Configurazione Shibboleth per l'adesione ai profili di garanzia

Simone Lanzarini
CINECA

Adesione ai profili di garanzia – Cosa serve fare sul IDP

Affinché una organizzazione possa avvalersi dei profili di garanzia delle identità digitali della Federazione IDEM occorre che il proprio Identity Provider:

1. Rilasci l'attributo **eduPersonAssurance** (SAML 2.0) o il claim **edu_person_assurance** (OIDC)

2. Sappia gestire richieste SP contenenti **AuthnContextClassRef** (SAML 2.0) o acr (OIDC)
   - Per i profili IDEM-P0 ed IDEM-P1
     - https://refeds.org/profile/sfa (OBBLIGATORIO)
     - https://refeds.org/profile/mfa (OPZIONALE)
   - Per i profili IDEM-P2 ed IDEM-P3
     - https://refeds.org/profile/mfa (OBBLIGATORIO)

Rilascio dell'attributo **eduPersonAssurance**

Definizione attributo eduPersonAssurance

conf/attribute-resolver.xml

Definizione dell'attributo su attribute-resolver:

```
<AttributeDefinition id="eduPersonAssurance" xsi:type="Simple">
    <InputDataConnector ref="myConnector" attributeNames="assurance"/>
 </AttributeDefinition>
```

Per il reperimento dell'attributo ci sono varie opzioni ...

Reperimento attributo – Caso 1

conf/attribute-resolver.xml

Caso semplice: tutti gli utenti dell'organizzazione hanno lo stesso LoA. In questo caso è possibile definire un **connettore statico**

```
<AttributeDefinition id="eduPersonAssurance" xsi:type="Simple">
    <InputDataConnector ref="staticAttributes" attributeNames="assurance"/>
</AttributeDefinition>
```

Definizione del data connector per utente con profilo **IDEM-P1**:

```
<DataConnector id="staticAttributes" xsi:type="Static">
    <Attribute id="assurance">
        <Value>https://refeds.org/assurance</Value>
        <Value>https://refeds.org/assurance/ID/unique</Value>
        <Value>https://refeds.org/assurance/ID/eppn-unique-no-reassign</Value>
        <Value>https://refeds.org/assurance/IAP/low</Value>
        <Value>https://refeds.org/assurance/IAP/medium</Value>
        <Value>https://refeds.org/assurance/ATP/ePA-1m</Value>
        <Value>https://idem.garr.it/af/IDEM-P0</Value>
        <Value>https://idem.garr.it/af/IDEM-P1</Value>
        <Value>https://refeds.org/profile/cappuccino</Value>
    </Attribute>
</DataConnector>
```

