UPKI Federation
-2009 Pilot Operation-

Yamaji, K., Kataoka, T., Nishimura, T., Shimaoka, M., Nakamura, M., Sonehara, N. and Okabe, Y.

Japan National Institute of Informatics

Contents

- Federation
  - 2008 Feasibility Study
  - 2009 Pilot Operation

- Experimental Application
  - Institutional IdP and VO IdP

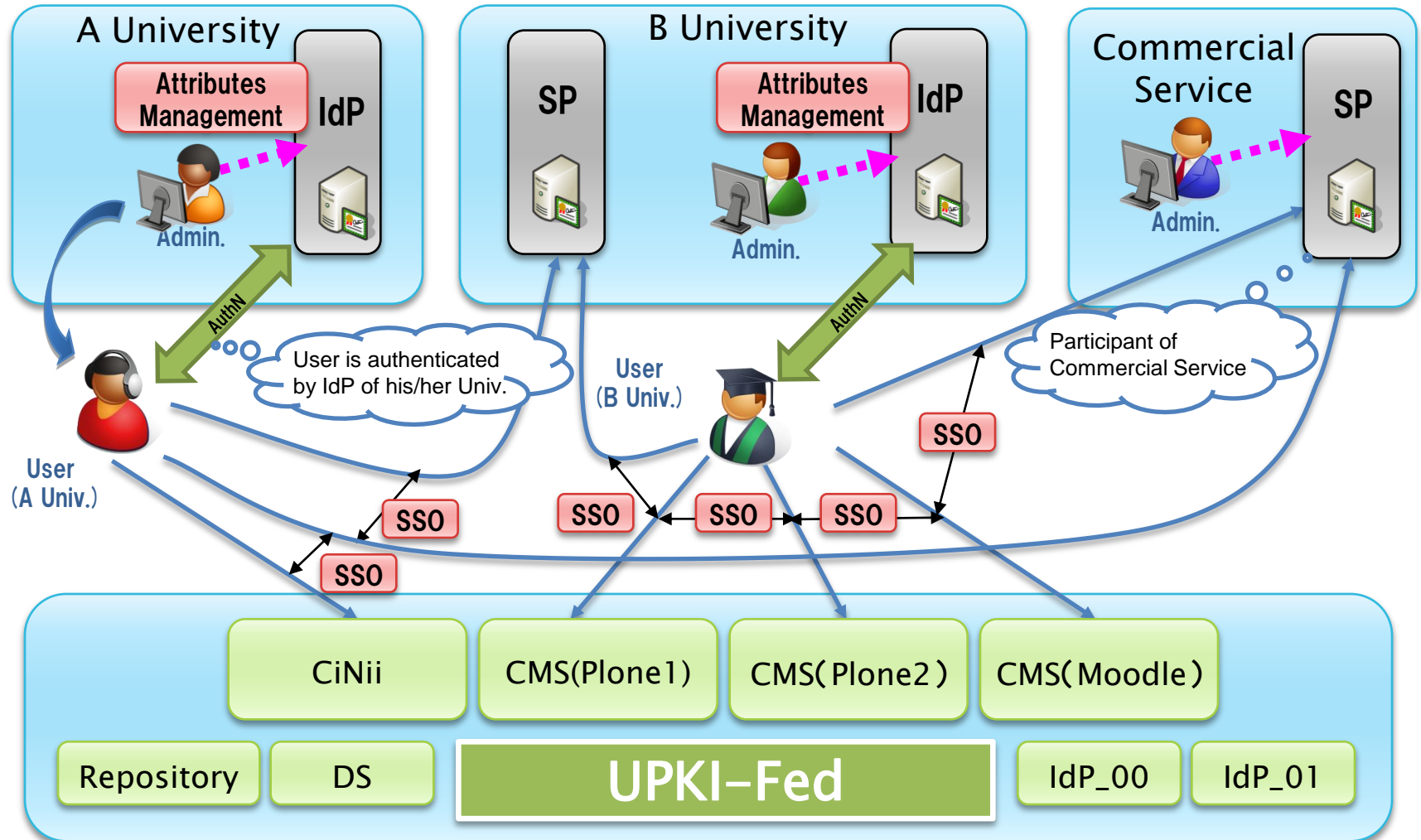# 2008 Feasibility Study: What we did

▸ Preparation
  ▸ Setup documents
  ▸ VMWare Image for IdP
  ▸ test-bed including DS, repository (see next slide)

