Toward campus portal with shibboleth middleware

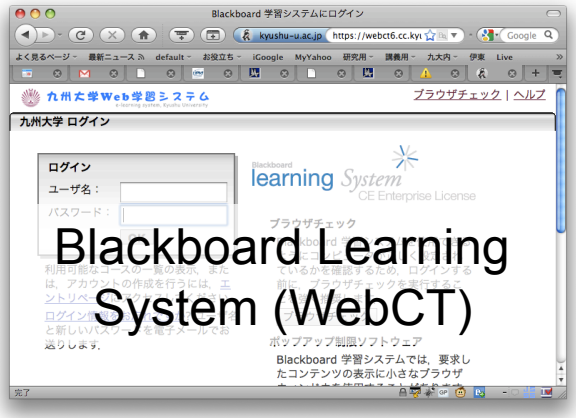
Eisuke Ito and Masanori Nakakuni
itou@cc.kyushu-u.ac.jp, Kyushu University
nak@fukuoka-u.ac.jp, Fukuoka University

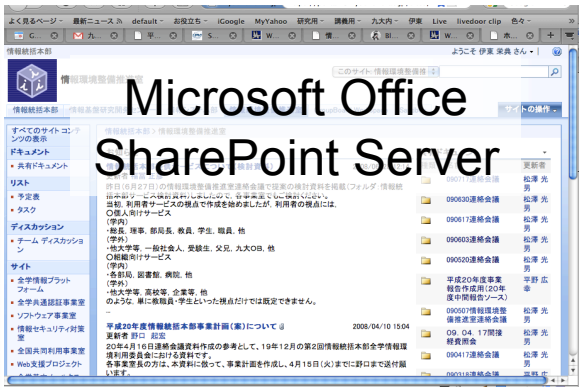
Outline

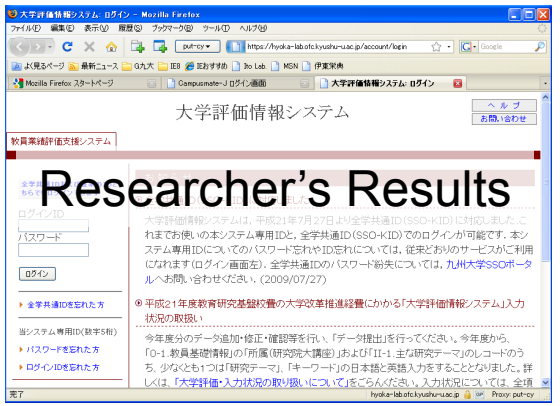
1. Background
2. Shibboleth
3. Campus portal
4. Solution
5. Conclusion

1. Background

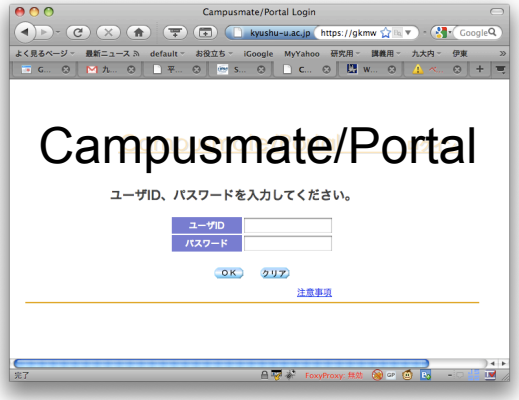
- Closed/Private web services increase in University
  - WebCT, e-Syllabus, researcher & resources, student portal, etc…
  - Those systems are independently implemented.
- Single ID/PW and SSO (Single Sign-on)
  - Unify ID&PW (Single ID/PW)
  - SSO
    - Reverse proxy type SSO system will be installed.
    - Shibboleth SSO system is installing.
- But, Information sources are still distributed.
  - Campus portal is required to realize one stop service

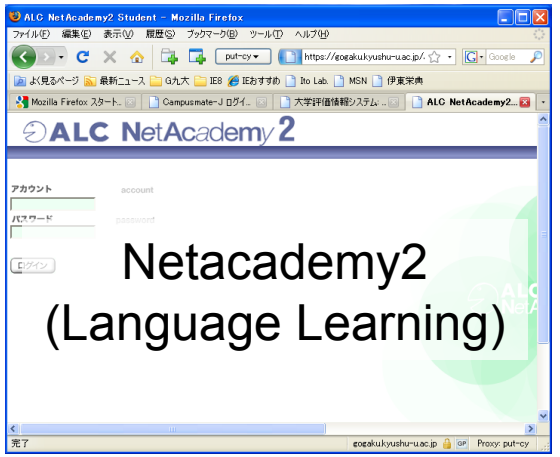

Blackboard Learning System (WebCT)

