AAI Resource Registry Guide

Version: 20080612 Authors: LH, TL

AAI web page: http://www.switch.ch/ Contact: aai@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 the already integrated explanations. It explains the most important aspects and processes that are needed to register and maintain Home Organization and Resource Descriptions.

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

Table of Contents

1. Description of the Resource Registry

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. The intended users of the Resource Registry are Resource and Home Organization administrators.

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

- **Attribute requirements declaration**
  Resource administrators specify the required attributes to provide for accessing the resource. In addition, desired attributes can be listed too. Desired attributes should provide additional benefit to justify their use. The data protection principle counts: Process only data which is really necessary!
- **Resource 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!

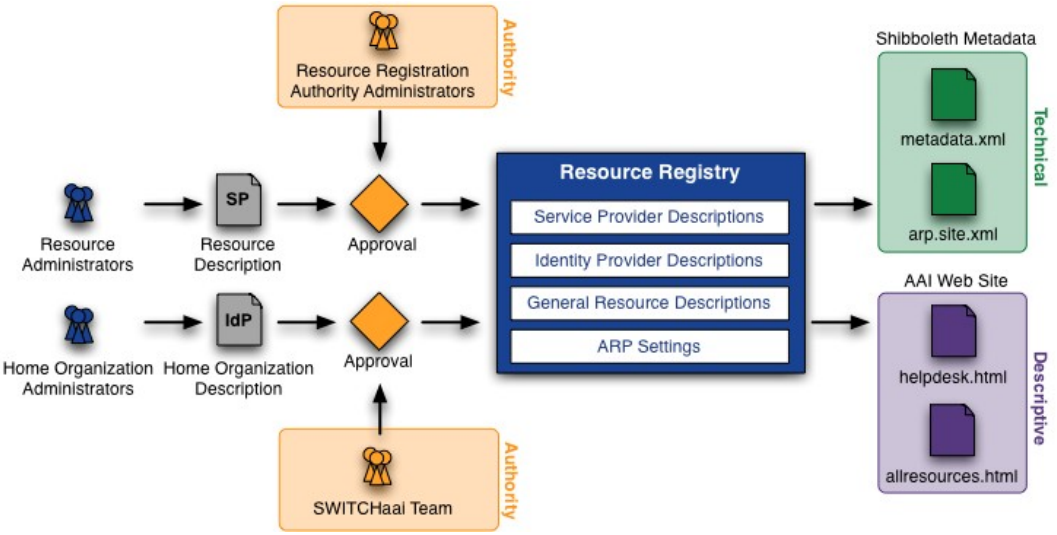

Figure 1: Resource Registry overview

- **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 alerted by e-Mail, whenever approval is required for changes made to Resource Description in the Resource Registry.
- **Identity Providers 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 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 also is 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 relating to the federation.

The Resource Registry is written in PHP 5 using PEAR/QuickForm and MySQL.

2. Login

The Resource Registry is accessible via https://aai-rr.switch.ch/ and requires an account in SWITCHaai or AAI Test. The start page contains a short description of the Resource Registry and two login buttons. These login buttons are the entrance to the Resource Registry for the production SWITCHaai Federation and the AAI Test Federation.

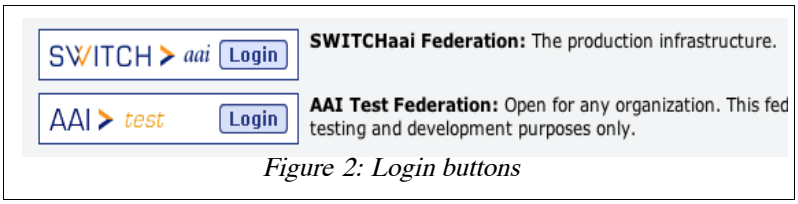

Figure 2: Login buttons

To log in one has to click on the login button that represents the federation of which ones Home Organization is part of. After the authentication at a Home Organization one gets redirected back to the Resource Registry. Provided the Resource Registry receives all the required attributes from the Home Organization, login is successful. The required attributes are:

- Given Name
- Surname
- E-Mail Address (optional)
- Unique Identifier
- Business telephone number (optional)
- Home Organzation Name
- Home Organization Type

Note: Whether you log in via SWITCHaai or AAI-Test doesn't matter, the Resource Registry and its procedures work almost the same. However, when you are logged in via the AAI Test Federation you cannot modify Resource Descriptions or Home Organization Descriptions that are part of the production SWITCHaai Federation. This is due to security considerations. The opposite way, editing AAI Test Resource Descriptions with a SWITCHaai acccount, is possible though.

When a user logs in the first time, a data protection agreement (see Figure 3) has to be first accepted. 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 some cases where an administrator needs to ask you something (e.g. fingerprint of your self-signed certificate) on the phone.

Therefore, you have to give your consent for the storage of personal information. SWITCH won't use personal data for anything else than for AAI related matters and no data will be used or processed by third parties.

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.

Note: To log out of the Resource Registry (and all other AAI-enabled applications), the easiest and safest way is to just close the web browser. This will destroy all sessions that you may have for the Resource Registry, the WAYF and yourIdentity Provider.

3. Configuration Sections

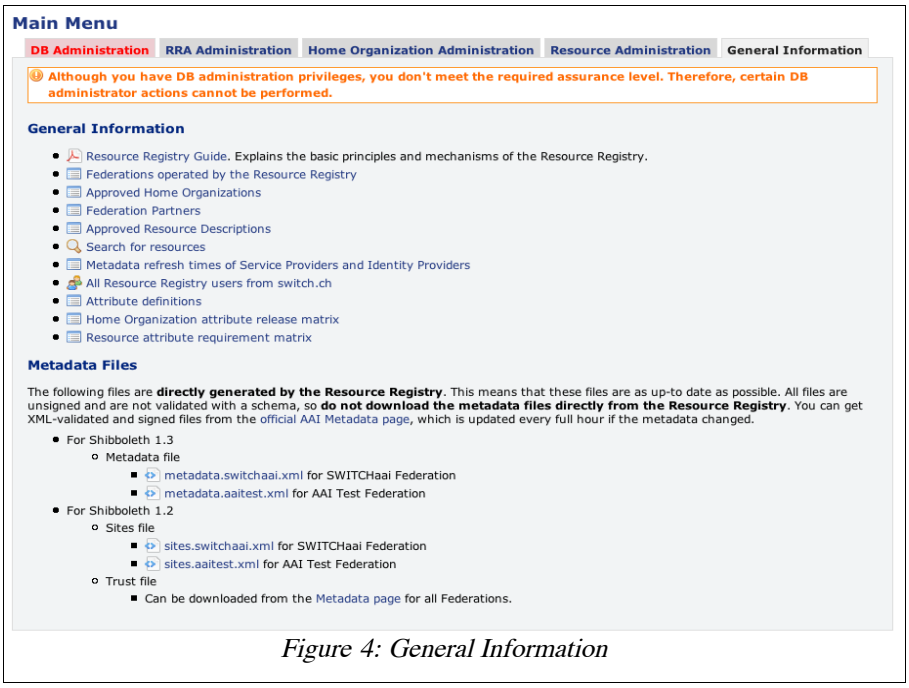

Figure 4: General Information

After successful authentication, you see to the main menu of the Resource Registry. Depending on your privileges and roles (see Chapter 4), you will see between two and five different tabs reflecting the administration and access rights you have.

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.

At the bottom you also find links to the metadata that is directly generated by the Resource Registry. In the federation metadata files all Home Organizations and Resource Descriptions managed by the Resource Registry are reflected.

Figure 5 shows the 'Resource Administration' options. Unless you already have registered a resource you can only add a new Resource Description.

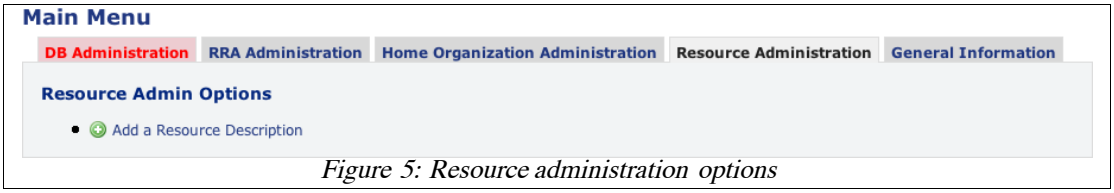

Figure 5: Resource administration options

When you have registered a resource and if it was approved by a Resource Registration Authority (RRA) administrator (see Chapter 4) of your Home Organization, the Resource Administration section looks like in Figure 6.

Figure 6: View withmultiple approved Resource Descriptions

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

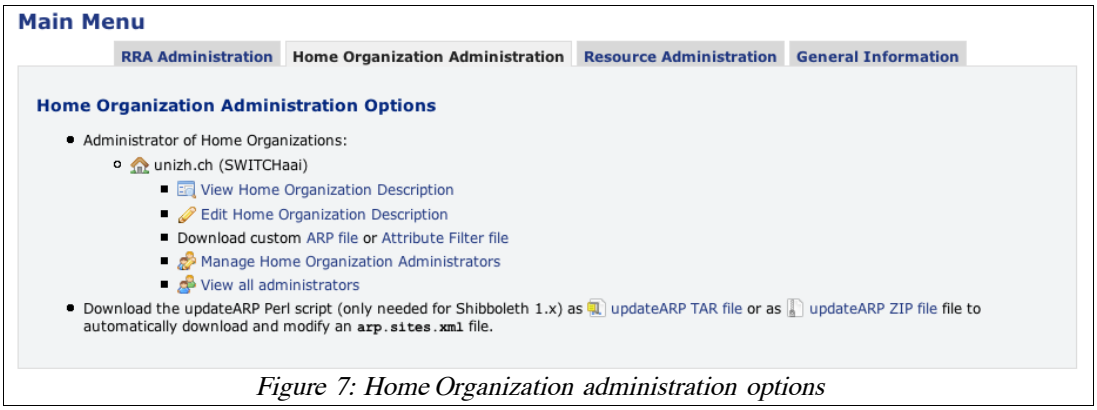

Figure 7: Home Organization administration options

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

Figure 8: Resource Registration Authority administration options

Note: You may not see all of the above administration options because only the options are shown that reflect one's roles. To get the role of a Home Organization administrator, you either have to register a Home Organization or you have to be given that role by another Home Organization administrator. The same applies for a Resource Registration Authority (RRA) administrator. To become a Resource administrator one can register a Resource and the administration rights are received after approval by an RRA administrator. Alternatively, the Resource administration rights also can be granted by another Resource administrator.

4. Roles

Every user in the Resource Registry can have one or more roles that grant certain administration rights. Currently, the following roles are defined:

- Resource administrator
  Registers and manages one or more Resource Descriptions. See Chapter 5.
- Home Organization administrator
  At least one person per Home Organization. Manages Home Organization Description and attribute release settings. See Chapter 6.
- Resource Registration Authority administrator
  At least one person per Home Organization. Approves or rejects new or modified Resource Descriptions. See Chapter 7.

When a user logs in for the first time he has none of the above roles assigned unless he was invited by another administrator. All administrator roles can be transferred to any other user with an AAI account. E.g. the administrator of Home Organization X could make any other user with an AAI account also 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. Two users are invited by manually entering their e-Mail addresses. Clicking on "Apply" results in one user (that already was in the Resource Registry database) being added directly as administrator. The other (unknown) user receives an e-Mail containing an invitation link that will grant him the administration rights.

