Introduction about SAML based Identity federation

Kazu Yamaji, NII Japan

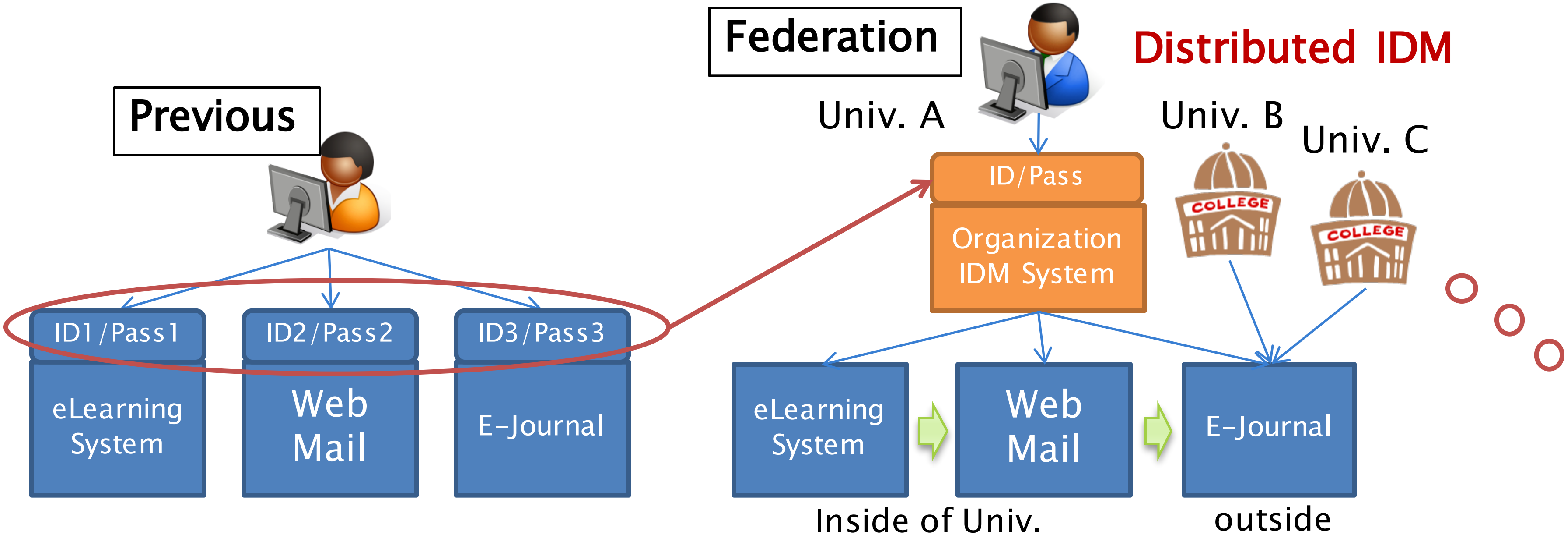
Eko-Konnect Repository Workshop and eduID Policy meeting, 27 Jan 2020

Today’s Topics

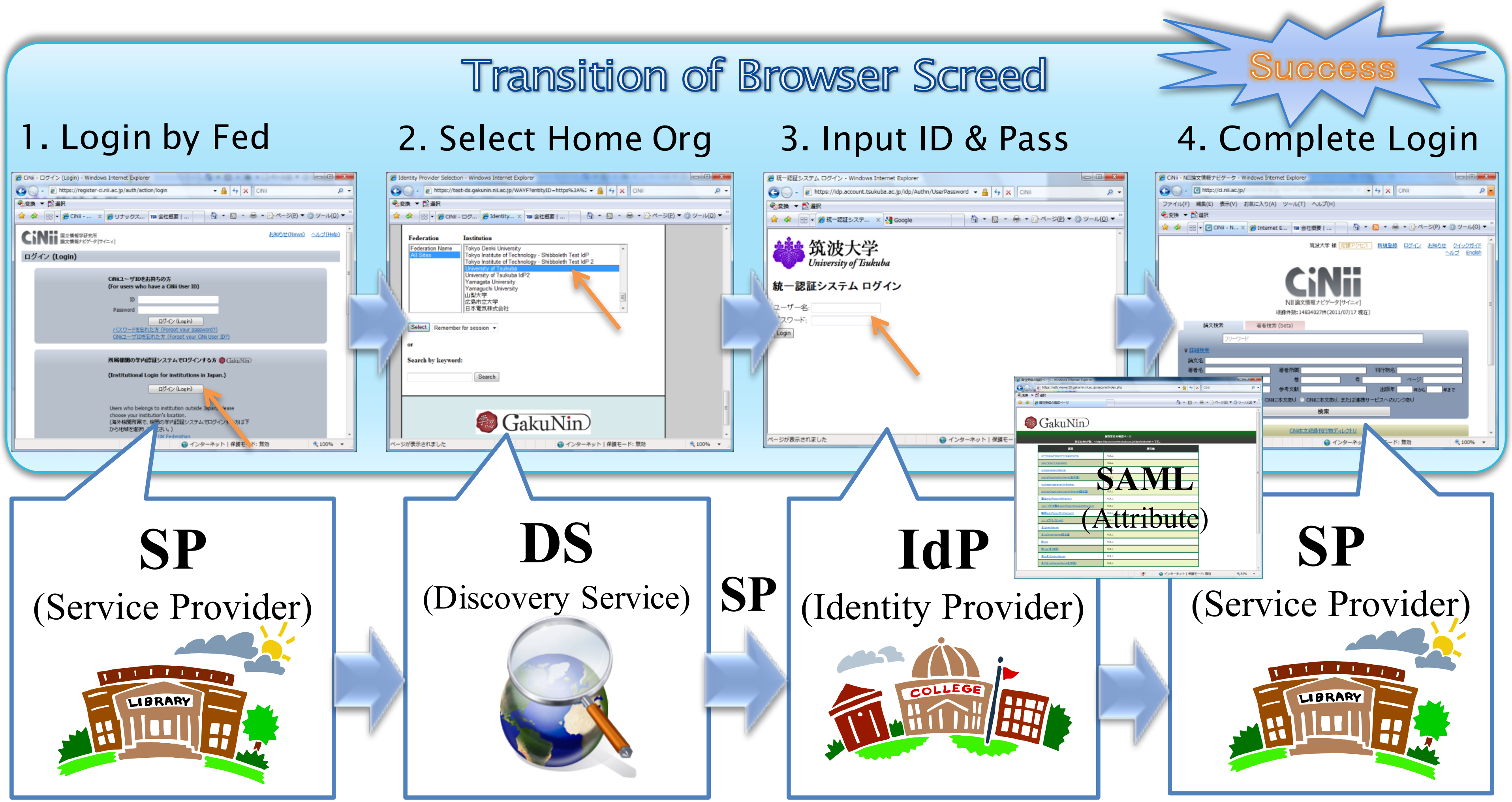
- Overview of the Federation
- Technical Information (if necessary)

What is this for

- The Federation
  - provides a single sign on (SSO) to access web services for education and research.
  - makes sharing protected online resources easier(SSO), safer(privacy-preserving), and more scalable(distributed identity management) in our age of digital resources and services.



Authn Flow by the Federation



Transition of Browser Screed

Success

1. Login by Fed

CiNii - ログイン (Login) - Windows Internet Explorer
https://register-ci.nii.ac.jp/auth/action/login

ログイン (Login)

CiNiiユーザIDをお持ちの方
(For users who have a CiNii User ID)

ID
Password
ログイン (Login)
パスワードを忘れた方 (Forgot your password?)
CiNiiユーザIDを忘れた方 (Forgot your CiNii User ID?)

