(54) 发明名称
个性化芯片卡的方法

(57) 摘要
本发明涉及个性化芯片卡 (CHIPK) 的方法，其中包括部分个性化在芯片卡 (CHIPK) 的存储器 (MEM) 中存储密钥信息 (KEY1)。鉴于补充的个性化向所述芯片卡 (CHIPK) 上传输指令序列定义 ((BSD) 和向所述芯片卡 (CHIPK) 传输安装芯片应用程序的指令序列 (BS)。所述指令序列具有通过所述芯片卡 (CHIPK) 执行的芯片卡指令。根据本发明所述的方法，对于各自的芯片卡指令 (B1、B2、B3、B4、B5) 进行使用所述密钥信息 (KEY1) 且由此以被防护的方式进行检验：该芯片卡指令 (B1、B2、B3、B4、B5) 是否满足所述指令序列定义 (BSD)。并且，如果满足，就由芯片卡 (CHIPK) 执行相关的芯片卡指令 (B1、B2、B3、B4、B5)。
1. 个性化芯片卡 (CHIPK) 的方法, 其中
   a. 为了进行部分个性化, 在芯片卡 (CHIPK) 的一个存储器 (MEM) 中存储一种密钥信息 (KEY1)，
   b. 为了进行补充的个性化，
      i. 向所述芯片卡 (CHIPK) 传输一种指令序列定义 (BSD)
      ii. 向所述芯片卡 (CHIPK) 传输一种安装芯片应用程序的指令序列 (BS)，所述指令
          序列具有通过所述芯片卡 (CHIPK) 执行的芯片卡指令 (B1、B2、B3、B4、B5)，
      iii. 对于各自的芯片卡指令 (B1、B2、B3、B4、B5) 使用所述密钥信息 (KEY1) 并且由此
           以被防护的方式进行检验; 该芯片卡指令 (B1、B2、B3、B4、B5) 是否满足所述指令序列定义
           (BSD)，并且，
      iv. 如果满足, 就由芯片卡 (CHIPK) 执行相关的芯片卡指令 (B1、B2、B3、B4、B5)。
   2. 如权利要求 1 所述的的方法，
      其特征在于，
      为了执行所述指令序列 (BS)，设置一种针对所述芯片卡的访问权, 并且在执行一个相
      应的芯片卡指令 (B1、B2、B3、B4、B5) 之前检验所述访问权的存在，
      在肯定的检验结果的情况下, 执行相关的芯片卡指令 (B1、B2、B3、B4、B5); 在否定的检
      验结果的情况下，不执行相关芯片卡指令 (B1、B2、B3、B4、B5)。
   3. 如以上权利要求中任一项所述的方法，
      其特征在于，
      密钥信息 (KEY1) 是芯片卡独特的或者是芯片卡编组独特的。
   4. 如权利要求 1 或者 2 所述的方法，
      其特征在于，
      鉴于补充的个性化, 向芯片卡 (CHIPK) 传输进行补充个性化的补充个性化例程
      (EPERS)。
   5. 如权利要求 1 或者 2 所述的方法，
      其特征在于，
      所述指令序列定义 (BSD) 规定一个状态自动装置的状态 (BZ, Z1, Z2, Z3, Zn) 和状态
      转移, 所述状态自动装置从一个相应的状态 (BZ, Z1, Z2, Z3, Zn) 切换到一个规定的、与以前所
      取状态状态不同的序列状态, 其中给一个相应的状态 (BZ, Z1, Z2, Z3, Zn) 分别配属一个规定的
      的芯片卡指令, 该规定的芯片卡指令可以在该状态 (BZ, Z1, Z2, Z3, Zn) 下执行。
   6. 如权利要求 2 所述的方法，
      其特征在于，
      在芯片卡 (CHIPK) 的一个优选的非易失存储器 (MEM) 中, 存储指令序列定义 (BSD)、指
      令序列 (BS)、补充的个性化例程 (EPERS)、一个通过执行所述指令序列 (BS) 直到一个相应
      的芯片卡指令 (B1, B2, B3, B4, B5) 部分安装的芯片卡应用程序 (APPDATA)，所述访问权、状
      态自动装置和 / 或所述状态自动装置分别采取的状态 (BZ, Z1, Z2, Z3, Zn, EZ)。
   7. 如权利要求 2 所述的方法，
      其特征在于，
      在完全执行了所述指令序列 (BS) 以后
a. 在所述芯片卡（CHIPK）上存储表明执行了补充的个性化的信息，
b. 在芯片卡（CHIPK）上删除所述访问权，和 / 或
c. 删除指令序列定义（BSD），指令序列（BS），补充的个性化例程（EPERS），状态自动装置和 / 或所述状态自动装置的一种状态。

8. 如权利要求 1,2,6,7 中任一项所述的方法，
    其特征在于，
    一个指令序列（BS）的芯片卡指令（B1, B2, B3, B4, B5）包含针对另一个指令序列（BS）的指令序列定义（BSD）。

