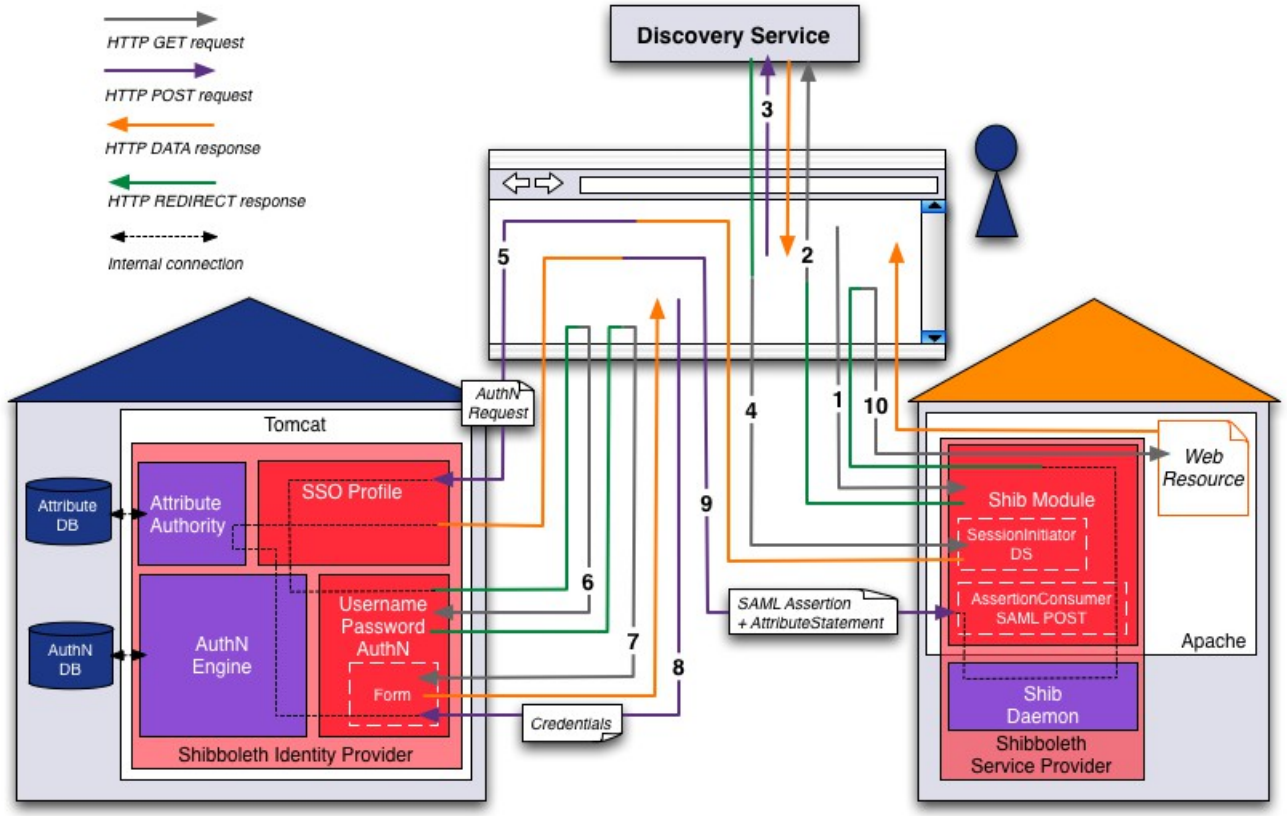
Il rilascio degli Attributi

MARCO PANELLA

Shibboleth Login Procedure



http://www.switch.ch/aai/demo/2/expert.html

Attributo

- Pezzo di informazione su un utente
- Ha un identificatore univoco (nome) cui corrispondono uno o più valori
- Categorie di attributi
  - Caratteristiche personali
  - Contatti del soggetto
  - Dati per l'autorizzazione e l'accounting

Gli attributi nella Federazione

- La Federazione ha definito un insieme minimo di attributi
  - Il documento ST_A è lo standard di IDEM:
  - Definisce la denominazione, la sintassi, la semantica degli attributi standard
- IdP e SP possono concordare lo scambio di altri attributi
  - L'IdP comunque deve sempre verificare le ragioni per le quali viene richiesto ogni attributo che possa veicolare dati personali

