[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G06K 7/00
H04Q 7/32

[12] 发明专利申请公开说明书

[21] 申请号 200410075599.1

[43] 公开日 2005 年 8 月 17 日

[11] 公开号 CN 1655172A

[22] 申请日 2004.12.15
[21] 申请号 200410075599.1
[30] 优先权
[32] 2003.12.15 [33] JP [31] 416381/2003
[32] 2003.12.15 [33] JP [31] 416650/2003
[71] 申请人 松下电器产业株式会社
地址 日本大阪府
[72] 发明人 峰村淳 小泉正彦

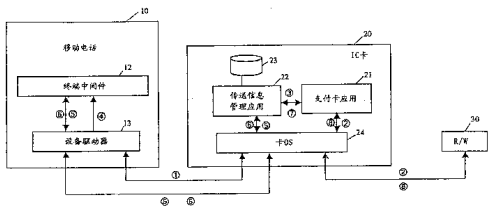
[74] 专利代理机构 北京市柳沈律师事务所
代理人 黄小临 王志森

权利要求书 4 页 说明书 22 页 附图 11 页

[54] 发明名称 安全设备和信息处理系统

[57] 摘要

本发明的 IC 卡包括第一通信单元、第二通信单元、和可以访问卡应用的传送信息管理单元。传送信息管理单元保存彼此相关的从外部 R/W 经由第一通信单元传送的处理标识符以及从移动电话经由第二通信单元传送的 PIN。从外部 R/W 接收到处理标识符和数据请求的卡应用读取其相应处理标识符与从传送信息管理单元接收的处理标识符相匹配的 PIN，并且将该 PIN 传送给外部 R/W。因此，即使在移动电话落在其他恶意的人手中，而且 PIN 已写入安 IC 卡的情况下，也不会从 IC 卡中读出 PIN，除非从外部 R/W 传送的处理标识符与相应于 PIN 的处理标识符相匹配。



ISSN1008-4274

1、 一种安全设备，包括:

第一通信单元;

第二通信单元；以及

一个或多个卡功能单元;

传送信息管理单元，其可以访问所有卡功能单元;

其中该传送信息管理单元保存互相相关的从外部读/写器经由第一通信单元传送的处理标识符以及从信息处理装置经由第二通信单元传送的数据;以及

经由第一通信单元接收到来自外部读/写器的处理标识符和数据请求的所述卡功能单元，在相应处理标识符与从传送信息管理单元接收的处理标识符相匹配时读取数据，并且将数据传送给外部读/写器。

2、 如权利要求 1 所述的安全设备，其中所述传送信息管理单元从保存数据中选择相应于与由卡功能单元接收的处理标识符匹配的处理标识符的数据；以及所述卡功能单元获取所选择的数据。

3、 如权利要求 1 所述的安全设备，其中按照时间更新从外部读/写器传送的处理标识符。

4、 如权利要求 1 所述的安全设备，其中当所述卡功能单元没有从传送信息管理单元获得数据而未成功地向外部读/写器传送数据时，在下一个通信周期中，通过在预定时间内进行的第一通信单元将与前一 pp 信息相同的处理标识符从外部读/写器重新传送到卡功能单元。

5、 一种安全设备，包括:

第一通信单元;

第二通信单元；以及

一个或多个卡功能单元;

传送信息管理单元，其可以访问所有卡功能单元;

其中经由第一通信单元接收到来自外部读/写器的数据要求的所述卡功能单元读取保存在传送信息管理单元中的从信息处理装置传送的数据，并且将该数据传送给外部读/写器，而且当数据没有在预定时间内读取时，所述传送信息管理单元根据从信息处理装置经由第二通信单元传送的指令清除数

据。

6、 如权利要求 1 或 5 所述的安全设备，其中所述第一通信单元执行非接触通信，而所述第二通信单元执行接触通信。

7、 一种安装有如权利要求 1 所述的安全设备的信息处理装置，包括：

状态监视单元，用于通过安全设备的第一通信单元监视通信结束；以及

中间件，一旦所述状态监视单元检测到通信结束，该中间件就通过安全设备的第二通信单元访问安全设备的传送信息管理单元，并且获取保存在传送信息管理单元中的处理标识符和数据请求；

其中所述中间件将响应于数据请求而输入的数据和处理标识符传送到传送信息管理单元。

8、 一种安装有如权利要求 5 所述的安全设备的信息处理装置，包括：

状态监视单元，用于通过安全设备的第一通信单元监视通信结束；以及

中间件，用于通过安全设备的第二通信单元将输入数据写入安全设备的传送信息管理单元；以及

其中当没有在预定时间内执行通过安全设备的第一通信单元进行的通信处理时，所述中间件就将写入传送信息管理单元的数据清除。

9、 如权利要求 7 或 8 所述的信息处理装置，其中所述安全设备以可拆分方式附接到该信息处理装置。

10、 如权利要求 7 或 8 所述的信息处理装置，其中所述安全设备集成地嵌入到该信息处理装置中。

11、 一种安全设备，包括：

第一通信单元；

第二通信单元；以及

一个或多个卡功能单元；以及

传送信息插入单元，其可以访问所有卡功能单元；

其中经由第一通信单元从外部读/写器接收到对提供服务所需的个人身份信息的请求的所述卡功能单元、读取保存在传送信息插入单元中的个人身份信息，并且将该信息传送给外部读/写器；以及

在所述卡功能单元与外部读/写器经由第一通信单元开始进行通信之前，所述传送信息插入单元保存从信息处理装置经由第二通信单元写入的个人身份信息。

12、 一种安全设备，包括:

第一通信单元;

第二通信单元;

一个或多个卡功能单元;

传送信息插入单元，其可以访问所有卡功能单元;

其中经由第一通信单元从外部读/写器接收到对提供服务所需的个人身份信息的请求的所述卡功能单元、在个人身份信息保存在传送信息插入单元中的情况下读取个人身份信息并且将该信息传送给外部读/写器，或者在个人身份信息没有保存在传送信息插入单元中的情况下，将关于服务的特定信息写入到传送信息插入单元中；以及

所述传送信息插入单元经由第二通信单元向信息处理装置提供关于服务的特定信息，并且保存从信息处理装置写入的个人身份信息。

13、 如权利要求 11 或 12 所述的安全设备，其中所述第一通信单元执行非接触通信，而所述第二通信单元执行接触通信。

14、 一种安装有如权利要求 11 所述的安全设备的信息处理装置，包括:

状态监视单元，用于通过安全设备的第一通信单元监视通信结束；以及

中间件，用于显示输入个人身份信息的屏幕和将所输入的个人身份信息经由安全设备的第二通信单元写入安全设备的传送信息插入单元。

15、 一种安装有如权利要求 12 所述的安全设备的信息处理装置，包括:

状态监视单元，用于通过安全设备的第一通信单元监视通信结束；以及

中间件，一旦所述状态监视单元检测到通信结束，该中间件就通过安全设备的第二通信单元访问安全设备的传送信息插入单元，并且获取在传送信息插入单元中保存的关于服务的特定信息，以及

该中间件根据获取的信息显示关于服务的列表信息，以及显示用于输入提供服务所需的个人身份信息的屏幕，并且将所输入的个人身份信息写入传送信息插入单元。

16、 如权利要求 15 所述的信息处理装置，其中该信息处理装置根据所获取的信息显示服务列表信息，并提示输入提供服务所需的服务特定信息和个人身份信息，并且将所输入的服务特定信息和个人身份信息写入到传送信息插入单元。

17、 如权利要求 14 或 15 所述的信息处理装置，其中所述安全设备以可

拆分方式附接到该信息处理装置。

18、 如权利要求 14 或 15 所述的信息处理装置，其中所述安全设备集成地嵌入到该信息处理装置中。

19、 一种终端装置，用于与配备有多个卡功能单元的安全设备进行通信，并执行从多个可用服务中选择的服务；

其中该终端装置激活相应于所选服务的卡功能单元，并请求提供服务所需的个人身份信息，而且在从卡功能单元传送的个人身份信息为异常的情况下，选择另一个服务，并且激活相应于该服务的卡功能单元及请求提供该服务所需的个人身份信息。

安全设备和信息处理系统

技术领域

本发明涉及一种例如 IC 卡的安全设备，以及一种安装了该安全设备的信息处理装置，例如移动电话，所述信息处理装置防止写入到所述安全设备的数据，例如 PIN，被滥用的事故。本发明还涉及一种例如 IC 卡的安全设备，一种安装了该安全设备的信息处理装置，例如移动电话，以及一种与上述安全设备通信以进行服务的例如 POS 终端的终端装置，所述终端装置使得在执行卡功能时所需要的个人身份信息的输入变得容易。

背景技术

近年来，IC 卡已经广泛的应用到具有收费功能的电子支付卡、电子月票、以及预付火车票中。最近，随着微型制造技术的提高，在市场上已经推出具有相对大容量的 IC 卡。这样的 IC 卡，其中存储了执行卡服务的多种卡应用，可以被用作支持多种应用的多应用卡。

IC 卡的通信系统包括接触通信系统，其读/写器与 IC 卡的电子触点的接触允许对记录信息的读/写，以及非接触通信系统，其使用无线通信而非与读/写器的物理接触进行信息交换。

IC 卡的国际标准包括 ISO7816 和 ISO14443。这些国际标准描述了 IC 卡上的卡应用和读/写器上的终端应用之间的数据交换是基于从终端应用发送到卡应用的“命令”，以及从卡应用发送到终端应用的“响应”。指定命令或响应的格式的 APDU(应用协议数据单元,Application Protocol Data Unit)是由上述标准规定的。由此，所述 IC 卡仅仅以被动方式操作。

近来，将能够进行接触通信和非接触通信的芯片形状 IC 卡安装在移动电话中，并且使用所述移动电话代替电子钱包和电子月票已是常识。例如，如果预付火车票信息被记录在 IC 卡上，当用户操作他/她移动电话上的某些键来显示剩余金额时，该指令就从移动电话经由接触通信输入到 IC 卡中，而 IC 卡上的剩余金额信息就被读出并显示在移动电话的屏幕上。当将移动电话放置得对着车站的自动检票口时，读取或重写信息数据指令就经由非接触通

信输入到移动电话的 IC 卡中，而记录在 IC 卡上的剩余金额数据就根据这一指令进行更新。

日本专利公开专利第 2003-60748 描述了以下装置，其在通过安装在移动电话上的 IC 卡成功进行非接触通信时，使用移动电话上的显示单元显示卡功能的成功完成。所述 IC 卡开始多个卡应用中由外部读/写器指定的卡应用，根据所使用的服务执行与外部读/写器的基于卡的通信(非接触通信)。在成功完成基于卡通信的基础上，IC 卡将指示通信结束的通知信号和应用 ID 发送到移动电话的控制器。接收到信息的控制器根据应用 ID 从移动电话的显示单元输出预定控制信息。

安装了 IC 卡的移动电话包括小键盘、显示器、通信功能块、以及应用执行功能块。通过与由 IC 卡经由非接触通信进行的卡处理相协调地使用这样的移动电话功能，可以实现便利性、操作性和功能性更强的服务。日本专利公开第 2003-60748 描述的装置致力于通过利用移动电话的显示单元与 IC 卡的非接触通信处理相协调地提供显示。

符合相应国际标准的 IC 卡能够进行返回对经由非接触通信从外部读/写器接收的命令的响应的被动操作。不像日本专利公开第 2003-60748 所描述的 IC 卡，这样的 IC 卡自身不能向移动电话的控制器传送通知信号或应用 ID。

发明者新近开发出了一种 IC 卡，该 IC 卡能够根据国际标准有效传送关于基于来自外部读/写器的指令进行的卡处理的信息。图 7 示出了 IC 卡 400 和安装了 IC 卡 400 的移动电话 300 的结构，其中由移动电话 300、IC 卡 400 和外部读/写器 500 协调执行的处理顺序由圈绕数字来指示。

IC 卡 400 包括：多个卡应用 410，用于执行由服务提供者创建的各种不同的服务；信息传送卡应用 420，用于集中传送/接收到达/来自移动电话 300 的信息；信息存储器部分 430，用于临时存储要传送的信息；以及卡 OS 440，用于执行通信和文件管理。所述移动电话 300 包括：终端应用 310，用于执行与卡应用 410 处理相协调的操作；中间件(middleware)320，用于执行到终端应用 310 的信息传送；以及设备驱动器 330，用于控制移动电话 300 的操作。

IC 卡 400 上的所有卡应用 410 都可以访问信息传送卡应用 420，以便将从外部读/写器 500 发送到卡应用 410 的信息写入到信息传送卡应用 420 的信息存储部分 430 中。

一旦与信息传送卡应用 420 进行了互相验证，移动电话 300 的中间件 320 就可以无限制地访问信息传送卡应用 420。

通过经由设备驱动器 330 进行轮询，移动电话 300 的中间件 320 监视 IC 卡 400 的状态(1)。当用户将移动电话 300 对着外部读/写器 30 放置时，在外部读/写器 500 的非接触通信范围中的 IC 卡 400 就被激活，而外部读/写器 500 指定的卡应用 410 执行由外部读/写器 500 指令的处理(32)。根据这一处理，卡应用 410 将现在需要发送到移动电话 300 的信息写入到信息传送卡应用 420(3)。

