(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 103957210 A
(43)申请公布日 2014.07.30

(21)申请号 201410181142.2

(22)申请日 2014.04.30

(71)申请人 捷德（中国）信息科技有限公司
地址 330096 江西省南昌市高新开发区火炬大街 399 号

(72)发明人 方瑜

(74)专利代理机构 北京三友知识产权代理有限公司 11127
代理人 贾磊

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)
G06F 21/34(2013.01)

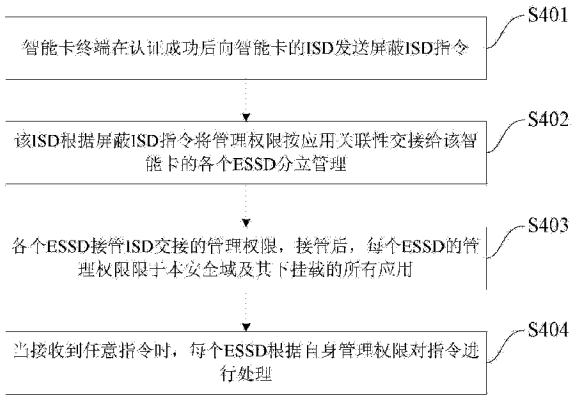
权利要求书2页 说明书6页 附图5页

(54)发明名称

智能卡及其安全控制方法、装置和系统

(57)摘要

本发明提供了一种智能卡及其安全控制方法、装置和系统，该方法包括：智能卡终端在认证成功后向智能卡的 ISD 发送屏蔽 ISD 指令；所述 ISD 根据所述屏蔽 ISD 指令将管理权限按应用关联性交接给所述智能卡的各个 ESSD 分立管理；各个所述 ESSD 接管所述 ISD 交接的管理权限，接管后，每个所述 ESSD 的管理权限限于本安全域及其下挂载的所有应用；当接收到任意指令时，每个所述 ESSD 根据自身管理权限对所述指令进行处理。本发明实现了联合发卡的各个发卡方可将自己的应用仅受自己的安全域控制，因而，提高了联合发卡的各个发卡方的数据安全性。



CN 103957210 A

1. 一种 ISD 侧的安全控制方法，其特征在于，包括以下步骤：

接收智能卡终端发送的认证请求；

对所述认证请求进行认证，生成认证结果并将其发送至所述智能卡终端；

接收所述智能卡终端在认证成功后发送的屏蔽主安全域 ISD 指令；

根据所述屏蔽 ISD 指令将管理权限按应用关联性交接给本智能卡的各个增强型辅助安全域 ESSD 分立管理。

2. 根据权利要求 1 所述的 ISD 侧的安全控制方法，其特征在于，所述根据所述屏蔽 ISD 指令将管理权限按应用关联性交接给本智能卡的各个 ESSD 分立管理，具体包括：

将本智能卡的生命周期状态推送给本智能卡的各个 ESSD；

取消所述 ISD 的令牌验证服务；

将 GP 系统应用程序编程接口的访问对象转接到与该应用关联的 ESSD 上。

3. 根据权利要求 1 所述的 ISD 侧的安全控制方法，其特征在于，在所述根据所述屏蔽 ISD 指令将管理权限按应用关联性交接给本智能卡的各个 ESSD 分立管理之后，还包括：

拒绝任何指令。

4. 一种 ESSD 侧的安全控制方法，其特征在于，包括以下步骤：

接管 ISD 交接的管理权限，接管后，每个 ESSD 的管理权限限于本安全域及其下挂载的所有应用；

当接收到任意指令时，每个所述 ESSD 根据自身管理权限对所述指令进行处理。

5. 一种智能卡终端侧的安全控制方法，其特征在于，包括以下步骤：

向智能卡的 ISD 发起认证请求；

接收所述 ISD 返回的认证结果；

当所述认证结果为成功认证时，向所述 ISD 发送屏蔽 ISD 指令。

6. 根据权利要求 5 所述的智能卡终端侧的安全控制方法，其特征在于，所述屏蔽 ISD 指令包括修改 ISD 的应用标识 AID 为无效 AID 指令。

7. 一种智能卡安全控制方法，其特征在于，包括以下步骤：

智能卡终端在认证成功后向智能卡的 ISD 发送屏蔽 ISD 指令；

所述 ISD 根据所述屏蔽 ISD 指令将管理权限按应用关联性交接给所述智能卡的各个 ESSD 分立管理；

各个所述 ESSD 接管所述 ISD 交接的管理权限，接管后，每个所述 ESSD 的管理权限限于本安全域及其下挂载的所有应用；

当接收到任意指令时，每个所述 ESSD 根据自身管理权限对所述指令进行处理。

8. 一种 ISD，其特征在于，包括：

认证处理模块，用于接收智能卡终端发送的认证请求，对所述认证请求进行认证，生成认证结果并将其发送至所述智能卡终端；

管理权限交接模块，用于接收所述智能卡终端在认证成功后发送的屏蔽 ISD 指令，根据所述屏蔽 ISD 指令将管理权限按应用关联性交接给本智能卡的各个 ESSD 分立管理。