▸ Explanatory meeting
  ▸ Ask to attend both IT people and librarians from each institutes

▸ Development
  ▸ setup test SP
  ▸ support institutes to setup IdP, SP
  ▸ metadata distribution
  ▸ feasibility test instruction
  ▸ share information by wiki, mailing-list, mail magazine

▸ Participants meeting
  ▸ report status from all institutions

▸ Preparation for next step
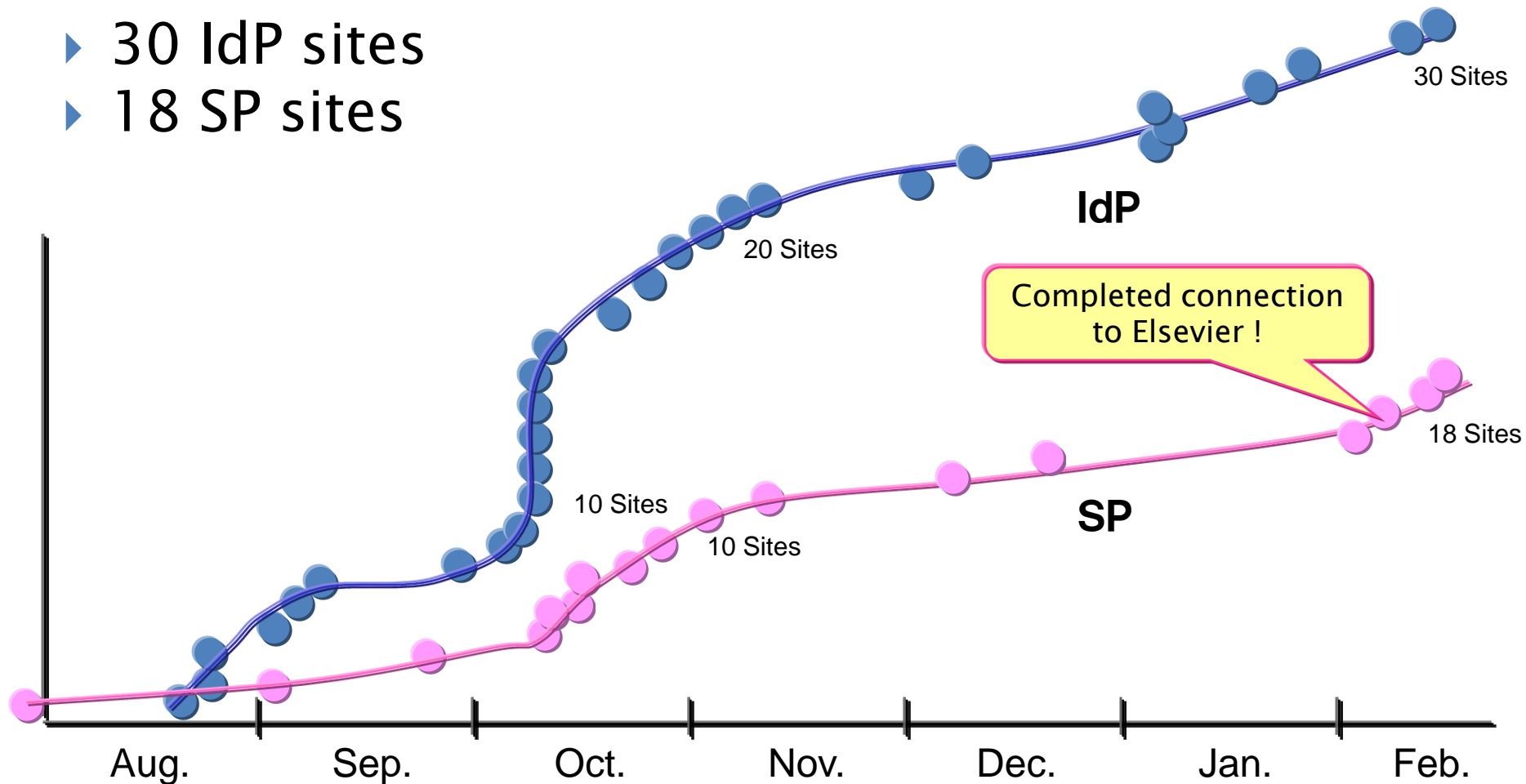 ▸ discussion and development of policy for pilot operation
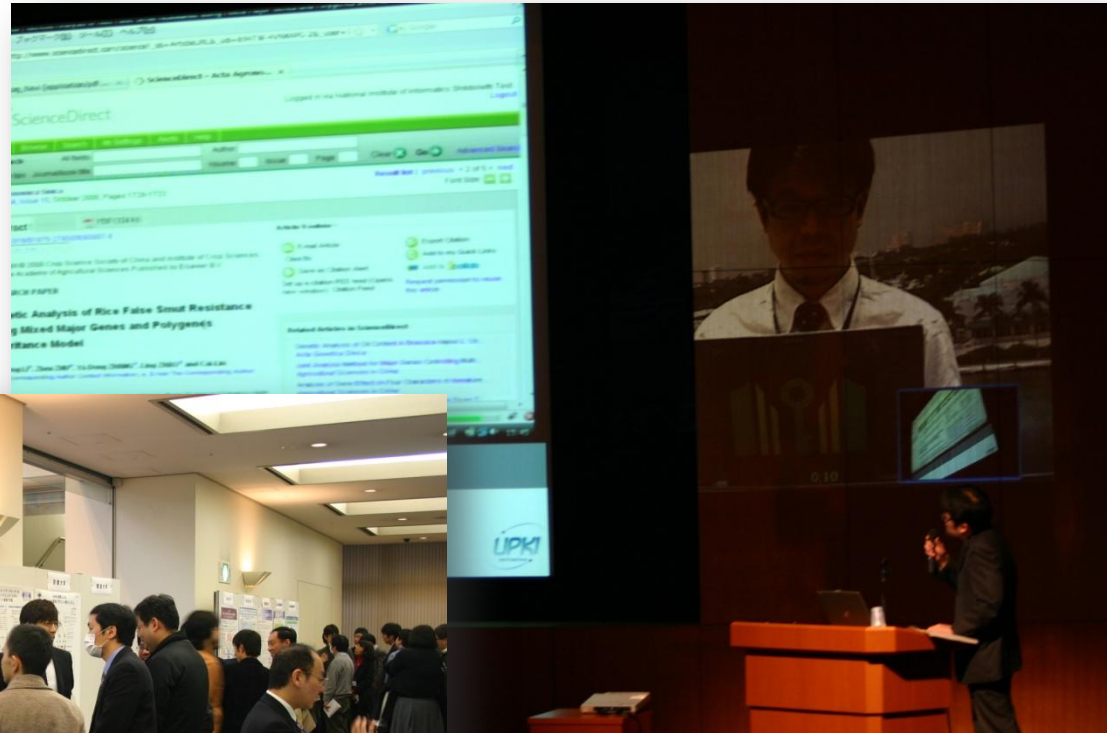
▸

