(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 108345782 B
(45)授权公告日 2021.02.12

(21)申请号 201710187668.5

(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 108345782 A

(43)申请公布日 2018.07.31

(30)优先权数据
106102830 2017.01.25 TW
106201379 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 史瞳 谢琼慧

(51)Int.Cl.
G06F 21/35(2013.01)
G06F 21/60(2013.01)

(56)对比文件
US 2014289121 A1,2014.09.25
CN 101030175 A,2007.09.05
CN 105653986 A,2016.06.08
CN 101247336 A,2008.08.20

审查员 郭岚晞

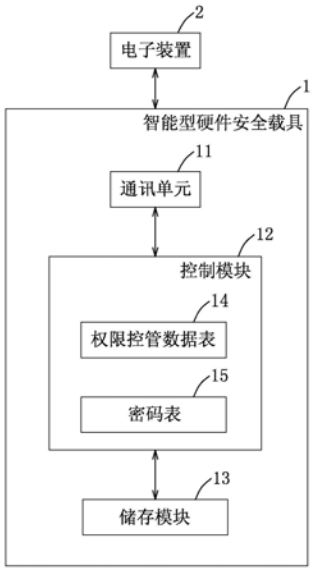
权利要求书2页 说明书7页 附图6页

(54)发明名称

智能型硬件安全载具

(57)摘要

一种智能型硬件安全载具，能与一电子装置电耦接，并包括一通讯单元、一储存模块及一具有一权限控管数据表及一密码表的控制模块，该电子装置通过该通讯单元传送一认证信息给该控制模块，且该控制模块判断该认证信息合法后，允许该电子装置通过该连接器与其建立联机，并接受该电子装置传来的一使用者识别码及一使用者密码，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一使用者密码相符时，允许该电子装置在该权限范围内使用该储存模块。



CN 108345782 B

1.一种智能型硬件安全载具,能与一电子装置电耦接,其特征在于:

该智能型硬件安全载具包括:

一通讯单元;

一储存模块,具有一隐密数据区;及

一控制模块,其与该通讯单元及该储存模块电连接,并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;

借此,该电子装置能通过该通讯单元传送一认证信息给该控制模块,且该控制模块判断该认证信息合法后,允许该电子装置通过该通讯单元与其建立联机,并接受该电子装置传来的一使用者识别码及一使用者密码,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,允许该电子装置在该权限范围内使用该储存模块;其中,该电子装置执行一应用程序,并通过该应用程序传送该应用程序的该认证信息给该控制模块,而该控制模块记录有该应用程序的一应用程序识别码及一应用程序密码,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应用程序识别码及该应用程序密码相符时,即判定该应用程序合法;且该控制模块判断该权限允许存取该隐密数据区时,允许该电子装置存取该隐密数据区,并且该控制模块判断该权限允许规划该隐密数据区时,该电子装置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,允许该电子装置存取该私密空间,并将该电子装置传来的数据进行加密后再存入该私密空间,或者将该电子装置需要的数据从该私密空间读出并对其解密后,再传送给该电子装置。

2.根据权利要求1所述的智能型硬件安全载具,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,允许该电子装置对该权限控管数据表及/或该密码表进行设定及更新。

3.根据权利要求1所述的智能型硬件安全载具,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电子装置存取该金融芯片时,将该电子装置通过该通讯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,并通过该通讯单元回传该交易押码给该电子装置。

4.根据权利要求1所述的智能型硬件安全载具,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,且接受该电子装置通过该通讯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,并通过该通讯单元回传该交易押码给该电子装置。

5.根据权利要求1所述的智能型硬件安全载具,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电子装置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,并将该密钥及该电子装置通过该通讯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,并通过该通讯单

元回传该交易押码给该电子装置。

6.根据权利要求1所述的智能型硬件安全载具，其特征在于：该通讯单元是一连接器。

7.根据权利要求1所述的智能型硬件安全载具，其特征在于：该通讯单元包含一连接器及一短距离无线通信接口，且该连接器与该电子装置电连接时，该电子装置通过该连接器与该控制模块通讯，该连接器未与该电子装置电连接时，该电子装置通过该短距离无线通信接口与该控制模块通讯。

