

Αυθεντικοποίηση Χρηστών

Η υπηρεσία Login είναι βασισμένη στο πρότυπο OAuth 2.0 protocol (<http://tools.ietf.org/html/draft-ietf-oauth-v2-12>).

Το OAuth 2.0 περιγράφει ένα σύνολο μεθόδων για την απόκτηση ενός Access Token από τρίτες εφαρμογές.

Το Access Token αντιπροσωπεύει την άδεια του χρήστη, και χρησιμοποιείται για την πρόσβαση στα δεδομένα του από τρίτες εφαρμογές.

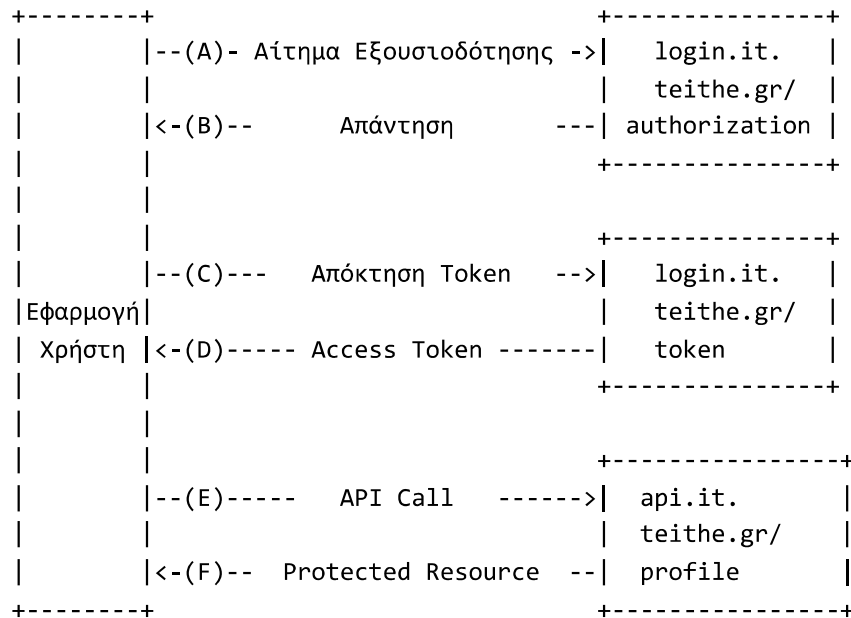
Το OAuth 2.0 περιγράφει 5 τύπους απόκτησης ενός Access Token:

1. Authorization code (Server Side εφαρμογές)
2. Implicit (Client Side (browser) εφαρμογές)
3. Resource owner credentials
4. Client credentials
5. Refresh token

Το IT LOGIN υποστηρίζει **Authorization code**, **Implicit**, **Refresh token** και **Client credentials**.

Λήψη ενός Access Token

1. Authorization code (Server Side εφαρμογές)



A. Αίτημα Εξουσιοδότησης

Ανακατευθυνση του χρήστη στο URL Εξουσιοδότησης

```
https://login.it.teithe.gr/authorization/?client_id=CLIENT_ID&response_type=code&scope=SCOPE1,SCOPE2&redirect_uri=REDIRECT_URL
```

client_id : Client ID της εφαρμογής. Δημιουργείται από το μενού "Οι εφαρμογές μου". | Υποχρεωτική παράμετρος

response_type : Για το Authorization code θα πρέπει να έχει την τιμή "code". | Υποχρεωτική παράμετρος

scope : Λίστα με τις διαθέσιμες τιμές μπορεί να βρεθεί εδώ (/apps/doc/scope). Μπορείτε να ορίσετε παραπάνω από μια πρόσβαση κάθε φορά, π.χ &scope=id,cn | Υποχρεωτική παράμετρος

redirect_uri : URL επιστροφή στην εφαρμογή. Θα πρέπει να είναι στην λίστα των URL που δηλώσατε κατά την δημιουργία της εφαρμογής σας. | Υποχρεωτική παράμετρος

state : CSRF (https://en.wikipedia.org/wiki/Cross-site_request_forgery) token. Η τιμή που θα ορίσετε σε αυτό το πεδίο θα επιστραφεί στο URL επιστροφής που έχετε ορίσει για την εφαρμογή. | Προαιρετική παράμετρος

Σε αυτή την φάση ο χρήστης θα πρέπει να συνδεθεί και στην συνέχεια να αποδεχτεί η να απορίψει την πρόσβαση που ζητάει η εφαρμογή.

B. Απάντηση

Αν ο χρήστης δεχτεί την πρόσβαση που ζηται η εφαρμογή τότε θα μεταφερθεί στο URL επιστροφής με μια παράμετρο code που η τιμή της θα χρησιμοποιηθεί στο βήμα Γ για την απόκτηση Access Token.

```
http://your-redirect-uri?code=CODE
```

Αν ο χρήστης απορρίψει την πρόσβαση στην εφαρμογή τότε θα μεταφερθεί πάλι στο URL επιστροφής με τις παραμέτρους error,error_reason,error_description.

```
http://your-redirect-uri?error=access_denied&error_reason=user_denied&error_description=Permission+Denied
```

Θα πρέπει να διαχειριστείτε στην εφαρμογή σας αυτή την κατάσταση.

