Ολοκλήρωση υπηρεσιών καταλόγου ενοποιημένης πρόσβασης (LDAP Server και μηχανισμός shibboleth) για πιστοποίηση των μελών της Ακαδημαϊκής και Ερευνητικής κοινότητας" και πρόσβασή τους σε διιδρυματικές εφαρμογές

Παραδοτέο: Ένταξη καταλόγων στην υποδομή ταυτοποίησης και εξουσιοδότησης (Authentication & Authorization Infrastructure – AAI)

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

1. ΕΙΣΑΓΩΓΗ

Η Υποδομή Ταυτοποίησης και Εξουσιοδότησης του ΕΔΕΤ (*Authentication & Authorization Infrastructure - AAI*) επιτρέπει σε διαφορετικούς οργανισμούς να συνεργάζονται στην εκχώρηση δικαιωμάτων πρόσβασης για εφαρμογές που έχουν διιδρυματικό χαρακτήρα. Μέσω της υποδομής, οι χρήστες της Ομοσπονδίας μπορούν να λάβουν υπηρεσίες με ασφάλεια και εμπιστευτικότητα των προσωπικών τους δεδομένων χρησιμοποιώντας απλά τον ιδρυματικό τους λογαριασμό.

Η υλοποίηση και ένταξη ενός **Παρόχου Ταυτότητας** στην Ομοσπονδία του ΕΔΕΤ έχει πολλαπλό όφελος για τους χρήστες του:

- η είσοδος στις συνδεδεμένες με την Ομοσπονδία υπηρεσίες γίνεται με τη χρήση του υπάρχοντος ιδρυματικού λογαριασμού του χρήστη, χωρίς να απαιτείται ξεχωριστή εγγραφή
- τα στοιχεία που αφορούν την ταυτότητα, ιδιότητα και προέλευση του κάθε χρήστη δεν είναι απαραίτητο να αποστέλλονται στον κάθε πάροχο υπηρεσίας, παρέχοντας δυνατότητα *ανώνυμης* πιστοποιημένης πρόσβασης

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

2. ΠΕΡΙΓΡΑΦΗ ΛΕΙΤΟΥΡΓΙΑΣ IDP ΓΙΑ ΤΗΝ ΕΙΣΟΔΟ ΕΝΟΣ ΧΡΗΣΤΗ ΣΕ ΕΝΑΝ ΠΑΡΟΧΟ ΥΠΗΡΕΣΙΩΝ (SP)

Σε μία ομοσπονδία AAI συμμετέχουν δύο τύποι οντοτήτων.

- Πάροχοι Ταυτότητας - Identity Providers (IDPs): Οι IDPs κατέχουν την πληροφορία σχετικά με τους χρήστες ενός οργανισμού όπως π.χ. τα στοιχεία τους, τα credentials τους και τα δικαιώματά τους
- Πάροχοι Υπηρεσιών - Service Providers (SPs): Οι SPs προφέρουν υπηρεσίες προς τους χρήστες των οργανισμών που μετέχουν στην ομοσπονδία

Η λειτουργία του shibboleth IDP βασίζεται στην ανταλλαγή μηνυμάτων σύμφωνα με το πρωτόκολο SAML με συμβατούς service providers. Η διαδικασία login ενός χρήστη ενός IDP σε έναν SP είναι η εξής:

1. Ο χρήστης επισκέπτεται τη σελίδα του Service Provider και επιλέγει να κάνει login μέσω της Ομοσπονδίας.
2. Ο χρήστης ανακατευθύνεται στη σελίδα WAYF (Where Are You From) της Ομοσπονδίας, όπου επιλέγει τον οργανισμό στον οποιο ανήκει
3. Ο χρήστης ανακατευθύνεται στη σελίδα του IDP του οργανισμού όπου και εισάγει τα credentials του.
4. Ο IDP παράγει ένα κρυπτογραφημένο SAML μήνυμα και ανακατευθύνει τον χρήστη στην αρχική σελίδα του Service Provider με το μήνυμα αυτό.
5. Ο Service provider αποκρυπτογραφεί το SAML μήνυμα για να πάρει πληροφορίες για τον χρήστη υπό μορφή ενός ID και ζευγαριών attibute – value.

3. ΔΙΑΔΙΚΑΣΙΑ ΕΝΤΑΞΗΣ ΦΟΡΕΑ ΣΤΗΝ ΟΜΟΣΠΟΝΔΙΑ AAI

Για την ένταξη ενός οργανισμού στην ομοσπονδία του ΕΔΕΤ απαιτείται η εγκατάσταση και λειτουργίας από μέρους του ενός Παρόχου Ταυτότητας (IDP).

Στη συνέχεια και εφόσον ο φορέας διαθέτει IDP, πρέπει να ολοκληρωθούν τα εξής βήματα για την ένταξή του στην Ομοσπονδία:

1. Δημιουργία Ψηφιακών Πιστοποιητικών
2. Παραμετροποίηση Identity Provider
3. Δημοσίευση των μεταδεδομένων του Identity Provider στην Ομοσπονδία.

Στα κεφάλαια που ακολουθούν περιγράφονται λεπτομερώς τα παραπάνω βήματα.