8.根据权利要求1所述的智能型硬件安全载具，其特征在于：该通讯单元包含一连接器及一与该连接器电连接的短距离无线通信接口，且该连接器与该电子装置电连接时，该电子装置通过该连接器与该控制模块通讯，并通过该连接器与该短距离无线通信接口电连接，以通过该短距离无线通信接口收发一无线讯号；该连接器未与该电子装置电连接时，该电子装置通过该短距离无线通信接口与该控制模块通讯。

9.根据权利要求1至8中任一权利要求所述的智能型硬件安全载具，其特征在于：该智能型硬件安全载具还包括一电路板，该通讯单元设置在该电路板上，且该储存模块与该控制模块被整合于一芯片中并设置在该电路板上。

10.根据权利要求1至8中任一权利要求所述的智能型硬件安全载具，其特征在于：该智能型硬件安全载具还包括一电路板，该通讯单元设置在该电路板上，且该控制模块是一设置在该电路板上的第一芯片，该储存模块是一设置在该电路板上的第二芯片。

智能型硬件安全载具

技术领域

[0001] 本发明涉及一种随身装置,特别是涉及一种智能型硬件安全载具。

背景技术

[0002] 现有配置连接器的随身装置,例如USB随身碟能让使用者借由其连接器与一电子装置电连接,以供该电子装置读取其中储存的数据或储存电子装置写入的数据并随身携带,可谓相当地方便。然而该随身装置本身通常不具有权限控管功能,而易遭有心人士不当窃取或更动其中储存的数据。因此,若能赋予随身装置本身权限控管的能力,将能防止随身装置在未通过其验证程序的情况下被不当地存取。

发明内容

[0003] 本发明的目的在于提供一种能对使用者进行身份验证及权限控管之智能型硬件安全载具。

[0004] 本发明一种智能型硬件安全载具,能与一电子装置电耦接,并包括一通讯单元、一储存模块及一控制模块,该控制模块与该通讯单元及该储存模块电连接,并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;该电子装置能通过该通讯单元传送一认证信息给该控制模块,且该控制模块判断该认证信息合法后,允许该电子装置通过该通讯单元与其建立联机,并接受该电子装置传来的一使用者识别码及一使用者密码,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,允许该电子装置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,该电子装置执行一应用程序,并通过该应用程序传送该应用程序的该认证信息给该控制模块,而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符时,即判定该应用程序合法。

[0006] 在本发明的一些实施态样中,该储存模块具有一隐密数据区,且该控制模块判断该权限允许存取该隐密数据区时,允许该电子装置存取该隐密数据区。

[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规划该隐密数据区时,该电子装置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,允许该电子装置存取该私密空间,并将该电子装置传来的数据进行加密后再存入该私密空间,或者将该电子装置需要的数据从该私密空间读出并对其解密后,再传送给该电子装置。

[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设定与更新该权限控管数据表及/或该密码表时,允许该电子装置对该权限控管数据表及/或该密码表进行设定及更新。

[0009] 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电子装置存取该金融芯片时，将该电子装置通过该通讯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，并通过该通讯单元回传该交易押码给该电子装置。

[0010] 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，且接受该电子装置通过该通讯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，并通过该通讯单元回传该交易押码给该电子装置。

[0011] 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电子装置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，并将该密钥及该电子装置通过该通讯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，并通过该通讯单元回传该交易押码给该电子装置。

[0012] 在本发明的一些实施态样中，该通讯单元是一连接器；或者，该通讯单元包含一连接器及一短距离无线通信接口，且该连接器与该电子装置电连接时，该电子装置通过该连接器与该控制模块通讯，该连接器未与该电子装置电连接时，该电子装置通过该短距离无线通信接口与该控制模块通讯；又或者，该通讯单元包含一连接器及一与该连接器电连接的短距离无线通信接口，且该连接器与该电子装置电连接时，该电子装置通过该连接器与该控制模块通讯，并通过该连接器与该短距离无线通信接口电连接，以通过该短距离无线通信接口收发一无线讯号，而该连接器未与该电子装置电连接时，该电子装置通过该短距离无线通信接口与该控制模块通讯。

[0013] 在本发明的一些实施态样中，该智能型硬件安全载具还包括一电路板，该通讯单元设置在该电路板上，且该储存模块与该控制模块被整合于一芯片中并设置在该电路板上。

[0014] 在本发明的一些实施态样中，该智能型硬件安全载具还包括一电路板，该连接器设置在该电路板上，且该储存模块与该控制模块被整合于一芯片中并设置在该电路板上；或者，该控制模块是一设置在该电路板上的第一芯片，该储存模块是一设置在该电路板上的第二芯片。