Normativa

- D.lgs. 30 giugno 2003, n. 196
  - Codice in materia di protezione dei dati personali
- La Federazione definisce tre livelli
  - Obbligatori, Raccomandati, Opzionali
  - Anche gli obbligatori non possono essere considerati anonimi in tutte le circostanze
    - Es. IdP con pochi utenti
- Scelta dell'utente se consentire l'invio dei dati personali all'SP

Attributi obbligatori

- EduPersonScopedAffiliation
  - Tipo di affiliazione
  - Organizzazione di appartenenza
- eduPersonTargetedId
  - Individua univocamente (in forma pseudo-anonima) l'utente
    - Es. Memorizzare le preferenze dell'utente

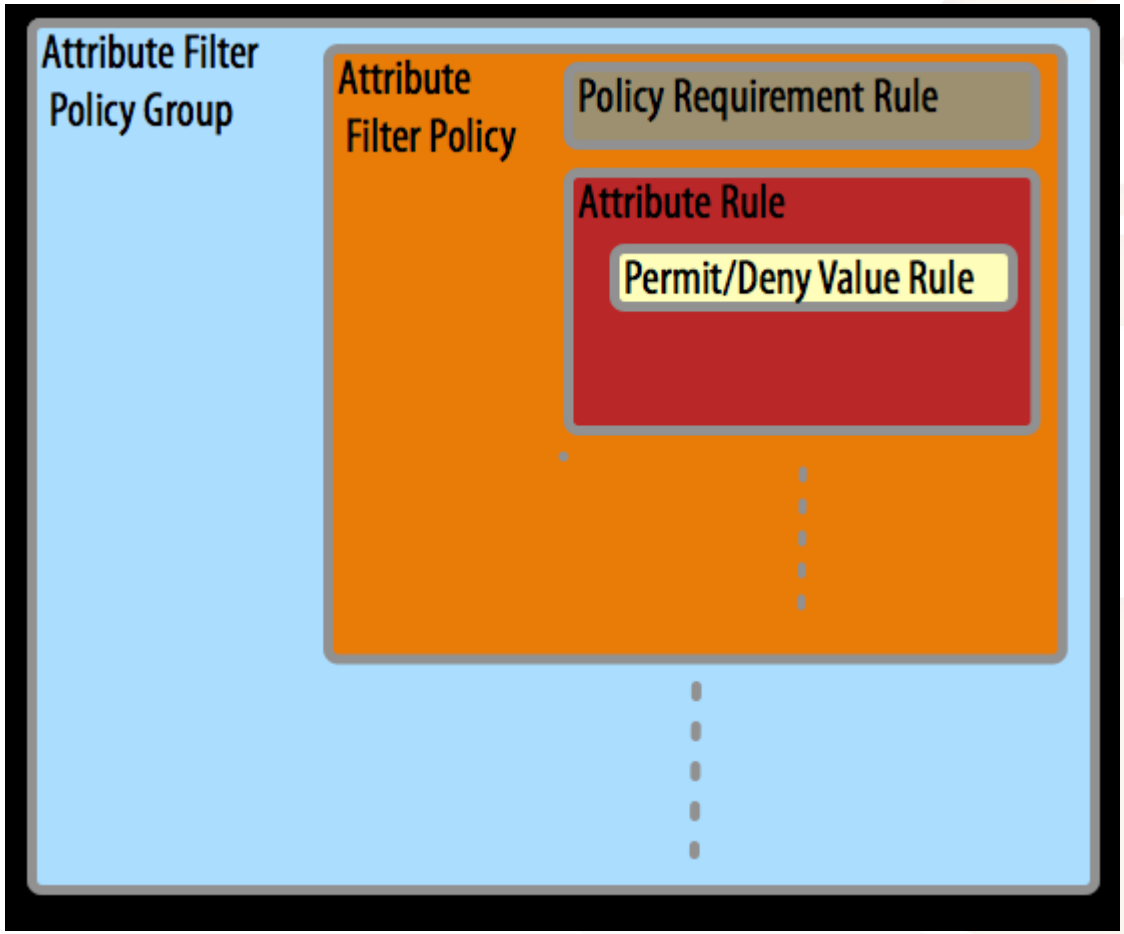
Configurazione di shibboleth

- ${SHIB_HOME}/conf/attribute-filter.xml
- Serie di Attribute Filter Policy
  - Costituiscono un Attribute Filter Policy Group
  - Elemento che definisce la policy
- Ogni policy è costituita da
  - Una e una sola Policy Requirement Rule
  - Una o più Attribute Rule
    - Composta da una e una sola Permit o Deny Value

