

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.  
H04L 12/22 (2006.01)



# [12] 发明专利说明书

专利号 ZL 02820572.3

[45] 授权公告日 2009年8月26日

[11] 授权公告号 CN 100534043C

[22] 申请日 2002.10.17 [21] 申请号 02820572.3  
[30] 优先权

[32] 2001.10.18 [33] US [31] 09/978,701

[32] 2002.1.22 [33] US [31] 10/051,249

[86] 国际申请 PCT/IB2002/004288 2002.10.17

[87] 国际公布 WO2003/034409 英 2003.4.24

[85] 进入国家阶段日期 2004.4.16

[73] 专利权人 诺基亚公司

地址 芬兰埃斯波

[72] 发明人 奥利·伊蒙恩 纳达拉扎·阿索肯  
帕努·S·玛卡恩

[56] 参考文献

US5621797B 1997.4.15

US6032260B 2000.2.21

审查员 庞 艳

[74] 专利代理机构 北京市中咨律师事务所  
代理人 杨晓光 李 峰

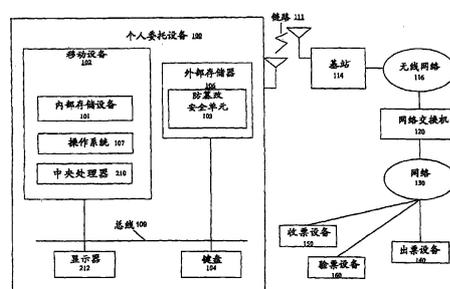
权利要求书 12 页 说明书 16 页 附图 6 页

[54] 发明名称

通信设备中保证票据安全的方法、系统

[57] 摘要

在通信设备中用于安全票据的方法，系统和计算机程序产品。该方法，系统和计算机程序产品使用密码系统和外部读-写保护单元，以便安全地传送和存储通信设备用户的关键数据。使用本发明能防止在不被第三方发觉的情况下欺骗性地使用第三方的服务。



1. 一种用于通信设备中的安全票据的系统，包括：
  - 包括第一存储设备的移动设备；
  - 包括第二存储设备的安全单元；
  - 至少一个第三方设备；以及与所述第一存储设备，所述第二存储设备和所述第三方设备通信的位于所述移动设备中的处理器，其被构造成：
  - 认证所述安全单元；
  - 创建并启动至少一个计数器，其被存储在所述安全单元的所述第二存储设备中；
  - 从所述第三方设备接收至少一个电子票据，并且在所述第一存储设备中存储所述至少一个电子票据；
  - 向所述至少一个第三方设备兑现存储在所述第一存储设备中的所述至少一个电子票据；以及
  - 更新所述第二存储设备中计数器的计数器值，以对应于所述电子票据向所述第三方设备的兑现；其中所述计数器值代表票据的使用数量。
2. 如权利要求 1 所述的系统，其中存储在所述第二存储设备中的所述计数器是单调增加的计数器，其包括对应于每个所存储电子票据的唯一标识和所关联的当前值。
3. 如权利要求 1 所述的系统，其中存储在所述第二存储设备中的计数器是单调减少的计数器，其包括对应于每个所存储电子票据的唯一标识和所关联的当前值。
4. 如权利要求 1 所述的系统，其中所述至少一个第三方设备发送的所述至少一个电子票据包括所述第二存储设备中的计数器的计数器值，其中计数器值由第三方设备确定为对应于第三方提供的服务的使用数量。

5. 如权利要求 1 所述的系统，其中所述第一存储设备是所述通信设备中的内部存储器设备，并且所述第二存储设备是由所述通信设备以可拆卸方式接纳的防篡改存储器设备。

6. 如权利要求 5 所述的系统，其中所述第二存储设备是电子卡，其被通信设备接纳。

7. 如权利要求 1 所述的系统，其中所述处理器是所述通信设备中的中央处理器。

8. 如权利要求 1 所述的系统，其中所述移动设备，安全单元和第三方设备之间的通信包括使用通信设备的操作系统执行多个协议，其中所述多个协议包括票据请求和存储协议，票据使用协议，以及验票协议。

9. 如权利要求 1 所述的系统，其中所述第二存储设备还包括生产商的证书，签名密钥对和加密密钥对。

10. 如权利要求 1 所述的系统，其中所述至少一个第三方设备还包括加密密钥对和签名密钥对。

11. 如权利要求 1 所述的系统，其中所述至少一个第三方设备还包括出票设备，收票设备，以及验票设备。

12. 如权利要求 1 所述的系统，其中所述至少一个第三方设备包括多个收票设备。

13. 如权利要求 1 所述的系统，其中通信设备包括蜂窝电话，卫星电话，个人数字助理，个人委托设备或者蓝牙设备。

14. 一种用于通信设备中的安全票据的方法，包括：

认证安全单元；

通过从移动设备发送在所述安全单元中创建计数器的请求，以及经由提供唯一计数器 ID 并初始化计数器中的值为零而在所述安全单元中创建计数器，在所述安全单元中创建并启动至少一个计数器；

向至少一个第三方设备请求至少一个电子票据；

在所述通信设备的存储设备中存储从所述至少一个第三方设备接收的所述至少一个电子票据；

向所述至少一个第三方设备兑现存储在所述存储设备中的所述至少一个电子票据;

更新所述安全单元中的计数器值以对应于所述电子票据向至少一个第三方设备的兑现;

其中所述计数器值代表票据的使用数量。

15. 如权利要求 14 所述的方法, 其中由所述至少一个第三方设备发送的所述电子票据包括所述安全单元中的计数器的计数器值, 其中由所述至少一个第三方设备确定计数器值为对应于第三方提供的服务的使用数量。

16. 如权利要求 14 所述的方法, 其中所述存储设备是通信设备中的内部存储器设备。

17. 如权利要求 14 所述的方法, 其中所述安全单元包括由所述通信设备以可拆卸方式接纳的防篡改读写存储器设备。

18. 如权利要求 14 所述的方法, 还包括在所述至少一个第三方设备中存储所述安全单元的公开密钥, 和在所述至少一个第三方设备中存储主密钥。

19. 如权利要求 14 所述的方法, 其中所述至少一个第三方设备包括出票设备, 收票设备, 以及验票设备。

20. 一种在系统中用于保证票据安全而请求, 创建和存储票据的方法, 该系统包括具有第一存储设备的移动设备, 具有安全单元的安全保护单元, 安全单元包括具有证书和一对加密密钥的第二存储设备, 以及至少一个第三方设备, 其具有密码主公开密钥并被构造成开出票据, 该方法包括:

认证所述安全单元;

通过从所述移动设备发送在所述安全单元中创建计数器的请求, 以及经由提供唯一计数器 ID 并初始化计数器中的值为零而在所述安全单元中创建计数器, 在所述安全单元中创建并启动至少一个计数器;

向所述第三方设备请求至少一个票据;

由所述第三方设备创建至少一个票据；  
从所述第三方设备接收至少一个票据；以及  
在所述第一存储设备中存储所接收的所述至少一个票据；  
其中所述计数器值代表票据的使用数量。

21. 如权利要求 20 所述的方法，其中所述认证安全单元的步骤包括：

所述移动设备向安全单元发送真实证书的请求；  
所述安全单元发送证书作为应答；  
所述移动设备接收所述证书；以及  
所述移动设备验证所接收的证书是否合格。

22. 如权利要求 20 所述的方法，其中所述创建和启动至少一个计数器的步骤包括：

所述移动设备发送在安全单元中创建计数器的请求；  
所述安全单元通过提供唯一计数器 ID 并初始化计数器为 0，来创建计数器；以及  
所述安全单元向所述移动设备发送所创建的计数器 ID。

23. 如权利要求 20 所述的方法，其中所述请求至少一个票据的步骤包括：

所述移动设备向所述第三方设备发送：  
从所述安全单元接收的新创建的计数器 ID；  
安全单元的证书；以及  
安全单元的公开密钥。

24. 如权利要求 20 所述的方法，其中创建至少一个票据的步骤包括：

所述第三方设备从移动设备接收计数器 ID，安全单元的证书，以及安全单元的公开密钥；

所述第三方设备通过在认证方数据上形成签名来创建至少一个票据，该认证方数据包括接收的计数器 ID，所述第三方设备的公开密钥，

代表票据的容许使用数量的数、以及附加信息；

所述第三方设备生成与所接收的计数器 ID 相关的消息认证密钥；以及

所述第三方设备通过用安全单元的所述公开密钥加密所接收的计数器 ID 以及所产生的消息认证密钥，创建加密密钥。

25. 如权利要求 20 所述的方法，其中所述接收至少一个票据的步骤包括：

所述移动设备接收所述第三方设备创建的至少一个票据，所述票据是认证方数据上的签名，所述认证方数据包括所接收的计数器 ID，所述第三方设备的公开密钥，代表票据的容许使用数量的数，以及附加信息；以及所述移动设备接收所述第三方设备通过用安全单元的公开密钥加密所接收的计数器 ID 以及相关消息认证密钥而创建的加密密钥。

26. 如权利要求 20 所述的方法，其中所述存储至少一个票据的步骤包括：

所述移动设备在所述第一存储设备中存储所接收的由所述第三方设备创建的至少一个票据，所述票据是认证方数据上的签名，所述认证方数据包括所接收的计数器 ID，所述第三方设备的公开密钥，代表票据的容许使用数量的数，以及附加信息；

所述移动设备向所述安全单元传送所接收的，由所述第三方设备通过用安全单元的公开密钥加密所接收的计数器 ID，以及第三方设备生成并与计数器 ID 关联的消息认证密钥而创建的加密密钥；

