X.509 Privilege Management Infrastructures for Dynamic Delegation of Authority between Sites

David Chadwick
d.w.chadwick@kent.ac.uk
Motivations

• To allow people to delegate their roles to colleagues, so that they can perform tasks within the VO that were previously denied to them
• To ease the management of permissions in the VO through distribution and delegation, which aids scalability (as opposed to centralised control)
• To facilitate inter-organisation federations, by allowing one organisation to leverage the role allocations in another organisation and thereby give them access to their resources in a controlled manner
Assigning and Delegating Privileges in Organisations

Resource Owner

Assigns privilege

Privilege Holder

“I authorise this Privilege Holder to use this resource in the following ways”
signed The Resource Owner

“I delegate authority to this End User to use this resource in this limited way”
signed The Privilege Holder

Delegates privilege

End User (Privilege Holder)
Privilege Checking in Organisations

End User (Privilege Holder) issues a command ( Asserts Privilege) "Please purchase this product from company X" signed the End User ( Privilege Verifier)

Q. "Is this user authorised to perform this task?"
X.509 Privilege Management Entities

Source of Authority (SoA)
(Root of Trust)

Assigns privilege

Trusts

Attribute Authority (AA)

Asserts privilege (optional)

Delegate privilege

Privilege Holder (End Entity)

Privilege Verifier

Asserts privilege
X.509 PMI Token

- Is called an Attribute Certificate (AC)
- Very similar to a Public Key Certificate (PKC)
- Essentially the public key is replaced by a set of attributes

The attributes can be anything:
- Privileges e.g. permission to read a file
- Roles e.g. Project manager, researcher
- Personal attributes e.g. Age, Height, Sex
- Qualifications e.g. degrees, diplomas
- Professional body memberships e.g. IEEE, ACM
- Other tokens e.g. electronic credit cards, frequent flyer memberships, clearances, classifications etc.

- Therefore can support DAC, MAC, RBAC, ABAC
- Critical Factor – they are *digitally signed* by the Issuer
Assigning Privileges in X.509 (2001)
Limitations in X.509 (2001) model

• Privilege assigner (AA) needs to have a public/private key pair in order to sign the AC

• AC chains could get very long, therefore relatively poor performance
  - but not as bad as XML encryption/signing 😊
The X.509 (2005) Delegation Service

Delegation Policy

Points to issuer

Points to holder

Points to Issued On Behalf Of

Issuing Service (DIS)

SOA

Bill

Issues AC to

AA

Alice

Issues AC to

End Entity

Bob

Issues AC to

Delegation Policy
Advantages of Introducing a DIS

- DIS can support a fully secure audit trail (just like a CA)
- DIS can enforce corporate assignment and delegation policy efficiently
- Managers do not need to be PKC enabled in order to delegate authority. DIS can support multiple authentication methods e.g. via Shibboleth
- DIS can improve performance of AC chain validation
  - Shortens the AC chain length to 2 (SoA → DIS’s AC → end entity’s AC)
  - Reduces the number of ACRLs that need to be published
- When a manager’s AC is revoked or expires, we do not necessarily need to revoke all the end entity ACs, because they still can validate successfully
DIS Web Service

Authenticate DIS Client (SSL)

DIS PEP
Web service interface

Issue AC
-holder
-attributes
-validity time

Credential LDAP server

Credential Validation Service

PERMIS RBAC

PDP

Request
Authorisation

IssueAC

Sign AC

Delegation Issuing Policy

Issuer’s AC

Issue AC holder attributes validity time
PERMIS DIS Implementation

Web browser

SSL or Shibboleth

Apache

DIS Web Service Interface

DIS Java

GGF15, 3 October 2005 © 2005, University of Kent
DIS Web Browser Interface

Issue new Attribute Certificate

Search LDAP Server

By Common Name (CN): [add your search string here]

Search | Choose

No entries found.

Roles to be assigned to the Holder

Available roles

- Student
- Staff
- Professor
- Researcher
- Admin

Assigned roles

- Add Role
- Remove Role

Validity Period

From: 2005 Jan 1 To: 2005 Jan 1

Delegation illustration

Issuer (you)

Holder

Can the Holder delegate this/these role(s)?

Yes | No

Done
Issue new Attribute Certificate

Search LDAP Server

By Common Name (CN): stuart

Search

Holder DN: cn=Stuart,ou=staff,c=PERMIS,c=gb

Roles to be assigned to the Holder

Available roles
Student
Staff
Professor
Researcher
Admin

Assigned roles
Researcher

Validity Period
From: 2005 Jan 1
To: 2006 Jan 1

Delegation illustration

Issuer
(you)

Holder
Delegation Approved as Requested

Delegation Requested:

<table>
<thead>
<tr>
<th>Holder</th>
<th>cn=Stuart,ou=staff,o=PERMIS,c=gb</th>
</tr>
</thead>
<tbody>
<tr>
<td>Roles requested</td>
<td>Researcher</td>
</tr>
<tr>
<td>From Date</td>
<td>January 01, 2005</td>
</tr>
<tr>
<td>To Date</td>
<td>January 01, 2006</td>
</tr>
<tr>
<td>Can the Holder use this Attribute Certificate?</td>
<td>YES</td>
</tr>
<tr>
<td>Delegation Depth</td>
<td>Holder WON'T BE ALLOWED to delegate privileges in this Attribute Certificate to anyone</td>
</tr>
</tbody>
</table>

Delegation Approved:

<table>
<thead>
<tr>
<th>Holder</th>
<th>cn=Stuart,ou=staff,o=PERMIS,c=gb</th>
</tr>
</thead>
<tbody>
<tr>
<td>Roles approved</td>
<td>Researcher</td>
</tr>
<tr>
<td>From Date</td>
<td>January 01, 2005</td>
</tr>
<tr>
<td>To Date</td>
<td>January 01, 2006</td>
</tr>
<tr>
<td>Can the Holder use this Attribute Certificate?</td>
<td>Holder CAN assert privileges</td>
</tr>
<tr>
<td>Delegation Depth</td>
<td>Holder WON'T BE ALLOWED to delegate privileges in this Attribute Certificate to anyone</td>
</tr>
</tbody>
</table>

Issue another AC
PERMIS Authorisation System

Initiator

PUSH
Submit Access Request

Authentication Service
GT4 PEP

Present Access Request

Target

GGF OGSA SAML Authz protocol

SAML Wrapper

getcreds request/response
decision request/response

The PERMIS Java API
Credential Validator
PDP

PKI

Retrieve Policy and Role ACs (pull)

Retrieve Role ACs (push)

User Credentials

LDAP Directories

User Credentials
Multiple Domain Architecture

- User’s Grid request
- Direct
- Spawned
- Localized
- X.509 ACs
- Policy
- Delegate Credentials
- Apache
- DIS Web Service
- LDAP Credential Store
- GT4 PEP
- PERMIS PDP
- GT4 PEP
- PERMIS PDP
- X.509 ACs
Demonstration - Apache with PERMIS
RBAC Authorisation

Apache Server

Apache Authentication

mod_permis

PERMIS Protected Resource

User request

Credential LDAP Server

Pull ACs

LDAP Directory

Authzn Policy

The PERMIS API

JNI connector

CVD

PDP
Acknowledgement

• This work was funded primarily under the JISC DyVOSE project, with partners at the University of Glasgow and University of Edinburgh

• Any Questions ????????????