或标准的对称算法应用于 PKRIP、一个或更多个动态变量以及存储在读取器装置中的对称秘密值的服务器侧副本，从而生成将对称秘密与第一外部动态变量和至少第二内部或外部动态变量进行组合的 OTP 或电子签名，从而服务器侧将私人密钥相关输入参数的值分配至第一外部动态变量，并且将存储在读取器装置中的对称秘密值分配至对称秘密，并且将一个或更多个动态变量中的一个分配至至少第二内部或外部动态变量。

在特定实施例中，读取器装置可用于多个用户。读取器装置可以由应用提供者例如通过邮件分配至其用户中的一些用户。读取器装置还可以用于在例如超市或网络商店中进行出售。读取器装置适于与 PKI 装置例如智能卡进行交互，智能卡由政府机构发放给公民以用作这些公民的电子 id 卡并且智能卡包括私人密钥和相关联的证书并且能够使用私人密钥进行非对称密码操作从而例如生成数字签名或者使用与私人密钥相关联的公共密钥对加密的数据进行解密。所有的读取器包括对于所有读取器相同的特定询问。所有的读取器装置还包括对于所有读取器装置相同的对称读取器秘密。应用提供者还例如通过使用挂号邮件以安全的方式将个人激活代码提供给用户。激活代码可以包括十进制数字序列。每个激活代码的值对于每个用户而言是秘密的并且是个性化的。激活代码被确定成使得外人难以预测该值。激活代码可以例如为随机数字或者通过将加密密钥与用户 ID 以密码的形式

进行组合来导出。为了检测印刷错误，激活代码可以具有校验数字。应用提供者保持跟踪哪个用户已经接收到哪个激活代码。

应用提供者邀请用户以对用户进行登记。为了登记，用户登陆并且使用现有认证机制例如使用静态口令与他 / 她的用户 ID 组合来进行验证。然后，用户将他或她的 PKI 装置（例如，其电子 ID 卡）插入至他或她的读取器装置并且在读取器装置上输入他或她的激活代码。读取器装置请求用户插入他 / 她的 PKI 装置并且向 PKI 装置输入 PIN。读取器装置将 PIN 提交至 PKI 装置以用于验证。读取器装置然后命令 PKI 装置使用存储在用户的 PKI 装置中的用户的私人密钥对上述询问进行数字签名。读取器装置接收得到的数字签名并且根据数字签名导出 PKRIP，例如，可以采用数字签名中出现的非对称密码的前五个字节并且将这五个字节转换成其十进制表示。读取器然后通过对每个 PKRIP 数字与由用户输入的激活代码中的对应的数字进行以 10 为模 (modulo-10) 相加来对 PKRIP 进行加密。读取器将因此加密的 PKRIP 显示在其显示器上并且用户将所显示的加密的 PKRIP 传输至登记应用（例如，通过将加密的 PKRIP 复制到在用户的网络浏览器中的登记应用的网页上）。应用提供者检索提供至特定用户的激活代码并且使用激活代码来对所接收的正在使用的加密的 PKRIP 进行解密。应用提供者然后（例如，在数据库中）存储链接至用户的用户 ID 的 PKRIP。

从现在开始，当用户想要访问应用提供者的应用时，用户被请求通过提供他 / 她的用户 ID 以及由他 / 她的读取器装置连同他 / 她的 PKI 装置生成的 OTP 来进行登录。读取器装置如以下那样生成 OTP。读取器装置请求用户插入他 / 她的 PKI 装置并且输入 PKI 装置 PIN。读取器装置将 PIN 提交至 PKI 装置以用于验证。然后，读取器装置将上述询问提交至 PKI 装置并且命令 PKI 装置使用存储在 PKI 装置上的用户私人密钥对该询问进行数字签名。读取器装置接收所得到的数字签名并且根据该数字签名导出与针对登记阶段导出的 PKRIP 相同的 PKRIP。读取器通过使用对称密码算法将 PKRIP 与动态变量（例如，读取器装置的实时时钟或者由读取器装置保持的计数器的值）和上述对称读取器秘密以密码的形式进行组合来生成 OTP。读取器装置可以例如将 PKRIP 和动态变量进行组合，并且例如使用对称读取器秘密作为 AES 加密密钥来使用 AES 加密算法对该组合进行加密，此后，读取器可以对所得到的密码的一部分（例如前三个字节）进行十进制换算，并且将结果作为 OTP 显示在读取器的显示器上以用于用户传输至应用。在一个实施例中，读取器装置可以将 PKRIP 值馈送至 OTP 生成算法，OTP 生成算法采取至少两个动态变量，两个动态变量中至少之一最初被认为是外部动态变量（例如，询问）并且读取器装置为所述至少两个动态变量分配 PKRIP 值。例如，读取器装置可以使用利用两个动态变量的 OTP 算法 :第一内部基于时间的动态变量和最初认为被分配了由应用生成的询问值的第二外部动态变量，从而读取器装置将 PKRIP 值分配至第二动态变量。

应用的认证部件如以下那样验证所接收的 OTP。认证部件将用户 ID 用作搜索密钥来检索与用户关联的 PKRIP 值。认证部件确定对称读取器秘密的值。认证部件确定在生成所接收的 OTP 时所使用的动态变量的值。然后，认证部件使用与由读取器装置使用的算法相似的对称密码算法将所检索的 PKRIP 值和确定的动态变量的值与确定的对称读取器秘密以密码的形式进行组合。然后，将该密码组合的结果与所接收的 OTP 进行比较。认证部件例如可以将所接收的 PKRIP 值和所确定的动态变量的值进行组合，并且使用对称读取器秘密作为 AES 加密密钥来使用 AES 加密算法对该组合进行加密，此后，可以对所得到的密码的

一部分（例如，前三个字节）进行十进制换算，并且检查结果与所接收的 OTP 是否相同。在一个实施例中，认证部件包括两层。第一层为内层，该内层能够验证使用对称秘密、第一动态变量以及最初认为是外部动态变量例如询问的第二动态变量生成的 OTP。内层具有期待要验证的 OTP、密钥以及外部动态变量值的接口。第二层为外层，该外层由应用调用以验证所接收的 OTP。外层包括对称读取器秘密并且基于从调用应用接收的用户 ID 来确定用户的 PKRIP 值。为了验证 OTP，外层调用内层并且传递 OTP 和对称读取器秘密，并且传递作为第二外部动态变量的值的 PKRIP 值。内层验证 OTP 并且将结果返回至外层，外层将结果返回至应用。

本实施例的一个优点在于，用户可以使用任何的读取器装置并且甚至可以在任何时刻从一个读取器装置改变至另一读取器装置。

在另一特定实施例中，读取器装置可用于多个用户。读取器装置可以由应用提供者例如通过邮件分配至其用户中的一些用户。读取器装置还可以用于在例如超市或网络商店中进行出售。读取器装置适于与 PKI 装置例如智能卡进行交互，智能卡由政府机构发放给公民以用作这些公民的电子 id 卡并且智能卡包括私人密钥和相关联的证书并且能够使用私人密钥进行非对称密码操作从而例如生成数字签名或者使用与私人密钥相关联的公共密钥对加密的数据进行解密。所有的读取器装置包括对于每个读取器装置唯一的特定询问。所有的读取器装置还包括对于每个读取器装置唯一的对称读取器秘密。所有的读取器装置还具有对于每个读取器装置唯一的秘密激活密钥。

应用提供者邀请用户以对用户进行登记。为了登记，用户登陆并且使用现有认证机制例如使用静态口令与他 / 她的用户 ID 组合来进行验证。然后，用户将他或她的 PKI 装置（例如，其电子 ID 卡）插入至他或她的读取器装置并且在读取器装置上输入他或她的激活代码。读取器装置请求用户插入他 / 她的 PKI 装置并且向 PKI 装置输入 PIN。读取器装置将 PIN 提交至 PKI 装置以用于验证。读取器装置然后命令 PKI 装置使用存储在用户的 PKI 装置中的用户的私人密钥对其读取器装置询问进行数字签名。读取器装置接收得到的数字签名并且根据数字签名导出 PKRIP，例如，可以采用数字签名中出现的非对称密码的前五个字节并且将这五个字节转换成器十进制表示。读取器然后通过对每个 PKRIP 数字与在读取器装置的激活密钥中的对应的数字进行以 10 为模相加来对 PKRIP 进行加密。读取器将因此加密的 PKRIP 显示在其显示器上并且用户将所显示的加密的 PKRIP 传输至登记应用（例如，通过将加密的 PKRIP 复制到在用户的网络浏览器中的登记应用的网页上）。用户还将他或她正在使用的读取器装置的序列号传输至应用。

应用提供者具有列出链接至对应的读取器装置的序列号的读取器装置专用对称读取器秘密和认证密钥的数据库。应用检索用户使用的读取器装置的激活密钥并且将该激活密钥用于对所接收的加密的 PKRIP 进行解密。然后，应用提供者（例如，在数据库中）存储 PKRIP 和链接至用户的用户 ID 的读取器装置的序列号。

从现在开始，当用户想要访问应用提供者的应用时，用户被请求通过提供他 / 她的用户 ID 以及由他 / 她的读取器装置连同他 / 她的 PKI 装置生成的 OTP 来进行登录。读取器装置如以下那样生成 OTP。读取器装置请求用户插入他 / 她的 PKI 装置并且向 PKI 装置输入 PIN。读取器装置将 PIN 提交至 PKI 装置以用于验证。然后，读取器装置将其读取器装置专用询问提交至 PKI 装置并且命令 PKI 装置使用在 PKI 装置上存储的用户私人密钥对该询

问进行数字签名。读取器装置接收所得到的数字签名并且根据数字签名导出与登记阶段导出的 PKRIP 相同的 PKRIP。读取器通过使用对称密码算法将 PKRIP 与动态变量（例如，读取器装置的实时时钟或者由读取器装置保持的计数器的值）和其读取器装置专用对称读取器秘密以密码的形式进行组合来生成 OTP。读取器装置可以例如将 PKRIP 和动态变量进行组合并且例如使用读取器装置专用对称读取器秘密作为 AES 加密密钥使用 AES 加密算法来对该组合进行加密，此后，读取器可以对所得到的密码的一部分（例如前三个字节）进行十进制换算，并且将结果作为 OTP 显示在其显示器上以用于用户传输至应用。在一个实施例中，读取器装置可以将 PKRIP 值馈送至 OTP 生成算法，OTP 生成算法采取至少两个动态变量，两个动态变量中至少之一最初被认为是外部动态变量（例如，询问）并且读取器装置为所述至少两个动态变量分配 PKRIP 值。例如，读取器装置可以使用利用两个动态变量的 OTP 算法：第一内部基于时间的动态变量和最初认为被分配了由应用生成的询问值的第二外部动态变量，从而读取器装置将 PKRIP 值分配至第二动态变量。

应用的认证部件如以下那样验证所接收的 OTP。将用户 ID 用作搜索密钥，认证部件检索 PKRIP 值以及与用户关联的读取器装置的序列号。认证部件使用用户的读取器装置的序列号来确定读取器装置专用对称读取器秘密的值。认证部件确定在生成所接收的 OTP 时所使用的动态变量的值。然后，使用与由读取器装置使用的算法相似的对称密码算法将所检索的 PKRIP 值和确定的动态变量的值与确定的对称读取器秘密以密码的形式进行组合。然后，将该密码组合的结果与所接收的 OTP 进行比较。认证部件例如可以将所检索的 PKRIP 值和所确定的动态变量的值进行组合并且使用对称读取器秘密作为 AES 加密密钥使用 AES 加密算法来对该组合进行加密，此后，认证部件可以对所得到的密码的一部分（例如，前三个字节）进行十进制换算，并且检查该结果与所接收的 OTP 是否相同。在一个实施例中，认证部件包括两层。第一层为内层，该内层能够验证使用对称秘密、第一动态变量以及最初认为是外部动态变量例如询问的第二动态变量生成的 OTP。内层具有期待要验证的 OTP、密钥以及外部动态变量的值的接口。第二层为外层，该外层由应用调用以验证所接收的 OTP。外层包括对称读取器秘密并且基于从如上所述的调用应用接收的用户 ID 来确定用户的 PKRIP 值和读取器装置专用对称读取器秘密。为了验证 OTP，外层调用内层并且传递 OTP 和对称读取器秘密，并且传递作为第二外部动态变量的值的 PKRIP 值。内层验证 OTP 并且将结果返回至外层，外层将结果返回至应用。

本实施例的一个优点在于，由下述事实提供额外的安全性：为了生成有效的 OTP，不仅需要访问用户的 PKI 装置（以及用户的 PKI 装置的 PIN），还需要访问用户在登记阶段登记的读取器装置。

本发明的其他方面如以下所述。

在本发明的一些实施例中，如图 23 所图示，认证设备 (2310) 包括用于接收数据的数据输入接口 (2320)、用于交换数据的通信接口 (2330)、用于能够进行非对称密码计算的单独的可移除安全装置 (2390)（例如有 PKI 功能的智能卡）的命令和响应、一个或更多个数据处理部件 (2340)、一个或更多个存储器部件 (2345)、用于接收数据或指令或来自用户的其他输入的用户输入接口 (2350) 以及将数据（特别是 OTP 和 / 或 MAC) 或消息或其他输出提供给用户的用户输出接口 (2360)。

认证设备可以适于生成一次性口令 (OTP)，一次性口令可以包括消息认证代码 (MAC,

message authentication code)。因此,除非另有指示,否则术语 OTP 可以不仅在狭意上指示 OTP,而且还指示 MAC。认证设备可以适于通过将动态变量与认证设备和验证实体例如应用或认证服务器共享的秘密数据元素以密码的形式进行组合来生成一次性口令。在一些实施例中,认证设备可以适于通过使用由秘密数据元素参数化的对称密码算法将动态变量和秘密数据元素以加密的形式进行组合来生成一次性口令。在一些实施例中,对称密码算法可以包括对称密码算法例如 DES(数据加密标准,Data Encryption Standard)或者 AES(高级加密标准,Advanced Encryption Standard)。在一些实施例中,对称加密算法可以包括例如基于 SHA-1(安全散列算法 1)算法或 MD5(消息摘要 5)算法的密钥散列算法例如 HMAC(密钥散列消息认证代码)算法。用于生成 OTP(和 MAC)的共享的数据元素因此称为 OTP 密钥。OTP 密钥也可以称为 OTP 生成密钥,特别是在讨论使用 OTP 密钥(的值)生成 OTP 和/或 MAC 时。OTP 密钥可以可可选地称为 OTP 验证密钥,特别是在讨论使用 OTP 密钥(的值)来验证 OTP 或 MAC 的合法性时。OTP 和/或 MAC 也称为动态凭证并且 OTP 密钥也称为动态凭证生成密钥。在一些实施例中,动态变量可以包括询问值和/或计数值和/或时间值和/或业务数据或可以由认证设备根据询问值和/或计数值和/或时间值和/或业务数据来生成。在一些实施例中,认证设备可以通过用户输入接口接收来自用户的询问和/或业务数据。在一些实施例中,认证设备可以包括实时时钟以提供由认证设备生成基于时间的 OTP 的时间值。在一些实施例中,认证设备包括计数器以提供由认证设备生成基于计数器的 OTP 的计数值。在一些实施例中,认证设备通过用户输入接口向用户例如以例如可以显示在认证设备的显示器上或者可以被作为合成语音提供至用户的数字串或字母字符的形式提供所生成的 OTP。

在一些实施例中,用户输入接口包括键盘。在一些实施例中,用户输出接口包括显示器。

在一些实施例中,数据输入接口包括光学接口。在一些实施例中,数据输入接口包括用于(例如,从访问设备的计算机屏幕)获取照片的相机。在一些实施例中,认证设备适于在使用认证设备的相机获取的照片中检测以特定格式(例如,QR 代码或者二维条形码)对数据编码的二维图像。在一些实施例中,数据输入接口包括声音接口。在一些实施例中,数据输入接口包括 USB 接口。在一些实施例中,认证设备可以为尺寸适中重量适中紧凑便携式装置即最大长度为 15 厘米、最大宽度为 9 厘米、最大厚度为 2 厘米以及重量小于 200 克的装置。

在一些实施例中,单独的可移除安全装置可以为小型紧凑轻型便携式装置即在任何方向上的最大延伸为 10 厘米并且重量小于 100 克的装置。在一些实施例中,单独的可移除安全装置可以为智能卡。在一些实施例中,单独的可移除安全装置可以为 ISO/IEC 7810 ID-1 大小的智能卡。在一些实施例中,可移除安全装置可以为 USB(通用串行总线)密钥。

在一些实施例中,通信接口适于使得用户能够容易地移除或代替认证设备可以与其进行通信的单独的可移除安全装置。在一些实施例中,通信接口包括用于接受可移除安全装置并且与可移除安全装置进行通信的外部可访问槽。在一些实施例中,通信接口需要用户将用户的安全装置插入至用于与用户的安全装置进行通信的这样的外部可访问槽中。在一些实施例中,通信接口包括智能卡接口,并且单独的可移除安全装置包括智能卡。在一些实施例中,智能卡可以为具有 PKI 功能。在一些实施例中,通信接口包括外部可访问智能卡读

取器。在一些实施例中，通信接口可以适于接受 ISO/IEC 7810 ID-1 大小的智能卡。在一些实施例中，通信接口可以适于接受 ISO/IEC 7810 ID-3 大小的智能卡。在一些实施例中，通信接口可以适于与非接触智能卡进行通信。在一些实施例中，通信接口可以适于与接触式智能卡进行通信。在一些实施例中，通信接口可以与 ISO/IEC 规范兼容。

在一些实施例中，一个或更多个存储器部件可以适于永久地存储数据。在一些实施例中，一个或更多个存储器部件可以适于（安全地）存储密码秘密例如对称或非对称解密密钥。在一些实施例中，一个或更多个存储器部件可以适于存储软件和 / 或固件。在一些实施例中，一个或更多个存储器部件可以适于存储配置数据。在一些实施例中，一个或更多个存储器部件可以包括 RAM 和 / 或 ROM 存储器。

在一些实施例中，一个或更多个数据处理部件可以包括用于控制数据输入接口、通信接口、用户输入接口和 / 或用户输出接口的处理器和 / 或控制器。在一些实施例中，一个或更多个数据处理部件可以包括适于执行密码算法例如对称或非对称解密算法的处理部件。在一些实施例中，一个或更多个数据处理部件可以包括 ASIC 或 FPGA。

在一些实施例中，在认证设备被分配至用户时，认证设备（还）不包括与特定用户关联的 OTP 密钥。为了使得能够生成为了认证用户或者认证由用户提交的业务数据而要验证的 OTP（可以包括 MAC），认证设备需要将验证 OTP 的实体也知道的并且与用户关联的 OTP 密钥。

