International Symposium on Grids and Clouds (ISGC) 2024
25-29 March 2024
Academia Sinica, Taipei, Taiwan

A Study of Credential Policy and Credential Practice Statement for an Authentication Proxy Service

Eisaku Sakane, Motonori Nakamura, Akinori Mizumoto

National Institute of Informatics
Japan

© 2024 National Institute of Informatics

Background

- We developed an authentication proxy service and started pilot operation from October 2023.
- Toward operation in production level, we need a policy for credential and operation, namely, credential policy and credential practice statement (CrP/CrPS).

- In this presentation, we make a report on the study contents of CrP/CrPS establishment for the authentication proxy service.

Authentication Proxy Service: Orthros

- Purposes:
  - guarantees user's identity and authenticator to collaborating service providers (SPs),
  - enhances assurance level for identity and authenticator by
  - binding the other independent identity providers (IdPs) or
  - aggregating attributes from IdPs

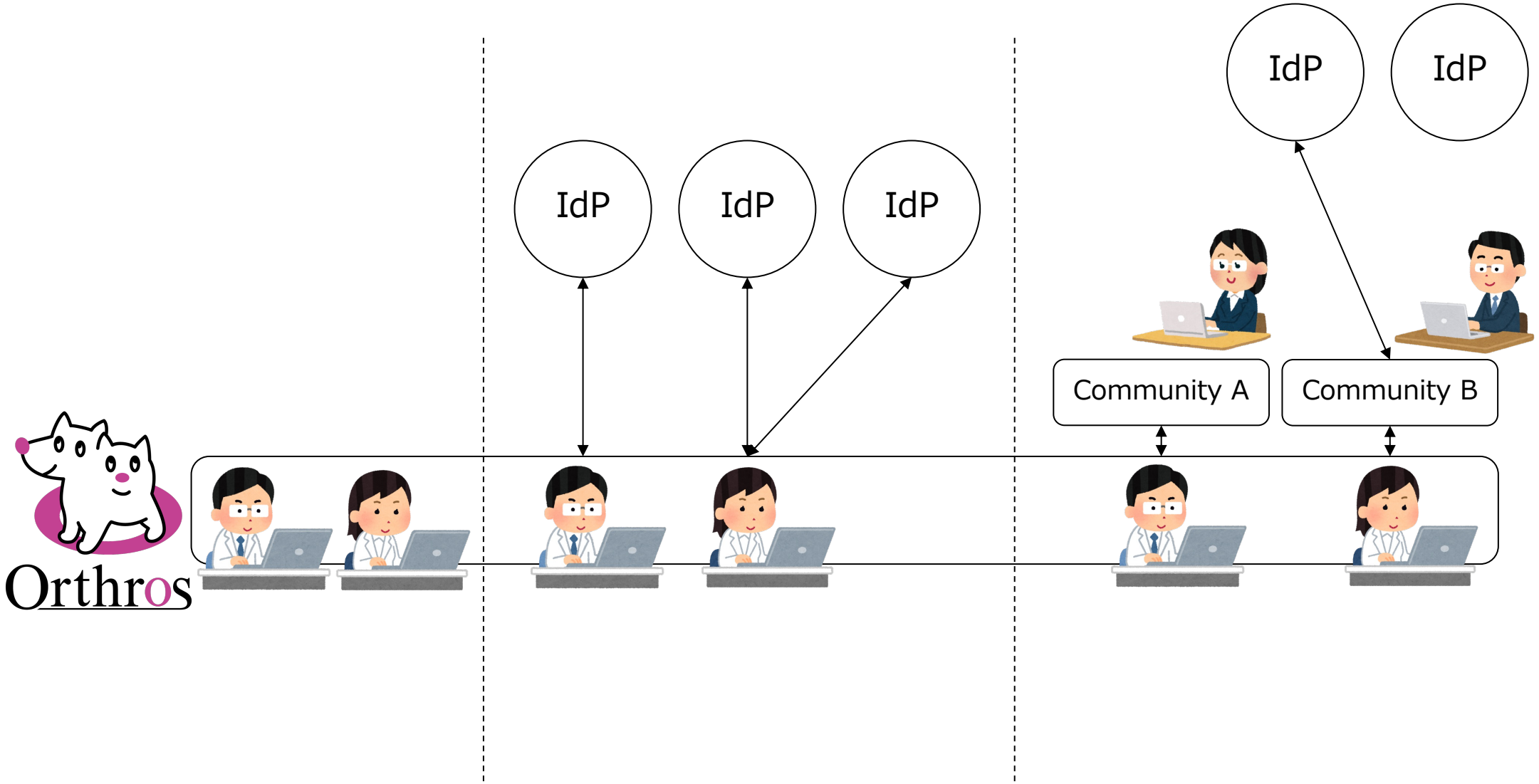
- Fundamental user attributes
  - fundamental private information (full name, postal address, date of birth, sex),
  - home organization name (e.g. university, institution, company, etc),
  - The others that home organization or binding IdP can assure

