

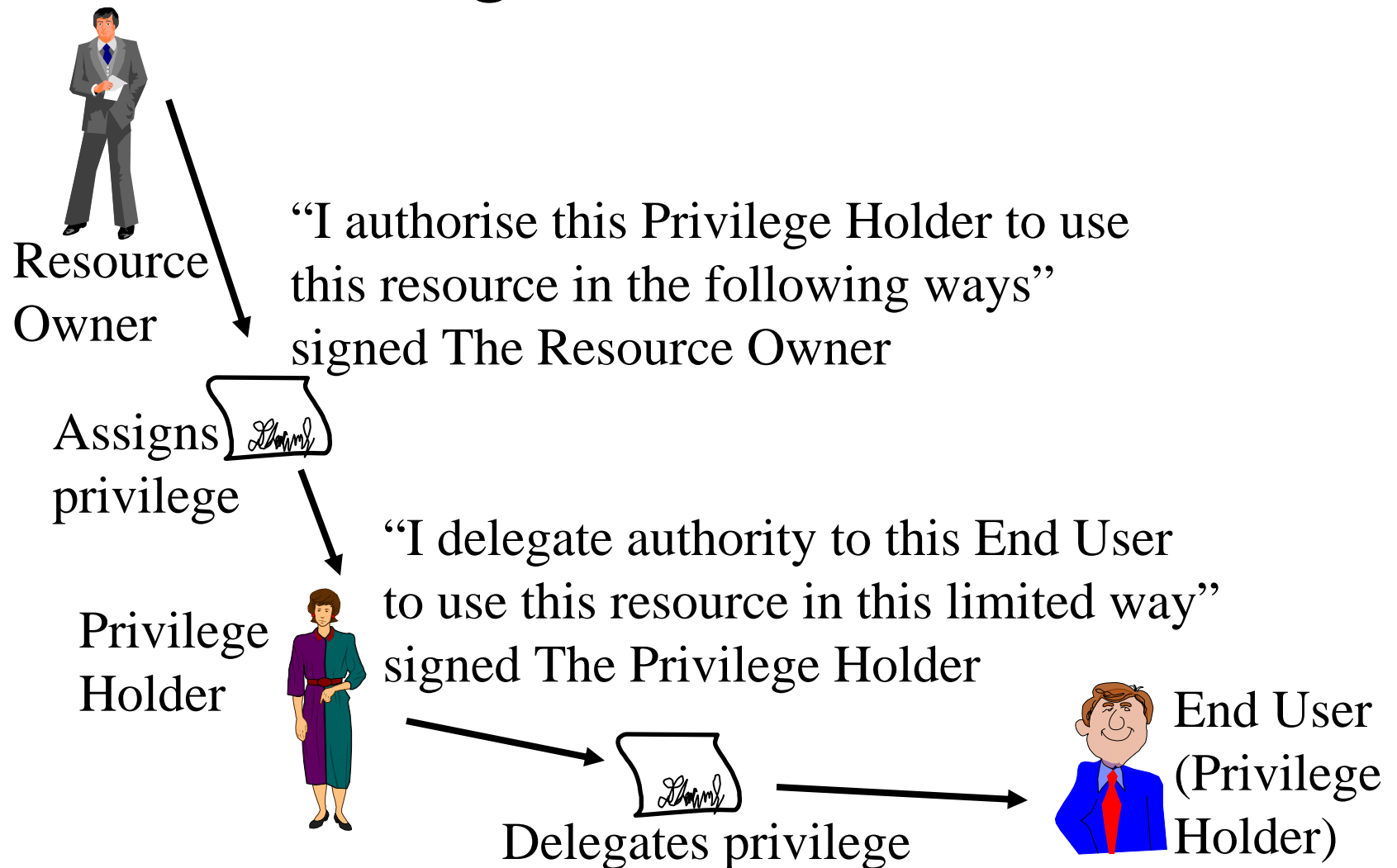
Delegation Issuing Service for X.509

David Chadwick
University of Kent

Contents

- Delegation of Authority in Organisations
- X.509 Delegation Model (2001 edition)
- New Delegation Service Model (2005 edition)
- Implementing the DIS in PERMIS
- Comparison with other models
- Further standardisation work still needed

