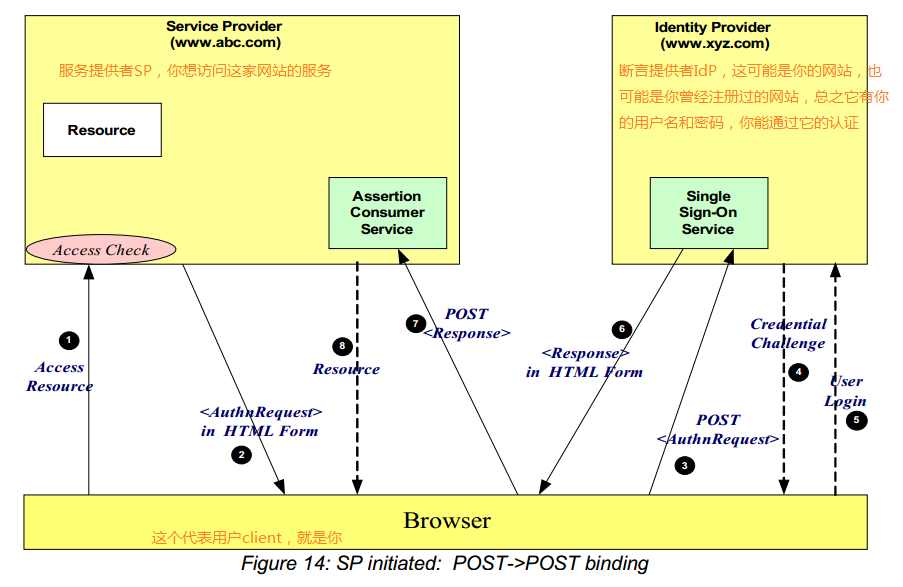
任务:<http://jira.tianhong.cn/browse/SAAS-441>

Demo: https://github.com/OpenConext/Mujina

1 认证流程图(之一)