9. 如权利要求 1,2,6,7 中任一项所述的方法，
    其特征在于，
    在执行了所述指令序列的最后一个芯片卡指令以后，调出一个检测例程以检测成功的个性化，并且所述检测例程在识别出错误的补充的个性化的情况下在所述芯片卡（CHIPK）上存储表明该错误的个性化的信息。

10. 如权利要求 1,2,6,7 中任一项所述的方法，
    其特征在于，
    鉴于部分个性化而执行例程，
    所述例程在芯片卡（CHIPK）上预留一个存储器区域，用于收纳鉴于补充的个性化而执行所述指令序列（BS）时产生的芯片卡应用程序的数据（APPDATA）。

11. 如权利要求 1,2,6,7 中任一项所述的方法，
    其特征在于，
    禁止调出不包含在所述指令序列（BS）中的芯片卡指令（BS）直到完全执行完所述指令序列为止。
个性化芯片卡的方法

迄今为止，在大多数情况下，由芯片卡的制造商、由办证单位或者获得信任的业务供应商在受到防护的个性化中心对芯片卡进行个性化，在相应的芯片卡上记录有卡独特的或者个人独特的数据。

在这样一种个性化中心，在芯片卡加载客户特定的个性化数据，例如：一个使用者的姓名、其账号或者其它客户专门的数据或者应用程序。所述个性化中心通常通过采电子的、机械的安全机制和/或组织措施针对未授权的操纵（Manipulation）加以防护，因为在其中处理安全性相关的数据（例如所述芯片卡使用者的个人数据、PIN等等），并且要避免未经授权者获取信息以及避免未经授权者对个性化过程的影响。

例如在人员识别的芯片卡的情况下，如果要求最大的安全性，尤其是针对操纵或者伪造存储在所述芯片卡中的数据，于是至今通常在受到防护的个性化中心进行所述个性化。

在个性化中心以外没有受到防护的的环境中的个性化至今只有在安全性要求很低的芯片卡的情况下才进行。

一个芯片卡的个性化通常包含激活芯片卡上的一个或者多个应用程序同时产生安全密钥和/或安全密钥对，例如所谓对称的密钥或者RSA密钥（RSA：发明人Rivest、Shamir和Adleman命名的加密算法）。在此，事实表明与其他的个性化步骤相比产生安全密钥对的成本很高。在一个个性化中心，在一个规定的时间段中处理的芯片卡的数量显著地受相应芯片卡的安全机制的产生时间的影响。

芯片卡的个性化往往不能够结束于唯一的个性化设置，因为在芯片卡的发放时刻还不完全知道要在芯片卡上播放和在芯片卡上安装什么应用程序。此外，还在可以包含多个应用程序的多重应用芯片卡的情况下，需要在超过所述芯片卡的使用期限时激活应用程序。根据现有技术，只要求相应的安全性规定，为此就要把所述芯片卡再次带到所述受到防护的个性化中心。

本发明的技术问题提出一种个性化芯片卡的灵活方法。

该技术问题通过一种具有权利要求1特征的方法得以解决。本发明的有利的实施方式在从属权利要求中说明。

在如本发明所述的方法的情况下，为了（最好是在一个受到防护的个性化中心进行的）鉴于部分个性化而对一种芯片卡实施部分的个性化，在所述芯片卡的一个（最好是易失的）存储器中存储一种密钥信息，所述密钥信息例如由一种卡独特的安全消息密钥和/或一种实体密钥组成。这样的一种非易失存储器例如可以实现为所述芯片卡上的EEPROM。根据本发明，鉴于一种也可以在没有受到防护的环境中执行的补充个性化，向所述芯片卡上传输一种指令序列定义和一种安装芯片应用程序的指令序列，所述指令序列具有通过所述芯片卡的执行的芯片卡指令。此外，对于该指令序列的一个相应的芯片卡指令进行使用所述密钥信息并由此受到防护的检验，该芯片卡指令是否满足所述指令序列定义。如果满足，就通过芯片卡执行相关的芯片卡指令。

应当指出，所述说明的方法顺序不必对应于特征的时间顺序。例如可以在执行
单个的芯片卡指令之前，相关联地在所述补充的个性化开始执行芯片卡指令的检验。

[0011] 优选的是可以在采用密钥信息的条件下在对芯片卡再现所述指令序列或者在芯片卡上安装所述指令序列的情况下保障所述指令序列的有效性。于是在采用所述指令序列定义的条件下进行的指令序列的检验可以在处理完所述指令序列的情况下借助于所述密钥信息进行而无需附加的保障。

[0012] 借助于指令序列定义检验指令序列的优点在于：由此可以保证，只能够执行非操纵的起源于可信赖位置的指令序列，因只有它们才满足所述指令序列定义。

[0013] 利用如本发明所述的方法可以在无防护的区域，例如在使用者的私人住宅中、移动无线卡的地区销售办公室、雇员卡的芯片卡编码室、信用卡和用户卡的银行分支机构或者身份证和身份芯片卡的申报机构可靠地进行补充的个性化，为满足高安全性的要求，所述补充的个性化至今只能够在受到防护的个性化中心进行。

