A Study of Credential Integration Model in Academic Research Federation Supporting a Wide Variety of Services

International Symposium Grids & Clouds 2018
20th – 23rd March 2018
Academia Sinica, Taipei, Taiwan

Eisaku SAKANE, Takeshi NISHIMURA, Kento Aida, Motonori NAKAMURA

National Institute of Informatics, Japan

NII
National Institute of Informatics

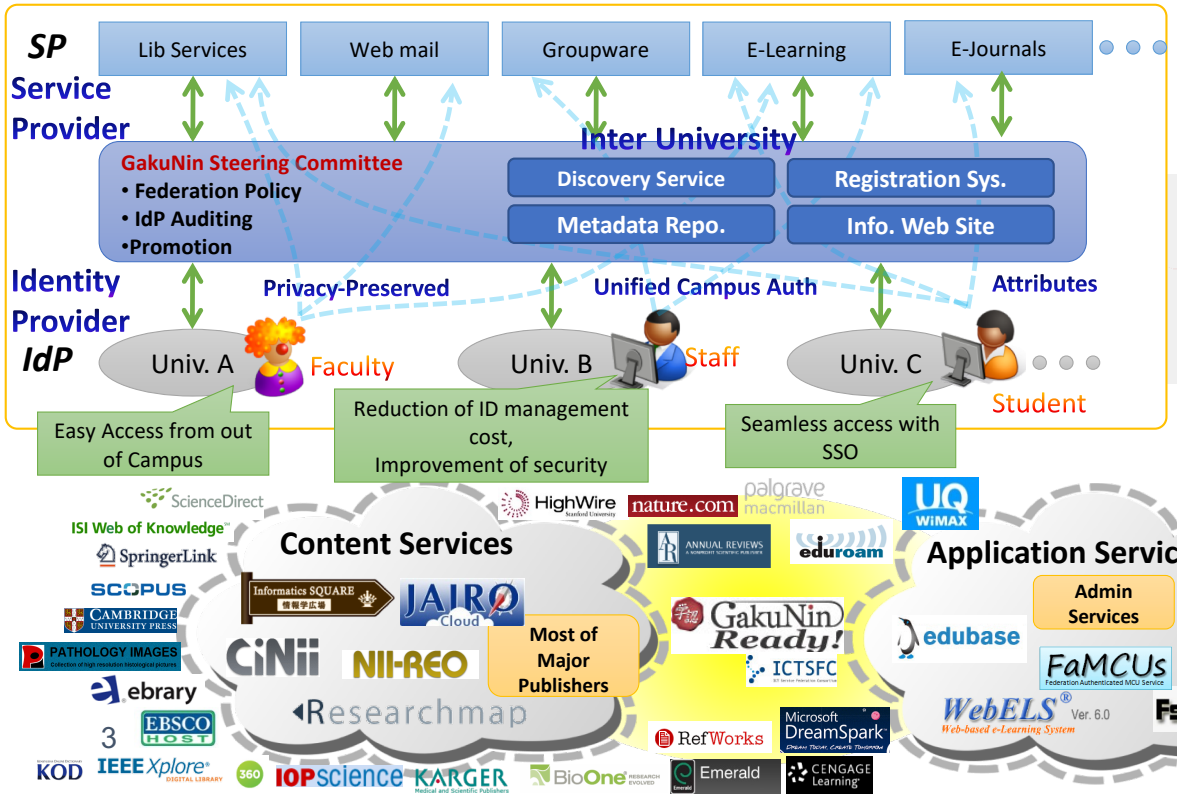
Outline

- Introduction to GakuNin and HPCI
- Issues
- Consideration of credential integration
- Related works
- Summary

