Introduction

Migrazione da IdP v2 a v3

Aggiornamento IdP e nuovi standard

Daniele Albrizio - albrizio@units.it

IDEM Day 2018 - Roma ISTAT

https://bit.ly/2juhOmU

Perché migrare

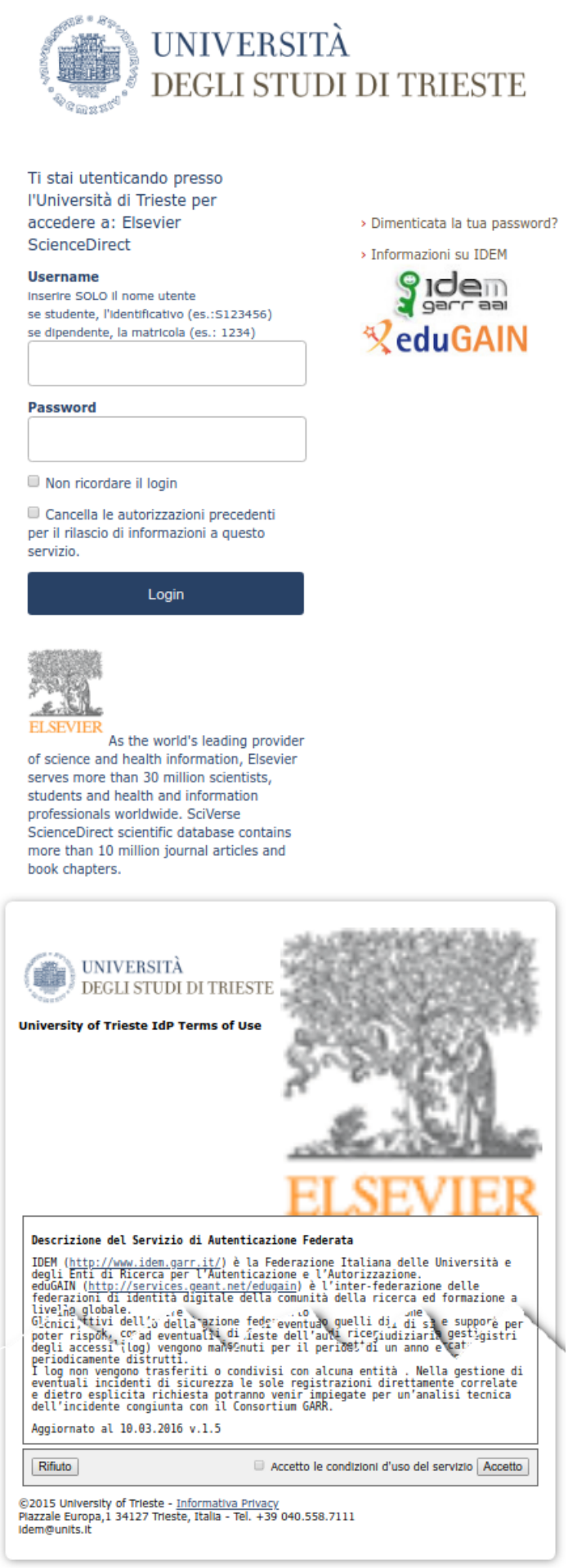
- versione 2 > EoL 31.7.2016
- Cogliere l'occasione per abbandonare SAML1 in favore di SAML2
- GDPR compliance (strumenti per la)

Consenso esplicito

- Consent
- Informativa (ToU) al primo accesso (con versioning)
- Consenso al rilascio degli attributi prima di rilasciarli all'SP insieme al...
- ...link all'informativa sul trattamento dati dell'SP (se pubblicato nei metdati dell'SP - mdui:PrivacyStatem

Consenso esplicito

- Accettazione dei ToU **registrata** nel log idp-consent-audit.log.
  - '20180502T200018Z|https://sdauth.sciencedirect.com/ |TermsAccepted|*principal* |my-tou-1.5||true'
- I consensi specifici restano in un **cookie sicuro** sul browser (a scadenza programmabile lato IdP).
- **Al cambiare** della versione nel ToU o del set di attributi da rilasciare, può essere *ripresentata la pagina automaticamente*.


UNIVERSITÀ
DEGLI STUDI DI TRIESTE
Ti stai utenticando presso l'Università di Trieste per accedere a: Elsevier ScienceDirect
Username
Inserire SOLO il nome utente
se studente, l'identificativo (es.:S123456)
se dipendente, la matricola (es.: 1234)
Password
Non ricordare il login
Cancella le autorizzazioni precedenti per il rilascio di informazioni a questo servizio.
Login
› Dimenticata la tua password?
› Informazioni su IDEM
idem garr aai
eduGAIN
ELSEVIER
As the world's leading provider of science and health information, Elsevier serves more than 30 million scientists, students and health and information professionals worldwide. SciVerse ScienceDirect scientific database contains more than 10 million journal articles and book chapters.

+++

UNIVERSITÀ
DEGLI STUDI DI TRIESTE
University of Trieste IdP Terms of Use
ELSEVIER
Descrizione del Servizio di Autenticazione Federata
IDEM (http://www.idem.garr.it/) è la Federazione Italiana delle Università e degli Enti di Ricerca per l'Autenticazione e l'Autorizzazione.
eduGAIN (http://services.geant.net/edugain) è l'inter-federazione delle federazioni di identità digitale della comunità della ricerca ed formazione a livello globale.
Gli amministratori tecnici, attivi dell'Ateneo della azione federativa, hanno accesso agli eventuali dati di sistema e supporto per poter rispondere ad eventuali richieste dell'autorità giudiziaria gestori degli accessi (log) vengono mantenuti per il periodo di un anno e cat periodicamente distrutti.
I log non vengono trasferiti o condivisi con alcuna entità . Nella gestione di eventuali incidenti di sicurezza le sole registrazioni direttamente correlate e dietro esplicita richiesta potranno venir impiegate per un'analisi tecnica dell'incidente congiunta con il Consortium GARR.
Aggiornato al 10.03.2016 v.1.5
Rifiuto
Accetto le condizioni d'uso del servizio
Accetto
©2015 University of Trieste - Informativa Privacy
Piazzale Europa,1 34127 Trieste, Italia - Tel. +39 040.558.7111
idem@units.it

