

Resource Registry: New formula

Now with 50% more user-friendly ingredients and less than 0.5% bugs



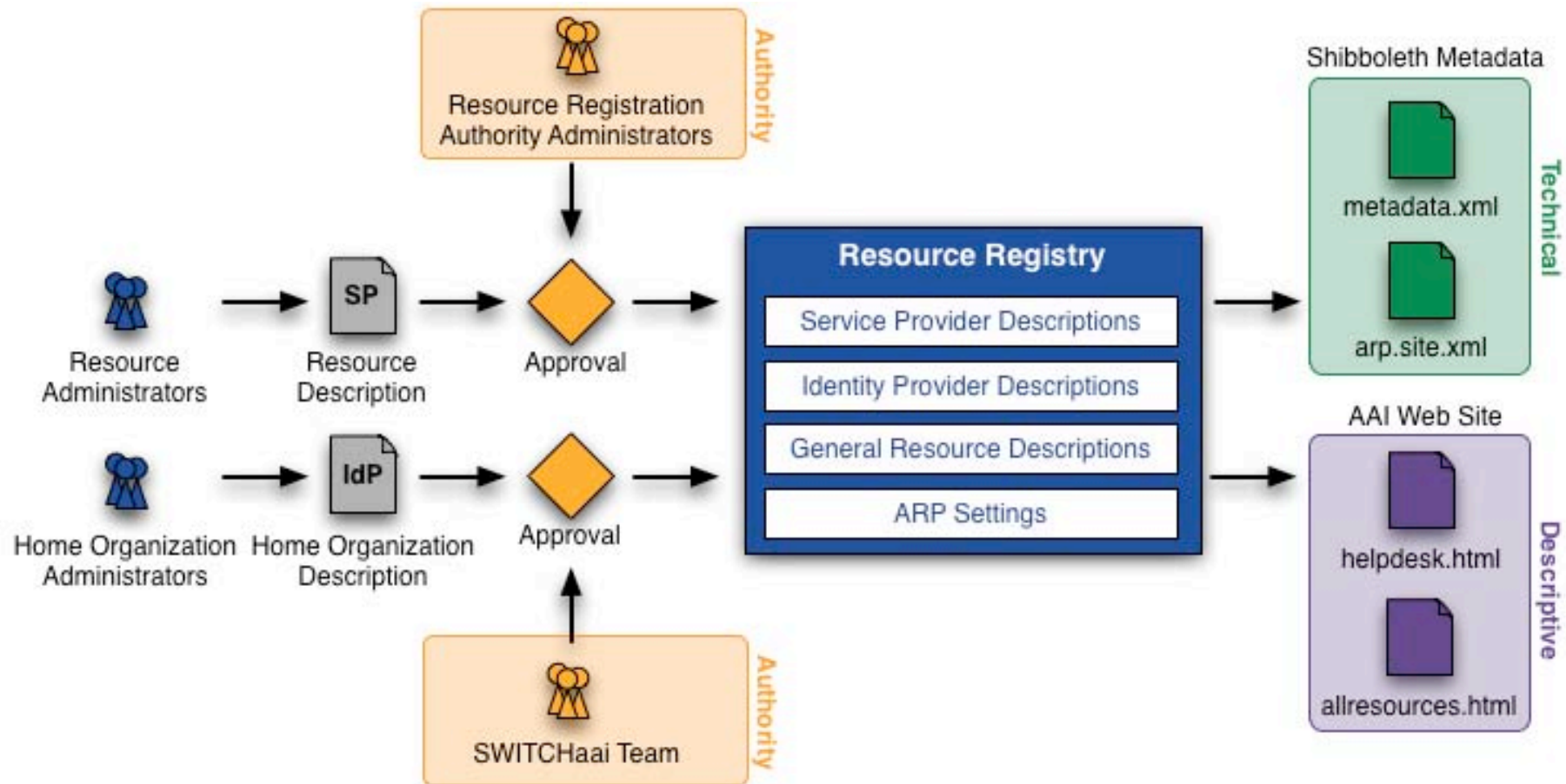
SWITCH

Serving Swiss Universities

Lukas Hämmerle

lukas.haemmerle@switch.ch

The basic purpose and principles



Main tool to manage the SWITCHaai Federation

What's new?