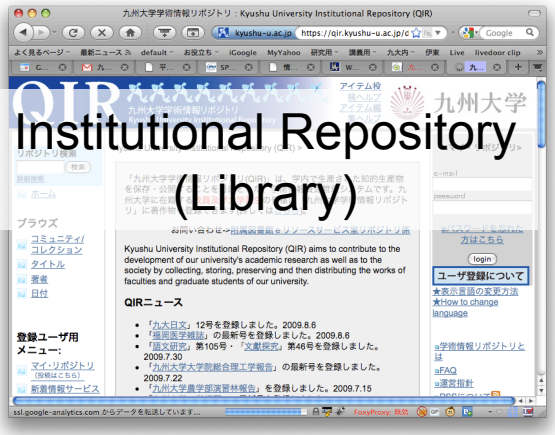

Microsoft Office SharePoint Server

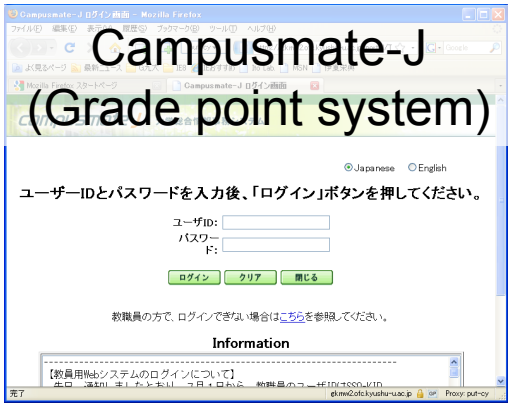

Researcher's Results

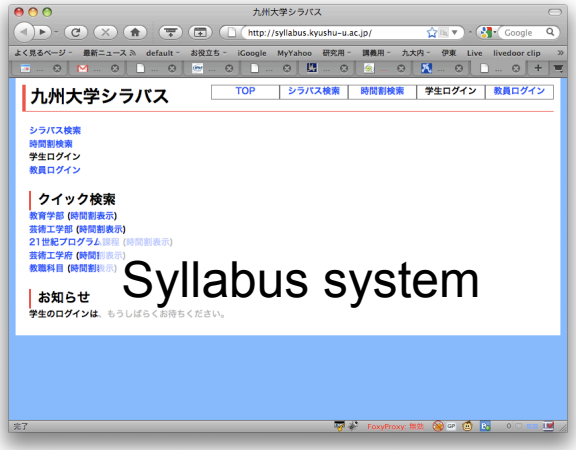

Mirapoint Web Mail


Campusmate/Portal


Netacademy2 (Language Learning)


Institutional Repository (Library)


Campusmate-J (Grade point system)


Syllabus system

1. Background (Cont.)

- Problem: it is difficult to gather information from private services
- Distributed web SSO (single sign on) systems are developed
  - such as *OpenID* and *Shibboleth*
  - NII of Japan deploys Shibboleth SSO
    - Common (Uniformed/standardized) SSO platform may appear.
  - Kyushu university is installing Shibboleth IdP
- Common platform makes easy to exchange data between systems.

Goal

- We are constructing common SSO platform with Shibboleth.
- On the platform, we may establish something method for information exchange between private services.
- And make a university portal