+++

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

Stai per accedere al servizio:
sp-test.units.it

Informazioni da comunicare al Servizio

Common Name	**ALBRIZIO DANIELE**
Name	**DANIELE**
Surname	**ALBRIZIO**
Tax Code Legacy	**LBR**
Mail address	**albrizio@units.it**
Account Name	
Account Name (ePPN)	**s.units.it**
eduPersonAffiliation simple affiliation info	**member** **staff**
eduPersonScopedAffiliation affiliation info	**staff@units.it** **member@units.it**
Active Directory Groups	**CN=UG ,OU uts** **CN= =it** **CN= uts** **CN= =ds** **CN= ut** **CN=r** **CN=U** **CN=Li** **CN= un** **CN=U ut** **CN=a C=i** **CN=A uni** **CN=UG =ut** **CN=UG S,OU=ut** **CN= ds,DC=u** **CN=nd C=ur** **CN=Us ,DC=ds,D** **CN=A_ nit**
Opaque per-service identifier eduPersonTargetedID	**rZCEXsm**
Further authorizations	**urn:mace:dir:entitlement:common-lib-terms** **urn:mace:teren** **http://elearning.u-gov.it/idemcategories?id=U-GOV-INTR** **http://elearning.u-gov.it/idemcategories?id=U-GOV-A** **http://elearning.u-gov.it/idemcategories?id=U-GOV-R** **http://elearning.u-gov.it/idemcategories?id=U-GOV-C** **urn:mace:terena.org** **http://elearning.u-gov.it/idemcategories?id=U-GOV-PC** **http://elearning.u-gov.it/idemcategories?id=U-GOV-RU** **http://e-academy.com/eligibility/idemfero.units.it/faculty**
affiliationID	**member** **staff**
Display Name	**DANIELE ALBRIZIO**
eMail (does not respect mace:dir)	**albrizio@units.it**
Preferred language	**it-it**
Home organization	**units.it**
Home organization type	**urn:schac:homeOrganizationType:int:university**
Tax Code	**urn:schac:personalUniqueID:it:CF:LBR**
Phone	**+39 040 558**

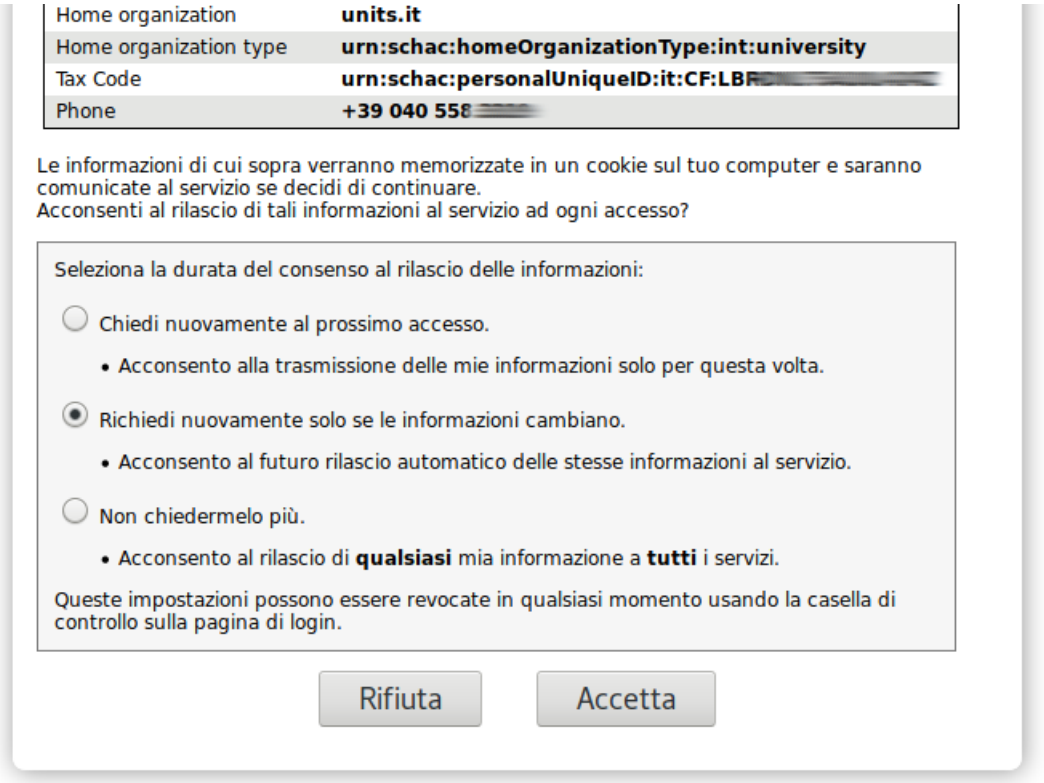
Le informazioni di cui sopra verranno memorizzate in un cookie sul tuo computer e saranno comunicate al servizio se decidi di continuare.
Acconsenti al rilascio di tali informazioni al servizio ad ogni accesso?

