



UNIVERSITÀ
DEGLI STUDI
DI PADOVA

EUMEDCONNECT2 AAI information day

Rome, 9 November 2010

Stefano Zanmarchi

Università di Padova

stefano.zanmarchi@unipd.it



Agenda

- **I Federations**

11.00 – 11.30 Coffe Break

- **II Digital Identity Management**

13.00 – 14.00 Lunch Break

- **III AAI and Shibboleth**

15.30 – 16.00 Coffe Break

- **IV Trust within the Federation**



- **I Federations**

- II Digital Identity Management

- III AAI and Shibboleth

- IV Trust within the Federation



Introduction

- This information day was organized in collaboration with the IDEM Federation.
- What is IDEM?
The *Access Management Federation* of Italian universities and research institutions.
GARR coordinates IDEM and supplies technical and administrative support for the management of the *Authentication and Authorization Infrastructure* based on the SAML standard
- We'll get back to all these concepts later

- The main aim of IDEM is to create and support a common framework to facilitate trusted web access of users (researchers, teachers and students) of the participating institutions (universities and research institutions) to resources (e.g. journals, instruments, data).
- As of october 2010 (www.idem.garr.it)
 - 22 participating members
 - 31 resources

Participating Members

CASPUR
CILEA
Consiglio Nazionale delle Ricerche
GARR
ISTAT
Politecnico di Milano
Università "Ca' Foscari" Venezia
Università degli Studi di Bari "Aldo Moro"
Università degli Studi di Cagliari
Università degli Studi di Ferrara
Università degli Studi di Milano-Bicocca
Università degli Studi di Modena e Reggio Emilia
Università degli Studi di Padova
Università degli Studi di Parma
Università degli Studi di Pavia
Università degli Studi di Torino
Università degli Studi di Trento
Università degli Studi di Urbino "Carlo Bo"
Università degli Studi "Roma Tre"
Università di Bologna
Università IUAV di Venezia
Università Politecnica delle Marche

Resources

AAI WIKI
CILEA Digital Library
Emeroteca Virtuale
GARR VCONF
Moodle-Shib
Nilde Utenti
Pathology Atlases
ScienceDirect
Scopus
SP di Prova
SpringerLink
TERENA Certificate Service (TCS)
TERENA Certificate Service (TCS)
WiFi CASPUR
WiFi UniFE (Wi-Fe)
WiFi UniTO
WiFi@ToCNR
YouBlog
ALMA ARC
Botta e Risposta
IDEM (intranet)
IDEM AUTH JOOMLA
IEEE Xplore
Spaces (wiki)
Web Of Knowledge
WiFi CNR Pisa

IDEM Governance

- Member Board
 - composed by representatives of all participating institutions
- Policy Committee
 - performs organizational tasks
 - 8 members elected by the Member Board
 - 1 member designated by GARR
- Technical and Scientific Committee
 - performs technical tasks
 - 12 members elected by the Policy Committee
 - 1 member designated by GARR

- Focused on higher education in Switzerland
- Coordinated by SWITCH – The Swiss Education and Research Network
- The federation covers all Swiss universities as well as some universities of applied sciences
- 300000 users (>96% of all persons in Swiss higher education)
- 9.2 M logins/year

- Operated by Internet2
- A community of more than 4.5 million end users.
(Source: Higher Education Students, Faculty, and Staff, Integrated Postsecondary Education Data System. Calculated April 2010.)
- 255 current participants
 - Higher Education Participants (182)
 - Government and Nonprofit Laboratories, Research Centers, and Agencies (7)
 - Sponsored Partners (66)

National Federations in the world

Survey (2010) by REFEDs
<https://refeds.terena.org>

1. .at ACOnet-AAI
2. .au AAF
3. .br CAFe
4. .ca CAF
5. .ch SWITCHaai
6. .cz eduID
7. .de DFN-AAI
8. .dk WAYF
9. .es SIR
10. .fi Haka
11. .fr Fédération Éducation-Recherche
12. .gr GRNET
13. .hr AAI@EduHr

14. .hu eduID
15. .ie Edugate
16. .it IDEM
17. .jp GakuNin
18. .lv LAIFE
19. .nl SURFnet
20. .no FEIDE
21. .nz Tuakiri
22. .pt RCTSaaI
23. .se SWAMID
24. .si ArnesAAI
25. .uk UK Access Management
Federation for Education and
Research
26. .us InCommon



Federation Costs

REFEDs Survey (2010) shows:

- **Manpower:**
 - from best effort (0.5 FTE) to ~ 6-7 FTE
- **Budget not disclosed, apart from:**
 - Haka (.fi): ~300 K€/year
 - Tuakiri (.nz): ~860 K€/year
 - UK Access Management Federation: ~1,37M€/year
- **Incomes:**
 - Usually part of the NREN budget
 - Some federations apply membership fee



Inter-federation interoperability

Three distinct methods for facilitating interoperability between federations:

- Confederations: federation of federations, highly hierarchical control
- Peering: bi-/multi-lateral agreements
- Virtual Organizations (VOs): not under single hierarchical control



Confederations

- Sets of cooperating federations, or “federated federations”, governed by an overarching organisation, with member federations administered locally.



Peering

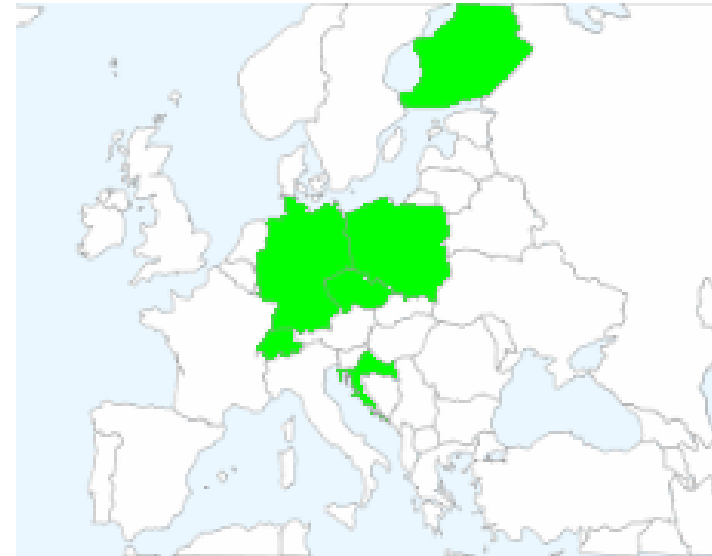
- Two (or more) federations establishing inter-federation trust links, with a trust model which relies on federations independently entering into bi-/multi-lateral agreements



Virtual Organizations

- Groups of associations of users, from one or more federations, not under single hierarchical control, joining forces to achieve a common goal, bringing to the collaboration a subset of their resources, sharing those at their discretion and each under their own conditions.

- Project by GÉANT
- Based on SAML
- It's not a Federation, it's a service to connect Federations
- www.edugain.org



- Pre-pilot phase:
Croatia, Czech Republic, Finland, Germany, Poland and Switzerland


- Cross-Nordic authentication system for higher education and research. Students and staff members in a Nordic university or research institution can use a single username and password to access services in other Nordic countries
- Finland, Norway, Denmark, Sweden, Iceland
- Based on SAML 2.0 technology (SimpleSAMLphp and Shibboleth)
- Kalmar 2, because the 1st Kalmar Union lasted from 1397 to 1524 (economical, political and military cooperation)
- <http://www.kalmar2.org>





The Australian/New Zealand co-federation

- No operational New Zealand Access Federation yet
- Three NZ Institutions have joined the Australian Access Federation (AAF) as best endeavours members:
 - The University of Auckland
 - The University of Canterbury
 - Lincoln University
- Ongoing NZFed Project aims:
 - Establish the NZ Access Federation
 - Link the NZ Access Federation to AAF
- <https://nzfed.auckland.ac.nz>

- 
-
- I Federations
 - **II Digital Identity Management**
 - III AAI and Shibboleth
 - IV Trust within the Federation

Identity Management is important



"On the Internet, nobody knows you're a dog."

©The New Yorker Collection 1993 Peter Steiner
From cartoonbank.com. All rights reserved.

Peter Steiner,
The New Yorker,
5 July 1993



Basic concepts: authentication

- **Authentication:**
the process of verifying the authenticity of the claim about the user's identity:
verification that the user is who he claims to be.
- Identity can be proven by
 - something you know (a password)
 - something you have (smart cards, USB tokens, or pk certificates)
 - something you are, represented by positive photo identification, fingerprints, biometrics, or other techniques

Basic concepts: authorization

■ Authorization:

the process of verifying whether a user has the right to access protected resources.

■ Typically digital systems perform authorization checks based on user identity information:

- “who” he is

- some of his “attributes”:

- Role (professor, student, alumnus)

- University tuition fees paid (yes|no)

“who” is defined by a set of “identifying” attributes



Authentication vs. Authorization

- Authentication & Authorization are two distinct processes
- Often performed in a row by the same application, but still distinct
- Abbreviations:
 - AuthN (Authentication)
 - AuthZ (Authorization)



Digital Identity

- Digital systems represent users (but also devices, resources,...) in their domain as digital **entities**.

