

Shibboleth Plumbing: Implementation and Architecture

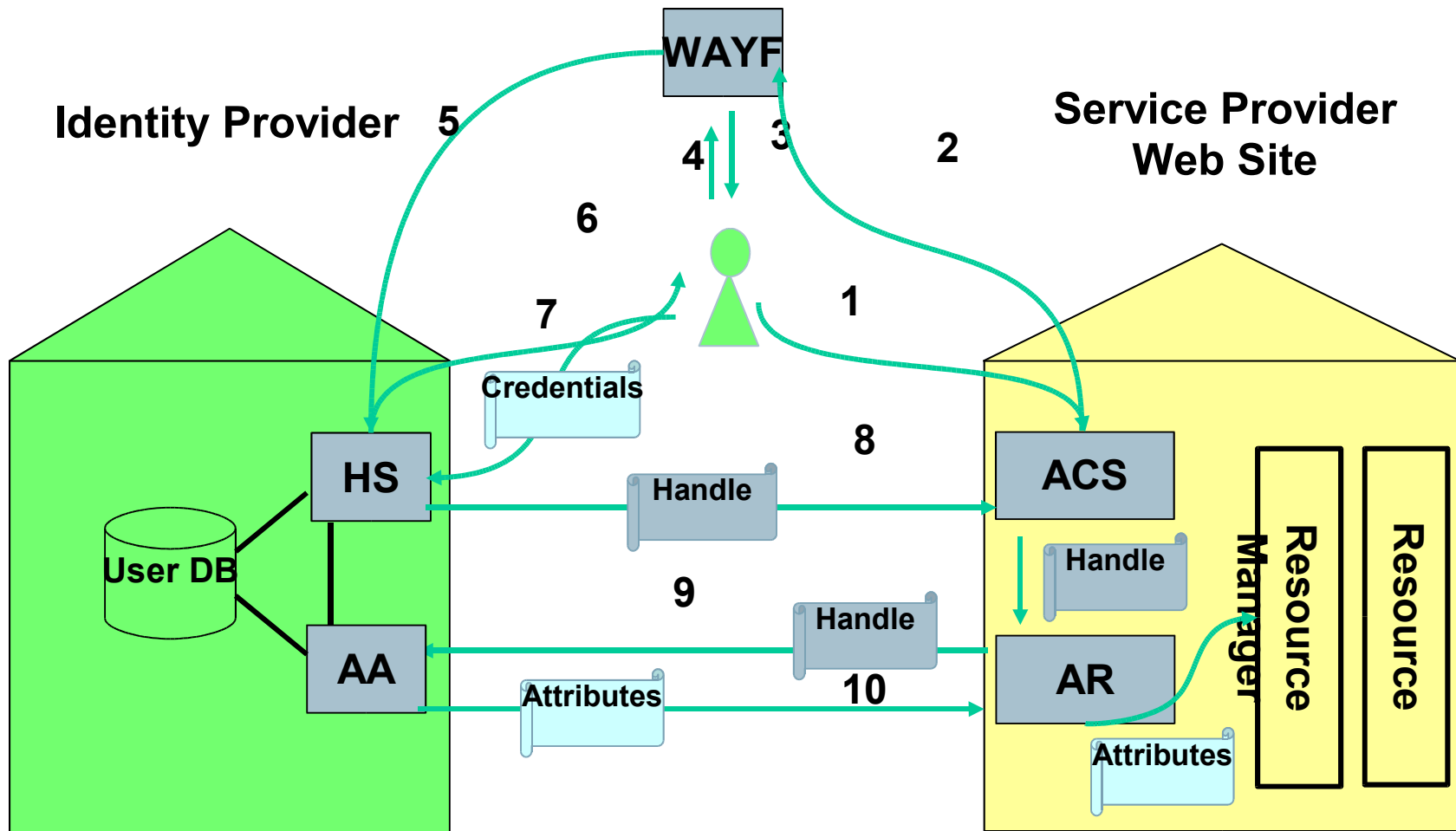
Nate Klingenstein
Internet2

<http://shibboleth.internet