所述安全单元由所接收的加密密钥恢复出消息认证密钥；

所述安全单元存储消息认证密钥并将其与计数器 ID 相关联；以及所述安全单元向移动设备发送确认。

27. 一种在用于票据安全的系统中使用票据的方法，该系统包括：

具有第一存储设备的移动设备，在第一存储设备中存储有票据；具有安全单元的安全保护单元，该安全单元包括第二存储设备，第二存储设备具有证书，一对加密密钥和涉及所存储票据的至少一个计数器，计

数器具有唯一计数器 ID，计数器值以及消息认证密钥；以及至少一个第三方设备，第三方设备具有密码主公开密钥，所述第三方设备被构造成兑现票据，该票据是认证方数据上的签名，所述认证方数据包括计数器 ID，所述第三方设备的公开密钥，代表票据的容许使用数量的数，以及附加信息，该方法包括：

所述移动设备向所述第三方设备发送所存储的票据以便兑现；

所述第三方设备检查所接收票据的有效性；

如果票据被认为有效，所述第三方设备向所述移动设备发送质询；

通过发送对应的计数器 ID 和所接收的质询，针对涉及要兑现的票据的计数器，所述移动设备在所述安全单元中启动计数器更新；

所述安全单元用所述第三方设备规定的值更新所述计数器；

所述安全单元产生授权令牌，该授权令牌是使用存储在计数器中的消息认证密钥计算得到的消息认证码；

所述安全单元向所述移动设备发送所产生的授权令牌；

所述移动设备向所述第三方设备传送所接收的授权令牌；

所述第三方设备使用所接收票据中的密钥验证所接收的授权令牌；

以及

所述第三方设备对比票据中的容许使用数量检查计数器的当前值，并向移动设备发送对应于检查结果的消息；

其中所述计数器值代表票据的使用数量。

28. 如权利要求 27 所述的方法，其中所接收票据的有效性的检查包括验证票据上的签名，和票据中附加信息的有效性检查。

29. 如权利要求 27 所述的方法，其中对应于计数器值检查结果的消息是被证实有效的票据，其作为认证方数据上的签名，所述认证方数据包括全部从所接收的授权令牌获得的所述计数器 ID，所述公开密钥和所述当前计数器值，以及附加信息。

30. 如权利要求 27 所述的方法，还包括在第一存储设备中存储所接收的被证实有效的票据。

31. 如权利要求 27 所述的方法，还包括：

所述移动设备接收作为计数器值检查结果的消息，其表明票据被完全使用；

所述移动设备向所述安全单元发送请求以删除所述计数器；以及作为应答，所述安全单元回送删除计数器请求的结果。

32. 如权利要求 27 所述的方法，其中票据是多用途票据，该方法包括；

向第三方设备发送所存储的票据，其中也向第三方设备发送所存储的被证实有效的票据，并且使用在被证实有效的票据中的附加信息进行存取控制。

33. 一种在用于安全票据的系统中检查票据的方法，该系统包括：

具有第一存储设备的移动设备，在第一存储设备中存储有票据；具有安全单元的安全保护单元，该安全单元包括第二存储设备，第二存储设备具有证书，一对加密密钥和涉及所存储票据的至少一个计数器，计数器被创建成具有唯一计数器 ID，并且被初始化从而具有计数器值为零以及消息认证密钥；以及至少一个第三方设备，第三方设备具有密码主公开密钥，所述第三方设备被构造成检查票据，该票据是认证方数据上的签名，所述认证方数据包括计数器 ID，所述第三方设备的公开密钥，代表票据的容许使用数量的数，以及附加信息，该方法包括：

所述移动设备向所述第三方设备发送所存储的票据以便检查；

所述第三方设备检查所接收票据的有效性；

所述第三方设备向所述移动设备发送质询；

通过发送对应的计数器 ID 和所接收的质询，针对涉及要检查的票据的计数器，所述移动设备在所述安全单元中启动计数器读取；

所述安全单元产生授权令牌，该授权令牌是使用存储在计数器中的消息认证密钥计算得到的消息认证码；

所述安全单元向所述移动设备发送所产生的授权令牌；

所述移动设备向所述第三方设备传送所接收的授权令牌；以及

所述第三方设备通过使用所接收票据中的密钥验证所接收的授权令牌，并且向所述移动设备发送指示验证结果的消息；

所述移动设备接收作为检查计数器值的结果的消息，该计数器值表示该票据被完全使用；

所述移动设备向所述安全单元发送删除所述计数器的请求；

所述安全单元返回所述删除计数器请求的结果作为响应；

其中所述计数器值代表票据的使用数量。

34. 一种用于票据系统的安全系统，包括：

具有第一存储设备的装置；

连接到第一存储设备的安全保护单元，所述安全保护单元具有包括第二存储设备的安全单元，第二存储设备具有一对加密密钥和证书，以及在所述安全单元中的至少一个计数器，该计数器包括唯一计数器 ID 和计数器值；

通过从所述装置发送在所述安全单元中创建计数器的请求，以及经由提供唯一计数器 ID 并初始化计数器中的值为零而在所述安全单元中创建计数器，来创建所述计数器；

至少部分被存储在所述第一存储设备中的至少一个票据，其具有关于安全单元的加密密钥之一，计数器 ID 的信息；以及

所述装置向安全单元发送请求，以便在安全单元中计数器 ID 所标识的各计数器中通过递增或递减对应于所述票据的使用的计数器值来更新所述计数器；

其中所述计数器值代表票据的使用数量。

35. 一种在系统中用于保证票据安全而请求，创建和存储票据的方法，该系统包括具有第一存储设备的移动设备，具有安全单元的安全保护单元，该安全单元包括第二存储设备，第二存储设备具有证书和一对加密密钥，以及至少一个被构造成开出票据的第三方设备，该方法包括：

认证所述安全单元；

通过从所述移动设备发送在所述安全单元中创建计数器的请求，以及经由提供唯一计数器 ID 并初始化计数器中的值为零而在所述安全单元中创建计数器，在所述安全单元中创建至少一个计数器；

向所述第三方设备请求至少一个票据；

由所述第三方设备创建至少一个票据；

从所述第三方设备接收至少一个票据；以及

在第一存储设备中存储所接收的所述至少一个票据；

其中所述计数器值代表票据的使用数量。

36. 如权利要求 35 所述的方法，其中所述认证安全单元的步骤包括步骤：

所述移动设备向安全单元发送真实证书的请求；

所述安全单元发送证书作为应答；

所述移动设备接收所述证书；以及

所述移动设备验证所接收的证书是否合格。

37. 如权利要求 35 所述的方法，其中创建至少一个计数器的步骤包括：

所述移动设备发送在安全单元中创建计数器的请求；

所述安全单元通过提供唯一计数器 ID 并初始化计数器为 0，来创建计数器；以及

所述安全单元向所述移动设备发送所创建的计数器 ID。

38. 如权利要求 35 所述的方法，其中所述请求至少一个票据的步骤包括：

所述移动设备向所述第三方设备发送从所述安全单元接收的新创建的计数器 ID，安全单元的证书，以及安全单元的公开密钥。

39. 如权利要求 35 所述的方法，其中所述第三方设备创建至少一个票据的步骤包括：

从移动设备接收计数器 ID，安全单元的证书，以及安全单元的公开密钥；

通过在认证方数据上形成签名来创建至少一个票据，所述认证方数据包括所接收的计数器 ID，所接收的公开密钥，代表票据的容许使用数量的数，以及附加信息。

40. 如权利要求 35 所述的方法，其中接收至少一个票据的步骤包括：

所述移动设备接收所述第三方设备创建的至少一个票据，该票据是认证方数据上的签名，所述认证方数据包括所接收的计数器 ID，所接收的公开密钥，代表票据的容许使用数量的数，以及附加信息。

41. 如权利要求 35 所述的方法，其中所述存储至少一个票据的步骤包括：

在所述第一存储设备中存储所接收的由所述第三方设备创建的至少一个票据，该票据是认证方数据上的签名，所述认证方数据包括所接收的计数器 ID，所接收的公开密钥，代表票据的容许使用数量的数，以及附加信息。

42. 一种在用于安全票据的系统中使用票据的方法，该系统包括具有第一存储设备的移动设备，在第一存储设备中存储有票据；具有安全单元的安全保护单元，安全单元包括第二存储设备，第二存储设备具有证书，一对加密密钥和涉及所存储票据的至少一个计数器，所述计数器被创建成具有唯一计数器 ID 并且被初始化为具有为零的计数器值；以及至少一个第三方设备，第三方设备被构造成兑现票据，所述票据是认证方数据上的签名，所述认证方数据包括计数器 ID，安全保护单元的公开密钥，代表票据的容许使用数量的数，以及附加信息，该方法包括：

所述移动设备向所述第三方设备发送所存储的票据以便兑现；

所述第三方设备检查所接收票据的有效性；

如果票据被认为有效，所述第三方设备向所述移动设备发送质询；

通过发送对应的计数器 ID 和所接收的质询，针对涉及要兑现的票据的计数器，所述移动设备在所述安全单元中启动计数器更新；

所述安全单元用所述第三方设备规定的值更新所述计数器；

所述安全单元生成作为认证方数据上的签名的授权令牌，所述认证方数据包括所述计数器 ID，计数器的当前值，以及安全单元的公开密钥；

所述安全单元向所述移动设备发送所产生的授权令牌；

所述移动设备向所述第三方设备传送所接收的授权令牌；

所述第三方设备使用所接收票据中的密钥验证所接收的授权令牌；

以及

所述第三方设备对比票据中的容许使用数量检查计数器的当前值，并向移动设备发送对应于检查结果的消息；

所述移动设备接收作为检查计数器值的结果的消息，该计数器值表示该票据被完全使用；

所述移动设备向所述安全单元发送删除所述计数器的请求；

所述安全单元返回所述删除计数器请求的结果作为响应；

其中所述计数器值代表票据的使用数量。

43. 如权利要求 42 所述的方法，其中所接收票据的有效性的检查包括验证票据上的签名，和票据中附加信息的有效性检查。

44. 如权利要求 42 所述的方法，其中对应于计数器值检查结果的消息是被证实有效的票据，该票据是认证方数据上的签名，所述认证方数据包括全部从所接收的授权令牌获得的所述计数器 ID，所述公开密钥和所述计数器当前值，以及附加信息。

