[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G06F 1/00

[12] 发明专利说明书

[21] ZL 专利号 96196400.6

[45] 授权公告日 2004 年 6 月 23 日

[11] 授权公告号 CN 1154902C

[22] 申请日 1996.8.8 [21] 申请号 96196400.6
[30] 优先权
[32] 1995. 8.21 [33] FR [31] 95/09952
[32] 1995.11. 3 [33] FR [31] 95/13038
[86] 国际申请 PCT/FR1996/001269 1996.8.8
[87] 国际公布 WO1997/007448 法 1997.2.27
[85] 进入国家阶段日期 1998.2.20
[71] 专利权人 柯内·色布
地址 法国姬安库
[72] 发明人 柯内·色布
审查员 刘 栩

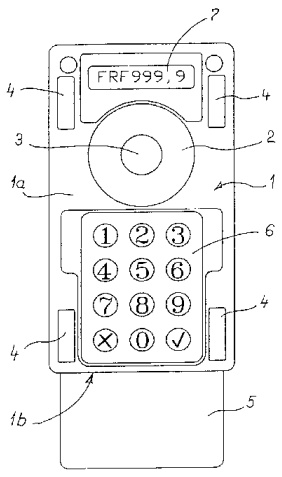
[74] 专利代理机构 上海专利商标事务所
代理人 张政权

权利要求书 6 页 说明书 15 页 附图 12 页

[54] 发明名称 状态访问装置及方法

[57] 摘要

本发明涉及一种状态访问装置，欲用于与主电子设备连机，其以一指针装置结合至少一个微电路卡连结器所构成，其特点在于：其亦结合个人数据读取构件，特别是对个人用户，及此该个人信息为与储存于微电路卡 5 上的本地信息作比较，而不需将该个人信息传送至主设备作比较。



ISSN1008-4274

1．一种状态访问装置，用于与主电子设备连机，其由包含至少一微电路卡连结器的指针接口装置所构成，

其特征在于：所述状态访问装置还包括用于获得对于使用者为特定的个人信息数据的装置，该个人信息数据包括代表该使用者之密码，且该个人信息数据与储存于微电路卡（5）中的本地信息数据作比较，以提供使用者的验证信息数据，该验证信息数据被传送至该主电子设备，而不需将该个人信息数据传送至主电子设备。

2．根据权利要求1所述的状态访问装置，其特征在于：用于获得对于使用者为特定的个人信息数据的装置包含：一个用于输入字母及数字识别码的键盘，或者一个设有一感知区以输入一手写个人信息数据的面板。

3．根据权利要求1或2所述的状态访问装置，其特征在于：此用于获得对于使用者为特定的个人信息数据的装置包括一用以输入一个生物信息识别信号的感测器，包括指纹图像感测器和／或眼睛内部图像感测器，和／或一结合语音辨别装置的语音感测器。

4．根据权利要求1所述的状态访问装置，其特征在于：其包括一用以键入个人信息数据的键盘，和／或用以监视交易处理的显示装置。

5．根据权利要求1所述的状态访问装置，其特征在于：此用于获得对于使用者为特定的个人信息数据的装置包含导致在主电子设备的荧光屏上显示虚拟键盘的装置，所述虚拟键盘具有图形显示（51），且于每一次启动上述装置，其配置可以随机方式改变，其中，取得个人信息数据是通过指向所述图形显示（51）及在所述图形显示（51）后定位此指针的位置时验证而具体制成，此指针信息的处理及其在模拟荧光屏上的确认在此唯一的状态访问装置中具体制成。

6．根据权利要求1所述的状态访问装置，其特征在于：用于获得个人信息数据的装置包含一个用于取得及数字化该使用者声音的模块。

7．根据权利要求1所述的状态访问装置，其特征在于：其包括语音合成装置与语音再现装置，以用于交易处理的控制。

8．根据权利要求1所述的状态访问装置，其特征在于：此用于获得个人信息数据的装置包含一个被指向的触按区，其包括一叠置于触按区的触控表面上的键盘的显示。

9．根据权利要求1所述的状态访问装置，其特征在于：其包括一工作时钟，及传送至此指针接口装置的登录日期的数字数据，此数据包括一由储存于微电路卡（5）中的数据所允许计算的数据序列，及由使用者所键入的数据与一时钟所传送的时序。

10．根据权利要求1所述的状态访问装置，其特征在于：其包括允许与主电子设备在网络线上共同操作的装置，当插入电子钱包或信用卡，可执行下列全部或一部份的密码交易操作：

（a）付款（b）还款（c）取消操作（d）货币选择，和/或当插入电子钱包，可执行下列安全密码交易的全部或一部份，（e）由一银行帐户载入电子钱包的数据（f）传送电子钱包的金额值至银行账户（g）由一电子钱包传送一金额值至另一电子钱包，（h）由一电子钱包借款及查核其信用卡的信用度。

11．根据权利要求1所述的状态访问装置，其特征在于：其包括允许与主电子设备分开独立操作和/或共同操作的装置，当电子钱包或信用卡被置入其内时，可执行下列全部或一部份操作：（a）确认目前金额值或存款余额（b）读取最近交易的清单或记录清单（c）锁住一电子钱包（d）改变识别码。

12．根据权利要求1所述的状态访问装置，其特征在于：其包括在相同微电路卡内的金融操作之间执行交易处理的装置。

13．根据权利要求1所述的状态访问装置，其特征在于：其包括一含有电子钱包操作的装置，及在两电子钱包连续插入一相同连接器之间，允许其执行下列全部或一部份操作的装置：（a）由一电子钱包传送一金额值至另一电子钱包（b）由一电子钱包传送一金额值至此装置本身（c）由电子钱包信用借款或向电子钱包贷款，或贷款给一信用卡相同金额或由一信用卡借款相同金额（d）取消此操作。

14．根据权利要求1所述的状态访问装置，其特征在于：含有电子钱包操作的上述装置被包括于一可移动的微电路卡（5）中。

15．根据权利要求1所述的状态访问装置，其特征在于：其亦包括一指示笔和/或数字式触摸屏，以及一显示装置，其中，当所述状态访问装置包括数字式触摸屏时，此数字式触摸屏与显示装置为叠置。

16．一种在用于与主电子设备连机的状态访问装置中对主电子设备访问提供安全的过程的方法，所述状态访问装置由包含至少一微电路卡连结器的指针接口装置所构成，所述状态访问装置还包括用于获得对于使用者为特定的个人信息数据的装置，该个人信息数据包括代表该使用者的密码，且该个人信息数据与储存于微电路卡（5）

中的本地信息数据作比较，以提供使用者的验证信息数据，该验证信息数据被传送至该主电子设备，而不需将该个人信息数据传送至主电子设备，所述方法的特征在于：该主电子设备之至少一项特定功能是仅当使用者输入与微电路卡中被储存的信息数据相符的个人信息数据后，方可允许使用者访问，且查证个人信息数据与记录于微电路卡中的信息数据的相符性是在包含连接至主电子设备的微电路读卡机的接口装置内实现，而不需将个人信息数据传送至主电子设备。

17．根据权利要求１６所述的过程的方法，其特征在于：信息以通信协议的码帧形式传送，码帧包括一组字段，每一个字段由包括多个预定比特的编码序列所构成，每一个码帧具有一识别字段（ＦＩＤ）及具有至少下列其中一个字段：

－用于指针信息的字段，

－关于保密装置信息的字段。

18．根据权利要求17所述的过程的方法，其特征在于：关于保密装置信息的字段包括下列依序说明字段的全部或一部份：

－检查字段（ＯＰＣ），

－定义保密操作信息长度（ＤＬＥＮ）的字段，

－包括全部或一部份保密操作信息（ＣＬＧ）或（ＲＰＬ）的字段，

－检查该信息正确完整性的字段（ＣＲＣ）。

19．根据权利要求18所述的过程的方法，其特征在于：此检查字段（ＯＰＣ）至少包括下列信息数据：

－有关一个或多个保密操作的密码（ＯＰＣ．Ｃ）

－由该码帧所影响之保密操作的地址（ＯＰＣ．Ａ），

－关于一以延伸码帧所传送的保密操作的信息数据字段的字节数目（ＯＰＣ．Ｓ），其中，此数目（ＯＰＣ．Ｓ）至少等于字段长度（ＯＰＣ）。

20．根据权利要求17所述的过程的方法，其特征在于：此接口装置具有驱动器，该驱动器供给用于指示至此应用软件的信息，及同时提供信息传送至该应用软件或另一个同时启动的应用软件及其保密操作装置。

21．根据权利要求１６所述的过程的方法，其特征在于：提供安全包括使用一允许计数器（ＬＣＮＴ），其以所设定安装或允许的限制次数，检查相同密码操作的多次传送。

22．根据权利要求21所述的过程的方法，其特征在于本地与远端安全密码装置

间密码作业的传送操作包括下列全部或一部分步骤：

一参加的保密装置的相互确认，

一目的装置上操作码的安全密码拷贝，

一确认拷贝的有效性，

一确认原始装置中密码操作的无效性。

23．根据权利要求 22 所述的过程的方法，其特征在于：所述参加的保密装置的相互确认的步骤包括一个被安装于保密装置之一上用于储存、管理与执行的保密操作，或者用于分散式操作该密码操作的操作，通过使用该接口装置读取的个人唯一数据码确认传送的发出者，而不需将此码传送至该会话式电子设备。

24．根据权利要求 23 所述的过程的方法，其特征在于：确认原始装置中密码操作的无效性的步骤包括将其密码清除，及将除了此密码操作的分散操作装置以外的资源释放，且此计数器被减 1 。

25．根据权利要求 22 所述的过程的方法，其特征在于：此接口装置具有驱动器，该驱动器供给用于指示至此应用软件的信息，及同时提供信息传送至该应用软件或另一个同时启动的应用软件及其保密操作装置。

26．根据权利要求 1 6 所述的过程的方法，其特征在于：此接口装置具有驱动器，该驱动器供给用于指示至此应用软件的信息，及同时提供信息传送至该应用软件或另一个同时启动的应用软件及其保密操作装置。

27．根据权利要求 1 6 所述的过程的方法，其特征在于：此主电子设备传送目前有关交易至状态访问装置，此信息被以语音合成转换，及此交易的有效性确认是通过插入此装置中的微电路卡的拥有人的字语的发音或预设片语的语音指令具体实现。

28．一种在用于与主电子设备连机的状态访问装置中以密码数据处理交易的过程的方法，所述状态访问装置由包含至少一微电路卡连结器的指针接口装置所构成，所述状态访问装置还包括用于获得对于使用者为特定的个人信息数据的装置，该个人信息数据包括代表该使用者的密码，且该个人信息数据与储存于微电路卡（ 5 ）中的本地信息数据作比较，以提供使用者的验证信息数据，该验证信息数据被传送至该主电子设备，而不需将该个人信息数据传送至主电子设备，所述方法的特征在于包括将使用者个人信息数据与储存于微电路卡中的数据作比较的步骤，此比较步骤在该状态访问装置内执行，其可构成一防止计算机欺骗者的防火墙。

