



24-25 Novembre 2009
Roma, Sede centrale ENEA

I Metadati per il protocollo SAMLv2

Giancarlo Birello - CNR CERIS
Simona Venuti - GARR

SAMLv2 Standard

**SAML definisce sullo standard XML-base:
definizioni, protocolli, modalita' di connessione, profili**

- **SAML assertion** contiene un pacchetto di informazioni di sicurezza
- **SAML protocol** si riferisce a COSA viene trasmesso
- **SAML binding** determina la modalita' di richiesta o risposta standard
 - **HTTP Artifact Binding** usa ARP (Artifact Resolution Protocol) e SAML SOAP Binding per risolvere un messaggio per referenza
- **SAML profile** e' una manifestazione concreta di una combinazione particolare di definizioni, protocolli e modalita' di connessione che identificano una particolare struttura (Es. IdP o SP)
- I profili sono racchiusi nei **RUOLI**

SAMLv2 Standard

Definisce formati di metadati estensibili
Organizzati in ruoli derivati dai profili SAML

Ruoli:

- Identity Provider
- Service Provider
- Affiliation
- Attribute Authority
- Attribute Consumer
- Policy Decision Point

Cosa sono i metadati

“informazioni su informazioni”
“dati che riguardano i dati”

Descrizioni di oggetti elaborabili automaticamente
detti “machine understandable” relativi ad una risorsa

Informazioni di carattere descrittivo, strutturale,
amministrativo, tecnico-gestionale relative ad un oggetto
o ad un insieme di oggetti

A cosa servono

I profili SAML2 richiedono che una **federazione si accordi** per quanto riguarda le entita' che ne fanno parte, le risorse, il supporto e gli endpoint che espletano effettivamente i servizi federati

In questo contesto i metadati servono per **descrivere** tutte queste informazioni in un modo standardizzato

E' un modo **ordinato** di annotare i servizi, le entita' le URI di riferimento e i ruoli che riflettono i profili SAML

Le macchine che espletano i servizi, sia di autenticazione che di risorse, accedono a questo elenco per **comprendere** come capire chi ha diritto a fare cosa, come deve farlo e dove sono le sue credenziali

