Interfederation

Getting ready to cross borders

Serving Swiss Universities

Lukas Hämmerle
Thomas Lenggenhager
aai@switch.ch

Bern, 24. May 2011

Getting ready for the future

- Today
  - SWITCHaai is mostly bound to a CH/LI borders
    - Exception
      - International Federation Partners
      - Foreign users in the Virtual Home Organization (VHO)
  - Many national AAI's in place

- With interfederation we will be able to cross the borders
  - Swiss users will be able to access opted-in foreign SPs
  - Foreign users will be able to access opted-in Swiss SPs

- eduGAIN from GÉANT3 is the first interfederation service SWITCHaai will co-operate with
  - Others might follow

eduGAIN

http://edugain.org

What's different with interfederation?

- No longer a single legal or policy framework
  - Each federation has its own
  - eduGAIN has one as well [1]

- No single 'interfederation helpdesk' in case of problems
  - Debugging involves probably more parties
  - Involved parties will generally know less about each other

- Different sets of attributes used internationally
  - e.g. no studyLevel or studyBranch attributes

[1] http://www.geant.net/service/edugain/resources/Pages/home.aspx

What's to consider for IdPs?

- Release of personal information to foreign SPs
  - Install and activate User Consent for attribute release (uApprove)
  - Check your default Attribute Release Policy
    - To whom to release what by default?
  - Constantly review whether specific Attribute Policy Rules are necessary

What's to consider for SPs?

- Who shall be allowed to use my service?
  - Users from IdPs from
    - My Organization
    - SWITCHaai Federation
    - Interfederation
    - or my own selective set of IdPs
      Shibboleth SP software is capable of white- or black-listing IdPs with the metadata filter.

- Which attributes does my service **really** require?
  - Be as restrictive as possible
  - Check what IdPs might be able to provide

Interfederation & New AAI Legal Framework

- Temporary 'pilot' interfederation in 2011
  - Institutions invited to join during 2011,
    - if they have a use case for using interfederation either from their user-base or their SPs
    - or if they are interested to gain experience and be an early adopter!
  - Not yet covered by existing AAI framework, therefore each institution has to **opt-in** first
    - AAI OpCom Representative has to confirm that the institution is willing to participate in this pilot and is ready to go
    - After that, each entity of that institution can opt-in.
  - Interested to join? ➡ Contact the SWITCHaai Team!

How to enable Interfederation

Getting ready to technically cross federation borders

SWITCH

Serving Swiss Universities

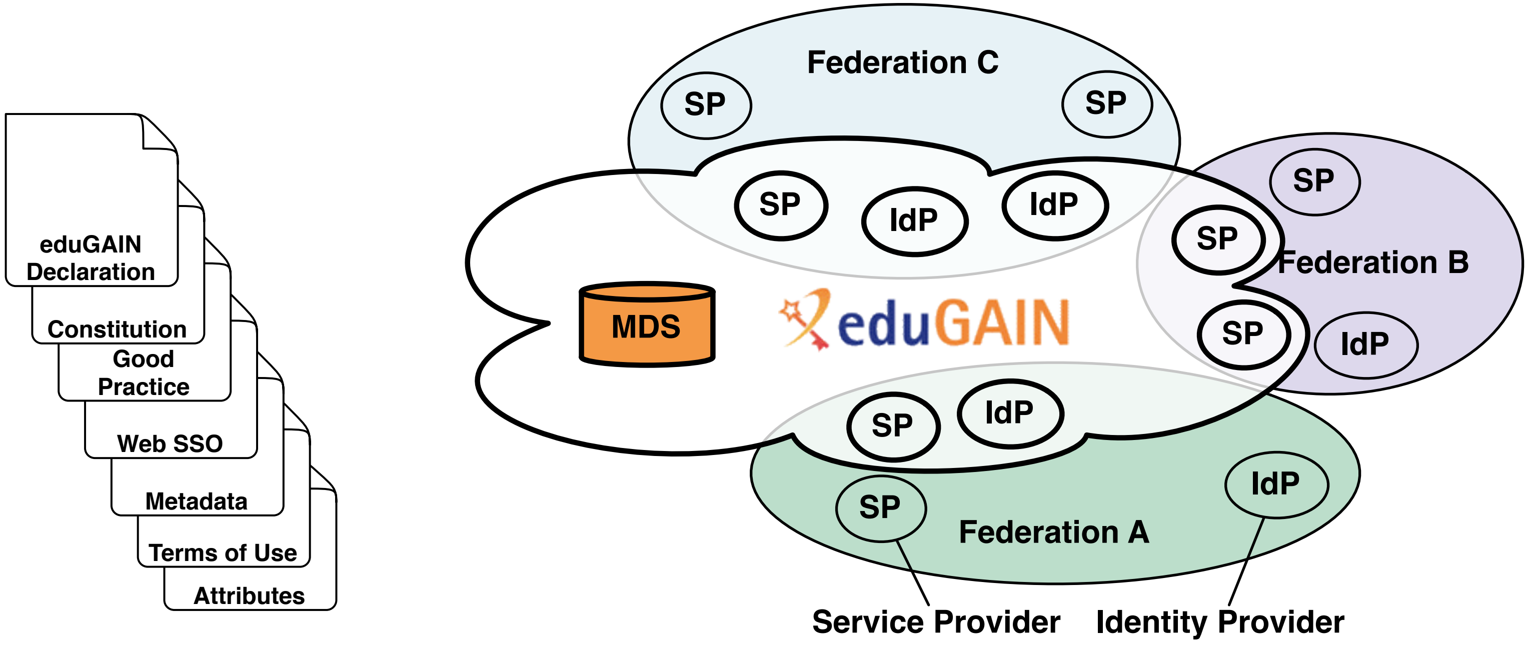
Lukas Hämmerle
lukas.haemmerle@switch.ch