[0014] 耗费时间的个性化步骤（尤其是生成证书和密钥对）可以鉴于补充的个性化进行。在此有利的是，这种耗费时间的步骤不必在个性化中心进行并且在所述个性化中心可以达到较短的个性化时间/芯片卡，并且所述个性化中心可以在较短的时间中对芯片卡进行部分个性化。

[0015] 此外还有利的是，其中在其发射后可以进一步再现其它应用程序的多用途芯片卡不必为激活应用程序而重新送到个性化中心来进行完全的个性化。激活这样的其它应用程序可以鉴于补充的个性化进行。也就是说，带有应用程序的补充的个性化例如可以由芯片卡的使用者自己在所述个性化中心之外的其住宅中进行。

[0016] 芯片卡指令的检验例如可以通过使用一种安全证书密钥作为密钥信息进行并且从而保证；在使用伪造的安全证书密钥的情况下阻止向所述芯片卡传输指令序列和/或指令密钥信息。此外，所述芯片卡例如可以含有一种 RSA 密钥对的私人密钥作为密钥信息。指令序列和/或指令序列定义的传输可以借助于公开的芯片卡 RSA 密钥加密以进行防护。

[0017] 此外，该芯片卡而且只有该芯片卡才可以用存储在芯片卡的私人密钥解密所述指令序列和/或指令序列定义。此外还可以把一个验证密钥或者签字密钥用作密钥信息，以确保指令序列和/或指令序列定义由所期待的地点产生和传输。优选的是由进行部分个性化的个性化中心产生和传输。

[0018] 优选的是，在执行所述指令序列的各芯片卡指令之前，在指令序列定义的辅助下检验要执行的芯片卡指令是否满足指令序列定义。在规定的检验结果的情况下，执行所述芯片卡指令；在规定的检验结果的情况下，不执行所述芯片卡指令。

[0019] 根据本发明的一个扩展方案，为了执行所述指令序列可以设置对芯片卡的访问权，并且在扫描各自的芯片卡指令之前检验所述访问权是否存在。在规定的检验结果的情况下，执行相关芯片卡指令；在规定的检验结果的情况下，阻止执行相关芯片卡指令。

[0020] 有利的，所述访问权可以在调出所述指令序列时通过操作系统设定。在另一个实施方式中可以在执行所述指令序列的各芯片卡指令之前设定一个配属给所述芯片卡指令的访问权并且在执行完以后重新删除。

[0021] 一个芯片卡指令的这种访问权例如可以包含对一个确定的存储区域的写入权。一个访问权的另一个例子是一个芯片卡指令产生一种加密的密钥或者产生可以验证的权利。
令。此外借助这样一种检验例程可以简单地实现：在补充的个性化以外执行芯片卡指令的情况下不能执行任何只被允许在补充的个性化中的指令。

[0022]根据本发明的一个扩展方案，所述密钥信息可以是芯片卡独特的或片片卡编组独特的。一个相应的芯片卡编组例如可以配置在所述芯片卡的一个相应的产品模块、所述芯片卡的相应的产品模块、所述芯片卡的相应的产品模块或者配置在所有制造的芯片卡。从而可以在部分个性化的情况下限制在什么芯片卡上可以执行相应的指令序列（只在一个单个的芯片卡），在一个芯片卡组上还是在所有的芯片卡上。

[0023]根据本发明的一个有利的实施方式，所述指令序列定义可以规定一种状态自动装置的状态和状态传输，所述状态自动装置从各自的状态切换到一个与所述所采取的状态不同的序列状态，其中对一个相应的状态配置一个规定的芯片卡指令，所述规定的芯片卡指令可以在该状态下执行。

[0024]可以对（优选的是全部的）所述指令序列包含信息模式，用所述信息模式可以通过在所述指令序列中的芯片卡指令比较查对一个相应的要执行的指令序列的芯片卡指令是否满足所述指令序列定义，和/或在处理完所述指令序列以后是否处理所有包含在所述指令序列中的芯片卡指令并且从而完整地处理完所述指令序列。在此可以按照以下方式执行所述指令序列：使得所述指令序列对所述指令序列的每个芯片卡指令包含一个标识所述芯片卡指令的信息，最好利用尽可能简明信息的指示。

[0025]有利的是，所述状态自动装置的状态图不包含任何分支、弯道或者回归。由此可以在补充个性化芯片卡的情况下把指令序列的执行限制于执行部分个性化的个性化点为之一部分的那些指令序列。由于没有回归，可以确保不加改变地、一次性地、实质上完全地和/或按正确的顺序执行一种贯彻所述状态图的指令序列。从而针对未授权的第三方的操作防护芯片卡的使用者。

[0026]此外可以在芯片卡的一个优选的非易失存储器或中存储指令序列定义、指令序列、一个通过把所述指令序列处理至一个相应的芯片卡指令部分安装的芯片卡应用程序、访问权、状态自动装置和/或所述状态自动装置相应采取的状态。由此可以在中断以后延续一个中断的补充的个性化。在采用一个非易失存储器存所说明的信息的情况下还可以在中断电源后延续所述补充的个性化。

