Researches on Authentication Integration at NII, Japan

APGridPMA face-to-face meeting
March 9th 2020
Academia Sinica, Taipei, Taiwan

Eisaku SAKANE
National Institute of Informatics
Contents

• A Study of Credential Integration Model in Academic Research Federation Supporting a Wide Variety of Services
  • PoS(ISGC 2018 & FCDD)016

• Toward Single Sign-on Establishment for User-friendly Inter-Cloud Environment
  • PoS(ISGC2019)028
A Study of Credential Integration Model in Academic Research Federation Supporting a Wide Variety of Services
Outline

• Introduction to GakuNin and HPCI
• Issues
• Consideration of credential integration between GakuNin and HPCI
• Discussion
• Related works
• Summary
An Academic Identity Federation in Japan

- Build up new ICT infrastructure to support R&E based on SSO technologies
- Provides trust framework (technologies, policies and assessment)
- Offers value added services (academic discount, etc.) by collaboration with commercial
- Improves usability and security with continuous R&D (including multifactor/cert. auth.)
HPCI: High Performance Computing Infrastructure

HPCI authentication system features include:
• Single user ID and multiple accounts called HPCI-ID, HPCI and local accounts
  • HPCI accounts are managed by identity providers.
• A hierarchical initial identity vetting system based on face-to-face meetings with photo-IDs
• Two kinds of credentials for services in HPCI:
  • Shibboleth assertion for Web services: certificate issuance, CMS, etc.
  • GSI proxy certificate for access to supercomputers and storages
Difference between HPCI and GakuNin

• What is difference between HPCI and GakuNin?

• IdP in HPCI is different from IdP in GakuNin:
  • GakuNin IdP is managed by an academic institution and covers all constituent members of its academic institution.
  • HPCI IdP is managed by a supercomputer center (university or institute) and covers only HPCI users who are not only academic researchers but also industrial ones.

• Why did HPCI build dedicated IdPs?
  • HPCI IdP has to satisfy a strict LoA imposing identity vetting via a face-to-face meeting.
  • HPCI IdP needs to cover industrial researchers.
  • HPCI is not a common service to all constituent members of an academic institution like e-Journals.

• Only if HPCI users are academic ones, at least HPCI and GakuNin IdPs should be integrated.
Guiding question

• How do we integrate HPCI IdP and GakuNin IdP in order that academic users only need to manage one credential?

• We select GakuNin IdP as primary identity provider because GakuNin IdP is operated by home organization that user belongs to.

• How do we apply a credential issued by GakuNin IdP to HPCI services?
Authentication flow in HPCI

- Initial Identity Vetting
  - Shibboleth IdP
  - Shibboleth SP
  - myproxy-logon
  - gsi-login

- HPCI account issuing (IdP)
  - Shibboleth SAML
  - Certificate issuing as a Web service
  - Bridging
  - GSI
    - Supercomputers, Storages

Registered data
- Name
- Affiliation
Possibilities for GakuNin credential application

1. Initial Identity Vetting
2. Shibboleth IdP
3. Shibboleth SP
4. Shibboleth SAML
5. Certificate issuing as a Web service
6. Supercomputers, Storages
7. GSI
8. myproxy-logon
9. gsi-login
10. HPCI account issuing (IdP)

Registered data:
- Name
- Affiliation

Check

NII National Institute of Informatics
We consider applying the GakuNin credential to the initial identity vetting in HPCI IdM.
Basic idea:
Initial identity vetting with external credential

1. Presenting some credential
2. Inquiry about the applicant
0. Agree with cooperation

identity vetting based on an LoA
notifying the applicant of the inquiry

an applicant

Trusted Third Party (CA, IdP, ...)
IdM

generalized our previous work, PoS(ISGC2017)009
Initial identity vetting with credential issued by GakuNin IdP

1. Access to a Web service for initial vetting
2. Shibboleth authentication

the applicant already has the account.

an applicant

0. Agree with cooperation

generalized our previous work, PoS(ISGC2017)009
Initial identity vetting with credential issued by GakuNin IdP (Cont’d)

0. Agree with cooperation

2. Shibboleth authentication
2.1. The IdP authenticates the applicant.
2.2. The IdP confirms whether the applicant allows the IdP to send the required attributes to the IdM.
2.3. The IdM can check the identity data against the information provided by the IdP.
Discussion

• Do the proposed procedure provide the same level of assurance?
  • HPCI IdM must vet the identity of user based on a face-to-face meeting with a photo-ID.

The user present her/his photo-ID issued by home university.