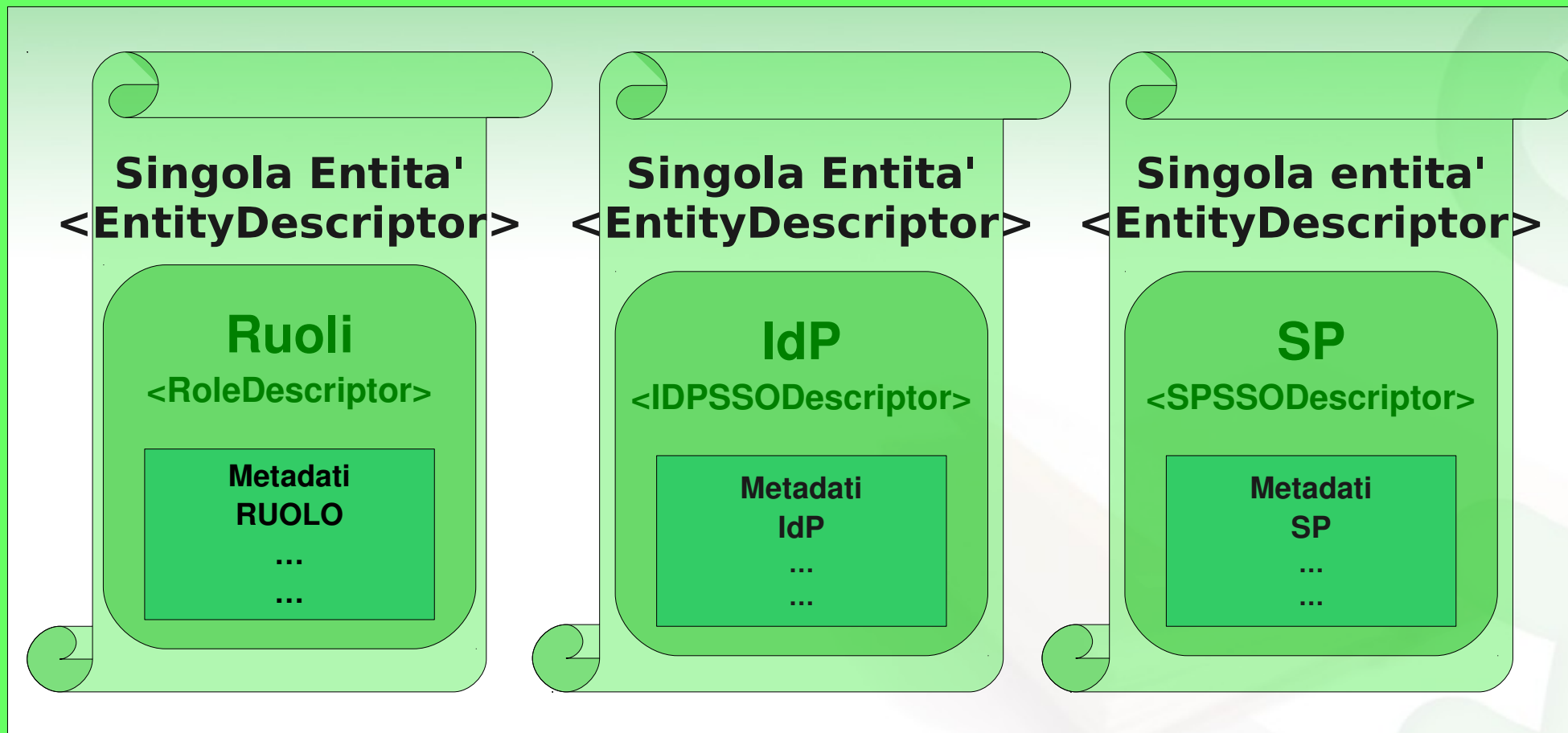
A chi servono

- Gli IdP si assicurano che l'SP sia autentico tramite una lista di 'trusted' SP
- Gli IdP trovano informazioni relative agli endpoint degli SP dove mandare le info
- Gli SP verificano la firma di una assertion tramite la chiave pubblica dell' IdP
- Gli SP risolvono referenze tramite una lista di endpoint relativi all'Artifact Resolution Service

Metadati in SAMLv2

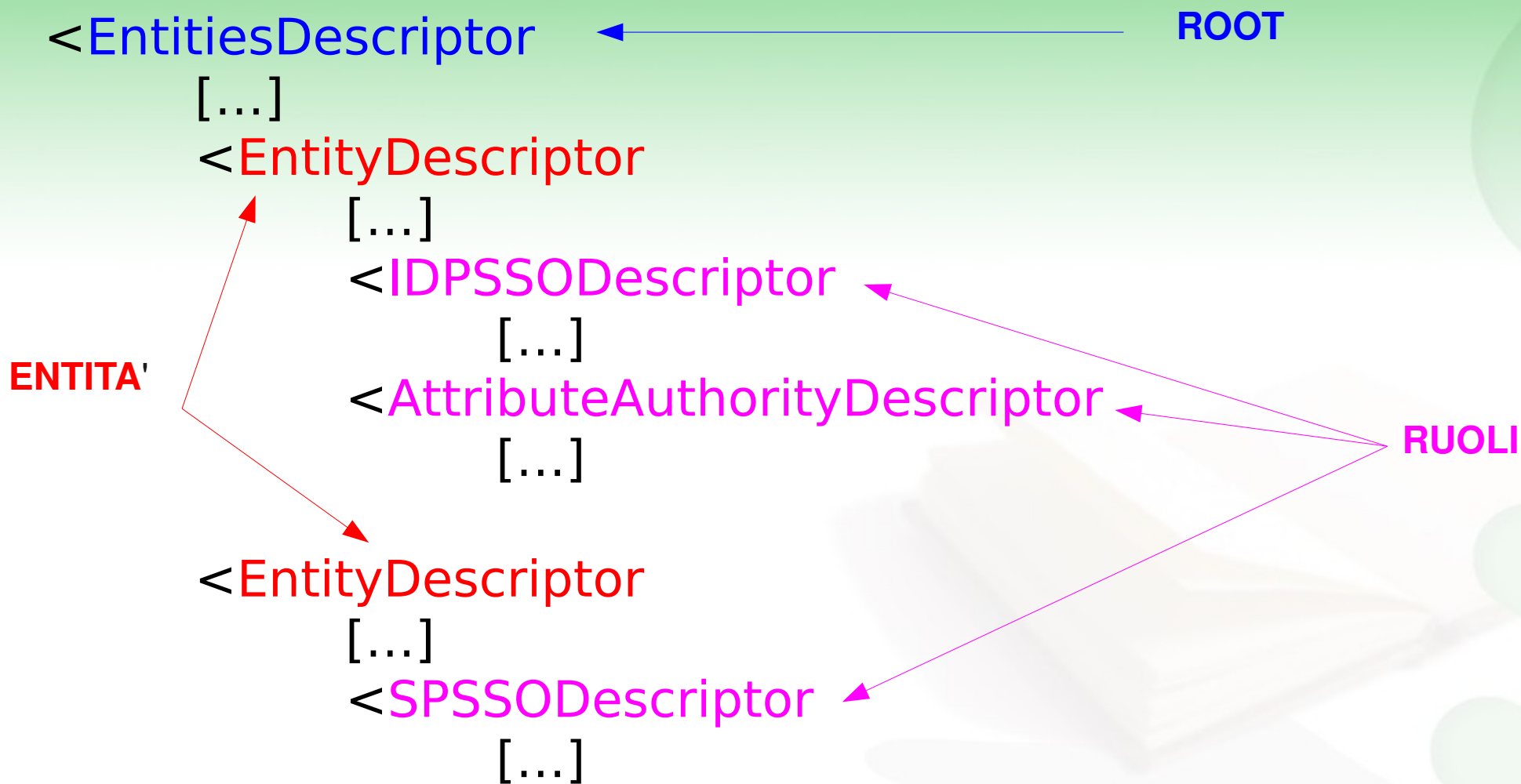
- I metadati sono raggruppati secondo i diversi ruoli
- Un ruolo e' la combinazione di protocolli SAML e profili supportati dalle singole entita'
- Ogni ruolo e' descritto da un elemento derivato dal tipo base RoleDescriptor
- I RoleDescriptor sono raggruppati dentro l'elemento contenitore EntityDescriptor, unita' primaria dei metadati
- Piu' EntityDescriptor possono essere raggruppati in gruppi nidificati, tutti sotto l'elemento EntitiesDescriptor
- Sono inoltre descritti e stabiliti tutti i sistemi supportati per stabilire un ambiente di fiducia fra gli attori

