Shibboleth

Shibboleth itself does not provide authentication nor access control. It defines a set of protocols for secure passing of identity information between users’ home institutions and service providers (targets). It relies on the home institution to establish the user’s identity and on the resource provider to grant access to the user based on the user’s attributes released by the home institution. The attributes are written in SAM, an international standard developed by the OASIS. The users only have to reveal their true identity to their home institution, while Shibboleth will release only minimal amount of information necessary for the access decision to be made. For instance, for a researcher to access a genome database, the information passed to the database provider may only include “this user is a researcher at our institution” but not the user’s real name. This infrastructure depends on a level of trust established between organisations in a Shibboleth federation.

FAME-PERMIS

PERMIS (Privilege and Role Management Infrastructure Standards) is a policy-based access control engine that can be integrated with Shibboleth to help resource providers (targets) make their access control decisions.

FAME part of the project is responsible for providing extensions to support multi-factor authentication (e.g. by means of username-passwords, IP addresses, soft or hard certificate tokens, etc.) and single sign-on (SSO). Each of the authentication methods will further be assigned a Level of Assurance (LoA), based on NIST Draft Recommendation for Electronic Authentication and according to the strength of the authentication method used. The LoA will be fed into PERMIS authorisation engine, which will be extended to include this additional attribute in its access control decision making. LoA will be passed to PERMIS via Shibboleth as a SAML message. In this way, for instance, users authenticated by means of smart-card will have an option to use their username-password pairs in case when there is no access to a smart card reader, with their LoA adjusted accordingly.

Overview

The JISC Core Middleware Programme is working on improving the way in which users from different institutions access resources on the Web. Currently, users are required to maintain multiple username-password pairs for different resources. In addition, users may posses more than one credential, such as a certificate or a smart-card. To resolve access management issues, a strategy based on Shibboleth has been adopted.

Contact

Dr. Ning Zhang, University of Manchester (nzhang@cs.man.ac.uk)
Prof. David Chadwick, University of Kent (D.W.Chadwick@kent.ac.uk)

Web

www.fame-permis.org  www.permis.org