Αν ο χρήστης δεν δεχτεί να δώσει πρόσβαση στην εφαρμογή, τότε δεν θα μπορέσετε να αποκτήσετε πρόσβαση στο Access Token.

C. Απόκτηση Token

Σε αυτό το βήμα θα πρέπει να ανταλλάξετε το code που λάβατε στο προηγούμενο βήμα με ένα Access Token.

Η εφαρμογή θα πρέπει να στείλει ένα POST request (Content-Type: application/x-www-form-urlencoded) στο 'https://login.it.teithe.gr/token' συμπεριλαμβάνοντας:

client_id : Client ID της εφαρμογής. Δημιουργείται από το μενού "Οι εφαρμογές μου". | Υποχρεωτική παράμετρος

client_secret : Client Secret της εφαρμογής. | Υποχρεωτική παράμετρος

grant_type : Για το Authorization code θα πρέπει να έχει την τιμή "authorization_code". | Υποχρεωτική παράμετρος

code : Την τιμή code που λάβατε στο προηγούμενο βήμα. | Υποχρεωτική παράμετρος

D. Access Token

Αν όλα τα στοιχεία ήταν σωστά τότε η απάντηση θα είναι σε μορφή JSON ως εξής:

```
{
  "access_token": "ACCESS TOKEN VALUE",
  "user": "USER ID"
}
```

access_token : Το Access Token λήγει σε 2 λεπτά από την έκδοση του.

user : Μοναδικό αναγνωριστικό χρήστη.

Αν υπήρξε κάποιο σφάλμα η απάντηση είναι πάλι ένα JSON object ως εξής:

```
{
  "error": {
    "message": "Human readable message.",
    "code": CODE_NUMBER
  }
}
```

message : Κείμενο με την περιγραφή του σφάλματος.

code : Κωδικός σφάλματος.

E. Api Call

Με το Access Token που λάβατε στο προηγούμενο βήμα κάντε αιτήσεις στο <https://api.it.teithe.gr>. Για περισσότερες πληροφορίες πατήστε εδώ (https://github.com/apavliidi/IT_API/wiki/API-Documentation).

Παράδειγμα:

```
curl -X GET \
  -H "x-access-token: ACCESS_TOKEN" \
  -H "Content-Type:application/json" \
  api.it.teithe.gr/profile
```

F. Απάντηση

Αν το Access Token ισχύει τότε θα λάβετε ως απάντηση ένα JSON Object ως εξής:

```
{
  "am": "123456",
  "regyear": "2012",
  "regsem": "2",
  "sem": "2",
  "givenName;lang-el": "ΓΕΩΡΓΙΟΣ",
  "sn;lang-el": "ΠΑΠΑΔΟΠΟΥΛΟΣ",
  "fathersname;lang-el": "ΙΩΑΝΝΗ",
  "eduPersonAffiliation": "student",
  "eduPersonPrimaryAffiliation": "it",
  "title": "Undergraduate Student",
  "title;lang-el": "Προπτυχιακός Φοιτητής",
  "cn;lang-el": "ΓΕΩΡΓΙΟΣ ΠΑΠΑΔΟΠΟΥΛΟΣ",
  "cn": "GEORGIOS PAPADOPOULOS",
  "sn": "PAPADOPOULOS",
  "givenName": "GEORGIOS",
  "fathersname": "IOANNH",
  "secondarymail": "-",
  "telephoneNumber": "0",
  "labeledURI": "-",
  "id": "1234",
  "mail": "mail@mail.com",
  "pwdChangedTime": "20180808152441Z",
  "socialMedia": {
    "socialMediaExtra": []
  },
  "profilePhoto": ""
}
```

Επιστρέφει τα στοιχεία του χρήστη.

Αν το Access Token δεν ισχύει τότε θα λάβετε ως απάντηση ένα JSON Object ως εξής:

```
{
  "error": {
    "message": "Human readable message.",
    "type": "ERRORTYPE"
    "code": CODE NUMBER
  }
}
```

2. Implicit (Client Side (browser) εφαρμογές)

```
+-----+
|      |--(A)- Αίτημα Εξουσιοδότησης ->| login.it.  |
|      |                                | teithe.gr/ |
|      |<-(B)-- Απάντηση Token      ---| authorization |
|      |                                +-----+
|Εφαρμογή|
|Χρήστη |                                +-----+
|      |--(C)----- API Call  ----->| api.it.    |
|      |                                | teithe.gr/ |
|      |<-(D)-- Protected Resource  --| profile    |
|      |                                +-----+
```