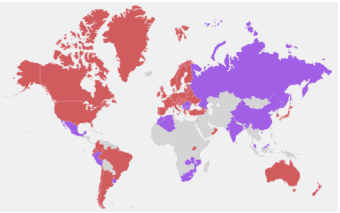
National Institute of Informatics

GakuNin An Academic Identity Federation in Japan

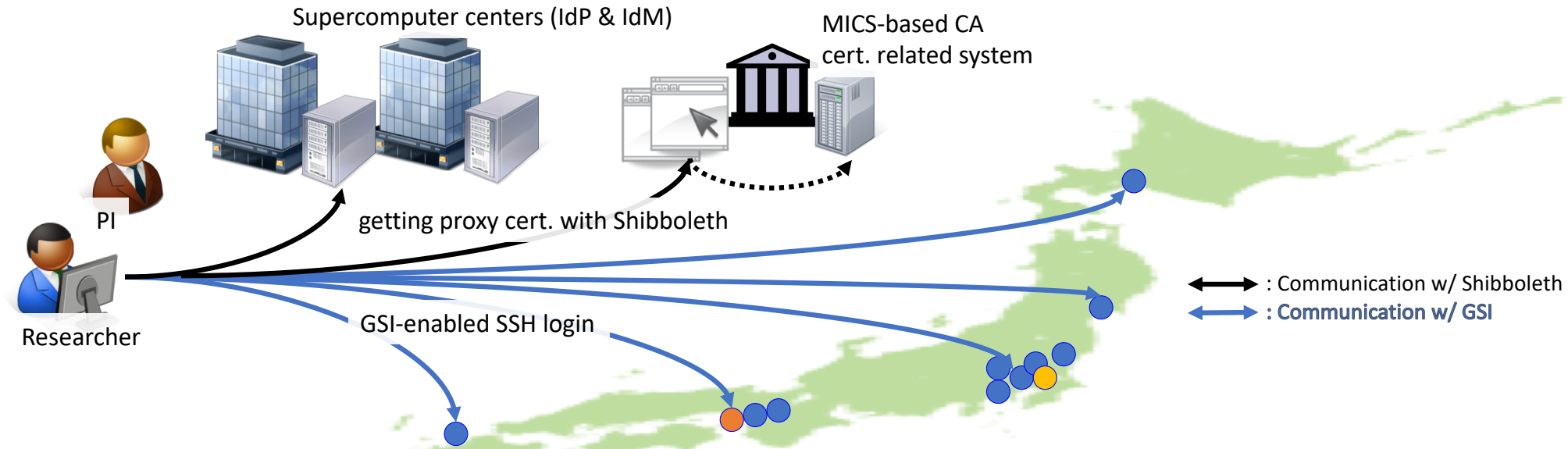
- Build up new ICT infrastructure to support R&E based on SSO technologies
- Provides trust framework (technologies, policies and assessment)
- Offers value added services (academic discount, etc.) by collaboration with commercial
- Improves usability and security with continuous R&D (including multifactor/cert. auth.)



Academic Federations have been established per country basis



HPCI: High Performance Computing Infrastructure



HPCI authentication system features include:

- Single user ID and multiple accounts called HPCI-ID, HPCI and local accounts
  - HPCI accounts are managed by identity providers.
- A hierarchical initial identity vetting system based on face-to-face meetings with photo-IDs
- Two kinds of credentials for services in HPCI:
  - Shibboleth assertion for Web services: certificate issuance, CMS, etc.
  - GSI proxy certificate for access to supercomputers and storages

National Institute of Informatics

Difference between HPCI and Gakunin

- What is difference between HPCI and Gakunin?
- IdP in HPCI is different from IdP in Gakunin:
  - Gakunin IdP is managed by an academic institution and covers all constituent members of its academic institution.
  - HPCI IdP is managed by a supercomputer center (university or institute) and covers only HPCI users who are not only academic researchers but also industrial ones.
- Why did HPCI build dedicated IdPs ?
  - HPCI IdP has to satisfy a strict LoA imposing identity vetting via a face-to-face meeting.
  - HPCI IdP needs to cover industrial researchers.
  - HPCI is not a common service to all constituent members of an academic institution like e-Journals.
- Only if HPCI users are academic ones, at least HPCI and Gakunin IdPs should be integrated.

