Shibboleth

SWITCH
Serving Swiss Universities

Shibboleth Install Fest: Hands-on Technical Workshop

Handouts

29-30 August, 2012
Basel, Switzerland

Table of Contents

Federated Identity Management

SWITCH
Serving Swiss Universities

SWITCHaai Team
aai@switch.ch

Agenda

- What is Federated Identity Management?
- What is a Federation?
- The SWITCHaai Federation
- Interfederation

Evolution of Identity Management

- Stone Age
  Application maintains unique credential 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

Federated Identity

- Current mechanisms assume applications are within the same administrative domain
  - Adding a user from outside means creating an account within your IdM system. This could result in the new user having access to more than just the intended application.

- Federated Identity Management (FIM) securely shares information managed at a users home organization with remote services.
  - Within FIM systems it doesn't matter if the service is in your administrative domain or another. It's all handled the same.

Federated Identity

- In Federated Identity Management:
  - Identity Providers (IdP) publish authentication and identity information about users
  - Service Providers (SP) consume this information and make it available to an application
  - An IdP or SP is generically known as an **entity**
- The first principle within federated identity management is the active protection of user information
  - Protect the user’s credentials
    - only the IdP ever handles the credential
  - Protect the user’s identity information, including identifier
    - customized set of information released to each SP

What does it do for me?

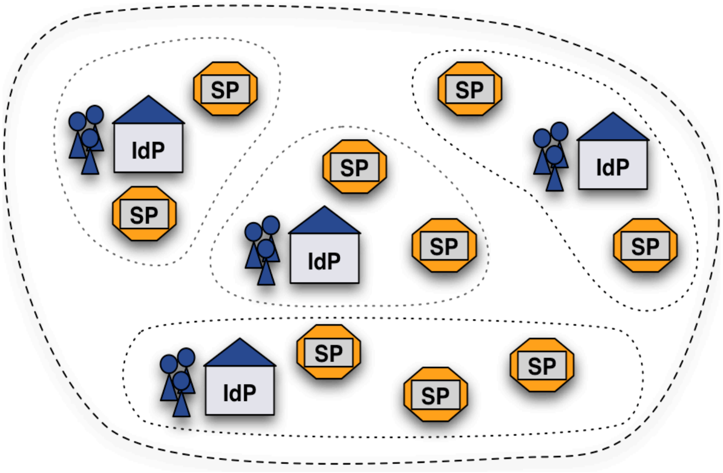
- Reduces work
  - Authentication-related calls to Penn State University’s helpdesk dropped by 85% after they installed Shibboleth
- Provides current data
  - Studies of applications that maintain user data show that the majority of data is out of date. Are you “protecting” your app with stale data?
- Insulation from service compromises
  - In FIM 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.

Some other gains

- Users generally find the resulting single sign-on experience to be nicer than logging in numerous times.
- Usability-focused individuals like that the authentication process is consistent regardless of the service accessed.
- A properly maintained federation drastically simplifies the process of integrating new services.

What is a Federation?

- A group of organizations running IdPs and SPs that agree on a common set of rules and standards
  - It's a label for people to talk about such a collection of organizations
  - An organization may belong to more than one federation at a time
- The grouping can be on a regional level (e.g. SWITCHaai) or on a smaller scale (e.g. large campus)
- IdPs and SPs 'know' nothing about federations



What are these rules of which you speak?

- Technical Interoperability
  - Supported protocols
  - User authentication mechanisms
  - User attribute specifications
  - Accepted X.509 certificates
- Legal Interoperability
  - Membership agreement/contract
  - Federation operation policies
  - Requirements on identity management practices
- Others
  - Common/best operational practices http://switch.ch/aai/bcp

What does a Federation do?

- At a minimum a federation maintains the list of which IdPs and SPs are in the federation
- Most federations also
  - define agreements, rules, and policies
  - provide some user support (documentation, email list, etc.)
  - operate a central discovery service and test infrastructure
- Some federations
  - provide self-service tools for managing IdP and SP data
  - install IdPs and SPs for members
  - provide application integration support
  - host or help with outsourced IdPs
  - provide tools for managing “guest” users
  - develop custom tools for the community

Federation Metadata

11

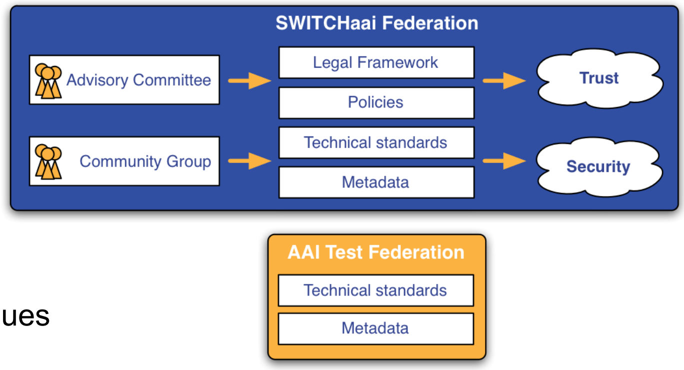
- An XML document that describes every federation entity
- Contains
  - Unique identifier for each entity known as the entityID
  - Endpoints where each entity can be contacted
  - Certificates used for signing and encrypting data
- May contain
  - Organization and person contact information
  - Information about which attributes an SP wants/needs
- Metadata is usually distributed by a public HTTP URL
  - The metadata should be digitally signed
  - Bilateral metadata exchange scales very badly
- Metadata must be kept up to date so that
  - New entities can work with existing ones
  - Old, or revoked, entities are blocked

http://switch.ch/aai/metadata

SWITCHaai: An Example Federation (1)

12

- SWITCH consults with two bodies
  - Advisory Committee deals with policies and legal framework
  - Community Group deals with technical/operational issues



SWITCHaai Federation

Advisory Committee → Legal Framework, Policies → Trust

Community Group → Technical standards, Metadata → Security

AAI Test Federation

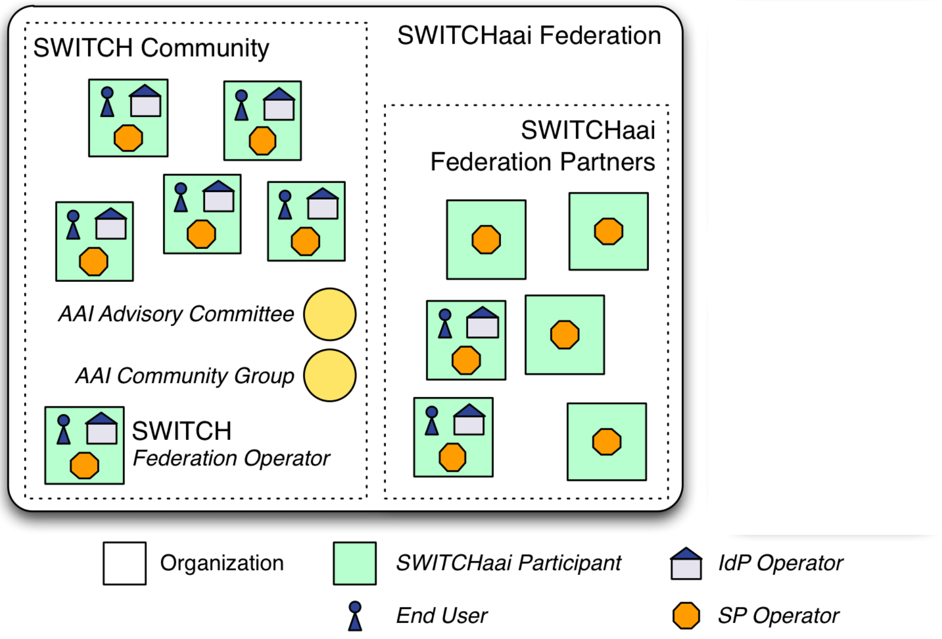
Technical standards

Metadata

- Two classes of SWITCHaai Participants
  - SWITCH Community
    - Organization fits the definition from the SWITCH Service Regulations
  - Federation Partner
    - Organization sponsored by a SWITCHaai Participant from the SWITCH Community

http://switch.ch/aai/about/federation/

SWITCHaai: An Example Federation (2)

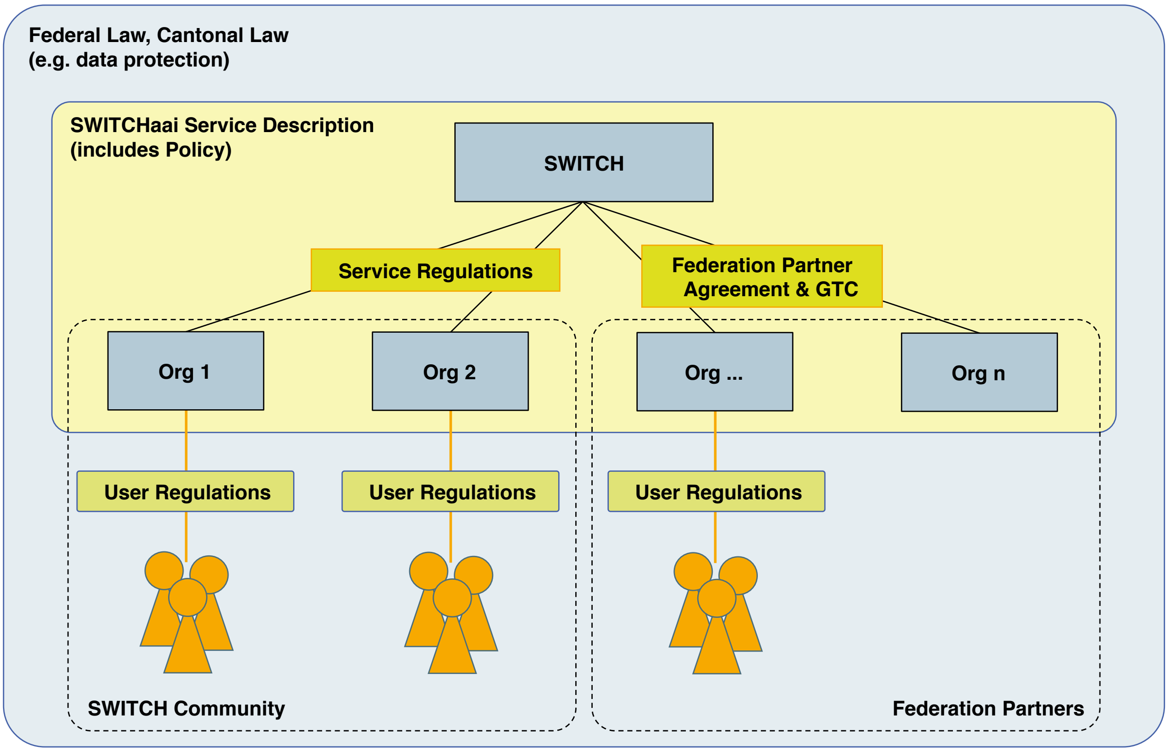


- SWITCH operates the SWITCHaai Federation
- AAI is a Basic Service for the SWITCH Community

SWITCHaai: Rules, Policies, & Agreements

- SWITCHaai Service Description (includes the Policy)
  concepts and rules for all entities in the federation
- Federation Partner Agreement
  legal contract between SWITCH and federation partner
- Certificate Acceptance Policy
  policy certificates accepted by the federation
- AAI Attribute Specification
  minimum set of core and optional attributes supported by federation entities

SWITCHaai: The Legal Framework



Federal Law, Cantonal Law
(e.g. data protection)

SWITCHaai Service Description
(includes Policy)

SWITCH

Service Regulations

Federation Partner Agreement & GTC

Org 1

Org 2

Org ...

Org n

User Regulations

User Regulations

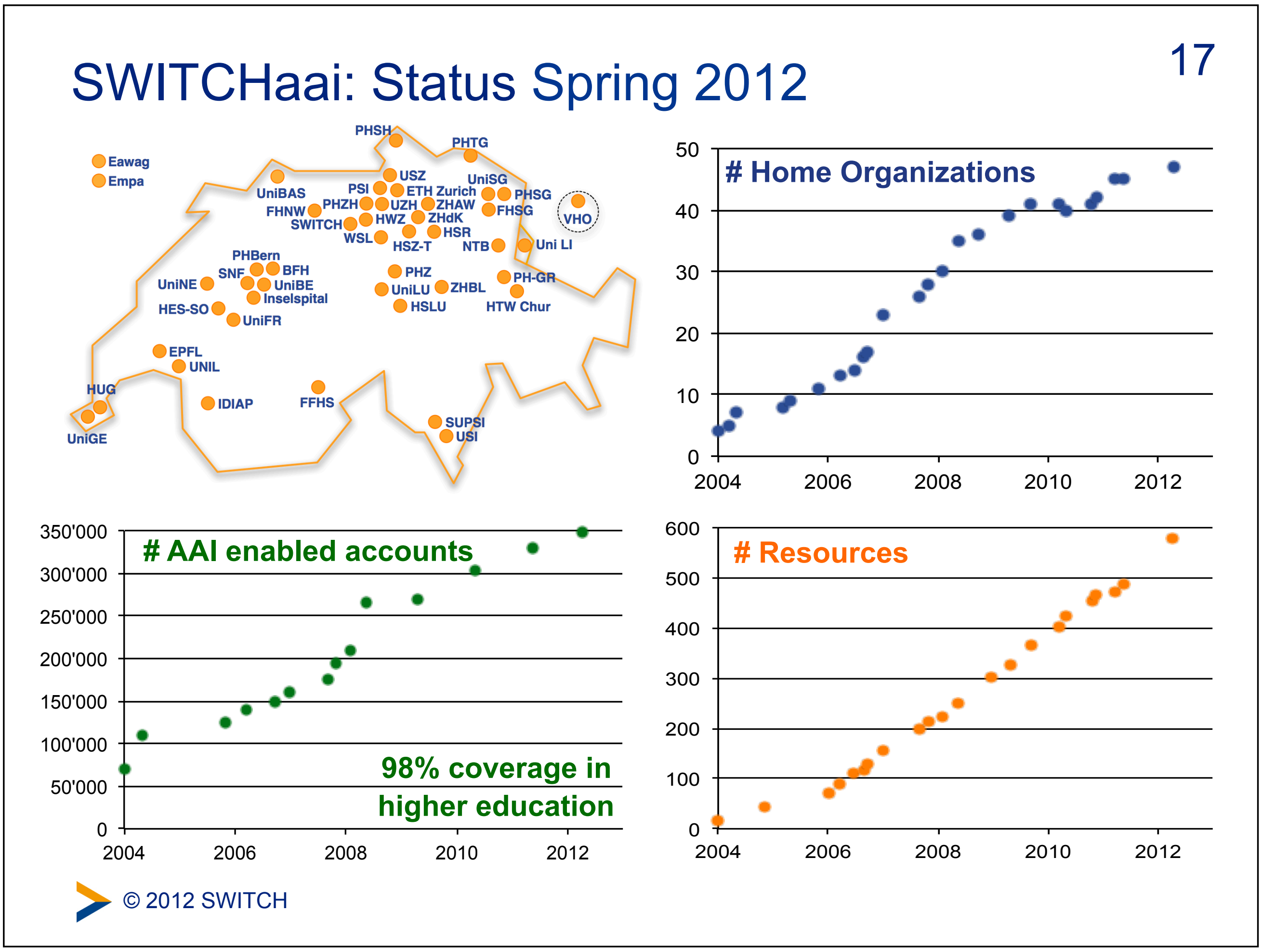
User Regulations

SWITCH Community

Federation Partners

SWITCHaai: Services Provided

- Rules, policies and agreements
- Documentation: installation/migrations guides, HowTos
- Call-in helpdesk and support mailing list
- Centralized Services
  - Discovery Service
  - Resource Registry (metadata management)
  - Virtual Home Organization (VHO)
  - Attribute Viewer
  - Group Management Tool
- uApprove Shibboleth IdP plugin
- Test federation
- Some application integration support
- Training

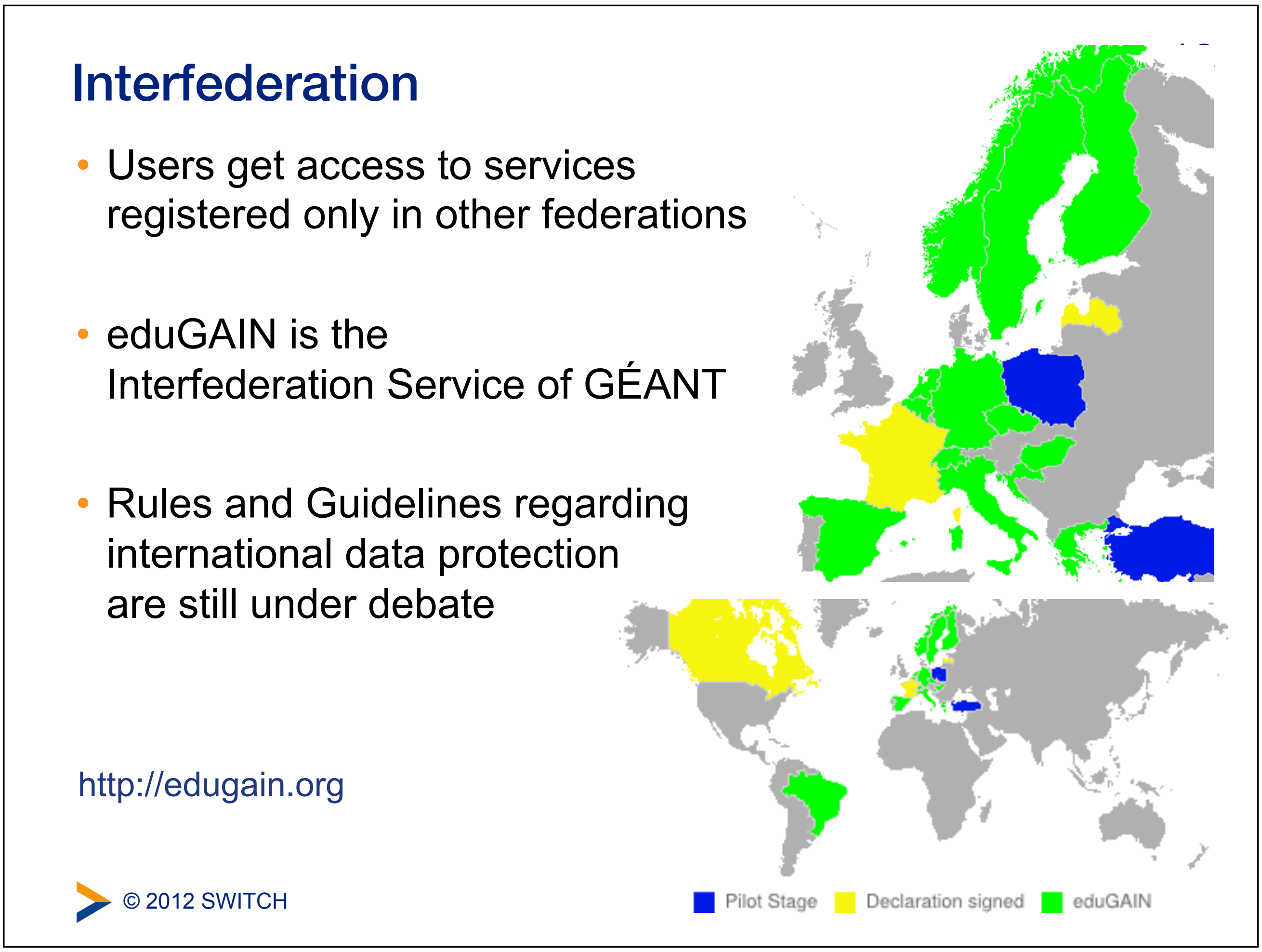


SWITCHaai: Status Spring 2012

17

98% coverage in higher education

© 2012 SWITCH



Interfederation

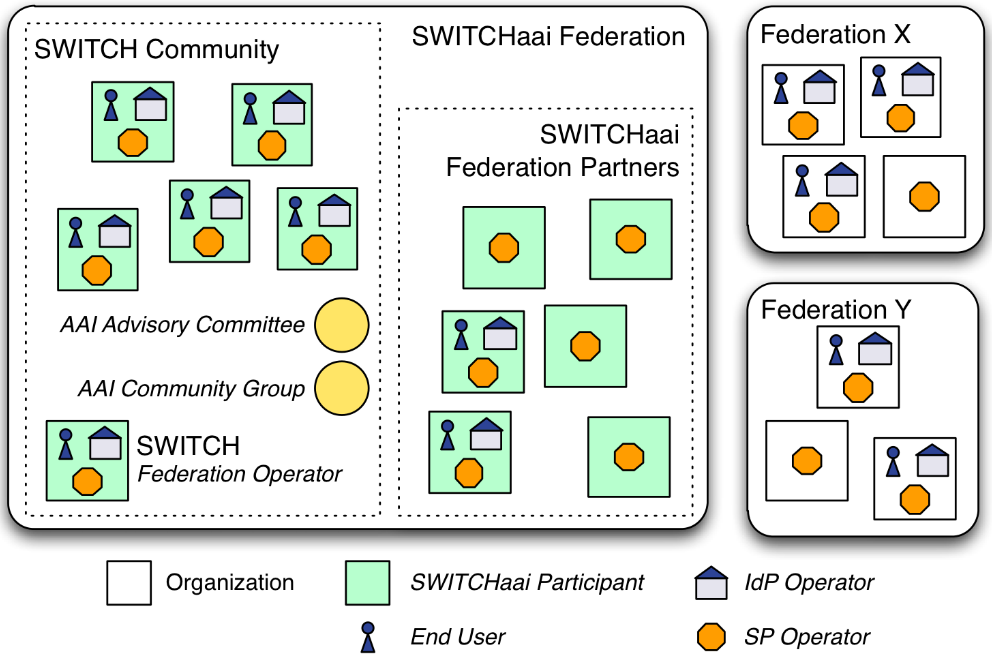
- Users get access to services registered only in other federations
- eduGAIN is the Interfederation Service of GÉANT
- Rules and Guidelines regarding international data protection are still under debate

http://edugain.org

🟦 Pilot Stage 🟨 Declaration signed 🟩 eduGAIN

© 2012 SWITCH

Interfederation (2)



http://switch.ch/aai/interfederation

AAI Login Demo

SWITCH
Serving Swiss Universities

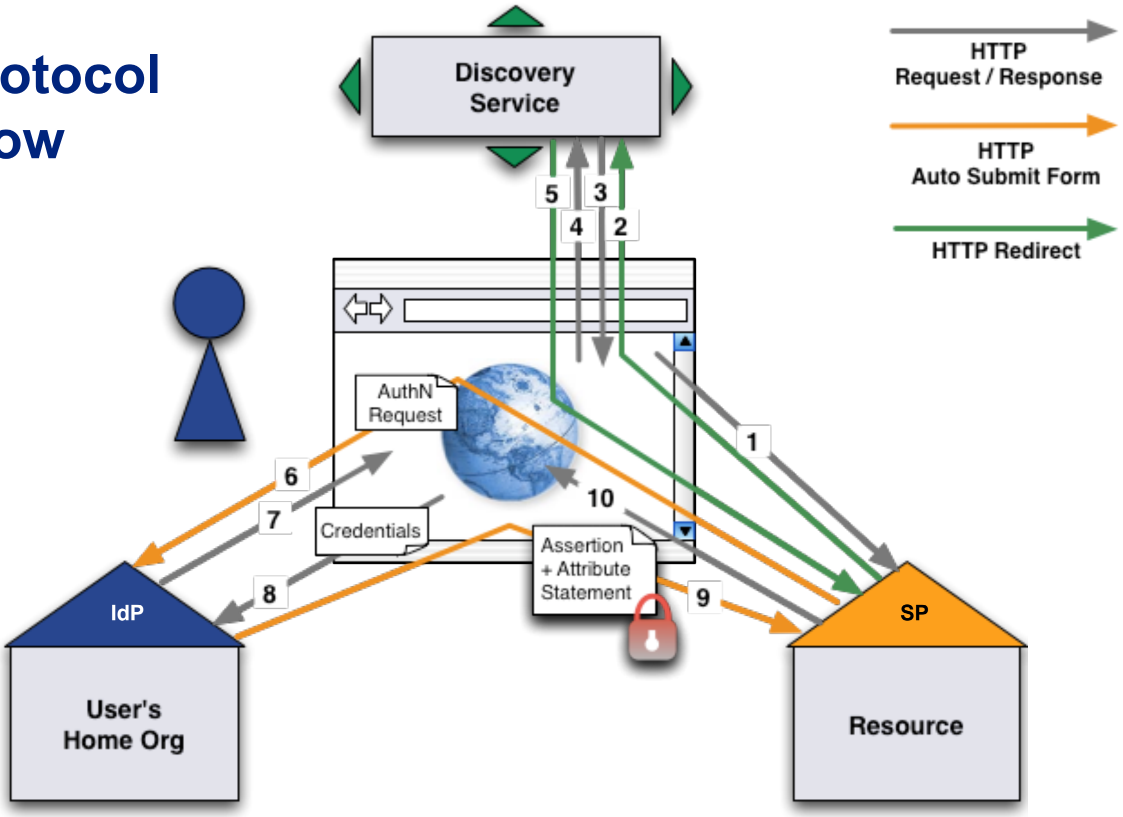
SWITCHaai Team
aai@switch.ch

Basel, 29. August 2012

Agenda

- Illustration of protocol flow
  SAML2, Web Browser SSO
- Live demonstration

Protocol Flow

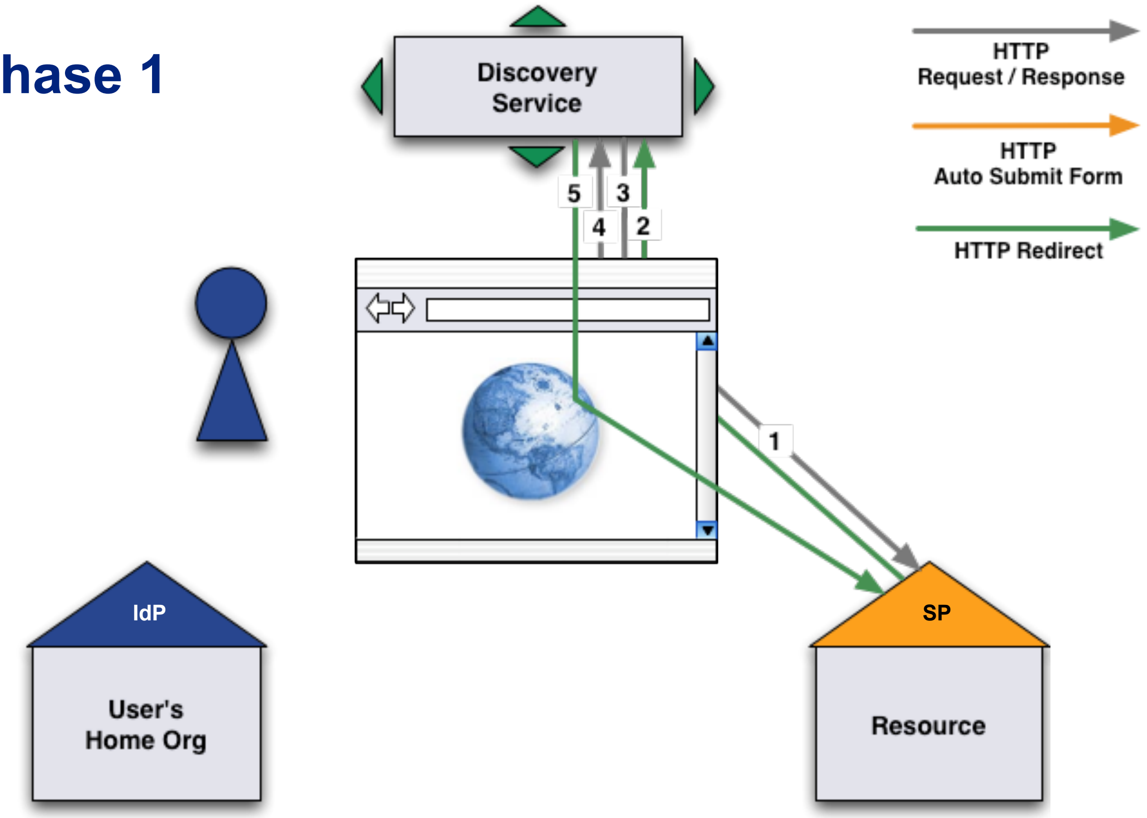


http://www.switch.ch/aai/demo/

Phase 1

First access to the Service Provider and Identity Provider discovery

Phase 1



First access to the Service Provider and Identity Provider discovery

① The user opens a web browser and accesses the Service Provider.

② The user is redirected to the Discovery Service by the Service Provider. Consequently, the web browser sends a new request to the Discovery Service.

③ The Discovery Service answers with the web page that allows the user to select an Identity Provider.

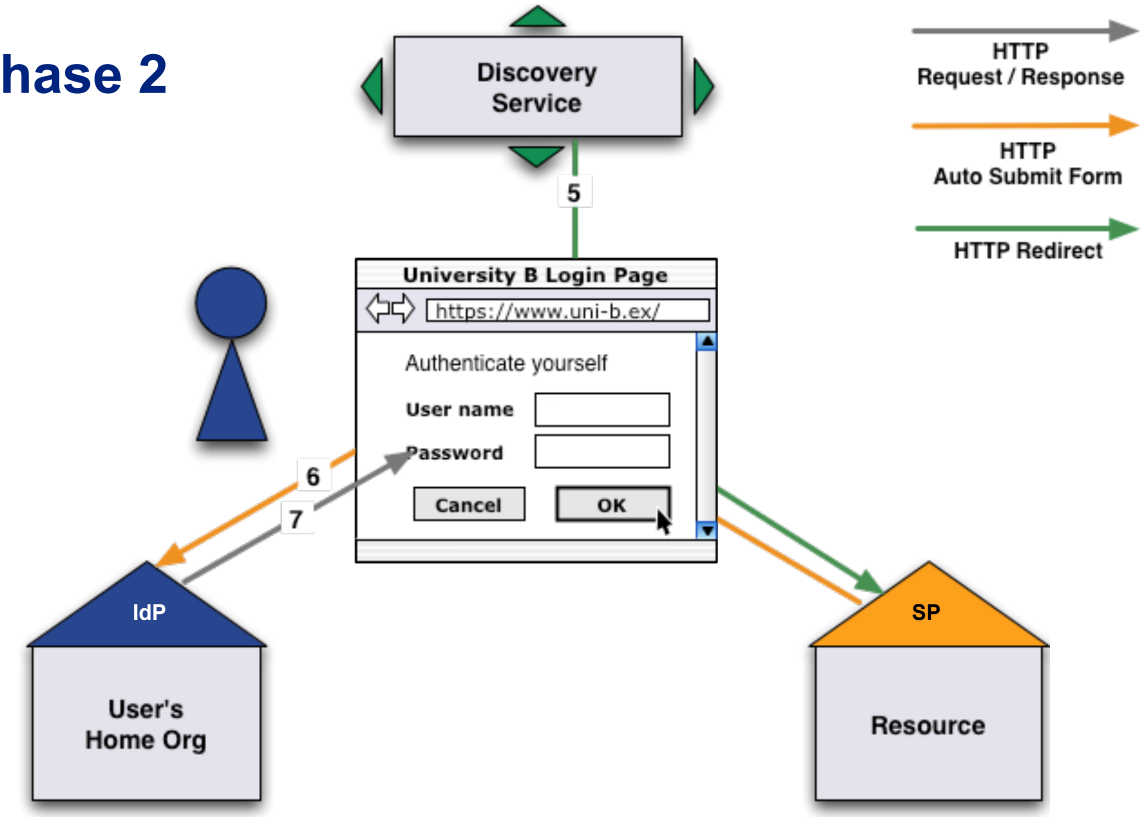
④ On the Discovery Service page, the user submits the Identity Provider selection.

⑤ The Discovery Service sends a redirect to the SP return destination, including the IdP selection.

Phase 2

Session initiation and authentication request

Phase 2



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>
```

Session initiation and authentication request

⑤ The browser is redirected to the Service Provider by the Discovery Service.

⑥ The session initiator of the Service Provider creates an authentication request and returns it within an auto-submit-post-form to the browser.

The browser posts the SAML AuthN Request automatically to the Identity Provider using JavaScript.

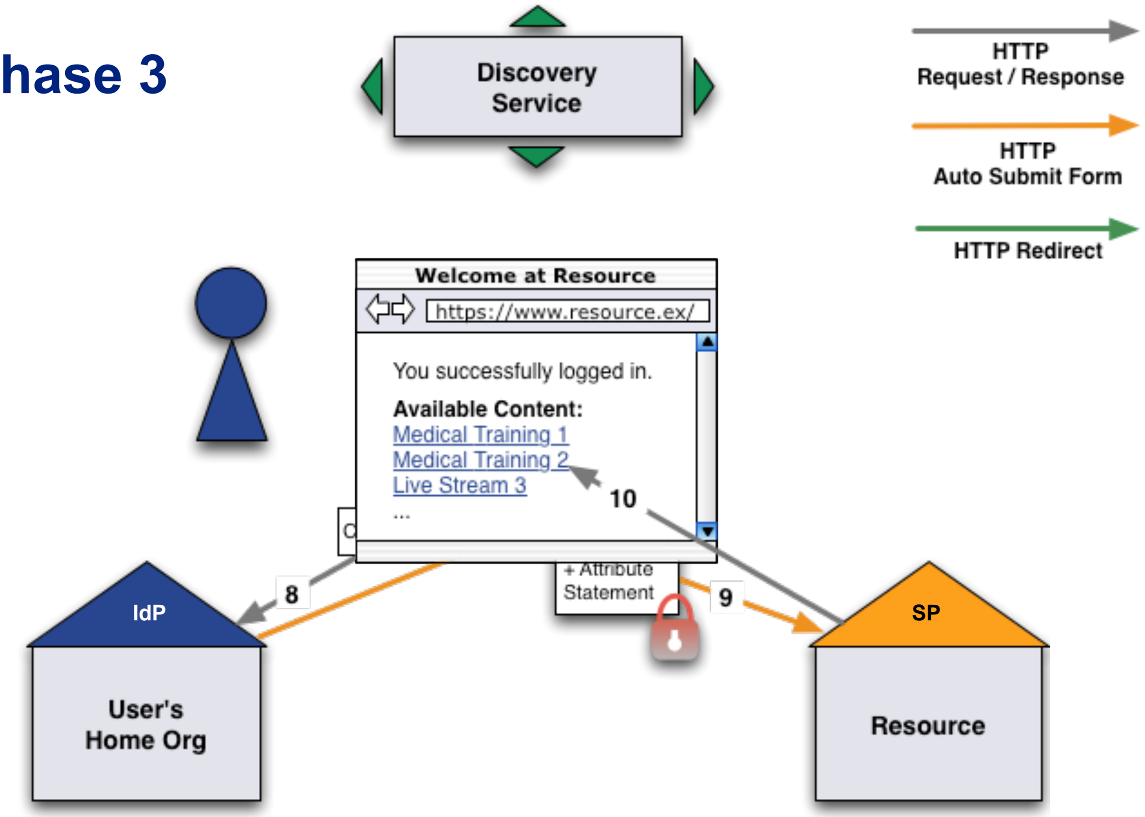
Session initiation and authentication request

⑦ The Identity Provider checks the authentication request. Because the user hasn't yet been authenticated, the Identity Provider sends a redirect to the appropriate login page (usually: Username/Password).

Phase 3

Authentication, attribute statement and access

Phase 3



SAML Assertion + Attribute Statement

Plain HTML

```
<html xml:lang="en">
  <body onload="document.forms[0].submit()">
    <form action="https://aai-demo.switch.ch/Shibboleth.sso/SAML2/POST" method="post">
      <div>
        <input type="hidden" name="RelayState" value="ss:mem:23e3a3b1268acd89dc226bb1ce0d0c6ba7ecf773"/>
        <input type="hidden" name="SAMLResponse"
            value="PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4KPHNhbWxwO8...
            ...vbj0iW1scDVlc+PC9zYW1scRGLsTgiPz4KPlc3U+"/>
      </div>
    </form>
  </body>
</html>
```

SAML Assertion + Attribute Statement

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>
```

Authentication, attribute statement and access

⑧ The user types his username and password credentials and submits them to the Identity Provider.

⑨ The Identity Provider verifies the credentials. If authentication succeeds, the IdP issues an assertion for the SP and returns it within an auto-submit-post-form to the browser.

The web browser immediately posts the SAML Assertion to the Service Provider with use of Javascript automatically.

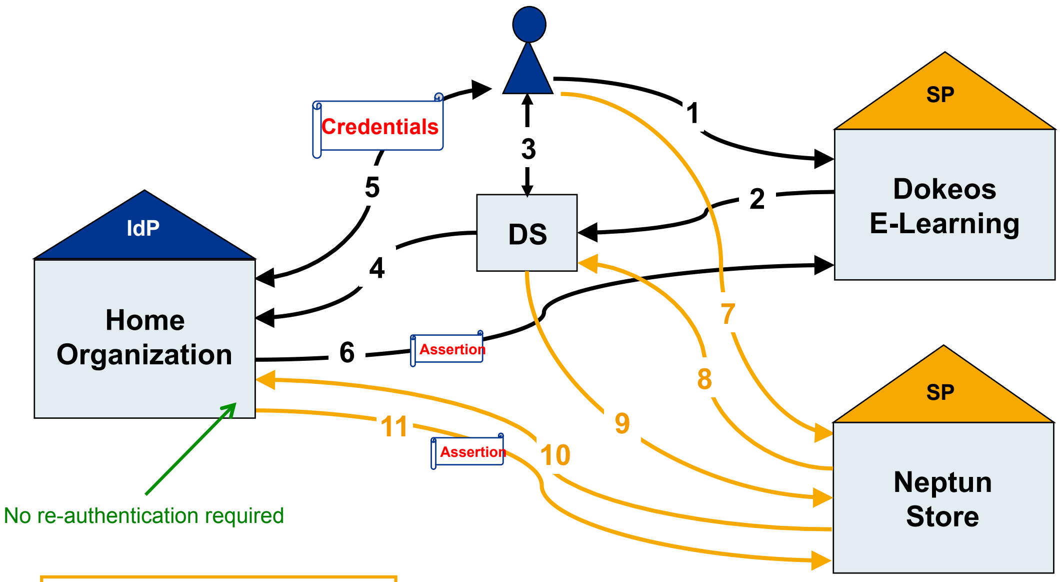
The Service Provider processes the SAML assertion including the authentication and attribute statements.

Authentication, attribute statement and access

⑩ Finally, the Service Provider starts a new session for the user and redirects the user to the previously requested resource.

Now, the user is authenticated and gets access to the resource depending on the access rules configured for the resource.

Accessing multiple SPs



IdP: Identity Provider
SP: Service Provider
DS: Discovery Service

Live Demo

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

Links

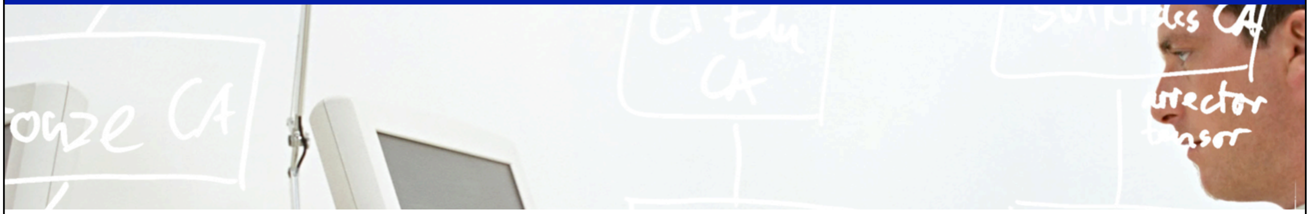
The AAI Demo shows how AAI works.

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

The AAI Attribute Viewer shows which attributes are released by an Identity Provider.

https://aai-viewer.switch.ch/

AAI Attributes



SWITCH

Serving Swiss Universities

Beatrice Huber

bea.huber@switch.ch

Basel, 29.August 2012

Agenda

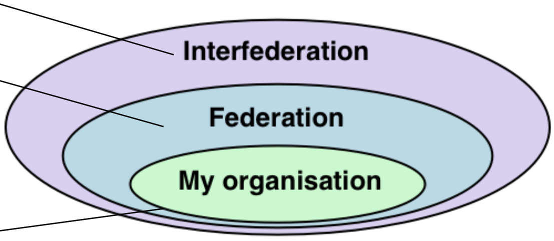
- attribute usage
- attribute scope
- user identifier attributes

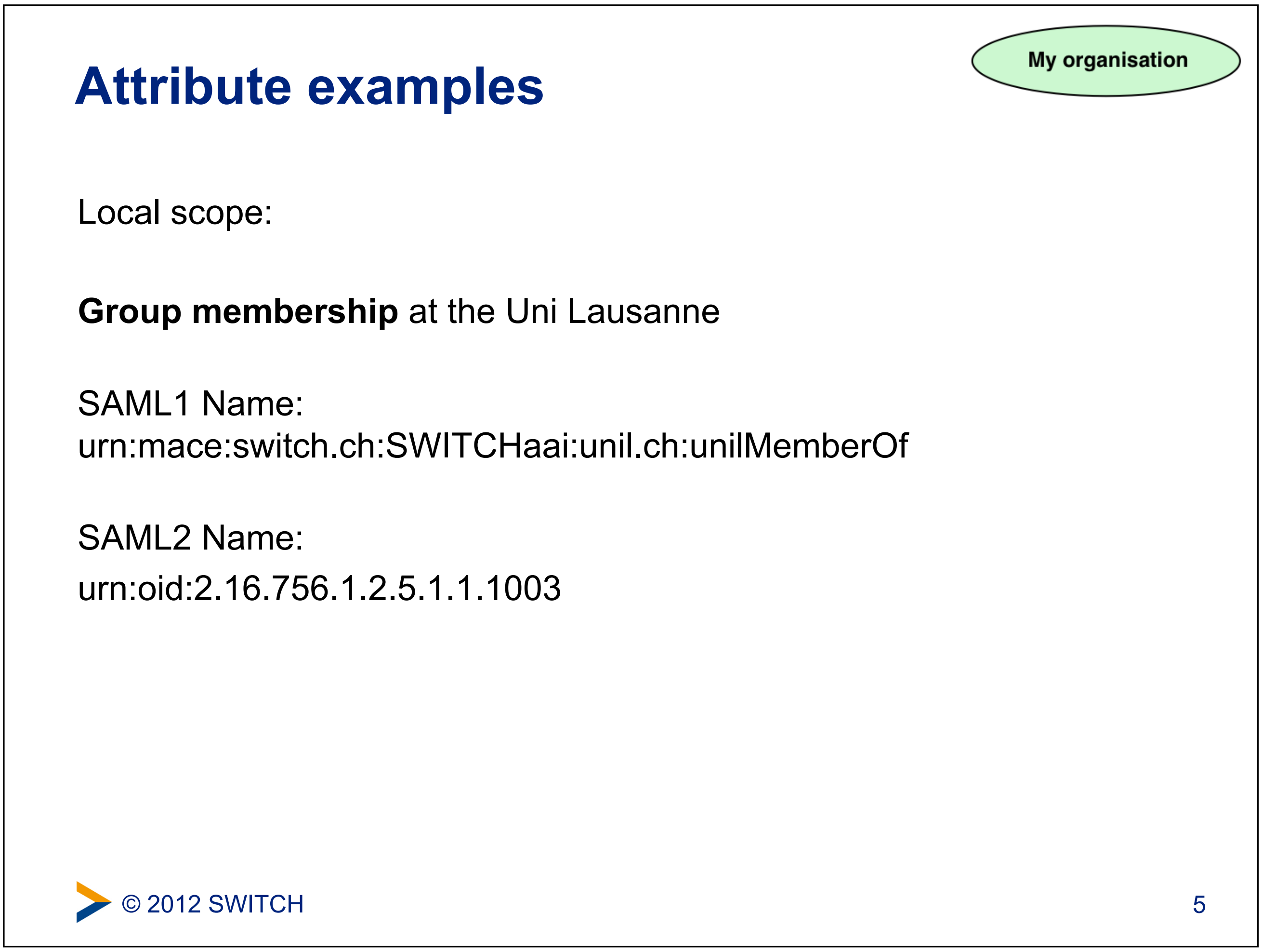
Attribute usage

- identification
- authorisation
  - Access decision based on attribute values
  - individual or role based access control
- additional user information
  - Portal personalization e.g. preferred language
- accounting

Attribute scopes

- Standardized
- SWITCHaai
  - Core
  - Other
- Local





My organisation

Attribute examples

Local scope:

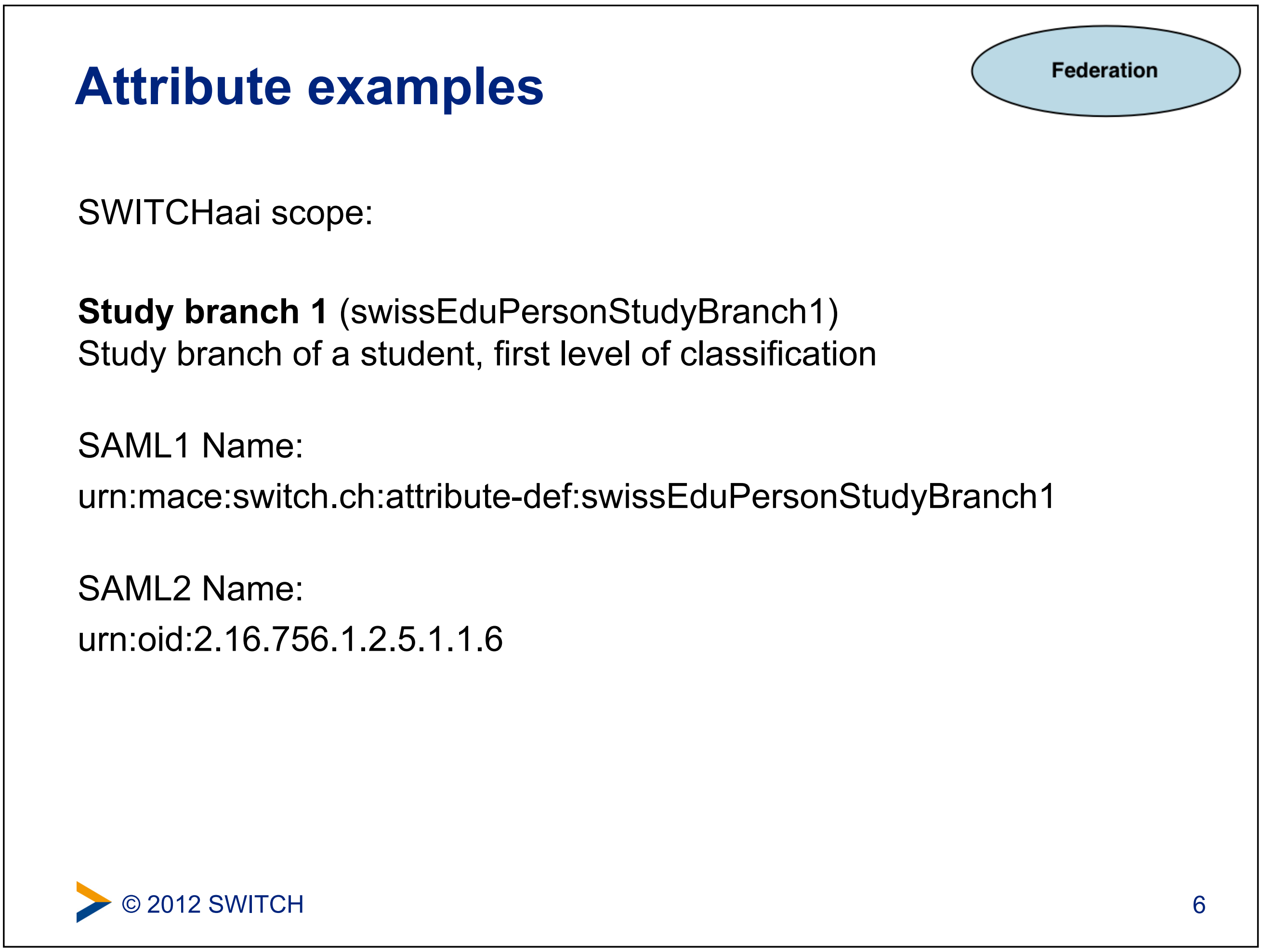
Group membership at the Uni Lausanne

SAML1 Name:
urn:mace:switch.ch:SWITCHaai:unil.ch:unilMemberOf

SAML2 Name:
urn:oid:2.16.756.1.2.5.1.1.1003

© 2012 SWITCH

5



Federation

Attribute examples

SWITCHaai scope:

Study branch 1 (swissEduPersonStudyBranch1)
Study branch of a student, first level of classification

SAML1 Name:
urn:mace:switch.ch:attribute-def:swissEduPersonStudyBranch1

SAML2 Name:
urn:oid:2.16.756.1.2.5.1.1.6

© 2012 SWITCH

6

SWITCHaai Attributes

Federation

Personal
Unique Identifier
Surname
Given name
E-mail
Persistent ID
User ID
Matriculation number
Employee number
Address(es)
Phone number(s)
Preferred language
Date of birth
Card UID

Group Membership
Home Organization Name
Home Organization Type
Affiliation

Study branch
Study level
Staff category
Group membership
Organization Path
Organizational Unit Path

Implementation of Attributes

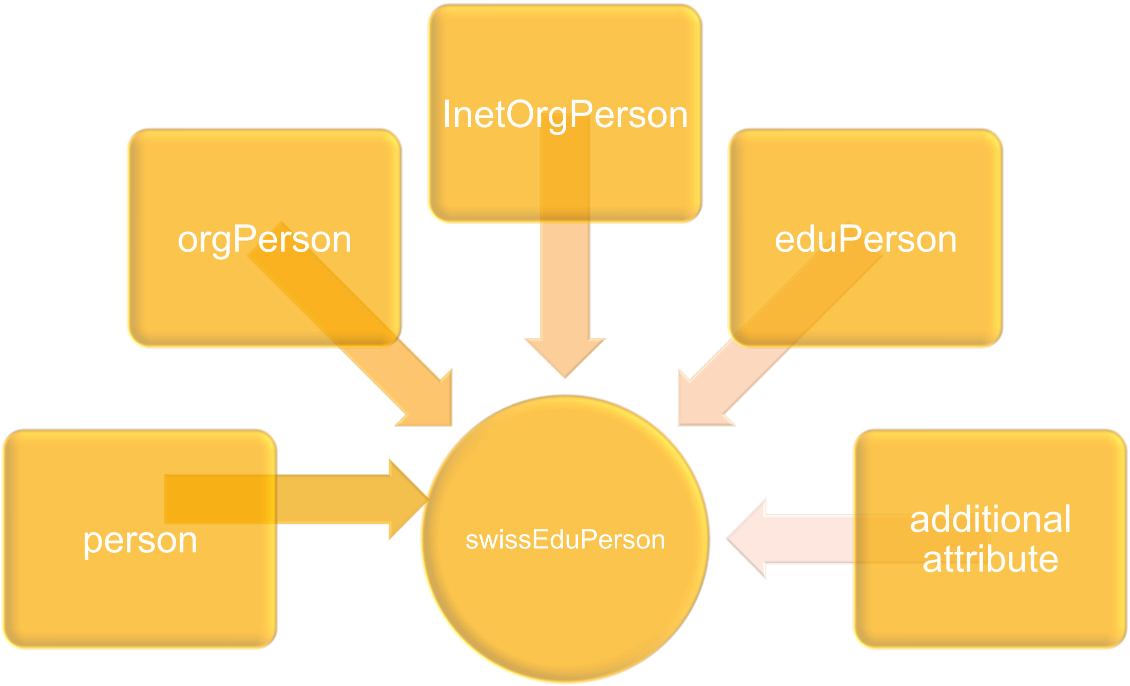
- Core Attributes
- Other Attributes

AAI Attribute Specification: http://switch.ch/aai/attributes

© 2012 SWITCH

swissEduPerson definition

Federation



InetOrgPerson

orgPerson

eduPerson

person

swissEduPerson

additional attribute

© 2012 SWITCH

Standardized Attributes

Interfederation

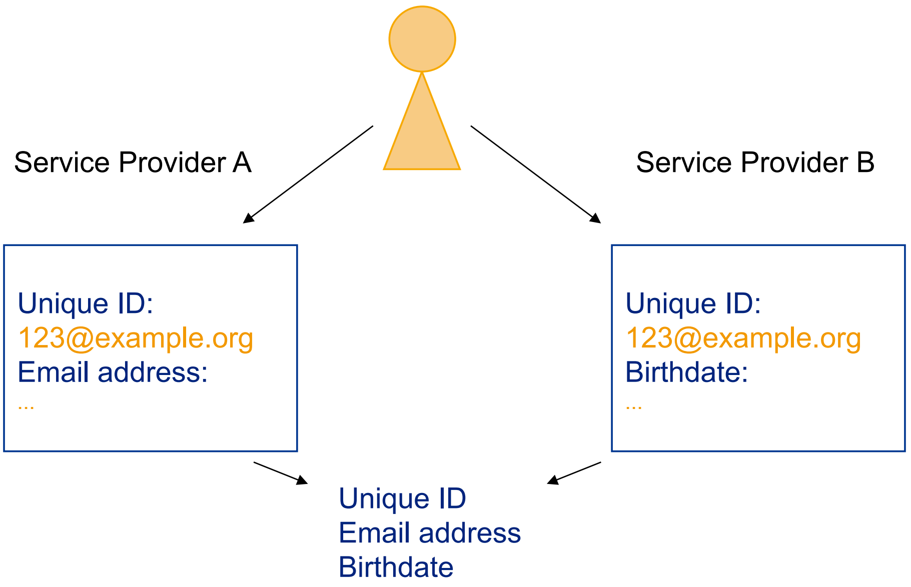
- Relevant for communication with entities from other federation via eduGAIN (or on bilateral basis)

Friendly name	Defined in	Example
displayName	eduPerson	Beatrice Huber
common name (cn)	eduPerson	Beatrice Huber
mail	eduPerson	bea.huber@switch.ch
eduPersonAffiliation eduPersonScopedAffiliation	eduPerson	staff staff@switch.ch
schacHomeOrganization	SCHAC	switch.ch
schacHomeOrganizationType	SCHAC	urn:mace:terena.org:schac:homeOrganizationType:int:NREN

User identifier attributes

Federation

- Using account linking, the data is worth even more.



