Lanka Education and Research Network

SAML, Identity Provider, Service Provider & Federation

IAM in Campus Networks

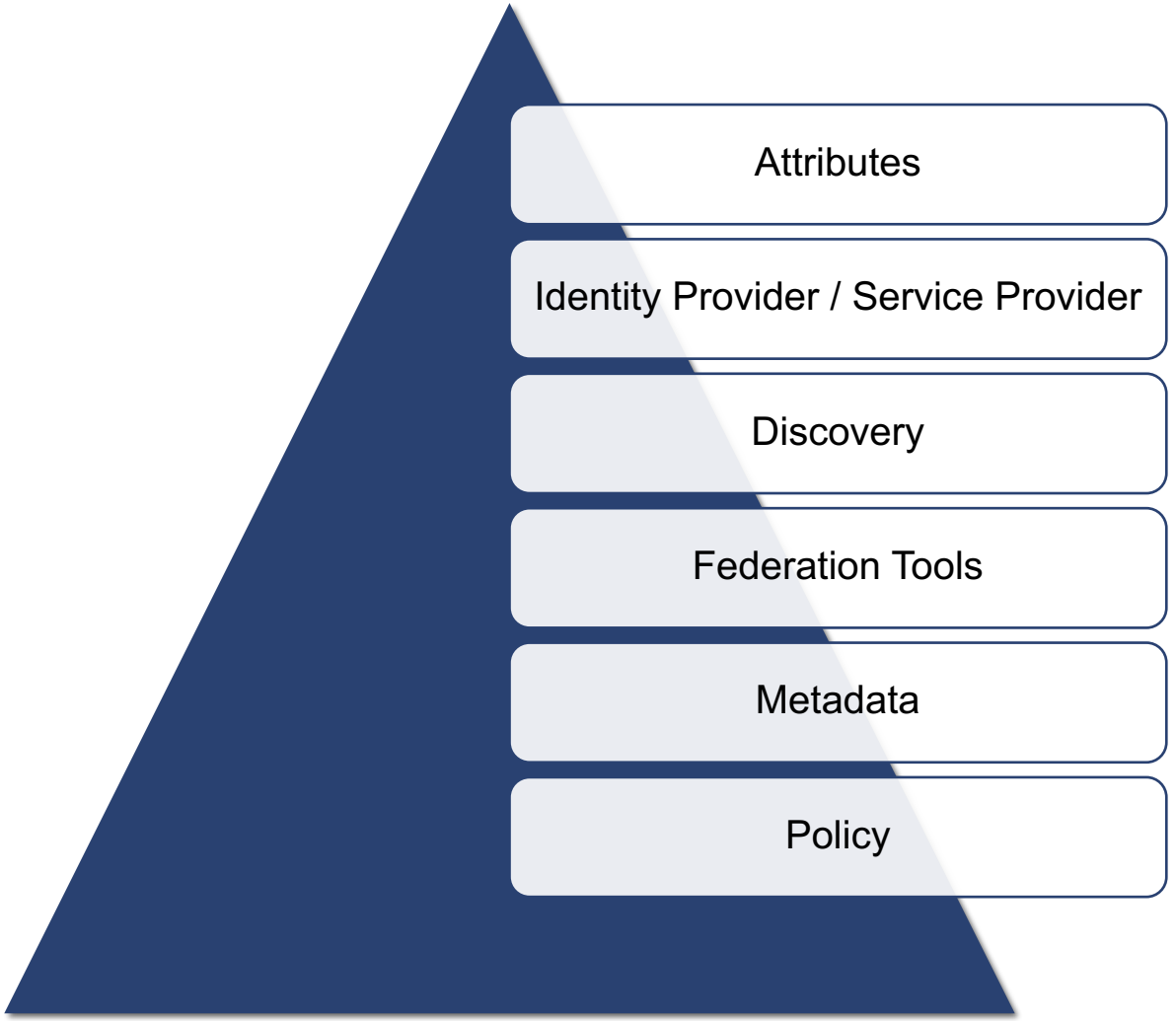
27th September 2018

Workshop on Federated Identity Management

LEARN

Based on APAN-Backfire / Tuakiri / AAF / SWITCH / IDEM content on IAM

Building Blocks of Federation



Identity Providers

Organisations with users run Identity Providers

- Provide a login page
- Provides a mechanism for consent of attribute release
- Login page is branded to the organisation
- Login against the organisation LDAP or AD
- Manages password reset
- Provisions and de-provisions accounts
- Agrees to the federation policies

Can be used for campus Single Sign-on as well as federated SSO!

Service Providers

Run by organizations that have something to offer the federation community

- Hands off authentication to IdPs
- Obtains attributes from IdPs
- Agrees to the federation policies

Discovery

A mechanism they allows the user to select their organisation where they will login. Discovery can occur at either

The federation

- All IdPs will be listed
- User can select to have their IdP always selected
- Federation look and feel

By the service

- SP can list a sub-set of IdPs
- Look and feel is that of the SP

Users quickly understand the extra step in authentication

Note: Some commercial access management software providers don't fully understand discovery – provide enterprise SSO

Metadata

- The Metadata is a technical document that contains technical details of all IdPs and SPs in the federation.
- Cryptographically signed by the federation operator
- Policy and Processes determine which IdPs and SPs are published in the metadata
- All IdPs and SPs regularly consume the metadata
- Provided the trust in the federation!

Note: Some commercial access management software vendors have difficulty dealing with federation metadata!

