What's new in Shibboleth 2

Chad La Joie
Internet2 & SWITCH

Agenda

- Affiliation Disclaimer
- New Features: General
- IdP/SP Changes
- What do you need to know right now?
- What's in the Future

New Features: General

- SAML 2
  - SP control of authentication
    - Request authentication mechanism
    - Force re-authentication
    - Request passive authentication
  - Encryption of sensitive information
  - Persistent, opaque, name identifiers (handles)
- Metadata improvements:
  - Support for metadata retrieval in-process
  - Large metadata file support

Identity Provider 2.0

- Moved from a SAML Identity Provider to a security protocol platform that happens to support SAML
- What does that really mean to you?
  - Not a lot
  - Most of the changes are internal and hidden
  - Development of new features becomes a lot easier

Identity Provider 2.0

- Full support for different authentication methods
  - Methods: LDAP, Kerberos, Secure ID, IP address
  - Existing SSO solutions are still supported
  - Kaspar will demonstrate first extension
- True session management
  - Timeouts: Whole sessions, authentication method

INTERNET®

Identity Provider 2.0

- Support for complex attribute values content
- New Attribute Filtering Policy
  - Replaces ARPs and AAPs
  - Many more matching features (boolean operations, authentication method, attribute values, etc.)
  - Multi-policy support
- Support for gathering of metrics:
  - Apache style access log
  - IdP audit log: who got what info how?
  - Both in easily parsed format

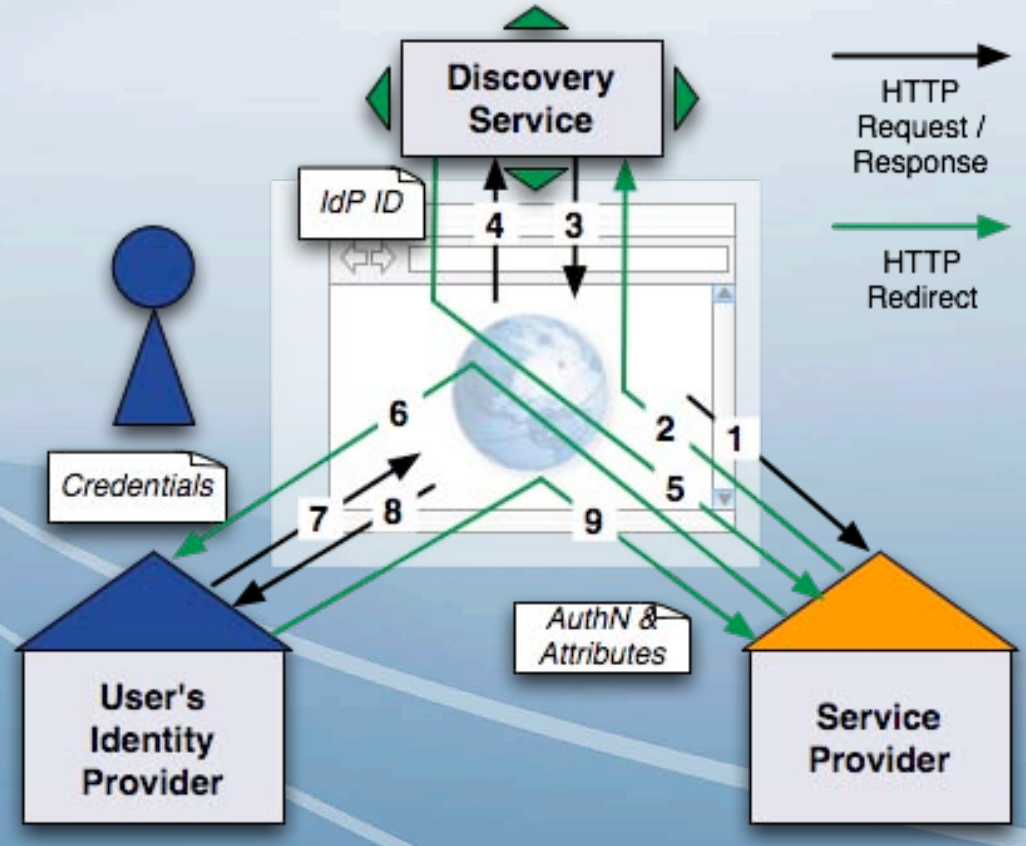
Discovery Service

- New name for the WAYF
- New Features:
  - Multiple federation support
  - Different views (e.g. test and production views)
  - Easily branded
  - SAML discovery protocol support
- Still written in Java

SP Changes

- Mostly internal work
- Multi-protocol support enabled by new discovery service
- Improved attribute extraction and caching
- Use of new Attribute Filtering Policy language
- Support for ODBC based storage of state
- Significant performance improvements

New Shibboleth 2.0 Flow



- User access resources (1)
- SP communicates with discovery service to determine IdP (2-5) NEW
- SP sends AuthN request (6)
- User authenticates (7,8)
- IdP sends AuthN & attribute information (9)
- No IdP to SP communication NEW

INTERNET2®

Why should I upgrade my IdP?

- Improved support for multiple authentication methods
- Better tools for creating and controlling release of attributes
- Less complex deployment options; no need for Apache, other SSO solutions, separate attribute authority virtual host and certificate
- Improved support for clustered IdPs
- Facilities for easily gathering metrics

Why should I upgrade my SP?

- Easier to deploy; less conflicts with operating system libraries
- Better performance and improved clustering support
- More attributes (e.g. AuthN method) and improved content access control mechanisms
- Force re-authentication and passive authentication

What do you need to know now?

- IdP endpoint URLs are changing
  - http://example.org/idp/saml2/POST/SSO
- Metadata needs some changes:
  - Public key/cert must be embedded for encryption
  - List SAML 2 as supported protocol when SAML 2 enabled
- Attribute push default attribute delivery mechanism in SAML 2
- 2.0 software interoperates with 1.3 software

What's Coming?

- Shibboleth 2.0 Release; Dec/Jan
- Java-based service provider
- Additional SAML 2 support: Single Logout, NameID management and mapping
- Support for additional protocols: ADFS, Cardspace, eAuth, WS-Trust
- Initial support for aggregating attributes, either at the IdP or SP, from multiple IdPs