[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06K 17/00 (2006.01)
B41J 2/175 (2006.01)

[12] 发明专利说明书

专利号 ZL 03809815.6

[45] 授权公告日 2007 年 12 月 12 日

[11] 授权公告号 CN 100354884C

[22] 申请日 2003.2.28 [21] 申请号 03809815.6

[30] 优先权

[32] 2002. 3. 1 [33] US [31] 60/361,253

[32] 2002. 4.19 [33] US [31] 60/373,967

[86] 国际申请 PCT/US2003/006187 2003.2.28

[87] 国际公布 WO2003/075218 英 2003.9.12

[85] 进入国家阶段日期 2004.11.1

[73] 专利权人 法格电子公司

地址 美国明尼苏达州

[72] 发明人 加里·M·克兰费尔特

托马斯·C·普拉特纳

约瑟夫·F·舒勒

利奥尼德·S·格申维奇

大卫·W·凯泽 加里·R·霍兰

[56] 参考文献

WO0043932A2 2000.7.27

US20010036275A1 2001.11.1

CN1192015A 1998.9.2

审查员 王咪娜

[74] 专利代理机构 中科专利商标代理有限责任公司

代理人 罗松梅

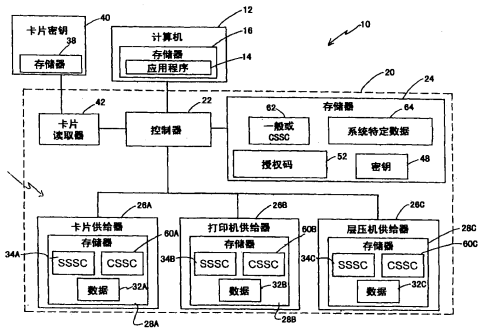
权利要求书 5 页 说明书 9 页 附图 5 页

[54] 发明名称

身份证制造安全

[57] 摘要

身份证制造安全限制只与授权的供给器一起使用身份证制造系统(10)。只有当发现已解译的供给器特定安全码(SSSC)和/或用户特定安全码(CSSC)有效时，才授权和身份证制造系统一起使用供给器。



1．一种授权供给器与身份证制造系统一起使用的方法，包括步骤：

a）从供给器的存储器中检索供给器特定安全码 SSSC 和供给器特定数据；

b）使用供给器特定数据来解译 SSSC；以及

c）当已解译的 SSSC 有效时，授权和身份证制造系统一起使用供给器；

d）当已解译的 SSSC 不是有效时，防止与身份证制造系统一起使用该供给器。

2．根据权利要求 1 所述的方法，其特征在于所述授权步骤 c）包括将已解译的 SSSC 和供给器授权码进行比较，其中当其与供给器授权码相对应时，则所述已解译的 SSSC 是有效的。

3．根据权利要求 1 所述的方法，其特征在于所述解译步骤 b）包括使用供给器特定数据解码或解密供给器 SSSC。

4．根据权利要求 1 所述的方法，其特征在于包括：

e）检索供给器用户特定安全码 CSSC；

f）检索系统 CSSC 和系统特定数据；

g）使用供给器特定数据解译供给器 CSSC；

h）系统特定数据解译系统 CSSC；以及

i）解译的系统 CSSC 和已解译的供给器 CSSC 相对应时，授权和身份证制造系统一起使用该供给器；

j）解译的供给器 CSSC 与已解译的系统 CSSC 不对应时，防止与身份证制造系统一起使用该供给器。

5．根据权利要求 4 所述的方法，其特征在于所述系统 CSSC 是应用程序 CSSC，且系统特定数据是应用程序特定数据。

6．根据权利要求 4 所述的方法，其特征在于所述系统 CSSC 是身份证制造设备 CSSC，且系统特定数据是身份证制造设备特定数据。

7．根据权利要求 1 所述的方法，其特征在于所述供给器是卡片供给器，和墨盒、热打印色带或覆盖薄片供给器。

8．一种授权供给器和身份证制造系统一起使用的方法，包括步骤：

a）从供给器的存储器中检索供给器用户特定安全码 CSSC 和供给器特定数据；

b）从身份证制造系统的存储器中检索系统 CSSC 和系统特定数据；

c）使用供给器特定数据来解译供给器 CSSC；

d）使用系统特定数据来解译系统 CSSC；以及

e）当已解译的系统 CSSC 和已解译的供给器 CSSC 相对应时，授权和身份证制造系统一起使用供给器；

f）当已解译的供给器 CSSC 与已解译的系统 CSSC 不对应时，防止与身份证制造系统一起使用该供给器。

9．根据权利要求 8 所述的方法，其特征在于所述系统 CSSC 是应用程序 CSSC，且系统特定数据是应用程序特定数据。

10．根据权利要求 8 所述的方法，其特征在于所述系统 CSSC 是身份证制造设备 CSSC，且系统特定数据是身份证制造设备特定数据。

11．根据权利要求 8 所述的方法，其特征在于解译步骤 c）包括：使用存储在身份证制造系统的存储器中的私钥来解密或解码供给器 CSSC。

12．根据权利要求 8 所述的方法，其特征在于解译步骤 d）包括：使用存储在身份证制造系统的存储器中的私钥来解密或解码系统 CSSC。

13．根据权利要求 8 所述的方法，其特征在于授权步骤 e）包括：比较已解译的供给器 CSSC 和已解译的系统 CSSC，其中当已解译的 CSSC 和已解译的系统 CSSC 相匹配时，授权与系统一起使用该供给器。

14．根据权利要求 8 所述的方法，其特征在于包括：

g）供给器特定安全码 SSSC；

h）供给器特定数据来解译 SSSC；以及

i）解译的 SSSC 有效时，授权和身份证制造系统一起使用供给器。

15．根据权利要求 14 所述的方法，其特征在于所述授权步骤 i）将已解译的 SSSC 和存储在身份证制造系统的存储器中的供给器授权码进行比较，其中只有当已解译的 SSSC 与供给器授权码相对应时，所述供给器才是有效的。