Configurazione di Shibboleth

<AttributeFilterPolicy id=" *NOME DELLA POLICY* ">
<!-- Policy Requirement Rule would go here -->
<!-- Attribute Rules would go here -->
</AttributeFilterPolicy>

Si possono utilizzare anche più file distinti da indicare in ${SHIB_HOME}/conf/service.xml



© R.Conte
ST_attributi

Policy Requirement Rule

- Una ed una sola per ogni Policy
- Definisce se la policy è attiva oppure no rispetto alla particolare richiesta
- Si possono concatenare (AND e/o OR) più regole semplici

Attribute Rule

- Definisce, per un singolo attributo, se e quali valori sono rilasciati all'interno della policy
- Ogni regola contiene una ed una sola
  - Permit o Deny Value Rule

```
<AttributeRule attributeID="transientId">
<!-- Permit/Deny Rules go here -->
</AttributeRule>
```

Permit o Deny Value Rule

- Definisce quali valori del particolare attributo sono rilasciati, qualora la Policy Requirement Rule fosse vera
- Si possono concatenare (AND e/o OR) diverse basic:Rule

Criteri utilizzabili 1

ANY - Always evaluates to true

AND - Evaluates to true if all contained rules are true

OR - Evaluated to true if any contained rule is true

NOT - Evaluates to true if the contained rule evaluates to false

AttributeRequesterString - Evaluates to true if the attribute requester's entity ID matches a given string

AttributeIssuerString - Evaluates to true if the attribute issuer's entity ID matches a given string

PrincipalNameString - Evaluates to true if the user's principal name matches a given string

AuthenticationMethodString - Evaluates to true if the method used to authenticate the user matches a given string

AttributeValueString - Evaluates to true if the value of a given attribute matches a given string

AttributeScopeString - Evaluates to the true if the scope of a value of a given attribute matches a given string

Criteri utilizzabili 2

* AttributeRequesterRegex - Evaluates to true if the attribute requester's entity ID matches a given regular expression

* AttributeIssuerRegex - Evaluates to true if the attribute issuer's entity ID matches a given regular expression

* PrincipalNameRegex - Evaluates to true if the user's principal name matches a given regular expression

* AuthenticationMethodRegex - Evaluates to true if the method used to authenticate the user matches a given regular expression

* AttributeValueRegex - Evaluates to true if the value of a given attribute matches a given regular expression

* AttributeScopeRegex - Evaluates to the true if the scope of a value of a given attribute matches a given regular expression

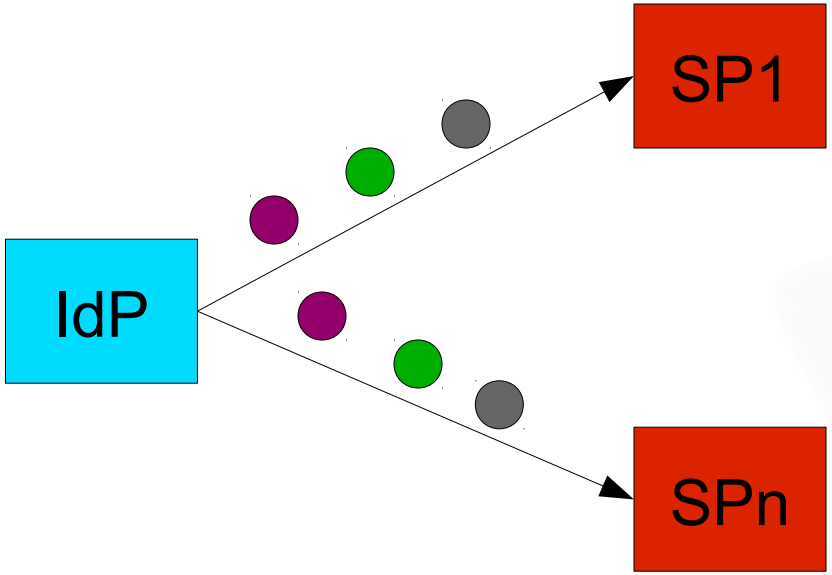
* Script - Evaluates a scriptlet to determine if the rule evaluates to true

