[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G07F 7/10 (2006.01)

[12] 发明专利说明书

专利号 ZL 200680036149.9

[45] 授权公告日 2009 年 11 月 18 日

[11] 授权公告号 CN 100561527C

[22] 申请日 2006.8.29
[21] 申请号 200680036149.9
[30] 优先权
[32] 2005. 8.30 [33] GB [31] 0517615.1
[86] 国际申请 PCT/GB2006/003205 2006.8.29
[87] 国际公布 WO2007/026139 英 2007.3.8
[85] 进入国家阶段日期 2008.3.28
[73] 专利权人 埃塞博斯有限公司
地址 英国伦敦
[72] 发明人 B·S·霍赫菲尔德
[56] 参考文献
WO2004066130A2 2004.8.5
CN1214779A 1999.4.21
US20040143551A1 2004.7.22
US6575372B1 2003.6.10
审查员 任淑华
[74] 专利代理机构 永新专利商标代理有限公司
代理人 韩 宏

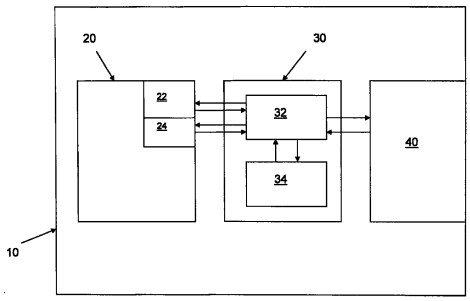
权利要求书 3 页 说明书 5 页 附图 1 页

[54] 发明名称

改进的智能卡系统

[57] 摘要

一种可编程智能卡设备(10)，带有文件系统(22、24)和使设备上文件系统与至少一个设备外文件和/或应用接口的操作软件。 还包括脚本引擎(32)，其可运行一个或多个与特定形式的应用相关的应用协议数据单元(APDU)以修改所述文件系统结构和/或内容，或者用于访问所述文件系统或者与之相关的任何安全条件的命令。 所述可编程智能卡设备(10)具有比较器装置(34)，其可由所述脚本引擎(32)运行的安全 APDU 配置，从而所述比较器装置(34)用于将一个或多个参考命令与实现交易所运行的命令进行比较，并且根据所述比较器装置(34)进行的所述比较的结果，限制或者防止对这些数据、文件系统、命令或者安全条件的进一步访问或者修改。 因而，由于比较器(34)为每个要进行的不同类交易进行配置，所以智能卡设备可以在智能卡设备自身可用的存储器和处理能力的限制下提供改进的安全性。



1、一种可编程智能卡设备（10），带有文件系统（22、24）和使设备上文件系统与至少一个设备外文件和/或应用接口的操作软件，而且包括脚本引擎（32），其可运行一个或多个应用协议数据单元（APDU）以修改所述文件系统的结构和/或内容，或者用于访问所述文件系统或者与之相关的任何安全条件的命令；所述可编程智能卡设备（10）的特征在于：其包括比较器装置（34），其可由所述脚本引擎（32）运行的安全 APDU 配置，并且所述比较器装置（34）用于将一个或多个参考命令与如下命令进行比较：实现访问和/或修改设备上数据或文件系统的应用所执行的命令，或者用于访问所述系统或者与之相关的任何安全条件的命令，并且根据所述比较器装置（34）进行的所述比较的结果，限制或者防止对这些数据、文件系统、命令或者安全条件的进一步访问或者修改。

2、根据权利要求 1 的设备，其中所述比较器装置（34）用于将所述脚本引擎(32)运行的用于修改设备上数据、文件、命令或者安全条件的 APDU 代码与参考代码进行比较。

3、根据权利要求 2 的设备，其中所述比较器装置（34）还用于将所述脚本引擎运行的所述 APDU 的至少一个操作数与参考操作数进行比较。

4、根据权利要求 2 或 3 的设备，其中所述比较器装置（34）用于将所述脚本引擎运行的所述 APDU 的所述代码和/或操作数与代表多个参考值的参考代码或操作数进行比较。