Service Provider A

Service Provider B

Unique ID:
123@example.org
Email address:
…

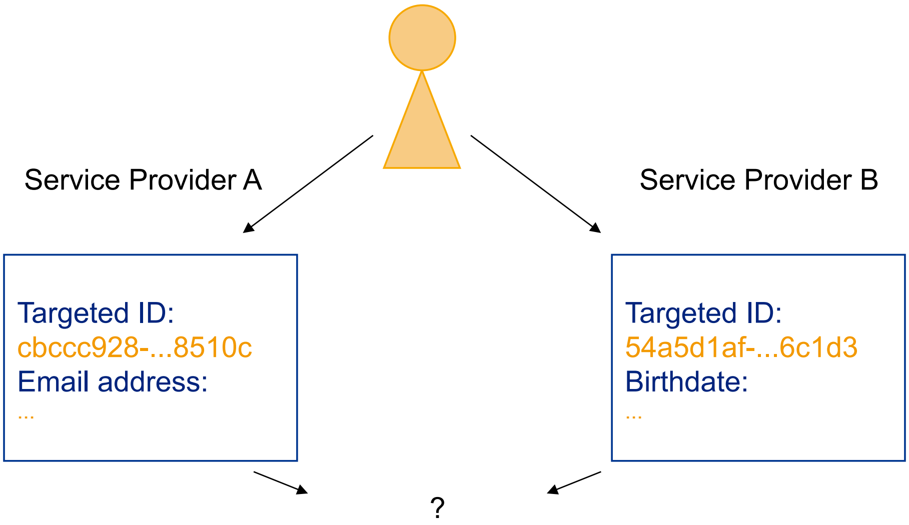
Unique ID:
123@example.org
Birthdate:
…

Unique ID
Email address
Birthdate

persistent ID (eduPersonTargetedID)

Example persistent ID

```
https://idp.example.org/idp/shibboleth!
 https://sp.example.org/shibboleth!
 f74698d6-854c-480c-b566-702006318cc3c
```



Service Provider A

Targeted ID:
cbccc928-...8510c
Email address:
...

Service Provider B

Targeted ID:
54a5d1af-...6c1d3
Birthdate:
...

?

Email vs persistent ID vs Unique ID

Properties	Email	Unique ID	persistent ID
scoped	✓	✓	✓
persistent	✓	✓	✓
opaque	×	✓	✓
non-reusable	×	✓	✓
targeted	×	×	✓
revocable	×	×	✓

Introduction to Shibboleth

SWITCH

Serving Swiss Universities

SWITCHaai Team
aai@switch.ch

Agenda

- What is Shibboleth?
- IdP/SP Communication
- Shibboleth 1 & 2
- Support Resources

Shibboleth – Origin and Consortium

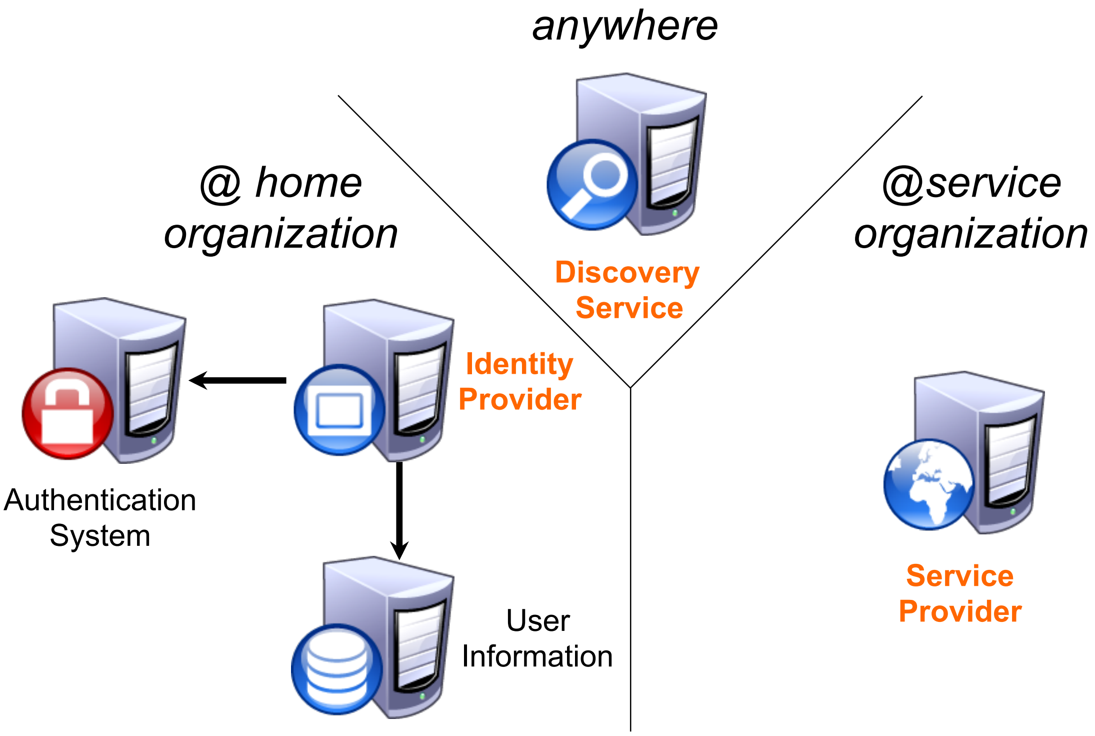
- The Origin
  - Internet2 in the US launched the open source project
- The name
  - Word **Shibboleth** was used to identify members of a group
- The standard
  - Based on Security Assertion Markup Language (SAML)
- The Consortium
  - The new home for Shibboleth development
  - collect financial contributions from deployers worldwide

http://shibboleth.net

What is Shibboleth?

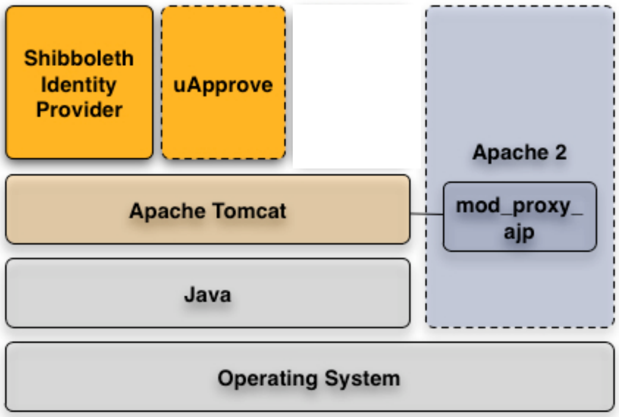
- Technically it's a project group, like Apache or Eclipse, whose core team maintains a set of software components
- Most people think of it as the set of software components
  - OpenSAML C++ and Java libraries
  - Shibboleth Identity Provider (IdP)
  - Shibboleth Service Provider (SP)
  - Shibboleth Discovery Service (DS)
  - Shibboleth Metadata Aggregator (MA)
- 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 Components



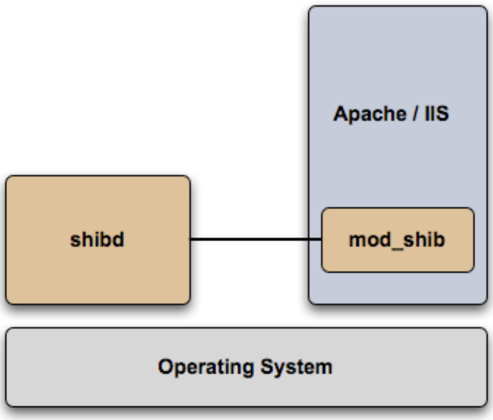
Shibboleth Components: Identity Provider

- What is it?
  - A Java Servlet (2.4) web application
- What does it do?
  - 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



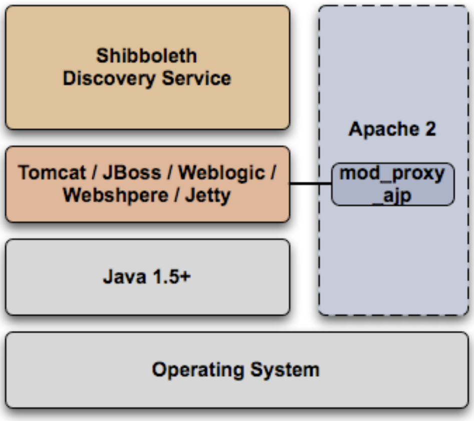
Shibboleth Components: Service Provider

- What is it?
  - mod_shib: A C++ web server (Apache/IIS) module
  - shibd: A C++ daemon - keeps state when web server processes die
- What does it do?
  - Optionally initiates the request for authentication and attributes
  - Processes incoming authentication and attribute information
  - Optionally evaluates content access control rules



Shibboleth Components: Discovery Service

- What is it?
  - A Java Servlet (2.4) web application
- What does it do?
  - Asks the user to select their home organization from a list



See also an Alternative Implementation: http://switch.ch/aai/wayf

Terminology (1)

- SAML - Security Assertion Markup Language
  The standard describing the XML messages sent back and forth by the Shibboleth components (two versions: 1.1, 2.0)
- Profile - Standard describing how to use SAML to accomplish a specific task (e.g. SSO, attribute query)
- Binding - Standard that describes how to take a profile message and send it over a specific transport (e.g. HTTP)
- Front-channel - A binding that sends message through a user’s browser via redirects or form posts
- Back-channel - A binding where the entities connect directly to each other

Terminology (2)

- entityID - Unique identifier for an IdP or SP
- Assertion - The unit of information in SAML
- NameID - An identifier by which an IdP knows a user
- Attribute - A named piece of information about a user

Shibboleth Supported Profiles

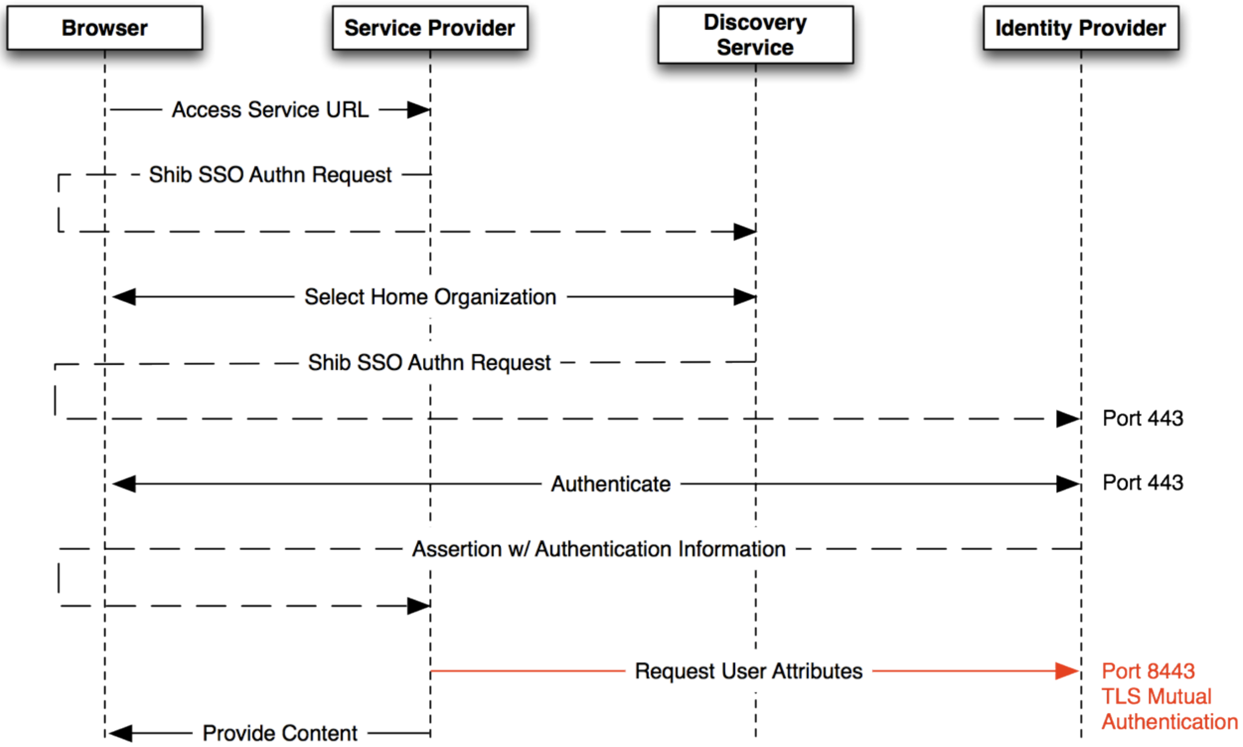
11

- SAML 1
  - Shibboleth SSO
  - Attribute Query
  - Artifact Resolution
- SAML 2
  - SSO
  - Attribute Query
  - Artifact Resolution
  - Enhanced Client
  - Single Logout (SP-only)
- Discovery
  - Shibboleth 1 Discovery (WAYF)
  - SAML 2 Discovery Service

https://wiki.shibboleth.net/confluence/display/DEV/Supported+Protocols

Shibboleth Communication Flow: Shibboleth 1

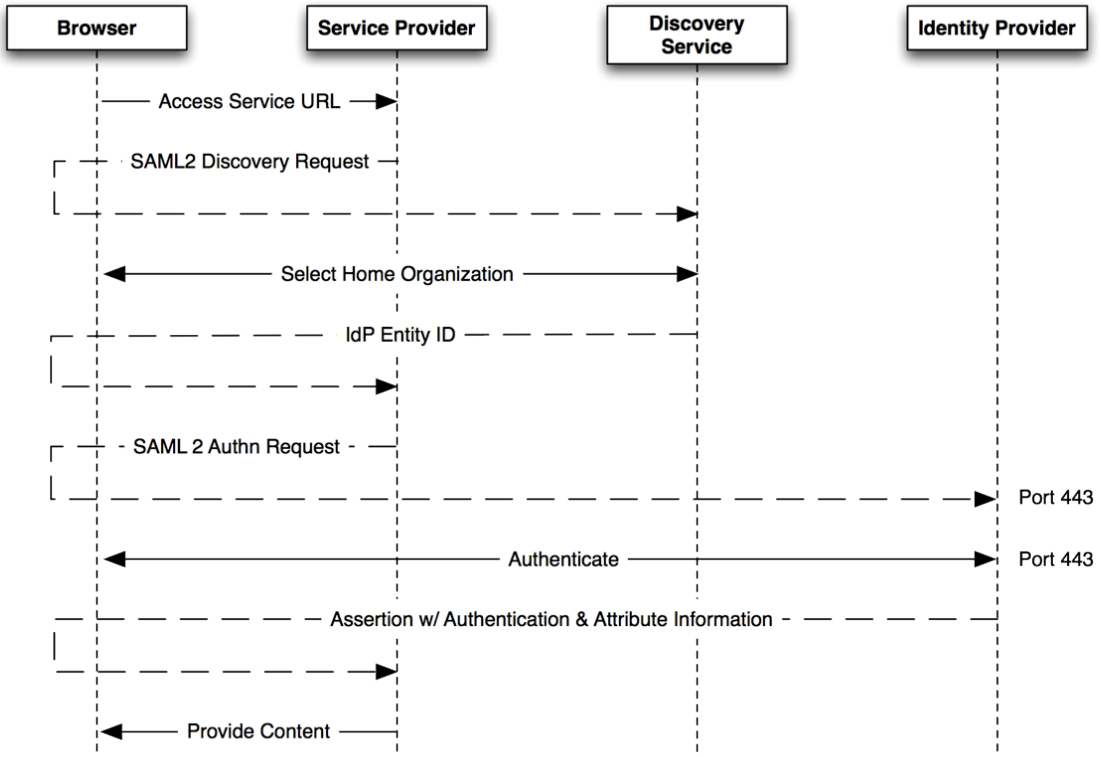
12



Problems with Shibboleth 1 SSO Flow

- The SP does not know which IdP will receive its request and so it can not tailor the authentication request
  - Which protocol to use?
  - Which keys to use for encryption?
- The IdP must have a second SSL port in order for the SP to make its attribute query (attribute pull model)
  - Twice the number of crypto operations
  - Two request/response pairs for every authentication

Shibboleth Communication Flow: Shibboleth 2 SSO



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

15

Odds and Ends

- Shibboleth knows nothing about federations, it just consumes metadata in order to:
  - locate the entity to which messages are sent
  - determine what protocols the entity supports
  - determine what signing/encryption keys to use
- The IdP is CPU bound, unlike most web apps
  - No support for crypto-acceleration currently
  - Support for clustering though

16

Shibboleth 1.3 to 2.X migration

- Shibboleth 2 is backwards compatible with 1.3
  - Obviously new SAML 2 features don’t work with Shibboleth 1.3
- Entity’s should embed their certificates in their metadata
  - This is required in order to support SAML 2 encryption
- The Shibboleth team recommends URLs for entityIDs
  - IdP entityID: **`https://HOSTNAME/idp/shibboleth`**
  - SP entityID: **`https://HOSTNAME/shibboleth`**
  - These URLs can then be used to get the metadata for the entity

SP Migration: Attribute Names

- Version 1.3 placed attributes in HTTP Headers

```
HTTP_SHIB_EP_AFFILIATION            staff
HTTP_SHIB_INETORGPERSON_GIVENNAME   Lukas
```

- Version 2.0 (when using Apache) places attributes in server environment and uses slightly different names as a result

```
Shib-EP-Affiliation                 staff
Shib-InetOrgePerson-givenName       Lukas
```

- Version 2.0 supports the old method but the new method guarantees that information can not be spoofed

Support Resources

- First, check with your Federation
  - http://switch.ch/aai/support/documents
  - http://switch.ch/aai/support/help
- Shibboleth Wiki
  - https://wiki.shibboleth.net/confluence/display/SHIB2
- Shibboleth User’s Mailing List Archive
  - http://marc.info/?l=shibboleth-users
- Shibboleth User’s Mailing List
  - http://shibboleth.net/community/lists.html

Resource Registry

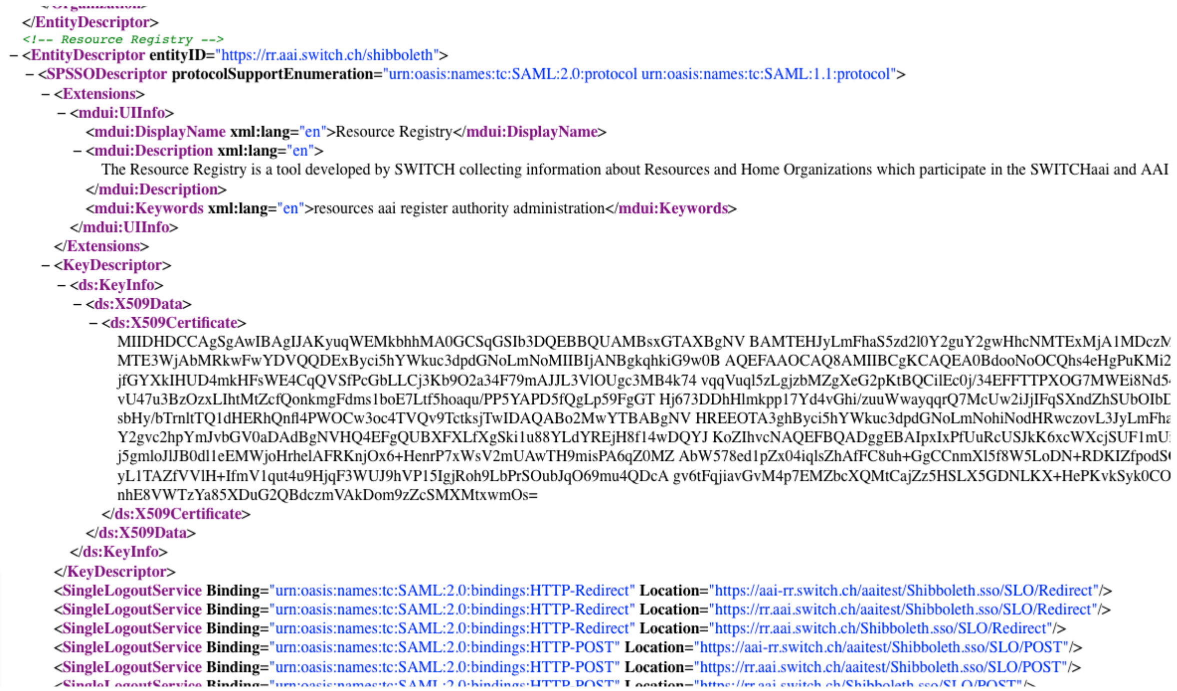
How to manage Federation metadata and other descriptions

SWITCH

Serving Swiss Universities

SWITCHaai Team
aai@switch.ch

The Initial <Problem>



```
</EntityDescriptor>
<!-- Resource Registry -->
– <EntityDescriptor entityID="https://rr.aai.switch.ch/shibboleth">
  – <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol urn:oasis:names:tc:SAML:1.1:protocol">
    – <Extensions>
      – <mdui:UIInfo>
          <mdui:DisplayName xml:lang="en">Resource Registry</mdui:DisplayName>
        – <mdui:Description xml:lang="en">
            The Resource Registry is a tool developed by SWITCH collecting information about Resources and Home Organizations which participate in the SWITCHaai and AAI
          </mdui:Description>
          <mdui:Keywords xml:lang="en">resources aai register authority administration</mdui:Keywords>
        </mdui:UIInfo>
      </Extensions>
    – <KeyDescriptor>
      – <ds:KeyInfo>
        – <ds:X509Data>
          – <ds:X509Certificate>
              MIIDHDCCAgSgAwIBAgIJAKyuqWEMkbhhMA0GCSqGSIb3DQEBBQUAMBsxGTAXBgNV BAMTEHJyLmFhaS5zd2l0Y2guY2gwHhcNMTExMjA1MDcz
              MTE3WjAbMRkwFwYDVQQDExByci5hYWkuc3dpdGNoLmNoMIIBIjANBgkqhkiG9w0B AQEFAAOCAQ8AMIIBCgKCAQEA0BdooNoOCQhs4eHgPuKMi2
              jfGYXkIHUD4mkHFsWE4CqQVSfPcGbLLCj3Kb9O2a34F79mAJJL3VlOUgc3MB4k74 vqqVuql5zLgjzbMZgXeG2pKtBQCilEc0j/34EFFTTPXOG7MWEi8Nd5
              vU47u3BzOzxLIhtMtZcfQonkmgFdms1boE7Ltf5hoaqu/PP5YAPD5fQgLp59FgGT Hj673DDhHlmkpp17Yd4vGhi/zuuWwayqqrQ7McUw2iJjIFqSXndZhSUbOIb
              sbHy/bTrnltTQ1dHERhQnfl4PWOCw3oc4TVQv9TctksjTwIDAQABo2MwYTBABgNV HREEOTA3ghByci5hYWkuc3dpdGNoLmNohiNodHRwczovL3JyLmFh
              Y2gvc2hpYmJvbGV0aDAdBgNVHQ4EFgQUBXFXLfXgSki1u88YLdYREjH8f14wDQYJ KoZIhvcNAQEFBQADggEBAIpxIxPfUuRcUSJkK6xcWXcjSUF1mU
              j5gmloJlJB0dl1eEMWjoHrhelAFRKnjOx6+HenrP7xWsV2mUAwTH9misPA6qZ0MZ AbW578ed1pZx04iqlsZhAfFC8uh+GgCCnmXl5f8W5LoDN+RDKIZfpodS
              yL1TAZfVVlH+IfmV1qut4u9HjqF3WUJ9hVP15IgjRoh9LbPrSOubJqO69mu4QDcA gv6tFqjiavGvM4p7EMZbcXQMtCajZz5HSLX5GDNLKX+HePKvkSyk0CO
              nhE8VWTzYa85XDuG2QBdczmVAkDom9zZcSMXMtxwmOs=
            </ds:X509Certificate>
          </ds:X509Data>
        </ds:KeyInfo>
      </KeyDescriptor>
      <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://aai-rr.switch.ch/aaitest/Shibboleth.sso/SLO/Redirect"/>
      <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://rr.aai.switch.ch/aaitest/Shibboleth.sso/SLO/Redirect"/>
      <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://rr.aai.switch.ch/Shibboleth.sso/SLO/Redirect"/>
      <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://aai-rr.switch.ch/aaitest/Shibboleth.sso/SLO/POST"/>
      <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://rr.aai.switch.ch/aaitest/Shibboleth.sso/SLO/POST"/>
      <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://rr.aai.switch.ch/Shibboleth.sso/SLO/POST"/>
```

Shibboleth needs SAML 2 metadata to know all entities!

Difficulties and Goals

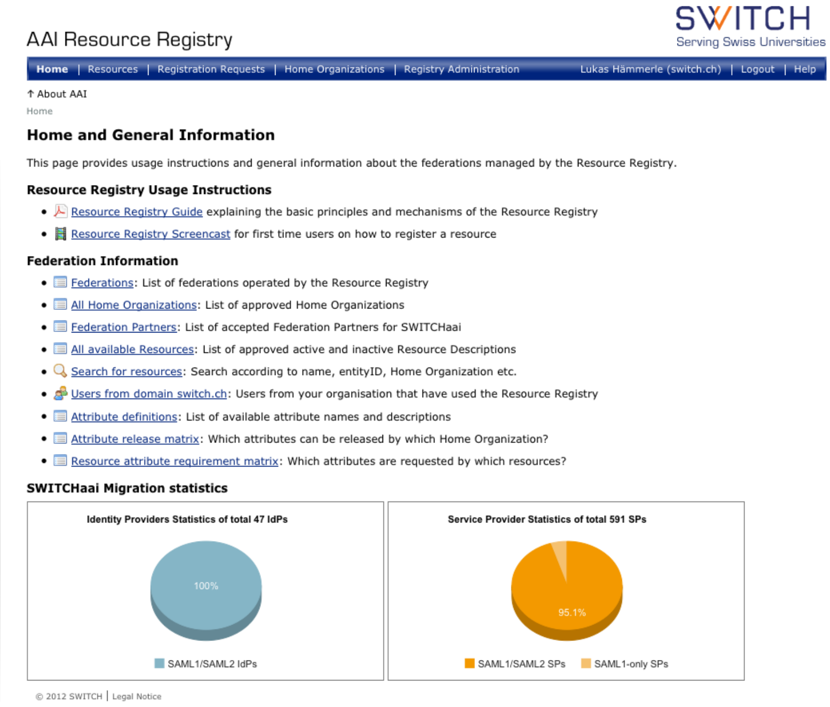
- Editing XML files by hand is error-prone and clumsy
- Managing the federation metadata by hand is cumbersome
- Legal processes should be technically supported
- Multiple federations must be managed

A web-based tool to solve these problems!

Goals for such a Tool:

- Scalable metadata management
- Support administrative processes
- Provide auxiliary functions to support federation
- As little overhead as possible

The AAI Resource Registry


AAI Resource Registry
SWITCH
Serving Swiss Universities
Home | Resources | Registration Requests | Home Organizations | Registry Administration
Lukas Hämmerle (switch.ch) | Logout | Help
↑ About AAI
Home

Home and General Information

This page provides usage instructions and general information about the federations managed by the Resource Registry.

Resource Registry Usage Instructions

- Resource Registry Guide explaining the basic principles and mechanisms of the Resource Registry
- Resource Registry Screencast for first time users on how to register a resource

Federation Information

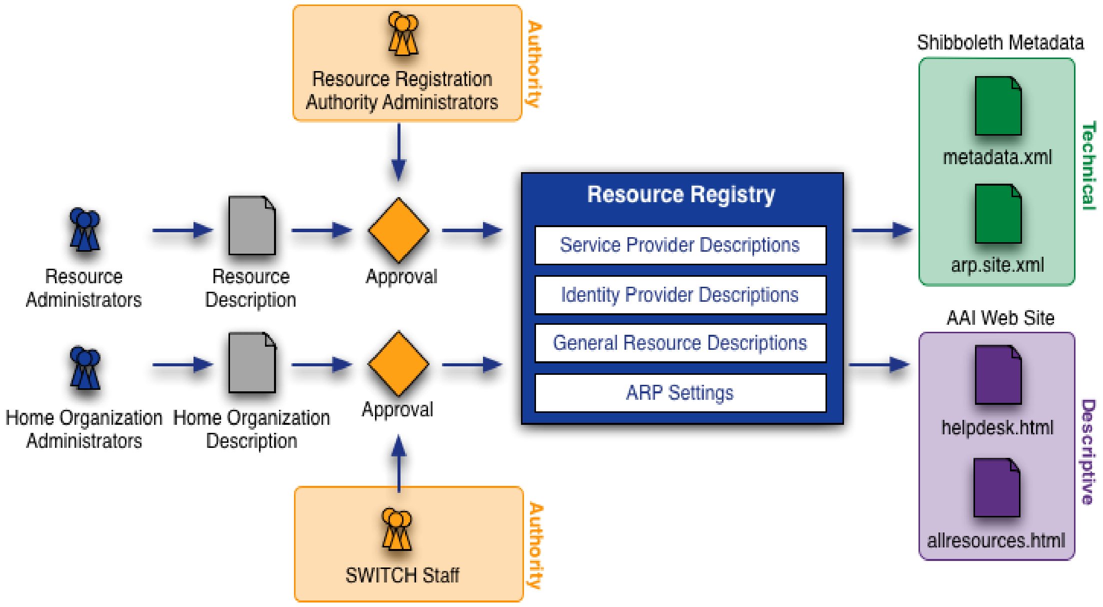
- Federations: List of federations operated by the Resource Registry
- All Home Organizations: List of approved Home Organizations
- Federation Partners: List of accepted Federation Partners for SWITCHaai
- All available Resources: List of approved active and inactive Resource Descriptions
- Search for resources: Search according to name, entityID, Home Organization etc.
- Users from domain switch.ch: Users from your organisation that have used the Resource Registry
- Attribute definitions: List of available attribute names and descriptions
- Attribute release matrix: Which attributes can be released by which Home Organization?
- Resource attribute requirement matrix: Which attributes are requested by which resources?

SWITCHaai Migration statistics

Identity Providers Statistics of total 47 IdPs
100%
SAML1/SAML2 IdPs
Service Provider Statistics of total 591 SPs
95.1%
SAML1/SAML2 SPs
SAML1-only SPs
© 2012 SWITCH | Legal Notice

Web: https://rr.aai.switch.ch

Resource Registry Processes



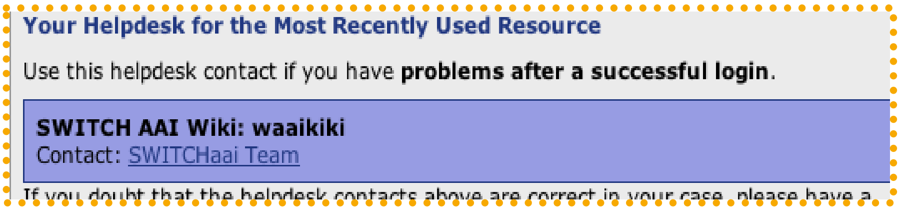
Before an SP/IdP description becomes part of federation metadata, it must be approved by an authority first

Roles in the Resource Registry

- **Resource Registry Administrator**
  SWITCH staff members. Can edit/delete everything
- **Home Organisation Administrator**
  User that can manages the description/metadata of an organisation
  - **Attribute Administrator**
    Subset of privileges of Home Organisation administrator
    User that can change the attribute release policy of an organisation
- **Resource Administrator**
  Creates and manages descriptions of AAI services/Service Providers
- **Resource Registration Authority Administrator**
  Approves descriptions of AAI services/Service Providers

Output of Resource Registry

- **Metadata,** see **http://www.switch.ch/aai/metadata/**
- **Configuration files** for IdPs and SPs (shibboleth2.xml, …)
- **Helpdesk webpage** shows contact personse/helpdesk for your SP



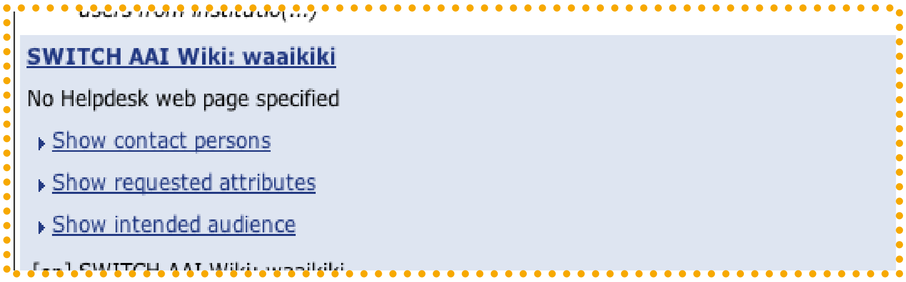
Your Helpdesk for the Most Recently Used Resource

Use this helpdesk contact if you have **problems after a successful login**.

SWITCH AAI Wiki: waaikiki
Contact: SWITCHaai Team

If you doubt that the helpdesk contacts above are correct in your case, please have a

- **Public Resource list**, see **http://www.switch.ch/aai/participants/**



users from institutio(...)

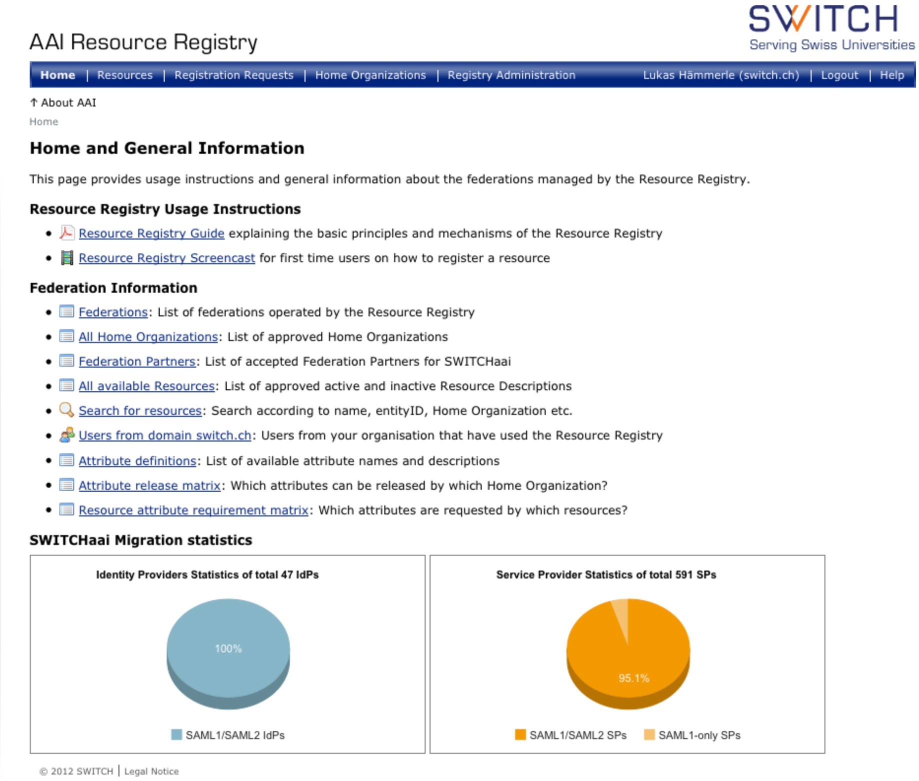
SWITCH AAI Wiki: waaikiki

No Helpdesk web page specified

- ▸ Show contact persons
- ▸ Show requested attributes
- ▸ Show intended audience

[-] SWITCH AAI Wiki: waaikiki

Live Demonstration



AAI Resource Registry

SWITCH
Serving Swiss Universities

Home | Resources | Registration Requests | Home Organizations | Registry Administration | Lukas Hämmerle (switch.ch) | Logout | Help

↑ About AAI
Home

Home and General Information

This page provides usage instructions and general information about the federations managed by the Resource Registry.

Resource Registry Usage Instructions

- Resource Registry Guide explaining the basic principles and mechanisms of the Resource Registry
- Resource Registry Screencast for first time users on how to register a resource

Federation Information

- Federations: List of federations operated by the Resource Registry
- All Home Organizations: List of approved Home Organizations
- Federation Partners: List of accepted Federation Partners for SWITCHaai
- All available Resources: List of approved active and inactive Resource Descriptions
- Search for resources: Search according to name, entityID, Home Organization etc.
- Users from domain switch.ch: Users from your organisation that have used the Resource Registry
- Attribute definitions: List of available attribute names and descriptions
- Attribute release matrix: Which attributes can be released by which Home Organization?
- Resource attribute requirement matrix: Which attributes are requested by which resources?

SWITCHaai Migration statistics

Identity Providers Statistics of total 47 IdPs
100%
SAML1/SAML2 IdPs
Service Provider Statistics of total 591 SPs
95.1%
SAML1/SAML2 SPs
SAML1-only SPs

© 2012 SWITCH | Legal Notice

Embedded WAYF

Integration of the Discovery Service into a service

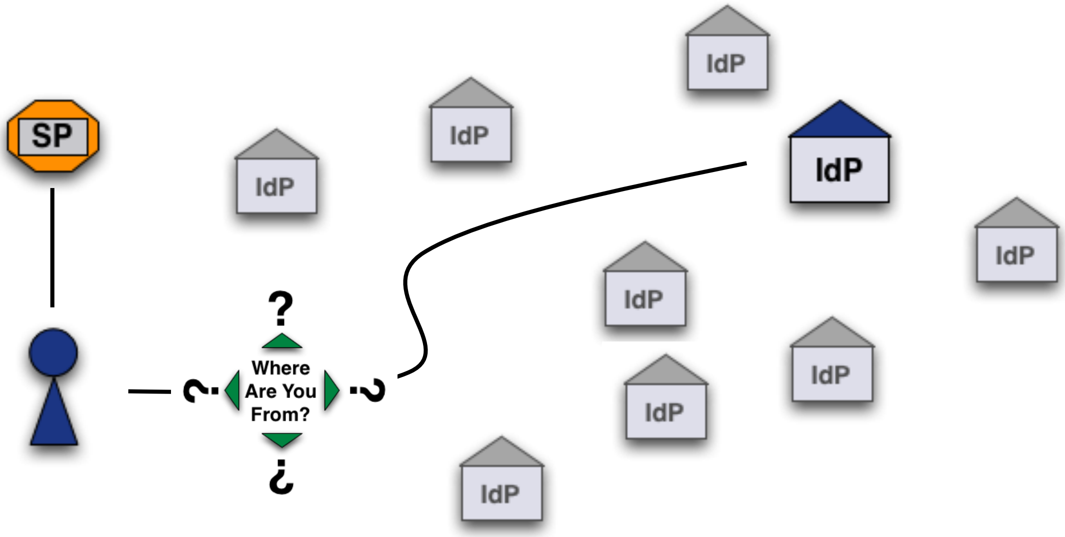
SWITCH

Serving Swiss Universities

SWITCHaai Team
aai@switch.ch

The Problem

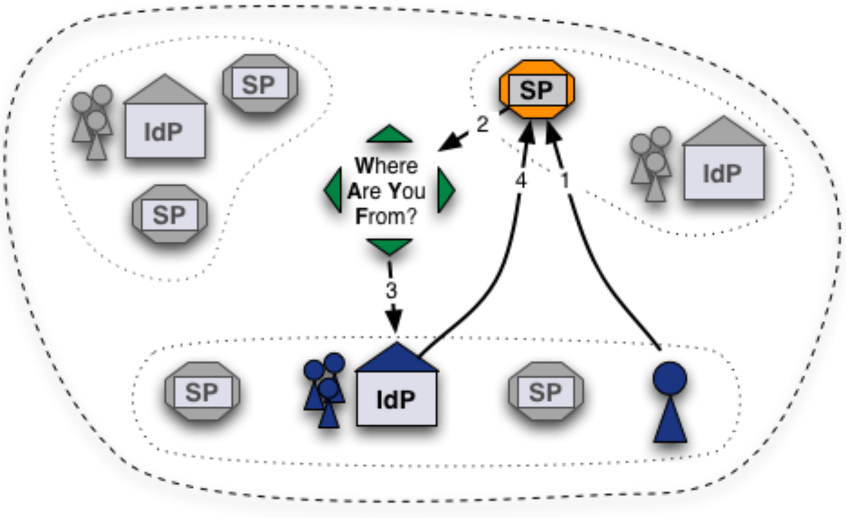
In a federated environment, the user has to declare where he wants to authenticate.



The easiest way is to ask the user “Where Are You From?”

Solution 1: Central WAYF

- The classic way: One WAYF per Federation



Centralized WAYF: Considerations

- “The WAYF is the worst possible way of doing IdP Discovery except for all the others” (Scott Cantor, SP developer)

👍 Very convenient for Resource administrators

No deployment, installation or maintenance needed

👍 User statistics can be generated for federation

👍 User has to select his IdP only once per session

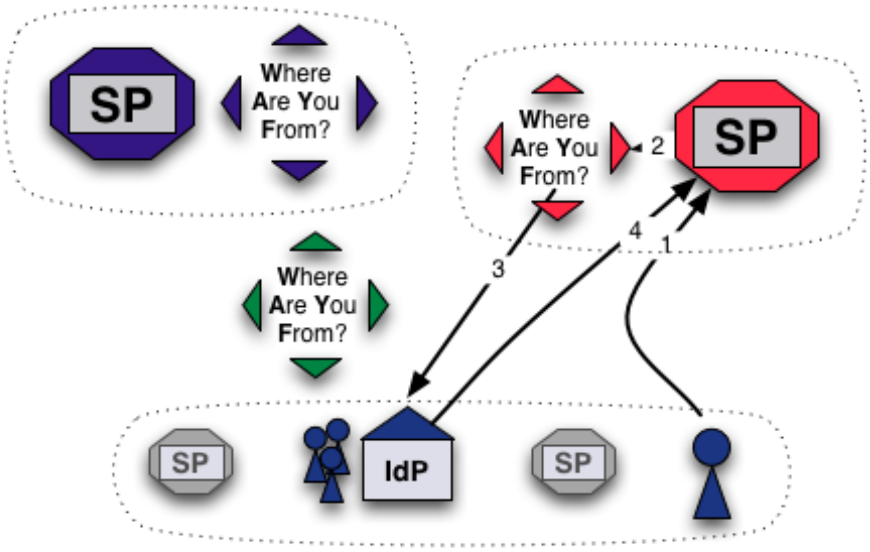
👎 Yet another domain the user comes across

👎 Another custom look & feel

👎 No controls regarding IdPs that are displayed

Solution 2: Distributed WAYF

- More and more used: One WAYF per Resource



Distributed WAYF: Considerations

- Mostly e-learning administrators of larger resources want best usability and look&feel for their user

👍 Complete control for Resource administrators

Limit IdPs to relevant ones, adapt look&feel, integrate into resource

👍 No redirects to another host

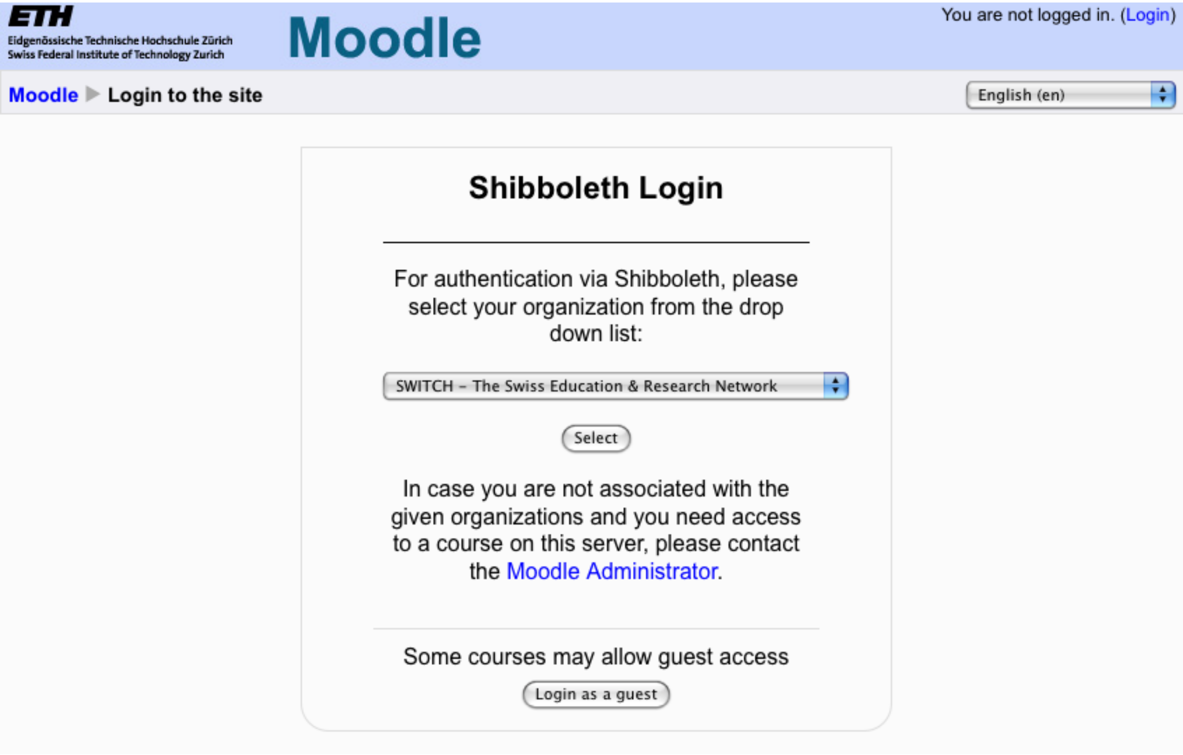
👍 One click less when optimally integrated

👎 Integration/Implementation/Maintenance work for admins

👎 No federation user statistics

👎 User may have to choose IdP for each resource again

Distributed WAYF Example



ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich
Moodle
You are not logged in. (Login)
Moodle ▶ Login to the site
English (en)

Shibboleth Login

For authentication via Shibboleth, please select your organization from the drop down list:

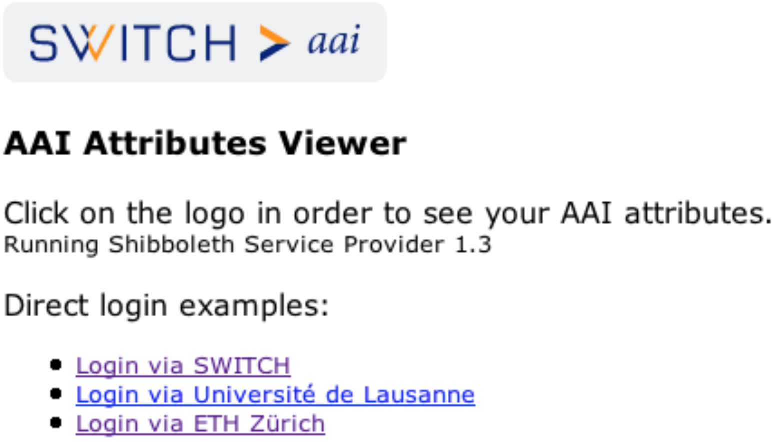
SWITCH - The Swiss Education & Research Network

In case you are not associated with the given organizations and you need access to a course on this server, please contact the Moodle Administrator.