2.edu/docs/plumbing.sxi>

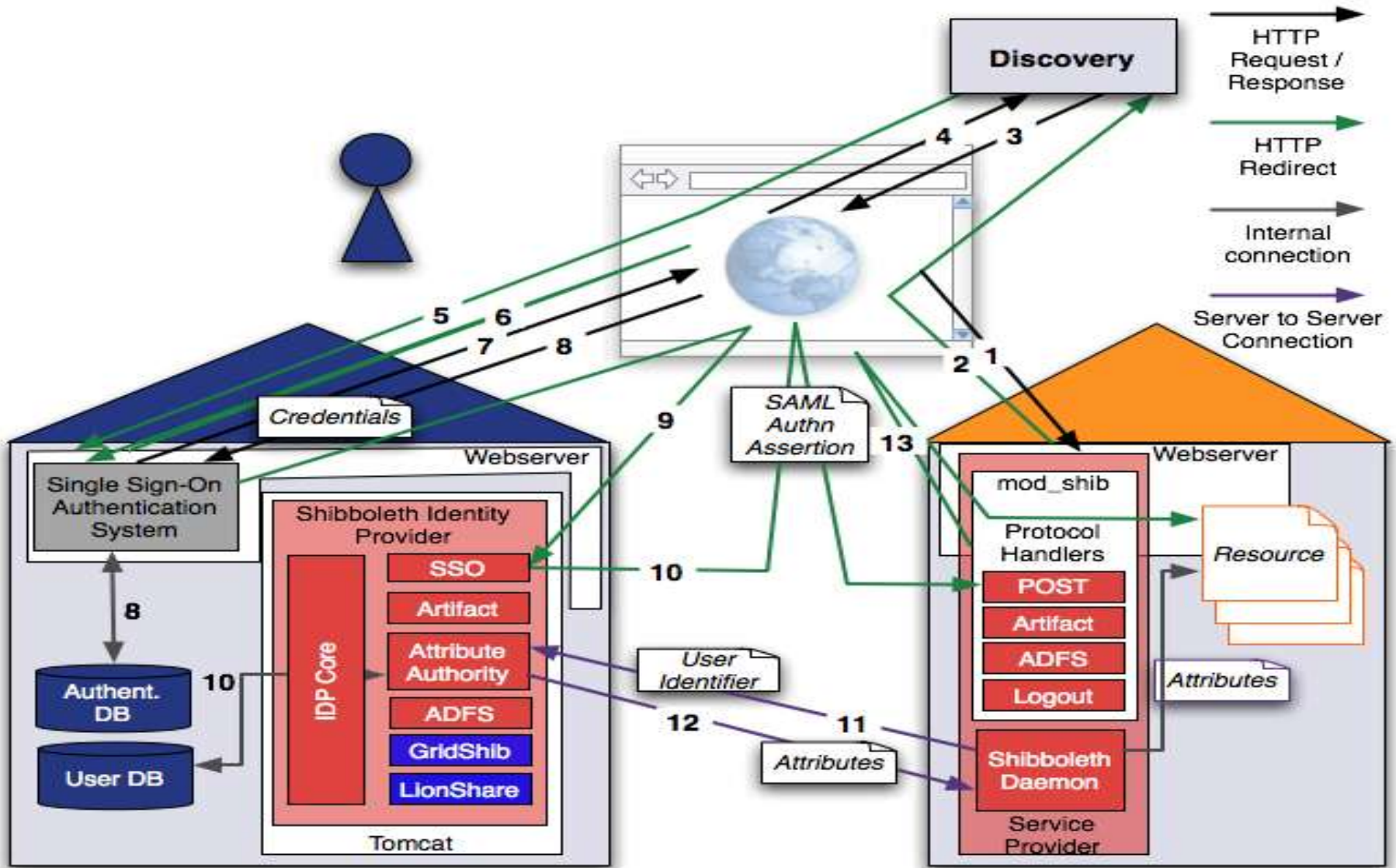
Overview

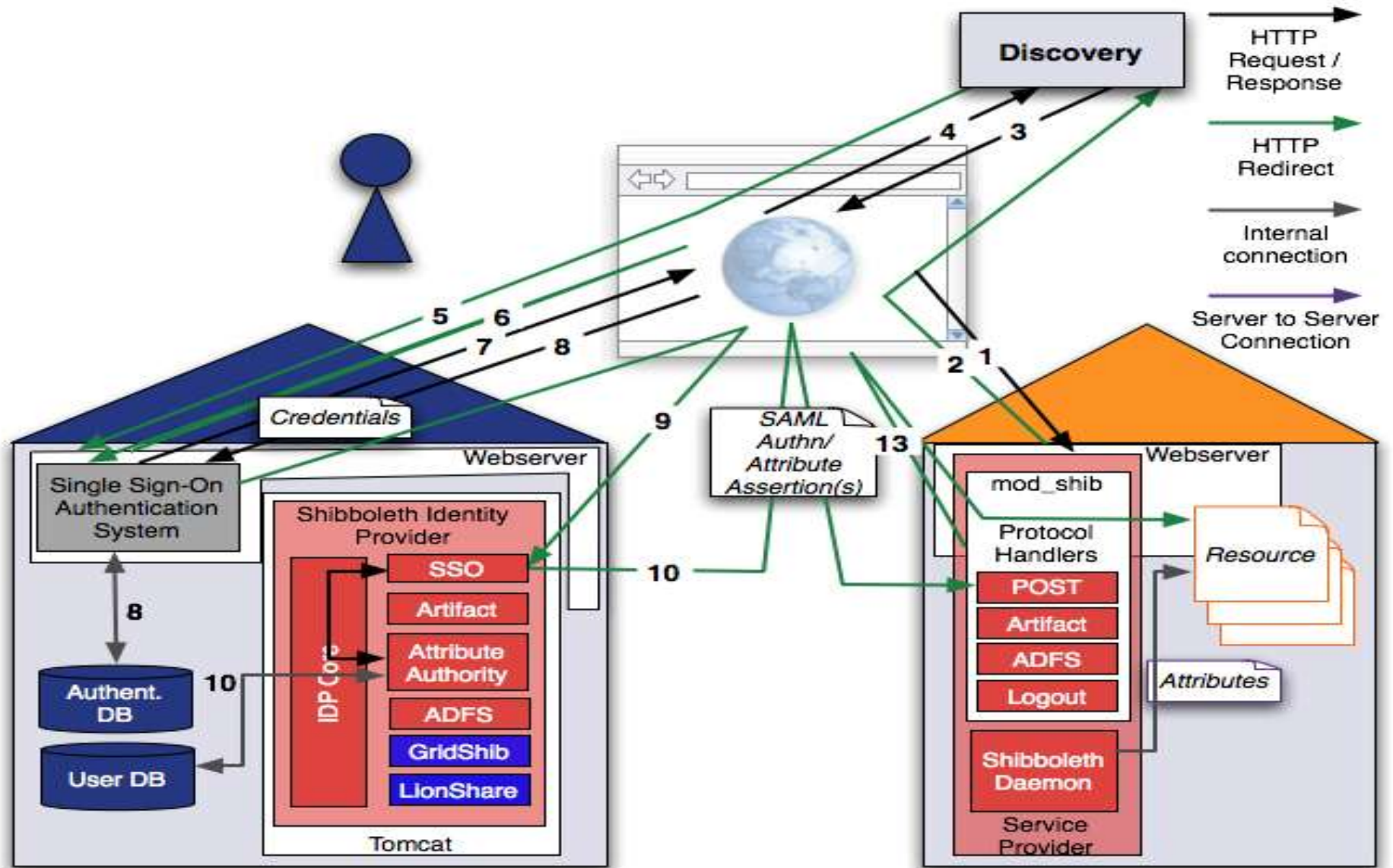
- Advanced Flows
- The IdP
- The SP
- The WAYF – Thomas Lenggenhager
- Deployment Considerations
- Example Applications
- Handing off to deployment – John Paschoud
- Questions & Answers

