点融网简介

- 成立于2012年，总部位于上海
- 中国在线市场化借贷中介行业的领导者
- 中国互联网金融协会的常务理事单位之一

通用安全的 token化解决方案

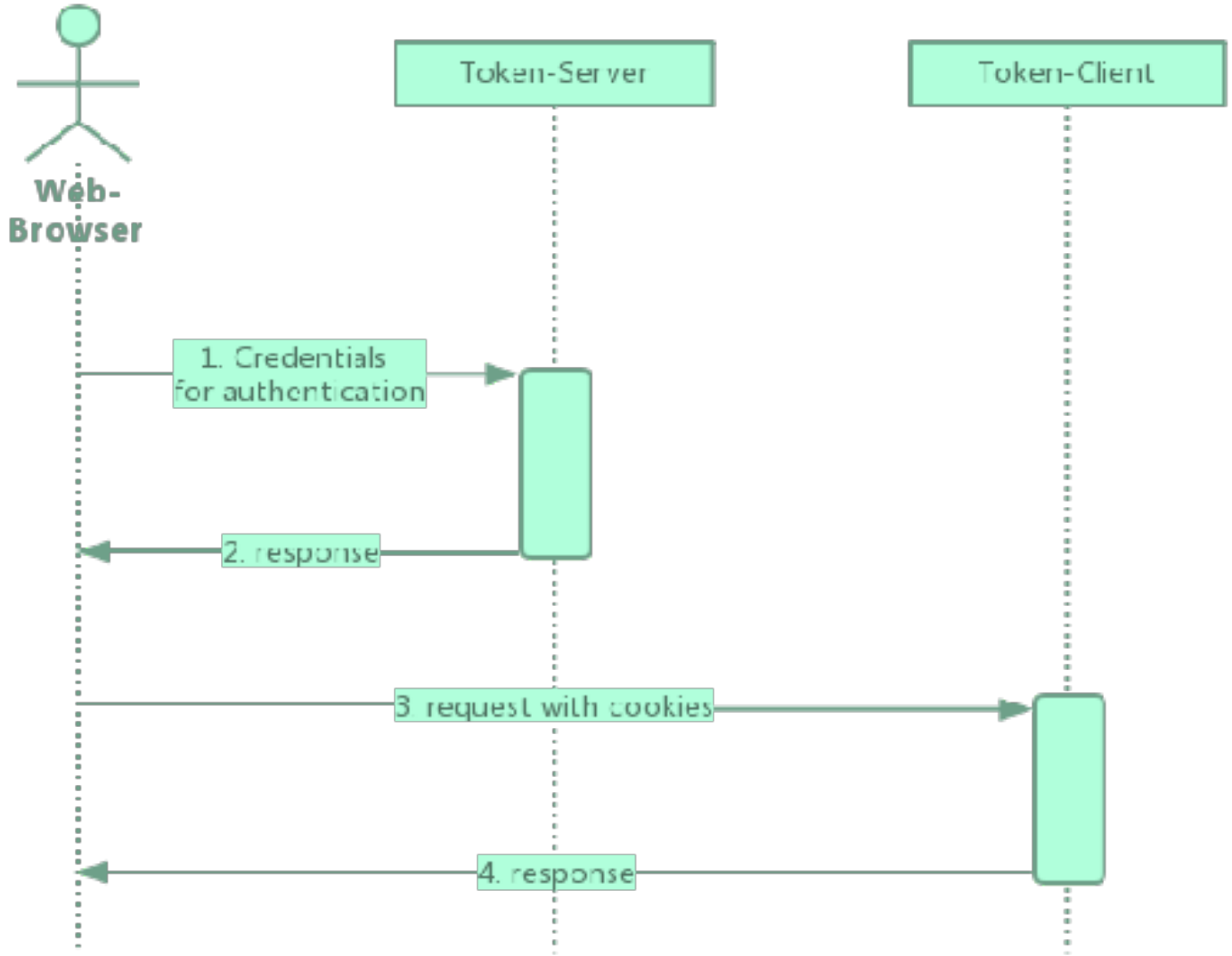
分享一种灵活、可伸缩配置、无状态但又可控的分布式认证方案

present by 点融·钱晟龙

点融 DIANRONG

Token化协议过程

通用安全的token化解决方案



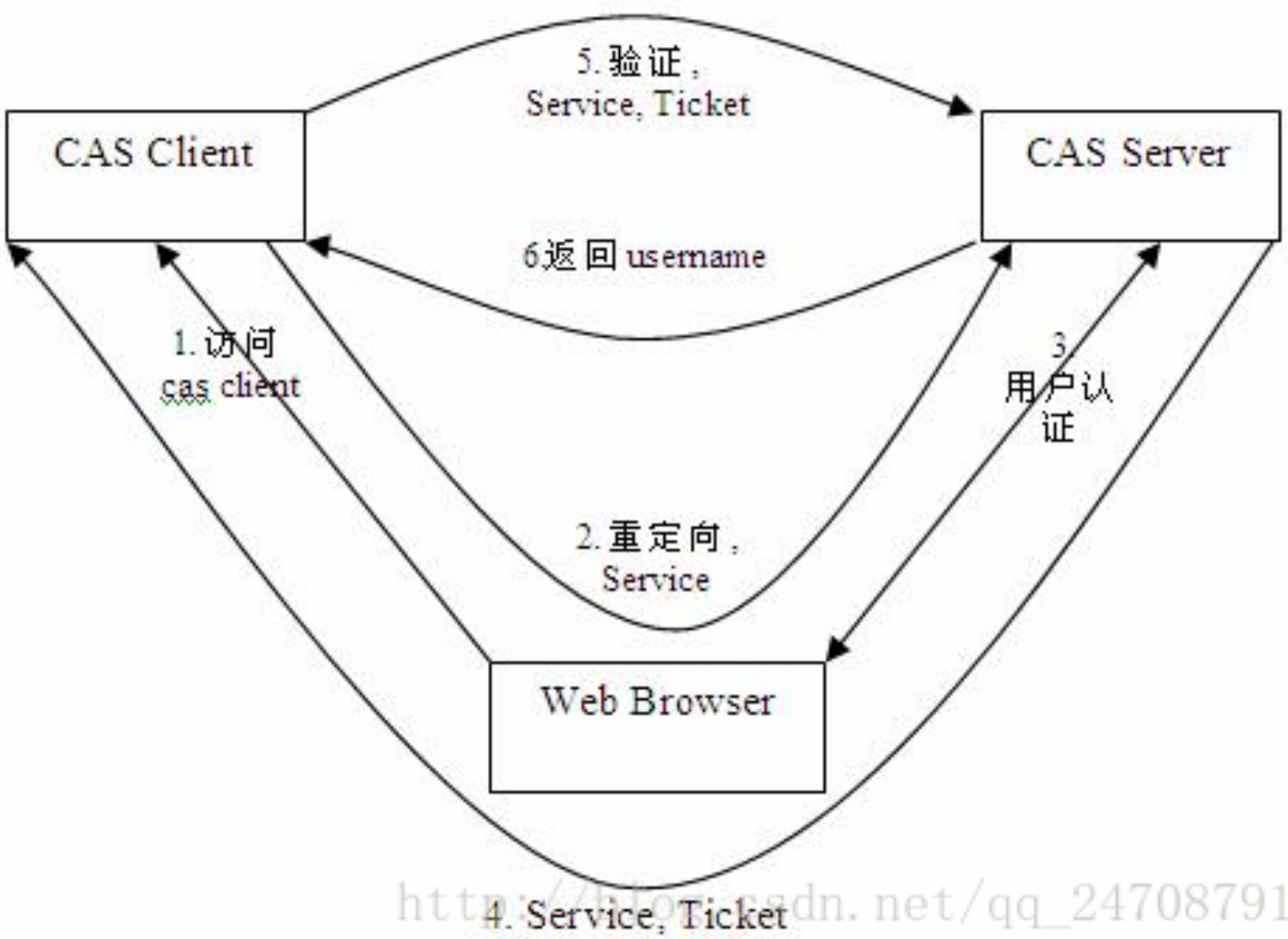
Token化的优势

通用安全的token化解决方案

- 无状态、性能
- 解耦
- 适用于现代Clients
- 方便
- 标准

CAS 的SSO协议过程

通用安全的token化解决方案



Token化的缺点

通用安全的token化解决方案

安全问题

通用安全的token化解决方案

Token or SessionId 放Cookie中, 容易发生的安全漏洞

1. Man-in-the-Middle

2. Cross-Site Scripting (XSS)

3. Cross-Site Request Forgery (CSRF)

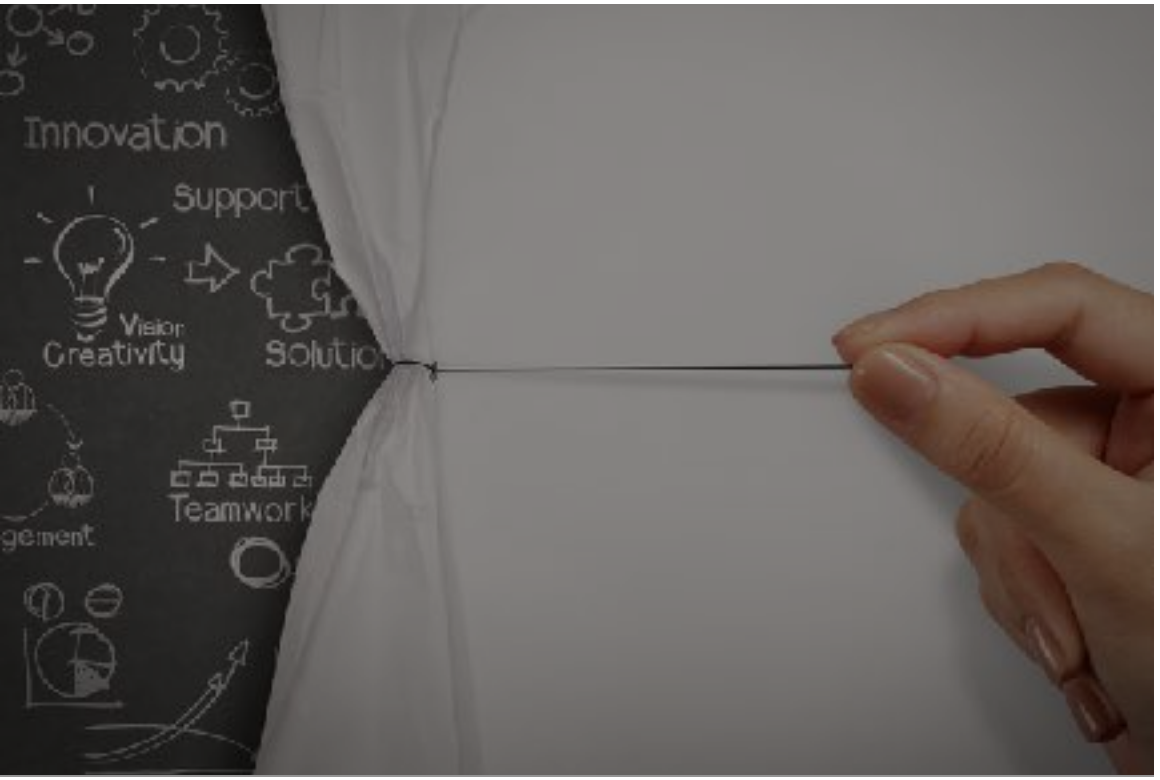
Man-in-the-Middle

通用安全的token化解决方案