- New look & feel



The screenshot shows the SWITCH AAI Resource Registry website. At the top, the SWITCH logo is in blue and orange, followed by the text "AAI Resource Registry" in orange. Below this is a navigation bar with links for "Network", "NetServices", "Security", "Internet Domains", and "About". The main heading is "AAI Resource Registry Login". Underneath, there is a "Login" section. A paragraph states: "SWITCH currently operates two federations in two different infrastructures:". Below this are two login options, each in a box. The first box contains the SWITCH logo, a right-pointing chevron, the text "aai", and a "Login" button. To the right of this box is the text "SWITCHaai Federation: The production infrastructure". The second box contains the AAI logo, a right-pointing chevron, the text "test", and a "Login" button. To the right of this box is the text "AAI Test Federation: Open for any organization for testing and development purposes only." At the bottom of the login section, there is a note: "Click on the login link, depending in which of the above federations your Home O".

What's new?

- New look & feel
 - Tabbed navigation



The screenshot displays a web application interface with a 'Main Menu' section. It features four tabs: 'RRA Administration', 'Home Organization Administration', 'Resource Administration', and 'General Information'. The 'Resource Administration' tab is highlighted with a red oval. Below the tabs, the 'Resource Admin Options' section is visible, containing a list of resource descriptions with associated actions like 'View', 'Edit', 'Download configuration', 'Delete', and 'Administrators'.

Main Menu

RRA Administration | Home Organization Administration | **Resource Administration** | General Information

Resource Admin Options

- Add a Resource Description
- Approved Resource Descriptions:
 - **"SWITCH, VHOtools"** (SWITCHaai)
 View | Edit | Download configuration | Delete | Administrators
 - **"SWITCH AAI Wiki: waaikiki"** (SWITCHaai)
 View | Edit | Download configuration | Delete | Administrators
 - **"SWITCH Tools"** (SWITCHaai)
 View | Edit | Download configuration | Delete | Administrators
 - **"SIP User Management (devel)"** (SWITCHaai)
 View | Edit | Download configuration | Delete | Administrators

What's new?


- New look & feel
 - Consistent look for descriptions
 - Light blue for Home Organizations - Light orange for Resources


The screenshot shows the 'Home Organization Menu' interface. At the top, there are navigation tabs: 'RRA Administration', 'Home Organization Administration', 'Resource Administration', and 'General Information'. Below the tabs, the breadcrumb path is 'Home Organization Description menu of "SWITCH - Serving Swiss Universities" - Home Organization Menu'. The main heading is 'Edit the Home Organization Description'. A note states: 'Change the following descriptions to modify your Home Organization Description. But please keep in mind that any change you make here will become active immediately as soon as the metadata is published every hour.' Below this, there is a list of eight items, each with a pencil icon and a label: 1. General Information, 2. Technical Information, 3. Used certificates, 4. List of contacts, 5. Supported Attributes, 6. General Attribute Release Policy Rules, 7. Specific Attribute Release Policy Rules, and 8. Setup & Environment Information. At the bottom, there is a button labeled 'View Home Organization Description' with a document icon.