- What assurance depends on
  - procedure for identity proofing carried out by Orthros itself,
  - the other IdP bound by user self-service,
  - community
    - the word "community" means a department of a university/institution, research community, etc

- Attribute for authorization and access control
  - no handling except for the above fundamental attributes

  - We discuss separately attribute management for authorization and access control.
    - Role-based, Attribute-based AuthZ/AC

What assurance depends on



Basic Idea

- RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

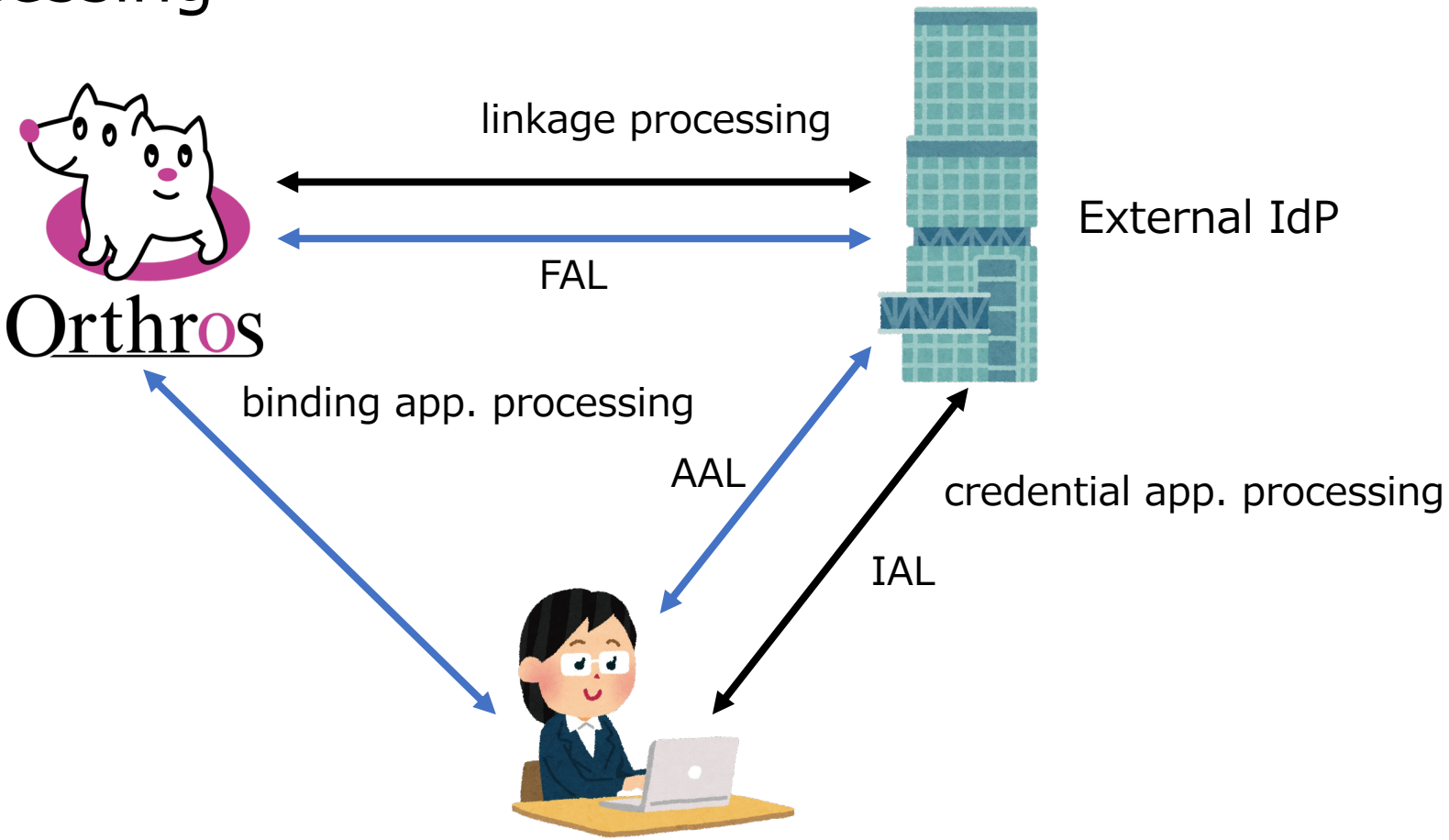
- We extend (replace?)
  - X.509 PKI certificate policy → credential policy
  - certification practices → credential practices

CrP/CrPS document structure – RFC3647-based

1. Introduction
   - 1.X. Participants
     including external independent IdP
2. Publication and Repository Responsibilities
3. Identification and Authentication
   - 3.X. Initial Identity Validation
     - 3.X.1. Service provider
     - 3.X.2. external independent identity provider or attribute provider
     - 3.X.3. End user
4. Credential Life-Cycle Operational Requirements
   - 4.X. Credential Application
   - …
5. Facility, Management, and Operational Controls
6. Technical Security Controls
7. Credential Profiles
8. Compliance Audit and Other Assessment
9. Other Business and Legal Matters

