IDEM: Specifiche Tecniche e Attributi

Raffaele Conte

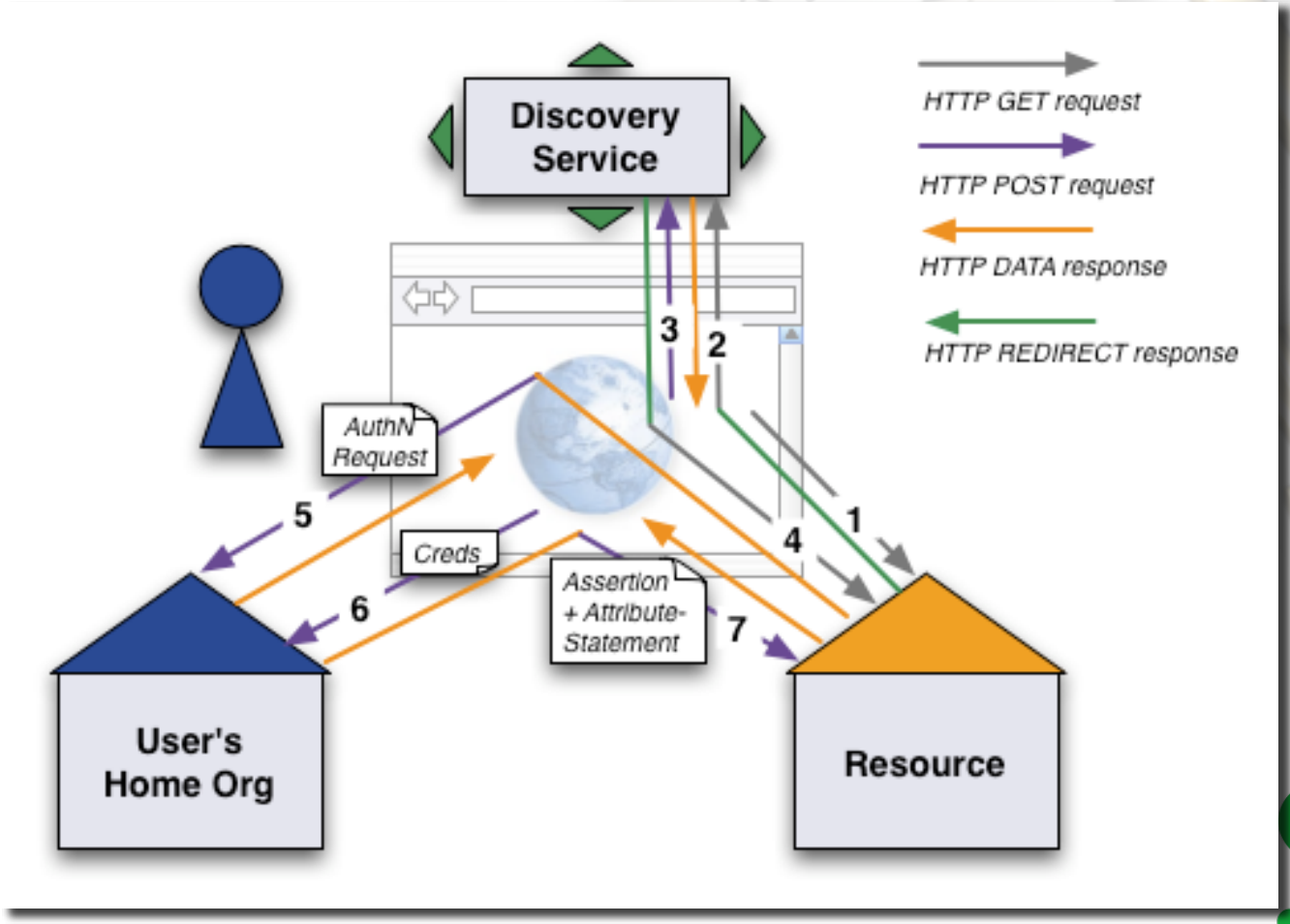
Istituto di Fisiologia Clinica

Comitato di Gestione - Federazione IDEM

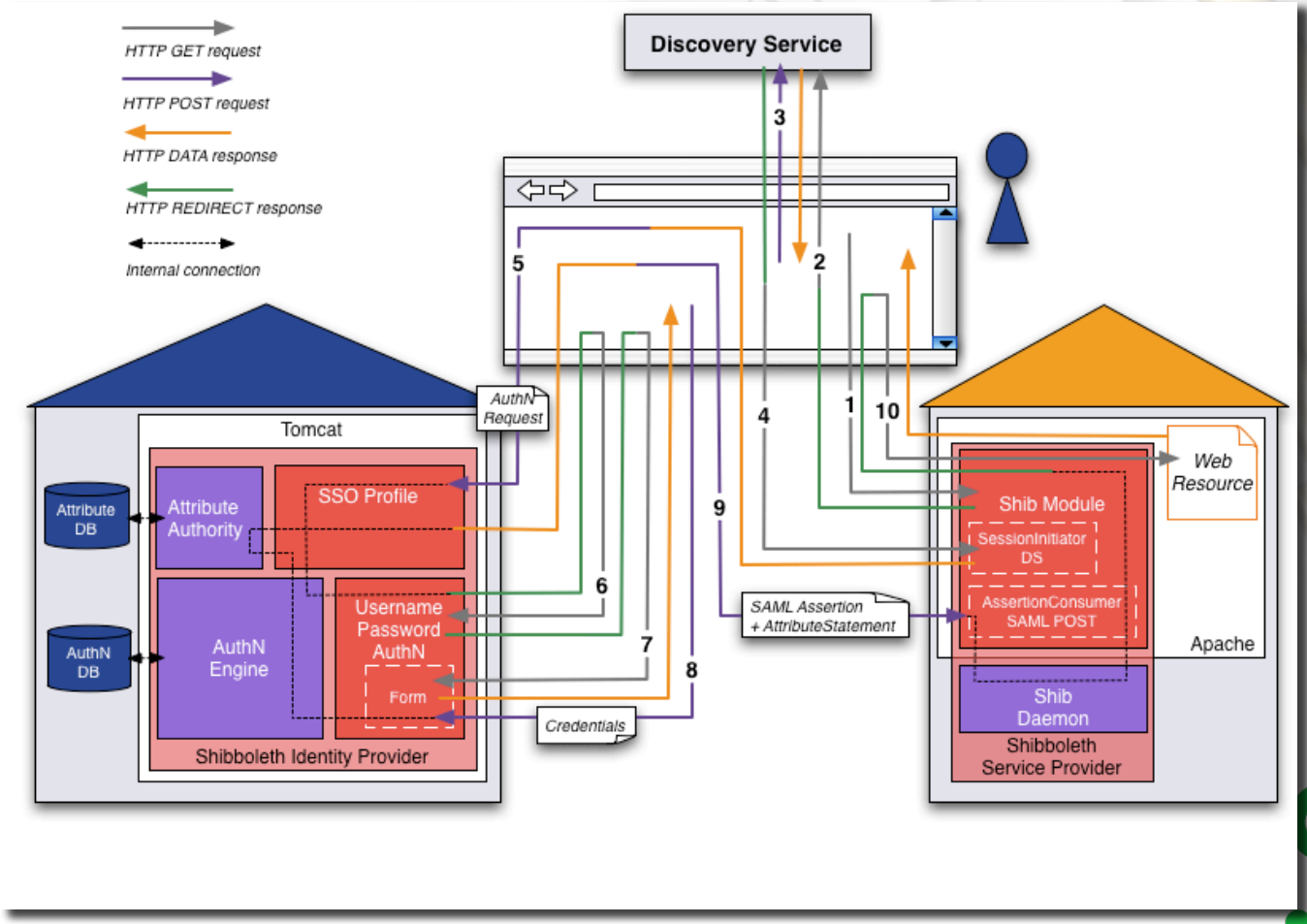
Cos'è una Federazione per l'AA

- È un insieme di regole tecniche e procedure condivise su cui si costruiscono relazioni di fiducia

Le relazioni nella Federazione



Le relazioni nella Federazione



Perché un documento sulle Doc. Specifiche Tecniche

- Non è un manuale di installazione
- È necessario per stabilire le regole di "convivenza" in modo da ottenere l'interoperabilità fra i partecipanti
- Fornisce info tecniche, Illustra le scelte fatte per IDEM e, quando necessario, suggerisce le configurazioni per implementarle