29．根据权利要求 28 所述的过程的方法，其特征在于：信息以通信协议的码帧

形式传送，码帧包括一组字段，每一个字段由包括多个预定比特的编码序列所构成，每一个码帧具有一识别字段（ＦＩＤ）及具有至少下列其中一个字段：

－用于指针信息的字段，

－给予保密操作信息长度的字段。

30．根据权利要求29 所述的过程的方法，其特征在于：关于保密装置信息的字段包括下列依序说明字段的全部或一部份：

－检查字段（ＯＰＣ），

－定义保密操作信息长度（ＤＬＥＮ）的字段，

－包括全部或一部份保密操作信息（ＣＬＧ）或（ＲＰＬ）的字段，

－检查该信息正确完整性的字段（ＣＲＣ）。

31．根据权利要求30所述的过程的方法，其特征在于：此检查字段（ＯＰＣ）至少包括下列信息数据：

－有关一个或多个保密操作的密码（ＯＰＣ．Ｃ）

－由该码帧所影响之保密操作的地址（ＯＰＣ．Ａ），

－关于一以延伸码帧所传送的保密操作的信息数据字段的字节数目（ＯＰＣ．Ｓ），其中，此数目（ＯＰＣ．Ｓ）至少等于字段长度（ＯＰＣ）。

32．根据权利要求29所述的过程的方法，其特征在于：此接口装置具有驱动器，该驱动器供给用于指示至此应用软件的信息，及同时提供信息传送至该应用软件或另一个同时启动的应用软件及其保密操作装置。

33．根据权利要求28所述的过程的方法，其特征在于：此接口装置具有驱动器，该驱动器供给用于指示至此应用软件的信息，及同时提供信息传送至该应用软件或另一个同时启动的应用软件及其保密操作装置。

34．一种用以在配置接口装置的会话式电子设备中进行保密操作的管理与执行的过程的方法，用于根据一个通信协议而控制一个图形用户接口，其特征在于：该通信协议包括保密操作之一个延伸通信协议，且该方法包括一个本地处理步骤，用于通过以该接口装置输入个人密码至该接口装置之内而辨识该使用者，且使得记录于一个微电路卡内的个人数据的保密操作被导入至一个植入于该接口装置内的一个连接器，而不需要将该密码传送至该会话式电子设备。

35．根据权利要求34所述的过程的方法，其特征在于：信息以通信协议的码帧形式传送，码帧包括一组字段，每一个字段由包括多个预定比特的编码序列所构成，

每一个码帧具有一识别字段（ＦＩＤ）及具有至少下列其中一个字段：

－用于指针信息的字段，

－给予保密操作信息长度的字段。

36．根据权利要求35所述的过程的方法，其特征在于：关于保密装置信息的字段包括下列依序说明字段的全部或一部份：

－检查字段（ＯＰＣ），

－定义保密操作信息长度（ＤＬＥＮ）的字段，

－包括全部或一部份保密操作信息（ＣＬＧ）或（ＲＰＬ）的字段，

－检查该信息正确完整性的字段（ＣＲＣ）。

37．根据权利要求36所述的过程的方法，其特征在于：此检查字段（ＯＰＣ）至少包括下列信息数据：

－有关一个或多个保密操作的密码（ＯＰＣ．Ｃ）

－由该码帧所影响之保密操作的地址（ＯＰＣ．Ａ），

－关于一以延伸码帧所传送的保密操作的信息数据字段的字节数目（ＯＰＣ．Ｓ），其中，此数目（ＯＰＣ．Ｓ）至少等于字段长度（ＯＰＣ）。

38．根据权利要求35所述的过程的方法，其特征在于：此接口装置具有驱动器，该驱动器供给用于指示至此应用软件的信息，及同时提供信息传送至该应用软件或另一个同时启动的应用软件及其保密操作装置。

39．根据权利要求34所述的过程的方法，其特征在于：此接口装置具有驱动器，该驱动器供给用于指示至此应用软件的信息，及同时提供信息传送朝向相同或另一个同时启动的应用软件及其保密操作装置。

状态访问装置及方法

技术领域

本发明涉及一种状态访问装置的领域，其以指针装置结合一个或数个用于微电路卡的连结器所制成。

此装置被设计用以运行由微电路卡装置口令的交易，以确认卡片固定器和/或检查不同阶段的交易。

此类应用主要对于主设备资源的状态访问，及对与主设备连接或连机的外部设备所提供资源作状态访问，储存于主设备或与主设备连接或连机的外部设备或电子提款机等的允许软件操作的管理。

定义

“微电路卡”的意义为一支持装置，通常为一卡片，包括一个或数个集成电路运行处理功能和/或储存操作智能卡，或微处理器卡片，通常称之为“芯片卡”，无接点卡或ＰＣＭＣＩＡ卡，其即皆为此例子。

“微电路卡连结器”为依标准或特定通信协议操作信号交换于硬件与微电路卡接口间的任何装置。信号交换可以电气连接或无线链路，例如电磁波或光链路运行。

“主设备”意即计算机终端机，工作站，个人计算机，多媒体终端机等，特别是，但非绝对的，所有上述设备包括双向连接装置，皆可为暂时性的或永久性连接至本地或公众通信网络。

此项“指针装置”意即任何手动操作装置，用户可用于操作可见图像物件。其为使用于具有荧光屏及一以可见图像物件操作用户图形界面的会话式主设备。此例如包括一光机械鼠标器，需要一特殊滚动装置的光鼠标器，一滚球或轨迹球，一数字笔，或一光标，一触按指针器，一摇杆或一电动摇杆，或一用于ＣＤ-Ｉ远端控制摇杆系统。

背景技术

此接口装置与其所命令的设备共同连接，及其以ＲＳ232接口，ＵＳＢ通信

端口，或一相等系统连接，或于其他情况由无线传输链路连接，例如以红外线或微波链路。在一些情况，特别是当此主设备为一可携带式计算机，这些装置可集成安装于此设备内，甚至此装置代替一本身内含单元。

一般而言，其为可易于相互替换的装置，因多数主设备制造商已采用共同标准。及与主装备比较，其亦相当便宜，及与主设备无关，其可毫无困难地以相等装置替换。

其于现有技术描述中已建议集成一微电路卡连接器于特定接口指针装置中。此例如ＥＰ485275欧洲专利或德国专利ＤＥ326735中所述。在ＥＰ485275欧洲专利申请案中所述的接口装置提出最新技艺的装置。其包括一微电路卡连接器，直接连接至计算机与接口装置间的共同端子，允许有关指针功能信号交换，及对微电路卡所具有的口令功能操作的信号交换。此接口装置于此微电路卡及其所连接的计算机间以透通性方式操作。对此接口装置不作任何信号处理，其仅确保于微电路卡与计算机间的电气连接。因此个人识别码键入整个过程处理在主设备上完成，此为不方便的，及对例如 INTERNET（互联网）公众网络的商业发展形成甚大阻碍。

此技艺的实际问题

实际上，现今主设备几乎皆连接至少一个网络，不论于一机构内，或至一公众网络，例如 INTERNET。因此对第三者连接本身至主设备，及检查其所处理的数据，为可能及很容易的。有一些技术解决方法以过滤第三者的访问数据，但这些解决方法违反大多数用户的开放精神，及其所希望提升的通信层次。其亦需作复杂选定，以获得最佳性能，而此通常超过一般用户的能力范围。

发明内容

本发明的目的为克服上述缺点，而提出一状态访问装置，其可大为提高安全程度，以防止第三者欲经由主设备与一公众或内部网络间的链路取得此微电路所含有的口令或访问键，而作不允许的任意侵入。若侵入计算机的内存中将不允许访问用户的证明数据。

根据本发明的一个方面，提供一种状态访问装置，用于与主电子设备连机，其由包含至少一微电路卡连结器的指针接口装置所构成，所述状态访问装置还包括用于获得对于使用者为特定的个人信息数据的装置，该个人信息数据包括代表该使用者之密

码，且该个人信息数据与储存于微电路卡（5）中的本地信息数据作比较，以提供使用者的验证信息数据，该验证信息数据被传送至该主电子设备，而不需将该个人信息数据传送至主电子设备。

根据本发明的另一方面，提供一种在用于与主电子设备连机的状态访问装置中对主设备访问提供安全的过程的方法，所述状态访问装置由包含至少一微电路卡连结器的指针接口装置所构成，所述状态访问装置还包括用于获得对于使用者为特定的个人信息数据的装置，该个人信息数据包括代表该使用者的密码，且该个人信息数据与储存于微电路卡（5）中的本地信息数据作比较，以提供使用者的验证信息数据，该验证信息数据被传送至该主电子设备，而不需将该个人信息数据传送至主电子设备，所述方法的特点在于：该主设备之至少一项特定功能是仅当使用者输入与微电路卡中被储存的信息数据相符的个人信息数据后，方可允许使用者访问，且查证个人信息数据与记录于微电路卡中的信息数据的相符性是在包含连接至主设备的微电路读卡机的接口装置内实现，而不需将个人信息数据传送至主设备。

根据本发明的另一方面，提供一种在用于与主电子设备连机的状态访问装置中以密码数据处理交易的过程的方法，所述状态访问装置由包含至少一微电路卡连结器的指针接口装置所构成，所述状态访问装置还包括用于获得对于使用者为特定的个人信息数据的装置，该个人信息数据包括代表该使用者的密码，且该个人信息数据与储存于微电路卡（5）中的本地信息数据作比较，以提供使用者的验证信息数据，该验证信息数据被传送至该主电子设备，而不需将该个人信息数据传送至主电子设备，所述方法的特点在于包括将使用者个人信息数据与储存于微电路卡中的数据作比较的步骤，此比较步骤在该状态访问装置内执行，其可构成一防止计算机欺骗者的防火墙。

根据本发明的另一方面，提供一种用以在配置接口装置的会话式电子设备中进行保密操作的管理与执行的过程的方法，用于根据一个通信协议而控制一个图形用户接口，其中：该通信协议包括保密操作之一个延伸通信协议，且该方法包括一个本地处理步骤，用于通过以该接口装置输入个人密码至该接口装置之内而辨识该使用者，且使得记录于一个微电路卡内的个人数据的保密操作被导入至一个植入于该接口装置内的一个连结器，而不需要将该密码传送至该会话式电子设备。

为达到上述本发明的目的，事实上本发明的微电路卡可于本地操作，意即于接口指针装置中，而非于主设备中操作。此为基本特色。其确保于一端为用户识别，及另一端为计算机及其可连接的通信网络间作分隔。

用户识别的装置创建于接口指针装置中，其仅允许用户访问。其可取得通常为秘密的个人数据，例如其本人口令。此数据被由本地微计算器以记录于此卡片内的数据查核。此微计算器通常集成于微电路卡中，但亦可能结合于此接口装置中。此项确认并不包括由此装置或本发明的处理其传送至计算机的任何机密数据。比较后以对用户的认可或未认可的数据显示，其为传至计算机仅有的数据。此可实际上避免被第三者以本地或电话网络作介接连机至计算机取得例如口令的机密数据。

