(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 106209749 B
(45)授权公告日 2020.09.25

(21)申请号 201510231075.5
(22)申请日 2015.05.08
(65)同一申请的已公布的文献号
申请公布号 CN 106209749 A
(43)申请公布日 2016.12.07
(73)专利权人 阿里巴巴集团控股有限公司
地址 英属开曼群岛大开曼资本大厦一座四层847号邮箱
(72)发明人 方强 彭骏涛 朱红儒
(74)专利代理机构 北京清源汇知识产权代理事务所(特殊普通合伙) 11644
代理人 冯德魁
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)
G06F 21/41(2013.01)

(56)对比文件
CN 103188237 A,2013.07.03
CN 103179134 A,2013.06.26
CN 103051630 A,2013.04.17
US 2004158574 A1,2004.08.12
CN 104580184 A,2015.04.29
CN 101651666 A,2010.02.17
CN 101202753 A,2008.06.18

审查员 朱星杰

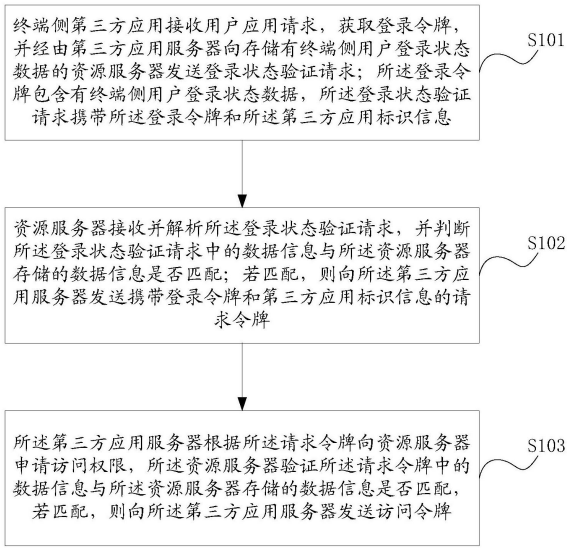
权利要求书6页 说明书16页 附图5页

(54)发明名称

单点登录方法及装置、相关设备和应用的处理方法及装置

(57)摘要

一种基于登录状态的单点登录方法及装置，包括：终端侧第三方应用接收用户应用请求，获取登录令牌，并经第三方应用服务器向存储有终端侧用户登录状态数据的资源服务器发送登录状态验证请求；登录令牌包含有终端侧用户登录状态数据，登录状态验证请求携带登录令牌和第三方应用标识信息；资源服务器接收并解析登录状态验证请求，判断登录状态验证请求中的数据信息与资源服务器存储的数据信息是否匹配；第三方应用服务器根据请求令牌向资源服务器申请访问权限，资源服务器验证请求令牌中的数据信息与资源服务器存储的数据信息是否匹配，向第三方应用服务器发送访问令牌；从而避免多次弹出登录框；本发明还提供相关设备和应用的处理方法及装置。



CN 106209749 B

1.一种基于登录状态的单点登录方法,其特征在于,包括:

终端侧第三方应用接收用户应用请求,获取登录令牌,并经由第三方应用服务器向存储有终端侧用户登录状态数据的资源服务器发送登录状态验证请求;所述登录令牌包含有终端侧用户登录状态数据,所述登录状态验证请求携带所述登录令牌和所述第三方应用标识信息;

所述资源服务器接收并解析所述登录状态验证请求,并判断所述登录状态验证请求中的数据信息与所述资源服务器存储的数据信息是否匹配;若匹配,则向所述第三方应用服务器发送携带登录令牌和第三方应用标识信息的请求令牌;

所述第三方应用服务器根据所述请求令牌向资源服务器申请访问权限,所述资源服务器验证所述请求令牌中的数据信息与所述资源服务器存储的数据信息是否匹配,若匹配,则向所述第三方应用服务器发送访问令牌;

其中,所述获取登录令牌,包括:

所述终端侧将用户的登录请求发送至所述资源服务器;并接收所述资源服务器返回的根据所述登录请求生成的登录令牌;所述登录请求包括:所述终端侧标识信息和用户账户信息;所述登录令牌包括:终端侧标识、终端侧临时ID和登录状态值。

2.根据权利要求1所述的基于登录状态的单点登录方法,其特征在于:所述终端侧接收所述资源服务器返回的根据所述登录请求生成的登录令牌,包括:

所述终端侧接收所述资源服务器发送的所述登录令牌的失效时间选择请求。

3.根据权利要求1所述的基于登录状态的单点登录方法,其特征在于:所述终端侧向所述第三方应用服务器发送的登录令牌,和向所述资源服务器发送的登录请求,采用对称加密方式对所述登录令牌和登录请求中的数据加密传输。

4.根据权利要求1所述的基于登录状态的单点登录方法,其特征在于:向所述第三方应用服务器发送携带登录令牌和第三方应用标识信息的请求令牌,还包括:

所述资源服务器向所述终端侧发送授权服务选择请求;

所述资源服务器接收所述终端侧用户根据所述授权服务选择请求所选择的授权服务内容。

5.根据权利要求1所述的基于登录状态的单点登录方法,其特征在于:包括:

封装所述经由第三方应用服务器向存储有终端侧用户登录状态数据的资源服务器发送的登录状态验证请求;

封装所述第三方应用服务器接收的携带登录令牌和第三方应用标识信息的请求令牌;

封装所述第三方应用服务器接收的访问令牌。

6.根据权利要求5所述的基于登录状态的单点登录方法,其特征在于:所述第三方应用服务器向所述资源服务器发送登录状态验证请求,和所述第三方应用服务器根据所述请求令牌向资源服务器申请访问权限,采用非对称加密的方式,对所述登录状态验证请求和申请访问权限中的数据加密及传输。

7.根据权利要求1所述的基于登录状态的单点登录方法,其特征在于:所述终端标识信息通过所述用户的MAC地址与SIM卡中的身份信息串联哈希获得。

8.根据权利要求1所述的基于登录状态的单点登录方法,其特征在于:所述登录令牌是所述资源服务器根据所述应用请求中的数据信息以及登录状态数据哈希获得。

9.根据权利要求1所述的基于登录状态的单点登录方法，其特征在于：所述请求令牌是所述资源服务器根据所述登录令牌和所述第三方应用标识哈希获得。

10.根据权利要求1所述的基于登录状态的单点登录方法，其特征在于：所述访问令牌是所述资源服务器根据所述请求令牌和所述第三方应用标识哈希获得。

11.根据权利要求1所述的基于登录状态的单点登录方法，其特征在于：向所述第三方应用服务器发送访问令牌，包括：所述资源服务器存储所述访问令牌，并删除所述登录令牌和请求令牌。

12.一种基于登录状态的单点登录装置，其特征在于，包括：

终端管理单元，用于终端侧第三方应用接收用户应用请求，获取登录令牌，并经由第三方应用管理单元向存储有终端侧用户登录状态数据的授权认证登录管理单元发送登录状态验证请求；所述登录令牌包含有终端侧用户登录状态数据，所述登录状态验证请求携带所述登录令牌和所述第三方应用标识信息；

授权认证登录管理单元，用于接收并解析所述登录状态验证请求，并判断所述登录状态验证请求中的数据信息与所述授权认证登录管理单元中存储的数据信息是否匹配；若匹配，则向所述第三方应用管理单元发送携带登录令牌和第三方应用标识信息的请求令牌；

第三方应用管理单元，用于根据所述请求令牌向所述授权认证登录管理单元申请访问权限，所述授权认证登录管理单元验证所述请求令牌中的数据信息与所述授权认证登录管理单元存储的数据信息是否匹配，若匹配，则向所述第三方应用管理单元发送访问令牌；

其中，所述终端管理单元包括：

登录令牌获取单元，用于终端侧将用户的登录请求发送至资源服务器，并接收所述资源服务器返回的根据所述登录请求生成的登录令牌；所述登录请求包括：所述终端侧标识信息和用户账户信息；所述登录令牌包括：终端侧标识、终端侧临时ID和登录状态值。

13.根据权利要求12所述的基于登录状态的单点登录装置，其特征在于，所述登录令牌获取单元包括：

失效时间选择单元，用于接收所述资源服务器发送的所述登录令牌的失效时间选择请求。

14.根据权利要求12所述的基于登录状态的单点登录装置，其特征在于，所述终端管理单元包括：

第一数据加密传输单元，用于所述终端侧向所述第三方应用服务器发送的登录令牌，和向所述资源服务器发送的登录请求，采用对称加密方式对所述登录令牌和登录请求中的数据加密传输。

15.根据权利要求12所述基于登录状态的单点登录装置，其特征在于，所述授权认证管理单元包括：

授权服务选择请求发送单元，用于资源服务器向终端侧发送授权服务选择请求；

授权服务选择接收单元，用于所述终端侧获取所述用户根据所述授权服务选择请求所选择的授权服务内容，并发送至所述资源服务器。

16.根据权利要求12所述基于登录状态的单点登录装置，其特征在于，所述第三方应用管理单元包括：

封装单元，用于封装所述经由第三方应用服务器向存储有终端侧用户登录状态数据的

资源服务器发送的登录状态验证请求;所述第三方应用服务器接收的携带登录令牌和第三方应用标识信息的请求令牌;和所述第三方应用服务器接收的访问令牌。

17.根据权利要求16所述的基于登录状态的单点登录装置,其特征在于,所述第三方应用管理单元包括:

第二数据加密传输单元,用于所述第三方应用服务器向所述资源服务器发送登录状态验证请求,和所述第三方应用服务器根据所述请求令牌向资源服务器申请访问权限,采用非对称加密的方式,对所述登录状态验证请求和申请访问权限中的数据加密及传输。

18.一种基于登录状态的终端侧发送登录请求的方法,其特征在于,包括:

终端侧第三方应用接收应用请求获取登录令牌;

并经由第三方应用服务器向存储有终端侧用户登录状态数据的资源服务器发送登录状态验证请求;所述登录令牌包含有终端侧用户登录状态数据,所述登录状态验证请求携带所述登录令牌和所述第三方应用标识信息;

其中,所述资源服务器接收并解析所述登录状态验证请求,并判断所述登录状态验证请求中的数据信息与所述资源服务器存储的数据信息是否匹配;若匹配,则向所述第三方应用服务器发送携带登录令牌和第三方应用标识信息的请求令牌;

所述第三方应用服务器根据所述请求令牌向资源服务器申请访问权限,所述资源服务器验证所述请求令牌中的数据信息与所述资源服务器存储的数据信息是否匹配,若匹配,则向所述第三方应用服务器发送访问令牌;

所述获取登录令牌,包括:

所述终端侧将用户的登录请求发送至所述资源服务器;并接收所述资源服务器返回的根据所述登录请求生成的登录令牌;所述登录请求包括:所述终端侧标识信息和用户账户信息;所述登录令牌包括:终端侧标识、终端侧临时ID和登录状态值。

19.根据权利要求18所述的基于登录状态的终端侧发送登录请求的方法,其特征在于,所述终端侧接收所述资源服务器返回的根据所述登录请求生成的登录令牌,包括:

所述终端侧接收所述资源服务器发送的所述登录令牌的失效时间选择请求。

20.根据权利要求18所述的基于登录状态的终端侧发送登录请求的方法,其特征在于:所述终端侧向所述第三方应用服务器发送的登录令牌,和向所述资源服务器发送的登录请求,采用对称加密方式对所述登录令牌和登录请求中的数据加密传输。

21.一种基于登录状态的终端侧发送登录请求的装置,其特征在于,包括:

终端管理单元,用于终端侧第三方应用接收用户应用请求,获取登录令牌,并经由第三方应用管理单元向存储有终端侧用户登录状态数据的授权认证登录管理单元发送登录状态验证请求;所述登录令牌包含有终端侧用户登录状态数据,所述登录状态验证请求携带所述登录令牌和所述第三方应用标识信息;

其中,所述授权认证登录管理单元,用于接收并解析所述登录状态验证请求,并判断所述登录状态验证请求中的数据信息与所述授权认证登录管理单元中存储的数据信息是否匹配;若匹配,则向所述第三方应用管理单元发送携带登录令牌和第三方应用标识信息的请求令牌;

所述第三方应用管理单元,用于根据所述请求令牌向所述授权认证登录管理单元申请访问权限,所述授权认证登录管理单元验证所述请求令牌中的数据信息与所述授权认证登

录管理单元存储的数据信息是否匹配，若匹配，则向所述第三方应用管理单元发送访问令牌；

所述终端管理单元包括：

登录令牌获取单元，用于所述终端侧将用户的登录请求发送至资源服务器；并接收所述资源服务器返回的根据所述登录请求生成的登录令牌；所述登录请求包括：所述终端侧标识信息和用户账户信息；所述登录令牌包括：终端侧标识、终端侧临时ID和登录状态值。

22.根据权利要求21所述的基于登录状态的终端侧发送登录请求的装置，其特征在于，所述登录令牌获取单元包括：

失效时间选择单元，用于接收所述资源服务器发送的所述登录令牌的失效时间选择请求。

23.根据权利要求21所述的基于登录状态的终端侧发送登录请求的装置，其特征在于，包括：

第一数据加密传输单元，用于所述终端侧向所述第三方应用服务器发送的登录令牌，和向所述资源服务器发送的登录请求，采用对称加密方式对所述登录令牌和登录请求中的数据加密传输。

24.一种基于登录状态的资源服务器授权认证方法，其特征在于，包括：

资源服务器接收并解析来自第三方应用服务器发送的登录状态验证请求；

判断所述登录状态验证请求中的数据信息与所述资源服务器存储的数据信息是否匹配；若匹配，则向所述第三方应用服务器发送携带登录令牌和第三方应用标识信息的请求令牌；

其中，所述资源服务器接收并解析的登录状态验证请求是通过下述方式获得：

接收来自终端侧第三方应用通过接收用户应用请求，获取登录令牌后，并经由所述第三方应用服务器向存储有终端侧用户登录状态数据的资源服务器发送的登录状态验证请求；所述登录令牌包含有终端侧用户登录状态数据，所述登录状态验证请求携带所述登录令牌和所述第三方应用标识信息；

所述获取登录令牌，包括：

所述终端侧将用户的登录请求发送至所述资源服务器；并接收所述资源服务器返回的根据所述登录请求生成的登录令牌；所述登录请求包括：所述终端侧标识信息和用户账户信息；所述登录令牌包括：终端侧标识、终端侧临时ID和登录状态值；

当所述资源服务器判断出所述登录状态验证请求中的数据信息与所述资源服务器存储的数据信息匹配、向所述第三方应用服务器发送携带登录令牌和第三方应用标识信息的请求令牌之后，还包括：

所述第三方应用服务器根据所述请求令牌向所述资源服务器申请访问权限，所述资源服务器验证所述请求令牌中的数据信息与所述资源服务器存储的数据信息是否匹配，若匹配，则向所述第三方应用服务器发送访问令牌。

25.根据权利要求24所述的基于登录状态的资源服务器授权认证方法，其特征在于：向所述第三方应用服务器发送携带登录令牌和第三方应用标识信息的请求令牌，还包括：

所述资源服务器向所述终端侧发送授权服务选择请求；

终端侧获取用户根据所述授权服务选择请求所选择的授权服务内容，并发送至所述资

源服务器。

26.一种基于登录状态的资源服务器授权认证装置,其特征在于,包括:

授权认证登录管理单元,用于接收并解析所述登录状态验证请求,并判断所述登录状态验证请求中的数据信息与所述授权认证登录管理单元中存储的数据信息是否匹配;若匹配,则向第三方应用管理单元发送携带登录令牌和第三方应用标识信息的请求令牌;

其中,所述授权认证登录管理单元接收并解析的登录状态验证请求是通过如下方式获得:

接收来自终端管理单元通过接收用户应用请求,获取登录令牌后,并经由所述第三方应用管理单元向存储有终端侧用户登录状态数据的授权认证登录管理单元发送的登录状态验证请求;所述登录令牌包含有终端侧用户登录状态数据,所述登录状态验证请求携带所述登录令牌和所述第三方应用标识信息;

所述终端管理单元包括:

登录令牌获取单元,用于所述终端侧将用户的登录请求发送至所述资源服务器;并接收所述资源服务器返回的根据所述登录请求生成的登录令牌;所述登录请求包括:所述终端侧标识信息和用户账户信息;所述登录令牌包括:终端侧标识、终端侧临时ID和登录状态值;

当所述授权认证登录管理单元判断出所述登录状态验证请求中的数据信息与所述授权认证登录管理单元存储的数据信息匹配、并向所述第三方应用管理单元发送携带登录令牌和第三方应用标识信息的请求令牌之后,还包括:

所述第三方应用管理单元根据所述请求令牌向所述授权认证登录管理单元申请访问权限,所述授权认证登录管理单元验证所述请求令牌中的数据信息与所述授权认证登录管理单元存储的数据信息是否匹配,若匹配,则向所述第三方应用管理单元发送访问令牌。

27.根据权利要求26所述的基于登录状态的资源服务器授权认证装置,其特征在于,所述授权认证登录管理单元包括:

授权服务选择请求发送单元,用于所述资源服务器向终端侧发送授权服务选择请求;

授权服务选择接收单元,用于所述终端侧获取用户根据所述授权服务选择请求所选择的授权服务内容,并发送至所述资源服务器。

28.一种基于登录状态的第三方应用访问权限请求方法,其特征在于,包括:

第三方应用服务器接收来自资源服务器发送的携带登录令牌和第三方应用标识信息的请求令牌,所述登录令牌包含有终端侧用户登录状态数据;

所述第三方应用服务器根据所述请求令牌向资源服务器申请访问权限,所述资源服务器验证所述请求令牌中的数据信息与所述资源服务器存储的数据信息是否匹配,若匹配,则所述第三方应用服务器接收所述资源服务器发送的访问令牌。

29.根据权利要求28所述的基于登录状态的第三方应用访问权限请求方法,其特征在于,包括:

封装经由第三方应用服务器向存储有终端侧用户登录状态数据的资源服务器发送的登录状态验证请求;

封装所述第三方应用服务器接收的携带登录令牌和第三方应用标识信息的请求令牌;

封装所述第三方应用服务器接收的访问令牌。

30.根据权利要求29所述的基于登录状态的第三方应用访问权限请求方法，其特征在于：所述第三方应用服务器向所述资源服务器发送登录状态验证请求，和所述第三方应用服务器根据所述请求令牌向资源服务器申请访问权限，采用非对称加密的方式，对所述登录状态验证请求和申请访问权限中的数据加密及传输。

31.一种基于登录状态的第三方应用访问权限请求的装置，其特征在于，包括：

第三方应用管理单元，用于根据请求令牌向授权认证登录管理单元申请访问权限，所述授权认证登录管理单元验证所述请求令牌中的数据信息与所述授权认证登录管理单元存储的数据信息是否匹配，若匹配，则向所述第三方应用管理单元发送访问令牌；

所述请求令牌携带登录令牌和第三方应用标识信息，所述登录令牌包含有终端侧用户登录状态数据。

32.根据权利要求31所述的基于登录状态的第三方应用访问权限请求的装置，其特征在于，所述第三方应用管理单元包括：

封装单元，用于封装所述第三方应用管理单元中所述登录令牌、所述请求令牌以及所述访问令牌的数据信息。

33.根据权利要求32所述的基于登录状态的第三方应用访问权限请求的装置，其特征在于，所述第三方应用管理单元包括：

第二数据加密传输单元，用于所述第三方应用服务器向资源服务器发送登录状态验证请求，和所述第三方应用服务器根据所述请求令牌向资源服务器申请访问权限，采用非对称加密的方式，对所述登录状态验证请求和申请访问权限中的数据加密及传输。

单点登录方法及装置、相关设备和应用的处理方法及装置

技术领域

[0001] 本申请涉及计算机通信领域，具体涉及一种单点登录的方法及装置，相关设备和应用的处理方法及装置。

背景技术

[0002] 单点登录(Single Sign On)，简称为SSO，是目前比较流行的企业业务整合的解决方案之一。SSO的定义是在多个应用系统中，用户只需要登录一次就可以访问所有相互信任的应用系统，也就是说，将登录映射到其他应用中用于同一个用户的登录的机制。

[0003] 在单点登录模式中通常存在以下三个要素::Gatekeeper(入口检查单元)、Authenticator(身份认证单元)和Credential Store(用户凭证存储单元)，其中，Gatekeeper:对用户的请求进行验证和重定向;Authenticatior:对用户进行认证;Credential Srore:凭证库存放认证的凭证或票据;一个单点登录的过程通常包括以下四个阶段：

[0004] 用户向资源拥有者发起请求，请求经过Gatekeeper，Gatekeeper会验证用户是否已经建立与资源拥有者的会话，若没有则验证是否具备单点登录会话。

[0005] 当Gatekeeper发现未建立单点登录会话时，用户被重定向至认证者页面，提示用户输入账户信息，认证者对账户信息进行校验，若成功则为用户建立Login session。

[0006] 认证者对login session进行校验，验证成功后Gatekeeper建立Login session。

[0007] 认证者实现Token重定向实现认证者和Gatekeeper的通信。

[0008] 目前主流的SSO协议有OPENID、SAML(Security Assertion Markup Language)、CAS(Central Authentication Service)和Oauth(Open Authorization)等;下面就上述SAML和Oauth协议进行介绍：

[0009] 一、SAML

[0010] SAML是一种基于XML的安全描述语言，利用XML对认证和授权信息进行编码实现在异构安全系统间信息的交换和处理。互联网发展至今天，各种网络应用层出不穷，用户为了保护自己的个人信息，需要通过口令的方式作为个人信息的安全保障，然而，若每个站点都需要各自的一套口龙，用户将有难以控制的大量口令。所以SSO单点登录理念开始流行，通过SSO，某个Web站点可以与其他站点共享用户身份信息，SAML就是这种通信协议。