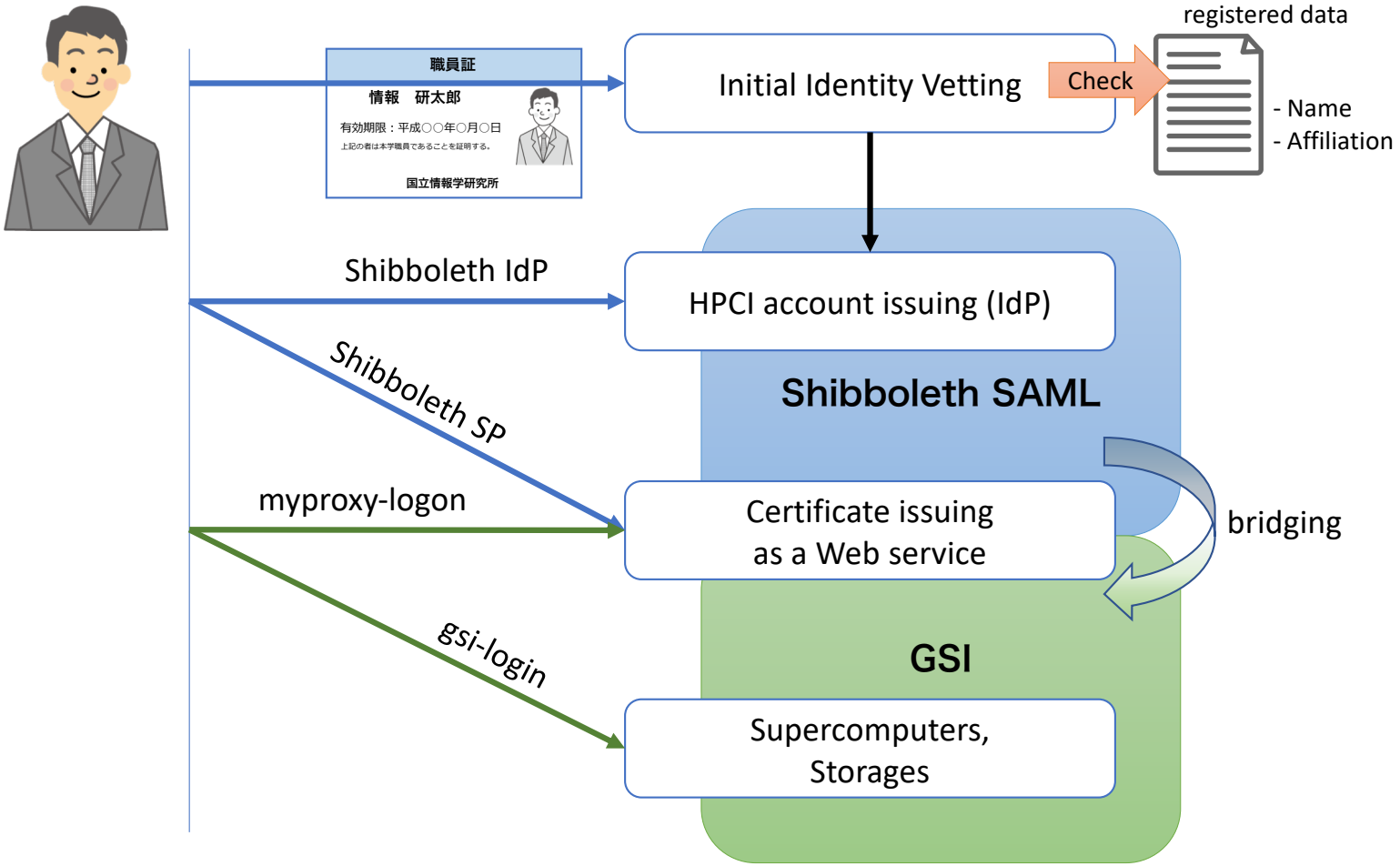
NII
National Institute of Informatics

Guiding question

- How do we integrate HPCI IdP and GakuNin IdP in order that academic users only need to manage one credential?
- We select GakuNin IdP as primary identity provider because GakuNin IdP is operated by home organization that user belongs to.
- How do we apply a credential issued by GakuNin IdP to HPCI services?