5、根据权利要求 1 至 3 中任意一项的设备，其中所述比较器装置（34）用于将实现应用所执行的命令序列与参考序列进行比较。

6、根据权利要求 1 至 3 中任意一项的设备，其中所述比较器装置（34）用于在它未检测到与代表期望的命令、期望的多个命令或命令序列的参考

命令或多个参考命令的匹配时，限制或者防止对数据、文件系统、命令或者安全条件的进一步访问或修改。

7、根据权利要求 1 至 3 中任意一项的设备，其中所述比较器装置（34）用于在它检测到与参考命令或多个参考命令的匹配时，限制或者防止对数据、文件系统、命令或者安全条件的进一步访问或修改。

8、根据权利要求 1 至 3 中任意一项的设备，其中所述脚本引擎（32）用于运行从至少一个采用自描述消息的网络（因特网）标准语言格式的文件得到的一个或多个 APDU。

9、一种用于配置根据权利要求 1—8 任意一项的所述可编程智能卡设备的方法，所述方法包括：

提供读卡接口设备，用于将所述可编程智能卡设备的读卡器与所述可编程智能卡设备接口，以及

向所述可编程智能卡设备加载包括至少一个 APDU 的应用脚本，所述至少一个 APDU 用于修改所述设备上文件的结构和内容，或者用于访问所述文件系统或者与之相关的任何安全条件的命令；

所述方法的特征在于：上载至所述可编程智能卡设备的所述脚本还包括由所述智能卡设备上的脚本引擎运行以配置比较器装置的安全 APDU，所述比较器装置用于将一个或多个参考命令与如下命令进行比较：实现访问和/或修改设备上数据或文件系统的应用所执行的命令，或者用于访问所述系统或者与之相关的任何安全条件的命令；

根据所述比较器装置执行的所述比较的结果，限制或者防止对这些数据、文件系统、命令或者安全条件的进一步访问或者修改。

10、根据权利要求 9 的方法，其中可以向所述可编程智能卡设备加载多个不同应用脚本，每个所述应用脚本具有与之相关的安全 APDU；每当加载应用脚本时将所述相关的安全 APDU 加载至所述设备，这样，每次由所述脚本引擎运行不同的应用脚本时，所述比较器装置被重新配置。

11、根据权利要求 9 或 10 的方法，其中所述应用脚本和安全 APDU 从至少一个采用自描述消息的网络（因特网）标准语言格式的文件得到。

改进的智能卡系统

技术领域

本发明涉及智能卡系统的改进，具体涉及改进这种系统中安全结构的可能性。

背景技术

国际专利申请 No WO03/049056 中描述的智能卡系统包括可编程智能卡设备，其带有文件系统和操作软件，使设备上的文件系统可以和至少一个设备外的文件和/或应用交互，还包括脚本引擎，其可以运行一个或多个应用协议数据单元（APDU）以修改文件系统的结构和/或内容，或用于访问文件系统或者与之相关的任何安全条件的命令。

这样的系统中，可编程智能卡设备包括存储在设备上的存储器内的一个或多个应用和/或数据文件。例如，文件可能包括卡携带者的银行结余的详细内容，或者进行过或待进行的财务交易的详细内容。为了保证这些数据的完整性，保存这些文件和文件所包括的数据的存储器只能由卡上的处理器访问。该处理器包括脚本引擎，其可以运行从接口设备上载的脚本（卡可以插入到接口设备或者与之连接），以修改卡上的文件系统的结构或内容，或者用于访问文件系统或者与之相关的任何安全条件的命令。

在国际专利申请 No WO03/049056 的系统中，将脚本写成自描述性消息的网络（因特网）标准语言格式的文件，并将脚本从中央“密室”通过因特网安全传输到一个或多个接口设备，在接口设备，可将脚本加载到一个或多个用户的智能卡设备上。因而，因为可以用如可扩展置标语言（XML）的网络标准语言通过因特网安全传输文件，所以可以快速便捷地利用因特网分发智能卡设备上的应用软件的更新或者修改或重新格式化系统中使用的卡上的数据，同时保持高级别的安全性。