[0011] SAML实现用户通过认证提供方(IDP)授权获取认证，将IDP颁发的口令作为凭证去登入目标站点，目标站点可以通过口令确认用户的信息。

[0012] SAML标准主要由声明和请求/响应协议两部分构成。声明是SAML的基本数据对象，是对主体(用户、计算机)的安全信息(身份、权限等)的XML描述形式。SAML声明能够传递三种信息:主体完成认证行为的信息、主体的属性信息以及关于主体是否允许访问特定资源的授权决议信息。因此，对应的SAML声明包括三种形式:认证声明、属性声明和授权决议声明。其中认证声明描述与认证成功事件相关的信息(如认证的机构、方式和有效期等);授权决议声明描述许可权查询和检查的结果，决定是否接受主体对资源的访问请求;属性声明

描述与主体的认证和授权决议相关的信息(如主体的标志、所属用户组、角色、可访问的资源及权限等)

[0013] 如图1所示,图1是SAML的工作流程图,其实现步骤如下:

[0014] 1)Subject向IDP请求凭证(方法是提交用户名、密码);

[0015] 2)IDP通过验证Subject提供的信息,来确定是否提供凭证以及将服务请求同时提交给SP;

[0016] 3)假如Subject的验证信息正确,他将获取IDP的凭证以及将服务请求同时提交给SP;

[0017] 4)SP接受到Subject的凭证,它是提供服务之前必须验证此凭证,于是,它产生了一个SAML请求,要求IDP对凭证断言;

[0018] 5)凭证是IDP产生的,它当然知道凭证的内容,于是它回应一个SAML断言给SP;

[0019] 6)SP信任IDP的SAML断言,它会根据断言结果确定是否为Subject提供服务。

[0020] 二、Oauth协议

[0021] Oauth是一种开放的协议,为桌面程序或者基于B/S的web应用提供了一种简单的,标准的方式去访问需要用户授权的API服务。Oauth认证协议具备简单、安全、开放的特点。

[0022] Oauth认证协议包含三个带有认证信息的URL,分别是:

[0023] a.User Authorization URL:授权Request Token访问地址;

[0024] b.Request Token URL:未授权Request Token访问地址;

[0025] c.Access Token URL:Access Token访问地址。

[0026] 如图2所示,图2为Oauth工作流程如下:

[0027] 1)用户点击第三方应用,第三方应用向认证服务器发起请求request_token。

[0028] 2)认证服务器创建token及密钥并发送给第三方应用。

[0029] 3)第三方应用将用户重定向。

[0030] 4)认证服务器向用户发起申请,请求授权。

[0031] 5)用户进行授权。

[0032] 6)认证服务器将用户重定向至第三方应用服务器。

[0033] 7)第三方应用服务器向认证服务器申请access_token。

[0034] 8)认证服务器创建Access_token并发放给第三方服务器。

[0035] 9)第三方服务器利用access_token申请认证服务器上的用户资源。

[0036] 上述的两种协议均存在各自的缺点,例如:通过Oauth协议进行登录,由于不存在多个第三方应用可以复用令牌机制,这就造成当更换第三方应用程序进行登录时需要再次弹出登录对话框,从而使得用户体验很不好,尤其在一些对操作简易型要求较高的应用场景中,若采用这种认证授权协议,可能会造成其他的对用户使用的影响;且在进行用户授权过程中,需要第三方应用服务器对用户登录请求进行重定向至认证服务器,授权完成后重定向用户操作至第三方应用,两次重定向会对用户的使用产生影响,且存在重定向过程中数据截获的可能性。而SAML协议,能够实现单次登录多次授权,但由于基于XML的设计,授权服务器中的授权模块仅可完成在开发阶段进行授权内容的更改,且SAML协议在作为单点登录限制使用时,其作用为通过断言对用户在认证服务器已经注册过的权限内容进行验证。在这种机制下,通过SAML协议无法实现用户对第三方应用的权限管理,用户体验不好。

[0037] 如何提供一种单点登录的方法，能够解决多应用授权重复申请及用户无法再次选择向第三方应用授权内容的不足，提高现有单点登录认证协议的破解难度并改善用户体验。

发明内容

[0038] 本申请提供一种基于登录状态的单点登录方法及装置，终端侧发送登录请求的方法及装置，资源服务器授权认证方法及装置，第三方应用访问权限请求方法及装置，以解决现有上述技术问题。

[0039] 本申请提供一种基于登录状态的单点登录方法，包括：

[0040] 终端侧第三方应用接收用户应用请求，获取登录令牌，并经由第三方应用服务器向存储有终端侧用户登录状态数据的资源服务器发送登录状态验证请求；所述登录令牌包含有终端侧用户登录状态数据，所述登录状态验证请求携带所述登录令牌和所述第三方应用标识信息；

[0041] 资源服务器接收并解析所述登录状态验证请求，并判断所述登录状态验证请求中的数据信息与所述资源服务器存储的数据信息是否匹配；若匹配，则向所述第三方应用服务器发送携带登录令牌和第三方应用标识信息的请求令牌；

[0042] 所述第三方应用服务器根据所述请求令牌向资源服务器申请访问权限，所述资源服务器验证所述请求令牌中的数据信息与所述资源服务器存储的数据信息是否匹配，若匹配，则向所述第三方应用服务器发送访问令牌。

[0043] 优选的，所述获取登录令牌，包括：

[0044] 所述终端侧将用户的登录请求发送至所述资源服务器；并接收所述资源服务器返回的根据所述登录请求生成的登录令牌；所述登录请求包括：所述终端侧标识信息和用户账户信息；所述登录令牌包括：终端侧标识、终端侧临时ID和登录状态值。

[0045] 优选的，所述终端侧接收所述资源服务器返回的根据所述登录请求生成的登录令牌，包括：所述终端侧接收所述资源服务器发送的所述登录令牌的失效时间选择请求。

[0046] 优选的，所述终端侧向所述第三方应用服务器发送的登录令牌，和向所述资源服务器发送的登录请求，采用对称加密方式对所述登录令牌和登录请求中的数据加密传输。

[0047] 优选的，向所述第三方应用服务器发送携带登录令牌和第三方应用标识信息的请求令牌，还包括：所述资源服务器向所述终端侧发送授权服务选择请求；所述资源服务器接收所述终端侧用户根据所述授权服务选择请求所选择的授权服务内容。

[0048] 优选的，包括：封装所述经由第三方应用服务器向存储有终端侧用户登录状态数据的资源服务器发送的登录状态验证请求；封装所述第三方应用服务器接收的携带登录令牌和第三方应用标识信息的请求令牌；封装所述第三应用服务器接收的访问令牌。

[0049] 优选的，所述第三方应用服务器向所述资源服务器发送登录状态验证请求，和所述第三方应用服务器根据所述请求令牌向资源服务器申请访问权限，采用非对称加密的方式，对所述登录状态验证请求和申请访问权限中的数据加密及传输。

[0050] 优选的，所述终端标识信息通过所述用户的MAC地址与SIM卡中的身份信息串联哈希获得。

[0051] 优选的，所述登录令牌是所述资源服务器根据所述应用请求中的数据信息以及登

录状态数据哈希获得。

[0052] 优选的，所述请求令牌是所述资源服务器根据所述登录令牌和所述第三方应用标识哈希获得。

[0053] 优选的，所述访问令牌是所述资源服务器根据所述请求令牌和所述第三方应用标识哈希获得。

[0054] 优选的，向所述第三方应用服务器发送访问令牌，包括：所述资源服务器存储所述访问令牌，并删除所述登录令牌和请求令牌。

[0055] 本申请还提供一种基于登录状态的单点登录装置，包括：

[0056] 终端管理单元，用于终端侧第三方应用接收用户应用请求，获取登录令牌，并经由第三方应用管理单元向存储有终端侧用户登录状态数据的授权认证登录管理单元发送登录状态验证请求；所述登录令牌包含有终端侧用户登录状态数据，所述登录状态验证请求携带所述登录令牌和所述第三方应用标识信息；

[0057] 授权认证管理单元，用于接收并解析所述登录状态验证请求，并判断所述登录状态验证请求中的数据信息与所述授权认证登录管理单元中存储的数据信息是否匹配；若匹配，则向所述第三方应用管理单元发送携带登录令牌和第三方应用标识信息的请求令牌；

[0058] 第三方应用管理单元，用于根据所述请求令牌向授权认证登录管理单元申请访问权限，所述授权认证登录管理单元验证所述请求令牌中的数据信息与所述授权认证登录管理单元存储的数据信息是否匹配，若匹配，则向所述第三方应用管理单元发送访问令牌。

[0059] 优选的，所述终端管理单元包括：登录令牌获取单元，用于终端侧将用户的登录请求发送至所述资源服务器，并接收所述资源服务器返回的根据所述登录请求生成的登录令牌；所述登录请求包括：所述终端侧标识信息和用户账户信息；所述登录令牌包括：终端侧标识、终端侧临时ID和登录状态值。

[0060] 优选的，所述登录令牌获取单元包括：失效时间选择单元，用于接收所述资源服务器发送的所述登录令牌的失效时间选择请求。

[0061] 优选的，所述终端管理单元包括：第一数据加密传输单元，用于所述终端侧向所述第三方应用服务器发送的登录令牌，和向所述资源服务器发送的登录请求，采用对称加密方式对所述登录令牌和登录请求中的数据加密传输。

[0062] 优选的，所述授权认证管理单元包括：授权服务选择请求发送单元，用于所述资源服务器向终端侧发送授权服务选择请求；授权服务选择接收单元，用于所述终端侧获取所述用户根据所述授权服务选择请求所选择的授权服务内容，并发送至所述资源服务器。

[0063] 优选的，所述第三方应用管理单元包括：封装单元，用于封装所述经由第三方应用服务器向存储有终端侧用户登录状态数据的资源服务器发送的登录状态验证请求；所述第三方应用服务器接收的携带登录令牌和第三方应用标识信息的请求令牌；和所述第三应用服务器接收的访问令牌。

[0064] 优选的，所述第三方应用管理单元包括：第二数据加密传输单元，用于所述第三方应用服务器向所述资源服务器发送登录状态验证请求，和所述第三方应用服务器根据所述请求令牌向资源服务器申请访问权限，采用非对称加密的方式，对所述登录状态验证请求和申请访问权限中的数据加密及传输。

[0065] 本申请还提供一种基于登录状态的终端侧发送登录请求的方法，包括：

[0066] 终端侧第三方应用接收应用请求获取登录令牌；

[0067] 并经由第三方应用服务器向存储有终端侧用户登录状态数据的资源服务器发送登录状态验证请求；所述登录令牌包含有终端侧用户登录状态数据，所述登录状态验证请求携带所述登录令牌和所述第三方应用标识信息。

[0068] 优选的，所述获取登录令牌包括：所述终端侧将用户的登录请求发送至所述资源服务器；并接收所述资源服务器返回的根据所述登录请求生成的登录令牌；所述登录请求包括：所述终端侧标识信息和用户账户信息；所述登录令牌包括：终端侧标识、终端侧临时ID和登录状态值。