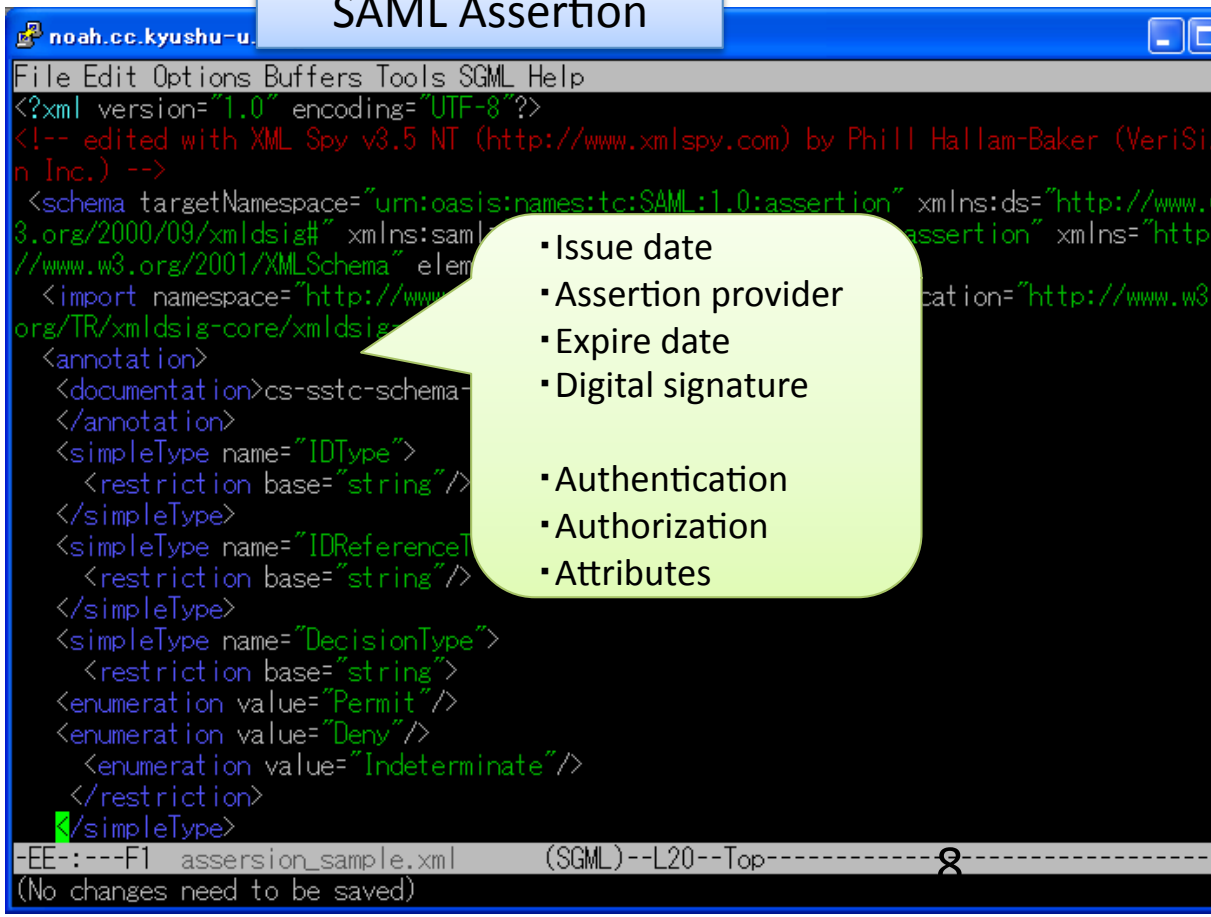
Outline

1. Background
2. Shibboleth
3. Campus Portal
4. Solution
5. Conclusion

SAML

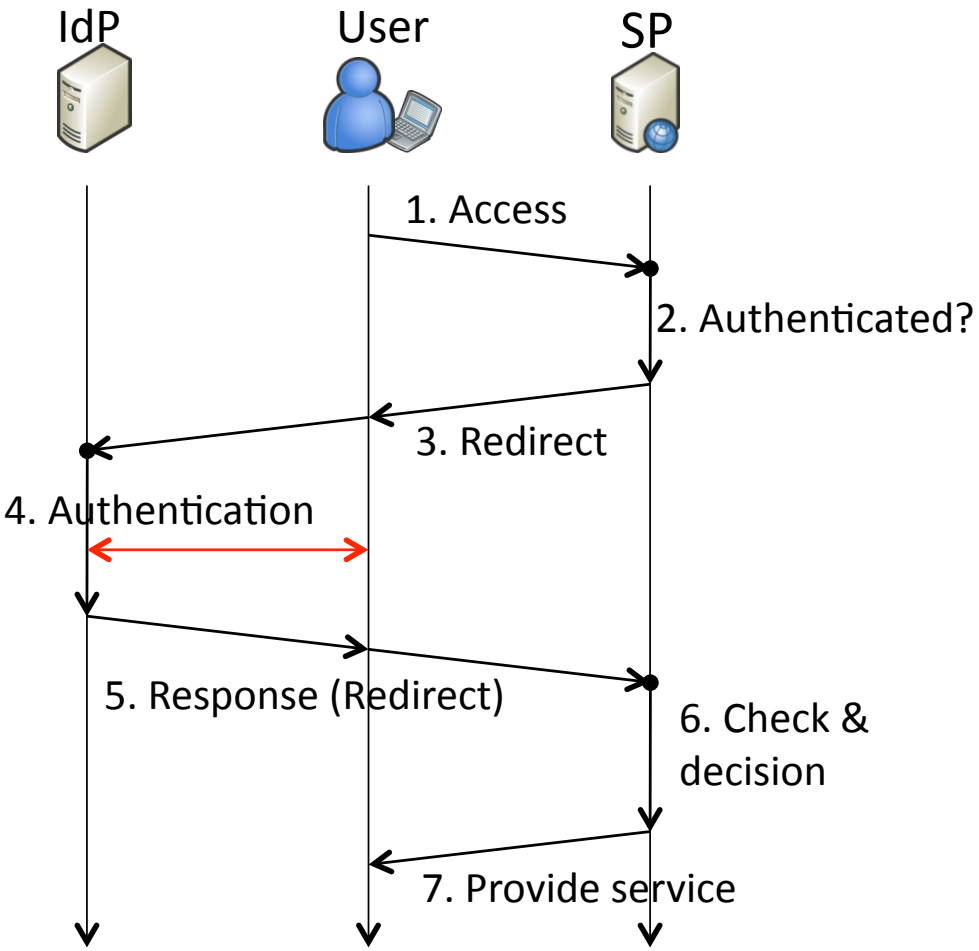
- SAML (Security Assertion Markup Language)
  - XML based data exchange protocol defined by OASIS
  - http://docs.oasis-open.org/security/saml/v2.0/
- 3 players
  - User and browser
  - IdP（Identity Provider）
    - User account, authentication
  - SP（Service Provider）
- SAML assertion
  - Authentication
  - Attribute
  - Authorization Decision
  - SAML over HTTP
  - SAML over SOAP

SAML Assertion



SAML

(Security Assertion Markup Language)



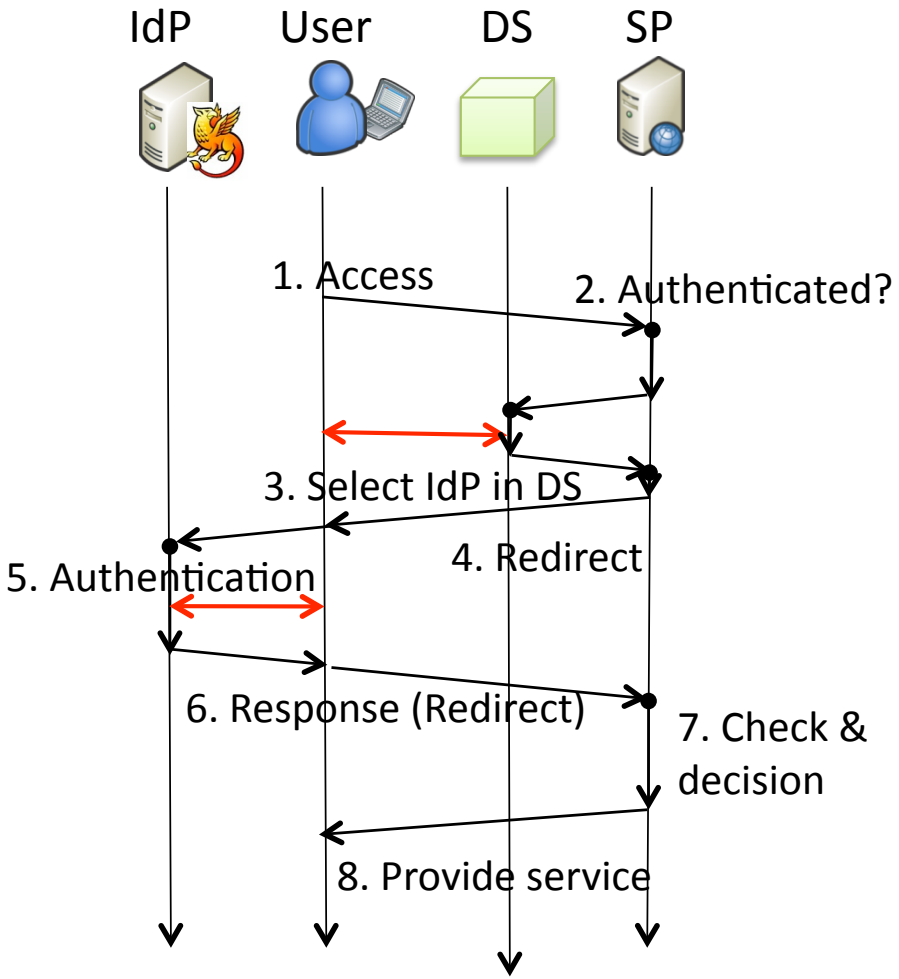
1. A user accesses to an SP.
2. SP checks authenticated or not. If not, SP make a SAML authentication request.
3. SP returns redirection message to IdP.
4. User enter his/her credential to the IdP.
5. IdP returns message to redirect SP
6. SP decides to provide service or not, based on returned SAML assertion.
7. SP provides service to the user.