Reperimento attributo – Caso 2

conf/attribute-resolver.xml

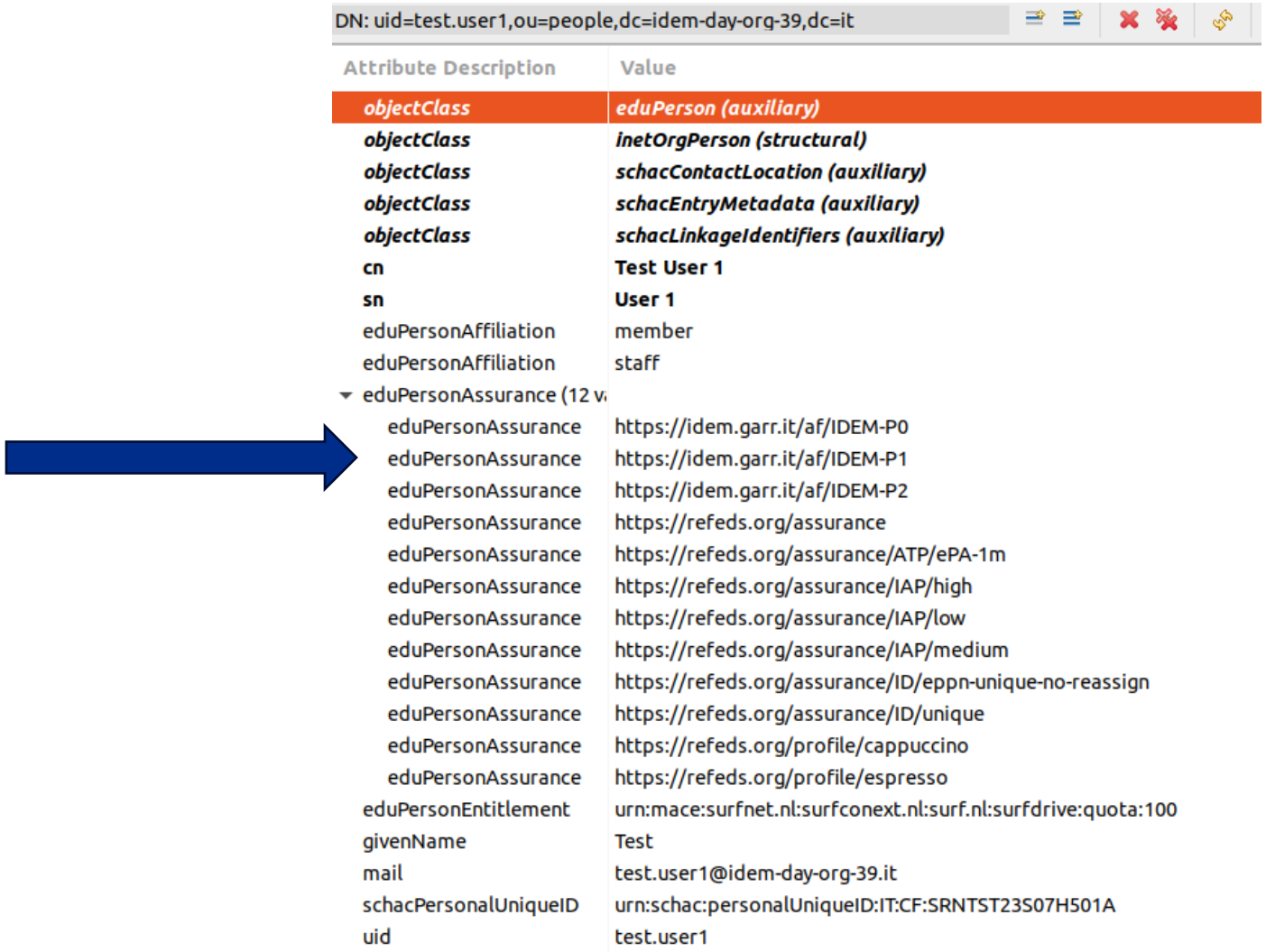
Non tutti gli utenti dell'organizzazione hanno lo stesso LoA, si configura il reperimento dell'attributo dal **connettore LDAP**

```
<AttributeDefinition id="eduPersonAssurance" xsi:type="Simple">
    <InputDataConnector ref="myLDAP" attributeNames="eduPersonAssurance"/>
</AttributeDefinition>
```

Reperimento attributo – Caso 2

conf/attribute-resolver.xml

Esempio di record LDAP con valorizzazione dell'attributo eduPersonAssurance **IDEM-P2**:



DN: uid=test.user1,ou=people,dc=idem-day-org-39,dc=it

Attribute Description	Value
objectClass	*eduPerson (auxiliary)*
objectClass	*inetOrgPerson (structural)*
objectClass	*schacContactLocation (auxiliary)*
objectClass	*schacEntryMetadata (auxiliary)*
objectClass	*schacLinkageIdentifiers (auxiliary)*
cn	**Test User 1**
sn	**User 1**
eduPersonAffiliation	member
eduPersonAffiliation	staff
eduPersonAssurance (12 v	
eduPersonAssurance	https://idem.garr.it/af/IDEM-P0
eduPersonAssurance	https://idem.garr.it/af/IDEM-P1
eduPersonAssurance	https://idem.garr.it/af/IDEM-P2
eduPersonAssurance	https://refeds.org/assurance
eduPersonAssurance	https://refeds.org/assurance/ATP/ePA-1m
eduPersonAssurance	https://refeds.org/assurance/IAP/high
eduPersonAssurance	https://refeds.org/assurance/IAP/low
eduPersonAssurance	https://refeds.org/assurance/IAP/medium
eduPersonAssurance	https://refeds.org/assurance/ID/eppn-unique-no-reassign
eduPersonAssurance	https://refeds.org/assurance/ID/unique
eduPersonAssurance	https://refeds.org/profile/cappuccino
eduPersonAssurance	https://refeds.org/profile/espresso
eduPersonEntitlement	urn:mace:surfnet.nl:surfconext.nl:surf.nl:surfdrive:quota:100
givenName	Test
mail	test.user1@idem-day-org-39.it
schacPersonalUniqueID	urn:schac:personalUniqueID:IT:CF:SRNTST23S07H501A
uid	test.user1