[0027]这附带提高了防止操纵的安全性，因为操纵者不能通过简单手段例如中间电源删除或部分地有效的指令序列并且替换同样操作的指令序列和指令序列定义。

[0028]延续一个中断的补充个性化可以优选地在自动装置上一次采取的状态的情况下通过延长所述指令序列进行。作为可供选择的替代方案可以如此地延续一个中断的补充的个性化，使在其开始重新执行所述指令序列并且在此忽略所有已经处理完的芯片卡指令直到执行还没有处理完的芯片卡指令。

[0029]根据本发明的一个扩展方案，可以在完全执行了所述指令序列以后，在所述芯片卡上存储一个表明所执行的补充的个性化的信息，在所述芯片卡上删除访问权，和/或在芯片卡上删除指令序列定义、指令序列、状态自动装置的一种状态。在此，表明执行了的补充的个性化的信息还可以说明在执行了个性化以后删除的信息代表，并且从而通过其不存在表明已经结束了所述个性化。

[0030]尤其有利的是，可以删除在补充的个性化完成以后不再需要的数据和芯片卡指
令，并且可以从而空出存储器容量。此外还可以由芯片的 Embedded 操作系统分析芯片卡上的数据的存在或者不存在，以识别所述芯片卡是否处于执行一个补充的个性化或者是否已经结束了所述补充的个性化，或者是否还没有开始所述补充的个性化。依赖于该分析，所述芯片卡的 Embedded 操作系统可以附加地判断是否执行要用不同的访问权限执行的指令。

【0031】根据本发明的一个扩展方案，一个指令序列的芯片卡指令，优选的是所述指令序列的最后一个芯片卡指令，包含对另一个指令序列的指令序列定义。由此可以缓存地执行指令序列，并且可以把长的指令序列切成多个短的、模块的指令序列并且相继地执行。

【0032】此外可以在执行了所述指令序列的最后一个芯片卡指令以后调出一个检测例程以检测成功地补充的个性化，并且所述检测例程在识别出错误的补充的个性化的情况下在所述芯片卡上存储表明该错误的个性化的信息。从而所述芯片卡的一个程序可以通过简单地读取信息识别是否没有错误地个性化了一个应用程序，并且只有在没有错误的情况下访问该应用程序。在此，该检测例程可以永久地存储在所述芯片卡上，可以是所述指令序列的一部分，或者如同所述指令序列那样由于补充的个性化而传输到所述芯片卡上并且在结束以后重新删除掉。

【0033】根据本发明的一个扩展方案，可以基于部分个性化执行一种例程，所述例程预定一个存储器区域或者一个在芯片卡上的目录，用于收集鉴于补充的个性化执行所述指令序列时产生的数据。从而可以保证，在执行完所述补充的个性化以后不会出现存储器缺乏或者存储器过载并且可以只完全地执行其芯片卡指令写入在该事先预留的存储器区域内的指令序列。

【0034】根据本发明的一个扩展方案，可以禁止调出不包含在所述指令序列中的芯片卡指令一直到完全执行完所述指令序列为止。由此只有在完全地执行了所述的个性化并且结束以后才能够一个芯片卡用于其确定的用途。

【0035】下面参照附图说明本发明。

【0036】在附图中：
【0037】图 1 表示在一个个性化中心运行的一个芯片卡的部分个性化，
【0038】图 2 表示在无防护的环境中进行所述芯片卡的补充的个性化，
【0039】图 3 表示具有加载并且永久存在的用于执行补充的个性化化的模块的芯片卡，
【0040】图 4 表示在一个个性化中心执行一个指令序列的情况下的芯片卡，而
【0041】图 5 表示作为带有状态和状态转移的状态自动装置的指令序列定义。

【0042】在图 1 中表示在一个个性化中心 PZ 运行的一个芯片卡 CHIPK 的部分个性化。在本例中假定，通过一个在其含有的针对其它的芯片卡单义的、表示为权限检验的芯片卡号 ID 标识所述芯片卡 CHIPK。优选地在制造芯片卡 CHIPK 时就已经把所述芯片卡号 ID 敷设在所述芯片卡 CHIPK 上了。一个个性化中心 PZ 的电子和 / 或机械加以防护的区域通过一个虚线表示，通过一种芯片卡读 / 写装置 CHIPLES 用图 1 中示出的方法访问所述芯片卡 CHIPK。在所述芯片卡读 / 写装置 CHIPLES 与芯片卡 CHIPK 之间的连接通过一个宽带的粗体虚线表示，芯片卡读 / 写装置 CHIPLES 与部分个性化模块 KEYGEN 之间的连接也可以一个宽带的粗体虚线表示。所述部分个性化模块 KEYGEN 控制所述芯片卡读 / 写装置 CHIPLES 并且执行用于部分个性化所述芯片卡 CHIPK 的例程。

