# 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: Σχεδιασμός σχήματος καταλόγου και διασύνδεση με το πληροφοριακό σύστημα παροχής δεδομένων***

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

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. ΕΙΚΟΝΕΣ



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. ΕΙΣΑΓΩΓΗ

## 2.1 ΑΝΤΙΚΕΙΜΕΝΟ ΚΑΙ ΔΟΜΗ ΤΟΥ ΠΑΡΑΔΟΤΕΟΥ

Το παρόν έργο παραδίδεται στο πλαίσιο της πράξης «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» και αφορά την υπηρεσία **Uregister** που εξυπηρετεί την ενημέρωση των ιδρυματικών υπηρεσιών καταλόγου με τους ηλεκτρονικούς λογαριασμούς των καθηγητών, των ερευνητών και του προσωπικού, καθώς και τη διαδικασία μετάβασης στη νέα αυτή υποδομή.

Στο παρόν κείμενο θα αναλυθούν τα αρχιτεκτονικά στοιχεία της υπηρεσίας, καθώς και οι επιλογές υλοποίησης. Γίνεται επίσης ανάλυση των υποστηρικτικών δομών που είναι απαραίτητες για τη λειτουργία του συστήματος και τέλος παρουσιάζεται ένας σύντομος οδηγός χρήσης της υπηρεσίας. Ειδικά για τους σκοπούς επίδειξης και διαμόρφωσης των χαρακτηριστικών οθονών της διαδικτυακής εφαρμογής έχει χρησιμοποιηθεί το εικονικό ίδρυμα «ΤΕΙ Χαλκιδικής».

## 2.2 ΣΥΝΟΠΤΙΚΗ ΠΕΡΙΓΡΑΦΗ ΤΗΣ ΥΠΗΡΕΣΙΑΣ

Η υπηρεσία ενεργοποίησης λογαριασμού χρήστη απαιτεί τη διασύνδεση με μια υποδομή βάσης δεδομένων, η οποία θα παρέχει τα βασικά στοιχεία των χρηστών. Τα στοιχεία αυτά χρησιμοποιούνται ως μέσο επιβεβαίωσης ταυτότητας και μετέπειτα χρησιμοποιούνται για την εγγραφή του χρήστη. Απαραίτητη φυσικά είναι και η διασύνδεση με την υπηρεσία καταλόγου, που αποτελεί τον αποδέκτη των ενεργειών της εφαρμογής.

Η μελέτη και ανάπτυξη της υπηρεσίας πραγματοποιήθηκε στα ακόλουθα στάδια:

- Ορισμός απαραίτητων πηγαίων στοιχείων για την εγγραφή
- Επιλογές υλοποίησης
- Υλοποίηση βασικής υπηρεσίας
- Ενσωμάτωση με περιφερειακά συστήματα και έλεγχος λειτουργίας

### 2.2.1 Ορισμός απαραίτητων στοιχείων για την εγγραφή

Η ενεργοποίηση του λογαριασμού ενός χρήστη απαιτεί την εγγραφή στην υποδομή καταλόγου ενός συνόλου στοιχείων. Επιπροσθέτως μια ομάδα στοιχείων θεωρείται απαραίτητη για λόγους ταυτοποίησης του ατόμου που θα εγγραφεί.

Σε αυτά τα απολύτως απαραίτητα δεδομένα προστίθενται ένα σύνολο με βοηθητικά δεδομένα, που προστίθενται στην υπηρεσία καταλόγου σαν περιγραφικά στοιχεία.

Ο ορισμός των απολύτως απαραιτήτων δεδομένων έγινε αφού ολοκληρώθηκε η δημιουργία του πρότυπου καταλόγου που χρησιμοποιείται στα εκπαιδευτικά ιδρύματα.

Ο πρότυπος κατάλογος αυτός έχει ως απαραίτητα δομικά στοιχεία:

- ένα μοναδικό αναγνωριστικό (AcademicPersonID)
- το username του χρήστη (uid)
- και την τριάδα των κωδικών (digestHA1, sambaNTPassword και UserPassword) που απαιτούνται για τις διαφορετικές κατηγορίες διαπίστευσης.

Αυτά τα δεδομένα εμπλουτίζονται από προσωπικά δεδομένα, που αποθηκεύονται μόνο ύστερα από επιβεβαίωση του χρήστη και δημιουργούν το σύνολο της εικόνας του ατόμου.

Ο πρότυπος κατάλογος αυτός ονομάζεται auth Ldap, και ο ορισμός του αναλύεται στην αντίστοιχη ενότητα.

Μοναδική πηγή αυτών των δεδομένων θεωρείται η βάση δεδομένων που παρέχει κάθε Ίδρυμα / Φορέας.

### 2.2.2 Επιλογή προγραμματιστικού περιβάλλοντος και συστήματος υλοποίησης

Δεδομένης της μη ύπαρξης κάποιας εφαρμογής ανοιχτού λογισμικού που να καλύπτει τις ανάγκες της υπηρεσίας ή ένα σύνολο αυτών, η υλοποίηση της υπηρεσίας γίνεται εκ του μηδενός, με ιδιαίτερη έμφαση στις διεπαφές προς τα εξωτερικά συστήματα, αλλά και την δυνατότητα παραμετροποίησης βάσει των αναγκών των ιδρυμάτων.

Για την ανάπτυξη της υπηρεσίας επιλέχθηκε η χρήση γλώσσας PHP, η οποία παρουσιάζει αρκετά μεγάλη λειτουργικότητα, τόσο στο κομμάτι της επικοινωνίας με τις υφιστάμενες βάσεις δεδομένων, όσο και με τις υπηρεσίες καταλόγου. Το σύνολο της υπηρεσίας θα φιλοξενείται σε μια δομή βασισμένη σε τεχνολογίες ανοιχτού λογισμικού, κάτι που άλλωστε είναι και βασικό προαπαιτούμενο.

### 2.2.3 Υλοποίηση βασικής υπηρεσίας

Η υλοποίηση της υπηρεσίας περιλαμβάνει δύο στάδια εφαρμογής. Το λειτουργικό κομμάτι και το κομμάτι παρουσίασης.

Αυτά τα δύο στάδια αναπτύχτηκαν ως διαφορετικές οντότητες και συγχωνεύτηκαν ώστε να δημιουργηθεί το τελικό αποτέλεσμα. Στο τμήμα της παρουσίασης επιλέχθηκε η χρήση του Foundation framework, με στόχο την δημιουργία μιας κοινής εικόνας της εφαρμογής, σε οποιαδήποτε πλατφόρμα επιλέγει ο χρήστης(pc/κινητά/tablet). Πέρα από τις πολλές διευκολύνσεις που παρουσιάζει το σύστημα αυτό, πολύ σημαντικό ρόλο στην επιλογή της διαδραμάτισε και η πολύ καλή υποστήριξη και τεκμηρίωση από την ομάδα ανάπτυξης.

Το λειτουργικό κομμάτι υλοποιήθηκε με την χρήση μιας σειράς βιβλιοθηκών που διευκολύνουν την διεκπεραίωση των αναγκών της εφαρμογής. Αυτές οι βιβλιοθήκες παρότι αποτελούν σημαντικό κομμάτι της εφαρμογής, υλοποιούν μόνο ένα περιφερειακό τμήμα της. Το βασικά λειτουργικό κομμάτι δημιουργήθηκε εκ του μηδενός σε τεχνολογία php.

### 2.2.4 Ενσωμάτωση με περιφερειακά συστήματα και έλεγχος λειτουργίας.

Σημαντικό κομμάτι της εφαρμογής αποτελεί η ενσωμάτωση με τα περιφερειακά συστήματα. Αυτά τα συστήματα αποτελούνται τόσο από τα κανάλια λήψης και εγγραφής πληροφοριών, που είναι άλλωστε το κύριο αντικείμενο της εφαρμογής, όσο και με βοηθητικές εφαρμογές του όλου οικοδομήματος identity. Σε αυτές τις εφαρμογές περιλαμβάνονται οι διευκολύνσεις αποστολής SMS, η εφαρμογή αλλαγής κωδικού και εφαρμογής πολιτικών.

Στον τομέα της αποστολής και λήψης πληροφοριών, υπήρξε η ανάγκη για επικοινωνία με μια σειρά από διαφορετικές τεχνολογίες βάσεων δεδομένων, και γι αυτό το λόγο επιλέχθηκε η

χρήση της βιβλιοθήκης ADOdb, δίνοντας έτσι ένα επίπεδο αφαιρετικότητας, το οποίο είναι επιθυμητό για την σωστή συντήρηση της εφαρμογής σε βάθος χρόνου. Όσον αφορά τις υποδομές καταλόγου χρησιμοποιήθηκε η εγγενής δυνατότητα επικοινωνίας με LDAP καταλόγους.

Τέλος στον τομέα της επικοινωνίας με εξωτερικά web services, χρησιμοποιούνται απλές κλήσεις JSONRPC.

# 3. ΥΛΟΠΟΙΗΣΗ ΥΠΗΡΕΣΙΑΣ – ΑΝΤΙΚΕΙΜΕΝΟ

Πριν την υλοποίηση της υπηρεσίας, προηγήθηκε ο αυστηρός ορισμός των αποδεκτών της. Αυτό έγινε διότι βάσει αυτού του ορισμού αυτού, κλήθηκαν τα ερευνητικά και ακαδημαϊκά ιδρύματα να ορίσουν και να συμπληρώσουν μια βάση δεδομένων που θα αποτελεί πρωτογενή πηγή πληροφοριών για το σύστημα. Σημειώνεται πως ενώ έχει γίνει ακριβής ορισμός των προδιαγραφών των βάσεων αυτών (HRMS dbview), είναι αναγκαία η διευκρίνιση των πεδίων που δεν επιτρέπεται να έχουν ελλιπή στοιχεία, αφού θα αποτελέσουν τον ακρογωνιαίο λίθο της εκκίνησης της εφαρμογής **Uregister**.

Σε δεύτερο στάδιο ορίστηκε και το σύνολο των επιτρεπτών ενεργειών των χρηστών, κάτι που αποτέλεσε και το βασικό οδηγό προδιαγραφών της ίδιας της εφαρμογής.

## 3.1 ΧΡΗΣΤΕΣ ΤΗΣ ΥΠΗΡΕΣΙΑΣ

Η υπηρεσία απευθύνεται στο σύνολο των ακαδημαϊκών ιδρυμάτων και των ερευνητικών φορέων, που επιθυμούν να αυτοματοποιήσουν τον κύκλο διαχείρισης των ηλεκτρονικών λογαριασμών των μελών τους, τουλάχιστον όσον αφορά στη φάση της εγγραφής, καθώς και να βελτιώσουν την ποιότητα των στοιχείων που καταγράφονται στις υπηρεσίες καταλόγου τους.

Στην παρούσα φάση ο σχεδιασμός της υπηρεσίας ορίζει πως αποδέκτες είναι οι καθηγητές και το προσωπικό ενός ακαδημαϊκού ιδρύματος και οι ερευνητές και το προσωπικό ενός ερευνητικού φορέα. Αυτοί οι αποδέκτες δεν δύνανται να χρησιμοποιήσουν την υπηρεσία αν δεν έχουν κάνει την αρχική τους εγγραφή στο πληροφοριακό σύστημα διαχείρισης προσωπικού του ιδρύματος/φορέα. Άλλωστε η υπηρεσία παρέχει τη διαδικασία ενεργοποίησης ενός λογαριασμού για τον χρήστη και δεν νοείται αρχικοποίηση της οντότητας του αν δεν υπάρχει ήδη στο πρωτογενές σύστημα.

Οι λεπτομέρειες της εγγραφής στο πληροφοριακό σύστημα διαχείρισης προσωπικού είναι εκτός αντικειμένου της εφαρμογής **Uregister**, παρόλα αυτά στο πλαίσιο της εφαρμογής

αυτής θεωρείται απαραίτητη η ύπαρξη των παρακάτω στοιχείων καθώς είναι κρίσιμα για την ταυτοποίηση του ατόμου και ενεργοποίηση του λογαριασμού του.

- ΑΦΜ
- ΑΜΚΑ
- Δευτερεύον κανάλι επικοινωνίας

Όσον αφορά τα στοιχεία ΑΦΜ και ΑΜΚΑ, τηρούνται οι προδιαγραφές που έχουν ορίσει οι εκδούσες αρχές αυτών των στοιχείων. Σχετικά με το δευτερεύον κανάλι επικοινωνίας, έχουν οριστεί δυο διαφορετικά πιθανά πεδία, η εξωτερική email διεύθυνση και το κινητό τηλέφωνο. Είναι υποχρεωτική η ύπαρξη ενός εκ των δυο, αλλά συνίσταται η χρήση του κινητού τηλεφώνου, καθώς θεωρείται πως διασφαλίζει σε μεγαλύτερο βαθμό την επιθυμητή ασφάλεια.

Τα τρία παραπάνω πεδία θα αποτελούν τα στοιχεία διαπίστευσης των χρηστών και γι αυτό το λόγο είναι υποχρεωτικά. Σε κάθε περίπτωση είναι υποχρέωση του ιδρύματος / φορέα να έχει συμπληρωμένα αυτά τα στοιχεία, ειδάλλως δεν θα δύναται να συνεχιστεί η ενεργοποίηση λογαριασμού για τους χρήστες.

## 3.2 ΥΠΗΡΕΣΙΕΣ

Η μοναδική υπηρεσία που παρέχεται είναι η ενεργοποίηση του λογαριασμού για τον χρήστη.

Αυτή η ενεργοποίηση ξεκινά με την είσοδο του χρήστη στην εφαρμογή του ιδρύματος/φορέα και την εισαγωγή των βασικών στοιχείων διαπίστευσης. Μετά την επιτυχή ταυτοποίηση των στοιχείων με αυτά που βρίσκονται αποθηκευμένα στην βάση, το σύστημα αποστέλλει στον χρήστη ένα μοναδικό PIN με το οποίο επιβεβαιώνεται η ταυτότητα του χρήστη και η φυσική του παρουσία στο κανάλι επικοινωνίας που έχει επιλεγεί. Με αυτό τον τρόπο αποτρέπονται πιθανές προσπάθειες αντιποίησης ταυτότητας.

Σημειώνεται πως πριν γίνει η αποστολή του PIN γίνεται μια σειρά ελέγχων για τον χρήστη, ώστε να διαπιστωθεί εάν είναι δυνατή η ενεργοποίηση του λογαριασμού του. Σε αυτούς τους ελέγχους περιλαμβάνονται έλεγχοι για τυχόν ήδη ενεργοποιημένο λογαριασμό, για

δυνατότητα χρήσης συγκεκριμένων στοιχείων ταυτότητας αλλά και πιο βασικούς ελέγχους, όπως τις βασικές διασυνδέσεις του συστήματος.

Εφόσον οι έλεγχοι ολοκληρωθούν με επιτυχία και αποσταλεί ο κωδικός PIN, τότε παρουσιάζεται στο χρήστη η δυνατότητα εισαγωγής του 6ψηφιου αυτού κωδικού. Η επιτυχής επιβεβαίωση οδηγεί στη σελίδα ενεργοποίησης, με την προϋπόθεση ότι ο χρήστης συμφωνεί με τα στοιχεία που αναγνωρίζει το σύστημα γι αυτόν.

Σε αυτήν την περίπτωση ο χρήστης οφείλει να εισάγει ένα επιθυμητό όνομα χρήστη (αν αυτό δεν παρέχεται ήδη από το σύστημα ΒΔ) και κωδικό, τα οποία θα τον χαρακτηρίζουν πλέον στις συνδέσεις με τις ομοσπονδιακές υπηρεσίες και θα είναι σύμφωνα με τις πολιτικές ασφαλείας που ακολουθεί το Ίδρυμα.

Με την εισαγωγή των στοιχείων αυτών ξεκινά μια σειρά νέων ελέγχων, τόσο σχετικά με την ποιότητα των ίδιων των στοιχείων, όσο και τη μοναδικότητα τους στις κατάλληλες υποδομές. Αν δεν παρουσιαστεί κάποιο λάθος σε σχέση με τα στοιχεία, ολοκληρώνεται η ενεργοποίηση του λογαριασμού με την εισαγωγή των στοιχείων στην υπηρεσία καταλόγου.

Η υπηρεσία δεν διαθέτει κάποιο άλλο τμήμα της εφαρμογής για τη δοκιμή από χρήστη της ορθής ολοκλήρωσης της διαδικασίας. Έτσι αν υπάρχει τέτοια ανάγκη, ο μοναδικός τρόπος επαλήθευσης είναι ο έλεγχος μέσω της εισόδου σε μια ομοσπονδιακή υπηρεσία.

Εναλλακτικά προτείνεται και η είσοδος στην εφαρμογή Arcanum, που αποτελεί το σύστημα διαχείρισης κωδικών και πολιτικών για τα ακαδημαϊκά ιδρύματα και τους ερευνητικούς φορείς.

