Introduction to Federated Identity

Nate Klingenstein
Internet2
ndk@internet2.edu

国立情報学研究所

２００７年６月１日

Today's Topics

- The basics of identity management
- Introduction to federated identity around the world
- Relationship to PKI and other systems
- How to connect an IdP and SP to your applications
- Introduction to installing Shibboleth

Why manage identities yourself?

- Campus people need to be involved
  - Human resources (HR)
  - Student information (SIS)
  - Departments
  - Application developers & maintainers
- Providers of software and services need to be involved
- Without good identity management, research is hard to do

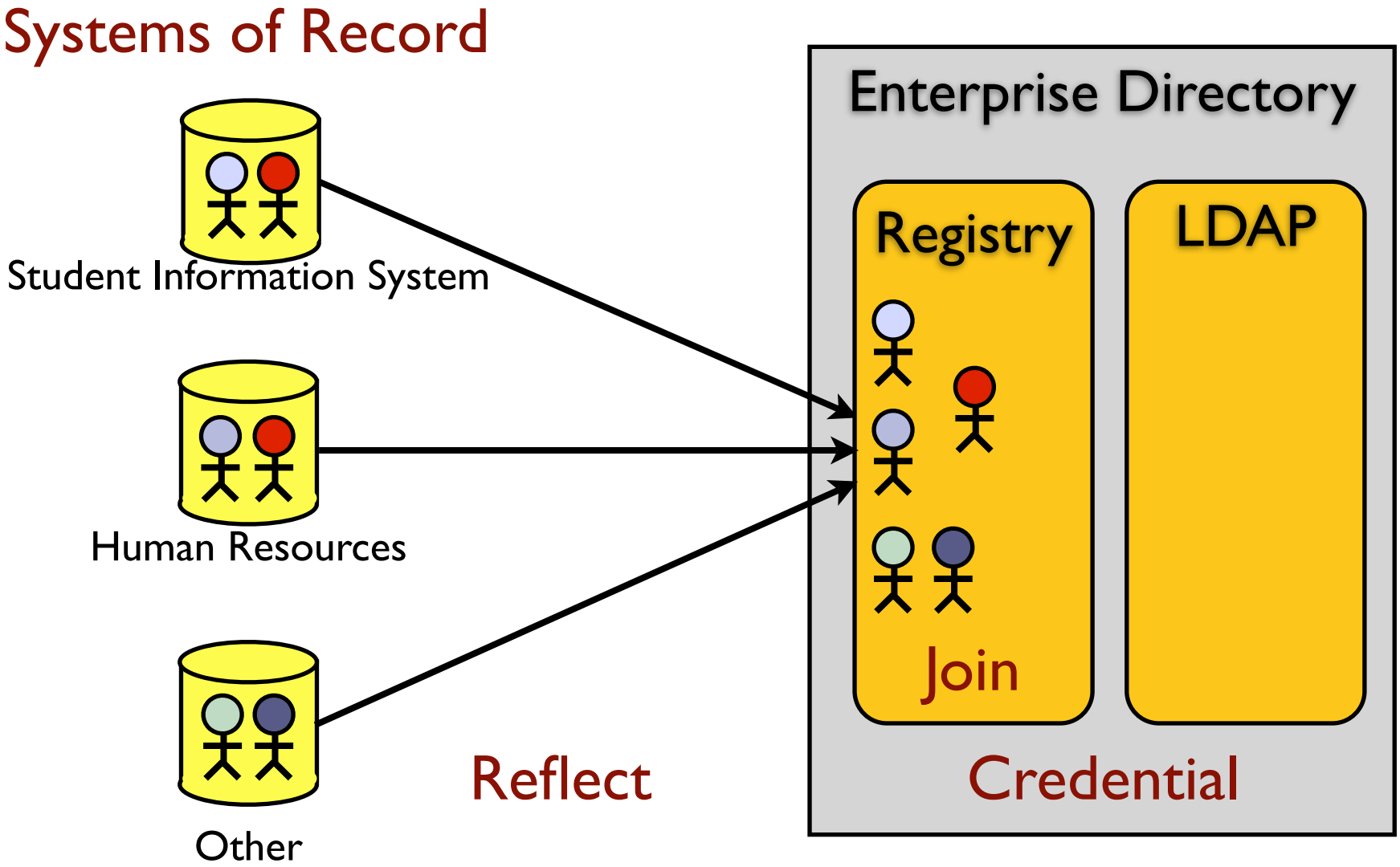
The Ultimate Identity Management Goal

- Deliver the identity information that an application needs
  - Sometimes authentication
  - Sometimes attributes
  - Sometimes authorization
- Securely
- Simply

