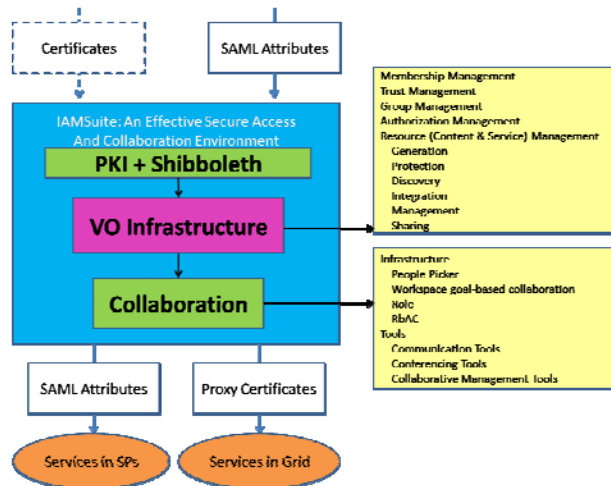


Collaboration Toolkit for Virtual Organization

(Version 1.0)



A toolkit for eResearch Projects and Departments, wishing to leverage Federated ID for accessing data, resources and collaboration tools

Introduction

All research projects are different, but most project infrastructures are more equal than not. They all require some form of collaboration between project members across different institutions, dissemination of research results, security restrictions on resources between public accessibility and protected ones.

IAMSuite is built to satisfy the above requirements. It provides a common environment for researchers to perform collaboration in a *Virtual Organization (VO)* context. Users from different institutions can gather in a common place, share resources, and collaborate without the need to worry about common infrastructure such as security (authentication and authorization).

A particular feature of IAMSuite is the notion of trust within the VO where a Role-based Access Control (RBAC) authorization based on user's attributes is enforced throughout the system. Single Sign-On is achieved through use of Shibboleth as implementation of Security Assertion Mark-up Language (SAML) standard.

Shibboleth allows institutions from different domains to communicate through the same SAML standard to establish trust between them. Once the trust is established, SAML allows transfer of attributes from home organization (Identity Provider – IdP) to service organization (Service Provider – SP). SPs can use the supplied attributes to provide fine-grain authorization on its services/resources.



Figure 1. IAMSuite interface

IAMSuite, as a service being offered by an SP, uses the attributes for its RBAC on a range of its internal resources and services as well as external shared resources. External

resources can be shared within IAMSuite to allow subset of users within the VO (given the right permissions) to gain access to those resources. For example, Joe would be able to share photos of his last holiday (hosted in a service in the federation) to some members of his 'Holiday Paradise' VO and yet he would know that his photos are safe from unwanted public access.

IAMSuite implementation is seen as a service within the broader federation. IAMSuite is capable of being connected to a range of Service Providers to form a *mini* federation. This allows certain services that are relevant to the Virtual Organization to be identifiable (and accessible) from within IAMSuite alone hence simplifying the management of those services.

When IAMSuite is used to access services from the wider federation, the SP needs to treat IAMSuite as a *mini* federation (containing at least an IdP) in which it is capable of supplying VO attributes. IAMSuite acts as multiple Attribute Authority – SAML entity within IdP that supplies user's attributes – to those SPs.

The approach employed by IAMSuite to allow it to communicate to the wider federation is known as Federation Peering.

IAMSuite v1.0 alpha allows quick and easy installation/testing using pre-existing systems or with the support of MAMMS Shibboleth VMWare setup.

Objectives

In short, IAMSuite objectives are:

- Providing trust federation management functionalities that facilitating Shibboleth IdPs and SPs joining IAMSuite trust federation
- Providing a shibboleth single sign-on infrastructure for team collaboration
- Providing People Picker connection to search collaboration partners
- Providing an integration and sharing environment for protected resources and services/tools
- Providing familiar environment for developers to develop the tools and for users to access those resources and tools
- Providing general framework for specific developers to build their collaborative applications
- Providing Grid access including Grid proxy generation

IAMSuite Features

The followings are some of the selected features of IAMSuite. For information of complete IAMSuite's features, please refer to our website.

- GridSphere portal-based as familiar environment for both users and tool developers

- Goals and workspace oriented allowing resources and tools to be readily available in one interface
- Wide range of collaboration tools (content repositories, wikis, forums, video meeting, instant messaging, calendaring, etc)
- Easy integration of *shibbolized* tools
- SSO to integrated tools
- Ability to propagate VO attributes to integrated tools
- RBAC authorization on resources and services
- Integration on other environments such as access to grid resources via proxy certificate generation
- Ability to represent as a single VO instance or as a multiple sub-VOs instance
- Multiple languages supported
- Third party collaboration workspaces integration



Figure 2. Transfer of VO attributes when accessing resources through IAMSuite (notice SSO)

VO Memberships

Users in IAMSuite are divided into:

- **Guest** – can access permitted workspaces
- **User** – can activate portlet-based tools into IAMSuite as well as accessing permitted workspaces
- **Admin** – ability to manage workspace, groups, and resources as well as all **User**'s capability
- **Super** – ability to manage VO memberships, IdPs and SPs, and all **Admin**'s capability

A typically VO would have one or two **Super** users, a handful of **Admin** users, and lots of **Users** and **Guests**.

Resources, Services, and RBAC

Authorization based on RBAC is employed in IAMSuite in which only users who belong to appropriate group and roles can gain perform various functionalities in workspaces over specified resources/services.

Users are able to share resources and services (local and remote) in VO and set appropriate permissions to them. Permissions set is enforced internally within IAMSuite and is

transformed to appropriate VO attributes to external resources to support enforcement of fine-grain access control. Remote resources/services can use the supplied VO attributes to grant appropriate access to the user.

Content Folder, as logical grouping of resources, may contain a collection of items that have same default permission set unless explicitly modified.



Figure 3. Assigning roles and permissions to users on resources

There are two types of sharing mode for services and resources:

- **Shared** – other users can use the service/resource in their workspaces, i.e. content repositories are typically shared between users but the content of the repository may have restrictions for subset of users
- **Private** – only the owner can use the service/resource or the service can only be used in the current workspace by assigned members.



Figure 4. Resources and Services

IAMSuite allows users to gain access to configured services by means of releasing VO attributes to those services. VO attributes could be in the form of the user's role in the current workspace or her mapped role as required by the end Service Provider as understood by IAMSuite. For example, user's role "Project Manager" in IAMSuite is transformed into "Editor" on Content Repository when the user is trying to access this particular Content Repository (transformation is automatic as defined during integration of such services).

Furthermore, access to the services is categorized into three different types:

- **None** – the service does not require authentication and authorization, i.e. public service
- **Internal** – the VO will release information about the user to the service, i.e. the VO is using its *internal* attributes to be supplied to the SP
- **Federation IdP** – the service only trusts attributes coming from a federation IdP, i.e. SP only receives user's attributes from federation IdP (as oppose to VO internal IdP)

Collaboration within a Federation

IAMSuite provides administration management of the list of trusted IdP and SP. Only users from allowable IdP can access the VO and only the trusted SPs are accessible by the users within the VO.



Figure 5. Configure user base of the VO

IAMSuite Development

This software was developed by the Meta Access Management System (MAMS) project at Macquarie University, Sydney, Australia. The MAMS project is funded by the Australian Federal Government's Department of Education, Science and Training (DEST) as part of "Backing Australia's Ability" program.



References

IAMSuite: <http://federation.org.au/IAMSuite>

MAMS Federation : <http://federation.org.au>

MAMS: <http://mams.melcoe.mq.edu.au>

Contact Mail: iamsuite@mams.org.au