

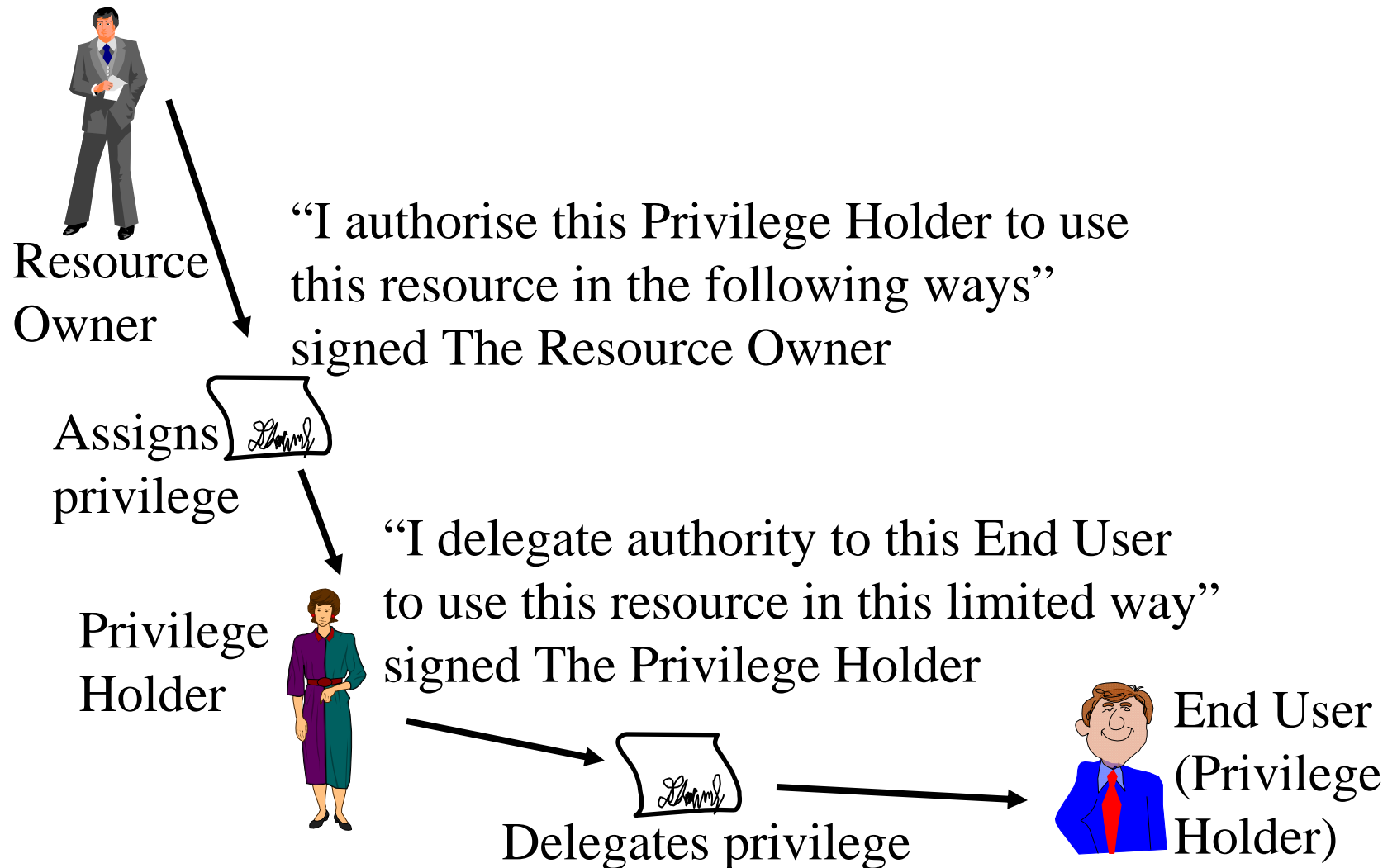
X.509 Privilege Management Infrastructures for Dynamic Delegation of Authority between Sites

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



Privilege Checking in Organisations

End
User
(Privilege
Holder)



Issues a
command
(Asserts
Privilege)