2008 Feasibility Study: System Environment

2008 Feasibility Study: Participants

▸ 27 Institutions
▸ 30 IdP sites
▸ 18 SP sites

2008 Feasibility Study:
UPKI Symposium (February 23, 2009)

2009 Pilot Operation

We are HERE
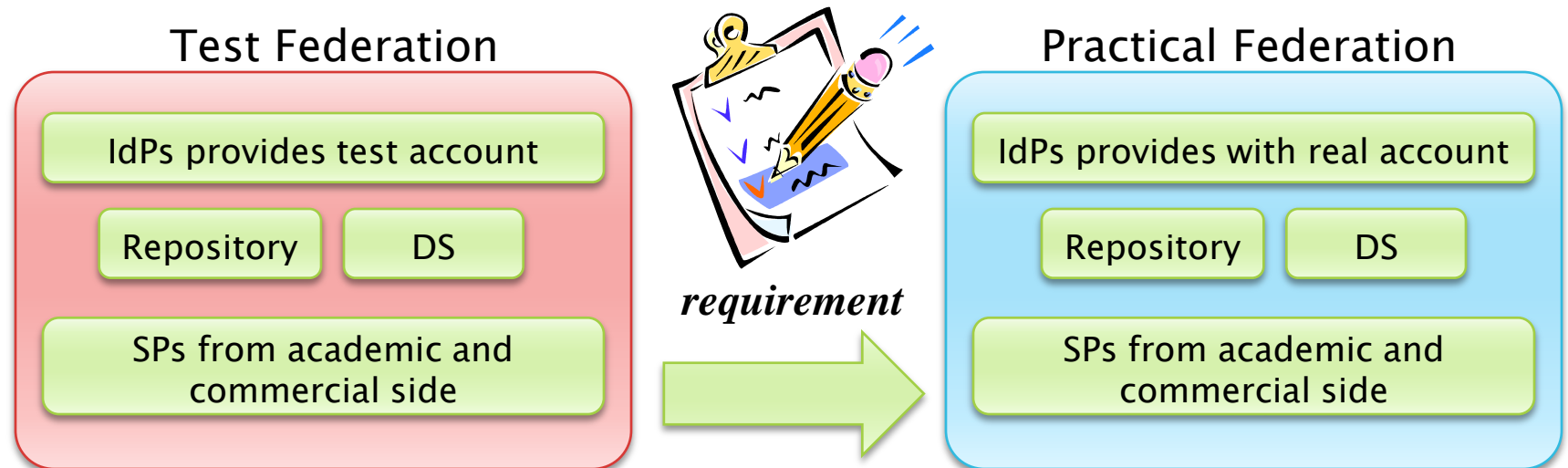
FY2008	FY2009	FY2010
Feasibility Study	Pilot Operation	Practical Operation
Connection using test account	Connection using real account under campus policies	Practical operation with real account and service
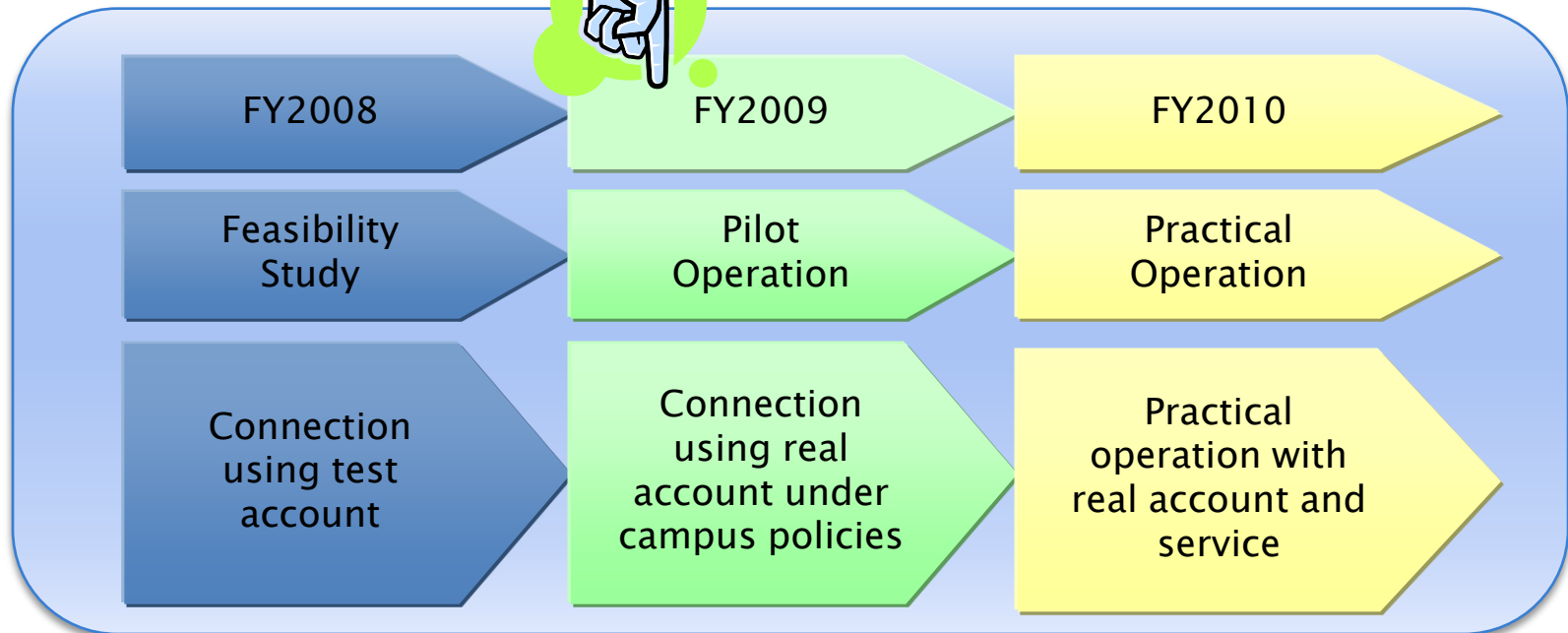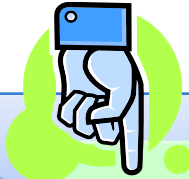
2009 Pilot Operation:
What we do