The proposed procedure can intuitively be regarded as the initial identity vetting based on a face-to-face meeting.
Discussion (Cont’d)

• Another possibility of GakuNin credential application.
  • Due to the end of GSI support, HPCI needs to reconsider the authentication and authorization system in HPCI to access to supercomputers and storages.
  • Credential for Web services may be changed by new AA system in HPCI.
  • However the GakuNin credential application to initial identity vetting will remain almost unchanged.
Related Works

• *Snctfi* from AARC’s policy work
  • maybe able to corroborate our proposed procedure with Snctfi.
Summary

• We proposed a credential integration model in which GakuNin credential (SAML assertion) can be used to the initial identity vetting in HPCI.

• Our approach can be extended to more general case.
• Our proposed procedure in initial identity vetting should be corroborated with a trust framework.
Toward Single Sign-on Establishment for User-friendly Inter-Cloud Environment
Outline

• Background
• Issues
• Design & Implementation
• Discussion
• Summary
Background

• Many different clouds are available to offer a variety of services.
• Users can choose various services from multiple cloud vendors according to the demands of the users.

• Single sign-on mechanism is indispensable for *inter-cloud* computing environment.

• In general, a single sign-on mechanism works within a cloud environment provided by a single cloud vendor.
• However, the single sign-on mechanism that *extends* across multiple clouds is not always established at the beginning of use.
Background (cont’d)

• For example, an academic researcher who can obtain a SAML assertion from the home organization should be enabled to access a public cloud with the assertion.
• Since many cloud vendors, of course, already supports major authentication technologies such as SAML and OpenID Connect, technically the credential issued by the home organization will be usable for access to public clouds.
• However, it is often hard for the identity provider operated by the home organization to manage the user attributes that the cloud vendor requires, because the operating department of the IdP is responsible only for attributes that are assigned naturally in terms of the constitute member of organization, and it will be quite a burden to manage various attributes for users individually unless the cloud service is provided for all members as a common service.
Guiding Questions

• How do we build a mechanism for handling necessary attributes information based on the credential issued by the home organization?

• What should we do in order not to impose a burden on administrators of the identity provider?
Design

• Gateway service approach
  • authenticate users with credentials issued by the home organization.
  • provide a function that allows Service Provider to set attribute *types* that the SP requires.
  • provide a function that allows users or representatives to set the *values* of the required attributes.
  • make an assertion that is composed of the required attributes and the fundamental attributes managed by the home IdP, and send it to the SP.
  • provide users with a user-friendly interface for access to available services.
Cloud Gateway Service

- A web portal system for federated identity w/SAML.
- CGS can show available services as icon.
  - permitted by organization
  - permitted by group
- Typical flow is the following:
  - User accesses to the CGS.
  - Internal SP in the CGS responds and embedded DS shows the list of IdP to the user.
  - The DS redirects to IdP specified by the user.
  - After the authentication succeeded, the CGS displays the available services as icon.
  - The CGS redirects to the SP that provides the service selected by clicking.
  - The service interprets the entityId of the IdP and then redirects to the IdP.
  - The service receives the assertion sent by the IdP with SSO.
  - The user now uses the service.
Implementation

- Access to AWS with SAML 2.0 assertion via the GakuNin CGS.

1. Access to the /Unsolicited endpoint.
2. Redirect to Shibboleth SP.
3. Select an IdP on DS.
4. Authenticate with the home IdP.
5. Convey the ID to Shibboleth IdP.
6. Get the attribute values specified.
7. Generate the necessary attributes and send them.

- Set an AWS Role and the required attributes beforehand.

<table>
<thead>
<tr>
<th>attribute name</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWSName</td>
<td></td>
</tr>
<tr>
<td>AWSRole</td>
<td>&lt;fixed value&gt;</td>
</tr>
</tbody>
</table>

GakuNin Cloud Gateway Service
E. Sakane, National Institute of Informatics
Flow for access to AWS with SAML

• AWS account user creates a Role and a SAML-ID provider according to the AWS instruction.
  • determine the set of names and values of attribute for authorization.

• Administrator of SP connector for AWS globally sets up the required attribute names and sets common fixed values for any AWS roles.

• Group administrator sets user configurable values, the AWS Role and SAML-ID provider.

• User, a member of the group, can access the AWS Role by just clicking the icon.
Discussion

• Required attributes can sent to AWS without any changes of setting of the home organization IdP.

• Home organization IdP does not need to modify the setting of the IdP by using the AWS support of GakuNin CGS even if the organization provides AWS services to all constitute members.

• If there are different AWS roles that require different attributes, the administrator of SP connector for AWS must setup all attributes.

• The administrator of SP connector AWS must grasp all attributes that all AWS Roles defined by any groups in the GakuNin CGS require.
Summary

- We proposed a model that realizes single sign-on in an inter-cloud environment by designing required attributes assignment mechanism.
- Based on the GakuNin CGS, we implemented the functions that allow users to access to Amazon Web Service with SAML 2.0.
- Our approach can be applied to the other services that support SAML 2.0.
- We will examine more services and improve the proposed system.
  - Dropbox supported.