AAI Resource Registry Guide

Version: 8/14/24 Authors: LH, TL

AAI web page: https://help.switch.ch/aai/ Contact: eduid@switch.ch

This guide is aimed at users of the Switch Resource Registry and is intended to serve as a complimentary source of information to explanations and examples that are already integrated into the Resource Registry. It explains the most important aspects and processes to create, maintain and administrate Home Organization and Resource Descriptions.

Note: The screenshots in this guide may not reflect the actual interface because the Resource Registry is constantly extended and developed further.

Table of Contents

1. Description of the Resource Registry

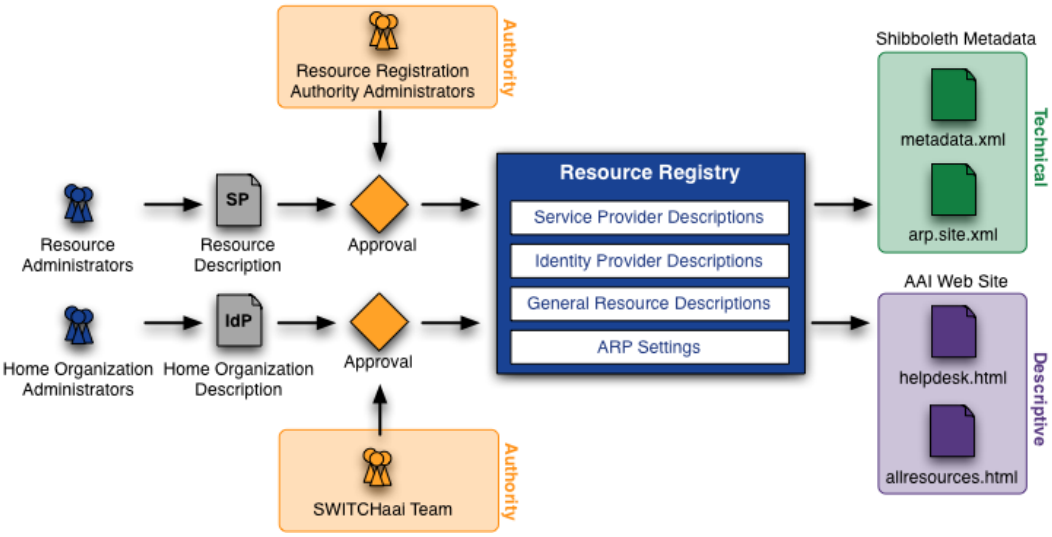

Figure 1: Resource Registry overview

The Resource Registry is a web-based tool developed by Switch to manage information about Resources and Home Organizations participating in the SWITCHaai and AAI Test federations, which are operated by Switch. Since 2011 the Resource Registry is also capable of handling interfederated Resources and Home Organisations via eduGAIN. A Resource is the description of a SAML or an OpenID Connect service.

The intended users of the Resource Registry are users registering SAML and OpenID Connect services

The Resource Registry's main purpose and features are (see Figure 1):

- **Attribute/claim requirements declaration**
  Resource administrators specify the required attributes/claims to provide for accessing the service. In addition, desired attributes can be listed too. Desired attributes/claims should provide additional benefit to justify their use. The data protection principle counts: Process only data which is really necessary!
- **Intended audience declaration**
  Resource administrators can also specify from which Home Organizations it will accept users. For example, a Resource is only of interest to medical students. Then, there is no point in adding that Resource to the metadata of the universities not offering medical studies at all. However, it is still the duty of the Resource to configure its authorization rules properly!
- **Federation Members can control resources within their organization domain**
  Each Resource needs to get approved before its entry gets activated in the Resource Registry. Each Federation Member approves Resources from its own domain and from the Federation Partners it sponsors. It delegates this control to one or more people who act as Resource Registration Authority administrators for the Federation Member. They are notified by e-Mail, whenever approval is required for changes made to Resource Description in the Resource Registry.
- **Supported attributes declaration**
  Not all of the attributes specified for SWITCHaai are mandatory to implement. The Identity Providers can document within their Resource Registry entry which ones are

implemented and potentially available to Resources.

- **Generate federation metadata**
  Based on the information collected, the crucial federation metadata files for the Identity Providers as well as Service Providers can be generated. Each Identity Provider needs to know all potential Service Providers with whom it should communicate and vice versa.
- **Generate attribute release policy/filters**
  Each SAML Identity Provider has to maintain the Attribute Release Policy (ARP) configuration. The Resource Registry provides them tailored templates for the ARP and in some cases notifies the Identity Provider administrators in case of changes.
- **Generate configuration files**
  The Resource Registry can generate some configuration files for Service Providers and Identity Providers using information contained in its database.
- **Generate federation information and help pages**
  Because the Resource Registry is also used to manage the attributes, attribute usage and requirement as well as contact information for all Resources and Home Organizations, it also can be used to generate various statistics and lists about to the federation.

2. Login

The Resource Registry is accessible via https://rr.aai.switch.ch/ and requires an account in the SWITCHaai federation. Users without an account of a university, can create an account on the “Switch edu-ID” Identity Provider.
The Resource Registry home page contains a short description of the service.

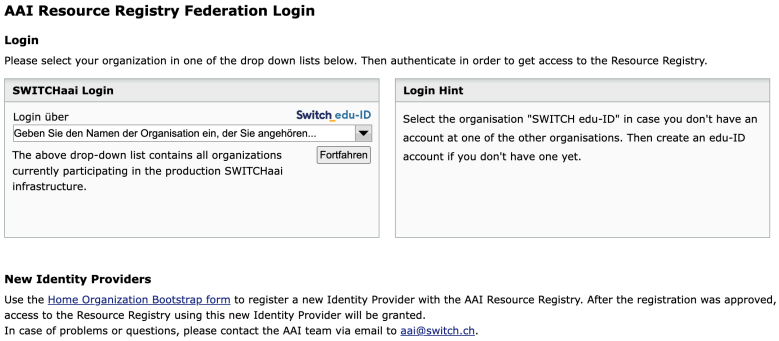

Figure 2: Login buttons

After authentication at a Home Organization one is redirected back to the Resource Registry. Provided the Resource Registry receives all the required attributes from the Home Organization, login is successful. The Resource Registry needs the following attributes:

- Given Name (required)
- Surname (required)
- E-Mail Address (required)
- Unique ID (swissEduPersonUniqueID or eduPersonPrincipalName) (required)
- Targeted ID (optional)
- Business telephone number (optional)
- Mobile number (optional)
- Home Organzation Name (required)
- Home Organization Type (optional)

When a user logs in the first time, a data storage consent screen (see Figure 3) has to be accepted first. In order to send notification e-Mails at least given name, surname and e-Mail address have to be stored in the Resource Registry database. The phone number is used in cases where an administrator needs to ask or confirm some data (e.g. fingerprint of a self-signed certificate) over the phone.

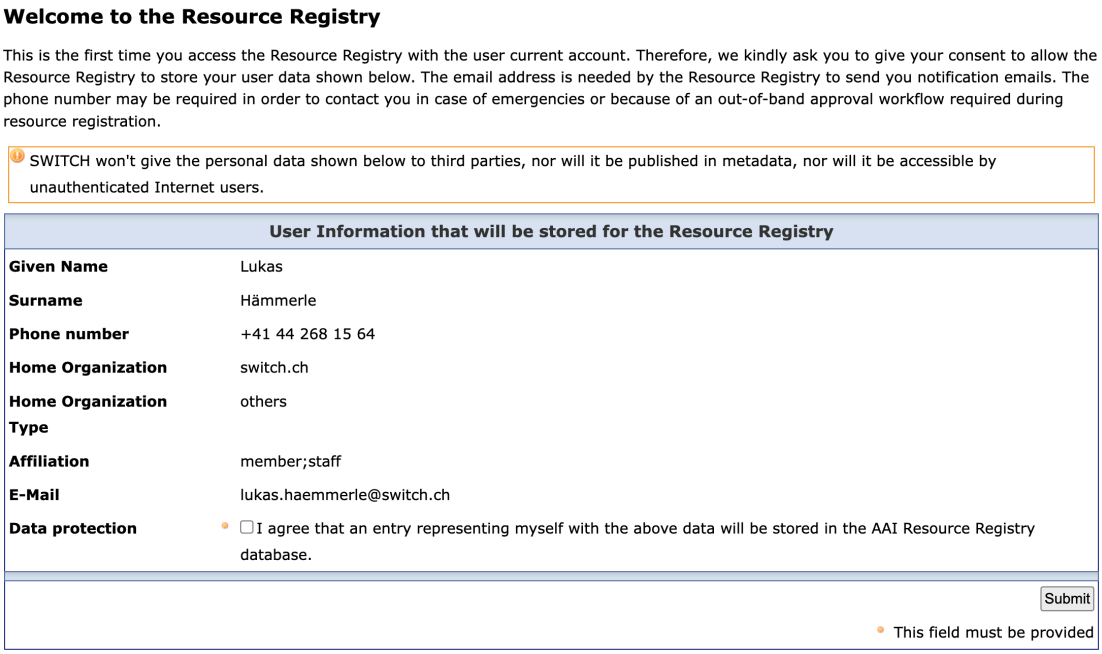

Figure 3: Resource Registry data storage consent

Note: In case you just have set up a Home Organization but it is not yet registered in the Resource Registry, read the section 'Home Organization Administrator' on how to register a Home Organization for the first time.

3. Administration Interface

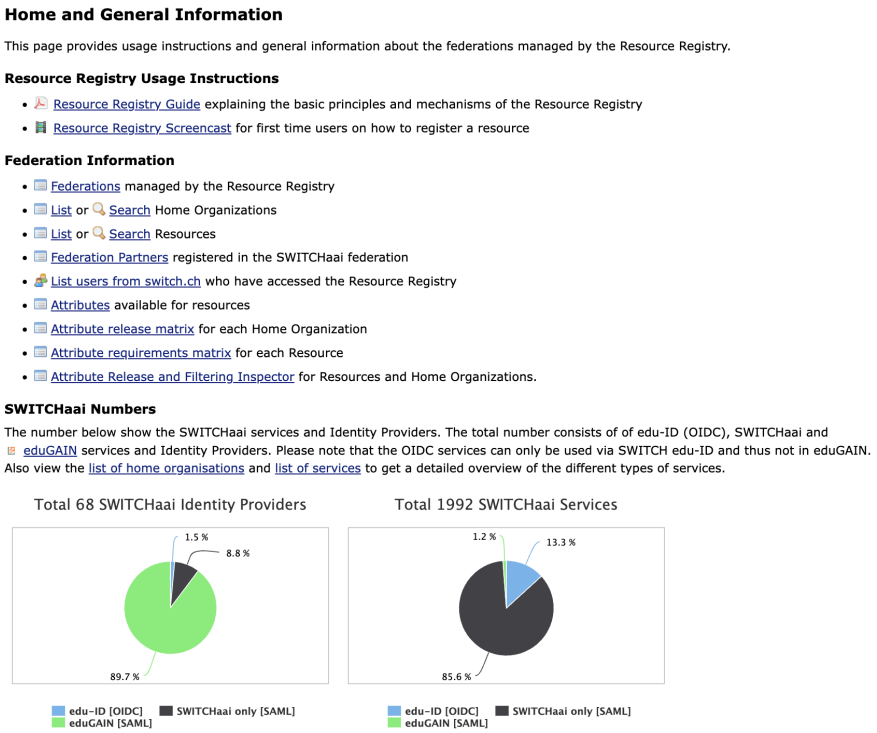

Figure 4: Main Menu

After successful authentication, one is in the main menu of the Resource Registry. Depending on the privileges and roles (see Chapter 4), there are between two and five different links in the navigation bar. They reflect the administration and access rights a user has.

Figure 4 shows the 'General Information' section that provides various lists, search forms as well as matrixes that describe the federations managed by the Resource Registry. All users of the Resource Registry have access to this section.

Figure 5 shows the 'Resource Administration' options. If a user has no administration privileges for any Resource Descriptions he can only add new Resource Descriptions. Otherwise, a user sees links to manage all approved Resource Descriptions.

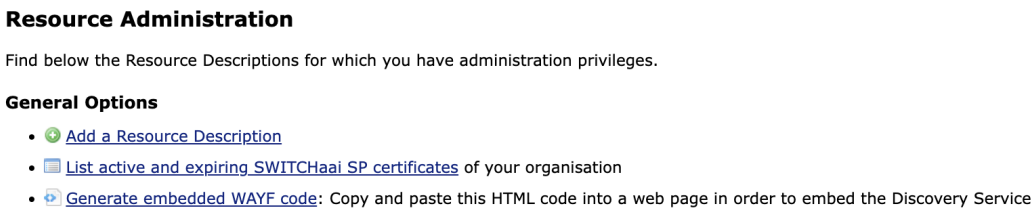

Figure 5: Resource administration options

When registering a resource and after it was approved by a Resource Registration Authority (RRA) administrator (see Chapter 4), the Resource Administration section looks like in Figure 6.