Every digital entity has a finite number of **attributes** defining it's identity.

- Example of a user's digital identity attributes:
 - Username
 - Password
 - X.509 Digital Certificate
 - Name, surname
 - Home organization
 - Role within home organization



Digital Identity

- **Identifiers:** a subset of attributes that unambiguously identify the entity. Examples:
 - Social ID Number
 - (name, surname, place of birth, date of birth)
- Not easy to define:

To Plato's definition of a man as an animal, bipedal and featherless, Diogenes plucked a chicken and declared, "Here is Plato's man."



Identity Management

*“Hear me! For I am such and such a person
Above all, do not mistake me for someone else!”
- Friedrich Nietzsche, *Ecce Homo**

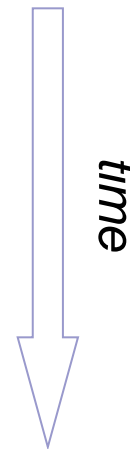
- What is Identity Management (IM)?

*“Identity Management is the set of business processes, and a supporting infrastructure, for the creation, maintenance, and use of digital identities”
- The Burton Group*

- It is more than account creation, more than directories, authentication, access controls, etc.
It includes policy, process, governance, trust, and new ways of thinking about IT

Identity Management

- Identity Management is a continuous process:
as people travel through an Institution from their very first time to their retirement they must be tracked without creating duplicates
- Example: as time goes by Anne Smith could be:
 - student
 - student & university staff
 - alumnus & university staff
 - alumnus
 - alumnus & professor
 - ...





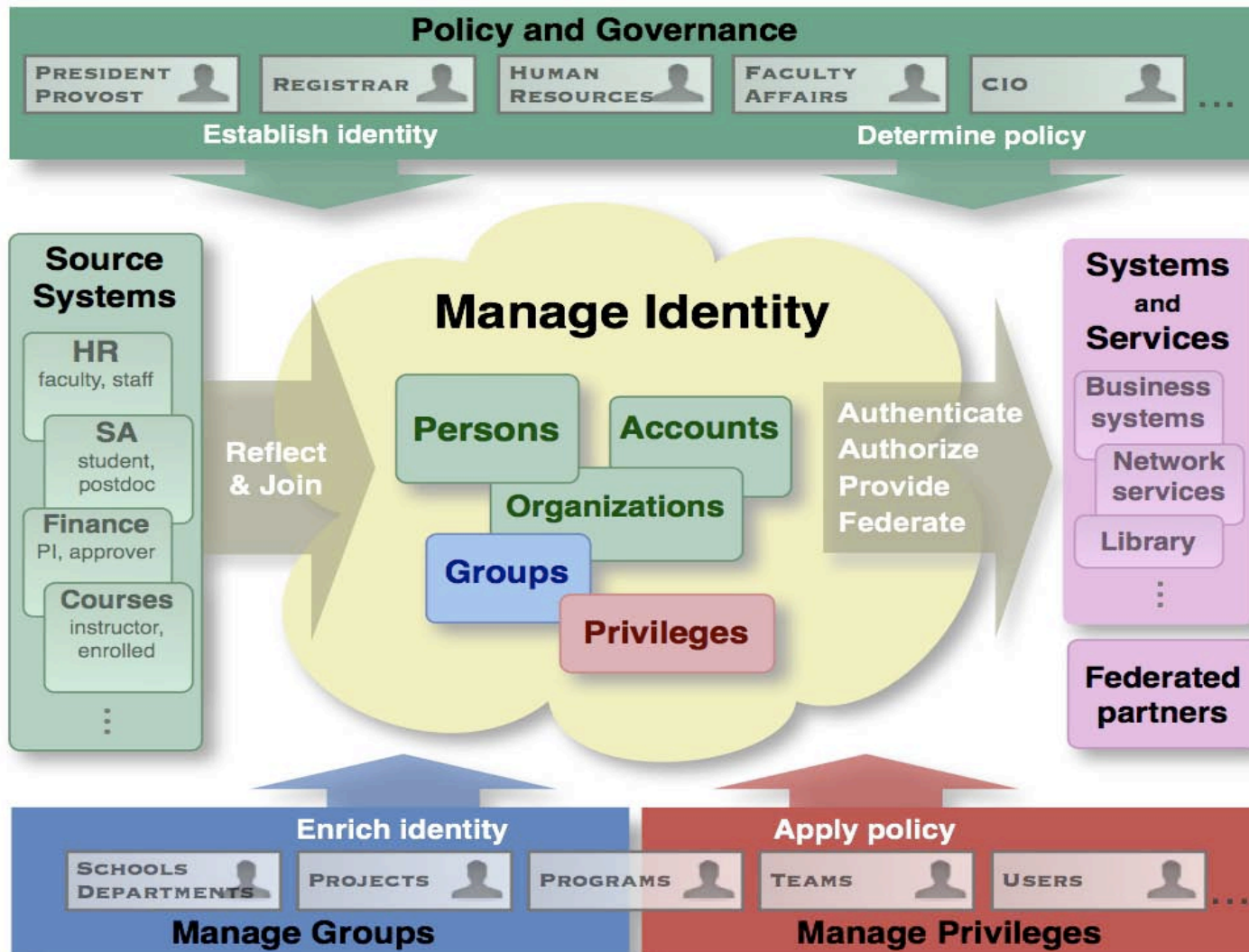
Identity and Access Management

- Identity and Access Management (IAM) is more than IM:

“Identity management refers to the policies, processes, and technologies that establish user identities and enforce rules about access to digital resources” (www.educase.edu)

- IM and IAM are often used interchangeably

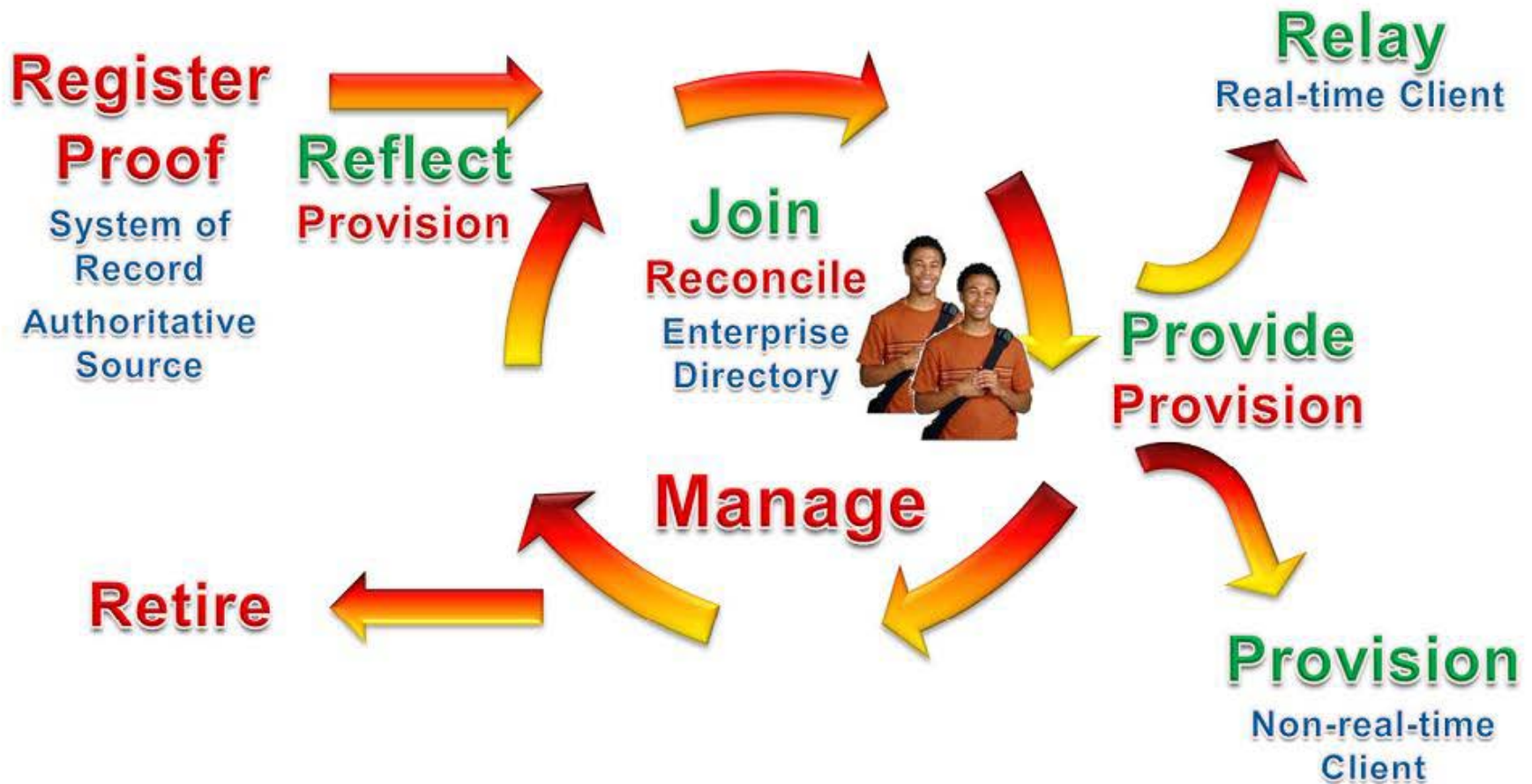
IAM Stakeholders



Source: <http://www.internet2.edu/pubs/200703-IS-MW.pdf>



IAM Lifecycle





IAM Process

- IAM is a continuous and demanding process
- Better done only once (centralize!)
- Starting point: your Systems of Record (SoRs):
 - Student Info. and HR Systems, Department IT Systems
- End (and start-again) point: place each person in the enterprise registry with a unique ID & identity attributes, and track changes in SoRs.
- Can be divided in a set of “IAM functions”