【0043】在本实施例中假定：所述部分个性化模块 KEYGEN 优先地根据 PRA 把密钥信息
KEY1 和 KEY2 生成密钥对。此外，部分个性化模块 KEYGEN 与数据库 CHIPDB 连接，这由一个宽的粗体虚线表示，所述数据库尤其包含一个列表 TABKEY, 所述列表具有芯片号, 即：ID 对一个密钥信息即 KEY2 的配属。对数据和存储器的写 / 读访问通过所谓的部件进行并且以虚线的箭头表示。除了所述单义的芯片卡号以外，所述芯片卡 CHIPK 还包含一个通常构成为 EEPROM 的存储器 MEM, 以能够永久并且可改写地存储数据。

图中没有显示出，作为在数据库 CHIPDB 中存储芯片卡号和密钥信息的可供选择的替代方案，可以在采用一个仅为个性化中心 PZ 所知的密钥的条件下借助于适当的或重建的方法由部分个性化模块 KEYGEN 导出所述密钥信息 KEY1 和 / 或 KEY2。

图 2 大致示出通过在个性化中心 PZ 请求一个指令序列 BS 和一个指令序列 DSB 导入所述补充的个性化以及其向芯片卡 CHIPK 的传输。在此芯片卡 CHIPK 处于没有受到防护的的环境中。这种受到没有防护的的环境在下文中称为个性化地点 HB，在所述站点执行补充的个性化。在该实施例中假定；所述个性化地点 HB 是一个芯片卡使用者的家，即，私人住宅，或者办公室，在此，其它可能的个性化地点可以是区域的个性化办公室、芯片卡发行站点譬如银行和受保护公司，还可以是个性化中心 PZ。

在图 2 中对应于图 1 示出个性化中心 PZ 中的数据库 CHIPK 和列表 TABKEY。同样类似于图 1 示出芯片卡 CHIPK，芯片卡号 ID、存储器 MEM、密钥信息 KEY1、一个第二芯片卡读 / 写装置 CHIPLES2 以及这二者之间的连接，其中所述芯片卡 CHIPK 和芯片卡读 / 写装置 CHIPLES2 没有位于个性化中心 PZ 中而是处于一个进行所述补充个性化的个性化地点 HB 中。在由虚线示出的个性化地点 HB 中有一个通信模块 KOM1, 所述通信模块 KOM1 控制所述在外芯片卡读 / 写装置 CHIPLES2 并且可以通过一个因特网连接与个性化中心 PZ 中的一个通信模块 KOM2 连接。在此，一个因特网连接只是优选的多个连接可能性之一。

在该实施例中假定所述通信模块 KOM1 用 HTTPS 协议 (HTTPS : HyperText Transport Protocol Secure) 建立一个因特网连接，向通信模块 KOM2 发送一个消息 REQ 并且后者在应答中同样地在使用 HTTPS 协议的条件下发送一个数据消息，即：指令序列定义 BS 和所属的指令序列定义 DSB；优选地是加密的。进行 HTTPS 加密尤其是例如采用存储在所述芯片卡 CHIPK 上的密钥信息 KEY1 和 / 或所述个性化中心 PZ 的公开的密钥。

除了在该实施例中假定的因特网连接以外还有所有类型的口头的、书面的或者电子的连接，例如无线电连接或者电话连接。此外电子连接的情况下可以有各种通信用的协议，例如 HTTP、HTTPS、SMTP 或者一种优先权协议。所述连接还是可以离线地进行，就是说不用直接的电子连接进行，或者通过离线 / 在线组合进行，其中对个性化中心 PZ 的请求通过因特网连接传输而应答不用直接的电子连接进行。尤其是在一个可供选择的替代方案中还可以向个性化中心 PZ 电话地发出请求，而不必从所述个性化中心 PZ 直接在线地传输要传输的数据，而是存储在 CDROM、磁盘、磁带或者交换的数据载体上，由邮局发送并且通过所述通信模块 KOM1 读取。

由一个宽的粗体线示出，通过模块 KOM2 有对数据库 CHIPDB 和发生模块 BSGEN 的访问以产生或者查明指令序列 BS 和指令序列定义 DSB。过在该实施例中假定的在通信模块 KOM1 和 KOM2 之间的消息 REQ 和 DAT 的传输通常地通过箭头示出。从发生模块 BSGEN 起直至芯片卡 CHIPK 的存储器 MEM 的指令序列 BS 和指令序列 DSB 的传输路线由一个虚线箭头示出。
[0050] 在图中没有示出的是在个性化地点 HB 中的一个用于与使用者互动的终端，在所述终端上运行一种执行可能的情况下需要的与使用者的互动。这例如，反问是否要建立下载所述指令序列 BS 的一个因特网连接。在一个优选的实施方式中，芯片卡读 / 写装置 CHIPLE2S，通信模块 KOM1 和所述的终端是一个具有标准部件和标准操作系统的工作站计算机的部分。

