

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2015 年 7 月 9 日 (09.07.2015)



(10) 国际公布号
WO 2015/101249 A1

- (51) 国际专利分类号:
G06F 21/12 (2013.01)
- (21) 国际申请号: PCT/CN2014/095272
- (22) 国际申请日: 2014 年 12 月 29 日 (29.12.2014)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201310741044.5 2013 年 12 月 30 日 (30.12.2013) CN
- (71) 申请人: 中国银联股份有限公司 (CHINA UNION-PAY CO., LTD.) [CN/CN]; 中国上海市浦东新区含笑路 36 号银联大厦, Shanghai 200135 (CN)。
- (72) 发明人: 郭伟 (GUO, Wei); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。周钰 (ZHOU, Yu); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。陈成钱 (CHEN, Chengqian); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。

- (74) 代理人: 中国专利代理 (香港) 有限公司 (CHINA PATENT AGENT (HK)LTD.); 中国香港特别行政区香港湾仔港湾道 23 号鹰君中心 22 字楼, Hong Kong (CN)。
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。
- (84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE,

[见续页]

(54) Title: DEVICE USED FOR SECURE INFORMATION INTERACTION AND APPARATUS

(54) 发明名称: 用于安全性信息交互的设备及装置

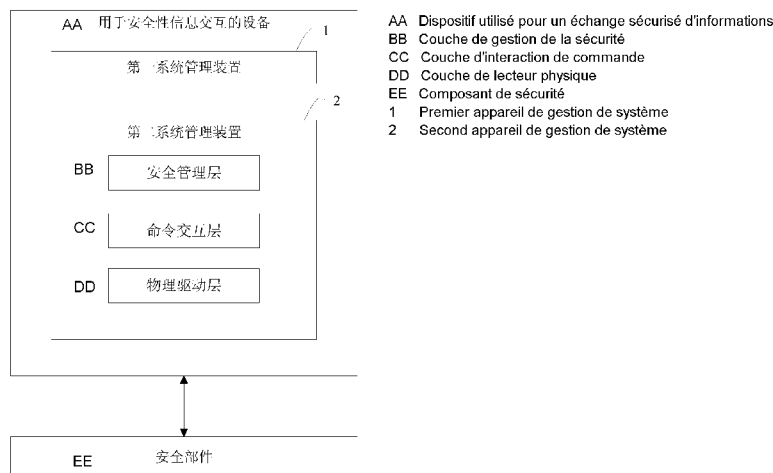


图 1 / Fig. 1

(57) Abstract: The present invention provides a device used for secure information interaction and a security component management apparatus, wherein the security component management apparatus can provide a running environment for a security application under a secure mode so as to execute a secure information interaction process and the security component management apparatus manages different types of security components through a unified interface protocol. The device used for the secure information interaction and the security component management apparatus disclosed by the present invention have high security, wide applicability and lower complexity.

(57) 摘要: 本发明提出了用于安全性信息交互的设备及安全部件管理装置。其中, 所述安全部件管理装置能够为安全性应用提供安全模式下的运行环境, 以执行安全性信息交互过程, 其中, 所述安全部件管理装置通过统一的接口协议管理不同类型的安全部件。本发明所公开的用于安全性信息交互的设备及安全部件管理装置具有高度的安全性以及广泛的适用性, 并且复杂度较低。



WO 2015/101249 A1



IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO,
RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI,
CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD,
TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

用于安全性信息交互的设备及装置

技术领域

本发明涉及用于信息交互的设备及装置，更具体地，涉及用于安全性信息交互的设备及装置。

背景技术

目前，随着计算机和网络应用的日益广泛以及不同领域的业务种类的日益丰富，用于安全性信息交互（即对安全性要求较高的信息交互，例如金融领域中的交易处理过程）的设备（尤其是基于移动终端的安全性信息交互设备）及装置变得越来越重要。

在现有的技术方案中，为了提高信息交互设备的安全性，典型地采用如下方式：使用具有较高安全性的安全单元（SE）来存储用户的敏感信息，并结合对应的安全部件（例如 NFC 模块）一起工作。

然而，现有的技术方案存在如下问题：由于不同的安全单元具有不同的管理和数据交互模式（例如使用不同的数据传输协议），故在存在多个安全单元的情况下，整个系统的复杂度显著增加（例如需要支持多个数据传输协议）并且操作过程繁琐（例如不同数据传输协议之间的转换），其次，由于所有安全单元以及相应的安全部件均在非安全的运行环境下工作，故仍然难于从根本上防止安全信息被窥探和篡改的潜在风险。

