



(12)发明专利

(10)授权公告号 CN 106295394 B

(45)授权公告日 2018.11.23

(21)申请号 201610585856.9

(22)申请日 2016.07.22

(65)同一申请的已公布的文献号

申请公布号 CN 106295394 A

(43)申请公布日 2017.01.04

(73)专利权人 飞天诚信科技股份有限公司

地址 100085 北京市海淀区学清路9号汇智大厦B楼17层

(72)发明人 陆舟 于华章

(51)Int.Cl.

G06F 21/62(2013.01)

(56)对比文件

CN 102761549 A,2012.10.31,

CN 103139181 A,2013.06.05,

WO 2010/000298 A1,2010.01.07,

CN 105577691 A,2016.05.11,

CN 104954330 A,2015.09.30,

CN 105656856 A,2016.06.08,

US 2013/0086645 A1,2013.04.04,

刘镛等.“基于国内开放平台的OAuth认证框架研究”.《信息通信技术》.2011,(第06期),第43-46页.

审查员 周杨

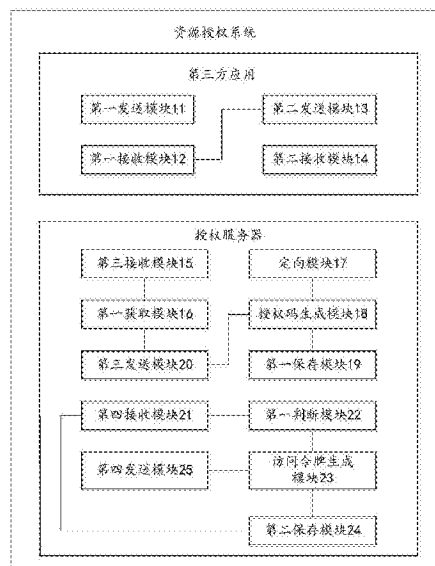
权利要求书11页 说明书15页 附图5页

(54)发明名称

资源授权方法及系统和授权服务器及工作方法

(57)摘要

本发明公开资源授权方法及系统和授权服务器及工作方法,授权服务器的工作方法包括:当授权服务器接收到第三方应用发送的获取授权码请求时以预存的访问权限列表为参数定向到授权页面,当接收到允许授权信息时生成授权码,将授权码与访问权限列表对应存储,并根据预存的重定向URL向第三方应用回传授权码;当授权服务器收到到第三方应用发送的包含授权码、应用标识符、应用密码的获取令牌请求时,根据获取令牌请求判断授权码是否有效,并根据应用标识符和应用密码判断所述第三方应用是否合法,若判断均为是则生成访问令牌,并将访问令牌发送给所述第三方应用。本发明用户可以设置第三方应用的访问权限和有效期,有效的防止资源泄露。



1. 一种资源授权的方法,其特征在于,包括:

步骤A1、第三方应用向授权服务器发送包含应用标识符的获取授权码请求;

步骤A2、所述授权服务器根据所述应用标识符获取预存的重定向URL,以预存的访问权限列表为参数定向到授权页面,若接收到允许授权信息则生成授权码,将所述授权码、所述应用标识符和所述预存的访问权限列表对应存储;根据所述重定向URL向所述第三方应用回传所述授权码;

步骤A3、所述第三方应用向所述授权服务器发送包含所述授权码、所述应用标识符和应用密码的获取令牌请求;

步骤A4、所述授权服务器判断所述授权码是否有效,并根据所述应用标识符和所述应用密码判断所述第三方应用是否合法,若判断均为是则生成访问令牌,根据所述应用标识符获取所述预存的访问权限列表,将所述访问令牌和所述预存的访问权限列表对应存储,将所述访问令牌发送给所述第三方应用,否则结束;

所述步骤A4之后还包括:

步骤101、所述第三方应用向资源服务器发送包含所述访问令牌和资源标识的获取资源请求;

步骤102、所述资源服务器将所述访问令牌和所述资源标识发送给所述授权服务器;

步骤103、所述授权服务器判断访问令牌是有效,判断与访问令牌对应保存的访问权限列表中是否包含所述资源标识,若判断均为是则向资源服务器发送包含资源标识的允许访问信息,执行步骤104,否则结束;

步骤104、所述资源服务器将与资源标识相对应的资源发送给所述第三方应用。

2. 如权利要求1所述的方法,其特征在于,所述步骤A1之前还包括:第三方应用在授权服务器进行注册,授权服务器中预存有第三方应用的应用标识符、应用密码和重定向URL。

3. 如权利要求2所述的方法,其特征在于,

所述步骤A3具体为:第三方应用将应用标识符与应用密码进行加密生成应用密文信息,向所述授权服务器发送包含应用密文信息和授权码的获取令牌请求;

所述根据应用标识符和应用密码判断第三方应用是否合法具体包括,授权服务器从获取访问令牌请求中获取应用密文信息,将应用密文信息解密获取应用标识符和应用密码,根据应用标识符和应用密码判断第三方应用是否合法。

4. 如权利要求1所述的方法,其特征在于,所述步骤A1之后,所述步骤A2之前还包括:所述授权服务器根据所述应用标识符判断所述第三方应用是否已注册,是则执行步骤A2,否则向授权服务器发送应用标识无效信息,结束。

5. 如权利要求1所述的方法,其特征在于,所述访问权限列表具体为由资源标识形成的列表。

6. 如权利要求1所述的方法,其特征在于,所述获取授权码请求中还包括第一重定向URL;

所述根据所述应用标识符获取预存的重定向URL之后,所述以预存的所述访问权限列表为参数定向到授权页面之前还包括:授权服务器判断所述第一重定向URL与预存的重定向URL是否相同,是则以预存的所述访问权限列表为参数定向到授权页面,否则向所述第三方应用返回第一重定向URL无效信息,结束。

7. 如权利要求1所述的方法,其特征在于,若所述获取授权码请求中还包括第一访问权限列表;

所述步骤A1之后,所述步骤A2之前还包括:所述授权服务器判断预存的访问权限列表是否包含所述第一访问权限列表,是则所述授权服务器以所述第一访问权限列表为参数定向到预存的授权页面,若接收到允许授权信息则生成授权码,将所述授权码、所述应用标识符和所述第一访问权限列表对应存储;根据所述重定向URL向所述第三方应用回传授权码;执行步骤A3;否则执行步骤A2;

所述生成访问令牌之后,所述将访问令牌发送给第三方应用之前还包括:授权服务器根据应用标识符获取所述第一访问权限列表,将所述访问令牌和所述第一访问权限列表对应存储。

8. 如权利要求1所述的方法,其特征在于,所述允许授权信息中具体包括用户允许访问的资源的资源标识组成的第二访问权限列表;

所述将所述授权码和所述应用标识符对应存储具体为:授权服务器将所述授权码、所述应用标识符和所述第二访问权限列表对应存储;

所述生成访问令牌之后,所述将访问令牌发送给第三方应用之前还包括:授权服务器根据应用标识符获取所述第二访问权限列表,将所述访问令牌和所述第二访问权限列表对应存储。

9. 如权利要求1所述的方法,其特征在于,所述步骤A4还包括:授权服务器获取服务器的当前时间,根据当前时间生成访问令牌过期时间,并将所述访问令牌和所述访问令牌过期时间对应保存;

所述步骤102之后,所述步骤103之前还包括:所述授权服务器根据所述访问令牌获取所述访问令牌过期时间,判断所述访问令牌是否过期,是则结束,否则执行步骤103。

10. 如权利要求9所述的方法,其特征在于,所述步骤A4还包括:授权服务器生成刷新令牌,并将所述访问令牌、所述访问令牌过期时间和所述刷新令牌对应保存,将所述访问令牌和所述刷新令牌发送给所述第三方应用;

若所述授权服务器判定访问令牌过期之后还包括:

步骤201、所述授权服务器向所述第三方应用发送访问令牌过期信息;

步骤202、所述第三方应用向所述授权服务器发送包含所述应用标识符、所述应用密码和所述刷新令牌的更新令牌请求;

步骤203、所述授权服务器判断所述刷新令牌是否有效,并根据所述应用标识符和所述应用密码判断所述第三方应用是否合法,若判断均为是时更新访问令牌,并生成新的访问令牌过期时间,返回步骤A4。

11. 如权利要求10所述的方法,其特征在于,

所述步骤202具体包括:所述第三方应用将所述应用标识符和所述应用密码进行加密生成应用密文信息,发送包含所述应用密文信息和刷新令牌的更新令牌请求;

所述根据应用标识符和应用密码判断第三方应用是否合法具体包括:授权服务器将所述应用密文信息解密获取所述应用标识符和所述应用密码,并根据所述应用标识符和所述应用密码判断第三方应用是否合法。

12. 如权利要求1所述的方法,其特征在于,

所述步骤A2还包括:授权服务器获取服务器当前时间作为授权码生成时间,根据授权码生成时间生成授权码过期时间;

所述步骤A4具体为:所述授权服务器获取服务器当前时间和授权码过期时间,判断授权码是否过期;判断所述授权码是否有效,并根据所述应用标识符和所述应用密码判断所述第三方应用是否合法,若判断均为是则生成访问令牌,将所述访问令牌发送给所述第三方应用,否则结束。

13.一种资源授权系统,其特征在于,包括第三方应用、授权服务器;

所述第三方应用包括:

第一发送模块,用于向授权服务器发送包含应用标识符的获取授权码请求;

第一接收模块,用于接收授权服务器回传的授权码;

第二发送模块,用于向所述授权服务器发送包含所述授权码、所述应用标识符和应用密码的获取令牌请求;

第二接收模块,用于接收授权服务器发送的访问令牌;

所述授权服务器包括:

第三接收模块,用于接收获授权码请求;

第一获取模块,用于根据所述第三接收模块接收到的所述获取授权码请求中的所述应用标识符获取预存的重定向URL;

定向模块,用于以预存的访问权限列表为参数定向到授权页面,并接收允许授权信息;

授权码生成模块,若所述定向模块接收到允许授权信息后生成授权码;

第一保存模块,用于将所述授权码生成模块生成的授权码、所述应用标识符和所述预存的访问权限列表对应存储;

第三发送模块,用于根据所述第一获取模块获取到的重定向URL向所述第三方应用回传所述授权码生成模块生成的授权码;

第四接收模块,用于接收所述第三方应用发送的获取令牌请求;

第一判断模块,用于判断所述第四接收模块接收到的获取令牌请求中的所述授权码是否有效,并根据所述第四接收模块接收到的获取令牌请求中的所述应用标识符和所述应用密码判断所述第三方应用是否合法;

访问令牌生成模块,用于若所述第一判断模块判断均为是时生成访问令牌;

第二保存模块,用于根据第四接收模块接收到的获取令牌请求中的所述应用标识符获取所述预存的访问权限列表,将所述访问令牌生成模块生成的访问令牌和所述预存的访问权限列表对应存储;

第四发送模块,用于将所述访问令牌生成模块生成的所述访问令牌发送给所述第三方应用;

所述系统还包括资源服务器;

所述第三方应用还包括:

第五发送模块,用于向资源服务器发送包含所述访问令牌和资源标识的获取资源请求;

资源服务器,包括:

