Η ΥΠΟΔΟΜΗ IDM ΑΠΟ ΤΗΝ ΟΠΤΙΚΗ ΤΟΥ ΔΙΑΧΕΙΡΙΣΤΗ ΙΔΡΥΜΑΤΟΣ

Βασίλης Τσουκαλάς,

Πανεπιστημιούπολη Καβάλας, ΔΙΠΑΕ

Τμήμα Πληροφορικής

Ο **Διαχειριστής Ιδρύματος** της υποδομής **ID**entity **M**anagement θα πρέπει να γνωρίζει τουλάχιστον τις εξής συνιστώσες που αφορούν την υποδομή IDM, ώστε να μπορεί να τη διαχειρίζεται αποτελεσματικά:

1. Την Αρχιτεκτονική της Υποδομής IDM.
2. Τις υπηρεσίες του ιδρύματος που θα κάνουν authentication από την IDM υποδομή.
3. Ποιες από τις υπηρεσίες κάνουν authentication μέσω CAS (sso.teiemt.gr) και ποιες από τις (υπόλοιπες) υπηρεσίες κάνουν authentication μέσω ιδρυματικού LDAP (ds.teiemt.gr) ή DS.
4. Ποιες από τις υπηρεσίες παραμετροποιεί και ποιες δεν παραμετροποιεί ο διαχειριστής για τη διασύνδεση με την IDM υποδομή.
5. Πως παραμετροποιεί ο διαχειριστής τις υπηρεσίες που παραμετροποιεί ο ίδιος.
6. Πως αντιμετωπίζει ο διαχειριστής ένα αίτημα νέας υπηρεσίας -όπου διαχειριστής δε θα είναι ο ίδιος, αλλά κάποιος άλλος (π.χ. υπάλληλος με σύμβαση έργου) - που πρέπει να κάνει authentication από την IDM υποδομή.
7. Υπάρχει πολιτική αλλαγής κωδικού των χρηστών που βρίσκονται στον IDM και τι επιπτώσεις μπορεί να έχει αυτό;
8. Διαχείριση λογαριασμών e-mail και συγχρονισμός με την υποδομή IDM.

Η περιγραφή που ακολουθεί χρησιμοποιεί ως παράδειγμα την Πανεπιστημιούπολη Καβάλας με domain

teiemt.gr

1. Η Αρχιτεκτονική IDM

Η αρχιτεκτονική IDM μπορεί να αποτελείται από αρκετά επιμέρους συστήματα-εξυπηρετητές, αλλά ενδεχομένως δεν ενδιαφέρουν όλα αυτά το διαχειριστή του ιδρύματος. Οι εξυπηρετητές που κυρίως τον ενδιαφέρουν είναι οι εξής:

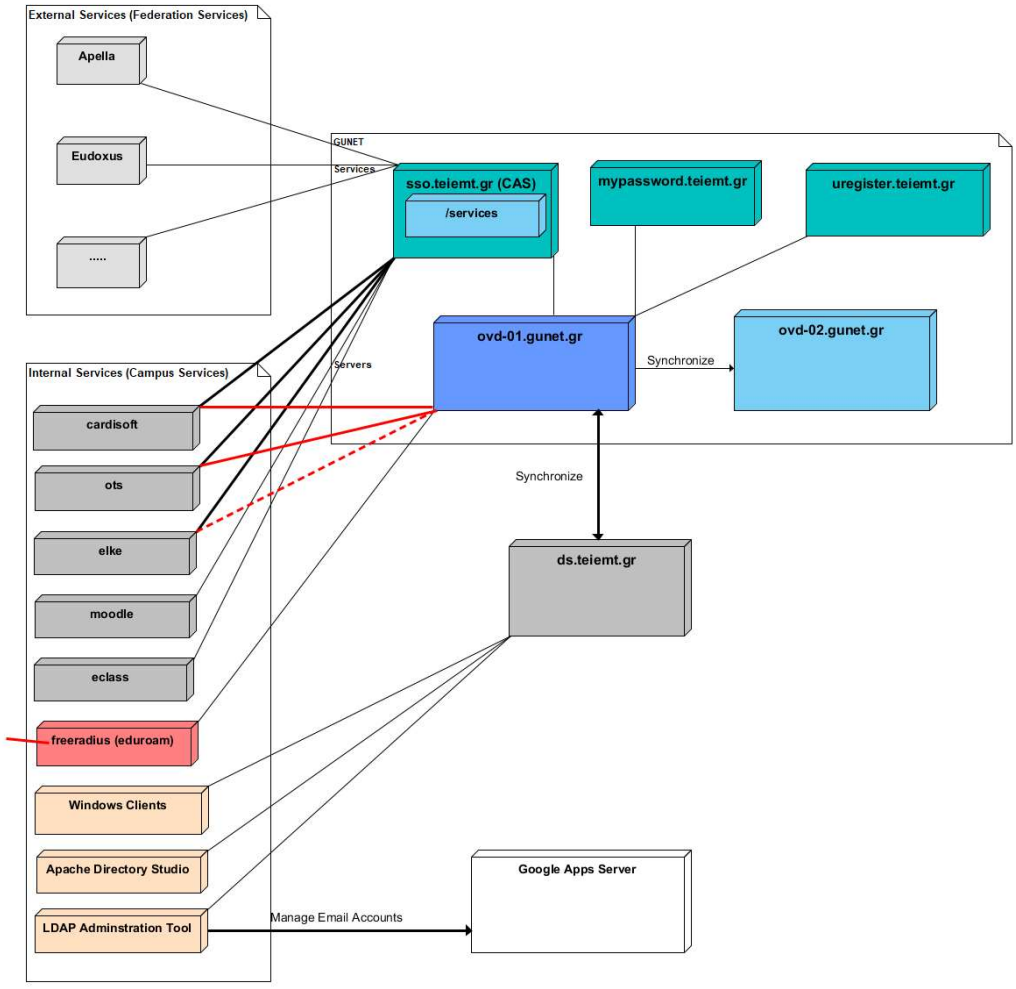
i. Ο **ovd-01.gunet.gr** (**OVD-01**) είναι ο κεντρικός LDAP του GUNET ο οποίος συγχρονίζει για λόγους backup στον ovd-02.gunet.gr. Σε αυτόν τον εξυπηρετητή βρίσκεται πληροφορία που σχετίζεται με το authentication. Όλες οι υπηρεσίες άμεσα ή έμμεσα γίνονται authenticate από τον OVD-01.

ii. Το **uregister.teiemt.gr** είναι η υπηρεσία που κάνει εγγραφή ένα νέο χρήστη (*ή οριστικοποιεί την εγγραφή ενός **νέου** χρήστη*) στην υποδομή IDM δηλαδή προσθέτει ένα ldap user account στον ovd-01.gunet.gr (*και ένα **πλήρες** ldap user account στον*

ds.teiemt.gr). *Οι χρήστες του ιδρύματος χρησιμοποιούν εκτενώς αυτή την υπηρεσία εφόσον πρέπει να εγγραφούν.*

iii. Το **mypassword.teiemt.gr** είναι η υπηρεσία που αλλάζει τον κωδικό ενός υπάρχοντος χρήστη που βρίσκεται στον ovd-01.gunet.gr. *Οι χρήστες του ιδρύματος χρησιμοποιούν εκτενώς αυτή την υπηρεσία εφόσον αλλάζουν το password*.

iv. Το **sso.teiemt.gr** (CAS Server) (που διασυνδέεται με το ovd-01.gunet.gr) είναι η υπηρεσία που εξασφαλίζει το authentication όλων των ομοσπονδιακών υπηρεσιών (εξωτερικές υπηρεσίες-Federation Services) (με εξαίρεση το eduroam), αλλά και των περισσότερων εσωτερικών υπηρεσιών (Campus Services) εντός του ιδρύματος. Όταν ένας χρήστης Moodle, E-class, Eudoxus ή Apella κ.ο.κ δίνει στοιχεία σύνδεσης τότε τα στοιχεία του φτάνουν στον sso.teiemt.gr και αυτός κάνει ένα request στον ovd-01.gunet.gr (εφόσον εκεί υπάρχει ο κωδικός του) για να αυθεντικοποιηθεί. *Αν εκτός από την αυθεντικοποίηση η υπηρεσία Moodle, E-class, Eudoxus ή Apella κ.ο.κ πρεπει να επιστρέψει στοιχεία όπως επώνυμο, ονομα κλπ τότε ο ovd-01.gunet.gr αιτείται τις πληροφορίες από τον DS και τις επιστρέφει στην υπηρεσία.*



