Raccomandazione: i Metadati per la Federazione IDEM

Verso una definizione di IDEM METADATA PROFILE

Barbara Monticini - GARR

Cosa è successo nel corso del 2012

- Introduzione del parametro **validUntil** (5 gg.)
- Rafforzato l'uso <OrganizationDisplayName> per Sp definendo «service_name **erogato da** organization» («**provided by**» se in lingua inglese)
- Nei metadati di IDEM i nuovi entity (e quelli modificati nell'anno) si sono arricchiti di **MDUI** e **doppia lingua** (quando disponibile)
- Nei metadati di eduGAIN tutti gli entity rispettano le raccomandazioni di **interoperabilità** (è vero? prox. slide)
- Installato il **Discovery Service** di Shibboleth nella federazione di test, presto sarà in IDEM

Test sui metadati prodotti per eduGAIN

Federation's metadata URL: https://www.idem.garr.it/docs/conf/signed-edugain.metadata.xml

Entities SHOULD have language variants of certain elements. All entities SHOULD have an English variant and a local one. You may set a number of language tags which will be then treated as local languages and the validator will issue a warning if none of these languages appears within language variants of the entities. You may set the language to "en" so that no warnings are generated if no other language variants are present in the entities.

If no language tags are set, the validator will complain only if no non-English variants are found.

Select your language tag: it — *click to add next language tag*

or

skip local language checks

Metadata URL contains only one entity (not signed, no EntitiesDescriptor tag)

We check all MUSTs and SHOULDs from the eduGAIN profile requirements and recommendations (see eduGAIN Metadata Profile).

Validate | Only show entities list | Clear

Checking if metadata at https://www.idem.garr.it/docs/conf/signed-edugain.metadata.xml meet eduGAIN profile requirements and recommendations
(see "eduGAIN Metadata Profile")

You declared "it" as your language tag.

General info | Errors | Warnings | Detailed info | Entities list

Metadata validation passed successfully

- Signature verification passed

Template per arricchire i metadati di idp e sp

- Grazie a questa esperienza oggi siamo pronti a distribuire dei template:
  - Traccia per Idp
  - Traccia per Sp
- Il servizio continua a farsi carico della correttezza sintattica e semantica dei metadati e delle eventuali normalizzazioni necessarie

I TAG raccomandati in IDEM

- Chiavi crittografiche
  - Non scadute
  - Conformi a quelle in uso nel server
- MDUI (slide a parte)
- SP :: AttributeConsumingService (slide a parte)
- Organization
  - OrganizationName (*lingua locale ed inglese*)
  - OrganizationDisplayName (*lingua locale ed inglese*)
  - OrganizationURL (*lingua locale ed inglese*)
- ContactPerson
  - Un indirizzo impersonale -> *una lista o un servizio*

MDUI - Estensioni per l'interfaccia utente

- All'interno del tag <md:Extensions> di IDPSSO e SPSSO
- L'elemento root è <mdui:UIInfo> e può contenere:
  - <mdui:DisplayName> - come OrganizationDisplayName, 33 car.
  - <mdui:Description> - max 100 car. (tipo «onmouseover», per sp)
  - <mdui:InformationURL> - pagina associata alla risorsa / all'idp
  - <mdui:PrivacyStatementURL> - per idp e uApprove
  - <mdui:Logo> - url protetta https, .png con sfondo trasparente:
    - Logo 16px per 16px
    - Logo 80px (width) per 60px (height)
  - <mdui:Keywords> - per idp parole chiave, categorie, etichette
  - <mdui:DiscoHints> - per idp: IP, domini e geo loc.

SP e dichiarazione degli attributi richiesti

- Ogni <md:SPSSODescriptor> può contenere:
  - <md:AttributeConsumingService>
    - <md:ServiceName>
    - <md:ServiceDescription>
    - Lista <md:RequestedAttribute>
      - definisce se sono **Required** o **Useful** con l'opzione **isRequired=«true|false»**
      - definisce i valori ammissibili per quell'attributo con **<saml:AttributeValue>**

I TAG obbligatori e opzionali per eduGAIN

- Ogni <md:EntityDescriptor>:
  - <md:ContactPerson> (obbl.)
  - <mdrpi:RegistrationInfo> (obbl.)
    - Ci pensa il servizio **idem-help**
  - <md:Organization> (opz.)
- Ogni <md:IDPSSODescriptor> e <md:SPSSODescriptor>:
  - <mdui:DisplayName> (opz.)
  - <mdui:Description> (opz.)
- Ogni md:SPSSODescriptor:
  - <md:AttributeConsumingService> (opz.):
    - Lista <md:RequestedAttribute>, definisce se sono **Required** o **Useful**:
      - isRequired=«true|false»

Usare xml:lang appropriate

- Come decidere quale lingua inserire?
  - Le entity italiane devono avere lang=it
  - Le entity italiane possono avere lang=en
    - Nel caso di url la pagina deve essere in lingua inglese
  - Le entity italiane in eduGAIN devono avere lang=it e lang=en

Alcuni comandi utili per controlli xml

- Controllo sintattico: xmlwf
- Controllo semantico: usando gli schema
  - saml-schema-metadata-2.0.xsd
  - sstc-saml-idp-discovery.xsd
  - sstc-saml-metadata-ui-v1.0.xsd

Conclusioni e considerazioni per il futuro

- Controllare i certificati in uso sul server (idp e/o sp) e quelli dei metadati
  - Devono coincidere
  - Meglio se non scaduti!
  - In preparazione controllo automatico certificati scaduti
- Iniziare ad usare i template per i metadati
  - MDUI Logo

Riferimenti

- eduGAIN
  - http://www.geant.net/service/edugain/resources/Documents/eduGAIN%20Metadata%20profile.pdf
  - https://aai.pionier.net.pl/Metadata/
- REFEDS: Raccomandazioni MDUI
  - https://refeds.terena.org/index.php/MDUI_-_Federation_recommendations
- Librerie OPENSAML
  - https://wiki.shibboleth.net/confluence/display/OpenSAML/Home
- SP di test con Discovery Service
  - https://sp-test.garr.it