* AttributeRequesterInEntityGroup - Evaluates to true if the attribute requester is defined within a given entity group in SAML metadata

* AttributeIssuerInEntityGroup - Evaluates to true if the attribute issuer is defined within a given entity group in SAML metadata

Esempio 1

- Attributo rilasciato a chiunque, qualunque valore esso assuma

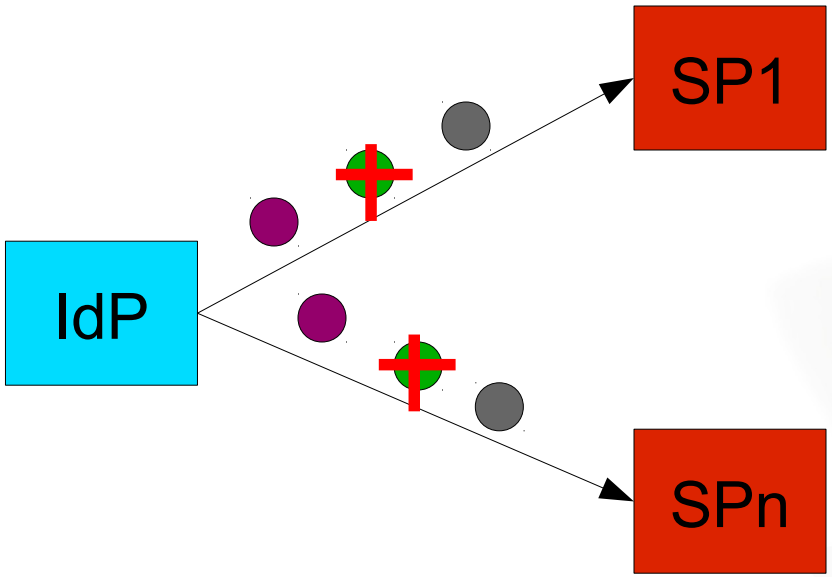


Esempio 1

```
<AttributeFilterPolicy id="releaseToAnyone">
    <PolicyRequirementRule xsi:type="basic:ANY" />
    <AttributeRule attributeID="transientId">
        <PermitValueRule xsi:type="basic:ANY" />
    </AttributeRule>
</AttributeFilterPolicy>
```

