[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/32 (2006.01)

[12] 发明专利说明书

专利号 ZL 200510105502.1

[45] 授权公告日 2009 年 9 月 16 日

[11] 授权公告号 CN 100542088C

[22] 申请日 2005.9.23
[21] 申请号 200510105502.1
[30] 优先权
[32] 2005.8.11 [33] CN [31] 200510090183.1
[73] 专利权人 北京握奇数据系统有限公司
地址 100015 北京市朝阳区首都机场路万红西街 2 号
[72] 发明人 高 翔 王国荣
[56] 参考文献
CN1526218A 2004.9.1
CN1421816A 2003.6.4
CN1421817A 2003.6.4
审查员 高胜凯

[74] 专利代理机构 北京同达信恒知识产权代理有限公司
代理人 李 欣

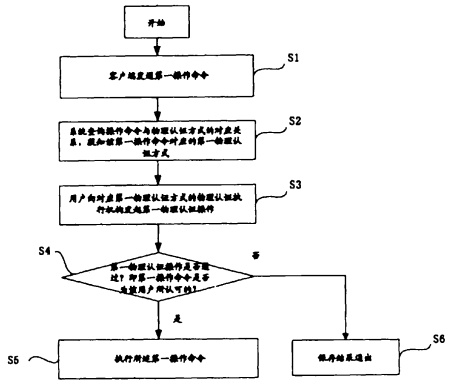
权利要求书 4 页 说明书 15 页 附图 8 页

[54] 发明名称

一种物理认证方法及一种电子装置

[57] 摘要

本发明涉及一种物理认证方法及实现这种方法的装置，该方法使用存储于电子装置中的操作控制列表，由合法使用者以物理的方式对电子装置进行的操作给以认证，从而在合法使用者和电子装置之间建立了绑定(对应)关系，不仅解决了网络交易中身份认证和交易认证的问题，保证了网络环境中客户端的安全，而且解决了数据存储设备防病毒的问题，保证了使用者数据的安全性。 本发明方法包括：设置一操作命令与物理认证方式的对应关系，当执行操作命令时，使用所述的物理认证方式进行认证。 本发明装置包括微处理器、操作通信接口、智能卡芯片和物理认证执行机构。



1、一种物理认证方法，适用于网络环境下的客户端通过电子装置执行操作命令的系统，其特征在于，设置操作命令与物理认证方式的对应关系，当进行安全运算操作时，包括以下步骤：

S1、客户端向电子装置发送进行安全运算操作的第一操作命令；

S2、系统查询所述的操作命令与物理认证方式的对应关系，获知所述第一操作命令对应的第一物理认证方式；

S3、用户向设置于电子装置上的对应于所述第一物理认证方式的物理认证执行机构发起第一物理认证操作，如果第一物理认证操作通过，表明客户端发送的第一操作命令为该用户所认可的，进入步骤S4，否则，结束流程；

S4、电子装置执行所述第一操作命令。

2、如权利要求1所述的方法，其特征在于，所述的操作命令与物理认证方式的对应关系，为操作控制列表，所述的操作控制列表中，设置操作命令内容以及对应的物理认证方式。

3、根据权利要求2所述的方法，其特征在于，所述的操作控制列表为二维列表，二维列表的行和列分别对应于操作命令内容以及对应的物理认证方式。

4、如权利要求3所述的方法，其特征在于，所述的操作控制列表中，还包括物理认证操作有效性判断规则。

5、如权利要求4所述的方法，其特征在于，所述的操作控制列表中，还包括物理认证操作的最大延时等待时间或有效截止时间。

6、根据权利要求1所述的方法，其特征在于，所述步骤S1中，所述操作命令包括安全运算命令和数据读写命令，所述安全运算命令包括数据加密、数据解密、数字签名、数字摘要，所述数据读写命令包括SCSI（Small Computer Systems Interface 小型计算机系统接口）规定的读写命令。

7、如权利要求1所述的方法，其特征在于，所述步骤S2和S3中，所述的物理认证方式，包括生物特征认证或操作特征认证。

8、如权利要求7所述的方法，其特征在于，所述的生物特征认证，包括指纹特征认证或瞳孔特征认证或口唇特征认证。

9、如权利要求7所述的方法，其特征在于，所述的操作特征认证，包括：按键操作或拨动开关操作。

10、如权利要求1所述的方法，其特征在于，所述的步骤S3，进一步包括以下步骤：S31、用户向物理认证执行机构发起第一物理认证信息；

S32、物理认证执行机构接收所述第一物理认证信息，并比较所述第一物理认证信息与存储的对应物理认证信息是否一致，如果一致，进入步骤S33，如果不一致，进入步骤S34；

S33、用户第一物理认证通过；

S34、拒绝用户通过第一物理认证。

11、如权利要求1所述的方法，其特征在于，所述的步骤S2中，还包括系统向用户发送物理认证提示信息的步骤。

12、如权利要求11所述的方法，其特征在于，所述的物理认证提示信息，可以是声音提示信息、触觉提示信息或者视觉提示信息。

13、如权利要求1所述的方法，其特征在于，所述第一操作命令为一组命令组合。

14、如权利要求1所述的方法，其特征在于，所述第一操作命令与物理认证方式的对应关系为逻辑表达关系，包括一对一，一对多或多对多的关系。

15、如权利要求1所述的方法，其特征在于，还包括当第一操作命令包含第一关键字时，对所述第一关键字进行第一验证的步骤。

16、一种电子装置，与网络环境下的客户端相连，其特征在于，包括：

操作运算模块，用于执行安全运算操作命令；

数据存储模块，用于保存用户数据和应用数据；

操作控制对应关系模块，设置有操作命令与物理认证方式的对应关系；

物理认证模块，用于接收用户输入的物理认证信息，并对其进行物理认证，

如果认证结果为通过，表明客户端向本电子装置发送的进行安全运算操作的命令为该用户所认可的，并将认证结果发送给处理模块；

处理模块，用于接收客户端向本电子装置发送的进行安全运算操作的命令信息，根据所述操作命令向操作控制对应关系模块请求对应的物理认证方式，并接收物理认证模块发送的认证结果；在接收到物理认证模块发送的认证结果为认证通过时，还用于向操作运算模块发送执行相关安全运算操作的命令，并接收操作运算模块的执行结果。

17、如权利要求16所述的装置，其特征在于，所述物理认证模块包括物理认证执行机构和认证比较模块；

所述的物理认证执行机构，用于接收用户输入的物理认证信息，并将所述的物理认证信息发送给所述的认证比较模块；

所述的认证比较模块，用于比较用户输入物理认证信息与系统存储信息，并得出认证结果。

18、如权利要求16所述的装置，其特征在于，所述的操作控制对应关系模块，包括：

操作控制列表存储模块，存储有操作控制列表；

操作控制列表查询模块，根据处理模块发送请求，向操作控制列表存储模块发送查询请求，并将所述的查询结果发送给处理模块。

19、如权利要求16所述的装置，其特征在于，所述的处理模块，还包括通信接口模块，与处理模块相连，用于处理模块和客户端之间进行信息交互。

20、如权利要求19所述的装置，其特征在于，所述的通信接口模块，可以是通用串行接口模块、高速串行接口模块、并行接口模块或火线（IEE1394）接口模块。

21、如权利要求16所述的装置，其特征在于，所述的物理认证模块，可以包括下述内容之一或者组合：

生物特征识别模块、操作特征识别模块。

22、如权利要求16所述的装置，其特征在于，还包括物理认证操作提示模块，其与处理模块相连，用于提示用户在物理认证模块上执行物理认证。

23、如权利要求22所述的装置，其特征在于，所述的物理认证操作提示模块，可以包括下述内容之一或者组合:

