

(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 6 月 1 日 (01.06.2017)



(10) 国际公布号
WO 2017/088677 A1

- (51) 国际专利分类号:
H04L 9/32 (2006.01)
- (21) 国际申请号: PCT/CN2016/105668
- (22) 国际申请日: 2016 年 11 月 14 日 (14.11.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510819162.2 2015 年 11 月 23 日 (23.11.2015) CN
- (71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 开曼群岛英属开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。
- (72) 发明人: 张治中 (ZHANG, Zhizhong); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。
- (74) 代理人: 北京三友知识产权代理有限公司 (BEIJING SANYOU INTELLECTUAL PROPERTY AGENCY LTD.); 中国北京市金融街 35 号国际企业大厦 A 座 16 层, Beijing 100033 (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: USER KEY STORAGE METHOD AND SERVER

(54) 发明名称: 一种用户密钥存储方法及服务器

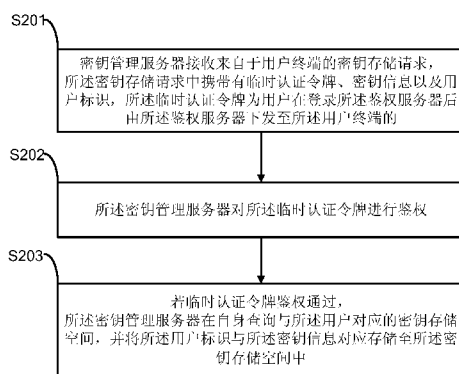


图 2

S201 A KEY MANAGEMENT SERVER RECEIVES A KEY STORAGE REQUEST FROM A USER TERMINAL. THE KEY STORAGE REQUEST CARRYING A TEMPORARY AUTHENTICATION TOKEN, KEY INFORMATION, AND A USER IDENTITY, AND THE TEMPORARY AUTHENTICATION TOKEN BEING ISSUED TO THE USER TERMINAL BY AN AUTHENTICATION SERVER AFTER A USER LOGS IN THE AUTHENTICATION SERVER.

S202 THE KEY MANAGEMENT SERVER AUTHENTICATES THE TEMPORARY AUTHENTICATION TOKEN.

S203 IF THE TEMPORARY AUTHENTICATION TOKEN HAS PASSED THE AUTHENTICATION, THE KEY MANAGEMENT SERVER SELF-QUERIES A KEY STORAGE SPACE CORRESPONDING TO THE USER, AND STORES THE USER IDENTITY AND THE KEY INFORMATION IN THE KEY STORAGE SPACE CORRESPONDINGLY.

(57) Abstract: Disclosed are a user key storage method and a server. A key management server receives a key storage request from a user terminal, and authenticates a temporary authentication token in the key storage request. The temporary authentication token is issued to the user terminal by an authentication server after a user logs in the authentication server, so if the temporary authentication token has passed the authentication, the key management server can self-query a key storage space corresponding to the user, and store a user identity and key information in the key storage space correspondingly. Thus, a dedicated interface does not need to be disposed between servers to implement storage of a user key, thereby greatly simplifying a development flow, reducing the development cost, guaranteeing the security and improving the development efficiency.

(57) 摘要:

[见续页]

WO 2017/088677 A1

本发明公开了一种用户密钥存储方法及服务器。密钥管理服务器首先接收来自于用户终端的密钥存储请求，并对密钥存储请求中的临时认证令牌进行鉴权，由于临时认证令牌为用户在登录鉴权服务器后由鉴权服务器下发至用户终端，因此若临时认证令牌鉴权通过，密钥管理服务器即可在自身查询与用户对应的密钥存储空间，并将用户标识与密钥信息对应存储至密钥存储空间中。从而无需再在服务器之间设置专用接口实现用户密钥的存储，极大简化了开发流程以及减少了开发成本，并在保障安全性的同时提高了开发效率。

一种用户密钥存储方法及服务器

本申请要求 2015 年 11 月 23 日递交的申请号为 201510819162.2、发明名称为“一种用户密钥存储方法及服务器”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

5

技术领域

本申请涉及通信技术领域，特别涉及一种用户密钥存储方法。本申请同时还涉及一种服务器。

10 背景技术

随着互联网技术的不断发展，人们现在通过互联网能够完成各种自己所需要的东西。在用户通过网络提供或获取服务时，一般都需要在服务提供商或网络运营商注册属于自己的账号，并设置相对应的密码。