After entering the two email addresses and submitting the form, one should see a page like in Figure 10. As can be seen, invitations can also be revoked from an invited user, thus invalidating an invitation link.

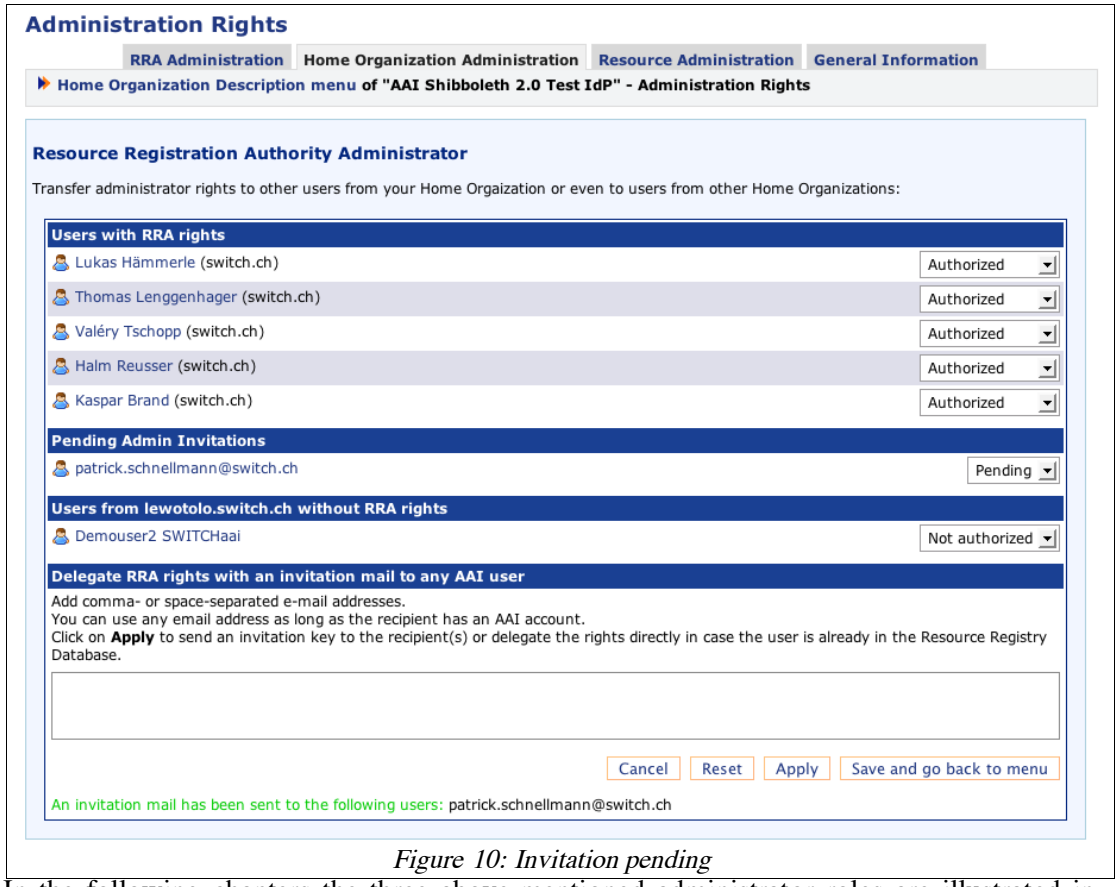

Figure 10: Invitation pending

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

5. 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.

Figure 11: Resource Description sections

As can be seen, the Resource Description contains several sections, each of them should but not all of them have to be completed, and some of them won't require more input because of reasonable default values. 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 2.0 Service Provider, you can use the Shibboleth 2.0 wizard that completes many of the required sections by using the Service Provider's self-generated Metadata. In order to use the wizard, you will have to provide the URL to the Service Provider's Metadata handler URL.

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 you can continue further, which is why they are grayed out beforehand.

In Figure 12 you see an example of this section:

First you have to 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.

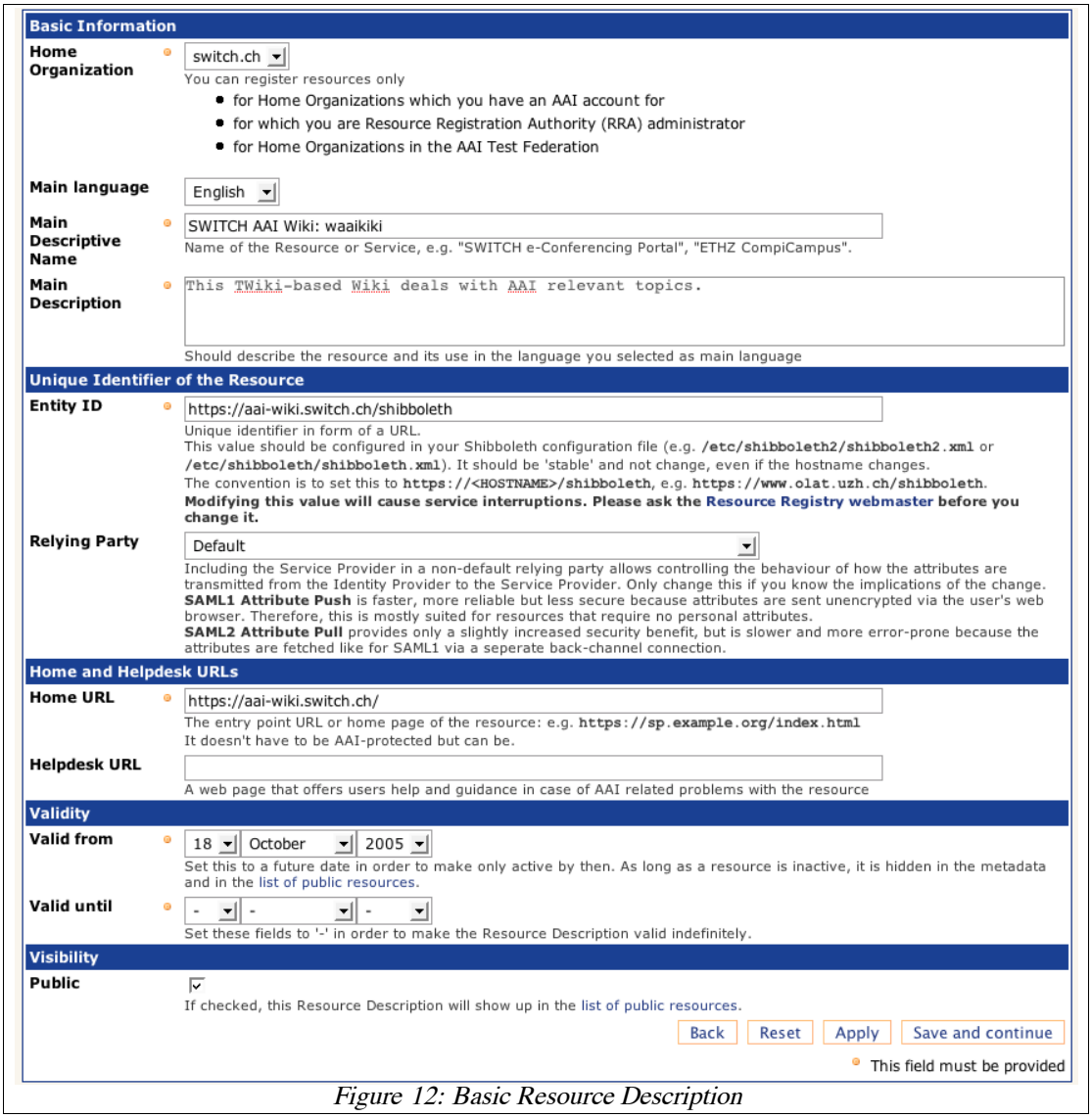

Figure 12: Basic Resource Description

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.

The entityID (formerly known as providerId) is of great importance because it is the identifier for a resource. Be sure to check that you insert the value that you configured or will configure in your *shibboleth.xml* or *shibboleth2.xml* file of your Shibboleth Service Provider if you haven't already.

Warning: Don't change the entityID 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 up to one day where your Resource may not be accessible from some Identity Providers.

Relying Party: Depending in which relying party a resource is, it has to fetch the attributes from an identity provider or it receives the attributes directly via an authenticated user's web browser. For most cases, it is recommended to leave this with the default setting.

Validity: If your resource 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.

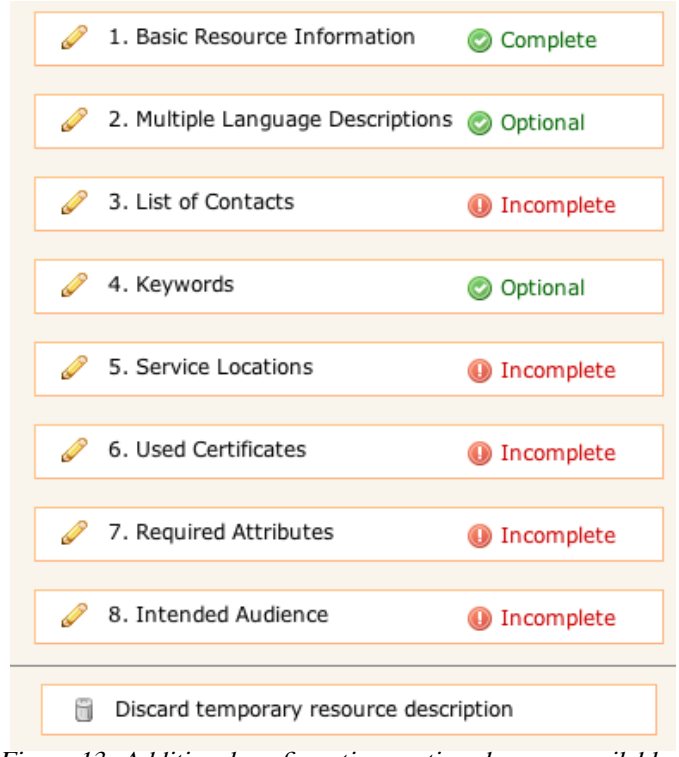

Figure 13: Additional configuration sections become available

Multiple Language Descriptions

The multilingual language descriptions can be used to supply a name and a description for the Resource in multiple languages. These additional descriptions then will be shown on public resource listing web pages provided the visibility is marked public.

List of Contacts

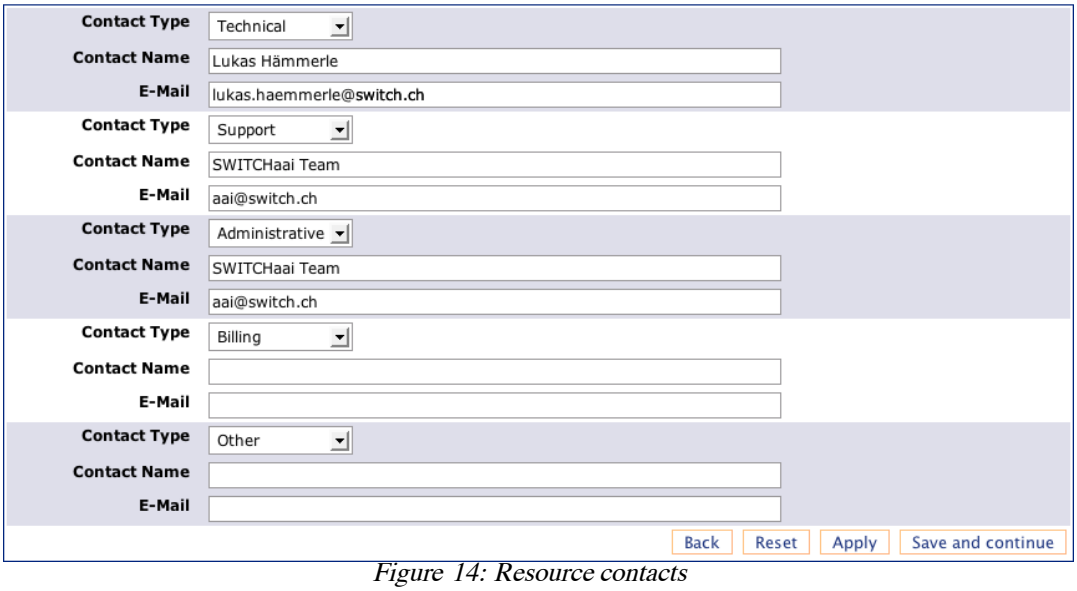

Figure 14: Resource contacts

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. 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.

Keywords

Adding keywords that describe the resource, allows searching for specific resources within the Resource Registry.

Service Locations

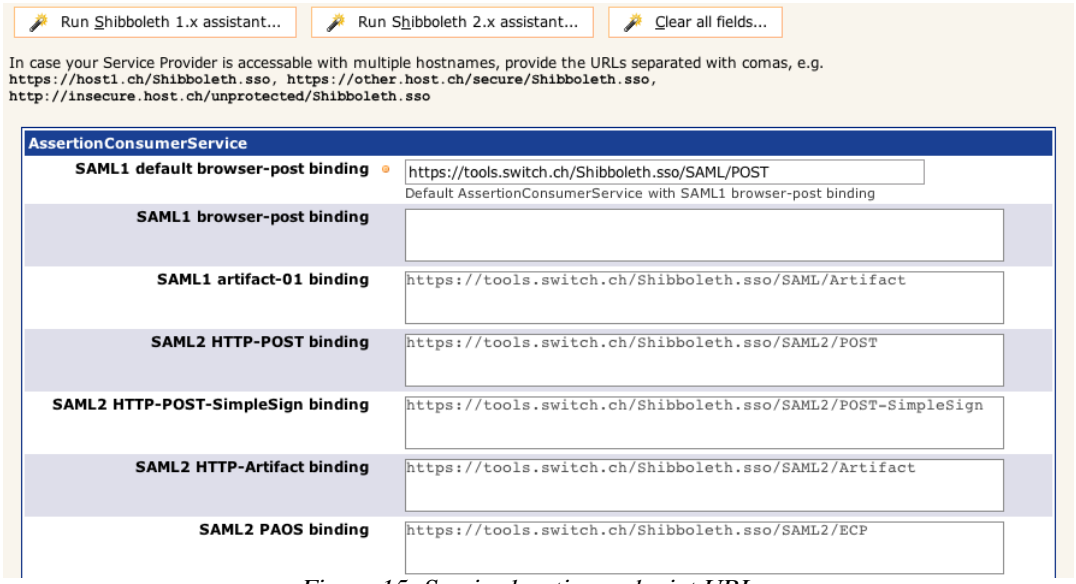

Figure 15: Service location endpoint URLs

In this section, which is shown in Figure 15, you define the SAML endpoint URLs of the

Service Provider. 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.

Warning: As applies to the entityID, changes of the endpoint URLs need to propagate first to all identity providers before they become active.

Note: Although you will see endpoint URLs for multiple SAML 2 Single Logout Services, this feature so far has only been implemented on the Service Provider side. However, in order for it to work as expected the Identity Provider first has to support this feature as well. Unfortunately, Single Logout is a problem that is not very easy to solve, which is why it won't be implemented earlier than Shibboleth 2.2.

Used Certificates

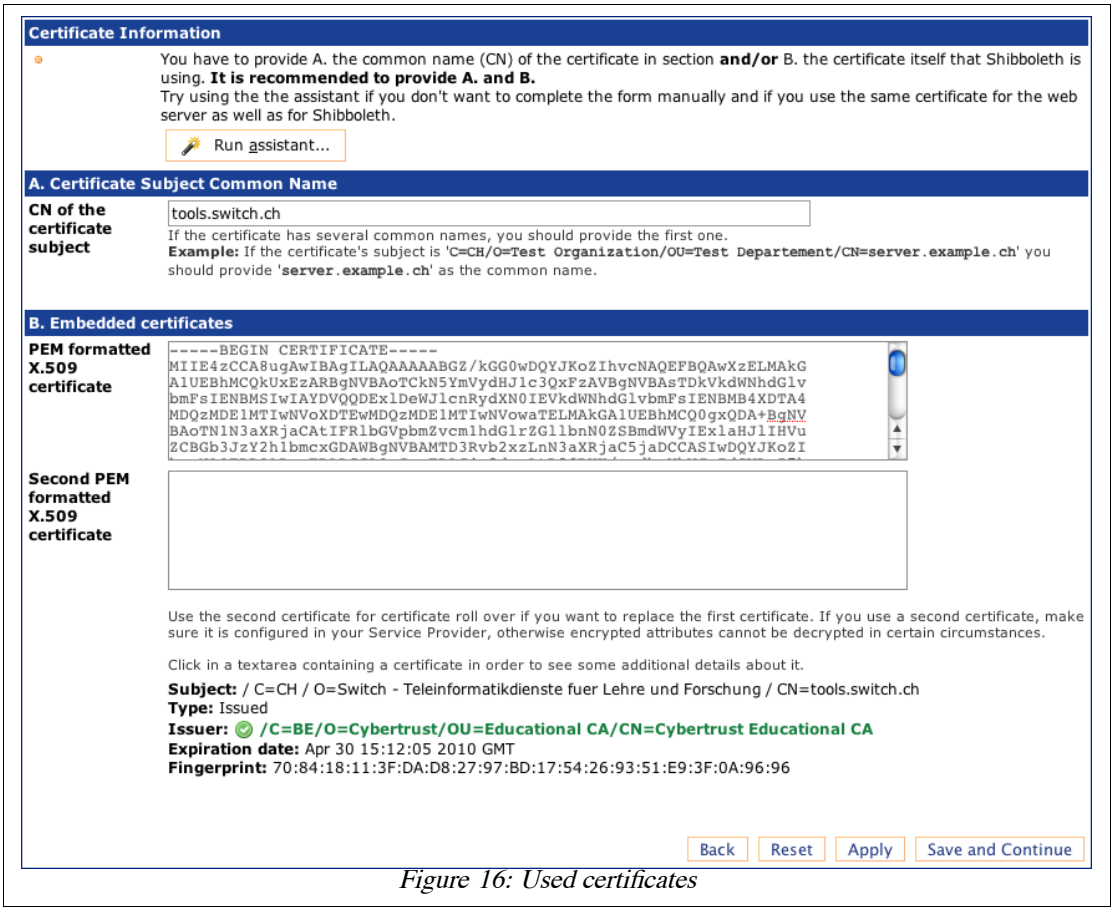

Figure 16: Used certificates

Provide the certificate subject common name and/or the certificate itself, that later on will be used by your Service Provider. Depending on the certificate that you provide, a different way of approving the Resource Description later on is used. As is shown in Figure 16, a second certificate could be added as a backup certificate for roll-over procedures. The order of the two certificates doesn't matter.

Warning: As with the entityID changes of these values need to propagate first to all identity providers before they become active.

Required attributes

The Required attributes section is very important because it affects the Attribute Release Policies (ARP) and attribute filters of all Identity Providers. As shown in Figure 17, you have to declare which attributes your Resource really requires in order to work and which attributes are desired or nice to have.

The attributes on the right-hand side of the page are local attributes, that are not officially supported but can be used by some Home Organizations for internal or bilateral use only.

Note: Please keep in mind that the Swiss Data Protection law states that only absolutely necessary user information shall be requested and processed. This implies that you should declare only attributes as 'required' that are essential for the proper functioning of your Resource.

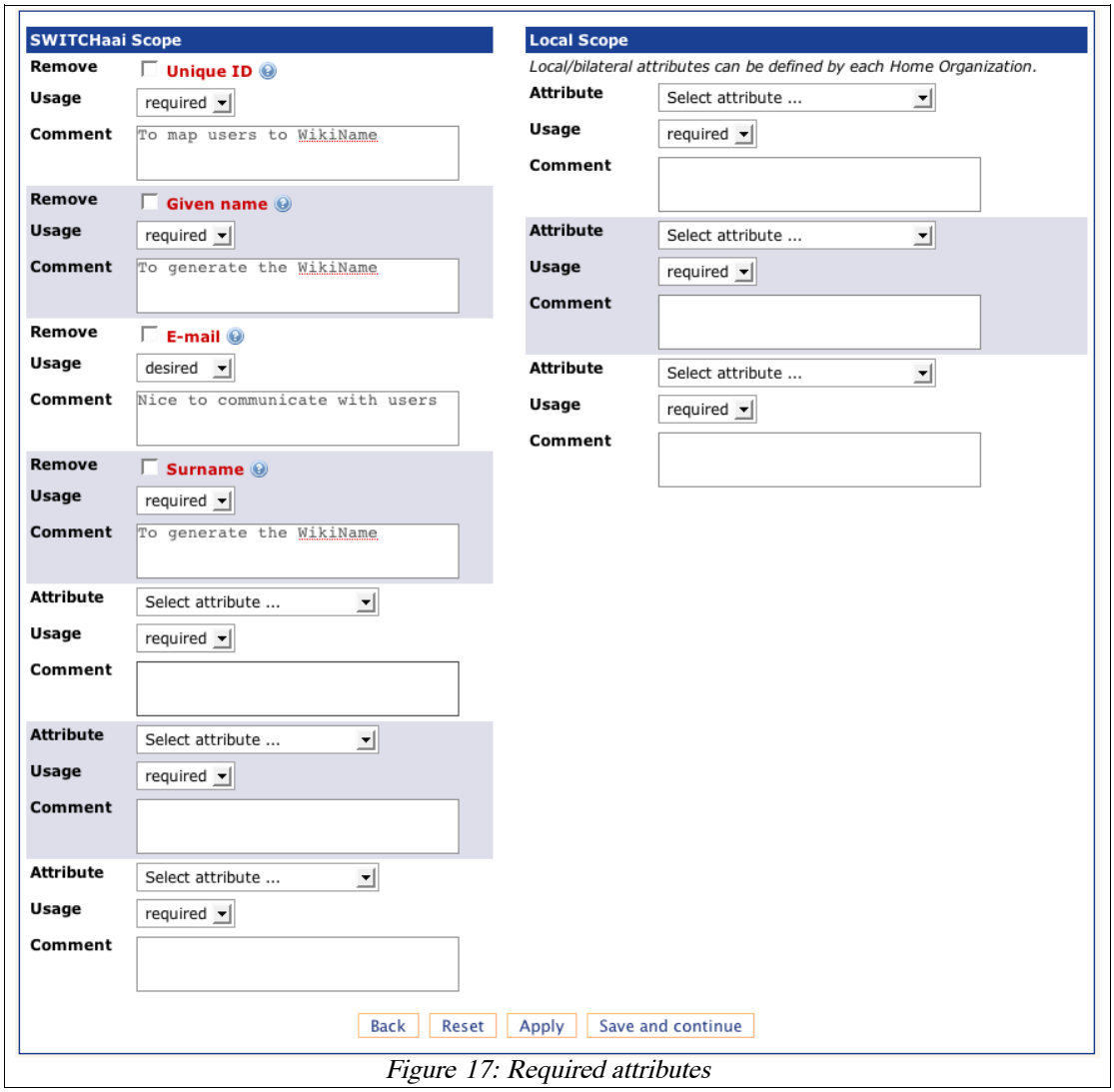

Figure 17: Required attributes

Resource Audience settings

The last section of a Resource Description configures the intended audience settings of the Resource. Assume your Resource is an e-learning tool for medical students. In that case it makes no sense to allow users from a university not offering medical studies to access it. On the other hand, you may want that SWITCH staff members can access the Resource for debugging or development purposes. So, you probably would protect your Resource in the web server's configuration with something like:

```
AuthType shibboleth
ShibRequireSession On
ShibExportAssertion On
require homeOrganizationType university hospital
require homeOrganization switch.ch
```

Since only you know the configuration of your authorization and access rules, it is impossible for Home Organization administrators to know to which Resources their users have access to. Therefore, you should declare the intended audience in the Resource Registry. Please refer to Figure 18 to see how this looks like.

Note: Be accurate but not too restrictive when declaring filling out this form because it also will affect the ARP files and attribute filters of the Identity Providers.

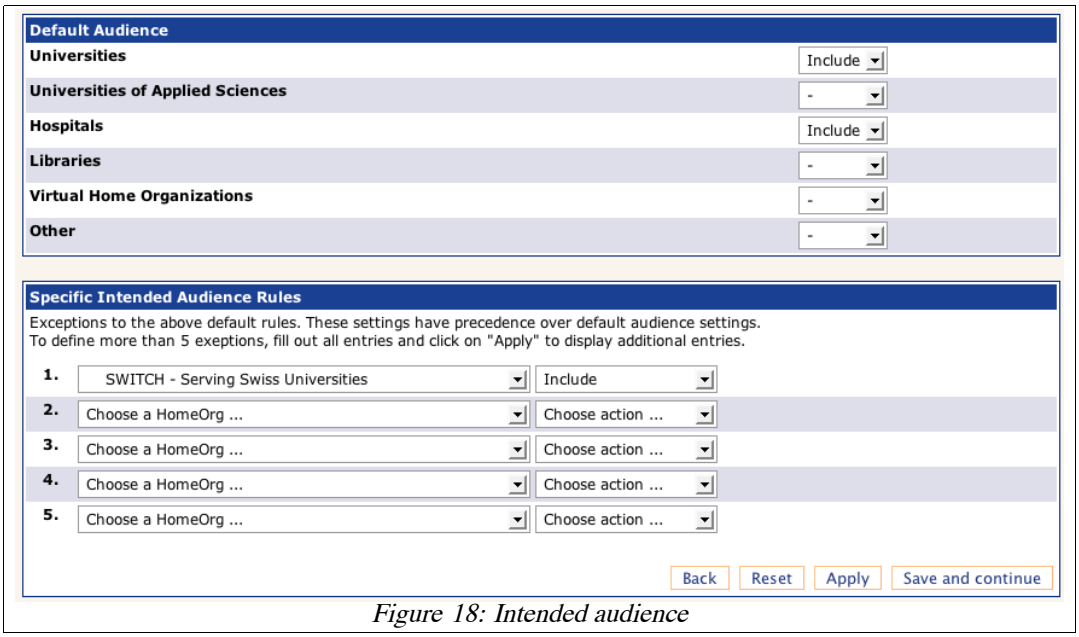

Figure 18: Intended audience

This as well as the "Required Attributes" sections have a direct influence on the ARP and attribute filter files that are generated for each Home Organization. In the ARP/attribute filter files of a Home Organization only Resources appear that may include users of a Home Organization.

Submit Resource Description for Approval

Finally, if all sections were completed, the Resource Description has to be submitted and approved before it becomes active. One of the Resource Registration Authority (RRA) administrators having the rights to approve Resource Descriptions for your Home Organization has to examine and approve it, provided it is complies with the AAI Policies and the Swiss data protection law.

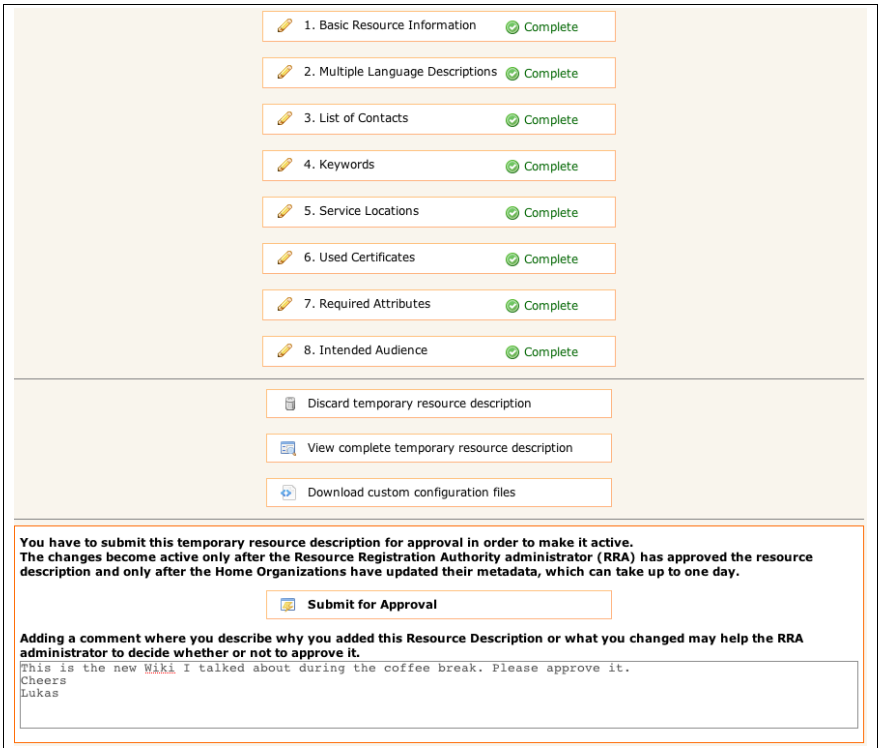

Figure 19: Completed Resource Description

As you can see, there is also a button to discard the temporary Resource Description. This will delete all changes you made but will leave the most recently approved Resource Description intact.

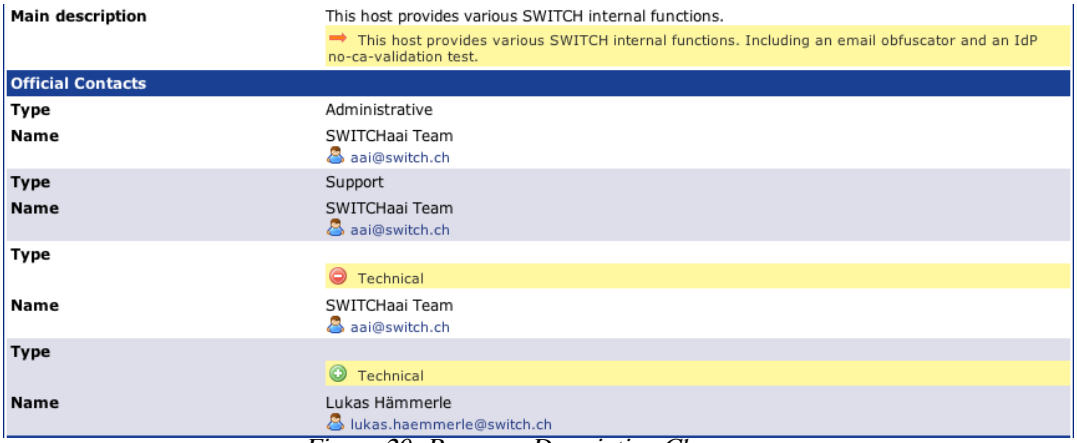

Figure 20: Resource Description Changes

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

Using information available in the Resource Description, one also can download a set of custom-tailored configuration files that can be used to configure the Service Provider. 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 can download either the Service Provider main configuration file (*shibboleth.xml* or *shibboleth2.xml*) or a whole set of configuration files, which are specifically adapted for the SWITCHaai or AAI Test federation.

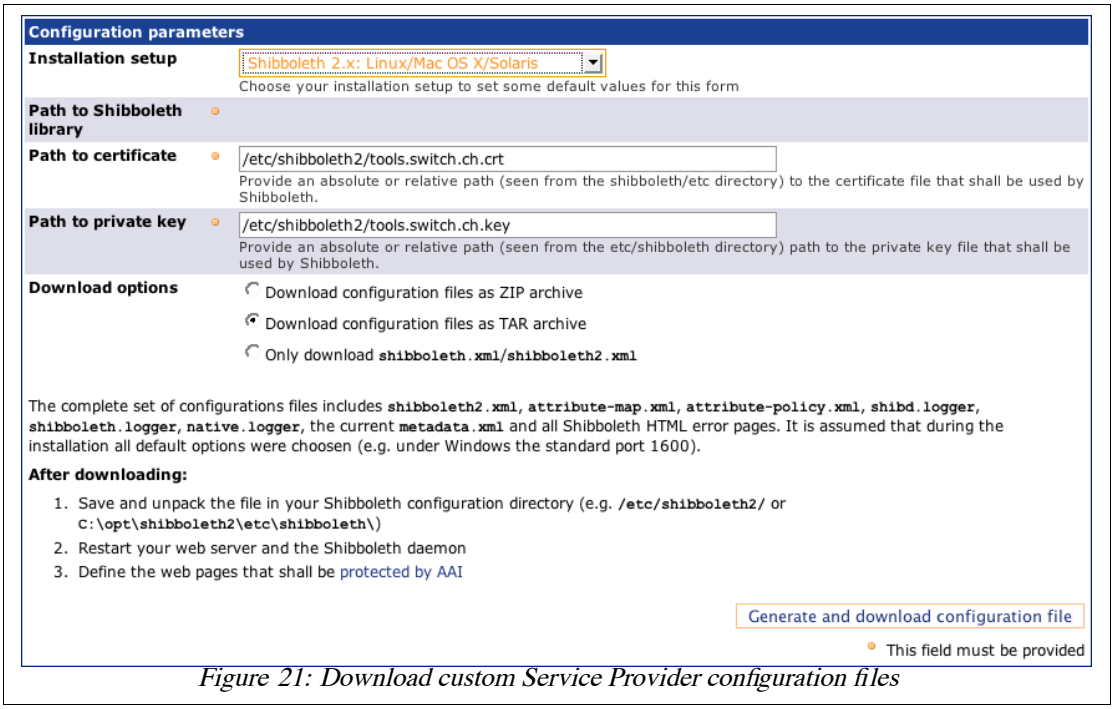

Figure 21: Download custom Service Provider configuration files

If you click on the 'Submit for Approval' button, an e-Mail is sent to all RRA administrators with the request to approve your Resource Description. In the text field you can add a comment for the RRA administrator, e.g. to exactly describe what this Resource is used for or what and why you changed something. This is very useful for the RRA administrator in order to decide whether your changes are justified or not. Therefore, it is strongly recommended to add a comment.

After a Resource has been approved, it is included in the official federation metadata. It also will be included in the attribute release policy/filter files of the Identity Providers. Furthermore, you also become the initial administrator of the Resource Description together with any additional users you invited via email during the Basic Resource description setup. You can transfer this role also to other users later on. All Resource administrators have equal rights, there is no master Resource administrator.

Duties as a Resource administrator

It is essential that all Home Organizations have an up to-date description of all Resources. 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: There will be 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 each full hour if something changed. The Identity Provider should at least update metadata once a day. SWITCH even recommends to update hourly.

Warning: Replacing/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.

For policy reasons every Home Organization needs at least one RRA administrator, whose task is to approve Resource Descriptions. This includes the approval or rejection of

Resource Descriptions. An RRA administrator basically has to check that all Resources that are operated within his Home Organization are operated in compliance with the SWITCHaai Service Agreement (see http://www.switch.ch/aai/agreement/).

6. Home Organization Administrator

When an organization decides to join the SWITCHaai or the AAI Test Federation, it has to set up an Identity Provider on the technical side and it has – in the case of SWITCHaai - to sign the SWITCHaai Service Agreement. When these two steps are completed, the new Home Organization has to be registered with the Resource Registry. In order to do so, the Home Organization administrator has to provide the necessary (technical) information that resources require to communicate with that Home Organization.

Bootstrapping a Home Organization Registration.

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

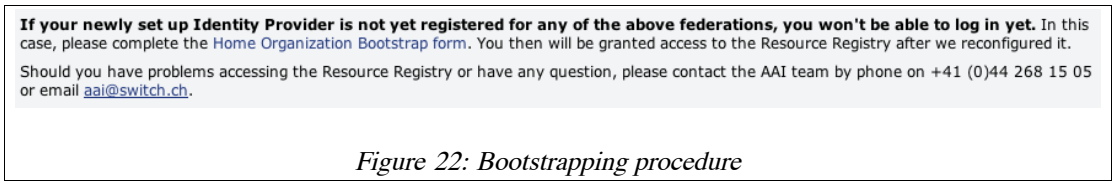

Figure 22: Bootstrapping procedure

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

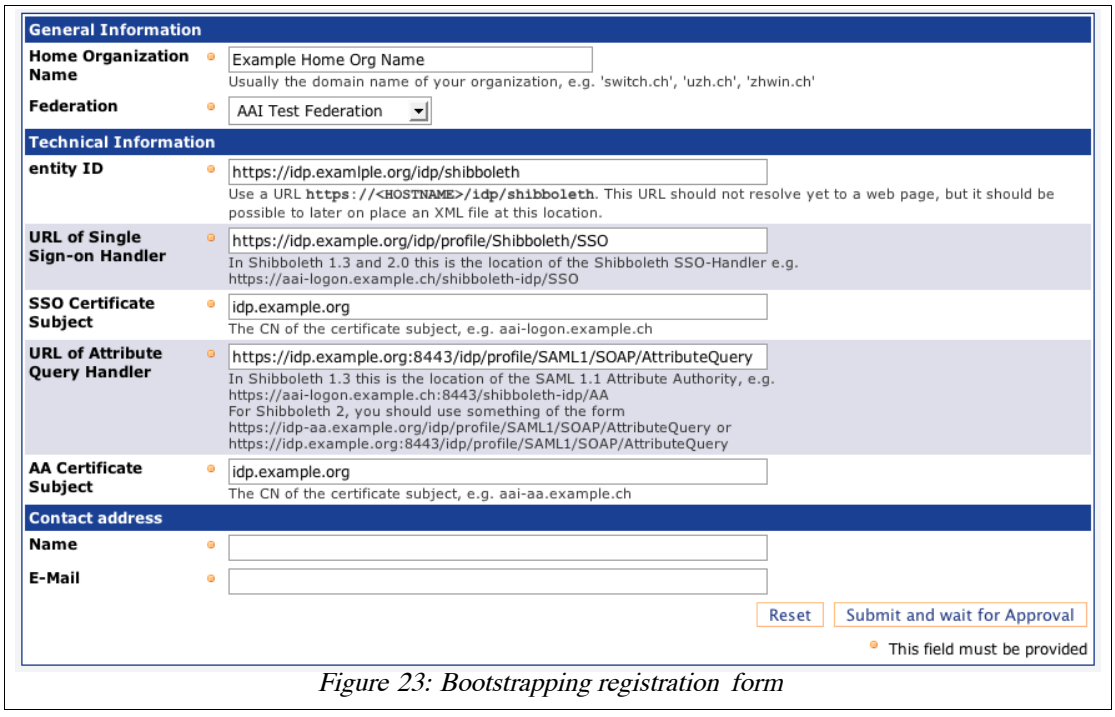

Figure 23: Bootstrapping registration form

Fill in the required information and click on the submit button.

Note: For now, one can only register SAML 1 Identity Providers using this bootstrapping process. After the Home Organization was approved by SWITCH, the Home Organization administrator can upgrade the description to be SAML 2 compliant.

Figure 24: Adding a new Home Organization Description

After submission of the bootstrapping form SWITCH will then approve or reject the new Home Organization within some days. In either case, you will receive a notification email with further instructions. After the Home Organization has been approved, you should be able to access the Resource Registry with an account of the newly set up Identity Provider.

The first time you log in as user from an newly approved Home Organization you will not only receive Home Organization rights as shown in Figure 24 but also Resource Registration Authority administration rights, described in the following Chapter .

You will have multiple options as Home Organization administrator. It is recommended that you edit the Home Organization description again because the first time you access the Resource Registry, only a very basic SAML 1.1 representation is created using data you entered during the Home Organization registration process. Edit the Home Organization Description by clicking the link *"Edit Home Organization Description"* on top of the page. This will bring you to the Home Organization Description menu shown in Figure 25. There, you will have to edit several sections in order to define various aspects of your Home Organization.

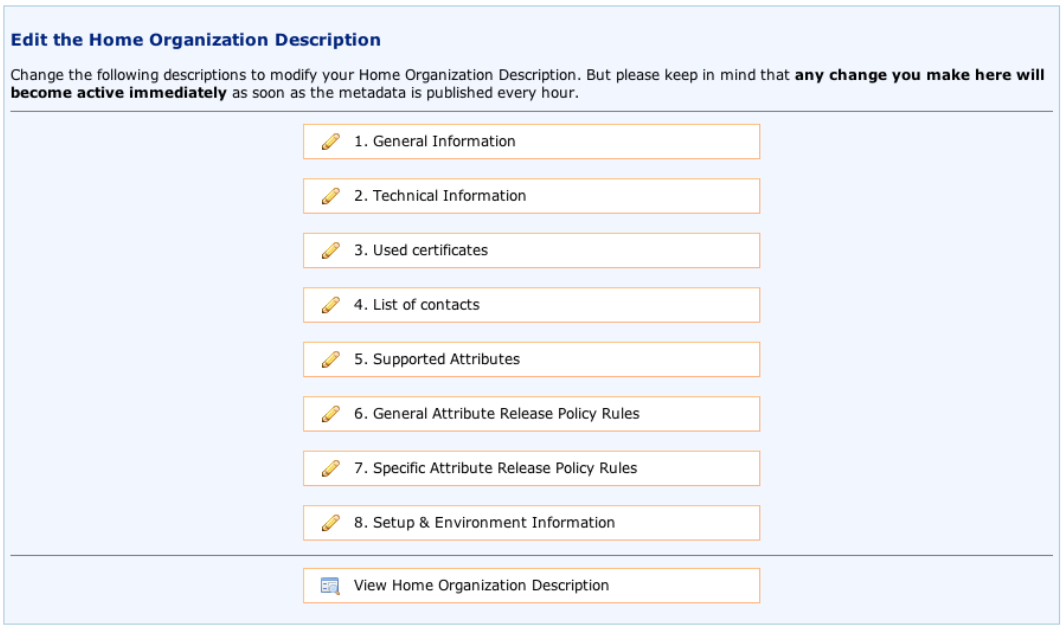

Figure 25: Home Organization Editing Menu

General Information

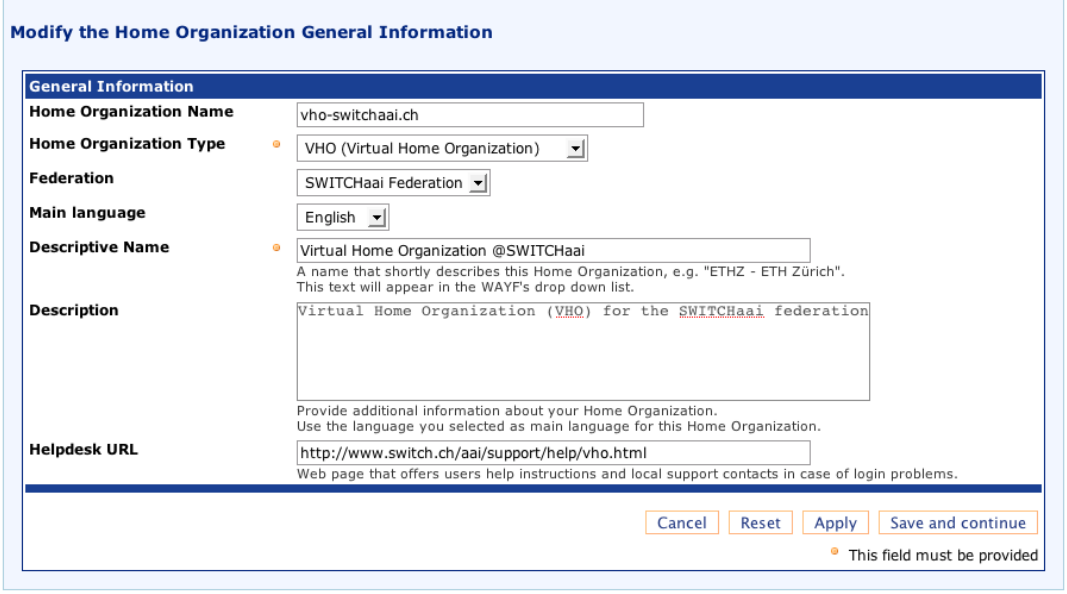

Figure 26: General Information

In the General Information section you first define 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. All of these settings 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.