Esempio 2

- Attributo rilasciato a chiunque, solo per alcuni valori ben definiti

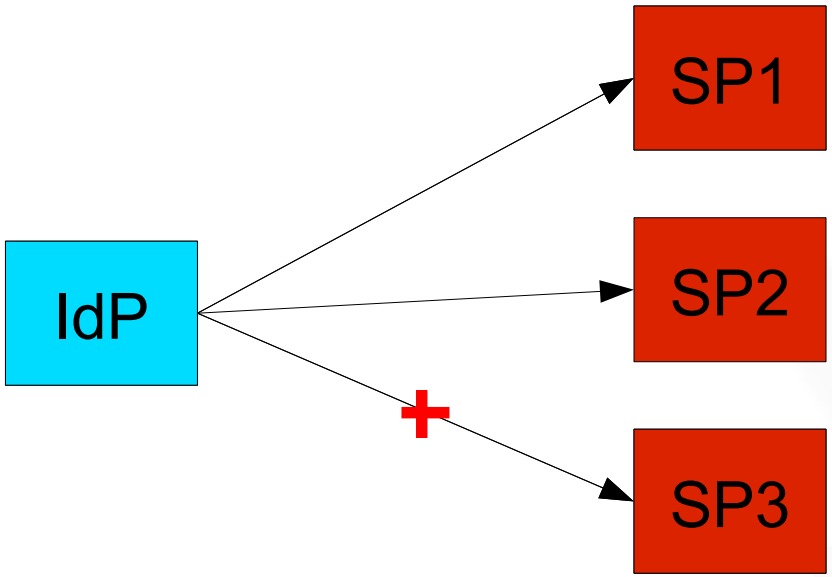


Esempio 2

```
<AttributeFilterPolicy id="releaseToAnyone">
   <PolicyRequirementRule xsi:type="basic:ANY" />
      <AttributeRule attributeID="eduPersonAffiliation">
      <PermitValueRule xsi:type="basic:OR">
         <basic:Rule xsi:type="basic:AttributeValueString" value="faculty"
ignoreCase="true"/>
                  …
         <basic:Rule xsi:type="basic:AttributeValueString" value="alum"
ignoreCase="true"/>
      </PermitValueRule>
   </AttributeRule>
</AttributeFilterPolicy>
```

Esempio 3

- Rilasciare un attributo a due particolari SP



Esempio 3

```
<AttributeFilterPolicy id="releaseToTwoSP">
    <PolicyRequirementRule xsi:type=”basic:OR”>
        <basic:Rule xsi:type="basic:AttributeRequesterString"
value=”http://sp1.example.org” />
        <basic:Rule xsi:type="basic:AttributeRequesterString"
value=”http://sp2.example.org” />
    </PolicyRequirementRule>
     <AttributeRule attributeID="mail">
          <PermitValueRule xsi:type="basic:ANY” />
     </AttributeRule>
</AttributeFilterPolicy>
```

Esempio 4

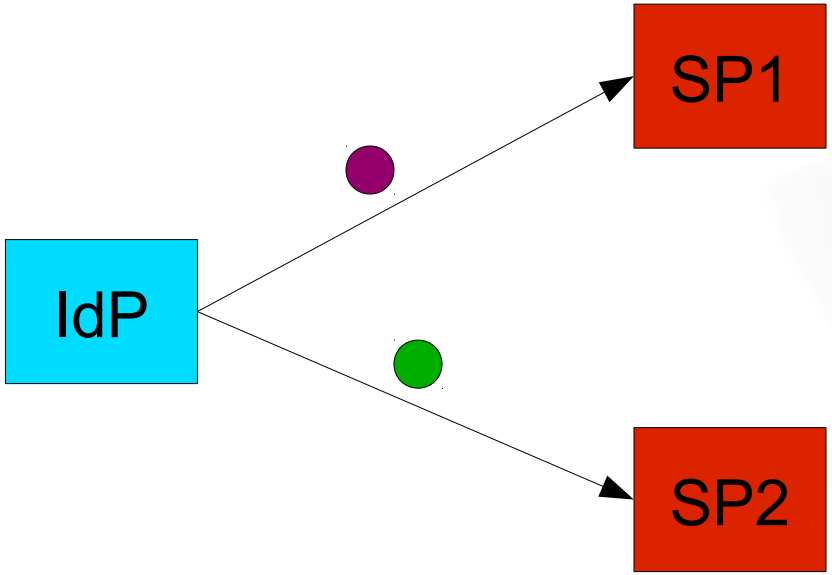
- Negare un attributo in funzione di un altro
  - Deny ha la precedenza sulla Permit

Esempio 4

```
<AttributeFilterPolicy id="denyOnPrivacyAttribute">
    <PolicyRequirementRule xsi:type="basic:AttributeValueString"
attributeID=”privacyAttr” value=”true” />
      <AttributeRule attributeID="givenname">
          <DenyValueRule xsi:type="basic:ANY"/>
      </AttributeRule>
      <AttributeRule attributeID="sn">
          <DenyValueRule xsi:type="basic:ANY"/>
      </AttributeRule>
</AttributeFilterPolicy>
```

Attributo multivalore-multiscopo

- Alcuni attributi possono contenere valori multipli
- Rilasciare un valore di un attributo ad un SP e un altro valore ad un secondo SP



