Release Check Evaluation Rules

Evaluation:

This page contains information on the IdP test results of the eduGAIN Attribute Release Check Service (EARCS), which allows users from an eduGAIN Identity Provider to check whether it properly releases information in form of attributes is to eduGAIN-enabled services.

The check results are reflected by the following verdicts:

Test Verdicts

A	IdP sends all necessary information
B	IdP sends minimal information
C	IdP sends basic information while some required information is missing
C	IdP sends eduPersonTargetedID with the wrong (legacy) syntax
D	IdP sends superfluous personal information
D	IdP sends some subset of the requested information, but not the basic information (see definition below)
F	Incorrect value syntax (except for eduPersonTargetedID above)
F	R&S category support is indicated but its requirements are not satisfied
F	No attributes received

Attribute Release Training

To get a better understanding of attribute release in general, how it affects services in eduGAIN and what to consider to properly implement it, we strongly recommend to have a look at the GÉANT online course on "Successful Attribute Release".

Bonus points (A-C)

- IdP R&S support is indicated

Penalty points (A-C)

- Redundant attributes are missing, but information is available
- IdP sends superfluous non-personal information (see below for definitive list)

Statement for the **"No Entity Category Test"**

For this test a Service Provider is used that does have no entity categories such as REFEDS R&S or the GÉANT Data Protection Code of Conduct but just declares the attributes eduPersonScopedAffiliation, schacHomeOrganization, email and eduPersonPrincipalName as required attributes in metadata. The result of this test is one of the following two statements:

"*Good data privacy but bad usability*":
This means that the IdP was not releasing any attributes to this test SP even though it requested them. This behaviour is rather restrictive from a usability point of view because users most likely won't get access to eduGAIN services that have no entity categories unless the IdP has configured any specific attribute release rules. Still, IdP administrators in some countries feel safer with this setup from a legal/data privacy perspective.

"*Good usability but bad data privacy*":
This means that the IdP released some or all required attributes to this test SP just because the SP requested them. This policy is used by few Identity Providers. It is easy to implement and in most cases is beneficial to users because they gain access to more services because their attributes are released by default. From a privacy point of view some argue that IdPs using this approach might be a bit too generous in releasing data about the user, especially in case there is no user consent enforced during the login process (which the EARCS check does not know about) or for services that are not relevant for the users studies or job. However, so far there are worldwide no cases known in the community where IdPs got into legal issues using this approach.

Terminology

- **Attribute**: A non-empty SAML Attribute sent as a part of a SAML AttributeStatement
- **Information**: Either an attribute or a set of attributes for which a transformation or combination algorithm is available to produce data for an application (ie: *e-mail, affiliation*, *name*)
- **Requested information**: The set of attributes or meta-attributes (such as a non-reassigned identifier or a name), that is requested by the SP by using SAML metadata, whether or not *isRequired* is flagged.
- **All necessary information**: Set of released attributes that can provide all requested information
- **Minimal information = required information**: If the tested SP has an entity category, where the minimal set is defined (such as R&S), the minimal information is the minimal set. Otherwise it is the set of attributes that can provide the subset of requested information, where *isRequired="true"* is set in the SP's SAML metadata.
- **Basic information**: A set of attributes, including at least a persistent identifier represented by at least one of:
    - eduPersonPrincipalName
    - eduPersonTargetedID (a SAML 2.0 persistent NameID, either sent in the SAML Assertion's Subject or as a SAML Attribute)
    - eduPersonUniqueId
- **Superfluous attribute**: Attribute that is sent by the IdP even though the information is not requested by the SP. Sending the same attribute in different NameFormats does not count as superfluous information. A *redundant attribute* does not count as superfluous information, if the source attribute(s) is/are requested. As a special case, eduPersonTargetedID is not a superfluous attribute if eduPersonPrincipalName is requested either directly via a `RequestedAttribute` metadata element or indirectly by declaring R&S entity category.
- **R&S requirements**: According to the R&S specification, the following attributes must be provided by an R&S IdP:
    - eduPersonPrincipalName
    - mail
    - displayName OR (givenName AND sn)
- **Redundant attributes**: Information that can be extracted from one or more attributes:
    - schacHomeOrganization <= eduPersonScopedAffiliation
    - schacHomeOrganization <= eduPersonPrincipalName
    - eduPersonAffiliation <= eduPersonScopedAffiliation
    - cn <= sn+givenName
    - displayName <= sn+givenName
    - cn <= displayName
    - displayName <= cn
    - as a special case, even though *sn* and *givenName* can not be reliably extracted from *cn* or *displayName*, however for EARC ranking, they are treated as redundant to both *cn* and *displayName.*
    - eduPersonTargetedID <= SAML 2.0 persistent NameID
- **Personal information**: All received attributes **except for**
    - schacHomeOrganization
    - schacHomeOrganizationType
    - eduPersonAffiliation
    - eduPersonScopedAffiliation
    - o
    - eduPersonEntitlement with the value of "urn:mace:dir:entitlement:common-lib-terms" (other values are treated as personal attributes)

REST/JSON API

There is a simple API to query the test verdicts for all Identity Providers and for a particular one.

Query all Identity Provider Results:

Query Format: HTTP GET to

https://release-check.edugain.org/api/results/

Example: https://release-check.edugain.org/api/results/

This will return all the tested Identity Providers with their basic information, test verdicts and a URL to the details page. The response is a JSON-encoded.

Query Results for one specific Identity Provider:

Query Format: HTTP GET to

https://release-check.edugain.org/api/results/#URL-encoded IdP EntityID#

Example: https://release-check.edugain.org/api/results/https%253A%252F%252Fpapi.kfki.hu%252Fidp%252Fshibboleth

This will return information for the specific Identity Provider whose URL-encoded entityID is added to the query URL.