A Brief Survey of Some Related Work
or
The Battle of the Heavyweights

DIX BoF, IETF 65
RL "Bob" Morgan
Topics

- SAML
- Liberty
- WS–Federation
- Identity Metasystem
SAML

- OASIS Standard, now at version 2.0
  - TC begun in 2001 by several vendors with similar but incompatible web SSO products, customers demanding interop, inter-organization (aka federation) support
  - v1.x specified basic web SSO functions
  - v2.0, based on input from Liberty Alliance etc, provides SSO, logout, ID management, privacy features, modularity to support non-web profiles
SAML Basics

• XML–syntax assertion formats
  – authentication, attribute, authorization–decision
  – assertion contains issuer, conditions, sig
  – request/response protocol for moving them
    • can be moved in many other ways too

• web browser signon profile
  – two major styles (artifact and POST)
  – attributes can be pulled by RP or pushed via browser
  – authn request can modify interaction with user
SAML Features

• Sessions, logout, identifier admin, etc
• SAML "metadata"
  – standardizes service description to automate site interaction
• extensibility
  – user identifiers, attributes, assertion conditions, metadata, authn context, etc
• SAML components reusable in many contexts
  – attribute statements in Kerberos, SIP, TLS
  – authn methods in SIP, SOAP
SAML Success?

• Many (>12) interoperable implementations
  – commercial and open-source
• Many large-scale adoptions
  – US Gov E-Authentication, other governments, many higher-ed federations, industry shared apps, many outsourced biz relationships, etc
• Continued active participation in TC
• Active development of opensaml library
SAML Failure?

- People continue to invent web signon schemes ...
  - docs too long to read?
  - too complicated to implement?
  - too hard to deploy identity provider?
  - extensibility not easy enough?
  - not available to PHP?
    - focus has been on webserver integration
SAML mods to meet DIX requirements?

• under discussion in SAML community
  – remove XML signature dependency ?
  – remove strong security requirements ?
  – remap to non–XML syntax ?
  – make attribute statement contents visible ?
    • this is implementation option now
    • maybe specify human–readable attr display?
  – maybe it's just about libraries in all languages ?
Liberty Alliance

• Identity Framework (ID–FF) is just SAML 2.0
• Service Framework (ID–WSF)
  - framework for accessing identity-based services using SOAP (aka "Web Services") eg mail, calendar, address book, group mgt
  - layered on ID–FF security/privacy, plus WS–Sec, WS–Addressing
  - discovery, access, access control across distributed/federated providers with privacy
  - v 2.0 out "soon"
WS–Federation

• component of WS–* spec set
  – i.e., WS–Sec, WS–Trust, etc
  – "passive profile" is clone of SAML browser profile
  – "active profile" specifies federated access for SOAP–based clients/servers

• supported in Microsoft ADFS product
  – and compatible products from others

• can use SAML assertions internally ...
Identity Metasystem

• Microsoft vision, architecture, implementation

• vision:
  – "identity backplane" to link disparate identity systems
    • user identity provider uses system X, app uses system Y, security token service does translation

• architecture:
  – WS–Trust protocol supports token translation function
  – client–side component supports user interaction
Identity Metasystem

• implementation: InfoCard
  – "identity selector" that makes user's set of identity choices visible, manipulable as "cards", is new Windows platform function
  – cards can be self-generated (with key, ssh-like) or issued by identity provider
  – interacts with IdPs, apps via WS-Trust

• others working on compatible implementations

• WS-Trust being standardized in OASIS
Role for DIX WG?

- Clarify competing requirements?
- Clarify deployment barriers?
- Clarify security gradient?
- ...