Ευρωπαϊκή Ένωση
Ευρωπαϊκό Ταμείο Περιφερειακής Ανάπτυξης
ψηφιακήελλάδα
Όλα είναι δυνατά
Επιχειρησιακό Πρόγραμμα "Ψηφιακή Σύγκλιση"
ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
Ποιότητα ζωής για όλους
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης
Hellenic Academic Libraries Link
HEAL-LINK
Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών
Υποδομή Πιστοποίησης και Εξουσιοδότησης ΑΑΙ
Shibboleth.

Ομοσπονδία HEAL-Link

Ανώτατα Εκπαιδευτικά & Ερευνητικά Ιδρύματα

Παράρτημα - 4

Εικονικός Οργανισμός Προέλευσης (VHO)

Περιγραφή της υπηρεσίας

Πολιτική Εγγραφής

1 ΕΙΣΑΓΩΓΗ

Συνηθίζεται να υπάρχουν αρκετοί τελικοί χρήστες, οι οποίοι δεν είναι εγγεγραμμένοι σε κάποιο ίδρυμα και συνεπώς δε διαθέτουν ιδρυματικό λογαριασμό παρόλο που έχουν για κάποιο χρονικό διάστημα σχέση με το εν λόγω ίδρυμα. Τέτοια παραδείγματα χρηστών είναι:

1. Συνεργάτες έργων που εργάζονται σε ιδιωτικές εταιρίες.
2. Συνεργάτες έργων που προέρχονται από ξένα πανεπιστήμια.
3. Προγραμματιστές που εργάζονται σε ιδιωτικές εταιρίες και προσφέρουν υπηρεσίες προγραμματισμού και συνεχούς υποστήριξης.

Υπάρχουν δύο επιλογές για το πώς μπορεί να υποστηριχθούν τέτοιοι τελικοί χρήστες:

- Η εφαρμογή μιας ξεχωριστής μεθόδου σύνδεσης για μη-AAI χρήστες και η τοπική διαχείριση των διαπιστευτηρίων των χρηστών.
- Η ενσωμάτωση αυτών των τελικών χρηστών στον Εικονικό Οργανισμό Προέλευσης (VHO), που λειτουργεί από την Ομοσπονδία HEAL-Link, και ο οποίος τους μετατρέπει σε AAI χρήστες για τους διαθέσιμους πόρους.

Η πολιτική του παρόντος εγγράφου καθορίζει τους κανόνες μεταξύ των Ιδιοκτητών των πόρων και της Ομοσπονδίας HEAL-Link, όταν εφαρμόζεται η Β επιλογή.