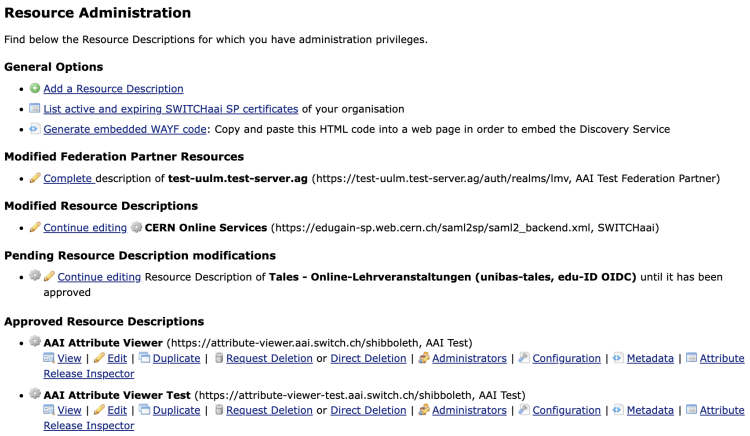

Figure 6: View with multiple approved Resource Descriptions

For Home Organization administrators, the corresponding administration options look like in Figure 7.

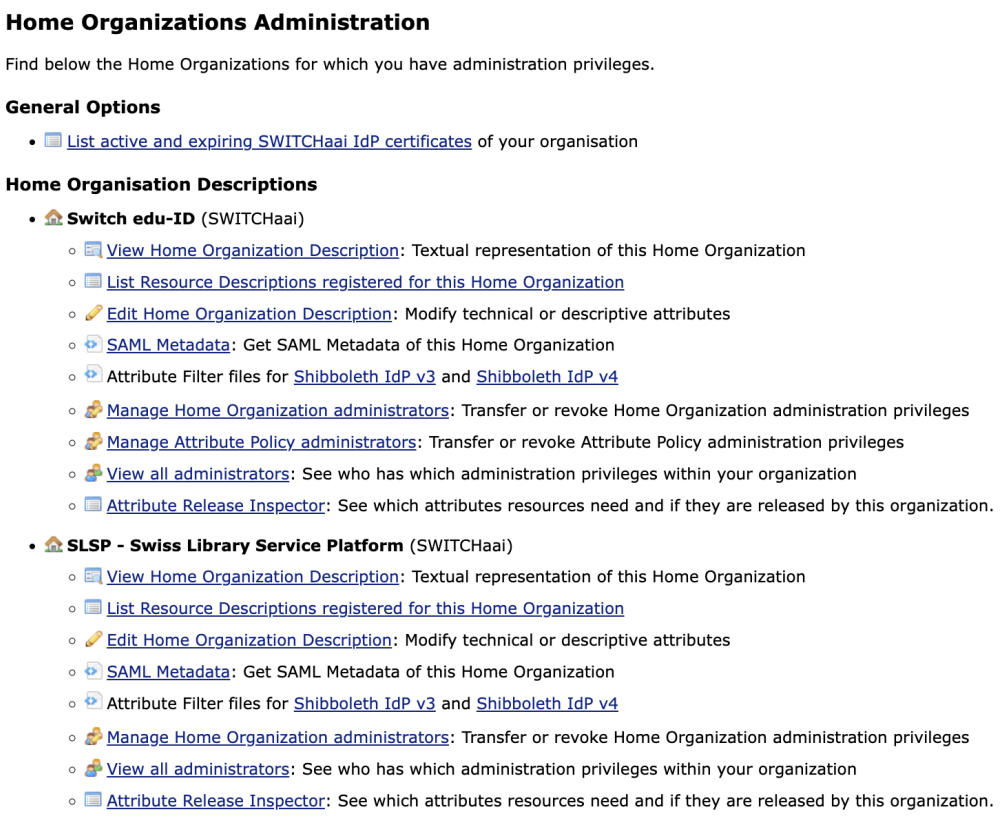

Figure 7: Home Organization administration options

The options for a Resource Registration Authority administrator look like in Figure 8.

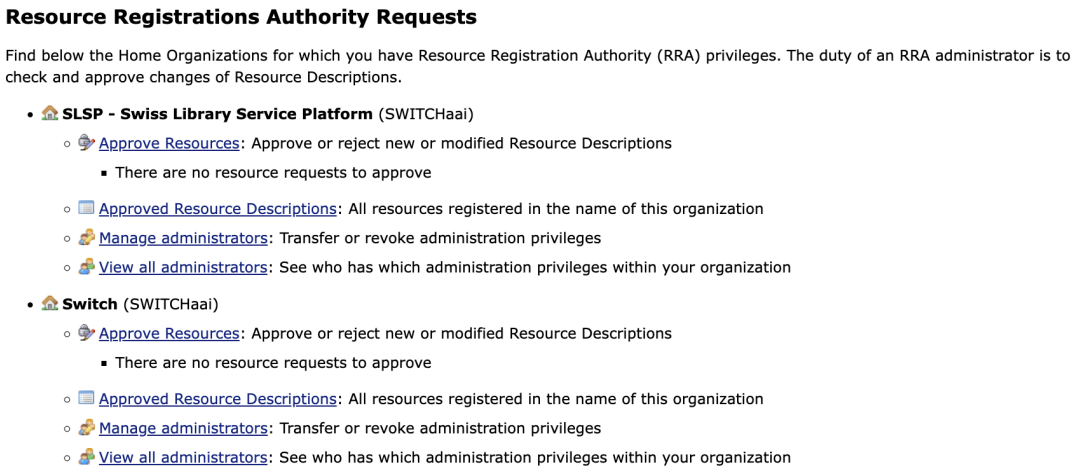

Figure 8: Resource Registration Authority administration options

Note: One may not see all of the above administration options because certain privileges are required to see them.

4. Roles

Every user in the Resource Registry can have one or more roles with additional administration privileges. These are:

- Resource administrator (of a Resource)
  Registers and manages one or more Resource Descriptions. See Chapter 4.1.
- Attribute Release Policy administrator (of a Home Organisation)
  Optional role that can be assigned to users that have the limited right to set the default and specific attribute release policies of a SAML Home Organisation. See Chapter 4.2.
- Home Organization administrator (of a Home Organisation)
  At least one person per Home Organization. Manages Home Organization Description and attribute release settings. See Chapter 4.2.
- Resource Registration Authority administrator (of a Home Organisation)
  At least one person per Home Organization. Approves or rejects new or modified Resource Descriptions. See Chapter 4.3.
- Resource Registry Operator (for everyting)
  Can view, edit and delete any entry. May require two-factor authentication. This role is reserved for operators of the Resource Registry.

A user logging in for the first time has none of the above roles assigned unless this person was invited by another administrator with an invitation link for a particular role. All administrator roles can be transferred to any other user. E.g. the administrator of Home Organization X could make any other user an administrator of X. Vice versa any Home Organization administrator can revoke rights for users of the same the Home Organization he has the rights for.

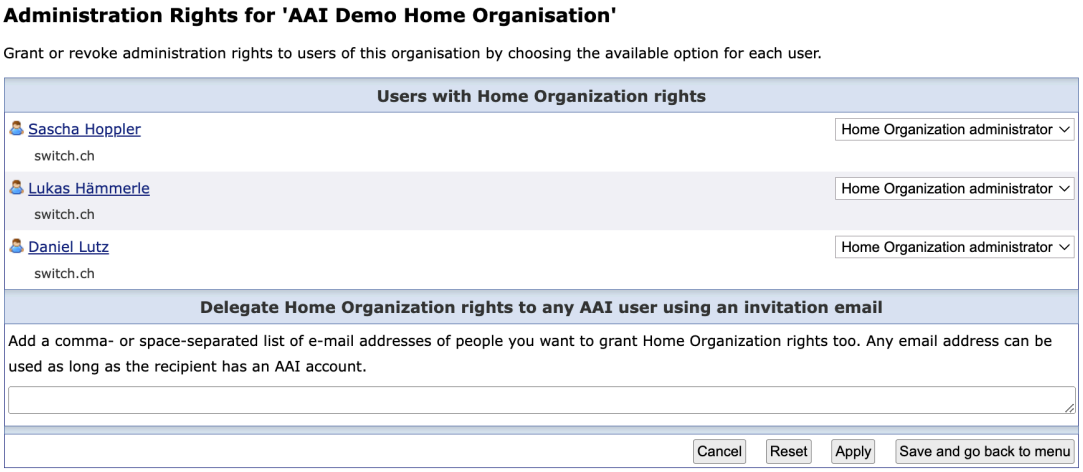

Figure 9: Manage administration rights

Figure 9 illustrates how to grant or revoke Resource Registration Authority rights to or from other users. Users can be invited by manually entering their e-Mail addresses in the text area at the bottom of the page. The invited users receive an e-Mail containing an invitation link that will grant them the administration rights that were bound to this invitation.

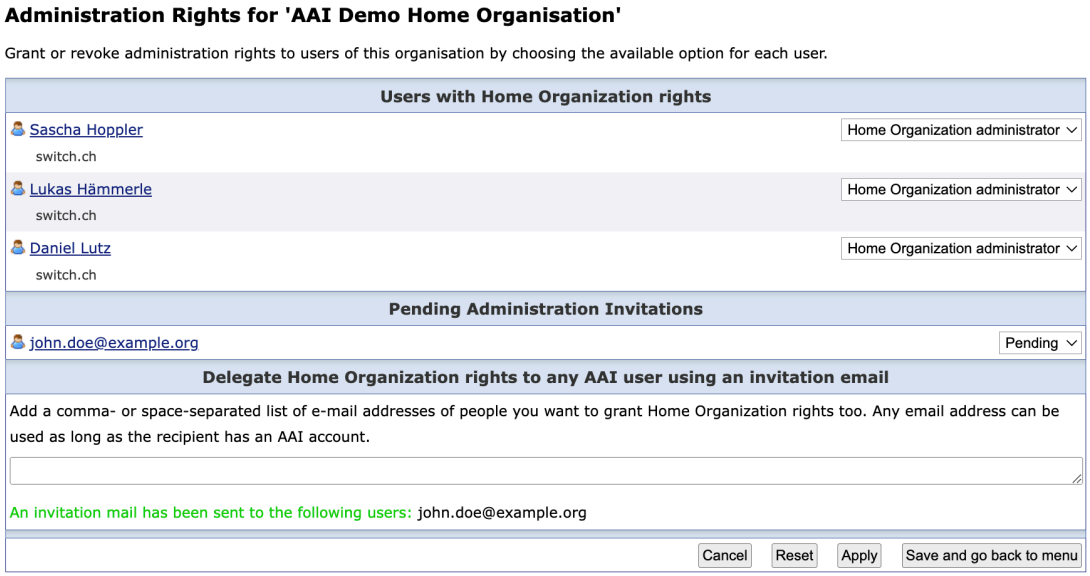

Figure 10: Invitation pending

Figure 10 shows a pending invitation. Invitations can also be revoked.

In the following chapters the above-mentioned administrator roles are illustrated in greater detail.

4.1. Resource Administrator

Unless you were invited as a Resource administrator, you find the Resource administrator options empty as shown in Figure 5. So, the only option will be to add a Resource Description. Clicking the link 'Add a Resource Description' one sees a page like in Figure 11.

One then has to choose first if a Resource Descriptions for a SAML or OpenID Connect service should be created. The registration for both is very similar as similar data has to be provided.

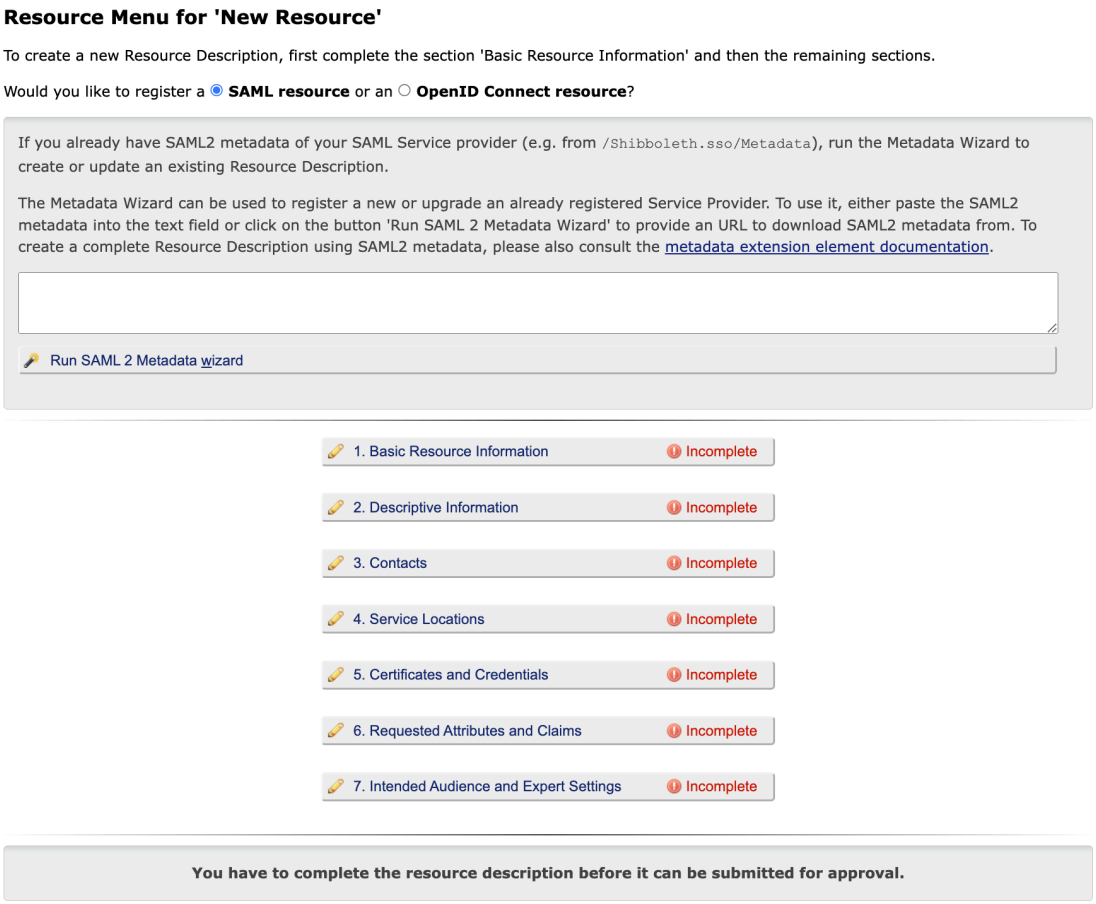

Figure 11: SAML Resource Description sections

Figure 11 shows all sections of a SAML Resource Description. It contains several sections that have to be completed.. When all sections are marked green, the Resource Description can be submitted for approval.