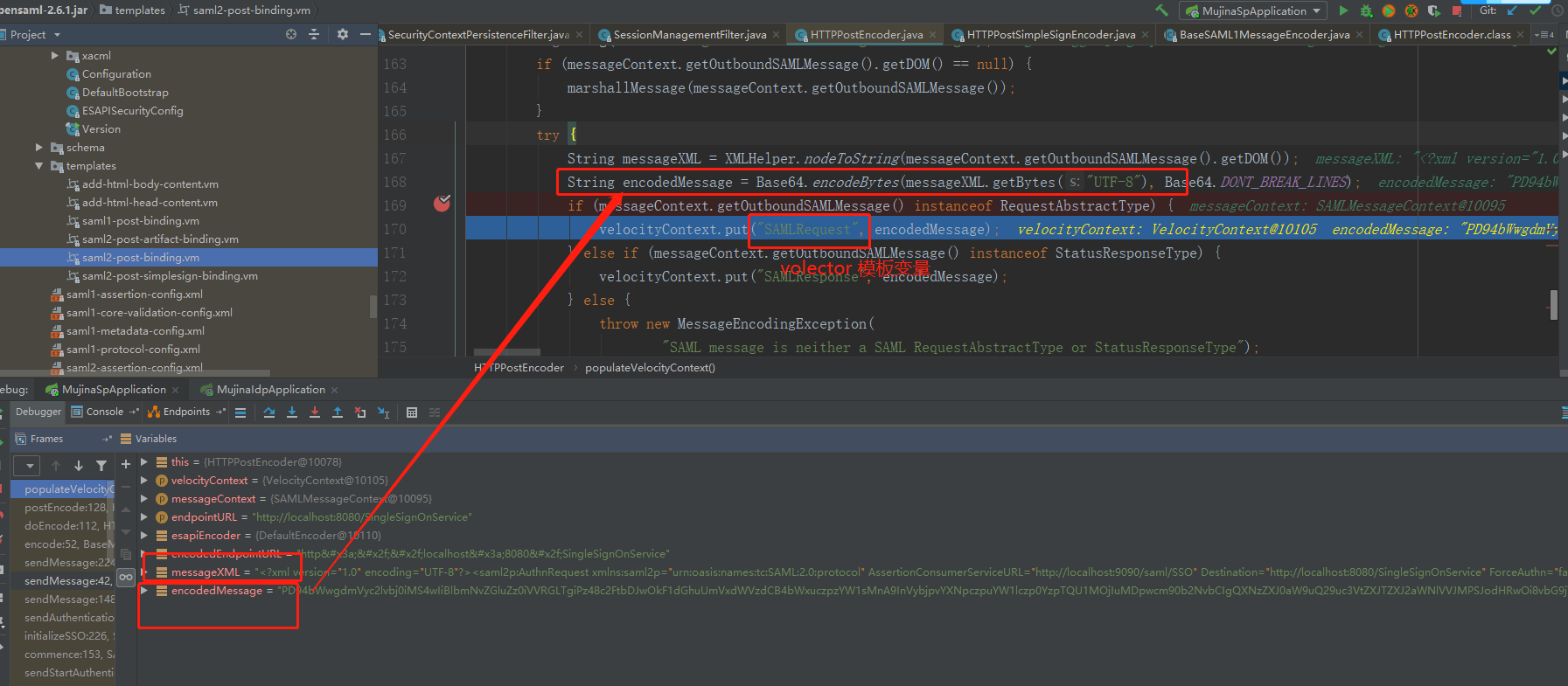


2.认证实现步骤

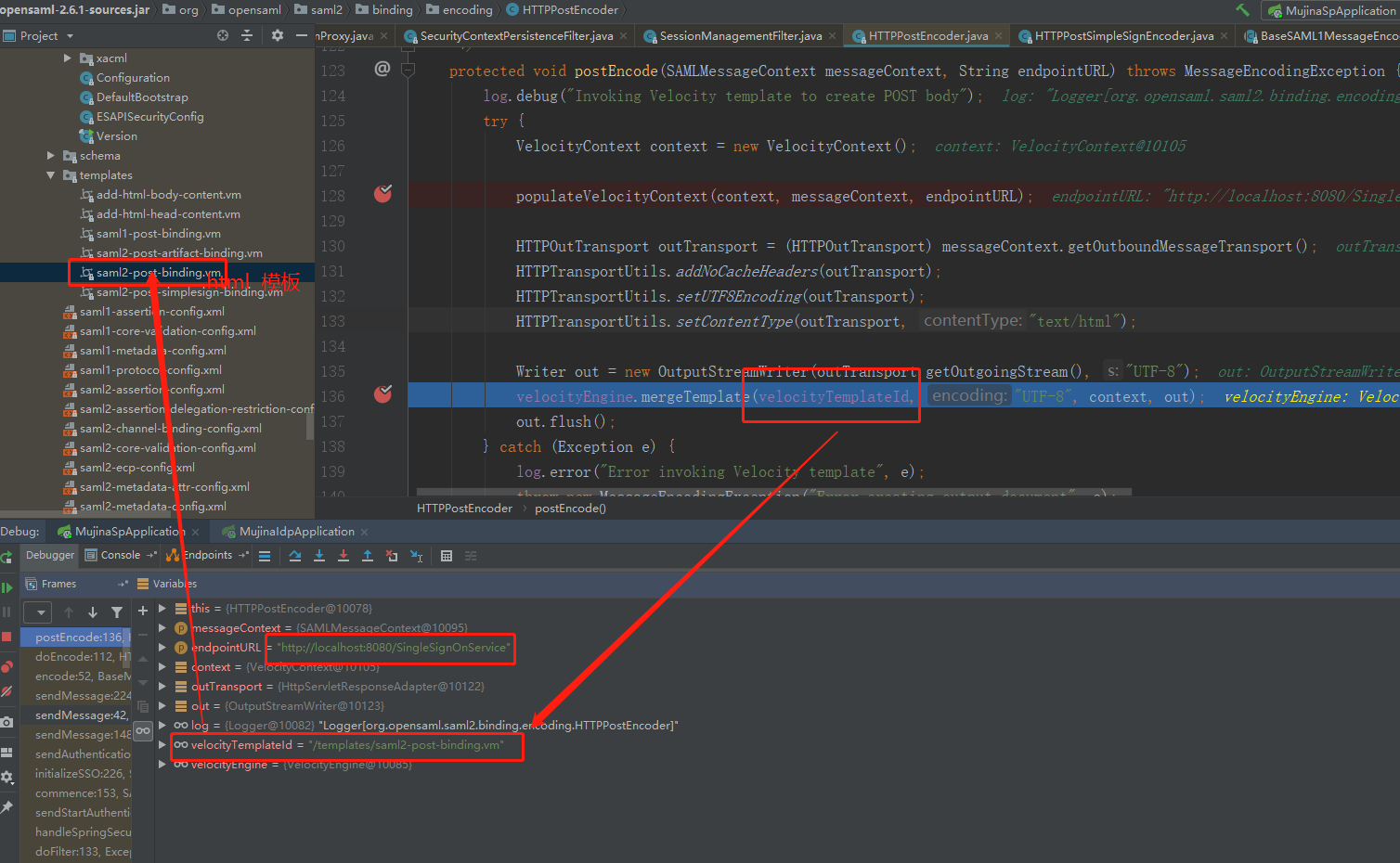
2.1.client向sp申请资源

<http://localhost:9090/sss>

