THE ITALIAN RESEARCH & EDUCATION NETWORK | Consortium GARR

Attribute Release Management

come le Organizzazioni possono rilasciare gli attributi personali rispettando la legge privacy

Barbara Monticini

Quinto Convegno IDEM - Lecce 13 - 15 Maggio 2015

Sommario

- Data Protection Code of Conduct (CoC)
- Gli elementi «Entity Category»
- Profilo SAML 2.0 per il Data Protection CoC
- Ricette per le Home Organization
- Implementare il rilascio sicuro di attributi agli SP CoC-compliant
- Riferimenti

GEANT Data Protection Code of Conduct (CoC)

Propone un **approccio** per applicare i requisiti delle direttive EU sulla protezione dei dati nell'ambito delle federazioni di identità.

Definisce delle **regole** per gli SP che intendono ricevere gli attributi dalle Home Organization

Auspica una maggiore «**apertura**» da parte delle Home Organization verso gli SP conformi al Codice di Condotta

Regole CoC per Service Provider

[**Legal compliance**]

[**Purpose limitation**]

[**Data minimisation**] to minimise the Attributes requested from a Home Organisation to those that are adequate, relevant and not excessive for enabling access to the service

[**Data retention**]

[**Third parties**]

Gli elementi «Entity Category»

Sono elementi SAML 2.0 usati per annunciare la conformità di una entità (SP/IdP) al Codice di Condotta:

- Semantica per Service Provider:
  - Sottostà alle leggi EU sulla protezione dei dati
  - Rispetta il Codice di Condotta
  - E' conforme al profilo SAML 2 per DP CoC
- Semantica per Identity Provider:
  - Rilascia gli attributi richiesti agli SP che rispettano il CoC senza ulteriori interventi amministrativi

Profilo SAML 2.0 per il Data Protection Code of Conduct

Valore (URI) usato come Attribute Value:

http://www.geant.net/uri/dataprotection-code-of-conduct/v1

Requisiti nei metadati per gli SP CoC:

- Entity Category attribute
- mdui:PrivacyStatement (MUST)
- mdui:DisplayName/Description (RECOMM.)
- Attributi richiesti (MUST)

Requisiti nei metadati per gli IdP CoC:

- Entity Category support attribute

Ricette per le Home Organization

1. Prendere visione del documento **GÉANT Data Protection Code of Conduct for SPs**
2. Definire una **lista completa degli attributi** che l'Organizzazione è disposta a rilasciare agli SP rispettosi del Code of Conduct
3. Capire se la Home Organisation ha **intenzione** di rilasciare attributi agli SP rispettosi del CoC
4. Valutare l'introduzione nell'IdP di un meccanismo di **consenso informato per l'utente**
5. Configurare l'IdP per **rilasciare** agli SP conformi al CoC solo ed esattamente gli attributi che questi richiedono

Quali attributi?

Evitare il rilascio di «Dati sensibili»

Essere troppo restrittivi può portare il SP a negare l'accesso all'utente

Il Profilo di eduGAIN raccomanda il rilascio di:

- displayName, cn, mail, eduPersonAffiliation, eduPersonScopedAffiliation, eduPersonPrincipalName, SAML2 Persistent NameID (eduPersonTargetedID), schacHomeOrganization and schacHomeOrganizationType

Se un SP richiede solo un determinato valore per un attributo rilasciare solo quel valore

Configurazione per IdP v2.3.4

Rilascio di un insieme **fisso** di attributi a SP CoC

```
<AttributeFilterPolicy id="releaseToCoC">
  <PolicyRequirementRule
xsi:type="saml:AttributeRequesterEntityAttributeExactMatch"
  attributeName="http://macedir.org/entity-category"
  attributeValue="http://www.geant.net/uri/dataprotection-code-of-conduct/v1"/>

    <AttributeRule attributeID="displayName">
        <PermitValueRule xsi:type="basic:ANY"/>
    </AttributeRule>
    <AttributeRule attributeID="email">
        <PermitValueRule xsi:type="basic:ANY"/>
    </AttributeRule>
    <AttributeRule attributeID="eduPersonPrincipalName">
        <PermitValueRule xsi:type="basic:ANY"/>
    </AttributeRule>
    <AttributeRule attributeID="schacHomeOrganization">
        <PermitValueRule xsi:type="basic:ANY"/>
    </AttributeRule>
</AttributeFilterPolicy>
```

Configurazione per IdP v2.3.4

Rilascio di un insieme **dinamico** di attributi a SP CoC (non nativo ma usando un plug-in di uApprove)

```
<AttributeFilterPolicy id="releaseToCoC"
      xmlns:ua="http://www.switch.ch/aai/idp/uApprove/mf">

    <PolicyRequirementRule xsi:type="saml:AttributeRequesterEntityAttributeExactMatch"
        attributeName="http://macedir.org/entity-category"
        attributeValue="http://www.geant.net/uri/dataprotection-code-of-conduct/v1"/>

    <AttributeRule attributeID="displayName">
        <PermitValueRule xsi:type="ua:AttributeInMetadata" onlyIfRequired="true"/>
    </AttributeRule>
    <AttributeRule attributeID="email">
        <PermitValueRule xsi:type="ua:AttributeInMetadata" onlyIfRequired="true"/>
    </AttributeRule>
    <AttributeRule attributeID="eduPersonPrincipalName">
        <PermitValueRule xsi:type="ua:AttributeInMetadata" onlyIfRequired="true"/>
    </AttributeRule>
    <AttributeRule attributeID="schacHomeOrganization">
        <PermitValueRule xsi:type="ua:AttributeInMetadata" onlyIfRequired="true"/>
    </AttributeRule>
</AttributeFilterPolicy>
```

Configurazione per IdP v2.4+

Rilascio di un insieme **dinamico** di attributi a SP CoC

```
<afp:AttributeFilterPolicy id="releaseToCoC">
   <afp:PolicyRequirementRule    xsi:type="saml:AttributeRequesterEntityAttributeExactMatch"
       attributeName="http://macedir.org/entity-category"
       attributeValue="http://www.geant.net/uri/dataprotection-code-of-conduct/v1" />

   <afp:AttributeRule attributeID="displayName">
      <afp:PermitValueRule xsi:type="saml:AttributeInMetadata" onlyIfRequired="true"/>
   </afp:AttributeRule>

   <afp:AttributeRule attributeID="email">
      <afp:PermitValueRule xsi:type="saml:AttributeInMetadata" onlyIfRequired="true"/>
   </afp:AttributeRule>

   <afp:AttributeRule attributeID="commonName">
     <afp:PermitValueRule xsi:type="saml:AttributeInMetadata" onlyIfRequired="true"/>
   </afp:AttributeRule>
</afp:AttributeFilterPolicy>
```

Riferimenti

- Geant Code of Conduct:
  - http://www.geant.net/uri/dataprotection-code-of-conduct/v1
- Ricette per un SP:
  - https://wiki.edugain.org/Recipe_for_a_Service_Provider
- Ricette per un IdP:
  - https://wiki.edugain.org/Recipe_for_a_Home_Organisation
- Monitoring tool:
  - monitor.edugain.org/coc