

ID-Federation in Japan for trustfull inter-domain ubiquitous services

Ito, Eisuke

Research Institute For Information Technology, Kyushu University : Associate Professor :
Information Science

<https://hdl.handle.net/2324/15948>

出版情報 : 2007-12-20
バージョン :
権利関係 :

2nd ICUT, Dec.20-22, 2007.
Bali, Indonesia.

ID Federation in Japan for trustful inter/ intra-institutional ubiquitous services

Eisuke ITO

*Research Institute for Information Technology,
Kyushu University*

itou@cc.kyushu-u.ac.jp

Outline



1. Introduction
2. Solutions for user authN problems
3. ID-federation
4. UPKI in Japan
5. IdM in Kyushu University
6. Conclusion

1. Introduction

- Recently, a variety of information services are being provided.
- Various aspects
 - Layer: Network , Transport, Application or Web
 - Content-type: text, document, picture, voice, movie, ...
 - Target user: young or senior, male or female, biz or entertainment, ...
 - **Open or Closed**
 - **Members only**
 - Many institutional services are closed.

User authN in closed service

- Closed services need user authN to identify a user
 - To provide personalized service
 - To be secure (keep secret, privacy)
 - To consider compliance
- The more closed service are provided, the more ID/passwd are issued.
 - For end-users, authN becomes complicated.
 - For administrators, user account management becomes complicated.
- SSO (Single Sign On) is requested, especially web applications

AuthN = Authentication

Inter-Domain Services

- Research and development of inter-domain service
 - Mash-up or Web-service
 - Development of new service with composition of multiple web services.
 - Grid computing
 - Wireless LAN roaming
 - Mutual exchange of e-Learning contents
 - (Unit exchange program among universities)

Objectives

Realize authN platform for trustful inter/intra-institutional (domain) services

- For inter-institutional services,
 - ID Federation between institutions (domains)
 - UPKI in Japan
- For intra-institutional services,
 - Identity Integration for all members
 - Deploy a campus-wide authentication infrastructure

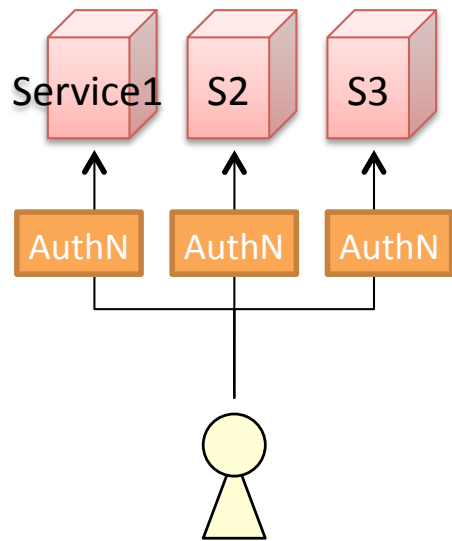
Outline



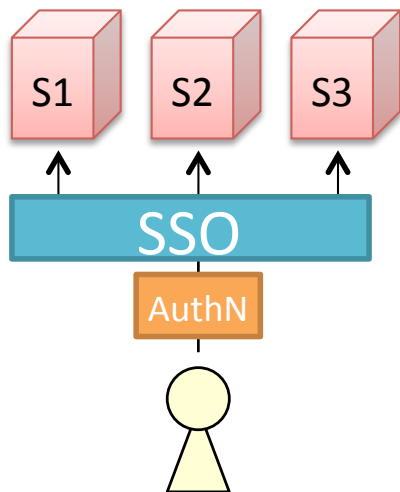
1. Introduction
2. Solutions for user authN problems
3. ID-federation
4. UPKI in Japan
5. IdM in Kyushu University
6. Conclusion

2. Solutions for user authN problems

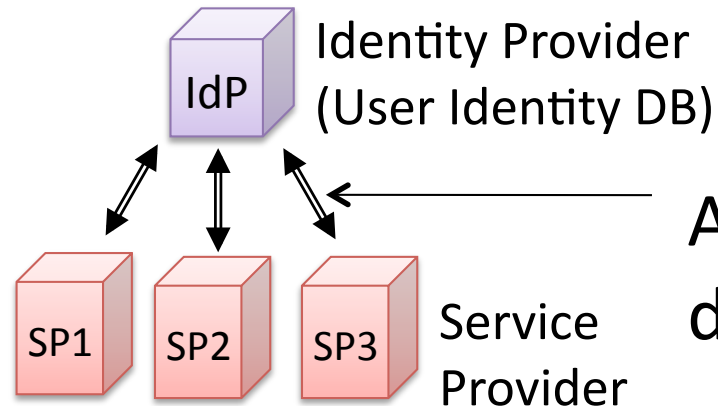
- SSO (Single Sign On)
 - Once a user authenticates, then gain access to the resources of multiple service systems.
- Divide SP and IdP
 - SP: Service Provider
 - IdP: Identity Provider
- AuthN/AuthZ data exchange
 - SAML: Security Assertion Markup Language
- Identity Integration
 - Set a centralized user DB in an institution/organization,
 - Any service looks up the DB.
- ID Federation
 - Make alliance between institutions
 - Mutually exchange user authN/authZ information