发声装置、发光装置、振动装置。

24、如权利要求16所述的装置，其特征在于，所述的数据存储模块可以是EPROM、EEPROM、智能卡芯片、非易失性存储器(NAND FLASH)、硬盘或移动硬盘。

一种物理认证方法及一种电子装置

技术领域

本发明涉及计算机和通信安全领域，尤其是一种物理认证方法及一种电子装置，利用存储于安全认证装置中的操作控制列表，由合法使用者以物理的方式对安全认证装置进行的操作给以认可。

技术背景

在任何网络交易环境中，安全问题主要存在于信源、信宿和信道，或者说存在于服务器、网络和客户端。目前服务器的安全性可以通过采用物理控制、安全管理、高等级硬件平台与操作系统、系统与网络安全软件及设备等手段来保证。网络上数据传输的安全性可通过基于密码学方法的数据加解密技术解决而且效果很好。客户端是指安装在用户的计算机上的应用程序及其相关的软硬件运行环境，由于网络管理系统无法控制用户的计算机并对其计算机进行检查，并且，网络环境下的客户端使用者获得服务的方式是通过网络，取代了传统面对面获得服务的方式，服务方式的这种改变使得客户端使用者由自然人转变为“网络人”。因此，客户端“网络人”身份的合法性和交易的合法性就成为保证客户端安全性的重要手段。

在现有技术中，通过客户端对使用者的身份进行合法性认证的技术主要有基于智能卡技术、类似于通用总线钥匙（USB KEY）等电子装置的口令验证技术、PKI（公共密钥基础设施）体系的数字签名技术等，这些技术虽然能够实现对使用者的身份认证，但不能够解决使用者对交易合法性认证的问题，即不能解决合法使用者与电子装置之间绑定的问题。驻留于用户计算机中的“木马”程序能够通过监测客户端应用程序的运行过程，在合法使用者完全不知情的情

况下，获得合法使用口令，并能够启动电子装置生成合法的数字签名，完成网上交易过程，存在较大安全隐患。

此外，现有的数据存储设备，如移动硬盘或U盘，当与计算机连接时，计算机上的恶意程序可以在使用者不知情的情况秘密地读取数据存储设备中的内容，或者秘密地向数据存储设备中写内容，导致数据存储设备成为病毒的传播者。

发明内容

为克服现有技术的不足，本发明的目的在于提供一种物理认证方法及一种电子装置，合法使用者可以通过物理的方式对安全认证装置进行操作给以认证，从而实现对交易的认证或对数据读写操作的认证。

一种物理认证方法，适用于网络环境下的客户端通过电子装置执行操作命令的系统，其特征在于，设置操作命令与物理认证方式的对应关系，当进行安全运算操作时，包括以下步骤：

S1、客户端向电子装置发送进行安全运算操作的第一操作命令；

S2、系统查询所述的操作命令与物理认证方式的对应关系，获知所述第一操作命令对应的第一物理认证方式；

S3、用户向设置于电子装置上的对应于所述第一物理认证方式的物理认证执行机构发起第一物理认证操作，如果第一物理认证操作通过，表明客户端发送的第一操作命令为该用户所认可的，进入步骤S4，否则，结束流程；

S4、电子装置执行所述第一操作命令。

所述的操作命令与物理认证方式的对应关系，为操作控制列表，所述的操作控制列表中，设置操作命令内容以及对应的物理认证方式。

所述的操作控制列表为二维列表，二维列表的行和列分别对应于操作命令内容以及对应的物理认证方式。

所述的操作控制列表中，还包括物理认证操作有效性判断规则。

所述的操作控制列表中，还包括物理认证操作的最大延时等待时间或有效截止时间。

所述步骤 S1 中，所述操作命令包括安全运算命令和数据读写命令，所述安全运算命令包括数据加密、数据解密、数字签名、数字摘要，所述数据读写命令包括 SCSI（Small Computer Systems Interface 小型计算机系统接口）规定的读写命令。

所述步骤 S2 和 S3 中，所述的物理认证方式，包括生物特征认证或操作特征认证。所述的生物特征认证，包括指纹特征认证或瞳孔特征认证或口唇特征认证。所述的操作特征认证，包括：按键操作或拨动开关操作。

所述的步骤 S3，进一步包括以下步骤：

S31、用户向物理认证执行机构发起第一物理认证信息；

S32、物理认证执行机构接收所述第一物理认证信息，并比较所述第一物理认证信息与存储的对应物理认证信息是否一致，如果一致，进入步骤 S33，如果不一致，进入步骤 S34；

S33、用户第一物理认证通过；S34、拒绝用户通过第一物理认证。

所述的步骤 S2 中，还包括系统向用户发送物理认证提示信息的步骤。

所述的物理认证提示信息，可以是声音提示信息、触觉提示信息或者视觉提示信息。

一种电子装置，与网络环境下的客户端相连，其特征在于，包括：

操作运算模块，用于执行安全运算操作命令；

数据存储模块，用于保存用户数据和应用数据；

操作控制对应关系模块，设置有操作命令与物理认证方式的对应关系；

物理认证模块，用于接收用户输入的物理认证信息，并对其进行物理认证，如果认证结果为通过，表明客户端向本电子装置发送的进行安全运算操作的命令为该用户所认可的，并将认证结果发送给处理模块；

处理模块，用于接收客户端向本电子装置发送的进行安全运算操作的命令

信息，根据所述操作命令向操作控制对应关系模块请求对应的物理认证方式，并接收物理认证模块发送的认证结果；在接收到物理认证模块发送的认证结果为认证通过时，还用于向操作运算模块发送执行相关安全运算操作的命令，并接收操作运算模块的执行结果。

所述物理认证模块包括物理认证执行机构和认证比较模块；

所述的物理认证执行机构，用于接收用户输入的物理认证信息，并将所述的物理认证信息发送给所述的认证比较模块；

所述的认证比较模块，用于比较用户输入物理认证信息与系统存储信息，并得出认证结果。

所述的操作控制对应关系模块，包括：

操作控制列表存储模块，存储有操作控制列表；

操作控制列表查询模块，根据处理模块发送请求，向操作控制列表存储模块发送查询请求，并将所述的查询结果发送给处理模块。

所述的处理模块，还包括通信接口模块，与处理模块相连，用于处理模块和客户端之间进行信息交互。

所述的通信接口模块，可以是通用串行接口模块、高速串行接口模块、并行接口模块或火线（IEE1394）接口模块。

所述的物理认证模块，可以包括下述内容之一或者组合：

生物特征识别模块、操作特征识别模块。

所述的装置，还包括物理认证操作提示模块，其与处理模块相连，用于提示用户在物理认证模块上执行物理认证。

所述的物理认证操作提示模块，可以包括下述内容之一或者组合：

发声装置、发光装置、振动装置。

所述的数据存储模块可以是 EPROM、EEPROM、智能卡芯片、非易失性存储器(NAND FLASH)、硬盘或移动硬盘。

本发明的优点在于：通过不同的物理方式操作状态建立合法使用者和物理

认证装置之间的绑定关系，从而保证了网络环境中客户端的安全。这种绑定关系的建立，不仅解决了网络交易中身份认证和交易认证的问题，而且解决了数据存储设备防病毒的问题。通过这种身份认证和交易认证最终保证的不仅仅是合法的设备在做交易,而是合法的使用者在做交易，保证了合法的设备的每一笔交易都是得到合法使用者的授权和认证，从而保证了整个网络交易体系的安全有效。

附图说明

图 1 为本发明电子装置的逻辑构成图;

图 2 为本发明电子装置简化实施构成图;

图 3 为本发明主流程图;

图 4 为本发明实施例 1 的流程图;

图 5 为本发明实施例 2 的流程图;

图 6 为本发明实施例 3 的流程图;

图 7 为本发明实施例 4 的流程图;