45. 如权利要求 42 所述的方法，还包括在第一存储设备中存储所接收的被证实有效的票据。

46. 如权利要求 42 所述的方法，其中票据是多用途票据，并且该方法包括：

向第三方设备发送所存储的票据，其中也向第三方设备发送所存储的被证实有效的票据，并且使用在被证实有效的票据中的附加信息进行存取控制。

47. 一种在用于安全票据的系统中检查票据的方法，该系统包括具

有第一存储设备的移动设备，在第一存储设备中存储有票据；具有安全单元的安全保护单元，安全单元包括第二存储设备，第二存储设备具有证书，一对加密密钥和涉及所存储票据的至少一个计数器，所述计数器被创建成具有唯一计数器 ID 并且被初始化为具有为零的计数器值；以及至少一个第三方设备，第三方设备被构造成检查票据，所述票据是认证方数据上的签名，所述认证方数据包括计数器 ID，安全保护单元的公开密钥，代表票据的容许使用数量的数，以及附加信息，该方法包括；

所述移动设备向所述第三方设备发送所存储的票据以便检查；

所述第三方设备检查所接收票据的有效性；

所述第三方设备向所述移动设备发送质询；

通过发送对应的计数器 ID 和所接收的质询，针对涉及要检查的票据的计数器，所述移动设备在所述安全单元中启动计数器读取；

所述安全单元产生授权令牌，该授权令牌是认证方数据上的签名，所述认证方数据包括所述计数器 ID，计数器的当前值，和安全单元的公开密钥；

所述安全单元向所述移动设备发送所产生的授权令牌；

所述移动设备向所述第三方设备传送所接收的授权令牌；以及

所述第三方设备通过使用所接收票据中的密钥验证所接收的授权令牌，并且向所述移动设备发送指示验证结果的消息；

所述移动设备接收作为检查计数器值的结果的消息，该计数器值表示该票据被完全使用；

所述移动设备向所述安全单元发送删除所述计数器的请求；

所述安全单元返回所述删除计数器请求的结果作为响应；

其中所述计数器值代表票据的使用数量。

## 通信设备中保证票据安全的方法、系统

### 相关专利申请书的交叉引用

此申请是标题为“用于在个人通信设备中的完整性保护存储的方法，系统和计算机程序产品”，2001年10月18日提交的美国专利申请09/978,701的部分延续，在此对其进行了交叉引用。

### 技术领域

本发明涉及用于复本保护的方法，系统和计算机程序产品。本发明还涉及在通信设备中使用的复本保护。

### 背景技术

在过去的几年中，在我们日常生活的各个方面，通信设备的使用增长迅速。随着通信设备，例如个人委托设备的普及，保护设备所使用的关键数据已变的越来越重要。个人委托设备一个普遍特性是使用电子凭证或票据。个人委托设备的用户可以接收并在设备的存储器中存储电子票据，并使用电子票据作为对第三方提供的服务的支付。例如，可以使用电子票据支付公共演出，马戏，公共交通，等等的准入。通常由委托的第三方预先支付票据并且贷记给终端用户，或者由运营商通过电话帐单对用户收费。然而，虽然对于普通消费者，电子票据的使用提供了更强的灵活性，但也产生了开出电子票据的第三方的新的安全问题。

例如，票据的开出方希望防止个人委托设备的用户修改或复制所开出的票据以乘坐公共交通旅游。乘坐公共交通旅游的权利以电子票据的形式批准给用户，该电子票据规定了使用的数量。然而，如果用户能以某种方式修改或复制票据，用户可以进行不限次数的旅行，而不需要为每次使用向票据开出方支付费用。

已经使用了密码学的各种方法，以保护关键数据免受不可察觉的修改或复制。密码学涉及编码或者加密数字数据，以便使数据对于除

了预期接收者之外的所有人不可理解。换句话说，数据被加密并且将解密密钥交给那些已支付了数据使用费的终端或用户。对此，通过阻止非授权方使用和更改数据，密码系统能被用于保护数据的私密性和完整性。除了加密，也使用数据源的认证以便保证例如只有拥有正确密钥的一方才能产生消息认证码（MAC）的正确签名。

例如，由数字化的声音，字母和/或数字组成的明文消息可以被数字编码，并且然后使用复杂的数学算法(根据所给的一组数或数字，即密码密钥，变换编码的消息)进行加密。密码密钥是数据位的序列，其可根据所使用的算法或密码系统随机选择或者具有特殊的数学性质。在计算机上实现的精密的密码学算法可以变换和操作长度为数百或数千位的数，并能阻止任何已知的未授权的解密方法。密码学算法有两个基本类另：对称密钥算法和非对称密钥算法。

对称密钥算法使用相同的密码密钥用于通信发送方的加密以及通信接收方的解密。对称密钥密码系统建立在共享密钥的两方的互相信任上，以便使用密码系统防备不信任的第三方。熟知的对称密钥算法是由国际标准和技术监督局首先公布的国家数据加密标准（DES）算法。见联邦注册，1975年3月17日，卷40，第52号，以及1975年8月1日，卷40，第149号。当针对该通信会话装载密码密钥（DES密码密钥为56位长）时，发送方密码设备使用DES算法加密消息（会话密钥）。当装载与加密所使用的密钥相同的密钥时，接收方密码设备使用DES算法的相反算法解密所加密的消息。

非对称密钥算法使用不同的密码密钥进行加密和解密。在使用非对称密钥算法的密码系统中，用户公开加密密钥并对解密密钥保密，从公开的加密密钥获得私有的解密密钥是不可能的。因此，知道特定用户的公开密钥的任何人可以加密针对此用户的消息，而只有对应于此公开密钥的私有密钥的拥有者才能解密消息。此公开/私有密钥系统首先在Differ和Hellman，“密码学的新方向”，IEEE信息理论学报，1976年11月，以及美国专利4,200,770（Hellman等人）中公开，在此对所述文献进行了参考引用。最常使用的用于加密和签名的公开密钥

系统是RSA公开密钥密码。RSA是公开密钥加密算法，其发明于1977年并以其发明人Rivest, Shamir和Adleman命名。密码学领域的最新发展是数字签名。数字签名是不涉及秘密，但通过使数据与特定私有密钥的拥有者相关来保护数据免受不为察觉的改变的机制。因此，数字签名非常难以伪造。

虽然可以使用标准密码学方法实现安全票据的大多数方面，然而防止复制要求收票设备保留有关先前所使用票据的状态信息。然而，在具有许多不同收票设备（例如，每个总线上一个）的离线票据收集情景中，没有为全部收票设备所共享的公共受信存储器。

因此，希望能提供一种系统，方法和计算机程序产品，其能在通信设备，例如使用防篡改安全单元的个人委托设备中提供安全票据。在此所公开的本发明实施例的系统，方法和计算机程序产品满足了此需求。

#### 发明内容

用于防止复制票据所使用的关键数据的方法，系统和计算机程序产品，其用于通信设备。

本发明实施例的方法，系统和计算机程序产品使用了防篡改安全单元和密码，用于安全地传送和存储通信设备所使用的票据。

本发明实施例涉及使用以下至少两个基本通信协议实现通信设备，防篡改安全单元以及第三方设备之间的通信：1) 票据请求和存储协议，以及2) 票据使用协议。

根据本发明实施例，通信设备中的单元和第三方设备之间的通信还包括验票协议。

本发明的目的之一在于提供一种用于通信设备中的安全票据的系统，包括：包括第一存储设备的移动设备；包括第二存储设备的安全单元；至少一个第三方设备；以及与所述第一存储设备，所述第二存储设备和所述第三方设备通信的位于所述移动设备中的处理器，其被构造成：认证所述安全单元；创建并启动至少一个计数器，其被存储在所述安全单元的所述第二存储设备中；从所述第三方设备接收至少一个电子票据，并且在所述

第一存储设备中存储所述至少一个电子票据；向所述至少一个第三方设备兑现存储在所述第一存储设备中的所述至少一个电子票据；以及更新所述第二存储设备中计数器的计数器值，以对应于所述电子票据向所述第三方设备的兑现；其中所述计数器值代表票据的使用数量。

本发明的目的之一在于提供一种用于通信设备中的安全票据的方法，包括：认证安全单元；通过从移动设备发送在所述安全单元中创建计数器的请求，以及经由提供唯一计数器ID并初始化计数器中的值为零而在所述安全单元中创建计数器，在所述安全单元中创建并启动至少一个计数器；向至少一个第三方设备请求至少一个电子票据；在所述通信设备的存储设备中存储从所述至少一个第三方设备接收的所述至少一个电子票据；向所述至少一个第三方设备兑现存储在所述存储设备中的所述至少一个电子票据；更新所述安全单元中的计数器值以对应于所述电子票据向至少一个第三方设备的兑现；其中所述计数器值代表票据的使用数量。

