CARSI:
Cross University Identity Management and Resource Sharing over CERNET

Dr. PING CHEN
Peking University
Oct, 21st, 2008
Agenda

- Current AAI Situation over CERNET
- Our Plan: CARSI
- CARSI Components
  - CARSI Infrastructure
  - CARSI Federation Contract Negotiation & Audit
  - CARSI Federation Provider Registry
  - CARSI Virtual Resource Directory
  - CARSI OpenIdP
  - CARSI Services
- Current Deployment
- Conclusion
Application Authentication is developing.

University A
- Web Mail
- e-Learning

University B
- e-Journals
- Literature DB

University C
- Research DB
- e-Learning

Identity management
Authentication
Access control
Resource

北京大学 Peking University
Application Authentication is developing.

University A
- Web Mail
- e-Learning

University B
- e-Journals
- Literature DB

University C
- Research DB
- e-Learning

Identity management
Access control
Resource

北京大学 Peking University
Current AAI situation over CERNET

- AAI: Authentication & Authorization Infrastructure
- Most Univ. have campus-wide IDM, identity management
- Univ. web applications run in two ways:
  - No AA, accessed publicly without protection
  - With AA, only be visited by a closed set of users
- Cross-univ. AAI is important to resource sharing
  - Sharing object can be user identity
  - Sharing object can also be web applications
Application Authentication is developing.

北京大学 Peking University
Our Plan: CARSI

Cernet Authentication and Resource Sharing Infrastructure

Goals:

- To integrate university IDMs to a CERNET AAI federation
- To share univ. user account resources over CERNET
- To share existing protected web application resources from a closed set of users to CERNET federation users
- To protect existing unprotected web applications
- To provide a basic AAI middleware for CERNET applications
- To standardize and simplify application’s upgrade to AAI-protected
- To push new applications among universities

北京大学 Peking University
Shibboleth

- An Internet2 Middleware Initiative
- Designed for exchanging attributes across security domains - universities
- Supports cross-domain Single Sign-On and resource sharing
- Network applications of one domain trust authentication results provided by other domains
- Fine-grained application authorization is based on attributes exchanged between different domains.
- Adopted by about 20 NREN, such as: inCommon, SWITCH, …
- Based on SAML standard

北京大学 Peking University
Work flow of Shibboleth
CARSI Components

CARSI-Portal
- Web-Portal
- CARSI-Uid
- CARSI-WAYF
- CARSI-VRD

CARSI-FPR
- Admin Mgmt
- Provider Mgmt
- Provider Register

CARSI-IdP
- SSO Service
- Attribute Release
- Authn Authority
- User DB
- DT/CAS/DB/LDAP/Others

CARSI-FPR
- SAML/Shibboleth

CARSI-FCN
- Contract & Negotiation
- User Tracing
- Inter-visit Stat
- Log Collector
- Log Analyzer

CARSI-OpenIdP
- SSO Service
- Attribute Release
- Authn Authority
- Local Authn
- User DB
- BBS/IPGW/NM/S/DT/LIB/ERP/Others

CARSI-Uid
- CARSI-SP
- Assertion Consumer
- Access Control

CARSI-Fed

北京大学 Peking University
1. CARSI infrastructure

- CARSI-Fed: cross-domain federation
- CARSI-portal
  - A web portal for fed user to login
  - A web portal providing a resource list for fed users
- CARSI-WAYF/DS: where are you from
- CARSI-VRD: Virtual Resource Directory
- CARSI-Person: CARSI User Attribute Specification
  - CARSI-Uid (Universal user identity): localid@domainid
- CARSI-IdP: shibboleth IdP +
- CARSI-SP: shibboleth SP +
CARSI Workflow

- **Way 1:**
  1. Portal login
  -> 2. select application from resource list
  -> 3. visit web application
  -> 4. visit other applications, SSO

- **Way 2:**
  1. visit a web application
  -> 2. redirected to portal to login
  -> 3. visit application
  -> 4. visit other applications, SSO
Infrastructure Workflow
Way 1 Demo

Web browser

CARSId
IdP

CARSId
Portal

CARSId
VRD

CARSId
WAYF

CARSId
SP

Application

北京大学
Peking University
Infrastructure Workflow
Way 1 Demo

1. login with CARSI-Uid

- Web browser

- CARSI
  - IdP

- CARSI Portal

- CARSI SP
  - VRD
  - WAYF

- CARSI SP
  - Application
Infrastructure Workflow
Way 1 Demo

Web browser

2. Redirect to IdP
3. Pass auth, redirect to VRD

4. Resource list returned to user

CARSI IdP
CARSI Portal
CARSI SP
CARSI VRD
CARSI WAYF

CNG106 基于CNGI网络环境的跨机构统一认证与授权
北京大学 Peking University
Infrastructure Workflow
Way 1 Demo