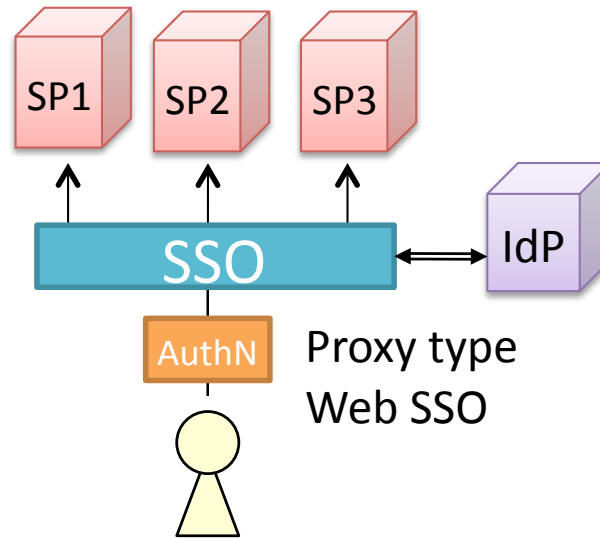
Single Sign On



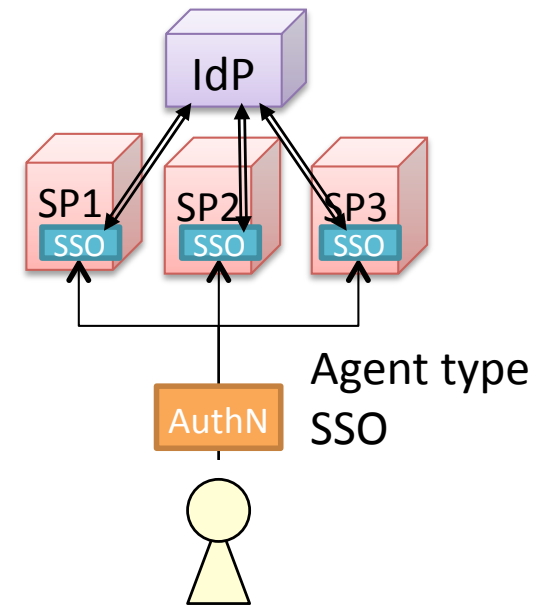
Divide SP and IdP



AuthN/AuthZ
data exchange



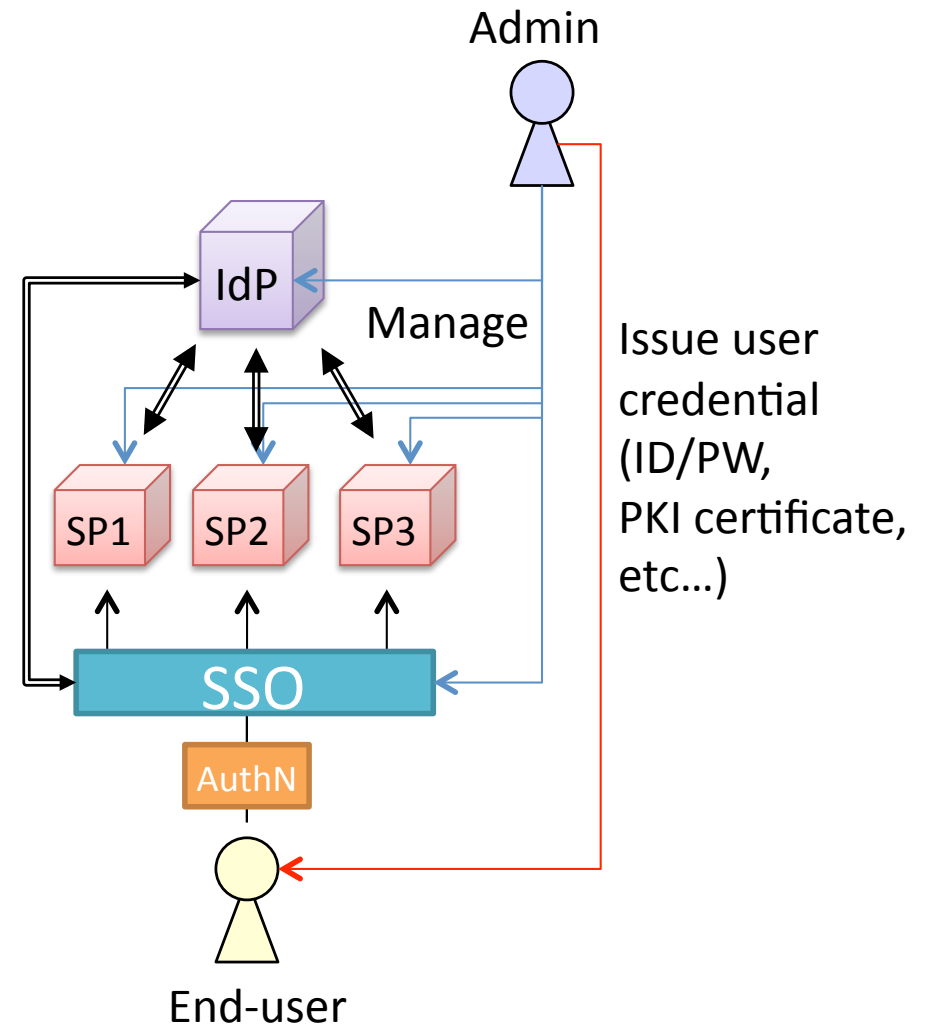
Proxy type
Web SSO



Agent type
SSO

Identity Integration

- Intra-Institutional services
 - Set a centralized user DB in a institution/organization, any service lookup the DB.
- Purpose
 - Reduce administration cost
 - The president can control all systems

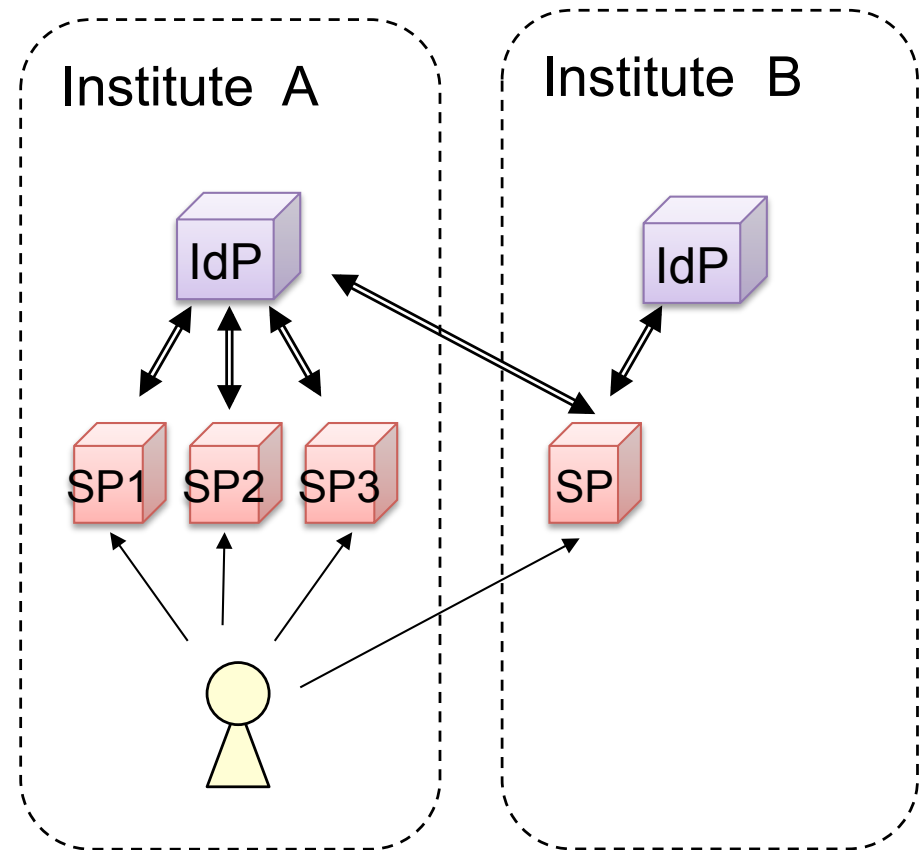


Outline

1. Introduction
2. Solutions for user authN problems
- 3. ID-federation
4. UPKI in Japan
5. IdM in Kyushu University
6. Conclusion

3. ID-Federation

- Federated organizations mutually exchange user identity data
- Ex.
 - Institute *A* and *B* are federated.
 - User of institute *A* accesses to an SP of *B*
 - The User sends the same credential to the SP for user AuthN.