Federation Metadata

An XML document that describes **every federation entity**

- Contains
  - Unique identifier for each entity known as the **entityID**
  - Endpoints where each entity can be contacted
  - Certificates used for signing and encrypting data
- May contain
  - Organization and person contact information
  - Information about which attributes an SP wants/needs
- Metadata is usually distributed by a public HTTP URL
  - The metadata should be digitally signed
  - Signature should be verified!
- Metadata must be kept up to date, so that
  - new entities can interoperate with existing ones
  - old or revoked entities are blocked

Identifiers

DON'T assume successful authentication means the user is authorized for service.

Campus

- CONSIDER stronger authentication (e.g., multi-factor) over password strengthening (increasing length, complexity requirements)

Vendor

- DO let the identity provider handle authentication
- DO rely on browser-based authentication for non-browser applications.
- DON’T use service-specific passwords unless there are no alternatives.
- DO use forced re-authentication when appropriate.

Identifiers

Campus

- DO expect the typical vendor to have a single, set model for creating user accounts on their systems.
- DO practice "defensive programming" when setting up provisioning services.
- DON'T require out-of-band acceptance of Terms of Use.
- DON'T expect robust de-provisioning support.
- DO handle username changes.

Vendor:

- DO support just-in-time provisioning based on user attributes passed in SAML assertions whenever possible.
- DO consider standardizing your provisioning (and de-provisioning) APIs.
- DO manage your provisioning API in a way that respects the service subscriber interests.

Identifiers – eduPerson Schema

eduPerson specification is to support LDAP operations to include an **auxiliary object class** for campus directories. It consists of a set of data elements or attributes about individuals within higher education, along with recommendations on the syntax and semantics of the data that may be assigned to those attributes.

- eduPersonAffiliation
- eduPersonNickname
- eduPersonOrgDN
- eduPersonOrgUnitDN
- eduPersonPrimaryAffiliation
- eduPersonPrincipalName
- eduPersonEntitlement
- eduPersonPrimaryOrgUnitDN
- eduPersonScopedAffiliation
- eduPersonTargetedID
- eduPersonAssurance
- eduPersonPrincipalNamePrior
- eduPersonUniqueId
- eduPersonOrcid

Ref: http://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201602.html

ORCID

Vision

ORCID's vision is a world where all who participate in research, scholarship, and innovation are uniquely identified and connected to their contributions across disciplines, borders, and time.

Mission

ORCID provides an identifier for individuals to use with their name as they engage in research, scholarship, and innovation activities. We provide open tools that enable transparent and trustworthy connections between researchers, their contributions, and affiliations. We provide this service to help people find information and to simplify reporting and analysis.

https://orcid.org/

Identifiers

Both Campus and Vendor: DO support a varied set of identifiers.

Both Campus and Vendor: CONSIDER the use of eduPersonTargetedID where appropriate.

Both Campus and Vendor: DO use standard definitions of identifiers and attributes.

Both Campus and Vendor: DON'T mistake eduPersonPrincipalName for a valid email address.

Campus: DO standardize internally on a stable "serial number" for users.

Campus: DO make eduPersonPrincipalName useful.

Identifiers – What we going to use

User Identifiers

eduPersontargetedID

eduPersonPrincipalName

UID

ORCID

eduPersonUniqueID

Personalisation

Display Name

GivenName

Surname

Title

eMail

Group membership

eduPersonPrincialName

eduPersonEntitlement

Group Member

Organisational

Organisation Name

Organisation domain name

SAML

Security Assertion Markup Language (SAML) is an open standard that allows identity providers (IdP) to pass authorization credentials to service providers (SP).

That is you can use one set of credentials to log into many different websites. It's much simpler to manage one login per user than it is to manage separate logins to email, moodle, library systems, world-wide labs etc.

SAML transactions use Extensible Markup Language (XML) for standardized communications between the identity provider and service providers. SAML is the link between the authentication of a user's identity and the authorization to use a service.

SAML

SAML works by passing information about users, logins, and attributes between the identity provider and service providers.

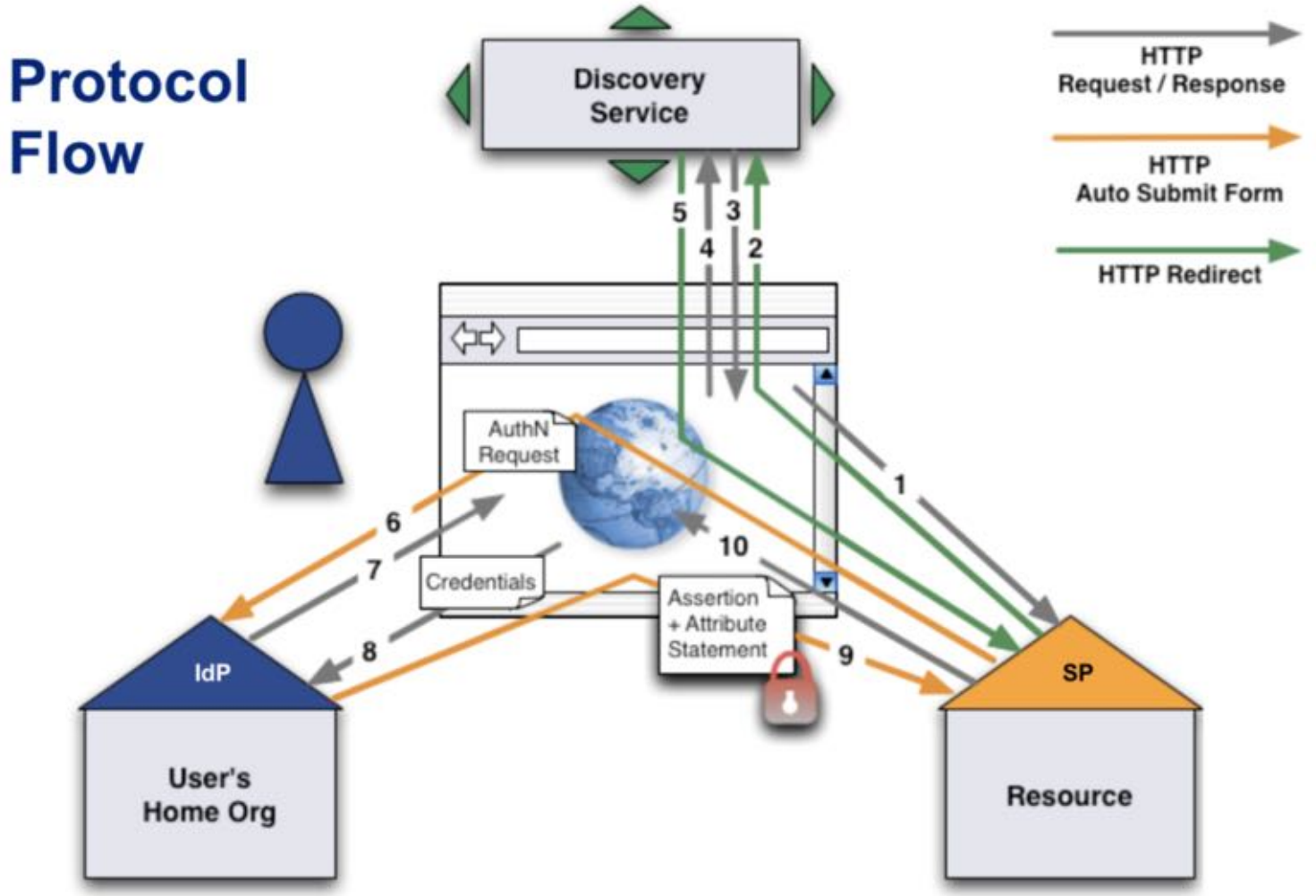
Each user logs in once to Single Sign On with the identify provider, and then the identify provider can pass SAML attributes to the service provider when the user attempts to access those services.