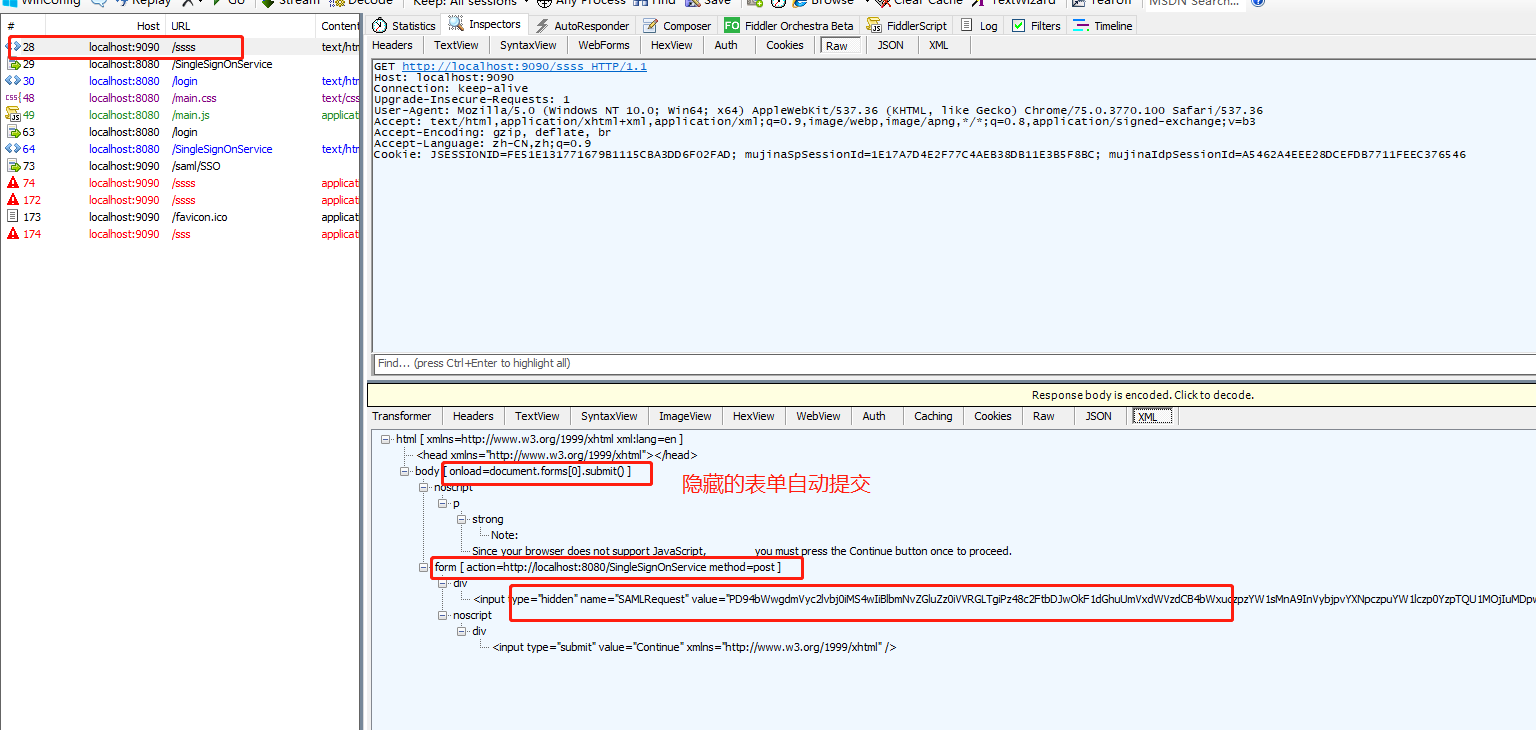
sp检测到client没有证证，生成authRequet后，并通过Volector 模板生成html输出给client(AuthRequest 通加是加签名后，再base64 encode 输出到前台)



