A Study of Authentication Proxy Service for Various Research Communities

*National Institute of Informatics
**Kyoto University
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.)
Background

• Necessity for a new trust framework in Japan
  • GakuNin has provided a stable trust framework to academia in Japan.
  • There are many research communities in Japan, but they don’t always rely on
    IdPs in GakuNin because all GakuNin IdP do not satisfy the requirement of the
    communities.
  • As a result, a trust framework has been formed in each research community.
  • Many of users in the research communities are also constituent members of
    IdPs that join GakuNin.
  • It is natural for users to demand to use home organization account for services
    in the research communities. In other words, users shouldn’t want to manage
    several accounts.
Request from Research Communities

- Authenticating users that don’t have suitable IdP accounts.
  - Users that RC offers services not always possess the account of an IdP joining GakuNin.
  - RC want to rely on IdP that provides sufficient identity assurance.
- Grasping authenticator level
  - Password only or multi-factor authentication
  - For certain services RC want users to impose MFA.
- Identification user that belongs to several organization.
- Ensuring user identity moving between different organizations.
  - SP want to provide continuously and efficiently services to users moving between different organizations.
- Support for suitable attributes for purpose
  - e.g., grasping whether resident or not (export control)
Key Components in New GakuNin Trust Framework

- **GakuNin IAL/AAL**
  - Stipulation of IAL and AAL

- **Authenticator Registry**
  - Evaluation of authenticators based on GakuNin AAL

- **Authentication Proxy Service "Orthros"**
  - AL matching, credential bridging, attribute coordination

- **IdP Hosting Service**
  - Addressing issues of IdP building and operation

- **Advanced Group Management**
  - Support for high and complex authorization control
Development of Authentication Proxy Service

- Support for the new GakuNin trust framework.
- Bridging between IdPs and SPs, and enabling IAL/AAL management and attribute assurance.
- Enabling research communities to delegate identity vetting to user’s IdP.

- Attribute Providers
- Identity vetting
- Binding & synthetic IAL/AAL matching
- Ensuring attributes by Project managers
- Collab. w/ business
- Authentication Proxy

IdP, Org, SP

Individual number, gBizID, mobile vendors ORCID, Org. contracted MS/Google, home IdP

Project, KAGRA, HPCI, etc.

OpenIDP-ng

MDX/GakuNin RDM SP

GakuNin/eduGAIN
Use case 1 – credential bridging

- Researchers of companies use GakuNin RDM with ORCiD credential.

1. Binding user with ORCiD beforehand.
2. Requesting access
3. Redirecting to Orthros.
4. Authenticating with ORCiD.
5. Sending assertion
6. Succeed in access
Use case 2 – IAL enhancement

• By binding several ID, IAL required by SP is satisfied.
Design and Implementation of Orthros

• Core part of authentication proxy (IDaaS)
  • SELMID – https://ctc-insight.com/selmid

• User interface part
  • developed in-house

• Fundamental functions
  • ID management, login, ID binding, management of ID binding, attribute management

• SP management (for SP administrator)
  • handling IAL/AAL imposed by each SP

• Agreement management for each SP
  • Getting user agreement when user initially login to SP
  • Enabling user to confirm or cancel the current status of agreement.
  • Enabling administrator to check the status of agreement of user.

• Attribute assurance
  • Enabling administrator to ensure attributes of user whom the administrator manage.
  • e.g. ensuring user affiliation attribute
Design and Implementation of Orthros (Cont’d)

- More functions implemented
  - Notification at changing mail address.
  - Termination of account.
  - Management of IdP linkage.
  - Forcible password resetting.

- Linking external IdPs
  - Linked: LINE, Google, Yahoo! JAPAN, Facebook, Twitter
  - Now in progress: gBizID, ORCiD

- Linking more SPs
Sign-up (1/4)
Sign-up (2/4)
Sign-up (3/4)

アカウント

メールアドレス: [redacted]
マイナンバー: 0216e57c-3cf-48d9-9ee0-89763815e10e
UL: Level1
ePPN: 20651aae-4837-4881-a592-016e57e0707c@opensidp.nii.ac.jp

利用中のSPの連携同意状況

サービスの認証連携状況

<table>
<thead>
<tr>
<th>サービス名</th>
<th>連携状況</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gitee</td>
<td>自動連携</td>
</tr>
<tr>
<td>OpenID</td>
<td>自動連携</td>
</tr>
<tr>
<td>LINE</td>
<td>自動連携</td>
</tr>
<tr>
<td>Google</td>
<td>自動連携</td>
</tr>
<tr>
<td>Yahoo!JAPAN</td>
<td>自動連携</td>
</tr>
<tr>
<td>Facebook</td>
<td>自動連携</td>
</tr>
<tr>
<td>Twitter</td>
<td>自動連携</td>
</tr>
<tr>
<td>OpenID</td>
<td>自動連携</td>
</tr>
</tbody>
</table>

認証連携を行う
Sign-up (4/4)
Linking external ID (1/4)
Linking external ID (2/4)
Linking external ID (3/4)
## Linking external ID (4/4)

A screenshot of a webpage showing the status of service authentication connections. The services listed are:
- GBizID: Not linked
- OpenIDP: Not linked
- LINE: Not linked
- Google: Not linked
- Yahoo! Japan: Not linked
- Facebook: Not linked
- Twitter: Not linked
- ORCID: Linked

The page also includes links to manage authentication connections.
ログイン（1/4）
Login (2/4)
Login (3/4)

Sign in

Email or 16-digit ORCID ID
example@email.com or 0000-0001-2345-6789

Password

SIGN IN

Forgot your password or ORCID ID?
Don't have an ORCID ID yet? Register now

or

Access through your institution

Sign in with Google

Sign in with Facebook
Future Plan

• Toward Orthros in production operation
  • Migration OpenIdP to Orthros
    • OpenIdP supports users who do not possess an account of IdP that joins GakuNin.
  • Linkage external IdP (gBizID, ORCID) in production operation.
  • Enabling user to select attributes that user send to each SP.
  • Home IdP Binding at organization change.
  • Support for GakuNin IAL/AAL policy.
  • Enhancement of attribute handling for authorization.

• AL enhancement scheme.

• Operation policy and practice statement should be published.
Summary

• We developed an authentication proxy service, called “Orthros”, to solve the issues of current research situation in Japan.

• Orthros can
  • support new GakuNin trust framework,
  • match IAL/AAL required by SP or ensured by IdP,
  • enhance assurance level,
  • bridge different credentials,
  • coordinate attributes.

• We plan to proceed to trial operation in FY2023.