[0051] 还有可以如此地实施通信模块 KOM2：使得只接受满足一个在含在内的可靠的例行（图中未示出）的连接愿望。此外所述通信模块 KOM2 还可以与一个网页服务器（未示出）连接，可以是一个网页服务器的一个模块或包含一个网页服务器，以提供与芯片卡 CHIPK 的使用者因特网连接的可能性。尤其是对向所述使用者显示一个在一个网页可选择的可以激活的芯片卡应用程序列表、优选的在读取和分析芯片卡号 ID 以后，以只显示自由切换所述芯片卡 CHIPK 的芯片卡应用程序。

[0052] 图 3 和图 4 中示意地示出各自的带有用于执行补充的个性化加载的和永久存在的模块的芯片卡 CHIPK。在此，图 3 示出在输入但是在执行完指令序列 BS 和指令序列定义 BSD 之前的一种状态。图 4 示出在上执行四个芯片卡指令 B1、B2、B3、B4 以后执行指令序列 BS 的前五个芯片卡指令 B5 的情况下芯片卡 CHIPK。此外，在图 3 和图 4 中示出的芯片卡 CHIPK 还具有一个在存储器 MEM 中的出错计数器 FEHLZ。所述出错计数器 FEHLZ 是一种数据字段，存述数据字段中存在出错的类型和 / 或关于出现的错误的其它细节。存储器 MEM 包含密钥信息 KEY1、指令序列定义 BSD 和指令序列 BS，所述指令序列的特征在于：该指令序列可以按指令而向芯片卡 CHIPK 进行传输并且执行（图中未示出），或者把指令作为完整的序列存储在芯片卡中并且然后分步骤执行。存储器 MEM 的一个空闲的存储区域通过一个虚线的矩形表示。通过部分地执行指令序列 BS（从 B1 至 B4）产生的应用程序数据 APPDATA，由一个在存储器 MEM 内的画阴影的矩形表示。指令序列 BS 的单个指令 B1、B2、B3、B4、B5 在指令序列 BS 中示出，其中通过三个点表明，所述指令序列 BS 可以包含任意数量的指令。以对应的方式，各个指令序列定义单元 D1、D2、D3、D4、D5 在指令序列定义 BSD 中示出。此外芯片卡 CHIPK 包含一个补充的个性化例程 EPERS，由一个虚线箭头表示，所述个性化例程 EPERS 读访问指令序列 BS 和指令序列定义 BSD，并且由一个贯穿的箭头表示，读写访问出错计数器 FEHLZ 和可供使用的空间的存储器 FRE1MEM。在此，通过一个沿执行方向的双箭头示出指令 B1、B2、B3、B4、B5 和指令序列定义单元 D1、D2、D3、D4、D5 的分步骤执行。

[0053] 鉴于补充的个性化而进行的指令 B1、B2、B3、B4、B5 尤其可以是具有在所述芯片卡的一个易失或者非易失的存储器 MEM 上的写入权的指令以及产生安全证书或者密钥对的指令。

[0054] 图 5 示出一个指令定义 DSB，所述指令定义在一种状态自动装置的意义上规定状态和状态转移，其中把其状态 Z1、Z2、Z3、Zn 表示为圆圈并且把状态转移表示为状态 Z1、Z2、Z3、Zn 之间的箭头。所述状态转移通过指令序列定义单元 D1、D2、D3、D4、Dn、Dn+1 说明，在指令序列 BS 中示出，其执行引起所述状态转移。开始状态 BZ 确定状态自动装置的开始状态 BZ 确定状态，所述状态表示能成功地执行完指令序列 BS。通常开始状态 BZ 和结束状态 EZ 是相同的并且如果不进行任何补充的个性化就对应于芯片卡 CHIPK 的中性状态。

[0055] 图 1 示出在个性化中心 PZ 中芯片卡 CHIPK 的部分个性化。在本实施例中芯片卡 CHIPK 包含单义的、不可改变的芯片卡号 ID，通过所述芯片卡号 ID 可以标识芯片卡 CHIPK。
部分个性化模块 KEYPEN 从芯片卡读 / 写装置 CHIPLEES 要求所述芯片卡号 ID, 并且向数据库
CHIPDB 传输该芯片卡号 ID, 从而在所述数据库中产生在列表 TABKEY 中的记录。列表 TABKEY
中优选地为所有发放的芯片卡存储各一个记录。

【0056】 部分个性化模块 KEYGEN 优选地根据 RSA 方法或者可供选择替代地根据适当的密
钥导出方法产生优选地芯片卡个别的密钥信息 KEY1 和 KEY2。视采用的方法而异, 部分个性化
模块 KEYGEN 向数据库 CHIPDB 传输密钥 KEY2, 从而把它们向芯片卡 ID 配属地存储在列表
TABKEY 中。部分个性化模块 KEYGEN 向所述芯片卡读 / 写装置传输密钥信息 KEY1, 所述
芯片卡读 / 写装置把得到的密钥信息 KEY1 写入在芯片卡 CHIPK 的非易失存储器 MDM 中。密
钥信息 KEY 持久地预留在所述非易失存储器中。从而可以只用很少的步骤和很少的开销对
芯片卡 CHIPK 进行部分个性化。

