APGrid PMA Update

Eisaku Sakane

National Institute of Informatics

66th EUGridPMA Meeting
Nikhef, Amsterdam, NL
February 13, 2026

General Status

- Chair and Vice Chair (2026.01-2027.12)
  - Chair: Eisaku Sakane (HPCI, Japan)
- 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, 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. 2025*	*110, 186, 17*	*Y*		*ATLAS, CMS, e-Science*
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*	*Mar. 2025*	*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 (11)	*AIST CA (JP), APAC CA (AU), AusCert (AU), HPCI CA (JP), MYIFAM CA (MY), NCHC CA (TW), NECTEC CA (TH), NAREGI CA (JP), PRAGMA CA (US), HKU CA (CN), CNIC CA (CN), SDG CA (CN)*					

Relying Party	ccTLD	Note
HPCI	JP	

From Previous APGridPMA Meeting in July

- Regional Identity & Access Management Collaborations
  - Identity & Access Management (IAM) WG @APAN - Support SAML2/federated AuthN services buildup & conversion based on eduGAIN (REFEDS) collaborations.
  - IAM-WG sessions were held in APAN 61 (Dhaka, Bangladesh).
- 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

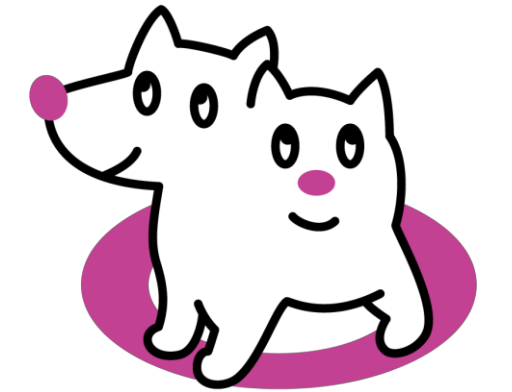
- 36th APGridPMA Meeting – will be held in Taipei, collocated with ISGC 2026.
- 37th APGridPMA Meeting – will be held in Auckland, NZ, collocated with APAN62.

GakuNin & HPCI Activities

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

Work in Progress - GakuNin

- Medium-scale demonstration experiment FY2025
  - started in last December
  - preparation for experiment in FY2026
    - re-organizing requirements, brushing up documents, sharing use-cases, …
- Authentication proxy service “Orthros”
  - covering users without federated-ID (non-academia user, etc.)
  - linking entities with their external IDs
  - Orthros itself has supported Passkey.