第六发送模块,用于接收所述第三方应用发送的获取资源请求,并将所述获取资源请

求中的所述访问令牌和所述资源标识发送给授权服务器；

第五接收模块，用于接收所述授权服务器发送的允许访问信息，向所述第三方应用发送与所述资源标识相对应的资源；

所述授权服务器还包括：

第五判断模块，用于接收资源服务器发送的所述访问令牌和所述资源标识；判断所述访问令牌是否有效，判断与所述访问令牌访问对应的访问权限列表中是否包含所述资源标识；

第七发送模块，用于若所述第五判断模块判断均为是时向资源服务器发送包含资源标识的允许访问信息。

14. 如权利要求13所述的系统，其特征在于，所述授权服务器还包括：第三保存模块，用于保存第三方应用的应用标识符、应用密码和重定向URL。

15. 如权利要求14所述的系统，其特征在于，

所述第二发送模块包括：

第一加密子模块，用于将应用标识符与应用密码进行加密生成应用密文信息；

第一发送子模块，用于向所述授权服务器发送包含应用密文信息和授权码的获取令牌请求；

所述第四接收模块包括：

第一接收子模块，用于接收所述第三方应用发送的获取令牌请求；

第一解密模块，用于从获取访问令牌请求中获取应用密文信息，将应用密文信息解密获取应用标识符和应用密码。

16. 如权利要求13所述的系统，其特征在于，所述授权服务器还包括：

第二判断模块，用于根据所述第三接收模块接收到的获取授权码请求中的应用标识符判断所述第三方应用是否已注册；

所述第一获取模块，具体用于若所述第二判断模块判定第三方应用已注册之后根据所述第三接收模块接收到的所述获取授权码请求中的所述应用标识符获取预存的重定向URL。

17. 如权利要求13所述的系统，其特征在于，所述访问权限列表具体为由资源标识形成的列表。

18. 如权利要求13所述的系统，其特征在于，所述第三接收模块接收到的所述获取授权码请求中还包括第一重定向URL；

所述授权服务器还包括：

第三判断模块，用于判断所述第一重定向URL与所述第一获取模块获取到的预存的重定向URL是否相同；

所述定向模块，具体用于若所述第三判断模块判定第一重定向URL与所述第一获取模块获取到的预存的重定向URL相同时根据所述第三接收模块接收到的所述获取授权码请求中的所述应用标识符获取预存的重定向URL。

19. 如权利要求13所述的系统，其特征在于，所述第三接收模块接收到的所述获取授权码请求中还包括第一访问权限列表；

所述授权服务器还包括：

第四判断模块,用于判断预存的访问权限列表是否包含所述第一访问权限列表;

所述定向模块,具体用于若所述第四判断模块判定预存的访问权限列表包含所述第一访问权限列表时以所述第一访问权限列表为参数定向到授权页面,并接收允许授权信息;所述第一保存模块,用于将所述授权码生成模块生成的授权码、所述应用标识符和所述第一访问权限列表对应存储;所述第二保存模块,用于将所述访问令牌生成模块生成的访问令牌和根据所述获取令牌请求中的所述应用标识符获取到所述第一访问权限列表对应存储;

所述定向模块,还用于若所述第四判断模块判定预存的访问权限列表不包含所述第一访问权限列表时以所述预存的访问权限列表为参数定向到授权页面,并接收允许授权信息;所述第一保存模块,还用于将所述授权码生成模块生成的授权码、所述应用标识符和所述预存的访问权限列表对应存储;所述第二保存模块,还用于将所述访问令牌生成模块生成的访问令牌和根据获取令牌请求中的所述应用标识符获取到的所述预存的访问权限列表对应存储。

20.如权利要求13所述的系统,其特征在于,所述定向模块接收到的所述允许授权信息中包括用户允许访问的资源的资源标识组成的第二访问权限列表;

所述第一保存模块,还用于将所述授权码生成模块生成的授权码、所述应用标识符和所述定向模块接收到的所述允许授权信息中包含的第二访问权限列表对应存储;

所述第二保存模块,还用于将所述访问令牌生成模块生成的访问令牌和将所述定向模块接收到的所述允许授权信息中包含的第二访问权限列表对应存储。

21.如权利要求13所述的系统,其特征在于,所述授权服务器还包括:

访问令牌过期时间生成模块,用于获取服务器的当前时间,根据当前时间生成访问令牌过期时间;

所述第二保存模块,用于根据第四接收模块接收到的获取令牌请求中的所述应用标识符获取对应保存的访问权限列表,将所述访问令牌生成模块生成的访问令牌和所述访问令牌过期时间生成模块生成的所述访问令牌过期时间对应存储;

第六判断模块,用于根据所述访问令牌获取所述访问令牌过期时间,判断所述访问令牌是否过期;

所述第五判断模块,用于若所述第六判断模块判定所述访问令牌没有过期之后接收资源服务器发送的所述访问令牌和所述资源标识;判断所述访问令牌是有效,判断与所述访问令牌对应的访问权限列表中是否包含所述资源标识。

22.如权利要求21所述的系统,其特征在于,所述授权服务器还包括:

刷新令牌生成模块,用于生成刷新令牌;还用于若第七判断模块判定所述刷新令牌有效且判定所述第三方应用合法之后生成刷新令牌;

第八发送模块,用于若所述第六判断模块判定所述访问令牌过期之后向所述第三方应用发送访问令牌过期信息;

所述第四发送模块,用于将所述访问令牌生成模块生成的所述访问令牌和所述刷新令牌生成模块生成的刷新令牌发送给所述第三方应用;

所述访问令牌生成模块,还用于若所述第七判断模块判定所述刷新令牌有效且判定所述第三方应用合法之后生成访问令牌;

访问令牌过期时间生成模块,还用于若所述第七判断模块判定所述刷新令牌有效且判定所述第三方应用合法之后获取服务器的当前时间,根据当前时间生成访问令牌过期时间;

所述第二保存模块,用于根据第四接收模块接收到的获取令牌请求中的所述应用标识符获取对应保存的访问权限列表,将所述访问令牌生成模块生成的访问令牌、所述访问令牌过期时间生成模块生成的所述访问令牌过期时间和所述刷新令牌生成模块生成的刷新令牌对应存储;

第六接收模块,用于接收所述第三方应用发送的更新令牌请求;

第七判断模块,用于判断所述刷新令牌是否有效,并根据所述应用标识符和所述应用密码判断所述第三方应用是否合法;

所述第三方应用还包括:

第九发送模块,用于向所述授权服务器发送包含所述应用标识符、所述应用密码和所述刷新令牌的更新令牌请求。

23.如权利要求22所述的系统,其特征在于,

所述第九发送模块,包括:

第二加密子模块,用于将所述应用标识符和所述应用密码进行加密生成应用密文信息;

第二发送子模块,用于发送包含所述应用密文信息和刷新令牌的更新令牌请求;

所述第六接收模块,包括:

第二接收子模块,用于接收所述第三方应用发送的更新令牌请求;

第二解密子模块,用于将所述更新令牌请求中的所述应用密文信息解密获取所述应用标识符和所述应用密码。

24.如权利要求13所述的系统,其特征在于,所述授权服务器还包括:

授权码过期时间生成模块,用于获取服务器当前时间作为授权码生成时间,根据授权码生成时间生成授权码过期时间;

所述第一判断模块,具体用于获取服务器当前时间和授权码过期时间,判断授权码是否过期;判断所述授权码是否有效,并根据所述应用标识符和所述应用密码判断所述第三方应用是否合法。

25.一种授权服务器的工作方法,其特征在于,包括:

步骤B1、当授权服务器接收到第三方应用发送的包含应用标识符的获取授权码请求时,根据所述应用标识符获取预存的重定向URL,以预存的访问权限列表为参数定向到授权页面,若接收到允许授权信息则生成授权码,将所述授权码、所述应用标识符和所述预存的访问权限列表对应存储;根据所述重定向URL向所述第三方应用回传授权码;

步骤B2、当所述授权服务器接收到所述第三方应用发送的包含所述授权码、所述应用标识符和应用密码的获取令牌请求时,判断所述授权码是否有效,并根据所述应用标识符和所述应用密码判断所述第三方应用是否合法,若判断均为是则生成访问令牌,根据应用标识符获取所述预存的访问权限列表,将所述访问令牌和所述预存的访问权限列表对应存储,将所述访问令牌发送给所述第三方应用,否则结束;

所述步骤B2之后还包括:

当授权服务器接收到资源服务器发送的所述访问令牌和所述资源标识之后,判断访问令牌是有效,判断与访问令牌对应保存的访问权限列表中是否包含所述资源标识,若判断均为是则向资源服务器发送包含资源标识的允许访问信息。

26. 如权利要求25所述的方法,其特征在于,所述步骤B1之前还包括:第三方应用在授权服务器进行注册,授权服务器中预存有第三方应用的应用标识符、应用密码和重定向URL。

27. 如权利要求26所述的方法,其特征在于,所述根据应用标识符和应用密码判断第三方应用是否合法具体包括,授权服务器从获取访问令牌请求中获取应用密文信息,将应用密文信息解密获取应用标识符和应用密码,根据应用标识符和应用密码判断第三方应用是否合法。

28. 如权利要求25所述的方法,其特征在于,所述授权服务器接收到第三方应用发送的包含应用标识符的获取授权码请求之后,所述根据所述应用标识符获取预存的重定向URL之前还包括:所述授权服务器根据所述应用标识符判断所述第三方应用是否已注册,是则根据所述应用标识符获取预存的重定向URL,否则向授权服务器发送应用标识无效信息,结束。

29. 如权利要求25所述的方法,其特征在于,所述访问权限列表具体为由资源标识形成的列表。

30. 如权利要求25所述的方法,其特征在于,所述获取授权码请求中还包括第一重定向URL;

所述根据所述应用标识符获取预存的重定向URL之后,所述以预存的所述访问权限列表为参数定向到授权页面之前还包括:授权服务器判断所述第一重定向URL与预存的重定向URL是否相同,是则以预存的所述访问权限列表为参数定向到授权页面,否则向所述第三方应用返回第一重定向URL无效信息,结束。

31. 如权利要求25所述的方法,其特征在于,若所述获取授权码请求中还包括第一访问权限列表;

所述授权服务器接收到第三方应用发送的包含应用标识符的获取授权码请求之后,所述根据所述应用标识符获取预存的重定向URL之前还包括:所述授权服务器判断预存的访问权限列表是否包含所述第一访问权限列表,是则所述授权服务器以所述第一访问权限列表为参数定向到预存的授权页面,若接收到允许授权信息则生成授权码,将所述授权码、所述应用标识符和所述第一访问权限列表对应存储;根据所述重定向URL向所述第三方应用回传授权码;执行步骤B2;否则根据所述应用标识符获取预存的重定向URL;

所述生成访问令牌之后,所述将访问令牌发送给第三方应用之前还包括:授权服务器根据应用标识符获取所述第一访问权限列表,将所述访问令牌和所述第一访问权限列表对应存储。

32. 如权利要求25所述的方法,其特征在于,所述允许授权信息中具体包括用户允许访问的资源的资源标识组成的第二访问权限列表;

所述将所述授权码和所述应用标识符对应存储具体为:授权服务器将所述授权码、所述应用标识符和所述第二访问权限列表对应存储;

所述生成访问令牌之后,所述将访问令牌发送给第三方应用之前还包括:授权服务器

根据应用标识符获取所述第二访问权限列表,将所述访问令牌和所述第二访问权限列表对应存储。

33.如权利要求25所述的方法,其特征在于,所述步骤B2还包括:授权服务器获取服务器的当前时间,根据当前时间生成访问令牌过期时间,并将所述访问令牌和所述访问令牌过期时间对应保存;

所述接收到资源服务器发送的所述访问令牌和所述资源标识之后,所述判断访问令牌是有效之前还包括:所述授权服务器根据所述访问令牌获取所述访问令牌过期时间,判断所述访问令牌是否过期,是则结束,否则判断访问令牌是有效。

34.如权利要求33所述的方法,其特征在于,所述步骤B2还包括:授权服务器生成刷新令牌,并将所述访问令牌、所述访问令牌过期时间和所述刷新令牌对应保存,将所述访问令牌和所述刷新令牌发送给所述第三方应用;