然而，虽然国际专利申请 No WO03/049056 中的基本系统是安全的，但是我们理解，仍然期望进一步提高系统的安全性。对于如处理财务交易

的安全性至关重要的智能卡应用来说，命令序列和发送至智能卡设备的应答及智能卡设备发出的应答必需符合特定的流。虽然可以开发特定应用软件在卡上运行，但是只有在接收到期望的下一条命令时才能正常应答，相反，如果命令不是所期望的那条，就给出错误。该方法在管理方面有所有通常存在的缺陷，特别是更新和修改。

发明内容

根据本发明，提供一种可编程智能卡设备，带有文件系统和使设备上文件系统与至少一个设备外文件和/或应用接口的操作软件，而且包括脚本引擎，其可运行一个或多个应用协议数据单元（APDU）以修改文件系统的结构和/或内容，或者用于访问文件系统或者与之相关的任何安全条件的命令；智能卡设备的特征在于，其包括比较器装置，其可由脚本引擎运行的安全 APDU 配置，并且比较器用于将一个或多个参考命令与如下命令进行比较：实现访问和/或修改设备上数据或文件系统的应用所运行的命令，或者用于访问系统或者与之相关的任何安全条件的命令，并且根据比较器装置进行的比较的结果，限制或者防止对这些数据、文件系统、命令或者安全条件的进一步访问或者修改。

因而，在国际专利申请 No WO03/049056 中描述的智能卡系统中，用脚本引擎来设置卡。可以通过设置卡提高安全，这样，通过仅比较命令代码或者比较代码和操作数，卡期望并从而监控某些命令序列的出现。

本发明还提供配置上述智能卡设备的方法，该方法包括：提供读卡接口设备，用于将可编程智能卡设备的读卡器与可编程智能卡设备接口；以及向可编程智能卡设备加载包括至少一个 APDU 的应用脚本，至少一个 APDU 用于修改设备上文件的结构和内容，或者用于访问文件系统或者与之相关的任何安全条件的命令；其中，上载至可编程智能卡设备的脚本还包括由智能卡设备上的脚本引擎运行以配置比较器装置的安全 APDU，比较器装置用于将一个或多个参考命令与如下命令进行比较：实现访问和/或修改设备上数据或文件系统的应用所执行的命令，或者用于访问系统或者与之相关的任何安全条件的命令；根据比较器装置执行的比较的结果，限制或者防止对这些数据、文件系统、命令或者安全条件的进一步访问或者

修改。

下面以示例方式参考附图详细描述本发明的实施例。

附图说明

附图是根据本发明的智能卡设备的示意图。

具体实施方式

图中简要示出上述系统中使用的智能卡设备 10。

设备 10 包括设备上存储器 20，其上存储有文件 22 和 24，还包括处理器 30，其包括脚本引擎 32 和可配置比较器 34。如前所述，设备上存储器 20 只可以由处理器 30 访问，不能从智能卡 10 以外直接访问。设备 10 还包括接口装置 40，其使得设备 10 与外部接口设备（未示出）交互。

对于所述示例，假定存储的文件 22 和 24 包括分别代表智能卡设备用户持有的某种财务账户的当前账户结余和上次账户结余的数据。当用卡来授权从用户账户转帐时，设备 10 与接口设备交互，以上载包括一个或多个应用协议数据单元（APDU）的文件，应用协议数据单元由脚本引擎 32 在设备 10 上运行，以修改设备存储器 20 中保存的各个文件的内容。交易可能很复杂，涉及多个命令，这些命令修改多个文件的内容，但是，简单起见，这里只考虑一个修改。

当卡用户使用设备 10 对向第三方进行的支付授权时，文件 22 内保存的当前账户结余被复制到文件 24，文件 24 存储上次账户结余，然后，修改文件 22 中的当前账户结余，以示出新的更小的结余。