本发明的目的之一在于提供一种在系统中用于保证票据安全而请求，创建和存储票据的方法，该系统包括具有第一存储设备的移动设备，具有安全单元的安全保护单元，安全单元包括具有证书和一对加密密钥的第二存储设备，以及至少一个第三方设备，其具有密码主公开密钥并被构造成开出票据，该方法包括：认证所述安全单元；通过从所述移动设备发送在所述安全单元中创建计数器的请求，以及经由提供唯一计数器ID并初始化计数器中的值为零而在所述安全单元中创建计数器，在所述安全单元中创建并启动至少一个计数器；向所述第三方设备请求至少一个票据；由所述第三方设备创建至少一个票据；从所述第三方设备接收至少一个票据；以及在所述第一存储设备中存储所接收的所述至少一个票据；其中所述计数器值代表票据的使用数量。

本发明的目的之一在于提供一种在用于票据安全的系统中使用票据的方法，该系统包括：具有第一存储设备的移动设备，在第一存储设备中存储有票据；具有安全单元的安全保护单元，该安全单元包括第二存储设备，第二存储设备具有证书，一对加密密钥和涉及所存储票据的至少一个计数

器，计数器具有唯一计数器ID，计数器值以及消息认证密钥；以及至少一个第三方设备，第三方设备具有密码主公开密钥，所述第三方设备被构造成兑现票据，该票据是认证方数据上的签名，所述认证方数据包括计数器ID，所述第三方设备的公开密钥，代表票据的容许使用数量的数，以及附加信息，该方法包括：所述移动设备向所述第三方设备发送所存储的票据以便兑现；所述第三方设备检查所接收票据的有效性；如果票据被认为有效，所述第三方设备向所述移动设备发送质询；通过发送对应的计数器ID和所接收的质询，针对涉及要兑现的票据的计数器，所述移动设备在所述安全单元中启动计数器更新；所述安全单元用所述第三方设备规定的值更新所述计数器；所述安全单元产生授权令牌，该授权令牌是使用存储在计数器中的消息认证密钥计算得到的消息认证码；所述安全单元向所述移动设备发送所产生的授权令牌；所述移动设备向所述第三方设备传送所接收的授权令牌；所述第三方设备使用所接收票据中的密钥验证所接收的授权令牌；以及所述第三方设备对比票据中的容许使用数量检查计数器的当前值，并向移动设备发送对应于检查结果的消息；其中所述计数器值代表票据的使用数量。

本发明的目的之一在于提供一种在用于安全票据的系统中检查票据的方法，该系统包括：具有第一存储设备的移动设备，在第一存储设备中存储有票据；具有安全单元的安全保护单元，该安全单元包括第二存储设备，第二存储设备具有证书，一对加密密钥和涉及所存储票据的至少一个计数器，计数器被创建成具有唯一计数器ID，并且被初始化从而具有计数器值为零以及消息认证密钥；以及至少一个第三方设备，第三方设备具有密码主公开密钥，所述第三方设备被构造成检查票据，该票据是认证方数据上的签名，所述认证方数据包括计数器ID，所述第三方设备的公开密钥，代表票据的容许使用数量的数，以及附加信息，该方法包括：所述移动设备向所述第三方设备发送所存储的票据以便检查；所述第三方设备检查所接收票据的有效性；所述第三方设备向所述移动设备发送质询；通过发送对应的计数器ID和所接收的质询，针对涉及要检查的票据的计数器，所述移

动设备在所述安全单元中启动计数器读取；所述安全单元产生授权令牌，该授权令牌是使用存储在计数器中的消息认证密钥计算得到的消息认证码；所述安全单元向所述移动设备发送所产生的授权令牌；所述移动设备向所述第三方设备传送所接收的授权令牌；以及所述第三方设备通过使用所接收票据中的密钥验证所接收的授权令牌，并且向所述移动设备发送指示验证结果的消息；所述移动设备接收作为检查计数器值的结果的消息，该计数器值表示该票据被完全使用；所述移动设备向所述安全单元发送删除所述计数器的请求；所述安全单元返回所述删除计数器请求的结果作为响应；其中所述计数器值代表票据的使用数量。

本发明的目的之一在于提供一种用于票据系统的安全系统，包括：具有第一存储设备的装置；连接到第一存储设备的安全保护单元，所述安全保护单元具有包括第二存储设备的安全单元，第二存储设备具有一对加密密钥和证书，以及在所述安全单元中的至少一个计数器，该计数器包括唯一计数器ID和计数器值；通过从所述装置发送在所述安全单元中创建计数器的请求，以及经由提供唯一计数器ID并初始化计数器中的值为零而在所述安全单元中创建计数器，来创建所述计数器；至少部分被存储在所述第一存储设备中的至少一个票据，其具有关于安全单元的加密密钥之一，计数器ID的信息；以及所述装置向安全单元发送请求，以便在安全单元中计数器ID所标识的各计数器中通过递增或递减对应于所述票据的使用的计数器值来更新所述计数器；其中所述计数器值代表票据的使用数量。

本发明的目的之一在于提供一种在系统中用于保证票据安全而请求，创建和存储票据的方法，该系统包括具有第一存储设备的移动设备，具有安全单元的安全保护单元，该安全单元包括第二存储设备，第二存储设备具有证书和一对加密密钥，以及至少一个被构造成开出票据的第三方设备，该方法包括：认证所述安全单元；通过从所述移动设备发送在所述安全单元中创建计数器的请求，以及经由提供唯一计数器ID并初始化计数器中的值为零而在所述安全单元中创建计数器，在所述安全单元中创建至少一个计数器；向所述第三方设备请求至少一个票据；由所述第三方设备创建至

少一个票据；从所述第三方设备接收至少一个票据；以及在第一存储设备中存储所接收的所述至少一个票据；其中所述计数器值代表票据的使用数量。

本发明的目的之一在于提供一种在用于安全票据的系统中使用票据的方法，该系统包括具有第一存储设备的移动设备，在第一存储设备中存储有票据；具有安全单元的安全保护单元，安全单元包括第二存储设备，第二存储设备具有证书，一对加密密钥和涉及所存储票据的至少一个计数器，所述计数器被创建成具有唯一计数器ID并且被初始化为具有为零的计数器值；以及至少一个第三方设备，第三方设备被构造成兑现票据，所述票据是认证方数据上的签名，所述认证方数据包括计数器ID，安全保护单元的公开密钥，代表票据的容许使用数量的数，以及附加信息。该方法包括：所述移动设备向所述第三方设备发送所存储的票据以便兑现；所述第三方设备检查所接收票据的有效性；如果票据被认为有效，所述第三方设备向所述移动设备发送质询；通过发送对应的计数器ID和所接收的质询，针对涉及要兑现的票据的计数器，所述移动设备在所述安全单元中启动计数器更新；所述安全单元用所述第三方设备规定的值更新所述计数器；所述安全单元生成作为认证方数据上的签名的授权令牌，所述认证方数据包括所述计数器ID，计数器的当前值，以及安全单元的公开密钥；所述安全单元向所述移动设备发送所产生的授权令牌；所述移动设备向所述第三方设备传送所接收的授权令牌；所述第三方设备使用所接收票据中的密钥验证所接收的授权令牌；以及所述第三方设备对比票据中的容许使用数量检查计数器的当前值，并向移动设备发送对应于检查结果的消息；所述移动设备接收作为检查计数器值的结果的消息，该计数器值表示该票据被完全使用；所述移动设备向所述安全单元发送删除所述计数器的请求；所述安全单元返回所述删除计数器请求的结果作为响应；其中所述计数器值代表票据的使用数量。

本发明的目的之一在于提供一种在用于安全票据的系统检查票据的方法，该系统包括具有第一存储设备的移动设备，在第一存储设备中存储

有票据；具有安全单元的安全保护单元，安全单元包括第二存储设备，第二存储设备具有证书，一对加密密钥和涉及所存储票据的至少一个计数器，所述计数器被创建成具有唯一计数器ID并且被初始化为具有为零的计数器值；以及至少一个第三方设备，第三方设备被构造成检查票据，所述票据是认证方数据上的签名，所述认证方数据包括计数器ID，安全保护单元的公开密钥，代表票据的容许使用数量的数，以及附加信息，该方法包括：所述移动设备向所述第三方设备发送所存储的票据以便检查；所述第三方设备检查所接收票据的有效性；所述第三方设备向所述移动设备发送质询；通过发送对应的计数器ID和所接收的质询，针对涉及要检查的票据的计数器，所述移动设备在所述安全单元中启动计数器读取；所述安全单元产生授权令牌，该授权令牌是认证方数据上的签名，所述认证方数据包括所述计数器ID，计数器的当前值，和安全单元的公开密钥；所述安全单元向所述移动设备发送所产生的授权令牌；所述移动设备向所述第三方设备传送所接收的授权令牌；以及所述第三方设备通过使用所接收票据中的密钥验证所接收的授权令牌，并且向所述移动设备发送指示验证结果的消息；所述移动设备接收作为检查计数器值的结果的消息，该计数器值表示该票据被完全使用；所述移动设备向所述安全单元发送删除所述计数器的请求；所述安全单元返回所述删除计数器请求的结果作为响应；其中所述计数器值代表票据的使用数量。

