Title

Allowing the user to define the attribute release policy

Authors

Roland Hedberg, roland.hedberg@umu.se

ITS, Umeå University, Sweden

Keywords

User Managed Access SAML2

Abstract

It is reasonable to assume that as the identity federations grows the task of maintaining the identity providers attribute release policy increases. Categorizing service providers using entity categories is one attempt to alleviate the burden on the system administrators. Another would be to allow each user to individually control the release of her attributes.
User managed access (UMA) is a profile and extension to OAuth 2.0 . UMA defines how resource owners can control protected-resource access by clients operated by arbitrary requesting parties, where the resources reside on any number of resource servers, and where a centralized authorization server governs access based on resource owner policy.
Combining SAML2 and UMA might then be one way of allowing individuals to manage their attribute release.
But the SAML2+UMA combination may also solve other problems like:

- having different entities managing different portions of the same dataset or
- letting an IdP gather information from several different datasets under the same or different policy regimes or
- having the users information in one central place and then allowing different identity providers access to user controlled views of the users information.

This talk will describe a SAML2+UMA implementation and also demonstrate one or more use cases.

Acknowledgements

The work on the UMA implementation was done within the Geant3+ JRA3T2 task.

References

Author Biographies

Roland Hedberg is senior researcher at ICT Services and System Development (ITS), Umeå University, Sweden. His main research areas includes distribute authorisation and authentication service infrastructure and identity management. He has participated actively in development, standardisation and deployment of LDAP in the IETF and various

operational forums. Presently he is involved in standardisation and development of OAuth2, OpenID Connect and UMA. He is leader for the JRA3T2 subtasks within the GEANT3+ project and participates in JRA3T1. In each of these he designs and implements service infrastructure. He is also co-chair of TERENAs Task Force on European Middleware Coordination and Collaboration (TF-EMC2).