V 订阅 H5 接入安全规范及实施方案

文档修订历史

修订版本	修订作者	修订备注
1.0	苏钟伟	初稿

目 录

1 概述 3

1.1 背景 3

1.2 名词解释 3

1.3 参考资料 3

2 安全标准规范 4

2.1 安全标准解释 4

2.2 业务流程图 5

2.3 方案实施流程图 6

1 概述

1.1 背景

H5 消息订阅由于暴露在开放的公域 H5 页面上，并且 deeplink 方式无法稳定的被动校验来源方合法标识，所以需要 CP 在订阅时主动带上身份标识（token）进行请求，并且 CP 在获取有效 token 的同时需要进行请求自身的合法校验。

1.2 名词解释

CP：合作接入方

deeplink：一种服务拉起方式规范

token：调用方的合法身份标识，一般由服务方通过调用方的注册开发者账号及秘钥信息生成

1.3 参考资料

微信 H5 支付：https://pay.weixin.qq.com/wiki/doc/apiv3/open/pay/chapter2_6_2.shtml

2 安全标准规范

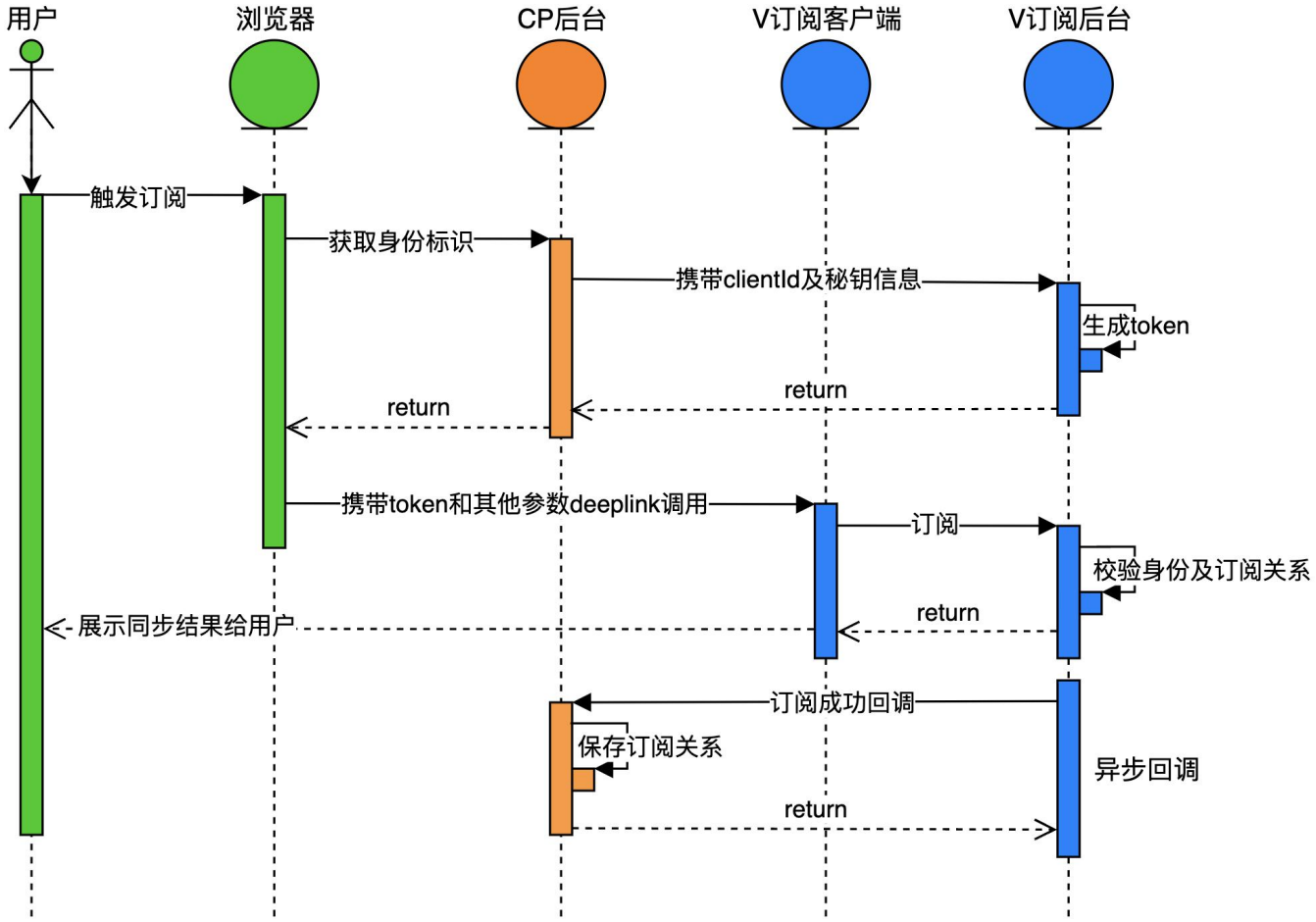
2.1 安全标准解释

浏览器到 V 订阅客户端及到 V 订阅服务器端采用 token 进行身份校验，安全上达到要求。浏览器到 CP 服务后台获取 token 这一环节如果没有身份识别措施会导致攻击者随意拿到合法的 token 信息进行攻击，所以推荐以下两种安全校验措施：