[0069] 优选的，所述终端侧接收所述资源服务器返回的根据所述登录请求生成的登录令牌，包括：所述终端侧接收所述资源服务器发送的所述登录令牌的失效时间选择请求。

[0070] 优选的，所述终端侧向所述第三方应用服务器发送的登录令牌，和向所述资源服务器发送的登录请求，采用对称加密方式对所述登录令牌和登录请求中的数据加密传输。

[0071] 本申请还提供一种基于登录状态的终端侧发送登录请求的装置，包括：终端管理单元，用于终端侧第三方应用接收用户应用请求，获取登录令牌，并经由第三方应用管理单元向存储有终端侧用户登录状态数据的授权认证登录管理单元发送登录状态验证请求；所述登录令牌包含有终端侧用户登录状态数据，所述登录状态验证请求携带所述登录令牌和所述第三方应用标识信息。

[0072] 优选的，所述终端管理单元包括：登录令牌获取单元，用于终端侧将用户的登录请求发送至所述资源服务器，并接收所述资源服务器返回的根据所述登录请求生成的登录令牌；所述登录请求包括：所述终端侧标识信息和用户账户信息；所述登录令牌包括：终端侧标识、终端侧临时ID和登录状态值。

[0073] 优选的，所述登录令牌获取单元包括：失效时间选择单元，用于接收所述资源服务器发送的所述登录令牌的失效时间选择请求。

[0074] 优选的，第一数据加密传输单元，用于所述终端侧向所述第三方应用服务器发送的登录令牌，和向所述资源服务器发送的登录请求，采用对称加密方式对所述登录令牌和登录请求中的数据加密传输。

[0075] 本申请还提供一种基于登录状态的资源服务器授权认证方法，包括：

[0076] 资源服务器接收并解析自来第三方应用服务器发送的登录状态验证请求；

[0077] 判断所述登录状态验证请求中的数据信息与所述资源服务器存储的数据信息是否匹配；若匹配，则向所述第三方应用服务器发送携带登录令牌和第三方应用标识信息的请求令牌。

[0078] 优选的，向所述第三方应用服务器发送携带登录令牌和第三方应用标识信息的请求令牌，还包括：

[0079] 所述资源服务器向所述终端侧发送授权服务选择请求；

[0080] 所述终端侧获取所述用户根据所述授权服务选择请求所选择的授权服务内容，并发送至所述资源服务器。

[0081] 本申请还提供一种基于登录状态的资源服务器授权认证装置，包括：

[0082] 授权认证管理单元，用于接收并解析所述登录状态验证请求，并判断所述登录状态验证请求中的数据信息与所述授权认证登录管理单元中存储的数据信息是否匹配；若匹

配，则向所述第三方应用管理单元发送携带登录令牌和第三方应用标识信息的请求令牌。

[0083] 优选的，所述授权认证登录管理单元包括：

[0084] 授权服务选择请求发送单元，用于所述资源服务器向终端侧发送授权服务选择请求；

[0085] 授权服务选择接收单元，用于所述终端侧获取所述用户根据所述授权服务选择请求所选择的授权服务内容，并发送至所述资源服务器。

[0086] 本申请还提供一种基于登录状态的第三方应用访问权限请求方法，包括：

[0087] 第三方应用服务器接收来自资源服务器发送的携带登录令牌和第三方应用标识信息的请求令牌；

[0088] 所述第三方应用服务器根据所述请求令牌向资源服务器申请访问权限，所述资源服务器验证所述请求令牌中的数据信息与所述资源服务器存储的数据信息是否匹配，若匹配，则所述第三方应用服务器接收所述资源服务器发送的访问令牌。

[0089] 优选的，包括：封装所述经由第三方应用服务器向存储有终端侧用户登录状态数据的资源服务器发送的登录状态验证请求；

[0090] 封装所述第三方应用服务器接收的携带登录令牌和第三方应用标识信息的请求令牌；

[0091] 封装所述第三应用服务器接收的访问令牌。

[0092] 优选的，所述第三方应用服务器向所述资源服务器发送登录状态验证请求，和所述第三方应用服务器根据所述请求令牌向资源服务器申请访问权限，采用非对称加密的方式，对所述登录状态验证请求和申请访问权限中的数据加密及传输。

[0093] 本申请还提供一种基于登录状态的第三方应用访问权限请求的装置，包括：第三方应用管理单元，用于根据所述请求令牌向授权认证登录管理单元申请访问权限，所述授权认证登录管理单元验证所述请求令牌中的数据信息与所述授权认证登录管理单元存储的数据信息是否匹配，若匹配，则向所述第三方应用管理单元发送访问令牌。

[0094] 优选的，所述第三方应用管理单元包括：封装单元，用于封装所述第三方应用管理单元中所述登录令牌、所述请求令牌以及所述访问令牌的数据信息。

[0095] 优选的，所述第三方应用管理单元包括：第二数据加密传输单元，用于所述第三方应用服务器向所述资源服务器发送登录状态验证请求，和所述第三方应用服务器根据所述请求令牌向资源服务器申请访问权限，采用非对称加密的方式，对所述登录状态验证请求和申请访问权限中的数据加密及传输。

[0096] 与现有技术相比，本申请提供的一种基于登录状态的单点登录方法，通过引入登录状态，在资源服务器与第三方应用服务器之间验证具有登录状态的令牌信息是否相同，从而一方面，消除第三方应用将用户登录过程重定向及授权结束后再次重定向至第三方应用的过程，在增强对第三方应用安全验证的同时，避免多个第三方应用登录时弹出登录框，增加用户使用的便利性。另一方面，实现经过安全认证授权后才可以访问第三方应用，并在不在本地终端保存证书的情况下实现对第三方应用的动态授权操作，减轻了终端上的代码开发量，并提高了授权过程的安全性。

附图说明

[0097] 为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请中记载的一些实施例，对于本领域普通技术人员来讲，还可以根据这些附图获得其他的附图。

[0098] 图1是现有技术中采用SAML协议实现单点登录的工作流程图；

[0099] 图2是现有技术中采用Oauth协议实现单点登录的工作流程图；

[0100] 图3是本申请提供的一种基于登录状态的单点登录方法实施例的流程图；

[0101] 图4是本申请提供的一种基于登录状态的单点登录装置实施例的结构示意图；

[0102] 图5是本申请提供的一种基于登录状态的终端侧发送登录请求方法的流程图；

[0103] 图6是本申请提供的一种基于登录状态的终端侧发送登录请求装置的结构示意图；

[0104] 图7是本申请提供的一种基于登录状态的资源服务器授权认证方法的流程图；

[0105] 图8是本申请提供的一种基于登录状态的资源服务器授权认证装置的结构示意图；

[0106] 图9是本申请提供的一种基于登录状态的第三方应用访问权限请求方法的流程图；

[0107] 图10是本申请提供的一种基于登录状态的第三方应用访问权限请求装置的结构示意图。

具体实施方式

[0108] 在下面的描述中阐述了很多具体细节以便于充分理解本申请。但是本申请能够以很多不同于在此描述的其它方式来实施，本领域技术人员可以在不违背本申请内涵的情况下做类似推广，因此本申请不受下面公开的具体实施的限制。

[0109] 请参考图3所示，图3是本申请提供的一种基于登录状态的单点登录方法第一实施例的流程图。该方法包括以下步骤：

[0110] 步骤S101：终端侧第三方应用接收用户应用请求，获取登录令牌，并经由第三方应用服务器向存储有终端侧用户登录状态数据的资源服务器发送登录状态验证请求；所述登录令牌包含有终端侧用户登录状态数据，所述登录状态验证请求携带所述登录令牌和所述第三方应用标识信息。

[0111] 步骤S102：资源服务器接收并解析所述登录状态验证请求，并判断所述登录状态验证请求中的数据信息与所述资源服务器存储的数据信息是否匹配；若匹配，则向所述第三方应用服务器发送携带登录令牌和第三方应用标识信息的请求令牌。

[0112] 步骤S103：所述第三方应用服务器根据所述请求令牌向资源服务器申请访问权限，所述资源服务器验证所述请求令牌中的数据信息与所述资源服务器存储的数据信息是否匹配，若匹配，则向所述第三方应用服务器发送访问令牌。

[0113] 下面以终端侧为移动设备，资源服务器为淘宝服务器，第三方应用服务器为微博服务器，详细说明本申请各个步骤的实现过程，具体如下：

[0114] 步骤S101：终端侧第三方应用接收用户应用请求，获取登录令牌，并经由第三方应

用服务器向存储有终端侧用户登录状态数据的资源服务器发送登录状态验证请求;所述登录令牌包含有终端侧用户登录状态数据,所述登录状态验证请求携带所述登录令牌和所述第三方应用标识信息。

[0115] 该步骤中,移动终端上的微博应用接收用户的应用请求,并获取移动终端的登录令牌,获取的登录令牌后经微博服务器向存储有用户登录状态数据的淘宝服务器发送登录状态验证请求。在该步骤中,所述获取登录令牌可以采用如下方式获得:

[0116] 用户向移动终端发起登录请求,此处的登录请求是用户进入所述移动终端时的登录请求。移动终端将登录请求重定向至淘宝服务器;并接收所述淘宝服务器返回的根据所述登录请求生成的登录令牌;所述登录请求中包括:账户信息和终端标识信息等信息;淘宝服务器根据登录请求生成登录令牌(login_token),也就是说,可以根据所述临时ID,终端标识信息和登录状态等哈希获得,因此,所述登录令牌包括:终端侧标识、终端侧临时ID和登录状态值。

[0117] 在移动终端获得登录令牌后,将登录令牌和微博应用标识信息作为登录状态验证请求发送至淘宝服务器,请求淘宝服务器验证登录令牌与淘宝服务器中存储的登录状态数据信息是否相同。

[0118] 其中,所述移动终端能够接收由淘宝服务器发送的临时ID,并存入SIM卡的SE模块划定的安全域中并维护该临时ID,用以查找与该临时ID相对应的用户登录令牌等相关信息。

[0119] 所述移动终端的标识信息可以通过MAC地址与SIM卡中的身份信息串联哈希获得。

[0120] 为便于提高数据的安全性,在本实施中对所述移动终端向所述淘宝服务器发送的登录令牌等数据信息,以及向所述微博服务器发送的登录请求等数据信息,进行加密后传输。为提高数据的安全性,移动终端不保存任何私钥证书,也就是说,移动终端的密钥一次一密,使用一次后自动失效,因此,对于移动终端向所述淘宝服务器(资源服务器)或向微博服务器(第三方应用服务器)发送的数据信息可以采用对称加密的方式。此处所述的数据信息包括:所述登录令牌和第三方应用标识信息进行对称加密处理。

[0121] 所述对称加密可以采用3DES加密算法,即:将所述临时ID、终端侧标识、登录状态和APPkey拼接的数据平均分成三段,构成登录令牌与第三方应用标识的三个密钥,进而申请密文;实现对登录令牌与第三方应用标识的加密。