#### 附图说明

附图具体图解了在通信设备中实现安全票据的本发明实施例的方法，系统和计算机程序产品，在这些图中类似的引用编号指明类似的单元。

图1是根据本发明的实施例，图解通信设备的网络图。

图2是根据本发明的实施例，图解密码使用的网络图。

图3是根据本发明的实施例，图解通信设备的详细图。

图4是根据本发明的实施例，图解执行票据请求和存储协议的流程图。

图5是根据本发明的实施例，图解执行票据使用协议的流程图。

图6是根据本发明的实施例，描述执行验票协议的流程图。

### 具体实施方式

图1的本发明实施例图解了在通信设备中的安全票据系统。

个人委托设备100是无线手持电话，卫星电话，个人数字助理，或者蓝牙设备，或者任何其他通信设备。个人委托设备（PTD）100包括移动设备（ME）102和安全保护单元(secure element)106。移动设备102包括内部存储设备101，操作系统107以及中央处理器210。外部存储器106包括防篡改安全单元（SE）103。防篡改是本领域所熟知的术语，其定义了安全保护部分或存储器或存储设备。防篡改边界使攻击者难以得到安全保护部分内的内部单元和数据。安全单元框架的示例是基于ISO/IEC 7816，有触点，使用定义在ISO/IEC 7816中的AID（应用标识符），并且具有根据本发明实施例的附加功能的集成电路身份识别卡。其他示例包括安全MMC（多媒体卡），嵌入式硬件，等等。安全单元103是电子卡，例如智能卡，快闪卡，和WIM卡，其被个人委托设备100接纳并完全可拆卸。

移动设备102经由总线109与安全单元103通信。另外，个人委托设备100经由连接111，其通常但不必是无线连接，与第三方设备140，150以及160通信，用于接收和传送电子票据。通信链路的示例可以包括例如GSM，GPRS，WCDMA，DECT，WLAN，PSTN，ISDN，ADSL和xDSL连接，或者有线电视环境中的DOCSIS回送信道，或者任何短距离连接，如蓝牙，红外。使用操作系统107和中央处理器210执行的各种协议实现移动设备102，外部存储器106与第三方设备140，150以及160之间的通信。在一个实施例中，用于移动设备102，安全单元103和第三方设备140，150以及160之间通信的协议包括票据请求和

存储协议，票据使用协议以及验票协议。

图1中的个人委托设备100可连接到无线网络116，例如通过从个人委托设备100发送并由基站天线114接收的，诸如调频信号的信号。可以理解，移动设备102除了移动通信能力外，也可以被提供短距离连接能力。从无线网络116，经由网络130和无线网络交换机120，个人委托设备能被连接到各种第三方设备140，150，160。网络130可以是服务器，内联网，因特网，公共电话交换网（PSTN），专用交换网（PBX）等等。设备的用户（没有示出）能使用显示器212和键盘104，经由总线109与个人委托设备100通信。

发明实施例中的第三方设备140，150，160是被连接到计算机服务器，或被连接到计算机网络130等等的设备，其由第三方拥有或操作，并被个人委托设备100的用户用以处理和监视第三方服务的使用。例如，第三方向个人委托设备100的用户提供服务，其可以涉及支付公共交通，公共演出的准入，等等。个人委托设备100的用户预先为服务付费，并且之后通过出票设备140经由连接111和图1中所示的其余网络将电子票据贷记给该用户。有时，第三方必须检查或验证存储在个人委托设备中的电子票据数量，其通过使用验票设备160完成。在接收电子票据之后，用户能通过向收票设备150发送票据使用或向第三方兑现票据。

在此还使用简化的示例描述了安全单元103和用于安全票据的票据。安全单元103包括多个计数器，证书和一对密码密钥。每个计数器包括唯一计数器标识，即计数器ID以及计数器值。当计数器被创建和启动时，计数器为0。计数器值代表了票据的使用数量，并当使用了所关联的票据时，每次递增。

安全单元：

- 证书（由生产商发放）
- 密码密钥对（公开密钥，私有密钥），例如，RSA密钥对。
- 计数器：

|        | <u>计数器ID</u> | <u>计数器值</u> |
|--------|--------------|-------------|
| [计数器1] | 12345        | 5           |
| [计数器2] | 12346        | 3           |
| [计数器3] | 12347        | 1           |
| [计数器4] | 12349        | 0           |

在此示例中，安全单元包括n个计数器，每个与一个开出的票据相关联。票据本身被存储在移动设备的第一存储设备中。计数器1有唯一标识号“12345”，并且计数器1的值是“5”，其表示相关票据已被使用了5次。相对比地，与计数器ID“12346”相关联的票据已被使用了3次。此示例中，此安全设备的公开密钥是“12abc”。由出票设备开出并被存储在移动设备的第一存储设备中的每个票据可以被描述如下：

|       | <u>计数器ID</u> | <u>公开密钥</u> | <u>N</u> | <u>附加信息</u>       | <u>签名</u> |
|-------|--------------|-------------|----------|-------------------|-----------|
| [票据1] | 12345        | 12abc       | 10       | Greyhound         | 3458a     |
| [票据2] | 12346        | 12abc       | 10       | Suburban train    | 25f72     |
| [票据3] | 12347        | 12abc       | 3        | Ginema "stardust" | 807       |
| [票据n] | 12349        | 12abc       | 1        | State Filharmonic | b62gp     |

(座位234, 2002年5月23日)

每个票据具有签名，其能使用票据开出方的公开密钥来验证。因为示例中的全部票据已经由不同出票设备开出，其具有不同签名，且可以使用出票设备的公开密钥验证签名。当票据被出示给收票设备时，收票设备通过验证票据中的签名来检查票据的有效性。第一个票据与计数器ID“12345”相关联，并由“Greyhound 公司”出票，可使用10次。相对应的，与计数器ID“12347”相关联的票据由影院公司“stardust”出票，可使用3次。附加信息可以规定权利，如在示例中，“State Filharmonic”出票的票据规定某个日期以及某个座位。如果将存储在安全单元中的“计数器值”与票据中的“N”值比较，可以发现，具有带计数器ID“12345”的票据的用户已使用了“Greyhound 公司”的服务5

次，并还能使用“Greyhound 公司”的5次服务。

图2根据本发明的实施例，更具体地图解了用于通过移动设备102，安全单元103以及第三方设备140，150实现安全票据的密码。移动设备102在个人委托设备100的内部存储设备101中存储票据数据101A。票据数据101A对应于从出票设备140接收并且用户还没有兑现的有效票据。更重要地，所涉及的第三方信任安全单元103。安全单元103使用公开密钥103C和对应的私有密钥103D，仅实现受信计数器应用。另外，移动设备102还可以请求生产商证书103B以确保外部安全设备103是由受信生产商发放的。

使用安全单元103存储多个单调增加或减少的计数器。每个计数器由唯一标识计数器ID103A和当前关联值组成，当前关联值代表了电子票据的使用，个人委托设备100的用户可兑现该电子票据。例如，每次兑现电子票据时，更新计数器值并将其存储在个人委托设备100的安全单元103中。如先前所提及的，安全单元103包括公开和私有密钥103C，103D以及卡证书103B。

本发明的第三方设备包括出票设备140，收票设备150，以及验票设备160。出票设备用于在支付第三方服务之后，向个人委托设备100的用户开出电子票据。另外，收票设备150被用于兑现电子票据，并且验票设备160被用于检查用户是否拥有正确兑现的票据。每个第三方设备包括公开和私有密钥140A，140B，150A，150B，160A，160B。假定用户信任个人委托设备100，但第三方不信任个人委托设备100。因此，每个第三方设备能使用公开和私有密钥140A，140B，150A，150B，160A，160B加密关键数据，以便和个人委托设备100进行电子票据的安全通信。第三方设备中的密钥140A，140B，150A，150B，160A，160B可以是加密密钥，签名密钥或者主密钥。主密钥是被全部开票，收票以及验票设备140，150，160共享的公共对称密钥。

图3是本发明的另一个实施例，其图解了个人委托设备100中的安全票据系统。图3与图1的区别在于此系统包括多个收票设备150。个人委托设备100的用户能在第三方拥有的任何收票设备150上兑现出票设

备140开出的电子票据。换句话说，用户经由图1的连接111和其余网络向收票设备150发送电子票据。根据本发明，系统还可以包括多于一个出票设备140或多于一个验票设备160（没有示出）。

图4-6图解了本发明使用协议的实施例，所述协议用于通过移动设备102，安全单元103和第三方设备140，150，160之间的通信实现个人委托设备100的安全票据。

图4图解了涉及执行票据请求和存储协议的步骤，此协议被用于在个人委托设备100中接收和存储电子票据。开始，在步骤S1，移动设备102请求安全单元103中所存储的卡证书103B。在发明的另一个实施例中，卡证书本身没有被存储在安全单元103中，但针对卡证书的URL地址形式的指针被存储在安全单元103中，其中在步骤S1，移动设备102向URL请求卡证书。如先前所提及的，证书确保安全单元103是由受信生产商发放的。在步骤S2，安全单元103发送卡证书103B，其被移动设备102使用证书链验证为合格(compliant)的卡。可以使用两个证书，以便移动设备102验证安全单元103拥有合格的卡证书103B。例如，移动设备102向安全单元103的生产商发放的证书，和外部安全单元103的生产商向安全设备103自身发放的合格卡证书。在步骤S2，安全单元103还发送公开密钥103C或者卡证书103B。在步骤S3，移动设备102发出创建计数器请求，以便创建新的计数器以对应于将要接收并且之后由第三方设备140，150，160兑现以及/或者检查的电子票据。在步骤S4，安全单元103发送计数器ID，其被用以唯一标识计数器。在步骤S5，移动设备102向出票设备140传送计数器ID，公开密钥以及安全单元103的生产商证书。在步骤S6，出票设备140生成票据。票据是在出票设备的认证方数据上的签名，该数据由所生成票据的计数器ID 103A，公开密钥103C以及使用数量N（没有示出）组成。使用数量例如是用户被容许使用此票据的数量（例如，票据可用10次，则有N=10）。另外，认证方数据可以包括个人委托设备100使用的其它相关信息，例如，与票据相关的座位号码和/或日期和/或时间。例如，使用开票协议开出的票据类似于票据 = Sig\_Issuer((counterID /Public Key\_Device