## 3.3 ΡΥΘΜΙΣΕΙΣ ΕΦΑΡΜΟΓΗΣ

Η εγκατάσταση της εφαρμογής προϋποθέτει τον ορισμό ενός συνόλου ρυθμίσεων, απαραίτητων για την ομαλή λειτουργία. Αυτές οι ρυθμίσεις αναλύονται ακολούθως.

| Ρύθμιση app | Τιμή | Επεξήγηση |
|---|---|---|
| **Name** | Uregister | Όνομα εφαρμογής |
| **version** | 0.3 | Τρέχουσα έκδοση |
| **session_name** | ureg | Όνομα συνεδρίας που θα χρησιμοποιηθεί |
| **Path** | / | Σχετικό μονοπάτι εγκατάστασης από το ριζικό του web server |
| **hash_salt** | SECRET | Μυστική φράση για δημιουργία ID |
| **hash_length** | 30 | Μήκος id που δημιουργείται |
| **hash_dictionary** | 0123456789ABCDEF | Αλφαριθμητικά που χρησιμοποιούνται για ID |

| Ρυθμιση raintpl | Τιμή | Επεξήγηση |
|---|---|---|
| **tpl_dir** | templates/ | Κατάλογος προτύπων εμφάνισης |
| **cache_dir** | cache/ | Κατάλογος αποθήκευσης προσωρινών αρχείων |

| Ρύθμιση mongo | Τιμή | Επεξήγηση |
|---|---|---|
| **host** | localhost | Όνομα εξυπηρετητή βάσης |
| **db** | uregister | Όνομα βάσης |

| | | |
|---|---|---|
| **collection** | pins | Όνομα πίνακα |

| **Ρύθμιση sms** | **Τιμή** | **Επεξήγηση** |
|---|---|---|
| **key** | occdd226e86foc13f | Μυστικό κλειδί |
| **url** | https://ws.gunet.gr/?service=sms &key=occdd226e86f | Διεύθυνση υπηρεσίας SMS |
| **message** | %s. Επιβεβαίωση ταυτότητας. Για να συνεχίσετε την εγγραφή εισάγετε το PIN:%s στην φόρμα εγγραφής μέχρι τις: %s' | SMS μήνυμα προς χρήστη |

| **Ρύθμιση mail** | **Τιμή** | **Επεξήγηση** |
|---|---|---|
| **host** | Relay.teixal.gr | Εξυπηρετητής mail |
| **port** | 25 | Πόρτα σύνδεσης |
| **smtpsecure** | | Χρήση ασφαλούς σύνδεσης |
| **auth** | false | Χρήση αυθεντικοποίησης |
| **User** | | Όνομα χρήστη |
| **pass** | | Κωδικός |
| **from** | noreply@teixal.gr | Διεύθυνση αποστολέα |

| | | |
|---|---|---|
| **fromName** | Υπηρεσία Εγγραφής | Όνομα αποστολέα |
| **subject** | PIN επιβεβαίωσης εγγραφής | Θέμα μηνύματος |
| **message** | %s.<br>Επιβεβαίωση ταυτότητας.<br>Για να συνεχίσετε την εγγραφή εισάγετε το PIN:%s στη φόρμα εγγραφής μέχρι τις: %s | SMS μήνυμα προς χρήστη |

| **Ρύθμιση pin** | **Τιμή** | **Επεξήγηση** |
|---|---|---|
| **duration** | 900 | Διάρκεια ζωής PIN |
| **resendtime** | 20 | Χρόνος μη επαναποστολής |

| **Ρύθμιση institution.default** | **Τιμή** | **Επεξήγηση** |
|---|---|---|
| **code** | teixal | Μοναδικός κωδικός ιδρύματος |
| **iid** | 001 | Αριθμητικός κωδικός ιδρύματος |
| **country_code** | GR | Κωδικός χώρας |
| **name** | ΤΕΙ Χαλκιδικής | Όνομα ιδρύματος |
| **pinChannel** | array('mail','sms') | Δευτερεύοντα κανάλια |

| | | |
|---|---|---|
| | | επικοινωνίας |
| **simulateSMS** | false | Μη αποστολή SMS |
| **simulateMail** | false | Μη αποστολή mail |
| **enable_maces** | true | Ενεργοποίηση πεδίων mace |
| **schacPersonalUniqueID_prefix** | urn:mace:terena.org:schac:personalUniqueID:gr:%s:%s | Συμβολοσειρά δημιουργίας mace |
| **schacPersonalUniqueID** | array('SSN','TIN'), | Στοιχεία δημιουργίας mace |
| **schGrAcPersonIDKey_prefix** | urn:mace:teixal.gr:%s:hrms.teixal.gr:1:%s | Συμβολοσειρά δημιουργίας mace |
| **schGrAcPersonIDKey** | array('personid','hrmsid'), | Στοιχεία δημιουργίας mace |
| **digestRealm** | teixal.gr | Πεδίο για δημιουργία κωδικού digest |
| **contact** | **Πληροφορίες επικοινωνίας** | |
| **name** | Γιώργος Καλογήρου | Όνομα υπευθύνου επικοινωνίας |
| **office** | Διεύθυνση Διοικητικού | Γραφείο επικοινωνίας |
| **email** | george@teixals.gr | Email επικοινωνίας |
| **phone** | 2310-12345678 | Τηλέφωνο επικοινωνίας |
| | | |
| **backupcontact** | **Δευτερεύουσες Πληροφορίες επικοινωνίας** | |
| **name** | Νικολοπούλου Γεωργία | Όνομα υπευθύνου επικοινωνίας |
| **office** | Διεύθυνση Διοικητικού | Γραφείο επικοινωνίας |

| | | |
|---|---|---|
| **email** | georgia@teixal.gr | Email επικοινωνίας |
| **phone** | 2310-12345678 | Τηλέφωνο επικοινωνίας |
| | | |
| **db** | **Στοιχεία σύνδεσης βάσης δεδομένων** | |
| **type** | mssql | Τύπος βάσης |
| **host** | vd.teixal.gr | Εξυπηρετητής |
| **port** | 1433 | Πόρτα σύνδεσης |
| **dbname** | STAFF | Όνομα βάσης |
| **dbtable** | v_employees | Όνομα πίνακα |
| **user** | vduser | Όνομα χρήστη |
| **pass** | xxxxxxx | Κωδικός |

| | | |
|---|---|---|
| **ldap** | **Στοιχεία σύνδεσης με υπηρεσία καταλόγου** | |
| **host** | localhost | Εξυπηρετητής |
| **port** | 389 | Πόρτα σύνδεσης |
| **binddn** | cn=admin,dc=teixal,dc=gr | |
| **basedn** | cn=admin,dc=teixal,dc=gr | |
| **pass** | xxxxx | Κωδικός |
| | | |
| **password_strength_policy** | Παράμετροι ισχύος κωδικών | |

| | | |
|---|---|---|
| **PW_CHECK_LEVENSHTEIN** | 2 | Παράμετρος LEVENSHTEIN |
| **PW_CHECK_MIN_LEN** | 6 | Ελάχιστο μήκος |
| **PW_CHECK_MIN_UNIQ** | 5 | Πλήθος μοναδικών χαρακτήρων |
| **PW_CHECK_MIN_LCS** | 40 | Μήκος LCS |
| **PW_CHECK_MIN_NON_ALPHA** | 2 | Πλήθος μη αλφαριθμητικών χαρακτήρων |
| **PW_MIN_CONSECUTIVE_NUMBERS** | 3 | Μέγιστο πλήθος συνεχόμενων αριθμών |
| | | |
| **password_strength_tests** | array('regexpTest', 'consecutivenumbersTest', 'lengthTest', 'similarityTest', 'uniqueTest'), | Έλεγχοι κωδικών |
| | | |

Στις παραπάνω ρυθμίσεις θα πρέπει να προστεθούν και οι ρυθμίσεις του αρχείου καταγραφής.

Σε αυτές ορίζονται ένα η περισσότερα κανάλια καταγραφής και ένας η περισσότεροι handlers που αναλαμβάνουν να καταγράψουν τα διαφορετικά μηνύματα της εφαρμογής.

Σημειώνεται πως ακολουθείται το πρότυπο των επιπέδων καταγραφής FATAL, ERROR, WARN, INFO, DEBUG, TRACE.

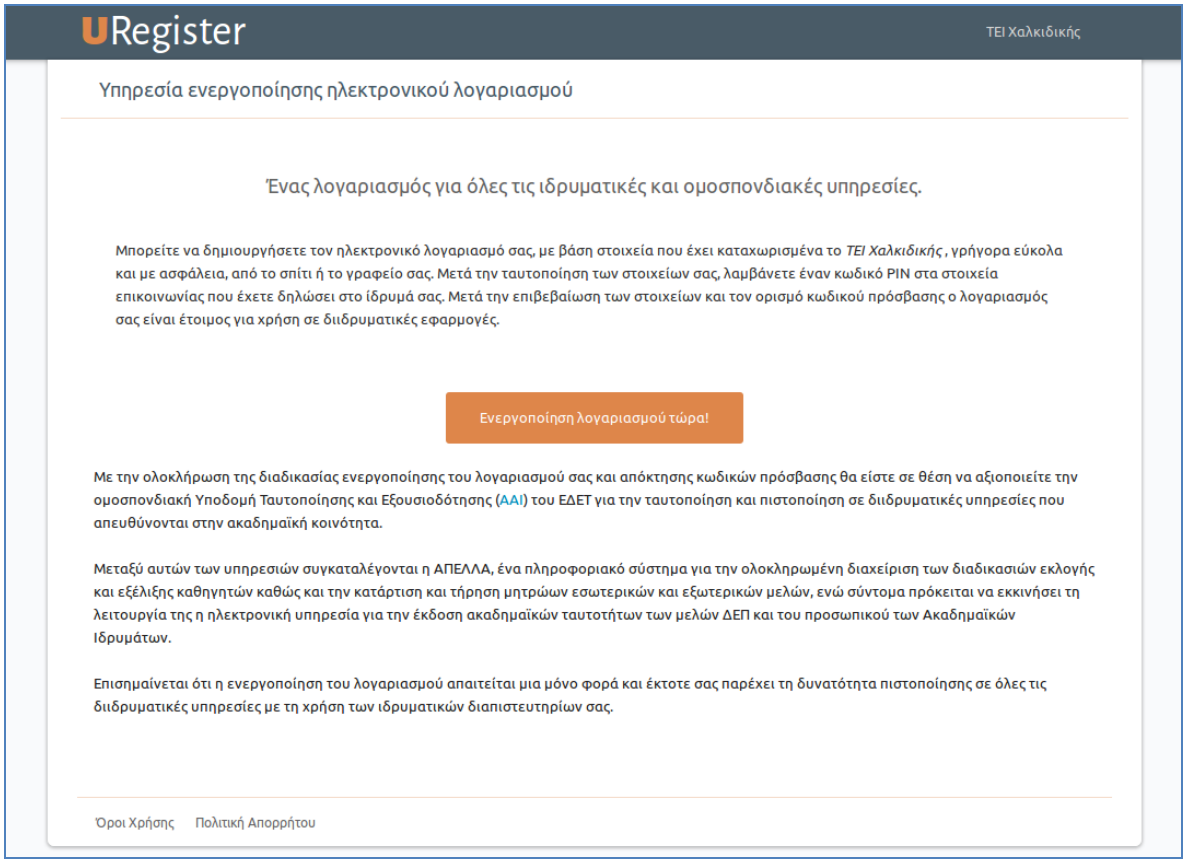
Το σύνολο των ρυθμίσεων αυτών αποθηκεύεται στο αρχείο ./config/config.php, ενώ οι ρυθμίσεις που αφορούν στο σύστημα καταγραφής βρίσκονται στο αρχείο ./config/logconfig.xml

Παράδειγμα αρχείων ρυθμίσεων ακολουθεί στο παράρτημα.

# 4. ΣΕΝΑΡΙΑ ΧΡΗΣΗΣ

Ακολούθως αναλύεται όλη η διαδικασία ενεργοποίησης όπως αυτή παρουσιάζεται στο χρήστη.

Η είσοδος στην εφαρμογή παρουσιάζει στον χρήστη μια σελίδα πληροφοριών, που ενημερώνει για τους στόχους της υπηρεσίας και τα οφέλη που αποκομίζονται από αυτή.



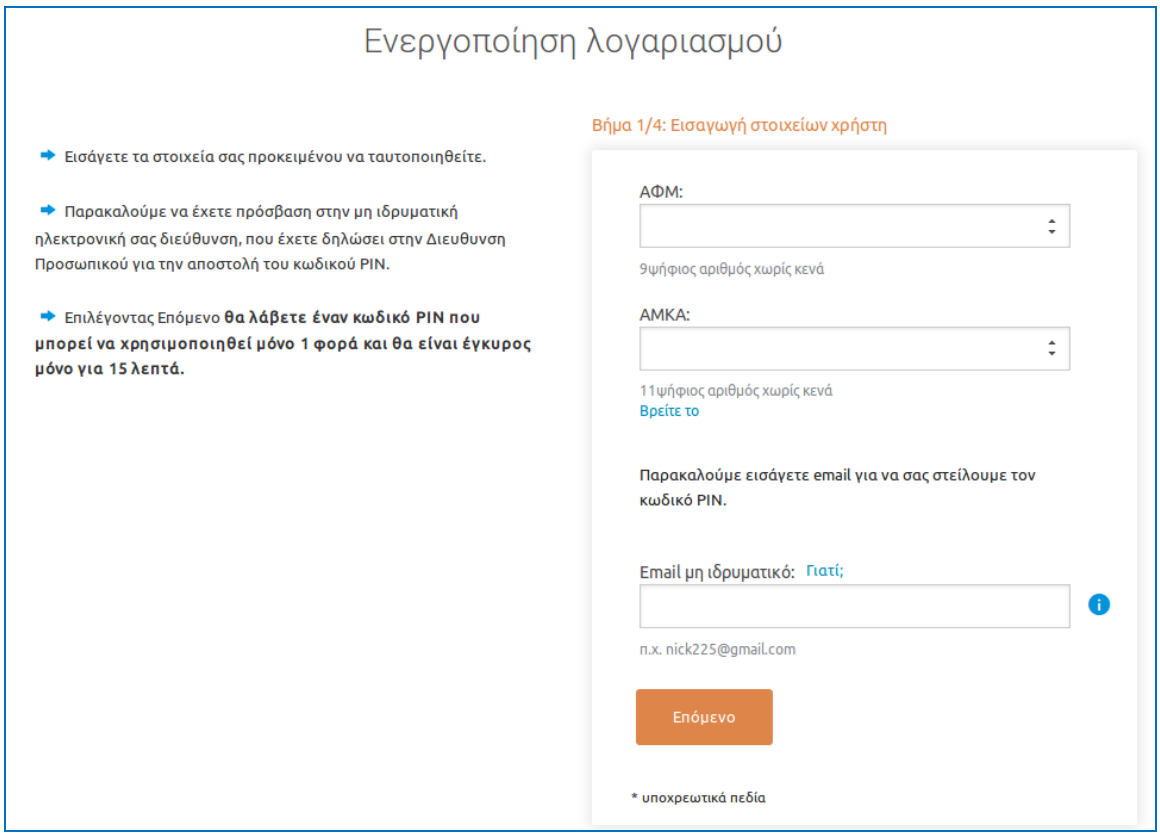

Εικόνα 1 - Εισαγωγική σελίδα

Η μόνη επιλογή που παρουσιάζεται είναι η ενεργοποίηση του λογαριασμού, η επιλογή της οποίας οδηγεί στη βασική σελίδα εισαγωγής στοιχείων για τον χρήστη.

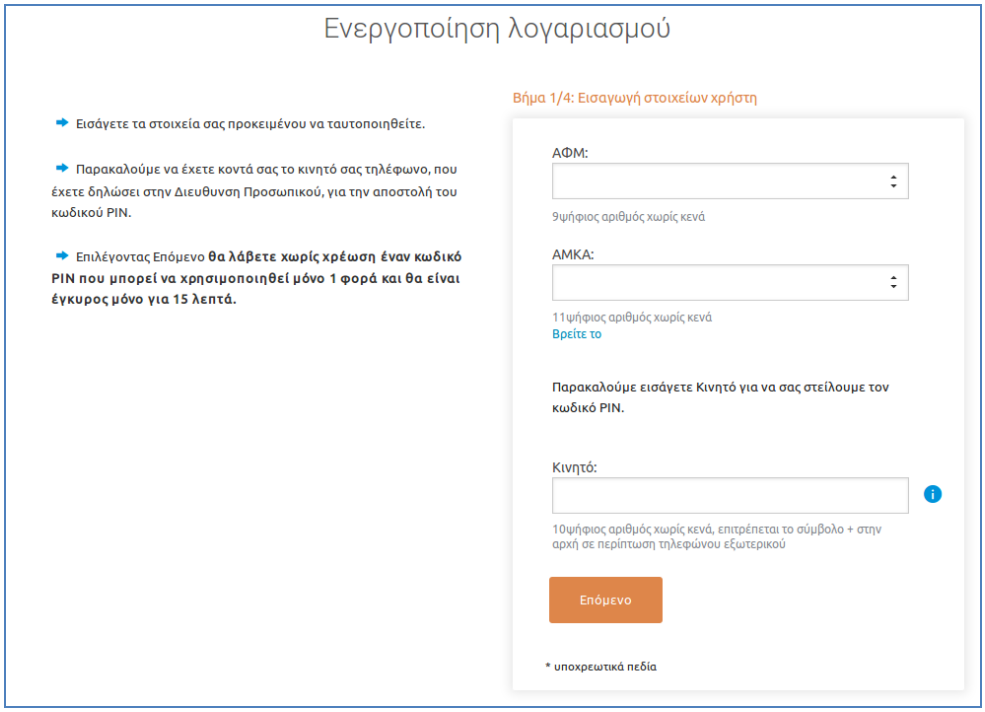
Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
ΕΣΠΑ 2007-2013
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ
Με τη συγχρηματοδότηση της Ελλάδας και της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

Ανάλογα με τις επιλογές του ιδρύματος υπάρχει το ενδεχόμενο ο χρήστης να κληθεί να εισάγει ως δευτερεύον κανάλι επικοινωνίας το κινητό του τηλέφωνο ή το email του.