Orthros

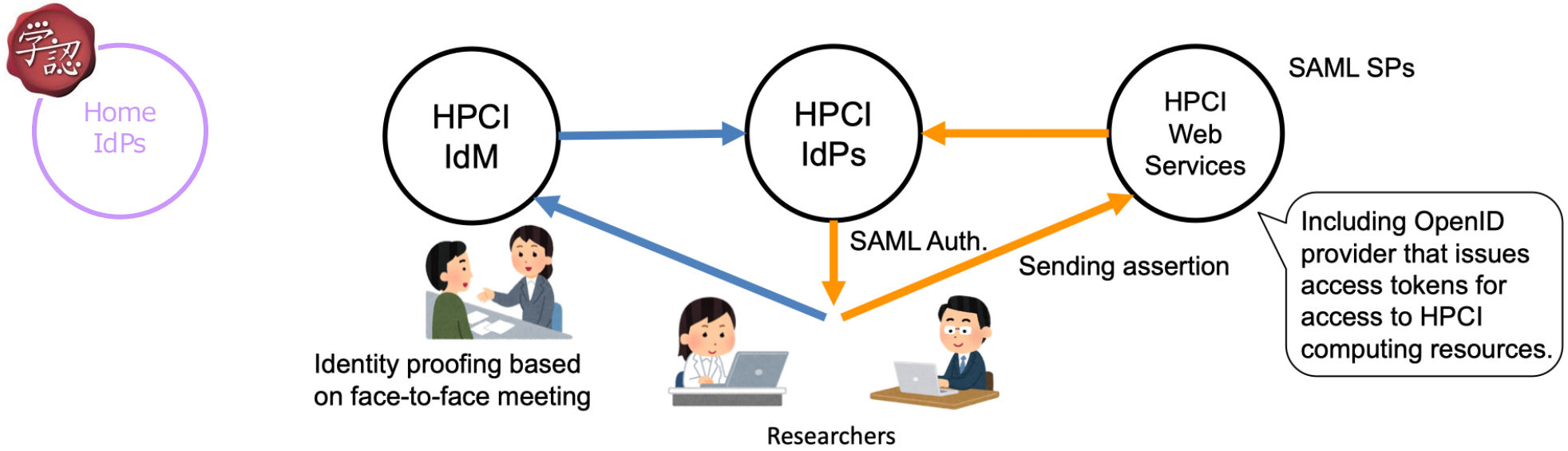
Work in Progress - HPCI

- Provisioning an end-user access environment
  - including the token-based client software packages
  - released as a container image and Homebrew packages
- Authenticator AL enhancement
  - introducing Passkey as authenticator to HPCI OpenID provider (Keycloak)
  - establishing user-self authenticator initialization procedure with recovery codes
- Shibboleth metadata registration practice
  - replacing public X.509 certificate in metadata with private

- New system supporting access control translation, attribute service and authrization

What HPCI Should Do

- We want to be able to use GakuNin to authenticate HPCI users.



- HPCI needs to delegate authentication to GakuNin.
  - Delegation to GakuNin cannot be done by simply replacing the HPCI IdP with a GakuNin IdP. Why?

What HPCI Should Do (Cont'd)

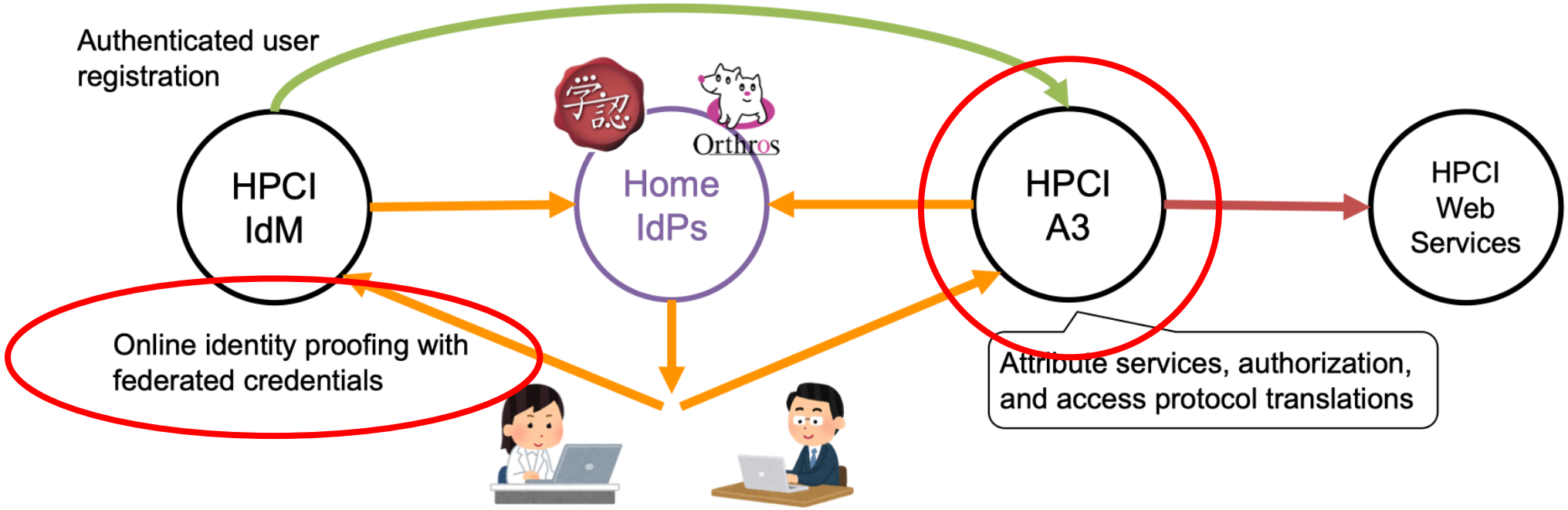
- The HPCI IdP effectively also holds HPCI authorization information.
  - While the HPCI IdP only has HPCI users, the GakuNin (home) IdP has users other than HPCI s.
  - For this reason, the authorization criteria are simple for the HPCI SP.

