Resource Registry

How to manage Federation metadata and other descriptions



SWITCH

Thomas Bärecke aai@switch.ch

SWITCHaai Introduction Course Bern, 1. March 2013

The Initial <Problem>

× × · 8

</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 </mdu:Description>

<mdui:Keywords xml:lang="en">resources aai register authority administration</mdui:Keywords>

- </mdui:UIInfo>
- </Extensions>
- <KeyDescriptor>
- <ds:KeyInfo>
- <ds:X509Data>
 - <ds:X509Certificate>

MIIDHDCCAgSgAwIBAgIJAKyuqWEMkbhhMA0GCSqGSIb3DQEBBQUAMBsxGTAXBgNV BAMTEHJyLmFhaS5zd2l0Y2guY2gwHhcNMTExMjA1MDczM MTE3WjAbMRkwFwYDVQQDExByci5hYWkuc3dpdGNoLmNoMIIBIjANBgkqhkiG9w0B AQEFAAOCAQ8AMIIBCgKCAQEA0BdooNoOCQhs4eHgPuKMi2 jfGYXkIHUD4mkHFsWE4CqQVSfPcGbLLCj3Kb9O2a34F79mAJJL3VIOUgc3MB4k74 vqqVuql5zLgjzbMZgXeG2pKtBQCilEc0j/34EFFTTPXOG7MWEi8Nd5 vU47u3BzOzxLIhtMtZcfQonkmgFdms1boE7Ltf5hoaqu/PP5YAPD5fQgLp59FgGT Hj673DDhHlmkpp17Yd4vGhi/zuuWwayqqrQ7McUw2iJjIFqSXndZhSUbOIbL sbHy/bTrnltTQ1dHERhQnfl4PWOCw3oc4TVQv9TctksjTwIDAQABo2MwYTBABgNV HREEOTA3ghByci5hYWkuc3dpdGNoLmNohiNodHRwczovL3JyLmFha Y2gvc2hpYmJvbGV0aDAdBgNVHQ4EFgQUBXFXLfXgSki1u88YLdYREjH8f14wDQYJ KoZIhvcNAQEFBQADggEBAIpxIxPfUuRcUSJkK6xcWXcjSUF1mU j5gmloJIJB0d11eEMWjoHrheIAFRKnj0x6+HenrP7xWsV2mUAwTH9misPA6qZ0MZ AbW578ed1pZx04iqlsZhAfFC8uh+GgCCnmX15f8W5LoDN+RDKIZfpodSt yL1TAZfVVIH+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/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-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/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/aaitest/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



Home | Resources | Registration Requests | Home Organizations | Registry Administration

Thomas Baerecke (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

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

Federation Information

- Ederations: List of federations operated by the Resource Registry
- All Home Organizations: List of approved Home Organizations
- Eederation Partners: List of accepted Federation Partners for SWITCHaai
- Image: All available Resources: List of approved active and inactive Resource Descriptions
- Q 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?

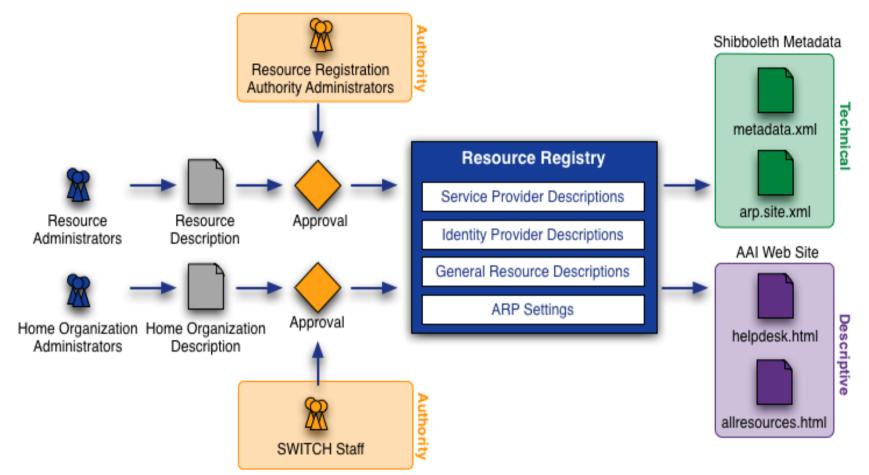
SWITCHaai Migration statistics





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 persons/helpdesk for your SP

Your most recently used Resource's helpdesk

Contact the helpdesk of the Resource you wanted to connect to, if you experience **problems after successful login**.

Forge: Project Hosting Platform Support Contact: <u>SWITCHaai Team</u>, +41 44 268 15 05

Find the Resource in the list of Resources grouped by Home Organization or in the long list of all public Resources.

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

AAI Wiki - Waaikiki No Helpdesk web page specified Show contact persons Show requested attributes Show intended audience [en] AAI Wiki - Waaikiki



Live Demonstration

AAI Resource Registry

S₩ITCH

Home | Resources | Registration Requests | Home Organizations | Registry Administration Th

Thomas Baerecke (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

- JAR Resource Registry Guide explaining the basic principles and mechanisms of the Resource Registry
- 📓 <u>Resource Registry Screencast</u> for first time users on how to register a resource

Federation Information

- Ederations: List of federations operated by the Resource Registry
- All Home Organizations: List of approved Home Organizations
- Ederation Partners: List of accepted Federation Partners for SWITCHaai
- <u>All available Resources</u>: List of approved active and inactive Resource Descriptions
- Q 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
- <u>Attribute definitions</u>: 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



