GÉANT

SAML Metadata 101
Upper layer

Peter Schober, ACOnet (Austria)

GÉANT SA5 T4 Training
Vienna, April 21st & 22nd, 2015

SAML Metadata cont'd

Making SAML entities more user-friendly/useful:

- md:Organization

- md:ContactPerson

- md:RequestedAttributes

- MDUI

- Entity Attributes (Categories)

md:Organization

- Names the "owner" or "provider" of the entity

- Also has a DisplayName and a URL

- Use is inconsistent internationally, though.

Example: eduID.at convention

`Organization` get's the full legal name

`OrganizationDisplayName` the "cleaned up" name

`OrganizationURL` has the organization's home page

md:ContactPerson

- Gives you the name and/or contact details of someone to ask things or report problems with an Entity.

- Has different types, most important ones:
  - support, technical, administrative

- Again: Use is inconsistent internationally.

Example: eduID.at convention
At least a "technical" contact type that has a role email address, "support" type if available.

MDUI

Metadata Extension for User Interface elements (`mdui:…`)

- DisplayName, Description, {PrivacyPolicy,Info}URL, Logo
    - `md:OrganizationDisplayName` vs. `mdui:DisplayName`

- Discovery Info: IP ranges, domains, geolocations

Allows building of more user-friendly user interfaces, discovery processes or error handling. Demos: eduID.at Service Catalog, ACOnet Filesender error handling, eduID.at Demo SP.

Allows SPs to express the attributes they need to function, with some limitations. IDPs can use this info to automate policy decisions.

eduID.at FileSender example
(Show online)

Entity Category "Code of Conduct"
Used by the GÉANT Data Protection Code of Conduct for SPs!

Entity Attributes (Categories)

Metadata Extension for Entity Attributes (`mdattr:…`)

- Allows assigning arbitrary SAML attributes (NameFormat, Name, Value/s) to SAML entities (instead of Subjects)

- Popular for assigning Entities to "Categories", in order to group them and create policy rules for whole categories.

Entity Category

Used by the GÉANT Data Protection Code of Conduct for SPs!

Used by REFEDS Research & Scholarship (R&S)!