5. Select an application to visit
6. Visit SP-protected application
7. First time visit the resource, redirect to WAYF
8. Redirect to visiting user’s IdP
9. The user has passwd auth, redirect to SP

Web browser

CARSI IdP
CARSI Portal
CARSI VRD
CARSI WAYF
CARSI SP
CARSI SP Application
Infrastructure Workflow
Way 1 Demo

10. Pass authorization, user accesses application

Web browser

CARSId P

CARSIS P

CARSIPortal

CARSIVRD

CARSISWAYF

CARSIS Application

北京大学Peking University
2. CARSI FCNA

Federation Contract Negotiation & Audit

Goal:
- How many and what kind of influences does cross-domain AAI bring to users(IdP) and applications(SP)?
- How is CARSI being used? What’s user’s using habit?

Methods:
- Federation log record, aggregation and analysis: IdP log, SP log, Portal log, WAYF log, etc.
- Resource sharing statistics
  - Based on IdP, how many IdP users visit other-domain applications, their using habit, etc
  - Based on SP, which domain and what kind of users visit it, what is the peak visiting time, etc
- User’s behavior and action tracking
  - Tracing user’s visiting sequence
  - Which visiting sequence is more adopted?
  - How cross-domain AAI benefit them?
CARSI FCNA interfaces
3. CARSI FPR: Federation Provider Registry

- A system for federation members to manage domain/IdP/SP by themselves
- Administrator management is one function:
  - Role based: FedAdmin, OrgAdmin, IdPAdmin, SPAdmin
- IdP/SP management is another function:
  - Followed with corresponding management policy
- IdP/SP/Admin policy
3. CARSI FPR: Federation Provider Registry

- **FedAdmin**
  - To manage member administrator accounts and member IdP/SPs

- **OrgAdmin**
  - To manage Admins of a domain/university
  - Activated by paper documents stamped with organization seal
  - 1 domain may have multiple admins with OrgAdmin role

- **IdPAdmin**
  - To manage 1 IdP
  - Activated by OrgAdmin or other IdPAdmin for the same IdP
  - 1 IdP may have multiple admins with IdPAdmin role

- **SPAdmin**
  - To manage 1/n SPs
  - Activated by OrgAdmin or other SPAdmin for the same SP
  - 1 SP may have multiple admins with SPAdmin role
4. CARSI VRD: Virtual Resource Directory

- A list of sharing web applications
- One part of CARSI-Portal
- Synchronized with FPR-registered SPs
- SP protected
- Classified and exhibited for user access
5. CARSI-OpenIdP

- An open identity provider
- Freely registered
- Mainly for federation test purpose
6. CARSI-Services

- **Goals:**
  - To simplify the upgrade of univ. user accessible applications to federation applications with no or little modification to application codes.

- **Current Situations:**
  - CARSI candidate applications have different authn and access control requirements and implementing ways.
  - Resource diversity increases CARSI federation integration difficulty.
  - Resource complexity hinders federation application resource abundance and federation scale extension.
Applications: Before joining CARSI Fed

- Authn and authr are considered together as AAI (Authn and Authr Infrastructure) or IdM (Identity Management).
- Some app. required authn with simple or no authr policies.
- Some app. already had authn and authr policies implemented in modules loosely coupled with application logic.
- Some app. already had authn and authr policies dispersed in application codes, and difficult to be separated from applications.
- Some app. support some kind of campus-wide identity management.
- Some app. was planning to enforce access control.
- Some had been shibbolethed.
Applications: After joining CARSI Fed

- Authn and authr work at different parts of CARSI Fed.
- Over CARSI infrastructure, users are authenticated by home IdP.
- Authr is implemented differently depending on application requirements and application legacy implementing ways.
  - It can be no authr, for example, the authn-only resources.
  - It can be an independent module of CARSI SP with interfaces to applications, for example, the authn and authr independent resources.
  - It can be merged in applications with interfaces to CARSI SP, for example, the authn and authr embedded resources.
  - It can be shibbolethed by other organizations, for example, the fed attr relying resources.
- CARSI-Services Platform is proposed to support the above four classes of authr implementing ways.
## CARSI Web Application Classification