Οι δύο αυτές περιπτώσεις φαίνονται ακολούθως:

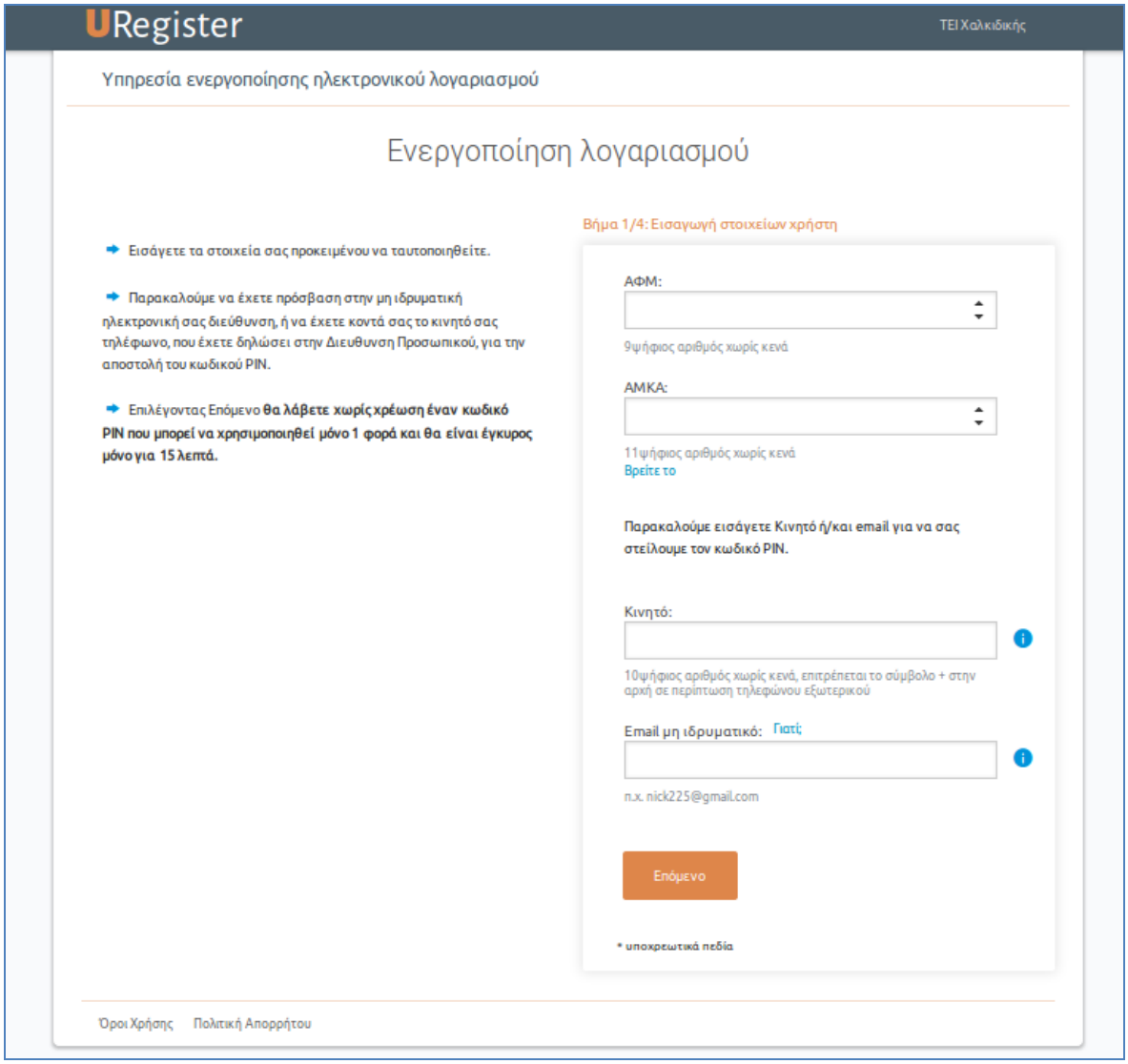



Εικόνα 2 - Χρήση email ως κανάλι επικοινωνίας



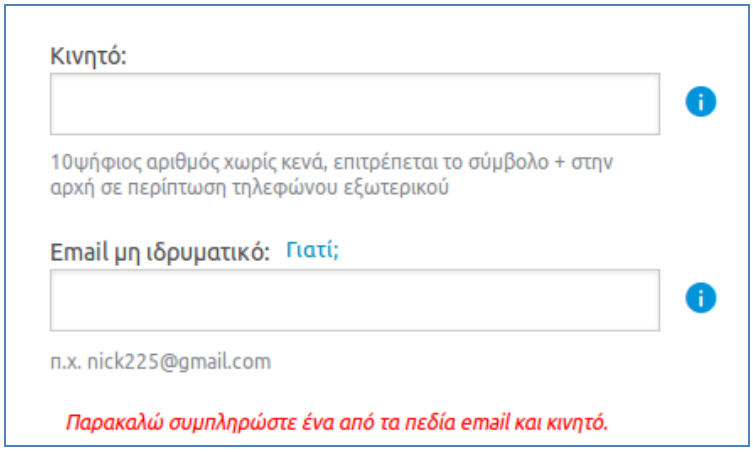

Εικόνα 3 - Χρήση SMS ως κανάλι επικοινωνίας

Η απόφαση για τη χρήση e-mail ή sms πρέπει να ληφθεί κεντρικά από την αρμόδια υπηρεσία του εκπαιδευτικού ιδρύματος. Γενικά συνίσταται η χρήση του κινητού τηλεφώνου σαν δευτερεύον κανάλι επικοινωνίας, όμως σε πολλές περιπτώσεις δεν υπάρχουν αναλυτικά στοιχεία για όλους τους χρήστες. Σε μερικές περιπτώσεις ενδείκνυται η χρήση ενός εκ των δύο πεδίων, ώστε τελικά να χρησιμοποιηθεί αυτό το όποιο θα επιλέξει ο χρήστης.




Εικόνα 4 - Εισαγωγή στοιχείων

Για να γίνει δυνατή η μετάβαση στην επόμενη σελίδα αρκεί ο χρήστης να εισάγει τα ορθά τα στοιχεία: ΑΦΜ, ΑΜΚΑ και ένα εκ των κινητό ή e-mail. Η εφαρμογή απαιτεί τουλάχιστον ένα εκ των δυο πεδίων να είναι συμπληρωμένα προτού επιτραπεί η υποβολή της φόρμας.




Εικόνα 5 - Μήνυμα λάθους - Μη συμπλήρωση καναλιού επικοινωνίας

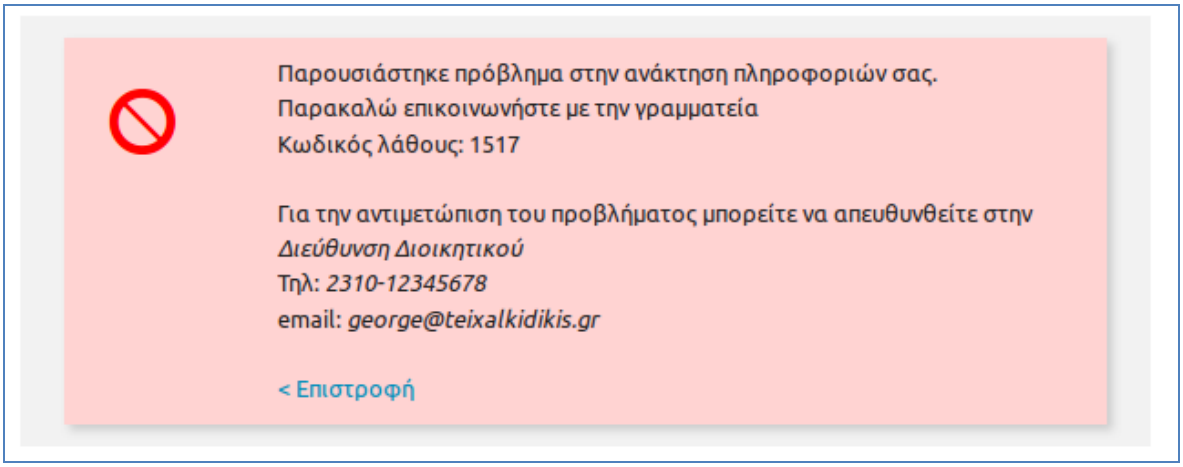
Ενδεχομένως ο χρήστης να επιλέξει την εισαγωγή τόσο του κινητού τηλεφώνου όσο και του e-mail, χωρίς αυτό βέβαια να προσφέρει κάτι περισσότερο στην ασφάλεια της εφαρμογής.

Έχοντας ο χρήστης εισάγει τα στοιχεία περιμένει τη διασταύρωση με τα αντίστοιχα στοιχεία που αποθηκεύονται στη βάση δεδομένων του ιδρύματος/φορέα. Εφόσον αυτά είναι ίδια και ο χρήστης δεν έχει ολοκληρώσει την ενεργοποίηση στο παρελθόν, τότε το σύστημα θα προχωρήσει τη διαδικασία.

Στο ενδεχόμενο που ο χρήστης δε βρεθεί στη βάση δεδομένων, παρουσιάζεται ένα σχετικό μήνυμα λάθους στην οθόνη και ο χρήστης ανακατευθύνεται στην αρχική σελίδα.


Εικόνα 6 - Απουσία χρήστη

Σε περίπτωση που η αναζήτηση δώσει περισσότερα από ένα αποτελέσματα τότε ο χρήστης και πάλι θα δει ένα αντίστοιχο μήνυμα λάθους.

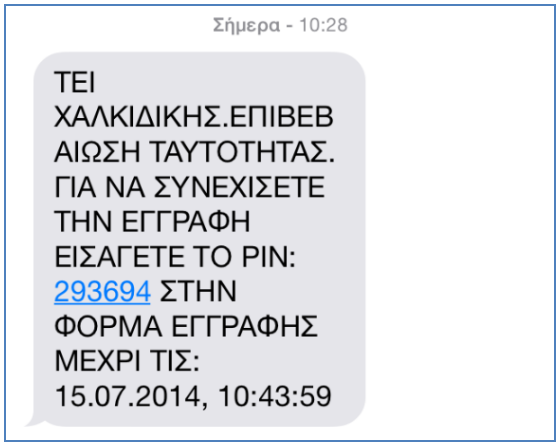



Εικόνα 7 - Πολλαπλοί χρήστες

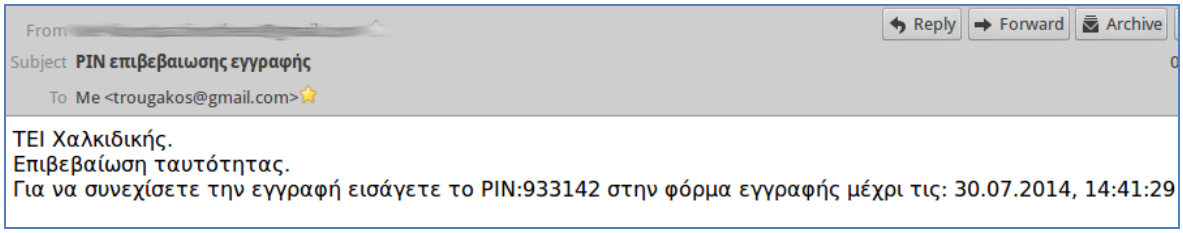
Αυτό το μήνυμα δεν περιλαμβάνει πλήρεις πληροφορίες, για λόγους ασφαλείας, διαθέτει όμως έναν κωδικό λάθους που μπορεί να χρησιμοποιηθεί στην επικοινωνία του ατόμου με τις υποστηρικτικές δομές του ιδρύματος

Όταν η αναζήτηση έχει ως αποτέλεσμα ένα μοναδικό άτομο, τότε το σύστημα αποστείλει το μοναδικό εξαψήφιο αναγνωριστικό, που χρησιμοποιείται για την ταυτοποίηση του χρήστη.

Το μήνυμα που λαμβάνεται περιέχει την βασική πληροφορία του κωδικού PIN, αλλά και την διάρκεια ζωής του.

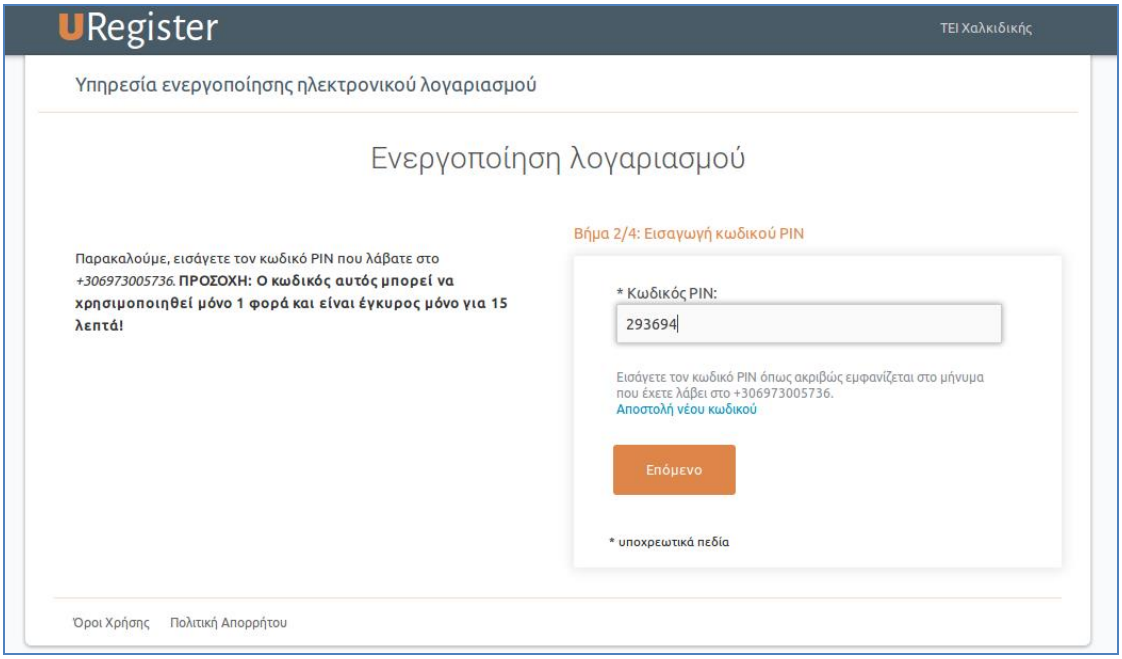



Εικόνα 8–Παράδοση PIN μέσω SMS



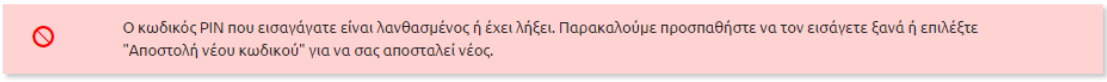

Εικόνα 9 - Παράδοση PIN μέσω email

Ο χρήστης λαμβάνοντας αυτό το μήνυμα οφείλει να εισάγει τον μοναδικό κωδικό στο πεδίο επιβεβαίωσης ώστε να πιστοποιηθεί πως είναι ο ιδιοκτήτης του λογαριασμού και να προχωρήσει πλέον στο επόμενο βήμα που αποτελεί τον πυρήνα της εφαρμογής.