IAM Functions 1

- *Reflect*: obtain populations of interest from an authoritative System of Record (SoR, e.g. Student Info System or HR System) and place selected information into an enterprise registry. Also track changes to institutional data from changes in SoR.
- *Join/Reconcile*: remove ambiguities and resolve information from multiple SoRs about a person. Results in a person being placed in the enterprise registry with a unique identifier.
- *Credential*: issue credentials (username/password)



IAM Functions 2

- *Manage*: manage Authorization information (e.g. Affiliation, Groups, Privileges, Entitlements)
- *Authenticate*: make sure who the person is
- *Provide*: provide the identity and authZ information to resources for access decisions. Methods:
 - *Provision*: push IAM info to made available to resources, to retrieve when needed
 - *Relay/Deliver*: information made available when requested
- *Authorize*: allow/deny decision for access to resources
- *Log*: track usage for auditing and accounting purposes

Why Institutional (centralized) IAM?



©Steve Devoti www.educause.edu/ir/library/pdf/CAMP08110A.pdf



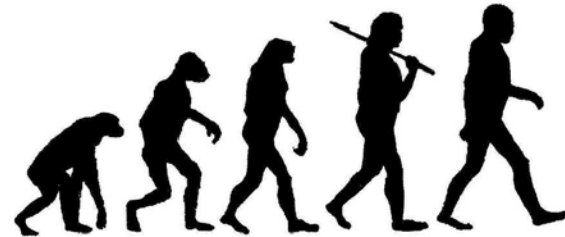


Why IAM?

- Simplifies user scaling (5000, 10000, 15000,...)
- Promotes the introduction of new services
- Reduces the incremental cost to implement a new service
- Reduce IT costs (many organizations save 30% or more by just implementing password management)
- Last but not least: bedrock for Single Sign On!

Evolution of IAM

- Stone Age:
Application maintains credentials (username & password) and identity information for each user



- Bronze Age
Credentials are centralized (e.g. Kerberos, LDAP) but applications maintain all user identity information
- Iron Age
Credentials and core identity information is centralized and application maintains only app-specific user data

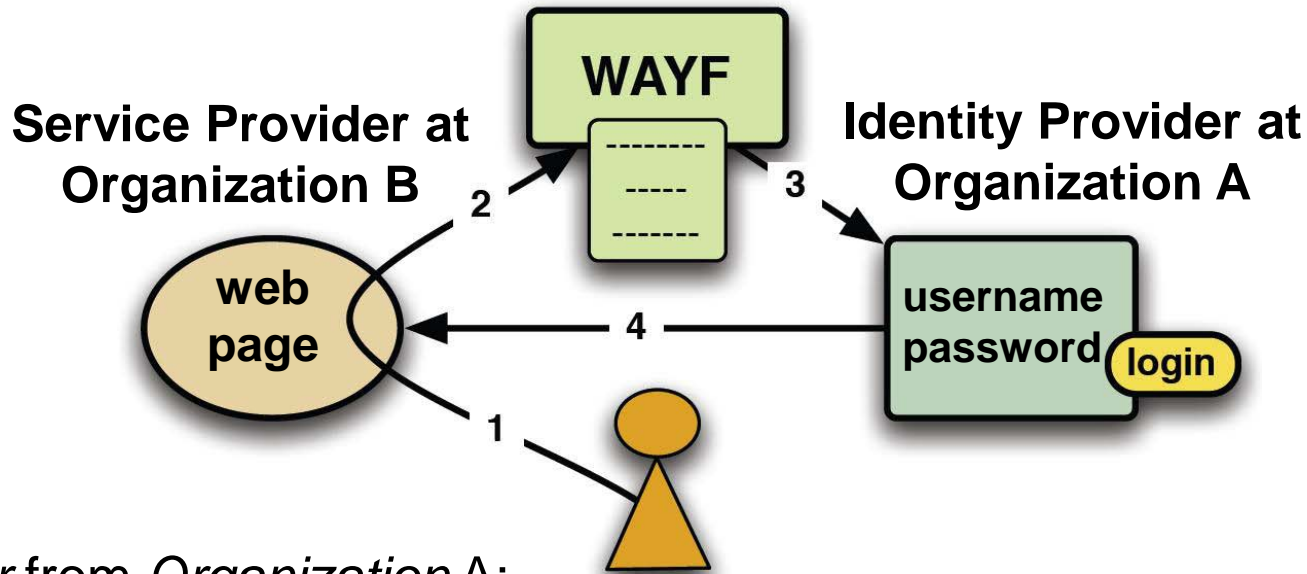
These solutions assume applications are within the same administrative domain.



Federated Identity and Access Management

- Classical IAM solutions assume applications are within the same administrative domain
- Federated Identity and Access Management (FIAM) is the next step:
sharing identity information managed only at the user's "*home organization*" with applications of "external organizations" outside the user's administrative domain.
- Successful idea: the number of federations is growing

Basic concept of FIAM



A user from Organization A:

1. tries accessing a protected resource on a Service Provider at Organization B
2. gets redirected to the WAYF where he chooses the Identity Provider of his Home Organization from a list.
3. gets redirected to the IdP's login page.
4. upon successful authentication gets redirected to the Service Provider carrying identity data (*attributes*) about himself.
The SP decides whether to grant access or not to the web page.

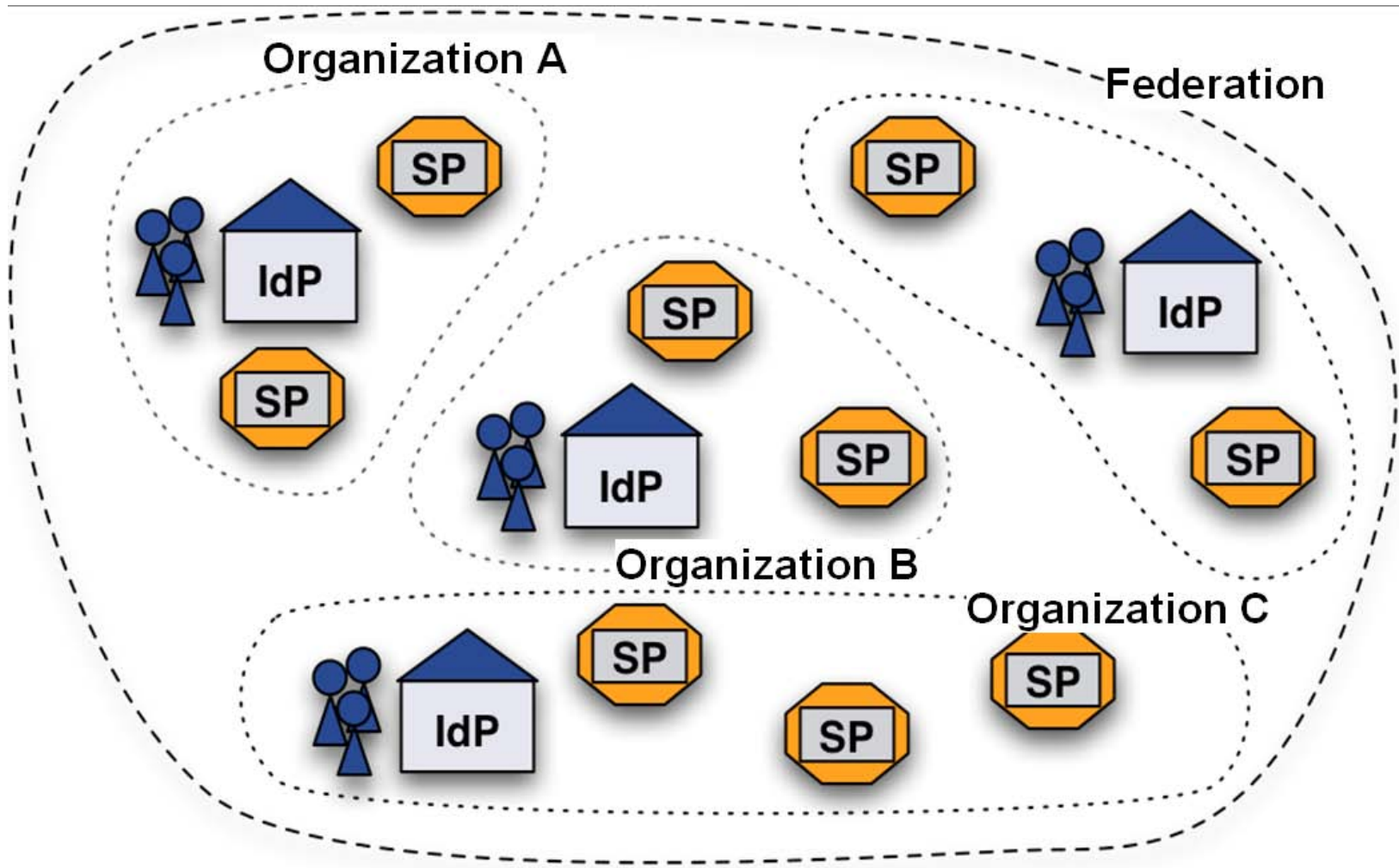


What is a Federation?