[0015] 本发明的有益的效果在于：借由设置在智能型硬件安全载具中的控制模块对要存取智能型硬件安全载具的储存模块(尤其是隐密数据区)之电子装置进行访问权限的控管，而达成本发明对智能型硬件安全载具的使用者进行身份验证及权限控管。

附图说明

[0016] 图1是一电路方块图，说明本发明智能型硬件安全载具的一实施例主要包含的电路方块。

[0017] 图2是一电路方块图，说明本实施例的通讯单元的一实施态样。

[0018] 图3是一电路方块图，说明本实施例的通讯单元的另一实施态样。

[0019] 图4是一电路方块图，说明本实施例的控制模块及储存模块主要包含的电路方块。

[0020] 图5是一示意图，说明本实施例的控制模块及储存模块以整合于一芯片的方式设置在电路板上。

[0021] 图6是一示意图，说明本实施例的控制模块及储存模块以各自独立的芯片型式设置在电路板上。

具体实施方式

[0022] 下面结合附图及实施例对本发明进行详细说明。

[0023] 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。

[0024] 参阅图1，是本发明智能型硬件安全载具的一实施例，本实施例的智能型硬件安全载具1外观尺寸类似随身碟(或行动碟)而可随身携带，但并不以此为限。其主要包括一用以与一电子装置2通讯的通讯单元11，一与通讯单元11电连接的控制模块12及一与控制模块12电连接的储存模块13。其中电子装置2可以是例如智能型手机、平板计算机、笔记本电脑、个人计算机等主动式电子设备。通讯单元11可以是现有的连接器111(见图2)，例如一般的USB连接器插头、一mini USB连接器插头、一micro USB连接器插头或其组合，并不以此为限，举凡现行用于连接一外接周边装置或随身装置至一主动式电子装置的连接器规格皆适用于本实施例。

[0025] 此外，如图2所示，通讯单元11除了连接器111之外，还可包含一短距离无线通信接口112，例如NFC(近场通讯)接口，借此，当该连接器111与电子装置2电连接时，该电子装置2能通过该连接器111与该控制模块12通讯，当该连接器111未与该电子装置2电连接时，该电子装置2若具有短距离无线通信功能(例如NFC功能)，即能借由与智能型硬件安全载具1相互靠近，而通过该短距离无线通信接口112与智能型硬件安全载具1的该控制模块12通讯。

[0026] 或者，如图3所示，该通讯单元11除了包含连接器111以外，还包含一与该连接器111电连接的短距离无线通信接口112，例如NFC接口；借此，当该连接器111与该电子装置2电连接时，该电子装置2能通过该连接器111与该控制模块12通讯，且若该电子装置2不具有短距离无线通信功能(例如NFC功能)，电子装置2则可以通过该连接器111与该短距离无线通信接口112电连接，以通过该短距离无线通信接口112与另一电子装置(图未示)进行短距离无线通信；而当该连接器111未与该电子装置2电连接时，若该电子装置2具有短距离无线通信功能(例如NFC功能)，则该电子装置2即能通过智能型硬件安全载具1的该短距离无线通信接口112与该控制模块12通讯。

[0027] 如图1所示，该控制模块12具有一权限控管数据表14及一密码表15。其中该权限控管数据表14记录至少一使用者的使用者识别码及其使用该储存模块13的一权限，该密码表15记录该使用者识别码及其对应的一使用者密码。借此，当智能型硬件安全载具1通过通讯单元11与电子装置2电连接后，电子装置2为了存取储存模块13内的数据而执行一应用程序时，该应用程序需先通过通讯单元11传送一认证信息给该控制模块12，由该控制模块12根据该认证信息判断该应用程序合法时，才允许该应用程序(即电子装置2)与其建立联机，然后该电子装置2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12，该

控制模块12根据该权限控管数据表14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15的该使用者密码是否相符，若是，才允许该电子装置2的该应用程序在该权限范围内使用该储存模块13。借此，达到对欲使用智能型硬件安全载具1的使用者进行身份验证及权限控管，而达到防止智能型硬件安全载具1被不当地任意存取的目的。