[0122] 可以理解的是,所述对称加密还可以选用其他加密算法,例如:DES算法,TDEA算法,Blowfish算法,RC5算法或IDEA算法等。

[0123] 在上述步骤中,对于用户的登录状态可以通过设置移动终端登录状态的失效时间实现对登录状态的控制,例如:可以通过在移动终端设置cookie来实现,可以理解的是,也可以在淘宝服务器端通过设置session实现登录令牌的失效时间;也可以设定为当用户退出终端侧第三方应用,则代表登录状态失效;从而更好的保护数据安全。

[0124] 在该步骤中,所述移动终端向所述淘宝服务器发送的数据信息可以通过专线URL发送,也就是说,用户信息、密码登录以及登录状态验证请求等相关数据信息都可以通过专线URL发送至淘宝服务器。

[0125] 步骤S102:资源服务器接收并解析所述登录状态验证请求,并判断所述登录状态验证请求中的数据信息与所述资源服务器存储的数据信息是否匹配;若匹配,则向所述第

三方应用服务器发送携带登录令牌和第三方应用标识信息的请求令牌。

[0126] 在该步骤中，当所述淘宝服务器接收到登录状态验证请求时，会向所述微博应用服务器申请微博应用标识(APPkey)，将其与所述存储的登录令牌作为登录状态验证请求比对的对象，如果比对结果相同，则淘宝服务器向所述微博应用服务器发送携带登录令牌和微博应用标识信息的请求令牌。比较方式可以是将上述通过3DES加密的数据解密后获得临时ID、登录状态、移动终端标识和微博应用标识信息(APPkey)，与存储在淘宝服务器中的登录令牌和微博应用标识信息比对，获得验证结果。

[0127] 在比较结果相同，所述淘宝服务器向所述微博方应用服务器发送携带登录令牌和微博应用标识信息的请求令牌之前，还可以根据微博应用功能设计，由移动终端的用户选择微博应用的不同授权内容，移动终端的用户可以根据移动终端显示的界面进行选择并发送淘宝服务器，淘宝服务器接收所述移动终端用户根据所述授权服务选择请求所选择的授权服务内容；之后根据所述授权服务内容与所述登录令牌、微博应用标识信息向所述微博应用服务器发送请求令牌，以获取访问的权限。

[0128] 通过授权服务选择实现用户对授权内容的选择而非仅能通过后台对用户访问资源服务器权限的验证，增加系统的可用性。

[0129] 需要说明的是，当微博服务器获取到访问令牌后，所述淘宝服务器会将发送至微博服务器的访问令牌存储到淘宝服务器划定的安全域中，在微博服务器通过访问令牌完成相应的操作后，淘宝服务器清除请求令牌；或者淘宝服务器在发送完访问令牌后清除清除令牌。

[0130] 其中，当移动终端登录成功后，会在淘宝服务器中维护移动终端的登录状态，所述登录状态可以根据设定的登录状态的失效时间改变登录状态。另外，淘宝服务器对不同用户登录移动终端并在登录成功后还会生成一个对应该用户的随机的临时ID，发送至移动终端，由移动终端维护该临时ID。

[0131] 在该步骤中，由淘宝服务器根据所述移动终端发送的数据信息生成的登录令牌(login_token)，是通过临时ID、用户上传的标识信息(账户信息)和终端标识信息哈希得到；所述请求令牌(request_token)是根据登录令牌(login_token)与微博应用标识信息哈希生成；访问令牌(access_token)是根据请求令牌(request_token)与微博应用标识信息哈希生成。

[0132] 步骤S103：所述第三方应用服务器根据所述请求令牌向资源服务器申请访问权限，所述资源服务器验证所述请求令牌中的数据信息与所述资源服务器存储的数据信息是否匹配，若匹配，则向所述第三方应用服务器发送访问令牌。

[0133] 在该步骤中，微博应用服务器根据获得的请求令牌向淘宝服务器申请访问的权限，淘宝服务器将请求令牌中的数据信息与其存储的登录状态数据比对，比对结果相同，则向所述微博服务器发送访问令牌。此时，微博服务器可以通过访问令牌获取到淘宝账号信息，也就是说，在进入微博应用时，可以通过淘宝服务器中相关的淘宝账户信息登录微博应用，进而避免繁琐的注册等步骤。同时，本申请的验证过程是在微博服务器与淘宝服务器之间进行，不存在移动终端的验证，因此，不会在登录请求验证过程中重定向至移动终端，而导致用户多次输入，降低使用的便捷性。

[0134] 在该步骤中，所述微博应用服务器向所述淘宝服务器发送的数据信息可以通过

SDK(软件开发工具包:Software Development Kit)封装后发送。

[0135] 根据上述可以获知,所述微博应用服务器向所述淘宝服务器和所述移动终端所要获取的数据信息包括:

[0136] 1.接收登录令牌向淘宝服务器发送登录状态验证请求。

[0137] 2.接收携带登录令牌和微博应用标识信息的请求令牌。

[0138] 3.接收来自淘宝服务器发送的访问令牌。

[0139] 上述登录令牌(Login_token)、请求令牌(request_token)以及访问令牌(access_token),所述三个令牌的数据信息可以在微博应用服务器的SDK中,通过三条专用的封装线实现封装,即:登录令牌(Login_token)通过登录令牌封装线URL封装;所述请求令牌(request_token)通过请求令牌封装线URL将登录令牌与第三方应用标识信息封装(Login_token+Appkey);所述访问令牌(access_token)通过访问令牌封装线URL将请求令牌与第三方应用标识信息封装(access_token+Appkey)。

[0140] 通过微博应用服务器SDK的封装,能够实现对移动终端登录令牌的调用,防止非授权的其他应用调用登录令牌。

[0141] 为提高微博应用服务与所述淘宝服务器之间数据传输的安全性,所述微博应用服务器对其发送至淘宝服务器的数据进行加密,虽然微博应用服务器和淘宝服务器都可以存储密钥,但由于微博应用服务器向淘宝服务器传输数据的链路安全性较低,因此,在微博应用服务器向淘宝服务器传输数据时采用的数据传输加密方式为非对称加密方式,所述非对称加密可以选择RSA、Elgamal、背包算法、Rabin、D-H或ECC(椭圆曲线加密算法)等算法实现。可以理解的是,所述微博应用服务器向淘宝服务器传输数据时采用的数据传输加密方式也可以为对称加密方式。

[0142] 在步骤S103中,当淘宝服务器验证的所述请求令牌中的数据信息与所述淘宝服务器存储的数据信息相匹配时,便向所述微博应用服务器发送访问令牌,所述微博应用服务器在接收到访问令牌后,将访问令牌保存至微博应用服务器所划分的安全域中,并清除请求令牌的数据信息。可以理解的是,如果匹配失败,请求令牌的相关数据信息也将被清除。

[0143] 本申请提供的一种基于登录状态的单点登录方法,通过引入登录状态,一方面,消除第三方应用将用户登录过程重定向及授权结束后再次重定向至第三方应用的过程,在增强对第三方应用安全验证的同时,避免多个第三方应用登录时弹出登录框,增加用户使用的便利性。另一方面,实现经过安全认证授权后才可以访问第三方应用,并在不在本地终端保存证书的情况下实现对第三方应用的动态授权操作,减轻了终端上的代码开发量,并提高了授权过程的安全性。

[0144] 以上是对本申请提供一种基于登录状态的单点登录方法实施例的说明,与前述基于登录状态的单点登录方法实施例相对应,本申请还公开了一种基于登录状态的单点登录装置,请参看图4,其为本申请提供的一种基于登录状态的单点登录装置实施例的结构示意图。由于装置实施例基本相似于方法实施例,所以描述得比较简单,相关之处参见方法实施例的部分说明即可。下述描述的装置实施例仅仅是示意性的。

[0145] 如图4所示,本申请提供一种基于登录状态的单点登录装置,包括:终端管理单元201,授权认证管理单元202和第三方应用管理单元203。

[0146] 所述终端管理单元201,用于终端侧第三方应用接收用户应用请求,获取登录令

牌，并经由第三方应用管理单元203向存储有终端侧用户登录状态数据的授权认证登录管理单元202发送登录状态验证请求；所述登录令牌包含有终端侧用户登录状态数据，所述登录状态验证请求携带所述登录令牌和所述第三方应用标识信息。

[0147] 所述终端管理单元201包括：登录令牌获取单元2011和第一数据加密传输单元2012；其中，所述登录令牌获取单元2011，用于终端侧将用户的登录请求发送至所述资源服务器，并接收所述资源服务器返回的根据所述登录请求生成的登录令牌；终端侧向所述资源服务器发送的登录请求的相关数据信息可以通过专线URL传输。所述登录请求包括：所述终端侧标识信息和用户账户信息；所述登录令牌包括：终端侧标识、终端侧临时ID和登录状态值。所述第一数据加密传输单元2012，用于在所述终端侧获取登录令牌，并经由第三方应用服务器向存储有终端侧用户登录状态数据的资源服务器发送登录状态验证请求中，采用非对称的方式对所述登录令牌和第三方应用标识的数据加密并传输。

[0148] 为提高用户数据的安全性，所述登录令牌获取单元2011进一步包括：失效时间选择单元，用于接收所述资源服务器发送的所述登录令牌的失效时间选择请求。

[0149] 可以理解的是，所述终端管理单元201还可以包括：标识信息管理单元2013和临时ID管理单元2014。其中，所述标识信息管理单元2013，用于管理终端侧标识信息，所述终端侧标识可以通过终端侧的MAC地址与SIM卡中的身份信息串联哈希得到。所述临时ID管理单元2014，用于存放由授权认证管理单元202发送的临时ID，所述临时ID管理单元2014可以为SIM卡的SE模块划定的安全域。

[0150] 所述授权认证管理单元202，用于接收并解析所述登录状态验证请求，并判断所述登录状态验证请求中的数据信息与所述授权认证登录管理单元中存储的数据信息是否匹配；若匹配，则向所述第三方应用管理单元203发送携带登录令牌和第三方应用标识信息的请求令牌。

[0151] 为提高系统的可用性，所述授权认证管理单元202包括：授权服务选择请求发送单元和授权服务器选择结接收单元；其中，所述授权服务选择请求发送单元用于所述资源服务器向终端侧发送授权服务选择请求。所述授权服务器选择结接收单元授权服务选择接收单元，用于所述终端侧获取所述用户根据所述授权服务选择请求所选择的授权服务内容，并发送至所述资源服务器。

[0152] 可以理解的是，所述授权认证管理单元202还可以包括：临时ID生成单元2021、身份认证单元2022以及登录状态管理单元2023，其中，所述临时ID生成单元2021，用于根据终端侧的登录请求生成与终端侧对应的随机的临时ID，该随机的临时ID会在终端管理单元201中的临时ID管理单元2014中维护。所述身份认证单元2022，用于验证终端管理单元201发送的账户信息，认证用户的身份信息。所述登录状态管理单元2023，用于在用户向终端侧管理单元发送登录请求，终端侧管理单元将登录请求重定向至授权认证管理单元并在登录成功后，可以在授权认证管理单元中的登录状态管理单元2023中维护该用户在终端侧的登录状态。

