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: Δράσεις εκπαίδευσης τεχνικού προσωπικού

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

Αντικείμενο 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 διϊδρυματικές εφαρμογές» είναι η ανάπτυξη ή αναβάθμιση Υπηρεσιών Καταλόγου και Υποδομής Ταυτοποίησης και Εξουσιοδότησης σε όλους τους Ακαδημαϊκούς και Ερευνητικούς Φορείς που είναι διασυνδεδεμένοι στο ΕΘΝΙΚΟ ΔΙΚΤΥΟ ΕΡΕΥΝΑΣ & ΤΕΧΝΟΛΟΓΙΑΣ (ΕΔΕΤ). Στόχος είναι η ένταξη στους καταλόγους των μελών του Ακαδημαϊκού και Διοικητικού Προσωπικού, ώστε να μπορούν να απολαμβάνουν τις υπηρεσίες που παρέχονται στην Ερευνητική και Ακαδημαϊκή Κοινότητα.

Μέσω της υποδομής, οι χρήστες έχουν πρόσβαση σε υπηρεσίες με ασφάλεια και εμπιστευτικότητα των προσωπικών τους δεδομένων, χρησιμοποιώντας τον ιδρυματικό τους λογαριασμό.

Το παρόν παραδοτέο εντάσσεται στο πλαίσιο αυτής της πράξης και περιλαμβάνει αρχικά, τις δράσεις εκπαίδευσης του Τεχνικού Προσωπικού που πραγματοποιήθηκαν και οι οποίες ήταν απαραίτητες για την επιτυχή διασύνδεση των Ακαδημαϊκών και Ερευνητικών Φορέων στην Ομοσπονδία καθώς και την μετέπειτα ορθή λειτουργία της υπηρεσίας του καταλόγου από τους χρήστες τους. Οι δράσεις αυτές αφορούσαν την ενημέρωση των τεχνικών υπευθύνων των Φορέων σχετικά με τα πλεονεκτήματα χρήσης του καταλόγου ενοποιημένης πρόσβασης, καθώς και σχετικά με τις τεχνολογίες ασφαλής υλοποίησης και χρήσης του από τα μέλη τους.

Επιπλέον, στο παρόν παραδοτέο θα παρουσιαστούν και οι δράσεις εκπαίδευσης που πραγματοποιήθηκαν στο Τεχνικό Προσωπικό του κάθε Φορέα και αφορούσαν τη διαδικασία της εγκατάστασης και της μετέπειτα ορθής διαχείρισης του αναπτυχθέντος πληροφοριακού συστήματος των καταλόγων ενοποιημένης πρόσβασης και πιστοποίησης.

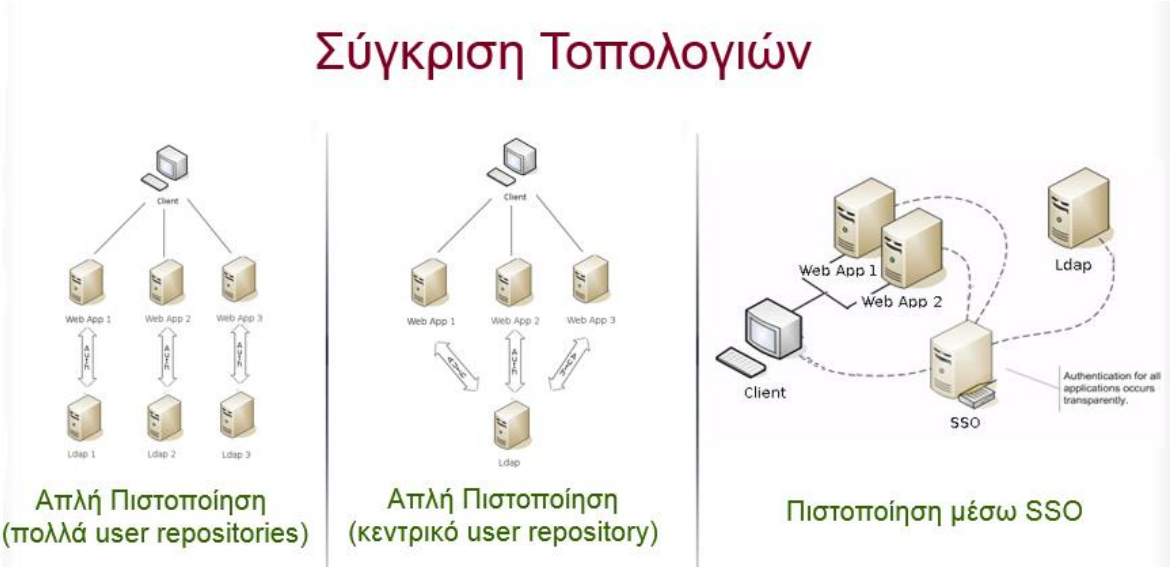
2. ΔΡΑΣΕΙΣ ΕΚΠΑΙΔΕΥΣΗΣ ΣΧΕΤΙΚΑ ΜΕ ΤΙΣ ΤΕΧΝΟΛΟΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ ΚΑΙ ΑΣΦΑΛΗΣ ΧΡΗΣΗΣ ΤΟΥ ΚΑΤΑΛΟΓΟΥ ΕΝΟΠΟΙΗΜΕΝΗΣ ΠΡΟΣΒΑΣΗΣ ΚΑΙ ΤΑ ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΧΡΗΣΗΣ ΤΟΥ

Οι δράσεις υποστήριξης των φορέων υπηρεσιών (SP) για την ένταξή τους στις υπηρεσίες ενοποιημένης ταυτοποίησης περιλάμβαναν δράσεις ενημέρωσης και παροχής τεχνικής βοήθειας, αρχικά, για την επιτυχή διασύνδεσή των Φορέων στις υπηρεσίες ενοποιημένης ταυτοποίησης, καθώς και την εξασφάλιση της ομαλής λειτουργίας τους στη συνέχεια.

2.1 ΕΝΗΜΕΡΩΣΗ ΣΧΕΤΙΚΑ ΜΕ ΤΑ ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΧΡΗΣΗΣ ΤΟΥ ΚΑΤΑΛΟΓΟΥ ΕΝΟΠΟΙΗΜΕΝΗΣ ΠΡΟΣΒΑΣΗΣ ΓΙΑ ΕΝΔΟΪΔΡΥΜΑΤΙΚΕΣ ΚΑΙ ΔΙΪΔΡΥΜΑΤΙΚΕΣ ΕΦΑΡΜΟΓΕΣ

Κατά τη διάρκεια του έργου, πραγματοποιήθηκαν δράσεις ενημέρωσης των τεχνικών υπεύθυνων των Φορέων σχετικά με τα πλεονεκτήματα που θα έχει για τους χρήστες τους, η χρήση του καταλόγου ενοποιημένης πρόσβασης.

Ειδικότερα, παρουσιάστηκαν με παραδείγματα, τα συγκριτικά πλεονεκτήματα αυτής της μεθόδου, σε σχέση με την διαδικασία που ακολουθούνταν μέχρι εκείνη τη στιγμή από τον κάθε Φορέα, ενώ, οι τεχνικοί υπεύθυνοι των Φορέων ενημερώθηκαν, επίσης, και για τις υπηρεσίες στις οποίες θα μπορούν να έχουν πρόσβαση οι χρήστες τους μέσω του καταλόγου ενοποιημένης πρόσβασης.



Επίσης, κατά τη διάρκεια των δράσεων αυτών, παρουσιάστηκε στους υπεύθυνους των Φορέων η Υποδομή Ταυτοποίησης και Εξουσιοδότησης, η οποία επιτρέπει σε διαφορετικούς οργανισμούς να συνεργάζονται στην εκχώρηση δικαιωμάτων πρόσβασης για εφαρμογές που έχουν διιδρυματικό χαρακτήρα. Μέσω της υποδομής, οι χρήστες του Φορέα μπορούν να λάβουν υπηρεσίες με ασφάλεια και εμπιστευτικότητα των προσωπικών τους δεδομένων χρησιμοποιώντας απλά τον ιδρυματικό τους λογαριασμό.

Επιπλέον, έγινε παρουσίαση της Ομοσπονδίας του ΕΔΕΤ, στην οποία συμμετέχουν μέλη της Ακαδημαϊκής, Ερευνητικής και Εκπαιδευτικής κοινότητας της Ελλάδας καθώς και Φορείς που ενδιαφέρονται να παρέχουν υπηρεσίες σε αυτή.

Τέλος, παρουσιάστηκαν λεπτομερώς τα πολλαπλά οφέλη που απολαμβάνουν οι χρήστες των Φορέων που είναι ενταγμένοι στον κατάλογο ενοποιημένης πρόσβασης, όπως:

- είσοδο σε όλες τις συνδεδεμένες με την Ομοσπονδία υπηρεσίες
- είσοδο στις συνδεδεμένες με την Ομοσπονδία υπηρεσίες με τη χρήση του υπάρχοντος ιδρυματικού λογαριασμού του χρήστη, χωρίς να απαιτείται ξεχωριστή εγγραφή

- τα στοιχεία που αφορούν την ταυτότητα, ιδιότητα και προέλευση του κάθε χρήστη δεν είναι απαραίτητο να αποστέλλονται στον κάθε πάροχο υπηρεσίας, παρέχοντας δυνατότητα *"ανώνυμης"* πιστοποιημένης πρόσβασης.

2.2 ΕΝΗΜΕΡΩΣΗ ΣΧΕΤΙΚΑ ΜΕ ΤΙΣ ΤΕΧΝΟΛΟΓΙΕΣ ΚΕΝΤΡΙΚΗΣ ΠΙΣΤΟΠΟΙΗΣΗΣ (CAS) ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΟΥΝΤΑΙ ΓΙΑ ΤΗΝ ΑΣΦΑΛΗ ΕΙΣΟΔΟ ΤΩΝ ΧΡΗΣΤΩΝ ΣΤΙΣ ΥΠΗΡΕΣΙΕΣ

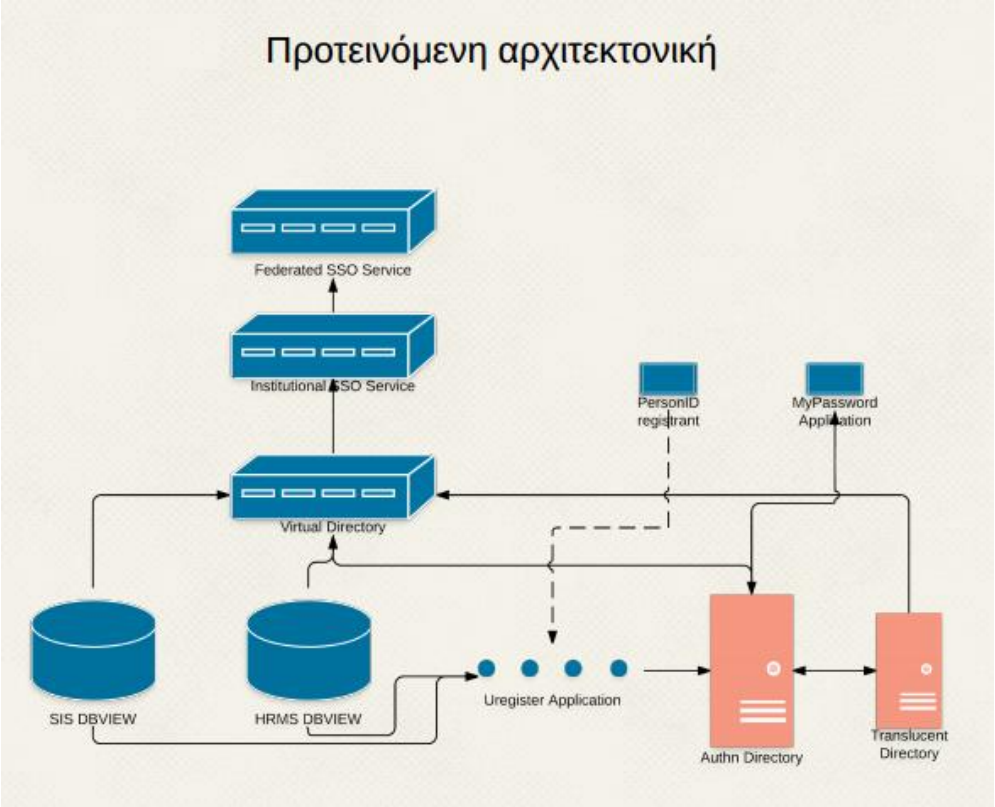
Επιπρόσθετα με τις δράσεις ενημέρωσης που αναφέρθηκαν στην προηγούμενη ενότητα και αφορούσαν τα πλεονεκτήματα χρήσης του καταλόγου ενοποιημένης πρόσβασης για την πρόσβαση σε ενδοϊδρυματικές και διϊδρυματικές εφαρμογές, εξειδικευμένες ενημερώσεις πραγματοποιήθηκαν στους τεχνικούς υπεύθυνους των Φορέων και όσον αφορά τις τεχνολογίες που χρησιμοποιούνται για την υλοποίηση και την ασφαλή χρήση των υπηρεσιών του καταλόγου από τους χρήστες τους.

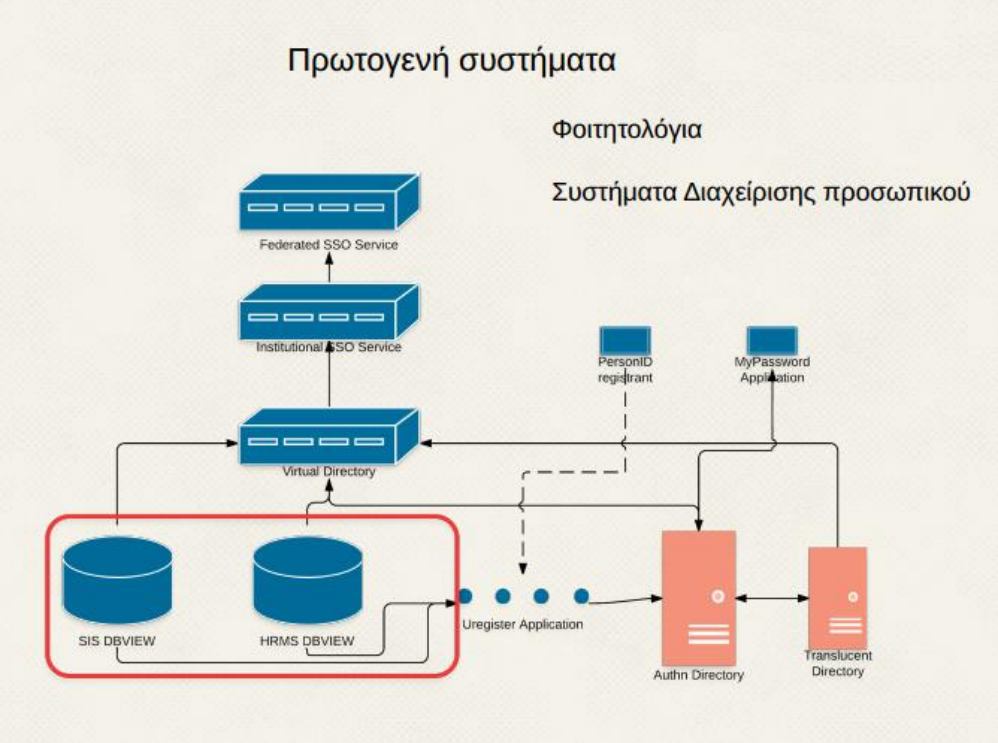
Ειδικότερα, οι τεχνικοί υπεύθυνοι των Φορέων ενημερώθηκαν σχετικά με την τεχνολογία κεντρικής ταυτοποίησης (CAS) και τα πλεονεκτήματα που αυτή προσφέρει, τόσο όσον αφορά την ασφάλεια εισόδου των χρηστών, όσο και την ελαχιστοποίηση των πόρων που χρησιμοποιούνται για την ταυτοποίησή τους.

Στο παράρτημα 2 που ακολουθεί στο τέλος του παρόντος εγγράφου, παρατίθενται οι διαφάνειες που χρησιμοποιήθηκαν στα πλαίσια αυτών των δράσεων ενημέρωσης των τεχνικών υπευθύνων των Φορέων.

3. ΔΡΑΣΕΙΣ ΕΚΠΑΙΔΕΥΣΗΣ ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΕΓΚΑΤΑΣΤΑΣΗ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΤΟΥ ΑΝΑΠΤΥΧΘΕΝΤΟΣ ΠΛΗΡΟΦΟΡΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ ΤΩΝ ΚΑΤΑΛΟΓΩΝ

Οι δράσεις εκπαίδευσης των τεχνικών υπευθύνων που πραγματοποιήθηκαν, δεν αφορούσαν μόνο την ενημέρωση τους γύρω από τη χρήση και τους τρόπους υλοποίησης του καταλόγου ενοποιημένης πρόσβασης. Αφορούσαν, επίσης, και την εκπαίδευση των τεχνικών υπεύθυνων σχετικά με τον τρόπο εγκατάστασης του πληροφοριακού συστήματος των καταλόγων στο Φορέα τους και τη διασύνδεσή του με τα υπόλοιπα-υφιστάμενα πληροφοριακά συστήματα του Φορέα.