[0028] 具体而言，如图4所示，本实施例的控制模块12主要包含一控制器芯片121及刻录于控制器芯片121中的一控制韧体122以及一应用程序编程接口(application program interface;API)123，且该权限控管数据表14及该密码表15被刻录储存在控制韧体122中。其中如下表1所示，密码表15存有智能型硬件安全载具1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)，供验证使用者的身份。且实际上储存在密码表15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15还存有被控制模块12认可且合法的每一个应用程序的一识别码及其对应的一密码。

[0029]

密码表	
使用者识别码	使用者密码

[0030]

ID1	CODE1
ID2	CODE2
ID3	CODE3

[0031] 表1

[0032] 储存模块13主要包括一系统数据区131及一隐密数据区132。系统数据区131主要储存智能型硬件安全载具1的基本操作信息(basic operation information)。而隐密数据区132并无法被电子装置2存取，亦即电子装置2在未经控制模块12的授权下，并不能对隐密数据区132储存的档案或数据进行读取、写入或修改。相反地，电子装置2只有在完成控制模块12特定的验证及授权程序之后，才能通过控制模块12的控制器芯片121中的控制韧体122存取储存模块13的隐密数据区132。所以，电子装置2与智能型硬件安全载具1电连接后，并无法显示智能型硬件安全载具1的隐密数据区132给使用者，且只有当使用者借由电子装置2通过所述验证及授权程序后，使用者才能通过电子装置2存取隐密数据区132。

[0033] 因此，如下表2所示，该权限控管数据表14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的权限为可对隐密数据区132进行读取及写入，使用者识别码ID2的权限为可读取隐密数据区132，使用者识别码ID3的权限为可对隐密数据区132进行读取、写入及删除等，故该权限控管数据表14主要供验证使用者是否具有对隐密数据区132进行读取、更新及/或删除的权限。

[0034]

权限控管数据表	
使用者识别码	权限
ID1	读取、写入
ID2	读取
ID3	读取、写入、删除

[0035] 表2

[0036] 举例来说，假设隐密数据区132储存有一密钥，且该密钥是被用于一行动支付作业，则当电子装置2欲使用该密钥以执行一行动支付时，电子装置2会执行一应用程序(例如一种行动支付软件)并要求使用者输入其使用者识别码及/或使用者密码(或者该应用程序也可以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)。接着电子装置2的该应用程序将其包含有一识别码及一密码的认证信息、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12，则控制模块12的应用程序编程接口123会先执行一建立联机功能，根据密码表15，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15中，若是，则判定该应用程序合法。接着，应用程序编程接口123执行一权限控管管理功能，根据权限控管数据表14的记录，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，例如CODE2与密码表15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122读取储存于隐密数据区132的该密钥，且由控制韧体122根据该密钥及该要被押码的数据产生一交易押码并通过该通讯单元11回传给电子装置2，使电子装置2能据以进行后续的行动支付作业。

[0037] 此外，如图4所示，本实施例的控制模块12还可包含一金融芯片120，其中储存有一发行该金融芯片120之金融机构的密钥及一押码程序。因此，当电子装置2欲使用该密钥执行一行动支付，并通过上述控制模块12的身份及权限验证后，控制模块12的应用程序编程接口123会将电子装置2通过应用程序经由该通讯单元11传来的一要被押码的数据传送给金融芯片120，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，并通过应用程序编程接口123经由该通讯单元11回传给电子装置2，使电子装置2能据以进行后续的行动支付作业。有关上述金融芯片120应用于行动支付的细节可参见中国台湾第I537851号专利。

[0038] 因此，当控制模块12不论是否包含金融芯片120，若电子装置2要用于行动支付的该密钥储存在储存模块13的隐密数据区132时，则由控制韧体122读取储存于隐密数据区132的该密钥，并执行预存于控制器芯片121内的该押码程序，使根据该密钥及电子装置2提供之该要被押码的数据产生一交易押码。有关此行动支付的细节可参见中国台湾第I509542专利。

[0039] 或者，当控制模块12内包含金融芯片120，但行动装置1要用于行动支付的该密钥(由非发行金融芯片120之金融机构提供)是储存在隐密数据区132时，则由控制韧体122读取储存于隐密数据区132的该密钥，并将该密钥及要被押码的数据传送给金融芯片120，由金融芯片120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。

[0040] 又或者，若电子装置2要用于行动支付的该密钥是储存在金融芯片120内时，则控

制模块12的控制韧体122会将要被押码的数据传送给金融芯片120，由金融芯片120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120可视实际应用所需而被包含于控制模块12中或者省略。