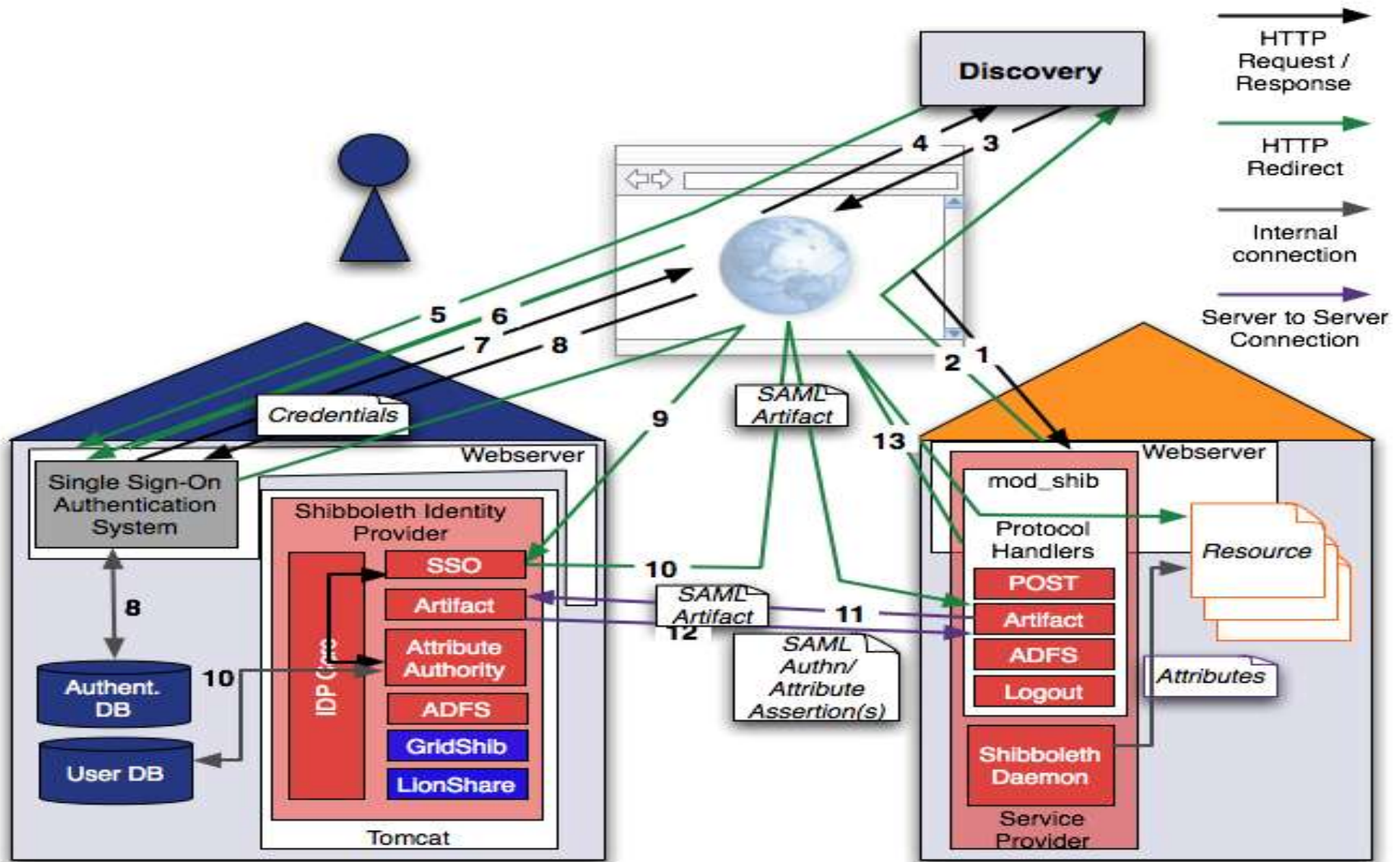
Shibboleth 1.2 & Earlier



© SWITCH







Installation

- Ant
- Binaries
- Eclipse
- Build from source
- Installation of other packages (mod_jk) the hardest part
- Easy
 - No, really, it is!
- Still too much vi; we're working on it

