Consortium GARR
THE ITALIAN EDUCATION & RESEARCH NETWORK

Attribute Release Policy (ARP), Definizione Dinamica degli Attributi & Entity Category

Verso un rilascio semplificato degli Attributi

Corso Shibboleth IdP - 22-23/01/2020

Marco Malavolti - marco.malavolti@garr.it

Agenda

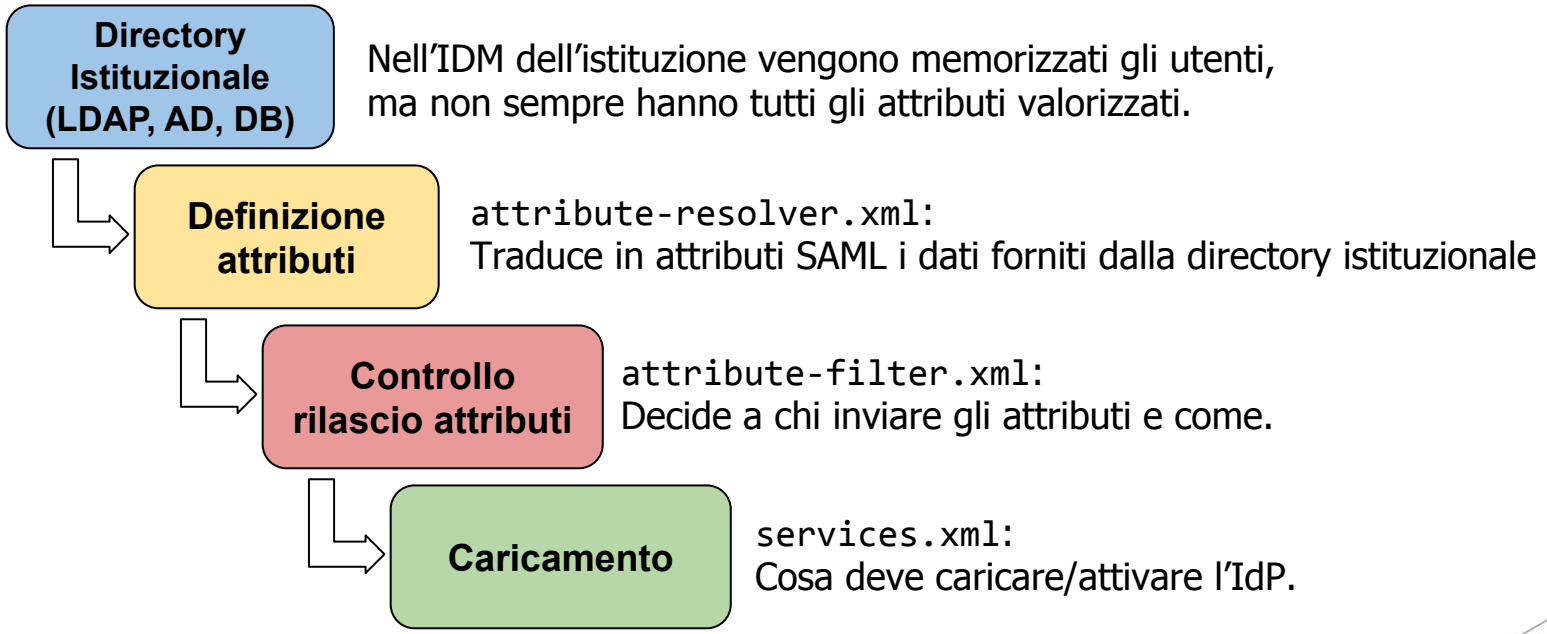
1. **Attribute Release Policy (ARP)**: Come si definiscono e come si rilasciano gli attributi SAML in un IdP Shibboleth.

2. **Definizione Dinamica degli Attributi:** Come si generano nuovi attributi a partire da quelli già esistenti.

3. **Entity Category**: Come si rilasciano gli attributi in modo scalabile e sicuro.