图 24 示出根据本发明的方面的用于使用认证设备和用户的安全装置来生成用于认证用户和 / 或业务的 OTP 和 / 或 MAC 的方法。

在步骤 2410 中，服务器部件可以确定数学上相关的 OTP 密钥的值（步骤 2411）和初始化种子（步骤 2412）的值。服务器可以将 OTP 密钥与特定用户进行关联 (2415)。可以使用非对称加密算法例如 RSA(Rivest-Shamir-Adleman) 算法使用公共 - 私人密钥对的公共密钥对初始化种子进行加密 (2420)，该公共私人密钥对的私人密钥存储在用户的安全装置上。加密的初始化种子可以被传输 (2425) 至用户的认证设备例如作为可以由认证设备接收的初始化消息的一部分。用户的认证设备然后可以将加密的初始化种子提交 (2430) 至用户的安全装置以进行解密，安全装置可以使用非对称解密算法例如 RSA 使用存储在安全装置上的用户的私人密钥对加密的初始化种子进行解密，并且安全装置可以将解密的初始化种子返回至认证设备。用户的认证设备然后可以使用解密的初始化种子导出 (2435) OTP 密钥的值。然后，用户的认证设备可以在如上所述生成 (2440)OTP 和 / 或 MAC 时使用 OTP 密钥值。在一些实施例中，认证设备借助于其用户输出接口将生成的 OTP 或 MAC 传输 (2445) 至用户。然后，所生成的 OTP 或 MAC 可以被传输至 (2450) 例如远程应用，以用于认证用户或至远程应用的用户业务。因此接收的 OTP 或 MAC 然后可以由验证服务器部件进行验证 (2460)。验证服务器部件可以访问与用户关联的 OTP 密钥的值并且可以在验证所接收的 OTP 或 MAC 时使用该 OTP 密钥。在成功验证 (2460)OTP 或 MAC 时，远程应用可以采取合适的动作 (2470) 例如准许访问用户或者接受由用户提交的业务。

OTP 密钥的初始化——服务器侧

在一些实施例中，确定 OTP 密钥的值和将 OTP 密钥值提供至认证设备可以如以下那样进行。初始化服务器可以针对给定用户确定 OTP 密钥的值以及与 OTP 密钥在数学上相关的至少一个初始化种子的值。服务器可以将用户与和初始化种子在数学上相关的 OTP 密钥进

行关联。将进一步描述 OTP 密钥和初始化种子与用户如何相关和关联的细节。假设用户具有包括公共 - 私人密钥对中的私人密钥的安全装置，该安全装置适于使用由前述私人密钥参数化的非对称密码算法对使用由前述公共 - 私人密钥对的公共密钥参数化的对应的非对称密码算法加密的数据进行解密。服务器可以获得与用户关联的公共 - 私人密钥对的公共密钥。例如，服务器可以针对多个用户从包括多个公共密钥的数据库中检索公共密钥。该步骤可能需要用户提供识别用户的数据元素，例如，用户 id 或者用户名称或用户的国家 id 号或者用户的社会保险号或者用户的安全装置的序列号。例如，在一个实施例中，多个公民可以具有包括公共 - 私人密钥对的电子国家 id 卡，并且服务器可以访问包括与公民关联的公共密钥的中心登记并且可以使用国家 id 号的用户名称来检索与特定用户关联的公共密钥。服务器收集至少包括初始化种子的初始化消息。服务器使用由与用户关联的公共密钥参数化的非对称密码算法对初始化消息的至少一部分进行加密，从而初始化消息的加密的部分包括初始化种子的至少一部分。

初始化消息还可以包括其他数据元素例如一个或更多个随机数 (nonce)，或者初始化种子的未使用与用户关联的公共密钥进行加密的部分，或者识别用户或用户的安全装置或与用户关联的公共密钥的数据，或者识别用户的认证设备的数据。在一些实施例中，初始化消息的一部分可以使用与用户的认证设备关联的认证设备密钥来进行加密。在一些实施例中，该认证设备密钥为与认证设备已知的私人密钥对应的公共密钥。在一些实施例中，该认证设备密钥为在服务器和认证设备之间共享的秘密密钥。在一些实施例中，认证设备密钥在某批次的认证设备中的所有认证设备之间共享。在一些实施例中，每个单独的认证设备可以针对认证设备密钥具有自身单独的值。在这样的实施例中，服务器可以需要识别认证设备的数据，以便确定要使用的认证设备（例如，通过将认证设备识别数据用作密钥导出种子以用于生成正确的认证设备密钥或者在数据库中搜索正确的认证设备密钥）。在一些实施例中，初始化种子的一部分可以使用认证设备密钥进行加密。在一些实施例中，初始化种子的一部分可以使用认证设备密钥和用户的公共密钥进行加密。在一些实施例中，初始化消息的使用认证设备密钥和用户公共密钥进行加密的部分可以首先使用认证设备并且然后使用用户的公共密钥进行加密。在一些实施例中，初始化消息的使用认证设备密钥和用户的公共密钥进行加密的部分可以首先使用用户的公共密钥并且然后使用认证设备密钥进行加密。

然后，初始化消息可以用于用户的认证设备。

在一些实施例中，可以由用户开始 OTP 密钥初始化处理。例如，用户可以使用访问设备（例如，PC、平板电脑、台式计算机、智能电话……）例如通过访问网站或者通过发送邮件来接触初始化服务器，并且作为响应，服务器可以收集初始化消息并且例如以嵌入在网页中或电子邮件中的形式将所收集的初始化消息发送至用户的访问设备。在其他实施例中，初始化服务器可以针对多个用户主动地收集初始化消息。在一些实施例中，可以存储主动收集的初始化消息以供将来使用。在其他实施例中，主动收集的初始化消息可以例如以嵌入在电子邮件中的形式被主动发送至合适的用户。

初始化消息至认证设备的传输

在一些实施例中，初始化消息可用于用户的访问设备（例如，PC、平板电脑、台式计算机、智能电话……）。例如，初始化消息可以例如以嵌入在网页中或者电子邮件中的形式经

由因特网发送至用户访问设备。在一些实施例中，初始化消息可以由用户的访问设备传输至用户的认证设备。在一些实施例中，初始化消息可以由访问设备或者由另一装置借助于非定向通信信道传输至认证设备。访问设备可以经由用户的访问设备的人类输出接口来输出初始化消息的表示。访问设备可以在访问设备的显示器上输出例如在图像中被编码或在图像的序列中被编码或者被编码为时变光学图案的的初始化消息，或者访问设备可以使用访问设备的音频输出来输出被编码为音频声音的序列的初始化消息。认证设备可以捕获由访问设备输出的初始化消息的该表示。例如，在一个实施例中，认证设备可以包括例如包括相机的光学输入接口并且可以捕获由用户的访问设备显示并且使用初始化消息编码的一个或更多个图像（例如，图像可以包括QR代码），并且认证消息可以对所捕获的图像进行解密从而获得初始化消息。在另一实施例中，认证设备可以包括例如包括多个光学检测器的光学输入接口并且可以扫描由访问设备显示的、使用初始化消息编码的时变光学图案并且可以对时变光学图案进行解密从而获得初始化消息。在又一实施例中，认证设备可以包括声音输入接口并且可以捕获由用户的访问设备发出的、已经使用初始化消息编码的音频声音的序列，并且认证设备可以对这些声音进行解密从而获得初始化消息。

在一些实施例中，认证设备存储所获得的初始化消息以供将来处理。在其他实施例中，认证设备立即进行对初始化消息的处理。

OTP 密钥的初始化——认证设备侧

从初始化消息中检索初始化种子

认证设备例如以上述方式中之一获得由初始化服务器准备的初始化消息。认证设备可以如以下那样从初始化消息中提取初始化种子。认证设备可以促使用户将他或她的安全装置提供给认证设备（例如，在一些实施例中，认证设备可以包括智能卡读取器并且用户可以被促使将他或她的智能卡插入至认证设备中）。认证设备可以提取初始化消息的已使用用户的公共密钥进行加密的至少一些部分。初始化消息的已使用用户的公共密钥进行加密并且认证设备从初始化消息中提取的这些部分可以包括初始化种子的已使用用户的公共密钥进行加密的部分。认证设备可以将这些加密的部分提交至用户的安全装置并且可以请求用户的安全装置使用用户的私人密钥对加密的部分进行解密。用户的安全装置可以使用用户的私人密钥和非对称解密算法对加密的部分进行解密并且将初始化消息的新解密的部分返回至认证设备。认证设备可以从用户的安全装置接收初始化消息的新解密的部分。认证设备还可以提取包括在初始化消息中的初始化种子的未使用用户的私人密钥进行加密的部分。认证设备然后可以从初始化种子的已从初始化消息提取的各个部分收集初始化种子。

在一些实施例中，安全装置可以由 PIN 保护。在一些实施例中，安全装置可以要求 PIN 输入并且在进行涉及在安全装置中存储安全密钥的非对称密码操作之前验证所输入的 PIN 的正确性。在一些实施例中，认证设备可以适于请求用户输入 PIN，捕获由用户提供的 PIN（例如，借助于用户输入接口），并且将由用户提供的 PIN 传输至安全装置以用于验证。

在一些实施例中，还可以由初始化服务器使用不同于与用户关联的公共密钥的其他密钥对初始化消息（或者初始化消息的一部分）进行附加加密。在这样的实施例中，认证设备可以使用认证设备已知的（秘密）解密密钥对附加加密的初始化消息（或者初始化消息的附加加密的一部分）进行解密。在一些实施例中，使用对称加密算法使用初始化服务器和

认证设备二者均已知的对称加密密钥实现附加加密，并且认证设备可以使用该密钥来对附加加密的初始化消息进行解密。在其他实施例中，使用非对称密码算法使用公共密钥（其对应的私人密钥为认证设备已知）来完成加密，并且认证设备使用该私人密钥对附加加密的初始化消息（或者初始化消息的附加加密的一部分）进行解密。

在一些实施例中，用于对该附加加密进行解密的解密密钥对于每个认证设备而言是唯一的，并且初始化服务器例如使用用户可以例如在初始化处理期间提供的标识符（例如，用户的认证设备的序列号）来检索合适的加密密钥。在一些实施例中，解密密钥对于认证设备组而言是相同的，并且认证服务器仅需要知道用户的认证设备所属的认证设备组，从而确定正确的加密密钥。例如，在一些实施例中，所有的认证设备可以属于相同的组，即，所有认证设备可以共享相同的解密密钥。

这样的附加加密可以确保仅有效的认证设备或者甚至仅特定认证设备可以从初始化消息中检索初始化种子。例如，在一些实施例中，每个认证设备具有其自身唯一的解密密钥并且某些认证设备可以被放入黑名单（例如，原因为怀疑其已经包括在或落入恶意团体手中）并且这样的附加加密可以确保仅针对未落入黑名单的认证设备收集初始化消息并且初始化消息可以仅由未落入黑名单的认证设备进行加密。在实施例中，从而每个认证设备具有其自身唯一的解密密钥，该特征可以用于确保即使初始化消息被阻拦，初始化消息也不会被与初始化消息预期的认证设备不同的认证设备使用。

在一些实施例中，初始化消息可以包括其他数据元素，所述其他数据元素可以使得认证设备验证所接收的初始化消息是否一致、其完整性是否还未被损坏和/或所接收的消息是否确实应由该认证设备接收。初始化消息可以例如包括可由目标认证设备验证的目标认证设备的标识符、错误检测代码、冗余代码、消息认证代码和/或签名。

在一些实施例中，初始化消息可以包括与用户的公共密钥或者用户的公共密钥的证书有关的数据元素。

认证设备可以处理初始化种子，例如以确定 OTP 密钥的值，如以下详细描述。

初始化种子与 OTP 密钥之间的关系

在一些实施例中，初始化种子包括 OTP 密钥，并且在初始化处理之后，服务器和认证设备二者均可以简单地存储 OTP 密钥以供将来生成或验证 OTP。

在一些实施例中，初始化服务器确定初始化种子，并且初始化服务器和认证设备使用对应的导出机制导出相同的对应 OTP 密钥。例如，初始化服务器和认证服务器可以使用相同的导出机制，以从初始化种子导出 OTP 密钥。

在一些实施例中，初始化服务器确定 OTP 密钥并且使用第一密钥导出机制根据 OTP 密钥导出对应的初始化种子，并且认证设备适于使用与第一导出机制互补的第二导出机制根据初始化机制导出 OTP 密钥值，以使得认证设备导出与初始化服务器导出初始化种子所根据的 OTP 密钥值相同的 OTP 密钥值。例如，在一些实施例中，初始化服务器可以通过对 OTP 密钥值进行加密根据 OTP 密钥值导出初始化种子，并且认证设备可以通过对初始化种子进行解密根据初始化种子导出 OTP 密钥值。在一些实施例中，初始化服务器和认证设备共享加密/解密密钥并且使用对称加密/解密算法。在一些实施例中，初始化服务器可以使用共享的加密/解密密钥来使用对称加密算法对初始化消息的一部分进行加密。在一些实施例中，认证设备可以使用共享的加密/解密密钥来对初始化消息的已经由例如初始化服务

器进行加密的一部分进行解密。

在一些实施例中，由认证设备根据初始化种子导出 OTP 密钥值可以包括使用认证设备已知的秘密数据元素。在一些实施例中，该秘密数据元与初始化服务器共享。在一些实施例中，对于每个单独的认证设备，秘密数据元具有唯一的值。在一些实施例中，该秘密数据元素由认证设备组共享。例如，在一些实施例中，根据初始化种子导出 OTP 密钥值可以包括对存储在认证设备中的初始化种子和秘密数据元素进行逐位排除或操作。

在一些实施例中，由认证设备根据初始化种子导出 OTP 密钥值可以包括使用与用户的安全装置关联的数据元素例如与存储在用户的安全装置上的私人密钥有关的数据元素（例如，与公共密钥对应的用于对初始化消息的一部分进行加密的私人密钥）。与存储在安全装置上的私人密钥有关的这样的数据元素可以包括与该私人密钥对应的公共密钥或者与和该私人密钥关联的公共密钥证书不同的另一数据元素（例如，证书序列号或者用户名称或者用户的电子邮件地址）。这可以提供 OTP 密钥值和用户的安全装置（并且因此用户）之间的另外的链接。在一些实施例中，认证设备可以例如通过从安全装置读取数据元素例如公共密钥证书来从用户安全装置获得该额外的数据元素。

在一些实施例中，OTP 密钥值的导出可以包括使用额外的数据元素，这可以因此称为激活代码，该额外的数据元例如由初始化服务器确定并例如借助于带外信道例如邮件或电子邮件或提供至用户的手机的文本消息（例如，sms）被提供至用户，并且用户然后借助于认证设备的用户输入接口将该额外的数据提供至认证设备。激活代码可以例如包括字符串。在一些实施例中，激活代码可以包括 PIN 值。

在一些实施例中，在从初始化消息中检索初始化种子时，认证设备可以生成和存储与 OTP 密钥关联并且包括认证设备在后来生成和再生 (regenerate)OTP 密钥时可以使用的数据元素的数据集合。在一些实施例中，认证设备使用包括在该数据集合中的数据元素生成和再生 OTP 密钥可以包括使用如以下将要更详细阐述的用户安全装置。

OTP 密钥的使用期限

在一些实施例中，认证设备使用如上所述的初始化种子和用户安全装置来确定 OTP 密钥的值并且将所获得的 OTP 密钥值存储不确定的时间，以使其可以用于后来的任何 OTP 生成而不另外需要用户的安全装置。

使用安全装置来解锁用于生成 OTP 的 OTP 密钥

在一些实施例中，OTP 密钥具有不确定的使用期限，但是认证设备可以需要用户给出用于对初始化消息进行解密的安全装置用作用于使用 OTP 密钥生成 OTP 的条件。例如，在使用用于生成 OTP 的 OTP 密钥之前，认证设备可以促使安全装置被提供并且在安全装置被提供时，认证设备可以以与结合图 6 至图 9 在以上讨论的实施例相似的方式验证其是否为正确的安全装置。例如，在一些实施例中，认证设备可以存储使得认证设备识别正确的安全装置的数据元素（例如，存储在安全装置上的公共密钥证书的序列号）并且可以通过将询问提交至安全装置来认证安全装置，以用于安全装置使用存储在安全装置上的私人密钥进行签名。认证设备可以通过使用对应的公共密钥来验证签名并且可选地验证公共密钥的证书。在一些实施例中，认证设备可以存储询问和对应的参考响应，将询问提交至安全装置并且将从安全装置接收到的响应与所存储的参考响应进行比较。

在一些实施例中，所获得的 OTP 密钥值可以仅具有有限的使用期限，并且此后，认证设

备丢弃或删除 OTP 密钥值，使得认证设备必须再生用于以后的 OTP 生成的 OTP 密钥值。在一些实施例中，认证设备使用与 OTP 密钥关联并且由认证设备存储并且包括认证设备可以用于生成 OTP 密钥值（可以使用用户的安全装置）的数据元素的数据集合来再生 OTP 密钥值。

在一些实施例中，可以鉴于在特定事件（如 OTP 密钥值的生成或者 OTP 密钥值在生成 OTP 时的首次使用）之后经过的实际时间来限定 OTP 密钥的使用期限。在其他实施例中，可以鉴于 OTP 密钥值用于例如生成 OTP 的次数来限定 OTP 密钥值的使用期限。在又一些实施例中，由认证设备生成 OTP 值可以涉及使用与 OTP 密钥关联的用户的安全装置，并且当用户的安全装置从认证设备移除时认证设备可以丢弃所生成的 OTP 值。

再生 OTP 密钥时使用安全装置

在一些实施例中，OTP 密钥的生成（再生）可能需要认证设备使用用户的安全装置。尤其，在一些实施例中，OTP 密钥的生成（再生）可以包括认证设备请求用户的安全装置使用存储在安全装置上的用户的私人密钥来进行非对称密码操作。在一些实施例中，与用于再生 OTP 密钥的私人密钥相同的私人密钥可以用于对初始化消息进行解密。在一些实施例中，用户的安全装置存储多于一个的公共 / 私人密钥对的多于一个的私人密钥，并且与用于再生 OTP 密钥的私人密钥不同的私人密钥可以用于对初始化消息进行解密。

在一些实施例中，认证设备在用于再生 OTP 密钥的算法中将该非对称密码操作的结果用作输入数据。在一些实施例中，认证设备可以存储数据元素，并且为了再生 OTP 密钥，认证设备可以将该存储的数据元素提交至安全装置，并且安全装置使用其私人密钥对该提交的数据元进行非对称密码操作并且将结果返回至认证设备，认证设备在用于再生 OTP 密钥的以后的计算中使用该返回结果。即，在一些实施例中，再生的 OTP 密钥可以为安全装置的私人密钥和存储在认证设备中的值的函数。