Shibboleth 1.3 Assertions & Bindings

- SAML 1.0/1.1 Authentication Assertion
- SAML 1.0/1.1 Attribute Assertion
- SAML 2.0 Metadata
- SAML 1.1 HTTP/POST & Artifact
- SOAP over HTTP over SSL/TLS
- Interoperability
 - Burton Group
 - eAuthentication

1.3 Extended Profiles

- Lionshare
- GridShib
- ADFS
- Much simpler in 2.0

SAML & Shibboleth 2.0

- Single Logout
- Authentication Request
- Decoupled from the web?
- Enhanced Client Profile (ECP)
- Interoperability

Delegation

- Allowing a third party to act on the behalf of a principal...
- With limitations
 - Duration
 - Permissions
- Used by portals, agents, etc.

Delegation Techniques

- Liberty Alliance
- WS-Trust
- draft-cantor-saml-ss0-delegation
- Recursive Delegation

Steven Carmody of IEEE and Brown

- Identity Federation vs. Federated Identity
- Bi-directional Persistent Pseudonyms
 - Expression of these pointers to third parties
 - Handling requests based on these pointers
- What makes an IdP an IdP?
- Strong homology to delegation

Single Logout

- Many different kinds of session
- Inter-realm functionality exponentially compounds the problem
 - Negative permissions are always hard
- 1.3: Cookies & homeURL
- SAML 2.0 Profile
 - Implementation and application support will be critical
- The ultimate: close the browser