Seleziona la durata del consenso al rilascio delle informazioni:

- ○ Chiedi nuovamente al prossimo accesso.
  - Acconsento alla trasmissione delle mie informazioni solo per questa volta.
- ◉ Richiedi nuovamente solo se le informazioni cambiano.
  - Acconsento al futuro rilascio automatico delle stesse informazioni al servizio.

```
<!-- CODICE FISCALE ITALIA -->
<resolver:AttributeDefinition xsi:type="ad:Simple"
xmlns="urn:mace:shibboleth:2.0:resolver:ad"
id="schacPersonalUniqueID" sourceAttributeID="schacCF">
    <resolver:Dependency ref="schacCF" />
    <resolver:DisplayName xml:lang="it">Codice Fiscale</resolver:DisplayName>
    <resolver:DisplayName xml:lang="en">Tax Code</resolver:DisplayName>
    <resolver:DisplayDescription xml:lang="it">Codice Fiscale</resolver:DisplayDescription>
    <resolver:DisplayDescription xml:lang="en">Tax Code</resolver:DisplayDescription>
    <resolver:AttributeEncoder xsi:type="enc:SAML2String"
    name="urn:oid:1.3.6.1.4.1.25178.1.2.15"
    friendlyName="schacPersonalUniqueID" />
</resolver:AttributeDefinition>
```

Descrizione utente in varie lingue In realtà l'attributo è schacPersonalUniqueID



+++

Nova architettura

- Il container di default passa da Tomcat a Jetty
- Molto più leggero. Più immediato per chi non ha esperienza di Tomcat.
- OpenJDK
- Secure cookies client-side
- rigenerare la chiave di cifratura ogni giorno con seckeygen a cron

Fringe benefits

- Miglior supporto ldap/AD

- connection pooling
- ldap backend type distinti fra openldap e AD (ActiveDirectoryAuthenticationResponseHandler)
- Miglior supporto dei backend database
- gestione migliore del DB failover

Fringe benefits

- idp-process.log: Messaggi di warning molto più chiari per l'**amministratore**
- Condizioni di errore **user-facing** maggiormente gestite (user experience più confortevole)
- Interfaccia utente in **responsive** web design (per tutti i dispositivi)
- Interfaccia completamente (e facilmente) internazionalizzabile
- Testo delle pagine modificabile runtime (reload automatico temporizzato)

Fringe benefits

- FileBackedHTTPMetadataProvider
- Carica metadati via web e li tiene in memoria anche dopo il riavvio
- EntityRoleWhiteListFilter
- carica solo i metadati filtrati, ad esempio, per ruolo (e.g. tutti e soli gli SP {esclude gli IdP} per maggiore minore impronta in memoria)
- https://wiki.shibboleth.net/confluence/display/IDP30/EntityRoleWhiteListFilter

Fringe benefits

- Reloadable services
- Attribute Filter
- Attribute Resolver
- Credentials
- Metadata Providers
- UI properties
- Logging parameters

+++

un servizio si riavvia così

```
$ ./reload-service.sh -id shibboleth.AttributeResolverService
$ curl -s http[s]://localhost:[port]/idp/profile/admin/reload-service?id=shibboleth.AttributeR
```

access-control.xml

```
   <!-- Map of access control policies used
    to limit access to administrative functions. -->
  <util:map id="shibboleth.AccessControlPolicies">
    <entry key="AccessByIPAddress">
      <bean parent="shibboleth.IPRangeAccessControl"
        p:allowedRanges="#{ {'127.0.0.1/32', '::1/128} }" />
    </entry>
  </util:map>
```

+++

Unattended reload

- services.properties
  - idp.service.**logging**.checkInterval = PT5M
  - idp.service.**relyingparty**.checkInterval =...
  - idp.service.**metadata**.checkInterval =...
  - idp.service.**attribute.resolver**.checkInterval...
  - idp.service.**attribute.filter**.checkInterval =...
  - idp.service.**nameidGeneration**.checkInterval...
  - idp.service.**access**.checkInterval = PT5M

Fringe benefits

- Logging
- Mail alert degli errori
- Rotazione e compressione dei log / cancellazione dei vecchi file
- Recovery da situazioni di I/O failure
- Supporto nativo CAS

Extra Power

Power Features

Extra Power

- Profili di relying parties basati su gruppi, tag, metadati su cui applicare particolari...
  - AFP
  - consent policies
  - algoritmi di crittografia personalizzati
  - configurazioni SLO
  - ecc...

Extra Power

- dipendenze degli attributi (Dependency) in modo da poter fare il merge di attributi con id sorgenti differe (TemplateAttribute)
- Tipo di autenticazione selezionabile per singolo SP
- SSO disabilitabile per IP (vedi caso SPID) o con checkbox sulla pagina di login
- Supporto per blacklist e whitelist di algoritmi di firma e crittografia (Poodle docet)

Attenzione però...

- APIs non backward-compatibili: estensioni personalizzate dovranno molto probabilmente essere aggiorr funzionare con la versione 3 (scripted attribute e webflow)
- Attribute Filtering: L'ID dell'attributo è ora obbligatorio per tutte le policy (era opzionale)
- Molte funzionalita' disabilitate di default in caso di upgrade (consent, NameID generation, ecc...)

Clustering

- Terracotta non piu' supportato
- Sincronizzare le chiavi del keystore per i secure cookies
- db (NameID:persistent/ePTID) su un cluster esterno
- memcached consigliato in caso di Single Logout

Single/Global Logout

https://wiki.shibboleth.net/confluence/display/IDP30/LogoutConfiguration

- Supporto allo SLO ***quasi*** maturo
- Necessario session tracking lato server e non basta
- HTML LocalStorage lato browser
- server-side storage service JPAStorageService o MemcachedStorageService +++
- Percorso non lineare, costellato di problemi e malfunzionamenti.
- Pubblicheremo alcuni suggerimenti e problemi riscontrati e risolti.