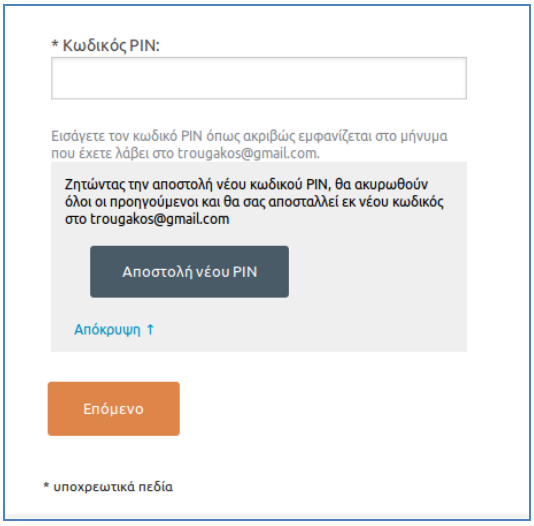

Εικόνα 10 - Εισαγωγή PIN

Η αποτυχημένη εισαγωγή PIN έχει ως αποτέλεσμα ένα μήνυμα λάθους, το οποίο όμως δεν αλλάζει τη σελίδα που βρίσκεται ο χρήστης ώστε να μπορέσει να δοκιμάσει εκ νέου την εισαγωγή του κωδικού.




Εικόνα 11 - Εισαγωγή Λανθασμένου κωδικού PIN

Σημειώνεται πως αν ο χρήστης επιθυμεί, μπορεί να γίνει αποστολή νέου κωδικού PIN. Αυτό θα έχεις αποτέλεσμα να ακυρωθούν όλοι οι πιθανοί προηγούμενοι κωδικοί. Σε κάθε περίπτωση κανείς κωδικός δεν έχει διάρκεια ζωής μεγαλύτερη από 15 λεπτά, κάτι που άλλωστε αναφέρεται και στο μήνυμα που αποστέλλεται.

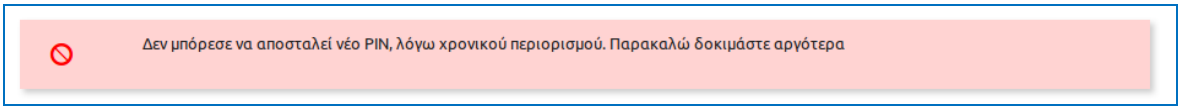



**Εικόνα 12 - Αποστολή νέου PIN**

Η αποστολή νέου PIN διατηρεί τον χρήστη στην ίδια οθόνη, δίνοντας απλά ένα μήνυμα επιβεβαίωσης.

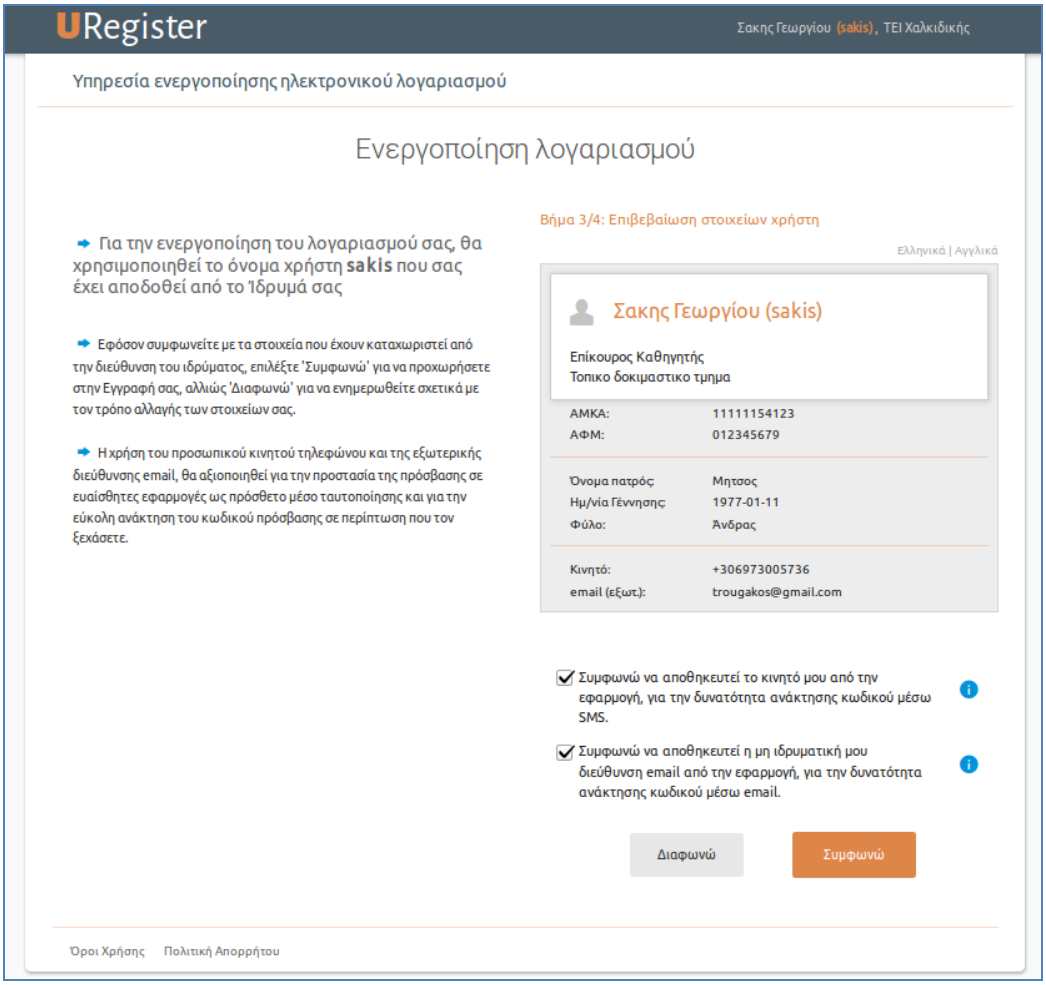

**Εικόνα 13 - Επιτυχημένη αποστολή νέου PIN**

Στο σύστημα έχει ενσωματωθεί έλεγχος συχνότητας αποστολής PIN. Δεν επιτρέπεται νέα αίτηση για PIN, εάν πρώτα δεν έχουν παρέλθει 15 δευτερόλεπτα από την τελευταία φορά που ζητήθηκε η αποστολή του PIN. Στην περίπτωση που γίνει απόπειρα νωρίτερα του αναφερόμενου χρόνου, ο χρήστης ειδοποιείται ώστε να δοκιμάσει αργότερα. Το χρονικό διάστημα αναμονής είναι παραμετροποιήσιμο από το αρχείο ρυθμίσεων.



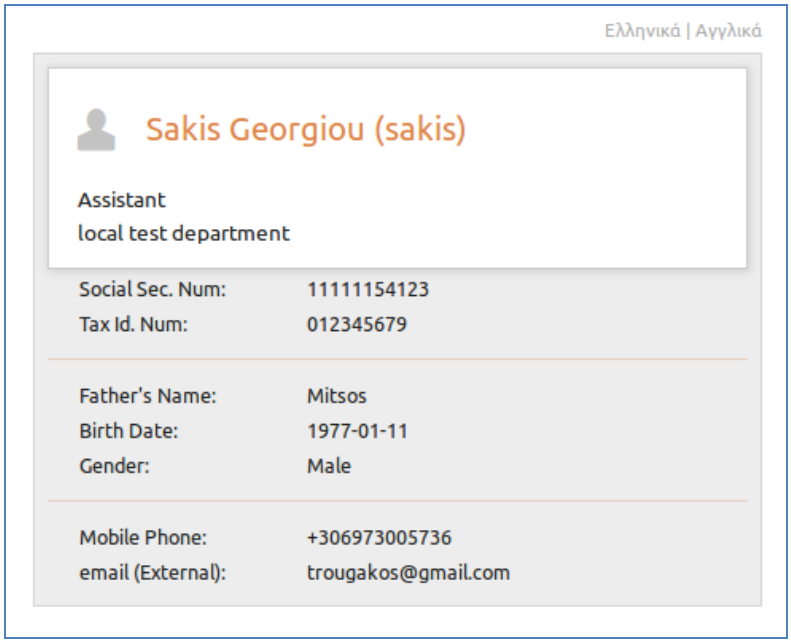

**Εικόνα 14 - Αποτυχία αποστολής PIN**

Επόμενο βήμα στη διαδικασία αποτελεί η επιβεβαίωση των στοιχείων του χρήστη. Τα στοιχεία που παρουσιάζονται έχουν προκύψει από το ίδρυμα/φορέα, συχνά όμως δεν είναι εντελώς ακριβή. Γι αυτό το λόγο δίνεται μια συνοπτική εικόνα στον χρήστη, ώστε να μπορεί να επιβεβαιώσει την ορθότητα, ή να κάνει αίτηση για αλλαγή εφόσον διαπιστώσει ότι υπάρχουν ασυνέπειες.



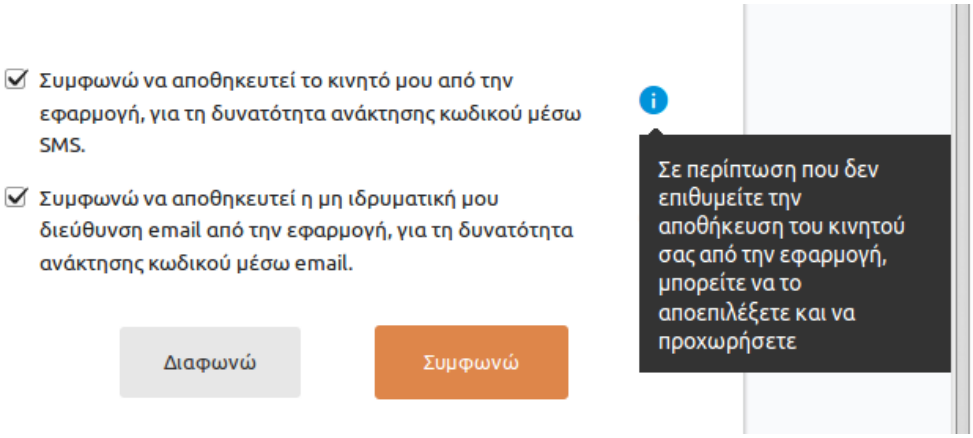

Εικόνα 15 - Επιβεβαίωση στοιχείων

Στον χρήστη δίνεται η δυνατότητα για επισκόπηση των στοιχείων του και σε αγγλική γλώσσα, αν αυτό παρέχεται από το ίδρυμα/φορέα του.

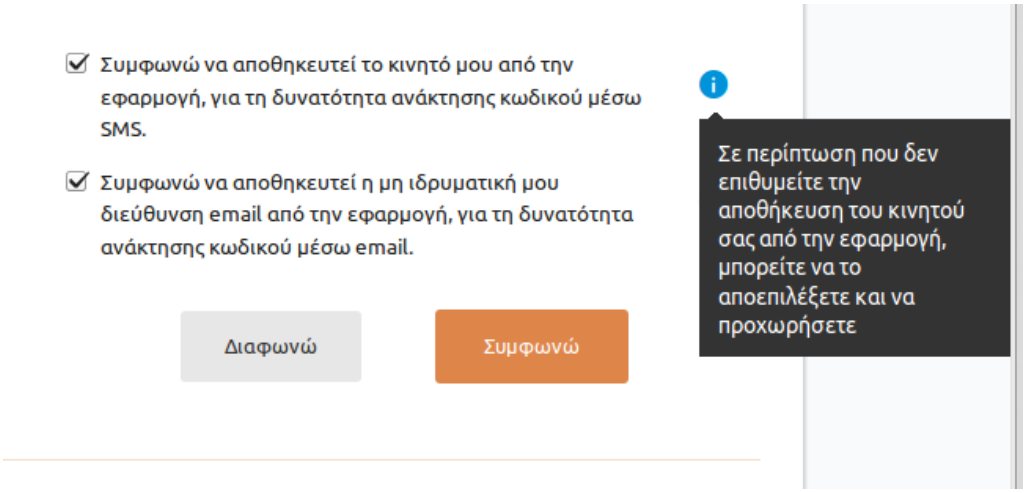



Εικόνα 16 - Στοιχεία χρήστη στην Αγγλική

Στο ίδιο σημείο γίνονται δύο βασικές ερωτήσεις, σχετικά με το αν επιτρέπει ο χρήστης την αποθήκευση των στοιχείων επικοινωνίας του. Τα στοιχεία αυτά αποτελούν προσωπικά δεδομένα και γι αυτό η αποθήκευση τους θα πρέπει να γίνει με τη συγκατάθεση του ατόμου. Ο χρήστης μπορεί να επιλέξει να μην αποθηκευθούν, χωρίς αυτό να έχει κάποια αρνητική συνέπεια στην διαδικασία ενεργοποίησης. Για τη διευκόλυνσή του υπάρχουν περιγραφικά μηνύματα που εξηγούν τη χρήση των στοιχείων αυτών.

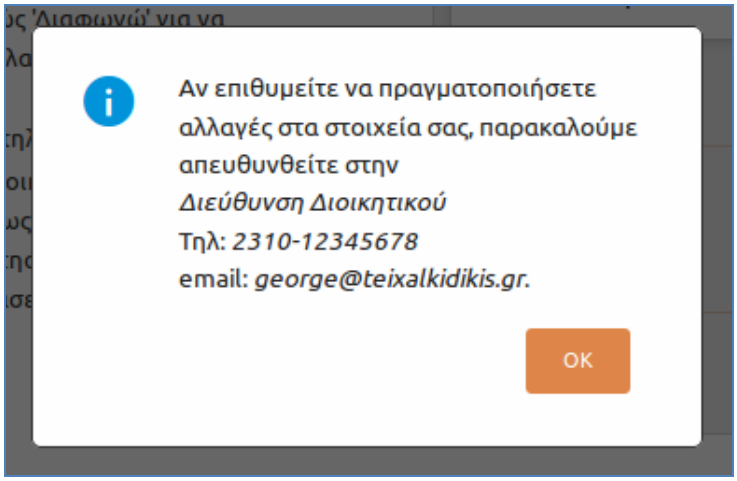


Εικόνα 17 - Ενημέρωση σχετικά με την χρήση email



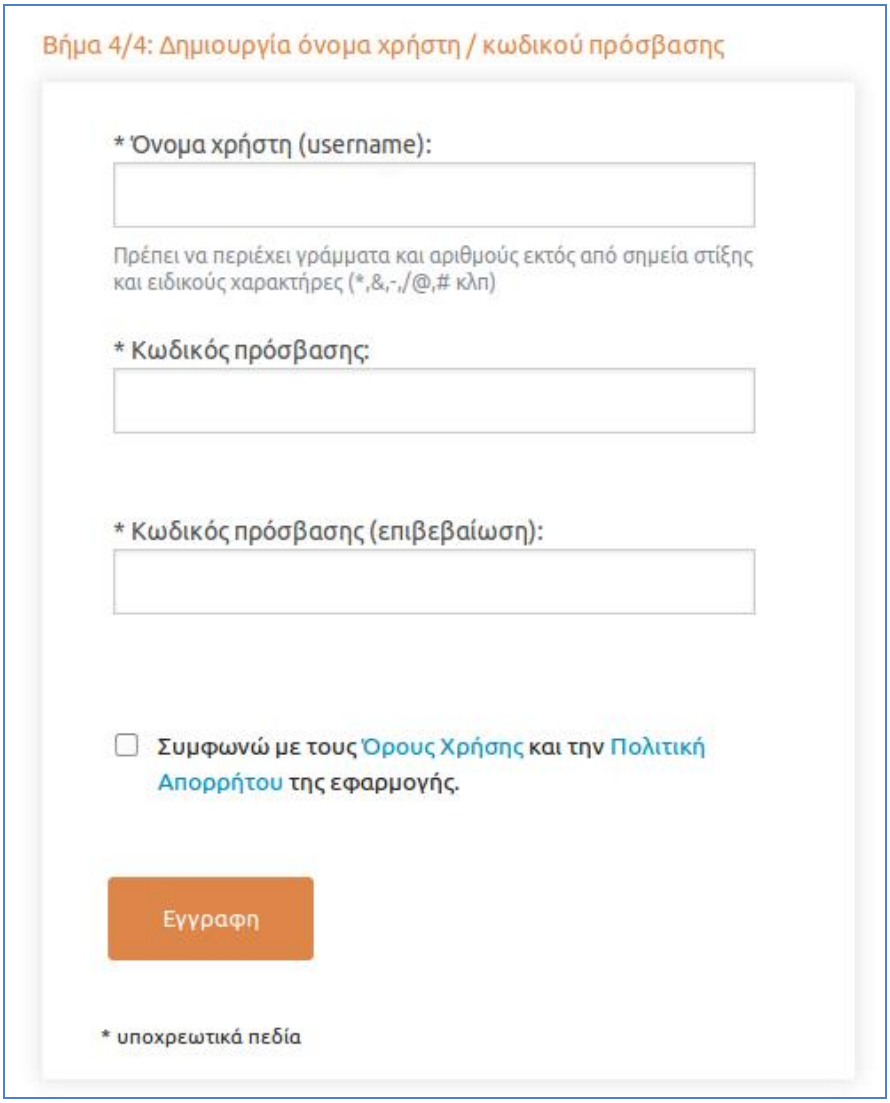

Εικόνα 18 - Ενημέρωση σχετικά με την χρήση κινητού τηλεφώνου

Υπάρχει πάντα το ενδεχόμενο, τα στοιχεία που έχει αποθηκεύσει ένα ίδρυμα/φορέας για κάποιον χρήστη να είναι μη ακριβή. Σε αυτή την περίπτωση ο χρήστης μπορεί να επιλέξει την επιλογή «Διαφωνώ» και θα λάβει τα στοιχεία επικοινωνίας με την αρμόδια υπηρεσία.