3.1 ΔΗΜΙΟΥΡΓΙΑ ΨΗΦΙΑΚΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

Για την κρυπτογράφηση της επικοινωνίας μεταξύ των πελατών - χρηστών και του IDP αλλά και μεταξύ των μελών της Ομοσπονδίας χρησιμοποιούνται ψηφιακά πιστοποιητικά. Το ΕΔΕΤ παρέχει τη σχετική υπηρεσία PKI μέσω της οποίας είναι δυνατόν να εκδοθούν ψηφιακά πιστοποιητικά υπογεγραμμένα από γνωστή Αρχή Πιστοποίησης η οποία είναι ήδη εγκατεστημένη στη συντριπτική πλειοψηφία όλων των πελατών. Αν ο οργανισμός μετέχει ήδη στην υπηρεσία PKI του ΕΔΕΤ προτείνεται η χρήση πιστοποιητικού από την υπηρεσία αυτή.

Παρακάτω περιγράφονται οι ενέργειες για την έκδοση πιστοποιητικού είτε self-singed είτε μέσω της υπηρεσίας PKI του ΕΔΕΤ.

3.1.1 Δημιουργία keystore

Για την έκδοση ψηφιακού πιστοποιητικού απαιτείται η δημιουργία ενός private key το οποιο σε java περιβάλλον γίνεται με τη δημιουργία ενός keystore χρησιμοποιώντας το εργαλείο keytool.

windows:

```
$[JAVA_HOME]\bin\keytool.exe -genkeypair -alias idp -keysize 4096 -keyalg RSA -sigalg SHA256withRSA -validity 1095 -dname "C=GR,O=$[ORG_NAME],OU=$[ORG_NAME] IDP,CN=$[IDP_URL]" -keystore C:\opt\certificate\idp.keystore
```

Linux:

```
$[JAVA_HOME]/bin/keytool -genkeypair -alias idp -keysize 4096 -keyalg RSA -sigalg SHA256withRSA -validity 1095 -dname "C=GR,O=$[ORG_NAME],OU=$[ORG_NAME] IDP,CN=$[IDP_URL]" -keystore /opt/certificate/idp.keystore
```

Αν χρησιμοποιηθεί self-signed πιστοποιητικό τότε αυτό έχει ήδη δημιουργηθεί με την παραπάνω εντολή και περιέχεται στο keystore. Αν γίνει υπογραφή του πιστοποιητικού μέσω της υπηρεσίας PKI τότε πρέπει να ακολουθηθούν τα βήματα της επόμενης παραγράφου.

3.1.2 Έκδοση πιστοποιητικού μέσω της υπηρεσίας PKI του ΕΔΕΤ

Δημιουργία certificate signing request:

windows:

```
$[JAVA_HOME]\bin\keytool.exe -keystore C:\opt\certificate\idp.keystore -certreq -alias idp -file C:\opt\certificate\idp.csr
```

linux:

```
$[JAVA_HOME]/bin/keytool -keystore /opt/certificate/idp.keystore -certreq -alias idp -file /opt/certificate/idp.csr
```

Το παραγόμενο αρχείο idp.csr υποβάλλεται ως certificate signing request στην υπηρεσία PKI του ΕΔΕΤ και όταν ολοκληρωθεί η διαδικασία υπογραφής παράγεται ένα αρχείο τύπου PKCS7 (.p7b) το οποίο περιέχει το πιστοποιητικό και τις σχετικές με αυτό αρχές πιστοποίησης. Με την παρακάτω εντολή εισάγετε το πιστοποιητικό στο keystore:

windows:

```
$[JAVA_HOME]\bin\keytool.exe -keystore C:\opt\certificate\idp.keystore -import -trustcacerts -file chain.p7b
```

linux:

```
$[JAVA_HOME]/bin/keytool -keystore /opt/certificate/idp.keystore -import -trustcacerts -file chain.p7b
```

3.1.3 Εξαγωγή public και private key

Για τη λειτουργία του shibboleth idp απαιτείται η εξαγωγή των public και private keys σε PEM format. Η εξαγωγή του public key γίνεται με την παρακάτω εντολή:

windows:

```
$[JAVA_HOME]\bin\keytool.exe -keystore C:\opt\certificate\idp.keystore -alias idp -file C:\opt\certificate\idp.crt -exportcert -rfc
```

linux:

```
$[JAVA_HOME]/bin/keytool -keystore /opt/certificate/idp.keystore -alias idp -file /opt/certificate/idp.crt -exportcert -rfc
```

Η εξαγωγή του private key μπορεί να γίνει με τον κώδικα που παρέχεται ExportPriv.java και με τις ακόλουθες εντολές

windows:

```
$[JAVA_HOME]\bin\javac ExportPriv.java
$[JAVA_HOME]\bin\java ExportPriv C:\opt\certificate\idp.keystore "Ο κωδικός του keystore"
```

idp “Ο κωδικός του keystore” > C:\opt\certificate\idp.key

linux:

$[JAVA_HOME]/bin/javac ExportPriv.java

$[JAVA_HOME]/bin/java ExportPriv /opt/certificate/idp.keystore “Ο κωδικός του keystore” idp “Ο κωδικός του keystore” > /opt/certificate/idp.key

3.2 ΠΑΡΑΜΕΤΡΟΠΟΙΗΣΗ IDENTITY PROVIDER

Τα βασικά αρχεία ρυθμίσεων του Shibboleth IDP βρίσκονται στο φάκελο

$[IDP_HOME]\idp\conf

και είναι τα εξής:

- **idp.properties**: Οι βασικές ρυθμίσεις για τη λειτουργία του IDP.
- **ldap.properties**: Οι ρυθμίσεις για τη σύνδεση στο LDAP (Active Directory).
- **metadata-providers.xml**: Τα metadata των συνεργαζόμενων SAML2 service providers
- **saml-nameid.properties, saml-nameid.xml**: Ρύθμιση του attribute που θα λετουργεί ως αναγνωριστικό για τους χρήστες.
- **attribute-resolver.xml**: Ορίζεται ο τρόπος με τον οποίο παίρνουν τιμές τα attributes που στέλνονται στους Service Providers.
- **attribute-filter.xml**: Ορίζεται ποια από τα ορισμένα στο attribute-resolver.xml attributes επιστρέφονται σε κάθε service provider.