Attribute Release Policy (ARP)

La Politica per il rilascio degli attributi è il modo con cui un IdP decide **cosa, come e a chi rilasciare gli attributi** dei suoi utenti e prevede:



Definizione dinamica degli Attributi

attribute-resolver.xml: <AttributeDefinition>

All'interno dell'**attribute-resolver.xml** vengono collezionati diversi **<AttributeDefinition>** che consentono di definire gli attributi supportati dall'IdP.

```
<AttributeDefinition xsi:type="TIPO" id="ID-UTILIZZATO-DA-ATTRIBUTE-FILTER">
  <DisplayName xml:lang="it">VALORE MOSTRATO NELLA PAGINA DI CONSENSO PER L'UTENTE</DisplayName>
  <DisplayDescription xml:lang="it">DESCRIZIONE DEL VALORE ESPOSTO DALL'ATTRIBUTO</DisplayDescription>
  <InputAttributeDefinition ref="ID DI ALTRO <AttributeDefinition> DA CUI PRENDERE IL VALORE COME INPUT" />
  <InputAttributeDataConnector ref="ID DI UN <DataConnector>" attributeNames="attributo1-da-DC,attributo2-da-DC" />
  <AttributeEncoder xsi:type="Tipologia del valore in uscita"   (SAML2String, SAML2ScopedString, SAML2XMLObject, SAML2Base64)
                    name="OID corrispondente all'attributo"     (per un riconoscimento globale)
                    friendlyName="displayName"                  (nome parlante, spesso corrispondente all'id)
                    encodeType="false" />                       (settare sempre a 'false')
  <!-- [...] -->
</AttributeDefinition>
```

<AttributeDefinition> - Scoped

Il tipo "**Scoped**" definisce un attributo come risultato della fusione di un attributo con uno scope separati da "@".

Esempio:
https://github.com/ConsortiumGARR/idem-shib-idp-course/blob/4c16fa1db73ddea3c92ab8900dfbae5c6f2215e2/2020/22-23%20Gennaio/attribute-resolver-dynamic.xml#L98

<AttributeDefinition> - Template

Il tipo "**Template**" definisce un attributo come risultato dell'applicazione del template creato secondo le nostre esigenze.

Esempio:
https://github.com/ConsortiumGARR/idem-shib-idp-course/blob/cb8ae6ac76bbc7ec5e02553eed7410664847c2ee/2020/22-23%20Gennaio/attribute-resolver-dynamic.xml#L13

<AttributeDefinition> - Mapped

Il tipo "**Mapped**" definisce un attributo come risultato di una mappatura di N valori in 1 solo.

Esempio:
https://github.com/ConsortiumGARR/idem-shib-idp-course/blob/cb8ae6ac76bbc7ec5e02553eed7410664847c2ee/2020/22-23%20Gennaio/attribute-resolver-dynamic.xml#L29

<AttributeDefinition> - Scripted

Il tipo "**Scripted**" definisce un attributo come risultato dell'elaborazione di uno script.

Esempio:
https://github.com/ConsortiumGARR/idem-shib-idp-course/blob/cb8ae6ac76bbc7ec5e02553eed7410664847c2ee/2020/22-23%20Gennaio/attribute-resolver-dynamic.xml#L63

attribute-resolver.xml - <DataConnector>

All'interno dell'**attribute-resolver.xml** vengono collezionati diversi **<DataConnector>** che recuperano gli attributi interni, da LDAP/ Database, e permettono di utilizzarli come input degli **<AttributeDefinition>.**

```
<!-- ========================================== -->
<!--      Data Connectors                       -->
<!-- ========================================== -->

<DataConnector xsi:type="TIPO" id="ID-UTILE-AD-ATTRIBUTE-DEFINITION" [...ALTRI ATTRIBUTI XML UTILI AL TIPO DI DC...]>
    [...ALTRI <TAG> DI SUPPORTO AL TIPO SCELTO...]
</DataConnector>
```

<DataConnector> - RelationalDatabase

Il tipo "**RelationalDatabase**" recupera i valori da assegnare ad un attributo da un database come risultato di una query.

Esempio di Connessione al Database:
https://github.com/ConsortiumGARR/idem-shib-idp-course/blob/51508bdea3d1f87d71d6565f8e22182b371418d9/2020/22-23%20Gennaio/global.xml#L17

Esempio di DataConnector:
https://github.com/ConsortiumGARR/Ansible-Shibboleth-IDP-SP-Debian/blob/2a00c44d1ec7b57e74ece6565494be511fca189c/roles/shib3idp_configure/files/attribute-resolver-dbsql.xml#L45

<AttributeDefinition> + <DataConnector>

La combinazione tra `<AttributeDefinition>` e `<DataConnector>` consente ad un Identity Provider Shibboleth di definire quali attributi SAML sono da lui supportati e come vengono valorizzati.

