(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101416204 B
(45)授权公告日 2012.05.09

(21)申请号 200780012048.2

(22)申请日 2007.03.29

(30)优先权数据
098865/2006 2006.03.31 JP
075217/2007 2007.03.22 JP

(85)PCT申请进入国家阶段日
2008.10.06

(86)PCT申请的申请数据
PCT/JP2007/056982 2007.03.29

(87)PCT申请的公布数据
WO2007/119594 JA 2007.10.25

(73)专利权人 松下电器产业株式会社
地址 日本大阪府

(72)发明人 田靡雅基 竹内康雄 鹤切惠美 德田泰久

(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 胡琪

(51)Int.Cl.
G06K 19/07(2006.01)
G06F 21/24(2006.01)
G06K 17/00(2006.01)
G06K 19/10(2006.01)

(56)对比文件
CN 1441385 A,2003.09.10, 全文.
CN 1726478 A,2006.01.25, 全文.
US 6233683 B1,2001.05.15, 全文.
US 20050234825 A1,2005.10.20, 全文.
JP 10-143774 A,1998.05.29, 全文.
CN 1549198 A,2004.11.24, 全文.

审查员 陈丽娜

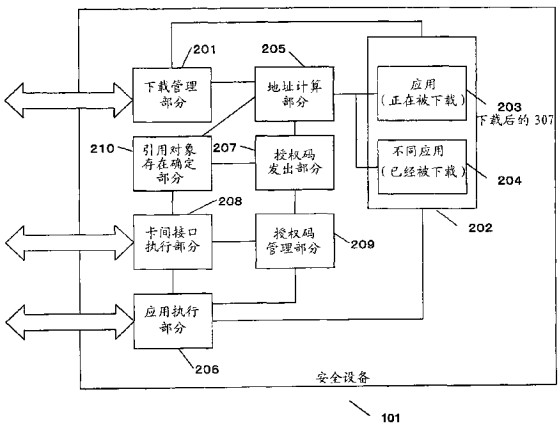
权利要求书 1 页 说明书 28 页 附图 35 页

(54)发明名称

安全设备

(57)摘要

有可能解决由一个安全设备拥有的服务器应用不能被由另一个安全设备拥有的客户机应用使用的问题。一安全设备包括:应用存储单元(202),用于存储客户机应用,作为执行数据处理的应用;地址计算单元(205),用于判定所述应用存储部单元(202)是否具有用于向/从所述客户机传送数据的服务器应用;以及引用对象存在判定单元(210),用于当所述地址计算单元(205)已经判定所述应用存储单元(202)没有用于向/从第一客户机应用传送数据的第一服务器应用时,判定是否另一安全设备具有第一服务器应用。



CN 101416204 B

1. 一种安全设备，包括：

应用存储部分，其存储客户机应用，作为用于执行数据处理的应用；

地址计算部分，其确定所述应用存储部分是否具有用于向和从所述客户机应用传送数据的服务器应用；

引用对象存在确定部分，当所述地址计算部分确定所述应用存储部分不具有用于向和从第一客户机应用传送数据的第一服务器应用时，该引用对象存在确定部分确定不同安全设备是否具有所述第一服务器应用；

卡间接口执行部分，其访问所述不同安全设备，其中，所述引用对象存在确定部分根据所述卡间接口执行部分的结果确定所述不同安全设备是否具有所述第一服务器应用；

授权码发出部分，当所述引用对象存在确定部分确定所述不同安全设备具有所述第一服务器应用时，该授权码发出部分发出用于许可引用所述第一服务器应用的授权码；以及

应用执行部分，其根据所述授权码来执行所述第一客户机应用。

2. 按照权利要求 1 所述的安全设备，还包括授权码管理部分，其至少管理包含所述不同安全设备具有的第一服务器应用的应用标识符的管理信息，

其中，当执行第一客户机应用时，所述应用执行部分基于所述管理信息向引用对象发送所述应用标识符、所述引用对象和要传送到所述引用对象的参数的至少一个，作为响应。

3. 按照权利要求 1 所述的安全设备，还包括：安全性管理部分，其提供由所述卡间接口执行部分发送和接收的数据的安全性。

4. 按照权利要求 1 所述的安全设备，其中，当所述授权码发出部分响应于所述第一客户机应用的使用限制而发出使用受限授权码时，所述应用执行部分根据所述授权码限制从所述第一客户机应用引用所述第一服务器应用。

5. 按照权利要求 1 所述的安全设备，还包括：下载管理部分，其下载第二客户机应用，其中

如果所述卡间接口执行部分不能引用第二服务器应用，则所述授权码发出部分发出临时授权码，用于许可所述下载管理部分下载所述第二客户机应用。

6. 按照权利要求 5 所述的安全设备，其中，当卡间接口执行部分能够引用所述第二服务器应用时，在所述第二服务器应用和按照所述临时授权码被许可下载的第二客户机应用之间进行数据通信。

7. 按照权利要求 1 所述的安全设备，还包括：堆栈操作部分，其使得应用执行部分根据来自所述不同安全设备具有的所述第一服务器应用的命令和基于所述处理的返回值来执行第一客户机应用。

8. 按照权利要求 1 所述的安全设备，其中，

所述应用执行部分使得所述卡间接口执行部分获取具有所述第一服务器应用的所述不同安全设备的使用状态，并且

当所述使用状态指示其中不能使用不同安全设备的状态时，所述卡间接口执行部分接收用于指示不能使用所述不同安全设备的数据。

9. 按照权利要求 1 所述的安全设备，其中，

所述客户机应用包含观看权限和被观看的内容，并且

所述服务器应用检查在从所述客户机应用传送的观看权限内涉及的条件。

安全设备

技术领域

[0001] 本发明涉及安全设备和连接到所述安全设备的外部机器。

背景技术

[0002] 当前，关注 IC 卡作为安全设备。开发了允许在发行卡后向其下载应用的多应用兼容卡，以用于改善用户的方便性，并且降低想要提供 IC 卡服务的企业的进入屏障。

[0003] 近来，已经提出了包括 IC 芯片内的大容量存储器的、可用作 IC 卡扩展存储器保护区域的设备（以下称为安全存储卡），并且已经使得有可能满足 IC 卡应用数据的较大容量的需要。因为可以使安全存储卡适合于移动机器的大小，因此可以预期所述安全存储卡将被直接地插入到具有用于开发的插槽的移动机器内，以用作使用所述移动机器的 EC（电子商务）服务。

[0004] 在此，将简述 IC 卡的硬件配置。

[0005] 图 30 是关于 IC 卡的硬件的功能方框图。IC 卡 3001 包括 CPU（中央处理单元）3002、ROM（只读存储器）3003、易失性存储器（例如 RAM：随机存取存储器）3004、易失性存储器（例如 EEPROM：电可擦除可编程只读存储器）3005 和输入 / 输出接口 3006。CPU 3002 执行计算。ROM 3003 是不能被重写的只读存储器。ROM 3003 的存储内容在制造 IC 卡时被确定，并且不能在以后被改变。RAM 3004 是可以被读和写的存储器。如果关断电源，EEPROM 3005 的内容被保留。输入 / 输出接口 3006 负责在 IC 卡和外部系统之间的数据交换。在 CPU 3002 中执行的程序通常被称为“应用”。用于执行应用的代码被存储在 ROM 3003 或者 EEPROM 3005 内。除了在图 30 中所示的部件之外，IC 卡可以包括加密协处理器，用于加密操作。

[0006] 在 IC 卡内安装的应用和外部系统（读取器）使用在 ISO/IEC 7816-4 中定义的 APDU（应用协议数据单元）来交换数据。APDU 由通过读取器给出到 IC 卡的命令和从 IC 卡向读取器返回的响应构成。

[0007] 图 31 示出了 APDU 命令 3101，并且由首标和主体构成。所述主体具有任何期望的长度，并且如果其为空则可以不存在。所述首标由类 (CLA)、指令 (INS) 和参数 1 和 2(P1 和 P2) 构成。

[0008] 图 32 示出了 APDU 响应命令 3201，并且由数据部分和状态字 (SW) 构成。

[0009] 所述 IC 卡具有应用防火墙的特征。所述应用防火墙表示当多个应用共存在 IC 卡内时，一个应用不能调用不同应用的函数或者向不同的应用的对象进行数据访问，除非所述不同的应用明确地给出用于访问的接口。

[0010] 已知可共享的接口对象 (SIO) 为在应用之间的对象共享方法（参见专利文件 1）。

[0011] 以下，用于提供 SIO 的应用将被称为服务器应用，并且使用 SIO 的应用将被称为服务器应用。

[0012] 例如，提出了一种方法，其有效地用于通过下述方式来显示没有显示器的 IC 卡的使用结果：向移动电话内插入安装了两种应用的 IC 卡（芯片），通过进行在票据检查机器

和票据检查应用之间的非接触通信来通过票据检查，由在卡内的票据检查应用将结果传送到显示应用，并且通过由移动电话与显示应用进行接触通信而在移动电话的屏幕上显示结果。

[0013] 在这个示例内，票据检查应用作为客户机应用，并且所述显示应用作为服务器应用。

[0014] 专利文件 1 ：国际专利公开第 2003-522988 号

发明内容

[0015] 本发明要解决的问题

[0016] 为了使用诸如 IC 卡的设备来通过票据检查或者进入和离开检查，期望整个处理将在大约一到几秒内完成。因为 IC 卡的 CPU 处理能力与通用的 PC 或者移动机器相比较低，因此经常在下载时间执行链接，并且将中间值设置为地址引用对象 (referent)。在需要的时候调用存储器进行使用的技术（诸如动态链接库）不能用于 IC 卡应用，因为链接处理变为瓶颈。

[0017] 因此，对于许多 IC 卡，如果在其中未安装服务器应用的状态中下载客户机应用，则其导致作为链接错误的失败。

[0018] 因此，在已经存在的现有技术内，服务器应用和客户机应用必须存在于同一卡内。

[0019] 但是，可以从多个客户机应用使用一些服务器应用，并且在所有所拥有的卡中安装同一服务器应用，不能有效地使用 IC 卡的有限存储器中的大部分。

[0020] 本发明被实现来解决在相关技术中的问题，并且本发明的目的是提供一种方法，用于如果当下载客户机应用时在同一卡内不存在服务器应用，则许可下载，并且当所述客户机应用被执行时与在不同卡中安装的服务器应用相结合地工作（以下称为卡间接口使用）。

[0021] 解决所述问题的手段

[0022] 本发明是一种安全设备，其包括 ：应用存储部分，用于存储用于执行数据处理的应用的客户机应用 ；地址计算部分，用于确定所述应用存储部分是否具有用于向和从客户机应用传送数据的服务器应用 ；引用对象存在确定部分，用于当所述地址计算部分确定所述应用存储部分没有用于向和从第一客户机应用传送数据的第一服务器应用时，确定不同安全设备是否具有所述第一服务器应用 ；卡间接口执行部分，其访问所述不同安全设备，其中，所述引用对象存在确定部分根据所述卡间接口执行部分的结果确定所述不同安全设备是否具有所述第一服务器应用 ；授权码发出部分，当所述引用对象存在确定部分确定所述不同安全设备具有所述第一服务器应用时，该授权码发出部分发出用于许可引用所述第一服务器应用的授权码 ；以及应用执行部分，其根据所述授权码来执行所述第一客户机应用。

[0023] 因此，如果在家庭 (home) 安全设备中不存在服务器应用，则可以进行检查以查看是否可以按照不同的安全设备的服务器应用来执行家庭安全设备的客户机应用。

[0024] 本发明的优点

[0025] 本发明具有可以减少在安全设备中的存储区域的优点。

附图说明

[0026] 图 1 是本发明的实施例 1 中的系统配置的图。

[0027] 图 2 是实施例 1 中的安全设备的方框图。

[0028] 图 3 是示出在下载期间和下载后的应用区域的图。

[0029] 图 4 是实施例 1 中的不同安全设备的方框图。

[0030] 图 5 是实施例 1 中的读取器 - 写入器的方框图。

[0031] 图 6 是当在卡内存在引用对象时的处理的流程图。

[0032] 图 7 是当在卡内不存在引用对象时的处理的流程图。

[0033] 图 8 是用于示出在实施例 1 内的地址空间的图。

[0034] 图 9 是用于示出授权码表的示例的图。

[0035] 图 10 是被提供授权码的应用的处理的流程图。

[0036] 图 11a 是用于示出命令和响应的示例的图 (a)。

[0037] 图 11b 是用于示出命令和响应的示例的图 (b)。

[0038] 图 12 是本发明的实施例 2 中的安全设备的方框图。

[0039] 图 13 是实施例 2 中的不同安全设备的方框图。

[0040] 图 14 是示出向 / 从读取器 - 写入器的输入和输出之间的关系的图。

[0041] 图 15 是本发明的实施例 3 中的读取器 - 写入器的方框图。

[0042] 图 16 是实施例 3 中的处理的流程图。

[0043] 图 17 是本发明的实施例 4 中的读取器 - 写入器的方框图。

[0044] 图 18 是实施例 4 中的处理的流程图。

[0045] 图 19 是本发明的实施例 5 中的处理的流程图。

[0046] 图 20 是实施例 5 中的授权码表的示例。

[0047] 图 21 是实施例 5 中的发出授权码的流程图。

[0048] 图 22 是用于示出指令的示例的图。

[0049] 图 23 是用于示出临时授权码管理表的示例的图。

[0050] 图 24 是本发明的实施例 7 中的安全设备的方框图。

[0051] 图 25 是实施例 7 中的不同安全设备的方框图。

[0052] 图 26 是用于示出由应用执行部分处理的帧 (frame) 的示例的图。

[0053] 图 27 是用于示出由堆栈控制部分建立的数据的示例的图。

[0054] 图 28 是当在同一安全设备中存在引用对象应用时下载应用的流程图。

[0055] 图 29 是实施例 2 中提供安全的流程图。

[0056] 图 30 是关于 IC 卡的硬件的功能方框图。

[0057] 图 31 是 APDU 命令的格式图。

[0058] 图 32 是 APDU 响应的格式图。

[0059] 图 33a 是用于示出由读取器 - 写入器处理的数据类型定义的图 (1)。

[0060] 图 33b 是用于示出由读取器 - 写入器处理的数据类型定义的图 (2)。

[0061] 参考标号的描述

[0062] 101 安全设备

[0063] 102 不同安全设备

[0064] 103 读取器 - 写入器

[0065] 201 下载管理部分

[0066] 202 应用存储部分

[0067] 203 应用（正在被下载）

[0068] 204 不同应用（已经被下载）

[0069] 205 地址计算部分

[0070] 206 应用执行部分

[0071] 207 授权码发出部分

[0072] 208 卡间接口执行部分

[0073] 209 授权码管理部分

[0074] 210 引用对象存在确定部分

[0075] 301 正在被下载的应用

[0076] 302 应用代码数据区域

[0077] 303 应用计算数据区域

[0078] 304 应用数据区域

[0079] 305 应用代码数据

[0080] 306 应用计算数据

[0081] 307 下载后的应用

[0082] 308 应用代码

[0083] 309 下载数据

[0084] 401 服务器应用

[0085] 501 排他控制通信部分

[0086] 502 应用控制部分

[0087] 801 存储器空间

[0088] 802 对于应用许可的区域

[0089] 803 系统区域

[0090] 901 授权码表

[0091] 1101、1103、1105、1107 响应

[0092] 1102 选择命令

[0093] 1104、1108 共享命令

[0094] 1106 INVOKE（调用）命令

[0095] 1201 安全设备

[0096] 1202 安全性管理部分

[0097] 1301 安全设备

[0098] 1302 卡间接口执行部分

[0099] 1303 安全性管理部分

[0100] 1401 对读取器－写入器的输入（来自安全设备的响应）

[0101] 1402 来自读取器－写入器的输出（到不同安全设备的命令）

[0102] 1403 对读取器－写入器的输入（来自不同安全设备的响应）

[0103] 1404 来自读取器－写入器的输出（到安全设备的命令）

[0104] 1501 读取器－写入器

[0105] 1502 拥有者管理部分

[0106] 1701 读取器－写入器

[0107] 1702 拥有者检查信息输入部分

[0108] 1703 下载条件确定部分

[0109] 2001 授权码表

[0110] 2201 指令

[0111] 2301 临时授权码管理表

[0112] 2401 安全设备

[0113] 2402 客户机应用

[0114] 2403 堆栈操作部分

[0115] 2501 不同安全设备

[0116] 2502 堆栈控制部分

[0117] 2601 部分应用

[0118] 2602 帧 1

[0119] 2603 帧 2ROM

[0120] 2604 堆栈

[0121] 2605 局部变量

[0122] 2701 响应数据

[0123] 3001 IC 卡

[0124] 3002 CPU

[0125] 3003 ROM

[0126] 3004 RAM

[0127] 3005 EEPROM

[0128] 3006 输入／输出接口

[0129] 3101 APDU 命令

[0130] 3201 APDU 响应

[0131] 3301 由读取器－写入器处理的数据结构定义书

具体实施方式

[0132] 本发明涉及一种安全设备，用于如果当下载客户机应用时在同一卡中不存在服务器应用，则许可下载，并且当所述客户机应用被执行时与在不同卡中安装的服务器应用相结合地工作。

[0133] 实施例 1 是涉及安全设备的发明，所述安全设备用于如果当下载客户机应用时在同一卡中不存在服务器应用，则许可下载，并且当所述客户机应用被执行时与在不同卡中安装的服务器应用相结合地工作。

[0134] 实施例 2 是涉及一种系统的发明，所述系统用于当设备彼此相结合地工作时提供安全性。

[0135] 实施例 3 是涉及一种（第一）系统的发明，所述系统用于当一安全设备和一不同

的安全设备彼此相结合地工作时检查所述安全设备的拥有者和所述不同的安全设备的拥有者的相同性。

[0136] 实施例 4 是涉及一种（第二）系统的发明，所述系统用于当一安全设备和一不同的安全设备彼此相结合地工作时检查所述安全设备的拥有者和所述不同的安全设备的拥有者的相同性。

[0137] 实施例 5 是涉及与在其中安装了服务器应用的安全设备的生命周期相关联的客户机应用的使用控制方法的发明。

[0138] 实施例 6 是涉及当服务器应用不存在于同一卡中时的客户机应用的有条件下载方法和条件检查方法的发明。

[0139] 实施例 7 是涉及请求在不同的安全设备中安装的服务器应用执行处理并且在客户机应用中使用所述服务器应用的处理数据的方法的发明。

[0140] 将使用附图来讨论本发明的所述实施例。应当明白，本发明不限于下述的具体实施例，在不脱离本发明的精神和范围的情况下，可以以各种形式来体现本发明。

[0141] （实施例 1）

[0142] 在实施例 1 中描述的本发明提供了一种安全设备，用于如果当下载客户机应用时在同一卡中不存在服务器应用，许可下载，并且当所述客户机应用被执行时与在不同卡中安装的服务器应用相结合地工作。

[0143] 例如，下述情况是可能的：本发明被应用到安全设备，所述安全设备包含作为服务器应用的显示器应用，用于在移动电话的屏幕上显示客户机应用的处理结果；以及作为客户机应用的通信票据应用和预付应用。

[0144] 或者，本发明也可以被应用到下述示例，其中，在用于检查观看权限的服务器应用和用于存储观看权限和所观看内容的客户机应用之间的关系中，所述客户机应用向所述服务器应用传送观看权限，并且除非由所述服务器应用执行的、在所述观看权限内包含的年限 (age)、次数、过期日期、总的回放时间等的条件检查通过，否则不能观看所述内容。

[0145] 将使用图 1-11 和 28 来讨论所述实施例。

[0146] 图 1 是示出所述实施例中的安全设备和不同安全设备的结合系统的图，并且所述结合系统由安全设备 101、不同安全设备 102 和读取器 - 写入器 103 构成。

[0147] 图 2、4 和 5 分别是在图 1 内所示的安全设备 101、不同安全设备 102 和读取器 - 写入器 103 的方框图。

[0148] 图 2 是示出如上所述的安全设备 101 的配置的方框图。

[0149] 下载管理部分 201 与读取器 - 写入器 103 进行通信，并且管理用于向安全设备 101 下载应用的操作。

[0150] 应用存储部分 202 包含正在被下载的应用 203 和已经被下载的应用 204。

[0151] 图 3 示出了由在图 2 中的应用存储部分 202 中的应用占用的区域。

[0152] 由正在被下载的应用 301(203) 保留的区域是应用代码数据区域 302、地址计算数据区域 303 和应用数据区域 304。

[0153] 应用代码数据 305 被存储在应用代码数据区域 302 内，并且地址计算数据 306 被存储在地址计算数据区域 303 内。

[0154] 由下载后的应用 307 占用的区域是应用代码数据区域 302 和应用数据区域 304。

应用代码 308 被存储在应用代码数据区域 302 内，并且应用数据 309 被存储在应用数据区域 304 内。

[0155] 地址计算部分 205 使用在正在被下载的应用 203 中的应用代码数据 305 和应用计算数据 306 以及已经被下载的不同应用 204 来执行要被下载的应用 203 的“地址解析”。

[0156] 所述“地址解析”是指在函数调用或者对象访问时间引导数据的引用对象的地址的更新。

[0157] 在地址解析后，删除地址计算数据区域 303，并且在下载完成后，由应用代码 308 和应用数据 309 构成的应用 307 被存储在应用存储部分 202 中作为已经下载的应用。

[0158] 安全设备 101 的应用执行部分 206 按照来自读取器－写入器 103 的命令来执行已经下载的应用 307。

[0159] 例如，下述技术被广泛地知道：字节代码作为应用代码 308 被存储，并且对象作为应用数据 309 被存储在应用存储部分 202 中，并且作为应用执行部分 206 的虚拟机解释字节代码并执行处理。

[0160] 在包括实施例 1 的说明书中的实施例的说明中使用这样的处理系统。在由虚拟机管理的存储空间内的每个地址被表示为 16 比特（两个字节）。

[0161] 授权码发出部分 207 在地址解析期间从地址计算部分 205 接收到请求时发出“授权码”。下面说明“授权码”。

[0162] 此时，引用对象存在确定部分 210 检查是否“在不同安全设备中存在引用对象”。下面说明这个操作。

[0163] 卡间接口执行部分 208 在地址解析期间从引用对象存在确定部分 210 接收到请求时或者在应用 307 的执行时间从应用执行部分 206 接收到请求时，与不同安全设备 102 进行通信。

[0164] 图 4 是示出如上所述的不同安全设备 102 的配置的方框图。

[0165] 在不同安全设备 102 内，用于为不同应用 204 提供接口以明确地访问的应用（以下将称为服务器应用 401。另一方面，使用所述接口的应用以下将被称为客户机应用 307（在图 2 中为下载后的应用 307））被存储在应用存储部分 402 内，并且由应用执行部分 403 执行。

[0166] 图 5 是用于示出如上所述的读取器－写入器 103 的配置的方框图。

[0167] 读取器－写入器 103 可以与安全设备 101、不同安全设备 102 等多个安全设备通信，并且单独地识别安全设备 101 和不同安全设备 102 来进行通信。

[0168] 为了执行如上所述的操作，读取器－写入器 103 由下述部分构成：排他(exclusive)控制通信部分 501，用于防止要发送到安全设备 101 的数据被错误地发送到不同安全设备 102（并且反之亦然）；以及应用控制部分 502，用于向安全设备 101 中的应用 307 和不同安全设备中的服务器应用 401 发送命令，并且处理响应。

[0169] 例如，已知下述设备：一种读取器－写入器，其具有多个插槽，用于与插入到每个插槽中的安全设备接触，并且与所述安全设备通信；一种读取器－写入器，用于与在无线电波的到达范围内的多个安全设备进行非接触通信；等等。

[0170] 应用控制部分 502 可以是：1) 全部存在于读取器－写入器 103 中的情况，或者 2) 一部分存在于读取器－写入器 103 中并且剩余部分通过网络而存在于不同的设备中的情

况；两者在说明书中类似地被处理。

[0171] 在所述实施例中，将讨论在具有如上所述的部件的安全设备 101、不同安全设备 102 和读取器－写入器 103 之间的数据传送。

[0172] 在包含所述实施例的应用内，除非明确地另外说明，通常控制部分（未示出）执行数据传送等。

[0173] 在说明所述实施例的特征部分之前，首先将使用图 7 和 28 来说明当在同一安全设备中存在引用对象的应用时的应用下载。

[0174] 安全设备 101 中的下载管理部分 201 接收从读取器－写入器 103 发送的应用下载命令，并且将处理结果发送至读取器－写入器 103 作为响应。一般，通过重复操作来执行应用下载。

[0175] （步骤 1(S2801)）

[0176] 在安全设备 101 中，响应于在从读取器－写入器 103 发送的下载命令中指定的大小而保留应用代码数据区域 302、地址计算数据区域 303 和应用数据区域 304，并且从所述下载命令提取应用代码数据 305 和地址计算数据 306，并存储在相应的区域中。

[0177] （步骤 2(S2802)）

[0178] 在安全设备 101 中，在提取了应用代码数据 305 和地址计算数据 306 后，地址计算部分 205 在从下载管理部分 201 接收到请求时执行地址解析。

[0179] 地址计算部分 205 在应用代码数据 305 的顶部开始，以字节为单位进行解释。例如，当读取指令代码的“invokeinterface（调用接口）”以便经由由不同应用 204 提供的接口 (IF) 而调用函数时，地址计算部分 205 响应于“invokeinterface”而执行处理，如图 6 内所示。