在一些实施例中，如果另外的安全装置（具有另外的私人密钥）被提供给认证设备，则认证设备可以仍然会生成 OTP 密钥，然而，该 OTP 密钥将会具有与正确的 OTP 密钥不同的值（原因在于，另外的安全装置的私人密钥不同），使得当认证设备此后使用该不同的 OTP 密钥来生成 OTP 时，所生成的 OTP 也将会不正确，并且将会在验证处理中被拒绝。在一些实施例中，认证设备存储使得认证设备标识或识别正确的安全装置并且在不正确或不期望的安全装置被提供的情况下则警告用户的数据元素。

在一些实施例中，认证设备可以存储使用用户的公共密钥进行加密的值，并且为了再生 OTP，认证设备可以请求用户的安全装置以在安全装置可以使用该解密的值再生 OTP 值时使用用户的私人密钥对该存储的值进行解密。

例如，在一些实施例中，认证设备可以确定根据其可以再生 OTP 密钥的值，使用用户的公共密钥对该值进行加密，并且存储加密的值。为了再生 OTP 密钥，认证设备可以请求用户的安全装置以在安全装置可以使用该解密的值再生 OTP 值时使用用户的私人密钥来对该存储（加密）的值进行解密。在一些实施例中，认证设备可以例如在认证设备的初始化期间从安全装置获得该公共密钥。在一些实施例中，认证设备可以将公共密钥存储在例如与 OTP 密钥关联的数据集合中以供将来使用。

在一些实施例中，使用公共密钥加密的存储值可以包括 OTP 密钥自身。在其他实施例中，使用公共密钥加密的存储值可以包括可以由认证设备用户用于再生 OTP 密钥的中间

值。例如，在一些实施例中，在丢弃 OTP 密钥之前，认证设备确定中间对称加密密钥（例如可以为随机数）、使用中间对称加密密钥使用对称加密算法对 OTP 密钥进行加密、使用安全装置的私人密钥使用非对称加密算法对中间对称加密密钥进行加密、存储加密的 OTP 密钥和加密的中间对称加密密钥并且然后可以丢弃 OTP 密钥的清除值（clear value）和中间对称加密密钥的清除值。此后，当认证设备需要再生 OTP 密钥时，该认证设备向安全装置提交所存储的使用安全装置的公共密钥进行加密的加密的中间对称加密密钥。然后，安全装置使用其私人密钥对该加密的中间对称加密密钥进行解密并且将该解密的中间对称加密密钥返回至认证设备。认证设备然后使用中间对称加密密钥对加密的 OTP 密钥进行解密。在一些实施例中，不必使用这样的中间对称加密密钥对 OTP 密钥自身进行加密和存储，认证密钥可以对一些中间导出种子进行加密和存储。这可以例如在再生实际 OTP 密钥时使用其他数据元素的实施例的情况下进行。

在其他实施例中，认证设备可以例如存储询问并且可以请求用户的安全装置使用用户的私人密钥对该询问进行签名。认证设备然后可以使用安全装置经由该询问产生的签名导出 OTP 密钥。

例如，在一些实施例中，在丢弃 OTP 密钥之前，认证设备确定询问，将询问提交至由安全装置的私人密钥签署的安全装置，根据由安全装置经由该询问生成的签名导出中间加密密钥，使用该中间加密密钥对 OTP 密钥进行加密，存储加密的 OTP 密钥并且然后可以丢弃 OTP 密钥的清除值。此后，当认证设备需要再生 OTP 密钥时，认证设备将相同的询问提交至安全装置。安全装置对提交的询问进行签名并且将签名返回至认证设备。认证设备然后可以根据该签名导出中间加密密钥并且将中间加密密钥用于对加密的 OTP 密钥进行解密。在一些实施例中，不必使用中间对称加密密钥加密和存储 OTP 密钥本身，认证密钥可以解密和存储一些中间导出种子。这可以例如在再生实际 OTP 密钥时还使用其他数据元素的实施例的情况下进行。在一些实施例中，询问可以为可以被硬编码的固定值。在一些实施例中，询问可以为随机值并且认证设备存储该询问。在一些实施例中，认证设备可以在每次丢弃 OTP 密钥时使用相同的询问。在其他实施例中，认证设备可以在每次或仅一些时候在丢弃 OTP 密钥时针对询问确定不同的值。

在一些实施例中，认证设备总是将相同的静态值提供给用户的安全装置，从而再生特定 OTP 密钥的值。例如，认证设备在初始化处理期间针对特定 OTP 密钥确定一个值（例如，使用用户的公共密钥加密的询问或值），该值由认证设备存储且针对该特定 OTP 密钥不再变化并且由认证设备提供给用户的（例如，使用用户的私人密钥签名或者由用户的私人密钥解密的）安全装置从而获得然后用于生成（再生）OTP 密钥的第二值。

在一些实施例中，认证设备可以随时更新该存储值。在一些实施例中，该存储值可以在 OTP 密钥再生特定次数之后（例如，在每次再生时）更新。在一些实施例中，认证设备更新存储的值以及一些其他数据元素，使得认证设备仍然可以使用存储的值和其他数据元素的更新的值来再生相同的 OTP 密钥。认证设备可以例如针对其支持的每个 OTP 密钥将存储值和其他数据元素存储在与 OTP 密钥关联的数据集合中。例如，在一些实施例中，当认证设备再生 OTP 密钥（或者更一般地，当认证设备更新用于再生的用于再生 OTP 密钥的存储数据元素时，其因此将称为再生数据）时，认证设备可以根据生成数据的存储值确定还将称为中间导出值的值，根据该值可以导出 OTP 密钥值（例如，OTP 密钥值自身或者原始初始化种

子或者一些其他中间值）。然后，认证设备可以生成随机（或者伪随机）值。

在一些实施例中，该随机值被存储作为询问的更新值，并且认证设备将该更新的询问提交至要进行签名的用户的安全装置。然后，认证设备可以根据中间导出值和经过更新的询问生成的签名来计算称为补偿值的值。认证设备可以存储该补偿值以及更新的询问。该补偿值可以由认证设备计算，使得认证设备可以经过存储的更新的询问和存储的补偿值根据用户的安全装置签名随后再生中间导出值的原始值。例如，认证设备可以经过更新的询问通过对中间导出值和签名的特定部分进行逐位异或来计算补偿值。随后，认证设备则可以通过使得用户的安全装置对存储的更新的询问进行签名来再生中间导出值（并且随后还生成 OTP 密钥）并且然后对存储的补偿值以及前面提及的签名的特定部分执行逐位异或。

在其他实施例中，认证设备可以根据中间导出值和随机值来计算补偿值并且存储该补偿值。该补偿值可以由认证设备来计算，使得认证设备随后可以通过将随机值和存储的补偿值进行组合来再生中间导出值的原始值。认证设备可以使用用户的公共密钥对随机值进行加密并且可以存储该加密的随机值。随后，认证设备可以通过首先请求用户的安全装置使用用户的私人密钥对加密的随机值进行解密并且然后将解密的随机值与补偿值进行组合来再生原始中间导出值。例如，在一些实施例中，认证设备可以通过对随机值和原始中间导出值执行逐位异或来计算补偿值，并且相似地，随后可以通过对解密的随机值和存储的补偿值执行逐位异或来再生原始中间导出值。

在又一些其他实施例中，认证设备可以适于根据其存储的第一值以及其根据与安全装置的公共密钥（密码地）有关并且可以存储在安全装置上的数据元素导出的第二值来生成（再生）OTP 密钥。为了在已经丢弃 OTP 密钥之后再生 OTP 密钥，认证设备可以促使用户提供他或她的安全装置。认证设备可以获得与数据元素有关的公共密钥。认证设备可以由安全装置使用与公共密钥对应的私人密钥基于密码操作借助于询问响应方法来认证安全装置。认证设备可以例如将询问提交至安全装置以由安全装置进行签名，并且认证设备可以验证该签名。在成功验证安全装置时，认证设备可以根据与从安全装置获得的公共密钥有关的数据元素来导出第二值，并且使用导出的第二值以及存储的第一值来再生 OTP 密钥。在一些实施例中，与公共密钥有关的数据元素可以为公共密钥本身。在一些实施例中，与公共密钥有关的数据元素可以为根据认证设备从安全装置接收公共密钥的证书以及公共密钥自身的数据元素，并且认证该安全装置可以包括验证该证书。在一些实施例中，由认证设备存储的第一值可以为从初始化消息提取的初始化种子。

在一些实施例中，丢弃 OTP 密钥可以包括从认证设备的（多个）存储器部件擦除 OTP 密钥的值。

在其他实施例中，当认证设备丢弃 OTP 密钥时，认证设备不从其（多个）存储器部件中擦除 OTP 密钥，而是使存储器中的 OTP 密钥无效（例如，通过设置指示 OTP 密钥的无效状态的与 OTP 密钥有关的标记）。然后，再生 OTP 密钥可以包括（例如，通过重新设置与 OTP 密钥关联的指示 OTP 密钥的状态是有效的标记）重新激活存储器中的 OTP 密钥，而不是计算或重新导出 OTP 密钥的值。在一些实施例中，认证设备存储 OTP 以及密码的形式链接至用户的安全装置上的公共 / 私人密钥对的公共密钥的识别数据元素（即，链接至与存储在相同安全装置上的私人密钥对应的公共密钥的数据元素，安全装置用于对由认证设备用于

导出或确定 OTP 密钥的值的初始值进行解密；该数据元素可以借助于公共密钥的证书链接至这样的公共密钥；该数据元素可以例如包括用户的名称或者证书序列号或者公共密钥自身）。在一些实施例中，作为重新激活 OTP 密钥的必须条件，认证设备可以需要与 OTP 密钥关联的用户安全装置并且可以读取与识别数据元素相链接的公共密钥和 / 或公共密钥的证书，并且可以通过使用该公共密钥进行询问 - 响应认证来认证安全装置（例如，将询问发送至安全装置，以由安全装置提交至使用与公共密钥对应的私人密钥的非对称密码操作例如签名操作，并且使用公共密钥来验证结果，即，该询问 - 响应认证的响应）。在一些实施例中，认证设备还可以验证该公共密钥的证书。在一些实施例中，该公共密钥与用于对初始化种子进行解密的私人密钥对应的公共密钥相同。

支持多用户和多应用

在一些实施例中，认证设备仅支持一个 OTP 密钥，并且认证设备仅能用于一个用户，并且同一 OTP 密钥用于用户通过使用由认证设备生成的 OTP 访问的所有应用。

在其他实施例中，认证设备可以支持多个 OTP 密钥。例如，认证设备可以存储多个数据集合，其中每个数据集合与不同的 OTP 关联，并且其中每个数据集合包括认证设备可以用于获得与数据集合关联的 OTP 密钥的数据。

支持多个应用

在一些实施例中，认证设备可以支持多于一个的 OTP 密钥，并且同一用户的不同 OTP 密钥可以与不同应用关联。例如，认证设备可以存储多个数据集合，其中每个数据集合与不同的 OTP 关联，并且，其中每个数据集合包括认证设备可以用于获得与数据集合关联的 OTP 密钥的数据，并且其中，每个数据集合还包括应用标识符。认证设备可以使用这些应用标识符来辅助用户在生成针对特定应用的 OTP 时选择合适的 OTP 密钥。例如，应用标识符可以包括应用名称，并且认证设备可以使用其提供给用户的菜单中的应用名称，使得用户可以选择认证设备应为哪个应用生成 OTP。在一些实施例中，包括与特定应用关联的 OTP 密钥的初始化种子的初始化消息也可以包括这样的应用标识符。

在一些实施例中，单个初始化消息可以包括用于多于一个应用的初始化数据（例如，初始化种子和应用标识符）。

在一些实施例中，应用网络服务器可以向用户指出他们可以如何开始初始化处理，从而使用适于该应用的 OTP 密钥来使其认证设备个性化。例如，应用的网络服务器的登录页面可以包括链接至初始化服务器的链接。如果用户采用该链接，则初始化服务器将开始对该用户的初始化处理。

支持多个用户

在一些实施例中，认证设备可以支持多于一个 OTP 密钥，并且不同的 OTP 密钥可以与不同的用户关联。例如，认证设备可以存储多个数据集合，其中每个数据集合与不同的 OTP 密钥关联，其中每个数据集合包括认证设备可以用于获得与该数据集合关联的 OTP 密钥的数据，并且其中每个数据集合还可以包括与用户关联的数据元素。与用户关联的该数据元素可以例如包括用户标识符（例如，用户的国家 id 号或者用户的社会保险号），或者其可以包括用户的安全装置的标识符，或者其可以包括与用户的安全装置上的用户私人密钥关联的标识符例如与用户的私人密钥关联的证书的序列号。在一些实施例中，当用户将他或她的安全装置提供给认证设备时，认证设备可以检索存储在安全装置上的数据（例如，用户的

全国id或证书的序列号）并且将该数据与存储在认证设备中的与认证设备支持的各个OTP密钥关联的各个数据集合中的对应的用户关联数据元素进行比较。在这种方式下，认证设备可以确定和选择可以与认证设备的当前用户提供给认证设备的给定安全装置一起使用的数据集合，并且可以因此将这些数据集合区别于和可能偶尔使用同一认证设备的其他用户的安全装置关联的数据集合。

在一些实施例中，当用户将他或她的安全装置提供给认证设备时，认证设备可以验证该安全装置是否已经具有与安全装置关联的数据集合。如果不具有，则认证设备可以建议用户开始初始化处理，从而获得初始化消息，使得认证设备可以针对给定安全装置构建数据集合。

支持额外的认证设备

在一些实施例中，初始化服务器可以针对不同的认证设备收集多于一个的初始化消息，以使它们生成相同的OTP密钥。在这种方式下，用户可以初始化多于一个的认证设备，并且可以使用其中任何一个与他或她的安全装置一起来生成有效OTP。

本发明的一个方面提供了一种设备，该设备包括：认证设备，其用于生成动态凭证，认证设备包括适于使用对称密码算法生成包括一次性口令和/或消息认证代码的动态凭证的处理部件，对称密码算法将秘密凭证生成密钥与动态变量的值以密码的形式进行组合；存储器部件，其用于永久地或暂时地存储秘密凭证生成密钥；用户输入接口，其用于接收来自用户的输入；通信接口，其用于与所述用户的安全设备进行通信，该安全设备包括存储器，该存储器用于安全地存储与所述用户关联的第一公共/私人密钥对的第一私人密钥并且适于使用所述第一私人密钥进行非对称密码计算，其中，所述非对称密码计算至少包括非对称密码解密操作，数据输入接口用于接收至少包括初始化种子的初始化消息，初始化种子的至少一部分使用所述第一公共/私人密钥对的第一公共密钥进行加密；从而，认证设备适于从初始化消息至少提取初始化种子的所述第一加密的部分，以将初始化种子的第一加密的部分（使用通信接口）提交至所述用户的安全装置从而所述安全装置使用所述公共密钥和所述非对称密码解密操作对初始化种子的第一加密的部分进行解密，从安全装置（使用通信接口）接收由安全装置解密的初始化种子的第一部分，以及至少根据初始化种子的所述解密的第一部分来导出所述秘密凭证生成密钥的值并且将所述秘密凭证生成密钥的所述导出值至少暂时地存储在所述存储器部件中。

在一些实施例中，初始化种子的第一加密的部分可以包括整个初始化种子。在一些实施例中，初始化种子可以包括或可以为秘密凭证生成密钥。

在一些实施例中，认证设备还可以适于限制秘密凭证生成密钥的使用期限。在一些实施例中，认证设备适于根据特定准则确定是否已超过秘密凭证生成密钥的使用期限。在一些实施例中，认证设备还可以适于在其确定出已超过秘密凭证生成密钥的使用期限之后丢弃秘密凭证生成密钥。在一些实施例中，认证设备丢弃秘密凭证生成密钥可以包括认证设备从存储器部件擦除秘密凭证生成密钥的值。在一些实施例中，秘密凭证生成密钥的使用期限鉴于从特定事件开始经过的时间来限定，并且在已经经过该时间之后认证设备丢弃该秘密凭证生成密钥。例如，认证设备可以在认证设备已经获得秘密凭证生成密钥的值之后的固定时间（例如，一小时）将秘密凭证生成密钥丢弃。在一些实施例中，鉴于从认证设备已经获得秘密凭证生成密钥的值开始秘密凭证生成密钥的值已经被用于生成动态凭证的

次数来限定秘密凭证生成密钥的使用期限。例如，认证设备可以适于对自从认证设备已经获得秘密凭证生成密钥的值之后认证设备使用秘密凭证生成密钥的次数进行计数并且在该次数超过特定固定阈值时丢弃该值。在一些实施例中，秘密凭证生成密钥在其被使用一次后被丢弃。在一些实施例中，鉴于特定事件来限定秘密凭证生成密钥的使用期限。例如，在一些实施例中，认证设备可以要求提供用于生成动态凭证的所述安全装置并且可以在移除安全装置时丢弃秘密凭证生成密钥。

在一些实施例中，认证设备还可以适于在秘密凭证生成密钥的值被丢弃之后再生秘密凭证生成密钥的值。在一些实施例中，认证设备适于将与秘密凭证生成密钥关联的包括第一再生值的数据集合存储在存储器部件中，并且认证设备再生秘密凭证生成密钥的值可以包括：认证设备向所述用户的安全装置提交所述第一再生值，以使所述用户的安全装置使用存储在用户的安全装置中的第一公共/私人密钥对的第二私人密钥利用非对称密码算法来处理所述第一再生值，认证设备从用户的安全装置接收由用户的安全装置使用所述第二私人密钥处理所述第一再生值的所得值，并且根据所述第一所得值导出秘密凭证生成密钥的值。在一些实施例中，所述第一公共/私人密钥对可以与所述第一公共/私人密钥对相同。

在一些实施例中，所述第一再生值包括初始化种子的所述第一加密的部分。在一些实施例中，所述第一再生值包括使用与所述第二私人密钥对应的第二公共密钥加密的秘密凭证生成密钥，并且再生秘密凭证生成密钥的值包括认证设备向所述用户安全装置提交所述加密的秘密凭证生成密钥，以使所述用户的安全装置使用在用户的安全装置中存储的所述第二公共/私人密钥对的所述第二私人密钥对加密的秘密凭证生成密钥进行解密。在一些实施例中，初始化种子的所述第一加密的部分包括秘密凭证生成密钥。在一些实施例中，认证设备再生秘密凭证生成密钥的值包括认证设备向所述用户安全装置提交初始化种子的第一加密的部分，以使所述用户安全装置使用在用户安全装置中存储的所述第一公共/私人密钥对的所述第一私人密钥对初始化种子的第一加密的部分进行解密。

在一些实施例中，认证设备适于在丢弃秘密凭证生成密钥之前确定第一再生值。在一些实施例中，认证设备通过使用与所述第二私人密钥对应的公共密钥对认证设备可用于再生秘密凭证生成密钥的值进行加密来确定第一再生值。在一些实施例中，该值可以包括秘密凭证生成密钥。