Note: In case you already have an installed and configured Shibboleth Service Provider, you can use the Shibboleth wizard that completes many of the required sections by using the Service Provider's self-generated Metadata. To use the wizard, you will have to provide the URL to the Service Provider's Metadata handler URL. Alternatively, you can also provide metadata directly in case the Service Provider is not (yet) reachable via the network.

Basic Resource Information

The Basic Resource Information section is for providing the most essential details of the Resource Description. You must complete this section first before completing any other section.

In Figure 12 you see an example of this section:

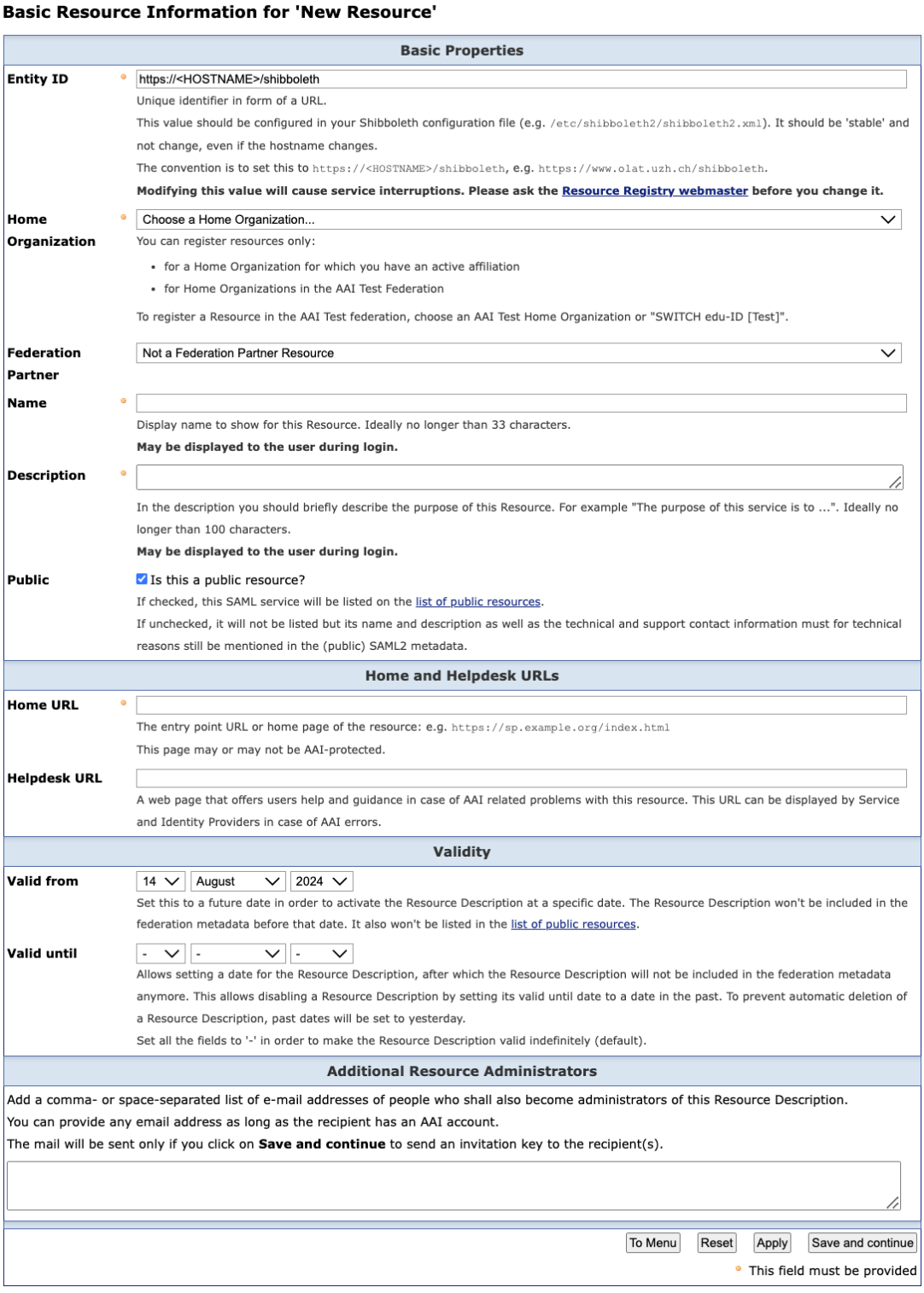

Figure 12: Basic Resource Description

First provide an identifier for the service and then decide for which federation and for which Home Organization you register a Resource. You can only register Resources for Home Organizations that you have an account for or for which your are Resource Registration Administrator of or for AAI Test Home Organizations.

If you are testing something related to AAI and if no real users are involved, choose a Home Organization from the AAI Test Federation if possible, e.g. AAI Demo Home Organisation.

The entityID (or clientID for OpenID Connect) is of great importance because it is the

identifier of the service. Ensure to check that you insert the value that you for your service.

Warning: Don't change the entityID or clientID unless you know exactly what you are doing. A change of this value as well as some other values must propagate to all Identity Provider first before it becomes active. The propagation time can be between one hour up to several days (when interfederated service is available via eduGAIN) where login may not be possible for your service because Identity Providers haven't yet downloaded the latest metadata file.

Validity: If your service is only temporarily available or shall only become active sometime in the future, you can specify this in the resource validity section. A Resource only is mentioned in the metadata and ARP files if it is valid at the moment the metadata is generated.

Visibility: Un-checking the public checkbox will hide the Resource Description within the Resource Registry from non-RRA users and in public resource lists on the Switch web page. It also will affect the metadata and ARP generation in the sense that name and description of the resource won't be included in these files.

After the form was successfully submitted, one returns to the resource menu that contains all the configuration sections of the Resource Description. As you can see, additional options have now become available.

Figure 13: Additional configuration sections become available

Descriptive Information

Service name and descriptions as well as logos and other information be provided in multiple languages. At least one English name and description must be provided. The service name and description may be shown on the login page and web pages listing all public resources.

List of Contacts

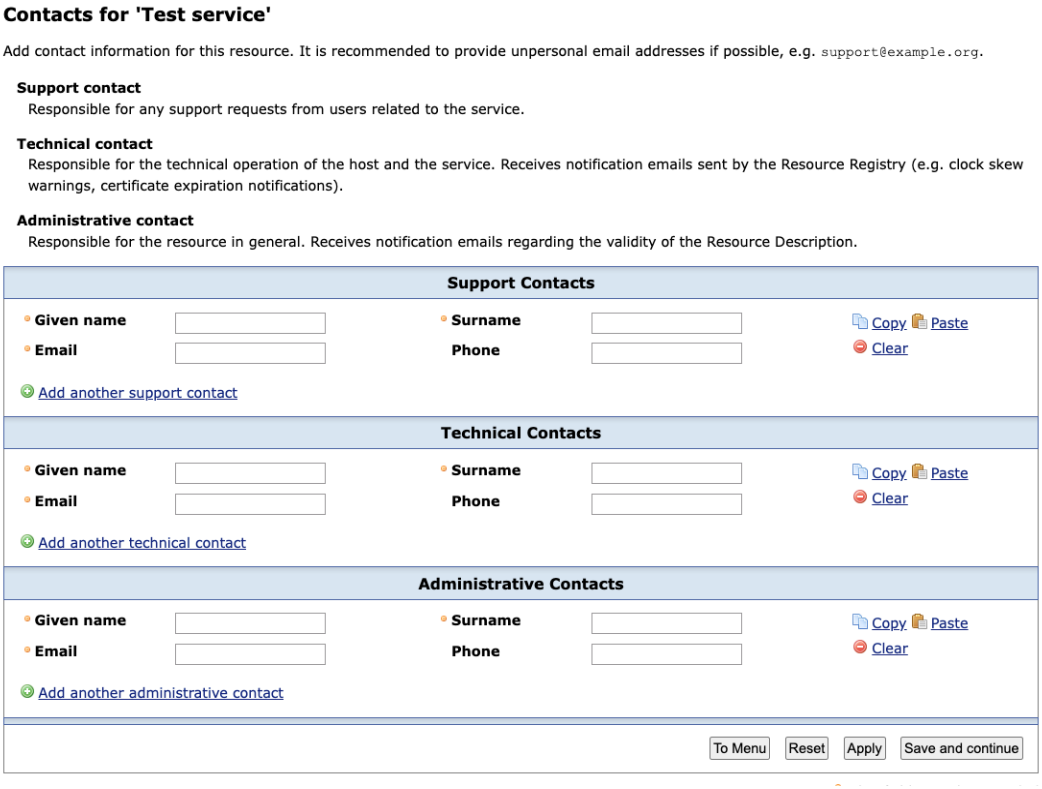

Figure 14: Resource contacts

At least three contacts must be provided for every Resource: an administrative, a technical and a support contact. These then will be shown on the Resource Registry itself as well as on SWITCH's public resource list as well as in the federation metadata. As can be seen in Figure 14, more than three contacts could be provided if needed.

Note: Support and technical contact names and addresses should be non-personal if possible. It should also be taken into account that these addresses will show up not only in the federation metadata but also on web pages showing all services of the federation.

Service Locations

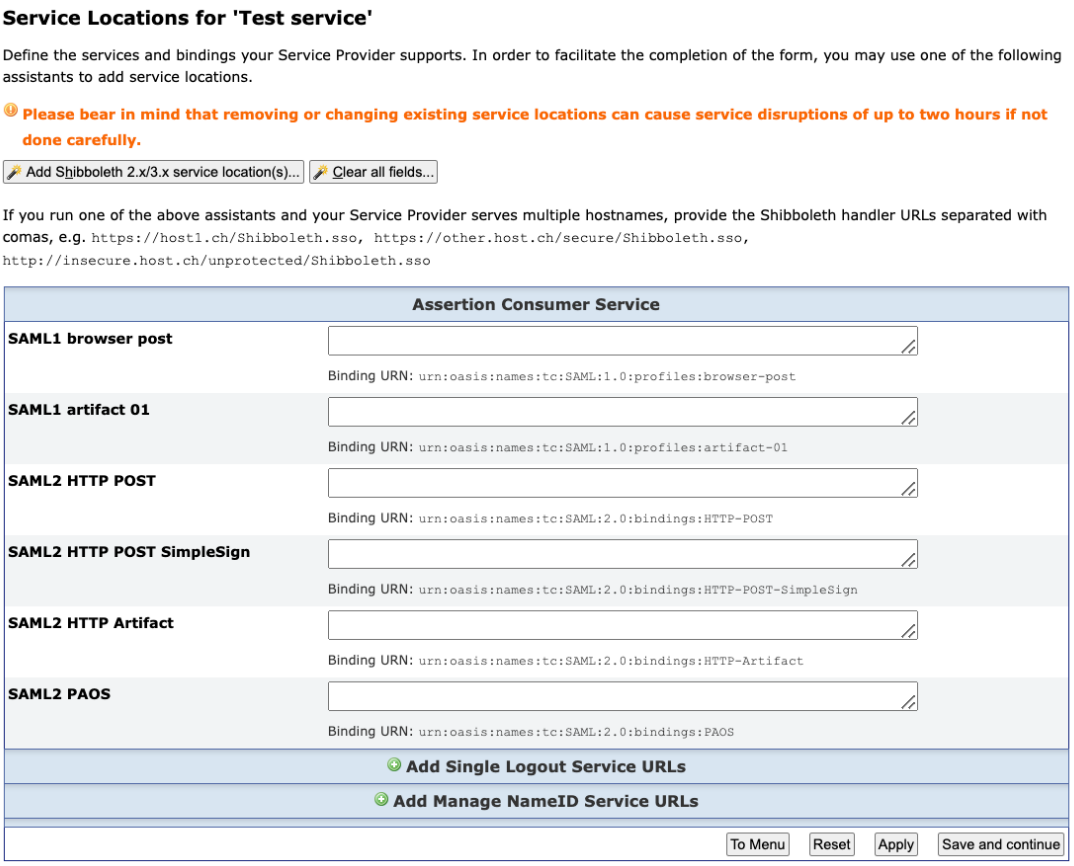

Figure 15: Service location endpoint URLs

In this section, which is shown in Figure 15, you define the SAML endpoint URLs of the Service Provider. If you were using the wizard, this section probably already was completed for you. Otherwise, the easiest way to complete it is to use one of the assistants. If you plan to operate the resource using multiple host names, you should provide service locations for all host names protected by your Service Provider.

