ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

ΚΕΝΤΡΟ ΔΙΑΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑΣ

Κέντρο Διαλειτουργικότητας

Υπηρεσία Αυθεντικοποίησης υπαλλήλων Φορέων με την χρήση Κωδικών Δημόσιας Διοίκησης (oAuth2.0.PA)

Version 2.5 – 08/08/2024

Πίνακας περιεχομένων

1. Περιγραφή

Η διαδικτυακή υπηρεσία ***Αυθεντικοποίησης υπαλλήλων Φορέων με την χρήση Κωδικών Δημόσιας Διοίκησης (oAuth2.0.PA)*** (στο εξής θα αναφέρεται ως υπηρεσία Αυθεντικοποίησης Χρηστών oAuth2.0_PA) μπορεί να χρησιμοποιηθεί από τους Φορείς του Δημοσίου σε εφαρμογές διαδικτύου.

Κάθε Φορέας ο οποίος έχει ανάγκη πιστοποίησης των υπαλλήλων του σε εφαρμογές διαδικτύου, μπορεί να αξιοποιήσει την υπηρεσία ***Αυθεντικοποίησης Χρηστών oAuth2.0_PA***, μέσω της οποίας χρησιμοποιούνται με ασφαλή τρόπο τα διαπιστευτήρια που έχει εκδόσει ο υπάλληλος για αυτήν τη χρήση.

Η υπηρεσία ***Αυθεντικοποίησης Χρηστών oAuth2.0_PA*** επιστρέφει στον Φορέα ως πληροφορία το ΑΦΜ και βασικά στοιχεία του χρήστη (όπως Όνομα, Επώνυμο, Πατρώνυμο, Μητρώνυμο, username).

Η υπηρεσία ***Αυθεντικοποίησης Χρηστών oAuth2.0_PA*** έχει υλοποιηθεί με βάση το πρωτόκολλο oAuth2.0.

Για τη χρήση της υπηρεσία διατίθενται τα παρακάτω :

Πιλοτικό περιβάλλον : https://test.gsis.gr/oauth2servergov

userAuthorizationUri=https://test.gsis.gr/oauth2servergov/oauth/authorize
accessTokenUri=https://test.gsis.gr/oauth2servergov/oauth/token
oauth2serverUserInfoURL=https://test.gsis.gr/oauth2servergov/userinfo?format=xml
logoutUrl=https://test.gsis.gr/oauth2servergov/logout

Παραγωγικό περιβάλλον : https://oauth2.gsis.gr/oauth2servergov

userAuthorizationUri=https://oauth2.gsis.gr/oauth2servergov/oauth/authorize
accessTokenUri=https://oauth2.gsis.gr/oauth2servergov/oauth/token
oauth2serverUserInfoURL=https://oauth2.gsis.gr/oauth2servergov/userinfo?format=xml
logoutUrl=https://oauth2.gsis.gr/oauth2servergov/logout

2. Υλοποίηση του oAuth2.0 client protocol

Για να χρησιμοποιήσει ο Φορέας την υπηρεσία ***Αυθεντικοποίησης Χρηστών oAuth2.0_PA*** θα πρέπει να αναπτύξει μια εφαρμογή-πελάτη (client) σύμφωνα με τις απαιτήσεις του πρωτοκόλλου oAuth2.0.

Η εφαρμογή-πελάτης θα ενσωματωθεί στο πληροφοριακό σύστημα ή στην εφαρμογή του Φορέα και θα ανακατευθύνει τον χρήστη στο Κέντρο Διαλειτουργικότητας (ΚΕ.Δ) όπου εισάγει τα υπηρεσιακά διαπιστευτήρια – **προσοχή όχι τα ατομικά διαπιστευτήρια του υπαλλήλου στο taxisnet** - στην κατάλληλη οθόνη. Στην συνέχεια μετά την σύμφωνη γνώμη του χρήστη επιστρέφει στον Φορέα ως πληροφορία το ΑΦΜ και βασικά στοιχεία του χρήστη (Όνομα, Επώνυμο, Πατρώνυμο, Μητρώνυμο, username ή Επωνυμία, username). Το username αφορά περιγραφή του χρήστη και όχι το username στο taxisnet

Τα πεδία που επιστρέφει η εφαρμογή είναι:

ΑΦΜ	char(12 char)
ΕΠΩΝΥΜΟ	varchar2(45 char)
ΟΝΟΜΑ	varchar2(20 char)
ΠΑΤΡΩΝΥΜΟ	varchar2(20 char)
ΜΗΤΡΩΝΥΜΟ	varchar2(20 char)
USERNAME	varchar2(256 byte)
ΕΤΟΣ	number(4)

Ο Φορέας θα πρέπει στην υλοποίηση της εφαρμογής-πελάτη να ενσωματώσει το πρωτόκολλο oAuth2.0 (oAuth2 client protocol). Το Κέντρο Διαλειτουργικότητας (ΚΕ.Δ) παρέχει μια δοκιμαστική εφαρμογή-πελάτη (oAuth2 client demo) για τη διευκόλυνση των Φορέων στην ενσωμάτωση του πρωτοκόλλου oAuth2.0.

Περισσότερα μπορείτε να βρείτε στο τεχνικό εγχειρίδιο της υπηρεσία «Αυθεντικοποίηση Χρηστών oAuth2.0».

2.1 Υποβολή Αιτήματος Χρήσης της Υπηρεσίας στην ΕΔΑ

Ο Φορέας υποβάλλει αίτημα στην Εφαρμογή Διαχείρισης Αιτημάτων Διαλειτουργικότητας (ΕΔΑ) για την χρήση της υπηρεσίας ***Αυθεντικοποίησης Χρηστών oAuth2.0_PA***.

Στο αίτημα ο Φορέας καταχωρεί στην ΕΔΑ το URL του πληροφοριακού συστήματος που κάνει κλήση της υπηρεσίας για το πιλοτικό και το παραγωγικό περιβάλλον, π.χ. https://myserver.mydomain.gr/myoauth2PAclient/myUserInfo

Θα πρέπει να συμπληρωθεί αναλυτικά ο σκοπός χρήσης του αιτήματος ως προς την Εφαρμογή που θα αξιοποιήσει την υπηρεσία oAuth2.0_PA.

Μετά την έγκριση του αιτήματος για την πιλοτική λειτουργία, ο Φορέας δημιουργεί μέσω της ΕΔΑ τους κωδικούς (username και password) που θα χρησιμοποιήσει για την κλήση της υπηρεσίας κατά τη διάρκεια των δοκιμών.

Συγκεκριμένα ανοίγοντας το αίτημα και επιλέγοντας από την αριστερή στήλη την επιλογή «Χρήστες Υπηρεσιών» μπορεί να δηλώσει το password του πιλοτικού χρήστη που του δίνεται.

Μετά την έγκριση του αιτήματος για την παραγωγική λειτουργία, ο Φορέας δημιουργεί μέσω της ΕΔΑ τους κωδικούς (username και password) που θα χρησιμοποιήσει για την κλήση της υπηρεσίας για την παραγωγική λειτουργία της εφαρμογής του.

Αναλυτικά η διαδικασία υποβολής αιτήματος αναφέρεται στις Οδηγίες χρήσης «Ε.Δ.Α. Διαλειτουργικότητας: Εφαρμογή Διαχείρισης Αιτημάτων Διαλειτουργικότητας», Κεφάλαιο 4.

2.2 Έκδοση Υπηρεσιακών Διαπιστευτηρίων

Για να δημιουργήσει ένας υπάλληλος υπηρεσιακά διαπιστευτήρια (λογαριασμό δημόσιας διοίκησης) θα πρέπει να εισέλθει με τους προσωπικούς του κωδικούς Taxisnet στη εφαρμογή https://webapps.gsis.gr/dsae/govuser και ακολουθώντας τις οδηγίες της υπηρεσίας Κωδικοί Δημόσιας Διοίκησης να δημιουργήσει τα νέα υπηρεσιακά διαπιστευτήρια.

2.3 Αποσύνδεση Εφαρμογής

Για λόγους ασφάλειας προτείνεται να γίνεται πάντοτε αποσύνδεση της εφαρμογής ώστε να μην παραμένει συνδεδεμένος ο χρήστης στον φυλλομετρητή.