所属機関の学内認証システムでログインする方 GakuNin
(Institutional Login for institutions in Japan.)
ログイン (Login)

Users who belongs to institution outside Japan, please choose your institution's location.
(海外機関所属で、機関の学内認証システムでログインする方は下から地域を選択 さい。)
UK Federation

2. Select Home Org

Identity Provider Selection - Windows Internet Explorer
https://test-ds.gakunin.nii.ac.jp/WAYF?entityID=https%3A%2

Federation	Institution
Federation Name All Sites	Tokyo Denki University Tokyo Institute of Technology - Shibboleth Test IdP Tokyo Institute of Technology - Shibboleth Test IdP 2 University of Tsukuba University of Tsukuba IdP2 Yamagata University Yamaguchi University 山梨大学 広島市立大学 日本電気株式会社

Select | Remember for session

or

Search by keyword:

Search

GakuNin

ページが表示されました

3. Input ID & Pass

統一認証システム ログイン - Windows Internet Explorer
https://idp.account.tsukuba.ac.jp/idp/Authn/UserPassword

筑波大学
University of Tsukuba

統一認証システム ログイン

ユーザー名:
パスワード:
Login

属性受信の確認ページ - Windows Internet Explorer
https://attrviewer20.gakunin.nii.ac.jp/secure/index.php

GakuNin

SAML
(Attribute)

4. Complete Login

CiNii - NII論文情報ナビゲータ - Windows Internet Explorer
http://ci.nii.ac.jp/

筑波大学 様 定額アクセス 新規登録 ログイン お知らせ クイックガイド ヘルプ English

CiNii
NII 論文情報ナビゲータ[サイニィ]
収録件数: 14834027件(2011/07/17 現在)

論文検索 | 著者検索 (beta)

フリーワード
詳細検索
論文名
著者名 | 著者所属 | 刊行物名
巻 | 号 | ページ
参考文献 | 出版年 年から 年まで
CiNiiに本文あり ○ CiNiiに本文あり、または連携サービスへのリンクあり
検索
CiNii本文収録刊行物ディレクトリ

SP
(Service Provider)

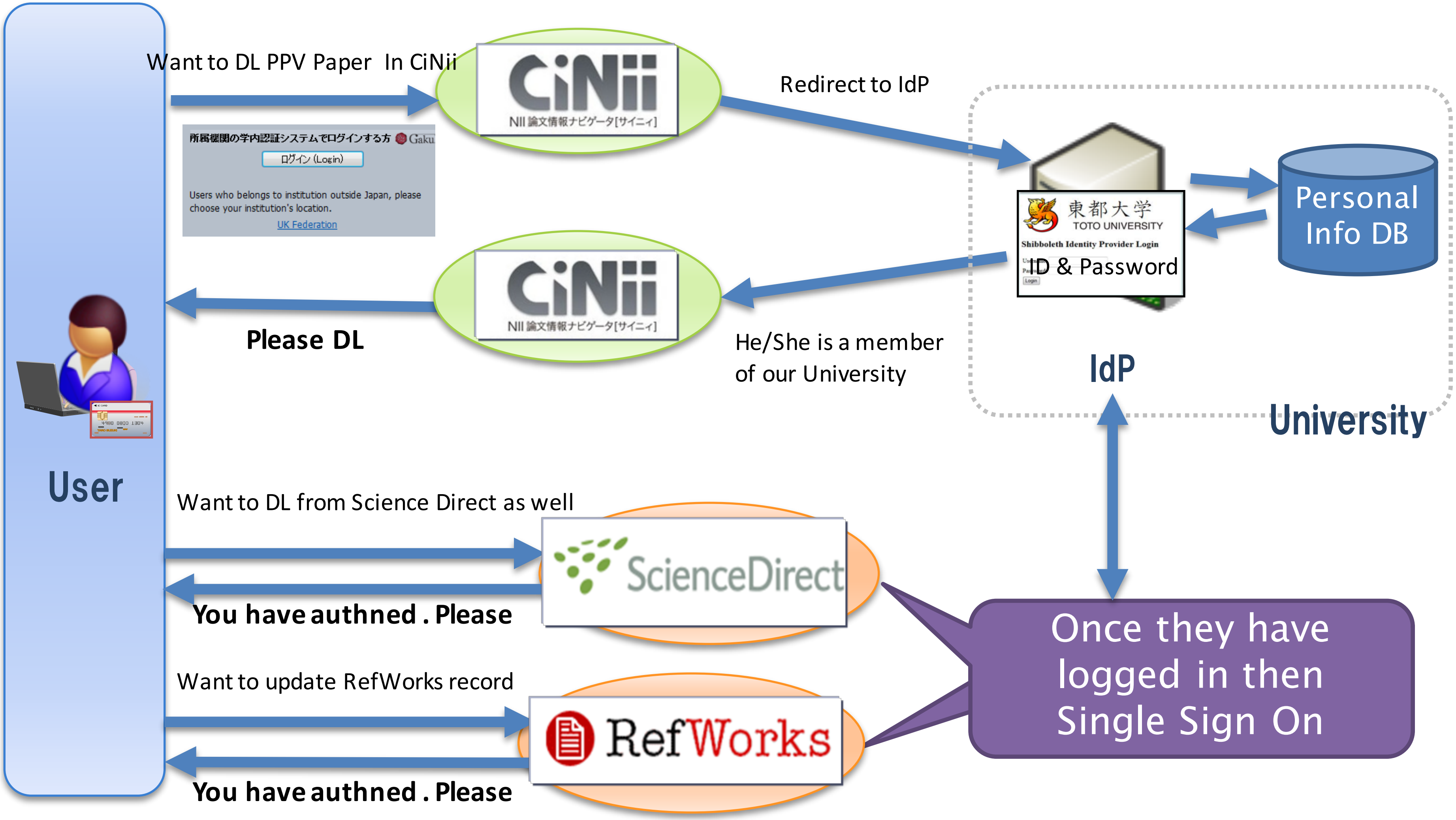
DS
(Discovery Service)

SP

IdP
(Identity Provider)

SP
(Service Provider)

Example of Utility by EJ related SPs



User

Want to DL PPV Paper In CiNii

所属機関の学内認証システムでログインする方

ログイン (Login)

Users who belongs to institution outside Japan, please choose your institution's location.

UK Federation

Redirect to IdP

東都大学
TOTO UNIVERSITY

Shibbboleth Identity Provider Login

ID & Password

Login

Personal Info DB

IdP

University

He/She is a member of our University

Please DL

Want to DL from Science Direct as well

You have authned . Please

Want to update RefWorks record

You have authned . Please

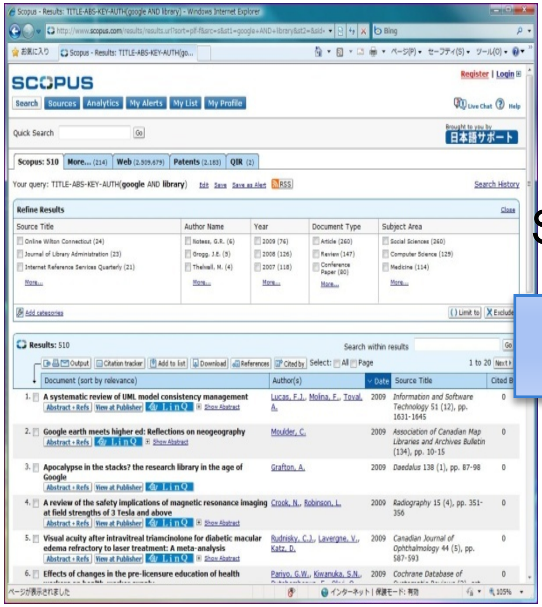
Once they have logged in then Single Sign On

Example of Utility by EJ related SPs

Search Paper

Read Paper

Mange Paper



1. A systematic review of UML model consistency management — Lucas, F.J., Molina, F., Toval, A. — 2009 — Information and Software Technology 51 (12), pp. 1631-1645

2. Google earth meets higher ed: Reflections on neogeography — Moulder, C. — 2009 — Association of Canadian Map Libraries and Archives Bulletin (134), pp. 10-15

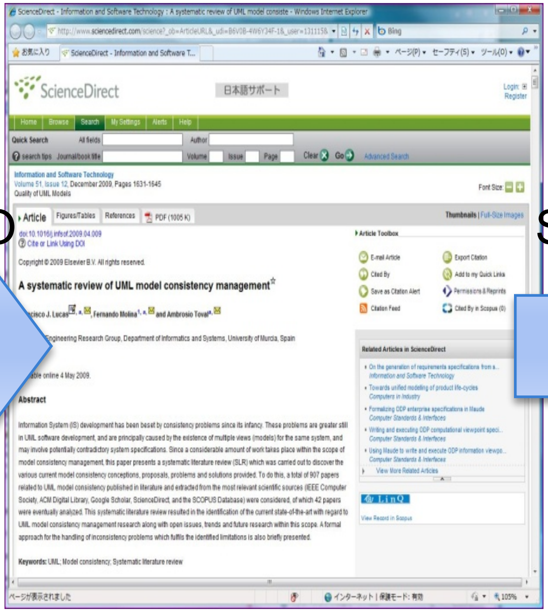
3. Apocalypse in the stacks? the research library in the age of Google — Grafton, A. — 2009 — Daedalus 138 (1), pp. 87-98

4. A review of the safety implications of magnetic resonance imaging at field strengths of 3 Tesla and above — Crook, N., Robinson, L. — 2009 — Radiography 15 (4), pp. 351-356

5. Visual acuity after intravitreal triamcinolone for diabetic macular edema refractory to laser treatment: A meta-analysis — Rudnisky, C.J., Lavergne, V., Katz, D. — 2009 — Canadian Journal of Ophthalmology 44 (5), pp. 587-593

6. Effects of changes in the pre-licensure education of health — Pariyo, G.W., Kiwanuka, S.N., — 2009 — Cochrane Database of

SSO



Information and Software Technology
Volume 51, Issue 12, December 2009, Pages 1631-1645
Quality of UML Models

Copyright © 2009 Elsevier B.V. All rights reserved.