The service provider requests the authorization and authentication from the identify provider.

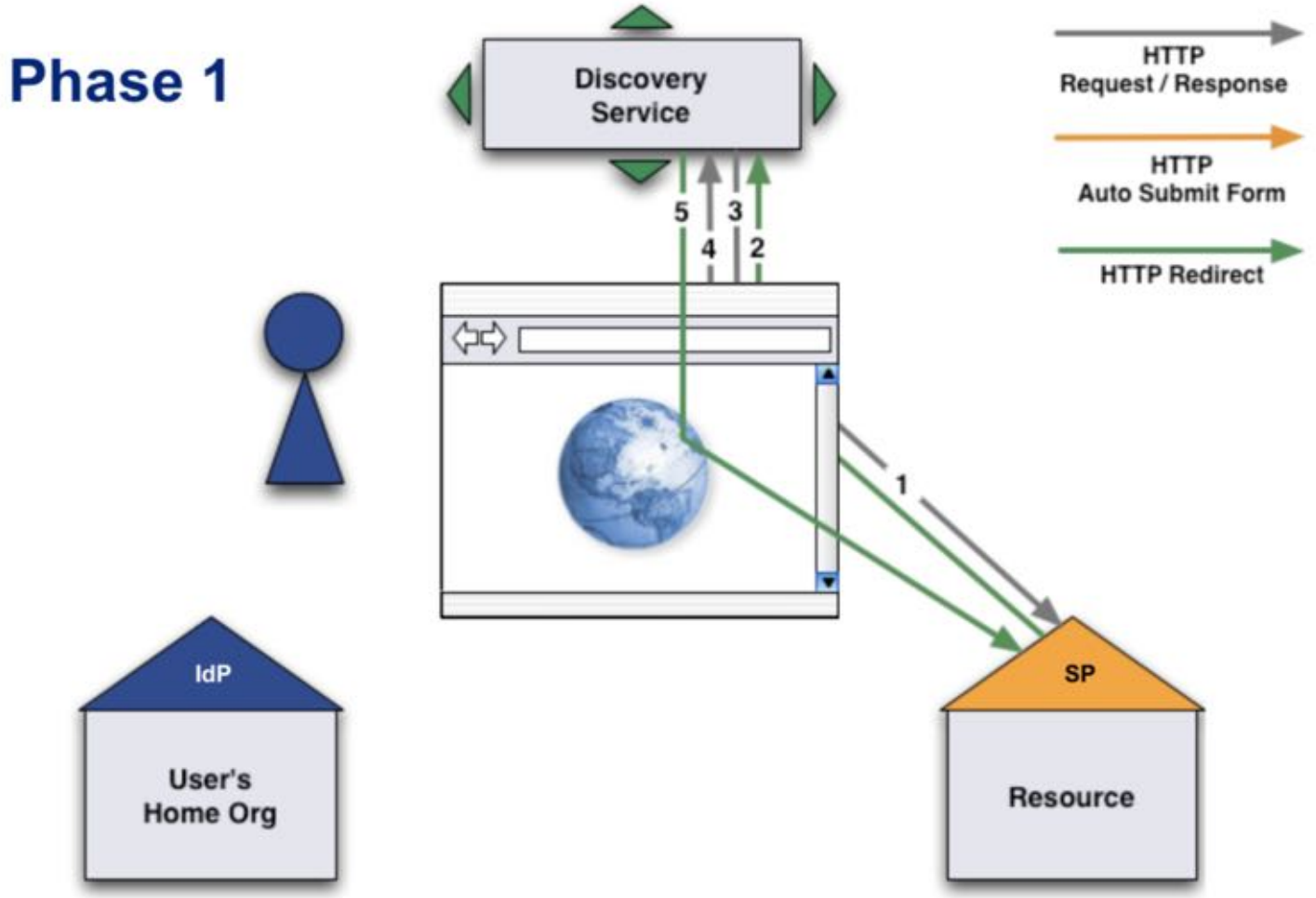
Since both of those systems speak the same language – SAML – the user only needs to log in once.