Bern, 24. Mai 2011

Areas Affected by Interfederation

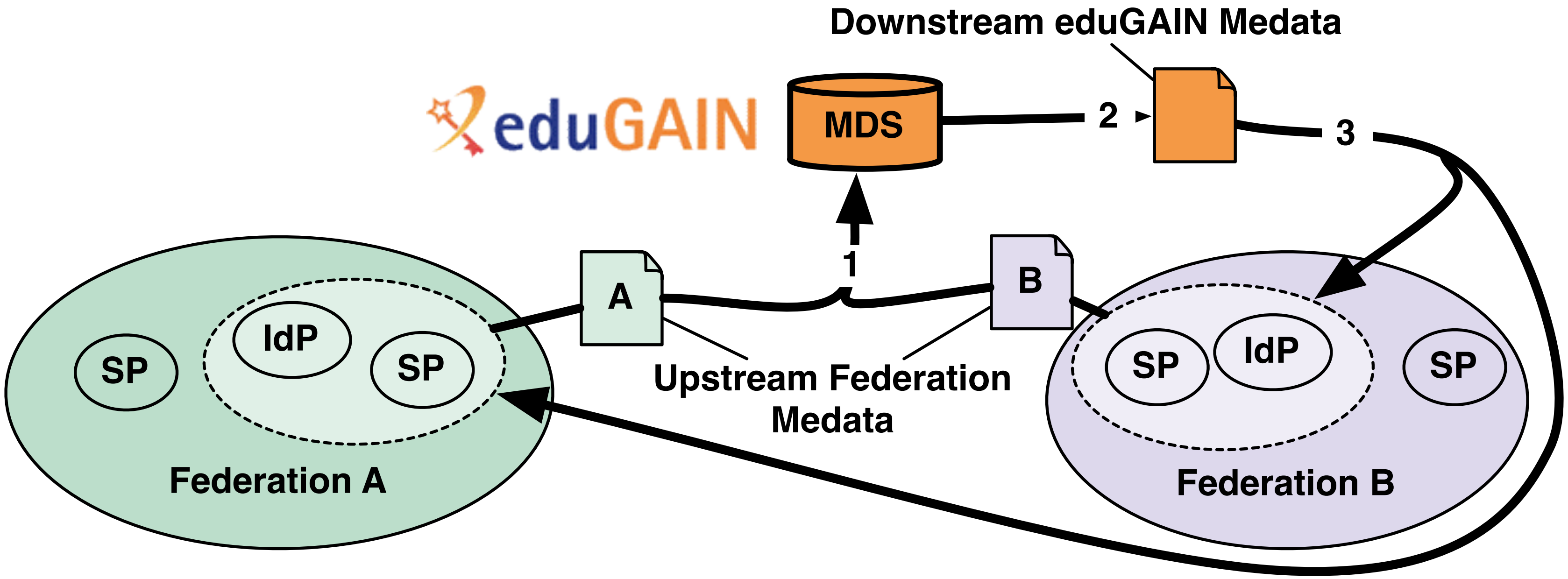
- Metadata Publishing & Consumption
- Supported Attributes
- Attribute Release
- Discovery Service
- Rollout to IdPs & SPs

Architecture of eduGAIN



- Subset of entities in a national federation also in eduGAIN
- Profile and policies **try** to harmonize environments
- Participants use interoperable SAML 2.0 (saml2int)
- Central SAML metadata service (MDS)