16．根据权利要求 8 所述的方法，其特征在于所述供给器是卡片供给器，和墨盒、热打印色带或覆盖薄片供给器。

17．一种身份证制造系统，包括：

身份证制造设备；

配置与身份证制造设备一起使用的供给器，所述供给器包括包含有供给器特定安全码 SSSC 和供给器特定数据的存储器；

应用程序，包括微型处理器可执行的指令，所述指令包括：

a）从供给器的存储器中检索 SSSC 和供给器特定数据；

b）使用供给器特定数据来解译 SSSC；以及

c）当已解译的 SSSC 有效时，授权和身份证制造设备一起使用供给器；以及

d）当已解译的 SSSC 不是有效时，防止与身份证制造系统一起使用该供给器。

18．根据权利要求 17 所述的系统，其特征在于所述供给器是卡片供给器，和墨盒、热打印色带或覆盖薄片供给器。

19．一种身份证制造系统，包括：

身份证制造设备；

配置与身份证制造设备一起使用的供给器，所述供给器包括包含有供给器用户特定安全码 CSSC 和供给器特定数据的存储器；以及

应用程序，包括微型处理器可执行的指令，所述指令包括：

a）从供给器的存储器中检索供给器 CSSC 和供给器特定数据；

b）检索系统 CSSC 和系统特定数据；

c）使用供给器特定数据来解译供给器 CSSC；

d）使用系统特定数据来解译系统 CSSC；以及

e）当已解译的系统 CSSC 和已解译的供给器 CSSC 相对应时，授权和身份证制造设备一起使用供给器；

f）当已解译的系统 CSSC 与已解译的供给器 CSSC 不对应时，防止与身份证制造设备一起使用该供给器。

20．根据权利要求 19 所述的系统，其特征在于所述供给器是卡片供给器，和墨盒、热打印色带或覆盖薄片供给器。

21．一种设置授权与身份证制造系统一起使用的供给器的方法，包括步骤：

a）产生针对用户的用户特定安全码 CSSC；

b）在安全数据库中存储 CSSC；

c）在供给器的存储器中存储 CSSC；

以及

d）配置身份证制造系统，以使其只能和具有 CSSC 的供给器一起操作。

22．根据权利要求 21 所述的方法，其特征在于所述存储步骤 c）包括利用 CSSC 替代已存储的一般码。

23．根据权利要求 21 所述的方法，其特征在于由身份证制造系统的经销商进行所述存储步骤 c）。

24．根据权利要求 21 所述的方法，其特征在于所述配置步骤 d）包括利用 CSSC 替代已存储在身份证制造系统的存储器中的一般码。

25．根据权利要求 21 所述的方法，其特征在于所述配置步骤 d）包括当第一次与供给器一起操作该系统时，利用 CSSC 更新与身份证制造系统相对应的一般码。

26．根据权利要求 21 所述的方法，其特征在于编码或加密所述 CSSC。

27．根据权利要求 24 所述的方法，其特征在于所述身份证制造系统包括具有存储器的身份证打印机。

28．根据权利要求 21 所述的方法，其特征在于所述身份证制造

系统包括卡片产生应用程序，能够访问身份证制造系统的存储器；以及

配置步骤 d）包括当第一次与供给器一起操作该系统时，通过应用程序利用 CSSC 更新与身份证制造系统相对应的一般码。

身份证制造安全

技术领域

一般地，本发明涉及身份证制造，更具体地，涉及身份证制造系统的安全，以便防止未授权的使用身份证制造设备和相应的供给器。

背景技术

通常，身份证制造系统包括计算机、在计算机上运行的至少一个卡片制造应用程序和例如身份证打印机或层合机的至少一个身份证制造设备。在身份证打印机的情况下，卡片制造应用程序能够将纹理和图形信息相结合，以形成与身份证打印机要打印的图像相对应的打印任务。然后，身份证打印机通过使用热打印机构或喷墨打印机构将图像打印到从卡片供给器提供的卡片衬底上，从而处理了打印任务。热打印机构使用了热打印色带供给器，而喷墨打印机构使用了墨盒供给器。当身份证制造设备是层合机时，卡片生产应用程序能够控制身份证层合机的操作，使用覆盖薄片（overlaminate）供给器来层合所印制卡片。身份证制造应用程序还能够控制其它身份证处理设备，例如数据编码器和卡片抛掷器。

对于仿冒身份证的安全具有很高的需求。已经使用了设置这种安全的方法来生产难以复制或修改的身份证。例如，可以利用包括例如全息摄影的定制安全标记的层压供给器来层合所印制的身份证。此外，身份证可以包括能够呈现篡改卡片企图的材料的特殊层。但是，这些定制供给器中的投资提供了对于仿冒的安全的错觉。

例如，能够进入定制供给器的仿冒者可以克服增强对于仿冒和篡改的安全的方法。然后，仿冒者能够得到身份证制造系统并使用定制的供给器，从而可能产生不可检测的仿冒的身份证。

持续的需求的在于改进身份证制造安全，更具体地，在于改进对

于身份证仿冒的安全。

发明内容

通过限制身份证制造系统以使只能和授权的供给器一起进行操作，本发明改进了身份证制造的安全。根据本发明的此方面，将供给器特定安全码（SSSC）和供给器特定数据存储在身份证制造系统供给器的存储器中。使用供给器特定数据来解译 SSSC。最后，只有当发现已解译的 SSSC 有效时，才授权和身份证制造系统一起使用供给器。按照这种方式，能够防止和被确定为无效的供给器一起来操作身份证制造系统。

根据本发明的另一方面，配置身份证制造系统，以便只能和具有对应于用户特定安全码（CSSC）的供给器一起进行操作。根据本发明的此方面，从供给器的存储器中检索供给器 CSSC 和供给特定数据。此外，从身份证制造系统的存储器中检索系统 CSSC 和系统特定 CSSC。使用供给器特定数据和系统特定数据分别来解译供给器 CSSC 和系统 CSSC。最后，当已解译的系统 CSSC 和已解译的供给器 CSSC 相对应时，授权和身份证制造系统一起使用该供给器。