2 ΟΡΙΣΜΟΙ

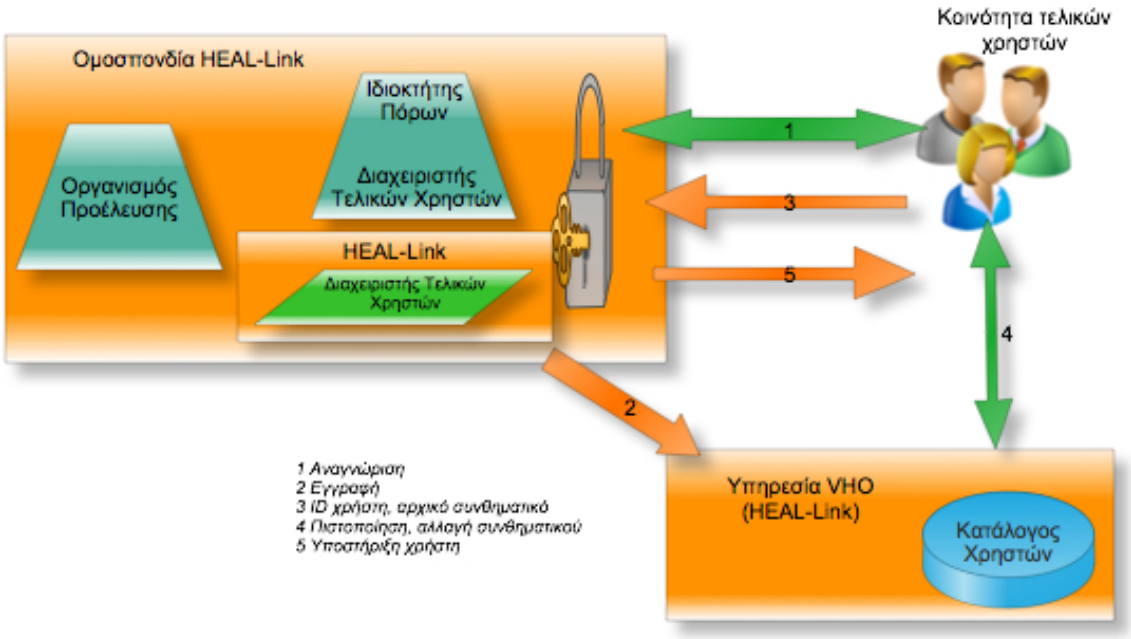
ΥΠΕ	Υποδομή Πιστοποίησης και Εξουσιοδότησης.
(AAI)	(Στο κείμενο χρησιμοποιείται η αγγλική συντομογραφία AAI: Authentication and Authorization Infrastructure)
Συνεργαζόμενο ίδρυμα (Affiliate)	Εάν πρόκειται για ένα φυσικό ή νομικό πρόσωπο, κάποιο άλλο πρόσωπο ή οντότητα, που ασκεί έλεγχο σε αυτό το πρόσωπο ή οντότητα, ή βρίσκεται υπό έλεγχο από αυτήν, ή τελεί υπό κοινό έλεγχο από το ίδιο πρόσωπο ή οντότητα. (Ο HEAL-Link είναι ένας μη κερδοσκοπικός οργανισμός και δεν ασχολείται με οποιαδήποτε θέματα μετοχικού κεφαλαίου με οποιονδήποτε οργανισμό).
Ιδιοχαρακτηριστικά (Attributes)	Πληροφορίες/στοιχεία των Τελικών Χρηστών, που απαιτούνται για τις αποφάσεις ελέγχου πρόσβασης.
Πιστοποίηση (Authentication)	Διαδικασία απόδειξης της ταυτότητας ενός ήδη καταχωρισμένου Τελικού Χρήστη.
Εξουσιοδότηση (Authorization)	Διαδικασία χορήγησης ή άρνηση παροχής πρόσβασης σε έναν συνδρομητικό πόρο ενός πιστοποιημένου Τελικού Χρήστη.
Μέλος Ομοσπονδίας (Federation Member)	Ορίζεται στο «Έγγραφο για την ακολουθητέα πολιτική» της Ομοσπονδίας.
Οργανισμός Προέλευσης (Home Organization)	Συμβαλλόμενοι οργανισμοί (εκτός των Συνεργατών της Ομοσπονδίας) όπως, ακαδημαϊκά ιδρύματα ή δημόσιοι οργανισμοί που εγγράφουν Εξουσιοδοτημένους Χρήστες. Κάθε ίδρυμα-μέλος μπορεί να έχει πολλούς Οργανισμούς Προέλευσης. Η δυνατότητα πρόσβασης των οργανισμών αυτών θα ελέγχεται από την Ομοσπονδία HEAL-Link πριν από οποιαδήποτε εξουσιοδότηση.
Ιδιοκτήτης Πόρων (Resource owner)	Ο οργανισμός ο οποίος παρέχει τους πόρους στα μέλη της Ομοσπονδίας HEAL-Link.
Πόροι (Resources)	Υλικό στο οποίο παρέχεται πρόσβαση, π.χ. εφαρμογές, ιστοσελίδες, βάσεις δεδομένων, συστήματα, κ.λπ., με βάση την αρχική συμφωνία με τον αντίστοιχο Ιδιοκτήτη Πόρων.
VHO Service Subscriber	Ο Οργανισμός που έχει συνδρομή στην υπηρεσία VHO.
Εικονικός Οργανισμός	Ένας κατάλογος χρηστών, που επιτρέπει στον ιδιοκτήτη Πόρων την εγγραφή εξουσιοδοτημένων χρηστών, που δεν έχουν καταγραφεί με άλλο τρόπο από οποιονδήποτε Οργανισμό Προέλευσης, να παρέχει

