



Greek School Network
Network for Education

Προδιαγραφές για την Εγγραφή μιας Υπηρεσίας στην Κεντρική Υπηρεσία Πιστοποίησης (SSO) του Πανελληνίου Σχολικού Δικτύου (ΠΣΔ)

Για να εγγράψετε μια υπηρεσία στην Κεντρική Υπηρεσία Πιστοποίησης (Single Sign-On - SSO) του ΠΣΔ (Πανελλήνιο Σχολικό Δίκτυο) απαιτούνται συγκεκριμένα βήματα και προσοχή στις τεχνικές προδιαγραφές. Το παρόν έγγραφο χωρίζεται σε δύο κύριες ενότητες: Η πρώτη ενότητα καλύπτει τη διαδικασία εγγραφής και τα απαραίτητα βήματα που πρέπει να ακολουθήσετε, ενώ η δεύτερη ενότητα αναλύει τις απαιτούμενες τεχνικές προδιαγραφές που πρέπει να τηρήσετε.

Προαπαιτούμενα βήματα διασύνδεσης μιας υπηρεσίας:

- Υποβολή Αιτήματος:** Πρέπει να υποβάλετε ένα αίτημα είτε μέσω του συστήματος στη διεύθυνση <https://helpdesk.sch.gr/>, είτε να απευθυνθείτε στο αρμόδιο helpdesk της περιοχής σας.
- Δήλωση Προστασίας και Εχεμύθειας:** Η υπηρεσία πρέπει να πληροί τις προϋποθέσεις της Δήλωσης προστασίας και Εχεμύθειας Προσωπικών Δεδομένων Χρηστών του Π.Σ.Δ.
- Κριτήρια Διασύνδεσης:** Πρέπει να μας γνωστοποιήσετε τα κριτήρια διασύνδεσης ενός χρήστη του ΠΣΔ στην υπηρεσία, προκειμένου να μπορέσουμε να εξακριβώσουμε την ορθή λειτουργία της με έναν demo χρήστη. Συγκεκριμένα, αυτά περιλαμβάνουν:
 - **Umdobject:** Κατηγορία του χρήστη (π.χ., teacher, ateacher, pteacher, student, personel, account).
 - **Business Category:** Κατηγορία μονάδας με δύο τιμές (Βαθμίδα / Κατηγορία).
 - **Βαθμίδα:** Πρωτοβάθμια/Δευτεροβάθμια.
 - **Κατηγορία:** Σχολική, Διοικητική, Υποστηρικτική μονάδα.
- Σύνδεσμοι Σύνδεσης και Αποσύνδεσης:** Θα πρέπει να γνωστοποιήσετε τα σημεία της ιστοσελίδας όπου βρίσκονται οι σύνδεσμοι για το login και το logout.
- Διάρκεια Συνεδρίας (Session):** Πρέπει να γνωστοποιηθεί ο χρόνος που η εφαρμογή διατηρεί ζωντανό το session του χρήστη μετά από ένα SSO login, χωρίς να ξαναρωτά τον SSO για την κατάσταση σύνδεσης του χρήστη.

Τεχνικές προδιαγραφές:

1. Υποστήριξη HTTPS

- **Προδιαγραφή:** Η υπηρεσία πρέπει πάντα να υποστηρίζει το HTTPS.
- **Εξήγηση:** Η χρήση του HTTPS είναι απαραίτητη για να εξασφαλιστεί η ασφαλής επικοινωνία μεταξύ της υπηρεσίας και του συστήματος SSO. Το HTTPS κρυπτογραφεί τα δεδομένα που μεταδίδονται μεταξύ του περιηγητή του χρήστη και της υπηρεσίας, προστατεύοντας ευαίσθητες πληροφορίες, όπως τα διαπιστευτήρια σύνδεσης και τα δεδομένα του χρήστη.
- **Δράση:** Πριν εγγράψετε μια υπηρεσία στο SSO του ΠΣΔ, βεβαιωθείτε ότι η υπηρεσία σας είναι ρυθμισμένη να χρησιμοποιεί HTTPS. Αποκτήστε και εγκαταστήστε ένα έγκυρο πιστοποιητικό SSL/TLS για να ενεργοποιήσετε ασφαλείς συνδέσεις.