Riepilogo



Metadati FEDERAZIONE <EntitiesDescriptor>

Metadati in SAMLv2 e IDEM



namespace

Riferiti ai link specifici dove sono definiti

saml:	urn:oasis:names:tc:SAML:2.0:assertion	SAMLCore
samlp:	urn:oasis:names:tc:SAML:2.0:protocol	SAMLCore
md:	urn:oasis:names:tc:SAML:2.0:metadata	SAMLMeta-xsd
ds:	http://www.w3.org/2000/09/xmldsig#	XMLSig
xenc:	http://www.w3.org/2001/04/xmlenc#	XMLEnc
xs:	http://www.w3.org/2001/XMLSchema	Schema1

Specifico di Shibboleth

shib: urn:mace:shibboleth:metadata:1.0 shibboleth-metadata-1.0.xsd

namespace in IDEM

<EntitiesDescriptor

```
xmlns="urn:oasis:names:tc:SAML:2.0:metadata"  
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"  
xmlns:shibmd="urn:mace:shibboleth:metadata:1.0"  
  
xsi:schemaLocation=  
"urn:oasis:names:tc:SAML:2.0:metadata sstc-saml-schema-metadata-2.0.xsd  
urn:mace:shibboleth:metadata:1.0 shibboleth-metadata-1.0.xsd  
http://www.w3.org/2001/04/xmenc# xenc-schema.xsd  
http://www.w3.org/2000/09/xmldsig# xmldsig-core-schema.xsd"
```

```
Name="urn:mace:garr.it:idem"
```

```
validUntil="2010-01-01T00:00:00Z">
```

```
[...]
```

Tipi Base

I tipi di direttive di base possono essere semplici o complessi

Semplice: “**EntityID**” definisce univocamente un attore tramite la sua URI

```
<simpleType name="EntityIDType">
  <restriction base="anyURI">
    <maxLength value="1024">
  </restriction>
</simpleType>
```

Complesso: “**EndPoint**” definisce la URI a cui si deve rivolgere un attore per una certa funzione, richiedono parametri che sono tipi definiti nei namespace (Binding[req], Location[req], ResponseLocation[opt])

```
<complexType name="EndpointType">
  <sequence>
    <any namespace="##other" processContents="lax" minOccurs="0"
      maxOccurs="unbounded"/>
  </sequence>
  <attribute name="Binding" type="anyURI" use="required"/>
  <attribute name="Location" type="anyURI" use="required"/>
  <attribute name="ResponseLocation" type="anyURI" use="optional"/>
  <anyAttribute namespace="##other" processContents="lax"/>
</complexType>
```

Tipi Base in IDEM

<EntityDescriptor **entityID**="https://shibidp.unipr.it/idp/shibboleth"

[...]

<IDPSSODescriptor

[...]

<**SingleSignOnService**

Binding="urn:mace:shibboleth:1.0:profiles:AuthnRequest"

Location="https://shibidp.unipr.it/idp/profile/Shibboleth/SSO" />

[...]

<EntityDescriptor **entityID**="https://fire.rettorato.unito.it/shibboleth">

<SPSSODescriptor

[...]

<**AssertionConsumerService** **index**="1" **isDefault**="true"

Binding="urn:oasis:names:tc:SAML:1.0:profiles:browser-post"

Location="https://fire.rettorato.unito.it/Shibboleth.sso/SAML/POST"/>

[...]

SEMPLICE

COMPLESSO

Nota sulle stringhe e/o URI

Elementi: `type="string"` e/o `type="anyURI"`

- Non e' possibile inserire dei valori nulli o spazi
- Ci sono eccezioni per quanto riguarda gli attributi, dove si possono usare
- Dalla versione 2.2 di SAML non saranno piu' permessi, neanche negli attributi

La federazione IDEM sconsiglia di usare valori nulli o spazi per qualsiasi elemento

Elemento Root

- E' il “contenitore” per tutte le direttive SAML
- Descrive sia una singola entita' che multiple
 - Nel caso di singola entita' il root element deve essere `<EntityDescriptor>`
 - Nel caso di entita' multiple il root element deve essere `<EntitiesDescriptor>`

Al suo interno si trovano le regole per quella singola entita' e valide solo per quella

Elemento Root in IDEM

```

<EntitiesDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0"
xsi:schemaLocation="urn:oasis:names:tc:SAML:2.0:metadata sstc-saml-schema-metadata-2.0.xsd
urn:mace:shibboleth:metadata:1.0 shibboleth-metadata-1.0.xsd http://www.w3.org/2001/04/xmlenc#
xenc-schema.xsd http://www.w3.org/2000/09/xmldsig# xmldsig-core-schema.xsd"
Name="urn:mace:garr.it:idem" validUntil="2010-01-01T00:00:00Z">
[...]
    <EntityDescriptor entityID="https://shibidp.unipr.it/idp/shibboleth"
xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:shibmd="urn:mace:shibboleth:metadata:1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        [...]
    </EntityDescriptor>
    <EntityDescriptor entityID="https://idp.unimore.it/idp/shibboleth">
        [...]
    </EntityDescriptor>
[...]
</EntitiesDescriptor>