9. 一种 ESSD，其特征在于，包括：

管理权限接管模块，用于接管 ISD 交接的管理权限，接管后，每个所述 ESSD 的管理权限限于本安全域及其下挂载的所有应用；

指令处理模块，用于当接收到任意指令时，根据自身管理权限对所述指令进行处理。

10. 一种智能卡终端，其特征在于，包括：

认证发起模块，用于向智能卡的 ISD 发起认证请求，接收所述 ISD 返回的认证结果；

屏蔽 ISD 指令发起模块，用于在所述认证结果为成功认证时，向所述 ISD 发送屏蔽 ISD 指令。

11. 一种智能卡，其特征在于，包括：

至少一个权利要求 9 所述的 ESSD；以及，

一个权利要求 8 所述的 ISD。

12. 一种智能卡安全控制系统，其特征在于，包括：

权利要求 10 所述的智能卡终端；以及，

权利要求 11 所述智能卡。

智能卡及其安全控制方法、装置和系统

技术领域

[0001] 本发明涉及智能卡的安全控制技术，尤其是涉及一种智能卡及其安全控制方法、装置和系统。

背景技术

[0002] Global Platform 规范（以下简称 GP 规范）是国际通用的智能卡行为管理规范。所有的 Java 卡都遵循 GP 规范。在 GP 规范中，发行方安全域 (ISD，Issuer Security Domain) 拥有最高的管理权限，比如全局删除 (Global Delete)、令牌验证 (Token Verification)、卡片生命周期状态等等，其中，ISD 也称为主安全域。

[0003] 目前国内有很多的多应用联合发卡的场景。GP 规范针对多应用场景，提供了辅助安全域 (SSD，Supplementary Security Domain) 的功能，各个应用可以挂载到各自的 SSD 下，那么各个应用仅受其挂载的 SSD 和 ISD 的管理。

[0004] 但是，如图 6 所示，按照现有 GP 规范，一张卡片上只能有一个 ISD，该 ISD 拥有最高的管理权限，可以锁定、删除卡上的任何应用。通常，联合发卡的发卡方是相互合作的关系，权限应用是平等的，因此，联合发卡的发卡方不希望任何一方掌管 ISD，都希望自己的应用仅受自己安全域的控制，针对这样的应用场景，标准的 GP 规范无法实现该需求。

发明内容

[0005] 本发明的目的在于提供一种智能卡及其安全控制方法、装置和系统，以实现联合发卡的各个发卡方可将自己的应用仅受自己的安全域控制，提高各个发卡方的数据安全性。

[0006] 为达到上述目的，一方面，本发明提供了一种 ISD 侧的安全控制方法，包括以下步骤：

[0007] 接收智能卡终端发送的认证请求；

[0008] 对所述认证请求进行认证，生成认证结果并将其发送至所述智能卡终端；

[0009] 接收所述智能卡终端在认证成功后发送的屏蔽主安全域 ISD 指令；

[0010] 根据所述屏蔽 ISD 指令将管理权限按应用关联性交接给本智能卡的各个增强型辅助安全域 ESSD 分立管理。

[0011] 本发明的 ISD 侧的安全控制方法，所述根据所述屏蔽 ISD 指令将管理权限按应用关联性交接给本智能卡的各个 ESSD 分立管理，具体包括：

[0012] 将本智能卡的生命周期状态推送给本智能卡的各个 ESSD；

[0013] 取消所述 ISD 的令牌验证服务；

[0014] 将 GP 系统应用程序编程接口的访问对象转接到与该应用关联的 ESSD 上。

[0015] 本发明的 ISD 侧的安全控制方法，在所述根据所述屏蔽 ISD 指令将管理权限按应用关联性交接给本智能卡的各个 ESSD 分立管理之后，还包括：

[0016] 拒绝任何指令。

[0017] 另一方面，本发明还提供了一种 ESSD 侧的安全控制方法，包括以下步骤：

[0018] 接管 ISD 交接的管理权限，接管后，每个 ESSD 的管理权限限于本安全域及其下挂载的所有应用；

[0019] 当接收到任意指令时，每个所述 ESSD 根据自身管理权限对所述指令进行处理。

[0020] 再一方面，本发明还提供了一种智能卡终端侧的安全控制方法，包括以下步骤：

[0021] 向智能卡的 ISD 发起认证请求；

[0022] 接收所述 ISD 返回的认证结果；

[0023] 当所述认证结果为成功认证时，向所述 ISD 发送屏蔽 ISD 指令。

[0024] 本发明的智能卡终端侧的安全控制方法，所述屏蔽 ISD 指令包括修改 ISD 的应用标识 AID 为无效 AID 指令。

[0025] 再一方面，本发明还提供了一种智能卡安全控制方法，包括以下步骤：

[0026] 智能卡终端在认证成功后向智能卡的 ISD 发送屏蔽 ISD 指令；

[0027] 所述 ISD 根据所述屏蔽 ISD 指令将管理权限按应用关联性交接给所述智能卡的各个 ESSD 分立管理；；

[0028] 各个所述 ESSD 接管所述 ISD 交接的管理权限，接管后，每个所述 ESSD 的管理权限限于本安全域及其下挂载的所有应用；

[0029] 当接收到任意指令时，每个所述 ESSD 根据自身管理权限对所述指令进行处理。

[0030] 再一方面，本发明还提供了一种 ISD，包括：

[0031] 认证处理模块，用于接收智能卡终端发送的认证请求，对所述认证请求进行认证，生成认证结果并将其发送至所述智能卡终端；

[0032] 管理权限交接模块，用于接收所述智能卡终端在认证成功后发送的屏蔽 ISD 指令，根据所述屏蔽 ISD 指令将管理权限按应用关联性交接给本智能卡的各个 ESSD 分立管理。

