AAI - Authentication and Authorization Infrastructure

Authentication - finding out who the user is

Authorization - finding out what is a user allowed to do and what not

## 

## Weblicht

* <https://weblicht.sfs.uni-tuebingen.de/weblicht/>
* authentication via federated login (Shibboleth SAML2).
  + authentication to user interface only
* authentication = authorization
  + every authenticated user has permissions to do everything
* all Weblicht services are publicly available (if we knew the URL and have API documentation e.g., from Download Chain xml we could theoretically use it without Weblicht)
  + there are no authentication/authorization checks in the background
* Weblicht Waas
  + <https://weblicht.sfs.uni-tuebingen.de/WaaS/>
  + API key (secret token) generation after authentication, validity for 3 months (https://weblicht.sfs.uni-tuebingen.de/WaaS/api/1.0/chain/process)
  + <https://weblicht.sfs.uni-tuebingen.de/WaaS/api/1.0/chain/process>
    - api key verification
* REVISED by

## LAPPS/Galaxy

* <http://galaxy.lappsgrid.org/>
* Vassar and Brandeis LAPPS servers
  + [http://vassar.lappsgrid.org/language-services](http://grid.anc.org:8080/service_manager/language-services)
    - All services will be moving to https:// in the near future
  + <http://eldrad.cs-i.brandeis.edu:8080/service_manager/language-services>
* local user accounts
* Web API ~~based on a generated key (secret token)~~ Three ways to access:
  + Access service URL directly. No authorization required.
  + Access through the service manager. Username/password required.
  + Web API through Galaxy. API token issued by Galaxy UI.
* authentication != authorization
  + authorization to e.g., LDC via OAuth key (must be validated and copy&paste manually), valid for six hours
* REVISED by Keith Suderman

## 