```

Elemento Root in IDEM

```
<EntitiesDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
```

```
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0"  
xsi:schemaLocation="urn:oasis:names:tc:SAML:2.0:metadata sstc-saml-schema-metadata-2.0.xsd  
urn:mace:shibboleth:metadata:1.0 shibboleth-metadata-1.0.xsd http://www.w3.org/2001/04/xmenc#  
xenc-schema.xsd http://www.w3.org/2000/09/xmldsig# xmldsig-core-schema.xsd"  
Name="urn:mace:garr.it:idem" validUntil="2010-01-01T00:00:00Z">
```

```
[...]
```

```
  <EntityDescriptor entityID="https://shibidp.unipr.it/idp/shibboleth"
```

```
    xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
```

```
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#" 
```

```
xmlns:shibmd="urn:mace:shibboleth:metadata:1.0"
```

```
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
  [...]
```

```
  </EntityDescriptor>
```

```
  <EntityDescriptor entityID="https://idp.unimore.it/idp/shibboleth">
```

```
    [...]
```

```
  </EntityDescriptor>
```

```
[...]
```

```
</EntitiesDescriptor>
```

Elemento Root in IDEM

```
<EntitiesDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0"
xsi:schemaLocation="urn:oasis:names:tc:SAML:2.0:metadata sstc-saml-schema-metadata-2.0.xsd
urn:mace:shibboleth:metadata:1.0 shibboleth-metadata-1.0.xsd http://www.w3.org/2001/04/xmenc#
xenc-schema.xsd http://www.w3.org/2000/09/xmldsig# xmldsig-core-schema.xsd"
Name="urn:mace:garr.it:idem" validUntil="2010-01-01T00:00:00Z">
```

[...]

```
<EntityDescriptor entityID="https://shibidp.unipr.it/idp/shibboleth"
xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:shibmd="urn:mace:shibboleth:metadata:1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
[...]
```

```
</EntityDescriptor>
```

```
<EntityDescriptor
[...]
```

```
</EntityDescriptor>
```

[...]

```
</EntitiesDescriptor>
```

EntitiesDescriptor

- Si riferisce ad un contenitore di altre entita'
- Deve contenere uno o piu' EntityDescriptor/EntitiesDescriptor
- Se e' nella 'root' deve contenere 'validUntil' o 'cacheDuration'
- Puo' contenere estensioni facoltative comuni a tutte le entita'

Direttive supportate:

- ID [opzionale]
- validUntil [opzionale]
- cacheDuration [opzionale]
- Name [opzionale]
- <ds:Signature> [opzionale]
- <Extensions> [opzionale]
- <EntitiesDescriptor> oppure <EntityDescriptor> [almeno uno]

**NB: Se e' un elemento Root obbligatoriamente valorizzare
o validUntil o cacheDuration**

EntitiesDescriptor IDEM

```
<EntitiesDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0"
xsi:schemaLocation="urn:oasis:names:tc:SAML:2.0:metadata sstc-saml-schema-metadata-2.0.xsd
urn:mace:shibboleth:metadata:1.0 shibboleth-metadata-1.0.xsd http://www.w3.org/2001/04/xmlenc#
xenc-schema.xsd http://www.w3.org/2000/09/xmldsig# xmldsig-core-schema.xsd"
Name="urn:mace:garr.it:idem"
validUntil="2010-01-01T00:00:00Z">
```

<Extensions>

```
<shibmd:KeyAuthority VerifyDepth="2">
```

```
<ds:KeyInfo>
```

```
<ds:X509Data><ds:X509Certificate> MIIC [...] </ds:X509Certificate></ds:X509Data>
```

```
</ds:KeyInfo>
```

```
<ds:KeyInfo>
```

```
<ds:X509Data><ds:X509Certificate> MIIE [...] </ds:X509Certificate></ds:X509Data>
```

```
</ds:KeyInfo>
```

```
</shibmd:KeyAuthority>
```

</Extensions>

```
[...]
```

```
</EntitiesDescriptor>
```

EntitiesDescriptor IDEM

```
<EntitiesDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:shibmd="urn:mace:shibboleth:metadata:1.0"
xsi:schemaLocation="urn:oasis:names:tc:SAML:2.0:metadata sstc-saml-schema-metadata-2.0.xsd
urn:mace:shibboleth:metadata:1.0 shibboleth-metadata-1.0.xsd
http://www.w3.org/2001/04/xmenc# xenc-schema.xsd http://www.w3.org/2000/09/xmldsig# xmldsig-
core-schema.xsd" Name="urn:mace:garr.it:idem"
validUntil="2010-01-01T00:00:00Z">
```

<Extensions>

```
<shibmd:KeyAuthority VerifyDepth="2">
```

```
<ds:KeyInfo>
```

```
<ds:X509Data><ds:X509Certificate> MIIC [...] </ds:X509Certificate> </ds:X509Data>
```

```
</ds:KeyInfo>
```

```
<ds:KeyInfo>
```

```
<ds:X509Data><ds:X509Certificate> MIIE [...] </ds:X509Certificate> </ds:X509Data>
```

```
</ds:KeyInfo>
```

```
</shibmd:KeyAuthority>
```

</Extensions>

```
[...]
```

</EntitiesDescriptor>

EntitiesDescriptor IDEM

```
<EntitiesDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0"
xsi:schemaLocation="urn:oasis:names:tc:SAML:2.0:metadata sstc-saml-schema-metadata-2.0.xsd
urn:mace:shibboleth:metadata:1.0 shibboleth-metadata-1.0.xsd http://www.w3.org/2001/04/xmlenc#
xenc-schema.xsd http://www.w3.org/2000/09/xmldsig# xmldsig-core-schema.xsd"
Name="urn:mace:garr.it:idem"
validUntil="2010-01-01T00:00:00Z">
```