[0041] 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13的隐密数据区132可记录一使用者的一身份识别数据，借此，当电子装置2执行一应用程序要读取该身份识别数据，而自动提供或者由使用者输入一使用者识别码及其使用者密码给控制模块12时，应用程序编程接口123以如同上述程序验证应用程序合法后，根据权限控管数据表14判断该使用者识别码具有存取该隐密数据区132的权限，并判断该使用者密码与该密码表15记录的使用者密码相符时，则允许该电子装置2通过控制韧体122读取储存于隐密数据区132的该身份识别数据，以供电子装置2进行后续身份识别的应用。

[0042] 而针对权限控管功能，主要是在使用者取得智能型硬件安全载具1之前，将预先建立的权限控管数据表14及密码表15通过应用程序编程接口123刻录在控制韧体122中，其中密码表15主要记录使用智能型硬件安全载具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14主要记录每一使用者识别码及其对储存模块13之隐密数据区132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132的权限将会有所不同。

[0043] 且应用程序编程接口123除了上述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，其能让电子装置2执行一应用程序与应用程序编程接口123建立联机后，并通过上述权限控管管理功能的验证及授权，让使用者根据实际应用所需，对权限控管数据表14及密码表15进行设定与更新。

[0044] 而针对私密空间功能，当电子装置2执行的一应用程序与控制模块12的应用程序编程接口123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12的应用程序编程接口123能根据电子装置2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132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、各种身份或会员凭证等。并且控制模块12可在权限控管数据表14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。

[0045] 针对个资保护功能，控制模块12的应用程序编程接口123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等算法对数据进行加密或解密。例如当电子装置2执行的一应用程序与控制模块12的应用程序编程接口123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笔个资数据至隐密数据区132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123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122将加密后的该个资数据写入隐密数据区132的该个资保护区块。而若电子装置2的该应用程序要读取存于隐密数据区132的该个资保护区块的数据时，控制韧体122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123，使应用该加解密功能对该数据解密后，再通过控制韧体122将解密后的数据传送给电子装置2。

[0046] 此外，在本实施例中，如图5所示，该智能型硬件安全载具1具有一电路板10，且通讯单元11、控制模块12及储存模块13是设置在该电路板10上，且该储存模块13与该控制模块12是被整合于一芯片中，再通过电路板10与通讯单元11电连接。

[0047] 或者，在本实施例中，如图6所示，控制模块12及储存模块13也可以各自独立地设置在智能型硬件安全载具1的电路板10'上，且控制模块12是以一第一芯片的型态实现，储存模块13是以一第二芯片的型态实现。

[0048] 综上所述，本发明借由设置在智能型硬件安全载具1中的控制模块12，对要存取智能型硬件安全载具1的储存模块13(尤其是隐密数据区132)之电子装置2进行访问权限的控管，而达成本发明对智能型硬件安全载具1的使用者进行身份验证及权限控管的功效与目的。