▸ Documents
  ▸ Federation Policy, System Specification
▸ Event and Training
  ▸ IdP and SP implementation
  ▸ Discussion among IT people and Librarians
▸ Recruiting
  ▸ IdP: University, College
  ▸ SP: Major Publishers, Domestic Services

Test Federation

IdPs provides test account

Repository

DS

SPs from academic and commercial side

requirement

Practical Federation

IdPs provides with real account

Repository

DS

SPs from academic and commercial side

2009 Pilot Operation:
16 Attributes

Name	OIDs
mail	0.9.2342.19200300.100.1.3
sn	2.5.4.4
o	2.5.4.10
ou	2.5.4.11
givenName	2.5.4.42
displayName	2.16.840.1.113730.3.1.241

Name	eduPerson OIDs
eduPersonAffiliation	1.3.6.1.4.1.5923.1.1.1.1
eduPersonPrincipalName	1.3.6.1.4.1.5923.1.1.1.6
eduPersonEntitlement	1.3.6.1.4.1.5923.1.1.1.7
eduPersonScopedAffiliation	1.3.6.1.4.1.5923.1.1.1.9
eduPersonTargetedID	1.3.6.1.4.1.5923.1.1.1.10
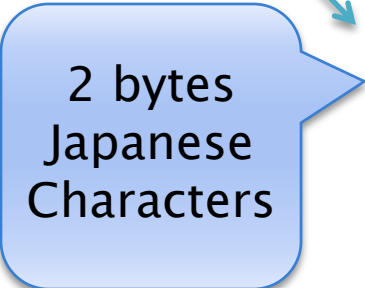
Name	UPKI-Fed OIDs
jasn	1.3.6.1.4.1.32264.1.1.1
jaGivenName	1.3.6.1.4.1.32264.1.1.2
jaDisplayName	1.3.6.1.4.1.32264.1.1.3
jao	1.3.6.1.4.1.32264.1.1.4
jaou	1.3.6.1.4.1.32264.1.1.5

2 bytes Japanese Characters

2009 Pilot Operation: Communicating with Major SPs

- ▶ **Practical Federation**
  - ▶ Elsevier: Science Direct and SCOPUS

- ▶ **Test Federation (connecting test)**
  - ▶ Refworks
  - ▶ Thomson   Web of Knowledge and EndNote Web
  - ▶ Springer   SpringerLink
  - ▶ LWW/Ovid   OvidSP
  - ▶ NII   CiNii
  - ▶ …

Difficulties

Need to ask to modify the SP setup which is practically operating

2009 Pilot Operation: Communicating with IdPs and Domestic SPs

- IdPs
  - Benefit to University Manager, IT section and Libraries
    - Especially, setup round table for IT people and Librarians
  - Understanding (do NOT hesitate) to release personal information
  - From test IdP to practical IdP
    - Facilitate "consensus building effort" among the institution

- Domestic SPs
  - IdP first? or SP first? The chicken and the egg

So far
1. Obtain number of test IdPs in feasibility study
2. Communicate with major overseas SPs

Future
3. Facilitate to operate practical IdPs
4. Recruits domestic SPs

Produce Positive Feedback

Move a Topic

Federation
- 2008 Feasibility Study
- 2009 Pilot Operation
  - Documents
  - Event and Training
  - Recruiting

Example of Extended Application *(Informatics Square)*
- Usual: Simple IdP and SP communication
- Extended: Institutional IdP and VO IdP communication
  - VO (academic society) IdP ≒ Attribute Provider from the view point of Institutional IdP

Institutional IdP and VO IdP: Concept of Informatics Square

▸ What (contents)