<Extensions>

```
<shibmd:KeyAuthority VerifyDepth="2">
```

```
<ds:KeyInfo>
```

```
<ds:X509Data><ds:X509Certificate> MIIC [...] </ds:X509Certificate></ds:X509Data>
```

```
</ds:KeyInfo>
```

```
<ds:KeyInfo>
```

```
<ds:X509Data><ds:X509Certificate> MIIE [...] </ds:X509Certificate></ds:X509Data>
```

```
</ds:KeyInfo>
```

```
</shibmd:KeyAuthority>
```

```
</Extensions>
```

[...]

```
</EntitiesDescriptor>
```

EntityDescriptor

E' l'unita' di metadato per una singola entita'
Deve contenere almeno un ruolo

Direttive supportate:

- entityID: [req] identificativo unico, URI entita'
- ID: [opt] id usato come riferimento interno
- <ds:Signature>: [opt] elemento per verificare la firma
- <Extensions>: [opt] per utilizzare direttive non SAML.
Es. direttive specifiche Shibboleth
- <RoleDescriptor> | <IDPSSODescriptor> | <SPSSODescriptor> |
<AuthnAuthorityDescriptor> | <AttributeAuthorityDescriptor> |
<PDPDescriptor>: **[al. uno]** indica il ruolo dell'attore nella federazione
- <AffiliationDescriptor>: [in alternat. ai ruoli] indica un tipo di affiliazione
- <Organization> [opt]
- <ContactPerson> [opt]

EntityDescriptor in IDEM

Identity Provider

<EntityDescriptor entityID="https://idp.unimore.it/idp/shibboleth">

<IDPSSODescriptor protocolSupportEnumeration=...>

[...]

</IDPSSODescriptor>

RUOLI

<AttributeAuthorityDescriptor protocolSupportEnumeration=...>

[...]

</AttributeAuthorityDescriptor>

<Organization>

[...]

</Organization>

<ContactPerson contactType="technical">

[...]

</ContactPerson>

</EntityDescriptor>

EntityDescriptor in IDEM

Service Provider

```
<EntityDescriptor entityID="https://idp.unimore.it/idp/shibboleth">
```

```
  <SPSSODescriptor protocolSupportEnumeration=...>
```

```
    [...]
```

```
  </SPSSODescriptor>
```

RUOLO

```
  <Organization>
```

```
    [...]
```

```
  </Organization>
```

```
  <ContactPerson contactType="technical">
```

```
    [...]
```

```
  </ContactPerson>
```

```
</EntityDescriptor>
```

Organization e ContactPerson

- Dati facoltativi
- Natura descrittiva
- Utile per WAYF e servizi
- Comoda reperibilita' riferimenti tecnici/amministrativi
- Fortemente consigliato l'uso (alcuni SP lo richiedono per funzionare)
- Rapida consultazione di elenco attributi/elementi

Organization e ContactPerson in IDEM

<Organization>

<OrganizationName xml:lang="en">CINECA-GARR-MCU
Service Provider</OrganizationName>

<OrganizationDisplayName xml:lang="en">CINECA-GARR-
MCU</OrganizationDisplayName>

<OrganizationURL
xml:lang="en">http://www.cineca.it/</OrganizationURL>

</Organization>

<ContactPerson contactType="technical"> **[req]**

<GivenName>Franca</GivenName>

<SurName>Fiumana</SurName>

<EmailAddress>f.fiumana@cineca.it</EmailAddress>

</ContactPerson>

Tipi di ContactType: technical, support, administrative, billing, other

RoleDescriptor

- Tipo astratto che serve come base per descrizione di ruoli
- I suoi elementi sono comuni a tutti i ruoli derivati

Direttive supportate:

- ID: [opt]
- ValidUntil, caheDuration: [opt]
- **protocolSupportEnumeration**: [req] URI che identificano il tipo e la versione del protocollo supportato, citando il namespace SAML relativo
- errorURL: [req] pagina di riferimento per errori
- <ds:Signature>: [opt] elementi di firma/verifica della firma
- <Extensions>: [opt] direttive ulteriori non SAML (Es: Shibboleth)
- <**KeyDescriptor**>: [opt] chiavi/certificati di firma e crittazione
- <Organization>; <ContactPerson>: [opt] riferimenti

RoleDescriptor in IDEM

Nel caso di IDEM non è necessario estendere lo standard:

- una macchina IdP fa soltanto IdP, stessa cosa per l'SP
- ad ogni entita' corrisponde sempre un ruolo specifico
- non necessitiamo usare la direttiva astratta RoleDescriptor

<KeyDescriptor>

Informazioni sulle chiavi crittografiche che le entita' usano

Informazioni sul tipo di uso che se ne fa (per firmare o ricevere dati crittati)

Informazioni sul tipo di algoritmo supportato dall'entita'

Informazioni aggiuntive sulle configurazioni dei suddetti algoritmi

Direttive supportate:

- **use:** [opt] “*encryption | signing*” indica lo scopo d'uso della chiave
- **<ds:KeyInfo>:** [req] elemento che indentifica una chiave (v. slide succ.)
- **<EncryptionMethod>:** [opt] specifica l'algoritmo supportato dall'entita'