Η αποσύνδεση της εφαρμογής μπορεί να γίνει με τον εξής τρόπο:

Με browser redirect – **όχι με GET/POST** - στο logout url όπου ορίζεται το αντίστοιχο path για να γίνεται redirection σε σελίδα της εφαρμογής-πελάτη. Το αντίστοιχο path της σελίδας θα πρέπει να συμφωνεί με το domain name που έχει δηλωθεί στην ΕΔΑ.

Δηλαδή σε url της μορφής:

https://test.gsis.gr/oauth2servergov/logout/{clientId}/?url=https://xxx.gr/….

(για το πιλοτικό περιβάλλον) και στο

https://www1.gsis.gr/oauth2servergov/logout/{clientId}/?url=https://xxx.gr/….

(για το παραγωγικό περιβάλλον),

όπου το τμήμα ***'?url=https://xxx.gr/…'*** είναι το redirection url για το logout που θα πρέπει να συμφωνεί με το domain name που έχει δηλωθεί στην ΕΔΑ.

3. Περιγραφή του flow της υπηρεσίας Oauth2.0_PA

Το Oauth2.0_PA flow έχει 3 βήματα που αντιστοιχούν σε 3 endpoint, όπως φαίνεται παρακάτω (.properties αρχείο στο demo java oauth2.0 client):

Call Gsis TEST - PILOT
#Identification FOREA
clientId=<Pilot User name created by system on your request>
clientSecret=<Pilot Password created on your request>
oauth2serverUserInfoURL=https://test.gsis.gr/oauth2servergov/userinfo?format=xml
accessTokenUri=https://test.gsis.gr/oauth2servergov/oauth/token
userAuthorizationUri=https://test.gsis.gr/oauth2servergov/oauth/authorize
debugMode=false

Μετά το 1ο βήμα καλώντας στο https://test.gsis.gr/oauth2servergov/oauth/authorize το οποίο κάνει browser redirect και στο οποίο βάζουμε στη φόρμα τα taxinet credentials, παίρνουμε το "code".

Με αυτό το code + client_id + client_secret + redirect_url **(τα ζεύγη client_id + client_secret τα ενεργοποιούμε μέσα από την Εφαρμογή Διαχείρισης Αιτημάτων – ΕΔΑ, 1 ζευγάρι για τον πιλοτικό χρήστη και 1 ζευγάρι για τον παραγωγικό, και αντίστοιχα δηλώνουμε 1 redirect_url για το πιλοτικό και 1 για το παραγωγικό)** πάμε στο 2ο βήμα και καλούμε το https://test.gsis.gr/oauth2servergov/oauth/token .

Παράδειγμα με curl παρακάτω:

```
curl -X POST 'https://test.gsis.gr/oauth2servergov/oauth/token' \
-H 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'client_id=*******' \
--data-urlencode 'client_secret=*******' \
--data-urlencode 'code=V1YEAW' \
--data-urlencode 'state=PEH5Nb_hpQnZpdzxdI20N' \
--data-urlencode 'scope=read' \
--data-urlencode 'grant_type=authorization_code' \
--data-urlencode 'redirect_uri=**********************'
```

Αφού πάρουμε το token πάμε στο 3ο βήμα και καλούμε το https://test.gsis.gr/oauth2servergov/userinfo?format=xml για να πάρουμε τα στοιχεία του χρήστη,

Παράδειγμα με curl παρακάτω:

```
curl https://test.gsis.gr/oauth2servergov/userinfo?format=xml -H "Authorization: Bearer ********-****-****-****-****************"
```

Προσοχή το scope να είναι πάντα read, το state είναι προαιρετικό, αν και οι περισσότερες αν όχι όλες οι client εφαρμογές το χρησιμοποιούν.

Στον παρακάτω σύνδεσμο μπορείτε να βρείτε βιβλιοθήκες και παραδείγματα για σχεδόν όλες τις γνωστές γλώσσες προγραμματισμού:

https://oauth.net/code/

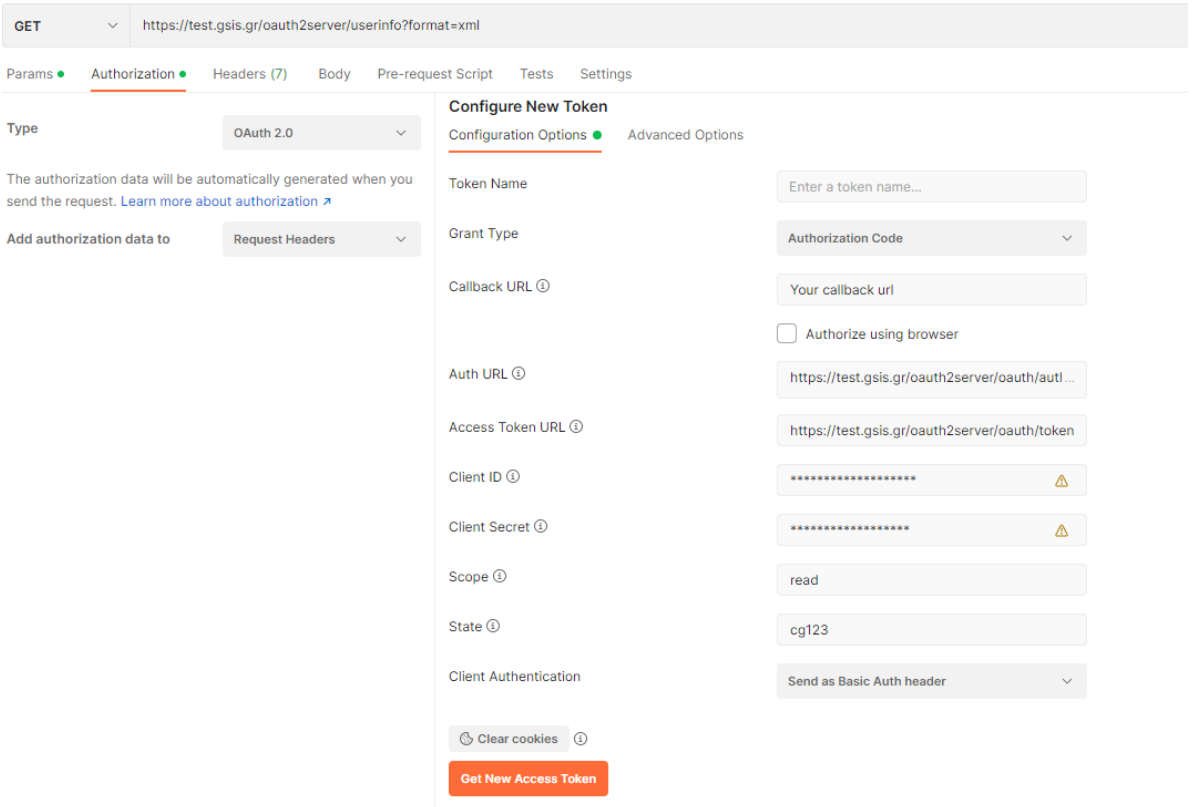
4. Χρήση εργαλείου Postman

Για διευκόλυνση στη διαδικασία υλοποίησης μπορείτε να χρησιμοποιήσετε το εργαλείο Postman. Ο Postman παρέχει έναν τρόπο για να εκτελέσετε εύκολα τον έλεγχο ενός τελικού σημείου για το οποίο έχει πραγματοποιηθεί έλεγχος ταυτότητας από το oAuth2.0_PA.

