EDIT Community Single Sign-On

Why Community Single Sign-On?
- The EDIT platform provides a multitude of web-based taxonomic applications and services.
- The diversity of service providers reflects the highly distributed, cross-national organisational infrastructure of biodiversity institutions and collections in general.
- Result is a problem of identity management
  - system administrators must register users and maintain several access control lists for each individual service.
  - users must remember a number of login/password combinations to access these different services
- Need for a comfortable single sign-on (SSO) solution
  - reflecting the specifics of biodiversity infrastructures

Community Single Sign-On (CSSO) features
- Uses the Security Assertion Markup Language (SAML) web profile (e.g. Shibboleth, OpenSSO, SimpleSAMLphp)
- Only a single identity and password(1) per user
- users may keep their home institution accounts
- Attribute Based Access Control (ABAC) for service providers
- considerably reduced administrative costs
- definition of individual access control policies
- Aim: provide protected access to all EDIT platform components
- Open to all biodiversity institutions or service contributors
- e.g. CATE or LifeWatch already expressed interest
- Vision: Build up a biodiversity community federation
  - trusted interaction without bilateral agreements
  - binds institutions to a common set of policies & practices

EDIT Federation
- Identity Provider (IdP) is responsible for
  - secure user login and attribute delivery to SPs
- Service Provider (SP) provides cross-organisational access
  - to web resources for federated users
  - defines individual access control policies
- EDIT’s first version is in production
  - (1 IdP, 3 SPs)
  - CDM Portals (Drupal), Developer Tools (Trac, Subversion)
  - ExpertsDatabase, ATBI-Sites (Drupal, coming soon)
  - Taxonomic Editor, CATE (Spring, evaluated)

Attribute | Authentication | Description
--- | --- | ---
eduPersonPrincipalName | yes | login id
eduPersonAffiliation | yes | groups/roles
eduPersonTargetedID | yes | unique id
mail | no | email address
givenName | no | given name
postalAddress | no | address
telephoneNumber | no | phone number
sn | no | surname
cn | no | common name

Current list of common attributes of the EDIT federation

How to join?
- Minimal platform requirements:
  - (virtual) web server or hosted web space
  - read access to SSL web server certificate
  - Integrate your web application(s) as Service Provider
  - the most convenient way to start
  - some demo setups available (e.g. Drupal, Trac)
  - Integrate your institution’s users as Identity Provider
  - requires some planning and preparation efforts
  - e.g. user database attribute mapping, security policies setup
  - Contact us for individual installation support
  - any application scenario explicitly welcome(!)

Find more information at http://dev.e-taxonomy.eu/trac/wiki/CSSO or contact Lutz Suhrbier (suhrbier@inf.fu-berlin.de)