Migrazione

strategie di migrazione

- Solo patch di sicurezza ...oppure...
- Usare le nuove potenzialità

Solo patch di sicurezza

- Crare una copia completa della macchina in produzione e operare su questa
- Installare* il nuovo Shibboleth su quello vecchio
- Far partire il nuovo IdP
- Drogare il file hosts del/i client usato/i per i test
- Correggere gli errori guardando il idp-process.log
- Spegnere l'IdP in produzione (planned downtime)
- Sincronizzare il db del persistentID
- Accendere il nuovo IdP in produzione

Usare le nuove potenzialità

- Installare il sistema operativo da zero (Debian/Ubuntu/...)
- Installare* il nuovo Shibboleth (fresh install)
- Portare i file di configurazione nella nuova directory *conf* avendo cura di non sovrascrivere quelli di defa

Fresh install

- Personalmente uso le estensioni .orig e .v2 per individuare:
  - v2: il file funzionante nel vecchio IdP
  - orig: i file originali della distribuzione di cui esiste una copia modificata in produzione

Mantenere l'identità dell'IdP

- Vanno portati così come sono:
  - idp-metadata.xml
  - idp.crt (che va nella nuova dir credentials)
  - idp.key (che va nella nuova dir credentials)
  - modalità di generazione del persistentID con il salt associato
  - Chiave e certificato del web server

Passi fino alla produzione

- Far partire il nuovo IdP
- Drogare il file hosts del/i client usato/i per i test
- Correggere gli errori guardando il idp-process.log
- Una volta che tutto funziona, implementare le nuove funzionalità, una alla volta

Messa in produzione

- Spegnere l'IdP in produzione (planned downtime)
- Sincronizzare il db del persistentID

- Accendere il nuovo IdP in produzione

Drogare il file degli host

- /etc/hosts
- C:\Windows\System32\drivers\etc

Formato:

IP address sviluppo	FQDN produzione
140.105.78.12	idp.units.it

- Usare la finestra "incognito" del browser / ripulire i cookies

Installazione e configurazione

(*) HOWTO Install and Configure a Shibboleth IdP v3.3.2 on Ubuntu Linux LTS 16.04 with Apache2 + Jetty9

GitHub https://bit.ly/2rkOP9s

UpgradingFromV2

https://wiki.shibboleth.net/confluence/display/IDP30/UpgradingFromV2

saml2:NameID persistent generation and storage

- Distribuito su 3 file:
- saml-nameid.properties
- saml-nameid.xml
- c14n/subject-c14n.xml
- Prendere nota di come lo si generava finora:
- algoritmo di crittografia
- composizione dell'attributo
- salt

relying-parties.xml

splittato in due file:

- **relying-parties.xml** con gli hook ai beans per effettuare fine-tuning su encryption o altre condizioni com presentazione o meno del ToU, ecc...
- **metadata-providers.xml** con gli hook ai MetadataProvider di tipo FilesystemMetadataProvider e

FileBackedHTTPMetadataProvider

Deprecati (FILTER)

esempi:

Legacy	Current
basic:AND	AND
basic:ANY	ANY
basic:AttributeScopeString	Scope
basic:AttributeValueRegex	ValueRegex
saml:AttributeRequesterInEntityGroup	InEntityGroup

Deprecati (FILTER)

Namespace deprecati

basic: e saml:

https://wiki.shibboleth.net/confluence/display/IDP30/AttributeFilterLegacyNameSpaceMapping

Deprecati (FILTER)

- PolicyRequirementRule*Reference*
- PermitValueRule*Reference*
- DenyValueRule*Reference*

Elementi deprecati (RESOLVER)

Namespace deprecati

- ad:
- dc:
- enc:
- pc:

Elementi deprecati (RESOLVER)

- CryptoTransientId (attribute type)
- TransientId (attribute type)

- SAML1StringNameIdentifier (encoder type)
- SAML2StringNameID (encoder type)

portati tutti nel servizio di NameID Generation

E' tutto a posto?

- Run e aggiustamenti successivi della configurazione secondo i warning molto esaustivi dell'idp-process.

```
org.springframework.beans.factory.xml.XmlBeanDefinitionStoreException:
Line 235 in XML document from file
/opt/shibboleth-idp/conf/metadata-providers.xml]
is invalid; nested exception is
org.xml.sax.SAXParseException;
lineNumber: 235; columnNumber: 62; cvc-complex-type.2.4.a:
Invalid content was found starting with
element 'RelyingParty'.
One of '{"urn:mace:shibboleth:2.0:metadata":MetadataProvider}'
is expected.
```

Indicazione del file interessato dal problema. Riga e colonna dell'errore. Tipo di errore. Cosa invece ci si sare

WHAT'S NEXT

Scorsa sull' XML

come si presentano alcune configurazioni

- Backend multipli ldap
- AD con OU multiple
- PolicyRequirementRule : il caso delle entity category
- filtro epEntitlement a seconda del requestor
- personalizzazione di un relying party

Authenticare utenti da diversi LDAP

https://github.com/ConsortiumGARR/idem-tutorials/blob/master/idem-fedops/HOWTO-Shibboleth/Solutions/HOWTO%20Configure%20a%20Shibboleth%20IdP%20v3.2.1%20to%20authenticate%20Users%20existing%20LDAP%20Servers.md

Mappando AuthHandlers, DnResolvers multipli tramite *util:map* e usando 2 DataConnector in failover

Autenticare da un Active Directory su 4 OU diverse

https://wiki.shibboleth.net/confluence/display/IDP30/Authenticating+against+multiple+OU%27s

Mappando AuthHandlers, DnResolvers multipli tramite *util:map* e usando 4 DataConnector in failover