[0180] “processing responsive（作出响应而处理）”表示定义了诸如“invokeinterface”的各种指令代码，并且处理在指令代码之间不同。

[0181] 紧随“invokeinterface”的一个字节控制要调用的自变量，随后的 2 个字节的“0002”是地址计算数据 306 的索引。地址计算部分 205 根据地址计算数据 306 的索引来引用对应的地址计算数据 306。

[0182] 图 6 中所示的引用对象“01800000”由包、类令牌 (class token)、方法标识号等构成，并且地址计算部分 205 使用它们来提取指示要调用的函数的顶部位置的地址，并且将索引“0002”转换为被调用的地址“a000”。

[0183] （步骤 3(S2803)）

[0184] 在安全设备 101 中，在解释了所有的应用代码数据 305 后，地址计算部分 205 向下载管理部分 201 发送地址计算完成的通知。

[0185] （步骤 4(S2804)）

[0186] 在安全设备 101 中，下载管理部分 201 释放存储变得不需要的地址计算数据的区域 303。但是，所述步骤可以是选用的，虽然考虑到卡的存储器资源，其是非常有效的。

[0187] （步骤 5(S2805)）

[0188] 当从读取器－写入器 103 接收到“应用初始化”请求命令时，下载管理部分 201 初始化应用。

[0189] “应用初始化”用于生成每个应用的实例，并且设置对象中的初始值。数据被存储

在应用数据区域 304 中作为应用数据 309。

[0190] 其后，使得有可能对于来自读取器－写入器 103 的命令，应用执行部分 206 选择和执行应用 307 或者 204。

[0191] 已经描述了当地址解析导致成功时的处理。

[0192] 接着，将使用图 7 来讨论因为要引用的应用不存在于卡内而不能执行地址解析的情况。

[0193] 在图 7 内，为了与如上所述的（步骤 2(S2802)）相同地执行不同应用的函数调用的地址解析，地址计算部分 205 识别在安全设备 101 中不存在引用对象。

[0194] 地址计算部分 205 请求引用对象存在确定部分 210 检查“在不同安全设备 102 中是否存在对应的引用对象”。

[0195] 此时，地址计算部分 205 向引用对象存在确定部分 210 传送存在检查信息，其包含引用对象应用的标识符应用标识数据 (AID)、方法 ID、自变量的数量等。

[0196] 从引用对象存在确定部分 210 向卡间接口执行部分 208 传递存在检查信息，卡间接口执行部分 208 然后通过读取器－写入器 103 向不同安全设备 102 传送所述存在检查信息。

[0197] 不同安全设备 102 检查由存在检查信息指示的函数存在，然后向安全设备 101 传送表示使用许可或者使用拒绝的许可检查信息。

[0198] 由安全设备 101 的卡间接口执行部分 208 接收的许可检查信息被传递到引用对象存在确定部分 210，并且如果作为引用对象存在确定部分 210 检查许可检查信息的结果而许可使用不同安全设备 102 的服务器应用 401，则请求授权码发出部分 207 发出授权码。如果所述使用被拒绝，则授权码发出部分 207 发出错误。

[0199] 如果发出错误，则通过下载管理部分 201 向读取器－写入器 103 返回 SW，其表示“因为不存在引用对象，因此下载产生错误”。

[0200] 授权码的长度是与地址相同的被必要地更新的长度；例如，如果以两个字节表示地址，则授权码也是两个字节。

[0201] 授权码由指示其中不许可应用布置的地址区域的信息和由授权码管理部分管理的表的索引构成。

[0202] 图 8 示出了安全设备 101 中的地址空间。

[0203] 当通过 0000h 到 EFFFh 来表示存储器空间 801 中的、对于应用布置所许可的存储器空间 802 时，对于所述应用不许可的区域（例如系统区域）803 是 F000h 到 FFFFh。

[0204] 例如，作为授权码，给出了 FF02h，其指示在对于应用 803 不许可的区域的范围内的表的索引“2”并通过后半部分的一个字节来指示。在这种情况下，在发出授权码后，引用对象应用的标识符（服务器应用 401）、方法 ID、自变量的数量等被存储在由授权码管理部分 209 管理的授权码表 901 的索引“2”的行中。

[0205] 接着，将使用图 10 和 11 来说明被提供授权码的应用（客户机应用 307）的执行操作。

[0206] 图 10 示出了操作流程，图 11 示出了在安全设备 101、不同安全设备 102 和读取器－写入器 103 之间传送的命令和响应的示例。

[0207] 将使用在图 10 中的操作流程来讨论安全设备 101、不同安全设备 102 和读取

器 - 写入器 103 的操作。

[0208] 图 33 示出了用于描述由读取器 - 写入器 103 处理的数据的结构的定义书 3301。定义书 3301 从在图 33a 内所示的数据行向在图 33b 的左边所示的数据行继续，并且进一步向在图的右边所示的数据行继续。在此，使用用于定义标准的语言的 ASN.1（抽象语法表示 1）进行说明。而且，在 C 语言内，具有 typedef 关键字的数据类型的定义也是可能的。

[0209] 在所述实施例中的定义书和实现方式之间的关系，即所定义的数据类型考虑什么命令 / 响应被加到定义书 3301 中的评述。在此，描述了 APDU 的发送和接收，但是可以执行基于 HTTP（超文本传送协议）的数据的发送和接收。

[0210] 因此，可以以各种形式来实现在读取器 - 写入器 103 内的数据类型定义和由在 IC 卡内安装的应用（客户机应用 307、服务器应用 401）和读取器 - 写入器 103 交换的数据的结构。以下，将跳过在实施例 2-7 内的类似说明。

[0211] （执行操作步骤 1(S1001)）

[0212] 假定安全设备 101 中的客户机应用 307 已经开始（未示出）。

[0213] 对应于从读取器 - 写入器 103 发送的命令 1 的处理由安全设备 101 的应用执行部分 206 执行。

[0214] 对于由客户机应用提供的每个功能，命令 1 可以以各种格式存在，诸如用于检查在视频内容观看时间的许可条件的请求。

[0215] 在读取表示方法调用的指令代码后，应用执行部分 206 取出紧随在所述指令代码之后的地址信息。

[0216] 应用执行部分 206 确定由地址信息指示的区域是否是“对于应用所许可的区域”，并且如果所述区域是许可的区域，则应用执行部分调用地址。

[0217] 如果所述区域不是许可的区域，则应用执行部分 206 识别授权码，并且将所述授权码传递到授权码管理部分 209，并且将在所述方法内使用的参数传递到卡间接口执行部分 208。

[0218] 授权码管理部分 209 读取在授权码内包含的索引，取出在授权码表 901 内包含的引用对象应用的 AID，并且将所述 AID 传递到卡间接口执行部分 208。

[0219] 卡间接口执行部分 208 在响应 1101 的数据部分设置引用对象应用的 AID，在响应 1101 的 SW 内设置表示用于使用卡间接口的请求的数据，并且向读取器 - 写入器 103 发送响应 1101。

[0220] （执行操作步骤 2(S1002)）

[0221] 当读取器 - 写入器 103 的排他控制通信部分 501 从安全设备 101 接收响应 1101 时，应用控制部分 502 分析所述响应，并且识别安全设备 101 想要使用卡间接口。

[0222] 应用控制部分 502 处理从安全设备 101 接收的数据（来自安全设备 101 的响应），将其作为命令传送到不同安全设备 102，处理从不同安全设备 102 接收的数据（来自不同安全设备 102 的响应），并且将其作为命令传送到安全设备 101，直到识别出从安全设备 101 接收的响应意味着卡间接口使用完成。

[0223] 如果读取器 - 写入器 103 首先从安全设备 101 接收到包含想要使用卡间接口的消息的响应，则读取器 - 写入器 103 将来自安全设备 101 的响应处理为在图 11 内所示的选择命令 1102，并且将所述命令发送到不同安全设备 102。

[0224] 在不同安全设备 102 的应用存储部分 402 中存储的服务器应用 401 按照选择命令 1102 而开始。

[0225] 在后面的说明内，将服务器应用 401 实现远程方法调用 (RMI) 的情况作为示例。

[0226] RMI 是在 Java（注册商标）卡 TM 中定义的技术，并且是用于在读取器 - 写入器中操作以调用卡的远程对象的方法的应用的机制。

[0227] 实现 RMI 的服务器应用 401 响应于来自读取器 - 写入器 103 的选择命令 1102 而向读取器 - 写入器 103 返回包含 INS 和对象 ID 的响应 1103。

[0228] （执行操作步骤 3(S1003)）

[0229] 读取器 - 写入器 103 在图 11(a) 中所示的共享命令 1104 中的数据部分中设置来自服务器应用 401 的响应 1103，并且向安全设备 101 的卡间接口执行部分 208 发送共享命令 1104。

[0230] 共享命令 1104 是专用于当安全设备 101 想要使用卡间接口时从读取器 - 写入器 103 向安全设备 101 发送的命令的命令；期望应当分配唯一的 INS。

[0231] 安全设备 101 的卡间接口执行部分 208 在图 11(b) 中所示的响应 1105 的数据部分中设置从服务器应用 401 传递的包含 INS 和对象 ID 的请求数据、在授权码表 901 中存储的方法 ID、和从安全设备 101 的应用执行部分 206 传递的参数，在响应 1105 的 SW 中设置用于使用卡间接口的请求，并且向读取器 - 写入器 103 返回响应 1105。

[0232] （执行操作步骤 4(S1104)）

[0233] 读取器 - 写入器 103 解释使用卡间接口的请求，并且向服务器应用 401 发送基于在响应 1105 的数据部分中存储的数据而建立的 INVOKE（调用）命令。

[0234] 服务器应用 401 使用所述方法 ID 和参数来执行处理，并且向读取器 - 写入器 103 返回响应 1107。

[0235] （执行操作步骤 5(S1005)）

[0236] 读取器 - 写入器 103 在图 11(b) 中所示的共享命令 1108 的数据部分中设置服务器应用的 INVOKE 命令处理结果（例如仅仅在响应 1107 中所示的 SW），并且向安全设备 101 的卡间接口执行部分 208 发送共享命令 1108。

[0237] 卡间接口执行部分 208 向应用执行部分 206 传递服务器应用的 INVOKE 命令处理结果。

[0238] 其后，应用执行部分 206 继续服务器应用的 INVOKE 命令处理结果的处理，并且向读取器 - 写入器 103 发送对于命令 1 的响应 1109。

[0239] 对于命令 1 的响应 1109 包含意味着成功的 9000h，并且不包含 SW，所述 SW 包含想要使用卡间接口的消息。

[0240] 因此，读取器 - 写入器 103 识别卡间接口使用完成的含义，并且停止在安全设备 101 和安全设备 102 之间的随后的传送。

[0241] 或者，可以从安全设备 101 发送明确地表示卡间接口使用完成的 SW。

[0242] 如上所述，所述实施例使得有可能不仅访问在安全设备中安装的服务器应用，而且访问在不同安全设备中安装的服务器应用。

[0243] 因此，不必为每个所拥有的安全设备安装普通用途的应用，并且这个益处对于缺少存储器资源的安全设备是有效的。

[0244] 即，产生了用户益处：可以在第二个卡和以后的卡中安装不同的应用代替服务器应用。

[0245] 而且，客户机应用的源代码在同一安全设备中安装的服务器应用的使用中和在不同安全设备中安装的服务器应用的使用中变得相同。

[0246] 因此，通常当用户的方便性改善并且使用场景被扩大时，在开发者身上的负担也趋向于扩大；另一方面，所述应用开发者可以如前开发，而不接收在系统内扩大用户使用场景的效果。

[0247] 已经开发的应用的下载和执行不受影响（保证反向兼容）。

[0248] 因此，有利于从先前的安全设备向在所述实施例中提出的安全设备的过渡。

[0249] （实施例 2）

[0250] 在本发明的实施例 2 内，将讨论当安全设备和不同安全设备彼此结合地工作时的安全性提供。

[0251] 将使用图 12-14 来说明实施例 2。

[0252] 图 12 是用于示出在所述实施例中的安全设备 1201 的配置的方框图。

[0253] 图 12 中的下载管理部分 201、应用存储部分 202、正在被下载的应用 203（下载后的客户机应用 307）、已经下载的应用 204、地址计算部分 205、应用执行部分 206、授权码发出部分 207、卡间接口执行部分 208、授权码管理部分 209 和引用对象存在确定部分 210 与图 2 中的那些类似。

[0254] 与图 2 中的安全设备 101 的那些相同的部件通过相同的附图标号来表示。

[0255] 下面给出详细说明，其集中于安全性管理部分 1202、在实施例 1 中描述的图 2 中的安全设备 101 和在实施例 2 中描述的图 12 中的安全设备 1201 之间的差别点：

[0256] 安全性管理部分 1202 在发出在实施例 1 中描述的授权码的阶段和在应用执行期间引用不同安全设备的阶段“提供安全”。

[0257] 表达“提供安全”用于表示用于认证通信方（不同安全设备）的所述设备（安全设备）的外部认证、用于认证所述设备的通信方的内部认证（以下所述外部认证和所述内部认证将被统称为相互认证）、所传送的数据的隐藏和篡改检测等的执行，并且使用加密技术来实现它们。

[0258] 在实施例中，在“有可能可以从未预先注册以使用服务器应用的不确定数量的客户机应用使用服务器应用”的前提下，使用公开密钥加密来讨论如上所述的“安全性提供”。

[0259] 公开密钥加密一般在处理速度上次于公共密钥加密。

[0260] 因此，进行外部认证和内部认证，并且使用公开密钥加密来共享会话密钥（或者会话密钥的种子），并且使用会话密钥按照公共密钥加密来执行通信数据的加密和解密以及篡改检测。

[0261] 为了向所述实施例应用如上所述的开放密钥和会话密钥加密技术，下面的三种“安全性提供”方法是可能的：

[0262] 方法 1：进行外部认证和内部认证，并且在发出授权码的阶段共享会话密钥，并且当在应用执行期间引用不同安全设备时，使用会话密钥。

[0263] 方法 2：进行外部认证和内部认证，并且在发出授权码的阶段共享会话密钥的种子，并且安全设备和不同安全设备在应用执行期间按照同一算法从会话密钥的种子建立会

话密钥，并且使用所述会话密钥。

[0264] 方法 3：进行外部认证和内部认证，并且在发出授权码的阶段和在应用执行期间引用不同安全设备的阶段共享会话密钥。

[0265] 所述方法在处理时间和所传送的数据上略为不同，但是在基本思想上是相同的。

[0266] 因此，在所述实施例中，将举例说明如上所述的三种方法的方法 1。

[0267] 图 13 是示出在所述实施例中的不同安全设备 1301 的配置的方框图。

[0268] 图 13 中的应用执行部分 206、应用存储部分 202 和服务器应用 401 与图 4 中的那些类似。

[0269] 所述不同安全设备与图 4 中的不同安全设备 102 的不同在于卡间接口执行部分 1302 和安全性管理部分 1303。

[0270] 卡间接口执行部分 1302 在通过安全设备 1301 发出授权码的阶段和在应用执行期间引用不同安全设备的阶段执行通信。

[0271] 安全性管理部分 1303 具有类似于安全性管理部分 1202 的功能的功能，并且提供安全。

[0272] 将说明具有如上所述的配置的安全设备 1201 和不同安全设备 1301 的操作。

[0273] 开始，将讨论发出授权码的阶段。

[0274] 为了像在实施例 1 中描述的（步骤 2）那样执行不同应用的函数调用的地址解析，安全设备 1201 的地址计算部分 205 识别在卡中不存在引用对象。

[0275] 接着，地址计算部分 205 请求引用对象存在确定部分 210 检查“在不同安全设备 102 中是否存在对应的引用对象”。

[0276] 在图 29 中示出了下面的操作流程：

[0277] （安全性提供步骤 1(S2901)）

[0278] 在从引用对象存在确定部分 210 接收到请求时，安全设备 1201 的卡间接口执行部分 208 获取安全性管理部分 1202 具有的安全设备 1201 的卡公开密钥证书 A 和由安全性管理部分 1202 生成的随机数 a。

[0279] 安全设备 1201 的卡间接口执行部分 208 向不同安全设备 1301 的卡间接口执行部分 1302 发送卡公开密钥证书 A 和随机数 a。

[0280] （安全性提供步骤 2(S2902)）

[0281] 不同安全设备 1301 的卡间接口执行部分 1302 向安全性管理部分 1303 传送卡公开密钥证书 A 和随机数 a，安全性管理部分 1303 然后执行证书验证，并且获取安全设备 1201 的卡 ID 和卡公开密钥 A。

[0282] 接着，不同安全设备 1301 的安全性管理部分 1303 生成随机数 b，并且按照卡秘密密钥 B 来加密所述随机数 a。

[0283] 随后，加密的随机数 a 和不同安全设备 1301 的卡公开密钥证书 B 被传送到卡间接口执行部分 1302。

[0284] 不同安全设备 1301 的卡间接口执行部分 1302 向卡间接口执行部分 208 发送随机数 b、加密的随机数 a 和不同安全设备 1301 的卡公开密钥证书 B。

[0285] （安全性提供步骤 3(S2903)）

[0286] 安全设备 1201 的卡间接口执行部分 208 向安全性管理部分 1202 传送随机数 b、加

密的随机数 a 和不同安全设备 1301 的卡公开密钥证书 B，安全性管理部分 1202 然后执行证书验证，并且获取不同安全设备 1301 的卡 ID 和卡公开密钥 B。

[0287] 接着，安全性管理部分 1202 按照所述卡公开密钥 B 来解密加密的随机数 a，并且检查所述随机数是否匹配所生成的随机数 a（外部认证完成）。

[0288] 随后，安全性管理部分 1202 按照卡密钥 A 来加密随机数 b，并且将其传送到卡间接口执行部分 208。

[0289] 卡间接口执行部分 208 向不同安全设备 1301 的卡间接口执行部分 1302 发送加密的随机数 b。

[0290] （安全性提供步骤 4(S2904)）

[0291] 不同安全设备 1301 的卡间接口执行部分 1302 向安全性管理部分 1303 传送加密的随机数 b，安全性管理部分 1303 然后按照卡密钥 B 来解密加密的随机数 b，并且检查所述随机数是否匹配所生成的随机数 b（内部认证完成）。

[0292] （安全性提供步骤 5(S2905)）

[0293] 接着，不同安全设备 1301 的安全性管理部分 1303 建立会话密钥，按照卡公开密钥 A 来加密会话密钥，并且向卡间接口执行部分 1302 传送加密的会话密钥。

[0294] 卡间接口执行部分 1302 向安全设备 1201 的卡间接口执行部分 208 发送加密的会话密钥。

[0295] 卡间接口执行部分 208 向安全性管理部分 1202 传送加密的会话密钥，安全性管理部分 1202 然后按照所述卡密钥 A 来解密加密的会话密钥，并且获取会话密钥（共享会话密钥完成）。

[0296] 在这个阶段，在通过在如上所述的步骤中的交换和产生而新保留的数据中，安全性管理部分 1202 至少需要保留会话密钥，并且安全性管理部分 1303 至少需要保留安全设备 1201 的卡 ID 和会话密钥。

[0297] 在完成如上所述的安全性提供步骤 5 后，从引用对象存在确定部分 210 向安全设备 1201 的卡间接口执行部分 208 传送存在检查信息，其包含引用对象应用的标识符、方法 ID、自变量的数量等，安全设备 1201 然后通过读取器－写入器 103 向不同安全设备 1301 传送所述存在检查信息。

[0298] 此时，安全设备 1201 的安全性管理部分 1202 使用会话密钥来加密所述发送数据，并且给出篡改检测数据。

[0299] 不同安全设备 1301 检查在存在检查信息内指示的函数存在，然后向安全设备 1201 传送用于表示使用许可的信息。

[0300] 而且，在这种情况下，不同安全设备 1301 的安全性管理部分 1303 使用会话密钥来加密发送数据，并且给出篡改检测数据。

[0301] 由安全设备 1201 的卡间接口执行部分 208 接收的信息在安全性管理部分 1202 中经历使用会话密钥的解密和篡改检查，然后被传送到引用对象存在确定部分 210。

[0302] 如果许可使用，则引用对象存在确定部分 210 请求授权码发出部分 207 发出授权码。

[0303] 如果拒绝使用，则发出错误，并且通过下载管理部分 201 向读取器－写入器 103 返回 SW，该 SW 表示“因为不存在引用对象，所以下载导致失败”。

[0304] 接着，将说明被提供授权码的客户机应用的执行。基本上，其类似于实施例 1，并且其间的差别如下：

[0305] 首先，使用由安全性管理部分 1202 和 1303 管理的会话密钥来加密来自安全设备 1201 和不同安全设备 1301 的响应。

[0306] 其次，加密来自安全设备 1201 和不同安全设备 1301 的响应，因此，读取器 - 写入器 103 不可能解释、提取必要的数据、以及建立命令。

[0307] 因此，读取器 - 写入器 103 需要从所述响应的数据部分提取必要的数据，在命令中建立数据，并且向安全设备 1201 和不同安全设备 1301 发送所述命令。

[0308] 接着，将使用图 10 来说明在通过安全设备 1201、不同安全设备 1301 和读取器 - 写入器 103 的客户机应用执行期间的操作流程。

[0309] 在下面的说明中，假定图 10 中的安全设备 101 被原样应用为安全设备 1201，并且不同安全设备 102 被原样应用为不同安全设备 1301。

[0310] 还假定安全设备 1201 中的客户机应用 307 已经开始。

[0311] （执行操作步骤 1(S1001)）

[0312] 通过安全设备 1201 的应用执行部分 206 来执行对应于从读取器 - 写入器 103 发送的命令 1 的处理，

[0313] 在读取表示方法调用的指令代码后，应用执行部分 206 取出紧随所述指令代码的地址信息。

[0314] 确定所述地址信息是否是对于应用所许可的区域，并且，如果所述区域是许可的区域，则调用所述地址。

[0315] 如果所述区域“不”是许可区域，则识别授权码，并且将授权码传送到授权码管理部分 209。

[0316] 授权码管理部分 209 读取在授权码中包含的索引，取出在表格 901 中包含的引用对象应用的 AID，并且将所述引用对象应用的 AID 传送到卡间接口执行部分 208。

[0317] 卡间接口执行部分 208 在响应的数据部分中设置引用对象应用的 AID，在响应的 SW 中设置表示使用卡间接口的请求的数据，并且向读取器 - 写入器 103 发送所述响应。

[0318] （执行操作步骤 2(S1002)）

[0319] 当读取器 - 写入器 103 的排他控制通信部分 501 接收到所述响应时，应用控制部分 502 分析所述响应，并且识别安全设备 1201 想要使用卡间接口。

[0320] 应用控制部分 502 处理从安全设备 1201 接收的数据（来自安全设备 1201 的响应），将其作为对于不同安全设备 1301 的命令传送到不同安全设备 1301，处理从不同安全设备 1301 接收的数据（来自不同安全设备 1301 的响应），并且将其作为对于安全设备 1201 的命令传送到安全设备 1201，直到识别出从安全设备 1201 接收的数据表示卡间接口使用完成。

[0321] 如果读取器 - 写入器 103 首先从安全设备 1201 接收到包含想要使用卡间接口的消息的响应，则读取器 - 写入器 103 将所述响应处理为选择命令，并且向不同安全设备 1301 发送该命令。

[0322] 不同安全设备 1301 的服务器应用 401 按照选择命令而启动。

[0323] 在随后的说明内，将服务器应用 401 实现远程方法调用 (RMI) 的情况作为示例。

[0324] 实现 RMI 的服务器应用 401 向读取器 - 写入器 103 返回包含 INS 和对象 ID 的响应，作为对于选择命令的响应。

[0325] （执行操作步骤 3(S1003)）

[0326] 读取器 - 写入器 103 在共享命令的数据部分中设置来自服务器应用 401 的响应，并且向安全设备 1201 的卡间接口执行部分 208 发送所述共享命令。

[0327] 卡间接口执行部分 208 保存从服务器应用 401 传送的 INS 和对象 ID。

[0328] 虽然在附图中未示出保留 INS 和对象 ID 的方法，但是可以在安全设备 1201 内提供存储器来用于保留它们。

[0329] 其后，在安全性管理部分 1202 和 1303 中使用会话密钥来加密来自安全设备 1201 和不同安全设备 1301 的响应。

[0330] 在安全性管理部分 1202 和 1303 中使用会话密钥来解密从相关方接收的数据，然后，在卡间接口执行部分 208 和 1302 中执行处理。

[0331] 图 14 示出了在向读取器 - 写入器 103 的输入和来自读取器 - 写入器的输出之间的关系。

[0332] 读取器 - 写入器 103 向不同安全设备 1301 发送来自安全设备 1201 的响应 1401 的数据部分作为命令 1402。

[0333] 在命令 1404 的数据部分中设置来自不同安全设备 1301 的响应 1403，并且添加用于共享命令的首标以便发送到安全设备 1201。

[0334] 安全设备 1201 的卡间接口执行部分 208 在响应的数据部分中设置请求数据，该请求数据包含从不同安全设备 1301 的服务器应用 401 传送的 INS 和对象 ID、由安全设备 1201 的应用执行部分 206 指定的方法 ID、和从应用执行部分传送的参数，并且安全设备 1201 的卡间接口执行部分 208 在 SW 中设置用于使用卡间接口的请求，并向读取器 - 写入器 103 返回。

