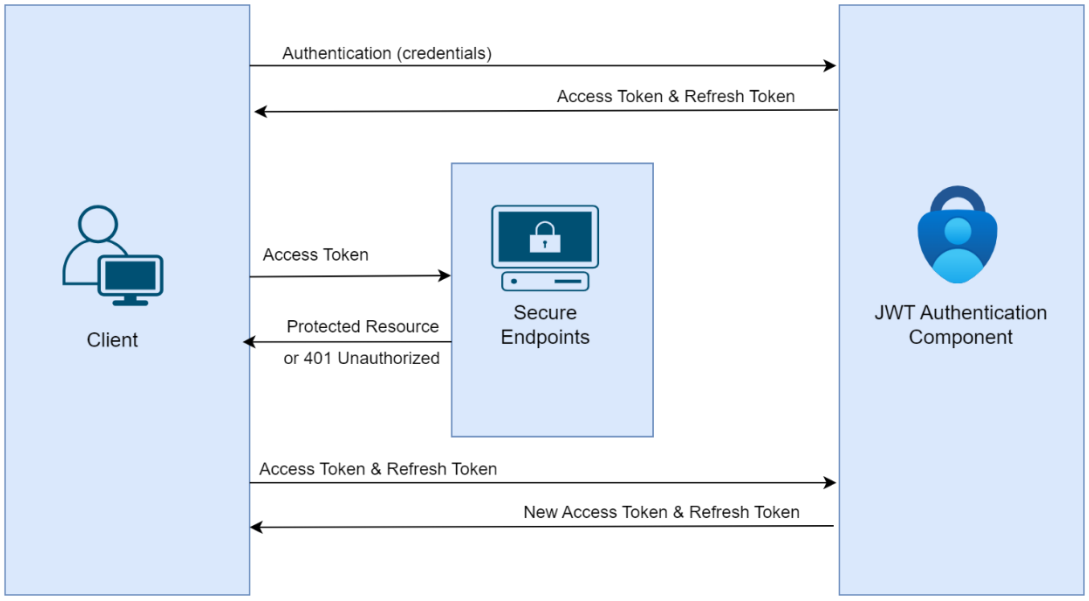
Χρήση Υπηρεσιών Διαλειτουργικότητας - Web API (REST) - Αυθεντικοποίηση μέσω JWT tokens

Περιγραφή αυθεντικοποίησης για τη χρήση των Υπηρεσιών Διαλειτουργικότητας - Web API (Services API)

Τα services που παρέχονται χρησιμοποιούν authentication μέσω της χρήσης JWT access tokens, καθώς και refresh tokens για τη διευκόλυνση της χρήσης και ελαχιστοποίηση των φορών που χρειάζεται ο χρήστης να δώσει τα διαπιστευτήριά του. Στο διάγραμμα παρακάτω απεικονίζεται η λειτουργία της αυθεντικοποίησης με τη χρήση των JWT access tokens.



Περιγραφή ορθής χρήσης

Για την ορθή χρήση της λειτουργίας αυθεντικοποίησης της πρόσβασης στις υπηρεσίες μας πρέπει να ακολουθηθούν τα παρακάτω βήματα:

1) Απόκτηση πρόσβασης

   Ο χρήστης στέλνει τα διαπιστευτήριά του και αν αυτά είναι σωστά λαμβάνει ένα JWT access Token και ένα refresh token. Το access token έχει διάρκεια ζωής 3 ωρών, ενώ το refresh token 7 ημερών. Οι διάρκειες αυτές δύναται να αλλάξουν κατόπιν ενημέρωσης.

   Action endpoint: api/authentication

2) Κλήση για πρόσβαση σε προστατευμένους πόρους

Σε κάθε επόμενη κλήση συμπεριλαμβάνεται στην κεφαλίδα (header) το access token.

3) Αποτυχία κλήσης και αίτημα για refresh token

   Αν το access token έχει λήξει (έχουν παρέλθει οι 3 ώρες), τότε επιστρέφεται 401 Unauthorized. Σε αυτή την περίπτωση μπορεί να γίνει αίτημα για νέο access token, χωρίς να δοθούν εκ νέου τα διαπιστευτήρια, στέλνοντας το παλιό access token μαζί με το refresh token του. Το νέο access token, μπορεί να χρησιμοποιηθεί για να πραγματοποιηθεί η κλήση που απέτυχε, καθώς και όλες οι επόμενες κλήσεις.

   Action endpoint: api/authentication/refresh

4) Αποτυχία κλήσης αιτήματος refresh token

   Αν το refresh token έχει λήξει, δηλαδή έχουν παρέλθει 7 ημέρες από την ώρα που δημιουργήθηκε και αποστάλθηκε, τότε θα επιστραφεί 401 Unauthorized. Σε αυτή την περίπτωση, θα πρέπει να επαναληφθεί το βήμα 1 για να αποκτηθεί ένα νέο access token, δίνοντας τα διαπιστευτήρια.

   - Failed endpoint: api/authentication/refresh
   - Action endpoint: api/authentication

5) Αποσύνδεση (προαιρετική)

   Στην κλήση αποσύνδεσης πρέπει να αποστέλλεται και το refresh token, το οποίο θα ανακληθεί (γίνει revoked). Με την ανάκληση μειώνεται η διάρκεια χρήσης του token στη διάρκεια ζωής του access token (3 ώρες), αντί των 7 ημερών του refresh token. Προφανώς, μετά από κάθε αποσύνδεση πρέπει η διαδικασία πρόσβασης να ξεκινήσει πάλι από το 1ο βήμα.

   - Action endpoint: api/authentication/logout

Προβλεπόμενη χρήση

Με βάση τις παραπάνω δυνατότητες, η ορθή χρήση για «συνεχόμενη λειτουργία» εμπεριέχει:

- Χρήση Authentication -> Λήψη Access και Refresh Token
- Τήρηση Access και Refresh Token και χρήση του Access Token για τις επόμενες 3 ώρες
- Κάθε 3 ώρες ή όποτε χρειαστεί (Response 401) εντός των 7 ημερών από την τελευταία λήψη token: Χρήση Refresh -> Λήψη νέων Access και Refresh Token

!Προσοχή: το σύνολο των κλήσεων εμπεριέχει έλεγχο ορθής χρήσης και περιορισμό κλήσεων και σε όποια περίπτωση γίνει υπέρβαση επιστρέφεται 429 Too Many Requests.

Λανθασμένη χρήση

Παρακάτω παρατίθενται κάποια παραδείγματα λανθασμένης χρήσης.

1) Για κάθε κλήση λαμβάνεται πρώτα ένα access token.

   κλήση για access token, κλήση με το access token, κλήση για access token, κλήση με το access token…

2) Λαμβάνεται αρχικά ένα access token και έπειτα για κάθε κλήση ζητείται πρώτα ένα refresh token.

   κλήση για access token, κλήση με το access και refresh token για να πάρω νέο access token, κλήση με το νέο access token, κλήση με το access και refresh token για να πάρω νέο access token, κλήση με το νέο access token…

Σημείωση: Ο γενικός κανόνας είναι ότι αποφεύγεται να γίνεται κλήση για λήψη access token αν δεν είναι αυτό απαραίτητο.