在一些实施例中，与秘密凭证生成密钥关联的所述数据集合还包括第二再生值，并且认证设备还适于使用所述第二再生值和所述第一所得值再生秘密凭证生成值。在一些实施例中，第二再生值包括使用对称加密算法使用再生加密密钥加密的再生种子。在一些实施例中，认证设备再生秘密凭证生成密钥包括认证设备向安全装置提交第一再生值，以使安全装置使用非对称签名算法和所述第二私人密钥进行签名，接收所得签名，根据所述所得签名导出再生加密密钥，使用所导出的再生加密密钥来使用对称解密算法对第二再生值进行解密以获得所述再生种子，并且根据解密的再生种子来导出第二秘密凭证生成值。在一些实施例中，再生种子可以包括初始种子。在一些实施例中，再生种子可以包括秘密凭证生成密钥。

在一些实施例中，认证设备适于在丢弃秘密凭证生成密钥之前确定第一再生值和第二再生值。在一些实施例中，认证设备通过选择询问来确定第一再生值并且通过确定再生种

子和再生加密密钥并且使用所述再生加密密钥对所述再生种子进行加密以获得第二再生值来确定第二再生值，从而认证设备通过向安全装置提交第一再生值以使安全装置使用非对称签名算法和所述第二私人密钥进行签名，接收所得签名，根据所述所得签名导出再生加密密钥来确定再生加密密钥，并且从而再生种子被确定成是与秘密凭证生成密钥有关的值，使得认证设备可以根据所述再生种子来导出秘密凭证生成密钥。在一些实施例中，再生种子包括初始化种子。在一些实施例中，再生种子包括秘密凭证生成密钥。

在一些实施例中，认证设备还可以适于捕获通过用户的访问设备的用户输出接口输出或发出并且对初始化消息的表示进行编码的信号，并且认证设备还可以适于从捕获的信号提取初始化消息并且对其进行解密。在一些实施例中，认证设备包括相机并且认证设备适于使用相机拍摄对初始化消息进行编码的图像的照片并且在访问设备的显示器上显示照片，并且认证设备适于从使用相机拍摄的照片中提取图像并且对图像进行解密以获得在图像中编码的初始化消息。在一些实施例中，认证设备包括麦克风，并且认证设备适于使用麦克风记录对初始化消息进行编码的音频信号并且由访问设备的扬声器发出音频信号，并且认证设备适于从音频信号提取初始化消息并对其进行解密。

在一些实施例中，用于生成动态凭证的对称密码算法可以包括散列算法。例如，在一些实施例中，对称密码算法可以包括使用秘密凭证生成密钥参数化的键入的散列算法并且将动态变量的值作为输入。例如，在一些实施例中，对称密码算法可以包括使用秘密凭证生成密钥参数化并且对根据动态变量导出的值进行加密的对称加密算法。

在一些实施例中，动态变量可以根据时间值导出。在一些实施例中，认证设备可以包括提供认证设备可以使用的时间值的时钟以确定动态变量的值。在一些实施例中，动态变量可以根据计数值导出。在一些实施例中，认证设备可以存储或保持该计数并且在特定事件时更新计数。在一些实施例中，认证设备可以在每次认证设备生成动态凭证时更新计数值。例如，在一些实施例中，认证设备可以在每个凭证生成之前或之后增加计数。在一些实施例中，可以根据由认证设备存储和保持并且由认证设备在特定事件时更新的值来导出动态值。例如，认证设备可以通过将当前值提交至散列算法并且由该散列算法的结果替代当前值来更新该事件相关值。在一些实施例中，可以根据在认证设备外部生成并且被提供至认证设备的询问来导出该动态变量。在一些实施例中，用户输入接口可以适于接收由用户提供至认证设备的询问。在一些实施例中，可以根据可以表示用户想要提交至应用的业务并且被提供至认证设备的业务数据来导出动态变量。在一些实施例中，用户输入接口可以适于接收由用户提供至认证设备的业务数据。

在一些实施例中，认证设备可以包括用户输出接口。在一些实施例中，认证设备可以适于使用用户输出接口来将生成的动态凭证传输至用户。在一些实施例中，用户输出接口可以包括显示器，并且认证设备可以以字符串的形式将生成的动态凭证提供给用户。在一些实施例中，字符串仅包括十进制数字。在一些实施例中，字符串包括字母数字。

本发明的另一方面提供了使用用于生成动态凭证的秘密凭证生成密钥初始化特定用户的认证设备的方法，该方法包括步骤：在服务器处确定秘密凭证生成密钥和初始化种子，从而秘密凭证生成密钥和初始化种子由允许根据初始化种子导出秘密凭证生成密钥的算法在数学上关联，在服务器处将秘密凭证生成密钥与所述特定用户关联，在服务器处使用公共/私人密钥对（其私人密钥存储在所述用户的安全装置上）的公共密钥利用非对称加

密算法对初始化种子的至少第一部分进行加密，在服务器收集包括初始化种子的经加密的所述第一部分和初始化种子的任何其他部分的初始化消息，将所述初始化消息发送至用户的认证设备，在所述认证设备处接收初始化消息，在认证设备处从所接收的初始化消息中提取初始化种子的经加密的第一部分和初始化种子的任何其他部分，在认证设备处与用户的由用户提供给认证设备的安全设备进行通信，由认证设备将初始化种子的经加密的第一部分提交至所述安全装置，在安全装置处使用所述私人密钥对初始化种子的经加密的第一部分进行解密并且将初始化种子的经解密的第一部分返回至认证设备，在认证设备处接收初始化种子的经解密的第一部分，并且在认证设备处根据初始化种子导出秘密凭证生成密钥。

在一些实施例中，在服务器处确定秘密凭证生成密钥和初始化种子包括选择初始化种子的值并且根据所选择的初始化种子的值计算秘密凭证生成密钥。例如，秘密凭证生成密钥可以具有与所选择的初始化种子的值相同的值，或者可以被计算为初始化种子的选择值的一次散列函数。在一些实施例中，在服务器处确定秘密凭证生成密钥和初始化种子包括选择秘密凭证生成密钥的值并且根据秘密凭证生成密钥的选择值来计算初始化种子。例如，可以通过使用加密密钥（其对应的解密密钥对于认证设备是已知的）对秘密凭证生成密钥的选择值进行加密来计算初始化种子。

在一些实施例中，方法包括另外的步骤：至少暂时将导出的秘密凭证生成密钥存储在认证设备的存储器部件中。

在一些实施例中，方法包括另外的步骤：在服务器处使用与认证设备已知的解密密钥匹配的加密密钥对初始化种子的至少第二部分进行加密并且在认证设备处使用所述解密密钥对初始化种子的所述第二部分进行解密。在一些实施例中，所述解密密钥的值对于所述特定认证设备是特定的。在一些实施例中，认证设备与其他认证设备共享所述解密密钥的值。

在一些实施例中，将所述初始化消息发送至用户的认证设备的步骤包括：服务器将初始化消息发送至用户的访问设备并且访问设备通过访问设备的用户输出接口发出使用初始化消息的表示进行编码的信号，并且在所述认证设备处接收初始化消息的步骤包括认证设备捕获所述信号并且对所述信号进行解密以获得所述初始化消息的表示。在一些实施例中，认证设备包括相机并且访问设备包括显示器，并且初始化消息的表示包括二维图像，并且该方法包括如下另外的步骤：访问设备将所述二维图像显示在访问设备的显示器上，并且认证设备拍摄所述图像的照片，从所述照片提取所述二维图像并且对所述图像进行解码以获得初始化消息。

在一些实施例中，认证设备可以包括用于生成以上所述的动态凭证的认证设备中任何一个。

本发明的又一方面提供了用于由特定用户的认证设备和安全装置生成第一动态凭证的方法，该方法包括以下步骤：使用用于生成上述动态凭证的秘密凭证生成密钥根据初始化特定用户的认证设备的方法中的任何方法来对所述特定用户的所述认证设备进行初始化，获得动态变量的值，并且将第一动态凭证确定为使用对称密码算法将所述动态变量的所述值与所述秘密凭证生成密钥以密码的形式进行组合的结果。

在一些实施例中，用于生成第一动态凭证的方法包括另外的步骤：根据时间相关值导

出所述动态变量的所述值。在一些实施例中，用于生成第一动态凭证的方法包括另外的步骤：根据由认证设备保持和更新的计数来导出所述动态变量的值。在一些实施例中，用于生成第一动态凭证的方法包括另外的步骤：根据在认证设备外部生成并且可以被提供至认证设备的询问来导出所述动态变量的所述值。在一些实施例中，认证设备借助于认证设备的用户输入接口接收来自用户的询问。在一些实施例中，用于生成第一动态凭证的方法包括另外的步骤：根据表示用户想要由应用执行的业务的业务数据来导出所述动态变量的所述值，所述应用可以例如由远程应用服务器控制。在一些实施例中，认证设备借助于认证设备的用户输入接口来接收来自用户的业务数据。在一些实施例中，认证设备经由认证设备的数据输入接口来接收业务数据并且借助于认证设备的人类输出接口将业务数据提供给用户以用于查看，并且借助于认证设备的用户输入接口来捕获用户针对业务数据提供的批准。

在一些实施例中，用于生成第一动态凭证的方法包括另外的步骤：认证设备生成可以提供给用户的所生成的所述动态凭证的表示，并且认证设备借助于认证设备的人类输出接口将所述表示提供给用户。

在一些实施例中，用户生成第一动态凭证的方法包括另外的步骤：认证设备对照一组准则验证所述秘密凭证生成密钥的使用期限是否已过期，并且如果所述使用期限已过期，则认证设备可以在生成所述第一动态凭证之后丢弃所述秘密凭证生成密钥。在一些实施例中，所述丢弃可以包括认证设备从认证设备的存储器部件擦除秘密凭证生成密钥。在一些实施例中，所述丢弃可以包括认证设备使得存储在认证设备的存储器部件中的秘密凭证生成密钥无效。

在一些实施例中，用于生成第一动态凭证的方法包括另外的步骤：认证设备在使用所述秘密凭证生成密钥生成第二动态凭证之前再生秘密凭证生成密钥。在一些实施例中，再生秘密凭证生成密钥包括：认证设备要求用户的安全装置被提供并且与安全装置进行通信，认证设备将第一再生值提交至安全装置，安全装置接收所述第一再生值并且将第一再生值用作使用与用户关联的第二公共/私人密钥对的存储在安全装置上的第二私人密钥来参数化的非对称密码操作的输入，安全装置将由安全装置进行的所述非对称密码操作的结果返回至认证设备，并且认证设备使用所述结果。

在一些实施例中，所述认证设备使用所述结果包括认证设备验证所述结果。在一些实施例中，安全装置的所述非对称密码操作包括使用由所述第二私人密钥参数化的非对称密码签名算法生成对所接收的第一再生值的签名，所述结果包括所述签名，并且所述认证设备验证所述结果包括验证所述签名包括在所述结果中。在一些实施例中，第一再生值包括由认证设备生成的随机询问。在一些实施例中，认证设备丢弃秘密凭证生成密钥可以包括认证设备使得存储在认证设备的存储器部件中的秘密凭证生成密钥无效，并且认证设备使用安全装置进行的所述非对称密码操作的所述结果可以包括如果所述结果的验证成功则重新激活存储在认证设备的存储器部件中的秘密凭证生成密钥。

在一些实施例中，认证设备可以在丢弃秘密凭证生成密钥之前确定中间值，并且所述第一再生值包括使用由与所述公共/私人密钥对的所述第二私人密钥对应的第二公共密钥参数化的非对称加密算法加密的所述中间值。在一些实施例中，所述安全装置的所述非对称密码操作包括使用由所述第二私人密钥参数化的非对称解密算法对所接收的第一再

生值进行解密，所述结果包括解密的中间值，并且所述认证设备使用所述结果包括认证设备使用解密的中间值来获得秘密凭证生成密钥的值。在一些实施例中，中间值包括秘密凭证生成密钥。在一些实施例中，中间值包括初始化密钥。

在一些实施例中，认证设备可以在丢弃秘密凭证生成密钥之前确定第二再生值，并且认证设备使用安全装置进行的非对称密码操作的所述结果包括认证设备将所述第二再生值与所述结果以数学的方式或密码的方式进行组合以确定秘密凭证生成密钥的值。在一些实施例中，确定第二再生值包括确定中间再生种子和使用中间加密密钥对中间再生种子进行加密，并且第二再生值包括使用中间加密密钥加密的中间再生种子，并且认证设备使用安全装置进行的所述非对称密码操作的所述结果包括根据所述结果导出与所述中间加密密钥匹配的中间解密密钥，并且对经加密的所述中间再生种子进行解密，并且根据经解密的中间再生种子导出秘密凭证生成密钥的值。在一些实施例中，中间再生种子包括秘密凭证生成密钥。在一些实施例中，中间再生种子包括初始化种子。在一些实施例中，认证设备确定中间解密密钥的值（例如，随机数）并且通过使用所述第二公共密钥对中间解密密钥进行加密来确定所述第一再生值，并且认证设备通过将第一再生值提交至安全装置以由第二私人密钥进行解密来恢复中间解密密钥。在一些实施例中，认证设备确定第一再生值（例如，随机数），并且通过将第一再生值提交至安全装置以由第二私人密钥进行签名来第一次确定第二中间加密密钥的值，并且根据得到的签名导出中间加密密钥，通过使用如上所述的中间加密密钥对中间再生种子进行加密来使用中间加密密钥确定第二再生值，存储第一再生值和第二再生值，再生密钥凭证生成密钥：通过将第一再生值重新提交至安全装置以由第二私人密钥进行签名并且根据所得签名重新导出中间加密密钥来再生中间加密密钥，并且使用再生的中间加密密钥来对第二再生值进行解密，以获得中间再生种子的值，以及根据所获得的中间再生种子的值来导出秘密凭证生成密钥。

本发明的再一方面提供了使用认证设备例如如上所述的认证设备用于确保用户与远程应用服务器之间的交互的方法，该方法包括步骤：在应用服务器处接收用户的请求，应用户的请求在认证设备处根据上述生成动态凭证的方法中的任何方法来生成动态凭证，使得验证服务器可以获得与用户关联的秘密动态凭证生成密钥，在验证服务器处接收所生成的动态凭证，在验证服务器处使用所述秘密动态凭证生成密钥来验证所接收的动态凭证的有效性，并且如果验证出所接收的动态凭证是有效的，则在远程应用服务器处批准所述请求。

本发明的方面的优点

本发明的特定实施例的优点在于，服务器从不需要访问用户的安全装置（服务器仅需要能够获得用户的公共密钥），并且服务器不需要跟踪哪个用户正在使用哪个认证设备。特别地，用户不需要获得由用户的安全装置使用存储在该装置上的用户私人密钥执行的非对称密码操作的结果。这意味着认证设备可以不需要能够将例如由用户的安全装置提供的数字信息例如由用户的安全装置使用用户的私人密钥以密码的形式生成的数据（例如，签名或对询问的响应）（直接或间接地）传输至服务器侧。在一些实施例中，认证设备具有用于接收初始化消息的非定向数据输入接口（例如，用于捕获显示在计算机屏幕上的图像的相机）就足够了。在一些实施例中，初始化消息在信号中被编码，该信号可以由用户的访问设备的用户输出接口输出，并且认证设备具有适于捕获该信号的数据输入接口。在这样的实施例中，认证设备可以使用不需要任何专用硬件或软件接口来与用户的安全装置进行通信

的访问设备来远程地初始化。为了初始化认证设备，访问设备还不需要不同于标准用户输出接口的任何其他接口来将数字数据发送至认证设备并且不需要任何接口来接收来自认证设备的数据。在一些实施例中，认证设备可以（针对特定用户的安全装置）仅偶尔接收初始化消息。在一些实施例中，认证设备可以（针对特定用户安全装置）仅接受初始化消息一次。在一些实施例中，认证设备的用于接收初始化消息的数据输入接口可以具有高数据速率以确保迅速传输任何初始化数据，这增强了用户的便利性。在一些实施例中，例如，在认证设备仅需要偶尔接收初始化消息的情况下，认证设备的用于接收初始化消息的数据输入接口可以具有低速度速率，这可以使得实现低成本并且在仅需要偶尔接收初始化消息的情况下，用户能接受低速率。

使用认证设备相关密钥对初始化消息的一些部分进行加密的优点

通过使用认证设备相关密钥对初始化消息的一些部分进行加密，可以确保仅访问了匹配解密密钥的认证设备能够对这些部分进行解密和使用。因此，通过使用认证设备相关密钥对初始化种子的一部分进行加密，从而仅一个特定认证设备或者特定组的认证设备需要访问对应的解密密钥，可以确保仅这些目标的认证设备可以获得初始化种子。这意味着意图暗中拦截初始化消息以及可以在某时间点处需要访问用户安全装置的攻击者仍然不能够获得初始化种子（例如，用于导出 OTP 生成密钥以欺骗地生成有效 OTP）。在每个认证设备已经使用其解密密钥的自身唯一的参数化的情况下尤其成立。在这种情况下，任何初始化消息仅可与其所针对的特定认证设备一起使用。请求初始化消息的任何人可以识别他 / 她的认证设备。如果攻击者请求多个初始化消息旨在与其自身的认证设备一起使用，然后，攻击者将必需识别其认证设备。这可以由例如欺骗检测机制使用来发现潜在的欺骗尝试（例如，如果针对相同的认证设备请求初始化消息的异常号码，或者如果针对黑名单的认证设备请求初始化消息）。

（借助于针对业务数据的 OTP 和动态 MAC）本发明能够确保远程应用，从而安全性是基于高安全性密码协议，然而，更特别地，受益于在用户的安全装置上的用户公钥 - 私人密钥对，不要求由用户使用的用于访问应用的访问设备适于与保存用户的公共 - 私人密钥对的用户安全装置进行通信。应用可以确保的是，不提供连接至用户安全装置或者甚至用户的认证设备的任何数字连接。

前文已经描述包括方法或者设备的若干方面或者实施例。在另一方面中，本发明包括在计算机可读介质上记录的指令序列，这些指令在由处理器执行时执行已经描述的那些方法。也可以通过数字网络如因特网来实现软件传送。因而在又一方面中本发明涵盖包括指令序列的信息承载信号，这些指令在由处理器执行时执行已经描述的那些方法。

应当理解，术语“包括 (comprises)/ 包括 (comprising)”当在本说明中使用时，意在指示状态特征、步骤或部件的存在，而不是排除一个或更多个其他特征、步骤、部件及其组的存在和添加。

