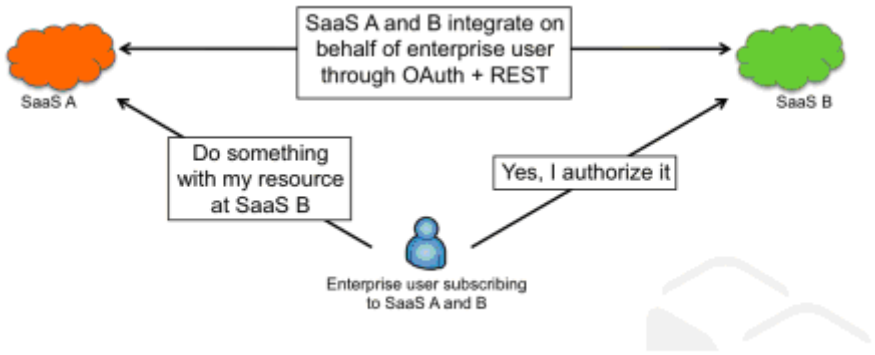
# 1.1 OAuth and OpenClinica

Use of the REST API is dependent on authentication via the OAuth protocol (version 2). OAuth is a security protocol that enables users to grant third-party access to their web resources without sharing their passwords. See http://oauth.net/2/ and http://hueniverse.com/2010/05/introducing-oauth-2-0/ for more information on OAuth 2.0.




(Source: http://cloud.dzone.com/news/enterprise-saas-integration)

The communication/authentication steps between the OAuth client and server are described below.

(D) = Designer - OAuth Client

(OC) = Authorized OpenClinica Instance OAuth service provider

1. (D) /access.....

2. (D) hits restTemplate call to OC

3. (D) throws exception - No OAuth 2 security context has been established.

Unable to access resource 'ocInstance'.

4. (D) As part of exception bubbling up OAuth2ClientContextFilter line 77 triggered results in

response.sendRedirect ::

http://localhost:8080/OpenClinica-web-SNAPSHOT/oauth/user/authorize?client_id=designer&redirec

t_uri=http%3A%2F%2Flocalhost%3A8080%2FDesigner-0.1.0.BUILD-SNAPSHOT%2Faccess%3Fhost%3Dhttp%3A%2F%2Flocalhost%3A8080%26app%3DOpenClinica-web-SNAPSHOT%26study_oid%3DS_DEFAULTS1%26provider_user%3Droot&response_type=code

5. (OC) redirect hits OC

6. (OC) initiates http://localhost:8080/OpenClinica-web-SNAPSHOT/oauth/confirm_access

7. (OC) the above url initiates a maybe just a normal request or REST call back to (D)

8. (D) in OAuth2ClientContextFilter the request URL looks like http://localhost:8080/Designer-0.1.0.BUILD-SNAPSHOT/access?host=http://localhost:8080&app=OpenClinica-web-SNAPSHOT&study_oid=S_DEFAULTS1&provider_user=root&code=2zLl3b

9. (D) hits /access .. controller code again

10. (D) hits restTemplate call to OC

11. (D) throws

org.springframework.security.oauth2.consumer.OAuth2AccessTokenRequiredException:

No OAuth 2 security context has been established. Unable to access resource 'ocInstance'.

12. (D) As part of exception bubbling up OAuth2ClientContextFilter line 77 triggered results in

13. (D) line 83 in OAuth2ClientContextFilter will trigger REST Call to

http://localhost:8080/OpenClinica-web-SNAPSHOT/oauth/authorize

14. (D) response from above call produces an accessToken

15. (D) returns back to  /access ... controller code execution

16. (D) hits restTemplate call to OC

17. (D) call succeeds

Every time /access..... is invoked, Designer will receive the request and ask OpenClinica.com to check if the URL is an authorized instance (ie, an Enterprise instance or a Community instance that has registered here). If that check fails the user will be automatically directed to an error page. The above check will be continuously performed through out the OAuth handshake to check the validity of the URL.

Approved for publication by Cal Collins. Signed on 2014-08-06 9:47AM

Not valid unless obtained from the OpenClinica document management system on the day of use.