若所述授权服务器判定访问令牌过期之后还包括:

步骤301、所述授权服务器向所述第三方应用发送访问令牌过期信息;

步骤302、当所述授权服务器接收到所述第三方应用发送的包含所述应用标识符、所述应用密码和所述刷新令牌的更新令牌请求之后,判断所述刷新令牌是否有效,并根据所述应用标识符和所述应用密码判断所述第三方应用是否合法,若判断均为是则更新访问令牌,并生成新的访问令牌过期时间,返回步骤B2。

35.如权利要求34所述的方法,其特征在于,

所述根据应用标识符和应用密码判断第三方应用是否合法具体包括:授权服务器将所述应用密文信息解密获取所述应用标识符和所述应用密码,并根据所述应用标识符和所述应用密码判断第三方应用是否合法。

36.如权利要求25所述的方法,其特征在于,

所述步骤B1还包括:授权服务器获取服务器当前时间作为授权码生成时间,根据授权码生成时间生成授权码过期时间;

所述步骤B2具体为:所述授权服务器获取服务器当前时间和授权码过期时间,判断授权码是否过期;判断所述授权码是否有效,并根据所述应用标识符和所述应用密码判断所述第三方应用是否合法,若判断均为是则生成访问令牌,将所述访问令牌发送给所述第三方应用,否则结束。

37.一种授权服务器,其特征在于,包括

第三接收模块,用于接收获授权码请求;

第一获取模块,用于根据所述第三接收模块接收到的所述获取授权码请求中的应用标识符获取预存的重定向URL;

定向模块,用于以预存的访问权限列表为参数定向到授权页面,并接收允许授权信息;

授权码生成模块,用于若所述定向模块接收到允许授权信息后生成授权码;

第一保存模块,用于将所述授权码生成模块生成的授权码、所述应用标识符和所述预存的访问权限列表对应存储;

第三发送模块,用于根据所述第一获取模块获取到的重定向URL向第三方应用回传所述授权码生成模块生成的授权码;

第四接收模块,用于接收所述第三方应用发送的获取令牌请求;

第一判断模块,用于判断所述第四接收模块接收到的获取令牌请求中的所述授权码是否有效,并根据所述第四接收模块接收到的获取令牌请求中的所述应用标识符和应用密码判断所述第三方应用是否合法;

访问令牌生成模块,用于若所述第一判断模块判断均为是时生成访问令牌;

第二保存模块,用于根据第四接收模块接收到的获取令牌请求中的所述应用标识符获取所述预存的访问权限列表,将所述访问令牌生成模块生成的访问令牌和所述预存的访问权限列表对应存储;

第四发送模块,用于将所述访问令牌生成模块生成的所述访问令牌发送给所述第三方应用;

所述授权服务器还包括:

第五判断模块,用于接收资源服务器发送的所述访问令牌和资源标识;判断所述访问令牌是有效,判断与所述访问令牌访问对应的访问权限列表中是否包含所述资源标识;

第七发送模块,用于若所述第五判断模块判断均为是时向资源服务器发送包含资源标识的允许访问信息。

38.如权利要求37所述的服务器,其特征在于,还包括:第三保存模块,用于保存第三方应用的应用标识符、应用密码和重定向URL。

39.如权利要求38所述的服务器,其特征在于,所述第四接收模块包括:

第一接收子模块,用于接收所述第三方应用发送的获取令牌请求;

第一解密模块,用于从获取访问令牌请求中获取应用密文信息,将应用密文信息解密获取应用标识符和应用密码。

40.如权利要求37所述的服务器,其特征在于,还包括:

第二判断模块,用于根据所述第三接收模块接收到的获取授权码请求中的应用标识符判断所述第三方应用是否已注册;

所述第一获取模块,具体用于若所述第二判断模块判定第三方应用已注册之后根据所述第三接收模块接收到的所述获取授权码请求中的所述应用标识符获取预存的重定向URL。

41.如权利要求37所述的服务器,其特征在于,所述访问权限列表具体为由资源标识形成的列表。

42.如权利要求37所述的服务器,其特征在于,所述第三接收模块接收到的所述获取授权码请求中还包括第一重定向URL;

所述服务器还包括:

第三判断模块,用于判断所述第一重定向URL与所述第一获取模块获取到的预存的重定向URL是否相同;

所述定向模块,具体用于若所述第三判断模块判定第一重定向URL与所述第一获取模块获取到的预存的重定向URL相同时根据所述第三接收模块接收到的所述获取授权码请求中的所述应用标识符获取预存的重定向URL。

43.如权利要求37所述的服务器,其特征在于,所述第三接收模块接收到的所述获取授权码请求中还包括第一访问权限列表;

所述服务器还包括:

第四判断模块,用于判断预存的访问权限列表是否包含所述第一访问权限列表;

所述定向模块,具体用于若所述第四判断模块判定预存的访问权限列表包含所述第一访问权限列表时以所述第一访问权限列表为参数定向到授权页面,并接收允许授权信息;所述第一保存模块,用于将所述授权码生成模块生成的授权码、所述应用标识符和所述第一访问权限列表对应存储;所述第二保存模块,用于将所述访问令牌生成模块生成的访问令牌和根据所述获取令牌请求中的所述应用标识符获取到所述第一访问权限列表对应存储;

所述定向模块,还用于若所述第四判断模块判定预存的访问权限列表不包含所述第一访问权限列表时以所述预存的访问权限列表为参数定向到授权页面,并接收允许授权信息;所述第一保存模块,还用于将所述授权码生成模块生成的授权码、所述应用标识符和所述预存的访问权限列表对应存储;所述第二保存模块,还用于将所述访问令牌生成模块生成的访问令牌和根据获取令牌请求中的所述应用标识符获取到的所述预存的访问权限列表对应存储。

44. 如权利要求37所述的服务器,其特征在于,所述定向模块接收到的所述允许授权信息中包括用户允许访问的资源的资源标识组成的第二访问权限列表;

所述第一保存模块,还用于将所述授权码生成模块生成的授权码、所述应用标识符和所述定向模块接收到的所述允许授权信息中包含的第二访问权限列表对应存储;

所述第二保存模块,还用于将所述访问令牌生成模块生成的访问令牌和所述定向模块接收到的所述允许授权信息中包含的第二访问权限列表对应存储。

45. 如权利要求44所述的服务器,其特征在于,还包括:

访问令牌过期时间生成模块,用于获取服务器的当前时间,根据当前时间生成访问令牌过期时间;

所述第二保存模块,用于根据第四接收模块接收到的获取令牌请求中的所述应用标识符获取对应保存的访问权限列表,将所述访问令牌生成模块生成的访问令牌和所述访问令牌过期时间生成模块生成的所述访问令牌过期时间对应存储;

第六判断模块,用于根据所述访问令牌获取所述访问令牌过期时间,判断所述访问令牌是否过期;

所述第五判断模块,用于若所述第六判断模块判定所述访问令牌没有过期之后接收资源服务器发送的所述访问令牌和所述资源标识;判断所述访问令牌是有效,判断与所述访问令牌访问对应的访问权限列表中是否包含所述资源标识。

46. 如权利要求45所述的服务器,其特征在于,还包括:

刷新令牌生成模块,用于生成刷新令牌;还用于若第七判断模块判定所述刷新令牌有效且判定所述第三方应用合法之后生成刷新令牌;

第八发送模块,用于若所述第六判断模块判定所述访问令牌过期之后向所述第三方应用发送访问令牌过期信息;

所述第四发送模块,用于将所述访问令牌生成模块生成的所述访问令牌和所述刷新令牌生成模块生成的刷新令牌发送给所述第三方应用;

所述访问令牌生成模块,还用于若所述第七判断模块判定所述刷新令牌有效且判定所述第三方应用合法之后生成访问令牌;

所述访问令牌过期时间生成模块,还用于若所述第七判断模块判定所述刷新令牌有效且判定所述第三方应用合法之后获取服务器的当前时间,根据当前时间生成访问令牌过期时间;

所述第二保存模块,用于根据第四接收模块接收到的获取令牌请求中的所述应用标识符获取对应保存的访问权限列表,将所述访问令牌生成模块生成的访问令牌、所述访问令牌过期时间生成模块生成的所述访问令牌过期时间和所述刷新令牌生成模块生成的刷新令牌对应存储;

第六接收模块,用于接收所述第三方应用发送的更新令牌请求;

第七判断模块,用于判断所述刷新令牌是否有效,并根据所述应用标识符和所述应用密码判断所述第三方应用是否合法。

47. 如权利要求46所述的服务器,其特征在于,

所述第六接收模块,包括:

第二接收子模块,用于接收所述第三方应用发送的更新令牌请求;

第二解密子模块,用于将所述更新令牌请求中的所述应用密文信息解密获取所述应用标识符和所述应用密码。

48. 如权利要求37所述的服务器,其特征在于,还包括:

授权码过期时间生成模块,用于获取服务器当前时间作为授权码生成时间,根据授权码生成时间生成授权码过期时间;

所述第一判断模块,具体用于获取服务器当前时间和授权码过期时间,判断授权码是否过期;判断所述授权码是否有效,并根据所述应用标识符和所述应用密码判断所述第三方应用是否合法。

资源授权方法及系统和授权服务器及工作方法

技术领域

[0001] 本发明涉及通信领域,特别涉及资源授权方法及系统和授权服务器及工作方法。

背景技术

[0002] 目前资源授权是通过第三方应用获取到提供资源的应用的用户名和密码从而得到所有资源的访问权限,但是这种资源授权方式存在以下问题:第三方应用为了后续的服务会保存用户的密码,这样很不安全;第三方应用可以访问所有的资源,用户没有办法设置访问范围和有效期;用户只有修改提供资源的应用的密码才能收回第三方应用的访问权限;如果有一个第三方应用程序被破解,就会导致用户密码泄露,以及所有被密码保护的资源泄露。

发明内容

[0003] 本发明的目的是避免用户资源被滥用,提供资源授权方法及系统和资源授权服务器及工作方法。

[0004] 本发明方法是通过下述技术方案实现的:

[0005] 一种资源授权的方法,包括:

[0006] 步骤A1、第三方应用向授权服务器发送包含应用标识符的获取授权码请求;

[0007] 步骤A2、授权服务器根据应用标识符获取预存的重定向URL,以预存的访问权限列表为参数定向到授权页面,若接收到允许授权信息则生成授权码,将授权码、应用标识符和预存的访问权限列表对应存储;根据重定向URL向第三方应用回传授权码;

[0008] 步骤A3、第三方应用向授权服务器发送包含授权码、应用标识符和应用密码的获取令牌请求;

[0009] 步骤A4、授权服务器判断授权码是否有效,并根据应用标识符和应用密码判断第三方应用是否合法,若判断均为是则生成访问令牌,根据应用标识符获取预存的访问权限列表,将访问令牌和预存的权限列表对应存储,将访问令牌发送给第三方应用,否则结束。

[0010] 一种资源授权系统,包括第三方应用、授权服务器;

[0011] 第三方应用包括:

[0012] 第一发送模块,用于向授权服务器发送包含应用标识符的获取授权码请求;

[0013] 第一接收模块,用于接收授权服务器回传的授权码;

[0014] 第二发送模块,用于向授权服务器发送包含授权码、应用标识符和应用密码的获取令牌请求;

[0015] 第二接收模块,用于接收授权服务器发送的访问令牌;

[0016] 授权服务器包括:

[0017] 第三接收模块,用于接收获取授权码请求;

[0018] 第一获取模块,用于根据第三接收模块接收到的获取授权码请求中的应用标识符获取预存的重定向URL;