- ▸ Electronic journals published by Japanese academic societies for informatics.
- ▸ Conference paper and materials published by the above societies.
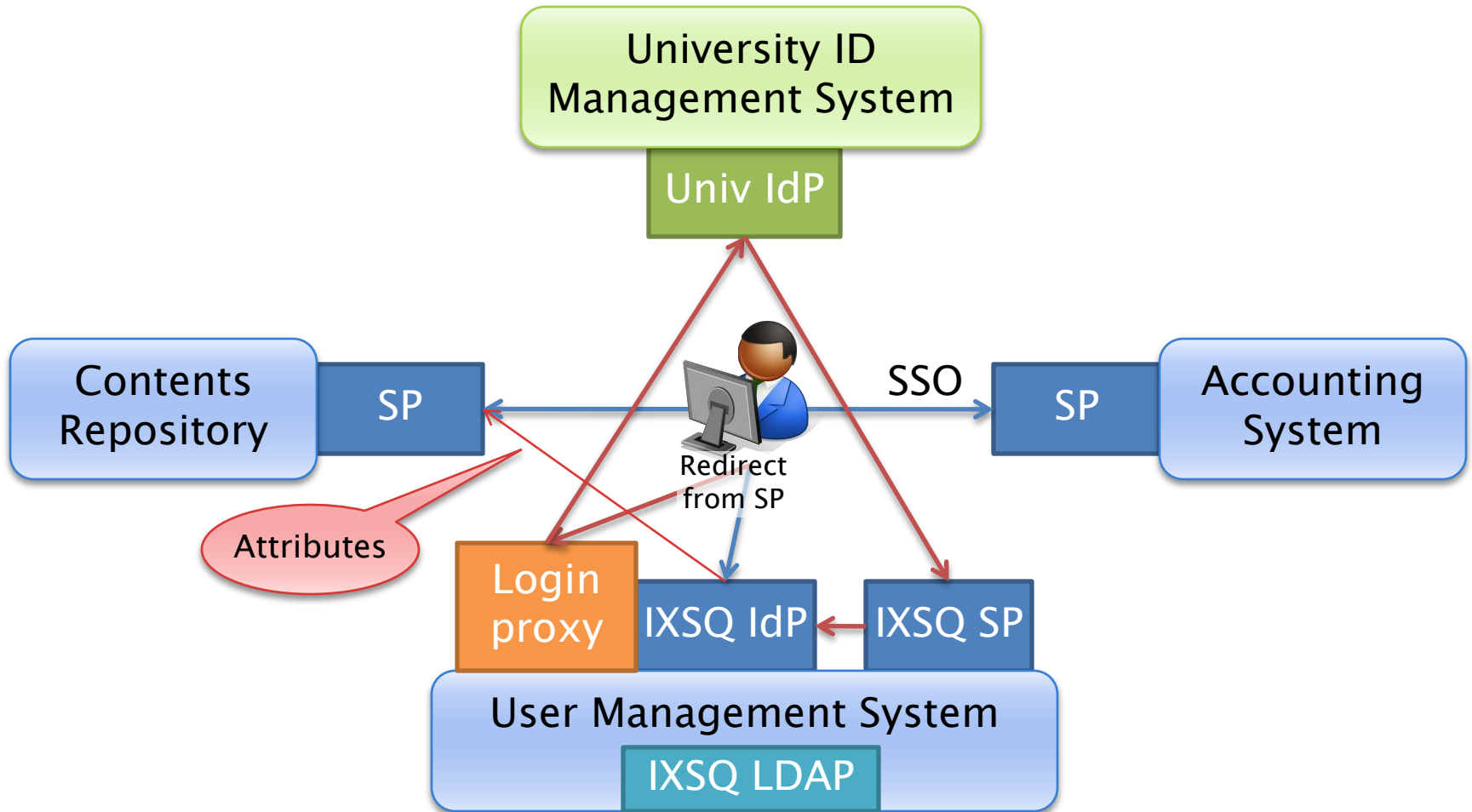- ▸ Supplemental data and/or multimedia data related to the above papers.

▸ How (contributors)