103/N/other\_info)。在步骤S6，票据被发送到移动设备102并被存储在内部存储设备101中。

如果出票设备140还想要确定安全单元103以及票据数据101A的真实性，出票设备140可在创建票据之前向移动设备102发出质询。在此实例中，移动设备102响应质询，其中发出读计数器请求，并回送包括当前计数器值的安全单元103的认证数据上的签名。如果签名和数据被验证为正确的，则出票设备140将创建并开出有效票据。

图5根据本发明实施例图解了票据使用协议。在步骤S7，移动设备102通过使用例如图1中所示的网络连接向收票设备150发送票据，从而兑现票据。在步骤S8，收票设备150通过向移动设备102发出质询来作为应答。在步骤S9，移动设备102通过以收票设备150发送的质询为输入参数向安全单元103发送请求，启动对应于票据的计数器ID的更新计数器。作为更新请求的结果，安全单元103通过递增或递减计数器值并产生授权令牌，从而更新计数器。授权令牌是在认证方数据上的签名，该数据除了包含其他参数外，还包含计数器ID，当前计数器值以及公开密钥103C。例如，使用票据使用协议的授权令牌类似于  $\text{AuthToken} = \text{Sig\_Device } 103 \text{ (Update\_Response/counterID /Challenge/Current\_Value)}$ 。

在步骤S10，安全单元103向移动设备102回送授权令牌。在步骤S11，移动设备102向收票设备150传递授权令牌。收票设备150使用安全单元103的公开密钥103C验证在授权令牌上的签名，然后检查当前计数器值。收票设备150检查计数器值以确保计数器值小于或等于N。在步骤S12，收票设备150向移动设备102发送计数器值的确认。

可选地，收票设备150可以向移动设备102发送验证有效的票据，其包含计数器ID 103A，公开密钥103C以及当前计数器值和任何其他附加信息。然后，移动设备102将接收被验证有效的票据并将其存储在内部存储设备101中。

一旦使用完票据（例如，计数器值 = N），移动设备102可删除计数器。在步骤S13，移动设备102向外部安全单元103发送请求以便删除

计数器。移动设备102发送请求以及计数器ID 103A。在步骤S14，安全单元103通过回送删除计数器请求的结果来应答。例如，应答是成功或失败。

出票设备140开出的票据也可以包括多用途票据。在多用途票据的情况下，移动设备102可以发送原始票据，以及从收票设备150获得的验证有效的票据组。然后，收票设备150会使用附加信息（即，验证有效的票据）以作出关于存取控制的决定。另外，收票设备150还可以替换旧票据或开出新票据。对此，收票设备150也起出票设备140的作用。

图6根据发明的实施例图解了验票协议。在步骤S15，移动设备102向验票设备160发送票据。在步骤S16，验票设备160向移动设备102发送质询。在步骤S17，移动设备102通过使用验票设备160的质询作为输入参数向安全单元103发送读计数器请求，启动对应计数器ID的读计数器。在步骤S18，安全单元103向移动设备102发送授权令牌，其包含计数器的当前值。例如，使用验票协议发送的授权令牌类似于  $\text{AuthToken} = \text{Sig\_Device } 103 \text{ (Read\_Response/counterID/Challenge/current\_value)}$ 。在步骤S19，移动设备102向验票设备160传送来自安全单元103的授权令牌。验票设备160使用公开密钥103C检查计数器的当前值。在步骤S20，验票设备160向移动设备102发送确认以指示检查的状态。验票设备160的检查的状态为成功或失败。

在可选实施例中，在票据使用协议中，步骤S7可以与步骤S11结合，同样地，在验票协议中，步骤S15可以与步骤S19结合。

在另一个实施例中，质询值（例如在票据使用协议的步骤S8中，或者在验票协议的步骤S16中）可以是周期性改变的广播质询，其对于在给定时间段内运行协议的全部用户设备是共同的。

在本发明的另一个实施例中，所开出的票据是在认证方数据上的签名，其包括使用主密钥的加密，可以用以从出票设备140向收票设备150，以及从收票设备150向验票设备160传送对票据的引用及其MACKey。所有实体共享数据安全通信的主密钥。

在另一个实施例中，票据包括一组加密，每个收票器150有一个。每个单独的加密可以是公开密钥加密或者共享密钥加密。因为会导致较少的票据，如果收票器的数量较小 (<10)，希望使用后一种加密。

在另一个实施例中，收票设备150能经由安全通道联系出票设备140并获得密钥。在此实例中，密钥可以是针对出票设备密钥数据库的索引密钥。这在使用数量很大的多用途票据的情况中是希望得到的。在此实施例中，每个收票设备150针对给定的票据，只需要联系一次出票设备140。

另外，作为可选的计算授权令牌方案，可以使用MAC作为认证方法。MAC可以是码函数，例如以公开密钥103C作为MAC函数的密钥的HMAC-MD5。例如，如果使用MAC函数作为认证方法，出票协议会如下变化。在响应票据请求时，出票设备140创建票据，并且还通过使用安全单元103的公开加密密钥103C加密计数器ID和MAC密钥 (MACKey)，计算所加密的密钥 (EncKey)。例如，使用出票协议和MAC发出的票据为 Ticket = Sig\_Issuer (counterID /Public Key\_Device 103/N/Other\_Info), EncKey = Enc\_device 103 (counterID / MACKey)。移动设备102输入所接收的加密的密钥EncKey进入安全单元103。安全单元103由EncKey恢复出MACKey，并使用MACKey将认证方法设置为MAC。安全单元103向移动设备102发送确认。如果使用MAC作为认证方法，其他协议会有与上述相似的改变。

尽管在这里已经具体描述了图解实施例，然而应当注意并理解，已提供的描述和附图只用于图解目的，并且在不违背本发明的精神和范围的情况下，以上可以在形式上和细节上增加其他的变化。已使用的术语和表述是说明性的，而不是限制性的。这里没有限定术语或表述的使用将任何与所示和描述的特征或其部分等同的特征排除在外。