Some courses may allow guest access

2.b Direct Login URLs

- A separate login link for specific IdPs
- 1 click direct redirect to IdP without going via WAYF
- Useful when only users of few IdPs use resource



AAI Attributes Viewer

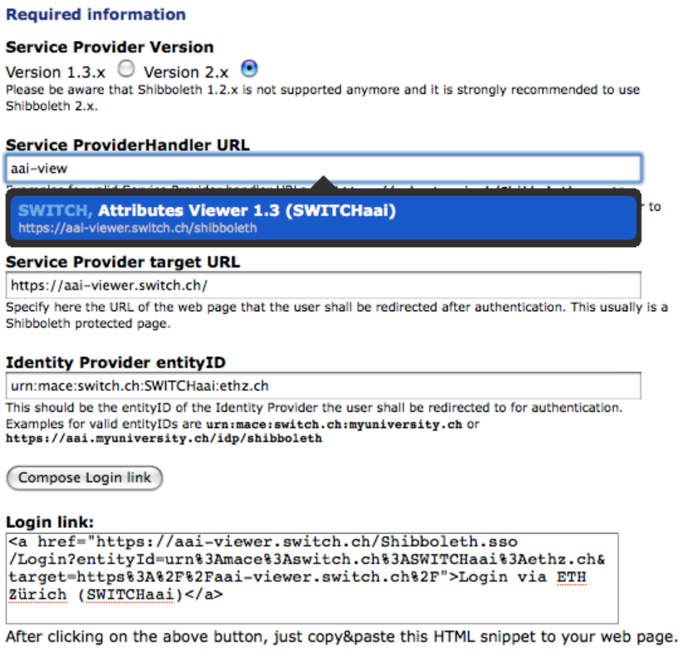
Click on the logo in order to see your AAI attributes.
Running Shibboleth Service Provider 1.3

Direct login examples:

- Login via SWITCH
- Login via Université de Lausanne
- Login via ETH Zürich

Example: https://aai-viewer.switch.ch/

Composing Login URLs



Required information

Service Provider Version

Version 1.3.x ○ Version 2.x ●

Please be aware that Shibboleth 1.2.x is not supported anymore and it is strongly recommended to use Shibboleth 2.x.

Service ProviderHandler URL

aai-view

SWITCH, Attributes Viewer 1.3 (SWITCHaai)
https://aai-viewer.switch.ch/shibboleth

Service Provider target URL

https://aai-viewer.switch.ch/

Specify here the URL of the web page that the user shall be redirected after authentication. This usually is a Shibboleth protected page.

Identity Provider entityID

urn:mace:switch.ch:SWITCHaai:ethz.ch

This should be the entityID of the Identity Provider the user shall be redirected to for authentication. Examples for valid entityIDs are `urn:mace:switch.ch:myuniversity.ch` or `https://aai.myuniversity.ch/idp/shibboleth`

Login link:

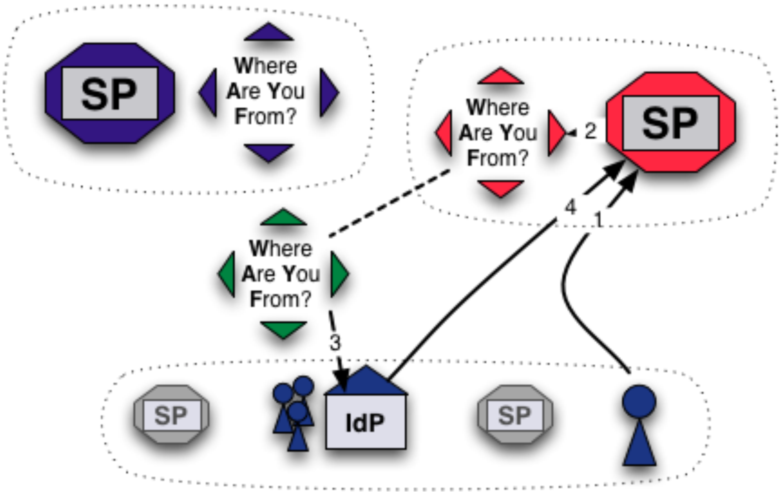
```
<a href="https://aai-viewer.switch.ch/Shibboleth.sso
/Login?entityId=urn%3Amace%3Aswitch.ch%3ASWITCHaai%3Aethz.ch&
target=https%3A%2F%2Faai-viewer.switch.ch%2F">Login via ETH
Zürich (SWITCHaai)</a>
```

After clicking on the above button, just copy&paste this HTML snippet to your web page.

http://www.switch.ch/aai/support/serviceproviders/sp-compose-login-url.html

Solution 3: Embedded WAYF

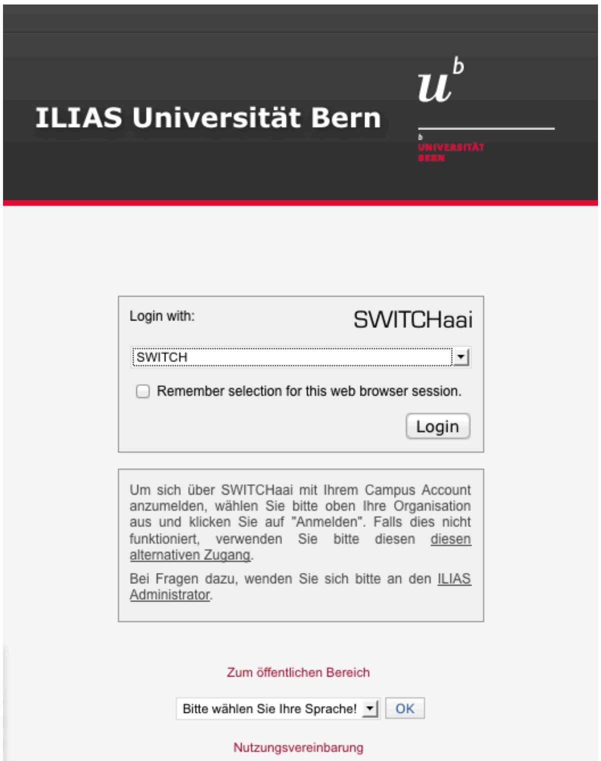
- The new idea: Embed WAYF on Resource, customize look and feel but effectively still transparently use central WAYF



How the embedding works

- Works like Google Ads :-)
- Embedd 2 JavaScripts:
  - Configurator Script
    - Influences look and feel (colors, size, etc.)
    - Excludes IdPs from list
    - Add IdPs from other federations
  - Logic Script
    - The same URL for all instances of the embedded WAYF
    - Generated by and loaded from central WAYF
    - Cookies from central WAYF can be read this way!
      This allows IdP preselection or direct redirection

Embedded WAYF Example



ILIAS Universität Bern

Login with: SWITCHaai

SWITCH

□ Remember selection for this web browser session.

Login

Um sich über SWITCHaai mit Ihrem Campus Account anzumelden, wählen Sie bitte oben Ihre Organisation aus und klicken Sie auf "Anmelden". Falls dies nicht funktioniert, verwenden Sie bitte diesen diesen alternativen Zugang.

Bei Fragen dazu, wenden Sie sich bitte an den ILIAS Administrator.

Zum öffentlichen Bereich

Bitte wählen Sie Ihre Sprache! OK

Nutzungsvereinbarung

Instructions:

1. Copy & paste sample HTML code to your web page
2. Adapt at least 3 settings
3. Done

What you get:

Always up-to date, fully customizable, self-maintained, 1 click-saving Discovery Service

Example:

https://ilias.unibe.ch/

Embedded WAYF: Considerations

- Use advantages of central and distributed approach

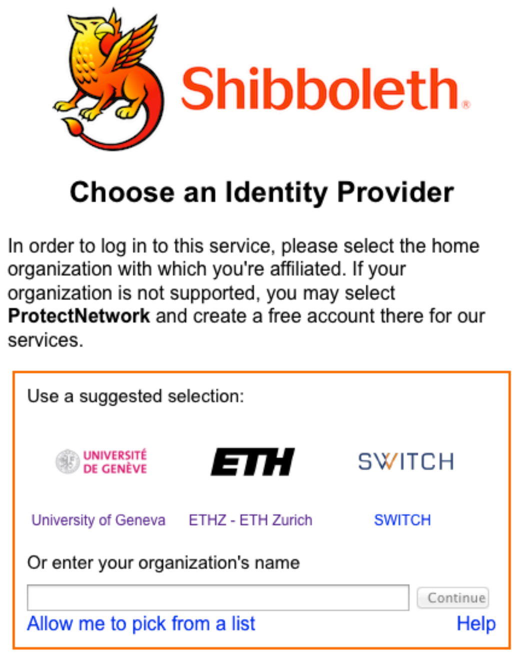
👍 Complete control for Resource administrators
  Limit IdPs to relevant ones, adapt look&feel, integrate into resource
👍 No redirects to another host
👍 Saves at least one click
👍 Very convenient for Resource administrators
  No deployment, installation or maintenance needed
👍 User statistics can be generated for federation

👎 (User needs Javascript enabled or use alternative fallback)
👎 (Central WAYF must be well secured and high available)

http://www.switch.ch/aai/support/serviceproviders/sp-embedded-wayf.html

Alternative I: Embedded Discovery Service

- Works like Embedded WAYF
- Independent from a central service
- Requires Shibboleth SP >= 2.4
- Search-as-you-type or select from list
- JS, CSS and HTML only
- Very easy to customize



Choose an Identity Provider

In order to log in to this service, please select the home organization with which you're affiliated. If your organization is not supported, you may select **ProtectNetwork** and create a free account there for our services.

Use a suggested selection:

University of Geneva ETHZ - ETH Zurich SWITCH

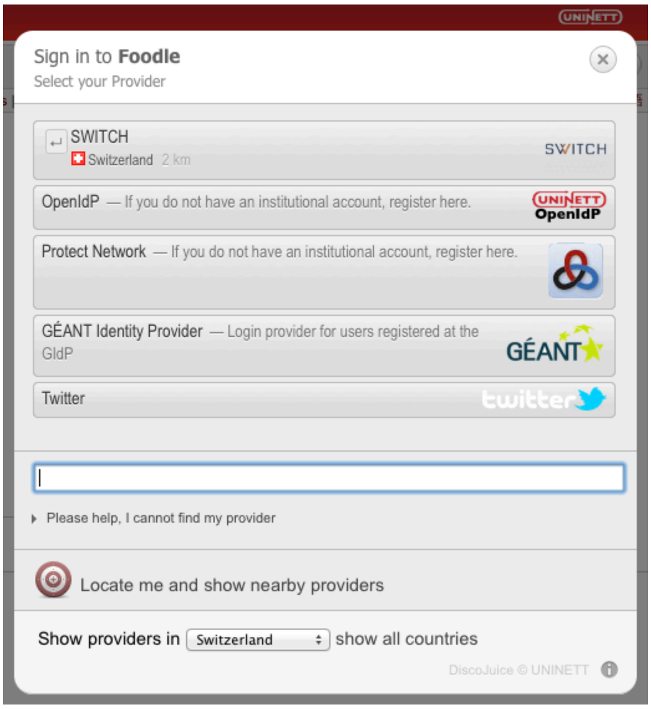
Or enter your organization's name

Allow me to pick from a list Help

https://wiki.shibboleth.net/confluence/display/EDS10/Embedded+Discovery+Service

Alternative II: Disco Juice

- Very comprehensive Discovery Service
- Well suited for services with users from many IdPs
- Search-as-you-type only
- Uses Geo IP and metric to guess user's IdP
- Based on PHP and JS



Sign in to **Foodle**

Select your Provider

SWITCH
Switzerland 2 km

OpenIdP — If you do not have an institutional account, register here.

Protect Network — If you do not have an institutional account, register here.

GÉANT Identity Provider — Login provider for users registered at the GIdP

Twitter

Please help, I cannot find my provider

Locate me and show nearby providers

Show providers in Switzerland show all countries

DiscoJuice © UNINETT

http://discojuice.org/

Virtual Home Organization & Guest Login

SWITCH

Serving Swiss Universities

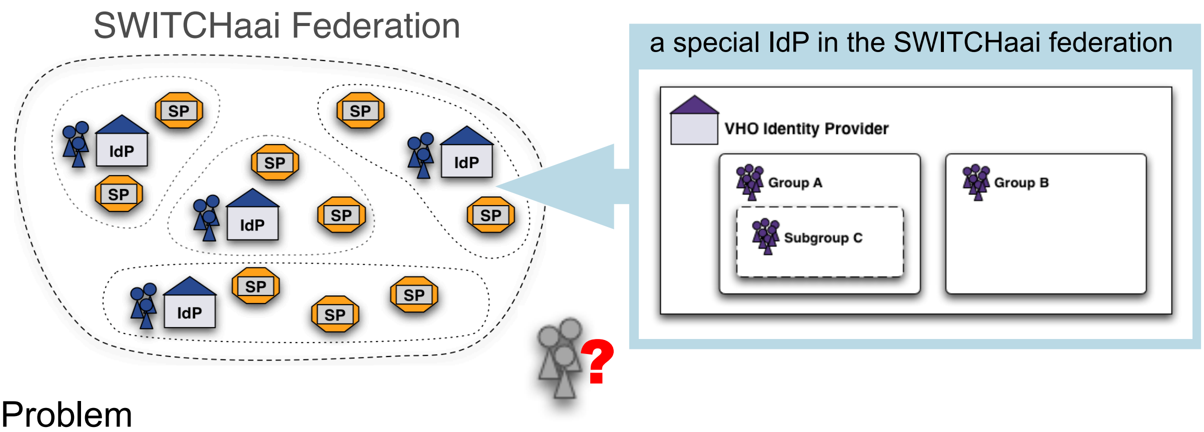
SWITCHaai Team
aai@switch.ch

Agenda

2

1. Motivation & Context
2. SWITCH VHO Service
3. VHO Administration Tool
4. Guest Login

Motivation & Context



Problem

- Resource (SP) configured to only accept AAI users
- Users from outside the federation need access to the resource

Solution

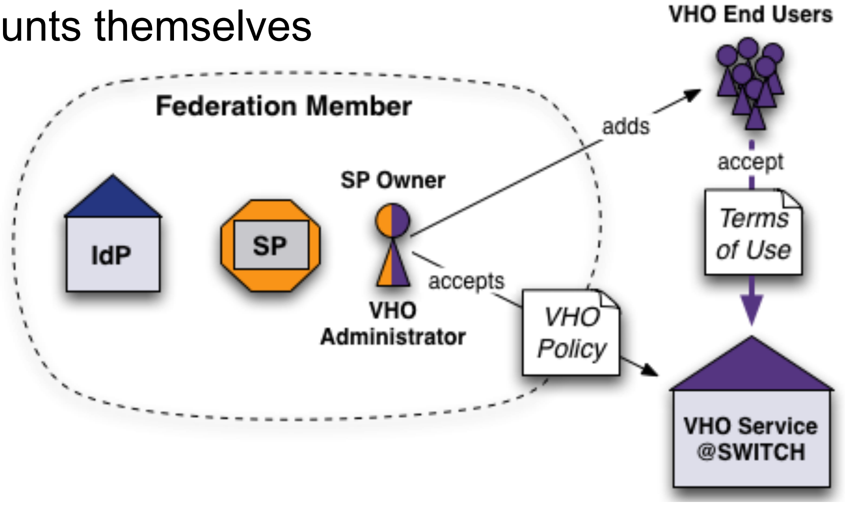
- Resource owner manages these users in the Virtual Home Organization (VHO)

Agenda

1. Motivation & Context
2. SWITCH VHO Service
3. VHO Administration Tool
4. Guest Login

SWITCH VHO Service

- Targeted end user groups
  - Attendees of a further education or other training
  - Collaboration projects from private companies or foreign universities, which are not in the SWITCHaai federation
- Resource owners can manage end user accounts themselves



VHO End Users

Federation Member

adds

accept

SP Owner

IdP

SP

Terms of Use

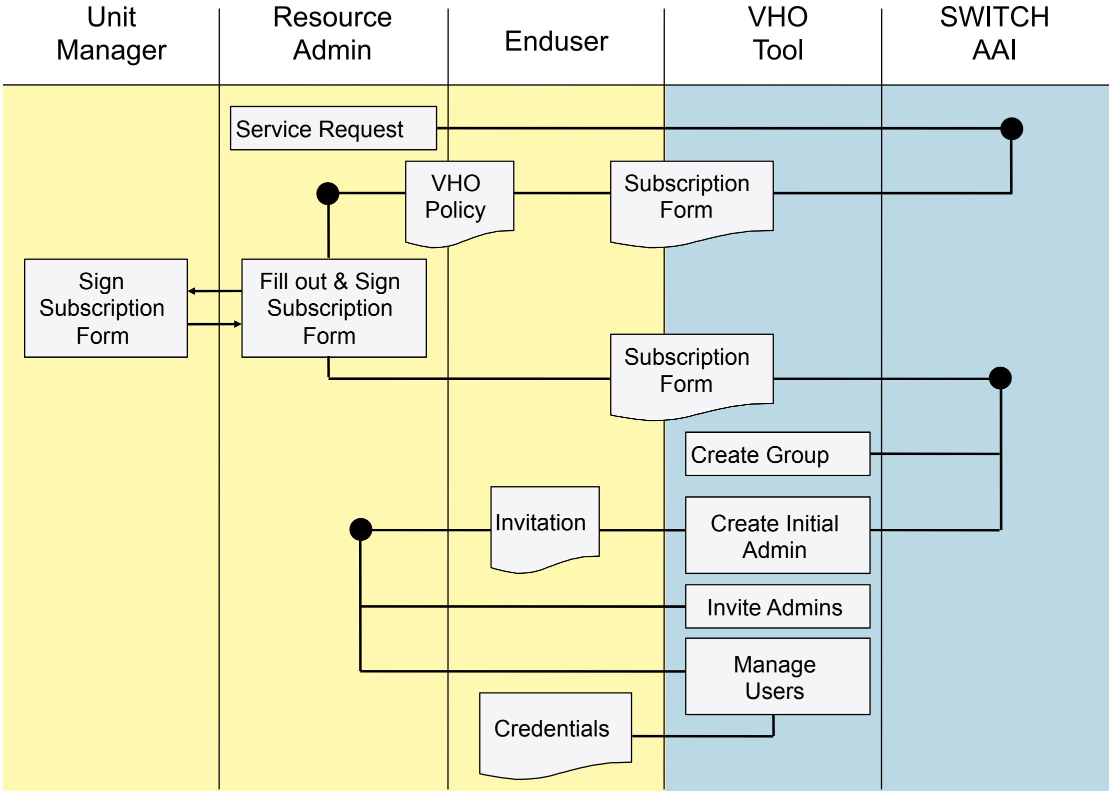
accepts

VHO Administrator

VHO Policy

VHO Service @SWITCH

Service Subscription Process



Unit Manager

Resource Admin

Enduser

VHO Tool

SWITCH AAI

Service Request

VHO Policy

Subscription Form

Sign Subscription Form

Fill out & Sign Subscription Form

Subscription Form

Create Group

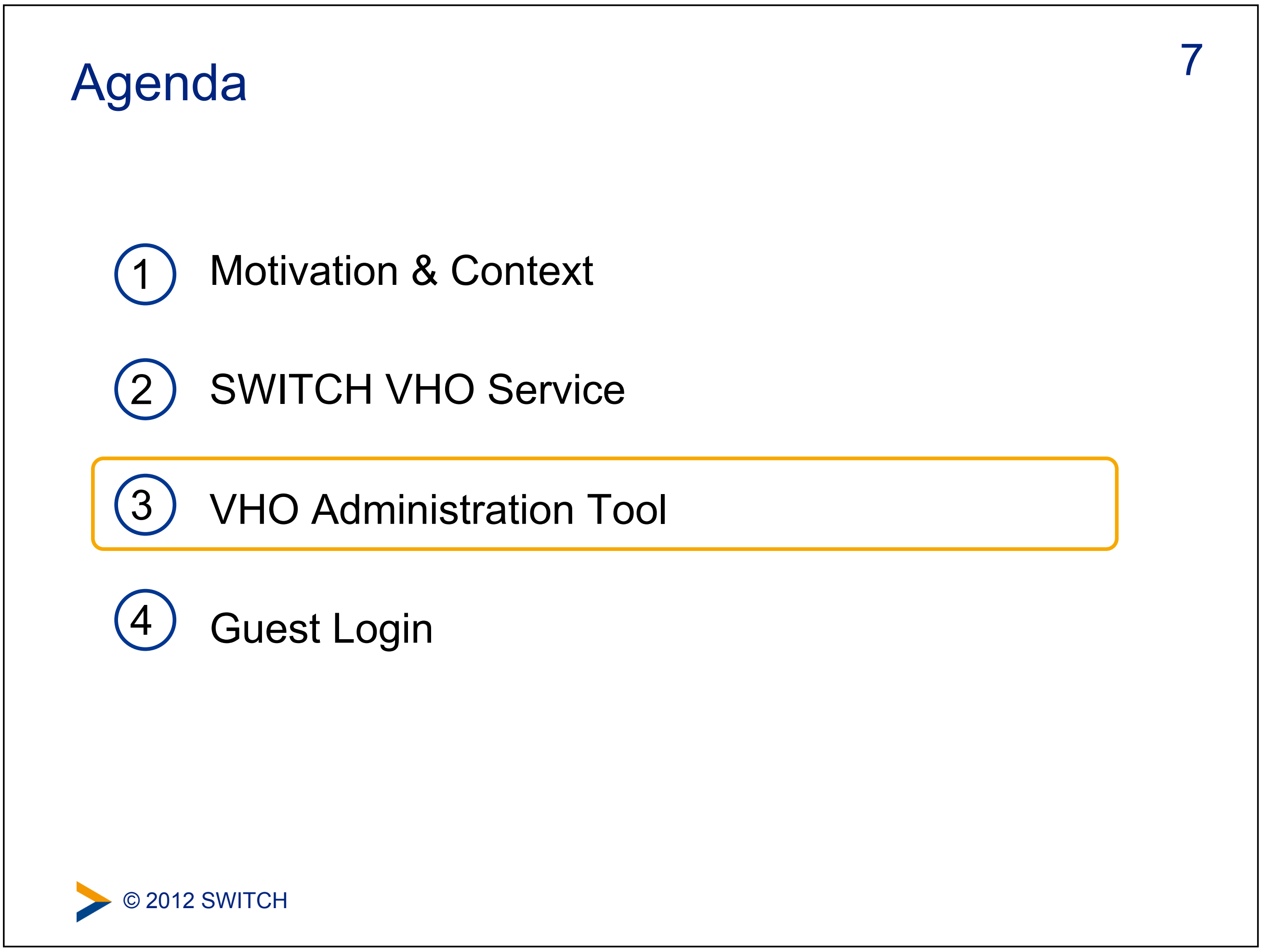
Invitation

Create Initial Admin

Invite Admins

Manage Users

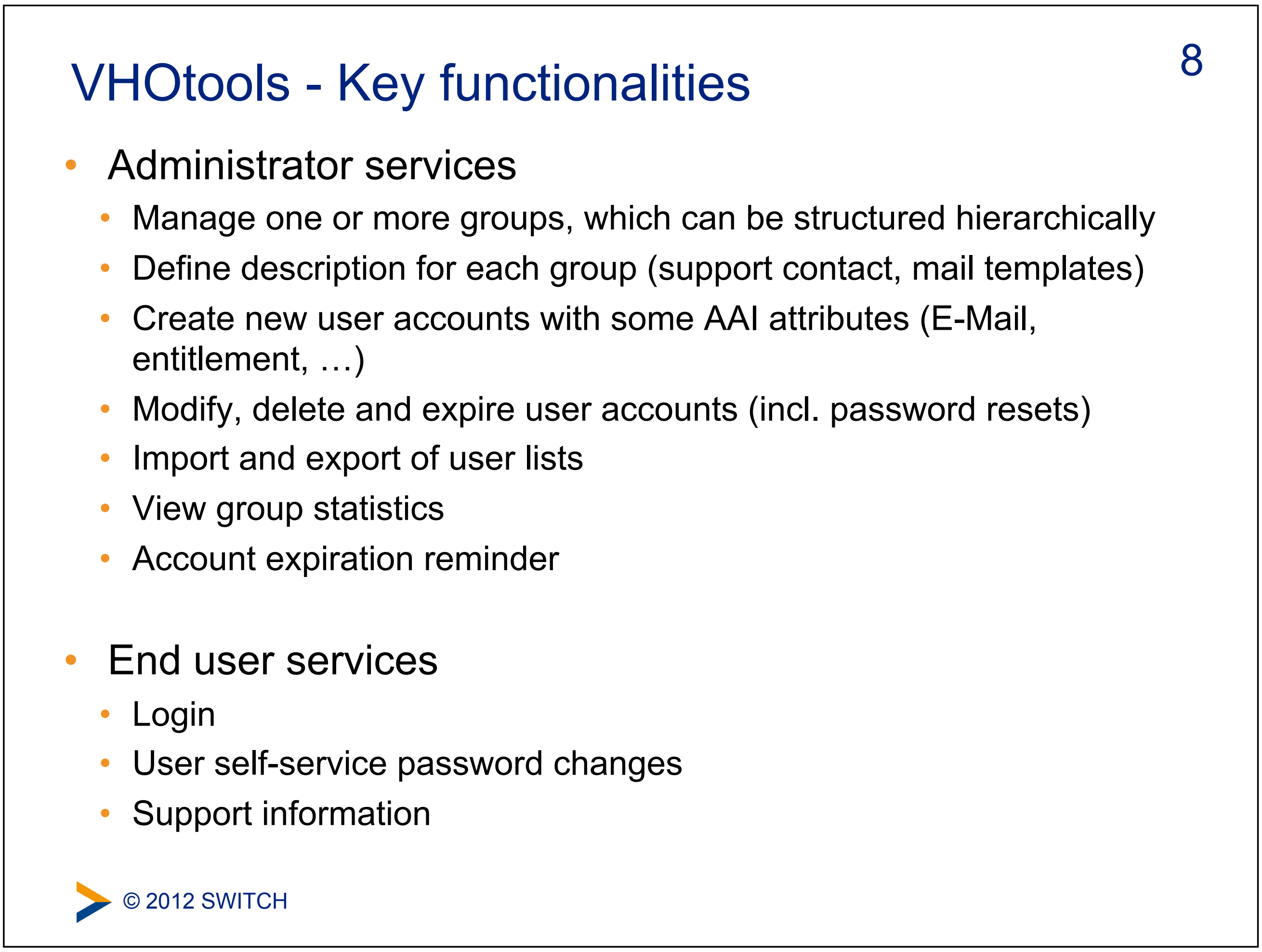
Credentials



Agenda

7

1. Motivation & Context
2. SWITCH VHO Service
3. VHO Administration Tool
4. Guest Login



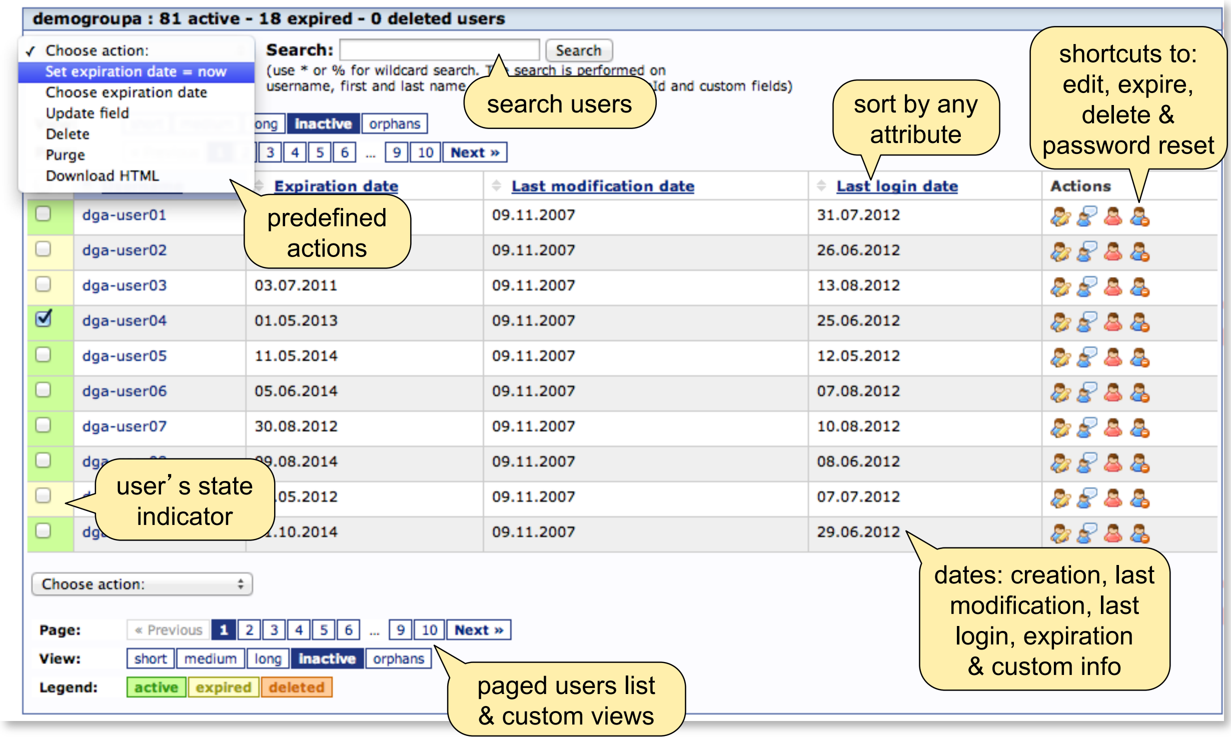
VHOtools - Key functionalities

8

- Administrator services
  - Manage one or more groups, which can be structured hierarchically
  - Define description for each group (support contact, mail templates)
  - Create new user accounts with some AAI attributes (E-Mail, entitlement, …)
  - Modify, delete and expire user accounts (incl. password resets)
  - Import and export of user lists
  - View group statistics
  - Account expiration reminder

- End user services
  - Login
  - User self-service password changes
  - Support information

Screenshots administration tool (1)



demogroupa : 81 active - 18 expired - 0 deleted users

Search: ▭ Search

(use * or % for wildcard search. T search is performed on username, first and last name ld and custom fields)

		Expiration date	Last modification date	Last login date	Actions
□	dga-user01		09.11.2007	31.07.2012	
□	dga-user02		09.11.2007	26.06.2012	
□	dga-user03	03.07.2011	09.11.2007	13.08.2012	
☑	dga-user04	01.05.2013	09.11.2007	25.06.2012	
□	dga-user05	11.05.2014	09.11.2007	12.05.2012	
□	dga-user06	05.06.2014	09.11.2007	07.08.2012	
□	dga-user07	30.08.2012	09.11.2007	10.08.2012	
□	dga	9.08.2014	09.11.2007	08.06.2012	
□		.05.2012	09.11.2007	07.07.2012	
□	dg	.10.2014	09.11.2007	29.06.2012	

Page: « Previous 1 2 3 4 5 6 ... 9 10 Next »

View: short medium long inactive orphans

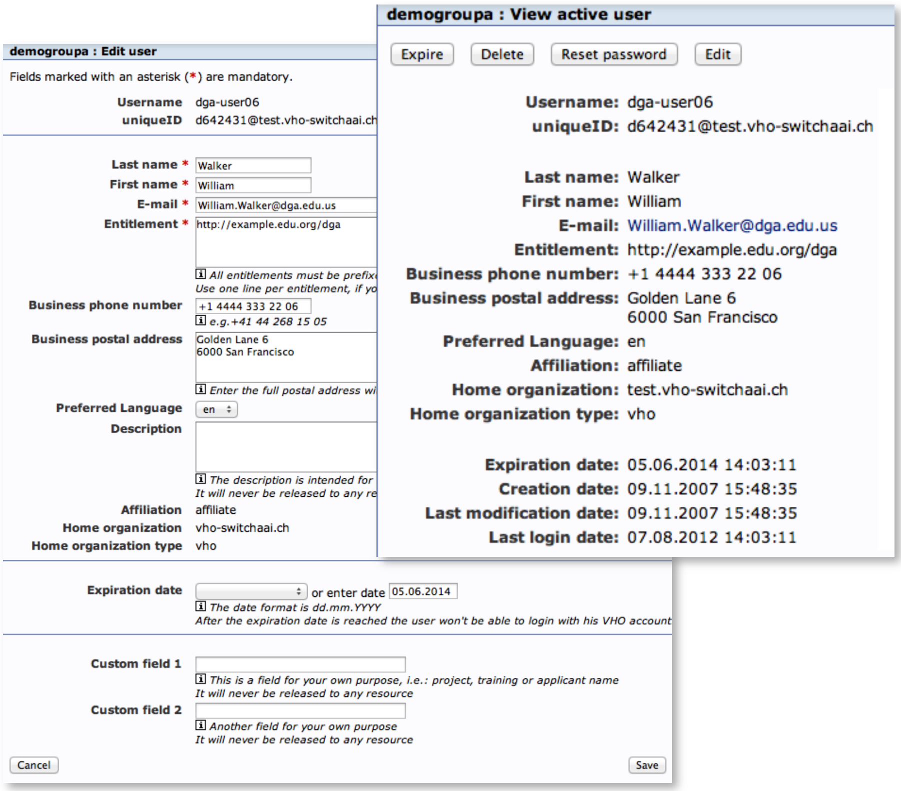
Legend: 🟩 active 🟨 expired 🟧 deleted

search users
sort by any attribute
shortcuts to: edit, expire, delete & password reset
predefined actions
user's state indicator
dates: creation, last modification, last login, expiration & custom info
paged users list & custom views

© 2012 SWITCH

Screenshots administration tool (2)

Create or modify user accounts using web forms...



demogroupa : Edit user

Fields marked with an asterisk (*) are mandatory.

Username	dga-user06
uniqueID	d642431@test.vho-switchaai.ch
Last name *	Walker
First name *	William
E-mail *	William.Walker@dga.edu.us
Entitlement *	http://example.edu.org/dga ℹ *All entitlements must be prefix* *Use one line per entitlement, if yo*
Business phone number	+1 4444 333 22 06 ℹ *e.g.+41 44 268 15 05*
Business postal address	Golden Lane 6 6000 San Francisco ℹ *Enter the full postal address wi*
Preferred Language	en
Description	ℹ *The description is intended for* *It will never be released to any re*
Affiliation	affiliate
Home organization	vho-switchaai.ch
Home organization type	vho
Expiration date	or enter date 05.06.2014 ℹ *The date format is dd.mm.YYYY* *After the expiration date is reached the user won't be able to login with his VHO account*
Custom field 1	ℹ *This is a field for your own purpose, i.e.: project, training or applicant name* *It will never be released to any resource*
Custom field 2	ℹ *Another field for your own purpose* *It will never be released to any resource*

demogroupa : View active user

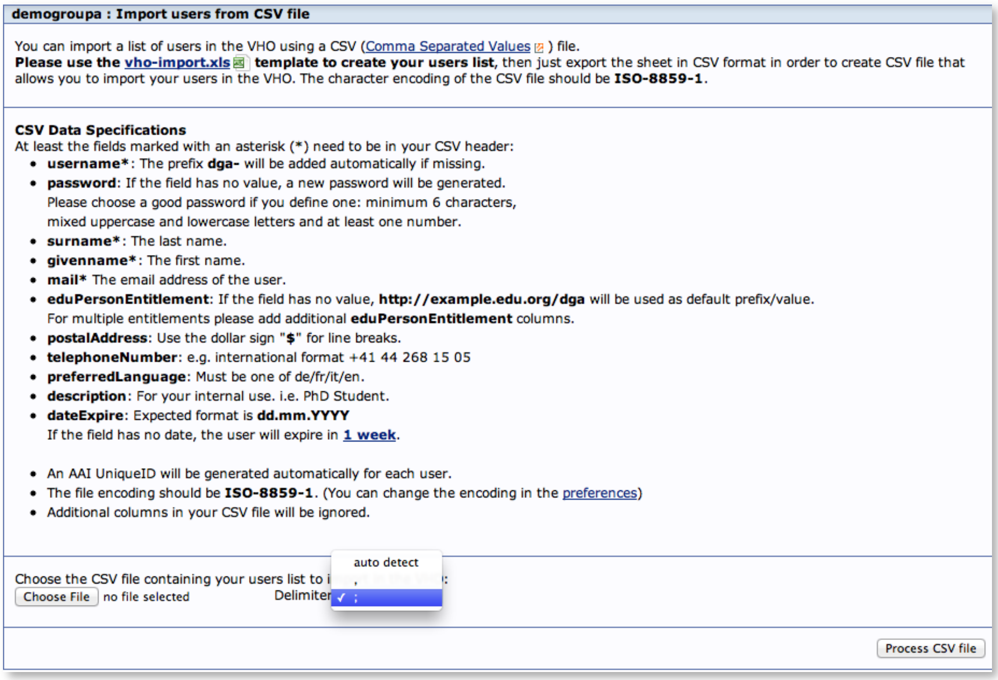
Username:	dga-user06
uniqueID:	d642431@test.vho-switchaai.ch
Last name:	Walker
First name:	William
E-mail:	William.Walker@dga.edu.us
Entitlement:	http://example.edu.org/dga
Business phone number:	+1 4444 333 22 06
Business postal address:	Golden Lane 6 6000 San Francisco
Preferred Language:	en
Affiliation:	affiliate
Home organization:	test.vho-switchaai.ch
Home organization type:	vho
Expiration date:	05.06.2014 14:03:11
Creation date:	09.11.2007 15:48:35
Last modification date:	09.11.2007 15:48:35
Last login date:	07.08.2012 14:03:11

© 2012 SWITCH

11

Screenshots administration tool (3)

...or easy mass user creation by file upload



demogroupa : Import users from CSV file

You can import a list of users in the VHO using a CSV (Comma Separated Values) file.
Please use the vho-import.xls template to create your users list, then just export the sheet in CSV format in order to create CSV file that allows you to import your users in the VHO. The character encoding of the CSV file should be **ISO-8859-1**.

CSV Data Specifications
At least the fields marked with an asterisk (*) need to be in your CSV header:

- **username***: The prefix **dga-** will be added automatically if missing.
- **password**: If the field has no value, a new password will be generated.
  Please choose a good password if you define one: minimum 6 characters, mixed uppercase and lowercase letters and at least one number.
- **surname***: The last name.
- **givenname***: The first name.
- **mail*** The email address of the user.
- **eduPersonEntitlement**: If the field has no value, **http://example.edu.org/dga** will be used as default prefix/value.
  For multiple entitlements please add additional **eduPersonEntitlement** columns.
- **postalAddress**: Use the dollar sign "**$**" for line breaks.
- **telephoneNumber**: e.g. international format +41 44 268 15 05
- **preferredLanguage**: Must be one of de/fr/it/en.
- **description**: For your internal use. i.e. PhD Student.
- **dateExpire**: Expected format is **dd.mm.YYYY**
  If the field has no date, the user will expire in **1 week**.

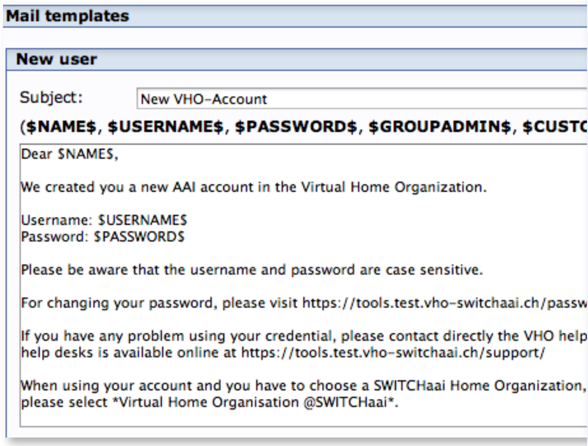
- An AAI UniqueID will be generated automatically for each user.
- The file encoding should be **ISO-8859-1**. (You can change the encoding in the preferences)
- Additional columns in your CSV file will be ignored.

Choose the CSV file containing your users list to i :
Choose File no file selected Delimiter

© 2012 SWITCH

12

Screenshots administration tool (4)



Mail templates

New user

Subject: New VHO-Account

($NAME$, $USERNAME$, $PASSWORD$, $GROUPADMIN$, $CUSTC

Dear $NAME$,

We created you a new AAI account in the Virtual Home Organization.

Username: $USERNAME$
Password: $PASSWORD$

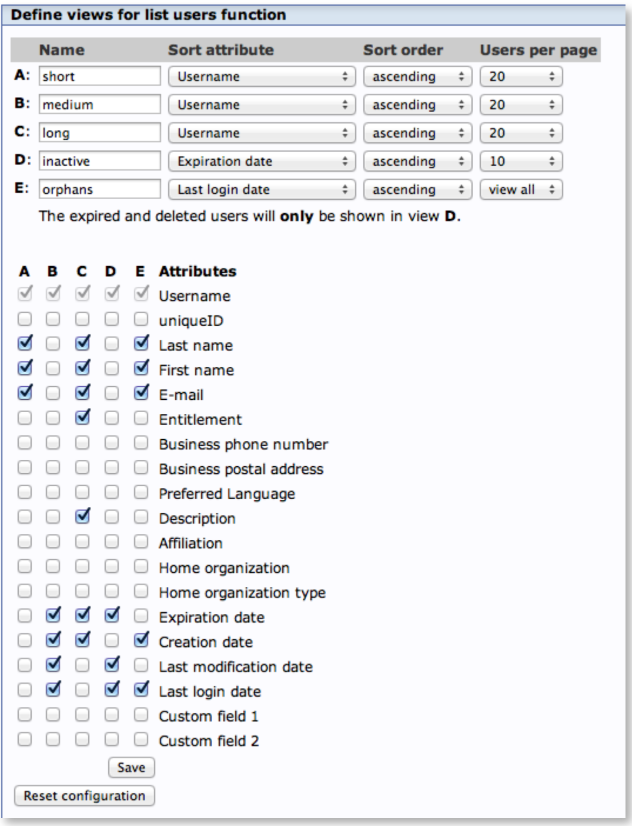
Please be aware that the username and password are case sensitive.

For changing your password, please visit https://tools.test.vho-switchaai.ch/passw

If you have any problem using your credential, please contact directly the VHO help
help desks is available online at https://tools.test.vho-switchaai.ch/support/

When using your account and you have to choose a SWITCHaai Home Organization,
please select *Virtual Home Organisation @SWITCHaai*.

Customize e-mail templates for 'new user' or 'reset password' notifications



Define views for list users function

	Name	Sort attribute	Sort order	Users per page
A:	short	Username	ascending	20
B:	medium	Username	ascending	20
C:	long	Username	ascending	20
D:	inactive	Expiration date	ascending	10
E:	orphans	Last login date	ascending	view all

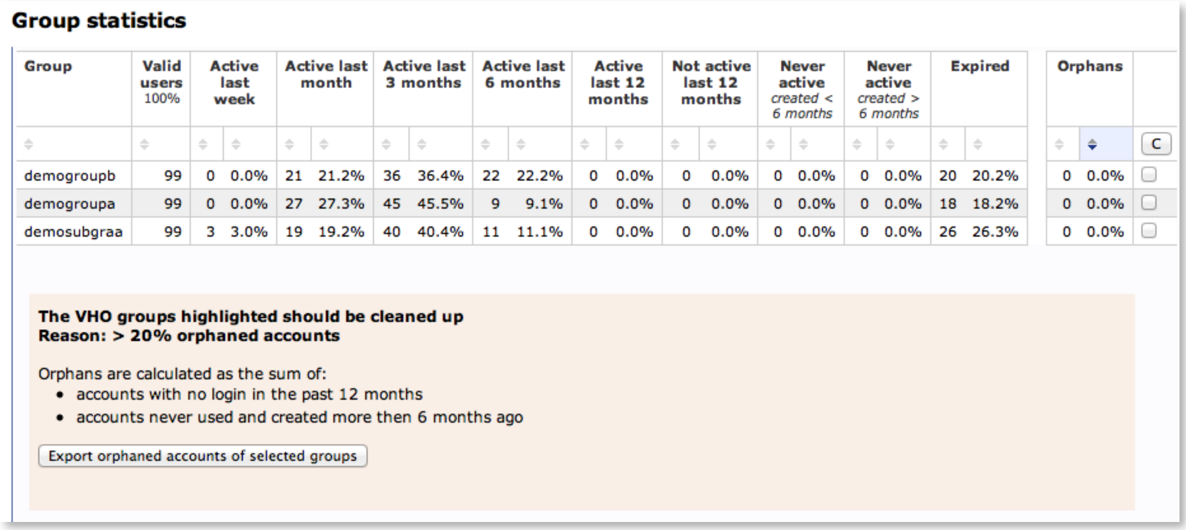
The expired and deleted users will **only** be shown in view **D**.

A	B	C	D	E	Attributes
☑	☑	☑	☑	☑	Username
□	□	□	□	□	uniqueID
☑	□	☑	□	☑	Last name
☑	□	☑	□	☑	First name
☑	□	☑	□	☑	E-mail
□	□	☑	□	□	Entitlement
□	□	□	□	□	Business phone number
□	□	□	□	□	Business postal address
□	□	□	□	□	Preferred Language
□	□	☑	□	□	Description
□	□	□	□	□	Affiliation
□	□	□	□	□	Home organization
□	□	□	□	□	Home organization type
□	☑	☑	☑	□	Expiration date
□	☑	☑	□	☑	Creation date
□	☑	□	☑	□	Last modification date
□	☑	□	☑	☑	Last login date
□	□	□	□	□	Custom field 1
□	□	□	□	□	Custom field 2

Define custom views for the list of users

© 2012 SWITCH

Screenshots administration tool (5)



Group statistics

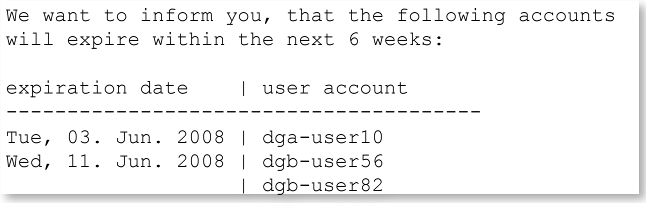
Group	Valid users 100%	Active last week		Active last month		Active last 3 months		Active last 6 months		Active last 12 months		Not active last 12 months		Never active *created < 6 months*		Never active *created > 6 months*		Expired		Orphans		C
demogroupb	99	0	0.0%	21	21.2%	36	36.4%	22	22.2%	0	0.0%	0	0.0%	0	0.0%	0	0.0%	20	20.2%	0	0.0%	☐
demogroupa	99	0	0.0%	27	27.3%	45	45.5%	9	9.1%	0	0.0%	0	0.0%	0	0.0%	0	0.0%	18	18.2%	0	0.0%	☐
demosubgraa	99	3	3.0%	19	19.2%	40	40.4%	11	11.1%	0	0.0%	0	0.0%	0	0.0%	0	0.0%	26	26.3%	0	0.0%	☐

The VHO groups highlighted should be cleaned up
Reason: > 20% orphaned accounts

Orphans are calculated as the sum of:

- accounts with no login in the past 12 months
- accounts never used and created more then 6 months ago

Account expiration reminder notification



```
We want to inform you, that the following accounts
will expire within the next 6 weeks:

expiration date     | user account
---------------------------------------
Tue, 03. Jun. 2008 | dga-user10
Wed, 11. Jun. 2008 | dgb-user56
                   | dgb-user82
```

VHOtools demo access

SWITCH provides a demo access to the VHOtools with some dummy group and user entries.

Try it out yourself!

`https://tools.test.vho-switchaai.ch/`

choose this organisation

`Test Virtual Home Organisation`

use these credentials

```
username: switch-demoadmin(AAITest)
password: demoadmin
```

For further information

http://switch.ch/aai/vho/

Agenda

15

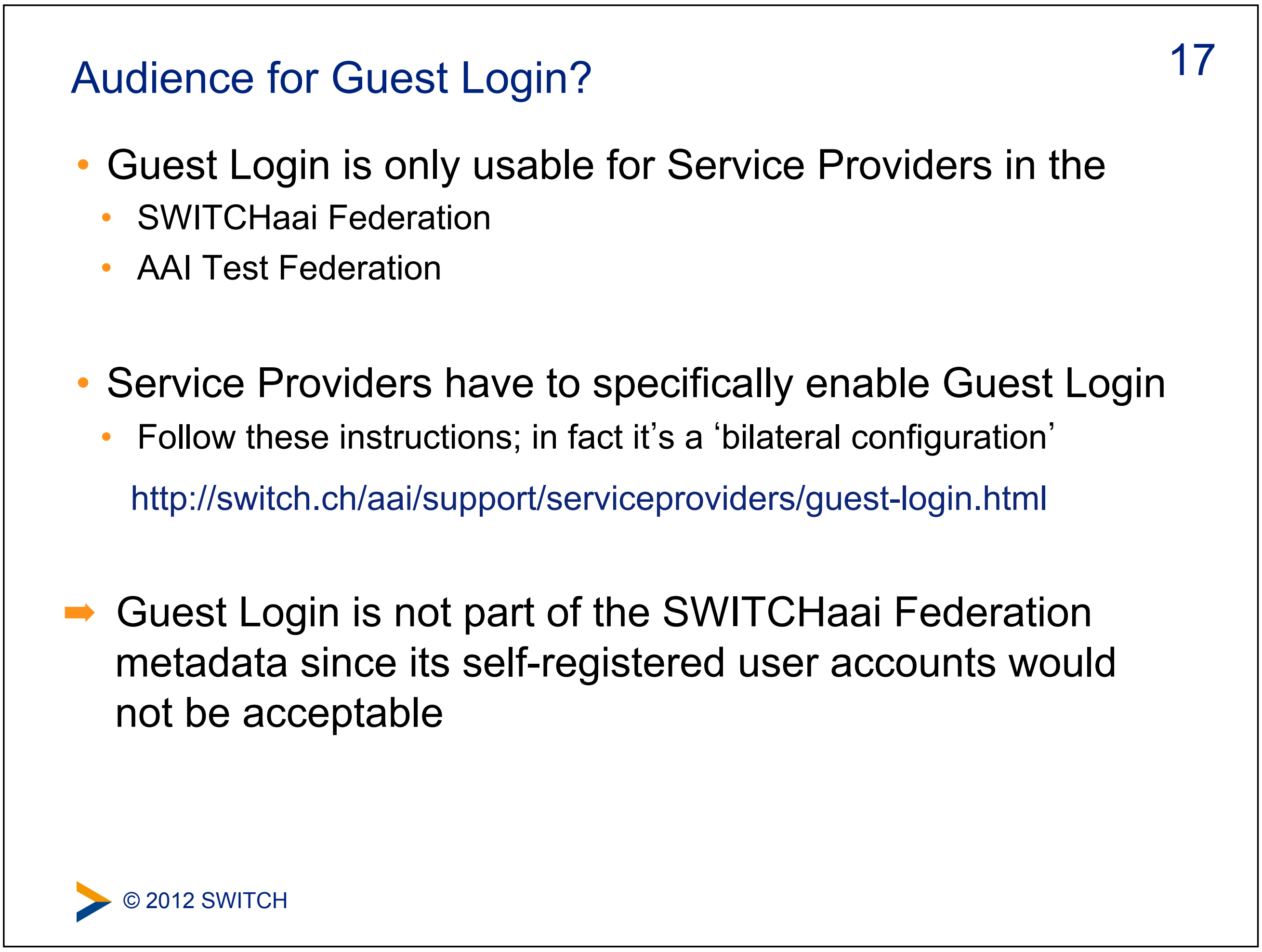
1. Motivation & Context
2. SWITCH VHO Service
3. VHO Administration Tool
4. Guest Login

Why a Guest Login?