Προέλευσης (Virtual Home Organization or VHO)	πρόσβαση σε αυτούς τους εγκεκριμένους χρήστες σε ορισμένους πόρους.
Διαχειριστής Τελικού Χρήστη (End User Administrator)	Ένα πρόσωπο καθορισμένο από τον Ιδιοκτήτη Πόρων ή την Ομοσπονδία HEAL-Link, το οποίο είναι υπεύθυνο για τη διατήρηση των δεδομένων των χρηστών για τον συγκεκριμένο πόρο ή αντίστοιχα για το συγκεκριμένο μέλος του HEAL-Link.

3 Η ΥΠΗΡΕΣΙΑ VHO

3.1 Περιγραφή της υπηρεσίας

Η Υπηρεσία VHO παρέχεται από την Ομοσπονδία HEAL-Link και μπορούν να εγγραφούν σε αυτήν τόσο οι Ιδιοκτήτες Πόρων όσο και οι Οργανισμοί Προέλευσης των μελών[1] της Ομοσπονδίας HEAL-Link. Δίνει τη δυνατότητα στον Ιδιοκτήτη Πόρων να δημιουργήσει λογαριασμούς AAI για χρήστες, που δεν ανήκουν σε έναν Οργανισμό Προέλευσης. Ένας τέτοιος λογαριασμός θα θεωρείται έγκυρος για το σύνολο των πόρων, που ανήκουν στον αντίστοιχο Ιδιοκτήτη Πόρων.



Εικόνα 1 Υπηρεσία VHO: Αλληλεπιδράσεις

Η εφαρμογή VHO αποτελείται από έναν κατάλογο Τελικών Χρηστών με έναν διαχειριστή Τελικών Χρηστών μέσω διαδικτύου και τις αντίστοιχες διεπαφές Τελικών Χρηστών.

Ο συνδρομητής στην υπηρεσία VHO καθορίζει τουλάχιστον ένα Διαχειριστή Τελικών Χρηστών, ο οποίος θα μπορεί να:

- καταχωρίζει νέους Τελικούς Χρήστες.
- καθορίζει τα πεδία user ID[2] and τον αρχικό κωδικό.

---

[1] Όλα τα μέλη της Ομοσπονδίας θα πρέπει να έχουν ήδη υπογράψει το αντίστοιχο συμφωνητικό: HEAL-Link AAI Service Agreement.

[2] Το ID χρήστη έχει τη μορφή <πρόθεμα>-<ξεχωριστό μέρος>, πχ “heal-link-uid123”. Η ομοσπονδία HEAL-Link καθορίζει το πρόθεμα του ID των χρηστών για κάθε Εικονικό Οργανισμό Προέλευσης.

- διαγράφει και να τροποποιεί υφιστάμενους Τελικούς Χρήστες.
- καθορίζει νέους κωδικούς.

Ο Τελικός Χρήστης θα μπορεί να:

- αποδέχεται τους Όρους Χρήσης και να αλλάζει τον κωδικό του.
- έχει υποστήριξη από το Διαχειριστή Τελικών Χρηστών.

Όταν ένας Τελικός Χρήστης εισέλθει στο σύστημα για πρώτη φορά, θα πρέπει να αποδεχθεί τους Όρους Χρήσης.