3.1 ΕΓΚΑΤΑΣΤΑΣΗ ΚΑΙ ΟΡΘΗ ΧΡΗΣΗ ΤΟΥ ΠΛΗΡΟΦΟΡΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ ΤΩΝ ΚΑΤΑΛΟΓΩΝ

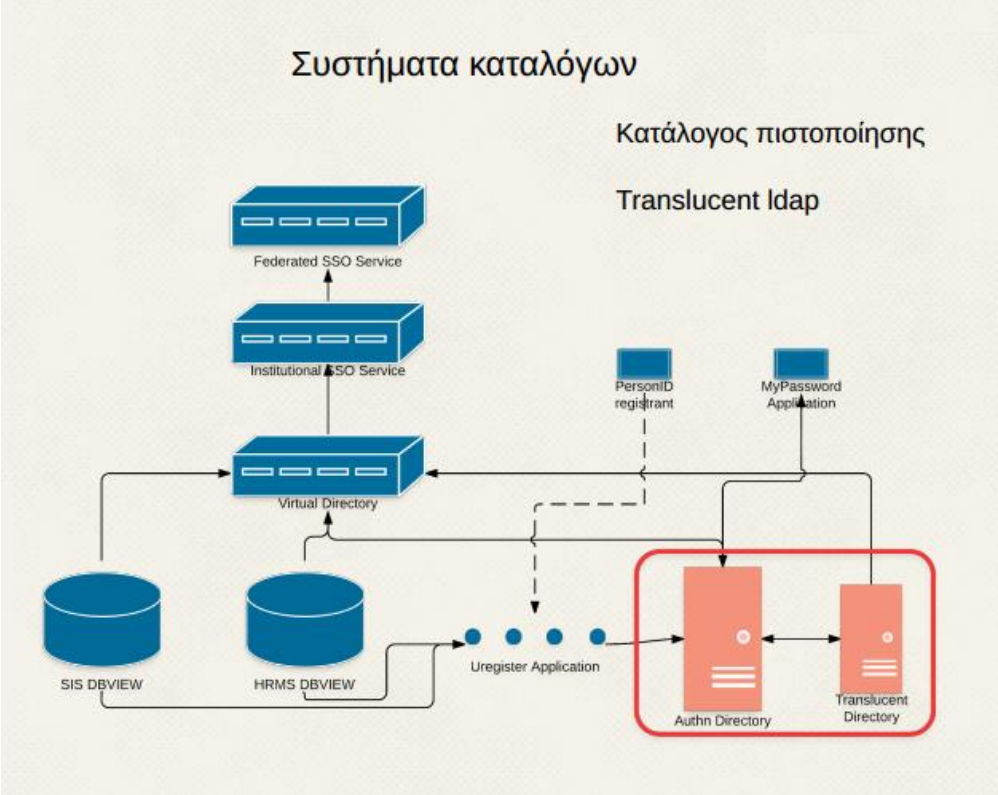
Τελικός στόχος των υπηρεσιών καταλόγου είναι η δημιουργία ενός συνολικού object για κάθε ενδιαφερόμενο χρήστη. Αυτό το object δεν βρίσκεται αποκλειστικά σε μια υποδομή, αλλά διανέμεται σε επιμέρους καταλόγους, οι οποίοι έχουν διακριτούς ρόλους. Επομένως, η εγκατάσταση του πληροφοριακού συστήματος των Καταλόγων περιλάμβανε την εγκατάσταση άλλων επιμέρους καταλόγων. Αυτοί είναι οι εξής:

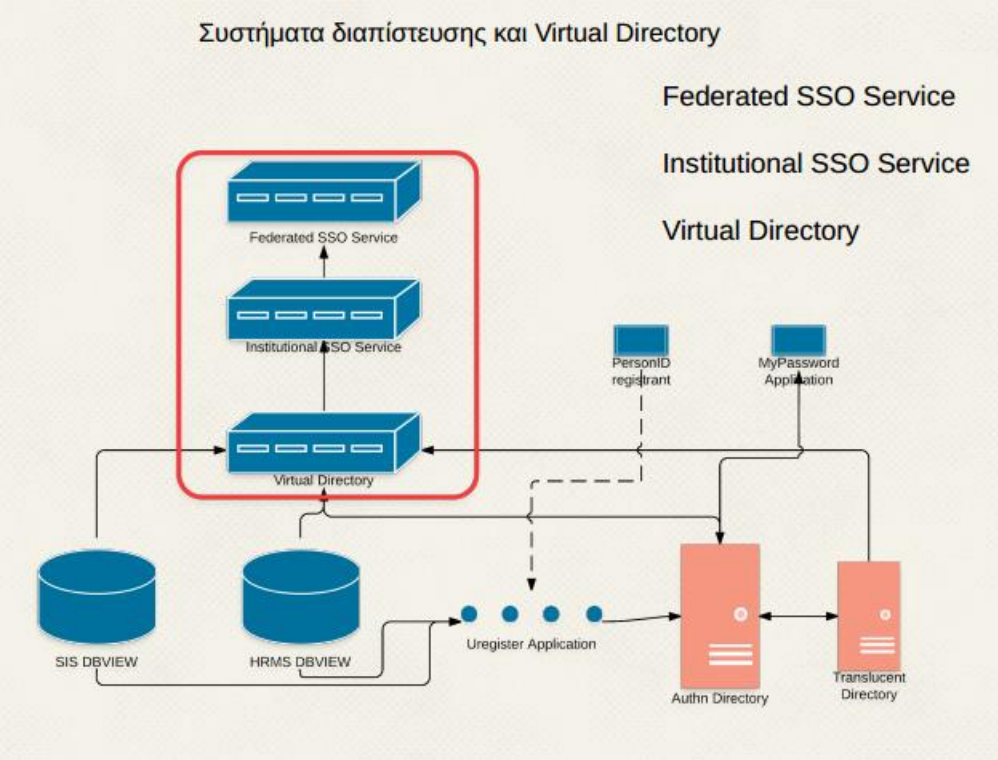
- **Virtual Directory**. Είναι ένας κατάλογος, τα περιεχόμενα του οποίου, ωστόσο, προκύπτουν δυναμικά από τα στοιχεία που διατηρούν πρωτογενή πληροφοριακά συστήματα για τον χρήστη και εστιάζουν κυρίως σε στοιχεία όπως το όνομα, η ιδιότητα, η οργανωτική μονάδα στην οποία ανήκει ο χρήστης κ.α. Τέτοια πληροφοριακά 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)

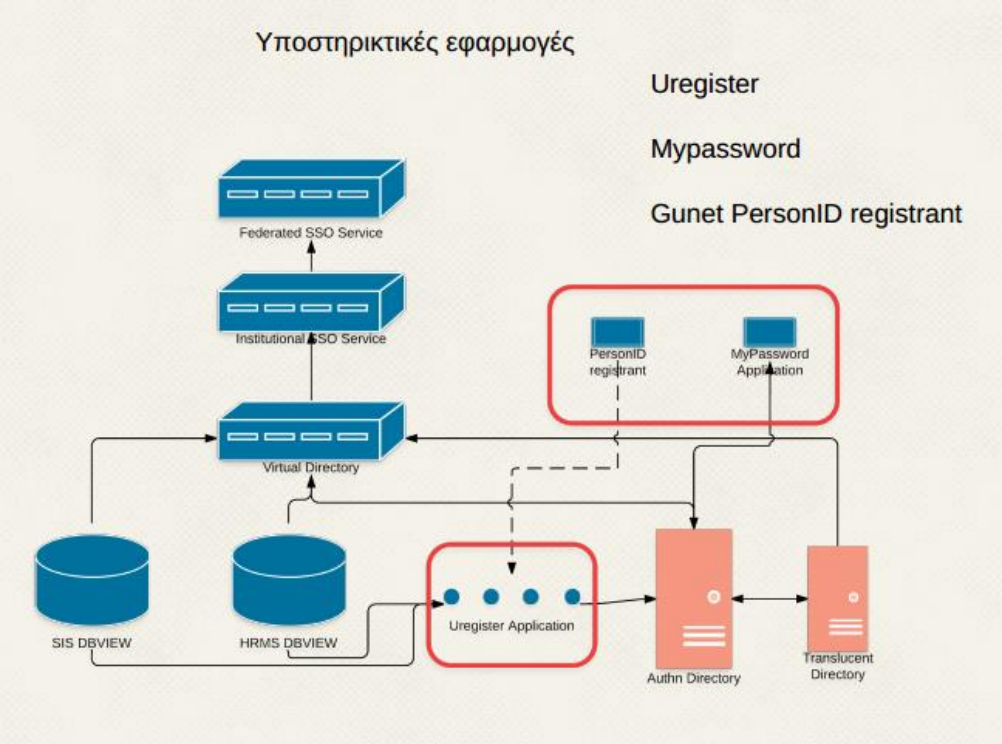
- **Translucent Directory**. Είναι ένας κατάλογος, ο οποίος είναι επικουρικός στη προτεινόμενη αρχιτεκτονική. Εξυπηρετεί την αποθήκευση προσωπικών και δευτερευόντων στοιχείων ενός χρήστη, εφόσον αυτά δεν ακυρώνουν τα στοιχεία που προέρχονται από πρωτογενή και εξουσιοδοτημένα πληροφοριακά συστήματα. Τέτοια στοιχεία μπορεί να προκύπτουν από επέκταση του ldap object με πεδία που χρειάζονται για ειδικές υπηρεσίες / εφαρμογές που λειτουργούν στον φορέα.

- **Authentication Directory**. Είναι ένας κατάλογος, του οποίου αποκλειστική αποστολή είναι η 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.


Συστήματα καταλόγων
Κατάλογος πιστοποίησης
Translucent ldap
Federated SSO Service
Institutional SSO Service
PersonID registrant
MyPassword Application
Virtual Directory
SIS DBVIEW
HRMS DBVIEW
Uregister Application
Authn Directory
Translucent Directory


Συστήματα διαπίστευσης και Virtual Directory
Federated SSO Service
Institutional SSO Service
Virtual Directory
Federated SSO Service
Institutional SSO Service
PersonID registrant
MyPassword Application
Virtual Directory
SIS DBVIEW
HRMS DBVIEW
Uregister Application
Authn Directory
Translucent Directory

Για την ορθή χρήση και διαχείριση του πληροφοριακού συστήματος, απαιτείται, επίσης, η εγκατάσταση των υποστηρικτικών εφαρμογών ενεργοποίησης λογαριασμού χρήστη Uregister και διαχείρισης κωδικών πρόσβασης Mypassword που θα παρουσιαστούν στις επόμενες ενότητες.



3.2 ΥΠΗΡΕΣΙΑΣ ΕΝΕΡΓΟΠΟΙΗΣΗΣ ΛΟΓΑΡΙΑΣΜΟΥ ΧΡΗΣΤΗ UREGISTER

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.

Ουσιαστικά, 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 προέρχονται από άλλα περιφερικά πληροφοριακά συστήματα.

3.3 ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΚΩΔΙΚΩΝ ΠΡΟΣΒΑΣΗΣ MYPASSWORD

Η εφαρμογή αυτή χρησιμοποιείται για τη διαχείριση και ανάκτηση των κωδικών πρόσβασης και πολιτικών για χρήστες σε υπηρεσίες καταλόγου. Η υπηρεσία απευθύνεται στο σύνολο των εγγεγραμμένων χρηστών, στην υπηρεσία καταλόγου του ιδρύματος, τόσο στους καθηγητές , όσο και στο προσωπικό του ιδρύματος.

Κύριος στόχος της υπηρεσίας θεωρείται αφενός η αυτοματοποίηση της διαδικασίας ανάκτησης κωδικού για τους παραπάνω χρήστες, χρησιμοποιώντας εναλλακτικά κανάλια επικοινωνίας, αφετέρου η εύκολη δημιουργία και εφαρμογή πολιτικών για τους κωδικούς που επιλέγονται. Το σύστημα, μέσω της αυτοματοποίησης των παραπάνω διαδικασιών έχει σαν στόχο την αποφόρτιση των αιτημάτων προς το ανθρώπινο δυναμικό, αλλά και την επιτάχυνση της εξυπηρέτησης κάθε ανάγκης χρηστών, τέτοιας κατηγορίας.

Η παροχή της υπηρεσίας γίνεται αυτόματα σε όλους τους χρήστες που είναι εγγεγραμμένοι σε ένα ίδρυμα χωρίς την ανάγκη κάποιας ενεργοποίησης εκ μέρους τους αλλά απαιτεί την ύπαρξη δευτερευόντων στοιχείων επικοινωνίας. Αυτά τα στοιχεία εισάγονται μαζικά στο σύστημα καταλόγου ή σε δεύτερο χρόνο από τους ίδιους τους χρήστες.

Η εφαρμογή έχει σαν στόχο δυο μεγάλες κατηγορίες λειτουργιών. Τις λειτουργίες που προορίζονται προς τους **χρήστες** και τις λειτουργίες προς τους **διαχειριστές**.

Στην πρώτη περίπτωση, στους **χρήστες** δίνεται η δυνατότητα για τις παρακάτω διαδικασίες :

- Ανάκτηση κωδικού με χρήση email.
- Ανάκτηση κωδικού με χρήση sms.
- Εισαγωγή δευτερευόντων στοιχείων επικοινωνίας
- Αλλαγή κωδικού.

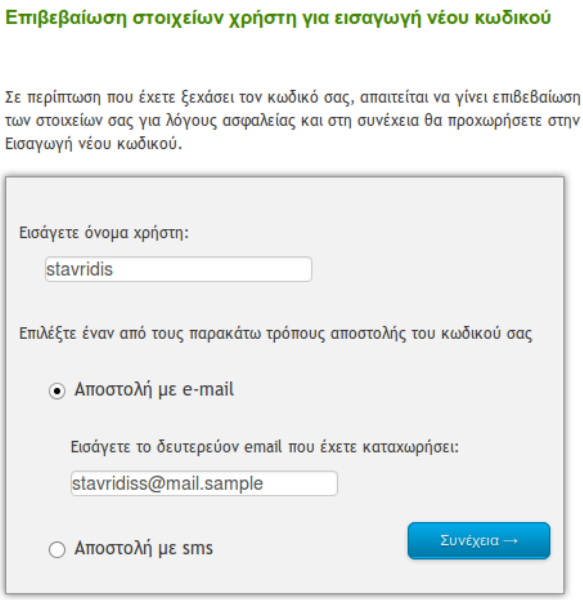
Στους **διαχειριστές** το πλήθος των λειτουργιών είναι πιο εκτεταμένο. Συγκεκριμένα οι λειτουργίες που ορίστηκαν σαν αναγκαίες είναι.

- Απεικόνιση λίστας χαρακτηριστικών χρηστών
- Αναφορά προβλημάτων
- Προβολή διαχειριστών
- Επιβολή πολιτικής σε χρήστες
- Αναζήτηση χρηστών και προχωρημένη αναζήτηση με βάση φίλτρα ldap
- Προβολή πολιτικών κωδικών και δημιουργία νέων
- Προβολή πληροφοριών χρήστη και αλλαγή κωδικού

Με την εγκατάσταση της εφαρμογής, οι διαχειριστές του Ιδρύματος μπορούν να παρέχουν πλέον τις ακόλουθες υπηρεσίες.

3.3.1 Ανάκτηση κωδικού

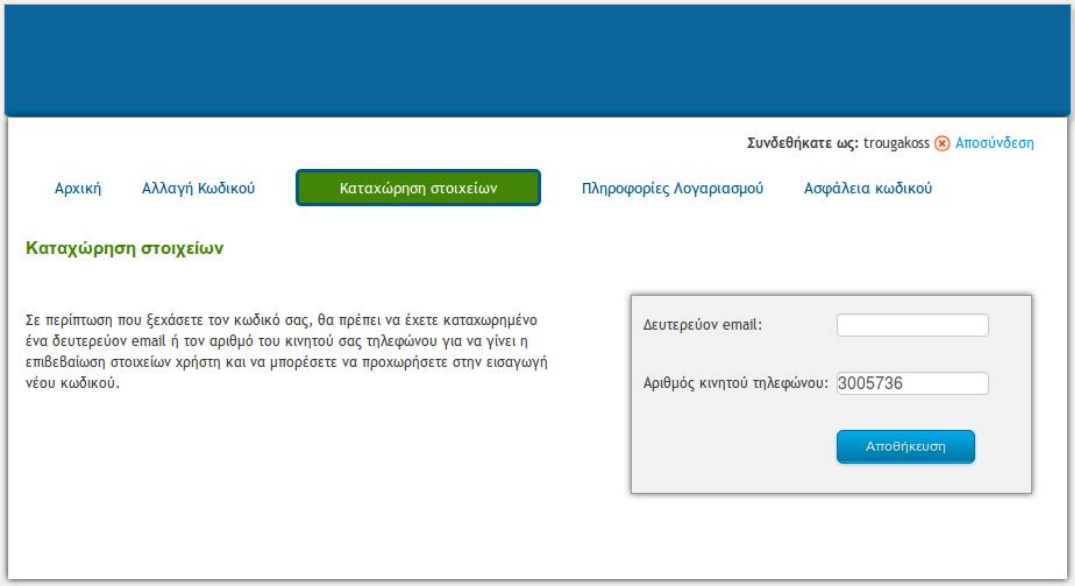
Η λειτουργία ανάκτησης κωδικού αποτελεί την βασικότερη παροχή στους χρήστες της υπηρεσίας. Οι χρήστες έχοντας ήδη εγγραφεί στην υπηρεσία καταλόγου, παρακινούνται να συμπληρώσουν δευτερεύοντα στοιχεία επικοινωνίας. Τα απαραίτητα στοιχεία στην παρούσα φάση είναι είτε μια δευτερεύουσα διεύθυνση email, είτε αριθμός κινητού τηλεφώνου. Και στις δυο περιπτώσεις τα στοιχεία αυτά χρησιμοποιούνται ώστε να αποσταλεί στον χρήστη μια μοναδική διεύθυνση εισόδου στην υπηρεσία, όπου εκεί δίνεται η δυνατότητα δημιουργίας νέου κωδικού. Σημειώνεται πως και στις δυο περιπτώσεις η αίτηση ξεκινά από τον χρήστη, μέσω της κατάλληλης φόρμας, και το δευτερεύον μέσο επικοινωνίας χρησιμοποιείται για την διασφάλιση της ταυτότητας του χρήστη. Δεν υπάρχει καμιά ουσιαστική διαφοροποίηση στη χρήση email, είτε sms, και ουσιαστικά η επιλογή του επαφίεται στην ευχέρεια του χρήστη της υπηρεσίας.



