Resource Registry Updates

A look through the keyhole at upcoming changes

Lukas Hämmerle
lukas.haemmerle@switch.ch

Berne, 13. August 2014

Disclaimer

- Following Updates in Resource Registry will become active only end of August

- Implementation still subject to changes

- Feedback on Resource Registry in general is welcome

Upcoming Changes in Resource Registry

- In Resource Administration:

  SP

  – Section "6. Requested Attributes"
  – Section "7. Intended Audience and Interfederation"

- In Home Organisation Administration:

  IDP

  – Section "7. Attribute Release Settings"

- And some smaller changes not worth mentioning

Requested Attributes I

Requested Attributes

Specify on this page the user attributes which are **required** or **desired** by the resource. A Resource receives at maximum those attributes that it requests. It is, however, not guaranteed that a Resource always receives all attributes it requests because not all attributes are implemented by all organisations and sometimes organisations decide not to release certain attributes about their users.

General Recommendations

A Resource MUST request only the attributes that are adequate, relevant and not excessive to the Resoruce. One of the key principles of the data protection law is: **Request as few attributes as necessary!** Consequently, only declare attributes as required if they are essential for the operation of the resource. Declare attributes as desired if they are "nice-to-have".

- Show recommendations for Resources accessed primarily by SWITCHaai users
- Show recommendations for interfederation Resources als accessed by non-SWITCHaai users

Common Attribute Sets

Select in the list an attribute set to mark frequently requested sets of attributes.

SWITCHaai Attributes
  Non-identifiable SWITCHaai Core attributes
  SWITCHaai Core attributes
  All SWITCHaai attributes
eduGAIN attributes recommended to implement for Identity Provider
  Non-identifiable recommended attributes
  All recommended attributes
REFEDS Research & Scholarship Attributes
  Minimal R&S attributes
  All R&S attributes

🗑 Remove all attributes

Recommendations for SWITCHaai / Interfederation use-cases

Assistant to mark attributes of popular attribute sets

Requested Attributes II

New categorization of attributes: SWITCHaai Core, Standardized, Other, Local/Bilateral

Marked attribute. In this case non-identifying SWITCHaai core attributes

Attributes

Select for each attribute whether it is **required** or **desired** by the Resource. Also describe in the text field (in english) why and for what reason an attribute is required or desired. This helps Home Organization administrators managing their attribute release policies.

SWITCHaai Core Attributes

SWITCHaai Core attributes **must be** available for all users. Therefore, a Home Organisation must be able to release these attributes. However, the Home Organisation's attribute release policy controls whether or not an attribute is released to a Resource.

Attribute	Coverage	Necessity	Declare why the resource needs it
Affiliation eduPersonAffiliation	▮▮▮▮	Required	To test whether this attribute is available
E-mail email	▮▮▮▮	Required	
Given name givenName	▮▮▮▮	–	
Home organization swissEduPersonHomeOrganization	▮▮▮▮	Required	
Home organization type swissEduPersonHomeOrganizationType	▮▮▮▮	Required	
Surname surname	▮▮▮▮	–	
Targeted ID/Persistent ID eduPersonTargetedID	▮▮▮▮	Required	To test whether this attribute is available
Unique ID swissEduPersonUniqueID	▮▮▮▮	–	

How many organisations can reelease the attribute

© 2014 SWITCH

5

Intended Audience and Interfederation

GÉANT Data Protection Code of Conduct (CoCo)

☐ Commit to the GÉANT Data Protection Code of Conduct (CoCo)

The GÉANT Data Protection Code of Conduct (CoCo) contains a set of data privacy rules that the operator of a service can commit to. The effect is that Identity Providers from abroad are more likely to release user attributes to this service because the commitment to the CoCo enhances the trust that users data is processed with care.

Supporting the GÉANT Data Protection Code of Conduct should not be a problem for most Swiss services because the rules mentioned in the CoCo are also covered in the Swiss data privacy law.

SWITCH recommendeds to commit to the GÉANT Data Protection Code of Conduct for Interfederation services.

⚠ **Currently, you cannot commit to the GÉANT Data Protection Code of Conduct because the following requirement is not met: No English privacy URL provided! In order to be compliant with the GÉANT Data Protection Code of Conduct, a URL to an English privacy policy page must be provided for this Resource. Please add a Privacy Statement URL that meets the requirements and then return to this page to enable the CoCo.**

Support for entity categories

REFEDS Research & Scholarship (R&S)

☐ Apply for to the REFEDS Research & Scholarship (R&S)

The REFEDS R&S (R&S) entity category is applicable to resources that "support research and scholarship interaction, collaboration or management as an essential component". Candidates for the Research and Scholarship (R&S) Category are Resources that support research and scholarship interaction, collaboration or management as their primary activity. This excludes services for access to licensed content such as e-journals. If a Resource is in the R&S entity category, Identity Providers from higher education and research insitutions abroad are more likely to release user attributes to it.

SWITCH recommendeds in particular to Interfederation-enabled services to apply for the R&S category.