该信息包括终端应用(包括中间件)的名称、要传送到终端应用的信息、以及所请求的卡应用的 ID。

检测到 IC 卡 400 非接触通信的结束的移动电话 300 的设备驱动器 330 通知中间件 320 该事件(4)。中间件 320 执行与信息传送卡应用 420 的相互验证，并且访问信息传送卡应用 420，然后获得其中保存的信息(5)。中间件 320 基于从信息传送卡应用 420 获得的信息激活指定的终端应用 310。终端应用 310 执行指定处理。当指定了中间件 320 时，中间件 320 自身执行处理(6)。

例如，在支付终端的外部读/写器 500 请求输入信用支付处理所需的个人身份号码(PIN)时，已解释了所获得的信息的中间件 320 就在移动电话 300 的显示器上显示 PIN 输入窗口。当用户输入 PIN 时，中间件 320 就将 PIN 写入信息传送卡应用 420。

PIN 信息由卡应用 410 读取，并根据外部读/写器 500 的指令被发送到外部读/写器 500，其中当用户再一次将移动电话 300 对着外部读/写器 500 放置时卡应用 410 被激活。在连接到外部读/写器 30 的中心进行 PIN 的匹配。如果匹配成功，就执行支付处理。

在装置上，如果在 PIN 被写入信息传送卡应用 420 的信息存储部分 430(即，完成支付处理之前的状态)中的状态下移动电话 300 被偷或丢失，并落在别人手里，则 PIN 可能被滥用以支付未经移动电话主人的允许而购买的商品。

在移动电话上安装符合国际标准的 IC 卡并使移动电话执行与通过 IC 卡上的非接触通信进行的卡处理相协调的操作需要新的基本原理(philosophy)，而且存在许多问题需要解决。

例如，在安装了 IC 卡的移动电话对着支付终端的外部读/写器放置以执

行支付处理的情况下，输入支付所要求的个人身份号码(PIN)的尝试涉及诸如下列问题：何时输入 PIN 而不中断 IC 卡的非接触通信，如何从 IC 卡向移动电话发送 PIN 输入请求，以及如何经由 IC 卡将从移动电话输入的 PIN 发送到支付终端。

在安装在移动电话上的 IC 卡是支持多个服务的多应用卡的情况下，要输入的 PIN 必须支持待激活的支付服务(待激活的应用)。这就提出了用户应该如何输入支持卡应用 PIN 的问题。

当用户将安装了多应用卡的移动电话对着外部读/写器放置时，执行单服务的单元的外部读/写器对 IC 卡指定卡应用，随后是卡应用与外部读/写器之间的卡通信。在用户输入支持卡应用的 PIN 情况下，用户必须在输入 PIN 之前，从大量保存在 IC 卡中的卡应用中选择相关卡应用。这对于用户来说是非常麻烦的。

在这种情况下，当显示保存在 IC 卡中的卡应用列表(卡应用 ID 的列表)时，选择卡应用的工作量就减小了，虽然出于安全的观点通常 IC 卡不提供保存在其上的卡应用列表。

在多应用卡具有公司 A 和公司 B 的信用卡功能，而且外部读/写器支持这两种服务的情况下，希望使用来自公司 A 的卡功能的用户选择相关卡应用，并输入 PIN，这也要求大量选择卡功能的工作量。

发明内容

本发明解决了上述问题，其目的在于提供一种能够防止写入到安全设备的数据，例如 PIN 被滥用的安全设备和信息处理装置。

本发明解决了上述问题，其目的在于提供一种能够简化用户执行卡服务所需的 PIN 的输入，并由此增强卡功能便利性的安全设备、信息处理装置和终端装置。

由此，本发明提供了一种安全设备，包括第一通信单元、第二通信单元和一个或多个卡功能单元(卡应用)，其特征在于该安全设备包括可以访问所有卡功能单元的传送信息管理单元，该传送信息管理单元相互结合地保存从外部读/写器经由第一通信单元发送的处理标识符以及从信息处理装置经由第二通信单元发送的数据，经由第一通信单元接收到来自外部读/写器的处理标识符和数据请求的该卡功能单元，在相应处理标识符匹配所接收的处理标

识符时从传送信息管理单元读取数据，并且将数据发送到外部读/写器。

因此，即使在信息处理装置落入另一个恶意的人手中并且包括 PIN 的数据已写入安全设备的情况下，也不能从安全设备读取数据，除非从处理终端传送的处理标识符与相应于数据的处理标识符相匹配。这防止了使用该数据的非法处理。

该安全设备的特征在于：传送信息管理单元从保存数据中选择相应于与由卡功能单元接收的处理标识符匹配的处理标识符的数据，而卡单元获得所选择的数据。

传送信息管理单元从保存数据选择符合其自身的相应的数据。

根据本发明，按照时间更新从外部读/写器传送的处理标识符。

因此，当预定时间过去时，从处理终端传送的处理标识符就与相应于数据的处理标识符不同，那么就不再从安全设备中读取数据。

该安全设备特征在于：当卡功能单元未获得来自传送信息管理单元的数据而没有成功地向外部读/写器传送数据时，在下一个通信周期里，通过在预定时间内进行的第一通信单元将与前一 pp 信息相同的处理标识符从外部读/写器重新传送到卡功能单元。

因此，在信息处理装置对着外部读/写器放置以进行支付处理的程序中，即使当首次放置信息处理装置时包括 PIN 的数据没有保存在传送信息管理单元中并且支付处理失败，用户也可以将 PIN 从信息处理装置写入传送信息管理单元，并在预定时间内放置信息处理装置。外部读/写器保存已在支付处理中失败的处理标识符预定时间以在下一次卡处理中重新使用，并从传送信息管理单元中读取相应于处理标识符的数据，由此成功进行支付处理。

本发明提供一种安全设备，包括第一通信单元、第二通信单元、和一个或多个卡功能单元，其特征在于该安全设备包括可以访问所有卡功能单元的传送信息管理单元，经由第一通信单元接收到来自外部读/写器的数据请求的该卡功能单元读取保存在传送信息管理单元中的从信息处理装置传送的数据，并且将该数据传送给外部读/写器，当没有在预定时间内读取数据时，传送信息管理单元就根据从信息处理装置经由第二通信单元传送的指令清除数据。

因此，即使在信息处理装置在其他恶意人手中并且包括 PIN 的数据已写入安全设备的情况下，当经过预定时间，例如 30 秒数据时数据就会被清除。

这防止了使用该数据的非法处理。

根据本发明的安全设备的特征在于第一通信单元执行非接触通信，而第二通信单元执行接触通信。

本发明提供一种安装有所述安全设备的信息处理装置，其特征在于该信息处理装置包括用于通过安全设备的第一通信单元监视通信结束的状态监视单元以及中间件，一旦状态监视单元检测到通信结束，中间件就经由安全设备的第二通信单元访问安全设备的传送信息管理单元，并且获得保存在传送信息管理单元中的处理标识符和数据请求，并且该中间件将响应于数据请求和处理标识符输入的数据传送给传送信息管理单元。

由此，安全设备可以管理彼此相关的由用户输入的包括 PIN 的数据和 pp 信息。在从处理终端传送的处理标识符与相应于数据的处理标识符不匹配的情况下，可以停止从安全设备中读取数据。

本发明提供一种安装有所述安全设备的信息处理装置，其特征在于该信息处理装置包括用于通过所述安全设备的第一通信单元监视通信结束的状态监视单元，以及用于将输入的数据经由安全设备的第二通信单元写入安全设备的传送信息管理单元的中间件，并且当在预定时间内没有经由安全设备的第一通信单元执行通信处理时，该中间件就清除写入到传送信息管理单元的数据。

在预定时间内信息处理装置监视安全设备的状态。在同时不执行对安全设备和外部读/写器的处理的情况下，信息处理装置清除写入安全设备的数据。安全设备以可拆分的方式附接到信息处理装置，或者集成地嵌入到信息处理装置中。

根据本发明的安全设备和信息处理装置防止从安全设备读取数据，而且即使在信息处理装置被偷或丢失并落入了其他恶意的人手中，同时包括 PIN 的数据已写入安全设备的情况下，也可以防止对数据的滥用。

本发明提供一种安全设备，包括第一通信单元、第二通信单元、和一个或多个卡功能单元(卡应用)，其特征在于该安全设备包括可以访问所有卡功能单元的传送信息插入(intervening)单元，并且经由第一通信单元从外部读/写器接收到对提供服务所需的个人身份信息的请求的所述卡功能单元读取保存在传送信息插入单元中的个人身份信息，并且将该信息传送给外部读/写器，而且在卡功能单元与外部读/写器经由第一通信单元进行通信之前，传

送信息插入单元就保存从信息处理装置经由第二通信单元写入的个人身份信息。

首先向安全设备的传送信息插入单元写入用户从信息处理装置(个人身份信息预输入系统)输入的个人身份信息。由外部读/写器激活的卡功能单元从传送信息插入单元读取个人身份信息，并且将信息传送到外部读/写器。外部读/写器连续地更新要被激活的卡功能单元(或卡服务)，直到成功达到个人身份信息的匹配。用户由此只需输入关于期望的服务的个人身份信息以享用期望的服务，而没有选择卡服务的负担。

本发明提供一种安全设备，包括第一通信单元、第二通信单元、和一个或多个卡功能单元(卡应用)，其特征在于该安全设备包括可以访问所有卡功能单元的传送信息插入单元，并且经由第一通信单元从外部读/写器接收到关于服务的特定信息和对提供服务所需的个人身份信息的请求的所述卡功能单元，在个人身份信息保存在传送信息插入单元中的情况下读取个人身份信息并且将该信息传送给外部读/写器，或者在个人身份信息没有保存在传送信息插入单元中的情况下，将关于服务的特定信息写入到传送信息插入单元中，并且所述传送信息插入单元经由第二通信单元向信息处理装置提供关于服务的特定信息，并保存从信息处理装置写入的个人身份信息。

向安全设备的传送信息插入单元写入从外部读/写器接收的关于服务的特定信息，而且该信息被读入到显示服务列表信息的信息处理装置。用户检查列表信息，并输入关于期望服务的个人身份信息(列表信息显示系统)。

根据本发明的安全系统的特征在于第一通信单元执行非接触通信，而第二通信单元执行接触通信。

本发明提供一种信息处理装置，该装置安装有个人身份信息预先输入系统的安全设备，其特征在于该信息处理装置包括用于通过安全设备的第一通信单元监视通信结束的状态监视单元，以及中间件，用于显示输入个人身份信息的屏幕并且将所输入的个人身份信息经由安全设备的第二通信单元写入安全设备的传送信息管理单元。

由用户从信息处理装置输入的个人身份信息首先通过中间件被写入安全设备的传送信息插入单元中。

本发明提供一种信息处理装置，其安装有列表信息显示系统的安全设备，其特征在于该信息处理装置包括用于通过安全设备的第一通信单元监视通信

结束的状态监视单元，以及中间件，一旦状态监视单元检测到通信结束，该中间件就通过所述安全设备的第二通信单元访问安全设备的传送信息管理单元，并且获取在传送信息插入单元中保存的关于服务的特定信息，并且所述中间件根据获得的信息显示服务的列表信息，同时显示用于输入提供服务所需的个人身份信息的屏幕，并且将所输入的个人身份信息写入信息传送插入单元。

由此，即使在用户不了解外部读/写器所处理的服务时，用户也只需要从服务列表信息输入关于期望服务的个人身份信息以享用想要的服务。用户不需要选择卡应用。

根据权利要求 15 的信息处理装置根据所获得信息显示服务列表信息，提示输入服务特定信息和提供服务所需的个人身份信息，并且将所输入服务特定信息和个人身份信息写入到传送信息插入单元中。

在此设备上，由于用户输入了服务和提供服务所需的个人身份信息，因此用户必须另外指定一服务。在将相同的 PIN 设置到多于一个服务的情况下，可以从可用服务中选择并执行一个服务。

所述安全设备以可拆分方式附接到信息处理装置，或者集成地嵌入到信息处理装置中。

本发明提供一种终端装置，用于与配备有多个卡功能单元的安全设备进行通信并且执行从多个可用服务中选择的服务，其特征在于该终端装置激活相应于所选服务的卡功能单元，并请求提供服务所需的个人身份信息，并且在从卡功能单元传送的个人身份信息出现为异常的情况下，选择另一个服务，并且激活相应于该服务的卡功能单元并请求提供该服务所需的个人身份信息。