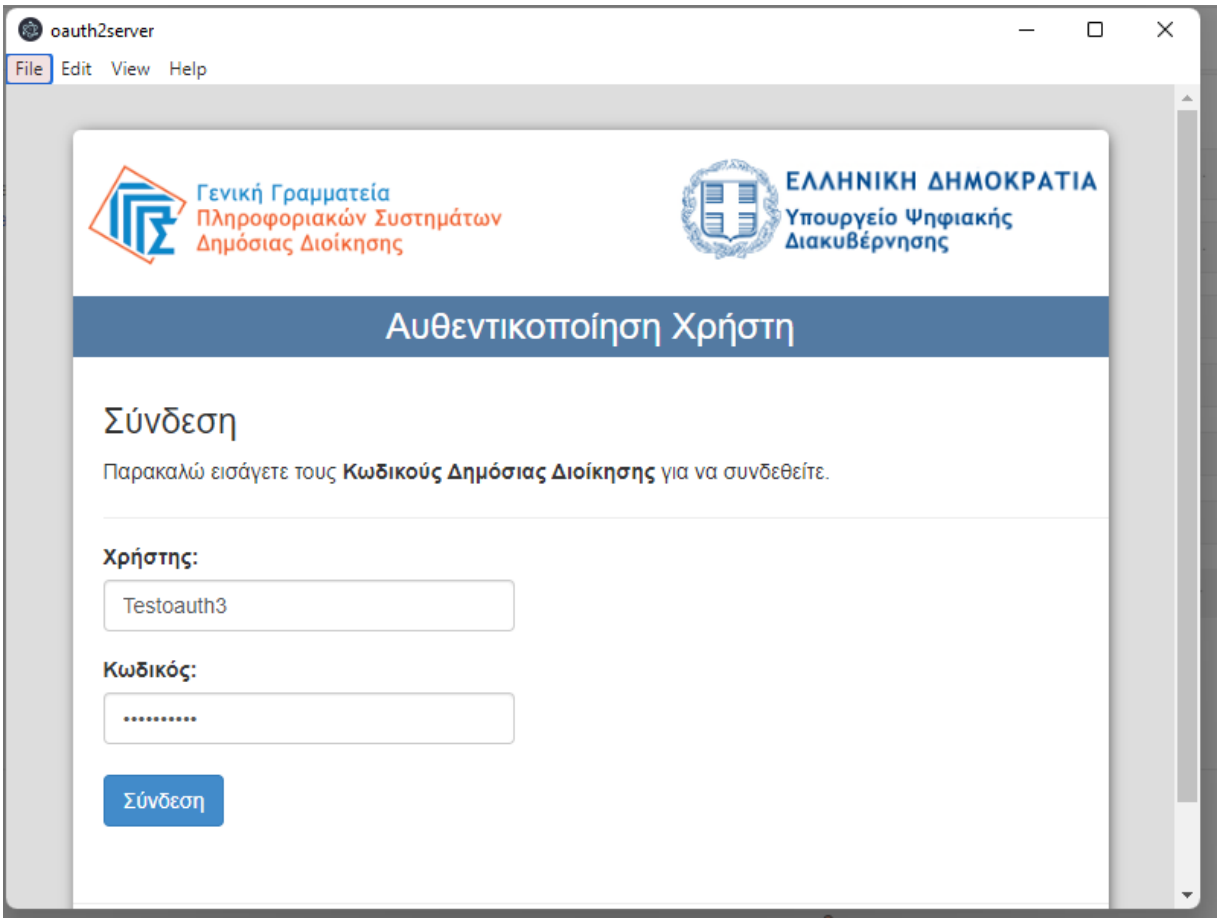
Παρακάτω είναι οι μεταβλητές που πρέπει να συμπληρώσετε:

Grant Type : Authorization Code
Callback URL : To url που έχετε δηλώσει στο αίτημα σας
Auth URL : https://test.gsis.gr/oauth2servergov/oauth/authorize
Access Token URL : https://test.gsis.gr/oauth2servergov/oauth/token
Scope : read
Client Id: To client_id του αιτήματος σας
Client Secret: To client_secret του αιτήματος σας