[0033] 再一方面，本发明还提供了一种 ESSD，包括：

[0034] 管理权限接管模块，用于接管 ISD 交接的管理权限，接管后，每个所述 ESSD 的管理权限限于本安全域及其下挂载的所有应用；

[0035] 指令处理模块，用于当接收到任意指令时，根据自身管理权限对所述指令进行处理。

[0036] 再一方面，本发明还提供了一种智能卡终端，包括：

[0037] 认证发起模块，用于向智能卡的 ISD 发起认证请求，接收所述 ISD 返回的认证结果；

[0038] 屏蔽 ISD 指令发起模块，用于在所述认证结果为成功认证时，向所述 ISD 发送屏蔽 ISD 指令。

[0039] 再一方面，本发明还提供了一种智能卡，包括：

[0040] 至少一个如上所述的 ESSD；以及，

[0041] 一个如上所述的 ISD。

[0042] 再一方面，本发明还提供了一种智能卡安全控制系统，包括：

[0043] 如上所述的智能卡终端；以及，

[0044] 如上所述智能卡。

[0045] 本发明中，在认证成功后智能卡终端向智能卡的 ISD 发送屏蔽 ISD 指令，ISD 根据屏蔽 ISD 指令将管理权限按应用关联性交接给该智能卡的各个 ESSD 分立管理，各个 ESSD 接管 ISD 交接的管理权限后，ISD 完全丧失了所有的管理能力，每个 ESSD 的管理权限限于本安全域及其下挂载的所有应用，也就是说，任何一个 ESSD 仍然没有访问和管理其他 ESSD 的权限。从而实现了联合发卡的各个发卡方可将自己的应用仅受自己的安全域控制，因而，提高了联合发卡的各个发卡方的数据安全性。

附图说明

[0046] 此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，并不构成对本发明的限定。在附图中：

[0047] 图 1 为本发明实施例的智能卡终端侧的安全控制方法的流程图；

[0048] 图 2 为本发明实施例的 ISD 侧的安全控制方法的流程图；

[0049] 图 3 为本发明实施例的 ESSD 侧的安全控制方法的流程图；

[0050] 图 4 为本发明实施例的智能卡安全控制方法的流程图；

[0051] 图 5 为本发明实施例的智能卡安全控制系统的结构图；

[0052] 图 5a 为图 5 中智能卡的结构图；

[0053] 图 5b 为图 5a 中智能卡的 ISD 的结构图；

[0054] 图 5c 为图 5a 中智能卡的 ESSD 的结构图；

[0055] 图 5d 为图 5 中智能卡终端的结构图；

[0056] 图 6 为现有 GP 规范下的智能卡安全控制架构图；

[0057] 图 7 为本发明实施例的智能卡安全控制架构图。

具体实施方式

[0058] 为使本发明的目的、技术方案和优点更加清楚明白，下面结合实施例和附图，对本发明做进一步详细说明。在此，本发明的示意性实施例及其说明用于解释本发明，但并不作为对本发明的限定。

[0059] 下面结合附图，对本发明的具体实施方式作进一步的详细说明。

[0060] 参考图 1 所示，本发明实施例的智能卡终端侧的安全控制方法，包括以下步骤：

[0061] 步骤 S101、向智能卡的 ISD 发起认证请求。

[0062] 步骤 S102、接收该 ISD 返回的认证结果。其中，认证结果通常为返回码。

[0063] 步骤 S103、当认证结果为成功认证时，向该 ISD 发送屏蔽 ISD 指令。智能卡终端在接收到认证结果后会进行认证结果检查，如果是成功认证，则向发送屏蔽 ISD 指令。可见，只有认证成功，才能进行 ISD 屏蔽。其中，屏蔽 ISD 指令可以有多种形式，例如，屏蔽 ISD 指令可以为修改 ISD 的应用标识 (AID，Application Identifier) 为无效 AID 指令，当然，也可以采用其他特殊指令来实现。

[0064] 参考图 2 所示，本发明实施例的 ISD 侧的安全控制方法，包括以下步骤：

[0065] 步骤 S201、接收智能卡终端发送的认证请求。

[0066] 步骤 S202、对认证请求进行认证，生成认证结果并将其发送至智能卡终端。

[0067] 步骤 S203、接收智能卡终端在认证成功后发送的屏蔽 ISD 指令。

[0068] 步骤 S204、根据屏蔽 ISD 指令将管理权限按应用关联性交接给本智能卡的各个增强型辅助安全域 (ESSD，Enhanced Supplementary Security Domain)。ISD 收到该指令后，将执行一系列的处理，所谓的根据屏蔽 ISD 指令将管理权限按应用关联性交接给本智能卡的各个 ESSD 分立管理，具体包括 :将本智能卡的生命周期状态推送给本智能卡的各个 ESSD ;取消 ISD 的令牌验证服务 ;将 GP 系统应用程序编程接口 (即 GPSystem API) 的访问对象转接到与该应用关联的 ESSD 上。

[0069] 在 ISD 屏蔽后，ISD 将拒绝任何指令，例如，对于任何指令都返回拒绝代码 0X6D00，此后 ISD 完全丧失了所有的管理能力，那么智能卡就会处于各个 ESSD 分立管理的局面，各个应用仅受其挂载的 ESSD 的管理。这样的局面很好的解决了各个发卡方所期望的 :自己的应用仅受自己的安全域的控制 ;没有任何一方能力跨越安全域管理。