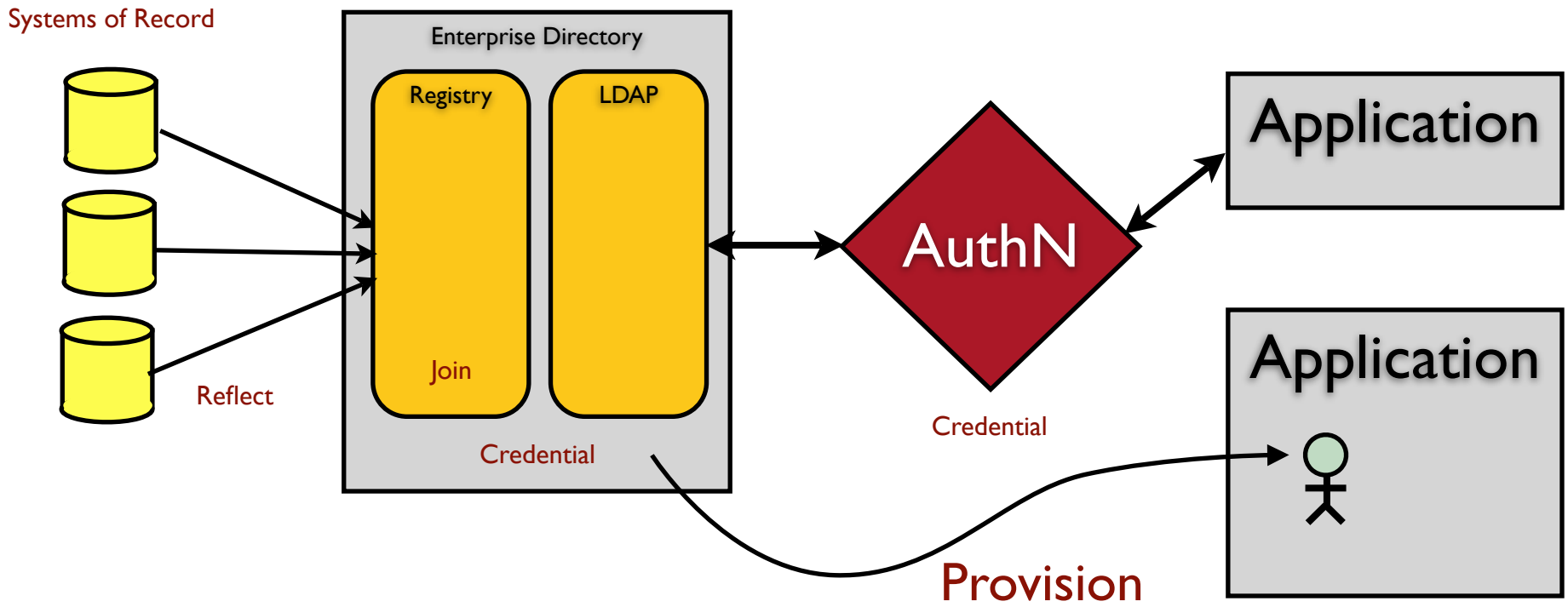
Good data starts at home

- Registration processes
- Creating accounts, entering names and addresses, managing person data
  - Figuring out who is responsible for what
- Authentication
- Deleting accounts & identities

