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: Εγκατάσταση, λειτουργία και συντήρηση εικονικών καταλόγων και παρόχων ταυτότητας (IdP)

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 (Το οικοσύστημα που περιλαμβάνει όλους τους φορείς της ΕΔΕΤ και οι οποίοι δυνητικά μπορούν να έχουν πρόσβαση στις υπηρεσίες της) 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 πολλαπλά οφέλη 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 και ανάπτυξη διακριτού μηχανισμού πιστοποίησης
- 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. Ο κάθε πάροχος υπηρεσίας ορίζει τα στοιχεία που χρειάζεται από τους παρόχους ταυτότητας και εκείνοι καθορίζουν εάν αποδέχονται ή όχι την αποστολή αυτών των στοιχείων. Επιπροσθέτως, ακόμη και στην περίπτωση που οι πάροχοι ταυτότητας συναινούν στη συγκεκριμένη αποστολή στοιχείων, ο εκάστοτε χρήστες έχει τη δυνατότητα να αρνηθεί και να μην συμμετέχει στην εν λόγω υπηρεσία.

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.

1. 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
2. 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 πρωτόκολλο SAML με συμβατούς service providers. Η διαδικασία login ενός χρήστη ενός IDP σε έναν SP είναι η εξής:

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

3. ΕΓΚΑΤΑΣΤΑΣΗ ΑΠΑΡΑΙΤΗΤΟΥ ΛΟΓΙΣΜΙΚΟΥ ΓΙΑ ΤΗΝ ΕΝΤΑΞΗ ΤΟΥ ΦΟΡΕΑ ΣΤΗΝ ΟΜΟΣΠΟΝΔΙΑ AAI

Για την ένταξη ενός Φορέα στην Ομοσπονδία του ΕΔΕΤ απαιτείται η υλοποίηση ενός Παρόχου Ταυτότητας συμβατού με τα πρότυπα SAML 2.0 του οργανισμού OASIS. Στις εγκαταστάσεις που έγιναν χρησιμοποιήθηκε ο Shibboleth Identity Provider του Shibboleth Consortium https:\\shibboleth.net\products\identity-provider.html.

Απαιτούμενη για τη λειτουργία του Shibboleth Identity Provider είναι η ύπαρξη του ακόλουθου λογισμικού

- Java Runtime Environment
- Java Servlet Container

Ο Shibboleth Identity Provider εκμεταλλευόμενος τις cross-platform δυνατότητες της Java μπορεί να εγκατασταθεί τόσο σε λειτουργικό σύστημα Microsoft Windows όσο και σε λειτουργικό σύστημα Linux.

3.1 ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ MS WINDOWS

3.1.1 JRE

Ως Java Runtime Environment χρησιμοποιήθηκε το Server JRE της Oracle http:\\www.oracle.com\technetwork\java\javase\downloads\index.html στην έκδοση για windows x64.

Τα περιεχόμενα του ληφθέντος συμπιεσμένου αρχείου πρέπει να γίνουν extract στον φάκελο

```
C:\opt\java
```

Ο φάκελος στον οποία εγκαθίσταται η java (C:\opt\java) στη συνέχεια αναφέρεται ως **$[JAVA_HOME]**

3.1.2 Shibboleth Identity Provider

Για τον Shibboleth Identity Provider προτείνεται η χρήση της τελευταίας έκδοσής του (3) https:\\shibboleth.net\downloads\identity-provider\latest\ στη διάθεσή της σε μορφή συμπιεσμένου αρχείου (.zip). Τα περιεχόμενα του συμπιεσμένου αρχείου γίνονται extract σε μία προσωρινή τοποθεσία, η οποία στη συνέχεια αναφέρεται ως **$[INSTALL_BASE]**. Για την εγκατάσταση σε ένα Command Prompt εκτελούνται οι ακόλουθες εντολές ώστε να εκκινήσει ο installer του shibboleth.

```
cd $[INSTALL_BASE]\bin
set JAVA_HOME=$[JAVA_HOME]
install.bat
```

Η διαδικασία εγκατάστασης κάνει τα απαραίτητα ερωτήματα για μία βασική εγκατάσταση του shibboleth IDP. Θεωρείται πως:

1. **$[IDP_URL]** είναι το domain name στο οποίο θα λειτουργεί ο IDP π.χ. login.organization.gr
2. **$[ORG_URL]** είναι το βασικό domain του οργανισμού π.χ. organization.gr

3. **$[IDP_HOME]** είναι ο φάκελος στον οποίο θα εγκατασταθεί ο shibboleth idp και ο οποίος προτείνεται να είναι ο

C:\opt\shibboleth-idp

Στα ερωτήματα του installer πρέπει να δοθούν οι ακόλουθες απαντήσεις:

Source (Distribution) Directory: **$[INSTALL_BASE]**
Installation Directory: **$[IDP_HOME]**
Hostname: **$[IDP_URL]**
SAML EntityID: https://**$[IDP_URL]**/idp/shibboleth
Attribute Scope: **$[ORG_URL]**
TLS Private Key Password: [Ένα password για το private key του ψηφιακού πιστοποιητικού του IDP]
Cookie Encryption Key Password: [Ένα password για το encryption key των cookies]

3.1.3 Tomcat

Ως servlet container χρησιμοποιήθηκε ο open source web server και servlet container Apache Tomcat http://tomcat.apache.org/. Προτείνεται ο Tomcat 8 http://tomcat.apache.org/download-80.cgi στην έκδοση συμπιεσμένου αρχείου. Τα αρχεία του Tomcat πρέπει να γίνουν extract στον φάκελο

C:\opt\tomcat

Ο φάκελος αυτός στη συνέχεια αναφέρεται ως **$[CATALINA_BASE]**.

Στη συνέχεια πρέπει να αντιγραφεί το jar αρχείο που βρίσκεται στη διεύθυνση

https://build.shibboleth.net/nexus/service/local/repositories/releases/content/net/shibboleth/utilities/trustany-ssl/1.0.0/trustany-ssl-1.0.0.jar

στο φάκελο **$[CATALINA_BASE]**\lib ώστε να υποστηρίζεται η back channel δυνατότητα του shibboleth IDP.

Για να δημιουργηθεί το windows service που θα εκκινεί τον tomcat πρέπει να τρέξουν οι παρακάτω εντολές (δείτε και συνημμένο αρχείο service-install.bat).

```
set JAVA_HOME="$[JAVA_HOME]"

set TOMCAT_HOME="$[CATALINA_BASE]"

set IDP_HOME="$[IDP_HOME]"


"%TOMCAT_HOME%\bin\tomcat8.exe" //IS//Tomcat8 --Description "Apache Tomcat 8 Server" --DisplayName "Apache Tomcat 8.0" --Install "%TOMCAT_HOME%\bin\tomcat8.exe" --LogPath "%TOMCAT_HOME%\logs" --StdOutput auto --StdError auto --Classpath "%TOMCAT_HOME%\bin\bootstrap.jar;%TOMCAT_HOME%\bin\tomcat-juli.jar" --Jvm "%JAVA_HOME%\jre\bin\server\jvm.dll" --StartMode jvm --StopMode jvm --StartPath "%TOMCAT_HOME%" --StopPath "%TOMCAT_HOME%" --StartClass org.apache.catalina.startup.Bootstrap --StopClass org.apache.catalina.startup.Bootstrap --StartParams start --StopParams stop --JvmOptions "-Didp.home=%IDP_HOME%;-Dcatalina.home=%TOMCAT_HOME%;-Dcatalina.base=%TOMCAT_HOME%;-Djava.endorsed.dirs=%TOMCAT_HOME%\endorsed;-Djava.io.tmpdir=%TOMCAT_HOME%\temp;-Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager;-
```

```
Djava.util.logging.config.file=%TOMCAT_HOME%\conf\logging.properties" --JvmMs 128 --JvmMx 1024
```

ΠΡΟΣΟΧΗ: *στην παραπάνω εντολή το IDP_HOME πρέπει να δοθεί με unix style path separators /, δηλαδή π.χ. C:/opt/shibboleth-idp.*

Για την επεγκατάσταση του service τρέχετε τις εντολές

```
set TOMCAT_HOME="$[CATALINA_BASE]"

"%TOMCAT_HOME%\bin\tomcat8.exe" //DS//Tomcat8
```

3.2 ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ LINUX

3.2.1 JRE

Προτείνεται η εγκατάσταση του Oracle JDK 8 με χρήση του package manager του λειτουργικού συστήματος ώστε να είναι δυνατές οι αυτόματες ενημερώσεις. Σε λειτουργικό σύστημα Debian Jessie αυτό μπορεί να γίνει με τις παρακάτω εντολές:

- sudo add-apt-repository ppa:webupd8team/java
- sudo apt-get update
- sudo apt-get install oracle-java8-installer

Εναλλακτικά μπορεί να χρησιμοποιηθεί το JDK της Oracle http://www.oracle.com/technetwork/java/javase/downloads/index.html στην έκδοση για linux x64.

Τα περιεχόμενα του ληφθέντος συμπιεσμένου αρχείου πρέπει να γίνουν extract στον φάκελο

```
/opt/java
```

Ο φάκελος στον οποίο εγκαθίσταται η java (/usr/lib/jvm/java-8-oracle/ ή /opt/java για manual εγκατάσταση) στη συνέχεια αναφέρεται ως **$[JAVA_HOME]**

3.2.2 Shibboleth Identity Provider

Για τον Shibboleth Identity Provider προτείνεται η χρήση της τελευταίας διαθέσιμης έκδοσής του (3) https://shibboleth.net/downloads/identity-provider/latest/ σε μορφή συμπιεσμένου αρχείου (.zip). Τα περιεχόμενα του συμπιεσμένου αρχείου γίνονται extract σε μία προσωρινή τοποθεσία, η οποία στη συνέχεια αναφέρεται ως **$[INSTALL_BASE]**. Για την εγκατάσταση σε ένα Command Prompt εκτελούνται οι ακόλουθες εντολές ώστε να εκκινήσει ο installer του shibboleth.

```
cd $[INSTALL_BASE]/bin
export JAVA_HOME=$[JAVA_HOME]
./install.sh
```

Η διαδικασία εγκατάστασης κάνει τα απαραίτητα ερωτήματα για μία βασική εγκατάσταση του shibboleth IDP. Θεωρείται πως:

1. **$[IDP_URL]** είναι το domain name στο οποίο θα λειτουργεί ο IDP π.χ. login.organization.gr
2. **$[ORG_URL]** είναι το βασικό domain του οργανισμού π.χ. organization.gr
3. **$[IDP_HOME]** είναι ο φάκελος στον οποίο θα εγκατασταθεί ο shibboleth idp και ο οποίος προτείνεται να είναι ο

/opt/shibboleth-idp

Στα ερωτήματα του installer πρέπει να δοθούν οι ακόλουθες απαντήσεις:

Source (Distribution) Directory: **$[INSTALL_BASE]**

Installation Directory: **$[IDP_HOME]**

Hostname: **$[IDP_URL]**

SAML EntityID: https://**$[IDP_URL]**/idp/shibboleth

Attribute Scope: **$[ORG_URL]**

TLS Private Key Password: [Ένα password για το private key του ψηφιακού πιστοποιητικού του IDP]

Cookie Encryption Key Password: [Ένα password για το encryption key των cookies]

3.2.3 Tomcat

Ως servlet container χρησιμοποιήθηκε ο open source web server και servlet container Apache Tomcat http://tomcat.apache.org/ στην έκδοση 8. Προτείνεται η εγκατάσταση του tomcat 8 από τον package manager του λειτουργικού συστήματος ώστε να είναι δυνατές οι αυτόματες ενημερώσεις.

Σε λειτουργικό σύστημα Debian Jessie αυτό μπορεί να γίνει με τις παρακάτω εντολές:

- sudo apt-get update
- sudo apt-get install tomcat8

Εναλλακτικά μπορεί να ληφθεί ως συμπιεσμένο αρχείο .tar.gz από τη διεύθυνση http://tomcat.apache.org/download-80.cgi . Τα αρχεία του Tomcat πρέπει να γίνουν extract στον φάκελο

```
/opt/tomcat
```

Στην περίπτωση της manual εγκατάστασης πρέπει γίνουν οι εξής επιπλέον ενέργειες:

- Να δημιουργηθεί ο χρήστης υπό τον οποίο θα τρέχει ο tomcat

```
useradd -s /bin/bash -d $[CATALINA_BASE] tomcat
```

- Να ρυθμιστούν σωστά τα permissions των φακέλων. Για τις σχετικές οδηγίες δείτε την παράγραφο 5 “Θέματα Ασφάλειας”.

- Να δημιουργηθεί το σχετικό init script /etc/init.d/tomcat8 και να ενεργοποιηθεί με τις παρακάτω εντολές

```
chmod a+x /etc/init.d/tomcat8
update-rc.d tomcat8 defaults
```

Το αρχείο αυτό βρίσκεται συνημμένο με το όνομα tomcat8.init.

- Να δημιουργηθεί το αρχείο /etc/default/tomcat8 με το εξής περιεχόμενο

```
export CATALINA_HOME=$[CATALINA_BASE]
export CATALINA_BASE=$[CATALINA_BASE]
export TOMCAT8_USER=$[TOMCAT_USER]
export TOMCAT8_GROUP=$[TOMCAT_USER]
export JAVA_HOME=$[JAVA_HOME]
export JAVA_OPTS="-Xmx1024m -Djava.awt.headless=true -Didp.home=$[IDP_HOME]"
export AUTHBIND=yes
```

- Να εγκατασταθεί το πακέτο authbind και να ρυθμιστεί ώστε να επιτρέπει στον tomcat να ακούει στην privileged port 443 με τις εξής εντολές

```
sudo touch /etc/authbind/byport/443
```

```
sudo chmod 500 /etc/authbind/byport/443
sudo chown $[TOMCAT_USER] /etc/authbind/byport/443
```

Ο φάκελος εγκατάστασης του tomcat (/var/lib/tomcat ή /opt/tomcat για manual εγκατάσταση) στη συνέχεια αναφέρεται ως **$[CATALINA_BASE]**.

Στη συνέχεια πρέπει να αντιγραφεί το jar αρχείο που βρίσκεται στη διεύθυνση

https://build.shibboleth.net/nexus/service/local/repositories/releases/content/net/shibboleth/utilities/trustany-ssl/1.0.0/trustany-ssl-1.0.0.jar

στο φάκελο **$[CATALINA_BASE]**/lib ώστε να υποστηρίζεται η back channel δυνατότητα του shibboleth IDP.

4. ΠΑΡΑΜΕΤΡΟΠΟΙΗΣΗ ΛΟΓΙΣΜΙΚΟΥ

4.1 SHIBBOLETH 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 λειτουργεί 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.

4.1.1 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.

1. 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 .
2. 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.
3. idp.cookie.* : Ρυθμίσεις για τα cookie που χρησιμοποιείται από τον IDP, οι προτεινόμενες τιμες είναι:
    1. idp.cookie.secure = true
    2. idp.cookie.httpOnly = true
    3. idp.cookie.maxAge = 31536000
4. idp.sealer.* : Ρυθμίσεις σχετικά με την κρυπτογράφηση που χρησιμοποιείται εσωτερικά στον IDP, παραμένουν όπως ρυθμίζονται κατά την εγκατάσταση.
5. 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
    1. idp.signing.key = %{idp.home}/../certificate/idp.key

2. idp.signing.cert = %{idp.home}/../certificate/idp.crt

6. 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)
   1. idp.encryption.key = %{idp.home}/../certificate/idp.key
   2. idp.encryption.cert = %{idp.home}/../certificate/idp.crt

4.1.2 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:

- 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.
- 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. **$[DC_ADDRESS]**: DNS όνομα ή IP διεύθυνση του Active Directory domain controller.
2. **$[BASE_DN]**: Το αρχείο που περιέχει το πιστοποιητικό που χρησιμοποιείται από το Active Directory σε περίπτωση που γίνεται ασφαλής σύνδεση LDAP (port 636).

3. **$[BASE_DN]:** Το distinguished name κάτω από το οποίο βρίσκονται όλα τα accounts των χρηστών που θα χρησιμοποιούν τον IDP. Αν βρίσκονται όλοι οι χρήστες κάτω από κάποιο συγκεκριμένο Organizational Unit τότε το DN του OU αυτού, αλλιώς το distinguished name του active directory domain.
4. **$[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:

1. idp.authn.LDAP.ldapURL = ldap://**$[DC_ADDRESS]**:389 .
2. idp.authn.LDAP.useStartTLS = true
3. idp.authn.LDAP.sslConfig = certificateTrust
4. idp.authn.LDAP.trustCertificates = **$[DC_CERTIFICATE]**

Αν δεν χρησιμοποιείται ασφαλής σύνδεση ρυθμίζονται ως εξής:

5. idp.authn.LDAP.ldapURL = ldap://**$[DC_ADDRESS]**:636 .
6. idp.authn.LDAP.useStartTLS = true
7. idp.authn.LDAP.sslConfig. Μένει σχολιασμένο.
8. 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.

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

4.1.3 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 θα 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
```

4.1.4 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 νέο 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" />
```

4.1.5 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 αυτή 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 στατικά 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.

4.1.6 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 τους φορείς, ενώ άλλους SPs διαχειρίζονται τρίτοι οι οποίοι μετά από συνεννόηση με το ΕΔΕΤ προσφέρουν τις υπηρεσίες τους προς τους συμμετέχοντες 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 για 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 εισηγμένος 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>
```

4.1.7 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.

4.2 Apache Tomcat

Ο shibboleth IDP χρειάζεται να είναι προσβάσιμος μέσω internet σε δύο πόρτες, μία για το βασικό application και μία για το legacy attribute resolver. Το ποιες ακριβώς πόρτες

χρησιμοποιούνται αναφέρεται ρητά στα metadata, συστήνεται πάντως η χρήση αντιστοίχως των 443 και 8443. Η σύνδεση και στις δύο πόρτες πρέπει να γίνει με χρήση https.

Οι σχετικές ρυθμίσεις γίνονται στο αρχείο

```
$[CATALINA_BASE]\conf\server.xml
```

και φαίνονται στη συνέχεια:

```
<Service name="Catalina">
  <Connector port="443"
    protocol="org.apache.coyote.http11.Http11Protocol"
    maxThreads="150"
    SSLEnabled="true"
    scheme="https"
    secure="true"
    clientAuth="false"
    keystoreFile="/opt/certificate/idp.keystore"
    keystorePass="το password που δόθηκε κατά τη δημιουργία του πιστοποιητικού"
    keyAlias="idp"
```

```
  SSLProtocol="TLS"
/>

<Connector port="8443"
  protocol="org.apache.coyote.http11.Http11NioProtocol"
  maxThreads="150"
  SSLEnabled="true"
  scheme="https"
  secure="true"
  clientAuth="want"
  keystoreFile="/opt/certificate/idp.keystore"
  keystorePass="το password που δόθηκε κατά τη δημιουργία του πιστοποιητικού"
  keyAlias="idp"
  SSLProtocol="TLS"
 trustManagerClassName="net.shibboleth.utilities.ssl.TrustAnyCertificate"
/>

<Engine name="Catalina" defaultHost="localhost">
  <Host name="localhost"
     appBase="webapps"
    unpackWARs="false"
     autoDeploy="false"
```

```
      xmlValidation="false"
       xmlNamespaceAware="false">

       <Valve className="org.apache.catalina.valves.AccessLogValve"
          directory="logs"
          prefix="localhost_access_log" suffix=".txt"
          pattern="%h %l %u %t &amp;quot;%r&amp;quot; %s %b" />
     </Host>
   </Engine>
 </Service>
```

Το java application του shibboleth idp βρίσκεται σε μορφή .war πακέτου στο φάκελο

```
$[IDP_HOME]\war\idp.war
```

Για να ενεργοποιηθεί το application στον tomcat πρέπει να προστεθεί στο configuration του tomcat το αρχείο

```
$[CATALINA_BASE]\conf\Catalina\localhost\idp.xml
```

με το εξής περιεχόμενο

```
<Context docBase="$[IDP_HOME]/war/idp.war"
        privileged="true"
        antiResourceLocking="false"
        swallowOutput="true" />
```

Για την επιτάχυνση της διαδικασίας εκκίνησης του tomcat προτείνεται η προσάρτηση των παρακάτω γραμμών κώδικα στο property tomcat.util.scan.StandardJarScanFilter.jarsToSkip του αρχείου **$[CATALINA_BASE]**\conf\catalina.properties.

```
,\
activation-1.1.jar,\
antlr-2.7.7.jar,\
aopalliance-1.0.jar,\
bcprov-jdk15on-1.51.jar,\
c3p0-0.9.2.1.jar,\
commons-codec-1.10.jar,\
commons-collections-3.2.1.jar,\
commons-compiler-2.7.8.jar,\
commons-lang-2.4.jar,\
cryptacular-1.0.jar,\
dom4j-1.6.1.jar,\
guava-18.0.jar,\
hibernate-commons-annotations-4.0.4.Final.jar,\
hibernate-core-4.3.5.Final.jar,\
hibernate-entitymanager-4.3.5.Final.jar,\
```

```
hibernate-jpa-2.1-api-1.0.0.Final.jar,\
httpclient-4.3.6.jar,\
httpclient-cache-4.3.6.jar,\
httpcore-4.3.3.jar,\
idp-attribute-api-3.1.2.jar,\
idp-attribute-filter-api-3.1.2.jar,\
idp-attribute-filter-impl-3.1.2.jar,\
idp-attribute-filter-spring-3.1.2.jar,\
idp-attribute-resolver-api-3.1.2.jar,\
idp-attribute-resolver-impl-3.1.2.jar,\
idp-attribute-resolver-spring-3.1.2.jar,\
idp-authn-api-3.1.2.jar,\
idp-authn-impl-3.1.2.jar,\
idp-cas-api-3.1.2.jar,\
idp-cas-impl-3.1.2.jar,\
idp-consent-3.1.2.jar,\
idp-core-3.1.2.jar,\
idp-profile-api-3.1.2.jar,\
idp-profile-impl-3.1.2.jar,\
idp-profile-spring-3.1.2.jar,\
idp-saml-api-3.1.2.jar,\
idp-saml-impl-3.1.2.jar,\
```

```
idp-schema-3.1.2.jar,\
idp-session-api-3.1.2.jar,\
idp-session-impl-3.1.2.jar,\
idp-ui-3.1.2.jar,\
jandex-1.1.0.Final.jar,\
janino-2.7.8.jar,\
javassist-3.18.1-GA.jar,\
java-support-7.1.1.jar,\
javax.json-1.0.4.jar,\
javax.json-api-1.0.jar,\
jboss-logging-3.1.3.GA.jar,\
jboss-logging-annotations-1.2.0.Beta1.jar,\
jboss-transaction-api_1.2_spec-1.0.0.Final.jar,\
jcl-over-slf4j-1.7.10.jar,\
jcommander-1.47.jar,\
joda-time-2.7.jar,\
jsr305-3.0.0.jar,\
ldaptive-1.0.6.jar,\
logback-classic-1.1.2.jar,\
logback-core-1.1.2.jar,\
mail-1.4.7.jar,\
mchange-commons-java-0.2.3.4.jar,\
```

```
ognl-2.6.11.jar,\
opensaml-core-3.1.1.jar,\
opensaml-messaging-api-3.1.1.jar,\
opensaml-messaging-impl-3.1.1.jar,\
opensaml-profile-api-3.1.1.jar,\
opensaml-profile-impl-3.1.1.jar,\
opensaml-saml-api-3.1.1.jar,\
opensaml-saml-impl-3.1.1.jar,\
opensaml-security-api-3.1.1.jar,\
opensaml-security-impl-3.1.1.jar,\
opensaml-soap-api-3.1.1.jar,\
opensaml-soap-impl-3.1.1.jar,\
opensaml-storage-api-3.1.1.jar,\
opensaml-storage-impl-3.1.1.jar,\
opensaml-xmlsec-api-3.1.1.jar,\
opensaml-xmlsec-impl-3.1.1.jar,\
slf4j-api-1.7.10.jar,\
spring-aop-4.1.5.RELEASE.jar,\
spring-beans-4.1.5.RELEASE.jar,\
spring-binding-2.4.1.RELEASE.jar,\
spring-context-4.1.5.RELEASE.jar,\
spring-context-support-4.1.5.RELEASE.jar,\
```

```
spring-core-4.1.5.RELEASE.jar,\
spring-expression-4.1.5.RELEASE.jar,\
spring-extensions-5.1.1.jar,\
spring-jdbc-4.1.5.RELEASE.jar,\
spring-js-2.4.1.RELEASE.jar,\
spring-js-resources-2.4.1.RELEASE.jar,\
spring-orm-4.1.5.RELEASE.jar,\
spring-tx-4.1.5.RELEASE.jar,\
spring-web-4.1.5.RELEASE.jar,\
spring-webflow-2.4.1.RELEASE.jar,\
spring-webmvc-4.1.5.RELEASE.jar,\
spymemcached-2.11.4.jar,\
stax2-api-3.1.4.jar,\
stax-api-1.0-2.jar,\
velocity-1.7.jar,\
woodstox-core-asl-4.4.1.jar,\
xml-apis-1.0.b2.jar,\
xmlsec-2.0.3.jar
```

4.3 Ρυθμισεις Active Directory

Το Active Directory δεν απαιτεί κάποια ρύθμιση για να λειτουργήσει με το shibboleth IDP. Προτείνεται όμως να ενεργοποιηθεί η δυνατότητα κρυπτογραφημένης σύνδεσης

ldap καθώς και να γίνει extend το σχήμα του Active Directory με το EduPerson σχήμα ώστε να αποθηκεύονται σε αυτό και τα σχετικά attributes.

4.3.1 Ενεργοποίηση κρυπτογραφημένης σύνδεσης ldap

Για την ενεργοποίηση της κρυπτογραφημένης σύνδεσης από τον IDP στο active directory απαιτείται:

1. Η εγκατάσταση ψηφιακού πιστοποιητικού στον Active Directory Domain Controller
2. Η ρύθμιση του IDP να εμπιστεύεται το συγκεκριμένο πιστοποιητικό

Το πιστοποιητικό που θα εγκατασταθεί στον Domain Controller πρέπει να έχει τα εξής χαρακτηριστικά:

- Να έχει εκδοθεί για το πλήρες όνομα (Fully Qualified Domain Name) του domain controller
- Η επέκταση Extended Key Usage να περιέχει το Server Authentication (1.3.6.1.5.5.7.3.1) object identifier
- Να έχει εκδοθεί από αρχή πιστοποίησης που εμπιστεύεται ο domain controller.

Για την έκδοση ενός τέτοιου πιστοποιητικού μπορεί να χρησιμοποιηθούν τα scripts που βρίσκονται στον φάκελο miniCA στα συνημμένα αρχεία. Τα scripts αυτά δημιουργούν μία μικρή αρχή πιστοποίησης (script InitCA) και στη συνέχεια με βάση αυτή μπορούν να δημιουργηθούν πιστοποιητικά για τους domain controllers χρησιμοποιώντας το script createCert.sh. Τα scripts αυτά απαιτούν τη χρήση openssl και bash.

Το πιστοποιητικό της αρχής πιστοποίησης πρέπει να εγκατασταθεί στα “Trusted Root Certification Authorities” του service account Active Directory Domain Services, ενώ το

πιστοποιητικό του Domain Controller στα personal certificates του service account Active Directory Domain Services. Η ενεργοποίηση του πιστοποιητικού γίνεται με επανεκκίνηση της υπηρεσίας του Active Directory Domain Services.

Για την ενεργοποίηση της κρυπτογραφημένης σύνδεσης από τον IDP στο Active Directory αποθηκεύεται στον φάκελο credentials του IDP το public key του πιστοποιητικού του domain controller στο αρχείο **$[DC_CERTIFICATE]**. Στη συνέχεια γίνονται οι ακόλουθες ρυθμίσεις:

Αρχείο ldap.properties:

```
idp.authn.LDAP.useStartTLS = true
idp.authn.LDAP.sslConfig = certificateTrust
idp.authn.LDAP.trustCertificates = $[DC_CERTIFICATE]
```

Αρχείο attribute-resolver.xml:

Προστίθεται το ακόλουθο element στον LDAP DataConnector

```
<dc:StartTLSTrustCredential id="LDAPtoIdPCredential" xsi:type="sec:X509ResourceBacked">
  <sec:Certificate>
    %{idp.attribute.resolver.LDAP.trustCertificates}
  </sec:Certificate>
</dc:StartTLSTrustCredential>
```

4.3.2 Εισαγωγή στο Active Directory του EduPerson schema

Το EduPerson σχήμα είναι ένα σύνολο από attributes συχνά χρησιμοποιούμενα στην ακαδημαϊκή κοινότητα. Περισσότερες πληροφορίες για το ορισμό των πεδίων και τον τρόπο χρήσης του μπορούν να βρεθούν στη δημοσιευμένη πολιτική της ομοσπονδίας του ΕΔΕΤ http://aai.grnet.gr/policy/policy-el.pdf . Τα πεδία αυτά δεν περιέχονται στα υπάρχοντα schemas του Active Directory. Για την ευκολότερη διαχείρισή τους προτείνεται:

1. Η επέκταση του Active Directory ώστε να περιέχει το EduPerson schema
2. Η προσθήκη σχετικής καρτέλας στην κονσόλα Active Directory Users and Computers.

Η εισαγωγή του EduPerson schema στο Active Directory γίνεται χρησιμοποιώντας ένα LDAP Data Interchange Format αρχείο (ldif), το οποίο περιέχει τους σχετικούς ορισμούς και το built-in εργαλείο των windows ldifde με την παρακάτω εντολή:

- ldifde -i -f eduPerson.adschema.ldif -v -j <PATH TO LOGFILES>

Τα περιεχόμενα του αρχείου eduPerson.adschema.ldif είναι τα εξής:

- #
  ==========
  ==========
  ========
- #

- # File: eduPerson.ldf
- # Version: 200806
- #
- # This file should be imported with the following command while logged in to the Domain Controller as an Admin User:
- # ldifde -i -f eduPerson.adschema.ldif -v -j <PATH TO LOGFILES>
- #
- # REMEMBER TO SEARCH AND REPLACE $[BASE_DN] WITH YOUR DC SUFFIX
- #
- # ==========
- #
- # ==========
- # Attributes
- # ==========
- dn: CN=eduPersonAffiliation,CN=Schema,CN=Configuration,$[BASE_DN]

- changetype: ntdsschemaadd
- objectClass: top
- objectClass: attributeSchema
- cn: eduPersonAffiliation
- lDAPDisplayName: eduPersonAffiliation
- adminDisplayName: eduPersonAffiliation
- adminDescription: Specifies the person's relationship(s) to the institution, permissible values: faculty, student, staff, alum, member, affiliate, employee
- attributeID: 1.3.6.1.4.1.5923.1.1.1.1
- attributeSyntax: 2.5.5.12
- oMSyntax: 64
- isSingleValued: FALSE
- searchFlags: 1
- showInAdvancedViewOnly: TRUE
- systemOnly: FALSE
-
- dn: CN=eduPersonNickname,CN=Schema,CN=Configuration,$[BASE_DN]
- changetype: ntdsschemaadd
- objectClass: top
- objectClass: attributeSchema
- cn: eduPersonNickname
- lDAPDisplayName: eduPersonNickname

- adminDisplayName: eduPersonNickname
- adminDescription: Person's nickname, or the informal name by which they are accustomed to be hailed
- attributeID: 1.3.6.1.4.1.5923.1.1.1.2
- attributeSyntax: 2.5.5.12
- oMSyntax: 64
- isSingleValued: FALSE
- searchFlags: 1
- showInAdvancedViewOnly: TRUE
- systemOnly: FALSE
-
- dn: CN=eduPersonOrgDN,CN=Schema,CN=Configuration,$[BASE_DN]
- changetype: ntdsschemaadd
- objectClass: top
- objectClass: attributeSchema
- cn: eduPersonOrgDN
- lDAPDisplayName: eduPersonOrgDN
- adminDisplayName: eduPersonOrgDN
- adminDescription: Specifies the person's relationship(s) to the institution, permissible values: faculty, student, staff, alum, member, affiliate, employee
- attributeID: 1.3.6.1.4.1.5923.1.1.1.3
- attributeSyntax: 2.5.5.12

- oMSyntax: 64
- isSingleValued: TRUE
- searchFlags: 0
- showInAdvancedViewOnly: TRUE
- systemOnly: FALSE
-
- dn: CN=eduPersonOrgUnitDN,CN=Schema,CN=Configuration,$[BASE_DN]
- changetype: ntdsschemaadd
- objectClass: top
- objectClass: attributeSchema
- cn: eduPersonOrgUnitDN
- lDAPDisplayName: eduPersonOrgUnitDN
- adminDisplayName: eduPersonOrgUnitDN
- adminDescription: The distinguished name(s) (DN) of the directory entries representing the person's Organizational Unit(s)
- attributeID: 1.3.6.1.4.1.5923.1.1.1.4
- attributeSyntax: 2.5.5.12
- oMSyntax: 64
- isSingleValued: FALSE
- searchFlags: 0
- showInAdvancedViewOnly: TRUE
- systemOnly: FALSE

-
- dn: CN=eduPersonPrimaryAffiliation,CN=Schema,CN=Configuration,$[BASE_DN]
- changetype: ntdsschemaadd
- objectClass: top
- objectClass: attributeSchema
- cn: eduPersonPrimaryAffiliation
- lDAPDisplayName: eduPersonPrimaryAffiliation
- adminDisplayName: eduPersonPrimaryAffiliation
- adminDescription: Specifies the person's PRIMARY relationship to the institution in broad categories such as student, faculty, staff, alum, etc
- attributeID: 1.3.6.1.4.1.5923.1.1.1.5
- attributeSyntax: 2.5.5.12
- oMSyntax: 64
- isSingleValued: TRUE
- searchFlags: 1
- showInAdvancedViewOnly: TRUE
- systemOnly: FALSE
-
- dn: CN=eduPersonPrincipalName,CN=Schema,CN=Configuration,$[BASE_DN]
- changetype: ntdsschemaadd
- objectClass: top

- objectClass: attributeSchema
- cn: eduPersonPrincipalName
- lDAPDisplayName: eduPersonPrincipalName
- adminDisplayName: eduPersonPrincipalName
- adminDescription: The "NetID" of the person for the purposes of inter-institutional authentication. It should be represented in the form "user@scope" where scope defines a local security domain
- attributeID: 1.3.6.1.4.1.5923.1.1.1.6
- attributeSyntax: 2.5.5.12
- oMSyntax: 64
- isSingleValued: TRUE
- searchFlags: 1
- showInAdvancedViewOnly: TRUE
- systemOnly: FALSE
-
- dn: CN=eduPersonEntitlement,CN=Schema,CN=Configuration,$[BASE_DN]
- changetype: ntdsschemaadd
- objectClass: top
- objectClass: attributeSchema
- cn: eduPersonEntitlement
- lDAPDisplayName: eduPersonEntitlement
- adminDisplayName: eduPersonEntitlement

- adminDescription: URI (either URN or URL) that indicates a set of rights to specific resources
- attributeID: 1.3.6.1.4.1.5923.1.1.1.7
- attributeSyntax: 2.5.5.12
- oMSyntax: 64
- isSingleValued: FALSE
- searchFlags: 1
- showInAdvancedViewOnly: TRUE
- systemOnly: FALSE
-
- dn: CN=eduPersonPrimaryOrgUnitDN,CN=Schema,CN=Configuration,$[BASE_DN]
- changetype: ntdsschemaadd
- objectClass: top
- objectClass: attributeSchema
- cn: eduPersonPrimaryOrgUnitDN
- lDAPDisplayName: eduPersonPrimaryOrgUnitDN
- adminDisplayName: eduPersonPrimaryOrgUnitDN
- adminDescription: The distinguished name (DN) of the directory entry representing the person's primary Organizational Unit(s)
- attributeID: 1.3.6.1.4.1.5923.1.1.1.8
- attributeSyntax: 2.5.5.12
- oMSyntax: 64

- isSingleValued: TRUE
- searchFlags: 0
- showInAdvancedViewOnly: TRUE
- systemOnly: FALSE
-
- dn: CN=eduPersonScopedAffiliation,CN=Schema,CN=Configuration,$[BASE_DN]
- changetype: ntdsschemaadd
- objectClass: top
- objectClass: attributeSchema
- cn: eduPersonScopedAffiliation
- lDAPDisplayName: eduPersonScopedAffiliation
- adminDisplayName: eduPersonScopedAffiliation
- adminDescription: Specifies the person's affiliation (see eduPersonAffiliation) within a particular security domain, the values consist of a left (affiliation) and right component (security domain) separated by an "@" sign
- attributeID: 1.3.6.1.4.1.5923.1.1.1.9
- attributeSyntax: 2.5.5.12
- oMSyntax: 64
- isSingleValued: FALSE
- searchFlags: 1
- showInAdvancedViewOnly: TRUE
- systemOnly: FALSE

-
- dn: CN=eduPersonTargetedID,CN=Schema,CN=Configuration,$[BASE_DN]
- changetype: ntdsschemaadd
- objectClass: top
- objectClass: attributeSchema
- cn: eduPersonTargetedID
- lDAPDisplayName: eduPersonTargetedID
- adminDisplayName: eduPersonTargetedID
- adminDescription: Specifies the person's relationship(s) to the institution, permissible values: faculty, student, staff, alum, member, affiliate, employee
- attributeID: 1.3.6.1.4.1.5923.1.1.1.10
- attributeSyntax: 2.5.5.12
- oMSyntax: 64
- isSingleValued: FALSE
- searchFlags: 0
- showInAdvancedViewOnly: TRUE
- systemOnly: FALSE
-
- dn: CN=eduPersonAssurance,CN=Schema,CN=Configuration,$[BASE_DN]
- changetype: ntdsschemaadd
- objectClass: top
- objectClass: attributeSchema

- cn: eduPersonAssurance
- lDAPDisplayName: eduPersonAssurance
- adminDisplayName: eduPersonAssurance
- adminDescription: Set of URIs that assert compliance with specific standards for identity assurance.
- attributeID: 1.3.6.1.4.1.5923.1.1.1.11
- attributeSyntax: 2.5.5.12
- oMSyntax: 64
- isSingleValued: FALSE
- searchFlags: 0
- showInAdvancedViewOnly: TRUE
- systemOnly: FALSE
-
- dn:
- changetype: modify
- add: schemaUpdateNow
- schemaUpdateNow: 1
- -
-
-
- # ==========

- # Object classes
- # ==========
- dn: CN=eduPerson,CN=Schema,CN=Configuration,$[BASE_DN]
- changetype: ntdsschemaadd
- objectClass: classSchema
- cn: eduPerson
- lDAPDisplayName: eduPerson
- adminDisplayName: eduPerson
- adminDescription: Consists of a set of data elements or attributes about individuals within higher education
- governsID: 1.3.6.1.4.1.5923.1.1.2
- objectClassCategory: 3
- subclassOf: top
- rdnAttId: cn
- mayContain: 1.3.6.1.4.1.5923.1.1.1.1
- mayContain: 1.3.6.1.4.1.5923.1.1.1.2
- mayContain: 1.3.6.1.4.1.5923.1.1.1.3
- mayContain: 1.3.6.1.4.1.5923.1.1.1.4
- mayContain: 1.3.6.1.4.1.5923.1.1.1.5
- mayContain: 1.3.6.1.4.1.5923.1.1.1.6

- mayContain: 1.3.6.1.4.1.5923.1.1.1.7
- mayContain: 1.3.6.1.4.1.5923.1.1.1.8
- mayContain: 1.3.6.1.4.1.5923.1.1.1.9
- mayContain: 1.3.6.1.4.1.5923.1.1.1.10
- mayContain: 1.3.6.1.4.1.5923.1.1.1.11
- defaultObjectCategory: CN=eduPerson,cn=Schema,cn=Configuration,$[BASE_DN]
- systemOnly: FALSE
-
- dn:
- changetype: modify
- add: schemaUpdateNow
- schemaUpdateNow: 1
- -
-
- dn: CN=User,CN=Schema,CN=Configuration,$[BASE_DN]
- changetype: modify
- add: auxiliaryClass
- auxiliaryClass: eduPerson
- -
-
- dn:

- changetype: modify
- add: schemaUpdateNow
- schemaUpdateNow: 1
- -

Στα παραπάνω πρέπει να αντικατασταθεί το $[BASE_DN]με το distinguished name του active directory domain. Σημειώνεται ότι το παραπάνω σχήμα είναι ελαφρώς αλαγμένο σε σχέση με τους default ορισμούς του eduPerson schema στο ότι όλα attributes τύπου Distinguished Name είναι ορισμένα ως απλά text attributes. Ο λόγος είναι ότι το Active Directory απαιτεί όλα τα attributes τύπου Distinguished Name να έχουν τιμές κάτω από το distinguished name του active directory domain. Καθώς αυτό μπορεί να μη συνάδει με τις τιμές που είναι επιθυμητό να δημοσιεύονται στο shibboleth επιλέχθηκε να είναι απλά text πεδία ώστε να παίρνουν όλες τις δυνατές τιμές.

Η ενεργοποίηση της επιπλέον καρτέλας σχετικά με το EduPerson schema στην κονσόλα Active Directory Users and Computers γίνεται με την εγκατάσταση του σχετικού λογισμικού που έχει αναπτύξει και διανέμει το ΕΔΕΤ. Λεπτομερείς οδηγίες για την εγκατάσταση μπορούν να βρεθούν στη σχετική σελίδα https://code.grnet.gr/projects/edupersonproperties .

5. ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ

Ο shibboleth IDP δεν αποθηκεύει εσωτερικά κάποια ευαίσθητη πληροφορία για τους χρήστες καθώς διαβάζει τα δεδομένα από τον κατάλογο χρηστών. Παρόλα αυτά είναι ένα σύστημα στο οποίο εισάγουν οι χρήστες τα credentials τους και χρησιμοποιείται για authentication και authorization σε διάφορες υπηρεσίες, συνεπώς είναι ιδιαίτερα ευαίσθητο από την άποψη ασφάλειας.

Για το λόγο αυτό συστήνεται να δίνεται μεγάλη προσοχή στις ενημερώσεις όλων των εμπλεκόμενων υποσυστημάτων. Το λειτουργικό σύστημα στο οποίο είναι εγκατεστημένος ο shibboleth IDP πρέπει να λαμβάνει όλες τις ενημερώσεις ασφαλείας. επίσης, πρέπει να παρακολουθούνται οι ενημερώσεις της Java, του Tomcat αλλά και του ίδιου του IDP και να εφαρμόζονται όλες οι ενημερώσεις ασφαλείας.

Επιπλέον συστήνεται ο tomcat να τρέχει υπό έναν χρήστη που δεν έχει διαχειριστικά δικαιώματα στο λειτουργικό σύστημα αλλά ούτε δικαιώματα να αλλάζει το configuration του IDP. Οι φάκελοι οι οποίοι απαιτείται να είναι εγγράψιμοι από τον χρήστη αυτόν είναι :

- Στην εγκατάσταση του tomcat οι φάκελοι
  - work
  - temp
  - logs
- Στην εγκατάσταση του shibboleth IDP οι φάκελοι
  - logs
  - metadata

Οι ρυθμίσεις στα filesystem permissions μπορούν να γίνουν με τις εντολές:

windows:

```
set IDP_HOME="$[IDP_HOME]"
set JAVA_HOME="$[JAVA_HOME]"
set TOMCAT_HOME="$[CATALINA_BASE]"
set CERTIFICATE="C:\opt\certificate"

set TOMCAT_USER=$[TOMCAT_USER]

icacls %IDP_HOME%    /grant Administrators:(OI)(CI)F
icacls %JAVA_HOME%   /grant Administrators:(OI)(CI)F
icacls %TOMCAT_HOME% /grant Administrators:(OI)(CI)F
icacls %CERTIFICATE% /grant Administrators:(OI)(CI)F

icacls %IDP_HOME%    /grant %TOMCAT_USER%:(OI)(CI)RX
icacls %JAVA_HOME%   /grant %TOMCAT_USER%:(OI)(CI)RX
icacls %TOMCAT_HOME% /grant %TOMCAT_USER%:(OI)(CI)RX
icacls %CERTIFICATE% /grant %TOMCAT_USER%:(OI)(CI)RX

icacls %IDP_HOME%    /inheritance:r
icacls %JAVA_HOME%   /inheritance:r
icacls %TOMCAT_HOME% /inheritance:r
```

```
icacls %CERTIFICATE% /inheritance:r


icacls %IDP_HOME%\logs      /grant %TOMCAT_USER%:(OI)(CI)F
icacls %IDP_HOME%\metadata /grant %TOMCAT_USER%:(OI)(CI)F
icacls %TOMCAT_HOME%\work  /grant %TOMCAT_USER%:(OI)(CI)F
icacls %TOMCAT_HOME%\temp  /grant %TOMCAT_USER%:(OI)(CI)F
icacls %TOMCAT_HOME%\logs  /grant %TOMCAT_USER%:(OI)(CI)F
```

Linux:

```
IDP_HOME="$[IDP_HOME]"
JAVA_HOME="$[JAVA_HOME]"
TOMCAT_HOME="$[CATALINA_BASE]"
CERTIFICATE="/opt/certificate"
TOMCAT_USER=$[TOMCAT_USER]


chown -R root:$TOMCAT_USER $IDP_HOME
chown -R root:$TOMCAT_USER $JAVA_HOME
chown -R root:$TOMCAT_USER $TOMCAT_HOME
chown -R root:$TOMCAT_USER $CERTIFICATE


chmod -R g-w,o-rwx $IDP_HOME
```

```
chmod -R g-w,o-rwx $JAVA_HOME
chmod -R g-w,o-rwx $TOMCAT_HOME
chmod -R g-w,o-rwx $CERTIFICATE

chmod -R g+w $IDP_HOME/logs
chmod -R g+w $IDP_HOME/metadata
chmod -R g+w $TOMCAT_HOME/work
chmod -R g+w $TOMCAT_HOME/temp
chmod -R g+w $TOMCAT_HOME/logs
```

Η ρύθμιση του service του tomcat ώστε να τρέχει υπό τον **$[TOMCAT_USER]** γίνεται από τη σχετική κονσόλα services των windows.

Επιπλέον συνιστάται η ημερήσια ανανέωση των κλειδιών που χρησιμοποιεί ο IDP για εσωτερική κρυπτογράφηση και τα οποία περιέχονται στο αρχείο sealer.jks. Η ανανέωση αυτή μπορεί να γίνει με την παρακάτω εντολή

windows:

```
SET IDP_HOME=C:\opt\shibboleth-idp
SET JAVA_HOME=C:\opt\java

cd %IDP_HOME%\credentials
%IDP_HOME%\bin\seckeygen.bat --storefile sealer.jks --storepass
'$[SEALER_PASS]' --versionfile sealer.kver --alias secret
```

Linux:

```
#!/bin/bash

export IDP_HOME=/opt/shibboleth-idp
export JAVA_HOME=/usr/lib/jvm/java-8-oracle

cd $IDP_HOME/credentials

$IDP_HOME/bin/seckeygen.sh --storefile sealer.jks --storepass
'$[SEALER_PASS]' --versionfile sealer.kver --alias secret
```

Στα παραπάνω το **$[SEALER_PASS]** πρέπει να αντικατασταθεί με την τιμή που υπάρχει στη ρύθμιση idp.sealer.storePassword στο αρχείο idp.properties.