这样的交易中，在为了实现交易而由脚本引擎 32 运行的 APDU 中的一系列命令中，有下面的一对命令：

COPY value in file 22 to file 24（复制 文件 22 中的值至文件 24）

WRITE new current balance to file 22（写入 新的当前结余至文件 22）

上述系统中，智能卡设备 10 插入或者连接到接口设备，在要开始交易时，接口设备将一个或多个 APDU 上载至设备处理器 32，然后，该一个或多个 APDU 由脚本引擎 32 运行，以修改文件 22 和 24 中的数据。根据本发明，APDU 包括安全 APDU 即“监察”APDU，其用于以适用于要进行的

交易的方式配置比较器34。实践中，安全APDU提供参考命令或代码，由脚本引擎32运行的命令与这些命令或代码进行比较。

在上述例子中，由脚本引擎32运行安全APDU时，安全APDU可以配置比较器34,这样比较器34可以进行比较以检测期望的一对命令"COPY value in file 22 to file 24"和"WRITE new current balance to file 22"。除非比较器做出肯定性匹配，交易就中止。

所给出的例子非常简单，但是要理解，比较器32可配置用于以同样方式监控很长的命令序列。

此外，比较器32可被配置为仅将命令的一部分与安全APDU提供的参考进行比较。例如，比较器可以确定"复制"命令是否包括文件名或文件标识符，在要进行特定交易时，要从该文件复制数据。或者，只监控命令内的操作数或者命令出现的序列，例如，检查"复制"命令后是否总跟着"写入"命令。

某些情况下，检测到匹配的情况下，可能也需要配置比较器32使交易中止。在上述交易中，例如，脚本引擎32无合适理由而从文件24到文件22进行复制，因而，如果检测到这样的命令，可能意味着正在进行诈骗。因而，比较器34可被配置为检测命令"COPY form file 22 to file 24"的存在，将其作为限制或防止对智能卡设备10上的文件或数据进行进一步修改的基础。

类似的，为了鉴别交易而寻求得到肯定匹配时，"否定匹配"可以基于部分比较。例如，如果特定命令序列中根本不应该出现某个文件时，比较器34可简单地被配置为寻找如特定设备上文件的文件名的特定代码，例如"文件24"。

或者，比较器34可被配置为检测命令和操作数的组合。上述例子中，比较器34可被配置为检测要从文件24进行复制的任何命令，因为这样的命令对于要进行的交易是不适当的。

复杂情况下，脚本引擎32和安全APDU就参考集合的肯定或否定匹配都是期望的，比较器34可被配置为检测特定的命令序列而不是一个命令。如果期望的命令集合不是简单的线性序列而是包括如国际专利申请WO2005/064555中描述的逻辑或者算数驱动分支，那么可用脚本引擎能力