<KeyInfo>

Contiene istruzioni per trovare le chiavi per la verifica delle firme digitali
Puo' contenere chiavi, nomi, certificati e ogni tipo di chiave pubblica
Puo' contenere informazioni sulla distribuzione delle chiavi o key agreement
Estrema flessibilita' nello specificare il tipo di chiavi usate

All'interno di KeyInfo puo' essere specificato il nome della chiave, o il DN
mediante l'elemento **KeyName**

Puo' essere inserita direttamente la parte pubblica del certificato con **X509Data**:

X509SubjectName: DN del certificato

X509SKI: codifica base64 del SubjectKeyIdentifier del certificato

X509CertificateElement: codifica base64 del certificato stesso

X509CRL: codifica base64 della lista CRL

X509IssuerSerial: seriale

Possono essere aggiunte opzioni da altri namespace

Tutti i certificati presenti DEVONO essere riferiti alle chiavi di validazione
oppure essere parte di una catena di certificazione che deve terminare in un
certificato contenente la chiave della/e **Certification Authority**

<KeyDescriptor> in IDEM

La catena di Certification Authority per la Federazione:

```
<Extensions>
  <shibmd:KeyAuthority VerifyDepth="2">
    <ds:KeyInfo>
      <ds:X509Data>
        <!-- Globalsign GTE ct_root -->
        <ds:X509Certificate> MIIC </ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
    <ds:KeyInfo>
      <ds:X509Data>
        <!-- Educational CA sureserverEDU -->
        <ds:X509Certificate> MIIE </ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
  </shibmd:KeyAuthority>
</Extensions>
```

<KeyDescriptor> in IDEM

Certificato di un Identity Provider:

```
<KeyDescriptor>  
  <ds:KeyInfo>  
    <ds:X509Data>  
      <ds:X509Certificate>MIID</ds:X509Certificate>  
    </ds:X509Data>  
  </ds:KeyInfo>  
</KeyDescriptor>
```

Certificato di un Service Provider:

```
<KeyDescriptor use="signing">  
  <ds:KeyInfo>  
    <ds:KeyName>fire.rettorato.unito.it</ds:KeyName>  
  </ds:KeyInfo>  
</KeyDescriptor>
```

SSODescriptorType

- Estende RoleDescriptor per IdP e SP
- Aggiunge supporto SingleSignON
- Tipo complesso per raggruppare parti comuni di entita' che supportano SingleSignON

Direttive supportate:

- **<ArtifactResolutionService>**: [opt] descrive gli Indexed endpoint che supportano il protocollo ARP (viene da <md:ArtifactResolutionService>)
- **<SingleLogoutService>**: [opt] tipo di endpoint che supporta il profilo di SingleLogout. Utilizzato per "scollegare" tutti gli utenti di una sessione
- **<ManageNameIDService>**: [opt] tipo di endpoint che supporta il profilo di Name Identifier Management, per modificare impostazioni fra IdP e SP
- **<NameIDFormat>**: [opt] URI con la lista dei formati di name identifier supportati dal sistema

SSODescriptorType in IDEM

Identity Provider che supporta Shibboleth 1.x e 2.x:

```
<IDPSSODescriptor protocolSupportEnumeration="urn:mace:shibboleth:1.0
    urn:oasis:names:tc:SAML:1.1:protocol urn:oasis:names:tc:SAML:2.0:protocol">
  <ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding"
    Location="https://shibidp.unipr.it:8443/idp/profile/SAML1/SOAP/ArtifactResolution" index="1"/>
  <ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
    Location="https://shibidp.unipr.it:8443/idp/profile/SAML2/SOAP/ArtifactResolution" index="2"/>
  <NameIDFormat>urn:mace:shibboleth:1.0:nameidentifier</NameIDFormat>
  <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameidformat:transient</NameIDFormat>
  <SingleSignOnService Binding="urn:mace:shibboleth:1.0:profiles:AuthnRequest"
    Location="https://shibidp.unipr.it/idp/profile/Shibboleth/SSO" />
  <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    Location="https://shibidp.unipr.it/idp/profile/SAML2/POST/SSO" />
  <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign"
    Location="https://shibidp.unipr.it/idp/profile/SAML2/POST-SimpleSign/SSO" />
  <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
    Location="https://shibidp.unipr.it/idp/profile/SAML2/Redirect/SSO" />
</IDPSSODescriptor>
```

SSODescriptorType in IDEM

Identity Provider che supporta Shibboleth 1.x e 2.x:

```
<IDPSSODescriptor protocolSupportEnumeration="urn:mace:shibboleth:1.0  
urn:oasis:names:tc:SAML:1.1:protocol urn:oasis:names:tc:SAML:2.0:protocol">
```

```
<ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding"  
Location="https://shibidp.unipr.it:8443/idp/profile/SAML1/SOAP/ArtifactResolution" index="1"/>  
<ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"  
Location="https://shibidp.unipr.it:8443/idp/profile/SAML2/SOAP/ArtifactResolution" index="2"/>  
<NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat>  
<NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameidformat:transient</NameIDFormat>
```

```
<SingleSignOnService Binding="urn:mace:shibboleth:1.0:profiles:AuthnRequest"  
Location="https://shibidp.unipr.it/idp/profile/Shibboleth/SSO" />  
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"  
Location="https://shibidp.unipr.it/idp/profile/SAML2/POST/SSO" />  
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign"  
Location="https://shibidp.unipr.it/idp/profile/SAML2/POST-SimpleSign/SSO" />  
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"  
Location="https://shibidp.unipr.it/idp/profile/SAML2/Redirect/SSO" />  
</IDPSSODescriptor>
```