Contenuto del documento

- Implementazioni e Software
- Autenticazione
- Firewall
- Discovery Service
- Nomenclatura
- Attributi
- Metadati
- Riferimenti per gli utenti
- Comunicazioni ai partecipanti
- Operatività del servizio
- Logging

Contenuto del documento

- Implementazioni e Software
- Autenticazione
- Firewall
- Discovery Service
- Nomenclatura
- Attributi
- Metadati
- Riferimenti per gli utenti
- Comunicazioni ai partecipanti
- Operatività del servizio
- Logging

Agenda

Protocolli

- Il protocollo su cui la Federazione si basa è SAML 2
- È fortemente consigliato l'uso di NTP

  le asserzioni hanno una validità (tipicamente 5')

Applicativi

- Shibboleth 1.3 deprecato *(Internet2 non aggiungerà più nuove funzionalità e non lo supporterà più da giugno 2010)*
- Shibboleth 2.x è indicato (e supportato) per tutte le nuove installazioni
  (e possibilmente anche per le vecchie!! ;-)
  - *+ semplice da installare e configurare*
  - *+ informazioni nei log*
  - *migliore gestione metadati*
  - *IdP Tomcat-only*
  - *...*

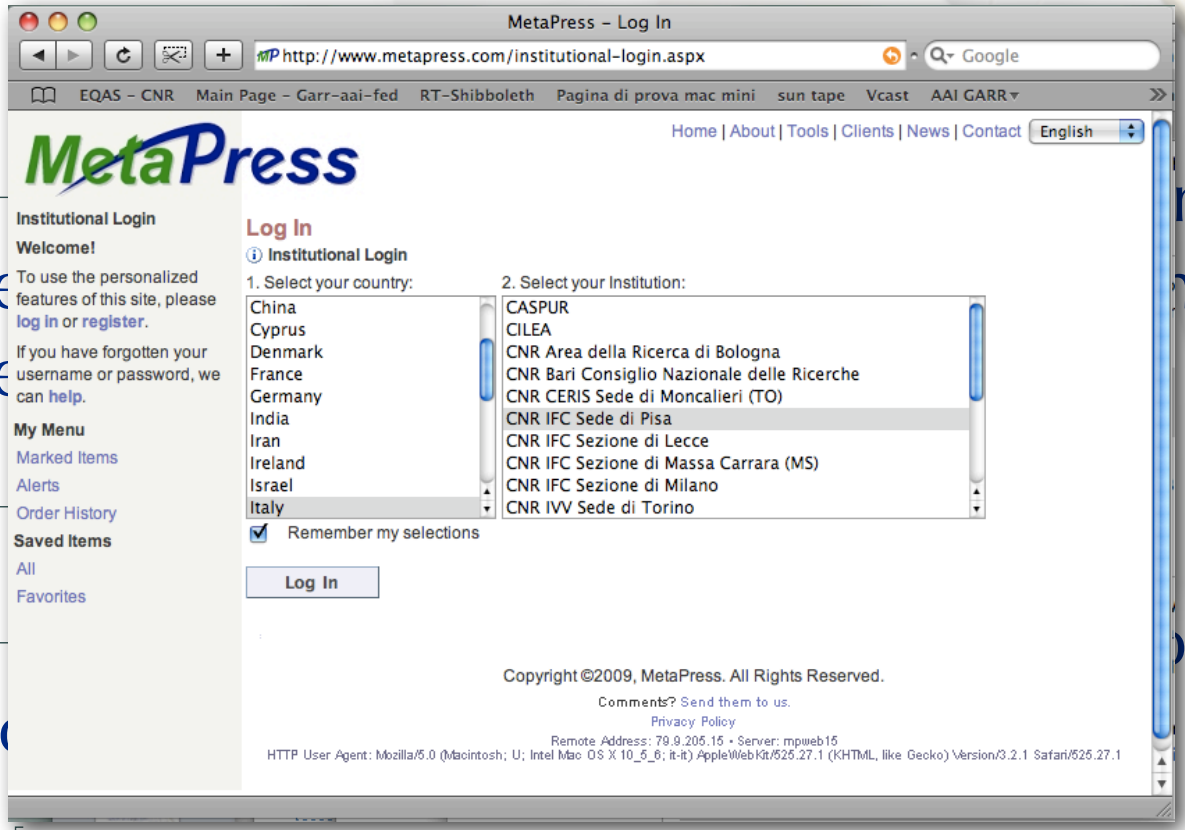
Applicativi

- Shibboleth 1.3 deprecato *(Internet2 non aggiungerà più nuove funzionalità e non lo supporterà più da giugno 2010)*
- Shibboleth 2.x è indicato (e supportato) per tutte le nuove installazioni
  (e possibilmente anche per le vecchie!! ;-)
  - *+ semplice da installare e configurare*
  - *+ informazioni nei log*
  - *migliore gestione metadati*
  - *IdP Tomcat-only*
  - ...

Discovery Service

- La Federazione gestisce e mantiene un servizio centrale di WAYF con cui l'utente seleziona la Home Organisation
- https://wayf.idem.garr.it
- Il servizio contiene l'elenco completo e le coordinate degli IdP in IDEM
- Alcuni fornitori possono avere un proprio WAYF

Discovery Service



- Alcuni fornitori possono avere un proprio WAYF

Nomenclatura

- IDEM garantisce l'uniformità della nomenclatura degli Enti aderenti
- Per i fornitori di servizi con un proprio WAYF, è compito della Federazione comunicare le corrette denominazioni
- Il processo di "normalizzazione" viene effettuato da IDEM all'atto dell'adesione

Metadati: cosa?

- Il file contiene le *"Carte d'Identità"* (in XML) dei partecipanti *"fidati"*
- È lo strumento con cui si costruiscono le relazioni di fiducia

NO altri metodi (verifica CRL ecc.)

Metadati: quando?

- Ogni partecipante, per verificare l'identità della controparte e comunicare, utilizza il relativo certificato contenuto nei metadati