生成html

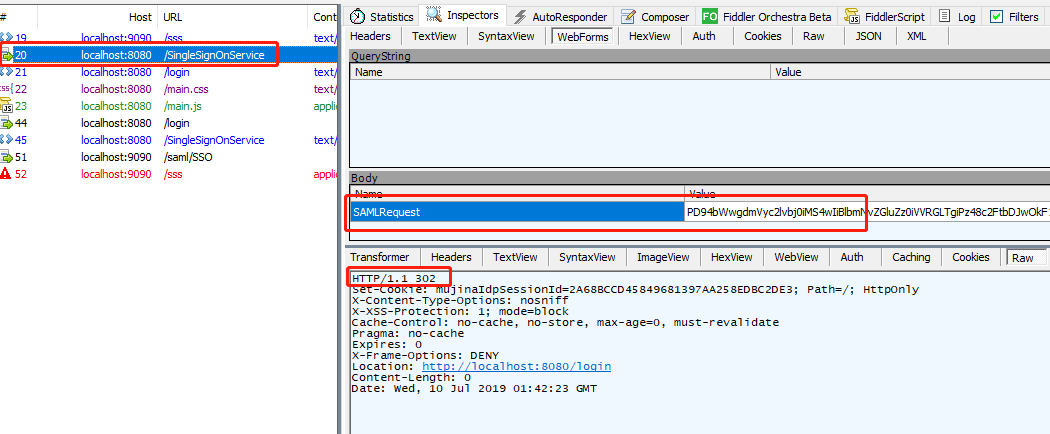


client收到的信息

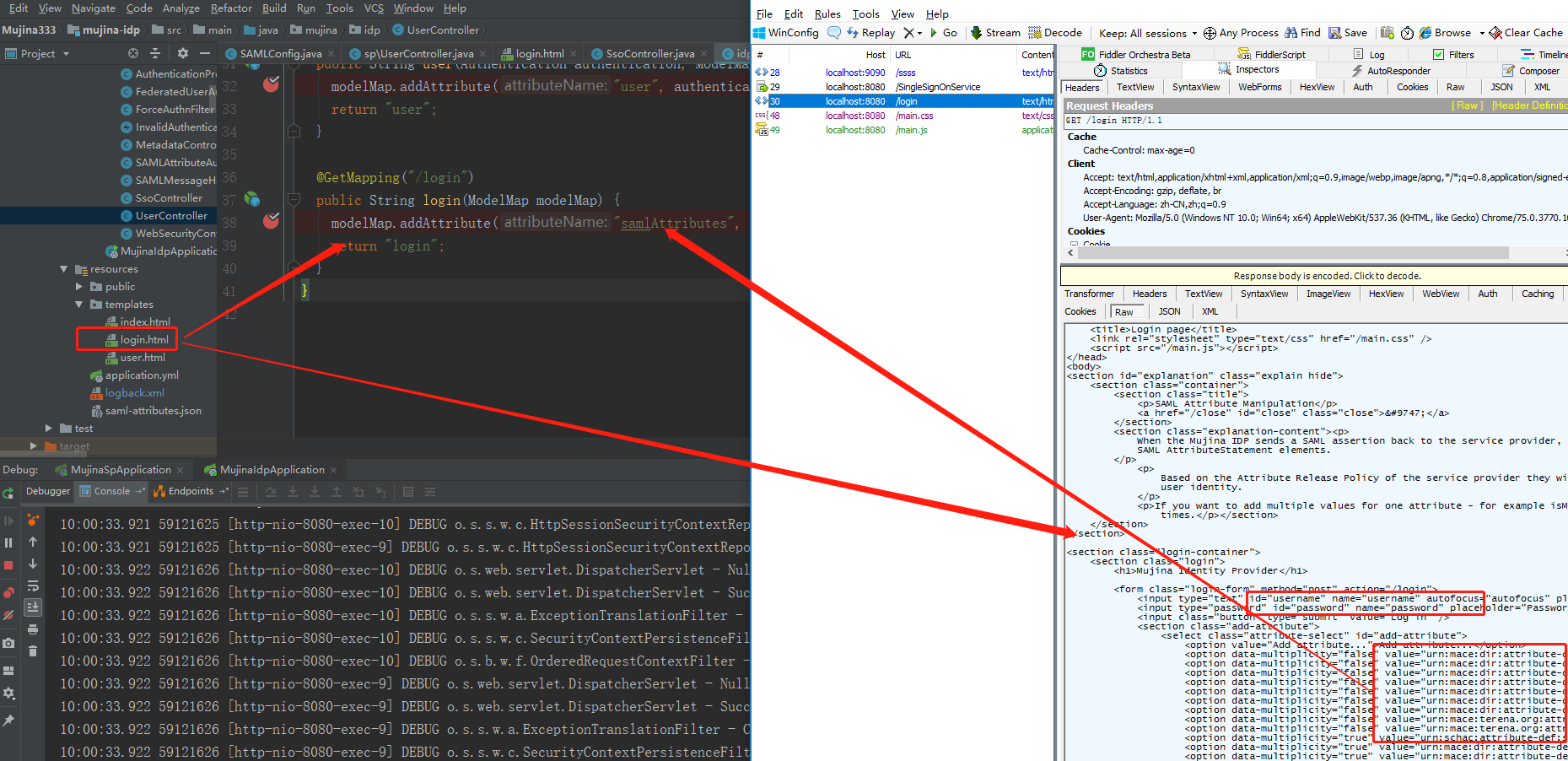
2.2.client向idp发送授权申请

1.收到sp的authRequet,信息后，自动把信息提交的idp

2.idp 收到authRequest,通知client重定向到填写申请表单页面

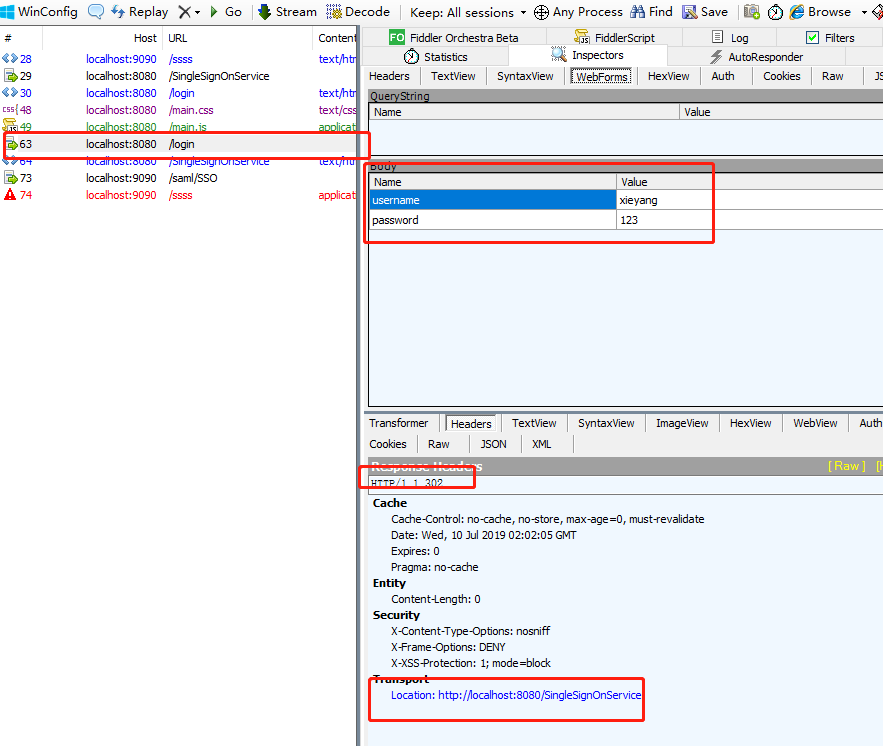