- In FIAM:
 - **Identity Providers*** (IdP) perform authentication and publish identity information (attributes) about users
 - **Service Providers*** (SP) consume this information and pass it to applications that provide the user with the requested resources (typically web pages)
- A **Federation** is a group of collaborating organizations running IdPs and SPs that share:
 - Technical agreements (protocols, Idap schemas,...)
 - Trust agreements

(*) Shibboleth terminology

Federation Components



[source: switch.ch/aa/]



Federation: Security & Privacy


FIAM allows active protection of:

- User's credentials

- only the IdP handles the credentials
- only the IdP performs user authentication

- User's identity information

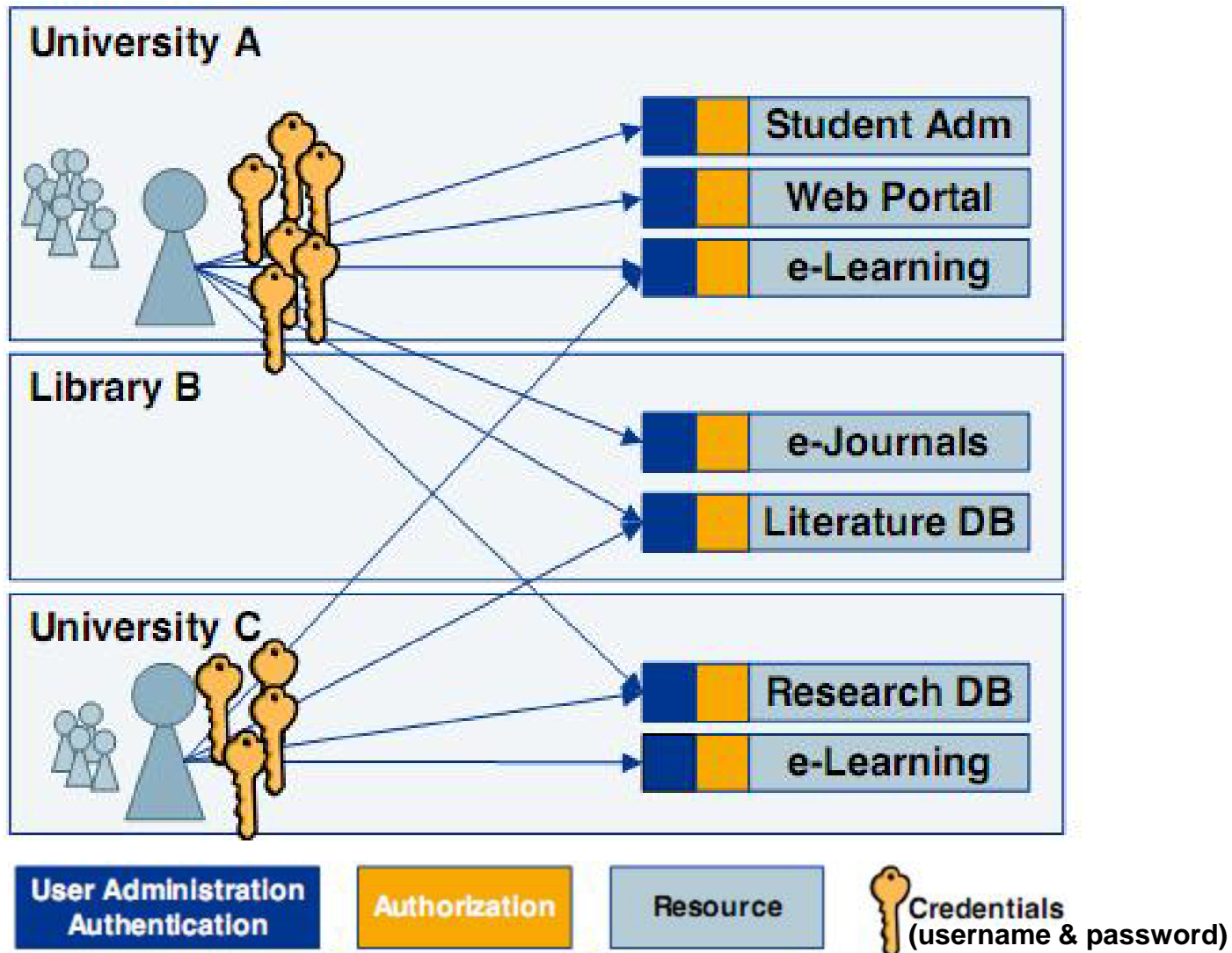
- the IdP releases a customized set of information to each SP
- only the minimal set of attributes necessary for the specific SP to provide the service

- 
-
- I Federations
 - II Digital Identity Management
 - **III AAI and Shibboleth**
 - IV Trust within the Federation

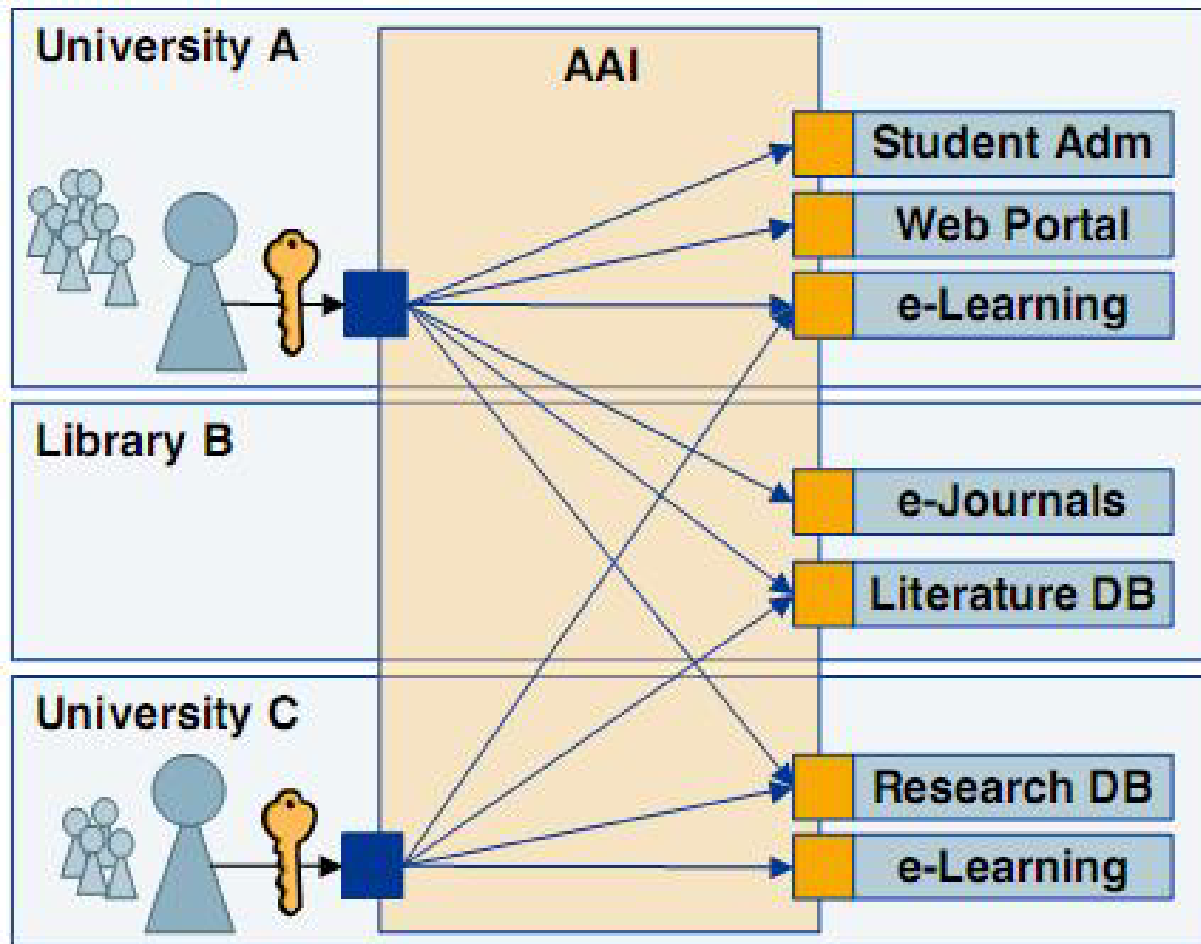
Authentication and Authorization Infrastructure