【0057】 为了激活芯片卡应用程序和 / 或数据 (最好在另一个个性化地点和在一个较迟的时
刻) 在部分个性化的芯片卡 CHIPK 中安装这样一种应用程序和 / 或这样一种数据。为此
所需要的方法步骤在图 2 中大致示出：

【0058】 在使用者的家 HB 中, 使用者把转交给他的芯片卡 CHIPK 插入进一个芯片卡读 / 写
装置 CHIPLEES2 并且依照没有详细地说明的方式开始所述补充的个性化。接着通信模块
KOM1 读取芯片号 ID 并且优选地通过所述密钥信息 KEY 和 / 或个性化中心 PZ 的一个公开的
密钥加密地用消息 REQ 向个性化中心 PZ 中的通信模块 KOM2 传输所述芯片号 ID 以请求发
放一个指令序列 BS 和指令序列定义 BSD。视芯片卡 CHIPK 的实施方式而异, 同样地可以针
对有待激活的不同应用程序请求而规定不同的消息 REQ, 或者规定一种具有说明要激活芯
片的哪个应用程序参数的消息 REQ。

【0059】 通信模块 KOM2 在在时在事先解密的情况下从消息 REQ 提取所传输的芯片卡号 ID,
并且从消息 REQ 中确定在一个较迟的步骤中在芯片卡 CHIPK 上要激活哪个应用程序。通信
模块 KOM2 联系数据库 CHIPDB 并且查询在该数据库存储在列表 TABKEY 中的密钥信息 KEY2。
此外通信模块 KOM2 从发生模块 BEGENT 请求一个指令序列 BS 以在较迟的时间产生芯片卡应
用程序和所属匹配的指令序列定义 BSD, 其中有时对其产生由通信模块 KOM2 提供密钥信息
KEY2 并且通过发生模块 BEGENT 应用。然后在采用密钥信息 KEY2 和指令序列 BS 的情况下如
此地产生指令序列定义 BSD 使得 : 可以在芯片卡 CHIPK 上把它用于不同的标准检验指令序
列 BS 的执行。

【0060】 取决于有待激活什么芯片卡应用程序, 所述发生模块产生或者取读取安放所述应用
程序的指令序列 BS 和所述指令序列定义, 其中最好在采用密钥信息 KEY2 的条件下芯片卡
独特地加密这两者, 并且从而只能对包含匹配的密钥信息 KEY1 的芯片卡进行解密。此外可
以产生一种在执行时在芯片卡 CHIPK 上安装多个应用程序的指令序列 BS。附加地所述补充
的个性化例程 EPERS 同样地发生模块 BEGENT 提供同所述芯片卡传输 (图中未示出)。如果
对不同的指令序列采用不同的个性化例程这是有利的。

【0061】 通信模块 KOM2 用一个优选地借助于密钥信息 KEY2 加密的和 / 或可以借助于个
性化中心 PZ 的公开的密钥核实的数据消息 DAT 向使用者家 HB 中的通信模块 KOM1 发送指令
序列 BS 和指令序列定义 BSD 以及在一定的情况下发送补充的个性化例程 EPERS。向芯片
卡 CHIPK 传输指令序列 BS 和指令定义 BSD 中的通信模块 KOM1 在使用芯片卡读 / 写装置
CHIPLES2 的条件下把指令序列 BS 和指令序列定义 BSD 写入芯片卡 CHIPK 的存储器 MEM 中。
此外通信模块 KOM 发起调出补充的个性化例程 EPERS，以在所述鉴于补充的个性化执行指令序列 BS。

[0062] 在图 3 中示意地示出再现指令序列 BS 和指令序列定义 BSD 以后在调出补充的个性化例程 EPERS 以后的芯片卡 CHIPK。如果指令序列 BS 和指令序列定义 BSD 加密地在所述芯片卡上播放，就通过所述补充的个性化例程在使用密钥信息 KEY1 的条件下解密它们。

[0063] 优选地在使用标准装置的条件下，采用密钥信息 KEY1 进行解密从而保证后续借助于指令序列信息 BSD 检验指令序列 BS，因为只能够解密对于通过密钥信息 KEY1 准备的指令序列 BS 的解密进行解密。从而不言而明地防止执行其它的指令序列。通过防护整个指令序列 BS 不言而明地防护了指令序列 BS 的各自的芯片卡指令 B1、B2、B3、B4、B5。

[0064] 一个含在补充的个性化例程 EPERS 中的指示器指示所述指令序列 BS 的下一个要执行的指令。这是在指令序列 BS 的第一个指令 B1 的开始。与之并列地另一个含有的指示器指示要分析的指令序列定义 D1，所述第一个要分析的指令序列定义指示给指令 B1，其中在该应用程序例中假定所述指令序列定义 BSD 包含整个指令序列 BS 的信息模式，并且对每个指令刚好有一个指令序列定义单元。

[0065] 一个第三所含的指示器指示在空闲的存储器 FREIMEM 中分配给要安装的应用程序的存储器区域。在本发明的另一个实施方式中，可以已经鉴于部分个性化而为所述应用程序预留该存储器区域。

[0066] 图示为指示器在此只是为了进行说明引入的，并且在实施一种芯片卡 CHIPK 时也可以不用指示器地加以解决。出错计数器 FEHLZ 或已存在于芯片卡 CHIPK 上或者是通过补充的个性化例程 EPERS 在存储器 MEM 中产生。

[0067] 现在补充的个性化例程 EPERS 读取（图中未示出）指令序列 BS 的第一个指令序列 BS 并且借助于所属的指令序列定义单元 D1 检验，要执行的指令 B1 是否满足该指令序列定义单元 D1。从而可以确保，不会执行任何不允许的指令并且不执行任何在伪造的序列中的指令。只要指令 B1 满足指令序列单元 D1，就通过芯片卡 CHIPK 执行它，并且只要它涉及对存储器 MEM 的一种写命令，就用应用程序数据 APPDATA 写入存储器 FREIMEM 的一个部分。从而空闲的存储器 FREIMEM 减少。接着如此地进一步切换所述指示器，使它把下一个要执行的指令设定为指令 B2 并且把下一个要分析的指令序列定义单元设定为单元 D2。

[0068] 在出现错误的情况下，不进一步切换所述指示器并且提高所述出错计数器 FEHLZ。可以按照不同方式进行在出现错误以后的其它行为，例如可以中断指令序列 BS 的执行，或者可以尝试另一次执行所述指令。在中断指令序列 BS 的情况下可以将所述指示器复位到指令序列定义 BSD，或者可以把它预留在应为的话中，以在向芯片卡 CHIPK 传输另一个指令序列 BS 以后在该处继续所述执行。

[0069] 补充的个性化例程 EPERS 或者芯片卡 CHIPK 的操作系统例程可以检验出计数器 FEHLZ 并且在超过一个限定阈值的情况下，可以触发一个动作，例如使芯片卡 CHIPK 不可以使用。

[0070] 图 4 示意地示出在成功地执行指令序列 BS 的四个指令 B1、B2、B3 和 B4 以后的芯片卡 CHIPK。类似地在所述本发明的实施方式中在执行完四个指令以后还分析四个指令序列定义单元 D1、D2、D3、D4。一个原来空闲的四个空闲的存储器区域在执行指令 B1、B2、B3、B4 的情况下用于存储应用程序数据 APPDATA。在执行完指令序列 BS 的所有指令以后并列于所
有的指令序列定义成功地分析指令序列定义 BSD 的指令序列定义并且把所希望的应用程序加载在应用程序数据 APPDATA 中。从而安装芯片卡应用程序并且可以结束所述补足的个性化。

[0071] 可以由补足的个性化例程 EPERES 删除指令序列定义 BS 和指令序列定义 BSD。此外可以结束该例程。在结束所述补足的个性化之后，芯片卡 CHIPL 可以使用现在存储在其上的应用程序。

[0072] 芯片卡 CHIPK 可以向通信模块 KOM1 发送关于成功地执行指令序列定义 BS 的消息（未示出），所述通信模块 KOM1 可以在一个终端的屏幕上向所述使用者显示信息。

[0073] 此外，所述通信模块 KOM1 可以向个性化中心 PZ 发送一个对应的消息（未示出）。[0074] 图 5 示意地示出一个规定一种状态自动装置的指令序列定义 BSD。成功地分析一个指令序列定义单元 D1 和从而成功地执行一个指令 B1 使得所述状态自动装置能够从起始状态 BZ 变换到状态 Z1。如果成功地分析指令序列定义单元 D2 并且从而成功地执行完指令 B2，自动装置又离开该状态并且进一步转换到唯一的后续状态 Z2。因为在图 5 中所示的状态自动装置在状态图中根本没有前向或者后向的弯道，只有一种指令序列定义单元的结果，即完全地贯彻状态自动装置并且把它带入结束状态 EZ。然后该结束状态如每个起始状态 BZ 那样又取通常处于芯片卡 CHIPK 正常运行的一种状态，也就是在补足的个性化以外的状态。

[0075] 从而可以确保：在一个对应于指令序列定义 BSD 的规定的指令序列中执行完指令序列 BS 的所有指令，指令的序列满足指令序列定义 BSD 不执行任何以后嵌入指令序列 BS 中的指令。

[0076] 通过从起始状态 BZ 转移出可以控制释放从此以后的访问权，例如通过设定一个访问权对确定的存储区域的写入权。通过转移到结束状态后可以重新收回这种访问权。如果在其执行以前检查每个芯片卡指令的由之需要的访问权，可以从而达到在执行一个补足的个性化的芯片卡指令具有足够的访问权，并且禁止补足的个性化以外的这种芯片卡指令。

[0077] 本实施例包含在个性化中心 PZ 的验证、受到防护的指令序列定义 BZ 的转移、通过指令序列定义 BSD 检验指令序列 BS，所述指令序列定义 BSD 规定一种无弯道的状态自动装置。从而满足对数字签名应用的通常很高的安全要求。通过个别地结合所说明的特征并且通过个别地实施这种，使得该发明的实施方式能够根据个性化中心的具体安全规定而准确移植该安全规定。
图 5