[0153] 所述授权认证管理单元202还包括：令牌生成单元2024，用于根据所述临时ID终端标识哈希生成登录令牌(login_token)；根据所述登录令牌和第三方应用标识哈希生成请求令牌(request_token)；根据所述请求令牌和第三方应用标识哈希生成访问令牌(access_token)。

[0154] 第三方应用管理单元203，用于根据所述请求令牌向授权认证登录管理单元申请访问权限，所述授权认证登录管理单元验证所述请求令牌中的数据信息与所述授权认证登录管理单元存储的数据信息是否匹配，若匹配，则向所述第三方应用管理单元203发送访问令牌。

[0155] 为提高安全性，所述第三方应用管理单元203还包括：封装单元2031，用于封装所述第三方应用管理单元203中所述登录令牌、所述请求令牌以及所述访问令牌的数据信息。所述封装单元2031可以封装三条专线URL，分别是登录令牌(Login_token)通过登录令牌封装线URL封装；所述请求令牌(request_token)通过请求令牌封装线URL将登录令牌与第三方应用标识信息封装(Login_token+Appkey)；所述访问令牌(access_token)通过访问令牌封装线URL将请求令牌与第三方应用标识信息封装(access_token+Appkey)。

[0156] 可以理解的是，在所述第三方应用管理单元203向所述授权认证管理单元202传输数据时，可以通过对数据进行加密，提高数据的安全性。因此，第三方应用管理单元203还包括：第二数据加密传输单元2032，用于采用非对称加密的方式，对所述登录状态验证请求中的数据信息加密及传输。

[0157] 可以理解的是，所述第二数据加密传输单元2032也可以采用对称加密的方式。

[0158] 第三方应用标识管理单元2033，用于生成第三方应用的唯一识别码，即：Appkey；提供认证授权管理单元202进行识别。

[0159] 令牌管理单元2034，用于在收到访问令牌后，将访问令牌保存在第三方应用管理单元中划定搞得安全域中，并清除请求令牌的相关数据信息。

[0160] 以上是对本申请提供的一种基于登录状态的单点登录方法及装置进行的说明，下面针对基于登录状态的终端侧发送登录请求方法和装置进行说明。

[0161] 由上述基于登录状态的单点登录方法及装置可以看出，由于基于登录状态的终端侧发送登录请求方法和装置的实施例基本相似于上述基于登录状态的单点登录方法和装置的实施例，所以描述得比较简单，相关之处参见基于登录状态的单点登录方法实施例的部分说明即可。下述针对基于登录状态的终端侧发送登录请求方法和装置的描述仅仅是示意性的。

[0162] 请参考图5所示，图5是本申请提供的一种基于登录状态的终端侧发送登录请求方法的流程图。

[0163] 本申请提供一种基于登录状态的终端侧发送登录请求的方法，包括：

[0164] 步骤S501：终端侧第三方应用接收应用请求获取登录令牌；

[0165] 步骤S502：并经由第三方应用服务器向存储有终端侧用户登录状态数据的资源服务器发送登录状态验证请求；所述登录令牌包含有终端侧用户登录状态数据，所述登录状态验证请求携带所述登录令牌和所述第三方应用标识信息。

[0166] 所述获取登录令牌包括：所述终端侧将用户的登录请求发送至所述资源服务器；并接收所述资源服务器返回的根据所述登录请求生成的登录令牌；所述登录请求包括：所述终端侧标识信息和用户账户信息；所述登录令牌包括：终端侧标识、终端侧临时ID和登录状态值。

[0167] 所述终端侧接收所述资源服务器返回的根据所述登录请求生成的登录令牌，包括：所述终端侧接收所述资源服务器发送的所述登录令牌的失效时间选择请求。

[0168] 采用对称加密方式对所述登录令牌和第三方应用标识的数据加密。或者说，由所述终端侧发送的数据通过对称加密的方式加密，提高数据的安全性。

[0169] 请参考图6所示，图6是本申请提供的一种基于登录状态的终端侧发送登录请求装置的结构示意图。

[0170] 本申请提供一种基于登录状态的终端侧发送登录请求的装置，包括：终端管理单元201，用于终端侧第三方应用接收用户应用请求，获取登录令牌，并经由第三方应用管理单元203向存储有终端侧用户登录状态数据的授权认证登录管理单元发送登录状态验证请求；所述登录令牌包含有终端侧用户登录状态数据，所述登录状态验证请求携带所述登录令牌和所述第三方应用标识信息。

[0171] 所述终端管理单元201包括：登录令牌获取单元2011，用于终端侧将用户的登录请求发送至所述资源服务器，并接收所述资源服务器返回的根据所述登录请求生成的登录令牌；所述登录请求包括：所述终端侧标识信息和用户账户信息；所述登录令牌包括：终端侧标识、终端侧临时ID和登录状态值。

[0172] 为提高用户数据的安全性，所述登录令牌获取单元2011进一步包括：失效时间选择单元，用于接收所述资源服务器发送的所述登录令牌的失效时间选择请求。

[0173] 可以理解的是，所述终端管理单元201还可以包括：第一数据加密传输单元2012，标识信息管理单元2013和临时ID管理单元2014。

[0174] 所述第一数据加密传输单元2012，用于在所述终端侧获取登录令牌，并经由第三方应用服务器向存储有终端侧用户登录状态数据的资源服务器发送登录状态验证请求中，采用非对称的方式对所述登录令牌和第三方应用标识的数据加密并传输。

[0175] 所述标识信息管理单元2013，用于管理终端侧标识信息，所述终端侧标识可以通过终端侧的MAC地址与SIM卡中的身份信息串联哈希得到。

[0176] 所述临时ID管理单元2014，用于存放由授权认证管理单元202发送的临时ID，所述临时ID管理单元2014可以为SIM卡的SE模块划定的安全域。

[0177] 以上部分内容是对本申请提供的一种基于登录状态的终端侧发送登录请求方法和装置的说明。根据上述内容，可以理解的是，本申请还提供一种基于登录状态的资源服务器授权认证方法和装置，由于基于登录状态的资源服务器授权认证方法和装置的实施例基本相似于上述基于登录状态的单点登录方法和装置的实施例，所以描述得比较简单，相关之处参见基于登录状态的单点登录方法和装置实施例的部分说明即可。下述针对基于登录状态的资源服务器授权认证方法和装置的描述仅仅是示意性的。

[0178] 请参考图7所示，图7是本申请提供的一种基于登录状态的资源服务器授权认证方法的流程图。

[0179] 本申请提供一种基于登录状态的资源服务器授权认证方法，包括：

[0180] 步骤S701：资源服务器接收并解析自来第三方应用服务器发送的登录状态验证请求；

[0181] 步骤S702：判断所述登录状态验证请求中的数据信息与所述资源服务器存储的数据信息是否匹配；若匹配，则向所述第三方应用服务器发送携带登录令牌和第三方应用标识信息的请求令牌。

[0182] 在步骤S702中，向所述第三方应用服务器发送携带登录令牌和第三方应用标识信

息的请求令牌，还包括：

[0183] 所述资源服务器向所述终端侧发送授权服务选择请求；

[0184] 所述终端侧获取所述用户根据所述授权服务选择请求所选择的授权服务内容，并发送至所述资源服务器。

[0185] 请参考图8所示，图8是本申请提供的一种基于登录状态的资源服务器授权认证装置的结构示意图。

[0186] 本申请提供一种基于登录状态的资源服务器授权认证装置，包括：

[0187] 授权认证管理单元202，用于接收并解析所述登录状态验证请求，并判断所述登录状态验证请求中的数据信息与所述授权认证登录管理单元中存储的数据信息是否匹配；若匹配，则向所述第三方应用管理单元203发送携带登录令牌和第三方应用标识信息的请求令牌。

[0188] 所述授权认证登录管理单元202包括：

[0189] 授权服务选择请求发送单元，用于所述资源服务器向终端侧发送授权服务选择请求；

[0190] 授权服务选择接收单元，用于所述终端侧获取所述用户根据所述授权服务选择请求所选择的授权服务内容，并发送至所述资源服务器。

[0191] 可以理解的是，所述授权认证管理单元202还可以包括：临时ID生成单元2021、身份认证单元2022以及登录状态管理单元2023，其中，所述临时ID生成单元2021，用于根据终端侧的登录请求生成与终端侧对应的随机的临时ID，该随机的临时ID会在终端管理单元201中的临时ID管理单元2014中维护。所述身份认证单元2022，用于验证终端管理单元201发送的账户信息，认证用户的身份信息。所述登录状态管理单元2023，用于在用户向终端侧管理单元发送登录请求，终端侧管理单元将登录请求重定向至授权认证管理单元并在登录成功后，可以在授权认证管理单元中的登录状态管理单元2023中维护该用户在终端侧的登录状态。

[0192] 所述授权认证管理单元202还包括：令牌生成单元2024，用于根据所述临时ID终端标识哈希生成登录令牌(login_token)；根据所述登录令牌和第三方应用标识哈希生成请求令牌(request_token)；根据所述请求令牌和第三方应用标识哈希生成访问令牌(access_token)。

[0193] 以上部分内容是对本申请提供的一种基于登录状态的资源服务器授权认证方法和装置的说明。根据上述内容，可以理解的是，本申请还提供一种基于登录状态的第三方应用访问权限请求方法和装置，由于基于登录状态的第三方应用访问权限请求方法和装置的实施例基本相似于上述基于登录状态的单点登录方法和装置的实施例，所以描述得比较简单，相关之处参见基于登录状态的单点登录方法和装置实施例的部分说明即可。下述针对基于登录状态的第三方应用访问权限请求方法和装置的描述仅仅是示意性的。

[0194] 请参考图9所示，图9是本申请提供的一种基于登录状态的第三方应用访问权限请求方法的流程图。

[0195] 本申请还提供一种基于登录状态的第三方应用访问权限请求方法，包括：

[0196] 步骤S901：第三方应用服务器接收来自资源服务器发送的携带登录令牌和第三方应用标识信息的请求令牌；

[0197] 步骤S902:所述第三方应用服务器根据所述请求令牌向资源服务器申请访问权限,所述资源服务器验证所述请求令牌中的数据信息与所述资源服务器存储的数据信息是否匹配,若匹配,则所述第三方应用服务器接收所述资源服务器发送的访问令牌。

[0198] 所述经由第三方应用服务器向存储有终端侧用户登录状态数据的资源服务器发送登录状态验证请求,采用SDK封装后发送。

[0199] 采用非对称加密的方式,对所述登录状态验证请求中的数据信息加密及传输。

[0200] 请参考图10所示,图10是本申请提供的一种基于登录状态的第三方应用访问权限请求装置的结构示意图。

[0201] 本申请还提供一种基于登录状态的第三方应用访问权限请求的装置,包括:

[0202] 第三方应用管理单元203,用于根据所述请求令牌向授权认证登录管理单元申请访问权限,所述授权认证登录管理单元验证所述请求令牌中的数据信息与所述授权认证登录管理单元存储的数据信息是否匹配,若匹配,则向所述第三方应用管理单元203发送访问令牌。

[0203] 所述第三方应用管理单元203包括:封装单元2031,用于封装所述第三方应用管理单元203中所述登录令牌、所述请求令牌以及所述访问令牌的数据信息。所述封装单元2031可以封装三条专线URL,分别是登录令牌(Login_token)通过登录令牌封装线URL封装;所述请求令牌(request_token)通过请求令牌封装线URL将登录令牌与第三方应用标识信息封装(Login_token+Appkey);所述访问令牌(access_token)通过访问令牌封装线URL将请求令牌与第三方应用标识信息封装(access_token+Appkey)。

[0204] 所述第三方应用管理单元203包括:第二数据加密传输单元2032,用于采用非对称加密的方式,对所述登录状态验证请求中的数据信息加密及传输。

[0205] 可以理解的是,在所述第三方应用管理单元203向所述授权认证管理单元202传输数据时,可以通过对数据进行加密,提高数据的安全性。因此,第三方应用管理单元203还包括:第二数据加密传输单元2032,用于采用非对称加密的方式,对所述登录状态验证请求中的数据信息加密及传输。

[0206] 第三方应用标识管理单元2033,用于接收并存储由授权认证管理单元202发送的针对第三方应用的唯一识别码,即:Appkey。

[0207] 令牌管理单元2034,用于在收到访问令牌后,将访问令牌保存在第三方应用管理单元中划定搞得安全域中,并清除请求令牌的相关数据信息。

[0208] 此部分内容是对本申请提供的一种基于登录状态的第三方应用访问权限请求方法和装置的说明。由于基于登录状态的第三方应用访问权限请求方法和装置的实施例基本相似于上述基于登录状态的单点登录方法和装置的实施例,所以描述得比较简单,相关之处参见基于登录状态的单点登录方法和装置实施例的部分说明即可。

[0209] 在一个典型的配置中,计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[0210] 内存可能包括计算机可读介质中的非永久性存储器,随机存取存储器(RAM)和/或非易失性内存等形式,如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

[0211] 1、计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方

法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括非暂存电脑可读媒体(transitory media)，如调制的数据信号和载波。

[0212] 2、本领域技术人员应明白，本申请的实施例可提供为方法、系统或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0213] 本申请虽然以较佳实施例公开如上，但其并不是用来限定本申请，任何本领域技术人员在不脱离本申请的精神和范围内，都可以做出可能的变动和修改，因此本申请的保护范围应当以本申请权利要求所界定的范围为准。

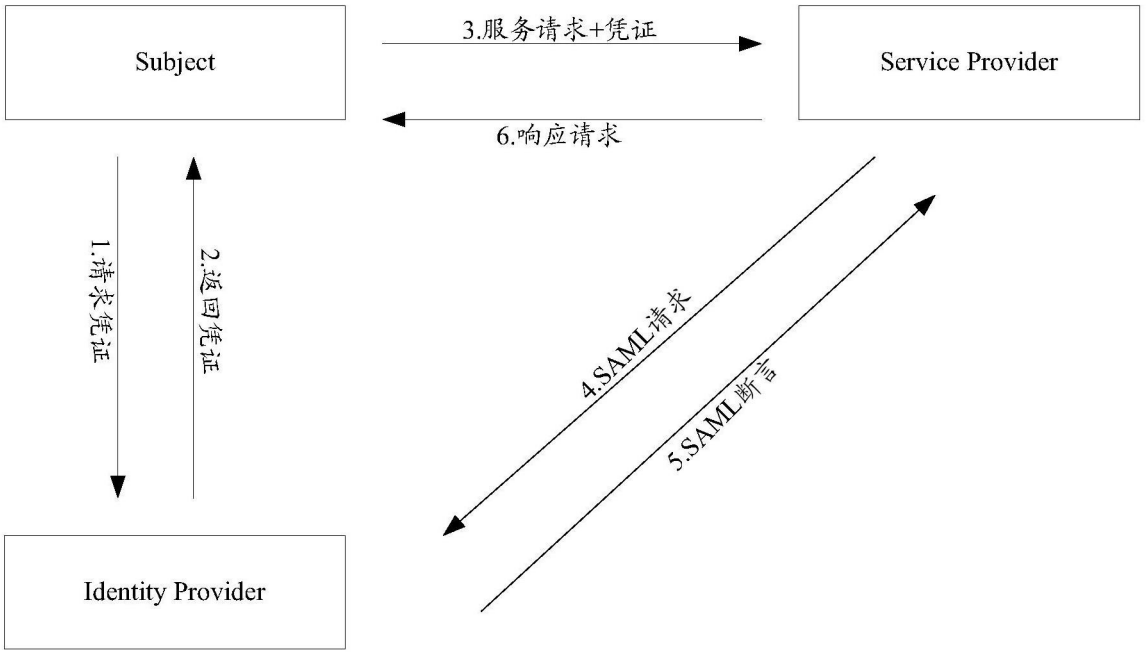

Subject
Service Provider
3.服务请求+凭证
6.响应请求
1.请求凭证
2.返回凭证
4.SAML请求
5.SAML断言
Identity Provider

图1

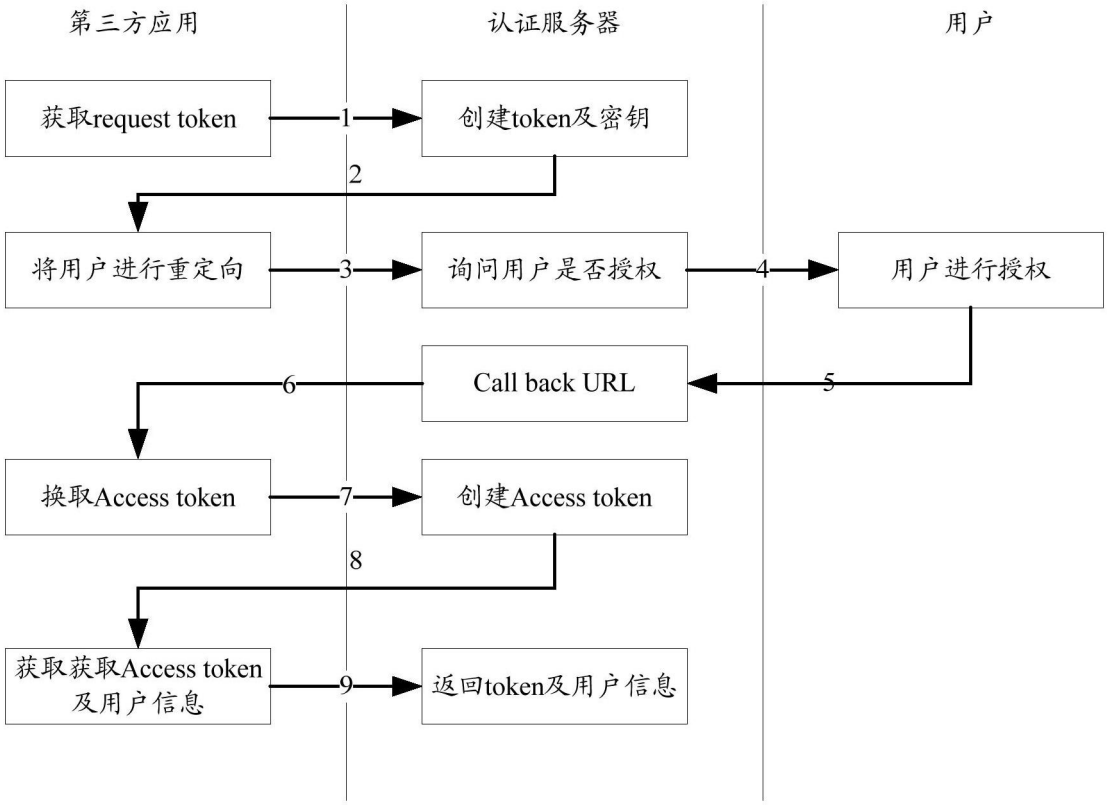

第三方应用
认证服务器
用户
获取request token
1
创建token及密钥
2
将用户进行重定向
3
询问用户是否授权
4
用户进行授权
Call back URL
6
5
换取Access token
7
创建Access token
8
获取获取Access token
及用户信息
9
返回token及用户信息

图2

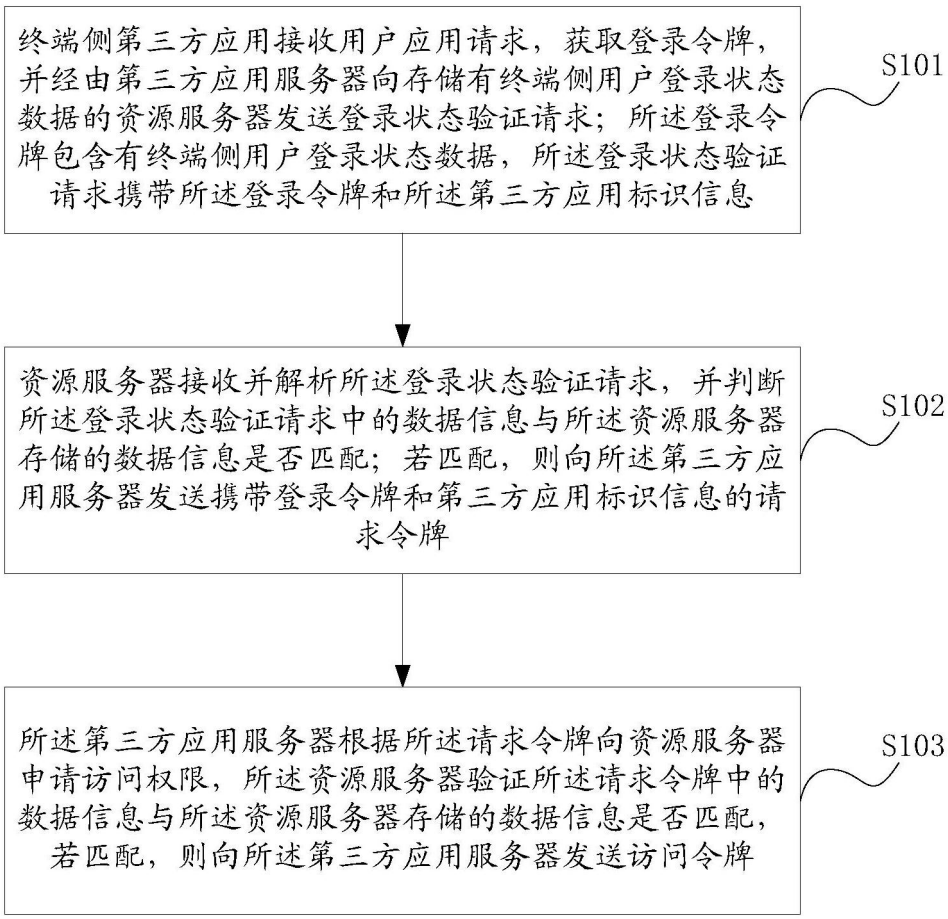

终端侧第三方应用接收用户应用请求，获取登录令牌，并经由第三方应用服务器向存储有终端侧用户登录状态数据的资源服务器发送登录状态验证请求；所述登录令牌包含有终端侧用户登录状态数据，所述登录状态验证请求携带所述登录令牌和所述第三方应用标识信息
S101
资源服务器接收并解析所述登录状态验证请求，并判断所述登录状态验证请求中的数据信息与所述资源服务器存储的数据信息是否匹配；若匹配，则向所述第三方应用服务器发送携带登录令牌和第三方应用标识信息的请求令牌
S102
所述第三方应用服务器根据所述请求令牌向资源服务器申请访问权限，所述资源服务器验证所述请求令牌中的数据信息与所述资源服务器存储的数据信息是否匹配，若匹配，则向所述第三方应用服务器发送访问令牌
S103