⚠ **Currently, you cannot apply for the REFEDS R&S category because the following requirement is not met: The service must have an information URL to get in the R&S category. Please set an Information URL for this resource and then return to this page.**

Interactive warning messages if entity category requirements are not met

Attribute Release I

Entity Categories policies influence IdP attribute release:

1. **Default Policies**
   General release rules for individual attributes, depending on whether they are required or desired.
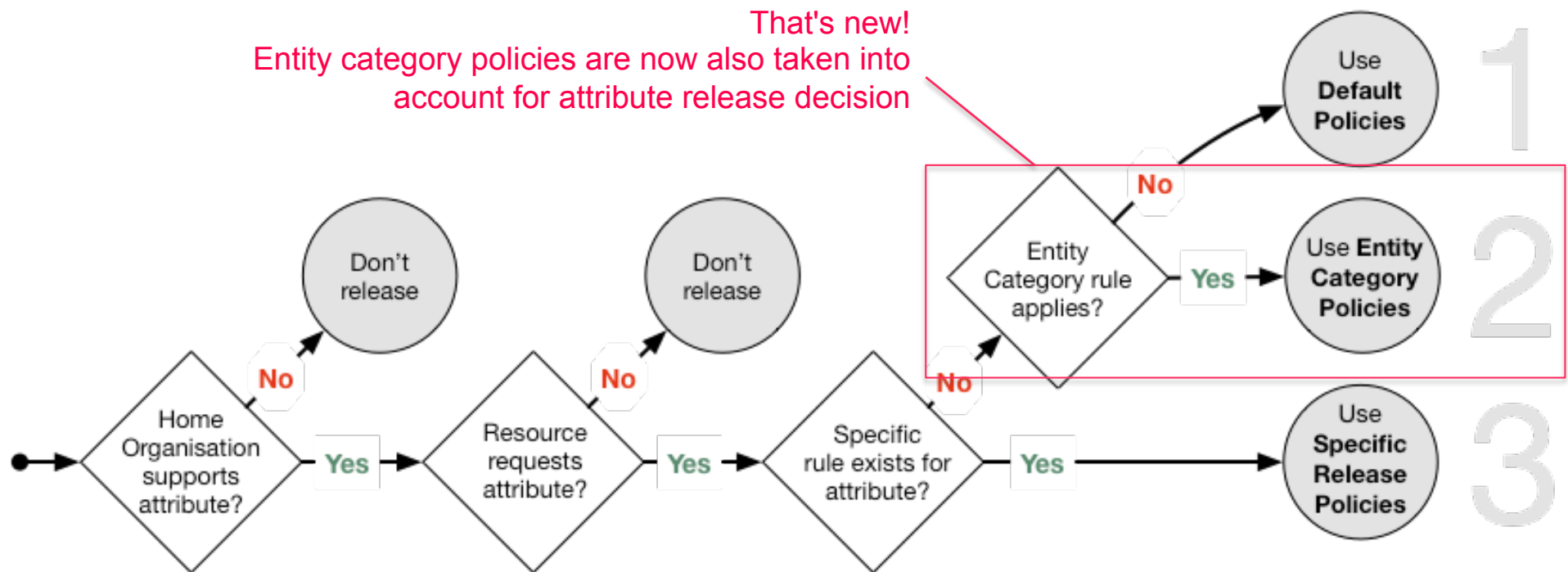
2. **Entity Category Policies**
   Release rules that apply if Resources belong to a certain entity

3. **Resource Specific Policies**
   Release rules for specific Resources to create rules that always have precedence

Attribute Release II

Decision tree of new attribute release

That's new!
Entity category policies are now also taken into account for attribute release decision

Attribute Release III

New policy section for entity category-based attribute release

2. Entity Category Policies

Entity Category Policies apply whenever a Resource claims to meet the category's requirements. The claim is part of the Service Provider's metadata. Entity Category Policies have higher priority than the default release policies for individual attributes. However, they have lower priority then the Resource Specific Attribute Release Policy rules.
Together with a user attribute release consent module (i.e. uApprove), attribute release based on the entity categories below should provide enough confidence from a data protection point of view to release the requested attributes also to Interfederation-enabled resources abroad.

GÉANT Data Protection Code of Conduct (CoCo)
Resources in the GÉANT Data Protection Code of Conduct (CoCo) entity category declare to respect the CoCo's behavioral rules and that they are located in either EU/EEA or a country with adequate data protection (e.g. Switzerland).

The CoCo was created by GÉANT, the international research infrastructure project that also created and operates eduGAIN and eduroam. SWITCH contributes to GÉANT.

| Release required attributes (default) |
| Release required attributes (default) |
| Release all required and desired attributes |

an attribute is only released if its release scope is neither **nobody** nor **my organisation's resources**. Is the attribute release for this entity category disabled, only the default and specific release rules apply.

REFEDS Research & Scholarship (R&S)
Resources in the REFEDS Research & Scholarship (R&S) category "enhance the research and scholarship activities" and are of benefit to R&S user communities.

REFEDS specified this entity category. It is the interest group of research and education identity federations world-wide. SWITCH contributes to REFEDS.

| Release minimal set of R&S attributes (default) |

The minimal R&S attribute set includes the attributes:

- **Principal name**
- **E-mail**
- **Name** (**Given name** and **surname** or alternatively **Display name**)

The complete set with all R&S attributes additionally includes:

- **Targeted ID/Persistent ID**
- **Scoped Affiliation**

Is the attribute release for this entity category disabled, only the default and specific release rules apply.

9