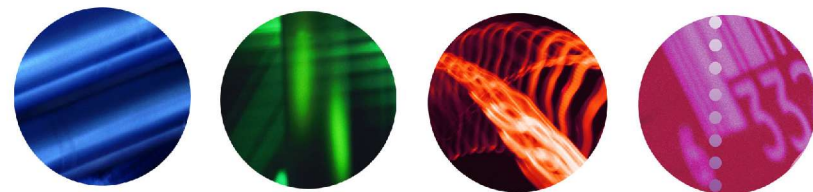


## Overview of Shibboleth

Alan Robiette, JISC Development Group

[<a.robiette@jisc.ac.uk>](mailto:a.robiette@jisc.ac.uk)



Supporting education and research

# JISC's agenda in AAA

---

- To develop new and extend existing technologies in access management (AAA), which are
  - Standards-based
  - Aligned with other national and international developments
  - Aimed at future service deployment, in national and/or institutional contexts
  - Designed to address certain scenarios which are currently difficult to handle



# Key scenarios

---

- A next-generation AAA infrastructure must support the following scenarios:
    - Internal (intra-institutional) applications as well as use between organisations
    - Management of access to third-party digital library-type resources (as now)
    - Inter-institutional use – stable, long-term resource sharing between defined groups (e.g. shared e-learning scenarios)
    - Inter-institutional use – ad hoc collaborations, potentially dynamic in nature (virtual organisations or VOs)
- 



# VO characteristics

---

- A VO's members typically belong to more than one real organisation
    - Wishing to share resources across real-world organisational boundaries (often problematic in security terms)
    - VO membership – which may be more or less formal – could be based on numerous criteria (discipline, project, course enrolment, personal interests ...)
    - The authority regulating VO membership could equally take many forms
    - And timescales may be very varied also
- 



# Principles (1)

---

- Authentication is the responsibility of the user's home site
    - Requests to authenticate the user should be routed back to the home site and take place there
    - National infrastructure will require institution-wide authentication services which can be interfaced with other AAA components
    - JISC has commissioned some evaluation work on single sign-on technologies which reported during the summer
- 



# Principles (2)

---

- Authorisation is the responsibility of the resource owner
  - Based on attributes supplied by the home site (and/or possibly other authorities)
  - Workable systems depend on agreed attribute naming and sources of authority
  - Progress towards more sophisticated management of digital rights (DRM) requires increased intelligence in the resource's decision engine

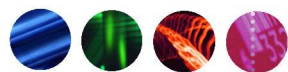
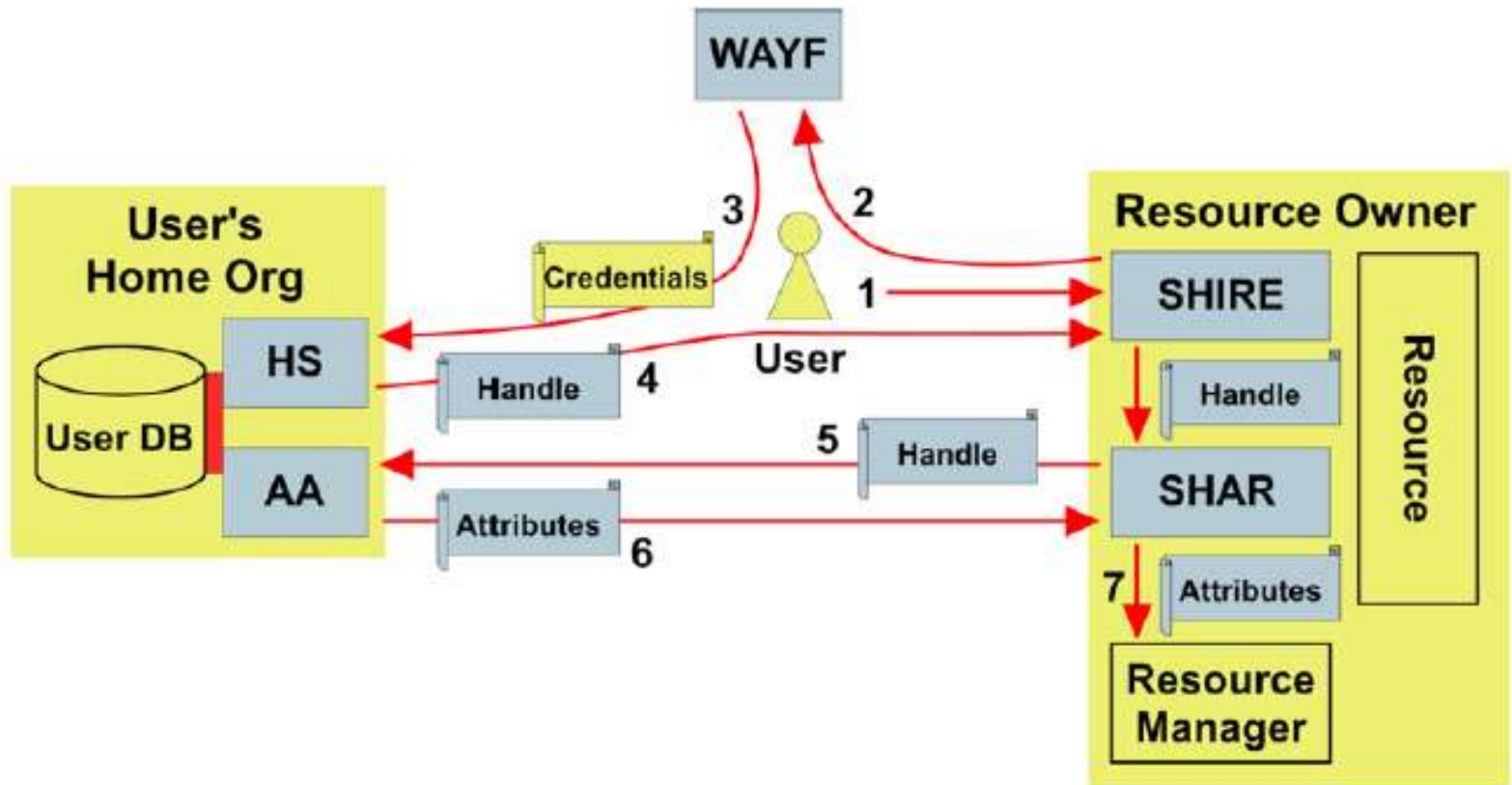


