SASL-SAML update

Klaas Wierenga
Kitten WG
9-Nov-2010
Topics

- Update on SASL-SAML draft
- Difference between SASL-SAML and SASL-SAML-EC
Changes in SASL-SAML draft

- **WG -00**
  - Sanitized GSS-API stuff
  - Editorial changes

- **-01**
  - Server redirect is URI instead of HTTP redirect
  - Security consideration about secure channel
SAML 2.0 WebSSO flow

1. Resource Request
2. Authentication Request
3. Request SSO Service
4. Authenticate both client and IdP
5. Authentication Statement
6. Client passes AuthN Statement to RP
SAML 2.0 and SASL

SAML 2.0 and SASL

SAML Client (browser)

SASL server

Application

SASL Client
Pros and Cons

- **SASL-SAML**
  - minimal change to SASL client
  - no extra application that is trusted with authentication credentials
  - no need to touch the IdP
    - rely on external program
    - 'strange' user experience

- **SASL-SAML-EC**
  - 'cleaner' solution
  - no need for external program
    - yet another piece of software to trust with user credentials
    - IdP needs to support the ECP profile
    - SASL client needs to implement the ECP profile