在目前生活中，互联网服务多种多样，用户需要注册各类网站，每个网站都要有用
15 户名、密码。网站按重要程度可简单分为以下两种：

(1) 高优先级账户，例如银行等金融账户，该类型的账户 ID 以及密码涉及用户的财产安全，需要用户妥善进行保管；

(2) 低优先级账户，例如各种论坛账户，该类型的账户或只注册看一次就不用再管。

为了帮助用户记录繁多的账号密码，现有技术提出了密码管理器以提高用户在页面
20 浏览时的使用体验。具体地，在当用户通过某网站完成注册之后，密码管理器将用户名、密码保存起来，后续在用户需要登录该网站时自动填写用户名、密码，若用户不想自己设置密码，还能在用户需要生成密码时自动生成密码。

作为目前使用率较高的一款密码管理器，Last Pass 能够以浏览器扩展的形式使用，当用户登录任何一个网站时会提示保存登录信息，后续用户访问该网站时将会自动填写
25 登录表单，免除记忆账密和手工输入的麻烦。以 Last Pass 为例，现有技术中的密钥管理系统的架构示意图如图 1 所示，其后端需要部署很重的服务用来做用户索引、数据索引以及数据存储。而且需要定义前后端接口。因此开发者要自行开发应用并部署至业务服务器上提供服务，而且开发者需要自己提供用户索引和数据索引服务，若开发者不用云存储的话，需要自己提供数据存储服务。

发明人在实现本发明的过程中发现，对于普通的开发者而言，其并不能负担大量用户的密钥存储所需要的服务器租赁以及架设费用，因此对于该类系统而言，服务器会成为性能瓶颈。而且不同开发者的设计以及开发习惯不同，导致此类系统耦合性高但可复用性差。

由此可见，如何在降低硬件使用成本以及缩短开发周期的前提下实现用户的密钥管理，成为本领域技术人员亟待解决的技术问题。

发明内容

本发明提供了一种用户密钥存储方法，用以在简化开发流程以及减少开发成本的前提下提高用户密钥的管理效率，该方法应用于包括密钥管理服务器、用户终端以及鉴权服务器的密钥管理系统中，包括：

所述密钥管理服务器接收来自于用户终端的密钥存储请求，所述密钥存储请求中携带有临时认证令牌、密钥信息以及用户标识，所述临时认证令牌为用户在登录所述鉴权服务器后由所述鉴权服务器下发至所述用户终端的；

所述密钥管理服务器对所述临时认证令牌进行鉴权；

若所述临时认证令牌鉴权通过，所述密钥管理服务器在自身查询与所述用户对应的密钥存储空间，并将所述用户标识与所述密钥信息对应存储至所述密钥存储空间中。

优选地，所述临时认证令牌具体为所述用户终端在所述用户登录所述鉴权服务器后向所述鉴权服务器请求获取的。

优选地，所述密钥信息至少包括用户账户、用户密码以及网站标识，在所述密钥管理服务器将所述用户标识与所述密钥信息对应存储至所述密钥存储空间之后，还包括：

当接收到来自于所述用户终端的密钥填写请求时，所述密钥管理服务器确定所述密钥填写请求对应的目标网站标识；

所述密钥管理服务器在所述密钥存储空间中查询与所述目标网站标识对应的用户账户以及用户密码；

所述密钥管理服务器将查询到的用户账户以及用户密码返回至所述用户终端。

优选地，所述密钥存储请求中还携带用户信息以及网站信息，在所述密钥管理服务器将所述用户标识与所述密钥信息对应存储至所述密钥存储空间之后，还包括：

所述密钥管理服务器根据所述用户信息、所述网站信息、所述用户标识以及所述待存储密钥生成用户索引。

优选地，在所述密钥管理服务器将所述用户标识与所述密钥信息对应存储至所述密钥存储空间之后，还包括：

当接收到来自于所述用户中的密钥检索请求时，根据所述密钥检索请求中携带的关键词以及所述用户索引生成搜索结果，并将所述搜索结果返回至所述用户终端。

5

本发明提供了一种服务器，用以在简化开发流程以及减少开发成本的前提下提高用户密钥的管理效率，该服务器用于作为密钥管理服务器应用于包括所述密钥管理服务器、用户终端以及鉴权服务器的密钥管理系统中，包括：

接收模块，接收来自于用户终端的密钥存储请求，所述密钥存储请求中携带有临时认证令牌、密钥信息以及用户标识，所述临时认证令牌为用户在登录所述鉴权服务器后由所述鉴权服务器下发至所述用户终端的；