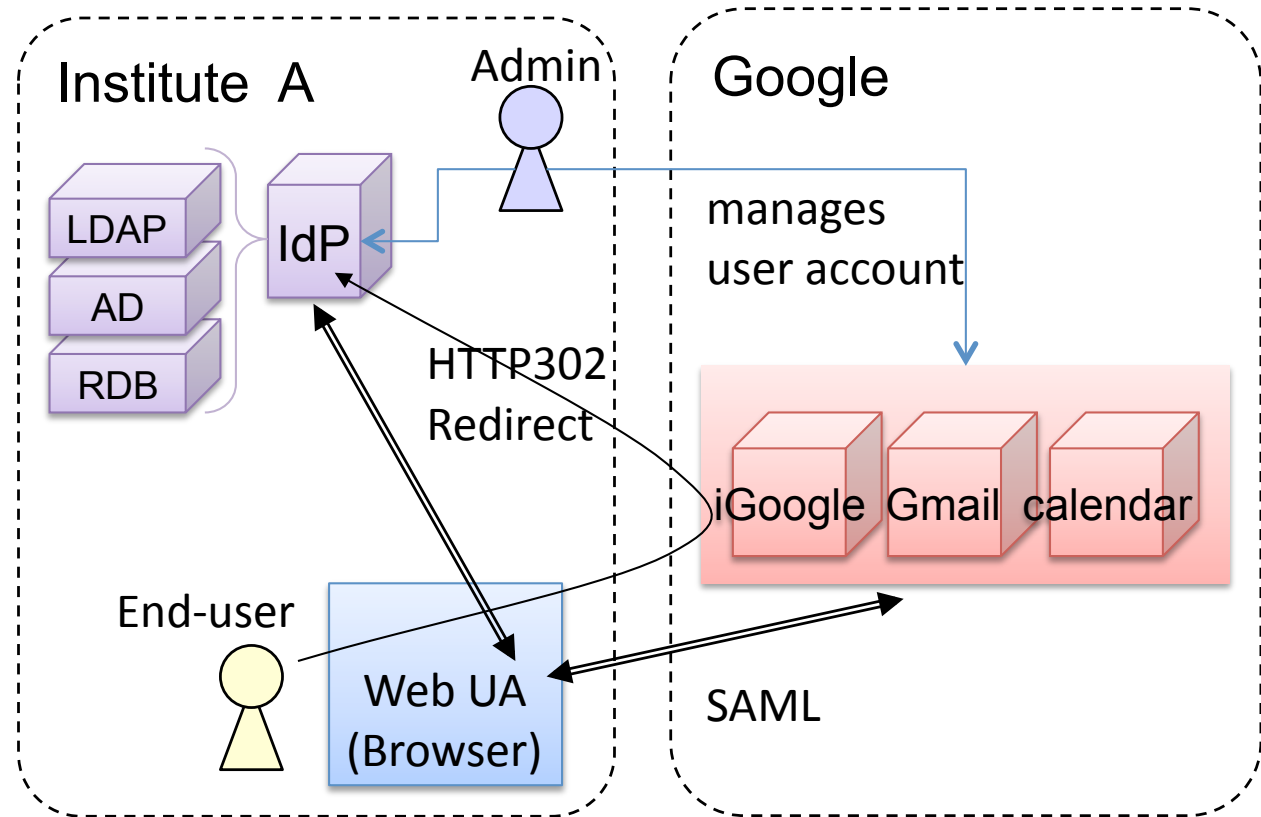


Federation systems

- Web based services systems
 - Google Apps Education Edition
- Eduroam
- Shibboleth
- OpenID

