(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 108345785 B
(45)授权公告日 2021.05.11

(21)申请号 201710187742.3

(22)申请日 2017.03.27

(65)同一申请的已公布的文献号
申请公布号 CN 108345785 A

(43)申请公布日 2018.07.31

(30)优先权数据
106102831 2017.01.25 TW
106201380 2017.01.25 TW

(73)专利权人 杨建纲
地址 中国台湾台北市

(72)发明人 杨建纲

(74)专利代理机构 北京泰吉知识产权代理有限公司 11355
代理人 张雅军 秦小耕

(51)Int.Cl.
G06F 21/44(2013.01)
G06F 21/78(2013.01)
G06Q 20/38(2012.01)
G06Q 20/40(2012.01)

(56)对比文件
US 2015161591 A1,2015.06.11
US 2003221115 A1,2003.11.27
US 2015200948 A1,2015.07.16
US 2014020083 A1,2014.01.16

审查员 杨美琴

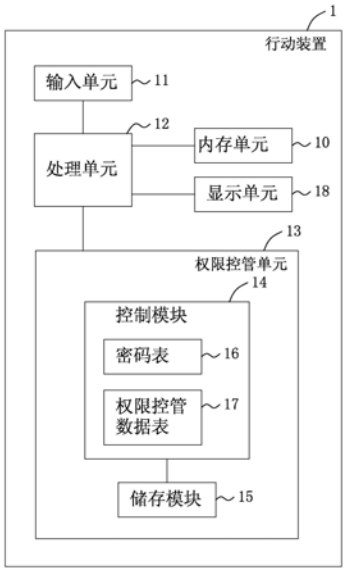
权利要求书2页 说明书6页 附图4页

(54)发明名称

内建智能安全行动装置

(57)摘要

一种内建智能安全行动装置，包括一包含一控制模块及一储存模块的权限控管单元、一储存一应用程序的内存单元及一处理单元，该处理单元通过该应用程序传送一认证信息给该权限控管单元，且该控制模块根据该认证信息判断该应用程序合法时，允许该处理单元与其建立联机，且该处理单元通过该应用程序传送一使用者识别码及一使用者密码给该控制模块，该控制模块根据一权限控管数据表查询该使用者识别码的一权限，并判断该使用者密码与记录在一密码表的一使用者密码相符时，允许该处理单元在该权限范围内使用该储存模块。



CN 108345785 B

1.一种内建智能安全行动装置,其特征在于:

该内建智能安全行动装置包括:

一权限控管单元,其包含一控制模块及一储存模块,该控制模块具有一权限控管数据表及一密码表,该权限控管数据表记录一使用者识别码及其使用该储存模块的一权限,该密码表记录该使用者识别码及其对应的一使用者密码;

一内存单元,储存一应用程序;及

一处理单元,与该权限控管单元及该内存单元电连接,且该处理单元执行该应用程序时,该应用程序传送一认证信息给该权限控管单元,且该控制模块根据该认证信息判断该应用程序合法时,允许该处理单元与其建立联机,且该处理单元通过该应用程序传送一使用者识别码及一使用者密码给该控制模块,该控制模块根据该权限控管数据表查询该使用者识别码的一权限,并判断该使用者密码与记录在该密码表的该使用者密码相符时,允许该处理单元在该权限范围内使用该储存模块;其中

该控制模块能对该储存模块规划一隐密数据区,且该控制模块判断该权限允许存取该储存模块的该隐密数据区时,则允许该处理单元存取该储存模块的该隐密数据区;该控制模块判断该权限允许规划该隐密数据区时,该处理单元能通过该控制模块对该隐密数据区规划多个私密空间,且该控制模块判断该权限允许存取所述私密空间至少其中之一时,允许该处理单元存取该私密空间,并将该处理单元传来的数据进行加密后再存入该私密空间,或者将该处理单元需要的数据从该私密空间读出并对其解密后,再传送给该处理单元。

2.根据权利要求1所述的内建智能安全行动装置,其特征在于:该控制模块记录有该应用程序的一识别码及一密码,且该控制模块判断该认证信息中包含的一识别码及一密码与该控制模块记录的该识别码及密码相同时,即判定该应用程序合法。

3.根据权利要求1所述的内建智能安全行动装置,其特征在于:该控制模块判断该权限允许设定与更新该权限控管数据表及/或该密码表时,允许该处理单元对该权限控管数据表及/或该密码表进行设定及更新。

4.根据权利要求1所述的内建智能安全行动装置,其特征在于:该行动装置包括一输入单元,其接受输入该使用者识别码及该使用者密码并将其传送给该处理单元。

5.根据权利要求1所述的内建智能安全行动装置,其特征在于:该控制模块还包含一金融芯片,其中储存一密钥及一押码程序,且该控制模块判断该权限允许该处理单元存取该金融芯片时,将该处理单元传来的一要被押码的数据传送给该金融芯片,使执行该押码程序,以该密钥对该要被押码的数据押码而产生一交易押码,并回传该交易押码给该处理单元。