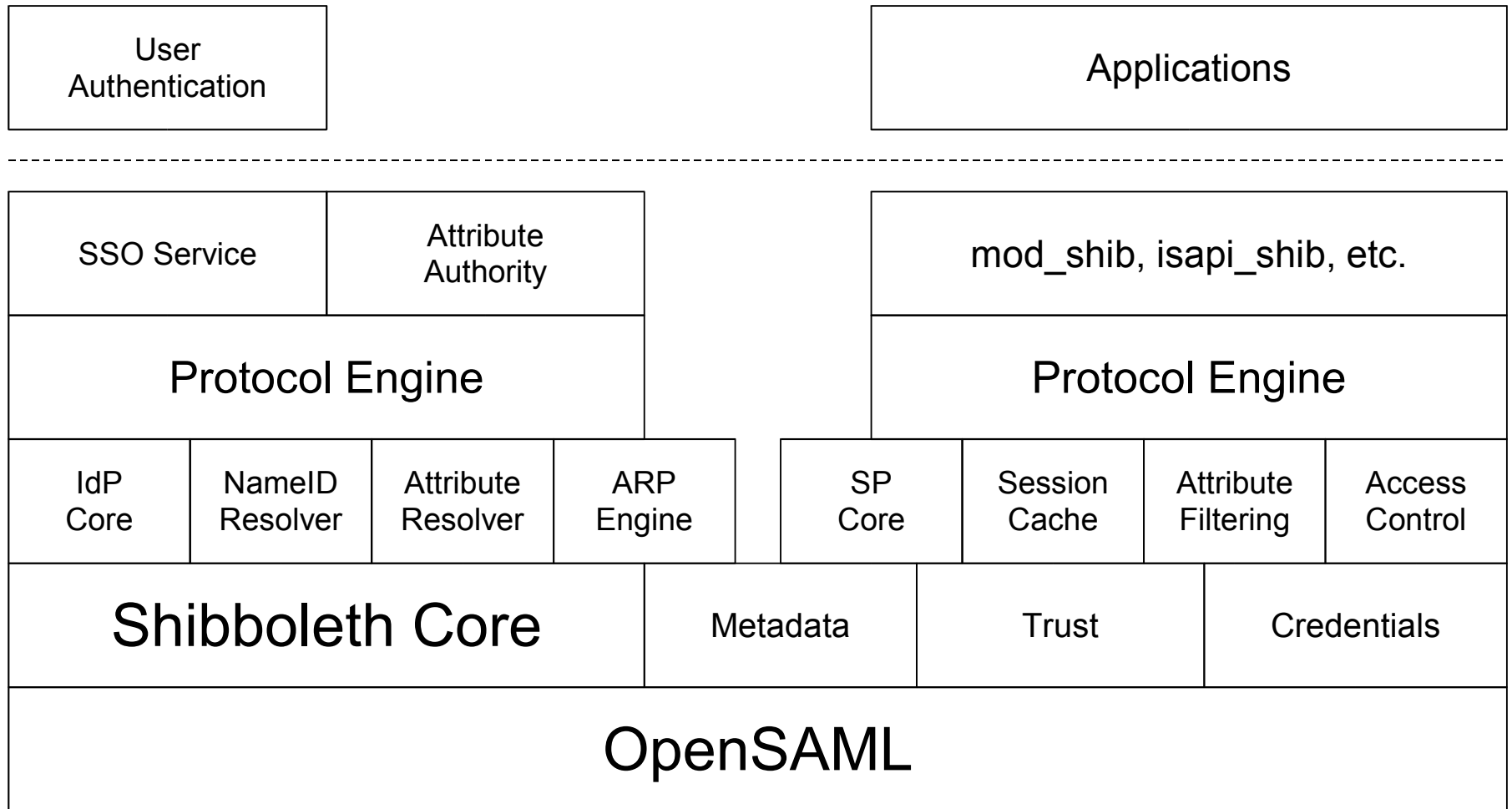
Naming

- Attributes
 - urn:mace:dir:attribute-def
 - urn:oid:
- Providers (providerId)
 - Same for SP's and IdP's
 - URI's (URL's or URN's)
 - Unique string names; NOT resource locations
 - ... yet?

Federations

- One of many trust structures
- Do Not Exist in the code
- Facilitate trust and simplify transfer between IdP's and SP's
 - ... but it's all bilateral in the end
- How many federations will the world have?
 - Peering?
 - Metadata, attribute, and certificate translation?
 - Dynamic trust?

Advanced Flows: More Boxes



Configuration Files

- Grand tour
 - idp.xml
 - httpd.conf
 - server.xml
 - jk.properties
 - resolver.xml
 - arp.site.xml
- Later, view them configured for applications

Attribute Resolver

- resolver.xml
- Java Generation
- JNDI
- JDBC
- Simple/Scoped

ARP's

- arp.site.xml
- Processing
- SHARPE

Authentication

- Apache/WebISO
- Tomcat/Java
- Multiple mechanism & LoA support
- Shibboleth authentication – 2.0?