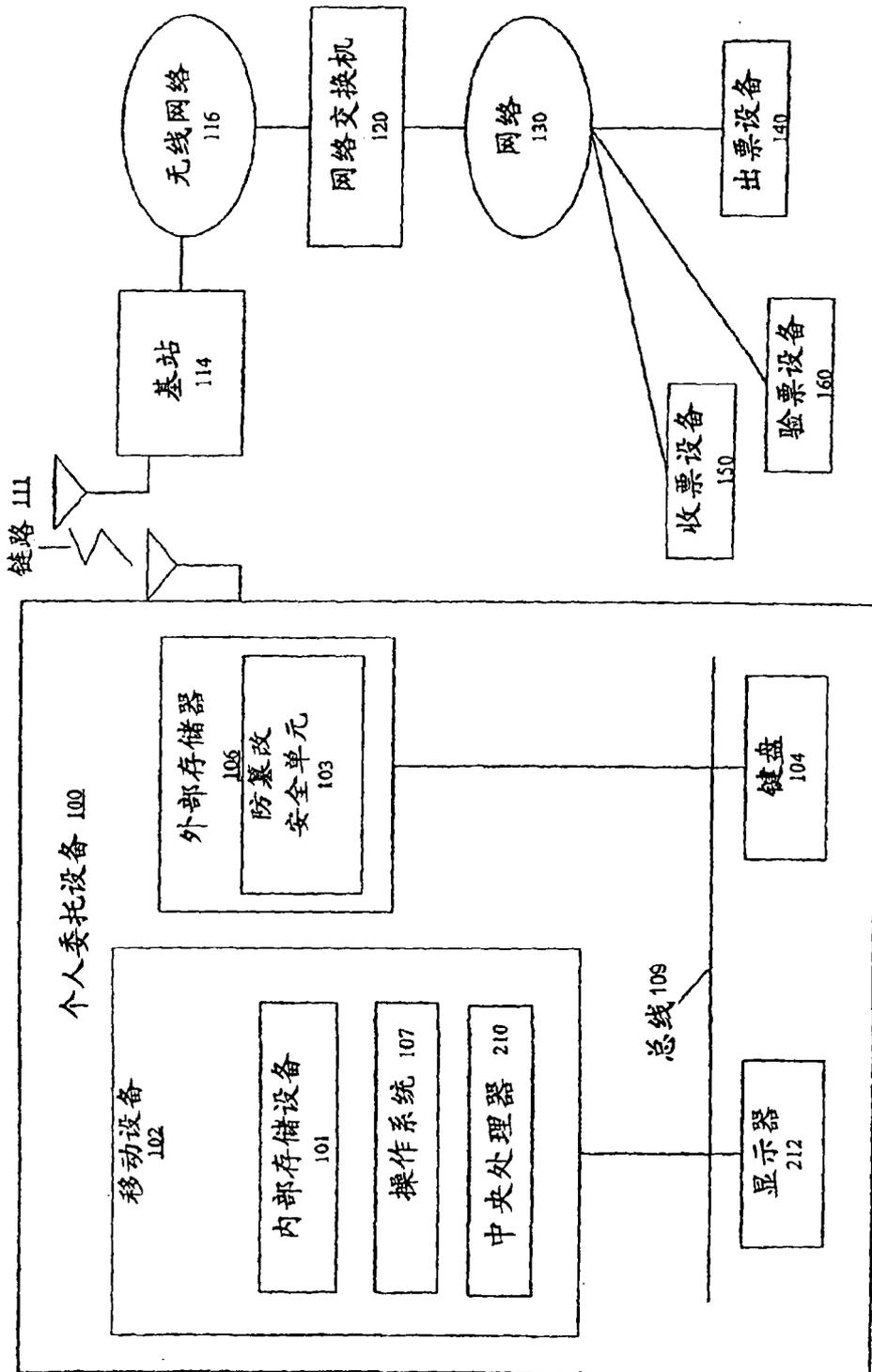


图1

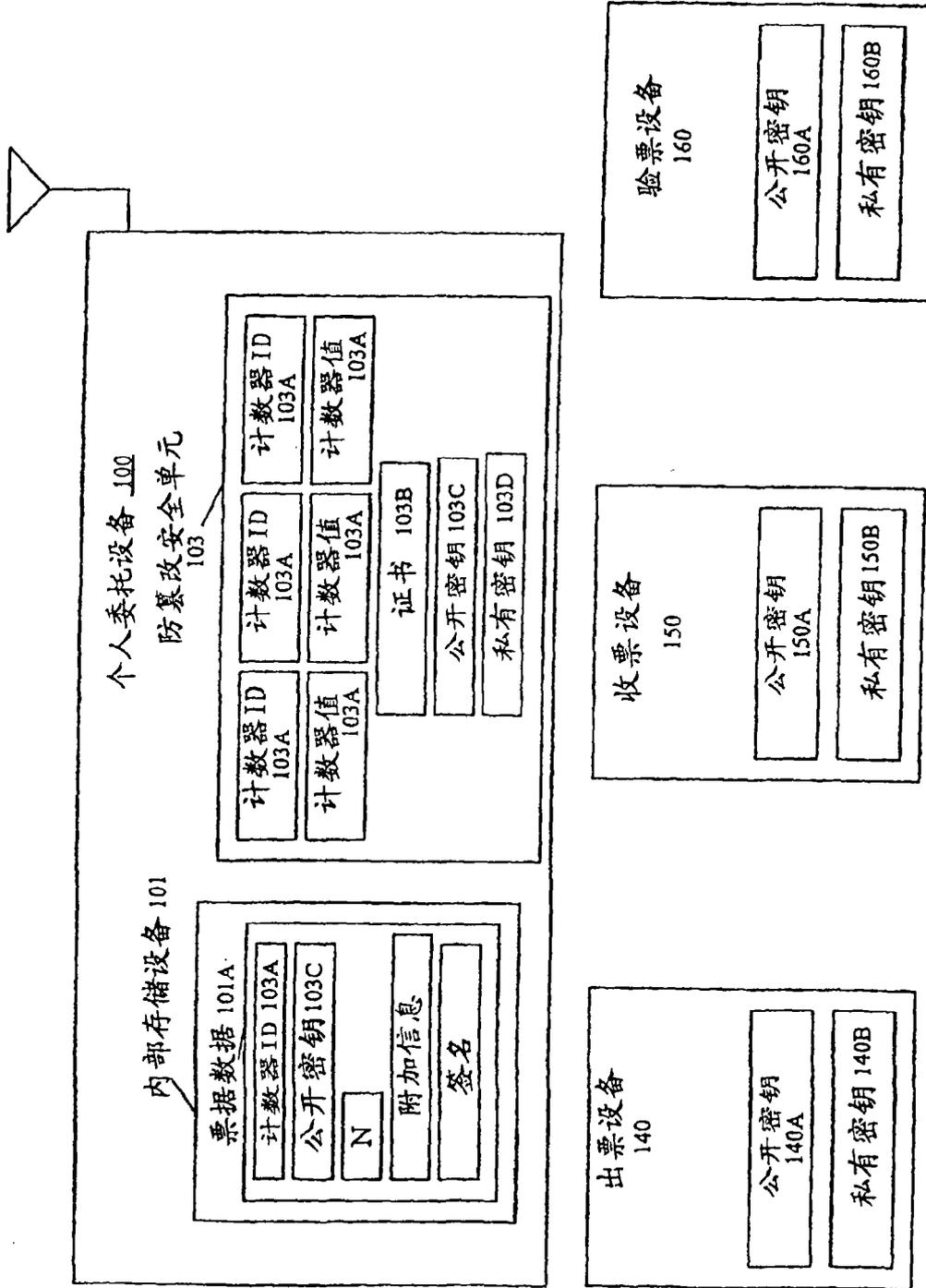


图2

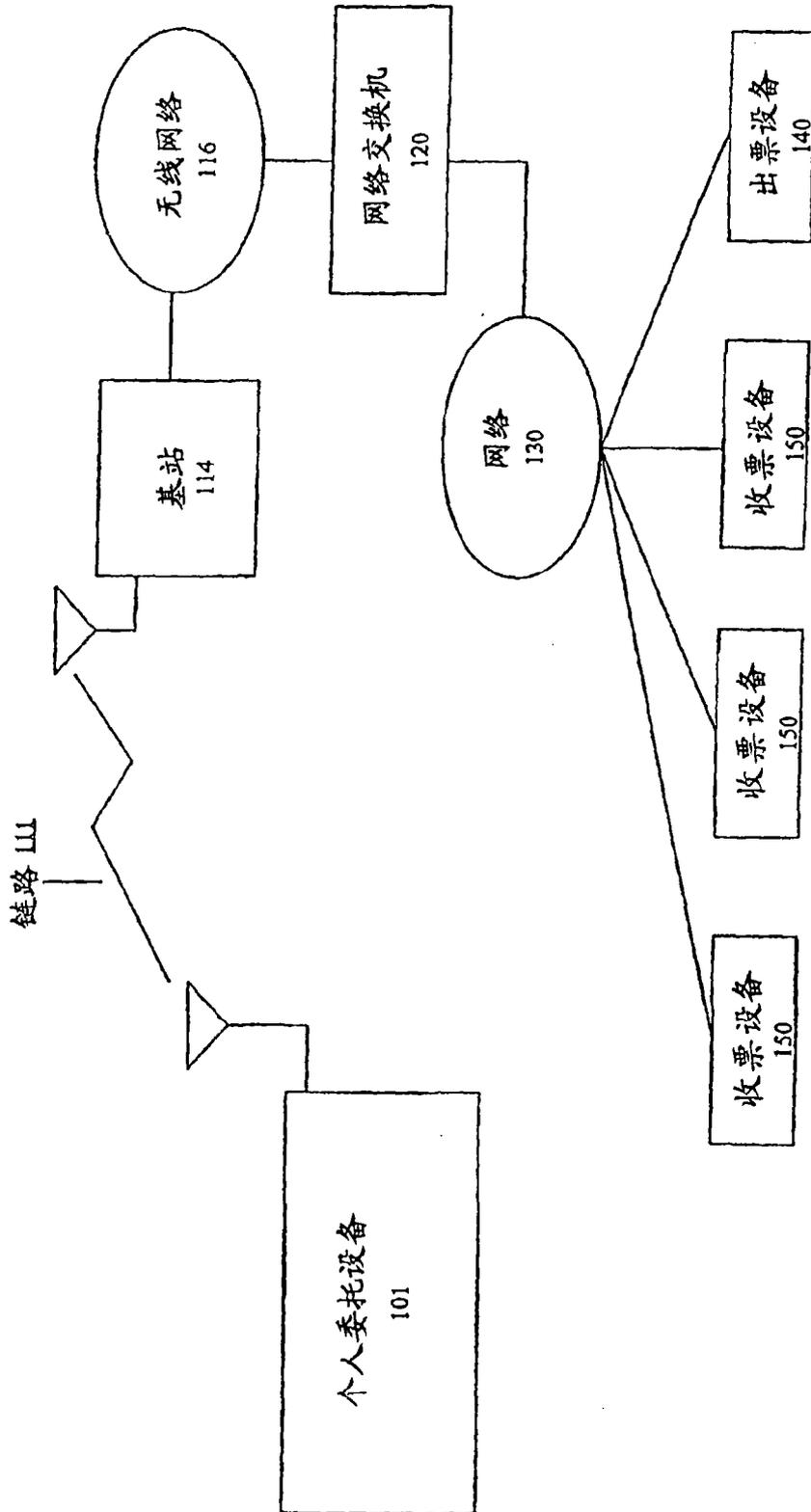


图3