v. Ο **ds.teiemt.gr** είναι ο ιδρυματικός (εσωτερικός ή τοπικός) LDAP ή αλλιώς **DS**. Αυτός έχει αμφίδρομο συγχρονισμό με τον *ovd-01.gunet.gr*. Δηλαδή στοιχεία που γράφονται στον ovd-01.gunet.gr μεταφέρονται στον ds.teiemt.gr αλλά και αντίστροφα στοιχεία που γράφονται στον ds.teiemt.gr (και που σχετίζονται με τα στοιχεία αυθεντικοποίησης) μεταφέρονται στον ovd-01.gunet.gr. *Σε ειδικές περιπτώσεις μπορεί να χρειαστεί να συγχρονιστεί πληροφορία –πλέον των στοιχείων αυθεντικοποίησης- που βρίσκεται στον DS προς τον OVD. Αυτό απαιτεί επιπλέον παραμετροποίηση και πρέπει να γίνει σε συνεννόηση με το GUNET. Σε τέτοιες περιπτώσεις ενδέχεται ο διαχειριστής ιδρύματος να πρέπει να τροφοδοτήσει την πληροφορία στον τοπικό του DS.*

Ο DS έχει (τουλάχιστο) τέσσερις σημαντικούς ρόλους:

α. Διασυνδέει εσωτερικές υπηρεσίες που δεν μπορούν –για οποιοδήποτε λόγο- να συνδεθούν στον CAS (sso.teiemt.gr). Ένα τέτοιο παράδειγμα είναι όταν πρέπει να κάνει authentication ένας Windows Client κάποιον χρήστη του ιδρύματος. Σε αυτή την περίπτωση το authentication το κάνει ο ds.teiemt.gr (και όχι ο ovd-01.gunet.gr ή ο CAS).

β. Μπορούν να δημιουργηθούν σε αυτόν ιδρυματικοί χρήστες που δεν βρίσκονται στην υποδομή IDM. Π.χ. Βοηθητικό προσωπικό χωρίς σχέση εργασίας με το ίδρυμα ή π.χ. λογαριασμοί υπηρεσιών (όταν μια cloud υπηρεσία πρέπει να αυθεντικοποιηθεί). Ένα ζωντανό παράδειγμα είναι ο δοκιμαστικός χρήστης της υπηρεσίας eduroam.

γ. Παράκαμψη της υποδομής IDM για προβληματική συμπεριφορά της υποδομής IDM που μπορεί να οφείλεται στο GUNET ή στο ίδρυμα ή σε προβλήματα δικτύου εκτός ιδρύματος.

δ. Ο DS περιέχει αναλυτικές πληροφορίες που αφορούν κάθε χρήστη ιδρύματος (πληροφορίες που δεν υπάρχουν στον OVD) όπως επώνυμο, όνομα, τηλέφωνο, ημερομηνία γέννησης, ιδρυματικό email κ.α. . Περιλαμβάνει επίσης ειδικά attributes με πληροφορίες απαραίτητες για τις ομοσπονδιακές και εσωτερικές υπηρεσίες.

** Ο DS επιπλέον περιλαμβάνει το login name του χρήστη που βρίσκεται –και είναι προφανώς ίδιο- στον OVD, αλλά στη συνήθη περίπτωση δεν περιλαμβάνει το πεδίο userPassword. Στη συνήθη περίπτωση όταν μια υπηρεσία κάνει αίτηση αυθεντικοποίησης απευθείας στον ds.teiemt.gr –επειδή αυτός δεν έχει τον κωδικό- ο ds.teiemt.gr είναι παραμετροποιημένος να κάνει forward το αίτημα αυθεντικοποίησης στον OVD.*