图 8 为本发明实施例 5 的流程图。

具体实施方式

下面结合说明书附图来说明本发明的具体实施方式。

请参阅图 1 本发明的装置构成图。本发明的电子装置的硬件系统 110 包括以下装置:

1、微处理器 140，用于接收客户端发送的操作命令信息，并将处理结果返回客户端；同时用于判断使用者提供的物理认证操作的有效性。该微处理器在生物特征识别认证模式下，从操作控制列表存储模块指定的位置读取存储物理认证生物特征识别比对信息，并与比较用户输入的生物特征识别信息进行对比，得出认证结果；在操作特征识别认证模式下，将用户输入的操作特征识别信息

与操作控制列表存储模块中规定的有效性判断原则进行对比，得出认证结果；在生物特征识别和操作特征识别组合的认证模式下，根据操作控制列表存储模块规定的顺序，先后按上述步骤进行生物特征识别认证和操作特征识别认证，得出认证结果。

2、操作命令通信接口 120 和通信接口芯片 130，其一端与所述微处理器 140 相连，另一端与客户端相连，用于在微处理器 140 和客户端之间进行操作命令和确认信息的交换，建立数据传输通道，进行数据交换，它包括任何可以满足通信性能要求的接口方式，如通用串行总线（USB）接口、串行接口、并行接口、火线(IEE1394)接口；

3、操作控制列表存储模块 150，连接微处理器，可以是固件存储器，如 ROM，EPROM，EEPROM 或非易失性存储器（NAND FLASH）这样存储器当中的任何合适的一种，但并不限于这些存储器，也可以是智能卡芯片，用于存储进行安全认证操作的操作控制列表；

4、操作控制列表查询模块 160，连接微处理器，用于在操作控制列表中查找客户端通过操作命令通信接口下发的操作命令，并判断此操作命令是否需要进行物理认证操作；

5、物理认证执行机构 170，包括指纹采集器、按键装置、拔动开关装置等，与微处理器相连，用于用户通过物理方式输入安全认证的各种操作；

6、操作运算模块 180，连接微处理器，用于完成操作控制列表指定的操作命令和控制操作控制列表的安全更新；

7、物理认证操作提示模块 190，包括发光二极管、蜂鸣器等，与微处理器相连，用于提示使用者在物理认证执行机构上进行物理认证操作；

8、数据存储模块 200，连接微处理器，可以是 EPROM，EEPROM 或非易失性存储器（NAND FLASH）、硬盘或移动硬盘这样存储器当中的任何合适的一种，但并不限于这些存储器，用于存储用户数据和应用数据。 在本发明的装置中，通信接口芯片 130、操作控制列表存储模块 150、操作控制列表查询模块

160、操作运算模块 180 可以部分或全部在微处理器 140 中，物理认证操作提示模块 190 也根据操作控制列表中描述的物理认证操作提示方式进行删减。

请参阅图 2，是本发明电子装置的具体实例，物理方式电子装置的硬件系统 210 包括以下装置：

电子装置通过 USB 通讯协议 220 与客户端连接，USB 接口芯片 230、微处理器 240 构成一条可与所述客户端通讯的数据传输通道。客户端通过 USB 通讯协议 220 和 USB 接口芯片 230 将数据传输给所述微处理器 240，该微处理器 240 先按 USB 通讯协议对收到的数据包进行数据完整性校验，并得到客户端下发的操作命令，如符合 ISO7816 标准的智能卡 APDU（应用协议数据单元）命令；符合 SCSI 规定的读写命令。

该微处理器 240 从智能卡芯片 260 中读取操作控制列表，并在操作控制列表中按 APDU 命令格式或 SCSI 规定的读写操作代码，通过逐条对比的方式查找此命令，判断此命令是否需要物理认证操作，若不需要，该微处理器 240 直接将此 APDU 命令发送给智能卡芯片 260，智能卡芯片 260 完成 APDU 命令指定的安全运算操作后，将执行结果回送微处理器 240；或者该微处理器 240 直接按 SCSI 规定对 NAND FLASH 270 进行读写操作，微处理器 240 按 USB 通讯协议 220，通过 USB 接口芯片 230，将执行结果传输给客户端；如果此命令需要物理认证操作，该微处理器 240 同时从操作控制列表中获得指定的物理认证操作及其属性信息，如物理认证操作为：揿按键；有效操作判断原则为：按键次数＝1 次；最大延时等待时间为 500 毫秒；有效截止日期为：2010 年 12 月 31；物理认证操作提示模式为：客户端。

根据操作控制列表中描述的物理认证操作提示模式，该微处理器 240 将从操作控制列表中得到此命令指定的物理认证操作及其属性信息，按 USB 通讯协议 220，通过 USB 接口芯片 230 将数据传输给客户端，并等待接收客户端返回的确认信息；该微处理器 240 收到客户端的确认信息后，根据操作控制列表的描述，检查使用者是否在 500 毫秒内完成了一次有效的按键 260 操作，如果在

有效时间内按键260操作有效，则该微处理器240将此APDU命令发送给智能卡芯片260，智能卡芯片260完成APDU命令指定的安全运算操作后，将执行结果回送微处理器240;或者该微处理器240按SCSI规定对NAND FLASH 270进行读写操作；否则该微处理器240拒绝执行此命令；微处理器240按USB通讯协议220，通过USB接口芯片230，将此命令的处理结果传输给客户端。

下面说明本发明一种物理认证方法的实施方案。

为了实现合法使用者与物理认证装置之间的绑定，本发明提出的操作控制列表，如表1所示。

表1操作控制列表结构

操作 / 功能	物理认证操作	有效操作判断规则	生物特征比对信息存储位置	最大延时等待时间	有效截止日期	物理认证操作提示模式
数据加密	揿按键	按键次数=N次（N≥1）	/	M毫秒（M≥1）	YY-MM-DD	客户端
数据解密	拔动位置开关	开关位置从A点拔到B点，再拔到A点	/	M毫秒（M≥1）	YY-MM-DD	灯光闪烁
数字签名	指纹比对	比对一致性	智能卡芯片中的EF10文件	M毫秒（M≥1）	YY-MM-DD	声音提示
SCSI规定的读操作	揿按键	按键次数=N次（N≥1）	/	M毫秒（M≥1）	YY-MM-DD	客户端
SCSI规定的写操作	揿按键	按键次数=N次（N≥1）	/	M毫秒（M≥1）	YY-MM-DD	客户端

在表1中包括操作命令内容和对应的物理认证方式，操作命令包括安全运算，该安全运算内容可以是数据加密、数据解密、数字签名、数字摘要等；和数据读写，该数据读写内容可以SCSI规定的读写操作等；物理认证方式包括操作特征识别认证、生物特征识别认证或者二者的组合，操作特征识别认证包括按键拨动位置开关；生物特征识别认证包括指纹比对、瞳孔比对、口唇特征

认证等。

该表 1 中还包括物理认证操作有效性判断规则，比如按键次数等。

该表 1 中还包括生物特征比对信息存储位置，如智能卡芯片中的 EF10 文件等。

该表 1 中还包括最大延时等待时间或有效截止时间。

下面举例说明表 1 的具体应用。

在有效时间内，当客户端要求物理认证装置完成数据加密运算时，物理认证装置只有在 500 毫秒内收到合法使用者的 1 次有效按键操作后，才能执行数据加密运算操作，并将运算结果返回客户端；

同样地，在有效时间内，当客户端要求物理认证装置完成数据解密运算时，物理认证装置只有在 500 毫秒内收到合法使用者的 1 次有效拔动位置开关操作后，才能执行数据解密运算操作，并将运算结果返回客户端；

在有效时间内，当客户端要求物理认证装置完成数据签名运算时，物理认证装置只有在 1000 毫秒内完成对合法使用者的指纹采集和对比，并且比对合法后，才能执行数据签名运算操作，并将运算结果返回客户端。