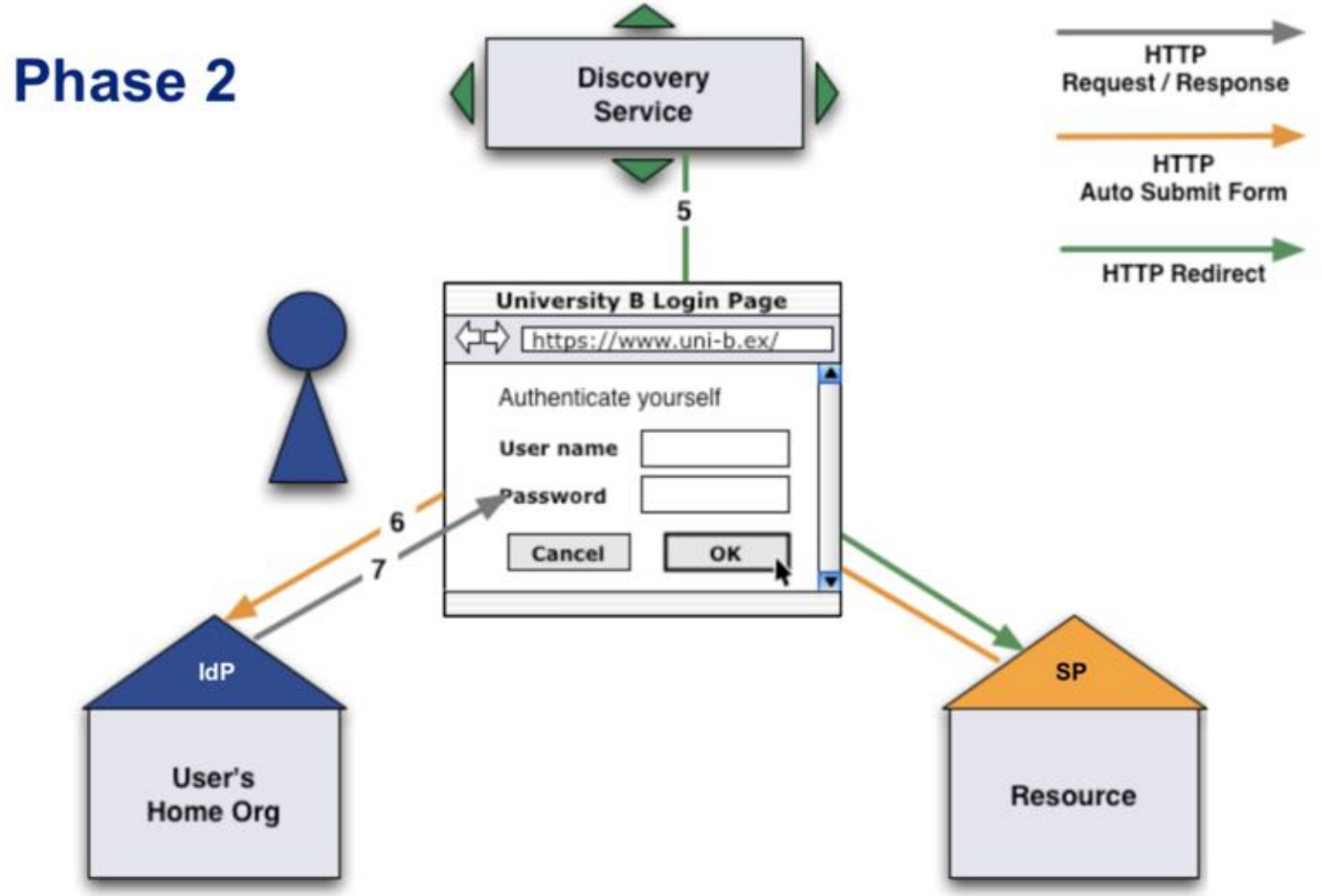
Each identity provider and service provider need to agree upon the configuration for SAML. Both ends need to have the exact configuration for the SAML authentication to work.

SAML


Protocol Flow
Discovery Service
HTTP Request / Response
HTTP Auto Submit Form
HTTP Redirect
5
3
4
2
AuthN Request
1
6
10
7
Credentials
Assertion + Attribute Statement
8
9
IdP
SP
User's Home Org
Resource

SAML


Phase 1
Discovery Service
HTTP Request / Response
HTTP Auto Submit Form
HTTP Redirect
5
4
3
2
1
IdP
User's Home Org
SP
Resource


Phase 2
Discovery Service
5
HTTP Request / Response
HTTP Auto Submit Form
HTTP Redirect
University B Login Page
https://www.uni-b.ex/
Authenticate yourself
User name
Password
Cancel
OK
6
7
IdP
User's Home Org
SP
Resource