该终端装置自动地从支持个人预先输入系统的多个可执行服务中选择并执行服务。

根据本发明的安全设备、信息处理装置和终端简化了在执行卡服务时所需的个人身份信息的用户输入。这加快了卡服务的执行。

根据本发明的安全设备仅执行接收命令和返回响应的被动操作，并且符合相应的国际标准。因此该安全设备具有普遍的通用性。

附图说明

图 1 是示出根据本发明第一个实施例的移动电话和 IC 卡的配置的方框图。

图 2 示出了根据本发明第一个实施例的 IC 卡的 PIN 信息管理形式。

图 3 是示出根据本发明第一个实施例的移动电话、IC 卡和外部读/写器的操作的顺序图。

图 4 是示出根据本发明第一个实施例的移动电话、IC 卡和外部读/写器的接着的操作的顺序图。

图 5 是示出根据本发明第二个实施例的移动电话和 IC 卡的配置的方框图。

图 6 是示出根据本发明第二个实施例的移动电话、IC 卡和外部读/写器的操作的顺序图。

图 7 是示出执行符合国际标准的操作的移动电话和 IC 卡的配置的方框图。

图 8 是示出根据本发明第三个实施例的移动电话和 IC 卡的配置的方框图。

图 9 说明了根据本发明第三个实施例的终端应用、卡应用和支付终端应用之间的关系。

图 10 是示出根据本发明第三个实施例的移动电话、IC 卡和外部读/写器的操作的顺序图。

图 11 是示出根据本发明第四个实施例的移动电话、IC 卡和外部读/写器的操作的顺序图。

图 12 是示出根据本发明第四个实施例的移动电话、IC 卡和外部读/写器的操作的顺序图(接图 11)。

具体实施方式

(第一个实施例)

根据本发明第一个实施例的安全设备是配备有非接触通信和接触通信两种功能的 IC 卡，而信息处理装置是对着信用卡支付终端放置的移动电话。以下是从移动电话写入 IC 卡的 PIN 情况。移动电话、IC 卡和支付终端的外部读/写器协同工作以便防止 PIN 被滥用。

附着于移动电话的 IC 卡通过接触通信向/从移动电话传送信息。当用户

将移动电话对着外部读/写器放置而且 IC 卡进入外部读/写器的非接触通信的范围时，IC 卡经由非接触通信向/从外部读/写器传送信息。

参见图 1，IC 卡 20 包括传送信息管理应用 22，用于集中地从/向多个支付卡应用 21 和移动电话 10 接收/传送信息并且与身份信息相结合地管理从移动电话 10 传送的 PIN 信息；信息存储部分 23，用于保存要传送的信息；卡 OS，用于执行通信和文件管理。移动电话 10 包括终端中间件 12，用于获得来自传送信息管理应用 22 的信息，并将用户输入的 PIN 信息传送给传送信息管理应用 22；以及设备驱动器 13，用于控制移动电话 10 的操作。

IC 卡 20 的所有支付卡应用可以访问传送信息管理应用 22，并将从外部读/写器 39 传送的信息写入支付卡应用 21，而且经由传送信息管理应用 22 将要传送到移动电话 10 的信息写入信息存储部分 23。

传送信息管理应用 22，例如在其中卡应用以 Java™ 语言创建的 Java™ 卡的情况下，可以使用可共享接口(Sharable Interface)实现。当使用防火墙将卡应用分开从而以一种安全方式将多个卡应用共存于一个 IC 卡中时，该可共享接口是一种可以访问卡应用而不会被防火墙阻挡的接口。

一旦与传送信息管理应用 22 进行了相互验证，移动电话 10 的终端中间件 12 就可以没有限制地访问传送信息管理应用 22。

在图 1 中，由移动电话 10、IC 卡 20 以及外部读/写器 30 协调执行的处理的顺序是由圈绕的数字表示的。

移动电话 10 的终端中间件 12 经由设备驱动器 13 监视 IC 卡 20 非接触通信的状态，并且为了这一目的一直向 IC 卡 20 传送轮询信号(1)。在非接触通信正在进行的情况下，为了处理状态监视 IC 卡 20 向轮询信号发送一个“通信中”的响应，或者在非接触通信没有进行的情况下，发送“非通信中”的响应。这就允许设备驱动器 30 检测 IC 卡 20 的非接触通信的结束。

当用户将移动电话 10 对着外部读/写器 30 放置时，进入外部读/写器的非接触通信范围中的 IC 卡就开始非接触通信，而外部读/写器 30 指定的支付卡应用 21 就被激活(2)。外部读/写器 30 请求已激活的支付卡应用 21 传送信用卡支付处理所需的个人身份号码(PIN)。

在这一实施中，外部读/写器 30 将 PIN 请求和唯一的处理标识符传送给支付卡应用 21。

每隔一段预定时间(例如 30 秒)，外部读/写器 30 更新处理标识符。或者

在响应于来自支付卡应用 21 的 PIN 请求返回 NG 的情况下，外部读/写器 30 可以利用例如“存储姓名+存储号码+检验计数器号码+日期+时间”作为处理标识符，而且可以将该处理标识符保存一预定时间，并对于下一次卡处理重新使用该处理标识符。

接收 PIN 请求的支付卡应用 21 访问传送信息管理应用 22，并读取保存在信息存储部分 23 中的 PIN 信息。

如图 2 所示，根据互相相关的 PIN 请求和基于 PIN 请求从移动电话 10 写入的 PIN 信息、信息存储部分 23 保存从外部读/写器 30 传送的处理标识符。如图 2(a)所示，在没有响应于 PIN 请求进行 PIN 输入的阶段中，仅仅输入 pp 信息。

接收到 PIN 请求的支付卡应用根据 PIN 请求读取与从外部读/写器 30 接收的处理标识符相应的 PIN 信息。在相应 PIN 信息没有保存在信息存储部分 23 的情况下，支付卡应用请求移动电话 22 用刚刚从外部读/写器 30 接收到信息存储部分 23 中的处理标识符和 PIN 请求重写信息存储部分 23 中的所述信息(3)，并对外部读/写器 30 做出不能回答 PIN 请求的响应。在这一情况下，在支付处理不成功的时候，支付卡应用和外部读/写器 30 之间的非接触通信结束。

用于 IC 卡 20 的状态监视的移动电话 10 的设备驱动器 13 检测 IC 卡 20 非接触通信的结束，并通知终端中间件该事件(4)。终端中间件 12 解释获得的信息，并在移动电话 10 的显示器上显示 PIN 输入窗口。当用户操作移动电话 10 上的按键以输入 PIN 时，终端中间件 12 将输入的 PIN 和处理标识符传送给传送信息管理应用 22(6)。传送信息管理应用 22 将 PIN 与处理标识符联合地写入信息存储部分 23。

当用户将移动电话 10 再一次对着外部读/写器 30 放置时，外部读/写器 30 激活支付卡应用，并将 PIN 请求和处理标识符传送给支付卡应用。支付卡应用访问传送信息管理应用 22，从信息存储部分 23 读取与处理标识符对应的 PIN 信息。除非从来自外部读/写器 30 的最后 PIN 请求开始到当前 PIN 请求之前还没有过去 30 秒时间，处理标识符都不会改变。支付卡应用可以从信息存储部分 23 读取相应于处理标识符的 PIN 信息(7)。

在支付卡应用已经成功读取了相应于 pp 信息的 PIN 信息的情况下，它将 PIN 信息传送给外部读/写器 30(8)，并且清除信息存储部分 23 中的处理标识

符。在支付卡应用未成功获得相应于 pp 信息的 PIN 信息的情况下，它重写信息存储部分 23 中的 pp 信息，并且丢掉上述 PIN，然后将 PIN 请求写入信息存储部分 23。

在连接到外部读/写器 30 的中心进行 PIN 的匹配。在匹配成功的情况下，就执行支付处理，支付处理 2 成功地终止。

这样，IC 卡 20 管理彼此相关的要按照时间更新的处理标识符以及由用户输入的 PIN。只有当由支付终端最近输入的处理标识符与相应于 PIN 的处理标示符相匹配时，才从 IC 卡 20 中抽取 PIN 信息。

因此，即使移动电话落入了其他恶意的人手中，同时 PIN 已经写入安装在其上的 IC 卡中的情况下，除非在利用授权用户曾要在其上进行支付的支付终端更新了 pp 信息之前执行了支付，否则支付企图将会失败。这在实质上防止了非法的支付。

支付终端上处理标识符的更新可以通过每隔预定时间丢弃保存在无人操作的 POS 中的当前处理标识符以更新在有人操作的 POS 情况中的 pp 信息来进行，保存在 POS 中的处理标识符可以根据收银员的指令来丢弃，以便更新处理标识符。

图 3 和 4 示出了移动电话 10、IC 卡 20 和外部读/写器 30 的处理流程。移动电话 10 的支付卡应用监视 IC 卡 20 的非接触通信(1)。当移动电话 10 对着外部读/写器 30 放置时，外部读/写器 30 指定支付卡应用，并指示它的激活(2)。接收到来自支付卡应用的激活 OK 响应后，外部读/写器 30 执行与支付卡应用的互相验证(3)，并将要提供给移动电话 10 的支付金额信息、处理标识符和 PIN 请求传送给支付卡应用(4)。

支付卡应用从传送信息管理应用 22 请求保存在信息存储部分 23 的信息(5)，搜索所获得的信息寻找匹配处理标识符的 PIN 信息。如果获得 PIN 信息失败，支付卡应用就访问传送信息管理应用 22 以便写入支付金额信息和 PIN 请求(6)。

将 NG 响应以外部读/写器 30 并且支付处理 1 失败地终止。

检测到 IC 卡 20 处理的结束(7)的移动电话 10 的终端中间件 12 指示传送信息管理应用 22 的激活(8)。接收到来自传送信息管理应用 22 的激活 OK 响应后，终端中间件 12 执行与传送信息管理应用 22 之间的互相验证(9)，并传送信息获取命令到传送信息管理应用 22(10)。接收到该命令后，传送信息管

理应用 22 向终端中间件 12 返回其响应数据包括支付金额信息、处理标识符和 PIN 请求的的响应(11)。终端中间件 12 解释所获取的信息(12)，并在移动电话 10 的显示器上显示支付金额和 PIN 输入窗口(13)。当用户操作移动电话 10 上的按键以输入 PIN 时，终端中间件 12 就访问传送信息管理应用 22 并写入 PIN(14)。

当用户将移动电话 10 再一次对着外部读/写器 30 放置时，外部读/写器 30 激活支付卡应用 21(15)，执行互相验证(16)，并将支付金额信息、处理标识符和 PIN 请求传送给支付卡应用(17)。

支付卡应用从传送信息管理应用 22 请求保存在信息存储部分 23 中的信息(18)，并获得信息(19)，搜索所获得的信息寻找匹配处理标识符的 PIN 信息，然后将所获得的 PIN 信息传送给外部读/写器 30(20)。

传送信息管理应用 22 可以作为搜索 PIN 的实体。在这种情况下，传送信息管理应用 22 接收来自支付卡应用的处理标识符，并且在于保存在信息存储部分 23 中的数据中找到相应 PIN 信息的情况下，将 PIN 信息输出给支付卡应用。

在连接到外部读/写器 30 的中心进行 PIN 的匹配。在匹配成功的情况下，执行支付处理，并且将处理结束通知从外部读/写器 30 传送给支付卡应用(21)。支付处理 2 成功地终止。

IC 卡 20 仅仅执行接收命令和返回响应的被动操作，而且符合相应国际标准。在尝试非法支付的情况下，即使已经写入了 PIN，也不会从 IC 卡中输出 PIN，这就防止了非法支付。

(第二个实施例)

本发明的第二个实施例描述了其中首先操作安装了 IC 卡的移动电话将 PIN 写入 IC 卡，然后将移动电话对着外部读/写器放置以进行支付处理的情况。移动电话监视 IC 卡的状态。在即使预定时间已经过去却还没有进行 IC 卡和外部读/写器的处理的情况下，就清除写入 IC 卡的 PIN，以便防止其他人可能的 PIN 滥用。

如图 5 所示，移动电话 10 包括终端中间件 12，其将用户输入的 PIN 写入 IC 卡 20 的传送信息管理应用 22，而且一旦经过预定时间，就将 PIN 清除；以及用户通知单元 14，显示是否输入 PIN 的寿命已经过去。移动电话 100 和

IC 卡 20 的其它配置与第一个实施例中所示的相同(图 1)。

移动电话 10 的终端中间件 12 在移动电话 10 的显示器上提供 PIN 输入窗口。用户期望要用于支付服务的支付卡应用，并输入支付服务所要使用个人身份号码(PIN)。终端中间件 12 获取当前时间并将当前时间设置为 PIN 寿命的开始时间。然后，终端中间件 12 访问传送信息管理应用 22，将它的 PIN 写入信息存储部分 23(1)，并且通过轮询方式监视 IC 卡 20 的状态(2)。终端中间件 12 通知用户通知单元 14PIN 寿命仍旧有效，之后用户通知单元显示所述信息(3)。

