APGrid PMA Update

Eisaku Sakane

National Institute of Informatics

63rd EUGridPMA Meeting
February 6, 2025

General Status

- Chair and Vice Chair (2024.01-2025.12)
  - Chair: Eisaku Sakane (HPCI CA, Japan)
  - Vice Chair: Sai Prasad (eMudhra)
- Routine Gathering
  - Spring: usually held together with ISGC in Taiwan
  - Autumn: Collocated with e-Science or APAN routine events
  - Virtual meeting will be arranged upon request or whenever there is any issue in-between F2F meetings
- Self Auditing Report: Once a year for each member CA
- Regional Catch-All CA: ASGCCA, now supporting users through local RAs in ID, IN, MN, MY, LK, NZ, PH, TH, VN

CA	ccTLD	Last Self Audit	#valid Cert	IPv6	Prod. eduGAIN SP	Main User Community
ASGC CA	*TW*	*Mar. 2024*	*110, 186, 17*	*Y*		*ATLAS, CMS, e-Science*
AusCert	*AU*			*Y*	*AAF*	*ATLAS*
HPCI CA	*JP*	*Aug. 2023*	*206, 109/264*	*Y*	*GakuNin/NII*	*HPC*
IGCA	*IN*	*Mar. 2018*	*38, 12*		*INFED/INFLIBNET*	*CMS*
IHEP CA	*CN*	*Mar. 2021*	*123, 125, (27)*	*Y*	CARSI (480+ entities)	*WLCG, Belle II, BES III, CEPC, JUNO*
KEK CA	*JP*	*Aug. 2023*	*140, 168*	*Y*	*GakuNin/NII*	*Belle II, ATLAS,ALICE, ILC, Muon g2*
KISTI CA	*KR*	*Aug. 2023*	*24, 30, 3*	*N*	*KAFE/KISTI*	*ALICE*
eMudhra	*COM*					*From Sep 2023*
Retired CA (10)	*AIST CA (JP), APAC CA (AU), MYIFAM CA (MY), NCHC CA (TW), NECTEC CA (TH), NAREGI CA (JP), PRAGMA CA (US), HKU CA (CN), CNIC CA (CN), SDG CA (CN)*					

From Previous APGridPMA Meeting in March

- Moving towards new AAI according to user communities or resource federation infrastructure
  - HPCI Japan: started operation on a token-based AAI based on OAuth-SSH, KeyCloak, OIDC agent and JWT-agent, and also considering cooperation with GakuNin. jwt-agent : https://github.com/oss-tsukuba/jwt-agent
  - ASGCCA, KEKCA: deploying token-based AAI model (INDIGO-IAM) for broader user communities.
  - SIFULAN Malaysian Access Federation offers IdP-as-a-Service to country-wide user communities.
- Regional Identity & Access Management Collaborations
  - Identity & Access Management (IAM) WG @APAN - Support SAML2/federated AuthN services buildup & conversion based on eduGAIN (REFEDS) collaborations.
- Communication
  - The APGridPMA began to use the Slack workspace: https://apgridpma.slack.com for prompt communication between members.
  - We are still considering efficient operation on communication tools such as webpage, mailing list.

Future meeting

- APGridPMA Meeting (virtual) last autumn was skipped.
  - Because the members' schedule did not be matched up with.
- 34th APGridPMA Meeting – will be held in Taipei, March 18, collocated with ISGC 2025.

- 35th APGridPMA Meeting – will be held this summer or autumn.

- APAN 59 will be held in Yokohama, Japan, March 3-7, 2025.

GakuNin & HPCI Activities

GakuNin: Academic Identity and Access Management Federation in Japan
HPCI: High Performance Computing Infrastructure in Japan

© 2024 National Institute of Informatics

Key Components in New GakuNin Trust Framework

GakuNin IAL/AAL

- Stipulation of IAL and AAL

By having IdP and SP refer to it, unified and efficient discussions can be made possible, and by each institution complying with it, the trust of GakuNin as a whole can be guaranteed. https://meatwiki.nii.ac.jp/confluence/x/JoSfBQ

Authenticator Registry

- Evaluation of authenticators based on GakuNin AAL

Evaluating authenticators, publishing the results, and encouraging universities and research institutes to promote multi-factor authentication at their IdPs. https://level2.gakunin.jp/

Authentication Proxy Service "Orthros"

- AL matching, credential bridging, fundamental attribute coordination

By mediating requests from SP and linking with IdP, it is possible to guarantee IAL and AAL.

IdP Hosting Service

- Addressing issues of IdP building and operation

Reduce the burden on universities and research institutions in building and operating IdPs, and allow all institutions to operate IdPs by choosing from a variety of operating formats that suit their institution.

Advanced Group Management

- Support for high and complex authorization control

In addition to basic attributes, group management can be based on attributes that general IdPs do not handle, making SP authorization management more efficient.

Authentication Proxy Service - Orthros

- What is Orthros trying to solve?
  "Problems that are difficult to solve with conventional IdPs alone that participate in GakuNin".
  - Authentication of researchers from institutions where it is difficult to participate in GakuNin.
    - Corporate researchers, people affiliated with local governments who contribute to research activities, etc.
  - Authentication of members of a community where researchers, students, and related parties from different institutions work together to conduct higher education and research activities with a common goal.
    - Research communities, educational communities that span organizations, etc.