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

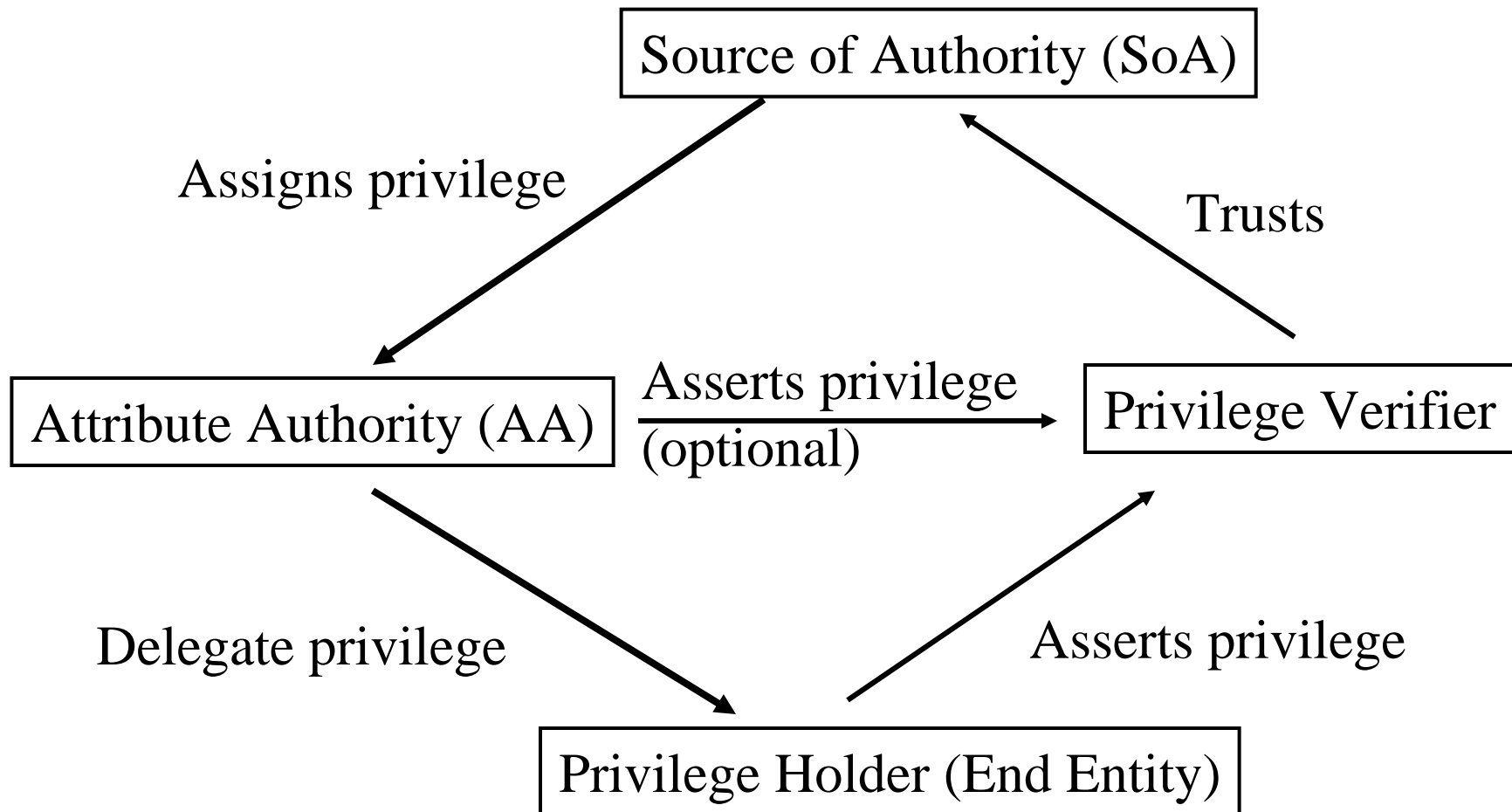


Privilege Verifier

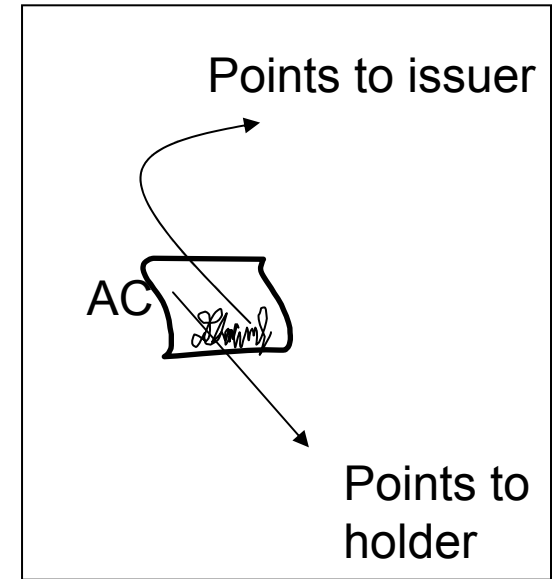
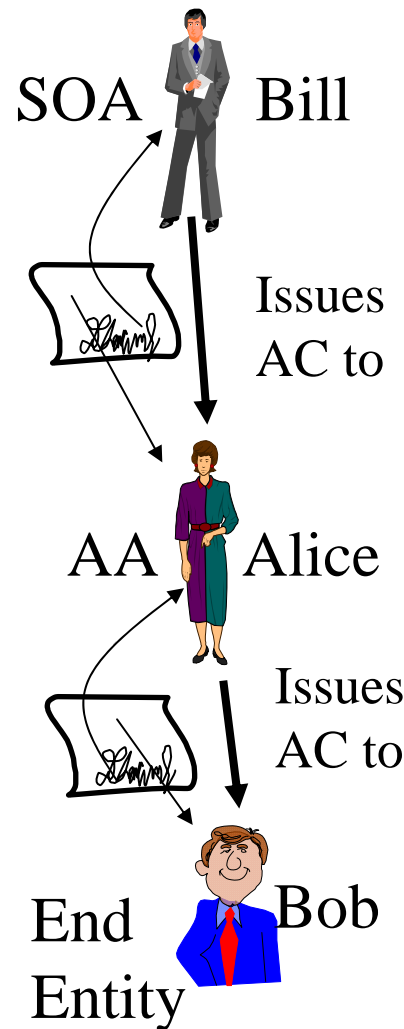