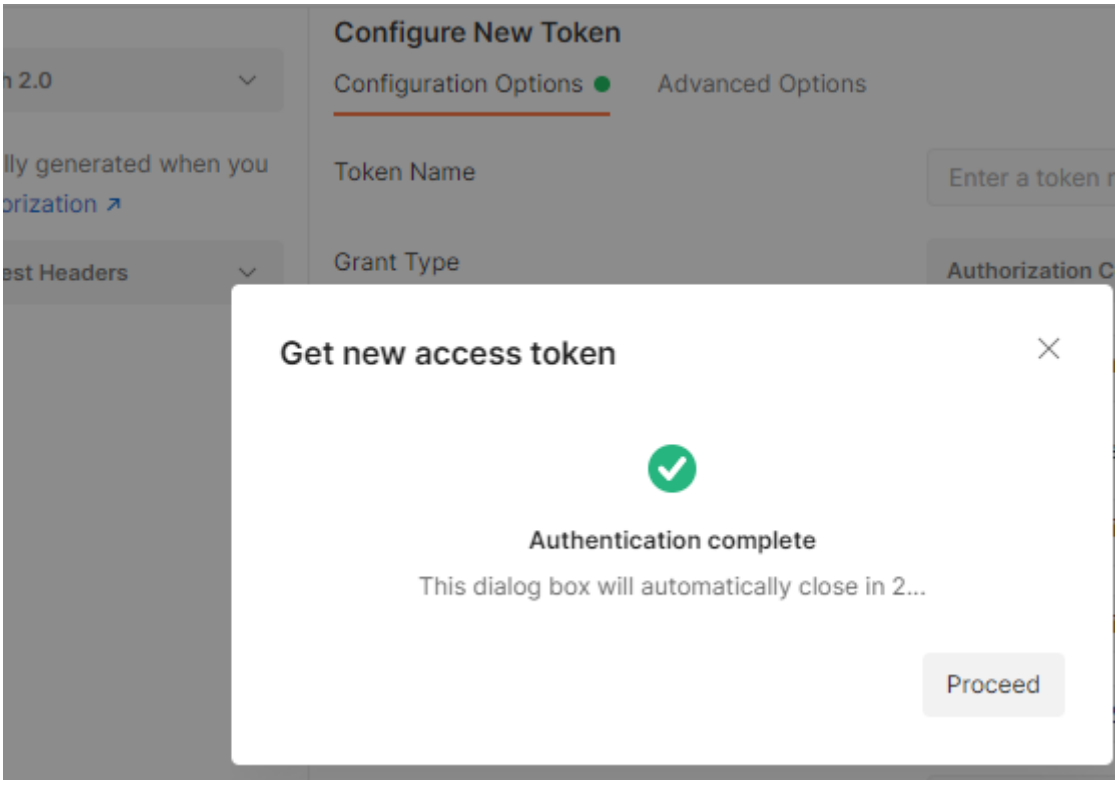
Με την συμπλήρωση των παραπάνω μπορείτε να πάρετε το Token, πατώντας το “Get New Access Token”.



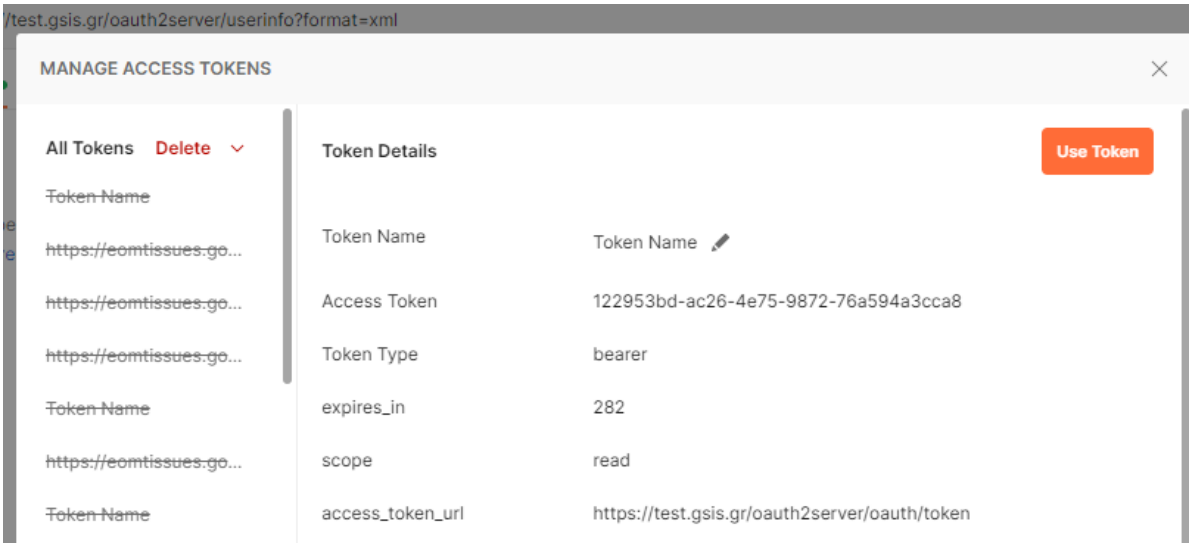
Σας παραπέμπει στην οθόνη για να δώσετε κωδικούς Taxisnet του χρήστη π.χ. Testoauth3/Testo@uth3