Σημειώνεται πως ανάλογα με τις επιλογές του διαχειριστή, δίνεται η δυνατότητα ενεργοποίησης ελέγχου captcha για τις αιτήσεις των χρηστών, ενώ η προσθήκη του ελέγχου για επιπλέον στοιχεία του χρήστη είναι μέσα στις υλοποιημένες δυνατότητες της εφαρμογής.

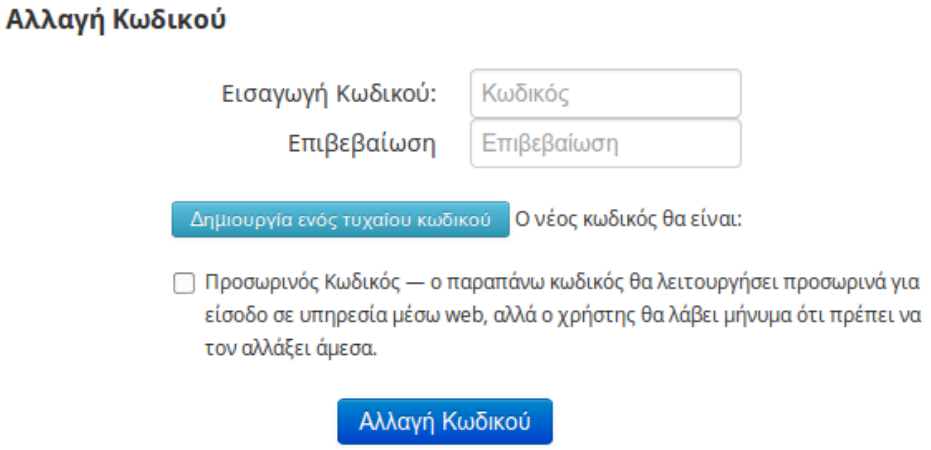
3.3.2 Εισαγωγή δευτερευόντων στοιχείων επικοινωνίας

Για την χρήση της λειτουργίας ανάκτησης/δημιουργίας κωδικού αναφέρθηκε πως είναι απαραίτητη η ύπαρξη στοιχείων επικοινωνίας για τα άτομα. Αυτά τα στοιχεία κατά ένα ποσοστό εισάγονται κατά την εγγραφή του χρήστη στις υπηρεσίες καταλόγου, και εφόσον υπάρχει η έγκριση του ιδίου. Σε περιπτώσεις που τα στοιχεία αυτά δεν είναι διαθέσιμα, είτε έχουν μεταβληθεί, οι χρήστες οφείλουν να τα ενημερώσουν. Αυτό γίνεται με την είσοδο στην υπηρεσία και την επιλογή “καταχώρηση στοιχείων”. Εκεί γίνεται η εισαγωγή των απαραίτητων στοιχείων που θα χρησιμοποιηθούν σε άλλες λειτουργίες.



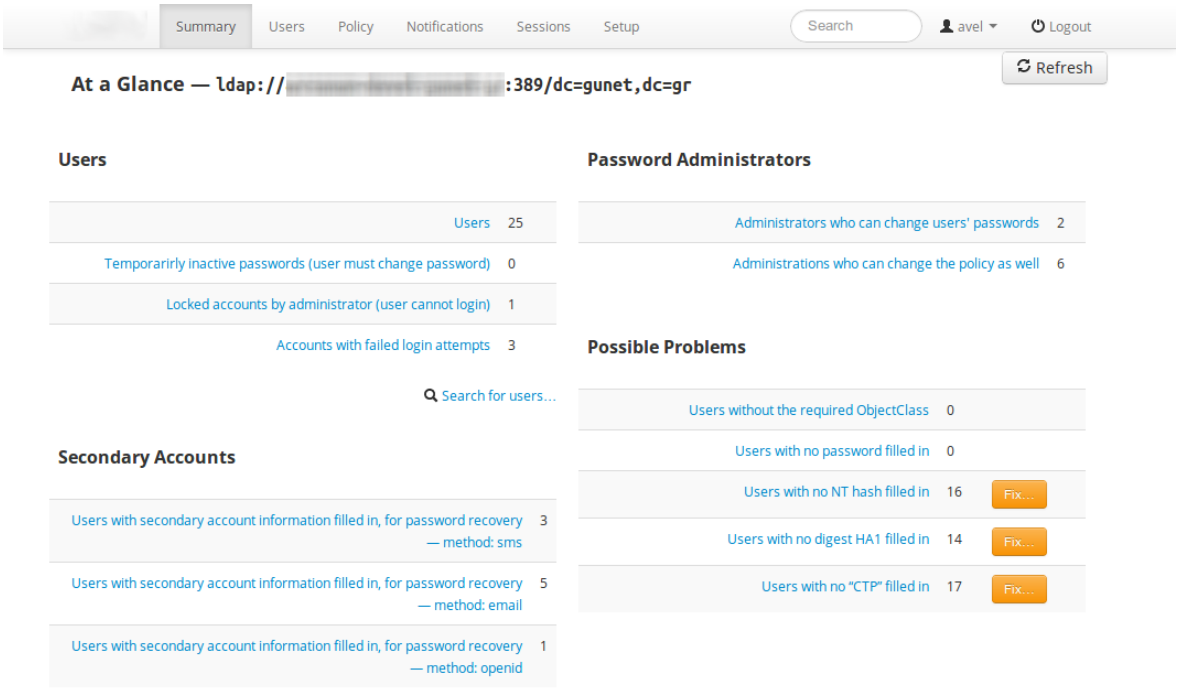
3.3.3 Αλλαγή κωδικού

Στην αλλαγή κωδικού, δίνεται στον χρήστη η δυνατότητα να αλλάξει τον κωδικό που έχει εισαχθεί από αυτόν στο σύστημα. Οι ουσιαστικές διαφοροποιήσεις περιλαμβάνουν τους ελέγχους σχετικά με τις πολιτικές κωδικών, αλλά και με τον τρόπο που μπορεί το σύστημα να ζητήσει την αλλαγή του κωδικού του χρήστη, όταν δεν πληροί πλέον κάποιες από τις προϋποθέσεις των πολιτικών. Κατά τα άλλα ακολουθείται η πάγια τακτική αλλαγής κωδικών.



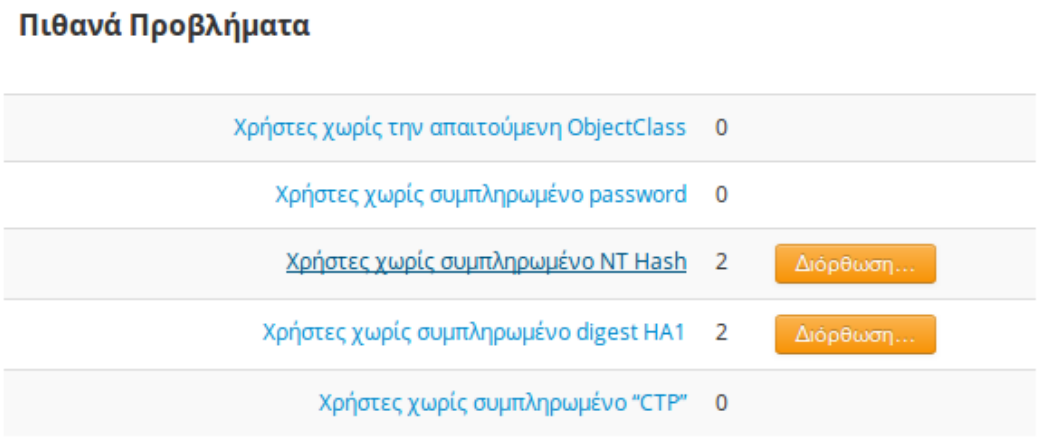
3.3.4 Απεικόνιση λίστας χαρακτηριστικών χρηστών.

Ο χρήστης με δικαιώματα διαχειριστή έχει την δυνατότητα της εποπτικής απεικόνισης των χαρακτηριστικών του συνόλου των δεδομένων της υπηρεσίας καταλόγου. Ουσιαστικά αυτό αποτελεί μια εικόνα της κατάστασης του συστήματος, στην οποία αναλύονται τα κυριότερα στοιχεία που έχουν σημασία για τους διαχειριστές. Αυτά αποτελούνται από μια συνολική εικόνα των χρηστών και μια εικόνα σχετικά με τα δευτερεύοντα στοιχεία επικοινωνίας τους. Επιπλέον δίνονται πληροφορίες σχετικά με το πλήθος και τις κατηγορίες των διαχειριστών. Σε όλες αυτές τις περιπτώσεις διατίθενται λεπτομέρειες, σχετικά με τις επιπλέον πληροφορίες των χρηστών και τα χαρακτηριστικά τους που έχουν σημασία για την εύρυθμη λειτουργία του συστήματος.



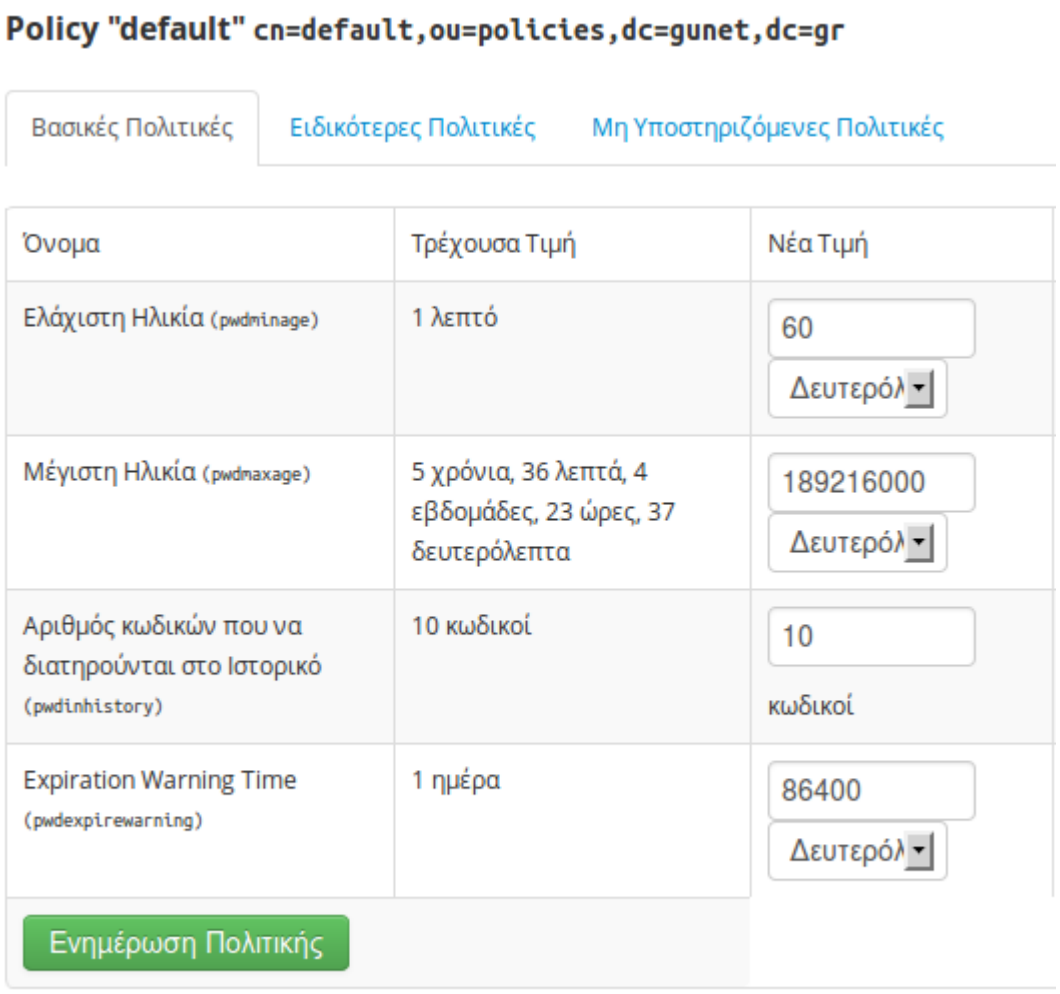
3.3.5 Αναφορά προβλημάτων

Στην συνολική εικόνα της κατάστασης του συστήματος, δίνεται στους διαχειριστές και μια λίστα πιθανών προβλημάτων που μπορούν να προκύψουν στο σύστημα. Αυτά τα προβλήματα συνήθως αναφέρονται σε χρήστες που δεν έχουν τα κατάλληλα στοιχεία, τους κατάλληλους κωδικούς, είτε ακόμα τις απαραίτητες , από το σύστημα, κλάσεις. Σε αυτές τις περιπτώσεις δίνεται δυνατότητα επιδιόρθωσης αυτών των θεμάτων.



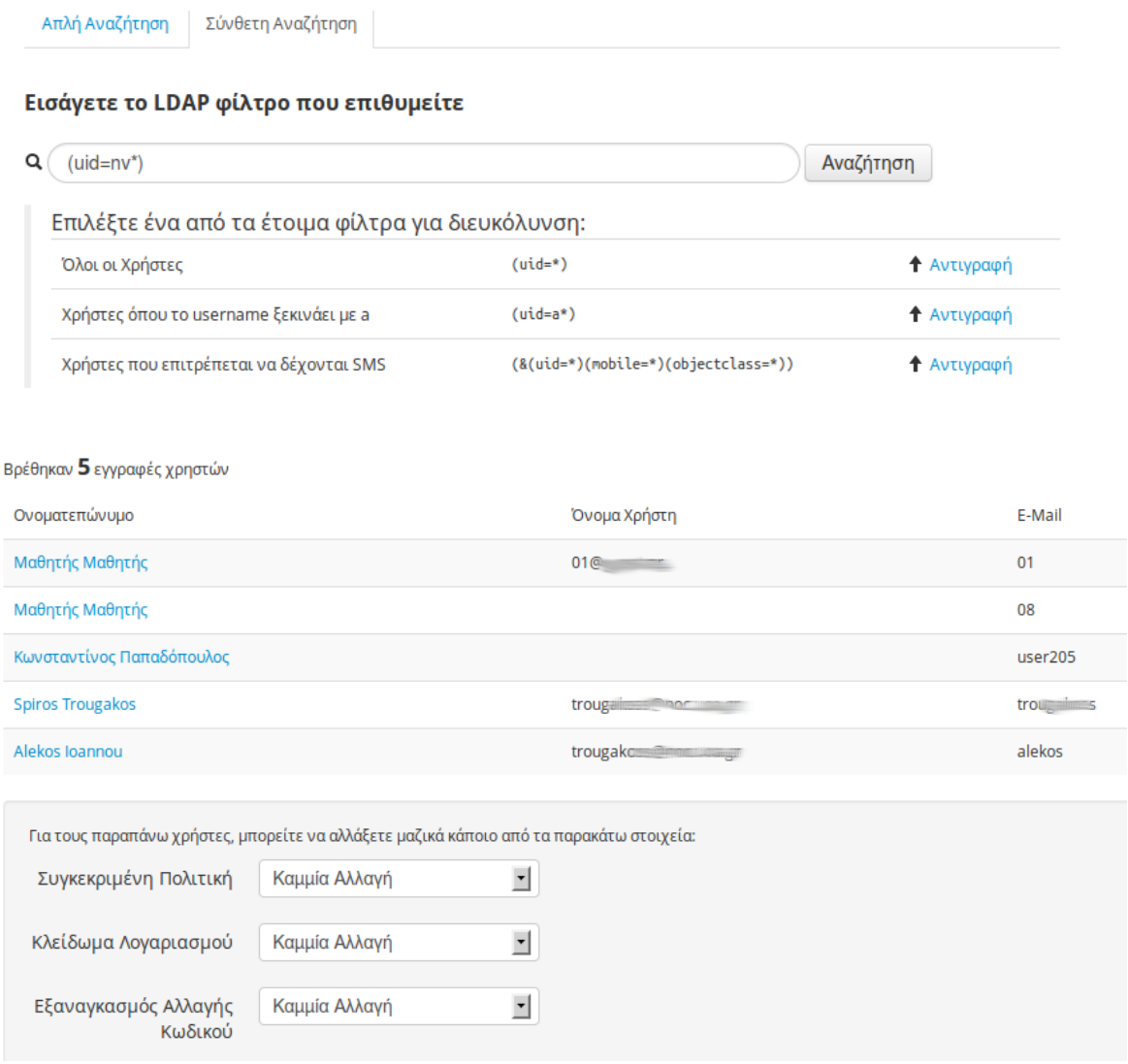
3.3.6 Δημιουργία και επιβολή πολιτικής σε χρήστες

Σε κάθε διαχειριστή δίνεται η δυνατότητα για τη δημιουργία πολλαπλών πολιτικών ασφαλείας για τους κωδικούς που χρησιμοποιούν οι χρήστες. Αυτές οι πολιτικές περιλαμβάνουν επιλογές σχετικά με τη διάρκεια και την πολυπλοκότητα των κωδικών, επιλογές σχετικά με τις αποτυχημένες προσπάθειες εισόδου στο σύστημα καθώς και για τα δικαιώματα των χρηστών πάνω στους κωδικούς τους.



