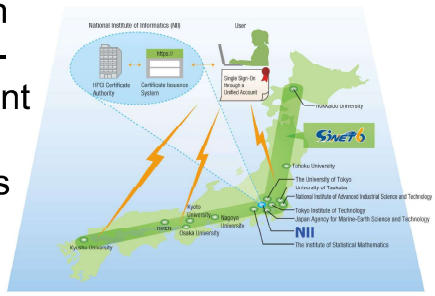
Practice of Efficient Identity Proofing in HPCI Sign-up with Federated Credentials

Identity Proofing – Old and New Challenges

HPCI is a distributed high performance computing infrastructure in Japan, composed of supercomputers and large file storages connected by the high speed network SINET. 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.

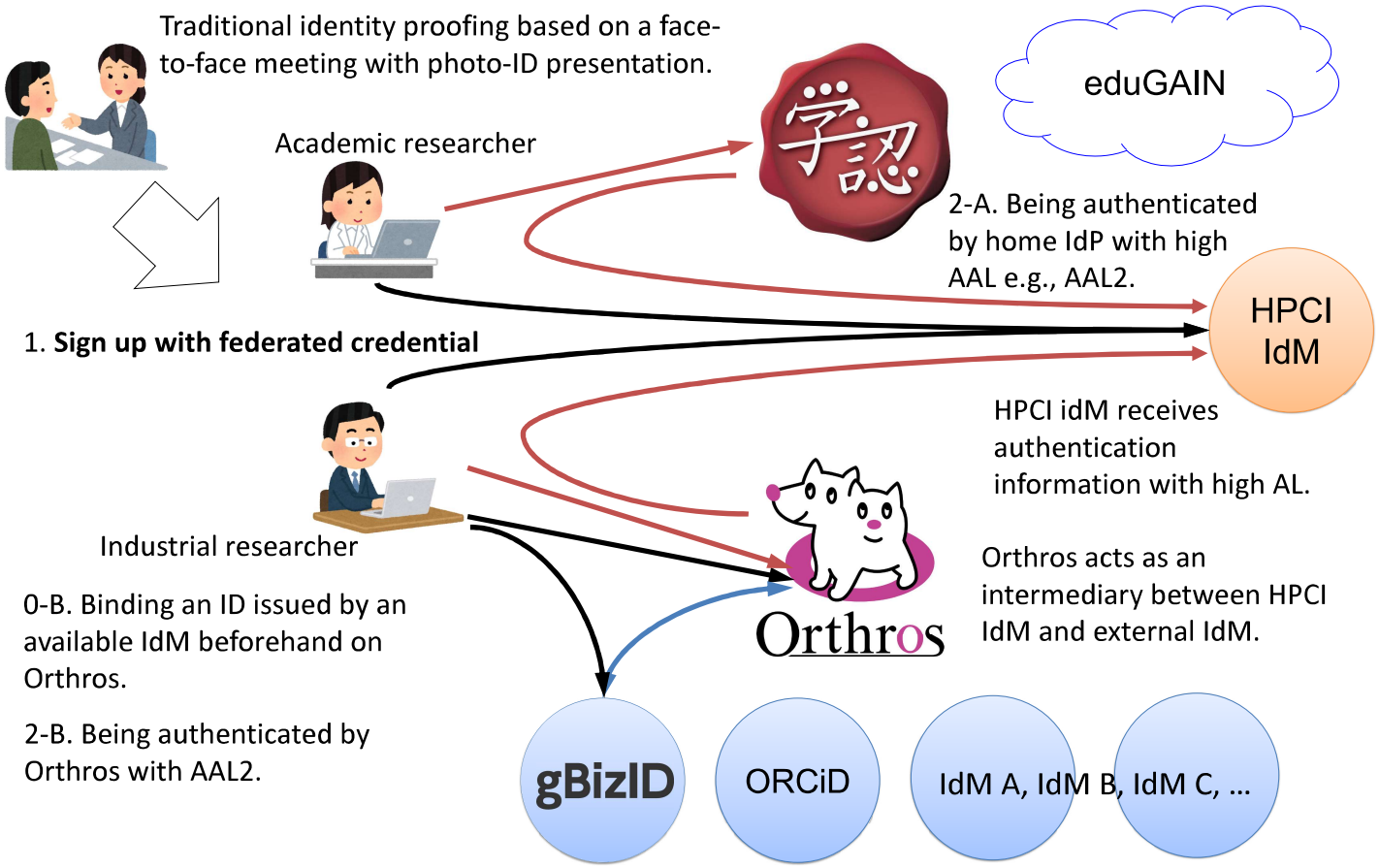


Basic Idea and Issues

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?

IAL: Identity assurance level
AAL: Authenticator assurance level



GakuNin and Next Generation Trust Framework

GakuNin is an academic identity and access management federation in Japan and provides the following for next-generation authentication federation:

- New trust framework that defines GakuNin assurance level: IAL2 and AAL2,
- An authentication proxy service, called “Orthros”.