*** Στην Πανεπιστημιούπολη Καβάλας υπάρχει μια μη συνήθης περίπτωση όπου -με βάση την πολιτική που ακολουθεί στη χρήση της υπηρεσίας e-mail- ο DS για κάθε user object περιλαμβάνεται το επιπλέον το χαρακτηριστικό userPassword. Αυτή η διαφοροποίηση επιτρέπει στον διαχειριστή ιδρύματος –αν το κρίνει σκόπιμο- να αυθεντικοποιεί υπηρεσίες απευθείας στον ds.teiemt.gr*

2. Υπηρεσίες του ιδρύματος που θα κάνουν authentication από την IDM υποδομή.

Υπηρεσίες του ιδρύματος είναι αυτές που βρίσκονται στην άμεση ευθύνη του διαχειριστή ιδρύματος και τις διαχωρίζουμε από τις **Ομοσπονδιακές υπηρεσίες** (External ή Federation Services) *που δεν αποτελούν ευθύνη του διαχειριστή ιδρύματος* (ανεξάρτητα από το γεγονός πως κάνουν authentication στην IDM υποδομή).

Να σημειώσουμε πως η απαλλαγή του διαχειριστή ιδρύματος από τη διαχείριση των ομοσπονδιακών υπηρεσιών είναι ένα από τα πολλά πλεονεκτήματα που προσφέρει η υποδομή του GUNET. Όταν προστίθενται αλλαγές στις ομοσπονδιακές υπηρεσίες απαιτούνται ενημερώσεις σε όλους τους ldaps (ds, ovd κλπ) της υποδομής IDM, όμως δεν ασχολείται ο διαχειριστής ιδρύματος.

Οι –εσωτερικές- υπηρεσίες της Πανεπιστημιούπολης Καβάλας που πέφτουν στην υποδομή IDM είναι οι εξής:

Φοιτητολόγιο (Cardisoft), Προσωπικό (OTS),

Ενδιάμεση βάση ELKE, Moodle,

E-Class, FreeRadius Server (Eduroam),

Windows Clients (όπου αυτό είναι επιθυμητό),

Open Source Λογισμικό (Apache Directory Studio) πρόσβασης στον ds.teiemt.gr,

Custom λογισμικό πρόσβασης/διαχείρισης (LDAP Administration Tool) ds.teiemt.gr,

Διαδικτυακή Εφαρμογή Διαχείρισης Ομάδων Μαθημάτων (Εργαστηριακών και Θεωρητικών).

3. Ποιες από τις υπηρεσίες κάνουν authentication μέσω CAS (sso.teiemt.gr) και ποιες από τις (υπόλοιπες) υπηρεσίες κάνουν authentication μέσω ιδρυματικού LDAP (ds.teiemt.gr)

Ο Διαχειριστής του ιδρύματος πρέπει να έχει ξεκαθαρίσει και να έχει πάντα σε εγρήγορση στο μυαλό του ποιες από τις ιδρυματικές υπηρεσίες συνδέονται με τον CAS (sso.teiemt.gr), και ποιες συνδέονται με τον τοπικό LDAP (ds.teiemt.gr). *Θα πρέπει επίσης να θυμάται μήπως υπάρχουν κατ' εξαίρεση κάποιες ιδρυματικές υπηρεσίες που δεν συνδέονται ούτε με τον CAS ούτε με τον DS.*

Στο ίδρυμα Καβάλας η κατανομή έχει ως εξής:

Υπηρεσίες που αυθεντικοποιούν χρήστες μέσω CAS:

Φοιτητολόγιο (Cardisoft), Προσωπικό (OTS),

Ενδιάμεση βάση ELKE,

Moodle,

E-Class

Υπηρεσίες που αυθεντικοποιούν χρήστες μέσω DS:

Windows Clients,

Open Source Λογισμικό πρόσβασης στον ds.teiemt.gr (Apache Directory Studio),

Custom λογισμικό πρόσβασης/διαχείρισης (LDAP Administration Tool) ds.teiemt.gr και

Διαδικτυακή Εφαρμογή Διαχείρισης Ομάδων Μαθημάτων.