2.3 client重定向到idp授权申请页面



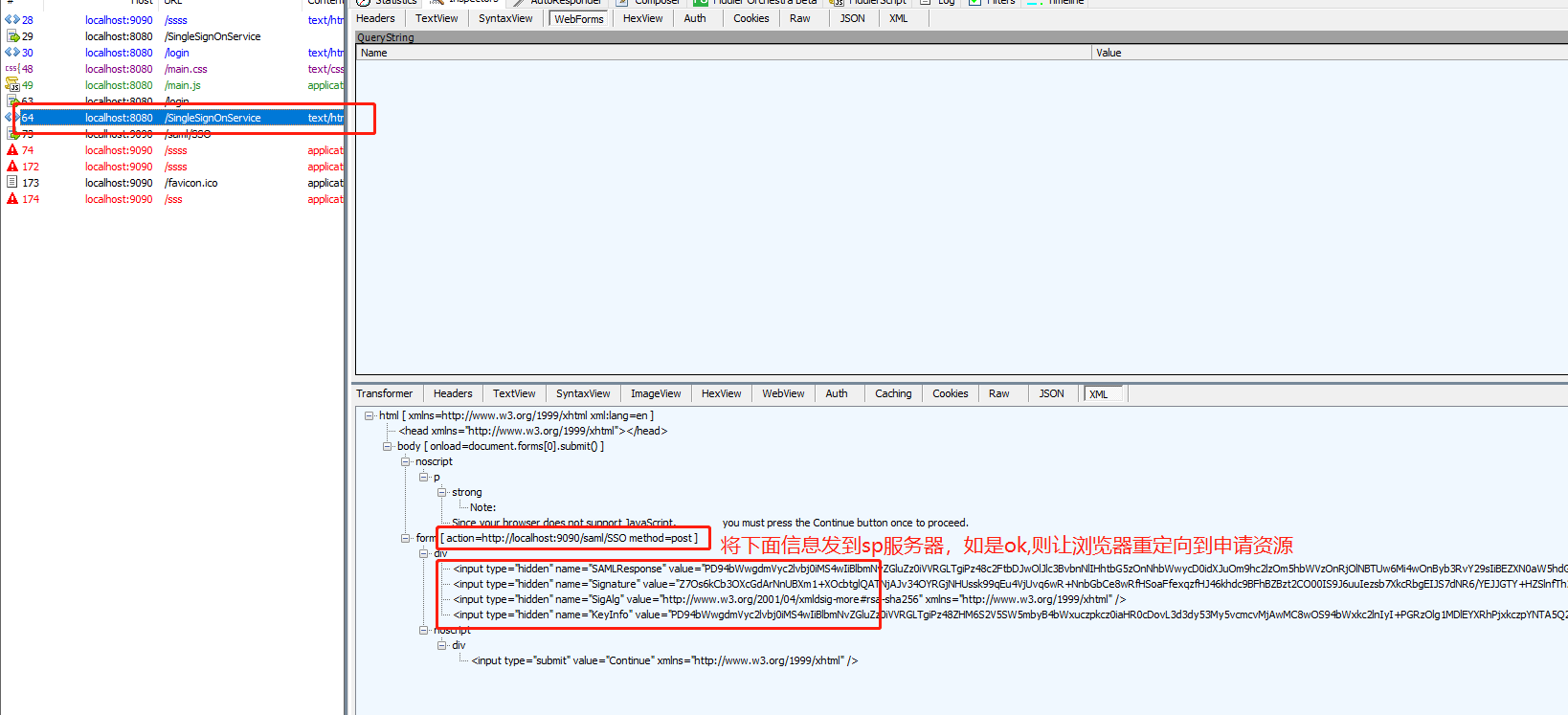
2.4 client 向idp发送授权申请信息

用户把帐号，密码提交到idp,如果认证通过后，通知client重定向到idp 的/SingleSignOnService



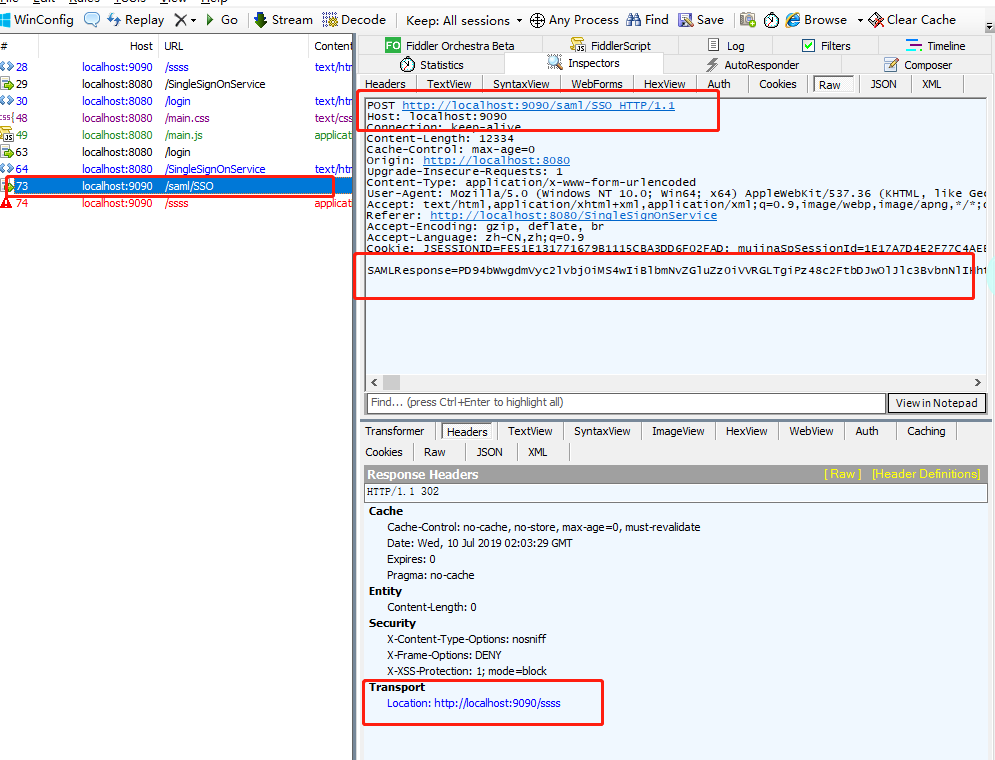
2.5 client重定向到idp /SingleSignOnService获取授权信息