  - Un SP parla solo con un IdP noto (i cui dati siano nel file dei MD)
  - Un IdP potrebbe parlare con un SP sconosciuto (se utilizzato il profilo *BrowserPOST* di SAML 1.1)

Metadati: contenuto

- Certificati
- Scope degli IdP *(es. ifc.cnr.it)*
  (deve corrispondere a quello degli attributi)
- Posizione (url) e tipologia dei componenti per lo scambio e l'utilizzo delle *assertion* dei partecipanti
- Descrizione testuale dei partecipanti

Metadati: i certificati

- È consentito l'utilizzo di certificati *self-signed* per la comunicazione SP-IdP (*back-channel*)
  - Il ruolo di Garante, affidato a una CA in una PKI, qui è svolto dalla Federazione
  - Equivale ad inserire la chiave pubblica, quindi minore tempo di verifica della controparte
  - Può essere rigenerato velocemente, quindi minore tempo di *downtime* in caso di compromissione del certificato

Metadati: gestione

- È necessario aggiornare i metadati al più ogni 24h
- È necessario comunicare il proprio frammento con messaggio firmato
- Il file è scaricabile solo con HTTPS, è fortemente consigliata la verifica della firma
- È consigliabile mantenere il file con diritti tali da non consentirne la modifica

Metadati: configurazione

- Consigliata per Shibboleth
  - Per IdP: `FileBackedHTTPMetadataProvider`
  - Per SP: `XML` (*reloadable resource*)
  - Per entrambi: `MetadataFilter` per la verifica della firma

Scopo del doc: ST - Attributi

- Standardizzare gli attributi scambiati fra i partecipanti alla Federazione. In particolare:
  - *denominazione*
  - *sintassi*
  - *semantica*

Scopo del doc: ST - Attributi

- Limitare l'uso degli attributi ai soli effettivamente necessari per l'erogazione del servizio
- Spetta comunque all'organizzazione limitare il rilascio (*Attribute Filter Policy*)

Denominazione e sintassi

- Sono state utilizzate denominazioni e sintassi degli schemi LDAP
  - LDAPv3 (RFC 4519)
  - Cosine
  - inetOrgPerson
  - eduPerson
  - SCHAC

L'insieme degli attributi

- Gli attributi sono suddivisi in:
  - **caratteristiche personali**: sn, givenName, cn, preferredLanguage ecc.
  - **contatti**: mail, telephoneNumber, mobile ecc.
  - **autorizzazione e accounting**: eduPersonScopedAffiliation, eduPersonTargetedID, eduPersonPrincipalName, eduPersonEntitlement

Notazione e metadati

- Necessari per comprendere le modalità di utilizzo dell'attributo
- È riportato l'identificativo dell'attributo, come urn, come indicato da SAML1 e SAML2, necessario per la configurazione
  - es.