因此，存在如下需求：提供具有高度的安全性以及广泛的适用性，并且复杂度较低的用于安全性信息交互的设备及装置。

发明内容

为了解决上述现有技术方案所存在的问题，本发明提出了具有高度的安全性以及广泛的适用性，并且复杂度较低的用于安全性信息交互的设备及装置。

本发明的目的是通过以下技术方案实现的：

一种安全部件管理装置，所述安全部件管理装置能够为安全性应用提供安全模式下的运行环境，以执行安全性信息交互过程，其中，所述安全部件管理

装置通过统一的接口协议管理不同类型的安全部件。

在上面所公开的方案中，优选地，所述安全部件管理装置能够为属于不同的服务提供方的安全性应用提供单独的安全模式下的运行环境。

在上面所公开的方案中，优选地，所述统一的接口协议包括安全管理层、命令交互层以及物理驱动层，所述安全管理层用于针对不同的安全部件执行相应的安全性操作，所述命令交互层用于按照不同的数据传输协议执行安全性应用与相应的安全部件之间的数据通信，所述物理驱动层用于在物理上实际驱动所述不同类型的安全部件。

在上面所公开的方案中，优选地，所述安全管理层所执行的安全性操作包括下列中的一个或多个：安全部件访问权限控制、安全部件识别、维护当前所使用的密钥、提供并维护安全性应用与相应的安全部件之间的安全通道。

在上面所公开的方案中，优选地，所述安全部件管理装置管理并维护安全部件列表，所述安全部件列表记录当前与用于安全性信息交互的设备相连接的每个安全部件的属性信息，所述属性信息包括安全部件名、安全部件标识符以及该安全部件所支持的功能。

在上面所公开的方案中，优选地，当新的安全部件被连接时，所述安全部件管理装置能够通过向所述新的安全部件发送识别命令的方式而从所述新的安全部件获取该安全部件的属性信息，并将所述属性信息记录在所述安全部件列表中，以及为所述新的安全部件分配安全部件标识符。

在上面所公开的方案中，优选地，所述安全部件管理装置能够通过所述统一的接口协议对安全部件执行如下操作：打开安全部件操作、安全部件读/写操作、安全部件查询操作、关闭安全部件操作。

本发明的目的也通过以下技术方案实现：

一种用于安全性信息交互的设备，所述用于安全性信息交互的设备包括：第一系统管理装置，所述第一系统管理装置为常规的应用提供运行环境；第二系统管理装置，所述第二系统管理装置为安全性应用提供安全模式下的运行环境，以执行安全性信息交互过程，

其中，在当前待运行的应用是常规的应用的情况下，所述用于安全性信息交互的设备将所述第一系统管理装置作为当前使用的系统管理装置，而在当前

待运行的应用是安全性应用的情况下，所述用于安全性信息交互的设备将所述第二系统管理装置作为当前使用的系统管理装置，

并且其中，所述第二系统管理装置通过统一的接口协议管理不同类型的安全部件。

5 在上面所公开的方案中，优选地，所述第二系统管理装置使用的资源与所述第一系统管理装置使用的资源相隔离。

在上面所公开的方案中，优选地，所述第二系统管理装置能够为属于不同的服务提供方的安全性应用提供单独的安全模式下的运行环境。

10 在上面所公开的方案中，优选地，所述统一的接口协议包括安全管理层、命令交互层以及物理驱动层，所述安全管理层用于针对不同的安全部件执行相应的安全性操作，所述命令交互层用于按照不同的数据传输协议执行安全性应用与相应的安全部件之间的数据通信，所述物理驱动层用于在物理上实际驱动所述不同类型的安全部件。

15 本发明所公开的用于安全性信息交互的设备及装置具有下列优点：由于能够使用统一的接口协议管理不同类型的安全部件，由此具有高度的安全性以及广泛的适用性，并且复杂度较低，从而能够从根本上防止安全信息被窥探和篡改的潜在风险。

附图说明

20 结合附图，本发明的技术特征以及优点将会被本领域技术人员更好地理解，其中：

图1是根据本发明的实施例的用于安全性信息交互的设备的示意性结构图。

25 具体实施方式

图1是根据本发明的实施例的用于安全性信息交互的设备的示意性结构图。如图1所示，本发明所公开的用于安全性信息交互的设备包括第一系统管理装置1和第二系统管理装置2。其中，所述第一系统管理装置1（例如常规的多媒体操作系统）为常规的应用提供运行环境。所述第二系统管理装置2为安