虽然已经使用一些特性描述了本发明的若干实施例，但是应当理解，本描述为示例性的并且不是限制性的；本发明的范围由所附权利要求确定。

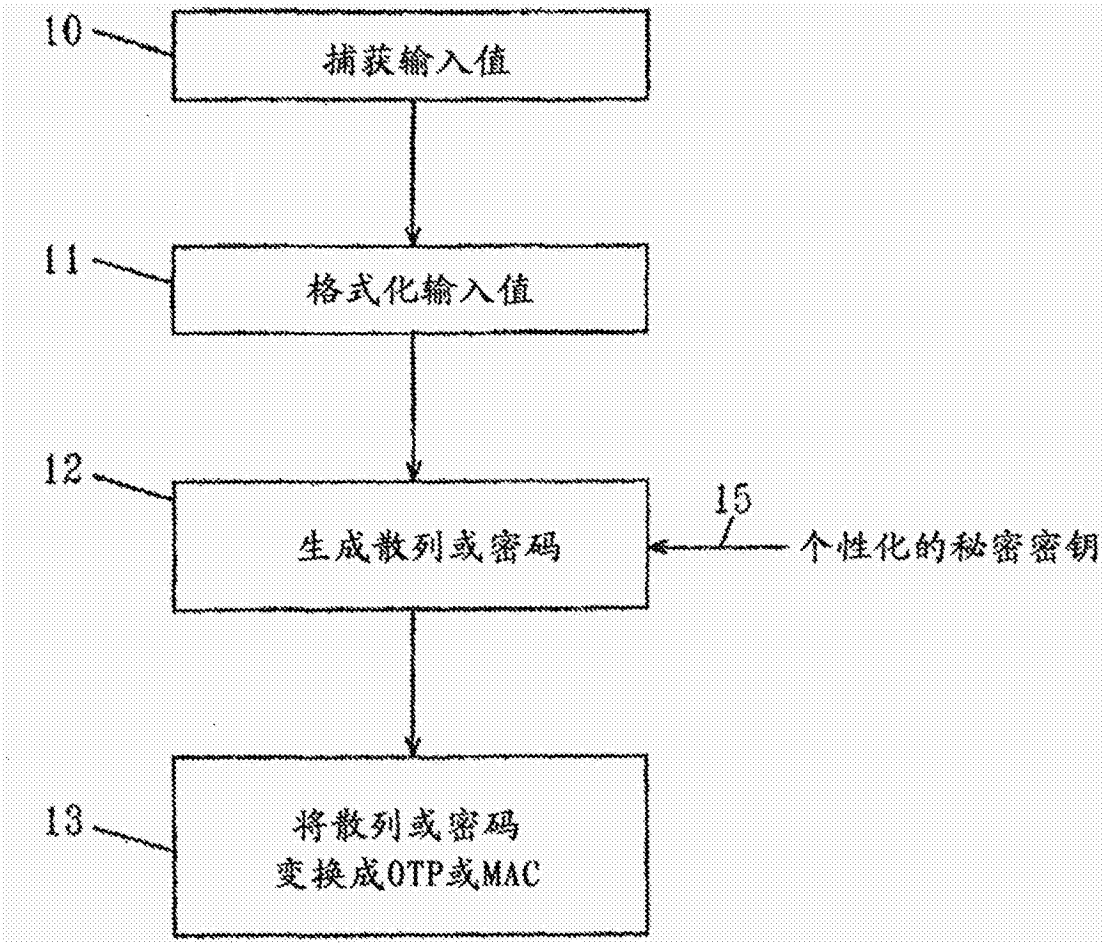

10
捕获输入值
11
格式化输入值
12
生成散列或密码
15
个性化的秘密密钥
13
将散列或密码
变换成OTP或MAC

图 1（现有技术）

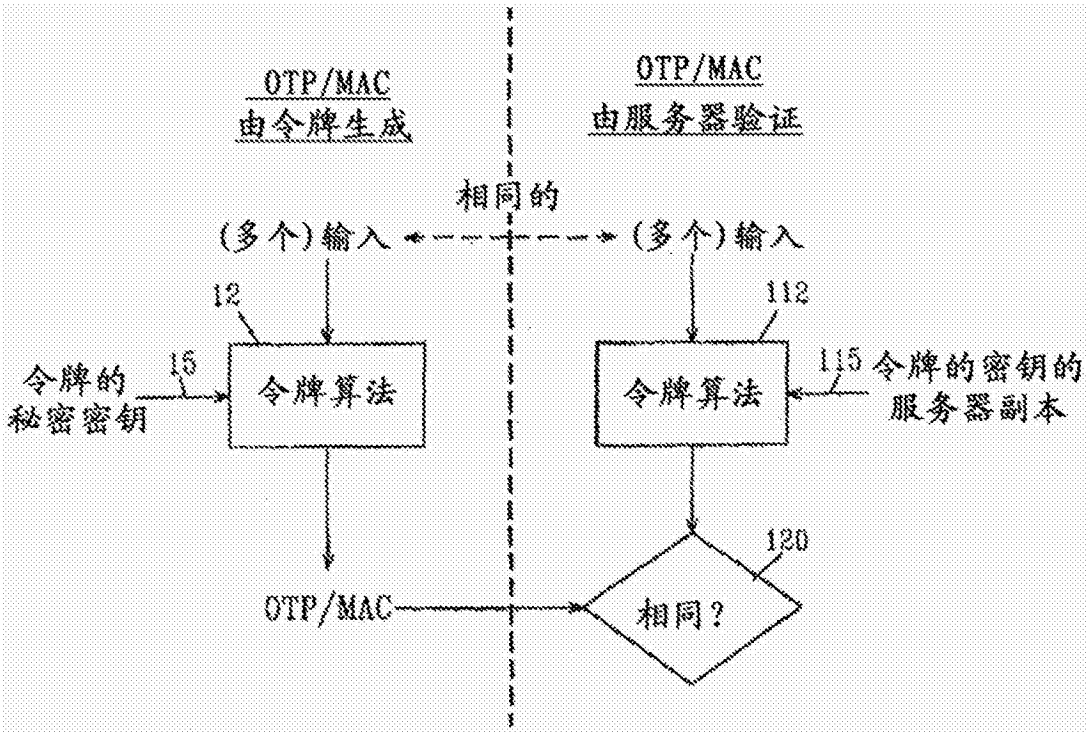

OTP/MAC
由令牌生成
OTP/MAC
由服务器验证
相同的
(多个)输入
(多个)输入
12
112
令牌的
秘密密钥
15
令牌算法
令牌算法
115
令牌的密钥的
服务器副本
120
OTP/MAC
相同?

图 2(现有技术)

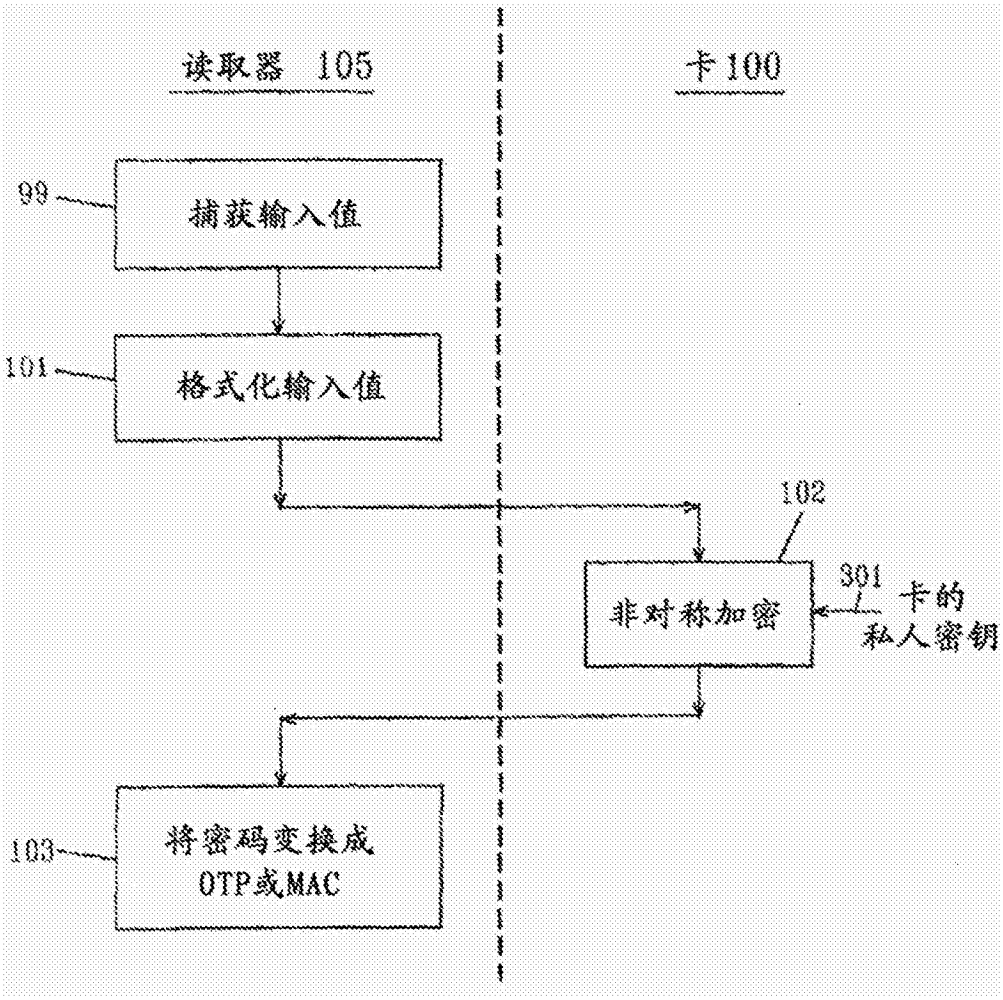

读取器 105
卡100
99
捕获输入值
101
格式化输入值
102
非对称加密
301
卡的
私人密钥
103
将密码变换成
OTP或MAC

图 3

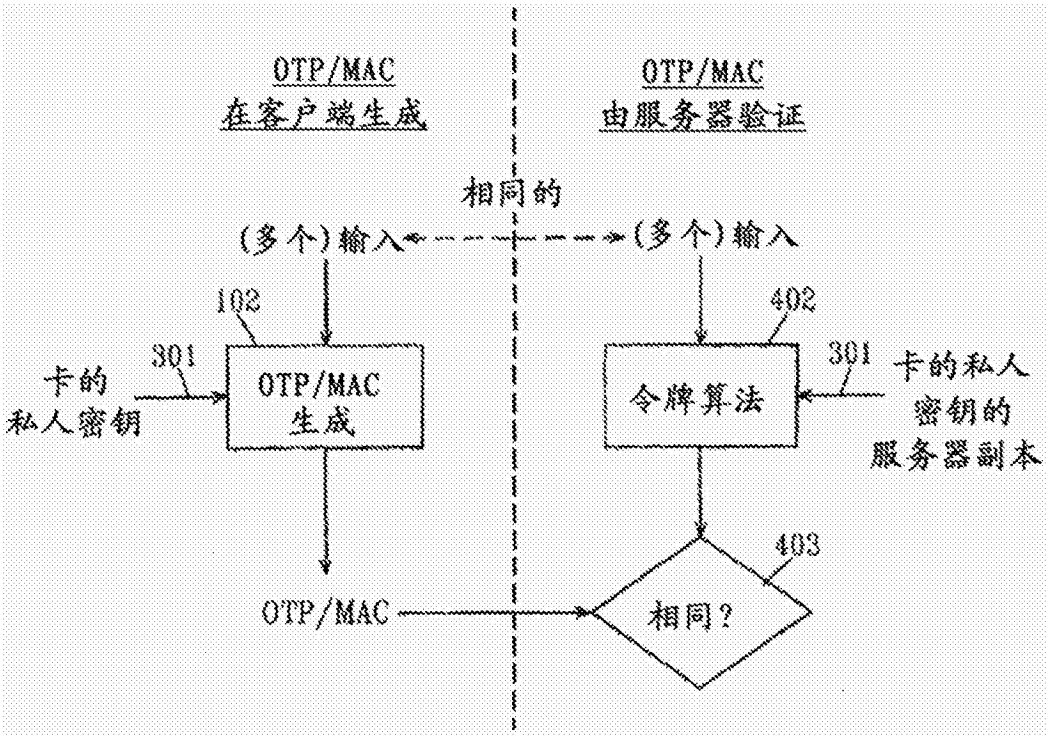

OTP/MAC
在客户端生成
OTP/MAC
由服务器验证
相同的
(多个)输入
(多个)输入
102
402
301
卡的
私人密钥
OTP/MAC
生成
令牌算法
301
卡的私人
密钥的
服务器副本
403
OTP/MAC
相同?

图 4

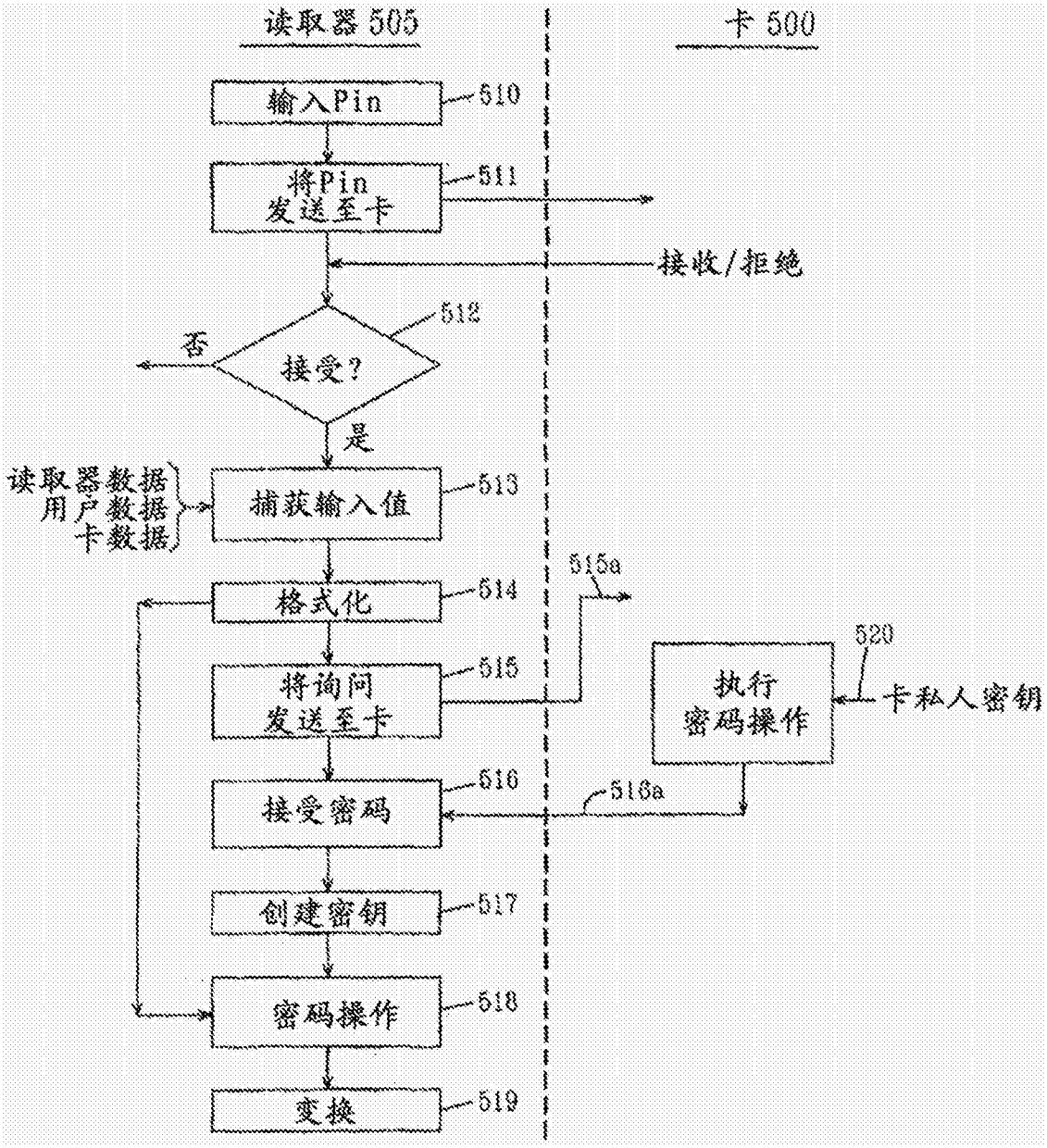

读取器505
卡500
输入Pin
510
将Pin
发送至卡
511
接收/拒绝
512
否
接受?
是
读取器数据
用户数据
卡数据
捕获输入值
513
格式化
514
515a
将询问
发送至卡
515
执行
密码操作
520
卡私人密钥
接受密码
516
516a
创建密钥
517
密码操作
518
变换
519

