

A Shibboleth View of Federated Identity

Steven Carmody

Brown Univ./Internet2

March 6, 2007

Giornata AA - GARR

Agenda

- Assumptions and Trends
- Identity Management and Shibboleth
- Shibboleth 2.0 Update
- Grids and Shibboleth
- Collaboration Tools/Applications/Vendors
- Licensed Library Resources
- eduRoam

Assumptions about Audience...

- Somewhat familiar with the concept of Federated identity
- Somewhat familiar with SAML, Liberty, WS* (and PAPI and A-Select)
- Somewhat familiar with the concept of Federations

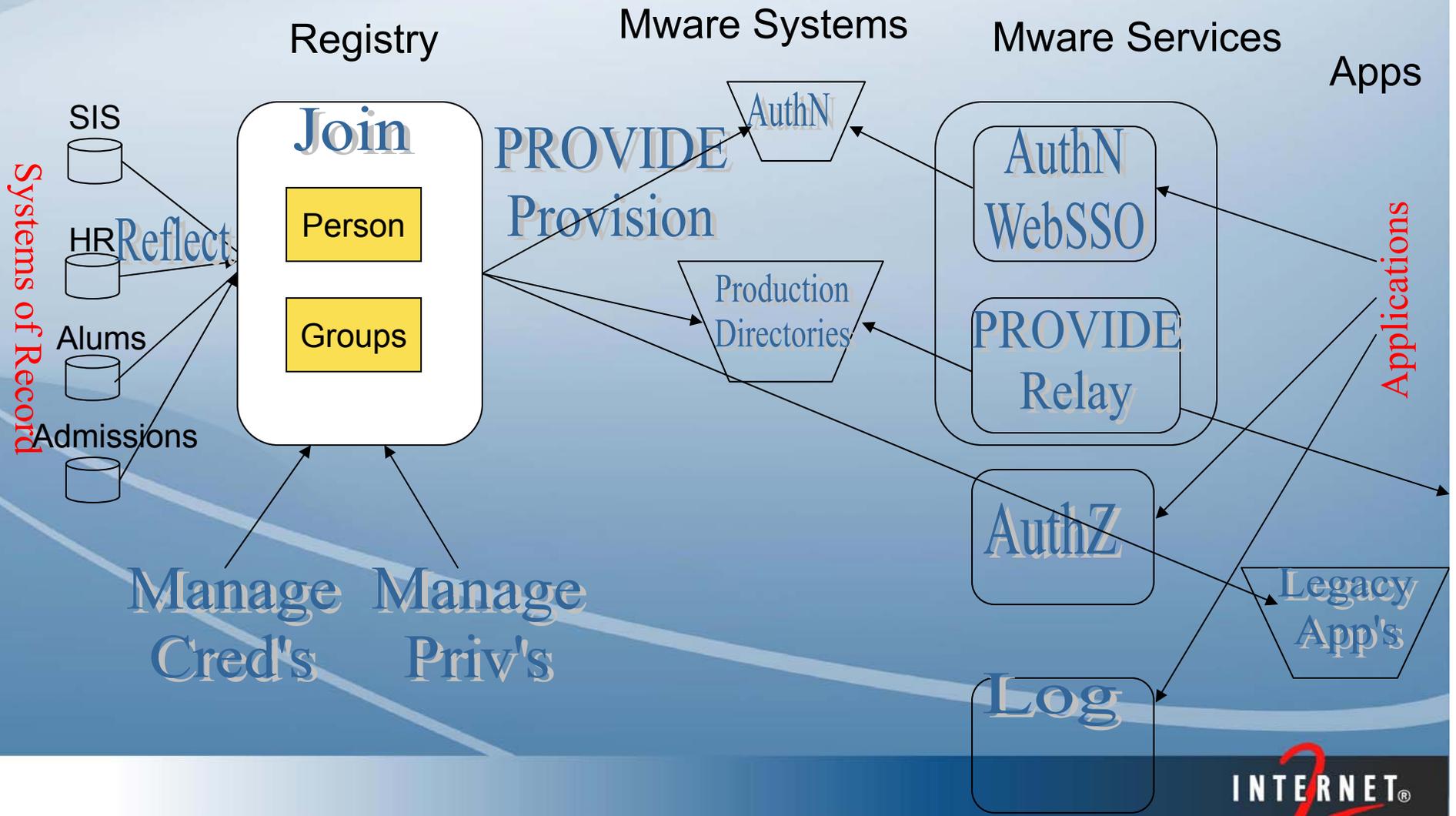
Trends in Identity Management

- Convergence of specifications
- Convergence of stakeholders in the identity space
- Higher Education/Research Federations moving toward production
- Federated Identity evolving from Web SSO to other applications
- Maturation of vendor products in the IdM space
- Increasingly, Federated IdM packages support multiple protocols; sites make choices based on “value add”
- Growing interest in using Levels of Assurance (LoA)
- Growing interest in Inter-Federation

