


Project no. 018340

**Project acronym: EDIT**

**Project title: Toward the European Distributed Institute of Taxonomy**

Instrument: Network of Excellence

Thematic Priority: Sub-Priority 1.1.6.3: "Global Change and Ecosystems"

# M5.19a CSSO Security Infrastructure fully functional

Due date of component: Month 35
Actual submission date: Month 35

Start date of project: 01/03/2006 Duration: 5 years

Organisation name of lead contractor for this component: 9 FUB-INF

Revision draft

| Project co-funded by the European Commission within the Sixth Framework Programme (2002-2006) | | |
|---|---|---|
| Dissemination Level | | |
| **PU** | Public | **X** |
| **PP** | Restricted to other programme participants (including the Commission Services) | |
| **RE** | Restricted to a group specified by the consortium (including the Commission Services) | |
| **CO** | Confidential, only for members of the consortium (including the Commission Services) | |

# M5.19a CSSO Security Infrastructure fully functional

## Objectives

The general objective of the activity covers the design of a security infrastructure for the platform and the introduction of a secure Single Sign-On service (SSO) for the platform. The task to be achieved within the third JPA concerns the integration of a Community Single Sign-On (CSSO) security infrastructure within the platform.

The CSSO enables the various EDIT service providers to protect their services and resources defining individual access control policies, while users can access different services using only one identity. The security infrastructure bases on the Shibboleth SSO framework which relies on the SAML protocol family. In particular, Shibboleth and SAML provide a federation concept to realise the community aspect.

This milestone reports on the enhancements achieved in comparison to component C5.83, the initial CSSO security infrastructure setup.

## Evaluation user attributes management software

While in component C5.83, the focus has been on establishing the single sign-on framework for EDIT which relies on available identity management systems, it turns out that in order to build up an EDIT federation a comfortable solution for user, group and attribute management would be appreciated. Thus, we started an investigation and evaluation process of suitable user and attribute management tools for Shibboleth (SAML).

Thereby, following management tools have been inspected: ShARPE[1], Group Management Tool[2], Grouper[3]/Signet[4] and OpenSSO[5]

ShARPE did not make any significant progresses since more than one year and is not compatible with the current Shibboleth or SAML version 2.x respectively. The Group Management Tool appeared to be quite closely coupled to the tool providing SWITCH Authentication and Authorization Infrastructure (AAI). Grouper and Signet are both developed by the Internet2 Middleware Initiative[6] also heading the Shibboleth development. While Grouper looks suitable to manage hierarchical groups and roles, a dedicated user management tool is missing. Signet provides centralised user privileges management, but has no active developer community and currently, there is a discussion about integrating it with Grouper. Finally, besides other features OpenSSO not only offers user, group and attribute management faciilites, but also federation management, centralised administration of remote service providers via policy agents, web service APIs for integration with web services (SOAP, REST). Further on, it provides several SAML V2.x profiles and integrates existing identity management solutions via connectors. OpenSSO is provided by SUN as Open Source.

In short, OpenSSO has been evaluated as most suitable tool for the purpose of EDIT. So, we replaced the initial Shibboleth IdP setup by OpenSSO. Simultaneously, the installation of our demonstration Shibboleth service provider (SP) has been upgraded to V2.1. This version supports the SAML V2.0 protocol, eases the integration and configuration processes for both OpenSSO and Shibboleth service providers in general. Additionally, it provides federated logout

1 http://www.federation.org.au/twiki/bin/view/Federation/ShARPE
2 http://www.switch.ch/aai/support/tools/gmt.html
3 http://grouper.internet2.edu/
4 http://signet.internet2.edu/
5 http://opensso.org/
6 http://middleware.internet2.edu/

feature missed by precedent Shibboleth versions. Further on, the SP demo setup demonstrating SSO features by mirroring the EDIT developer tools could have been kept unchanged.

Moreover, we are now able to integrate service and identity providers being not able to setup and configure their own web server instance (e.g. web hoster). For that, we checked out simpleSAMLphp[7], which only relies on a PHP environment and plays well with OpenSSO and Shibboleth.

Finally, our Shibboleth authentication Plugin for Drupal has been significantly improved by the Drupal community. So, we will use the community plugin now.

## Details

For more detailed information regarding CSSO or the current development state of this activity, please refer to the CSSO section within the WP5 developer's wiki[8].

7 http://rnd.feide.no/simplesamlphp

8 Detailed CSSO description in the WP5 developers wiki (http://dev.e-taxonomy.eu/trac/wiki/CSSO)