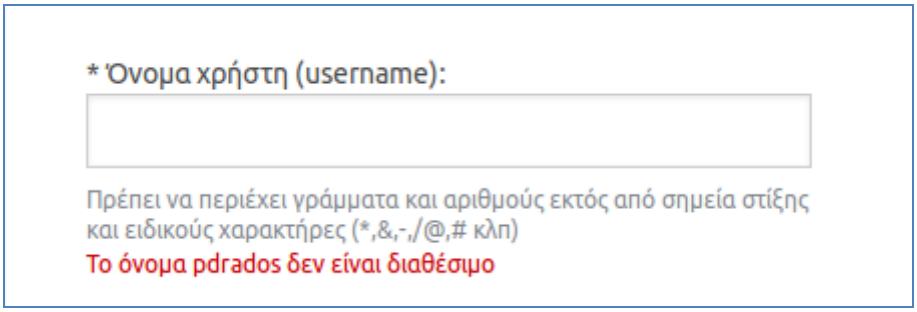

Εικόνα 19 - Μη ακριβή στοιχεία χρήστη

Το τελευταίο βήμα της εφαρμογής είναι πλέον η εισαγωγή του κωδικού για τον λογαριασμό του χρήστη. Σημειώνεται πως σε μια μεγάλη πλειοψηφία ιδρυμάτων υπάρχουν ήδη ονόματα χρηστών (uid) και προτιμάται να χρησιμοποιούνται αυτά. Αν δεν υπάρχει κάτι τέτοιο, τότε απλά δίνεται η δυνατότητα στον χρήστη για την εισαγωγή και ονόματος χρήστη, πέρα από τον κωδικό.



Εικόνα 20 - Φόρμα εισαγωγής για μη ύπαρξη loginname

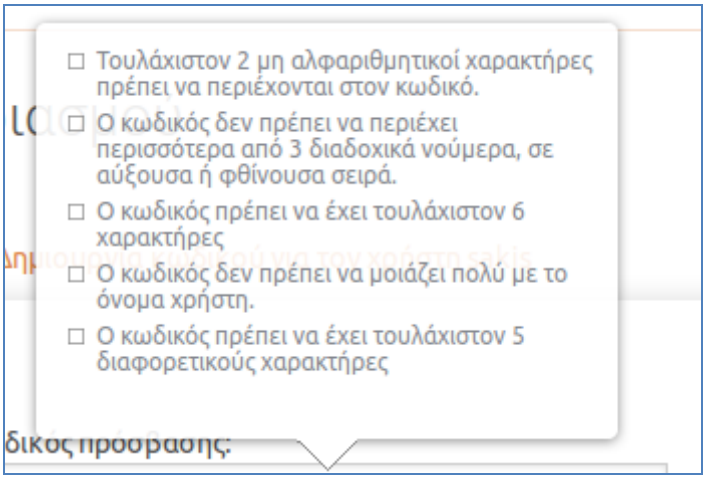
Στην περίπτωση που γίνει επιλογή ενός ονόματος χρήστη που ήδη χρησιμοποιείται το σύστημα αποτρέπει τη συνέχεια της διαδικασίας. Συστήνεται γενικά η συμπλήρωση των ονομάτων χρήσης στη βάση δεδομένων, ώστε να αποφεύγονται τέτοιες περιπτώσεις.




Εικόνα 21 - Μη επιτρεπτό όνομα χρήστη

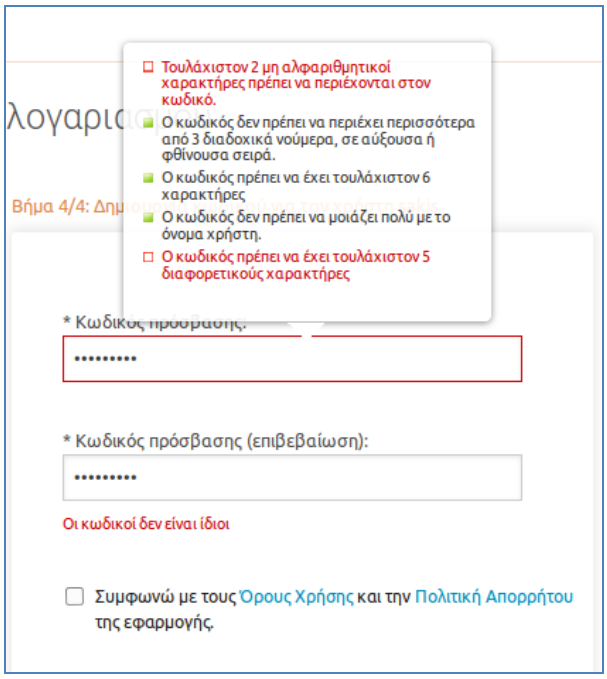
Πολύ σημαντικό βήμα της διαδικασίας αποτελεί η επιλογή κωδικού. Ακρογωνιαίος λίθος της εφαρμογής είναι η χρήση των πολιτικών και της ασφάλειας των κωδικών. Έτσι κάθε φορά που εισάγεται ένας κωδικός πραγματοποιείται μια σειρά ελέγχων, που έχουν οριστεί από τους διαχειριστές. Αν οι έλεγχοι αυτοί δεν έχουν θετικό αποτέλεσμα η διαδικασία δεν προχωρεί.

Με την πρώτη απόπειρα εισαγωγής κωδικού παρουσιάζονται οι γενικές οδηγίες, σχετικά με την ισχύ των κωδικών.



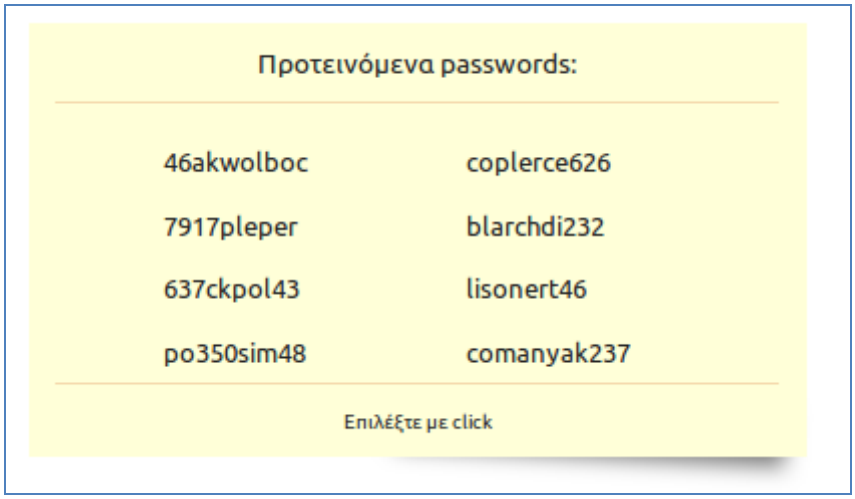

Εικόνα 22 - Οδηγίες ισχύς κωδικών

Αν ο κωδικός δεν είναι επιτρεπτός, ο χρήστης ειδοποιείται για το συγκεκριμένο πρόβλημα που προκύπτει.



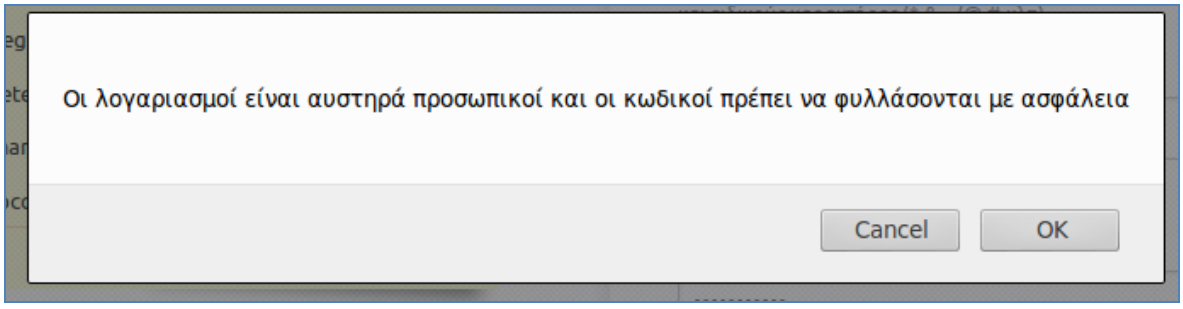

**Εικόνα 23 - Εισαγωγή μη επιτρεπτού κωδικού**

Για τη διευκόλυνση των χρηστών δίνεται μια λίστα κωδικών που παράγονται εκείνη την στιγμή για τον συγκεκριμένο χρήστη και μπορούν να χρησιμοποιηθούν, αφού πληρούν όλες τις προδιαγραφές ασφαλείας.




**Εικόνα 24 - Προτεινόμενοι κωδικοί**

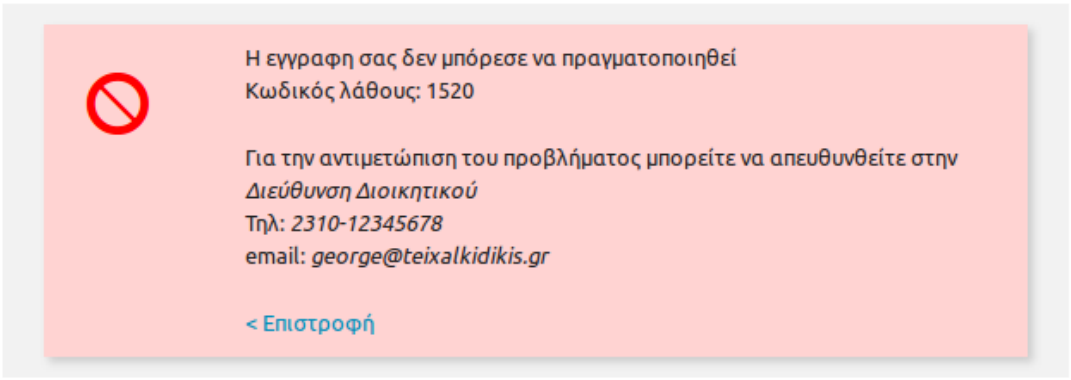
Με την επιλογή ενός αποδεκτού κωδικού, η ενεργοποίηση μπορεί να προχωρήσει. Ο χρήστης θα ενημερωθεί πως πρέπει να διατηρεί με ασφάλεια τον κωδικό του, και μπορεί να ολοκληρώσει την ενεργοποίηση.




**Εικόνα 25 - Μήνυμα ασφαλείας κωδικού**

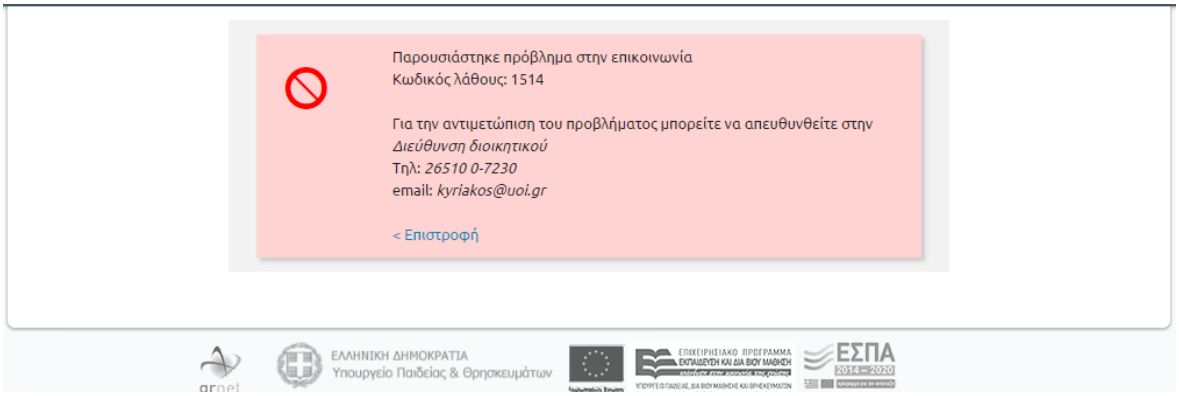
Σε περίπτωση που η εγγραφή δεν μπορεί να πραγματοποιηθεί, το αποτέλεσμα είναι η ανακατεύθυνση στη σελίδα λάθους και σε αυτή την περίπτωση ο χρήστης θα λάβει ένα

κωδικό λάθους ώστε να μπορεί σε επόμενη φάση η αρμόδια υπηρεσία να διαλευκάνει το πρόβλημα.




**Εικόνα 26 - Αποτυχημένη Εγγραφή λόγω μη συνδεσιμότητας**

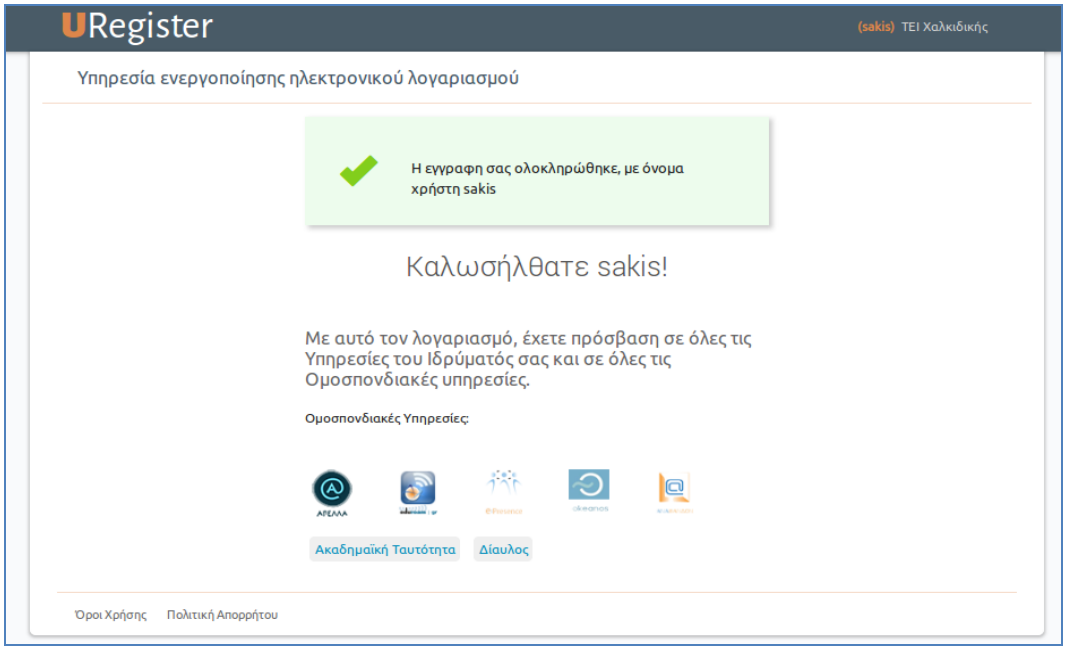
Στην περίπτωση που υπάρχει ήδη εγγεγραμμένος χρήστης και επιχειρηθεί εγγραφή με τα ίδια στοιχεία, η διαδικασία αποτυγχάνει. Ο χρήστης ειδοποιείται σχετικά και θα πρέπει να επικοινωνήσει με την αρμόδια υπηρεσία. Αν υπάρχει λάθος σε οποιοδήποτε στοιχείο, τότε θα γίνει η απαραίτητη διόρθωση από την υπηρεσία.




Εικόνα 27 - Αποτυχημένη εγγραφή – Ο χρήστης υπάρχει

Σημειώνεται ότι οι κωδικοί λάθους που μπορούν να παρουσιαστούν αναφέρονται αναλυτικά στο παράρτημα.

Η επιτυχημένη εγγραφή ολοκληρώνεται με το ακόλουθο μήνυμα, που περιγράφει τις δυνατές εφαρμογές του λογαριασμού που δημιουργήθηκε.




Εικόνα 28 - Επιτυχημένη εγγραφή

# 5. ΤΕΧΝΙΚΑ – ΑΡΧΙΤΕΚΤΟΝΙΚΑ ΣΤΟΙΧΕΙΑ

## 5.1 ΕΠΙΛΟΓΕΣ ΥΛΟΠΟΙΗΣΗΣ

Στο λογικό επίπεδο η εφαρμογή διατηρεί την λογική MVC(ModelViewController).

Με αυτή τη λογική διαχωρίζεται πλήρως το κομμάτι της εμφάνισης, από το λειτουργικό κομμάτι, και από το επίπεδο επικοινωνιών με τη βάση δεδομένων και τις υποδομές καταλόγου.