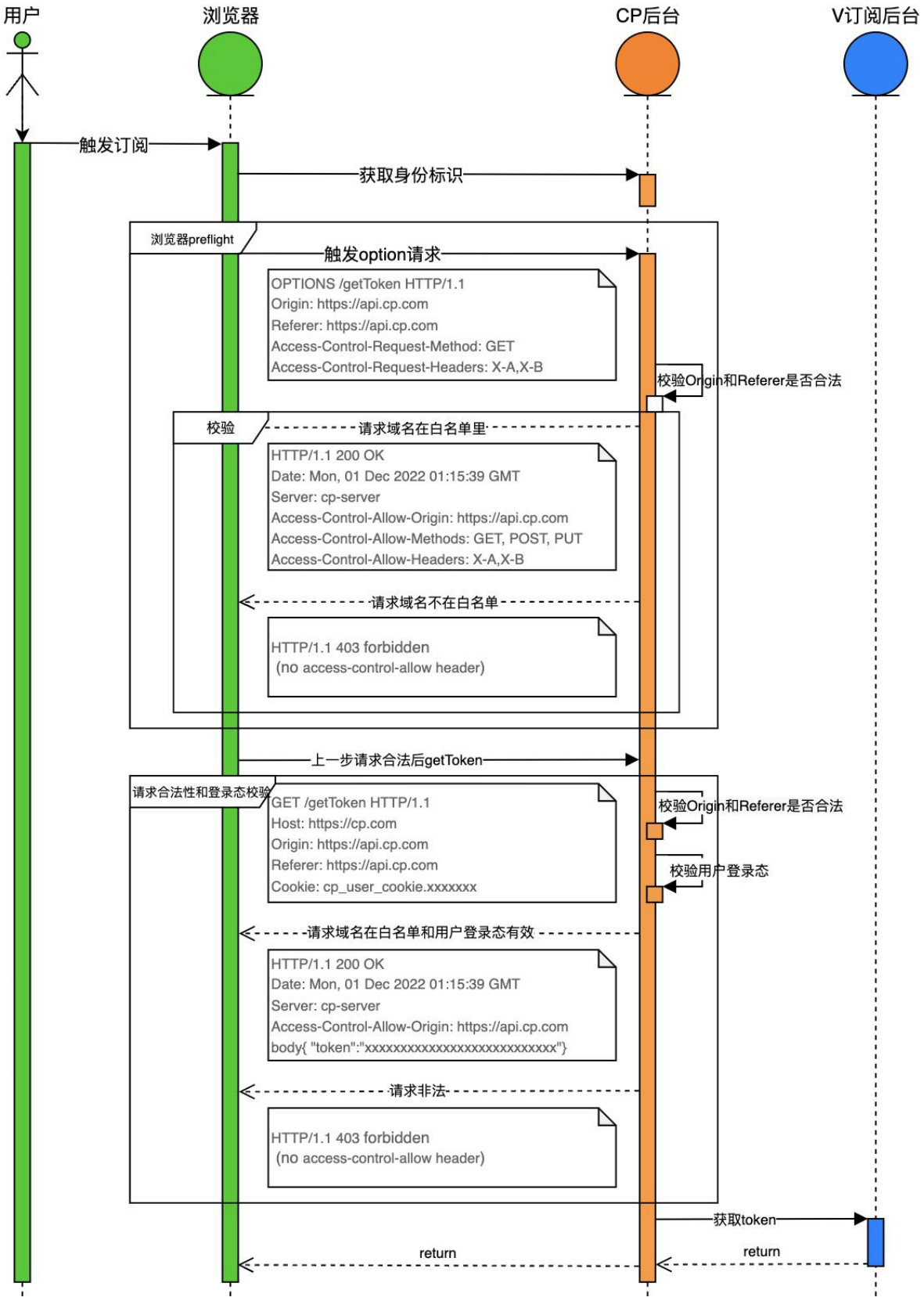
1）http 请求头校验请求来源域名是否是白名单内的（Origin、Referer），因为 Origin 在某些情况下不完整所以这里加上 Referer 一同校验；

2）在 1 的基础上校验用户系统的登录态是否合法（用户账号密码等方式登录）。

2.2 业务流程图


用户
浏览器
CP后台
V订阅客户端
V订阅后台
触发订阅
获取身份标识
携带clientId及秘钥信息
生成token
return
return
携带token和其他参数deeplink调用
订阅
校验身份及订阅关系
return
展示同步结果给用户
订阅成功回调
保存订阅关系
异步回调
return

2.3 方案实施流程图


用户
浏览器
CP后台
V订阅后台
触发订阅
获取身份标识
浏览器preflight
触发option请求
OPTIONS /getToken HTTP/1.1
Origin: https://api.cp.com
Referer: https://api.cp.com
Access-Control-Request-Method: GET
Access-Control-Request-Headers: X-A,X-B
校验Origin和Referer是否合法
校验
请求域名在白名单里
HTTP/1.1 200 OK
Date: Mon, 01 Dec 2022 01:15:39 GMT
Server: cp-server
Access-Control-Allow-Origin: https://api.cp.com
Access-Control-Allow-Methods: GET, POST, PUT
Access-Control-Allow-Headers: X-A,X-B
请求域名不在白名单
HTTP/1.1 403 forbidden
(no access-control-allow header)
上一步请求合法后getToken
请求合法性和登录态校验
GET /getToken HTTP/1.1
Host: https://cp.com
Origin: https://api.cp.com
Referer: https://api.cp.com
Cookie: cp_user_cookie.xxxxxxx
校验Origin和Referer是否合法
校验用户登录态
请求域名在白名单和用户登录态有效
HTTP/1.1 200 OK
Date: Mon, 01 Dec 2022 01:15:39 GMT
Server: cp-server
Access-Control-Allow-Origin: https://api.cp.com
body{ "token":"xxxxxxxxxxxxxxxxxxxxxxxxxxxx"}
请求非法
HTTP/1.1 403 forbidden
(no access-control-allow header)
获取token
return
return