- Federations need an AAI to work
- What is an AAI?
Middleware software system that allow the delegation of authentication and authorization issues to different instances.
- Distributed software:
 - Client component (=browser)
 - SP component
 - IdP component
- AAIs connect user communities to resources

Without AAI



With AAI



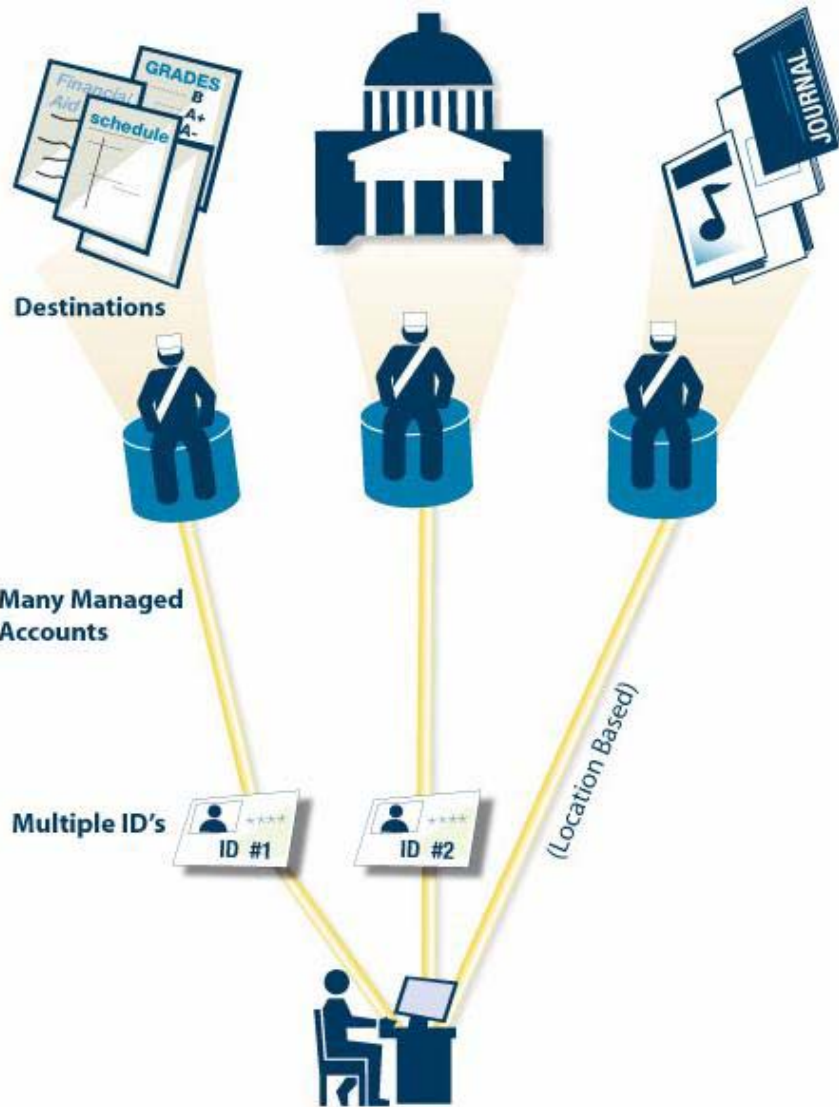
User Administration
Authentication

Authorization

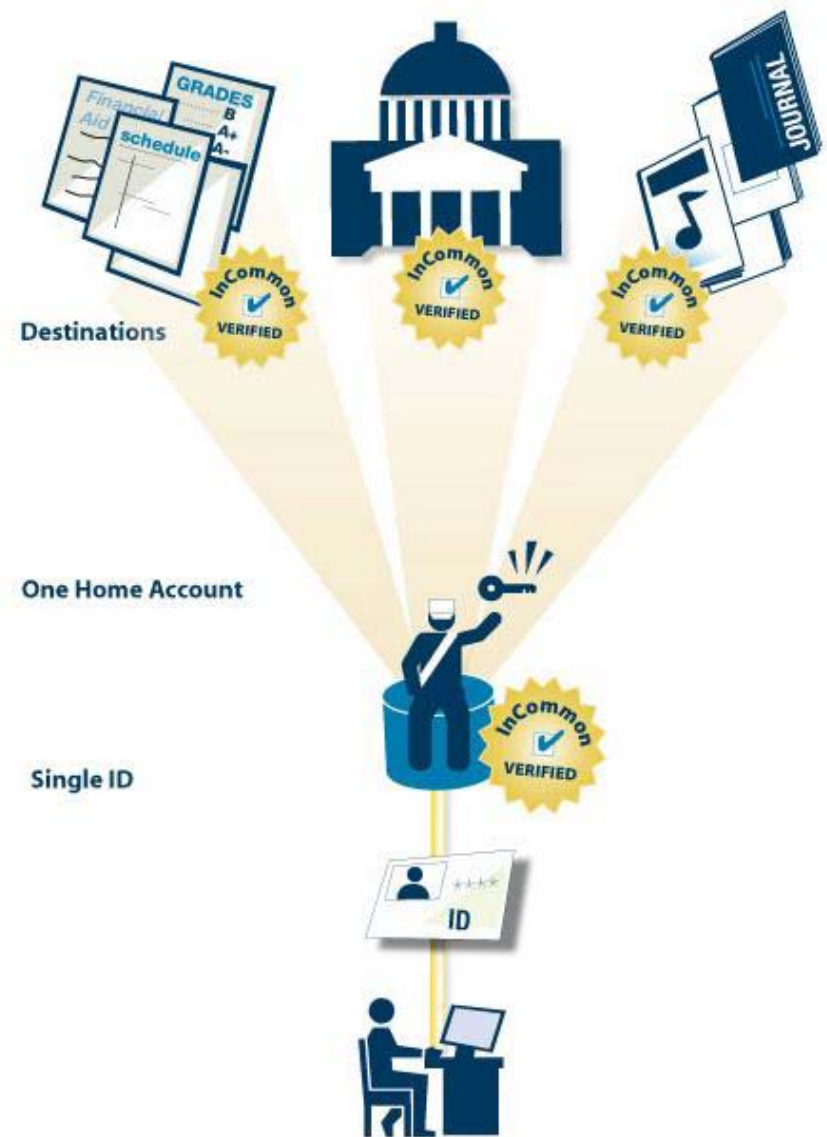
Resource

 Credentials
(username & password)

Without AAI



With AAI





Without AAI

- Tedious user registration at all resources
- Often outdated user data at resources
- Different login processes
- Many different usernames and passwords
- Many resources not protected due to difficulties
- Often IP-based authorization
- Costly implementation of inter-institutional access



With AAI: benefits for the user

- Single Sign On:
 - No more different usernames and passwords
 - Login performed just once at the user's home organization to access all resources
- User data always current, on all applications:
 - New phone number, address, ... immediately updated on all resources
- Privacy:
 - The accessed SP receives only attributes required to provide service. Often not even identity information: it might be enough to know that the user is enrolled at an Institution!

With AAI: benefits for the administrator

- Reduces work
 - Authentication-related calls to Penn State's helpdesk dropped by 85% after they installed Shibboleth
- No user registration and user data maintenance at resource needed
- Insulation from service compromises
 - In FIAM data is pushed to services as needed. If those services are compromised the attacker can't get everyone's data.
- Minimize attack surface area
 - Only the IdP needs to be able to contact user data stores. All effort can be focused on securing this one connection instead of one (more) connection per service.





With AAI: benefits for Institutions

- Efficient implementation of inter-institutional access. Easy to join.
- Collaboration between multiple organizations is simplified, exchange of knowledge is facilitated.
- Reduced administration costs: existing identity management system used for access to all resources
- High privacy requirements met, appropriate protection of personal information when accessing resources at other Institutions



AAI at work: a practical short tour

- Now I'll access some resources within my Institution and some outside it, but within the IDEM Federation
- We'll remove the cookies of the IdP and see what happens
- Nice videos (by JISC and AAF):
 - <http://www.youtube.com/watch?v=wBHiASr-pwk>
 - <http://www.youtube.com/watch?v=ewRUHB-UmNs>

Shibboleth®

- An Internet2 Middleware Project, an open source AAI, that enables web single sign on (SSO) across or within organizational boundaries
- Conceived in spring of 2000
- Based on the SAML standard
- Internationally used by universities
- <https://shibboleth.internet2.edu>



Why “Shibboleth”?