- How is Orthros solving the problem?
  Utilization of external ID platforms: Link IDs from existing external ID platforms on Orthros and mediate between the external ID platform and the SP.
  - SPs do not need to connect to each external ID platform individually.
  - Candidates for collaboration: Common authentication system for corporations and sole proprietors (gBizID), public personal authentication service (My Number card), ORCID, etc.
- Construct authentication assertions to be sent to SPs based on linking of users' external IDs. Support multi-factor authentication upon request.

- How far has Orthros progressed?
  - Already in operation as a successor to OpenIdP.
  - External ID infrastructure integration has been proven, and preparations are underway for formal integration.
  - Formulation and implementation of IAL/AAL specifications to support the new GakuNin trust framework (FY2024).
  - Consideration of use cases: Considering solutions to problems faced by some SPs.

Medium-scale Demonstration Experiment FY2024

- Purpose
  - This is a demonstration experiment to realize the use of academic e-resources based on the ID operation management of IAL2 and AAL2, which new GakuNin trust framework plans to newly establish in the future.
  - The purpose of this demonstration experiment is to enable IdP operation institutions participating in GakuNin to carry out IAL2 and AAL2-compliant ID operation management, thereby enabling collaborative research in open science and the use of services that require a higher level of security. Connection tests will be conducted to determine whether operation management is possible in line with the IAL2 and AAL2 standards currently under consideration by new GakuNin trust framework, from the standpoints of both strictness and convenience.
- Period: January 17, 2025 to March 31, 2025.
- 20 participants (University, Institute, Company)

Experiment content - IdP

1. Implementation
   Implement metadata notation, SAML Request and SAML Response syntax to realize ID operation management for IAL2 and AAL2 specified by GakuNin, and exchange opinions on its usefulness and availability.
2. Connection check
   Use GakuNin IAL2/AAL2-compatible SP for connection check to check the connection of SAML Request and SAML Response compatible with IAL2 and AAL2.
3. Service trial
   Trial out participating services that are planned to be compatible with GakuNin for the demonstration experiment; GakuNin RDM.
4. IDaaS trial
   Trial out GakuNin IAL2/AAL2-compatible IDaaS.
   - Extic (has identity proofing function using eKYC)
   - Orthros

Experiment content - SP

1. Implementation
   Implement metadata notation and SAML Request and SAML Response syntax to realize ID operation management for IAL2 and AAL2 specified by GakuNin, and exchange opinions on their usefulness and availability.
2. Connection check
   Receive attribute information required for service provisioning from participating institutions and confirm operation.
3. IDaaS trial
   Trial out GakuNin IAL2/AAL2-compatible IDaaS, receive attribute information required for service provisioning, and confirm operation.
   - Extic (has identity proofing function using eKYC)
   - Orthros

Implementation Guide

- SP
  1. A new GakuNin-compatible SP supports AuthnContextClassRef (AC2R). However, for IdPs that do not support AC2R, AC2R is not requested in the SAML Request.
  2. A new GakuNin-compatible SP requests AAL from a new GakuNin-compatible IdP in the SAML Request.

- IdP
  1. A new GakuNin-compatible IdP responds to a SAML Request sent from a new GakuNin-compatible SP by setting the identity assurance level and authenticator assurance level in eduPersonAssurance.

Newly introduced Attributes

- eduPersonAssurance

  Attribute information related to the assurance level of the identity proofing process (IAL) and authentication process (AAL) newly stipulated by new GakuNin trust framework.
  - Example notation
    - AAL1+IAL2
    - AAL2+IAL2

    No IAL1 should be clarified.
- gakuninIdentityAssuranceMethodReference

  Attribute information on the identity proofing method used in the identity proofing process.
  - Example notation
    - TRUSTED DB

      DB maintained by the payroll and academic affairs system. Accounts in this DB are evaluated as having conducted identity verification equivalent to IAL2 as an organization, as their admissions and hiring are carried out smoothly and without incident.
    - KYC
      - When face-to-face identity proofing is carried out.
      - When identity proofing is carried out using eKYC.
    - (Not clarified)

Online self-service for identity proofing: Sign up with federated credentials

Traditional identity proofing based on a face-to-face meeting with photo-ID presentation.

eduGAIN

Next-generation IAM trust framework provides high IAL/AAL.

Academic researcher

②-A. Being authenticated by home IdP with high AL.

HPCI IdM can receive authentication information with high AL.

HPCI IdM

① Sign-up with federated credential (self-service)

Industrial researcher

⓪-B. Binding an ID issued by an available IdM beforehand on Orthros

②-B. Being authenticated by Orthros with AAL2

Orthros acts an intermediary between HPCI IdM and external IdM.

Orthros

gBizID

ORCiD

IdM A, IdM B, IdM C, …

Plans in FY2024 (until March)

- GakuNin
  - We will summarize the result of the medium-scale demonstration experiment FY2024.
- HPCI
  - We will organize the required attributes for online self-service for identity proofing.