Federated Identity, PKI, and the Grid

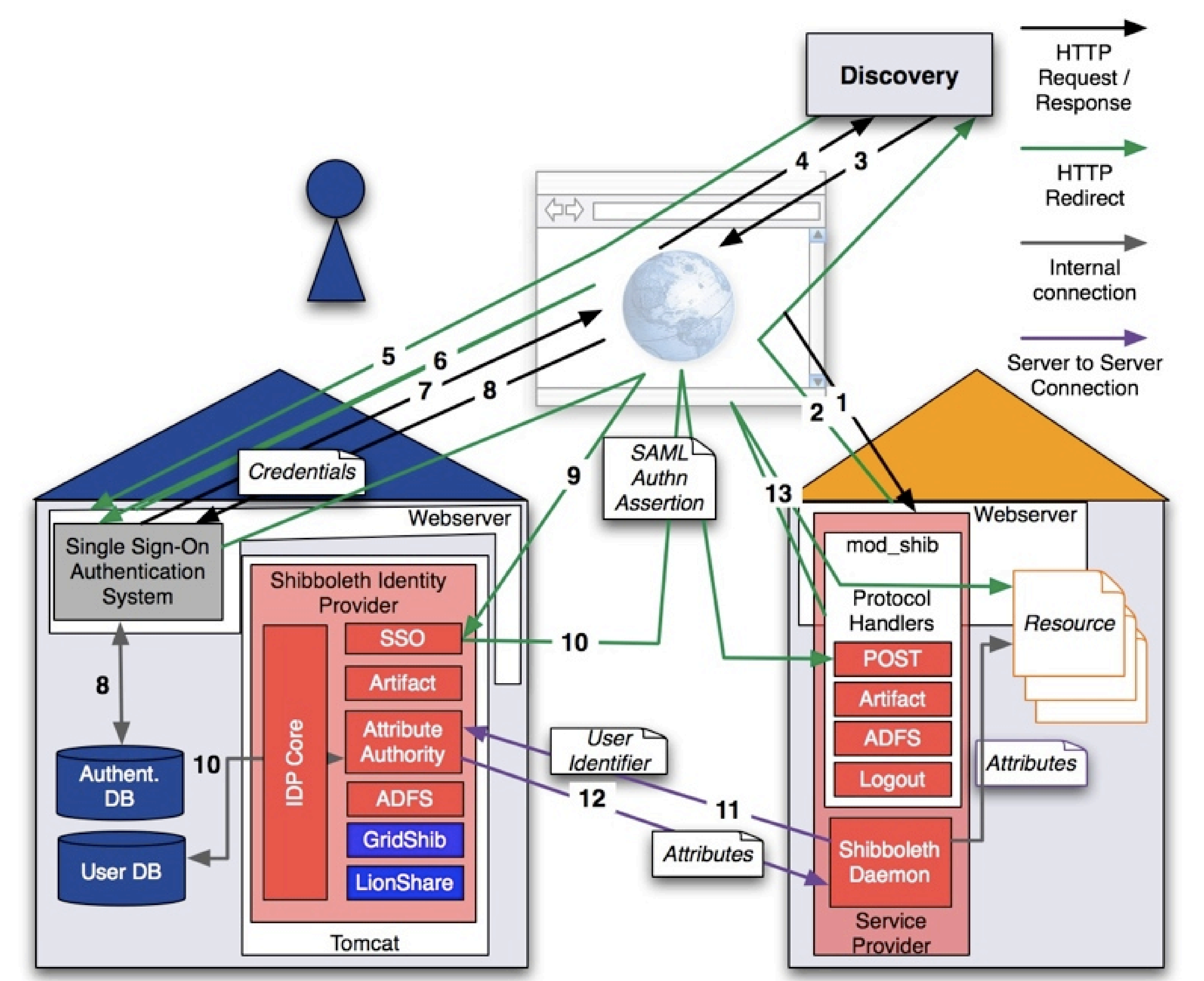
Nate Klingenstein
Internet2
ndk@internet2.edu

国立情報学研究所

２００７年６月１日

Federated Identity Review

- Takes identity from one authentication domain and “extends” it to access another
- Providers trust each other and rely on information from each other to authenticate users and grant access
- How does this trust work?