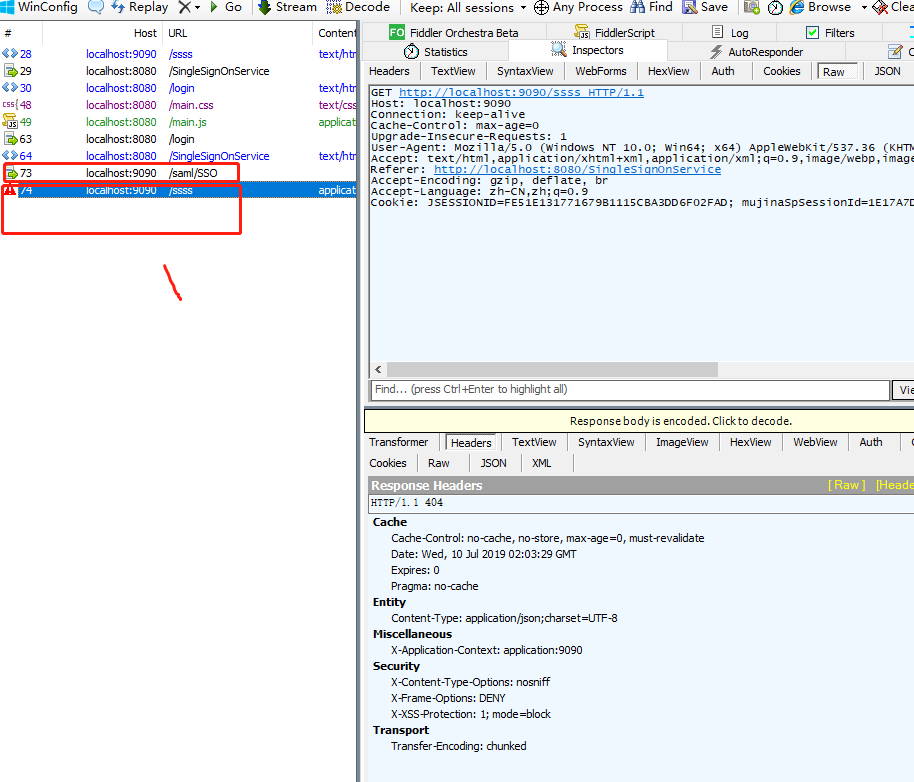
Client获取到授权信息后，以隐藏表单的形式，提交到sp的/saml/SSO



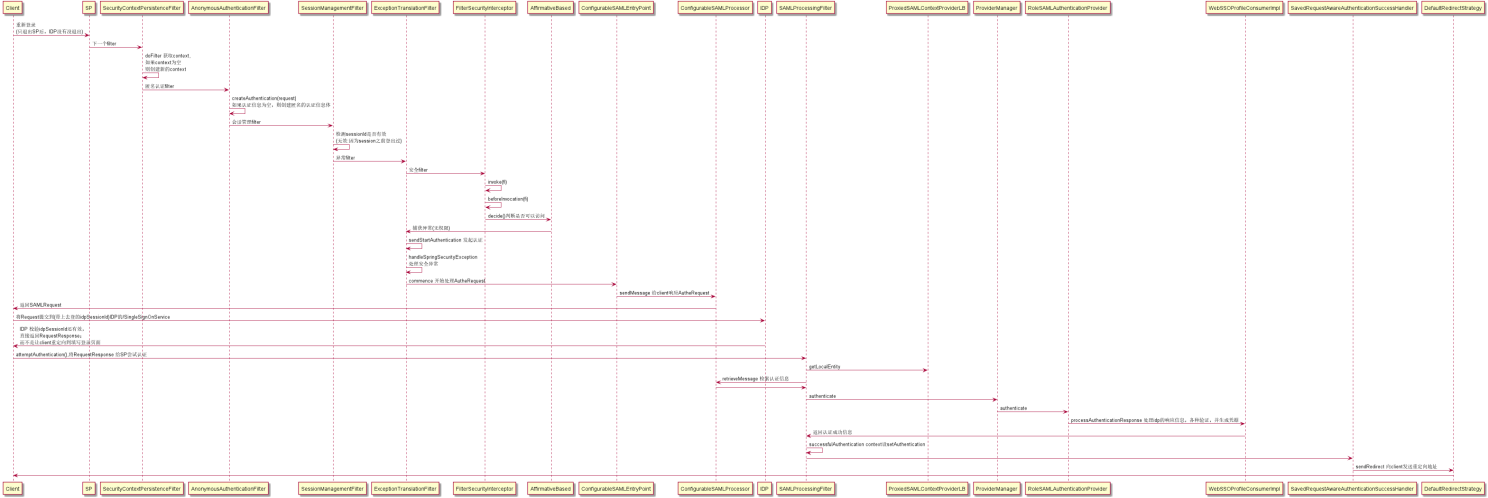
2.6 Client 把授权信息发给sp

sp收到client发过来的消息进行校验，如成功则让client重定向到资源页面