全性应用（即对安全性要求较高的应用，例如金融领域中的支付应用）提供安全模式下的运行环境，以执行安全性信息交互过程。其中，在当前待运行的应用是常规的应用的情况下，所述用于安全性信息交互的设备将所述第一系统管理装置1作为当前使用的系统管理装置，而在当前待运行的应用是安全性应用的情况下，所述用于安全性信息交互的设备将所述第二系统管理装置2作为当前使用的系统管理装置（示例性地，所述用于安全性信息交互的设备能够在所述第一系统管理装置1和所述第二系统管理装置2之间进行切换）。其中，所述第二系统管理装置2通过统一的接口协议管理不同类型的安全部件。

优选地，在本发明所公开的用于安全性信息交互的设备中，所述第二系统管理装置2使用的资源与所述第一系统管理装置1使用的资源（通过硬件机制或软件机制的方式）相隔离。

优选地，在本发明所公开的用于安全性信息交互的设备中，所述第二系统管理装置2能够为属于不同的服务提供方的安全性应用提供单独的安全模式下的运行环境。

优选地，在本发明所公开的用于安全性信息交互的设备中，所述统一的接口协议包括安全管理层、命令交互层以及物理驱动层，所述安全管理层用于针对不同的安全部件执行相应的安全性操作，所述命令交互层用于按照不同的数据传输协议执行安全性应用与相应的安全部件之间的数据通信，所述物理驱动层用于在物理上实际驱动所述不同类型的安全部件。

优选地，在本发明所公开的用于安全性信息交互的设备中，所述安全管理层所执行的安全性操作包括下列中的一个或多个：安全部件访问权限控制（例如，设置各个安全部件的访问权限要求）、安全部件识别（例如，识别新连接的安全部件并记录其所支持的功能和相关的参数，以及为其分配设备名）、维护当前所使用的密钥、提供并维护安全性应用与相应的安全部件之间的安全通道（例如，在所述安全通道内，数据被加密）。

优选地，在本发明所公开的用于安全性信息交互的设备中，所述第二系统管理装置2管理并维护安全部件列表，所述安全部件列表记录当前与用于安全性信息交互的设备相连接的每个安全部件的属性信息，所述属性信息包括安全部件名、安全部件标识符（ID）以及该安全部件所支持的功能。

优选地，在本发明所公开的用于安全性信息交互的设备中，当新的安全部件被连接到所述用于安全性信息交互的设备上时，所述第二系统管理装置2能够通过向所述新的安全部件发送识别命令的方式而从所述新的安全部件获取该安全部件的属性信息（例如，设备名、所支持的功能、能力信息等等），并将所述属性信息记录在所述安全部件列表中，以及为所述新的安全部件分配安全部件标识符（ID）。

优选地，在本发明所公开的用于安全性信息交互的设备中，所述第二系统管理装置2能够通过所述统一的接口协议对安全部件执行如下操作：打开安全部件操作（例如，其主要包括如下操作：在操作安全部件时向安全性应用提供操作标识，用于在多个安全性应用同时操作安全部件情况下识别各个安全性应用所对应的操作流程，以及保证各个操作流互相独立，其中，在安全部件被首次操作时，需激活该安全部件并且初始化该安全部件的各项参数，并根据该安全部件自身的需求返回结果数据）、安全部件读/写操作（其中，具体的读写操作过程与安全部件所提供的功能相关，例如，针对SIM卡形式的安全部件，可以通过该操作发送选择应用命令、读取应用相关数据命令等等）、安全部件查询操作（例如，查询安全部件对应的各项参数，例如，针对SIM卡形式的安全部件，可以查询相关的波特率、其所支持的应用协议等等参数）、关闭安全部件操作（例如，关闭针对目标安全部件的操作流，或者对目标安全部件进行睡眠甚至失效处理）。

示例性地，在本发明所公开的用于安全性信息交互的设备中，所述安全部件是下列中的一个或多个：安全单元（SE）、NFC 模块、生物识别模块、虚拟的安全运行环境、协处理器等等。

由上可见，本发明所公开的用于安全性信息交互的设备具有下列优点：由于能够使用统一的接口协议管理不同类型的安全部件，由此具有高度的安全性以及广泛的适用性，并且复杂度较低，从而能够从根本上防止安全信息被窥探和篡改的潜在风险。