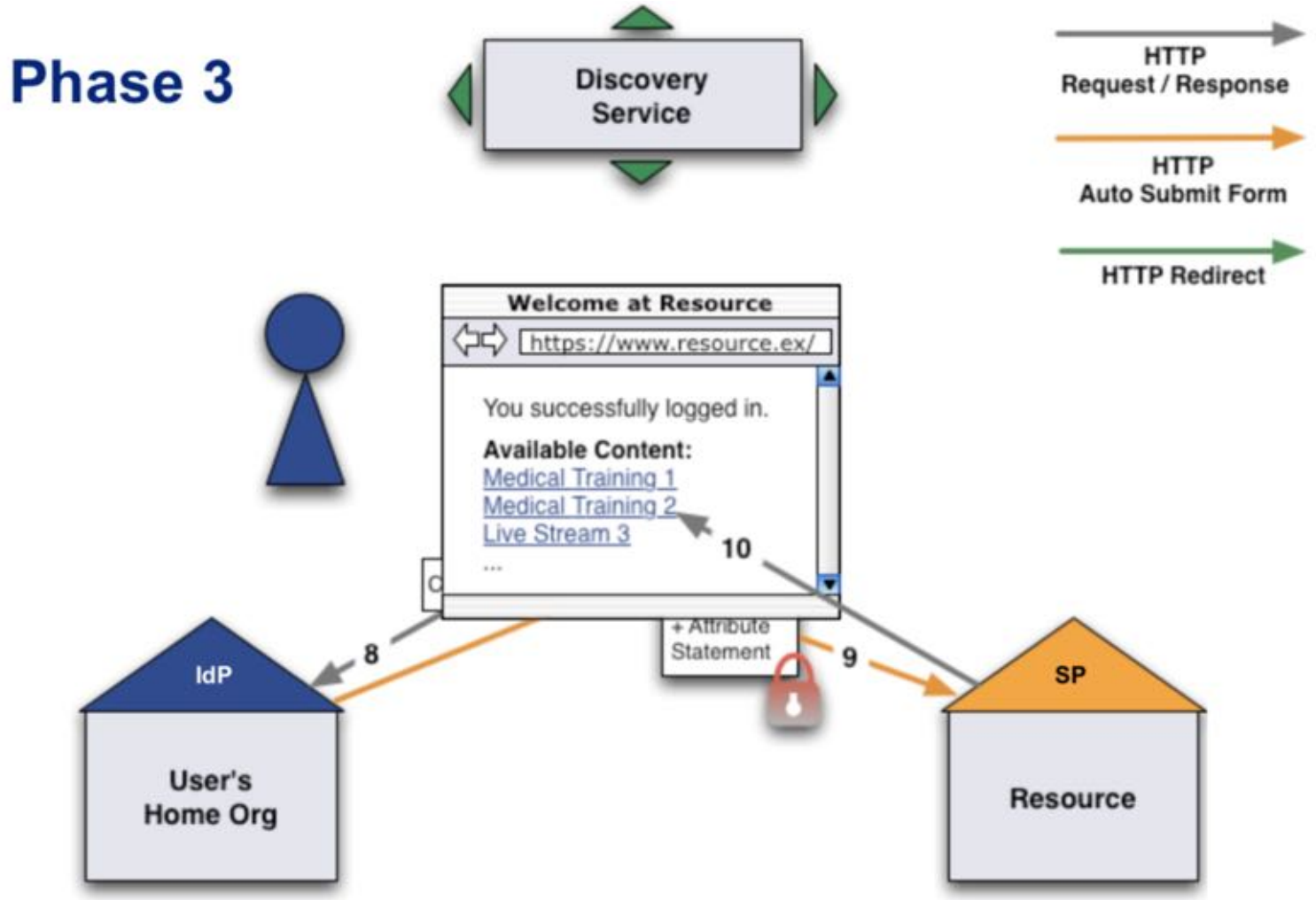
SAML AuthN Request

Plain HTML:

```
<html>
  <body onload="document.forms[0].submit()">
    <form method="POST" action="https://aai-demo-idp.switch.ch/idp/profile/SAML2/POST/SSO">
      <input type="hidden" name="RelayState" value="ss:mem:23e3a3b1268acd89dc226bb1ce0d0c6ba7ecf773"/>
      <input type="hidden" name="SAMLRequest"
          value="PHNhbWxwOkF1dGhuUmVxdWVzdCB4bWxuczpzYW1scD0idXJuOm9hc2lzOm5h...
          ...YXRlPSIxIi8+PC9zYW1scDpBdXRoblJlcXVlc3Q+"/>
    </form>
  </body>
</html>
```

SAML AuthN Request (Base64 decoded)

