APGrid PMA Update

Eisaku Sakane

National Institute of Informatics

30th TAGPMA Meeting

October 9, 2024

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*
CNIC CA	*CN*	*Aug. 2015*	*1*		CARSI (480+ entities)	
SDG CA	*CN*	*Aug. 2015*	*0*			
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 (8)	*AIST CA (JP), APAC CA (AU), MYIFAM CA (MY), NCHC CA (TW), NECTEC CA (TH), NAREGI CA (JP), PRAGMA CA (US), HKU CA (CN)*					

From Previous APGridPMA Meeting in March

- Moving towards new AAI according to user communities or resource federation infrastructure
  - HPCI Japan: start operation on a token-based AAI based on OAuth-SSH, KeyCloak, OIDC agent and JWT-agent, and also considering cooperation with GakuNin
  - 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 considering efficient operation on communication tools such as webpage, mailing list.

Future meeting

- 34th APGridPMA Meeting – will be virtual meeting in October
  - APAN 58 held in Islamabad, Pakistan, August 26 - 30, 2024.
- 35th APGridPMA Meeting
  - will be collocated with ISGC 2025.
  - APAN 59 will hold in Yokohama, Japan, March 3-7, 2025.

- 63rd EUGridPMA Meeting
  - will hold in CERN, February 5-7, 2024.
- 31st TAGPMA Meeting

Sign-up with federated credentials in HPCI

Collaboration with GakuNin and international IAM federations

Identity proofing – Old and new challenges

- HPCI identity management (IdM) system currently vets user identity based on a face-to-face meeting with photo-ID presentation. Such identity proofing process is still a heavy burden on users and also the HPCI IdM, because there is a diversity in the format of the photo-ID, in addition, the genuineness of the photo-ID is not easily confirmed by HPCI personnel.
- A solution to the above problem is for the HPCI IdM to not perform identity proofing itself, but to delegate it to external trusted IdMs or federations. Issues to realize such delegation are as follows:
  - What is an external IdM for industrial researchers?
    - Note that HPCI users are not only in academia but also industry.
  - Do the IdMs or federations meet the IAL imposed by the HPCI IdM?

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 receives 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, …

Identity proofing based on *genuine* MICS

- HPCI CA is a MICS-based CA.
  - External IdMs are IdPs operated by supercomputer centers in Japan.
  - Protocol between IdM and HPCI RA uses SAML.

- HPCI IdM will be a MICS-based IdM.
  - HPCI IdM will delegate identity proofing to *external* trusted IdM or federations; GakuNin IdP, public IdM, eduGAIN.
  - Protocol between HPCI IdM and external IdMs will be SAML.

Future plans

- We are considering a design and implementation of new sign-up with federated credential service.
- We plan to
  - make a proto-type experimentally,
  - define a SAML profile of federated credential and,
  - do a pilot operation next Spring