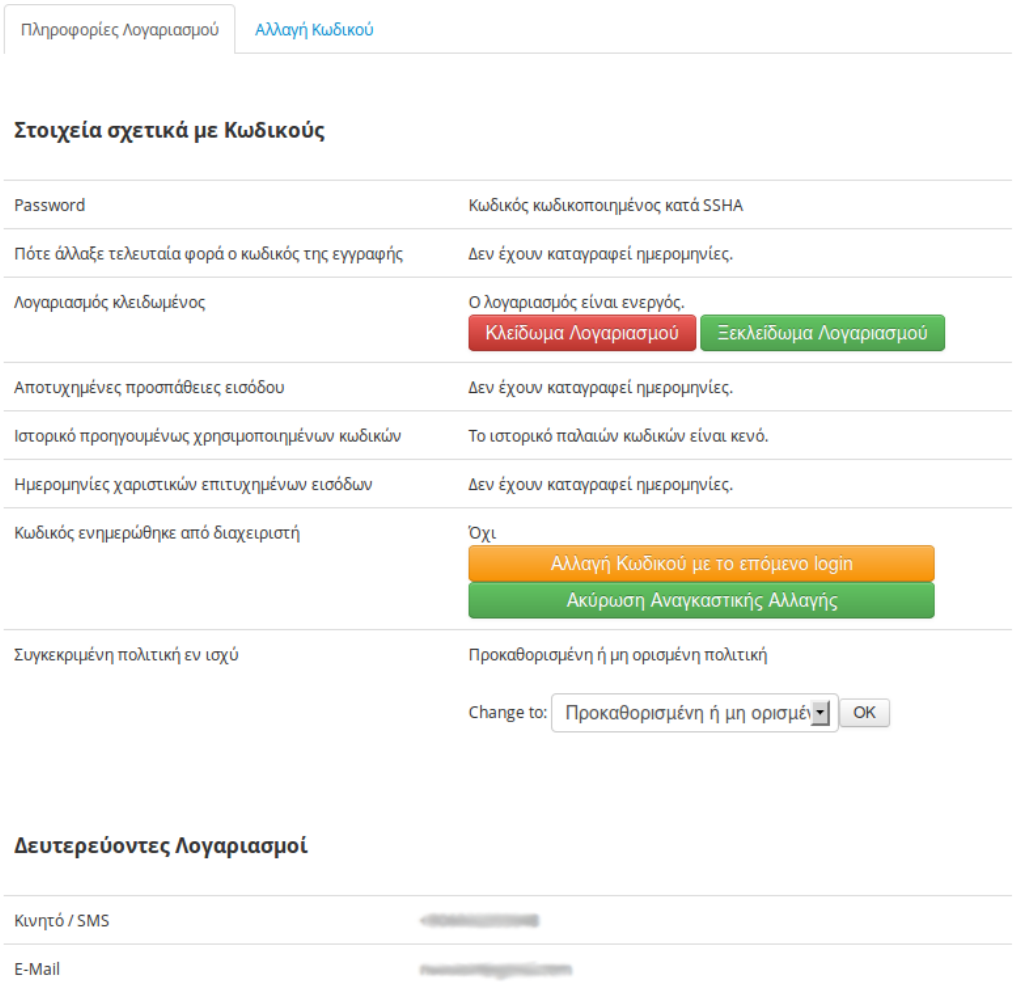
3.3.7 Αναζήτηση χρηστών και προχωρημένη αναζήτηση με βάση φίλτρα LDAP

Κάθε διαχειριστής έχει την δυνατότητα για αναζήτηση χρηστών. Αυτή η αναζήτηση μπορεί να διεκπεραιωθεί πέρα από την απλή χρήση ονομάτων και με την χρήση ldap φίλτρων, δίνοντας έτσι μια απευθείας αντιστοίχιση της εφαρμογής με την υποδομή που βασίζεται. Το αποτέλεσμα της αναζήτησης μπορεί να χρησιμοποιηθεί άμεσα για μια σειρά ενεργειών.



3.3.8 Προβολή πληροφοριών χρήστη και αλλαγή κωδικού

Κάθε εμφάνιση ονομάτων χρηστών στο σύστημα, είτε αποτελεί αποτέλεσμα αναζήτησης, είτε αναφέρεται στην λίστα χρηστών, έχει τη βοηθητική λειτουργία της εμφάνισης πληροφοριών. Οι διαχειριστές πέρα από την προβολή πληροφοριών έχουν την δυνατότητα ενεργειών πάνω στον λογαριασμό του χρήστη, αλλά και να ορίσουν υποχρεωτικές ενέργειες από πλευράς του χρήστη στην επόμενη είσοδό του.


Πληροφορίες Λογαριασμού
Αλλαγή Κωδικού
Στοιχεία σχετικά με Κωδικούς
Password
Κωδικός κωδικοποιημένος κατά SSHA
Πότε άλλαξε τελευταία φορά ο κωδικός της εγγραφής
Δεν έχουν καταγραφεί ημερομηνίες.
Λογαριασμός κλειδωμένος
Ο λογαριασμός είναι ενεργός.
Κλείδωμα Λογαριασμού
Ξεκλείδωμα Λογαριασμού
Αποτυχημένες προσπάθειες εισόδου
Δεν έχουν καταγραφεί ημερομηνίες.
Ιστορικό προηγουμένως χρησιμοποιημένων κωδικών
Το ιστορικό παλαιών κωδικών είναι κενό.
Ημερομηνίες χαριστικών επιτυχημένων εισόδων
Δεν έχουν καταγραφεί ημερομηνίες.
Κωδικός ενημερώθηκε από διαχειριστή
Όχι
Αλλαγή Κωδικού με το επόμενο login
Ακύρωση Αναγκαστικής Αλλαγής
Συγκεκριμένη πολιτική εν ισχύ
Προκαθορισμένη ή μη ορισμένη πολιτική
Change to:
Προκαθορισμένη ή μη ορισμέν
OK
Δευτερεύοντες Λογαριασμοί
Κινητό / SMS
E-Mail

4. ΠΑΡΑΡΤΗΜΑ 1 – ΠΑΡΟΥΣΙΟΛΟΓΙΑ ΔΡΑΣΕΩΝ ΕΚΠΑΙΔΕΥΣΗΣ

Στις δράσεις εκπαίδευσης που πραγματοποιήθηκαν χρησιμοποιήθηκε ένα πλήθος υπεύθυνων, τα ονόματα των οποίων παρουσιάζονται στον πίνακα που ακολουθεί.

Ονοματεπώνυμο εκπαιδευτών
Ζήσης Παλάσκας
Ιωάννης Κουρούπης
Παναγιώτης Κολυβάς
Νικόλαος Βουτσινάς
Αλέξανδρος Παναγόπουλος
Σταμάτης Στέφανος

Ακολούθως, παρουσιάζονται με συνοπτικό τρόπο πληροφορίες σχετικά με τις εκπαιδεύσεις που πραγματοποιήθηκαν, όπως για παράδειγμα το πότε διενεργήθηκαν, ποιο ήταν το περιεχόμενο τους και ποιοι συμμετείχαν.

Ημερομηνία εκπαίδευσης	5/2/2015
Περιεχόμενο εκπαίδευσης	Τεχνολογίες κεντρικής πιστοποίησης χρηστών για την ασφαλή είσοδό τους σε διιδρυματικές εφαρμογές
Τοποθεσία εκπαίδευσης	ΕΔΕΤ Α.Ε. (Τηλεδιάσκεψη)
Ονοματεπώνυμο συμμετεχόντων	Τηλέμαχος Σταμκόπουλος
	Παναγιώτης Βουτσκίδης
	Σάκης Κοτσαμανίδης
	Χριστίνα Αυγερινού
	Ανδρέας Σορτ
	Ζαχαρένια Γαροφαλάκη
	Νικόλαος Κασαπίδης
	Ιωάννης Θωίδης

	Ιωάννης Αλεξιάδης
	Αναστάσιος Ορφανίδης

Ημερομηνία εκπαίδευσης	6/2/2015
Περιεχόμενο εκπαίδευσης	Τεχνολογίες κεντρικής πιστοποίησης χρηστών για την ασφαλή είσοδό τους σε διιδρυματικές εφαρμογές
Τοποθεσία εκπαίδευσης	ΕΔΕΤ Α.Ε. (Τηλεδιάσκεψη)
Ονοματεπώνυμο συμμετεχόντων	Θεόδωρος Σαρικούδης
	Παναγιώτης Ιλαρίδης
	Αλέξανδρος Χαλκιόπουλος
	Βαγγέλης Γογγολίδης
	Αναστάσιος Φιλέλης
	Γεώργιος Χρυσολοράς
	Καλλιόπη Σωτηροπούλου

Ημερομηνία εκπαίδευσης	10/2/2015
Περιεχόμενο εκπαίδευσης	Τεχνολογίες κεντρικής πιστοποίησης χρηστών για την ασφαλή είσοδό τους σε διιδρυματικές εφαρμογές
Τοποθεσία εκπαίδευσης	ΕΔΕΤ Α.Ε. (Τηλεδιάσκεψη)
Ονοματεπώνυμο συμμετεχόντων	Ιωάννης Φενέρης
	Βασίλης Λούπας
	Παναγιώτης Αρφάνης
	Κυριάκος Ζερβουδάκης

Ημερομηνία	12/2/2015

εκπαίδευσης	
Περιεχόμενο εκπαίδευσης	Τεχνολογίες κεντρικής πιστοποίησης χρηστών για την ασφαλή είσοδό τους σε διιδρυματικές εφαρμογές
Τοποθεσία εκπαίδευσης	ΕΔΕΤ Α.Ε. (Τηλεδιάσκεψη)
Ονοματεπώνυμο συμμετεχόντων	Νικόλαος Μήλας
	Στέφανος Καρασαββίδης
	Ηλίας Τσιότσιας
	Κώστας Πλαχούρας
	Δημήτρης Βασιλειάδης
	Εμμανουήλ Δερμιτζάκης
	Χρήστος Πρασσάς
	Μαρία Σταυρουλάκη
	Κυριάκος Πούτος
	Ταξιάρχης Τσαπάρας

Ημερομηνία εκπαίδευσης	13/2/2015
Περιεχόμενο εκπαίδευσης	Τεχνολογίες κεντρικής πιστοποίησης χρηστών για την ασφαλή είσοδό τους σε διιδρυματικές εφαρμογές
Τοποθεσία εκπαίδευσης	ΕΔΕΤ Α.Ε. (Τηλεδιάσκεψη)
Ονοματεπώνυμο συμμετεχόντων	Χρήστος Πρασσάς
	Ελένη Στάθη
	Νικόλαος Νταλιακούρας

Ημερομηνία εκπαίδευσης	19/2/2015
Περιεχόμενο εκπαίδευσης	Παρουσίαση αρχιτεκτονικής σχήματος Καταλόγου και υποστηρικτικών υπηρεσιών του

	Θέματα διαλειτουργικότητας
Τοποθεσία εκπαίδευσης	ΕΔΕΤ ΑΕ
Ονοματεπώνυμο συμμετεχόντων	Κωνσταντίνος Γραμματικός
	Ιωάννης Κακαβάς
	Ζήνωνας Μούσμουλας
	Ιωάννης Μητσός

Ημερομηνία εκπαίδευσης	26/3/2015
Περιεχόμενο εκπαίδευσης	Θέματα Μετάβασης Θέματα διαλειτουργικότητας Θέματα IDM Security
Τοποθεσία εκπαίδευσης	Οικονομικό Πανεπιστήμιο Αθηνών
Ονοματεπώνυμο συμμετεχόντων	Γεώργιος Πολύζος
	Ηλίας Σιδέρης
	Μανώλης Ψυλλάκης
	Γεώργιος Αλεξανδρής

Ημερομηνία εκπαίδευσης	30/4/2015
Περιεχόμενο εκπαίδευσης	Θέματα Μετάβασης Θέματα διαλειτουργικότητας Θέματα IDM Security
Τοποθεσία εκπαίδευσης	Πανεπιστήμιο Κρήτης (Τηλεδιάσκεψη)
Ονοματεπώνυμο συμμετεχόντων	Μαρία Τσιμπιτά
	Ιωάννης Φραγκιαδάκης
	Μανώλης Ψυλλάκης

	Ηλίας Σιδέρης
	Άκης Χουρδάκης
	Νίκος Παναγιωτάκης
	Νίκος Ορφανουδάκης
	Αλέξανδρος Τσακουντάκης
	Νίκος Καπελώνης
	Μιχάλης Καλογήρου

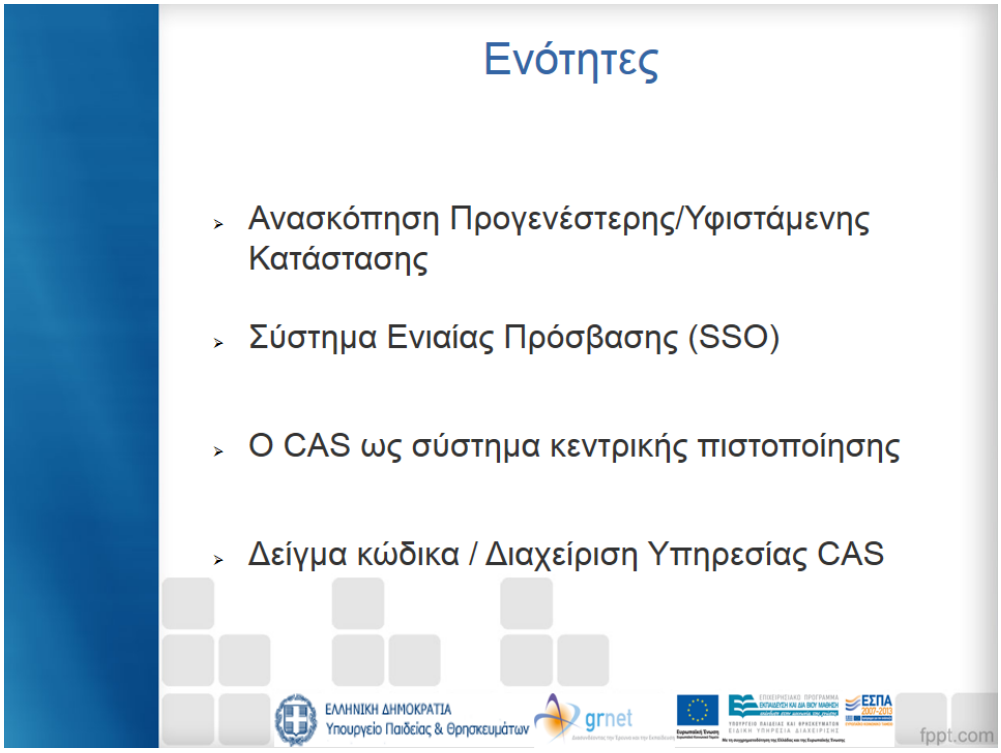
Ημερομηνία εκπαίδευσης	5/6/2015
Περιεχόμενο εκπαίδευσης	Θέματα Μετάβασης Θέματα διαλειτουργικότητας Θέματα IDM Security Θέματα Διαχείρισης Καταλόγων HandsOn και Demos (στα live)
Τοποθεσία εκπαίδευσης	Πανεπιστήμιο Πειραιώς
Ονοματεπώνυμο συμμετεχόντων	Ιωάννης Σμυρλής
	Ταξιάρχης Τσαπάρας
	Κυριάκος Πούτος
	Μαρία Σταυρουλάκη
	Νίκος Αβραντινής
	Άρης Σάκο
	Χρήστος Μανουσόπουλος