Basic IAM Functions

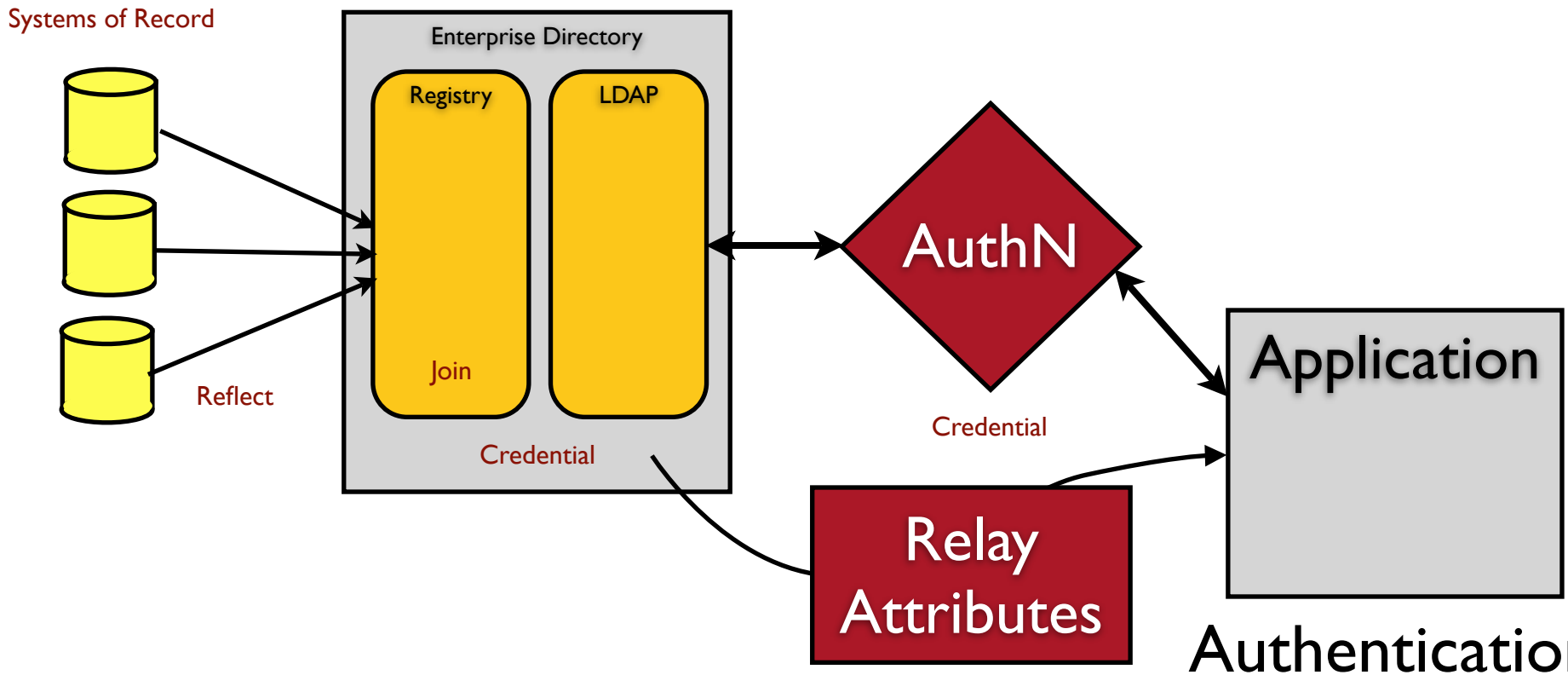


Basic IAM Functions



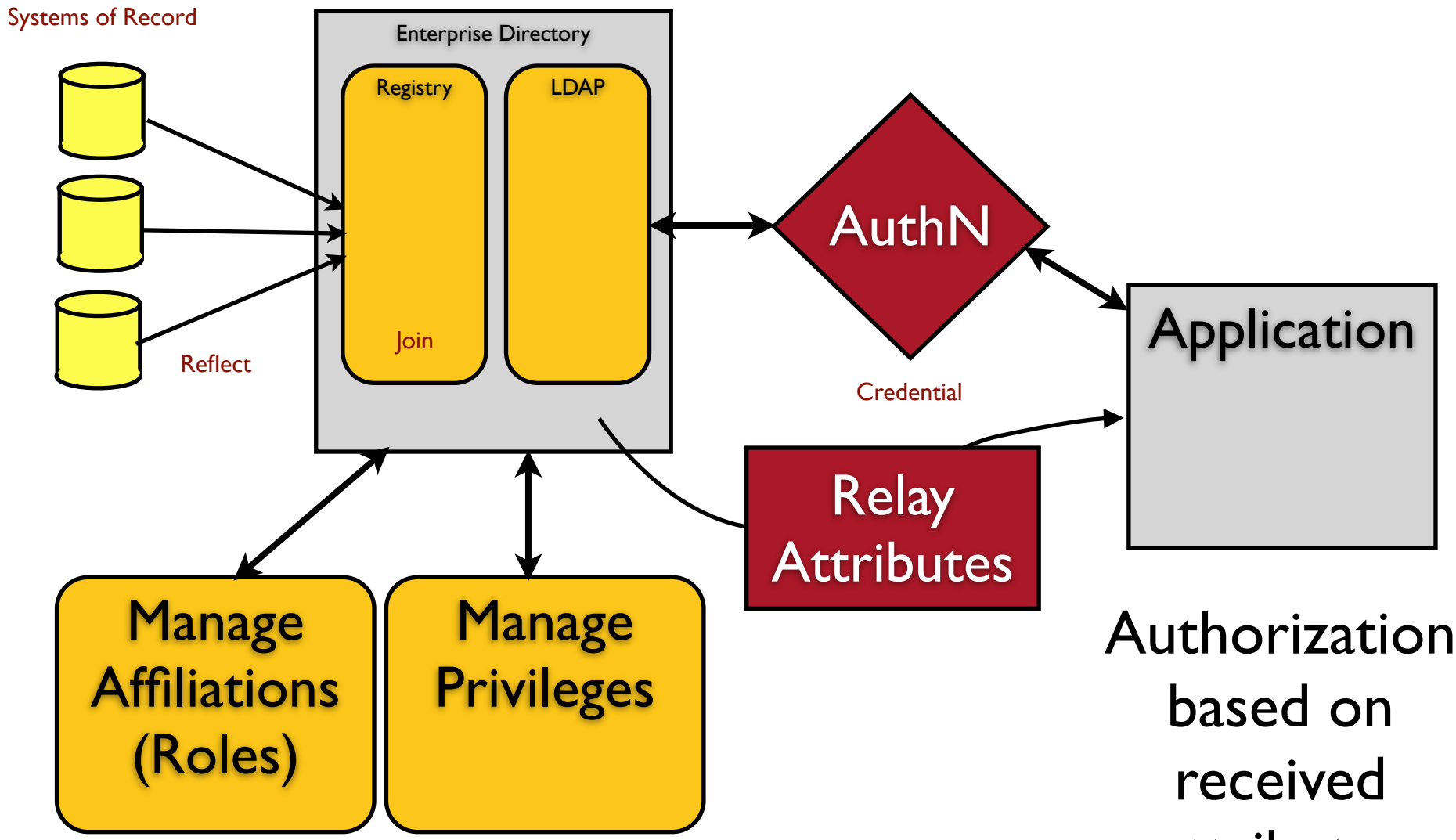
AuthN/Z based on local account

Basic IAM Functions



Authentication and authorization using relayed attributes

Basic IAM Functions



Good data goes around the world too

- Lots of educational applications and services are now located outside the university
  - Classes at other universities
  - Research groups
  - Content providers/scientific journals
  - Web-based applications like wiki's

Extending Campus Identity

- These outside organizations want to provide services for campus members
- They require information about people, but the campus is the authority for this information
- The ultimate goal is still the same
  - Get the data to the applications securely and simply

Federated Identity

- In many ways, it's not a new idea
  - Still doing the same things
- However, the application and the identity source can be in different organizations
- This means you have less control
- And things can't be as tightly connected

Existing technologies are not perfect

- IP Address authentication
  - Requires people be on campus or use a reverse proxy
  - Monitoring access is difficult
  - Not very secure
- PKI, direct username/password, etc.
  - External organization must be able to log on your users
  - Trust, revocation, password reading, more
  - No attributes

Existing technologies are not perfect

- Additional accounts
  - Yet another username/password to remember
  - Doesn’t solve the problem of getting trusted campus data when needed
- Possession of email address
  - *@*.ac.jp
- And more

