

Trust & Identity Incubator

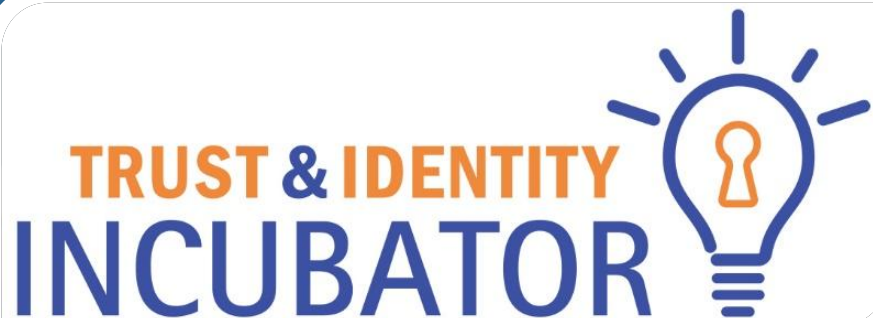
eduGAIN Service Catalogue

Branko Marović

Sprint Demo, 22-09-2021

Public

www.geant.org



What we did

- Analysed existing SAML based catalogues and selected a platform for our white-label prototype or solution
- Analysed and compared various types of service catalogues, identified matching features and attributes and identified the most relevant and suitable ones
- Matched attributes to the available data
- Developed a simple white-label catalogue starting from the IDEM solution
- Consolidated the analysis based on data reality and experience with our solution in an RFC document
- Asked stakeholders to provide feedback

eduGAIN Catalogue Service RFC

<https://docs.google.com/document/d/175DePh0JKmO6VPY04TqVXoDNLEpf-3IUTwfpQuK425Q/edit#>

- Yet to be commented by stakeholders
- The RFC is highlighting
 - The simplicity of the solution
 - Its white-label nature
- It is a moderate plea to gradually introduce curated data
- It proposes to more strongly engage federation and service operators

Currently proposed attributes (already available)

- **Service name** - Short localised service name; sourced from mdui:DisplayName; in the user's language if available, otherwise, default to English if available, but also offer other available languages
- **Description** - Localised one-paragraph description; from mdui:Description
- **Registrar** - The available registrar; sourced from mdrpi:RegistrationInfo
- **Logo** - Sourced from mdui:Logo; can also be multilingual (if there are some cultural adjustments text in the graphics)
- **Contacts** - Available values of md:ContactPerson
- **More service info** - Sourced from (localised) mdui:InformationURL
- **Privacy policy** - Sourced from mdui:PrivacyStatementURLSAML attributes - Requested and required attributes from sourced from md:RequestedAttribute and md:RequiredAttribute
- **Since** (first seen) - From the available metadata history
- **Last updated** - From the available metadata history
- **CatalogID** - A unique, URL usable, reference to the entity created as a sha1 hash over the SAML entityID

Proposed additional attributes*

* Not readily available from SAML metadata or their semantics needs to be agreed upon by the community

- **Access URL** - Direct link where the end-user may use the service. *Source: curated and obtained from the service*
- **Service provider (name)** - Sourced from md:OrganizationDisplayName, expandable to (typically longer) md:OrganizationName
- **Service category** - One or more values from a limited vocabulary list of categories as established by the eduGAIN community. In case entity categories are provided, these will be provided additionally on a national level
- **License info** - One or more values from a limited list of (high-level) classification as established by the eduGAIN community. Probably it is best to implement it as a binary selector, e.g.
 - *Commercial/Non-commercial*
 - *Restricted/Public*
 - *Subscription-based/Free*

Attributes that were left out of the RFC

Previously also selected (in the existing solutions)

- Status* - SPs would need to report it, many would not bother to
- Used SAML attributes (requested and required) - Perceived as too technical

Previously proposed for discussion

- GDPR-safe - Too contestable what it should mean and who should assert it
- Target users - SPs would report it, but the beauty is in the eye of the beholder, so it is more important how the readers would interpret it
- Hotness - eduGAIN F-ticks, feedback (score and count)? What is the most appropriate measure and how to collect it?
- (Catalogue data) sourced from - Could be perceived as an endorsement, not as a technical detail

These removals are reducing the usability of the catalogue as a promotional tool for services or a catalogue for end users.

Strategic choice: You cannot have a cake (propose a catalogue for the available data) and eat it too (request new data to be collected)!



Curating (meta)data

- Is potentially very labour intensive
- Is mostly in the interest of the service (to improve uptake)
- Is best done by the service

How can we get SPs to provide curated data?

Proposed model

- Any federation that exports SPs to eduGAIN will ask these SPs to provide the agreed-upon data.
- This activity provides a flow and additional data and will record the curated data in the catalogue.
- Federations may run a catalogue to present this data alongside SAML metadata-based information.



Concepts - “Catalogue Exchange”

Next to presenting the catalogue for eduGAIN, allow national federations to run their own local catalogue

- Assume minimal operational capabilities
- Consume curated data for eduGAIN services
- Support federations who already have a catalogue

Therefore:

- White label, lightweight, ‘Plain HTML’ catalogue (inspired by IDEM)
- A GUI for SPs to add curated data
- An API for federations that already have a catalogue

Proposed curated metadata engagement model

Federation operated catalogues

- Any federation that exports SPs to eduGAIN will direct the SP to the GUI to test existing SAML metadata for completeness and ask them to provide the agreed-upon curated data.
- To collect curated data a GUI is provided centrally, where federation operators may direct their SPs. The Catalogue GUI will:
 - Suggest SAML metadata improvements based on evaluating current SAML metadata of the SP and comparing that to the current best practices.
 - Allow services to create and maintain additional curated data fields.
- Federations that currently already operate catalogues with curated data, may provide that data on behalf of the services via the Catalogue r/w API.

Proposed engagement

- Any federation that exports SPs to eduGAIN will direct the SP to the GUI to test existing SAML metadata for completeness and ask them to provide the agreed-upon curated data.
- This activity provides a scalable flow, data structure and quality and will record the curated data in the Catalogue.
- Federations collect curated data via the API for their catalogue. If so required, a federation can make use of the white-label Catalogue to present this data.




Open Questions

- Do you consider the model where SPs provide curated data via a form as viable?
- Would you as a fed ops be willing to “chase” the SPs?
- Should we allow the inclusion of information typically found in SAML metadata if that is missing from metadata?
- Is a generic catalogue you can roll nationally and customize yourself appealing? Would you deploy that?

- What critical information did we miss so far which ***must*** be in the catalogue?

eduGAIN Service Catalogue

 Prepared the RFC

 How the approach was narrowed down to conform with the reality

 Perhaps too many internal assumptions, need to better document internal decisions?

 No feedback so far

Demo video

https://wiki.geant.org/download/attachments/247431187/SC_demo.mp4

Thank you

Any questions?

www.geant.org