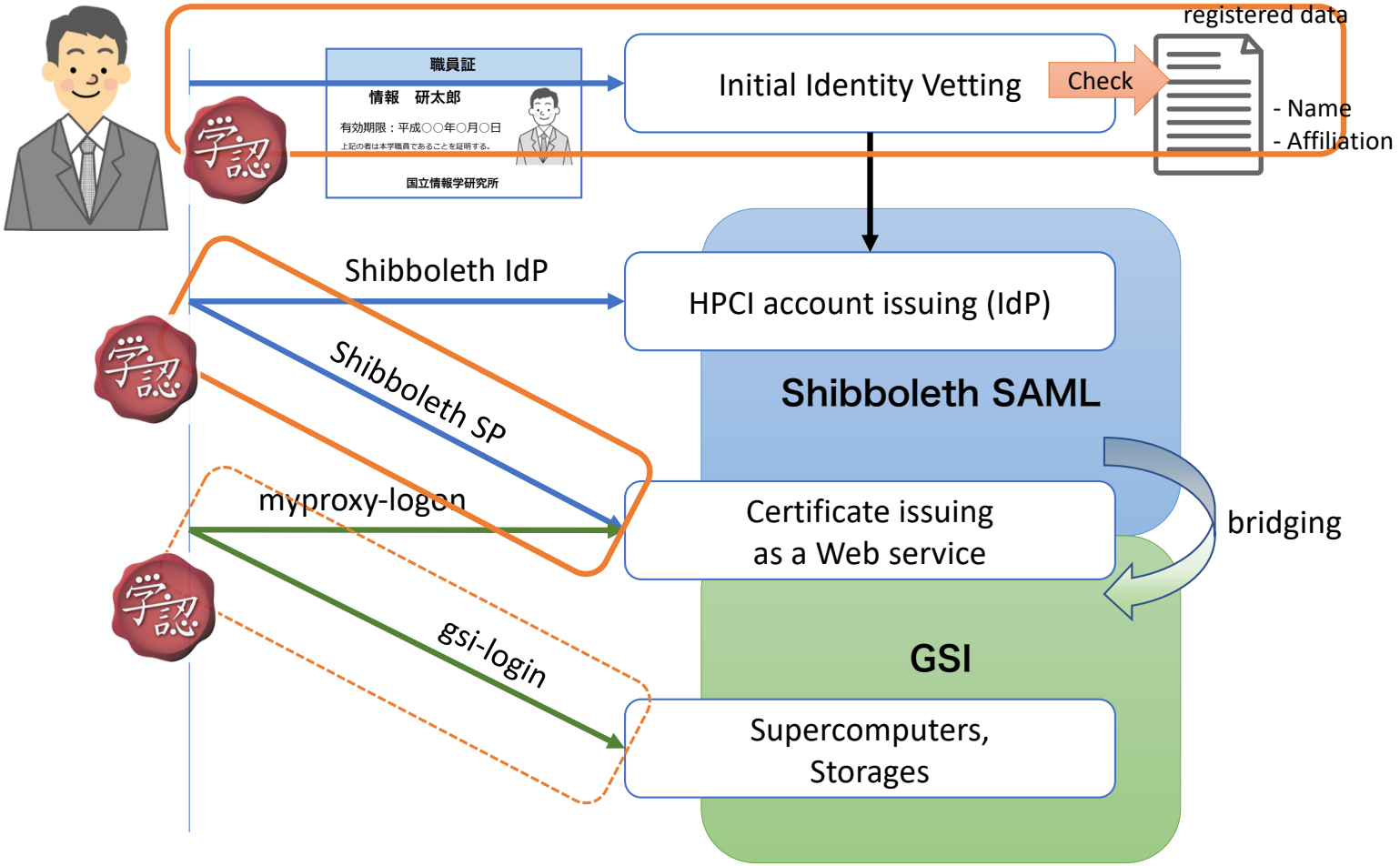
National Institute of Informatics

Authentication flow in HPCI



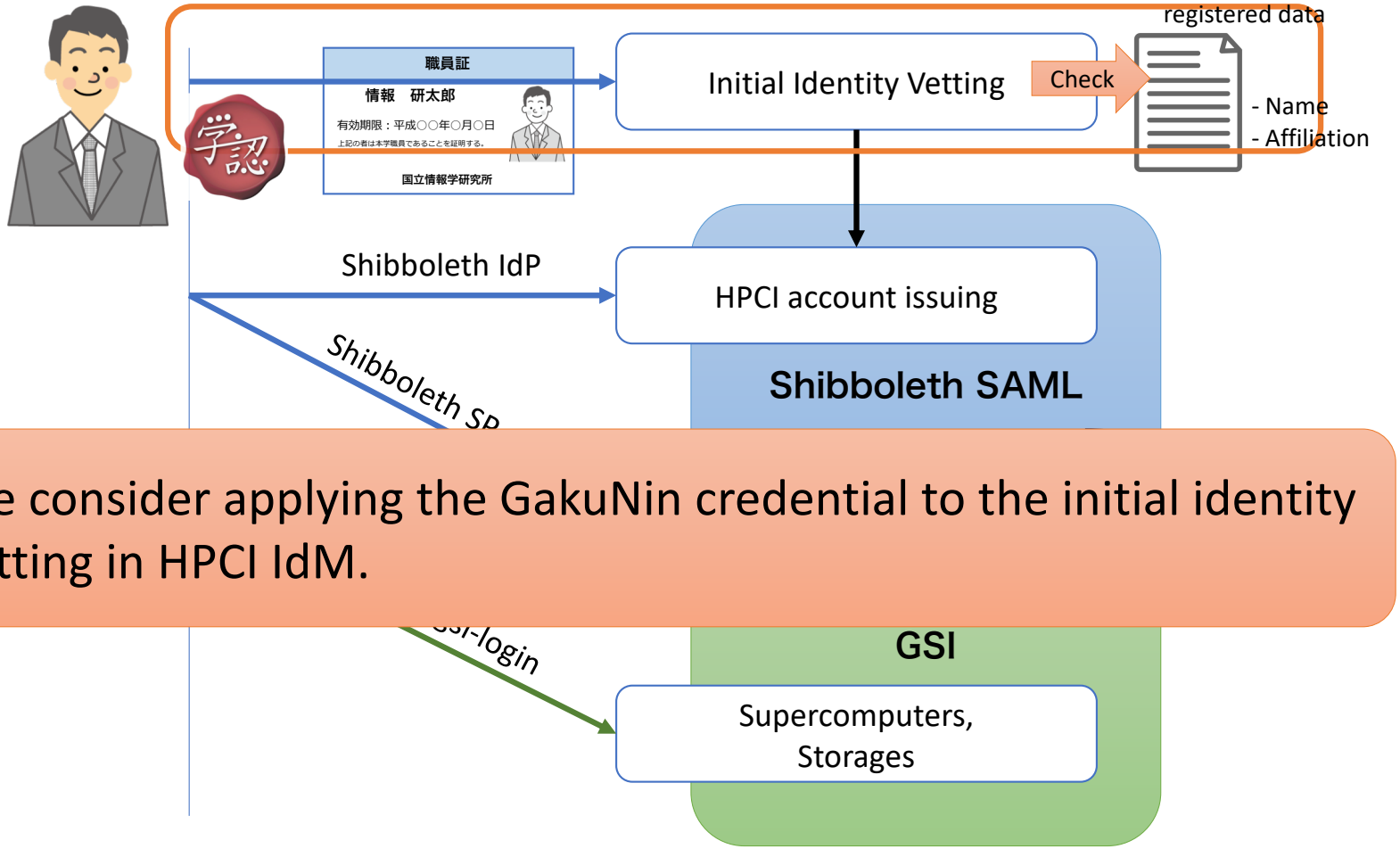
National Institute of Informatics