- [0019] 定向模块,用于以预存的访问权限列表为参数定向到授权页面,并接收允许授权信息;
- [0020] 授权码生成模块,若定向模块接收到允许授权信息后生成授权码;
- [0021] 第一保存模块,用于将授权码生成模块生成的授权码、应用标识符和预存的访问权限列表对应存储;
- [0022] 第三发送模块,用于根据第一获取模块获取到的重定向URL向第三方应用回传授权码生成模块生成的授权码;
- [0023] 第四接收模块,用于接收第三方应用发送的获取令牌请求;
- [0024] 第一判断模块,用于判断第四接收模块接收到的获取令牌请求中的授权码是否有效,并根据第四接收模块接收到的获取令牌请求中的应用标识符和应用密码判断第三方应用是否合法;
- [0025] 访问令牌生成模块,用于若第一判断模块判断均为是时生成访问令牌;
- [0026] 第二保存模块,用于根据第四接收模块接收到的获取令牌请求中的应用标识符获取预存的访问权限列表,将访问令牌生成模块生成的访问令牌和预存的权限列表对应存储;
- [0027] 第四发送模块,用于将访问令牌生成模块生成的访问令牌发送给第三方应用。
- [0028] 一种授权服务器的工作方法,包括:
- [0029] 步骤B1、当授权服务器接收到第三方应用发送的包含应用标识符的获取授权码请求时,根据应用标识符获取预存的重定向URL,以预存的访问权限列表为参数定向到授权页面,若接收到允许授权信息则生成授权码,将授权码、应用标识符和预存的访问权限列表对应存储;根据重定向URL向第三方应用回传授权码;
- [0030] 步骤B2、当授权服务器接收到第三方应用发送的包含授权码、应用标识符和应用密码的获取令牌请求时,判断授权码是否有效,并根据应用标识符和应用密码判断第三方应用是否合法,若判断均为是则生成访问令牌,根据应用标识符获取预存的访问权限列表,将访问令牌和预存的权限列表对应存储,将访问令牌发送给第三方应用,否则结束。
- [0031] 一种授权服务器,包括
- [0032] 第三接收模块,用于接收获授权码请求;
- [0033] 第一获取模块,用于根据第三接收模块接收到的获取授权码请求中的应用标识符获取预存的重定向URL;
- [0034] 定向模块,用于以预存的访问权限列表为参数定向到授权页面,并接收允许授权信息;
- [0035] 授权码生成模块,用于若定向模块接收到允许授权信息后生成授权码;
- [0036] 第一保存模块,用于将授权码生成模块生成的授权码、应用标识符和预存的访问权限列表对应存储;
- [0037] 第三发送模块,用于根据第一获取模块获取到的重定向URL向第三方应用回传授权码生成模块生成的授权码;
- [0038] 第四接收模块,用于接收第三方应用发送的获取令牌请求;
- [0039] 第一判断模块,用于判断第四接收模块接收到的获取令牌请求中的授权码是否有效,并根据第四接收模块接收到的获取令牌请求中的应用标识符和应用密码判断第三方应

用是否合法；

[0040] 访问令牌生成模块,用于若第一判断模块判断均为是时生成访问令牌；

[0041] 第二保存模块,用于根据第四接收模块接收到的获取令牌请求中的应用标识符获取预存的访问权限列表,将访问令牌生成模块生成的访问令牌和预存的权限列表对应存储；

[0042] 第四发送模块,用于将访问令牌生成模块生成的访问令牌发送给第三方应用。

[0043] 本发明方法的有益效果在于:可以控制第三方应用的访问权限和有效期,有效的防止资源泄露。

附图说明

[0044] 为了更清楚的说明本发明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的介绍,显而易见地,下面描述中的附图仅仅是本发明的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

[0045] 图1为本发明实施例2提供一种资源授权的方法的整体流程图；

[0046] 图2为本发明实施例2提供一种资源授权的方法的整体流程图；

[0047] 图3为本发明实施例3提供一种授权服务器的工作方法的流程图；

[0048] 图4为本发明实施例3提供一种授权服务器的工作方法的流程图；

[0049] 图5为本发明实施例4提供一种资源授权的系统的方框图。

具体实施方式

[0050] 下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,本领域技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都属于本发明保护的范围。

[0051] 实施例1

[0052] 本实施例提供一种资源授权的方法,包括:

[0053] 第三方应用预先在授权服务器中注册应用标识符、应用密码和重定向URL。

[0054] 步骤A1、第三方应用向授权服务器发送包含应用标识符的获取授权码请求；

[0055] 步骤A2、授权服务器根据应用标识符获取预存的重定向URL,以预存的访问权限列表为参数定向到授权页面,若接收到允许授权信息则生成授权码,将授权码、应用标识符和预存的访问权限列表对应存储;根据重定向URL向第三方应用回传授权码;

[0056] 具体的,访问权限列表具体为由资源标识形成的列表;

[0057] 优选的,步骤A1之后,在步骤A2之前还包括:授权服务器根据应用标识符判断第三方应用是否已注册,是则执行步骤A2,否则向授权服务器发送应用标识无效信息,结束。

[0058] 优选的,若获取授权码请求中还包括第一重定向URL时:

[0059] 步骤A2中,根据应用标识符获取预存的重定向URL之后,以预存的访问权限列表为参数定向到授权页面之前还包括:授权服务判断第一重定向URL与预存的重定向URL是否相同,是则以预存的访问权限列表为参数定向到授权页面,否则向第三方应用返回第一重定

向URL无效信息,结束。

[0060] 步骤A3、第三方应用向授权服务器发送包含授权码、应用标识符和应用密码的获取令牌请求;

[0061] 步骤A4、授权服务器判断授权码是否有效,并根据应用标识符和应用密码判断第三方应用是否合法,若判断均为是则生成访问令牌,根据应用标识符获取预存的访问权限列表,将访问令牌和预存的权限列表对应存储,将访问令牌发送给第三方应用,否则结束。

[0062] 优选的,步骤A3具体可以为:第三方应用将应用标识符与应用密码进行加密生成应用密文信息,发送包含应用密文信息和授权码的获取令牌请求;

[0063] 相应的,步骤A4中根据应用标识符和应用密码判断第三方应用是否合法具体包括,授权服务器从获取访问令牌请求中获取应用密文信息,将应用密文信息解密获取应用标识符和应用密码,根据应用标识符和应用密码判断第三方应用是否合法。

[0064] 优选的,若获取授权码请求中还包括第一访问权限列表;

[0065] 步骤A1与步骤A2之间还包括:授权服务器判断预存的访问权限列表是否包含第一访问权限列表,是则授权服务器以第一访问权限列表为参数定向到预存的授权页面,若接收到允许授权信息则生成授权码,将授权码、应用标识符和第一访问权限列表对应存储;根据重定向URL向第三方应用回传授权码;执行步骤A3;否则执行步骤A2;

[0066] 步骤A4中,生成访问令牌之后,将访问令牌发送给第三方应用之前还包括:授权服务器根据应用标识符获取第一访问权限列表,将访问令牌和第一访问权限列表对应存储。

[0067] 优选的,若允许授权信息中具体包括用户允许访问的资源的资源标识组成的第二访问权限列表;

[0068] 将授权码和应用标识符对应存储具体为:授权服务器将授权码、应用标识符和第二访问权限列表对应存储;

[0069] 生成访问令牌之后,将访问令牌发送给第三方应用之前还包括:授权服务器根据应用标识符获取第二访问权限列表,将访问令牌和第二访问权限列表对应存储。

[0070] 更进一步的,步骤A4之后还包括:

[0071] 步骤C1、第三方应用向资源服务器发送包含访问令牌和资源标识的获取资源请求;

[0072] 步骤C2、资源服务器将访问令牌和资源标识发送给授权服务器;

[0073] 步骤C3、授权服务器判断访问令牌是有效,判断与访问令牌访问对应保存的权限列表中是否包含资源标识,若判断均为是则向资源服务器发送包含资源标识的允许访问信息,执行步骤C4,否则结束;

[0074] 步骤C4、资源服务器将与资源标识相对应的资源发送给第三方应用。

[0075] 优选的,步骤A4还包括:授权服务器获取服务器的当前时间,根据当前时间生成访问令牌过期时间,并将访问令牌和访问令牌过期时间对应保存;

[0076] 相应的,步骤C2与步骤C3之间还包括:授权服务器根据访问令牌获取访问令牌过期时间,判断访问令牌是否过期,是则结束,否则执行步骤C3。

[0077] 优选的,步骤A4还包括:授权服务器生成刷新令牌,并将访问令牌、访问令牌过期时间和刷新令牌对应保存,将访问令牌和刷新令牌发送给第三方应用;

[0078] 若授权服务器判定访问令牌过期之后还包括:

[0079] 步骤D1、授权服务器向第三方应用发送访问令牌过期信息；

[0080] 步骤D2、第三方应用向授权服务器发送包含应用标识符、应用密码和刷新令牌的更新令牌请求；

[0081] 步骤D3、授权服务器判断刷新令牌是否有效，并根据应用标识符和应用密码判断第三方应用是否合法，若判断均为是则更新访问令牌，并生成新的访问令牌过期时间，返回步骤A4。

[0082] 实施例2

[0083] 本实施例提供一种资源授权方法，第三方应用在授权服务器中进行注册；授权服务器中运存有第三方应用的应用标识符、应用密码和重定向URL。本实施例以第三方应用请求用户信息为例进行说明，如图1和图2所示。

[0084] 步骤101、第三方应用向授权服务器发送包含应用标识符、第一重定向URL和第一访问权限列表的获取授权码请求。

[0085] 第一访问权限列表具体为第三方应用申请访问的资源标识列表，本实施例中，第一访问权限列表中包括：username和userAvatar，即用户名标识和用户头像标识；

[0086] 具体的，获取授权码请求具体为：

[0087] GET/authorize?response_type=code&client_id=s6BhdRkqt3&redirect_uri=https://client.example.com/cb&scope=username&userAvatarHTTP/1.1

[0088] Host:server.example.com

[0089] 其中，response_type=code表示授权请求类型是请求授权码；

[0090] client_id=s6BhdRkqt3表示应用标识符为s6BhdRkqt3；

[0091] redirect_uri=https://client.example.com/cb表示第一重定向URL为

[0092] https://client.example.com/cb；scope=username&userAvatar表示资源名称列表为userinfo、userinfo即用户信息标识，userAvatar即用户头像标识。

[0093] 若获取授权码请求中没有第一访问权限列表scope参数则表明第三方应用请求访问的资源为授权服务器中自定义的访问权限列表。授权请求中还包括：状态值state；

[0094] 步骤102、授权服务器根据获取授权码请求中的应用标识符判断第三方应用是否注册，是则执行步骤103，否则向第三方应用发送应用标识符无效信息，结束。

[0095] 优选的，步骤102还包括：授权服务器对获取授权码请求进行自定义的限制检查，若限制检查通过则执行步骤103，若限制检查未通过则执行错误提醒。自定义的限制检查可以包括：授权服务器判断获取授权码请求中是否缺少必需参数，本实施例中，必需参数为应用标识符和响应类型；授权服务器判断获取授权码请求中中是否存在不支持的参数；授权服务器判断获取授权码请求的格式是否正确。

[0096] 步骤103、授权服务器根据应用标识符获取预存的重定向URL，判断预存的重定向URL与第一重定向URL是否相同，是则执行步骤104，否则向第三方应用发送第一重定向URL无效信息，结束；