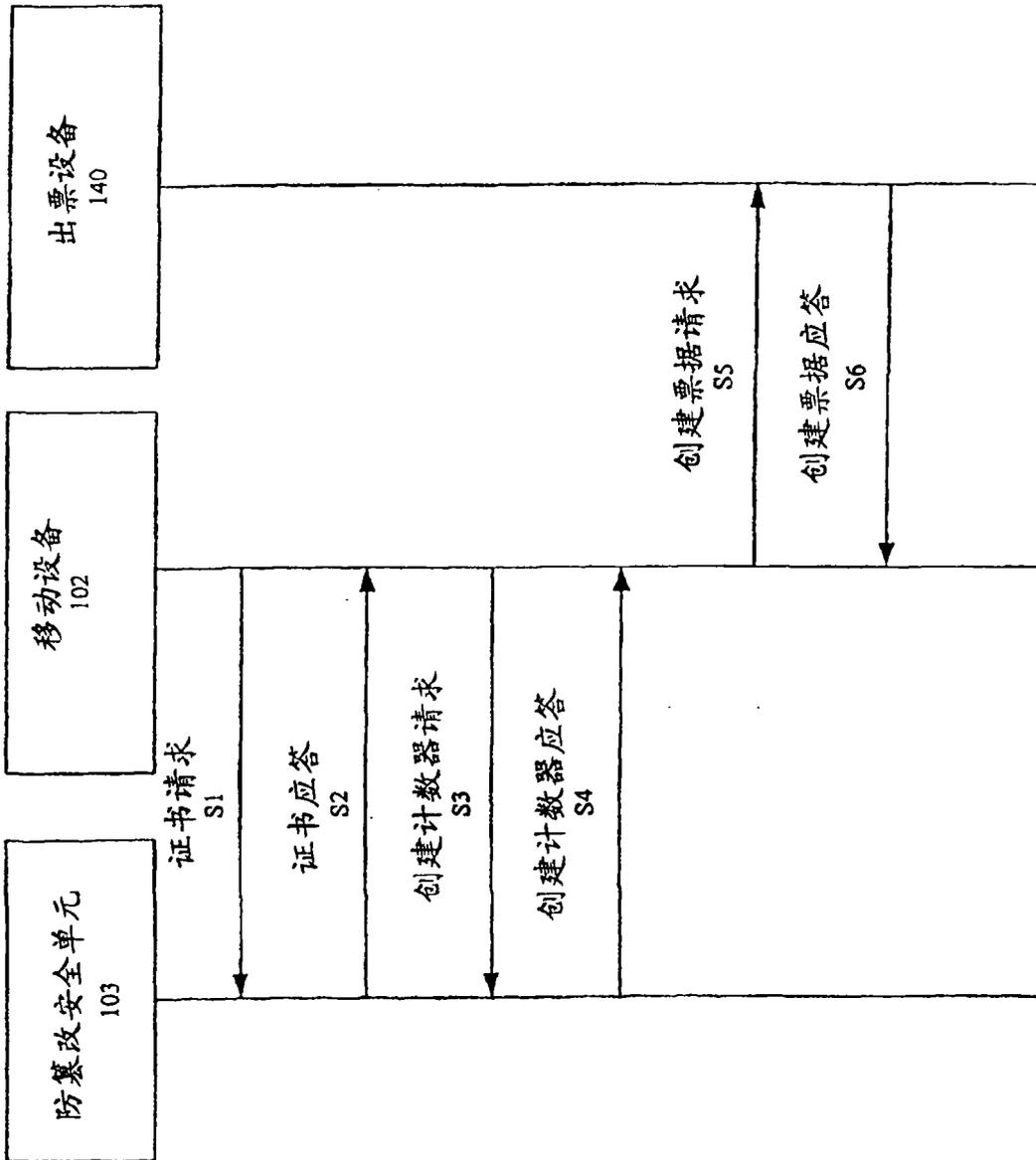


图4

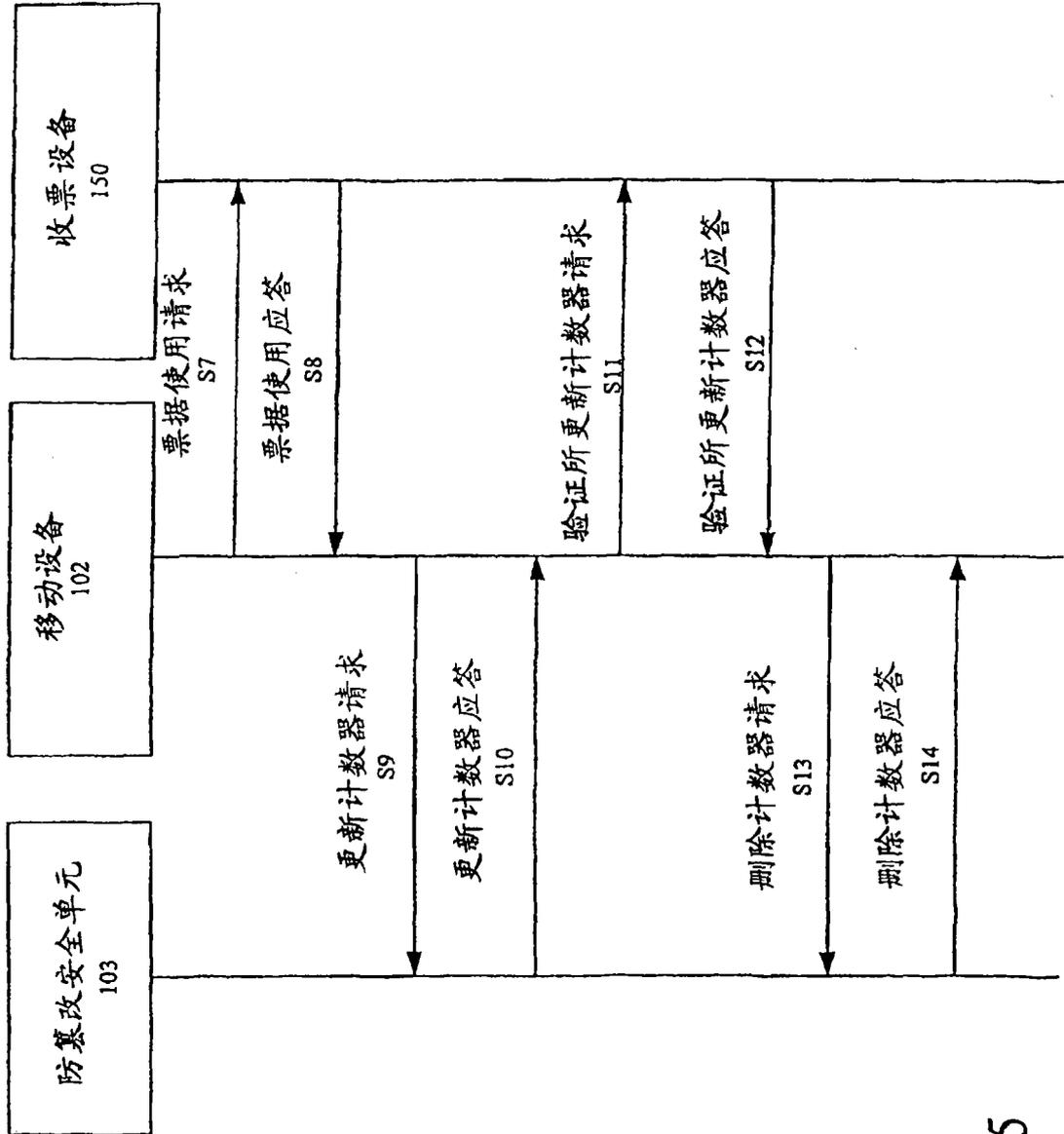


图5

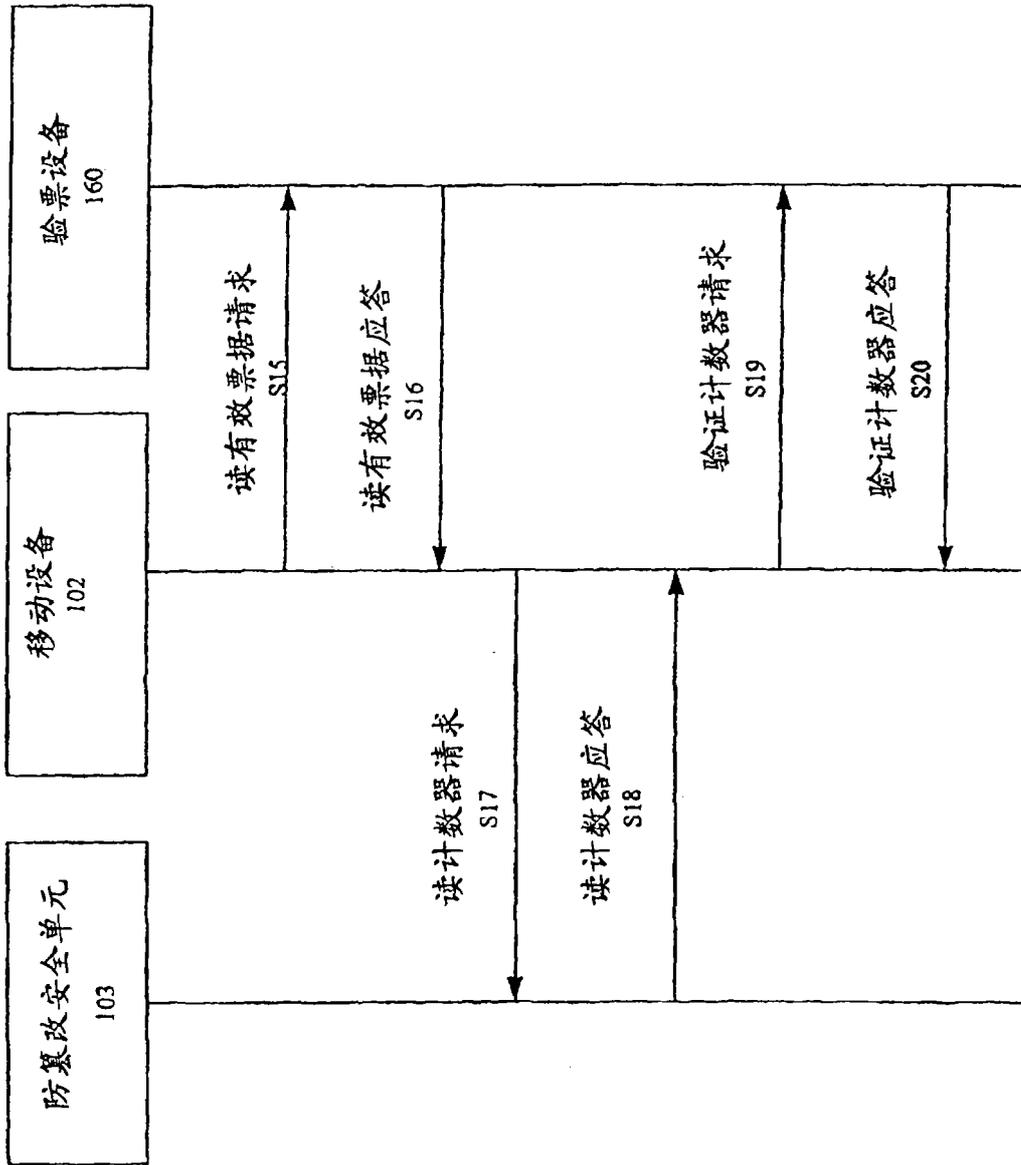


图6