“Please purchase this
product from company X”
signed the End User

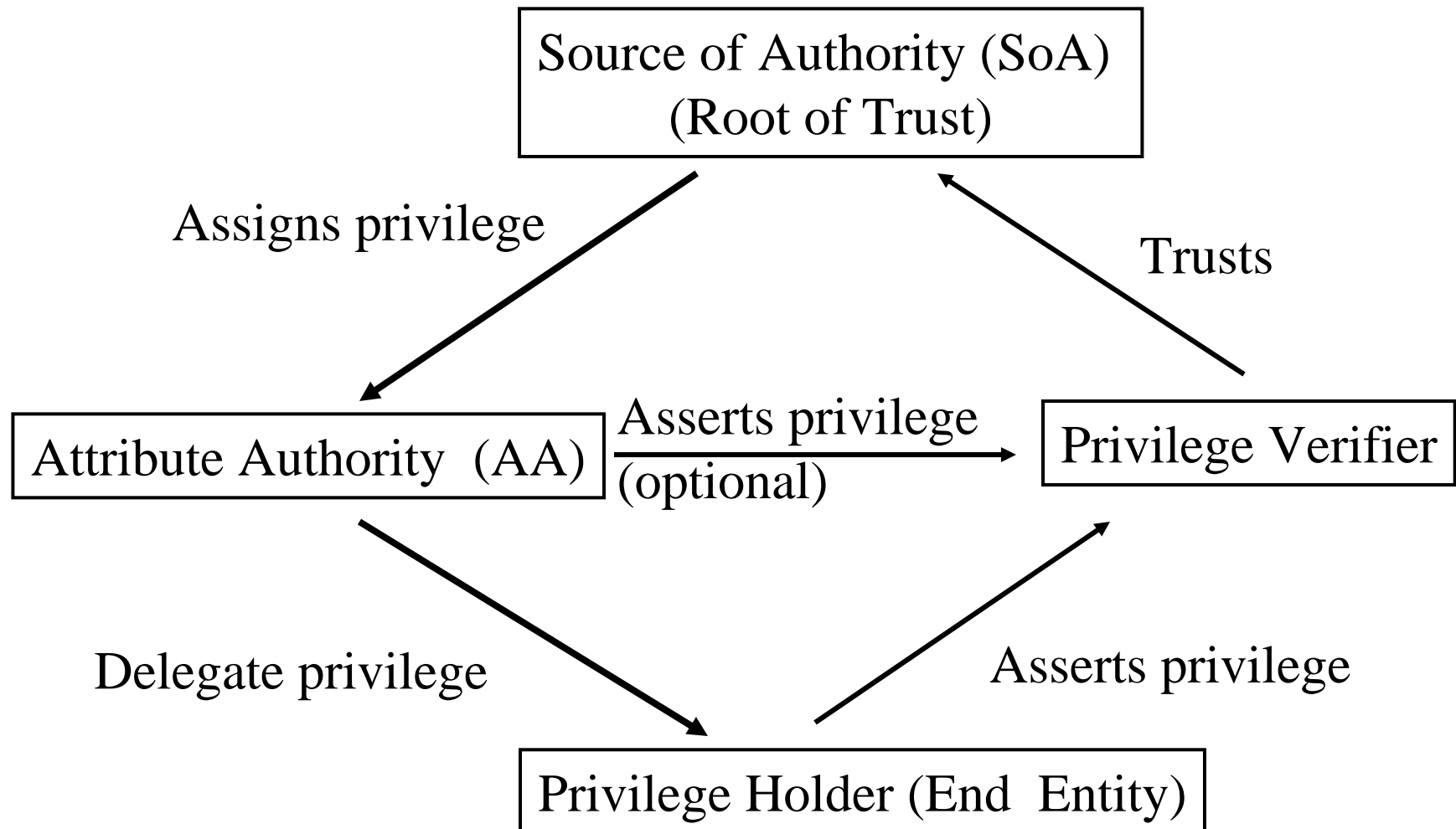


Privilege Verifier



Q. “Is this user authorised
to perform this task?”

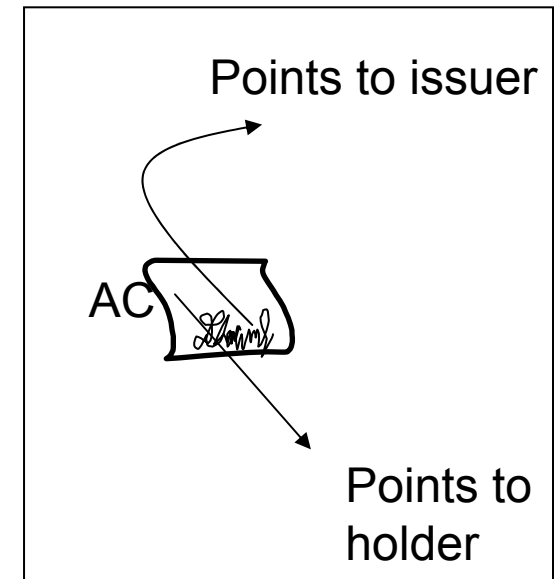