# Shibboleth

- An architecture developed by the Internet2 middleware community
  - NOT an authentication scheme (relies on home site infrastructure to do this)
  - NOT an authorisation scheme (leaves this to the resource owner)
  - BUT an open, standards-based protocol for securely transferring attributes between home site and resource site
  - Also provided as an open-source reference software implementation



# How does it work?



# Standards & technologies

---

- Shibboleth message flows defined in SAML
    - SAML = Security Assertion Mark-Up Language, standardised by OASIS
  - Standard attributes mostly from eduPerson and eduOrg schemas
    - But communities can extend these as required
  - Reference implementation uses Apache, Tomcat, Java, OpenSAML
- 



# Shibboleth pros

---

- Good international acceptance
    - US, Australia, some European countries
  - Basic software now well tested
    - Around 30 US universities working with it seriously, plus several content vendors
    - Swiss national HE system deployment
  - Satisfies the main requirements “out of the box”
    - Addresses digital library, shared e-learning and internal use scenarios
- 



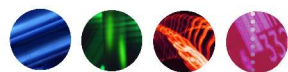
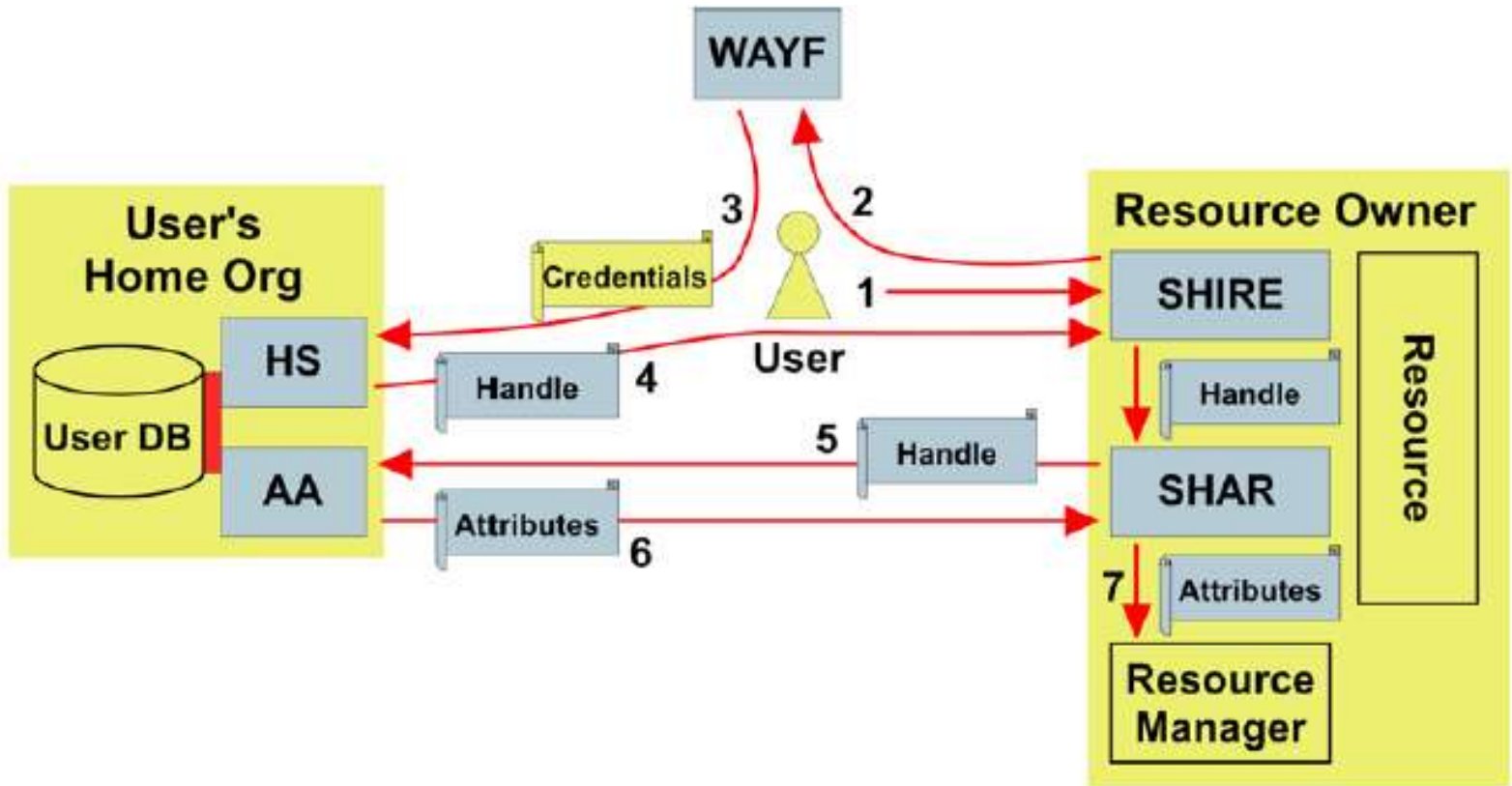
# Shibboleth cons

---

- Software still lacks user-friendly management tools
    - In its present state, still quite demanding to install and run
    - Might require outsourced or packaged services for smaller institutions?
  - Relatively unsophisticated authorisation model
    - Single attribute authority
    - No generalised decision engine
- 



# Architecture recap



# Coping with VOs

---

- **Problem:** typically a VO involves at least two sources of authority
    - User's identity derives from home institution