Για την υλοποίηση αυτού του διαχωρισμού χρησιμοποιήθηκαν μια σειρά βιβλιοθηκών, οι οποίες κρίθηκαν απαραίτητες, τόσο λόγω της σωστής τεκμηρίωσης τους, όσο και της αμεσότητα της παραγωγής αποτελέσματος.

Οι βιβλιοθήκες αυτές είναι οι ακόλουθες

- flightphp: Χρησιμοποιείται για τη δημιουργία της ροής της εφαρμογής. Ουσιαστικά χτίζει τον σκελετό της εφαρμογής, πάνω στον οποίο υλοποιούνται όλες οι υποπεριπτώσεις και βήματα της διαδικασίας ενεργοποίησης

- raintpl: Βιβλιοθήκη για την υλοποίηση των προτύπων των σελίδων παρουσίασης. Με τη χρήση αυτών γίνεται δυνατή η άμεση αλλαγή του τμήματος εμφάνισης της εφαρμογής και ο διαχωρισμός με το λογικό κομμάτι

- Jsonrpc: Βιβλιοθήκη που χρησιμοποιείται στις κλήσεις προς την υπηρεσία σύντομων μηνυμάτων

- log4php : Δημιουργία αρχείων καταγραφής λειτουργίας

- zend-config: Υλοποίηση της χρήσης αρχείου ρυθμίσεων, διαθέσιμου σε κάθε σημείο της εφαρμογής.

- phpmailer: Βιβλιοθήκη αποστολής email.

- adodb: Βιβλιοθήκη για την επικοινωνία με ένα σύνολο βάσεων δεδομένων. Επιλέγεται για λόγους ασφαλείας και διαφάνειας.

Επιπλέον από τις παραπάνω βιβλιοθήκες έχει χρησιμοποιηθεί μια τοπική βάση δεδομένων.

Κατά την μελέτη της εφαρμογής επιλέχθηκε να χρησιμοποιηθεί μια τοπική βάση, όσο το δυνατόν πιο ελαφρού αποτυπώματος. Στόχος της βάσης είναι η αποθήκευση των εξαψήφιων PIN που παράγονται για τους χρήστες, καθώς και των χρονικών ορίων ισχύς τους. Η επιλογή της τοπικής βάσης έχει σαν αποτέλεσμα και τη δυνατότητα για εγκατάσταση της εφαρμογής σε έναν εξυπηρετητή, χωρίς την χρήση διεπαφής με εξωτερικούς εξυπηρετητές. Επιπλέον κρίθηκε πως δεν χρειάζεται η ύπαρξη ενός πολύπλοκου σχήματος, αλλά περισσότερο ένας πίνακας με απλή δομή.

Για τους παραπάνω λόγους επιλέχθηκε η χρήση της Mongodb. Η εγκατάσταση της γίνεται παράλληλα με αυτήν της εφαρμογής και αποτελεί απαραίτητη προϋπόθεση για την λειτουργία της.

Τέλος πρέπει να αναφερθεί και η δημιουργία μιας νέας βιβλιοθήκης, της ACidGenerator. Η βιβλιοθήκη αυτή δημιουργήθηκε με στόχο την παροχή μοναδικών αναγνωριστικών στους χρήστες κατά την ενεργοποίηση των λογαριασμών τους. Αυτά τα χαρακτηριστικά είναι μοναδικά πανελληνίως και η συγκεκριμένη δραστηριότητα αποτέλεσε ένα ξεχωριστό κομμάτι ανάπτυξης εφαρμογής.

Περισσότερες λεπτομέρειες για την βιβλιοθήκη αυτή ακολουθούν στο παράρτημα.

## 5.2 ΑΡΧΙΤΕΚΤΟΝΙΚΗ-ΔΙΑΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑ

Σε φυσικό επίπεδο, ολόκληρη η εφαρμογή τοποθετείται σε μια εικονική μηχανή καθώς δεν απαιτεί μεγαλύτερη ποσότητα πόρων. Στην παρούσα φάση η λειτουργία απαιτεί την συνδεσιμότητα με δύο εξωτερικά συστήματα. Το ένα είναι το σύστημα βάσης δεδομένων , το οποίο αποτελεί το πρωτογενές σύστημα παροχής γνώσης, ενώ το δεύτερο είναι η υπηρεσία

καταλόγου, ο αποδέκτης της υπηρεσίας αυτής. Και τα δυο αυτά συστήματα τοποθετούνται σε εξωτερικά συστήματα.

Στο μέλλον υποστηρίζεται και η χρήση της βιβλιοθήκης ACidGenerator, από ένα κεντρικό σημείο και η αποδέσμευση της από το εσωτερικό της εφαρμογής. Η συνδεσιμότητα προβλέπεται να γίνει με την χρήση κλήσεων JSONRPC, κάτι που άλλωστε ήδη υποστηρίζεται από το σύστημα. Τέλος ιδιαίτερα σημαντική θέση κατέχει και η επικοινωνία με τη διεπαφή αποστολής SMS, που και αυτή γίνεται με χρήση του ίδιου πρωτόκολλου.

## 5.3 ΚΑΤΑΛΟΓΟΣ ΤΑΥΤΟΠΟΙΗΣΗΣ ΚΑΙ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ

Τελικός στόχος των υπηρεσιών καταλόγου στις οποίες αναφερόμαστε είναι η δημιουργία ενός συνολικού object για κάθε ενδιαφερόμενο χρήστη. Αυτό το object δεν βρίσκεται αποκλειστικά σε μια υποδομή, αλλά διανέμεται σε επιμέρους καταλόγους, οι οποίοι έχουν διακριτούς ρόλους. Αυτοί είναι οι εξής:

- **Virtual Directory**. Αφορά ένα κατάλογο τα περιεχόμενα του οποίου ωστόσο προκύπτουν δυναμικά από τα στοιχεία που διατηρούν πρωτογενή πληροφοριακά συστήματα για τον χρήστη και εστιάζουν κυρίως σε στοιχεία όπως το όνομα, η ιδιότητα, η οργανωτική μονάδα στην οποία ανήκει ο χρήστης κ.α. Τέτοια πληροφοριακά συστήματα μπορεί να είναι για παράδειγμα το πληροφοριακό σύστημα προσωπικού του φορέα. Μεταξύ άλλων το Virtual Directory ενοποιεί και τους δύο καταλόγους που αναφέρονται στη συνέχεια, κάτω από ένα κοινό ανά φορέα DIT suffix (π.χ. dc=teixal,dc=gr)
- **Translucent Directory**. Αφορά ένα κατάλογο ο οποίος είναι επικουρικός στη προτεινόμενη αρχιτεκτονική. Εξυπηρετεί την αποθήκευση προσωπικών και δευτερευόντων στοιχείων ενός χρήστη, εφόσον αυτά δεν ακυρώνουν τα στοιχεία που προέρχονται από πρωτογενή και εξουσιοδοτημένα πληροφοριακά συστήματα. Τέτοια στοιχεία μπορεί να προκύπτουν από επέκταση του ldap object με πεδία που χρειάζονται για ειδικές υπηρεσίες / εφαρμογές που λειτουργούν στον φορέα.

- **Authentication Directory**. Αφορά τον κατάλογο που έχει αποκλειστική αποστολή την ταυτοποίηση και αυθεντικοποίηση χρηστών. Αυτός περιλαμβάνει μόνο στοιχεία που είναι απαραίτητα για την ταυτοποίηση του χρήστη, την αυθεντικοποίηση του, και την εφαρμογή του Password Policy.

Η εφαρμογή Uregister δημιουργεί και διαχειρίζεται τα objects που βρίσκονται στον Authentication Directory. Συγκεκριμένα η εγγραφή ενός χρήστη στο URegister καταλήγει στη δημιουργία ενός "κεφαλικού" ldap object που περιλαμβάνει κατάλληλους δείκτες, ώστε το Virtual Directory να μπορεί στη συνέχεια να συνθέσει κάτω από αυτό όλες τις επιμέρους πληροφορίες για το χρήστη που προχέονται από άλλα περιφερικά πληροφοριακά συστήματα.

### 5.3.1 Δομή καταλόγου

Αναλυτικές πληροφορίες σχετικά με τις ρυθμίσεις παρατίθενται στο παράρτημα. Πέρα από τις ρυθμίσεις, έχουν οριστεί σαν απαραίτητα σχήματα που εισάγονται στον κατάλογο τα ακόλουθα ExtendedAuthSchema, SchAcSchema, SchGrAcSchema

Πλήρεις πληροφορίες σχετικά με τα παραπάνω σχήματα παρατίθενται στο παράρτημα.

Το πρότυπο object που δημιουργείται για τον χρήστη έχει ως ακολούθως:

```
dn: schGrAcPersonID=E795A73DF44596288316346CAA65F3,ou=People,dc=teixal,dc=gr
objectClass: simpleSecurityObject
objectClass: extendedAuthentication
objectClass: schacLinkageIdentifiers
objectClass: schGrAcIdentifiers
objectClass: schGrAcLinkageIdentifiers
objectClass: account
```

uid: sampleuser

userPassword:: bmVvc2tvc21vczE4

digestHA1: eda7ab39ca9718221a874d112a0bb292

mailForwardingAddress: sampleusers@teixal.gr

mobile: +306977777774

sambaNTPassword: 622AB59DDC3A0E5AC612AF675E47D20C

schacPersonalUniqueID: urn:mace:terena.org:schac:personalUniqueID:gr:SSN: 26011100000

schacPersonalUniqueID: urn:mace:terena.org:schac:personalUniqueID:gr:TIN: 022020200

schGrAcPersonID: E795A73DF44596288316346CAA65F3

schGrAcPersonIDKey: urn:mace:gunet.gr:personid:hrms.uoi.gr:1:1616

schGrAcPersonIDKey: urn:mace:gunet.gr:hrmsid:hrms.uoi.gr:1:442

schGrAcPersonSSN: 26011100000

schGrAcPersonTIN: 022020200

## Βασικά πεδία object χρήστη.

uid: Ονομα χρήστη

userPassword:: Βασικός κωδικός αυθεντικοποίησης

digestHA1: Κωδικός αυθεντικοποίησης digest

mailForwardingAddress: Δευτερεύουσα διεύθυνση email

mobile: Κινητό τηλέφωνο

sambaNTPassword: Κωδικός για SMB-encrypted-password authentication.

schacPersonalUniqueID: Μοναδικό ID

schacPersonalUniqueID: Μοναδικό ID

schGrAcPersonID: Μοναδικό χαρακτηριστικό ID χρήστη

schGrAcPersonSSN: ΑΜΚΑ χρήστη

schGrAcPersonTIN: ΑΦΜ χρήστη

Απολύτως απαραίτητα στοιχεία θεωρούνται το uid και οι τρεις κωδικοί, ενώ το RDN του χρήστη δημιουργείται μέσω του schGrAcPersonID. Επιπλέον απαραίτητες πληροφορίες είναι τα δεδομένα schGrAcPersonSSN και schGrAcPersonTIN, που αποτελούν τα στοιχεία ΑΜΚΑ και ΑΦΜ, που όπως αναφέρθηκε αποτελούν στοιχεία αντιστοίχισης της οντότητας με άλλες υποδομές.

### 5.3.2 Πολιτικές κωδικών (password policy)

Βασικό στοιχείο του καταλόγου είναι η ύπαρξη του σχήματος ppolicy. Αυτό είναι απαραίτητο για την υποστήριξη της λειτουργίας πολιτικών κωδικών, βασική προϋπόθεση για την λειτουργία της υπηρεσίας Arcanum.

Η πολιτική κωδικών είναι ένα σύνολο κανόνων που έχει σαν σκοπό να ενισχύσει την ασφάλεια στους κωδικούς μέσω της υποχρεωτικής χρήσης συγκεκριμένων κανόνων. Αυτοί οι κανόνες χωρίζονται στις ακόλουθες κατηγορίες:

**Ισχύς κωδικών**: Χρήση επιπλέον χαρακτήρων πέρα από τα απλά πεζά γράμματα, όπως αριθμούς, κεφαλαία και ειδικούς χαρακτήρες (πχ. @, #, $ ).

**Διάρκεια κωδικού**: Υποχρέωση αλλαγής κωδικών σε τακτά χρονικά διαστήματα και εφαρμογή πολιτικής για την χρήση παλαιοτέρων χρησιμοποιημένων κωδικών

**Συνήθεις πρακτικές**: Αποφυγή διαμοιρασμού κωδικών, υπολογιστών και αλλαγή κωδικών όταν υπάρχει υπόνοια παραβίασης του.

Η προεπιλεγμένη πολιτική συνίσταται στις ακόλουθες παραμέτρους

'pwdAllowUserChange' => 'TRUE', (Επιτρέπεται αλλαγή από τον χρήστη)

'pwdCheckQuality' => 0, (Έλεγχος ποιότητας κωδικού)

'pwdExpireWarning' => 86400, (Χρόνος ειδοποίησης για λήξη κωδικού)

'pwdFailureCountInterval' => 0, (Πλήθος επιτρεπτών αποτυχημένων προσπαθειών)

'pwdGraceAuthNLimit' => 0, (Πλήθος εισόδων στο σύστημα με ληγμένο κωδικό)

'pwdInHistory' => 10, (Πλήθος κωδικών στο ιστορικό της εφαρμογής)

'pwdLockout' => 'TRUE', (Αποκλεισμός χρήστη λόγω λανθασμένου κωδικού)

'pwdLockoutDuration' => 0, (Διάρκεια αποκλεισμού χρήστη)

'pwdMaxAge' => 31536000*6, // 6 years! (Μέγιστη διάρκεια ισχύς κωδικού )

'pwdMaxFailure' => 0, (Πλήθος αποτυχημένων συνδέσεων μέχρι την ακύρωση κωδικού)

'pwdMinAge' => 60, (Ελάχιστη διάρκεια μέχρι την αλλαγή ενός κωδικού)

'pwdMinLength' => 8, (Ελάχιστο μήκος κωδικού)

'pwdMustChange' => 'TRUE', (Υποχρέωση αλλαγής κωδικού στην επόμενη σύνδεση)

'pwdSafeModify' => 'FALSE', (Χρήση του παλιού κωδικού για την ανάθεση νέου)

Όλα τα παραπάνω τίθενται στην διάθεση του διαχειριστή για ορισμό, μέσω της εφαρμογής Arcanum, που δρα υποστηρικτικά στο όλο οικοδόμημα, ενώ είναι δυνατός και ο ορισμός πολλαπλών πολιτικών και εφαρμογής τους σε διαφορετικές ομάδες χρηστών.

# 6. ΣΥΜΠΕΡΑΣΜΑΤΑ

Ένας από τους αντικειμενικούς στόχους του έργου είναι η παροχή της δυνατότητας για ομοσπονδιακή πιστοποίηση των χρηστών. Αυτό επιτυγχάνεται με τη χρήση των διατάξεων SSO και VD. Τα συστήματα αυτά απαιτούν όμως την ύπαρξη μιας αυστηρώς ορισμένης υπηρεσίας καταλόγου. Αυτή την ανάγκη έρχεται να καλύψει η εφαρμογή **Uregister**.

Αναπτύχθηκε έτσι ένα σύστημα που σχεδιάστηκε με κύριο γνώμονα το υπολογιστικό περιβάλλον μέσα στο οποίο δρα. Έτσι αξιοποιήθηκαν πλήρως οι τρέχουσες υποδομές βάσεων δεδομένων και υπηρεσιών καταλόγου, έτσι ώστε η υπηρεσία να αποτελέσει τον συνδετικό κρίκο μεταφοράς των δεδομένων των χρηστών από τη μια διάταξη στην άλλη.

Η εφαρμογή προορίζεται να εγκαθίστανται σε κάθε ίδρυμα που μετέχει της διαδικασίας και απαιτεί ελάχιστη υποστήριξη από τους διαχειριστές. Πέρα από το αρχικό στάδιο που αναμένεται σημαντικός φόρτος, η εφαρμογή δεν απαιτεί σημαντικούς πόρους και σε βάθος χρόνου θα έχει χαμηλή χρήση, τόση ώστε να μπορεί να υποστηρίξει πλέον και μετάβαση του συνόλου των χρηστών στις νέες υποδομές.

# 7. ΑΝΑΦΟΡΕΣ

*ADOdb.* http://adodb.sourceforge.net/.

*Apache log4php.* http://logging.apache.org/log4php/.

*Flight php.* http://flightphp.com/.

*Foundation Framework.* http://foundation.zurb.com/.

*GUnet web services.* http://code.uoa.gr/p/gunetws/.

*Mongodb.* http://www.mongodb.org/.

*phpMailer.* http://github.com/PHPMailer/PHPMailer.

*Rain tpl.* www.raintpl.com.

*Zend Framework - config module.* http://framework.zend.com/.