本发明的新增特色如下：

本发明可容易地以下列不同特色提升性能：

-其包括一用以取得测定辨识信号的感测器，例如指纹影像感测器和/或眼睛影像感测器，和/或一语音辨认感测器；

-其包括用于处理交易的语音控制装置；

-此键盘及或此荧光屏为于鼠标器的上表面，以此方式，使连结于鼠标器外壳上的盖子为闭合位置，当此芯片卡的连结器未使用时，其可保护键盘和/或荧光屏；

-芯片卡插入槽在功能键与上述鼠标器外壳的主要部份间制成一标准高度导槽，及上述按键被装置于外壳主要部份上面；

-于此例中接口装置具有一指纹影像感测器，此装置的外壳具有一引导区，操作者可将例如手指、大姆指等放置其上；

-此装置包括一永久电源的时钟，其确保操作的日期登录，特别是金融上的操作；

-此装置具有至少两芯片卡的输入；

-其具有管理与运行装置，以至少一口令操作装置与主设备应用软件结合；

-其包括允许于口令操作的储存装置、管理与运行间口令操作传送的装置，及一微电路卡包括这些安全口令的分布式操作；

-其具有卡夹板与插脚及两芯片卡连结器，及具有读取，压缩及记录写入数据，及接着装入至主设备的装置；

-其包括个人多媒体辅助设备和/或集成装置以操作一个或多个桌上型应用装置，例如计算器、日记或时钟等；

-此装置包括一永久时钟，及将具有数据顺序的标注日期的数值数据传送至

接口设备的装置，除了时脉所提供的数据顺序外，此数据顺序为对于微电路卡的储存数据及用户键入数据的认可核算。

本发明亦有关于主设备中口令操作管理与运行处理，其包括在连机至主设备的接口装置中，将个人数据与记录于微电路卡中的数据作比较，而不需将该个人信息传送至主设备比较。此接口装置结合个人数据读取装置及至少一微电路卡连接器。

依一较佳的实施模式，此处理包括一由此接口装置指针装置的通信协议规格所衍生的延伸通信协议。此通信协议可于应用软件与指针间仅使用一串列端口，及依本发明口令装置结合于此装置中。

因此，依较佳的通信协议型式，数据及指令被以包括多个字段所组成的码框传送，每一个字段含有预定数目比特的编码顺序，每一码框包括一识别字段，及至少包括下列其中一个字段：

-指针信息字段，

-有关于安全口令装置信息字段

对于口令装置的信息字段必需包括一控制字段，其规定接于其后的可选择字段的信息型态，与定义安全口令操作信息的长度，及上述信息正确完整性的控制字段。

更进步地，此过程提供指针信息至应用软件，及同时确保信息传送至相同或另一同时启动的应用软件及其安全口令操作装置。

最好此装置以码框型式传送由安全口令装置所发出的信息，此码框第一个字段为特定指针码框，其依上述整个信息修改，或此信息分割为数个相同型式码框。因此，此指针码框及此延伸码框可被交替变换。

依一实施例，此安全口令储存及该口令操作的运行装置被结合于可拆装的小型微电路中。因此，该口令操作的储存与运行装置的管理及有效使用性可被制成，而与此装置的维护无关。

以下结合附图进一步说明本发明的结构特点及目的。

附图说明

图 1 为本发明可具体制成的鼠标器型(滑球此面上)状态访问装置的仰视图。

图 2 a 及图 2 b 为图 1 鼠标器的两种可具体制成实施例的外观图。

图 2 c 为说明用以操作此具体制成实施例的荧光屏。

图 3 为以概图说明于图 1 鼠标器外壳内部更进步的结构。

图 4 为依另一个可具体制成实施例的状态访问装置其滚球鼠标器型的俯视图。

图 5 为以外观图示说明图 4 实施例的可具体制成的模式。

图 6 为以状态示意图说明图 4 实施例的可具体制成的模式。

图 7 为以方块图说明具有测定控制的状态访问装置。

图 8 为具有测定控制的状态访问装置的俯视图。

图 9 为以外观概图说明无微计算机键盘但具有依本发明的触按指针装置。

图 10 为以一流程图说明藉由集讯卡插入依本发明具体制成可能模式的状态访问装置所提供口令操作的应用软件其可能的查询过程。

图 11 及图 12 为以流程图图示说明当集讯卡插入依本发明具体制成可能模式的状态访问装置其口令的安装与解除。

图 13 至图 18 为以图示说明依本发明具体制成可能模式的状态访问装置所使用通信码框的结构。

具体实施方式

依本发明，此装置将以滚球鼠标器型式说明描述，相同解决方法应用于其他指针装置。图 1 说明依本发明的装置由光机械鼠标器装置所衍生，其滚球 3 被以一盖子 2 支承于其外壳中。一键盘 6 配置于鼠标器外壳主要部份底面特定开口中。此开口的深度依键盘厚度及滑点 4 的厚度选择。因此整个装置并未接触引导滚球 3 的支承表面。

图 1 中所说明的装置包括一微电路卡连结器。于图 1 中一微电路卡 5，例如，依 I S O 7816 标准，或一无接点卡被于此设计的侧面槽插入此装置。此装置可包括插入两种型式微电路卡的装置，以辨别卡片的型式，及确认其正常插入。

因此按键 6 可被配置于鼠标器上盖，可以或无连结罩盖保护。此装置亦可以液晶显示 7 以控制交易及操作，及以一连接线连接至于主设备后面界接端口的插头而与主设备连机。此装置的电源可以内含方式具体制成，或由主设备制成。此电源供应可由一独立接口提供电源，或于多数情况，由连接至接口装置之端口（R S 232，U S B，G E O P O R T），或第二个端口(键盘，・・)提供电压。

此装置亦可结合一永久电源供应的时钟，其需用于金融交易的日期登录。其亦可包括允许创建使用电子钱包操作的安全口令装置。因此其可接收与保存钱，或一电子数值。此上述装置可被以一具有口令方式的微控制器具体制成，及结合一电子钱包操作，或使用具有电子钱包操作的第二个微电路卡连结器。此第二个电子钱包最佳为微电路卡5，及其配置于此装置内(例如GSM大小为15×25mm)。此使其更易于确认更换正确有效或失败。此内建金融功能相当于一电子钱包。

于图2c中所说明的一实施例为以相等的计算方式取代个人数据键入的键盘。此相等解决方式以一程序运行，而由主设备荧光屏50显示仿真键盘54的图形，其由仿真按键51、52所组成。此于键盘上仿真按键51被以随机方式配置，于此程序每一次启动皆不同。个人数据键入被依本发明状态访问装置指针功能进行。信号处理操作及于仿真键盘上指针位置确认被于此唯一接口装置上运行，而免除此确认位置数据传送至主设备。

于鼠标器外壳1一些附加结构为可能。

如于图2a及2b中的图示说明，可看到两种不同结构。

于此两种不同情况，此插槽1b配置于外壳1的侧边，于此鼠标器功能键的相反端，这些功能键于图2a及2b标号为8。此于图2b中图示说明的结构具有一优点，其可简化制造工具。此插槽1b位于导槽1c中，其通常创建于鼠标器接口的功能键8与鼠标器外壳1主要部份间的延伸空间中。

图3以图示说明于外壳1内更进步的结构。常规地于一滚球鼠标器的外壳内，具有两编码器轴41、42及一插入滚轮与此滚球永久接触。这些编码器轴41、42随着此滚球移动。此插入滚轮与滚球3接触的支承弹簧43为一螺状弹簧，其可减少于内部压力机构所需空间，如此可释出大量空间作为芯片卡的插入区域。

依本发明此滚球鼠标器型式的另一实施例以图4至图6说明，此键盘6配置于鼠标器的上表面，意即与底面相反的表面。当此芯片卡未使用连结器功能，一连接盖9用以保护此键盘6。此盖子9未于图4中表示出。其制成于上表面的延伸型状与外壳于闭合位置的型状相同。因此接口装置与常规鼠标器相同。

此盖子被以一转动轴臂10接合至此外壳1成可开闭装置，此转动轴臂中心轴于外壳1上。如上所述转动轴臂10本身对绕一转轴的外壳构成一中心轴，此一转轴其与接合至上述轴臂10的盖子9其中心轴平行。

一制止器10a于外壳1上制成，以限制此盖子9的开度。因此，此连结器可

使操作者由键盘区 6 完全打开盖子，以可方便作访问操作。而接口装置仍具紧密特色。若于一线上网络或本地网络一金融交易操作，此装置的操作者可键入下列不同操作：

-确认有效性，

-更正，删除最后一个键入的号码，

-交易记录，读取上一次交易的清单，

-帐号余额，读取剩余金额或帐号扣除余额，

于电子钱包中的金额值

-选择，对一电子钱包的当前选择，

-删除，取消当前交易，

-本地，停止与主设备通信，

-锁住芯片卡，

-电子钱包 / 卡片，选择电子钱包或插入卡片，

若提出接受交易则

-传送，启动传送操作，

此连结至主设备的装置包括适当的软件装置，及若连接至一信息网络可使用信用卡与电子钱包于线上对货品及服务以口令安全付款，且亦可使两远方金融交易者其金钱的传送更为保密安全。

例如，位于不同地方的两人，每一个人具有含数据机的个人计算机，依本发明可运行下列口令交易：

-由第一个人的信用卡传送金钱至另一个人的电子钱包；

-选择当前传送的货币；

-由第一个人的电子钱包传送金钱至另一个人的电子钱包；

-因此，两人可使用其银行所提供的电子钱包作线上金融交易服务；

-由当前帐号传送金钱至一电子钱包，或相反操作；

-兑换金钱为不同的货币，或者相反操作；

每一次卡片固定器识别为必要的，其个人口令，及其被键入识别码，此装置因此可提供一保护墙，以防止欺骗计算机者的侵入。

此外，此含有电子钱包装置的装置可允许下列操作：

-检查余额或扣除余额；

-读取交易记录；

-锁住电子钱包；

一芯片卡5可包括一些金融交易操作装置，例如一信用卡与至少一电子钱包。依本发明每一基本装置，于相同芯片卡本身金融交易操作间，具有运行金融交易的装置，因为此安全口令条件已被卡片本身连带确保。

此装置结合一内部电子钱包(E W)，或两个相同连结器，其中一个包括具有中介角色的电子钱包，亦可用于本地工作模式，于卡片对卡片交易，此卡片被成功地插入所提供的连接器中；

-以信用卡借款，及存入一电子钱包；

-由一电子钱包传送金钱至另一个电子钱包；

-保存金钱于电子钱包中；

-取消最后一次交易；

其应注意地是设定操作的装置，卡片固定器的识别(个人键入口令或信号)，及此芯片卡连结器装置，及指针装置(选择，确认，修改)，构成上述装置其每一种型式的结构，依本发明，结合与主设备串列通信的不同装置，键盘，显示器，电源供应器，电子钱包，我们可获得此相同种类的装置。

