



Ευρωπαϊκή Ένωση
Ευρωπαϊκό Ταμείο
Περιφερειακής Ανάπτυξης



ψηφιακή **εΡΑ**άδα
Όλα είναι δυνατά
Επιχειρησιακό Πρόγραμμα
"Ψηφιακή Σύγκλιση"

ΤΕΙ
ΣΕΡΡΩΝ



«Προηγμένες Ψηφιακές Υπηρεσίες για τον Πολίτη και τον Σπουδαστή στο ΤΕΙ Σερρών»

ΠΑΡΑΔΟΤΕΟ Π.1.4.2 «Θεσμοθέτηση διαδικασιών και ροών εργασίας για τις υπηρεσίες ΤΠΕ του ΤΕΙΣ – Κανονιστικό πλαίσιο χρήσης εφαρμογών»

Κανονιστικό πλαίσιο χρήσης

Υπηρεσίας Πιστοποίησης και Εξουσιοδότησης (Α.Α.Ι.) ΤΕΙ ΣΕΡΡΩΝ

Κείμενο πολιτικής

Έκδοση 0.1

Σάββας Πασχαλίδης
Θεόδωρος Σαρικούδης
Κωνσταντίνος Χειλάς

Μάρτιος 2013

Περιγραφή υπηρεσίας

Η Υπηρεσία Πιστοποίησης και Εξουσιοδότησης (Υ.Π.Ε.) έχει σκοπό την πιστοποίηση της ταυτότητας του χρήστη ηλεκτρονικών υπηρεσιών του ΤΕΙ ΣΕΡΡΩΝ και την εξουσιοδότησή του για χρήση αυτών των υπηρεσιών. Ο χρήστης κατέχοντας ένα μόνο ιδρυματικό λογαριασμό, με το μυστικό κωδικό του, μπορεί να χρησιμοποιεί μια πληθώρα υπηρεσιών χωρίς την ανάγκη εισαγωγής username/password σε κάθε μία ξεχωριστά. Η εισαγωγή των username, password γίνεται με ασφαλή μέθοδο σε ένα κεντρικό σημείο (Single Sign On –SSO), χωρίς να υφίσταται ανάγκη εισαγωγής τους για κάθε μία από τις υπηρεσίες που προσπελαύνει. Μετά την επιτυχημένη πιστοποίηση του χρήστη ακολουθεί η διαδικασία εξουσιοδότησης για κάθε συγκεκριμένη υπηρεσία που αυτός αιτείται να χρησιμοποιήσει. Με την ολοκλήρωση της εξουσιοδότησης που περιλαμβάνει και απελευθέρωση χαρακτηριστικών του χρήστη, αυτός μπορεί να απολαμβάνει υπηρεσίες, που συνδέονται με την Υ.Π.Ε., εύκολα και απρόσκοπτα.

Η Υ.Π.Ε. λειτουργεί και συντηρείται από το Κ.Λ.Δ. Η λειτουργία για δια-ιδρυματικές υπηρεσίες βασίζεται στο διεθνές πρότυπο SAML 2.0 που σήμερα υλοποιείται με το λογισμικό Shibboleth και θεωρείται η πλέον διαδεδομένη μέθοδος παροχής αντίστοιχων υπηρεσιών παγκοσμίως στον Ακαδημαϊκό χώρο.

Η Υ.Π.Ε. προσφέρει τις υπηρεσίες της σε όλους τους χρήστες του ΤΕΙ ΣΕΡΡΩΝ που αποκτούν ιδρυματικό λογαριασμό από το ΚΛΔ. Συνεργάζεται με όλες τις μονάδες του ΤΕΙ, αλλά και τρίτους παρόχους (Service Providers) που υλοποιούν ηλεκτρονικές υπηρεσίες τις οποίες επιθυμούν να προσφέρουν προς τα μέλη του ΤΕΙ μέσω του παγκόσμιου ιστού (web based services) εντασσόμενοι στην Υ.Π.Ε.