图 5

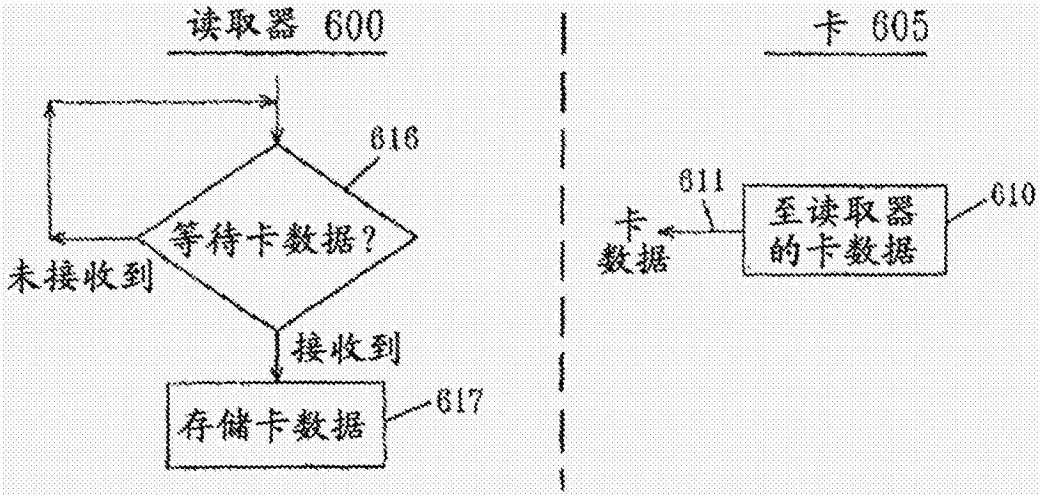

读取器 600
卡 605
616
等待卡数据?
未接收到
接收到
存储卡数据
617
611
卡
数据
至读取器
的卡数据
610

图 6

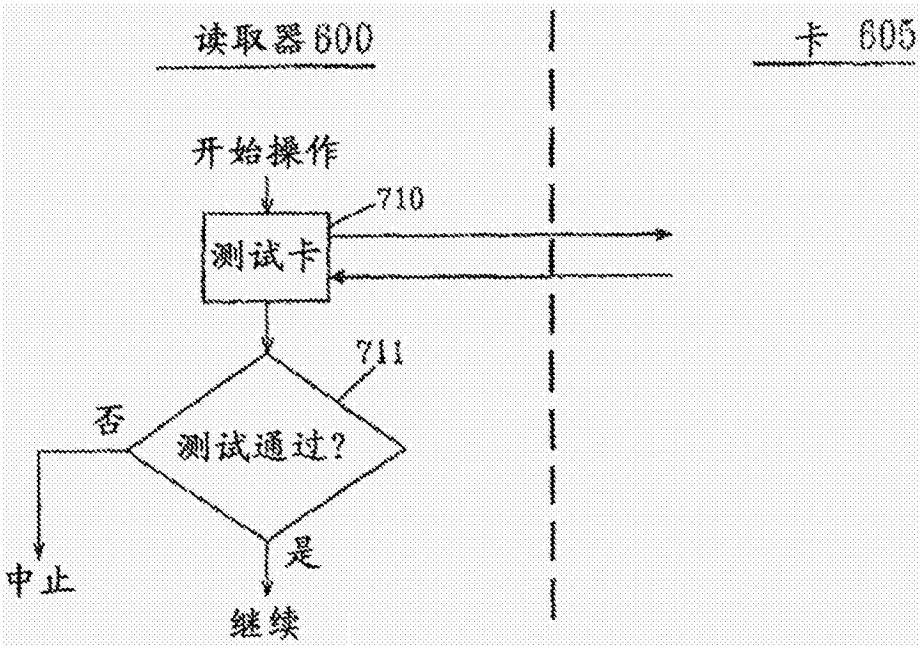

读取器600
卡 605
开始操作
710
测试卡
711
测试通过?
否
是
中止
继续

图 7

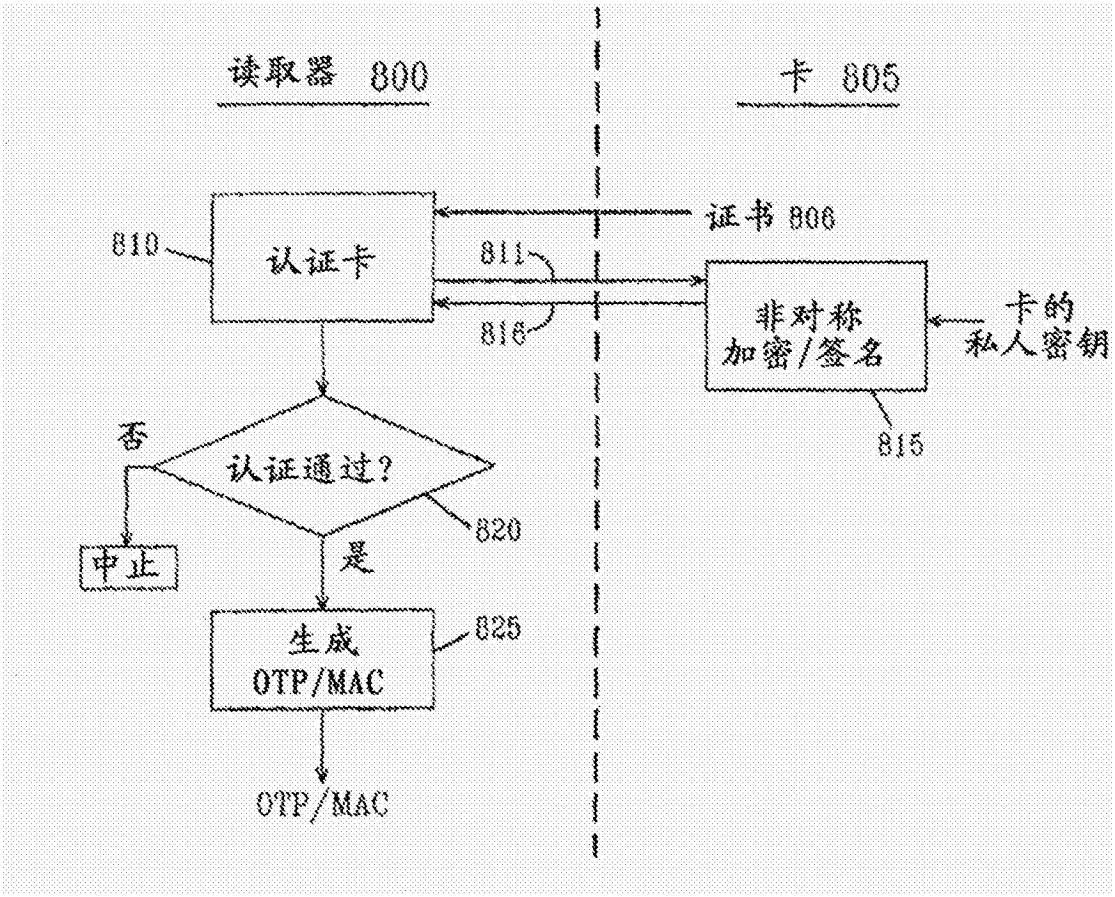

读取器 800
卡 805
证书 806
810
认证卡
811
816
非对称
加密/签名
卡的
私人密钥
815
否
认证通过?
820
中止
是
生成
OTP/MAC
825
OTP/MAC

图 8

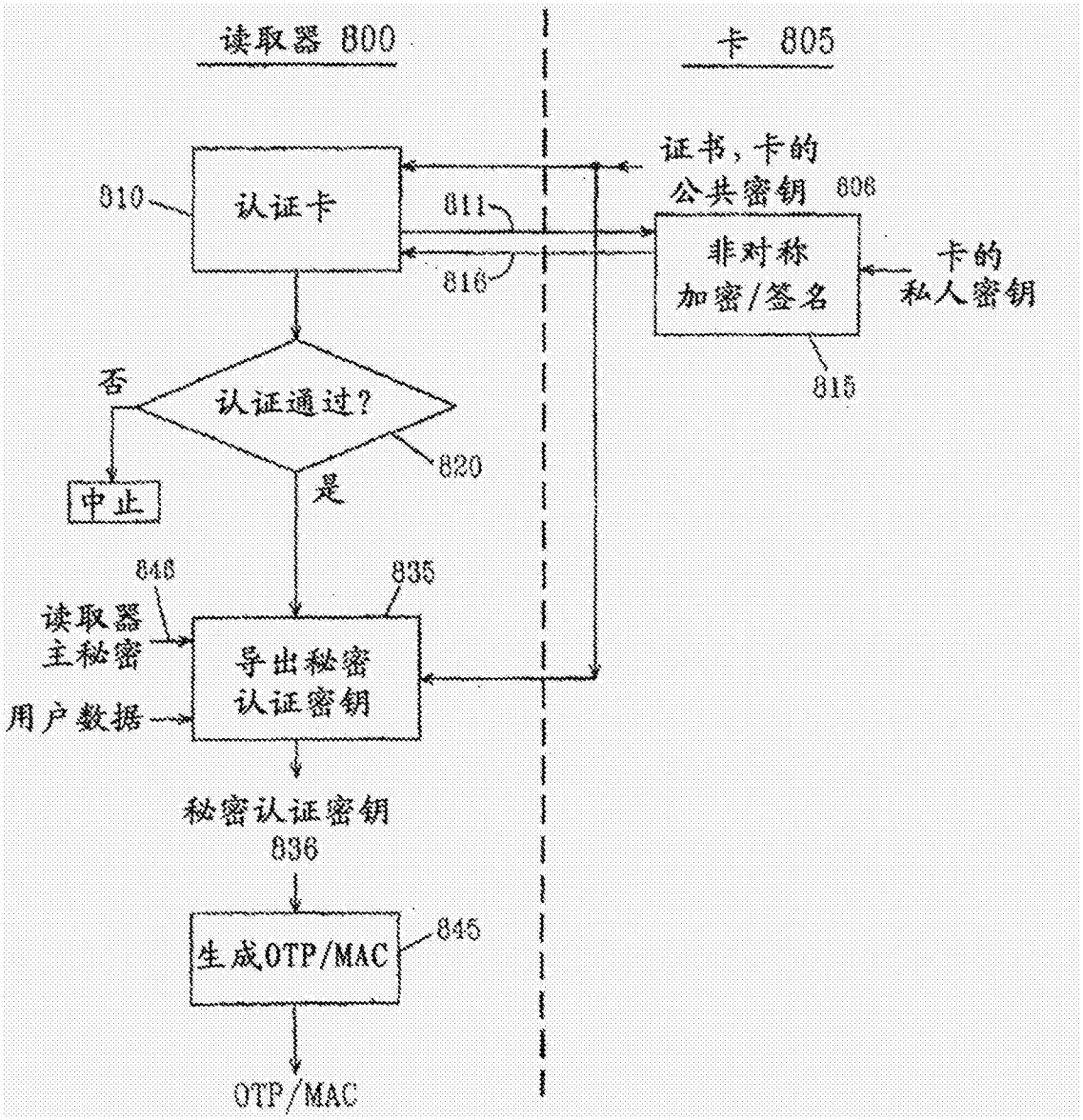

读取器 800
卡 805
证书，卡的
公共密钥 806
810
认证卡
811
816
非对称
加密/签名
卡的
私人密钥
815
否
认证通过？
820
是
中止
846
835
读取器
主秘密
用户数据
导出秘密
认证密钥
秘密认证密钥
836
生成OTP/MAC
845
OTP/MAC

图 9

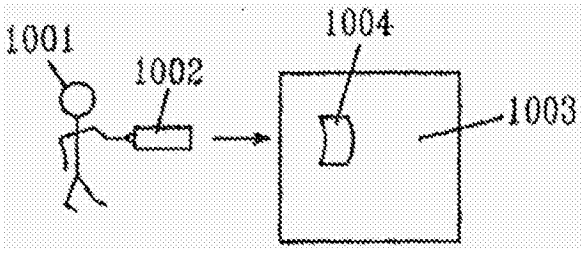

1001
1002
1004
1003

图 10

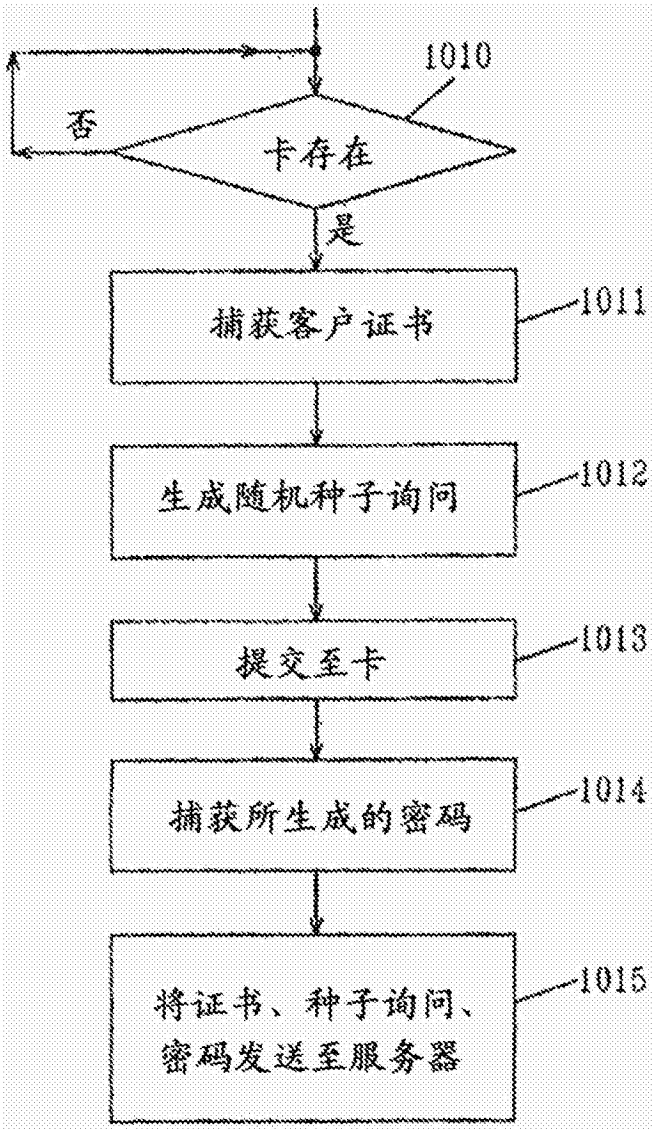

1010
否
卡存在
是
捕获客户证书
1011
生成随机种子询问
1012
提交至卡
1013
捕获所生成的密码
1014
将证书、种子询问、
密码发送至服务器
1015

图 11

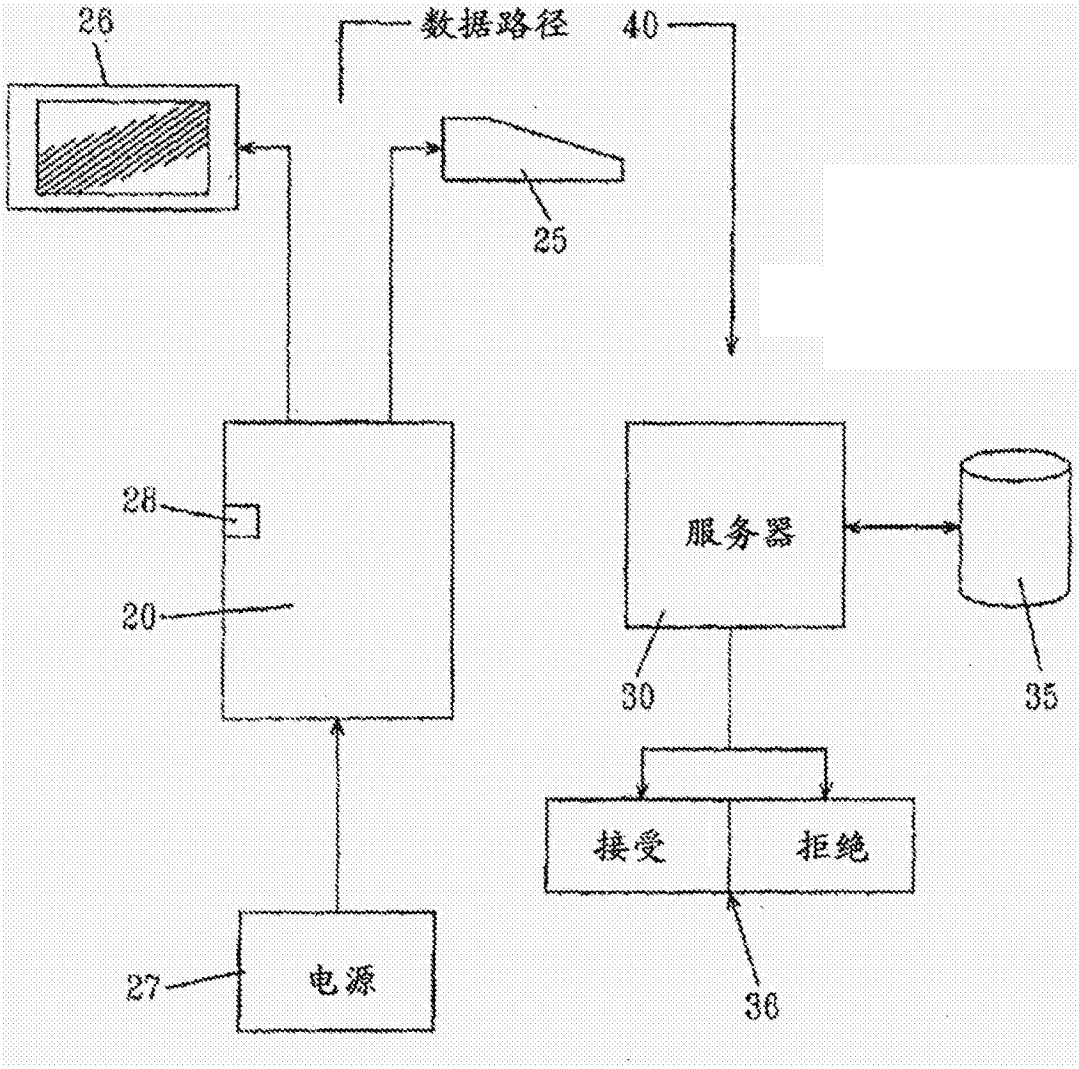


图 12

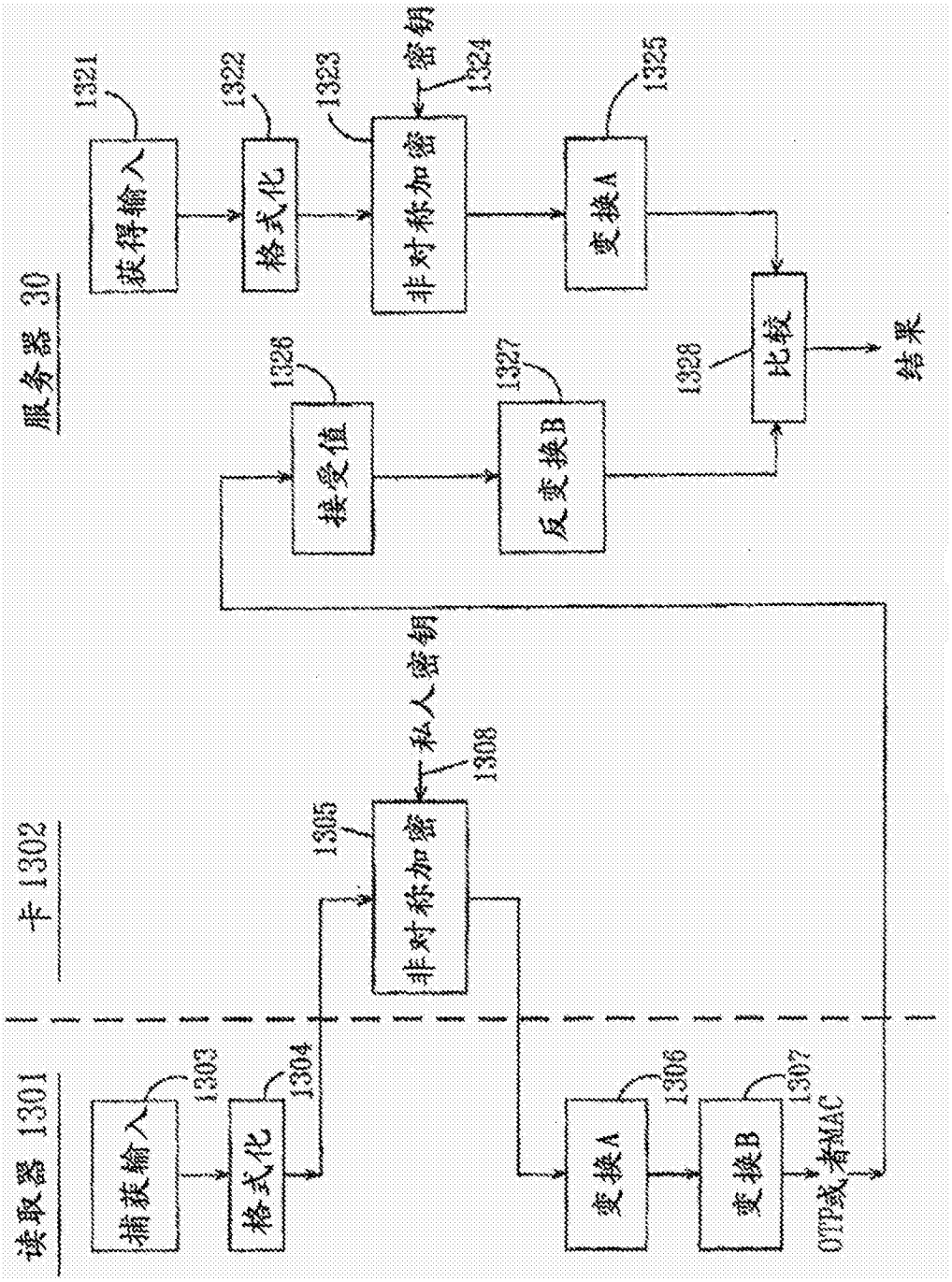

服务器 30
卡 1302
读取器 1301
获得输入
1321
格式化
1322
非对称加密
1323
密钥
1324
变换A
1325
比较
结果
1328
接受值
1326
反变换B
1327
私人密钥
1308
非对称加密
1305
捕获输入
1303
格式化
1304
变换A
1306
变换B
1307
OTP或者MAC