Filtri condizionali

Tramite l'introduzione di PolicyRequirementRule

+++

attribute-filter.xml - IDEM

```
<!-- Rule for IDEM SPs -->
<AttributeFilterPolicy id="releaseToIDEM">
 <PolicyRequirementRule xsi:type="RegistrationAuthority"
   registrars="http://www.idem.garr.it/"/>

 <!-- Attributes defined by "Specifiche Tecniche per la Compilazione
      e l'uso degli Attributi" version 2012 + modifiche -->
 <AttributeRule attributeID="displayName">
  <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
 </AttributeRule>
 <AttributeRule attributeID="surname">
  <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
 </AttributeRule>
 <AttributeRule attributeID="givenName">
  <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
 </AttributeRule>
 <AttributeRule attributeID="commonName">
  <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
 </AttributeRule>
 <AttributeRule attributeID="preferredLanguage">
  <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
 </AttributeRule>
 <AttributeRule attributeID="schacMotherTongue">
  <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
 </AttributeRule>
 <AttributeRule attributeID="title">
  <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
 </AttributeRule>
 <AttributeRule attributeID="schacPersonalTitle">
  <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
 </AttributeRule>
 <AttributeRule attributeID="schacPersonalPosition">
  <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
 </AttributeRule>
 <AttributeRule attributeID="email">
  <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
 </AttributeRule>
 <AttributeRule attributeID="telephoneNumber">
  <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
 </AttributeRule>
 <AttributeRule attributeID="facsimileTelephoneNumber">
  <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
 </AttributeRule>
 <AttributeRule attributeID="mobile">
  <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
 </AttributeRule>
 <AttributeRule attributeID="schacUserPresenceID">
  <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
 </AttributeRule>
 <AttributeRule attributeID="eduPersonOrgDN">
  <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
```

```
  </AttributeRule>
  <AttributeRule attributeID="eduPersonOrgUnitDN">
   <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
  </AttributeRule>
  <AttributeRule attributeID="eduPersonScopedAffiliation">
   <PermitValueRule xsi:type="AND">
     <Rule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
    <Rule xsi:type="OR">
     <Rule xsi:type="Value" value="faculty" ignoreCase="true" />
     <Rule xsi:type="Value" value="student" ignoreCase="true" />
     <Rule xsi:type="Value" value="staff" ignoreCase="true" />
     <Rule xsi:type="Value" value="alum" ignoreCase="true" />
     <Rule xsi:type="Value" value="member" ignoreCase="true" />
     <Rule xsi:type="Value" value="affiliate" ignoreCase="true" />
     <Rule xsi:type="Value" value="employee" ignoreCase="true" />
     <Rule xsi:type="Value" value="library-walk-in" ignoreCase="true" />
    </Rule>
   </PermitValueRule>
   </AttributeRule>
   <AttributeRule attributeID="eduPersonPrincipalName">
    <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
   </AttributeRule>
   <AttributeRule attributeID="eduPersonAffiliation">
    <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
   </AttributeRule>
   <AttributeRule attributeID="eduPersonEntitlement">
    <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
   </AttributeRule>

  </AttributeFilterPolicy>

 </AttributeFilterPolicyGroup>
```

Condizione per applicare questa AFP è che la Registration Authority... ... deve essere IDEM (verificato sui m

+++

attribute-filter.xml - R&S Entity Category

```
 <!-- Attribute Filter Policy Dinamica e compliant
      con la R&S Entity Category -->

 <AttributeFilterPolicy id="releaseDynamicSubsetRandSAttributeBundle">

  <PolicyRequirementRule xsi:type="saml:EntityAttributeExactMatch"
   attributeName="http://macedir.org/entity-category"
   attributeValue="http://refeds.org/category/research-and-scholarship"/>

   <!-- Attributi per la Research & Scholarship -->
   <!-- rilascia ePPN, ePTID, email, displayName,
      givenName, surname a tutti gli SP R/S -->
   <AttributeRule attributeID="eduPersonPrincipalName">
    <PermitValueRule xsi:type="ANY"/>
   </AttributeRule>
   <AttributeRule attributeID="eduPersonTargetedID">
    <PermitValueRule xsi:type="ANY" />
   </AttributeRule>
   <!-- l'attributo "email" indica l'attributo "mail" proveniente dalla directory -->
   <AttributeRule attributeID="email">
    <PermitValueRule xsi:type="ANY"/>
```

```
    </AttributeRule>
    <AttributeRule attributeID="displayName">
     <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="givenName">
     <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="surname">
     <PermitValueRule xsi:type="ANY" />
    </AttributeRule>

    </AttributeFilterPolicy>

  </AttributeFilterPolicyGroup>
```

Questa AFP si applica se l'Entity Attribute ha esattamente... ...questo nome e questo valore (verificato sui m

Scripted attribute

dove i tipi di attributo built-in non bastano più

+++

Necessità

- Per scopi autorizzativi ho necessità di popolare un attributo GroupList ad uso degli SP interni non federa gruppi AD di appartenenza dell'utente.

+++ attriute-resolver.xml

```
  <!-- Attributo per l'appartenenza ai gruppi AD -->

  <resolver:AttributeDefinition xsi:type="Script"
   xmlns="urn:mace:shibboleth:2.0:resolver:ad"
   id="GroupList">
    <resolver:Dependency ref="myLDAP_AD" />
    <ScriptFile>/opt/shibboleth-idp/scripts/populateGroups.js</ScriptFile>
  </resolver:AttributeDefinition>

  <resolver:AttributeDefinition xsi:type="ad:Simple"
   xmlns="urn:mace:shibboleth:2.0:resolver:ad"
   id="adGroup"
   sourceAttributeID="GroupList">
    <resolver:Dependency ref="GroupList" />
    <resolver:DisplayName xml:lang="en">Active Directory Groups</resolver:DisplayName>
    <resolver:DisplayName xml:lang="it">Gruppi Active Directory</resolver:DisplayName>
    <resolver:DisplayDescription xml:lang="en">Active Directory Group membership</resolver:Displ
    <resolver:DisplayDescription xml:lang="it">Lista dei gruppi di appartenenza in Active Direct
    <resolver:AttributeEncoder xsi:type="enc:SAML2String" name="urn:mace:dir:attribute-def:adGrc
  </resolver:AttributeDefinition>
```

Definisco un attributo di tipo Script passando come dipendenza la fonte dei dati e il path allo script in javascr l'attributo "esterno" referenziando lo script attribute creato in precedenza come attibuto sorgente e dipenden

+++

populateGroups.js

```
if (typeof memberOf != "undefined" && memberOf != null ){
  for ( i = 0; memberOf != null && i < memberOf.getValues().size(); i++ ){
    value = memberOf.getValues().get(i);
    GroupList.getValues().add(value);
  }
}
```