鉴权模块，对所述临时认证令牌进行鉴权；

处理模块，在所述临时认证令牌鉴权通过时，查询服务器自身与所述用户对应的密钥存储空间，并将所述用户标识与所述密钥信息对应存储至所述密钥存储空间中。

15 优选地，所述临时认证令牌具体为所述用户终端在所述用户登录所述鉴权服务器后向所述鉴权服务器请求获取的。

优选地，所述密钥信息至少包括用户账户、用户密码以及网站标识；还包括：

填充模块，在接收到来自于所述用户终端的密钥填写请求时确定所述密钥填写请求对应的目标网站标识，在所述密钥存储空间中查询与所述目标网站标识对应的用户账户以及用户密码，将查询到的用户账户以及用户密码返回至所述用户终端。

20 优选地，所述密钥存储请求中还携带用户信息以及网站信息，还包括：

生成模块，根据所述用户信息、所述网站信息、所述用户标识以及所述待存储密钥生成用户索引。

25 优选地，所述生成模块还在接收到来自于所述用户中的密钥检索请求时根据所述密钥检索请求中携带的关键词以及所述用户索引生成搜索结果，并将所述搜索结果返回至所述用户终端。

由此可见，通过应用本申请的技术方案，密钥管理服务器首先接收来自于用户终端的密钥存储请求，并对密钥存储请求中的临时认证令牌进行鉴权，由于临时认证令牌为用户在登录鉴权服务器后由鉴权服务器下发至用户终端，因此若临时认证令牌鉴权通过，

30

密钥管理服务器即可在自身查询与用户对应的密钥存储空间，并将用户标识与密钥信息对应存储至密钥存储空间中。从而无需再在服务器之间设置专用接口实现用户密钥的存储，极大简化了开发流程以及减少了开发成本，并在保障安全性的同时提高了开发效率。

5 附图说明

图 1 为现有技术中密钥管理系统的架构示意图；

图 2 为本申请提出的一种用户密钥存储方法的流程示意图；

图 3 为本申请具体实施例所提出的一种用户密钥管理方法的示意图；

图 4 为本申请提出的一种服务器的结构示意图。

10

具体实施方式

有鉴于背景技术中所提出的技术问题，本申请提出了一种用户密钥存储方法，如图 2 所示，该方法包括以下步骤：

S201，所述密钥管理服务器接收来自于用户终端的密钥存储请求，所述密钥存储请求中携带有临时认证令牌、密钥信息以及用户标识，所述临时认证令牌为用户在登录鉴权服务器后由所述鉴权服务器下发至所述用户终端的。

在现有的技术中，用户在利用设有密钥管理工具的终端设备进行密钥存储时，终端设备需要利用专门的 API 接口与业务服务器进行对接，并且开发者还需要基于业务服务器设置其他的服务器用来存储用户的密钥数据，这无疑极大的增加了密钥管理的开发成本以及开发难度。为此本申请提出了一套仅由密钥管理服务器、用户终端以及鉴权服务器所组成的密钥管理系统。其中用户终端除了向用户提供网站浏览功能之外，搭载前端展示处理的密钥管理工具，其可以为移动终端或者 PC 终端，与鉴权服务器以及密钥管理服务器之间能够实现不依赖于接口设置的报文通信以及信息存储。通过对服务器的存储和读取的 API 进行优化，简化了密码管理时的查询、存储、读取等工作，开发者不再需要像以前那样需要对这些通用功能进行开发。

基于以上密钥管理系统，当用户需要存储密钥时，用户将首先通过用户终端登录鉴权服务器，在用户成功登录鉴权服务器之后，用户终端将向鉴权服务器请求临时认证令牌，并将该临时认证令牌与用户标识以及密钥信息一同携带在密钥存储请求中发送至密钥管理服务器。

30 优选地，技术人员可以将密钥管理服务器布置于目前的网络存储服务平台中，该网

络存储服务平台必须在具有存储及读取功能的前提下提供通用的接口。在具体的应用场景中，为了能够便捷、快速地实现本申请的技术方案，该网络存储服务平台可采用能够对外提供海量、安全和高可靠的云存储服务的 OSS（Object Storage Service，对象存储）平台。在采用 OSS 平台上的服务器应用本申请提供的密钥管理方案时，开发人员或者普
5 通用户均可通过自身所使用的移动终端或者是 PC 终端直接与 OSS 平台的服务器进行交互，而无需再设置 API 接口。在此基础上，技术人员也可基于网络存储服务平台的无关性，容量和处理能力的弹性扩展进一步对网络的接口功能以及存储功能进行拓展，这些都属于本申请的保护范围。