3.2 Υποχρεώσεις της Ομοσπονδίας HEAL-Link

Για την εύρυθμη λειτουργία της Υπηρεσίας VHO, η Ομοσπονδία HEAL-Link, ως πάροχος της υπηρεσίας VHO, πρέπει να πληροί τις ακόλουθες προϋποθέσεις:

1. Η Ομοσπονδία HEAL-Link ακολουθεί την πολιτική των Οργανισμών Προέλευσης, όπως αυτή ορίζεται ως κομμάτι του εγγράφου για την Ακολουθητέα Πολιτική.
2. Η Ομοσπονδία HEAL-Link διατηρεί την πολιτική απελευθέρωσης ιδιοχαρακτηριστικών του Εικονικού Οργανισμού Προέλευσης σύμφωνα με τις ανάγκες του Συνδρομητή της Υπηρεσίας VHO.
3. Για να γίνει σαφής ο διαχωρισμός μεταξύ χρηστών του Εικονικού Οργανισμού Προέλευσης και τακτικών χρηστών (προερχόμενων από τα ιδρύματα-μέλη), η Ομοσπονδία HEAL-Link διασφαλίζει ότι ορισμένα ιδιοχαρακτηριστικά ορίζονται ως εξής:

   eduPersonScopedAffiliation = *affiliate@vho-heal-link.gr*

   eduPersonAffiliation = *affiliate*

   eduPersonOrgDN = *dc=vho-heal-link,dc=gr*
4. Η Ομοσπονδία HEAL-Link υποδεικνύει τεχνικές και διαχειριστικές πληροφορίες επικοινωνίας στους συνδρομητές της Υπηρεσίας VHO.
5. Η Ομοσπονδία HEAL-Link λαμβάνει τα απαραίτητα μέτρα για τη διασφάλιση της απρόσκοπτης λειτουργίας της υπηρεσίας, την παρακολούθηση της διαθεσιμότητας της υπηρεσίας και την υποστήριξη την Διαχειριστών Τελικών Χρηστών. Οι διακοπές λόγω προγραμματισμένων εργασιών συντήρησης θα ανακοινώνονται εκ των προτέρων.

3.3 Υποχρεώσεις του Συνδρομητή στην Υπηρεσία VHO

1. Ο Συνδρομητής της Υπηρεσίας VHO καταχωρεί τους Τελικούς Χρήστες, όπως ορίζεται στους κανόνες της πολιτικής Εγγραφής Τελικού Χρήστη (βλέπε Κεφάλαιο 4).

2. Ο Συνδρομητής της Υπηρεσίας VHO παρέχει υποστήριξη πρώτου επιπέδου στους καταχωρισμένους του Τελικούς Χρήστες.
3. Ο Συνδρομητής της Υπηρεσίας VHO υποδεικνύει στην Ομοσπονδία HEAL-Link τεχνικές και διαχειριστικές πληροφορίες επικοινωνίας.
4. Κατόπιν αιτήματος, ο Διαχειριστής Τελικού Χρήστη ενημερώνει την Ομοσπονδία HEAL-Link για τον αριθμό των χρηστών, που διαχειρίζεται τη συγκεκριμένη χρονική στιγμή, για το πώς αυτοί οι χρήστες συνδέονται με το Συνδρομητή της Υπηρεσίας VHO (ακριβής τρόπος σύνδεσης), καθώς επίσης και για τα αντίστοιχα αποδεικτικά δικαιολογητικά, που πρέπει να διαθέτει για τους εν λόγω χρήστες.

3.4 Τροποποιήσεις της Υπηρεσίας

Με μια εκ των προτέρων (τουλάχιστον 2 εβδομάδων) προειδοποίηση, η Ομοσπονδία HEAL-Link διατηρεί το δικαίωμα να επιφέρει αλλαγές, αν χρειαστεί, στη λειτουργικότητα, στις απαιτήσεις, στις διαδικασίες, στα ιδιοχαρακτηριστικά κλπ. του Εικονικού Οργανισμού Προέλευσης ή των χρηστών του.

4 ΠΟΛΙΤΙΚΗ ΕΓΓΡΑΦΗΣ ΤΕΛΙΚΟΥ ΧΡΗΣΤΗ

Παρόλο που η Ομοσπονδία HEAL-Link λειτουργεί την Υπηρεσία VHO, η καταχώριση των Τελικών Χρηστών και η συντήρηση των δεδομένων του Τελικού Χρήστη είναι υπό την ευθύνη του Συνδρομητή στην Υπηρεσία VHO. Θα πρέπει να υπάρχει πλήρης συμμόρφωση με τις διατάξεις περί προστασίας των προσωπικών δεδομένων που ορίζονται στη σύμβαση Παροχής Υπηρεσιών AAI.