[0097] 优选的，授权服务器根据应用标识符获取授权服务器中预存的重定向URL，判断预存的重定向URL与第一重定向URL是否相同，是则执行步骤104，否则向第三方应用发送第一重定向URL无效信息，并提供如何执行匹配操作的建议，结束；

[0098] 步骤104、授权服务器定向到身份认证页面，并接收用户身份信息。

[0099] 步骤105、授权服务器判断用户身份信息是否合法,是则执行步骤106,否则向第三方应用发送身份认证失败信息,结束;

[0100] 授权服务器判断是否能查找到与用户身份信息相匹配的信息,是则用户身份信息合法,否则用户身份信息不合法。本实施例中,用户身份信息具体为用户名和密码的组合。

[0101] 若资源服务器中预存有用户信息则步骤105还可以为:

[0102] 步骤105-1、授权服务器将用户身份信息发送给资源服务器;

[0103] 步骤105-2、资源服务器判断用户身份信息是否合法,是则执行步骤106,否则向授权服务器发送身份认证失败信息,结束;

[0104] 步骤106、授权服务器根据应用标识符获取预存的访问权限列表,判断预存的访问权限列表是否包含第一访问权限列表,是则以第一访问权限列表为参数定向到授权页面,执行步骤107,否则以预存的访问权限列表为参数定向到的授权页面,执行步骤107;

[0105] 步骤107、授权服务器判断是否接收到允许授权信息,是则执行步骤108,否则向第三方应用发送授权失败信息,结束。

[0106] 授权页面中罗列访问权限列表中的所有资源标识。

[0107] 步骤108、授权服务器接收第二访问权限列表,并生成授权码和授权码过期时间;将应用标识符、授权码和第二访问权限列表对应存储;

[0108] 本实施例中,若用户同意第三方应用访问用户名和用户头像,则第二访问权限列表具体包括username和userAvatar;

[0109] 授权码可以为授权服务器分配的随机字符串,本实施例中的code授权码为Splxl0BeZQQYbYS6WxSbIA。

[0110] 步骤109、授权服务器根据预存的重定向URL向第三方应用回传授权码。

[0111] 具体的,授权服务器将预存的重定向URL与授权码顺序拼接生成第二重定向URL。授权服务器重定向到第二重定向URL。

[0112] 具体为:

[0113] HTTP/1.1 302 Found

[0114] Location:https://client.example.com/cb?code=Splxl0BeZQQYbYS6WxSbIA

[0115] 其中,code授权码为Splxl0BeZQQYbYS6WxSbIA。

[0116] 步骤110、第三方应用将应用标识符和应用密码通过预设加密运算进行加密生成应用密文信息;

[0117] 本实施例中,第三方应用通过Basic Authentication机制将应用标识符和应用密码生成应用密文信息。

[0118] 步骤111、第三方应用根据应用密文信息、第一重定向URL和授权码生成获取访问令牌请求,并向授权服务器发送获取访问令牌请求。

[0119] 获取授权令牌请求是通过JSON格式发送,具体为:

[0120] POST/token HTTP/1.1

[0121] Host:server.example.com

[0122] Authorization:Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW

[0123] Content-Type:application/x-www-form-urlencoded

[0124] grant_type=authorization_code&code=Splxl0BeZQQYbYS6WxSbIA&redirect_

uri=https://client.example.com/cb

[0125] 其中,Authorization授权参数为Basic czZCaGRSa3F0MzpnWD

[0126] FmQmF0M2JW,其中,Basic为[RFC2617]定义的HTTP Basic验证机制;

[0127] czZCaGRSa3F0MzpnWD FmQmF0M2JW为通过Basic Authentication机制根据应用标识符和应用密码生成密文应用信息。grant_type授权类型为authorization_code,即授权码模式,code授权码为Splxl0BeZQQYbYS6WxSbIA,redirect_uri重定向URL为https://client.example.com/cb;

[0128] 步骤112、授权服务器从获取访问令牌请求中获取应用密文信息,对应用密文信息进行解密得到应用标识符和应用密码;

[0129] 步骤113、授权服务器根据应用标识符和应用密码判断第三方应用是否合法,是则执行步骤114,否则向第三方应用发送认证失败信息,结束;

[0130] 步骤114、授权服务器判断是否可以查询到与第一重定向URL和授权码匹配的信息,是则执行步骤115,否则向第三方应用发送认证失败信息,结束;

[0131] 步骤115、授权服务器根据授权码获取授权码过期时间,判断授权码是否过期,是则执行步骤116;否则向第三方应用返回授权码过期信息,结束;

[0132] 具体的,本实施例中,授权服务器获取服务器的当前时间,判断授权码过期时间是否大于服务器当前时间,是则授权服务器判定授权码没有过期,执行步骤116,否则授权服务器判定授权码过期,向第三方应用返回授权码过期信息,结束。

[0133] 步骤116、授权服务器生成访问令牌、刷新令牌和访问令牌过期时间,根据授权码获取第二访问权限列表,将访问令牌、第二访问权限列表和访问令牌过期时间对应存储;

[0134] 步骤117、授权服务器根据访问令牌、访问令牌过期时间和刷新令牌生成获取访问令牌响应,并将获取访问令牌响应发送至第三方应用;

[0135] 访问令牌可以为授权服务器分配的随机字符串,本实施例中的访问令牌具体为tGzv3J0kF0XG5Qx2TlKWIA;

[0136] 本实施例中的访问令牌、令牌类型、过期时间和刷新令牌等信息是通过JSON格式发送的;获取访问令牌响应具体为:

[0137] HTTP/1.1 200 OK

[0138] Content-Type:application/json;charset=UTF-8

[0139] Cache-Control:no-store

[0140] {

[0141] "access_token":"2YotnFZFEjrlzCsicMWpAA",

[0142] "token_type":"example",

[0143] "expires_in":3600,

[0144] "refresh_token":"tGzv3J0kF0XG5Qx2TlKWIA",

[0145] }

[0146] 授权服务器生成的访问令牌access_token具体为2YotnFZ FEjrlzCsicMWpAA;令牌类型token_type为example;过去时间expires_in为3600,表明访问令牌自授权服务器产生的时刻起,将在3600s之后过期;刷新令牌refresh_token为tGzv3J0kF0XG5Qx2TlK WIA。

[0147] 步骤118、第三方应用向资源服务器发送包含访问令牌和资源标识的获取资源请

求。

[0148] 本实施例中,第三方应用请求的资源标识为username,即用户名标识,获取资源请求具体如下:

[0149] POST/resourcesAPI/username/HTTP/1.1

[0150] Host:localhostExample:8000

[0151] Authorization:2YotnFZFEjrlzCsicMWpAA

[0152] Username为用户名标识,2YotnFZFEjrlzCsicMWpAA为访问令牌;

[0153] 步骤119、资源服务器将访问令牌和资源标识发送给授权服务器;

[0154] 步骤120、授权服务器判断访问令牌是有效,是则执行步骤121,否则向第三方应用发送访问令牌无效信息,结束。

[0155] 具体的,授权服务器判断是否可以查找到与访问令牌匹配的信息,是则执行步骤121,否则向第三方应用发送访问令牌无效信息,结束;

[0156] 步骤121、授权服务器根据访问令牌获取第二访问权限列表,判断第二访问权限列表中是否包含资源标识,是则执行步骤122,否则向第三方应用发送请求超范围信息,结束。

[0157] 步骤122、授权服务器获取当前时间并根据访问令牌获取访问令牌过期时间判断访问令牌是否过期,是则向第三方应用发送访问令牌过期信息,执行步骤123;否则向资源服务器发送包含资源标识的允许访问信息,执行步骤123;

[0158] 步骤123、资源服务器向第三方应用发送与资源标识对应的资源,结束。

[0159] 具体的,资源服务器中的每种资源都对应一个资源标识,本实施例中,资源服务器根据username获取对应的资源,即用户名,并将用户名发送给第三方应用。

[0160] 步骤124、第三方应用将应用标识符和应用密码通过预设加密运算进行加密生成应用密文信息,根据应用密文信息和刷新令牌生成更新令牌请求,并将更新令牌请求发送给授权服务器;

[0161] 具体的,更新令牌请求是通过JSON格式发送的,具体为:

[0162] POST/token HTTP/1.1

[0163] Host:server.example.com

[0164] Authorization:Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW

[0165] Content-Type:application/x-www-form-urlencoded

[0166] grant_type=refresh_token&refresh_token=tGzv3J0kF0XG5Qx2TlKWIA

[0167] 其中,Authorization授权参数为Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW,其中,Basic为[RFC2617]定义的HTTP Basic验证机制;czZCaGRSa3F0MzpnWDFmQmF0M2JW为应用标识符和应用密码通过Basic Authentication生成的应用密文信息,grant_type授权类型为refresh_token,即更新令牌;refresh_token更新令牌为tGzv3J0kF0XG5Qx2TlKWIA。

[0168] 步骤125、授权服务器从更新令牌请求中获取应用密文信息,对应用密文信息进行解密得到应用标识符和应用密码;

[0169] 步骤126、授权服务器根据应用标识符和应用密码判断第三方应用是否合法,是则执行步骤127,否则向第三方应用发送认证失败信息,结束;

[0170] 步骤127、授权服务器判断刷新令牌是否有效,是则执行步骤128,否则向第三方应用发送刷新令牌无效信息,结束

[0171] 具体的,授权服务器判断是否可以查询到与更新令牌请求中的刷新令牌一致的信息,是则执行步骤128,否则向第三方应用发送刷新令牌无效信息,结束;

[0172] 步骤128、授权服务器更新访问令牌、刷新令牌和访问令牌过期时间,并将更新后的访问令牌、刷新令牌访问令牌过期时间和第二访问权限列表对应保存,返回步骤117。

[0173] 以上所述的实施例只是本发明较优选的具体实施方式,本领域的技术人员在本发明技术方案范围内进行的通常变化和替换都应包含在本发明的保护范围内。

[0174] 实施例3

[0175] 本实施例提供一种授权服务器的工作方法,下面以第三方应用向资源服务器获取用户名为例进行说明:授权服务器中预存有第三方应用的应用标识符、应用密码和重定向URL,如图3和图4所示,包括:

[0176] 步骤201、授权服务器接收到第三方应用发送的包含应用标识符、第一重定向URL和第一访问权限列表的获取授权码请求,并根据获取授权码请求中的应用标识符判断第三方应用是否注册,是则执行步骤202,否则授权服务器向第三方应用发送应用标识符无效信息,结束。

[0177] 获取授权码请求具体包括:第三方应用的应用标识符、第一重定向URL和第一访问权限列表。

[0178] 第一访问权限列表具体为第三方应用申请访问的资源标识列表,本实施例中,第一访问权限列表中包括:username和userAvatar,即用户名标识和用户头像标识;

[0179] 具体的,获取授权码请求具体为:

[0180] GET/authorize?response_type=code&client_id=s6BhdRkqt3&redirect_uri=https://client.example.com/cb&scope=username&userAvatarHTTP/1.1

[0181] Host:server.example.com

[0182] 其中,response_type=code表示授权请求类型是请求授权码;

[0183] client_id=s6BhdRkqt3表示应用标识符为s6BhdRkqt3;

[0184] redirect_uri=https://client.example.com/cb表示第一重定向URL为https://client.example.com/cb;scope=username&userAvatar表示资源名称列表为userinfo、userinfo即用户信息标识,userAvatar即用户头像标识。

[0185] 若获取授权码请求中没有第一访问权限列表scope参数则表明第三方应用请求访问的资源为授权服务器中自定义的访问权限列表。授权请求中还包括:状态值state;