A systematic review of UML model consistency management

Francisco J. Lucas, Fernando Molina and Ambrosio Toval

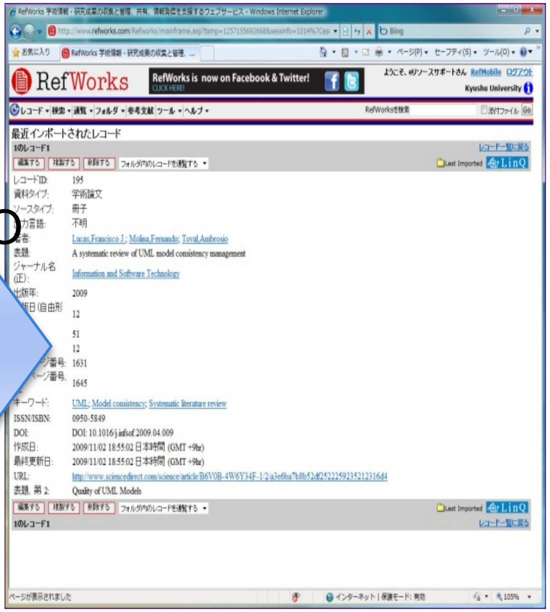
Software Engineering Research Group, Department of Informatics and Systems, University of Murcia, Spain

Available online 4 May 2009.

Abstract

Keywords: UML; Model consistency; Systematic literature review

SSO

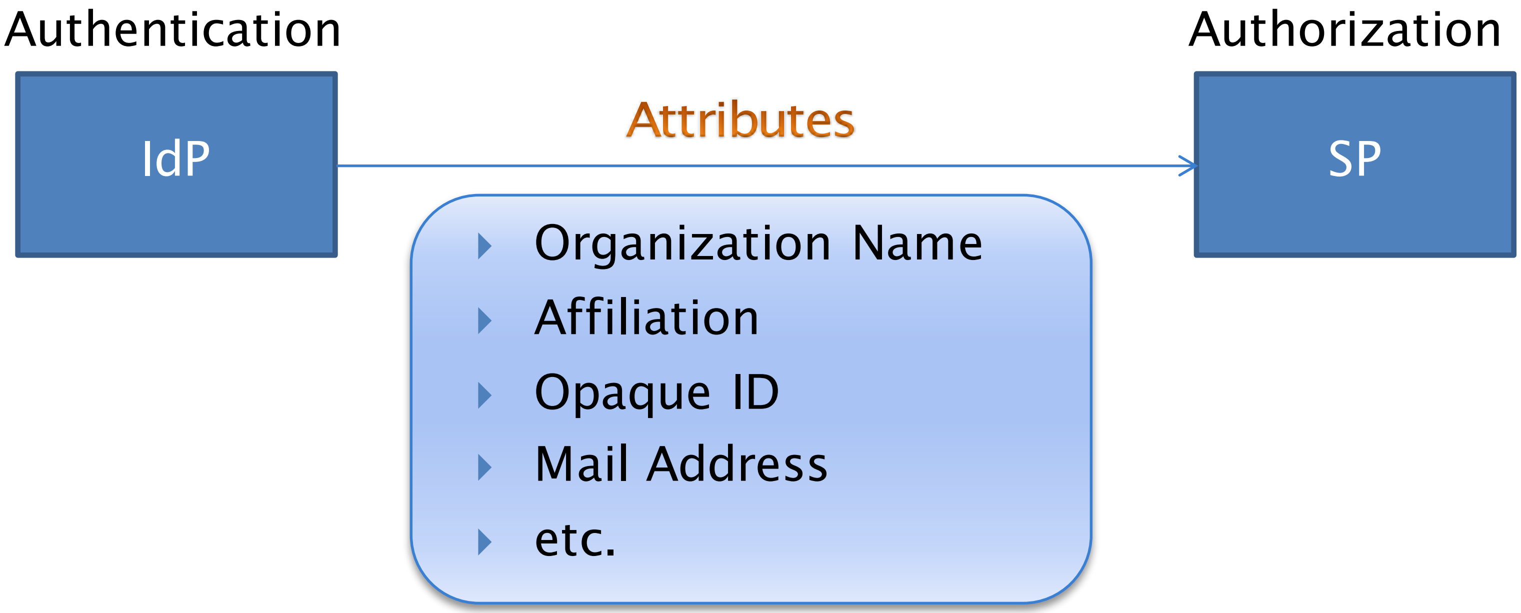

RefWorks
RefWorks is now on Facebook & Twitter!
Kyushu University
最近インポートされたレコード

レコードID: 195
資料タイプ: 学術論文
ソースタイプ: 冊子
表題: A systematic review of UML model consistency management
ジャーナル名: Information and Software Technology
出版年: 2009
キーワード: UML; Model consistency; Systematic literature review
ISSN/ISBN: 0950-5849
DOI: DOI: 10.1016/j.infsof.2009.04.009
叢書, 第2: Quality of UML Models

- Facilitate Remote Access
- Improve Usability by SSO etc.

Simply Saying

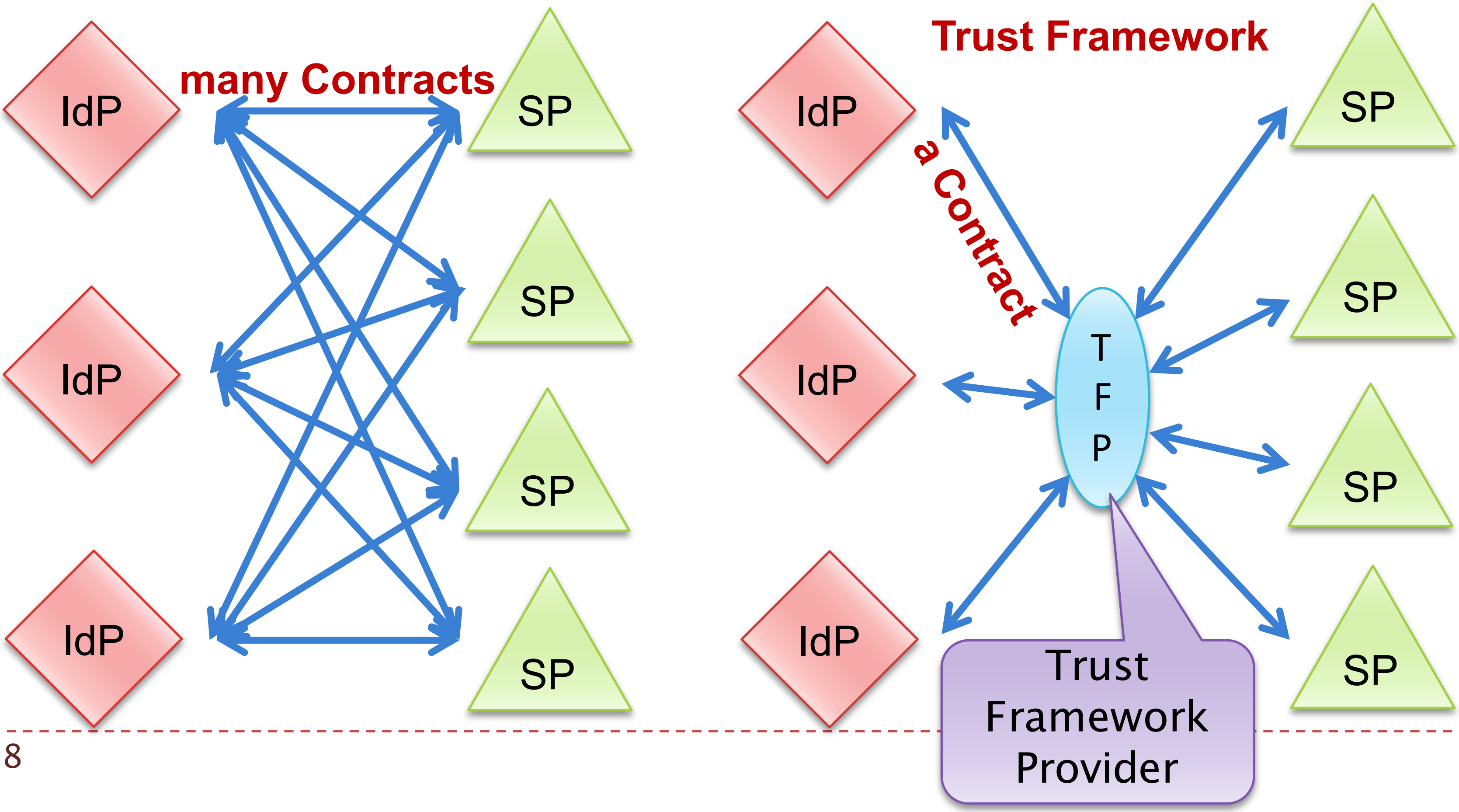
- The Federation is
  - Secure, scalable and easy login architecture by standard protocol: SAML