Ο Διαχειριστής Τελικού Χρήστη πραγματοποιεί την καταχώρηση των δεδομένων. Αυτός ή ένα έμπιστο τρίτο άτομο (πχ. ένας εκπρόσωπος του συμβαλλόμενου μέρους), πρέπει να εξακριβώσει την ταυτότητα των νέων χρηστών, που θα βασίζεται σε επίσημα έγγραφα[3](πχ ταυτότητα, διαβατήριο, έγγραφο εγγραφής στην υπηρεσία) και θα πρέπει να είναι σε θέση να συνδέσει το όνομα χρήστη του εγγεγραμμένου Τελικού Χρήστη με ένα πραγματικό πρόσωπο οποιαδήποτε στιγμή (με εξαίρεση τους δοκιμαστικούς λογαριασμούς και τους λογαριασμούς επισκεπτών, βλέπε παρακάτω).

Ο Διαχειριστής Τελικού Χρήστη είναι κυρίως υπεύθυνος για:

- τη σωστή και καλή διαχείριση των εν λόγω στοιχείων Τελικού Χρήστη (πχ. διαγραφή του τελικού χρήστη, όταν δεν είναι πλέον εξουσιοδοτημένος να χρησιμοποιήσει τον πόρο).
- τη δημιουργία ενός ονόματος χρήστη και αρχικού κωδικού πρόσβασης και την αρχική μετάδοση αυτών των διαπιστευτηρίων στον Τελικό Χρήστη.

Οι δοκιμαστικοί λογαριασμοί και οι λογαριασμοί επισκεπτών αποτελούν ειδική περίπτωση. Θα πρέπει να ανοίγονται μόνο σε περίπτωση που δεν είναι εφικτή η χρήση κάποιου προσωπικού λογαριασμού. Λογαριασμοί επισκεπτών χρησιμοποιούνται κατά κύριο λόγο για τους συμμετέχοντες σε κάποιο μάθημα. Οι κωδικοί πρόσβασης των λογαριασμών επισκεπτών πρέπει να αλλάζουν μετά τη λήξη των μαθημάτων. Δεν επιτρέπεται η δημοσίευση κωδικών πρόσβασης των λογαριασμών επισκεπτών ή των δοκιμαστικών λογαριασμών σε δημόσιες πηγές πληροφοριών (πχ. ιστοσελίδες, e-mail αρχεία, περιοδικά κλπ).

Το επώνυμο των δοκιμαστικών λογαριασμών και των λογαριασμών επισκεπτών πρέπει να ακολουθεί αυτούς τους κανόνες:

Δοκιμαστικός λογαριασμός: Το επώνυμο ξεκινάει με demo-

---

[3] Εναλλακτικά, η έμπιστη Τρίτη οντότητα μπορεί να παρέχει μια λίστα με πρώην εγγεγραμμένους χρήστες (π.χ. προσωπικό ή φοιτητές), εάν η πρώην διαδικασία εγγραφής είναι τόσο ακριβής όσο και η διαδικασία εγγραφής για τους χρήστες του Εικονικού Οργανισμού Προέλευσης (πχ. βασίζεται σε επίσημα έγγραφα).

Λογαριασμός επισκεπτών: Το επώνυμο ξεκινάει με guest-

Για κάθε δοκιμαστικό λογαριασμό και λογαριασμό επισκεπτών, ο Διαχειριστής Τελικού Χρήστη πρέπει να ενημερώνεται από ένα υπεύθυνο πρόσωπο επαφής (ενδεχομένως σε κάποιον εξωτερικό οργανισμό), το οποίο θα είναι σε θέση να προσδιορίσει τον πραγματικό χρήστη, εάν αυτό κριθεί απαραίτητο.

Η σύνταξη του παρόντος βασίστηκε στο έγγραφο: **SWITCHaai (AAI – Authentication and Authorization Infrastructure VHO Service Description & VHO Registration Policy, Switzerland).**