通过比较器 34 映射这些命令路径。

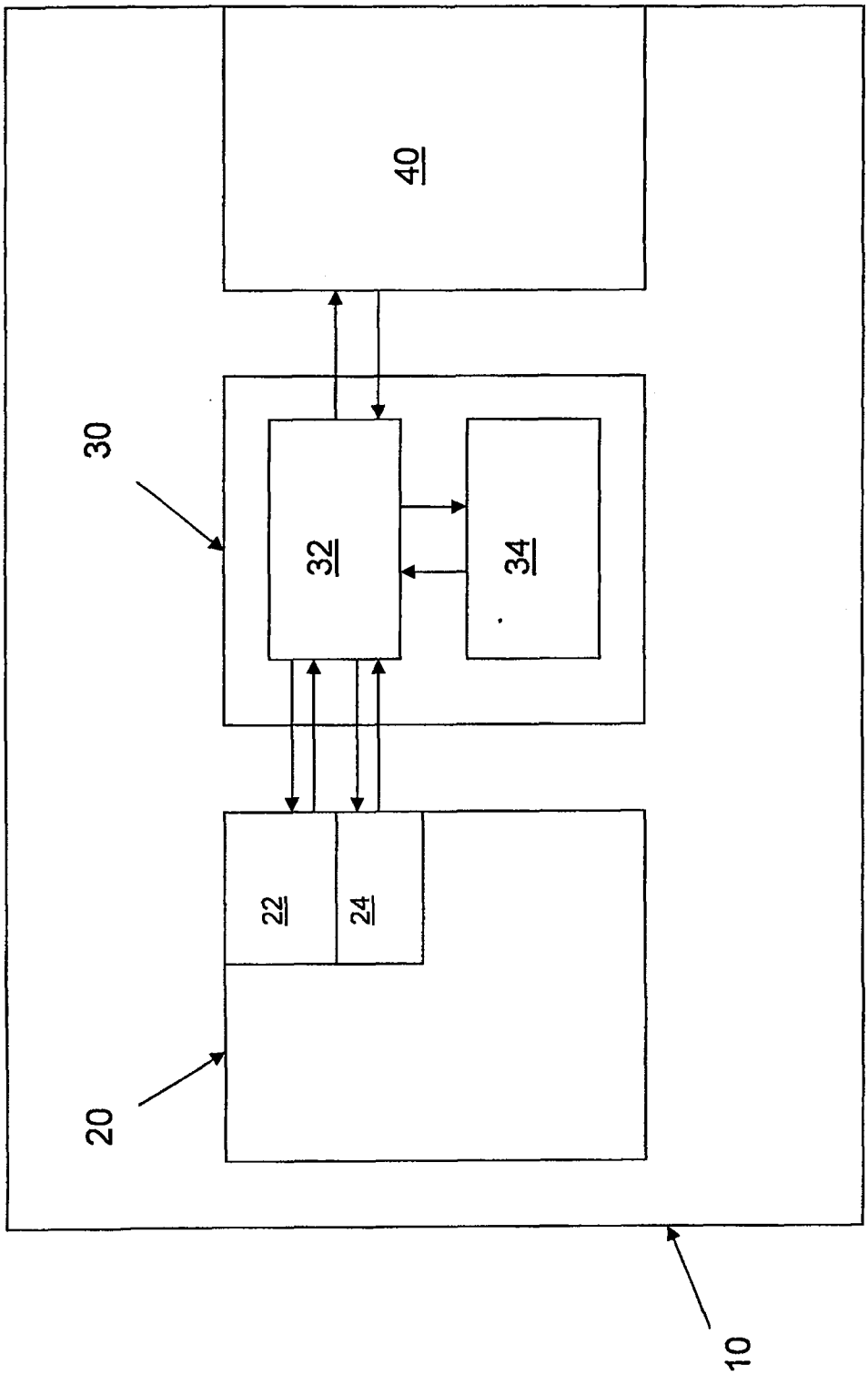
适当的话，比较器 34 还可以被配置为将命令与预定的一组或多个可能期望值进行比较，而不是仅与一个比较。

因而，APDU 的“期望命令”脚本和比较器一起工作，类似于状态机，脚本中的命令代表期望的命令序列，检测应该出现的命令或者检测不应该出现的命令，并且在特定比较产生特殊预定结果时，将状态设成“错误”。

应该理解，因为智能卡设备 10 上的比较器 34 由脚本引擎 32 根据安全 APDU 配置（在交易要开始时为每个交易上载作为命令序列一部分的安全 APDU），比较器 34 可以对要进行的特定交易类型进行适当的检查。

智能卡领域之外的在先技术设备利用进行这些比较的检查或者监控设备，但是这些设备硬连线到所处理的设备，而且，因为需要提供不同类型的交易，在先技术还要求更大的处理器能力和/或存储空间，这是在智能卡设备上不能提供的。利用在每次交易发生时为其配置的可配置比较器 34 意味着可以在智能卡设备上可用的相对小的处理器和存储器限制下，提供之前智能卡系统中不能使用的安全检查级别。

此外，如果发现对安全的新型诈骗攻击，或者需要处理新型交易，可以容易地根据需要修改脚本引擎 32 用来配置比较器 34 的用于每个类型交易的安全 APDU。


40
30
32
34
22
24
20
10