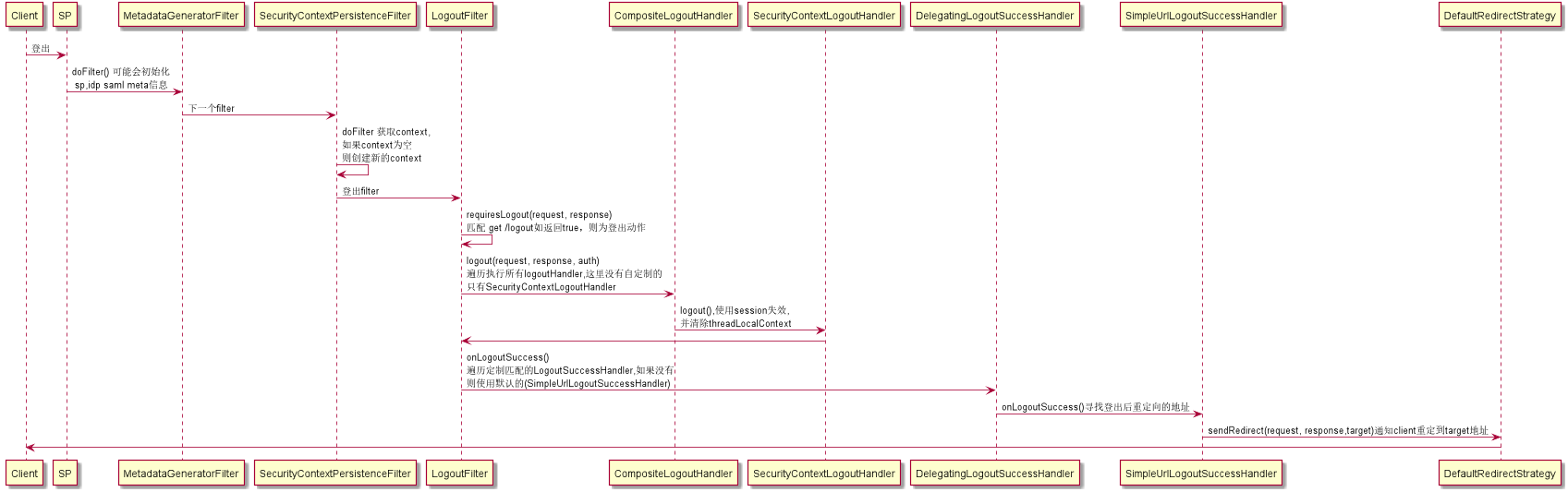
2.7 sp 收到授权信息后，请cleint重定向的资源页面



1. 只退出SP，重新登录流程

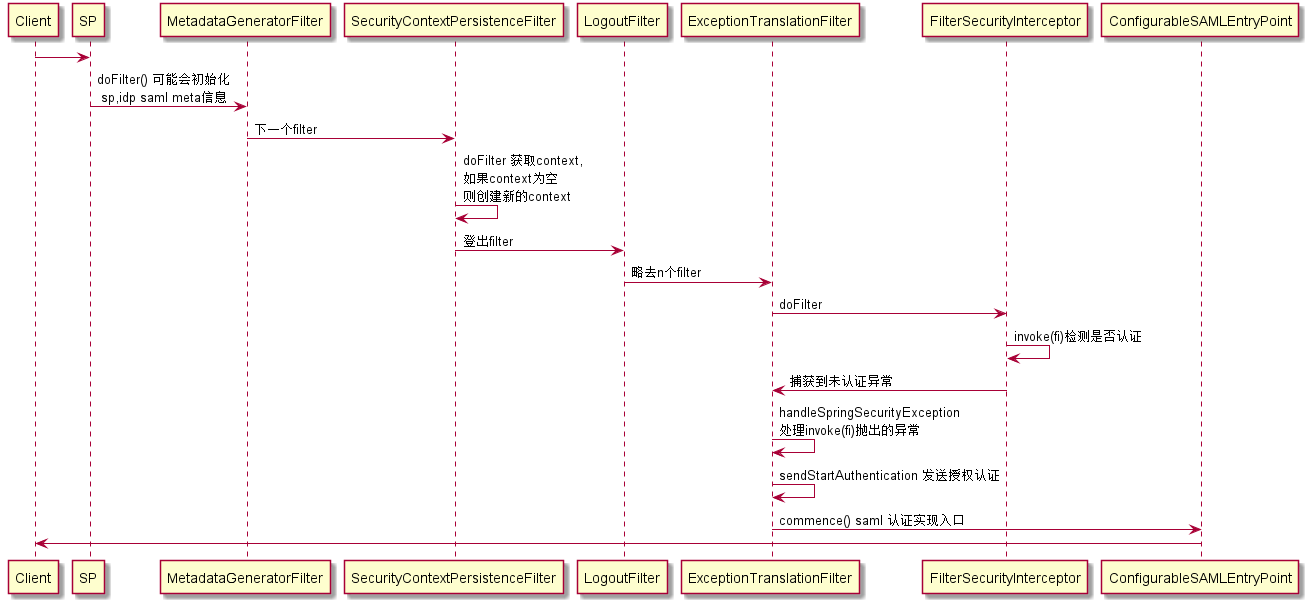


4.只退出SP，流程

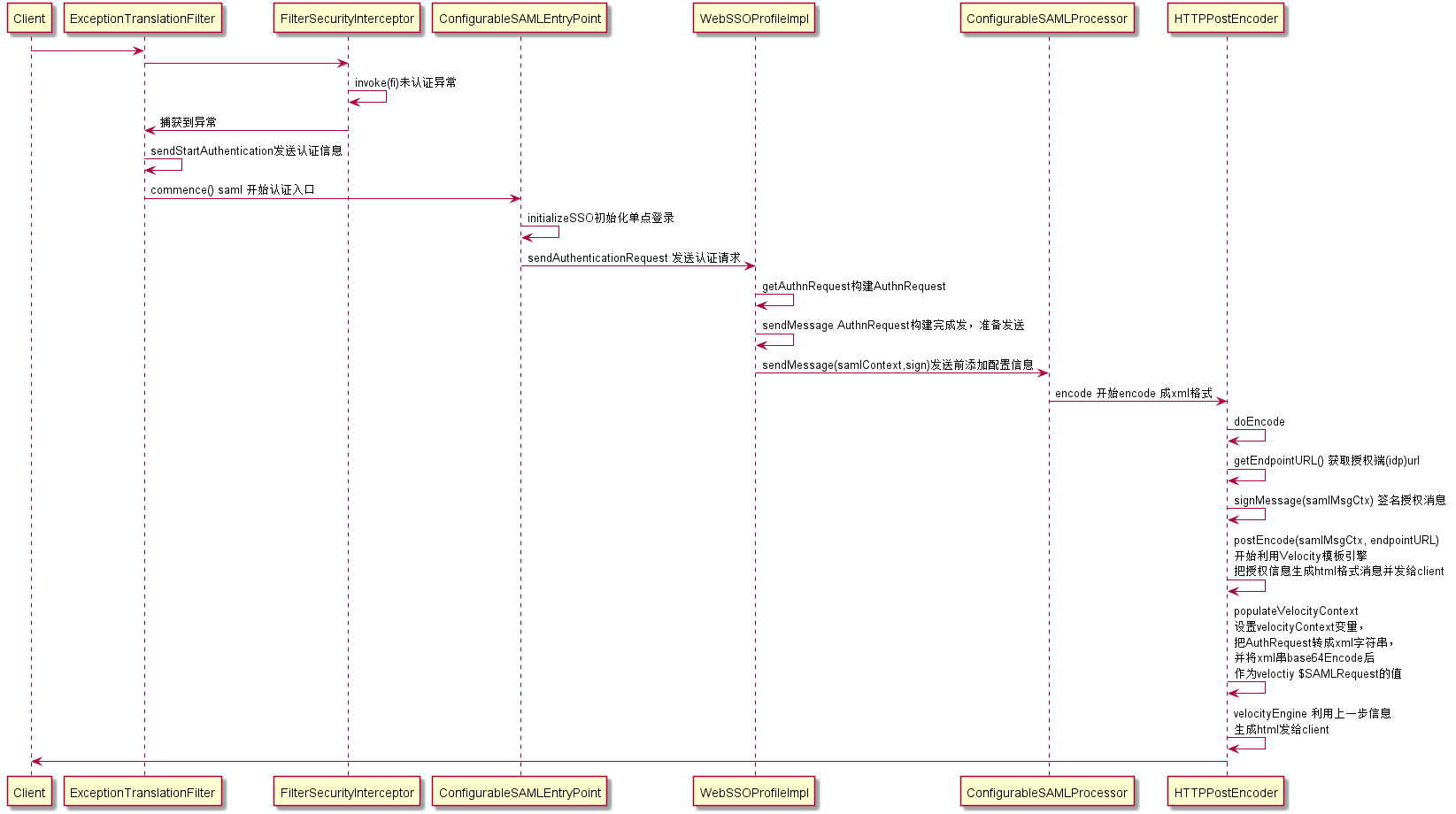


5.Spring-security-saml实现