Q. “Is this user authorised
to purchase these goods?”

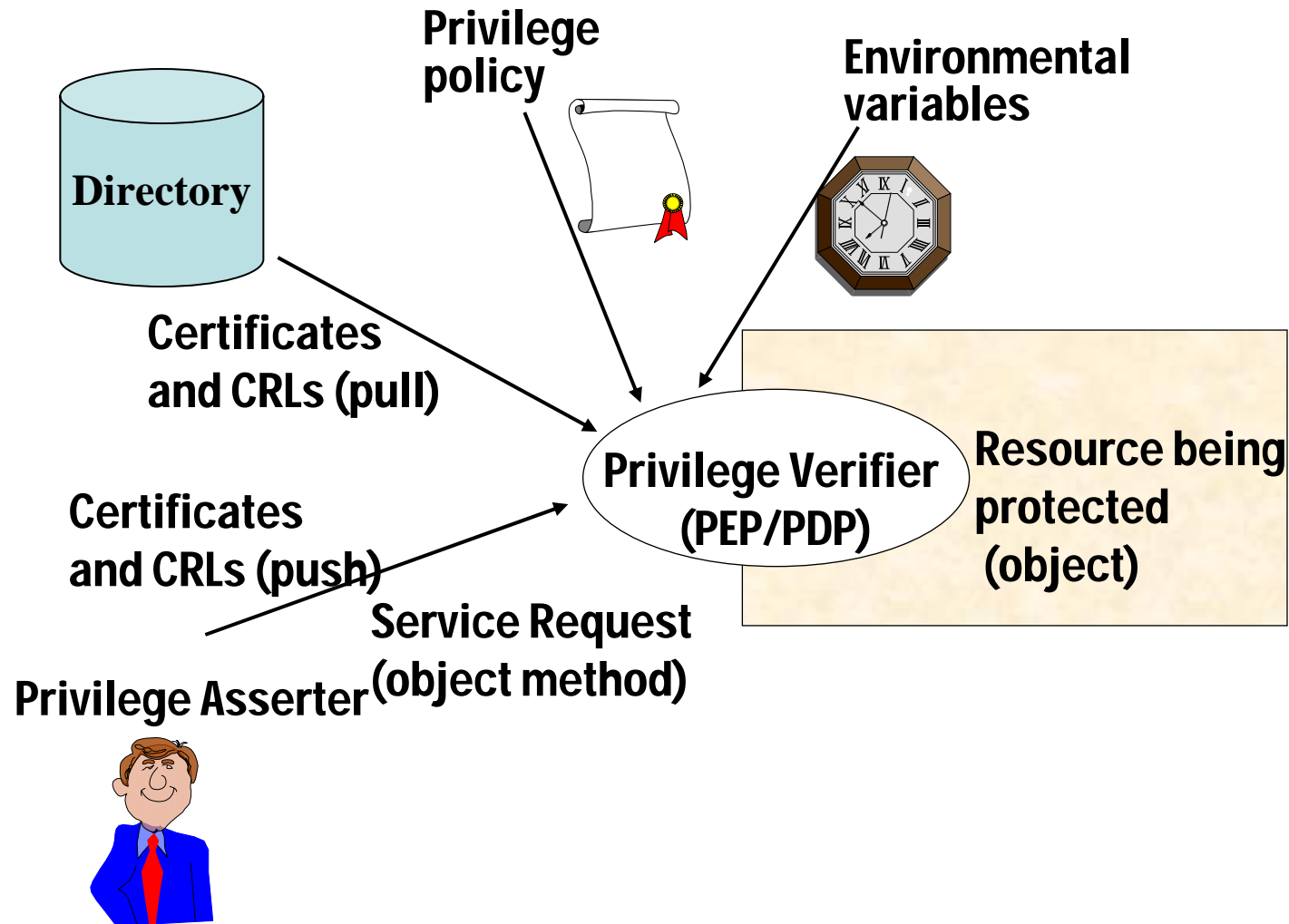
X.509 PMI Entities



Assigning Privileges in X.509 (2001)



