

Shibboleth, PKI, and the Grid

Nate Klingenstein
ndk@internet2.edu

25 January 2007
APAN 23 Manila

The Current Situation

- Most institutions already maintain accounts for students, staff, faculty, etc.
 - Authentication
 - Useful attributes
 - Class membership
 - Affiliation
 - Primary Identifier
- We already audit, account, help, punish, etc.
- It's our job -- and we take it seriously

The Global Shibbolization

- Authenticate locally; act globally
 - Using your existing authentication & directory systems
- Shibboleth project started ~2001
- Shibboleth 1.3 current, but 2.0 is imminent
 - Free, open-source, very active support list
- Great vendor collaboration
- Federated identity now has millions of users worldwide
 - U.K., Switzerland, Australia, France, U.S., Finland, Denmark, Norway, Germany, Sweden, Netherlands, most major content providers, etc.

But... what is it, and how does it work?

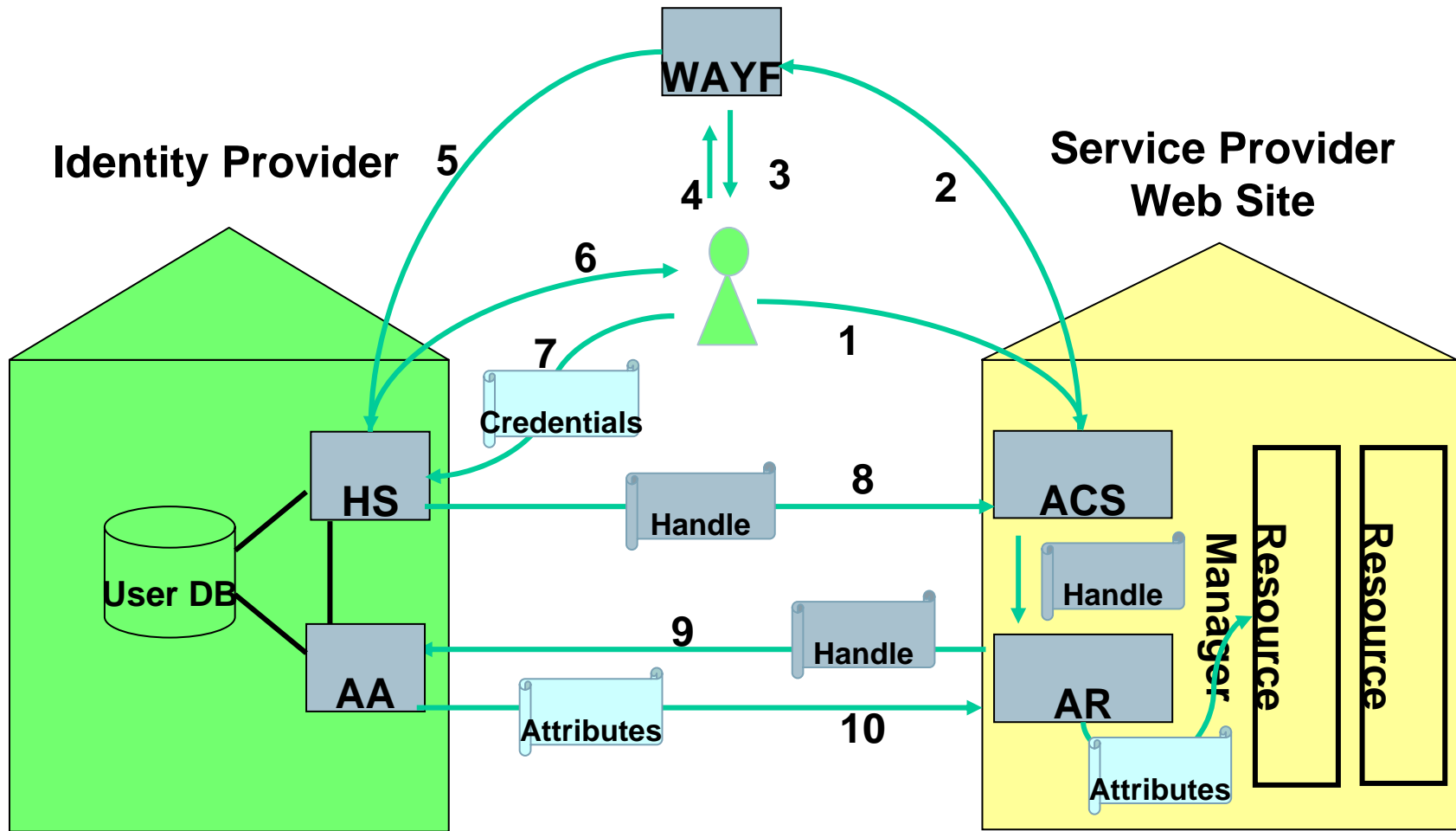
Federated Identity

Identity providers(IdP) assert attributes about users to service providers(SP), who then use the attributes to provide access.

A federation is a set of IdP's and SP's that agree to exchange attributes under common rules

- Limits account proliferation
- Encourages good identity management
- Single sign-on across organizations
- It's easy, it works, and it's free

The Architecture of Shibboleth



Why integrate Shibboleth with grids?

- Grids use x.509 certificates for authentication and authorization today;
- Why change?
 - Issuance
 - LoA mapping between grids
 - Trusted roots
 - Revocation
 - Portability
 - Keycards, etc.
 - Account management
 - Attributes & privileges
 - Users are lazy and make mistakes
- Most importantly: everything listed above becomes campus IT staff's problem -- and we thank you

So, Let's Federate

- Many researchers from many institutions work on one grid
- First conceived of by the GridShib project out of NCSA
 - <http://gridshib.globus.org>
- Later conceived of by lots of others
 - MAMS, SHEBANGS, ShibGrid, VOTES/GLASS, GridShibPermis, SLCS
- Each in a unique and interesting way...

The Fundamental Problems

- PKI credentials are embedded in many grid components
 - Shibboleth & co. speak SAML
- Divergent embedded base of grid middleware
 - Bootstrap?
 - Replace?
- Multiple possible interface points
 - For authN, authZ, and attributes
- How much security is *really* needed?
 - How much is too much?

**Blatant
Slide
Theft**

Common Ground

- End up with a proxy certificate
- Not much else...

- A grid that speaks SAML credentials natively
- Web services may be the unification of PKI & SAML access mechanisms
 - WS-Security(wsse:) bindings
- Combination of PKI and SAML for high LoA applications
 - Benefits of both
- Virtual Organization Management Toolkits
 - I AM Suite, MyVOCS
 - Soliciting new names: VOICE? NetVORK?



Any Questions?

Nate Klingenstein
ndk@internet2.edu