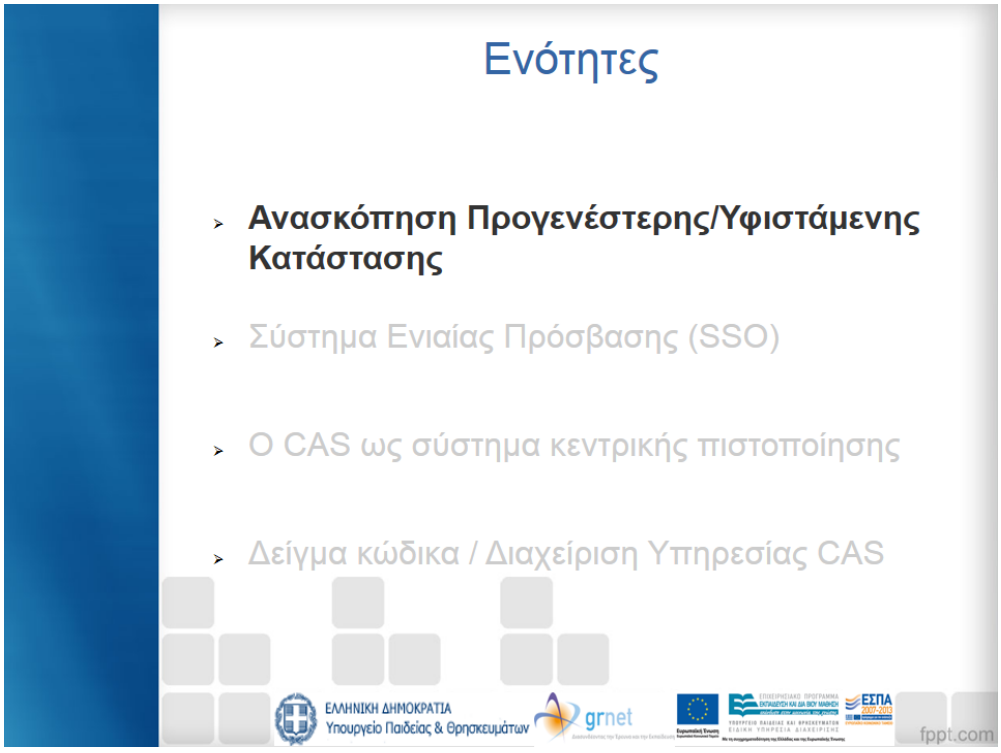
Ημερομηνία εκπαίδευσης	12/6/2015
Περιεχόμενο εκπαίδευσης	Θέματα Μετάβασης Θέματα διαλειτουργικότητας Θέματα IDM Security Θέματα Διαχείρισης Καταλόγων

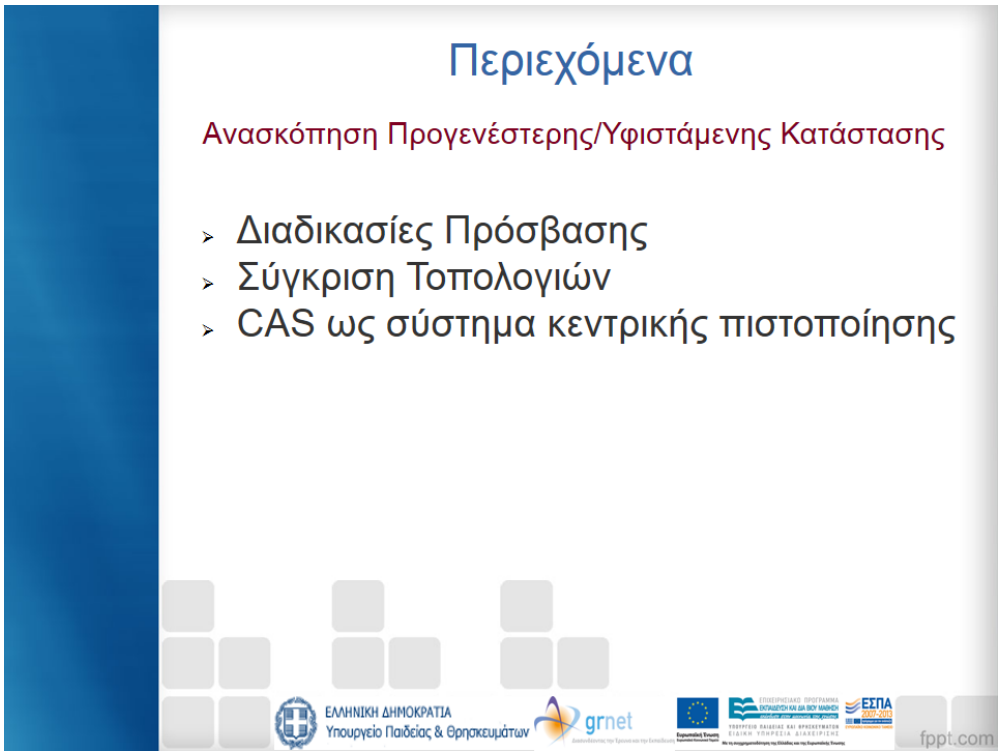
	HandsOn και Demos (στα live)
Τοποθεσία εκπαίδευσης	ΤΕΙ Πειραιά
Ονοματεπώνυμο συμμετεχόντων	Λευτέρης Μπλέτσας
	Ανδρέας Σορτ
	Εύη Αγγελή
	Διονύσιος Χριστόπουλος

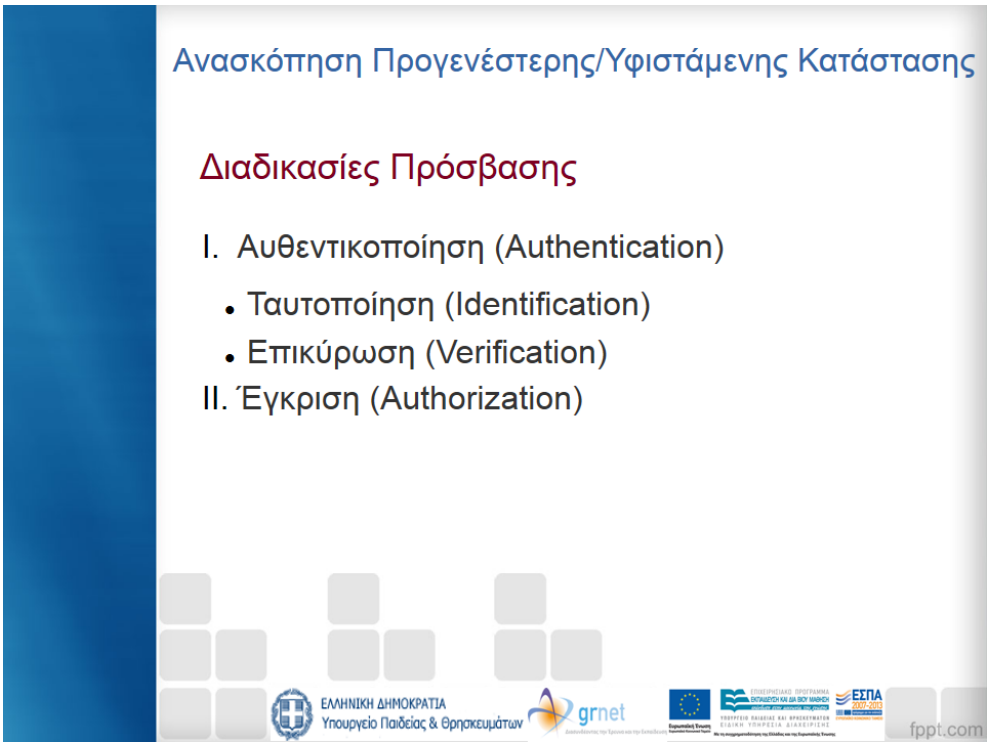
Ημερομηνία εκπαίδευσης	7/7/2015
Περιεχόμενο εκπαίδευσης	Θέματα Διαχείρισης Καταλόγων HandsOn και Demos (στα live)
Τοποθεσία εκπαίδευσης	Οικονομικό Πανεπιστήμιο Αθηνών
Ονοματεπώνυμο συμμετεχόντων	Μανώλης Ψυλλάκης
	Θεόδωρος Ντούσκας
	Γεώργιος Αλεξανδρής
	Μιχάλης Καλογήρου

5. Παραρτημα 2 – Παρουσιαση σχετικα με τις τεχνολογιες υλοποιησης και ασφαλης χρησης του καταλογου ενοποιημενης προσβασης και τα πλεονεκτηματα χρησης του


Ενότητες
Ανασκόπηση Προγενέστερης/Υφιστάμενης Κατάστασης
Σύστημα Ενιαίας Πρόσβασης (SSO)
Ο CAS ως σύστημα κεντρικής πιστοποίησης
Δείγμα κώδικα / Διαχείριση Υπηρεσίας CAS
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας & Θρησκευμάτων
grnet
fppt.com

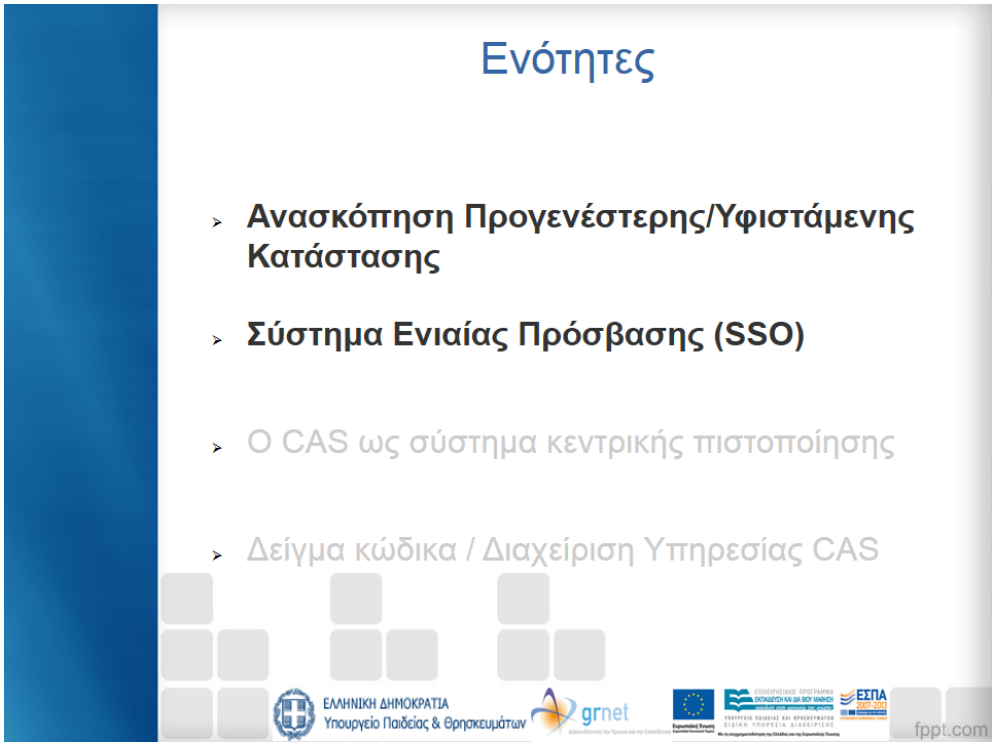

Ενότητες
Ανασκόπηση Προγενέστερης/Υφιστάμενης Κατάστασης
Σύστημα Ενιαίας Πρόσβασης (SSO)
Ο CAS ως σύστημα κεντρικής πιστοποίησης
Δείγμα κώδικα / Διαχείριση Υπηρεσίας CAS
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας & Θρησκευμάτων
grnet
fppt.com

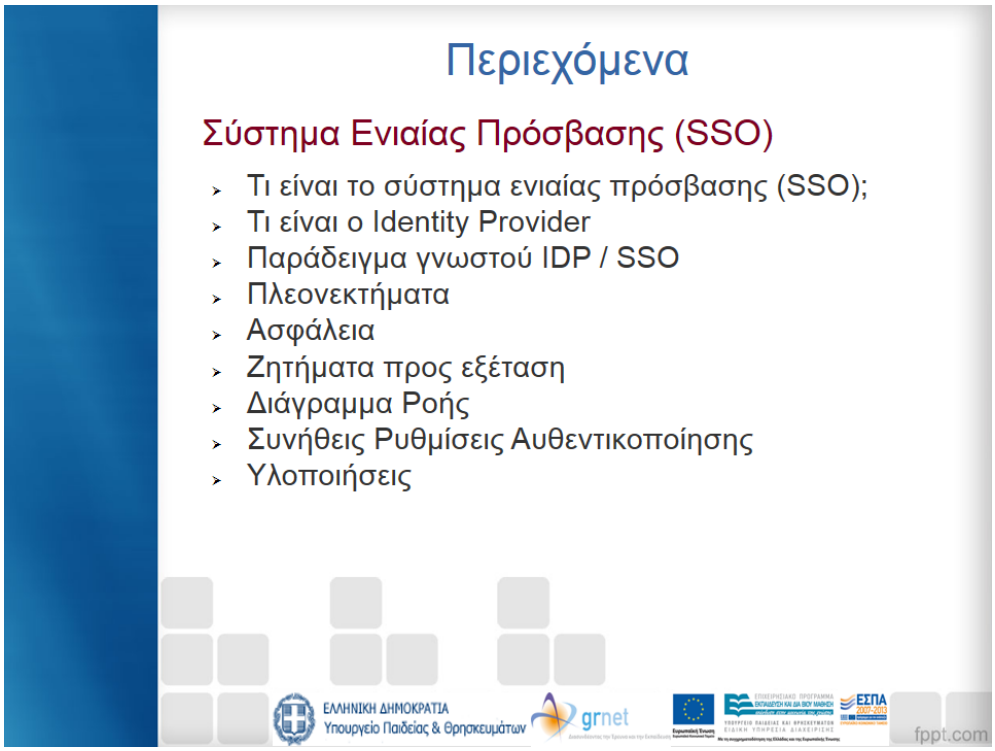

Περιεχόμενα
Ανασκόπηση Προγενέστερης/Υφιστάμενης Κατάστασης
Διαδικασίες Πρόσβασης
Σύγκριση Τοπολογιών
CAS ως σύστημα κεντρικής πιστοποίησης
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας & Θρησκευμάτων
grnet
ΕΣΠΑ 2007-2013
fppt.com

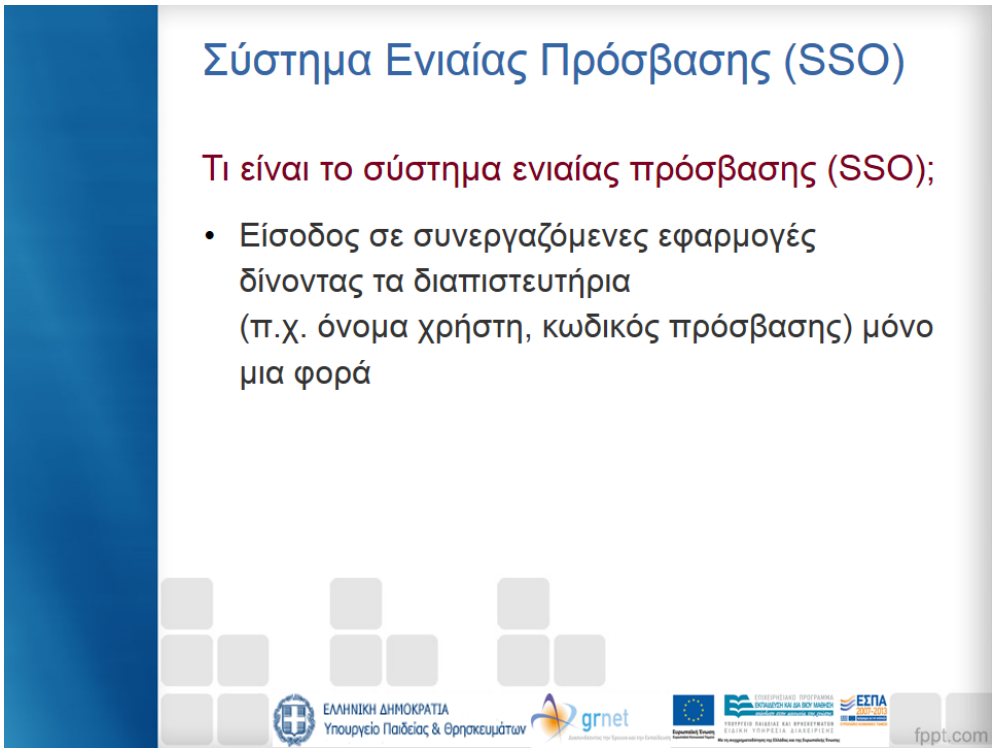

Ανασκόπηση Προγενέστερης/Υφιστάμενης Κατάστασης
Διαδικασίες Πρόσβασης
I. Αυθεντικοποίηση (Authentication)
Ταυτοποίηση (Identification)
Επικύρωση (Verification)
II. Έγκριση (Authorization)
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας & Θρησκευμάτων
grnet
ΕΣΠΑ 2007-2013
fppt.com