Link utili di riferimento:

- DataConnector Configuration
- AttributeDefinition Configuration

Caricamento: services.xml

Dato che è possibile avere più di un **attribute-resolver.xml** sul proprio IdP, il file di configurazione "**services.xml**" indicherà quali utilizzare:

```
<util:list id ="shibboleth.AttributeResolverResources">
  <value>%{idp.home}/conf/attribute-resolver.xml</value>
  <value>%{idp.home}/conf/attribute-resolver-v3_4-idem-custom.xml</value>
</util:list>
```

e dovrà essere riavviato il servizio per applicare il tutto sull'IdP:

- `/opt/shibboleth-idp/bin/reload-service.sh -id shibboleth.AttributeResolverService`

Attribute Filter: il controllore del rilascio

`attribute-filter.xml` è un file di configurazione che l'IdP usa per controllare il rilascio degli attributi verso le risorse federate/SP.

Un attributo può essere supportato nell'`attribute-resolver.xml`, ma non essere rilasciato perché non considerato dall'`attribute-filter.xml`.

Attribute Filter: meccanismo di applicazione

1. Valuta tutti gli `<AttributeFilterPolicyGroup>` in modo non ordinato.
2. Valuta tutti gli `<AttributeFilterPolicy>` interni agli `<AttributeFilterPolicyGroup>` in modo non ordinato.
3. Per ogni policy, se la `<PolicyRequirementRule>` è valida:
   - applica ogni `<AttributeRule>` annidata in modo che:
     i. Tutti gli attributi con `<PermitValueRule>` siano aggiunti alla "lista degli attributi permessi".
     ii. Tutti gli attributi con `<DenyValueRule>` siano aggiunti alla "lista degli attributi negati".
4. Il risultato finale è così calcolato:
   - Prendi la *lista degli attributi permessi*,
   - Rimuovi gli attributi presenti nella *lista degli attributi negati,*
   - Rimuovi tutti gli attributi *senza valore,*
   - Invia alla risorsa quel che rimane.

Attribute Filter: Controllare il rilascio degli attributi

1. Genero "**/opt/shibboleth-idp/conf/attribute-filter-example.xml**":

```
<AttributeFilterPolicyGroup id="ID-UNIVOCO-UTILE-PER-LOGGING"
       xmlns="urn:mace:shibboleth:2.0:afp"
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xsi:schemaLocation="urn:mace:shibboleth:2.0:afp http://shibboleth.net/schema/idp/shibboleth-afp.xsd">

   <!-- Rilascia ePPN, ePE e ePSA all'SP con entityID="https://sp.example.org/shibboleth". -->
   <AttributeFilterPolicy id="ID-UNIVOCO-DELLA-POLITICA-DI-RILASCIO">
       <PolicyRequirementRule xsi:type="Requester" value="https://sp.example.org/shibboleth" />

       <!-- L'attributo eduPersonPrincipalName NON viene rilasciato -->
       <AttributeRule attributeID="eduPersonPrincipalName">
           <DenyValueRule xsi:type="ANY" />
       </AttributeRule>

       <!-- L'attributo eduPersonEntitlement viene rilasciato solo col valore stabilito -->
       <AttributeRule attributeID="eduPersonEntitlement">
           <PermitValueRule xsi:type="Value" value="urn:mace:dir:entitlement:common-lib-terms" ignoreCase="true" />
       </AttributeRule>
   </AttributeFilterPolicy>
   ...
```