如图1所示，本发明公开了一种安全部件管理装置，所述安全部件管理装置能够为安全性应用（即对安全性要求较高的应用，例如金融领域中的支付应用）提供安全模式下的运行环境，以执行安全性信息交互过程，其中，所述安

全部件管理装置通过统一的接口协议管理不同类型的安全部件。

优选地，本发明所公开的安全部件管理装置能够为属于不同的服务提供方的安全性应用提供单独的安全模式下的运行环境。

5 优选地，在本发明所公开的安全部件管理装置中，所述统一的接口协议包括安全管理层、命令交互层以及物理驱动层，所述安全管理层用于针对不同的安全部件执行相应的安全性操作，所述命令交互层用于按照不同的数据传输协议执行安全性应用与相应的安全部件之间的数据通信，所述物理驱动层用于在物理上实际驱动所述不同类型的安全部件。

10 优选地，在本发明所公开的安全部件管理装置中，所述安全管理层所执行的安全性操作包括下列中的一个或多个：安全部件访问权限控制（例如，设置各个安全部件的访问权限要求）、安全部件识别（例如，识别新连接的安全部件并记录其所支持的功能和相关的参数，以及为其分配设备名）、维护当前所使用的密钥、提供并维护安全性应用与相应的安全部件之间的安全通道（例如，在所述安全通道内，数据被加密）。

15 优选地，本发明所公开的安全部件管理装置管理并维护安全部件列表，所述安全部件列表记录当前与用于安全性信息交互的设备相连接的每个安全部件的属性信息，所述属性信息包括安全部件名、安全部件标识符（ID）以及该安全部件所支持的功能。

20 优选地，当新的安全部件被连接时，本发明所公开的安全部件管理装置能够通过向所述新的安全部件发送识别命令的方式而从所述新的安全部件获取该安全部件的属性信息（例如，设备名、所支持的功能、能力信息等等），并将所述属性信息记录在所述安全部件列表中，以及为所述新的安全部件分配安全部件标识符（ID）。

25 优选地，本发明所公开的安全部件管理装置能够通过所述统一的接口协议对安全部件执行如下操作：打开安全部件操作（例如，其主要包括如下操作：在操作安全部件时向安全性应用提供操作标识，用于在多个安全性应用同时操作安全部件情况下识别各个安全性应用所对应的操作流程，以及保证各个操作流程互相独立，其中，在安全部件被首次操作时，需激活该安全部件并且初始化该安全部件的各项参数，并根据该安全部件自身的需求返回结果数据）、安全

部件读/写操作（其中，具体的读写操作过程与安全部件所提供的功能相关，例如，针对 SIM 卡形式的安全部件，可以通过该操作发送选择应用命令、读取应用相关数据命令等等）、安全部件查询操作（例如，查询安全部件对应的各项参数，例如，针对 SIM 卡形式的安全部件，可以查询相关的波特率、其所支持的
5 应用协议等等参数）、关闭安全部件操作（例如，关闭针对目标安全部件的操作流，或者对目标安全部件进行睡眠甚至失效处理）。

示例性地，在本发明所公开的安全部件管理装置中，所述安全部件是下列中的一个或多个：安全单元（SE）、NFC 模块、生物识别模块、虚拟的安全运行环境、协处理器等等。

10 由上可见，本发明所公开的安全部件管理装置具有下列优点：由于能够使用统一的接口协议管理不同类型的安全部件，由此具有高度的安全性以及广泛的适用性，并且复杂度较低，从而能够从根本上防止安全信息被窥探和篡改的潜在风险。

15 尽管本发明是通过上述的优选实施方式进行描述的，但是其实现形式并不局限于上述的实施方式。应该认识到：在不脱离本发明主旨和范围的情况下，本领域技术人员可以对本发明做出不同的变化和修改。

20

25

权利要求

1. 一种安全部件管理装置，所述安全部件管理装置能够为安全性应用提供安全模式下的运行环境，以执行安全性信息交互过程，其中，所述安全部件管理装置通过统一的接口协议管理不同类型的安全部件。

2. 根据权利要求1所述的安全部件管理装置，其特征在于，所述安全部件管理装置能够为属于不同的服务提供方的安全性应用提供单独的安全模式下的运行环境。

3. 根据权利要求2所述的安全部件管理装置，其特征在于，所述统一的接口协议包括安全管理层、命令交互层以及物理驱动层，所述安全管理层用于针对不同的安全部件执行相应的安全性操作，所述命令交互层用于按照不同的数据传输协议执行安全性应用与相应的安全部件之间的数据通信，所述物理驱动层用于在物理上实际驱动所述不同类型的安全部件。