Google Apps Education Edition

- Google Apps for educational organization
- Free service
- Enable ID Federation

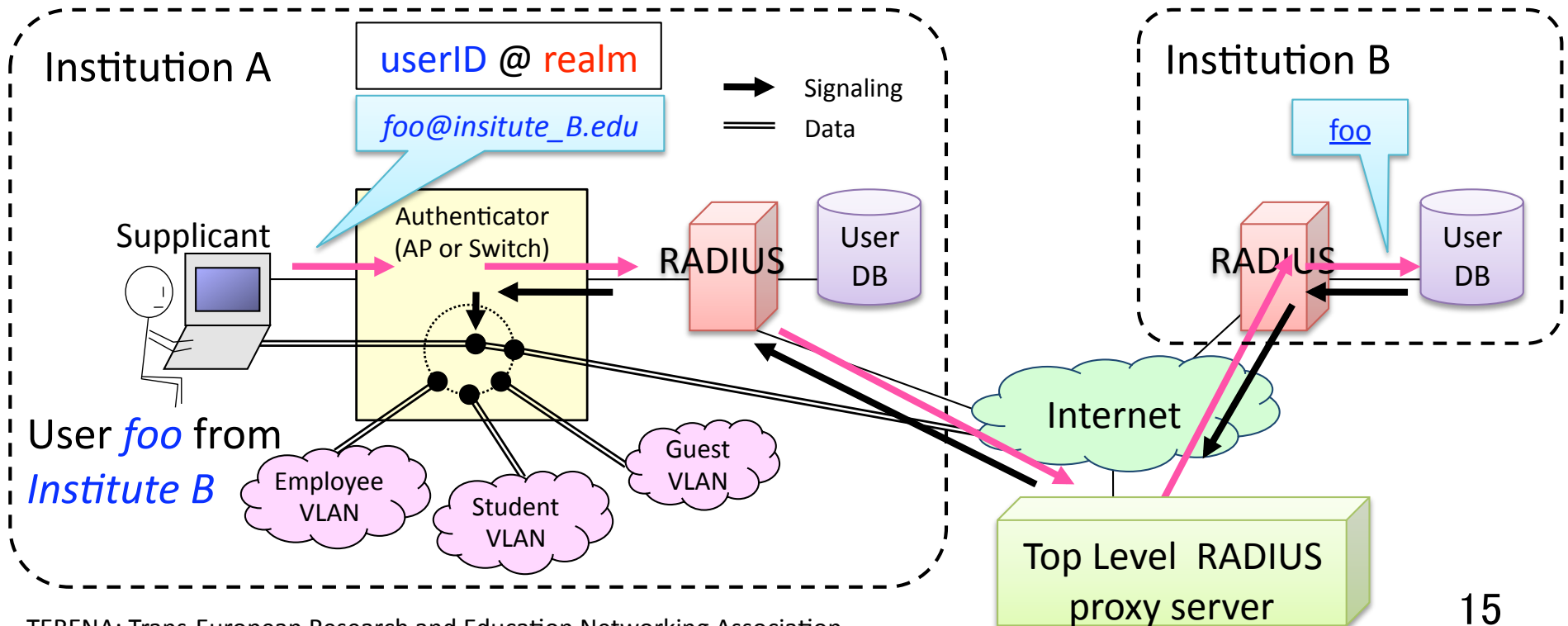
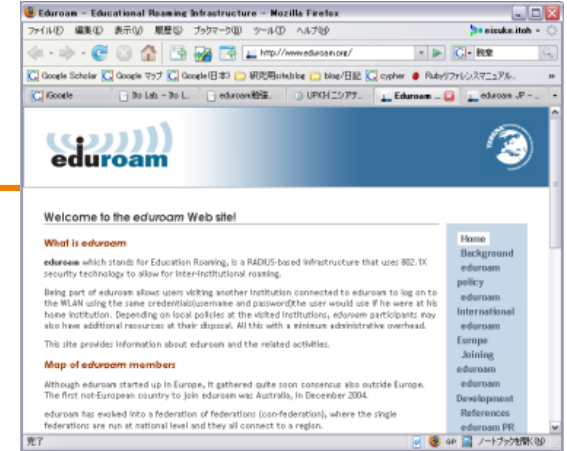


Microsoft Windows Live@edu
Yahoo! Mail Academic Edition

may have the same architecture.

eduroam

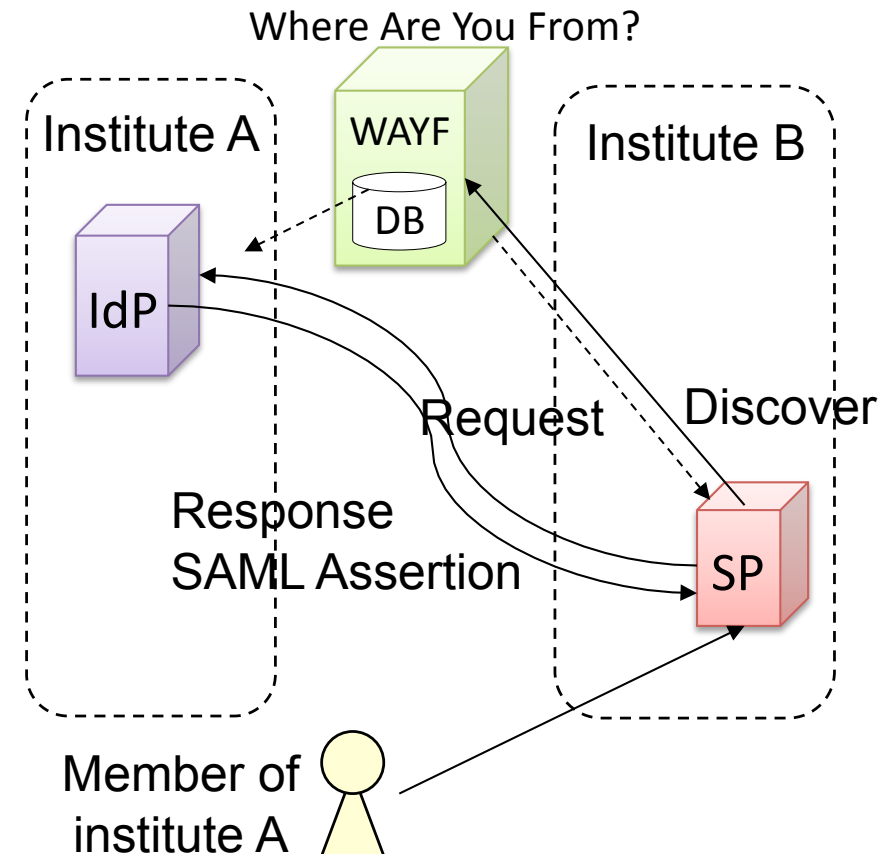
- Inter-institutional wireless roaming environment based on 802.1X and RADIUS
- Developed and deployed by TERENA
 - Mainly Europe, and Oceania. Asia was joined recently.



Shibboleth

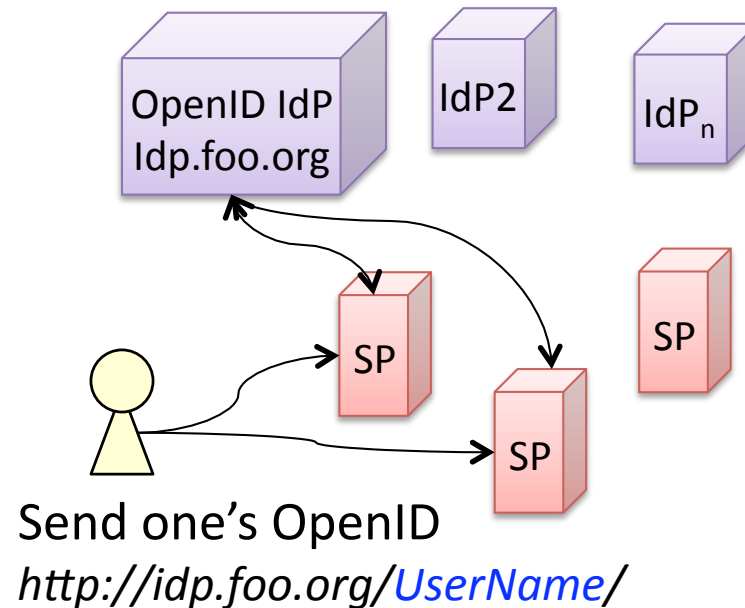
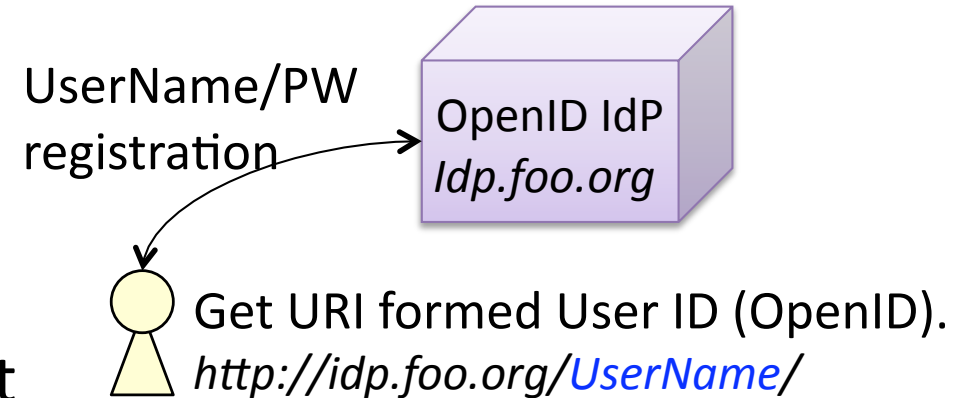


- Shibboleth
 - An Internet2 subproject
 - The name of middleware for Web SSO
- WAYF server must know IdPs
 - IdPs and the WAYF are tightly connected
- WAYF server becomes bottleneck.



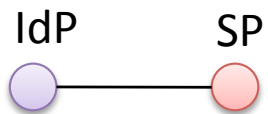
OpenID

- A decentralized SSO system
- User's identifier is represented as URI format
 - Easy to resolve where the IdP is.
 - Maintenance free
 - Easy to keep uniqueness without centralized control
- Problem
 - How to trust the IdP?

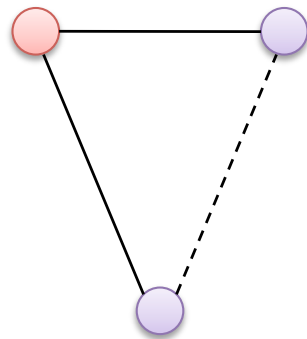


Federation structure

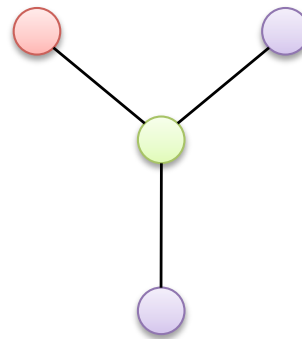
1 to 1



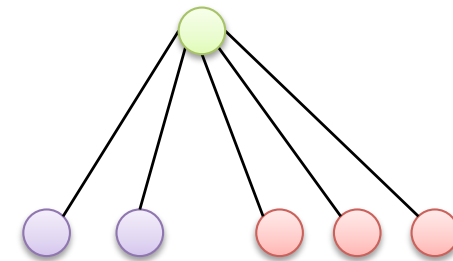
Network



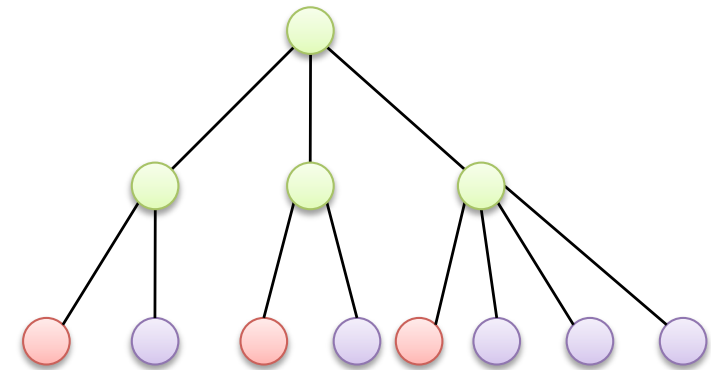
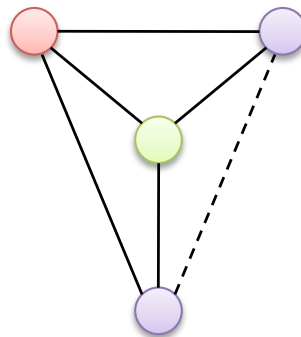
Broker or Bridge