    - User's VO membership and privileges derive from the VO's own authority
  - **Solution:** add more intelligence to the Shibboleth resource manager
    - Policy-driven decision engine
    - Multiple sources of authority
- 



# Permis

- What is Permis?
  - A policy-based decision engine
  - Policy expressed in XML (compliance with the OASIS XACML standard planned)
  - Supports multiple sources of authority
  - Decisions based on roles or discrete attributes of users
  - User attributes stored in X.509 standard attribute certificates
  - Stable, portable implementation now included in NMI release



# Shibboleth + Permis

---

- Extend Shibboleth resource manager by incorporating the Permis decision engine
    - Resource owners can then set much more complex policies, embodying their conditions of access
    - Attributes can be gathered from more than one location (and be supplied by more than one authority)
    - Thus meeting the needs of VOs and providing much more fine-grained control
- 



# What is JISC doing?

---

- Service building activities
    - Aimed at AY 2006/7
    - Critical mass of (JISC-funded) resources
    - Gaining experience in institutions
    - Cultivating publishers etc.
  - Development projects to enhance Shibboleth (starting to deliver)
    - Permis integration (just completed)
    - Also several test scenarios (Grid and other, e.g. shared e-learning)
- 



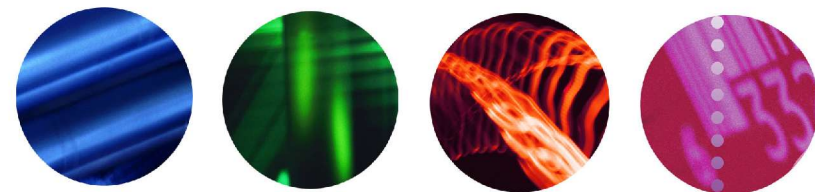
# Also ...

---

- New “virtual research environment” programme
  - Aim to bring together tools, services etc. in integrated user-friendly environments
  - Funding just awarded (Autumn 2004) to around 15 projects
  - Will require serious interfacing to security infrastructure
  - Watch this space!!



## Questions?



Supporting education and research