RuleType

RuleType

RuleType

l'attributeID DEVE essere uguale all'ID usato nell'attribute-resolver.xml

Attribute Filter: Controllare il rilascio degli attributi

```
<!-- L'attributo eduPersonScopedAffiliation viene rilasciato qualsiasi sia il valore per lui generato -->
<AttributeRule attributeID="eduPersonScopedAffiliation">
    <PermitValueRule xsi:type="AND">
        <Rule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
        <Rule xsi:type="OR">
            <Rule xsi:type="Value" value="faculty" ignoreCase="true" />
            <Rule xsi:type="Value" value="student" ignoreCase="true" />
            <Rule xsi:type="Value" value="staff" ignoreCase="true" />
            <Rule xsi:type="Value" value="alum" ignoreCase="true" />
            <Rule xsi:type="Value" value="member" ignoreCase="true" />
            <Rule xsi:type="Value" value="affiliate" ignoreCase="true" />
            <Rule xsi:type="Value" value="employee" ignoreCase="true" />
            <Rule xsi:type="Value" value="library-walk-in" ignoreCase="true" />
        </Rule>
    </PermitValueRule>
</AttributeRule>
</AttributeFilterPolicyGroup>
```

RuleType

RuleType

RuleType

Le *RuleType* sono applicabili sia a `<PolicyRequirementRule>` che ad `<AttributeRule>` e possono avere 2 modalità di applicazione: *PolicyRule* (ritorna yes/no) o *Matchers* (ritorna un intervallo di valori).

I **`<PolicyRequirementRule>`** usano di solito la "**`PolicyRule`**", mentre gli **`<AttributeRule>`** la "**`Matchers`**"

Attribute Filter: Controllare il rilascio degli attributi

2. Mi assicuro che l'Attribute Filter creato/modificato sia presente in `services.xml`:

```
<util:list id ="shibboleth.AttributeFilterResources">
   <value>%{idp.home}/conf/attribute-filter.xml</value>
   <value>%{idp.home}/conf/attribute-filter-example.xml</value>
</util:list>
```

3. Abilito le modifiche:
   - `/opt/shibboleth-idp/bin/reload-service.sh -id shibboleth.AttributeFilterService`

Entity Category

PROBLEMA

Gli utenti federati non riescono ad accedere alle risorse federate perché l'IdP della loro organizzazione non rilascia tutti gli attributi necessari agli SP

Entity Category: Cosa sono?

1. Sono delle policy basate sullo standard SAML V2.0 Metadata Extension for Entity Attributes Version 1.0 che un IdP o un SP può usare per migliorare la loro interazione.
2. Due significati principali:
   a. supporto (es.: rilascio attributi da IdP a SP con EC)
   b. conformità alle policy stabilite dalle EC (IdP e SP)
3. Le Entity Category sono attribuite a IdP e SP dagli Operatori di Federazione (Servizio IDEM)

Entity Category: Cosa sono?

1. Sono dei <TAG> aggiunti nei metadata di IdP e SP che certificano il rispetto di particolari policy da parte del gestore del servizio federato.
2. Le policy che rappresentano hanno una semantica condivisa e riconosciuta a livello di federazione
3. Sono basate su uno standard: SAML V2.0 Metadata Extension for Entity Attributes Version 1.0
   http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr-cd-01.pdf
4. Due significati principali:
   a. supporto e interoperabilità (principalmente IdP)
   b. appartenenza e conformità a determinate policy (IdP e SP)
5. Le Entity Category di IdP e SP sono richieste dai gestori dei servizi, ma è la Federazione che ne valida il supporto (attraverso IDEM Entity Registry)

Entity Category: Lato SP

```
<mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">

  <saml:Attribute xmlns:saml="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">

    <saml:AttributeValue>
       http://refeds.org/category/research-and-scholarship
    </saml:AttributeValue>

  </saml:Attribute>

</mdattr:EntityAttributes>
```

Entity Category: Lato IdP

```
<mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">

  <saml:Attribute xmlns:saml="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">

    <saml:AttributeValue>
       http://refeds.org/category/research-and-scholarship
    </saml:AttributeValue>

  </saml:Attribute>

</mdattr:EntityAttributes>
```

Entity Category: A cosa servono?

1. Dichiarano l'affidabilità di IdP e SP.
2. Permettono agli IdP di rilasciare attributi solo agli SP conformi alle policy indicate dalla/e EC.
3. Permettono agli SP di accettare autenticazioni/utenti solo da IdP conformi alle policy.
4. Rendono scalabile il rilascio degli attributi verso gli SP.
5. Migliorano l'interoperabilità delle federazioni di identità.

https://wiki.idem.garr.it/wiki/EntityAttribute

Entity Category: Quali sono?