本发明的另一方面针对配置身份证制造系统的方法，以便只能和具有对应 CSSC 的供给器一起进行操作。这里，针对用户产生 CSSC。接下来，将 CSSC 存储在供给器的安全数据库和存储器中。最后，配置身份证制造系统，以便只能和具有 CSSC 的供给器一起进行操作。

附图说明

图 1 是根据本发明实施例的身份证制造系统的简化图。

图 2 是示出了根据本发明实施例执行的安全检查的流程图。

图 3 是示出了根据本发明实施例的安全检查的流程图。

图 4 是示出了其中形成了定制供给器及其对应的身份证制造系统的方法的简化方框图。

图 5 是示出了能够由身份证制造系统实现的方法的流程图，所述方法用于执行图 2 和 3 中的流程图所示的安全检查。

具体实施方式

图 1 是示出了根据本发明实施例的身份证制造系统 10 的示意图。系统 10 通常包括具有存储在存储器 16 中的卡片制造应用程序与驱动软件 14 的计算机。系统 10 还包括由应用程序 14 控制的身份证制造设备 20，从而以某种方式来处理身份证。图 1 中系统 10 的一种选择是配置身份证制造设备 20，使其包括能够执行应用程序 14 的微型计算机，以便消除对分离计算机 12 的需要。

身份证制造设备 20 包括控制器 22、存储器 24 和通常被指明为 26 的一个或多个供给器。控制器 22 接收来自应用程序与驱动软件 14 的指令，从而据此处理身份证。设备 20 可以是身份证打印机、身份证层合机或其它卡片制造设备。为了简化本发明的图示和讨论，未示出设备 20 的打印、层合和其它卡片处理组件。

供给器 26 包括卡片供给器 26A、打印机供给器 26B、层合机供给器 26C 或其它卡片制造供给器。卡片供给器 26A 可以包括卡片盒或卡片夹持器，所述卡片夹持器包括单独身份证的供给器，用于将卡片提供给设备 20 的卡片处理组件。打印机供给器 26B 可以是用于热打印头的热打印色带，或用于喷墨打印头的墨盒。层合机供给器 26C 可以是覆盖薄片材料的供给器，用于应用到卡片表面的层合机一起使用。

每个供给器 26 包括存储器 28，控制器 22 通过供给器读取器 30 可以访问所述存储器。供给器读取器 30 可以通过直接电连接或使用射频（RF）通信方法的无线连接与每个供给器 26 的存储器 28 进行通信，并将包含在其中的数据提供给控制器 22。控制器 22 能够分析数据和/或与应用程序 14 互通数据。

包含在供给器 26 的存储器 28 中的数据可以包括有关供给器的普通信息。例如，存储器 28 可以包括有关供给器 26 是卡片供给器 26A、打印机供给器 26B、层合机供给器 26C 还是其它类型的供给器的信息。此外，普通供给器信息还包括例如包含在新卡片供给器 26A 中的卡片的数目、存储在打印机供给器 26B 中的墨水类型或墨水量和

存储在层合机供给器 26C 中的层合材料类型或层合材料量。此外，数据可以包括与特定供给器相关的供给器特定数据 32。例如，该供给器特定数据 22 可以包括唯一的序列号、唯一的日期信息（例如期满日期、生产日期、装运日期等）和实质上对于具体供给器是唯一的其它数据。

根据本发明的实施例，存储器 28 包括使用例如序列号等供给器特定数据 32 进行编码的、或利用供给器特定数据 32 和没有存储在供给器存储器 28 中的私钥进行加密的供给器特定安全码（SSSC）34。结果，SSSC 对于每个供给器 26 是唯一的。即，卡片供给器 26A 的 SSSC 34A 不同于打印机供给器 26B 的 SSSC 34B 和层合机供给器 26C 的 SSSC 34C，也不同于其它的卡片供给器。例如，能够将用于加密 SSSC 34 的私钥存储在卡片制造设备 20 的存储器 24 中、计算机 12 的存储器 16 中或包含在由卡片读取器 42 可读的卡片密钥 40 的存储器 38 中。

根据本发明的一个实施例，根据图 2 所示的流程图来进行第一级安全检查。在步骤 44，从卡片供给器 26 的存储器 28 中检索 SSSC 34 和供给器特定数据 32。这通常在控制器 22 的控制下，使用供给器特定数据 32 来完成。接下来，在步骤 46，使用供给器特定数据 32 来解译 SSSC 34。通过控制器 22 或计算机 12，根据来自应用程序 14 的指令来实现此操作。SSSC 34 的该解译通常包括根据预定的算法，使用供给器特定数据 32 来译解或解密 SSSC 34。可选地，能够使用供给器特定数据 32 和存储在系统存储器 24 或如上所述其它位置的对应私钥 48 来解密 SSSC 34。

在步骤 50，当确定已解译的 SSSC 34 有效时，授权使用供给器 26 和身份证制造系统 10。根据一个实施例，该授权步骤包括将已解译的供给器 26 的 SSSC 34 与存储器系统存储器 24 中的授权码 52 进行比较。当其匹配或对应于授权码 52 时，则确定该已解译的 SSSC 34 是有效的。如果发现有效，能够与供给 26 一起操作身份证制造系统 10。如果发现供给器 26 是无效的，例如，系统 10 能够使用控制器 22 来触发互锁机构，以防止与无效的供给器 26 一起操作系统 10。

根据本发明的另一方面，能够配置身份证制造系统 10，以使其只能和为特定用户定制的供给器 26 一起进行操作。根据一个实施例，供给器 26 和身份证制造系统 10 都包括用户特定安全码（CSSC）。使用供给器特定数据 32 对存储在供给器存储器 28 中的供给器 CSSC 60 进行加密，或使用供给器特定数据 32 和最好与用于加密 SSSC 34 的存储器 24 的私钥（密钥 48）不同的私钥对其进行加密。

