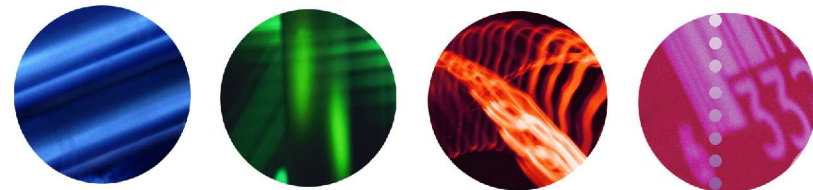


## **Shibboleth in the UK (JISC) Community**

Alan Robiette, JISC Development Group

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



Supporting education and research

# Outline

---

- Shibboleth
  - What is it?
  - What are its main strengths and weaknesses?
  - Why is it of interest to JISC?
  - JISC programmes of relevance
- Shibboleth and Grid security
  - Reflections on the problem space
  - What part can Shibboleth play in this?



# 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



# Why “Shibboleth”?

---

And the Gileadites took the passages of Jordan before the Ephraimites: and it was so, that when those Ephraimites which were escaped said, *Let me go over*; that the men of Gilead said unto him, *Art thou an Ephraimite?*

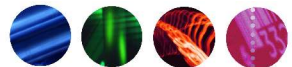
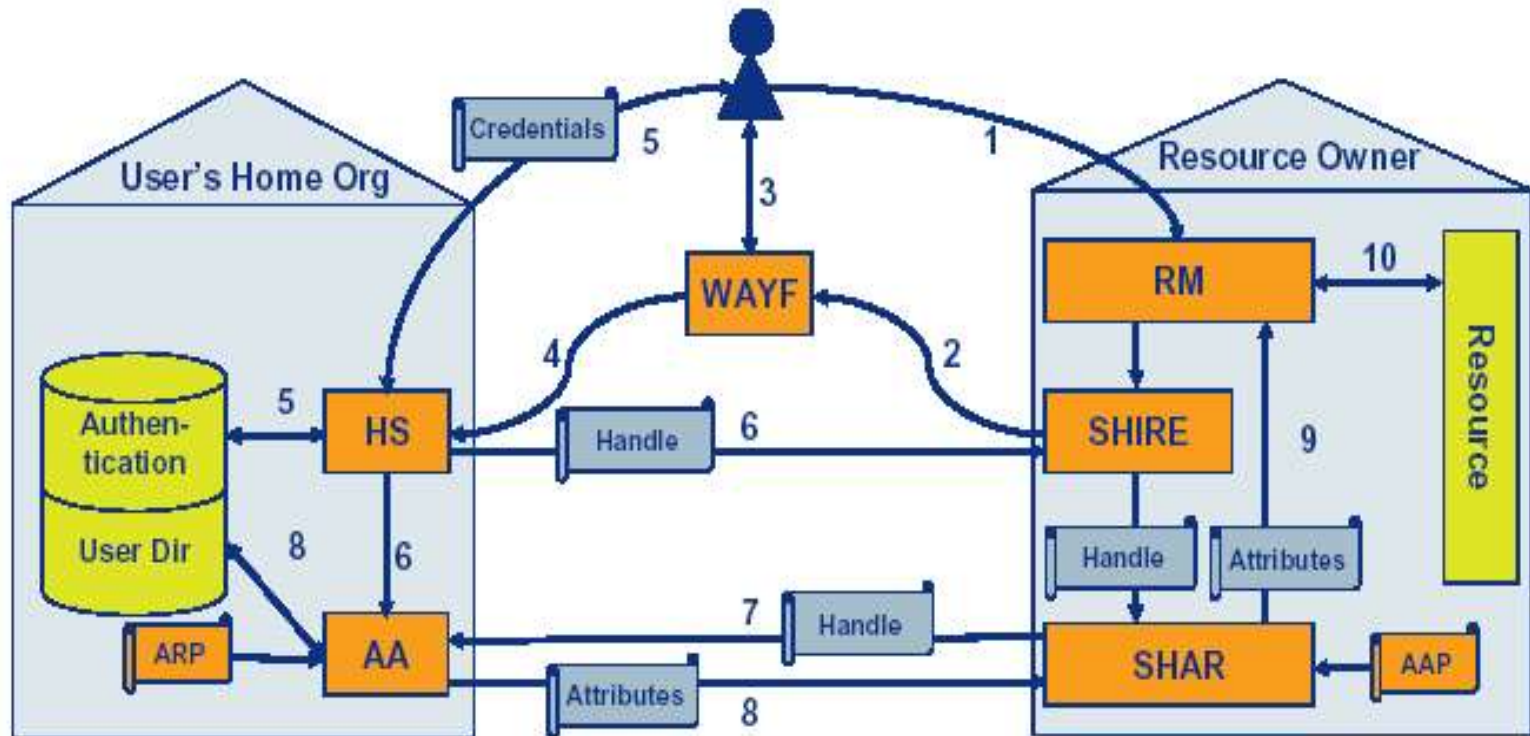
If he said, *Nay*; Then said they unto him, *Say now Shibboleth*: and he said *Sibboleth*: for he could not frame to pronounce it right.

