Attribute Release Update

Upcoming changes for IdP administrators

SWITCH

Lukas Hämmerle
lukas.haemmerle@switch.ch

Berne, 30. June 2016

IdP Attribute Release Changes

1. eduGAIN SPs without <RequestedAttributes>
2. R&S Changes
3. PersistentID NameFormat Changes

On the Changes

- All changes planned to become active in August 2016
- Separate announcement on aai-operations list will follow
- Generally, no actions required by SP and IdP administrators

1. eduGAIN SPs without <RequestedAttributes>

- Many eduGAIN SPs don't declare attributes they need ☹
- So far Resource Registry assigned such SPs a default set of "requested" unpersonal attribute:
  - schacHomeOrganization (e.g. "switch.ch")
  - schacHomeOrganizationType (e.g. "urn:schac:homeOrganizationType:int:NREN")
  - eduPersonScopedAffiliation (e.g. "staff@switch.ch")
  - eduPersonAffiliation (e.g. "staff")
  - eduPersonTargetedID (e.g. "yrV12dAmohZY+cE6dc34qu/Dubc=")
- Planned change: **No default attribute set anymore**
  - **No action needed from IdP admins**
  - **Low impact expected**

2. R&S Changes

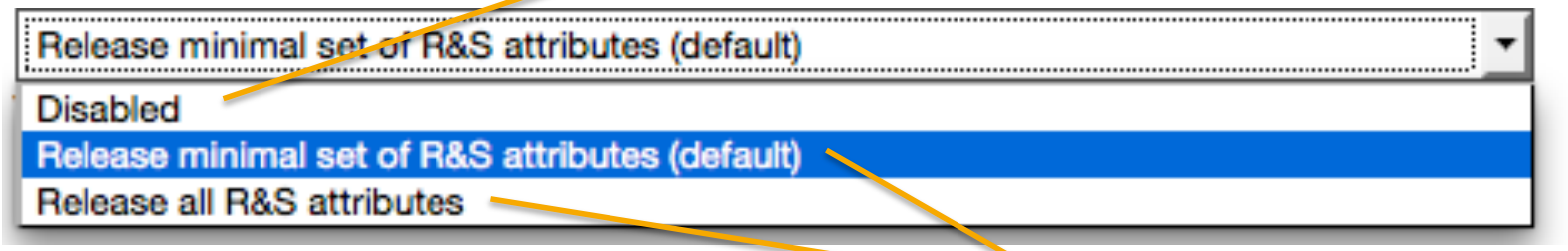
- REFEDS Research & Scholarship category
  - Federations can "tag" research and education SPs
  - https://refeds.org/category/research-and-scholarship
  - Allows easier/safer attribute release
  - Initial specification (2014) ➔ clarification proposal (2016)

- SWITCHaai was early adopter ➔ a few changes
  - No distinction anymore between minimal and full R&S attribute set

- Planned Change: **Clarification-conform implementation**
  - **No action needed by IdP admins. R&S Service Providers will additionally get affiliation and eduPersonTargetedID attribute**

Proposed Change in Resource Registry

- Current:



No eduGAIN-enabled IdP has chosen the "Disabled" option since 2014

Difference between default and full R&S set is only the "unpersonal" affiliation and the opaque eduPersonTargetedID attributes

- Future:

3. PersistentID NameIDFormat Changes

- transientID is default NameIDFormat for SWITCHaai SPs
  - Some SAML implementations require persistentID format
  - SAML2int.org also profile recommends persistentID format

- Planned Change (August):
  Support for using SAML2 persistent NameID
  - **No changes needed at IdPs**
  - **Better interoperability with non-Shib SAML implementations**

- Implications
  - AAI Resource Registry to support declaration of NameIDFormat
  - New SPs to use persistentID format by default
  - eduPersonTargetedID contains same value like persistentID
  - Eventually, migration from existing SPs to persistentID

Questions

Attribute Release Problem

- Most federations don't have a scalable attribute management like SWITCHaai has

  ➔ Many login problems, helpdesk requests, frustrated users, ...

- Solution was to create a metadata "flag" for SPs to whom a fixed set of attributes should be released

  ➔ REFEDS Research & Scholarship entity category

R&S Entity Category

- **REFEDS Research & Scholarship (R&S) Entity Category**
  - https://refeds.org/category/research-and-scholarship
  - To tag SPs that "enhance the research and scholarship"

- **Facilitates attribute release to R&S SPs**
  - Federation operators (like SWITCH) set and control which SPs get R&S flag
  - R&S SPs: non-commercial SPs used for research and education, e.g. SPs from CERN, LIGO, ...
  - Easy configuration, no/less privacy issues

- **For SWITCHaai IdPs only relevant in context of eduGAIN**
  - Has been in place since 2014

So what changes?

- R&S specification (from 2014) leaves too much room for interpretation ☹
  - SWITCHaai was early-adopter of this category
  - Today: Better consensus about implementation
  - (For SPs back-wards) compatible R&S Clarification Proposal

R&S Clarification Proposal

"The *R&S attribute bundle* consists (abstractly) of the following required data elements:

- *shared user identifier*
- *person name*
- *email address*

and one optional data element:

- *affiliation*

To be on the safe side, we propose to release both attributes because some SWITCHaai orgs cannot ensure that uniqueID/principal name never is reassigned

where *shared user identifier* is a persistent, non-reassigned, non-targeted identifier defined to be either of the following:

- eduPersonPrincipalName (if non-reassigned)
- eduPersonPrincipalName + eduPersonTargetedID

and where *person name* is defined to be either (or both) of the following:

- displayName
- givenName + sn"

Impact on Attribute Release

Number of attributes released to R&S SPs changes!

Compared to current default setting for IdPs:

+ Scoped Affiliation released
e.g. `staff@empa.ch`, `student@unige.ch`, `faculty@uzh.ch`

+ eduPersonTargetedID released
e.g. `yrVdvdAmohZYocE6dcGvqu/Dubc=`

+ Complete R&S attribute set released independent of `<RequestedAttributes>` element in metadata

Impact on IdPs

- **No action needed by IdP admins!**
  - Unless your organisation is not comfortable with R&S attributes being released to research and scholarship SPs
    - R&S-based attribute release has been in place since 2014 for all SWITCHaai Interfederation-enabled IdPs
    - No problems known of any SWITCHaai organisations
    - Default setting can be changed by Home Organisation administrator in Resource Registry
- **Benefit:**
  - **Better interoperability with R&S Service Providers in eduGAIN**
  - **(Slightly less helpdesk requests due to missing attributes)**