6.根据权利要求1所述的内建智能安全行动装置,其特征在于:该隐密数据区存有一密钥,该控制模块具有一押码程序,且该控制模块判断该权限允许该处理单元存取该隐密数据区时,读取储存于该隐密数据区的该密钥,且接受该处理单元传来的一要被押码的数据,并执行该押码程序,以该密钥对该要被押码的数据押码而产生一交易押码,并回传该交易押码给该处理单元。

7.根据权利要求1所述的内建智能安全行动装置,其特征在于:该控制模块还包含一储存一押码程序的金融芯片,该隐密数据区存有一密钥,且该控制模块判断该权限允许该处理单元存取该金融芯片及该隐密数据区时,该控制模块读取储存于该隐密数据区的该密

钥，并将该密钥及该处理单元传来的一要被押码的数据提供给该金融芯片，使执行该押码程序，以该密钥对该要被押码的数据押码而产生一交易押码，并回传该交易押码给该处理单元。

8.根据权利要求1所述的内建智能安全行动装置，其特征在于：该行动装置具有一主板，该处理单元设置在该主板上，且该权限控管单元是一设置在该主板上的芯片。

9.根据权利要求1所述的内建智能安全行动装置，其特征在于：该行动装置具有一主板，该处理单元设置在该主板上，且该控制模块是一设置在该主板上的第一芯片，该储存模块是一设置在该主板上的第二芯片。

10.根据权利要求1所述的内建智能安全行动装置，其特征在于：该行动装置具有一主板及一与该主板电连接的电路板，该处理单元设置在该主板上，且该权限控管单元是设置在该电路板上。

11.根据权利要求1所述的内建智能安全行动装置，其特征在于：该行动装置具有一主板及一与该主板电连接的电路板，该处理单元设置在该主板上，且该控制模块设置在该电路板上，该储存模块设置在该主板上。

12.根据权利要求1至11中任一权利要求所述的内建智能安全行动装置，其特征在于：该行动装置是一智能手机、一平板计算机或一笔记本电脑。

内建智能安全行动装置

技术领域

[0001] 本发明涉及一种行动装置,特别是涉及一种内建智能安全行动装置。

背景技术

[0002] 现有的行动装置,例如一智能手机让使用者可以借由外插一SD卡,并利用智能手机通过SD卡的验证及授权后,使用SD卡内存的交易凭证信息来执行一行动支付,例如中国台湾第I537851号专利。

发明内容

[0003] 本发明的目的在于提供一种由行动装置本身对使用者进行身份验证及权限控管之内建智能安全行动装置。

[0004] 本发明一种内建智能安全行动装置,包括一权限控管单元、一内存单元及一处理单元。该权限控管单元包含一控制模块及一储存模块,该控制模块具有一权限控管数据表及一密码表,该权限控管数据表记录一使用者识别码及其使用该储存模块的一权限,该密码表记录该使用者识别码及其对应的一使用者密码;该内存单元储存一应用程序;该处理单元与该权限控管单元及该内存单元电连接,且该处理单元执行该应用程序时,该应用程序传送一认证信息给该权限控管单元,且该控制模块根据该认证信息判断该应用程序合法时,允许该处理单元与其建立联机,且该处理单元通过该应用程序传送一使用者识别码及一使用者密码给该控制模块,该控制模块根据该权限控管数据表查询该使用者识别码的一权限,并判断该使用者密码与记录在该密码表的该使用者密码相符时,允许该处理单元在该权限范围内使用该储存模块。

[0005] 在本发明的一些实施态样中,该控制模块记录有该应用程序的一识别码及一密码,且该控制模块判断该认证信息中包含的一识别码及一密码与该控制模块记录的该识别码及密码相同时,即判定该应用程序合法。

[0006] 在本发明的一些实施态样中,该控制模块能对该储存模块规划一隐密数据区,且该控制模块判断该权限允许存取该储存模块的该隐密数据区时,则允许该处理单元存取该储存模块的该隐密数据区。

[0007] 在本发明的一些实施态样中,该控制模块判断该权限允许设定与更新该权限控管数据表及/或该密码表时,允许该处理单元对该权限控管数据表及/或该密码表进行设定及更新。

[0008] 在本发明的一些实施态样中,该控制模块判断该权限允许规划该隐密数据区时,该处理单元能通过该控制模块对该隐密数据区规划多个私密空间,且该控制模块判断该权限允许存取所述私密空间至少其中之一时,允许该处理单元存取该私密空间,并将该处理单元传来的数据进行加密后再存入该私密空间,或者将该处理单元需要的数据从该私密空间读出并对其解密后,再传送给该处理单元。

[0009] 在本发明的一些实施态样中,该行动装置包括一输入单元,其接受输入该使用者

识别码及该使用者密码并将其传送给该处理单元。

[0010] 在本发明的一些实施态样中，该控制模块还包含一金融芯片，其中储存一密钥及一押码程序，且该控制模块判断该权限允许该处理单元存取该金融芯片时，将该处理单元传来的一要被押码的数据传送给该金融芯片，使执行该押码程序，以该密钥对该要被押码的数据押码而产生一交易押码，并回传该交易押码给该处理单元。

[0011] 在本发明的一些实施态样中，该隐密数据区存有一密钥，该控制模块具有一押码程序，且该控制模块判断该权限允许该处理单元存取该隐密数据区时，读取储存于该隐密数据区的该密钥，且接受该处理单元传来的一要被押码的数据，并执行该押码程序，以该密钥对该要被押码的数据押码而产生一交易押码，并回传该交易押码给该处理单元。

[0012] 在本发明的一些实施态样中，该控制模块还包含一储存一押码程序的金融芯片，该隐密数据区存有一密钥，且该控制模块判断该权限允许该处理单元存取该金融芯片及该隐密数据区时，该控制模块读取储存于该隐密数据区的该密钥，并将该密钥及该处理单元传来的一要被押码的数据提供给该金融芯片，使执行该押码程序，以该密钥对该要被押码的数据押码而产生一交易押码，并回传该交易押码给该处理单元。

[0013] 在本发明的一些实施态样中，该行动装置具有一主板，该处理单元设置在该主板上，且该权限控管单元是一设置在该主板上的芯片；或者，该权限控管单元的该控制模块是一设置在该主板上的第一芯片，该权限控管单元的该储存模块是一设置在该主板上的第二芯片。

[0014] 在本发明的一些实施态样中，该行动装置具有一主板及一与该主板电连接的电路板，该处理单元设置在该主板上，且该权限控管单元是设置在该电路板上；或者，该权限控管单元的该控制模块设置在该电路板上，该权限控管单元的该储存模块设置在该主板上。

[0015] 在本发明的一些实施态样中，该行动装置是一智能手机、一平板计算机或一笔记本电脑。

[0016] 本发明的有益的效果在于：借由内建在行动装置中的该权限控管单元，能对该处理单元存取该权限控管单元中的该储存模块，尤其是该储存模块中的该隐密数据区进行访问权限的控管，并让该权限控管单元能以单一芯片或独立的两个芯片与该处理单元设置在同一个或不同的电路板上，而达成本发明的目的。

附图说明

[0017] 图1是一电路方块图，说明本发明行动装置的一实施例主要包含的电路方块。

[0018] 图2是一电路方块图，说明本实施例的权限控管单元主要包含的电路方块。

[0019] 图3是一示意图，说明本实施例的权限控管单元设置在主板上。

[0020] 图4是一示意图，说明本实施例的权限控管单元的控制模块及储存模块各自独立地设置在主板上。

[0021] 图5是一示意图，说明本实施例的权限控管单元设置在一与主板电连接的电路板上。

[0022] 图6是一示意图，说明本实施例的权限控管单元的储存模块设置在主板上，且权限控管单元的控制模块设置在一与主板电连接的电路板上。

具体实施方式

[0023] 下面结合附图及实施例对本发明进行详细说明。

[0024] 在本发明被详细描述之前，应当注意在以下的说明内容中，类似的组件是以相同的编号来表示。

[0025] 参阅图1，是本发明内建智能安全行动装置的一实施例，本实施例的行动装置1可以是智能手机、平板计算机、笔记本电脑等可携式电子装置，但不以此为限，且其主要包括一内存单元10、一输入单元11、一显示单元18，一与内存单元10、显示单元18及输入单元11电连接的处理单元12及一与处理单元12电连接的权限控管单元13。

[0026] 在本实施例中，输入单元11可以是一键盘或一触控面板。内存单元10储存有至少一应用程序，处理单元12可以是一应用处理器(Application Processor，AP)或中央处理器。权限控管单元13主要包含一控制模块14及一储存模块15，该控制模块14具有一密码表16及一权限控管数据表17。其中该权限控管数据表17记录至少一使用者识别码及其使用该储存模块15的一权限，该密码表16记录该使用者识别码及其对应的一使用者密码。借此，当该处理单元12为了存取储存模块15内的数据而执行一应用程序时，该应用程序会先传送一认证信息给该权限控管单元13，并由其中的该控制模块14根据该认证信息判断该应用程序合法时，才允许该处理单元12与其建立联机，然后该处理单元12通过该应用程序传送一使用者识别码及一使用者密码给该控制模块14，该控制模块14根据该权限控管数据表17查询该使用者识别码的一权限，并判断该使用者密码与记录在该密码表16的该使用者密码是否相符，若是，才允许该处理单元12在该权限范围内使用该储存模块15。借此，达到对欲存取储存模块15的使用者进行身份验证及权限控管的目的。

[0027] 具体而言，如图2所示，本实施例的控制模块14主要包含一控制器芯片141及刻录于控制器芯片141中的一控制韧体142以及一应用程序编程接口(application program interface;API)143，且该密码表16及该权限控管数据表17被刻录储存在控制韧体142中。其中如下表1所示，密码表16存有行动装置之使用者的使用者识别码(例如ID1、ID2、ID3等)与使用者密码(例如CODE1、CODE2、CODE3等)，供验正使用者的身份。且实际上储存在密码表16中的密码，是经过加密而以乱码化方式储存的密码，以确保密码不会遭到非法窃取。此外，密码表16还存有被权限控管单元13认可且合法的应用程序的一识别码及其对应的一密码。

[0028]

密码表	
ID1	CODE1
ID2	CODE2
ID3	CODE3

[0029] 表1

[0030] 储存模块15包括一系统部分151及一储存部分152。系统部分151内建基本操作信息(basic operation information)。储存部分152包括一隐密数据区153及一可视区154。可视区154允许被行动装置1的处理单元12(即操作系统(OS))存取，而相当于行动碟的用途，以Android®系统举例来说，可视区154能被档案管理程序(file management

program)存取。但隐密数据区153则无法被处理单元12(操作系统)存取,亦即处理单元12不能对隐密数据区153储存的档案进行读取、写入或修改。相反的,处理单元12只有在完成特定的验证及授权顺序之后,处理单元12才能通过控制器芯片141中的控制韧体142存取隐密数据区153。因此处理单元12无法显示隐密数据区153给使用者,且只有当时使用者借由处理单元12通过所述验证及授权顺序时,使用者才能通过处理单元12存取隐密数据区153。

[0031] 因此,如下表2所示,该权限控管数据表17主要储存使用者的使用者识别码(例如ID1、ID2、ID3等)与其对应的一权限,例如使用者识别码ID1的权限为可读取、写入隐密数据区153,使用者识别码ID2的权限为可读取隐密数据区153、使用者识别码ID3的权限为可读取、写入及删除隐密数据区153等,以供验证使用者是否具有对隐密数据区153数据之读取、更新和删除的权限。

[0032]

权限控管数据表	
ID1	读取、写入
ID2	读取
ID3	读取、写入、删除

[0033] 表2

[0034] 举例来说,假设隐密数据区153储存有一密钥,且该密钥是对应于一用于行动支付的虚拟帐户,则当行动装置1欲使用该密钥以执行一行动支付时,处理单元12会执行一应用程序(例如一种支付软件)并输出一讯息至行动装置1的一显示单元18,要求使用者从输入单元11输入其使用者识别码及/或使用者密码(当然应用程序也可以直接使用先前已记录的使用者识别码及使用者密码,而不需要使用者输入)。接着处理单元12的应用程序将其包含有一识别码及一密码的认证信息及该使用者密码以及与该行动支付相关的一要被押码的数据传送给控制模块14的应用程序编程接口143,则应用程序编程接口143会先执行一建立联机功能,根据密码表16,判断该应用程序提供的识别码及密码是否有记录在密码表16中,若是,则判定该应用程序合法。应用程序编程接口143接着执行一权限控管管理功能,根据权限控管数据表17确认该应用程序提供的使用者识别码,例如ID2的权限为读取,并判断该应用程序提供的使用者密码(ID2)与密码表16中记录的一使用者密码相符,则允许该应用程序通过控制韧体142读取储存于隐密数据区153的该密钥,且由控制韧体142根据该密钥及该要被押码的数据产生一交易押码并回传给处理单元12,使处理单元12据以进行后续的行动支付作业。

[0035] 此外,本实施例的控制模块14还可包含一金融芯片140,其中储存有一发行该金融芯片140之金融机构的密钥及一押码程序。因此,当行动装置1之处理单元12欲使用该密钥,并通过上述的身份及权限验证后,控制模块14的控制韧体142会将处理单元12通过应用程序传来的一要被押码的数据传送给金融芯片140,使执行押码程序,以该密钥对要被押码的数据押码而产生一交易押码,并通过该应用程序回传给处理单元12,使处理单元12据以进行后续的行动支付作业。有关上述本实施例之金融芯片应用于行动支付的细节可参见中国台湾第I537851号专利。

[0036] 由此可知,本实施例的控制模块14不论是否包含金融芯片140,若行动装置1要用

于行动支付的该密钥储存在隐密数据区153时，则于通过上述的身份及权限验证后，由控制韧体142读取储存于隐密数据区153的该密钥，并执行预存于控制模块14内的该押码程序，以根据该密钥及处理单元12提供之该要被押码的数据产生一交易押码，关于此行动支付的细节可参见中国台湾第I509542专利；或者，当控制模块14内包含金融芯片140，且行动装置1要用于行动支付的该密钥(由非发行金融芯片140之金融机构提供)是储存在隐密数据区153时，则于通过上述的身份及权限验证后，由控制韧体142读取储存于隐密数据区153的该密钥，并将该密钥及要被押码的数据传送给金融芯片140，由金融芯片140执行该押码程序，以该密钥对要被押码的数据押码而产生一交易押码；又或者，若行动装置1要用于行动支付的该密钥是储存在金融芯片140内时，则于通过上述的身份及权限验证后，控制模块14的控制韧体142会将要被押码的数据传送给金融芯片140，由金融芯片140执行该押码程序，以该密钥对要被押码的数据押码而产生一交易押码。因此金融芯片140可视实际应用所需而被包含于控制模块14中或者省略。

[0037] 再者，本实施例至少具有身份识别、权限控管、私密空间及个资保护四种功能。针对身份识别功能，该储存模块15的隐密数据区153可记录一使用者的一身份识别数据，当处理单元12执行一应用程序要读取该身份识别数据而自动提供或者由输入单元11输入一使用者识别码及其使用者密码给权限控管单元13时，应用程序编程接口143以如同上述程序验证应用程序合法后，并根据权限控管数据表17判断该使用者识别码具有存取该储存模块15的隐密数据区153的权限，并判断该使用者密码与该密码表16记录的使用者密码相符时，则允许该处理单元12通过控制韧体142读取储存于隐密数据区153的该身份识别数据，以供行动装置1进行后续身份识别的应用。

[0038] 而针对权限控管功能，主要是在使用者取得行动装置1之前，将预先建立的密码表16及权限控管数据表17通过应用程序编程接口143刻录在控制韧体142中，其中密码表16主要记录使用行动装置1之每一使用者的使用者识别码及其对应的使用者密码，权限控管数据表17主要记录每一使用者识别码及其对储存模块15之隐密数据区153中的数据读取、更新及删除等权限，因此不同的使用者对于隐密数据区153的权限会有所不同。

[0039] 且应用程序编程接口143除了上述的建立联机功能及权限控管管理功能外，还具有在线个人化作业(Preso)管理功能，其能让处理单元12执行一应用程序与应用程序编程接口143建立联机后，并于通过上述的身份及权限验证时，让使用者根据实际应用所需对密码表16及权限控管数据表17进行设定与更新，并能依实际应用所需将储存模块15规划(切割)成多个不同的区块以供储存不同类型的数据，例如上述储存部分152的可视区154及隐密数据区153。

[0040] 针对私密空间功能，当处理单元12执行的一应用程序与控制模块14的应用程序编程接口143已建立联机，并通过上述权限控管管理功能的验证及授权，控制模块14的应用程序编程接口143能根据处理单元12执行的该应用程序下达的指令，利用在线个人化作业(Preso)管理功能将隐密数据区153切割出多个私密空间，以供存放不同种类的私密资料，例如行动支付相关资料、个人医疗(就医)资料、各种凭证等。并且控制模块14可在权限控管数据表17中针对不同的使用者识别码(即不同的使用者)设定其对所述私密空间的访问权限。

[0041] 针对个资保护功能，控制模块14的应用程序编程接口143会建置一加解密功能，而

能使用3DES(Triple Data Encryption Algorithm symmetric-key block cipher)、AES(Advanced Encryption Standard)或RSA等演算法对数据进行加密或解密。例如当处理单元12执行的一应用程序与控制模块14的应用程序编程接口143已建立联机，并且通过上述权限控管管理功能的验证，且该应用程序要写入一个资数据至隐密数据区153的一个资保护区块(由上述在线个人化作业(Preso)管理功能规划的一私密空间，图未示)时，应用程序编程接口143会以该加解密功能对该个资数据进行加密，再通过控制韧体142将加密后的该个资数据写入隐密数据区153的该个资保护区块。而若处理单元12执行的该应用程序要读取存于隐密数据区153的该个资保护区块的数据时，控制韧体142会将数据从该个资保护区块读出并传送给应用程序编程接口143，使应用加解密功能对该数据解密后，再通过控制韧体142将解密后的数据传送给处理单元12。

[0042] 此外，在本实施例中，如图3所示，该行动装置1具有一主板100，该处理单元12及该权限控管单元13设置在该主板100上，且该权限控管单元13是以一芯片的型态实现。

[0043] 或者，在本实施例中，如图4所示，该权限控管单元13的该控制模块14及该储存模块15可以各自独立设置在该主板100上，且控制模块14是以一第一芯片的型态实现，储存模块15是以一第二芯片的型态实现。

[0044] 或者，在本实施例中，如图5所示，该行动装置1还具有一与该主板100电连接的电路板20，该处理单元12设置在该主板100上，且该权限控管单元13是设置在该电路板20上，并以一芯片的型态实现。

[0045] 又或者，在本实施例中，如图6所示，该处理单元12及该权限控管单元13的储存模块15设置在该主板100上，且储存模块15是以一芯片的型态实现，而该权限控管单元13的控制模块14设置在该电路板20上，并以一芯片的型态实现。

[0046] 综上所述，本发明借由内建在行动装置1中的权限控管单元13，对处理单元12于访问权限控管单元13中的储存模块15时，进行权限控管，尤其是对储存模块15中的隐密数据区153之访问权限控管，并让权限控管单元13能以单一芯片或独立的两个芯片与处理单元12设置在同一个或不同的电路板上，而达成本发明的功效与目的。

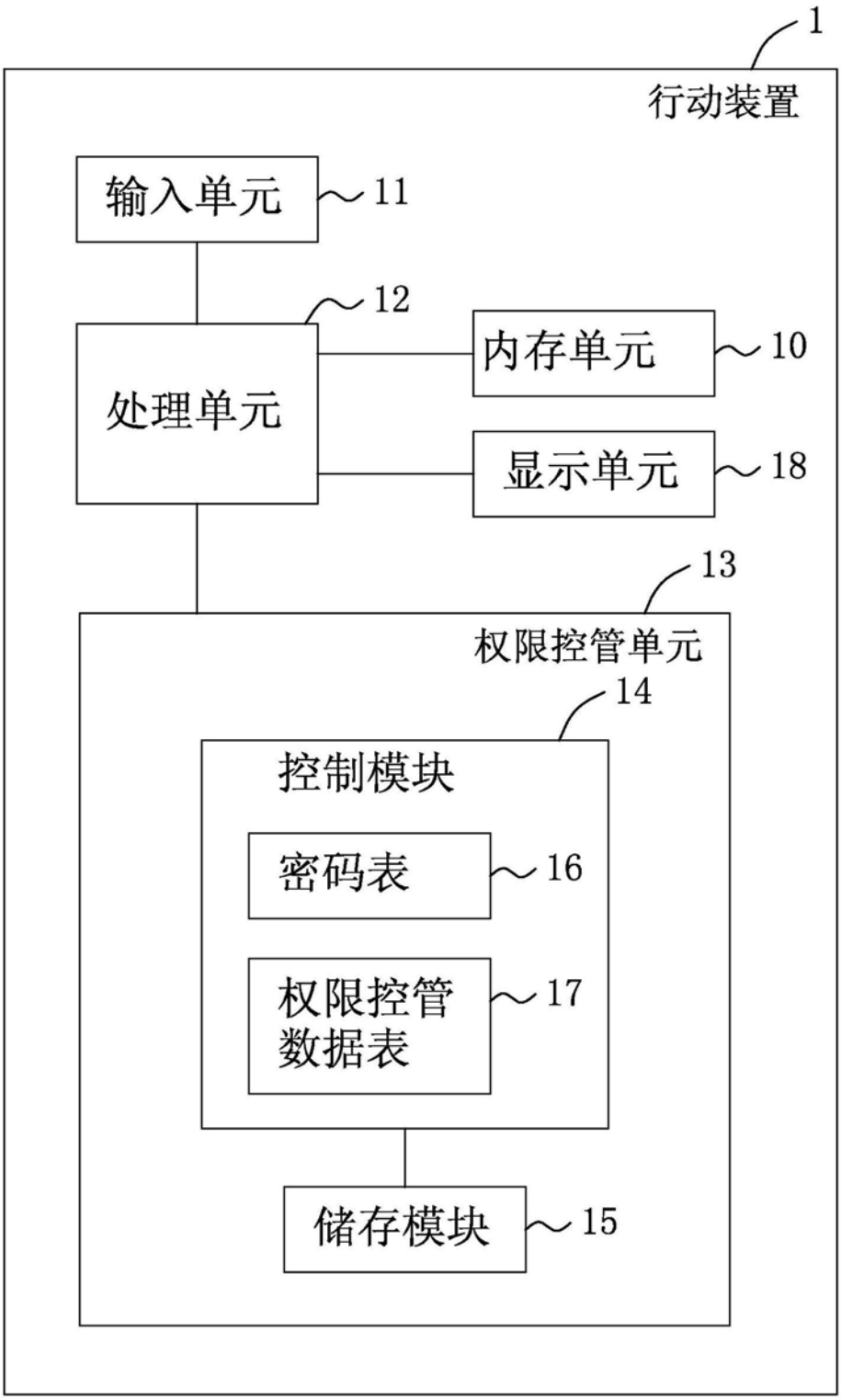

1
行动装置
输入单元
11
12
处理单元
内存单元
10
显示单元
18
13
权限控管单元
14
控制模块
密码表
16
权限控管
数据表
17
储存模块
15

图1

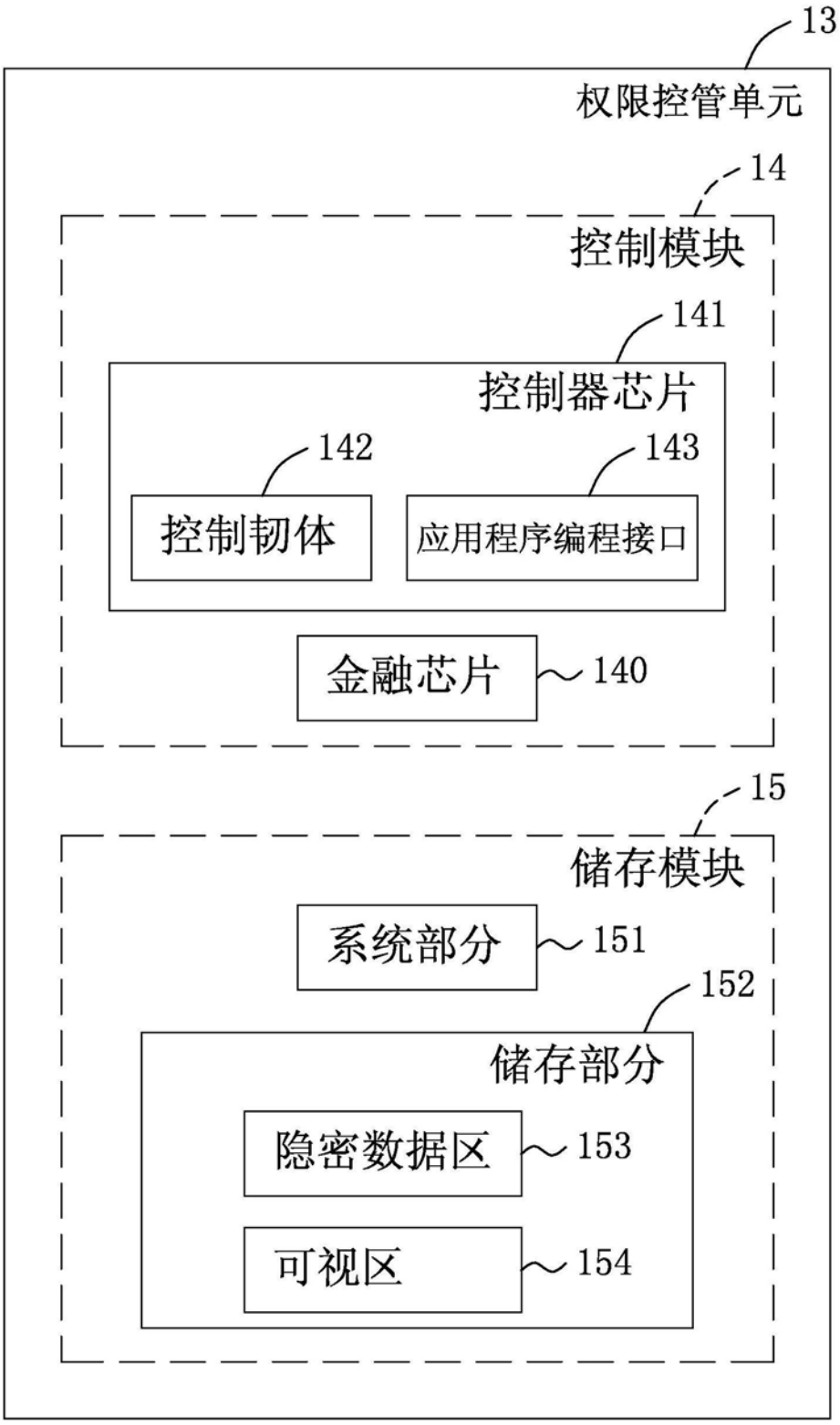

13
权限控管单元
14
控制模块
141
控制器芯片
142
控制韧体
143
应用程序编程接口
金融芯片
140
15
储存模块
系统部分
151
152
储存部分
隐密数据区
153
可视区
154