16

- Some AAI Services have users from outside the federation
- Resource owner does not want to manage guest accounts in a VHO-group; or doing so would not scale
- Self-registered user accounts with self-provided user attributes are acceptable for the service
  - no verification at all for given name and surname
  - e-mail address only verified on registration

  ➡ Do not rely on the quality of Guest Login user data!
- SWITCH needed a scalable Guest Login for the SWITCHtoolbox service

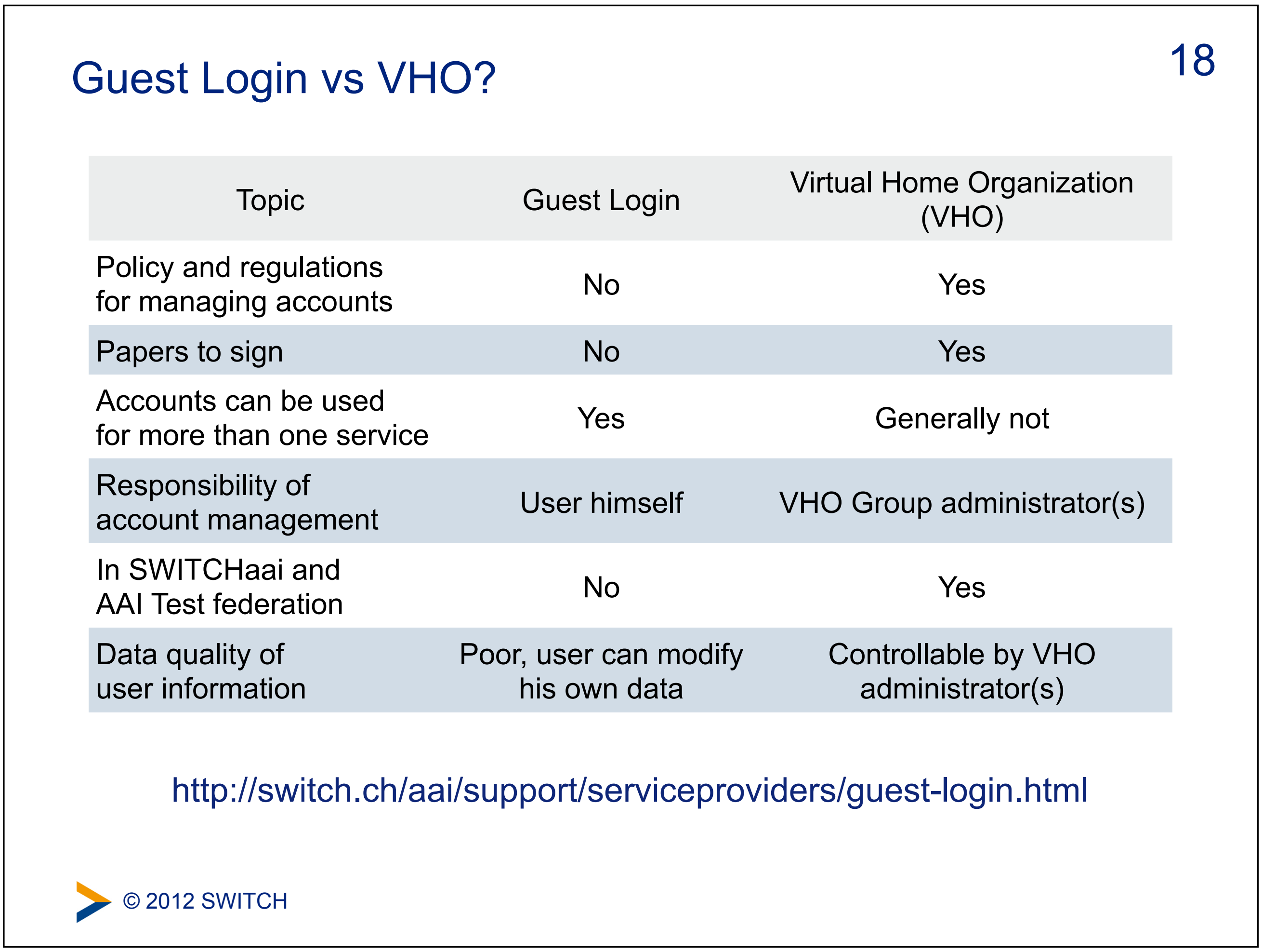


Audience for Guest Login?

- Guest Login is only usable for Service Providers in the
  - SWITCHaai Federation
  - AAI Test Federation
- Service Providers have to specifically enable Guest Login
  - Follow these instructions; in fact it's a 'bilateral configuration'

  http://switch.ch/aai/support/serviceproviders/guest-login.html

➡ Guest Login is not part of the SWITCHaai Federation metadata since its self-registered user accounts would not be acceptable



Guest Login vs VHO?

Topic	Guest Login	Virtual Home Organization (VHO)
Policy and regulations for managing accounts	No	Yes
Papers to sign	No	Yes
Accounts can be used for more than one service	Yes	Generally not
Responsibility of account management	User himself	VHO Group administrator(s)
In SWITCHaai and AAI Test federation	No	Yes
Data quality of user information	Poor, user can modify his own data	Controllable by VHO administrator(s)

http://switch.ch/aai/support/serviceproviders/guest-login.html

Solutions for Access Control

Light weight group management, access control and authorization

SWITCH
Serving Swiss Universities

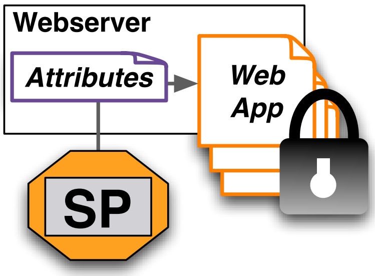
SWITCHaai Team
aai@switch.ch

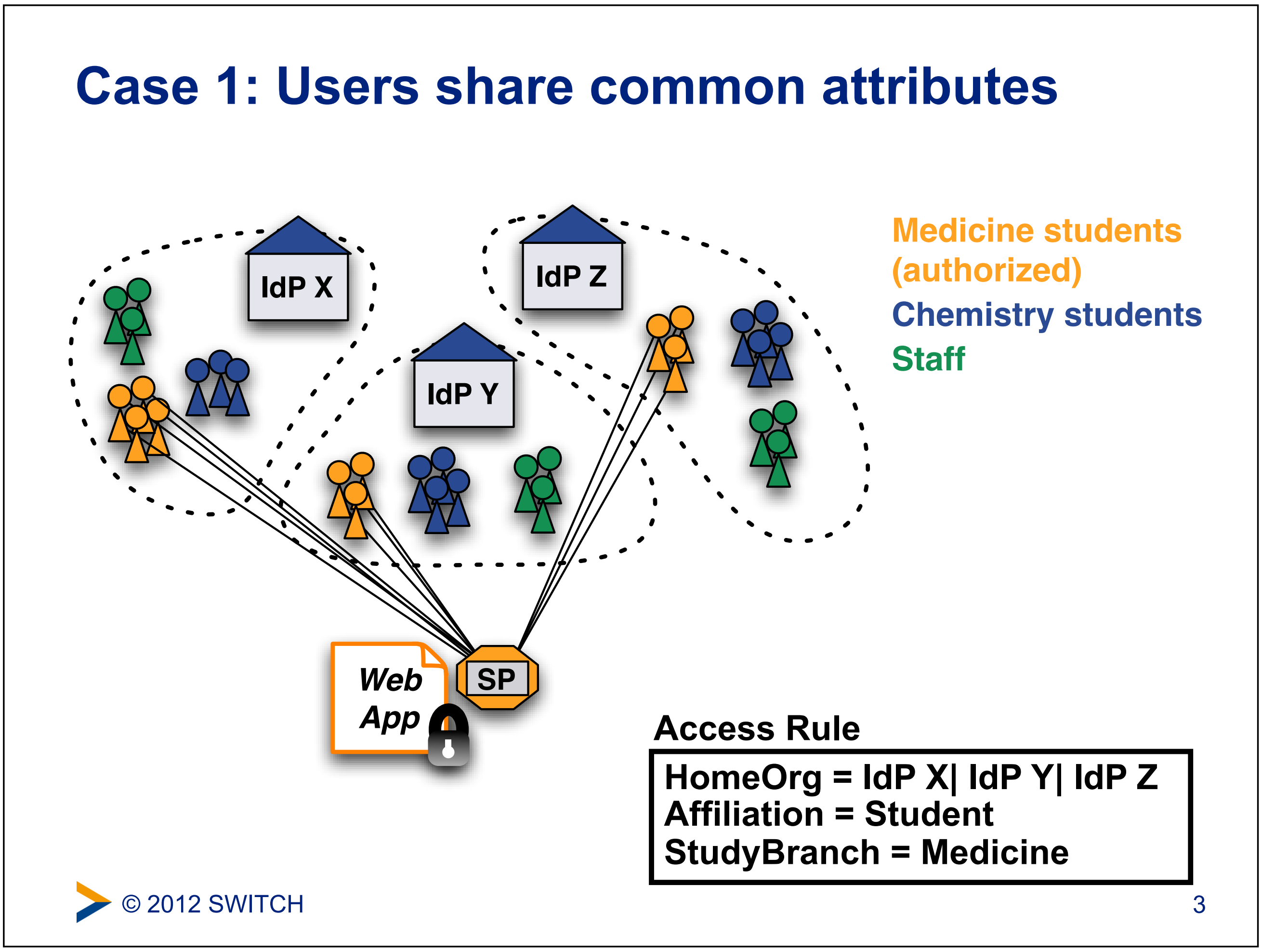
Situation

- Grant access to specific group of people
- All users have an AAI account
- Overhead for group administration should be small

- **Real life example:**

  The slides/photos of this workshop shall only be accessible by all people who attended this meeting.



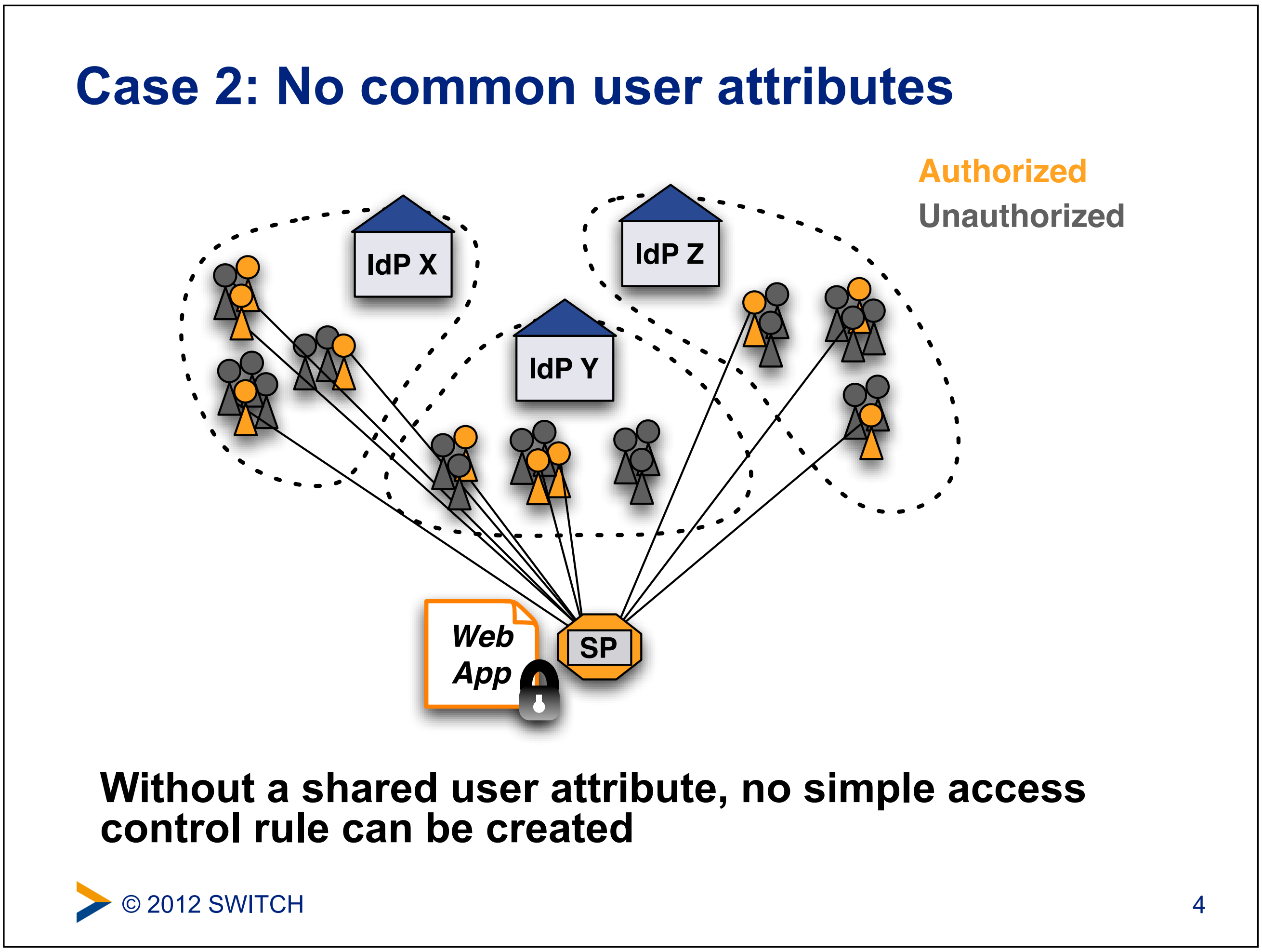


Case 1: Users share common attributes

Medicine students (authorized)
Chemistry students
Staff

Access Rule

HomeOrg = IdP X| IdP Y| IdP Z
Affiliation = Student
StudyBranch = Medicine



Case 2: No common user attributes

Authorized
Unauthorized

Without a shared user attribute, no simple access control rule can be created

Solution 1: Create a common attribute

- Add a common atttribute to user’s identity, e.g. an entitlement attribute

Access Rule

```
Require entitlement urn:mace:rediris.es:entitlement:wiki:jra5
```

⊕
- Very simple solution

⊖
- Additional work for user directory administrator
- Difficult to efficiently manage many entitlement values
- Only IdP admin can manage access
- **Only works for users from same organisation**

Solution 2.a: Use uniqueIDs or email

1. Get unique IDs or (AAI) email addresses from users
2. Create access rules like:

Access Rule

```
require uniqueID 465@idp-x.ch  234@idp-y.ch  […]
require email  hans.muster@idpx.ch pierre.m@idpz.ch […]
```

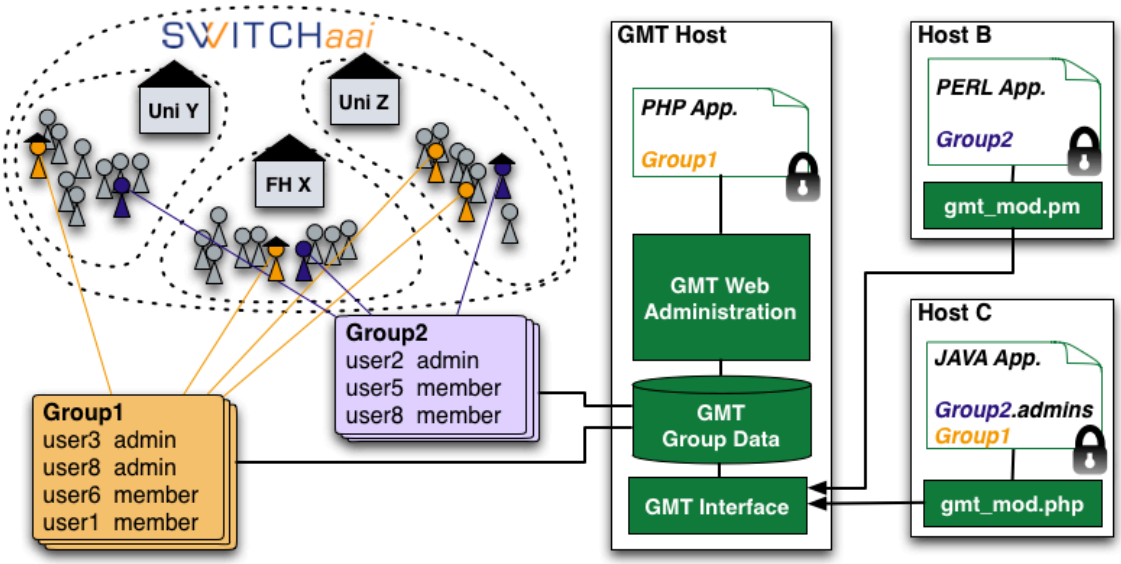
⊕
- Straight-forward solution

⊖
- SP administrator must know unique ID/Email address
- Difficult to efficiently manage for many users/apps
- **Only SP admin can manage access**

Solution 2.b: Group Management Tool

- Web based OpenSource PHP tool develop by SWITCH
- Manages multiple groups to protect multiple applications
- Users can be:
  - Invited to a group via email
  - Added to a group with a password
  - Added to a group based on their attributes
  - Moderated after they request to join a group
- GMT generates authorization files (Apache and Shibboleth)
  - Only works same host as GMT
- API and libraries for authorization on remote hosts

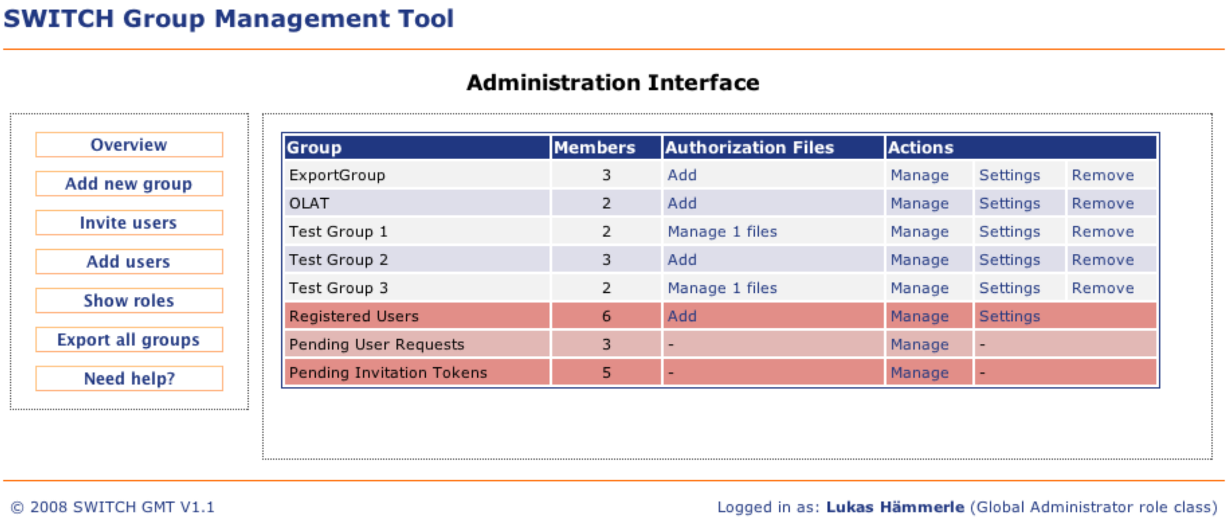
GMT Overview



Group2
user2 admin
user5 member
user8 member

Group1
user3 admin
user8 admin
user6 member
user1 member

GMT Administration Interface



SWITCH Group Management Tool

Administration Interface

- Overview
- Add new group
- Invite users
- Add users
- Show roles
- Export all groups
- Need help?

Group	Members	Authorization Files	Actions		
ExportGroup	3	Add	Manage	Settings	Remove
OLAT	2	Add	Manage	Settings	Remove
Test Group 1	2	Manage 1 files	Manage	Settings	Remove
Test Group 2	3	Add	Manage	Settings	Remove
Test Group 3	2	Manage 1 files	Manage	Settings	Remove
Registered Users	6	Add	Manage	Settings	
Pending User Requests	3	-	Manage	-	
Pending Invitation Tokens	5	-	Manage	-	

© 2008 SWITCH GMT V1.1

Logged in as: **Lukas Hämmerle** (Global Administrator role class)

GMT Authorization File Example

- Multiple groups can write to same authorization file
- Example of an .htaccess file

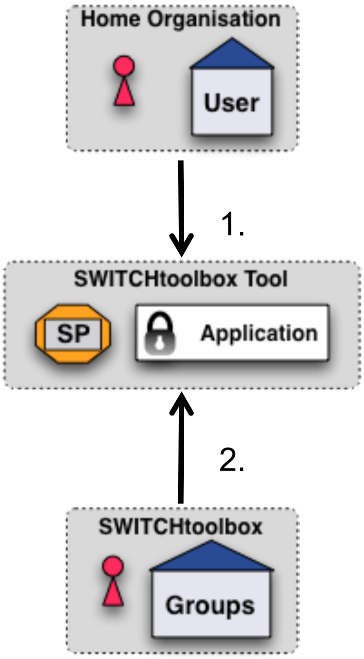
```
# Group Management Tool: Apache Authorization File
# DON'T EDIT LINES THAT CONTAIN ###
# AND ALSO DON'T REMOVE THE FOLLOWING TWO DIRECTIVES
AuthType shibboleth
ShibRequireSession On

require placeholder never.match

###START:Test_Group_1###
require uniqueID 023sdf-345fdg-23401@unizh.ch
require uniqueID 3141324sdd592@ethz.ch
###END:Test_Group_1###
```

Solution 2.c: SWITCHtoolbox

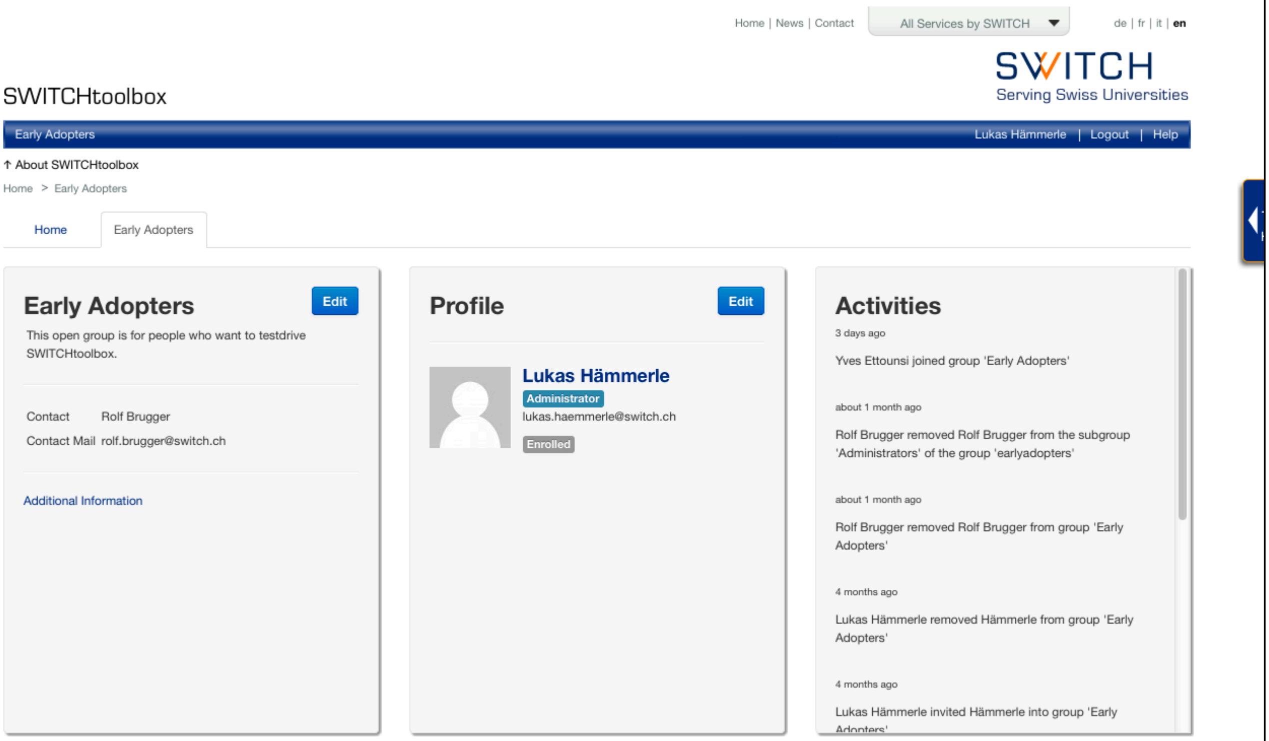
- Service Provider aggregates:
  - identity information from users's IdP
  - group information from SWITCHtoolbox IdP
- Application receives group membership information like any other Shibboleth attribute
- Everybody can create groups
- Allows easy access control rules



Access Rule

require isMemberOf https://toolbox.switch.ch/mygroup

SWITCHtoolbox Administration



Early Adopters

This open group is for people who want to testdrive SWITCHtoolbox.

Contact	Rolf Brugger
Contact Mail	rolf.brugger@switch.ch

Additional Information

Profile

Lukas Hämmerle

lukas.haemmerle@switch.ch

Activities

3 days ago

Yves Ettounsi joined group 'Early Adopters'

about 1 month ago

Rolf Brugger removed Rolf Brugger from the subgroup 'Administrators' of the group 'earlyadopters'

about 1 month ago

Rolf Brugger removed Rolf Brugger from group 'Early Adopters'

4 months ago

Lukas Hämmerle removed Hämmerle from group 'Early Adopters'

4 months ago

Lukas Hämmerle invited Hämmerle into group 'Early Adopters'

Add a Service as Tool

- SP needs only minor configuration change to be tool
- Tool can be public or private
  - Public tools can be subscribed/accessed by many different groups
- SWITCH offers already three public tools:
  - Wiki, Document Storage, Mailinglist
- Webpage: http://www.switch.ch/toolbox/

Summary

- GMT and SWITCHtoolbox are very similar
- GMT has to be installed and maintained yourself
  - Allows customization
  - Suited for few groups with few users
  - Only protects applications on same host or requires libraries
- SWITCHtoolbox is a service offered by SWITCH
  - Allows easier integration of application
  - Can manage hundreds of groups and sub groups
  - No software libraries required to protect remote applications
  - Multilingual
- **SWITCHtoolbox recommended in the long term!**

Service Provider Virtualization

Running multiple SPs on a single host

SWITCH

Serving Swiss Universities

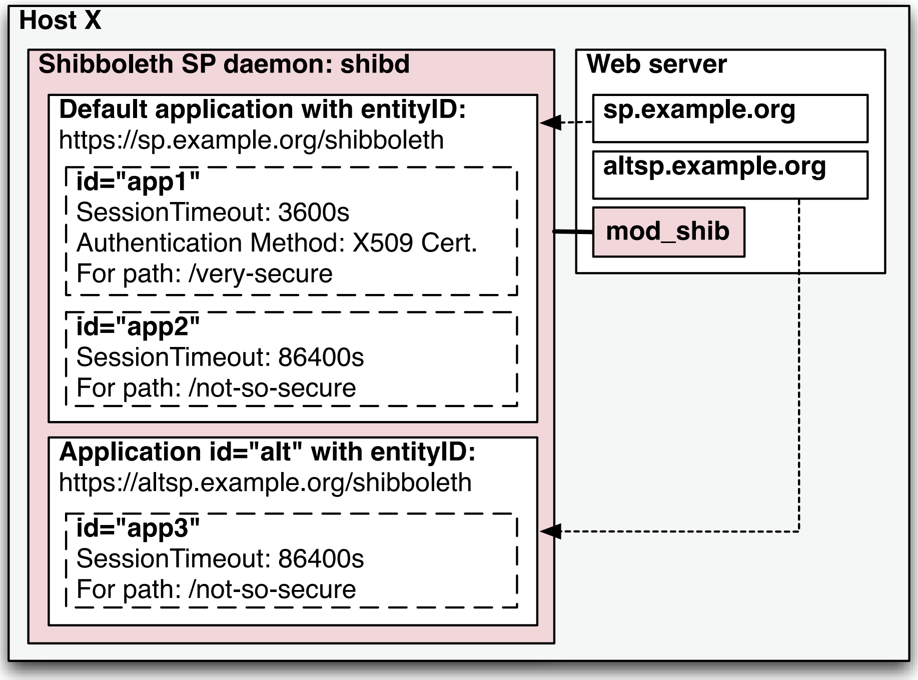
Kaspar Brand
aai@switch.ch

Physical vs. logical SP

A single physical SP can host any number of logical SPs

- A logical SP can then include any number of “applications”
- Applications can be configured on a per-path or per-virtual-host basis
- Web virtual hosting is often related but is also independent
- Applications can inherit or override default configuration settings on a piecemeal basis

Multiple applications and domains on a single host



shibboleth2.xml configuration

Add an **`ApplicationOverride`** element for each logical SP, and specify its own **`CredentialResolver`**:

```
<ApplicationDefaults id="default" policyId="default" ... >
  ...
  <ApplicationOverride id="altsp”
        entityID="https://altsp#.example.org/shibboleth">
    <CredentialResolver type="File"
        key="/etc/shibboleth/altsp-key.pem"
        certificate="/etc/shibboleth/altsp-cert.pem"/>
  </ApplicationOverride>
</ApplicationDefaults>
```

Note: when adding a customized **`Sessions`** element to the **`ApplicationOverride`**, be sure to spell out *all* its attributes (inheritance from **`ApplicationDefaults`** is disabled as soon as a **`Sessions`** element is present).

Apache httpd configuration

Define an additional **`VirtualHost`** for the logical SP, and map it to the respective **`ApplicationOverride`** from shibboleth2.xml:

```
<VirtualHost *:443>
  ServerName altsp#.example.org:443
  ...

  <Location />
    ShibRequestSetting applicationId altsp
  </Location>

</VirtualHost>
```

Recommendations

- use separate Apache **`VirtualHosts`** / IIS sites to run multiple, but distinct AAI-protected resources on a single host (avoid path-based separation of applications)
- define separate entity IDs for each resource, and create key pairs (self-signed certificates) for each of them
- register and manage each resource / logical SP in the AAI RR as a separate entity with its respective attribute requirements
- Further reading:
  https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPApplicationOverride

SP Hands-on Session

Installing and Configuring a Shibboleth 2 Service Provider

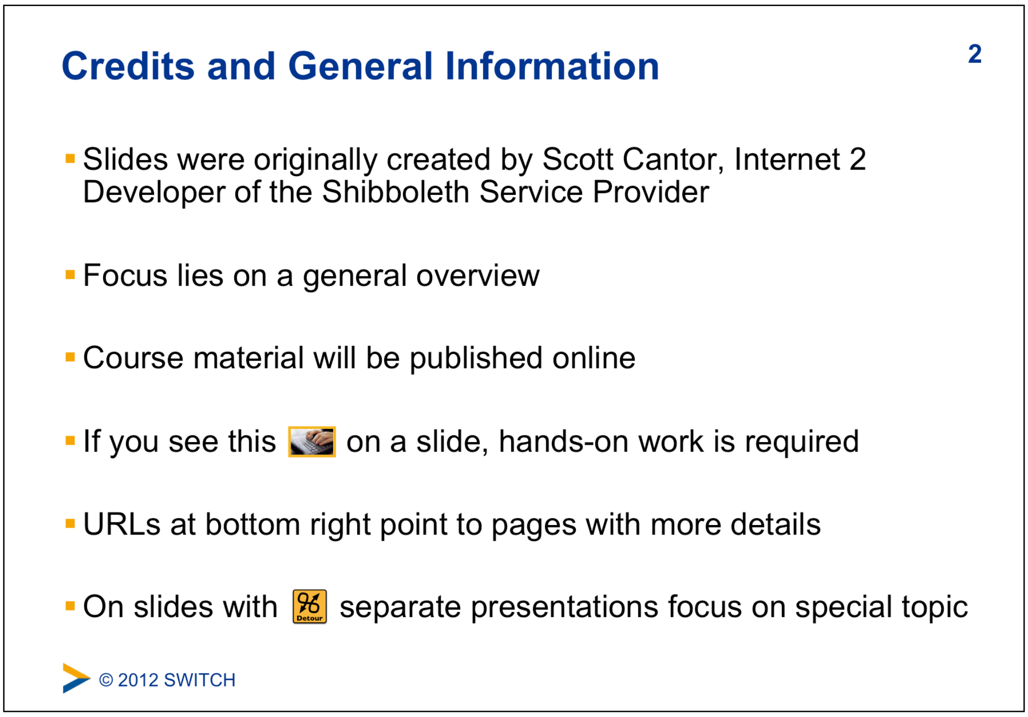
SWITCH
Serving Swiss Universities

Notes: ____

____

____

____



Credits and General Information

2

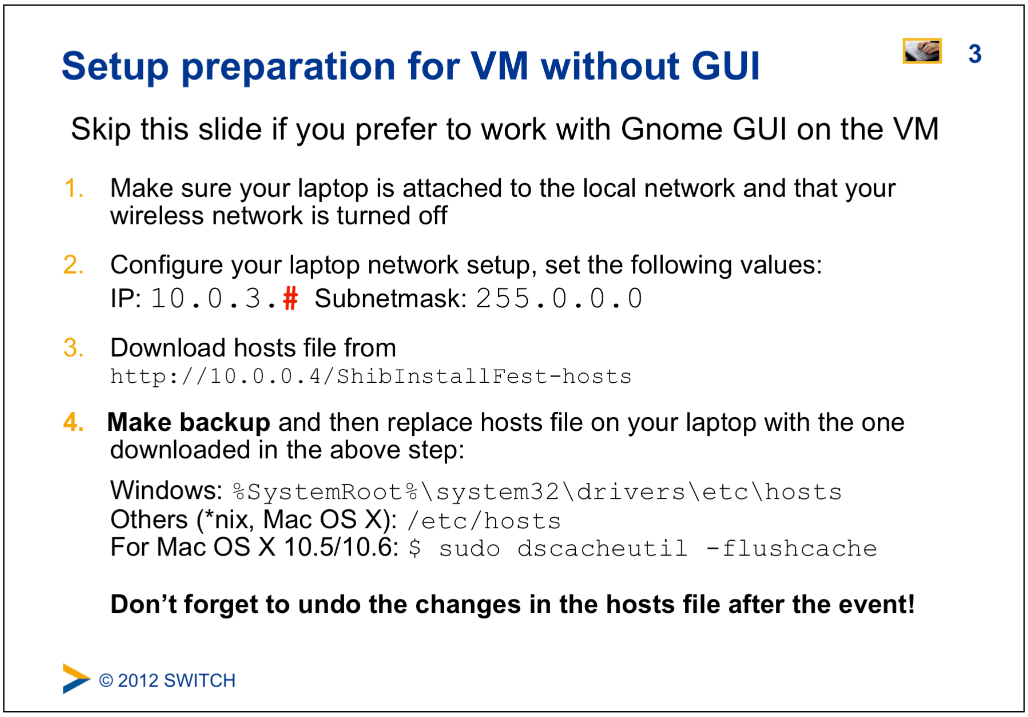
- Slides were originally created by Scott Cantor, Internet 2 Developer of the Shibboleth Service Provider
- Focus lies on a general overview
- Course material will be published online
- If you see this ⌨ on a slide, hands-on work is required
- URLs at bottom right point to pages with more details
- On slides with Detour separate presentations focus on special topic

Notes: ____

____

____

____



Setup preparation for VM without GUI

3

Skip this slide if you prefer to work with Gnome GUI on the VM

1. Make sure your laptop is attached to the local network and that your wireless network is turned off
2. Configure your laptop network setup, set the following values:
   IP: `10.0.3.#` Subnetmask: `255.0.0.0`
3. Download hosts file from
   `http://10.0.0.4/ShibInstallFest-hosts`
4. **Make backup** and then replace hosts file on your laptop with the one downloaded in the above step:

   Windows: `%SystemRoot%\system32\drivers\etc\hosts`
   Others (*nix, Mac OS X): `/etc/hosts`
   For Mac OS X 10.5/10.6: `$ sudo dscacheutil -flushcache`

   Don't forget to undo the changes in the hosts file after the event!

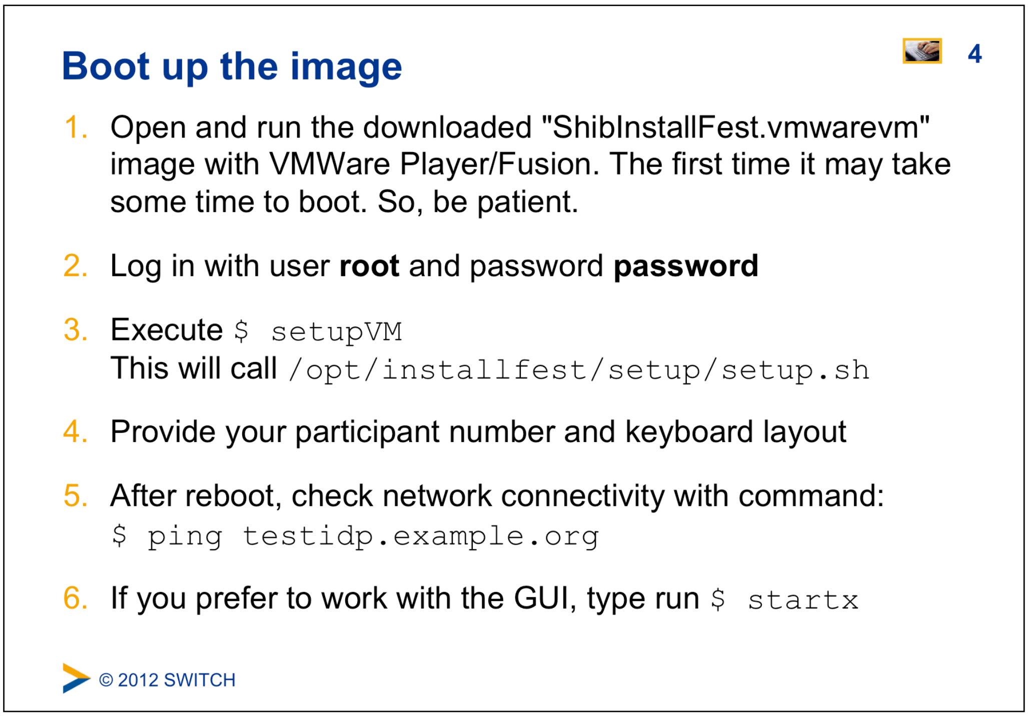
© 2012 SWITCH

Notes: ______________________________

____

____

____



Boot up the image

4

1. Open and run the downloaded "ShibInstallFest.vmwarevm" image with VMWare Player/Fusion. The first time it may take some time to boot. So, be patient.
2. Log in with user **root** and password **password**
3. Execute `$ setupVM`
   This will call `/opt/installfest/setup/setup.sh`
4. Provide your participant number and keyboard layout
5. After reboot, check network connectivity with command:
   `$ ping testidp.example.org`
6. If you prefer to work with the GUI, type run `$ startx`

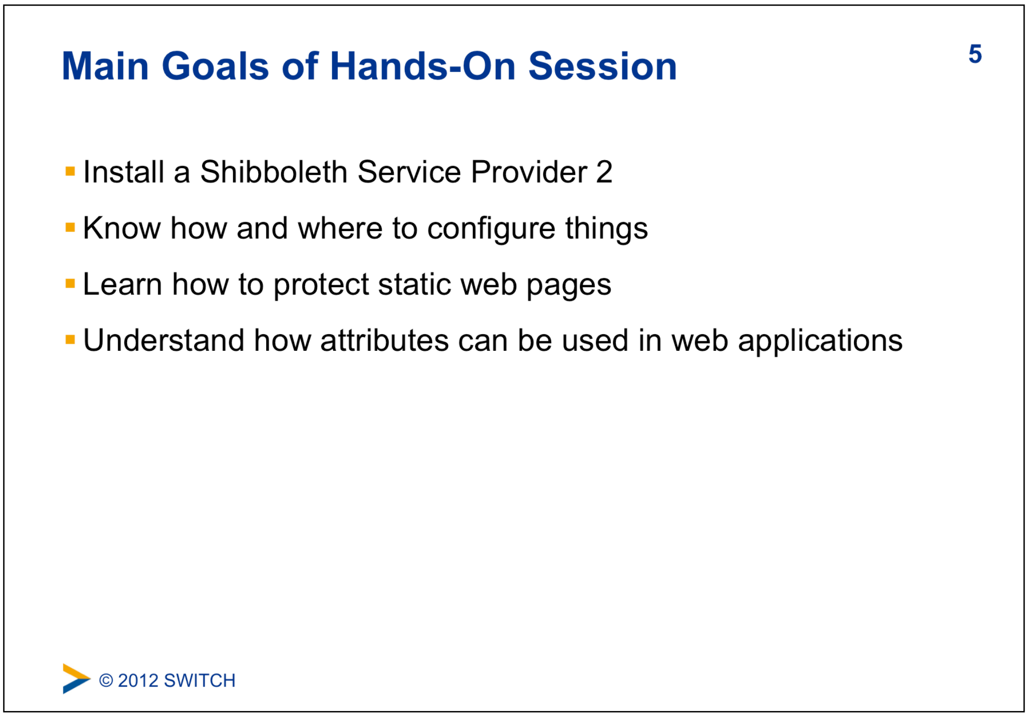
© 2012 SWITCH

Notes: ______________________________

____

____

____



Main Goals of Hands-On Session

5

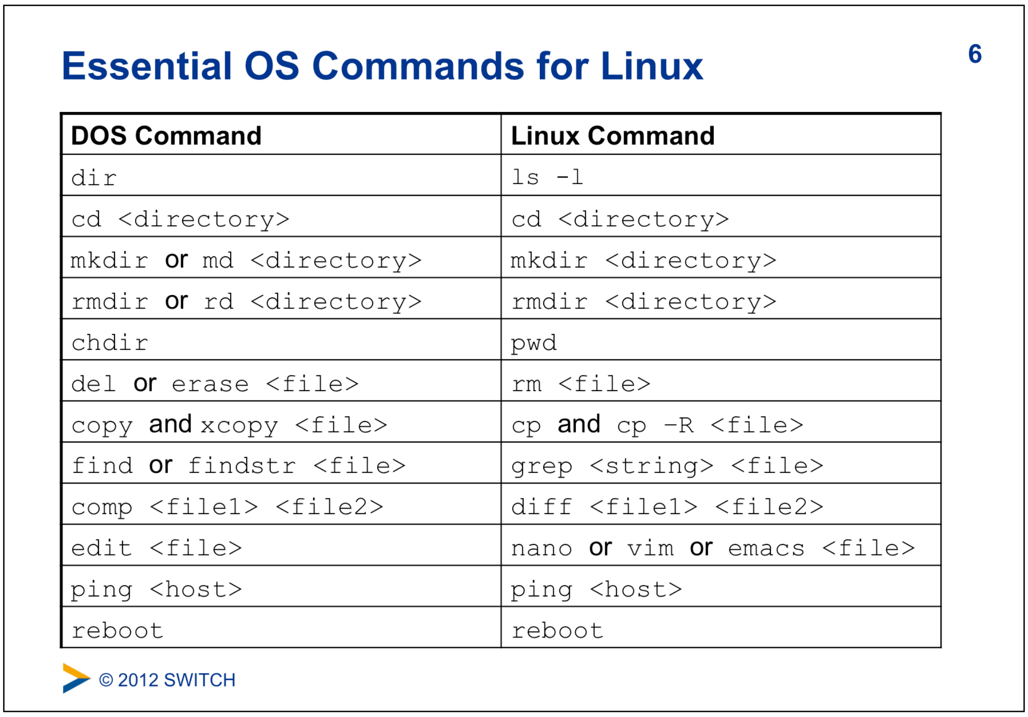
- Install a Shibboleth Service Provider 2
- Know how and where to configure things
- Learn how to protect static web pages
- Understand how attributes can be used in web applications

Notes: ______________________________

____

____

____



Essential OS Commands for Linux

6

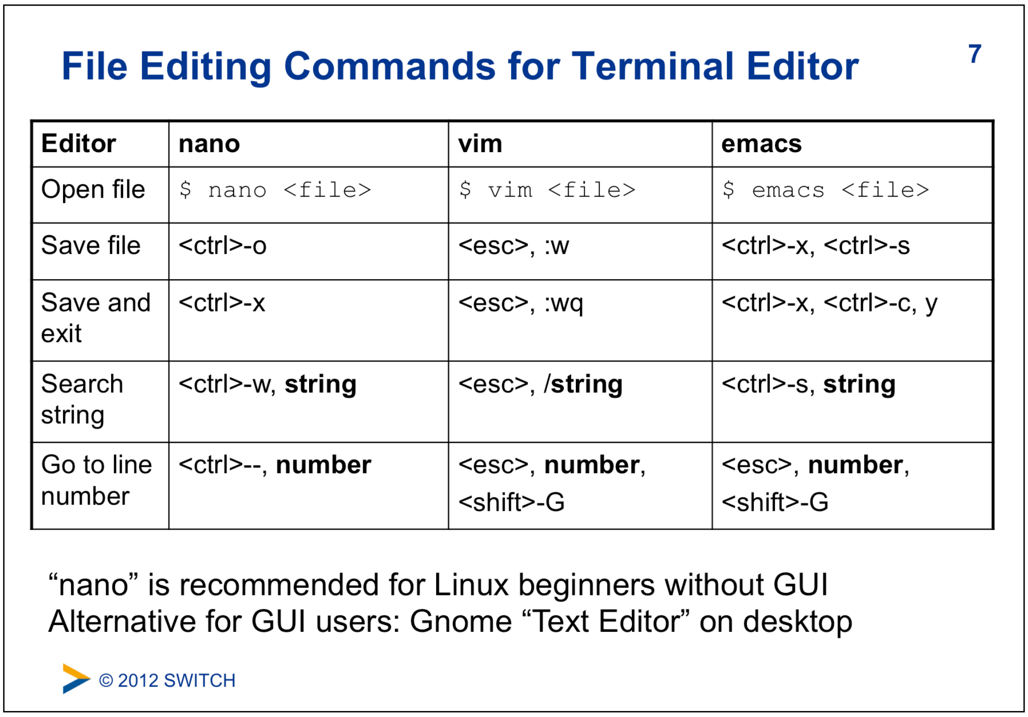
DOS Command	Linux Command
`dir`	`ls -l`
`cd <directory>`	`cd <directory>`
`mkdir` or `md <directory>`	`mkdir <directory>`
`rmdir` or `rd <directory>`	`rmdir <directory>`
`chdir`	`pwd`
`del` or `erase <file>`	`rm <file>`
`copy` and `xcopy <file>`	`cp` and `cp -R <file>`
`find` or `findstr <file>`	`grep <string> <file>`
`comp <file1> <file2>`	`diff <file1> <file2>`
`edit <file>`	`nano` or `vim` or `emacs <file>`
`ping <host>`	`ping <host>`
`reboot`	`reboot`

Notes: ______________________________

____

____

____



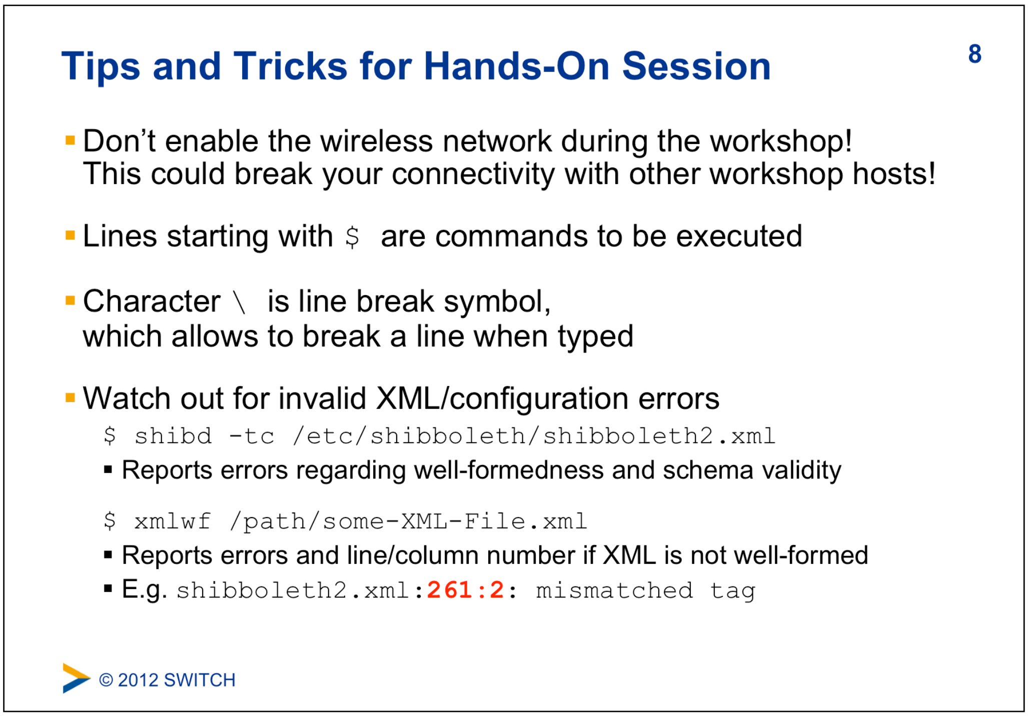
File Editing Commands for Terminal Editor

7

Editor	nano	vim	emacs
Open file	`$ nano <file>`	`$ vim <file>`	`$ emacs <file>`
Save file	<ctrl>-o	<esc>, :w	<ctrl>-x, <ctrl>-s
Save and exit	<ctrl>-x	<esc>, :wq	<ctrl>-x, <ctrl>-c, y
Search string	<ctrl>-w, **string**	<esc>, /**string**	<ctrl>-s, **string**
Go to line number	<ctrl>--, **number**	<esc>, **number**, <shift>-G	<esc>, **number**, <shift>-G

“nano” is recommended for Linux beginners without GUI
Alternative for GUI users: Gnome “Text Editor” on desktop

Notes: ____



Tips and Tricks for Hands-On Session

8

- Don’t enable the wireless network during the workshop!
  This could break your connectivity with other workshop hosts!
- Lines starting with `$` are commands to be executed
- Character `\` is line break symbol,
  which allows to break a line when typed
- Watch out for invalid XML/configuration errors