Discovery
HTTP Request / Response
HTTP Redirect
Internal connection
Server to Server Connection
1
2
3
4
5
6
7
8
9
10
11
12
13
Credentials
SAML Authn Assertion
Webserver
Single Sign-On Authentication System
Shibboleth Identity Provider
SSO
Artifact
Attribute Authority
ADFS
GridShib
LionShare
IDP Core
8
Authent. DB
User DB
10
Tomcat
User Identifier
Attributes
Webserver
mod_shib
Protocol Handlers
POST
Artifact
ADFS
Logout
Resource
Attributes
Shibboleth Daemon
Service Provider

Server Authentication in Federated Identity

- IdP’s and SP’s need to be able to authenticate each other
- “Metadata” is used to describe providers
  - Your provider’s metadata is for your partners to use
- Metadata associates providers with endpoints and keys or certificates
- Your provider presents its matching key to prove its identity

Server Authentication in Federated Identity

- Assertions, attributes, name identifiers, and more can be encrypted in SAML 2.0
- All messages protected by TLS/SSL
- Public Key Cryptography is critical for federated identity

Bearer Assertions

- Federated Identity uses “bearer” tokens in web browsers
    - If I have an assertion, it’s true about me
    - Makes delegation hard
    - Means there’s no way for an SP to authenticate a user directly
- Broken in a good way for most apps

Bearer Token Security

- Lots of safeguards are possible to prevent assertions from being stolen or misused
    - Very short time limits
    - Replay detection
    - Sometimes, IP address and other checks
    - Assertions are addressed to specific SP’s

Making bearer tokens more secure

- Some applications require greater security
  - Need to authenticate the user themselves to be really sure it’s the right person
- PKI is good for this, but it is tough to use for many people
  - Just ask 秋山さん

Three ways to combine PKI and SAML

- Use PKI to authenticate to an IdP
- Use PKI as confirmation when presenting a SAML assertion
- Put a SAML assertion or its information in an x.509 certificate

PKI/SAML Combination #1

- Use PKI to authenticate to the IdP
  - Means SP's don't have to understand PKI, your CA, or handle revocation
  - Still get extremely high-quality authentication
  - Easy to do this today with Shibboleth
- But what about security as the information goes to the SP?

PKI/SAML Combination #2

- SAML assertions can be “holder of key” assertions too
- When an assertion is presented, the client must also have the right private key
- Only a few deployments do this
  - In narrow applications

PKI/SAML Combination #3

- Place SAML information within an x.509 certificate
  - Backward compatibility is the only reason
    - But that’s a pretty good reason
- Do you try to populate lots of x.509 fields dynamically from SAML?
  - Or just attach the SAML in an extension?

Advantages to Combining PKI and Federated ID

- Fresh information
- Privacy preserved still
- Revocation is no problem
- PKI can do things federated identity can’t do alone, like signing & encryption

Advantages to Combining PKI and Federated ID

- Much more flexibility in issuance of user certificates
- User certificates help solve IdP discovery
- Still have to give keys to users though...

Federated Identity & the Grid

- Since researchers accessing the Grid usually come from a campus
- And the campus already manages these users' identities...
- Why not use federated identity to bring campus identities to the grid?

GridShib

- Project out of NCSA since ’04
- Attaches Shibboleth identities to GT4
- Places a special DN in a MyProxy certificate
- Queries for attributes using this DN

SLCS and EGEE, ShibGrid, DyVOSE, etc.

- Lots of other projects to attach Shibboleth to other Grid middleware
- Uses a similar strategy as GridShib
- Some integrate with VOMS and more
  - SLCS from EGEE is thinking hard about this
- All still use x.509 certificates
  - Backward compatibility is needed

OGSA

- New “express security” profile in drafts
- Profiles the use of WS-Security for OGSA
  - WS-Addressing
  - WS-Security SAML profile
  - WS-Security Username Token Profile
  - WS-Security x.509 Profile