终端中间件 12 连续获得当前时间并将其存储为最新时间并且检查是否预定时间(例如 30 秒)还没有过去。在预定时间已经过去了或者获取的当前时间已经变得比所存储的最新时间还要晚(时间已经返回)，或者输入了时间校正模式的情况下，终端中间件 12 就通知用户通知单元 14 PIN 寿命已经超时(4)。终端中间件 12 访问移动电话 20 的传送信息管理应用 22，并清除写入终端中间件 12 的 PIN(5)。用户通知单元 14 显示 PIN 寿命还没有过去。

如果在终端中间件 12 清除保存在信息存储部分 23 中的 PIN 之前、在 IC 卡 20 和外部读/写器 30 之间开始进行支付处理，那么外部读/写器 30 就从 IC 卡 20 的支付卡应用请求 PIN(6)，而且支付卡应用相应地访问传送信息管理应用 22 以读取由终端中间件 12 写入的 PIN 信息(7)，并将该 PIN 信息传送给外部读/写器 30(8)。在单次读取 PIN 时，传送信息管理应用 22 从信息存储部分 23 将 PIN 清除。

当 IC 卡 20 和外部读/写器 30 之间的支付处理终止时，已检测到这一处理的结束的移动电话 10 的终端中间件 12 访问传送信息管理应用 22 以检查已经清除了 PIN，并且在其已经被清除的情况下停止检查 PIN 寿命。在 PIN 没有被清除的情况下，终端中间件 12 继续检查 PIN 寿命。一旦 PIN 寿命过去，终端中间件 12 就访问传送信息管理应用 22 以清除 PIN。

这样，在 IC 卡 20 上，从输入开始在经过预定时间时或在经过预定时间之前，所输入 PIN 就被成功的清除了。即使在安装了 IC 卡的移动电话落入了其他恶意的人手中时，也可以防止了可能的非法支付。

即使用户输入的 PIN 与由外部读/写器 30 激活的支付卡应用的支付服务所使用的 PIN 不同，一旦 PIN 从信息存储部分 23 中读取出来，就将其清除。这允许一旦支付没有成功用户重新尝试 PIN 输入。用户不需要对待输入的 PIN

是否支持目标支付服务倾注太多注意。

安装在 IC 卡 20 上的支付卡应用是常规的卡应用，从而即使在从传送信息管理应用 22 获取的 PIN 不是用于该用户的情况下，支付卡应用也不再恶意存储 PIN。

通过使用例如以下方法限制可以参考信息存储部分 23 中的 PIN 的支付卡应用，进一步增强了 PIN 的安全性。

IC 卡配备有向外提供服务名称和卡应用 ID 信息对的功能。移动电话的终端中间件使用这一功能向用户提供服务名称和卡应用 ID 信息对，并指示用户输入应用的 PIN。该终端中间件将用户指定的支付卡应用指定为能够参考 PIN 的唯一支付卡应用。

图 6 示出了移动电话 10、IC 卡 20 和外部读/写器 30 的处理流程。

移动电话 10 的终端中间件 12 在移动电话 10 的显示器上显示 PIN 输入窗口(1)。当用户输入 PIN 时，终端中间件 12 将 PIN 写入 IC 卡 20 的传送信息管理应用 22(2)，并且通过轮流方式监视 IC 卡的状态(3)。当用户将移动电话 10 对着外部读/写器 30 放置时，外部读/写器 30 指定支付卡应用并指示其激活(4)。接收到来自支付卡应用的激活 OK 响应后，外部读/写器 30 执行与支付卡应用的互相验证(5)，并将支付金额信息和 PIN 请求传送给支付卡应用(6)。

支付卡应用从传送信息管理应用 22 请求保存在信息存储部分 23 中的 PIN 信息(7)，获得从终端中间件 12 写入的 PIN 信息(8)，并将该 PIN 信息传送给外部读/写器 30(9)。

在支付处理终止时，终端中间件 12 检测支付处理的结束(10)，并访问传送信息管理应用 22 以检查清除了写入的 PIN (11)。

在预定时间的状态监视过程中没有进行 IC 卡 20 和外部读/写器 30 的处理时，终端中间件 12 访问传送信息管理应用 22 并清除写入的 PIN(12)。

IC 卡 20 仅仅执行接收命令和返回响应的被动操作，而且符合相应国际标准。即使在写入了 PIN 的情况下，在预定时间后就将 PIN 清除，这防止了非法支付。

虽然已经介绍了防止用于接受支付的 PIN 的非法使用，本发明还可以用于防止用于激活应用时的验证的 PIN 或密码的非法使用。

虽然在上述例子中 IC 卡被安装在移动电话上，但是本发明并不限于此。

代替移动电话，可以使用各种各样的信息处理装置，例如PDA(个人数字助理)、电子邮件终端、小型个人计算机以及游戏机。只要其为能够根据APDU格式命令操作卡应用的安全设备，IC卡可以是任意形式。安全设备的形状可以是卡状或芯片状，或者它可以被嵌入到信息处理装置中。

本发明的安全设备和信息处理装置可以用于其中使用各种不同卡的卡功能的应用中，其中各种不同卡包括需要防止其他人滥用的支付卡、交通月票和火车票、游戏票、医疗卡、以及管理机构发行的卡。

(第三个实施例)

本发明的第三个实施例描述了以下情况，其中安全设备是具有非接触通信和接触通信两种功能的IC卡，而信息处理装置是移动电话，而且从移动电话输入IC卡与信用卡支付终端执行支付处理所需的PIN。

安装在移动电话上的IC卡通过接触通信与移动电话交换信息。在移动电话对着外部读/写器放置以便IC卡进入外部读/写器的范围的情况下，IC卡通过非接触通信与外部读/写器交换信息。

IC卡包括专有卡应用(传送信息插入应用)，用于向/从移动电话传送/接收信息。存储在IC卡中的任何卡应用都可以访问传送信息插入应用以写入或读取信息。在移动电话上，中间件负责向/从传送信息插入应用发送/接收信息。

图8示意性地说明了移动电话110、IC卡120和外部读/写器130的配置。IC卡120包括多个卡应用，用于执行由所提供服务创建的各种不同的服务；传送信息插入应用122，用于集中地向/从移动电话发送/接收信息；信息存储部分123，用于临时保存要传送的信息；卡OS124，用于执行通信和文件管理。移动电话110包括终端应用111，用于执行与卡应用121的处理相协调的移动电话中的操作；中间件112，用于执行信息到终端应用111的传送；以及设备驱动器113，用于控制移动电话110的操作。

图9说明了移动电话110的终端应用111、IC卡120的卡应用121和支付终端的支付终端应用之间的关系。IC卡120安装了支付应用A、支付应用B、支付应用C、支付应用D、电子车票应用A、电子车票应用B和住所钥匙(residence key)应用作为卡应用。支付终端包括支付终端应用，用于使用支付应用B和支付应用C执行支付服务。移动电话110安装了支付应用A、

支付应用 B、支付应用 C、支付应用 D、电子车票应用 B 和游戏应用终端应用 111。在移动电话 110 的显示屏幕上可以检查移动电话 110 中终端应用 111 的列表(菜单)。用户可以激活例如支付应用 A 的终端应用 111， 从 IC 卡 120 的支付应用 A 读取支付服务的剩余金额。如上所述，移动电话不能从 IC 卡 120 请求卡应用 211 的列表信息。

由于卡应用不总是具有相应的终端应用(例如在 IC 卡中不存在支付应用 B 的终端应用，而存在支付应用 B 的卡应用)，就不可能从移动电话 110 的显示屏幕上所显示的终端应用列表获得卡应用的列表信息。

IC 卡 120 的所有卡应用 121 都可以访问传送信息插入应用 122，并将从外部读/写器 130 传送到卡应用 121 的信息写入传送信息插入应用 122 的信息存储部分 123，同时由移动电话 110 的中间件 112 读取写入传送信息插入应用 122 的 PIN。

传送信息插入应用 122,例如在其中卡应用以 Java™ 语言创建的 Java™ 卡的情况下，可以使用可共享接口来实现。当使用防火墙将卡应用分开，从而以一种安全方式将多个卡应用共存于一个 IC 卡中时，可共享接口是可以访问卡应用而不会被防火墙阻挡的接口。

一旦与传送信息插入应用 122 进行了相互验证，移动电话 110 的中间件 112 就可以没有限制的访问传送信息插入应用 122。

移动电话 110 的设备驱动器 113 为了监视 IC 卡 120 非接触通信的状态，一直向 IC 卡 120 传送轮询信号。在非接触通信正在进行的情况下，为了处理状态监视，IC 卡 120 对轮询信号传送“通信中”的响应，或者在非接触通信没有进行的情况下，传送“非通信中”的响应。这就允许设备驱动器 113 检测 IC 卡 120 的非接触通信的结束。

图 10 示出了移动电话 110、IC 卡 120 和支付终端外部读/写器 130 的处理流程。

在这一装置上，希望执行支付处理的用户从移动电话 110 输入 PIN。在此实施中，移动电话 110 的中间件 112 在移动电话 110 的显示器上显示 PIN 输入窗口 (1)。用户操作移动电话 110 上的按键以输入目标支付服务的 PIN。假如用户希望进行支付应用 C 的服务时，就输入支付服务 C 的 PIN。PIN 输入是用来确认用户选择服务的意向。用户不必执行进一步选择服务的操作。

中间件 112 执行与 IC 卡 120 的传送信息插入应用 122 之间的相互验证，

并将用户所输入的PIN通过传送信息插入应用122写入信息存储部分123(2)，并且同时，移动电话110的中间件112开始监视IC卡120的状态(3)。

用户将安装了IC卡120的移动电话110对着支付终端的外部读/写器130放置。进入外部读/写器130范围中的IC卡120就开始非接触通信。

外部读/写器130为IC卡120指定相应于支付终端的支付服务的一个卡应用(在这一个例子中是支付应用B)，并指示其激活(4)。接收到来自卡应用(支付应用B)121的激活OK响应后，外部读/写器130执行与卡应用(支付应用B)121的互相验证(5)，并将要提供给移动电话的有关支付金额和PIN请求的信息传送给卡应用(支付应用B)121(6)。

接收到PIN请求后，卡应用(支付应用B)121访问传送信息插入应用122并请求保存在信息存储部分23中的信息(7)。从传送信息插入应用122获得由中间件112写入的PIN(8)后，卡应用(支付应用B)121将PIN传送给外部读/写器130(9)。

在连接到外部读/写器130的中心进行PIN的匹配。用户输入的PIN最初是用于支付服务C的支付服务的，从而匹配失败，并且从外部读/写器130向卡应用(支付应用B)121报告PIN异常(10)，与卡应用(支付应用B)121的支付处理失败地终止。

接下来，外部读/写器130为IC卡120指定相应于支付终端的支付服务的下一个卡应用(支付应用C)，并指示其激活(11)。接收到来自卡应用(支付应用C)121的激活OK响应后，外部读/写器130执行与卡应用(支付应用C)121的互相验证(12)，并将关于支付金额和PIN请求的信息传送给卡应用(支付应用C)121(13)。

接收到PIN请求后，卡应用(支付应用C)121访问传送信息插入应用122并请求保存在信息存储部分123中的信息(14)。获得由中间件112写入的PIN(15)后，卡应用(支付应用C)121将PIN传送给外部读/写器130(17)。

当PIN成功匹配时就执行支付处理，并且从外部读/写器130向卡应用(支付应用C)121发送处理结束通知(17)。由此IC卡120和外部读/写器130之间的非接触通信结束。

当IC卡120的非接触通信结束时，保持进行IC卡120的状态监视的移动电话110的中间件112检测非接触通信的结束。

尽管在这一个例子中外部读/写器130首先指定支付应用B作为待激活的

卡应用，但是外部读/写器 130 也可以首先指定支付应用 C。在这种情况下，当指定支付应用 C 时，支付处理是成功的，并且 IC 卡 120 和外部读/写器 130 之间的非接触通信结束。在这种情况下，在图 10 的处理流程中，执行从“处理状态监视(3)”进行到“卡应用的激活(11)”。

在支付终端只有相应于单个支付应用的支付终端应用(例如支付应用 C)的情况下，用户仅需输入一次用于支付应用的 PIN。接着，外部读/写器 130 指定支付应用 C 以执行将成功地终止的支付处理。在这种情况下，在图 10 的处理流程中，在“处理状态监视(3)”之后跟随步骤“卡应用的激活(11)”及随后的步骤。

这样，在这一装置上，从移动电话 110 输入的 PIN 被写入 IC 卡 120 的传送信息插入应用 122。由外部读/写器 130 激活的每一个卡应用 121 顺序地读取来自传送信息插入应用 122 的 PIN，并将 PIN 传送给外部读/写器 300。然后外部读/写器 130 顺序地更新要激活的卡应用，直到通过使用从卡应用传送的 PIN 支付处理成功。

在用户知道目标支付服务包括在支付终端处理的支付服务中的情况下，用户只需输入一次用于目标支付服务的 PIN 以享用期望的目标服务，而没有任何选择卡应用的负担。这在实质上增强了用户的便利性。

