Abfab Intro

Klaas Wierenga

klaas@cisco.com

IETF79, 11 November 2010
Outline

• History
• Example Use Case
• Basic Component choices
• Starting Points
• Deliverables
History

- Pain points in HigherEd community with federated access
  - WebSSO only does web
  - WebSSO has IdP discovery problem
  - WebSSO has problems with multiple affiliations
  - No uptake of Kerberos for inter-domain
  - Federated Network Access methods only do network access
- Idea: Combine strong points of WebSSO with those of Federated Network Access
- Bar BoF @ IETF77
- BoF @ IETF78
- Abfab WG created in September 2010
Example Use-case: Out-sourcing

Organizations increasingly want to:

• Reduce costs by out-sourcing commodity services to third party service providers.
• Use their own managed identities to provide SSO

SAML provides this for Web-based services...
• ...but not other types of services (IMAP, POP3, SMTP, CalDAV, etc).
• Identity Provisioning APIs exist, but they’re typically not appropriate.
Basic Components

• Authentication
  – EAP

• Assertions
  – SAML

• Federation
  – AAA (RADIUS, Diameter)

• Application Integration
  – GSS-API
Starting points

• draft-ietf-abfab-aaa-saml
  – Carry SAML over AAA

• draft-ietf-abfab-gss-eap
  – GSS-API Mechanism that encapsulates EAP

• draft-ietf-abfab-gss-eap-naming
  – Naming SAML assertions, SAML attributes and RADIUS attributes in GSS-API EAP mechanism
Deliverables

• Use cases (informational)
• Architecture document (informational)
• Update to the EAP applicability statement in RFC 3748 (standards track)
• Solution for using EAP methods to provide authentication within the application (standards track)
• Update to the Extended Master Session Key root key applicability statement in RFC 5295 (standards track)
• Description of GSS names and name attributes required by the solution (standards track)
• Descriptions of usability and user-interface concerns related to this work (informational)
• Protocol for carrying SAML messages in RADIUS and Diameter (standards track)