如上型式的接口装置加上芯片卡终端机功能，使用于金融交易访问控制，识别，及个人计算机或一会话式电视的长途电话操作装置。

其允许以信用卡或电子钱包及自身银行功能于线上对货品与服务付款。以此电子钱包(E W)型式，此装置可被用为金钱储存处以于线上网络或本区网络上交易付款。

此装置可使用个人付款装置(信用卡，电子钱包)，或不具名装置(电子钱包，E W)。以此方式，此装置以直接取代实体交易处理电子金钱，及可排除于操作者间实体的障碍。

此装置亦可用于商业网络管理，口令安全访问与保护软件。

此装置取代常规鼠标器或任何其他串列指针装置，及其结合一支持软件，以适合于每一种型式的主设备。通常其为一设计用于多媒体终端机的远端控制单元，及可被认为一指针装置(于个人计算机，会话式多媒体电视)。其亦可结合其他附加应用，例如会计计算器，剪报板，日记等。

以剪报板的型式设计具有一指示笔，及可选择的两个芯片卡接口，一记录写

入文件及压缩至内存，此装置较好可使用于从事医学专业人员。

图 7 说明一设定操作物体测定控制的结构，此控制使用于例如指纹扫瞄器或眼睛影像扫瞄器，其包括，例如指纹扫瞄器或眼睛影像扫瞄器的影像感测器 15 连接至图 7 中所示的接口微控制器 12。此微控制器 12 亦连接至一特定指针装置 11，一显示荧光屏 7 及一键盘 6。因此其经由接口 13 与外部芯片卡 5 通信，及经由接口 14 与内部芯片卡通信，及与上述接口装置于另一端所连接的微算机 19 通信。

于另一实施例，此微控制器 12 为很容易地连接至语音合成及辨认处理器 16，其例如连接至配置于外壳 1 中的话筒ＭＩＣ与一扩音机ＨＰ。一操作实施例包括于读取数据显示于荧光屏或主设备期间，确认用户语音信号。此具体实施模式可使语音辨认与记录于微电路卡 5 上的数字语音信号作比对，及以极少数的字语与演绎法作比对，而可简化集成电路。此为一低价位成本的方法，而此仅稍微降低其比较的安全性。

构成微控制器单元 12 的处理装置，为由感测器 15 所读取得测定物体的形状，和/或语音辨认单元 16 可以卡片 5 处理。此接收测定物体的值与储存于内存中测定物体的参考值作比较。于此实施例中，参考值与由感测器 15 或单元 16 读取的测定物体间作比较可以微控制器 12 具体运行。

其应注意的是，此微控制器的处理装置 12，可为一最佳化数学共同处理器，用于信号处理和/或口令图形计算。因此单元 16 的整个或一部份可很方便地集成于相同芯片或模块中。

此检查测定对像，例如一由感测器 15 所读取的影像，或由此单元 16 所制成的语音辨认取代用户的识别码，其因此不需由键盘 6 键入。

图 8 说明感测器 15 位于外壳 1 侧边的结构。此侧边制成一导引型状区 17，以置放用户的手指或姆指。ＥＮ1546 欧洲标准设计规范详细说明电子钱包的使用及操作。此外，ＥＭＶ欧洲标准详细说明以微电路卡付费的标准过程，及此类卡片的特色。

此接口装置可包括一无线通信媒体，以增加对主设备的机动性。无线电或红外线的方式可被使用以克服环境限制及那些所使用主系统的限制。

此接口装置可被集成于微算机本身内部。此型式的一实施例以图 9 说明。于此实施例，一微算机结合一触按指针装置 20。一键盘 6 为独立于计算机键盘Ｃ外，

其被集成于固定面板S上，而键盘C与触按指针装置20安装于其上。

更进步的，此装置的触按面板20被用以运行个人数据键入的键盘6(因为上述键盘为叠装于上述触按面板上)。此方式为永久显示型的。于另一实施例中，其可仅于卡片固定器的辨识操作期间以再现光线显示出，例如，其可以一电子萤光膜达成。

依本发明另一个此装置实施例，可操作语音合成装置及一适当字典。此字典可使用一授权服务器下载和/或以一口令过程修改。例如，此服务器可为状态访问装置制造者的型式。此装置可具有语音辨认装置，学习运行交易所需最少的命令；例如接受，取消或继续。例如检查显示于计算机荧光屏上的价格，例如$198·25，此过程包括传送此价格有关的数据至接口装置，其以合成及语音再生装置发出声音“1”，“9”，“8”，“·”，“2”，“5”，“元”，转换此信息。

接着此装置确认交易的价格，例如，由插入微电路卡的固定器发出指令”接受”语音，此语音指令可被记录。

现我们参照图10及下面本发明的其他特色。

此接口装置包括一口令操作装置，于下列的正文以启始“SAM”表示说明。以“口令操作装置”此项或SAM，意即目的软件包括一可运行码，及对于安全口令微电路中操作、驻存与运行其所需的所有特定资源，此安全口令微电路亦支持一安全口令操作系统。一典型SAM例子为此微电路卡所提供的电子钱包。一口令操作装置结合于接口装置中被制成，以至少一个应用软件用于与上述接口装置通信主电子设备中。

此应用软件及其安全口令以一个或数个码键的型式辨识相同秘密信息；其设定操作相同口令的演绎法，而可确认此键码。

一安全口令分布式操作装置因此被制成，以取代此应用软件的一般键码，以防止伪欺者。此安全口令操作装置很容易以一芯片卡运行，但不限制于芯片卡；接着以”SAM集讯卡”表示说明。例如，此卡片由称为分散卡或SAMD的第二个卡片装入，例如，其支持应用软件以防止伪欺者。于此文中，图10为一驻存于接口装置集讯卡内的SAM口令操作基本查询过程的流程图，其藉由一应用软件于本区运行或对与此接口装置通信的主设备访问。对此应用软件SAM的角色为一个保护键。SAM测试步骤101第一个步骤为生成一随机码(RNDC)，

其接着被记忆。于第二个步骤102，随机码(ＲＮＤＣ)被依此平衡键过程加密，其为已知技艺。此加口令被此应用软件及其ＳＡＭ认知。步骤102的结果为另一测试码(ＣＬＧ)被传送至ＳＡＭ。于步骤103，此应用软件检查是否其可传送出测试码(ＣＬＧ)至此装置通道。于步骤104，此测试信息(ＣＬＧ)被依一上述接口装置的指针装置通信协议规格相关的延伸通信协议传送至前往的ＳＡＭ。

于步骤105此应用软件等待ＳＡＭ响应一段缺省时间后，ＳＡＭ使用一演绎法以将测试码(ＣＬＧ)解密。

若ＳＡＭ为正确的，此解密键为相同，及取出一清楚的启始随机码。其反应(ＲＰＬ)被传送至此装置，以于步骤106由应用软件读取。接着步骤107包括比较启始随机码(ＲＮＤＣ)与反应(ＲＰＬ)。若其相同，则非伪骗者。此一ＳＡＭ过程测试被结合于保护性应用软件。若图10过程的108成功则仅有一种反应信息，而错误信息109实际上为很多种，及于其所有步骤中反应出可能的失败情况。

依本发明的口令操作装置安装的简化过程，或于此过程中的ＳＡＭ，如图11说明。

一ＳＡＭＤ口令操作装置分散卡可用于一些相同口令操作的安装。上述卡片包括对每一个口令操作装置的允许

计数器(ＬＣＮＴ)，以启始化该操作件所允许的安装次数。于步骤110，此应用软件的安装步骤需要一ＳＡＭＤ分散卡装于接口装置的连结器中。此过程被中断：

-若测试111未确认此ＳＡＭＤ分散卡，或欲计数器被允许安装次数的计数器为零。

-若测试112于此ＳＡＭ集讯卡中未读取足够内存，或此卡片未能取得欲被安装的ＳＡＭ。

-若测试114未确认此复制有效。

-若此111及112的条件符合，于113步骤传送ＳＡＭ由ＳＡＭＤ分散卡至此集讯卡ＳＡＭＣ卡。

此接口装置的连结器的微控制器启动传送，其接着以一标准安全口令数据传送过程于两卡片间进行传送。

于此传送期间，此微控制器仅作为于ＳＡＭＣ卡与ＳＡＭＤ卡间的链路通道。此ＳＡＭＣ集讯卡的操作系统使ＳＡＭ成为可运行型式。接着ＳＡＭＣ卡运

行 114 测试，其包括被称的为传送有效确认，及其后的ＳＡＭ正确工作确认。此确认包括仿真ＳＡＭ的查询，及检查其动作。此ＳＡＭＣ集讯卡由其内存中清除无效的ＳＡＭ。此ＳＡＭ的安装等于将一数值以一相同的交易机构传送至使用电子钱包系统的另一者。若ＳＡＭ被ＳＡＭＣ卡储存管理与运行的安全口令装置确认有效，此交易机构确保 115 步骤可运行，及此允许计数器ＬＣＮＴ被减 1。

依本发明于此处理过程中ＳＡＭ解除安装的简化流程图如图 12 中所示。

步骤 116 此应用软件解除安装ＳＡＭ所保护的程序，其需要插入ＳＡＭＤ分散卡或相等的装置于接口装置的连结器中。

测试 117 检查是否将解除安装的ＳＡＭ接受上述连结器中插入的卡片。若此ＳＡＭＤ卡为原始卡片，此ＳＡＭ码仍然存在，及步骤 119 将允许计数器增加 1（ＬＣＮＴ）。

若此ＳＡＭＤ非原始卡片，且若条件 120 其有足够内存，于步骤 121，此ＳＡＭ码被传送至ＳＡＭＣ集讯器卡，此与上述安装过程的步骤 113 为相同情况。而于步骤 121 中，ＳＡＭＤ卡操作系统生成一允许计数器（ＬＣＮＴ）且初值化设定为零。若ＳＡＭ码传送出，于步骤 122 此ＳＡＭＤ卡检查此复制的有效性，此与于ＳＡＭ安装流程图的步骤 114 相同。藉由于ＳＡＭ安装的相同交易装置，此解除安装操作确保ＳＡＭ卡中包括一有效的ＳＡＭ，及一允许计数器（ＬＣＮＴ）仅于”成功”模式时增加 1。其亦确保于步骤 123 由ＳＡＭＣ内存清除ＳＡＭ。此过程因此允许所有ＳＡＭＤ卡藉由解装过程已接收的口令操作装置与原始分散卡相同。一口令操作藉由插入装置确保其信息经过通信网络的传送正确与完整性，于彼此通信的两远端卡片间传送。因此一ＳＡＭ传送过程可视为一主设备至另一主设备的软件允许流通，其使用的通信网络为与上述ＳＡＭ解装过程相同。

于此情况，此分散卡片以目的集讯卡片取代。

使用于口令操作装置的管理与运行的通信协议最好为使用相同的串列通信通道以传送指针信息及安全口令信息。因此指针及微电路卡的终端机功能可提供接近同时操作，而其彼此分开独立。于该通信协议的结构中，此信息及指令被以码框型式传送，其整个由许多字段组成，每一个字段以具有设定数目比特的编码过程构成，此如图 13 中所示。因此，一码框需要包括一个识别字段（ＦＩＤ）及至少下面一个字段：