表 1 仅是操作控制列表的应用举例，并不是将物理认证装置实现的安全运算与合法使用者提供的物理认证操作的对应关系限定于此。

请参阅图 3 本发明的主流程图。在本发明方案中，客户端向电子装置发送安全运算命令，请求进行安全运算，根据本发明的物理认证方法，对该安全运算命令进行物理认证，具体包括以下步骤：

S1、客户端发送操作命令；

S2、查询所述的操作命令与物理认证方式的对应关系，获知所述操作对应的物理认证方式；

S3、用户向物理认证执行机构发起所述的物理认证操作；

S4、判断所述的物理认证是否通过？如果该物理认证通过，进入步骤 S5，否则，进入步骤 S6，结束流程；

S5、执行所述安全运算操作命令;

S6、保存结果退出，结束流程。

下面结合具体的电子装置的安全运算命令操作过程，来说明本发明的方案。

实施例 1:

如图 4 所示，是实施例 1 的一个流程示意图，从图中可见，主要包括以下步骤:

S11、客户端向电子装置发送安全运算命令;

S12、客户端接收电子装置的返回信息;

S13、客户端判断此安全运算是否需要物理认证操作？如果是，进入步骤 S14，如果否，进入步骤 S18;

S14、客户端向电子装置发送确认信息;

S15、客户端判断电子装置是否返回执行结果？如果是，进入步骤 S18，如果否，进入步骤 S16;

S16、客户端判断是否等待超时？如果是，进入步骤 S17，如果否，返回步骤 S15;

S17、客户端出错退出;

S18、客户端保存结果退出。

实施例 1 中，客户端根据电子装置返回信息判断该安全运算操作是否需要进行物理认证，如果需要物理认证，则返回确定信息给电子装置。电子装置先进行物理认证，再进行该安全运算操作。

实施例 2:

如图 5 所示，是实施例 2 的流程示意图，从图中可见，其包括如下步骤:

S21、客户端向电子装置发送安全运算命令;

客户端向电子装置发送安全运算命令，通过通讯接口将客户端的安全运算

请求命令传输给电子装置的微处理器。

S22、客户端接收电子装置的返回信息;

电子装置的微处理器在操作控制列表查找此安全运算命令，判断此命令是否需要进行物理认证，若不需要，微处理器直接按命令执行，并将执行结果传输给客户端，如果此命令需要进行物理认证，微处理器同时从操作控制列表中获得物理认证操作的状态及其属性信息，微处理器将物理认证操作状态及其属性信息通过通信接口传输给客户端，并等待接收客户端返回的确认信息。

S23、客户端判断安全运算结果是否返回？如果是进入步骤 S210，如果否进入步骤 S24;

S24，客户端判断是否需要提示用户进行物理认证操作？

如果系统设置有提示用户进行物理认证操作的设置，则进入步骤 S25，否则进入步骤 S26;

S25、客户端弹出信息框提示用户进行物理认证操作;

如果系统设置信息框提示用户进行物理认证，则弹出相关的信息框，提示用户进行相关物理认证操作。

S26、用户执行相关物理认证操作，向电子装置回送确认信息;

用户根据所述提示，通过电子装置的物理认证模块执行相关的物理认证操作，认证通过后，向电子装置回送确认信息。电子装置的微处理器收到客户端的确认信息后，检查物理认证操作状态，并判断此物理认证操作是否有效，如果物理认证操作有效，则执行该安全操作命令，如果物理认证操作无效，则拒绝执行此命令。

S27、客户端判断电子装置是否返回了安全运算结果？如果是，进入步骤 S210，如果否，进入步骤 S28;

S28、客户端判断等待是否超时？如果超时，进入步骤 S29，否则返回步骤 S27;

有效时间内如果电子装置没有返回安全运算结果，则进入步骤 S29。

S29、客户端提示出错，退出流程;

S210、客户端保存结果并退出流程。

实施例 2 增加了提示用户进行物理认证操作的相关方案。

实施例 3:

如图 6 所示，是实施例 3 的流程示意图，从图中可见，其包括如下步骤:

S31、客户端向电子装置发送读取操作控制列表命令;

S32、客户端接收电子装置返回的操作控制列表信息;

S33、客户端在操作控制列表中查找准备执行的安全运算命令;

S34、客户端判断该安全运算命令是否需要物理认证？如果是进入步骤 S35，如果否进入步骤 S312;

S35，客户端判断物理认证操作属性是否合法？如果是，进入步骤 S36，如果否，进入步骤 S311;

S36、客户端将该安全运算命令及其需要的物理认证操作信息或不需要物理认证操作信息发送给电子装置;

S37、电子装置判断该安全运算命令需要的物理认证操作是否有效？如果是，进入步骤 S38，如果否，进入步骤 S310;

S38、电子装置执行所述的安全运算命令，并将执行结果返回给客户端;

S39、客户端保存结果并退出流程;

S310、电子装置向客户端返回错误提示;

S311、客户端提示出错，退出流程;

S312、客户端向电子装置发送安全运算命令，进入步骤 S38。

实施例 3 中，客户端直接从电子装置中读取控制列表信息，并查找操作控制列表确定本次安全运算操作是否需要物理认证操作。并且增加了验证物理认证操作属性是否合法的步骤。

实施例 4:

如图 7 所示，是实施例 4 的流程示意图，从图中可见，其包括如下步骤:

S41、客户端向电子装置发送安全运算命令;

S42、电子装置在操作控制列表中查找该安全运算命令;

S43、电子装置判断该安全运算命令是否需要物理认证？如果是进入步骤 S44，如果否进入步骤 S410;

S44，电子装置判断物理认证操作属性是否合法？如果是，进入步骤 S45，如果否，进入步骤 S413;

S45,电子装置判断是否需要在本装置上提示用户进行物理认证操作？如果是进入步骤 S412，如果否进入步骤 S46;

S46,电子装置判断是否需要在客户端提示用户进行物理认证操作？如果是进入步骤 S47，如果否进入步骤 S49;

S47、电子装置将此命令需要的物理认证操作信息发送给客户端;

S48、电子装置接收客户端回送的确认信息;

S49、电子装置判断该安全运算命令需要的物理认证操作是否有效？如果是，进入步骤 S410，如果否，进入步骤 S413;

S410、电子装置执行所述的安全运算命令，并将执行结果返回给客户端;进入步骤 S411;

S411、客户端保存结果并退出流程。

S412、电子装置激活本装置上物理认证操作提示模块器件的工作状态，进入步骤 S49;

如果系统设置的物理认证操作提示模式为灯光闪烁，则按一固定频率点亮和熄灭电子装置上的发光二极管。

S413、电子装置向客户端返回错误提示。

S414、客户端提示出错，退出流程。

实施例 4 在实施例 3 的基础上，增加了在本装置和客户端上提示用户进行物理认证操作的步骤。

实施例 5:

如图 8 所示，是实施例 5 的一个流程示意图，从图中可见，主要包括以下步骤:

S51、客户端向电子装置发送 SCSI 规定的写命令;

S52、客户端接收电子装置的返回信息;

S53、客户端判断此写命令是否需要物理认证操作？如果是，进入步骤 S54，如果否，进入步骤 S58;

S54、客户端向电子装置发送确认信息;

S55、客户端判断电子装置是否成功执行写操作？如果是，进入步骤 S58，如果否，进入步骤 S56;

S56、客户端判断是否等待超时？如果是，进入步骤 S57，如果否，返回步骤 S55;

S57、客户端出错退出;

S58、客户端正常退出。

实施例 5 中，客户端根据电子装置返回信息判断该写操作是否需要进行物理认证，如果需要物理认证，则返回确定信息给电子装置。电子装置先进行物理认证，再进行该写操作。

实施例 6:

在网络交易环境下，客户端使用者想通过网上银行从自己的银行帐户将 1000 元人民币转帐到供电局指定的银行帐号，完成当月电费的缴纳。他可以通过以下操作步骤来实现:

首先，使用者通过物理认证装置在客户端登录网上银行服务，在完成口令验证和数据证书有效性验证等传统的身份认证后，使用者发出转帐 1000 元的申请。

然后，客户端将使用者的申请上传网上银行服务器，网上银行服务器根据使用者发出的申请，生成这笔网上交易的关键数据，并将这些关键数据回送客户端，要求使用者对这些关键数据进行数字签名确认。

再次，客户端向物理认证装置发送对这些关键数据进行数字签名的安全运算命令，使用者根据客户端或物理认证装置发出的物理认证操作提示信息，在物理认证装置的物理认证执行机构上进行物理认证操作。当使用者提供了有效的物理认证操作后，物理认证装置完成对这些关键数据的数字签名运算，并将运算结果反馈给客户端。

最后，客户端将得到的数字签名数据上传给网上银行服务器，网上银行服务器在验证了由客户端返回的使用者数字签名数据的合法性后，完成使用者指定的转帐交易。

实施例 6 将本发明电子装置应用于网上银行业务，结合了一个具体的网上银行业务进行说明，采用该物理认证方法，利用存储于安全认证装置中的操作控制列表，由合法使用者以物理的方式对安全认证装置进行的操作给以认可。由此可见，交易的安全性大为增强。

以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的权利要求范围之内。

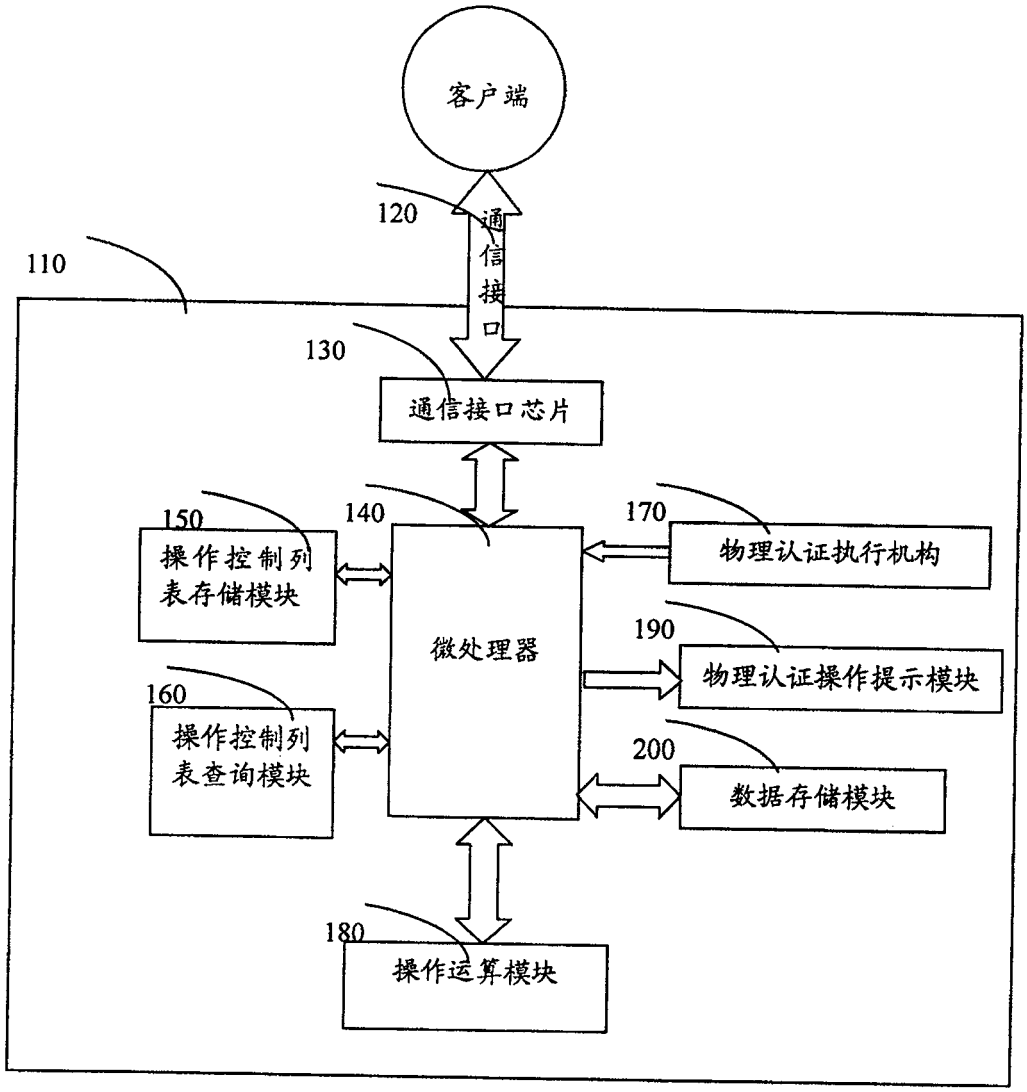

客户端
120
通信接口
110
130
通信接口芯片
150
操作控制列表存储模块
140
微处理器
170
物理认证执行机构
190
物理认证操作提示模块
160
操作控制列表查询模块
200
数据存储模块
180
操作运算模块

图 1

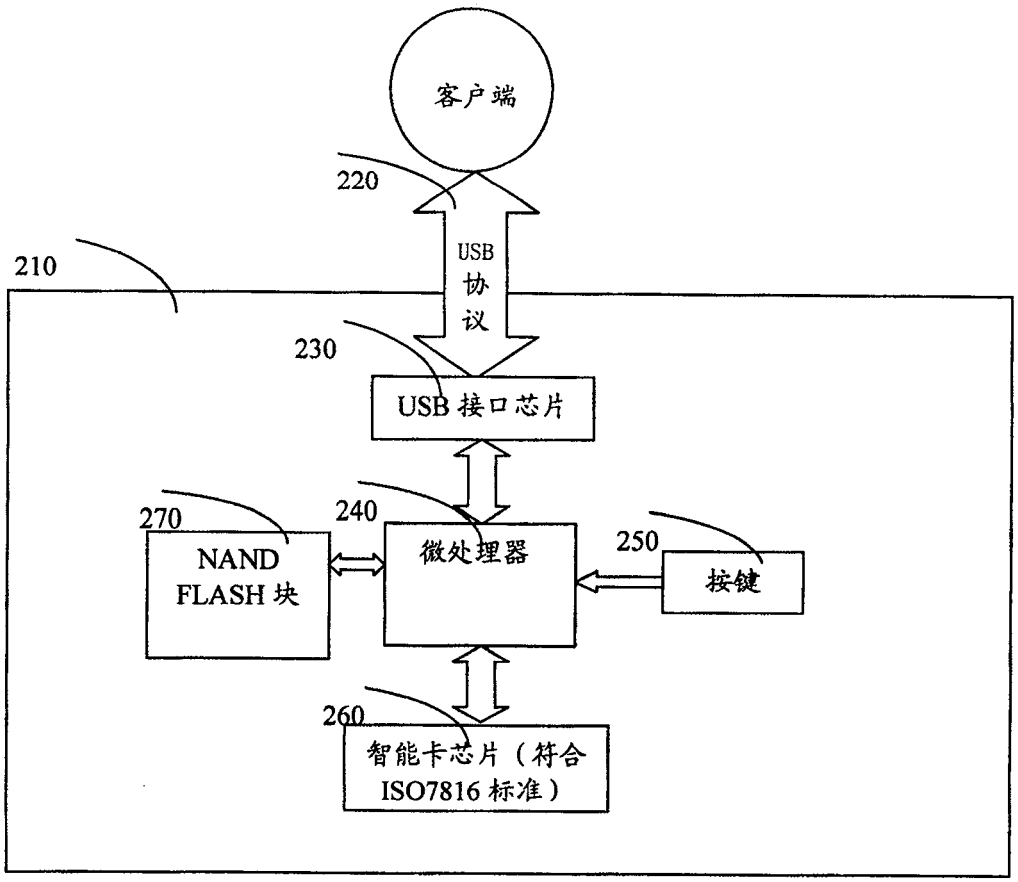

客户端
220
USB
协
议
210
230
USB 接口芯片
270
240
250
NAND
FLASH 块
微处理器
按键
260
智能卡芯片（符合
ISO7816 标准）