+++

eduPersonEntitlement

```
<!-- Risoluzione attributo eduPersonEntitlement -->
<resolver:AttributeDefinition
 xsi:type="ad:Simple"
 id="eduPersonEntitlement"
 sourceAttributeID="epeList">
  <resolver:Dependency ref="epeList" />
  <resolver:DisplayName xml:lang="it">Autorizzazioni ulteriori</resolver:DisplayName>
  <resolver:DisplayName xml:lang="en">Further authorizations</resolver:DisplayName>
  <resolver:DisplayDescription xml:lang="it">Autorizzazioni ulteriori</resolver:DisplayDescrip
  <resolver:DisplayDescription xml:lang="en">Further authorizations</resolver:DisplayDescripti
  <resolver:AttributeEncoder xsi:type="enc:SAML1String" name="urn:mace:dir:attribute-def:eduPe
  <resolver:AttributeEncoder xsi:type="enc:SAML2String" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7
</resolver:AttributeDefinition>

<resolver:AttributeDefinition xsi:type="Script"
   xmlns="urn:mace:shibboleth:2.0:resolver:ad"
   id="epeList">
  <resolver:Dependency ref="myLDAP_AD" />
  <ScriptFile>/opt/shibboleth-idp/scripts/epeList.js</ScriptFile>
</resolver:AttributeDefinition>
```

Definizione dell'attributo eduPersonEntitlement Indichiamo epeList come attributo sorgente Attributo sorgent
Referenziazione di uno script esterno con gli attributi del connettore Active Directory

+++

Necessità

- Mettere l'entitlement giusto i dipendenti universitari per poter richiedere un certificato personale Geant/T
- Aggiungere l'entitlement necessario per l'amministrazione del servizio al mio username

+++

scripts/epeList.js

```
// epe per Terena personal TCS per il personale docente e non docente
if (dn.contains("ou=personale,dc=ds,dc=units,dc=it")) {
  epeList.getValues().add("urn:mace:terena.org:tcs:personal-user");
}
/* Admins, by sAMAccountName */
sAMAccountName_value = sAMAccountName.getValues().get(0);
```

```
if (sAMAccountName_value == "555"){
 epeList.getValues().add("urn:mace:terena.org:tcs:personal-admin");
}
```

Permetto di generare certificati personali ad una OUall'utente amministratore viene *aggiunto* l'ePE di ammini

+++

stessa cosa per EZproxy hosted

```
// epe to administer hosted EZproxy instance
if (typeof memberOf != "undefined" && memberOf != null ){
 for ( i = 0; memberOf != null && i < memberOf.getValues().size(); i++ ){
  value = memberOf.getValues().get(i);
  // if clause targets AD group name
  if (value.indexOf("SBA-OCLC-Admins") > 0){
   epeList.getValues().add("it.units:sba-oclc-admin");
  }
 }
}
```

Aggiungo l'entitlement di amministrazion per gli utenti appartenenti al gruppo AD SBA-OCLC-Admins

+++

Riesco a fare le stesse cose usando un attributo di tipo Mapped?

Rilasciare l'eduPersonEntitlement...

...solo a chi se lo merita

+++

attribute-filter.xml - PolicyRequirementRule

```
<!-- TERENA Certificate Services TCS certificati personali -->
<AttributeFilterPolicy id="releaseToTCSpersonal">

 <PolicyRequirementRule xsi:type="AND">
  <Rule xsi:type="Requester" value="https://www.digicert.com/sso" />
  <Rule xsi:type="Value" attributeID="eduPersonAffiliation"
   value="staff"/>
 </PolicyRequirementRule>

 <AttributeRule attributeID="eduPersonEntitlement">
  <PermitValueRule xsi:type="ValueRegex"
  regex="^urn:mace:terena.org:tcs:.*$" />
 </AttributeRule>

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

```
    <PermitValueRule xsi:type="ANY" />
   </AttributeRule>
   <AttributeRule attributeID="mail">
    <PermitValueRule xsi:type="ANY" />
   </AttributeRule>
  </AttributeFilterPolicy>
```

quando (richiedente + particolare affiliazione) cosa (quale/i dei valori di entitlement)

altri attributi richiesti dal servizio

+++

Rilasciamo i valori di eduPersonEntitlement richiesti dal singolo servizio

```
  <!-- Release the 'eduPersonEntitlement' attribute with
   a specific value to Elsevier ScienceDirect SP
   (identified by its entityID) -->
  <AttributeFilterPolicy id="Elsevier_ScienceDirect">
   <PolicyRequirementRule xsi:type="Requester"
    value="https://sdauth.sciencedirect.com/" />

   <AttributeRule attributeID="eduPersonEntitlement">
    <PermitValueRule xsi:type="Value"
     value="urn:mace:dir:entitlement:common-lib-terms"
     ignoreCase="true" />
   </AttributeRule>
  </AttributeFilterPolicy>
```

Solo a ScienceDirect

Per l'attributo eduPersonEntitlement

Solo il valore urn:mace:dir:entitlement:common-lib-terms

sovrapposizione di più AttributeFilterPolicy

il caso di eduPersonEntitlement

- Buone pratiche di federazione applicano varie policy sugli attributi
- AFP IDEM default
- AFP IDEM onlyIfRequired
- AFP Code of Conduct
- AFP r+s
- AFP da resource registry

sovrapposizione di più AttributeFilterPolicy

il caso di eduPersonEntitlement

E' bene evitare la sovrapposizione di più regole di filtraggio.

Vediamo perché:

https://github.com/speedj/IdemDay18-Daniele/tree/master/eduPersonEntitlement

Casi d'uso avanzati

Tips from the Community

configurazioni interessanti

Personalizzare un relying party

SAP Cloud Platform

Courtesy Marco Pirovano

+++

relying-party.xml v2