Κατ' εξαίρεση Υπηρεσίες που δεν αυθεντικοποιούν χρήστες μέσω CAS ή μέσω DS:

FreeRadius Server (Eduroam): Η αυθεντικοποίηση των χρηστών γίνεται με απευθείας πρόσβαση στον κεντρικό LDAP του GUNET ovd-01.gunet.gr.

Να σημειώσουμε πως ο δοκιμαστικός χρήστης του eduroam δημιουργήθηκε στον ds.teiemt.gr, αλλά ο τοπικός radius server κάνει authenticate το δοκιμαστικό χρήστη (όπως και όλους τους χρήστες) στον ovd-01.gunet.gr. Αυτό είναι δυνατό γιατί ο δοκιμαστικός χρήστης που δημιουργήθηκε στον DS συγχρονίστηκε στον OVD-01.

4. Ποιες από τις υπηρεσίες παραμετροποιεί και ποιες δεν παραμετροποιεί ο διαχειριστής ιδρύματος για τη διασύνδεση με την IDM υποδομή.

Ο διαχειριστής ιδρύματος δεν παραμετροποιεί τις ομοσπονδιακές υπηρεσίες. Δεν παραμετροποιεί επίσης κανέναν από τους LDAPs που επηρεάζουν τις ομοσπονδιακές υπηρεσίες.

Ο διαχειριστής ιδρύματος παραμετροποιεί μόνο ιδρυματικές υπηρεσίες (Campus Servers/Services). Από τις ιδρυματικές υπηρεσίες δεν παραμετροποιεί επίσης το φοιτητολόγιο και το πρόγραμμα μισθοδοσίας (και ενδεχομένως ούτε το rescom). *Την παραμετροποίηση σε αυτές τις υπηρεσίες την αναλαμβάνουν οι ανάδοχες εταιρείες σε συνεργασία με το GUNET.*

Σημείωση

Όταν το φοιτητολόγιο ή το πρόγραμμα μισθοδοσίας πρόκειται να δημιουργήσουν ένα username στην υποδομή IDM πρέπει να εξασφαλίσουν ότι αυτό είναι μοναδικό. Αυτό επιτυγχάνεται κάνοντας ένα αίτημα στον OVD-01. Αυτό απεικονίζεται με τις κόκκινες γραμμές στον διάγραμμα της αρχιτεκτονικής. Η διακεκομμένη κόκκινη γραμμή αντιστοιχεί στην επίσημη υπηρεσία του RESCOM που ακόμα δεν υπάρχει. Οι μαύρες έντονες γραμμές αντιστοιχούν στα αιτήματα του GUNET προς τα DB Views.

5. Πως παραμετροποιεί ο διαχειριστής τις υπηρεσίες που παραμετροποιεί ο ίδιος (Περιληπτική Προσέγγιση-όχι Τεχνική).

Υπάρχει διαφορετική προσέγγιση στην παραμετροποίηση των υπηρεσιών που κάνουν authentication μέσω CAS και των υπηρεσιών που κάνουν authentication στον DS.

Παραμετροποίηση Υπηρεσιών για CAS

Α. Για να μπορέσει μια οποιαδήποτε υπηρεσία Χ να συνδεθεί με τον CAS (sso.teiemt.gr) θα πρέπει αρχικά να δοθεί πρόσβαση στην υπηρεσία Χ από την διαδικτυακή ιστοσελίδα https://sso.teiemt.gr/services .

Β. Εφόσον γίνει το Α η υπηρεσία Χ (κυρίως διαδικτυακή εφαρμογή) θα πρέπει να ενσωματώνει κατάλληλο plugin ή custom module (αν πρόκειται για custom εφαρμογή) ώστε να επικοινωνεί χωρίς προβλήματα με τον CAS Server (sso.teiemt.gr) .