The screenshot shows the 'Resource Menu' interface. At the top, there are navigation tabs: 'RRA Administration', 'Home Organization Administration', 'Resource Administration', and 'General Information'. Below the tabs, the breadcrumb path is 'Resource Description menu of "SWITCH, VHOTOOLS" - Resource Menu'. The main heading is 'Resource Menu'. A note states: 'Complete the Basic Resource Description in order to edit further details for the resource. If you modify an already approved resource you will have to change at least one description to submit it again for approval.' Another note states: 'In case you want to register an already fully configured Shibboleth Service Provider 2.x, you can use the following wizard to complete some sections using the self-generated metadata of the Service Provider:'. Below this, there is a button labeled 'Run Shibboleth 2.0 wizard' with a wizard icon. The main content area contains a list of eight items, each with a pencil icon and a label: 1. Basic Resource Information (Unchanged), 2. Multiple Language Descriptions (Unchanged), 3. List of Contacts (Unchanged), 4. Keywords (Unchanged), 5. Service Locations (Unchanged), 6. Used Certificates (Unchanged), 7. Required Attributes (Unchanged), and 8. Intended Audience (Unchanged). Below this list, there are three buttons: 'Discard temporary resource description', 'View complete temporary resource description', and 'Download custom configuration files'. At the bottom, there is a status bar that says 'You have not made any changes yet to this resource description'.

What's new?

- New look & feel
 - Multiple assistants and wizards improve ease-of-use

 Run Shibboleth 2.0 wizard

 Clear all fields...

 Run Shibboleth 2.x assistant...

 Run Shibboleth 1.x assistant...

 Run assistant to get certificate used by web server...

What's new?

- Shibboleth 2/SAML 2 support
E.g SAML 2 endpoints and specific Shibboleth 2 attribute filter

For **Shibboleth Identity Providers 2.x only**, define custom rules for certain further attributes, won't be released.

You may also remove a Resource completely. That is useful if you want to create filters.

In order to use your own rules, you create a separate `custom-attribute-filter`. Either choose to remove the Resource or select the attributes that you want to rule and set the value to '-' the general ARP rule applies.

Existing Specific ARP Rules

Resources

1. SWITCH, eConf Admin Portal, <https://econfadmin.switch.ch/shibboleth>

Specific ARP Rule

SingleSignOnService

SAML1 AuthnRequest binding <https://aai-logon.sw>

SAML2 HTTP-POST binding <https://aai-logon.sw>

SAML2 HTTP-POST-SimpleSign binding <https://aai-logon.sw>

SAML2 HTTP-Redirect binding <https://aai-logon.sw>

AttributeService

SAML1 SOAP binding <https://aai-logon.sw>

SAML2 SOAP binding <https://aai-logon.sw>

ArtifactResolutionService

SAML1 SOAP binding <https://aai-logon.sw>

SAML2 SOAP binding <https://aai-logon.sw>

What's new?

- Embedded certificate support

B. Embedded certificates


PEM formatted X.509 certificate

```
-----BEGIN CERTIFICATE-----
MIIE4zCCA8ugAwIBAgILAQAAAAABGZ/kGG0wDQYJKoZIhvcNAQEFBQAwXzELMAkG
A1UEBhMCQkUxEzARBgNVBAoTCkN5YmVydHJlc3QxZmFzAVBgNVBAsTDkVkdWNhdGlv
bmFsIENBMSIwIAYDVQDEx1DeWJlcnRydXN0IEVkdWNhdGlvbmFsIENBMB4XDTA4
MDQzMDElMTIwNVowXDTEwMDQzMDElMTIwNVowaTELMakGAlUEBhMCQ0gxQDA+BgNV
BAoTN1N3aXRjaCAatIFRlbGVpbmZvcmlhdGlrZGllbnN0ZSBmdWVyIEExlaHJlIHVu
ZCBGb3JzY2h1bmcxGDAWBgNVBAMTD3Rvb2xzLnN3aXRjaC5jaDCCASIwDQYJKoZI
```

Second PEM formatted X.509 certificate

Use the second certificate for certificate roll over if you want to replace the first certificate. If you use a s... sure it is configured in your Service Provider, otherwise encrypted attributes cannot be decrypted in cert...




Click in a textarea containing a certificate in order to see some additional details about it.