Tree

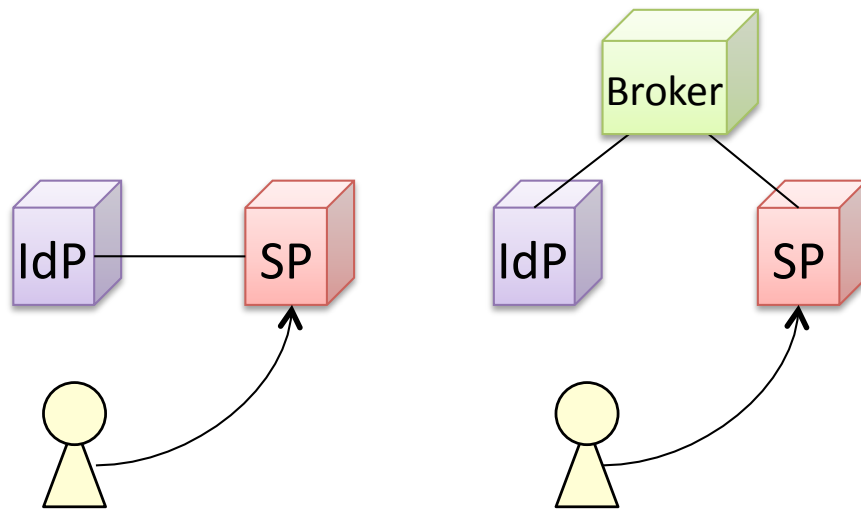


Hybrid



AuthN/AuthZ data exchange

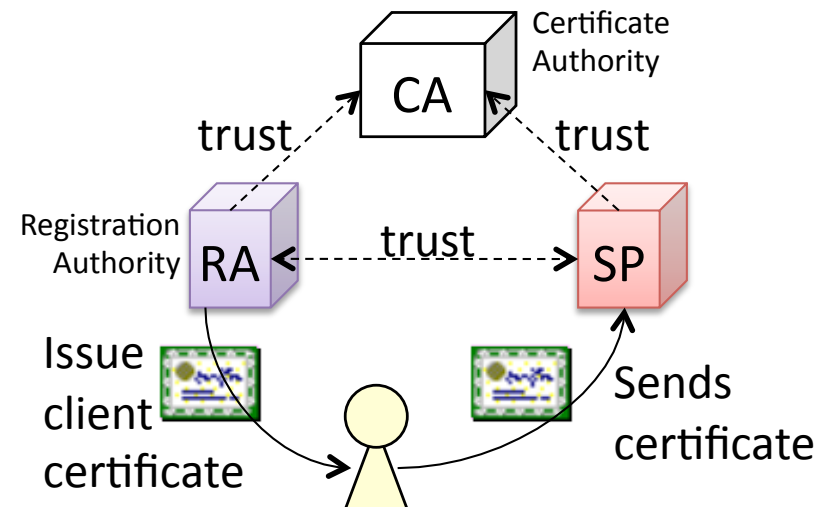
- On-demand exchange user authN/authZ data
 - Web apps, Shibboleth, eduroam, OpenID



Easy to implement
but NOT scalable

Broker is the
bottle neck.

- PKI style
 - Trust the same CA
 - Trust each other
 - No communication between entities



How to trust other institute CA/RA?
CRL distribution is difficult.

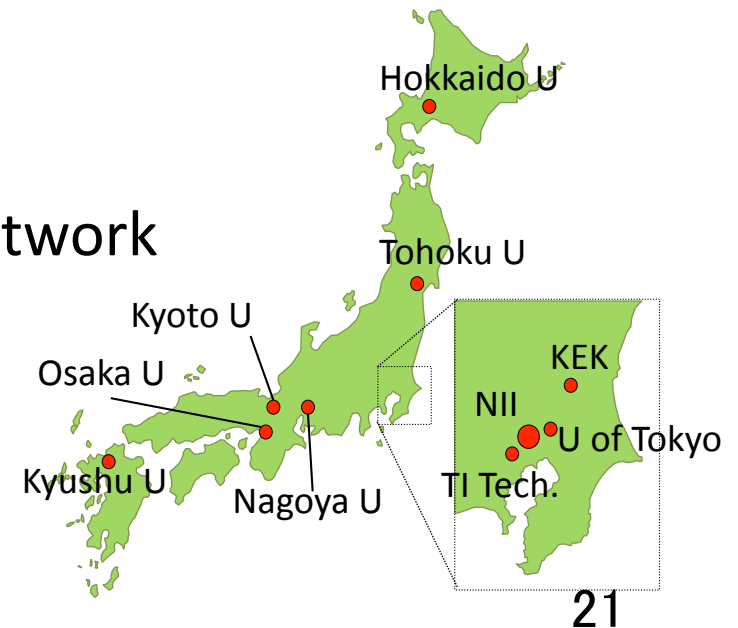
Outline

1. Introduction
2. Solutions for user authN problems
3. ID-federation
4. UPKI in Japan
5. IdM in Kyushu University
6. Conclusion



4. UPKI in Japan

- CSI (Cyber Science Infrastructure) Project
 - Since 2005,
 - NII (National Institute for Informatics) of Japan
- Purpose :
 - A nation-wide platform for inter-institutional services
- Four subprojects
 - Grid computing
 - Advanced high speed broadband network
 - Institutional repository for library
 - **UPKI**



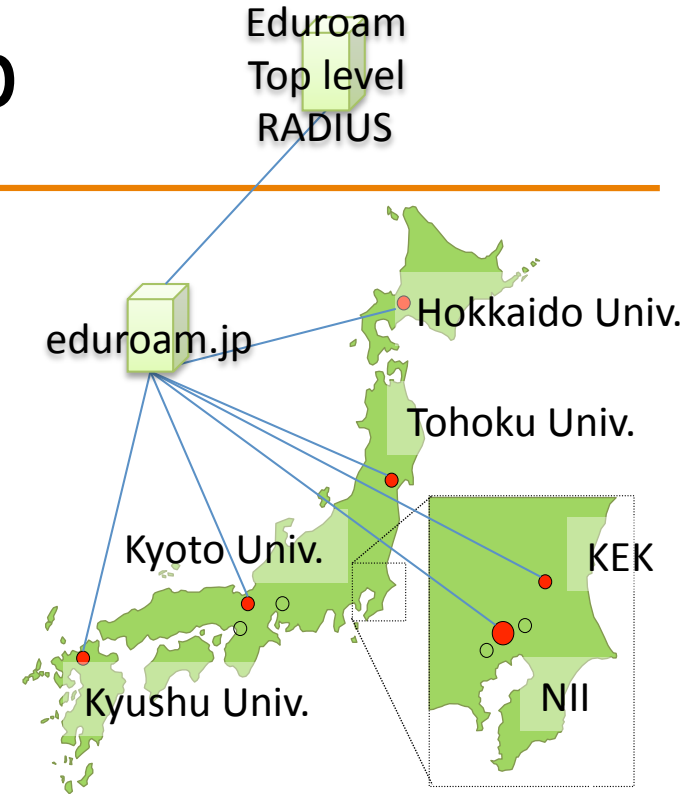
UPKI



-
- UPKI
 - U: University/Universal/Ubiquitous
 - Nation-wide electronic certification platform.
 - The inter-institutional exchange of user authN
 - Construct mutual trust among institutions.
 - Results
 - Publish template of CP/CPS for CA in University
 - Server certificate distribution
 - eduroam.jp

eduroam.jp

- eduroam experiment in JP
 - Part of UPKI project
 - 6 institutions are participated
 - Tohoku University is leading
 - Running JP Top RADIUS Server



Participated Institution (2007/9/13)

Institution	AuthN Used	Access Granted
National Institute of Informatics	802.1x	eduroam standard
Hokkaido Univ.	802.1x	?
Tohoku Univ.	802.1x, TKIP, PEAP	VPN
High Energy Accelerator Research Organization (KEK)	802.1x	?
Kyoto Univ.	802.1x	eduroam standard
Kyushu Univ.	802.1x	VPN(planned)

eduroam standard includes:
IPSec VPN, PPTP VPN, SSH,
HTTP, HTTPS, IMAP2/3/S, POP/
POP3, Passive FTP, SMTP/
SMTPS, RDP