Ανασκόπηση Προγενέστερης/Υφιστάμενης Κατάστασης
Σύγκριση Τοπολογιών
Απλή Πιστοποίηση (πολλά user repositories)
Απλή Πιστοποίηση (κεντρικό user repository)
Πιστοποίηση μέσω SSO
Web App 1
Web App 2
Ldap
Client
SSO
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας & Θρησκευμάτων
grnet
fppt.com


Ανασκόπηση Προγενέστερης/Υφιστάμενης Κατάστασης
CAS ως σύστημα κεντρικής πιστοποίησης
LDAP
RDBMS
Kerberos
Server
cas-server-1
cas-server-2
cas-server-3
Protocol
CAS v2
CAS v2
CAS v1
SAML 1.1
SAML 1.1
Clients
Google
Java Apps
PHP Apps
Apache
.NET Apps
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας & Θρησκευμάτων
grnet
fppt.com

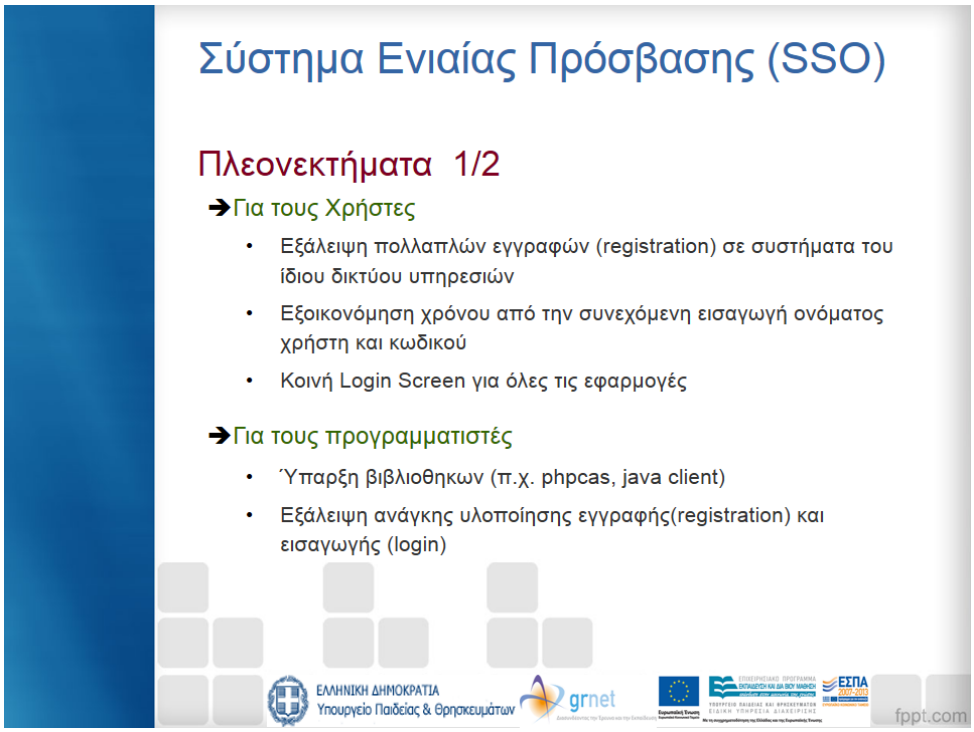

Ενότητες
Ανασκόπηση Προγενέστερης/Υφιστάμενης Κατάστασης
Σύστημα Ενιαίας Πρόσβασης (SSO)
Ο CAS ως σύστημα κεντρικής πιστοποίησης
Δείγμα κώδικα / Διαχείριση Υπηρεσίας CAS
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας & Θρησκευμάτων
grnet
fppt.com

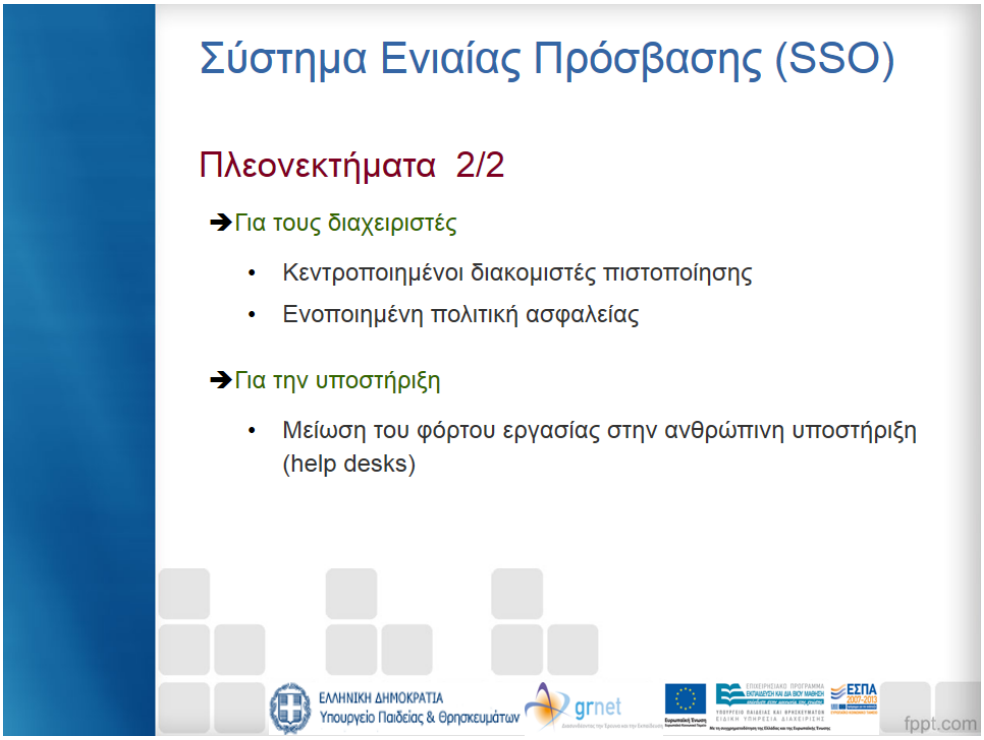

Περιεχόμενα
Σύστημα Ενιαίας Πρόσβασης (SSO)
Τι είναι το σύστημα ενιαίας πρόσβασης (SSO);
Τι είναι ο Identity Provider
Παράδειγμα γνωστού IDP / SSO
Πλεονεκτήματα
Ασφάλεια
Ζητήματα προς εξέταση
Διάγραμμα Ροής
Συνήθεις Ρυθμίσεις Αυθεντικοποίησης
Υλοποιήσεις
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας & Θρησκευμάτων
grnet
fppt.com

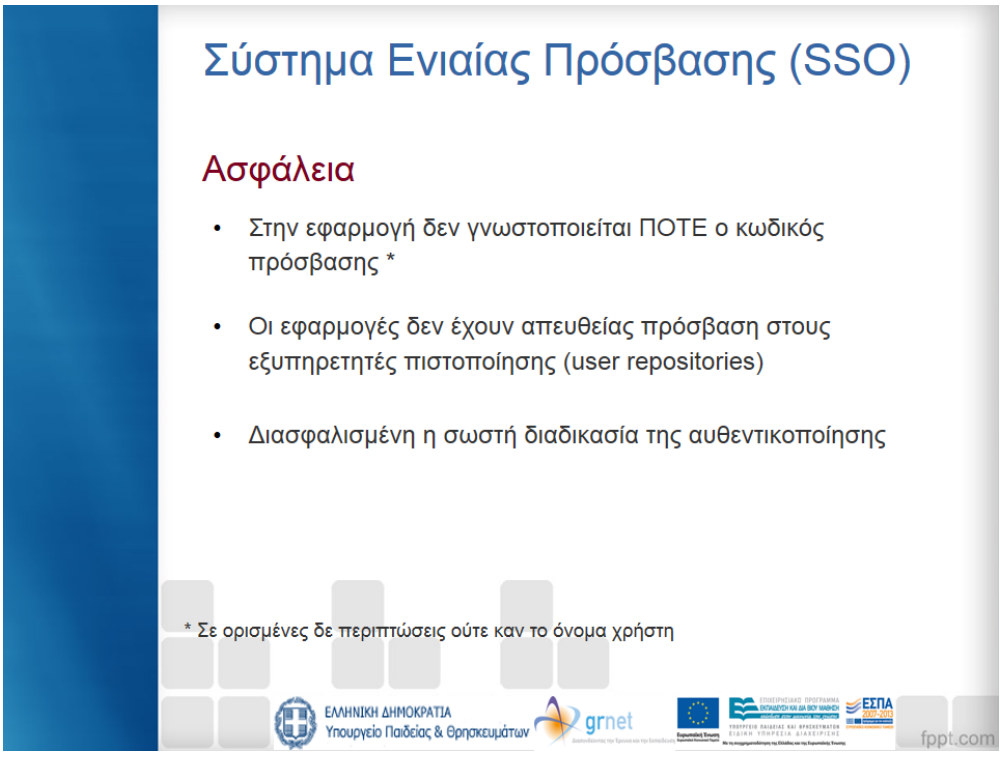

Σύστημα Ενιαίας Πρόσβασης (SSO)
Τι είναι το σύστημα ενιαίας πρόσβασης (SSO);
• Είσοδος σε συνεργαζόμενες εφαρμογές δίνοντας τα διαπιστευτήρια (π.χ. όνομα χρήστη, κωδικός πρόσβασης) μόνο μια φορά
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας & Θρησκευμάτων
grnet
fppt.com

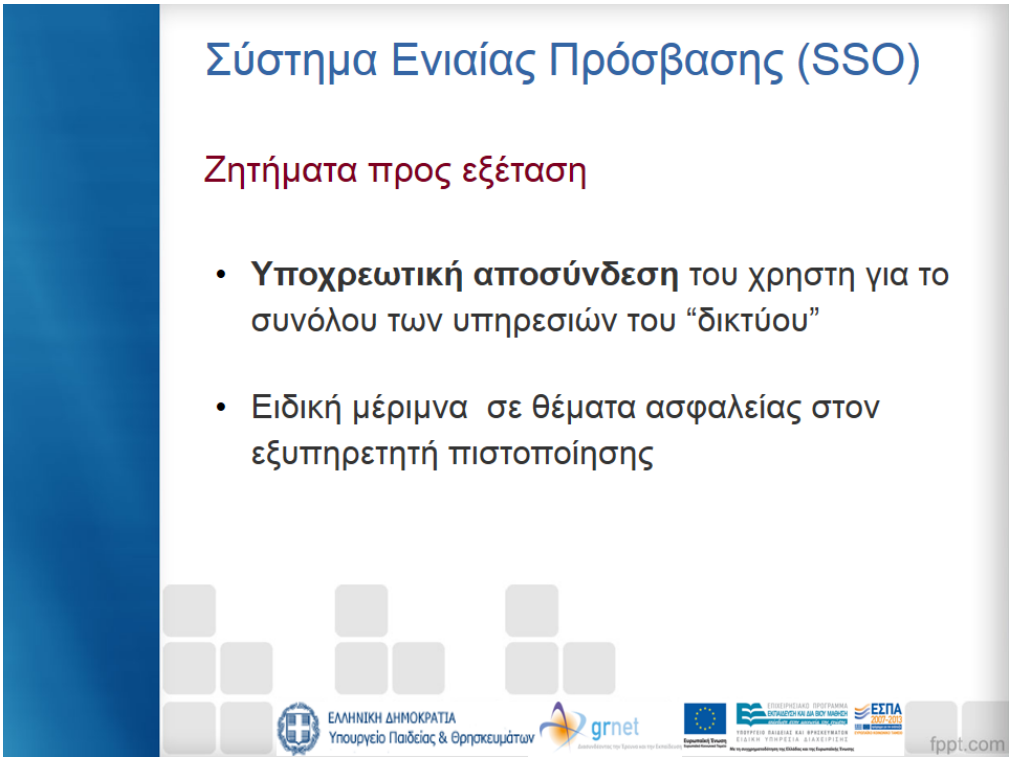

Σύστημα Ενιαίας Πρόσβασης (SSO)
Τι είναι ο Identity Provider
• Παρέχει υπηρεσίες πιστοποίησης των διαπιστευτηρίων ενός χρήστη
• Εξυπηρετεί τρίτους παρόχους υπηρεσιών (Service Providers SPs).
• Παρέχει πληροφορίες σχετικά με τον χρήστη που πιστοποιήθηκε.
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας & Θρησκευμάτων
grnet
fppt.com

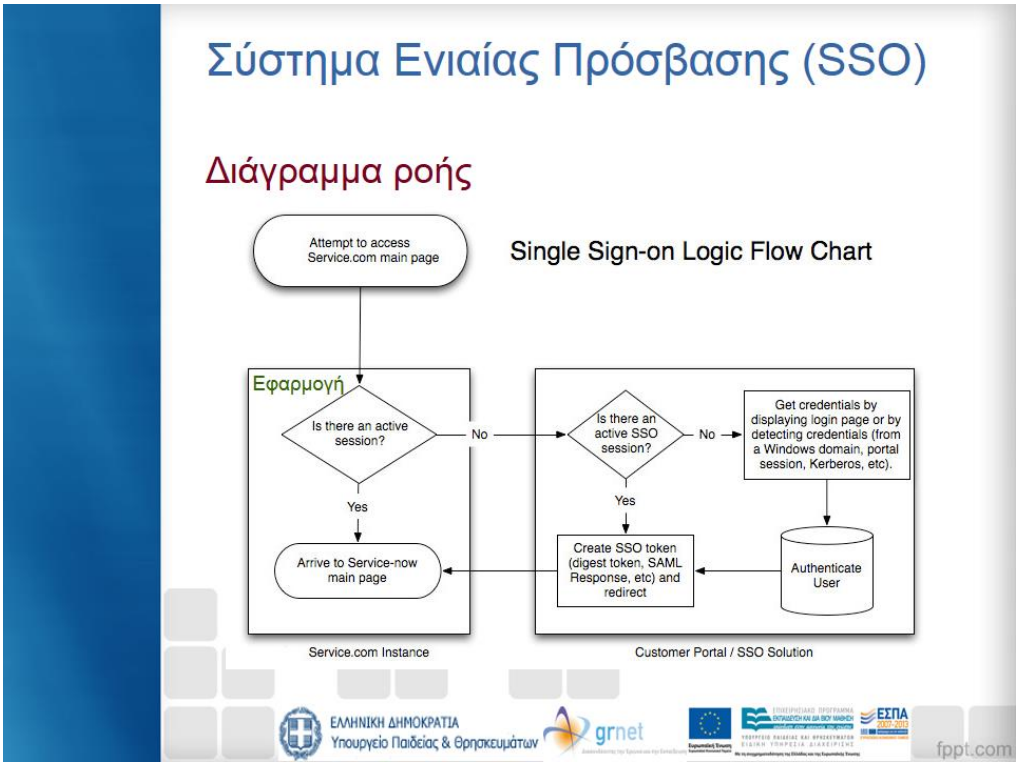

Σύστημα Ενιαίας Πρόσβασης (SSO)
Παράδειγμα γνωστού IDP / SSO
Παράδειγμα ενός παρόχου ταυτότητας που υποστηρίζει το SSO είναι η Google με τα Google Apps.
Ένας χρήστης, εισάγει μόνο μια μόνο φορά τα στοιχεία εισόδου του και έχει πρόσβαση σε πολλές εφαρμογές (mail, google drive κτλ).
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας & Θρησκευμάτων
grnet
ΕΣΠΑ 2007-2013
fppt.com


Σύστημα Ενιαίας Πρόσβασης (SSO)
Πλεονεκτήματα 1/2
➔Για τους Χρήστες
• Εξάλειψη πολλαπλών εγγραφών (registration) σε συστήματα του ίδιου δικτύου υπηρεσιών
• Εξοικονόμηση χρόνου από την συνεχόμενη εισαγωγή ονόματος χρήστη και κωδικού
• Κοινή Login Screen για όλες τις εφαρμογές
➔Για τους προγραμματιστές
• Ύπαρξη βιβλιοθηκων (π.χ. phpcas, java client)
• Εξάλειψη ανάγκης υλοποίησης εγγραφής(registration) και εισαγωγής (login)
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας & Θρησκευμάτων
grnet
ΕΣΠΑ 2007-2013
fppt.com


Σύστημα Ενιαίας Πρόσβασης (SSO)
Πλεονεκτήματα 2/2
➔Για τους διαχειριστές
• Κεντροποιημένοι διακομιστές πιστοποίησης
• Ενοποιημένη πολιτική ασφαλείας
➔Για την υποστήριξη
• Μείωση του φόρτου εργασίας στην ανθρώπινη υποστήριξη (help desks)
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας & Θρησκευμάτων
grnet
fppt.com