# 8. ΠΑΡΑΡΤΗΜΑ

## 8.1 ΒΙΒΛΙΟΘΗΚΗ ACIDGENERATOR

Στο πλαίσιο της δημιουργίας υποδομών καταλόγου στα ιδρύματα και κατά τη διαδικασία εισαγωγής χρηστών σε αυτές τις υποδομές, παρουσιάζεται η ανάγκη για τον ορισμό ενός μοναδικού ID που χαρακτηρίζει το άτομο. Είναι απαραίτητο να οριστεί αυτό το μοναδικό χαρακτηριστικό με σαφήνεια ώστε να ανταποκρίνεται στις παρούσες και μελλοντικές ανάγκες. Ακολούθως αναλύονται τόσο οι προδιαγραφές αυτού του πεδίου όσο και οι επιλογές υλοποίησης.

**Απαιτήσεις**

Βασική προϋπόθεσή είναι η μοναδικότητα του αναγνωριστικού πανελληνίως. Αυτό συνεπάγεται πως οι τιμές δεν μπορούν να επαναλαμβάνονται σε καμία περίπτωση, ούτε καν όταν αναφερόμαστε σε διαφορετικά εκπαιδευτικά ιδρύματα.

Αυτό αντιμετωπίζεται με την ύπαρξη ενός τμήματος που προσδιορίζει το εκπαιδευτικό ίδρυμα προέλευσης του ατόμου, μέσα στο ίδιο το αναγνωριστικό.

Κρίνεται σκόπιμο να υπάρχει και ένα κομμάτι του αναγνωριστικού που να προσδιορίζει τη χώρα προέλευσης του ατόμου. Έτσι σε συνδυασμό με το χαρακτηριστικό του τμήματος δημιουργείται ένα σύνολο ψηφίων που μεταφράζονται σε ένα ιεραρχικό σύστημα ονοματοθεσίας.

Τέλος το αναγνωριστικό χρήστη απαιτεί την ύπαρξη ενός τυχαίου αριθμού που θα δεν θα έχει καμιά εξάρτηση από την πραγματική υπόσταση του ατόμου. Αυτό το σύνολο ψηφίων απαιτείται να διατηρεί τη μοναδικότητα και την αποφυγή συγκρούσεων εσωτερικά σε ένα ίδρυμα/φορέα.

**Αλγοριθμικές Επιλογές**

Το μοναδικό χαρακτηριστικό του χρήστη επιλέγεται να αποτελείται από 25 αλφαριθμητικά ψηφία, τα οποία ακολούθως κωδικοποιούνται με μια μυστική φράση και έτσι δημιουργείται

Ένα μοναδικό αλφαριθμητικό, μήκους 32 ψηφιών, το οποίο αποτελεί και το επίσημο personID του χρήστη.

Τα 25 πηγαία ψηφία δημιουργίας του αναγνωριστικού αναλύονται ως ακολούθως

- 16 ψηφία έρχονται από την ώρα εγγραφής του χρήστη, χρησιμοποιώντας το unixtime και φτάνοντας σε επίπεδο microSecond. (Εναλλακτικά χρησιμοποιείται ο χρόνος μέχρι επίπεδο millisecond, και προστίθεται σε αυτόν ένα τριψήφιο τυχαίο αριθμητικό πεδίο.
- 4 ψηφία δίνουν το χαρακτηριστικό ιδρύματος προέλευσης του χρήστη.
- 4 ψηφία δίνουν το χαρακτηριστικό χώρας προέλευσης του χρήστη.
- 1 ψηφίο χρησιμοποιείται σαν έλεγχος εγκυρότητας.

**Υλοποίηση**

Για την υλοποίηση του personID επιλέγεται η δημιουργία αντιστοίχισης αριθμητικών πεδίων τόσο στα ιδρύματα όσο και για τις χώρες προέλευσης των ατόμων. Ιδιαίτερα στην περίπτωση της χώρας προέλευσης χρησιμοποιείται το πρότυπο ISO 3166 και χρησιμοποιείται το τριψήφιο αριθμητικό χαρακτηριστικό κάθε χώρας. Και στις δύο περιπτώσεις χρησιμοποιούνται τρία ψηφία, τα οποία συμπληρώνονται με έναν σταθερό τέταρτο, μη μηδενικό, για την αποφυγή μεταβλητού μήκους ψηφίων.

Το τελευταίο ψηφίο ελέγχου προσδιορίζεται με βάση τον αλγόριθμο Luhn, που είναι μια από τις πιο συχνά χρησιμοποιούμενες επιλογές γι αυτό το σκοπό.

Τέλος, η κωδικοποίηση του 25ψηφιου αριθμητικού γίνεται με την βιβλιοθήκη Hashids, τόσο διότι

παρέχει τη δυνατότητα χρήσης επιλεγμένου αλφαβήτου, όσο και για την απουσία επανάληψης αποτελεσμάτων.

Η δημιουργία του personID θα γίνεται κεντρικά από την αρχή διατήρησης της πληροφορίας. Για τις κατά τόπους υπηρεσίες θα υπάρχει μια διεπαφή που θα αναλαμβάνει την δημιουργία νέου χαρακτηριστικού personID.

## 8.2 Κωδικοι Λαθων

1. 'SESSION_EXPIRED' : 'code'=>1513, 'message'=>'Η συνεδρία έχει λήξει'
2. 'DB_ERROR': 'code'=>1514, 'message'=>'Παρουσιάστηκε πρόβλημα στην επικοινωνία'
3. 'LDAP_ERROR':'code'=>1515, 'message'=>'Παρουσιάστηκε πρόβλημα στην επικοινωνία'
4. 'NODB_USER':'code'=>1516, 'message'=>'Δεν βρέθηκε χρήστης με αυτά τα στοιχεία',
5. 'MULTIDB_USERS' : 'code'=>1517, 'message'=>'Πολλαπλοί χρήστες βρέθηκαν στην Βάση
6. 'MULTILDAP_USERS' : 'code'=>1518, 'message' => 'Πολλαπλοί χρήστες βρέθηκαν στον ldap'
7. 'USER_REGED' : 'code'=>1519, 'message'=>'Ο χρήστης έχει ήδη εγγραφεί
8. 'REG_ERROR' : 'code'=>1520, 'message'=>'Η εγγραφή δεν μπόρεσε να πραγματοποιηθεί στον ldap'
9. 'PIN_ERROR' : 'code'=>1521, 'message'=>'Δεν μπόρεσε να γίνει αποστολή PIN'
10. 'PIN_TIME_ERROR': 'code'=>1522, 'message'=>'Δεν μπορεί να γίνει αποστολή PIN λόγω χρονικού περιορισμού'
11. 'UID_ERROR' : 'code'=>1523, 'message'=>'Υπάρχει ασυνέπεια μεταξύ ονόματος χρήστη που ζητήθηκε και αυτό που υπάρχει στην βάση δεδομένων'
12. 'UID_ERROR' : 'code'=>1524, 'message'=>'Δεν ήταν δυνατόν να δημιουργηθεί μοναδικός κωδικός

## 8.3 Αρχειο Ρυθμισεων

```
<?php
/**
 * Configuration File for uregister
*/
return array(
'app' => array (
           'name'     => 'uregister',
           'version'=> '0.3',
           'session_name'   => 'ureg',
           'path'     => '/flight',
           'hash_salt'=> SECRETHASHSTRING,
           'hash_length'    => '30',
           'hash_dictionary'=> '0123456789ABCDEF',
),
'raintpl' => array (
           'tpl_dir'        => "templates/",
           'cache_dir'           => "cache/"
```

```
),
'mongo' => array(
            'host'=>'localhost',
            'db'=>'uregister',
            'collection'=>'pins'
),
      'acidProvider' => array(
            'url' => 'http://towas-devel.gunet.gr/',
            'method' => 'academicID.generateID'
            ),
'sms' => array(
            'key' => '0ccdd226e86f0c13f7b7f766035fbf08',
            'url'=> 'https://ws.gunet.gr/?service=sms&key=xxxxxx',
            'message' => '%s. Επιβεβαίωση ταυτότητας. Για να συνεχίσετε την εγγραφή εισάγετε το PIN:%s στην φόρμα εγγραφής μέχρι τις: %s'
            ),
'mail' => array(
            'host'=>'smtp.xxxxxx.com',
            'port'=>465,
            'smtpsecure'=>'ssl',
            'auth'=>true,
            'user'=> 'xxxxxx',
            'pass'=>'xxxxxx',
            'from'=>'noreply@teixal.gr',
            'fromName' => 'Registration Service',
            'subject' => 'PIN επιβεβαιωσης εγγραφής',
            'message' =>  "%s.<br>
            Επιβεβαίωση ταυτότητας. <br>
            Για να συνεχίσετε την εγγραφή εισάγετε το PIN:%s στην φόρμα εγγραφής μέχρι τις: %s"
            ),
'pin'=> array(
```

```
            'duration'=>900,
            'resendtime'=>20
            ),
'institution' => array(
      'default'=>array(
            'code' => 'local',
            'iid' => '001' ,
            'country_code' =>'AO',
            'name' => 'TEI Χαλκιδικής',
            'pinChannel' => array('mail','sms'),
            'simulateSms' => true,
            'simulateMail'=> true,
            'enable_maces' => true,

      'schacPersonalUniqueID_prefix'=>'urn:mace:terena.org:schac:personalUniqueID:gr:%s:%s',
      'schacPersonalUniqueID'=>array('SSN','TIN'),

      'schGrAcPersonIDKey_prefix'=>'urn:mace:teixal.gr:%s:hrms.teixal.gr:1:%s',
            'schGrAcPersonIDKey'=>array('personid','hrmsid'),
            'digestRealm'=>'teixal.gr',
            'contact'=> array(
                  'name' => 'Γιώργος Καλογήρου ',
                  'office'=> 'Διεύθυνση Διοικητικού',
                  'email' => 'george@teixal.gr',
                  'phone' => '2310-12345678',
                  ),
            'backupcontact'=> array(
                  'name' => 'Νικολοπούλου Γεωργία',
                  'office'=> 'Διεύθυνση Διοικητικού',
                  'email' => 'gnikolopoulou@teixal.gr',
                  'phone' => '26510-07308',
```

```
            ),
        'db'=> array(
            'type'=>'oracle',
            'host'=>'vd.teixal.gr:1521/Sdc.Glb',
            'dbtable'=>'v_employees',
            'user'=> 'vduser',
            'pass'=>'xxxxxxxxx'
        ),
        /*'db'=> array(
            'type'=>'mysql',
            'host'=>'localhost',
            'port'=>'3306',
            'dbname' => 'hrms',
            'dbtable'=>'dep',
            'user'=> 'xxxxxxxxx',
            'pass'=>'xxxxxxxxxxa'
            ),*/
        /*'db'=> array(
            'type'=>'mssql',
            'host'=>'vd.teixal.gr',
            'port'=>'1433',
            'dbname' => 'STAFF',
            'dbtable'=>'v_employees',
            'user'=> 'vduser',
            'pass'=>'xxxxxxx'
            ),*/
        'ldap' => array(
            'host'=>'localhost',
            'port'=>'389',
            'binddn'=>'cn=admin,dc=teixal,dc=gr',
            'basedn'=>'ou=people,dc=teixal,dc=gr',
```

```
                'pass'=>'xxxxxxxx',
                ),
            'password_strength_policy'=>array(
                    'PW_CHECK_LEVENSHTEIN' => 2,
                    'PW_CHECK_MIN_LEN' => 6,
                    'PW_CHECK_MIN_UNIQ' => 5,
                    'PW_CHECK_MIN_LCS' => 40,
                    'PW_CHECK_MIN_NON_ALPHA' => 2,
                    'PW_MIN_CONSECUTIVE_NUMBERS' => 3,
                ),
   //available tests are regexpTest, consecutivenumbersTest, lengthTest, similarityTest, uniqueTest'
     password_strength_tests'=>array('regexpTest', 'consecutivenumbersTest', 'lengthTest', 'similarityTest', 'uniqueTest'),
            ),
     ),
);
?>
```

## 8.4 Ρυθμισεις Καταγραφης

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration xmlns="http://logging.apache.org/log4php/">

     <appender name="thefile" class="LoggerAppenderFile">
       <layout class="LoggerLayoutPattern">
     <param name="conversionPattern" value="%date %-5level %sessionid %msg%n" />
        </layout>
       <param name="file" value="/var/log/uregister.log" />
```

```
        <param name="append" value="true" />
     </appender>
    <appender name="thesyslog" class="LoggerAppenderSyslog">
        <param name="ident" value="uregister" />
        <param name="facility" value="LOCAL5" />
        <param name="option" value="NDELAY|PID" />
         <layout class="LoggerLayoutPattern">
      <param name="conversionPattern" value="%logger %-5level %sessionid
%location %line %msg%n" />
         </layout>
    </appender>

<!--this logger writes to the app log -->
   <logger name="main">
        <level value="info" />
        <appender_ref ref="thafile" />
   </logger>
<!--this logger writes to the syslog -->
   <root>
         <level value="debug" />
        <appender_ref ref="thasyslog" />
   </root>

</configuration>
```

## 8.5 ΡΥΘΜΙΣΕΙΣ ΚΑΤΑΛΟΓΟΥ ΤΑΥΤΟΠΟΙΗΣΗΣ ΚΑΙ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ

```
dn: cn=config

objectClass: olcGlobal

cn: config

olcArgsFile: /var/run/slapd/slapd.args
```

```
olcLogLevel: none

olcPidFile: /var/run/slapd/slapd.pid

olcToolThreads: 1

structuralObjectClass: olcGlobal

entryUUID: b3ed2a20-6332-1033-83be-1f19e24c4a65

creatorsName: cn=config

createTimestamp: 20140428150830Z

entryCSN: 20140428150830.542191Z#000000#000#000000

modifiersName: cn=config

modifyTimestamp: 20140428150830Z


dn: cn=module{0},cn=config

objectClass: olcModuleList

cn: module{0}

olcModulePath: /usr/lib/ldap

olcModuleLoad: {0}back_mdb

olcModuleLoad: {1}constraint

olcModuleLoad: {2}unique

olcModuleLoad: {3}sssvlv

olcModuleLoad: {4}syncprov

structuralObjectClass: olcModuleList

entryUUID: b3edb5da-6332-1033-83c6-1f19e24c4a65

creatorsName: cn=config

createTimestamp: 20140428150830Z

entryCSN: 20140614130944.107660Z#000000#000#000000

modifiersName: cn=config

modifyTimestamp: 20140614130944Z
```

```
dn: cn=schema,cn=config
objectClass: olcSchemaConfig
cn: schema
structuralObjectClass: olcSchemaConfig
entryUUID: b3ed3cd6-6332-1033-83c1-1f19e24c4a65
creatorsName: cn=config
createTimestamp: 20140428150830Z
entryCSN: 20140428150830.542731Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20140428150830Z



dn: olcBackend={0}mdb,cn=config
objectClass: olcBackendConfig
olcBackend: {0}mdb
structuralObjectClass: olcBackendConfig
entryUUID: 8e4a2518-6335-1033-974f-e3d53141a157
creatorsName: cn=config
createTimestamp: 20140428152855Z
entryCSN: 20140428152855.888355Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20140428152855Z

dn: olcDatabase={-1}frontend,cn=config
objectClass: olcDatabaseConfig
```

```
objectClass: olcFrontendConfig

olcDatabase: {-1}frontend

olcAccess: {0}to * by dn.exact=gidNumber=0+uidNumber=0,cn=peercred,cn=external
 ,cn=auth manage by * break

olcAccess: {1}to dn.exact="" by * read

olcAccess: {2}to dn.base="cn=Subschema" by * read

structuralObjectClass: olcDatabaseConfig

entryUUID: 8e4a29e6-6335-1033-9750-e3d53141a157

creatorsName: cn=config

createTimestamp: 20140428152855Z

entryCSN: 20140428152855.888498Z#000000#000#000000

modifiersName: cn=config

modifyTimestamp: 20140428152855Z


dn: olcDatabase={0}config,cn=config

objectClass: olcDatabaseConfig

olcDatabase: {0}config

olcAccess: {0}to * by dn.exact=gidNumber=0+uidNumber=0,cn=peercred,cn=external
 ,cn=auth manage by * break

olcRootDN: cn=config

olcRootPW:: e1NTSEF9TnRnclVzZmpJa0U3OEg2OWt6OVVZckE0L2hoMmNiYWI=

structuralObjectClass: olcDatabaseConfig

entryUUID: 8e4a3012-6335-1033-9751-e3d53141a157

creatorsName: cn=config

createTimestamp: 20140428152855Z

entryCSN: 20140428152855.888657Z#000000#000#000000

modifiersName: cn=config
```

```
modifyTimestamp: 20140428152855Z

dn: olcDatabase={1}mdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcMdbConfig
olcDatabase: {1}mdb
olcDbDirectory: /var/lib/ldap/dc=gunet,dc=gr
olcSuffix: dc=gunet,dc=gr
olcAccess: {0}to dn.base="" by * read
olcAccess: {1}to attrs=userPassword by anonymous auth by dn="cn=admin,dc=gunet
 ,dc=gr" write by * none
olcAccess: {2}to attrs=digestHA1,sambaNTPassword by dn="cn=admin,dc=gunet,dc=g
 r" write by * none
olcAccess: {3}to dn.subtree="ou=People,dc=gunet,dc=gr" attrs=objectClass val.r
 egex="extendedAuthentication|schacLinkageIdentifiers|schGrAcLinkageIdentifier
 s|simpleSecurityObject" by dn="uid=replicationService,ou=Services,dc=gunet,dc
 =gr" none by dn="cn=admin,dc=gunet,dc=gr" manage by * none
olcAccess: {4}to dn.subtree="ou=People,dc=gunet,dc=gr" attrs=mailForwardingAdd
 ress,schGrAcPersonTIN,schGrAcPersonSSN,schGrAcPersonIDKey,schacPersonalUnique
 ID,mobile by dn="uid=replicationService,ou=Services,dc=gunet,dc=gr" none by d
 n="cn=admin,dc=gunet,dc=gr" manage by * none
olcAccess: {5}to dn.subtree="ou=People,dc=gunet,dc=gr" by dn="uid=replicationS
 ervice,ou=Services,dc=gunet,dc=gr" read by dn="cn=admin,dc=gunet,dc=gr" manag
 e by * none
olcAccess: {6}to * by dn="cn=admin,dc=gunet,dc=gr" manage by * none
olcLastMod: TRUE
olcRootDN: cn=admin,dc=gunet,dc=gr
```