IC 卡 120 仅仅执行接收命令和返回响应的被动操作，而且符合相应国际标准。

(第四个实施例)

本发明的第四个实施例描述一种即使在用户不知道支付终端所处理的支付服务的情况下，也可以提供简单的 PIN 输入的装置。

移动电话与 IC 卡的配置与第三个实施例相同(图 8)。

在输入 PIN 以开始 IC 卡 120 和外部读/写器 130 之间的卡通信之前，用户将移动电话 120 对着外部读/写器 130 放置。外部读/写器 130 顺序地激活相应于支付终端的支付服务的卡应用 121 以尝试支付处理。在这一实施中，外部读/写器 130 将标识支付服务的信息(例如支付终端应用名称)传送给卡应用 121。这一信息被写入传送信息插入应用 122。由于没有输入 PIN，无例外的由激活卡应用 121 开始的支付处理将失败。关于由支付终端处理的支付服务的信息被收集到传送信息插入应用 122。

移动电话 110 的中间件 112 从传送信息插入应用 122 读取这一信息，并在移动电话 110 上显示由支付终端处理的支付服务的列表信息。用户参考所显示的信息并输入目标支付服务的 PIN。

接下来，用户再一次将移动电话 110 对着外部读/写器 130 放置以开始 IC 卡 120 和外部读/写器 130 之间的卡通信。与之前的一轮相同，外部读/写器 130 顺序地激活相应于支付终端的支付服务的卡应用 121 以尝试支付处理。当用户激活了目标支付服务的卡应用 121 时，PIN 匹配成功，并且支付处理结束。

图 11 和 12 示出了移动电话 110、IC 卡 120 和支付终端的外部读/写器 300 的处理流程。

用户将安装了 IC 卡 120 的移动电话 110 对着支付终端的外部读/写器 130 放置。移动电话 110 的中间件 112 开始监视 IC 卡 120 的状态(1)。外部读/写器 130 为 IC 卡 120 指定相应于支付终端的支付服务的一个卡应用(在这一个例子中是支付应用 B)，并指示其激活(2)。接收到来自卡应用(支付应用 B)121 的激活 OK 响应后，外部读/写器 130 执行与卡应用(支付应用 B)121 的互相验证(3)，并将要提供给移动电话的关于支付金额和 PIN 请求的信息传送给卡应用(支付应用 B)121(4)。在这一实施中，外部读/写器 130 向卡应用(支付应用 B)121 传送支付终端应用 ID 和用于用户的显示应用名称。

接收到 PIN 请求后，卡应用(支付应用 B)121 访问传送信息插入应用 122 并请求保存在信息存储部分 123 中的信息(5)。从传送信息插入应用 122 获得的信息不包括 PIN(6)，从而卡应用(支付应用 B)121 向信息存储部分 123 写入从外部读/写器 130 经由传送信息插入应用 122 接收的支付金额信息、支付终端应用 ID 和用于用户的显示应用名称，并且向外部读/写器 130 返回 NG 响应。

已接收到 NG 响应的外部读/写器 130 指定相应于支付终端的另一个支付服务的卡应用(支付应用 C)，并指示其激活(8)。接收到来自卡应用(支付应用 C)121 的激活 OK 响应后，外部读/写器 130 执行与卡应用(支付应用 C)121 的互相验证(9)，并将支付金额信息、支付终端应用 ID 和用于用户的显示应用名称传送给卡应用(支付应用 C)121(10)。

卡应用(支付应用 C)121 访问终端中间件 112 并请求保存在信息存储部分 123 中的信息(11)。从传送信息插入应用 122 获得的信息不包括 PIN(12)，从

而卡应用(支付应用 C)121 向信息存储部分 123 写入从外部读/写器 130 通过传送信息插入应用 122 接收的支付金额信息、支付终端应用 ID 和用于用户的显示应用名称(13)，并向外部读/写器 130 返回 NG 响应。

这样，外部读/写器 130 顺序地指定相应于支付终端的支付服务的卡应用 121 以尝试支付处理。当所有的处理尝试都失败时，外部读/写器 130 结束与 IC 卡 120 之间的非接触通信。

通过设备驱动器 113 一直监视 IC 卡 120 的状态的移动电话 110 的终端中间件 112 检测 IC 卡 120 非接触通信的结束(14)，指示 IC 卡 120 的传送信息插入应用 122 的激活(15)。接收到来自传送信息插入应用 122 的激活 OK 响应后，中间件 112 执行与传送信息插入应用 122 之间的互相验证(16)，并传送信息获取命令给传送信息插入应用 122(17)。接收到该命令后，传送信息插入应用 122 向中间件 112 返回其响应数据包括保存在信息存储部分 123 中的信息(由支付终端处理的支付服务的支付终端应用 ID、以及支付金额信息)的响应(18)。中间件 112 解释所获取的信息(19)，并显示列出了支付金额和由支付终端处理的用于用户的支付服务的显示应用名称的服务选择窗口(20)，并接下来显示用于输入 PIN 的 PIN 输入窗口(21)。用户参考服务选择窗口，并且从 PIN 输入窗口输入用于目支付服务(在这一个例子中是与支付应用 B 相应的支付服务)的 PIN。中间件访问中间件 112 以将 PIN 写入信息存储部分 123(22)。

用户将安装了 IC 卡 120 的移动电话 110 再一次对着支付终端的外部读/写器 300 放置。外部读/写器 130 为 IC 卡 120 指定相应于支付终端的支付服务的一个卡应用(在这一个例子中是支付应用 B)，并指示其激活(23)。接收到来自卡应用(支付应用 B)121 的激活 OK 响应后，外部读/写器 130 执行与卡应用(支付应用 B)121 的互相验证(24)，并为用户将关于支付金额、支付终端应用 ID、用于用户的显示应用名称、以及 PIN 请求的信息传送给卡应用(支付应用 B)121(25)。

卡应用(支付应用 B)121 访问传送信息插入应用 122 并请求保存在信息存储部分 123 中的 PIN 信息。

一旦成功进行了 PIN 匹配，在支付终端执行支付处理，并从外部读/写器 130 向卡应用(支付应用 B)121(2)发送处理结束通知以终止支付处理。

这样，在该装置上，有关所有由支付终端处理的支付服务的信息都记录

在 IC 卡 120 的传送信息插入应用 122 中。这一信息读取到移动电话 110 中，并在移动电话 110 的显示器上列出。因此，用户从显示器了解可用的支付服务，并输入用于列表中目标支付服务的 PIN 以享用该服务，而没有任何选择卡应用的负担。

用户可以选择移动电话 110 的显示器上列出的有效支付服务之一，并从 PIN 输入窗口输入所选服务的 PIN。

在上述情况中，作为附加步骤用户必须选择支付服务，在为多个支付服务设置单一 PIN 时，这一步骤是有效的。在移动电话 110 的显示器上提供服务列表、将关于指定服务的信息和输入的 PIN 写入传送信息插入应用 122 的信息存储部分 123 的一系列操作可以由中间件 112 以及移动电话 110 的终端应用 111 来执行。注意，服务列表信息和 PIN 输入屏幕不需要在同一时间显示。

IC 卡 20 仅仅执行接收命令并返回响应的被动操作，并且符合相应的国际标准。

虽然在上述例子中，外部读/写器 130 将支付终端应用 ID 和用于用户的显示应用名称传送到激活的卡应用 121 并且卡应用 121 将该信息写入所述传送信息插入应用 122，所述卡应用 121 也可以如外部读/写器 130 所指示的那样先保存支付终端应用 ID 信息和用于用户的显示应用名称并且将该信息写入传送信息插入应用 122。

虽然在上述例子中 IC 卡被安装在移动电话上，但是本发明并不限于此。代替移动电话，可以使用各种各样的信息处理装置，例如 PDA(个人数字助理)、电子邮件终端、小型个人计算机、以及游戏机。只要其为能够根据 APDU 格式的命令操作卡应用的安全设备，IC 卡可以是任意形式。安全设备的形状可以是卡状或芯片状，或者它可以被嵌入到信息处理装置中。

虽然在上述例子中已经描述了输入 PIN 以接受支付处理，本发明还可以用于例如激活应用中验证所需的 PIN 或密码的个人身份信息的输入。

本发明的安全设备、信息处理装置和终端装置可以用于使用各种不同卡的卡功能的应用，这些各种不同卡包括支付卡、交通月票、火车票、游戏票、医疗卡以及管理机构发行的卡。因此本发明消除了执行卡功能必需的 PIN 或者密码的输入所伴随的麻烦操作。