Possibilities for GakuNin credential application



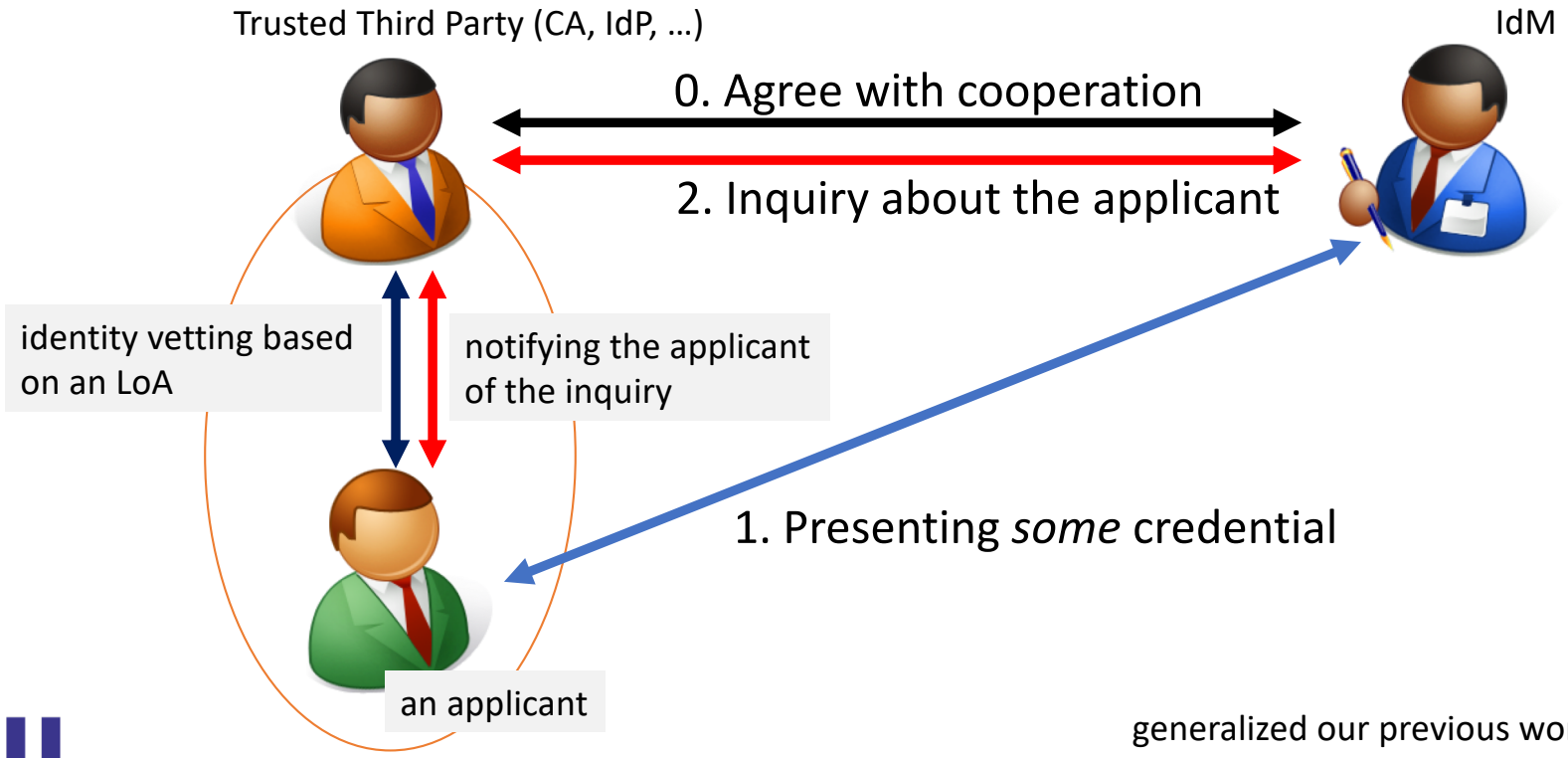
National Institute of Informatics

Possibilities for GakuNin credential application