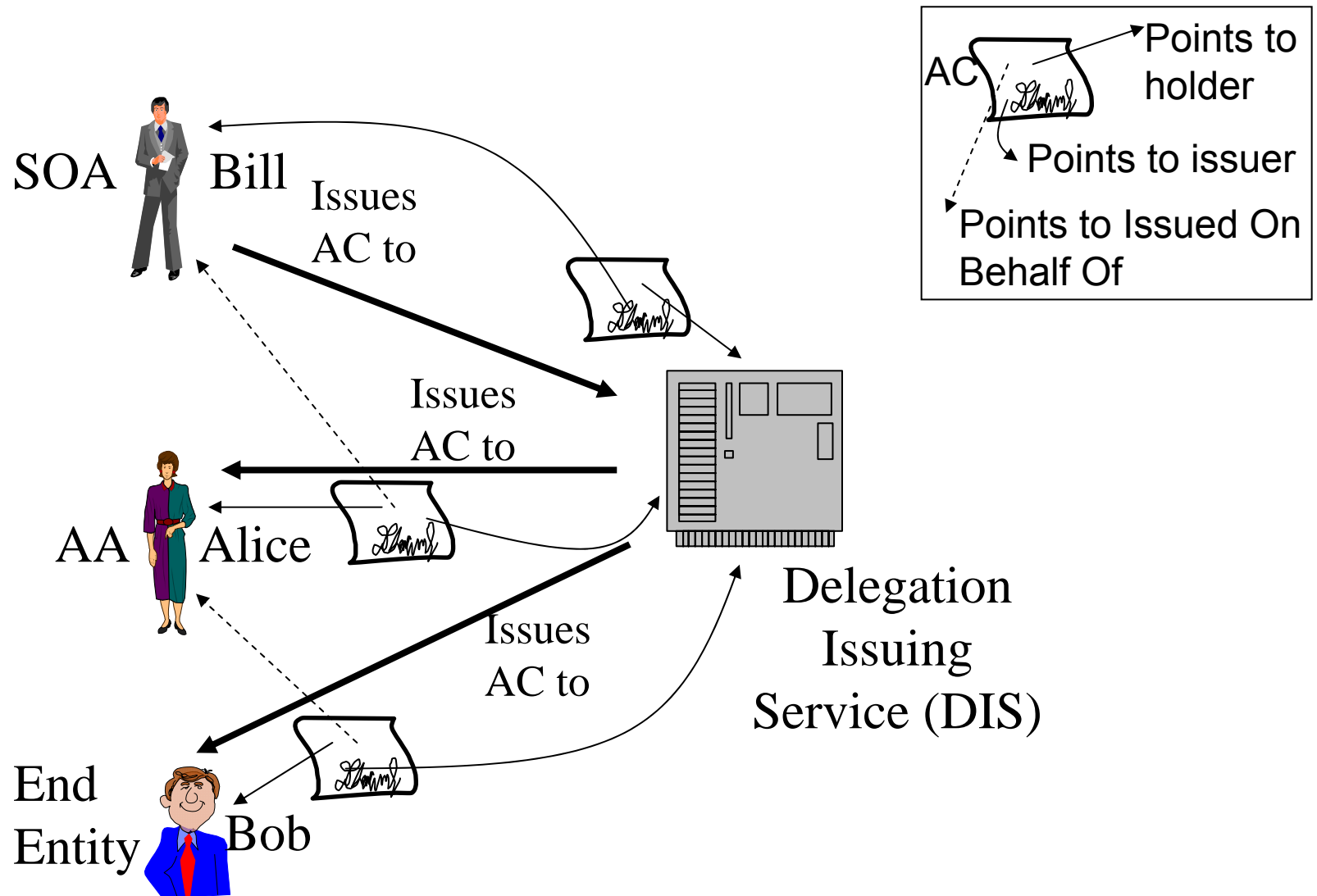
Verifying Privilege in X.509



Deficiencies in X.509 (2001) Model

- No way to flag that an AA cannot assert the privileges in the ACs it holds
- No way to allow a manager who does not have a PKI key pair to delegate authority
- Can be difficult to collect audit information if ability to issue ACs is fully distributed.
- Can be inefficient to enforce delegation policy by adding lots of extensions to the ACs e.g.
 - Delegated Name Constraints, Basic Attribute Constraints, Acceptable Certificate Policies
 - Central control vs. distributed control
- Most of these can be solved by introducing a Delegation Service

The X.509 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
- DIS can improve performance of AC chain validation if it is given the privileges
 - 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 may validate successfully (i.e. when DIS is operating in PMI mode)

DIS Deployment Models

- AC PKI mode
 - DIS issues ACs on behalf of managers but does not hold the privileges itself in its AC. Instead, its AC only contains the indirectIssuer extension (similar to indirect CRLs)
- PKI mode
 - DIS issues ACs on behalf of managers but does not have an AC itself. Instead its PKC contains indirectIssuer extension.
- PMI mode
 - DIS has its own AC, issued by SoA, with superset of all privileges it will delegate to others on behalf of managers. AC contains the noAssertion extension.