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. While the *entityID* used to be a URN of the form '*urn:mace:switch.ch:SWITCHaai:some-organization.ch*', we now recommend to use an entityID of the form of a URL (e.g. 'https://some-organization.ch/idp/shibboleth'), similar to the ID of Service Providers. It is highly recommended that the used host name

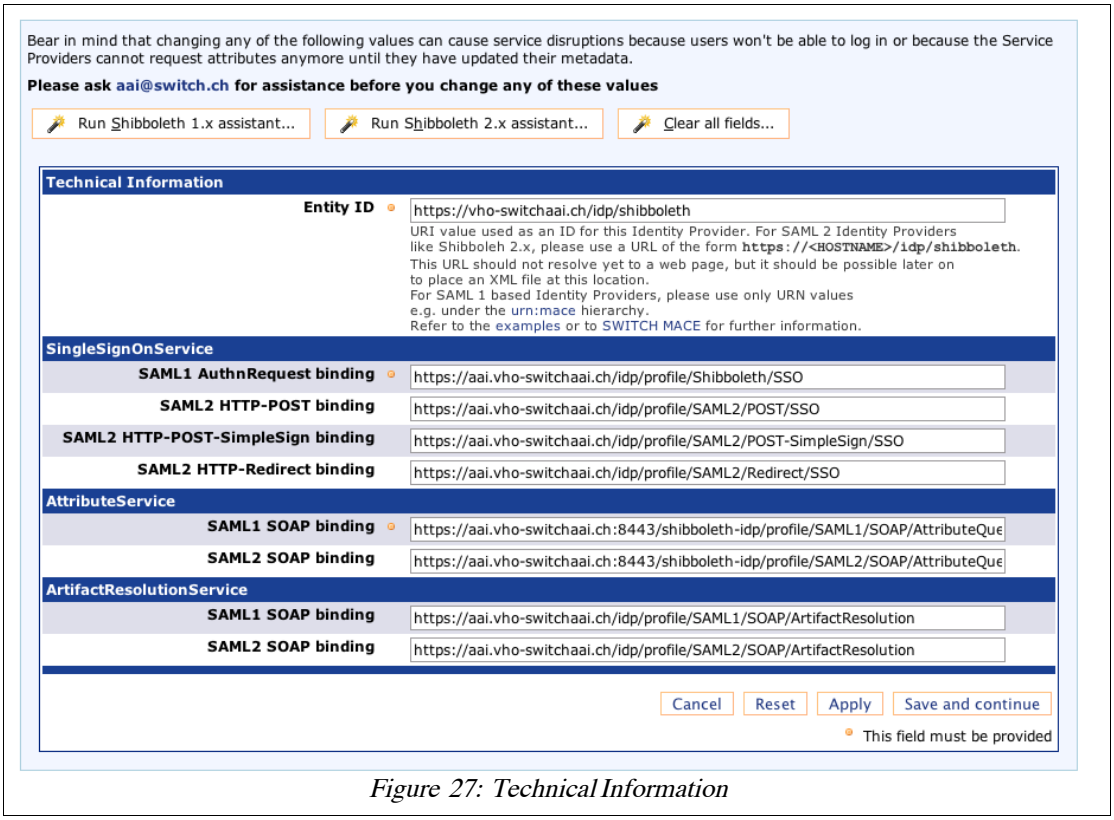

Figure 27: Technical Information

exists because in the future the *entityID* URL may be used to retrieve an entity's metadata. However, before you do this, please consult our migration guide on the AAI web page that will be available shortly after the Identity Provider deployment guide.

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

As for the Identity Provider service endpoints, you may use one of the available assistants in order to complete the form depending on which Identity Provider version you are using. The assistant then will use the root URL you provide to generate the default service locations for the given bindings as shown in Figure 27.

Note: Be sure that for the endpoints for the Attribute Service you are using either another port number (port 8443 is recommended) or a separate host name with it's own IP address. This is essential because on the Attribute Service endpoints, X.509 client authentication has to be enabled while on the other service locations it doesn't need to be enabled. Client authentication can only be reliably enabled on a separate IP or port.

Warning: Modifying any properties in the Technical Information section has to be done very carefully because these changes will take some time to propagate to all Service Providers. The propagation via the metadata may take up several days during which your users may not able to access Resources whose metadata has not yet been updated. If in doubt about a property you want to change, please send an email to aai@switch.ch for assistance.

Used Certificates

In the Used Certificates sections you have to provide the subject common names or the certificates themselves that are used by Shibboleth and the web server running the Identity Provider.

It is recommended that you provide subject common name as well as the certificates themselves although one of them would be sufficient to provide. Use the assistant in order to complete the form for you. As the name implies, the backup certificates could be used in case of emergency fall back certificates. This could be useful if your server was compromised and you have to replace the main certificates quickly. In such a case you

would just replace the certificates used by your web server and by Shibboleth with the backup certificates.

The Resource Registry will expire certificates if they have been used for more than 3 years even though the certificates validity may be longer. Before this is going to happen, you will however receive several notification emails announcing this procedure.

Certificate rollover must be done carefully. You have to make sure that the new certificate has been contained in the metadata for at least two days before the Service Provider actually can use this new certificate. Please refer to the Service Provider deployment guides at http://www.switch.ch/aai/support/serviceproviders/ on how to carry out the certificate rollover.

Note: If you want to make use of the backup certificates, make sure to add them in the Resource Registry for your Home Organization Description but don't actually store the private keys on the Identity Provider's host. Keep them in a safe location so that you can be sure they cannot be compromised as well in case your Identity Provider server should be compromised.

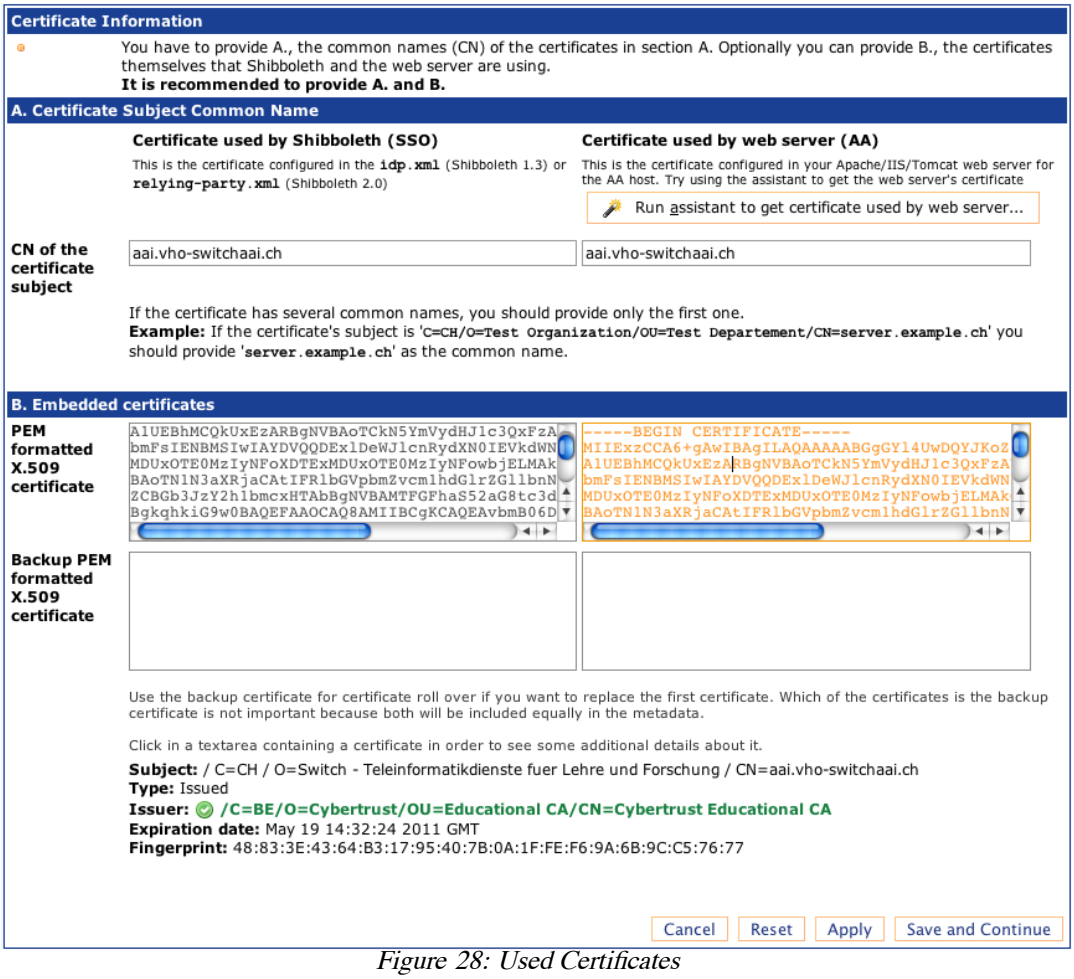

Figure 28: Used Certificates

List of Contacts

As for every Service Provider, one should add contact persons for a Home Organization that can be contacted in case of support or technical inquiries. Although it is not mandatory to provide contact persons, it is strongly recommended to do so. Support and technical contact names and addresses 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.

Supported Attributes

As the name suggests, the Supported Attributes section's purpose is to declare the attributes an Identity Provider can release. As depicted in Figure 29, on the left-hand side, one has to check the official SWITCHaai attributes that can be released by the Identity Provider. On the right-hand side, there are the local/bilateral attributes that are either used only within the same organization or within a small subset of organizations on the basis of a bilateral agreement.