IdP must be fixed for SP.

Shibboleth

- A Web SSO middleware (developed by Internet2)
  - http://shibboleth.internet2.edu/
- Assumption
  - User may belong with an organization.
  - The organization may issue one's credential such as ID/PW for user authentication.
- 4 Players
  - User and browser
  - IdP (Identity Provider)
  - SP (Service Provider)
  - DS (Discovery Service) ….
    - User selects his/her IdP (or Organization)
    - It was called WAYF（Where are you form?）in Shibboleth ver. 1.x
- Attribute based authorization
  - Organization may manage user account
  - User's attributes may be also manage users attributes

Shibboleth

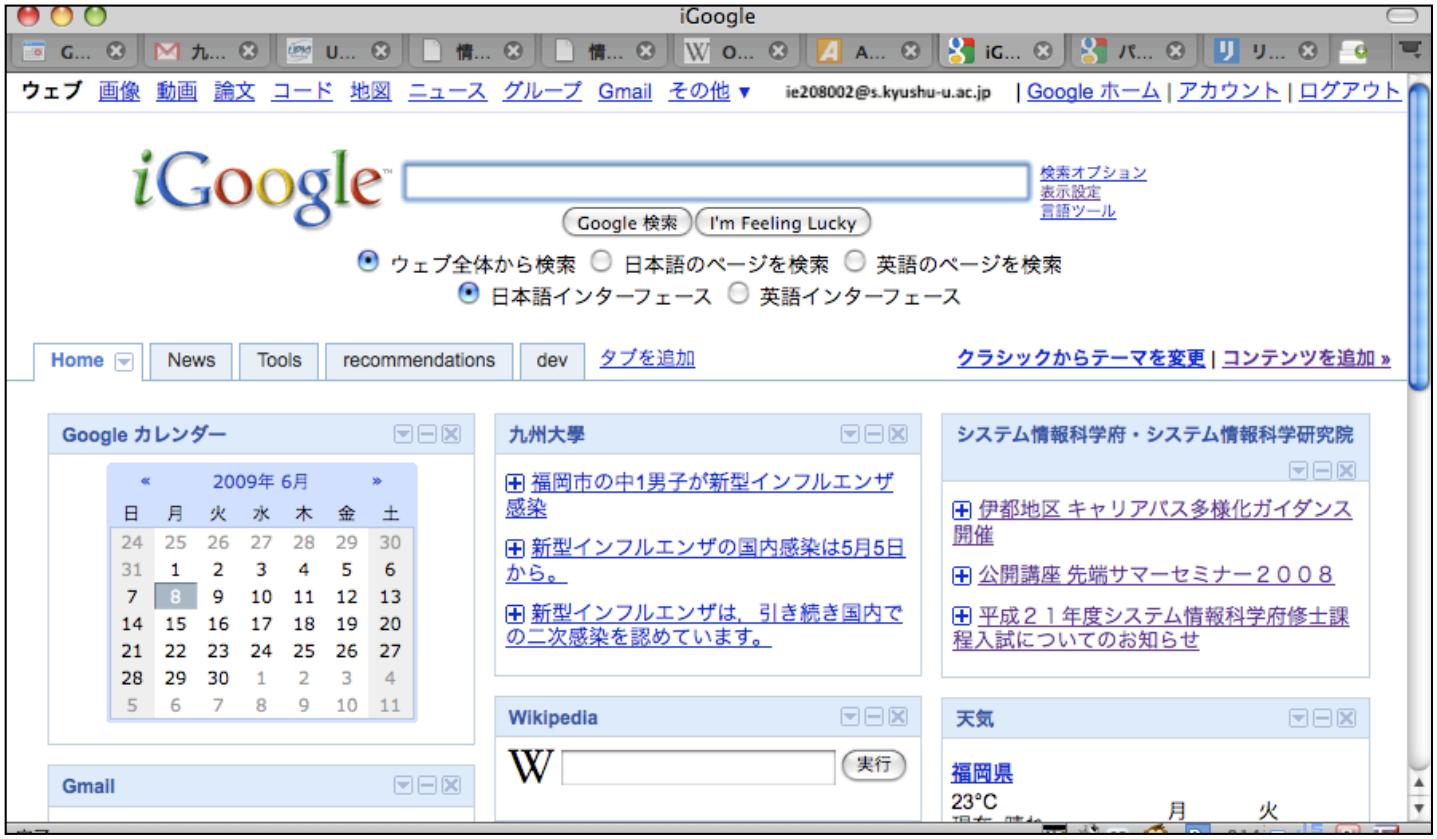


1. A user accesses to an SP.
2. SP checks authenticated or not. If not, SP makes a SAML authentication request.
3. Select his/her IdP in DS process
4. SP redirects to the IdP.
5. User enter his/her credential to the IdP.
6. IdP returns message to redirect SP
7. SP decides to provide service or not, based on returned SAML assertion.
8. SP provides service to the user.

