(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
2017 年 5 月 26 日 (26.05.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/084569 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01) *H04L 9/32* (2006.01)

(21) 国际申请号: PCT/CN2016/106009

(22) 国际申请日: 2016 年 11 月 16 日 (16.11.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510799005.X 2015 年 11 月 19 日 (19.11.2015) CN

(71) 申请人: **中国银联股份有限公司 (CHINA UNIONPAY 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: **褚红梅 (CHU, Hongmei)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 **才华 (CAI, Hua)**; 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, DJ, 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, KW, 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, 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))。

(54) Title: METHOD FOR ACQUIRING LOGIN CREDENTIAL IN SMART TERMINAL, SMART TERMINAL, AND OPERATING SYSTEMS

(54) 发明名称 : 在智能终端中获取登陆凭证的方法、智能终端以及操作系统

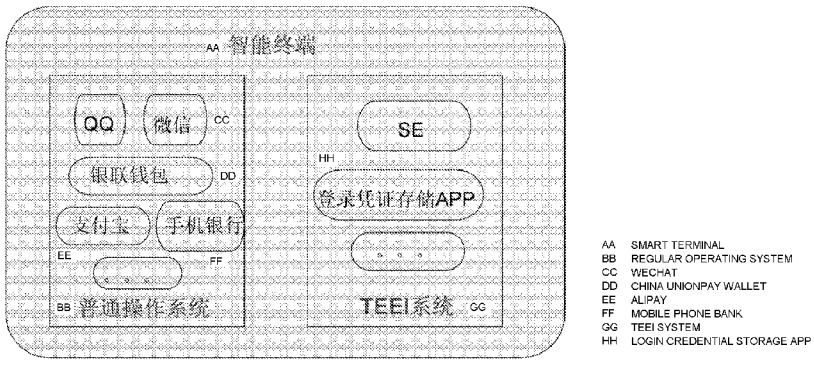

图 1

(57) **Abstract**: Disclosed is a method for acquiring a login credential in a smart terminal. The smart terminal comprises, running thereon, a first operating system and a second operating system, where the second operating system is provided with a security level higher than that of the first operating system. The method comprises: a user selects an application that needs to be used in the first operating system of the smart terminal, the application prompts the user either to enter a login credential or to log in automatically; when the user chooses to log in automatically, the first operating system launches a call request with respect to a login credential of the application to the second operating system; the second operating system verifies user identity and searches for the requested login credential on the basis of the call request; and the second operating system returns the login credential to the first operating system. Also disclosed are the smart terminal and the operating systems running on the smart terminal.

(57) 摘要:

[见续页]

WO 2017/084569 A1

本申请公开了一种在智能终端中获取登陆凭证的方法，所述智能终端包括运行于其上的第一操作系统和第二操作系统，其中所述第二操作系统具有比所述第一操作系统更高的安全级别，所述方法包括：用户在所述智能终端的第一操作系统中选择需要使用的应用，所述应用提示用户输入登陆凭证或自动录入；在用户选择自动录入后，所述第一操作系统向所述第二操作系统发起对所述应用的登陆凭证的调用请求；基于所述调用请求，所述第二操作系统验证用户身份并检索所请求的登陆凭证；以及所述第二操作系统向所述第一操作系统返回所述登陆凭证。本申请还公开了一种智能终端以及运行于智能终端上的操作系统。

在智能终端中获取登陆凭证的方法、智能终端以及操作系统

技术领域

[0001] 本发明涉及在智能终端中获取登陆凭证的方法、智能终端以及操作系统。

背景技术

[0002] 目前在智能终端上存在多种即时通讯类应用，如微信、QQ、邮箱等。一般而言，该类应用允许用户自动保存登录密码。用户为了省事，通常会选择这种自动保存免输入的方式。但是，这也带来一些问题，例如在安装有这些应用的移动终端遗失时，用户的隐私可能会泄露。甚至，在网络支付日益发展的今天，例如黑客容易通过各种技术手段攻破普通手机操作系统，从而获取用户的支付密码等敏感信息，从而造成用户财产的损失。

