# Regole per scambiare gli attributi

Entity Category e Code of Conduct

# Lo scambio di attributi tra Idp e Sp

- valutazione di ogni SP
- valutazione di ogni richiesta di attributi
- (approvazione)
- aggiornamento manuale politiche di rilascio attributi per ogni SP

# Lo scambio di attributi tra Idp e Sp

- valutazione di ogni SP
- valutazione di ogni richiesta di attributi
- (approvazione)
- aggiornamento manuale politiche di rilascio attributi per ogni SP

NON SCALA

# Entity Categories

*entità con caratteristiche comuni all'interno di una federazione*

OASIS **SAML V2.0 Metadata Extension for Entity Attributes**

**Per gli SP**: dichiarano di appartenere ad una o più Entity Category

**Per gli IdP**: rilasciano attributi in base alla Entity Category

# Entity Category attribute

- tipicamente utilizzato dai SP
- valore => URI
  - raccomandato URL in http/https
  - pagina web con le specifiche della categoria
- nessuna registrazione centralizzata

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
      entityID="https://service.example.com/entity">
  <md:Extensions>
    <mdattr:EntityAttributes
        xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
      <Attribute xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
          NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
          Name="http://macedir.org/entity-category">
        <AttributeValue>http://example.org/category/dog</AttributeValue>
        <AttributeValue>urn:oid:1.3.6.1.4.1.21829</AttributeValue>
      </Attribute>
    </mdattr:EntityAttributes>
  </md:Extensions>
  ...
</md:EntityDescriptor>
```

# Entity Category support attribute

- tipicamente utilizzato dagli IdP
- valore => URI
  - raccomandato URL in http/https => pagina web specifiche
  - può essere uguale a Entity Category attribute
  - può contenere *declinazioni* del supporto alla Entity Category

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
      entityID="https://idp.example.edu/entity">
  <md:Extensions>
    <mdattr:EntityAttributes
        xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
      <Attribute xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
          NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
          Name="http://macedir.org/entity-category-support">
        <AttributeValue>http://example.org/category/dog/basic</AttributeValue>
        <AttributeValue>http://example.org/category/dog/advanced</
AttributeValue>
        <AttributeValue>urn:oid:1.3.6.1.4.1.21829</AttributeValue>
      </Attribute>
    </mdattr:EntityAttributes>
  </md:Extensions>
</md:EntityDescriptor>
```

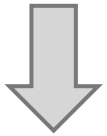
# Entity Categories e rilascio attributi

## Idp Shibboleth 2.3.4+

```
<AttributeFilterPolicy id="releaseToRandS">

  <PolicyRequirementRule
      xsi:type="saml:AttributeRequesterEntityAttributeExactMatch"
      attributeName="http://macedir.org/entity-category"
      attributeValue="http://example.org/category/dog"/>

  <AttributeRule attributeID="eduPersonPrincipalName">
    <PermitValueRule xsi:type="basic:ANY"/>
  </AttributeRule>

  <AttributeRule attributeID="email">
    <PermitValueRule xsi:type="basic:ANY"/>
  </AttributeRule>

</AttributeFilterPolicy>
```

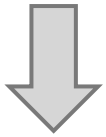
# Entity Categories e Federazione

Entity category auto-dichiarabili



La Federazione accetta il metadato (può monitorare l'uso)

Entity category soggette a processi di validazione e/o registrazione



La Federazione applica le politiche per la concessione dell'uso della Entity Category

# REFEDS Research and Scolarship Entity Category

https://refeds.org/category/research-and-scholarship/

# Data Protection Code of Conduct

**Progetto congiunto REFEDS GN3+**

**Ambito di applicazione**: Enti UE e Area Economica Europea (EEA)

**Normativa di riferimento**: Direttiva UE sulla protezione dei dati (95/46/EC - 24/10/1995)

# Direttiva UE: requisiti nel trattamento dei dati personali

- Sicurezza del trattamento
- Scopo trattamento
- Informare l'utente finale
- Basi legali per il rilascio degli attributi
  - Attributi necessari
  - Attributi opzionali con il consenso dell'utente

# Un difficile equilibrio per la comunità della ricerca

- Scalabilità
- Rischio vs semplicità
- Attrazione di nuovi servizi
- Protezione legale per gli enti che detengono i dati degli utenti finali
- Ruolo delle Federazioni
- Necessità di un approccio globale

# Code of Conduct: vincoli per i SP

- Richiedere il minor numero di attributi possibile
- Dichiarare la politica di tenuta dei dati
- Informare sulla sicurezza
- Informare sul trattamento diretta all'utente finale
- Rispetto del *Model Contract UE* per rilascio dati fuori da UE/EEA
- Informare tempestivamente le Organizzazioni di provenienza degli utenti finali di possibili compromissioni della sicurezza

[...]

# Code of Conduct: i metadata!

- Entity Category *Code of Conduct*
- Elenco degli attributi richiesti (md:requestedAttributes)
- URL del documento trattamento dati

  (mdui:privacyStatementURL)
- Nome del SP (mdui:displayName)
- Descrizione del SP (mdui:Description)

# Code of Conduct: i veri metadata

https://wiki.edugain.org/Recipe_for_a_Service_Provider

# GRAZIE PER LA PAZIENZA!