Warning: Changes in this section need to propagate first to all identity providers before they become active.

Certificates And Credentials

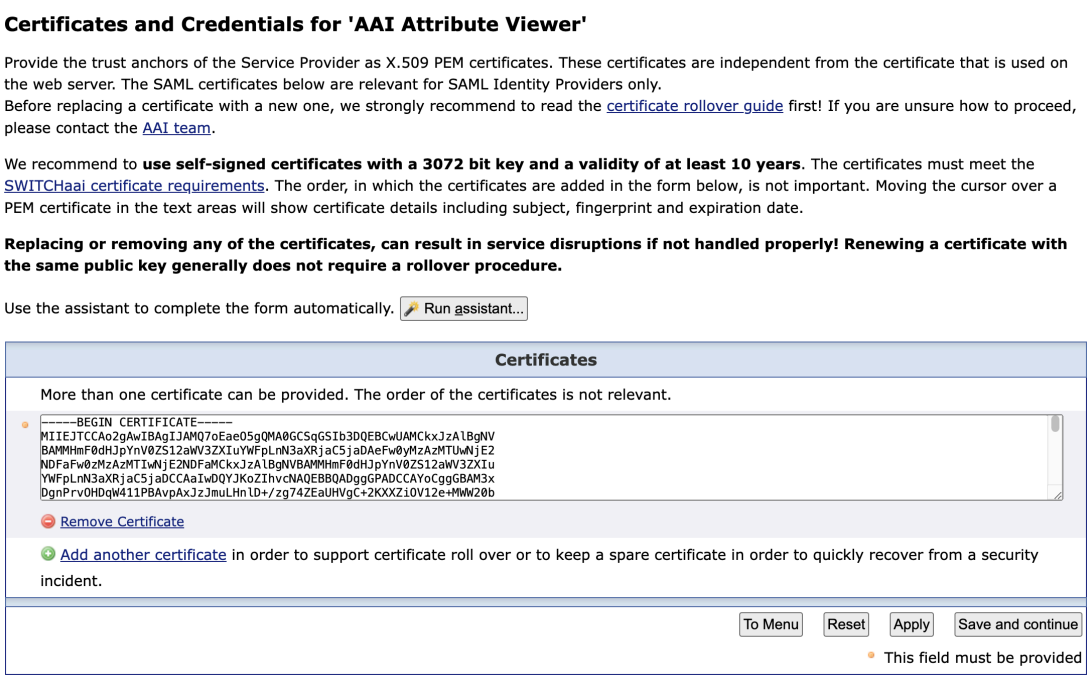

Figure 16: Used certificates

In this section one has to provide the X.509 PEM certificate, which is used by the SAML Service Provider or shared secrets or JWT tokens for OpenID Connect services. Please have a look at the certificate requirements page which are linked on this page. As is shown in Figure 16, a second certificate can be added as a backup certificate for roll-over procedures. If have to renew a certificate, please also have a look at the certificate migration guide which is also linked. The order of the two certificates doesn't matter.

Warning: Changes in this section need to propagate first to all Identity Providers before they become active.

Requested Attributes and Claims

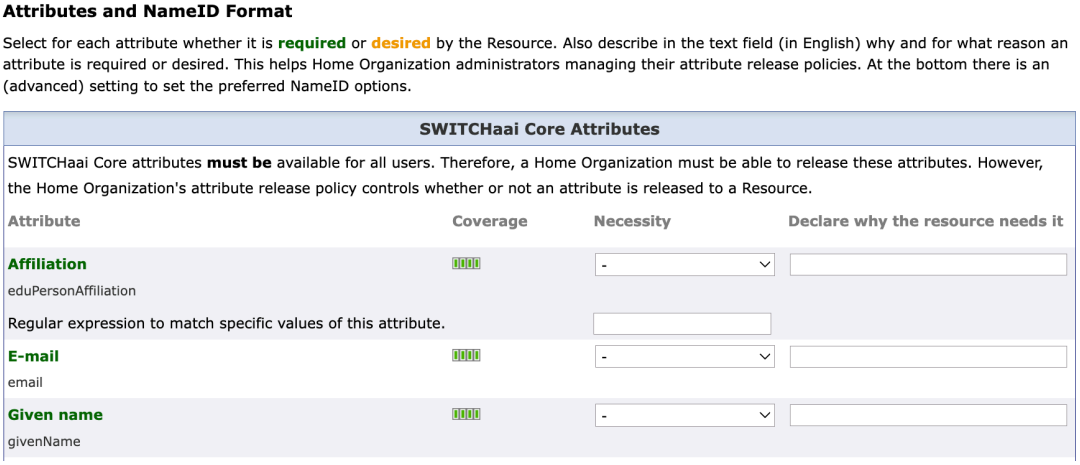

Figure 17: Required attributes

The Required attributes section is very important because it directly affects the Attribute Release Policies of all SAML Identity Providers and the edu-ID OpenID Connect Provider. As shown in Figure 17, one has to declare which attributes a service requires in order to work

and which attributes are desired/nice to have. It is recommended - and for some attributes mandatory - to provide a short comment why an attribute or claim is required or desired.

Note: Please keep in mind that the Swiss and EU data protection law states that only necessary user information shall be requested and processed. This implies that one should declare only attributes as 'required' that are essential for the proper functioning of a service.

Intended Audience and Expert Settings

The last section of a Resource Description configures some special settings and the intended audience settings of the Resource.

Some sevices may want to allow only users from specific organization types or only from from specific organisations. Using the intended audience settings it can be ensured that users e.g. on a Discovery Service or on Switch edu-ID can only select their organisation/identity from these eligible organizations. Figure 18 shows an example where the intended audience consists of all users from universities and users from Switch.

Note: Be accurate but not too restrictive when setting the intended audience because the settings on this page directly affect the Attribute Release Policy of the Identity Providers. Also, even though Identity Provider not in the intended audience generally restrict access to the service, the service should also additionally enforce access control and not rely solely on the attribute release policy of the Identity Provider, which prevent users from accessing the service.

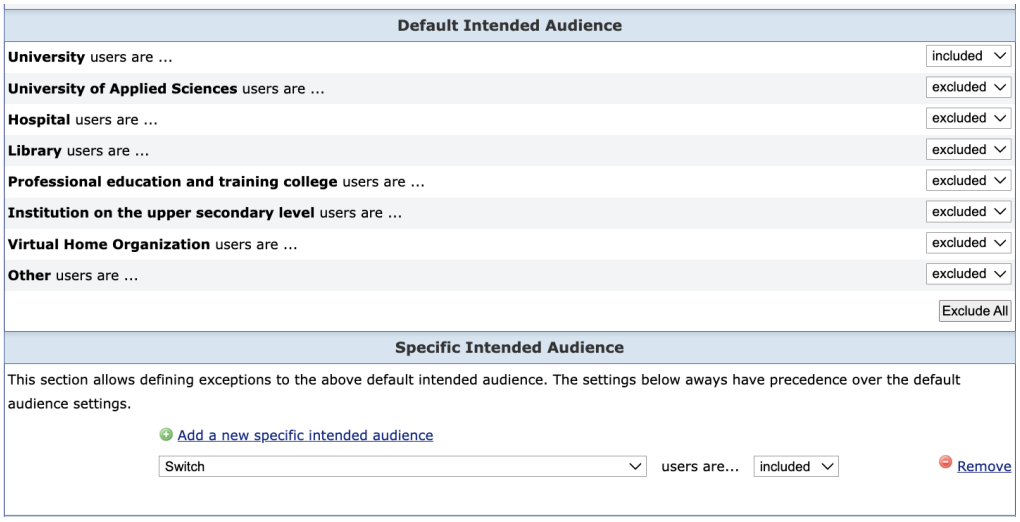

Figure 18: Intended audience

On this page there are also special settings that are mostly relevant for interfederated services (i.e. services accessible by eduGAIN users) or services with special needs for multi-factor authentication. Some of these expert settings – e.g. the interfederation checkbox - are only visible if the service or the Home Organization of the service meets some requirements (i.e. interfederation support is allowed only if the Home Organisation supports interfederation).

This section as well as the “Requested Attributes and Claims” sections have a direct influence on the Attribute Release Policy and attribute filter files that are generated for each Home Organization. In the attribute filter files of a Home Organization only those Resources will appear which included this Home Organization to the intended audience.

Submit Resource Description for Approval

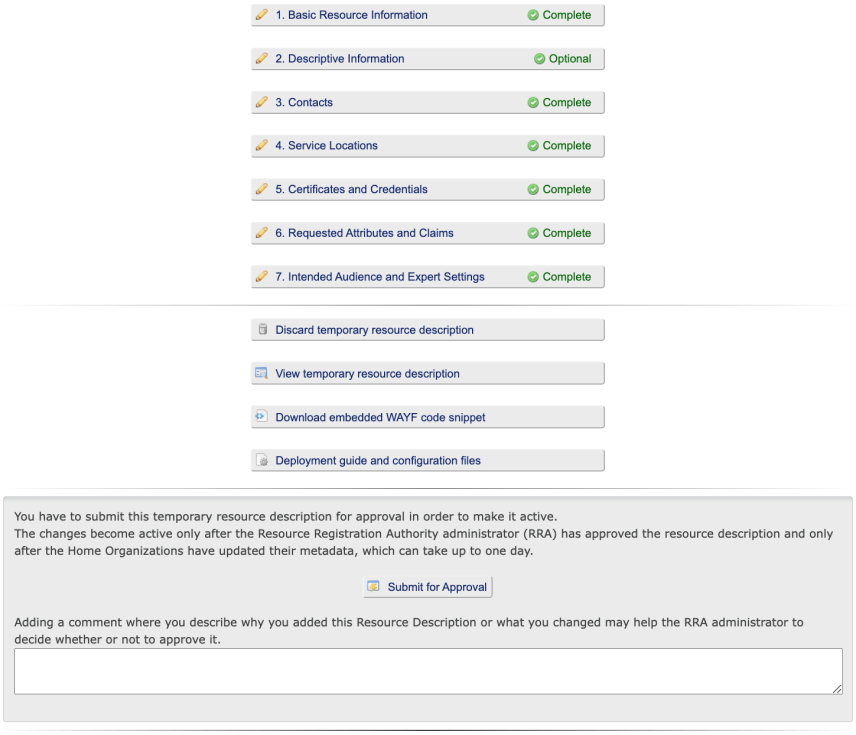

Figure 19: Completed Resource Description

Finally, if all sections are completed, the Resource Description has to be submitted and approved before it becomes active. One of the Resource Registration Authority (RRA) administrators for your Home Organization has to examine and approve it. This person will check whether you are eligible to register a Resource Description in the name of your organization, whether the service URLs you provided are within your organization's domain, whether the attribute requirements comply with the AAI Policies and the data protection law, etc.

There is also a button to discard the temporary Resource Description, which will delete all changes that have been made to an already approved Resource Description or will completely delete a not yet approved Resource Description.

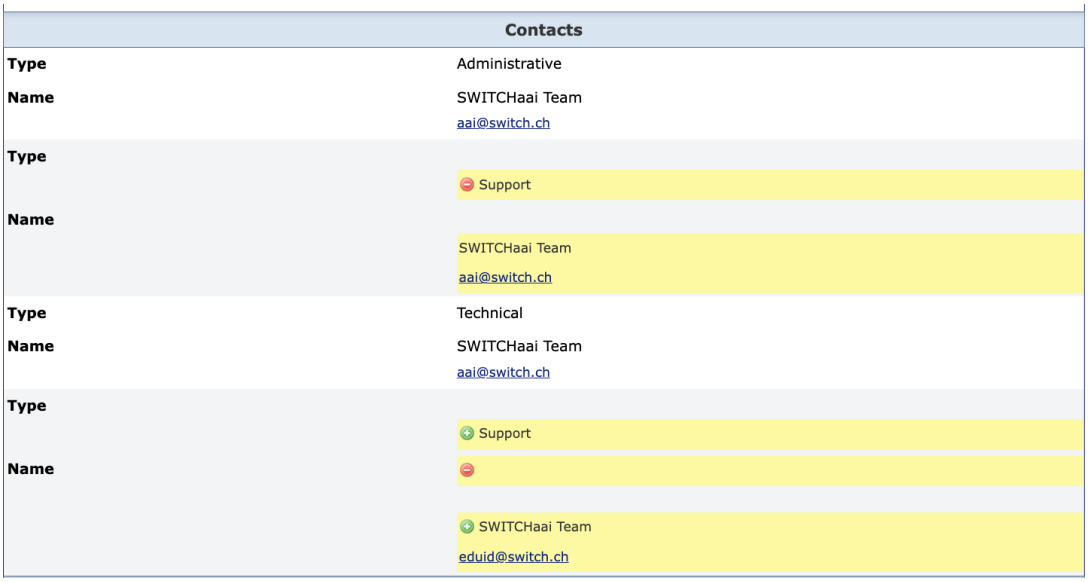

Figure 20: Resource Description Changes

Clicking on the 'View temporary resource description' button will show all changes (highlighted in yellow) that were applied to the last approved version, as shown in Figure 20.