- ▸ EJ -> Academic Societies
- ▸ Supplemental Data -> Researchers
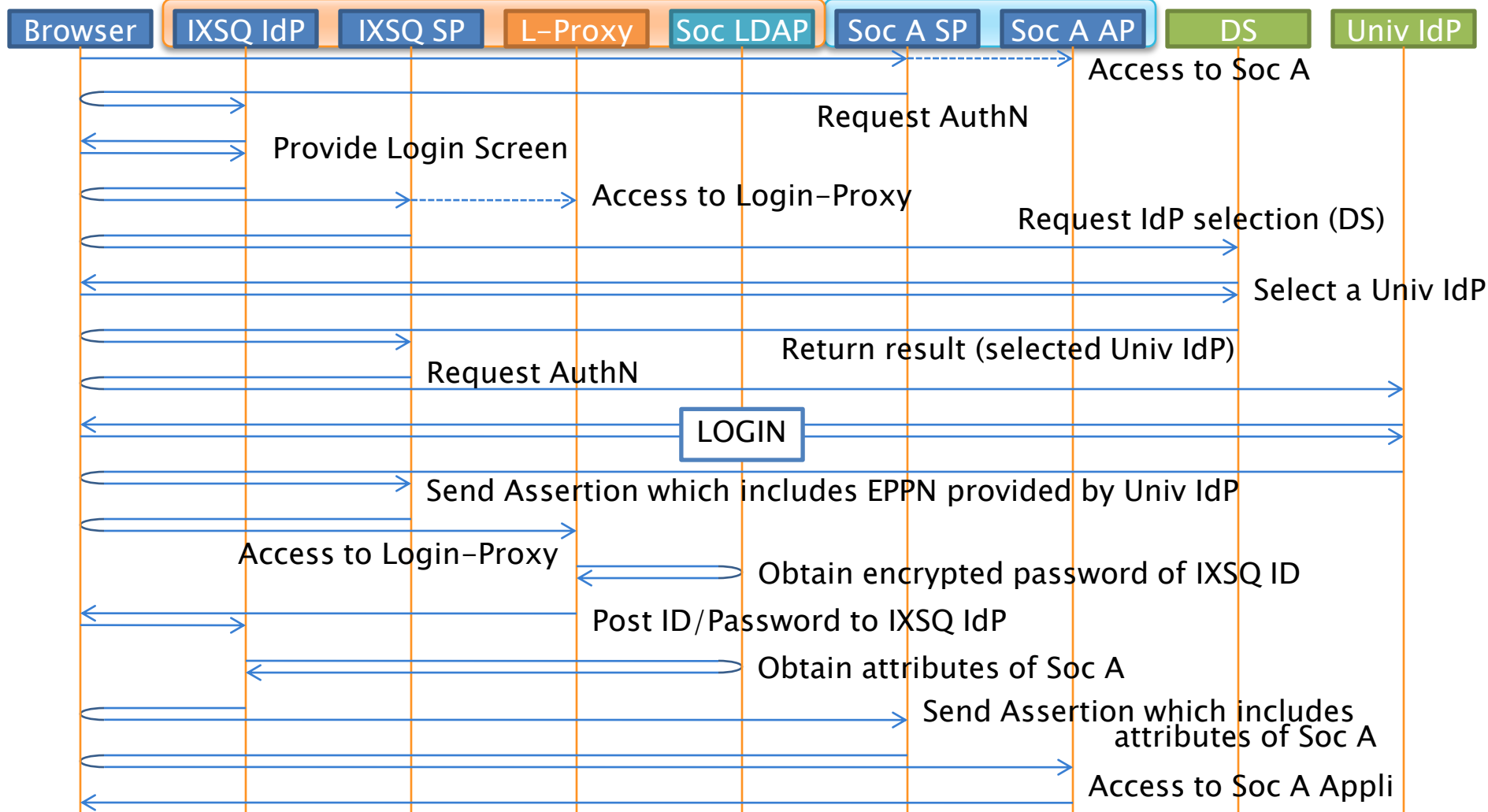- ▸ Shibbolized System (Repository, UMS, Accounting) ->NII
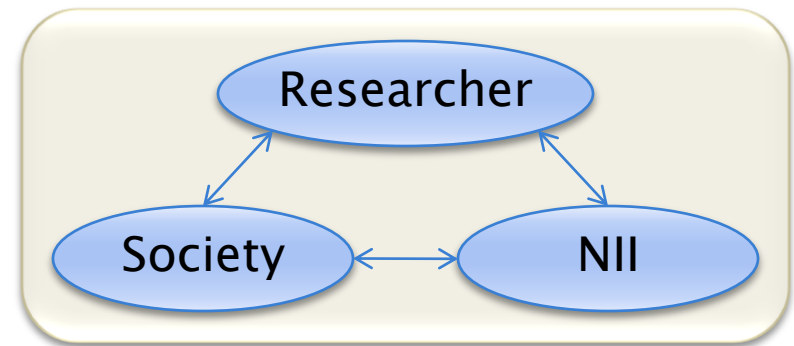
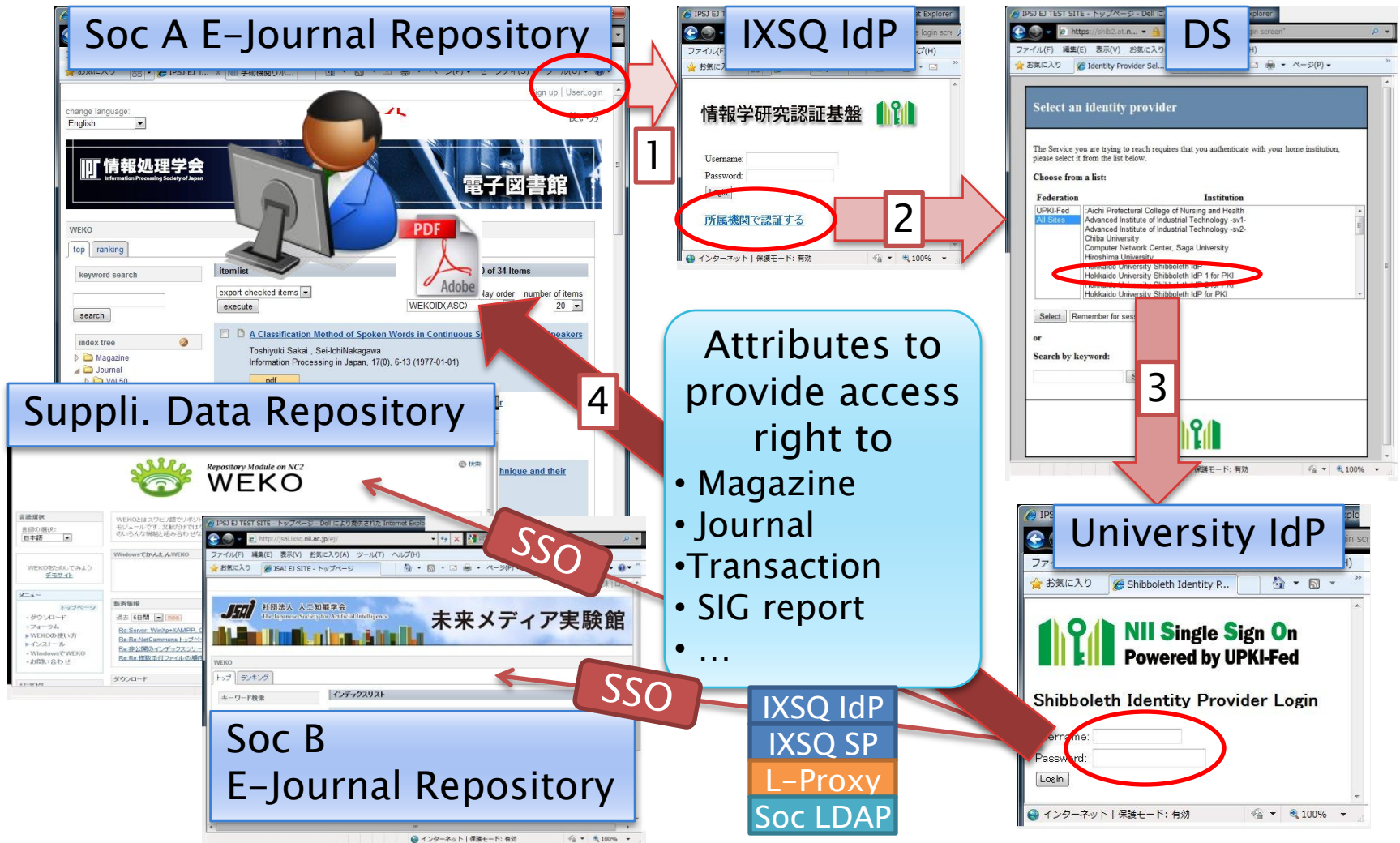# Institutional IdP and VO IdP: Schematic System Architecture

Institutional IdP and VO IdP: Sequence Diagram

Example: Login to Society A application by using university IdP

| Browser | IXSQ IdP | IXSQ SP | L-Proxy | Soc LDAP | Soc A SP | Soc A AP | DS | Univ IdP |

Access to Soc A

Request AuthN

Provide Login Screen

Access to Login-Proxy

Request IdP selection (DS)

Select a Univ IdP

Return result (selected Univ IdP)

Request AuthN

LOGIN

Send Assertion which includes EPPN provided by Univ IdP

Access to Login-Proxy

Obtain encrypted password of IXSQ ID

Post ID/Password to IXSQ IdP

Obtain attributes of Soc A

Send Assertion which includes attributes of Soc A

Access to Soc A Appli

Institutional IdP and VO IdP: Screen Images

Conclusions

- Federation in Pilot Operation
  - Deployment of IdP and SP
    - Case study
    - Strategies
    - Event Training

      Produce many more IdPs

  - Policy and Technical Guideline
  - Organization of Federation

  - Inter-federation with …possibly^^)

- Advanced Application