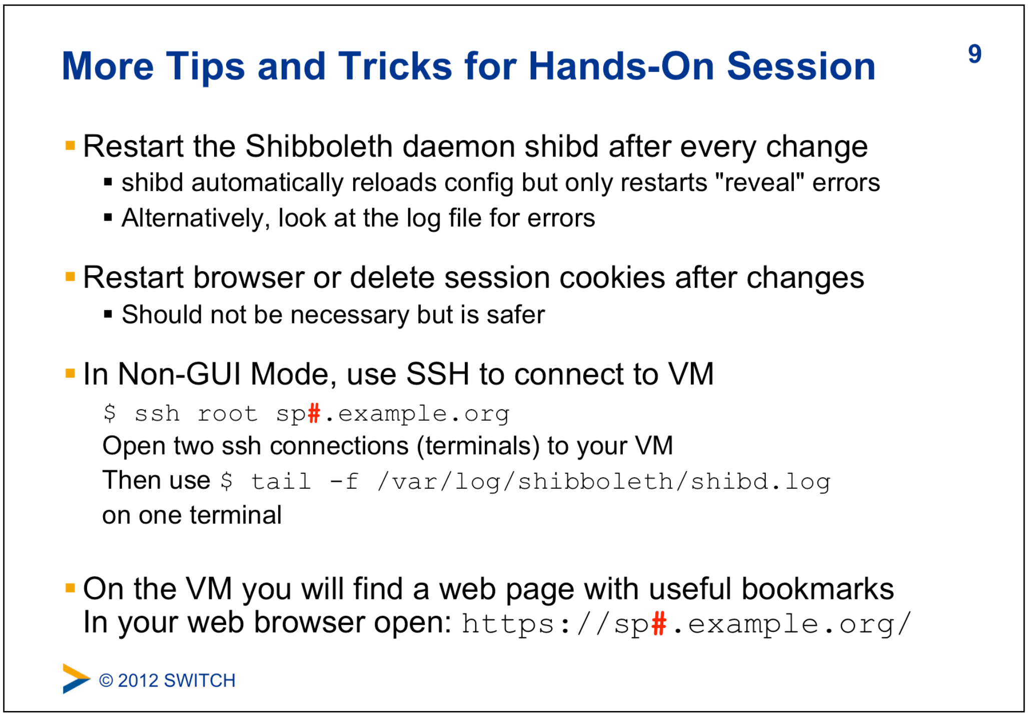
```
$ shibd -tc /etc/shibboleth/shibboleth2.xml
```

  - Reports errors regarding well-formedness and schema validity

```
$ xmlwf /path/some-XML-File.xml
```

  - Reports errors and line/column number if XML is not well-formed
  - E.g. `shibboleth2.xml:`**`261:2`**`: mismatched tag`

Notes: ____



More Tips and Tricks for Hands-On Session

9

- Restart the Shibboleth daemon shibd after every change
  - shibd automatically reloads config but only restarts "reveal" errors
  - Alternatively, look at the log file for errors
- Restart browser or delete session cookies after changes
  - Should not be necessary but is safer
- In Non-GUI Mode, use SSH to connect to VM

  ```
  $ ssh root sp#.example.org
  ```

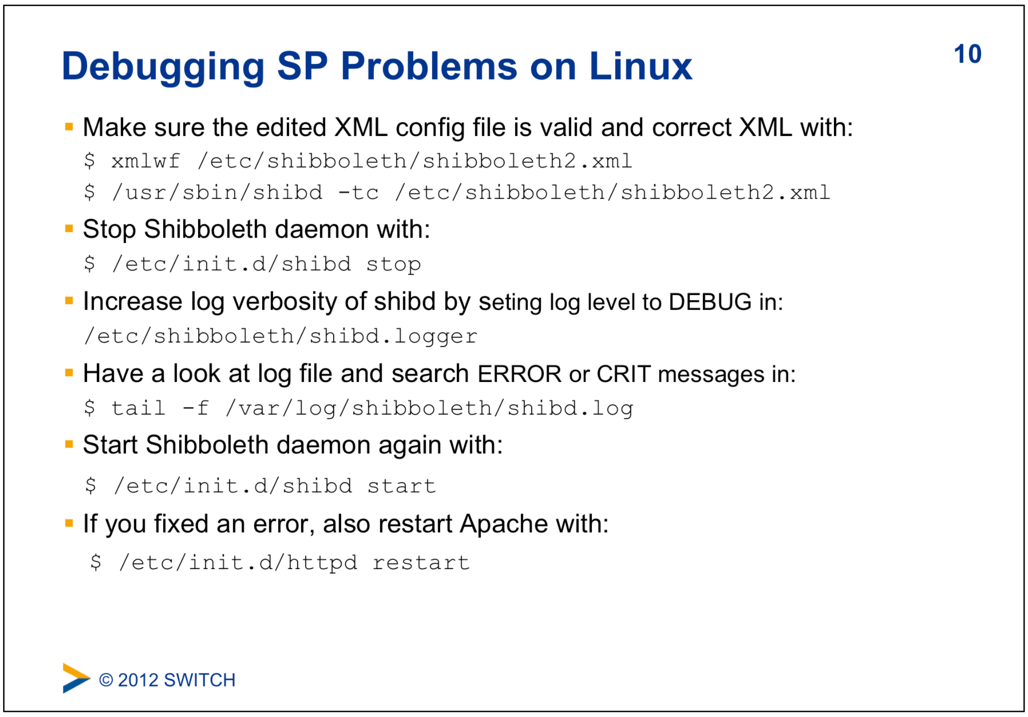
  Open two ssh connections (terminals) to your VM
  Then use `$ tail -f /var/log/shibboleth/shibd.log`
  on one terminal
- On the VM you will find a web page with useful bookmarks
  In your web browser open: `https://sp#.example.org/`

Notes: ____

____

____

____



Debugging SP Problems on Linux

10

- Make sure the edited XML config file is valid and correct XML with:

  ```
  $ xmlwf /etc/shibboleth/shibboleth2.xml
  $ /usr/sbin/shibd -tc /etc/shibboleth/shibboleth2.xml
  ```
- Stop Shibboleth daemon with:

  ```
  $ /etc/init.d/shibd stop
  ```
- Increase log verbosity of shibd by seting log level to DEBUG in:
  `/etc/shibboleth/shibd.logger`
- Have a look at log file and search ERROR or CRIT messages in:

  ```
  $ tail -f /var/log/shibboleth/shibd.log
  ```
- Start Shibboleth daemon again with:

  ```
  $ /etc/init.d/shibd start
  ```
- If you fixed an error, also restart Apache with:

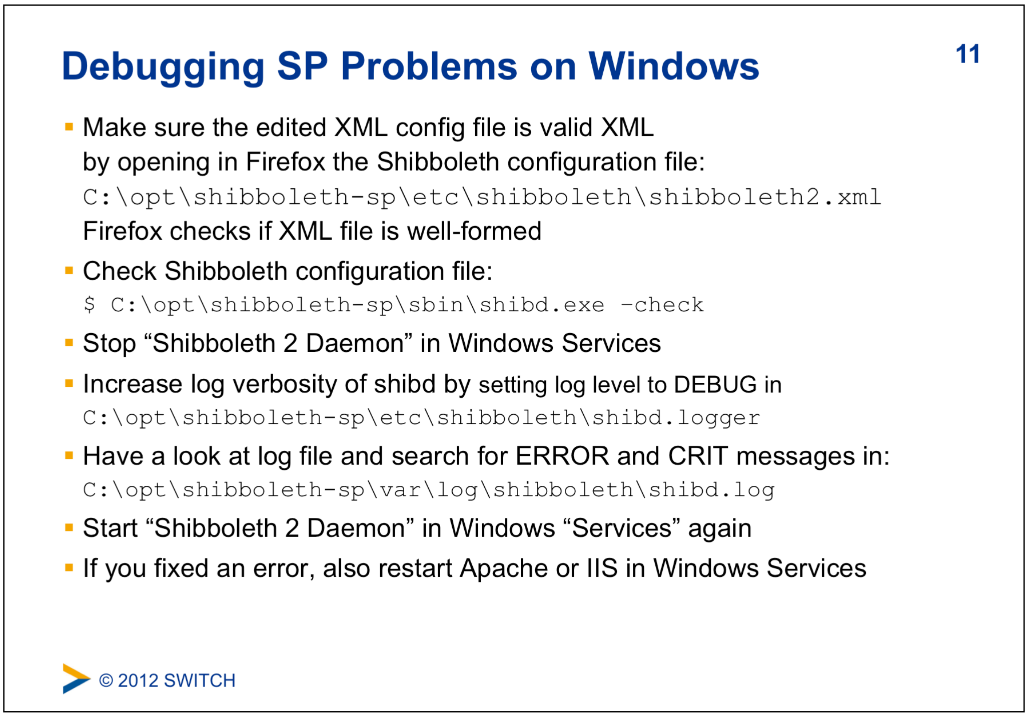
  ```
  $ /etc/init.d/httpd restart
  ```

Notes: ____

____

____

____



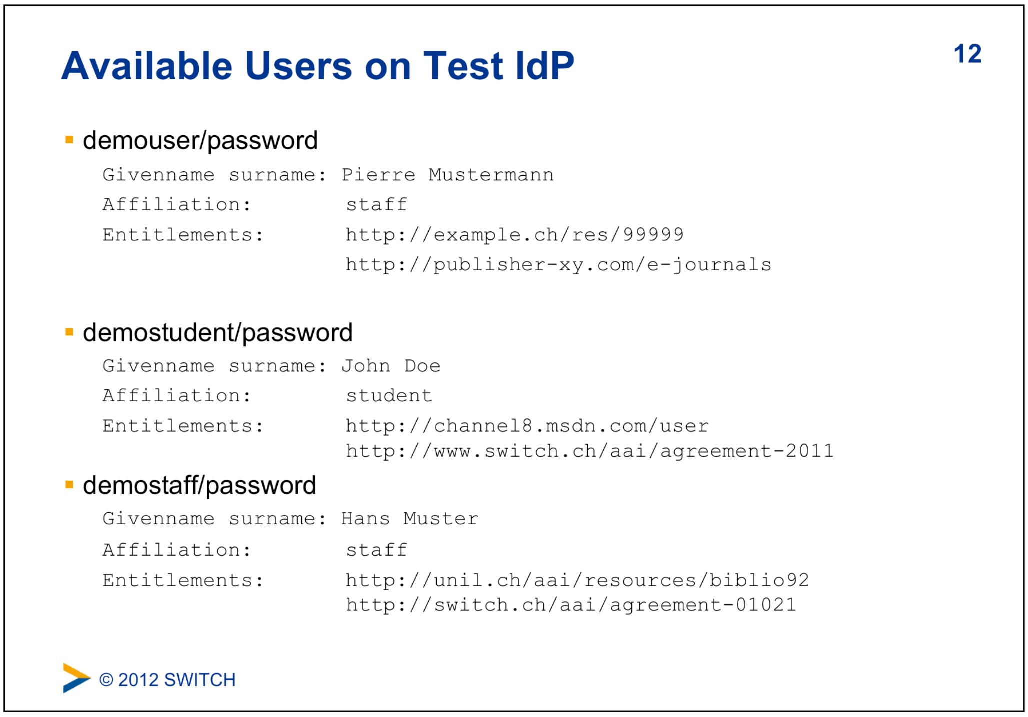
Debugging SP Problems on Windows

11

- Make sure the edited XML config file is valid XML by opening in Firefox the Shibboleth configuration file:
  ```
  C:\opt\shibboleth-sp\etc\shibboleth\shibboleth2.xml
  ```
  Firefox checks if XML file is well-formed
- Check Shibboleth configuration file:
  ```
  $ C:\opt\shibboleth-sp\sbin\shibd.exe -check
  ```
- Stop “Shibboleth 2 Daemon” in Windows Services
- Increase log verbosity of shibd by setting log level to DEBUG in
  ```
  C:\opt\shibboleth-sp\etc\shibboleth\shibd.logger
  ```
- Have a look at log file and search for ERROR and CRIT messages in:
  ```
  C:\opt\shibboleth-sp\var\log\shibboleth\shibd.log
  ```
- Start “Shibboleth 2 Daemon” in Windows “Services” again
- If you fixed an error, also restart Apache or IIS in Windows Services

© 2012 SWITCH

Notes:



Available Users on Test IdP

12

- demouser/password
  ```
  Givenname surname: Pierre Mustermann
  Affiliation:        staff
  Entitlements:       http://example.ch/res/99999
                      http://publisher-xy.com/e-journals
  ```
- demostudent/password
  ```
  Givenname surname: John Doe
  Affiliation:        student
  Entitlements:       http://channel8.msdn.com/user
                      http://www.switch.ch/aai/agreement-2011
  ```
- demostaff/password
  ```
  Givenname surname: Hans Muster
  Affiliation:        staff
  Entitlements:       http://unil.ch/aai/resources/biblio92
                      http://switch.ch/aai/agreement-01021
  ```

© 2012 SWITCH

Notes:

SP Overview and Installation

13

Goals:

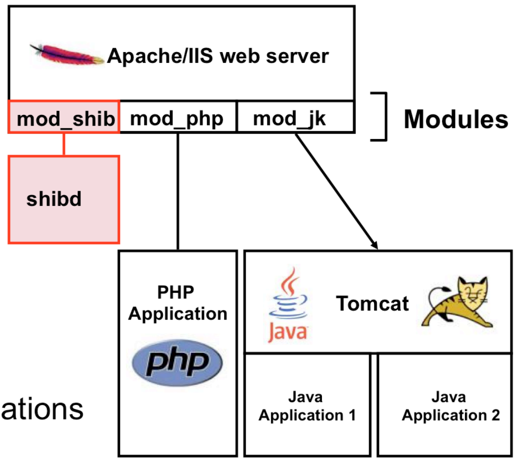
1. Terminology and SP Overview
2. Installation and Directory Structure
3. Generating Key and Certificate
4. Quick Sanity Check
5. Picking an entityID

Notes:

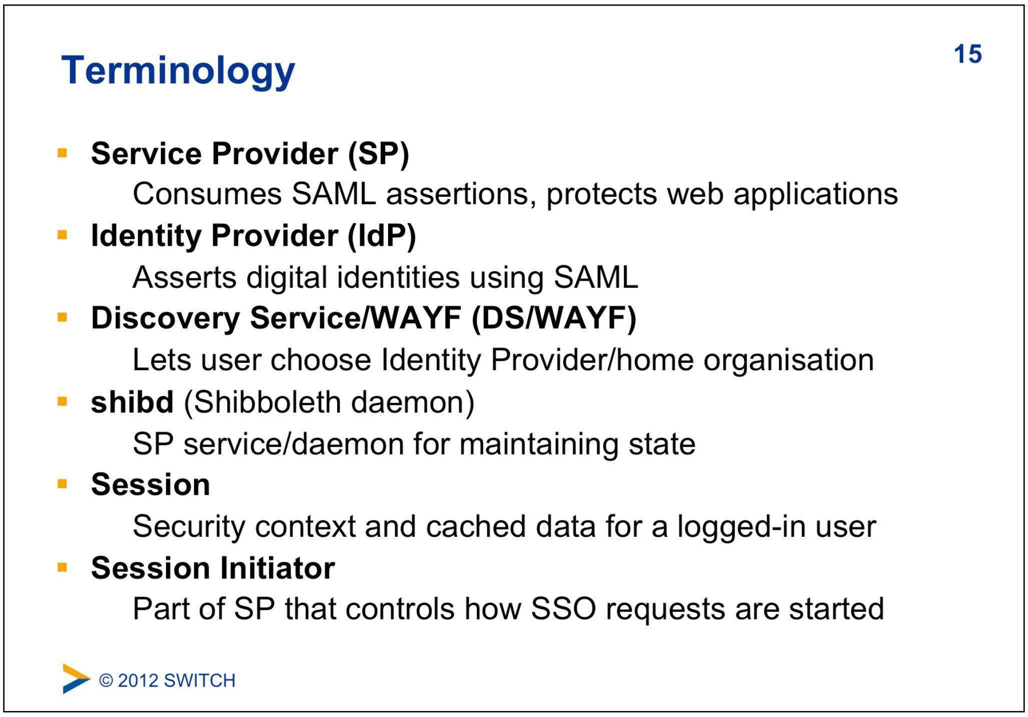
SP: Daemon & mod_shib

14

- Runs on: Linux, Solaris, Windows, Mac OS X, FreeBSD, …
- Protects web applications
- shibd processes attributes
- Can authorize users with
  - Apache directives
  - Shibboleth XML Access rules
- Provides attributes to applications



Notes:



Terminology

15

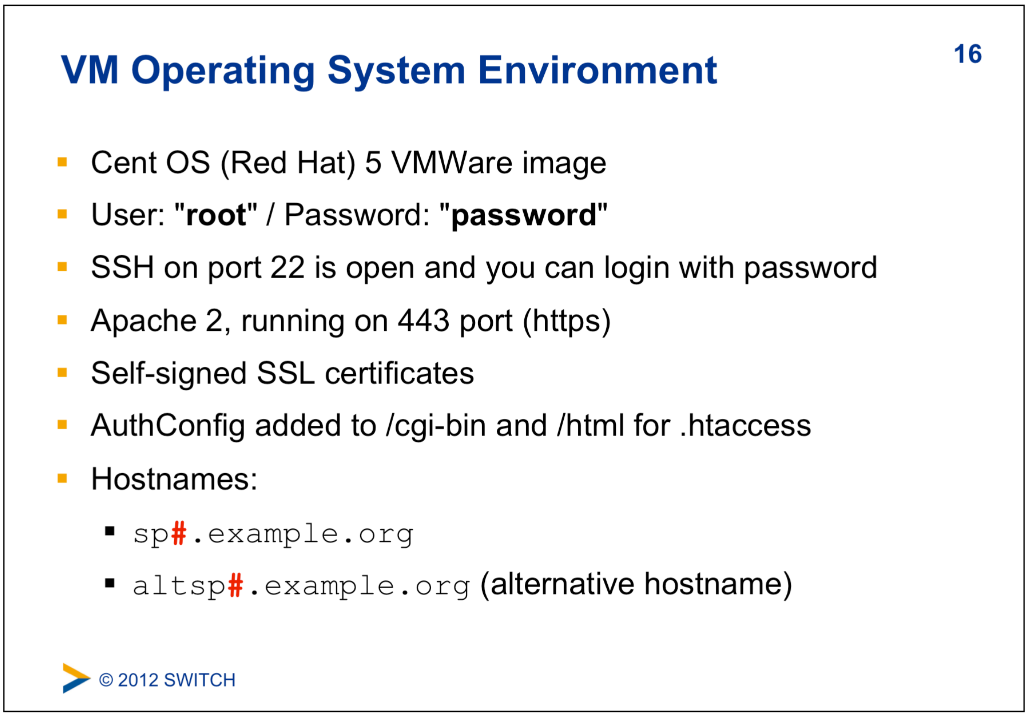
- **Service Provider (SP)**
  Consumes SAML assertions, protects web applications
- **Identity Provider (IdP)**
  Asserts digital identities using SAML
- **Discovery Service/WAYF (DS/WAYF)**
  Lets user choose Identity Provider/home organisation
- **shibd** (Shibboleth daemon)
  SP service/daemon for maintaining state
- **Session**
  Security context and cached data for a logged-in user
- **Session Initiator**
  Part of SP that controls how SSO requests are started

Notes: ______________________________

____

____

____



VM Operating System Environment

16

- Cent OS (Red Hat) 5 VMWare image
- User: "**root**" / Password: "**password**"
- SSH on port 22 is open and you can login with password
- Apache 2, running on 443 port (https)
- Self-signed SSL certificates
- AuthConfig added to /cgi-bin and /html for .htaccess
- Hostnames:
  - `sp#.example.org`
  - `altsp#.example.org` (alternative hostname)

Notes: ______________________________

____

____

____

SWITCHaai Deployment Guides

17

- Hands-on session has a general focus
- If you set up a production SP for SWITCHaai, please use
  http://www.switch.ch/aai/support/serviceproviders/
- SWITCHaai guides are custom-tailored and easier!

Notes:

Service Provider Installation in General

18

- On Mac OS X with MacPort:

```
$ port install shibboleth
```

- On Redhat:

```
$ yum install shibboleth
```

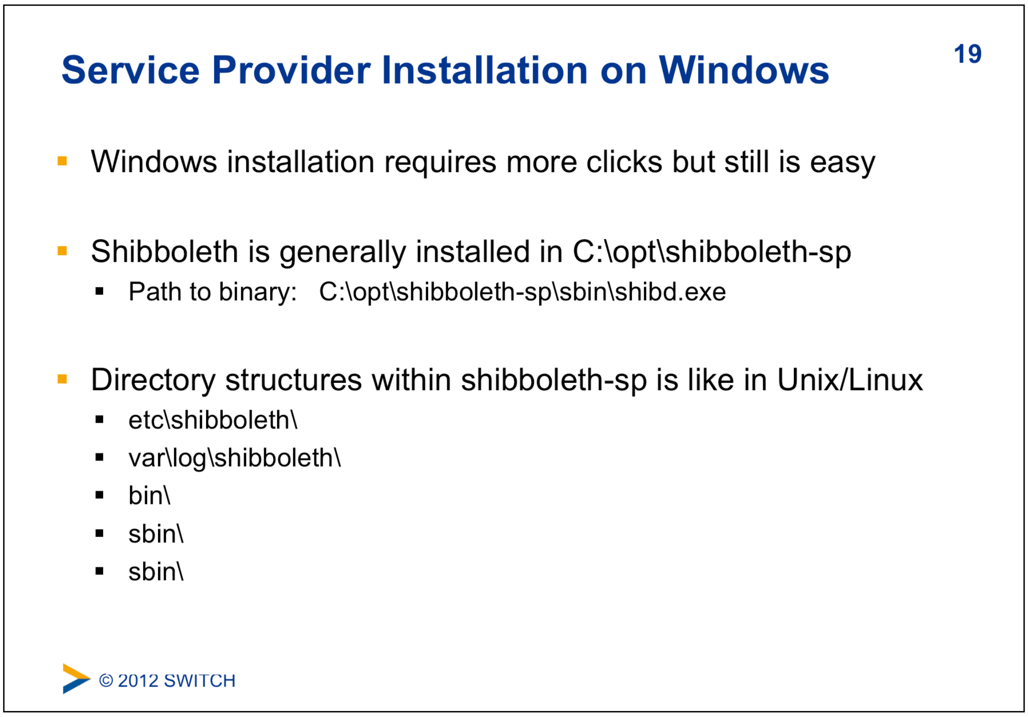
- On Debian:

```
$ apt-get install libapache2-mod-shib2
```

- Manual compilation not very difficult either
  - But more difficult to maintain efficiently
- And finally, on Windows ...

http://www.macports.org

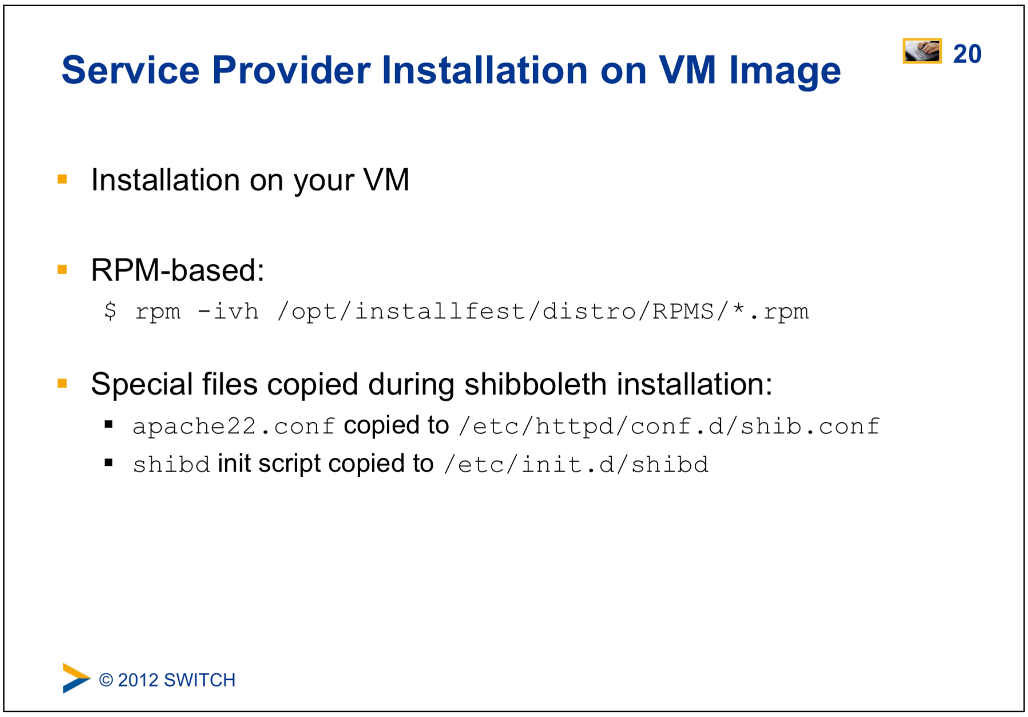
Notes:



Service Provider Installation on Windows

- Windows installation requires more clicks but still is easy
- Shibboleth is generally installed in C:\opt\shibboleth-sp
  - Path to binary: C:\opt\shibboleth-sp\sbin\shibd.exe
- Directory structures within shibboleth-sp is like in Unix/Linux
  - etc\shibboleth\
  - var\log\shibboleth\
  - bin\
  - sbin\
  - sbin\

Notes:



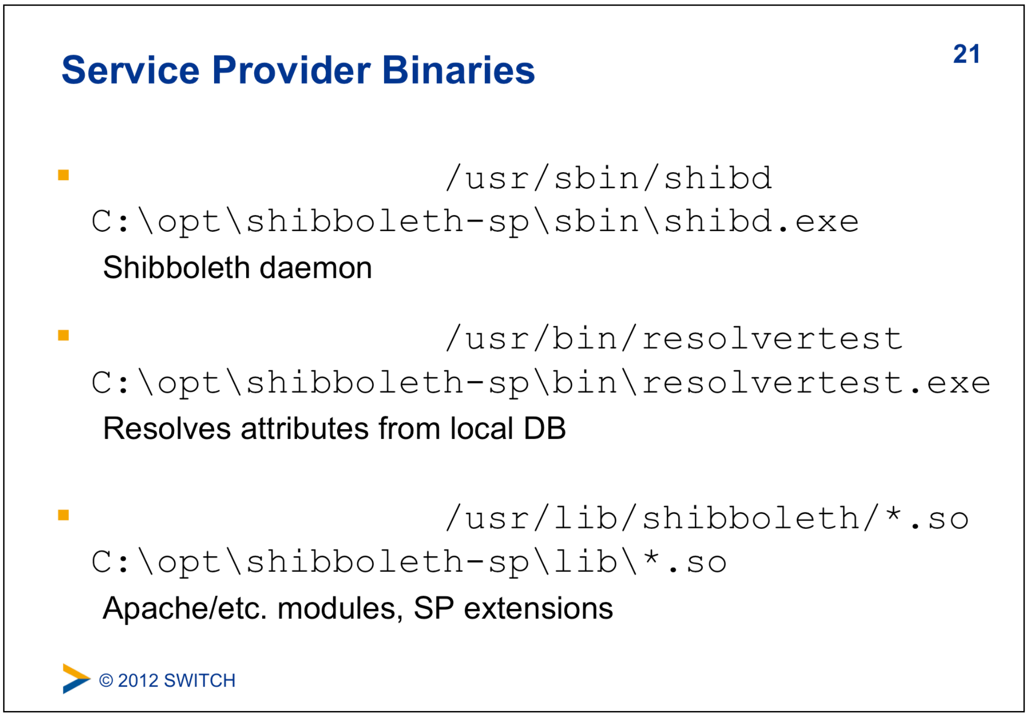
Service Provider Installation on VM Image

- Installation on your VM
- RPM-based:

```
$ rpm -ivh /opt/installfest/distro/RPMS/*.rpm
```

- Special files copied during shibboleth installation:
  - `apache22.conf` copied to `/etc/httpd/conf.d/shib.conf`
  - `shibd` init script copied to `/etc/init.d/shibd`

Notes:



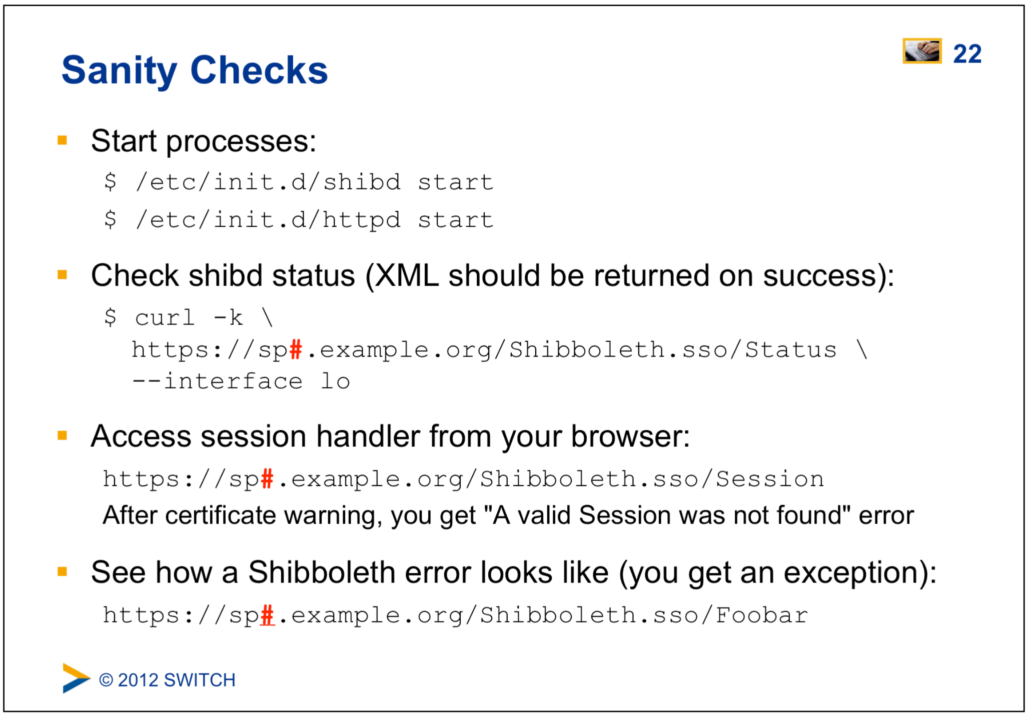
Service Provider Binaries

21

- `/usr/sbin/shibd`
  `C:\opt\shibboleth-sp\sbin\shibd.exe`
  Shibboleth daemon
- `/usr/bin/resolvertest`
  `C:\opt\shibboleth-sp\bin\resolvertest.exe`
  Resolves attributes from local DB
- `/usr/lib/shibboleth/*.so`
  `C:\opt\shibboleth-sp\lib\*.so`
  Apache/etc. modules, SP extensions

© 2012 SWITCH

Notes:



Sanity Checks

22

- Start processes:

```
$ /etc/init.d/shibd start
$ /etc/init.d/httpd start
```

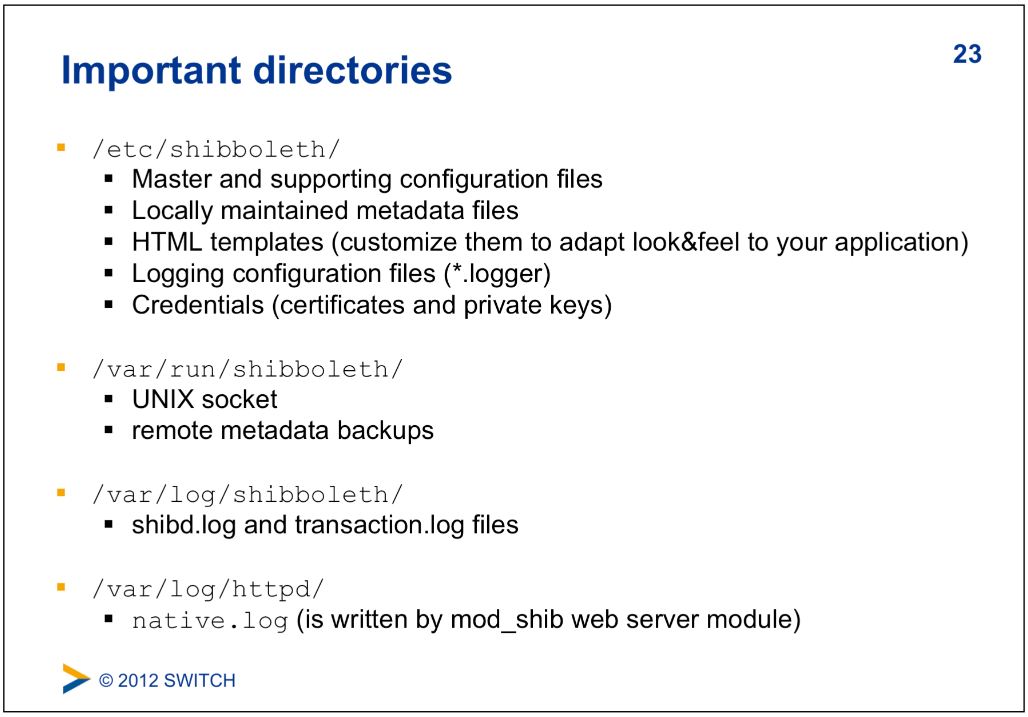
- Check shibd status (XML should be returned on success):

```
$ curl -k \
  https://sp#.example.org/Shibboleth.sso/Status \
  --interface lo
```

- Access session handler from your browser:
  `https://sp#.example.org/Shibboleth.sso/Session`
  After certificate warning, you get "A valid Session was not found" error
- See how a Shibboleth error looks like (you get an exception):
  `https://sp#.example.org/Shibboleth.sso/Foobar`

© 2012 SWITCH

Notes:



Important directories

23

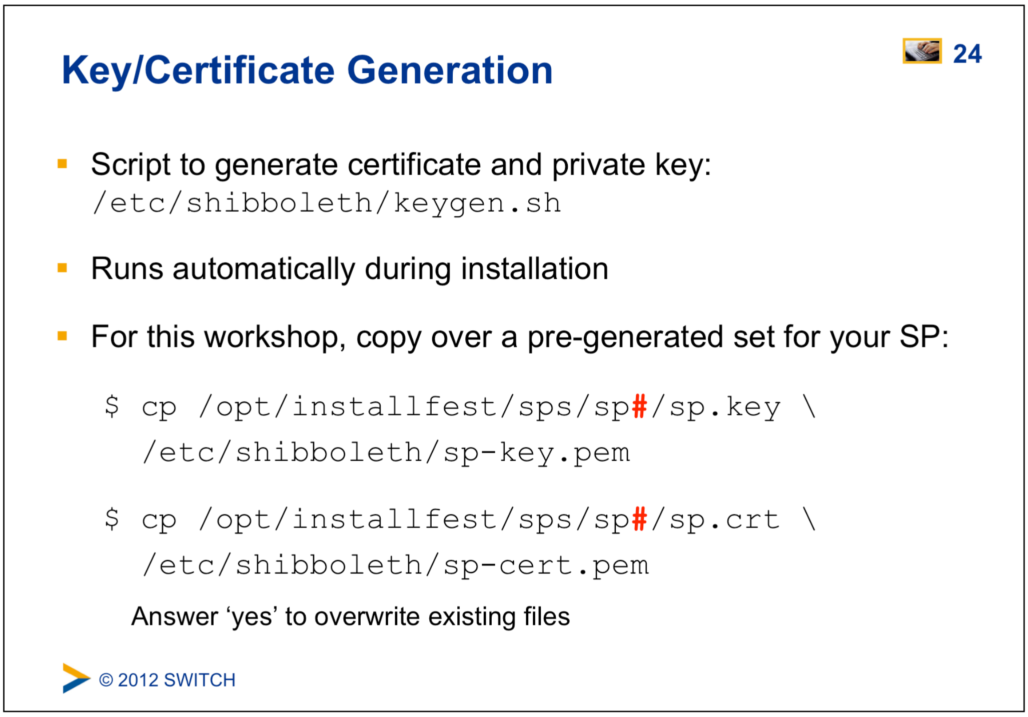
- `/etc/shibboleth/`
  - Master and supporting configuration files
  - Locally maintained metadata files
  - HTML templates (customize them to adapt look&feel to your application)
  - Logging configuration files (*.logger)
  - Credentials (certificates and private keys)
- `/var/run/shibboleth/`
  - UNIX socket
  - remote metadata backups
- `/var/log/shibboleth/`
  - shibd.log and transaction.log files
- `/var/log/httpd/`
  - `native.log` (is written by mod_shib web server module)

Notes: ______________________________

____

____

____



Key/Certificate Generation

24

- Script to generate certificate and private key:
  `/etc/shibboleth/keygen.sh`
- Runs automatically during installation
- For this workshop, copy over a pre-generated set for your SP:

```
$ cp /opt/installfest/sps/sp#/sp.key \
  /etc/shibboleth/sp-key.pem

$ cp /opt/installfest/sps/sp#/sp.crt \
  /etc/shibboleth/sp-cert.pem
```

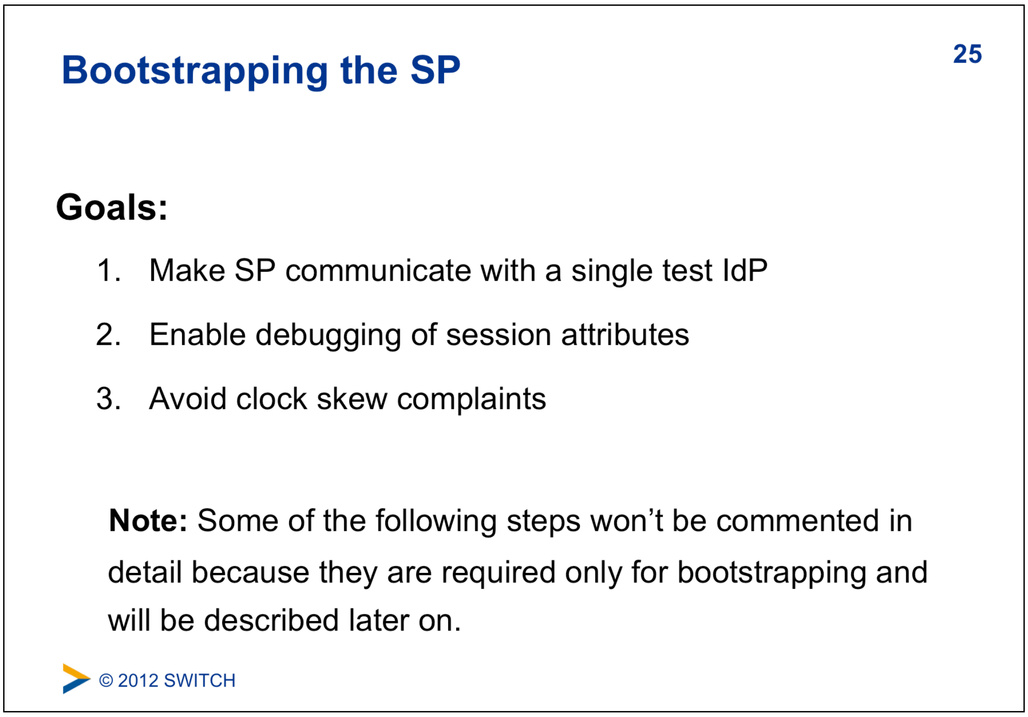
Answer ‘yes’ to overwrite existing files

Notes: ______________________________

____

____

____



Bootstrapping the SP

25

Goals:

1. Make SP communicate with a single test IdP
2. Enable debugging of session attributes
3. Avoid clock skew complaints

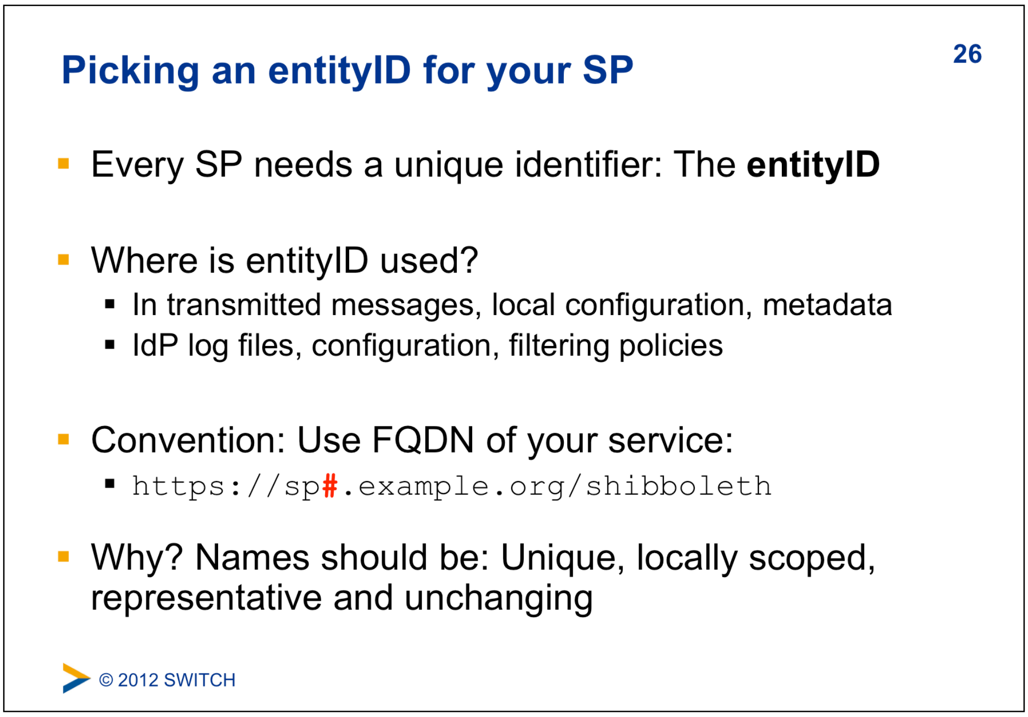
Note: Some of the following steps won't be commented in detail because they are required only for bootstrapping and will be described later on.

Notes: ______________________________

____

____

____



Picking an entityID for your SP

26

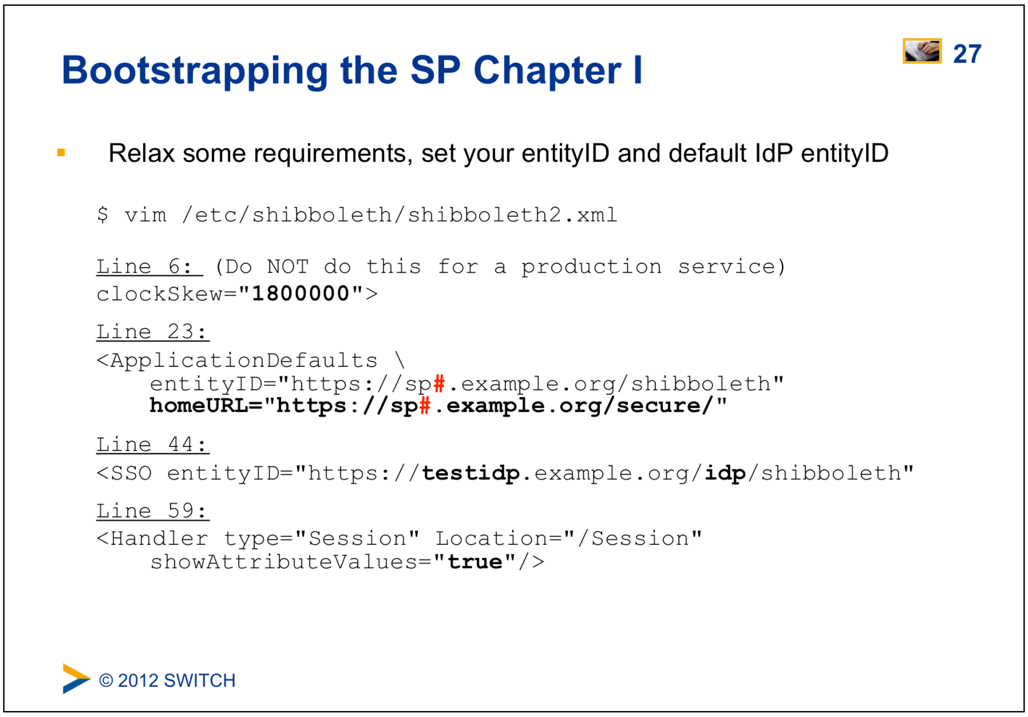
- Every SP needs a unique identifier: The **entityID**
- Where is entityID used?
  - In transmitted messages, local configuration, metadata
  - IdP log files, configuration, filtering policies
- Convention: Use FQDN of your service:
  - `https://sp#.example.org/shibboleth`
- Why? Names should be: Unique, locally scoped, representative and unchanging

Notes: ______________________________

____

____

____



Bootstrapping the SP Chapter I

27

- Relax some requirements, set your entityID and default IdP entityID

```
$ vim /etc/shibboleth/shibboleth2.xml

Line 6: (Do NOT do this for a production service)
clockSkew="1800000">

Line 23:
<ApplicationDefaults \
    entityID="https://sp#.example.org/shibboleth"
    homeURL="https://sp#.example.org/secure/"

Line 44:
<SSO entityID="https://testidp.example.org/idp/shibboleth"

Line 59:
<Handler type="Session" Location="/Session"
    showAttributeValues="true"/>
```

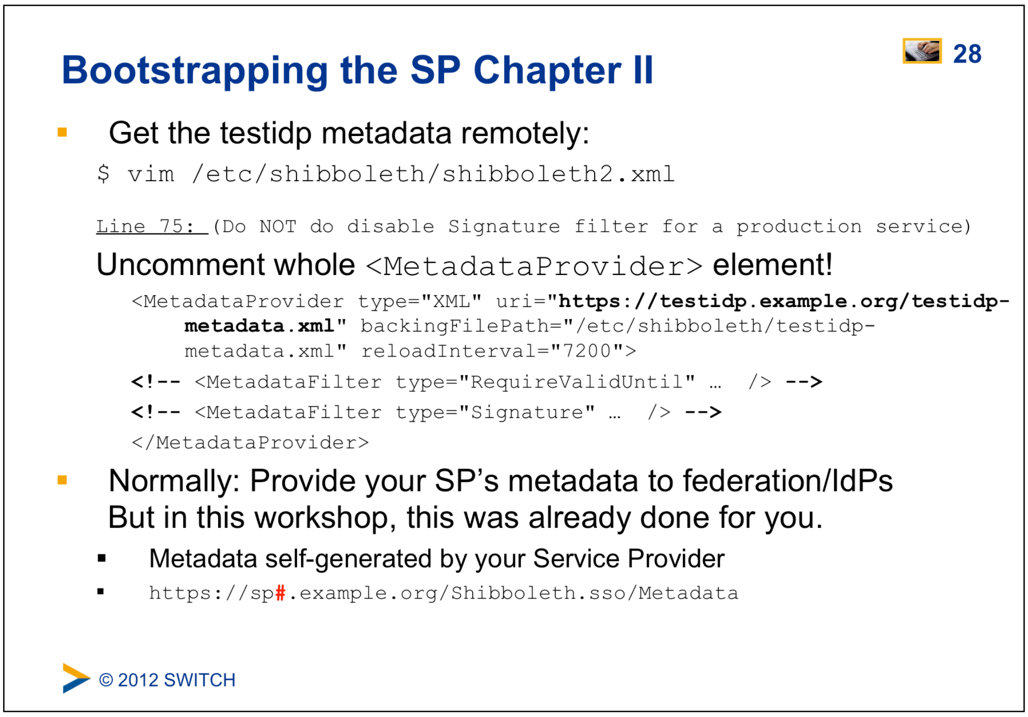
© 2012 SWITCH

Notes: ______________________________

____

____

____



Bootstrapping the SP Chapter II

28

- Get the testidp metadata remotely:

```
$ vim /etc/shibboleth/shibboleth2.xml
```

Line 75: (Do NOT do disable Signature filter for a production service)

Uncomment whole `<MetadataProvider>` element!

```
<MetadataProvider type="XML" uri="https://testidp.example.org/testidp-
    metadata.xml" backingFilePath="/etc/shibboleth/testidp-
    metadata.xml" reloadInterval="7200">
<!-- <MetadataFilter type="RequireValidUntil" …  /> -->
<!-- <MetadataFilter type="Signature" …  /> -->
</MetadataProvider>
```

- Normally: Provide your SP's metadata to federation/IdPs
  But in this workshop, this was already done for you.
  - Metadata self-generated by your Service Provider
  - `https://sp#.example.org/Shibboleth.sso/Metadata`

© 2012 SWITCH

Notes: ______________________________

____

____

____

Quick Test

29

- Make sure configuration works (should return "…is loadable"):

```
$ shibd -tc /etc/shibboleth/shibboleth2.xml
```

Service Provider reloads shibboleth2.xml automatically when it changed

- Try it with a browser:

```
https://sp#.example.org/secure/
```

`/secure/` is protecty by Shibboleth "by default". See bottom of file `/etc/httpd/conf.d/shib.conf`
Therefore, you should be forced to authenticate. Login at Test IdP with demouser/password and you should get access to this directory.

- Then call the Shibboleth session handler to see the attributes:

```
https://sp#.example.org/Shibboleth.sso/Session
```

You should see various attributes like affiliation, entitlement, eppn, etc.

Notes: ______________________________

____

____

____

AAI Resource Registry

30

Purpose of the SWITCHaai Resource Registry and how to use it

Please consult the table of contents to find this presentation in your hand-outs.

Notes: ______________________________

____

____

____

Logging Out

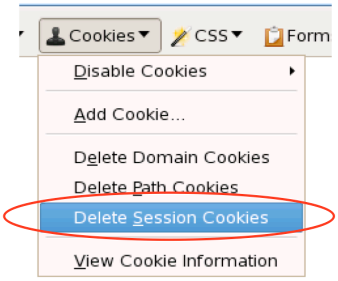
31

- To logout locally from the SP and kill your session:

```
https://sp#.example.org/Shibboleth.sso/Logout
```

But this won't delete your session on the IdP!

- **Close the browser and restart it again!**
- Or delete all your session cookies
  - Recommendation for testing: Use Firefox Web Developer extension



© 2012 SWITCH

Notes:

• Alternatively, comment out on about 146 in shibboleth2.xml the SAML2 Logout Initiator

Use a Discovery Service (WAYF)

32

- Change the default SessionInitiator:

```
$ vim /etc/shibboleth/shibboleth2.xml

Line 44:
<SSO discoveryProtocol="SAMLDS" \
   discoveryURL="https://ds.example.org/DS/WAYF"/>
```

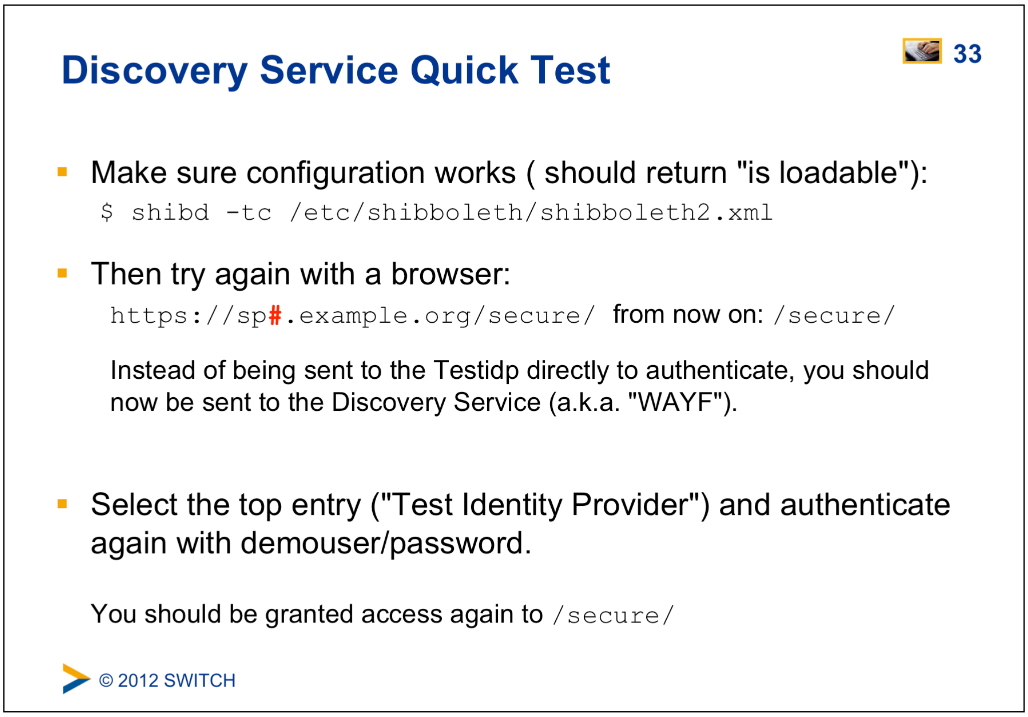
Remove the entityID attribute in the <SSO> element in order to use a Discovery Service

Restart Apache and Shibboelth

```
$ /etc/init.d/shibd restart
$ /etc/init.d/httpd restart
```

© 2012 SWITCH

Notes:



Discovery Service Quick Test

33

- Make sure configuration works (should return "is loadable"):

```
$ shibd -tc /etc/shibboleth/shibboleth2.xml
```

- Then try again with a browser:

  `https://sp#.example.org/secure/` from now on: `/secure/`

  Instead of being sent to the Testidp directly to authenticate, you should now be sent to the Discovery Service (a.k.a. "WAYF").