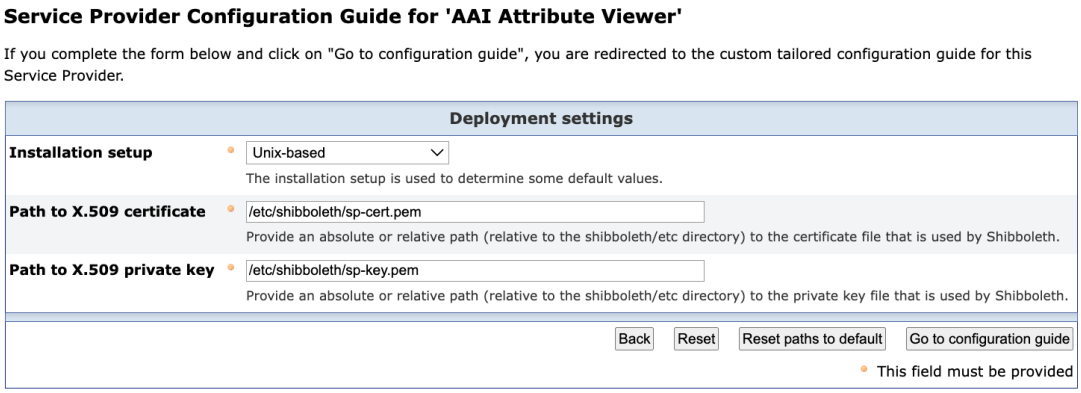

Figure 21: Download custom Service Provider configuration files

Using information available in the Resource Description, one also can be redirected to the configuration guide or download custom-tailored configuration code for the service. This is depicted in Figure 21. Selecting the setup that was used to install the Service Provider and providing the paths to certificate/key pair, one is redirected to the corresponding deployment guide where all needed configuration files can be directly downloaded.

If one clicks on the 'Submit for Approval' button, all RRA administrators are invited via e-mail to review and approve the Resource Description. It is recommended to add a comment in the text field for the RRA administrator, e.g. to describe what this Resource is used for or what and why something was changed. This is useful for the RRA administrator in order to decide whether the changes can be approved or not.

After a Resource has been approved, it is included in the official federation metadata at the full hour and at half past the full hour. It also will be included in the attribute release policy/filter files of the Identity Providers, which are generated at every full hour.

Furthermore, the person who created a new Resource Description also become the initial administrator of the Resource Description together with any additional users that are invited via email during the creation of the Basic Resource Information section. The role of a Resource Administrator can be transferred also to other users later on as described above.

Duties as a Resource Administrator

It is essential for the stability of a service that Resource Descriptions are as up-to-date as possible. Therefore, a Resource administrator should update the Resource Description as soon as a technical property has changed. E.g. this could for instance be adding an additional service location/host name or adding an additional rollover certificate or adding/removing requested attributes.

Note: Keep in mind that there is a propagation delay for changes applied to a Resource Description. First due to the required approval of the RRA administrator and second due to the delay for metadata refresh at the Home Organizations. The official metadata published by Switch is updated at least every full hour if something changed. The Identity Provider should update metadata at least once a day, most will update hourly.

Warning: Replacing or modifying certain Resource Description properties like certificates or service locations has to be done very carefully because these changes will take some time to propagate to all Identity Providers. The propagation via the metadata may take up to one day during which your Resource may not be available because some Identity Providers may still use metadata with old properties while other Identity Providers are already using the new properties. If in doubt about a property you want to change, please send an email to aai@switch.ch for assistance.

4.2. Home Organization Administrator

When an organization decides to join the SWITCHaai or the AAI Test Federation, it has either to set up a SAML Identity Provider or it has to adopt Switch edu-ID by supplying affiliation data to the edu-ID service. The latter option is the more comfortable and more future-proof, which also allows benefiting from all advantages of Switch edu-ID.

If an organisation nevertheless operates their own Identity Provider, this Identity Provider has to be registered and managed in the Resource Registry. To do so a Home Organization administrator has to provide the necessary (technical) information that services require to communicate with a SAML Home Organisation (it is currently not possible to run an own OpenID Connect Provider and register it with SWITCHaai).

Bootstrapping a Home Organization Registration.

After setting up of the new SAML Identity Provider, one has to go to https://rr.aai.switch.ch/. On the first page, you will find a link that guides you to the Home Organization Bootstrapping form.

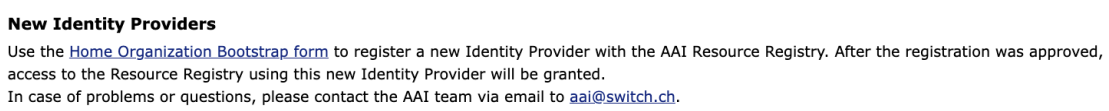

Figure 22: Bootstrapping procedure

On the following page some basic technical details about the Home Organization have to be provided.

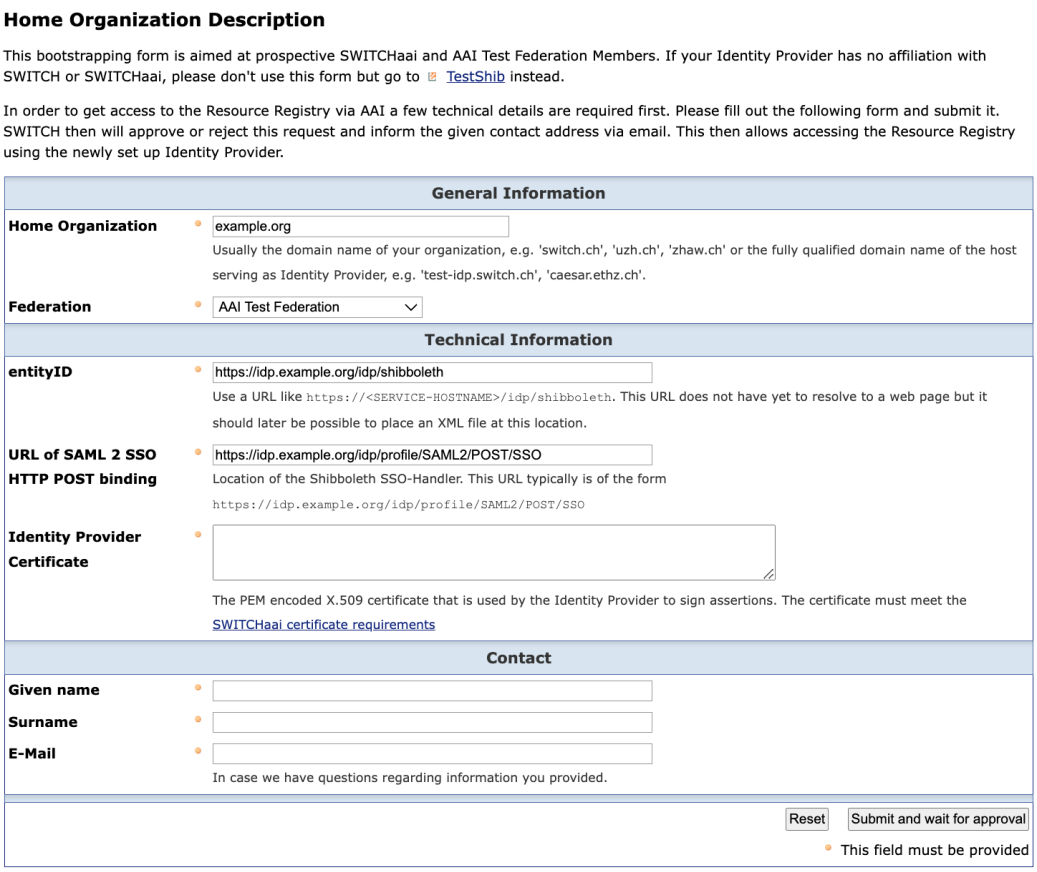

Figure 23: Bootstrapping registration form

Fill in the required information and click on the 'Submit and wait for approval' button afterwards.

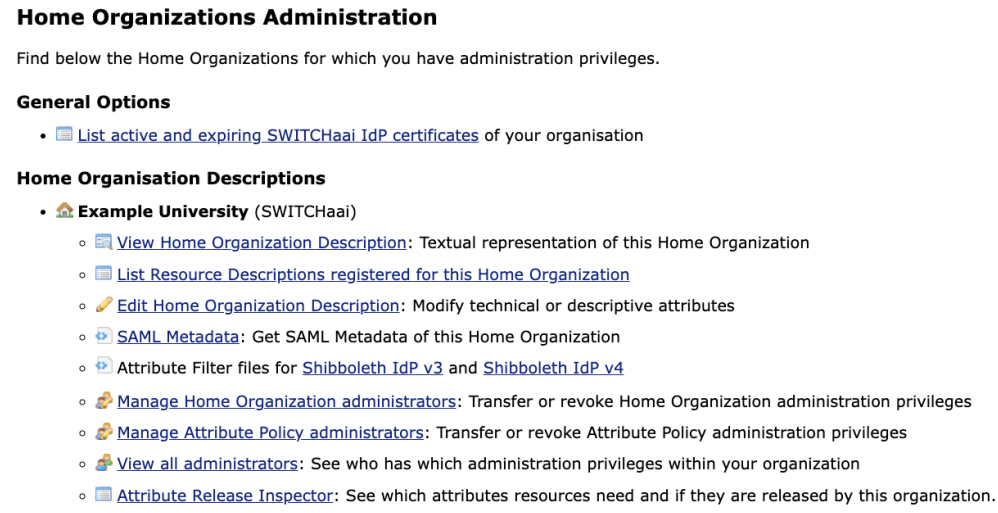

Figure 24: Adding a new Home Organization Description

After submission of the bootstrapping form, Switch will examine the registration data and approve or reject the new Home Organization within a few business days. In either case, you will receive a notification email with further instructions. After the Home Organization has

been approved, one is able to access the Resource Registry with an account of the approved Identity Provider.

The first time a user logs in as user from an newly approved Home Organization he receives not only Home Organization rights as shown in Figure 24 but also Resource Registration Authority administration rights, described in the following Chapter.

It is recommended to edit the Home Organization description after the first login because the data provided during the bootstrapping procedure is far from complete. Edit the Home Organization Description by clicking the link *"Edit Home Organization Description"* on top of the page. The resulting page will look like in Figure 25. There, one will have to edit several sections in order to define various aspects of a Home Organization.

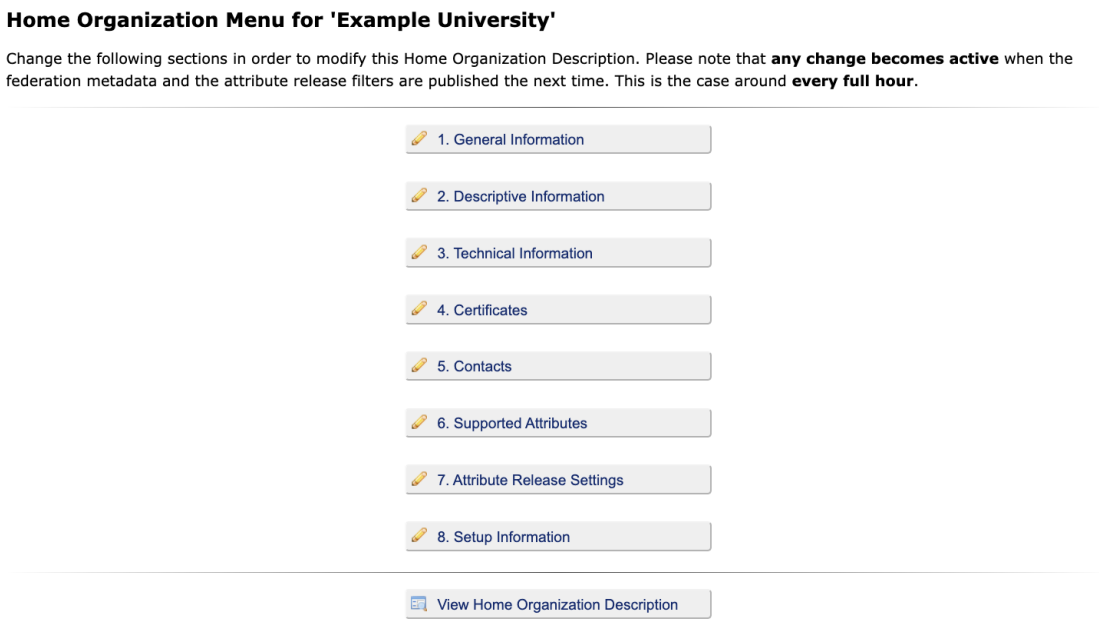

Figure 25: Home Organization Editing Menu

General Information

In the General Information section one first defines the very basic settings of a Home Organization like its name, its Federation, a description and a help desk web page like shown in Figure 26. The name and descriptions must be provided in English. Alternative version in other languages can be provided in the next section.