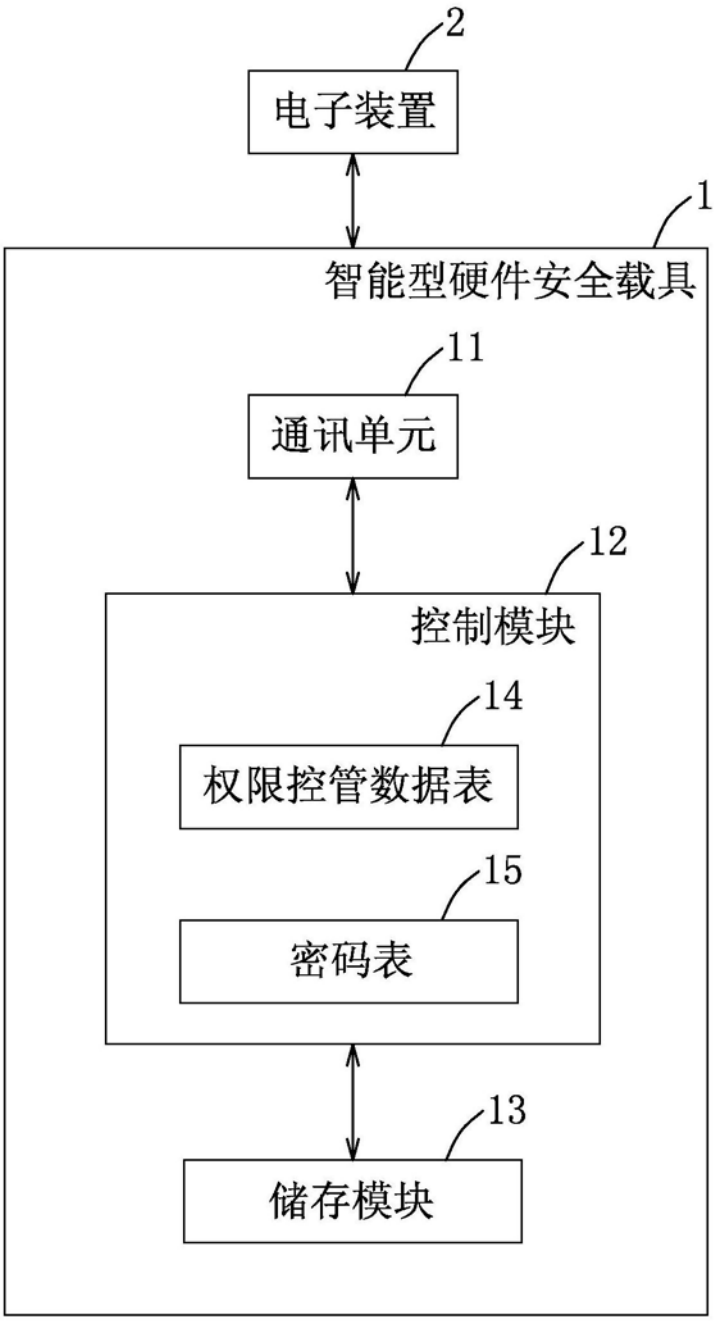


图1

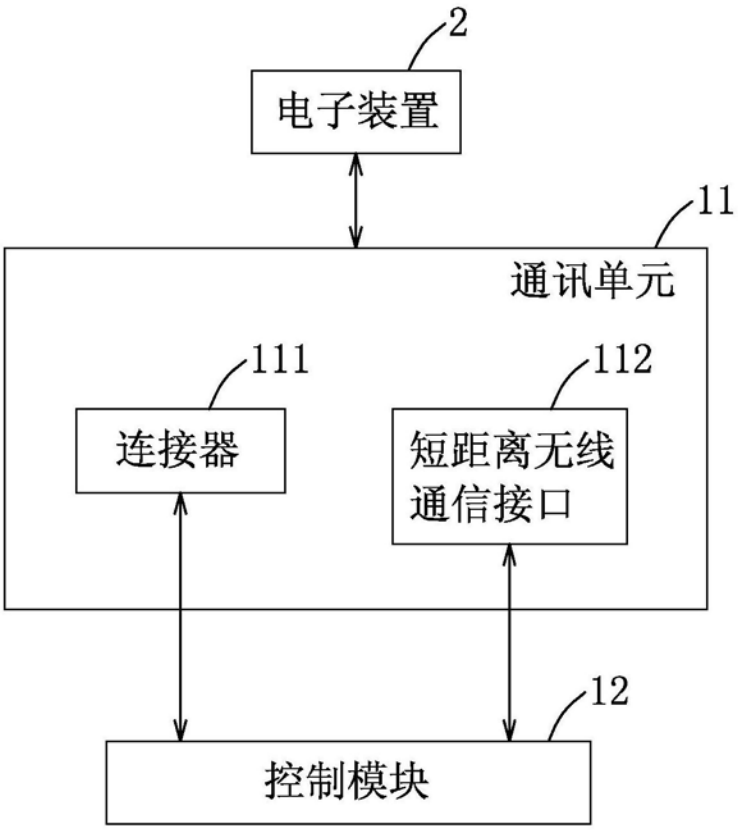


图2

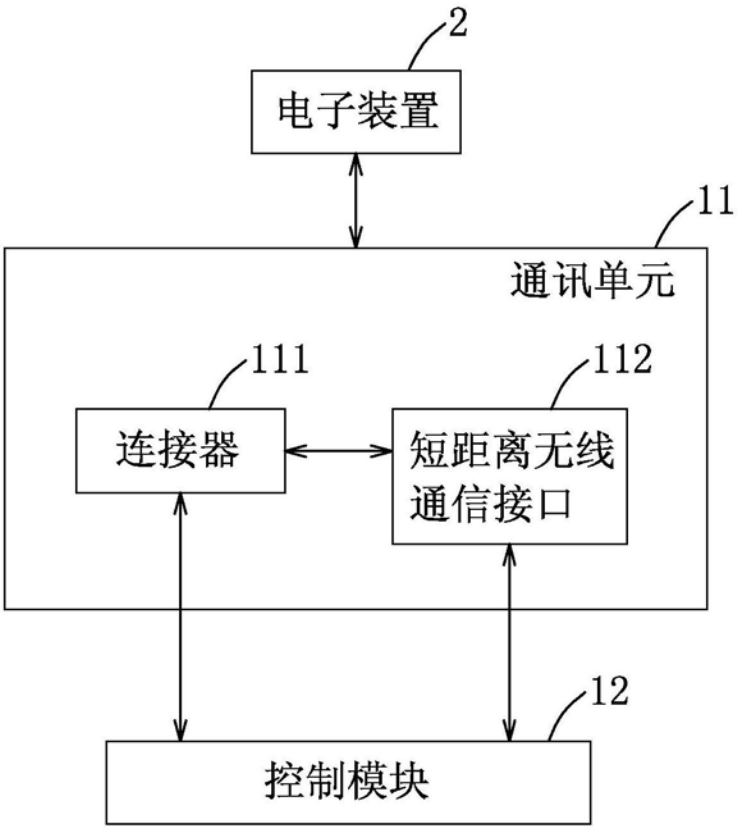


图3

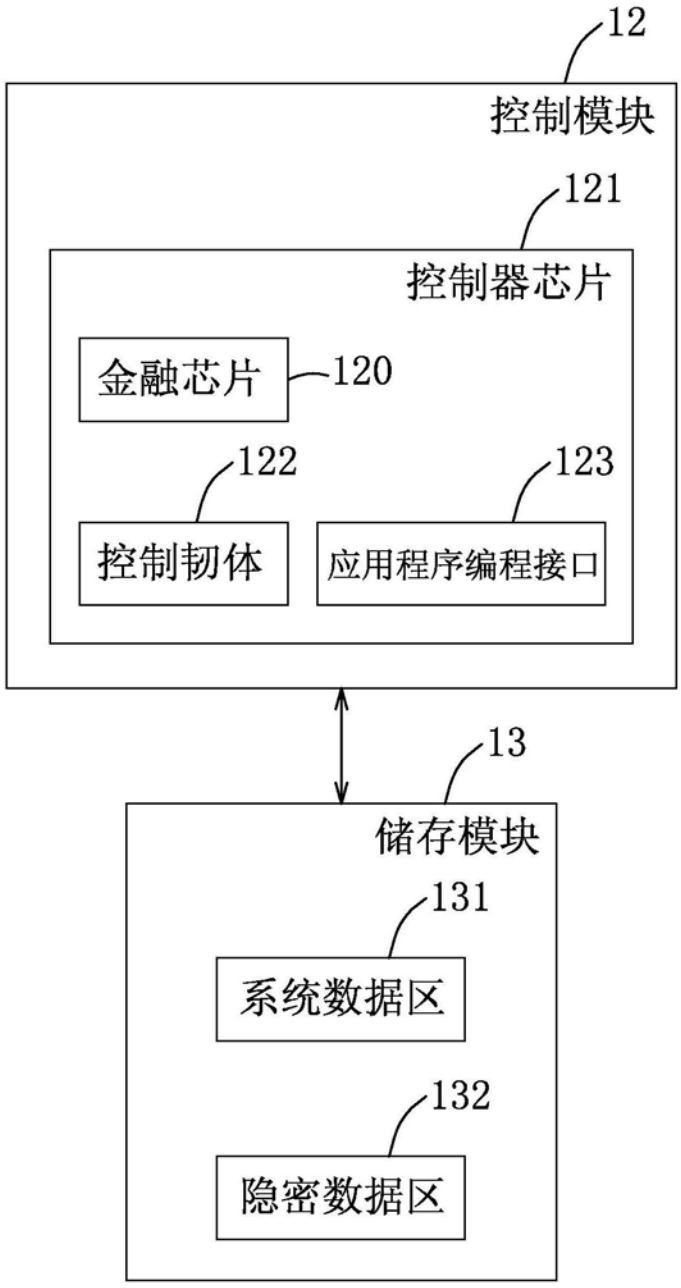

12
控制模块
121
控制器芯片
金融芯片
120
122
123
控制韧体
应用程序编程接口
13
储存模块
131
系统数据区
132
隐密数据区

图4

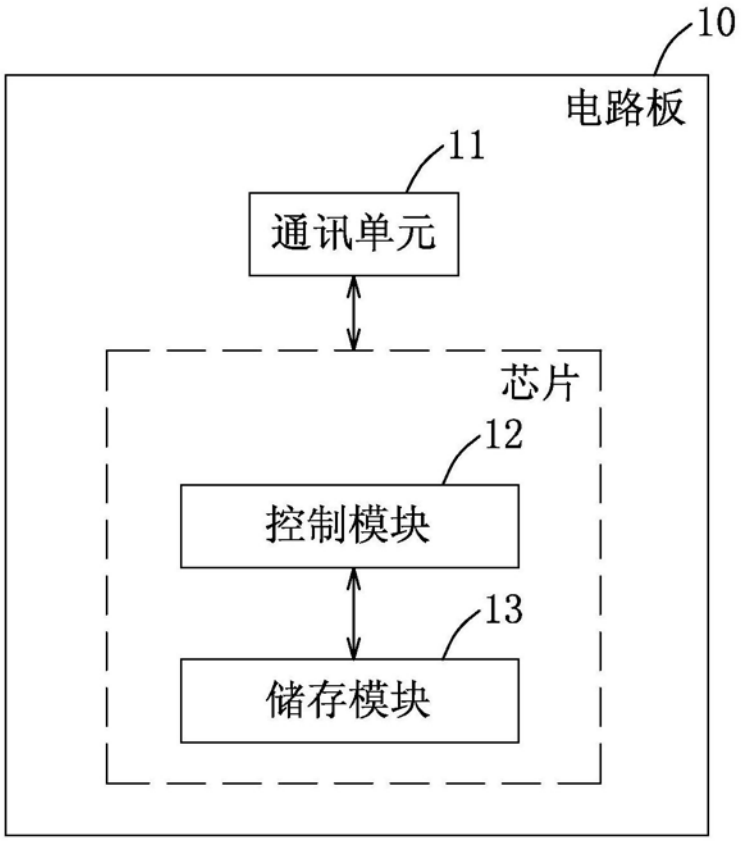


图5

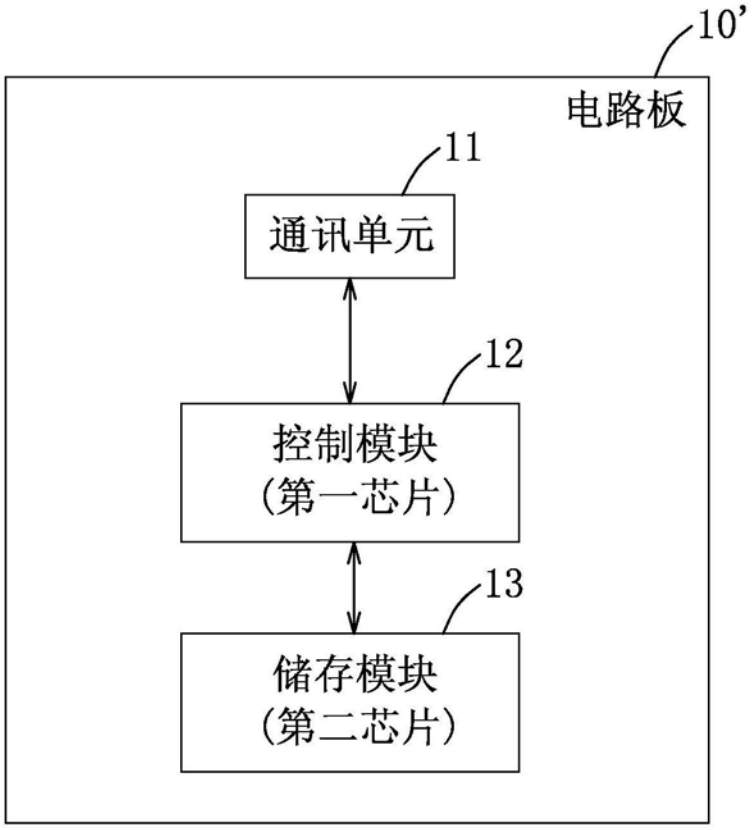


图6