Identity Services beyond Web Single Sign-On

Josh Howlett, JANET(UK)
TF-EMC2
29 June, 2011
Contents

• Standardisation

• Implementation

• Deployment

• CGAMS proposal
Standardisation

• Work happening in or around KITTEN
  – Charted to deliver SASL mechanisms for OpenID, SAML and Oauth
  – Web-bound authentication
    • draft-ietf-kitten-sasl-openid
    • draft-ietf-kitten-sasl-saml (WGLC)
    • draft-mills-kitten-sasl-oauth
  – Non-web authentication
    • draft-cantor-ietf-kitten-saml-ec
  – Other relevant work
    • draft-ietf-kitten-gssapi-naming-exts (WGLC)
Standardisation

- Work happening in or around ABFAB
  - Charted to deliver an EAP & SAML based federation architecture
  - draft-lear-abfab-arch
  - draft-ietf-abfab-gss-eap
  - draft-ietf-abfab-aaa-saml
  - draft-winter-abfab-eapapplicability
  - draft-perez-abfab-eap-gss-preauth
Implementation

- draft-ietf-kitten-sasl-saml
  - Experimental proof-of-concept?
- ABFAB
  - Project Moonshot
    - Support for Mac OS X, Linux, FreeBSD, JUNOS, Windows – should be mostly done by end of July.
    - Tested successfully with a number of applications (OpenSSH, OpenLDAP, Samba, Firefox, Apache, Adium, Jabberd...)
    - Live DVD available
  - University of Murcia
    - GSS pre-authentication for MIT Kerberos, using GSS EAP
    - Possible solution for scaling Kerberos cross-realm operation?
Deployment

• Project Moonshot
  – JANET RADIUS infrastructure modified to support ABFAB-based operation
    • National RADIUS proxy validates the claimed value of the GSS-Acceptor-Realm-Name attribute against Institutions’ registered realms (eg. Is the University of Oxford permitted to claim server.ox.ac.uk?).
  – Small number of test service providers already connected
  – Authenticate with any eduroam IdP today!
  – Technical pilot planned with UK HPC & Grid community, commencing in September or October.
  – Planning workshop on Thursday 7 July – all welcome...
CGAMS proposal

• Common Global Access Management System
  – BoF @ TNC 2011
  – http://webmedia.company.ja.net/edlabblogs/developmenteye/2011/05/10/proposal-for-a-common-global-access-management-system
  – Can we build an integrated infrastructure?
    • An access management system serving multiple communities and their networks, applications and services.
    • Reduce complexity
    • Increase functionality and scalability
  – Conclusions
    • The concept sounds like a good idea.
    • But the proposal needs more detail to assist evaluation
    • Proposed direction seems reasonable
  – Next steps