Ένταξη Παρόχου Υπηρεσιών (Service Provider)

Κάθε Πάροχος Υπηρεσιών που επιθυμεί να ενταχθεί στην Υ.Π.Ε. καταθέτει σχετικό αίτημα στο Κ.Λ.Δ. Το αίτημα εγκρίνει ή απορρίπτει το ΚΥΤΕΠ (Κέντρο Υποστήριξης Τεχνολογιών Επικοινωνιών και Πληροφορικής) μετά από εισήγηση του Κ.Λ.Δ. Για να ενταχθεί ένας πάροχος, οφείλει να εναρμονίζεται με τις απαιτήσεις και τους κανόνες λειτουργίας της Υ.Π.Ε. Συγκεκριμένα ο πάροχος υποχρεούται:

- να δηλώσει το εύρος της ιδιότητας των χρηστών που δικαιούνται να χρησιμοποιήσουν την εντασσόμενη υπηρεσία.
- να δηλώσει τα ελάχιστα και τα επιθυμητά χαρακτηριστικά (attributes) που χρειάζεται η εντασσόμενη υπηρεσία για την εξασφάλιση εξουσιοδότησης.
- να τεκμηριώσει τις απαιτήσεις της εντασσόμενης υπηρεσίας στην απελευθέρωση των απαιτούμενων χαρακτηριστικών. Η απελευθέρωση των απαιτούμενων χαρακτηριστικών θα γίνεται σε συνεννόηση με το Κ.Λ.Δ. και μετά από σχετική έγκριση
- να παρέχει μεταδεδομένα (metadata) κατά την ένταξη της υπηρεσίας και να ενημερώνει το Κ.Λ.Δ. για κάθε αλλαγή τους.
- να χρησιμοποιεί ψηφιακό πιστοποιητικό διακομιστή για τον διακομιστή που θα φιλοξενεί την εντασσόμενη υπηρεσία. Το πιστοποιητικό αυτό είτε εκδίδεται από την Αρχή Πιστοποίησης του ΤΕΙ ΣΕΡΡΩΝ, είτε από Α.Π. που ανήκει στον κύκλο εμπιστοσύνης της Α.Π. του ΤΕΙ, ή από Α.Π. η οποία είναι προ-εγκατεστημένη στους δημοφιλείς πλοηγούς (browsers).
- να τηρεί αρχεία καταγραφής εισόδου-εξόδου χρηστών στην εντασσόμενη υπηρεσία διάρκειας τουλάχιστον 12 μηνών, εκτός αν ορίζεται διαφορετικά από σχετική νομοθεσία.
- να παραδίδει τα αρχεία καταγραφής της εντασσόμενης υπηρεσίας σε περίπτωση κατάχρησής της και εφόσον ζητηθούν από την αρμόδια Δημόσια Αρχή. (Αρχεία καταγραφής παρόχων υπηρεσίας εντός του ΤΕΙ Σερρών αναζητούνται μέσω της Συνέλευσης του ΤΕΙ).
- να φροντίζει για την καλή, εύρυθμη και ασφαλή λειτουργία τόσο της εντασσόμενης υπηρεσίας όσο και του διακομιστή, συμπεριλαμβανομένου του λειτουργικού συστήματος και της δικτυακής σύνδεσής του.
- να χειρίζεται ως εμπιστευτικά τα χαρακτηριστικά των χρηστών που απελευθερώνονται στην υπηρεσία του από την ΥΠΕ και να μην τα επεξεργάζεται για σκοπούς πέραν της υπηρεσίας για την οποία συμφώνησε ο τελικός χρήστης
- να παρέχει υπηρεσίες που συνάδουν με την ακαδημαϊκή δραστηριότητα και δεν έρχονται σε σύγκρουση ή / και επικάλυψη με υφιστάμενες επίσημες ιδρυματικές υπηρεσίες του ΤΕΙ Σερρών
- να συμμορφώνεται στις υποδείξεις και τους κανόνες λειτουργίας της Υ.Π.Ε. όπως αυτές ορίζονται από το Κέντρο Υποστήριξης Τεχνολογιών Επικοινωνιών και Πληροφορικής.