- Select the top entry ("Test Identity Provider") and authenticate again with demouser/password.

  You should be granted access again to `/secure/`

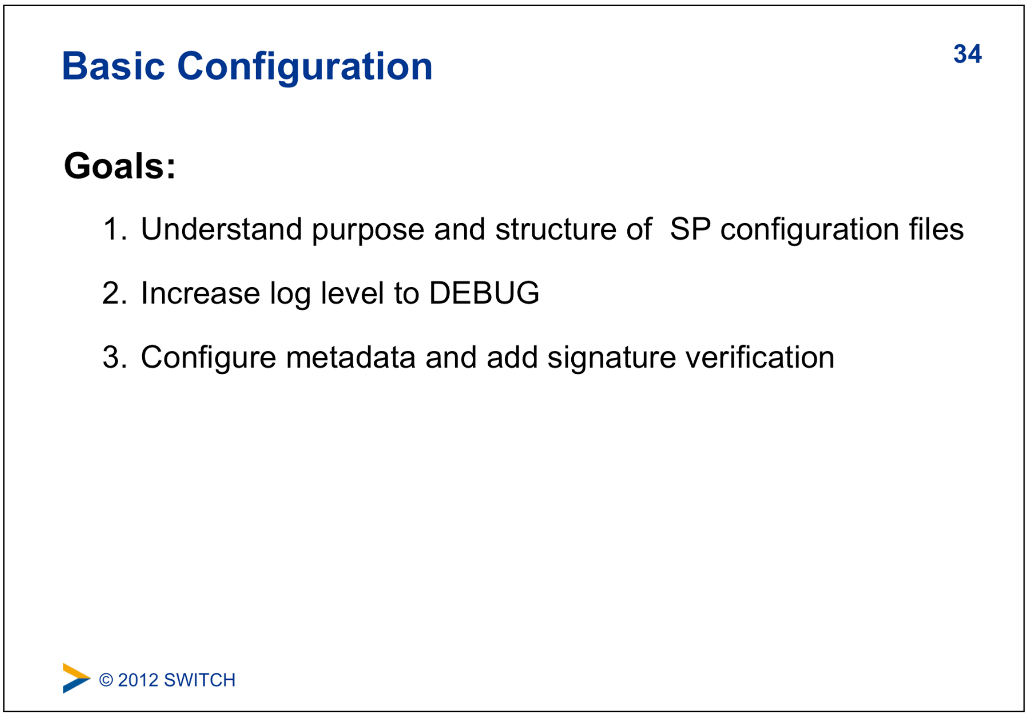
© 2012 SWITCH

Notes: ____________________

____

____

____



Basic Configuration

34

Goals:

1. Understand purpose and structure of SP configuration files
2. Increase log level to DEBUG
3. Configure metadata and add signature verification

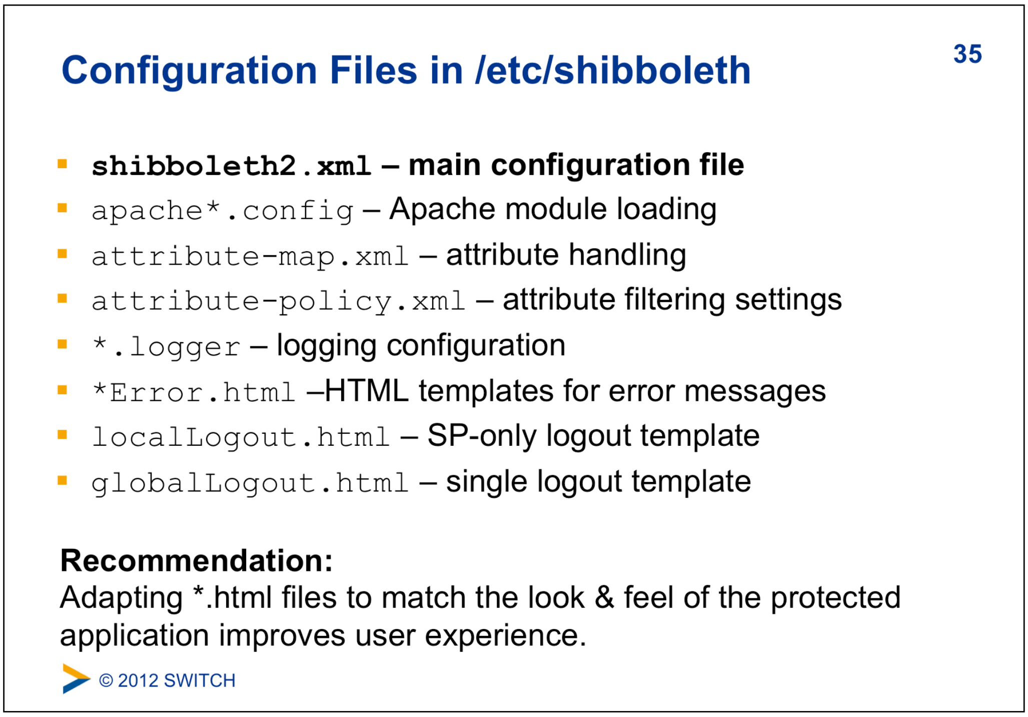
© 2012 SWITCH

Notes: ____________________

____

____

____



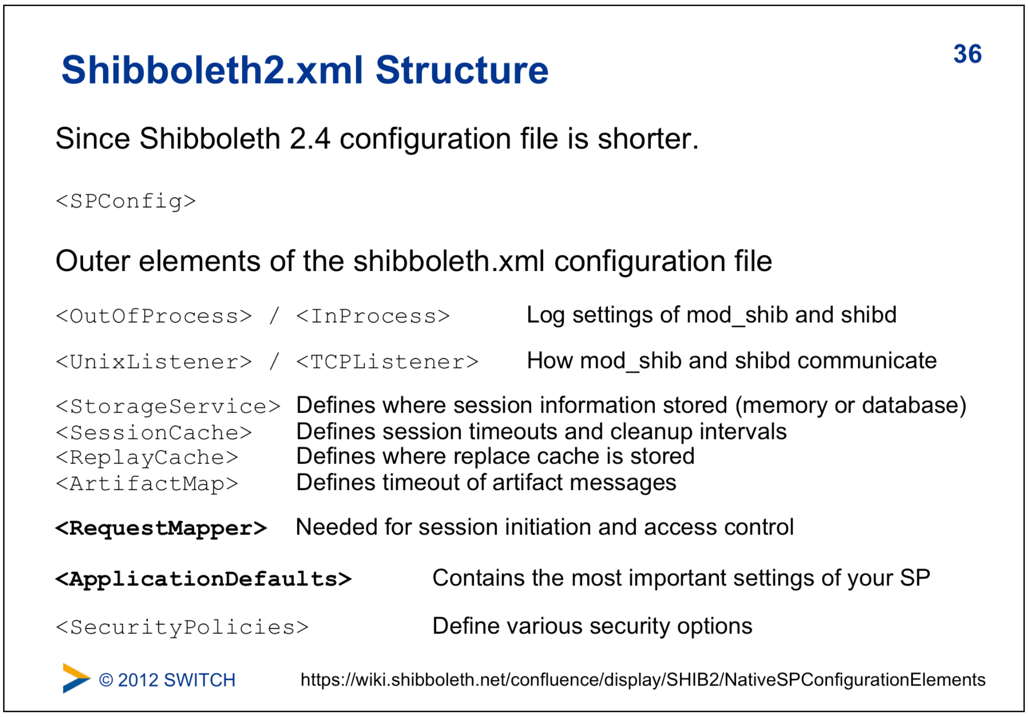
Configuration Files in /etc/shibboleth

35

- **`shibboleth2.xml` – main configuration file**
- `apache*.config` – Apache module loading
- `attribute-map.xml` – attribute handling
- `attribute-policy.xml` – attribute filtering settings
- `*.logger` – logging configuration
- `*Error.html` –HTML templates for error messages
- `localLogout.html` – SP-only logout template
- `globalLogout.html` – single logout template

Recommendation:
Adapting *.html files to match the look & feel of the protected application improves user experience.

Notes:



Shibboleth2.xml Structure

36

Since Shibboleth 2.4 configuration file is shorter.

`<SPConfig>`

Outer elements of the shibboleth.xml configuration file

`<OutOfProcess> / <InProcess>`	Log settings of mod_shib and shibd
`<UnixListener> / <TCPListener>`	How mod_shib and shibd communicate
`<StorageService>`	Defines where session information stored (memory or database)
`<SessionCache>`	Defines session timeouts and cleanup intervals
`<ReplayCache>`	Defines where replace cache is stored
`<ArtifactMap>`	Defines timeout of artifact messages
`<RequestMapper>`	Needed for session initiation and access control
`<ApplicationDefaults>`	Contains the most important settings of your SP
`<SecurityPolicies>`	Define various security options

https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPConfigurationElements

Notes:

ApplicationDefaults Structure

37

You are most likely to apply changes in <ApplicationDefaults>:

- **<Sessions>** Defines handlers and how sessions are initiated and managed. Contains <SSO>, <Logout>, <Handler>
- **<Errors>** Used to display error messages. E.g. logo, email and CSS
- <RelyingParty> (optional) To modify settings for certain IdPs/federations
- **<MetadataProvider>** Defines the metadata to be used by the SP
- <AttributeExtractor> Attribute map file to use
- <AttributeResolver> Attribute resolver file to use
- <AttributeFilter> Attribute filter file to use
- **<CredentialResolver>** Defines certificate and private key to be use
- <ApplicationOverride> (optional) Can override any of the above for certain applications

https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPConfigurationElements

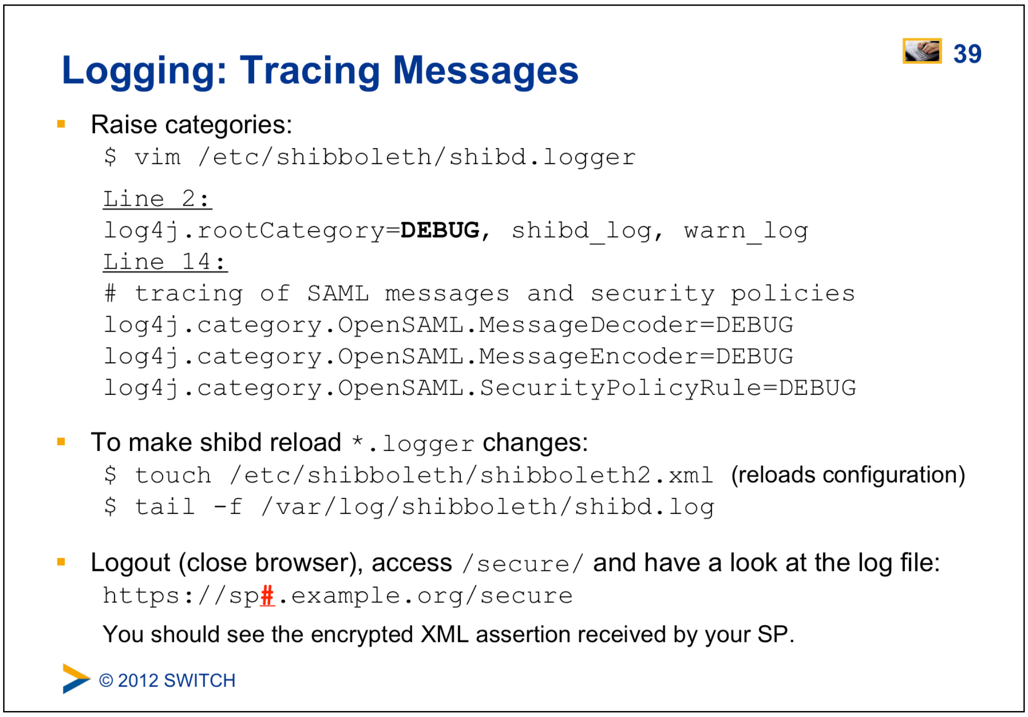
Notes:

Logging

38

- Your number one friend in case of problems
- `shibd.log` and `transaction.log` written by shibd, `native.log` written by mod_shib
- `*.logger` files contain predefined settings for output locations and a default logging level (INFO) along with useful categories to raise to DEBUG
- Log time is in UTC (Coordinated Universal Time)

Notes:



39

Logging: Tracing Messages

- Raise categories:

```
$ vim /etc/shibboleth/shibd.logger

Line 2:
log4j.rootCategory=DEBUG, shibd_log, warn_log
Line 14:
# tracing of SAML messages and security policies
log4j.category.OpenSAML.MessageDecoder=DEBUG
log4j.category.OpenSAML.MessageEncoder=DEBUG
log4j.category.OpenSAML.SecurityPolicyRule=DEBUG
```

- To make shibd reload `*.logger` changes:

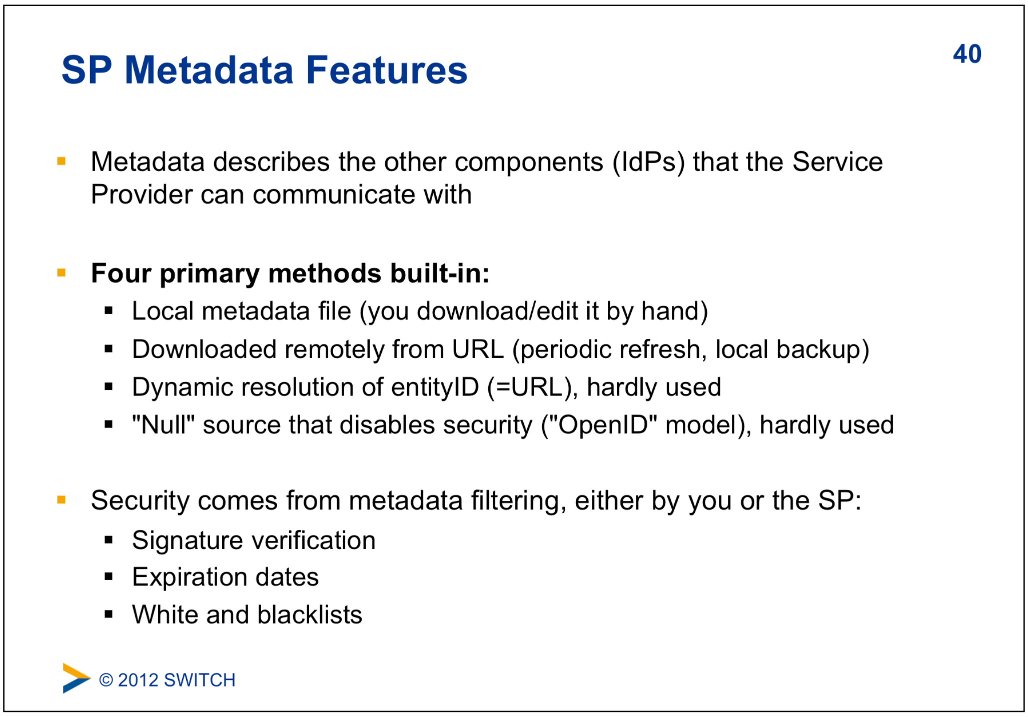
```
$ touch /etc/shibboleth/shibboleth2.xml  (reloads configuration)
$ tail -f /var/log/shibboleth/shibd.log
```

- Logout (close browser), access `/secure/` and have a look at the log file:

  `https://sp#.example.org/secure`

  You should see the encrypted XML assertion received by your SP.

Notes:

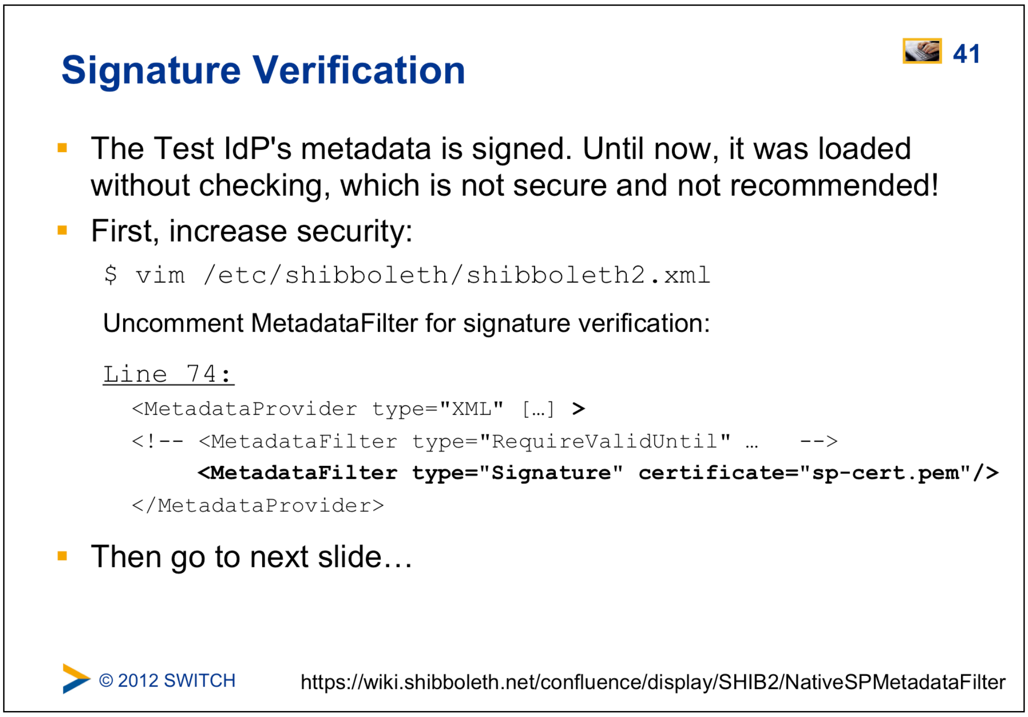


40

SP Metadata Features

- Metadata describes the other components (IdPs) that the Service Provider can communicate with
- **Four primary methods built-in:**
  - Local metadata file (you download/edit it by hand)
  - Downloaded remotely from URL (periodic refresh, local backup)
  - Dynamic resolution of entityID (=URL), hardly used
  - "Null" source that disables security ("OpenID" model), hardly used
- Security comes from metadata filtering, either by you or the SP:
  - Signature verification
  - Expiration dates
  - White and blacklists

Notes:



41

Signature Verification

- The Test IdP's metadata is signed. Until now, it was loaded without checking, which is not secure and not recommended!
- First, increase security:

```
$ vim /etc/shibboleth/shibboleth2.xml
```

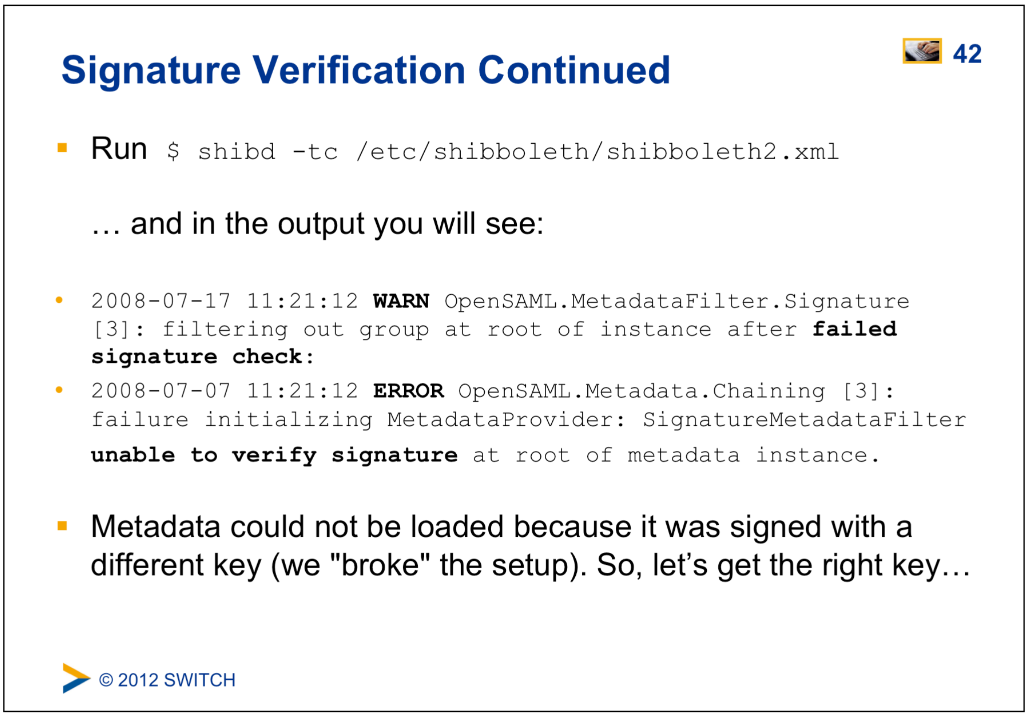
Uncomment MetadataFilter for signature verification:

```
Line 74:
  <MetadataProvider type="XML" […] >
  <!-- <MetadataFilter type="RequireValidUntil" …   -->
       <MetadataFilter type="Signature" certificate="sp-cert.pem"/>
  </MetadataProvider>
```

- Then go to next slide…

© 2012 SWITCH https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPMetadataFilter

Notes:



42

Signature Verification Continued

- Run `$ shibd -tc /etc/shibboleth/shibboleth2.xml`

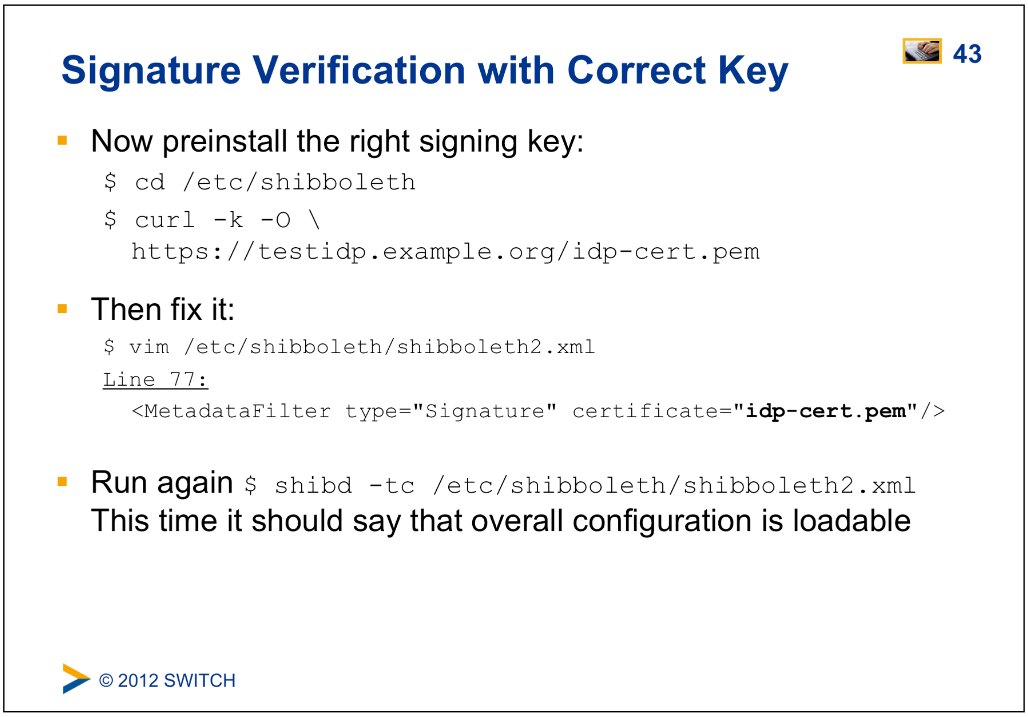
  … and in the output you will see:

```
• 2008-07-17 11:21:12 WARN OpenSAML.MetadataFilter.Signature
  [3]: filtering out group at root of instance after failed
  signature check:
• 2008-07-07 11:21:12 ERROR OpenSAML.Metadata.Chaining [3]:
  failure initializing MetadataProvider: SignatureMetadataFilter
  unable to verify signature at root of metadata instance.
```

- Metadata could not be loaded because it was signed with a different key (we "broke" the setup). So, let’s get the right key…

© 2012 SWITCH

Notes:



Signature Verification with Correct Key

43

- Now preinstall the right signing key:

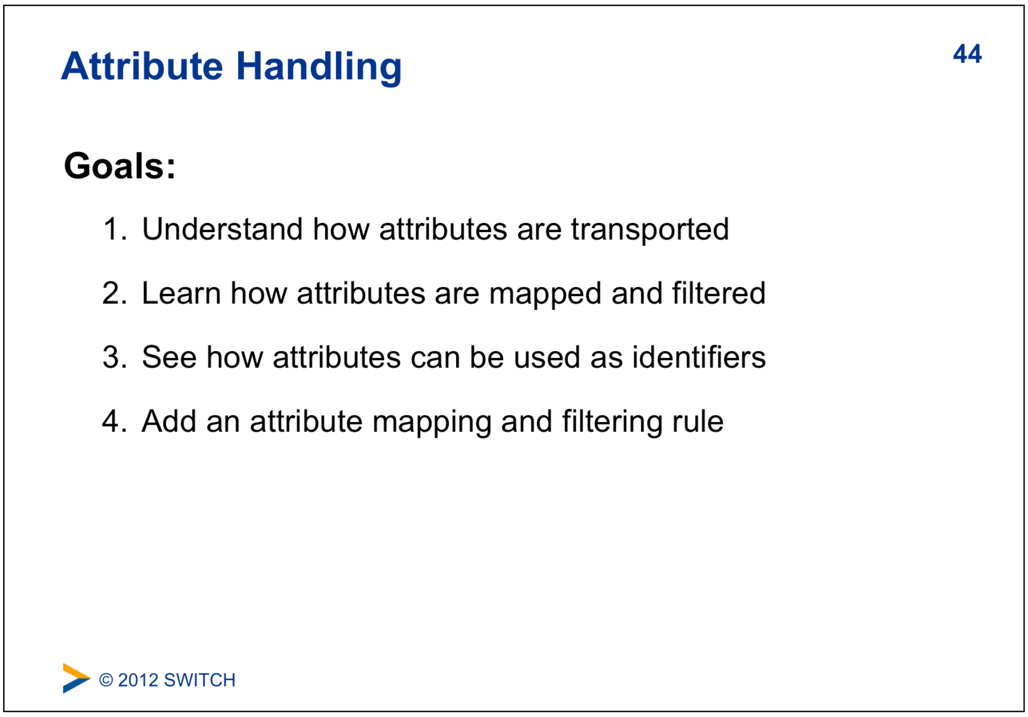
```
$ cd /etc/shibboleth
$ curl -k -O \
  https://testidp.example.org/idp-cert.pem
```

- Then fix it:

```
$ vim /etc/shibboleth/shibboleth2.xml
Line 77:
  <MetadataFilter type="Signature" certificate="idp-cert.pem"/>
```

- Run again `$ shibd -tc /etc/shibboleth/shibboleth2.xml`
  This time it should say that overall configuration is loadable

Notes: ______________________________



Attribute Handling

44

Goals:

1. Understand how attributes are transported
2. Learn how attributes are mapped and filtered
3. See how attributes can be used as identifiers
4. Add an attribute mapping and filtering rule

Notes: ______________________________

SP Attribute Terminology

45

- **Attribute Push**
  Delivering attributes with SSO assertion via web browser
- **Attribute Pull**
  Querying for attributes after SSO via back-channel (SP -> IdP)
- **Attribute Extraction**
  Decoding SAML information into neutral data structures mapped to environment or header variables
- **Attribute Filtering**
  Blocking invalid, unexpected, or unauthorized values based on application or community criteria
- **Attribute Resolution**
  Resolving a SSO assertion into a set of additional attributes (e.g. queries)

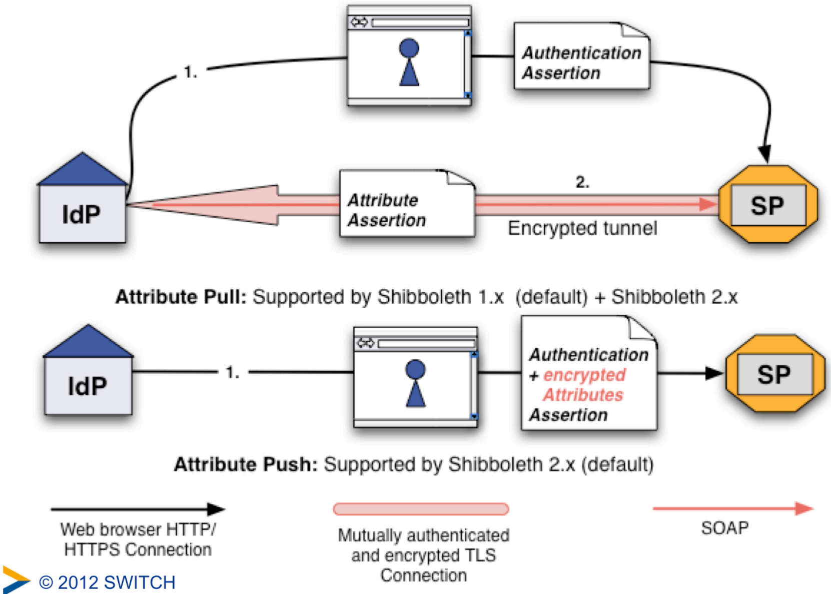
Notes: ______________________________

____

____

____

Attribute Pull vs Push


1.
Authentication Assertion
IdP
Attribute Assertion
2.
Encrypted tunnel
SP
IdP
1.
Authentication + encrypted Attributes Assertion
SP
Web browser HTTP/ HTTPS Connection
Mutually authenticated and encrypted TLS Connection
SOAP

Attribute Pull: Supported by Shibboleth 1.x (default) + Shibboleth 2.x

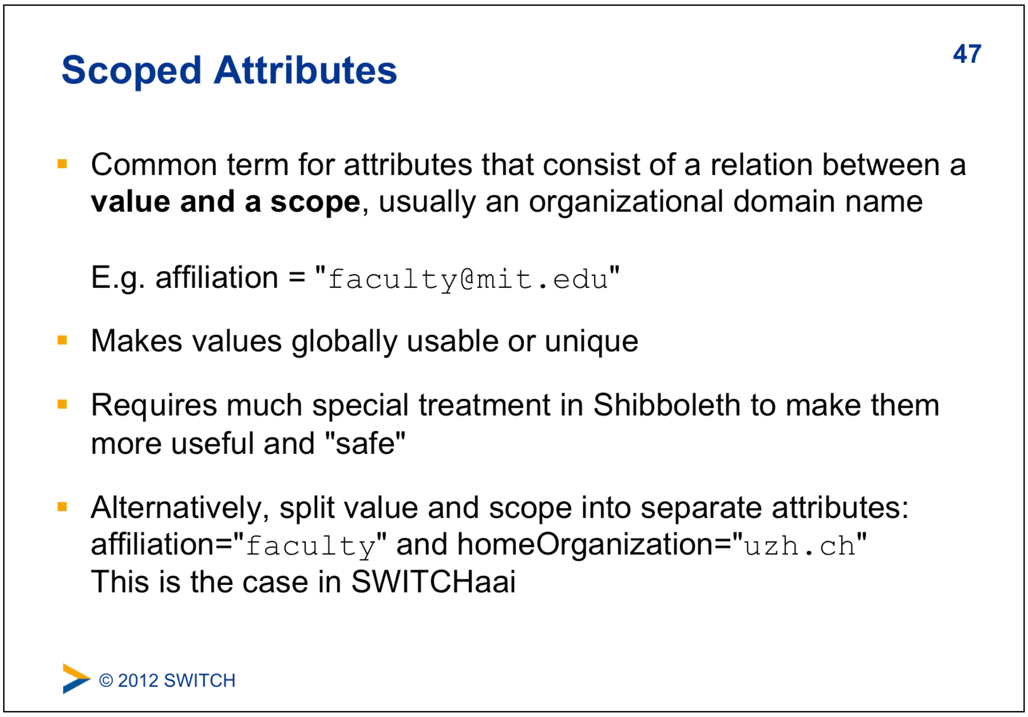
Attribute Push: Supported by Shibboleth 2.x (default)

Notes: ______________________________

____

____

____



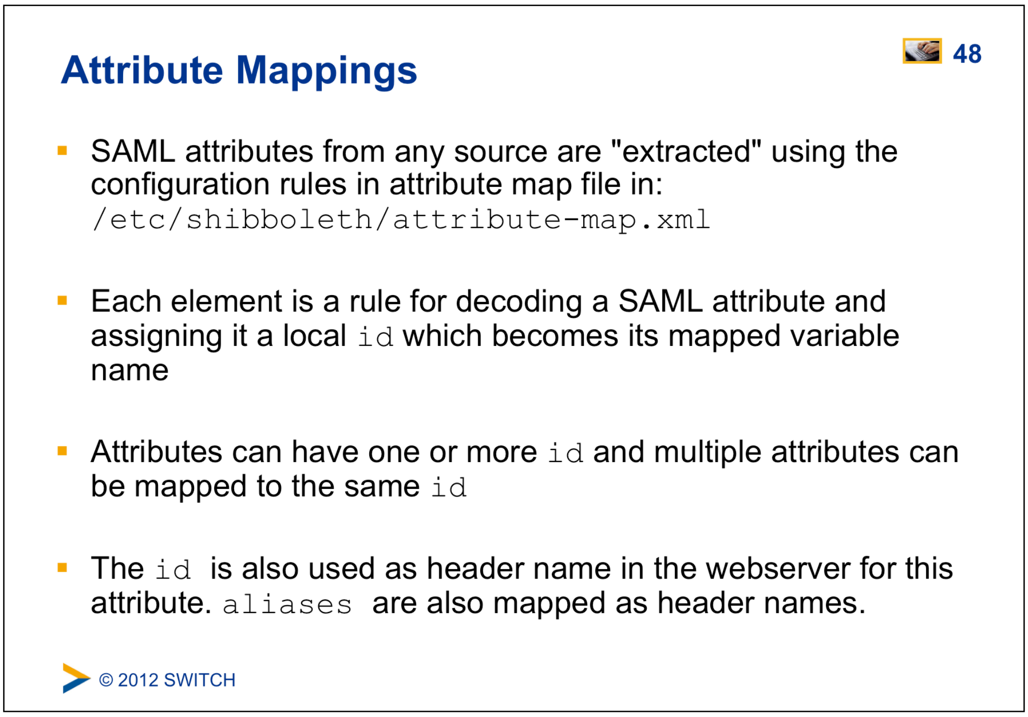
Scoped Attributes

47

- Common term for attributes that consist of a relation between a **value and a scope**, usually an organizational domain name

  E.g. affiliation = "`faculty@mit.edu`"
- Makes values globally usable or unique
- Requires much special treatment in Shibboleth to make them more useful and "safe"
- Alternatively, split value and scope into separate attributes: affiliation="`faculty`" and homeOrganization="`uzh.ch`"
  This is the case in SWITCHaai

Notes:

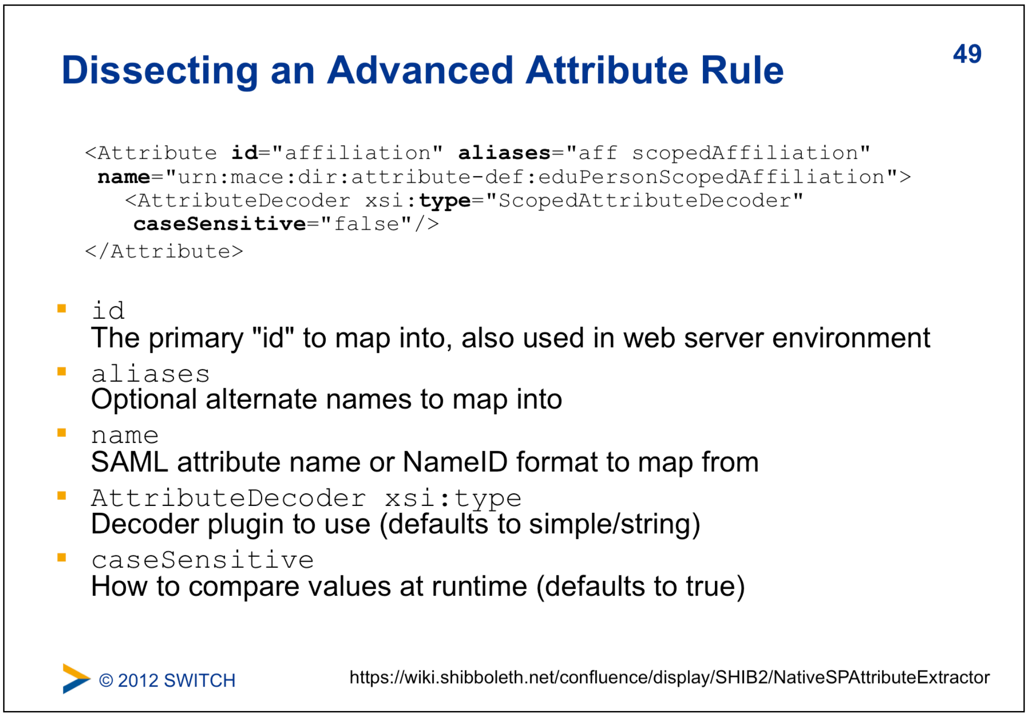


Attribute Mappings

48

- SAML attributes from any source are "extracted" using the configuration rules in attribute map file in: `/etc/shibboleth/attribute-map.xml`
- Each element is a rule for decoding a SAML attribute and assigning it a local `id` which becomes its mapped variable name
- Attributes can have one or more `id` and multiple attributes can be mapped to the same `id`
- The `id` is also used as header name in the webserver for this attribute. `aliases` are also mapped as header names.

Notes:



Dissecting an Advanced Attribute Rule

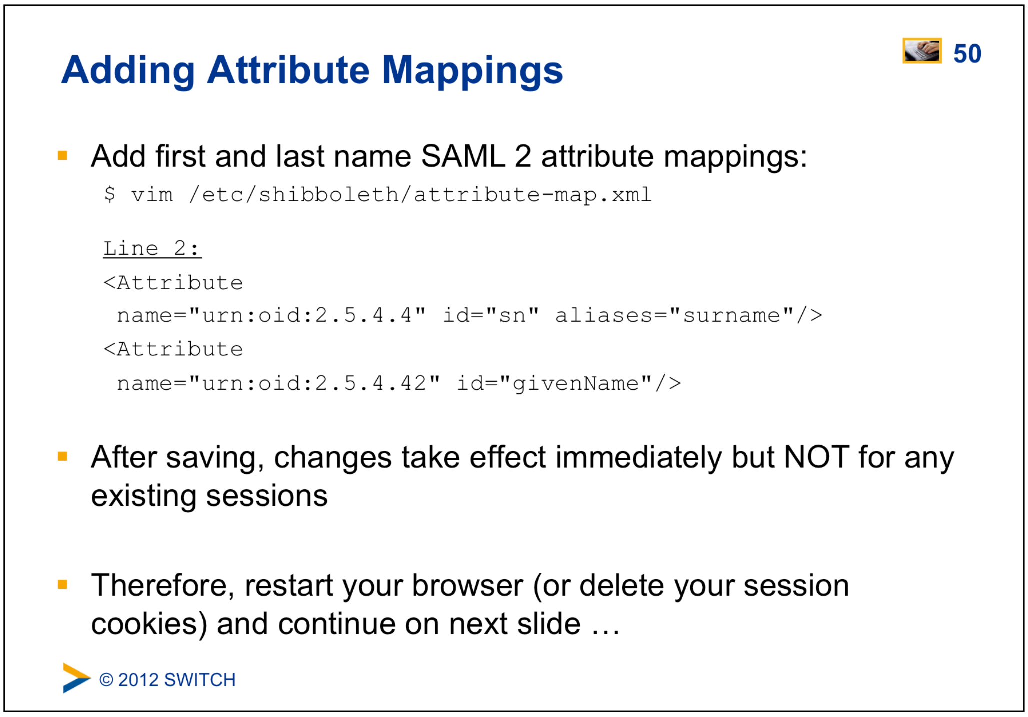
49

```
<Attribute id="affiliation" aliases="aff scopedAffiliation"
 name="urn:mace:dir:attribute-def:eduPersonScopedAffiliation">
   <AttributeDecoder xsi:type="ScopedAttributeDecoder"
    caseSensitive="false"/>
</Attribute>
```

- `id`
  The primary "id" to map into, also used in web server environment
- `aliases`
  Optional alternate names to map into
- `name`
  SAML attribute name or NameID format to map from
- `AttributeDecoder xsi:type`
  Decoder plugin to use (defaults to simple/string)
- `caseSensitive`
  How to compare values at runtime (defaults to true)

https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPAttributeExtractor

Notes:



Adding Attribute Mappings

50

- Add first and last name SAML 2 attribute mappings:

```
$ vim /etc/shibboleth/attribute-map.xml

Line 2:
<Attribute
 name="urn:oid:2.5.4.4" id="sn" aliases="surname"/>
<Attribute
 name="urn:oid:2.5.4.42" id="givenName"/>
```

- After saving, changes take effect immediately but NOT for any existing sessions

- Therefore, restart your browser (or delete your session cookies) and continue on next slide …

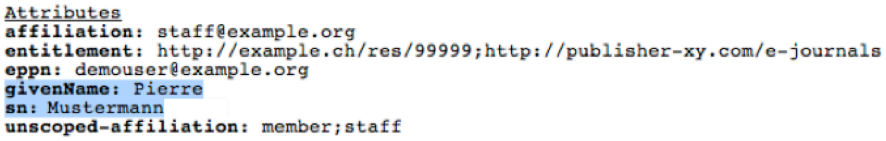
Notes:

Testing Added Attribute Mapping

51

- Then access `/secure/` again and log in with demouser/password. Access should be granted.
- After that, check the Shibboleth Session Handler to see the added attributes are now present:
  `https://sp#.example.org/Shibboleth.sso/Session`

  Now, you also should see the `givenName` and `sn` attributes.



```
Attributes
affiliation: staff@example.org
entitlement: http://example.ch/res/99999;http://publisher-xy.com/e-journals
eppn: demouser@example.org
givenName: Pierre
sn: Mustermann
unscoped-affiliation: member;staff
```

https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPHandler

Notes: ______________________________

____

____

____

Uncomment All Attribute Mappings

52

- Delete the added mapping for sn and givenName on lines 2 and 3 and uncomment all other attribute mappings.

  ```
  $ vim /etc/shibboleth/attribute-map.xml
  ```

  Around line 54:

  Remove `<!--`

  Around line 77:

  Remove `-->`

  Around line 78:

  Remove `<!--`

  Around line 13§:

  Remove `-->`

- Then logout, go to `/secure/` and access the Session handler
  You now also get `cn, mail` and `preferredLanguage`

Notes: ______________________________

____

____

____

User Identifier and SWITCHaai Attributes

53

Excursion about user identifier attributes and about SWITCHaai attributes in general.

Please consult the table of contents to find this presentation in your hand-outs.

Notes:

REMOTE_USER

54

- Special single-valued variable that all web applications should support for container-managed authentication of a unique user.
- Any attribute, once extracted/mapped, can be copied to REMOTE_USER
- Multiple attributes can be examined in order of preference, but only the first value will be used.

Notes:

Changing REMOTE_USER

55

- In case your application needs to have a remote user for authentication, you just could make shibboleth put an attribute (e.g. "mail") as REMOTE_USER:

```
/etc/shibboleth/shibboleth2.xml

Line 25 in <ApplicationDefaults>:
REMOTE_USER="mail eppn persistent-id targeted-id"
```

- If mail attribute is available, it will be put into REMOTE_USER
- Attribute `mail` has precedence over `eppn` in this case
- This allows very easy "shibbolization" of some web applications

Notes:

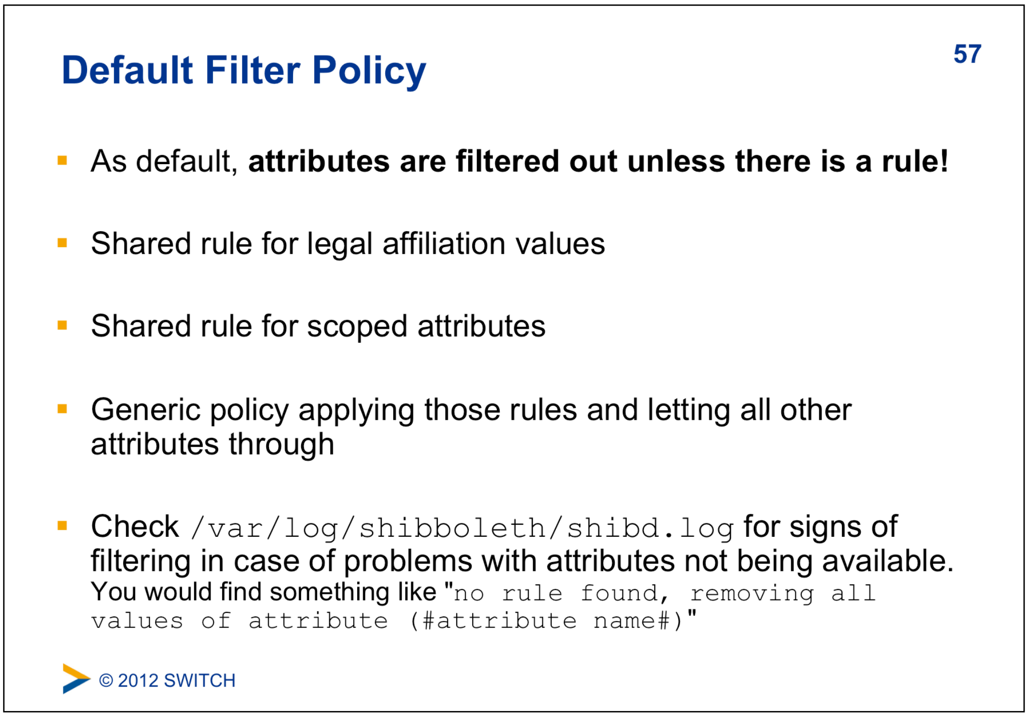
Attribute Filtering

56

- Answers the "who can say what" question on behalf of an application
- Service Provider can make sure that only allowed attributes and values are made available to application
- Some examples:
  - constraining the possible values or value ranges of an attribute (e.g. eduPersonAffiliation, telephoneNumber, ...)
  - limiting the scopes/domains an IdP can speak for (e.g. university x cannot assert faculty@university-z.edu)
  - limiting custom attributes to particular sources

https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPAttributeFilter

Notes:



Default Filter Policy

57

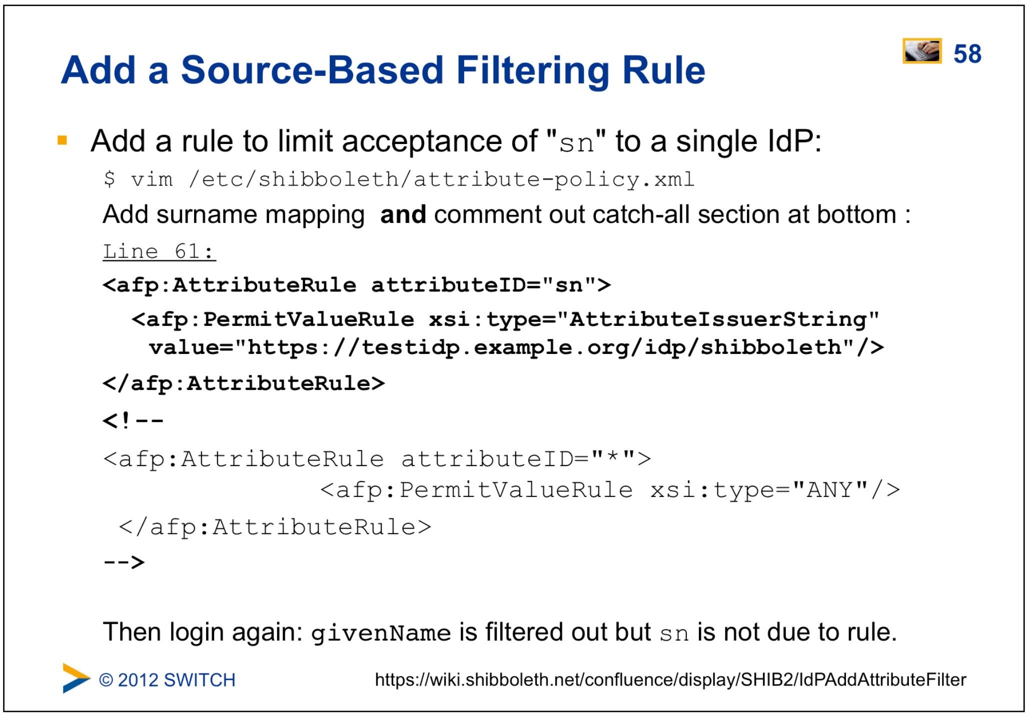
- As default, **attributes are filtered out unless there is a rule!**
- Shared rule for legal affiliation values
- Shared rule for scoped attributes
- Generic policy applying those rules and letting all other attributes through
- Check `/var/log/shibboleth/shibd.log` for signs of filtering in case of problems with attributes not being available.
  You would find something like "`no rule found, removing all values of attribute (#attribute name#)`"

Notes: ____

____

____

____



Add a Source-Based Filtering Rule

58

- Add a rule to limit acceptance of "`sn`" to a single IdP:

```
$ vim /etc/shibboleth/attribute-policy.xml
```

Add surname mapping **and** comment out catch-all section at bottom :

```
Line 61:
<afp:AttributeRule attributeID="sn">
  <afp:PermitValueRule xsi:type="AttributeIssuerString"
   value="https://testidp.example.org/idp/shibboleth"/>
</afp:AttributeRule>
<!--
<afp:AttributeRule attributeID="*">
              <afp:PermitValueRule xsi:type="ANY"/>
 </afp:AttributeRule>
-->
```

Then login again: `givenName` is filtered out but `sn` is not due to rule.

