Exemple Réel d'un DSQ montrant l'utilisation de son login FB pour accéder à une application web

http://www.u(vuml-diagrams.org/facebook-authentication-uml-sequence-diagram-example.html

(vu oct 2017)

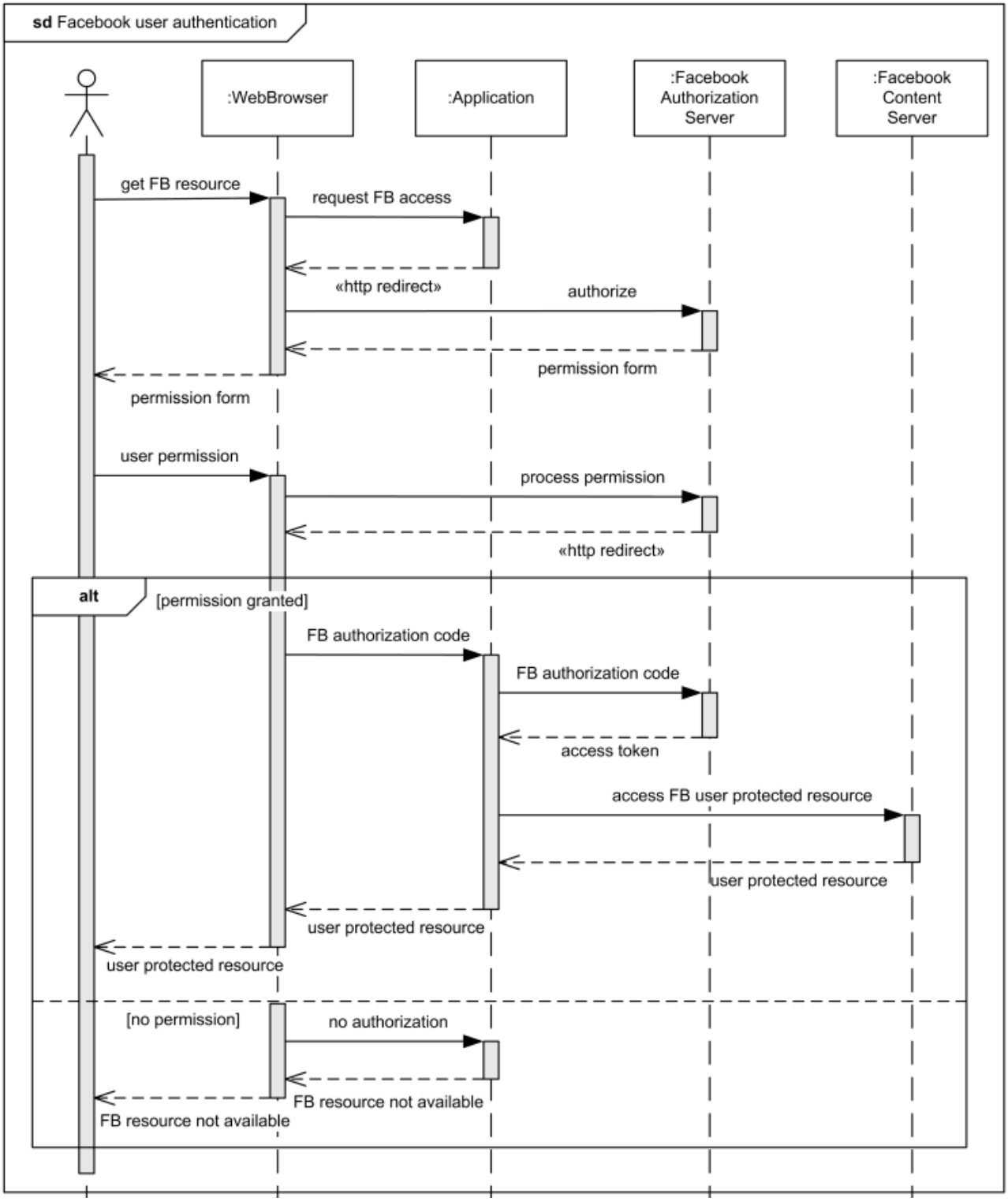
Voici un exemple de **diagramme de séquence UML** qui montre comment un utilisateur de Facebook (FB) peut être authentifié dans une application Web via son compte FB, ce qui va permettre l'accès à ses ressources FB. Facebook utilise le protocole OAuth 2.0 qui permet aux applications Web (appelées « client ») qui ne sont généralement pas propriétaires de la ressource FB, d'agir au nom de l'utilisateur FB pour demander l'accès aux ressources contrôlées et hébergées par le serveur FB. Au lieu d'utiliser les informations d'identification de l'utilisateur FB pour accéder aux ressources protégées, l'application Web obtient un *jeton d'accès* (access token).

L'application Web doit être enregistrée par Facebook pour avoir un ID d'application (client_id) et un code secret (client_secret). Lorsqu'une requête est envoyée à certaines ressources Facebook protégées, le navigateur Web (« agent utilisateur ») est redirigé vers le serveur d'autorisation de Facebook avec l'ID d'application, et l'URL vers laquelle l'utilisateur doit être redirigé après le processus d'autorisation.

L'utilisateur reçoit alors le formulaire de Demande d'Autorisation. Si l'utilisateur autorise l'application à récupérer ses données, le serveur d'autorisation Facebook redirige alors vers l'URI précédemment spécifiée avec le code d'autorisation (« chaîne de vérification »). Le code d'autorisation peut ainsi être échangé par l'application Web pour un jeton d'accès OAuth.

Si l'application Web obtient le jeton d'accès pour un utilisateur FB, elle peut effectuer des requêtes autorisées pour le compte de cet utilisateur en incluant le jeton d'accès dans les requêtes API Facebook Graph.

Si l'utilisateur n'a pas autorisé l'application Web, Facebook émet une demande de redirection vers l'URI spécifiée précédemment, et ajoute le paramètre *error_reason* pour informer l'application Web que la demande d'autorisation a été refusée.


sd Facebook user authentication
:WebBrowser
:Application
:Facebook Authorization Server
:Facebook Content Server
get FB resource
request FB access
«http redirect»
authorize
permission form
permission form
user permission
process permission
«http redirect»
alt
[permission granted]
FB authorization code
FB authorization code
access token
access FB user protected resource
user protected resource
user protected resource
user protected resource
[no permission]
no authorization
FB resource not available
FB resource not available