Metadata Flow in eduGAIN



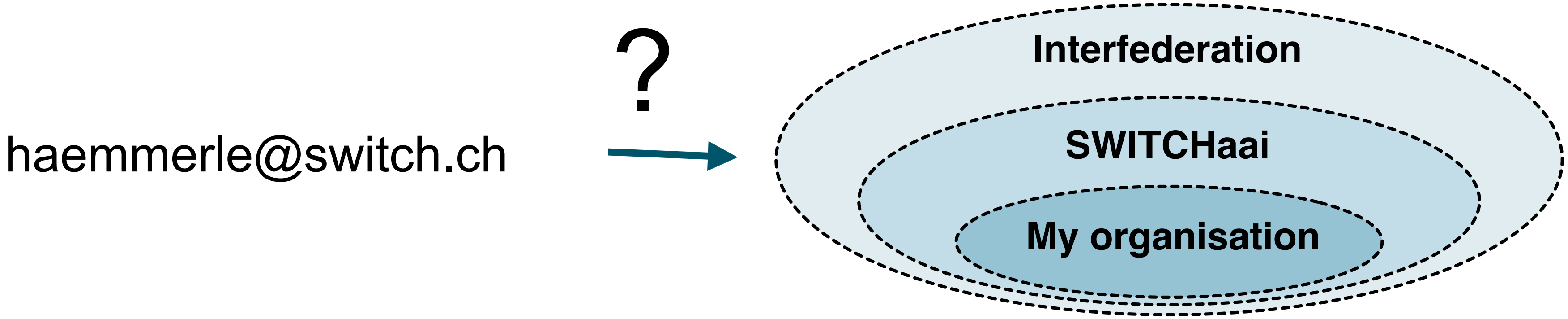
1. SWITCH publishes interfederation metadata subset
2. MDS aggregates all this metadata and republishes it
3. SWITCH processes and republishes eduGAIN metadata and interfederation SWITCHaai entities consume it

Attributes eduGAIN Recommends to Support

- Identity Provider will have to support additional attributes

	Attribute	Implementation Effort for SWITCHaai
New	displayName	Small, givenName + “ ” + surname
New	common name	Small, like displayName
	mail	Already supported
	eduPersonAffiliation	Already supported
New	eduPersonScopedAffiliation	Small, affiliation +
New	schacHomeOrganization	Already supported
New	schacHomeOrganizationType	Small, “urn:mace:terena.org:...” +
	eduPersonTargetedID	Already supported
	eduPersonPrincipalName	Deprecated, we recommend not to use

Attribute Release Policy


haemmerle@switch.ch

?

