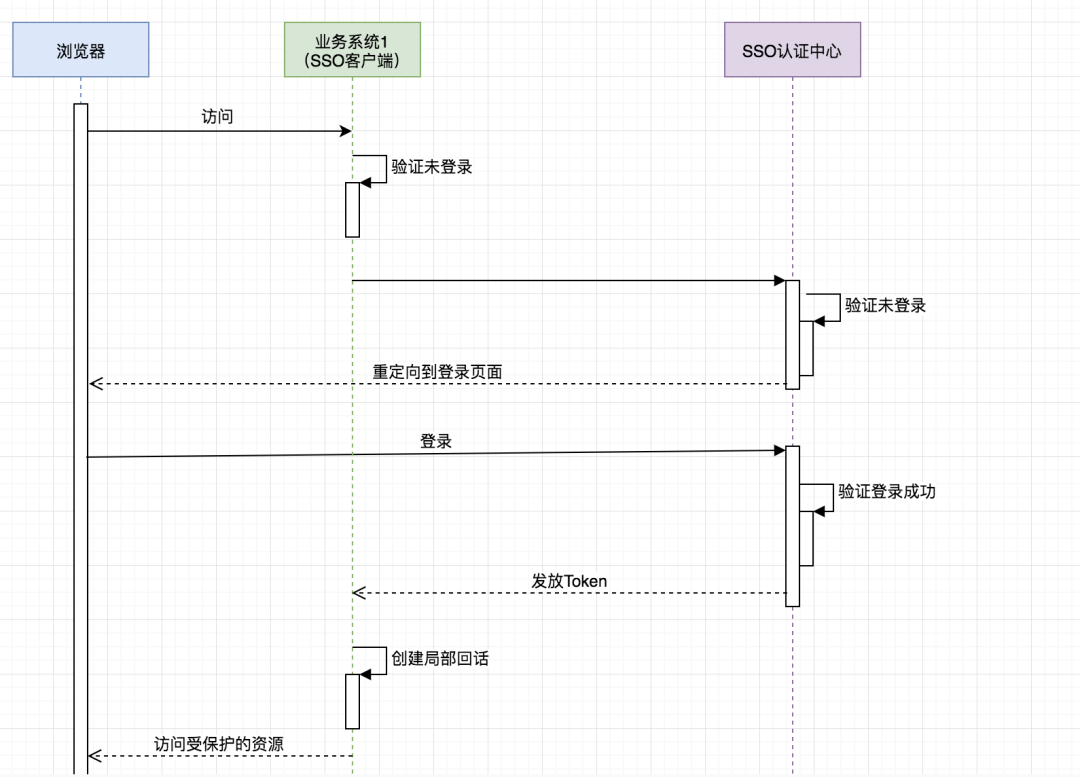


重要的是理解：

* SSO服务端和SSO客户端直接是通过授权以后发放Token的形式来访问受保护的资源
* 相对于浏览器来说，业务系统是服务端，相对于SSO服务端来说，业务系统是客户端
* 浏览器和业务系统之间通过会话正常访问
* 不是每次浏览器请求都要去SSO服务端去验证，只要浏览器和它所访问的服务端的会话有效它就可以正常访问



在OAuth2在有授权服务器、资源服务器、客户端这样几个角色，当我们用它来实现SSO的时候是不需要资源服务器这个角色的，有授权服务器和客户端就够了。

授权服务器当然是用来做认证的，客户端就是各个应用系统，我们只需要登录成功后拿到用户信息以及用户所拥有的权限即可

**3.1. Spring Security 、OAuth2、JWT、SSO**

，OAuth2是用来允许用户授权第三方应用访问他在另一个服务器上的资源的一种协议，它不是用来做单点登录的，但我们可以利用它来实现单点登录。在本例实现SSO的过程中，受保护的资源就是用户的信息（包括，用户的基本信息，以及用户所具有的权限），而我们想要访问这这一资源就需要用户登录并授权，OAuth2服务端负责令牌的发放等操作，这令牌的生成我们采用JWT，也就是说JWT是用来承载用户的Access\_Token的

最后，Spring Security是用于安全访问的，这里我们我们用来做访问权限控制