3. Campus Portal

- Portal is a web site that is a major starting site for users when they get connected to the web or that users tend to visit as an anchor site.
- Campus portal
  - One stop service for users
  - Good notice board for officials

iGoogle



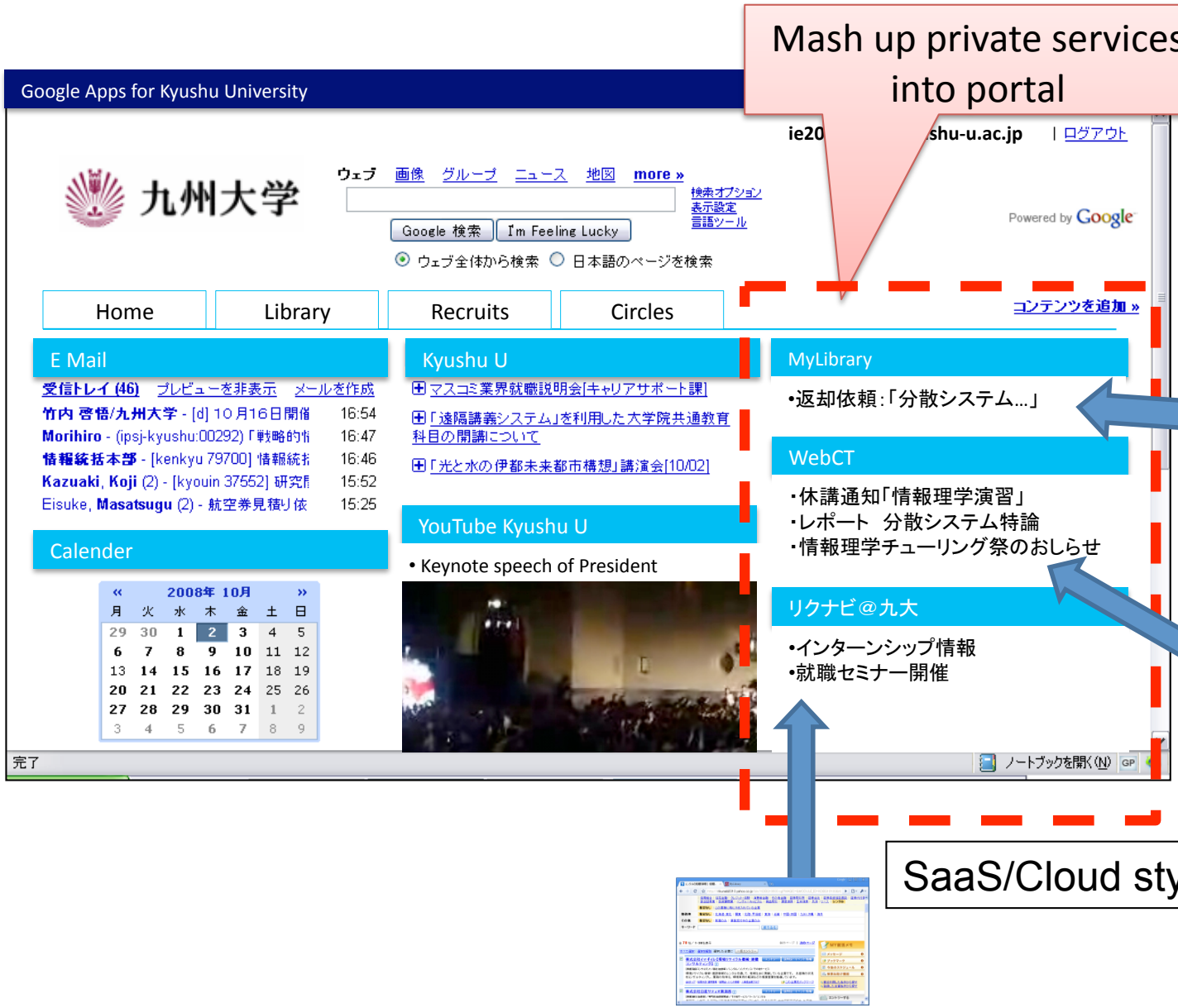
The start page of google apps (iGoogle) …. (Start page is not available, now.)

- It can include various site information with google gadget.
- It can use SAML based authentication（Shibboleth）

Yahoo! JAPAN


My Yahoo! - トップ
http://cm.my.yahoo.co.jp/
what is portal
MY YAHOO! JAPAN BETA
ウェブ 登録サイト 画像 動画 ブログ 辞書 知恵袋 地図 商品
検索
Yahoo! JAPAN - ヘルプ
トップ
+ページの追加
こんにちは、eisuke_itohさん [ログアウト]
メニューリスト
コンテンツの追加
My Yahoo!の設定
>>制限事項のお知らせ
活用ガイド
辞書検索
急上昇ワードランキング
Yahoo!ニュース - テクノロジー - BCN
・[新製品]レノボ・ジャパン、日本の個人向けノートPCを拡充、薄型「IdeaPad U350」など(BCN) - 2009/8/20 12:47
・[特集]PCでラジオのメリットとは？ 意外に使えるユニークなラジオたち(BCN) - 2009/8/20 12:45
・[経営戦略]Loilo、第三者割当増資を機に米国オフィスを開設、世界展開を本格化(BCN) - 2009/8/20 10:09
・[サービス]ライド、USBキーを使ったネットワークストレージサービスをオプション提供(BCN) - 2009/8/20 10:09
・[新製品]三菱電機、HDD/BD両方のレコーダーを内蔵した液晶テレビなど、AV関連新製品(BCN) - 2009/8/19 19:41
RSSコンテンツ
つながるMy Yahoo!
新着通知 注目記事 友だちに教える 知恵袋に聞く
人気記事ランキング
期間限定！「ドラゴンクエストIX」がMy Yahoo!の背景テーマに登場 -マイ★ブーム ～My Yahoo!編集部ブログ～
テーマ別のコンテンツをまとめて追加！「コンテンツセット」
トピックス
トピックス 経済 エンタメ スポーツ その他
国内
がん克服の元落語家 覚せい剤
ストーカー 積極事件化を指示
海外
アフガン大統領選、投票開始
アフガンでTBSカメラマン拘束
コンピュータ
サイバー犯罪過去最多に 上期
世界初 HDDとBD内蔵の液晶TV
サイエンス
小笠原 世界遺産へ外来種の壁
洪水に強いイネの遺伝子特定
地域
ウソ通報で警察好き少年逮捕
逮捕され死んだふり2時間半
生徒暴行の元コーチ無罪主張
阿久根市長 ブログに支持候補
在日中国人が生活保護費詐取
今日/明日の天気
福岡県 - 福岡(福岡)
今日の天気
最高33℃ 10%
最低27℃
明日の天気
最高32℃ 20%
最低27℃
衛星画像 - 天気図 - アメダス
指数情報: 紫外線 - ビール - 汗かき
PR
1800ページ以上 無料 イッキ読み スペシャル!
夏休み限定 週刊少年ジャンプ特集 なんと22作品
©SHUEISHA Inc.
パーソナルアシスタント
メール - 新着メール326通
2009年8月20日(木)
日 月 火 水 木 金 土
26 27 28 29 30 31 1
2 3 4 5 6 7 8
9 10 11 12 13 14 15
16 17 18 19 20 21 22
23 24 25 26 27 28 29
30 31 1 2 3 4 5
完了
FoxyProxy: 無効