图 13

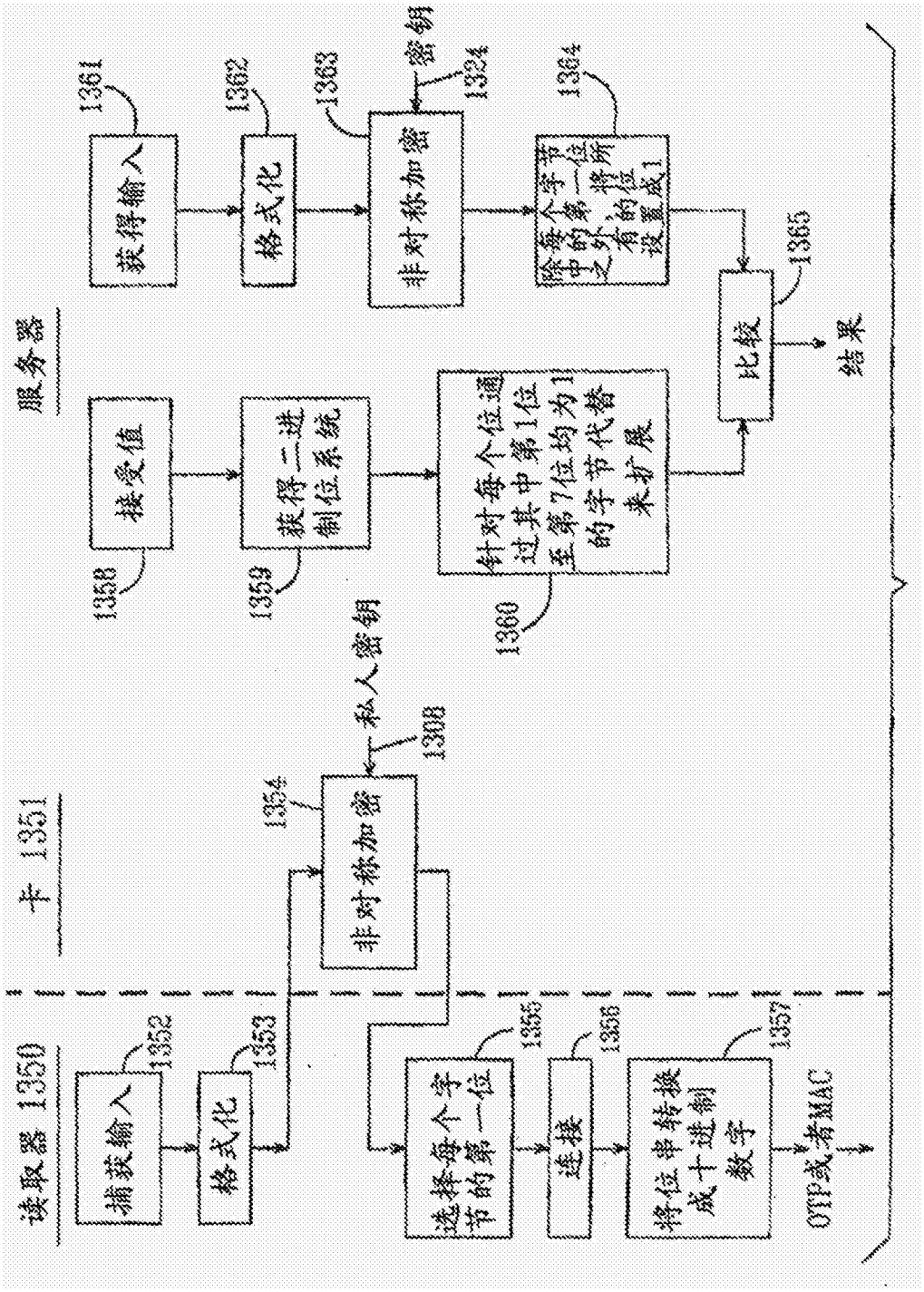

读取器 1350
卡 1351
服务器
捕获输入
1352
格式化
1353
非对称加密
1354
私人密钥
1308
选择每个字节的第一位
1355
连接
1356
将位串转换成十进制数字
1357
OTP或者MAC
接受值
1358
获得二进制位系统
1359
针对每个位通过其中第1位至第7位均为1的字节代替来扩展
1360
获得输入
1361
格式化
1362
非对称加密
1363
密钥
1324
除每个字节中的第一位之外的所有的位设置成1
1364
比较
1365
结果

图 14

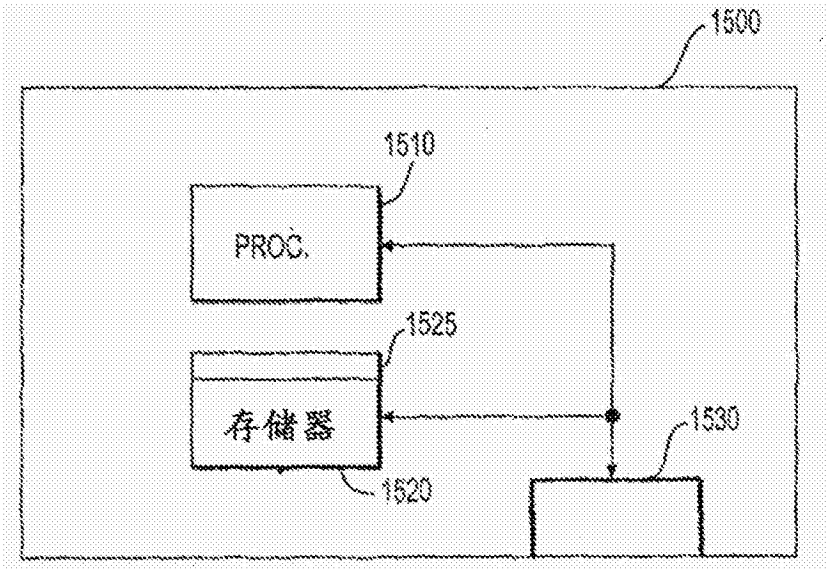

1500
1510
PROC.
1525
存储器
1530
1520

图 15

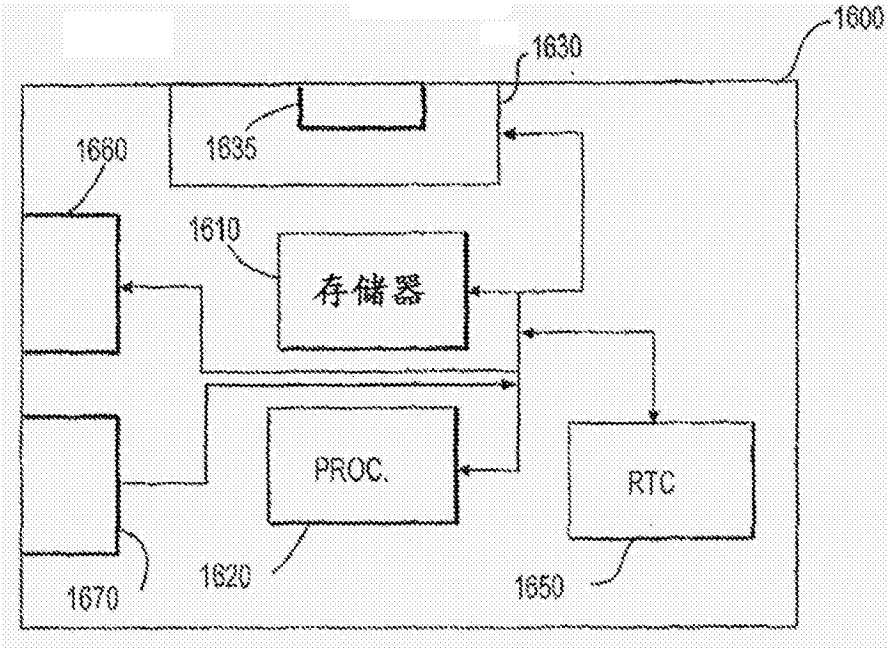

1600
1630
1635
1660
1610
存储器
PROC.
RTC
1620
1650
1670

图 16

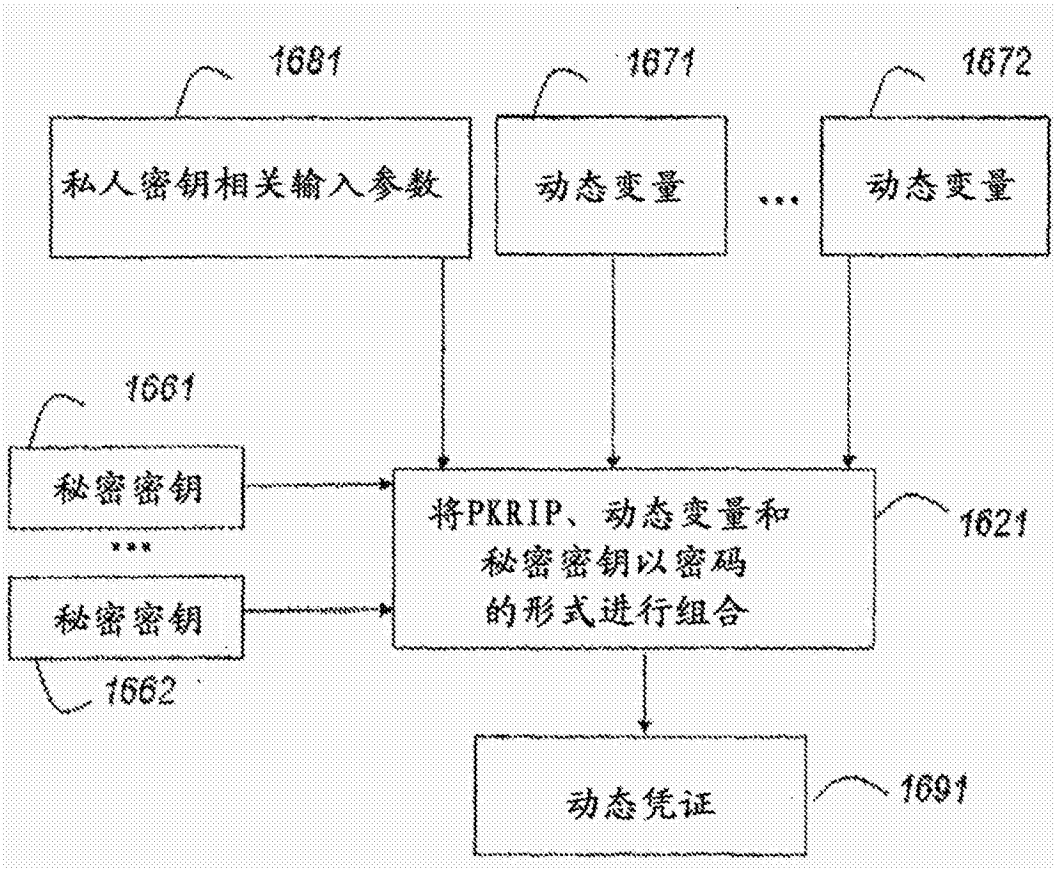

1681
1671
1672
私人密钥相关输入参数
动态变量
...
动态变量
1661
秘密密钥
...
秘密密钥
1662
将PKRIP、动态变量和
秘密密钥以密码
的形式进行组合
1621
动态凭证
1691

图 17

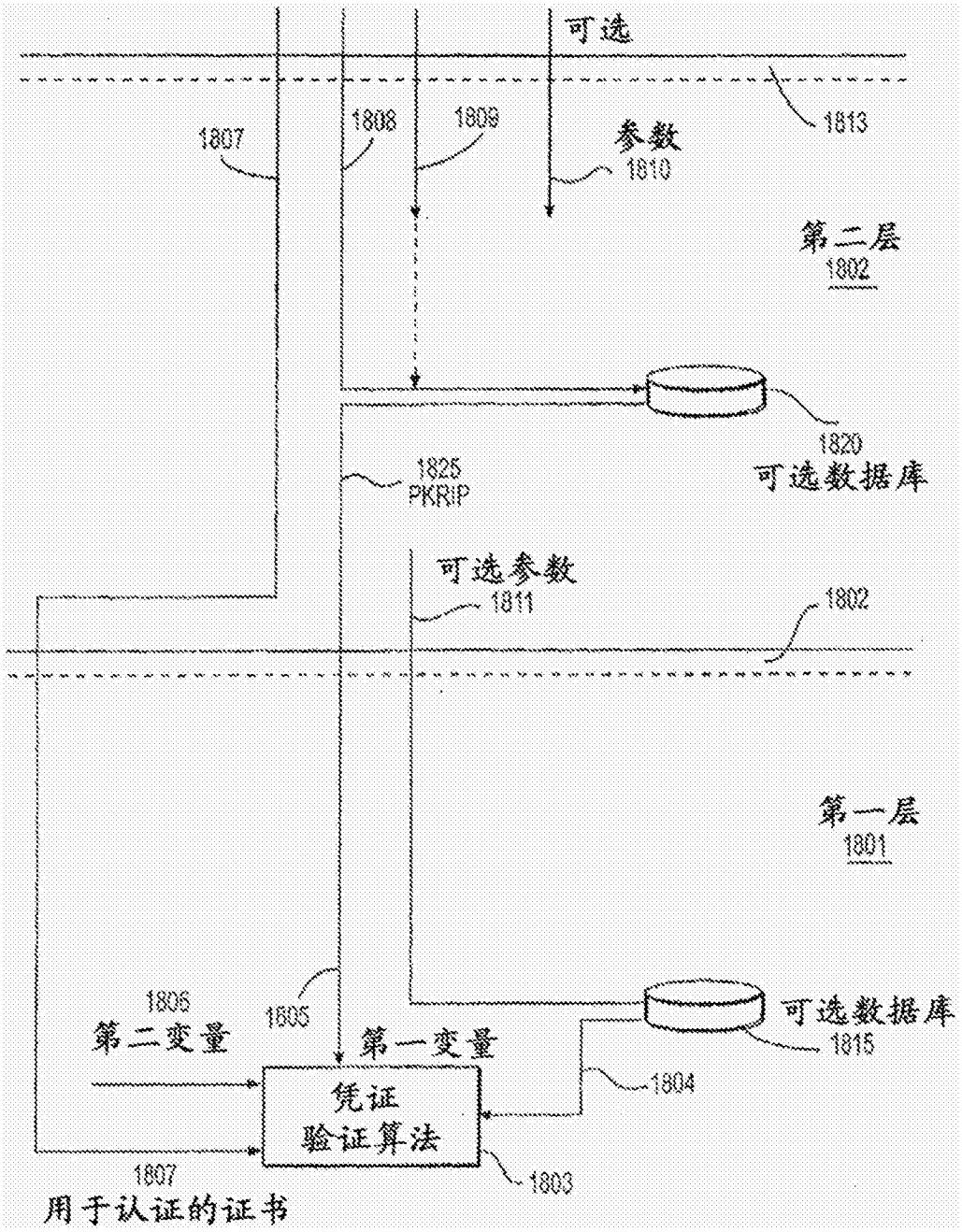

可选
1813
1807
1808
1809
参数
1810
第二层
1802
1820
可选数据库
1825
PKRIP
可选参数
1811
1802
第一层
1801
1806
第二变量
1805
第一变量
可选数据库
1815
凭证
验证算法
1804
1803
1807
用于认证的证书

图 18

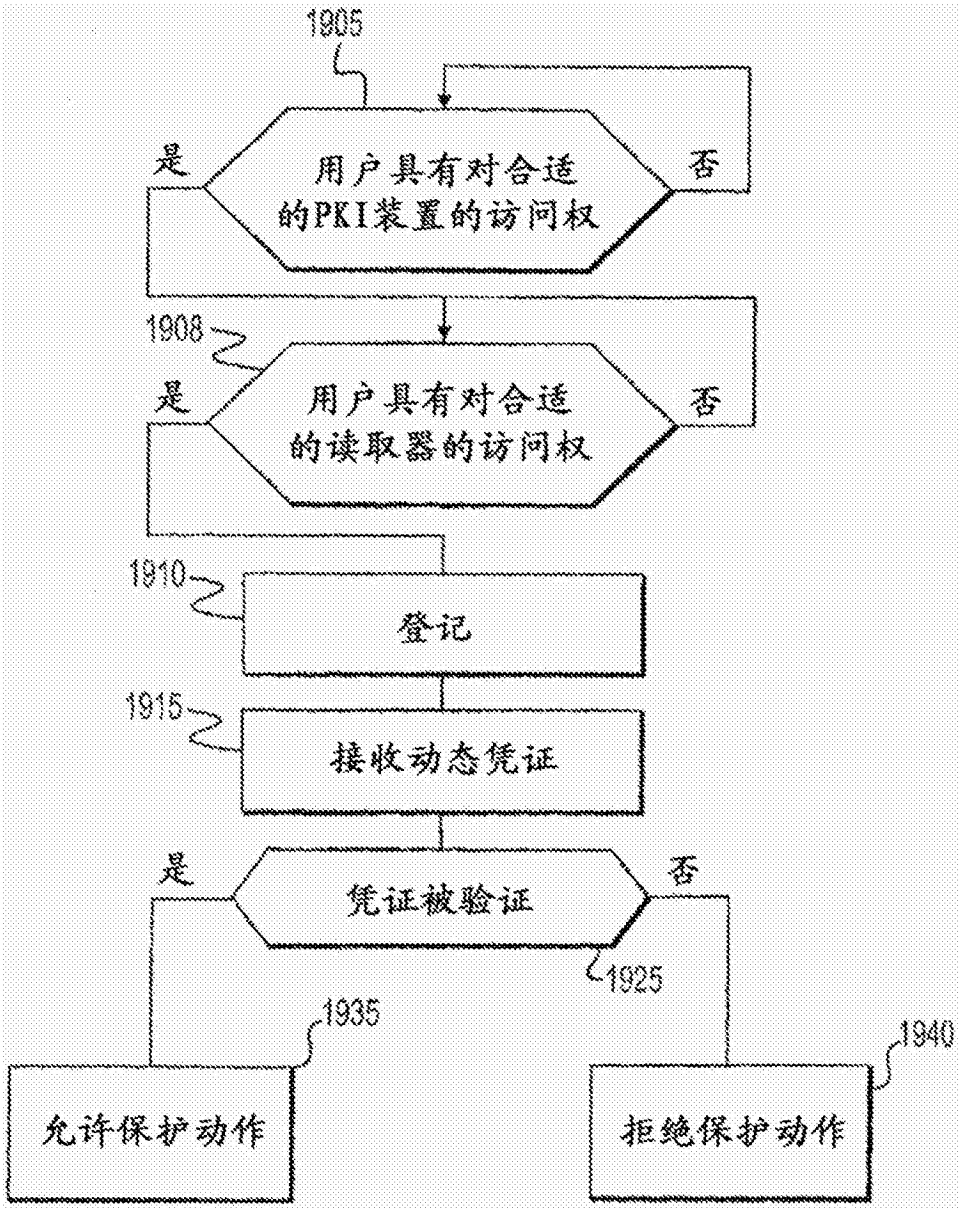

1905
用户具有对合适的PKI装置的访问权
是
否
1908
用户具有对合适的读取器的访问权
是
否
1910
登记
1915
接收动态凭证
凭证被验证
是
否
1925
1935
允许保护动作
1940
拒绝保护动作