National Institute of Informatics

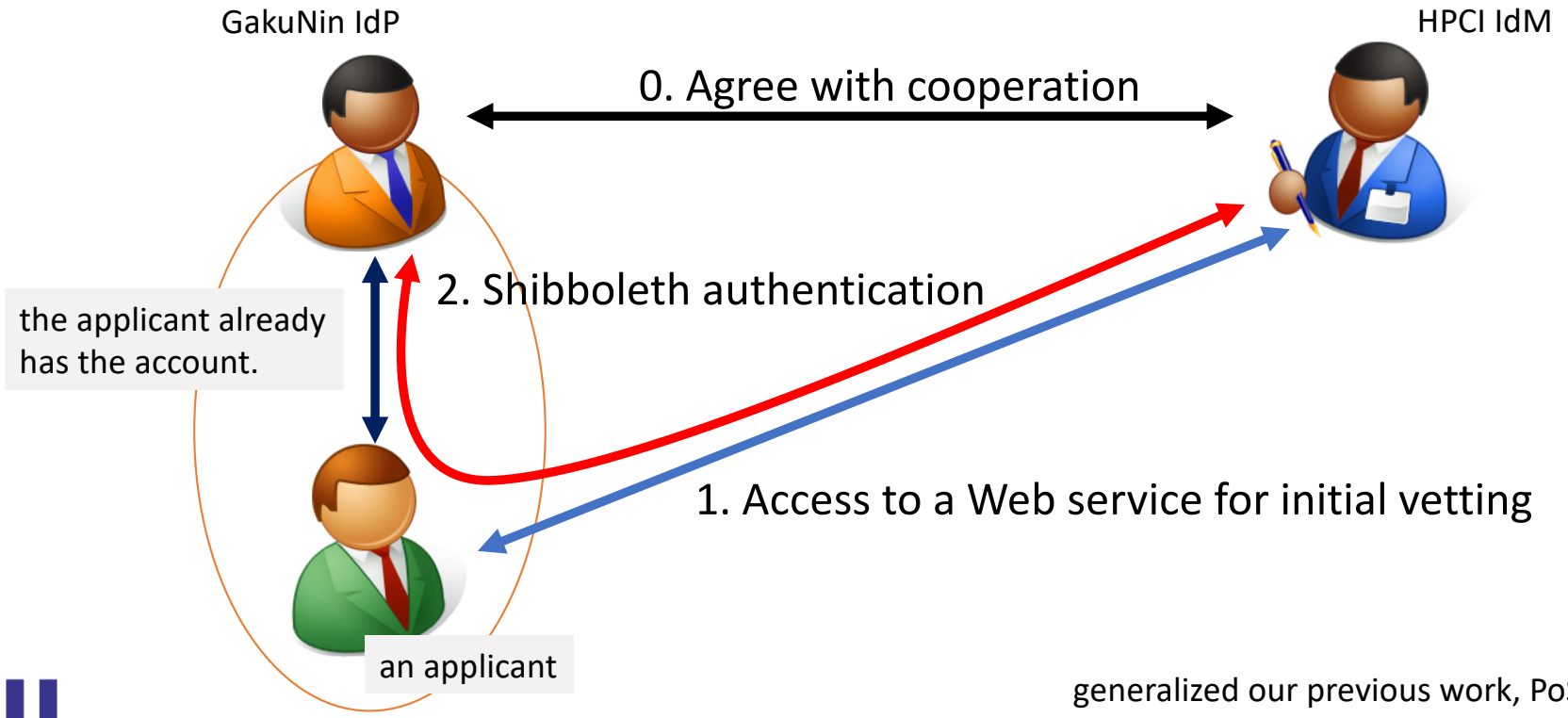
Basic idea:
Initial identity vetting with external credential