IDPSSODescriptor

**Estende SSODescriptor
con elementi propri di un Identity Provider**

Direttive supportate:

- **<SingleSignOnService>**: [almeno UNO] descrive gli endpoint per l'autenticazione che supportano il protocollo di Authentication Request. Contiene Binding e Location dove un SP può mandare richieste per richieste di autenticazione.
- **WantAuthnRequestSigned**: [opt] specifica se è necessaria la firma.
- **<NameIDMappingService>**: [opt] supporto al protocollo NameIDMap.
- **<AssertionIDRequestService>**: [opt] endpoint che supporta il profilo di Assertion Request.
- **<AttributeProfile>**: [opt] URI con la lista profili di attributi supportati.
- **<saml:Attribute>**: [opt] attributi SAML supportati dall'IdP.

IDPSSODescriptorType in IDEM

Identity Provider che supporta Shibboleth 2.x e 1.x:

```
<IDPSSODescriptor protocolSupportEnumeration="urn:mace:shibboleth:1.0
urn:oasis:names:tc:SAML:1.1:protocol urn:oasis:names:tc:SAML:2.0:protocol">
  <Extensions><shibmd:Scope regexp="false">ceris.cnr.it</shibmd:Scope></Extensions>
  <ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding"
    Location="https://shib2.to.cnr.it:8443/idp/profile/SAML1/SOAP/ArtifactResolution" index="1"/>
  <ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
    Location="https://shib2.to.cnr.it:8443/idp/profile/SAML2/SOAP/ArtifactResolution" index="2"/>
  <NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat>
  <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>
  <SingleSignOnService Binding="urn:mace:shibboleth:1.0:profiles:AuthnRequest"
    Location="https://shib2.to.cnr.it/idp/profile/Shibboleth/SSO"/>
  <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    Location="https://shib2.to.cnr.it/idp/profile/SAML2/POST/SSO"/>
  <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign"
    Location="https://shib2.to.cnr.it/idp/profile/SAML2/POST-SimpleSign/SSO"/>
  <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
    Location="https://shib2.to.cnr.it/idp/profile/SAML2/Redirect/SSO"/>
</IDPSSODescriptor>
```

IDPSSODescriptorType in IDEM

Identity Provider che supporta Shibboleth 2.x e 1.x:

```
<IDPSSODescriptor protocolSupportEnumeration="urn:mace:shibboleth:1.0
urn:oasis:names:tc:SAML:1.1:protocol urn:oasis:names:tc:SAML:2.0:protocol">
  <Extensions><shibmd:Scope regexp="false">ceris.cnr.it</shibmd:Scope></Extensions>
  <ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding"
    Location="https://shib2.to.cnr.it:8443/idp/profile/SAML1/SOAP/ArtifactResolution" index="1"/>
  <ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
    Location="https://shib2.to.cnr.it:8443/idp/profile/SAML2/SOAP/ArtifactResolution" index="2"/>
  <NameIDFormat>urn:mace:shibboleth:1.0:nameidentifier</NameIDFormat>
  <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>
```

```
<SingleSignOnService Binding="urn:mace:shibboleth:1.0:profiles:AuthnRequest"
  Location="https://shib2.to.cnr.it/idp/profile/Shibboleth/SSO"/>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Location="https://shib2.to.cnr.it/idp/profile/SAML2/POST/SSO"/>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign"
  Location="https://shib2.to.cnr.it/idp/profile/SAML2/POST-SimpleSign/SSO"/>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
  Location="https://shib2.to.cnr.it/idp/profile/SAML2/Redirect/SSO"/>
```

```
</IDPSSODescriptor>
```

IDPSSODescriptorType in IDEM

Identity Provider che supporta Shibboleth 1.x:

```
<IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol  
urn:mace:shibboleth:1.0">
```

```
<ArtifactResolutionService index="1"
```

```
  Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding"
```

```
  Location="https://idp.idem.garr.it/shibboleth-idp/Artifact" />
```

```
<NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat>
```

```
<SingleSignOnService Binding="urn:mace:shibboleth:1.0:profiles:AuthnRequest"
```

```
  Location="https://idp.idem.garr.it/shibboleth-idp/SSO" />
```

```
</IDPSSODescriptor>
```

SPSSODescriptorType

**Estende SSODescriptor
con elementi propri di un Service Provider**

Direttive supportate:

- **<AssertionConsumerService>**: [almeno UNO] descrive gli indexed endpoint e le binding location dove l'IdP deve mandare le risposte di autenticazione
- **<WantAssertionSigned>**: [opt] lo SP richiede all' IdP una risposta firmata
- **<AuthnRequestSigned>**: [opt] lo SP comunica all' IdP che intende firmare ogni richiesta
- **<AttributeConsumingService>**: [opt] descrive una applicazione o servizio fornito dall'SP che richiede espressamente alcuni attributi SAML che vanno qua elencati tramite l'elemento **<RequestedAttribute>**

SPSSODescriptorType in IDEM

Service Provider che supporta Shibboleth 2.x e 1.x:

<SPSSODescriptor protocolSupportEnumeration=...>
[...]

