FAME-PERMIS Project

University of Manchester
University of Kent

London, July 2006
FAME-PERMIS Project

- Stands for **Flexible Authentication Middleware Extension to PERMIS**
- Addresses Access Management with Shibboleth:
  - Authentication (FAME)
  - Authorisation (PERMIS)
- FAME-PERMIS is a collaboration between Universities of Manchester (FAME) and Kent (PERMIS)
- PERMIS:
  - Policy based access control decision engine for user authorisation
  - Decisions are made based upon: *(Subject, Target, Action)*
FAME-PERMIS Objectives

• Currently, there is no linkage between access control and user’s authentication level:
  – What authentication method user used?
    • PIN, IP address, password, strong password, certificate, smart card, biometric device
  – How strong and secure is this method?

• FAME:
  – Perform user authentication and assign Level of Authentication Assurance (LoA) to user
  – Support wide range of authentication methods
  – Provide Single Sign On (SSO)

• Use Shibboleth to link LoA derived by FAME with access control decision making provided by PERMIS

• Extend PERMIS:
  – Instead of (Subject, Target, Action),
  – We now have (Subject, Target, Action, LoA)
Why FAME-PERMIS?

• Users demand more authentication flexibility and support for out-of-office use and access to resources
• Need for role-based (not identity-based) Access Management:
  – Access is based on the user’s role within the institution (e.g. staff@man.ac.uk), rather than the users identity (e.g. j.smith@man.ac.uk)
• Improved security for resources (more fine-grained access control)
Benefits

• Multi-factor authentication
• Freedom to choose from several authentication methods
• When user is away or does not have all the technology required for authentication (e.g. card reader or biometric device), he/she may choose different authentication method
• Combine several authentication methods to gain higher LoA
• Access control decisions can now take into account the strength of the authentication method (how certain are we the user is indeed who he/she claims to be)
Implementation Infrastructure

- FAME-PERMIS uses JISC-adopted Shibboleth infrastructure to link FAME with PERMIS
- Shibboleth defines a set of protocols for secure passing of identity information between users’ home institutions (IdPs) and service providers (SPs)
- Shibboleth relies on the home institution to establish the user’s identity, and on the resource provider to grant access to the user based on the information about the user (i.e. user’s attributes) released by the home institution
FAME-Shibboleth-PERMIS Integration

- Check out our FAME-Shibboleth-PERMIS demo at Access Management Showcase on 18th July
FAME-PERMIS with GridSite

- GridSite uses X.509 certificates to authenticate users accessing Grid services and subsequently granting/denying read and write authorisation on this basis.

- GridSite wants to:
  - Allow its users access with username/passwords when user’s certificate is not present (user is away).
  - Give users authenticated with username/passwords a reduced set of options, e.g. users can view their running jobs but cannot modify them.

- FAME-Shibboleth can be integrated with GridSite in a similar manner as with Shibboleth-PERMIS:
  1) Authenticate Grid users using FAME (with 2 authentication options) to enable shibbolized user authentication across different institutions.
  2) Then have GridSite carry out authorisation as normal.
User tries to access an SP
User is redirected to the WAYF service.
User is redirected to his IdP’s FAME service to select an authentication service.
User authenticates himself
User is redirected back to the SP he initially tried to access
Contact

• FAME
  – Dr. Ning Zhang and Dr. Alexandra Nenadic (University Of Manchester)
  – E-mail: {nzhang, anenadic}@cs.man.ac.uk

• PERMIS
  – Prof. David Chadwick (University Of Kent)
  – E-mail: d.w.chadwick@kent.ac.uk

• GridSite
  – Dr. Andrew McNab (University Of Manchester)
  – Andrew.McNab@man.ac.uk