-指针信息字段；

-有关安全口令操作的信息字段；

此识别字段(ＦＩＤ)启始化接收装置，以分析其内含。对一接口指针装置及一指定功能模式，其码框具有一个固定长度。于此一码框，此最高比特被保留用以识别码框的启始点。依本发明设定通信协议的操作，使用相同方法以维持与常规指针装置兼容，及皆配置此指针信息于延伸码框的开始位置。因此其并未绝对认定指针码框为延伸码框识别字段的一部份(ＦＩＤ)，如于图 6 中的说明。例如，有关口令操作装置的信息字段，可以此码框的第一个字节其每一比特的设定值依相同原则说明。因此，此有关口令操作的信息字段包括下列全部或一部份字段，此字段依识别字段的一组比特(ＦＩＤ)其上述设定值所决定的位置依序描述：

-控制字段(ＯＰＣ)，

-定义安全口令操作信息长度(ＤＬＥＮ)的字段

-包括所有或一部份口令操作信息属性(ＣＬＧ)或(ＲＰＬ)的字段，

-确认上述信息正确完整性的控制字段。

此延伸码框可依此控制字段(ＯＰＣ)设定而有可变长度。若此码框包括一用于口令操作装置的(ＣＬＧ)信息，或一用于应用软件的(ＲＰＬ)信息，此(ＯＰＣ)字段接着为一(ＤＬＥＮ)字段，其定义该(ＣＬＧ)或(ＲＰＬ)信息长度的信息。此(ＤＬＥＮ)字段的长度为(ＣＬＧ)或(ＲＰＬ)信息所允许最大长度的函数。依本发明此装置的控制及处理装置忽略上述(ＣＬＧ)及(ＲＰＬ)信息的内容。此可选择字段(ＣＲＣ)可控制(ＣＬＧ)与(ＲＰＬ)信息的正确完整性。

延伸码框完全被其控制字段(ＯＰＣ)所定义，其至少包括下列信息(图 14)：

-有关一个或数个口令操作装置的(ＯＰＣ・Ｃ)操作码，

-有关口令操作装置的地址于(ＯＰＣ・Ａ)码框，

-有关延伸码框所传送的安全口令操作的信息字段其字节数目，此数目(ＯＰＣ・Ｓ)为至少等于字段长度(ＯＰＣ)。

此(ＯＰＣ・Ａ)地址亦应考虑用以访问口令操作装置的连结器。除了最后区段外，较长信息被以固定长度(ＯＰＣ・Ｓ)分割为数个更短的延伸码框分段传送。此方法确保此指针信息取得数据频率的均等性。

图 15 及图 18 说明于上面图 13 与图 14 中所述延伸码框结构的详细实施例。

图 15 说明一典型鼠标器所送出的码框。此码框包括 3 个字节，其最高比特未使用。这些比特被用以说明此延伸码框。

由此码框，图 16 说明此延伸码框的结构，其识别字段(ＦＩＤ)回复此指针码框，及设定此第一个字节的最高比特为 1。因此，此装置检知此延伸码框，及分析此为安全口令信息的控制字段(ＯＰＣ)的第四个字节。此第五个字节(ＤＬＥＮ＝m)表示一ＳＡＭ本身反应的字节长度，或结合前一个字节所提供其他二进位字段的字节长度，例如，此两个或三个字节的最高比特。此控制字段(ＣＲＣ)包括(ｎ)个字节。

图 17 及图 18 分别以图示说明延伸码框的第 4 个与第 5 个码框的结构，其以数个连续区段传送口令操作反应，对于ＯＰＣ・Ｓ＝8 的参数，一(ＲＰＬ)反应为 32 字节，及一(ＣＲＣ)为 16 比特。此(ＯＰＣ・Ｓ)字段表示对此装置驱动器，除了最后码框外，加至此指针码框后的口令操作其信息字段的字节数目。因此，此指针码框及延伸码框可被交替。

本发明于前面正文所论述说明为非作范围限制的例证。其应了解地是，一专业人士可具体制成一些实施例，但其应仍属于本发明的范畴中。

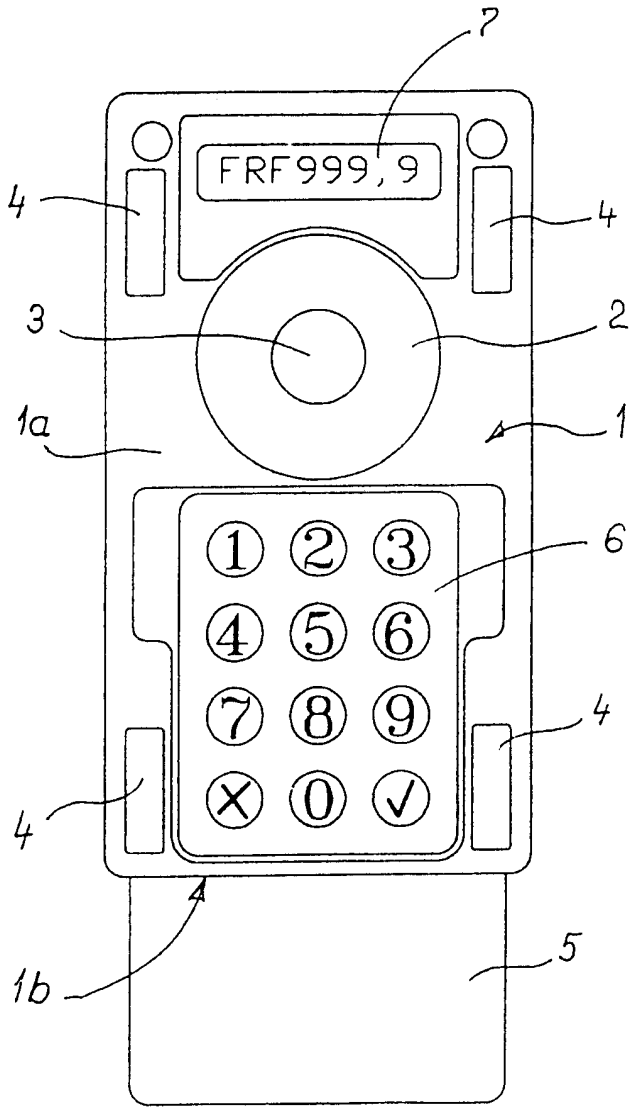


图 1

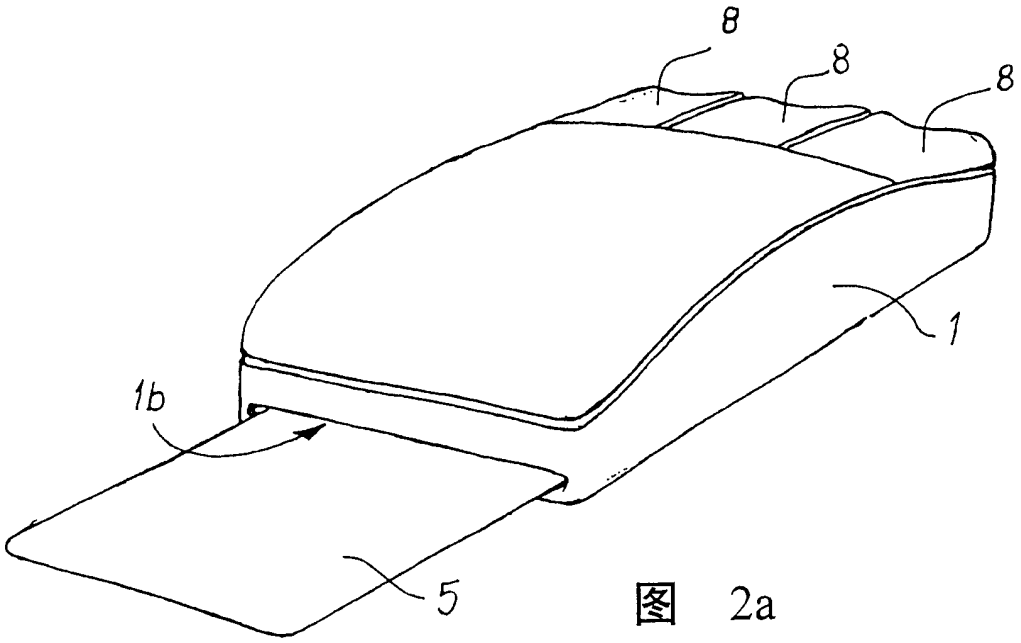


图 2a

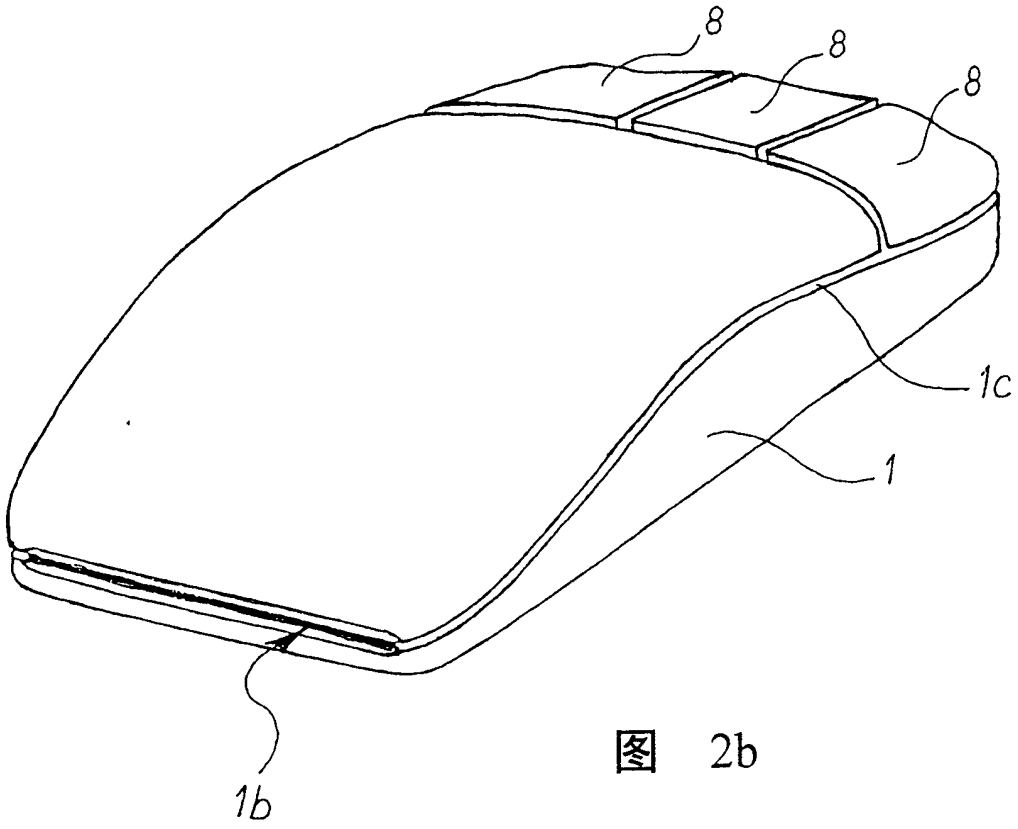


图 2b

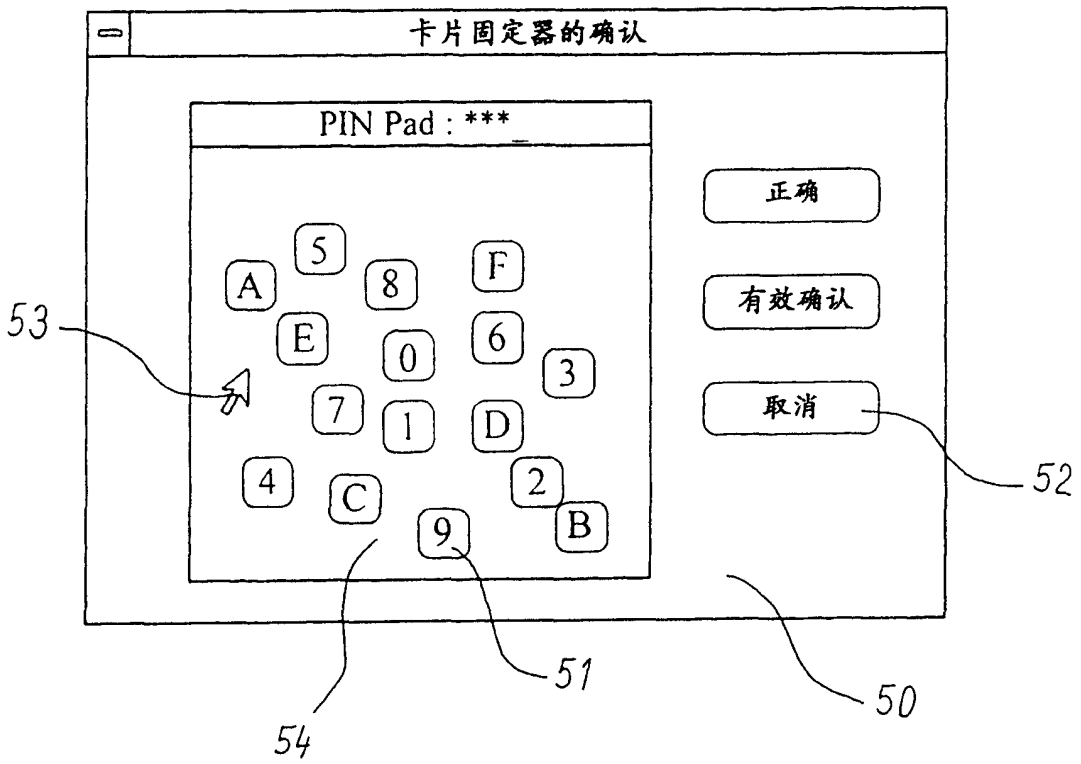


图 2c

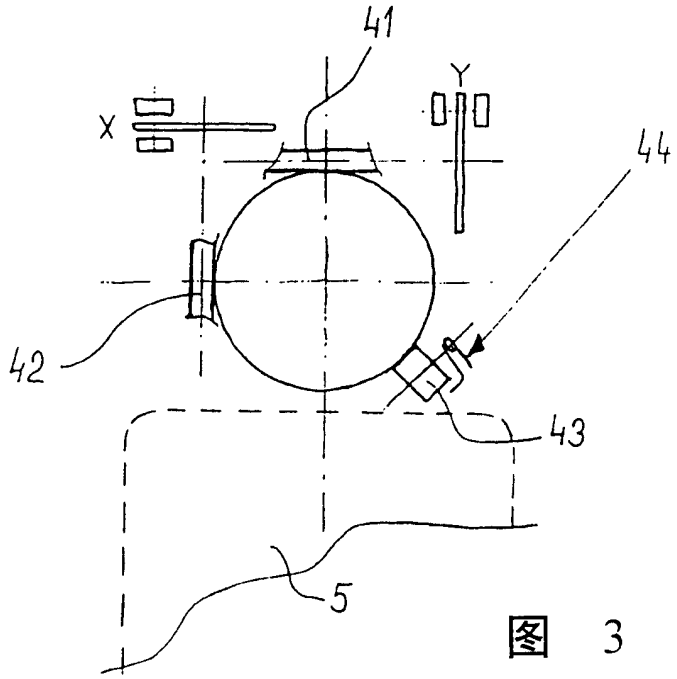


图 3

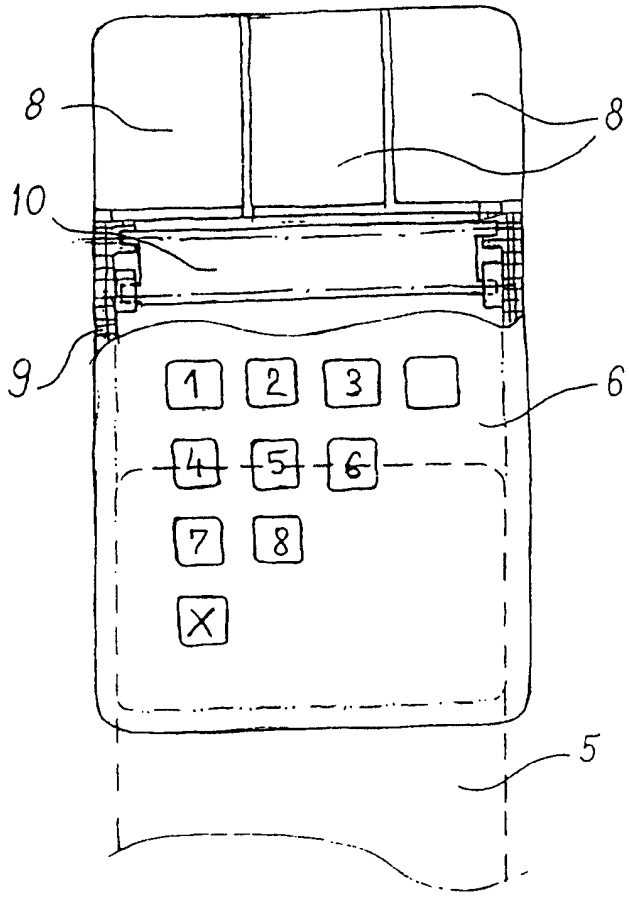


图 4

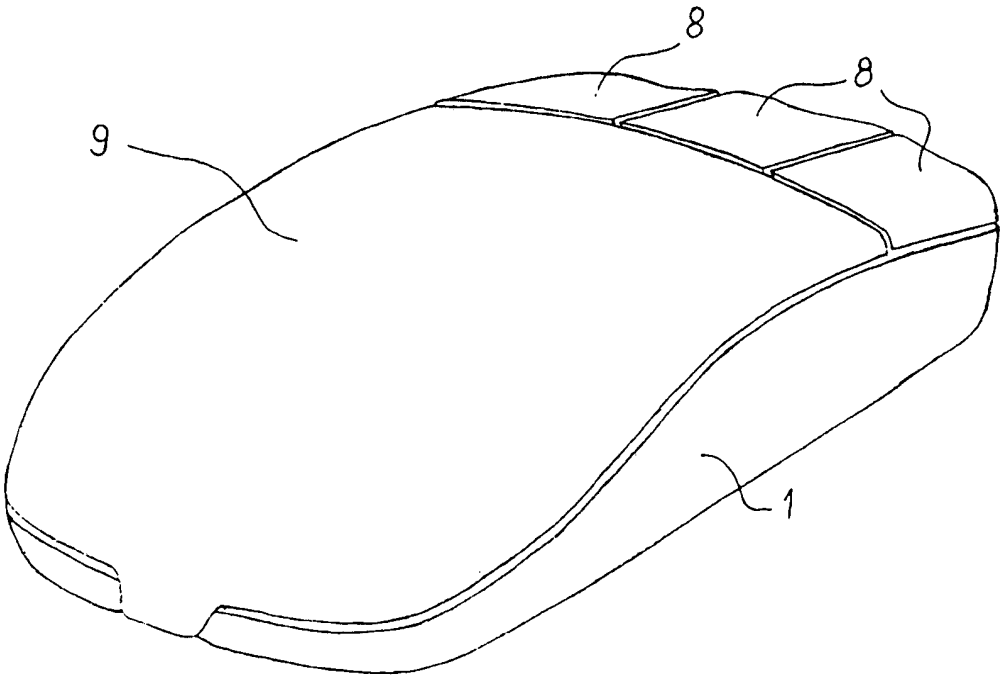


图 5

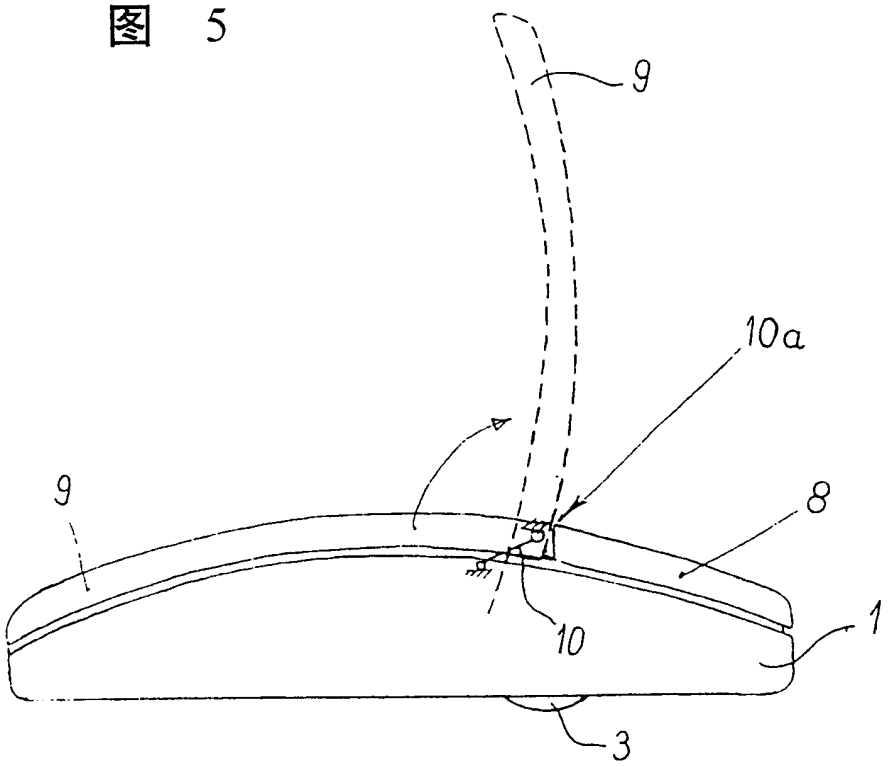


图 6

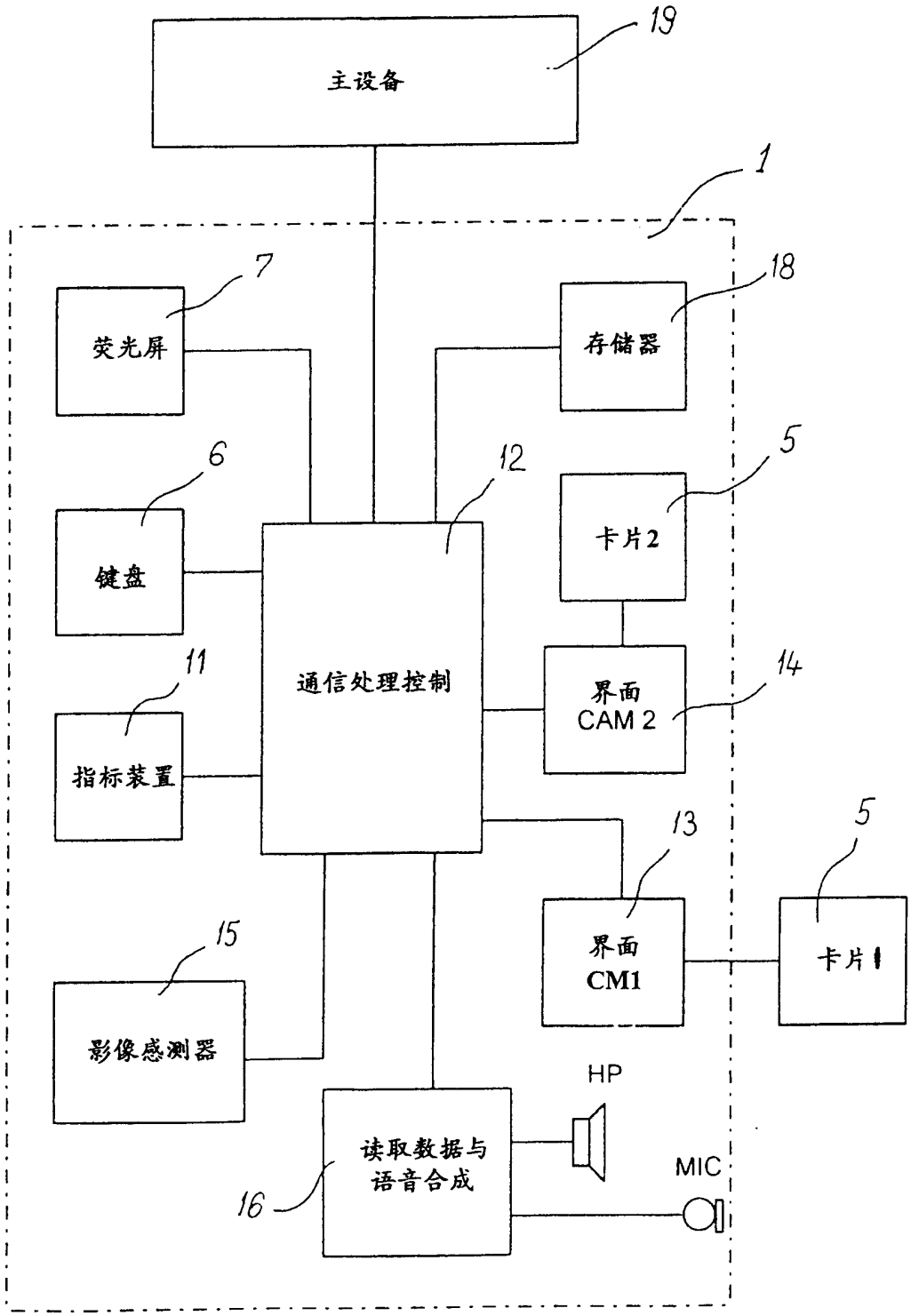

主设备
19
1
荧光屏
7
存储器
18
键盘
6
12
卡片2
5
通信处理控制
指标装置
11
界面
CAM 2
14
13
5
界面
CM1
卡片1
15
影像感测器
HP
读取数据与
语音合成
16
MIC

图 7

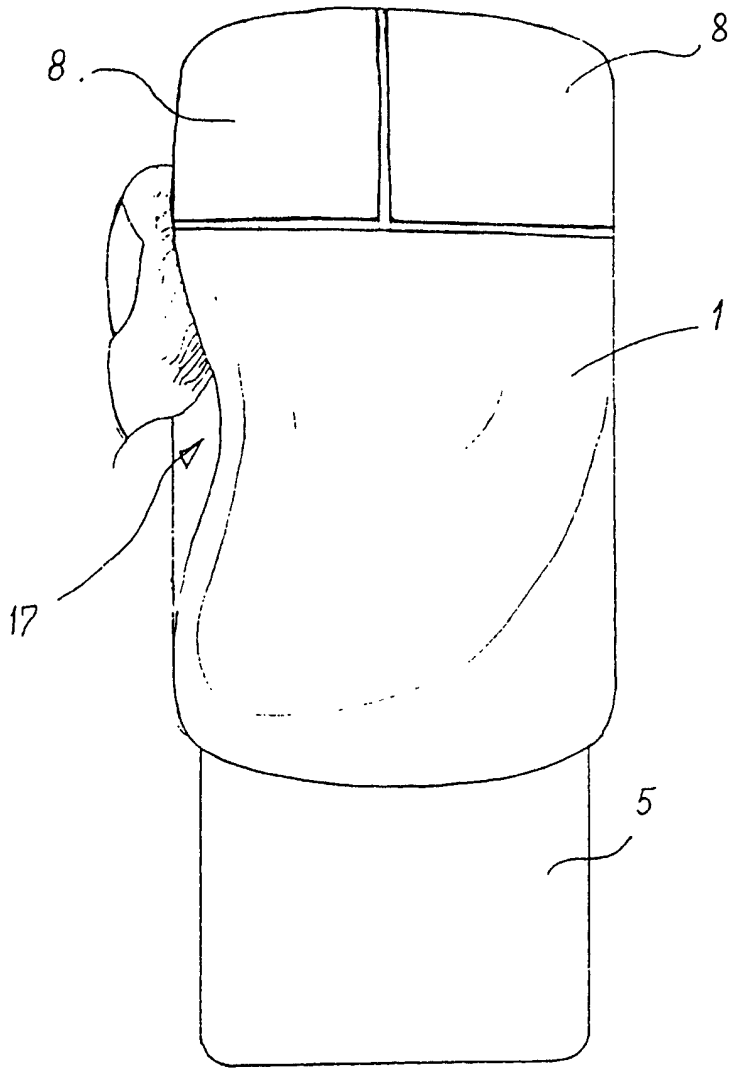


图 8

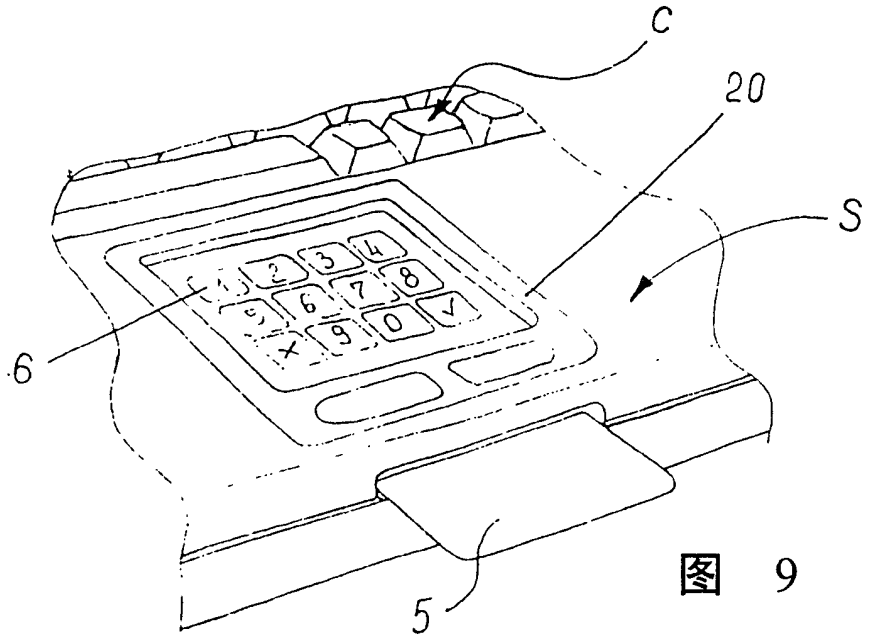


图 9

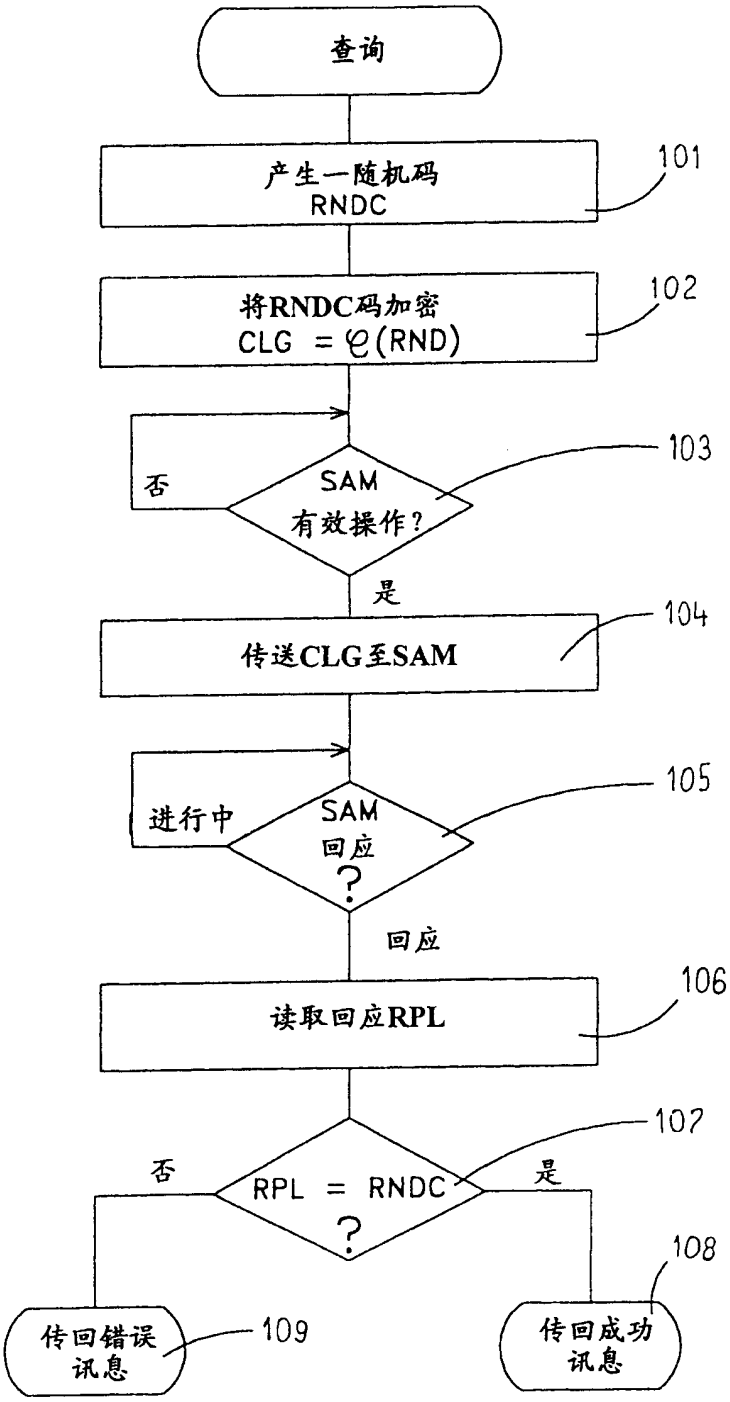

查询
产生一随机码
RNDC
101
将RNDC码加密
CLG = ℰ(RND)
102
否
SAM
有效操作?
103
是
传送CLG至SAM
104
进行中
SAM
回应
?
105
回应
读取回应RPL
106
否
RPL = RNDC
?
107
是
108
传回错误
讯息
109
传回成功
讯息