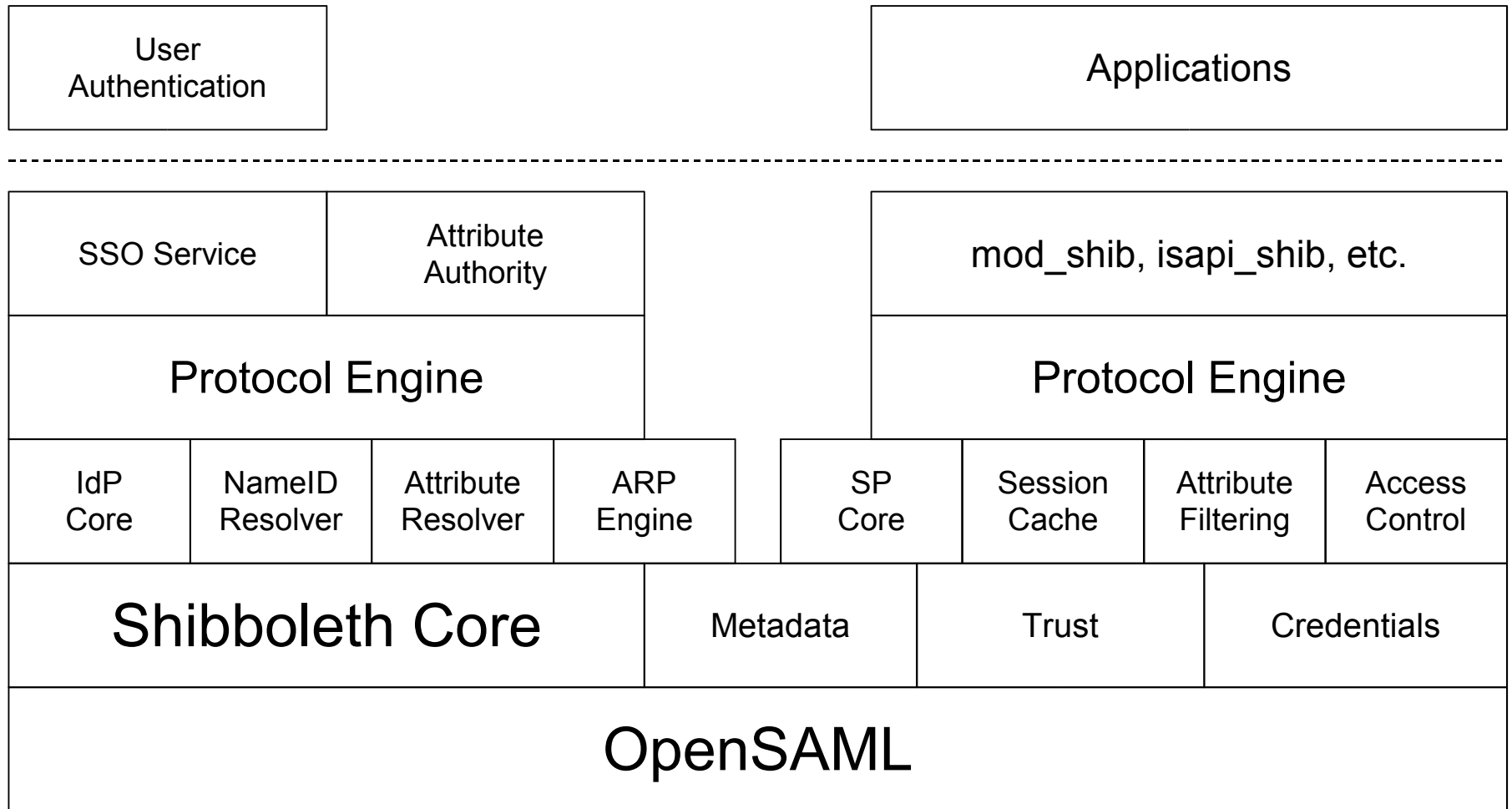
Logging & Auditing

- Logging Mechanisms
 - Built-In
 - Container logging
 - JULI
 - Log4J
- Errors
 - Interrealm error considerations
- Debugging & production configuration
- Demonstrations