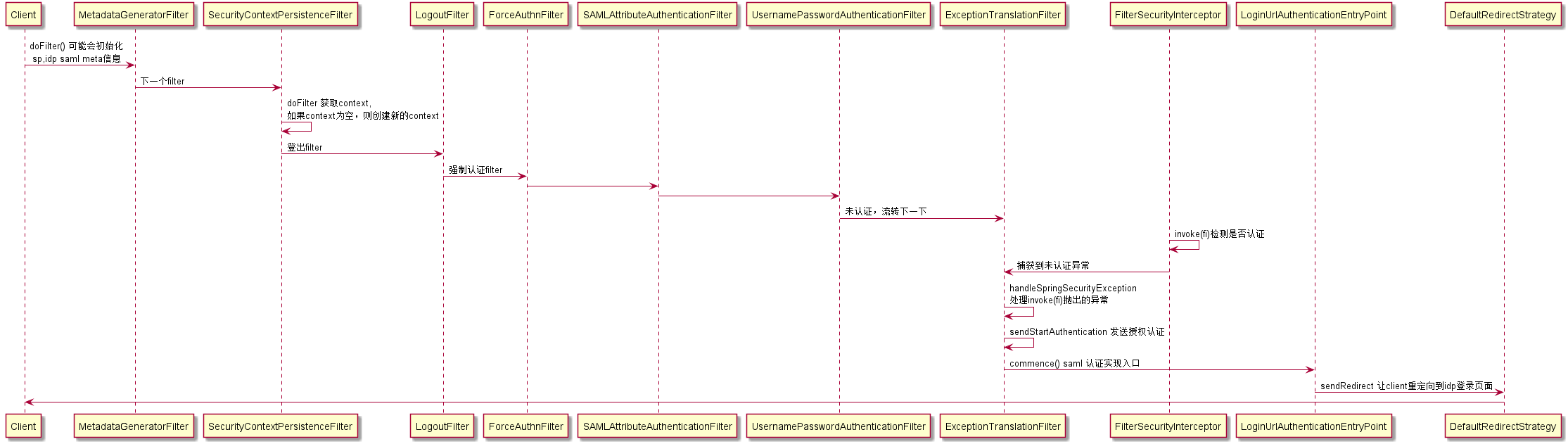
SP-Filter链路



SP生成认证请求链路



IPD-Filter链路



1. 定制化实现

6.1 IDP端

6.1.1 自定认证器AuthenticationProvider

6.2 SP端

6.2.1 自定认证器SAMLAuthenticationProvider

6.3共同