[0186] 优选的,步骤201还包括:授权服务器对授权请求进行自定义的限制检查,若限制检查通过,执行步骤203若限制检查未通过返回错误提醒。自定义的限制检查可以包括:授权服务器判断授权请求中是否缺少必需参数,本实施例中,必需参数为应用标识符以及响应类型;授权服务器判断授权请求中是否存在不支持的参数;授权服务器判断授权请求格式是否正确。

[0187] 步骤202、授权服务器根据应用标识符获取预存的重定向URL,判断预存的重定向URL与第一重定向URL是否相同,是则执行步骤203,否则授权服务器向第三方应用发送第一重定向URL无效信息,结束;

[0188] 具体的,授权服务器根据应用标识符获取授权服务器中预存的重定向URL,判断授权请求码中的第一重定向URL是否与授权服务器中预存的重定向URL是否一致,是则执行步

骤203,否则向第三方应用发送第一重定向URL无效信息,并提供如何执行匹配操作的建议,结束;

[0189] 步骤203、授权服务器定向到身份认证页面,并接收用户身份信息;

[0190] 步骤204、授权服务器判断用户身份信息是否合法,是则执行步骤205,否则授权服务器向第三方应用发送用户身份信息不合法信息,结束。

[0191] 具体的,授权服务器判断是否能查找到与用户身份信息相匹配的信息,是则用户身份信息合法,否则用户身份信息不合法。本实施例中,用户身份信息具体为用户名和密码的组合。

[0192] 步骤205、授权服务器根据应用标识符获取预存的访问权限列表,判断预存的访问权限列表是否包含第一访问权限列表,是则以第一访问权限列表为参数定向到授权页面,执行步骤206,否则以预存的访问权限列表为参数定向到的授权页面,执行步骤206;

[0193] 步骤206、授权服务器接受第二访问权限列表,并生成授权码和授权码过期时间;将应用标识符、授权码和第二访问权限列表对应存储;

[0194] 步骤207、授权服务器根据预存的重定向URL向第三方应用回传授权码。

[0195] 具体的,授权服务器将预存的重定向URL与授权码顺序拼接生成第二重定向URL。授权服务器重定向到第二重定向URL。

[0196] 具体为:

[0197] HTTP/1.1 302 Found

[0198] Location:https://client.example.com/cb?code=Sp1x10BeZQQYbYS6WxSbIA

[0199] 其中,code授权码为Sp1x10BeZQQYbYS6WxSbIA。

[0200] 步骤208、授权服务器接收到第三方应用发送的获取访问令牌请求,并从获取访问令牌请求中获取应用密文信息,并对应用密文信息进行解密得到应用标识符和应用密码。

[0201] 获取令牌请求包括:应用密文信息、授权码和第二重定向URL。

[0202] 步骤209、授权服务器根据应用标识符和应用密码判断第三方应用是否合法,是则执行步骤210,否则授权服务器向第三方应用发送认证失败信息,结束。

[0203] 步骤210、授权服务器判断是否可以查询到与第二重定向URL和授权码匹配的信息,是则执行步骤211,否则授权服务器向第三方应用发送认证失败信息,结束;

[0204] 步骤211、授权服务器根据授权码获取授权码过期时间,判断授权码是否过期,是则授权服务器向第三方应用返回授权码过期信息,结束,否则执行步骤212;;

[0205] 具体的,本实施例中,授权码的有效期为预设值,授权服务器获取服务器的当前时间,判断授权码生成时间与预设值之和是否大于服务器当前时间,是则授权服务器判定授权码没有过期,执行步骤212,否则授权服务器判定授权码过期,向第三方应用返回授权码过期信息,结束。

[0206] 步骤212、授权服务器生成访问令牌、刷新令牌和访问令牌过期时间,根据授权码获取第二访问权限列表,将访问令牌、第二访问权限列表和访问令牌过期时间对应存储;

[0207] 访问令牌为授权服务器生成的随机字符串;

[0208] 步骤213、授权服务器将访问令牌、访问令牌过期时间和刷新令牌发送至第三方应用;

[0209] 本实施例中的访问令牌、令牌类型、过期时间和刷新令牌等信息是通过JSON格式

发送的;具体为:

[0210] HTTP/1.1 200 OK

[0211] Content-Type:application/json;charset=UTF-8

[0212] Cache-Control:no-store

[0213] {

[0214] "access_token":"2YotnFZFEjrlzCsicMWpAA",

[0215] "token_type":"example",

[0216] "expires_in":3600,

[0217] "refresh_token":"tGzv3J0kF0XG5Qx2TlKWIA",

[0218] }

[0219] 授权服务器生成的访问令牌access_token具体为2YotnFZ FEjrlzCsicMWpAA;令牌类型token_type为example;过去时间expires_in为3600,表明访问令牌自授权服务器产生的时刻起,将在3600s之后过期;刷新令牌refresh_token为tGzv3J0kF0XG5Qx2TlKWIA。

[0220] 步骤214、授权服务器接收到资源服务器发送的资源标识和访问令牌,判断访问令牌是有效,是则执行步骤215,否则授权服务器向第三方应用发送访问令牌无效信息,结束。

[0221] 具体的,授权服务器判断是否可以查找到与访问令牌相同的信息,是则执行步骤215,否则向第三方应用发送访问令牌无效信息,结束;

[0222] 步骤215、授权服务器根据访问令牌获取第二访问权限列表,判断第二访问权限列表中是否包含资源标识,是则执行步骤216,否则授权服务器向第三方应用发送请求超范围信息,结束。

[0223] 步骤216、授权服务器获取当前时间并根据访问令牌获取过期时间判断访问令牌是否过期,是则执行步骤217;否则向资源服务器发送包含资源标识信息的允许访问信息,结束;

[0224] 步骤217、授权服务器接收到第三方应用发送的更新令牌请求,将更新令牌请求中的应用密文信息进行解密得到应用标识符和应用密码。

[0225] 步骤218、授权服务器根据应用标识符和应用密码判断第三方应用是否合法,是则执行步骤219,否则授权服务器向第三方应用发送认证失败信息,结束;

[0226] 步骤219、授权服务器判断更新令牌请求中的刷新令牌是否有效,是则执行步骤220,否则授权服务器向第三方应用发送刷新令牌无效信息,结束;

[0227] 步骤220、授权服务器更新访问令牌、刷新令牌和访问令牌过期时间,并将更新访问令牌、刷新令牌访问令牌过期时间和第二访问权限列表对应保存,返回步骤213。

[0228] 实施例4

[0229] 本实施例提供一种资源授权的系统,包括第三方应用、授权服务器;

[0230] 第三方应用包括:

[0231] 第一发送模块11,用于向授权服务器发送包含应用标识符的获取授权码请求;

[0232] 第一接收模块12,用于接收授权服务器回传的授权码;

[0233] 第二发送模块13,用于向授权服务器发送包含授权码、应用标识符和应用密码的获取令牌请求;

[0234] 具体的,第二发送模块13包括:

- [0235] 第一加密子模块,用于将应用标识符与应用密码进行加密生成应用密文信息;
- [0236] 第一发送子模块,用于向授权服务器发送包含应用密文信息和授权码的获取令牌请求;
- [0237] 第二接收模块14,用于接收授权服务器发送的访问令牌;
- [0238] 授权服务器包括:
- [0239] 第三接收模块15,用于接收获授权码请求;
- [0240] 第一获取模块16,用于根据第三接收模块15接收到的获取授权码请求中的应用标识符获取预存的重定向URL;
- [0241] 定向模块17,用于以预存的访问权限列表为参数定向到授权页面,并接收允许授权信息;
- [0242] 具体的,访问权限列表具体为由资源标识形成的列表。
- [0243] 授权码生成模块18,用于定向模块17接收到允许授权信息后生成授权码;
- [0244] 第一保存模块19,用于将授权码生成模块18生成的授权码、应用标识符和预存的访问权限列表对应存储;
- [0245] 第三发送模块20,用于根据第一获取模块16获取到的重定向URL向第三方应用回传授权码生成模块18生成的授权码;
- [0246] 第四接收模块21,用于接收第三方应用发送的获取令牌请求;
- [0247] 具体的,第四接收模块21包括:
- [0248] 第一接收子模块,用于接收第三方应用发送的获取令牌请求;
- [0249] 第一解密模块,用于从获取访问令牌请求中获取应用密文信息,将应用密文信息解密获取应用标识符和应用密码。
- [0250] 第一判断模块22,用于判断第四接收模块21接收到的获取令牌请求中的授权码是否有效,并根据第四接收模块21接收到的获取令牌请求中的应用标识符和应用密码判断第三方应用是否合法;
- [0251] 访问令牌生成模块23,用于若第一判断模块22判断均为是时生成访问令牌;
- [0252] 第二保存模块24,用于根据第四接收模块21接收到的获取令牌请求中的应用标识符获取预存的访问权限列表,将访问令牌生成模块23生成的访问令牌和预存的权限列表对应存储;
- [0253] 第四发送模块24,用于将访问令牌生成模块23生成的访问令牌发送给第三方应用。
- [0254] 第三保存模块,用于保存第三方应用的应用标识符、应用密码和重定向URL。
- [0255] 优选的,授权服务器还包括:第二判断模块,用于根据第三接收模块15接收到的获取授权码请求中的应用标识符判断第三方应用是否已注册;
- [0256] 相应的,第一获取模块16,具体用于若第二判断模块判定第三方应用已注册之后根据第三接收模块15接收到的获取授权码请求中的应用标识符获取预存的重定向URL。
- [0257] 优选的,若第三接收模块15接收到的获取授权码请求中还包括第一访问权限列表;
- [0258] 相应的,授权服务器还包括:
- [0259] 第四判断模块,用于判断预存的访问权限列表是否包含第一访问权限列表;

[0260] 定向模块17,具体用于若第四判断模块判定预存的访问权限列表包含第一访问权限列表时以第一访问权限列表为参数定向到授权页面,并接收允许授权信息;第一保存模块19,用于将授权码生成模块18生成的授权码、应用标识符和第一访问权限列表对应存储;第二保存模块24,用于将访问令牌生成模块18生成的访问令牌和根据获取令牌请求中的应用标识符获取到第一访问权限列表对应存储;

[0261] 定向模块17,还用于若第四判断模块判定预存的访问权限列表不包含第一访问权限列表时以预存的访问权限列表为参数定向到授权页面,并接收允许授权信息;第一保存模块19,还用于将授权码生成模块18生成的授权码、应用标识符和预存的访问权限列表对应存储;第二保存模块24,还用于将所述访问令牌生成模块23生成的访问令牌和根据获取令牌请求中的应用标识符获取到的预存的访问权限列表对应存储;

[0262] 进一步的,若第三接收模块15接收到的获取授权码请求中还包括第一重定向URL;

[0263] 相应的,授权服务器还包括:

[0264] 第三判断模块,用于判断第一重定向URL与第一获取模块16获取到的预存的重定向URL是否相同;

[0265] 定向模块17,具体用于若第三判断模块判定第一重定向URL与第一获取模块16获取到的预存的重定向URL相同时根据第三接收模块15接收到的获取授权码请求中的应用标识符获取预存的重定向URL。

[0266] 进一步的,若定向模块17接收到的允许访问信息中包括用户允许访问的资源的资源标识组成的第二访问权限列表;

[0267] 相应的,第一保存模块19,还用于将授权码生成模块18的授权码、应用标识符和定向模块17接收到的允许访问信息中包含的第二访问权限列表对应存储;

[0268] 第二保存模块24,还用于将访问令牌生成模块23生成的访问令牌和将定向模块17接收到的允许访问信息中包含的第二访问权限列表对应存储。

[0269] 若资源授权系统还包括资源服务器;

[0270] 第三方应用还包括:

[0271] 第五发送模块,用于向资源服务器发送包含访问令牌和资源标识的获取资源请求;