- “A use of language regarded as distinctive of particular group. First Known Use: 1638”
(www.merriam-webster.com)
- Hebrew *shibbōleth* “stream”; from the use of this word in Judg 12:6 as a test to distinguish Gileadites from Ephraimites
- During World War II the Dutch used the name of the town Scheveningen as a shibboleth to find out German infiltrators

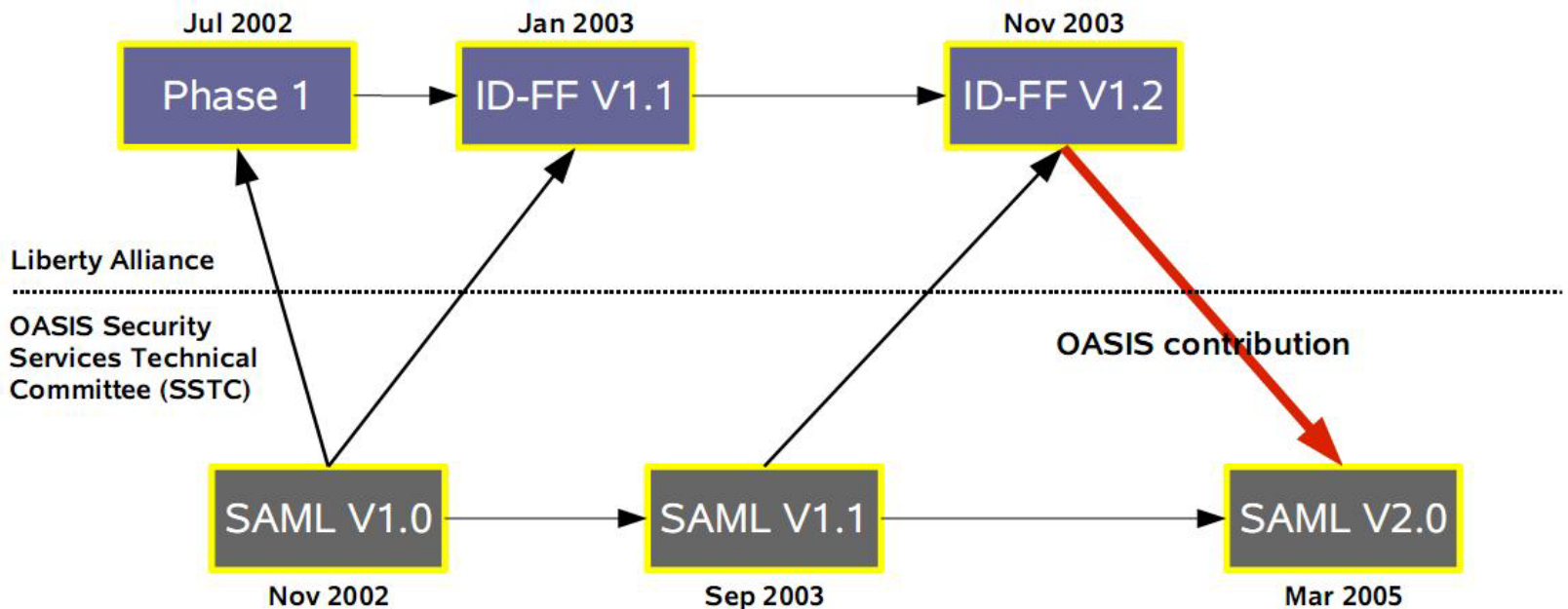


Shibboleth history

- Started 2000 under the MACE working group
- After an alpha, two betas, and two point releases were distributed to testing communities
Shibboleth 1.0 was released on July 1, 2003
(Partial implementation of SAML1)
- Shibboleth 1.3 was released on August 26, 2005
- Shibboleth 2.0 was released on March 19, 2008
(Partial implementation of SAML2)
- Current 2.2.0, released on Sept 23, 2010

SAML

- Security Assertion Markup Language
- XML-based framework for exchanging authentication and authorization data between entities

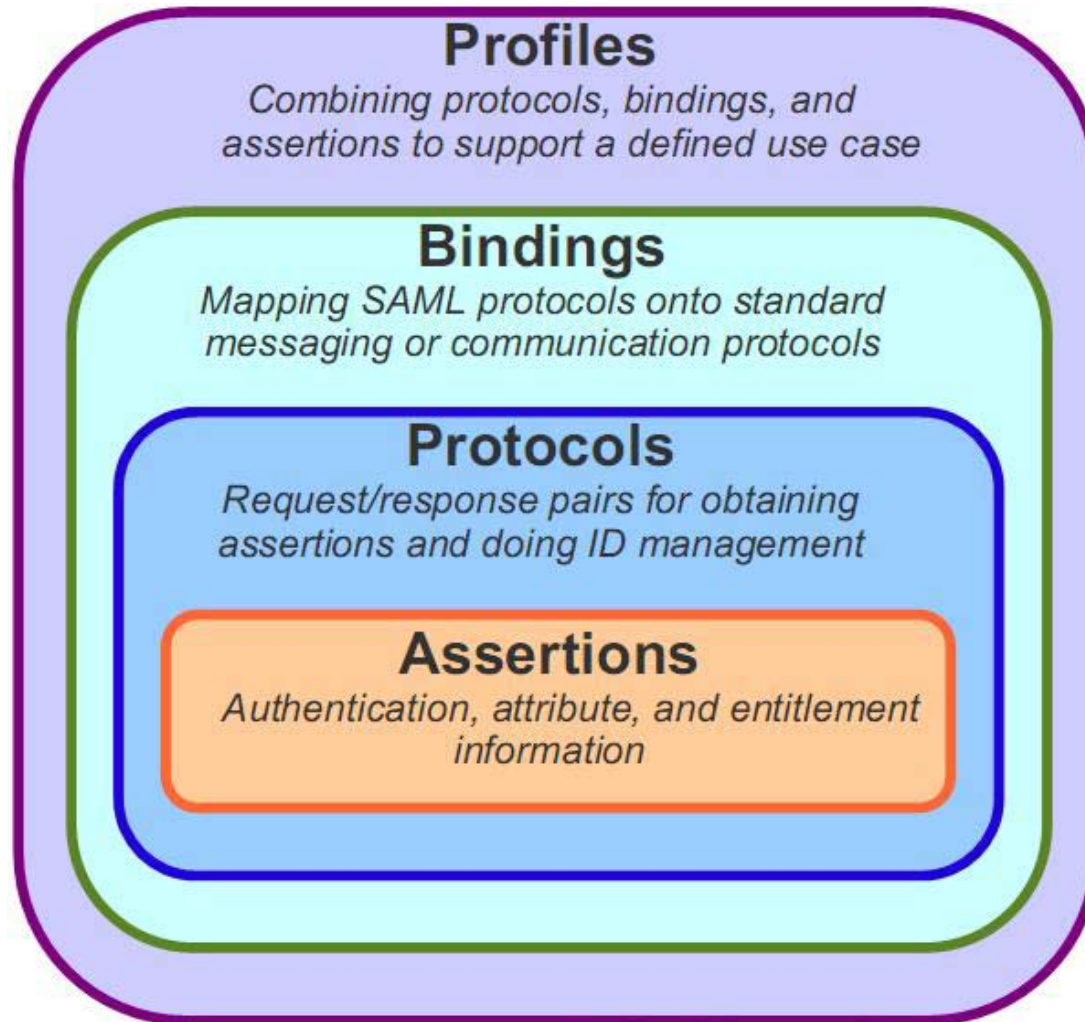




SAML

- SAML is the lingua franca of Federations
- SAML V2.0 not backwards-compatible
- OASIS standard
<http://docs.oasis-open.org/security/saml/v2.0/saml-2.0-os.zip>
- SAML “*profiles*” offer interop for a variety of *use cases*
- Shibboleth 2 implements SAML 2.0 “*Web Browser SSO Profile*”

SAML 2.0 Basic Concepts



SAML 2.0 Assertions

- A declaration containing one or more *statements* about a subject
 - Authentication statement: “Joe authenticated with a password at 9:00am”
 - Attribute statement: “Joe is a manager with a \$500 spending limit”
- It's all XML:

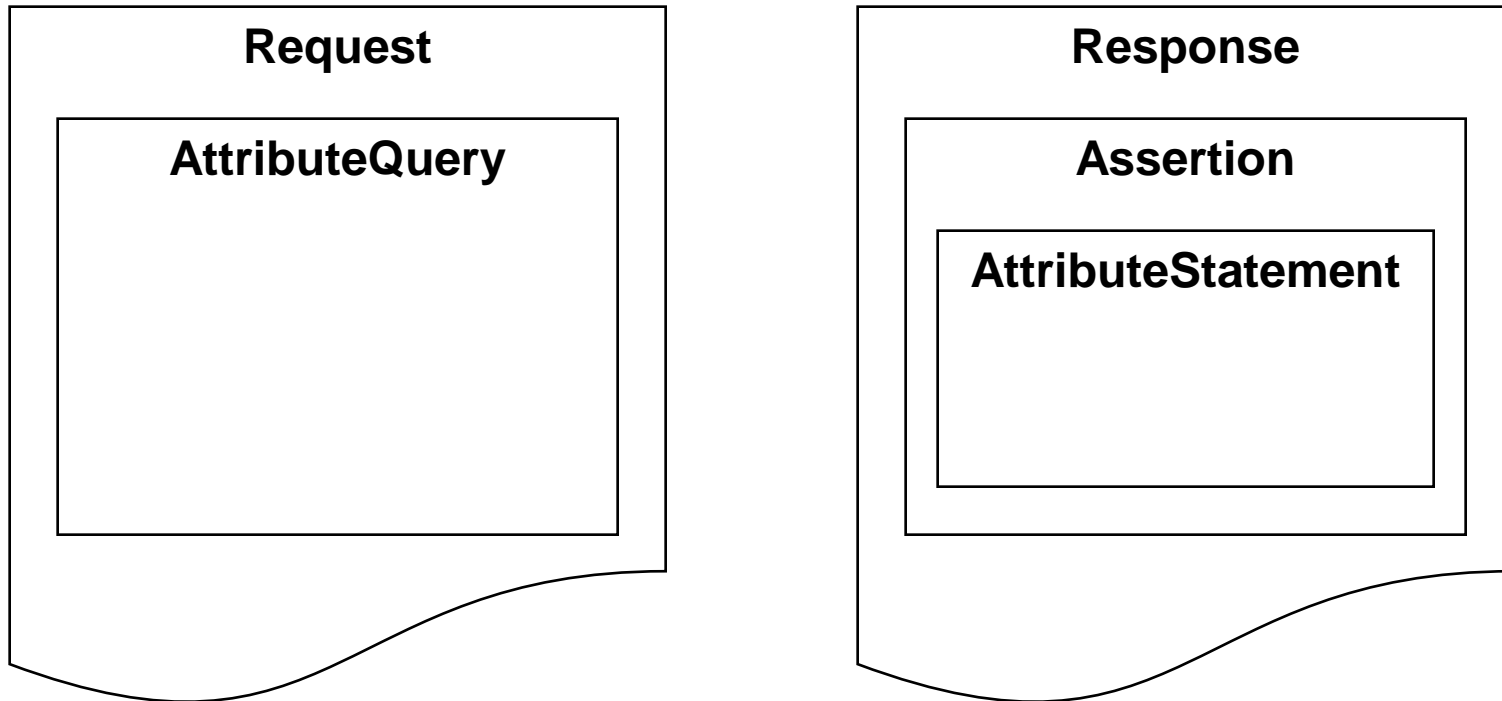
```
<saml:Assertion ... >
...
<saml:AuthnStatement
AuthnInstant="2005-01-31T12:00:00Z"
SessionIndex="67775277772">
<saml:AuthnContext>
<saml:AuthnContextClassRef>
urn:oasis:names:tc:SAML:2.0:ac:classes>PasswordProtectedTransport
</saml:AuthnContextClassRef>
</saml:AuthnContext>
</saml:AuthnStatement>
```



SAML 2.0 Protocols

- Request/response pairs that give the processing rules to be followed when producing or consuming assertions
 - Assertion Query and Request Protocol
 - Authentication Request Protocol
 - Artifact Resolution Protocol
 - Name Identifier Management Protocol
 - Single Logout Protocol
 - Name Identifier Mapping Protocol

SAML 2.0 Request/Response example



- How do we move around SAML requests/responses?
- No need to reinvent things: using standard protocols

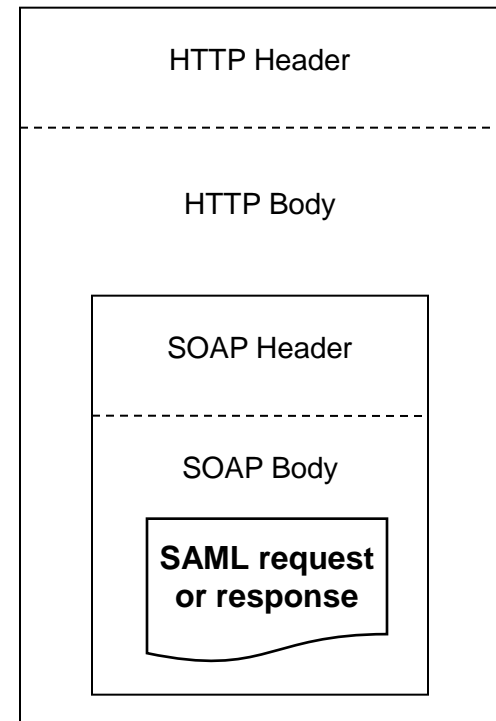


SAML 2.0 Bindings

- Mapping of a SAML protocols onto standard messaging or communication protocols
 - HTTP Redirect (GET) Binding
 - HTTP POST Binding
 - HTTP Artifact Binding
 - SAML URI Binding
 - SAML SOAP Binding (based on SOAP 1.1)
 - Reverse SOAP (PAOS) Binding