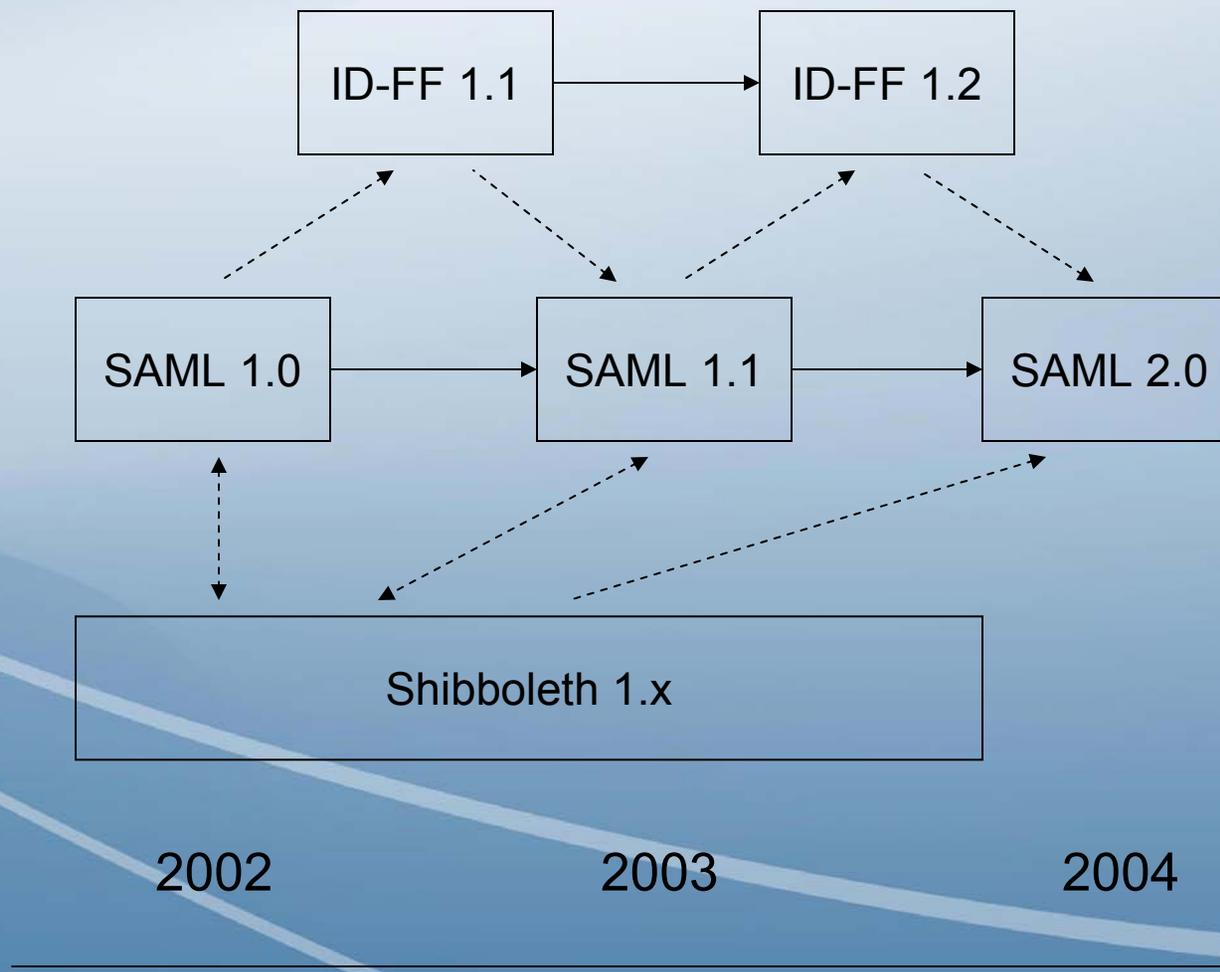
The I2/MACE IAM Model

Verb	Objects
<i>Reflect</i>	Data of interest from systems of record into registry, directory
<i>Join</i>	Identity information across systems
<i>Manage</i>	Credentials, group memberships, affiliations, privileges, services, policies
<i>Provide</i>	IAM info via <ul style="list-style-type: none">- run-time request/response- provisioning into App/Service stores
<i>Authenticate (AuthN)</i>	Claimed identities
<i>Authorize (AuthZ)</i>	Access or denial of access
<i>Log</i>	Usage for audit

I2/MACE -- The IaM Model



Shibboleth in the Standards Space



The (current) Shibboleth System is...

- an open source SAML-based Web SSO package
 - free to use and customize
- designed to SAML-enable applications.
- portable to a variety of platforms and web server environments.
- relies on pre-existing authentication and attribute sources.
- minimal rather than all-encompassing in its scope in order to make integration with existing environments and technology possible.

The (current) Shibboleth System is NOT...

- Usable in non-Browser scenarios (without a lot of hard thinking)
- an identity management system.
- a directory or database.
- a complete soup-to-nuts solution for authentication and attribute management.
- a world-class SSO system (largely because it's SAML 1.x-based at this stage).
- hard to deploy once you have a general template for how to proceed.