- 使用 https 加密信息， 避免中途有人监听窃取cookie.

Cross-Site Scripting (XSS)

通用安全的token化解决方案



- httpOnly
- Server-side, 保证自己依赖的包，和自己的代码不会包含可执行的代码
- Client-side，保证服务器返回的任何内容，都变得不可被执行

Cross-Site Request Forgery（CSRF）

通用安全的token化解决方案

Double-Submit Cookie

浏览器在访问页面的时候给浏览器两个cookie:

1、authentication cookie

2、 一个随机数cookie （cookieName 比如 xsrf-token)

当真的要访问比较敏感的方法时， 需要将2中的value放到header中去， 最后在服务器端判断 cookie中的xsrf-token的值和header中的值 是否是一样的.

安全要点总结

通用安全的token化解决方案

- 使用 Local Storage是不安全的，容易被xss攻击, cookie设置 HttpOnly 前端无感知
- 使用 Secure cookies 来将其存储在浏览器cookie中，cookie机制自动会将token传给服务器，通过https协议传输
- 敏感接口， CSRF保护是必要的.

Renew & Revoke --- part1 concepts

通用安全的token化解决方案

Access token & refresh token 签名tokens

- Access token拥有比较短的生存时间， 可以被认作为一个无状态的可信任的字符串
- Refresh token拥有比较长的生存时间，是用来换取access token的。refresh token应该可以被撤销(Database + cache)

Renew & Revoke --- part2 Examples

通用安全的token化解决方案

- **银行敏感应用**
  - Access token TTL(Time to live) : 5 minutes
  - Refresh token TTL : 30 minutes
- **普通应用**
  - Access token TTL: 30 minutes
  - Refresh token TTL : 2 hours
- **特殊身份不敏感应用(如今日头条、抖音)**
  - Access token TTL = 1 day
  - Refresh token TTL = 2 years (存储在数据库，可缓存，使用它的时候才进行验证)

服务端简单逻辑

通用安全的token化解决方案

access token 是否有效（签名 & 过期验证）

Yes?

允许继续请求

No?

尝试使用refresh token 得到一个新的access token.

拿得到新的access token吗?

Yes?

允许请求，以cookie的方式将该新access token返回给客户端

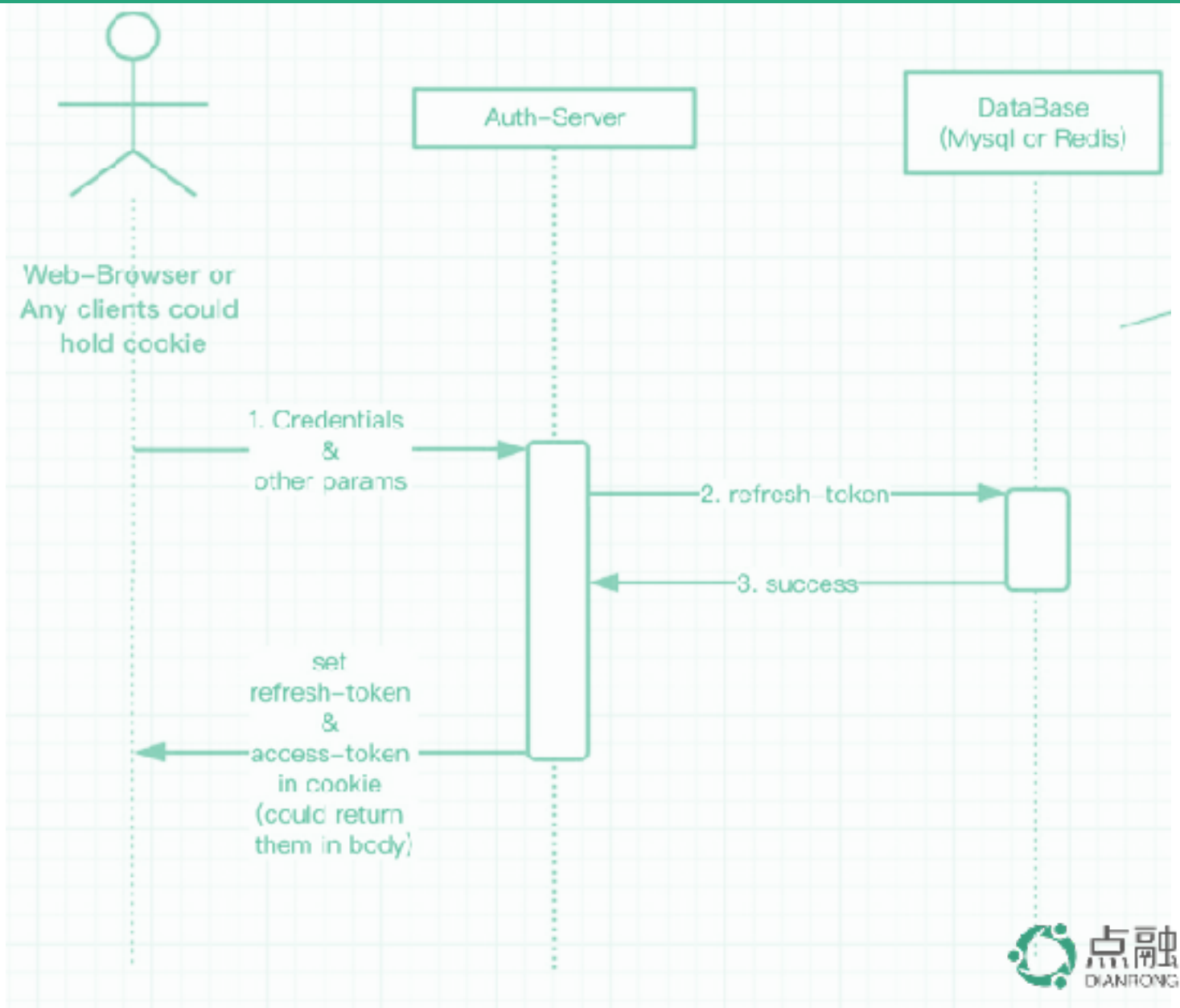
No?

拒绝请求，删除refresh token cookie、删除access token cookie

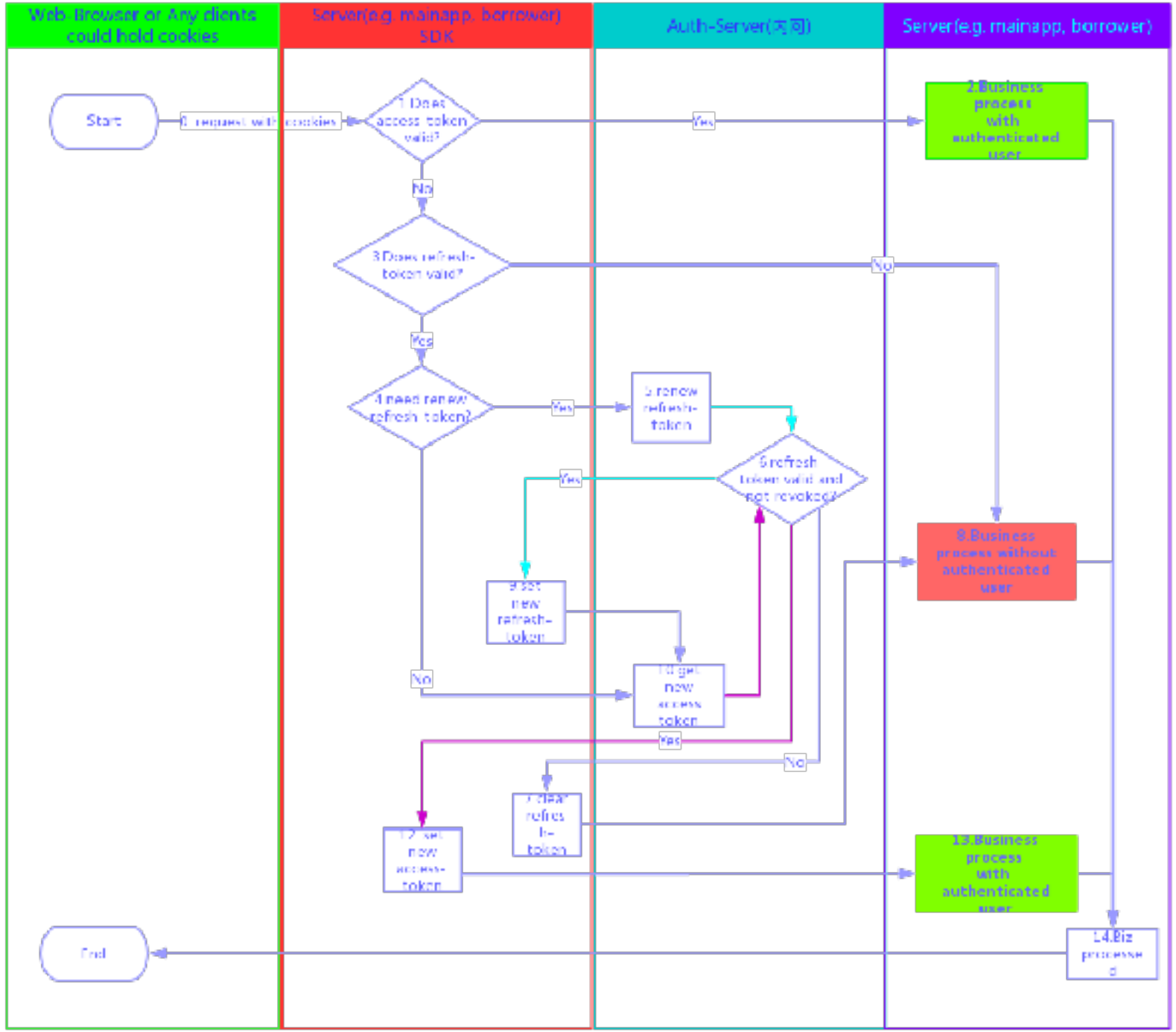
Server-side use case :

通用安全的token化解决方案

Server-side use case :



Client-side 流程图：



其他风险

通用安全的token化解决方案

- 签名密钥泄露
- 密钥被破解

签名 & 验签 算法

通用安全的token化解决方案

RSA or HMAC or 其他？

- 安全
- 性能

要点回顾:

- Token放进cookie, Cookie 应该 setSecure = true , httpOnly, .domain.com
- Token是一个针对 JSESSIONID 方式的改进
- Access Token + Refresh Token的方式 是一个非常好的scaling 策略
- 每一次使用refresh token(如 获取新access token、refresh token) 都需要访问服务器询问其状态

点融网
Dianrong.com

Q & A

Reference Links :

MAFIA
DIANRONG TECHNOLOGY
用技术创新改变传统金融

- 《流程图地址》
- 《滴滴passport经验》
- 《讲真别再用JWT了！》
- 《OWASP》

关注点融黑帮公众号，回复：点融 两个字可获得这些Links

- 《Building Secure User interfaces With JWTs(JSON Web Tokens) 》

Thanks!