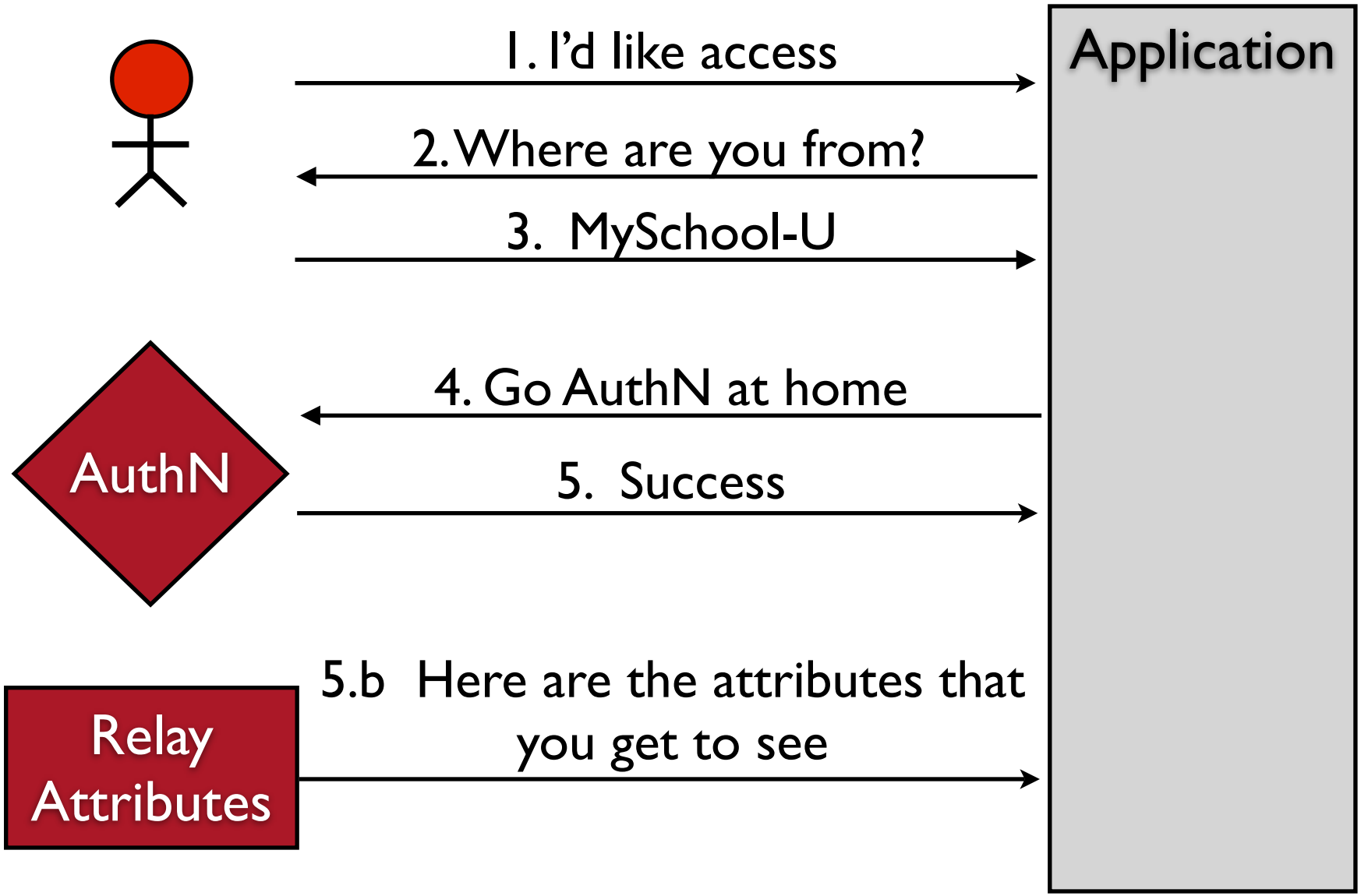
Federated Identity

- "Asserts" an identity in one domain to access services
  - In the same or a different domain
- Trust between the service provider and the identity provider is used
  - Usually done "out of band" by talking
  - Sometimes with a federation's help

