



Shibboleth, SAML, and PK(I/i)

Scott Cantor (cantor.2@osu.edu)
Internet2/MACE, The Ohio State University

April 29, 2003



Overview

Shibboleth uses SAML to provide access management for web-based resources in a manner that:

- is seamless (reduces barriers, clicks, sign-ons, etc.)
- is relatively secure (balanced against deployability)
- is manageable and scaleable (federated)
- preserves privacy and some degree of anonymity
- supports personalization (competing but not mutually exclusive with privacy)



Division of Duties

OpenSAML

- Implements messages and basic protocols defined by SAML 1.0
- Supports “context-free” signing and TLS exchanges

Shibboleth

- Concrete implementation of source and target site functionality (web server modules, caching, etc.)
- Adds privacy, federated trust, policy, metadata
- Framework for extending SAML exchanges with trust and policy constraints



Shibboleth and PKI

Shibboleth components, in the context of a federation, need to authenticate each other.

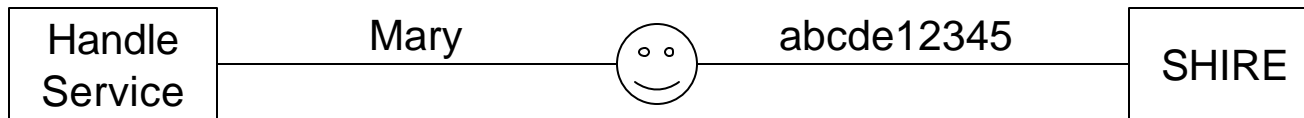
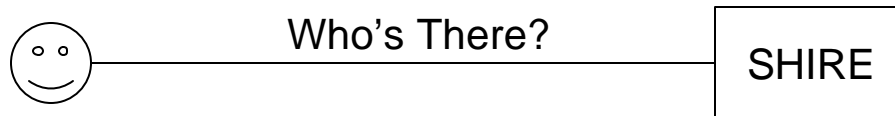
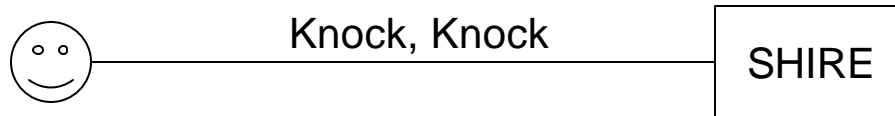
Could in theory use a variety of technologies (e.g. Kerberos), but in practice uses signatures and TLS authentication with X.509 certificates and RSA keypairs.

How many pieces are there?

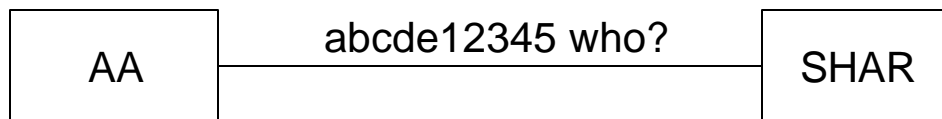


High Level Architecture

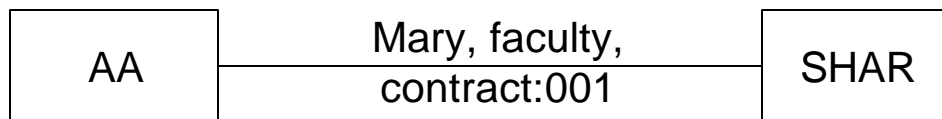
Knock, Knock...



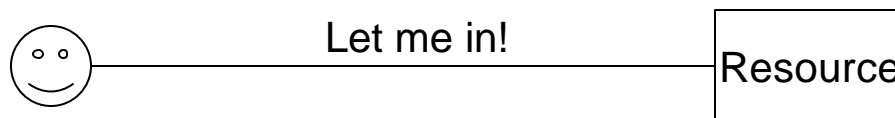
HS SSL Server
HS Signing Key
SHIRE SSL Server



SHAR SSL Client



AA SSL Server
AA Signing Key (opt)





Federated Trust Implementation

Currently a mix of code and libraries performing “traditional” certificate path validation using CA root lists via OpenSSL’s built-in verification.

Primary trust anchor is the Handle Service.

Specifics of InCommon’s trust infrastructure are yet to be finalized, but some models have emerged.



InCommon Proposals

Spectrum of models shift the burden between PKI and metadata:

- Certificate validation via traditional CA root lists and hostname/CN comparisons
- One CA vs. multiple CAs
- Name Constraints, Policy OIDs
- Pair-wise trust via signed metadata containing certificates or keys
- Implications for revocation



Federation Policy beyond PKI and SAML

- Semantics of Name Identifiers
- Attributes (federation currency)
- Attribute Release Policies
 - Constrains what an origin trusts a target to learn about its principals
- Attribute Acceptance Policies
 - Constrains what a target trusts an origin to assert to it independent of application policy; can be a mix of federation and target-specific policies