Attributo multivalore-multiscopo

```
<AttributeFilterPolicy id="ISI">
   <PolicyRequirementRule xsi:type="basic:AttributeRequesterString"
value=”https://sp.tshhosting.com/shibboleth” />
     <AttributeRule attributeID="eduPersonEntitlement">
        <PermitValueRule xsi:type="basic:AttributeValueString" value="urn:mace:dir:entitlement:common-
lib-terms" ignoreCase="true" />
     </AttributeRule>
</AttributeFilterPolicy>
<AttributeFilterPolicy id="TCS">
   <PolicyRequirementRule xsi:type="basic:AttributeRequesterString" value=”https://tcs-
personal.garr.it/simplesamlphp/module.php/saml/sp/metadata.php/default-sp” />
     <AttributeRule attributeID="eduPersonEntitlement">
        <PermitValueRule xsi:type="basic:OR”>
           <basic:Rule xsi:type=”basic:AttributeValueString"
value="urn:mace:urn:mace:terena.org:tcs:personal-user" ignoreCase="true" />
           <basic:Rule xsi:type=”basic:AttributeValueString"
value="urn:mace:urn:mace:terena.org:tcs:science-user" ignoreCase="true" />
        </PermitValueRule>
     </AttributeRule>
</AttributeFilterPolicy>
```

Wiki CASPUR

```
<AttributeFilterPolicy id="wiki_caspur">
    <PolicyRequirementRule xsi:type="basic:AttributeValueString"
AttributeRequesterString=”https://aai.caspur.it/shibboleth” />
      <AttributeRule attributeID="eppn">
          <PermitValueRule xsi:type="basic:ANY"/>
      </AttributeRule>
      <AttributeRule attributeID="mail">
          <PermitValueRule xsi:type="basic:ANY"/>
      </AttributeRule>
</AttributeFilterPolicy>
```

vConf GARR

```
<AttributeFilterPolicy id="vconf_garr”>
   <PolicyRequirementRule xsi:type="basic:AttributeValueString"
AttributeRequesterString=”https://vconf.garr.it/shibboleth” />
     <AttributeRule attributeID="sn">
        <PermitValueRule xsi:type="basic:ANY"/>
     </AttributeRule>
     <AttributeRule attributeID="givenname">
        <PermitValueRule xsi:type="basic:ANY"/>
     </AttributeRule>
     <AttributeRule attributeID="mail">
        <PermitValueRule xsi:type="basic:ANY"/>
     </AttributeRule>
</AttributeFilterPolicy>
```

Google 1

```
<AttributeFilterPolicy id="release_to_anyone">
      <PolicyRequirementRule xsi:type="basic:NOT"><basic:Rule xsi:type="basic:AttributeRequesterString"
value="google.com" />   </PolicyRequirementRule>
      <AttributeRule attributeID="transientId">          <PermitValueRule xsi:type="basic:ANY" />       </AttributeRule>
      <AttributeRule attributeID="eduPersonTargetedID">    <PermitValueRule xsi:type="basic:ANY" />       </AttributeRule>
      <AttributeRule attributeID="eduPersonAffiliation">
         <PermitValueRule xsi:type="basic:OR">
            <basic:Rule xsi:type="basic:AttributeValueString" value="faculty" ignoreCase="true" />
            <basic:Rule xsi:type="basic:AttributeValueString" value="student" ignoreCase="true" />
            <basic:Rule xsi:type="basic:AttributeValueString" value="staff" ignoreCase="true" />
            <basic:Rule xsi:type="basic:AttributeValueString" value="alum" ignoreCase="true" />
            <basic:Rule xsi:type="basic:AttributeValueString" value="member" ignoreCase="true" />
            <basic:Rule xsi:type="basic:AttributeValueString" value="affiliate" ignoreCase="true" />
            <basic:Rule xsi:type="basic:AttributeValueString" value="employee" ignoreCase="true" />
            <basic:Rule xsi:type="basic:AttributeValueString" value="library-walk-in" ignoreCase="true" />
         </PermitValueRule>
      </AttributeRule>
      <AttributeRule attributeID="eduPersonScopedAffiliation">  <PermitValueRule xsi:type="basic:ANY" />   </AttributeRule>
   </AttributeFilterPolicy>
```

Google 2

```
<AttributeFilterPolicy id="google_apps">
        <PolicyRequirementRule xsi:type="basic:AttributeRequesterString"
value="google.com" />
         <AttributeRule attributeID="principal">
            <PermitValueRule xsi:type="basic:ANY" />
        </AttributeRule>
    </AttributeFilterPolicy>
```

Riferimenti

- Wiki di Internet2
- Documento "Specifiche Tecniche Attributi"
- Presentazione di switch.ch