Key Concepts - Shibboleth in Your Environment

- Federated Administration
- Standards Based
- Attribute-Based Single Sign-On
- Management of Privacy
- Framework for a Variety of Policy and Management Models
- Extensible Authentication and Attribute Sharing

Shibboleth vs SAML

- Shibboleth v1.0 is a profile of SAML v1.1
 - Shibboleth Architecture document describes how Shibboleth uses SAML
 - Shibboleth extends SAML, defining a new NameIdentifier (the Handle)
- Shibboleth provides Value beyond SAML
 - The Shibboleth implementation includes a trust fabric implementation based on PKI
 - The Shibboleth implementation includes a framework and metadata for identifying IdPs and SPs
 - Current metadata format is from SAML v2
 - The Shibboleth implementation includes a mechanism (ARPs) to manage the release of attribute information to SPs
 - The Shibboleth SP implementation includes a mechanism for managing which sites are trusted to assert which attributes

Shibboleth as Web Single SignOn System

- Originally described as solution for cross-domain Single SignOn
 - Library Use Case
- Just as useful for intra-domain SSO
 - Provides single solution
- Shibboleth/SAML currently is not defined for use outside of Web SSO...

Shibboleth... the Next Generation

- Evolving to become a
 - Generalized standards-based security framework
 - Supporting multiple protocols
 - SAML v1.0, 1.1, 2.0
 - Microsoft ADFS
 - Liberty WFS
 - CardSpace
 - Providing added value across all protocol stacks
 - Usable in a variety of environments (web, client, n-tier, multi-protocol)

Significant Value-Add compared to Other SAML Implementations

- Management of Attribute Release
- Management of Attribute Acceptance
- *Real* support for the concept of Federations
- Better support for application integration (eg lazy sessions)

Shibboleth 2.0 Update

- Support for:
 - SAML v1.0, v1.1, v2.0
 - ADFS
 - Work underway on Liberty WSF
 - Experiments underway with CardSpace
- Support for the attribute ecosystem
- Trust management
- Java SP implementation

Shibboleth 2.0 -- Possible Follow-on Projects

- Attribute Aggregation at the SP
- Constrained Delegation
- New Approaches to the “Home Site Discovery Problem”
- Dynamic Metadata Acquisition

Grids and Shibboleth

- NSF supported GridShib package
 - TeraGrid is joining InCommon
 - Pilot starting soon
- EGEE work
- Privilege Management
 - Currently based on groups info into certs
 - Or using VOMS
 - Moving towards use of Signet/Grouper/Shib

Collaboration Tools/Applications/Vendors

- Evolution from...
 - Desktop applications -->
 - Web-based applications (intra-organization) -->
 - Web-based applications (inter-org -- “Virtual Organizations”)
- Applications include portals, wiki’s, etc
- Examples:
 - myVOCS
 - MAMS IAM Suite

Federated Internet2 Wiki

- <https://spaces.internet2.edu/homepage.action>
- Member of multiple Federations
- Accessible from single IdPs in other Federations
- Accessible from ProtectNetwork
 - <http://www.protectnetwork.com/>

Recent Events

- US Federal Federation (NSF, NIH grants management, student financial aid)
- Growing number state-based Federations
- Google -- Google Apps for Education
- Microsoft -- CardSpace

Shibboleth and Licensed Library Resources

Worldwide -- Federated SAML Adoption within Higher Education

- Australia
- Belgium
- Canada
- China
- Denmark
- Finland
- France
- Germany
- Greece
- New Zealand
- Norway
- Spain
- Spain
- Sweden
- Switzerland
- The Netherlands
- United Kingdom
- United States

Those Federations are Working Together to.....

- Learn to work together.....
- Prioritize which vendors to work with (to ask them to shibboleth-enable their product)
- Develop common definitions and uses for attributes
- Work through the home-site discovery problem
- Address inter-federation policy mapping issues
- Bring brainpower to bear on difficult problems

Evolution of Common Attribute Definitions

- Initially, for use with Information vendors
 - Addressing several different use cases
 - urn:mace:dir:entitlement:common-lib-terms
- Recently expanded to include other types of vendors

The Europeans Prioritized Vendor List

- Elsevier Science Direct
- EBSCO
- Thomson Scientific, ISI
- JSTOR
- Springer
- OVID (OvidWeb and WebSPIRS)
- Wiley
- Blackwell Publishing
- CSA
- Exlibris- Metalib
- EZProxy
- OUP Oxford University Press
- Proquest
- Taylor and Francis -- UK
- Thomson Learning (UK-LSE)
- Muse
- Nature
- Institute of Physics Publishing
- American Chemical Society
- Exlibris-SFX
- American Psychological Association

Other Vendors...

- TurnItIn
- Music (Napster, CDigix)
- MSDN Academic Alliance
 - <http://msdn.microsoft.com/academic/>
- American Education Services
 - <http://www.aessuccess.org/>
- The US Federal Government E-Authentication Initiative
 - <http://www.cio.gov/eauthentication/>

eduRoam

- Current eduroam has home site doing access control
 - Visited site does NOT have access to roaming user's identity or attributes
- Two proposals being pursued
 - DAME transporting SAML via DIAMETER
 - I2 using Radius, transporting SAML outside of Radius exchange

www.internet2.edu

INTERNET[®]
2