generalized our previous work, PoS(ISGC2017)009

National Institute of Informatics

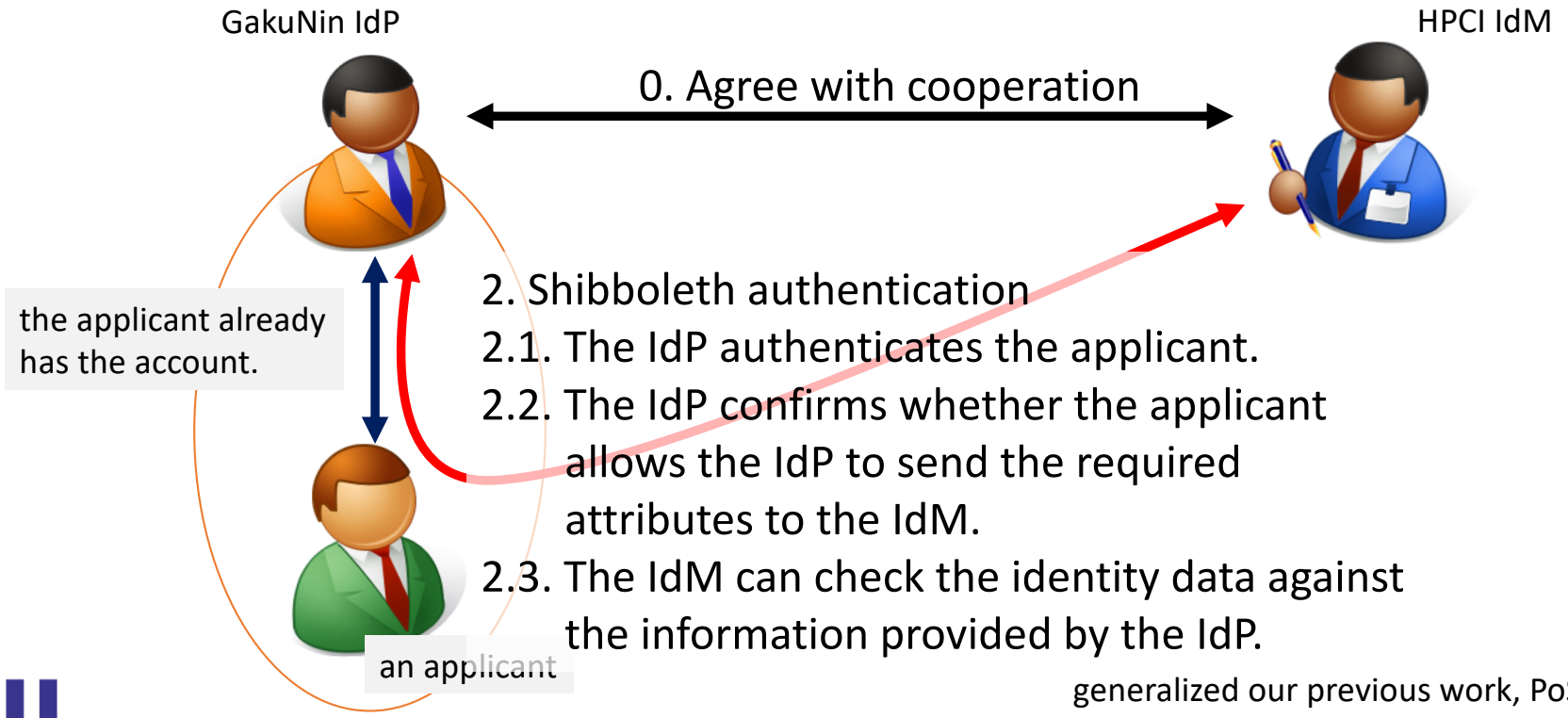
Initial identity vetting with credential issued by GakuNin IdP