Το Κ.Λ.Δ. γνωμοδοτεί σε θέματα καλής λειτουργίας και σύνδεσης της εντασσόμενης υπηρεσίας στην Υ.Π.Ε. προς τον πάροχο.

Το Κ.Λ.Δ., μετά την θετική έγκριση του ΚΥΤΕΠ, εντάσσει τη νέα υπηρεσία στην Υ.Π.Ε. περιλαμβάνοντας τα μεταδεδομένα της σε αυτά που αναγνωρίζει η Υ.Π.Ε. και εφαρμόζοντας την

εγκεκριμένη πολιτική εύρους χρηστών καθώς και απελευθέρωσης χαρακτηριστικών της εντασσόμενης υπηρεσίας.

Το ΚΥΤΕΠ του ΤΕΙ Σερρών ορίζεται ως μοναδικός κριτής και διαιτητής οποιουδήποτε αιτήματος ή / και διαφωνίας που ενδέχεται να προκύψει κατά την λειτουργία της εντασσόμενης υπηρεσίας.

Πλαίσιο Ιδρυματικού Παρόχου πιστοποίησης

Ο ιδρυματικός Πάροχος Πιστοποίησης (IdP) της Υ.Π.Ε. λειτουργεί υπό την διαχείριση του Κ.Λ.Δ. Συγκεκριμένα το ΚΛΔ φροντίζει ώστε ο IdP:

- να εξυπηρετεί το σύνολο των χρηστών ηλεκτρονικών υπηρεσιών του ΤΕΙ Σερρών
- να χρησιμοποιεί τεχνολογία συμβατή με SAML 2.0 στην υπηρεσία πιστοποίησης.
- να διατηρεί ασφαλή και να διαφυλάσσει από μη εγκεκριμένη από τον ίδιο το χρήστη έκθεση τα προσωπικά δεδομένα των χρηστών που εξυπηρετεί.
- να παρέχει ενημερωμένα μεταδεδομένα (metadata) για τις υπηρεσίες πιστοποίησής του.
- να χρησιμοποιεί έγκυρο ψηφιακό πιστοποιητικό διακομιστή εκδιδόμενο από έμπιστη Αρχή Πιστοποίησης
- να τηρεί αρχεία καταγραφής για τις δραστηριότητες της υπηρεσίας πιστοποίησης τουλάχιστον 12 μηνών εκτός αν ορίζεται διαφορετικά από σχετική νομοθεσία.
- να φροντίζει για την καλή, εύρυθμη και ασφαλή λειτουργία τόσο της υπηρεσίας πιστοποίησης όσο και του διακομιστή, συμπεριλαμβανομένου του λειτουργικού συστήματος και της δικτυακής σύνδεσής του.

Επιπλέον το Κ.Λ.Δ:

- παραδίδει τα αρχεία καταγραφής της υπηρεσίας πιστοποίησης στην εποπτεύουσα Επιτροπή ή τη Διοικούσα Αρχή του ΤΕΙ Σερρών σε περίπτωση κατάχρησής της Υ.Π.Ε. και εφόσον ζητηθούν από αυτές.
- τηρεί, συντηρεί και ανανεώνει τεκμηρίωση απελευθέρωσης χαρακτηριστικών των χρηστών που εξυπηρετεί ανά πάροχο υπηρεσίας.
- γνωμοδοτεί σε θέματα καλής λειτουργίας και σύνδεσης της υπηρεσίας πιστοποίησης στην Υ.Π.Ε. προς τον κάθε πάροχο υπηρεσιών

Το ΚΥΤΕΠ του ΤΕΙ Σερρών ορίζεται ως μοναδικός κριτής και διαιτητής οποιουδήποτε αιτήματος ή / και διαφωνίας που ενδέχεται να προκύψει κατά την λειτουργία της υπηρεσίας πιστοποίησης.