

## Electronic Identity An Authorisation Service



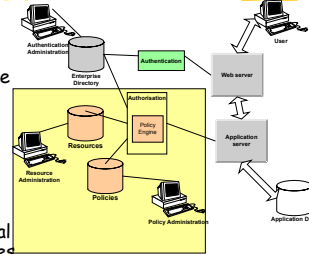
### A Network Based Infrastructural Service for Authorisation

Torbjörn Wiberg  
It-chef, UmU

## Electronic Identity A Development Project Starts



- We are starting a project to develop a network based infrastructural service for authorisation.
- By that we right now mean →
- We? Not finally decided yet.
- Financing - not a problem - some central funds and member fees

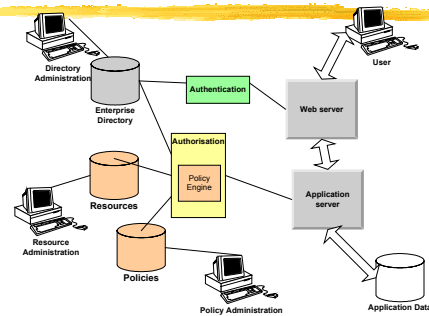


## Electronic Identity Why Such a Service?



- Our IT-systems are becoming more and more integrated and the concept of a user is widening to, in many cases, include all our students and/or personnel.
- It is becoming more and more unrealistic to manage users, accounts and access control within each application.
- What can be viewed as authentication from one system's point of view is authorisation in an enterprise view.
- This is a middleware service

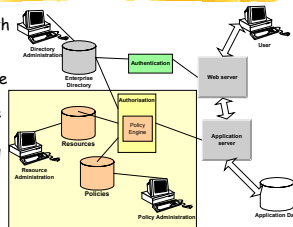
## Electronic Identity A Model Architecture



## Electronic Identity Service Model



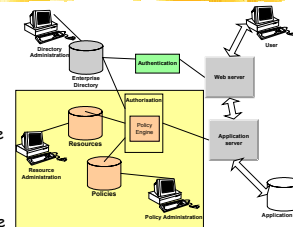
- The web server authenticates the user with a certain strength
- When the user wants to do something in the application (have access to a resource), the application server asks the authorisation server for advice
- The authorisation server receives the request and, using the policies for the application and information about the resource and the user, (does not) recommends access
- The application (does not) grants access to the resource



## Electronic Identity Some Deployment Models



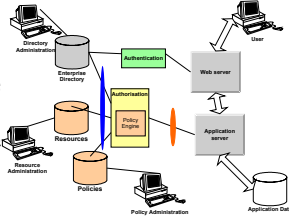
- serve one particular application at a particular university
- serve a common application that is deployed independently at several universities
- use a general role data base for a university and serve several smaller web applications at that university
- provide authorisation advice to ONE application that has users in different universities



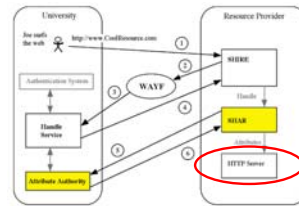
## Electronic Identity Specification Discussions



- We have focused on the functional specification of the Authorisation Server Interface (in red) and on the information needed by the Policy Engine. The protocol has not really been discussed.
- We are planning to define an API (in blue) to be used by the Policy Engine when retrieving information about users and resources
- Plugins for what info sources?
- We have not specified the Policy Engine



## Electronic Identity Relation to Shibboleth?



- From our point of view
- Shibboleth serves attributes

## Electronic Identity Project Organisation



- Up till now - a feasibility study
- Right now
  - setting up a steering committee consisting of representatives for the stakeholders
  - .. to make decisions of ambition and priorities
- Next month
  - Set up a construction team to complete the specification, get it approved and start
- Construction from June

## Electronic Identity Some Further Info on the Project?



- A network based infrastructural service for **Authentication and Authorisation**
- Cost of **construction** estimated to 1"6 - 2"4 sek (180' - 250' euro) depending on level of ambition
- Up till now 450'sek (50' euro) for planning and functional specification
- Risk now, basically organisational
  - A good policy engine is critical for the success of the project
  - Directory competence is available
  - Harmonisation of roles and directories "needed"
  - Use of identifiers has to be studied (locally)
    - see Early Harvest for examples
  - Implementation and **maintenance** organisation needed