TeraGrid

TeraGrid

In the summer of 2006, the GridShib project participated in the TeraGrid Authentication, Authorization and Account Management Workshop held at Argonne National Laboratory (Aug 30–31). As a result of this workshop, a TeraGrid testbed was proposed. The goals of the testbed were 1) to leverage campus authentication infrastructure, and 2) to employ attribute-based authorization at TeraGrid resources. To achieve these goals, a number of use cases were identified and targeted:

- New Individual User
- Existing Individual User
- Science Gateway
- Shib-enabled Science Gateway

A TeraGrid Science Gateway is a portal or suite of applications that provides access to an integrated set of resources.

Individual TeraGrid Users

One approach is to leverage the myVocs registration process.

A new TeraGrid user performs the following steps:

1. The principal registers with myVocs and thereby becomes a member of some TG community.
2. The principal requests a short-term EEC from the GridShib CA, which issues an authentication request to the myVocs !IdP on behalf of the principal.
3. The myVocs !IdP is protected by the myVocs SP, so the client browser is redirected to the federation WAYF where the principal chooses their preferred !IdP.
4. The WAYF redirects the client to their campus !IdP of choice, which identifies the principal.
5. The campus !IdP issues an authentication response to the myVocs SP.
6. If the campus !IdP does not push attributes, the myVocs SP queries the campus AA for attributes.
7. The myVocs SP exposes either the authentication response or the attribute response (depending on whether or not a query occurred) to the myVocs !IdP.
8. The myVocs !IdP captures the response exposed by the myVocs SP. The `<samlp:Response>` element is stripped away by the !IdP, leaving at most two `<saml:Assertion>` elements.
9. The myVocs !IdP nests the `<saml:Assertion>` elements in the `<saml:Advice>` element of an attribute assertion, which contains a VO membership attribute.
10. The myVocs !IdP issues an authentication response to the GridShib CA. If attribute push is enabled, the attribute assertion accompanies the response, otherwise the GridShib CA queries for attributes.
11. The GridShib CA strips the assertion(s) from the response and binds them to the EEC (according to the X.509 Binding for SAML).
12. The GridShib CA issues the EEC directly to the principal.
13. The principal authenticates to a TG resource using the SAML-decorated EEC.
14. The resource maps the VO membership attribute in the SAML assertion to a local user account.

An existing TG user registers their TG-issued certificate with the GridShib Certificate Registry at the myVocs !IdP. Instead of a VO membership attribute, the myVocs !IdP returns an attribute assertion containing a DN attribute. The GridShib CA uses this attribute as the DN of the EEC it issues to the principal.

TeraGrid Science Gateways

Assume all gateways wish to leverage community attributes, that is, attributes distinct from campus attributes. (Community attributes are referred to as VO attributes in myVocs.) This implies that all gateways will leverage the equivalent of a local SAML AA deployment. In the case of a shib-enabled gateway, a campus Shib AA is queried in addition to the local SAML AA. (The local SAML AA deployment could be a myVocs deployment, for example.)

$ **Science Gateway**: A principal authenticates to the gateway by unspecified means. The gateway issues a SAML attribute query to the local SAML AA on behalf of the principal. The SAML AA responds with an assertion containing a single `AttributeStatement` . Using its community credential, the gateway binds the SAML assertion to a proxy. The gateway uses the proxy obtained from the local query to request a grid service on behalf of the principal.

$ **Shib-enabled Science Gateway**: A principal authenticates to the gateway using campus credentials. First the gateway queries the campus Shib AA for attributes on behalf of the principal. The Shib AA responds with an assertion containing a single `AttributeStatement` . Next the gateway issues a SAML attribute query to the local SAML AA on behalf of the principal. Likewise the SAML AA responds with an assertion containing a single `AttributeStatement` . Using its community credential, the gateway binds the two SAML assertions to a proxy. The gateway uses this proxy to request a grid service on behalf of the principal.

Typical examples of Science Gateways are nanoHUB and National Virtual Observatory. In the case of a shib-enabled gateway, each query results in an additional SAML assertion. The two assertions are bound to a well-known extension in the proxy using an X.509 Binding for SAML.

At the GridSP, there is a new PIP (similar to the SAML authn assertion PIP) that processes every certificate in the chain, including the EEC. If there is a SAML assertion at the designated extension, the assertion is consumed by the PIP. Attributes, in particular, are aggregated over all certificates in the chain.