Subject: / C=CH / O=Switch - Teleinformatikdienste fuer Lehre und Forschung / CN=tools.switch.ch
Type: Issued
Issuer:  /C=BE/O=Cybertrust/OU=Educational CA/CN=Cybertrust Educational CA
Expiration date: Apr 30 15:12:05 2010 GMT
Fingerprint: 70:84:18:11:3F:DA:D8:27:97:BD:17:54:26:93:51:E9:3F:0A:96:96

What's new?

- Four-eyes approval support

Home Organization information for 'SWITCH - Serving Swiss Universities' (SWITCHaai)

Last Updated	
 Patrik Schnellmann	on 24. 4. 2008 22:02
 Edit this Home Organization description	
Basic Information	
Home Organization Name	switch.ch  Secure approval supported Resource descriptions for this Home Organization are approved by a different account than the one that created them. This Four-Eyes approval procedure increases security and decreases configuration errors.
Home Organization Type	Others
Federation	SWITCHaai Federation
Main language	English
Descriptive Name	SWITCH - Serving Swiss Universities
Description	SWITCH coordinates and operates the Shibboleth federation called "SWITCHaai". It supports the universities and other participants of the federation in adapting and using the services provided by the AAI.
Technical Information	
Provider ID	urn:mace:switch.ch:SWITCHaai:switch.ch

- Which Home Organizations are interested in this?

What's new?

- Fingerprint Approval
 - Only active in AAI Test for now
 - Has to be first accepted by the AAI Advisory Committee before general usage in SWITCHaai

Resources waiting for approval

Ubuntu Testmachine Halm Reusser (AAI Test)
view differences | edit

1. Requesting Resource Administrator:
Halm Reusser (switch.ch)
Phone number: **+41442681571**
2. Service Location URLs:
 - o <https://ubuntuhr.switch.ch/Shibboleth.sso/NIM/Artifact>
 - o <https://ubuntuhr.switch.ch/Shibboleth.sso/NIM/POST>
 - o <https://ubuntuhr.switch.ch/Shibboleth.sso/NIM/Redirect>
 - o <https://ubuntuhr.switch.ch/Shibboleth.sso/NIM/SOAP>
 - o <https://ubuntuhr.switch.ch/Shibboleth.sso/SAML/Artifact>
 - o <https://ubuntuhr.switch.ch/Shibboleth.sso/SAML/POST>
 - o <https://ubuntuhr.switch.ch/Shibboleth.sso/SAML2/Artifact>
 - o <https://ubuntuhr.switch.ch/Shibboleth.sso/SAML2/ECP>
 - o <https://ubuntuhr.switch.ch/Shibboleth.sso/SAML2/POST>
 - o <https://ubuntuhr.switch.ch/Shibboleth.sso/SAML2/POST-SimpleSign>
 - o <https://ubuntuhr.switch.ch/Shibboleth.sso/SLO/Artifact>
 - o <https://ubuntuhr.switch.ch/Shibboleth.sso/SLO/POST>
 - o <https://ubuntuhr.switch.ch/Shibboleth.sso/SLO/Redirect>
 - o <https://ubuntuhr.switch.ch/Shibboleth.sso/SLO/SOAP>
3. Certificate subject **common name: ubuntuhr.switch.ch**
4. Embedded certificates:
 - a. **Subject:** / C=CH / O=Switch - Teleinformatikdienste fuer Lehre und Forschung / CN=ubuntuhr.switch.ch
⚠ This is not a SWITCHaai-accepted certificate that requires the "four-eye principle" approval procedure!
Issuer: / C=CH / L=Zurich / O=SWITCH AAI / OU=AAI / CN=AAI Test CA / emailAddress=aai@switch.ch
Expiration date: May 21 14:34:09 2009 GMT
Fingerprint (SHA1):
Not shown before Resource Description is approved

SHA1 Fingerprint for embedded certificate a.

Please contact the requesting Resource Administrator (see 1. for contact details) and ask for the **first 8 alphanumeric characters of the SHA1 fingerprint (not including : or whitespace)** of this certificate.