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    AssertionConsumerServiceIndex="1"
    Destination="https://aai-demo-idp.switch.ch/idp/profile/SAML2/POST/SSO"
    ID="_f2f27516ec08af29501c749629b119d3"
    IssueInstant="2008-02-27T12:17:40Z"
    Version="2.0">
  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
    https://aai-demo.switch.ch/shibboleth
  </saml:Issuer>
  <samlp:NameIDPolicy xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
      AllowCreate="1"/>
</samlp:AuthnRequest>
```

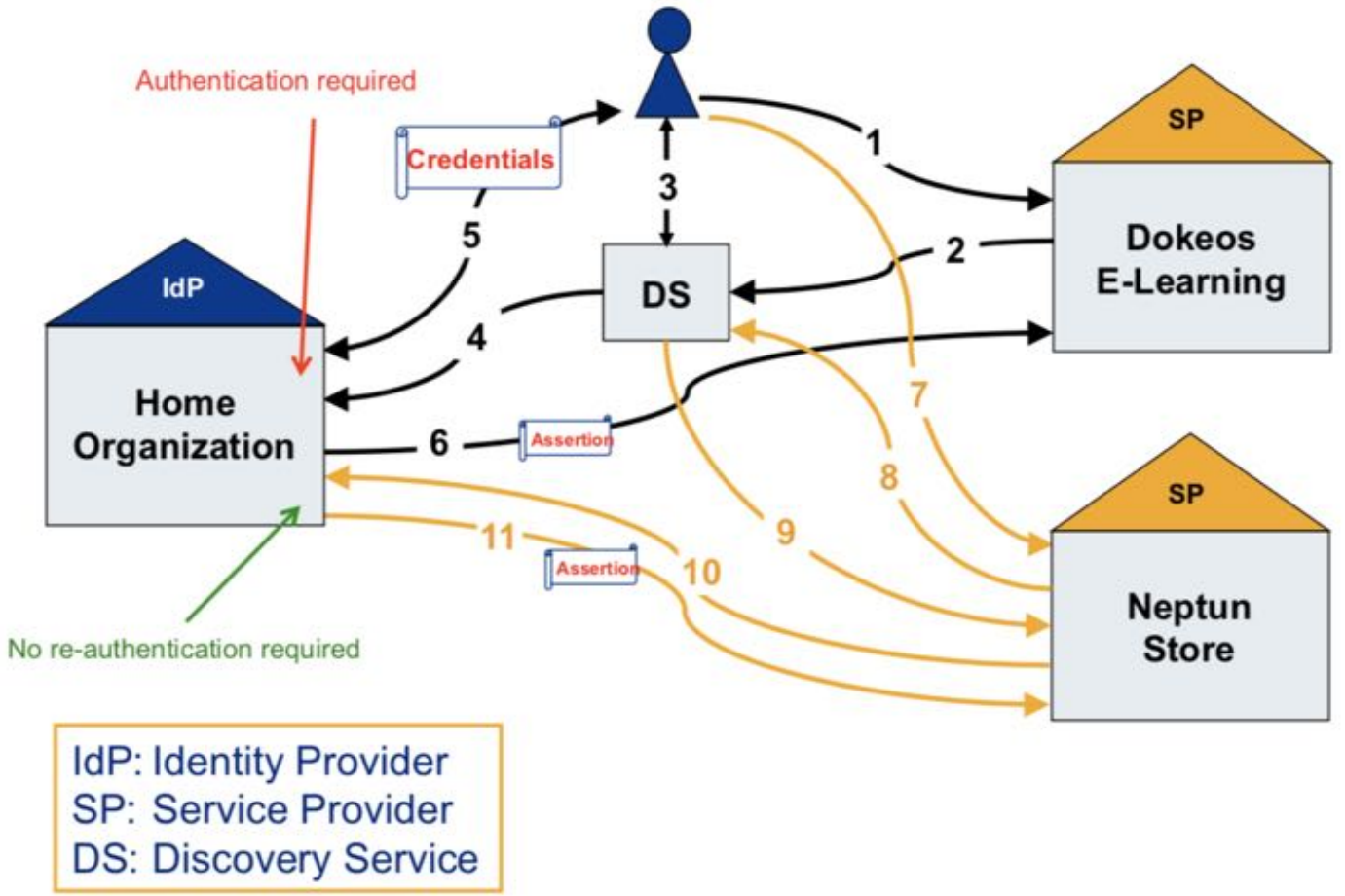

Phase 3
Discovery Service
HTTP Request / Response
HTTP Auto Submit Form
HTTP Redirect
Welcome at Resource
https://www.resource.ex/
You successfully logged in.
Available Content:
Medical Training 1
Medical Training 2
Live Stream 3
...
10
+ Attribute Statement
8
9
IdP
User's Home Org
SP
Resource

SAML

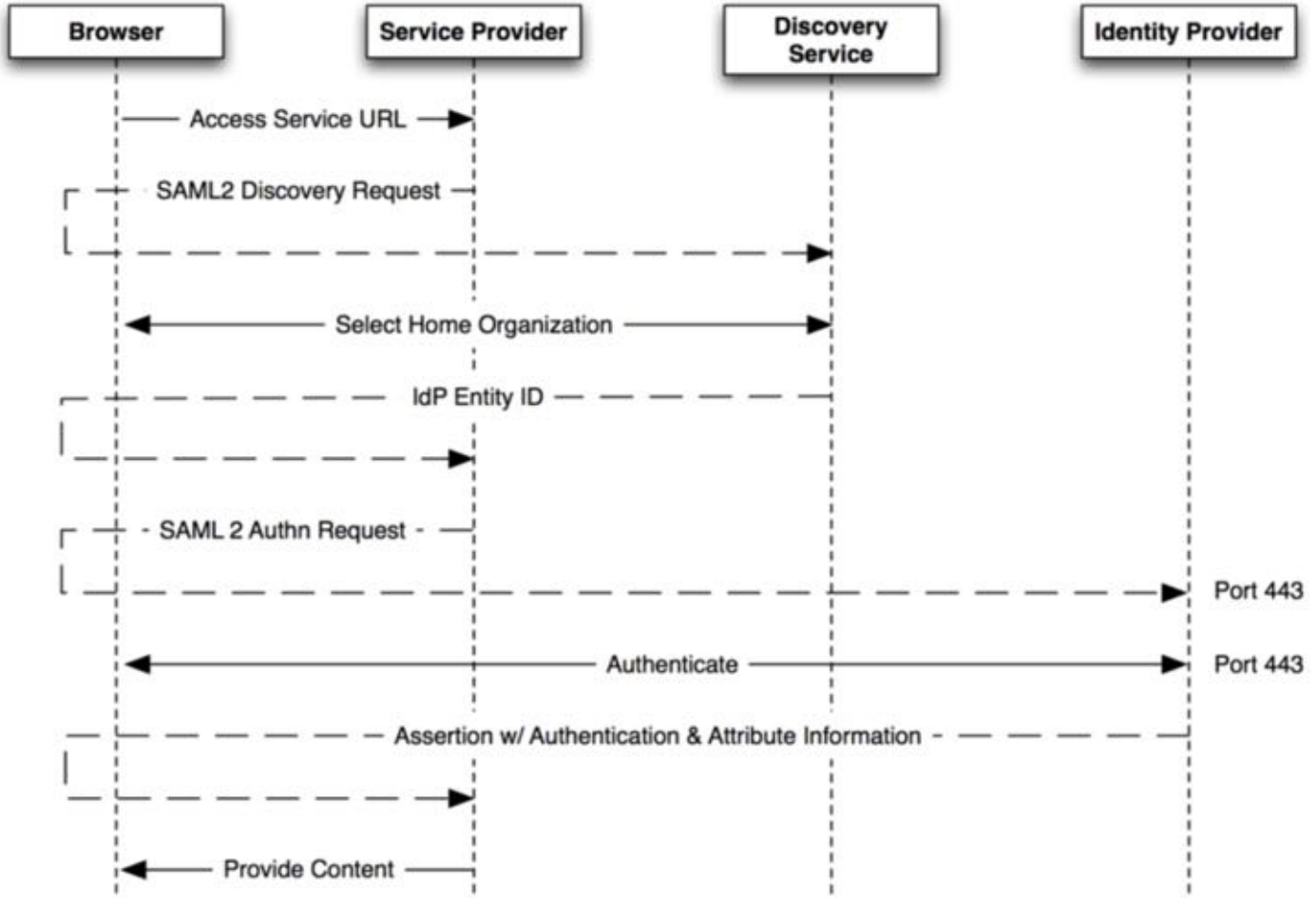
SAML Assertion + Attribute Statement, decrypted (Base64 decoded)