[0272] 资源服务器,包括:

[0273] 第六发送模块,用于接收第三方应用发送的获取资源请求,并将获取资源请求中的访问令牌和资源标识发送给授权服务器;

[0274] 第五接收模块,用于接收授权服务器发送的允许访问信息,向第三方应用发送与资源标识相对应的资源;

[0275] 授权服务器还包括:

[0276] 第五判断模块,用于接收资源服务器发送的访问令牌和资源标识;判断访问令牌是否有效,判断与访问令牌访问对应的权限列表中是否包含资源标识;

[0277] 第七发送模块,用于若第五判断模块判断均为是时向资源服务器发送包含资源标识的允许访问信息。

[0278] 授权服务器还包括:访问令牌过期时间生成模块,用于获取服务器的当前时间,根据当前时间生成访问令牌过期时间;

[0279] 相应的,第二保存模块24,还用于根据第四接收模块21接收到的获取令牌请求中的应用标识符获取对应保存的访问权限列表,将访问令牌生成模块23生成的访问令牌和访问令牌过期时间生成模块生成的访问令牌过期时间对应存储;

[0280] 第六判断模块,用于根据访问令牌获取访问令牌过期时间,判断访问令牌是否过期;

[0281] 第七判断模块,用于若第六判断模块判定访问令牌没有过期之后接收资源服务器发送的访问令牌和资源标识;判断访问令牌是有效,判断与访问令牌访问对应的权限列表中是否包含资源标识。

[0282] 授权服务器还包括:刷新令牌生成模块,用于生成刷新令牌;还用于若第七判断模块判定判断刷新令牌有效且判定第三方应用合法之后生成刷新令牌;

[0283] 第八发送模块,用于若第六判断模块判定访问令牌过期之后向第三方应用发送访问令牌过期信息;

[0284] 相应的,第四发送模块25,还用于将访问令牌生成模块23生成的访问令牌和刷新令牌生成模块生成的刷新令牌发送给第三方应用;

[0285] 访问令牌生成模块23,还用于若第七判断模块判定判断刷新令牌有效且判定第三方应用合法之后生成访问令牌;

[0286] 访问令牌过期时间生成模块,还用于若第七判断模块判定判断刷新令牌有效且判定第三方应用合法之后获取服务器的当前时间,根据当前时间生成访问令牌过期时间;

[0287] 第二保存模块24,还用于根据第四接收模块21接收到的获取令牌请求中的应用标识符获取对应保存的访问权限列表,将访问令牌生成模块23生成的访问令牌、访问令牌过期时间生成模块生成的访问令牌过期时间和刷新令牌生成模块生成的刷新令牌对应存储;

[0288] 第六接收模块,用于接收第三方应用发送的更新令牌请求;

[0289] 第六接收模块,包括:

[0290] 第二接收子模块,用于接收第三方应用发送的更新令牌请求;

[0291] 第二解密子模块,用于将更新令牌请求中的应用密文信息解密获取应用标识符和应用密码。

[0292] 第七判断模块,用于判断刷新令牌是否有效,并根据应用标识符和应用密码判断第三方应用是否合法;

[0293] 第三方应用还包括:

[0294] 第八发送模块,用于向授权服务器发送包含应用标识符、应用密码和刷新令牌的更新令牌请求。

[0295] 第八发送模块,包括:

[0296] 第二加密子模块,用于将应用标识符和应用密码进行加密生成应用密文信息;

[0297] 第二发送子模块,用于发送包含应用密文信息和刷新令牌的更新令牌请求;

[0298] 授权服务器中还包括:授权码过期时间生成模块,用于获取服务器当前时间作为授权码生成时间,根据授权码生成时间生成授权码过期时间;

[0299] 相应的,第一判断模块22,具体用于获取服务器当前时间和授权码过期时间,判断授权码是否过期;判断授权码是否有效,并根据应用标识符和应用密码判断第三方应用是否合法。

[0300] 以上所述,仅为本发明较佳的具体实施方式,但本发明的保护范围并不局限于此,任何熟悉本技术领域的技术人员在本发明揭露的技术范围内,可轻易想到的变化或替换,都应涵盖在本发明的保护范围之内。因此,本发明的保护范围应以权利要求的保护范围为准。