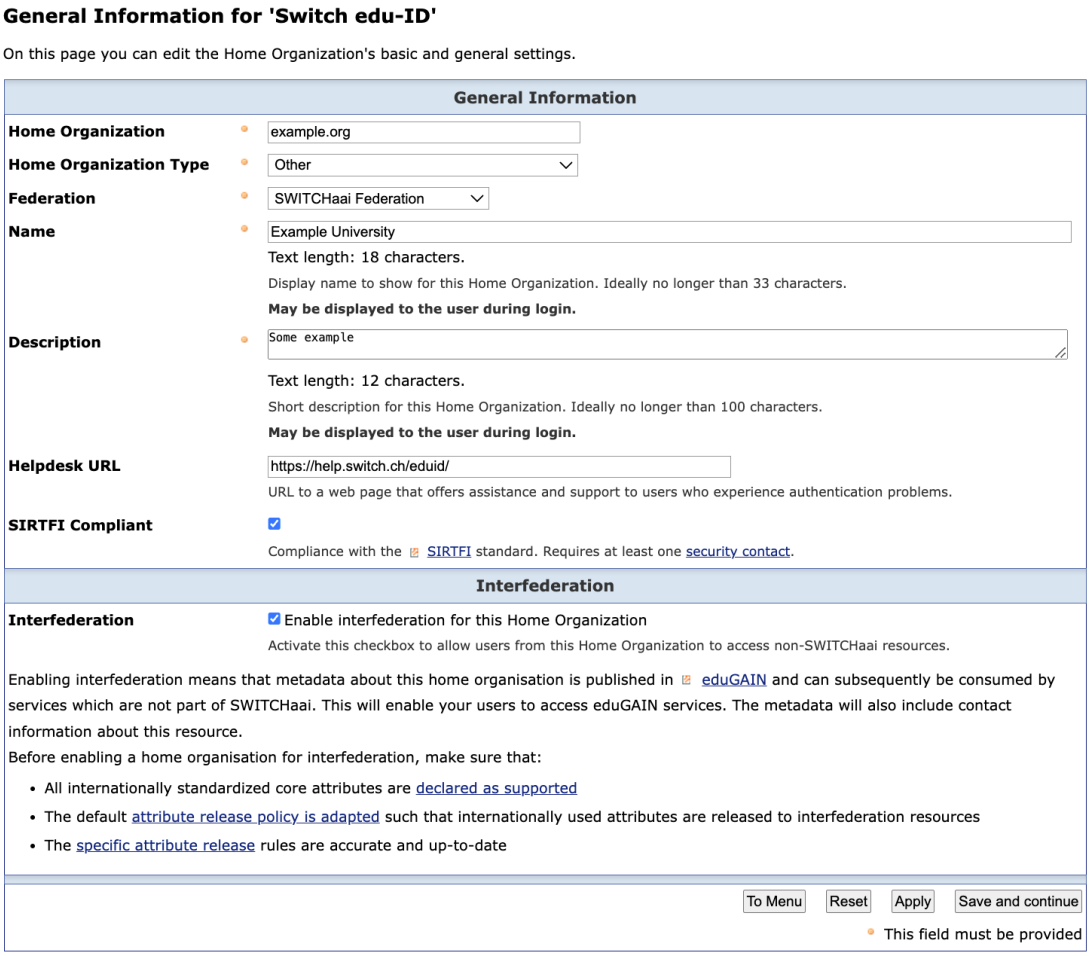

Figure 26: General Information

All settings in the section “General Information” are either of organizational or descriptive nature and are not technical in any way. Therefore, they could be changed without affecting the operation of an Identity Provider.

Descriptive Information

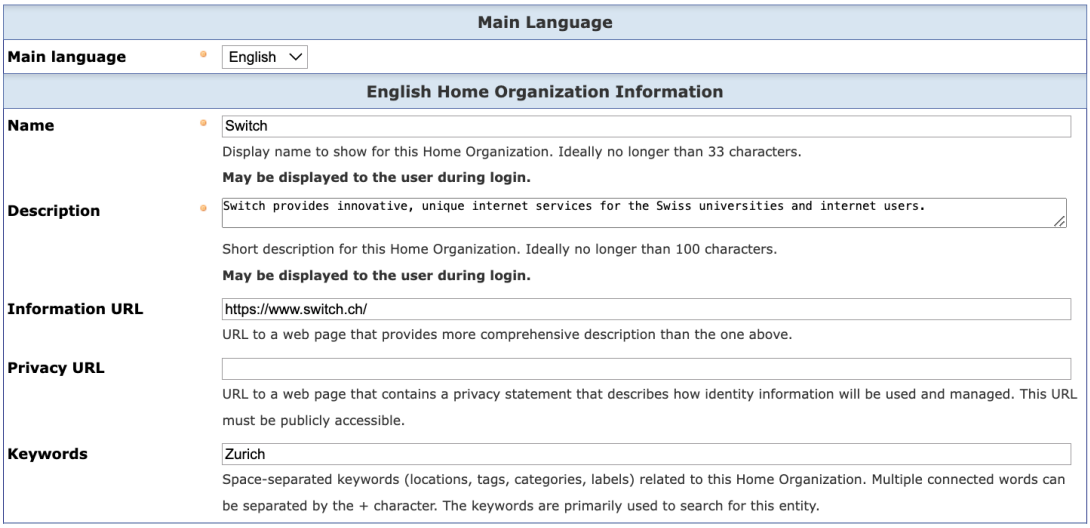

Figure 27: Additional Language Description

On this page one can add name and description of a Home Organisation in other languages than English. The main language for a Home Organization is the default language that will generally be used to display the name and description of a Home Organisation.

Also, links to information pages data privacy pages as well as logos and geo information can be provided on this page. The latter may be used on Discovery Services where users have to choose the organization to login with. Thanks to geo information a organization that is close to the user may be proposed.

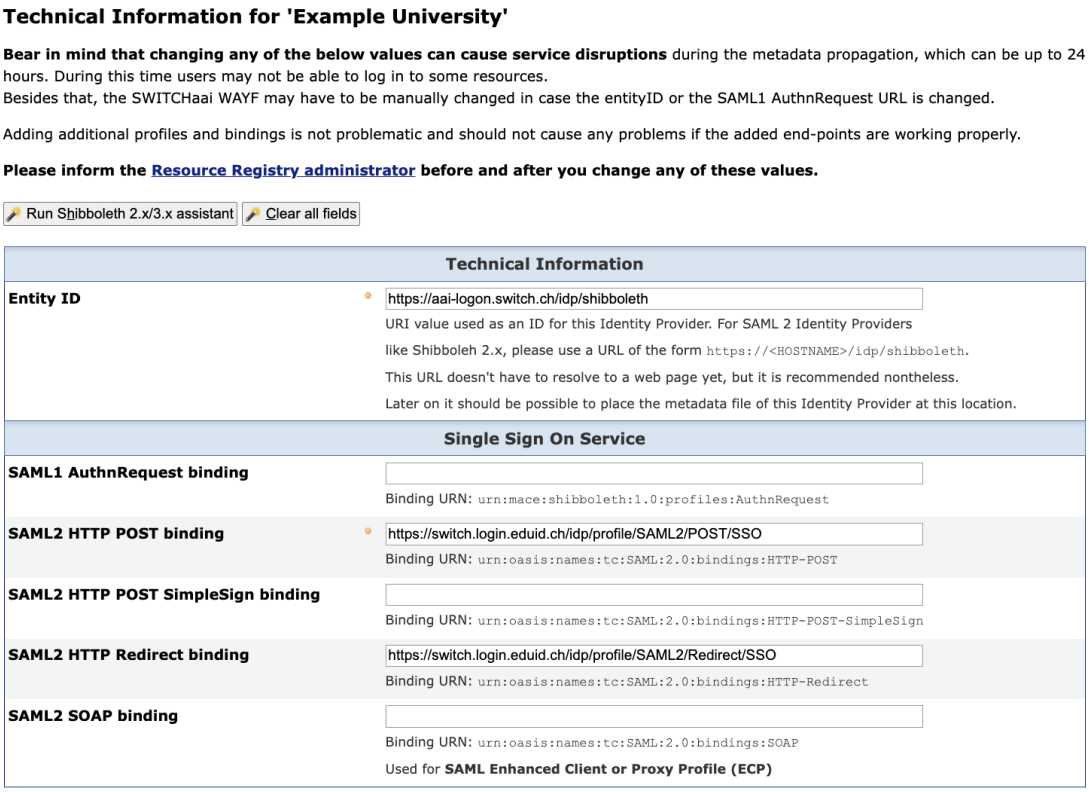

Figure 28: Technical Information

Technical Information

In the Technical Information section, one has to define the Identity Provider's *EntityID*, which is an ID following a special naming convention. The convention for the format of the *entityID* is to use a URL. More precisely, the URL should consist of 'https://' followed by the host name and the suffix '/idp/shibboleth', similar to the ID of Service Providers. This then look.s for example like 'https://some-organization.ch/idp/shibboleth'.

Note: It is highly recommended that the host name used in the entityID matches the hostname of the Identity Provider.

To set the SAML Identity Provider's endpoints, you may use one of the available assistants in order to complete the URLs. The assistant then will use the root URL of the web application you provide to generate the default service locations for the given bindings as shown in Figure 28.

Warning: Modifications of any properties in the Technical Information section have to be performed very carefully because these changes will take some time to propagate to all Service Providers. The propagation delay normally is between one and two hours for Resources that are configured according to the SWITCHaai deployment guides.

Used Certificates

In the Used Certificates sections the certificates used by Shibboleth and the web server have to be provided in PEM format. One can use the assistant in order to complete the form. The additional certificates can be used for certificate roll-over or for emergency fallback certificate.

In order to replace a certificate without any service disruptions, one has to make sure that the new certificate has been included in the federation metadata for at least one day before it can be used. Please refer to the Service Provider deployment guides at

http://www.switch.ch/aai/support/identityproviders/ on how to carry out the certificate rollover.

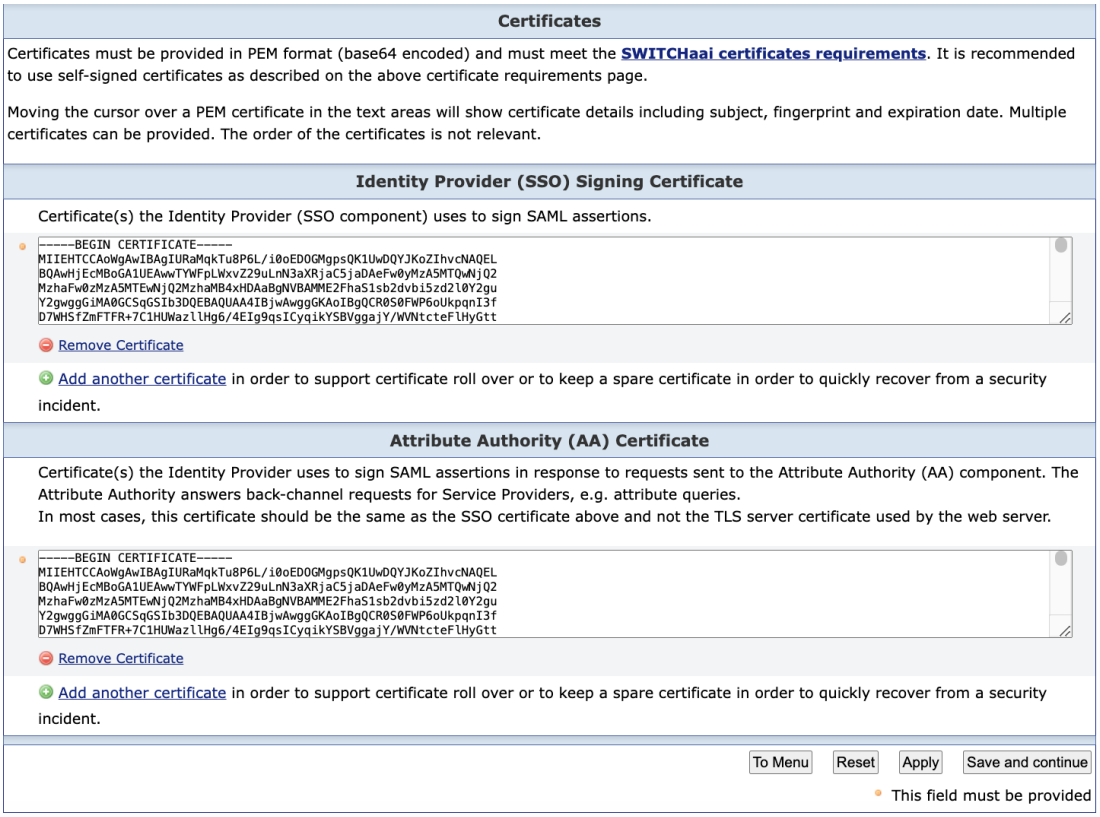

Figure 29: Used Certificates

The Resource Registry will not expire certificates automatically if they have expired. Before the expiration date, several notification emails are being sent to the technical contact address of a concerned Home Organization.