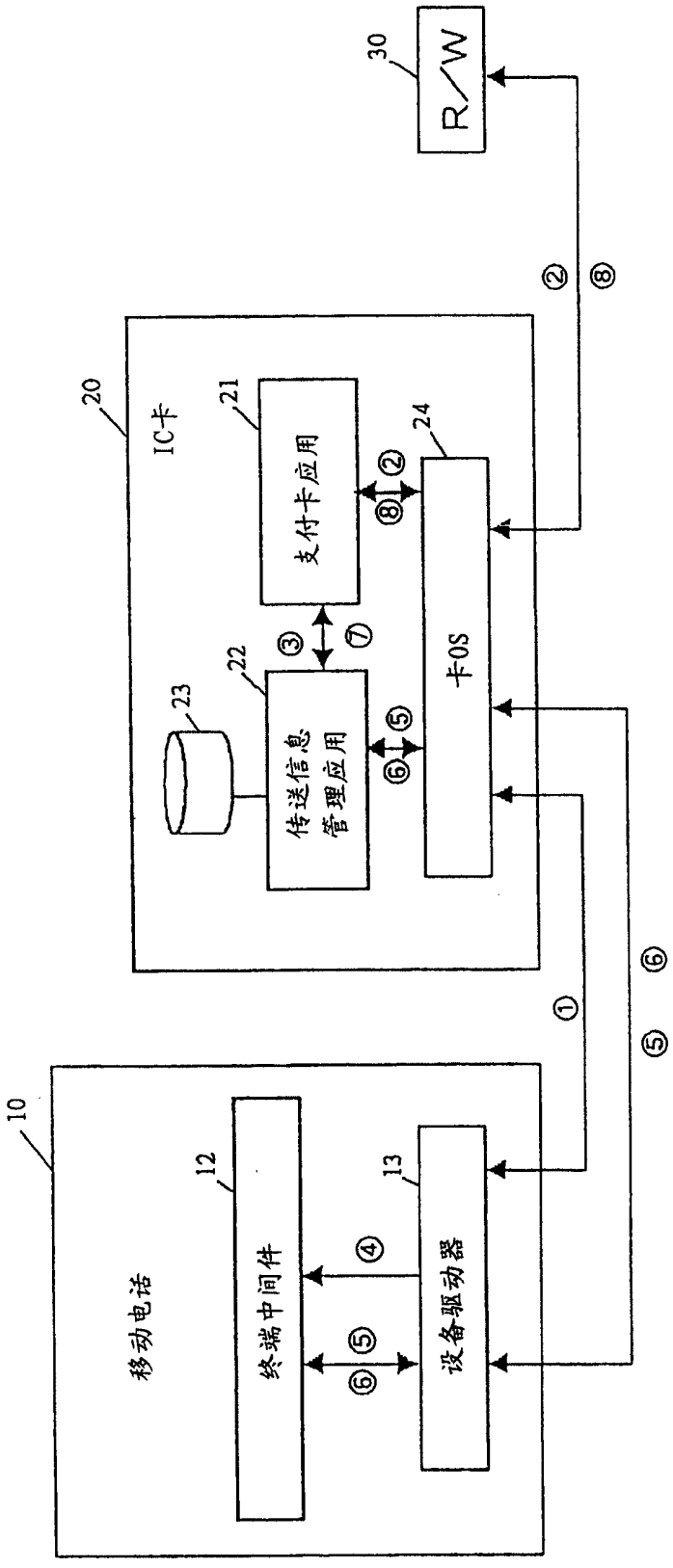

30
R/W
②
⑧
20
IC卡
21
支付卡应用
24
②
⑧
③
⑦
22
23
传送信息
管理应用
⑤
⑥
卡OS
⑥
⑤
①
10
移动电话
12
终端中间件
13
设备驱动器
④
⑤
⑥

图 1

(a) 处理标识符: 1301
PIN: 空

(b) 处理标识符: 1301
PIN: 1234

图 2

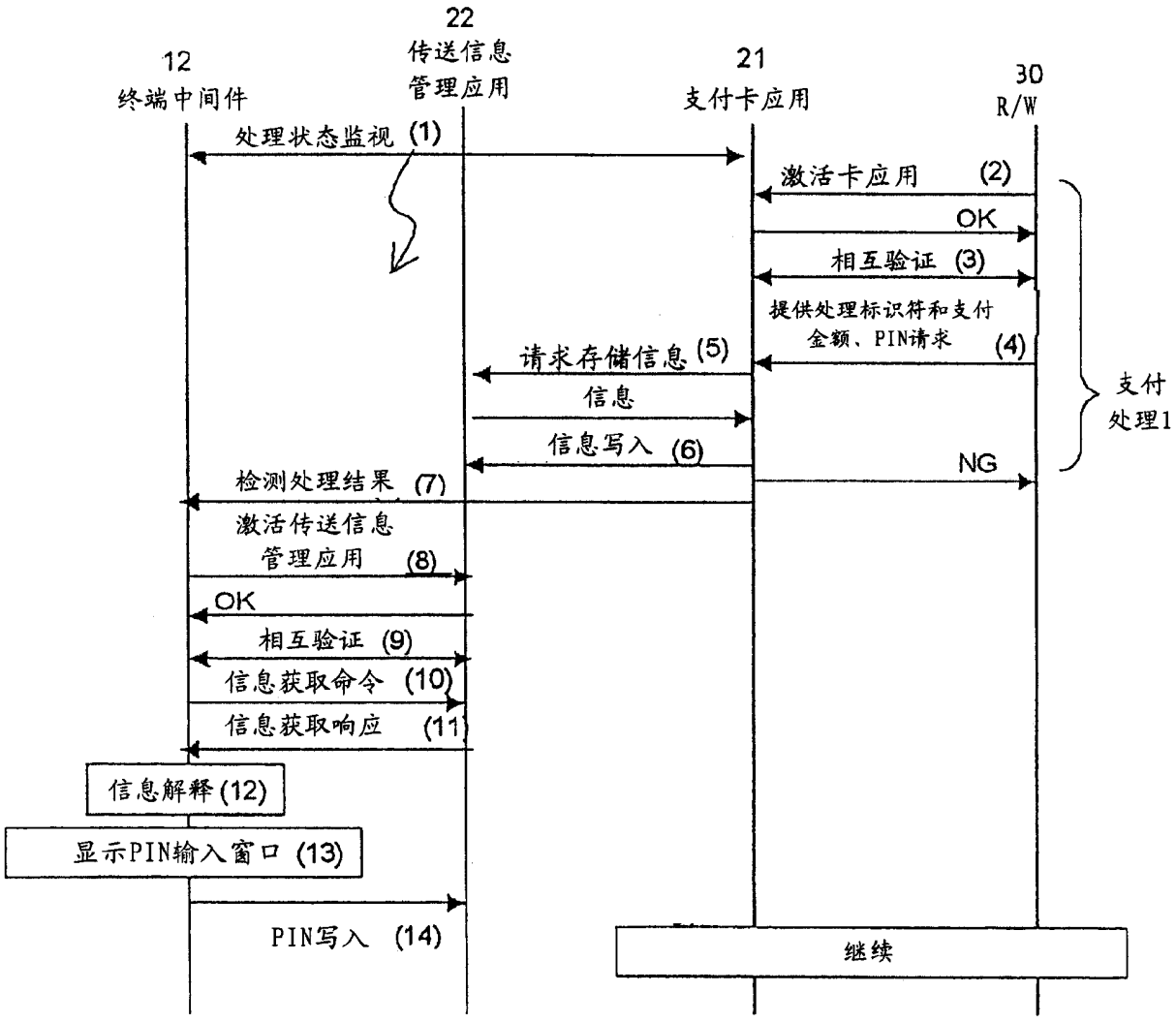


图 3

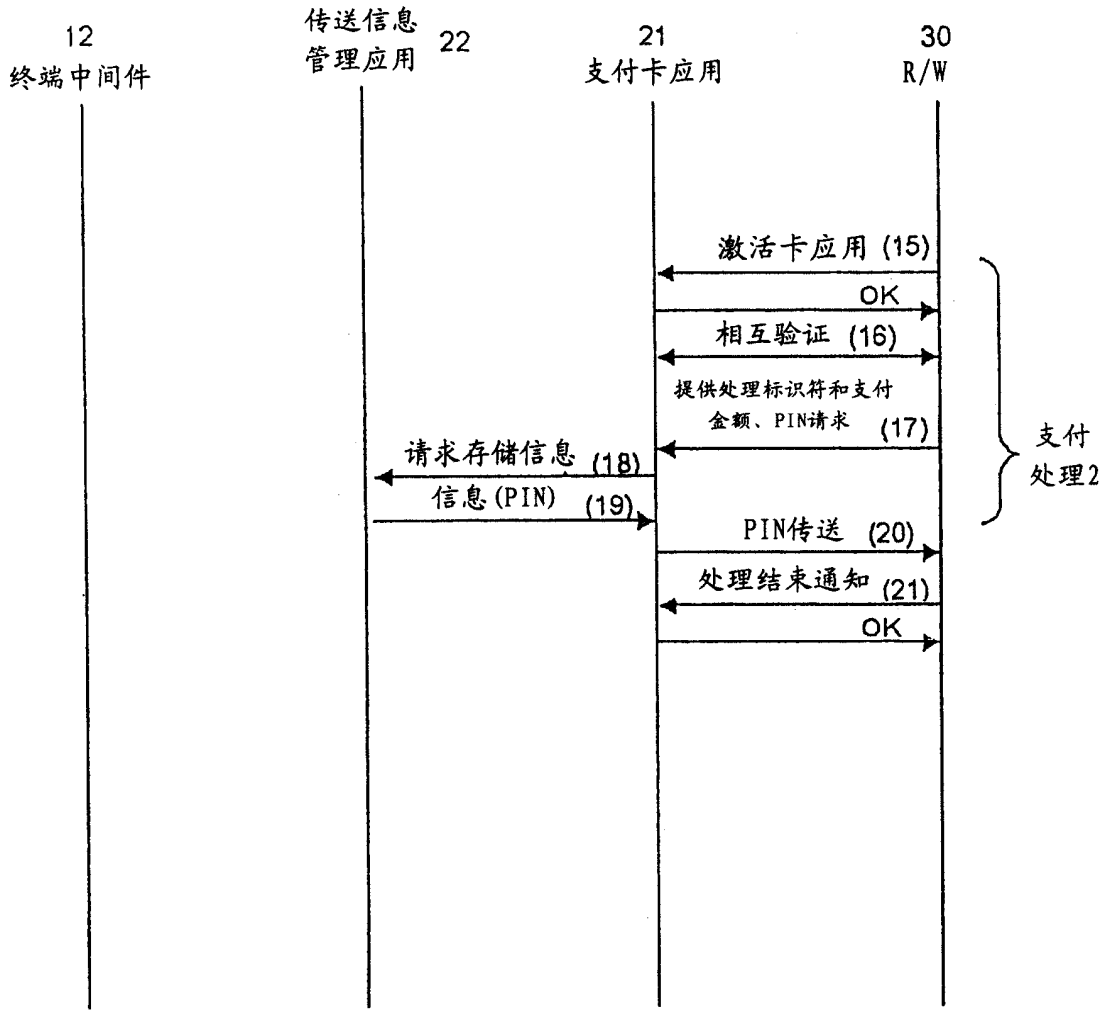

12
终端中间件
传送信息
管理应用
22
21
支付卡应用
30
R/W
激活卡应用 (15)
OK
相互验证 (16)
提供处理标识符和支付
金额、PIN请求 (17)
请求存储信息 (18)
信息(PIN) (19)
PIN传送 (20)
处理结束通知 (21)
OK
支付
处理2

图 4

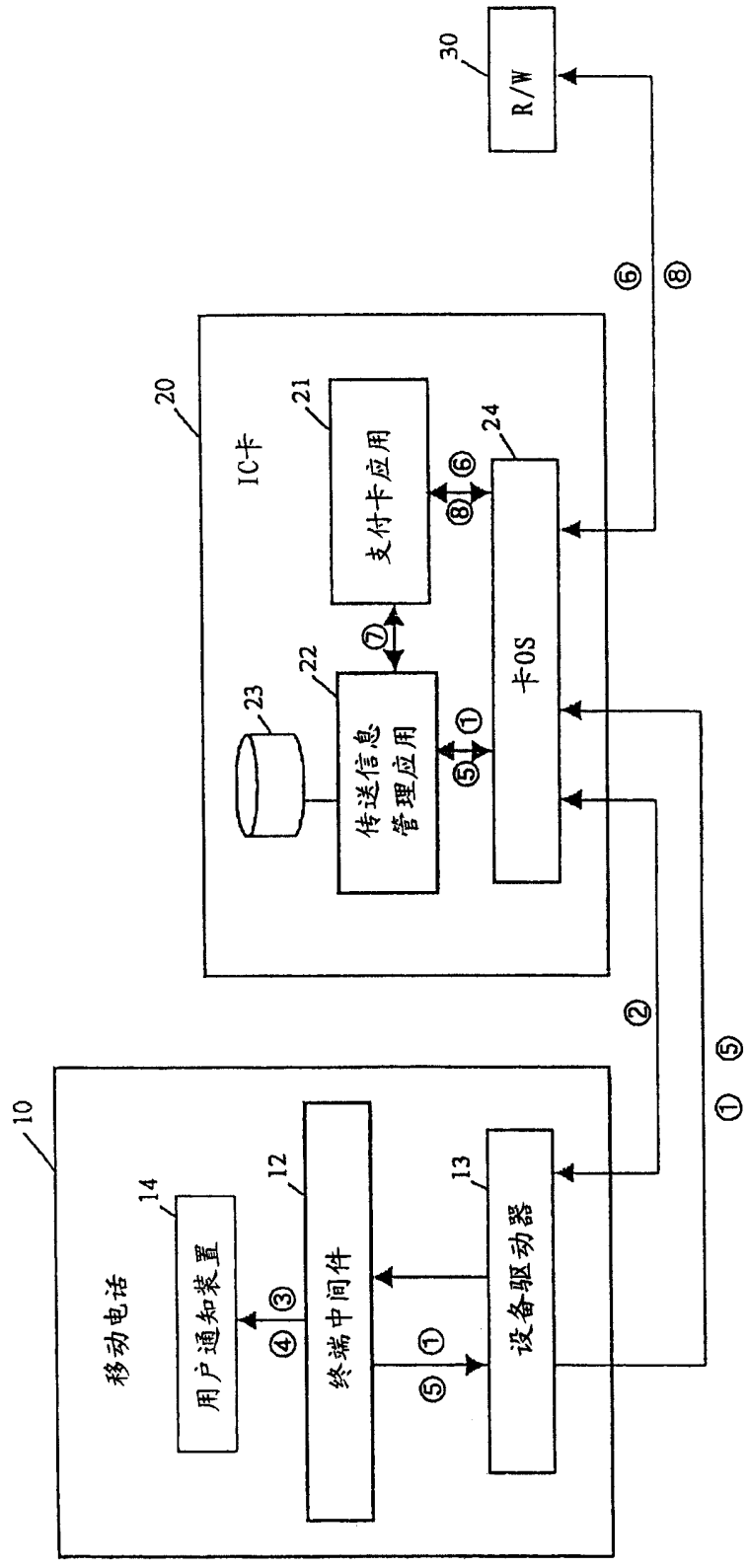

10
移动电话
14
用户通知装置
12
终端中间件
13
设备驱动器
20
IC卡
21
支付卡应用
22
传送信息管理应用
23
24
卡OS
30
R/W
①
②
③
④
⑤
⑥
⑦
⑧