An example command that shows how to get the fingerprint is:
`openssl x509 -fingerprint -sha1 -in /path/to/the/certificate.pem`

Windows users have **openssl** bundled in the `shibboleth-sp/bin` directory.

- Add the first 8 alphanumeric characters of the SHA1 fingerprint. The following case-insensitive forms are accepted `84:DD:29:D5` or `84dd29d5`

What's new?

- Additional information pages with lists and matrixes

User	HomeOrg administrator	RRR administrator	http://call-deb5.switch.ch/	https://aai-rr.switch.ch/sh	https://aai-viewer.switch.ch	https://aai-wiki.switch.ch/	https://atbash.chuv.ch/shib	https://basic.switch.ch/shi	https://bb.switch.ch/shibbo	https://devey.switch.ch/shi	https://econfin.switch.ch	https://faunus.switch.ch/sh	https://flow.net.switch.ch/	https://hera.switch.ch/shib
switch.ch														
? ?														
Altstätter Markus														
Baumann Kurt														
Beeli Nadja														
Bertolo Daniel														
Brand Kaspar														
Flury Placi												x		
Fritschi Daniel														
Furter Renato														
Gall Alexander													x	
Gartmann Rolf							x							
Guajana Ivan											x			
Hämmerle Lukas	x	x	x	x						x				

Home Organization	Resource	Federation Partner	swissEduPersonHomeOrganization	eduPersonAffiliation	swissEduPersonHomeOrganizationType	surName	givenName	mail
bfh.ch	BFH Moodle		R					
bfh.ch	Test SP		R	R	R	R	R	F
bfh.ch	vmremus Moodle-Testinstallation		R			R	R	
epfl.ch	Bibliothèque scientifique commune UNIL-EPFL		R			R	R	
epfl.ch	Tequila		R			R	R	F
ethz.ch	AAIproxy ETHZ		R		R			F
ethz.ch	e-collection		R	R	R	R	R	F
ethz.ch	e-collection III Test		R	R	R	R	R	F
ethz.ch	eAdressen Local		R	R	R	R	R	F
ethz.ch	EBSCO Information Services	x						
ethz.ch	ELMS Login		R	R		R	R	F
ethz.ch	Entwicklungs-System tim-5		R	R		R	R	F
ethz.ch	ESN Zürich		R	R	R	R	R	F
ethz.ch	ETH Alumni Student Login	x	R	R		R	R	F
ethz.ch	ETH, ID, TIM Test Machine		R			R	R	F

Live Demonstration

The screenshot shows a web browser window titled "AAI Resource Registry - Main Menu" with the URL https://aai-rr.switch.ch/menu.php#activate_general. The browser's address bar and tabs are visible. The page content includes a navigation menu with "Network", "NetServices", "Security", "Internet Domains", and "About Us". A red banner indicates "DEVELOPMENT MODE ACTIVATED". The "Main Menu" section has tabs for "DB Administration", "RRA Administration", "Home Organization Administration", "Resource Administration", and "General Information". A warning message states: "Although you have DB administration privileges, you don't meet the required assurance level. Therefore, certain DB administrator actions cannot be performed." The "General Information" section contains a list of links and descriptions, including "Resource Registry Guide", "Federations operated by the Resource Registry", "Approved Home Organizations", "Federation Partners", "Approved Resource Descriptions", "Search for resources", "Metadata refresh times of Service Providers and Identity Providers", "All Resource Registry users from switch.ch", "Attribute definitions", "Home Organization attribute release matrix", and "Resource attribute requirement matrix". The "Metadata Files" section explains that files are directly generated by the Resource Registry and provides a list of files for Shibboleth 1.3 and 1.2, including metadata and sites files. The footer shows "Logged in as: Lukas Hämmerle (switch.ch)", "© 2008 SWITCH | Contact | 22. 05. 2008", and the URL "aai-rr.switch.ch".