10 S202，所述密钥管理服务器对所述临时认证令牌进行鉴权。

S203，若所述临时认证令牌鉴权通过，所述密钥管理服务器在自身查询与所述用户对应的密钥存储空间，并将所述用户标识与所述密钥信息对应存储至所述密钥存储空间中。

在用户通过互联网进行活动的过程中，大多数情况下用户都是需要在网站填写自己
15 注册的用户名及密码，因此在本申请的一个优选实施例中，密钥信息应至少包括用户账户、用户密码以及网站标识，在密钥管理服务器将所述用户标识与所述密钥信息对应存储至所述密钥存储空间之后，若是接收到来自于所述用户终端的密钥填写请求，所述密钥管理服务器确定所述密钥填写请求对应的目标网站标识，在所述密钥存储空间中查询与
20 所述目标网站标识对应的用户账户以及用户密码，并将查询到的用户账户以及用户密码返回至所述用户终端，以此实现针对网站的用户名及密码的填写。

需要说明的是，虽然以上过程中仅以网站的用户名密码自动填充为例进行说明，然而当用户使用其他方式（例如 APP）进行登陆时，也可在此基础上针对标识进行改变以适应性地进行调整填充，这些都属于本申请的保护范围。

此外，为便于用户针对自己所存储的密码进行管理，密钥存储请求中还可携带用户
25 输入的自身的用户信息以及网站信息，在所述密钥管理服务器将所述用户标识与所述密钥信息对应存储至所述密钥存储空间之后，密钥管理服务器将根据所述用户信息、所述网站信息、所述用户标识以及所述待存储密钥生成用户索引，而在接收到来自于所述用户中的密钥检索请求时，密钥管理服务器即可根据所述密钥检索请求中携带的关键词以及所述用户索引生成搜索结果，并将所述搜索结果返回至所述用户终端。

30 通过以上方案可以看出，本申请的方案通过利用网络存储服务平台上的密钥管理服

务器所提供的云计算中开放的种种服务，取代了传统开发中的工作，省去了中间环节。将用户的请求与响应，直接与云计算中的服务打通，从而提高了现有的密钥管理效率。

为了进一步阐述本发明的技术思想，现结合如图 3 所示的具体应用场景，对本发明的技术方案进行说明。详细步骤如下：

S301，用户通过自身使用的终端设备（PC 设备或是移动终端）登录鉴权服务器；

S302，在安全登录了鉴权服务器之后，该用户在终端设备上打开密钥管理工具（该具体实施例中以 Last Pass 为例进行说明）。该密钥管理工具具有在线密码管理以及页面过滤的功能，能够记录用户通过终端设备在页面浏览过程中所填充的用户名及密码，同时识别当前浏览页面所需要填充的用户名及密码。

S303，密钥管理工具从鉴权服务器请求临时令牌 token；

S304，在接收到密钥管理工具的临时 token 请求之后，鉴权服务器需要为该密钥管理工具生成临时 token。在该具体实施例中，技术人员可以采用制定安全令牌服务（STS）生成临时 token，该安全令牌服务是一项发布、验证和续订安全令牌的 Web 服务，可以有效地保证临时 token 的安全性以及有效性。

S305，密钥管理工具在获得临时 token 后，利用该临时 token 取得获取访问网络存储服务平台的云服务的权限。开始查找与用户相关的记录信息，并将对应的用户名、密码以及其它数据等写在网络存储服务平台，同时将可以搜索的内容（例如用户名、网络名称等）放在云搜索服务中进行索引；

S306，用户在通过终端设备进行页面浏览的过程中需要进行密码填充时，通过密钥管理工具从网络存储服务平台获取所需的密码并填写至浏览页面，从而进行进一步的访问。

以上步骤在无需开发专用接口以及服务器的前提下，实现了用户在页面浏览过程中进行密码自动存储以及密钥自动填充的功能。然而，在相隔了一段时间未使用某一个账户之后，用户可能会遗忘当时登录该网站所使用的用户名，因此本具体实施例还提供了针对网站或是其他密码填充页面的搜索功能，具体如下：

S307，如果用户需要针对某一个网站或是密码填充页面搜索之前所填充的用户名及密码时，该用户可通过该密钥管理工具发起搜索请求，随后密钥管理工具将根据待搜索的网站或是填充页面的标识向网络存储服务平台请求云搜索服务，网络存储服务平台在接收到密钥管理工具的搜索请求之后，将根据 S305 中的索引在记录中查询之前用户所存

储的与该网站对应的所有用户名以及对应的密钥，并将搜索结果返回至密钥管理工具，后续密钥管理工具将获取到的与该网站对应的用户名、密码展示给用户。

基于与上述方法实施例相同的技术构思，本发明实施例还提供了一种服务器可以应用于上述方法流程中。

如图 4 所示，为本发明实施例提供的一种服务器的结构示意图，可以包括：

接收模块 401，接收来自于用户终端的密钥存储请求，所述密钥存储请求中携带有临时认证令牌、密钥信息以及用户标识，所述临时认证令牌为用户在登录所述鉴权服务器后由所述鉴权服务器下发至所述用户终端的；