图 2

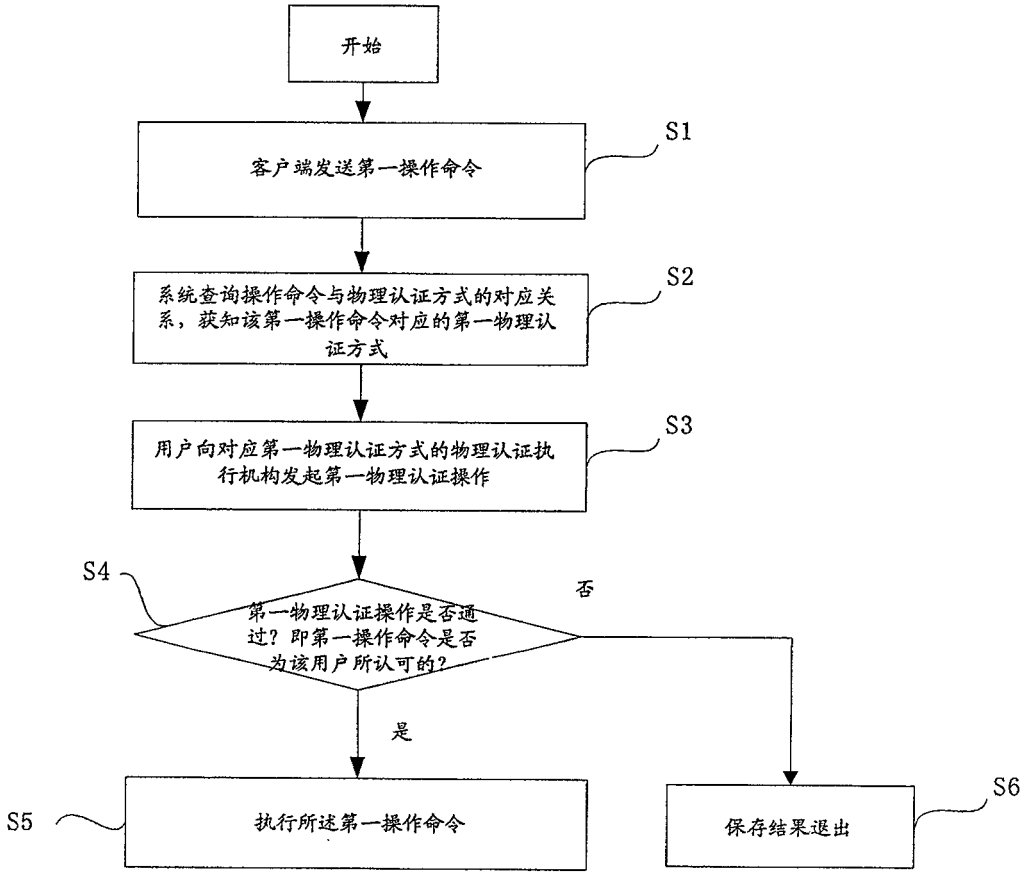

开始
客户端发送第一操作命令
S1
系统查询操作命令与物理认证方式的对应关系，获知该第一操作命令对应的第一物理认证方式
S2
用户向对应第一物理认证方式的物理认证执行机构发起第一物理认证操作
S3
S4
第一物理认证操作是否通过？即第一操作命令是否为该用户所认可的？
否
是
S5
执行所述第一操作命令
保存结果退出
S6

图 3

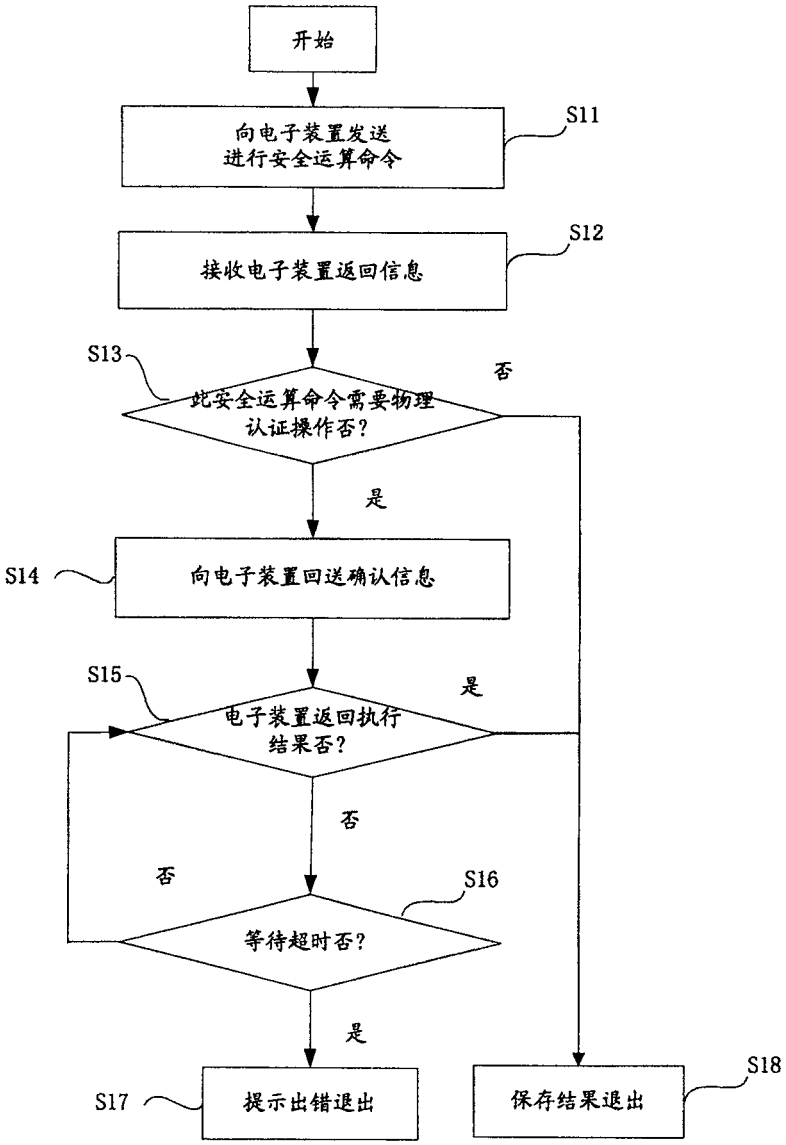

开始
向电子装置发送
进行安全运算命令
S11
接收电子装置返回信息
S12
S13
此安全运算命令需要物理
认证操作否?
否
是
S14
向电子装置回送确认信息
S15
电子装置返回执行
结果否?
是
否
否
S16
等待超时否?
是
S17
提示出错退出
保存结果退出
S18