图 5

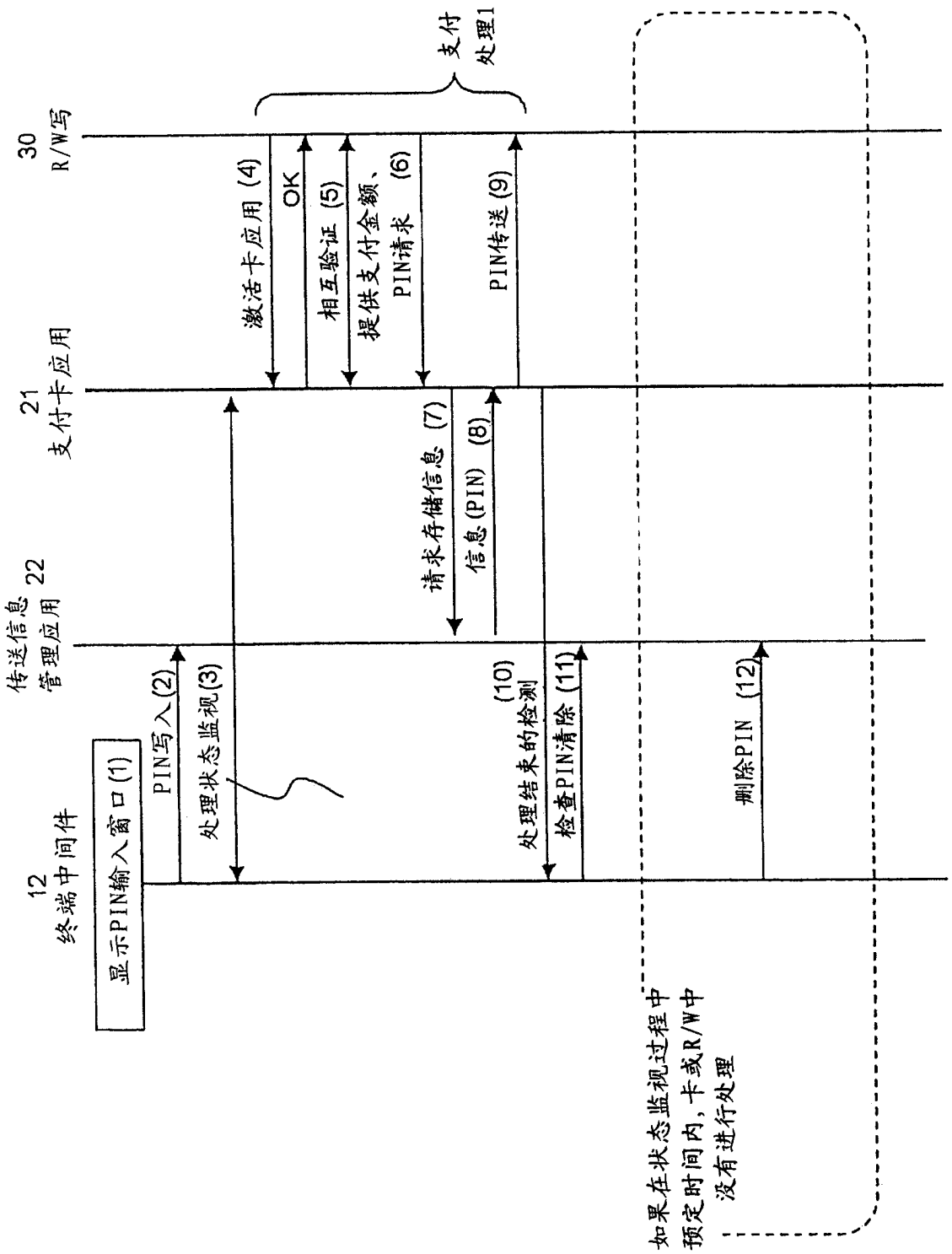

12
终端中间件
显示PIN输入窗口(1)
传送信息
管理应用
22
PIN写入(2)
处理状态监视(3)
21
支付卡应用
激活卡应用(4)
OK
相互验证(5)
提供支付金额、
PIN请求(6)
30
R/W写
支付
处理1
请求存储信息(7)
信息(PIN)(8)
PIN传送(9)
处理结束的检测(10)
检查PIN清除(11)
删除PIN(12)
如果在状态监视过程中
预定时间内,卡或R/W中
没有进行处理

图 6

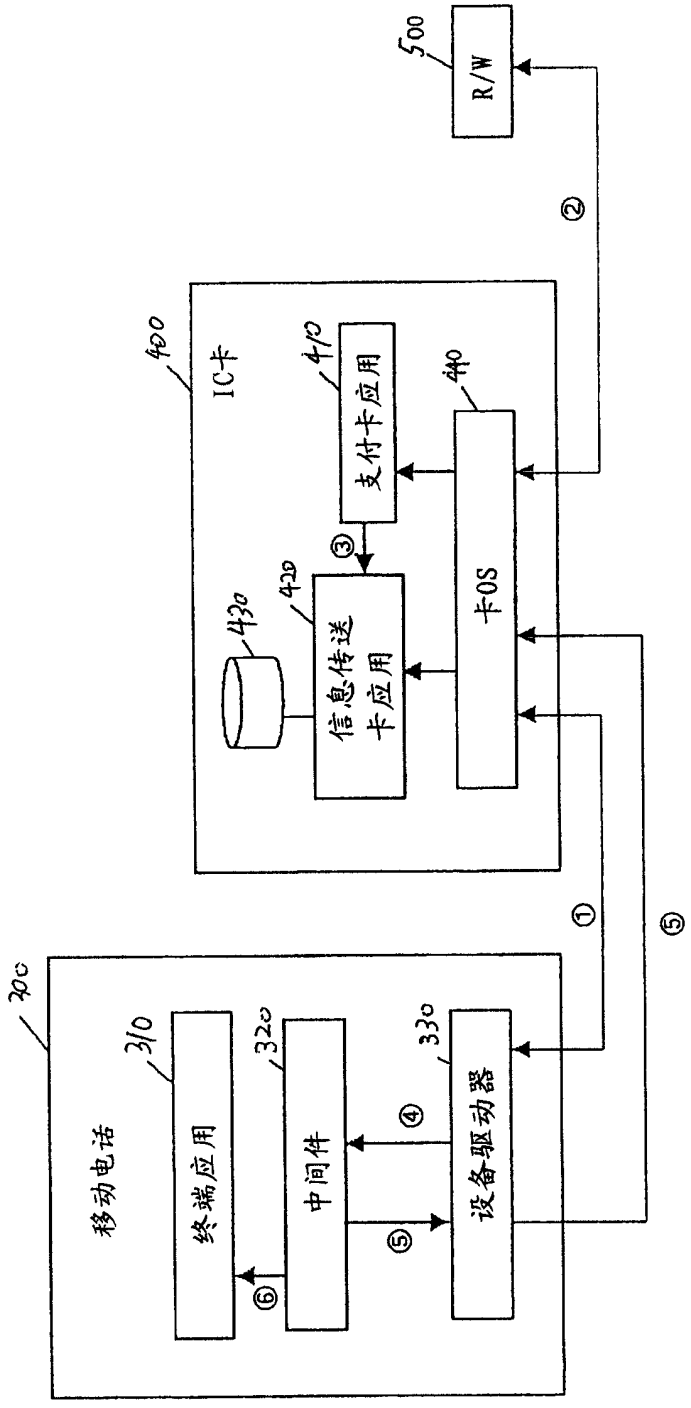

移动电话
200
终端应用
310
中间件
320
设备驱动器
330
IC卡
400
支付卡应用
410
卡OS
440
信息传送卡应用
420
430
R/W
500
①
②
③
④
⑤
⑥

图 7

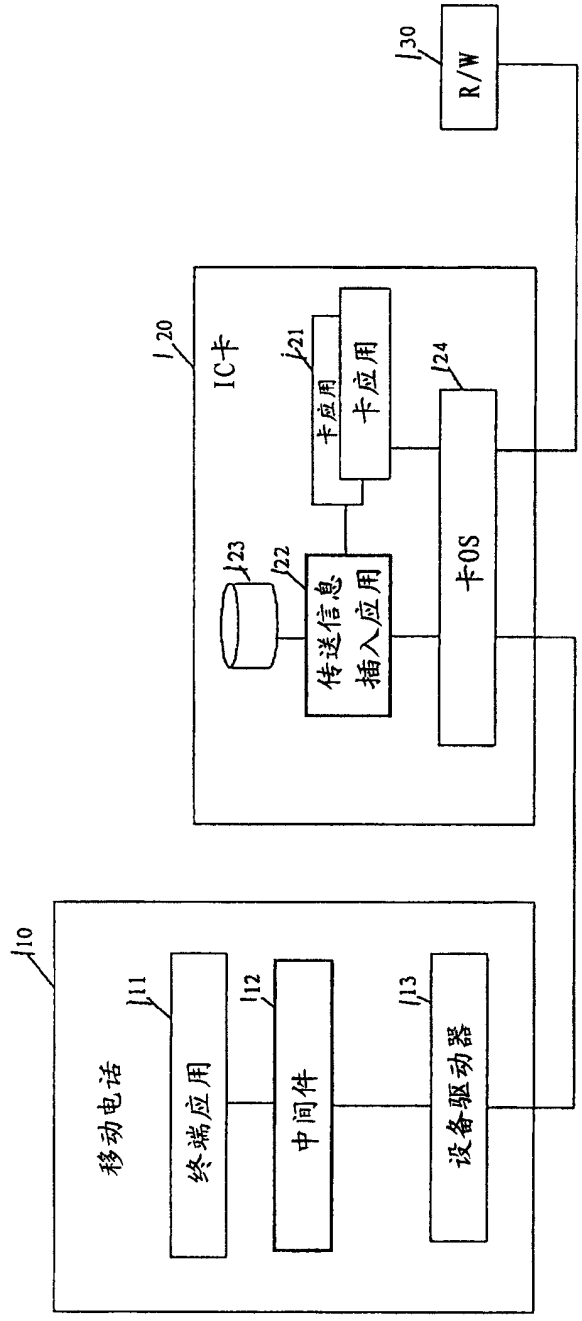

10
移动电话
11
终端应用
12
中间件
13
设备驱动器
20
IC卡
21
卡应用
卡应用
22
传送信息
插入应用
23
24
卡OS
30
R/W

图 8

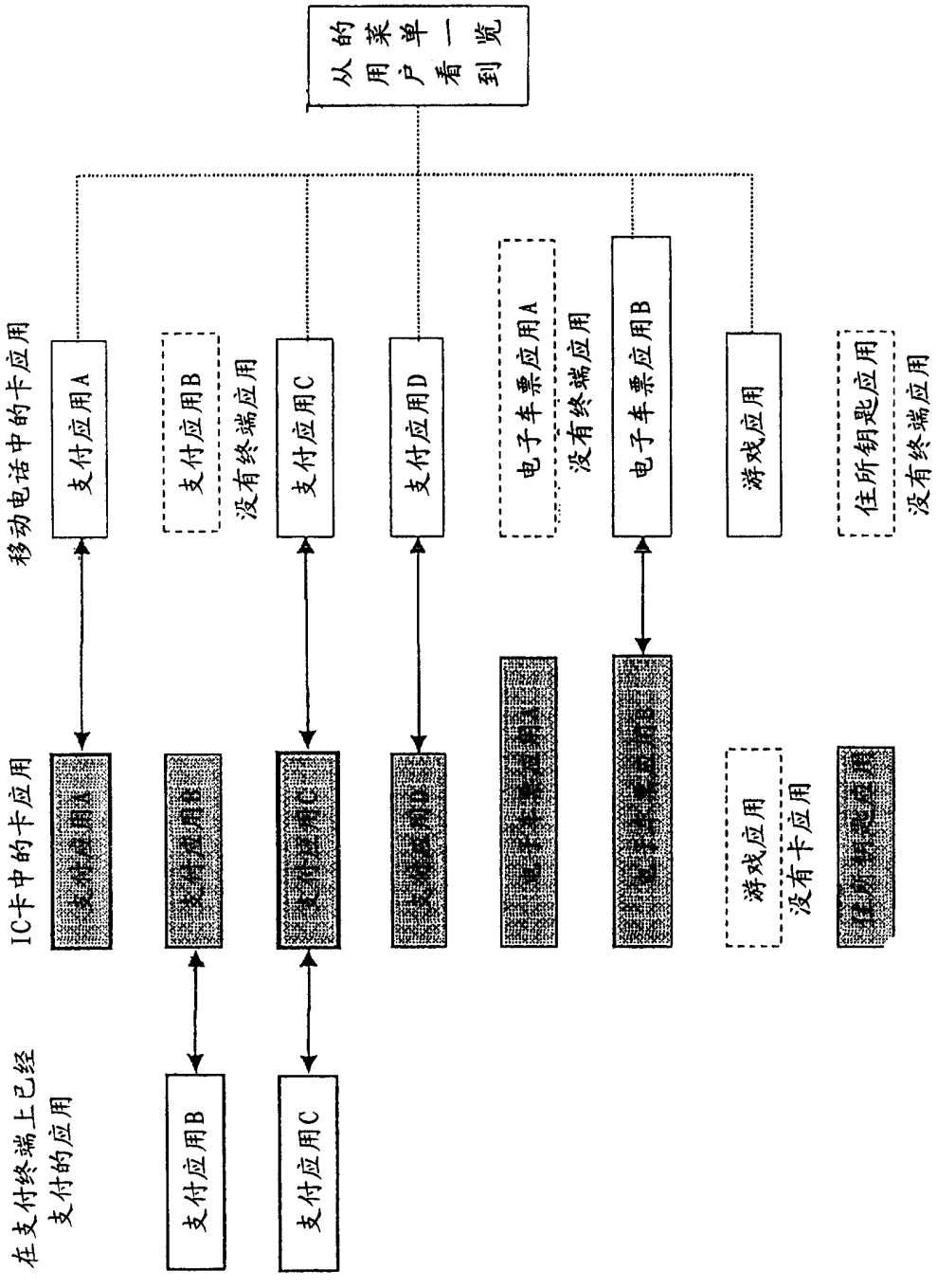

从的用菜户单一看到览
移动电话中的卡应用
支付应用A
支付应用B
没有终端应用
支付应用C
支付应用D
电子车票应用A
没有终端应用
电子车票应用B
游戏应用
住所钥匙应用
没有终端应用
IC卡中的卡应用
支付应用A
支付应用B
支付应用C
支付应用D
电子车票应用A
电子车票应用B
游戏应用
没有卡应用
住所钥匙应用
在支付终端上已经支付的应用
支付应用B
支付应用C

