Rethinking eduGAIN Trust

Why we need to enhance eduGAIN trust

In order to enhance attributes release, interoperability and cooperation among entities in international and cross-border use cases, the level of trust among member federations and entities in eduGAIN should be raised. This goal is also recognized in the critical success factors in the eduGAIN Strategy document [edugain-strategy].

To enhance attributes release, security and interoperability in a scalable manner, the R&E community defined a set of specifications, such as for example the ones defined by https://refeds.org/specifications. For some of these, federation operators act as registrars, while some others are used directly by entities without registration.

Because there is no trusted third party that certifies the intended use of these specifications, today there is no formal way of knowing if a registrar or an entity follows the set rules. As a consequence, these specifications in practice don't have the intended effect because entities may not always trust their use. This often leaves researchers and students having issues accessing international services because their Identity Provider does not trust the Service Provider to release the attributes, and/or because the Service Provider does not trust the attributes released by Identity Provider.

What do we want to achieve

Currently, trust in eduGAIN is limited to the relationship between eduGAIN and the participating federations. The aim is to extend the trust to the use of REFEDS, and other agreed international, specifications when used in eduGAIN. This would enable:

- **Federation operators** to support and promote the consistent use of these specifications seamlessly across their federation and eduGAIN;
- **Entities** to trust that these specifications are being properly followed; and
- **Academic users** to use their federated identities to the fullest extent striving for seamless user experience when accessing services.

What follows is a proposal to enhance the trust in specifications used by federations and entities in eduGAIN.

How to get there

In order to establish trust in using REFEDS, and other agreed international specifications, eduGAIN would need to set and mandate minimum common requirements for their use and carry out a verification process for registrars. Once the intended use of a specification has been verified, there are two complementary approaches that should be taken to implement it:

- **Rise the eduGAIN baseline** - where an approach would be to mandate the use of a certified specification for an entity to be published to eduGAIN (for example for SIRTFI);
- **Add filtering or signaling** - that would be applied by eduGAIN to express that an entity's use of a specification has been verified.

Depending on the specification, these two approaches can be used in a phased manner. They can also be combined in some cases, for example starting with an additional level of signaling as a first stage, and later on implementing a requirement to raise the eduGAIN baseline.

Add filtering or signaling

These approaches can be summarised as follows:

- **Filter an entity category or attribute**: eduGAIN filters out Entity Categories and Entity Attributes for entities coming from federations that do not pass the eduGAIN verification process for a given specification.
- **Signal by adding an entity attribute**: eduGAIN adds a conformance attribute value per each Entity Category and Entity Attribute for which the federation passes the eduGAIN verification process for a given specification.
  For example for Sirtfi, there would be an additional value of "https://edugain.org/refeds/sirtfi", such as:

```
<saml:Attribute
  Name="urn:oasis:names:tc:SAML:attribute:assurance-certification"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml:AttributeValue>https://refeds.org/sirtfi</saml:AttributeValue>
    <saml:AttributeValue>https://edugain.org/refeds/sirtfi</saml:AttributeValue>
</saml:Attribute>
```

Comparison of the above options:

	Filter entity category or attribute	**Signal by adding an entity attribute**
Trust	eduGAIN is the anchor.	eduGAIN is the anchor.
Transparency	Not transparent to which ECs are being certified (need to be combined with offline information about that)	Transparent
SP implementation complexity	Easy, SP does not need to interpret anything	More complex, SP needs to interpret tags differently for a local federation registered IdP and an international IdP (if the federation does not do additional filtering)
IdP implementation complexity	Easy, IdP does not need to interpret anything	More complex, IdP needs to interpret tags differently for a local federation registered IdP and an

		international IdP (if the federation does not do additional filtering)
Federation implementation complexity	Easy	Easy but federations may manage the added complexity of the extra verification entity attribute by choosing to filter entities lacking this additional attribute. This will make it easier for entities.
Interoperability	Potentially opens problems because some entities will have their entity category or attribute removed	Can enhance interoperability if implemented properly by IdPs, SPs and federations.
Incentive for implementation	Filtering is generally good incentive to implement stuff	Unless there are killer apps requiring this, there will be no incentive for implementation

eduGAIN verification process for specifications

TBD

References

[edugain-strategy]
https://docs.google.com/document/d/12ML76QVSI1n8N5jKRnMIBKeWlHH3Z2bMMJagcSwDBf0