```
olcRootPW:: e1NTSEF9UkgxckFBZ3ZMSFN6ckMwR3pTdWxvUmtiRi9iME1CdWU=

olcDbIndex: objectClass eq

structuralObjectClass: olcMdbConfig

entryUUID: 70c6b08c-6336-1033-93f7-857576a95b62

creatorsName: cn=config

createTimestamp: 20140428153515Z

entryCSN: 20140614003747.528580Z#000000#000#000000

modifiersName: cn=config

modifyTimestamp: 20140614003747Z


dn: olcOverlay={0}constraint,olcDatabase={1}mdb,cn=config

objectClass: olcConstraintConfig

objectClass: olcOverlayConfig

olcOverlay: {0}constraint

olcConstraintAttribute: schGrAcPersonSSN regex ^[[:digit:]]{11}$

olcConstraintAttribute: schGrAcPersonTIN regex ^[[:digit:]]{9}$

olcConstraintAttribute: uid count 1

olcConstraintAttribute: uid regex ^[a-z0-9]([._-]?[a-z0-9]){2,10}[a-z0-9]$ res
 trict="ldap:///ou=People,dc=gunet,dc=gr??sub"

olcConstraintAttribute: mailForwardingAddress regex ^[a-z0-9!#$%&'*+/=?^_`{|}~
 -]+(\.[a-z0-9!#$%&'*+/=?^_`{|}~-]+)*@([a-z0-9]([a-z0-9-]*[a-z0-9])?\.)+[a-z0-
 9]([a-z0-9-]*[a-z0-9])?$

olcConstraintAttribute: schGrAcPersonID regex ^[0-9A-F]{16,}$

structuralObjectClass: olcConstraintConfig

entryUUID: 94d18926-878e-1033-84da-2fae0b757cce

creatorsName: cn=config

createTimestamp: 20140613213653Z
```

```
entryCSN: 20140614005856.240933Z#000000#000#000000

modifiersName: cn=config

modifyTimestamp: 20140614005856Z


dn: olcOverlay={1}unique,olcDatabase={1}mdb,cn=config

objectClass: olcOverlayConfig

objectClass: olcUniqueConfig

olcOverlay: {1}unique

olcUniqueURI: ldap:///ou=People,dc=gunet,dc=gr?schGrAcPersonSSN,schGrAcPersonT
 IN?sub

olcUniqueURI: ldap:///?uid?sub

structuralObjectClass: olcUniqueConfig

entryUUID: 94d41a38-878e-1033-84db-2fae0b757cce

creatorsName: cn=config

createTimestamp: 20140613213653Z

entryCSN: 20140613213653.927744Z#000000#000#000000

modifiersName: cn=config

modifyTimestamp: 20140613213653Z


dn: olcOverlay={2}sssvlv,olcDatabase={1}mdb,cn=config

objectClass: olcOverlayConfig

objectClass: olcSssVlvConfig

olcOverlay: {2}sssvlv

structuralObjectClass: olcSssVlvConfig

entryUUID: 94d6c6d4-878e-1033-84dc-2fae0b757cce

creatorsName: cn=config

createTimestamp: 20140613213653Z
```

```
entryCSN: 20140613213653.945271Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20140613213653Z

dn: olcOverlay={3}syncprov,olcDatabase={1}mdb,cn=config
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: {3}syncprov
structuralObjectClass: olcSyncProvConfig
entryUUID: e5a85c3a-8810-1033-9b56-75b46ac744d8
creatorsName: cn=config
createTimestamp: 20140614130944Z
entryCSN: 20140614130944.111374Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20140614130944Z
```

## 8.6 ΑΠΑΡΑΙΤΗΤΑ ΣΧΗΜΑΤΑ

### 8.6.1 ExtendedAuth

```
dn: cn=extendedAuth,cn=schema,cn=config
changetype: add
objectClass: olcSchemaConfig
cn: extendedAuth
```

```
olcObjectIdentifier: GUnet 1.3.6.1.4.1.36215

olcObjectIdentifier: extendedAuth GUnet:2

olcObjectIdentifier: extendedAuthAttribute extendedAuth:1

olcObjectIdentifier: extendedAuthObjectClass extendedAuth:2

olcAttributeTypes: {0}( 1.3.6.1.4.1.7165.2.1.25
 NAME 'sambaNTPassword'
 DESC 'MD4 hash of the unicode password'
 EQUALITY caseIgnoreIA5Match
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{32} SINGLE-VALUE )

olcAttributeTypes: {1}( 2.16.840.1.113730.3.1.17
 NAME 'mailForwardingAddress'
 DESC 'User-specifiable mail forwarding address(es)'
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{256} )

olcAttributeTypes: {2}( extendedAuthAttribute:1
 NAME 'ctp'
 DESC 'CTP'
 EQUALITY caseIgnoreIA5Match
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{256} )

olcAttributeTypes: {3}( extendedAuthAttribute:2
 NAME 'digestHA1'
 DESC 'MD5 hash of the uid:realm:password string'
 EQUALITY caseIgnoreIA5Match
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{32} SINGLE-VALUE )

olcAttributeTypes: {4}( extendedAuthAttribute:3
 NAME 'authMethods'
 DESC 'Other authentication methods used for password reset or other purposes'
 EQUALITY caseIgnoreIA5Match
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{256} )
```

olcObjectClasses: {0}( extendedAuthObjectClass:1

NAME 'extendedAuthentication'

DESC 'Enables extended authentication attributes via additional password hashes and attributes that activates external authentication methods to be used for password reset'

SUP top

AUXILIARY

MAY( mobile $ sambaNTPassword $ mailForwardingAddress $ ctp $ digestHA1 $ authMethods ))

### 8.6.2 SchAcSchema

dn: cn=schac,cn=schema,cn=config

changetype: add

objectClass: olcSchemaConfig

cn: schac

olcObjectIdentifier: TERENA 1.3.6.1.4.1.25178

olcObjectIdentifier: schac TERENA:1

olcObjectIdentifier: schacExperimental schac:0

olcObjectIdentifier: schacObjectClass schac:1

olcObjectIdentifier: schacAttributeType schac:2

olcObjectIdentifier: schacExpObjClass schacExperimental:1

olcObjectIdentifier: schacExpAttr schacExperimental:2

olcAttributeTypes: ( schacAttributeType:1

NAME 'schacMotherTongue'

DESC 'RFC 3066 code for prefered language of communication'

EQUALITY caseExactMatch

SINGLE-VALUE

SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

olcAttributeTypes: ( schacAttributeType:2

NAME 'schacGender'

DESC 'Representation of human sex (see ISO 5218)'

EQUALITY integerMatch

SINGLE-VALUE

SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 )

olcAttributeTypes: ( schacAttributeType:3

NAME 'schacDateOfBirth'

DESC 'Date of birth (format YYYYMMDD, only numeric chars)'

EQUALITY numericStringMatch

ORDERING numericStringOrderingMatch

SUBSTR numericStringSubstringsMatch

SINGLE-VALUE

SYNTAX 1.3.6.1.4.1.1466.115.121.1.36 )

olcAttributeTypes: ( schacAttributeType:4

NAME 'schacPlaceOfBirth'

DESC 'Birth place of a person'

EQUALITY caseIgnoreMatch

ORDERING caseIgnoreOrderingMatch

SUBSTR caseIgnoreSubstringsMatch

SINGLE-VALUE

SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

olcAttributeTypes: ( schacAttributeType:5

NAME 'schacCountryOfCitizenship'

DESC 'Country of citizenship of a person. Format two-letter acronym according to ISO 3166'

EQUALITY caseIgnoreMatch

```
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
olcAttributeTypes: ( schacAttributeType:6
NAME 'schacSn1'
DESC 'First surname of a person'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
olcAttributeTypes: ( schacAttributeType:7
NAME 'schacSn2'
DESC 'Second surname of a person'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
olcAttributeTypes: ( schacAttributeType:8
NAME 'schacPersonalTitle'
DESC 'RFC1274: personal title'
EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SINGLE-VALUE
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15 )
olcAttributeTypes: ( schacAttributeType:9
NAME 'schacHomeOrganization'
DESC 'Domain name of the home organization'
EQUALITY caseIgnoreMatch
```

```
SUBSTR caseIgnoreSubstringsMatch
SINGLE-VALUE
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
olcAttributeTypes: ( schacAttributeType:10
NAME 'schacHomeOrganizationType'
DESC 'Type of the home organization'
EQUALITY caseIgnoreMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
olcAttributeTypes: ( schacAttributeType:11
NAME 'schacCountryOfResidence'
DESC 'Country of citizenship of a person. Format two-letter acronym according to ISO 3166'
EQUALITY caseIgnoreMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
olcAttributeTypes: ( schacAttributeType:12
NAME 'schacUserPresenceID'
DESC 'Used to store a set of values related to the network presence'
EQUALITY caseExactMatch
SUBSTR caseExactSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
olcAttributeTypes: ( schacAttributeType:13
NAME 'schacPersonalPosition'
DESC 'Position inside an institution'
EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
olcAttributeTypes: ( schacAttributeType:14
```

```
NAME 'schacPersonalUniqueCode'
DESC 'unique code for the subject'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
olcAttributeTypes: ( schacAttributeType:15
NAME 'schacPersonalUniqueID'
DESC 'Unique identifier for the subject'
EQUALITY caseExactMatch
ORDERING caseExactOrderingMatch
SUBSTR caseExactSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
olcAttributeTypes: ( schacAttributeType:17
NAME 'schacExpiryDate'
DESC 'Date from which the set of data is to be considered invalid (format YYYYMMDDhhmmssZ)'
EQUALITY generalizedTimeMatch
ORDERING generalizedTimeOrderingMatch
SINGLE-VALUE
SYNTAX 1.3.6.1.4.1.1466.115.121.1.24 )
olcAttributeTypes: ( schacAttributeType:18
NAME 'schacUserPrivateAttribute'
DESC 'Set of denied access attributes'
EQUALITY caseIgnoreIA5Match
SUBSTR caseIgnoreIA5SubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

```
olcAttributeTypes: ( schacAttributeType:19
 NAME 'schacUserStatus'
 DESC 'Used to store a set of status of a person as user of services'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
olcAttributeTypes: ( schacAttributeType:20
 NAME 'schacProjectMembership'
 DESC 'Name of the project'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
olcAttributeTypes: ( schacAttributeType:21
 NAME 'schacProjectSpecificRole'
 DESC 'Used to store a set of roles of a person inside a project'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
olcObjectClasses: ( schacObjectClass:1
 NAME 'schacPersonalCharacteristics'
 DESC 'Personal characteristics describe the individual person represented by the entry'
 AUXILIARY
 MAY (
 schacMotherTongue $
 schacGender $
 schacDateOfBirth $
```

schacPlaceOfBirth $

schacCountryOfCitizenship $

schacSn1 $

schacSn2 $

schacPersonalTitle )

)

olcObjectClasses: ( schacObjectClass:2

NAME 'schacContactLocation'

DESC 'Primary means of locating and contacting potential collaborators and other persons-of-interest at peer institutions'

AUXILIARY

MAY (

schacHomeOrganization $

schacHomeOrganizationType $

schacCountryOfResidence $

schacUserPresenceID )

)

olcObjectClasses: ( schacObjectClass:3

NAME 'schacEmployeeInfo'

DESC 'Employee information includes attributes that have relevance to the employee role, such as position, office hours, and job title'

AUXILIARY

MAY ( schacPersonalPosition ) )

olcObjectClasses: ( schacObjectClass:4

NAME 'schacLinkageIdentifiers'

DESC 'Used to link a directory entry with records in external data stores or other directory entries'

AUXILIARY

MAY ( schacPersonalUniqueCode $ schacPersonalUniqueID ) )

olcObjectClasses: ( schacObjectClass:5

NAME 'schacEntryMetadata'

DESC 'Used to contain information about the entry itself, often its status, birth, and death'

AUXILIARY

MAY ( schacExpiryDate ) )

olcObjectClasses: ( schacObjectClass:6

NAME 'schacEntryConfidentiality'

DESC 'Used to indicate whether an entry is visible publicly, visible only to affiliates of the institution, or not visible at all'

AUXILIARY

MAY ( schacUserPrivateAttribute ) )

olcObjectClasses: ( schacObjectClass:7

NAME 'schacUserEntitlements'

DESC 'Authorization for services'

AUXILIARY

MAY ( schacUserStatus ) )

olcObjectClasses: ( schacObjectClass:8

NAME 'schacGroupMembership'

DESC 'Groups used to provide/restrict authorization to entries and attributes'

AUXILIARY

MAY ( schacProjectMembership $ schacProjectSpecificRole ) )

olcAttributeTypes: ( schacExpAttr:3

NAME 'schacYearOfBirth'

DESC 'Year of birth (format YYYY, only numeric chars)'

```
EQUALITY numericStringMatch
ORDERING numericStringOrderingMatch
SUBSTR numericStringSubstringsMatch
SINGLE-VALUE
SYNTAX 1.3.6.1.4.1.1466.115.121.1.36 )
olcObjectClasses: ( schacExpObjClass:1
NAME 'schacExperimentalOC'
DESC 'Experimental Object Class'
AUXILIARY
MAY ( schacYearOfBirth) )
```

### 8.6.3 SchGrAcSchema

```
dn: cn=schGrAc,cn=schema,cn=config
changetype: add
objectClass: olcSchemaConfig
cn: schGrAc
olcObjectIdentifier: GUnet 1.3.6.1.4.1.36215
olcObjectIdentifier: schGrAc GUnet:1
olcObjectIdentifier: schGrAcExperimental schGrAc:0
olcObjectIdentifier: schGrAcObjectClass schGrAc:1
olcObjectIdentifier: schGrAcAttributeType schGrAc:2
olcObjectIdentifier: schGrAcExpObjectClass schGrAcExperimental:1
olcObjectIdentifier: schGrAcExpAttributeType schGrAcExperimental:2
olcAttributeTypes: {0}( schGrAcAttributeType:1.1
```

```
 NAME 'schGrAcPersonSSN'
 DESC 'Social Security Number'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
olcAttributeTypes: {1}( schGrAcAttributeType:1.2
 NAME 'schGrAcPersonTIN'
 DESC 'Tax Identification Number'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
olcAttributeTypes: {2}( schGrAcAttributeType:2.1
 NAME 'schGrAcPersonID'
 DESC 'The unique identifier of a person across institution'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
olcAttributeTypes: {3}( schGrAcAttributeType:2.2
 NAME 'schGrAcPersonIDKey'
 DESC 'The unique identifier of a person per authoritative system'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
olcAttributeTypes: {4}( schGrAcAttributeType:2.3
 NAME 'schGrAcDepartmentID'
 DESC 'The unique identifier of a department in the organization chart of the
institution'
```

```
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
olcAttributeTypes: {5}( schGrAcAttributeType:2.4
 NAME 'schGrAcProgramID'
 DESC 'The unique identifier of a students program'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
olcObjectClasses: {0}( schGrAcObjectClass:1
 NAME 'schGrAcLinkageIdentifiers'
 DESC 'Unique identifiers which are defined and maintained by the Greek state'
 AUXILIARY
 MAY ( schGrAcPersonSSN $ schGrAcPersonTIN )
 )
olcObjectClasses: {1}( schGrAcObjectClass:2
 NAME 'schGrAcIdentifiers'
 DESC 'Unique identifiers which are defined and maintained by GUnet'
 AUXILIARY
 MAY ( schGrAcPersonID $ schGrAcPersonIDKey $ schGrAcDepartmentID $
schGrAcProgramID )
 )
```