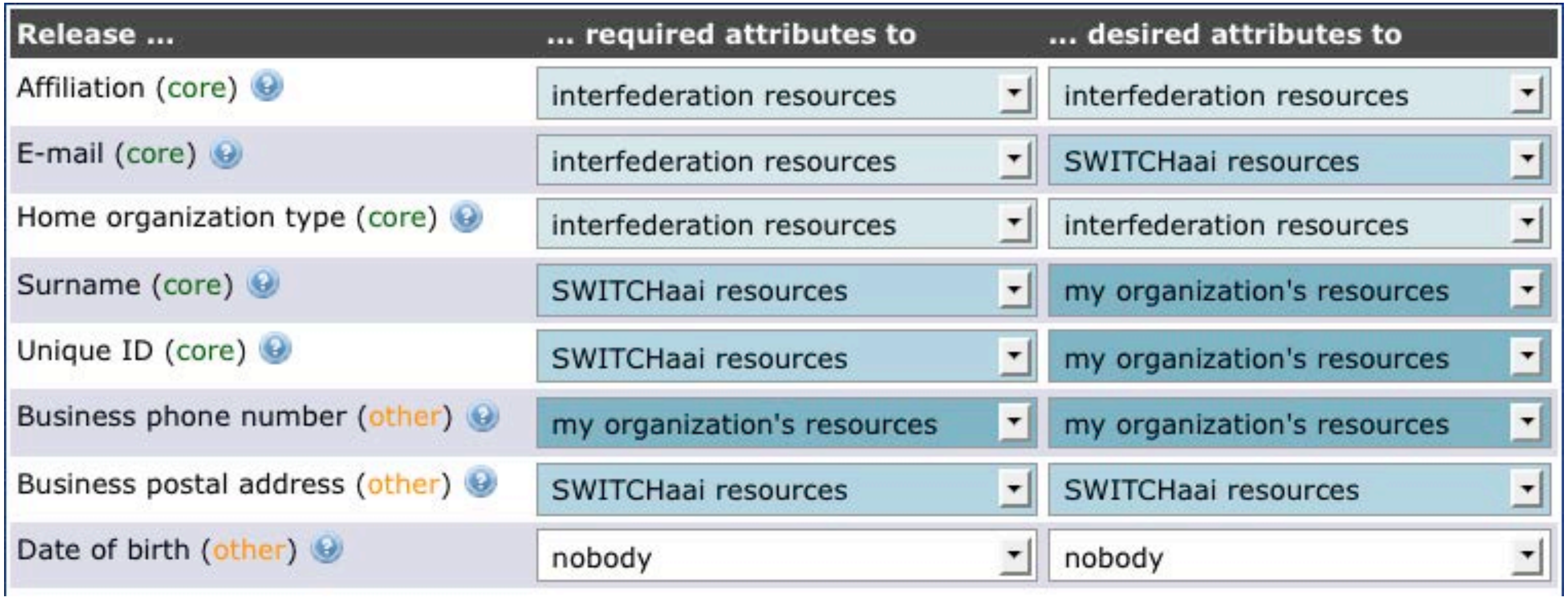
Interfederation

SWITCHaai

My organisation

- Each IdP admin can set:
  - A **default attribute release policy** for “required” and “desired” attributes
  - SP **specific attribute release policies**
- IdP admin defines release scope for an attribute
  - Release to: no one, organization, federation, interfederation
- Custom-tailored attribute policy files generated for each IdP
- IdPs download attribute release policy from RR
- IdP administrators receive “diffs” by email

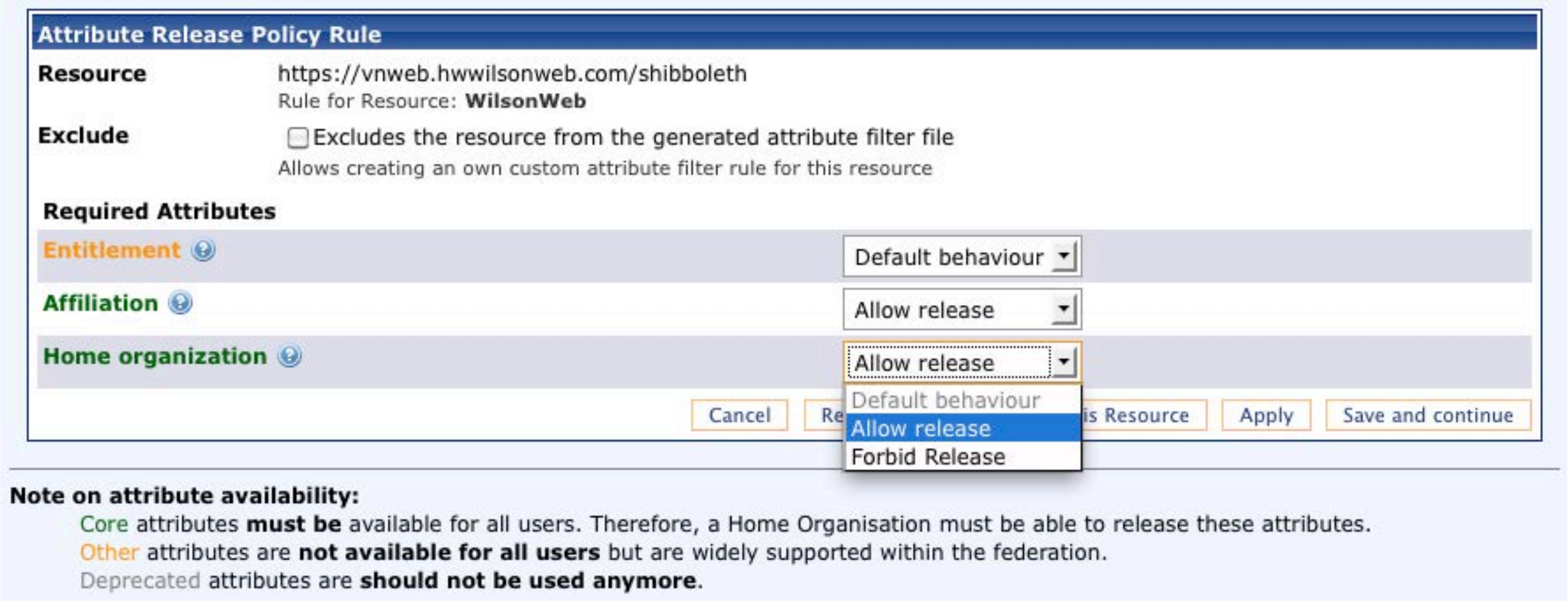
Default Release Policy of an IdP



Release ...	... required attributes to	... desired attributes to
Affiliation (core)	interfederation resources	interfederation resources
E-mail (core)	interfederation resources	SWITCHaai resources
Home organization type (core)	interfederation resources	interfederation resources
Surname (core)	SWITCHaai resources	my organization's resources
Unique ID (core)	SWITCHaai resources	my organization's resources
Business phone number (other)	my organization's resources	my organization's resources
Business postal address (other)	SWITCHaai resources	SWITCHaai resources
Date of birth (other)	nobody	nobody