类似地，将系统 CSSC 62 存储在系统存储器 24 中。能够作为存储系统 CSSC 和下述其它信息的系统存储器来操作存储器 16。优选地，使用系统特定数据 64 对系统 CSSC 62 进行编码，或使用系统特定数据 64 和最好不同于用于加密供给器 26 的供给器 CSSC 60 的私钥的私钥对其进行加密。系统 CSSC 62 可以采用以下形式：最好如存储器 24 中所示存储的对应于设备 20 的设备 CSSC，或最好存储在计算机 12 的存储器 16 中的对应于应用程序 14 的应用程序 CSSC 62。系统 10 可以使用应用程序和设备 CSSC 62。系统特定数据 64 是序列号或唯一地识别系统 10 的设备 20（设备特定数据）或应用程序 14（应用程序特定数据）的其它信息。优选地，将用于加密供给器和系统 CSSC 的私钥存储在供给器存储器 28 或系统存储器 24 的外部。根据一个实施例，将用于加密供给器和系统 CSSC 的私钥存储在卡片密钥 38 的存储器 37 中。

图 3 是系统 10 和具有供给器 CSSC 60 的供给器 26 的操作的流程图。在步骤 70，从供给器 26 的存储器 28 中检索供给器 CSSC 60 和供给器特定数据 32。如上所述，控制器 22 通过读取器 30 能够实现存储器 28 的该读取。控制器 22 或计算机 12 能够根据来自应用程序 14 的指令来分析供给器 CSSC 60 和供给器特定数据 32。接下来，在 72，从身份证制造系统 10 的存储器 24 中检索系统 CSSC 62 和系统特定数据 64。在 74，使用供给器特定数据 32 来解译供给器 CSSC 60。如上所述，这能够通过控制器 22 或应用程序 14 来实现。类似地，在 76，使用系统特定数据 64 来解译系统 CSSC 62。最后，在 78，当已解译的系统 CSSC 62 和已解译的供给器 CSSC 60 相对应时，授权使用供给器 26 和系统 10。

在第一次使用身份证制造系统 10 和定制的供给器之前，可以将系统 10 设置为一般的系统。因此，上述初始系统 CSSC 62 可以是一般码的形式。根据一个实施例，身份证制造系统 10 和定制的供给器 26 的第一次使用引起系统 CSSC 代替了一般码，优选地，使用已解译的供给器 CSSC 60 和系统特定数据 64 来产生所述系统 CSSC。

如上所述，通过使用对应的供给器特定数据 32 和系统特定数据 64 来译解或解码 CSSC 来实现供给器 CSSC 60 和系统 CSSC 62 的解译。可选地，通过使用适当的私钥来解密系统 CSSC 62 和供给器 CSSC 60 能够实现解译步骤。例如，使用存储在卡片密钥 38 的存储器 37 或系统存储器 24 中的私钥能够解密供给器 CSSC 60。

图 4 是示出了形成定制供给器 26 和其对应系统 10 的方法的简化方框图，其中系统 10 包括卡片制造设备 20 和应用程序与驱动软件 14。最初，如方框 80 所示，用户请求提供具有定制卡片制造供给器 26 的定制系统 10。典型地，将用户的定单提供给身份证制造系统 10 和供给器 26 的经销商 82，或者直接提供给设备 20 和供给器 26 的制造者 84。当处理定单时，将如方框 86 所示的秘密 CSSC 分配给用户，然后将该秘密 CSSC 存储在安全数据库 88 中。该特征使得特定的定制供给器 26 与对应的定制设备 20 和/或应用程序 14 相匹配。

优选地，如方框 90 所示，利用将一般安全码施加或存储到各个存储器 24 和 28 中或应用程序 14 的数据中，初始化编程身份证制造设备 20 和供给器 26，以使其作为一般设备进行操作。然后，如方框 92 所示，将与分配给用户的 CSSC 相对应的供给器 CSSC 60 编程到供给器 26 的存储器 28 中。如上所述，优选地，使用对于供给器 26 唯一的供给器特定数据 32 来编码或加密供给器 CSSC 60。

根据一个实施例，还可以通过将其存储在存储器 24 中和/或包括在应用程序 14 中，利用分配给用户的 CSSC 来编程卡片制造设备 20。可选地，具有 CSSC 60 的定制供给器 26 的安装自动地引起更新设备 20 或应用程序 14 的一般安全码，使其对应于供给器 CSSC。这使得将已经处于用户占有的一般设备 20 进行了更新，从而作为定制设备进行操作。一旦出现这种情况，设备 20 只能与具有对应供给器 CSSC

60 的定制供给器 26 一起进行操作。

如上所述，用户还可以通过授权的经销商 82 获得定制设备 20 和供给器 26。这里，将一般设备 20 和供给器 26 从制造者 84 处运送到经销商 82 处。对于新用户，经销商能够从制造者 82 那里请求针对该用户的秘密 CSSC，然后将该秘密 CSSC 存储在安全数据库 88 中。当具有分配的 CSSC 的用户向经销商 82 发出新的定单时，经销商 82 可以访问数据库 84，并检索与用户相对应的 CSSC。然后，如方框 94 所示，可以在由经销商运送到用户之前，将 CSSC 应用到供给器 26 或设备 20 中。

应当理解，在系统的制造者向经销商提供了唯一的 CSSC 的情况下，实际上将经销商看作是用户。于是，经销商提供了都和设备 20、应用程序 14 和具有对应 CSSC 的供给器 26 一起进行操作的系统 10 和供给器 26。

简而言之，能够配置卡片制造供给器 26、身份证制造设备 20 和应用程序 14，使其包括与用户相关的秘密 CSSC，限制其只能与对应的定制组件一起使用。最初，在 86 产生针对用户的 CSSC。该 CSSC 是根据用户定单 80 的。接下来，如 92 所示，将 CSSC 存储在卡片制造供给器 26 的安全数据库 88 和存储器 28 中。最后，配置包括身份证制造应用程序 14 和设备 20 的身份证制造系统 10，使其只能与具有 CSSC 的供给器 26 一起进行操作。通过将对应的 CSSC62 存储在设备 20 的存储器 24 或应用程序 14 的数据系统中，或通过当第一次使用定制供给器 26 和一般设备 20 或应用程序 14 时自动地产生系统 CSSC 60，能够实现以上操作。在这样的使用之后，配置身份证制造系统 10，使其只能与具有对应 CSSC 的定制供给器 26 一起进行操作。