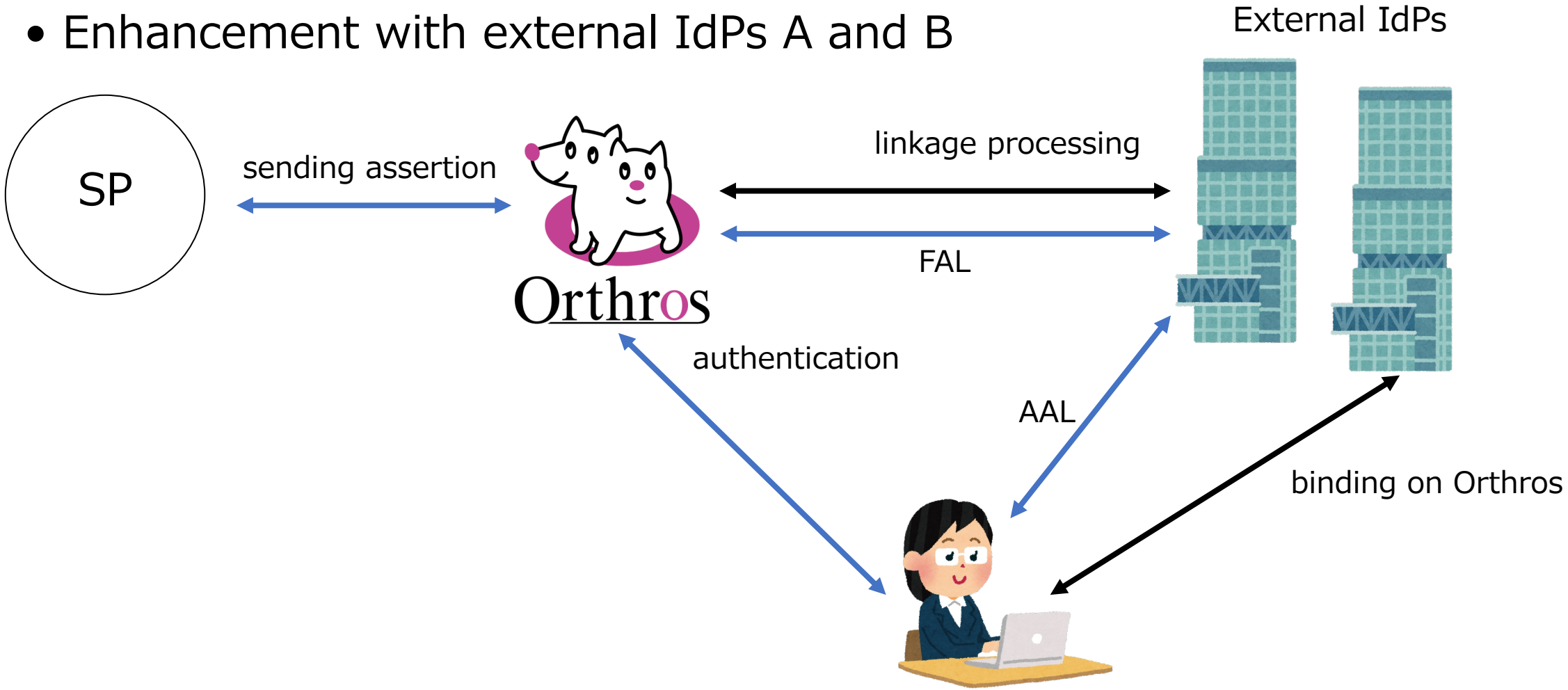
Points

- External IdP linkage processing
  - evaluation of IAL/AAL/FAL
- Binding processing



Points (cont'd)

- Refreshment of attributes aggregated from IdPs
  - Authentication with external IdP A
  - Enhancement with external IdPs A and B



Features of CrP/CrPS for Orthros

- CrP/CrPS for Orthros provides relying parties the information to confirm the assurance level of the following included in assertion:
  - identity proofing
  - authenticator
  - strength or freshness of attributes
  - freshness of bound account

- External IdP binding processing
  - described in “Attributes Life-Cycle Operational Requirements”
  - what user can bind
  - how Orthros evaluate the IAL/AAL/FAL of external IdPs
- Community-managed binding processing
  - user can obtain “Organization” attribute concerned with the community.
  - Community shall guarantee user’s identity.
  - Assurance depends on the policy managed by the community.

Summary

- We introduced an authentication proxy service, Orthros.
  - pilot operation since October 2023.
- Establishing the CrP/CrPS for Orthros, we explained the following:
  - RFC 3647-based document structure
  - points of CrP/CrPS
- We are still establishing the CrP/CrPS for Orthros, but we plan to publish the CrP/CrPS in the near future.