图 4

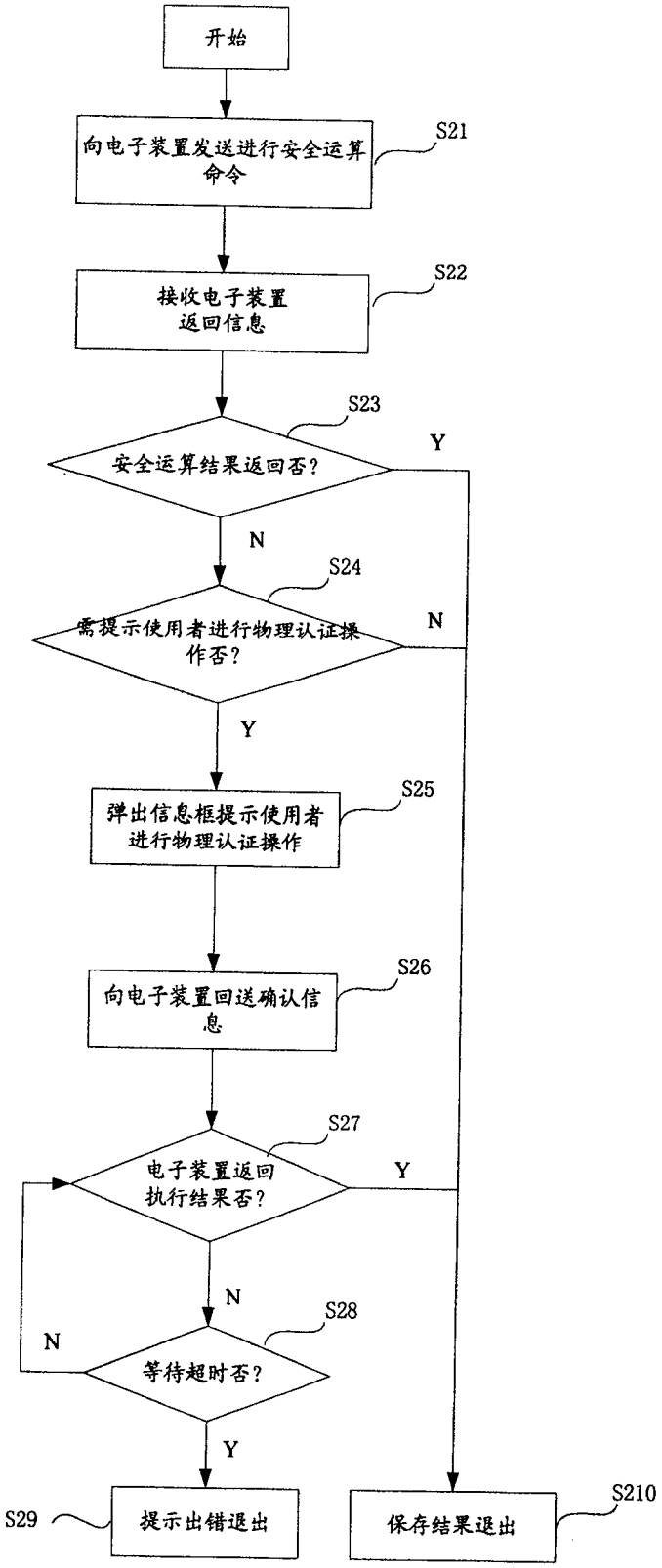

开始
向电子装置发送进行安全运算命令
S21
接收电子装置返回信息
S22
S23
安全运算结果返回否?
Y
N
S24
需提示使用者进行物理认证操作否?
N
Y
弹出信息框提示使用者进行物理认证操作
S25
向电子装置回送确认信息
S26
S27
电子装置返回执行结果否?
Y
N
S28
N
等待超时否?
Y
S29
提示出错退出
保存结果退出
S210

图 5

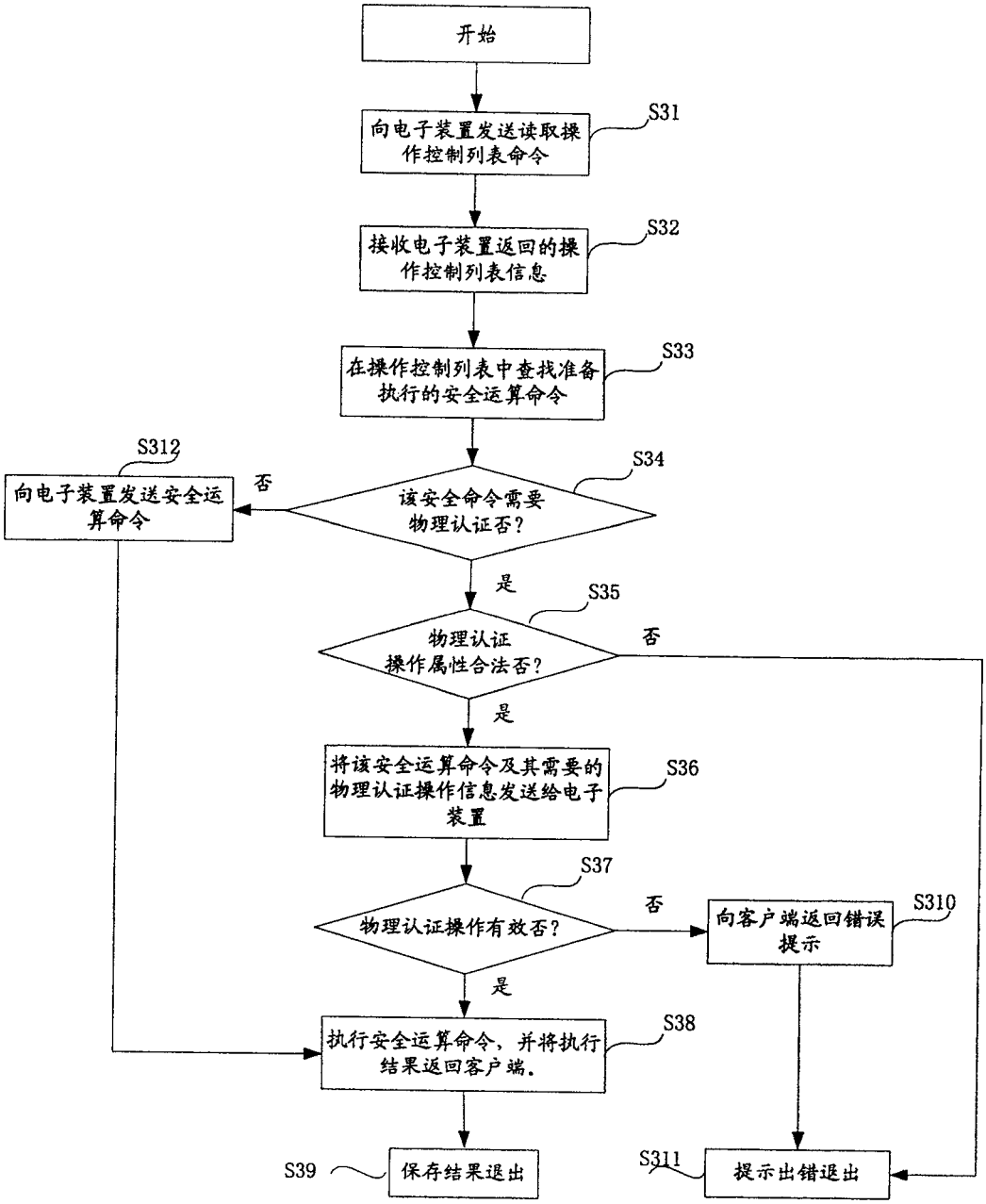

开始
向电子装置发送读取操作控制列表命令
S31
接收电子装置返回的操作控制列表信息
S32
在操作控制列表中查找准备执行的安全运算命令
S33
该安全命令需要物理认证否?
S34
否
向电子装置发送安全运算命令
S312
是
物理认证操作属性合法否?
S35
否
是
将该安全运算命令及其需要的物理认证操作信息发送给电子装置
S36
物理认证操作有效否?
S37
否
向客户端返回错误提示
S310
是
执行安全运算命令，并将执行结果返回客户端.
S38
保存结果退出
S39
提示出错退出
S311