图3

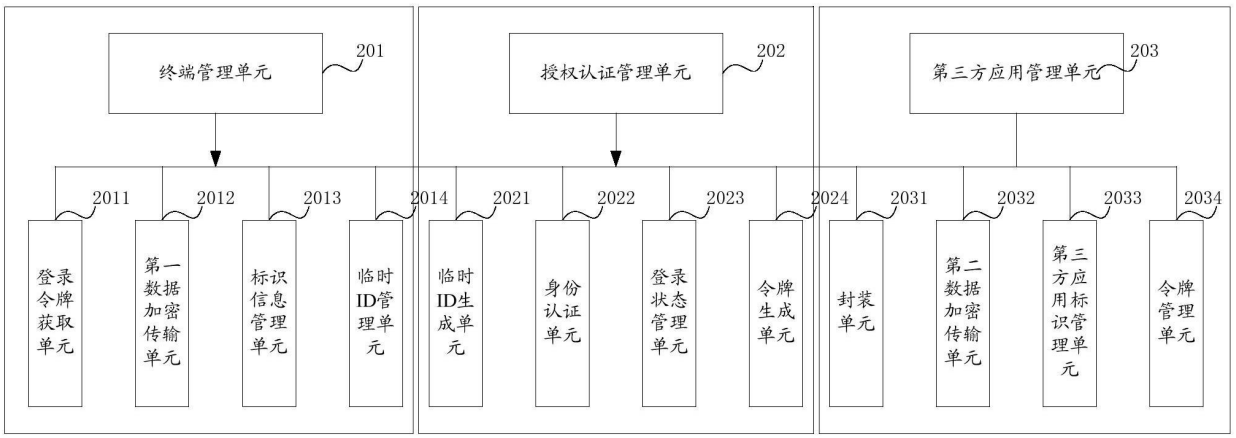

终端管理单元
201
授权认证管理单元
202
第三方应用管理单元
203
2011
2012
2013
2014
2021
2022
2023
2024
2031
2032
2033
2034
登录令牌获取单元
第一数据加密传输单元
标识信息管理单元
临时ID管理单元
临时ID生成单元
身份认证单元
登录状态管理单元
令牌生成单元
封装单元
第二数据加密传输单元
第三方应用标识管理单元
令牌管理单元

图4

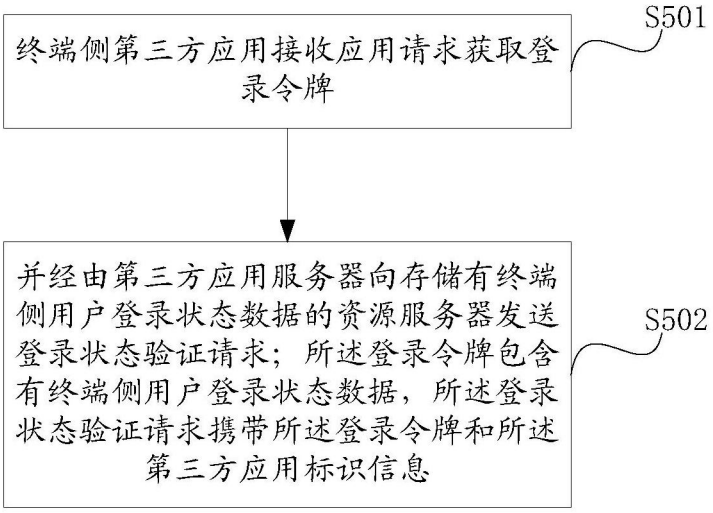

终端侧第三方应用接收应用请求获取登录令牌
S501
并经由第三方应用服务器向存储有终端侧用户登录状态数据的资源服务器发送登录状态验证请求；所述登录令牌包含有终端侧用户登录状态数据，所述登录状态验证请求携带所述登录令牌和所述第三方应用标识信息
S502

图5

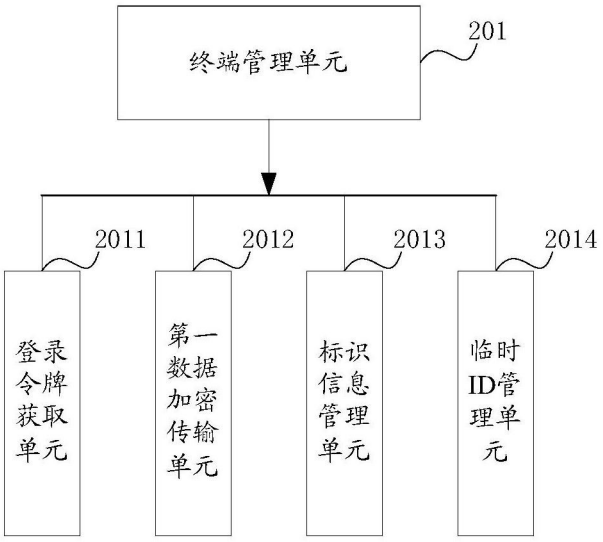

终端管理单元
201
2011
2012
2013
2014
登录令牌获取单元
第一数据加密传输单元
标识信息管理单元
临时ID管理单元

图6

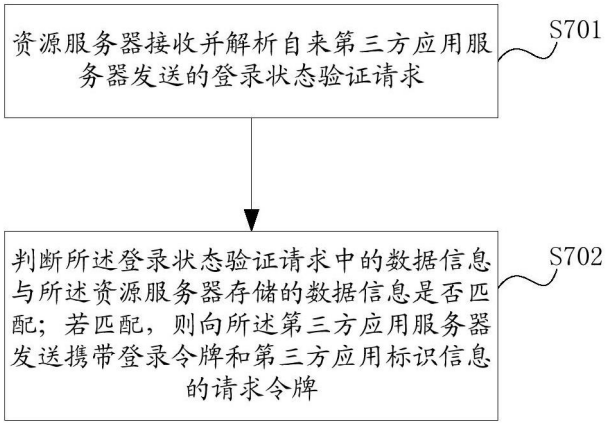

资源服务器接收并解析自来第三方应用服务器发送的登录状态验证请求
S701
判断所述登录状态验证请求中的数据信息与所述资源服务器存储的数据信息是否匹配；若匹配，则向所述第三方应用服务器发送携带登录令牌和第三方应用标识信息的请求令牌
S702

图7

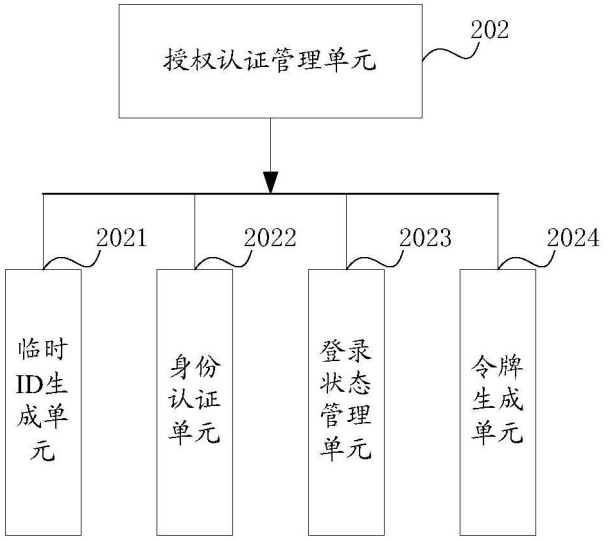

授权认证管理单元
202
2021
2022
2023
2024
临时ID生成单元
身份认证单元
登录状态管理单元
令牌生成单元

图8

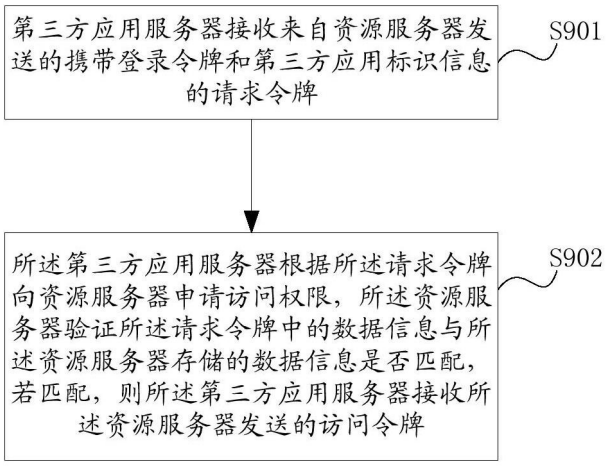

第三方应用服务器接收来自资源服务器发送的携带登录令牌和第三方应用标识信息的请求令牌
S901
所述第三方应用服务器根据所述请求令牌向资源服务器申请访问权限，所述资源服务器验证所述请求令牌中的数据信息与所述资源服务器存储的数据信息是否匹配，若匹配，则所述第三方应用服务器接收所述资源服务器发送的访问令牌
S902

图9

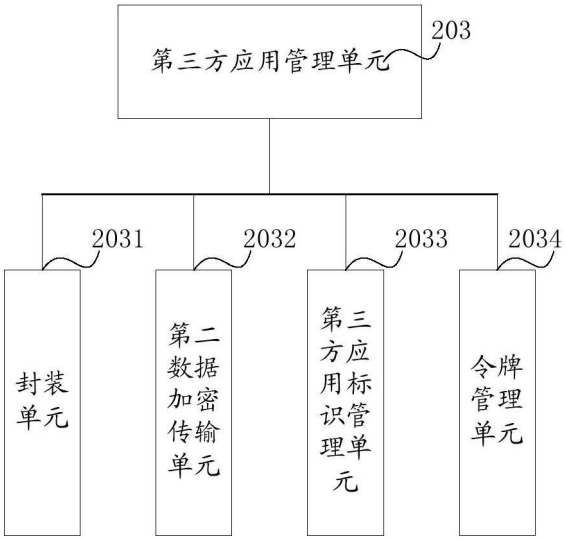

第三方应用管理单元
203
2031
2032
2033
2034
封装单元
第二数据加密传输单元
第三方应用标识管理单元
令牌管理单元

图10