```
<saml:Assertion ...>
  <saml:Issuer ...>
    https://aai-demo-idp.switch.ch/idp/shibboleth
  </saml:Issuer>
  <saml:Subject ...>
    <saml:NameID ...>
      _e7b68a04488f715cda642fbdd90099f5
    </saml:NameID>
    [...]
  </saml:Subject>
  [...]
  <saml:AuthnStatement ...
      AuthnInstant="2008-02-27T12:20:06.991Z"
      SessionIndex="4m2ETlKYtvbNEmBzVNo3UHLuKSdo3HqTUqAmeZiar94="
      SessionNotOnOrAfter="2008-02-27T12:50:06.991Z">
    [...]
  </saml:AuthnStatement>
  <saml:AttributeStatement ...>
    [...] (Attributes)
  </saml:AttributeStatement>
</saml:Assertion>
```

Accessing multiple SPs



SAML


Browser
Service Provider
Discovery Service
Identity Provider
Access Service URL
SAML2 Discovery Request
Select Home Organization
IdP Entity ID
SAML 2 Authn Request
Port 443
Authenticate
Port 443
Assertion w/ Authentication & Attribute Information
Provide Content

Shibboleth

Technically it's a project group, like Apache or Eclipse, whose core team maintains a set of software components

Most people think of it as the set of software components OpenSAML C++ and Java libraries

- Shibboleth Identity Provider (IdP)
- Shibboleth Service Provider (SP)
- Shibboleth Discovery Service (DS)

Taken together these components make up a federated identity management (FIM) platform.

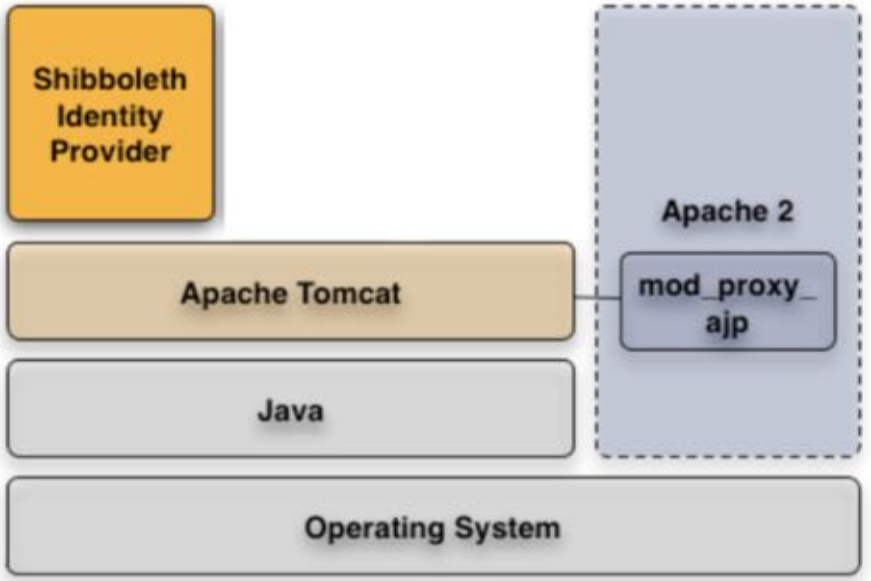