Στη συνέχεια παρατίθενται οι απαραίτητες ρυθμίσεις του IDP για την επιτυχή επικοινωνία με τους περισσότερους service providers στην ομοσπονδία του ΕΔΕΤ.

3.2.1 idp.properties: Βασικές ρυθμίσεις IDP

Στο αρχείο idp.properties βρίσκονται οι βασικές ρυθμίσεις σχετικά με τη λειτουργία του IDP. Όσες ρυθμίσεις δεν αναφέρονται στη συνέχεια παραμένουν στις default τιμές τους.

- idp.entityID : Ορίζει το entityID του IDP, το οποίο είναι το βασικό αναγνωριστικό του IDP. Με βάση το entityID αναγνωρίζουν όλοι οι συνεργαζόμενοι service providers της Ομοσπονδίας τον IDP συνεπώς οι αλλαγές στο πεδίο αυτό πρέπει να γίνονται πολύ προσεκτικά καθώς μπορεί να επηρεάσουν τους συνεργαζόμενους service providers. Η τιμή του entityID είναι μορφής URI αλλά δεν είναι απαραίτητο να είναι υπάρχον URL. Κατά την εγκατάσταση παίρνει την τιμή https://**$[IDP_URL]**/idp/shibboleth .
- idp.scope : Είναι η τιμή που προστίθεται σε attributes τύπου scoped, π.χ. το EduPrincipalName το οποίο παράγεται ως username@"idp.scope". Συνηθίζεται να ορίζεται ως το βασικό domain του οργανισμού.
- idp.cookie.* : Ρυθμίσεις για τα cookie που χρησιμοποιείται από τον IDP, οι προτεινόμενες τιμες είναι:
  - idp.cookie.secure = true
  - idp.cookie.httpOnly = true
  - idp.cookie.maxAge = 31536000
- idp.sealer.* : Ρυθμίσεις σχετικά με την κρυπτογράφηση που χρησιμοποιείται εσωτερικά στον IDP, παραμένουν όπως ρυθμίζονται κατά την εγκατάσταση.

- idp.signing.* : Το ψηφιακό πιστοποιητικό που χρησιμοποιείται για την ψηφιακή υπογραφή των SAML2 μηνυμάτων που ανταλλάζει ο IDP με τους service providers της Ομοσπονδίας. Ρυθμίζεται ώστε να δίνεται το πιστοποιητικό που παράχθηκε νωρίτερα
  - idp.signing.key = %{idp.home}/../certificate/idp.key
  - idp.signing.cert = %{idp.home}/../certificate/idp.crt
- idp.encryption.* : Το ψηφιακό πιστοποιητικό που χρησιμοποιείται για την κρυπτογράφηση των SAML2 μηνυμάτων που ανταλλάζει ο IDP με τους service providers της Ομοσπονδίας. Ρυθμίζεται ώστε να δίνεται το πιστοποιητικό που παράχθηκε νωρίτερα (παρ. 3.1)
  - idp.encryption.key = %{idp.home}/../certificate/idp.key
  - idp.encryption.cert = %{idp.home}/../certificate/idp.crt

3.2.2 ldap.properties: Ρυθμίσεις σύνδεσης σε LDAP

Στο αρχείο ldap.properties βρίσκονται οι ρυθμίσεις σχετικά με τη σύνδεση στον κατάλογο χρηστών με χρήση LDAP. Για τη σύνδεση σε Active Directory απαιτούνται:

1. Η δημιουργία στο Active Directory ενός απλού (μη διαχειριστή) χρήστη τον οποίο θα χρησιμοποιεί ο IDP για να συνδεθεί και να ψάξει για να κάνει authenticate τους χρήστες.
2. Να επιτρέπεται η δικτυακή επικοινωνία από τον server που φιλοξενεί τον IDP προς το Active Directory στις πόρτες του LDAP πρωτοκόλλου (389 και 636).

Για τη ρύθμιση του IDP είναι απαραίτητη η συλλογή των παρακάτω πληροφοριών σχετικά με το Active Directory:

1. **${DC_ADDRESS}**: DNS όνομα ή IP διεύθυνση του Active Directory domain controller.
2. **${DC_CERTIFICATE}**: Το αρχείο που περιέχει το πιστοποιητικό που χρησιμοποιείται από το Active Directory σε περίπτωση που γίνεται ασφαλής σύνδεση LDAP (port 636).
3. **${BASE_DN}:** Το distinguished name κάτω από το οποίο βρίσκονται όλοι τα accounts των χρηστών που θα χρησιμοποιούν τον IDP. Αν βρίσκονται όλοι οι χρήστες κάτω από κάποιο συγκεκριμένο Organizational Unit τότε το DN του OU αυτού, αλλιώς το distinguished name του active directory domain.
4. **${USERNAME_ATTRIBUTE}**: Το Active Directory attribute που περιέχει το username με το οποίο κάνουν login οι χρήστες. Συνήθως είναι το samAccountName.
5. **${IDP_USER_PRINCIPAL_NAME}**: Το Active Directory principalName του χρήστη με τον οποίο συνδέεται ο IDP στο Active Directory.
6. **${IDP_USER_PASSWORD}**: Το password του χρήστη με τον οποίο συνδέεται ο IDP στο Active Directory.

Αν χρησιμοποιείται ασφαλής σύνδεση στο Active Directory στο αρχείο ldap.properties γίνονται οι εξής ρυθμίσεις:

- idp.authn.LDAP.ldapURL = ldap://**${DC_ADDRESS}**:389 .
- idp.authn.LDAP.useStartTLS = true
- idp.authn.LDAP.sslConfig = certificateTrust
- idp.authn.LDAP.trustCertificates = **${DC_CERTIFICATE}**

Αν δε χρησιμοποιείται ασφαλής σύνδεση ρυθμίζονται ως εξής:

- idp.authn.LDAP.ldapURL = ldap://**${DC_ADDRESS}**:636 .

- idp.authn.LDAP.useStartTLS = true
- idp.authn.LDAP.sslConfig. Μένει σχολιασμένο.
- idp.authn.LDAP.trustCertificates. Μένει στη default τιμή.

Με βάση τα παραπάνω στο αρχείο ldap.properties ορίζονται οι παρακάτω τιμές. Όσες ρυθμίσεις δεν αναφέρονται πρέπει να παραμείνουν στις default τιμές τους.

- idp.authn.LDAP.authenticator : Ορίζει τον τρόπο σύνδεσης στο Active Directory. Πρέπει να έχει την τιμή bindSearchAuthenticator.
- idp.authn.LDAP.returnAttributes = **$[USERNAME_ATTRIBUTE]**
- idp.authn.LDAP.baseDN = **$[BASE_DN]**
- idp.authn.LDAP.subtreeSearch = true
- idp.authn.LDAP.userFilter = (**$[USERNAME_ATTRIBUTE]**={user})
- idp.authn.LDAP.bindDN = **$[IDP_USER_PRINCIPAL_NAME]**
- idp.authn.LDAP.bindDNCredential = **$[IDP_USER_PASSWORD]**
- idp.attribute.resolver.LDAP.searchFilter = (samAccountName=$requestContext.principalName)

3.2.3 metadata-providers.xml: Metadata Ομοσπονδίας

Για να είναι σε θέση ο IDP να επαληθεύει τους Service Providers με τους οποίους πρέπει να συνεργάζεται και να ανταλλάζει κρυπτογραφημένα μηνύματα με αυτούς πρέπει να γνωρίζει τα metadata τους. Τα metadata είναι ένα xml αρχείο με τα URL των endpoints του Provider, τα ψηφιακά πιστοποιητικά και κάποια πληροφοριακά στοιχεία.

Η ενημέρωση του IDP σχετικά με τα metadata ενός service provider γίνεται αποθηκεύοντας το στο φάκελο metadata του IDP και προσθέτοντας μία σχετική εγγραφή στο αρχείο metadata-providers.xml. Αν το αρχείο αποθηκευτεί ως π.χ. IDP_HOME/metdata/some_sp-metadata.xml τότε στο metadata-providers.xml πρέπει να προστεθεί η παρακάτω εγγραφή τύπου FilesystemMetadataProvider:

```
<MetadataProvider id="some_sp"  xsi:type="FilesystemMetadataProvider"
metadataFile="%{idp.home}/metadata/some_sp-metadata.xml"/>
```

Το ΕΔΕΤ δημοσιεύει και ενημερώνει τα metadata όλων των Identity και Service Providers που μετέχουν στην ομοσπονδία στη διεύθυνση

```
https://aai.grnet.gr/metadata.xml
```

Συνεπώς ο σωστός τρόπος λήψης των metadata της Ομοσπονδίας είναι χρησιμοποιώντας τον FileBackedHTTPMetadataProvider του shibboleth ο οποίος ανά τακτά χρονικά διαστήματα κατεβάζει τα metadata και τα αποθηκεύει τοπικά. Η ρύθμιση του FileBackedHTTPMetadataProvider γίνεται με την προσθήκη του παρακάτω XML element στο metadata-providers.xml:

```
<MetadataProvider id="GrnetURLMD"
  xsi:type="FileBackedHTTPMetadataProvider"
  backingFile="%{idp.home}/metadata/grnet-federation-metadata.xml"
  metadataURL="https://aai.grnet.gr/metadata.xml"
```

```
    maxRefreshDelay="PT4H">

      <MetadataFilter xsi:type="SignatureValidation"
        requireSignedMetadata="true"
        certificateFile="%{idp.home}/metadata/grnet-federation-metadata.crt">
      </MetadataFilter>
      <MetadataFilter xsi:type="EntityRoleWhiteList">
        <RetainedRole>md:SPSSODescriptor</RetainedRole>
      </MetadataFilter>
    </MetadataProvider>
```

Η παραπάνω ρύθμιση ελέγχει την υπογραφή των metadata που έχει γίνει με το πιστοποιητικό του aai.grnet.gr και το οποίο υπάρχει στα metadata (Element Signature/KeyInfo) και πρέπει να αντιγραφεί εκ των προτέρων στο αρχείο

```
$[IDP_HOME]\metadata\grnet-federation-metadata.crt
```

3.2.4 saml-nameid.properties, saml-nameid.xml: Ορισμός NameID

Στα αρχεία αυτά ρυθμίζεται ο τρόπος παραγωγής του αναγνωριστικού (SAML NameID) των χρηστών. Υπάρχουν δύο δυνατοί τύποι αναγνωριστικών:

- PersistentId: Πρόκειται για ένα αναγνωριστικό τύπου UUID το οποίο παραμένει σταθερό για κάθε χρήστη σε κάθε σύνδεση του σε κάποιον service provider. Είναι ο

συνιστώμενος τρόπος ταυτοποίησης ενός χρήστη του shibboleth. Παράγεται με βάση κάποιο attribute του χρήστη το οποίο **πρέπει** να παραμένει σταθερό καθώς δεν υπάρχει τρόπος γνωστοποίησης των συνεργαζόμενων service providers της Ομοσπονδίας ότι έχει υπάρξει κάποια αλλαγή. Σε περιβάλλον Active Directory συνίσταται να χρησιμοποιείται το attribute objectSid το οποίο είναι ένα μοναδικό αναγνωριστικό που αποδίδεται αυτόματα από το Active Directory και παραμένει αμετάβλητο μέχρι τη διαγραφή του account. Προσοχή πρέπει να δοθεί στο γεγονός ότι το objectSid δεν είναι δυνατόν να ξαναδημιουργηθεί. Αν ο λογαριασμός ενός χρήστη διαγραφεί και ξαναδημιουργηθεί με τα ίδια ακριβώς στοιχεία, το objectSid του νέου λογαριασμού θα είναι παρόλα αυτά διαφορετικό συνεπώς θα οδηγήσει σε νέα PersistentId.

- TransientId: Πρόκειται για ένα αναγνωριστικό τύπου UUID το οποίο αλλάζει σε κάθε σύνδεση ενός χρήστη. Ένα τέτοιο αναγνωριστικό είναι χρήσιμο σε περιπτώσεις όπου ο service provider χρειάζεται να ξέρει ότι ένας χρήστης είναι πιστοποιημένος χρήστης του οργανισμού αλλά όχι ποιος ακριβώς είναι.

Στο αρχείο saml-nameid.properties πρέπει να μπουν οι εξής ρυθμίσεις:

Για το transientId:

```
idp.transientId.generator = shibboleth.CryptoTransientIdGenerator
```

Για το persistendId ώστε να παράγεται από το attribute objectSid με hashing χρησιμοποιώντας αλγόριθμο SHA με salt ένα τυχαίο UUID **$[UUID]**:

```
idp.persistentId.generator = shibboleth.ComputedPersistentIdGenerator
idp.persistentId.sourceAttribute = objectSid
```

```
idp.persistentId.salt = {$[UUID]}

idp.persistentId.algorithm = SHA
```

Το **$[UUID]** μπορεί να παραχθεί με οποιονδήποτε UUIDv4 generator, π.χ. τη σελίδα https://www.uuidgenerator.net

Το saml nameID που χρησιμοποιείται σε κάθε σύνδεση εξαρτάται από τον τύπο ID (persistent ή transient) που ζητά ο service provider. Στο αρχείο saml-nameid.properties ρυθμίζονται τα default NameID που χρησιμοποιούνται όταν ένας service provider δεν ζητά κάποιον συγκεκριμένο τύπο ως εξής:

```
idp.nameid.saml2.default = urn:oasis:names:tc:SAML:2.0:nameid-format:persistent

idp.nameid.saml1.default = urn:mace:shibboleth:1.0:nameIdentifier
```

Για να ενεργοποιηθεί η χρήση του PersistentId σύμφωνα με τις παραπάνω ρυθμίσεις που έγιναν στο saml-nameid.properties πρέπει στο αρχείο saml-nameid.xml να γίνει uncomment το XML element

```
<ref bean="shibboleth.SAML2PersistentGenerator" />
```

3.2.5 attribute-resolver.xml: Ορισμός shibboleth attributes

Στο αρχείο αυτό ορίζονται τα user attributes που στέλνει ο IDP στους service providers καθώς και ο τρόπος με τον οποίο αποκτούν τιμές τα attributes αυτά. Κάθε attibute –

value ζευγάρι που στέλνει ο IDP στους SP αποτελείται από έναν συμφωνημένο object identifier για το attribute και μία τιμή. Το ΕΔΕΤ δημοσιεύει στη διεύθυνση http://aai.grnet.gr/policy/policy-el.pdf την πολιτική που ακολουθούν όλα τα μέλη της Ομοσπονδίας σχετικά με τα διαθέσιμα attributes και τις πιθανές τιμές τους. Συνοπτικά πρόκειται για τα πιο κοινά πεδία ενός καταλόγου χρηστών (όνομα, επώνυμο, mail κ.α.) που συμπληρώνονται από το σχήμα EduPerson (http://aai.grnet.gr/schemas/grEduPerson/). Το Eduperson schema είναι ένα σύνολο από attributes κοινά χρησιμοποιούμενο από ένα μεγάλο αριθμό ακαδημαϊκών οργανισμών παγκοσμίως.

Η τιμή ενός attribute για κάποιον χρήστη μπορεί να προκύπτει με έναν από τους ακόλουθους τρόπους:

- Να επιστρέφεται πάντα η ίδια τιμή ανεξαρτήτως του χρήστη
- Να είναι αυτούσια η τιμή ενός attribute του χρήστη όπως αυτό είναι αποθηκευμένη στον κατάλογο χρηστών του οργανισμούς
- Να παράγεται αυτόματα με βάση ένα ή περισσότερα attributes στον κατάλογο χρηστών ή με κάποιον άλλο υπολογισμό

Στο αρχείο attribute-resolver.xml υπάρχουν δύο βασικοί τύποι δηλώσεων:

- DataConnector: Ορίζει πηγές δεδομένων που προσφέρουν ένα συγκεκριμένο σύνολο από πεδία από τα οποία μπορούν να παίρνουν τιμές τα attributes που στέλνει ο IDP, όπως:
  - LdapDataConnector: Διαβάζει τα attributes από κάποιον LDAP κατάλογο όπως το Active Directory

Ένας ldap data connector για σύνδεση στο active directory και λήψη των πιο κοινών LDAP attributes με χρήση των ρυθμίσεων που έχουν γίνει στο αρχείο ldap.properties ορίζεται ως εξής:

```
<resolver:DataConnector id="MyActiveDirectory"
  xsi:type="LDAPDirectory"
  xmlns="urn:mace:shibboleth:2.0:resolver:dc"
  ldapURL="%{idp.attribute.resolver.LDAP.ldapURL}"
  baseDN="%{idp.attribute.resolver.LDAP.baseDN}"
  principal="%{idp.attribute.resolver.LDAP.bindDN}"
principalCredential="%{idp.attribute.resolver.LDAP.bindDNCredential}"
  useStartTLS="%{idp.attribute.resolver.LDAP.useStartTLS:true}">

  <dc:FilterTemplate>
    <![CDATA[
      %{idp.attribute.resolver.LDAP.searchFilter}
    ]]>
  </dc:FilterTemplate>

 <ReturnAttributes>
    objectSid displayName cn givenName sn sAMAccountName mail
    telephoneNumber o ou schacHomeOrganization schacPersonalUniqueCode
    grEduPersonUndergraduateBranch eduPersonAffiliation
    eduPersonPrimaryAffiliation eduPersonScopedAffiliation
    eduPersonEntitlement eduPersonOrgDN eduPersonOrgUnitDN
```

```
  eduPersonPrimaryOrgUnitDN
 </ReturnAttributes>
 <LDAPProperty name="java.naming.ldap.attributes.binary" value="objectSid"/>
 <LDAPProperty name="java.naming.referral" value="follow"/>
</resolver:DataConnector>
```

- StaticDataConnector: Παρέχει ένα σύνολο από στατικα ορισμένα attributes

Ένας static connector που παρέχει το όνομα του οργανισμού φαίνεται στη συνέχεια:

```
<resolver:DataConnector id="staticAttributes"
 xsi:type="Static" xmlns="urn:mace:shibboleth:2.0:resolver:dc">

   <Attribute id="o"><Value>$[ORG_NAME]</Value></Attribute>
 </resolver:DataConnector>
```

- AttributeDefinition: Ορίζει ένα νέο attribute δηλώντας
  - τον data connector που χρησιμοποιείται
  - το source attribute του data connector από το οποίο αντιγράφονται οι τιμές
  - τον τύπο του attribute:
    - Simple: Attribute που απλώς παίρνει την τιμή που έχει το source attribute
    - Scoped: Attribute το οποίο προκύπτει από το source attribute με προσάρτηση μίας σταθερής τιμής

- SAML2NameID: Attribute που μπορεί να χρησιμοποιηθεί ως Name Identifier

Στη συνέχεια φαίνεται ο ορισμός του attribute uid με τέτοιον τρόπο ώστε η τιμή του να προκύπτει από το Active Directory attribute samAccountName.

```
<resolver:AttributeDefinition
 xsi:type="ad:Simple"
 id="uid" sourceAttributeID="samAccountName">
 <resolver:Dependency ref="MyActiveDirectory"/>
 <resolver:AttributeEncoder xsi:type="enc:SAML1String"
   name="urn:mace:dir:attribute-def:uid" />
 <resolver:AttributeEncoder xsi:type="enc:SAML2String"
   name="urn:oid:0.9.2342.19200300.100.1.1" friendlyName="uid" />
</resolver:AttributeDefinition>
```

Στην Ομοσπονδία του ΕΔΕΤ χρησιμοποιούνται κατά βάση ένα σύνολο από attributes που περιγράφονται στη σχετική πολιτική. Στο συνημμένο attribute-resolver.xml μπορείτε να βρείτε τον ορισμός των πιο κοινών attributes.

3.2.6 attribute-filter.xml: Πολιτική αποστολής attributes

Στο αρχείο attribute-resolver.xml που περιγράφηκε στην προηγούμενη παράγραφο ορίζεται ο τρόπος που αποκτούν τιμές τα attributes που γνωρίζει ο idp. Το ποια από τα διαθέσιμα attributes αποστέλλονται σε κάθε service provider συγκεκριμένα ορίζεται στο

αρχείο attribute-filter.xml. Στο αρχείο αυτό υπάρχει ένα σύνολο από AttributeFilterPolicy Elements καθένα από τα οποία ορίζει

- Το entityID ή το groupID των service providers που αφορά το συγκεκριμένο policy
- Το σύνολο των attributes και τις δυνατές τιμές τους που στέλνονται

Στα metadata της Ομοσπονδίας του ΕΔΕΤ συμμετέχουν αρκετοί service providers κάποιους από τους οποίους διαχειρίζεται το ίδιο το ΕΔΕΤ και αφορούν υπηρεσίες προς του φορείς, ενώ άλλους SPs διαχειρίζονται τρίτοι οι οποίοι μετά από συνεννόηση με το ΕΔΕΤ προσφέρουν τις υπηρεσίες τους προς τους μετέχοντες φορείς. Το κατά πόσο ένας IDP επιθυμεί να αποστέλλει κάποιες συγκεκριμένες πληροφορίες σε έναν συγκεκριμένο service provider εξαρτάται από την πολιτική του εκάστοτε οργανισμού.

Η προτεινόμενη πολιτική είναι η εξής:

- Σε όλους τους service providers στέλνονται τα NameIDs (transient και persistent) που είναι απαραίτητα για τη λειτουργία και που δεν αποκαλύπτουν πληροφορίες για τον χρήστη.
- Στα metadata της Ομοσπονδίας οι service providers που διαχειρίζεται το ίδιο το ΕΔΕΤ και παρέχουν βασικές υπηρεσίες προς την ακαδημαϊκή κοινότητα είναι ομαδοποιημένοι κάτω από το group με entityID "http://aai.grnet.gr/entities/grnet/". Προς τους service providers αυτούς προτείνεται να στέλνονται οι βασικές πληροφορίες του χρήστη όπως όνομα, mail, θέση στον οργανισμό, αριθμός μητρώου καθώς είναι συνήθως απαραίτητες για να λαμβάνουν οι χρήστες τις υπηρεσίες του ΕΔΕΤ.
- Για κάθε ένα από τους υπόλοιπους (εκτός ΕΔΕΤ) service providers τους οποίους υπάρχει επιθυμία να μπορούν να χρησιμοποιούν οι χρήστες του οργανισμού ορίζεται ξεχωριστό FilterPolicy με τα κατά περίπτωση attributes που χρειάζεται να απελευθερώνονται. Σημειώνεται ότι στα metadata ενός service provider που είναι

εισαγμένος στην ομοσπονδία αναφέρονται λεπτομερώς τα attributes που απαιτούνται ή είναι απλώς επιθυμητά για τη σύνδεση ενός χρήστη στον SP αυτό.

Το παρακάτω παράδειγμα δείχνει τον ορισμό των απαραίτητων filter policies ώστε σύμφωνα και με τα παραπάνω να στέλνονται

- σε όλους τους service providers τα NameIDs (μέσω του release του source attribute objectSid).
- Στους service providers του ΕΔΕΤ να στέλνονται τα displayName και eduPersonAffiliation
- Στον service provider με entityID https://some.test.sp/shibboleth να στέλνεται μόνο το email.

```
<afp:AttributeFilterPolicy id="releaseAnonymousIdToAnyone">
 <afp:PolicyRequirementRule xsi:type="basic:ANY"/>
  <afp:AttributeRule attributeID="eduPersonTargetedID">
   <afp:PermitValueRule xsi:type="basic:ANY"/>
  </afp:AttributeRule>
  <afp:AttributeRule attributeID="objectSid">
   <afp:PermitValueRule xsi:type="basic:ANY"/>
  </afp:AttributeRule>
</afp:AttributeFilterPolicy>

<afp:AttributeFilterPolicy id="grnet-grnet">
 <afp:PolicyRequirementRule
      xsi:type="saml:AttributeRequesterInEntityGroup"
      groupID="http://aai.grnet.gr/entities/grnet/" />
```

```
    <afp:AttributeRule attributeID="displayName">
     <afp:PermitValueRule xsi:type="basic:ANY" />
    </afp:AttributeRule>
    <afp:AttributeRule attributeID="eduPersonAffiliation">
     <afp:PermitValueRule xsi:type="basic:ANY" />
    </afp:AttributeRule>
</afp:AttributeFilterPolicy>

<afp:AttributeFilterPolicy id="test">
  <afp:PolicyRequirementRule
        xsi:type="basic:AttributeRequesterString"
        value="https://some.test.sp/shibboleth" />
    <afp:AttributeRule attributeID="mail">
     <afp:PermitValueRule xsi:type="basic:ANY" />


    </afp:AttributeRule>
</afp:AttributeFilterPolicy>
```

3.2.7 Ρύθμιση Παραμέτρων UI

Για την προσαρμογή των βασικών παραμέτρων του UI του shibboleth IDP χρειάζεται να γίνουν οι εξής ρυθμίσεις στο αρχείο **$[IDP_HOME]**\messages\error-messages.properties

```
idp.title = $[ORG_NAME] Login Service
```

```
idp.title.suffix = Error

idp.logo = $[ORG_LOGO_URL]

idp.logo.alt-text = $[ORG_NAME] logo

idp.message = An unidentified error occurred.

idp.footer = $[ORG_NAME] Login Service
```

Σημειώνεται πως το λογότυπο του οργανισμού πρέπει να σερβίρεται με https σύνδεση αλλιώς ο browser του χρήστη δε θα το εμφανίζει. Προτείνεται να αποθηκευτεί στο root του tomcat και να δοθεί η παράμετρος idp.logo ως /../logo.png.

3.3 Δημοσιευση των μεταδεδομενων του Identity Provider στην Ομοσπονδια

Για να μπορέσουν οι service providers που μετέχουν στην ομοσπονδία να επικοινωνήσουν με τον IDP πρέπει να γνωρίζουν τα βασικά του στοιχεία, όπως τα ψηφιακά πιστοποιητικά που χρησιμοποιεί και τα endpoint τους. Για το λόγο αυτό πρέπει να δημοσιευτούν τα metadata του IDP εισαγωντάς τα στα metadata της Ομοσπονδίας.

Τα metadata του IDP βρίσκονται στο αρχείο **$[IDP_HOME]**\metadata\idp-metadata.xml και πρέπει να διαμορφωθούν σύμφωνα με το ακόλουθο παράδειγμα.

```
<?xml version="1.0" encoding="UTF-8"?>

  <EntityDescriptor entityID="https://$[IDP_URL]/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"
        xmlns:mdui="urn:oasis:names:tc:SAML:2.0:metadata:ui">

    <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">$[ORG_URL]</shibmd:Scope>
          <mdui:UIInfo xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui">
            <mdui:DisplayName
xml:lang="el">$[ORG_NAME_EL]</mdui:DisplayName>
            <mdui:DisplayName
xml:lang="en">$[ORG_NAME_EN]</mdui:DisplayName>
            <mdui:InformationURL
xml:lang="en">$[ORG_SITE_EN]</mdui:InformationURL>
            <mdui:InformationURL
xml:lang="el">$[ORG_SITE_EL]</mdui:InformationURL>
            <mdui:Logo height="93" width="343">$[ORG_LOGO_URL]</mdui:Logo>
          </mdui:UIInfo>
          <mdui:DiscoHints xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui">
            <mdui:DomainHint>$[ORG_URL]</mdui:DomainHint>
            <mdui:IPHint>$[ORG_IPs]</mdui:IPHint>
```

```
            </mdui:DiscoHints>
        </Extensions>
        <KeyDescriptor>
            <ds:KeyInfo>
                <ds:X509Data>
                    <ds:X509Certificate>
$[το public key του ψηφιακού πιστοποητικού του idp]
                    </ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </KeyDescriptor>
        <ArtifactResolutionService
Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding"
Location="https://$[IDP_URL]:8443/idp/profile/SAML1/SOAP/ArtifactResolution"
index="1"/>
        <ArtifactResolutionService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="https://$[IDP_URL]: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://$[IDP_URL]/idp/profile/Shibboleth/SSO"/>
        <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://$[IDP_URL]/idp/profile/SAML2/POST/SSO"/>
        <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign" Location="https://$[IDP_URL]/idp/profile/SAML2/POST-SimpleSign/SSO"/>
        <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://$[IDP_URL]/idp/profile/SAML2/Redirect/SSO"/>
    </IDPSSODescriptor>
    <AttributeAuthorityDescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol
urn:oasis:names:tc:SAML:2.0:protocol">
        <Extensions>
          <shibmd:Scope regexp="false">$[ORG_URL]</shibmd:Scope>
        </Extensions>
        <KeyDescriptor>
          <ds:KeyInfo>
            <ds:X509Data>
              <ds:X509Certificate>
$[το public key του ψηφιακού πιστοποητικού του idp]
              </ds:X509Certificate>
            </ds:X509Data>
          </ds:KeyInfo>
        </KeyDescriptor>
```

```
        <AttributeService Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-
binding"
Location="https://$[IDP_URL]:8443/idp/profile/SAML1/SOAP/AttributeQuery"/>
        <AttributeService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="https://$[IDP_URL]:8443/idp/profile/SAML2/SOAP/AttributeQuery"/>
        <NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-
format:transient</NameIDFormat>
    </AttributeAuthorityDescriptor>
    <Organization>
        <OrganizationName xml:lang="en">$[ORG_NAME_EN]</OrganizationName>
        <OrganizationName xml:lang="el">$[ORG_NAME_EL]</OrganizationName>
        <OrganizationDisplayName
xml:lang="en">$[ORG_NAME_EN]</OrganizationDisplayName>
        <OrganizationDisplayName
xml:lang="el">$[ORG_NAME_EL]</OrganizationDisplayName>
        <OrganizationURL xml:lang="en">$[ORG_SITE_EN]</OrganizationURL>
        <OrganizationURL xml:lang="el">$[ORG_SITE_EL]</OrganizationURL>
    </Organization>
    <ContactPerson contactType="technical">
        <Company>$[ORG_NAME_EN]</Company>
        <GivenName>$[TECHNICAL_PERSON_NAME]</GivenName>
        <SurName>$[TECHNICAL_PERSON_SURNAME]</SurName>
        <EmailAddress>$[TECHNICAL_PERSON_MAIL]</EmailAddress>
```

```
<TelephoneNumber>+$[TECHNICAL_PERSON_TELEPHONE]</TelephoneNumber>
    </ContactPerson>
    <ContactPerson contactType="support">
      <Company>$[ORG_NAME_EN]</Company>
      <GivenName>$[SUPPORT_PERSON_NAME]</GivenName>
      <SurName>$[SUPPORT_PERSON_SURNAME]</SurName>
      <EmailAddress>$[SUPPORT_PERSON_MAIL]</EmailAddress>

<TelephoneNumber>+$[SUPPORT_PERSON_TELEPHONE]</TelephoneNumber>
    </ContactPerson>
  </EntityDescriptor>
```

Τα metadata πρέπει να σταλούν στο Helpdesk του ΕΔΕΤ με το αίτημα εισαγωγής του IDP του οργανισμού στην ομοσπονδία του ΕΔΕΤ.