[0335] （执行操作步骤 4(S1004)）

[0336] 读取器 - 写入器 103 解释来自安全设备 1201 的用于使用卡间接口的请求，提取在响应（已经加密的 INVOKE 命令）的数据部分内存储的数据，并且将所述数据发送到不同安全设备 1301 的服务器应用 401 作为命令。

[0337] 服务器应用 401 使用方法 ID 和在 INVOKE 命令中指定的参数来执行处理，并且向读取器 - 写入器 103 返回处理结果。

[0338] （执行操作步骤 5(S1005)）

[0339] 读取器 - 写入器 103 向安全设备 1201 的卡间接口执行部分 208 发送在数据部分中设置的具有处理结果的共享命令。

[0340] 卡间接口执行部分 208 向应用执行部分 206 传送所述结果。

[0341] 其后，应用执行部分 206 继续所述结果的处理，并且向读取器 - 写入器 103 发送对于命令 1 的响应。

[0342] 对于命令 1 的响应一般不包含 SW，所述 SW 包含想要使用卡间接口的消息。

[0343] 因此，读取器 - 写入器 103 识别卡间接口使用完成的含义，并且停止在安全设备 1201 和不同安全设备 1301 之间的随后的传送。

[0344] 或者，可以从安全设备 1201 发送明确地表示卡间接口使用完成的 SW。

[0345] 在实施例 2 内，已经说明了用于在由安全性管理部分 1202 和 1303 的应用执行期间在不同安全设备的引用对象和引用的存在检查中提供安全的系统。

[0346] 如上所述的配置使得有可能防止安全设备的欺骗，防止窃听在安全设备之间交换的数据，并且检测数据的篡改。

[0347] （实施例 3）

[0348] 在本发明的实施例 3 内，将说明用于检查安全设备的拥有者和不同安全设备的拥有者匹配的（第一）系统。

[0349] 将使用图 12、13、15 和 16 来说明实施例 3。

[0350] 图 12 是用于示出所述实施例中的安全设备 1201 的配置的方框图，并且类似于在实施例 2 中所描述的。

[0351] 图 13 是示出所述实施例中的不同安全设备 1301 的配置的方框图，并且类似于在实施例 2 中所描述的。

[0352] 图 15 是示出所述实施例中的读取器 - 写入器 1501 的配置的方框图。

[0353] 图 15 中的排他控制部分 501 和应用控制部分 502 类似于图 5 中的排他控制部分 501 和应用控制部分 502。

[0354] 所述实施例的特征在于读取器 - 写入器，并且与如上所述的实施例 1 和实施例 2 的不同在其具有拥有者管理部分 1502 和下载条件确定部分 1503。

[0355] 拥有者管理部分 1502 管理安全设备 1201 的拥有者和在安全设备 1201 内设置的卡 ID。

[0356] 下载条件确定部分 1503 管理定义下载客户机应用的条件的下载条件信息。

[0357] 如果用户想要下载客户机应用，则读取器 - 写入器 1501 将对应的下载条件信息传送到应用控制部分 502，其然后执行处理来检查是否满足所述下载条件。

[0358] 在所述实施例中，下面将说明由安全设备 1201、不同安全设备 1301 和读取器 - 写入器 1501 构成的系统。

[0359] 在如上所述的实施例 1 和 2 内，当客户机应用执行地址解析时，如果服务器应用不存在于同一安全设备中，说明了使用在不同安全设备中存在的服务器应用的方法。

[0360] 在此，不考虑使用客户机应用来享受服务的“客户机应用拥有者（＝安全设备的拥有者）”和使用服务器应用来享受服务的“服务器应用拥有者（＝不同安全设备的拥有者）”等的相同性。

[0361] 在所述实施例中，如果需要客户机应用拥有者和服务器应用拥有者的某种关系，则说明一种检查和保证所需要的关系的方法。

[0362] 例如，假设服务器应用是信用应用，并且客户机应用是内容购买应用。

[0363] 在这种情况下，信用卡交易需要正确地了解“谁花了多少钱购买了什么内容”，因此会出现下述情况，其中，期望客户机应用的拥有者和服务器应用的拥有者应当是同一人。

[0364] 在所述实施例中，假定这样的情况，并且将说明当客户机应用执行地址解析时检查服务器应用拥有者和客户机应用拥有者的相同性的方法。

[0365] 下面两种模式被当作用于保证服务器应用拥有者和客户机应用拥有者的相同性的方法：

[0366] (1) 在读取器 - 写入器中检查相同性，然后，在安全设备中下载客户机应用。

[0367] (2) 在下载阶段对于每个安全设备执行个人认证（例如：PIN 检查），由此检查相同性。

[0368] 在实施例 3 中，将说明如上所述的 (1)。

[0369] 在实施例 4 中将说明如上所述的 (2)。

[0370] 为了描述如上所述的 (1)，以下是前提：（图 16 中的“开始”）

[0371] 读取器 - 写入器 1501 处于其可以与已经被下载了服务器应用的不同安全设备 1301 和已经被下载了客户机应用的安全设备 1201 通信的状态。

[0372] 下载客户机应用的条件被定义为“可以引用不同安全设备，在这种情况下，服务器应用拥有者和客户机应用拥有者是相同的”。

[0373] 读取器 - 写入器 1501 已经掌握了在安全设备 1201 中不存在服务器应用。

[0374] 可以使用一般的技术来实现所述前提，并且在附图内未示出所述前提。将使用图 16 的流程图来说明涉及如上所述的 (1) 的系统的操作。

[0375] 开始，如图 16 内所示，读取器 - 写入器 1501 向不同安全设备 1301 发送 SELECT（选择）命令，并且检查在不同安全设备中是否存在服务器应用。

[0376] 接着，按照 GETDATA 命令来获取被提供到不同安全设备 1301 的卡 ID。

[0377] 所述“卡 ID”是用于唯一地识别安全设备的信息；例如，其由对于卡发行者唯一的发行者标识号和用于唯一地识别由所述卡发行者发行的卡的卡标识号构成。

[0378] 同样，读取器 - 写入器 1501 也从安全设备 1201 获取卡 ID。

[0379] 读取器 - 写入器 1501 的应用到部分 502 请求拥有者管理部分 1502 检查按照如上所述获取的安全设备 1201 和不同安全设备 1301 的卡 ID 而相关联的安全设备的拥有者匹配。

[0380] 作为拥有者管理部分 1502 关于安全设备 1201 的拥有者和不同安全设备 1301 的拥有者是否匹配的确定的结果，如果两个安全设备的拥有者匹配，则读取器 - 写入器 1501 开始下载客户机应用。

[0381] 在此，读取器 - 写入器 1501 需要至少在安全设备 1201 的地址计算部分 205 执行地址解析之前向安全设备 1201 发送不同安全设备 1301 的卡 ID。

[0382] 安全设备 1201 在授权码管理部分 209 中存储所述卡 ID。

[0383] 当安全设备 1201 执行地址解析时，其识别服务器应用不存在于家用安全设备的安全设备 1201 中，并且检查服务器应用是否存在于不同安全设备 1301 内。

[0384] 在此，以类似的方式来执行在实施例 2 中所述的安全性提供步骤 1-5。

[0385] 但是，在所述步骤的执行期间，必须检查从不同安全设备 1301 的卡公开密钥证书获取的卡 ID 和在授权码管理部分 209 中存储的卡 ID 是否匹配。

[0386] 也可以跳过这一点，因为已经在读取器 - 写入器 1501 中检查了卡 ID 和拥有者的匹配。

[0387] 但是，除了在发送卡 ID 后针对用假的安全设备替换不同安全设备 1301 的威胁的先前检查之外，通过在地址解析期间再一次检查，安全级别改善。

[0388] 在实施例 3 中，已经说明了如果服务器应用和客户机应用被安装在不同安全设备，保证服务器应用拥有者和客户机应用拥有者的相同性的方法。

[0389] 检查所述相同性，由此，可以防止通过欺骗的客户机应用的下载。

[0390] 所述技术不仅可以应用于检查拥有者的相同性，而且可以应用于检查客户机应用拥有者是否是服务器应用拥有者的家人，属于同一组，等等。

[0391] 如上所述，可以提供能够灵活地设置和检查在服务器应用拥有者和客户机应用拥有者之间的关系的系统。

[0392] （实施例 4）

[0393] 在本发明的实施例 4 中，将说明用于检查安全设备的拥有者和不同安全设备的拥有者匹配的（第二）系统。

[0394] 将使用图 12、13、17 和 18 来说明实施例 4。

[0395] 图 12 是示出所述实施例中的安全设备 1201 的配置的方框图，并且类似于在实施例 2 中所描述的。

[0396] 图 13 是示出所述实施例中的不同安全设备 1301 的配置的方框图，并且类似于在实施例 2 中所描述的。

[0397] 图 17 是用于示出所述实施例中的读取器 - 写入器 1701 的配置的方框图。

[0398] 图 17 中的排他控制部分 501 和应用控制部分 502 类似于图 5 中的排他控制部分 501 和应用控制部分 502。

[0399] 拥有者管理部分 1502 类似于图 15 中的拥有者管理部分 1502。

[0400] 所述实施例与实施例 3 的不同在其具有拥有者信息检查输入部分 1702。

[0401] 提供拥有者信息检查输入部分 1702，以输入信息从而确定安全设备拥有者的合法性（示例 :PIN）。

[0402] 输入屏幕有可能作为拥有者信息检查输入部分 1702 的示例。

[0403] 但是，仅仅当应用控制部分 502 在从安全设备 1201 返回响应后将所述响应解释为用于提供 PIN 输入屏幕的请求并且请求拥有者信息检查输入部分 1702 输出屏幕时，显示所述屏幕。

[0404] 在所述实施例中，下面将说明由安全设备 1201、不同安全设备 1301 和读取器 - 写入器 1501 构成的系统。

[0405] 在实施例 1 和 2 内，当安全设备中的客户机应用执行地址解析时，如果服务器应用不存在于家用安全设备中，说明了使用在不同安全设备中存在的服务器应用的系统。

[0406] 在此，不考虑使用客户机应用来享受服务的“客户机应用拥有者（＝安全设备的拥有者）”和使用服务器应用来享受服务的“服务器应用拥有者（＝不同安全设备的拥有者）”等的相同性。

[0407] 在所述实施例中，如果需要客户机应用拥有者和服务器应用拥有者的某种关系，则像如上所述的实施例 3 中那样，说明用于检查和保证所需要的关系的方法。

[0408] 例如，假定服务器应用是信用应用，并且客户机应用是内容购买应用。在这种情况下，信用卡交易需要正确地了解“谁花了多少钱购买了什么内容”，因此会出现其中期望客户机应用的拥有者和服务器应用的拥有者应当是同一人的情况。

[0409] 因此，假定这样的情况，并且在所述实施例中，将使用图 18 说明当客户机应用执行地址解析时检查服务器应用拥有者和客户机应用拥有者的相同性的方法。

[0410] 为了描述在所述实施例中描述的发明，首先，说明前提。（图 18 中的“开始”）

[0411] 读取器 - 写入器处于其可以与已经被下载了服务器应用的不同安全设备和要被

下载了客户机应用的安全设备通信的状态。

[0412] 下载客户机应用的条件被定义为“可以引用不同安全设备，在这种情况下，服务器应用拥有者和客户机应用拥有者是相同的”。

[0413] 读取器－写入器已经掌握了在安全设备中不存在服务器应用。

[0414] 可以使用一般的技术来实现所述前提，并且在附图中未示出所述前提。

[0415] 将使用图 18 的流程图来说明涉及在实施例中描述的发明的系统的操作。

[0416] 开始，读取器－写入器 1701 向安全设备 1201 发送下载条件。

[0417] 下载管理部分 1201 接收所述下载条件，并且将其传送到安全性管理部分 1202，该安全管理器部分随后存储所述下载条件。

[0418] 接着，开始客户机应用下载。

[0419] 当安全设备 1201 执行地址解析时，其识别服务器应用不存在于家用安全设备的安全设备 1201 内，并且检查服务器应用是否存在于不同安全设备 1301 内。

[0420] 在此，以类似的方式来执行在实施例 2 中描述的安全性提供步骤 1-5。

[0421] 但是，在所述步骤的执行期间，安全设备 1201 的卡间接口执行部分 208 与读取器－写入器 1701 相结合地执行处理，以检查是否满足了在安全性管理部分 1202 中存储的下载条件。

[0422] 卡间接口执行部分 208 可以响应于所述下载条件而切换用于检查是否满足所述条件的处理。

[0423] 如果在所述实施例中下载条件是“可以引用不同安全设备，在这种情况下，所述服务器应用拥有者和所述客户机应用拥有者是相同的”，则向读取器－写入器 1701 发送作为输入 PIN 的请求的响应。

[0424] 读取器－写入器 1701 在排他控制部分 501 中接收所述响应，并且向应用控制部分 502 传送所述响应。

[0425] 应用控制部分 502 将所述响应解释为输入 PIN 的请求，并且请求拥有者信息检查输入部分 1702 显示屏幕。

[0426] 接着，拥有者在由拥有者信息检查输入部分 1702 显示的屏幕中输入 PIN。

[0427] 所输入的 PIN 被从排他控制部分 501 发送到不同安全设备 1301，并且被卡间接口执行部分 1302 接收。

[0428] 在从卡间接口执行部分 1302 接收到请求时，安全性管理部分 1303 执行 PIC 检查，并且经由读取器－写入器 1701 将结果发送至安全设备 1201。

[0429] 不必在安全性管理部分 1303 内执行 PIN 检查；例如，可以提供诸如 PIN 检查部分的部件。

[0430] 如果结果是“良好”，则安全设备 1201 的卡间接口执行部分 208 确定不同安全设备的拥有者与要被下载应用的安全设备的拥有者是相同的，并且继续地址解析。

[0431] 即使不同安全设备的拥有者与安全设备的拥有者不同，仍然存在不同安全设备的 PIN 检查产生良好的可能，因为所述安全设备的拥有者彼此相结合地工作。

[0432] 然后，在完成下载后，从安全设备向读取器－写入器发送不同安全设备的卡证书，所述读取器－写入器然后检查拥有者的相同性。结果，可以检测欺骗。

[0433] 如上所述，在实施例 4 内，已经说明了如果服务器应用和客户机应用被安装在不

同安全设备中时保证服务器应用拥有者和客户机应用拥有者的相同性的方法。

[0434] 特别是当在与拥有者信息数据库分离的环境中执行下载时，所述技术是最佳的。

[0435] （实施例 5）

[0436] 本发明的实施例 5 涉及与其中安装了服务器应用的安全设备的生命周期相关联的客户机应用的使用控制。

[0437] 将使用图 2、4、5、19 和 20 来说明实施例 5。

[0438] 图 2 是示出所述实施例中的安全设备 101 的配置的方框图，并且，部件类似于实施例 1 中所述的那些。

[0439] 图 4 是示出所述实施例中的不同安全设备 102 的配置的方框图，并且，部件与实施例 1 中所述的那些类似。

[0440] 图 5 是示出所述实施例中的读取器－写入器 103 的配置的方框图，并且，部件类似于实施例 1 中所述的那些。

[0441] 图 20 是在授权码管理部分 209 中包含的授权码表 2001，并且除了在图 9 中的索引、引用对象应用的标识符、方法 ID 和自变量的数量之外，还包含客户机应用的标识符。

[0442] 所述实施例与本发明的其他实施例的不同在于包含客户机应用的标识符。

[0443] 在所述实施例中，下面将说明由安全设备 101、不同安全设备 102 和读取器－写入器 103 构成的系统。

[0444] 如果服务器应用和客户机应用安装在同一安全设备中，则两个应用的生命周期与安全设备的生命周期相关联。

[0445] 即，如果安全设备是可用的，则两个应用是可用的；如果安全设备处于暂停或者放弃状态，则两个应用也变得不可用。

[0446] 在如上所述的实施例中服务器应用和客户机应用被安装在分离的安全设备中的情况下，当安全设备处于暂停或者放弃状态时，将说明系统如何工作。

[0447] 如果其中安装了服务器应用的不同安全设备（以下称为服务器设备）是可用的并且其中安装了客户机应用的读取器－写入器（以下称为客户机设备）是不可用的，则不产生问题，因为不能执行客户侧。

[0448] 另一方面，如果服务器设备是不可用的并且客户机设备是可用的，则需要与先前的处理不同的处理。

[0449] 即，需要向读取器－写入器返回“客户机应用不能使用，因为服务器设备暂停”的说明。

[0450] 期望应当尽早地进行所述返回。

[0451] 因此，在所述实施例中，将使用图 19 来说明当执行引用在不同安全设备中注册的服务器应用的客户机应用时检查不同安全设备的生命周期的处理。

[0452] 读取器－写入器 103 向安全设备 101 发送用于选择客户机应用的 SELECT 命令。

[0453] 安全设备 101 的应用执行部分 206 接收所述 SELECT 命令，并且将在数据部分中设置的客户机应用的 AID 传送到卡间接口执行部分 208。

[0454] 卡间接口执行部分 208 引用在授权码管理部分 209 中存储的授权码表 2001。

[0455] 如果在授权码表 2001 中不存在对应的客户机应用的 AID，则向应用执行部分 206 发送用于指示所述事实的通知，应用执行部分 206 然后执行通常的 SELECT 命令处理。

[0456] 如果对应的客户机应用的AID存在，则从授权码表2001提取在不同安全设备中安装的服务器应用的AID，并且向读取器－写入器103返回由服务器应用的AID和作为“用于向不同安全设备发送SELECT命令的请求”的数据构成的响应。

[0457] 读取器－写入器103根据从安全设备101的卡间接口执行部分208接收的数据建立SELECT命令，并且向不同安全设备102发送所述SELECT命令。

[0458] 接着，向安全设备101传送来自不同安全设备102的响应。

[0459] 安全设备101的卡间接口执行部分208分析所述响应，并且掌握不同安全设备102的可使用状态。

[0460] 如果不同安全设备102可用，则向卡间接口执行部分208发送用于指示所述事实的消息，卡间接口执行部分208然后执行通常的SELECT命令处理。

[0461] 如果不同安全设备102不可用，则向卡间接口执行部分208发送用于指示所述事实的消息，卡间接口执行部分208然后向读取器－写入器103返回设置了SW的响应，所述SW指示“客户机应用不能使用，因为不同安全设备不可用”。

[0462] 在实施例5内，已经说明了当安装了服务器应用的安全设备处于暂停或者放弃状态时、安装了客户机应用的安全设备的行为，其中，如果服务器应用和客户机应用安装在不同安全设备中，则会发生所述暂停或者放弃状态。

[0463] 在客户机应用的选择时间检查服务器应用的状态，从而与在客户机应用的处理执行期间检查服务器应用的状态的情况相比较，可以消除诸如在卡和读取器－写入器中的恢复处理的额外处理。

[0464] 也可以执行切换，以便仅仅在其中不使用服务器应用的功能的范围内执行客户机应用。

[0465] 如上所述，与其中服务器应用和客户机应用可用或者不可用的现有技术相反，使得在用于执行客户机应用的服务器内的服务器中有可能响应于应用的状态而选择处理，并且可以实现灵活的服务提供。

[0466] （实施例6）

[0467] 实施例6涉及当服务器应用不存在于同一卡中时客户机应用的有条件下载方法和条件检查方法的发明。

[0468] 例如，所述实施例可以被应用到下述系统：假如用户忘记携带安装了服务器应用的安全设备，如果在实际使用客户机应用之前引用了服务器应用，则所述系统许可客户机应用的下载。

[0469] 将使用图2、4、5、9、10、21、22和23来说明实施例6。

[0470] 图2是示出所述实施例中的安全设备101的配置的方框图，并且，部件类似于在实施例1中所述的那些。

[0471] 图4是示出所述实施例中的不同安全设备102的配置的方框图，并且，部件类似于在实施例1中所述的那些。

[0472] 图5是示出所述实施例中的读取器－写入器103的配置的方框图，并且，部件类似于在实施例1内所述的那些。

[0473] 图9示出了授权码表901的示例，并且，部件类似于在实施例1内所述的那些。

[0474] 所述实施例其特征在于图22、图23中所示的授权码、临时授权码等。

[0475] 图 22 是定义授权码发出部分 207 发出授权码的规则的指令。

[0476] 图 23 示出了由应用执行部分 206 管理的临时授权码管理表 2301 的示例。临时授权码管理表 2301 由索引、客户机应用的标识符、服务器应用的标识符和地址计算数据构成。

[0477] 在所述实施例中，下面将说明由安全设备 101、不同安全设备 102 和读取器 - 写入器 103 构成的系统。

[0478] 在实施例 1 中，描述了如果可以在使用服务器应用的接口下载客户机应用中引用在不同安全设备中安装的服务器应用，则发出授权码的方法。

[0479] 相反，在所述实施例中，将使用图 21 来说明各种授权码的发出和建立大多数所发出的授权码的方法。

[0480] 预先，按照用于设置从读取器 - 写入器 103 发送的应用的属性的命令来在授权码发出部分 207 中设置“应用类型”和“临时授权码发出许可”等。

[0481] “应用类型”是按照各种限制的应用的分类，诸如 :临时应用，其使用次数、使用时段等受限 ;或者，正式应用，其上未施加任何限制。

[0482] 因此，“应用类型”用于确定在应用上施加了什么限制。

[0483] “临时授权码发出许可”是虽然当引用对象存在确定部分 210 在地址解析时间检查对于服务器应用的引用时没有引用对象，但是不处理为下载错误，而是发出临时授权码的许可，并且，应用执行部分 206 必须在临时授权码的解释内“能够确定所述状态是其中还没有检查引用对象的状态”和“能够确定将许可所述状态多长时间”。

[0484] 例如，假定一种场景，其中，如果用户不具有安装了服务器应用的安全设备（例如忘记携带等），则临时下载客户机应用，然后，检查安装了服务器应用的安全设备，并且发出授权码。

[0485] 在所述实施例中，将说明在所假定的情况下的系统的操作。

[0486] 在图 21 中，直到“发出授权码”的流程类似于实施例 1 中的流程，并且在所述实施例中描述的发明的特征在于后面的处理。

[0487] （受限授权码的发出）

[0488] 将说明受限授权码的发出。

[0489] 预先，按照从读取器 - 写入器 103 发送的用于设置应用的属性的命令在引用对象存在确定部分 201 中设置“应用类型”。

[0490] 在此，假定所述应用被设置为临时应用，并且使用次数的上限为 3 次。

[0491] 直到在应用下载时开始地址解析、并且不同安全设备 102 向安全设备 101 传送表示使用许可的信息的流程与实施例 1 中的类似。

[0492] 引用对象存在确定部分 210 确定“良好”作为由卡间接口执行部分 208 分析所接收的信息的结果，然后请求授权码发出部分 207 发出使用所述“应用类型”的受限授权码。

[0493] 因为应用类型是临时应用并且使用次数是 3，因此，授权码发出部分 207 按照指令 2201 发出 FCB1h 作为受限授权码。

[0494] 按照指令 2201，用于指示其中不许可应用的布置的地址区域的信息的 FC-FDh 被分配给最上面的一种类型，随后的四个比特表示限制的类型和说明，并且最后四个比特给出了授权码表 901 的索引。

[0495] 在发出受限授权码后，在由授权码管理部分 209 管理的授权码表 901 内存储引用对象应用（服务器应用）的标识符、方法 ID 和自变量的数量等。

[0496] 接着，将使用图 10 来说明在被提供受限授权码的客户机应用的执行期间的操作。

[0497] 在此，将仅仅详细说明与实施例 1 中的步骤不同的步骤 10-1。

[0498] （步骤 10-1）

[0499] 假定在安全设备 101 中的客户机应用 307 已经开始。

[0500] 通过安全设备 101 的应用执行部分 206 来执行对应于从读取器－写入器 103 发送的命令 1 的处理。

[0501] 在读取表示方法调用的指令代码后，应用执行部分 206 取出紧随所述指令代码的地址信息。

[0502] 确定所述地址信息是否是应用所许可的区域，并且如果所述区域是被许可的区域，则调用所述地址。

[0503] 如果所述区域“不”是许可的区域，则识别授权码，并且，进一步确定授权码的类型。

[0504] 如果确定结果是受限授权码，则确定是否满足限制的类型和说明。

[0505] 例如，当施加使用限制时，如果剩余的重试数目达到 0，则发出表示“不再许可使用”的错误。

[0506] 如果剩余的重试数目未达到 0，则向授权码管理部分 209 传送受限授权码。

[0507] 为了检查剩余的重试数目，在使用时，可以更新受限授权码，或者，使用次数可以存储在授权码管理部分 209 中，并且可以与在受限授权码中包含的使用次数相比较。

[0508] 授权码管理部分 209 读取在受限授权码中包含的索引，取出在表 901 中包含的引用对象应用的 AID，并且向卡间接口执行部分 208 传送该 AID。

[0509] 卡间接口执行部分 208 在响应的数据部分中设置引用对象应用的 AID，在响应的 SW 中设置表示用于使用卡间接口的请求的数据，并且向读取器－写入器 103 发送响应 1101。