[0003] 因此，需要一种既能避免用户输入登陆凭证(如密码等)，同时又能保证较高安全性的方法和系统。

发明内容

[0004] 为了解决上述问题，本申请提供了一种在智能终端中获取登陆凭证的方法，所述智能终端包括运行于其上的第一操作系统和第二操作系统，其中所述第二操作系统具有比所述第一操作系统更高的安全级别，所述方法包括：用户在所述智能终端的第一操作系统中选择需要使用的应用，所述应用提示用户输入登陆凭证或自动录入；在用户选择自动录入后，所述第一操作系统向所述第二操作系统发起对所述应用的登陆凭证的调用请求；基于所述调用请求，所述第二操作系统验证用户身份并检索所请求的登陆凭证；以及所述第二操作系统向所述第一操作系统返回所述登陆凭证。

[0005] 上述方法还可包括：在注册阶段，用户预先在所述第二操作系统中建立所述第一操作系统中的一个或多个应用的主键与一个或多个登陆凭证之间的对应关系。

[0006] 在上述方法中，所述对应关系存储在所述第二操作系统内的一特定应用中。

[0007] 在上述方法中，所述调用请求包含需要使用的应用的主键以及用于验证用户身份的信息。

[0008] 在上述方法中，所述用于验证用户身份的信息包含指纹、虹膜以及数字密码中的一个或多个。

[0009] 上述方法还可包括：所述第一操作系统自动录入所述第二操作系统所反馈的所述登陆凭证，其中所述登陆凭证由所述第一操作系统的应用的后台系统进一步验证。

[0010] 上述方法还可包括：在退出所述应用之后或在所述登陆凭证的录入以及验证成功之后，所述第一操作系统自动清除所述登陆凭证。

[0011] 在上述方法中，所述第一操作系统为普通操作系统，而所述第二操作系统为 **TEEI** 操作系统。

[0012] 在上述方法中，所述普通操作系统为安卓操作系统或 **iOS** 操作系统。

[0013] 根据本申请的另一个方面，提供了一种智能终端。该智能终端包括：运行于所述智能终端上的第一操作系统，所述第一操作系统包括一个或多个应用；以及运行于所述智能终端上的第二操作系统，所述第二操作系统包括一个或多个应用，其中所述第二操作系统具有比所述第一操作系统更高的安全级别，以及其中，所述第二操作系统还配置成为所述第一操作系统中的一个或多个应用提供登陆凭证的存储空间。

[0014] 在上述智能终端中，所述第一操作系统向所述第二操作系统发起对所述应用的登陆凭证的调用请求；基于所述调用请求，所述第二操作系统验证用户身份并检索所请求的登陆凭证；以及所述第二操作系统向所述第一操作系统返回所述登陆凭证。

[0015] 在上述智能终端中，所述第二操作系统预先配置有所述第一操作系统中的一个或多个应用的主键与一个或多个登陆凭证之间的对应关系。

[0016] 在上述智能终端中，所述对应关系存储在所述第二操作系统的一特定应用中。

[0017] 在上述智能终端中，所述调用请求包含需要使用的应用的主键以及用于验

证用户身份的信息。

[0018] 在上述智能终端中，所述用于验证用户身份的信息包含但不限于指纹、虹膜以及数字密码中的一个或多个。

[0019] 在上述智能终端中，所述第一操作系统配置成自动录入所述第二操作系统所反馈的所述登陆凭证，其中所述登陆凭证由所述第一操作系统的应用的后台系统进一步验证。

[0020] 在上述智能终端中，所述第一操作系统配置成在退出所述应用之后或在所述登陆凭证的录入以及验证成功之后，自动清除所述登陆凭证。

[0021] 在上述智能终端中，所述第一操作系统为普通操作系统，而所述第二操作系统为 **TEEI** 操作系统。

[0022] 在上述智能终端中，所述普通操作系统为安卓操作系统或 **iOS** 操作系统。

[0023] 根据本申请的另一个方面，提供了一种安装于智能终端上的第二操作系统，所述操作系统配置成为运行于所述智能终端的另一个操作系统上的一个或多个应用提供登陆凭证的存储空间。

[0024] 按照本申请的方案，通过第二操作系统为第一操作系统中的各类 **APP** 应用提供了登陆凭证的存放容器，避免了用户记忆多个凭证的烦恼。另外，当前用户避免每次使用时都输入登录凭证，直接将登录凭证保存，虽然不需要用户操作，但是如果移动终端丢失或借用，很不安全。通过第二操作系统存储各类登录凭证，并在用户有登陆需求并身份识别通过后，自动检索和自动填写，也可以起到相应的效果，但是安全级别更高。上面所说的身份识别可以是用户触发“自动登录”时，自动获取到用户的指纹等生物识别信息，并在后台验证，不会影响用户的使用体验。此外，如果移动终端丢失或替换移动终端后，只需要在新的移动终端上用注册时的账号登陆即可下载所有已存储的登录凭证，原来终端上的登录凭证存储 **APP** 会被更新。

附图说明

[0025] 在参照附图阅读了本发明的具体实施方式以后，本领域技术人员将会更清楚地了解本发明的各个方面。本领域技术人员应当理解的是：这些附图仅仅用于配合具体实施方式说明本发明的技术方案，而并非意在对本发明的保护范围构成限制。

[0026] 图 1 是根据本申请的一个实施例的智能终端的示意图。

具体实施方式

[0027] 下面介绍的是本发明的多个可能实施例中的一些，旨在提供对本发明的基本了解，并不旨在确认本发明的关键或决定性的要素或限定所要保护的范围。容易理解，根据本发明的技术方案，在不变更本发明的实质精神下，本领域的一般技术人员可以提出可相互替换的其它实现方式。因此，以下具体实施方式以及附图仅是对本发明的技术方案的示例性说明，而不应当视为本发明的全部或者视为对本发明技术方案的限定或限制。

[0028] 银联开发的 TEEI(Trusted Executive Environment Integration 可信执行环境集成)系统是一个安全级别较高的操作系统。现在的安卓、iOS 系统很容易被黑客攻破，而攻破的一种主要方式就是截屏。比如按密码，黑客一旦进入正在操作的系统，使用者按在哪个位置、这个位置对应哪个数字就会被截取，如果终端上有 TEEI 系统，这些步骤将在 TEEI 系统里进行，黑客即使攻破安卓或 iOS 系统也没关系。而就 TEEI 系统本身的安全性而言，尽管没有一个系统是 100%安全的，但相对而言，“根 key”(根证书密钥文件)是最安全的，TEEI 系统就是一种根 key，其安全性比安卓与 iOS 系统都要高。

[0029] 图 1 是根据本申请的一个实施例的智能终端的示意图。该智能终端包括运行于所述智能终端上的第一操作系统，所述第一操作系统包括一个或多个应用(如 QQ、微信、银联钱包、支付宝、手机银行等应用)。如图 1 所示，该第一操作系统为普通操作系统，包括但不限于安卓操作系统和 iOS 操作系统。除了第一操作系统之外，该智能终端还包括第二操作系统，所述第二操作系统也包括一个或多个应用。在图 1 中，该第二操作系统为安全级别更高的 TEEI 系统，该 TEEI 系统包括登陆凭证存储应用，该应用配置成为普通操作系统中的一个或多个应用(例如银联钱包、支付宝、手机银行等)提供登陆凭证的存储空间。

[0030] 由于将一些重要的登陆凭证存储在本申请的智能终端安全级别较高的 TEEI 操作系统中，所以即使黑客攻破手机的普通操作系统也无法获取支付密码等敏感信息。

[0031] 根据本申请的一个实施例，智能终端的普通操作系统安装有各类 APP 应用，如需要实时身份验证的即时通讯类 APP、各类钱包 APP、手机银行 APP、

邮箱等。该普通操作系统配置成根据各类即时通讯应用的登陆请求，与 TEEI 操作系统交互，获取对应的登陆凭证。在一个实施例中，该普通操作系统配置成将 TEEI 操作系统反馈的登录凭证自动登陆。在一个实施例中，该普通操作系统配置成在登陆成功后及时删除，防止被恶意程序获取。

[0032] 根据本申请的一个实施例，第二操作系统(例如，TEEI 操作系统)配置成为各类安全级别较高的应用提供存储容器，包括但不限于 SE、登陆凭证存储 APP 等。

[0033] 根据本申请的一个实施例，登陆凭证存储 APP 可安装在 TEEI 操作系统上，并存储各类实时身份识别应用的登陆凭证。在一个实施例中，用户获取使用权限后，登陆凭证存储 APP 应用可根据普通操作系统提供的主键，检索对应的登录凭证，并将其反馈给普通操作系统。

[0034] 根据本申请的一个方面，提供了具体的业务流程。该业务流程可包括存储登录凭证、自动填写两个过程，具体如下：

(一) 注册并存储登陆凭证

1、 用户启动登录凭证存储 APP，并根据提示注册账户信息，此时该 APP 可获取移动设备的唯一识别号；

2、 用户根据系统情况，设置使用登录凭证存储 APP 的权限；

3、 在登录凭证存储 APP 中，输入并存储各类 APP 应用的登陆凭证，建立各类 APP 主键与登陆凭证的对应关系。

[0035] 需要指出的是，上述注册并存储登陆凭证的具体过程仅用作示例，而不是要对本发明进行限制。有必要指出的是，如果普通操作系统调用 TEEI 操作系统时，需要身份识别，那么调用登录凭证存储 APP 时可不需要身份识别。还需要指出的是，注册并存储各登录凭证后，后台系统可将账户信息、唯一识别号、各类 APP 主键与登陆凭证建立对应关系。在一个实施例中，为了使用效果，可将各类 APP 主键与登陆凭证之间的对应关系存放在 TEEI 操作系统中。在一个实施例中，每次调用登录凭证存储 APP 时，通过生物识别方法即可，不再需要输入注册账户信息。在一个实施例中，如果移动终端丢失或替换移动终端后，只需要在新的移动终端上用注册时的账号登陆即可下载所有已存储的登录凭证，原来终端上的登录凭证存储 APP 被更新。

[0036] (二) 自动填写过程

1、 用户在智能终端上选择需要使用的 APP 应用；

2、 APP 应用提示用户输入登陆凭证或自动录入；

3、 用户选择自动录入后，普通操作系统发起调用 TEEI 操作系统之下的登录凭证存储 APP 的请求(简称获取登录凭证的请求)，请求中包括需登录使用的 APP 主键，以及第 4 步操作所需要的验证信息(如指纹)等；

4、 TEEI 操作系统收到请求后，验证用户身份，如通过指纹、虹膜或数字密码等方式验证；

5、 验证通过后，TEEI 操作系统将获取登录凭证的请求发送给登录凭证存储 APP；

6、 登录凭证存储 APP 根据获取登录凭证的请求中的主键等信息检索对应的登录凭证；

7、 登录凭证存储 APP 将检索到的登录凭证反馈给普通操作系统；

8、 普通操作系统自动录入并由 APP 应用后台系统验证；

9、 当用户终止使用 APP 应用时，自动清除登录凭证；如果系统允许，也可在录入并验证成功后，系统自动清除登录凭证防止被不法程序获取。

[0037] 上述流程一方面通过 APP 应用凡用必验身份的措施，满足用户的安全需求，另一方面通过自动检索和自动填写的方式，减少用户的输入操作，提升了用户的使用体验。此外，在调用 TEEI 操作系统下的应用程序时，也通过必要的身份验证方式保证了使用的安全性，即使移动终端被丢失或借用，也不必担心其他人看到隐私信息。

[0038] 上述方案可从以下几方面确保支付的安全性：

(1) 采用安全访问控制措施，用户只有通过身份验证后，才可调用 TEEI 操作系统之下的登录凭证存储 APP；

(2) 将登录凭证存储 APP 放置在 TEEI 操作系统下，有效隔离了不法程序的恶意攻击。

[0039] 在一个实施例中，用户通过登录凭证存储 APP 应用来存储各类需要实时身份验证的 APP 的登陆凭证。当用户在智能终端上选择使用 APP 时，普通操作系统会将获取登陆凭证的请求发送给 TEEI 操作系统之下的登录凭证存储 APP，

登录凭证存储 APP 自动检索到对应的登录凭证后返回普通操作系统后，在用户无感知的情况下自动录入该登陆凭证。在该方案中，表面上用户只需触发需要使用的 APP 即可，不需要输入任何信息，即可自动录入已存储的对应的登录凭证。事实上，智能终端的后台在调用登录凭证存储 APP 获取登陆凭证时会通过指纹等便捷方式进行身份验证，在保证用户使用体验的同时，也保证了使用的安全性。

[0040] 上文中，参照附图描述了本发明的具体实施方式。但是，本领域中的普通技术人员能够理解，在不偏离本发明的精神和范围的情况下，还可以对本发明的具体实施方式作各种变更和替换。这些变更和替换都落在本发明权利要求书所限定的范围内。

权 利 要 求 书

1. 一种在智能终端中获取登陆凭证的方法，所述智能终端包括运行于其上的第一操作系统和第二操作系统，其中所述第二操作系统具有比所述第一操作系统更高的安全级别，其特征在于，所述方法包括：

用户在所述智能终端的第一操作系统中选择需要使用的应用，所述应用提示用户输入登陆凭证或自动录入；

在用户选择自动录入后，所述第一操作系统向所述第二操作系统发起对所述应用的登陆凭证的调用请求；

基于所述调用请求，所述第二操作系统验证用户身份并检索所请求的登陆凭证；以及

所述第二操作系统向所述第一操作系统返回所述登陆凭证。

2. 如权利要求 1 所述的方法，还包括：在注册阶段，用户预先在所述第二操作系统中建立所述第一操作系统中的一个或多个应用的主键与一个或多个登陆凭证之间的对应关系。

3. 如权利要求 2 所述的方法，其中，所述对应关系存储在所述第二操作系统内的一特定应用中。

4. 如权利要求 1 所述的方法，其中，所述调用请求包含需要使用的应用的主键以及用于验证用户身份的信息。

5. 如权利要求 4 所述的方法，其中，所述用于验证用户身份的信息包含但不限于指纹、虹膜以及数字密码中的一个或多个。

6. 如权利要求 1 所述的方法，还包括：所述第一操作系统自动录入所述第二操作系统所反馈的所述登陆凭证，其中所述登陆凭证由所述第一操作系统的应用的后台系统进一步验证。

7. 如权利要求 1 或 6 所述的方法，还包括：在退出所述应用之后或在所述登陆凭证的录入以及验证成功之后，所述第一操作系统自动清除所述登陆凭证。

8. 如权利要求 1 所述的方法，其中，所述第一操作系统为普通操作系统，而所述

第二操作系统为 TEEI 操作系统。

9. 如权利要求 8 所述的方法，其中，所述普通操作系统为安卓操作系统或 iOS 操作系统。

10. 一种智能终端，其特征在于，所述智能终端包括：

运行于所述智能终端上的第一操作系统，所述第一操作系统包括一个或多个应用；以及

运行于所述智能终端上的第二操作系统，所述第二操作系统包括一个或多个应用，其中所述第二操作系统具有比所述第一操作系统更高的安全级别，

其中，所述第二操作系统还配置成为所述第一操作系统中的一个或多个应用提供登陆凭证的存储空间。

11. 如权利要求 10 所述的智能终端，其中，所述第一操作系统向所述第二操作系统发起对所述应用的登陆凭证的调用请求；基于所述调用请求，所述第二操作系统验证用户身份并检索所请求的登陆凭证；以及所述第二操作系统向所述第一操作系统返回所述登陆凭证。

12. 如权利要求 10 或 11 所述的智能终端，其中，所述第二操作系统预先配置有所述第一操作系统中的一个或多个应用的主键与一个或多个登陆凭证之间的对应关系。

13. 如权利要求 12 所述的智能终端，其中，所述对应关系存储在所述第二操作系统的一特定应用中。

14. 如权利要求 11 所述的智能终端，其中，所述调用请求包含需要使用的应用的主键以及用于验证用户身份的信息。

15. 如权利要求 14 所述的智能终端，其中，所述用于验证用户身份的信息包含但不限于指纹、虹膜以及数字密码中的一个或多个。

16. 如权利要求 11 所述的智能终端，其中，所述第一操作系统配置成自动录入所述第二操作系统所反馈的所述登陆凭证，其中所述登陆凭证由所述第一操作系统的应用的后台系统进一步验证。