[0070] 参考图 3 所示，本发明实施例的 ESSD 侧的安全控制方法，包括以下步骤 :

[0071] 步骤 S301、接管 ISD 交接的管理权限，接管后，每个 ESSD 的管理权限限于本安全域及其下挂载的所有应用，也就说，任何一个 ESSD 仍然没有访问和管理其他 ESSD 的权限。

[0072] 本步骤中，ESSD 接管的功能如下 :

[0073] 1、ESSD 能够执行，如下载、安装、删除等基本管理功能 ;

[0074] 2、ESSD 本身不能被删除 ;

[0075] 3、ESSD 下，下载新的应用仅由 ESSD 控制，不需要得到 ISD 的验证 ;

[0076] 4、ESSD 接管 ISD 的生命周期状态作为自身的生命周期状态，ESSD 的生命周期状态将直接影响其下所挂载的应用 :

[0077] 1)、ESSD 处于 LOCKED 状态时，其下所有应用都不能被选择 ;

[0078] 2)、ESSD 处于 TERMINATED 状态时，该 ESSD 和其下所有应用都被终结 ;

[0079] 5、ESSD 的生命周期状态不影响其他的 ESSD 和应用 ;

[0080] 6、GPSystem API 不再访问 ISD 的生命周期状态，而将访问其对应的 ESSD 的生命周期状态，GPSystem API 将使用 ESSD 的状态标志作为访问和判断标志 :

[0081] 1)、GPSystem.lockCard() 将会锁定对应的 ESSD ;

[0082] 2)、GPSystem.terminateCard() 将会终结对应的 ESSD。

[0083] 实际上，ESSD 是由普通 SSD 在接管了 ISD 的部分管理权限后升级而成的。通过如下表 1 我们可以更加直观的看出 ISD 和 ESSD 在 ISD 被屏蔽前后的变化。

[0084] 表 1

[0085]

	活动的 ISD 和普通 SSD	屏蔽的 ISD 和 ESSD
ISD 的状态	● ISD 拥有全局的管理权限; ● SSD 下部分操作需要等到 ISD 的认证;	● ISD 拒绝所有指令; ● ESSD 下的所有操作无需 ISD 的认证;
SSD 的权限	● 能被 ISD 删除、锁定; ● 普通权限，相关操作需要 ISD 的认证;	● ESSD 无法删除 ● 扩展权限，无需 ISD 的认证;
Card life cycle	等同于 ISD 的 life cycle; 影响到智能卡上所有的应用;	对应到挂载的 ESSD 仅影响 ESSD 下挂载的应用;
GPSystem API	访问的是智能卡的 life cycle 状态	访问的是当前应用挂载的 ESSD 的 life cycle

[0086] 步骤 S302、当接收到任意指令时，每个 ESSD 根据自身管理权限对指令进行处理。

[0087] 结合图 4 所示，本发明实施例的智能卡安全控制方法，包括以下步骤：

[0088] 步骤 S401、智能卡终端在认证成功后向智能卡的 ISD 发送屏蔽 ISD 指令。

[0089] 步骤 S402、该 ISD 根据屏蔽 ISD 指令将管理权限按应用关联性交接给该智能卡的各个 ESSD 分立管理。具体参见上述步骤 S204。

[0090] 步骤 S403、该智能卡的各个 ESSD 接管该 ISD 交接的管理权限，接管后，每个 ESSD 的管理权限限于本安全域及其下挂载的所有应用，也就说，任何一个 ESSD 仍然没有访问和管理其他 ESSD 的权限。具体参见上述步骤 S301。

[0091] 步骤 S404、当接收到任意指令时，每个 ESSD 根据自身管理权限对指令进行处理。

[0092] 本发明实施例中，在认证成功后智能卡终端向智能卡的 ISD 发送屏蔽 ISD 指令，该 ISD 根据屏蔽 ISD 指令将管理权限按应用关联性交接给智能卡的各个 ESSD 分立管理（如图 7 所示），各个 ESSD 接管 ISD 交接的管理权限后，ISD 完全丧失了所有的管理能力，每个 ESSD 的管理权限限于本安全域及其下挂载的所有应用，也就是说，任何一个 ESSD 仍然没有访问和管理其他 ESSD 的权限。从而实现了联合发卡的各个发卡方可将自己的应用仅受自己的安全域控制，因而，提高了联合发卡的各个发卡方的数据安全性。

[0093] 参考图 5 ～图 5d 所示，本发明实施例的智能卡安全控制系统包括智能卡 5 和智能卡终端 6。其中：

[0094] 智能卡终端 6 包括：

[0095] 认证发起模块 61，用于向智能卡 5 的 ISD51 发起认证请求，接收智能卡 5 返回的认证结果。

[0096] 屏蔽 ISD 指令发起模块 62，用于在认证结果为成功认证时，向该 ISD51 发送屏蔽 ISD 指令。

[0097] 智能卡 5 通常包括一个 ISD51 和多个 ESSD52。，其中：

[0098] ISD51 包括：

[0099] 认证处理模块 511，用于接收智能卡终端 6 发送的认证请求，对认证请求进行认证，生成认证结果并将其发送至智能卡终端 6；

[0100] 管理权限交接模块 512，用于接收智能卡终端 6 在认证成功后发送的屏蔽 ISD 指令，根据屏蔽 ISD 指令将管理权限按应用关联性交接给本智能卡的各个 ESSD52 分立管理。

[0101] 每个 ESSD52 包括：

[0102] 管理权限接管模块 521，用于接管 ISD 交接的管理权限，接管后，各个 ESSD52 的管理权限限于本安全域及其下挂载的所有应用；也就说，任何一个 ESSD52 仍然没有访问和管理其他 ESSD52 的权限。

[0103] 指令处理模块 522，用于当接收到任意指令时，根据自身管理权限对指令进行处理。

[0104] 本发明实施例中，在认证成功后智能卡终端 6 向智能卡 5 的 ISD51 发送屏蔽 ISD 指令，该 ISD51 根据屏蔽 ISD 指令将管理权限按应用关联性交接给智能卡 5 的各个 ESSD52 分立管理，各个 ESSD52 接管 ISD51 交接的管理权限后，ISD51 完全丧失了所有的管理能力，每个 ESSD52 的管理权限限于本安全域及其下挂载的所有应用，也就是说，任何一个 ESSD52 仍然没有访问和管理其他 ESSD52 的权限。从而实现了联合发卡的各个发卡方可将自己的

应用仅受自己的安全域控制，因而，提高了联合发卡的各个发卡方的数据安全性。

[0105] 本领域技术人员还可以了解到本发明实施例列出的各种说明性逻辑块、单元和步骤可以通过硬件、软件或两者的结合来实现。至于是通过硬件还是软件来实现取决于特定的应用和整个系统的设计要求。本领域技术人员可以对于每种特定的应用，可以使用各种方法实现所述的功能，但这种实现不应被理解为超出本发明实施例保护的范围。

[0106] 本发明实施例中所描述的各种说明性的逻辑块，或单元都可以通过通用处理器，数字信号处理器，专用集成电路 (ASIC)，现场可编程门阵列或其它可编程逻辑装置，离散门或晶体管逻辑，离散硬件部件，或上述任何组合的设计来实现或操作所描述的功能。通用处理器可以为微处理器，可选地，该通用处理器也可以为任何传统的处理器、控制器、微控制器或状态机。处理器也可以通过计算装置的组合来实现，例如数字信号处理器和微处理器，多个微处理器，一个或多个微处理器联合一个数字信号处理器核，或任何其它类似的配置来实现。

[0107] 本发明实施例中所描述的方法或算法的步骤可以直接嵌入硬件、处理器执行的软件模块、或者这两者的结合。软件模块可以存储于 RAM 存储器、闪存、ROM 存储器、EPROM 存储器、EEPROM 存储器、寄存器、硬盘、可移动磁盘、CD-ROM 或本领域中其它任意形式的存储媒介中。示例性地，存储媒介可以与处理器连接，以使得处理器可以从存储媒介中读取信息，并可以向存储媒介存写信息。可选地，存储媒介还可以集成到处理器中。处理器和存储媒介可以设置于 ASIC 中，ASIC 可以设置于用户终端中。可选地，处理器和存储媒介也可以设置于用户终端中的不同的部件中。

[0108] 在一个或多个示例性的设计中，本发明实施例所描述的上述功能可以在硬件、软件、固件或这三者的任意组合来实现。如果在软件中实现，这些功能可以存储与电脑可读的媒介上，或以一个或多个指令或代码形式传输于电脑可读的媒介上。电脑可读媒介包括电脑存储媒介和便于使得让电脑程序从一个地方转移到其它地方的通信媒介。存储媒介可以是任何通用或特殊电脑可以接入访问的可用媒体。例如，这样的电脑可读媒体可以包括但不限于 RAM、ROM、EEPROM、CD-ROM 或其它光盘存储、磁盘存储或其它磁性存储装置，或其它任何可以用于承载或存储以指令或数据结构和其它可被通用或特殊电脑、或通用或特殊处理器读取形式的程序代码的媒介。此外，任何连接都可以被适当地定义为电脑可读媒介，例如，如果软件是从一个网站站点、服务器或其它远程资源通过一个同轴电缆、光纤电缆、双绞线、数字用户线 (DSL) 或以例如红外、无线和微波等无线方式传输的也被包含在所定义的电脑可读媒介中。所述的碟片 (disk) 和磁盘 (disc) 包括压缩磁盘、镭射盘、光盘、DVD、软盘和蓝光光盘，磁盘通常以磁性复制数据，而碟片通常以激光进行光学复制数据。上述的组合也可以包含在电脑可读媒介中。

[0109] 以上所述的具体实施例，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施例而已，并不用于限定本发明的保护范围，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

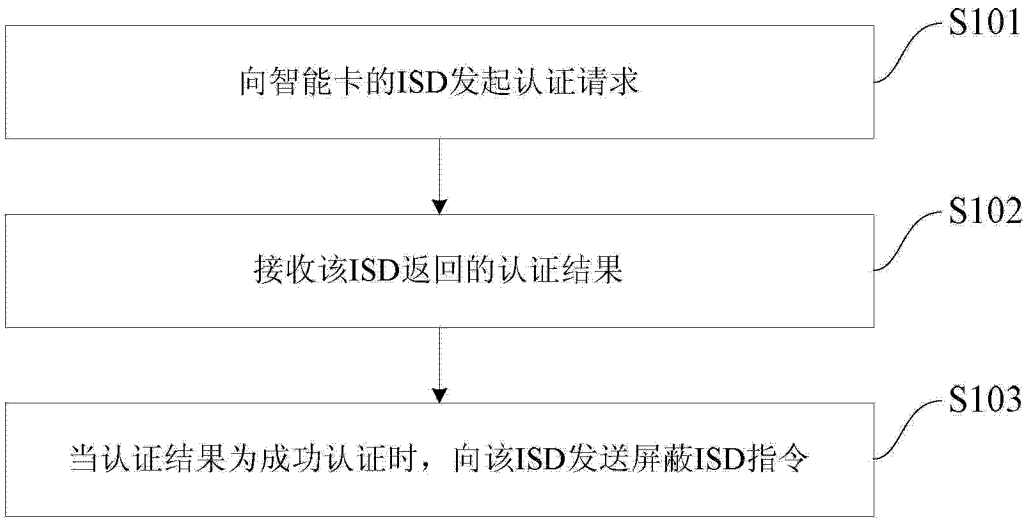

S101
向智能卡的ISD发起认证请求
S102
接收该ISD返回的认证结果
S103
当认证结果为成功认证时，向该ISD发送屏蔽ISD指令

图 1

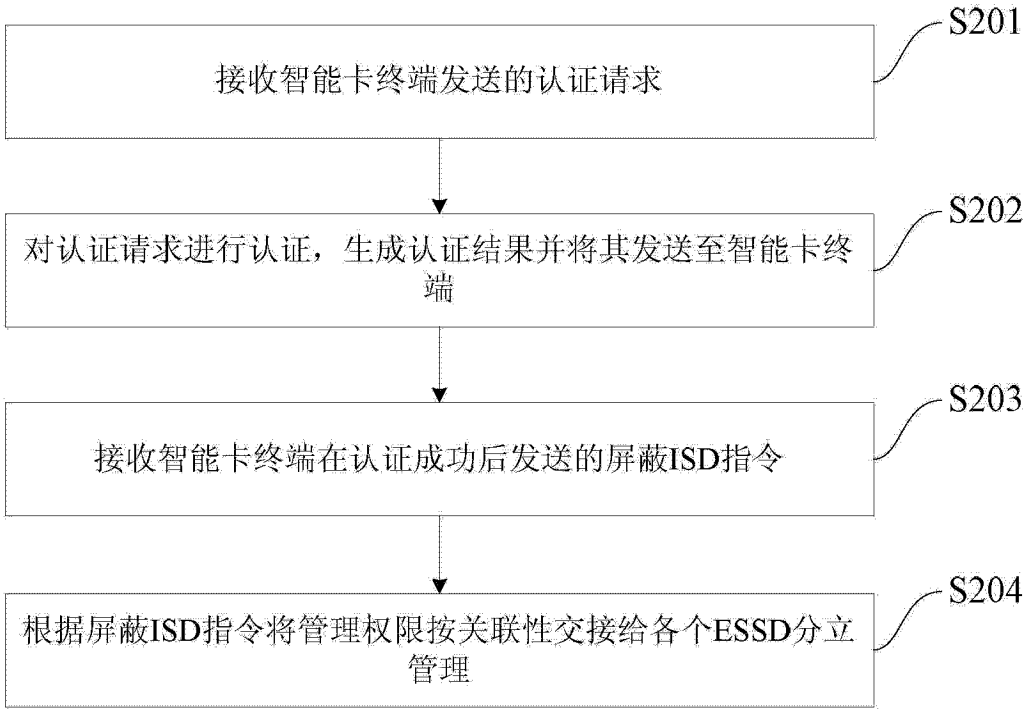

S201
接收智能卡终端发送的认证请求
S202
对认证请求进行认证，生成认证结果并将其发送至智能卡终端
S203
接收智能卡终端在认证成功后发送的屏蔽ISD指令
S204
根据屏蔽ISD指令将管理权限按关联性交接给各个ESSD分立管理

图 2

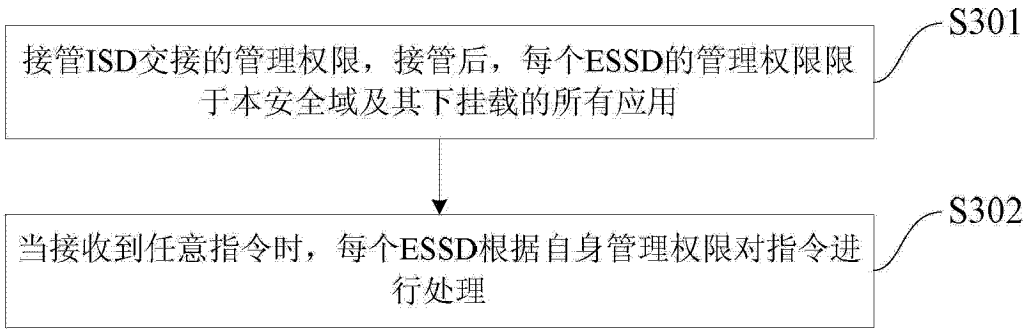

S301
接管ISD交接的管理权限，接管后，每个ESSD的管理权限限于本安全域及其下挂载的所有应用
S302
当接收到任意指令时，每个ESSD根据自身管理权限对指令进行处理

图 3

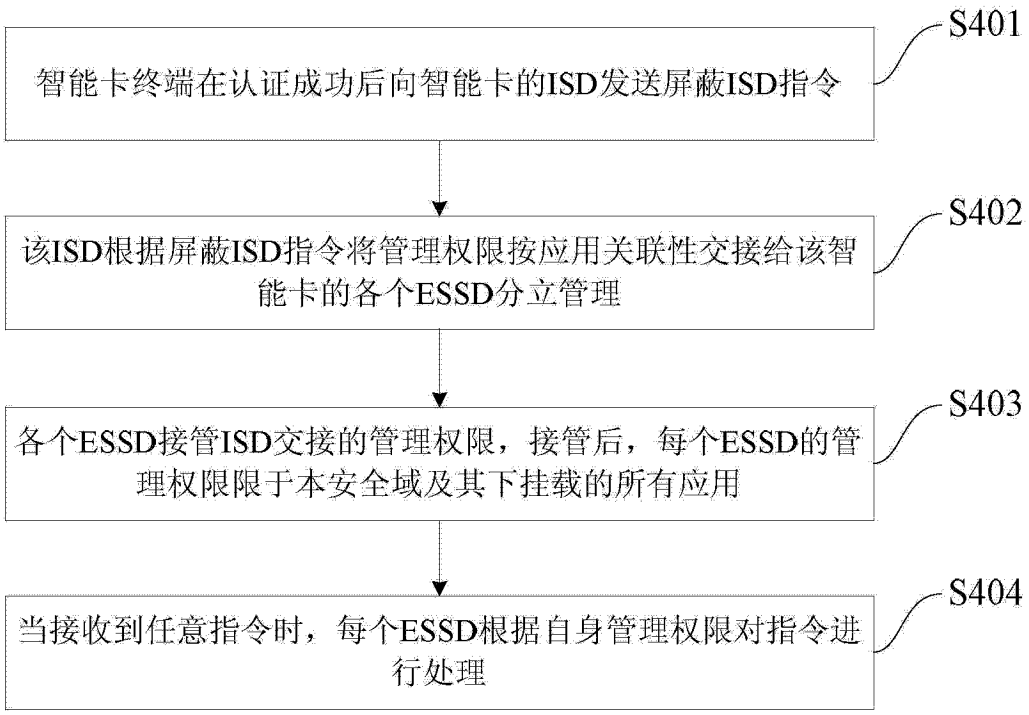

S401
智能卡终端在认证成功后向智能卡的ISD发送屏蔽ISD指令
S402
该ISD根据屏蔽ISD指令将管理权限按应用关联性交接给该智能卡的各个ESSD分立管理
S403
各个ESSD接管ISD交接的管理权限，接管后，每个ESSD的管理权限限于本安全域及其下挂载的所有应用
S404
当接收到任意指令时，每个ESSD根据自身管理权限对指令进行处理

图 4

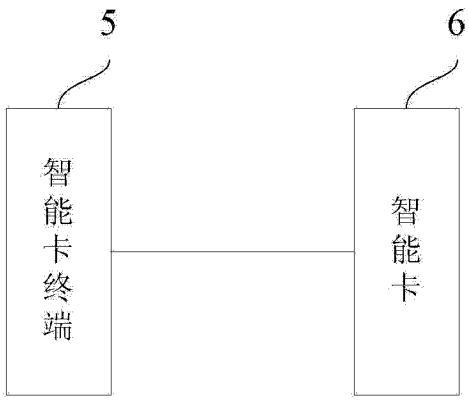


图 5

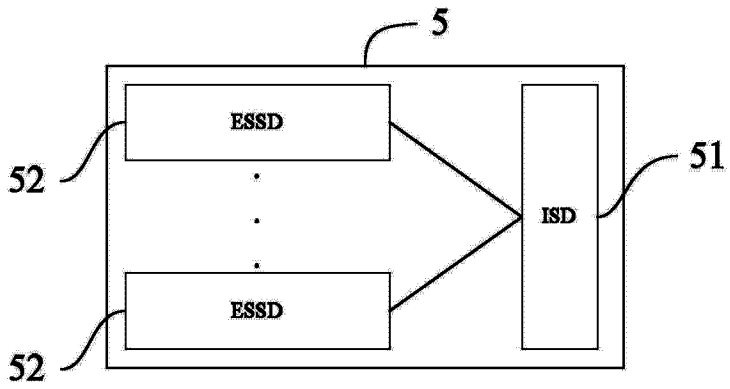


图 5a

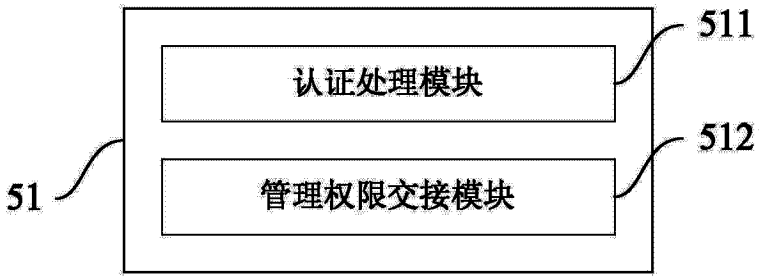


图 5b

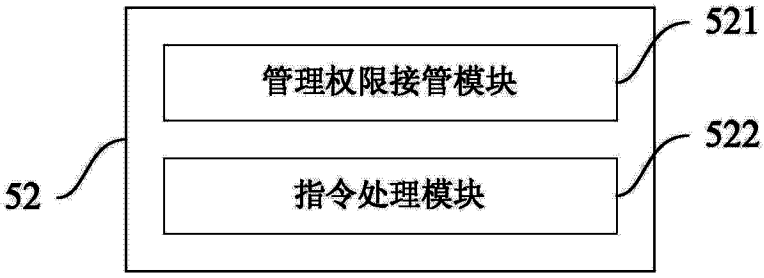


图 5c

图 5d

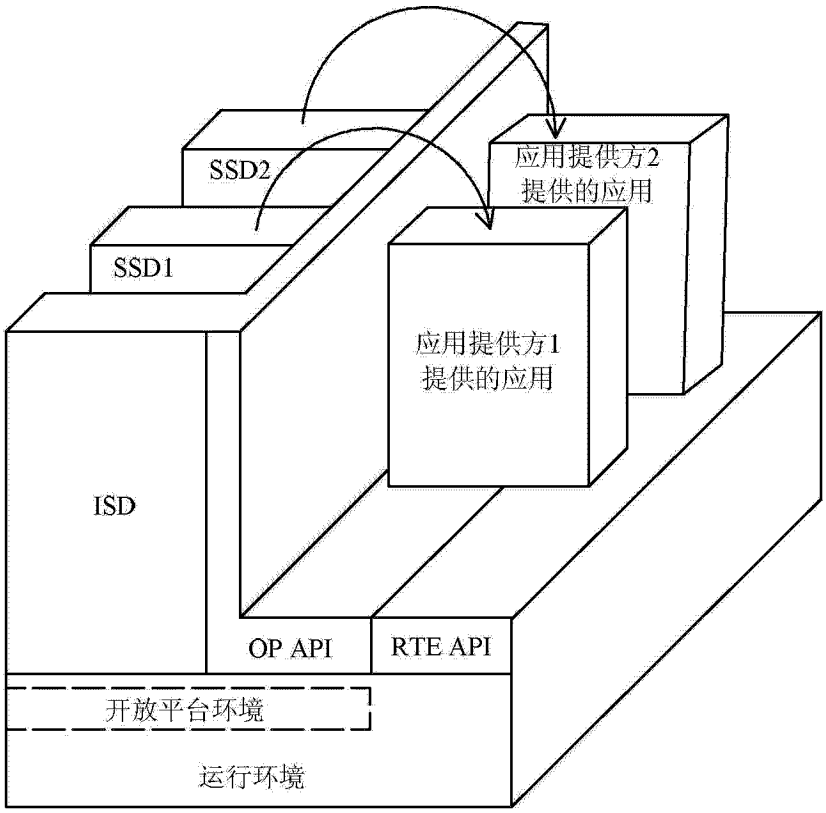

SSD2
SSD1
ISD
应用提供方2
提供的应用
应用提供方1
提供的应用
OP API
RTE API
开放平台环境
运行环境

图 6

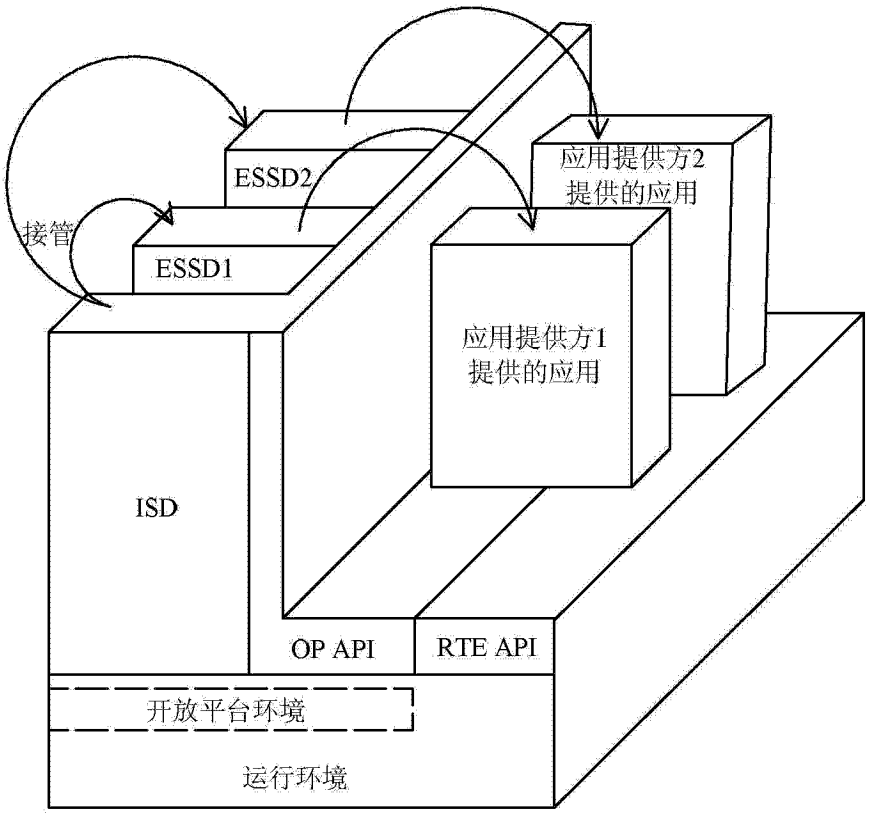

ESSD2
应用提供方2
提供的应用
接管
ESSD1
应用提供方1
提供的应用
ISD
OP API
RTE API
开放平台环境
运行环境

图 7