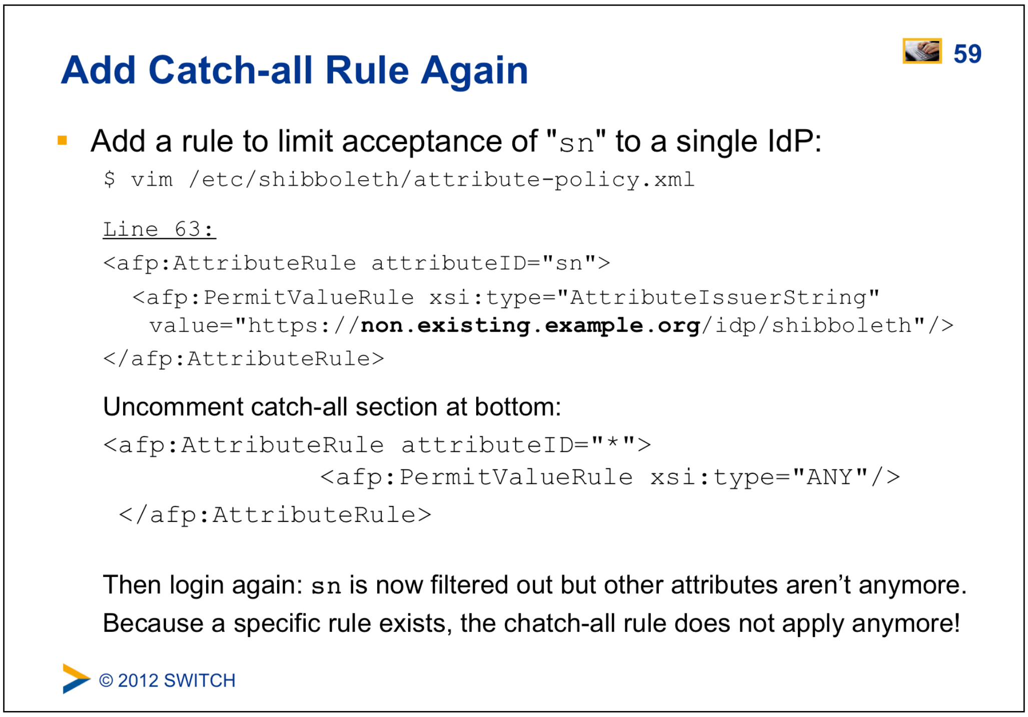
https://wiki.shibboleth.net/confluence/display/SHIB2/IdPAddAttributeFilter

Notes: ____

____

____

____



Add Catch-all Rule Again

59

- Add a rule to limit acceptance of "sn" to a single IdP:

```
$ vim /etc/shibboleth/attribute-policy.xml
```

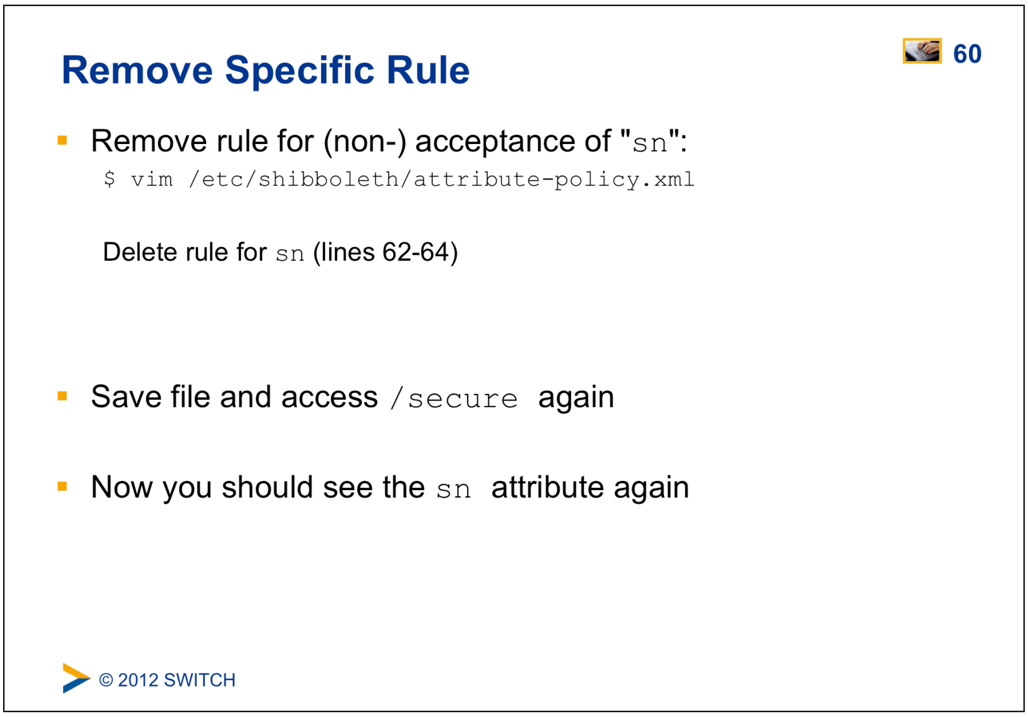
```
Line 63:
<afp:AttributeRule attributeID="sn">
  <afp:PermitValueRule xsi:type="AttributeIssuerString"
   value="https://non.existing.example.org/idp/shibboleth"/>
</afp:AttributeRule>
```

Uncomment catch-all section at bottom:

```
<afp:AttributeRule attributeID="*">
               <afp:PermitValueRule xsi:type="ANY"/>
 </afp:AttributeRule>
```

Then login again: `sn` is now filtered out but other attributes aren’t anymore. Because a specific rule exists, the chatch-all rule does not apply anymore!

Notes: ______________________________



Remove Specific Rule

60

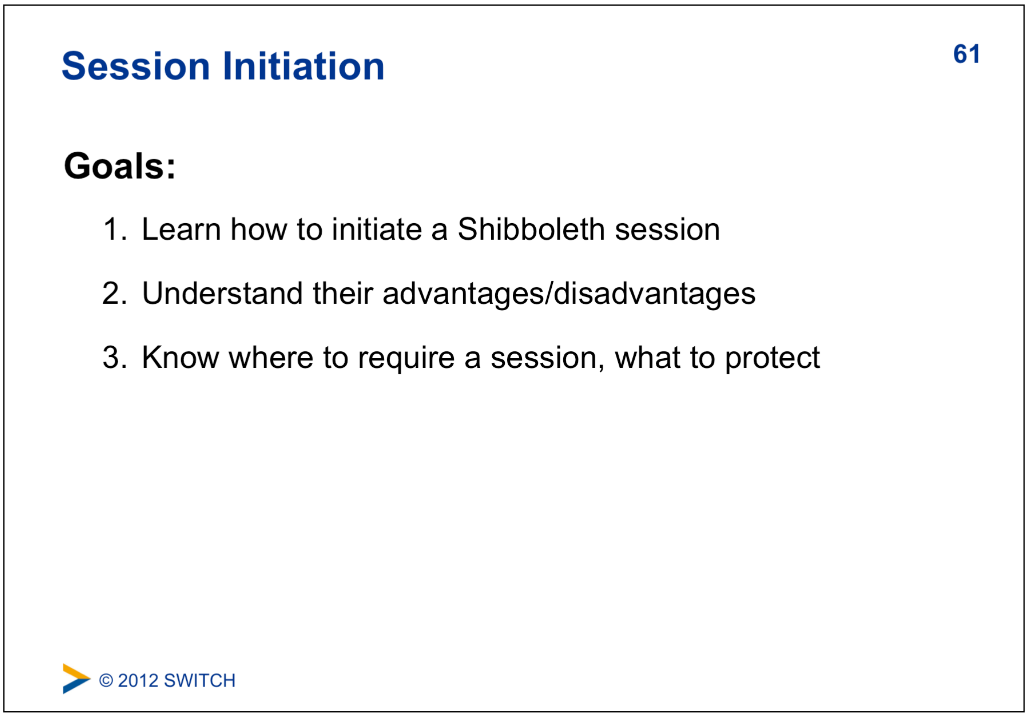
- Remove rule for (non-) acceptance of "sn":

```
$ vim /etc/shibboleth/attribute-policy.xml
```

Delete rule for `sn` (lines 62-64)

- Save file and access `/secure` again
- Now you should see the `sn` attribute again

Notes: ______________________________



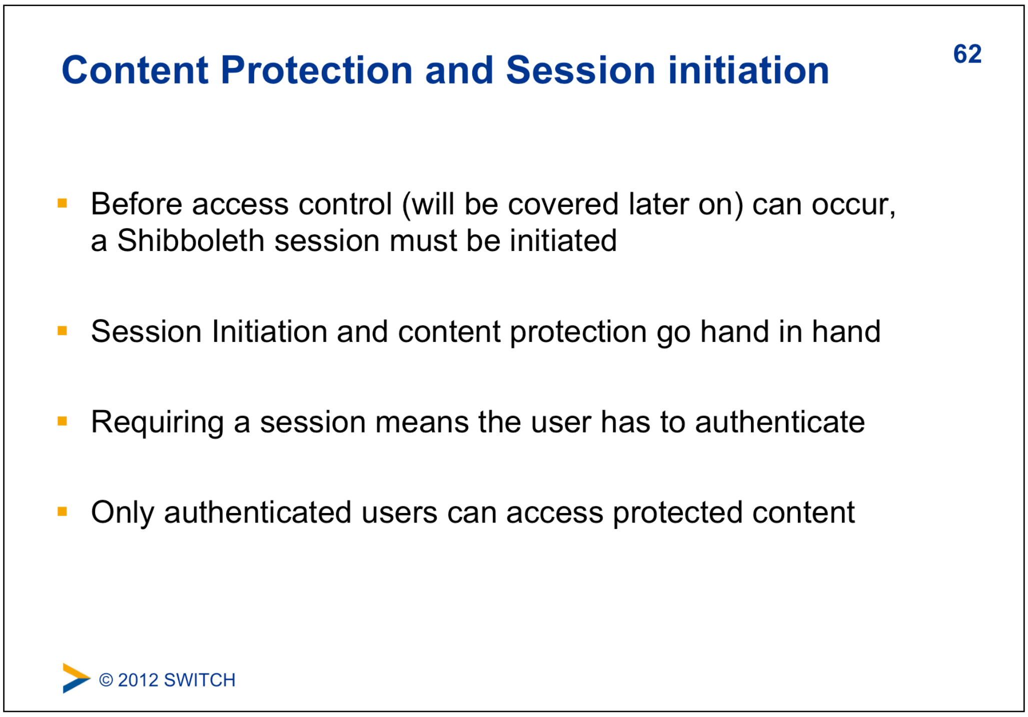
Session Initiation

61

Goals:

1. Learn how to initiate a Shibboleth session
2. Understand their advantages/disadvantages
3. Know where to require a session, what to protect

Notes: ________________________________

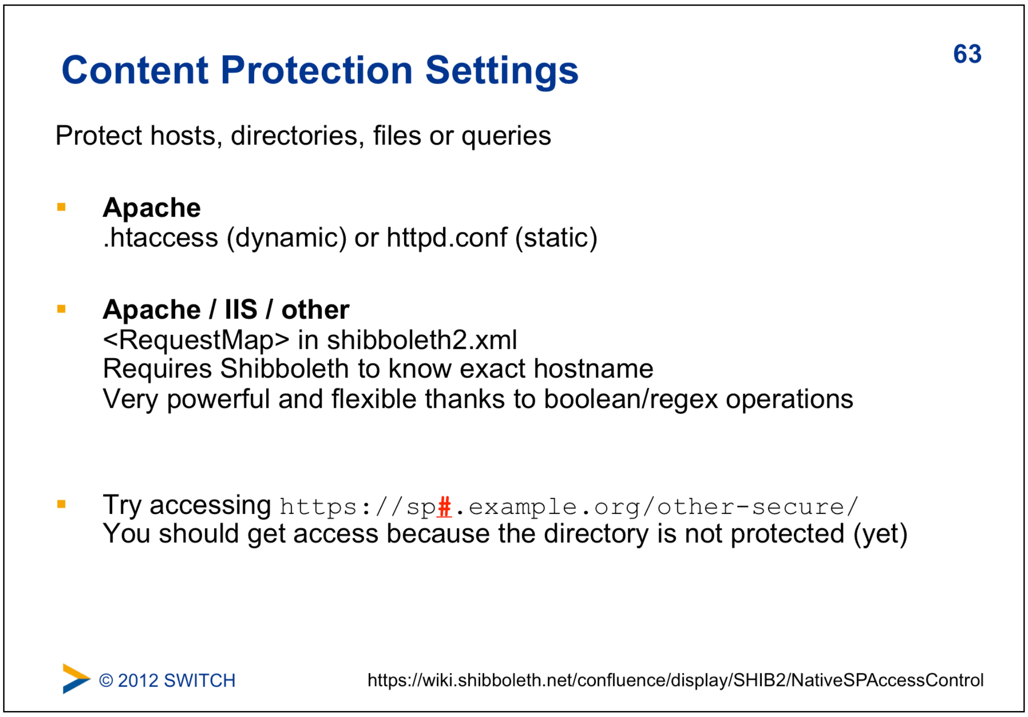


Content Protection and Session initiation

62

- Before access control (will be covered later on) can occur, a Shibboleth session must be initiated
- Session Initiation and content protection go hand in hand
- Requiring a session means the user has to authenticate
- Only authenticated users can access protected content

Notes: ________________________________



Content Protection Settings

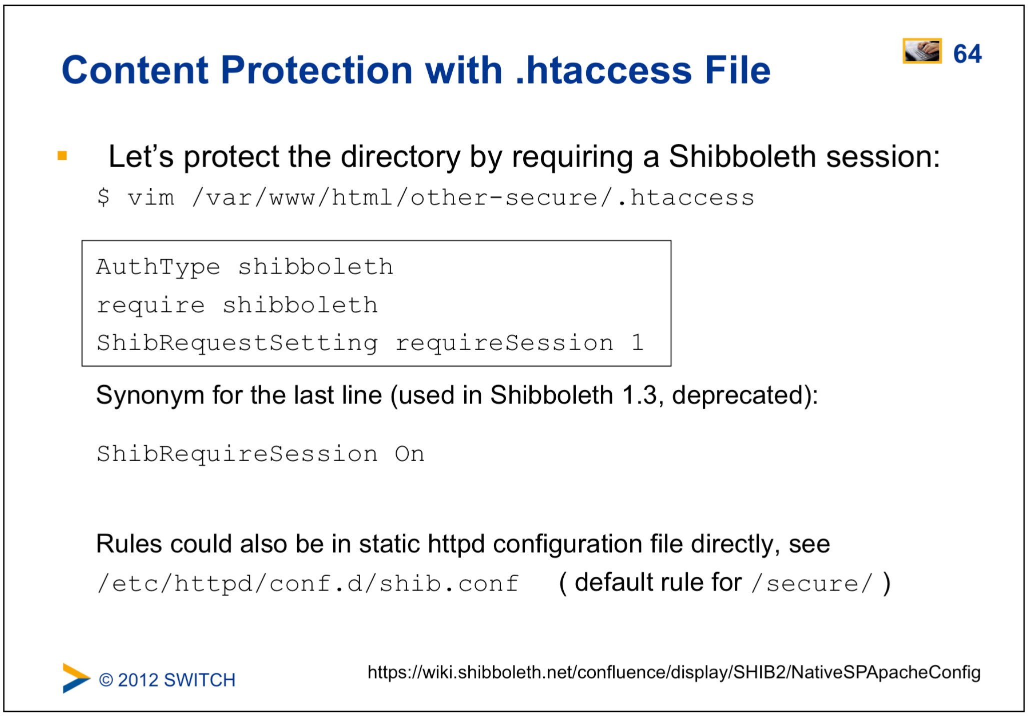
63

Protect hosts, directories, files or queries

- **Apache**
  .htaccess (dynamic) or httpd.conf (static)
- **Apache / IIS / other**
  <RequestMap> in shibboleth2.xml
  Requires Shibboleth to know exact hostname
  Very powerful and flexible thanks to boolean/regex operations
- Try accessing `https://sp#.example.org/other-secure/`
  You should get access because the directory is not protected (yet)

© 2012 SWITCH https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPAccessControl

Notes:



Content Protection with .htaccess File

64

- Let’s protect the directory by requiring a Shibboleth session:

```
$ vim /var/www/html/other-secure/.htaccess
```

```
AuthType shibboleth
require shibboleth
ShibRequestSetting requireSession 1
```

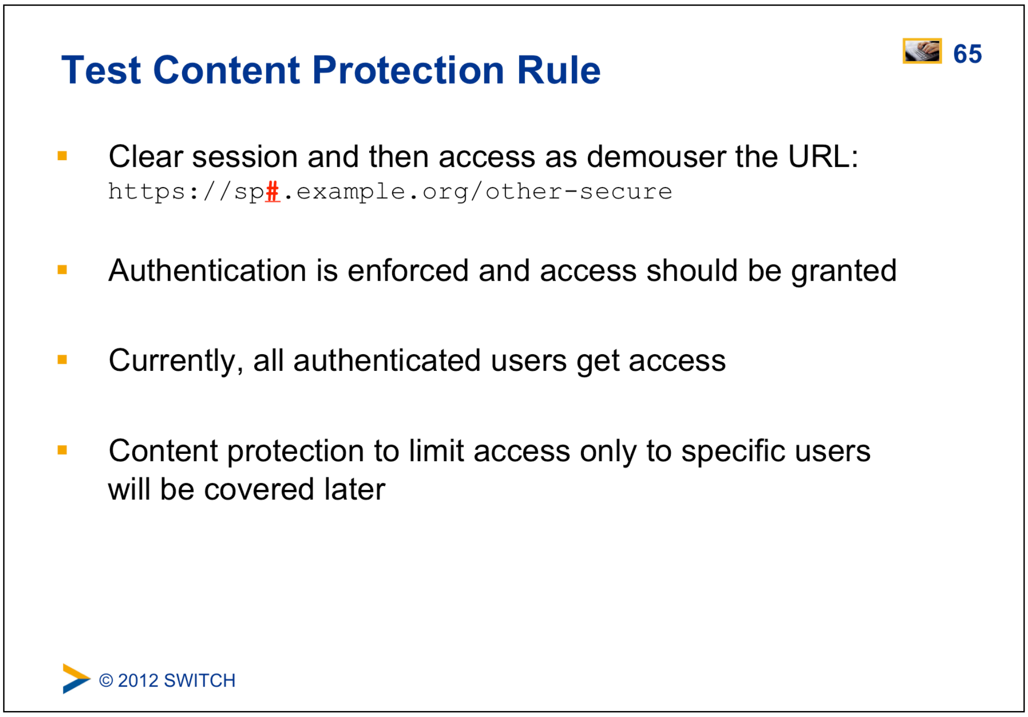
Synonym for the last line (used in Shibboleth 1.3, deprecated):

```
ShibRequireSession On
```

Rules could also be in static httpd configuration file directly, see
`/etc/httpd/conf.d/shib.conf` (default rule for `/secure/`)

© 2012 SWITCH https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPApacheConfig

Notes:

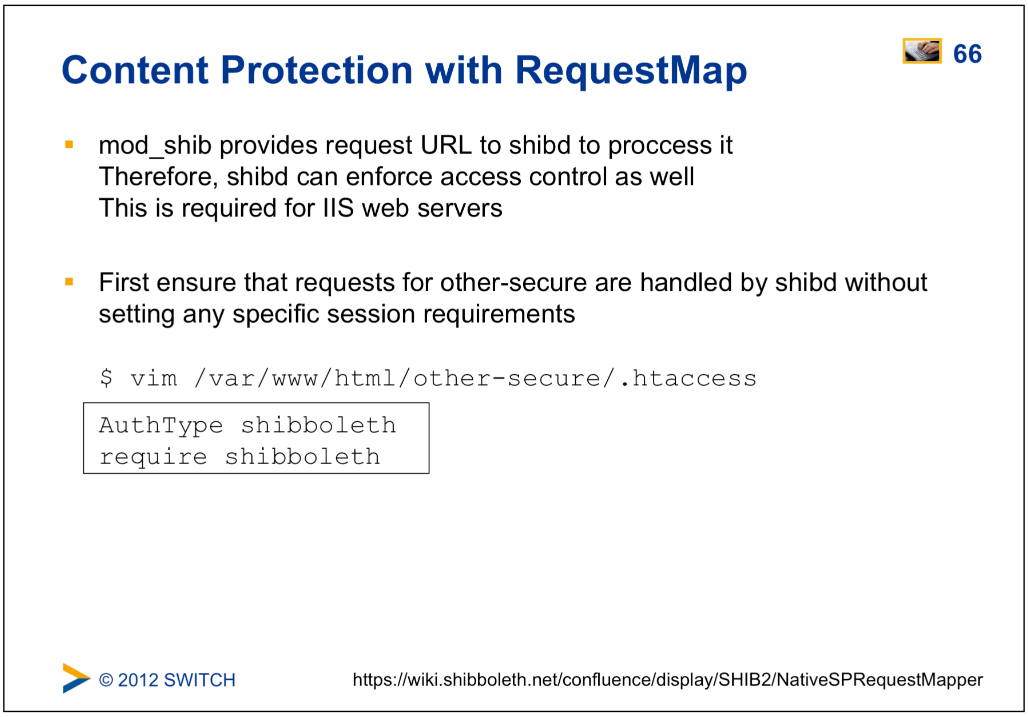


Test Content Protection Rule

65

- Clear session and then access as demouser the URL:
  `https://sp#.example.org/other-secure`
- Authentication is enforced and access should be granted
- Currently, all authenticated users get access
- Content protection to limit access only to specific users will be covered later

Notes:



Content Protection with RequestMap

66

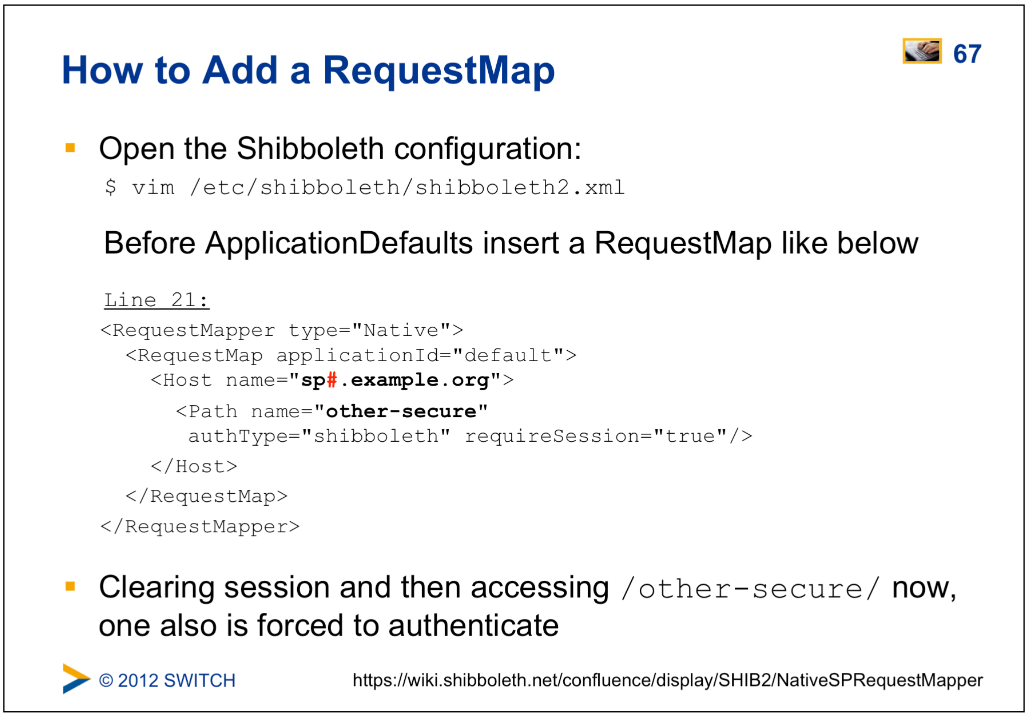
- mod_shib provides request URL to shibd to proccess it
  Therefore, shibd can enforce access control as well
  This is required for IIS web servers
- First ensure that requests for other-secure are handled by shibd without setting any specific session requirements

```
$ vim /var/www/html/other-secure/.htaccess
```

```
AuthType shibboleth
require shibboleth
```

https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPRequestMapper

Notes:



67

How to Add a RequestMap

- Open the Shibboleth configuration:

```
$ vim /etc/shibboleth/shibboleth2.xml
```

Before ApplicationDefaults insert a RequestMap like below

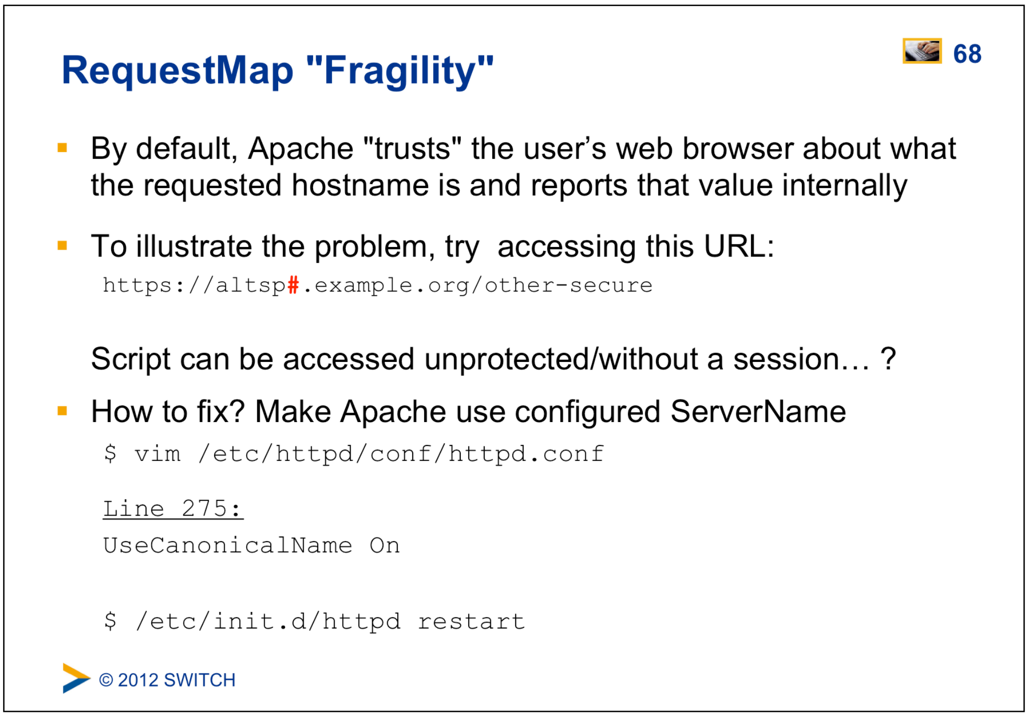
```
Line 21:
<RequestMapper type="Native">
  <RequestMap applicationId="default">
    <Host name="sp#.example.org">

      <Path name="other-secure"
       authType="shibboleth" requireSession="true"/>
    </Host>
  </RequestMap>
</RequestMapper>
```

- Clearing session and then accessing `/other-secure/` now, one also is forced to authenticate

https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPRequestMapper

Notes: ____________________



68

RequestMap "Fragility"

- By default, Apache "trusts" the user’s web browser about what the requested hostname is and reports that value internally
- To illustrate the problem, try accessing this URL:

```
https://altsp#.example.org/other-secure
```

Script can be accessed unprotected/without a session… ?

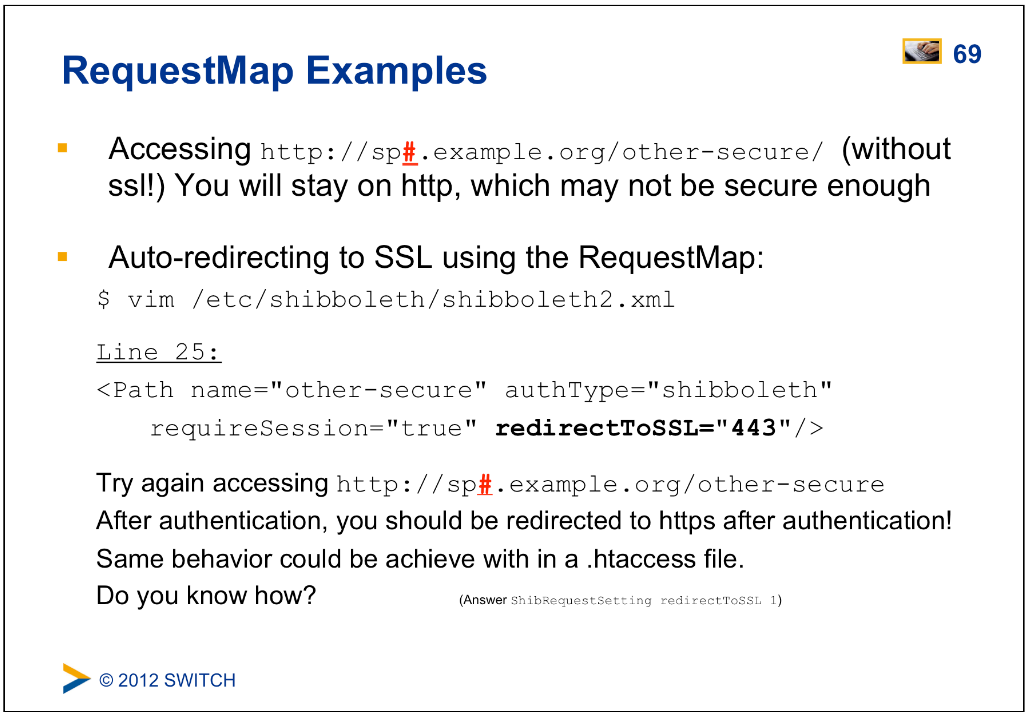
- How to fix? Make Apache use configured ServerName

```
$ vim /etc/httpd/conf/httpd.conf

Line 275:
UseCanonicalName On

$ /etc/init.d/httpd restart
```

Notes: ____________________



RequestMap Examples

69

- Accessing `http://sp#.example.org/other-secure/` (without ssl!) You will stay on http, which may not be secure enough

- Auto-redirecting to SSL using the RequestMap:

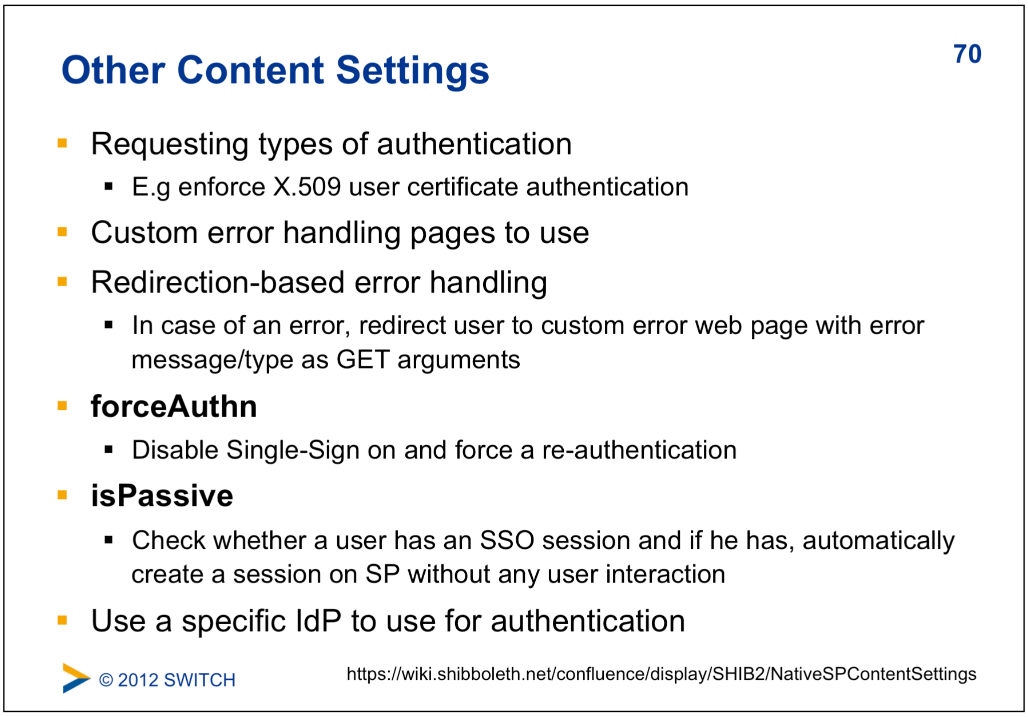
```
$ vim /etc/shibboleth/shibboleth2.xml
```

Line 25:

```
<Path name="other-secure" authType="shibboleth"
    requireSession="true" redirectToSSL="443"/>
```

Try again accessing `http://sp#.example.org/other-secure`
After authentication, you should be redirected to https after authentication!
Same behavior could be achieve with in a .htaccess file.
Do you know how? (Answer `ShibRequestSetting redirectToSSL 1`)

Notes: ____________________



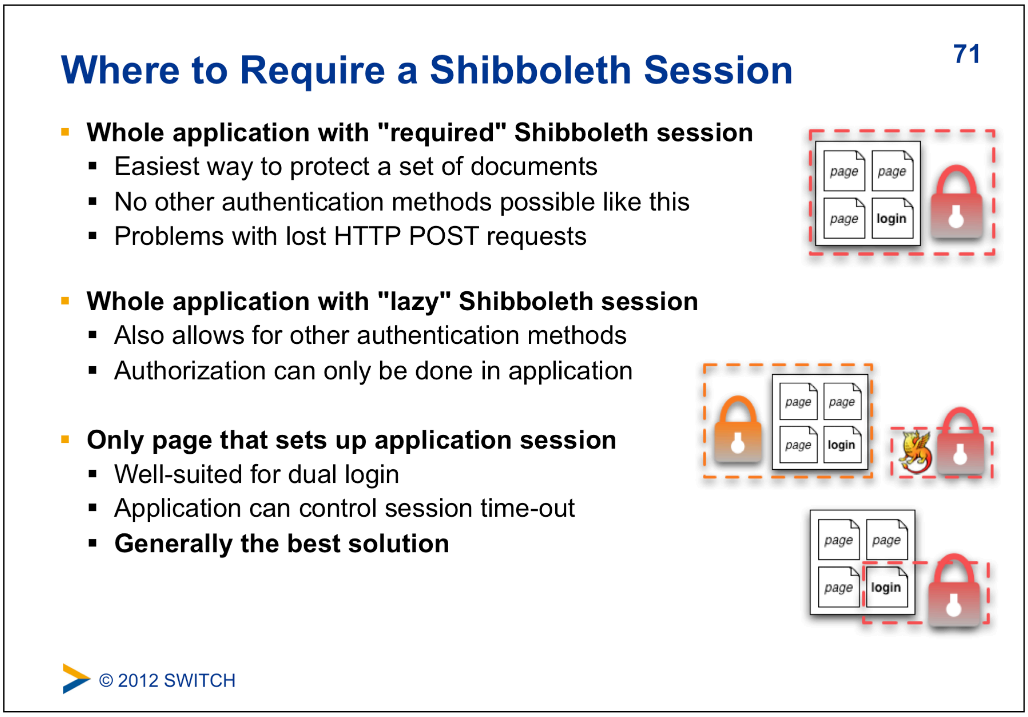
Other Content Settings

70

- Requesting types of authentication
  - E.g enforce X.509 user certificate authentication
- Custom error handling pages to use
- Redirection-based error handling
  - In case of an error, redirect user to custom error web page with error message/type as GET arguments
- **forceAuthn**
  - Disable Single-Sign on and force a re-authentication
- **isPassive**
  - Check whether a user has an SSO session and if he has, automatically create a session on SP without any user interaction
- Use a specific IdP to use for authentication

https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPContentSettings

Notes: ____________________



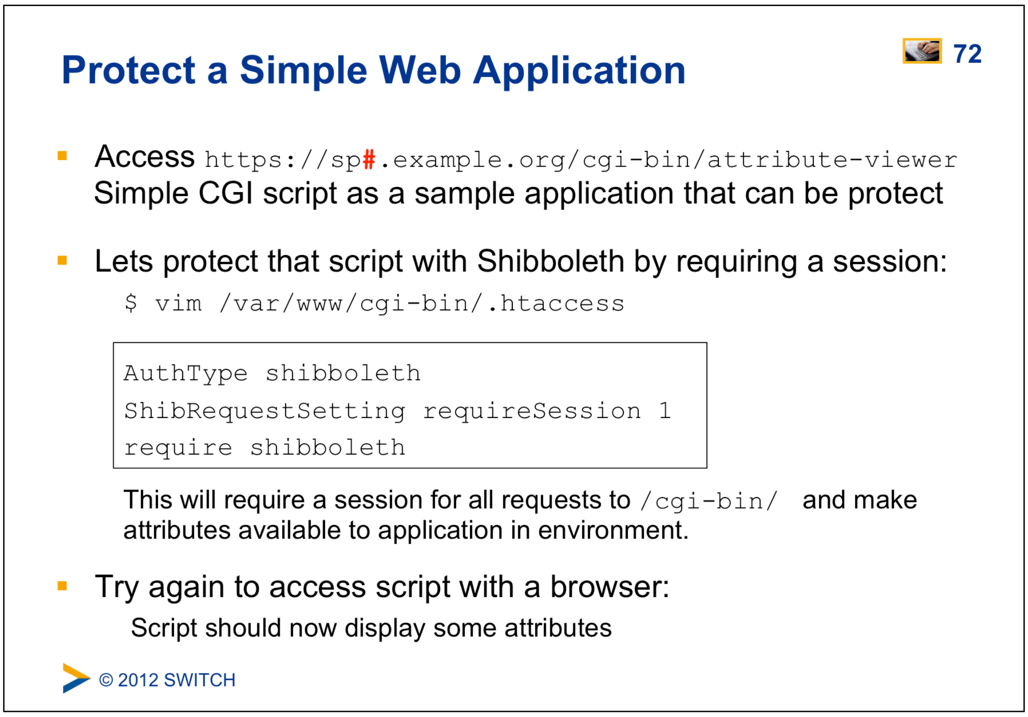
Where to Require a Shibboleth Session

71

- **Whole application with "required" Shibboleth session**
  - Easiest way to protect a set of documents
  - No other authentication methods possible like this
  - Problems with lost HTTP POST requests
- **Whole application with "lazy" Shibboleth session**
  - Also allows for other authentication methods
  - Authorization can only be done in application
- **Only page that sets up application session**
  - Well-suited for dual login
  - Application can control session time-out
  - **Generally the best solution**

© 2012 SWITCH

Notes: ______________________________



Protect a Simple Web Application

72

- Access `https://sp#.example.org/cgi-bin/attribute-viewer`
  Simple CGI script as a sample application that can be protect
- Lets protect that script with Shibboleth by requiring a session:

```
$ vim /var/www/cgi-bin/.htaccess
```

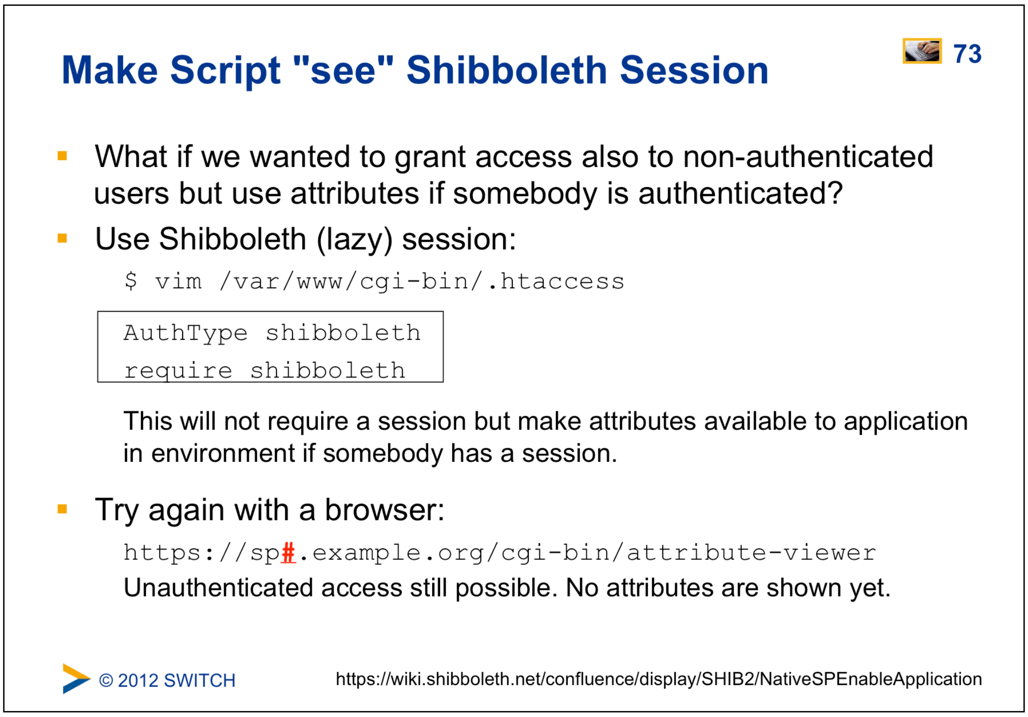
```
AuthType shibboleth
ShibRequestSetting requireSession 1
require shibboleth
```

This will require a session for all requests to `/cgi-bin/` and make attributes available to application in environment.

- Try again to access script with a browser:
  Script should now display some attributes

© 2012 SWITCH

Notes: ______________________________



Make Script "see" Shibboleth Session

73

- What if we wanted to grant access also to non-authenticated users but use attributes if somebody is authenticated?
- Use Shibboleth (lazy) session:

```
$ vim /var/www/cgi-bin/.htaccess
```

```
AuthType shibboleth
require shibboleth
```

This will not require a session but make attributes available to application in environment if somebody has a session.

- Try again with a browser:

```
https://sp#.example.org/cgi-bin/attribute-viewer
```

Unauthenticated access still possible. No attributes are shown yet.

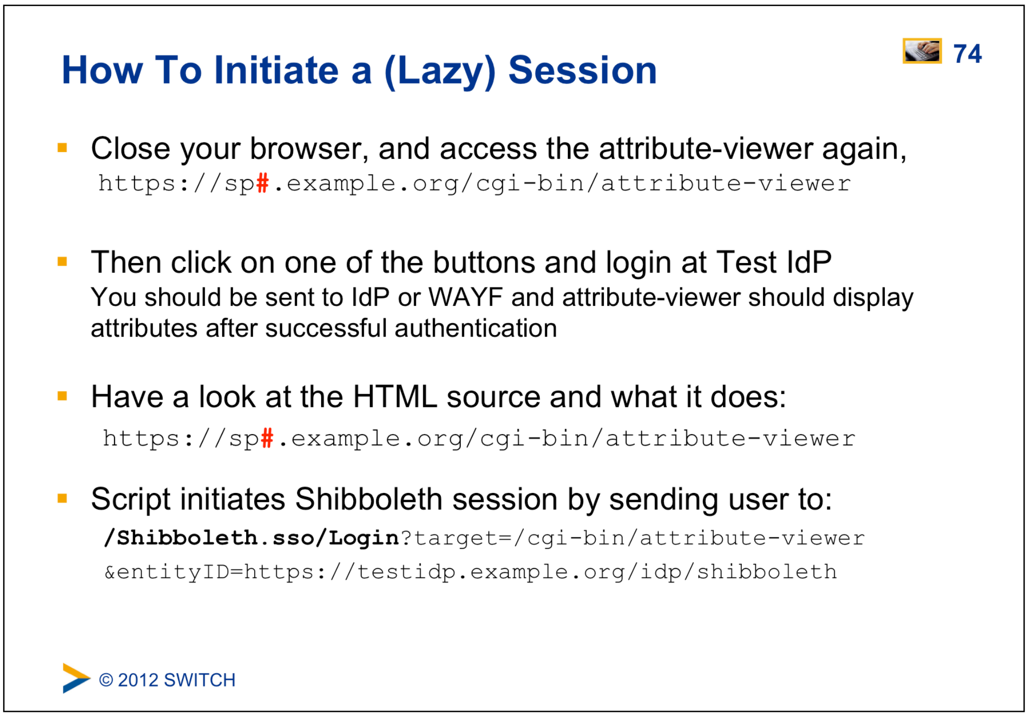
https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPEnableApplication

Notes: ____

____

____

____



How To Initiate a (Lazy) Session

74

- Close your browser, and access the attribute-viewer again,
  `https://sp#.example.org/cgi-bin/attribute-viewer`
- Then click on one of the buttons and login at Test IdP
  You should be sent to IdP or WAYF and attribute-viewer should display attributes after successful authentication
- Have a look at the HTML source and what it does:
  `https://sp#.example.org/cgi-bin/attribute-viewer`
- Script initiates Shibboleth session by sending user to:

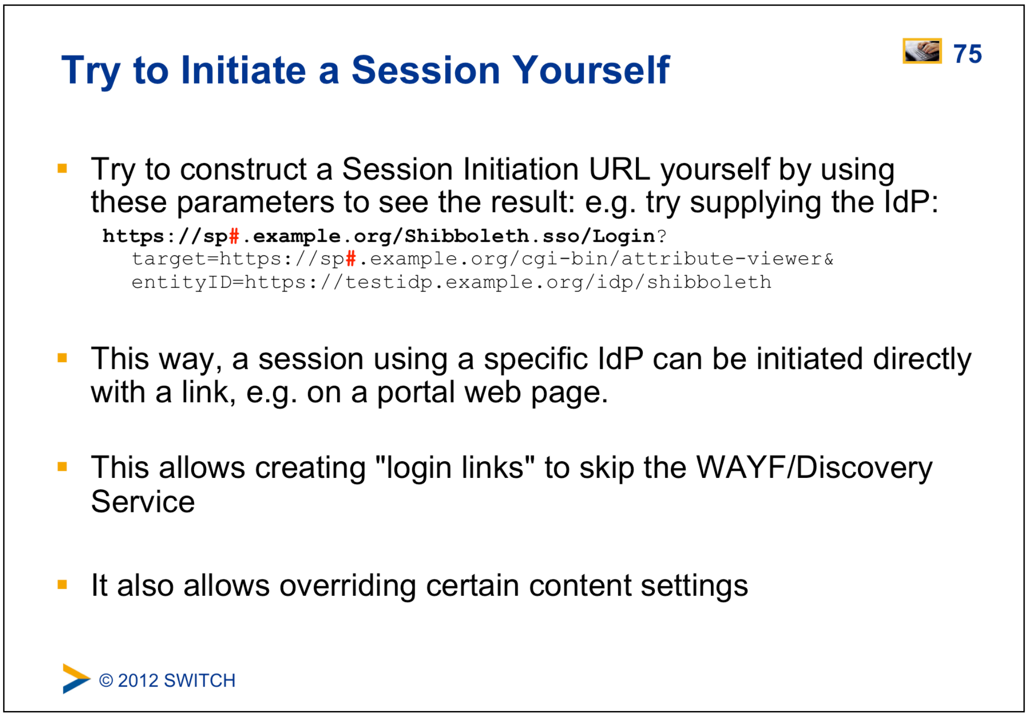
```
/Shibboleth.sso/Login?target=/cgi-bin/attribute-viewer
&entityID=https://testidp.example.org/idp/shibboleth
```

Notes: ____

____

____

____



Try to Initiate a Session Yourself

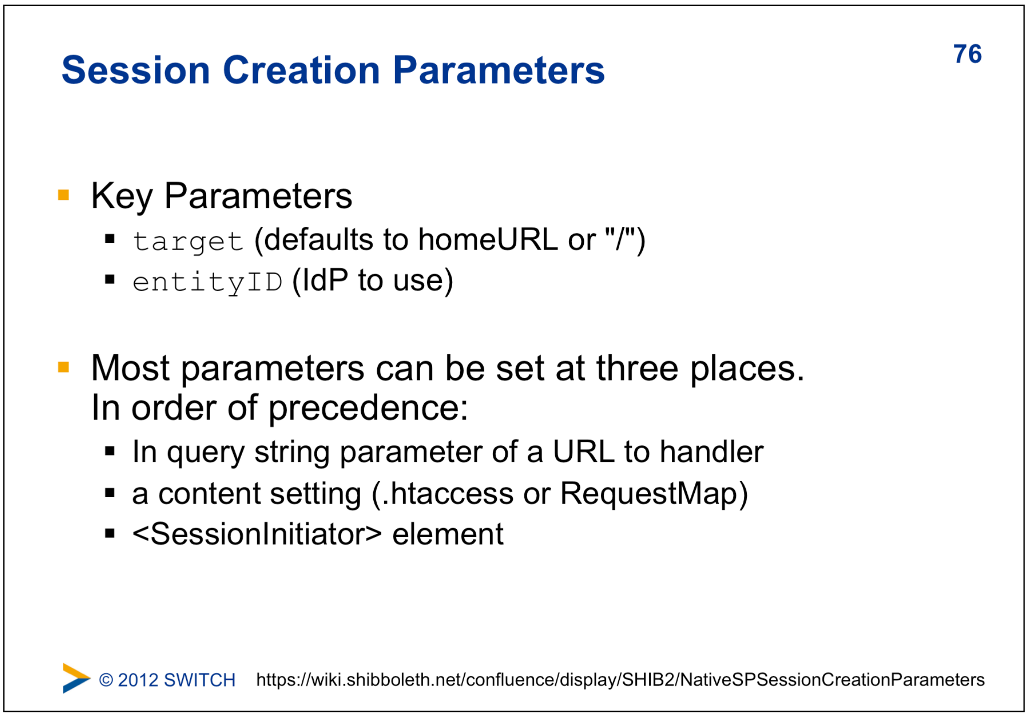
75

- Try to construct a Session Initiation URL yourself by using these parameters to see the result: e.g. try supplying the IdP:

```
https://sp#.example.org/Shibboleth.sso/Login?
   target=https://sp#.example.org/cgi-bin/attribute-viewer&
   entityID=https://testidp.example.org/idp/shibboleth
```

- This way, a session using a specific IdP can be initiated directly with a link, e.g. on a portal web page.
- This allows creating "login links" to skip the WAYF/Discovery Service
- It also allows overriding certain content settings

Notes:



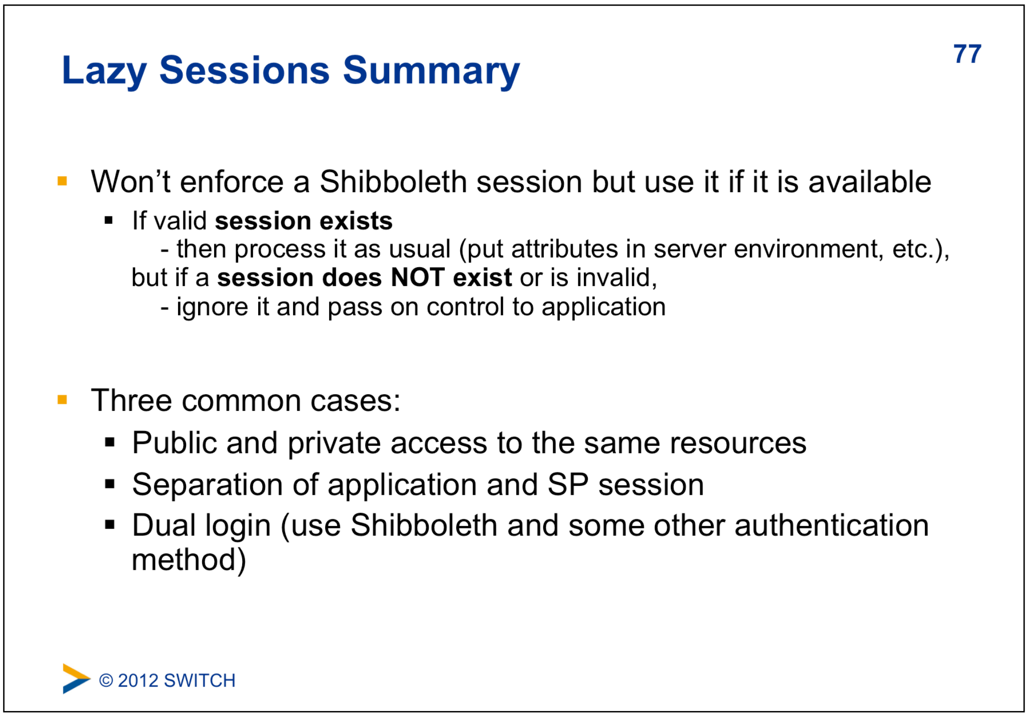
Session Creation Parameters

76

- Key Parameters
  - `target` (defaults to homeURL or "/")
  - `entityID` (IdP to use)
- Most parameters can be set at three places.
  In order of precedence:
  - In query string parameter of a URL to handler
  - a content setting (.htaccess or RequestMap)
  - <SessionInitiator> element

https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPSessionCreationParameters

Notes:



Lazy Sessions Summary

77

- Won’t enforce a Shibboleth session but use it if it is available
  - If valid **session exists**
    - then process it as usual (put attributes in server environment, etc.),

    but if a **session does NOT exist** or is invalid,
    - ignore it and pass on control to application
- Three common cases:
  - Public and private access to the same resources
  - Separation of application and SP session
  - Dual login (use Shibboleth and some other authentication method)

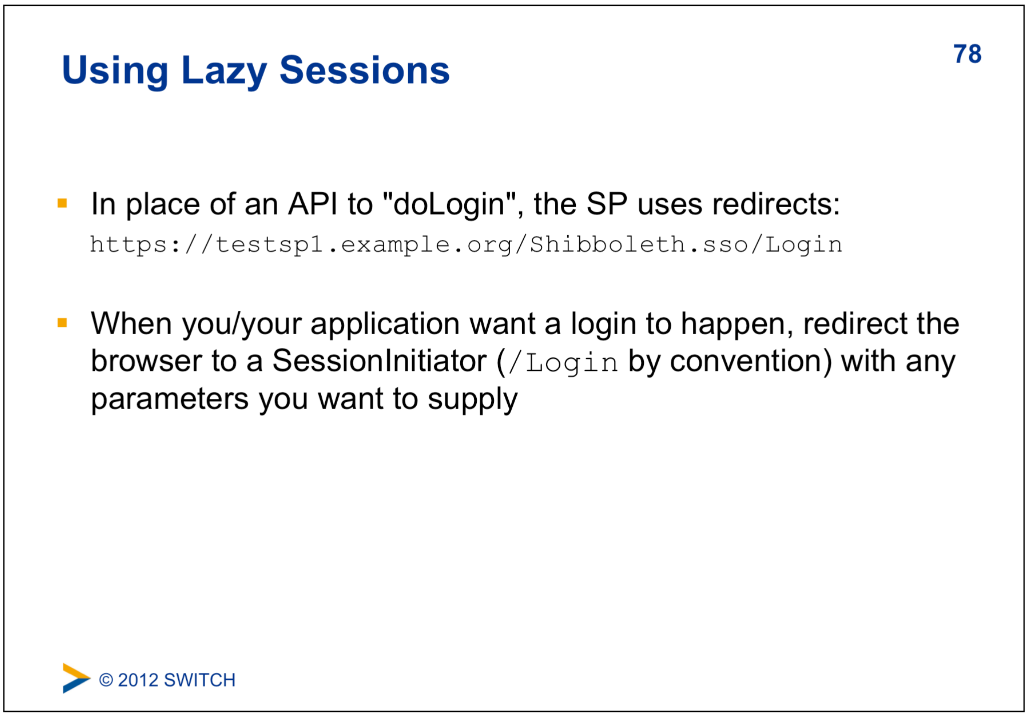
© 2012 SWITCH

Notes: ______________________________

____

____

____



Using Lazy Sessions

78

- In place of an API to "doLogin", the SP uses redirects:
  `https://testsp1.example.org/Shibboleth.sso/Login`
- When you/your application want a login to happen, redirect the browser to a SessionInitiator (`/Login` by convention) with any parameters you want to supply

© 2012 SWITCH

Notes: ______________________________

____

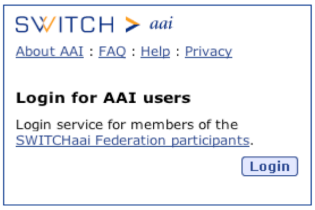
____

____

Some Concerns Regarding Dual Login

- Can be a viable option in case application must also be used by non-Shibboleth users

- Generally not recommended due to issues with:
  - **Usability:** Difficult to teach the users how to authenticate
  - **Security:** Shibboleth users shouldn't enter their password in the login form for the non-Shibboleth users…

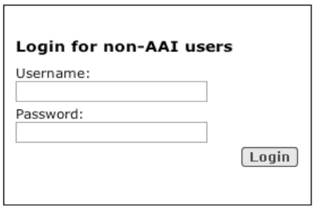


SWITCH > aai

About AAI : FAQ : Help : Privacy

Login for AAI users

Login service for members of the SWITCHaai Federation participants.