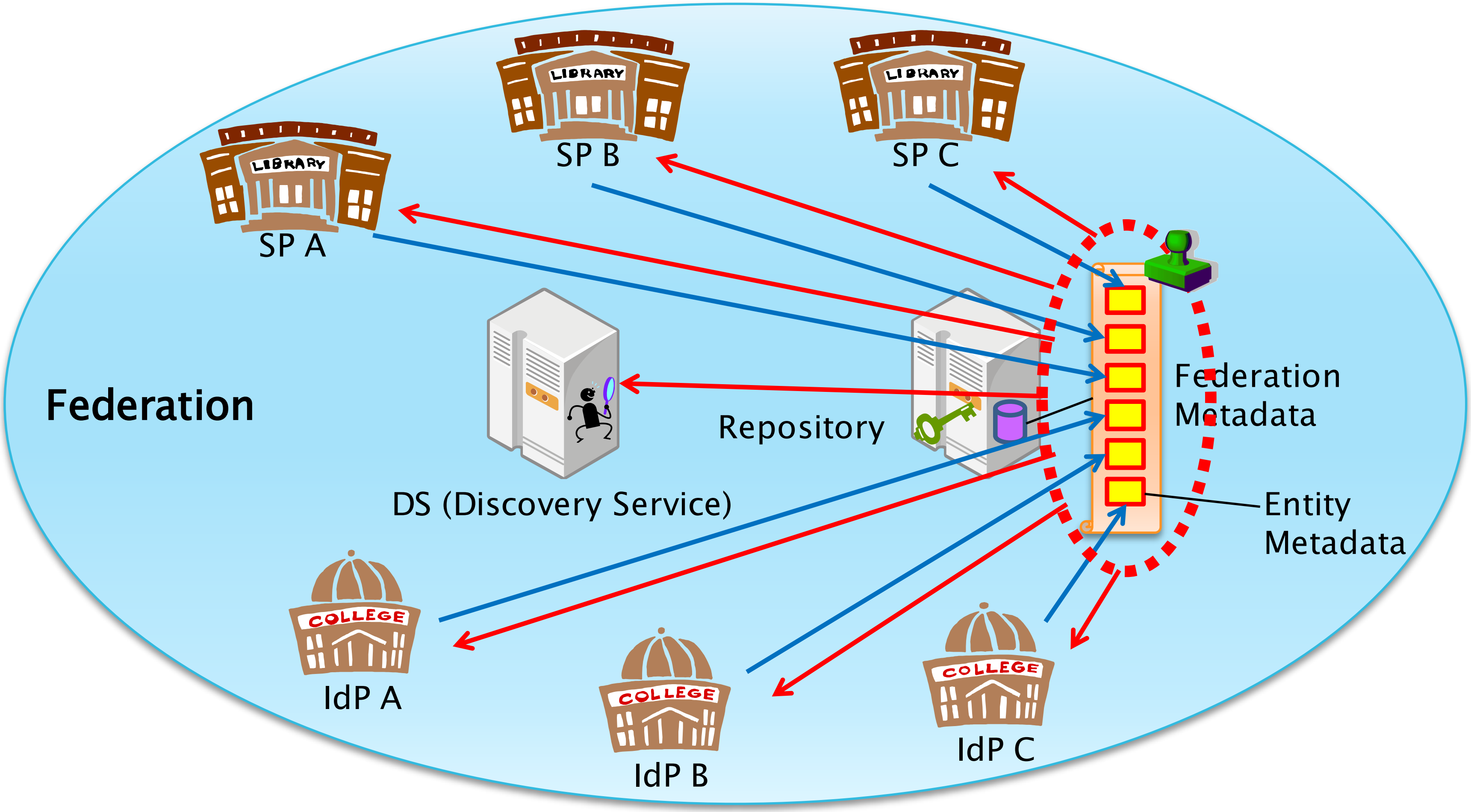
- Organization Name
- Affiliation
- Opaque ID
- Mail Address
- etc.

Effectiveness of trust framework

- Number of contract can be reduced from N×M to N+M by introducing a uniform policy



Building Relying Party by Metadata



Reliability of the relying party is confirmed by the singed metadata.

Benefits of the Federation

- Higher security
  - Policy-driven methods, using strong authorization controls over secure access channels, provide a higher-level security. This higher level also provides a secure mechanism for ensuring privacy in the exchange of identity and authorization attributes.
- Provide a standard conduit for collaboration
  - The Federation acts as a collection point and conduit for those wishing to provide and gain access to collaborative web based resources. Using a standard mechanism for connecting to this conduit provides economies of scale by reducing or removing the need to repeat integration work for each new collaborative work.
- Reduced account overhead
  - Account creation and management can be reduced for resource consumers who are not affiliated with the institution offering those resources. As a federation member, these resources are made available to other federation members who are responsible for managing those accounts.
- Economies of scale for contractual agreements
  - Some or all of the policy and legal requirements for bilateral agreements between institutions for sharing of resources may be consolidated by or leveraged from the Federation policies, agreements and requirements documents. This could minimize the need or scope of multiple relying party agreements.
- More granular control over access to and auditing of online resource distribution
  - Institutions currently offering resources restricted by IP address or other gross controls will be able use authorization decisions to enforce more granular control for the distribution of cost based resources. The results of which lead to a more consistent accounting of which resources are actually being utilized and by whom.

Benefits of the Federation

- End-User Benefits
  - **Ease user account management:** Users no longer have to manage an array of accounts and passwords.
  - **Privacy maintained:** Users identify themselves locally with their home institution, then pass only relevant and necessary attributes to the resource, maintaining privacy as necessary.
  - **Convenience and security:** Single sign-on reduces opportunities for accounts to be compromised and also allows users to access any number of resources while signing on only once.

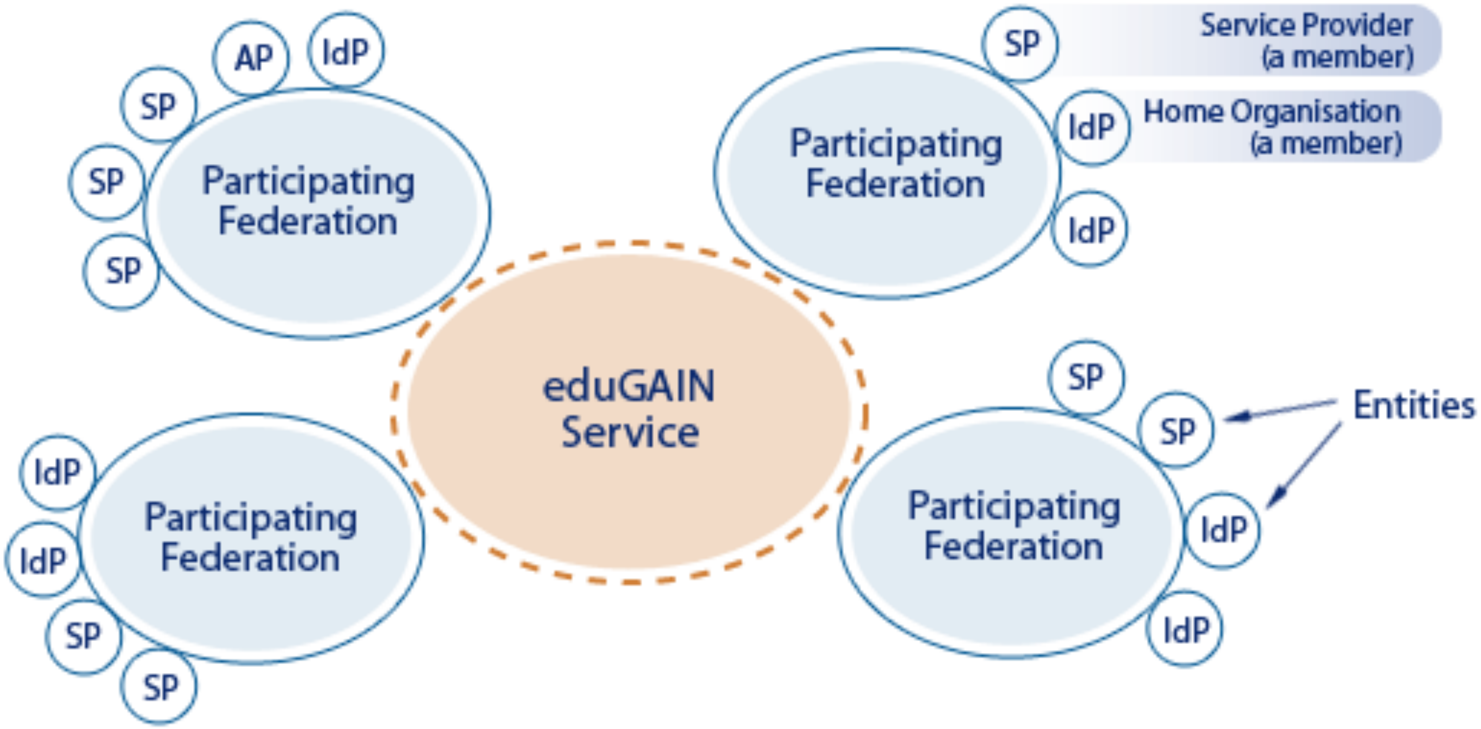
- Administrator Benefits
  - **Integrate** new users, services, and resource providers faster and easier
  - **Reduce** need for per-service account provisioning
  - **Extend existing** identity-management and resource services
  - **Create layers** of federation for various constituencies and consortia

World Wide Federation Map

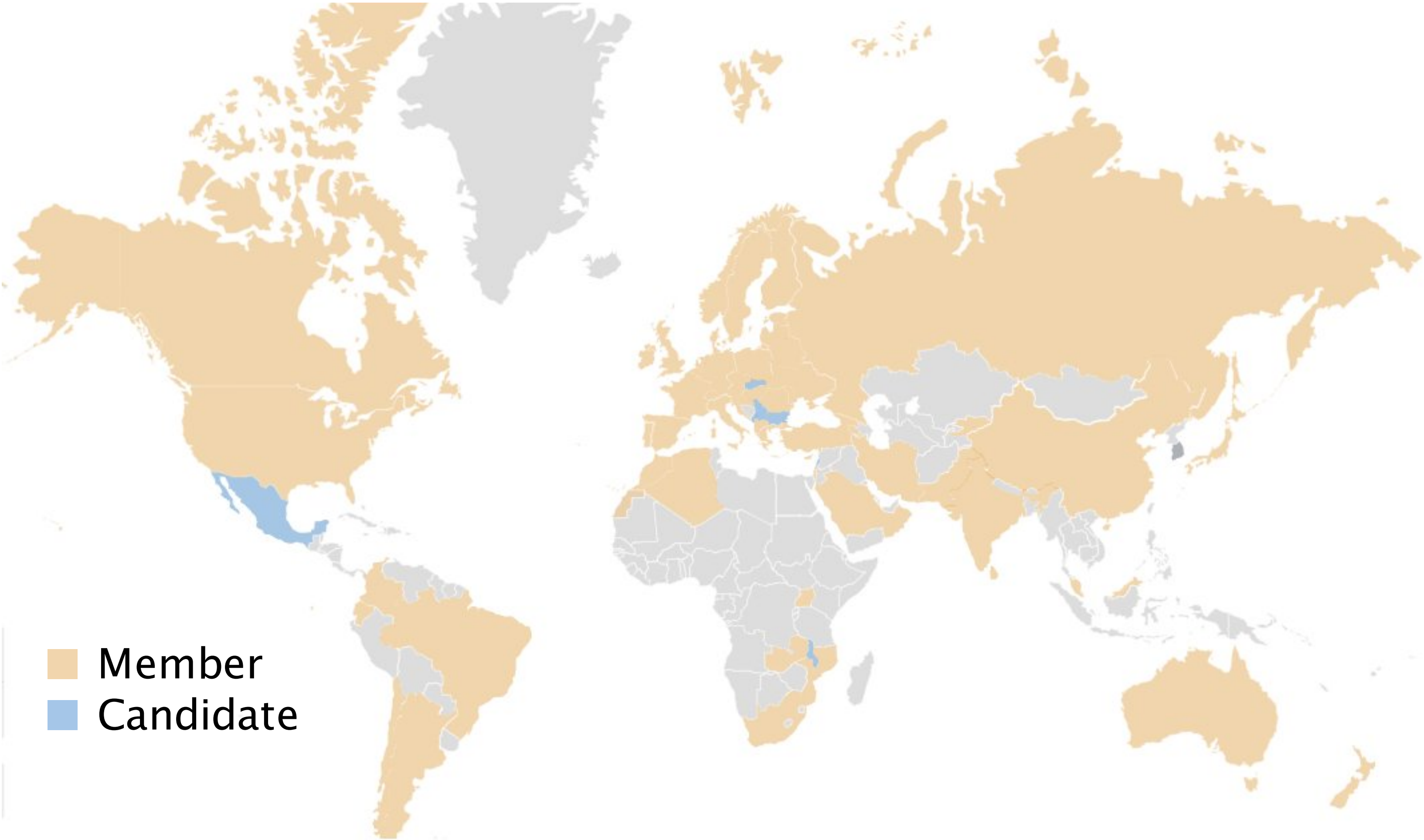
Interfederation

Interfederation by eduGAIN

PART OF THE GÉANT SERVICES PORTFOLIO



Federations in eduGAIN



Today’s Topics

- Overview of the Federation
- **Technical Information** (if necessary)

SAML and Shibboleth

SAML(Security Assertion Markup Language)

- Standard that allows secure web domains to exchange user authn and authz data
- Standardized by OASIS

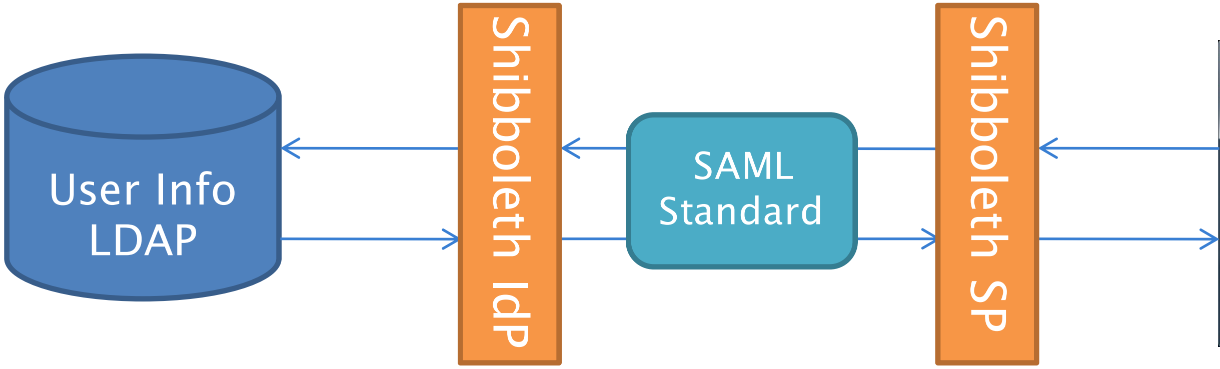
Shibboleth

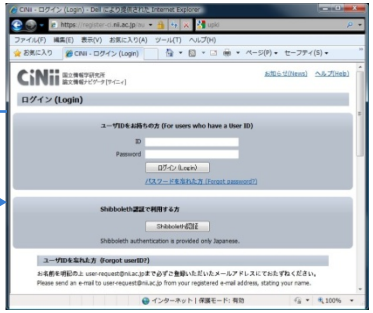
Shibboleth is a Middleware based on SAML