2. Υποστήριξη Λειτουργίας Αποσύνδεσης (Logout)

- **Προδιαγραφή:** Η υπηρεσία πρέπει να υποστηρίζει τη λειτουργία αποσύνδεσης (logout).
- **Εξήγηση:** Η αποσύνδεση είναι ουσιώδης για την εμπειρία του SSO. Όταν ένας χρήστης αποσυνδέεται από μια εφαρμογή, πρέπει να αποσυνδέεται και από όλες τις ενσωματωμένες εφαρμογές. Αυτό εξασφαλίζει ότι δεν μπορεί να προκύψει μη εξουσιοδοτημένη πρόσβαση αν ένας χρήστης αφήσει τη συνεδρία του χωρίς επίβλεψη.
- **Εξήγηση:** Η αποσύνδεση είναι ουσιώδης για την λειτουργικότητα του SSO. Όταν ένας χρήστης αποσυνδέεται από μια εφαρμογή, πρέπει να επικοινωνείται η αποσύνδεση και στην Κεντρική Υπηρεσίας Πιστοποίησης.
- **Δράση:** Όταν ένας χρήστης αποσυνδέεται από την εφαρμογή σας, πρέπει να αποστέλλετε ένα αίτημα GET στη διεύθυνση https://sso-01.sch.gr/logout?service={η_διεύθυνση_της_υπηρεσίας_σας_εδώ}

3. Μοναδικό URL ανά Υπηρεσία

- **Προδιαγραφή:** Η διεύθυνση URL που παρέχετε για την εγγραφή της υπηρεσίας στο SSO πρέπει να είναι μοναδική για κάθε εφαρμογή. Διάφορες εφαρμογές δεν πρέπει να χρησιμοποιούν την ίδια διεύθυνση URL.
- **Εξήγηση:** Για να διατηρηθεί μια καθαρή και οργανωμένη ενσωμάτωση των εφαρμογών στο SSO του ΠΣΔ, κάθε εφαρμογή πρέπει να έχει μοναδική διεύθυνση URL της υπηρεσίας. Αυτή η μοναδικότητα αποτρέπει τυχόν συγκρούσεις και εξασφαλίζει ότι το SSO του ΠΣΔ μπορεί να διακρίνει μεταξύ διαφορετικών εφαρμογών.
- **Δράση:** Κατά την εγγραφή της υπηρεσίας σας στο SSO του ΠΣΔ, παράσχετε μια μοναδική διεύθυνση URL που αντιστοιχεί στην εφαρμογή σας. Για παράδειγμα, αν έχετε δύο εφαρμογές, “app01” και “app02,” που φιλοξενούνται στον ίδιο τομέα, βεβαιωθείτε ότι εγγράφονται με διακριτές διευθύνσεις URL της υπηρεσίας, όπως:

- App01: <https://example.sch.gr/app01>
- App02: <https://example.sch.gr/app02>

4. Χρήση ενός συμβατού πρωτοκόλλου για τη διασύνδεση.

Τα υποστηριζόμενα πρωτόκολλα είναι τα ακόλουθα: CAS, OIDC, SAML 2.0. Το προτεινόμενο πρωτόκολλο διασύνδεσης είναι το CAS 3.0:

- **Προδιαγραφή:** Βεβαιωθείτε ότι η υπηρεσία σας χρησιμοποιεί την τελευταία σταθερή έκδοση μιας βιβλιοθήκης CAS Client που είναι συμβατή με το SSO του ΠΣΔ για την γλώσσα προγραμματισμού σας. Για παράδειγμα, τον Java CAS Client 4.0 ή τον PHP CAS Client 1.6.
- **Εξήγηση:** Η διατήρηση της βιβλιοθήκης CAS Client σε ενημερωμένη κατάσταση είναι απαραίτητη για τη διατήρηση της συμβατότητας με το SSO του ΠΣΔ. Οι νεότερες εκδόσεις μπορεί να περιλαμβάνουν σημαντικές ενημερώσεις ασφαλείας, διορθώσεις σφαλμάτων και βελτιώσεις που ενισχύουν την αξιοπιστία και την ασφάλεια της ενσωμάτωσης.
- **Δράση:** Ελέγξτε την επίσημη λίστα των CAS Clients που παρέχεται από το έργο CAS για την τελευταία σταθερή έκδοση που αντιστοιχεί στη γλώσσα προγραμματισμού σας. Μια ενδεικτική λίστα CAS Clients μπορεί να βρεθεί [εδώ](#). Βεβαιωθείτε ότι η υπηρεσία σας χρησιμοποιεί τη συνιστώμενη έκδοση του CAS Client για μια ομαλή και ασφαλή ενσωμάτωση με το SSO του ΠΣΔ.

Σε περίπτωση που δεν μπορεί να χρησιμοποιηθεί το CAS πρωτόκολλο τότε μπορεί να χρησιμοποιηθούν τα πρωτόκολλα OIDC και SAML.