    (SAML 1) urn:mace:dir:attribute-def:sn

    (SAML 2) urn:oid:2.5.4.4

Notazione: classificazione

- Gli attributi sono classificati come:
  - **obbligatori**: un IdP deve fornire questi attributi per poter fare parte della federazione
  - **raccomandati**: è fortemente raccomandato che un IdP fornisca questi attributi
  - **opzionali**: alcuni SP potrebbero richiedere questi attributi

Configurazione in Shibboleth

- Principali file lato IdP
  - `attribute-resolver.xml`: dove recuperare gli attributi ed eventualmente come modificarli
  - `attribute-filter.xml`: a chi rilasciare cosa
- Principali file lato SP
  - `attribute-map.xml`: estrarre gli attributi ed eventualmente rinominarli
  - `attribute-policy.xml`: rimaneggiare gli attributi

attribute-resolver

- Quasi tutti gli attributi possono essere definiti in Shibboleth 2 con il tipo *simple*

```
<resolver:AttributeDefinition id="cn" xsi:type="Simple"
    xmlns="urn:mace:shibboleth:2.0:resolver:ad"
    sourceAttributeID="cn">

  <resolver:Dependency ref="myLDAP" />

  <resolver:AttributeEncoder xsi:type="SAML1String"
      xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
      name="urn:mace:dir:attribute-def:cn" />

  <resolver:AttributeEncoder xsi:type="SAML2String"
      xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
      name="urn:oid:2.5.4.3" friendlyName="cn" />

</resolver:AttributeDefinition>
```

eduPersonPrincipalName

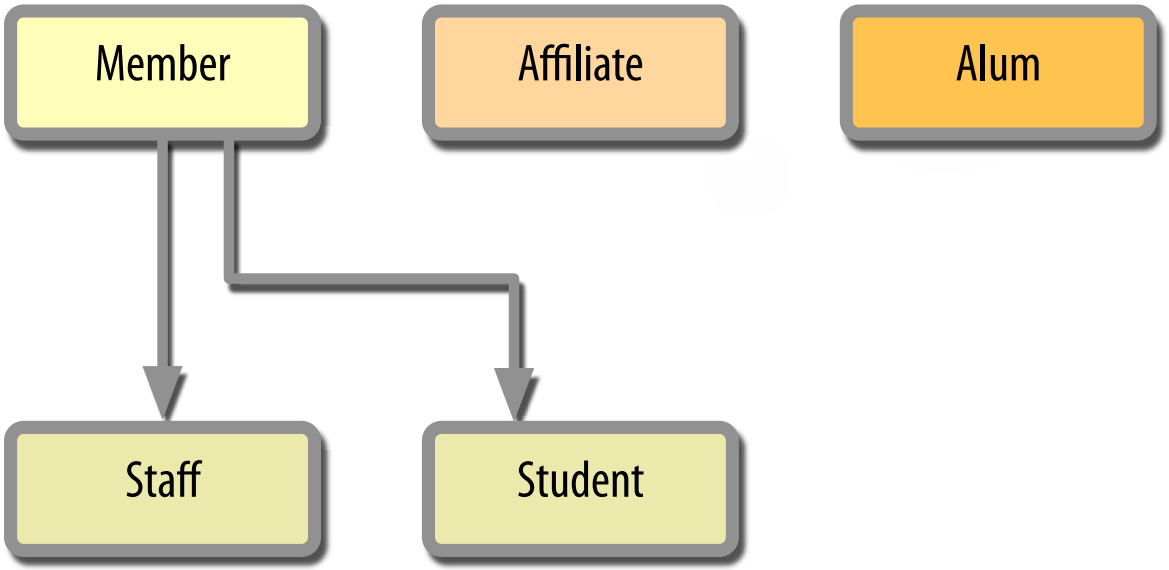
Configurazione con *scoped attribute*

```
<resolver:AttributeDefinition
      id="eduPersonPrincipalName" xsi:type="Scoped"
      xmlns="urn:mace:shibboleth:2.0:resolver:ad"
    scope="ifc.cnr.it" sourceAttributeID="uid">
    <resolver:Dependency ref="myLDAP" />

[...]
    <resolver:AttributeEncoder
        xsi:type="SAML2ScopedString"
        xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
        name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
        friendlyName="eduPersonPrincipalName" />
</resolver:AttributeDefinition>
```