<AssertionConsumerService

Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"

Location="http://vconf.garr.it/Shibboleth.sso/SAML2/POST" index="1" isDefault="true"/>

<AssertionConsumerService

Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign"

Location="http://vconf.garr.it/Shibboleth.sso/SAML2/POST-SimpleSign" index="2"/>

<AssertionConsumerService

Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"

Location="http://vconf.garr.it/Shibboleth.sso/SAML2/Artifact" index="3"/>

<AssertionConsumerService

Binding="urn:oasis:names:tc:SAML:1.0:profiles:browser-post"

Location="http://vconf.garr.it/Shibboleth.sso/SAML/POST" index="4"/>

<AssertionConsumerService

Binding="urn:oasis:names:tc:SAML:1.0:profiles:artifact-01"

Location="http://vconf.garr.it/Shibboleth.sso/SAML/Artifact" index="5"/>

[...]

</SPSSODescriptor>

SPSSODescriptorType in IDEM

Service Provider che supporta Shibboleth 1.x:

<SPSSODescriptor

```
protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol">  
<KeyDescriptor use="signing"> [...] </KeyDescriptor>  
<NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat>
```

```
<AssertionConsumerService index="1" isDefault="true"  
Binding="urn:oasis:names:tc:SAML:1.0:profiles:browser-post"  
Location="https://fire.rettorato.unito.it/Shibboleth.sso/SAML/POST"/>  
<AssertionConsumerService index="2"  
Binding="urn:oasis:names:tc:SAML:1.0:profiles:artifact-01"  
Location="https://fire.rettorato.unito.it/Shibboleth.sso/SAML/Artifact"/>
```

</SPSSODescriptor>

AttributeAuthorityDescriptor

Estende SSODescriptor con elementi e attributi propri Attribute Authority, cioe' le SAML authority che rispondono ai messaggi di query degli attributi

Direttive supportate:

- **<AttributeService>**: [almeno UNO] descrive gli endpoint che supportano il profilo di protocollo Attribute Query
- **<AssertionIDRequestService>**: [opt] endpoint che supportano il profilo di Assertion Request o la URI specifica
- **<AttributeProfile>**: [opt] URI che elenca i profili di attributi supportati da questa authority
- **<saml:Attribute>**: [opt] attributo SAML supportato dall'authority, possono essere specificati valori ulteriori, indicando i valori accettati

AttributeAuthority in IDEM

Ogni IdP della federazione IDEM ha nei metadati il proprio riferimento alla sua autorità di attributi:

```
<EntityDescriptor ...  
  [...]  
  <IDPSSODescriptor> [...] </IDPSSODescriptor>
```

<AttributeAuthorityDescriptor ...>

```
<AttributeService  
  Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding"  
  Location="https://shib2.to.cnr.it:8443/idp/profile/SAML1/SOAP/AttributeQuery"/>
```

```
<AttributeService  
  Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"  
  Location="https://shib2.to.cnr.it:8443/idp/profile/SAML2/SOAP/AttributeQuery"/>
```

</AttributeAuthorityDescriptor>

Esempio: IdP, SP e ADFS (1/2)

Modificare i metadati per far parlare un IdP e un SP Shibboleth con WindowsDirectoryService su WindowsServer2003R2

SP modificare dentro shibboleth.xml:

<Extensions>

<Library path="/usr/libexec/xmlproviders.so" fatal="true"/>

<Library path="/usr/libexec/adfs.so" fatal="true"/>

</Extensions>

<SessionInitiator isDefault="true" id="testshib"

Location="https://idp.uni.it/ADFS"

Binding="urn:mace:shibboleth:sp:1.3:SessionInit"

WayfURL="https://wayf.uni.it/adfs/ls"/>

Modificare metadati dello SP:

<SPSSODescriptor

protocolSupportEnumeration="http://schema.xmlsoap.org/ws/2003/07/secext">

<AssertionConsumerService Location="/ADFS" index="4"

Binding="http://schemas.xmlsoap.org/ws/2003/07/secext"

ResponseLocation=""/>

</SPSSODescriptor>

Esempio: IdP, SP e ADFS (2/2)

IdP: Installare prima le estensioni:
shib.ADFS.extensions-versione.tar

Modificare in idp.xml:

```
<RelyingParty name="urn:federation:NomeFederazione"  
  providerID="urn:federation:nomeProvider"  
  signingCredential="example_cred">  
  <NameID nameMapping="shm"/>  
</RelyingParty>
```

Modificare metadati:

```
<IDPSSODescriptor  
  protocolSupportEnumeration="http://schemas.xmlsoap.org/ws/2003/07/secext">  
  <SingleSignOnService  
    Binding="http://schemas.xmlsoap.org/ws/2003/07/secext"  
    Location="https://BER-DC1.Adatum.com/adfs/ls/">  
</IDPSSODescriptor>
```

Riferimenti

- **Metadata for the OASIS SAML v.2**
<http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf>
- **Assertions and Protocols for the OASIS SAML v.2**
<http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>
- **Profiles form the OASIS SAML v.2**
<http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf>
- **XML Signature Syntax and Processing (2nd edition)**
<http://www.w3.org/TR/xmldsig-core/>
- **Achieving Interoperability between Active Directory Federation Services and Shibboleth**
http://www.oxfordcomputergroup.com/ocg_/images/resources/ADFS%20White%20Paper%2002-07.pdf
- **GARR-IDEM metadata**
<https://www.idem.garr.it/docs/conf/idem-metadata.xml>
- **Specifiche Tecniche per la Federazione IDEM**
http://www.servizi.garr.it/index.php/it/documenti/doc_download/54-specifiche-tecniche-v10