Outline

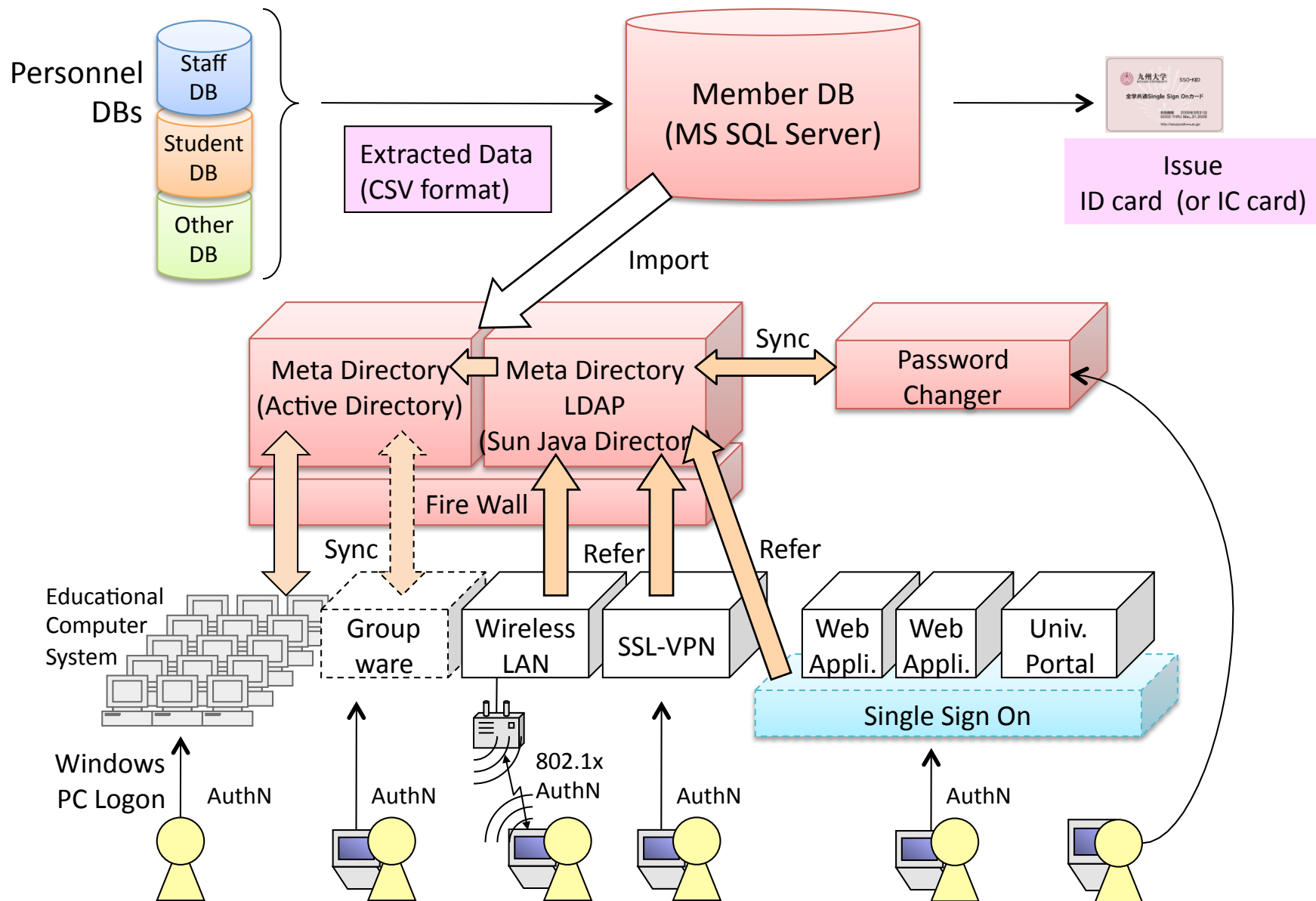
1. Introduction
2. Solutions for user authN problems
3. ID-federation
4. UPKI in Japan
5. IdM in Kyushu University
6. Conclusion



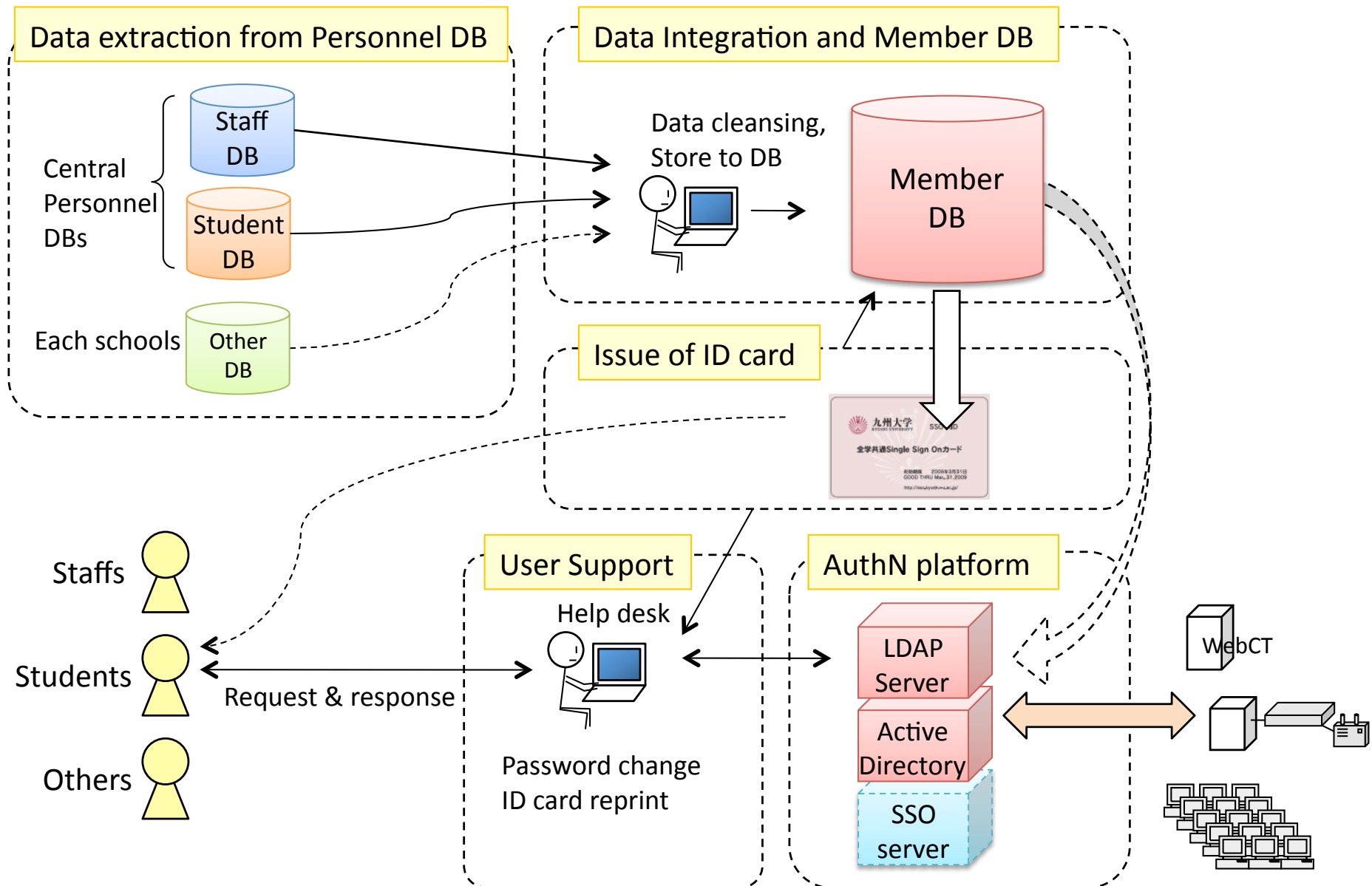
5. IdM in Kyushu Univ.