- Open Source project launched by EDUCAUSE/Internet2 in 2000
  - http://shibboleth.net/
- De facto standard in academic access management federation
  - Widely utilizes by European federations in addition to US
- simpleSAMLphp mainly utilizes by Nordic countries, will be the other choice

University

Resource Provider




CiNii - ログイン (Login) - Dell により提供された Internet Explorer
https://register-ci.nii.ac.jp/au
upki
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
お気に入り
CiNii - ログイン (Login)
ページ(P) セーフティ(S)
CiNii 国立情報学研究所 論文情報ナビゲータ[サイニィ]
お知らせ(News)
ヘルプ(Help)
ログイン (Login)
Shibboleth認証
インターネット | 保護モード: 有効
100%

ユーザIDをお持ちの方 (For users who have a User ID)

ID

Password

ログイン (Login)

パスワードを忘れた方 (Forgot password?)

Shibboleth認証で利用する方

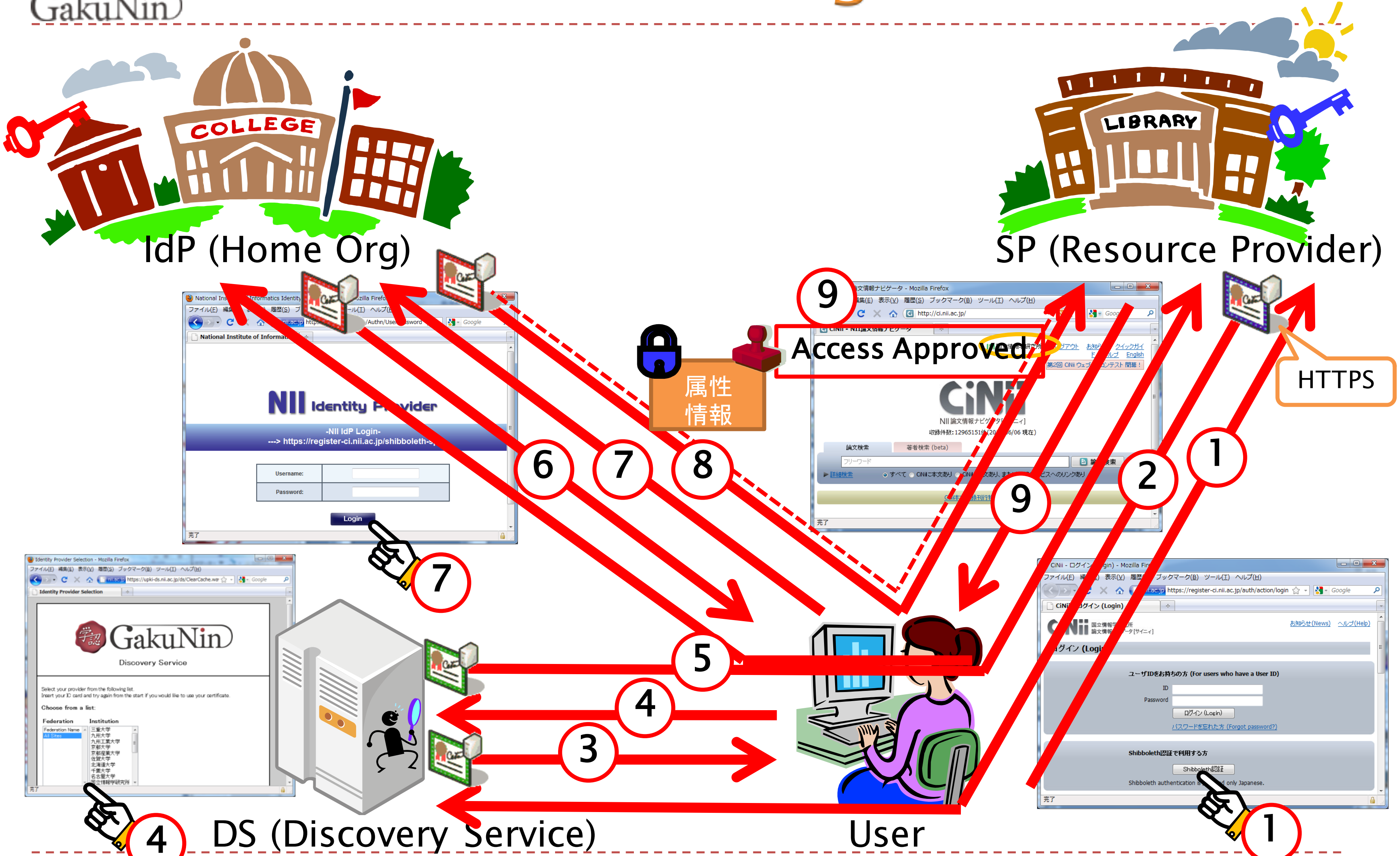
Shibboleth authentication is provided only Japanese.

ユーザIDを忘れた方 (Forgot userID?)

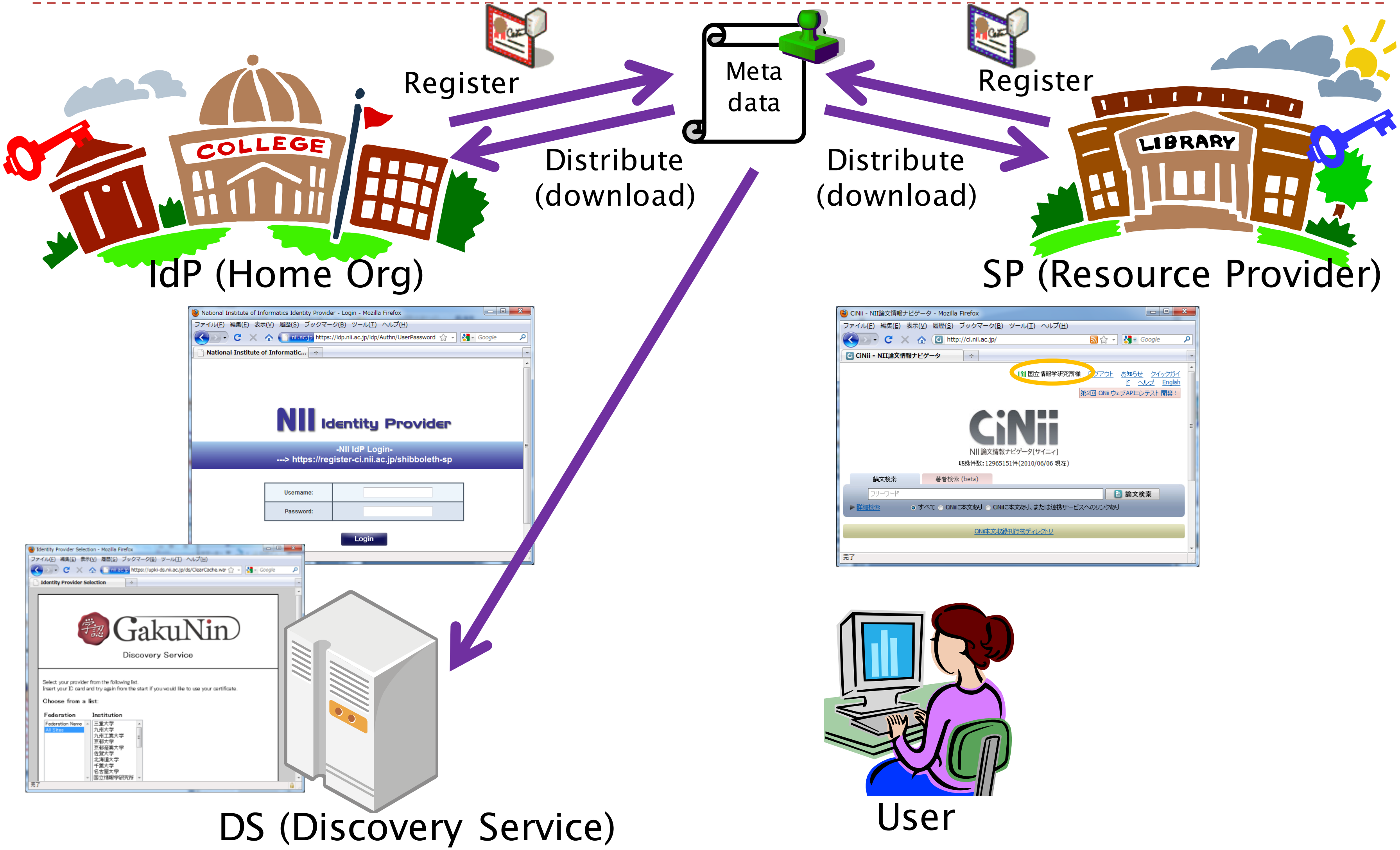
お名前を明記の上 user-request@nii.ac.jpまで必ずご登録いただいたメールアドレスにておたずねください。
Please send an e-mail to user-request@nii.ac.jp from your registered e-mail address, stating your name.