generalized our previous work, PoS(ISGC2017)009

National Institute of Informatics

Initial identity vetting with credential issued by GakuNin IdP (Cont'd)



generalized our previous work, PoS(ISGC2017)009

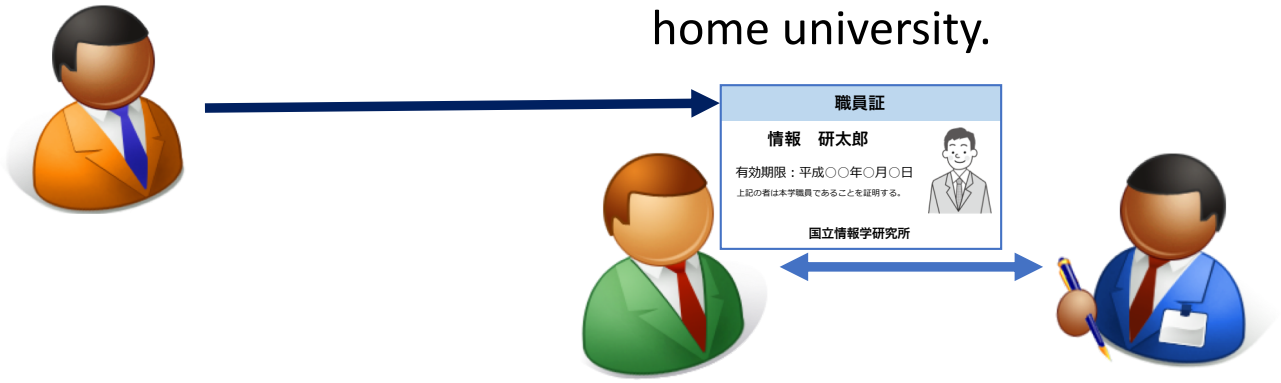
National Institute of Informatics

Discussion

- Do the proposed procedure provide the same level of assurance?
  - HPCI IdM must vet the identity of user based on a face-to-face meeting with a photo-ID.

GakuNin IdP (University)

The user present her/his photo-ID issued by home university.



The proposed procedure can intuitively be regarded the same as the initial identity vetting based on a face-to-face meeting.

National Institute of Informatics

Discussion (Cont'd)

- Another possibility of GakuNin crendential application.
  - Due to the end of GSI support, HPCI needs to reconsider the authentication and authorization system in HPCI to access to supercomputers and storages.
  - Credential for Web services may be changed by new AA system in HPCI.
  - However the GakuNin credential application to initial identity vetting will remain almost unchanged.

Related Works

- AARC Blueprint Architecture
- *Snctfi* from AARC's policy work

National Institute of Informatics

Summary

- We introduced authentication infrastructures, GakuNin and HPCI.
- We proposed a credential integration model in which GakuNin credential (SAML assertion) can be used to the initial identity vetting in HPCI.

- Our approach can be extended to more general case.
- Our approach should be corroborated with a trust framework.

National Institute of Informatics