Example: SAML 2.0 SOAP binding

```
<SOAP-ENV:Envelope ...>
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <samlp:Response ...>
      <samlp:Status>
        ...
      </samlp:Status>
      <saml:Assertion ...>
        ...
      </saml:Assertion>
    </samlp:Response>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```



Source: <http://grid.ncsa.illinois.edu/presentations/saml-intro-dec05.ppt>



SAML 2.0 Profiles

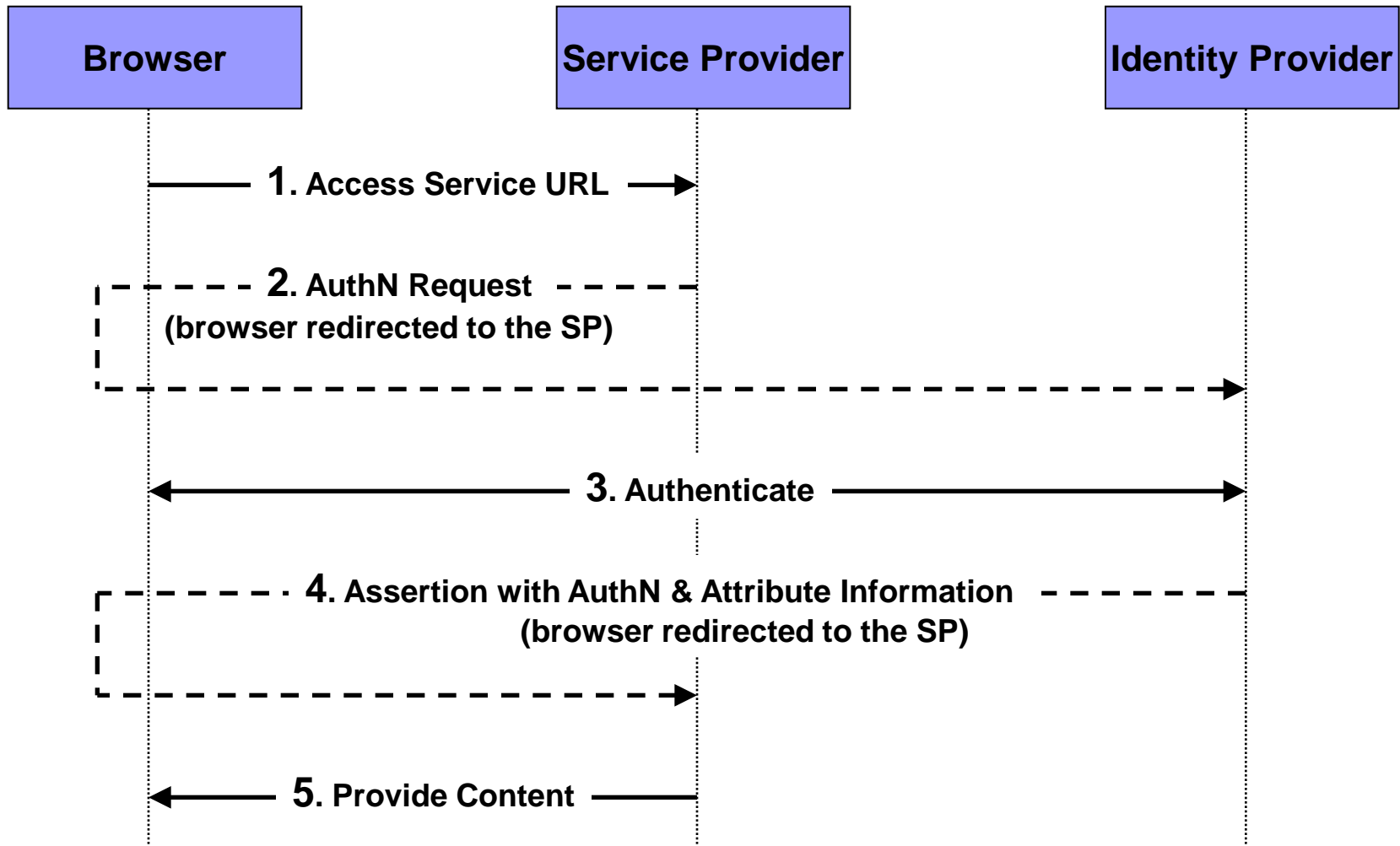
- Describe in detail how assertions, protocols, and bindings combine to support defined use cases. The most important is called “*Web Browser Single Sign On*” and addresses the use case of authZ and authN when accessing web applications across institutional boundaries
- 12 possible deployments of the “Web Browser SSO Profile” depending on the bindings chosen
 - The SP can use 4 (HTTP Redirect, HTTP POST and two forms of HTTP Artifact)
 - The IdP can use 3 (HTTP POST, two forms of HTTP Artifact)



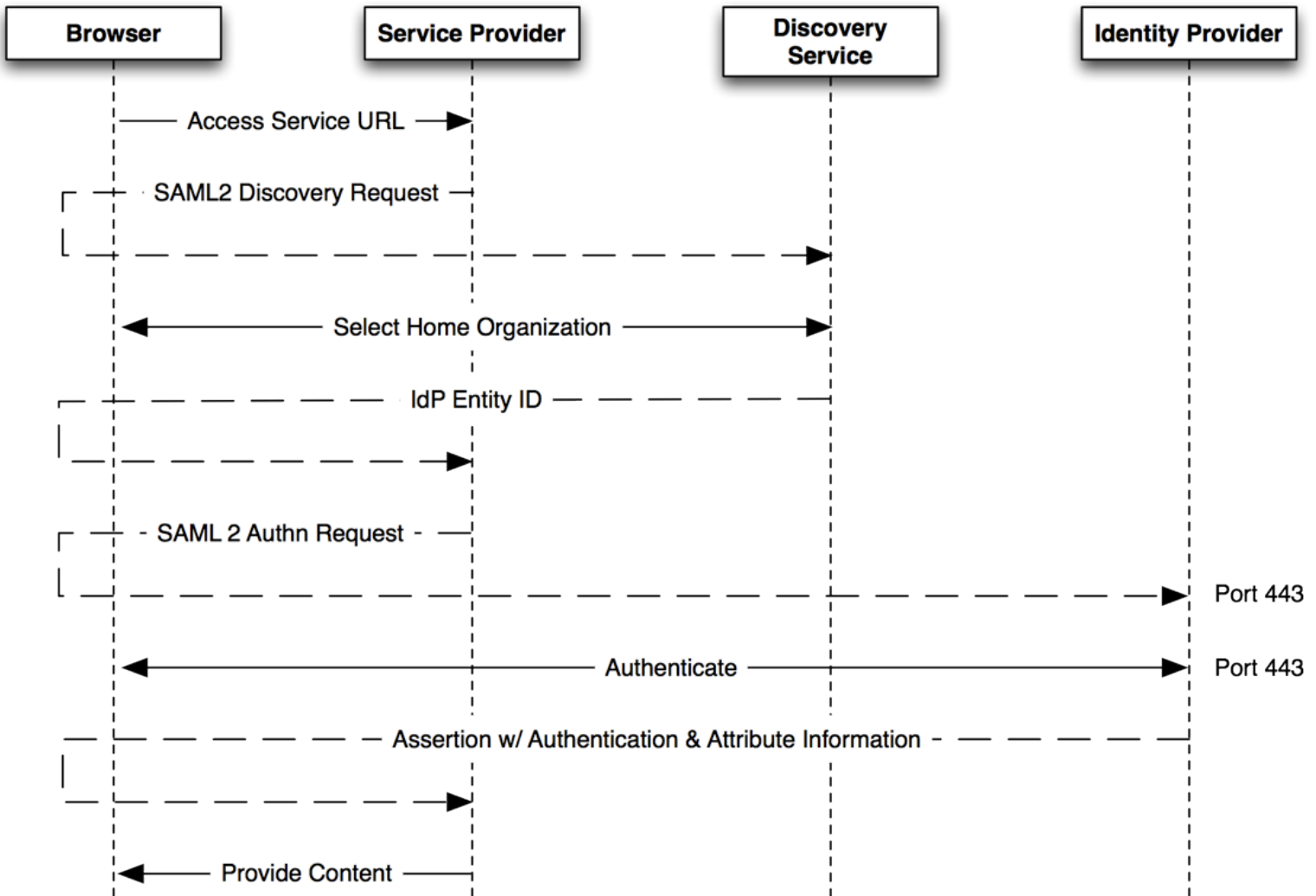
Shib at work: a practical short tour

- Install “Live HTTP Headers” on Mozilla Firefox
- Deactivate JavaScript
- Follow the shib communication flow
- Base64 decode SAML response from HTML source
<http://www.opinionatedgeek.com/dotnet/tools/base64decoder/>
- Try [Handler]/Shibboleth.sso/Session
- Nice demos:
<http://www.switch.ch/aai/demo/easy.html>
<http://www.switch.ch/aai/demo/medium.html>
<http://www.switch.ch/aai/demo/expert.html>

Shib Institutional Communication Flow



Interinstitutional Communication Flow



Source: <http://switch.ch/ai>

Single Log Out, Local Log Out

- Single Logout is a SAML 2.0 Profile
- Not (yet?) implemented in Shibboleth2

Read why

<https://spaces.internet2.edu/display/SHIB2/SLOIssues>

There is some hope ☺ though:

<http://www.switch.ch/export/sites/default/uni/security/aai/event/aai-info-day-2009/slides/AAI-ID09-51-SLO.pdf>

- Shibboleth 2 supports Local Log Out
 - [Handler]/Shibboleth.sso/Logout
 - but the IdP session remains active



Facts on Shibboleth

- Shib knows nothing about boundaries Federations, Cofederations, Peering, Virtual Organizations.
It “just” performs web browser SSO
- Easy setup, but
- Shib doesn't do any Identity Management
- Shib is not the only open source SAML implementation, see SimpleSAMLphp (<http://simplesamlphp.org/>)

Shibbolizing applications

- Sysadmin work:
 - Install SP and configure it to work with an IdP
 - Map attributes received from the IdP onto web server environment variables
- Programmer's use env variables as usual:

PHP:

```
if ($_SERVER['affiliation'] == 'staff')  
    { grantAccess() }
```

Perl:

```
if ($ENV{'affiliation'} == 'staff')  
    { &grantAccess() }
```

Java:

```
if (request.getHeader("affiliation").equals("staff") )  
    { grantAccess() }
```




Shibbolized applications

- Many applications already “shibbolized”: CMSs, Elearning Systems, Wikis,...
- Number keeps on growing
- <https://spaces.internet2.edu/display/SHIB2/ShibEnabled>



Links

- shibboleth.internet2.edu
- www.switch.ch/aai
- www.incommonfederation.org
- www.educause.edu
- www.ukfederation.org
- www.aaf.edu.au

- 
-
- I Federations
 - II Digital Identity Management
 - III AAI and Shibboleth
 - **IV Trust within the Federation**



Federation Manager

- A Federation is a group of collaborating Organizations running IdPs and SPs that share:
 - Technical agreements (protocols, Idap schemas,...)
It's not enough to agree on using Shibboleth!
 - Trust agreements
- The basis of Federations is *mutual trust*:
 - “I trust your authN process, you trust mine”
 - “I trust the user attributes you send me, you trust mine”
- A Federation Manager is needed to coordinate activities and, most important, to make trust possible



Organizations must agree on

- Technical Interoperability
 - Supported protocols
 - User authentication mechanisms
 - User attribute specifications
 - Accepted X.509 certificates
- Legal Interoperability
 - Membership agreement/contract
 - Federation operation policies
 - Requirements on IM practices
 - Procedures for handling sensitive personal information
- Others
 - Common best operational practices



IDEM Rules, Policies & Agreements

Technical and Legal IDEM documents:

- Member Accession Form
- Resource Registration Request
- Identity Provider Registration Request
- Memorandum of Understanding
- Rules of Participation
- Federation Regulation
- Attribute Specification
- DOPAU (IM practices)



Federation Manager's tasks I

- At a very minimum the Federation Manager
 - Acts as Trust “notary”: verifies the identity of Organizations and their delegated officers
 - Maintains the list of which IdPs and SPs are in the federation: the *federation metadata*



Federation Metadata

- An XML document describing every IdP and SP. Contains
 - Unique identifier (entityID) for each SP/IdP
 - Endpoints where each SPs/IdPs can be contacted
 - Certificates used for signing and encrypting exchanged data
- May contain
 - Organization and person contact information
 - Information about which attributes an SP wants/needs
- Usually distributed by a public HTTP URL
- Metadata **must** be kept up to date so that
 - New entities can work with existing ones
 - Old, or revoked, entities are blocked
- Metadata **should** be signed by the Federation Manager



Federation Manager's tasks II

Most Federation Managers also:

- Define agreements, rules, and policies for participants
- Provide some user support:
 - Documentation
 - Email list, helpdesk
 - Organize periodic meetings, workshops
- Operate a Central Discovery Service (WAYF)
- Operate a test infrastructure

Federation Manager's tasks III

Some Federation Managers:

- Provide self-service tools for managing IdP and SP data
- Install IdPs and SPs for members
- Verify that Organizations stand by their commitments
- Develop custom tools or application integration support :
 - Resource Registry
 - Virtual Home Organization
 - Group Management Tool
 - Attribute Viewer
 - Joomla idemauth
 - uApprove
 - AAIEye



Levels of Assurance (LOAs)

- Important part of the trust fabric
 - IdPs indicate how much trust is behind the authN event (e.g. “Level 1”, “Level 2”, ...)
 - SPs, based on their own needs and assessment of risks, determine what LOA they require to allow user access
- Assurance is separated into two concepts:
 - The strength of the processes used to identify the user at the time of user registration
 - The strength of the authN method(s) used
- Links:
 - <http://www.terena.org/activities/refeds/loa.html>
 - <http://www.aaf.edu.au/index.php/technical/levels-of-assurance/>



Thank you!

Q & A