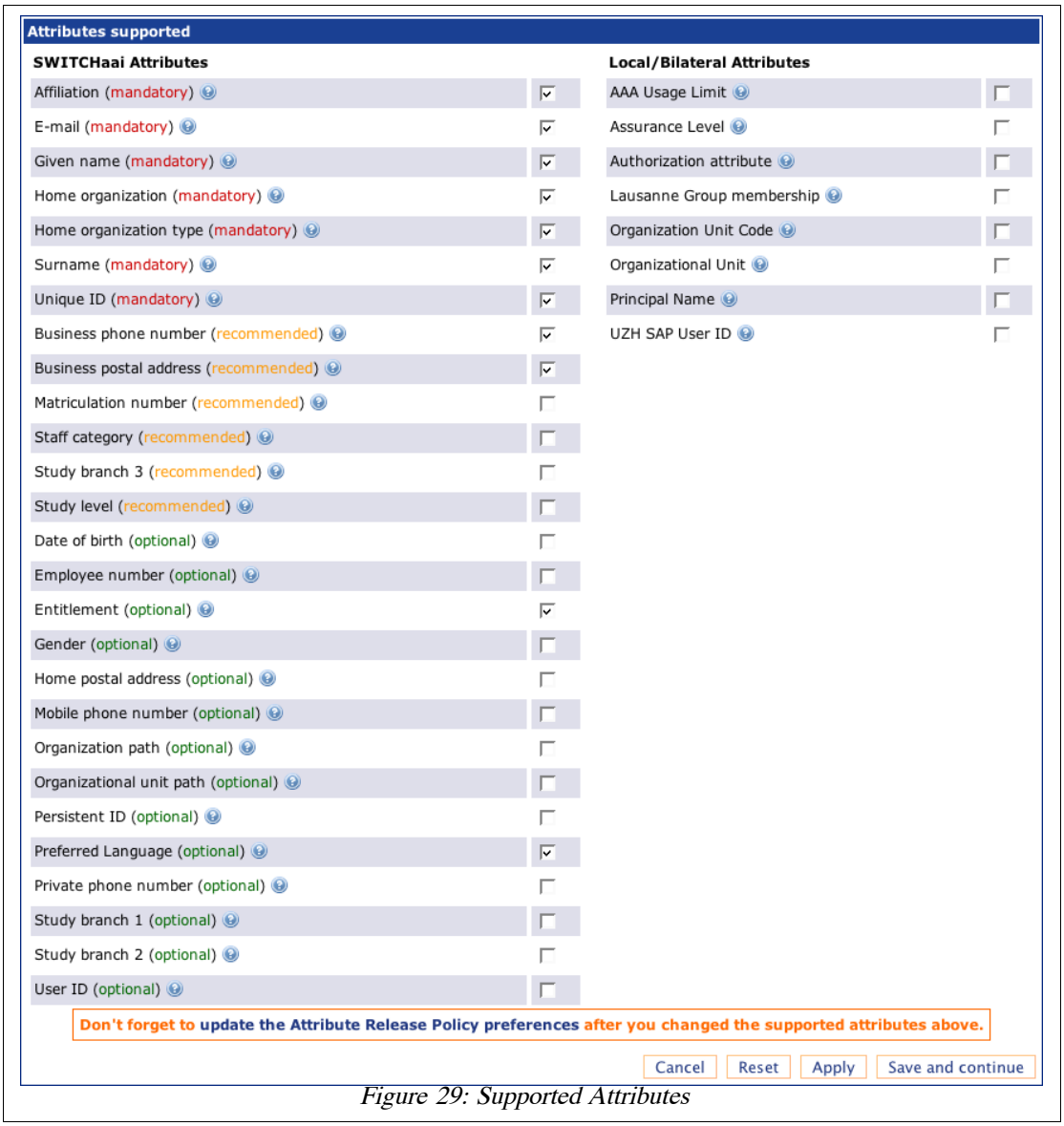

Figure 29: Supported Attributes

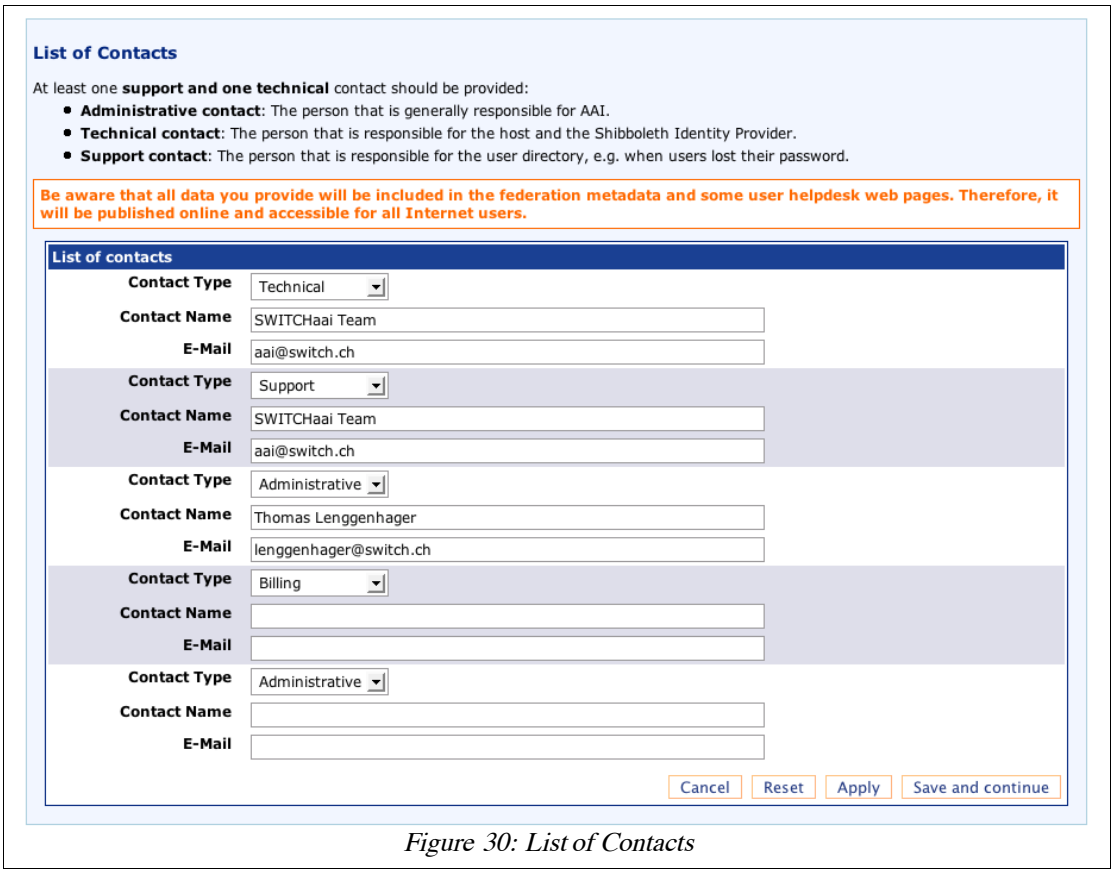

Figure 30: List of Contacts

According to the AAI Attribute Specification (see http://www.switch.ch/aai/attributes) your Identity Provider must be able to release at least the red (mandatory) attributes. However, the attributes will only be released if needed and generally only a small subset of attributes will be released to a resource.

General Attribute Release Policy

In the General Attribute Release Policy a Home Organization administrator defines the general behavior regarding the release of attributes that will be reflected in the generated arp.site.xml (Shibboleth 1.3) or attribute-filter.xml (Shibboleth 2.0) files. Basically, one defines whether an attribute shall be released in case a Resource administrator defines it as 'required' or as 'desired' as shown in Figure 30.

Note: Only these attributes are shown which can be released by an 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.

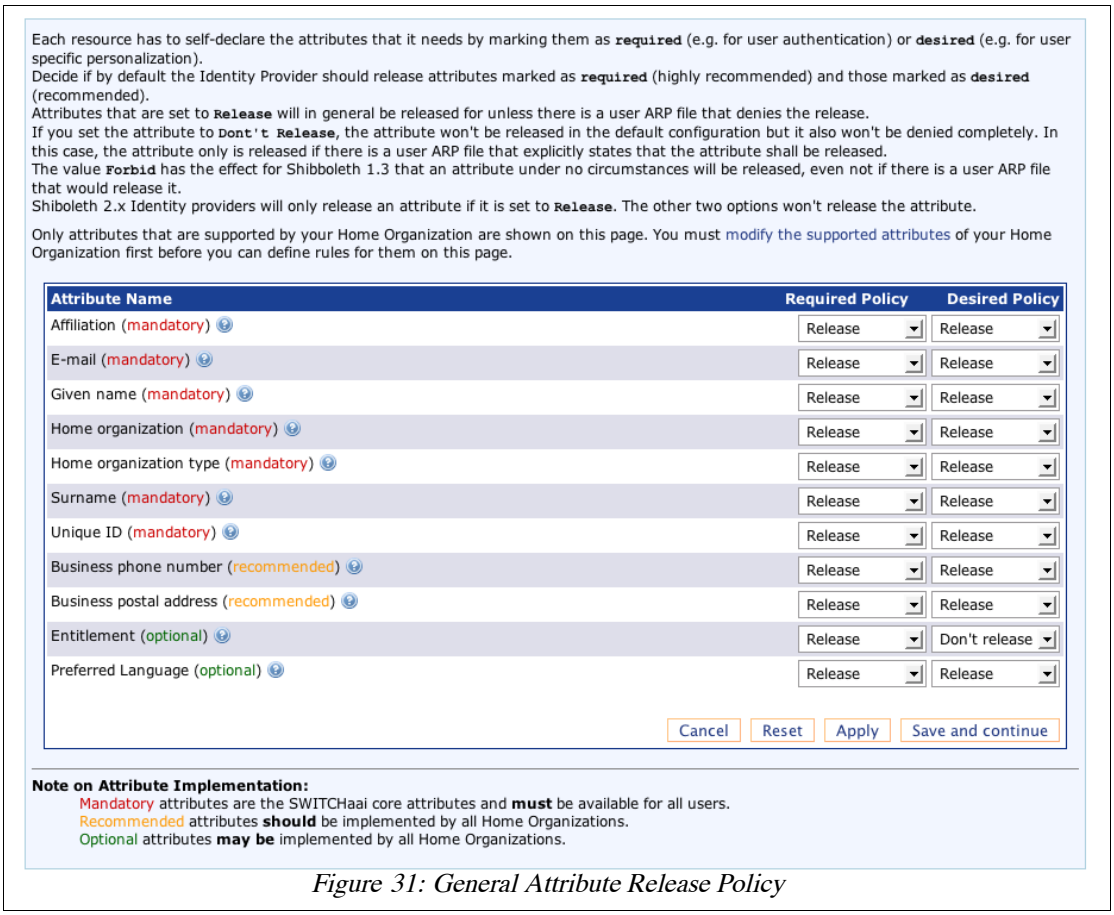

Figure 31: General Attribute Release Policy

Specific Attribute Release Policy

While you could define a very general attribute release policy in the previous section, you can define very fine-grained rules in the Specific Attribute Release Policy section. As is shown in Figure 32, one can create custom-tailored rules for each Resource. Either a Resource can be totally excluded from the attribute-filter or one can specify attributes that shall not be released even though they are required or desired by the Resource administrator. For every Resource only the required and desired attributes are shown. If no specific rule is created for an attribute, the general attribute release policy will be applied.

Excluding a Resource from the attribute-filter.xml file is useful if an Identity Provider administrator wants 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. These rules can base the release decision on almost any criteria that one can possibly think of.

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

Note: The Specific Attribute Policy can only be used in conjunction with a Shibboleth 2.0 Identity Provider because it only will affect the attribute-filter.xml files generated by the Resource Registry. In case of Shibboleth 1.3, one can define specific rules for the arp.site.xml file using the updateARP tool.

Home Organization Setup & Environment

The last Home Organization section is the '*Setup & Environment*' section, which is shown in Figure 33. It is purely informational and solely serves the SWITCHaai team members as well as other Home Organization administrators to examine how different Identity Providers are set up. This allows to compare similar setups in case of problems or planning setup changes.

