(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
2016 年 10 月 13 日 (13.10.2016)

WIPO | PCT

(10) 国际公布号
WO 2016/161968 A1

(51) 国际专利分类号:
H04L 12/24 (2006.01)

(21) 国际申请号: PCT/CN2016/078826

(22) 国际申请日: 2016 年 4 月 8 日 (08.04.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510167277.8 2015 年 4 月 10 日 (10.04.2015) 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: **李定洲 (LI, Dingzhou)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 **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)。

(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)。

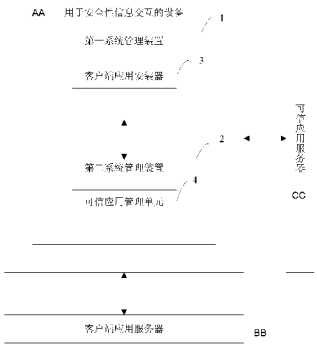
(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, 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, 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)。

[见续页]

(54) **Title**: EQUIPMENT FOR SECURITY INFORMATION INTERACTION

(54) **发明名称** : 用于安全性信息交互的设备



1 FIRST SYSTEM MANAGEMENT DEVICE
2 SECOND SYSTEM MANAGEMENT DEVICE
3 CLIENT APPLICATION INSTALLER
4 TRUSTWORTHY APPLICATION MANAGEMENT UNIT
AA EQUIPMENT FOR SECURITY INFORMATION INTERACTION
BB CLIENT APPLICATION SERVER
CC TRUSTWORTHY APPLICATION SERVER

图 1

(57) **Abstract**: Provided is an equipment for security information interaction. The equipment for security information interaction comprises a first system management device and a second system management device, wherein the first system management device provides an operating environment for a client application, the second system management device provides an operating environment under a secure mode for a trustworthy application associated with the client application, so as to execute a security information interaction process, and wherein when the client application is installed, the installation of the trustworthy application associated with the client application is triggered. The equipment for security information interaction disclosed by the present invention is convenient and efficient, has low cost and has a good compatible and maintainable application management mechanism. (FIG. 1)

(57) **摘要**: 本发明提出了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和第二系统管理装置，其中，所述第一系统管理装置为客户端应用提供运行环境，所述第二系统管理装置为与所述客户端应用相关联的可信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，并且其中，当所述客户端应用被安装时触发与其相关联的所述可信应用的安装。本发明所公开的用于安全性信息交互的设备具有方便快捷、成本较低并且具有良好的兼容性的和可维护性的应用管理机制。 (图 1)

WO 2016/161968 A1

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

技术领域

本发明涉及用于信息交互的设备，更具体地，涉及用于安全性信息交互的设备。

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）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，典型地在其中采用两个系统管理装置，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。

然而，上述现有的技术方案存在如下问题：由于安全性应用通常由客户端应用（其运行于第一系统管理装置（例如常规的多媒体操作系统）上，为用户提供操作接口）和可信应用（其运行于第二系统管理装置（例如基于可信执行环境的安全操作系统）上，以执行安全操作）组成，故通常采用将可信应用嵌入客户端应用内以打包的方式发布，然而，该方式需要改变常规的应用发布模式以及应用发布平台，并且无法实现安全环境下的可信应用的独立安装和升级。

因此，存在如下需求：提供方便快捷、成本较低并且具有良好的兼容性的和可维护性的应用管理机制的用于安全性信息交互的设备。

发明内容

为了解决上述现有技术方案所存在的问题，本发明提出了方便快捷、成本较低并且具有良好的兼容性的和可维护性的应用管理机制的用于安全性信息交互的设备。

本发明的目的是通过以下技术方案实现的:

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和第二系统管理装置,其中,所述第一系统管理装置为客户端应用提供运行环境,所述第二系统管理装置为与所述客户端应用相关联的可信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,并且其中,当所述客户端应用被安装时触发与其相关联的所述可信应用的安装。

在上面所公开的方案中,优选地,所述第一系统管理装置进一步包括客户端应用安装器,所述客户端应用安装器能够基于用户指令从客户端应用服务器下载并安装所需的客户端应用,并且所述客户端应用安装器在所述客户端应用安装完成后触发与其相关联的可信应用的安装操作。

在上面所公开的方案中,优选地,所述客户端应用安装器在所述客户端应用安装完成后以如下方式之一触发与其相关联的可信应用的安装操作:(1)从已安装的客户端应用中检测并获取关联可信应用配置信息,随之将所述关联可信应用配置信息传递到所述第二系统管理装置以触发相关的可信应用的安装操作,其中,所述关联可信应用配置信息被预先设定在所述客户端应用中,其包含与该客户端应用相关联的可信应用的下载地址信息以及该可信应用的标识符;(2)调用所述第一系统管理装置和所述第二系统管理装置之间的数据通信接口向所述第二系统管理装置发送可信应用安装请求以触发相关的可信应用的安装操作,其中,所述可信应用安装请求包含与该客户端应用相关联的可信应用的全局唯一标识符。