图 6

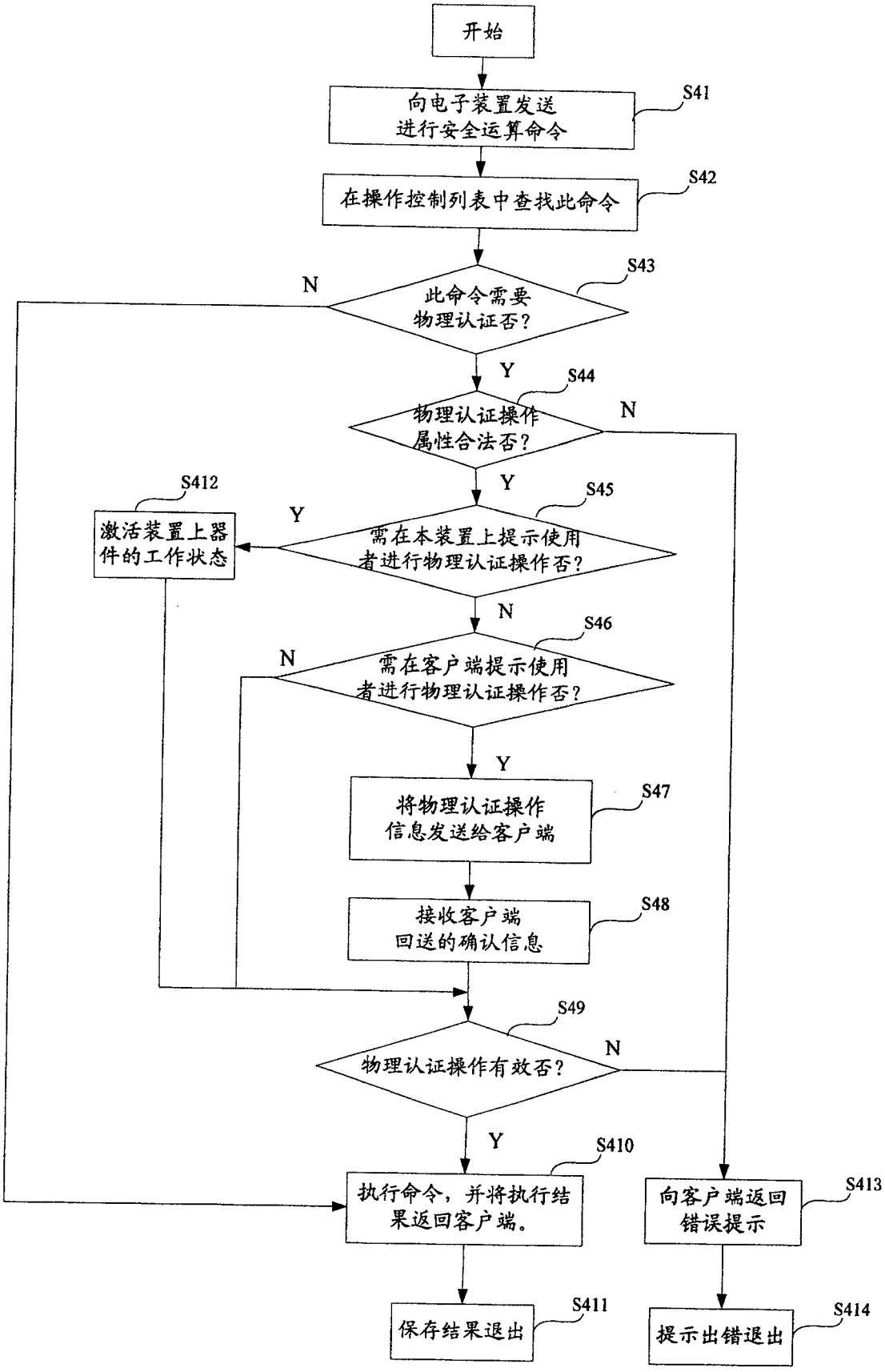

开始
向电子装置发送进行安全运算命令
S41
在操作控制列表中查找此命令
S42
此命令需要物理认证否？
S43
N
Y
物理认证操作属性合法否？
S44
N
Y
需在本装置上提示使用者进行物理认证操作否？
S45
Y
激活装置上器件的工作状态
S412
N
需在客户端提示使用者进行物理认证操作否？
S46
N
Y
将物理认证操作信息发送给客户端
S47
接收客户端回送的确认信息
S48
物理认证操作有效否？
S49
N
Y
执行命令，并将执行结果返回客户端。
S410
向客户端返回错误提示
S413
保存结果退出
S411
提示出错退出
S414

图 7

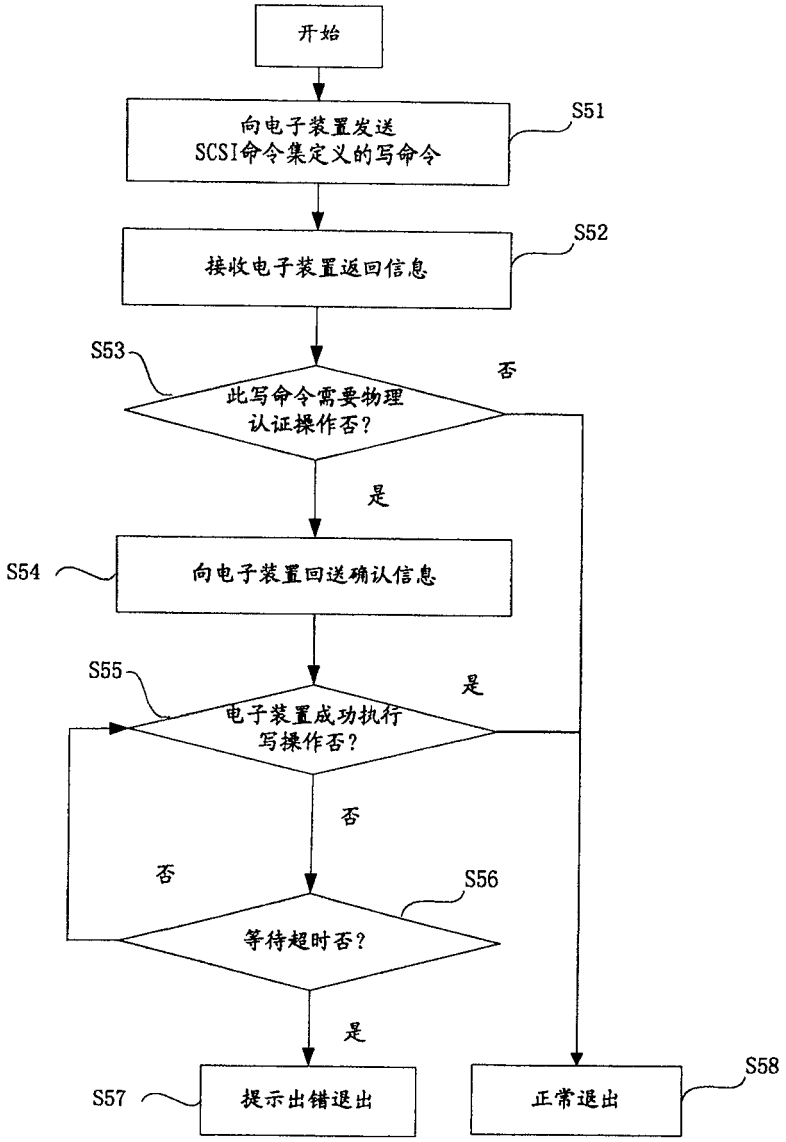

开始
向电子装置发送
SCSI命令集定义的写命令
S51
接收电子装置返回信息
S52
S53
此写命令需要物理
认证操作否?
否
是
S54
向电子装置回送确认信息
S55
电子装置成功执行
写操作否?
是
否
否
S56
等待超时否?
是
S57
提示出错退出
正常退出
S58

图 8