eduPersonScopedAffiliation

- Definisce la relazione fra utente ed Organizzazione nel formato *affiliation@organisation*
- Organizzazione nel formato DNS
- L'affiliazione prevede (al momento) come valori possibili:



eduPersonScopedAffiliation

- Configurazione:
  - *scoped attribute*
  - potrebbe *dipendere* da eduPersonAffiliation definito come *mapped attribute*

```
<resolver:AttributeDefinition
    id="eduPersonScopedAffiliation"
    xsi:type="Scoped"
    xmlns="urn:mace:shibboleth:2.0:resolver:ad"
    scope="ifc.cnr.it">

  <resolver:Dependency ref="eduPersonAffiliation" />

        [...]
</resolver:AttributeDefinition>
```

eduPersonScopedAffiliation

eduPersonAffiliation *(mapped attribute)*

```
  [...]
       <DefaultValue>affiliate</DefaultValue>

   [...]

       <ValueMap>
            <ReturnValue>staff</ReturnValue>
            <SourceValue>dirigente tecnologo</SourceValue>
            <SourceValue>dirigente di ricerca</SourceValue>
[...]
            <SourceValue>ricercatore</SourceValue>
            <SourceValue>personale tecnico-amministrativo</SourceValue>
            <SourceValue>specializzando</SourceValue>
       </ValueMap>
[...]
       <ValueMap>
            <ReturnValue>staff</ReturnValue>
            <SourceValue>direttore</SourceValue>
            <SourceValue>dirigente tecnologo</SourceValue>
[...]
```

eduPersonTargetedID

- Implementa il *persistent identifier* di SAML 2
- Permette la gestione di sessioni in forma anonima
- IDEM utilizza la versione 2006 (conforme a SAML 2)
- Prevede *un* valore diverso (max 256 char) *per ogni* SP
- *NON* deve essere riassegnato
- Dovrebbe essere mantenuto più a lungo possibile
- Valori nel formato:

```
nameQualifier!SPNameQualifier!stringa_opaca
```

eduPersonTargetedID

- Non è memorizzato in LDAP ma gestito direttamente da Shibboleth in maniera:
  - Algoritmica
    - ComputedID Data Connector
  - Per memorizzazione
    - StoredID Data Connector

eduPersonTargetedID

- Gestione algoritmica (`ComputedID`)
  - SHA-1 di un attributo + salt
  - Più semplice da trattare
  - Variando l'attributo sorgente variano tutti i valori con conseguente perdita personalizzazioni
  - NON può essere identificativo utente
  - Deprecato in Shibboleth 2.x

eduPersonTargetedID

- Gestione per memorizzazione (`StoredID`)
  - Primo valore è generato come per ComputedID
  - Richiede tabella in DB
  - Consente la revoca e rigenerazione
  - Può essere usato come identificativo

eduPersonTargetedID

Configurazione lato IdP (`attribute-resolver.xml`)

definizione attributo:

```
<resolver:AttributeDefinition
   id="eduPersonTargetedID"
   xsi:type="SAML2NameID"
   xmlns="urn:mace:shibboleth:2.0:resolver:ad"
   nameIdFormat="urn:oasis:names:tc:SAML:
   2.0:nameid-format:persistent"
   sourceAttributeID="computedID">

   <resolver:Dependency ref="persistentID" />

   <resolver:AttributeEncoder
      xsi:type="SAML2XMLObject"
      xmlns="urn:mace:shibboleth:
      2.0:attribute:encoder"
      name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10"
      friendlyName="eduPersonTargetedID" />
</resolver:AttributeDefinition>
```

eduPersonTargetedID

- Configurazione lato IdP (`attribute-resolver.xml`)
  - definizione "connector" con ComputeID:

```
<resolver:DataConnector
   xsi:type="ComputedId"
   xmlns="urn:mace:shibboleth:2.0:resolver:dc"
   id="persistentID"
   generatedAttributeID="persistentID"
   sourceAttributeID="SOME_ID"
   salt="<stringa casuale>">

   <resolver:Dependency ref="myLDAP" />
</resolver:DataConnector>
```