图 5 是示出了由身份证制造系统 10 实现以执行上述安全检查的方法的流程图。应当理解，该方法只是如何实现希望的身份证制造安全的一个示例，在不脱离本发明的精神和范围的前提下，可以添加或去除附加的步骤，或按照不同的定单来进行。通常在 100 开始该方法，其中请求使用身份证制造系统 10 来执行卡片处理功能，例如处理打印任务或执行其它卡片处理功能。这引起应用程序与驱动软件 14 或

控制器 22 请求读取供给器存储器 28。接下来，在 102，控制器 22 使用供给器读取器 30 读取供给器 26 的存储器 28 并将数据直接提供给应用程序 14，或如 104 所示，通过使用供给器特定数据 32 来解译 SSSC 34，实现上述安全的第一级。然后，如 106 所示，通过检查已解译的 SSSC 34 是否与例如存储在系统存储器 24 中的授权码 52 相匹配来验证供给器 26 的有效性。如果确定供给器 26 是无效的，则方法转移到 108，其中控制器 22 将供给器 26 无效通知给应用程序 14。此外，如 110 所示，能够将供给器 26 无效通知给系统 10 的用户。然后，使身份证制造系统 10 不能和供给器 26 一起使用，并终止卡片处理任务。

根据本发明的另一个实施例，当在 106 确定供给器 26 有效时，执行第二级安全检查。在步骤 112，如果必要，与供给器数据 32 一起检索供给器 CSSC 60。接下来，在 114，检索系统 CSSC 62 和系统特定数据 64。然后，在 116，分别使用供给器特定数据 32 和系统特定数据 64，解译供给器 CSSC 60 和系统 CSSC 62。

在 118，进行已解译的供给器 CSSC 60 和已解译的系统 CSSC 62 之间的比较，以确定其是否匹配。如果不比配，则可能是因为系统 CSSC 62 是一般码。因此，在 120 进行检查，以确定系统 CSSC 62 是否是一般码。如果系统 CSSC 62 是一般码，则在 122 产生与供给器 CSSC 60 相对应的 CSSC 并将其存储在存储器 24 中。根据一个实施例，使用已解译的供给器 CSSC 60、系统特定数据 64 和/或私钥来产生系统 CSSC 62。结果，之后配置身份证制造系统 10，以使其只能与具有对应 CSSC 的供给器一起操作。

在系统 CSSC 62 不是一般码的情况下，则其是针对不同于用于当前卡片处理功能的供给器 26 的对应定制供给器 26 而定制的。因此，防止操作安装了供给器 26 的系统 10 并终止卡片处理任务。然后，如 110 所示，将未授权的供给器通知给系统 10 的用户。

在 118 确定已解译的供给器 CSSC 60 与已解译的系统 CSSC 62 相对应的情况下，授权供给器 26 与系统 10 一起使用。因此，如 124 所示，开始卡片处理任务。

尽管已经参考优选实施例描述了本发明，在不脱离本发明的精神

和范围的前提下，本领域的技术人员认为可以进行形式和细节上的改变。例如，本领域的技术人员能够理解可以按照多种不同方式来实现供给器 SSSC 和供给器与系统 CSSC 的解译。解译的一般目的是执行供给器 SSSC、供给器 CSSC 和/或对应参考的某种处理（解码、译解或解密）。然后，将解译的结果用于确定是否授权与身份证制造系统一起使用该供给器。因此，供给器 SSSC、供给器 CSSC 或系统 CSSC 的解译可以包含码的直接处理和用于授权与身份证制造系统一起使用该供给器的对应参考的直接处理。例如，供给器 SSSC 的解译包括以下组件的直接处理：按照某种方式使用供给器特定数据的供给器 SSSC；使用供给器特定数据的对应参考（例如授权码）；或使用供给器特定数据的供给器 SSSC 和对应参考。类似地，供给器 CSSC 的解译包括以下组件的直接处理：按照某种方式使用供给器特定数据的供给器 CSSC；使用供给器特定数据的对应参考（例如系统 CSSC）；或使用供给器特定数据的供给器 CSSC 和对应参考。可以按照相同的方式来进行系统 CSSC 的解译。因此，供给器和系统 CSSC 的解译可以只包含供给器 CSSC 或系统 CSSC 的处理。