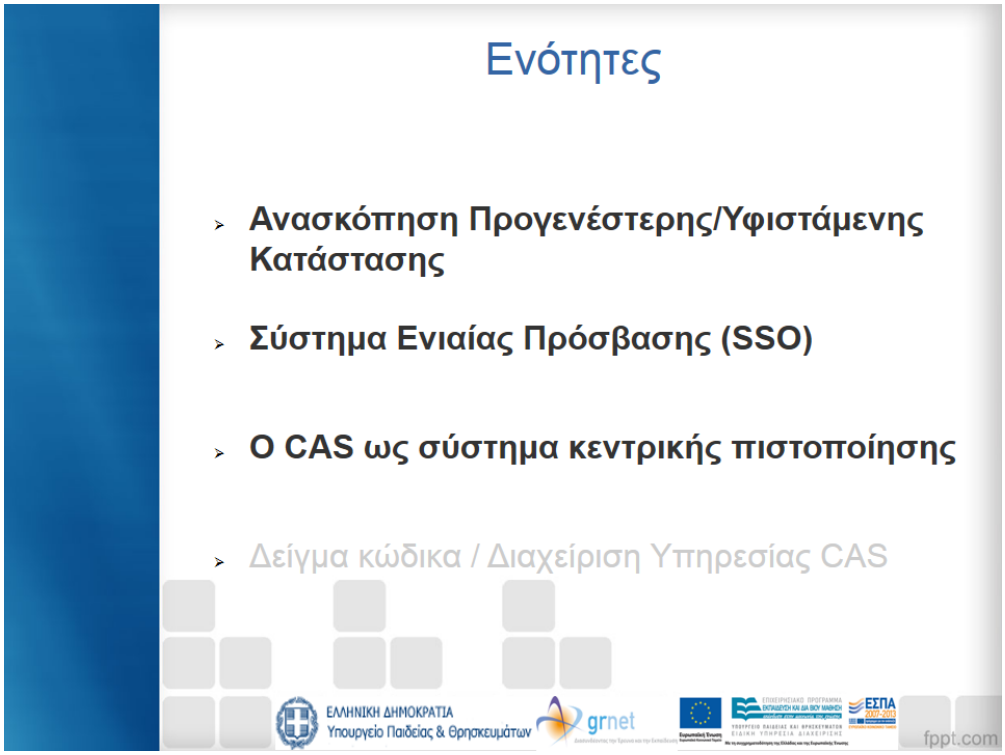

Σύστημα Ενιαίας Πρόσβασης (SSO)
Ασφάλεια
• Στην εφαρμογή δεν γνωστοποιείται ΠΟΤΕ ο κωδικός πρόσβασης *
• Οι εφαρμογές δεν έχουν απευθείας πρόσβαση στους εξυπηρετητές πιστοποίησης (user repositories)
• Διασφαλισμένη η σωστή διαδικασία της αυθεντικοποίησης
* Σε ορισμένες δε περιπτώσεις ούτε καν το όνομα χρήστη
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας & Θρησκευμάτων
grnet
fppt.com

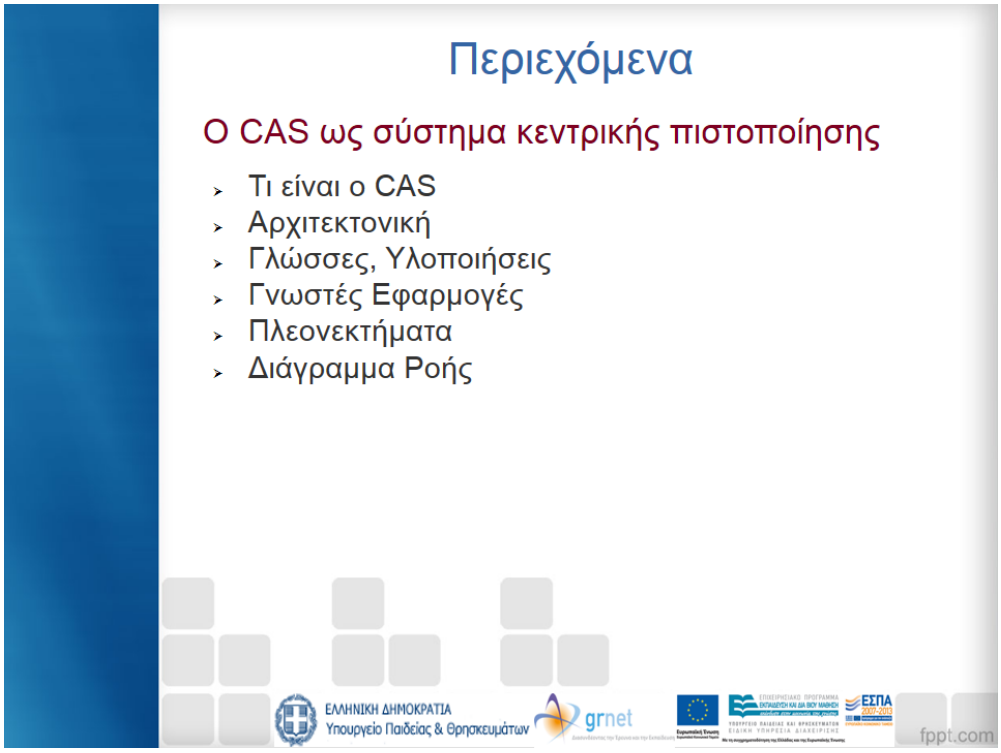

Σύστημα Ενιαίας Πρόσβασης (SSO)
Ζητήματα προς εξέταση
• Υποχρεωτική αποσύνδεση του χρηστη για το συνόλου των υπηρεσιών του “δικτύου”
• Ειδική μέριμνα σε θέματα ασφαλείας στον εξυπηρετητή πιστοποίησης
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας & Θρησκευμάτων
grnet
fppt.com

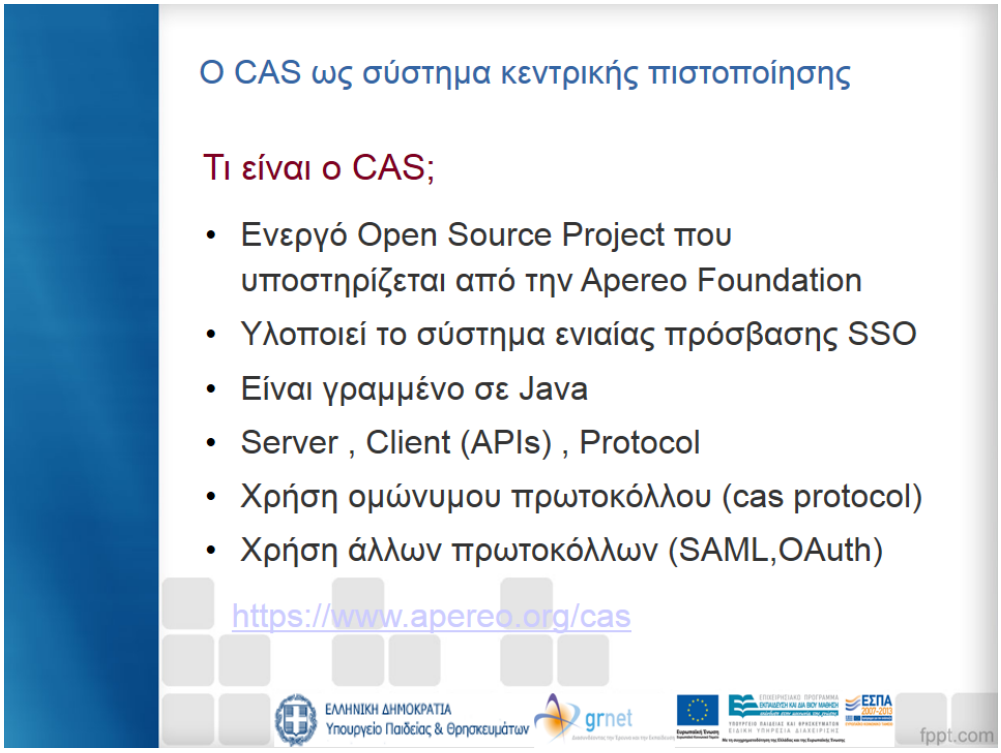

Σύστημα Ενιαίας Πρόσβασης (SSO)
Διάγραμμα ροής
Attempt to access Service.com main page
Single Sign-on Logic Flow Chart
Εφαρμογή
Is there an active session?
No
Yes
Arrive to Service-now main page
Is there an active SSO session?
No
Yes
Get credentials by displaying login page or by detecting credentials (from a Windows domain, portal session, Kerberos, etc).
Create SSO token (digest token, SAML Response, etc) and redirect
Authenticate User
Service.com Instance
Customer Portal / SSO Solution
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας & Θρησκευμάτων
grnet
fppt.com


Σύστημα Ενιαίας Πρόσβασης (SSO)
Συνήθεις Ρυθμίσεις
Συνήθεις τρόποι αυθεντικοποίησης :
➔Login Handlers
• Φόρμα Εισόδου (username/password)
• Kerberos
• Certificate / Smart card / e-token
• Integrated Windows Authentication
* Συνήθως χρησιμοποιείται Ldap Server, ως data source στο backend.
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας & Θρησκευμάτων
grnet
fppt.com


Σύστημα Ενιαίας Πρόσβασης (SSO)
Υλοποιήσεις
CAS
Shibboleth *
Facebook Connect
JBoss SSO
Active Directory Federation Services
HP IceWall SSO
IBM Enterprise Identity Mapping
Microsoft account
* Για ομοσπονδιακές υπηρεσίες (Federation)
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας & Θρησκευμάτων
grnet
fppt.com

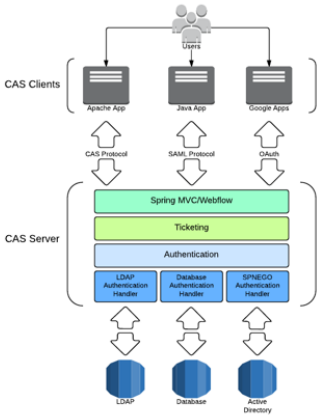

Ενότητες
Ανασκόπηση Προγενέστερης/Υφιστάμενης Κατάστασης
Σύστημα Ενιαίας Πρόσβασης (SSO)
Ο CAS ως σύστημα κεντρικής πιστοποίησης
Δείγμα κώδικα / Διαχείριση Υπηρεσίας CAS
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας & Θρησκευμάτων
grnet
fppt.com


Περιεχόμενα
Ο CAS ως σύστημα κεντρικής πιστοποίησης
Τι είναι ο CAS
Αρχιτεκτονική
Γλώσσες, Υλοποιήσεις
Γνωστές Εφαρμογές
Πλεονεκτήματα
Διάγραμμα Ροής
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας & Θρησκευμάτων
grnet
fppt.com


Ο CAS ως σύστημα κεντρικής πιστοποίησης
Τι είναι ο CAS;
Ενεργό Open Source Project που υποστηρίζεται από την Apereo Foundation
Υλοποιεί το σύστημα ενιαίας πρόσβασης SSO
Είναι γραμμένο σε Java
Server , Client (APIs) , Protocol
Χρήση ομώνυμου πρωτοκόλλου (cas protocol)
Χρήση άλλων πρωτοκόλλων (SAML,OAuth)
https://www.apereo.org/cas
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας & Θρησκευμάτων
grnet
fppt.com

Ο CAS ως σύστημα κεντρικής πιστοποίησης

Αρχιτεκτονική



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας & Θρησκευμάτων
grnet
fppt.com

Ο CAS ως σύστημα κεντρικής πιστοποίησης

Γλώσσες, Υλοποιήσεις

Μερικές από τις πιο γνωστές γλώσσες και υλοποιήσεις βιβλιοθηκών (client libraries)