An image of campus portal



Private services of Kyushu U

- MyLibrary

- WebCT

SaaS/Cloud style service

Problem of campus portal

- Difficult to integrate independent private services
  - How to extract information pieces from each sites?
  - How to pass through user authentication?
    - This is a barrier.
    - Common web SSO may make easier to break this barrier.

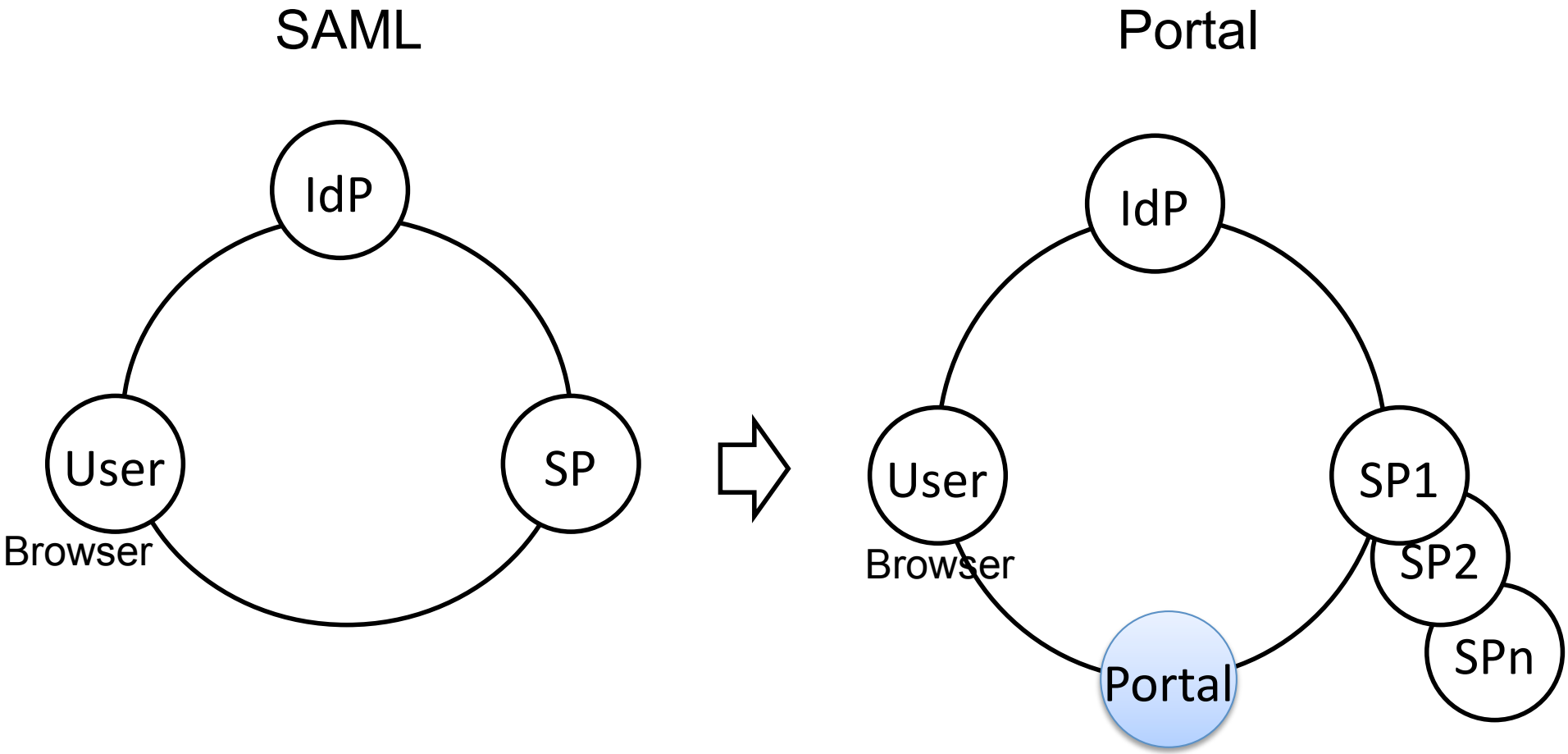
Outline

1. Background
2. Shibboleth
3. Campus Portal
4. Solutions
5. Conclusion

4. Solutions

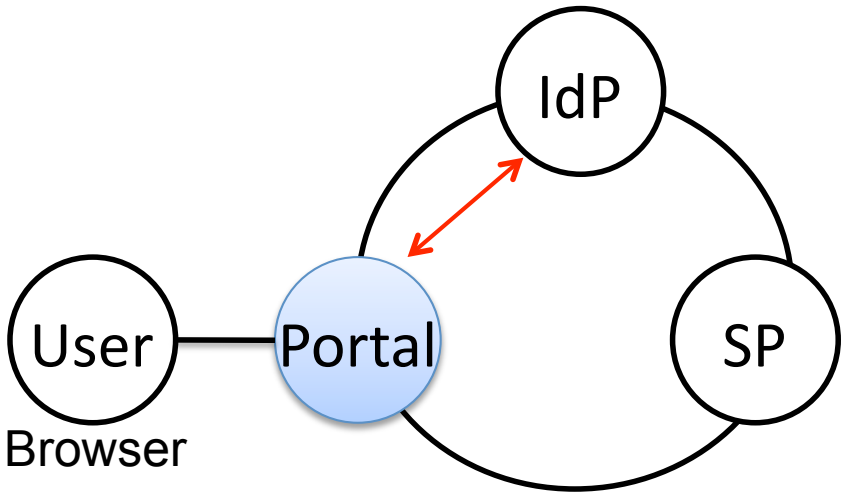
- We need a data exchange method between private services.
- We studied 4 methods
  1. HTTP proxy
  2. HTTP binding
  3. Artifact binding
  4. Unsolicited Response