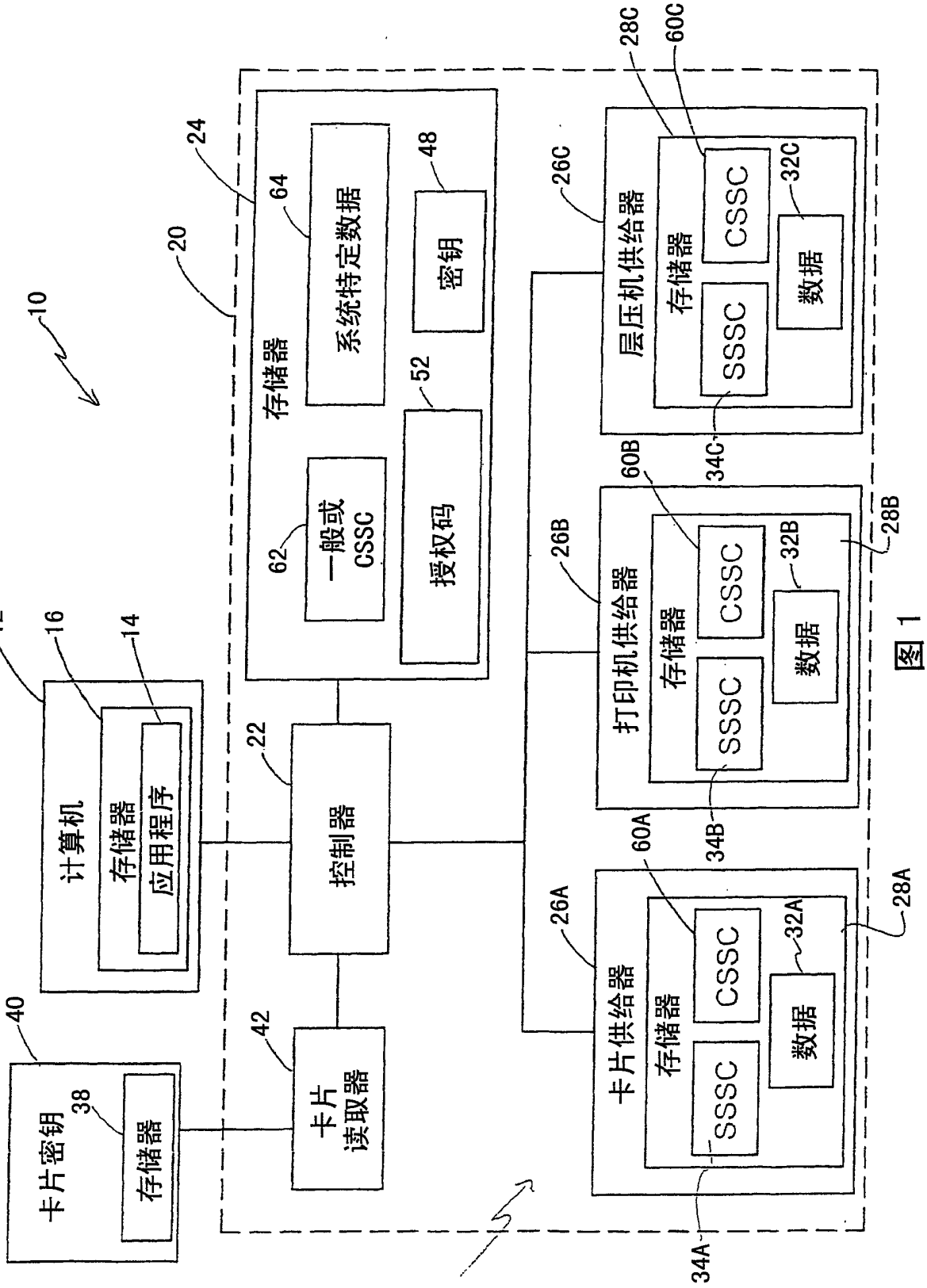

10
12
计算机
16
存储器
14
应用程序
40
卡片密钥
38
存储器
42
卡片读取器
22
控制器
20
24
存储器
64
系统特定数据
48
密钥
52
授权码
62
一般或CSSC
26A
卡片供给器
60A
存储器
CSSC
SSSC
32A
数据
28A
34A
26B
打印机供给器
60B
存储器
CSSC
SSSC
32B
数据
28B
34B
26C
层压机供给器
28C
60C
存储器
CSSC
SSSC
32C
数据
34C

图 1

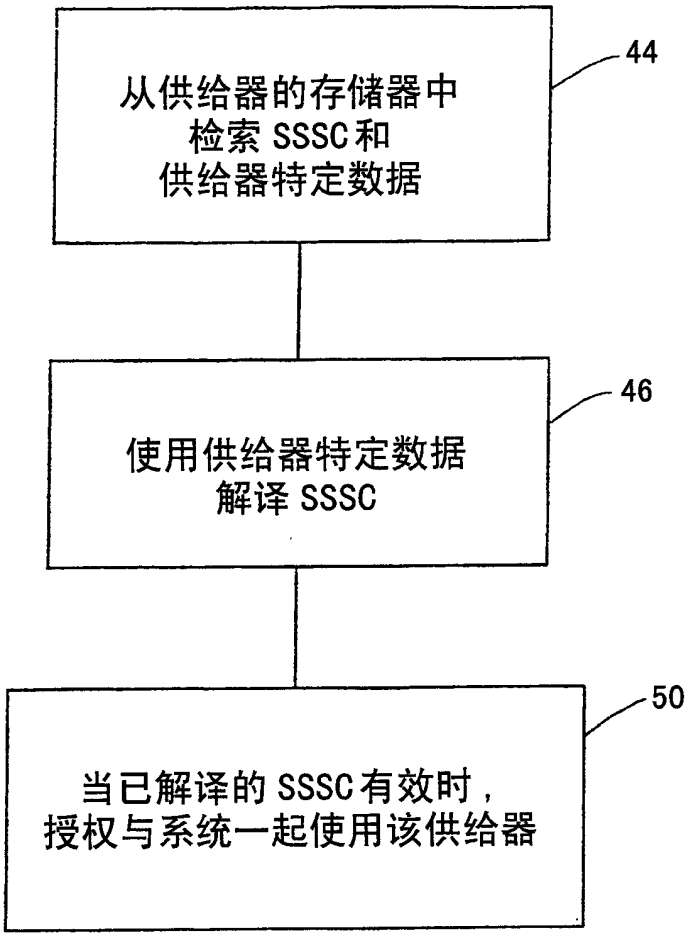

从供给器的存储器中
检索 SSSC 和
供给器特定数据
44
使用供给器特定数据
解译 SSSC
46
当已解译的 SSSC 有效时，
授权与系统一起使用该供给器
50