- Since 2005
- Construct IdM (Identity Management) System
 - Integrate user ID/PW, user Identity
 - Centralized user authentication platform
- Connect between applications and the IdM
- Identity Management Division

IdMS System Overview

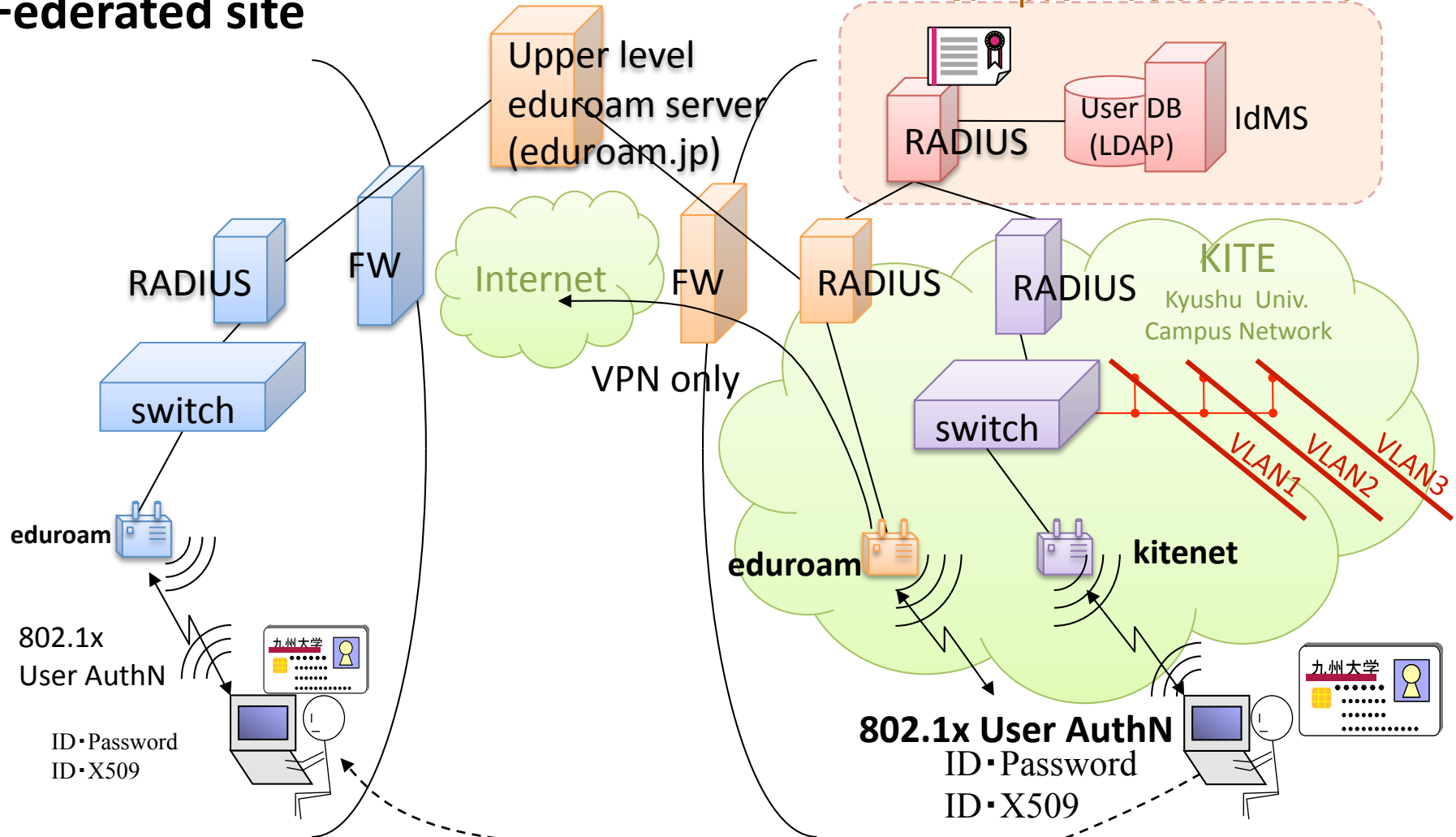


Work flow to update member data



For Campus Network & Roaming (under development)

eduroam Federated site



Outline

1. Introduction
2. Solutions for user authN problems
3. ID-federation
4. UPKI in Japan
5. IdM in Kyushu University
6. Conclusion



6. Conclusion

- For trustful inter/intra-institutional ubiquitous services,
 - Not only service cooperation
 - User AuthN/AuthZ cooperation is necessary.
- ID Federation
 - Introduced four systems
 - Discuss about ID federation styles and problems
- CSI and UPKI project in Japan
- IdM in Kyushu University

- In the fututure,
 - PKI based nationwide ID-federation (for inter-institutional services)
 - E-Tokens (such as IC card)
 - Authorization mechanism