鉴权模块 402，对所述临时认证令牌进行鉴权；

处理模块 403，若所述临时认证令牌鉴权通过，查询服务器自身与所述用户对应的密钥存储空间，并将所述用户标识与所述密钥信息对应存储至所述密钥存储空间中。

其中，所述临时认证令牌具体为所述用户终端在所述用户登录所述鉴权服务器后向所述鉴权服务器请求获取的。

所述密钥信息至少包括用户账户、用户密码以及网站标识；还包括：

填充模块，在接收到来自于所述用户终端的密钥填写请求时确定所述密钥填写请求对应的目标网站标识，在所述密钥存储空间中查询与所述目标网站标识对应的用户账户以及用户密码，将查询到的用户账户以及用户密码返回至所述用户终端。

所述密钥存储请求中还携带用户信息以及网站信息，还包括：

生成模块，根据所述用户信息、所述网站信息、所述用户标识以及所述待存储密钥生成用户索引。

所述生成模块还在接收到来自于所述用户中的密钥检索请求时根据所述密钥检索请求中携带的关键词以及所述用户索引生成搜索结果，并将所述搜索结果返回至所述用户终端。

通过应用本申请的技术方案，密钥管理服务器首先接收来自于用户终端的密钥存储请求，并对密钥存储请求中的临时认证令牌进行鉴权，由于临时认证令牌为用户在登录鉴权服务器后由鉴权服务器下发至用户终端，因此若临时认证令牌鉴权通过，密钥管理服务器即可在自身查询与用户对应的密钥存储空间，并将用户标识与密钥信息对应存储至密钥存储空间中。从而无需再在服务器之间设置专用接口实现用户密钥的存储，极大

简化了开发流程以及减少了开发成本，并在保障安全性的同时提高了开发效率。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到本发明可以通过硬件实现，也可以借助软件加必要的通用硬件平台的方式来实现。基于这样的理解，本
5 发明的技术方案可以以软件产品的形式体现出来，该软件产品可以存储在一个非易失性存储介质（可以是 CD-ROM，U 盘，移动硬盘等）中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本发明各个实施场景所述的方法。

本领域技术人员可以理解附图只是一个优选实施场景的示意图，附图中的模块或流
10 程并不一定是实施本发明所必须的。

本领域技术人员可以理解实施场景中的装置中的模块可以按照实施场景描述进行分布于实施场景的装置中，也可以进行相应变化位于不同于本实施场景的一个或多个装置中。上述实施场景的模块可以合并为一个模块，也可以进一步拆分成多个子模块。

上述本发明序号仅仅为了描述，不代表实施场景的优劣。

15 以上公开的仅为本发明的几个具体实施场景，但是，本发明并非局限于此，任何本领域的技术人员能思之的变化都应落入本发明的保护范围。

权利要求书

1、一种用户密钥存储方法，其特征在于，所述方法应用于包括密钥管理服务器、用户终端以及鉴权服务器的密钥管理系统中，该方法包括：

所述密钥管理服务器接收来自于用户终端的密钥存储请求，所述密钥存储请求中携带有临时认证令牌、密钥信息以及用户标识，所述临时认证令牌为用户在登录所述鉴权服务器后由所述鉴权服务器下发至所述用户终端的；

所述密钥管理服务器对所述临时认证令牌进行鉴权；

若所述临时认证令牌鉴权通过，所述密钥管理服务器在自身查询与所述用户对应的密钥存储空间，并将所述用户标识与所述密钥信息对应存储至所述密钥存储空间中。

2、如权利要求 1 所述的方法，其特征在于，

所述临时认证令牌具体为所述用户终端在所述用户登录所述鉴权服务器后向所述鉴权服务器请求获取的。

3、如权利要求 1 所述的方法，其特征在于，所述密钥信息至少包括用户账户、用户密码以及网站标识，在所述密钥管理服务器将所述用户标识与所述密钥信息对应存储至所述密钥存储空间之后，还包括：

当接收到来自于所述用户终端的密钥填写请求时，所述密钥管理服务器确定所述密钥填写请求对应的目标网站标识；

所述密钥管理服务器在所述密钥存储空间中查询与所述目标网站标识对应的用户账户以及用户密码；

所述密钥管理服务器将查询到的用户账户以及用户密码返回至所述用户终端。

4、如权利要求 1 所述的方法，其特征在于，所述密钥存储请求中还携带用户信息以及网站信息，在所述密钥管理服务器将所述用户标识与所述密钥信息对应存储至所述密钥存储空间之后，还包括：