- If HPCI authentication is delegated to the GakuNin IdP, we must consider how to handle HPCI authorization and access control.

HPCI IdP → Home IdP + HPCI Attribute Services

New HPCI AAI

- Integration of GakuNin IdPs with HPCI AAI:
- Online identity proofing with federated credentials,
  - Sign up with federated credentials
- Attribute services, authorization and access protocol translations discussed in AARC Blueprint Architecture.



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

Orthros acts an intermediary between HPCI IdM and external IdM.

gBizID

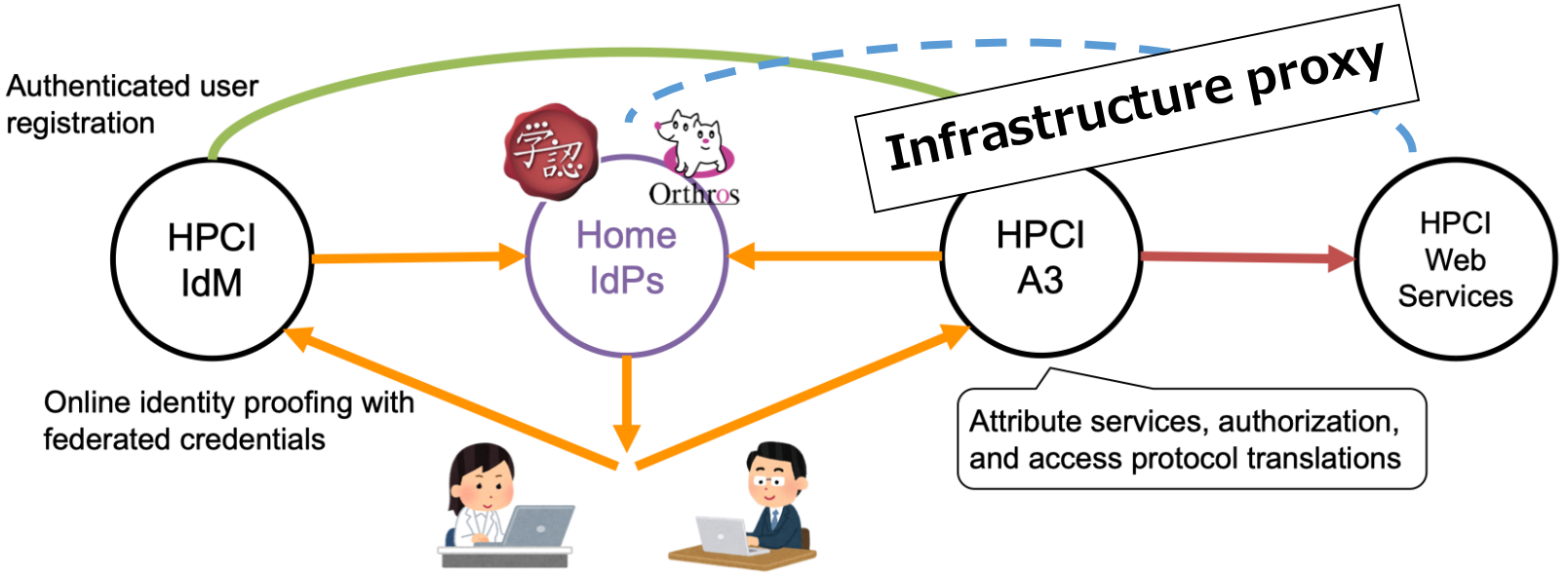
xID (JPKI)

ORCiD

IdM A, IdM B, …

HPCI A3 (tentative name)

- HPCI A3 supports attribute services, authorization and access protocol translations.
- As HPCI A3 mediates between the Home IdP and the HPCI SP, the HPCI SP does not need to connect to any Home IdP, and authorization control can continue to be performed relatively simply.



Summary

- HPCI must integrate Home IdPs with HPCI AAI.
- Federated Sign up service was designed.
- A new system (infrastructure proxy) should be needed and can provide the following features; attribute services, authorization and access protocol translations.

- Future Plan
  - FY2026: implement the federated sign up service and design a new system (HPCI A3)
  - FY2027: implement the prototype of new system and evaluate it
  - FY2028: build the new system in HPCI and start in production level operation