- Default policy can be defined for all supported attributes which are “required” or “desired” by an SP
  - Expressed in <AttributeConsumingService> element in metadata
- Otherwise, eduPersonTargetedID and some non-personal attributes are used as SP’s attribute requirements

SP Specific Attribute Release Policy



Attribute Release Policy Rule

Resource https://vnweb.hwwilsonweb.com/shibboleth
Rule for Resource: **WilsonWeb**

Exclude □ Excludes the resource from the generated attribute filter file
Allows creating an own custom attribute filter rule for this resource

Required Attributes

Entitlement	Default behaviour
Affiliation	Allow release
Home organization	Allow release

Note on attribute availability:

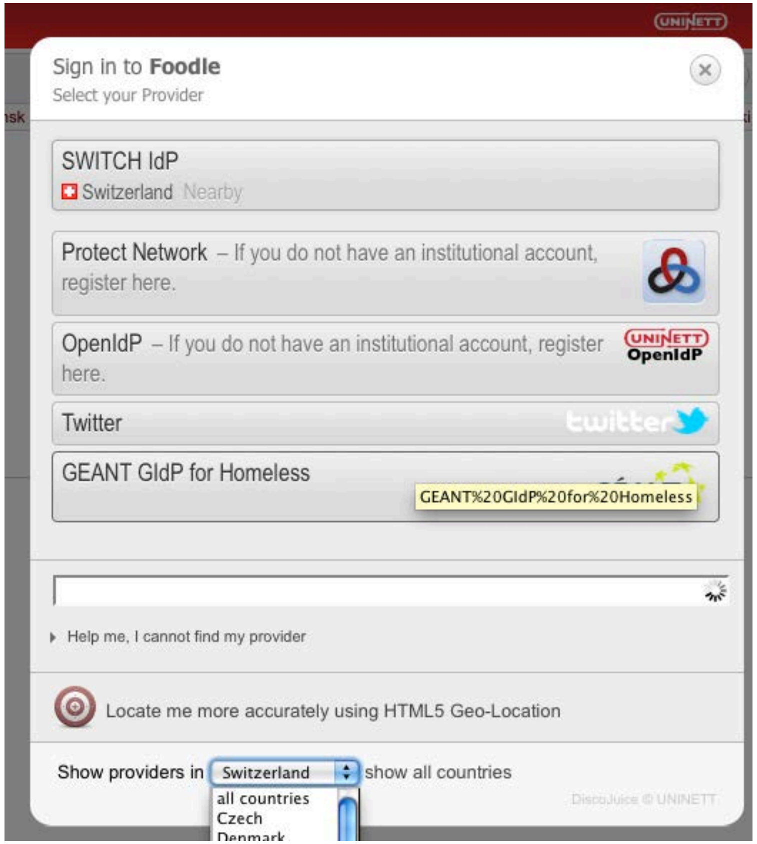
Core attributes **must be** available for all users. Therefore, a Home Organisation must be able to release these attributes.
Other attributes are **not available for all users** but are widely supported within the federation.
Deprecated attributes are **should not be used anymore**.

- Specific policy always overrules default policy
- Optionally exclude SPs from release policy

IdP Discovery and Interfederation

- Discovery is more challenging due to huge number of IdPs
- Two categories of interfederated services:
  - Services accessed by users from hundreds of IdPs
    - ❑ E.g. foodl.org, TNC registration platform
    - ❑ Requires a more complex solution like Shibboleth EDS or DiscoJuice
  - Services accessed by users from only few IdPs:
    - ❑ E.g. smaller research projects, bilaterally used services
    - ❑ Can be handled by simple login links or a manually managed Discovery Service