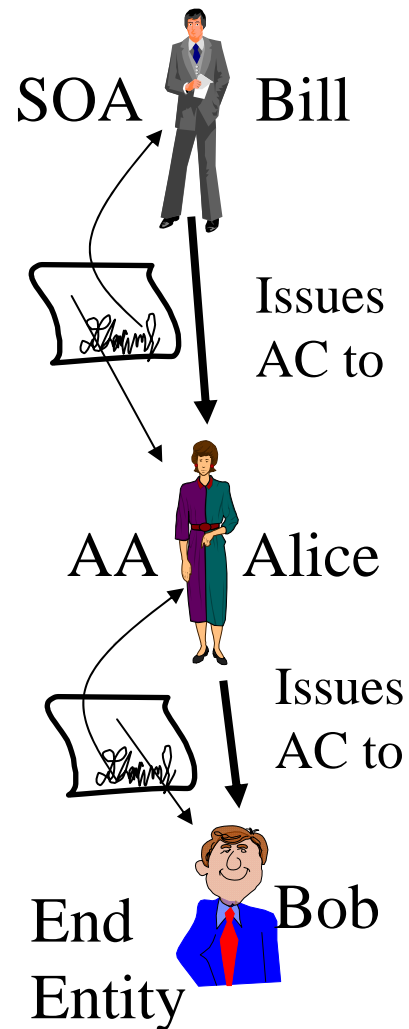
X.509 Privilege Management Entities



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

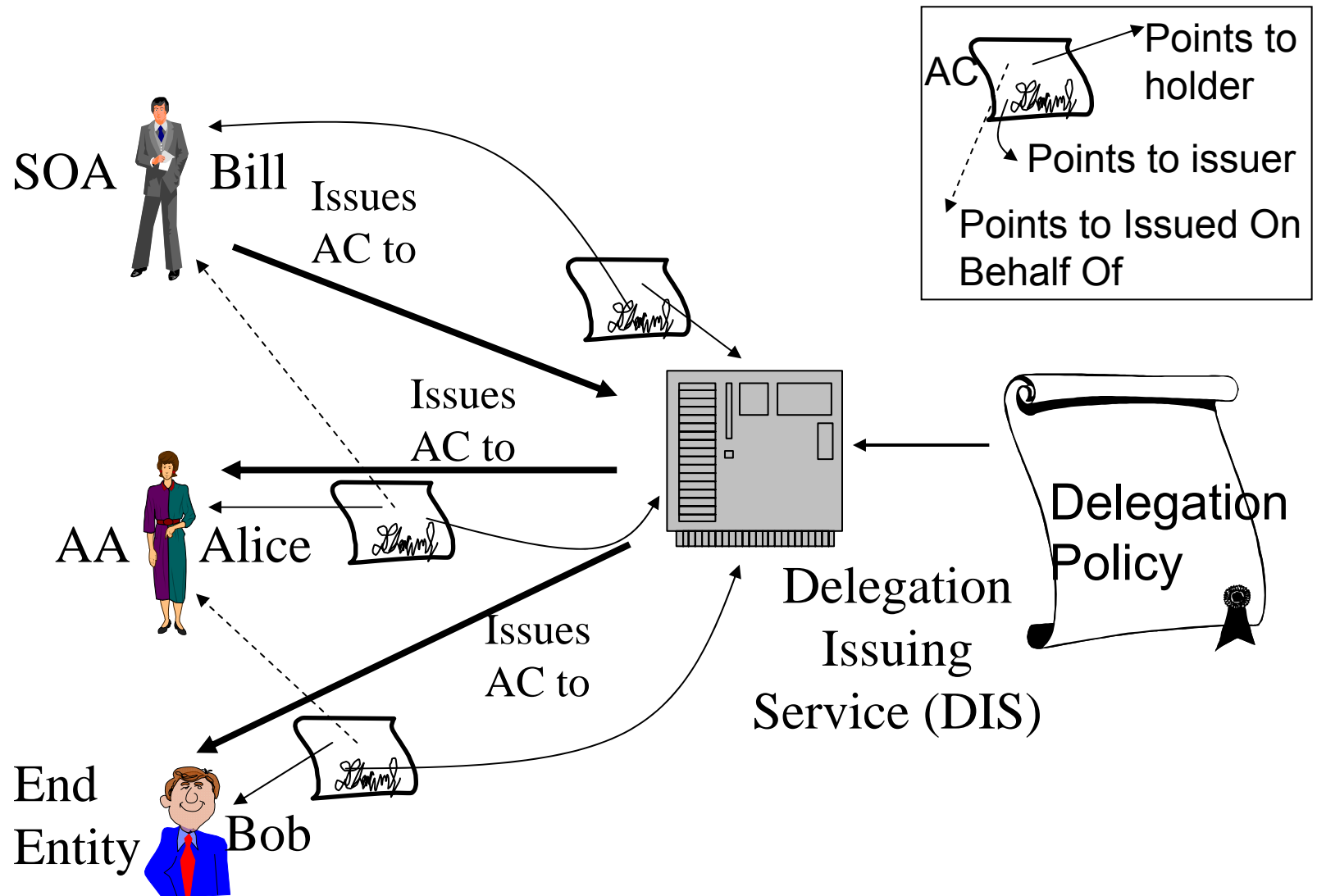
Assigning Privileges in X.509 (2001)