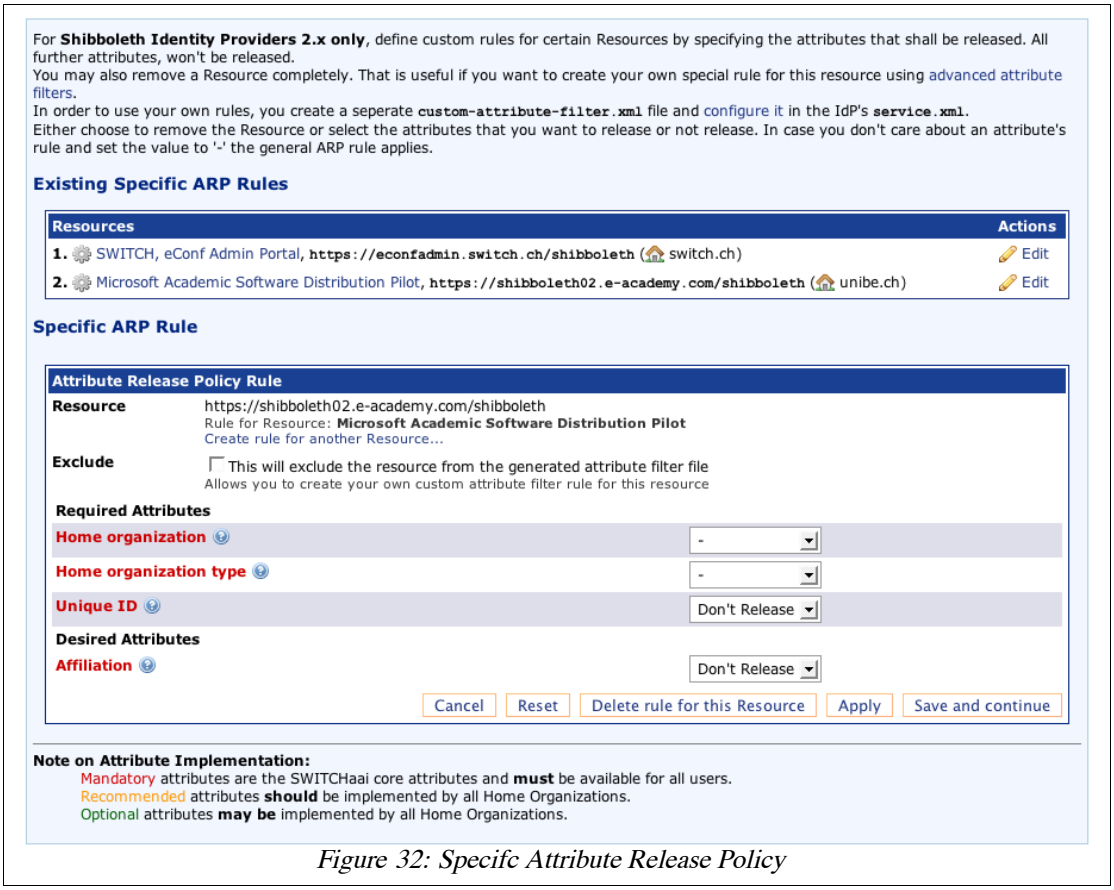

Figure 32: Specifc Attribute Release Policy

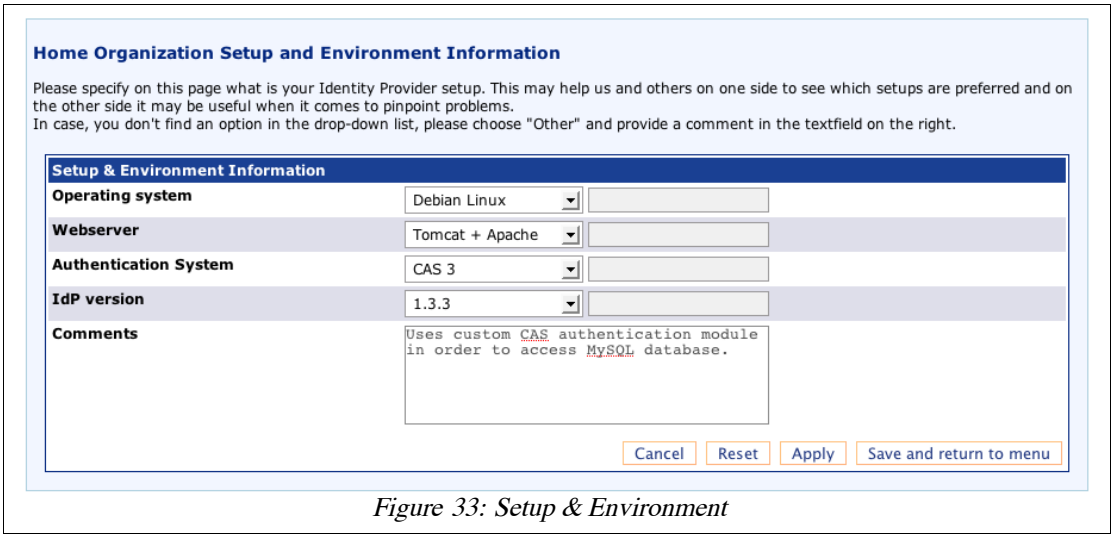

Figure 33: Setup & Environment

Duties as Home Organization administrator

Since 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 consult aai@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. For Shibboleth 1.3 there is a metadatarefresh script that can be used to automate it. We recommend to run this tool at least once a day. For Shibboleth 2.x please use the built-in metadata provider that reads the metadata from a URL and stores a backup copy locally. For Shibboleth 2.0 it is recommended to update metadata more frequently because the file only will be downloaded if it changed.

  Note: There will be a delay for changes to be applied, due to the delay for metadata refresh at the Service Providers.

- Regularly update your 1.3 Identity Provider's arp.site.xm file. SWITCH has developed a tool called updateARP that downloads your custom-tailored ARP file and can even more customize it according to rules you can set in aconfiguration. For a 2.x Identity Provider, please use the built-in attribute-filter provider that reads the file from a URL.

  Note: You don't have to restart your Identity Provider after updating the metadata or the ARP file. However, it takes about a minute until the Identity Provider notices that these files changed.

7. Resource Registration Authority Administrator

Duties as Resource Registration Authority (RRA) administrator

For policy reasons every Home Organization requires at least one RRA administrator, whose task it is to decide whether to approve or reject a submitted Resource Descriptions. Therefore, an RRA administrator has to examine and make sure that all Resources registered for his Home Organization are operated in compliance with the SWITCHaai Service Agreement (see http://www.switch.ch/aai/agreement/). In particular the following requirements have to be checked carefully:

- The person that created or modified a Resource Description is allowed to operate an AAI Resource in the name of your Home Organization.
- Every Resource has at least one valid contact person for administrative, technical and support inquiries.
- The Resource 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 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 prior to approve it. The Resource Registry will in some situations show 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 receive a notification e-Mail. After login, an RRA administrator will notice the Resource Descriptions that need to be approved in the Resource Registration tab as shown in Figure 34.

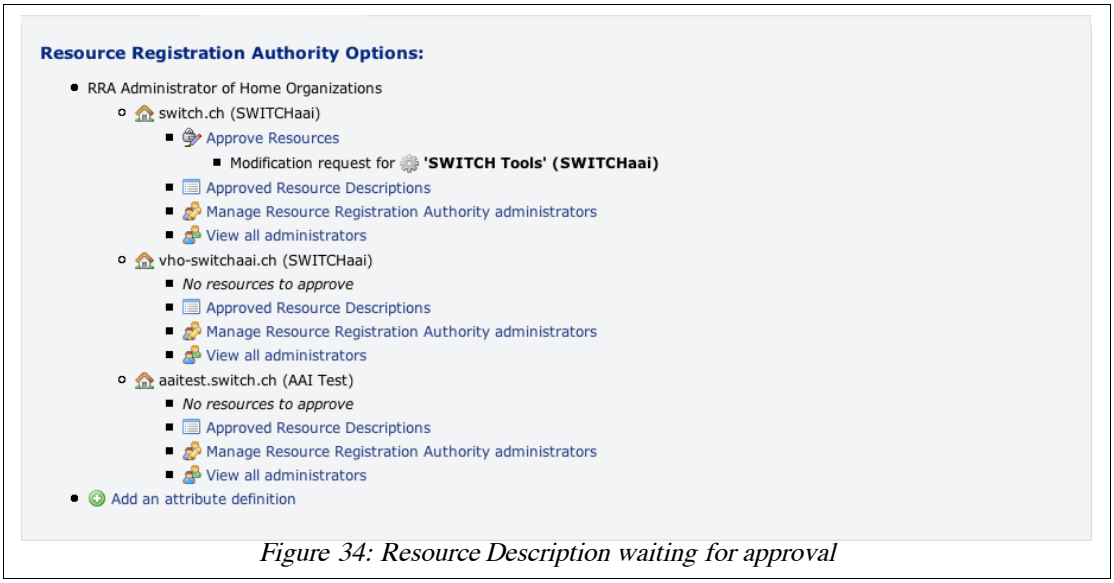

Figure 34: Resource Description waiting for approval

Clicking the *"Approve Resources"* link then leads to a page like in Figure 35.

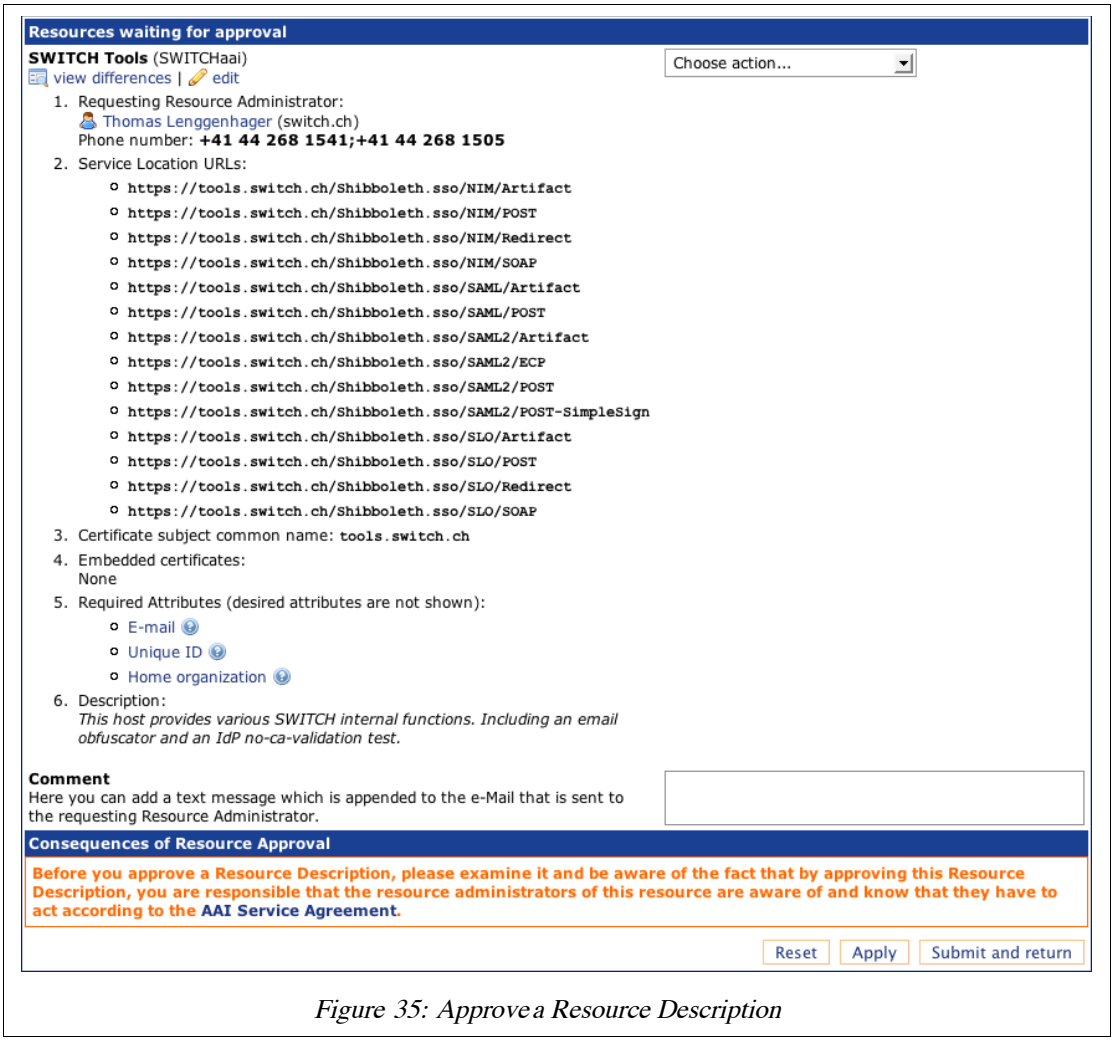

Figure 35: Approve a Resource Description

Figure 35 shows a single Resource Description to approve or reject. Clicking on '*View changes*' an RRA administrator can inspect the changes before approving it, as is shown in Figure 20.

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

Miscellaneous

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

Resource Registry data usage

As was pointed out, data stored in the Resource Registry doesn't only serve the management of the SWITCH federations but data also is used for informational purposes. In particular, the following web pages directly access data from the Resource Registry:

- http://www.switch.ch/aai/help
- http://www.switch.ch/aai/participants/allresources.html
- http://www.switch.ch/aai/participants/allhomeorgs.html
- http://www.switch.ch/aai/support/metadata/monitoring.php

If a Resource Description is changed, this is immediately reflected on the above web pages as soon as the change gets approved.

Facts about the Resource Registry

The Resource Registry was programmed in PHP5 and requires the PEAR QuickForm libraries as well as a MySQL database. For X.509 related functions openssl also has to be installed.

All development work has been done by SWITCH. The code is protected by a BSD-like license and can be requested by sending an email to aai@switch.ch.