17. 如权利要求 11 或 16 所述的智能终端，其中，所述第一操作系统配置成在退出所述应用之后或在所述登陆凭证的录入以及验证成功之后，自动清除所述登陆凭证。

18. 如权利要求 11 所述的智能终端，其中，所述第一操作系统为普通操作系统，而所述第二操作系统为 TEEI 操作系统。

19. 如权利要求 18 所述的智能终端，其中，所述普通操作系统为安卓操作系统或 iOS 操作系统。

20. 一种安装于智能终端上的第二操作系统，其特征在于，所述操作系统配置成为运行于所述智能终端的另一个操作系统上的一个或多个应用提供登陆凭证的存储空间。

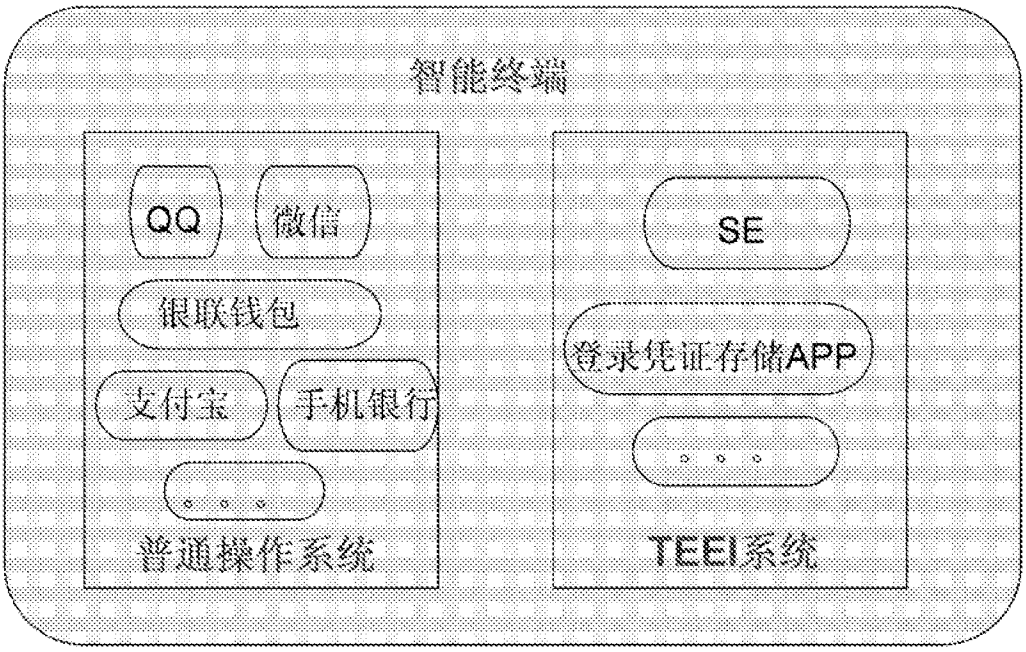

图 1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/106009

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i; H04L 9/32 (2006.01) 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)

H04L; G06F

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; DWPI; SIPOABS; WOTXT: operating system, certificate, software, procedure, first, second, one, another, two, plurality, operation, operating, system, OS, password, security, stor+, memor+, call+, obtain+, application, APP

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 105592072 A (CHINA UNIONPAY CO., LTD.), 18 May 2016 (18.05.2016), claims 1-20	1-20
X	CN 104424028 A (LENOVO (BEIJING) CO., LTD.), 18 March 2015 (18.03.2015), description, paragraphs [0030]-[0069]	1-20
A	CN 104618601 A (SHENZHEN COOLPAD TECHNOLOGIES CO., LTD.), 13 May 2015 (11.05.2015\3), the whole document	1-20
A	US 2013219192 A1 (SAMSUNG ELECTRONICS CO., LTD.), 22 August 2013 (22.08.2013), the whole document	1-20

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"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)

"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

"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

"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

"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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 January 2017 (24.01.2017)	**06 February 2017 (06.02.2017)**
Name and mailing address of the ISA/CN: 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 **LIU, Jian** Telephone No.: (86-10) **62411256**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/106009

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 105592072 A	18 May 2016	None	
CN 104424028 A	18 March 2015	None	
CN 104618601 A	13 May 2015	WO 2016123876 A1	11 August 2016
US 2013219192 A1	22 August 2013	KR 20130101632 A	16 September 2013

国际检索报告

国际申请号
PCT/CN2016/106009

A. 主题的分类

H04L 29/06(2006.01)i; H04L 9/32(2006.01)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)

H04L; G06F

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;DWPI;SIPOABS;WOTXT:第一，第二，一个，另一个，两，多，操作系统，凭证，密码，安全，存储，储存，保存，调用，获取，获得，应用，软件，程序，first，second，one，another，two，plurality，operation，operating，system，OS，password，security，stor+，memor+，call+，obtain+，application，APP

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
PX	CN 105592072 A (中国银联股份有限公司) 2016年 5月 18日 (2016-05-18) 权利要求1-20	1-20
X	CN 104424028 A (联想北京有限公司) 2015年 3月 18日 (2015-03-18) 说明书第[0030]-[0069]段	1-20
A	CN 104618601 A (深圳酷派技术有限公司) 2015年 5月 13日 (2015-05-13) 全文	1-20
A	US 2013219192 A1 (三星电子株式会社) 2013年 8月 22日 (2013-08-22) 全文	1-20

☐ 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	国际检索报告邮寄日期
2017年 1月 24日	2017年 2月 6日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	刘俭
传真号 (86-10)62019451	电话号码 (86-10)62411256

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/106009

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 105592072 A	2016年 5月 18日	无	
CN 104424028 A	2015年 3月 18日	无	
CN 104618601 A	2015年 5月 13日	WO 2016123876 A1	2016年 8月 11日
US 2013219192 A1	2013年 8月 22日	KR 20130101632 A	2013年 9月 16日