```
<!-- SAP Cloud Platform - Relying Party Configuration -->
<!-- SINTASSI PER Shib2 -->

<rp:RelyingParty
id="https://production.bocconi.ondemand.com/a287d8c16"
provider="https://idp.unibocconi-prod.it/idp/shibboleth"
defaultSigningCredentialRef="IdPCredential">

 <rp:ProfileConfiguration
 xsi:type="saml:ShibbolethSSOProfile"
 includeAttributeStatement="false"
 assertionLifetime="PT5M"
 signResponses="always"
 signAssertions="always"/>

 <rp:ProfileConfiguration
 xsi:type="saml:SAML1AttributeQueryProfile"
 assertionLifetime="PT5M"
 signResponses="always"
 signAssertions="always"/>

 <rp:ProfileConfiguration
 xsi:type="saml:SAML1ArtifactResolutionProfile"
 signResponses="always"
 signAssertions="always"/>

 <rp:ProfileConfiguration
 xsi:type="saml:SAML2SSOProfile"
 includeAttributeStatement="true"
 assertionLifetime="PT5M"
 assertionProxyCount="0"
 signResponses="always"
 signAssertions="always"
 encryptAssertions="never"
 encryptNameIds="never"/>
```

```
    <rp:ProfileConfiguration
    xsi:type="saml:SAML2ECPProfile"
    includeAttributeStatement="true"
    assertionLifetime="PT5M"
    assertionProxyCount="0"
    signResponses="always"
    signAssertions="always"
    encryptAssertions="never"
    encryptNameIds="never"/>

    <rp:ProfileConfiguration
    xsi:type="saml:SAML2AttributeQueryProfile"
    assertionLifetime="PT5M"
    assertionProxyCount="0"
    signResponses="always"
    signAssertions="always"
    encryptAssertions="never"
    encryptNameIds="never"/>

    <rp:ProfileConfiguration
    xsi:type="saml:SAML2ArtifactResolutionProfile"
    signResponses="always"
    signAssertions="always"
    encryptAssertions="never"
    encryptNameIds="never"/>

  </rp:RelyingParty>
```

+++

Errori (chiari) al reload del servizio

```
  org.springframework.beans.factory.xml.XmlBeanDefinitionStoreException:
  Line 235 in XML document from file
  [/opt/shibboleth-idp/conf/metadata-providers.xml]
  is invalid; nested exception is
  org.xml.sax.SAXParseException;
  lineNumber: 235; columnNumber: 62;
  The prefix "rp" for element "rp:RelyingParty" is not bound.
```

+++

```
  org.springframework.beans.factory.xml.XmlBeanDefinitionStoreException:
  Line 235 in XML document from file
  [/opt/shibboleth-idp/conf/metadata-providers.xml]
  is invalid;
  nested exception is org.xml.sax.SAXParseException;
  lineNumber: 235; columnNumber: 62; cvc-complex-type.2.4.a:
  Invalid content was found starting
  with element 'RelyingParty'.
  One of
  '{"urn:mace:shibboleth:2.0:metadata":MetadataProvider}'
  is expected.
```

+++

relying-party.xml v3

```
<!-- SAP Cloud Platform - Relying Party Configuration -->
<!-- SINTASSI PER Shib3 -->
<bean parent="RelyingPartyByName"
 c:relyingPartyIds="https://production.bocconi.ondemand.com/a287d8c16">
  <property name="profileConfigurations">
    <list>
      <bean parent="Shibboleth.SSO"
       p:assertionLifetime="PT5M"
       p:signResponses="true"
       p:signAssertions="true"  />
      <bean parent="SAML1.AttributeQuery"
       p:assertionLifetime="PT5M"
       p:signResponses="true"
       p:signAssertions="true" />
      <bean parent="SAML1.ArtifactResolution"
       p:signResponses="true"
       p:signAssertions="true" />
      <bean parent="SAML2.SSO"
       p:includeAttributeStatement="true"
       p:assertionLifetime="PT5M"
       p:signResponses="true"
       p:signAssertions="true"
       p:encryptAssertions="false"
       p:encryptNameIDs="false" />
      <bean parent="SAML2.ECP"
       p:includeAttributeStatement="true"
       p:assertionLifetime="PT5M"
       p:signResponses="true"
       p:signAssertions="true"
       p:encryptAssertions="false"
       p:encryptNameIDs="false" />
      <bean parent="SAML2.AttributeQuery"
       p:assertionLifetime="PT5M"
       p:signResponses="true"
       p:signAssertions="true"
       p:encryptAssertions="false"
       p:encryptNameIDs="false" />
      <bean parent="SAML2.ArtifactResolution"
      p:signResponses="true"
      p:signAssertions="true"
      p:encryptAssertions="false"
      p:encryptNameIDs="false" />
    </list>
  </property>
</bean>
```

Resilienza al reboot

credits: Simone Lanzarini

Problema:

- Qualora nel momento del riavvio una delle fonti dati (LDAP e/o DB) referenziate nel resolver non fosser momento raggiungibili, l'IDP non partirebbe correttamente, e sarebbe necessario un successivo riavvio servizio una volta ripristinata la disponibilità della fonte dati.

+++

Soluzione:

- Aggiungere al DataConnector di tipo xsi:type=LDAPDirectory o xsi:type="RelationalDatabase" questa pr

```
validatorRef="shibboleth.NonFailFastValidator"
```

Garantire rilascio attributi se una delle fonti è down

credits: Simone Lanzarini

Background:

- abbiamo due categorie di utenti, una con i dati su DB, l'altra con i dati su LDAP. Nel resolver gli attributi configurati con una doppia Dependency: dal connettore LDAP e da quello DB.

+++

Problema:

- qualora una delle due fonti dati (DB o LDAP) diventi indisponibile, fallisce il reperimento degli attributi ar presenti sull'altra fonte dati.

Soluzione:

- aggiungere un failover dataconnector

+++

Problema2:

- Non è banale attivare dei VERI connettori di failover, e metterne uno con dati fake non è corretto, in qua failure verrebbero ritornati attributi fake che non possiamo sapere come vengano trattati lato SP.

+++

Soluzione2:

- Definire un dataconnector fittizio di tipo static VUOTO ed inserirlo come FailoverDataConnector per TUT DataConnector

+++