Then they took him, and slew him at the passages of the Jordan: and there fell at that time of the Ephraimites forty and two thousand. (*Judges 12:5-6*)

---



# 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 a range of requirements “out of the box”
    - Addresses digital library, shared e-learning and internal use scenarios
- 



# Shibboleth cons

---

- Not currently fully web services compliant
    - In the sense of SOAP/WSDL etc. – uses SAML directly over http
      - Thus as is, mainly of value in browser-based contexts (also mainly for 1-tier situations)
  - Relatively unsophisticated authorisation model
    - Single attribute authority
    - No generalised decision engine
- 



# What is JISC doing?

---

- Three main programmes:
    - Shibboleth production infrastructure roll-out
      - More details in a moment
    - Middleware technology development
      - Aiming to extend the capabilities of Shibboleth (in liaison with Internet2 and others)
    - Virtual research environments programme
      - Exploring how full-featured, user-friendly environments can be built to support e-research across many disciplines
- 



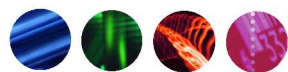
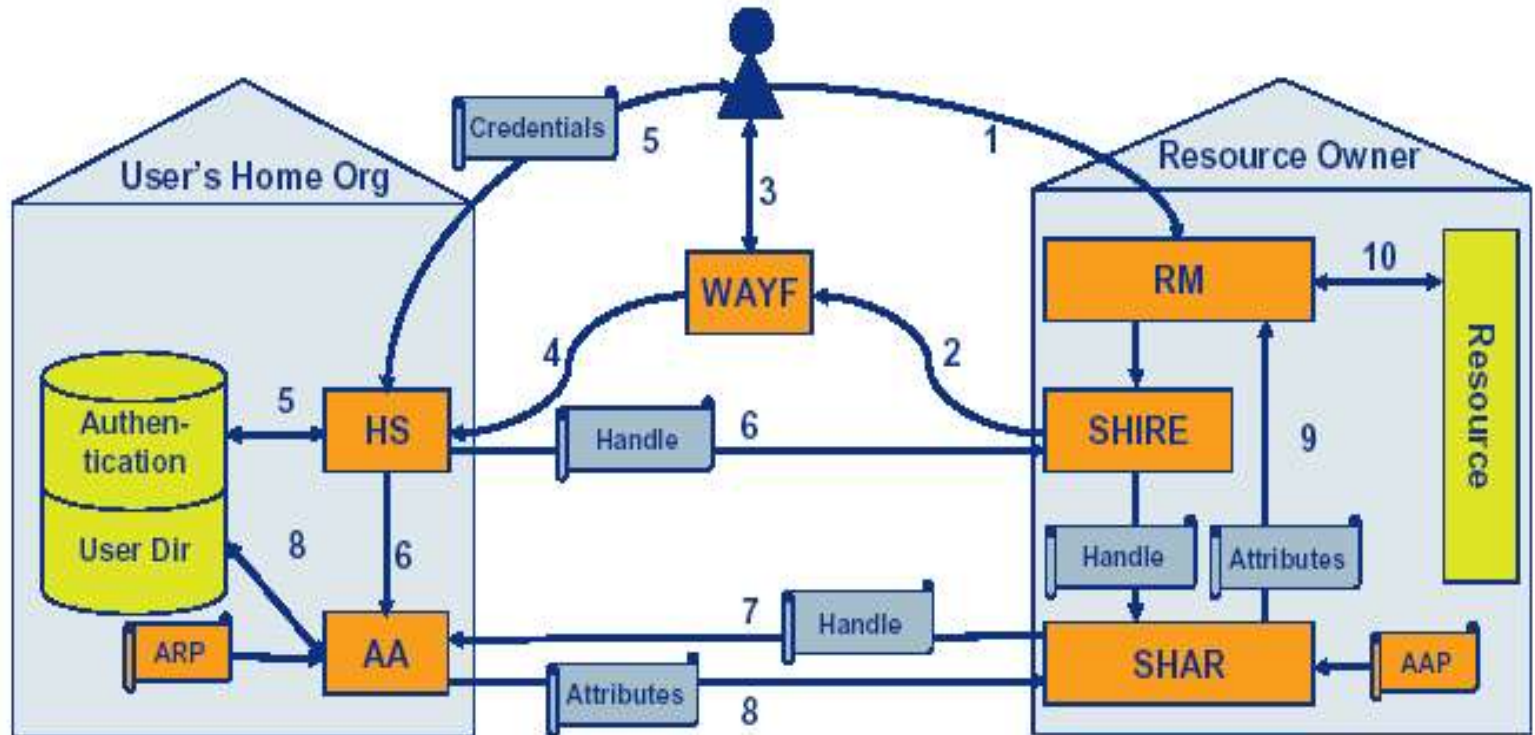
# Technology development