在上面所公开的方案中,优选地,所述第二系统管理装置包括可信应用管理单元,所述可信应用管理单元基于接收到的来自所述客户端应用安装器的关联可信应用配置信息或者可信应用安装请求而执行相关的可信应用的安装操作。

在上面所公开的方案中,优选地,当接收到所述关联可信应用配置信息后,所述可信应用管理单元解析所述关联可信应用配置信息以获取待安装的目标可信应用的下载地址信息和标识符,并随之与所述下载地址信息指示的可信应用服务器建立连接以基于所述标识符查找、下载并安装所述目标可信应用。

在上面所公开的方案中,优选地,当接收到所述可信应用安装请求后,所

述可信应用管理单元解析所述可信应用安装请求以获取待安装的目标可信应用的标识符，随之基于所述标识符检测所述目标可信应用是否已安装并运行在所述第二系统管理装置上，并且如果所述目标可信应用没有被安装，则与预先设定的可信应用服务器建立连接并基于所述标识符查找、下载并安装所述目标可信应用。

在上面所公开的方案中，优选地，所述预先设定的可信应用服务器由可信应用管理者预先配置，其具有指定的 IP 地址。

在上面所公开的方案中，优选地，所述可信应用管理单元能够独立地管理、更新和维护已安装的可信应用。

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。

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：可信应用的安装操作方便快捷，成本较低，并且可信应用的管理机制具有良好的兼容性和可维护性。

附图说明

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。

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）为客户端应用提供运行环境。所述第二系统管理装置2为与所述客户端应用相关联的可信应用（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，当所述客户端应用被安装时触发与其相关联的所述可信应用的安装。

优选地，在本发明所公开的用于安全性信息交互的设备中，所述第一系统管理装置1进一步包括客户端应用安装器3，所述客户端应用安装器3能够基于用户指令从客户端应用服务器下载并安装所需的客户端应用，并且所述客户端应用安装器3在所述客户端应用安装完成后触发与其相关联的可信应用的安装操作。

优选地，在本发明所公开的用于安全性信息交互的设备中，所述客户端应用安装器3在所述客户端应用安装完成后以如下方式之一触发与其相关联的可信应用的安装操作:（1）从已安装的客户端应用中检测并获取关联可信应用配置信息，随之将所述关联可信应用配置信息传递到所述第二系统管理装置2以触发相关的可信应用的安装操作，其中，所述关联可信应用配置信息被（例如应用设计或管理人员）预先设定在所述客户端应用中，其包含与该客户端应用相关联的可信应用的下载地址信息以及该可信应用的标识符（ID);（2）调用所述第一系统管理装置1和所述第二系统管理装置2之间的数据通信接口（API）向所述第二系统管理装置2发送可信应用安装请求以触发相关的可信应用的安装操作，其中，所述可信应用安装请求包含与该客户端应用相关联的可信应用的全局唯一标识符（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包括可信应用管理单元4，所述可信应用管理单元4基于接收到的来自所述客户端应用安装器3的关联可信应用配置信息或者可信应用安装请求而执行相关的可信应用的安装操作。

优选地，在本发明所公开的用于安全性信息交互的设备中，当接收到所述关联可信应用配置信息后，所述可信应用管理单元4解析所述关联可信应用配置信息以获取待安装的目标可信应用的下载地址信息和标识符，并随之与所述下载地址信息指示的可信应用服务器建立连接以基于所述标识符查找、下载并安装所述目标可信应用。

优选地，在本发明所公开的用于安全性信息交互的设备中，当接收到所述可信应用安装请求后，所述可信应用管理单元4解析所述可信应用安装请求以获取待安装的目标可信应用的标识符，随之基于所述标识符检测所述目标可信应用是否已安装并运行在所述第二系统管理装置2上，并且如果所述目标可信

应用没有被安装，则与预先设定的可信应用服务器建立连接并基于所述标识符查找、下载并安装所述目标可信应用。

优选地，在本发明所公开的用于安全性信息交互的设备中，所述预先设定的可信应用服务器由可信应用管理者预先配置，其具有指定的 IP 地址。

优选地，在本发明所公开的用于安全性信息交互的设备中，所述可信应用管理单元4能够独立地管理、更新和维护已安装的可信应用。

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。

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：可信应用的安装操作方便快捷，成本较低，并且可信应用的管理机制具有良好的兼容性和可维护性。

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。

权利要求

1. 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和第二系统管理装置，其中，所述第一系统管理装置为客户端应用提供运行环境，所述第二系统管理装置为与所述客户端应用相关联的可信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，并且其中，当所述客户端应用被安装时触发与其相关联的所述可信应用的安装。

2. 根据权利要求1所述的用于安全性信息交互的设备，其特征在于，所述第一系统管理装置进一步包括客户端应用安装器，所述客户端应用安装器能够基于用户指令从客户端应用服务器下载并安装所需的客户端应用，并且所述客户端应用安装器在所述客户端应用安装完成后触发与其相关联的可信应用的安装操作。

3. 根据权利要求2所述的用于安全性信息交互的设备，其特征在于，所述客户端应用安装器在所述客户端应用安装完成后以如下方式之一触发与其相关联的可信应用的安装操作：（1）从已安装的客户端应用中检测并获取关联可信应用配置信息，随之将所述关联可信应用配置信息传递到所述第二系统管理装置以触发相关的可信应用的安装操作，其中，所述关联可信应用配置信息被预先设定在所述客户端应用中，其包含与该客户端应用相关联的可信应用的下载地址信息以及该可信应用的标识符；（2）调用所述第一系统管理装置和所述第二系统管理装置之间的数据通信接口向所述第二系统管理装置发送可信应用安装请求以触发相关的可信应用的安装操作，其中，所述可信应用安装请求包含与该客户端应用相关联的可信应用的全局唯一标识符。

4. 根据权利要求3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包括可信应用管理单元，所述可信应用管理单元基于接收到的来自所述客户端应用安装器的关联可信应用配置信息或者可信应用安装请求而执行相关的可信应用的安装操作。

5. 根据权利要求4所述的用于安全性信息交互的设备，其特征在于，当接收到所述关联可信应用配置信息后，所述可信应用管理单元解析所述关联可信应用配置信息以获取待安装的目标可信应用的下载地址信息和标识符，并随之

与所述下载地址信息指示的可信应用服务器建立连接以基于所述标识符查找、下载并安装所述目标可信应用。

6. 根据权利要求5所述的用于安全性信息交互的设备，其特征在于，当接收到所述可信应用安装请求后，所述可信应用管理单元解析所述可信应用安装请求以获取待安装的目标可信应用的标识符，随之基于所述标识符检测所述目标可信应用是否已安装并运行在所述第二系统管理装置上，并且如果所述目标可信应用没有被安装，则与预先设定的可信应用服务器建立连接并基于所述标识符查找、下载并安装所述目标可信应用。