Interfederated Discovery Service Examples



Sign in to **Foodle**

Select your Provider

SWITCH IdP
Switzerland Nearby

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

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

Twitter

GEANT GIdP for Homeless

GEANT%20GIdP%20for%20Homeless

Help me, I cannot find my provider

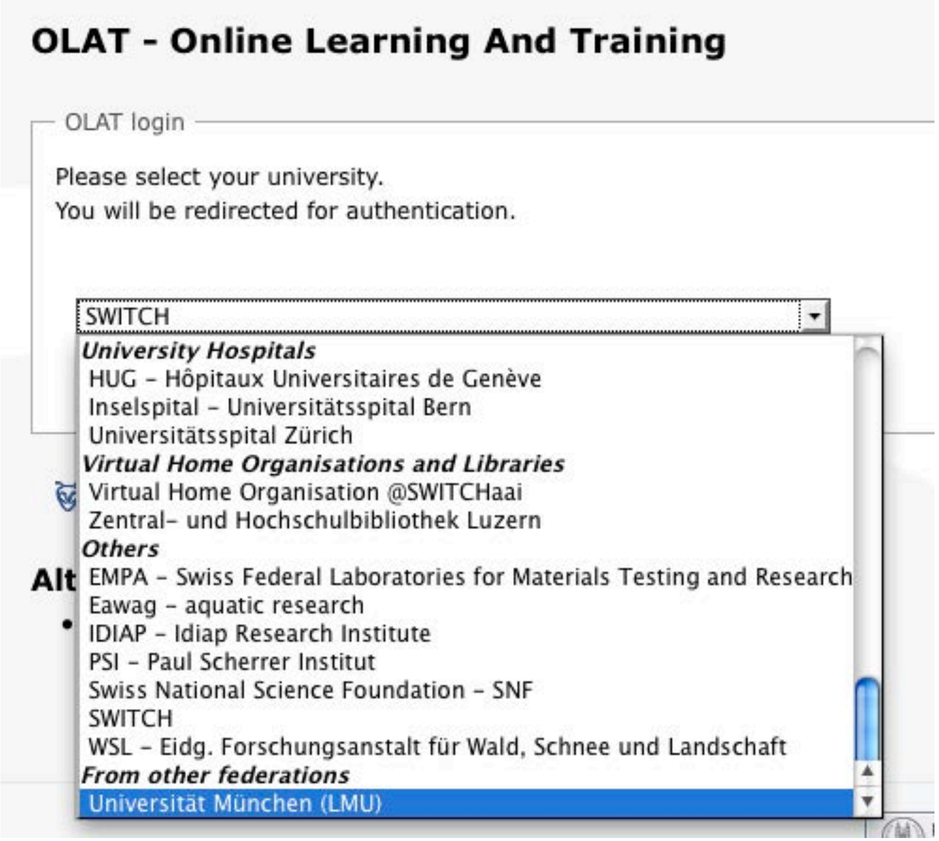
Locate me more accurately using HTML5 Geo-Location

Show providers in Switzerland show all countries

all countries
Czech
Denmark

DiscoJuice © UNINETT

Foodle with DiscoJuice



OLAT - Online Learning And Training

OLAT login

Please select your university.
You will be redirected for authentication.

SWITCH

University Hospitals
HUG – Hôpitaux Universitaires de Genève
Inselspital – Universitätsspital Bern
Universitätsspital Zürich
Virtual Home Organisations and Libraries
Virtual Home Organisation @SWITCHaai
Zentral- und Hochschulbibliothek Luzern
Others
EMPA – Swiss Federal Laboratories for Materials Testing and Research
Eawag – aquatic research
IDIAP – Idiap Research Institute
PSI – Paul Scherrer Institut
Swiss National Science Foundation – SNF
SWITCH
WSL – Eidg. Forschungsanstalt für Wald, Schnee und Landschaft
From other federations
Universität München (LMU)