4. 根据权利要求3所述的安全部件管理装置，其特征在于，所述安全管理层所执行的安全性操作包括下列中的一个或多个：安全部件访问权限控制、安全部件识别、维护当前所使用的密钥、提供并维护安全性应用与相应的安全部件之间的安全通道。

5. 根据权利要求4所述的安全部件管理装置，其特征在于，所述安全部件管理装置管理并维护安全部件列表，所述安全部件列表记录当前与用于安全性信息交互的设备相连接的每个安全部件的属性信息，所述属性信息包括安全部件名、安全部件标识符以及该安全部件所支持的功能。

6. 根据权利要求5所述的安全部件管理装置，其特征在于，当新的安全部件被连接时，所述安全部件管理装置能够通过向所述新的安全部件发送识别命令的方式而从所述新的安全部件获取该安全部件的属性信息，并将所述属性信息记录在所述安全部件列表中，以及为所述新的安全部件分配安全部件标识符。

7. 根据权利要求6所述的安全部件管理装置，其特征在于，所述安

全部件管理装置能够通过所述统一的接口协议对安全部件执行如下操作：打开安全部件操作、安全部件读/写操作、安全部件查询操作、关闭安全部件操作。

8. 一种用于安全性信息交互的设备，所述用于安全性信息交互的设备包括：

第一系统管理装置，所述第一系统管理装置为常规的应用提供运行环境；

第二系统管理装置，所述第二系统管理装置为安全性应用提供安全模式下的运行环境，以执行安全性信息交互过程，

10 其中，在当前待运行的应用是常规的应用的情况下，所述用于安全性信息交互的设备将所述第一系统管理装置作为当前使用的系统管理装置，而在当前待运行的应用是安全性应用的情况下，所述用于安全性信息交互的设备将所述第二系统管理装置作为当前使用的系统管理装置，

15 并且其中，所述第二系统管理装置通过统一的接口协议管理不同类型的安全部件。

9. 根据权利要求8所述的用于安全性信息交互的设备，其特征在于，所述第二系统管理装置使用的资源与所述第一系统管理装置使用的资源相隔离。

10. 根据权利要求9所述的用于安全性信息交互的设备，其特征在于，20 所述第二系统管理装置能够为属于不同的服务提供方的安全性应用提供单独的安全模式下的运行环境。

11. 根据权利要求10所述的用于安全性信息交互的设备，其特征在于，所述统一的接口协议包括安全管理层、命令交互层以及物理驱动层，所述安全管理层用于针对不同的安全部件执行相应的安全性操作，所述命令交互层用于按照不同的数据传输协议执行安全性应用与相应的安全部件之间的数据通信，所述物理驱动层用于在物理上实际驱动所述不同类型的25 安全部件。