图 19

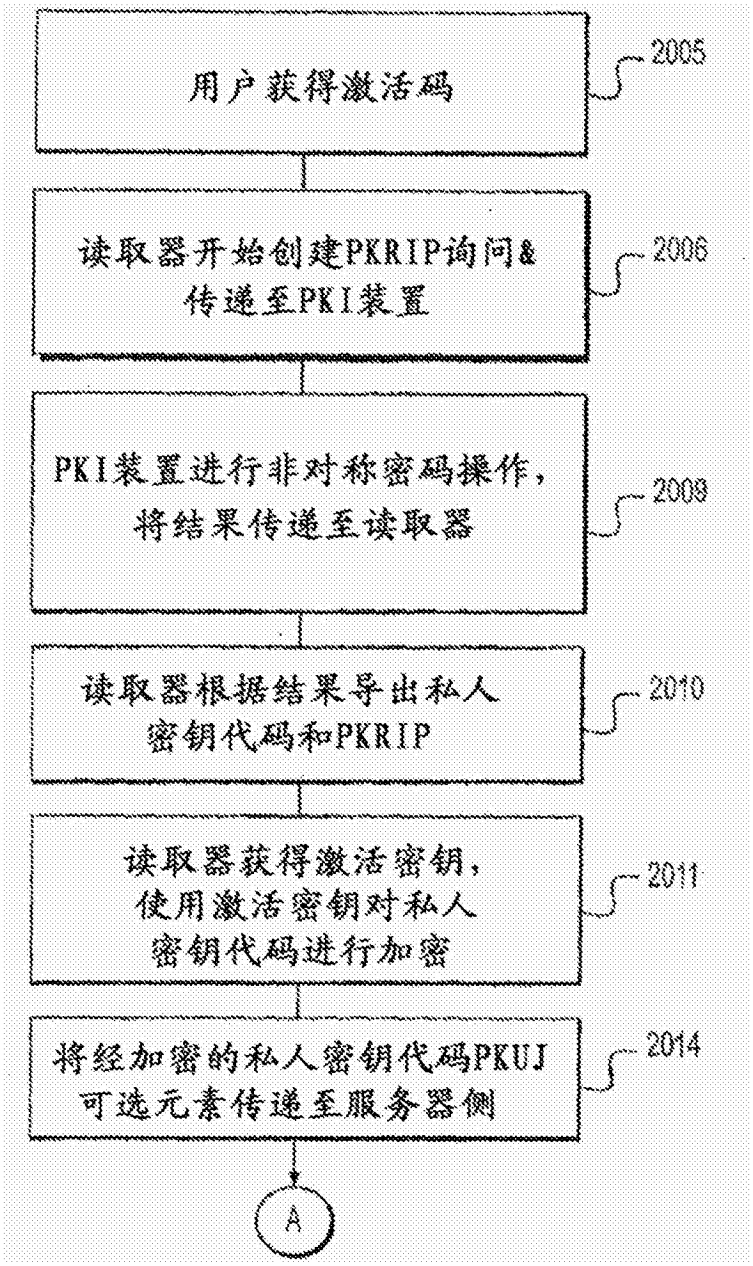

用户获得激活码
2005
读取器开始创建PKRIP询问&
传递至PKI装置
2006
PKI装置进行非对称密码操作，
将结果传递至读取器
2009
读取器根据结果导出私人
密钥代码和PKRIP
2010
读取器获得激活密钥，
使用激活密钥对私人
密钥代码进行加密
2011
将经加密的私人密钥代码PKUJ
可选元素传递至服务器侧
2014
A

图 20A

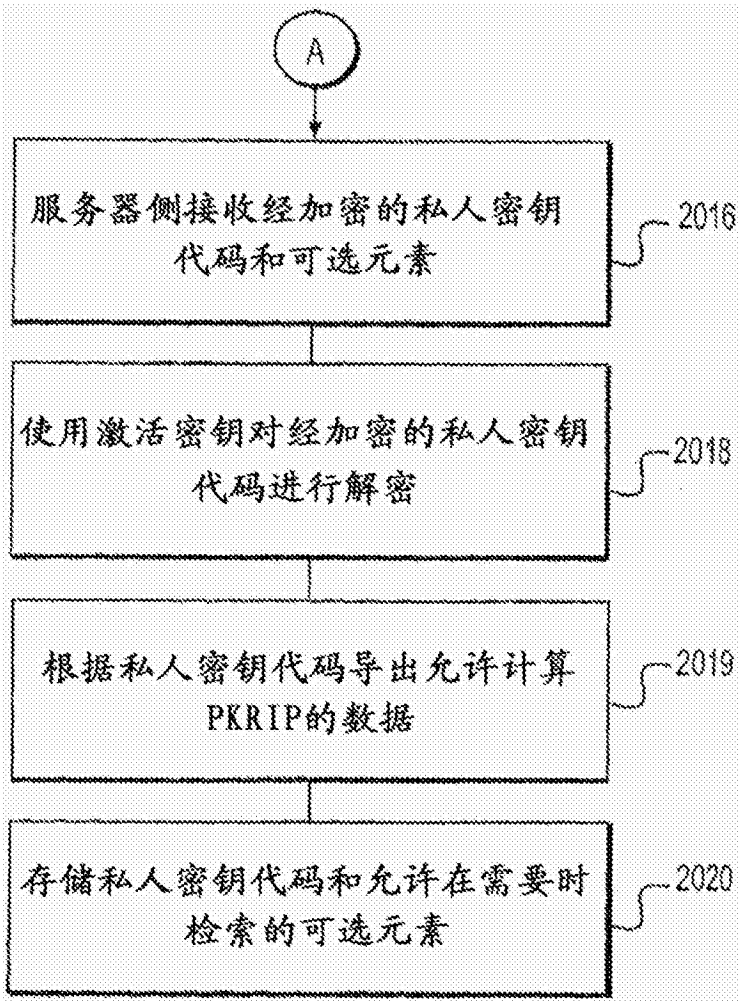

A
服务器侧接收经加密的私人密钥代码和可选元素
2016
使用激活密钥对经加密的私人密钥代码进行解密
2018
根据私人密钥代码导出允许计算PKRIP的数据
2019
存储私人密钥代码和允许在需要时检索的可选元素
2020

图 20B

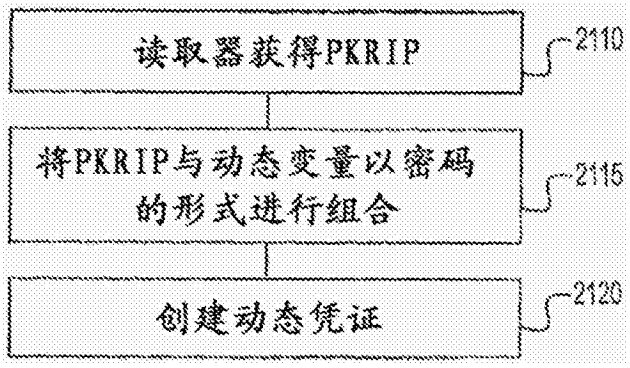

读取器获得PKRIP
2110
将PKRIP与动态变量以密码的形式进行组合
2115
创建动态凭证
2120

图 21

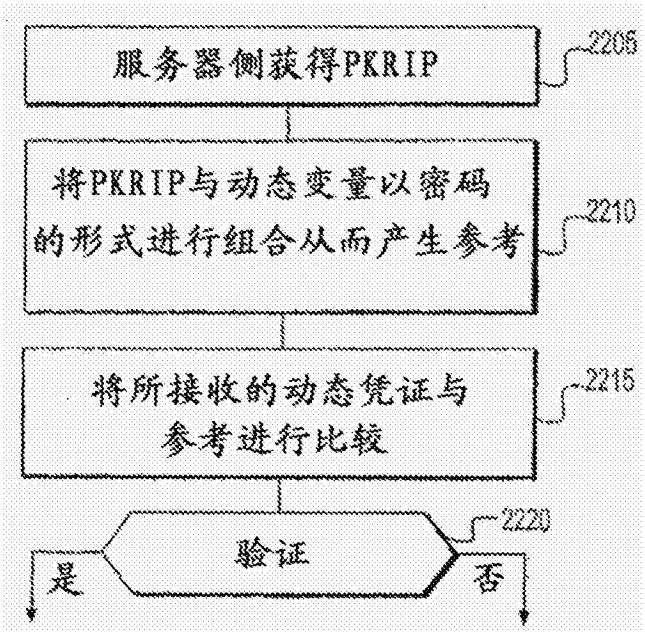

服务器侧获得PKRIP
2205
将PKRIP与动态变量以密码的形式进行组合从而产生参考
2210
将所接收的动态凭证与参考进行比较
2215
验证
2220
是
否

图 22

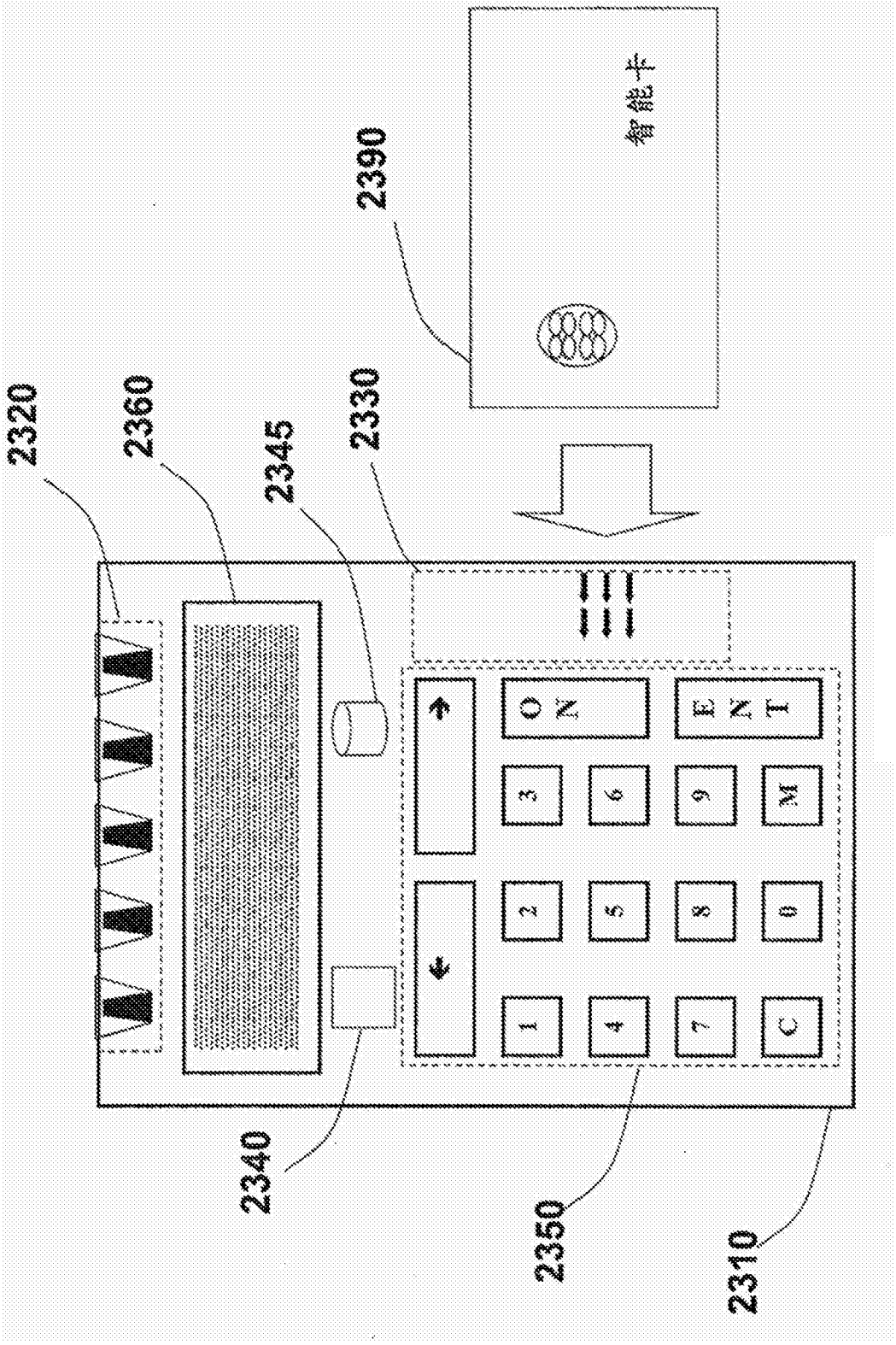

智能卡
2390
2320
2360
2345
2330
ON
ENT
3
6
9
M
2
5
8
0
1
4
7
C
2340
2350
2310

图 23

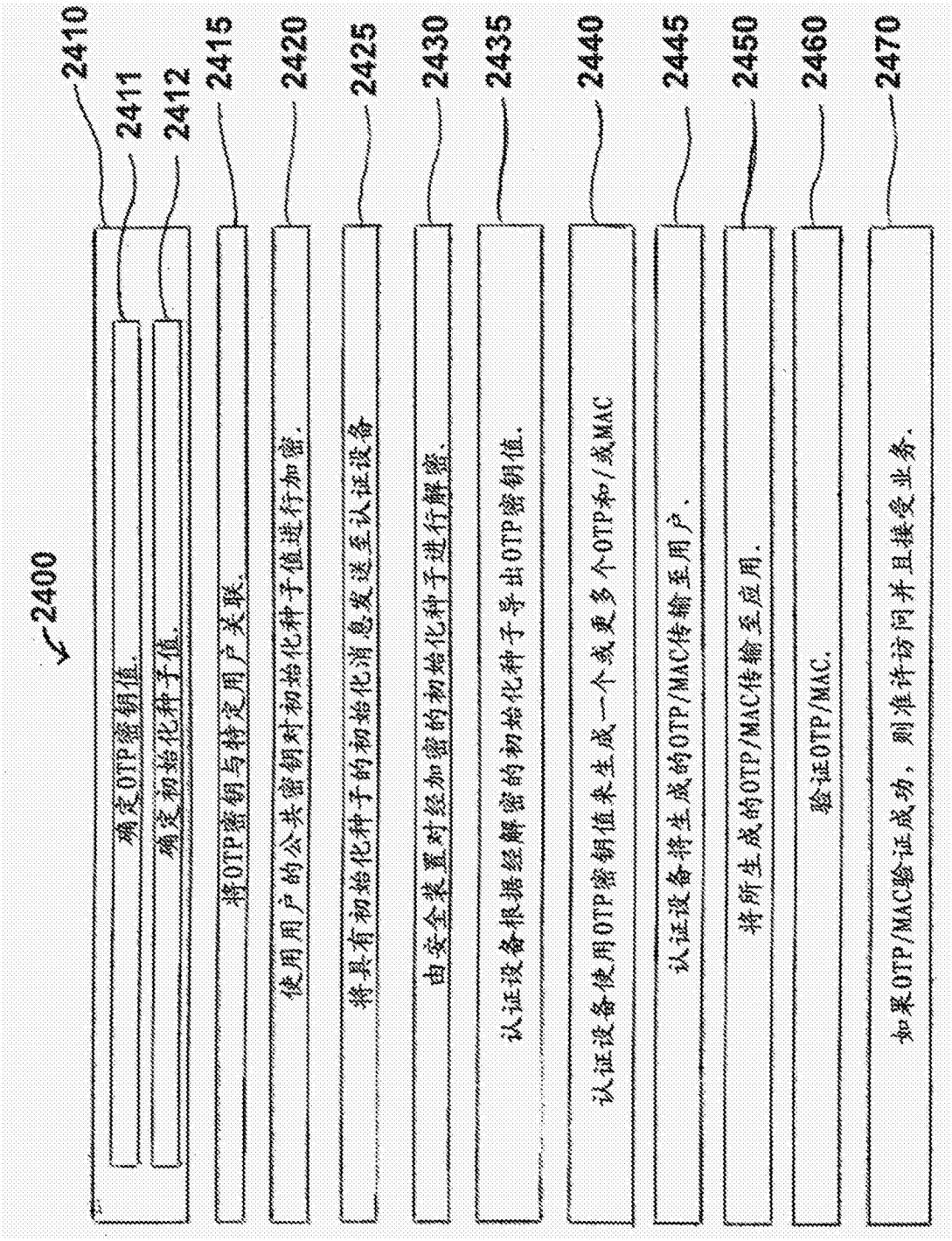

2400
2410
确定OTP密钥值.
2411
确定初始化种子值.
2412
2415
将OTP密钥与特定用户关联.
2420
使用用户的公共密钥对初始化种子值进行加密.
2425
将具有初始化种子的初始化消息发送至认证设备
2430
由安全装置对经加密的初始化种子进行解密.
2435
认证设备根据经解密的初始化种子导出OTP密钥值.
2440
认证设备使用OTP密钥值来生成一个或更多个OTP和/或MAC
2445
认证设备将生成的OTP/MAC传输至用户.
2450
将所生成的OTP/MAC传输至应用.
2460
验证OTP/MAC.
2470
如果OTP/MAC验证成功，则准许访问并且接受业务.

图 24