Something like a Filter which mediates SAML message

Shibboleth Flow Diagram



Building Relying Party by Metadata



National Institute of Informatics Identity Provider - Login - Mozilla Firefox

https://idp.nii.ac.jp/idp/Authn/UserPassword

NII Identity Provider

-NII IdP Login-
---> https://register-ci.nii.ac.jp/shibboleth-sp

Username:	
Password:	

Login

Identity Provider Selection - Mozilla Firefox

https://upki-ds.nii.ac.jp/ds/ClearCache.war

GakuNin Discovery Service

Select your provider from the following list.
Insert your IC card and try again from the start if you would like to use your certificate.

Choose from a list:

Federation	Institution
Federation Name All Sites	三重大学 九州大学 九州工業大学 京都大学 京都産業大学 佐賀大学 北海道大学 千葉大学 名古屋大学 国立情報学研究所

CiNii - NII論文情報ナビゲータ - Mozilla Firefox

http://ci.nii.ac.jp/

国立情報学研究所様 ログアウト お知らせ クイックガイド ヘルプ English

第2回 CiNii ウェブAPIコンテスト 開幕！

CiNii
NII 論文情報ナビゲータ[サイニィ]
収録件数：12965151件(2010/06/06 現在)

論文検索 著者検索 (beta)

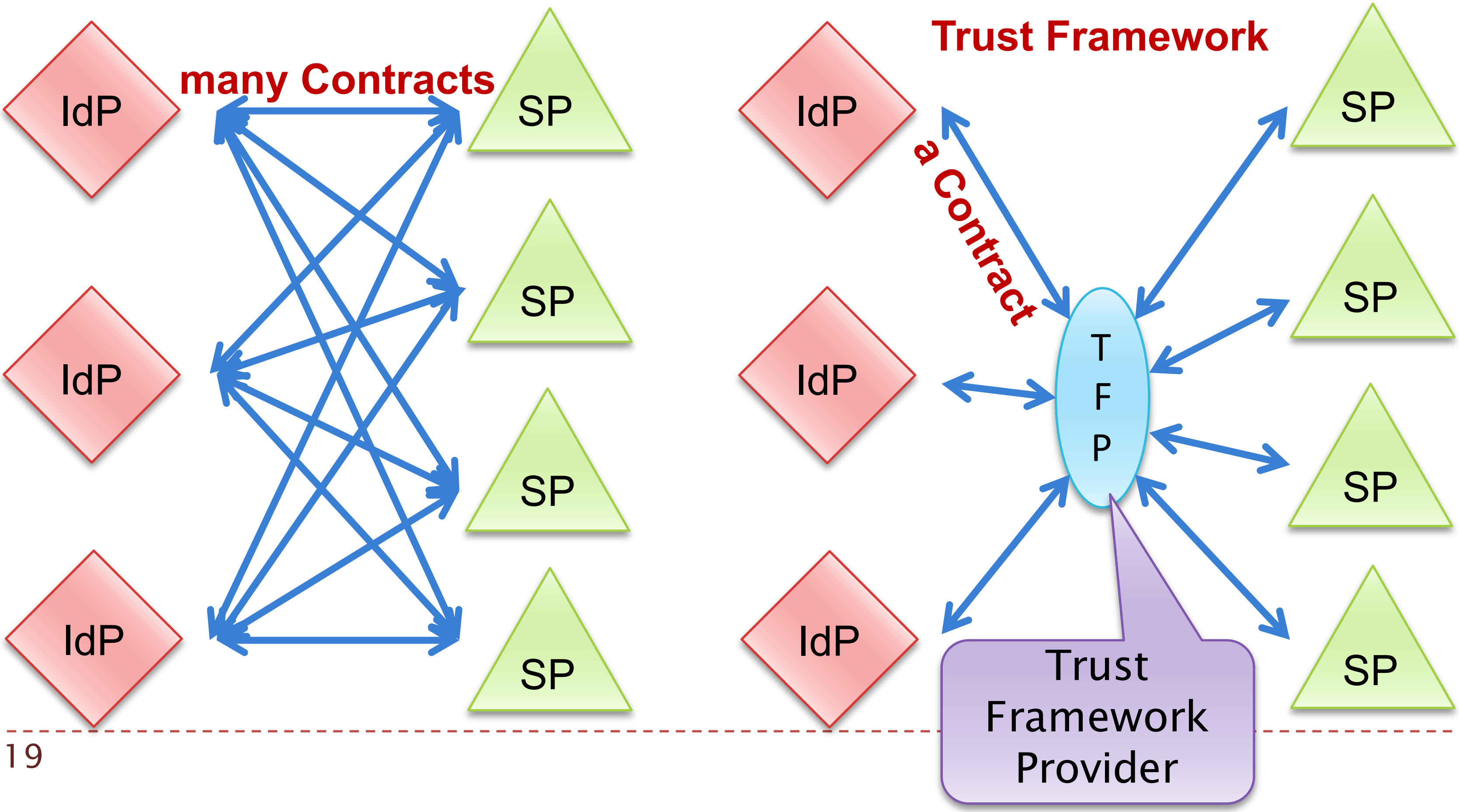
フリーワード 論文検索

▶ 詳細検索 ● すべて ○ CiNiiに本文あり ○ CiNiiに本文あり、または連携サービスへのリンクあり

CiNii本文収録刊行物ディレクトリ

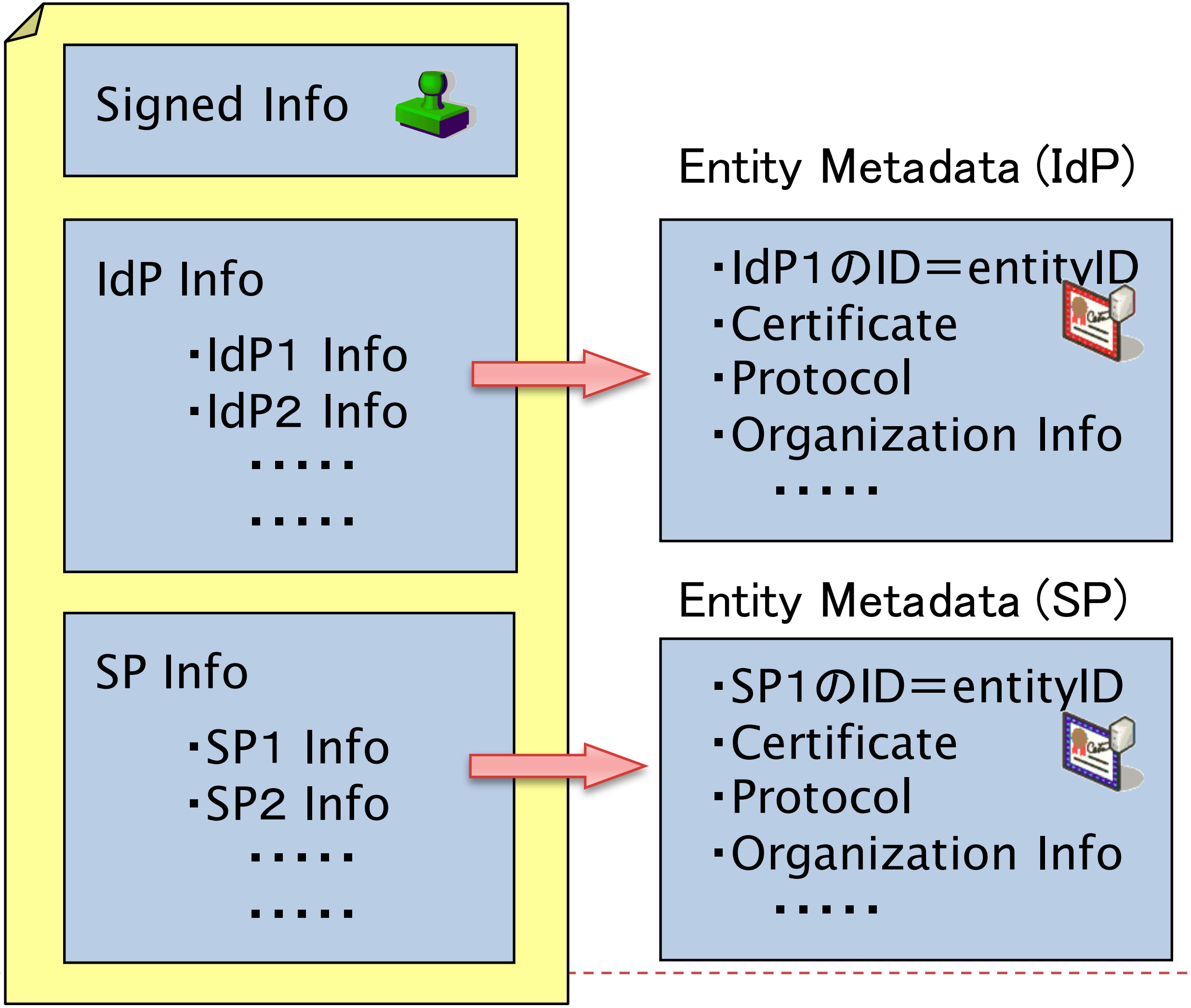
Effectiveness of trust framework

- Number of contract can be reduced from N×M to N+M by introducing a uniform policy



Contents of Metadata (XML)

Federation Metadata ≒ relying party



Signed Info

IdP Info

- ･IdP1 Info
- ･IdP2 Info

･･････

･･････

SP Info

- ･SP1 Info
- ･SP2 Info

･･････

･･････

Entity Metadata（IdP）

- ･IdP1のID＝entityID
- ･Certificate
- ･Protocol
- ･Organization Info

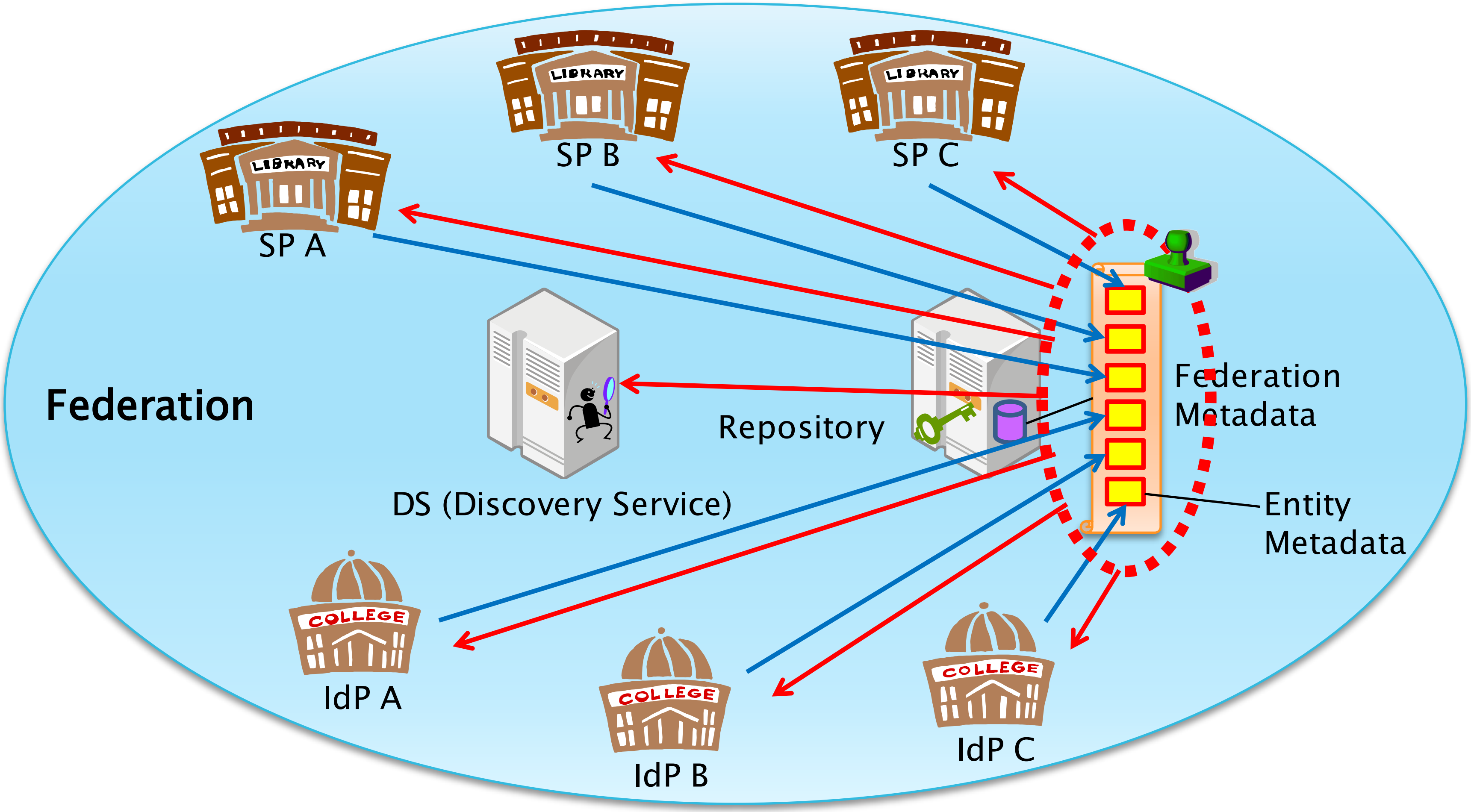
･･････

Entity Metadata（SP）

- ･SP1のID＝entityID
- ･Certificate
- ･Protocol
- ･Organization Info