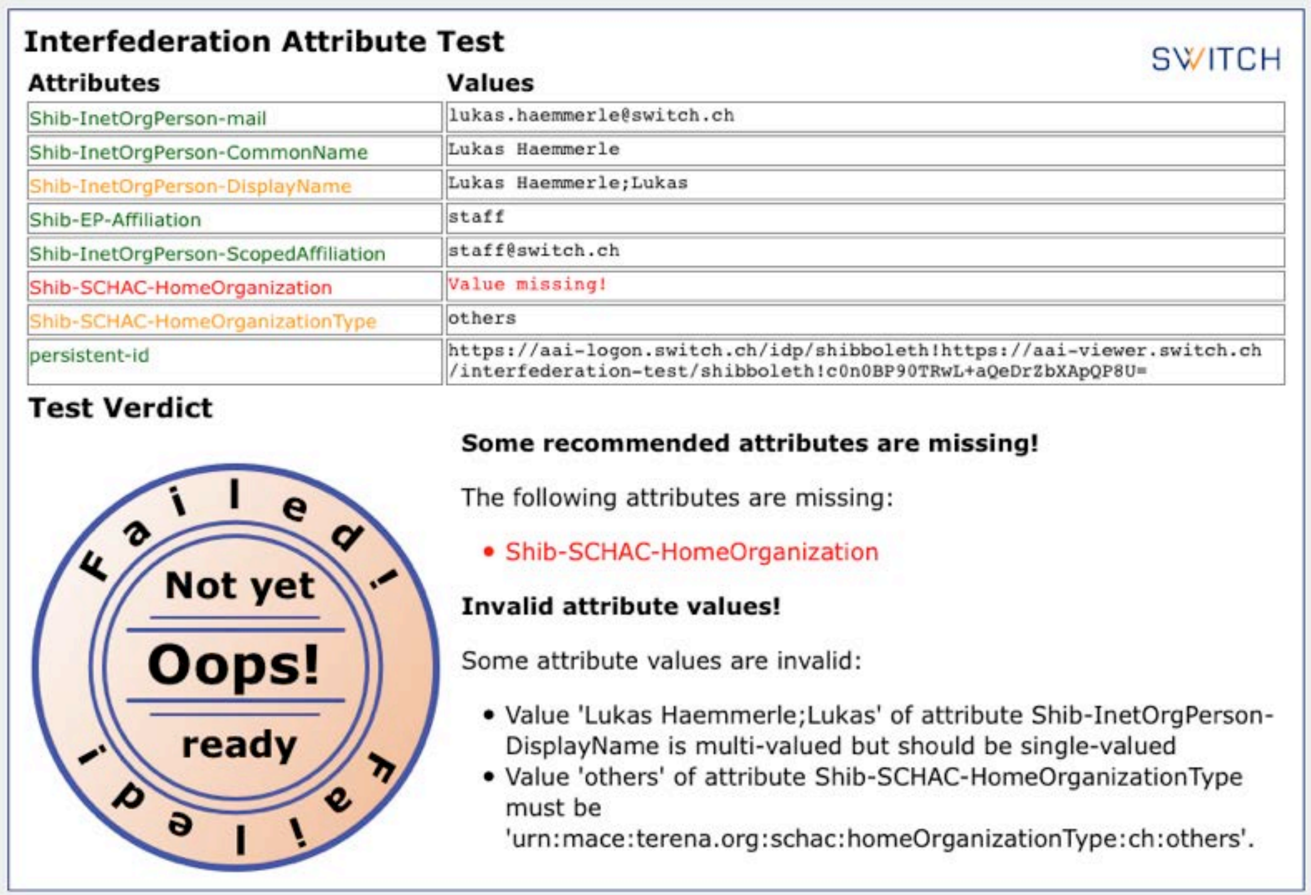
OLAT with Embedded WAYF

Deployment Guides

- Guides for Service Providers and Identity Providers
  - http://switch.ch/aai/docs/interfederation/idp-deployment.html
  - http://switch.ch/aai/docs/interfederation/sp-deployment.html
  - Step-by-step recipes may not be applicable for other federations

- Require a fully configured SWITCHaai SP and IdP
- IdPs should have uApprove installed

Failed Interfederation (Fitness) Test



Interfederation Attribute Test

Attributes	Values
Shib-InetOrgPerson-mail	lukas.haemmerle@switch.ch
Shib-InetOrgPerson-CommonName	Lukas Haemmerle
Shib-InetOrgPerson-DisplayName	Lukas Haemmerle;Lukas
Shib-EP-Affiliation	staff
Shib-InetOrgPerson-ScopedAffiliation	staff@switch.ch
Shib-SCHAC-HomeOrganization	Value missing!
Shib-SCHAC-HomeOrganizationType	others
persistent-id	https://aai-logon.switch.ch/idp/shibboleth!https://aai-viewer.switch.ch/interfederation-test/shibboleth!c0n0BP90TRwL+aQeDrZbXApQP8U=

Test Verdict

Some recommended attributes are missing!

The following attributes are missing:

- Shib-SCHAC-HomeOrganization

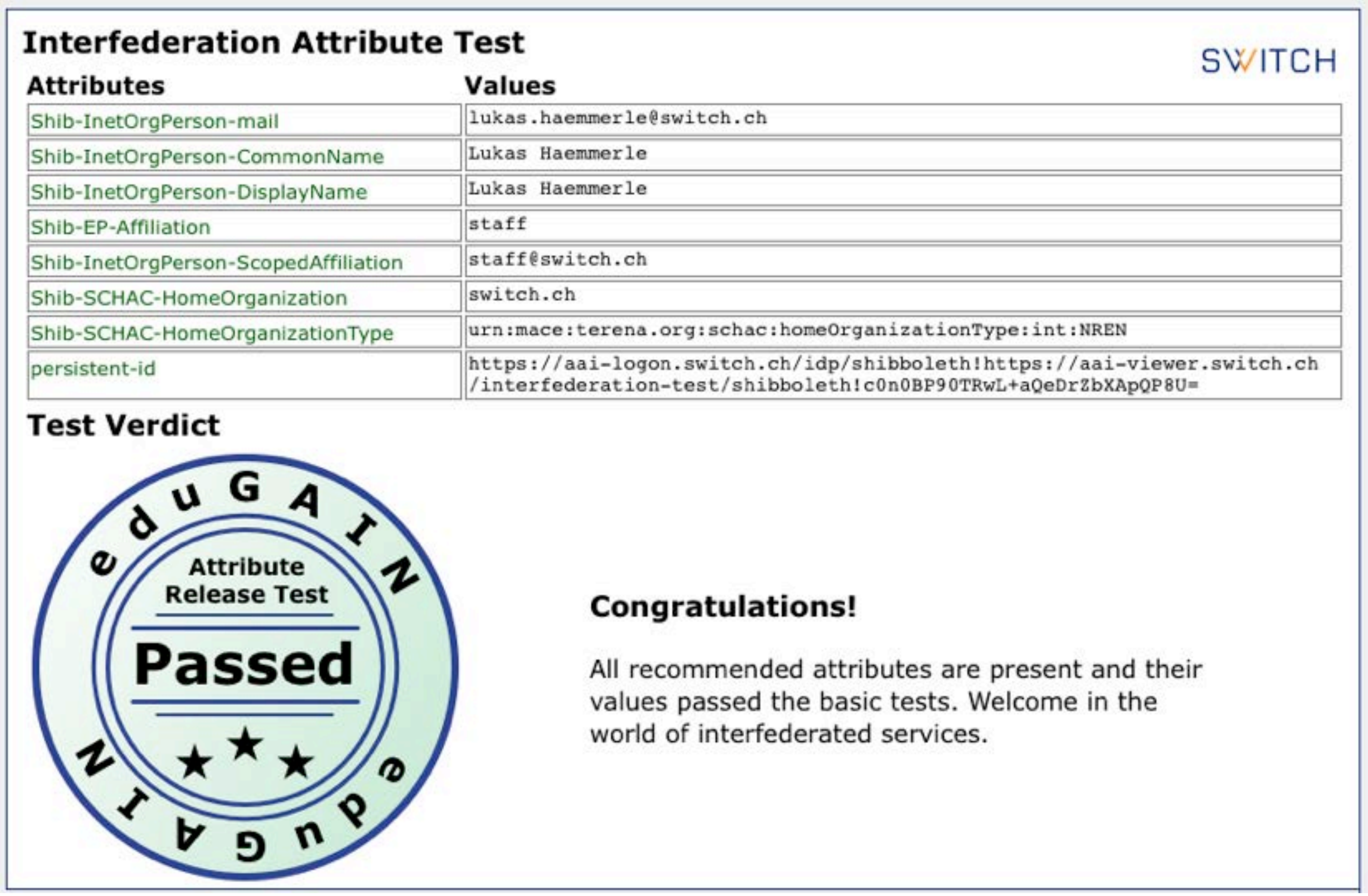
Invalid attribute values!

Some attribute values are invalid:

- Value 'Lukas Haemmerle;Lukas' of attribute Shib-InetOrgPerson-DisplayName is multi-valued but should be single-valued
- Value 'others' of attribute Shib-SCHAC-HomeOrganizationType must be 'urn:mace:terena.org:schac:homeOrganizationType:ch:others'.

- Missing attributes
- Attribute values not valid

Passed Interfederation (Fitness) Test



Interfederation Attribute Test

Attributes	Values
Shib-InetOrgPerson-mail	lukas.haemmerle@switch.ch
Shib-InetOrgPerson-CommonName	Lukas Haemmerle
Shib-InetOrgPerson-DisplayName	Lukas Haemmerle
Shib-EP-Affiliation	staff
Shib-InetOrgPerson-ScopedAffiliation	staff@switch.ch
Shib-SCHAC-HomeOrganization	switch.ch
Shib-SCHAC-HomeOrganizationType	urn:mace:terena.org:schac:homeOrganizationType:int:NREN
persistent-id	https://aai-logon.switch.ch/idp/shibboleth!https://aai-viewer.switch.ch /interfederation-test/shibboleth!c0n0BP90TRwL+aQeDrZbXApQP8U=

Test Verdict

Congratulations!

All recommended attributes are present and their values passed the basic tests. Welcome in the world of interfederated services.

- All recommended attributes available
- Correct attribute values

Demo

- How does this look like in the Resource Registry
- Interfederation fitness test
- Foodle as example Interfederation service