[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G06K 19/06
G06F 11/00

[12] 发明专利说明书

[21] ZL 专利号 97195304.X

[45] 授权公告日 2005 年 2 月 2 日

[11] 授权公告号 CN 1187709C

[22] 申请日 1997.4.14 [21] 申请号 97195304.X
[30] 优先权
[32] 1996. 4.15 [33] US [31] 60/015,743
[32] 1996.11.22 [33] US [31] 08/755,459
[86] 国际申请 PCT/US1997/006204 1997.4.14
[87] 国际公布 WO1997/039424 英 1997.10.23
[85] 进入国家阶段日期 1998.12.7
[71] 专利权人 尤比克公司
地址 美国明尼苏达州
[72] 发明人 D·R·图施 W·W·霍伊泽尔
审查员 卞喜双

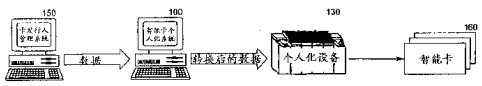
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 王 勇 叶恺东

权利要求书 3 页 说明书 25 页 附图 15 页

[54] 发明名称 用于智能卡个人化的系统和装置

[57] 摘要

一个智能卡个人化系统包括一个包含卡发行人数据格式模板、卡应用、卡操作系统命令和个人化设备规定的数据库，并为一个能够动态调整发行过程中的变化的卡发行过程提供一个集中的输入和输出接口，以允许卡发行人在卡发行过程中能够容易地改变格式、卡应用、卡操作系统和/或个人化设备(130)。 与任一个卡发行人管理系统(150)的系统接口管理向使用的特定个人化设备传输持卡人数据和卡应用，并维护用于实时和脱机询问的统计数据以支持临界管理和报告功能。 而且，系统还利用多种保密方法以防止欺诈行为的发生。



ISSN1008-4274

1.一种用于发行便携式编程数据载体的方法，包括步骤：

从一个卡发行人管理系统获取一个个人化设备标识符和一个持卡人的个人化数据；

从在由个人化设备标识符标识的数据库中的一个记录中获取用于一种个人化设备类型的设备特性数据；以及

向由个人化设备类型的设备特性数据指定的个人化设备传输个人化数据以发行数据载体。

2.如权利要求1所述的方法，还包括将个人化数据转换成一种内部格式，以便于将转换后的个人化数据传输到个人化设备的步骤。

3.如权利要求2所述的方法，其特征在于个人化数据从一种由卡发行人管理系统定义的格式被转换成依据格式模板数据的内部格式。

4.如权利要求3所述的方法，还包括从以一个数据格式标识符标识的数据库中的一个记录中获取格式模板数据的步骤，所述数据格式标识符由卡发行人管理系统提供。

5.如权利要求3所述的方法，还包括从卡发行人管理系统获取格式模板数据的步骤。

6.如权利要求3所述的方法，还包括从在由一个应用程序标识符标识的数据库中的一个应用数据记录中获取格式模板数据的步骤，所述应用程序标识符由卡发行人管理系统提供。

7.如权利要求1所述的方法，还包括步骤：

收集与数据载体发行相关的信息；以及

将来源于收集信息的统计数据报告给卡发行人管理系统。

8.如权利要求1所述的方法，还包括步骤：

从卡发行人管理系统中获取一个应用程序标识符；

从在由用应用程序标识符标识的数据库中的一个记录中获取应用数据；以及

将应用数据传输到由设备特性数据指定的个人化设备。

9.如权利要求1所述的方法，还包括步骤：

从一个保密源中获取保密数据；以及

将保密数据传输到由设备特性数据指定的个人化设备。

10.如权利要求1所述的方法，还包括步骤：

从卡发行人管理系统中获取一个卡操作系统标识符；

从在由操作系统标识符标识的数据库中的一个记录中获取编程控制命令；以及

将编程控制命令传输到由设备特性数据指定的个人化设备。

11.如权利要求10所述的方法，还包括步骤：

从卡发行人管理系统中获取一个应用程序标识符；

从在由应用程序标识符标识的数据库中的一个记录中获取应用数据；以及

将应用数据传输到由设备特性数据指定的个人化设备。

12.一种用于发行便携式编程数据载体的系统，包括：

一个卡发行人管理系统接口，用于从一个卡发行人管理系统获取一个个人化设备标识符和一个持卡人的个人化数据；

一个个人化设备接口，用于从在由个人化设备标识符标识的数据库中的一个记录中获取用于一种个人化设备类型的设备特性数据；以及

个人化设备接口，还用于向由个人化设备类型的设备特性数据指定的个人化设备传输个人化数据以发行数据载体。

13.如权利要求12所述的系统，其特征在于该系统还从在由一个由卡发行人管理系统提供的数据格式标识符标识的数据库中的一个记录中获取格式模板数据，并将个人化数据从一种由格式模板数据定义的格式转换成一种内部格式，以便于个人化设备接口向个人化设备传输转换后的个人化数据。

14.如权利要求12所述的系统，还包括一个跟踪/报告机，用于从与数据载体发行相关的系统中收集数据和将收集的数据报告给卡发行人管理系统。

15.如权利要求12所述的系统，还包括：

一个卡应用接口，用于从在由一个通过卡发行人管理系统接口获得的应用程序标识符标识的数据库中的一个记录中获取应用数据；以及

个人化设备接口，用于将应用数据传输到由设备特性数据指定的

个人化设备。

16. 如权利要求 12 所述的系统，还包括一个保密管理器，用于从一个保密源中获取保密数据并将保密数据传输到个人化设备接口。

17. 如权利要求 12 所述的系统，还包括：

一个卡操作系统接口，用于从在由一个通过卡发行人管理系统接口获得的卡操作系统标识符标识的数据库中的一个记录中获取编程控制命令；以及

个人化设备接口，用于将编程控制命令传输到由设备特性数据指定的个人化设备。

18. 如权利要求 17 所述的系统，还包括：

一个卡应用接口，用于从在由一个通过卡发行人管理系统接口获得的应用程序标识符标识的数据库中的一个记录中获取应用数据；以及

个人化设备接口，用于将应用数据传输到由设备特性数据指定的个人化设备。

19. 一种用于发行便携式编程数据载体的系统，包括：

个人化设备，用于接收一个数据流并据此对便携式编程数据载体进行个人化；

从一个卡发行人管理系统获取的个人化数据；以及

一个智能卡个人化系统，该系统具有包含从下述组中选出的一个或多个数据元的一个数据库：

数据格式模板元件，

卡应用数据元件，

卡操作系统元件，

和个人化设备元件，

其中智能卡个人化系统输出作为处理由至少一个被选择数据元支配的个人化数据结果的数据流。

20. 一种用于发行便携式编程数据载体的方法，包括步骤：

获取一个持卡人的个人化数据和设备特性数据；以及

将个人化数据传输到由设备特性数据指定的个人化设备以发行该数据载体。

用于智能卡个人化的系统和装置

技术领域

本发明涉及数据存储设备，特别涉及制造诸如信用卡、借贷卡、标识卡以及其它业务卡之类的便携式编程数据载体。

背景技术

随着向用户、顾客或雇员发送业务卡的组织数量的增加，要求这些卡被设计成能够满足其特殊服务或应用的需求。这些组织还希望这些卡包含关于持卡人的数据。现有的业务卡将这样的数据编码在卡背面的磁条中，但是一个磁条所能保存的数据量是有限的。一种新型的业务卡是在塑料卡中嵌入一个微处理器芯片以大大增加该卡的数据存储量。此外，对于发卡人，在某几种芯片中能够执行复杂的卡应用，并且该芯片可包含一种操作系统。在工业中，嵌有芯片的业务卡被视为便携式编程数据载体，更普遍地被称为“智能卡”。在一个智能卡的表面被浮刻和/或印制的同时，就以初始化和/或个人化数据对该卡的芯片进行编程。

初始化数据主要包括三种信息：应用数据、保密数据和印制数据。对于一种给定的卡应用来说，应用数据对所有卡都是公用的，并且应用数据包括应用程序码和变元。保密数据用于防止卡的欺诈使用，并且通常以“密钥”的形式出现。诸如一个徽标、条码和各种数字信息之类的印制数据位于卡的表面上。部分或全部相同数据也可以被浮刻在表面上。也可以采用光学技术使卡的部分或整个表面成为一个通过适当的光阅读机可访问数据的存储媒体。

通过一个所谓的“个人化”过程，以单个持卡人的特有信息对智能卡编程。用于一个智能卡的个人化信息类似于当前包含在非智能卡中的个人化信息，如持卡人姓名、帐号、卡的有效期限以及照片。由于卡的存储容量增大，一个智能卡中的芯片除了标准业务卡上的基本信息以外，还可以包含诸如个人签名的图形表示、用于确定授权给持卡人的服务种类的数据以及对那些服务的帐目限定之类的附加数据。

智能卡发行过程必须对每个个人化卡和个人化过程的结果进行

控制和报告。这样就必须保留多方面的报告和查帐文件以支持该卡的跟踪要求。

目前，一个智能卡发行系统必须被设计成能够满足一种特种卡应用，该应用是在一个特种卡操作系统的控制下被编程在一种特殊类型的智能卡上，并且能够将该卡的数据格式化以适用于发行该卡的特殊类型的个人化设备。无论这些变量中的一个（发行者应用、智能卡/卡操作系统和/或个人化设备）何时发生变化，整个发行系统都必须被重新配置，同时增加了在将个人化的智能卡发送给用户的过程中由卡的发行者所负担的时间和费用。此外，当前很多发行系统缺少一种用以向卡发行人提供关于任一批卡的状态的动态反馈的可行装置。

而且，如今所使用的智能卡发行系统利用了由卡的制造商或个人化设备的制造商所开发的专有方法。每个制造商为了鼓励各自的卡和设备的销售而对一种特殊的卡应用只开发一种唯一的个人化方案，并且每个方案仅专用于一个特定的卡发行人。这些唯一的方案试图使这些卡或设备的性能最优，而这种作法不能允许一个能够接受任一种卡操作系统和/或适用于任一种个人化设备的范围更宽、更一般化的个人化过程。

随着对智能卡的需求的增加，需要这样一种智能卡发行系统，它允许卡发行人使用任何类型的个人化设备及其相应的操作系统来处理多种智能卡，并将发行人的特种卡应用随所需的持卡人数据一起嵌入到任一种类型的智能卡中。

发明内容

根据本发明的一个方面，提供一种用于发行便携式编程数据载体的方法，包括步骤：

从一个卡发行人管理系统获取一个个人化设备标识符和一个持卡人的个人化数据；

从在由个人化设备标识符标识的数据库中的一个记录中获取用于一种个人化设备类型的设备特性数据；以及

向由个人化设备类型的设备特性数据指定的个人化设备传输个人化数据以发行数据载体。

根据本发明的另一个方面，提供一种用于发行便携式编程数据载

体的系统，包括：

一个卡发行人管理系统接口，用于从一个卡发行人管理系统获取一个个人化设备标识符和一个持卡人的个人化数据；

一个个人化设备接口，用于从在由个人化设备标识符标识的数据库中的一个记录中获取用于一种个人化设备类型的设备特性数据；以及

个人化设备接口，还用于向由个人化设备类型的设备特性数据指定的个人化设备传输个人化数据以发行数据载体。

根据本发明的另一个方面，提供一种存储在一个存储设备上用于生成便携式编程数据载体的数据结构，包括多个个人化设备元件，其中通过一个唯一的个人化设备标识符对每个个人化设备元件寻址并且每个个人化设备元件指定用于一种个人化设备的操作参数，使得个人化数据被适当地格式化以向发行该数据载体所用的个人化设备传输数据。

根据本发明的另一个方面，提供一种用于发行便携式编程数据载体的系统，包括：

个人化设备，用于接收一个数据流并据此对便携式编程数据载体进行个人化；

从一个卡发行人管理系统获取的个人化数据；以及

一个智能卡个人化系统，该系统具有包含从下述组中选出的一个或多个数据元的一个数据库：

数据格式模板元件，

卡应用数据元件，

卡操作系统元件，

和个人化设备元件，

其中智能卡个人化系统输出作为处理由至少一个被选择数据元支配的个人化数据结果的数据流。

根据本发明的的另一个方面，提供一种用于发行便携式编程数据载体的方法，包括步骤：

获取一个持卡人的个人化数据和设备特性数据；以及

将个人化数据传输到由设备特性数据指定的个人化设备以发行该数据载体。

根据本发明的的另一个方面，提供一种用于发行便携式编程数据载体的系统，包括一个系统接口，用于获取一个持卡人的个人化数据和设备特性数据，并将个人化数据传输到由设备特性数据指定的个人化设备以发行该数据载体。

根据本发明的的另一个方面，提供一种用于发行便携式编程数据载体的系统，包括一个接口装置，用于获取一个持卡人的个人化数据和个人化设备的特性数据，并将个人化数据传输到由该特性数据指定的个人化设备以发行该数据载体。

根据本发明的的另一个方面，提供一种用于发行便携式编程数据载体的系统，包括：

一个系统接口装置，用于从一个卡发行人管理系统获取一个个人化装置标识符和一个持卡人的个人化数据；

一个个人化接口装置，用于从在由个人化装置标识符标识的数据库中的一个记录中获取用于一种个人化装置类型的特性数据；以及

个人化接口装置，还用于向由个人化装置类型的特性数据指定的个人化装置传输个人化数据以发行数据载体。

通过向能够动态适应发行过程中的变化的智能卡个人化过程提供一个输入和输出的中央接口，智能卡个人化系统找出现有技术中的弱点。该系统与任一个发行人管理系统进行接口，管理持卡人数据的传输和对所用的特定个人化设备的卡应用，并采集对实时和脱机查询的统计量以支持关键的管理和报告功能。该系统维护关于发行人数据格式、卡操作系统、卡应用程序以及个人化设备类型的数据库。这个数据库使该系统能够处理数据的任意组合和排列，从而对发行人来说改进了成本和投放市场的时间。而且，该系统接口于不同的有关卡保密的方法论以减少欺诈行为的发生。

附图说明

图 1A 是表示与一个智能卡个人化系统相结合的智能卡发行过程的方框图。

图 1B 用于图 1A 所示的智能卡个人化系统的输入和输出连接的功能性方框图。

图 1C 是示出了构成图 1B 所示的智能卡个人化系统的一个实施例的软件模块和数据结构的功能性方框图。

图 2 是在图 1C 的基础上附加了一个管理智能卡密钥的保密模块的实施例的功能性方框图。

图 3 是示出管理多种类型的卡和个人化设备的最小配置的智能卡个人化系统的另一个实施例的功能性方框图。

图 4 是在图 3 的基础上附加了一个管理多个卡操作系统的模块的实施例的功能性方框图。

图 5 是图 4 的实施例附加了保密模块的功能性方框图。

图 6 是图 3 的实施例附加了一个管理多个卡应用的模块的功能性方框图。

图 7 是图 6 的实施例附加了保密模块的功能性方框图。

图 8 是用于实现智能卡个人化系统的各项功能的计算机软件的高级流程图。

图 9 是利用软件模块和数据记录的智能卡个人化系统的替换实施例的功能性方框图。

图 10 是用于实现图 9 所示的智能卡个人化系统实施例的各项功能的计算机软件的高级流程图。

图 11 是图 9 所示的智能卡个人化系统实施例所用的一个卡结构模板记录的数据字段图表。

图 12 是图 9 所示的智能卡个人化系统实施例所用的一个数据格式模板记录的数据字段图表。

图 13 是图 9 所示的智能卡个人化系统实施例所用的一个卡应用数据记录的数据字段图表。

图 14 是示出了由智能卡个人化系统所跟踪的例项的报告格式。

具体实施方式

在下述的实施例的详细描述中，参照作为其组成部分并以示出说明实现本发明的具体实施例的形式的附图。这些被详细描述的实施例足以使本领域的技术人员实施本发明，并应当理解也可以利用其他在不偏离本发明的主题和范围的前提下对结构、逻辑和电学方面作出改进的实施例。因此，下述的详细说明不能作为对本发明的限定，只有后述的权利要求才能限定本发明的范围。

附图中参考标号的起始数字通常相应于图号，出现在多幅附图中的相同部件以相同的参考标号为标识。

发行智能卡

标准的业务卡，如常用的信用卡对大多数人来说是熟悉的。一个业务卡通常具有被印制或浮刻在卡表面上的持卡人信息，如姓名和帐号。一般，业务卡包含一个包含有编码后的持卡人数据等的磁条。对每个业务卡的持卡人数据进行印制/浮刻/编码的过程被称之为“个人化”。每个业务卡还会经过一个被称为“初始化”的过程，在该过程中通用于一批卡的特种信息，如发行人标识符和批号等被设置在卡上。

一个智能卡与标准业务卡的区别在于一个计算机微处理器芯片被嵌入到塑料卡中以大大增加卡的数据存储量。在某些种类的智能卡中，卡制造商预先在芯片中装入几种可用的卡操作系统之一，并且在个人化过程中由该操作系统控制芯片的编程。此外，在特定种类的芯片中也可以执行指定给卡发行人的复杂卡应用。

一个智能卡初始化数据主要由三种类型的信息构成：应用数据、保密数据和印制数据。对于一个给定的卡应用来说，应用数据对所有的卡都是通用的，并且包括被编程到芯片中的应用程序代码和变量。一般用作密钥或保密函数的保密数据验证卡上的数据并防止卡的欺

诈使用。诸如徽标、条码和不同类型的数字信息之类的印制数据被印在卡的表面上。一些或所有相同的数据也可以被浮刻在表面上。也可以采用光学技术使智能卡的部分表面成为具有以适当的光阅读器可读取的数据的存储媒体。

智能卡的个人化信息相似于目前包含在非智能卡中的个人化信息，如持卡人姓名、帐号、卡有效期和照片。由于卡的存储容量增大，一个智能卡中的芯片除了标准业务卡上的基本信息以外，还可以包含诸如个人签名的图形表示、用于确定授权给持卡人的服务的种类的数据以及对那些服务的帐目限定之类的附加数据。

智能卡个人化系统

图 1A 示出了结合本发明的智能卡个人化系统的一个实施例的智能卡发行过程的组成部分。智能卡个人化系统 100 从一个卡发行人管理系统 150（一般专有于卡发行人）接收数据，将该数据转换成一个数据流，并将数据流输出到用于对智能卡 160 进行个人化的个人化设备 130。卡发行人管理系统 150 管理持卡人数据并确定要发行的卡的种类，要嵌入卡中的卡应用以及利用哪种个人化设备来发行用于一个特定持卡人的卡。如图 1A 所示，卡发行人管理系统一般为一个计算机程序，但智能卡个人化系统 100 也能够从其他的输入端接收数据，例如一个人从一个电话键盘区输入数据。

在图 1A 中将智能卡个人化系统 100 作为一个在计算机中执行的软件程序来说明。如下所述，智能卡个人化系统 100 访问定义了不同类型的卡和卡操作系统、卡应用和个人化设备的数据库记录。

软件和数据库的逻辑功能可以分布到一个客户/服务器网络中的多个计算机中或集中到一个处理器中。这些功能也可以被分布到通过标准局域网、广域网、专用电话线或其它用于宽松耦合处理器的通信装置相连接的处理器中。在工业标准工作站和/或个人计算机硬件上以及一个诸如 Unix、Windows95©或 Windows NT©之类的操作系统下执行该软件程序。

系统 100 控制卡打印机、浮刻设备和综合或附加智能卡接口设备，这些设备在图 1A 中以个人化设备 130 表示。个人化设备 130 还代表诸如大卷卡打印机/浮刻器、小卷卡打印机/浮刻器、自动出纳机（ATM）、销售点终端、无人售货机、个人计算机、网络计算机和联

机电信设备之类的设备。由于人们已经在已有的非智能卡个人化设备上进行了投资，所以很多卡发行人不会购买全新的智能卡个人化设备，而是在他们已有的个人化设备上增加一个智能卡接口设备，该接口设备能够在旧设备执行打印和浮刻功能的同时对卡中的芯片进行编程。在这样的配置中，运行智能卡个人化系统 100 的计算机系统或“主机”被物理连接到这两种设备或仅连接到其中一种设备上。在后一种情况中，主机控制直接相连的设备并与另一设备具有逻辑连接。设备与主机之间的物理连接依制造商和设备模型的不同而不同。通用工业标准连接包括串行 RS232、SCSI（小型计算机系统接口）、以太网和串行 TTL（晶体管-晶体管逻辑电路）。此外，一些设备需要一个专用的总线连接。

也可以通过标准局域网、广域网、专用电话线或其它用于传输数据的远程通信基础设施来实现智能卡个人化系统 100 和卡管理系统 150 和设备 130 之间的连接。在 1996 年 7 月 9 日授权给 Laing 等人的美国专利 No.5,524,857 中描述了在对智能卡个人化时所使用的这种远程连接。另一种连接对所属技术领域的技术人员来说是显而易见的并在本发明的范围之内。

图 1B 是智能卡个人化系统的一个实施例的方框图，用于说明智能卡个人化系统 100 与一个卡发行组织为了发行智能卡而采用的功能之间的逻辑连接。由卡发行组织保存的持卡人数据包含有关每个持卡人的信息，如姓名、帐号、卡的有效期以及可应用的服务。图 1B 中作为持卡人数据 152 的模型示出了将持卡人数据输入到卡发行人管理系统 150 中的几种方式。卡发行人管理系统 150 可以接收诸如磁带、软盘或 CD ROM 之类的计算机媒体上的持卡人数据。另外，可以通过一个诸如通用交换电话网络、分组交换网络，即 Internet、专用线路或电缆/卫星电视信号之类的联机连接来输入持卡人数据 152。将持卡人数据 152 输入到系统 150 中的其他方式对于所属技术领域的技术人员来说是显而易见的。

除卡发行人管理系统 150 之外，卡发行人通常还具有与智能卡个人化系统 100 接口的已有报告功能 154，以使卡发行人能够查阅由系统 100 保存的统计信息。同样，由卡发行人提供并表示为密钥管理器 111 和密钥数据库 128 的外部保密源提供了与卡发行人管理系统 150

和智能卡个人化系统 100 共同工作的保密函数。图 1B 还说明了支持具有附加智能卡接口设备的卡发行人的智能卡个人化系统 100 的一个替换实施例。系统 100 将个人化信息的一部分导向旧的个人化设备 130 并将数据的剩余部分导向对芯片编程的智能卡接口设备 132 中的后处理器 132。下面将详细描述这些功能。

后面附图所示的用于智能卡个人化系统 100 的软件程序的实施例作为代码模块的组合，其中每个模块执行发行过程的一个特定部分。在这些实施例中，通过定义的输入和输出程序调用来连接模块并通过用于对存在数据结构中的数据进行访问的标准数据询问命令来连接数据结构。模块之间以及模块和数据结构之间的通信协议根据编写模块所用的语言和用以支持数据库的基础数据管理系统的不同而不同。

图 1C 是图 1B 所示的没有外部保密功能的智能卡个人化系统 100 的更详细的功能性方框图。图 1C 示出了软件模块和数据库记录之间使智能卡个人化系统 100 能够在发行智能卡时组合多种发行人数据格式、卡操作系统、卡应用和个人化设备的内部连接。

智能卡个人化系统 100 向一个卡发行人管理系统 150 提供一个定制的卡发行人管理接口 101。在这个实施例中，卡发行人管理系统 150 从一个持卡人数据库 152 向系统 100 传送个人化数据。系统 100 中的每个软件模块都要求个人化数据以一种特定的内部格式被传送。由于个人化数据是由卡发行人定义的不同于软件模块所要求的内部格式的外部格式，所以系统 100 利用数据格式模板将个人化数据转换成内部格式。系统 100 通过一个经过卡发行人且系统 100 用于获得一个如记录 120 和卡发行人管理系统接口 101 之间的可选连接所述的可选数据格式模板记录 120（图 1C 中模型所示）的数据格式标识符来获得数据格式模板。另外，卡发行人以向系统 100 传送数据格式模板记录来取代数据格式标识符。在另一个实施例中，数据格式模板可以来源于卡应用记录 124 中的数据，该卡应用记录由经过发行人的应用程序标识符指定，如卡应用数据库 124 和卡发行人管理系统接口 101 之间的可选连接所述。

在图 1C 的替换实施例中，通过将保密函数作为卡应用记录的一部分传送到系统中而向智能卡个人化系统 100 的内部提供保密功能。

图 1C 中还示出了一个个人化数据格式与内部格式相匹配的替换实施例。由于在这个实施例中不需要外部和内部格式之间的转换，所以不需要数据格式模板，从而不存在数据格式记录 120，也不存在卡发行人管理系统接口 101 与数据格式记录 120 和卡应用数据库 124 之间的连接。数据格式记录 120 可由多个指示系统 100 的表组成，使得个人化数据的适当分列或指示持卡人数据记录的字段所出现的顺序的简表对于所属技术领域的技术人员来说是显而易见的。用于确定上述个人化数据的格式的各种替换过程隐含在这里所述的智能卡个人化系统 100 的所有实施例中。

利用一个由卡发行人管理系统 150 提供的卡标识符，一个卡操作系统接口模块 103 读取卡操作系统 122 专用的编程控制命令用于嵌入到所发行的卡中的微处理器芯片。编程控制命令利用个人化数据和卡发行人所选择的卡应用引导芯片的编码。

每个卡应用包括程序代码和作为应用数据 124 存在数据库中的可变数据，并且以一个应用程序标识符为标识。卡发行人管理系统 150 向系统 100 传送一个或多个被卡应用接口模块 105 使用以获得相应应用数据 124 的程序应用标识符。

由一个个人化设备标识符定义卡发行人意欲用来发行批量卡的个人化设备。一个个人化设备接口模块 107 获得相应于个人化设备标识符的个人化设备 130 类型所专有的设备特性数据 126。个人化设备接口 107 还获得编程控制命令、应用代码和变量以及转换后的个人化数据，并将这个数据的全部内容传送到设备特性数据 126 所指定的个人化设备 130 中以发行智能卡。

系统 100 的一个替换实施例支持一个这样的卡发行人，他已经通过使个人化设备接口 107 将转换后的个人化信息的一个子集导向旧的个人化设备 130 而将数据的剩余部分导向智能卡编程设备中的后处理器 132，从而增大其已有的带有一个智能卡编程设备的个人化设备。

智能卡个人化系统 100 还提供一个跟踪/报告模块/机 109，它从系统 100 的其它模块中收集统计信息并对作为硬拷贝报告 154 输出或作为卡发行人管理系统 150 中的一个报告功能的输入的统计信息进行格式化。由于这个统计信息是被实时采集的，所以卡发行人管理系统 150 能够交互地查询跟踪/报告模块 109 以便于在执行该模块时获得

有关智能卡个人化系统的统计信息。图 14 示出了由跟踪/报告模块 109 所监视的例项。

在图 2 所示的一个替换实施例中，智能卡个人化系统 100 包括一个以密钥管理器模块 111 和密钥数据库 128 的形式存在的保密源。在制造智能卡时，自动售货机在芯片上包括，保密结构以防止非授权的程序编写。通常根据编写在卡上的应用来实施保密体系。例如，编写在一个存储值应用中的密钥不同于被编写在保健应用中的密钥。保密体系的实施方案也随卡的类型不同而不同：一些卡只需要一个启动芯片编程的密钥，而另一些卡则需要多个密钥来启动芯片编程和执行附加的保密功能。图 2 示出了密钥管理器 111 在与一个需要多个密钥的卡上的保密体系接口时的基本功能。

如图 2 所示，密钥数据被存储在位于智能卡个人化系统 100 的外部的密钥数据库 128 中，并被卡发行人或其他保密源维护。扩展密钥管理器 111 来管理或多或少的密钥和与一个由智能卡个人化系统 100 本身管理的密钥数据库进行接口，这种作法依赖于应用、操作系统和特定卡发行应用所使用的个人化设备，并且对所属技术领域的技术人员来说是显而易见的。

密钥管理器 111 还提供了附加装置以保证密钥数据的真实性、完整性和安全性。在一个实施例中，通过不同的加密方法来确保密钥数据的真实性。通过数字签名装置来实现密钥数据的完整性，该数字签名装置利用公共密钥（public keys）来保证正在从有效源发送和接收密钥数据。通过对被传输的具有一个私人密钥的数据加密来保证密钥数据的安全性，该私人密钥与数据接收器共享并且数据接收器在接收数据的同时利用该私人密钥对数据进行解密。

在系统 100 从密钥数据库 128 中接收一个密钥记录之后，与卡操作系统接口 103 和卡应用接口 105 相连的密钥管理器 111 执行密钥的真实性、完整性和安全性功能。然后，系统 100 通过个人化设备接口 107 将密钥数据与其他卡数据一起传送到个人化设备 130 中。

在一个替换实施例中，密钥管理器 111 将保密信息送至智能卡个人化系统 100 的其他模块中。例如，在将数据送至智能卡个人化系统 100 之前，可通过卡发行人管理系统 150 对持卡人数据部分，如 PIN（个人标识号）代码进行加密。卡发行人管理系统接口 101 通过密钥

管理器 111 从密钥数据库 128 中读出加密密钥，并在将 PIN 代码编码或编程到磁条和/或芯片中之前对该数据解密。

在另一个替换实施例中，密钥管理器 111 是一个“钩”在智能卡个人化系统 100 中的代码，该系统为一个提供所需的保密功能的外部保密源提供一个通路连接。这种外部保密源的一个例子就是一个由第三者编写的保密管理器程序，该程序管理类似于密钥数据库 128 的由密钥和/或保密函数构成的保密数据库。保密函数是由保密管理器执行的外部例程，或由保密管理器传递并由智能卡个人化系统 100 执行以提供所需的保密函数的代码模块，或二者的组合。

图 3 示出了智能卡个人化系统 100 的最小配置。在这个实施例中，软件只启动卡发行人管理系统接口模块 101 和个人化设备接口模块 107。这个实施例允许卡发行人利用系统 100 对非智能卡进行个人化，从而节省两个分离的个人化系统的成本，同时允许卡发行人使用多种数据格式和多种类型的个人化设备。图 3 还示出了一个结合图 1C 的附加替换实施例，该实施例包括如上所述的跟踪/报告模块 109。

在另一个替换实施例中，当光编码设备被用作个人化设备 130 时，图 3 所示的智能卡个人化系统 100 对一个光业务卡上的数据进行编码。

图 4 和 5 描述了另一个在卡发行人没有将卡应用编写到智能卡芯片上时实现的替换实施例。这些实施例允许卡发行人通过在多种类型的个人化设备上附加不同的操作系统来发行多种卡，而无需重新配置智能卡个人化系统 100。结合图 1C，如上所述，图 4 包括支持报告和后处理的模块。图 5 示出了在图 4 的基础上附加了密钥管理器模块 111 的实施例，该密钥管理器模块 111 为用于向个人化设备 130 传输数据的卡操作系统接口 103 提供安全性。

同样地，图 6 和 7 描述了支持卡发行人将智能卡上的芯片只用作卡应用的数据存储设备，而在芯片上无需执行操作系统的实施例。智能卡个人化系统 100 支持多种卡应用，这些应用适用于以多种个人化设备发行的多种卡类型。除了密钥管理器 111 向卡应用接口 105 提供密钥和/或功能而不是向卡操作系统接口 103 提供密钥和/或功能之外，图 6 和 7 与图 4 和 5 是相似的。

图 8 是用于实现上述智能卡个人化系统 100 的功能的软件的一个

实施例的高级流程图。在块 801，该软件从卡发行人管理系统得到一个用于一批将被发行的业务卡的个人化设备标识符。根据将被发行的卡的种类，该软件同时还得到一个或多个应用程序标识符和/或一个卡操作系统标识符。然后该软件通过上述过程之一得到相应于个人化数据的格式的特定数据格式模板（块 803）。在块 805，该系统从由个人化设备标识符指定的个人化设备记录中得到用于发行成批的卡的个人化设备的设备特性数据。

如果一个卡操作系统标识符被卡发行人管理系统传递（块 807），则在块 809 该软件从相应于卡操作系统标识符的卡操作系统数据库记录中读出编程控制命令。块 811 和 813 在从数据库中读出应用数据，如代码和/或变量的同时，对一个卡应用执行相同的逻辑。此时，该软件已经得到了该批的所有卡所必需的公用数据，并通过该逻辑来开始循环发行对单个持卡人的卡。

卡发行人管理系统将一个持卡人的个人化数据传递到该软件（块 815），该系统将数据项从数据格式模板所定义的格式转换成智能卡个人化系统的模块所使用的内部格式（块 817）。如果卡芯片包含需要密钥的保密体系（块 819），则该软件在块 821 从适当的密钥源中得到执行密钥功能所需的密钥数据。

现在该软件准备将数据传送到个人化设备以对该卡编程。如果该卡被密钥保护，则在块 823 执行密钥功能并传送密钥数据。如果可用，就传送用于芯片操作系统的编程控制代码（块 825 和 827）；然后，如果需要，就传送应用代码和/或变量（块 829 和 831）。最后，发送被转换成内部格式的持卡人个人化数据（块 833）。

在数据被发送到卡中之后，该软件在块 839 向统计信息中加上适当的值，收集所述统计信息用于卡发行人管理系统。如果更多的同一批中的卡被持续发行（块 841），则该软件返回块 815 并获取下一个持卡人的个人化数据。否则，该软件确定卡发行人管理系统是否具有要发行的不同批号的卡（块 843）并返回块 801 以获取必要信息来重复对新的一批卡的操作。如果没有要发行的卡了，就退出该软件。

在不超出本发明范围的前提下，可以改变卡发行人管理系统 150 向智能卡个人化系统 100 传递必要数据的装置和智能卡个人化系统处理来自卡发行人管理系统的数据的顺序。由图 9 和 10 所述的替换实

施例所示出的系统 100 的不同操作环境说明了不同的排列。

在图 9 中，对于一个诸如分别相应于图 1B 所示的 111 和 128 的保密管理器 940 和保密数据库 942 之类的保密源来说，一个保密模块 911 作为一个进入智能卡个人化系统 100 的通路。保密管理器 940 控制对保密数据库 942 的访问并连接到保密通路 911 中以执行智能卡个人化系统 100 的必要保密功能。保密通路 911 与卡发行人管理系统接口 901 相连接，它允许接口 901 请求保密管理器 940 对由卡发行人管理系统 950 以加密格式传递的个人化数据进行解密。保密通路 911 也与卡应用接口 903 和卡操作系统接口 905 相连接，使得它能够向那些接口提供必要的密钥和/或保密函数，如上面结合图 2 所述。

而且，在利用卡标识符获得卡操作系统 924 专用的编程控制命令之前，图 9 所示的智能卡个人化系统 100 的实施例能够获得由应用程序标识符指定的应用数据 922。这个实施例允许在读取用于卡操作系统 924 的编程命令和设备特性数据 926 之前，将个人化数据和应用数据转换成内部格式，从而提高每个智能卡的处理速度。

标准业务卡具有被印制和浮刻到卡表面上的数据和/或被编码到卡上的磁条中的数据。利用智能卡，数据也可以被存到微处理器中的一个内部存储区中。相同数据可以被置于卡表面上、磁条中和芯片存储器中。卡中和卡上的数据的准确排列随正在被发行的智能卡的种类和卡发行人的要求而改变。

图 10 是图 9 所示实施例的高级流程图并结合图 11、12 和 13，进一步说明了如何利用不同的装置来实现智能卡个人化系统 100。卡发行人管理系统 950 在块 1001 向智能卡个人化系统 100 传递一个定义了智能卡的配置的卡结构模板。

图 11 说明了卡结构模板记录 1100 的数据结构的一个实施例。微处理器芯片标识符 1101 和卡操作系统标识符 1102（如果有）专指要被发行的智能卡的类型。主文件定义 1103 包含诸如芯片源和该芯片被更改的最后日期之类的控制信息。系统文件定义 1104、1105、1107 包含芯片存储器中的系统文件的位置地址。系统文件被卡操作系统使用并包含诸如用于卡和应用的 PIN 代码以及算法表之类的信息。在图 11 所示的实施例中，主文件和系统文件定义符合国际标准组织（ISO）指令号 7816-4。

卡结构模板记录 1100 的下面三个字段定义了卡表面和磁条上的数据的排列。如果信息被印制在卡上，如持卡人的照片 1109，则卡发行人管理系统 950 将该数据印制在卡表面上的位置传递到卡结构模板记录 1100 的打印模板中。相似地，要浮刻的数据在卡表面上的位置被传递到浮刻模板中，并且要被编码到磁条中的数据列被传递到磁条模板中。在卡结构模板记录 1100 中，浮刻数据包括持卡人的姓名（EMName）1111，帐号（EMAcct）1113，和有效日期（EMXdat）1115，以及由帐号（MSAcct）1117 和有效日期（MSXdat）1119 构成的磁条数据。在打印、浮刻和磁条模板中的数据项的个数随卡发行人所希望的智能卡的配置而变，这对所属技术领域的技术人员来说是显而易见的。

如果卡发行人想将卡应用编写到智能卡的芯片中，则在卡结构模板记录 1100 的字段 1121、1123、1125 中卡发行人将应用程序标识符传递到智能卡个人化系统 100。每个应用具有与其相关的特定保密函数（1127、1129、1131），并且该信息也被卡发行人管理系统 950 传递。卡结构模板记录 1100 还包含用于发行智能卡的个人化设备的个人化设备标识符 1123。

在一个替换实施例中，智能卡个人化系统 100 通常将所用的卡结构模板记录存储到一个内部数据库中，使得卡发行人管理系统 950 只需要传递一个卡结构模板标识符，该标识符标识哪个卡结构模板记录被用于特定的一批卡。

在块 1003，智能卡个人化系统 100 从卡发行人指定的一个预定位置中获得用于个人化数据的数据格式模板。如果卡发行人已经向系统 100 传递了一个数据格式标识符，则从数据格式数据库 920 中读出相应于该数据格式标识符的数据格式模板记录。另外，卡发行人可以传递数据格式模板记录本身。当数据格式标识符和数据格式模板记录都没有被传递到系统 100 时，由卡应用数据确定个人化数据的格式，下面将更详细地予以说明。

图 12 示出了一个数据格式模板记录的例子。数据格式模板记录 1200 定义了持卡人数据库 952 中的一个理想的个人化数据记录格式，其中帐号 1201 为第一字段，持卡人姓名 1202 为第二字段，卡的有效日期 1205 为第三字段。在一个实施例中，个人化数据记录是以

逗号定界的，所以无需用数据字段长度来定义记录格式。从而图 12 所示的数据格式模板记录 1200 完全定义了对智能卡个人化系统 100 的一个以逗号定界的个人化数据记录的结构：133444999922，Mary Jane Smith，0299。

在块 1007，智能卡个人化系统 100 获得相应于由卡发行人管理系统 950 传递的应用程序标识符的卡应用的应用数据 922。如果没有应用程序标识符被传递，则智能卡个人化系统 100 得到默认的应用数据（块 1008）。相应于应用程序标识符的卡应用数据记录中默认值和/或应用数据被插入到卡结构模板记录 1100 的相应字段中，即 1121、1123、1125。

图 13 示出了一个卡应用数据记录的实施例。卡应用数据记录 1300 中的第一字段是应用名称 1301。与其他基于计算机的应用程序一样，一个卡应用处理来自向自动出纳机一样的外部源或来自向编码到微处理器的存储器中的数据文件一样的内部源的数据。利用智能卡使微处理器执行适当的应用，并且该应用按顺序访问内部文件以读取或存储数据。为了访问内部数据，卡应用数据记录包含指向芯片存储器中的应用文件（1302、1305、1307）和应用文件内的字段位置的指针。在发行卡时，利用来自持卡人数据库 952 的数据对一些字段进行初始化。应用数据 1300 包括一个指向位于芯片存储器中的一个持卡人文件的地址 1303，并且定义持卡人文件包含以下三个字段：持卡人姓名（ICName）1309，帐号（ICAcct）1311 和有效日期（ICXdat）1313。附加内部数据被存储在其他应用文件中，并且那些附加文件的格式也是由应用数据 1300 定义的。

如果嵌入智能卡中的芯片包含一个由卡结构模板记录指定的操作系统，则智能卡个人化系统 100 在块 1011 从卡操作系统数据库 924 中得到一组用于操作系统的编程控制命令。每种操作系统的编程控制命令包括用于诸如生成和访问芯片存储器中的文件、在位于芯片存储器中的文件中读写记录之类的功能的命令，用于证实 PIN（个人标识号）代码的保密命令和用于改变存在芯片中的货币金额的控制处理。

在块 1013，智能卡个人化系统 100 从个人化设备数据库 926 中得到相应于卡结构模板记录中的个人化设备标识符的设备特性数据。设备特性数据中包括用于控制个人化设备操作的一组个人化编程控制

命令。在具有卡操作系统的情况下，个人化控制命令专用于设备的售主，但是通常包括面向管理、格式化和智能卡制造方面的命令。

当智能卡个人化系统100已经得到了定义一个智能卡所需的所有数据时，就准备好从卡发行人管理系统 950 接收个人化数据记录952。在每个个人化数据记录952在块1015被传递时，如果存在数据格式模板，智能卡个人化系统100在块1017就利用数据格式模板将个人化数据转换成内部格式，并利用卡应用数据和卡结构模板将个人化数据映象到用内部原本语言（internal scripting language）写成的命令原本（command script）中的变量中。下面进一步说明该转换和映象处理。利用诸如Basic、Java或C之类的标准编程语言代替内部原本语言的替换实施例也属于本发明的范围之内。

智能卡个人化系统100检查智能卡发行过程中各个不同部分的保密要求。在图11所示的卡结构模板的实施例中，在块1019由卡结构模板记录 1100 指定对应用的保密要求。如果有保密要求，则在块1021，智能卡个人化系统100从保密管理器940中获取保密数据和/或函数，并将这些函数加入到内部原本中。智能卡个人化系统100的一个替换实施例向用以从保密数据库 942 读取适当的保密数据和/或函数的保密管理器940传递卡操作系统和个人化设备的标识符以及应用程序标识符。保密函数通常利用来自附加数据源的数据结合存在芯片中或来自象保密管理器940一样的外部保密模块的算法表来执行密钥真实性、数据完整性、数据安全性的判断和其他结合图2所述的保密过程，其中所述附加数据源包括存在内部芯片文件中的数据，个人化数据952，操作系统数据库924，卡应用数据库922等。

一旦完成了内部命令原本，就必须将其转换成适用于本地的卡操作系统（如果存在）和个人化设备的专用编程控制命令，以便于将个人化数据传送到智能卡中。在这个实施例中，在块1025和1027，由一个原本语言注释器利用从卡操作系统数据库924和个人化设备数据库926中获取的信息执行这个转换过程。

在块1029，智能卡操作系统100将注释后的原本传递给个人化设备，该设备执行编程控制命令以将适当的个人化数据分别浮刻/印制到智能卡的表面上，编码到智能卡的磁条中和编写到智能卡的芯片中。如前所述，如果卡发行人选择购买一个附加的智能卡编程设备安

装到已有的个人化设备上，则智能卡个人化系统 100 的一个替换实施例直接将浮刻和编码的控制命令分配给个人化设备 930 而将用于芯片的控制命令分配给智能卡编程设备中的后处理器 132.

当一个卡的发行过程已经结束时，如果还有同一类型的其他卡等待发行，则智能卡个人化系统 100 获取下一个个人化数据记录（块 1033）。否则，智能卡个人化系统判断是否还有另一批不同类型的智能卡在等待发行（块 1001）并通过从卡发行人那里获得一个新的卡结构模板记录而再次开始发行过程。

在下面的例子中利用样本数据来进一步说明由图 9 和 10 所示的智能卡个人化系统 100 的实施例执行的处理过程。卡发行人管理系统 950 通过向智能卡个人化系统 100 发送一个卡结构模板记录，应用程序标识符，一个卡操作系统标识符，一个个人化设备标识符和一个可选的数据格式模板标识符或一个数据格式模板记录来请求发行过程的初始化。在这个例子中，卡发行人管理系统 950 传递一个包含下示标识符的应用资源模板记录。系统 100 利用上述和下面结合样本持卡人数据记录详细说明的过程之一得到一个数据格式模板。

应用资源模板记录

```
[A1]
DFT=CARD1.DFT
CAT=CARD1.CAT
CID=CHIPX.CID
CPT=CARD1.CPT
SOURCE=A1
```

记录中的第一语句标记了用于一个特定应用的信息的起始，在此例中为“A1”。接在后面的四条语句定义了用于卡结构模板记录（DFT）、卡应用记录（CAT）、卡操作系统记录（CID）以及个人化设备记录（CPT）的标识符。最后一条语句是由卡发行人管理系统 950 生成的一个包含持卡人数据记录的文件的名称。卡发行人管理系统 950 输入持卡人数据作为要发行一个卡的请求或要发行“一批”卡的请求。

系统 100 从数据库中读取与标识符相应的记录。然后系统 100 利用包含在卡结构模板和数据格式模板中的信息建立一个内部“原

本”，这个原本后来翻译成包含在卡操作系统和个人化设备记录中的特定命令，其中个人化设备记录指示个人化设备处理每个持卡人的个人化数据和向每个持卡人发送卡。

下面示出了持卡人数据记录 952 的两个例子。

持卡人数据记录
Smith, James^12653683091245^0998^041052^mmmm
Anderson, Sue^39485003984138^0297^110248^mmmm

在这些记录中，由卡发行人所定义的格式将帐户名（持卡人姓名）置于第一个字段内，其后依次为帐号、有效日期、出生日期和医疗保健数据。

在处理每个持卡人的数据记录 952 时，系统 100 利用数据格式模板对数据记录进行翻译。系统 100 还利用数据格式模板和卡应用记录 922 来验证数据 952 以保证正确的数据和格式。在下表的第一行中示出了与如上所示的持卡人记录格式相应的数据格式模板示例。包含在表中的 James Smith 个人化数据记录示出了数据格式模板与持卡人数据记录字段之间的一致性。数据格式模板给持卡人记录中的每个字段分配一个与在系统 100 内被使用的内部顺序相应的内部标签%1，%2 等。

数据格式模板记录				
%1	%2	%3	%4	%5
Smith, James^12653683091245^0998^041052^mmmm				

上述例子表示了最简单的情况，即一个持卡人数据记录 952 的字段是按照智能卡个人化系统 100 所使用的内部顺序排列的。这种一一对应意味着系统 100 无需将持卡人数据字段转换成内部字段顺序。在这样的情况下，是不需要数据格式模板记录的。这样，在一个替换实施例中，卡发行人不必向智能卡个人化系统 100 传递一个数据格式标识符，而只需传递一个用于通知系统 100 由于持卡人数据字段与内部字段顺序一一对应而不需要数据格式模板的指示器，如一个标志。系统 100 按照指示器的指示跳过转换步骤。

下面示出的更复杂的例子就是持卡人数据记录 952 的字段和字段中的数据相对内部系统顺序来说是无序的。在这种情况下就需要进行转换。

发行人格式中的持卡人数据

12653683091245 James Smith 0998 041052 mmmm

转换成内部格式的持卡人数据

Smith, James^12653683091245^0998^041052^mmmm

系统 100 利用数据格式模板将数据字段转换成上述内部顺序。该转换可能会导致数据字段的物理重排或可能是逻辑重排，其中每次系统 100 参照持卡人数据记录中的一个字段时，数据格式模板作为一个关键字被调用。为转换不同排列的持卡人数据而设计的各种数据格式模板对于所属技术领域的技术人员来说是显而易见的，就象本例用于上述最简单的表中的字段或一组分析的指令或其它手法的替换一样。

卡结构模板记录描述了卡上的芯片结构。在如下所示的例子中，$MF 项定义了一个根目录（3F00），而$DF 项定义了一个医疗应用（5F20）和一个记帐应用（5F10）。$EF 项定义的特殊应用，如包含帐户名的 6F00 和包含帐号的 6F10 位于每个目录中。所有用文件描述的数据驻留在卡结构模板中，并在智能卡发行过程中的不同情况下被参照。

卡结构模板记录

```
$CHIP=3102, MEM=8192, SIZE=N10
$MF PATH=x3F00, TAG=ROOT, TITLE='根目录', SIZE=D7194
$DF PATH=x3F005F10, TAG=ACCT, TITLE='帐户数据',
SIZE=D2048
$DF PATH=x3F005F20, TAG=MED, TITLE='医疗', SIZE=D1024
$EF PATH=x3F003100, TAG=ICCID, TITLE='发行人 ID',
FORMAT=T, SIZE=D10
$EF PATH=x3F005F205E00, TAG=MED1, TITLE='医疗简要表',
FORMAT=T, SIZE=D80
$EF PATH=x3F005F106F00, TAG=NAME, TITLE='帐户名',
FORMAT=T, SIZE=A30
$EF PATH=x3F005F106F10, TAG=ACCTID, TITLE='帐号',
FORMAT=T, SIZE=N14
$EF PATH=x3F005F106F20, TAG=EXPIRE, TITLE='有效期',
FORMAT=T, SIZE=N4
$EF PATH=x3F005F106F30, TAG=BIRTH, TITLE='出生日期',
FORMAT=T, SIZE=N6
```

卡应用记录 922 将持卡人数据 952“映象”到该应用所使用的数据字段中。如下所示的卡应用记录 922 的例子使其数据项按照被智能卡个人化系统 100 处理的顺序排列。

卡应用记录

```
$VL ICCID VALUE=1234509876
$VL MED1%5, TYPE=A
$VL NAME%1, TYPE=A
$VL ACCTID%2, TYPE=N
$VL EXPIRE%3, TYPE=N
$VL BIRTH%4, TYPE=N
$VL FMTACCT%2(1-4)-%2(5-9)-%2(10-14)
```

ICCID 项包含芯片标识符。其余除 FMTACCT 以外的各项都将一个“标记”映象到持卡人数据记录 952 的字段中，这些字段中包含信息（如上述数据格式模板中所定义的）并规定字段中的数据类型。这样，MED1 标记表示持卡人数据记录 952 的第五个字段并且数据为字母

格式。FMTACCT 项将持卡人数据记录 952 的第二个字段，即帐号，分成几段并在段间插入连字符。

卡操作系统记录 924 中包含对卡上的芯片编程所需的编程控制命令。如下所示的卡操作系统保持控制命令示例取自 ISO 指令号 7816-4 并且不作为任何特定卡操作系统的内部专有命令。

卡操作系统记录

```
SELECT A0A4000002%F
WRITE A0D0%O%L%D
READ A0B0%O%L%D
RESET VALUE=xFF
```

上述记录中的每一项包含一个标记，其后为用卡操作系统的自然语言编写的相应命令。可变的参数字段用“%”和一个字母表示，在处理每个卡时，在字段中填入适当的持卡人数据。

个人化设备记录 926 中包含个人化设备特性数据，如用于定义在一套特定的个人化设备上发行一个完整的卡所需的实际顺序和步骤的指令。此例中所使用的指令示例是假想的，并且不代表用于任何特定个人化设备的内部专用指令。

个人化设备记录

```
$EMBOSS
        #EMB#%FMTACCT%^%NAME%
$ENCODE
        #ENC#%%%ACCTID%^%NAME%
$IC
        #\@#
        @ICCID
        WRITE ICCID
        @NAME
        SELECT ACCT
        SELECT NAME
        WRITE NAME
        @ACCTID
        SELECT ACCTID
        WRITE ACCTID
        @EXPIRE
        SELECT EXPIRE
        WRITE EXPIRE
$PR
```

在每个卡被发行时，按照以“$”开头的项所定义的四步顺序处理上述个人化设备特性数据。卡应用记录 922 用于判断每个指令中的可变参数字段的值。

$EMBOSS 指令是一个以控制序列#EMB#开始的数据流，它通知个人化设备其后的数据应当被浮刻到卡上。指令中的每个数据字段位于一对百分号之间。在这种情况下，第一个数据字段是 FMTACCT，或如卡应用记录 922 中定义的格式化的帐户字段。系统 100 搜索卡应用记录 922 中的 FMTACCT 项并从持卡人记录 952 第一示例的第二个数据字段中生成数据串“1265-36830-91245”。下一个字段，NAME，取自持卡人记录 952 中的第一个数据字段。这样，持卡人记录 952 的第一示例的浮刻指令变成了#EMB%1265-36830-91245%%Smith, James%。

$ENCODE 指令使得系统 100 以同于浮刻指令的方式将持卡人数据编码到卡上的磁条中。依据后面的 IATA（国际空运协会）和 ISO 标准

的附加控制字符被插入到命令中。最终的指令为#ENC#%%%12653683091245%%Smith, James%.

$IC 命令规定了要存入芯片的存储器中的信息。卡操作系统记录 924 用于将个人化设备记录中的指令转换成用于操作系统的编程控制命令。一个控制序列，#\@#用于通知个人化设备后面的数据是芯片数据。要被保存的第一个字段是芯片标识符 ICCID。系统 100 按照以卡操作系统记录 924 中的 WRITE 标记标识的命令翻译个人化设备记录 926 中的 WRITE 标记。由于在应用记录 922 中没有为芯片标识符项指定偏移值，所以隐含值“0000”被加入%0 变量参数字段中。%L 变量参数字段被设置成卡结构模板中$CHIP 项中的 SIZE 字段的值，即“10”或十六进制的“0A”。%D 变量参数字段被设置成 ICCID 的值“1234509876”。最终的命令为 A0D000000A1234509876。

下面的命令使卡操作系统将持卡人姓名存入芯片上帐户目录中的帐户名文件中。系统 100 将 SELECT ACCT 命令转换成相应的卡操作系统命令。系统 100 找到卡操作系统记录 924 中的 SELECT 项和卡结构模板记录中的 ACCT 项，并以用于定义在 ACCT 项中的帐户目录的指定目录路径，即“5F10” 代替 SELECT 项中定义的命令中的%F 变量参数字段。最终的命令为 10A40000025F10。同样地，SELECT NAME 命令使系统 100 用帐户名文件“6F00”代替%F 变量参数字段。最终的命令为 A0A40000026F00。这个序列的最后一个命令是 WRITE 命令。系统 100 通过用隐含偏移值“0000”代替%0，用卡结构模板记录中 NAME 项所定义的 SIZE 字段值“30”或十六进制的“1E”代替%L 以及用持卡人数据记录 952 的第一示例中的持卡人姓名“Smith, James”代替%D 来翻译 WRITE 命令，以产生命令 A0D000001Esmith，James~~~~~~~~~~~~~~~，其中每个“~”代表一个空格以将名字填充到 30 个字符。

系统 100 以相似的方式处理个人化设备记录 926 中的其余命令，以产生一个包含了用于对持卡人数据记录 952 的第一示例发行一个卡的命令的接近的数据串：

#\@#A0D000000A1234509876A0A40000025F10A0A40000026F00A1D000001ESmith, James~~~~~~~~~~~A0A40000026F10A0A4000002E12653683091245A0A40000026F2040998.

$PR 命令使系统 100 向个人化设备发送命令数据流。

图 11、12 和 13 所示的数据格式和结合上述例子讨论的样本数据只是用于说明智能卡个人化系统 100 的各个实施例的不同功能。依使用的环境而定义所需的数据和格式对于所属技术领域的技术人员来说是显而易见的。

正如所属技术领域的技术人员来说亦为显而易见的，智能卡个人化系统 100 包括软件程序的替换实施例，在这些软件程序中利用不同于附图所示的模块执行系统的功能。在不偏离本发明的构思和范围的前提下，系统 100 可以以串行或并行方式或两种方式的组合来处理数据。软件程序可以用几种广泛使用的编程语言中的一种来编写，并且模块可以根据所选择的语言而被编码为子程序、子系统或对象。相似地，系统 100 所使用的数据被描述和表示为具体化在数据库中的逻辑记录，但本发明并不仅限于所描述的数据记录的排列，也不是任何特殊类型的隐含的数据管理系统的应用。来自销售者，如 Oracle、Sybase、Informix 或 Microsoft 的关系数据库提供了用于管理系统中基础数据所需的基本结构，无论它是集中式的还是分布式的，但也可以用其他组织形式的数据结构，即索引的平面文件来代替这些数据库而不超出本发明的范围。

而且，以硬件、固件或软硬件组合实施系统以及以不同方式分配模块和/或数据的本发明的替换实施例对于所属技术领域的技术人员来说是显而易见的并且不超出本发明的保护范围。

应当理解上述描述只是用于说明而非限定性的。参照上述描述，很多其他实施例对于所属技术领域的技术人员来说是显而易见的。因此，应当参照后述的权利要求书来确定本发明的保护范围。

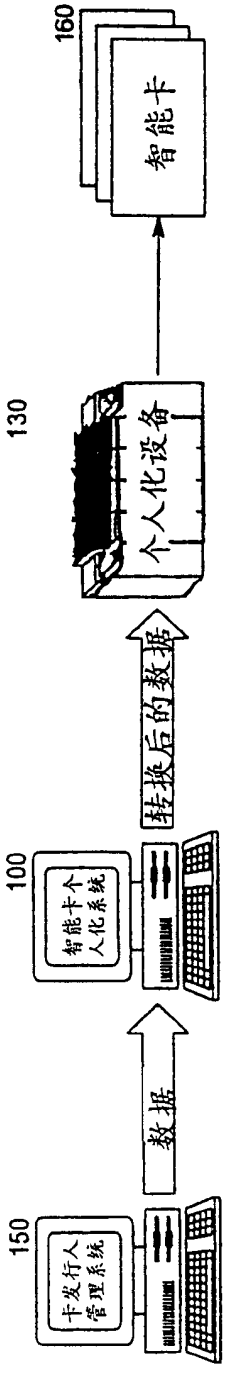


图 1A

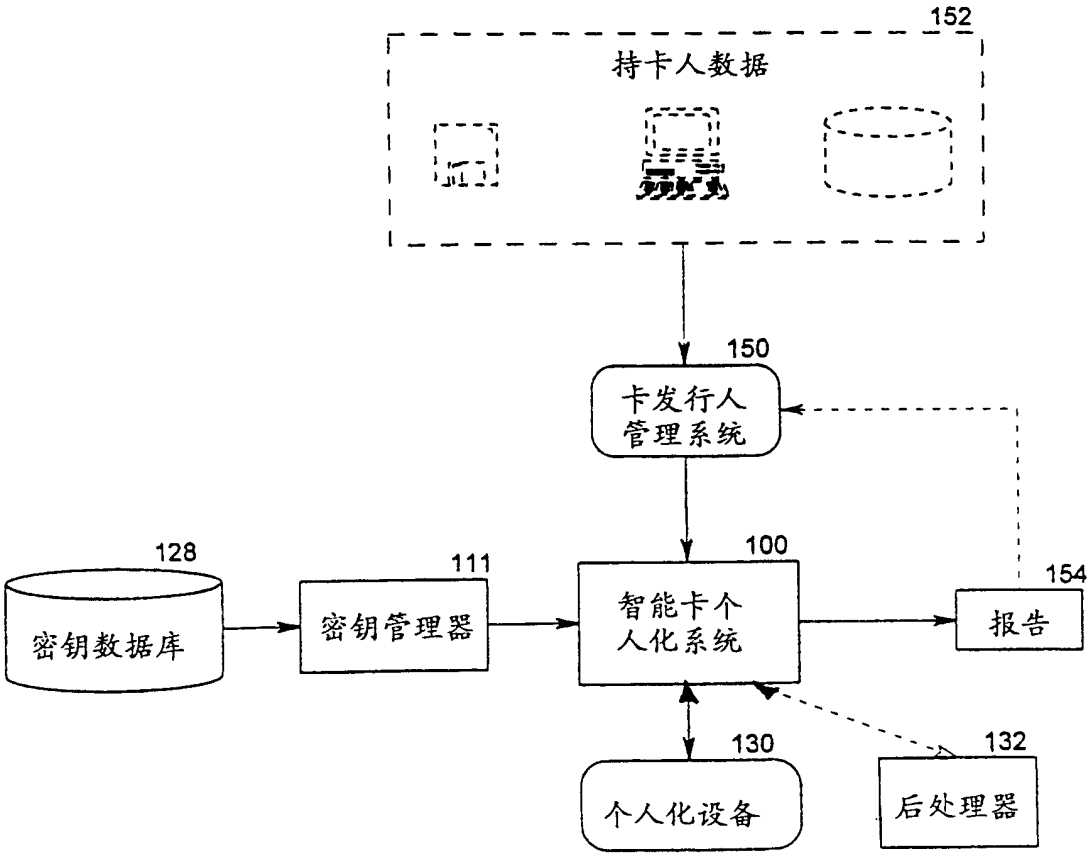

152
持卡人数据
150
卡发行人
管理系统
128
密钥数据库
111
密钥管理器
100
智能卡个
人化系统
154
报告
130
个人化设备
132
后处理器

图 1B

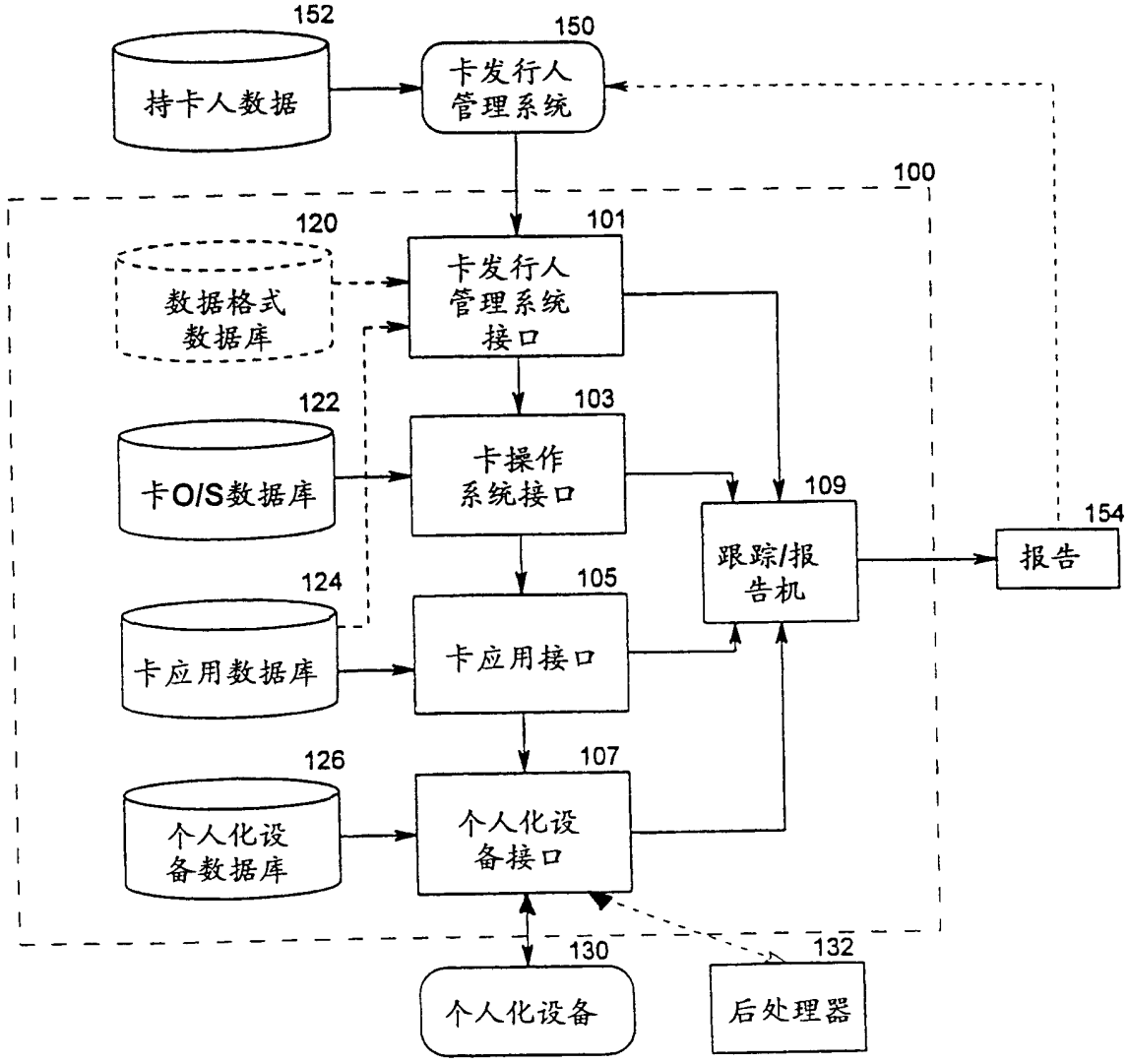

152
持卡人数据
150
卡发行人管理系统
100
120
数据格式数据库
101
卡发行人管理系统接口
122
卡O/S数据库
103
卡操作系统接口
109
跟踪/报告机
154
报告
124
卡应用数据库
105
卡应用接口
126
个人化设备数据库
107
个人化设备接口
130
个人化设备
132
后处理器

图 1C

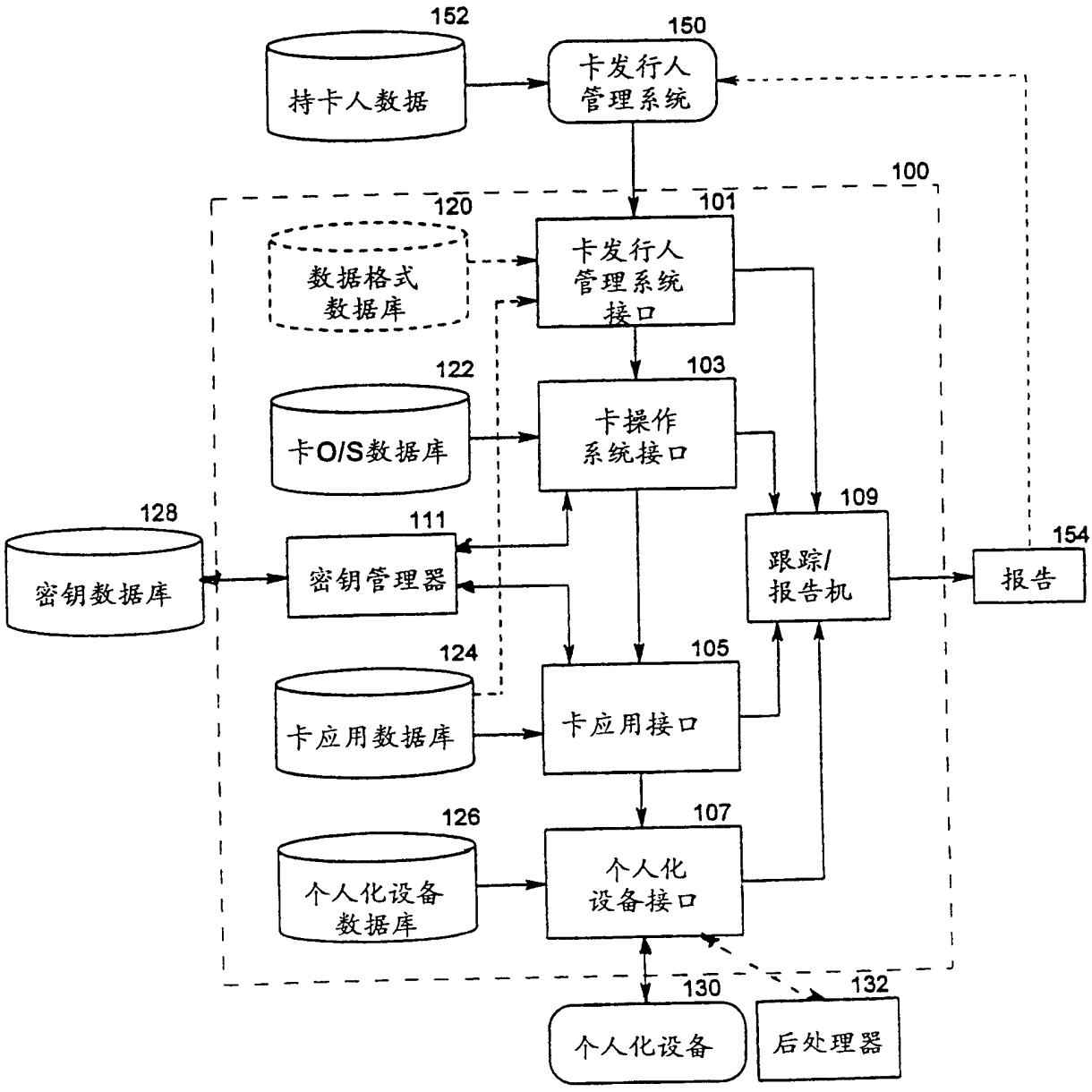

152
持卡人数据
150
卡发行人
管理系统
100
120
数据格式
数据库
101
卡发行人
管理系统
接口
122
卡O/S数据库
103
卡操作
系统接口
128
密钥数据库
111
密钥管理器
109
跟踪/
报告机
154
报告
124
卡应用数据库
105
卡应用接口
126
个人化设备
数据库
107
个人化
设备接口
130
个人化设备
132
后处理器

图 2

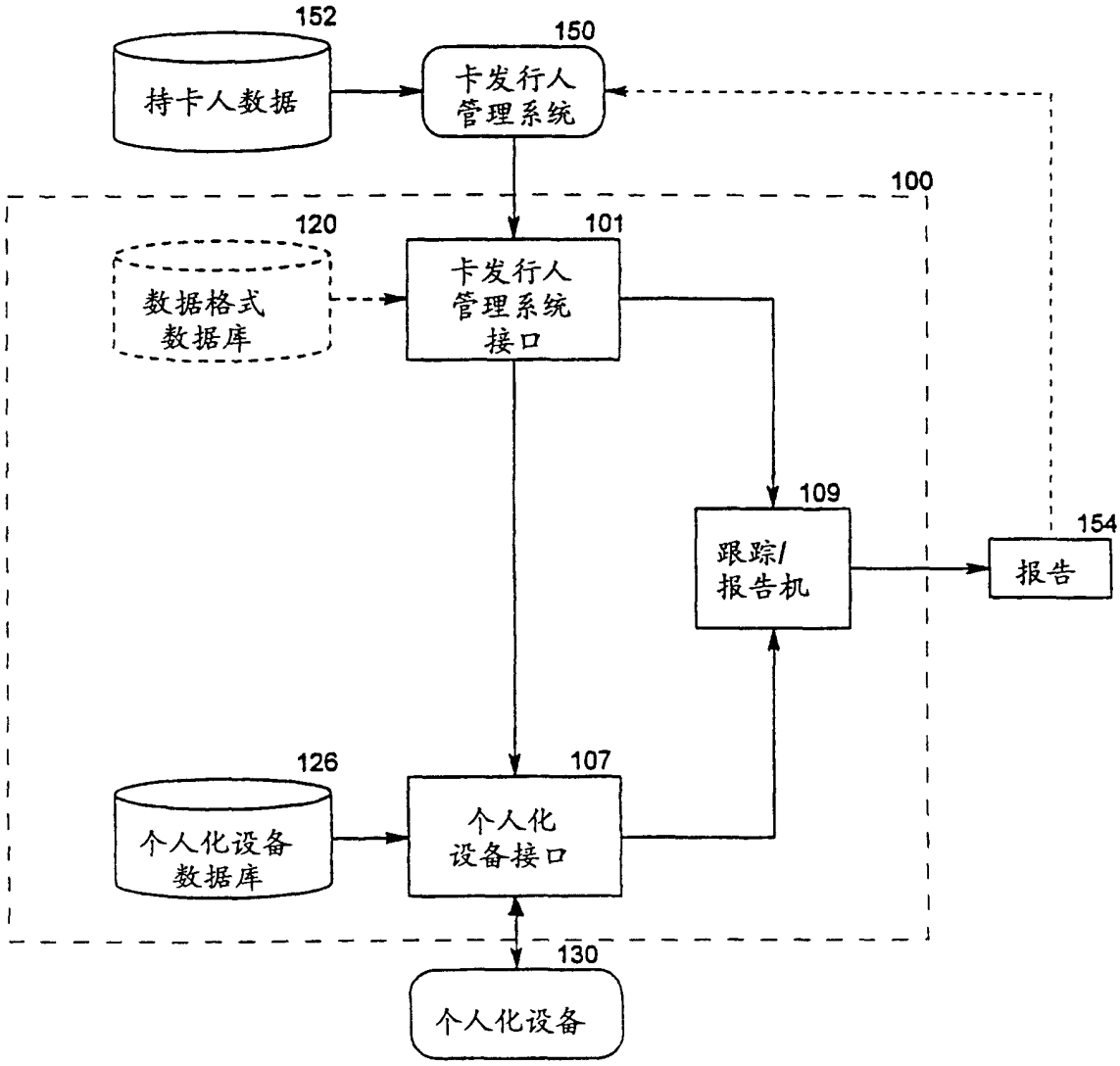

152
持卡人数据
150
卡发行人
管理系统
100
120
数据格式
数据库
101
卡发行人
管理系统
接口
109
跟踪/
报告机
154
报告
126
个人化设备
数据库
107
个人化
设备接口
130
个人化设备

图 3

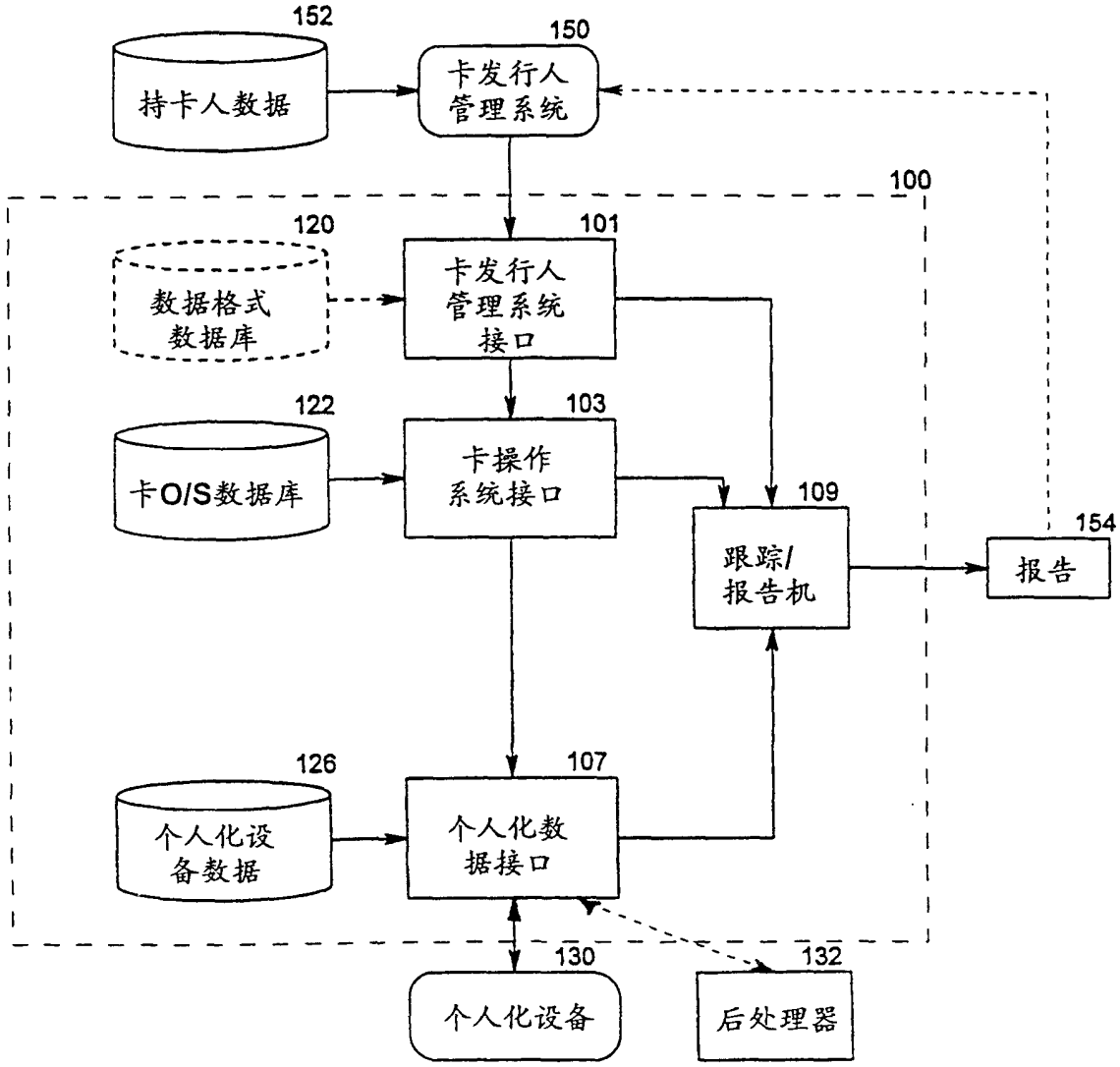

152
持卡人数据
150
卡发行人
管理系统
100
120
数据格式
数据库
101
卡发行人
管理系统
接口
122
卡O/S数据库
103
卡操作
系统接口
109
跟踪/
报告机
154
报告
126
个人化设
备数据
107
个人化数
据接口
130
个人化设备
132
后处理器

图 4

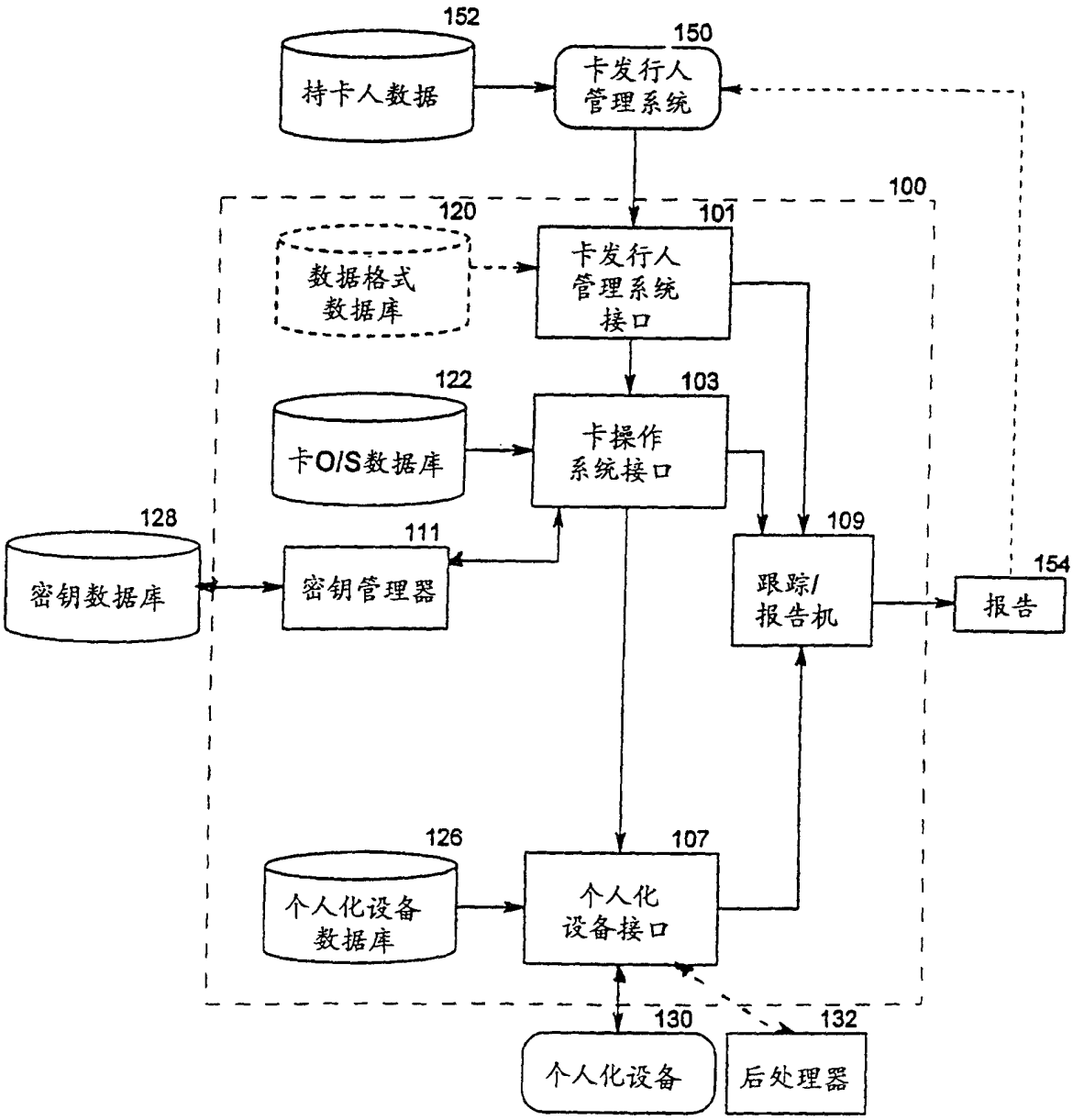

152
持卡人数据
150
卡发行人
管理系统
100
120
数据格式
数据库
101
卡发行人
管理系统
接口
122
卡O/S数据库
103
卡操作
系统接口
128
密钥数据库
111
密钥管理器
109
跟踪/
报告机
154
报告
126
个人化设备
数据库
107
个人化
设备接口
130
个人化设备
132
后处理器

图 5

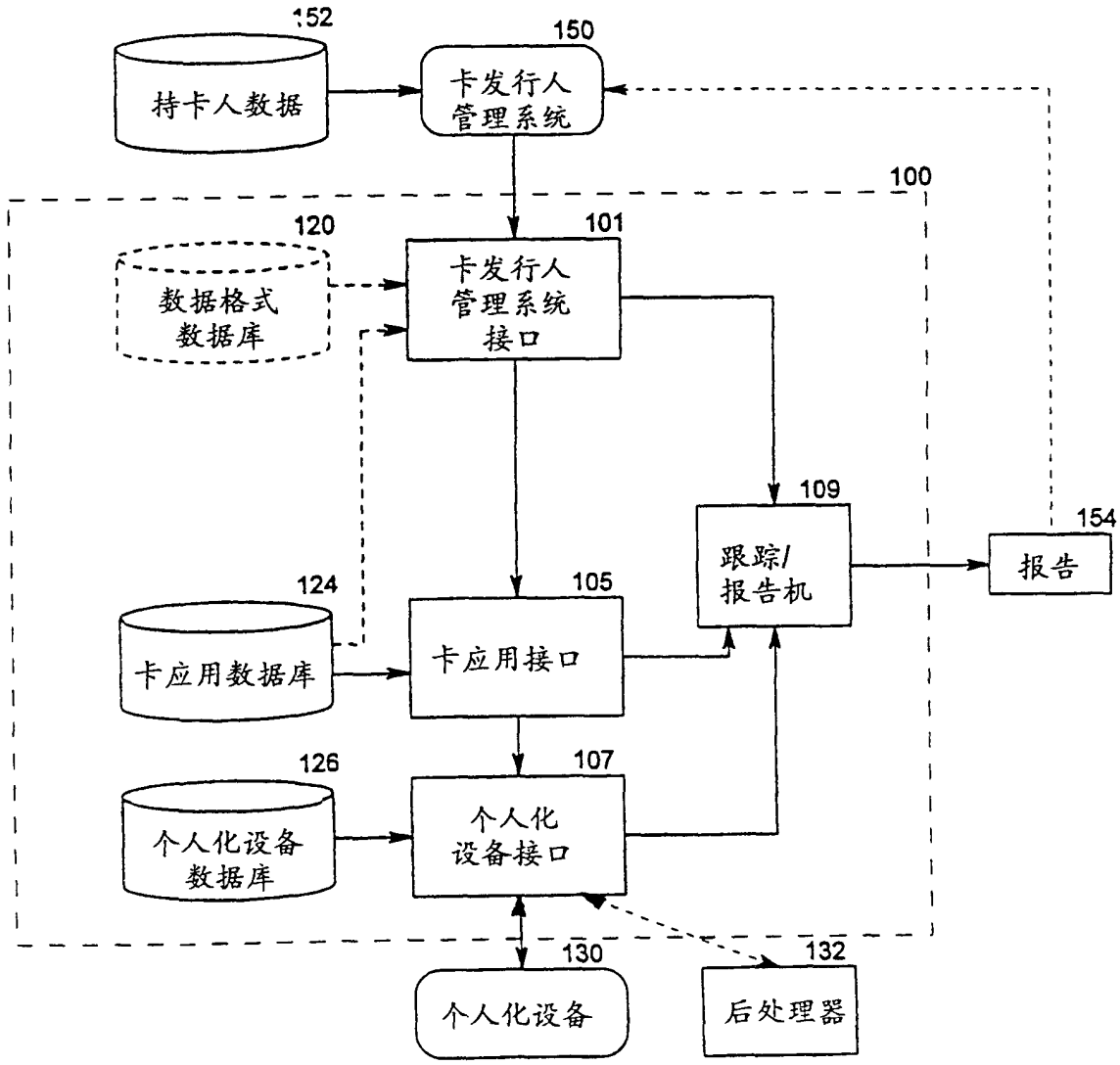

152
持卡人数据
150
卡发行人
管理系统
100
120
数据格式
数据库
101
卡发行人
管理系统
接口
109
154
跟踪/
报告机
报告
124
卡应用数据库
105
卡应用接口
126
个人化设备
数据库
107
个人化
设备接口
130
个人化设备
132
后处理器

图 6

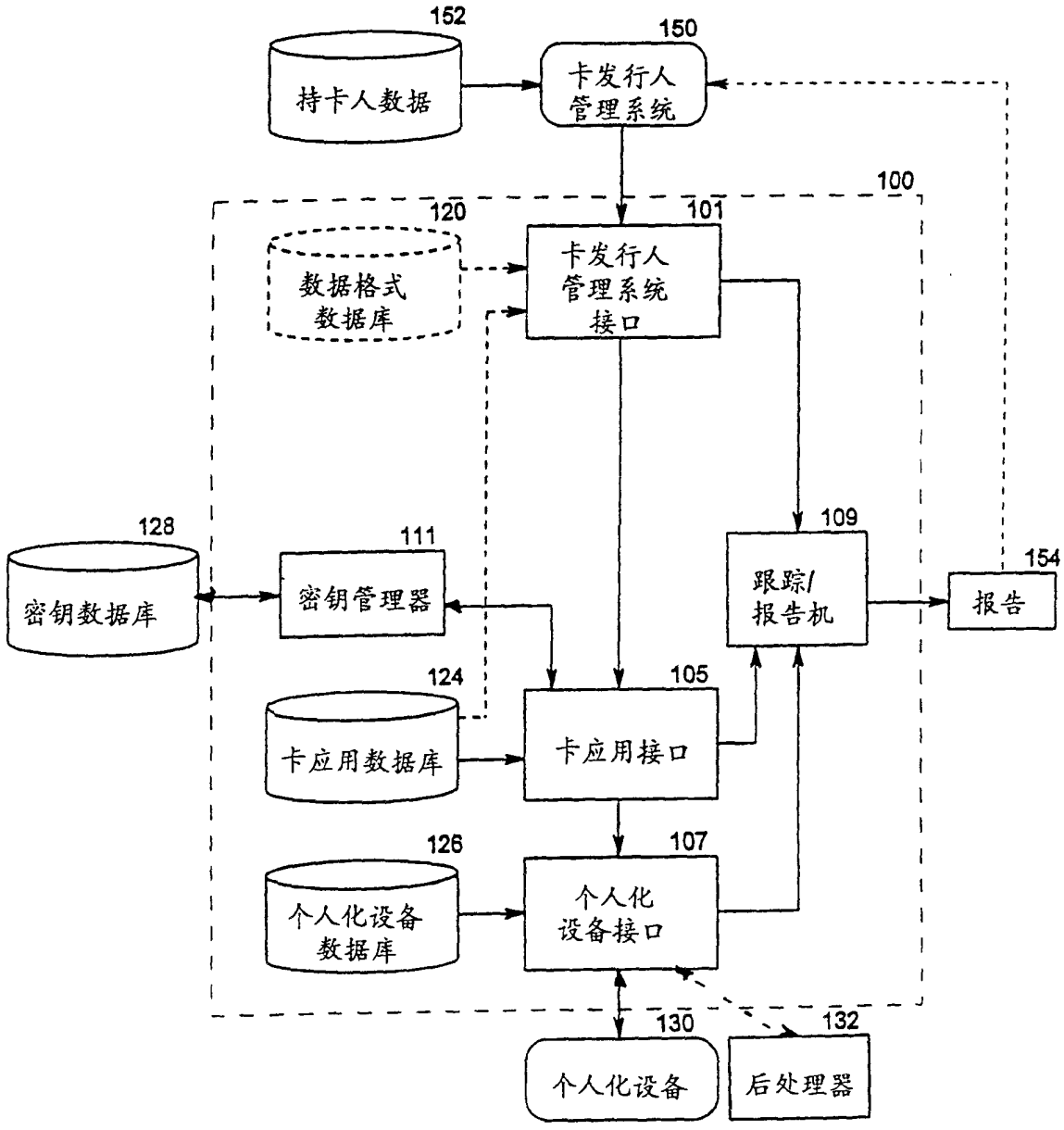

152
持卡人数据
150
卡发行人
管理系统
100
120
数据格式
数据库
101
卡发行人
管理系统
接口
128
密钥数据库
111
密钥管理器
109
跟踪/
报告机
154
报告
124
卡应用数据库
105
卡应用接口
126
个人化设备
数据库
107
个人化
设备接口
130
个人化设备
132
后处理器

图 7

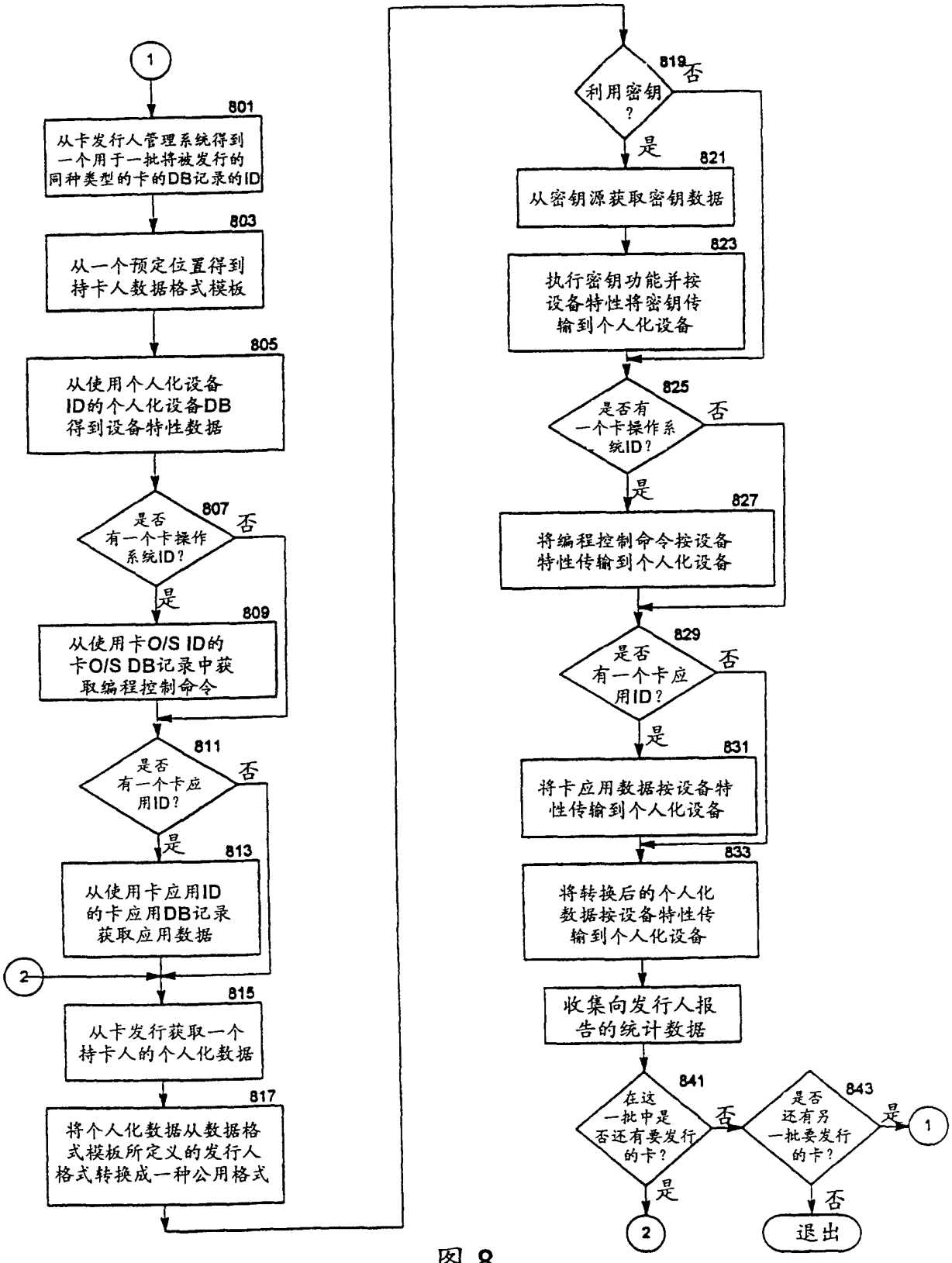

1
801
从卡发行人管理系统得到一个用于一批将被发行的同种类型的卡的DB记录的ID
803
从一个预定位置得到持卡人数据格式模板
805
从使用个人化设备ID的个人化设备DB得到设备特性数据
807
是否有一个卡操作系统ID?
否
是
809
从使用卡O/S ID的卡O/S DB记录中获取编程控制命令
811
是否有一个卡应用ID?
否
是
813
从使用卡应用ID的卡应用DB记录获取应用数据
2
815
从卡发行获取一个持卡人的个人化数据
817
将个人化数据从数据格式模板所定义的发行人格式转换成一种公用格式
819
利用密钥?
否
是
821
从密钥源获取密钥数据
823
执行密钥功能并按设备特性将密钥传输到个人化设备
825
是否有一个卡操作系统ID?
否
是
827
将编程控制命令按设备特性传输到个人化设备
829
是否有一个卡应用ID?
否
是
831
将卡应用数据按设备特性传输到个人化设备
833
将转换后的个人化数据按设备特性传输到个人化设备
收集向发行人报告的统计数据
841
在这一批中是否还有要发行的卡?
否
是
2
843
是否还有另一批要发行的卡?
是
1
否
退出

图 8

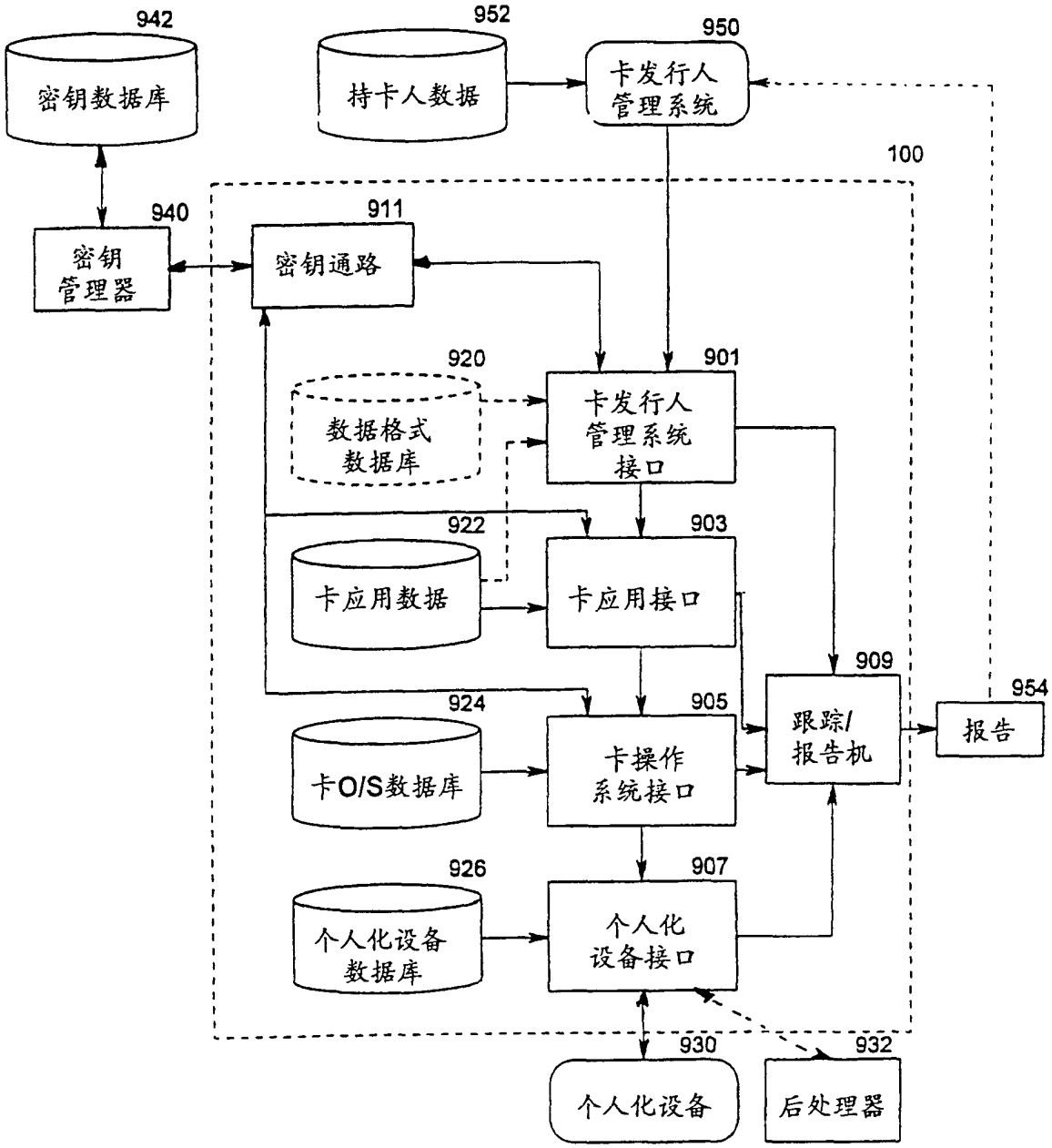

942
密钥数据库
952
持卡人数据
950
卡发行人管理系统
100
940
密钥管理器
911
密钥通路
920
数据格式数据库
901
卡发行人管理系统接口
922
卡应用数据
903
卡应用接口
909
954
924
卡O/S数据库
905
卡操作系统接口
跟踪/报告机
报告
926
个人化设备数据库
907
个人化设备接口
930
个人化设备
932
后处理器

图 9

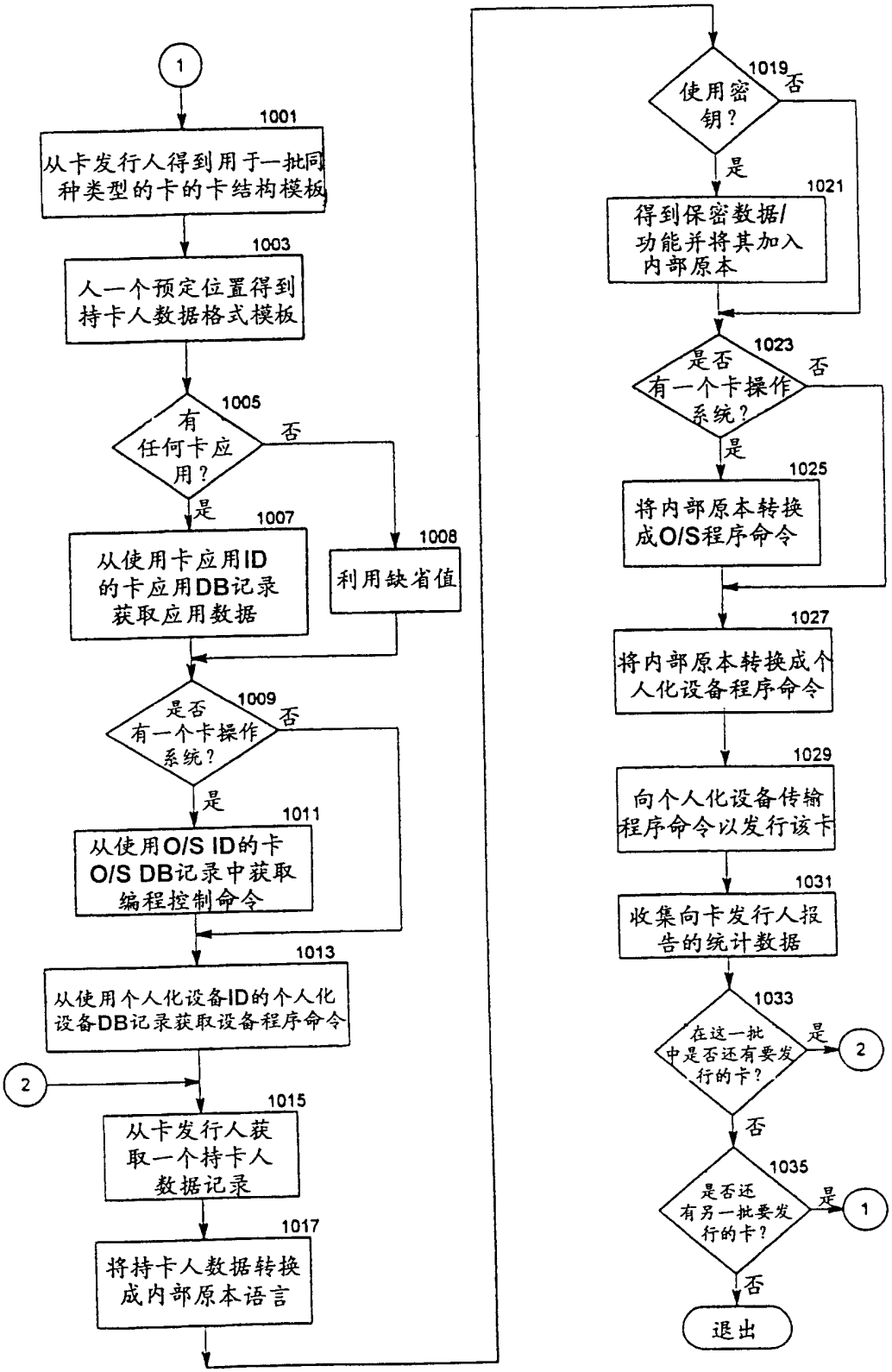

1
1001
从卡发行人得到用于一批同种类型的卡的卡结构模板
1003
人一个预定位置得到持卡人数据格式模板
1005
有任何卡应用？
否
是
1007
从使用卡应用ID的卡应用DB记录获取应用数据
1008
利用缺省值
1009
是否有一个卡操作系统？
否
是
1011
从使用O/S ID的卡O/S DB记录中获取编程控制命令
1013
从使用个人化设备ID的个人化设备DB记录获取设备程序命令
2
1015
从卡发行人获取一个持卡人数据记录
1017
将持卡人数据转换成内部原本语言
1019
使用密钥？
否
是
1021
得到保密数据/功能并将其加入内部原本
1023
是否有一个卡操作系统？
否
是
1025
将内部原本转换成O/S程序命令
1027
将内部原本转换成个人化设备程序命令
1029
向个人化设备传输程序命令以发行该卡
1031
收集向卡发行人报告的统计数据
1033
在这一批中是否还有要发行的卡？
是
2
否
1035
是否还有另一批要发行的卡？
是
1
否
退出

图 10

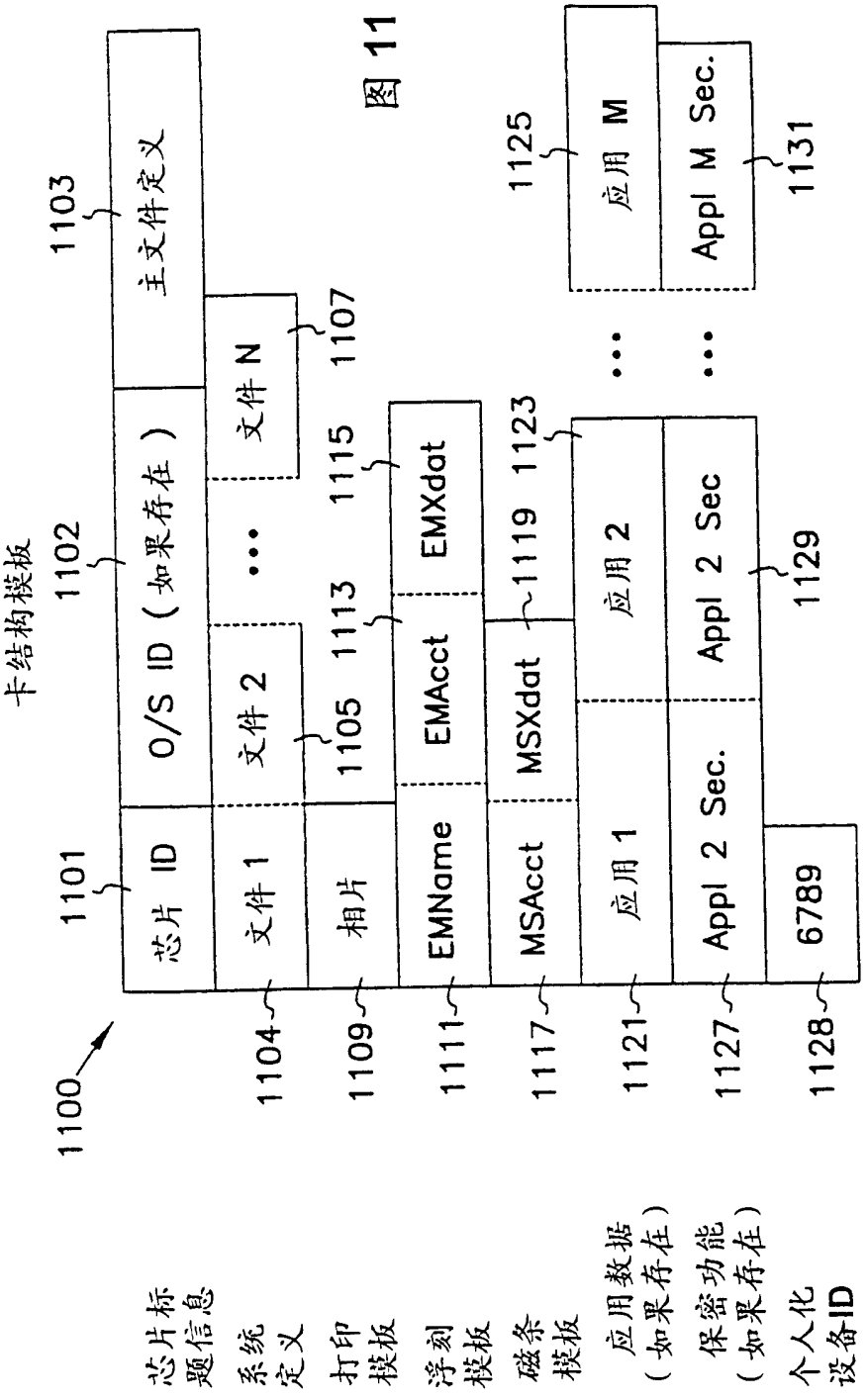

卡结构模板
1100
1101
1102
1103
芯片 ID
O/S ID (如果存在)
主文件定义
文件 1
文件 2
...
文件 N
1104
1105
1107
相片
1109
1111
EMName
EMAcct
EMXdat
1113
1115
MSAcct
MSXdat
1117
1119
1123
1125
应用 1
应用 2
...
应用 M
1121
Appl 2 Sec.
Appl 2 Sec
...
Appl M Sec.
1127
1129
1131
6789
1128
芯片标题信息
系统定义
打印模板
浮刻模板
磁条模板
应用数据(如果存在)
保密功能(如果存在)
个人化设备ID

图 11

数据格式模板
1200
1201
1203
1205
Acct. No.
姓名
Exp. Date
持卡人数据

图 12

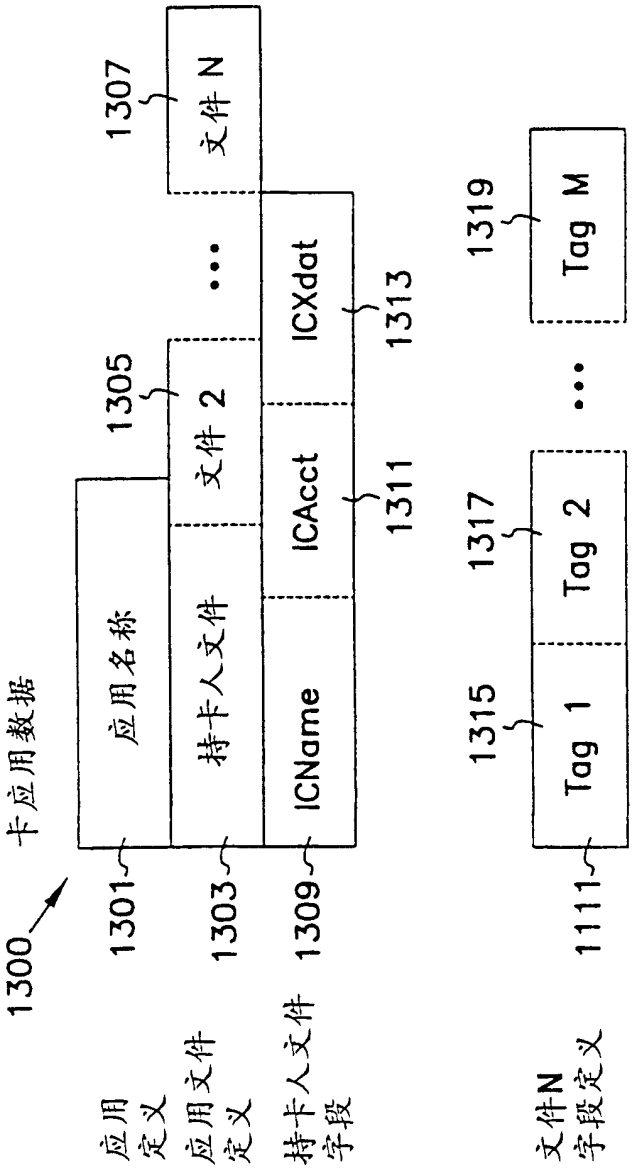

1300
卡应用数据
1301
应用名称
1303
持卡人文件
1309
ICName
ICAcct
1311
1305
文件 2
ICXdat
1313
1307
文件 N
1315
Tag 1
1317
Tag 2
1111
1319
Tag M
应用定义
应用文件定义
持卡人文件字段
文件N字段定义

图 13

样本报告项

卡材料
- 零件号
- 帐户姓名
- 零件说明
  - 塑料
  - 微控制器
  - 磁条
- 现有量
- 订单级别
- 计划下次打算订单日期/数量
- 资源再储存数据
  - 接收的批号
  - 自动售货机
  - 接收日期
  - 数量
  - 质量/等外品
- 资源使用数据
  - 作业号
  - 日期
  - 数量检查
  - 数量登记

原材料状态
- 成形材料
  - 零件号
    - 帐户姓名
    - 零件说明
    - 现有量
    - 订单级别
    - 计划下次打算订单日期/数量
    - 资源再储存数据
      - 接收的批号
      - 自动售货机
      - 接收日期
      - 数量
      - 质量/等外品
    - 资源使用数据
      - 作业号
      - 日期
      - 数量检查
      - 数量登记

软件配置
- 客户库
  - 接口库部件
- 应用库
  - 键卡
  - 应用数据库部件
- 卡O/S库
  - 成批卡
  - 卡O/S库部件
- 个人化设备库
  - 受支持的个人化设备

生产状态
- 成批机器
  - 批生产开始数据
    - 管理
      - 父母职业
      - 操作员
      - 日期/时间
      - 客户
    - 卡类型
      - 应用
        - 数据
          - 安全性要求
            - 静态
            - 动态
      - 操作系统
        - 动态安全性要求
      - 塑料卡类型（零件号）
      - 卡号码
    - 个人化设备
      - 片个人化设备
      - 卡个人化设备
  - 生产
    - 个人化卡
    - 卡误差
      - 误差类型
    - 卡总数

图 14