Expired certificates are kept and generally they still work because most SAML Service Provider care only about the public key in the certificate but not about expiration dates or the certificate subject.

List of Contacts

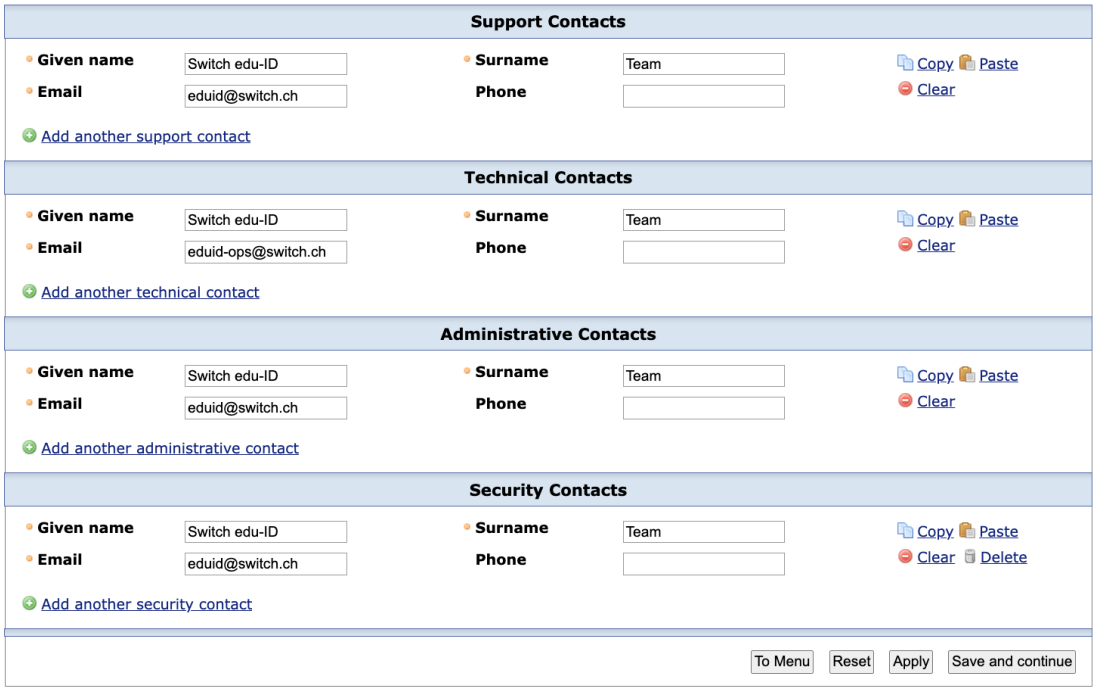

Figure 30: List of Contacts

There should be at least one technical contact for each Home Organization. Although it is not mandatory to provide also support and administrative contacts, it is recommended to do so. All contacts should be non-personal if possible. One also should be aware that these addresses will show up not only in the federation metadata but also on the list of all SWITCHaai Home Organizations.

It it also recommended to provide a security contact, which is required for example to support the Security Incident Response Trust Framework for Federated Identity (Sirtfi) framework.

Supported Attributes

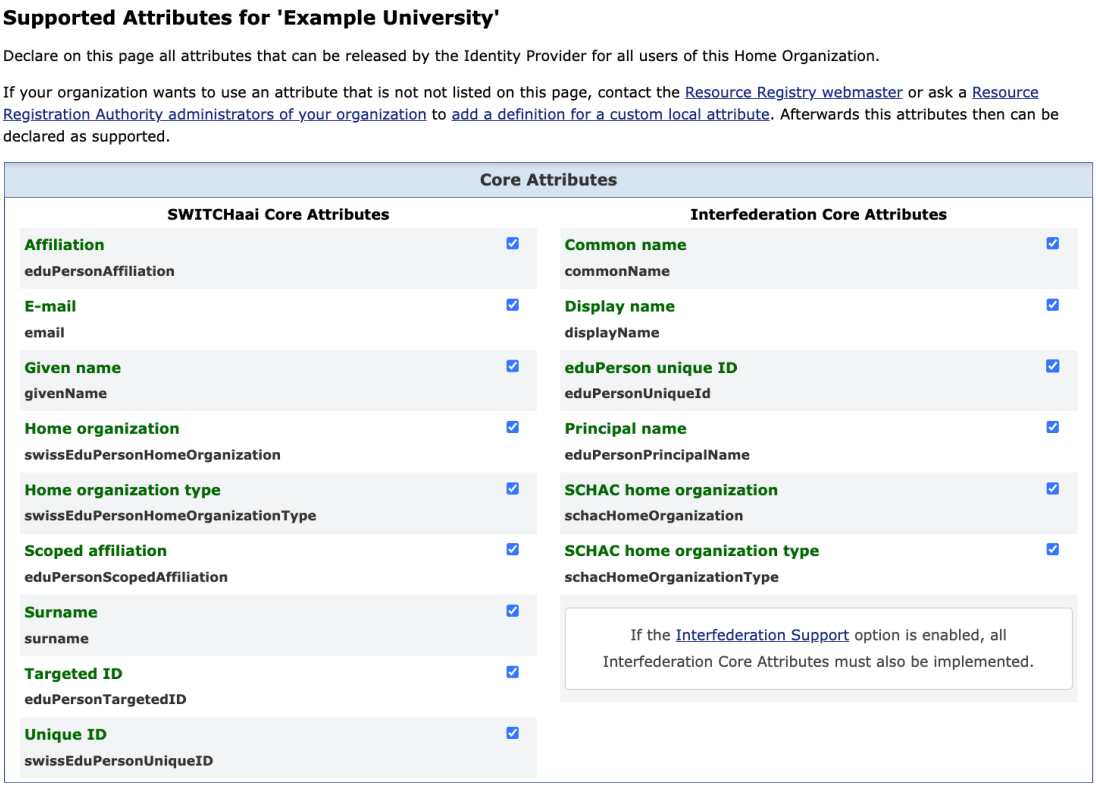

Figure 31: Supported Attributes

The Supported Attributes section's purpose is to declare the attributes an Identity Provider can release. As depicted in Figure 31, on the left-hand side, one has to check the SWITCHaai attributes that can be released by the Identity Provider.

According to the AAI Attribute specification an Identity Provider must be able to release at least the green core attributes in the SWITCHaai section. The attributes in orange are optional to support and some are used only locall/bilaterally.

Checked attributes will only be released if needed and generally only a subset of these attributes will be released to a service depending of the services attribute needs and the Attribute Release Policy of the Identity Provider.

If the interfederation option is enabled for a Home Organisation, additional attributes should be supported to be interoperable with entities from other federations, in particular the core attributes in the section “Interfederation Core Attributes”.

Attribute Release Settings

In this section a Home Organization or Attribute Release Policy administrator defines the rules to use when deciding if an attribute or some of its values are to be released to a service when a user logs in. The resulting rules are then written into an attribute-filter.xml file that a Shibboleth Identity Provider can download (most other SAML implementations don’t support attribute filtering loading external files).

The default Attribute Release Policy is defined by release scope for 'required' and 'desired' attributes as shown in Figure 30.

The release scopes are:

Nobody:

Attribute will not be released in general. This option is useful in case the release of an attribute is controlled only via specific attribute release rules mentioned below.

Resources of my organization:

Releases the attribute only to Resources which were registered by the same Home Organisation. This excludes all Federation Partner Resources.

Local Federation Resources:

Releases the attribute by default to all services in the same federation as this Home Organisation Description if the services request it.

Interfederation Resources:

Releases the attribute to all Resources in general, even such from other federations accessible via eduGAIN. This option is only available if interfederation support is enabled for this Home Organisation.

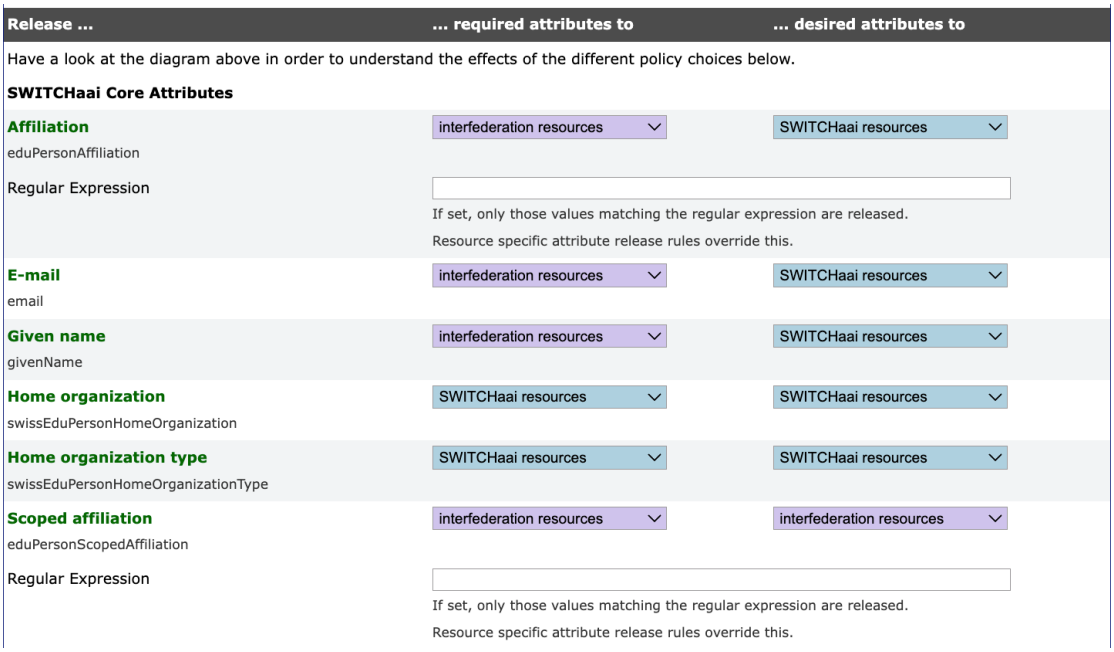

Figure 32: Default Attribute Release Policy

Note: Only those attributes are shown which can be released (i.e. are supported) by the Identity Provider. If you add an additional attribute in the Supported Attributes section, you should also define a general attribute release policy rule for this attribute. Otherwise, the default rule (release required attributes, don't release desired attributes) will be used.

There are also some entity categories like the REFEDS Research & Scholarship entity category that can be assigned to services. Services that are labelled with such an entity category can be treated specifically by defining the policies for Entity Categories.

Resource Specific Policies

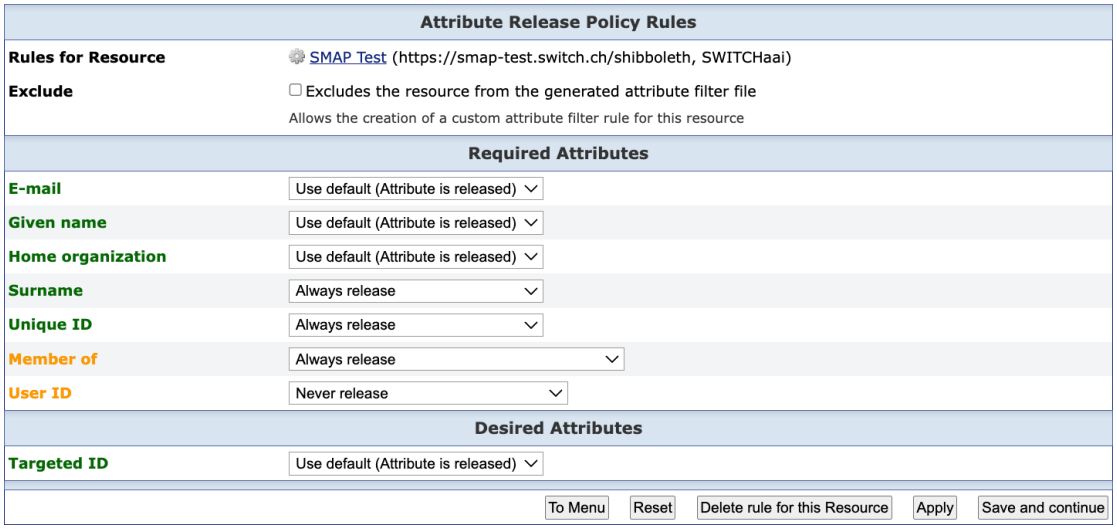

Figure 33: Specifc Attribute Release Policy

While one could define a very general attribute release policy in the previous section, the Resource Specific Policies Attribute Release Policy section allows defining very fine-grained rules for the attribute release. As is shown in Figure 33, one can create custom-tailored rules for each Resource. Either a whole Resource can be excluded completely from the attribute filter or one can set individual exceptions to the default rule for specific attributes.