所述密钥管理服务器根据所述用户信息、所述网站信息、所述用户标识以及所述待存储密钥生成用户索引。

5、如权利要求 4 所述的方法，其特征在于，在所述密钥管理服务器将所述用户标识与所述密钥信息对应存储至所述密钥存储空间之后，还包括：

当接收到来自于所述用户中的密钥检索请求时，根据所述密钥检索请求中携带的关键词以及所述用户索引生成搜索结果，并将所述搜索结果返回至所述用户终端。

6、一种服务器，用于作为密钥管理服务器应用于包括所述密钥管理服务器、用户终端以及鉴权服务器的密钥管理系统中，其特征在于，包括：

接收模块，接收来自于用户终端的密钥存储请求，所述密钥存储请求中携带有临时认证令牌、密钥信息以及用户标识，所述临时认证令牌为用户在登录所述鉴权服务器后由所述鉴权服务器下发至所述用户终端的；

鉴权模块，对所述临时认证令牌进行鉴权；

处理模块，在所述临时认证令牌鉴权通过时，查询服务器自身与所述用户对应的密钥存储空间，并将所述用户标识与所述密钥信息对应存储至所述密钥存储空间中。

7、如权利要求 6 所述的服务器，其特征在于，所述临时认证令牌具体为所述用户终端在所述用户登录所述鉴权服务器后向所述鉴权服务器请求获取的。

8、如权利要求 6 所述的服务器，其特征在于，所述密钥信息至少包括用户账户、用户密码以及网站标识；还包括：

填充模块，在接收到来自于所述用户终端的密钥填写请求时确定所述密钥填写请求对应的目标网站标识，在所述密钥存储空间中查询与所述目标网站标识对应的用户账户以及用户密码，将查询到的用户账户以及用户密码返回至所述用户终端。