图 2

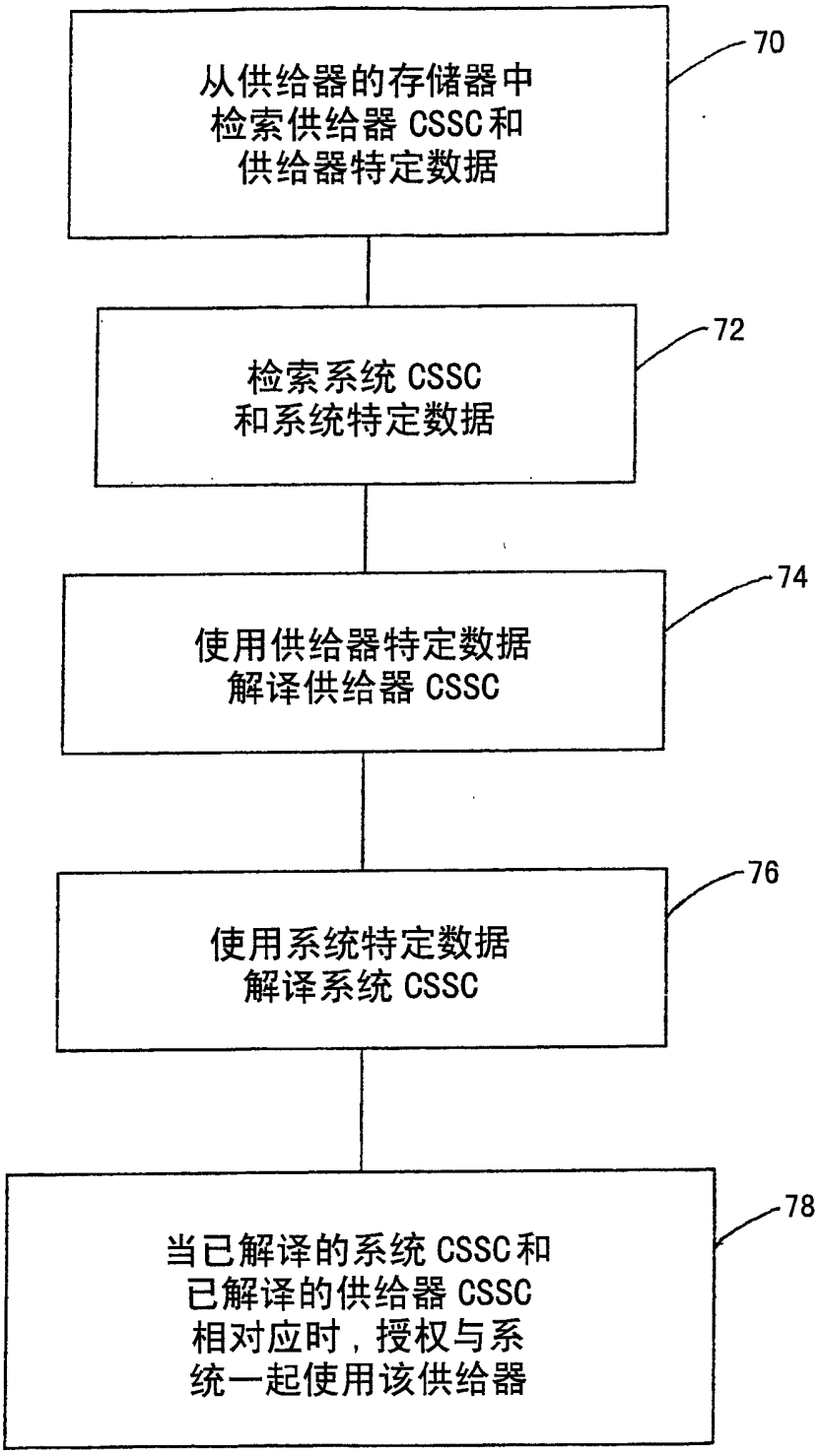

从供给器的存储器中
检索供给器 CSSC和
供给器特定数据
70
检索系统 CSSC
和系统特定数据
72
使用供给器特定数据
解译供给器 CSSC
74
使用系统特定数据
解译系统 CSSC
76
当已解译的系统 CSSC和
已解译的供给器 CSSC
相对应时，授权与系
统一起使用该供给器
78