Reperimento attributo – Caso 3

conf/attribute-resolver.xml

L'informazione necessaria a ricavare il LoA è presente su LDAP, con una semantica specifica dell'ente.
Definiamo un **mapped attribute**

```
<AttributeDefinition id="eduPersonAssurance" xsi:type="Mapped">
    <InputDataConnector ref="myLDAP" attributeNames="myCustomEduPersonAssurance"/>
        <ValueMap>
            <ReturnValue>https://refeds.org/assurance/IAP/low</ReturnValue>
            <SourceValue>MyCustomValue1</SourceValue>
            <SourceValue>MyCustomValue2</SourceValue>
        </ValueMap>
        <ValueMap>
            <ReturnValue>https://refeds.org/assurance/IAP/medium</ReturnValue>
            <SourceValue>MyCustomValue3</SourceValue>
       </ValueMap>
        <ValueMap>
            <ReturnValue>https://refeds.org/assurance/ID/unique</ReturnValue>
            <SourceValue>MyCustomValue4</SourceValue>
            <SourceValue>MyCustomValue5</SourceValue>
        </ValueMap>
        <ValueMap>
            <ReturnValue>https://refeds.org/assurance/ID/eppn-unique-no-reassign</ReturnValue>
            <SourceValue>MyCustomValue6</SourceValue>
        </ValueMap>
</AttributeDefinition>
```

Rif: https://shibboleth.atlassian.net/wiki/spaces/IDP4/pages/1265631555/MappedAttributeDefinition

Codifica attributo

conf/attributes/eduperson.xml

Sull'attribute registry va definita sia la codifica **SAML** che quella **OIDC**:

```
<bean parent="shibboleth.TranscodingProperties">
    <property name="properties">
        <props merge="true">
            <prop key="id">eduPersonAssurance</prop>
            <prop key="transcoder">SAML2StringTranscoder OIDCStringTranscoder</prop>
            <prop key="saml2.name">urn:oid:1.3.6.1.4.1.5923.1.1.1.11</prop>
            <prop key="saml2.encodeType">false</prop>
            <prop key="oidc.name">edu_person_assurance</prop>
            <prop key="displayName.en">Assurance level</prop>
            <prop key="displayName.de">Vertrauensgrad</prop>
            <prop key="displayName.fr">Niveau de confiance</prop>
            <prop key="displayName.it">Livello di sicurezza</prop>
            <prop key="displayName.ja">保証レベル</prop>
            <prop key="description.en">Set of URIs that assert compliance with specific standards for identity assurance.</prop>
            <prop key="description.de">URIs die eine gewisse Zusicherung für spezifische Standards des Vertrauens beinhalten</prop>
            <prop key="description.fr">Un ensemble d'URI qui attestent la conformité selon un standard pour les niveaux d'assurance d'identités</prop>
            <prop key="description.it">Un insieme di URI che asseriscono l'osservanza dei livelli di sicurezza richiesti</prop>
            <prop key="description.ja">IDの保証レベルに関して特定の基準に準拠していることを示すURI</prop>
        </props>
    </property>
</bean>
```

Rilascio attributo

conf/attribute-filter.xml
conf/oidc-attribute-filter.xml

Impostiamo il filter SAML in modo che l'attributo venga rilasciato agli SP che lo richiedono nei propri metadata (*)

```
<AttributeFilterPolicy id="metadata_based_release">
    <PolicyRequirementRule xsi:type="ANY"/>

    <AttributeRule attributeID="eduPersonAssurance">
        <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true"  attributeName="urn:oid:1.3.6.1.4.1.5923.1.1.1.11"/>
    </AttributeRule>

</AttributeFilterPolicy>
```

Analogamente impostiamo il rilascio del claim OIDC nello scope "profile"

```
<AttributeFilterPolicy id="OPENID_SCOPE_PROFILE">
   <PolicyRequirementRule xsi:type="oidc:OIDCScope" value="profile" />

        <AttributeRule attributeID="eduPersonAssurance">
            <PermitValueRule xsi:type="ANY" />
        </AttributeRule>
        [...]
```

(*) Rif: https://shibboleth.atlassian.net/wiki/spaces/IDP4/pages/1265631521/AttributeInMetadataConfiguration

Gestione dei contesti di autenticazione

Siamo quasi nel 2024
ed il tuo idp ancora
non supporta la MFA?

Se il tuo IDP non supporta la MFA
gli utenti non potranno accedere a
servizi che richiedono il profilo
IDEM-P2 o IDEM-P3

Serve la MFA

Occorre configurare l'idp affinchè supporti l'autenticazione a più fattori

Last, but not least

conf/authn/general-authn.xml
conf/authn/authn.properties

Una volta configurato l'idp per gestire la MFA non dimenticare di mappare gli authContextClassRef Refeds sfa ed mfa

```
<property name="supportedPrincipals">
<list>
    <bean parent="shibboleth.SAML2AuthnContextClassRef" c:classRef="https://refeds.org/profile/sfa"/>
    <bean parent="shibboleth.OIDCAuthnContextClassReference" c:classRef="https://refeds.org/profile/sfa"/>
    <bean parent="shibboleth.SAML2AuthnContextClassRef" c:classRef="https://refeds.org/profile/mfa"/>
    <bean parent="shibboleth.OIDCAuthnContextClassReference" c:classRef="https://refeds.org/profile/mfa"/>
 </list>
</property>
```

Grazie

Simone Lanzarini
s.lanzarini@cineca.it