---

- Main theme is to add more intelligence to the resource manager
    - Integrate PERMIS as decision engine
      - Policy-driven access control
      - Attributes can be from multiple authorities
    - Shibboleth/PERMIS/Apache integration completed by David Chadwick's group late 2004
    - Now in test by 4 other projects, with varied VO scenarios
- 



# Architecture recap



# Production roll-out

---

- Implement Shibboleth on JISC services
    - Provides a critical mass of Shibboleth-enabled resources
  - Gain experience on campuses
    - In a variety of institutions
  - Build the national components
    - Which are relatively few
  - Charm offensive with publishers
- 



# Questions for today

---

- How is “identity proofing” done?
    - By whom? To what standards?
  - How and where is authentication carried out?
    - One technology, or more than one?
  - How is authorisation handled?
    - Especially in multi-tier situations
  - And generally
    - Are we looking for a single magic bullet, or a kit of parts satisfying varied needs?
- 



# Answers (in the Shib case)

---

- How is “identity proofing” done?
    - Assumed to be by the user's home organisation, typically via standard registration practices
  - How and where is authentication carried out?
    - Always at the home organisation, using the on-campus norm
  - How is authorisation handled?
    - Always by the resource provider, on the basis of the attributes transferred
- 



# The n-tier problem

---

- Example
    - User accesses portal
    - Portal invokes a back-end service (e.g. a computation)
    - Computation needs to access data repository
    - Repository accesses storage device (possibly needing write/update rights)
    - Etc.
    - Different A&A conditions may apply at each of these stages
- 



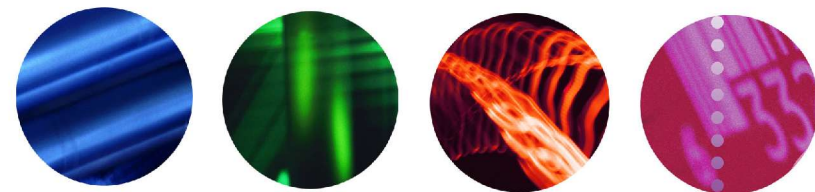
# What can Shib contribute?

---

- Standard Shibboleth can perform initial authentication into any web-enabled environment
    - Plus transfer of campus-based attributes, where these would be useful
    - This then requires additional technology to address any additional services downstream
  - Shibboleth + PERMIS offers more
    - Complete solution (including VO support) for any web-facing 1-tier situation
- 



## Questions?



Supporting education and research