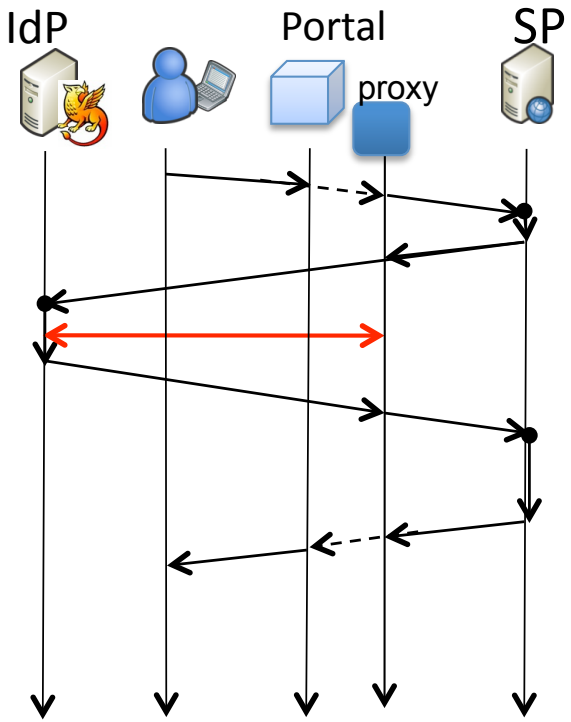
    - Above 2, 3, and 4 are proposed by M. Aoyagi et al. in this article.
      - Makiko Aoyagi, Manabu Okamoto, Michio Shimomura, “A study of authentication methods in Web service mash-up” IEICE SCIS 2009, 4D1-4, 2009. (in Japanese)


SAML
IdP
User
Browser
SP
Portal
IdP
User
Browser
SP1
SP2
SPn
Portal

(1) HTTP Proxy

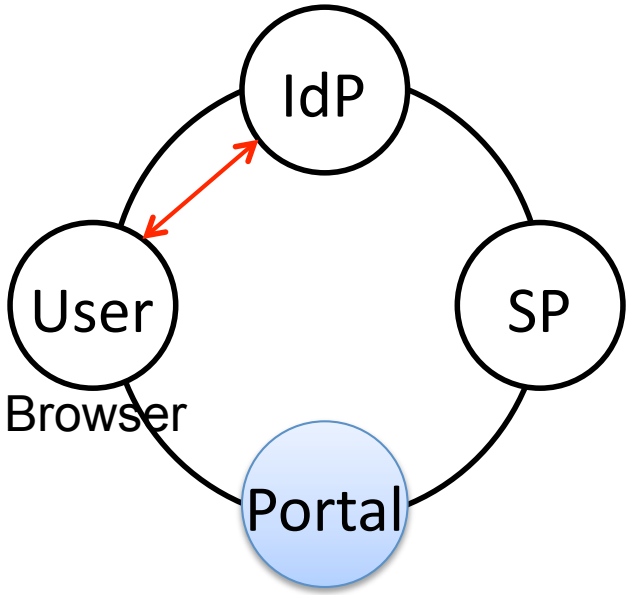
- User entrusts ones credential to portal.
  - Portal must be trustworthy.
- Portal acts as proxy of user (browser)
  - it sends user's ID/PW to SP or IdP.

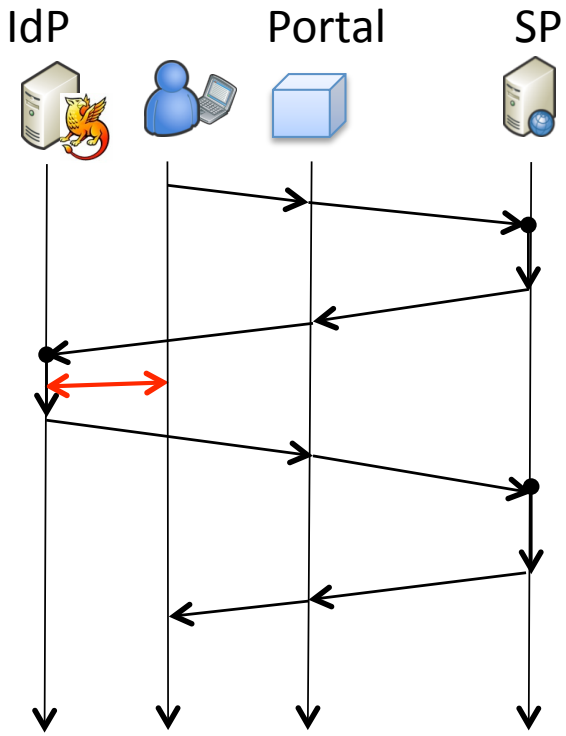




(2) HTTP Binding

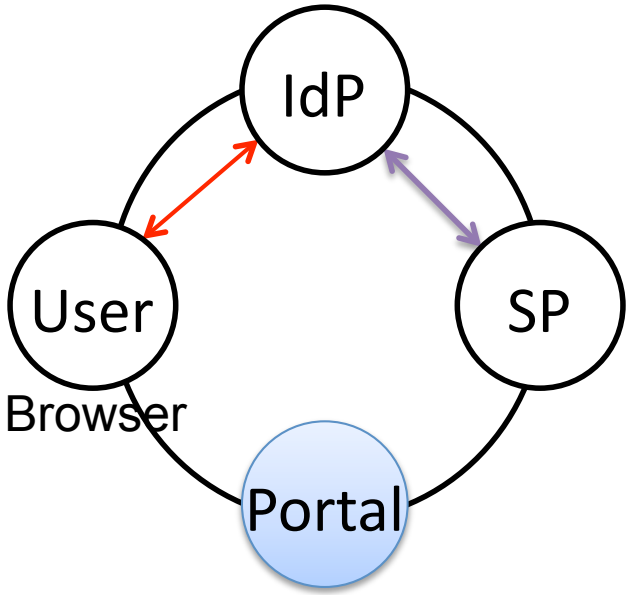
- Portal, SP, and IdP exchange SAML data directory.
  - After authentication at IdP, SP returns response, and returns information of SP using agent.