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>AOR – Authn only Res</td>
<td>Yes</td>
<td>No</td>
<td>CARSI</td>
<td>no</td>
</tr>
<tr>
<td>FAR – Fed Attribute-relying Res.</td>
<td>Yes</td>
<td>Yes</td>
<td>CARSI</td>
<td>Application</td>
</tr>
<tr>
<td>AAIR – Authn &amp; Authr Independent Res</td>
<td>Yes</td>
<td>Yes</td>
<td>CARSI</td>
<td>CARSI</td>
</tr>
<tr>
<td>AAER – Authn &amp; Authr Embedded Res</td>
<td>Yes</td>
<td>Yes</td>
<td>CARSI &amp; Application</td>
<td>Application</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------</td>
<td>----------------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>AOR – Authn only Res</strong></td>
<td>Yes</td>
<td>No</td>
<td>CARSI</td>
<td>No</td>
</tr>
<tr>
<td><strong>FAR – Fed Attribute-relying Res.</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>CARSI</td>
<td>Application</td>
</tr>
<tr>
<td><strong>AAIR – Authn &amp; Authr Independent Res</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>CARSI</td>
<td>CARSI</td>
</tr>
<tr>
<td><strong>AAER – Authn &amp; Authr Embedded Res</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>CARSI &amp; Application</td>
<td>Application</td>
</tr>
</tbody>
</table>
AOR - Authn-only Resource Workflow
## CARSI Web Application Classification

<table>
<thead>
<tr>
<th>Type</th>
<th>Authn-Required</th>
<th>Authr-Required</th>
<th>Authn Impl.</th>
<th>Authr Impl.</th>
</tr>
</thead>
<tbody>
<tr>
<td>AOR – Authn only Res</td>
<td>Yes</td>
<td>No</td>
<td>CARSI</td>
<td>no</td>
</tr>
<tr>
<td>FAR – Fed Attribute-relying Res.</td>
<td>Yes</td>
<td>Yes</td>
<td>CARSI</td>
<td>Application</td>
</tr>
<tr>
<td>AAIR – Authn &amp; Authr Independent Res</td>
<td>Yes</td>
<td>Yes</td>
<td>CARSI</td>
<td>CARSI</td>
</tr>
<tr>
<td>AAER – Authn &amp; Authr Embedded Res</td>
<td>Yes</td>
<td>Yes</td>
<td>CARSI &amp; Application</td>
<td>Application</td>
</tr>
</tbody>
</table>
FAR - Fed Attribute-Relying Resources

北京大学 Peking University
## CARSI Web Application Classification

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>AOR – Authn only Res</td>
<td>Yes</td>
<td>No</td>
<td>CARSI</td>
<td>no</td>
</tr>
<tr>
<td>FAR – Fed Attribute-relying Res.</td>
<td>Yes</td>
<td>Yes</td>
<td>CARSI</td>
<td>Application</td>
</tr>
<tr>
<td>AAIR – Authn &amp; Authr Independent Res</td>
<td>Yes</td>
<td>Yes</td>
<td>CARSI</td>
<td>CARSI</td>
</tr>
<tr>
<td>AAER – Authn &amp; Authr Embedded Res</td>
<td>Yes</td>
<td>Yes</td>
<td>CARSI &amp; Application</td>
<td>Application</td>
</tr>
</tbody>
</table>

北京大学 Peking University
AAIR - Authn&Authr Independent Resources

北京大学

Peking University
## CARSI Web Application Classification

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AOR – Authn only Res</strong></td>
<td>Yes</td>
<td>No</td>
<td>CARSI</td>
<td>no</td>
</tr>
<tr>
<td><strong>FAR – Fed Attribute-relying Res.</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>CARSI</td>
<td>Application</td>
</tr>
<tr>
<td><strong>AAIR – Authn &amp; Authr Independent Res</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>CARSI</td>
<td>CARSI</td>
</tr>
<tr>
<td><strong>AAER – Authn &amp; Authr Embedded Res</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>CARSI &amp; Application</td>
<td>Application</td>
</tr>
</tbody>
</table>
AAER - Authn&Authr Embedded Resources

北京大学 Peking University

1. Visit
2. 3/4. login
3. User Fed ID
4. Verify UFID
5. Verify UFID

CARS Portal
CARSI-Services Platform

- An unified platform to integrate most popular application resources.
  - Compatible to most web application resources.
- An extension to shibboleth authr framework.
  - An extension to SP to enforce application authr.
  - An extension to CARSI-Portal to mask resource diversity
- Part of the CARSI infrastructure.
  - Built on shibboleth.
  - To cooperate with other CARSI components to support four class resources.

北京大学 Peking University
Current Deployment

PKU SP-北京大学Peking University

Local AAI

PKU IdP

PKU SP-IPGW

RITT IdP

Local IPGW

RITT
Conclusion

**CARS I goals:**
- One univ. id can be used extendedly to federation
- Web applications can be more accessed by more people

**CARS I FCNA:**
- Trace user’s action, federation billing, federation negotiation

**CARS I FPR:**
- Self served possible for provider management

**CARS I-Services:**
- to make federation-wide application sharing easier and more applications can be in the federation resource family.
- tries to extend shibboleth authr framework
- an unified platform tried to integrate most popular application resources.
- Both legacy applications embedded with AA and developing application with clear AA interfaces can be integrated in it.
Thank You!

CARSI: http://www.carsi.edu.cn
Email: carsi@pku.edu.cn