Disadvantages of a DIS

- In AC PKI and PKI modes, the validation of the AC chain is more complex (see later)
- In PMI mode, on cross certification between PMIs, a DIS has to be cross certified rather than individual AAs, so there is some loss of granularity
- If all revocations are issued by the DIS, then ACRL could get very large (without distribution points)
- DIS's AC signing key is online so that it can be used dynamically to generate ACs. Can be unacceptable security weakness in some deployments

X.509 Support for DIS

- noAssertion extension, says that AC holder cannot assert the attributes in the AC
- indirectIssuer extension, says the cert holder is authorised to issues ACs on behalf of other AAs
- issuedOnBehalfOf extension, says which AA requested this AC to be issued

No Assertion Extension

- Prevents an AA (such as a DIS) from asserting the privileges it can delegate
noAssertion EXTENSION ::= {
SYNTAX NULL
IDENTIFIED BY { id-ce-noAssertion } }
- Always critical, and only in AA ACs
- What is to stop an AA issuing an AC to itself and omitting this extension?
 - SPKI determined nothing, so cannot support this
 - In X.509 all AAs have globally unique names. So if an AA cannot get an alias name from a trusted CA then PV can check all ACs issued to this AA.

Indirect Issuer Extension

- Needed in PKI and AC PKI modes to tell Privilege Verifier that the AA is authorised to issue ACs on behalf of other AAs
 - *otherwise I could issue an AC and say that it was Tony Blair who requested it ☺*
 - Not needed in PMI mode since DIS holds all the privileges it is delegating
- indirectIssuer EXTENSION ::= {
 SYNTAX NULL
 IDENTIFIED BY id-ce-indirectIssuer }
- Always set to non-critical

Issued On Behalf Of Extension

- Needed in PKI and AC PKI modes to validate certificate chains, so set to critical
- Can be used in PMI mode for audit purposes, so set to non-critical

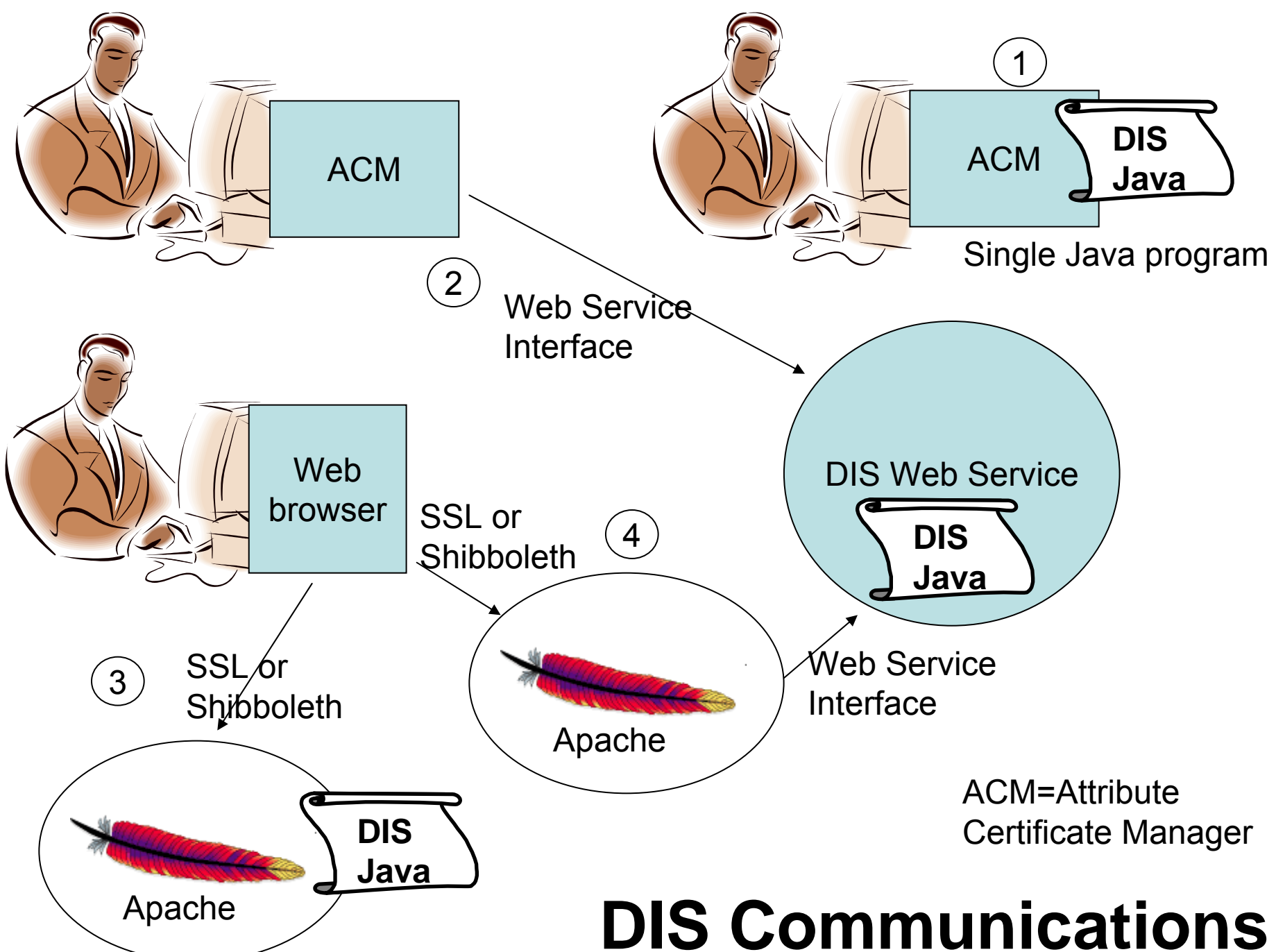
```
issuedOnBehalfOf EXTENSION ::= {  
  SYNTAX GeneralName  
  IDENTIFIED BY id-ce-issuedOnBehalfOf }
```