Γ. Πολλές φορές η υπηρεσία Χ –μετά τη σύνδεση ενός χρήστη- χρειάζεται πληροφορίες (μεταξύ τεχνικών χρησιμοποιείται η έννοια «κατέβασμα attributes») που βρίσκονται στον ds.teiemt.gr. Για παράδειγμα μετά το login του χρήστη η υπηρεσία Χ χρειάζεται να αντλήσει το ονοματεπώνυμο, το τηλέφωνο και την ημερομηνία γέννησης του χρήστη. Αυτή η πληροφορία μπορεί να αντληθεί αν:

1. Παραμετροποιηθεί επιπλέον η εφαρμογή https://sso.teiemt.gr/services ώστε ο διαχειριστής ιδρύματος να επιλέξει από το γραφικό περιβάλλον διεπαφής της εφαρμογής ποια attributes θα είναι διαθέσιμα στην υπηρεσία Χ.

2. Η υπηρεσία Χ στο plugin της ή στο custom module της ξέρει πώς να διαβάσει τα attributes που «κατεβαίνουν» από τον ovd-01.gunet.gr της IDM υποδομής.

Δ. Σε ασυνήθιστες περιπτώσεις μια υπηρεσία Χ –μετά τη σύνδεση ενός χρήστη- χρειάζεται «attributes» που δεν εμφανίζονται στην εφαρμογή του GUNET https://sso.teiemt.gr/services. Αυτό δε σημαίνει πως τα attributes αυτά δεν βρίσκονται στον ds.teiemt.gr. Σημαίνει απλώς πως τα attributes αυτά δεν έχουν προστεθεί στην εφαρμογή https://sso.teiemt.gr/services. Ο διαχειριστής ιδρύματος μπορεί να αιτηθεί στο GUNET να προστεθούν τα επιπλέον attributes* .

**Ωστόσο πρέπει να αποφεύγουμε τέτοιου είδους αιτήματα –εκτός και είναι πολύ μεγάλη ανάγκη- γιατί πρέπει να έχουμε στο μυαλό μας πως οι LDAPs δεν είναι Database Servers και αντιστοίχως πως τα directories δεν είναι databases.*

Παραμετροποίηση Υπηρεσιών για DS

Μια υπηρεσία Υ για να συνδεθεί με τον ds.teiemt.gr δεν διαφέρει πολύ σε σχέση με την παραμετροποίηση που χρειάζεται για να συνδεθεί με έναν OpenLDAP. Ωστόσο ο DS δομεί τα user objects με έναν συγκεκριμένο τρόπο και ο διαχειριστής χρειάζεται κάποια εξοικείωση με τη δομή τους.

Εν γένει απαιτείται να υπάρχει πρόσβαση σε ένα ldap χρήστη που να έχει πρόσβαση read σε όλα τα user objects του DS και επιπλέον να ενσωματωθεί στην υπηρεσία Υ το κατάλληλο ldap query.

Στον DS υπάρχει ο χρήστης RO που έχει δικαιώματα read σε όλα τα user objects που υπάρχουν στο directory του ds.teiemt.gr.

6. Πως αντιμετωπίζει ο διαχειριστής ένα αίτημα νέας υπηρεσίας - όπου διαχειριστής δε θα είναι ο ίδιος, αλλά κάποιος άλλος (π.χ. υπάλληλος με σύμβαση έργου) - που πρέπει να κάνει authentication από την IDM υποδομή.

Α. Αν προκύψει τέτοιο αίτημα αποκλείουμε σε αυτό το διαχειριστή πρόσβαση στον DS.

Β. Του γνωστοποιούμε πως πρέπει να ακολουθήσει τη διαδικασία που περιγράφεται στο 5. Παραμετροποίηση Υπηρεσιών για CAS.

Εφόσον ανοίξουμε πρόσβαση στην εφαρμογή του από τα https://sso.teiemt.gr/services του εξηγούμε πως είναι υποχρέωσή του να εξοικειωθεί με την ανάπτυξη λογισμικού (ή με την ενσωμάτωση plugin) για την επικοινωνία της εφαρμογής του με τον CAS Server (sso.teiemt.gr).

7. Υπάρχει πολιτική αλλαγής κωδικών των χρηστών που βρίσκονται στον IDM και τι επιπτώσεις μπορεί να έχει αυτό;

Όλοι οι κωδικοί των χρηστών που πέφτουν πάνω στην IDM υποδομή έχουν (παραμετροποιήσιμη) πολιτική λήγουν ένα χρόνο μετά την ενεργοποίηση του λογαριασμού τους από την υπηρεσία uregister.teiemt.gr. Αυτό που έχουν να κάνουν οι χρήστες είναι να χρησιμοποιήσουν την υπηρεσία mypassword.teiemt.gr για να αλλάξουν τον κωδικό τους. Μέχρι να γίνει αυτό δεν πρόκειται να έχουν πρόσβαση σε καμία υπηρεσία της υποδομής IDM.

*Παρατήρηση για τις υπηρεσίες που χρησιμοποιούν τις εξαιρετέες περιπτώσεις που περιγράφονται στις παραγράφους 1.ν και 1.ν δ ***

** Οι υπηρεσίες που συνδέονται στον DS ενδεχομένως να αυθεντικοποιούνται μετά τη λήξη του κωδικού του χρήστη μέχρι να συγχρονιστεί ο DS από τον OVD-01.*

*** Μόλις ο χρήστης αλλάξει τον κωδικό του από την υπηρεσία mypassword.teiemt.gr οι υπηρεσίες που έχουν πρόσβαση στον DS θα κάνουν authenticate τους χρήστες με τον προηγούμενο κωδικό μέχρι να ολοκληρωθεί ο συγχρονισμός του DS από τον OVD-01. Ο συγχρονισμός αυτός είναι πολύωρη διαδικασία και διαρκεί περίπου 4-6 ώρες (πάνω – κάτω).*

8. Διαχείριση λογαριασμών e-mail και συγχρονισμός με την υποδομή IDM.

Από τη στιγμή που οι χρήστες του ιδρύματος πέσουν στην υποδομή IDM και εφόσον θέλουμε να μπαίνουν οι χρήστες με τα ίδια στοιχεία σύνδεσης που υπάρχουν στους ldaps θα πρέπει να υποστηρίζονται από το διαχειριστή ιδρύματος οι παρακάτω λειτουργίες:

Α. Να δημιουργηθούν λογαριασμοί στον email server του ιδρύματος με στοιχεία που υπάρχουν στην υποδομή IDM.

Β. Να συγχρονίζονται οι κωδικοί (εφόσον αλλάζουν) –όπως ενδεχομένως και άλλα στοιχεία- των χρηστών στο email server με τον κωδικό (ή και τα αλλαγμένα στοιχεία) που υπάρχει στους ldaps.

Το ίδρυμα Καβάλας για να αντιμετωπίζει αυτά τα ζητήματα (όπως και πολλά άλλα διαχειριστικά ζητήματα) έχει κατασκευάσει Custom Εφαρμογή Διαχείρισης LDAP (LDAP Administration Tool) που όσον αφορά τα email κάνει τα εξής:

Η εφαρμογή συνδέεται με τον ds.teiemt.gr, βρίσκει τους νέους χρήστες που υπάρχουν στον DS και κάνοντας χρήση ενός API της GOOGLE τους δημιουργεί και με δυνατότητα τοποθέτησης σε Organization Units.

Η εφαρμογή συνδέεται με τον ds.teiemt.gr, βρίσκει τους χρήστες που έχουν υποστεί αλλαγές στον DS και κάνοντας χρήση του API της GOOGLE τους συγχρονίζει με τα νέα τους στοιχεία.

** Να σημειωθεί πως το περιβάλλον Google Apps For Education προσφέρει τις δυνατότητες παραμετροποίησης του Authentication των χρηστών μέσω LDAP ή και μέσω CAS Server. Θα μπορούσε ενδεχομένως να παραμετροποιηθεί η υπηρεσία Google Apps να βλέπει τον ds.teiemt.gr ή τον sso.teiemt.gr . Ωστόσο σε αυτή την περίπτωση θα πρέπει να σχεδιαστούν και να παραμετροποιηθούν προσεκτικά οι πολιτικές πρόσβασης των χρηστών (π.χ. θα έχει πρόσβαση ο χρήστης στο λογαριασμό email του μόλις πάψει να είναι ενεργός χρήστης του ιδρύματος; Και πως θα υποστηριχτεί αυτό από τεχνική σκοπιά; Είναι ευέλικτη μελλοντικά μια αλλαγή πολιτικής;).*