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"

C5.83 Setup the initial CSSO security infrastructure for the platform

Due date of component: Month 29
Actual submission date: Month 30

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

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

Revision: final

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)	

C5.83 Setup the initial CSSO security infrastructure for the platform

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 provides a federation concept to realise the community aspect.

This component reports on the initial setup of the Shibboleth single sign-on with regard to the establishment of an initial EDIT federation and the profiles elaborated in component C5.82.

Security Infrastructure

This component sets up the required Shibboleth components Identity Provider (IdP) and Service Provider (SP). The latter involves setting up an initial Public Key Infrastructure (PKI) in order to issue X.509 keys and certificates for EDIT related IdP and SP services. This also allows to establish secure communication channels between authorised services of the EDIT federation. For instance, a separate Linux system has been implemented on an encrypted device, where the graphical interface TinyCA[1] is running the openssl[2] library, which is used to provide the necessary Certification Authority (CA) functionality, such as issuing server certificates.

The IdP component has been configured. The IdP's task is to authenticate users of the EDIT federation and delivers attributes about authenticated users to requesting SPs of the EDIT federation. Currently, the user database is only running against a local LDAP directory, which is synchronising regularly to the user database of the EDIT developers. This is because in the current phase of the project EDIT, few applications are available. In addition to the prototype version of the ExpertsDB, EDIT developer tools like the Developers Wiki based on Trac and the version management system Subversion have been connected to the SSO system, in order to provide a solid base for testing and demonstrating the system's features.

The EDIT SP running on https://sp.e-taxonomy.eu mirrors the applications stated above and operates on the same databases as the "original" application located at http://dev.e-taxonomy.eu. This way, both installations can be used simultaneously without any data loss. This setup has turned out to provide a very handy showcase demonstrating the advantages of the CSSO infrastructure. In addition, it prepares for a smooth migration of these tools to the CSSO whenever appropriate. The third Shibboleth component identified in component C5.82, the "Where are you from"(WAYF) service is currently not installed, since this service is only needed when running more than one IdP instance.

Finally, the CSSO components Shibboleth Proxy and the CSSO Java-API, which is derived from the client part of the Shibboleth Proxy implementation, are ready to be used, too. The Shibboleth Proxy enables Shibboleth-unaware applications to connect automatically and make use of HTTP-based service providers protected by the Shibboleth authentication framework. Currently, the

1 http://tinyca.sm-zone.net/
2 http://www.openssl.org/

Java-API provides a simple software interface to EDIT software developers wanting to "shibbolise" their client application or web service, according to the profiles presented in component C5.82. Both components will be subject to further improvements as additional services and applications become ready for integration into the Shibboleth framework.

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[3].

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