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 ☺

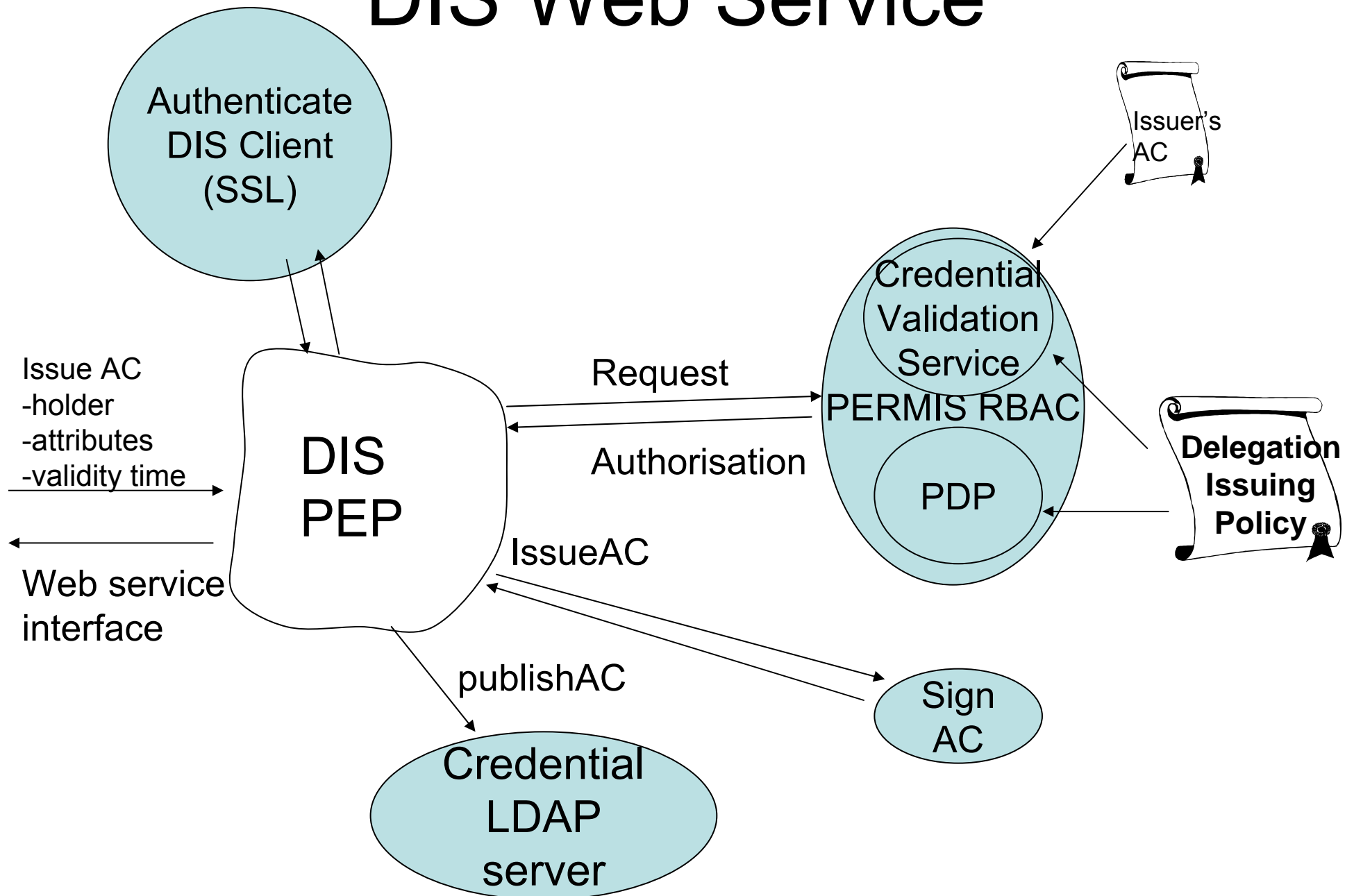
The X.509 (2005) Delegation Service



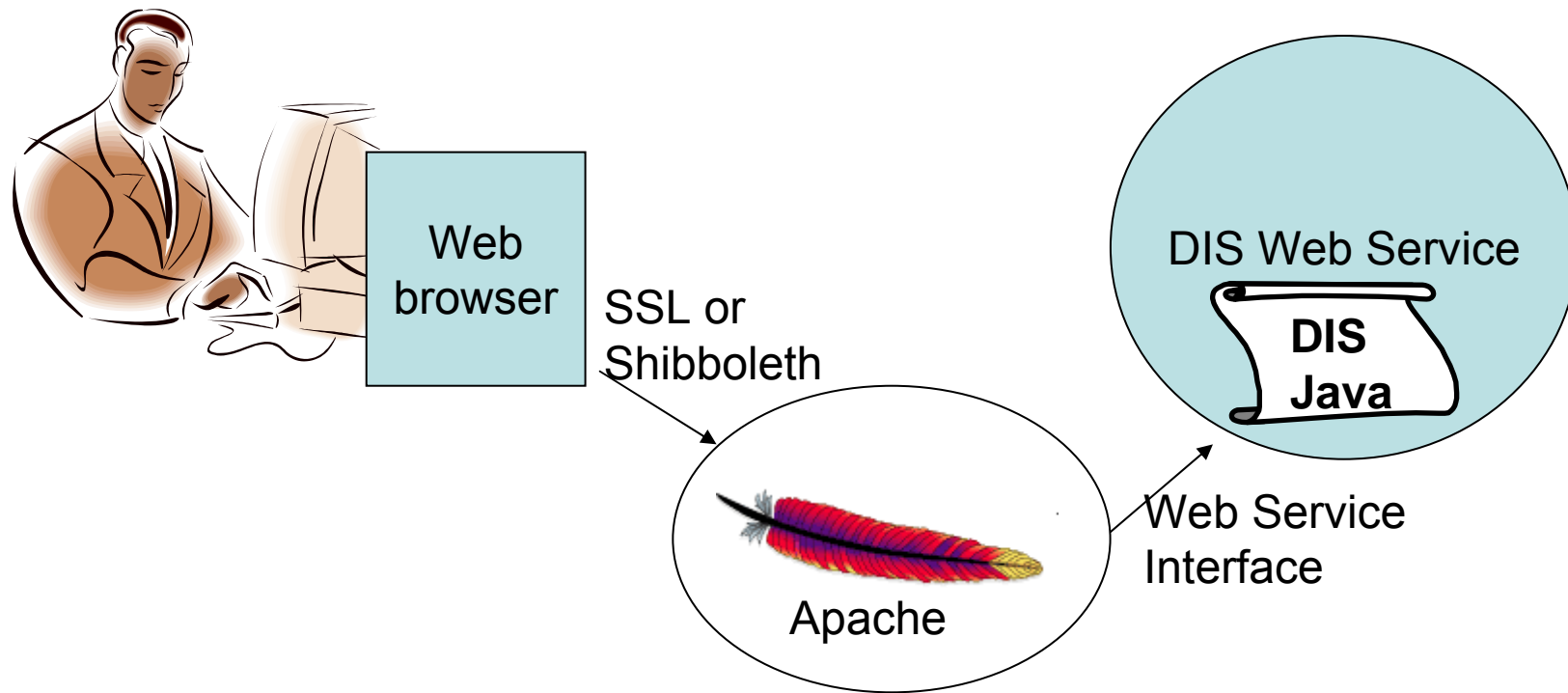
Advantages of Introducing a DIS

- 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



PERMIS DIS Implementation



DIS Web Browser Interface

Issue new Attribute Certificate - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://issrg-testbed.cs.kent.ac.uk:8080/dis/dis.php

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		Assigned roles
Student	Add Role Remove Role	
Staff		
Professor		
Researcher		
Admin		

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

Start C. I.. S. G. I.. D. R. R. F. S. A. G. G. F. I.. G. 12:33

Issue new Attribute Certificate - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://issrg-testbed.cs.kent.ac.uk:8080/dis/dis.php

Issue new Attribute Certificate

Search LDAP Server

By Common Name (CN)

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


Roles to be assigned to the Holder

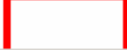
Available roles		Assigned roles
<div>Student</div> <div>Staff</div> <div>Professor</div> <div>Researcher</div> <div>Admin</div>	<div><input type="button" value="Add Role"/></div> <div><input type="button" value="Remove Role"/></div>	<div>Researcher</div>