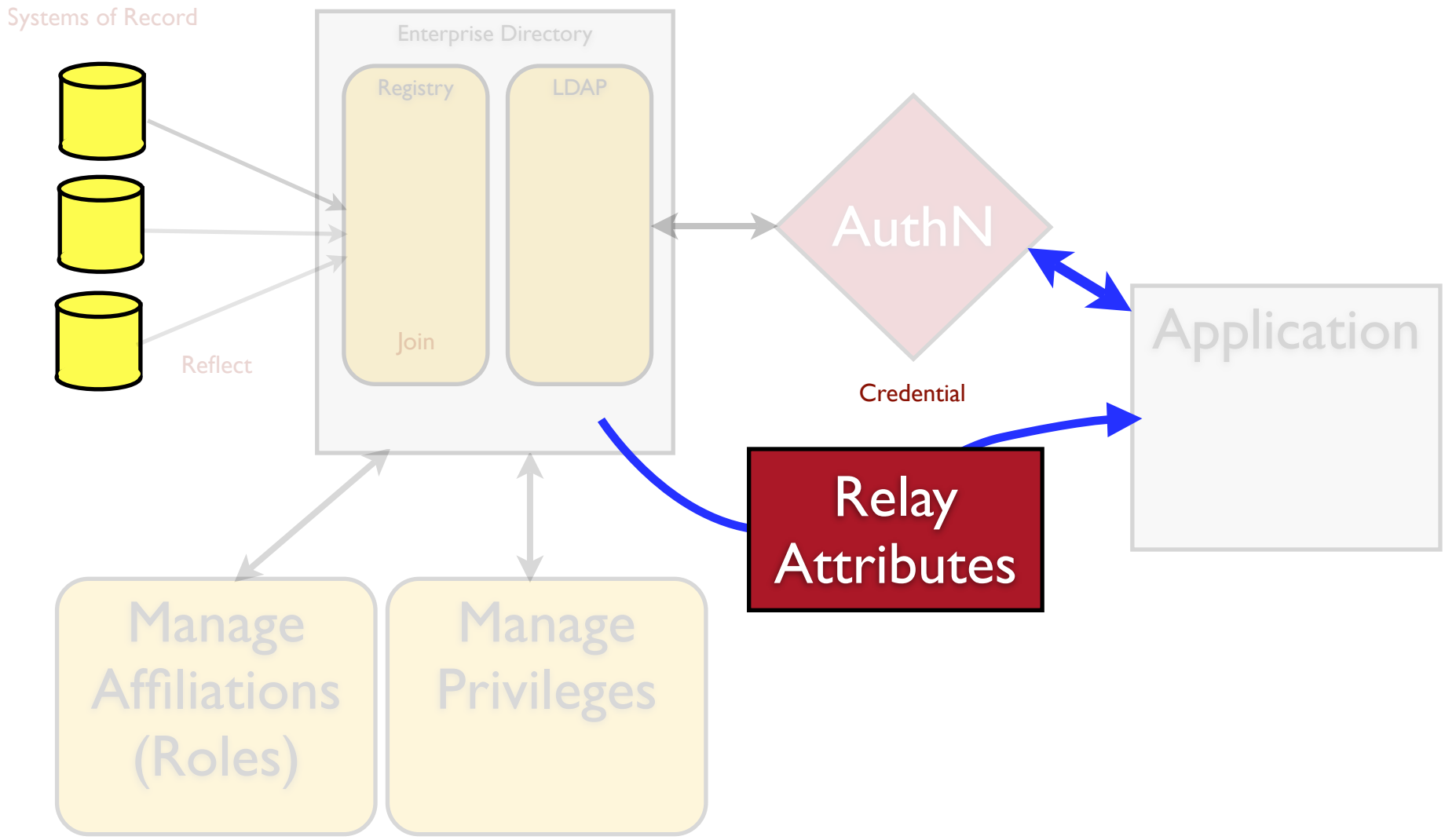
Federated Identity

- Lots of choices
  - Everyone can use any authentication they want
  - Everyone can put attributes anywhere they want
  - Everyone can trust who they want to trust
  - Everyone can use any SAML-based IdP or SP software they want