Verifying Claimed Privileges

- In PMI mode, existing standard procedure used
 - Chain of ACs is checked, issuer to holder back to trusted SoA. Attributes are checked for subsetting.
- In PKI and AC PKI modes, issuedOnBehalfOf extension is marked critical
 - Check AC of AA in issuedOnBehalfOf, that it has a superset of the privileges in this AC. If not, reject
 - Check that PKC or AC of issuer has indirectIssuer extension set. If not reject.
 - For each AC of the issuer that contains one or more of the delegated privileges, recurse up the chain
 - Stop when you get to ACs issued by trusted SoAs

Implementing the DIS

- Issues to be addressed
- Communications between AA and DIS
 - Several modes are envisaged, from Java API to web service interface
- Validating that AA is authorised to request a particular AC for a user
 - We can use the existing PERMIS PDP and Role Allocating Policy for this
- Minimising the PDP's processing time to reach a decision
 - We use the DIS PMI mode of operation
 - If DIS is made a root of trust then AC chain length is always one



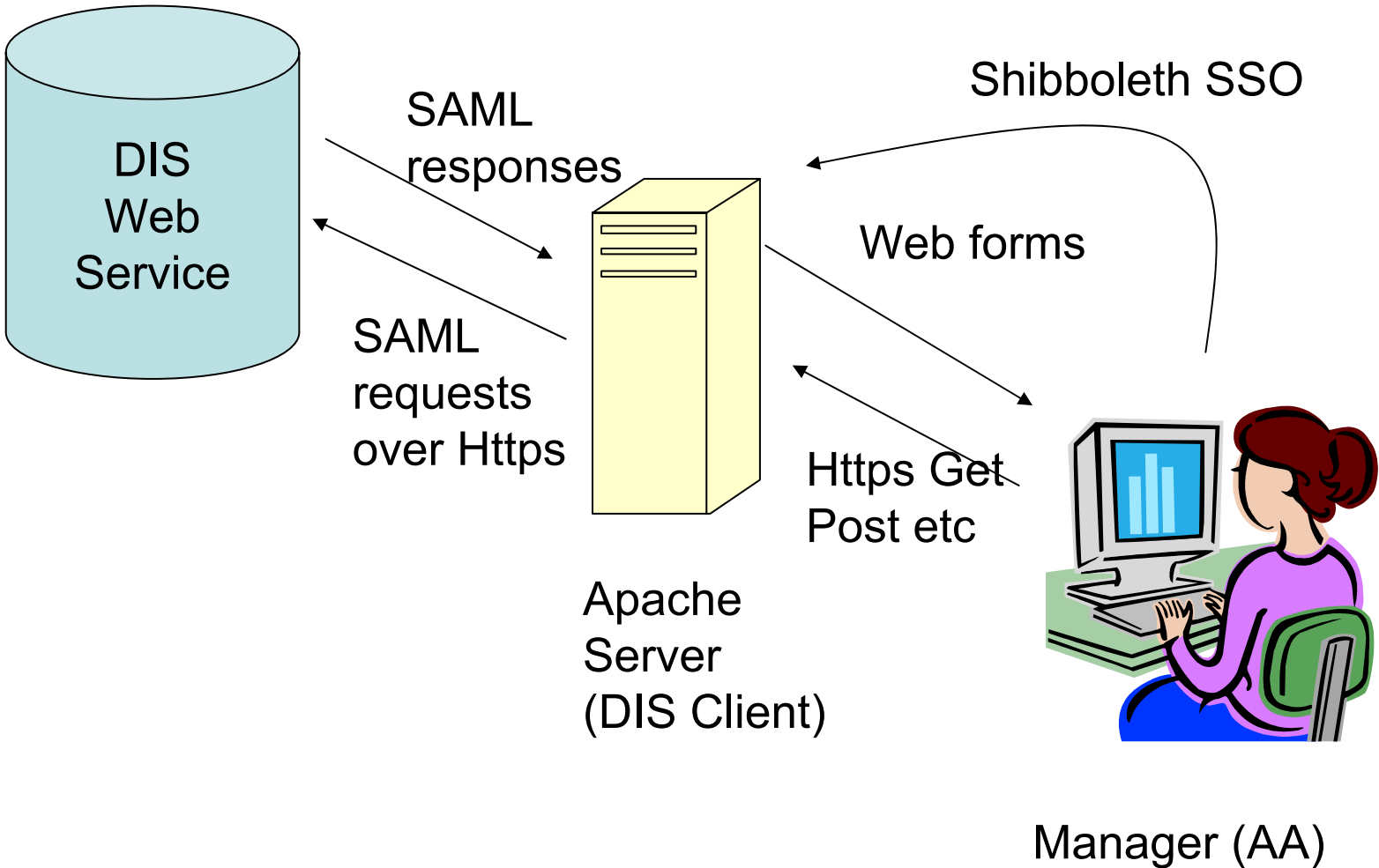
DIS Communications

PERMIS Attribute Certificate Manager

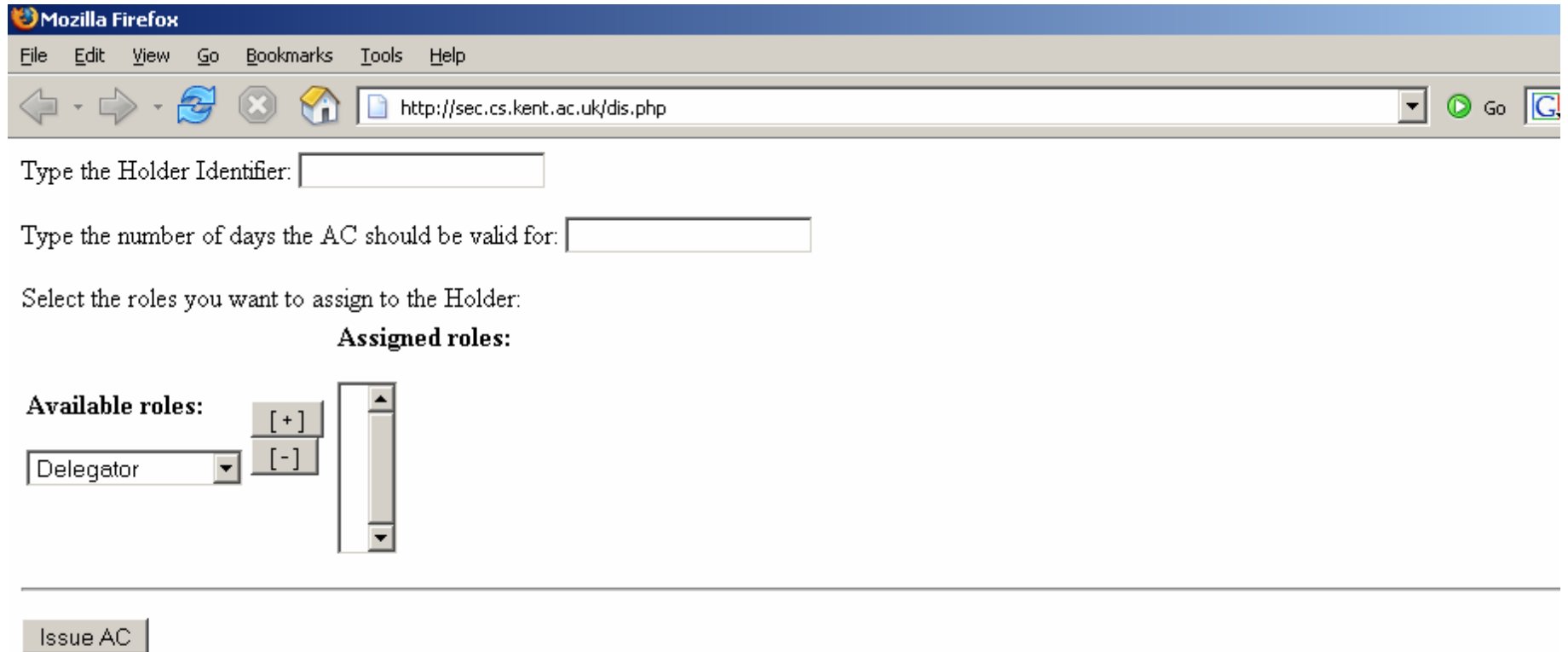
The screenshot shows a window titled "Management Tool" with a close button in the top right corner. The window is divided into several sections:

- Holder:** A text box labeled "Holder Name" contains the text "CN=A PERMIS Test User,O=PERMIS,C=GB". Below it is a button labeled "Browse Directory...".
- Information to include about the issuer:** Two checkboxes are present: "Issuer Name" (checked) and "Issuer Base Certificate ID" (unchecked).
- Validity information:** Two text boxes show dates: "Valid from 2005.04.18 0:0:0" and "to 2005.06.19 0:0:0". Below them is a button labeled "View Calendar...".
- Attributes:** A large text area on the right contains the text "permisRole". Below this area are three buttons: "New...", "Remove", and "Edit...".
- Extensions Editor:** A button labeled "Extensions Editor" is located below the "Attributes" section.
- Bottom:** Two buttons, "Generate and save" and "Cancel", are positioned at the bottom center of the window.