Validity Period

From: To:

Delegation illustration

Issuer (you) 

Holder 

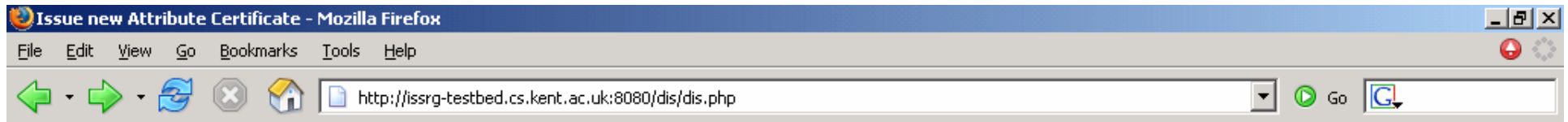
Done

Start

C:\Resea... Distribut... Inbox - ... Search M... tutorialC... Compose... Writing P... RE : Rom...

Adobe A... Microsoft... C:\WIND... LDAP Bro... Issue ne... 401 Auth... Compose...

20:06 Monday



Done - Delegation Approved as Requested

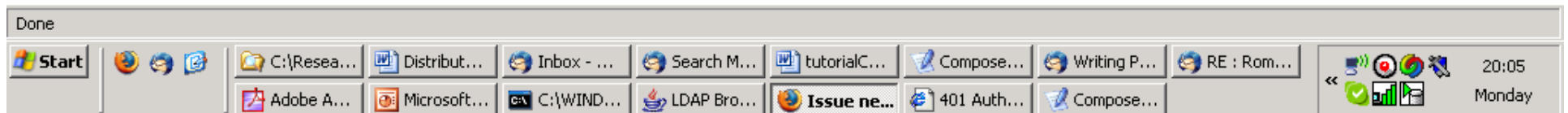
Delegation Requested:

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

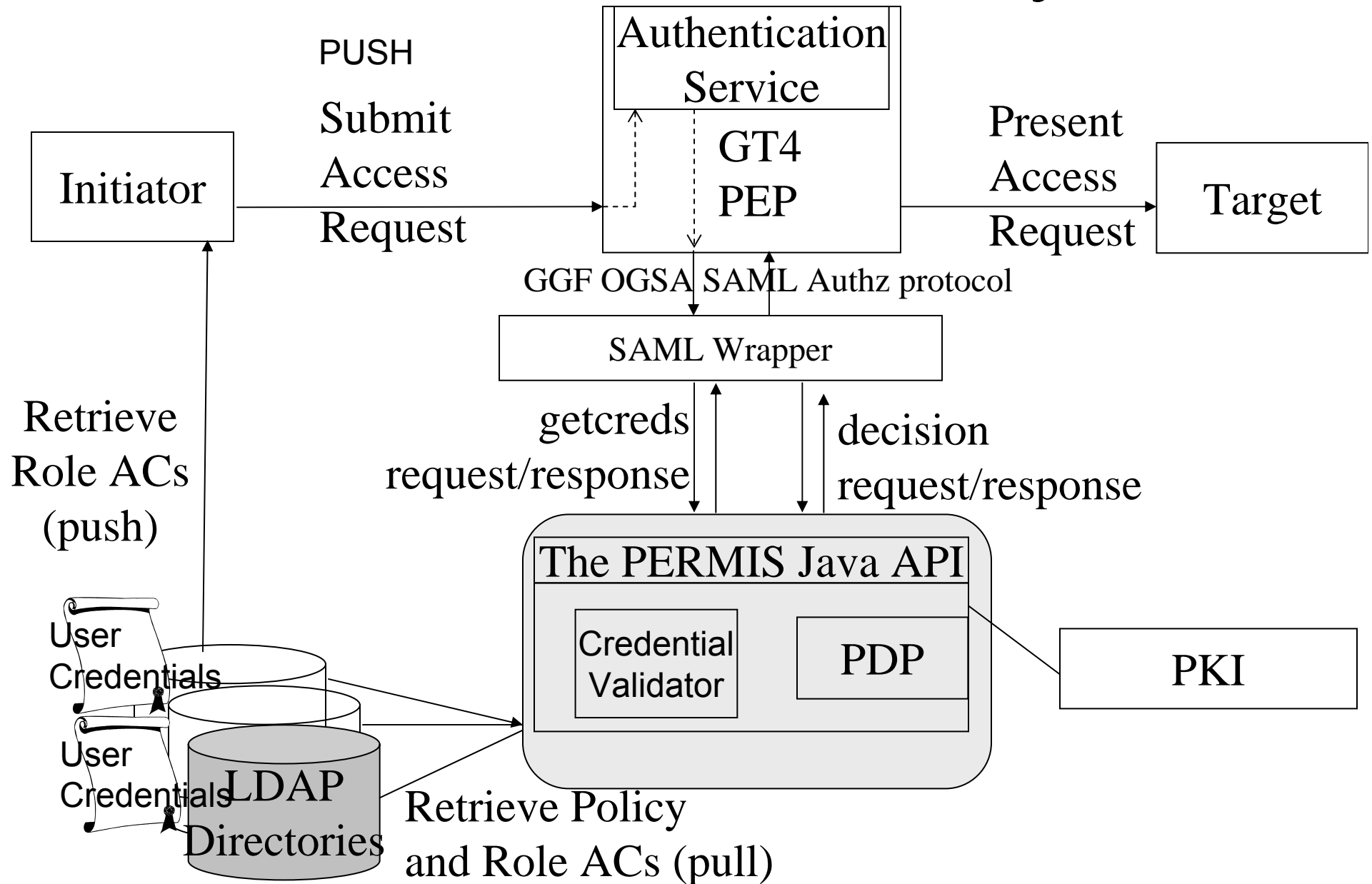
Delegation Approved:

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

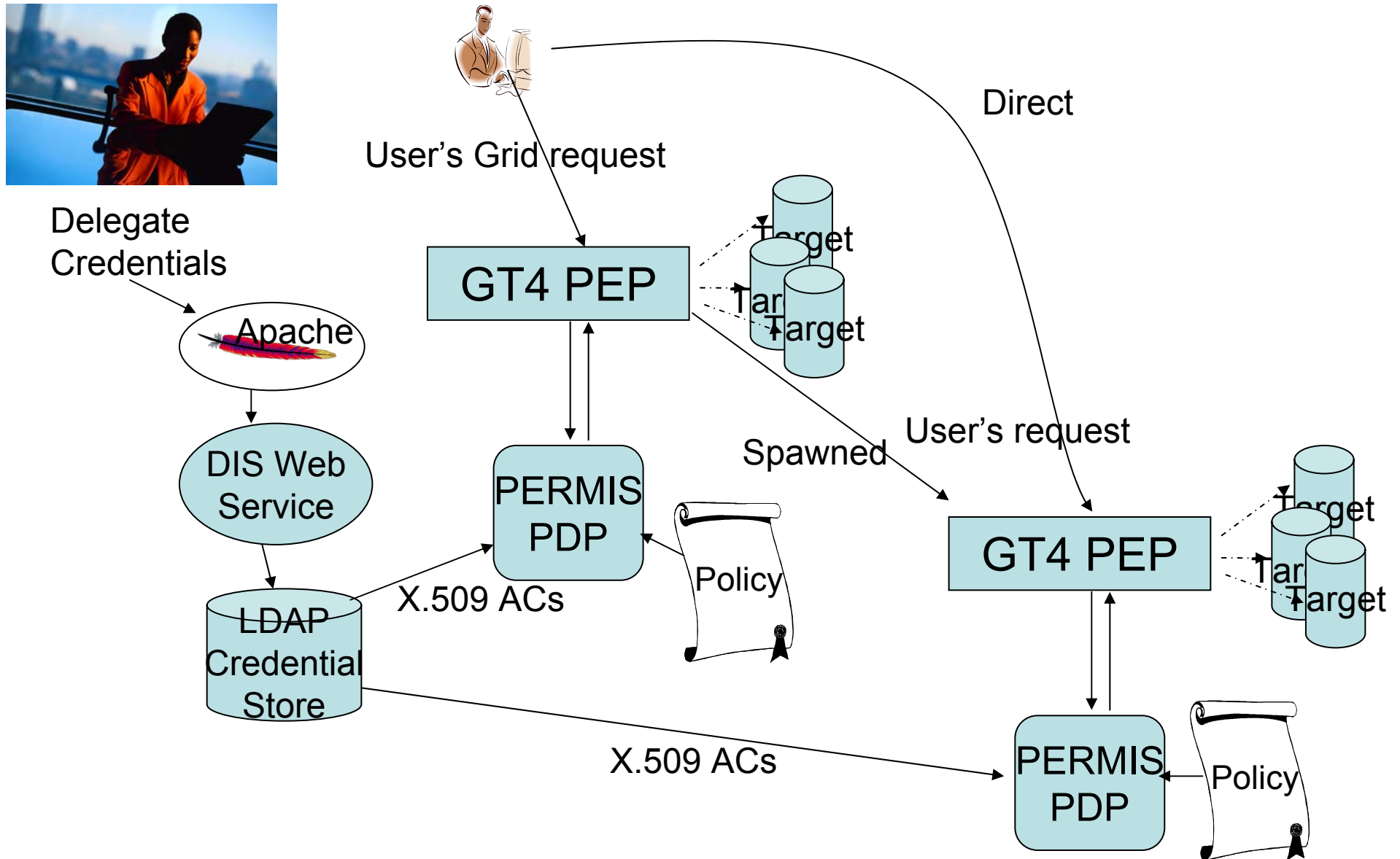
Issue another AC



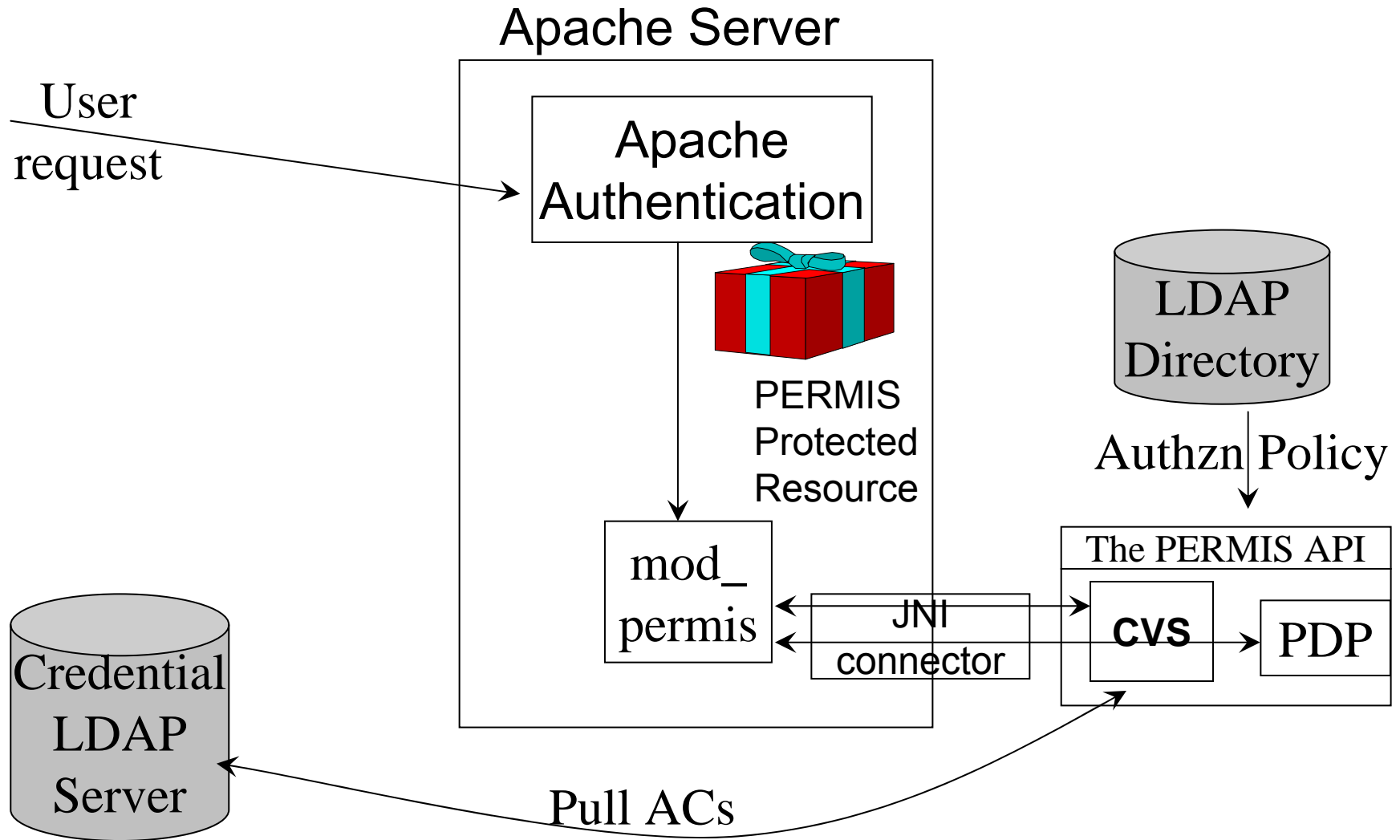
PERMIS Authorisation System



Multiple Domain Architecture



Demonstration - Apache with PERMIS RBAC Authorisation



Acknowledgement

- This work was funded primarily under the JISC DyVOSE project, with partners at the University of Glasgow and University of Edinburgh
- Any Questions ????????????