图 10

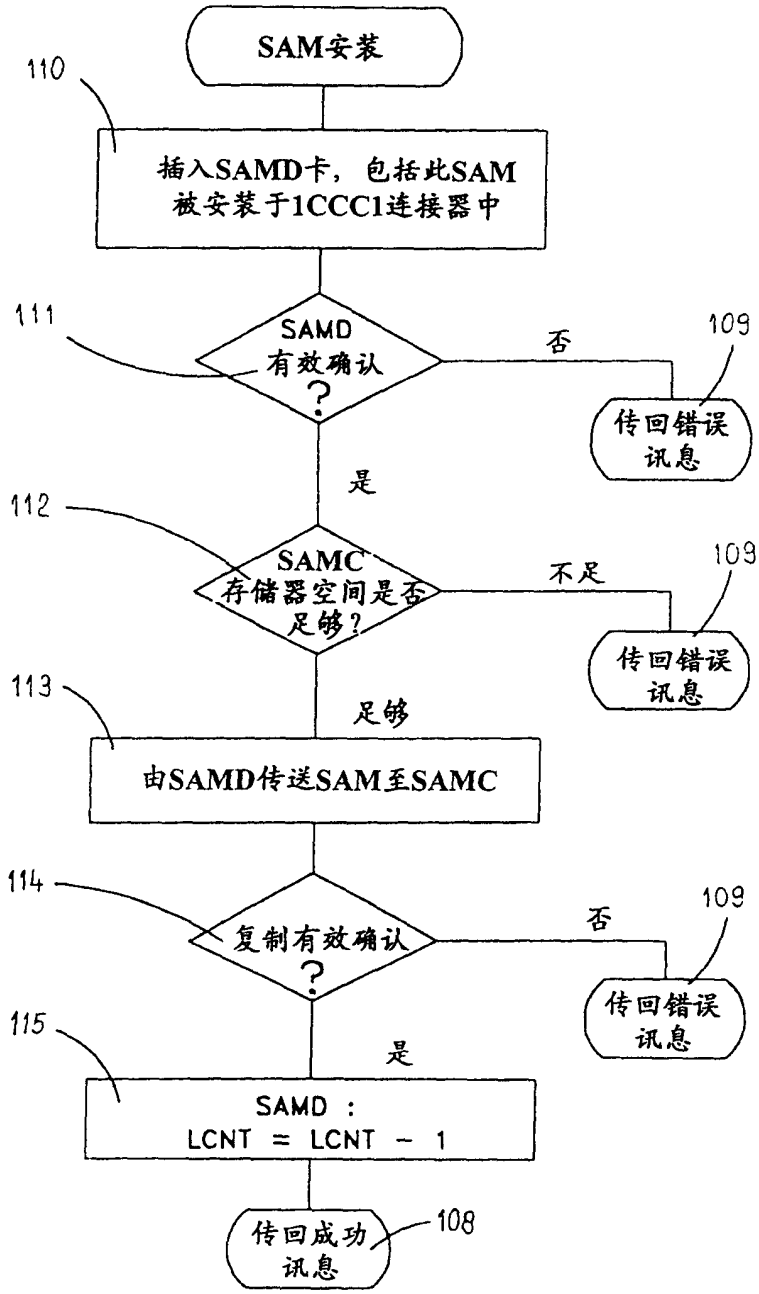

SAM安装
110
插入SAMD卡，包括此SAM
被安装于1CCC1连接器中
111
SAMD
有效确认
?
否
109
传回错误
讯息
是
112
SAMC
存储器空间是否
足够?
不足
109
传回错误
讯息
113
足够
由SAMD传送SAM至SAMC
114
复制有效确认
?
否
109
传回错误
讯息
115
是
SAMD :
LCNT = LCNT - 1
传回成功
讯息
108

图 11

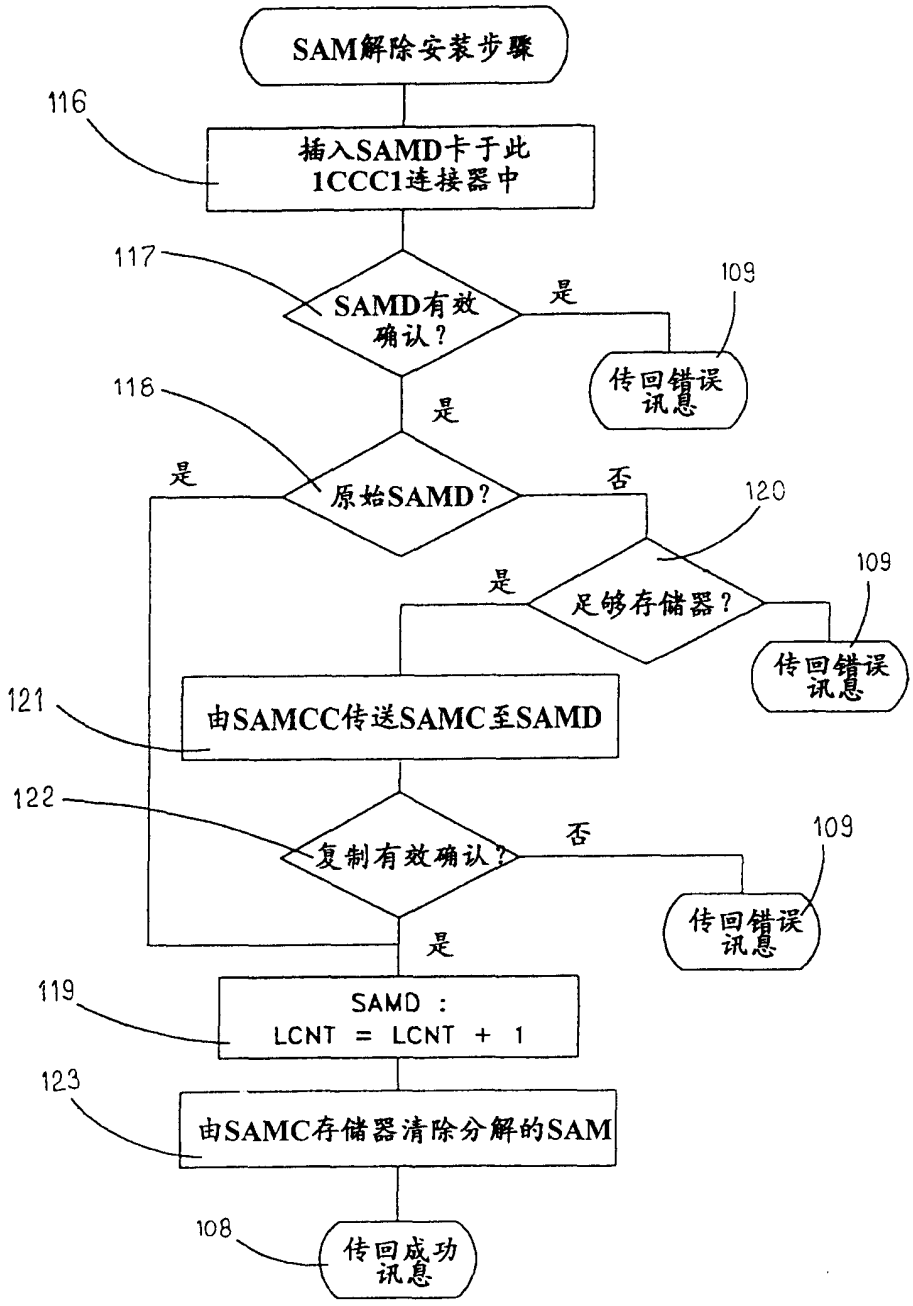

SAM解除安装步骤
116
插入SAMD卡于此1CCC1连接器中
117
SAMD有效确认?
是
109
传回错误讯息
是
116
原始SAMD?
是
否
120
足够存储器?
是
109
传回错误讯息
121
由SAMCC传送SAMC至SAMD
122
复制有效确认?
否
109
传回错误讯息
是
119
SAMD : LCNT = LCNT + 1
123
由SAMC存储器清除分解的SAM
108
传回成功讯息

图 12

FID	OPC	DLEN	CLG / RPL	CRC

图 13

OPC		
OPC.C	OPC.A	OPC.S

图 14

序列	7 MSB	6	5	4	3	2	1	0 LSB
比特 1	X	1	L	R	X7	X6	Y7	Y6
比特 2	X	0	X5	X4	X3	X2	X1	X0
比特 3	X	0	Y5	Y4	Y3	Y2	Y1	Y0

图 15

序列	7 MSB	6	5	4	3	2	1	0 LSB
比特 1	1	1	L	R	X7	X6	Y7	Y6
比特 2	X	0	X5	X4	X3	X2	X1	X0
比特 3	X	0	Y5	Y4	Y3	Y2	Y1	Y0
比特 4	OPC							
比特 5	DLEN = m							
比特 6	RPL_{m-1}							
...	...							
比特 m+6	RPL_0							
比特 m+7	CRC_{n-1}							
...	...							
比特 m+n+6	CRC_0							

图 16

m = 32 ; n =2 ; k = 8; FS_{00} ;

序列	7 MSB	6	5	4	3	2	1	0 LSB
比特 1	1	1	L	R	X7	X6	Y7	Y6
比特 2	X	0	X5	X4	X3	X2	X1	X0
比特 3	X	0	Y5	Y4	Y3	Y2	Y1	Y0
比特 4	OPC							
比特 5	DLEN = 32							
比特 6	RPL_{31}							
比特 7	RPL_{30}							
比特 8	RPL_{29}							
比特 9	RPL_{28}							
比特 10	RPL_{27}							
比特 11	RPL_{26}							

图 17

m = 32 ; n =2 ; k = 8; FS_{04} ;

比特 1	1	1	L	R	X7	X6	Y7	Y6
比特 2	X	0	X5	X4	X3	X2	X1	X0
比特 3	X	0	Y5	Y4	Y3	Y2	Y1	Y0
比特 4	RPL_{01}							
比特 5	RPL_{00}							
比特 6	CRC01							
比特 7	CRC00							

图 18