9、如权利要求 6 所述的服务器，其特征在于，所述密钥存储请求中还携带用户信息以及网站信息，还包括：

生成模块，根据所述用户信息、所述网站信息、所述用户标识以及所述待存储密钥生成用户索引。

10、如权利要求 9 所述的服务器，其特征在于，

所述生成模块还在接收到来自于所述用户中的密钥检索请求时根据所述密钥检索请求中携带的关键词以及所述用户索引生成搜索结果，并将所述搜索结果返回至所述用户终端。

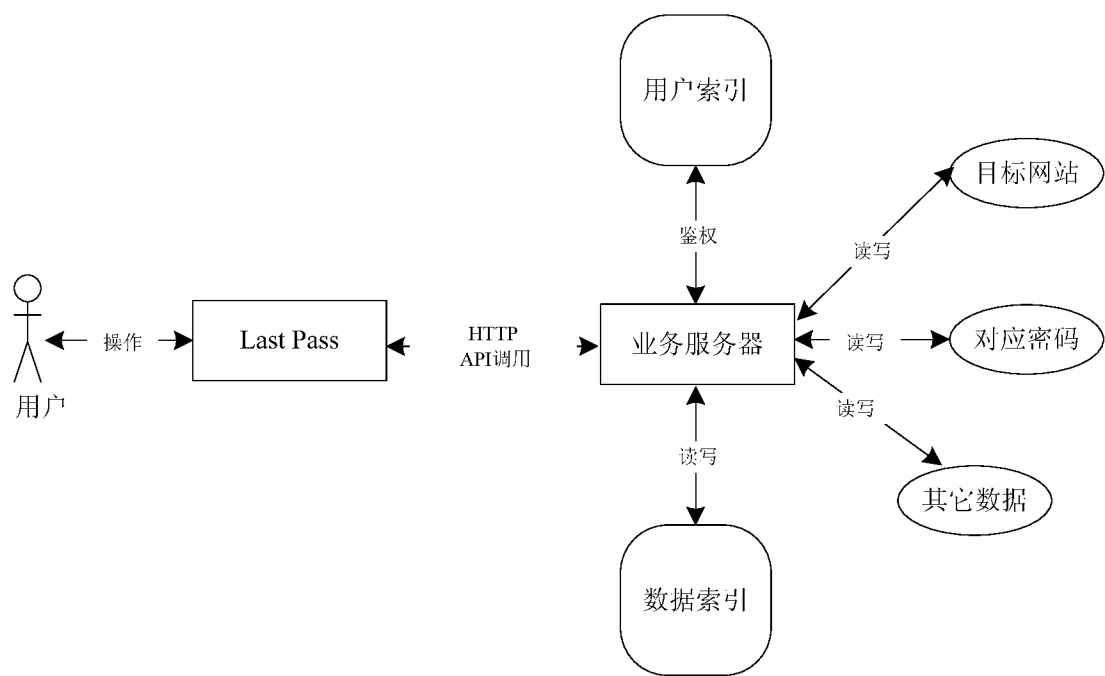


图 1

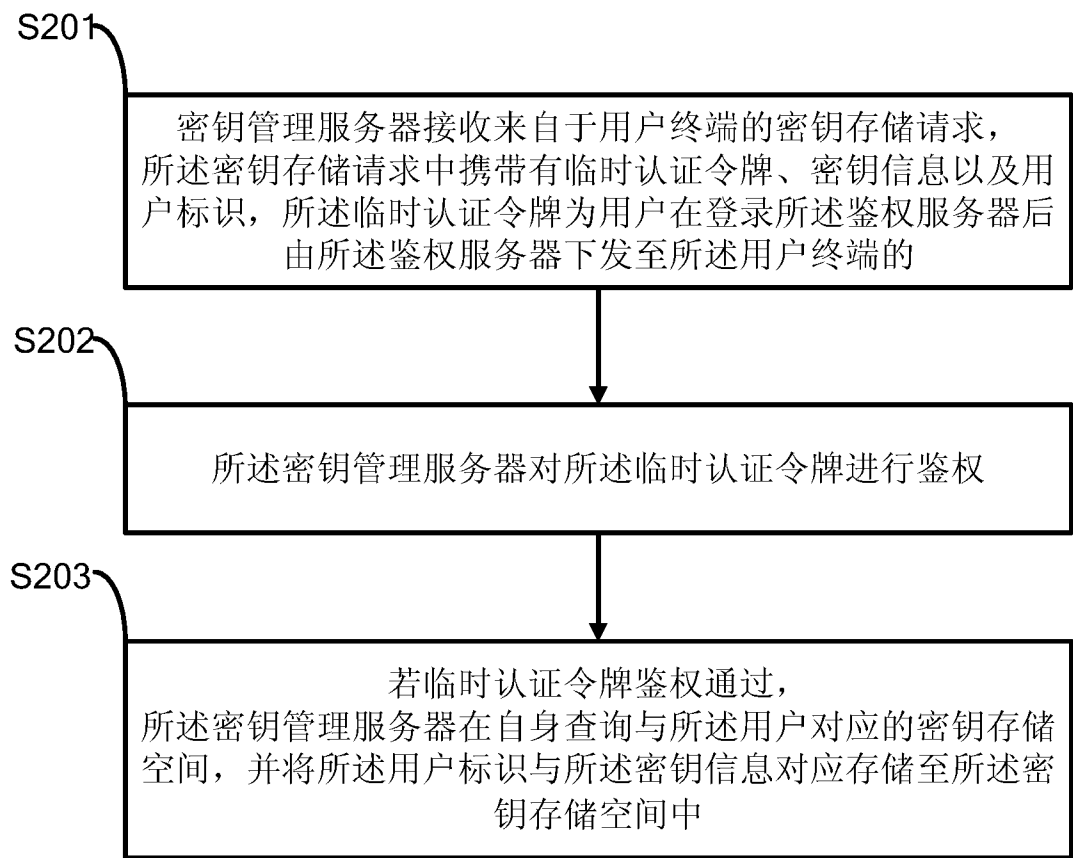


图 2

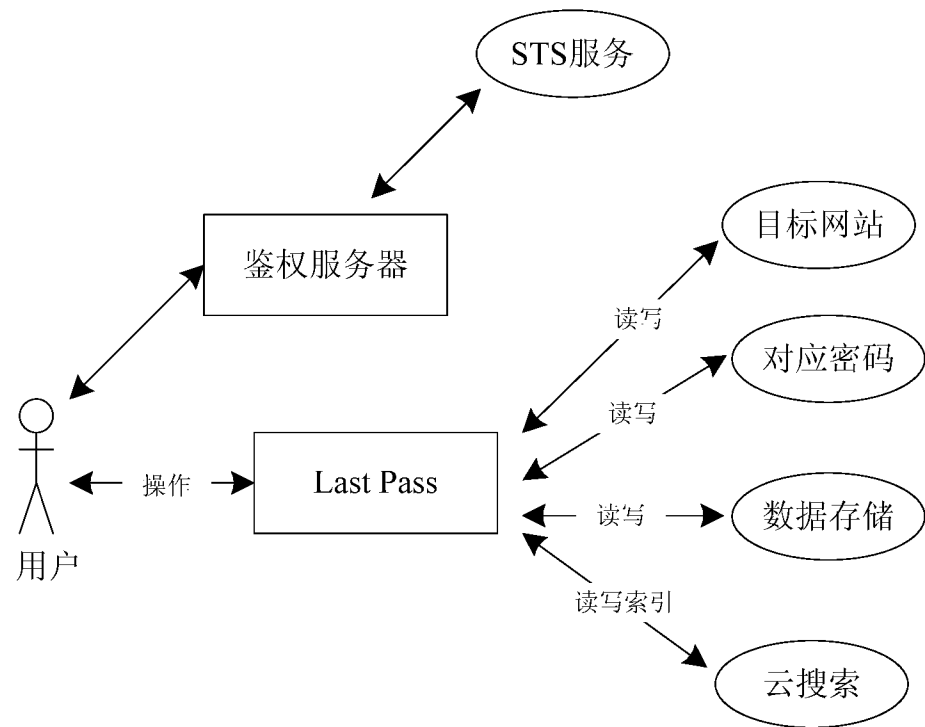


图 3

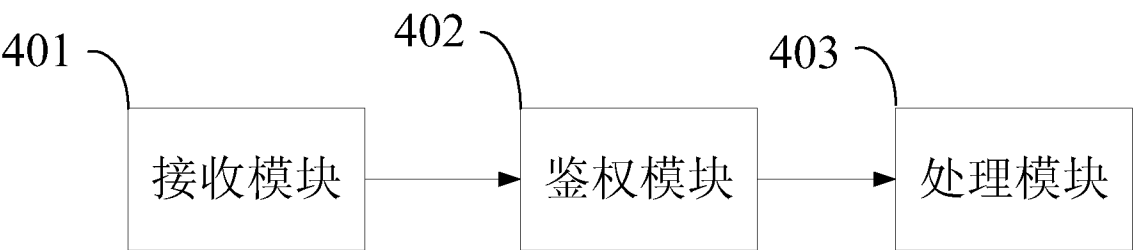


图 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/105668

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; H04Q; H04W

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: ZHANG, Zhizhong; ALIBABA; mobile station, login, user name, registered name, account number, nickname, key, pass code, authentication code, verification code, disposable, temporary, single, dynamic, authentication, verification, user, client, terminal, phone, PC, account, nick, name, password, token, passport, manage, storage, store, memory, save, buffer, multi, many, plentiful

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 103929306 A (TENDYRON CORPORATION), 16 July 2014 (16.07.2014), description, paragraphs [0056]-[00165]	1-10
Y	CN 103023875 A (UNITED ELECTRONICS CO., LTD.), 03 April 2013 (03.04.2013), description, paragraphs [0002], [0036] and [0057]-[0061]	1-10
Y	WO 2015149582 A1 (TENDYRON CORPORATION), 08 October 2015 (08.10.2015), description, page 6, last paragraph to page 21, paragraph 8	1-10

☐ 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 20 January 2017 (20.01.2017)	Date of mailing of the international search report 09 February 2017 (09.02.2017)