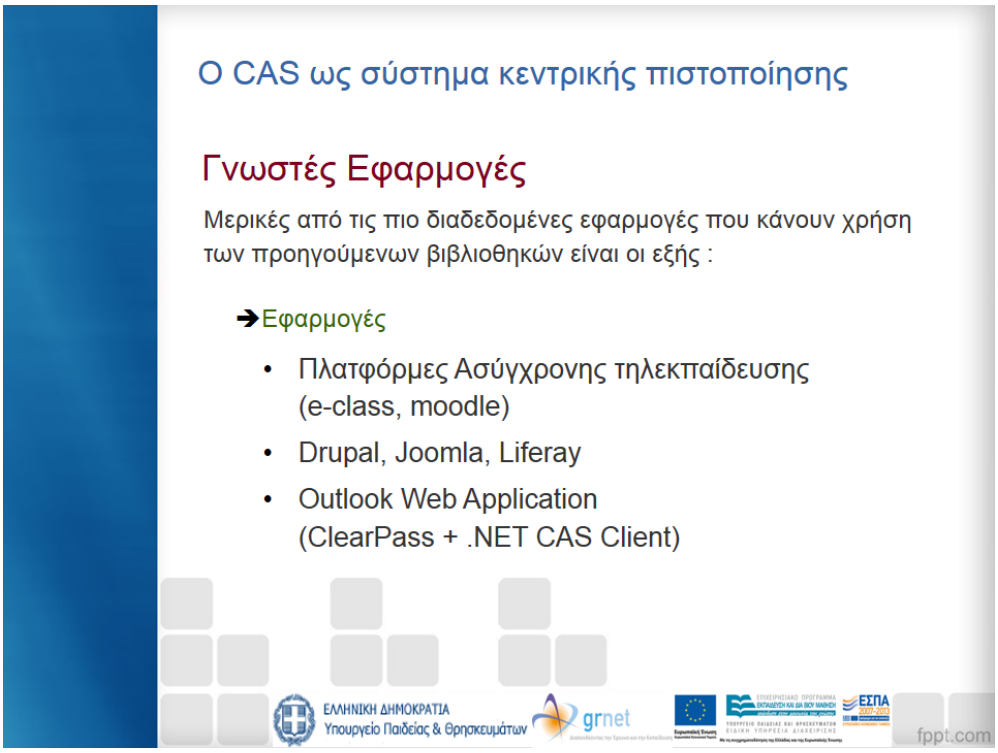
➔Γλώσσες

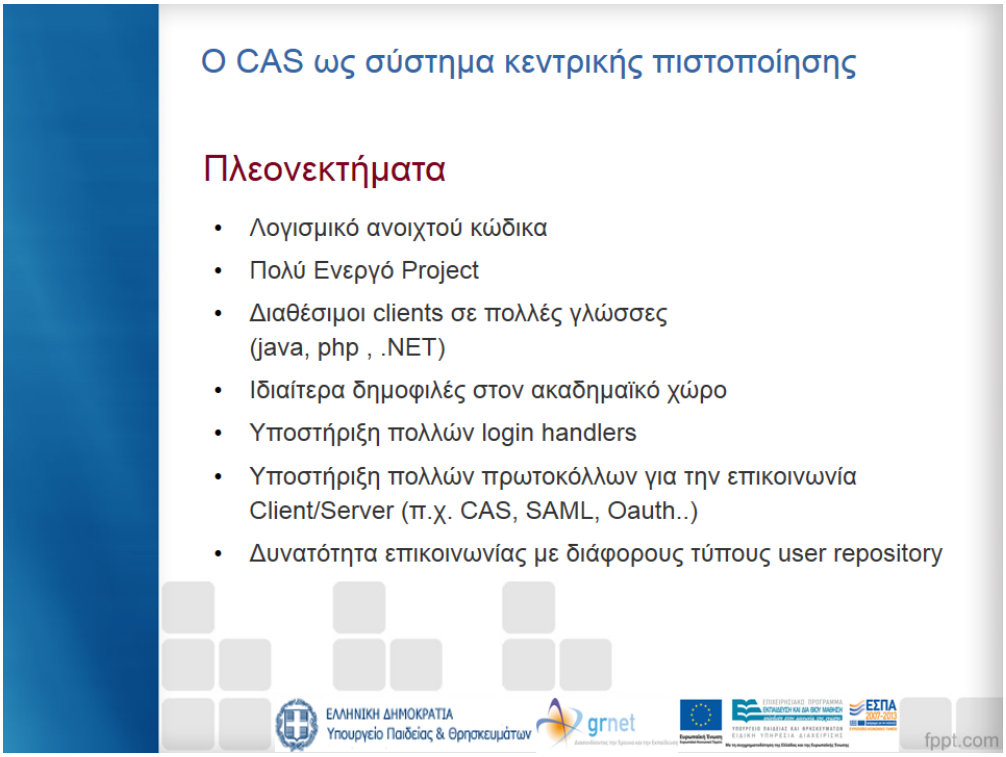
- Php
- Java
- .NET
- Python

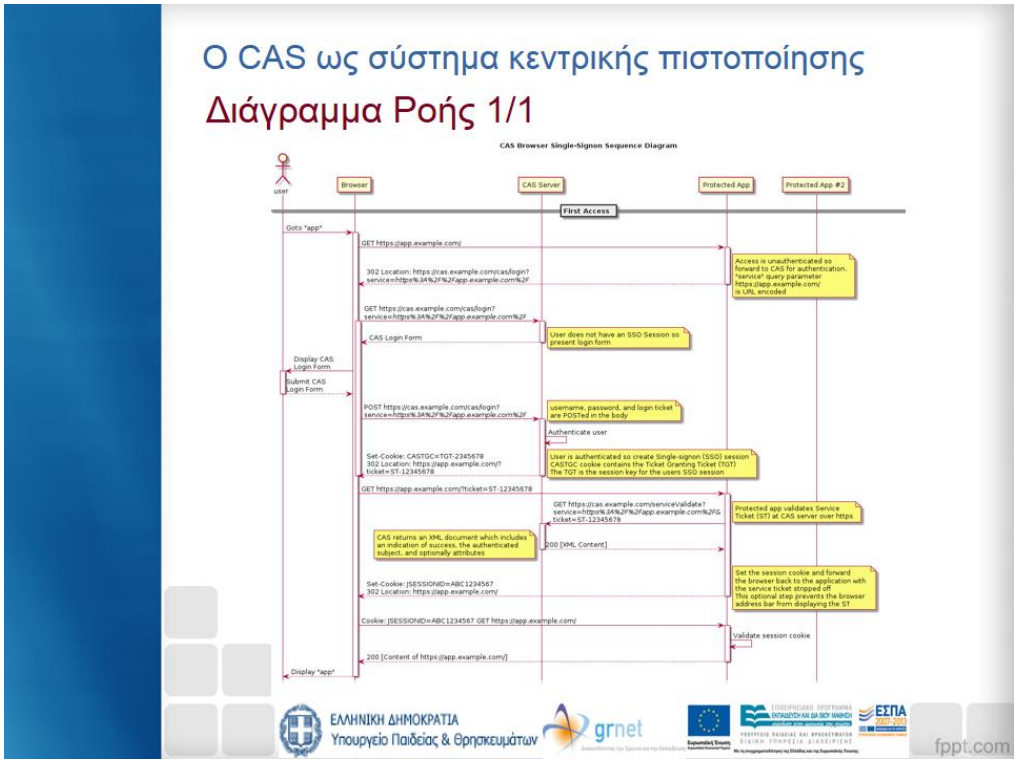
➔Υλοποιήσεις

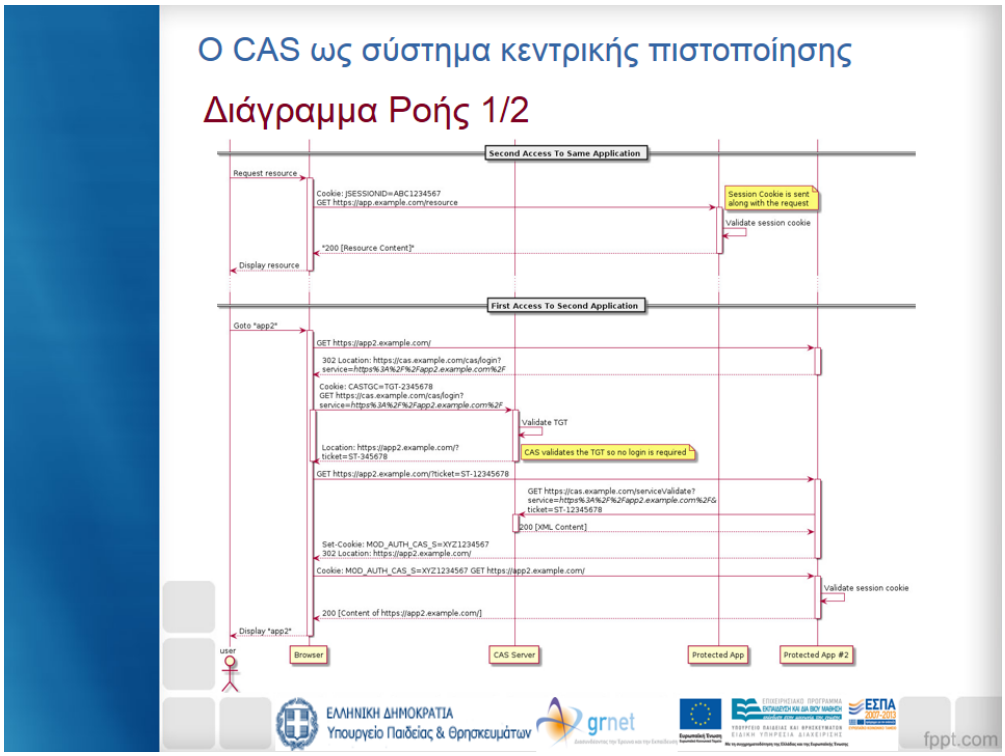
- PHP (phpCAS)
- Java (Java CAS Client)
- .NET (.NET CAS Client)
- Apache httpd Server (mod_auth_cas module)

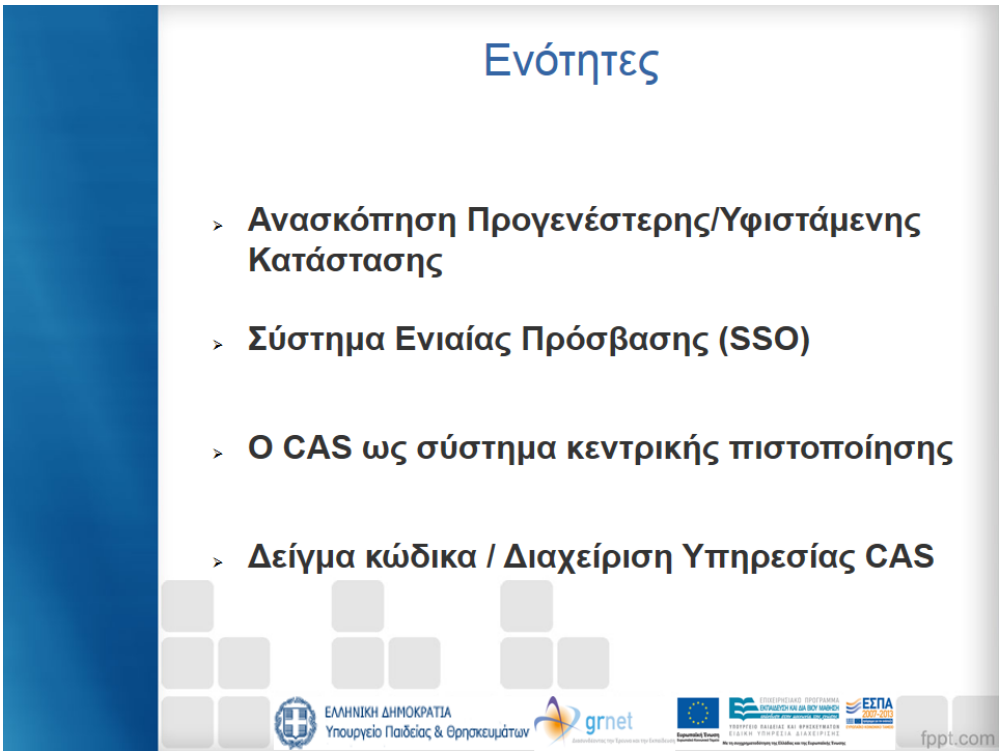
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας & Θρησκευμάτων
grnet
fppt.com

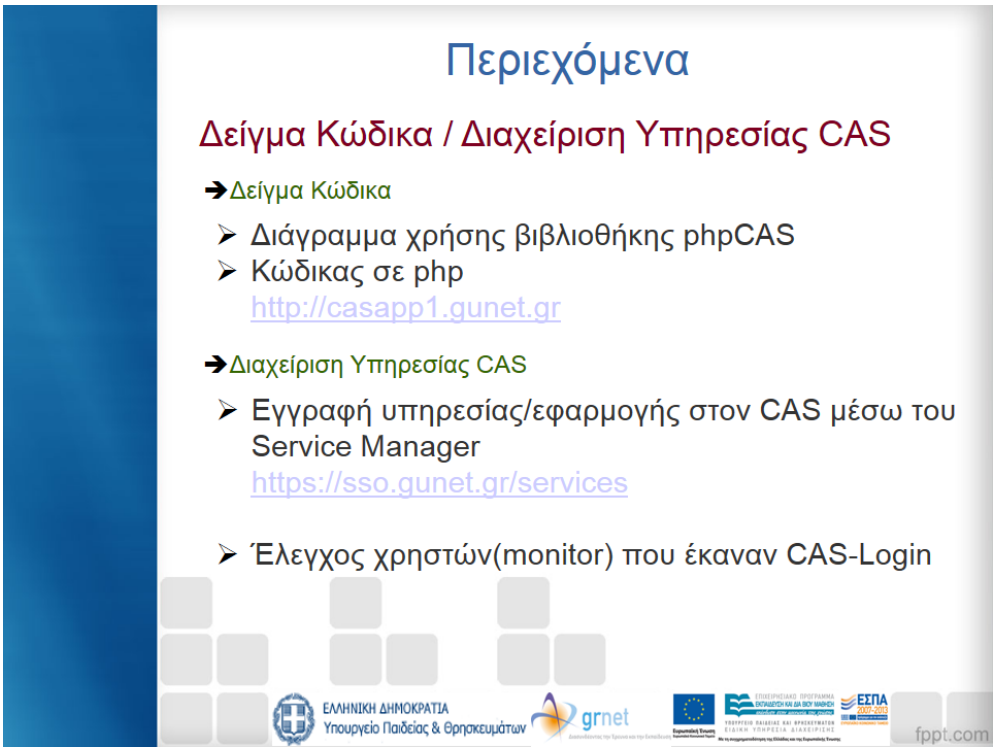

Ο CAS ως σύστημα κεντρικής πιστοποίησης
Γνωστές Εφαρμογές
Μερικές από τις πιο διαδεδομένες εφαρμογές που κάνουν χρήση των προηγούμενων βιβλιοθηκών είναι οι εξής :
➔Εφαρμογές
• Πλατφόρμες Ασύγχρονης τηλεκπαίδευσης (e-class, moodle)
• Drupal, Joomla, Liferay
• Outlook Web Application (ClearPass + .NET CAS Client)
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας & Θρησκευμάτων
grnet
fppt.com


Ο CAS ως σύστημα κεντρικής πιστοποίησης
Πλεονεκτήματα
• Λογισμικό ανοιχτού κώδικα
• Πολύ Ενεργό Project
• Διαθέσιμοι clients σε πολλές γλώσσες (java, php , .NET)
• Ιδιαίτερα δημοφιλές στον ακαδημαϊκό χώρο
• Υποστήριξη πολλών login handlers
• Υποστήριξη πολλών πρωτοκόλλων για την επικοινωνία Client/Server (π.χ. CAS, SAML, Oauth..)
• Δυνατότητα επικοινωνίας με διάφορους τύπους user repository
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας & Θρησκευμάτων
grnet
fppt.com


Ο CAS ως σύστημα κεντρικής πιστοποίησης
Διάγραμμα Ροής 1/1
CAS Browser Single-Signon Sequence Diagram
user
Browser
CAS Server
Protected App
Protected App #2
First Access
Goto "app"
GET https://app.example.com/
302 Location: https://cas.example.com/cas/login?service=https%3A%2F%2Fapp.example.com%2F
Access is unauthenticated so forward to CAS for authentication. "service" query parameter https://app.example.com/ is URL encoded
GET https://cas.example.com/cas/login?service=https%3A%2F%2Fapp.example.com%2F
CAS Login Form
User does not have an SSO Session so present login form
Display CAS Login Form
Submit CAS Login Form
POST https://cas.example.com/cas/login?service=https%3A%2F%2Fapp.example.com%2F
username, password, and login ticket are POSTed in the body
Authenticate user
Set-Cookie: CASTGC=TGT-2345678
302 Location: https://app.example.com/?ticket=ST-12345678
User is authenticated so create Single-signon (SSO) session
CASTGC cookie contains the Ticket Granting Ticket (TGT)
The TGT is the session key for the users SSO session
GET https://app.example.com/?ticket=ST-12345678
GET https://cas.example.com/serviceValidate?service=https%3A%2F%2Fapp.example.com%2FS&ticket=ST-12345678
Protected app validates Service Ticket (ST) at CAS server over https
CAS returns an XML document which includes an indication of success, the authenticated subject, and optionally attributes
200 [XML Content]
Set the session cookie and forward the browser back to the application with the service ticket stripped off
This optional step prevents the browser address bar from displaying the ST
Set-Cookie: JSESSIONID=ABC1234567
302 Location: https://app.example.com/
Cookie: JSESSIONID=ABC1234567 GET https://app.example.com/
Validate session cookie
200 [Content of https://app.example.com/]
Display "app"
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας & Θρησκευμάτων
grnet
fppt.com

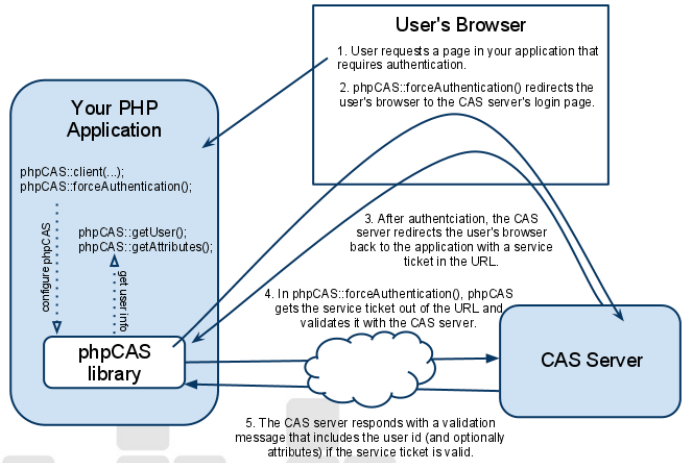

Ο CAS ως σύστημα κεντρικής πιστοποίησης
Διάγραμμα Ροής 1/2
Second Access To Same Application
Request resource
Cookie: JSESSIONID=ABC1234567
GET https://app.example.com/resource
Session Cookie is sent along with the request
Validate session cookie
200 [Resource Content]
Display resource
First Access To Second Application
Goto "app2"
GET https://app2.example.com/
302 Location: https://cas.example.com/cas/login?service=https%3A%2F%2Fapp2.example.com%2F
Cookie: CASTGC=TGT-2345678
GET https://cas.example.com/cas/login?service=https%3A%2F%2Fapp2.example.com%2F
Validate TGT
Location: https://app2.example.com/?ticket=ST-345678
CAS validates the TGT so no login is required
GET https://app2.example.com/?ticket=ST-12345678
GET https://cas.example.com/serviceValidate?service=https%3A%2F%2Fapp2.example.com%2FS&ticket=ST-12345678
200 [XML Content]
Set-Cookie: MOD_AUTH_CAS_S=XYZ1234567
302 Location: https://app2.example.com/
Cookie: MOD_AUTH_CAS_S=XYZ1234567 GET https://app2.example.com/
Validate session cookie
200 [Content of https://app2.example.com/]
Display "app2"
user
Browser
CAS Server
Protected App
Protected App #2
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας & Θρησκευμάτων
grnet
fppt.com


Ενότητες
Ανασκόπηση Προγενέστερης/Υφιστάμενης Κατάστασης
Σύστημα Ενιαίας Πρόσβασης (SSO)
Ο CAS ως σύστημα κεντρικής πιστοποίησης
Δείγμα κώδικα / Διαχείριση Υπηρεσίας CAS
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας & Θρησκευμάτων
grnet
ΕΣΠΑ 2007-2013
fppt.com


Περιεχόμενα
Δείγμα Κώδικα / Διαχείριση Υπηρεσίας CAS
➔Δείγμα Κώδικα
Διάγραμμα χρήσης βιβλιοθήκης phpCAS
Κώδικας σε php
http://casapp1.gunet.gr
➔Διαχείριση Υπηρεσίας CAS
Εγγραφή υπηρεσίας/εφαρμογής στον CAS μέσω του Service Manager
https://sso.gunet.gr/services
Έλεγχος χρηστών(monitor) που έκαναν CAS-Login
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας & Θρησκευμάτων
grnet
ΕΣΠΑ 2007-2013
fppt.com

Δείγμα κώδικα / Διαχείριση Υπηρεσίας CAS

Διάγραμμα χρήσης βιβλιοθήκης phpCAS



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας & Θρησκευμάτων
grnet
fppt.com

Δείγμα κώδικα / Διαχείριση Υπηρεσίας CAS

Κώδικας σε php

```
// Load the settings from the central config file
require_once 'config.php';
// Load the CAS lib
require_once $phpcas_path . '/CAS.php';
// Initialize phpCAS
phpCAS::client(SAML_VERSION_1_1, $cas_host, $cas_port, $cas_context);
// VALIDATING THE CAS SERVER IS CRUCIAL TO THE SECURITY OF THE CAS PROTOCOL!
phpCAS::setNoCasServerValidation();
// force CAS authentication
phpCAS::forceAuthentication();
// User Authenticated by the CAS server / Logout if desired
if (isset($_REQUEST['logout'])) {
phpCAS::logout();
}
?>

<h1>Successfull Authentication!</h1>
<?php require 'script_info.php' ?>
<p>the user's login is <b><?php echo phpCAS::getUser(); ?></b>.</p>
<p>phpCAS version is <b><?php echo phpCAS::getVersion(); ?></b>.</p>
<p><a href="?logout=">Logout</a></p>
```

Πηγή : https://github.com/Jasig/phpCAS

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας & Θρησκευμάτων
grnet
fppt.com


Μπορείτε να υποβάλετε ότι ερωτήσεις ή απορίες προέκυψαν από την παρούσα εκπαίδευση.
Ευχαριστούμε πολύ!
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας & Θρησκευμάτων
grnet
fppt.com