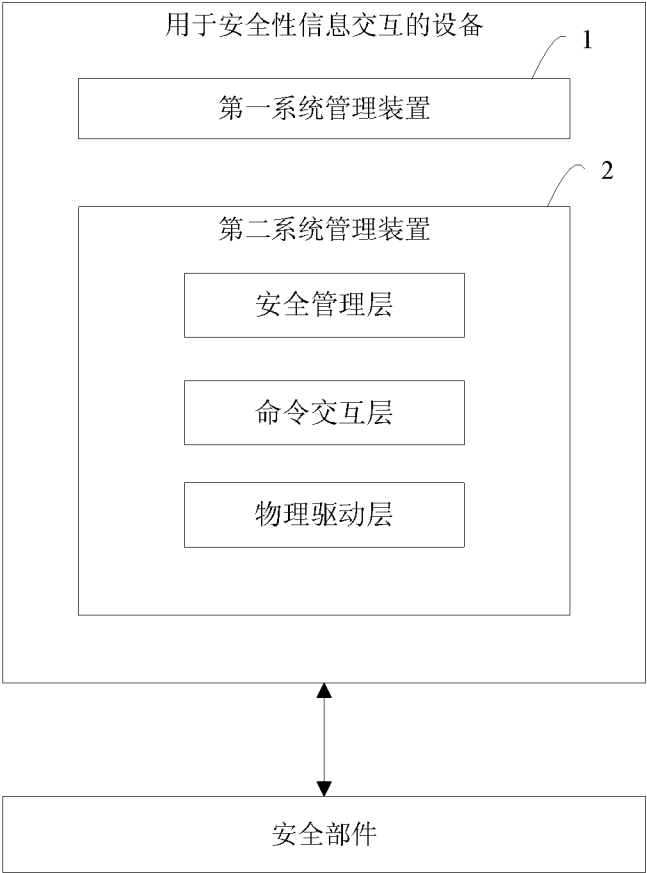


图 1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2014/095272

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/12 (2013.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F; H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS, CNTXT, CNKI, VEN: security, component, assembly, module, unit, management, information, exchange, multiple, different, type, uniform, interface, protocol, mode, environment, NFC, SE, SIM, security, secure, secured, element, module, component, unit, management, assembly, manag+, application

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 103164260 A (CHINA UNIONPAY JOINT CO LTD) 19 June 2013 (19.06.2013) description, paragraphs [0007]-[0029]	1-11
Y	CN 102346669 A (UNIV CHONGQING POSTS & TELECOM et al.) 08 February 2012 (08.02.2012) description, paragraphs [0002]-[0005], [0020]-[0030] and figures 1-3	1-11
A	CN 101452397 A (UNIV SHANGHAI JIAOTONG) 10 June 2009 (10.06.2009) the whole document	1-11
A	CN 102314373 A (LI, Peng) 11 January 2012 (11.01.2012) the whole document	1-11
A	MA, Hualiu Function and Implementation of Common Security Services Manager (CSSM). Computer & Digital Engineering. volume 30, issue 01, 20 February 2002 (20.02.2002), pages 60-62	1-11

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 25 March 2015	Date of mailing of the international search report 08 April 2015
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer WANG, Yue Telephone No. (86-10) 62089109

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/CN2014/095272

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103164260 A	19 June 2013	None	
CN 102346669 A	8 February 2012	CN 102346669 B	15 October 2014
CN 101452397 A	10 June 2009	CN 101452397 B	22 August 2012
CN 102314373 A	11 January 2012	CN 102314373 B	18 December 2013

A. 主题的分类 G06F 21/12 (2013.01) i 按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类		
B. 检索领域 检索的最低限度文献 (标明分类系统和分类号) G06F; H04L 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用)) CNABS, CNTXT, CNKI, VEN: 安全, 部件, 组件, 模块, 单元, 管理, 信息, 交互, 多, 不同, 类, 统一, 接口, 协议, 模式, 环境, NFC, SE, SIM, security, secure, secured, element, module, component, unit, management, assembly, manag+, application		
C. 相关文件		
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
Y	CN 103164260 A (中国银联股份有限公司) 2013年 6月 19日 (2013 - 06 - 19) 说明书第[0007]-[0029]段	1-11
Y	CN 102346669 A (重庆邮电大学 等) 2012年 2月 8日 (2012 - 02 - 08) 说明书第[0002]-[0005], [0020]-[0030]段、图1-3	1-11
A	CN 101452397 A (上海交通大学) 2009年 6月 10日 (2009 - 06 - 10) 全文	1-11
A	CN 102314373 A (李鹏) 2012年 1月 11日 (2012 - 01 - 11) 全文	1-11
Y	马骅骝. "安全服务管理层 (CSSM) 的功能和实现" 计算机与数字工程, 第30卷卷, 第01期期, 2002年 2月 20日 (2002 - 02 - 20), 第60-62页	1-11
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。		
* 引用文件的具体类型: "A" 认为不特别相关的表示了现有技术一般状态的文件 "E" 在国际申请日的当天或之后公布的在先申请或专利 "L" 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的) "O" 涉及口头公开、使用、展览或其他方式公开的文件 "P" 公布日先于国际申请日但迟于所要求的优先权日的文件 "T" 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 "X" 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 "Y" 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 "&" 同族专利的文件		
国际检索实际完成的日期 2015年 3月 25日		国际检索报告邮寄日期 2015年 4月 8日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局 (ISA/CN) 北京市海淀区蓟门桥西土城路6号 100088 中国 传真号 (86-10)62019451		授权官员 王越 电话号码 (86-10)62089109

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2014/095272

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	103164260	A	2013年 6月 19日	无			
CN	102346669	A	2012年 2月 8日	CN	102346669	B	2014年 10月 15日
CN	101452397	A	2009年 6月 10日	CN	101452397	B	2012年 8月 22日
CN	102314373	A	2012年 1月 11日	CN	102314373	B	2013年 12月 18日