[0510] 步骤 10-2 和随后的步骤类似于在发出授权码的实施例 1 中的那些，将不再讨论。

[0511] （临时授权码的发出）

[0512] 最后，将说明临时授权码的发出。

[0513] 假定预先在引用对象存在确定部分 210 中设置了应用属性，其表示在客户机应用被下载后直到选择了客户机应用时的临时许可状态的许可。

[0514] 因此，如果用户忘记携带安装了服务器应用的安全设备，则可以在实际使用客户机应用时，发出用于引用服务器应用的授权码。

[0515] 直到在应用下载时开始地址解析、并且表示使用许可的信息被传送到安全设备 101 的流程与实施例 1 中的类似。

[0516] 在这种情况下，安全设备 101 的卡间接口执行部分 208 接收用于指示要引用的应用不存在的信息，并且，引用对象存在确定部分 210 确定“不好”，然后检查设置了“临时授权码发出许可”，并且请求授权码发出部分 207 发出临时授权码。

[0517] 授权码发出部分 207 按照指令 2201 发出“FA02h”作为临时授权码。

[0518] 按照指令 2201，用于指示其中不许可应用的布置的地址区域的信息的 FA-FBh 被

分配给最上面的一种类型，并且后半部分的一种类型表示临时状态的许可条件。

[0519] 在发出受限授权码后，更新由应用执行部分 206 保留的临时授权状态管理表 2301。

[0520] 当发出临时授权码时，更新临时授权状态管理表 2301。

[0521] 当试图按照 SELECT 命令来选择应用时，应用执行部分 206 引用临时授权码管理表 2301，检查对于要选择的应用还没有执行利用服务器应用的地址解析，并且发出表示应用不可用的错误。

[0522] 为了使得有可能选择应用，变得需要 :1) 向同一安全设备下载服务器应用，或者 2) 执行与安装了服务器应用的不同安全设备的链接处理。

[0523] 1) 为了向同一安全设备下载服务器应用，按照已知的技术来下载服务器应用，然后，地址计算部分 205 引用由应用执行部分 206 管理的临时授权码管理表 2301，并且检查等待与服务器应用的链接处理的客户机应用的存在。

[0524] 如果存在客户机应用，使用在临时授权码管理表中保留的地址计算数据来执行地址解析。

[0525] 其后，从临时授权码管理表删除与已经被链接的客户机应用相关的行。

[0526] 2) 为了执行与安装了服务器应用的不同安全设备的链接处理，从读取器 - 写入器 103 发送链接专用的命令。

[0527] 所述链接专用命令由下述部分构成 :首标部分，其中可以将所述命令解释为链接专用命令 ;以及数据部分，其包含服务器应用的标识符。

[0528] 当下载管理部分 201 接收到链接专用命令何时，地址计算部分 205 引用由应用执行部分 206 管理的临时授权码管理表 2301，并且检查等待与服务器应用的链接处理的客户机应用的存在。

[0529] 如果等待链接处理的客户机应用存在，则在临时授权码管理表 2301 中保留的地址计算数据和服务器应用的标识符被传送到卡间接口执行部分 208，并且在卡间接口执行部分 208 和不同安全设备 102 之间检查引用对象的存在。

[0530] 当卡间接口执行部分 208 接收到表示使用许可的信息时，引用对象存在确定部分 210 请求授权码发出部分 207 发出授权码。

[0531] 授权码发出部分 207 发出授权码，并且授权码表 901 被更新。

[0532] 引用对象存在确定部分 210 请求应用执行部分 206 从临时授权码管理表删除与已经被链接的客户机应用相关的行。

[0533] 如上所述执行 1) 或者 2) 的处理，由此可以完成以后的客户机应用选择和执行。

[0534] 在实施例 6 中，已经说明了除了在实施例 1 中详细说明的授权码之外的受限授权码和临时授权码的发出和被提供授权码的应用的操作。

[0535] 受限授权码使得能够在不改变服务器应用侧的情况下限制使用次数等，以便可以将所述实施例应用到试验拷贝的临时应用的发出等。

[0536] 当下载客户机应用时，如果用户不具有安装了客户机应用的安全设备，则可以按照临时授权码来执行以后的链接处理。因此，消除了下述情况 :其中，虽然用户想要下载客户机应用，但是他或者她必须放弃下载客户机应用的想法，因为用户当时没有恰巧具有安装了服务器应用的安全设备。

[0537] 因此，相对于从服务提供商看的商业机会的丢失和从用户看的服务使用机会的丢失，所述实施例变为有效措施。

[0538] （实施例 7）

[0539] 实施例 7 是涉及请求在不同安全设备中安装的服务器应用执行处理并且在客户机应用内使用所述服务器应用的处理数据的方法的发明。

[0540] 将使用图 5 和 24-27 来说明本发明的实施例 7。

[0541] 图 24 是示出所述实施例中的安全设备 2401 的配置的方框图。

[0542] 下载管理部分 201、应用存储部分 202、应用 203 和 204、地址计算部分 205、应用执行部分 206、授权码发出部分 207、卡间接口执行部分 208、授权码管理部分 209 与实施例 1 中描述的那些相同。

[0543] 所述安全设备与在图 1 中所示的安全设备 101 的不同在客户机应用 2402 和堆栈操作部分 2403。

[0544] 客户机应用 2402 使用由在不同安全设备 2501 中安装的服务器应用提供的接口。

[0545] 堆栈操作部分 2403 在使用由服务器应用提供的接口时操作由客户机应用处理的堆栈。

[0546] 图 25 是示出在所述实施例中的不同安全设备 2501 的配置的方框图。应用存储部分 202、应用执行部分 206 和服务器应用 401 类似于在实施例 1 中描述的那些。

[0547] 所述安全设备与在图 4 中所示的不同安全设备 102 的不同在于堆栈控制部分 2502。

[0548] 所述堆栈控制部分 2502 对服务器应用执行控制，以对于来自在同一安全设备中安装的客户机应用的调用和来自在分离的安全设备中安装的客户机应用的调用执行相同的操作。

[0549] 图 5 是所述实施例中的读取器－写入器 103，并且类似于实施例 1 中的读取器－写入器。

[0550] 在所述实施例中，将描述由安全设备 2401、不同安全设备 2501 和读取器－写入器 103 构成的系统。

[0551] 在实施例 1 中，描述了下述情况：其中，来自服务器应用的响应不包含除了 SW 之外的任何数据（参见在图 11(a) 中的响应 1103）。

[0552] 如果响应由数据和 SW 构成，并且所述数据用于随后的客户机应用处理，则需要堆叠 (stack) 数据。

[0553] 已知如果在同一安全设备中存在服务器应用，则服务器应用中的处理结果的返回值被堆叠，并且被返回到调用者的客户机应用。

[0554] 但是，如果服务器应用不存在于同一安全设备中并且使用在不同安全设备中的服务器应用，则按照安全设备之间的通信协议在 APDU（应用协议数据单元）内存储返回值。

[0555] 因此，为了使得客户机应用执行相同的操作而与所述服务器应用存在于哪个安全设备中无关，变得必须从 APDU 提取返回值，并且在客户机应用的堆栈上存储返回值。

[0556] 在实施例 7 中，将说明在以后的客户机应用处理中使用来自服务器应用的返回值的方法。

[0557] 为了描述所述方法，下面说明前提条件：

[0558] 服务器应用被安装在不同安全设备中，并且客户机应用的地址解析完成。

[0559] 执行客户机应用，并且到图 10 中的步骤 10-3 的流程完成。

[0560] 像在实施例 1 中描述的系统的操作那样，执行前提。

[0561] 将说明如图 26 所示的、其中“method_1(方法 _1)”调用“method_2(方法 _2)”的情况。

[0562] 应用执行部分 206 以函数为单位建立帧 (frame)，并且执行处理。所述帧是用于从函数返回值、处理异常并且存储数据的多个部分和结果的工作区域。帧 1 被分配到“method_1”，帧 2 被分配到“method_2”。每个帧由局部变量和堆栈构成。

[0563] 在“method_1”调用“method_2”后立即产生帧 2。“method_2”使用帧 2 执行处理，并且最后返回“b”。

[0564] “返回‘b’”的表达用于表示按照指令码“sreturn”在帧 1 的堆栈上直接地堆叠“b”的值。在返回“b”后，消除帧 2。

[0565] 其后，“method_1”继续处理。

[0566] 因此，建立了函数到函数的调用。

[0567] 但是，如果“method_1”和“method_2”存在于不同的安全设备中，则实质上应当被堆叠在“method_1”的帧上的“method_2”的帧在不同安全设备的控制下，因此，“method_2”的处理结果不能直接地被存储在调用者的“method_1”的堆栈上。

[0568] 因此，下述机制变得必要 :所述机制使得有可能在“method_2”不能直接地在“method_1”的堆栈上存储处理结果的情况下，实现与“method_2”直接在所述堆栈上存储处理结果的必要操作相同的处理。

[0569] 因此，堆栈控制部分 2502 仅仅在来自在分离的安全设备中安装的客户机应用的引用时执行与用于在返回值 (示例 :sreturn) 的操作内涉及的指令代码的通常处理不同的处理。

[0570] 当从在分离的安全设备中安装的客户机应用调用时，调用者的帧不存在于应用执行部分 403 中。

[0571] 在这种情况下，堆栈控制部分 2502 负责“sreturn”的处理。

[0572] 堆栈控制部分 2502 停止向调用者帧的堆栈内写入，而是建立如图 27 所示的数据。

[0573] 在所述实施例中所述的发明内，建立和使用如图 27 中的数据，由此，如果客户机应用不存在于具有服务器应用的安全设备中，则可以在堆栈上存储处理结果。

[0574] 图 27 由表示“sreturn”的 TAG、表示返回值的长度的 LENGTH 和表示返回值的 Value 组成。

[0575] 这在从服务器应用发送的响应的数据部分中设置，并且作为调用结果被传送到用于执行客户机应用的安全设备 101。

[0576] 接着，将使用图 10 来说明在接收数据后的安全设备 2401 的操作。

[0577] 在所述实施例中的说明内，图 10 中的安全设备 101 被替换为安全设备 2401，并且不同安全设备 102 被替换为不同安全设备 2501。

[0578] 当客户机应用 2402 引用服务器应用时的步骤的步骤 10-1 到步骤 10-4 与实施例 1 中的那些步骤类似，因此不再说明，将说明返回服务器应用的处理结果的步骤 10-5。

[0579] 安全设备 2401 的卡间接口执行部分 208 接收共享命令，并且向堆栈操作部分 2403

传送所述共享命令的数据部分。

[0580] 堆栈操作部分 2403 解释表示“sreturn”的 TAG，并且在调用者（客户机应用）的帧的堆栈上存储值。

[0581] 其后，客户机应用也可以继续处理，就像服务器应用被安装在同一安全设备中那样。

[0582] 在实施例 6 中，已经说明了通过对于安全设备 2401 提供堆栈操作部分 2403 的对于不同安全设备 2501 提供堆栈控制部分 2502，使得客户机应用能够使用来自在不同安全设备中安装的服务器应用的返回值的而不向服务器应用和客户机应用的代码施加特殊处理的方法。

[0583] 客户机应用检查和使用来自服务器应用的返回值的场景经常发生，并且所述系统的优点很大。

[0584] 虽然已经参考特定实施例详细说明了本发明，但是对于本领域内的技术人员显然，可以在不脱离本发明的精神和范围的情况下，进行各种改变和修改。

[0585] 本申请基于 2006 年 3 月 31 日提交的日本专利申请（第 2006-098865 号）和在 2007 年 3 月 22 日提交的日本专利申请（第 2007-075217 号），它们通过引用被包含在此。

[0586] 产业上的应用性

[0587] 可以提供了具有下述优点的系统：可以通过本发明的安全设备和读取器 - 写入器来减少安全设备的存储区域。

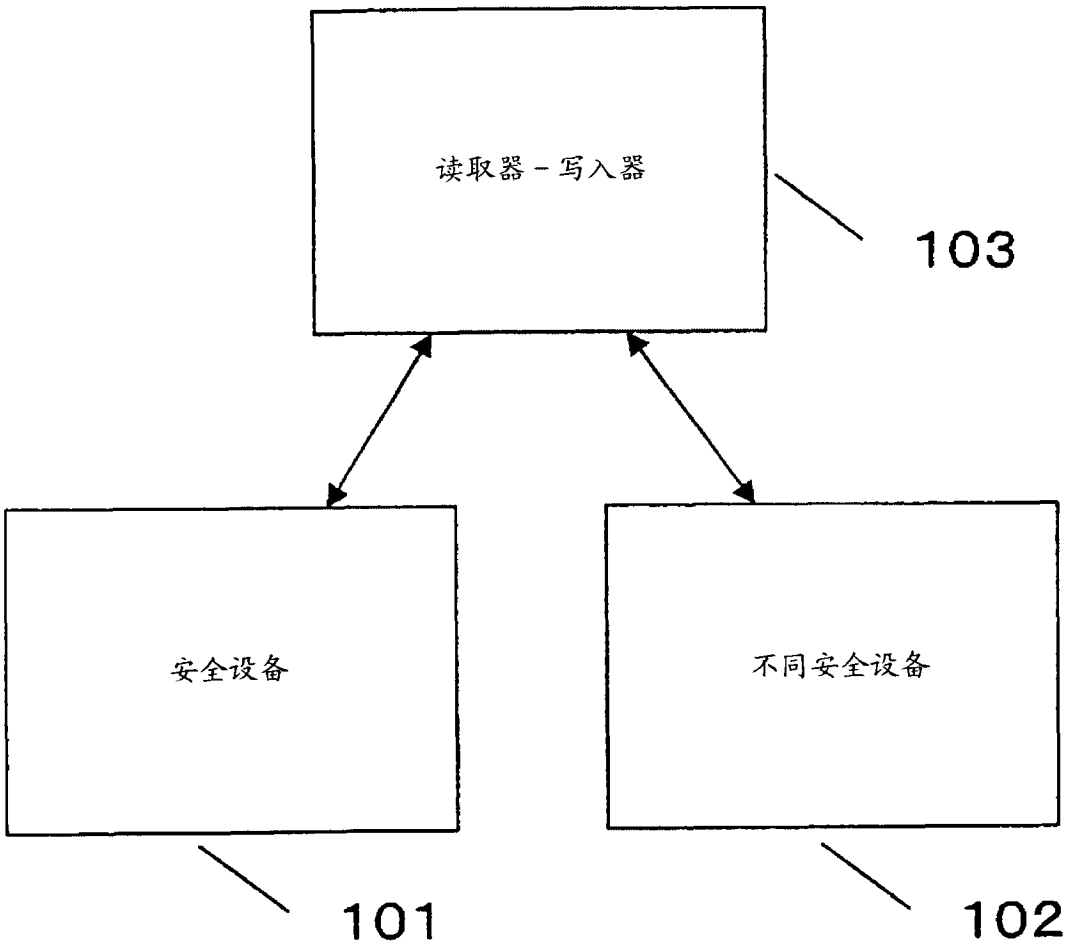


图 1

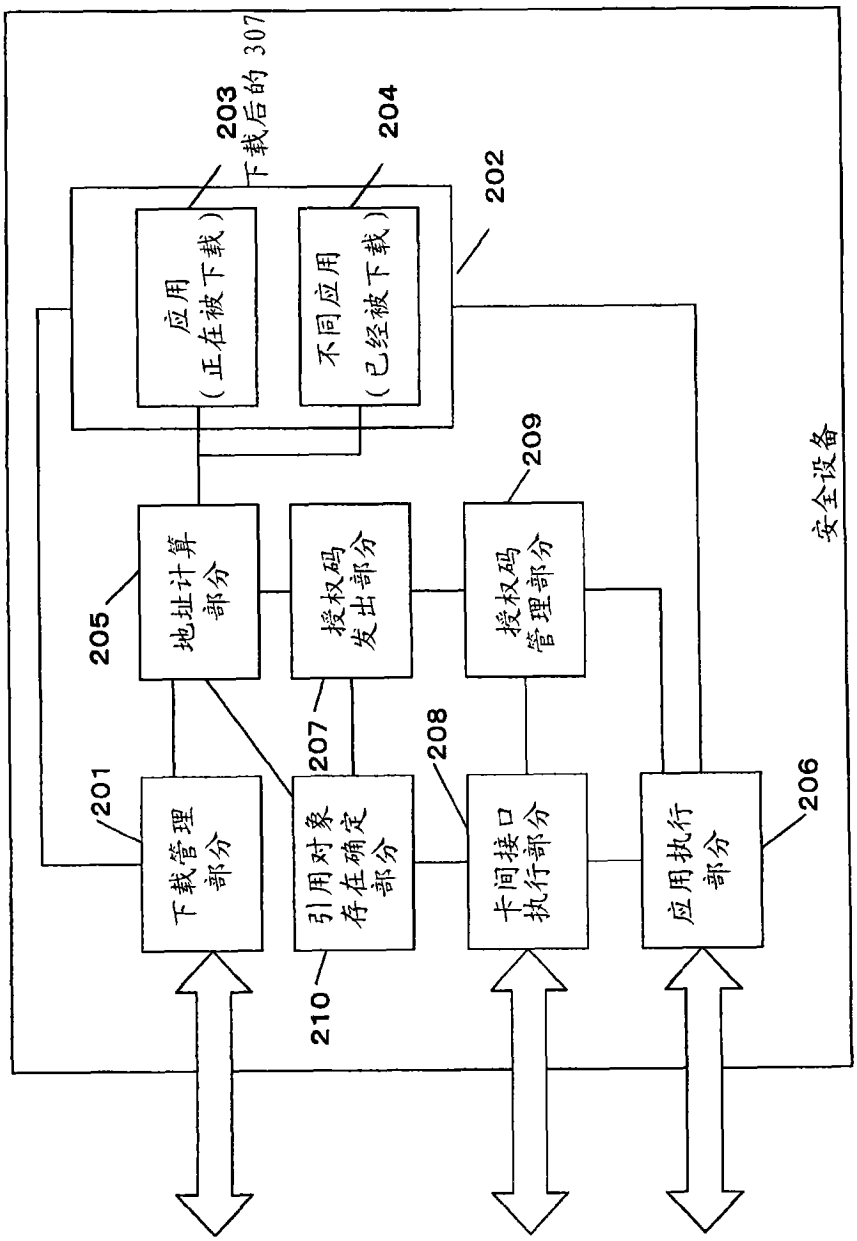

安全设备
101
应用
（正在被下载）
203
下载后的 307
不同应用
（已经被下载）
204
202
地址计算
部分
205
授权码
发出部分
207
授权码
管理部分
209
下载管理
部分
201
引用对象
存在确定
部分
210
卡间接口
执行部分
208
应用执行
部分
206

图 2

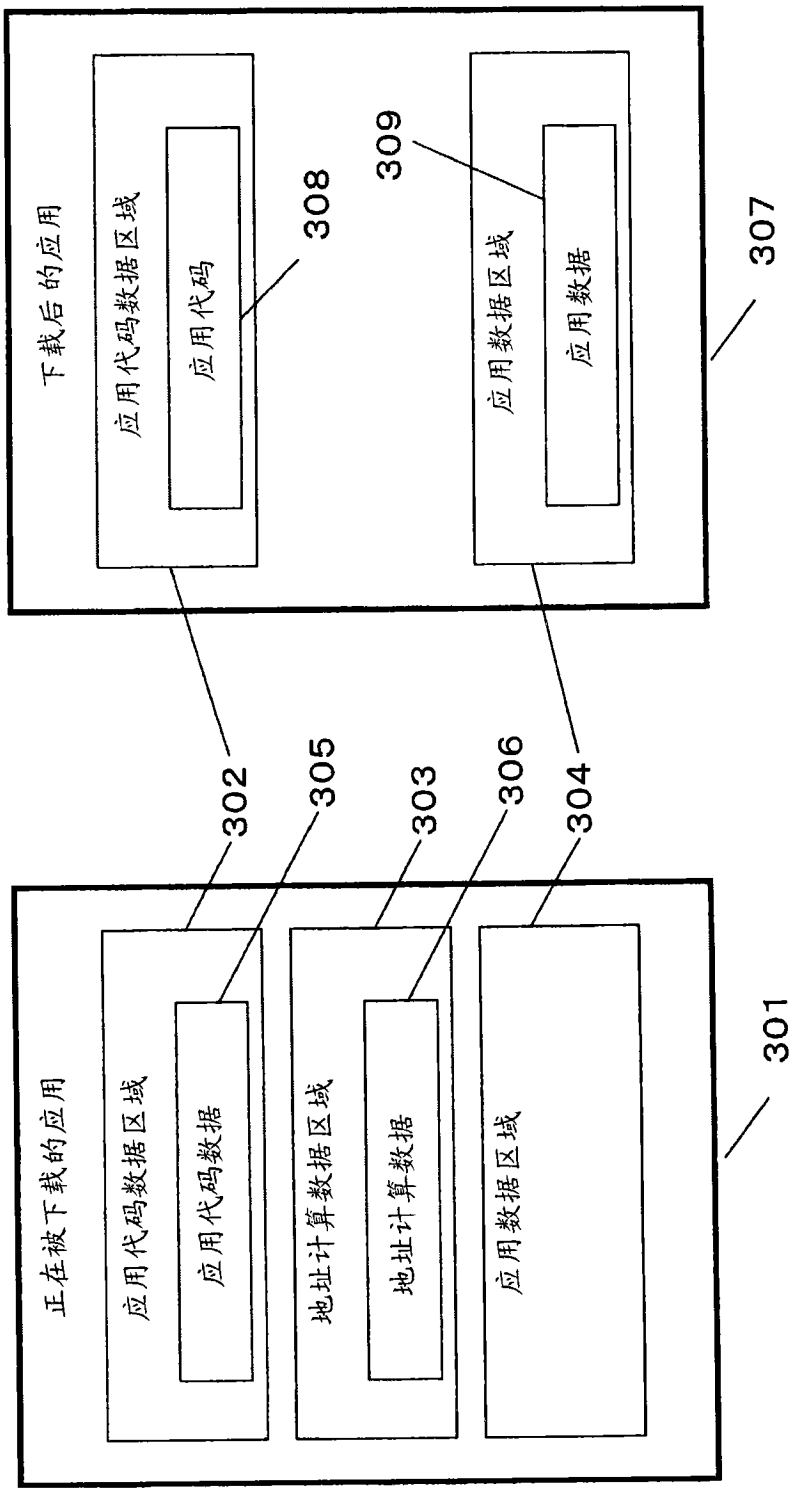

下载后的应用
应用代码数据区域
应用代码
308
309
应用数据区域
应用数据
307
302
305
303
306
304
正在被下载的应用
应用代码数据区域
应用代码数据
地址计算数据区域
地址计算数据
应用数据区域
301

图 3

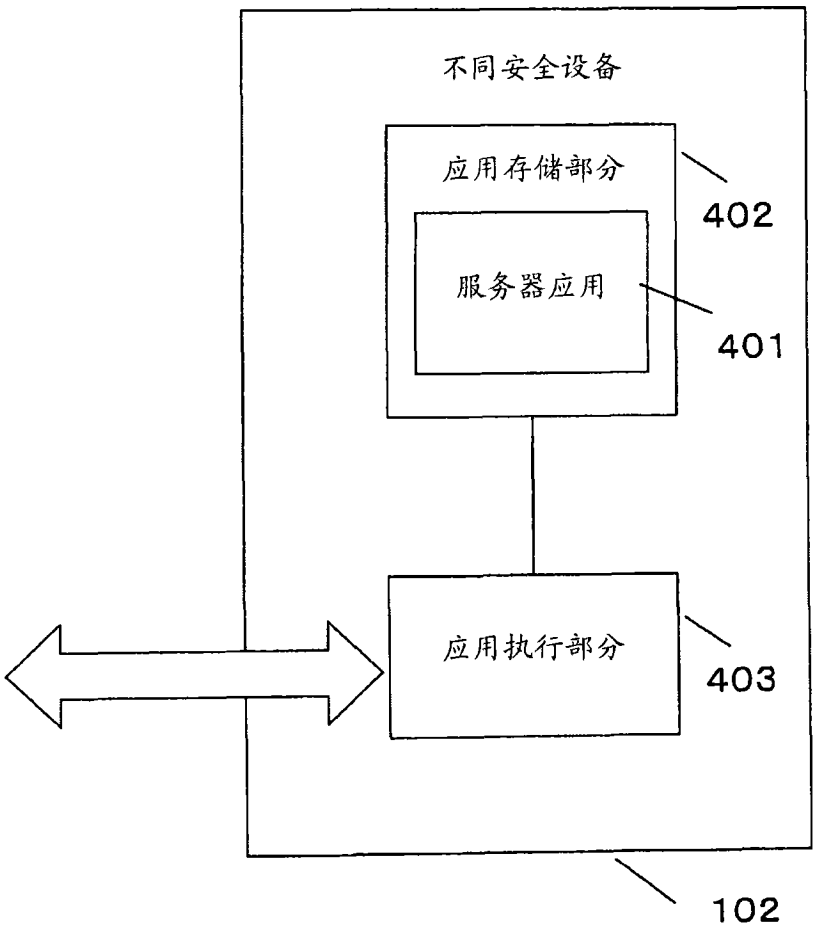


图 4

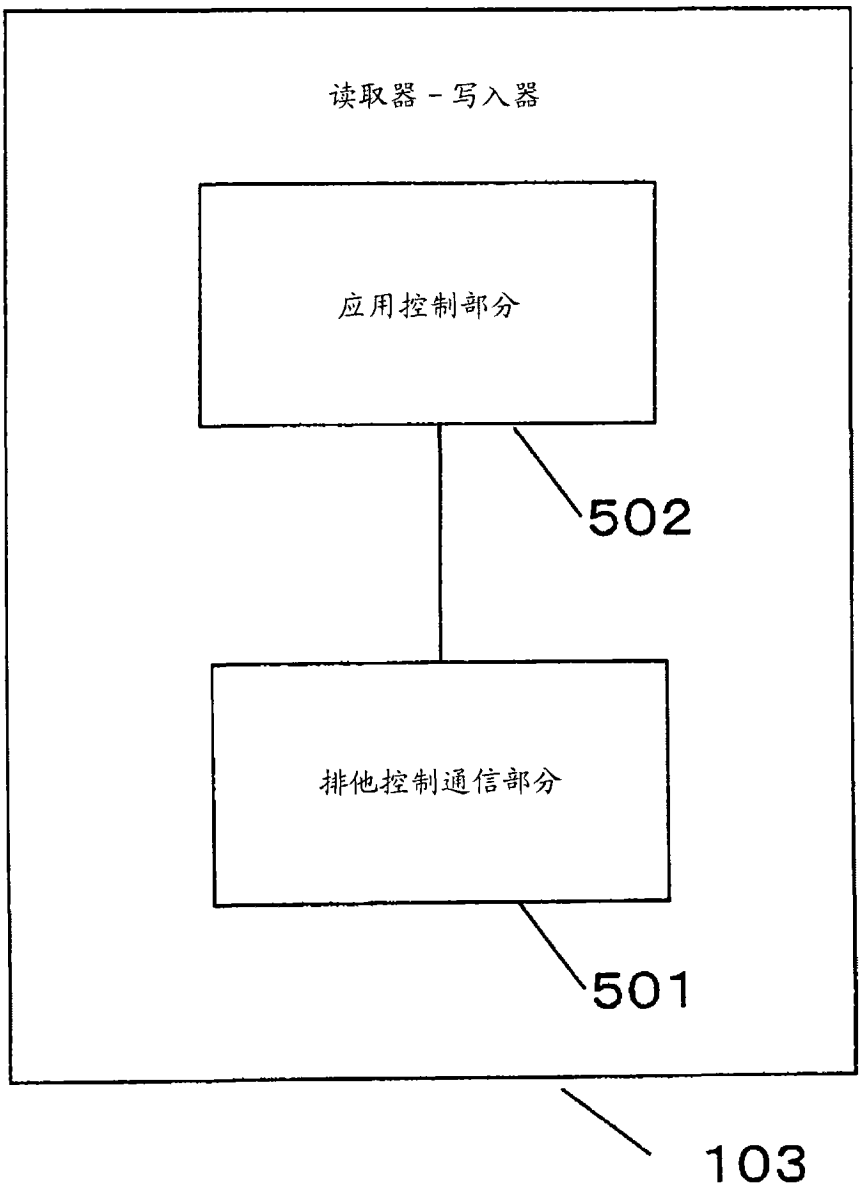


图 5

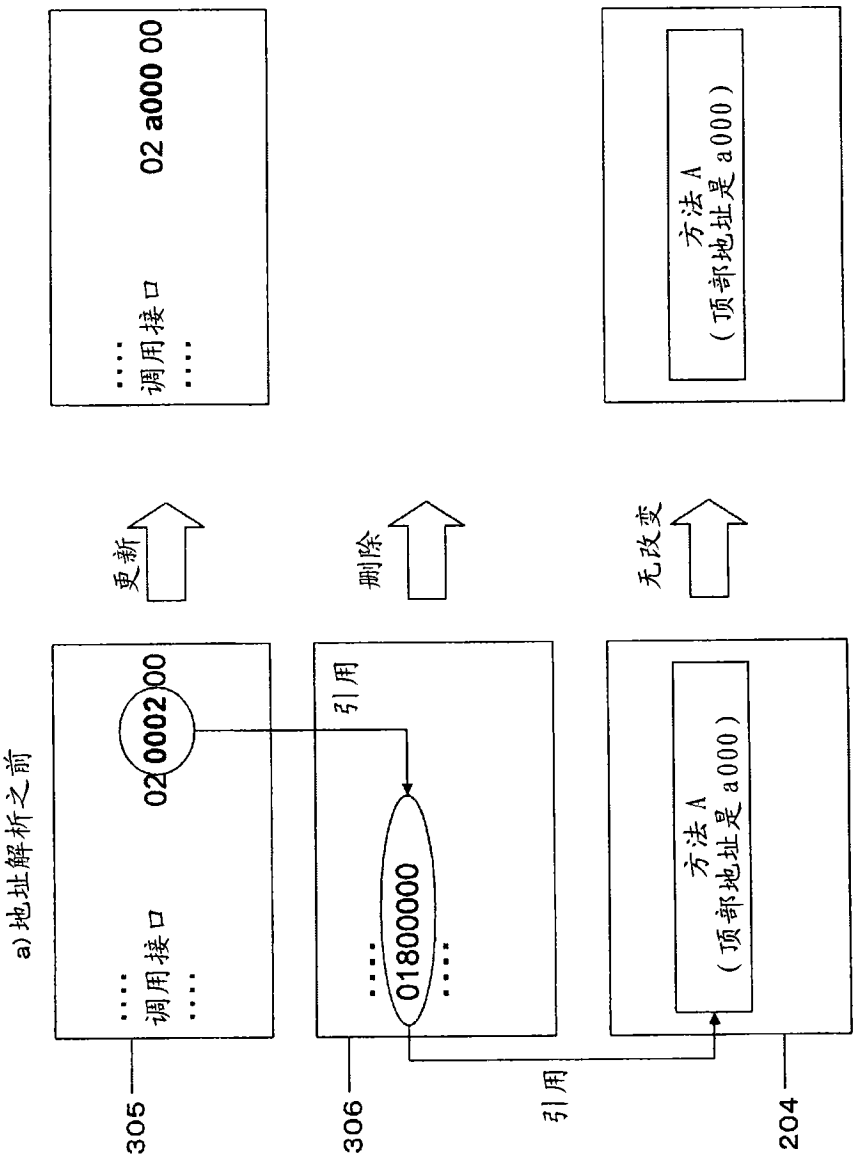

a)地址解析之前
....
调用接口
....
02 0002 00
305
引用
....
01800000
....
306
引用
204
方法 A
(顶部地址是 a000)
更新
删除
无改变
....
调用接口
....
02 a000 00
方法 A
(顶部地址是 a000)

图 6

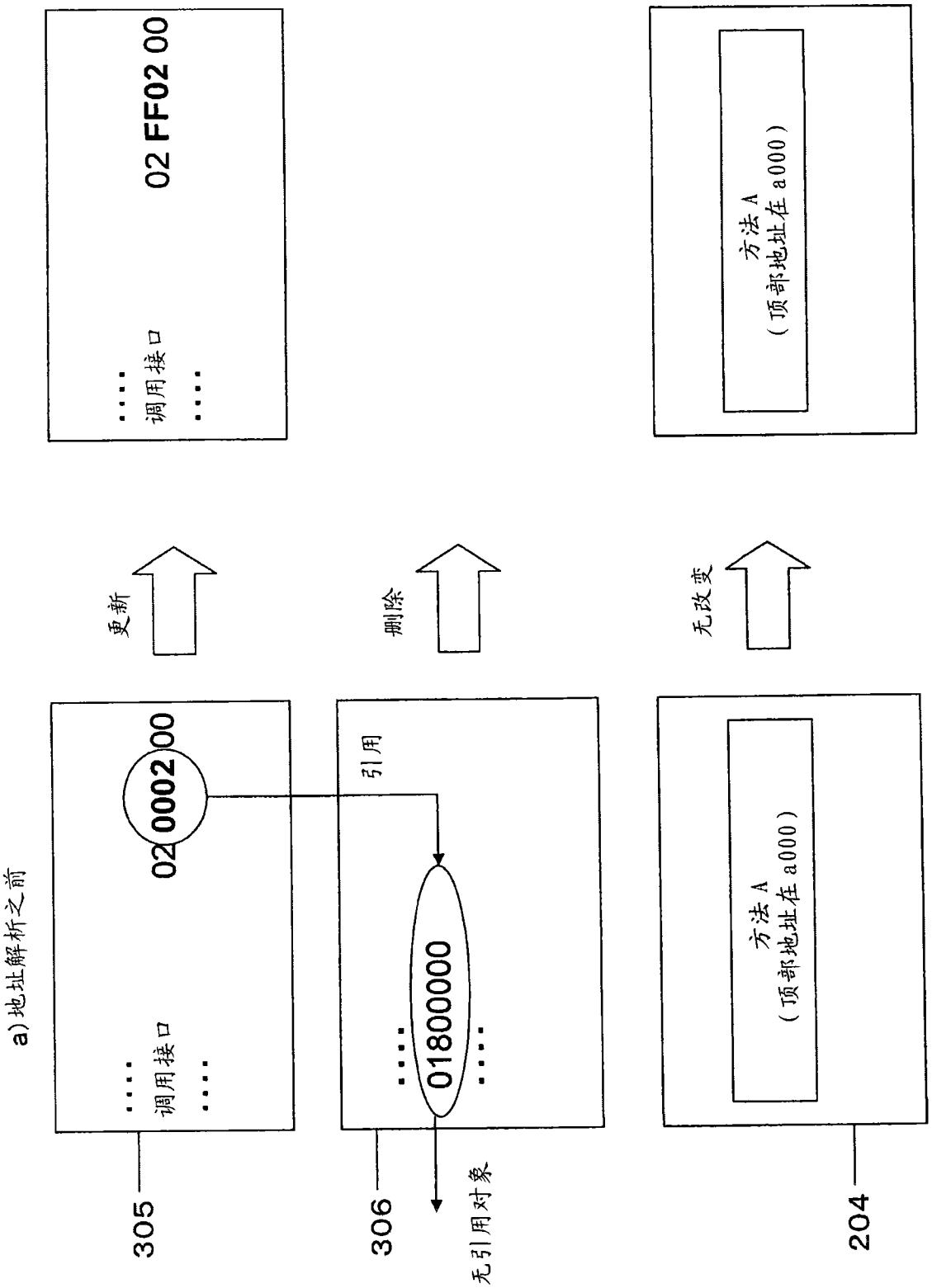

a)地址解析之前
02 0002 00
.....
调用接口
.....
305
引用
.....
01800000
.....
306
无引用对象
204
方法 A
(顶部地址在 a000)
更新
删除
无改变
02 FF02 00
.....
调用接口
.....
方法 A
(顶部地址在 a000)

图 7

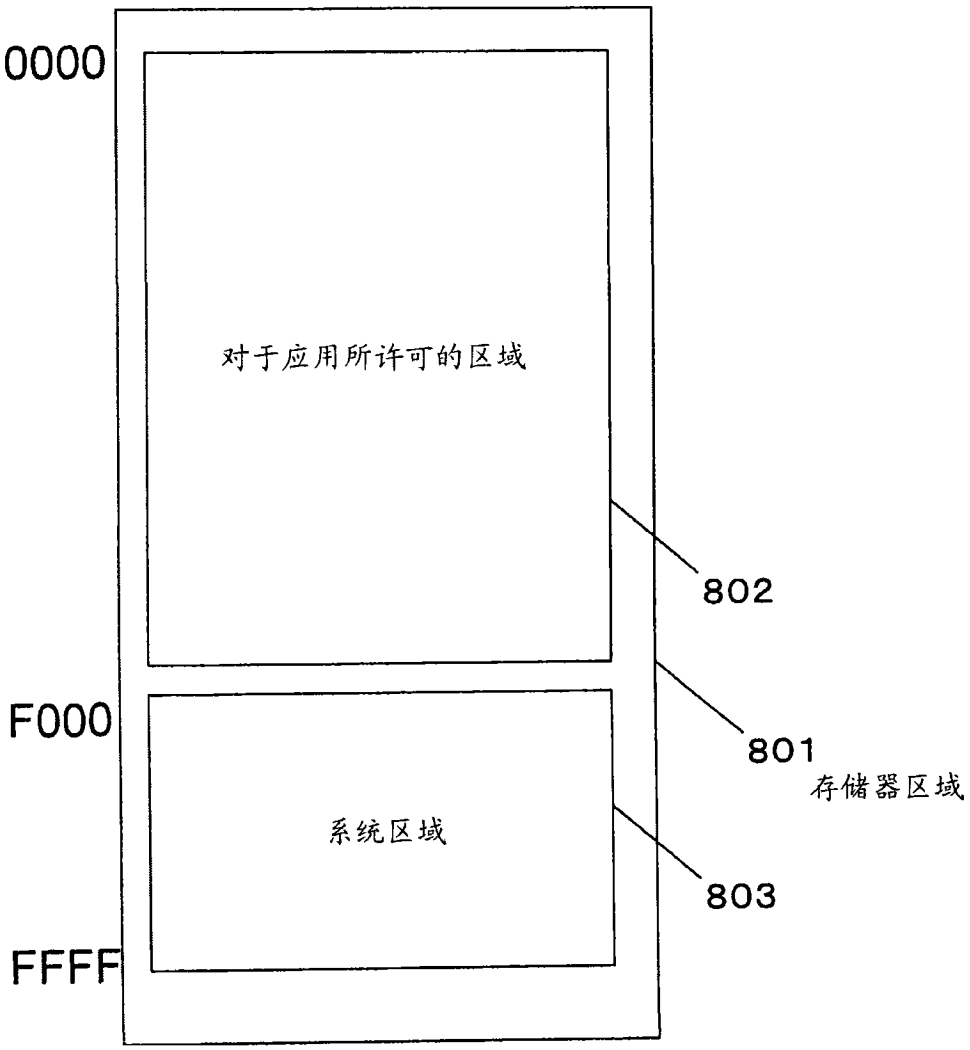


图 8

901 授权码表

索引	引用对象应用的标识符（AID）	方法 ID	自变量的数量
0	....	....	....
1	.....	....	....
2	102030405060	4	1

图 9

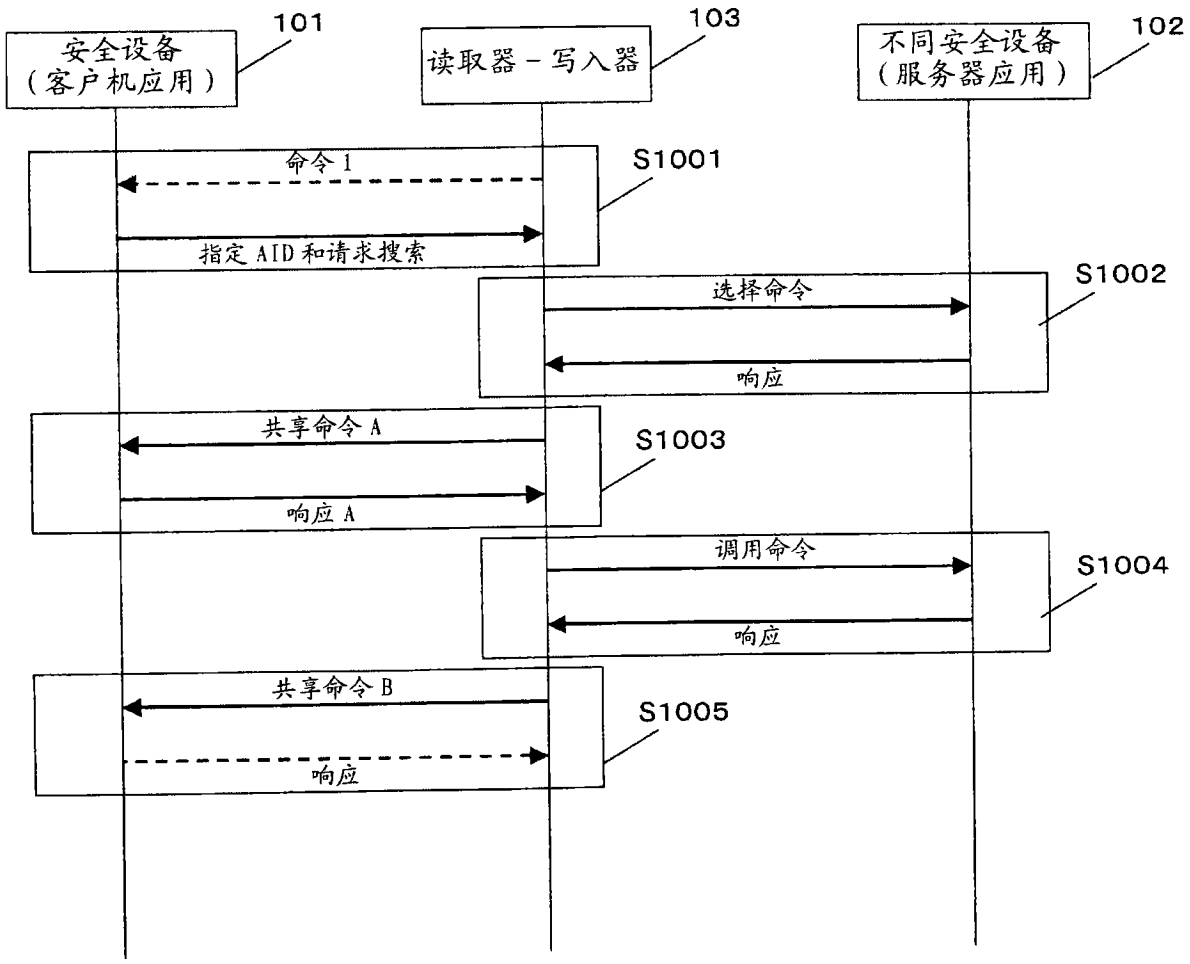

安全设备
（客户机应用）
101
读取器－写入器
103
不同安全设备
（服务器应用）
102
命令 1
S1001
指定 AID 和请求搜索
选择命令
S1002
响应
共享命令 A
S1003
响应 A
调用命令
S1004
响应
共享命令 B
S1005
响应

图 10

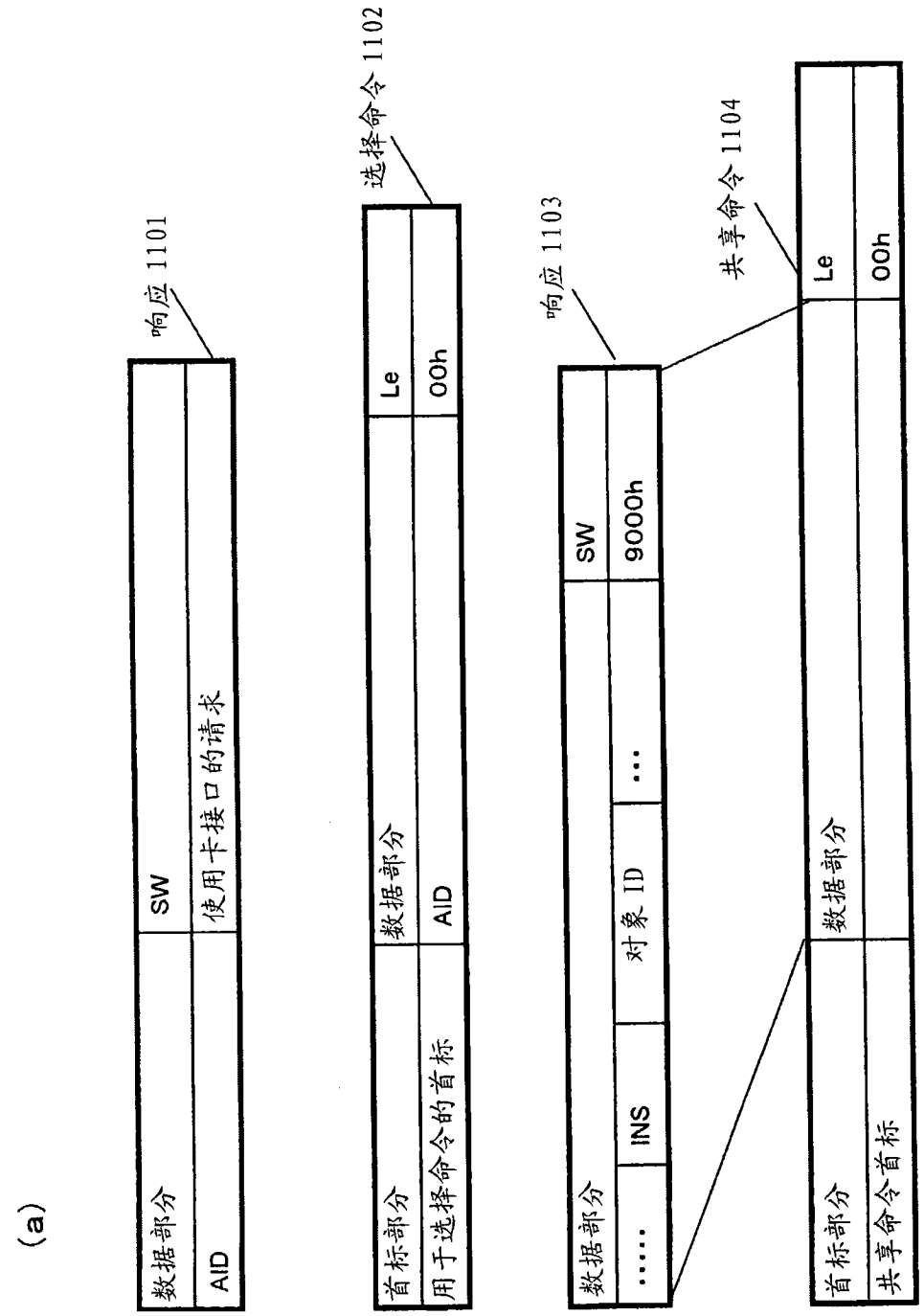

(a)
数据部分
AID
SW
使用卡接口的请求
响应 1101
首标部分
用于选择命令的首标
数据部分
AID
Le
00h
选择命令 1102
数据部分
.....
INS
对象 ID
...
SW
9000h
响应 1103
首标部分
共享命令首标
数据部分
Le
00h
共享命令 1104

图 11a

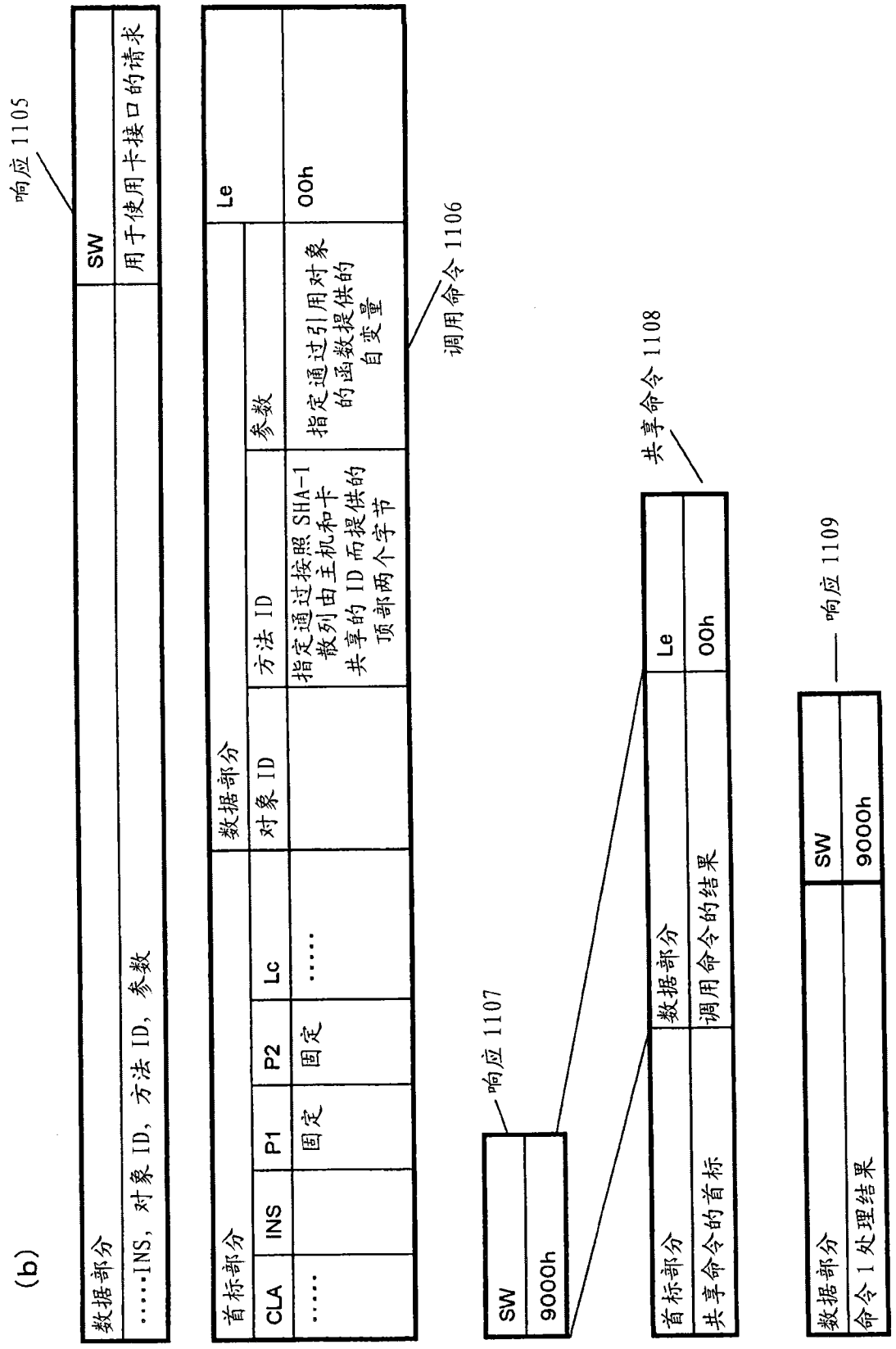

(b)
响应 1105
数据部分
……INS，对象 ID，方法 ID，参数
SW
用于使用卡接口的请求
首标部分
CLA
INS
P1
P2
Lc
……
固定
固定
数据部分
对象 ID
方法 ID
指定通过按照 SHA-1 散列由主机和卡共享的 ID 而提供的顶部两个字节
参数
指定通过引用对象的函数提供的自变量
Le
00h
调用命令 1106
响应 1107
SW
9000h
共享命令 1108
首标部分
共享命令的首标
数据部分
调用命令的结果
Le
00h
响应 1109
数据部分
命令 1 处理结果
SW
9000h

图 11b

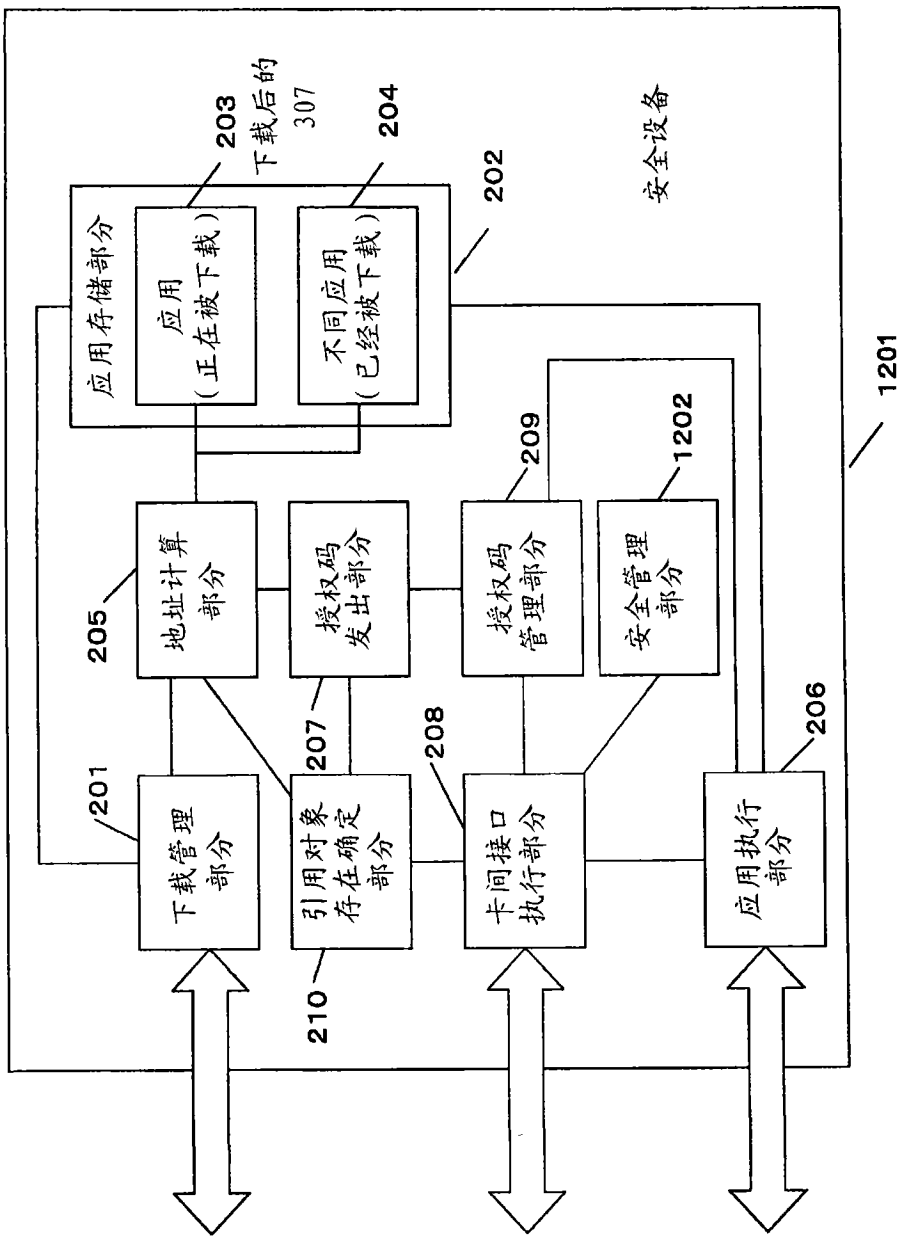

安全设备
1201
应用存储部分
203
下载后的
应用
（正在被下载）
307
204
不同应用
（已经被下载）
202
209
1202
205
地址计算
部分
授权码
发出部分
授权码
管理部分
安全管理
部分
201
207
208
206
下载管理
部分
引用对象
存在确定
部分
卡间接口
执行部分
应用执行
部分
210

图 12

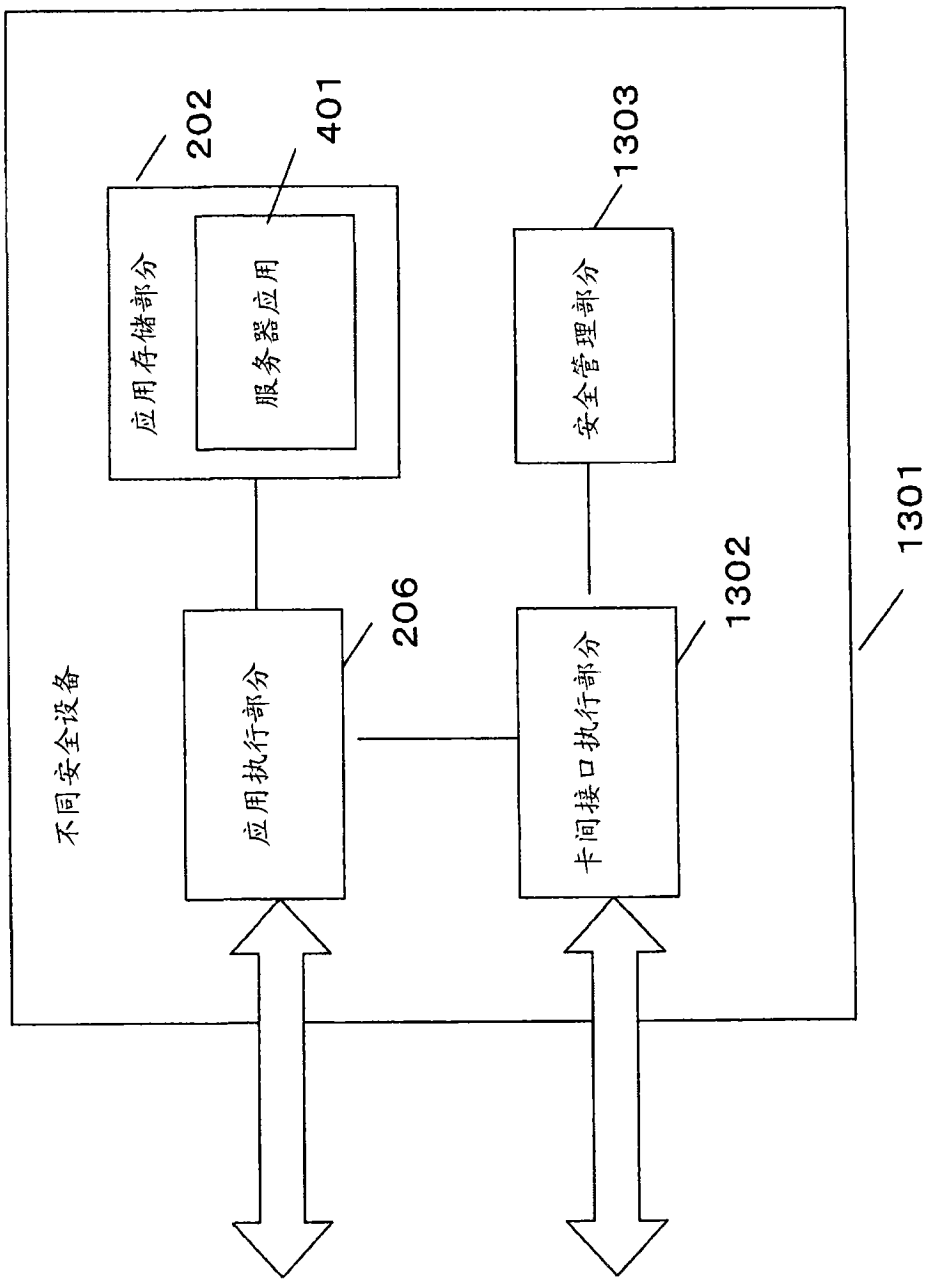

不同安全设备
应用存储部分
202
服务器应用
401
应用执行部分
206
安全管理部分
1303
卡间接口执行部分
1302
1301

图 13

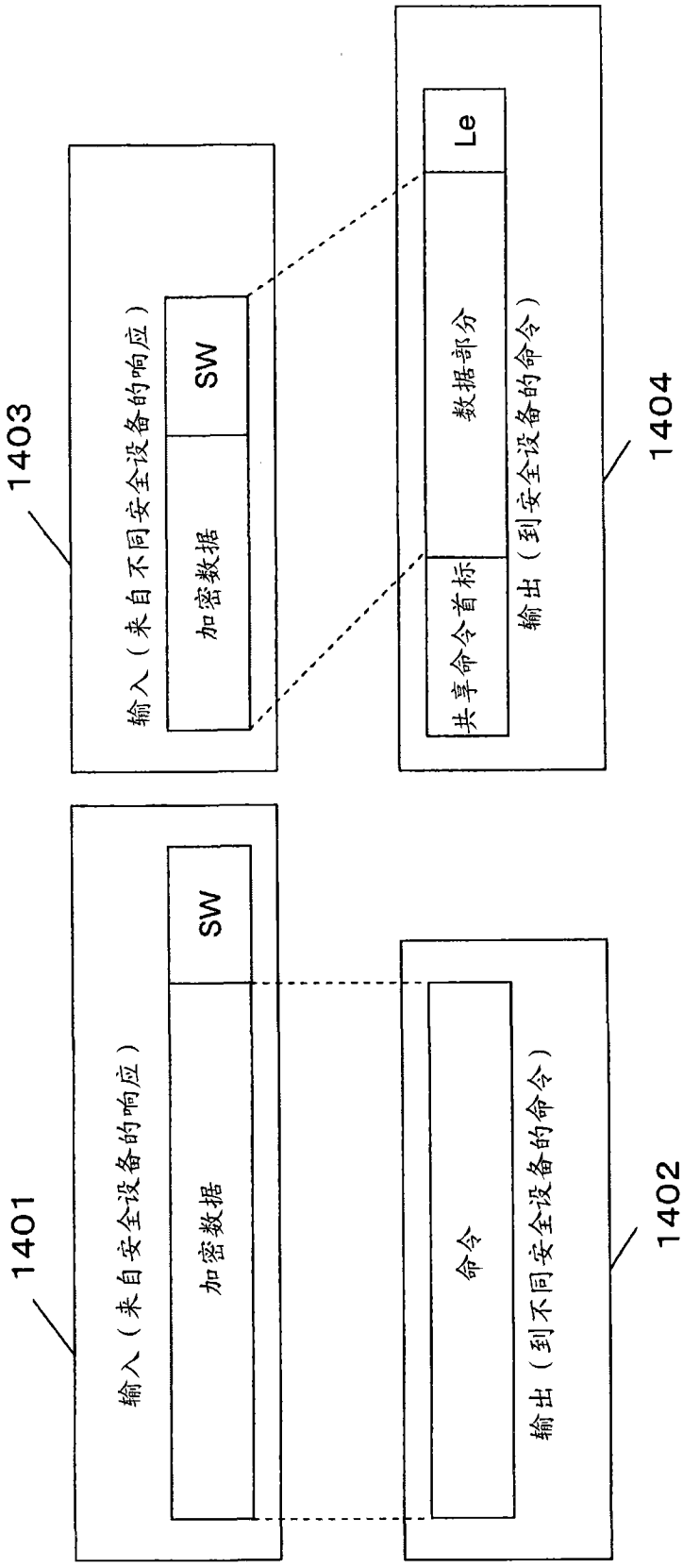

1401
输入（来自安全设备的响应）
加密数据
SW
1402
输出（到不同安全设备的命令）
命令
1403
输入（来自不同安全设备的响应）
加密数据
SW
1404
输出（到安全设备的命令）
共享命令首标
数据部分
Le

图 14

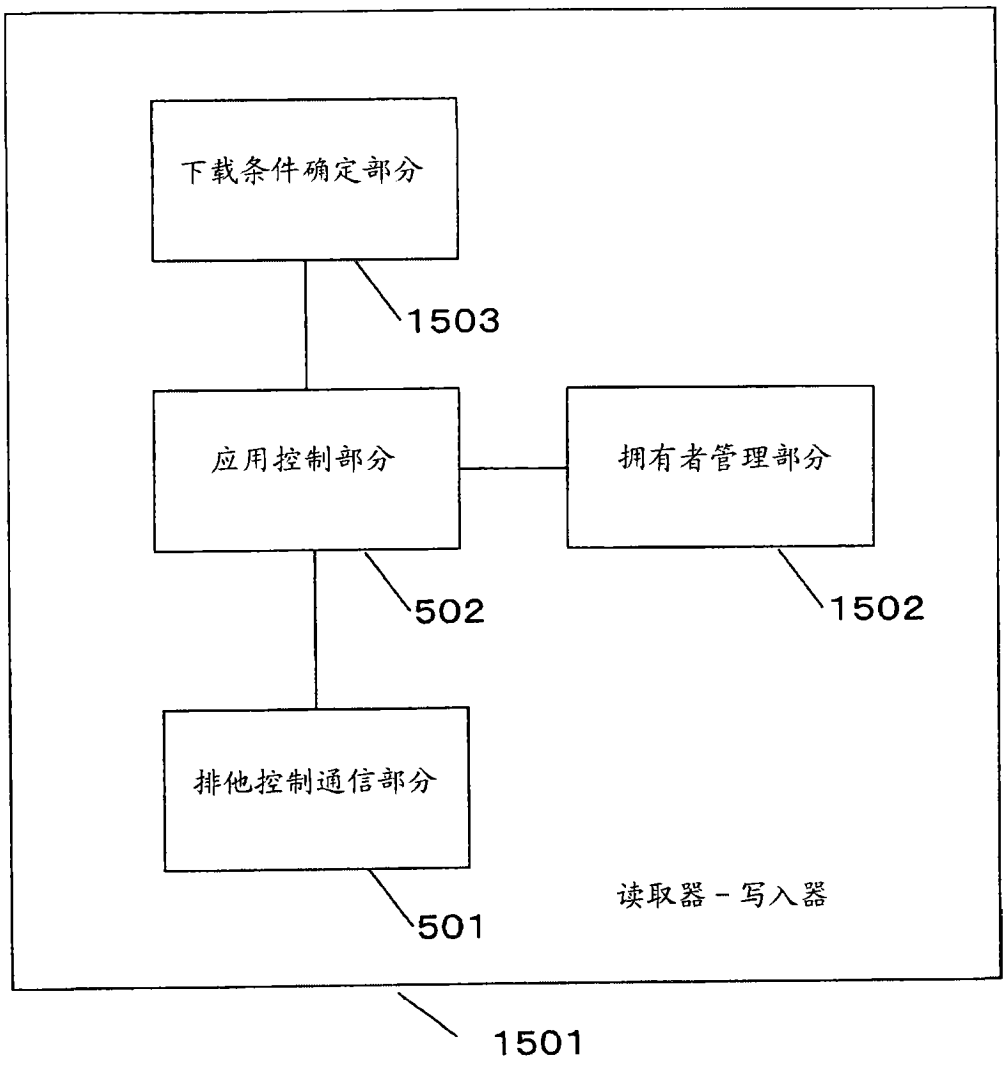

下载条件确定部分
1503
应用控制部分
拥有者管理部分
502
1502
排他控制通信部分
501
读取器－写入器
1501

图 15

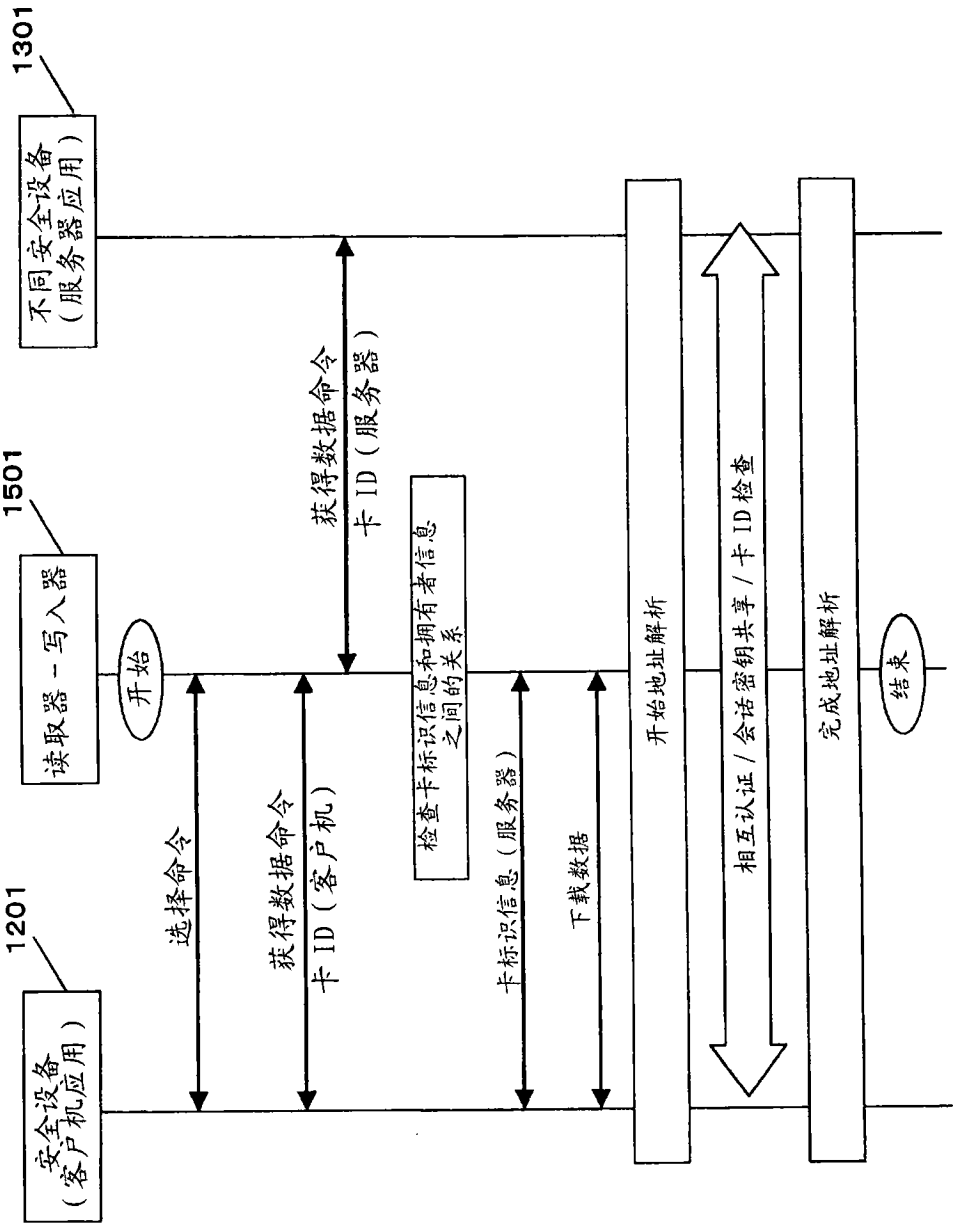

1301
不同安全设备
（服务器应用）
1501
读取器 - 写入器
1201
安全设备
（客户机应用）
开始
选择命令
获得数据命令
卡 ID（客户机）
获得数据命令
卡 ID（服务器）
检查卡标识信息和拥有者信息
之间的关系
卡标识信息（服务器）
下载数据
开始地址解析
相互认证 / 会话密钥共享 / 卡 ID 检查
完成地址解析
结束

图 16

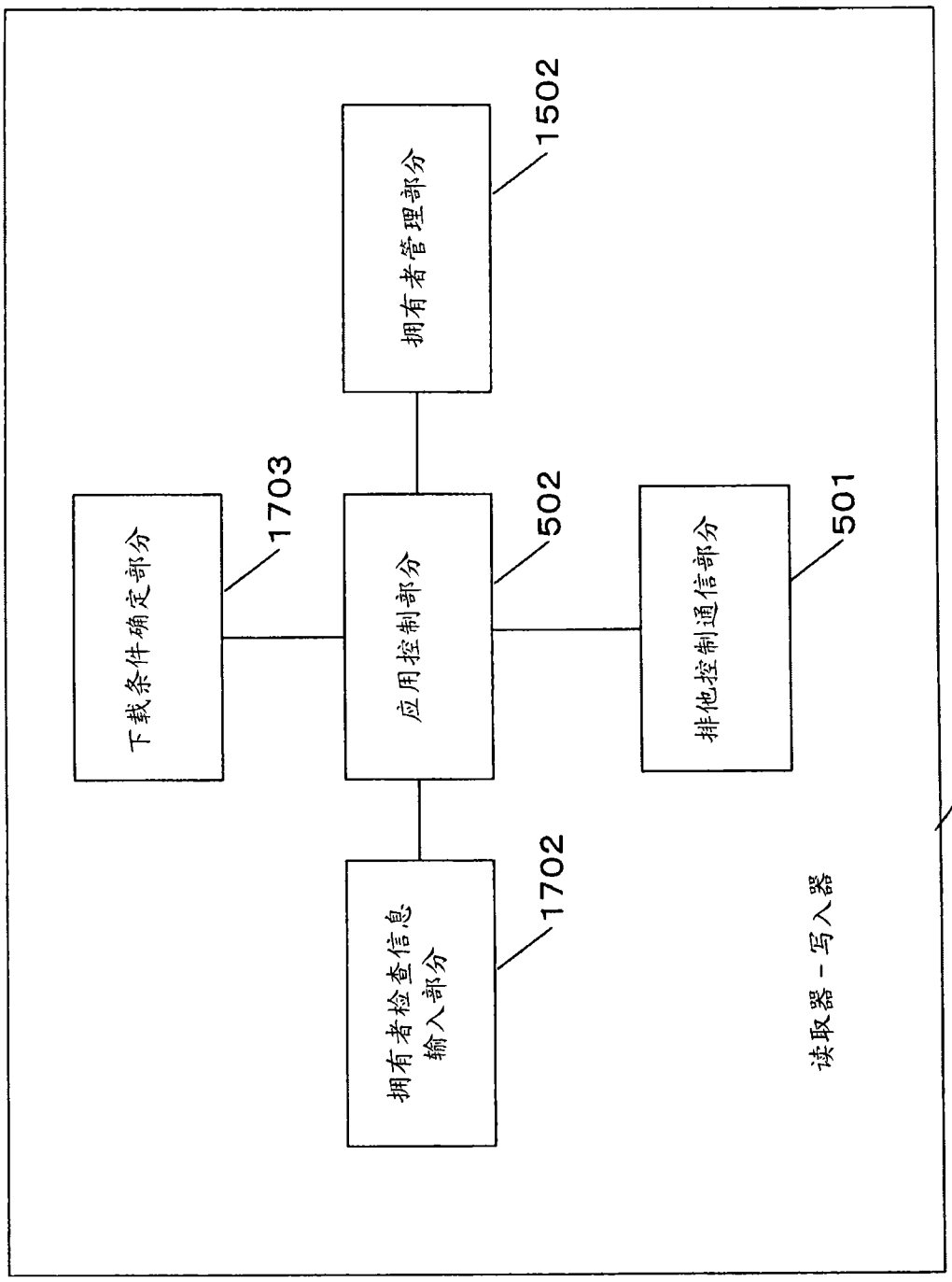

拥有者管理部分
1502
下载条件确定部分
1703
应用控制部分
502
排他控制通信部分
501
拥有者检查信息输入部分
1702
读取器 - 写入器
1701

图 17

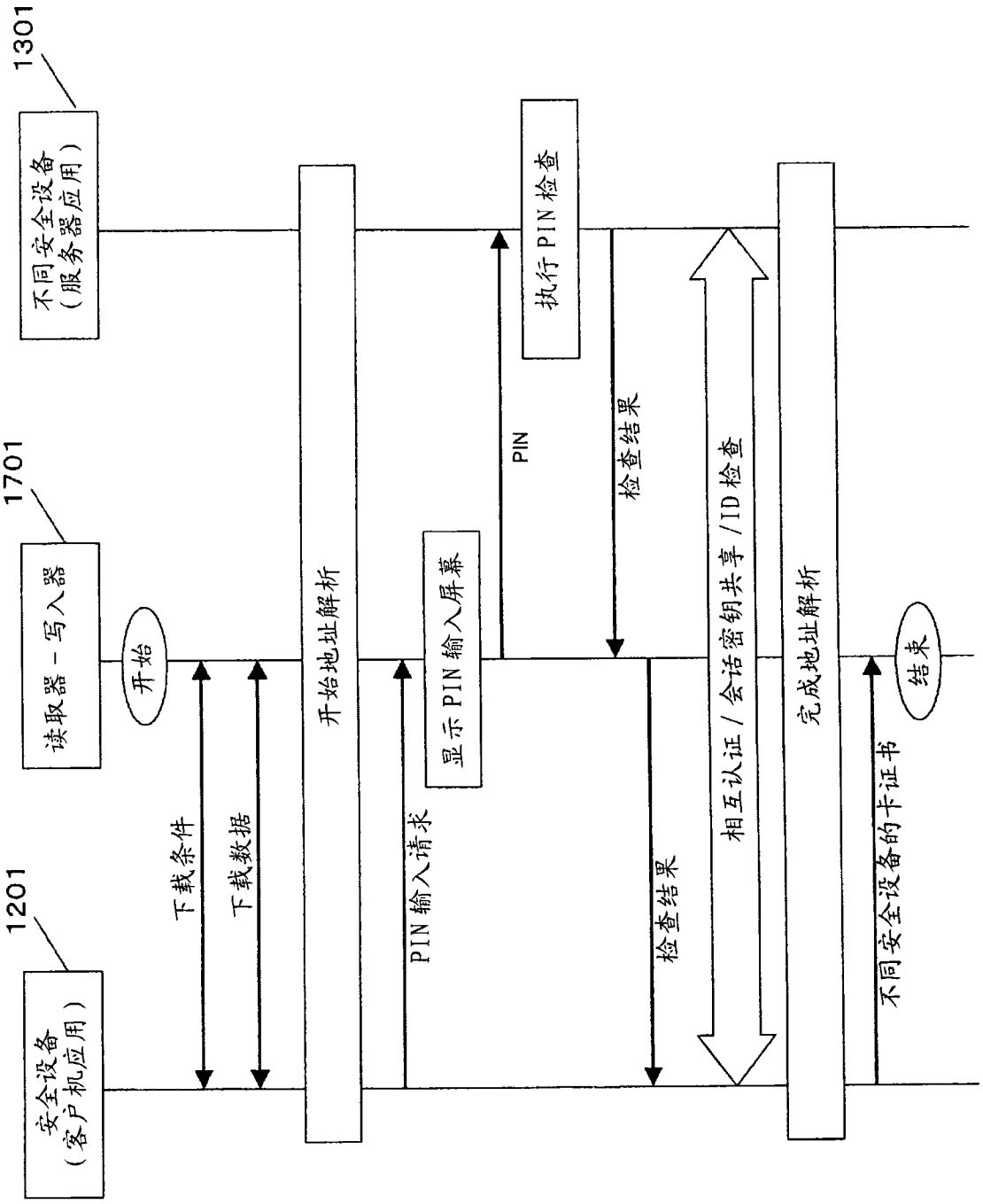

1301
不同安全设备
（服务器应用）
1701
读取器 - 写入器
1201
安全设备
（客户机应用）
开始
下载条件
下载数据
开始地址解析
PIN 输入请求
显示 PIN 输入屏幕
PIN
执行 PIN 检查
检查结果
检查结果
相互认证 / 会话密钥共享 /ID 检查
完成地址解析
结束
不同安全设备的卡证书

图 18

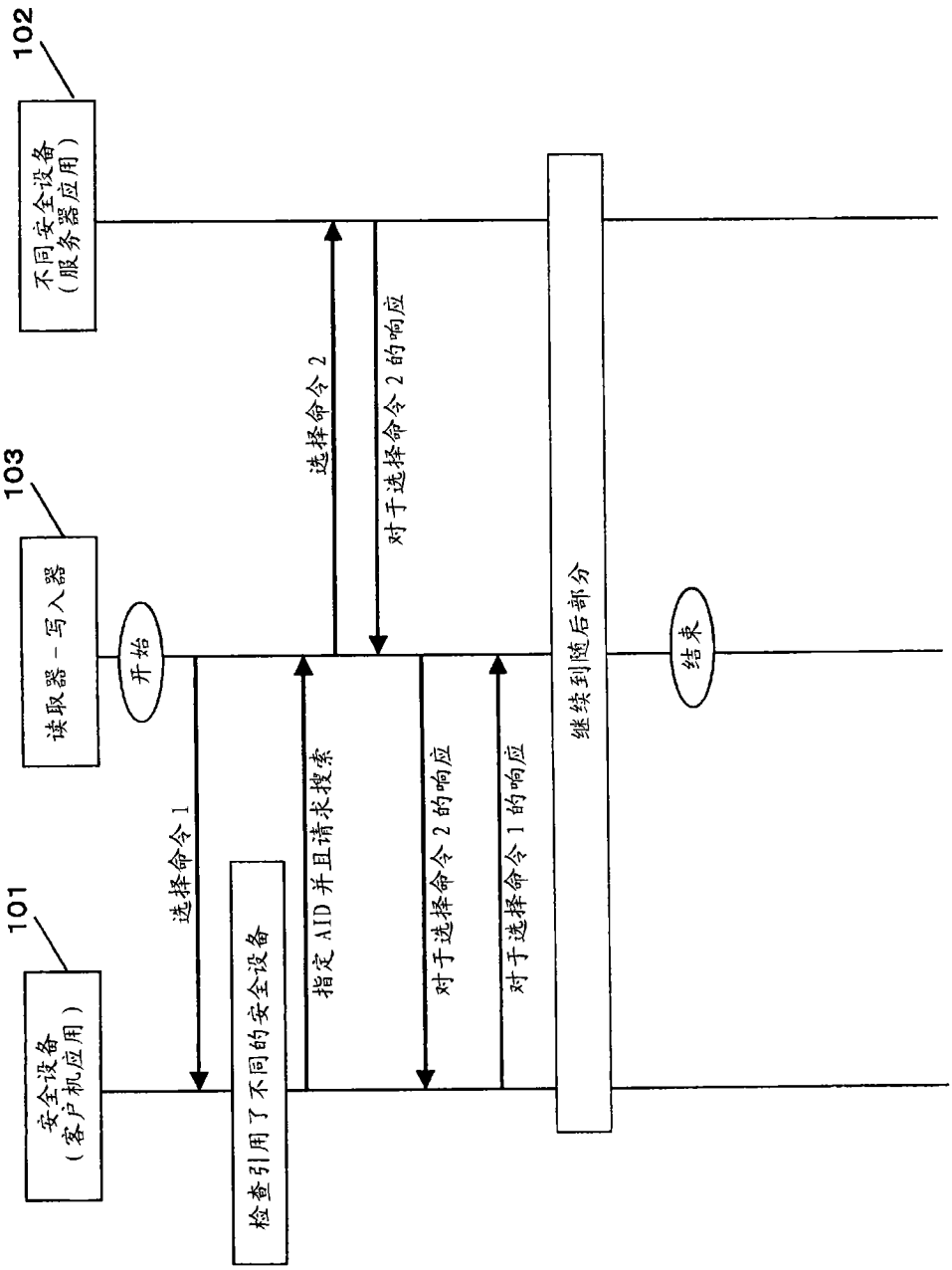

102
不同安全设备
（服务器应用）
103
读取器－写入器
101
安全设备
（客户机应用）
开始
选择命令 1
检查引用了不同的安全设备
选择命令 2
指定 AID 并且请求搜索
对于选择命令 2 的响应
对于选择命令 1 的响应
继续到随后部分
结束

图 19

2001授权码表

索引	客户机应用的标识符	引用对象应用的标识符	方法 ID	自变量的数量
0	0102030405	102030405060	02	02
1	0607080090a	102030405060	02	02
2	0b0c0d0e0f10	102030405060	02	02

图 20

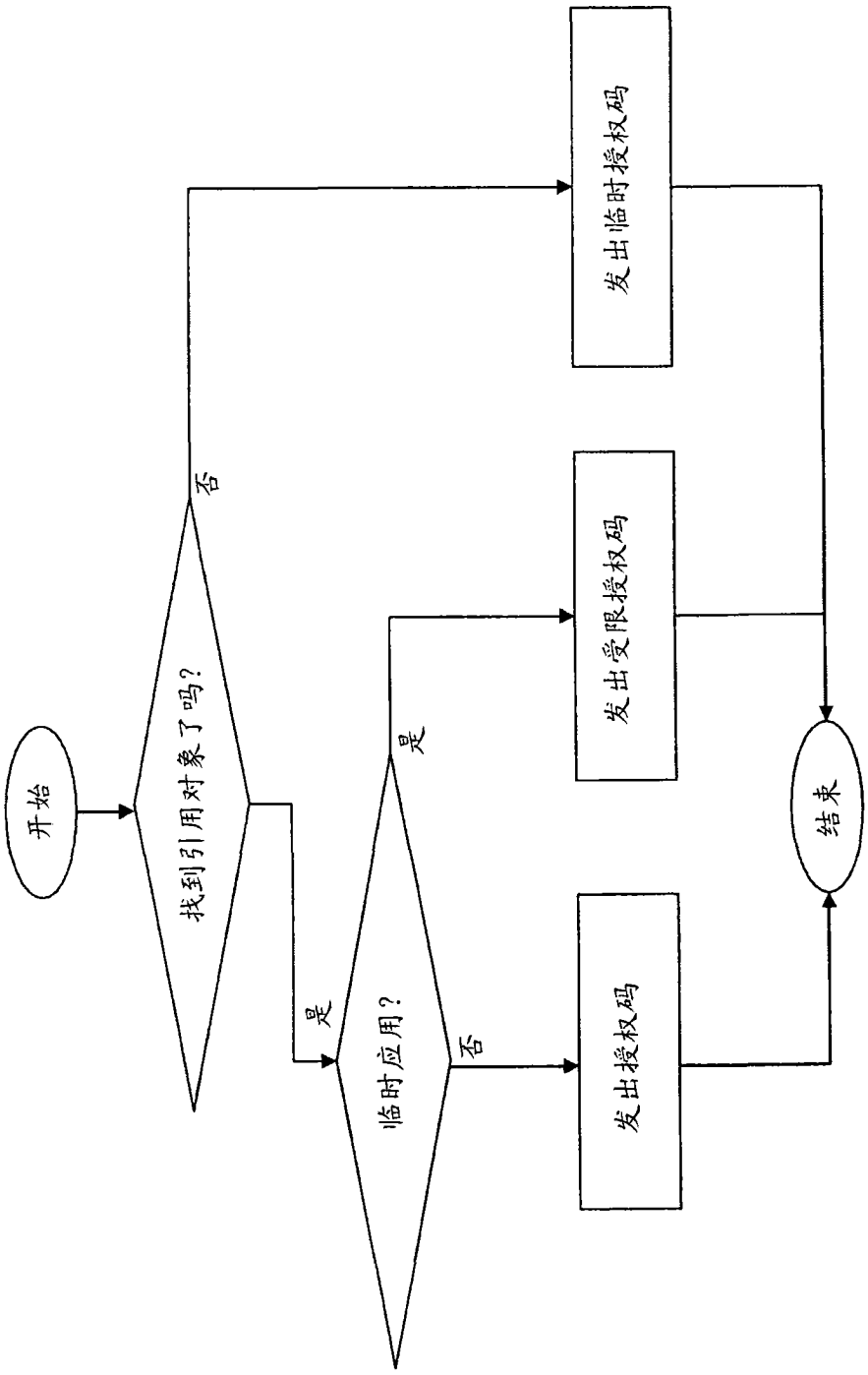


图 21

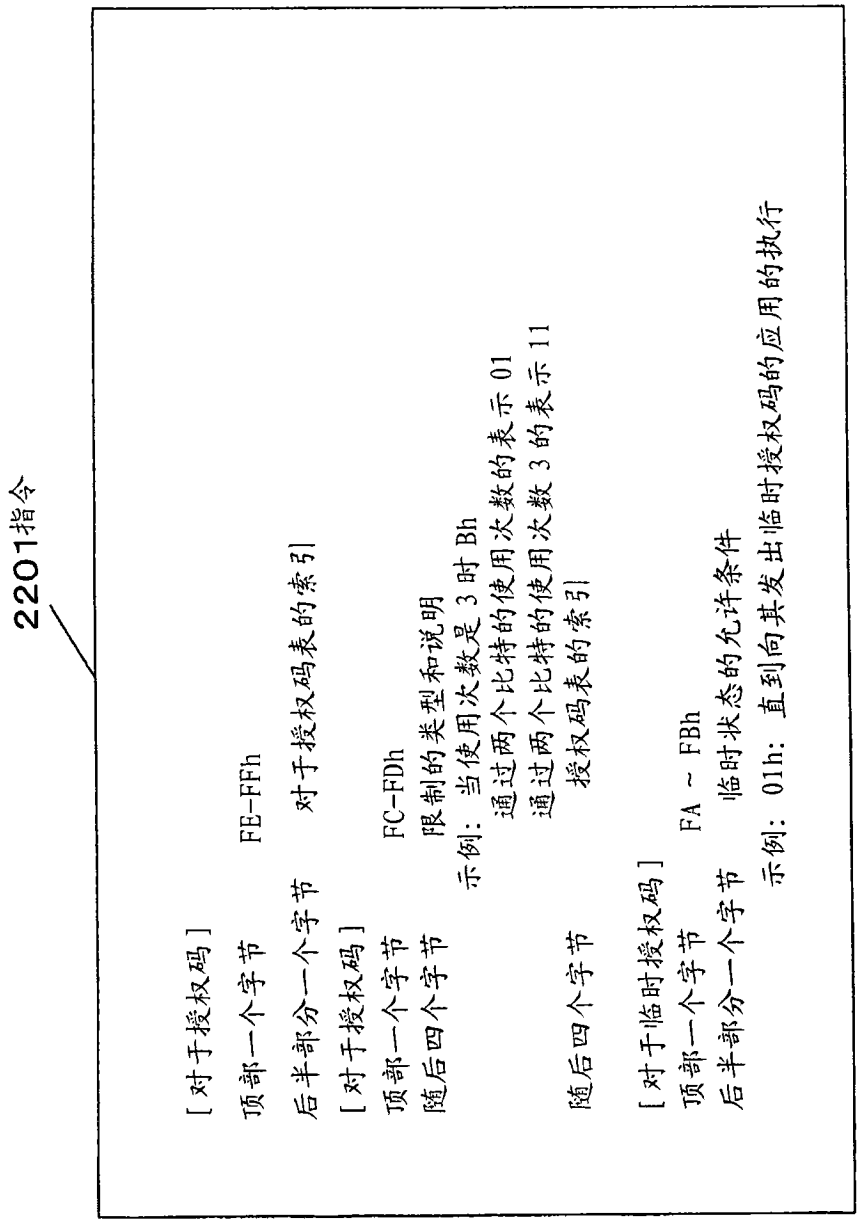

2201指令
[对于授权码]
顶部一个字节 FE-FFh
后半部分一个字节 对于授权码表的索引
[对于授权码]
顶部一个字节 FC-FDh
随后四个字节 限制的类型和说明
示例：当使用次数是 3 时 Bh
通过两个比特的使用次数的表示 01
通过两个比特的使用次数 3 的表示 11
授权码表的索引
随后四个字节
[对于临时授权码]
顶部一个字节 FA ~ FBh
后半部分一个字节 临时状态的允许条件
示例：01h：直到向其发出临时授权码的应用的执行

图 22

2301 临时授权码管理表

索引	客户机应用的标识符	引用对象应用的标识符	地址计算数据
0	0102030405	1020304050 60	01800000
1			
2			

图 23

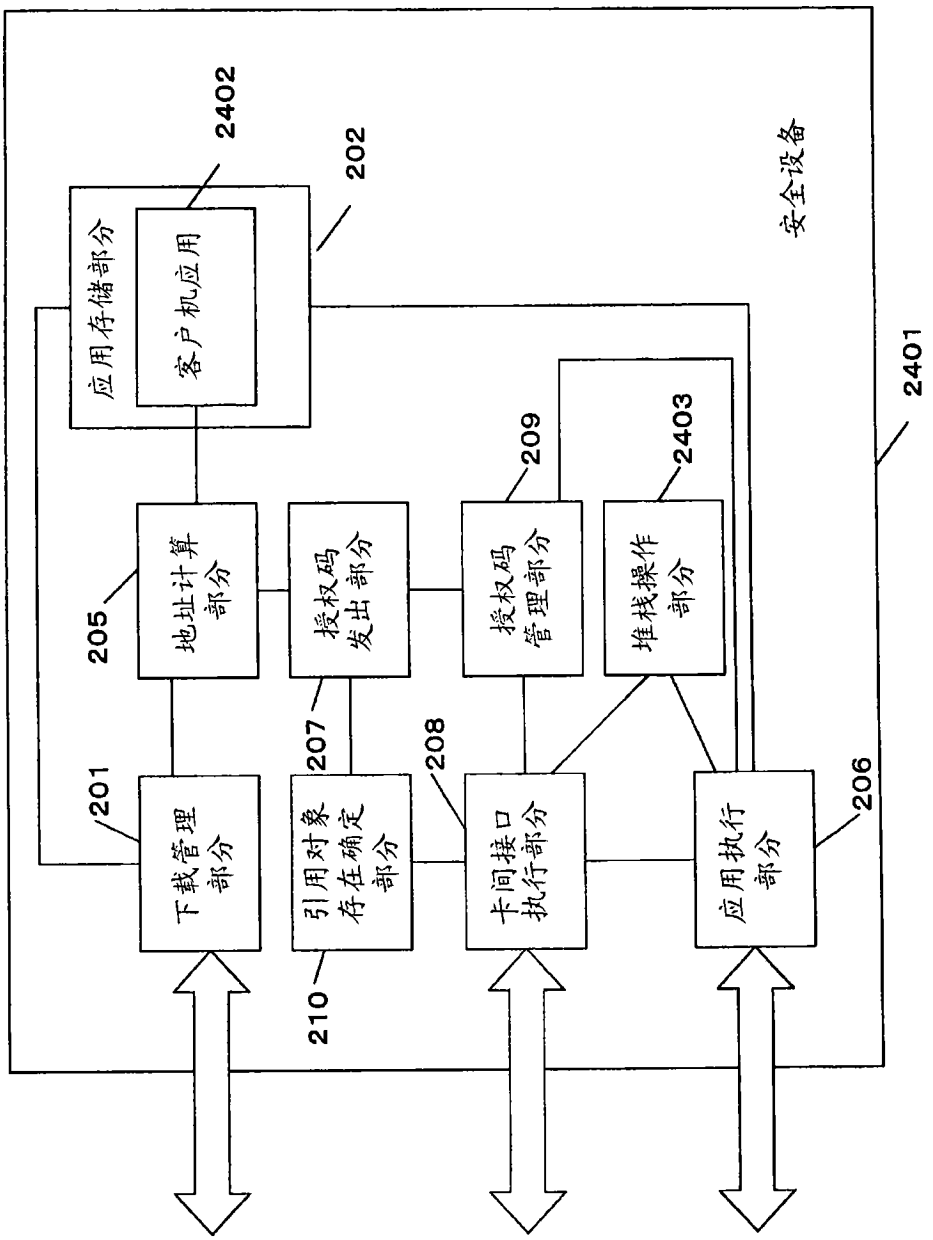

安全设备
2401
2402
202
应用存储部分
客户机应用
205
地址计算部分
207
授权码发出部分
209
授权码管理部分
2403
堆栈操作部分
201
下载管理部分
208
引用对象存在确定部分
卡间接口执行部分
206
应用执行部分
210

图 24

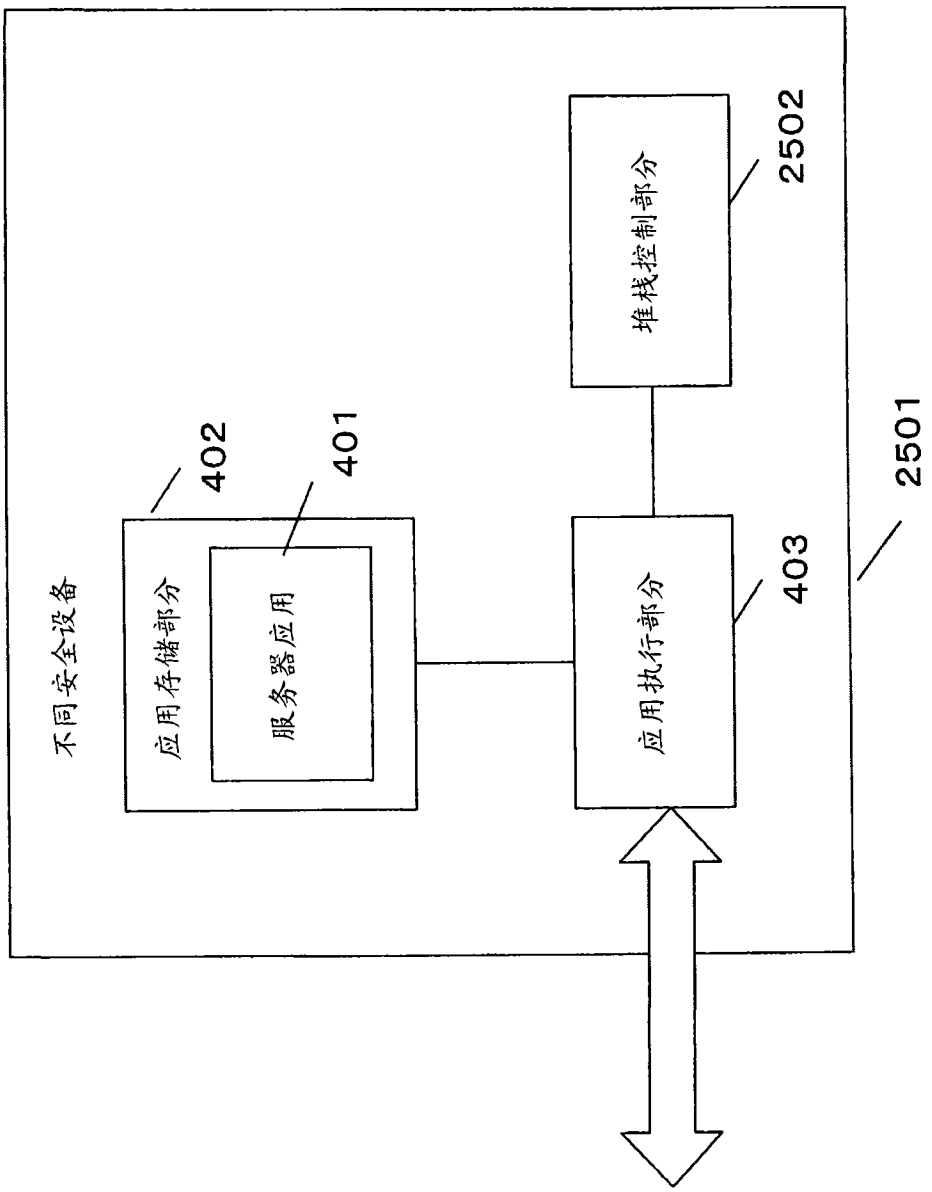


图 25

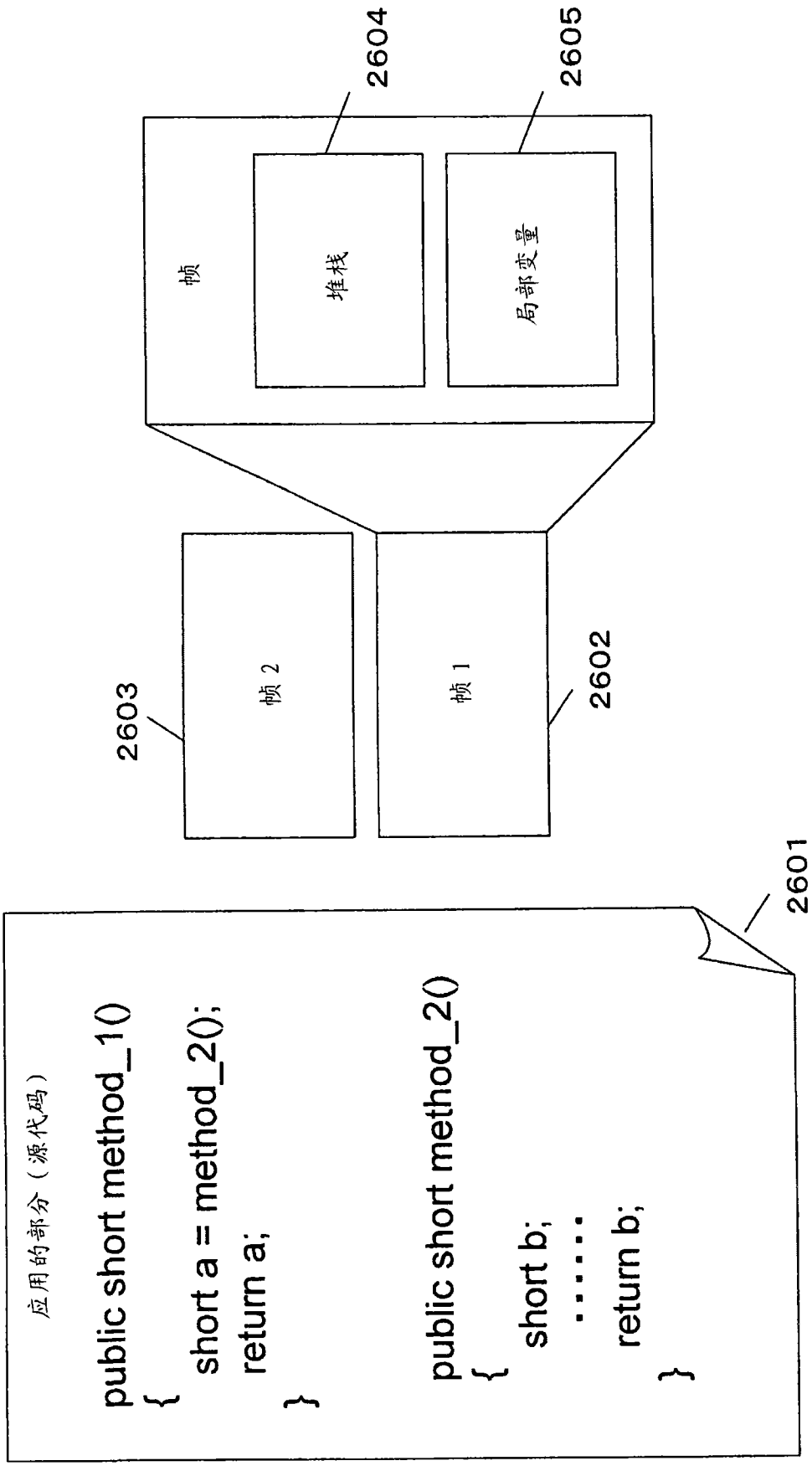

应用的部分（源代码）
public short method_1()
{
short a = method_2();
return a;
}
public short method_2()
{
short b;
……
return b;
}
2601
帧 1
帧 2
2602
2603
帧
堆栈
局部变量
2604
2605

图 26

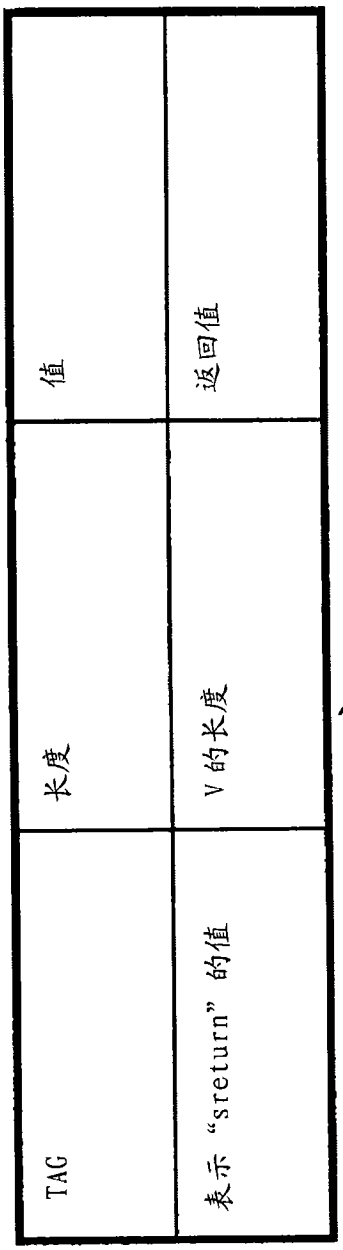


图 27

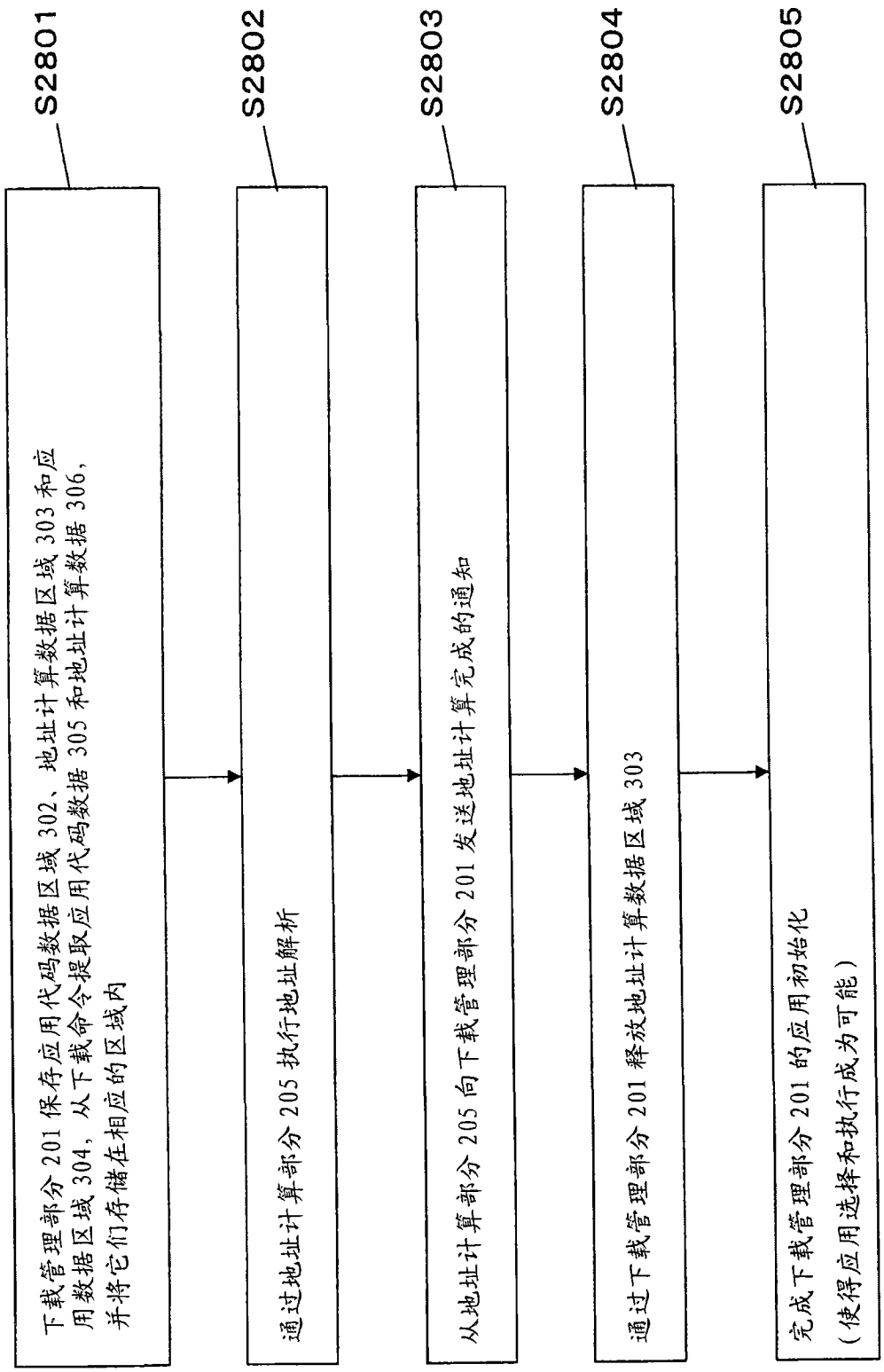

S2801
下载管理部分 201 保存应用代码数据区域 302、地址计算数据区域 303 和应用数据区域 304，从下载命令提取应用代码数据 305 和地址计算数据 306，并将它们存储在相应的区域内
S2802
通过地址计算部分 205 执行地址解析
S2803
从地址计算部分 205 向下载管理部分 201 发送地址计算完成的通知
S2804
通过下载管理部分 201 释放地址计算数据区域 303
S2805
完成下载管理部分 201 的应用初始化
（使得应用选择和执行成为可能）

图 28

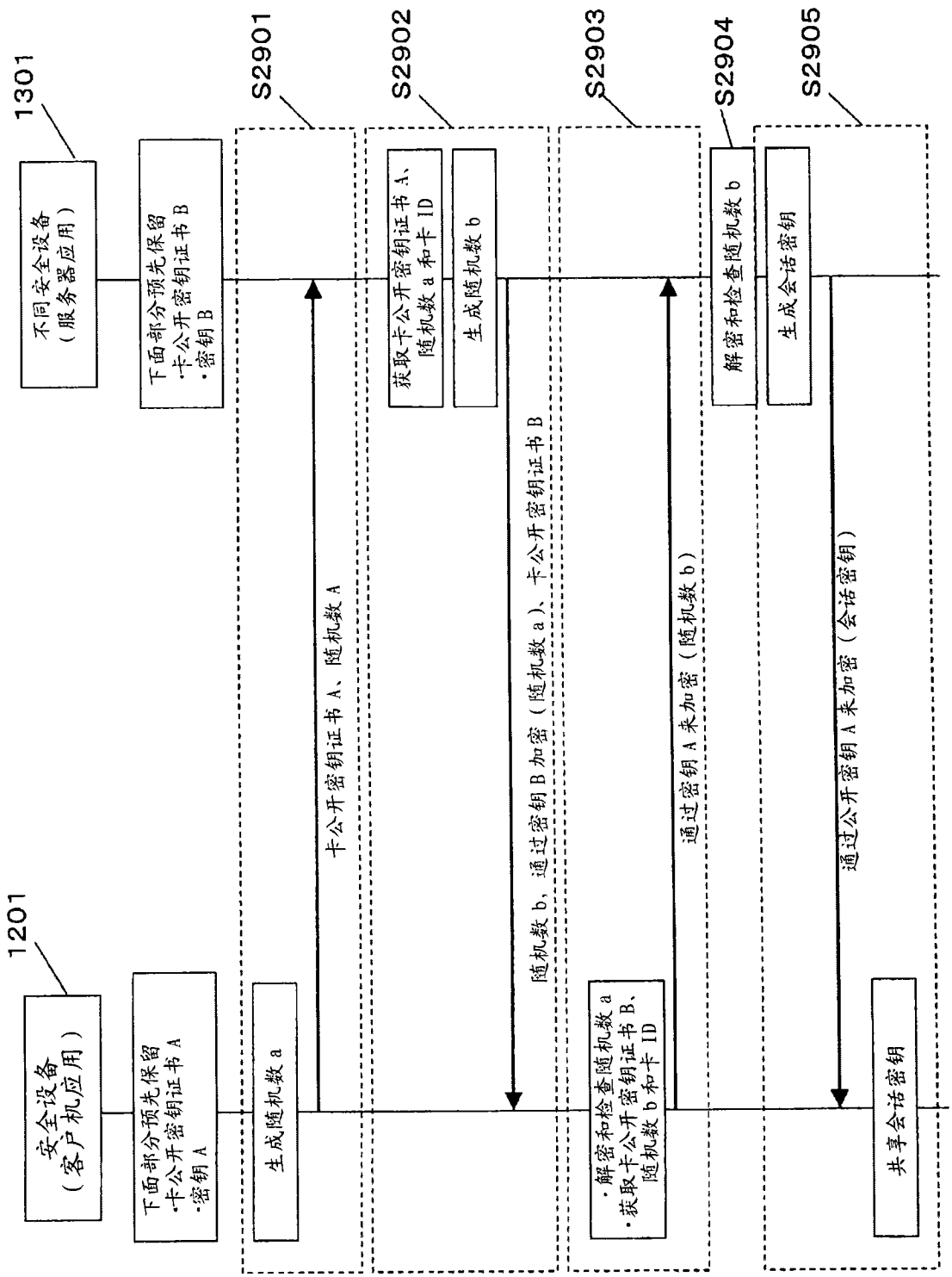

1201
安全设备
（客户机应用）
1301
不同安全设备
（服务器应用）
下面部分预先保留
·卡公开密钥证书 A
·密钥 A
下面部分预先保留
·卡公开密钥证书 B
·密钥 B
S2901
生成随机数 a
卡公开密钥证书 A、随机数 A
S2902
获取卡公开密钥证书 A、
随机数 a 和卡 ID
生成随机数 b
随机数 b，通过密钥 B 加密（随机数 a）、卡公开密钥证书 B
S2903
·解密和检查随机数 a
·获取卡公开密钥证书 B、
随机数 b 和卡 ID
通过密钥 A 来加密（随机数 b）
S2904
解密和检查随机数 b
S2905
生成会话密钥
通过公开密钥 A 来加密（会话密钥）
共享会话密钥

图 29

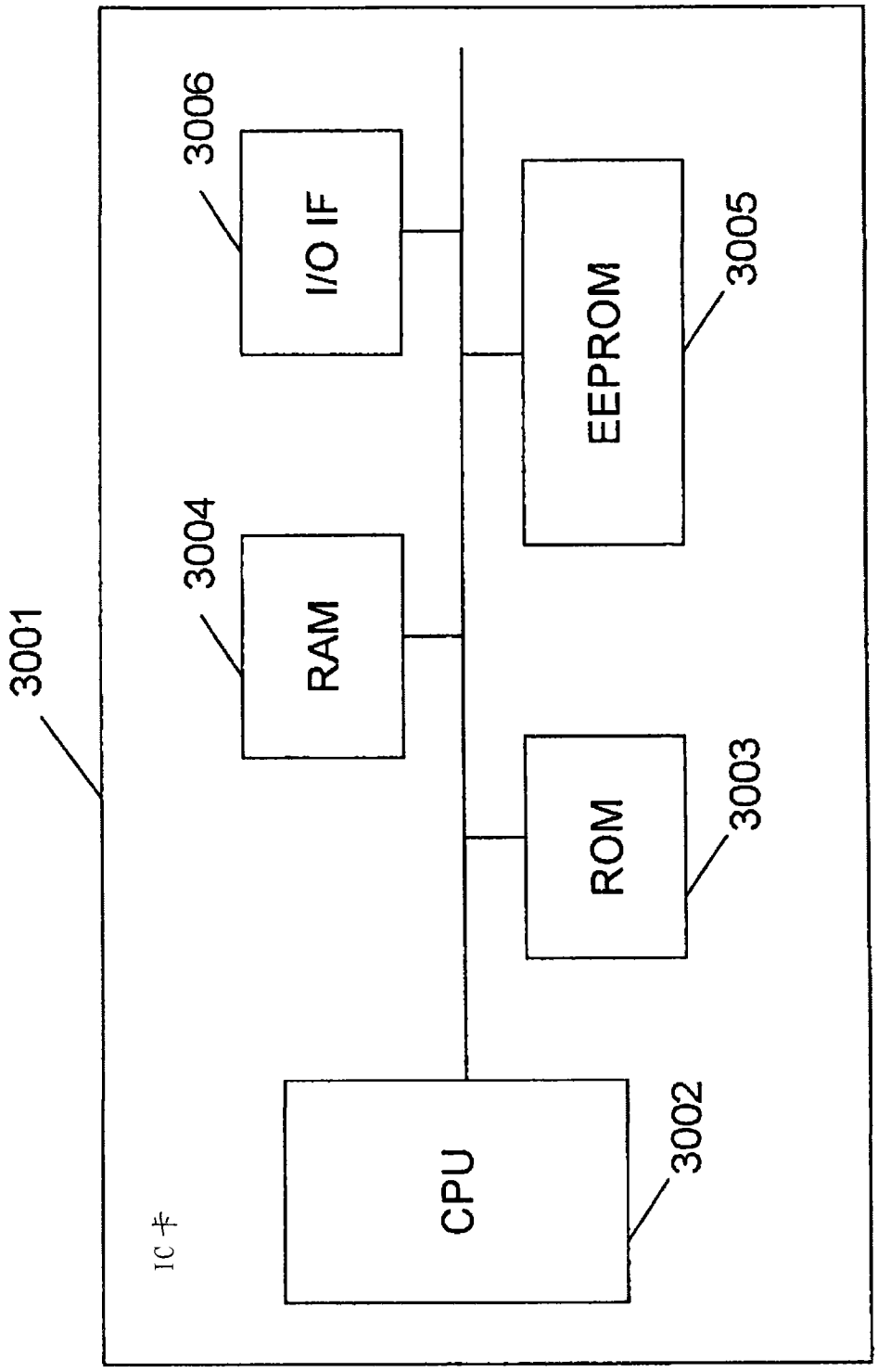


图 30

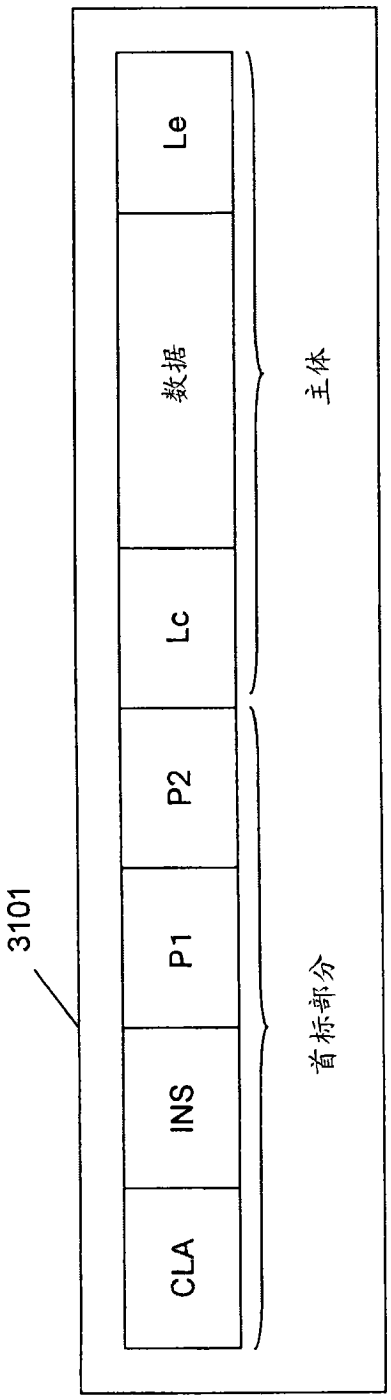


图 31

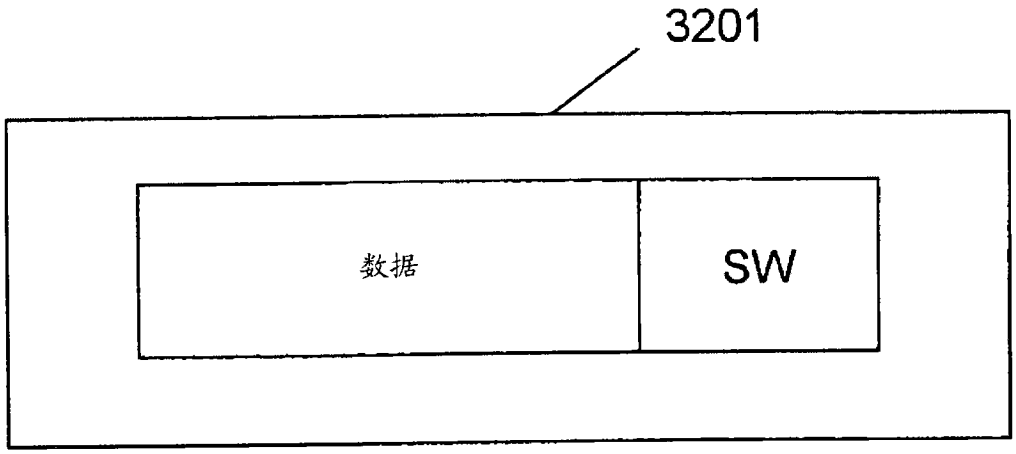


图 32

```
SHAREABLE DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

SHAREABLE-Protocol ::= CHOICE{
        msgStart                Start,                  --对应于命令 1
        respRequestHello        RequestHelloResponse,   --对应于响应 1101
        msgParentHello          ParentHello,            --对应于选择命令 1102
        respParentHello         ParentHelloResponse,    --对应于响应 1103
        msgNofityInfo           NofityInfo,             --响应于共享命令 1104
        respNotifyInfo          NofityInfoResponse,     --对应于响应 1105
        msgInvoke               Invoke,                 --对应于调用命令 1106

        respInvoke              InvokeResponse,         --对应于响应 1107
        msgNotifyResults        NotifyResults,          --对应于共享命令 1108
        msgNotifyResults        NotifyResultsResponse   --对应于响应 1109
    }

Start ::=AID

RequestHelloResponse ::=SEQUENCE{
        parentAID               AID,
        responseStatus          ErrorCode}

ParentHello ::=AID

ParentHelloResponse ::=SEQUENCE{
        ins                     INS,
        objectID                ObjectID,
        responseStatus          ErrorCode}
```

3301

图 33a

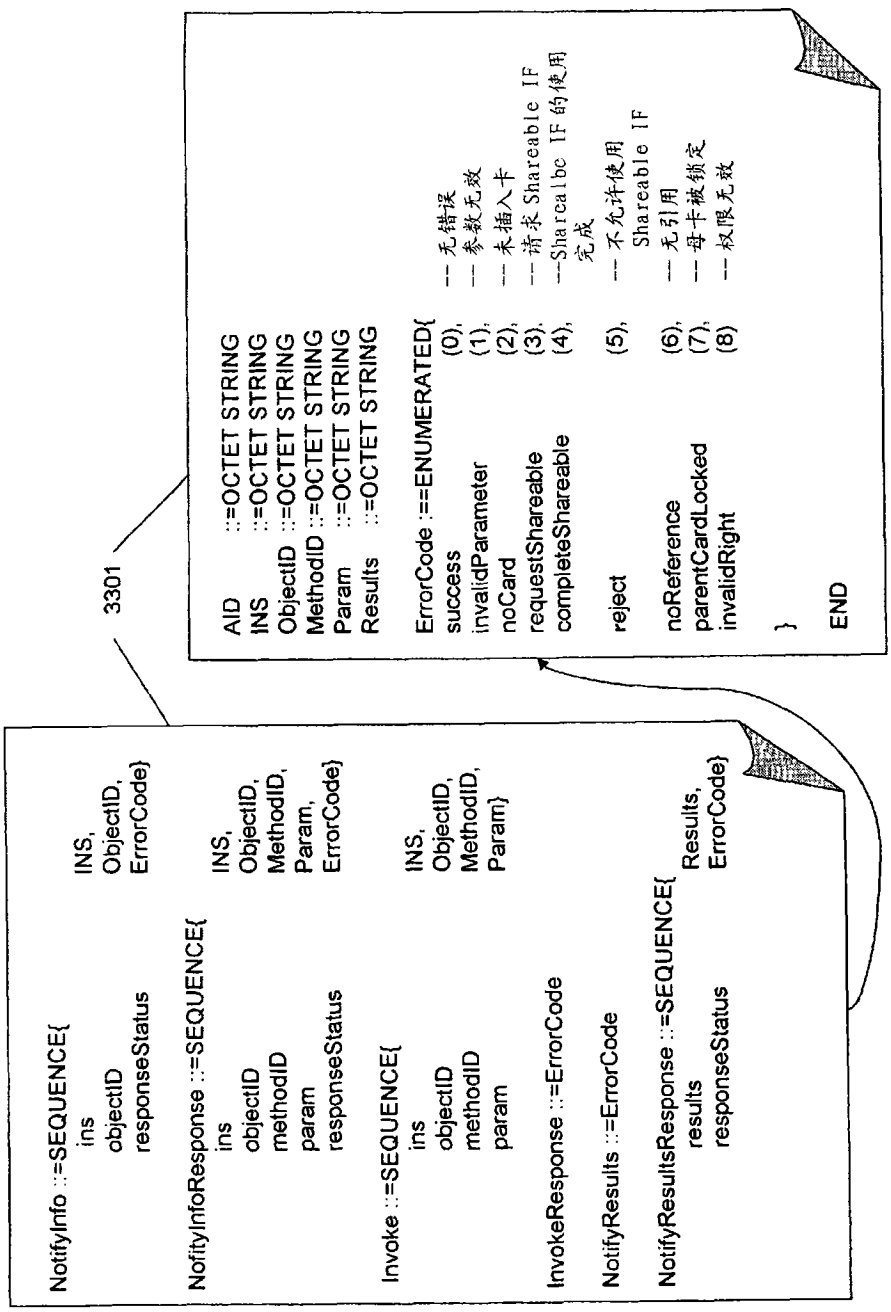

NotifyInfo ::=SEQUENCE{
ins INS,
objectID ObjectID,
responseStatus ErrorCode}
NotifyInfoResponse ::=SEQUENCE{
ins INS,
objectID ObjectID,
methodID MethodID,
param Param,
responseStatus ErrorCode}
Invoke ::=SEQUENCE{
ins INS,
objectID ObjectID,
methodID MethodID,
param Param}
InvokeResponse ::=ErrorCode
NotifyResults ::=ErrorCode
NotifyResultsResponse ::=SEQUENCE{
results Results,
responseStatus ErrorCode}
3301
AID ::=OCTET STRING
INS ::=OCTET STRING
ObjectID ::=OCTET STRING
MethodID ::=OCTET STRING
Param ::=OCTET STRING
Results ::=OCTET STRING
ErrorCode ::=ENUMERATED{
success (0), --无错误
invalidParameter (1), --参数无效
noCard (2), --未插入卡
requestShareable (3), --请求 Shareable IF
completeShareable (4), --Sharealbe IF 的使用完成
reject (5), -- 不允许使用 Shareable IF
noReference (6), -- 无引用
parentCardLocked (7), --母卡被锁定
invalidRight (8) --权限无效
}
END

图 33b