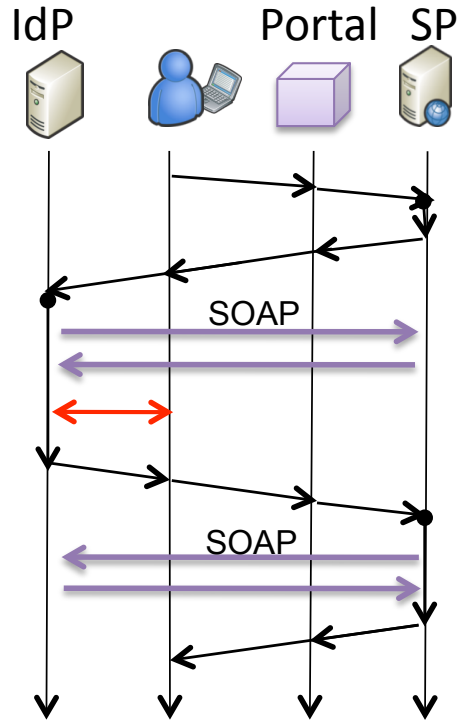




(3) Artifact Binding

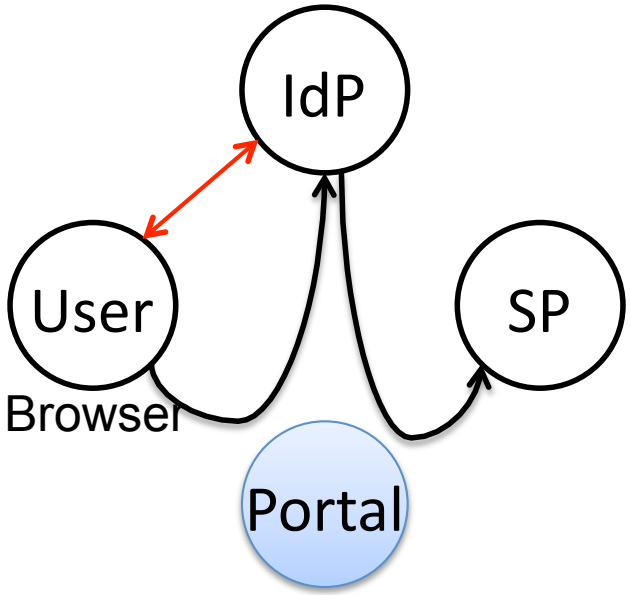
- IdP and SP exchange artifacts, where artifacts include session information.

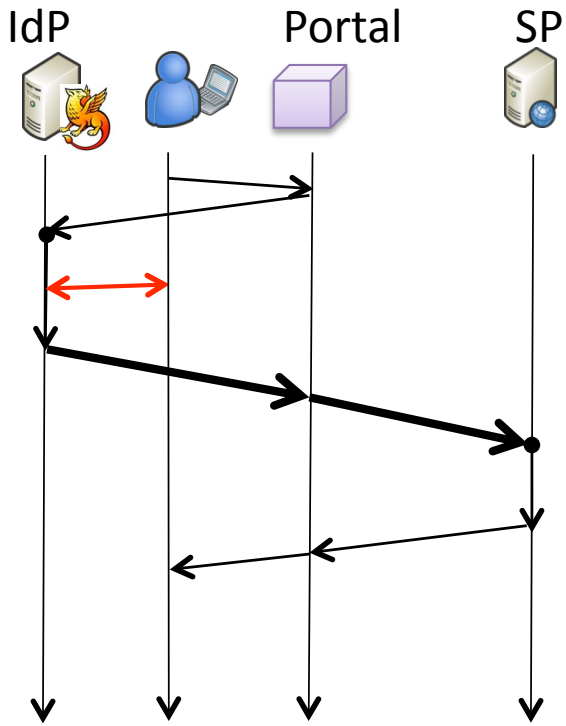




(4) Unsolicited Response

- IdP sends unsolicited response to SP.
- SP receives the unsolicited response, and invokes response process.





Comparison of each methods

- Each methods is familiar with SAML and Shibboleth

	HTTP Proxy	HTTP Binding	Artifact Binding	Unsolicited Response
SP	Specify IdP	Specify IdP	Specify IdP Additional SOAP process	Must supports unsolicited response.
IdP			Additional SOAP process	
Portal				
Merit	Easy to implement. Less portability.	Simple. Easy to implement.	Secure.	Simple. Easy to implement. Good for multiple SP's
Demerit	Portal becomes security bottle neck		Can't apply this method If communication between IdP and SP is limited.	

Prototype of HTTP Proxy

- Environments
  - IdP

OS	CentOS 5.1
Web	Tomcat 6.0
IdP	Shibboleth

  - SP

OS	CentOS 5.1
Web	Apache2.2
SP module	mod_shib2.2
Service	PukiWiki

  - Portal

OS	FreeBSD 7.0
Web Server	Apache 2.2
Programming	Ruby 1.8
HTTP User Agent	Mechanize 0.8

- Results
  - Success to integrate other service into portal.
  - But, not portable

5. Conclusion

- Common Shibboleth SSO platform makes easy to exchange data between closed/private services.
- On the platform, we may establish something method for information exchange between private services for campus portal.
- We studied 4 methods:
  - HTTP proxy
  - HTTP binding
  - Artifact binding
  - Unsolicited Response … (better than other)
- In the future,
  - Construct Shibboleth IdP
  - Shibbolize SPs
  - Make campus portal which integrates private services.