Excluding a Resource from the attribute-filter.xml file is useful if an Identity Provider administrator wants also to create a very custom-tailored rule for this Resource and therefore doesn't want it to include in the filter generated by the Resource Registry. Such rules can include advanced PolicyRequirementRules, which can base the release decision on a huge variety of criteria.

Warning: Be careful not to break services for your users because you exclude them from the attribute filter or because you exclude certain attributes that are required by the resource.

Note: The Attribute Release Policy rules only have an effect if the (Shibboleth) Identity Provider loads their attribute-filter.xml file directly from the Resource Registry. Other SAML implementations might have to configure the attribute release differently.

Setup Information

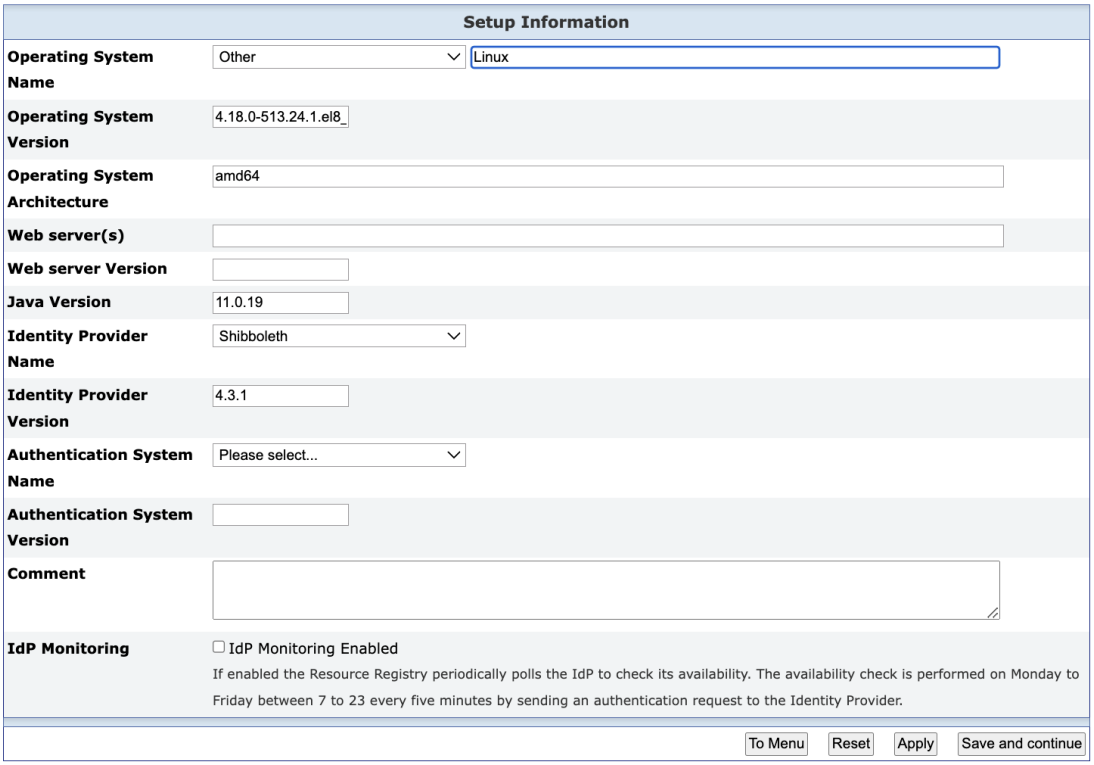

Figure 34: Setup & Environment Information

This section is shown in Figure 34. It is purely informational and solely serves Switch as the federation operator as well as other Home Organization administrators to examine how different Identity Providers are set up. This allows comparing similar setups in case of problems or intended setup changes or specifically notifying administrators in case of known security vulnerabilities.

The Resource Registry daily polls all Service and Identity Providers to update some of the setup and environment information. This is, however, only possible if they were deployed according to deployment guides that Switch offers. These guides include configuration files that allow the Resource Registry to access the status handlers.

Duties as Home Organization Administrator

Because the metadata generated by the Resource Registry heavily relies on the descriptions of Resources and Home Organizations, it is strongly recommended to keep them as up to-date as possible. Otherwise, problems may occur because third parties interacting with your Identity Provider may have outdated information. This means:

- If you change your Identity Provider DNS host names, modify its certificates, provide additional attributes for your users, please update the Home Organization Description. However, if you do so, please inform eduid@switch.ch beforehand because certain changes could cause service disruptions if not planned and carried out carefully.
- Regularly update the metadata of your Identity Provider. It is recommended to update metadata more frequently because the file only will be downloaded if it changed.

  Note: There will be a propagation delay of at least one hour for certain changes applied to the Home Organisation. To become active, a change in metadata first has to be downloaded by a Service Provider.

- Regularly inspect the attribute release policy mails that are sent to the technical contact address of a Home Organisation. In case you see a Resource that requests too many attributes, create an exception in the specific attribute release policy for this Resource.

4.3. Resource Registration Authority Administrator

Every Home Organization needs at least one Resource Registration Authority (RRA) administrator who approves Resource Descriptions. This includes the approval or rejection of Resource Descriptions. An RRA administrator basically should ensure that all Resources operated within the Home Organization are in compliance with the SWITCHaai Service Agreement (see https://help.switch.ch/eduid/docs/about/governance/legal/).

Home Organizations can decide to enforce stricter approval procedures requiring the requesting user and approving user to use different accounts. This feature is called 'four-eyes approval' and can be activated on request for a Home Organisation.

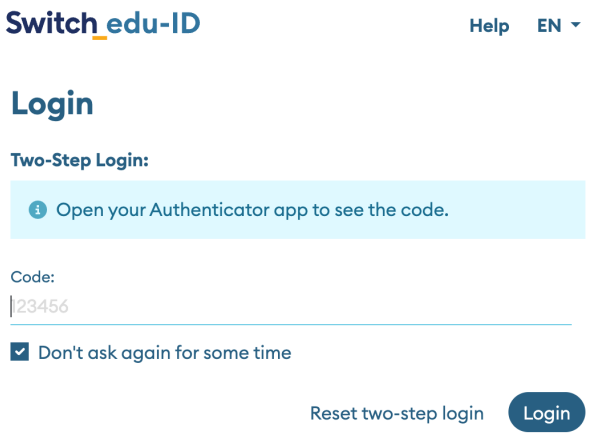

Figure 35: SMS Two-factor One-Time Password Authenticationn

In addition, the Resource Registry supports a mode where certain actions for specific Home Organisations require two-factor authentication. This is only supported for organizations that adopted Switch edu-ID. This then looks like in Figure 35.

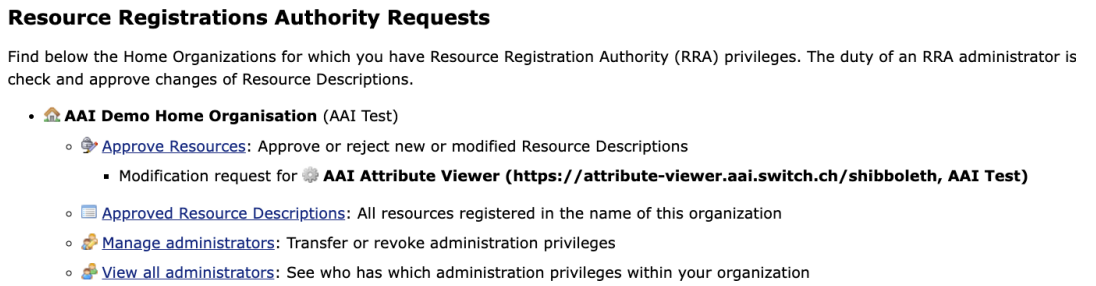

Figure 36: Resource Description waiting for approval

Duties as a Resource Registration Authority Administrator

The following duties apply for RRA administrators. Please check that:

- the person who created or modified a Resource Description is allowed to operate an AAI Resource in the name of your Home Organization.
- every Resource Description has at least one valid contact person for administrative, technical and support inquiries.
- the Resource Descriptions declares only as many attribute as required as are needed for its proper functioning and complies with the Swiss data privacy law.
- The Resource's end point URLs (service locations) point to eligible host names that are affiliated with the Home Organization.
- If any self-signed certificates are used, the RRA has to proof that the person that presumably registered the Resource Description is in possession of the certificate's private key.

In order to examine these details, an RRA administrator should inspect a Resource Description befor approving it. The Resource Registry will in some situations display warning messages when some of the above points should be checked in particular.

Every time a Resource Description is submitted for approval, all RRA administrators of the Home Organization the Resource was submitted for will receive a notification e-Mail. An RRA administrator will see the Resource Descriptions that still need approval on the Resource Registration Authority page as shown in Figure 36.

Clicking the *"Approve Resources"* link then leads to a page like in Figure 37.

Figure 37 shows a single Resource Description to approve or reject. Clicking on '*View changes*' an RRA administrator can inspect the difference between the currently active and the modified Resource Description.

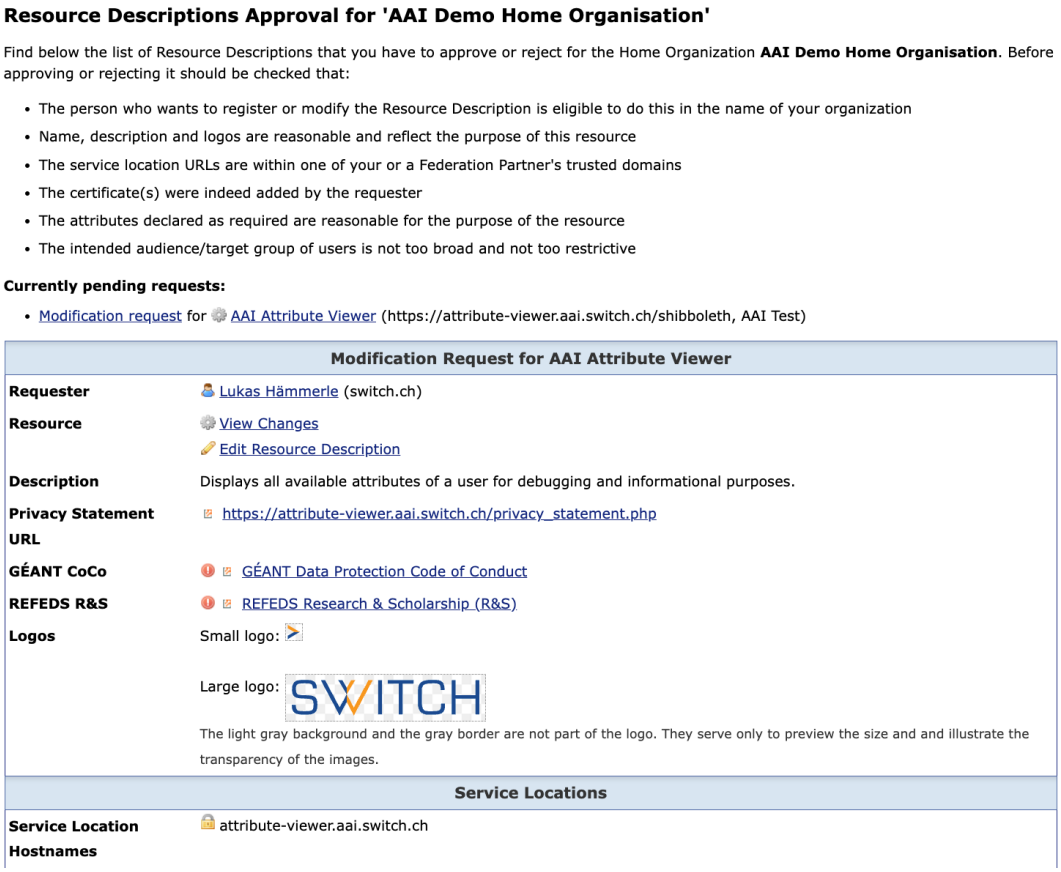

Figure 37: Approve a Resource Description

Together with the approval or rejection notification email a comment can be sent to the user who requested the modification of the Resource Description.

5. Miscellaneous

This chapter contains various topics that weren't mentioned above but that nevertheless deserve some attention.

5.1. Data Usage

Data stored in the Resource Registry is not only used for the management of the federations operated by Switch but it is also used to serve as information source to end users. In particular, the following web pages directly access the Switch Resource Registry database:

- https://help.switch.ch/aai/support/help/
- https://help.switch.ch/aai/participants/allresources/
- http://www.switch.ch/aai/participants/allhomeorgs.html
- https://help.switch.ch/aai/guides/discovery/login-link-composer/

If a Resource Description is changed, this is reflected on the above web pages as soon as the change gets approved. Changes of Home Organisation Descriptions become effective immediately.