图 9

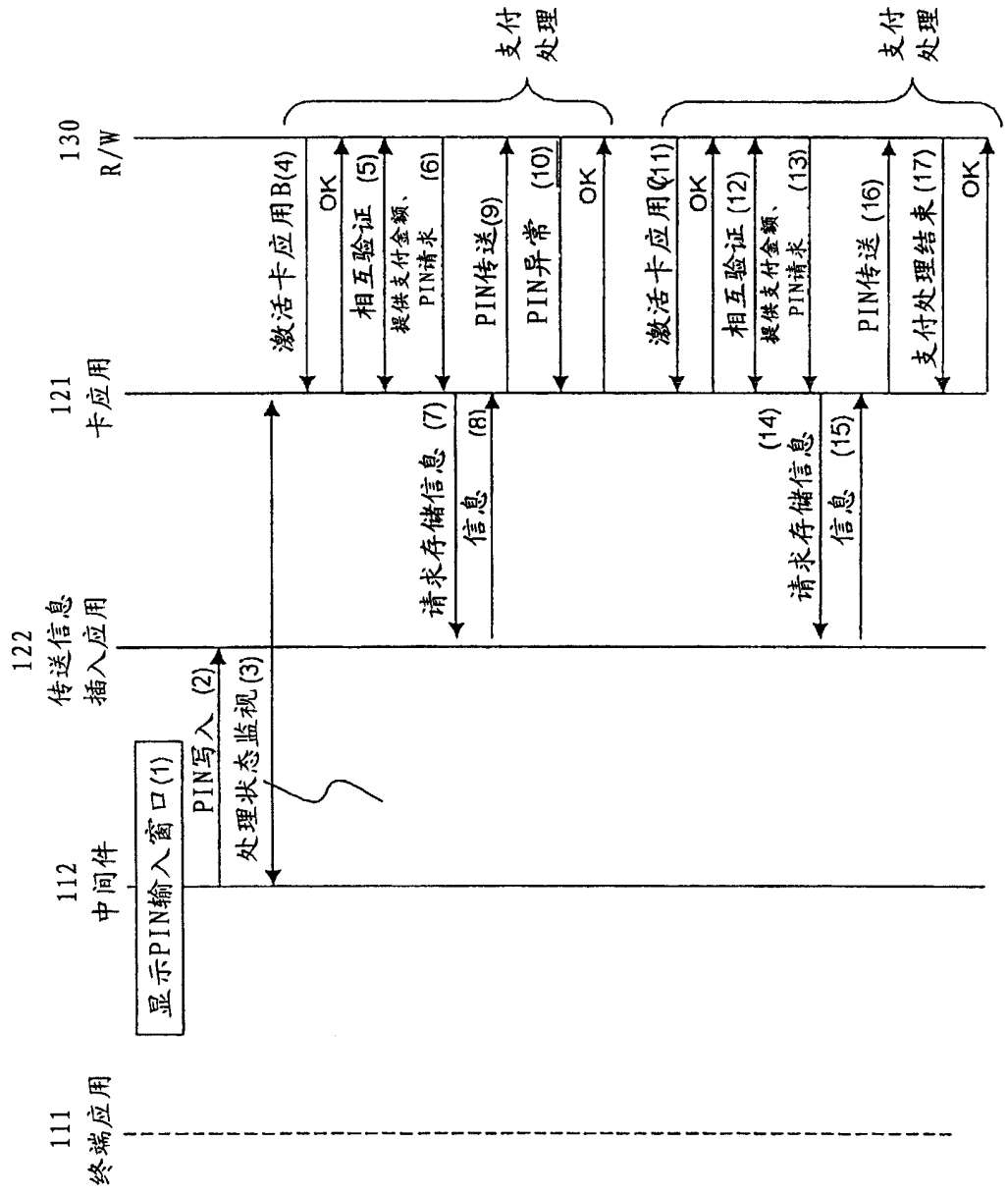

111
终端应用
112
中间件
122
传送信息
插入应用
121
卡应用
130
R/W
显示PIN输入窗口(1)
PIN写入 (2)
处理状态监视(3)
激活卡应用B(4)
OK
相互验证 (5)
提供支付金额、
PIN请求 (6)
请求存储信息 (7)
信息 (8)
PIN传送(9)
PIN异常 (10)
OK
支付
处理
激活卡应用C(11)
OK
相互验证 (12)
提供支付金额、
PIN请求 (13)
(14)
请求存储信息
信息 (15)
PIN传送 (16)
支付处理结束 (17)
OK
支付
处理

图 10

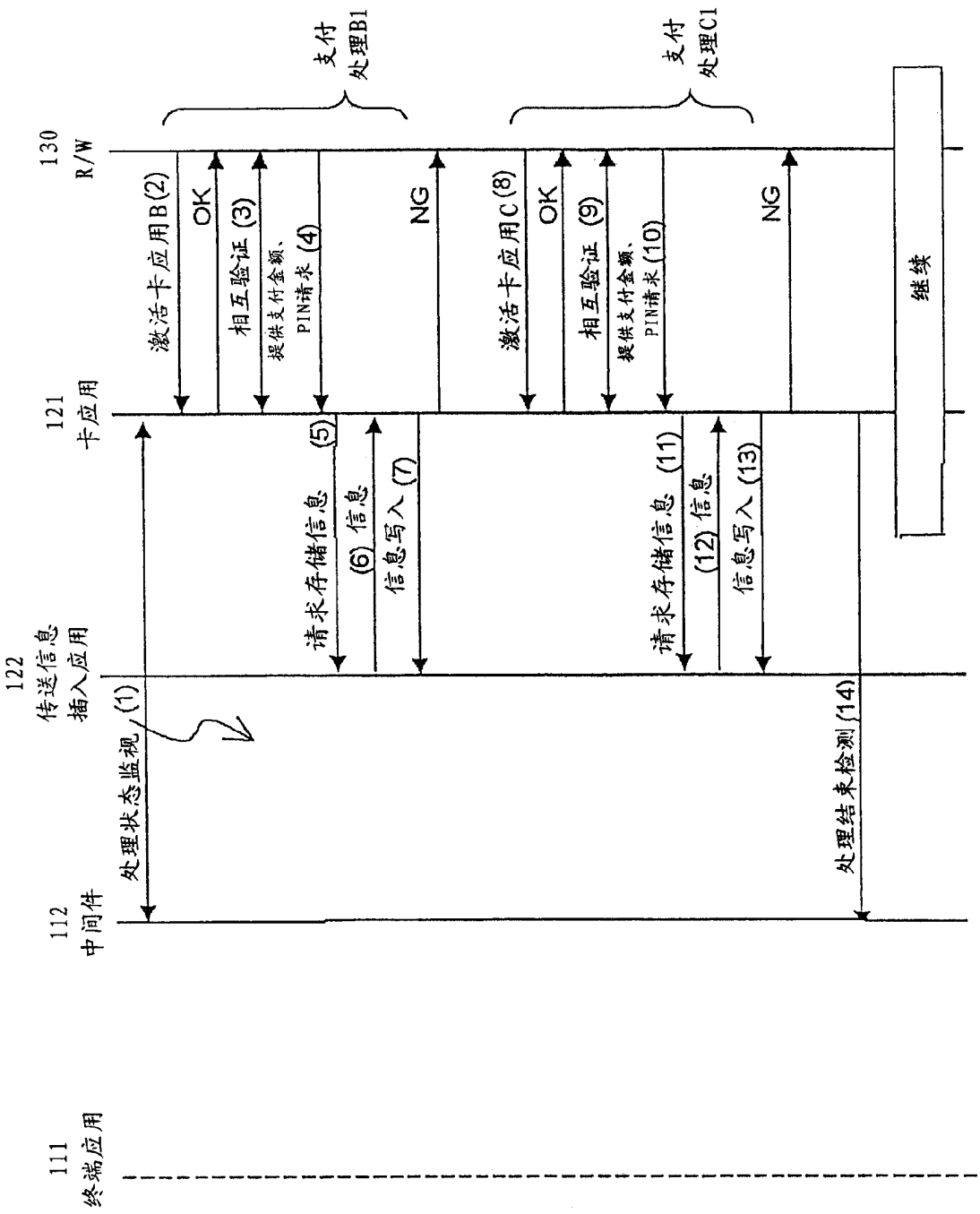

111
终端应用
112
中间件
122
传送信息
插入应用
121
卡应用
130
R/W
处理状态监视 (1)
激活卡应用B(2)
OK
相互验证 (3)
提供支付金额、
PIN请求 (4)
支付
处理B1
NG
请求存储信息 (5)
(6) 信息
信息写入 (7)
激活卡应用C(8)
OK
相互验证 (9)
提供支付金额、
PIN请求(10)
支付
处理C1
NG
请求存储信息 (11)
(12) 信息
信息写入 (13)
处理结束检测(14)
继续

图 11

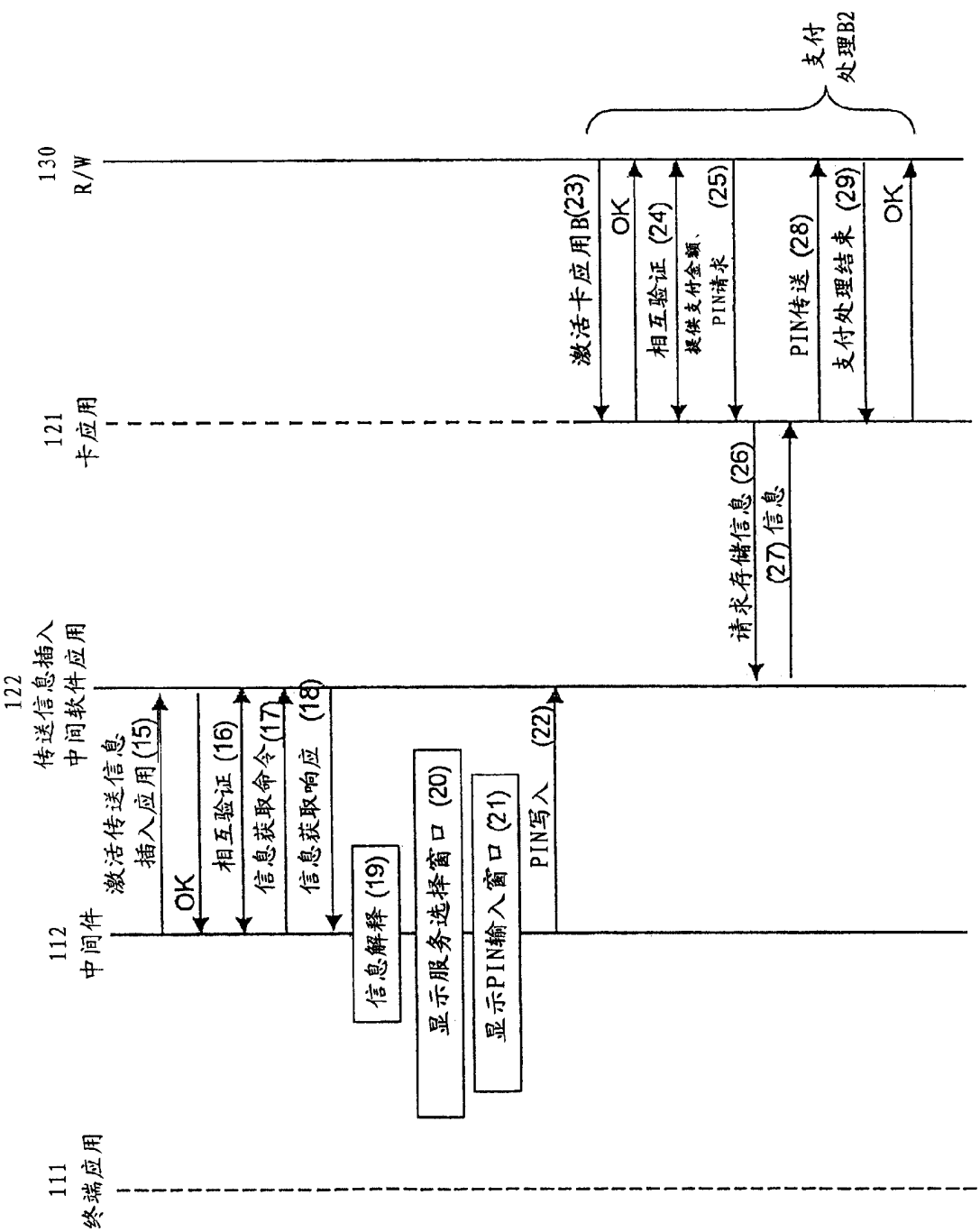

111
终端应用
112
中间件
122
传送信息插入
中间软件应用
121
卡应用
130
R/W
支付
处理B2
激活传送信息
插入应用 (15)
OK
相互验证 (16)
信息获取命令 (17)
信息获取响应 (18)
信息解释 (19)
显示服务选择窗口 (20)
显示PIN输入窗口 (21)
PIN写入 (22)
激活卡应用B(23)
OK
相互验证 (24)
提供支付金额、
PIN请求 (25)
请求存储信息 (26)
(27) 信息
PIN传送 (28)
支付处理结束 (29)
OK

图 12