图 3

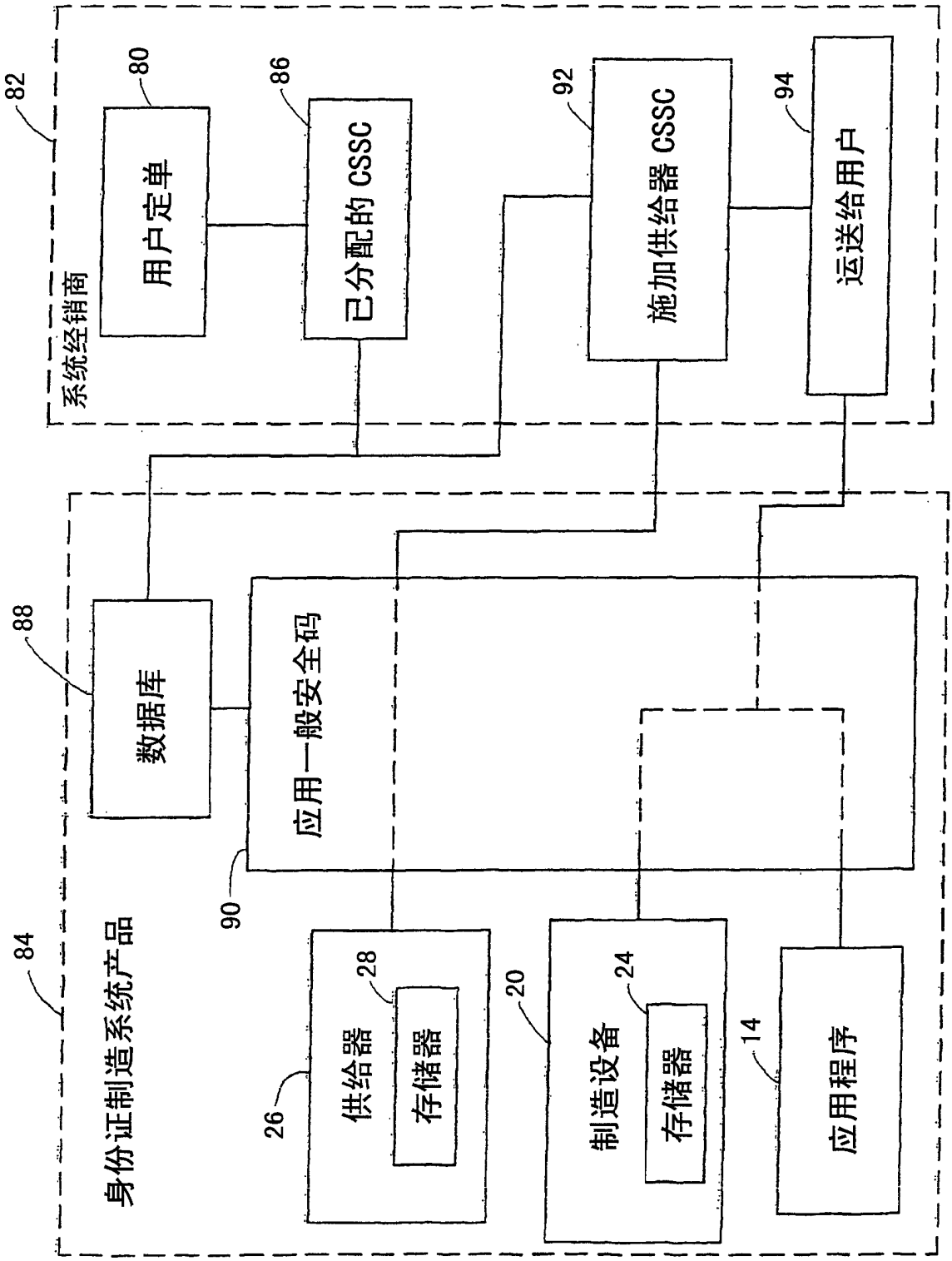

82
系统经销商
80
用户定单
86
已分配的 CSSC
92
施加供给器 CSSC
94
运送给用户
88
数据库
应用一般安全码
90
84
身份证制造系统产品
26
供给器
28
存储器
20
制造设备
24
存储器
14
应用程序

图 4

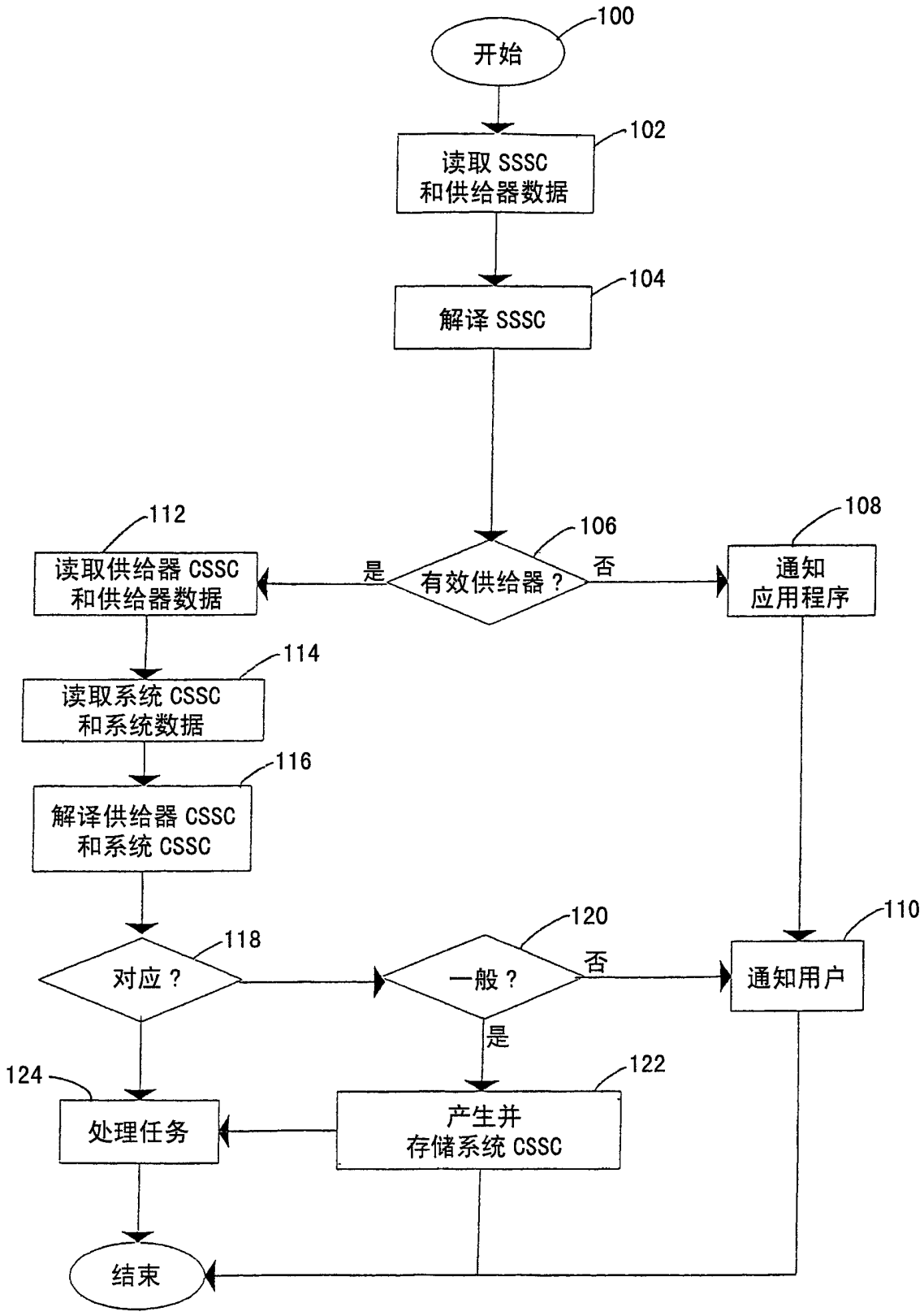

100
开始
102
读取 SSSC
和供给器数据
104
解译 SSSC
106
有效供给器？
是
否
112
读取供给器 CSSC
和供给器数据
108
通知
应用程序
114
读取系统 CSSC
和系统数据
116
解译供给器 CSSC
和系统 CSSC
118
对应？
120
一般？
否
110
通知用户
是
122
产生并
存储系统 CSSC
124
处理任务
结束

图 5