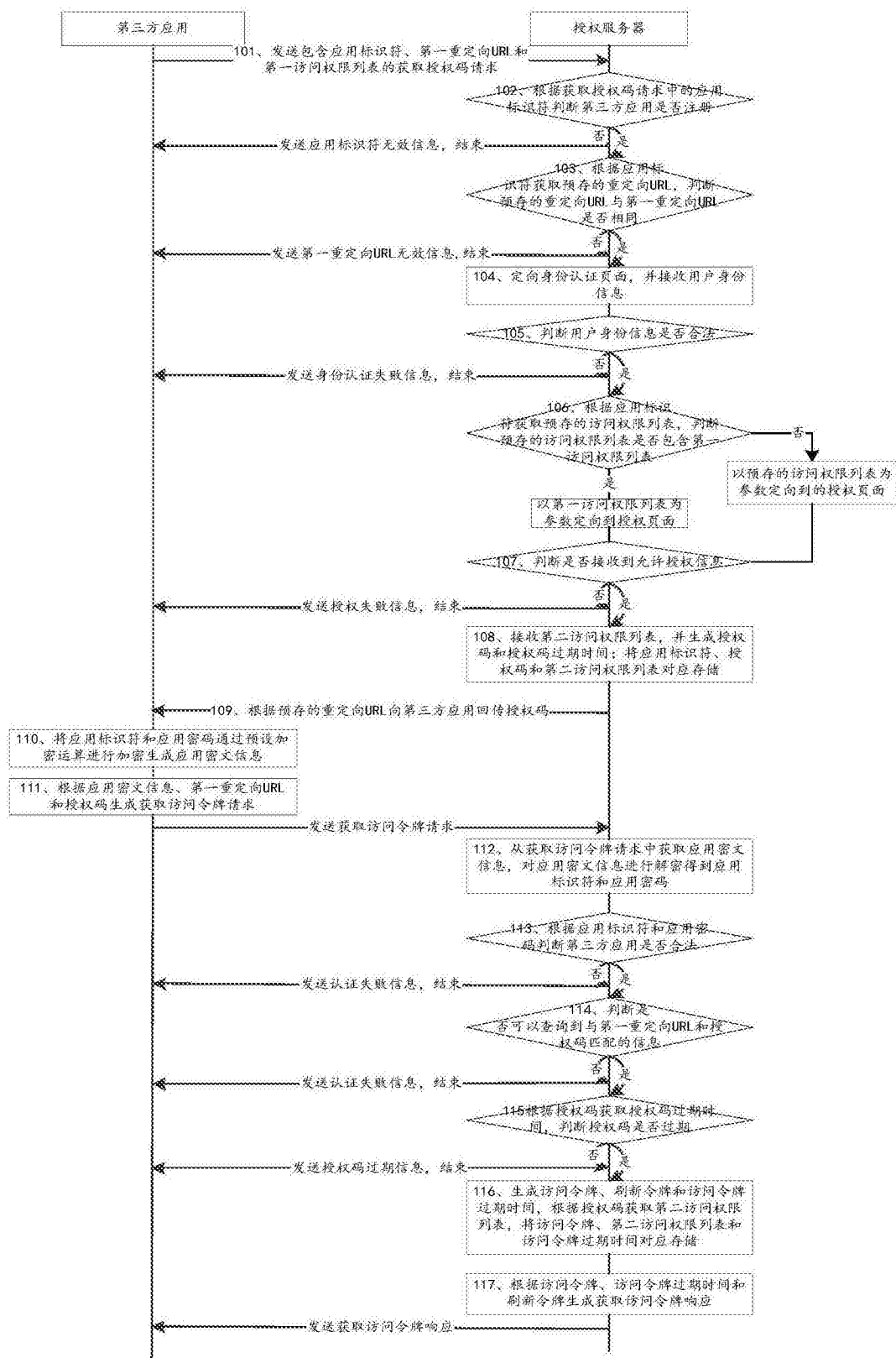


图1

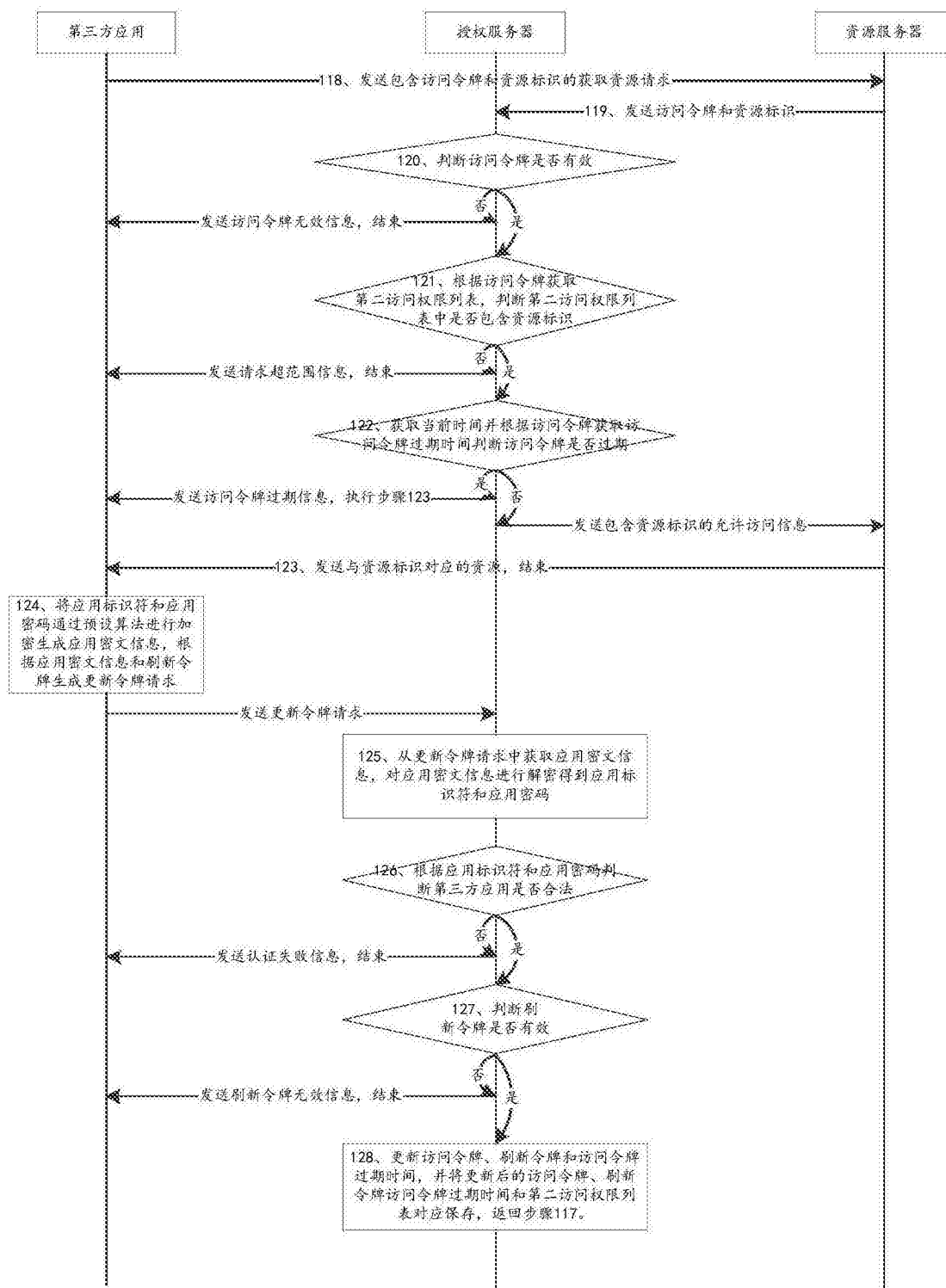


图2

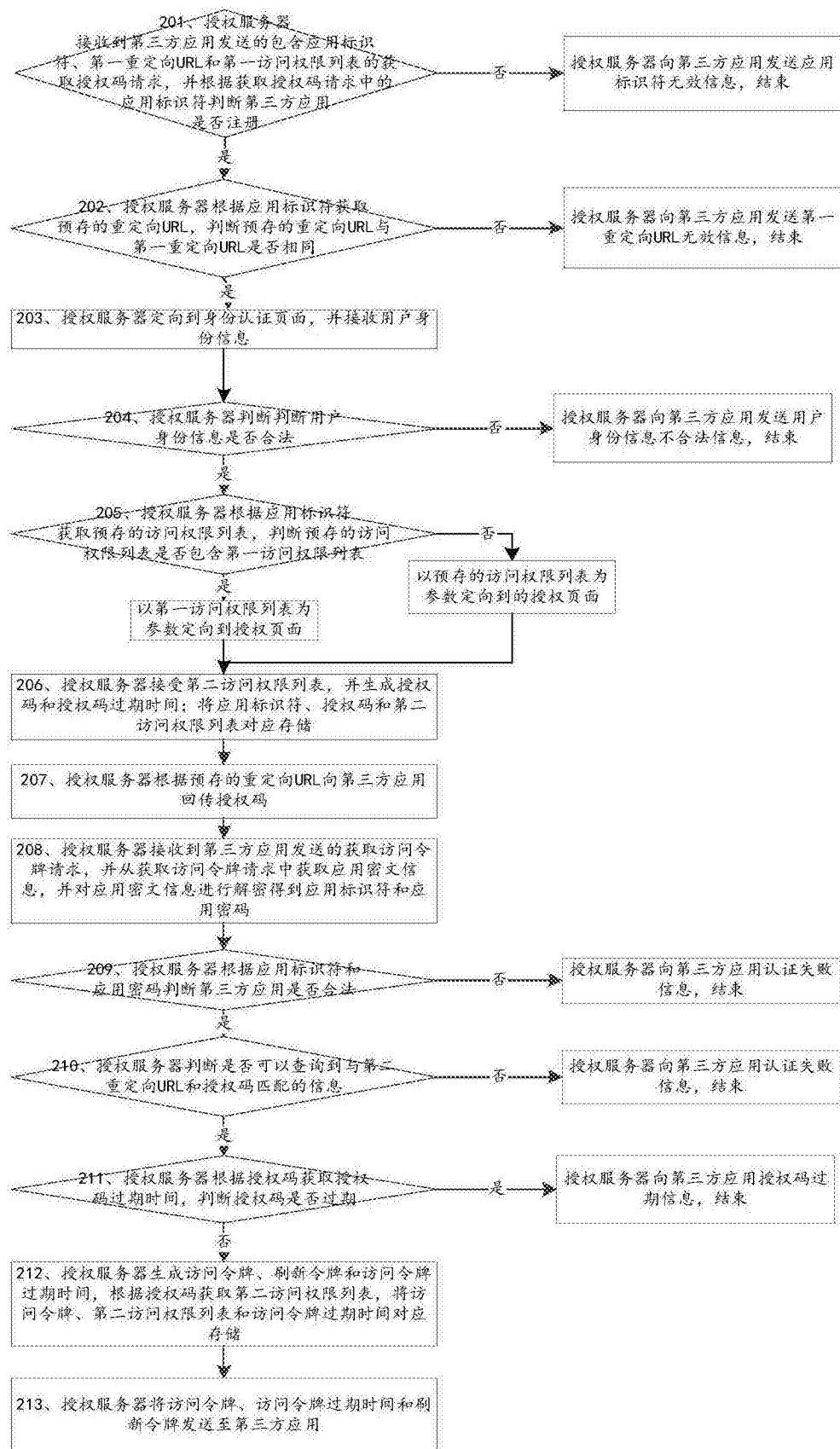


图3

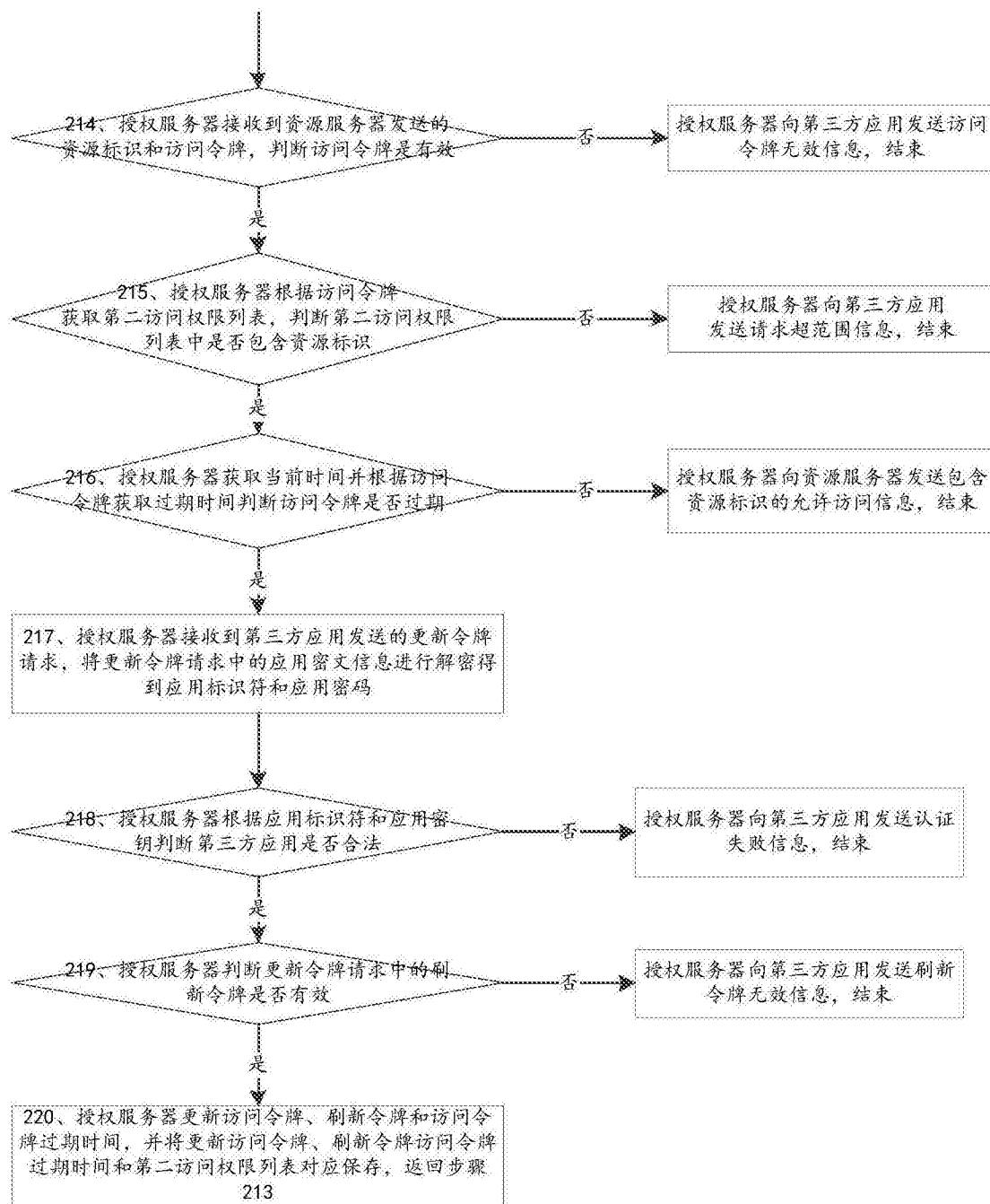


图4

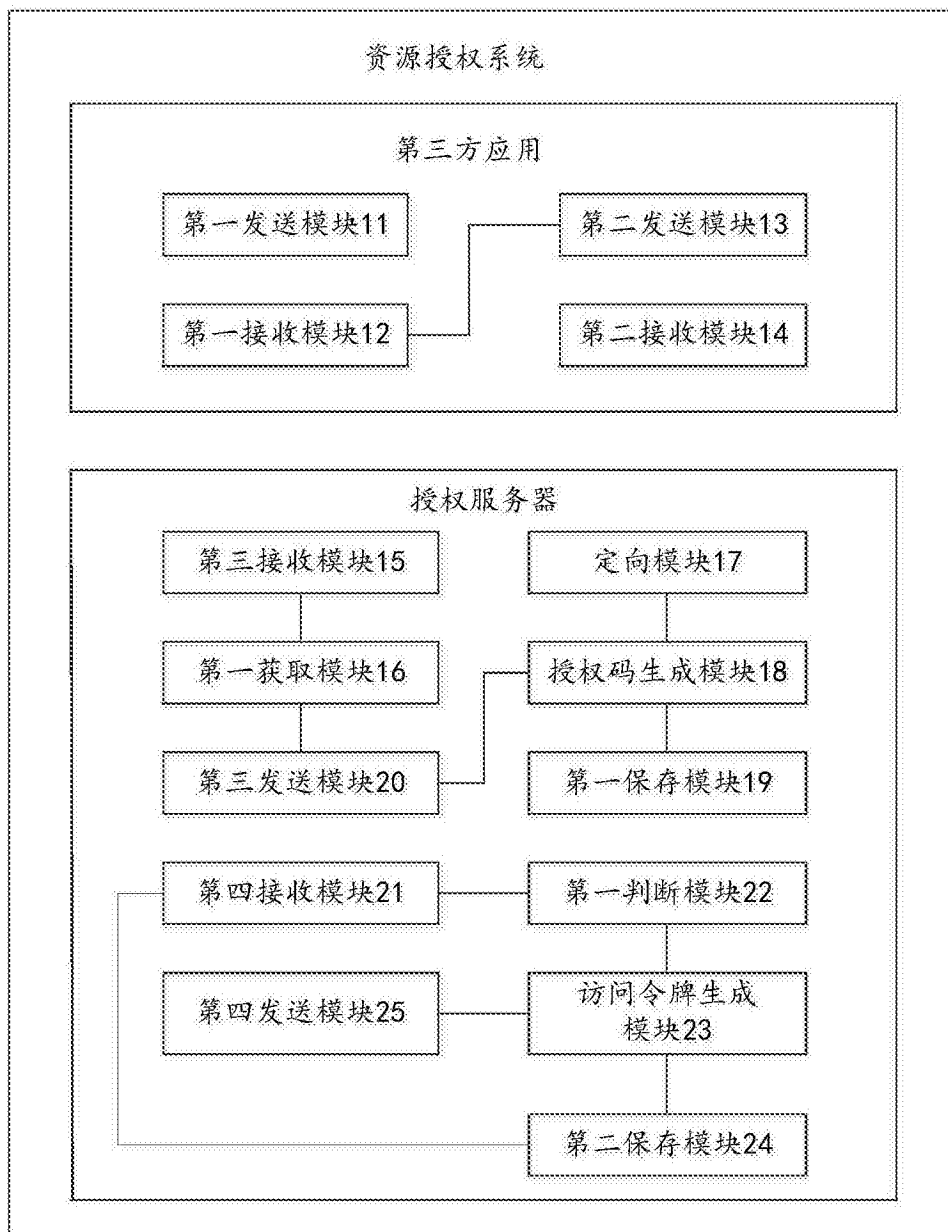


图5