3 Tiered Model



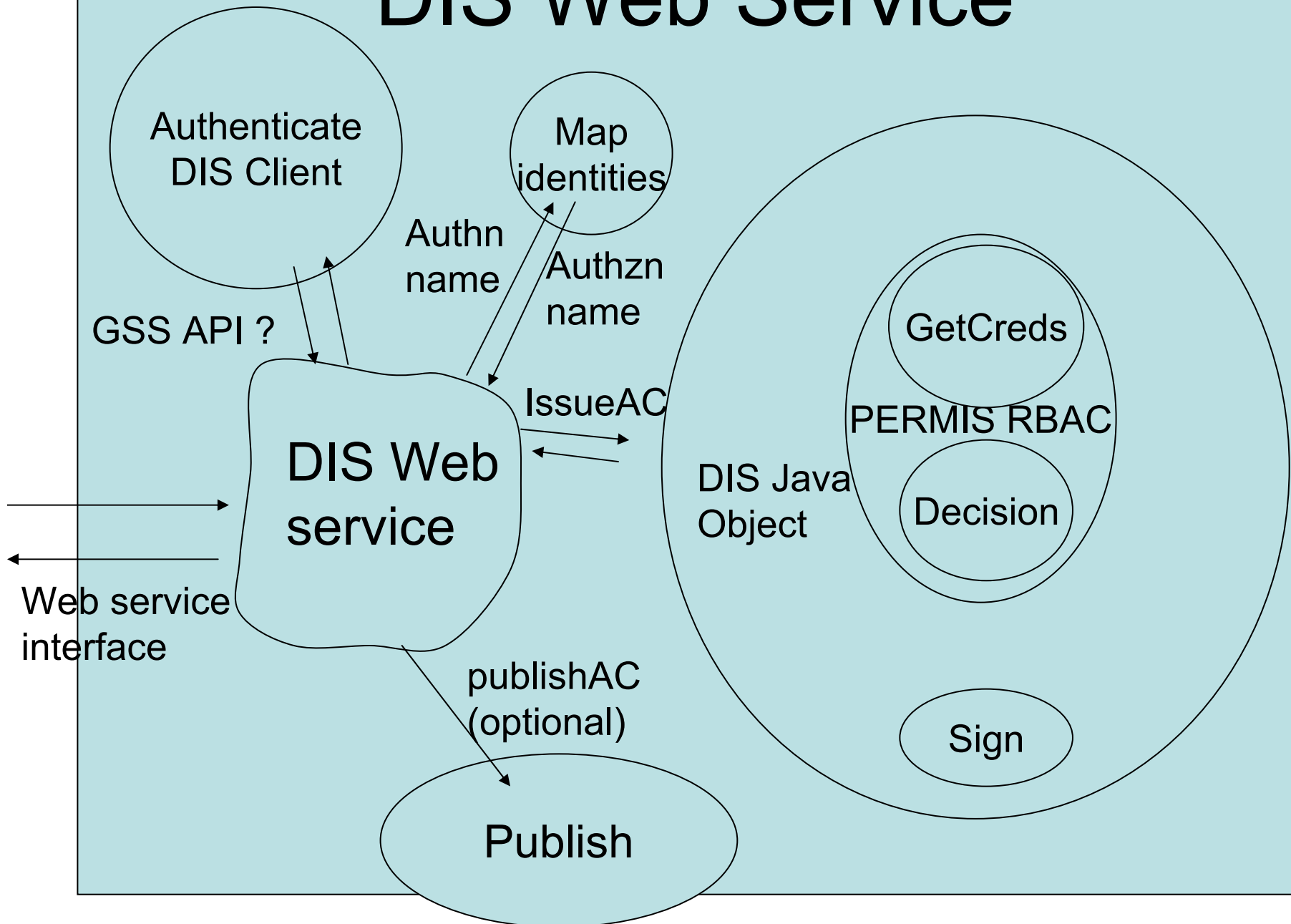
Pilot Web Browser Interface



The screenshot shows a Mozilla Firefox browser window with the address bar containing the URL `http://sec.cs.kent.ac.uk/dis.php`. The page content includes the following elements:

- A text input field labeled "Type the Holder Identifier:".
- A text input field labeled "Type the number of days the AC should be valid for:".
- A label "Select the roles you want to assign to the Holder:".
- A section titled "Assigned roles:" which is currently empty.
- An "Available roles:" section containing a dropdown menu with "Delegator" selected, and two buttons labeled "[+]" and "[-]" for adding and removing roles.
- A vertical list box to the right of the available roles, which is currently empty.
- A horizontal line separating the form from a button labeled "Issue AC" at the bottom.

DIS Web Service



Comparison of DIS with other

• ECMA 219 Delegation Models

- Has PACs and PAS. PAS is similar to DIS, but delegation is not supported through new PACs but rather through embedding Protection Values in original PAC. PV is hash of a secret Control Value. PAC holder gives PAC and secret CV to the delegate

• SPKI

- Authorisation certs similar to X.509 ACs. In SPKI delegation is flagged via a boolean, in X.509 as an integer signifying allowed depth. DIS in PMI mode can easily be applied to SPKI

• Grid Proxy Certs (RFC 3820)

- A PKC is issued to delegate by manager, and carries an indication of which rights are assigned to delegate

• Shibboleth

- Delegates authorisation and attribute assignment to a user's home site

Standards Work Still Needed

- AA info access
 - to say how/where to obtain the AC of the AA issuing this AC (similar to PKC AIA)
- Protocol to request an AC to be issued
 - Similar to PKCS#10 or CMP
- Web services protocol for accessing a DIS
- Cross certification between SoAs

Any Questions

- ???
??
??
??