```
<!-- Connettore di Failover - serve a consentire
 il rilascio degli attributi se uno dei connettori e down -->
<DataConnector id="failoverFakeConnector" xsi:type="Static">
</DataConnector>
```

Mapped attribute per eduPersonAffiliation

Credits Leonardo Mariani e Loredana Martusciello

- Si definisce il valore dell'attributo "eduPersonAffiliation" (perché mancanti nel server LDAP), sostituendo "employeeType" con i valori eduPersonAffiliation adeguati: member, staff, affliate, ecc. +++ attribute-res

```
<resolver:AttributeDefinition xsi:type="ad:Mapped"
  id="eduPersonAffiliation"
  dependencyOnly="true"
  sourceAttributeID="employeeType">
  <resolver:Dependency ref="myLDAP" />
  <resolver:AttributeEncoder xsi:type="enc:SAML2String"
   name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1"
   friendlyName="eduPersonAffiliation" />

    <ad:DefaultValue>affiliate</ad:DefaultValue>
    <!-- da completare con i ruoli all'interno del proprio ente -->

    <ad:ValueMap>
      <ad:ReturnValue>affiliate</ad:ReturnValue>

      <ad:SourceValue>convenzionato</ad:SourceValue>
      <ad:SourceValue>fornitore</ad:SourceValue>
      <ad:SourceValue>ospite</ad:SourceValue>
    </ad:ValueMap>

    <ad:ValueMap>
      <ad:ReturnValue>member</ad:ReturnValue>

      <ad:SourceValue>1\s.+</ad:SourceValue> <!-- Direttore -->
      <ad:SourceValue>2\s.+</ad:SourceValue> <!-- dipendente tempo indeterminato -->
      <ad:SourceValue>3\s.+</ad:SourceValue> <!-- dipendente tempo determinato -->
      <ad:SourceValue>4\s.+</ad:SourceValue> <!-- borsisti -->
      <ad:SourceValue>5\s.+</ad:SourceValue> <!-- collaboratori scientifici -->
      <ad:SourceValue>6\s.+</ad:SourceValue> <!-- Collaboratori con contratto d'opera -->
      <ad:SourceValue>7\s.+</ad:SourceValue> <!-- Collaboratori esterni -->
      <ad:SourceValue>8\s.+</ad:SourceValue> <!-- Collaboratori con assegno di ricerca -->
      <ad:SourceValue>9\s.+</ad:SourceValue> <!-- Collaboratori occasionali -->
      <ad:SourceValue>11\s.+</ad:SourceValue> <!-- Collaboratori con procedura comparativa -->
      <ad:SourceValue>10\s.+</ad:SourceValue> <!-- Collaboratori con contratto interinale -->
    </ad:ValueMap>

    <ad:ValueMap>
      <ad:ReturnValue>staff</ad:ReturnValue>

      <ad:SourceValue>1\s.+</ad:SourceValue> <!-- Direttore -->
      <ad:SourceValue>2\s.+</ad:SourceValue> <!-- dipendente tempo indeterminato -->
      <ad:SourceValue>3\s.+</ad:SourceValue> <!-- dipendente tempo determinato -->
      <ad:SourceValue>4\s.+</ad:SourceValue> <!-- borsisti -->
      <ad:SourceValue>5\s.+</ad:SourceValue> <!-- collaboratori scientifici -->
      <ad:SourceValue>6\s.+</ad:SourceValue> <!-- Collaboratori con contratto d'opera -->
      <ad:SourceValue>7\s.+</ad:SourceValue> <!-- Collaboratori esterni -->
      <ad:SourceValue>8\s.+</ad:SourceValue> <!-- Collaboratori con assegno di ricerca -->
      <ad:SourceValue>9\s.+</ad:SourceValue> <!-- Collaboratori occasionali -->
      <ad:SourceValue>11\s.+</ad:SourceValue> <!-- Collaboratori con procedura comparativa -->
      <ad:SourceValue>10\s.+</ad:SourceValue> <!-- Collaboratori con contratto interinale -->
    </ad:ValueMap>

    <ad:ValueMap>
      <ad:ReturnValue>student</ad:ReturnValue>

      <ad:SourceValue>4\s.+</ad:SourceValue> <!-- borsisti -->
      <ad:SourceValue>8\s.+</ad:SourceValue> <!-- Collaboratori con assegno di ricerca -->
    </ad:ValueMap>
```

```
</resolver:AttributeDefinition>
```

Uso dell'attributo **mapped**

Definizione dell'attributo sorgente e la sua dipendenza (ldap)

Definizione di un valore di default

Definizione delle mappature

Ringraziamenti

- Davide Vaghetti
- Barbara Monticini
- Francesco Sansone
- MARCO MALAVOLTI
- Nunzio Napolitano

Contributi alla community

- Shibboleth
  - Davide Bottalico - unina
  - Leonardo Mariani - iit cnr
  - Loredana Martusciello - iit cnr
  - Marco Pirovano - unibocconi
  - Simone Lanzarini - cineca
- SimpleSAMLphp (che pubblicheremo)
  - Enrico M.V. Fasanelli - infn lecce
  - Matteo Carangelo - iulm

This is the end

No more slides beyond this point

Ask questions, get some refreshments, do phonecalls, check your social networks and chats.

Copyleft

una lettera a Creative Commons, PO Box 1866, Mountain View, CA 94042, USA. Alcune immagini hanno lic
differenti e sono indicate sulle immagini stesse.

Technical

- See GitPitch Wiki for details.
- Use GitHub Flavored Markdown For Slide Content Creation https://guides.github.com/features/masterin