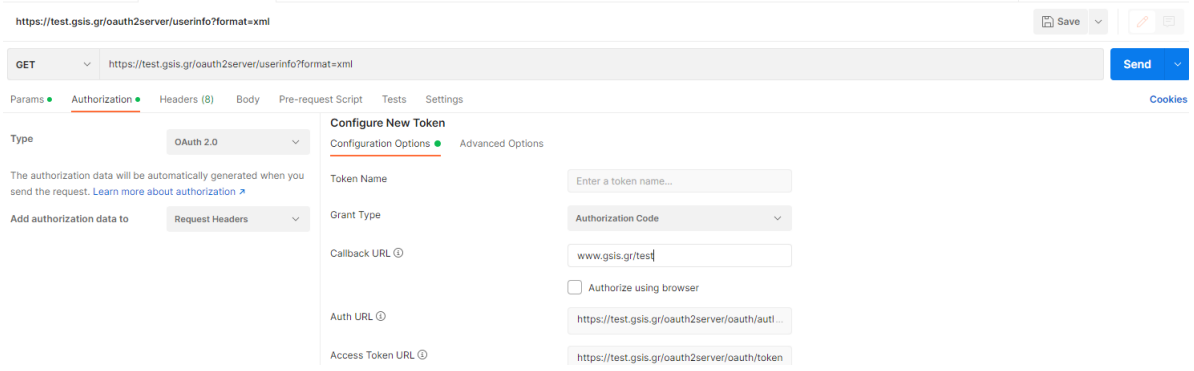
Αν τα στοιχεία που έχετε συμπληρώσει είναι σωστά εμφανίζεται το παρακάτω μήνυμα:



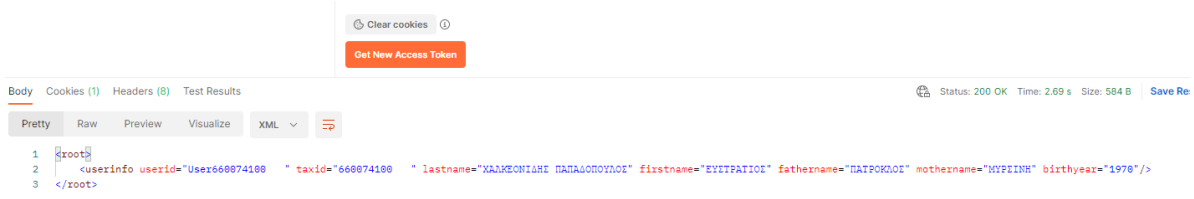
Και στην παρακάτω οθόνη επιλέγετε «Use Token»



Με αυτό το Token – το οποίο κρατιέται σε μεταβλητή και δεν χρειάζεται να το επανεκδίδουμε συνέχεια - μπορείτε να κάνετε την τελευταία κλήση, το URL της οποίας είναι το:
https://test.gsis.gr/oauth2servergov/userinfo?format=xml και το βάζουμε στην πάνω μπάρα.



Με αυτή την κλήση ολοκληρώνεται η διαδικασία της αυθεντικοποίησης Oauth2.0_PA και πλέον έχετε στη διάθεση σας τα στοιχεία που επιστρέφονται σε μια δομή δεδομένων XML.



5. Δοκιμαστικοί χρήστες

Για δοκιμή της υπηρεσίας μπορείτε να χρησιμοποιήσετε τους παρακάτω χρήστες:

USERNAME	PASSWORD	ΑΦΜ
Testoauth3	Testo@uth3	660074100
Testoauth4	Testo@uth4	660074111
Testoauth5	Testo@uth5	660074123
Testoauth6	Testo@uth6	660074135
Testoauth7	Testo@uth7	660074147

6. Αρχείο Καταγραφής Κλήσεων

Σύμφωνα με την Πολιτική Ορθής Χρήσης Διαδικτυακών Υπηρεσιών του Υπουργείου Ψηφιακής Διακυβέρνησης για την υπηρεσία Αυθεντικοποίηση υπαλλήλων Φορέων (oAuth2.0.PA) στο Αρχείο Καταγραφής κλήσεων θα πρέπει να τηρούνται τα παρακάτω:

Α/Α	Περιγραφή
1	ο μοναδικός αύξων αριθμός κλήσης στο Πληροφοριακό Σύστημά του
2	η ημερομηνία και ώρα της κλήσης
3	τα στοιχεία του χρήστη
4	Η Ip του χρήστη