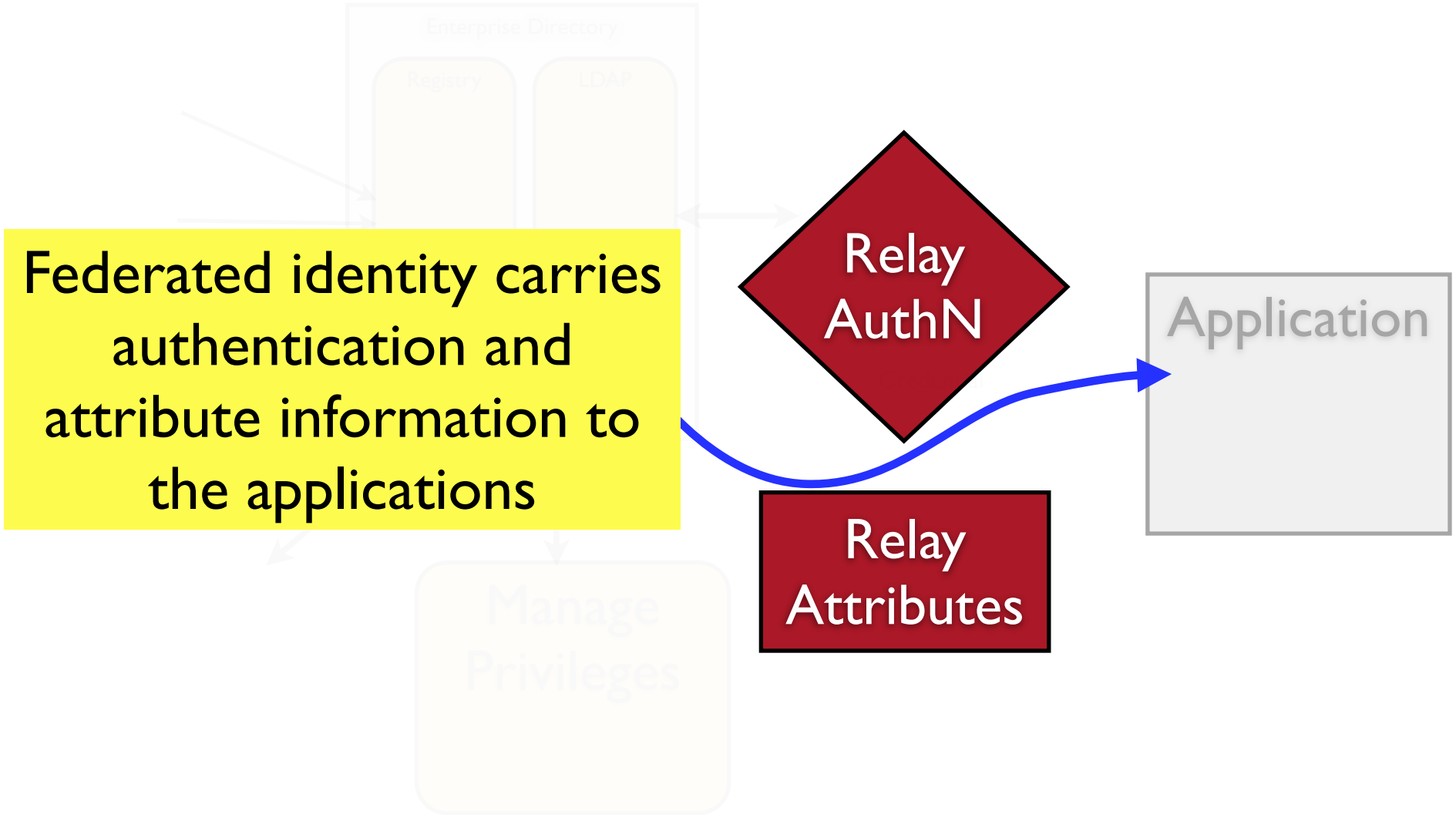
Simplified federated ID



Where does federated identity fit?



Where does federated identity fit?



IdP Discovery

- How do we determine which campus a user is from?
- A very hard problem with lots of possible answers
- I'll demonstrate two common ways
  - Buttons at the application
  - The "Where are you From?" WAYF Server

Let’s try it out!

http://www.switch.ch/aai/demo/

https://kohala.switch.ch/secure/

https://www.testshib.org/

Some important words

- Identity Provider (IdP)

  A system that sends information about authenticated users to Service Providers

- Service Provider (SP)

  A system that receives and processes information about users from IdP's. It protects resources and decides to grant access based on this information.

More important words

- Assertion

  A statement created by an IdP about a user's authentication or attributes.

- Request

  A request from an SP for an IdP to perform an action to create an assertion.

- Query

  A request from an SP to an IdP for information that already exists

Shibboleth

- Shibboleth Profile extends SAML 1.1 to add authentication request, handle
  - Contributed to SAML 2.0 specifications
- Shibboleth software is free, open-source implementation of SAML
  - 1.1 in Shibboleth 1.x
  - 2.0 in Shibboleth 2.0

Trust

- Federated identity relies on trust between providers & organizations
- The SP trusts the IdP to send true information about users
- The IdP trusts the SP to use attributes well
- Trust can get more complicated than this

Federations

- An organization that helps IdP's and SP's trust each other
  - It does a few other important things too
- IdP's and SP's in the same federation can work together easily
  - Federations are starting to connect to each other too
- Fix "handshake" problem

Federations around the world

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

Major Content Providers that use Shibboleth

- EBSCO
- JSTOR
- OCLC
- Elsevier ScienceDirect
- Thomson Gale
- Many, many more

InCommon

- U.S. higher education federation
- Over 50 universities and partners
- Most major content providers

- Many states have their own independent federations, e.g. Texas

Status of Haka Federation (Finland)

- **Operational 8/2005**
- **23 (of 48) Federation Members**
  - with 213 000 end users (68% of eduPersons; in universities 90%)
- **3 Federation partners**
  - Library content providers, ASP service providers
- **13 IdPs operational**
  - with 159 000 end users (51% of eduPersons)
- **20 SPs**
- **168 400 logins in March 2007**
- **federating sw: Shibboleth ver 1.3**
  - 2 IdPs still running Shibboleth 1.2

SPs in the Haka federation

Library services

- **Nelli portal (Ex libris Metalib)**
- **Library management system (Endeavor Voyager)**

eLearning

- **Moodle, A&O, Optima learning management systems**

CSC's services

- **Funet extranet**
- **Scientist's Interface**

Student administration

- **Application form for becoming a visiting student www.joopas.fi**

HR administration

- **Competence management system/ASP (Personec hr)**

Other administration

- **Process database for universities**

WLAN roaming (Jyväskylä polytech)