･･････

Building Relying Party by Metadata



Reliability of the relying party is confirmed by the singed metadata.

17 Attributes Utilized by GakuNin

Name (abbreviation)	Description
OrganizationName (o)	English name of the organization
jaOrganizationName (jao)	Japanese name of the organization
OrganizationalUnit (ou)	English name of a unit in the organization
jaOrganizationalUnit (jaou)	Japanese name of a unit in the organization
eduPersonPrincipalName (eppn)	Uniquely identifies an entity in GakuNin
eduPersonTargetedID	A pseudonym of an entity in GakuNin
eduPersonAffiliation	Staff, Faculty, Student, Member
eduPersonScopedAffiliation	Staff, Faculty, Student, Member with scope
eduPersonEntitlement	Qualification to use a specific application
SurName (sn)	Surname in English
jaSurName (jasn)	Surname in Japanese
givenName	Given name in English
jaGivenName	Given name in Japanese
displayName	Displayed name in English
jaDisplayName	Displayed name in Japanese
mail	E-mail address
gakuninScopedPersonalUniqueCode	Student or faculty, staff number with scope

Static

Not much used

Generate from ID

Generate LDAP tree

Not much used

Not so difficult to map the Shib Attr and LDAP

3 types of access on privacy

- Anonymous
  - Any identifier is not sent
  - Fit for e-Journals (a member (of a department) of the organization can access)
- Autonymous
  - eduPersonPrincipalName is sent
    - Unique identifier shared by all SPs (globally unique)
    - Similar to e-mail address
- Pseudonymous
  - eduPersonTargetedID is sent [hash(ePPN, entityID of SP)]
    - Persistent unique identifier to each SP
  - To avoid correlation of user activities among SPs