Login for non-AAI users

Username:

Password:

Notes: ______________________________

____

____

____

Virtual Home Organization and Guest Login

Excursion about dealing with user who don't have an AAI account already.

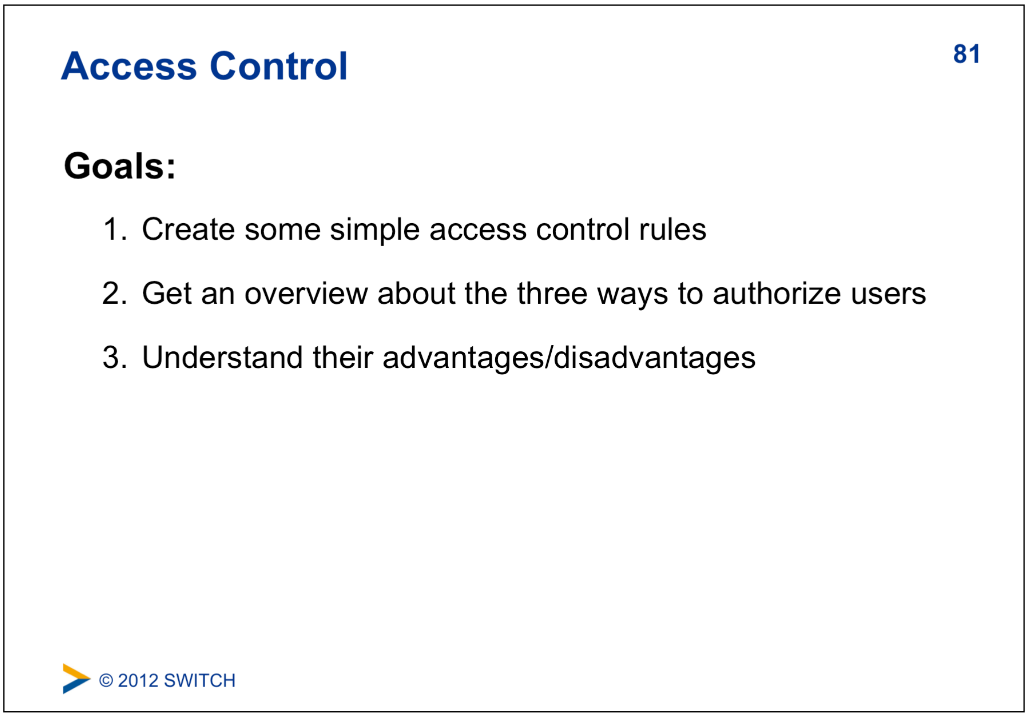
Please consult the table of contents to find this presentation in your hand-outs.

Notes: ______________________________

____

____

____



Access Control

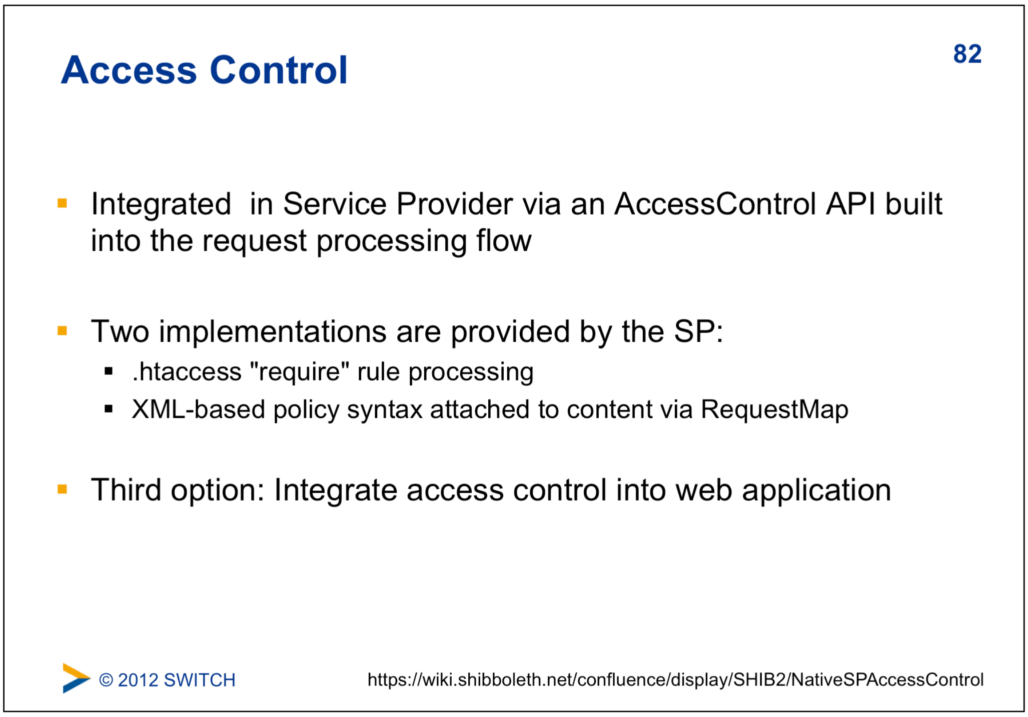
81

Goals:

1. Create some simple access control rules
2. Get an overview about the three ways to authorize users
3. Understand their advantages/disadvantages

© 2012 SWITCH

Notes:



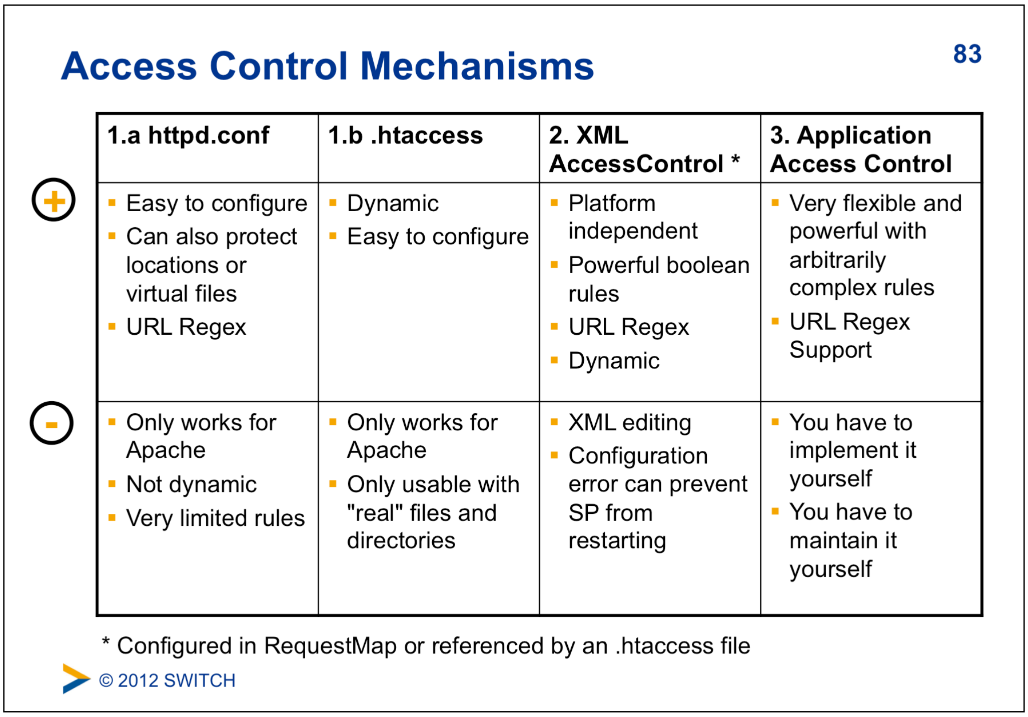
Access Control

82

- Integrated in Service Provider via an AccessControl API built into the request processing flow
- Two implementations are provided by the SP:
  - .htaccess "require" rule processing
  - XML-based policy syntax attached to content via RequestMap
- Third option: Integrate access control into web application

© 2012 SWITCH https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPAccessControl

Notes:



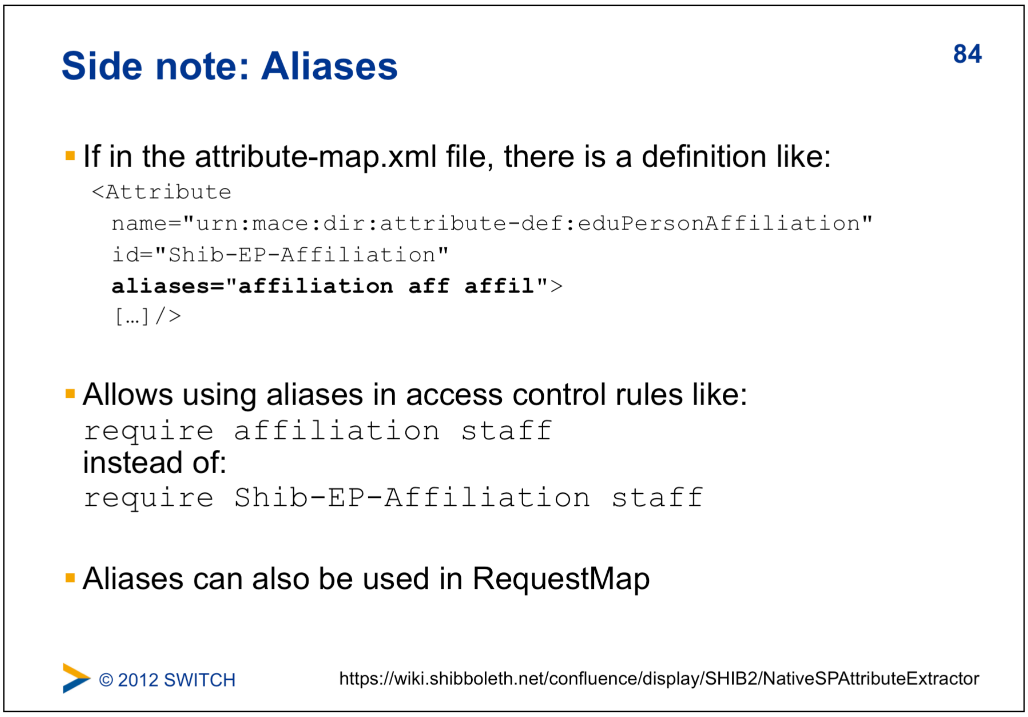
Access Control Mechanisms

83

	1.a httpd.conf	1.b .htaccess	2. XML AccessControl *	3. Application Access Control
⊕	- Easy to configure - Can also protect locations or virtual files - URL Regex	- Dynamic - Easy to configure	- Platform independent - Powerful boolean rules - URL Regex - Dynamic	- Very flexible and powerful with arbitrarily complex rules - URL Regex Support
⊖	- Only works for Apache - Not dynamic - Very limited rules	- Only works for Apache - Only usable with "real" files and directories	- XML editing - Configuration error can prevent SP from restarting	- You have to implement it yourself - You have to maintain it yourself

* Configured in RequestMap or referenced by an .htaccess file

Notes:



Side note: Aliases

84

- If in the attribute-map.xml file, there is a definition like:

```
<Attribute
  name="urn:mace:dir:attribute-def:eduPersonAffiliation"
  id="Shib-EP-Affiliation"
  aliases="affiliation aff affil">
  […]/>
```

- Allows using aliases in access control rules like:
  `require affiliation staff`
  instead of:
  `require Shib-EP-Affiliation staff`

- Aliases can also be used in RequestMap

https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPAttributeExtractor

Notes:

1. Apache httpd.conf or .htaccess Files

85

- Work almost like known Apache "require" rules
  E.g `require affiliation staff`
  or `require mail lukas@testidp.com chad@otheridp.org`
- Special rules:
  - `shibboleth` (no authorization)
  - `valid-user` (require a session, but NOT identity)
  - `user` (REMOTE_USER as usual)
  - `authnContextClassRef`, `authnContextDeclRef`
- Default is boolean "OR", use `ShibRequireAll` for AND rule
- Regular expressions supported using special syntax:

```
require rule ~ exp
e.g. require mail ~ ^.*@(it|faculty).example.org$
```

© 2012 SWITCH

Notes: ______________________________

____

____

____

1. Example .htaccess File

86

- Require a user to be a staff member:

```
$ vim /var/www/html/staff-only/.htaccess
```

```
AuthType shibboleth
ShibRequestSetting requireSession 1
require unscoped-affiliation staff
```

Then access : `https://sp#.example.org/staff-only/`
with demouser/password. Access should be granted.

- Then try the same again with demostudent/password
  Access should be denied

© 2012 SWITCH

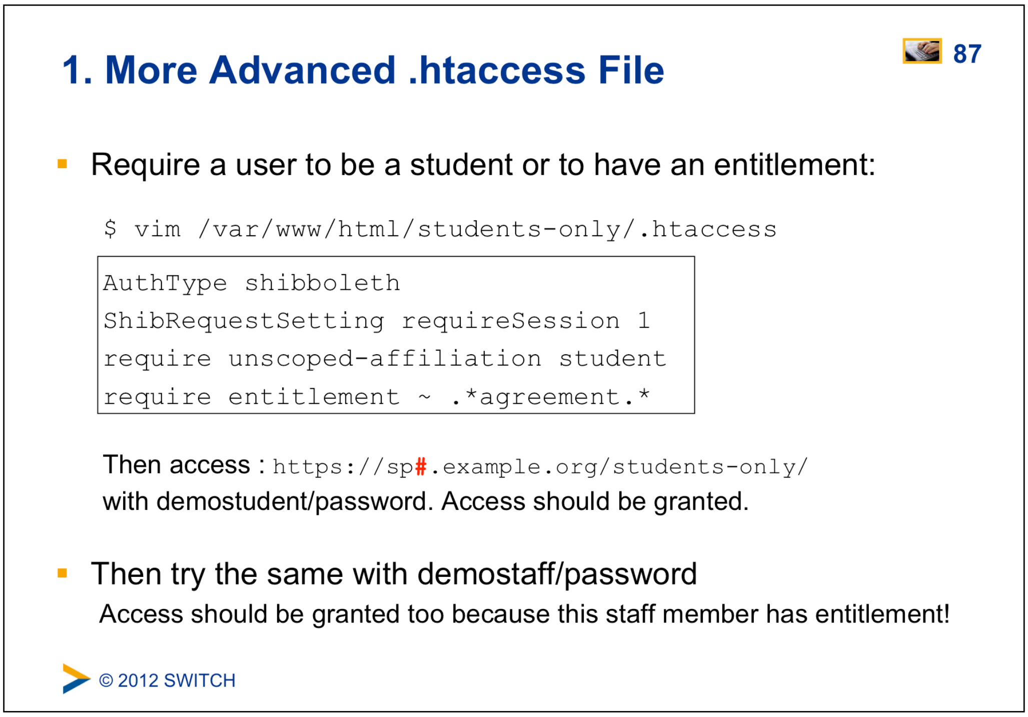
https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPApacheConfig

Notes: ______________________________

____

____

____



1. More Advanced .htaccess File

87

- Require a user to be a student or to have an entitlement:

```
$ vim /var/www/html/students-only/.htaccess
```

```
AuthType shibboleth
ShibRequestSetting requireSession 1
require unscoped-affiliation student
require entitlement ~ .*agreement.*
```

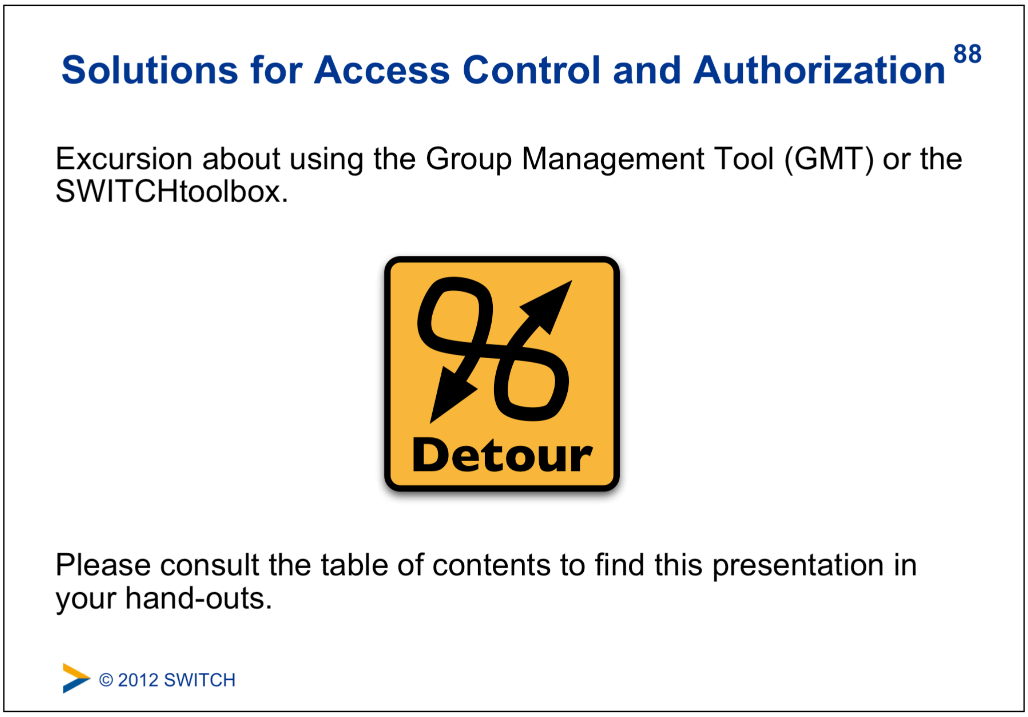
Then access : `https://sp#.example.org/students-only/`
with demostudent/password. Access should be granted.

- Then try the same with demostaff/password

Access should be granted too because this staff member has entitlement!

© 2012 SWITCH

Notes:



Solutions for Access Control and Authorization

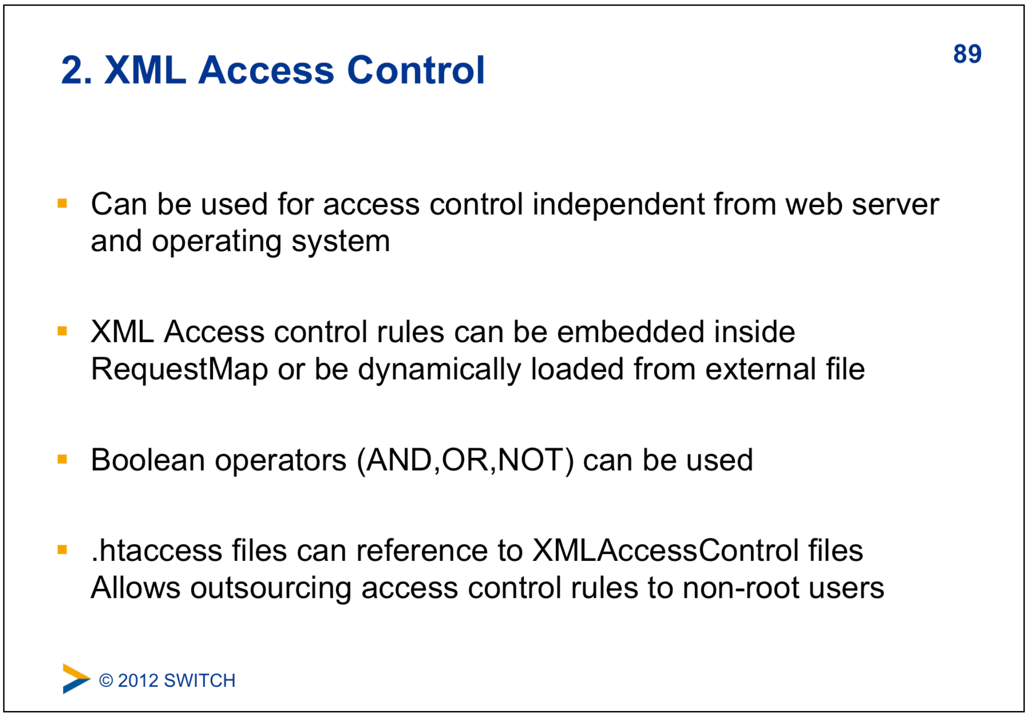
88

Excursion about using the Group Management Tool (GMT) or the SWITCHtoolbox.

Please consult the table of contents to find this presentation in your hand-outs.

© 2012 SWITCH

Notes:

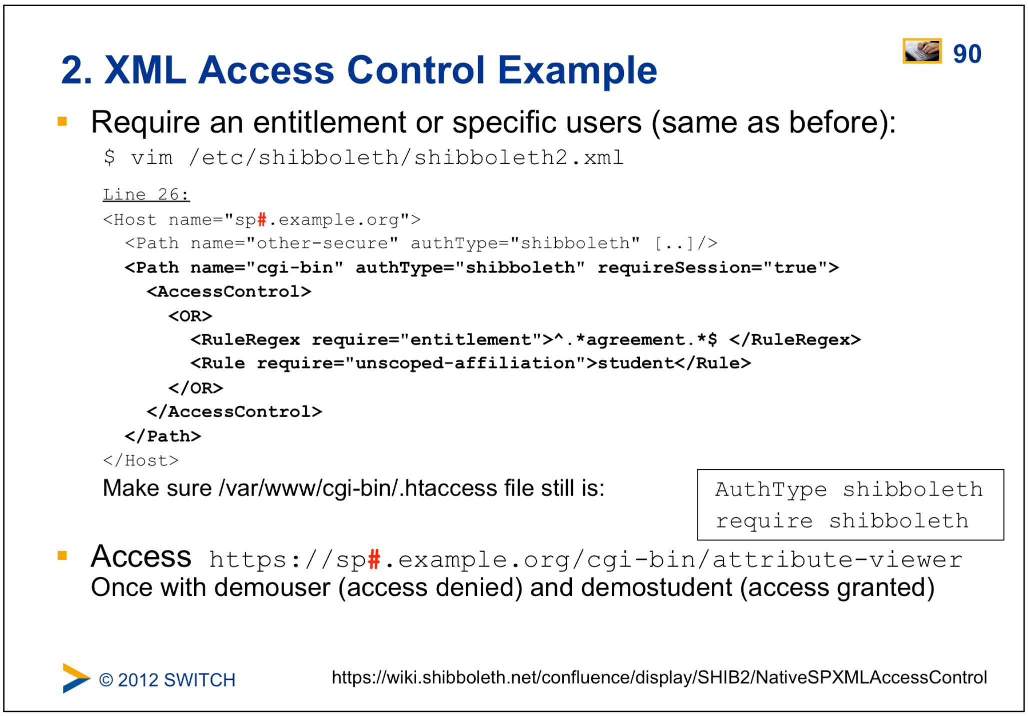


89

2. XML Access Control

- Can be used for access control independent from web server and operating system
- XML Access control rules can be embedded inside RequestMap or be dynamically loaded from external file
- Boolean operators (AND,OR,NOT) can be used
- .htaccess files can reference to XMLAccessControl files
  Allows outsourcing access control rules to non-root users

Notes:



90

2. XML Access Control Example

- Require an entitlement or specific users (same as before):

```
$ vim /etc/shibboleth/shibboleth2.xml
```

Line 26:

```
<Host name="sp#.example.org">
  <Path name="other-secure" authType="shibboleth" [..]/>
  <Path name="cgi-bin" authType="shibboleth" requireSession="true">
    <AccessControl>
      <OR>
        <RuleRegex require="entitlement">^.*agreement.*$ </RuleRegex>
        <Rule require="unscoped-affiliation">student</Rule>
      </OR>
    </AccessControl>
  </Path>
</Host>
```

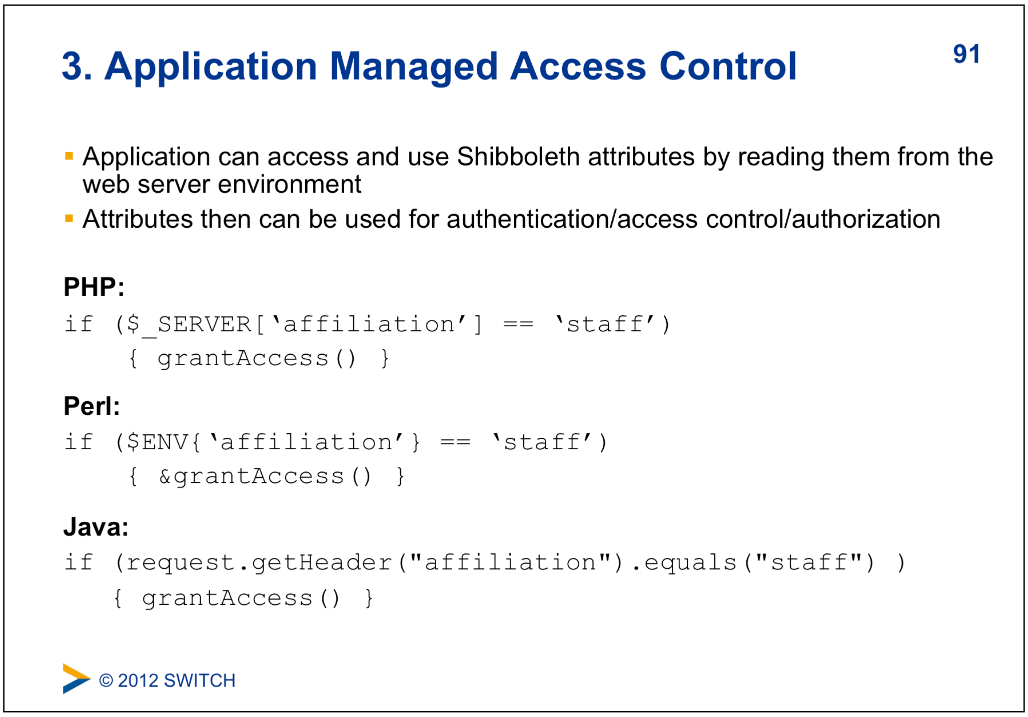
Make sure /var/www/cgi-bin/.htaccess file still is:

```
AuthType shibboleth
require shibboleth
```

- Access `https://sp#.example.org/cgi-bin/attribute-viewer`
  Once with demouser (access denied) and demostudent (access granted)

https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPXMLAccessControl

Notes:



3. Application Managed Access Control

91

- Application can access and use Shibboleth attributes by reading them from the web server environment
- Attributes then can be used for authentication/access control/authorization

PHP:

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

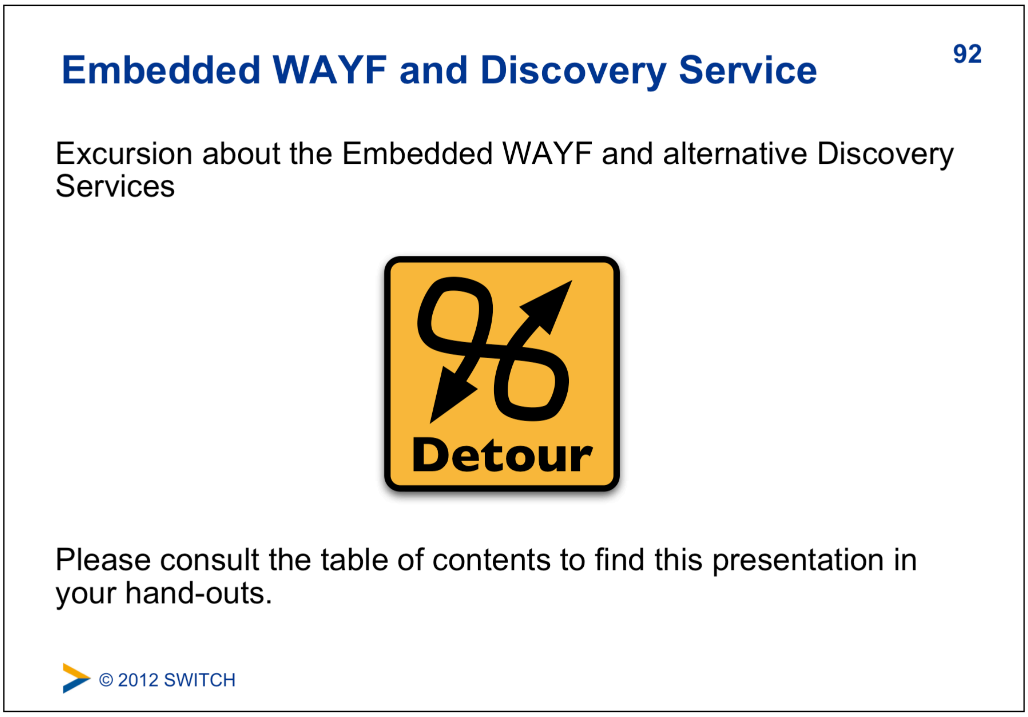
Perl:

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

Java:

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

Notes:



Embedded WAYF and Discovery Service

92

Excursion about the Embedded WAYF and alternative Discovery Services

Please consult the table of contents to find this presentation in your hand-outs.

Notes:

Using the SWITCHaai Embedded WAYF

93

Goals:

1. Add a Discovery Service/WAYF to a HTML web page
2. Configure Embedded WAYF
3. Learn about alternatives to Embedded WAYF

Notes: ____________________

____

____

____

How to Add Embedded WAYF

94

- In web browser open:
  https://ds.example.org/DS/WAYF/embedded-wayf.js/snippet.txt
- Copy the whole HTML snippet
- Then open /var/www/html/index.html in

  ```
  $ vim /var/www/html/index.html
  ```

  Paste the copied text at line 15

  ```
  Line 19:
  <!-- EMBEDDED-WAYF-START -->
  <script type="text/javascript"><!--
  // To use this JavaScript, please access:
  // https://ds.example.org/DS/WAYF/embedded-wayf.js/snippet.html
  // and copy/paste the resulting HTML snippet to an unprotected web page
    that
  [...]
  ```

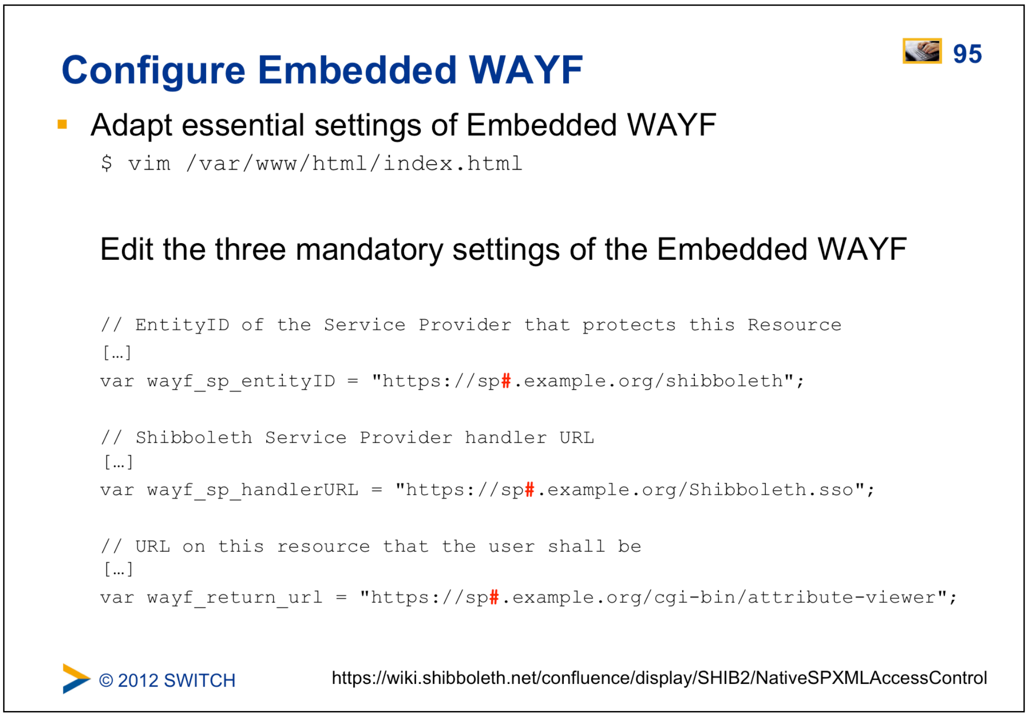
https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPXMLAccessControl

Notes: ____________________

____

____

____



Configure Embedded WAYF

95

- Adapt essential settings of Embedded WAYF

```
$ vim /var/www/html/index.html
```

Edit the three mandatory settings of the Embedded WAYF

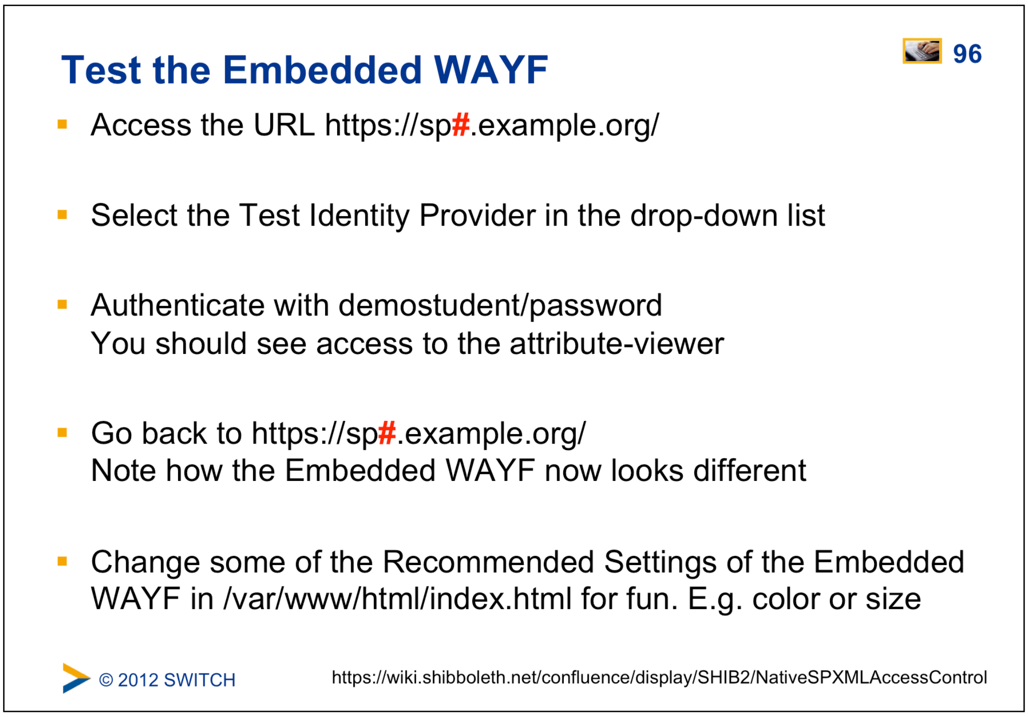
```
// EntityID of the Service Provider that protects this Resource
[…]
var wayf_sp_entityID = "https://sp#.example.org/shibboleth";

// Shibboleth Service Provider handler URL
[…]
var wayf_sp_handlerURL = "https://sp#.example.org/Shibboleth.sso";

// URL on this resource that the user shall be
[…]
var wayf_return_url = "https://sp#.example.org/cgi-bin/attribute-viewer";
```

https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPXMLAccessControl

Notes: ____



Test the Embedded WAYF

96

- Access the URL https://sp#.example.org/
- Select the Test Identity Provider in the drop-down list
- Authenticate with demostudent/password
  You should see access to the attribute-viewer
- Go back to https://sp#.example.org/
  Note how the Embedded WAYF now looks different
- Change some of the Recommended Settings of the Embedded WAYF in /var/www/html/index.html for fun. E.g. color or size

https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPXMLAccessControl

Notes: ____

Service Provider Virtualization

97

How to protect multiple applications with one physical Service Provider and how to have one Shibboleth application distributed across mulitple physical hosts.

Please consult the table of contents to find this presentation in your hand-outs.

Notes: ______________________________

____

____

____

Adding an Application

98

- **Goal:** Add a second application with a different entityID living on its own virtual host
- Add the application and map the host to it:

```
$ vim /etc/shibboleth/shibboleth2.xml

Line 23:
<RequestMap applicationId="default">
  <Host name="altsp#.example.org" applicationId="alt"/>

Around Line 128:
  <ApplicationOverride id="alt" entityID="https://
  altsp#.example.org/shibboleth"/>
</ApplicationDefaults>
```

https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPApplication

Notes: ______________________________

____

____

____

Turning off Canonical Names Again

99

- For the additional application, canonical names should be turned off again
- Add the application and map the host to it:

```
$ vim /etc/httpd/conf/httpd.conf

Line 273:
UseCanonicalName Off
```

- Restart Apache

```
$ /etc/init.d/httpd restart
```

Notes:

Test Added Application

100

- In order to test the added application, access

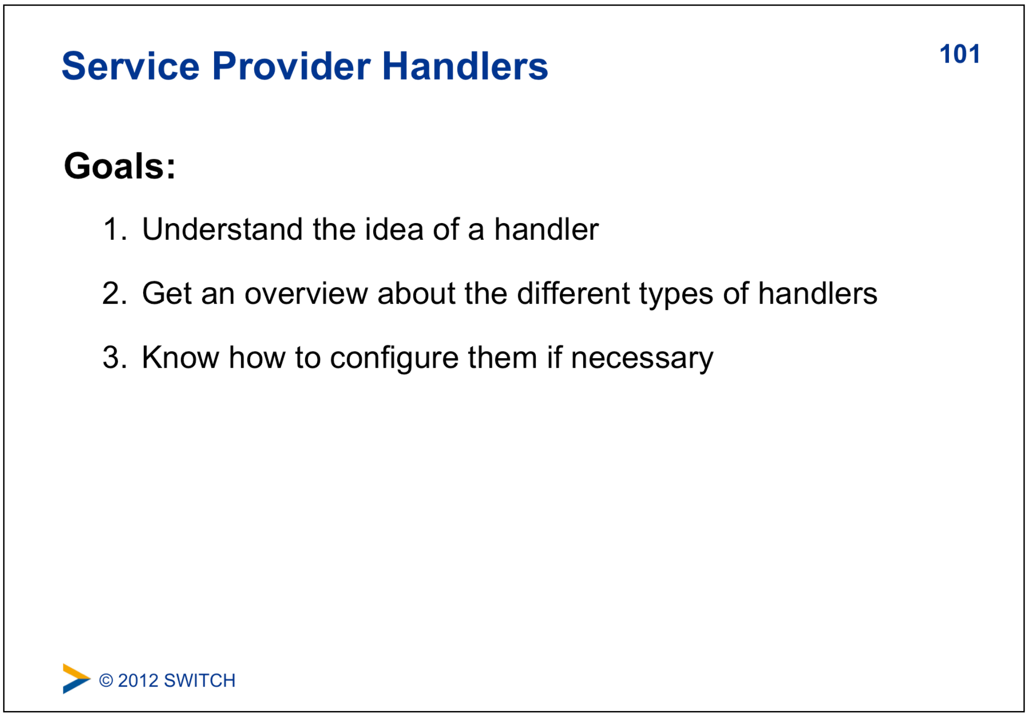
  `https://altsp#.example.org/secure/`

  authenticate and check the log file with:

```
$ less /var/log/shibboleth/shibd.log
```

- The IdP will release only givenName and surname to all SPs whose entityID matches “https://altsp.* “
  Therefore, the logical SP with entityID https://sp#.example.org/shibboleth/ will only get these two attributes.

Notes:



Service Provider Handlers

101

Goals:

1. Understand the idea of a handler
2. Get an overview about the different types of handlers
3. Know how to configure them if necessary

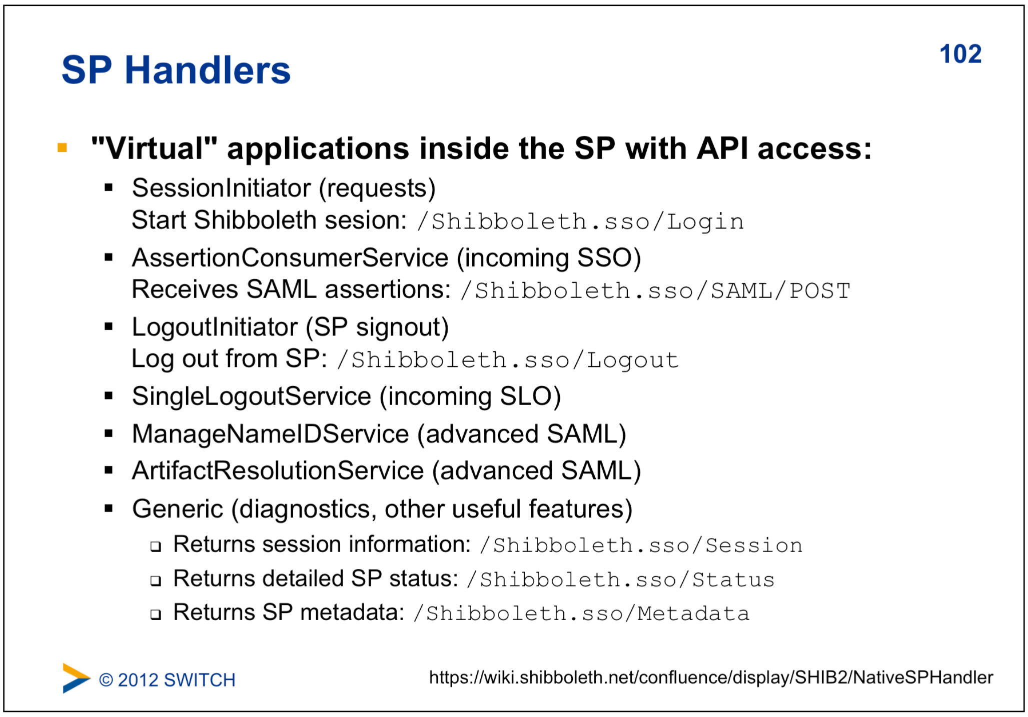
© 2012 SWITCH

Notes: ____

____

____

____



SP Handlers

102

- **"Virtual" applications inside the SP with API access:**
  - SessionInitiator (requests)
    Start Shibboleth sesion: `/Shibboleth.sso/Login`
  - AssertionConsumerService (incoming SSO)
    Receives SAML assertions: `/Shibboleth.sso/SAML/POST`
  - LogoutInitiator (SP signout)
    Log out from SP: `/Shibboleth.sso/Logout`
  - SingleLogoutService (incoming SLO)
  - ManageNameIDService (advanced SAML)
  - ArtifactResolutionService (advanced SAML)
  - Generic (diagnostics, other useful features)
    - ❑ Returns session information: `/Shibboleth.sso/Session`
    - ❑ Returns detailed SP status: `/Shibboleth.sso/Status`
    - ❑ Returns SP metadata: `/Shibboleth.sso/Metadata`

© 2012 SWITCH

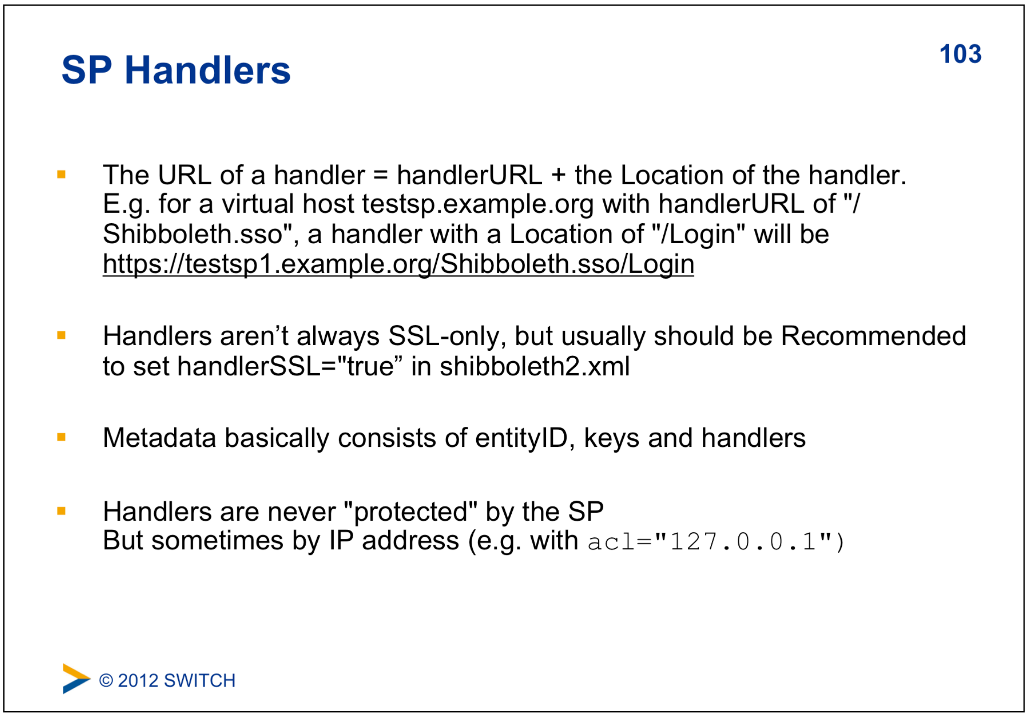
https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPHandler

Notes: ____

____

____

____



SP Handlers

103

- The URL of a handler = handlerURL + the Location of the handler. E.g. for a virtual host testsp.example.org with handlerURL of "/Shibboleth.sso", a handler with a Location of "/Login" will be https://testsp1.example.org/Shibboleth.sso/Login
- Handlers aren’t always SSL-only, but usually should be Recommended to set handlerSSL="true” in shibboleth2.xml
- Metadata basically consists of entityID, keys and handlers
- Handlers are never "protected" by the SP
  But sometimes by IP address (e.g. with `acl="127.0.0.1"`)

Notes: ____________________