

(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 12 月 30 日 (30.12.2015) WIPO | PCT



(10) 国际公布号
WO 2015/196665 A1

- (51) 国际专利分类号:
H04L 9/32 (2006.01)
- (21) 国际申请号: PCT/CN2014/089281
- (22) 国际申请日: 2014 年 10 月 23 日 (23.10.2014)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201410299506.7 2014 年 6 月 26 日 (26.06.2014) CN
- (71) 申请人: 小米科技有限责任公司 (XIAOMI INC.)
[CN/CN]; 中国北京市海淀区清河中街 68 号华润五彩城购物中心二期 13 层, Beijing 100085 (CN)。
- (72) 发明人: 张军 (ZHANG, Jun); 中国北京市海淀区清河中街 68 号华润五彩城购物中心二期 13 层由小米科技有限责任公司转交, Beijing 100085 (CN)。李琴 (LI, Shen); 中国北京市海淀区清河中街 68 号华润五彩城购物中心二期 13 层由小米科技有限责任公司转交, Beijing 100085 (CN)。吴廷彬 (WU, Tingbin); 中国北京市海淀区清河中街 68 号华润五彩城购物中心二期 13 层由小米科技有限责任公司转交, Beijing 100085 (CN)。
- (74) 代理人: 北京律智知识产权代理有限公司 (BEIJING INTELLIGAL INTELLECTUAL PROPERTY AGENT LTD.); 中国北京市朝阳区慧忠路 5 号远大中心 B 座 1802, 1803, 1805, Beijing 100101 (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: METHOD AND DEVICE FOR BINDING ACCOUNT NUMBER TO TOKEN KEY

(54) 发明名称: 绑定账号与令牌密钥的方法、装置

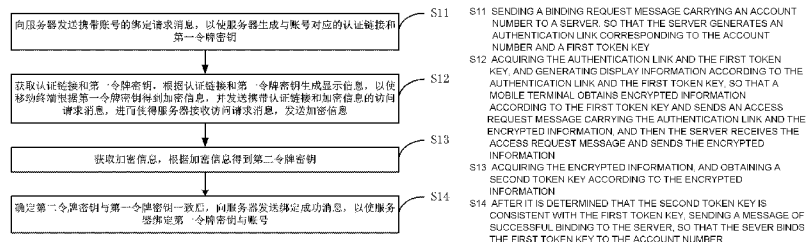


图1 / Fig. 1

(57) Abstract: The present disclosure relates to a method and device for binding an account number to a token key. The method comprises: sending a binding request message carrying an account number to a server, so that the server generates an authentication link corresponding to the account number and a first token key; acquiring the authentication link and the first token key, and generating display information according to the authentication link and the first token key, so that a mobile terminal obtains encrypted information according to the first token key and sends an access request message carrying the authentication link and the encrypted information, and then the server receives the access request message and sends the encrypted information; acquiring the encrypted information, and obtaining a second token key according to the encrypted information; and after it is determined that the second token key is consistent with the first token key, sending a message of successful binding to the server, so that the server binds the first token key to the account number. By means of the solution, a user does not need to backfill token information in the whole process, thereby reducing the complexity of user operations, and improving the user experience.

(57) 摘要: 本公开是关于一种绑定账号与令牌密钥的方法、装置, 该方法包括: 向服务器发送携带账号的绑定请求消息, 以使服务器生成与账号对应的认证链接和第一令牌密钥; 获取认证链接和第一令牌密钥, 根据认证链接和第一令牌密钥生成显示信息, 以使移动终端根据第一令牌密钥得到加密信息, 并发送携带认证链接和加密信息的访问请求消息, 进而使得服务器接收访问请求消息, 发送加密信息; 获取加密信息, 根据加密信息得到第二令牌密钥; 确定第二令牌密钥与第一令牌密钥一致后, 向服务器发送绑定成功消息, 以使服务器绑定第一令牌密钥与账号。该方案整个过程中用户无需再回填令牌信息, 从而降低了用户操作的繁琐程度, 提升了用户体验。

WO 2015/196665 A1

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

绑定账号与令牌密钥的方法、装置

本申请基于申请号为 201410299506.7、申请日为 2014 年 6 月 26 日的中国专利申请提出，并要求该中国专利申请的优先权，该中国专利申请的全部内容在此引入本申请作为参考。

技术领域

本公开涉及网络安全技术领域，尤其涉及一种绑定账号与令牌密钥的方法、装置。

10 背景技术

随着互联网技术的发展，网站提供的资源越来越丰富，有些网站可以提供免费邮箱，有些网站可以提供即时通信，有些网站可以提供视频，等等。用户若使用这些资源，需要在网页端注册账号、设置密码，注册成功后，在网页端使用账号和密码登录即可使用网站上的资源。

15 为了提高账号的安全性，很多网站推出安全认证方法，在账号登录过程中，除了使用密码外，还可以使用安全令牌。安全令牌是安装在移动终端上的应用程序，用户仅需要将服务器为账号分配的令牌密钥与账号绑定，即可在后续登录的时候使用，从而提高账号安全性。

20 发明内容

为克服相关技术中存在的问题，本公开提供一种绑定账号与令牌密钥的方法、装置。

根据本公开实施例的第一方面，提供一种绑定账号与令牌密钥的方法，包括：

向服务器发送携带账号的绑定请求消息，以使所述服务器生成与所述账号对应的认证链接和第一令牌密钥；

25 获取所述认证链接和所述第一令牌密钥，根据所述认证链接和所述第一令牌密钥生成显示信息，以使移动终端根据所述第一令牌密钥得到加密信息，并发送携带所述认证链接和所述加密信息的访问请求消息，进而使得所述服务器接收所述访问请求消息，发送所述加密信息；

获取所述加密信息，根据所述加密信息得到第二令牌密钥；

30 确定所述第二令牌密钥与所述第一令牌密钥一致后，向所述服务器发送绑定成功消息，以使所述服务器绑定所述第一令牌密钥与所述账号。

结合第一方面，在第一方面的第一种可能的实现方式中，根据所述认证链接和所述第一令牌密钥生成显示信息的步骤包括：

35 根据所述认证链接、所述第一令牌密钥和所述账号生成所述显示信息，以使所述移动终端根据所述第一令牌密钥和所述账号进行哈希运算，得到所述加密信息，或者，根据时

间戳、所述第一令牌密钥和所述账号进行哈希运算，得到所述加密信息。

根据本公开实施例的第二方面，提供一种绑定账号与令牌密钥的方法，包括：

接收网页端发送的携带账号的绑定请求消息；

生成与所述账号对应的认证链接和第一令牌密钥，以使所述网页端根据所述认证链接
5 和所述第一令牌密钥生成显示信息，进而使得移动终端根据所述第一令牌密钥得到加密信息，并发送携带所述认证链接和所述加密信息的访问请求消息；

接收所述访问请求消息，发送所述加密信息，以使所述网页端根据所述加密信息得到
第二令牌密钥，在确定所述第二令牌密钥与所述第一令牌密钥一致后，发送绑定成功消息；

接收所述绑定成功消息，绑定所述第一令牌密钥与所述账号。

10 结合第二方面，在第二方面的第一种可能的实现方式中，所述方法还包括：

建立与所述网页端的通信连接；

若在设定时长内未接收到所述移动终端发送的访问请求消息，则释放与所述网页端的
通信连接。

根据本公开实施例的第三方面，提供一种绑定账号与令牌密钥的方法，包括：

15 获取网页端的显示信息，所述显示信息是所述网页端根据服务器生成的认证链接和第一令牌密钥生成的，所述认证链接和所述第一令牌密钥是所述服务器根据所述网页端发送绑定请求消息中携带账号的生成的；

根据所述第一令牌密钥得到加密信息，并发送携带所述加密信息和所述认证链接的访问请求消息，以使所述服务器接收所述访问请求消息后，向所述网页端发送所述加密信息，
20 所述网页端根据所述加密信息得到第二令牌密钥，在确认所述第二令牌密钥与所述第一令牌密钥一致后，向所述服务器发送绑定成功消息，所述服务器接收到所述绑定成功消息后，绑定所述令牌密钥与所述账号。

结合第三方面，在第三方面的第一种可能的实现方式中，根据所述第一令牌密钥得到加密信息的步骤包括：

25 将所述第一令牌密钥作为所述加密信息；或者，

根据时间戳和所述第一令牌密钥进行哈希运算，得到所述加密信息。

结合第三方面，在第三方面的第二种可能的实现方式中，所述显示信息是所述网页端根据服务器生成的所述认证链接、所述第一令牌密钥和所述账号生成的，根据所述第一令牌密钥得到加密信息的步骤包括：

30 根据所述第一令牌密钥和所述账号进行哈希运算，得到所述加密信息；或者，
根据时间戳、所述第一令牌密钥和所述账号进行哈希运算，得到所述加密信息。

根据本公开实施例的第四方面，提供一种绑定账号与令牌密钥的装置，包括：

第一发送模块，用于向服务器发送携带账号的绑定请求消息，以使所述服务器生成与
所述账号对应的认证链接和第一令牌密钥；

35 第一获取模块，用于获取所述认证链接和所述第一令牌密钥；

第一生成模块,用于根据所述认证链接和所述第一令牌密钥生成显示信息,以使移动终端根据所述第一令牌密钥得到加密信息,并发送携带所述认证链接和所述加密信息的访问请求消息,进而使得所述服务器接收所述访问请求消息,发送所述加密信息;

第二获取模块,用于获取所述加密信息;

5 第二生成模块,用于根据所述加密信息得到第二令牌密钥;

第二发送模块,用于确定所述第二令牌密钥与所述第一令牌密钥一致后,向所述服务器发送绑定成功消息,以使所述服务器绑定所述第一令牌密钥与所述账号。

结合第四方面,在第四方面的第一种可能的实现方式中,所述第一生成模块包括:

10 生成单元,用于根据所述认证链接、所述第一令牌密钥和所述账号生成所述显示信息,以使所述移动终端根据所述第一令牌密钥和所述账号进行哈希运算,得到所述加密信息,或者,根据时间戳、所述第一令牌密钥和所述账号进行哈希运算,得到所述加密信息。

根据本公开实施例的第五方面,提供一种绑定账号与令牌密钥的装置,包括:

第一接收模块,用于接收网页端发送的携带账号的绑定请求消息;

15 生成模块,用于生成与所述账号对应的认证链接和第一令牌密钥,以使所述网页端根据所述认证链接和所述第一令牌密钥生成显示信息,进而使得移动终端根据所述第一令牌密钥得到加密信息,并发送携带所述认证链接和所述加密信息的访问请求消息;

第二接收模块,用于接收所述访问请求消息;

发送模块,用于发送所述加密信息,以使所述网页端根据所述加密信息得到第二令牌密钥,在确定所述第二令牌密钥与所述第一令牌密钥一致后,发送绑定成功消息;

20 第三接收模块,用于接收所述绑定成功消息;

绑定模块,用于绑定所述第一令牌密钥与所述账号。

结合第五方面,在第五方面的第一种可能的实现方式中,所述装置还包括:

建立模块,用于建立与所述网页端的通信连接;

25 释放模块,用于若在设定时长内未接收到所述移动终端发送的访问请求消息,则释放与所述网页端的通信连接。

根据本公开实施例的第六方面,提供一种绑定账号与令牌密钥的装置,包括:

获取模块,用于获取网页端的显示信息,所述显示信息是所述网页端根据服务器生成的认证链接和第一令牌密钥生成的,所述认证链接和所述第一令牌密钥是所述服务器根据所述网页端发送绑定请求消息中携带账号的生成的;

30 处理模块,用于根据所述第一令牌密钥得到加密信息,并发送携带所述加密信息和所述认证链接的访问请求消息,以使所述服务器接收所述访问请求消息后,向所述网页端发送所述加密信息,所述网页端根据所述加密信息得到第二令牌密钥,在确认所述第二令牌密钥与所述第一令牌密钥一致后,向所述服务器发送绑定成功消息,所述服务器接收到所述绑定成功消息后,绑定所述令牌密钥与所述账号。

35 结合第六方面,在第六方面的第一种可能的实现方式中,所述处理模块包括:

第一处理单元, 用于将所述第一令牌密钥作为所述加密信息; 或者,

第二处理单元, 用于根据时间戳和所述第一令牌密钥进行哈希运算, 得到所述加密信息。

结合第六方面, 在第六方面的第二种可能的实现方式中, 所述显示信息是所述网页端根据服务器生成的所述认证链接、所述第一令牌密钥和所述账号生成的, 所述处理模块包括:

第三处理单元, 用于根据所述第一令牌密钥和所述账号进行哈希运算, 得到所述加密信息; 或者,

10 第四处理单元, 用于根据时间戳、所述第一令牌密钥和所述账号进行哈希运算, 得到所述加密信息。

根据本公开实施例的第七方面, 提供一种网页端, 包括:

处理器;

用于存储处理器可执行指令的存储器;

其中, 所述处理器被配置为:

15 向服务器发送携带账号的绑定请求消息, 以使所述服务器生成与所述账号对应的认证链接和第一令牌密钥;

获取所述认证链接和所述第一令牌密钥, 根据所述认证链接和所述第一令牌密钥生成显示信息, 以使移动终端根据所述第一令牌密钥得到加密信息, 并发送携带所述认证链接和所述加密信息的访问请求消息, 进而使得所述服务器接收所述访问请求消息, 发送所述加密信息;

获取所述加密信息, 根据所述加密信息得到第二令牌密钥;

确定所述第二令牌密钥与所述第一令牌密钥一致后, 向所述服务器发送绑定成功消息, 以使所述服务器绑定所述第一令牌密钥与所述账号。

根据本公开实施例的第八方面, 提供一种服务器, 包括:

25 处理器;

用于存储处理器可执行指令的存储器;

其中, 所述处理器被配置为:

接收网页端发送的携带账号的绑定请求消息;

30 生成与所述账号对应的认证链接和第一令牌密钥, 以使所述网页端根据所述认证链接和所述第一令牌密钥生成显示信息, 进而使得移动终端根据所述第一令牌密钥得到加密信息, 并发送携带所述认证链接和所述加密信息的访问请求消息;

接收所述访问请求消息, 发送所述加密信息, 以使所述网页端根据所述加密信息得到第二令牌密钥, 在确定所述第二令牌密钥与所述第一令牌密钥一致后, 发送绑定成功消息;

接收所述绑定成功消息, 绑定所述第一令牌密钥与所述账号。

35 根据本公开实施例的第九方面, 提供一种移动终端, 包括:

处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器被配置为：

获取网页端的显示信息，所述显示信息是所述网页端根据服务器生成的认证链接和第一令牌密钥生成的，所述认证链接和所述第一令牌密钥是所述服务器根据所述网页端发送绑定请求消息中携带账号的生成的；

根据所述第一令牌密钥得到加密信息，并发送携带所述加密信息和所述认证链接的访问请求消息，以使所述服务器接收所述访问请求消息后，向所述网页端发送所述加密信息，所述网页端根据所述加密信息得到第二令牌密钥，在确认所述第二令牌密钥与所述第一令牌密钥一致后，向所述服务器发送绑定成功消息，所述服务器接收到所述绑定成功消息后，绑定所述令牌密钥与所述账号。

本公开的实施例提供的技术方案可以包括以下有益效果：网页端向服务器发送携带账号的绑定请求消息，以使所述服务器生成与所述账号对应的认证链接和第一令牌密钥；获取所述认证链接和所述第一令牌密钥，根据所述认证链接和所述第一令牌密钥生成显示信息，以使移动终端根据所述第一令牌密钥得到加密信息，并发送携带所述认证链接和所述加密信息的访问请求消息，进而使得所述服务器接收所述访问请求消息，发送所述加密信息；获取所述加密信息，根据所述加密信息得到第二令牌密钥；确定所述第二令牌密钥与所述第一令牌密钥一致后，向所述服务器发送绑定成功消息，以使所述服务器绑定所述第一令牌密钥与所述账号。可见，在绑定账号与令牌密钥的过程中，移动终端获取显示信息，然后根据显示信息中的第一令牌密钥生成加密信息，并进行后续流程，整个过程中用户无需再回填令牌信息，从而降低了用户操作的繁琐程度，提升了用户体验。

应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本公开。

附图说明

此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本发明的实施例，并与说明书一起用于解释本发明的原理。

图 1 是根据一示例性实施例示出的用于网页端的一种绑定账号与令牌密钥的方法的流程图。

图 2 是根据一示例性实施例示出的用于服务器的一种绑定账号与令牌密钥的方法的流程图。

图 3 是根据一示例性实施例示出的用于移动终端的一种绑定账号与令牌密钥的方法的流程图。

图 4 是根据一示例性实施例示出的一种绑定账号与令牌密钥的方法的流程图。

图 5 是根据一示例性实施例示出的与图 1 对应的绑定账号与令牌密钥的装置的框图。

图 6 是根据一示例性实施例示出的与图 2 对应的绑定账号与令牌密钥的装置的框图。

图 7 是根据一示例性实施例示出的一种绑定账号与令牌密钥的装置的框图。

图 8 是根据一示例性实施例示出的与图 3 对应的绑定账号与令牌密钥的装置的框图。

图 9 是根据一示例性实施例示出的一种移动终端的框图。

5 图 10 是根据一示例性实施例示出的一种服务器的框图。

具体实施方式

这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中
10 所描述的实施方式并不代表与本发明相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本发明的一些方面相一致的装置和方法的例子。

图 1 是根据一示例性实施例示出的一种绑定账号与令牌密钥的方法的流程图，如图 1 所示，该方法用于网页端中，包括以下步骤。

在步骤 S11 中，向服务器发送携带账号的绑定请求消息，以使服务器生成与账号对应的
15 的认证链接和第一令牌密钥。

若用户要绑定账号与令牌密钥，可以首先在移动终端上下载安全令牌，然后在网页端登录账号后，发起绑定请求消息，网页端将该绑定请求消息发送给服务器，其中，绑定请求消息中携带该账号。

服务器会根据绑定请求消息中的账号生成认证链接和第一令牌密钥，该认证链接可以是 URL（Uniform Resource Locator，统一资源定位符）等等。
20

在步骤 S12 中，获取认证链接和第一令牌密钥，根据认证链接和第一令牌密钥生成显示信息，以使移动终端根据第一令牌密钥得到加密信息，并发送携带认证链接和加密信息的访问请求消息，进而使得服务器接收访问请求消息，发送加密信息。

网页端获取服务器生成的认证链接和第一令牌密钥后，可以根据认证链接和第一令牌密钥生成显示信息，用户看到显示信息后，可以使用移动终端获取该显示信息，显示信息的类型不同，获取的方式也可能不同，下面列举两种方式进行说明。若显示信息是二维码，可以使用移动终端拍摄该二维码来获取；若显示信息是条形码，也可以使用移动终端拍摄该条形码来获取。
25

移动终端获取显示信息后，可以根据第一令牌密钥得到加密信息，然后向服务器发送携带认证链接和加密信息的访问请求消息。当服务器接收到该访问请求消息后，可以获取访问请求消息中携带的加密信息，然后发送加密信息。
30

在步骤 S13 中，获取加密信息，根据加密信息得到第二令牌密钥。

网页端获取服务器发送的加密信息后，可以根据加密信息得到第二令牌密钥。

在步骤 S14 中，确定第二令牌密钥与第一令牌密钥一致后，向服务器发送绑定成功消息，以使服务器绑定第一令牌密钥与账号。
35

判断第二令牌密钥与第一令牌密钥是否一致，若一致，则可以向服务器发送绑定成功消息，然后服务器可以绑定第一令牌密钥与账号。用户在后续登录账号时，可以同时使用密码和移动终端上保存到的第一令牌密钥，更好地实现对账号的保护。若第二令牌密钥与第一令牌密钥不一致，这有可能由于是在加密信息传输的过程中，已经被替换，这时则向服务器发送绑定失败消息，并显示，用户看到该消息后，可以重新发起绑定请求消息，再次请求进行令牌密钥与账号绑定。

从图 1 所示的流程中可以看出，在绑定账号与令牌密钥的过程中，移动终端获取显示信息，然后根据显示信息中的第一令牌密钥生成加密信息，并进行后续流程，整个过程中用户无需再回填令牌信息，从而降低了用户操作的繁琐程度，提升了用户体验。

上述 S12 中的根据认证链接和第一令牌密钥生成显示信息的步骤包括：

根据认证链接、第一令牌密钥和账号生成显示信息，以使移动终端根据第一令牌密钥和账号进行哈希运算，得到加密信息，或者，根据时间戳、第一令牌密钥和账号进行哈希运算，得到加密信息。

为了保证第一令牌密钥在网络传输中的安全性，网页端可以根据认证链接、第一令牌密钥和账号生成显示信息，这样移动终端就可以根据账号和第一令牌密钥进行哈希运算，得到加密信息；还可以根据时间戳、第一令牌密钥和账号进行哈希运算，得到加密信息。其中，时间戳可以从移动终端上获取。

相应地，服务器获取到加密信息后，转发给网页端，网页端也可以采用哈希运算对该加密信息解码，得到第二令牌密钥。

图 2 是根据一示例性实施例示出的一种绑定账号与令牌密钥的方法的流程图，如图 2 所示，该方法用于服务器中，包括以下步骤。

在步骤 S21 中，接收网页端发送的携带账号的绑定请求消息。

在步骤 S22 中，生成与账号对应的认证链接和第一令牌密钥，以使网页端根据认证链接和第一令牌密钥生成显示信息，进而使得移动终端根据第一令牌密钥得到加密信息，并发送携带认证链接和加密信息的访问请求消息。

在步骤 S23 中，接收访问请求消息，发送加密信息，以使网页端根据加密信息得到第二令牌密钥，在确定第二令牌密钥与第一令牌密钥一致后，发送绑定成功消息。

在步骤 S24 中，接收绑定成功消息，绑定第一令牌密钥与账号。

为了确保绑定可以及时完成，服务器还可以建立与网页端的通信连接，若在设定时长内未接收到移动终端发送的访问请求消息，则释放与网页端的通信连接，说明该次绑定失败，这样就可以释放网络资源，有效避免网络资源的浪费。

图 3 是根据一示例性实施例示出的一种绑定账号与令牌密钥的方法的流程图，如图 3 所示，该方法用于移动终端中，包括以下步骤。

在步骤 S31 中，获取网页端的显示信息，显示信息是网页端根据服务器生成的认证链接和第一令牌密钥生成的，认证链接和第一令牌密钥是服务器根据网页端发送绑定请求消

息中携带账号的生成的。

在步骤 S32 中, 根据第一令牌密钥得到加密信息, 并发送携带加密信息和认证链接的访问请求消息, 以使服务器接收访问请求消息后, 向网页端发送加密信息, 网页端根据加密信息得到第二令牌密钥, 在确认第二令牌密钥与第一令牌密钥一致后, 向服务器发送绑定成功消息, 服务器接收到绑定成功消息后, 绑定第一令牌密钥与账号。

若显示信息是网页端根据服务器生成的认证链接和第一令牌密钥生成的, 上述步骤 S32 根据第一令牌密钥得到加密信息包括:

将第一令牌密钥作为加密信息; 或者,

根据时间戳和第一令牌密钥进行哈希运算, 得到加密信息。

若显示信息是网页端根据服务器生成的认证链接、第一令牌密钥和账号生成的, 上述步骤 S32 根据第一令牌密钥得到加密信息的步骤包括:

根据第一令牌密钥和账号进行哈希运算, 得到加密信息; 或者,

根据时间戳、第一令牌密钥和账号进行哈希运算, 得到加密信息。

图 4 是根据一示例性实施例示出的一种绑定账号与令牌密钥的方法的流程图, 如图 4 所示, 该方法用于移动终端、网页端和服务器组成的系统中, 包括以下步骤。

在步骤 S40 中, 网页端获取携带账号的绑定请求消息后, 发送给服务器。

在步骤 S41 中, 服务器接收到绑定请求消息后, 生成与账号对应的认证链接和第一令牌密钥, 将认证链接和第一令牌密钥发送给网页端。

在步骤 S42 中, 网页端接收到认证链接和第一令牌密钥后, 根据认证链接、第一令牌密钥和账号生成二维码。

在步骤 S43 中, 移动终端获取二维码后, 根据时间戳、二维码中的第一令牌密钥和账号进行哈希运算, 得到加密信息, 向服务器发送携带认证链接和加密信息的访问请求消息。

在步骤 S44 中, 服务器接收到访问请求消息后, 将加密信息发送给网页端。

在步骤 S45 中, 网页端采用哈希运算对加密信息进行解码, 得到第二令牌密钥, 若第二令牌密钥与第一令牌密钥一致, 则向服务器发送绑定成功消息。

在步骤 S46 中, 服务器接收到绑定成功消息后, 绑定第一令牌密钥与账号。

用户在后续登录账号的过程中, 可以使用第一令牌密钥和密码进行登录, 从而有效保护账号的安全。

图 5 是根据一示例性实施例示出的一种绑定账号与令牌密钥的装置框图, 该装置对应与图 1 所示的方法。参照图 5, 该装置包括第一发送模块 51, 第一获取模块 52, 第一生成模块 53, 第二获取模块 54, 第二生成模块 55 和第二发送模块 56。

该第一发送模块 51 被配置为, 用于向服务器发送携带账号的绑定请求消息, 以使服务器生成与账号对应的认证链接和第一令牌密钥。

该第一获取模块 52 被配置为, 获取认证链接和第一令牌密钥。

该第一生成模块 53 被配置为, 根据认证链接和第一令牌密钥生成显示信息, 以使移动终端根据第一令牌密钥得到加密信息, 并发送携带认证链接和加密信息的访问请求消息, 进而使得服务器接收访问请求消息, 发送加密信息。

该第二获取模块 54 被配置为, 获取加密信息。

5 该第二生成模块 55 给配置为, 根据加密信息得到第二令牌密钥。

该第二发送模块 56 被配置为, 确定第二令牌密钥与第一令牌密钥一致后, 向服务器发送绑定成功消息, 以使服务器绑定第一令牌密钥与账号。

该第一生成模块 53 包括:

10 生成单元, 用于根据认证链接、第一令牌密钥和账号生成显示信息, 以使移动终端根据第一令牌密钥和账号进行哈希运算, 得到加密信息, 或者, 根据时间戳、第一令牌密钥和账号进行哈希运算, 得到加密信息。

图 6 是根据一示例性实施例示出的一种绑定账号与令牌密钥的装置框图, 该装置对应于图 2 所示的方法。参照图 6, 该装置包括第一接收模块 61, 生成模块 62, 第二接收模块 63, 发送模块 64, 第三接收模块 65 和绑定模块 66。

15 该第一接收模块 61 被配置为, 接收网页端发送的携带账号的绑定请求消息。

该生成模块 62 被配置为, 生成与账号对应的认证链接和第一令牌密钥, 以使网页端根据认证链接和第一令牌密钥生成显示信息, 进而使得移动终端根据第一令牌密钥得到加密信息, 并发送携带认证链接和加密信息的访问请求消息。

该第二接收模块 63 被配置为, 接收访问请求消息。

20 该发送模块 64 被配置为, 发送加密信息, 以使网页端根据加密信息得到第二令牌密钥, 在确定第二令牌密钥与第一令牌密钥一致后, 发送绑定成功消息。

该第三接收模块 65 被配置为, 接收绑定成功消息。

该绑定模块 66 被配置为, 绑定第一令牌密钥与账号。

25 图 7 是根据一示例性实施例示出的一种绑定账号与令牌密钥的装置框图, 该装置在如图 6 所示的装置的基础上还包括建立模块 67 和释放模块 68。

该建立模块 67 被配置为, 建立与网页端的通信连接。

该释放模块 68 被配置为, 若在设定时长内未接收到移动终端发送的访问请求消息, 则释放与网页端的通信连接。

30 图 8 是根据一示例性实施例示出的一种绑定账号与令牌密钥的装置框图, 该装置对应于如图 3 所示的方法。参照图 8, 该装置包括获取模块 81 和处理模块 82。

该获取模块 81 被配置为, 获取网页端的显示信息, 显示信息是网页端根据服务器生成的认证链接和第一令牌密钥生成的, 认证链接和第一令牌密钥是服务器根据网页端发送绑定请求消息中携带账号的生成的。

35 该处理模块 82 被配置为, 用于根据第一令牌密钥得到加密信息, 并发送携带加密信息和认证链接的访问请求消息, 以使服务器接收访问请求消息后, 向网页端发送加密信息,

网页端根据加密信息得到第二令牌密钥，在确认第二令牌密钥与第一令牌密钥一致后，向服务器发送绑定成功消息，服务器接收到绑定成功消息后，绑定第一令牌密钥与账号。

该处理模块 82 包括：

第一处理单元，用于将第一令牌密钥作为加密信息；或者，

5 第二处理单元，用于根据时间戳和第一令牌密钥进行哈希运算，得到加密信息。

若显示信息是网页端根据服务器生成的认证链接、第一令牌密钥和账号生成的，该处理模块 82 包括：

第三处理单元，用于根据第一令牌密钥和账号进行哈希运算，得到加密信息；或者，

第四处理单元，用于根据时间戳、第一令牌密钥和账号进行哈希运算，得到加密信息。

10 关于上述实施例中的装置，其中各个模块执行操作的具体方式已经在有关该方法的实施例中进行了详细描述，此处将不做详细阐述说明。

图 9 是根据一示例性实施例示出的一种用于绑定账号与令牌密钥的装置 800 的框图。例如，装置 800 可以是移动电话，计算机，数字广播终端，消息收发设备，游戏控制台，平板设备，医疗设备，健身设备，个人数字助理等。

15 参照图 9，装置 800 可以包括以下一个或多个组件：处理组件 802，存储器 804，电源组件 806，多媒体组件 808，音频组件 810，输入/输出（I/O）的接口 812，传感器组件 814，以及通信组件 816。

处理组件 802 通常控制装置 800 的整体操作，诸如与显示，电话呼叫，数据通信，相机操作和记录操作相关联的操作。处理组件 802 可以包括一个或多个处理器 820 来执行指令，以完成上述的方法的全部或部分步骤。此外，处理组件 802 可以包括一个或多个模块，便于处理组件 802 和其他组件之间的交互。例如，处理组件 802 可以包括多媒体模块，以方便多媒体组件 808 和处理组件 802 之间的交互。

25 存储器 804 被配置为存储各种类型的数据以支持在装置 800 的操作。这些数据的示例包括用于在装置 800 上操作的任何应用程序或方法的指令，联系人数据，电话簿数据，消息，图片，视频等。存储器 804 可以由任何类型的易失性或非易失性存储设备或者它们的组合实现，如静态随机存取存储器（SRAM），电可擦除可编程只读存储器（EEPROM），可擦除可编程只读存储器（EPROM），可编程只读存储器（PROM），只读存储器（ROM），磁存储器，快闪存储器，磁盘或光盘。

30 电源组件 806 为装置 800 的各种组件提供电力。电源组件 806 可以包括电源管理系统，一个或多个电源，及其他与为装置 800 生成、管理和分配电力相关联的组件。

35 多媒体组件 808 包括在所述装置 800 和用户之间的提供一个输出接口的屏幕。在一些实施例中，屏幕可以包括液晶显示器（LCD）和触摸面板（TP）。如果屏幕包括触摸面板，屏幕可以被实现为触摸屏，以接收来自用户的输入信号。触摸面板包括一个或多个触摸传感器以感测触摸、滑动和触摸面板上的手势。所述触摸传感器可以不仅感测触摸或滑动动作的边界，而且还检测与所述触摸或滑动操作相关的持续时间和压力。在一些实施例中，

多媒体组件 808 包括一个前置摄像头和/或后置摄像头。当装置 800 处于操作模式，如拍摄模式或视频模式时，前置摄像头和/或后置摄像头可以接收外部的多媒体数据。每个前置摄像头和后置摄像头可以是一个固定的光学透镜系统或具有焦距和光学变焦能力。

音频组件 810 被配置为输出和/或输入音频信号。例如，音频组件 810 包括一个麦克风（MIC），当装置 800 处于操作模式，如呼叫模式、记录模式和语音识别模式时，麦克风被配置为接收外部音频信号。所接收的音频信号可以被进一步存储在存储器 804 或经由通信组件 816 发送。在一些实施例中，音频组件 810 还包括一个扬声器，用于输出音频信号。

I/O 接口 812 为处理组件 802 和外围接口模块之间提供接口，上述外围接口模块可以是键盘，点击轮，按钮等。这些按钮可包括但不限于：主页按钮、音量按钮、启动按钮和锁定按钮。

传感器组件 814 包括一个或多个传感器，用于为装置 800 提供各个方面的状态评估。例如，传感器组件 814 可以检测到装置 800 的打开/关闭状态，组件的相对定位，例如所述组件为装置 800 的显示器和小键盘，传感器组件 814 还可以检测装置 800 或装置 800 一个组件的位置改变，用户与装置 800 接触的存在或不存在，装置 800 方位或加速/减速和装置 800 的温度变化。传感器组件 814 可以包括接近传感器，被配置用来在没有任何的物理接触时检测附近物体的存在。传感器组件 814 还可以包括光传感器，如 CMOS 或 CCD 图像传感器，用于在成像应用中使用。在一些实施例中，该传感器组件 814 还可以包括加速度传感器，陀螺仪传感器，磁传感器，压力传感器或温度传感器。

通信组件 816 被配置为便于装置 800 和其他设备之间有线或无线方式的通信。装置 800 可以接入基于通信标准的无线网络，如 WiFi，2G 或 3G，或它们的组合。在一个示例性实施例中，通信组件 816 经由广播信道接收来自外部广播管理系统的广播信号或广播相关信息。在一个示例性实施例中，所述通信组件 816 还包括近场通信（NFC）模块，以促进短程通信。例如，在 NFC 模块可基于射频识别（RFID）技术，红外数据协会（IrDA）技术，超宽带（UWB）技术，蓝牙（BT）技术和其他技术来实现。

在示例性实施例中，装置 800 可以被一个或多个应用专用集成电路（ASIC）、数字信号处理器（DSP）、数字信号处理设备（DSPD）、可编程逻辑器件（PLD）、现场可编程门阵列（FPGA）、控制器、微控制器、微处理器或其他电子元件实现，用于执行上述方法。

在示例性实施例中，还提供了一种包括指令的非临时性计算机可读存储介质，例如包括指令的存储器 804，上述指令可由装置 800 的处理器 820 执行以完成上述方法。例如，所述非临时性计算机可读存储介质可以是 ROM、随机存取存储器（RAM）、CD-ROM、磁带、软盘和光数据存储设备等。

一种非临时性计算机可读存储介质，当所述存储介质中的指令由网页端的处理器执行时，使得网页端能够执行一种绑定账号与令牌密钥的方法，所述方法包括：

向服务器发送携带账号的绑定请求消息，以使所述服务器生成与所述账号对应的认证链接和第一令牌密钥；

获取所述认证链接和所述第一令牌密钥，根据所述认证链接和所述第一令牌密钥生成显示信息，以使移动终端根据所述第一令牌密钥得到加密信息，并发送携带所述认证链接和所述加密信息的访问请求消息，进而使得所述服务器接收所述访问请求消息，发送所述加密信息；

获取所述加密信息，根据所述加密信息得到第二令牌密钥；

确定所述第二令牌密钥与所述第一令牌密钥一致后，向所述服务器发送绑定成功消息，以使所述服务器绑定所述第一令牌密钥与所述账号。

一种非临时性计算机可读存储介质，当所述存储介质中的指令由移动终端的处理器执行时，使得移动终端能够执行一种绑定账号与令牌密钥的方法，所述方法包括：

获取网页端的显示信息，所述显示信息是所述网页端根据服务器生成的认证链接和第一令牌密钥生成的，所述认证链接和所述第一令牌密钥是所述服务器根据所述网页端发送绑定请求消息中携带账号的生成的；

根据所述第一令牌密钥得到加密信息，并发送携带所述加密信息和所述认证链接的访问请求消息，以使所述服务器接收所述访问请求消息后，向所述网页端发送所述加密信息，所述网页端根据所述加密信息得到第二令牌密钥，在确认所述第二令牌密钥与所述第一令牌密钥一致后，向所述服务器发送绑定成功消息，所述服务器接收到所述绑定成功消息后，绑定所述令牌密钥与所述账号。

图 10 是根据一示例性实施例示出的一种用于绑定账号与令牌密钥的的装置 1900 的框图。例如，装置 1900 可以被提供为一服务器。参照图 10，装置 1900 包括处理组件 1922，其进一步包括一个或多个处理器，以及由存储器 1932 所代表的存储器资源，用于存储可由处理组件 1922 的执行的指令，例如应用程序。存储器 1932 中存储的应用程序可以包括一个或一个以上的每一个对应于一组指令的模块。此外，处理组件 1922 被配置为执行指令，以执行上述绑定账号与令牌密钥的方法，所述方法包括：

接收网页端发送的携带账号的绑定请求消息；

生成与所述账号对应的认证链接和第一令牌密钥，以使所述网页端根据所述认证链接和所述第一令牌密钥生成显示信息，进而使得移动终端根据所述第一令牌密钥得到加密信息，并发送携带所述认证链接和所述加密信息的访问请求消息；

接收所述访问请求消息，发送所述加密信息，以使所述网页端根据所述加密信息得到第二令牌密钥，在确定所述第二令牌密钥与所述第一令牌密钥一致后，发送绑定成功消息；

接收所述绑定成功消息，绑定所述第一令牌密钥与所述账号。

装置 1900 还可以包括一个电源组件 1926 被配置为执行装置 1900 的电源管理，一个有线或无线网络接口 1950 被配置为将装置 1900 连接到网络，和一个输入输出（I/O）接口 1958。装置 1900 可以操作基于存储在存储器 1932 的操作系统，例如 Windows Server™，

Mac OS X™, Unix™, Linux™, FreeBSD™ 或类似。

5 本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本发明的其它实施方案。本申请旨在涵盖本发明的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本发明的一般性原理并包括本公开未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本发明的真正范围和精神由下面的权利要求指出。

应当理解的是，本发明并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本发明的范围仅由所附的权利要求来限制。

权利要求

1、一种绑定账号与令牌密钥的方法，其特征在于，包括：

向服务器发送携带账号的绑定请求消息，以使所述服务器生成与所述账号对应的认证链接和第一令牌密钥；

5 获取所述认证链接和所述第一令牌密钥，根据所述认证链接和所述第一令牌密钥生成显示信息，以使移动终端根据所述第一令牌密钥得到加密信息，并发送携带所述认证链接和所述加密信息的访问请求消息，进而使得所述服务器接收所述访问请求消息，发送所述加密信息；

获取所述加密信息，根据所述加密信息得到第二令牌密钥；

10 确定所述第二令牌密钥与所述第一令牌密钥一致后，向所述服务器发送绑定成功消息，以使所述服务器绑定所述第一令牌密钥与所述账号。

2、根据权利要求1所述的方法，其特征在于，根据所述认证链接和所述第一令牌密钥生成显示信息的步骤包括：

15 根据所述认证链接、所述第一令牌密钥和所述账号生成所述显示信息，以使所述移动终端根据所述第一令牌密钥和所述账号进行哈希运算，得到所述加密信息，或者，根据时间戳、所述第一令牌密钥和所述账号进行哈希运算，得到所述加密信息。

3、一种绑定账号与令牌密钥的方法，其特征在于，包括：

接收网页端发送的携带账号的绑定请求消息；

20 生成与所述账号对应的认证链接和第一令牌密钥，以使所述网页端根据所述认证链接和所述第一令牌密钥生成显示信息，进而使得移动终端根据所述第一令牌密钥得到加密信息，并发送携带所述认证链接和所述加密信息的访问请求消息；

接收所述访问请求消息，发送所述加密信息，以使所述网页端根据所述加密信息得到第二令牌密钥，在确定所述第二令牌密钥与所述第一令牌密钥一致后，发送绑定成功消息；

接收所述绑定成功消息，绑定所述第一令牌密钥与所述账号。

25 4、根据权利要求3所述的方法，其特征在于，所述方法还包括：

建立与所述网页端的通信连接；

若在设定时长内未接收到所述移动终端发送的访问请求消息，则释放与所述网页端的通信连接。

5、一种绑定账号与令牌密钥的方法，其特征在于，包括：

30 获取网页端的显示信息，所述显示信息是所述网页端根据服务器生成的认证链接和第一令牌密钥生成的，所述认证链接和所述第一令牌密钥是所述服务器根据所述网页端发送绑定请求消息中携带账号的生成的；

35 根据所述第一令牌密钥得到加密信息，并发送携带所述加密信息和所述认证链接的访问请求消息，以使所述服务器接收所述访问请求消息后，向所述网页端发送所述加密信息，所述网页端根据所述加密信息得到第二令牌密钥，在确认所述第二令牌密钥与所述第一令

牌密钥一致后,向所述服务器发送绑定成功消息,所述服务器接收到所述绑定成功消息后,绑定所述令牌密钥与所述账号。

6、根据权利要求5所述的方法,其特征在于,根据所述第一令牌密钥得到加密信息的步骤包括:

- 5 将所述第一令牌密钥作为所述加密信息;或者,
根据时间戳和所述第一令牌密钥进行哈希运算,得到所述加密信息。

7、根据权利要求5所述的方法,其特征在于,所述显示信息是所述网页端根据服务器生成的所述认证链接、所述第一令牌密钥和所述账号生成的,根据所述第一令牌密钥得到加密信息的步骤包括:

- 10 根据所述第一令牌密钥和所述账号进行哈希运算,得到所述加密信息;或者,
根据时间戳、所述第一令牌密钥和所述账号进行哈希运算,得到所述加密信息。

8、一种绑定账号与令牌密钥的装置,其特征在于,包括:

第一发送模块,用于向服务器发送携带账号的绑定请求消息,以使所述服务器生成与所述账号对应的认证链接和第一令牌密钥;

- 15 第一获取模块,用于获取所述认证链接和所述第一令牌密钥;

第一生成模块,用于根据所述认证链接和所述第一令牌密钥生成显示信息,以使移动终端根据所述第一令牌密钥得到加密信息,并发送携带所述认证链接和所述加密信息的访问请求消息,进而使得所述服务器接收所述访问请求消息,发送所述加密信息;

第二获取模块,用于获取所述加密信息;

- 20 第二生成模块,用于根据所述加密信息得到第二令牌密钥;

第二发送模块,用于确定所述第二令牌密钥与所述第一令牌密钥一致后,向所述服务器发送绑定成功消息,以使所述服务器绑定所述第一令牌密钥与所述账号。

9、根据权利要求8所述的装置,其特征在于,所述第一生成模块包括:

- 25 生成单元,用于根据所述认证链接、所述第一令牌密钥和所述账号生成所述显示信息,
以使所述移动终端根据所述第一令牌密钥和所述账号进行哈希运算,得到所述加密信息,
或者,根据时间戳、所述第一令牌密钥和所述账号进行哈希运算,得到所述加密信息。

10、一种绑定账号与令牌密钥的装置,其特征在于,包括:

第一接收模块,用于接收网页端发送的携带账号的绑定请求消息;

- 30 生成模块,用于生成与所述账号对应的认证链接和第一令牌密钥,以使所述网页端根据所述认证链接和所述第一令牌密钥生成显示信息,进而使得移动终端根据所述第一令牌密钥得到加密信息,并发送携带所述认证链接和所述加密信息的访问请求消息;

第二接收模块,用于接收所述访问请求消息;

发送模块,用于发送所述加密信息,以使所述网页端根据所述加密信息得到第二令牌密钥,在确定所述第二令牌密钥与所述第一令牌密钥一致后,发送绑定成功消息;

- 35 第三接收模块,用于接收所述绑定成功消息;

绑定模块，用于绑定所述第一令牌密钥与所述账号。

11、根据权利要求 10 所述的装置，其特征在于，所述装置还包括：

建立模块，用于建立与所述网页端的通信连接；

5 释放模块，用于若在设定时长内未接收到所述移动终端发送的访问请求消息，则释放与所述网页端的通信连接。

12、一种绑定账号与令牌密钥的装置，其特征在于，包括：

获取模块，用于获取网页端的显示信息，所述显示信息是所述网页端根据服务器生成的认证链接和第一令牌密钥生成的，所述认证链接和所述第一令牌密钥是所述服务器根据所述网页端发送绑定请求消息中携带账号的生成的；

10 处理模块，用于根据所述第一令牌密钥得到加密信息，并发送携带所述加密信息和所述认证链接的访问请求消息，以使所述服务器接收所述访问请求消息后，向所述网页端发送所述加密信息，所述网页端根据所述加密信息得到第二令牌密钥，在确认所述第二令牌密钥与所述第一令牌密钥一致后，向所述服务器发送绑定成功消息，所述服务器接收到所述绑定成功消息后，绑定所述令牌密钥与所述账号。

15 13、根据权利要求 12 所述的装置，其特征在于，所述处理模块包括：

第一处理单元，用于将所述第一令牌密钥作为所述加密信息；或者，

第二处理单元，用于根据时间戳和所述第一令牌密钥进行哈希运算，得到所述加密信息。

20 14、根据权利要求 12 所述的装置，其特征在于，所述显示信息是所述网页端根据服务器生成的所述认证链接、所述第一令牌密钥和所述账号生成的，所述处理模块包括：

第三处理单元，用于根据所述第一令牌密钥和所述账号进行哈希运算，得到所述加密信息；或者，

第四处理单元，用于根据时间戳、所述第一令牌密钥和所述账号进行哈希运算，得到所述加密信息。

25 15、一种网页端，其特征在于，包括：

处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器被配置为：

30 向服务器发送携带账号的绑定请求消息，以使所述服务器生成与所述账号对应的认证链接和第一令牌密钥；

获取所述认证链接和所述第一令牌密钥，根据所述认证链接和所述第一令牌密钥生成显示信息，以使移动终端根据所述第一令牌密钥得到加密信息，并发送携带所述认证链接和所述加密信息的访问请求消息，进而使得所述服务器接收所述访问请求消息，发送所述加密信息；

35 获取所述加密信息，根据所述加密信息得到第二令牌密钥；

确定所述第二令牌密钥与所述第一令牌密钥一致后，向所述服务器发送绑定成功消息，以使所述服务器绑定所述第一令牌密钥与所述账号。

16、一种服务器，其特征在于，包括：

处理器；

5 用于存储处理器可执行指令的存储器；

其中，所述处理器被配置为：

接收网页端发送的携带账号的绑定请求消息；

生成与所述账号对应的认证链接和第一令牌密钥，以使所述网页端根据所述认证链接和所述第一令牌密钥生成显示信息，进而使得移动终端根据所述第一令牌密钥得到加密信息，并发送携带所述认证链接和所述加密信息的访问请求消息；

10

接收所述访问请求消息，发送所述加密信息，以使所述网页端根据所述加密信息得到第二令牌密钥，在确定所述第二令牌密钥与所述第一令牌密钥一致后，发送绑定成功消息；

接收所述绑定成功消息，绑定所述第一令牌密钥与所述账号。

17、一种移动终端，其特征在于，包括：

15

处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器被配置为：

获取网页端的显示信息，所述显示信息是所述网页端根据服务器生成的认证链接和第一令牌密钥生成的，所述认证链接和所述第一令牌密钥是所述服务器根据所述网页端发送绑定请求消息中携带账号的生成的；

20

根据所述第一令牌密钥得到加密信息，并发送携带所述加密信息和所述认证链接的访问请求消息，以使所述服务器接收所述访问请求消息后，向所述网页端发送所述加密信息，所述网页端根据所述加密信息得到第二令牌密钥，在确认所述第二令牌密钥与所述第一令牌密钥一致后，向所述服务器发送绑定成功消息，所述服务器接收到所述绑定成功消息后，

25

绑定所述令牌密钥与所述账号。

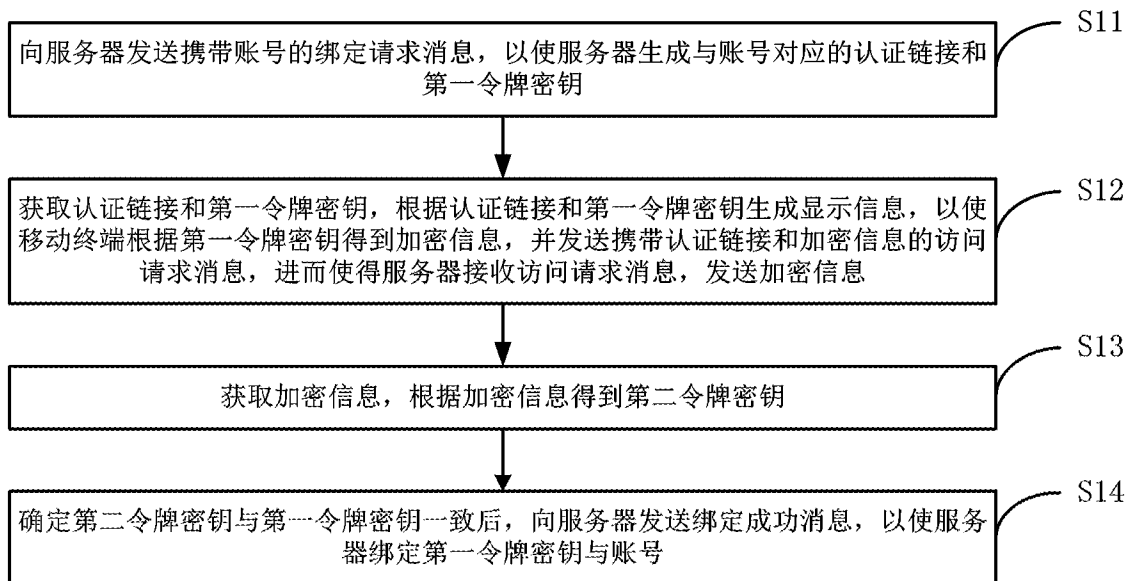


图1

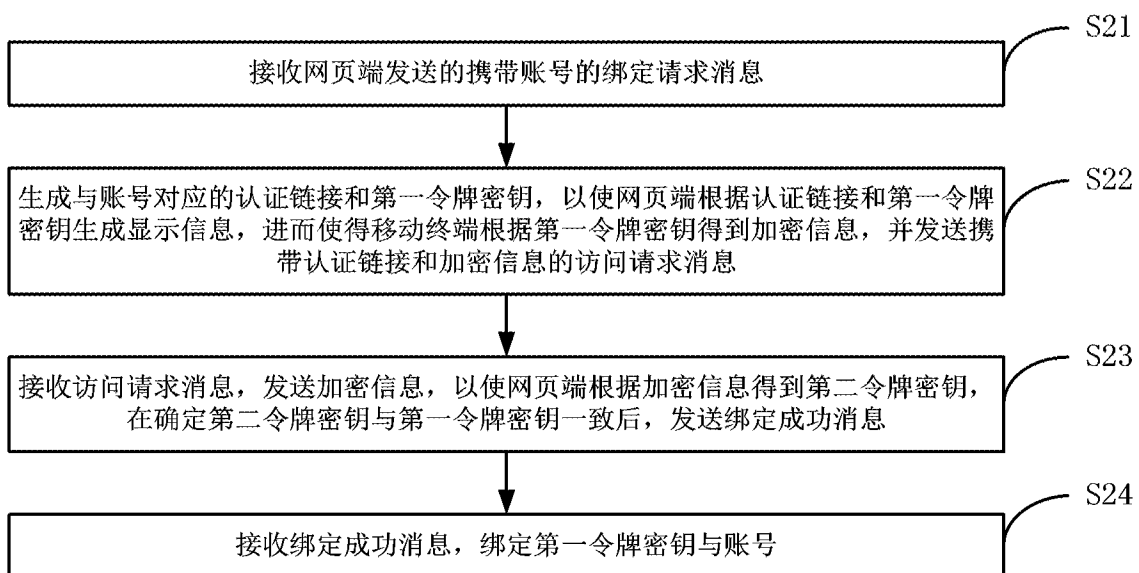


图2

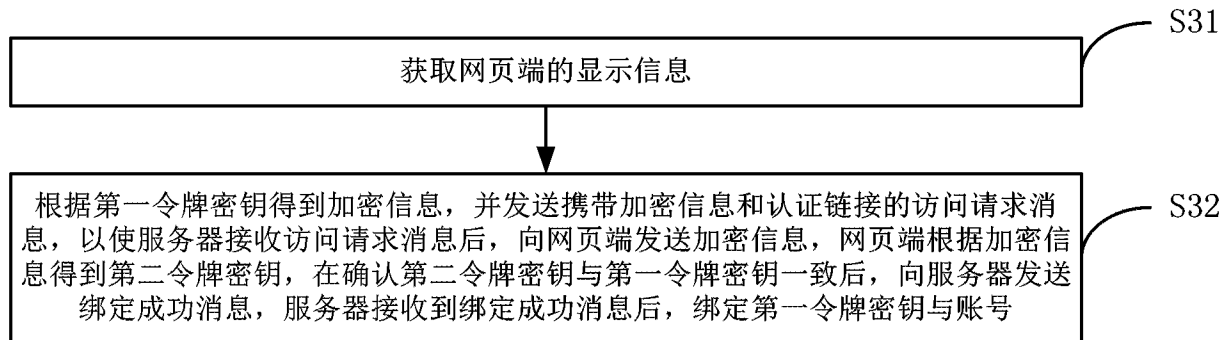


图3

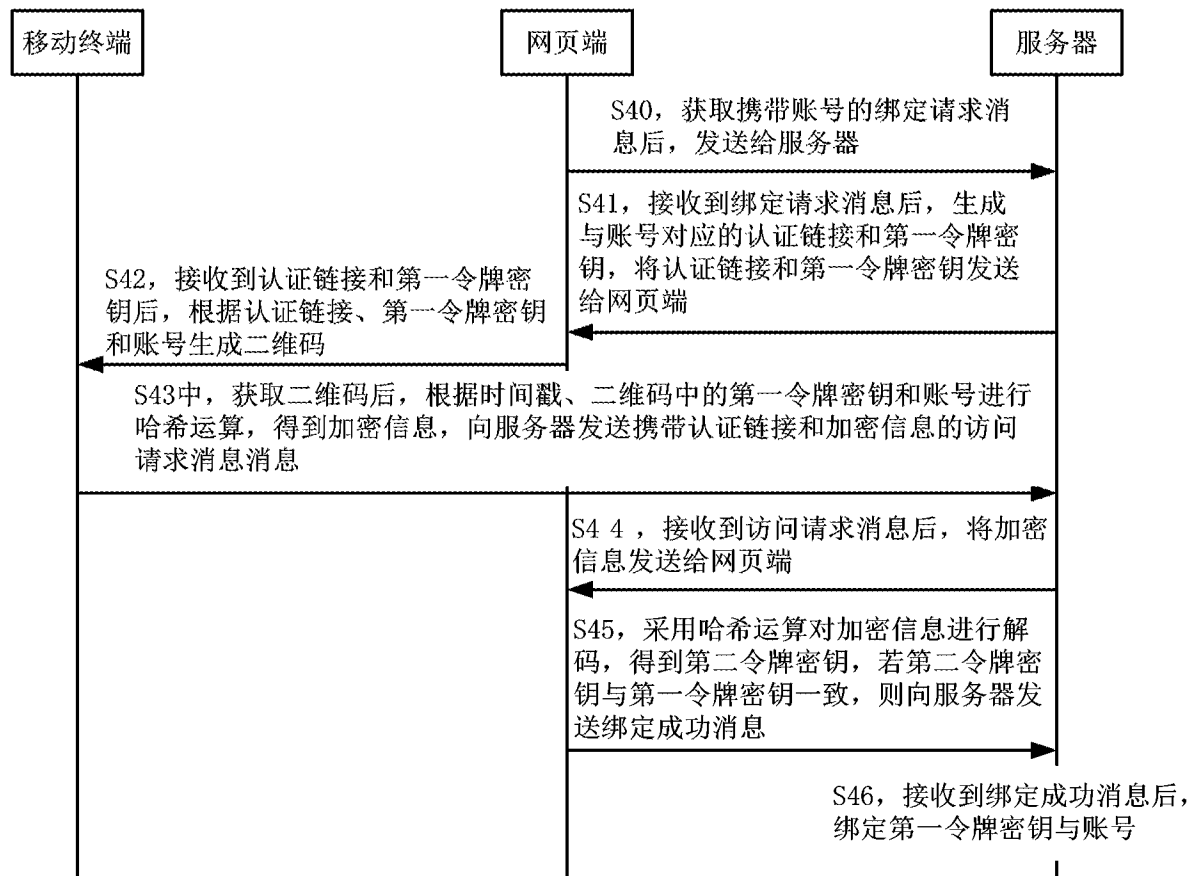


图4

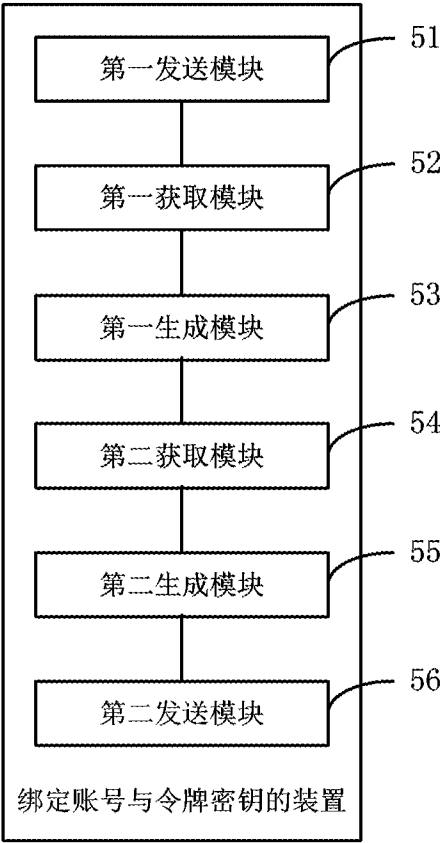


图5

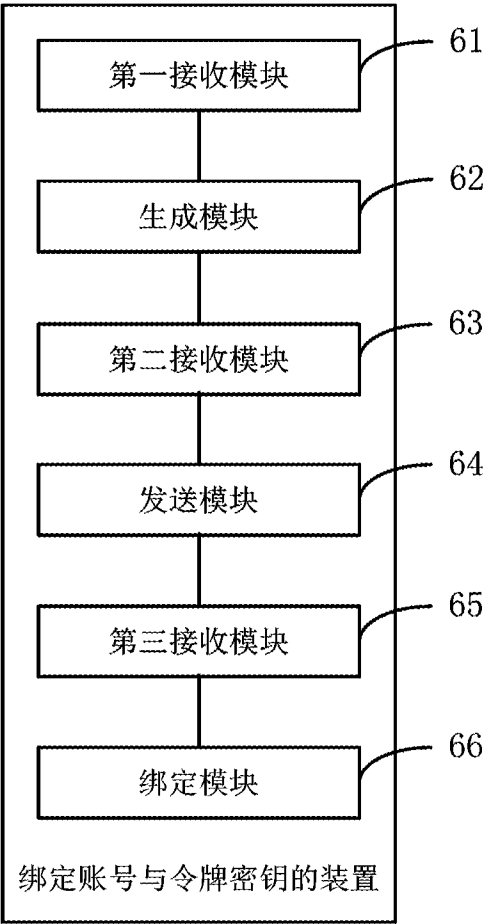


图6

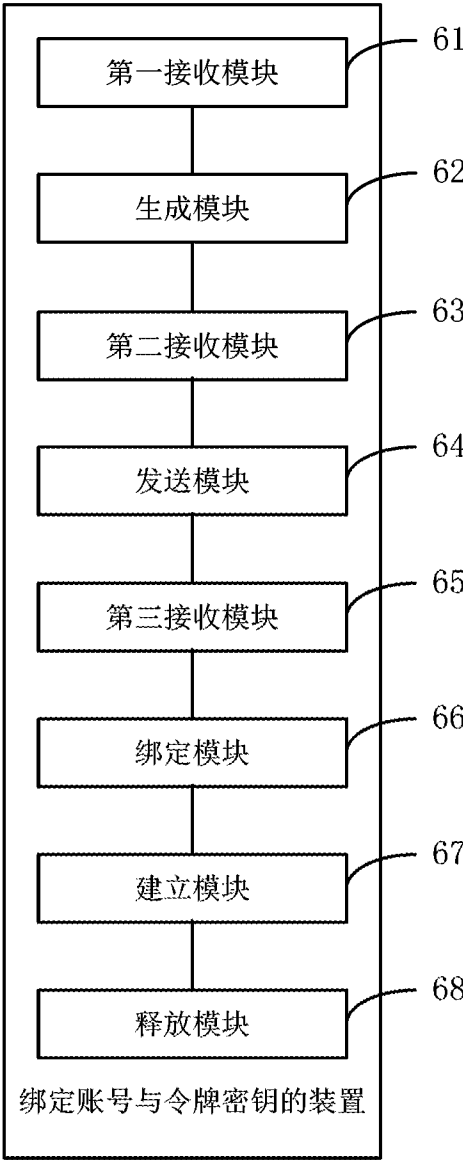


图7

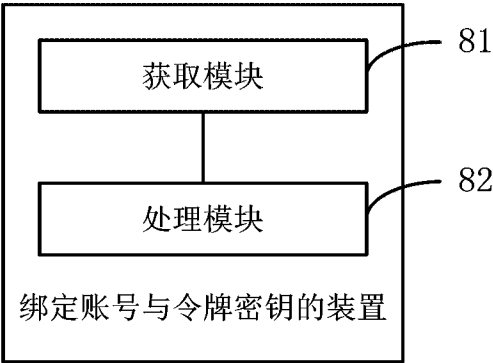


图8

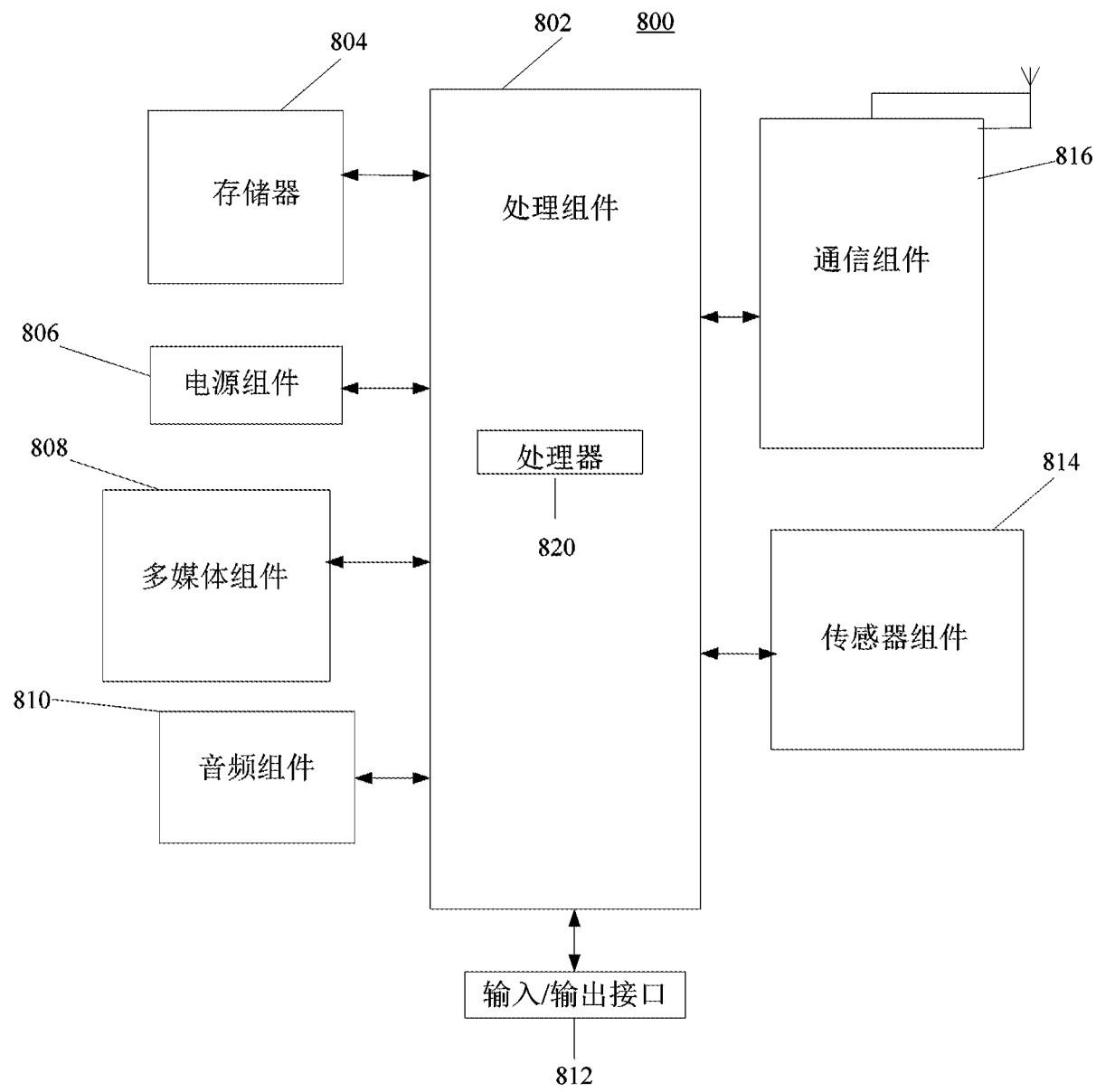


图9

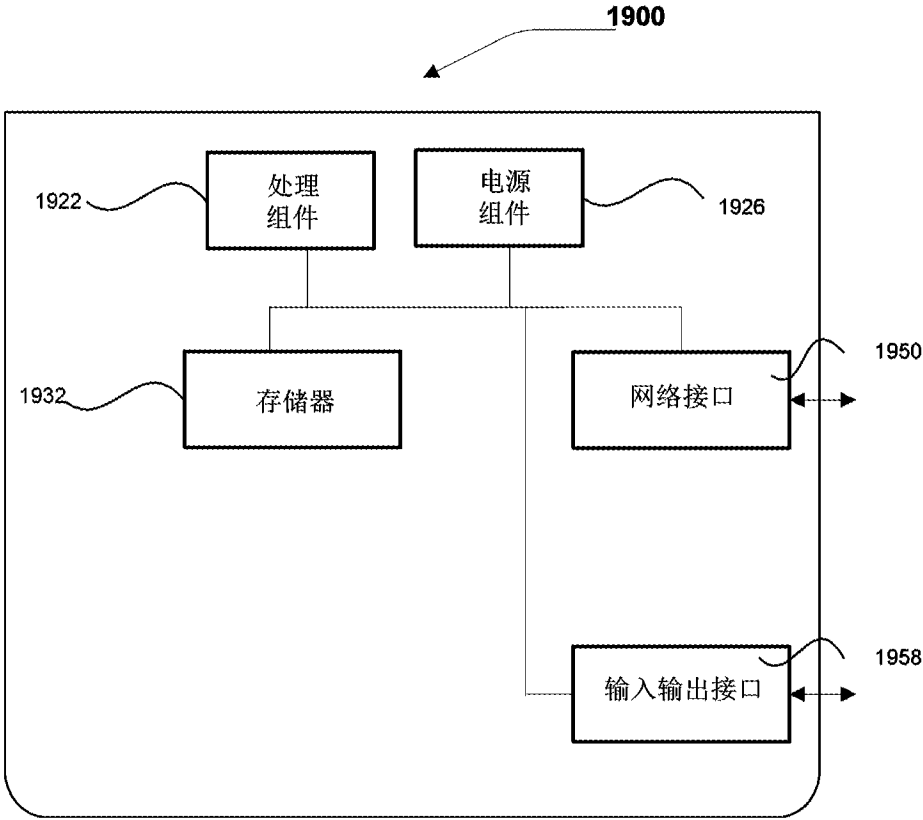


图10

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2014/089281

A. CLASSIFICATION OF SUBJECT MATTER

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; H04W; H04Q; H04W; 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, CPRSABS, CNTXT, CNKI, VEN: safety, account, username, token, bind+, key, verif+, authenticat+, logon, login

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 101582762 A (FEITIAN TECHNOLOGIES CO., LTD.), 18 November 2009 (18.11.2009), the whole document	1-17
A	CN 103179115 A (INSTITUTE OF INFORMATION ENGINEERING, CHINESE ACADEMY OF SCIENCES), 26 June 2013 (26.06.2013), the whole document	1-17
A	CN 103281186 A (SHANGHAI PEOPLE NETNETWORK SECURITY TECHNOLOGY CO., LTD.), 04 September 2013 (04.09.2013), the whole document	1-17
A	US 2006059346 A1 (SHERMAN, A. et al.), 16 March 2006 (16.03.2006), the whole document	1-17

☐ 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 26 March 2015 (26.03.2015)	Date of mailing of the international search report 01 April 2015 (01.04.2015)
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 ZHANG, Xin Telephone No.: (86-10) 62089567

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2014/089281

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101582762 A	18 November 2009	CN 101582762 B	13 July 2011
CN 103179115 A	26 June 2013	None	
CN 103281186 A	04 September 2013	None	
US 2006059346 A1	16 March 2006	JP 2006120148 A	11 May 2006
		EP 1635536 A3	23 January 2008
		EP 1635536 A2	15 March 2006

A. 主题的分类 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; H04W; H04Q; H04W; 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, CPRSABS, CNTXT, CNKI, VEN: 账号, 账户, 用户名, 令牌, 绑定, 密钥, 认证, 登录, 安全, account, username, token, bind+, key, verif+, authenticat+, logon, login		
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
A	CN 101582762 A (北京飞天诚信科技有限公司) 2009年 11月 18日 (2009 - 11 - 18) 全文	1-17
A	CN 103179115 A (中国科学院信息工程研究所) 2013年 6月 26日 (2013 - 06 - 26) 全文	1-17
A	CN 103281186 A (上海众人网络安全技术有限公司) 2013年 9月 4日 (2013 - 09 - 04) 全文	1-17
A	US 2006059346 A1 (SHERMAN, A. 等) 2006年 3月 16日 (2006 - 03 - 16) 全文	1-17
☐ 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 26日		国际检索报告邮寄日期 2015年 4月 1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 张鑫 电话号码 (86-10)62089567

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2014/089281

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	101582762	A	2009年 11月 18日	CN 101582762 B	2011年 7月 13日
CN	103179115	A	2013年 6月 26日	无	
CN	103281186	A	2013年 9月 4日	无	
US	2006059346	A1	2006年 3月 16日	JP 2006120148 A	2006年 5月 11日
				EP 1635536 A3	2008年 1月 23日
				EP 1635536 A2	2006年 3月 15日