You might also think of Shibboleth as a multi-protocol platform that enforces a consistent set of policies.

The Shibboleth software is widely used in the research and education environment

Shibboleth IDP

A Java Servlet web application

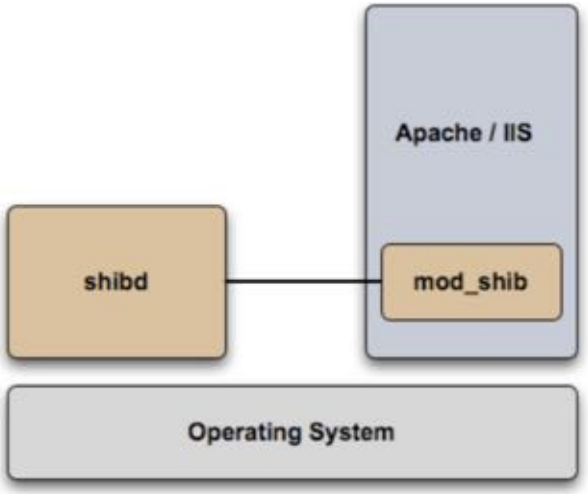
Connects to **existing** authentication and user data systems
Provides information about how a user has been authenticated
Provides user identity information from the data source

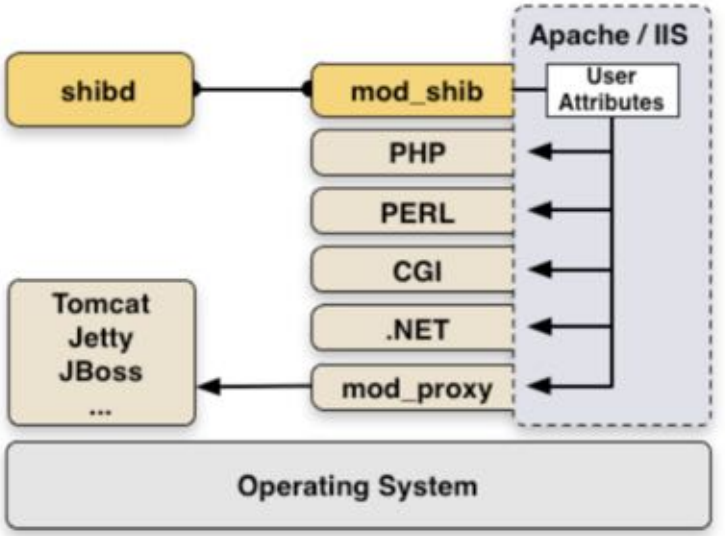


Shibboleth SP

Basically consists of,
- mod_shib: C++ web server (Apache/IIS) module
- shibd: C++ daemon - keeps state when web server processes die

- Used typically to initiates the request for authentication and attributes
- Processes incoming authentication and attribute information
- Optionally evaluates content access control rules





Resource Registry

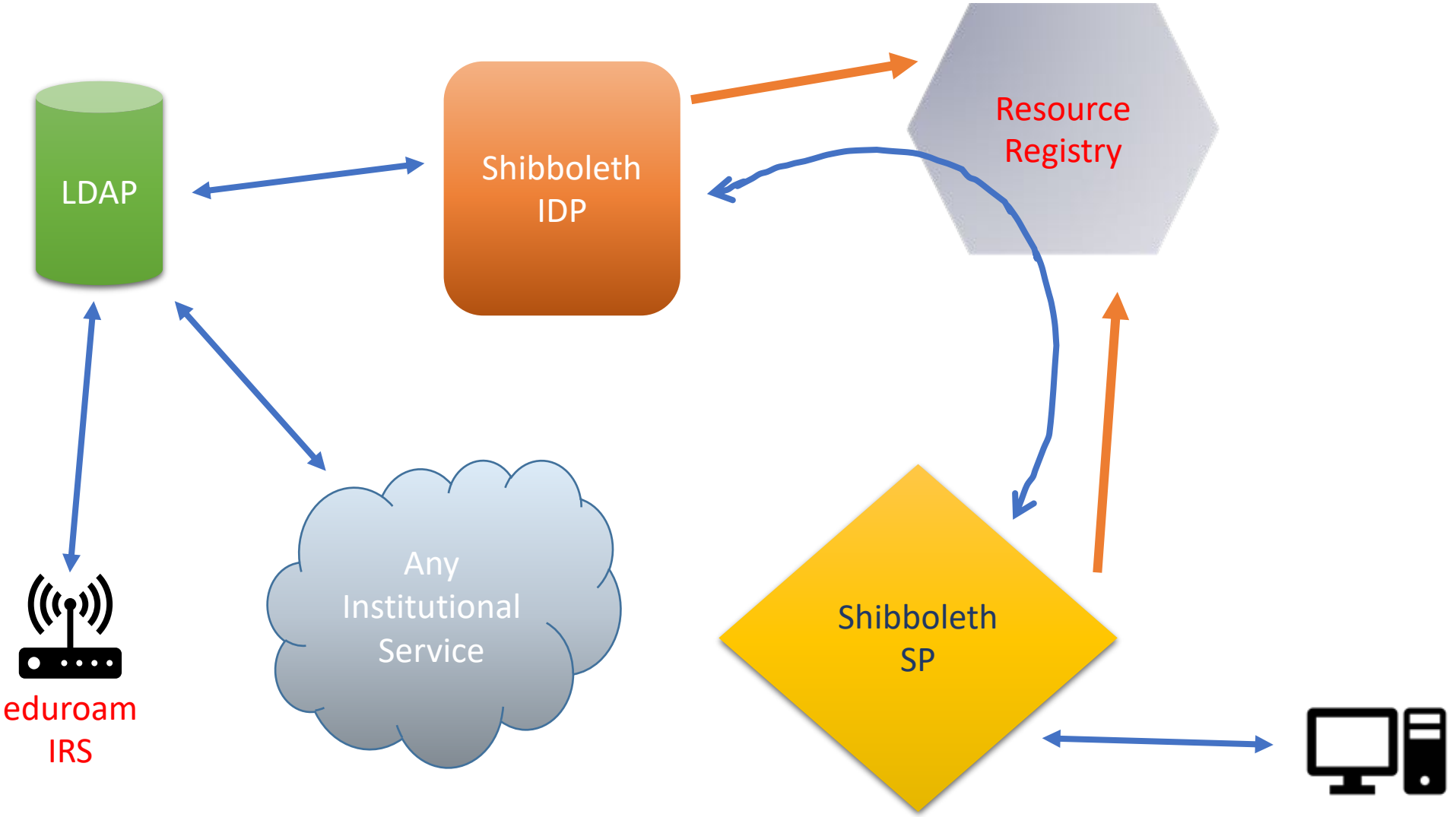
The “Resource Registry”, a central registry in the federation, generates the metadata and makes all IdPs and SPs know each other

The Resource Registry knows all IdPs, SPs, supported protocols, service locations and signing/encryption keys

A web based tool managed by the federation operator

LEARN Test Federation Metadata: https://fr-training.ac.lk/signed-metadata.xml

Proposed Federation dataflow at LEARN



Questions

Thank You

LEARN

Email: