链滴

跨域 Cookie 实现单点登录

作者：88250

原文链接：https://ld246.com/article/1407146861362

来源网站：链滴

<h3>单点登录</h3>
单点登录（SSO - Single Sign On）：对于同一个客户端（例如 Chrome 浏览器），只要登录一个子站（例如 a.com），则所有子站（b.com、c.com）都认为已经登录。
比如用户在登录淘宝后，跳转到天猫时就已经登录了。
<h3>用例步骤</h3>

未登录用户访问子站 a.com 进行登录，自动跳转到账户中心的统一登录页 <code>account.com/login</code>
用户在统一登录页进行登录，登录成功后显示登录跳转页
显示登录跳转页后自动跳转回 a.com，单点登录完成
用户在访问 b.com 时无需再次登录

<h3>实现原理</h3>
<h4>登录</h4>

统一登录页登录请求完成后响应为登录跳转页
登录跳转页中通知各子站进行登录
<pre class="prettyprint"><script src='b.com/login?uid=xxxx&token=xxxxx'></script>
<script src='c.com/login?uid=xxxx&token=xxxxx'></script></pre>

子站收到登录请求后验证 token 是否有效，有效的话在响应中设置 cookie（<code>user_toke=xxxx</code>）

<h4>token 验证</h4>

账户中心使用私钥加密 user id，生成 token
子站使用公钥解密 token，将得到的 user id 和参数 uid 对比，如果一样就是校验通过

<h4>登出</h4>

用户在某个子站主动登出时跳转到账户中心统一登出页 <code>account.com/logout?uid=xxxx&token=xxxx</code>
账户中心验证 token 后进行登出，在登出跳转页中通知各子站进行登出（设置 cookie），类似登录通知
子站收到登出请求后验证 token 是否有效，有效的话在响应中设置 cookie（删除 user_token）

<h3>关键点</h3>

浏览器渲染登录跳转页时将执行上面用 <code><script></code> 发送的登录通知请求，执行完后（或者超时）才跳转回前面登录的子站
登录通知请求是跨域的（当前域是账户中心 account.com），所以在响应中设置 cookie 时 IE 些版本需要设置 P3P 头
在验证 token 时可以考虑使用账户中心提供高性能的验证接口，子站进行调用