图2

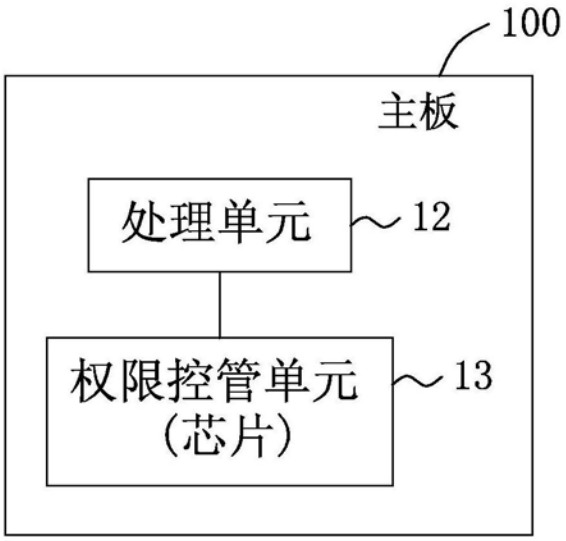

100
主板
处理单元
12
权限控管单元
(芯片)
13

图3

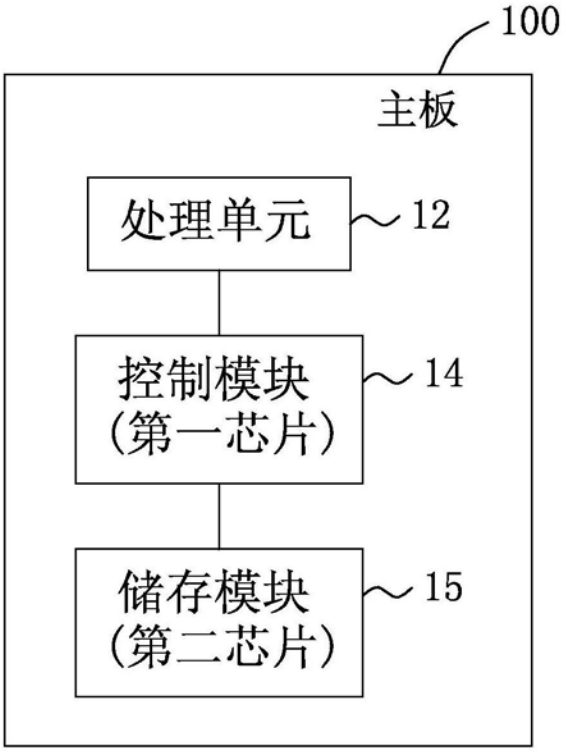

100
主板
处理单元
12
控制模块
(第一芯片)
14
储存模块
(第二芯片)
15

图4

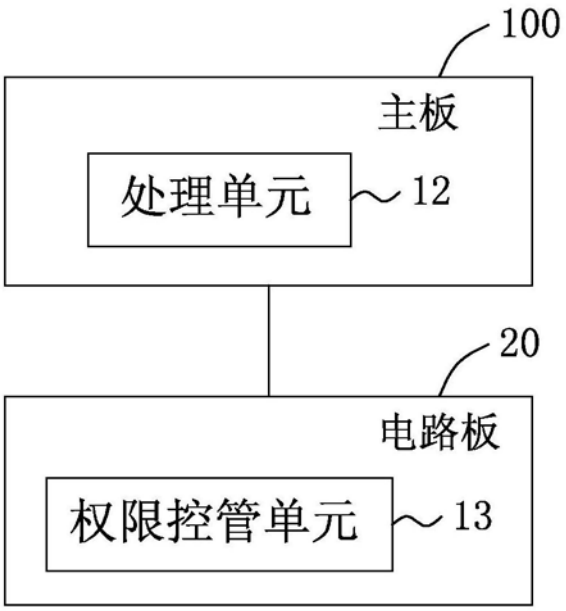

100
主板
处理单元
12
20
电路板
权限控管单元
13

图5

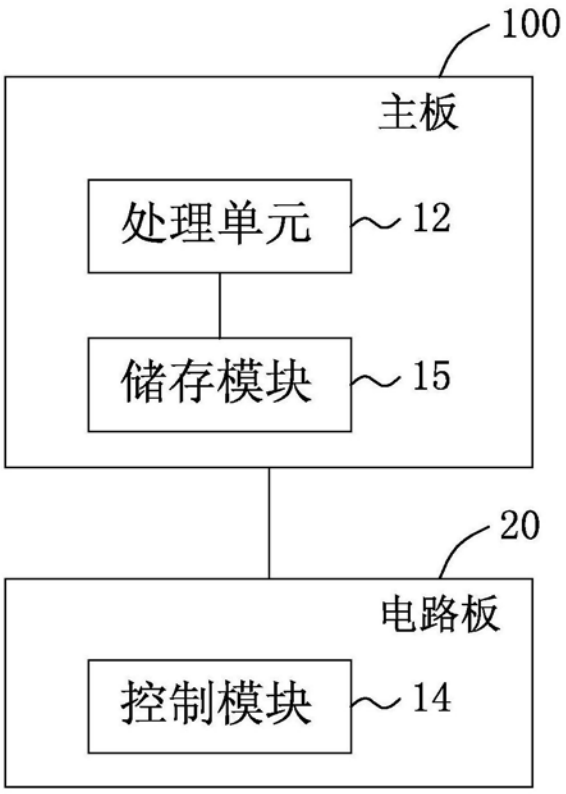

100
主板
处理单元
12
储存模块
15
20
电路板
控制模块
14

图6