Le EC supportate da IDEM sono:

1. **CoCo** - GÉANT Data Protection Code of Conduct
   (gestione dei dati personali)

2. **R&S** - REFEDS Research and Scholarship Entity Category
   (rilascio attributi agli enti di ricerca e alta formazione)

3. **SIRFTI** - Security Incident Response Trust Framework for Federated Identity
   (tracciabilità degli accessi - CERT)

https://wiki.idem.garr.it/wiki/EntityAttribute

Entity Category: quali sono - CoCo

CoCo - GÉANT Data Protection Code of Conduct

1. Rispetto delle direttive europee in materia di protezione dei dati personali.
2. I Service Provider che aderiscono al CoCo devono trattare correttamente i dati personali degli utenti ricevuti dagli IdP.
3. Gli Identity Provider che la supportano devono rilasciare gli attributi ai Service Provider che la implementano.

https://wiki.refeds.org/display/CODE/Introduction+to+Code+of+Conduct

Entity Category: quali sono - R&S

R&S - REFEDS Research and Scholarship Entity Category

1. E' assegnabile ad SP gestiti da enti di ricerca e alta formazione
   - sono escluse tutte le risorse che distribuiscono contenuti sotto licenza (es.: riviste elettroniche)
2. Gli Identity Provider che la supportano devono rilasciare uno specifico set di attributi agli SP che la dichiarano:
   eduPersonPrincipalName, **eduPersonTargetedID**, **email**, **displayName**, **givenName**, **surname**, **eduPersonScopedAffiliation** (opzionale per R&S, ma obbligatorio per IDEM)

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

Entity Category: quali sono - SIRFTI

SIRFTI - Security Incident Response Trust Framework for Federated Identity

1. Sirtfi è un framework nato per aiutare a identificare le entità federate capaci di reagire e collaborare nei casi in cui si verifichino incidenti di sicurezza legati ai processi di autenticazione federata

2. Lo scopo di Sirtfi è quello di fornire un modello scalabile di cooperazione nella gestione di eventuali incidenti di sicurezza

3. Sirtfi si applica indifferentemente a Service Provider e Identity Provider

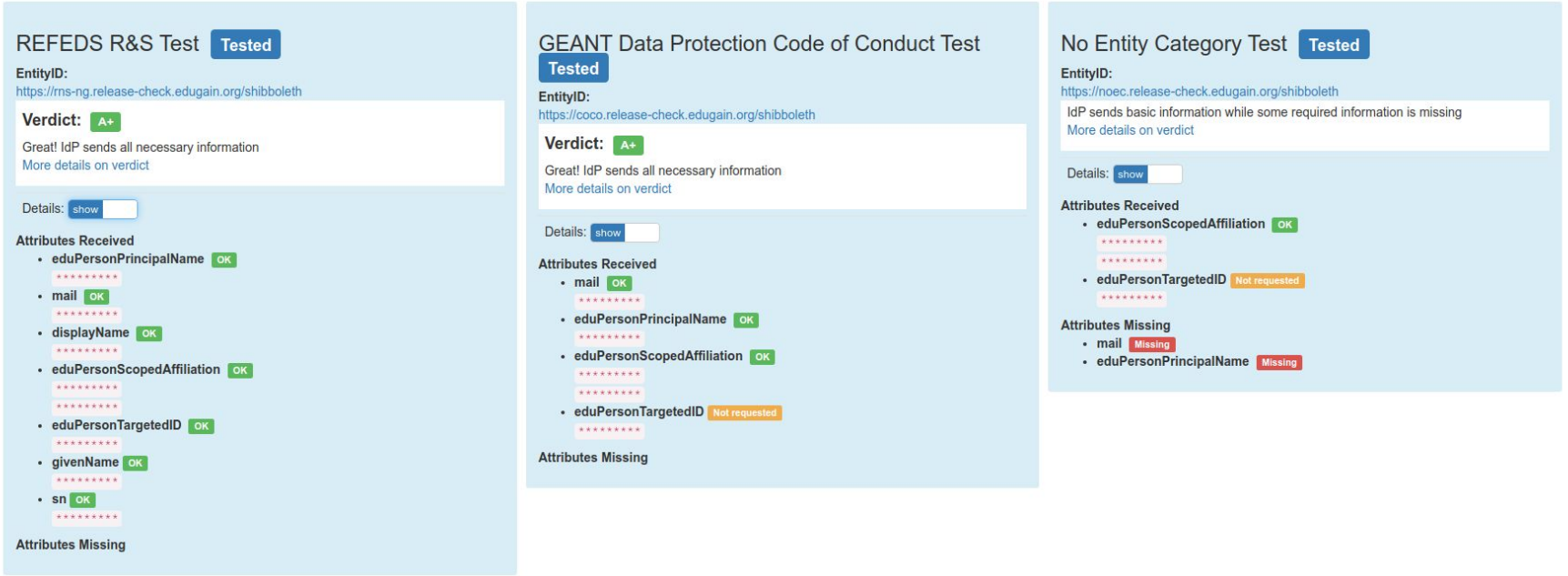
4. Autovalutazione: se tutte le asserzioni sono vere => OK SIRFTI
   https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf

https://refeds.org/sirtfi

Test sul rilascio degli attributi in eduGAIN

https://release-check.edugain.org/

Start the test



Test sul rilascio degli attributi in eduGAIN

Test sul rilascio degli attributi secondo EduGAIN CoCo:

```
/opt/shibboleth-idp/bin/aacli.sh \
  -n luigi -r  https://coco.release-check.edugain.org/shibboleth
```

Test sul rilascio degli attributi secondo RS:

```
/opt/shibboleth-idp/bin/aacli.sh \
  -n luigi -r  https://rns-ng.release-check.edugain.org/shibboleth
```

Per una EC sconosciuta o entità alle quali non si applicano filtri:

```
/opt/shibboleth-idp/bin/aacli.sh \
  -n luigi -r https://noec.release-check.edugain.org/shibboleth
```

Entity Category: Come si usano

1. Dal punto di vista degli IdP l'uso principale è l'implementazione dei filtri per il rilascio degli attributi agli SP
2. Usando le EC, non c'è la necessità di definire policy di rilascio attributi per ogni singolo SP
3. Con una sola policy di rilascio, vengono gestiti tutti gli SP che possiedono l'Entity Category nei loro metadati (anche quelli che ancora non esistono)
4. Quando un nuovo SP entra in federazione e fa richiesta dell'Entity Category, la federazione valuta la richiesta e in caso positivo la inserisce nei metadati dell'SP
5. Questo è sufficiente a far funzionare il meccanismo di rilascio degli attributi al nuovo SP da parte di tutti gli IdP che supportano l'Entity Category
6. NB: vanno usati preferibilmente con il meccanismo di consent, ovvero,
   è l'utente che esprime il consenso informato dell'invio dei suoi dati personali alla risorsa federata a cui vuole accedere.

Entity Category: Come si usano - attribute filter

1. Scaricare l'attribute-filter definito per le EC R&S e CoCo fornito da IDEM:
   - attribute-filter-v3-RS-CoCo.xml (in `/opt/shibboleth-idp/conf`)
2. Mi assicuro che l'Attribute Filter creato/modificato sia presente in `services.xml`:

```
<util:list id ="shibboleth.AttributeFilterResources">
   <value>%{idp.home}/conf/attribute-filter.xml</value>
   <value>%{idp.home}/conf/attribute-filter-v3-RS-CoCo.xml</value>
</util:list>
```

3. Abilito le modifiche:
   - `touch /opt/jetty/webapps/idp.xml`

Entity Category: Riferimenti

1. https://wiki.shibboleth.net/confluence/display/IDP30/EntityAttributesFilter
2. https://www.eventi.garr.it/it/idem-day-2018/idemday18/materiali-idem-2018/corso-aggiornamento-idp-e-nuovi-standard/265-davide-vaghetti-aggiornamento-idp-entity-categories-idem-day-2018/file
3. https://refeds.org/category/research-and-scholarship
4. https://wiki.idem.garr.it/wiki/EntityAttribute
5. http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr-cd-01.pdf

Domande?

marco.malavolti@garr.it
giuseppe.demarco@unical.it
maurizio.festi@unitn.it