UK Federation

- 68 members with many more soon
  - Official Shibboleth/SAML-based federation for all of UK education, including K-12
- Replaces Athens, a centralized nationwide authentication solution
- Athens will remain as a legacy service, but cost money, while Shibboleth is free

Norway's FEIDE

- A lot like Athens, but with SAML 2.0
  - One Sun Access Manager IdP feeds off many LDAP directories
    - Hard road, but working well now
  - Passwords are given to the central server, which then LDAP BIND's to campuses
- Denmark considering a "hybrid" model that has both kinds of IdP

Federations vs. Federated Identity

- A federation is not necessary to use federated identity
- A single IdP or SP may join many federations
- IdP's and SP's in a federation can make further agreements together

Campus Federations

- There is no technical difference between a federation of many schools and a federation on campus
  - Trust may be more close
- A campus may have only one IdP
  - Or in bad cases... several

Federating Technologies

- SAML 1.1
  - Shibboleth 1.x Profile
- SAML 2.0
- Liberty Alliance ID-WSF
- WS-Trust, WS-Federation, WS-*
- OpenID
- Cardspace

SAML 1.1

- Defines standard assertion and query formats
  - Attribute assertions
  - Authentication assertions
  - Attribute Query
- Defines protocols for carrying them

Shibboleth 1.x

- Builds on SAML 1.1
- Adds an authentication request
  - “Please authenticate this user and send them back to me.”
- Makes use of a “handle” as a temporary user reference
  - String for the following attribute query

SAML 2.0

- Designed using SAML 1.1, Shibboleth, and Liberty ID-FF 1.1 as inputs
- The major enterprise federation standard
- Assertions, requests, and queries

Some SAML 2.0 Vendor Implementations

- Oracle
- Sun
- IBM
- CA/Netegrity
- RSA
- Novell
- Google
- Symlabs
- Entrust
- PingIdentity
- Trustgenix
- Juniper

SAML 2.0

- Protocol bindings place assertions and questions in messages for transport
  - SOAP
  - HTTP
  - Others are possible

SAML 2.0

- Profiles standardize ways to accomplish common goals using the assertions, queries, and bindings
  - Web SSO Profile is the most commonly used
- Almost every major vendor has implemented SAML 2.0 support
  - But in different ways
  - Interoperability, with work

Cardspace

- Built into Windows Vista
- User interface for selecting identity information to access sites
- Cards represent an identity at an IdP
- Microsoft is funding Shibboleth/ Cardspace integration
- http://www.identityblog.com/?p=779

Liberty Alliance ID-WSF 2.0

- Defines formal SOAP web services for identity transactions
  - Getting a new identity token
  - Transforming existing identity tokens
- Uses SAML as a token format
- Enables delegation & more
- Not used as much as SAML

WS-Security

- Places security tokens in SOAP header
- Bindings for SAML, X.509, Username/ Password, Kerberos
- Works well with other standards
- Significant uptake within web services world

WS-Trust

- A container for identity tokens of many sorts
  - SAML, PKI, Kerberos, etc.
- Provides for transformation of these tokens from one type to another
- “Another layer of generalization”
  - Increases wire interoperability

WS-Federation

- Controversial specification developed by IBM and Microsoft. OASIS has a working group for it, but there are many complaints
  - Depends on unreleased specifications
  - Many parts overlap heavily with SAML

Other WS-*

- WS-SecureConversation
  - Like TLS/SSL, but for SOAP
- WS-SecurityPolicy
  - Allows a SOAP endpoint to describe what it wants to receive
- There are more, some standard, some not

OpenID

- Came from the world of blogs
  - How can I log into your blog using my blogging identity when there are many blog sites in the world?
- Allows a user to prove they are the owner of a URL
  - This URL is their identity
- No XML means simpler installation
  - HTTP Headers

OpenID

- No trust relationship between providers
- Users are responsible for deciding whether to trust a URL as a valid identity
  - URL's are often exchanged through trusted communication. "Yasuo emailed me this URL, and I know it's Yasuo because we have talked for years."

OpenID

- Can assert authentication
- Cannot assert authorization or attributes
  - But, some are trying to add attribute support
- Doesn’t cover all institutional needs
  - Very popular outside, though
  - Use campus login for some OpenID sites?