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 NING, Bo Telephone No.: (86-10) 62413288

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2016/105668

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103929306 A	16 July 2014	None	
CN 103023875 A	03 April 2013	None	
WO 2015149582 A1	08 October 2015	CN 103929307 A	16 July 2014

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; H04Q; H04W 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, EPDOC, CNKI: 张治中, 阿里巴巴, 客户, 用户, 移动台, 登陆, 登录, 用户名, 注册名, 帐号, 账户, 昵称, 多, 管理, 储存, 存储, 保存, 密码, 密钥, 口令, 通行证, 通行码, 认证码, 验证码, 一次性, 临时, 单次, 动态, 认证, 鉴权, 验证, user, client, terminal, phone, PC, account, nick, name, password, token, passport, manage, storage, store, memory, save, buffer, multi, many, plentiful		
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 103929306 A (天地融科技股份有限公司) 2014年 7月 16日 (2014 - 07 - 16) 说明书第[0056]-[00165]段	1-10
Y	CN 103023875 A (北京荣之联科技股份有限公司) 2013年 4月 3日 (2013 - 04 - 03) 说明书第[0002]、[0036]、[0057]-[0061]段	1-10
Y	WO 2015149582 A1 (天地融科技股份有限公司) 2015年 10月 8日 (2015 - 10 - 08) 说明书第6页最后一段至第21页第8段	1-10
☐ 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 2017年 1月 20日		国际检索报告邮寄日期 2017年 2月 9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) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10) 62019451		受权官员 宁波 电话号码 (86-10) 62413288

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/105668

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	103929306	A	2014年 7月 16日	无			
CN	103023875	A	2013年 4月 3日	无			
WO	2015149582	A1	2015年 10月 8日	CN	103929307	A	2014年 7月 16日