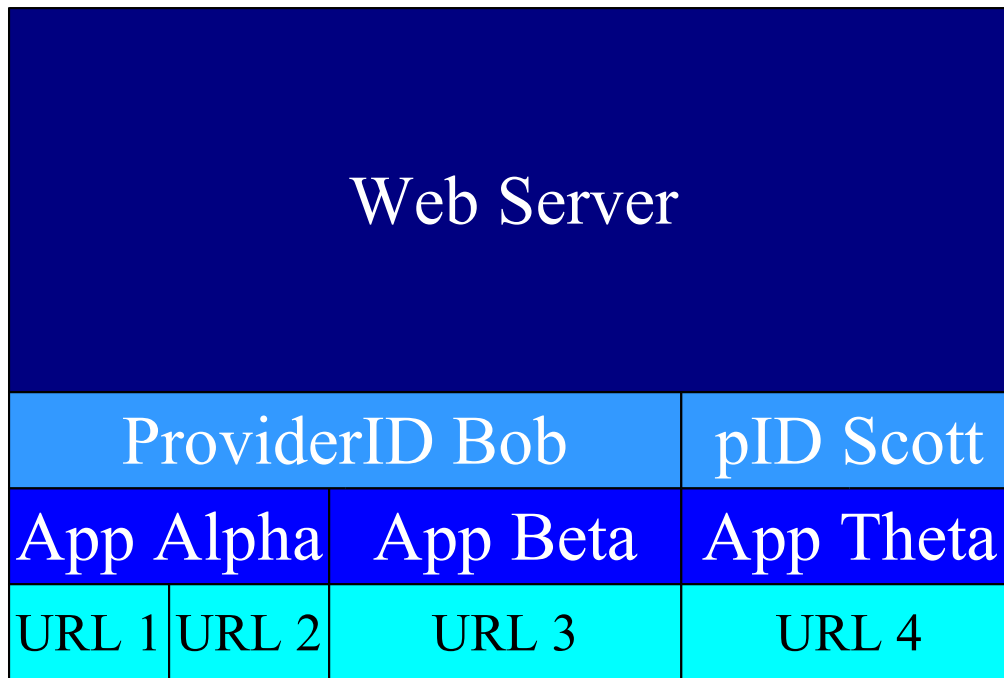
Production Deployment

- Efficiency
 - Load Testing Statistics
- High Availability
 - Failover
 - Load Balancing
- Security

Recycled Boxes



Service Provider Request Mapping



Webapps, pages, files, etc.
AAP's and access decisions
Lazy Session Initiation

Attribute Release, Policy Atom
Sessions, Most Settings

Externally Visible Resources

↑
Resource Requests

Configuration Files

- shibboleth.xml / sp.xml
- server.xml
- web.xml
- httpd.conf
- AAP.xml

The Many Flavors of “State”

- Authentication Assertion
- SSO Login
- WAYF Choice
- Attributes
- Shibboleth Session
- Application Session

Lazy Session Initiation

- Allows access of URL's before Shibboleth intervenes
- Construct special URL's to trigger attribute release & authn/z
 - URL to return
 - URL of the request handler
- `https://foo.com/Shibboleth.sso/SAML/POST?target=https%3A%2F%2Ffoo.com%2Fportal`

AAP's

- Map SAML attributes to usable values
- Header variables
- Vary by web server
- Utterly extensible
- aap.xml

Constructing SP Policy

- Restraining attribute acceptance & scope
- Apache directives / web.xml
- shibboleth.xml
- Export assertions/attributes for application-layer decision
- metadata.xml

Application Integration

- Handoffs & expirations
- Some applications will need to be modified
- Storing preferences
- Mind the @ (apologies to London)
- Examples: TWiki, Simple Portal
 - Many others in production

The WAYF and the Resource Registry

- Thomas Lenggenhager -- SWITCH

Examples!

Protocol Security

- Load balancing at SP is straightforward
 - ShibURLScheme
- checkAddress
- Assertion Confirmation
 - Bearer assertion
 - Holder of key
- SSL/TLS
- SAML = COOKIE

Attribute Use

- *Person
- persistentID
 - Generated vs. database
 - Auditing considerations
- eduPersonEntitlement
 - Is it a privilege?
 - Policy logic visibility
 - Is it a dynamic group?
- Identity
- Defining new attributes
 - Federation issue, or larger than that?

Scope

- Who can talk for whom?
- Who decides?
- What are they allowed to say?
- Metadata & SP Policy

Federation Operation

- Technical Needs
 - Hosted metadata.xml
 - Defined attributes?
 - WAYF?
- Policy Needs
- Granularity
- Federation Peering?

John Paschoud

- Moving from development to production support

What do you want to do?

- Q and hopefully A
- shibboleth-users@internet2.edu
- ndk@internet2.edu
-