eduPersonTargetedID

- Configurazione lato IdP (`attribute-resolver.xml`)
  - definizione "connector" con StoreID

```
<resolver:DataConnector
   xsi:type="StoredId"
   xmlns="urn:mace:shibboleth:2.0:resolver:dc"
   id="persistentID"
   sourceAttributeID="SOME_ID"
   salt="<stringa casuale>">

   <resolver:Dependency ref="myLDAP" />
   <ApplicationManagedConnection
      jdbcDriver="DRIVER_CLASS"
      jdbcURL="DATABASE_URL"
      jdbcUserName="DATABASE_USER"
      jdbcPassword="DATABASE_USER_PASSWORD" />

</resolver:DataConnector>
```

eduPersonTargetedID

Configurazione lato SP (`attribute-map.xml`):

```
<!-- First, the deprecated version: -->
<Attribute name="urn:mace:dir:attribute-def:eduPersonTargetedID"
    id="targeted-id">

    <AttributeDecoder xsi:type="ScopedAttributeDecoder"/>
</Attribute>

<!-- Second, the new version (note the OID-style name): -->
<Attribute name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10" id="persistent-id">

<AttributeDecoder xsi:type="NameIDAttributeDecoder"
    formatter="$NameQualifier!$SPNameQualifier!$Name"/>
</Attribute>

<!-- Third, the SAML 2.0 NameID Format: -->
<Attribute name="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
    id="persistent-id">

<AttributeDecoder xsi:type="NameIDAttributeDecoder"
    formatter="$NameQualifier!$SPNameQualifier!$Name"/>
</Attribute>
```

eduPersonTargetedID

Configurazione lato SP (`attribute-map.xml`):

```
<!-- First, the deprecated version: -->
<Attribute name="urn:mace:dir:attribute-def:eduPersonTargetedID"
    id="targeted-id">

    <AttributeDecoder xsi:type="ScopedAttributeDecoder"/>
</Attribute>

<!-- Second, the new version (note the OID-style name): -->
<Attribute name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10" id="persistent-id">

<AttributeDecoder xsi:type="NameIDAttributeDecoder"
    formatter="$NameQualifier!$SPNameQualifier!$Name"/>
</Attribute>

<!-- Third, the SAML 2.0 NameID Format: -->
<Attribute name="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
    id="persistent-id">

<AttributeDecoder xsi:type="NameIDAttributeDecoder"
    formatter="$NameQualifier!$SPNameQualifier!$Name"/>
</Attribute>
```

eduPersonEntitlement

- metodo di autorizzazione *"esplicita"*
  - es. "hanno diritto di accedere alla risorsa x solo gli utenti per cui l'attributo contiene la uri y"
    (y potrebbe essere l'identificativo di x)
  - es.:
    http://nilde.bo.cnr.it
    urn:mace:cnr.it:services:puma:docs:1234
- in questo modo è l'IdP che autorizza l'accesso a determinate risorse

Attribute Filter

- Si configura (di default sull'IdP) in `attribute-filter.xml`
- Insieme di regole per SP/attributo (o gruppi)
- È possibile utilizzare più file configurando service.xml
- IDEM "potrebbe" mettere a disposizione un file con attributi/SP in Federazione

Attribute Map

- Elenco di regole per l'estrazione degli attributi dalle asserzioni
- es.

```
<Attribute
   name="urn:mace:dir:attribute-def:eduPersonScopedAffiliation"
   id="affiliation">
   <AttributeDecoder
      xsi:type="ScopedAttributeDecoder"
      caseSensitive="false"/>
</Attribute>

<Attribute name="urn:oid:1.3.6.1.4.1.5923.1.1.1.9"
      id="affiliation">
   <AttributeDecoder
      xsi:type="ScopedAttributeDecoder"
      caseSensitive="false"/>
</Attribute>
```

Ringraziamenti

- Per la collaborazione alla redazione dei documenti:
  - Giancarlo Birello
  - Massimo Ianigro
  - Maria Laura Mantovani
  - Claudio Marotta
- Per il loro contributo
  - Francesco Malvezzi
  - Barbara Monticini

Domande?