7. 根据权利要求6所述的用于安全性信息交互的设备，其特征在于，所述预先设定的可信应用服务器由可信应用管理者预先配置，其具有指定的 IP 地址。

8. 根据权利要求7所述的用于安全性信息交互的设备，其特征在于，所述可信应用管理单元能够独立地管理、更新和维护已安装的可信应用。

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。

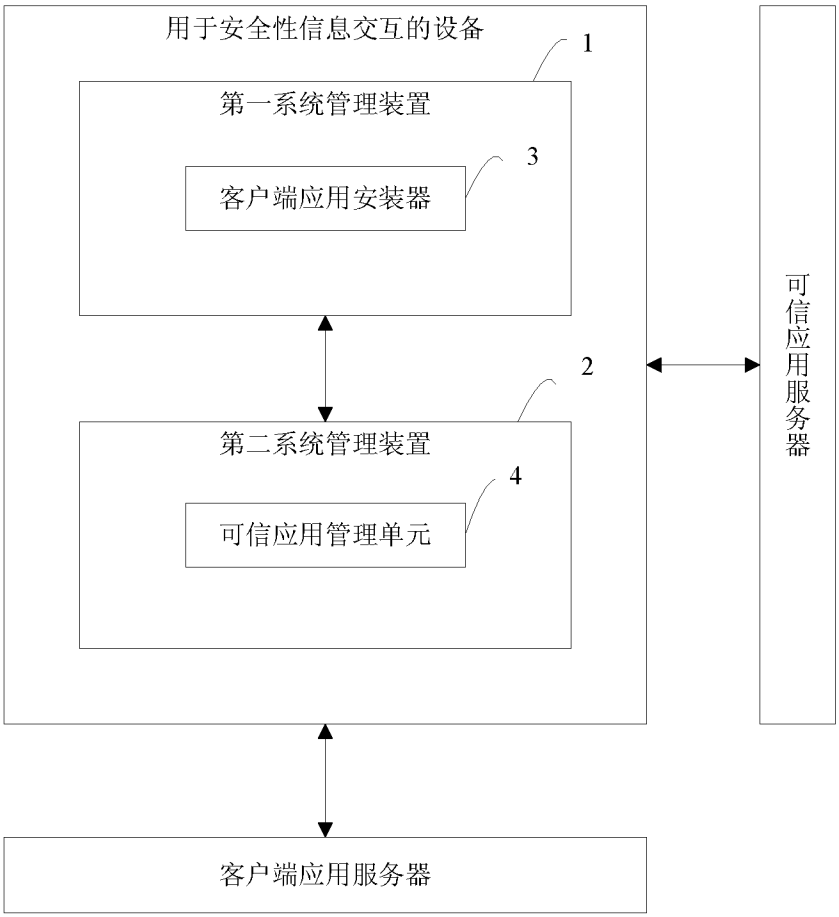

用于安全性信息交互的设备
1
第一系统管理装置
3
客户端应用安装器
2
第二系统管理装置
4
可信应用管理单元
可信应用服务器
客户端应用服务器

图 1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/078826

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/24 (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

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)

CNPAT, WPI, EPODOC, CNKI, IEEE: operating environment, operating system, client application, trustworthy application, transaction, pay, security, trust, credible, run, environment, OS, two, client, application, associate, relate, trigger, install, automatic

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 103942678 A (WUHAN TIANYU INFORMATION INDUSTRY CO., LTD.), 23 July 2014 (23.07.2014), description, paragraphs [0003]-[0041], and figure 1	1-9
Y	CN 103491080 A (EXCELSECU DATA TECHNOLOGY INC.), 01 January 2014 (01.01.2014), description, paragraphs [0056]-[0085]	1-9
A	CN 101937351 A (SURFILTER NETWORK TECHNOLOGY CO., LTD.), 05 January 2011 (05.01.2011), the whole document	1-9
A	CN 104020938 A (LENOVO (BEIJING) CO., LTD.), 03 September 2014 (03.09.2014), the whole document	1-9
A	CN 103890756 A (NOKIA SOLUTIONS AND NETWORKS OY), 25 June 2014 (25.06.2014), the whole document	1-9
A	CN 103152385 A (WANG, Yujiao), 12 June 2013 (12.06.2013), the whole document	1-9

☐ 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
13 June 2016 (13.06.2016)	**29 June 2016 (29.06.2016)**
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 **WU, Xianghui** Telephone No.: (86-10) **82245237**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/078826

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103942678 A	23 July 2014	None	
CN 103491080 A	01 January 2014	None	
CN 101937351 A	05 January 2011	None	
CN 104020938 A	03 September 2014	None	
CN 103890756 A	25 June 2014	US 2014237351 A1	21 August 2014
		WO 2013026478 A1	28 February 2013
		EP 2748722 A1	02 July 2014
		KR 20140065426 A	29 May 2014
CN 103152385 A	12 June 2013	None	

国际检索报告

国际申请号
PCT/CN2016/078826

A. 主题的分类

H04L 12/24(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

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））

CNPAT, WPI, EPODOC, CNKI, IEEE：交易，支付，安全，可信，运行环境，操作系统，两个，客户端应用，可信应用，关联，相关，触发，安装，自动，transaction, pay, security, trust, credible, run, environment, OS, two, client, application, associate, relate, trigger, install, automatic

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 103942678 A (武汉天喻信息产业股份有限公司) 2014年 7月 23日 (2014-07-23) 说明书第[0003]-[0041]段，图1	1-9
Y	CN 103491080 A (深圳市文鼎创数据科技有限公司) 2014年 1月 1日 (2014-01-01) 说明书第[0056]-[0085]段	1-9
A	CN 101937351 A (深圳市任子行网络技术股份有限公司) 2011年 1月 5日 (2011-01-05) 全文	1-9
A	CN 104020938 A (联想北京有限公司) 2014年 9月 3日 (2014-09-03) 全文	1-9
A	CN 103890756 A (诺基亚通信公司) 2014年 6月 25日 (2014-06-25) 全文	1-9
A	CN 103152385 A (王玉娇) 2013年 6月 12日 (2013-06-12) 全文	1-9

☐ 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
2016年 6月 13日	2016年 6月 29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	吴翔晖
传真号 (86-10)62019451	电话号码 (86-10)82245237

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/078826

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	103942678	A	2014年 7月 23日	无			
CN	103491080	A	2014年 1月 1日	无			
CN	101937351	A	2011年 1月 5日	无			
CN	104020938	A	2014年 9月 3日	无			
CN	103890756	A	2014年 6月 25日	US	2014237351	A1	2014年 8月 21日
				WO	2013026478	A1	2013年 2月 28日
				EP	2748722	A1	2014年 7月 2日
				KR	20140065426	A	2014年 5月 29日
CN	103152385	A	2013年 6月 12日	无			