A. Αίτημα Εξουσιοδότησης

Ανακατευθυνση του χρήστη στο URL Εξουσιοδότησης

```
https://login.it.teithe.gr/authorization/?client_id=CLIENT_ID&response_type=code&scope=SCOPE1,SCOPE2
```

client_id : Client ID της εφαρμογής. Δημιουργείται από το μενού "Οι εφαρμογές μου". | Υποχρεωτική παράμετρος

response_type : Για το Authorization code θα πρέπει να έχει την τιμή "code". | Υποχρεωτική παράμετρος

scope : Λίστα με τις διαθέσιμες τιμές μπορεί να βρεθεί εδώ (/apps/doc/scope). Αν δεν οριστεί η προεπιλεγμένη τιμή είναι "id". Μπορείτε να ορίσετε παραπάνω από μια πρόσβαση κάθε φορά, π.χ &scope=id,cn | Προαιρετική παράμετρος

state : CSRF (https://en.wikipedia.org/wiki/Cross-site_request_forgery) token. Η τιμή που θα ορίσετε σε αυτό το πεδίο θα επιστραφεί στο URL επιστροφής που έχετε ορίσει για την εφαρμογή. | Προαιρετική παράμετρος

Σε αυτή την φάση ο χρήστης θα πρέπει να συνδεθεί και στην συνέχεια να αποδεχτεί η να απορίψει την πρόσβαση που ζητάει η εφαρμογή.

B. Απάντηση

Αν ο χρήστης δεχτεί την πρόσβαση που ζητεί η εφαρμογή τότε θα μεταφερθεί στο URL επιστροφής με μια παράμετρο `access_token` που η τιμή της θα χρησιμοποιηθεί στο βήμα Γ για την απόκτηση Access Token.

```
http://your-redirect-uri#access_token=ACCESS_TOKEN
```

access_token : Το Access Token λήγει σε 2 λεπτά από την έκδοση του.

Αν ο χρήστης απορρίψει την πρόσβαση στην εφαρμογή τότε θα μεταφερθεί πάλι στο URL επιστροφής με τις παραμέτρους `error,error_reason,error_description`.

```
http://your-redirect-uri#error=access_denied&error_reason=user_denied&error_description=Permission+Denied
```

Θα πρέπει να διαχειριστείτε στην εφαρμογή σας αυτή την κατάσταση.

Αν ο χρήστης δεν δεχτεί να δώσει πρόσβαση στην εφαρμογή, τότε δεν θα μπορέσετε να αποκτήσετε πρόσβαση στο Access Token.

C. Api Call

Με το Access Token που λάβατε στο προηγούμενο βήμα μέσω του url κάντε αιτήσεις στο <https://api.it.teithe.gr>. Για περισσότερες πληροφορίες πατήστε εδώ (https://github.com/apavliidi/IT_API/wiki/API-Documentation).

Παράδειγμα:

```
curl -X GET \  
  -H "x-access-token: ACCESS_TOKEN" \  
  -H "Content-Type:application/json" \  
  api.it.teithe.gr/profile
```

D. Απάντηση

Αν το Access Token ισχύει τότε θα λάβετε ως απάντηση ένα JSON Object ως εξής:

```
{
  "am": "123456",
  "regyear": "2012",
  "regsem": "2",
  "sem": "2",
  "givenName;lang-el": "ΓΕΩΡΓΙΟΣ",
  "sn;lang-el": "ΠΑΠΑΔΟΠΟΥΛΟΣ",
  "fathersname;lang-el": "ΙΩΑΝΝΗ",
  "eduPersonAffiliation": "student",
  "eduPersonPrimaryAffiliation": "it",
  "title": "Undergraduate Student",
  "title;lang-el": "Προπτυχιακός Φοιτητής",
  "cn;lang-el": "ΓΕΩΡΓΙΟΣ ΠΑΠΑΔΟΠΟΥΛΟΣ",
  "cn": "GEORGIOS PAPADOPOULOS",
  "sn": "PAPADOPOULOS",
  "givenName": "GEORGIOS",
  "fathersname": "IOANNH",
  "secondarymail": "-",
  "telephoneNumber": "0",
  "labeledURI": "-",
  "id": "1234",
  "mail": "mail@mail.com",
  "pwdChangedTime": "20180808152441Z",
  "socialMedia": {
    "socialMediaExtra": []
  },
  "profilePhoto": ""
}
```

Επιστρέφει τα στοιχεία του χρήστη.

Αν το Access Token δεν ισχύει τότε θα λάβετε ως απάντηση ένα JSON Object ως εξής:


```
{
  "error": {
    "message": "Human readable message.",
    "type": "ERRORTYPE"
    "code": CODE NUMBER
  }
}
```

3. Refresh token

```
+-----+
|      |--(A)- Refresh Token ----->| login.it. |
|      |                               | teithe.gr/ |
|      |<-(B)-- Απάντηση Access Token-| authorization |
|      |                               +-----+
|Εφαρμογή|
|Χρήστη |                               +-----+
|      |--(C)----- API Call ----->| api.it.   |
|      |                               | teithe.gr/ |
|      |<-(D)-- Protected Resource --| profile   |
+-----+                               +-----+
```

A. Refresh Token

Σε αυτό το βήμα θα πρέπει να ανταλλάξετε το Refresh Token που λάβατε μαζί με το Access Token εφόσον η εφαρμογή σας έχει αυτή την πρόσβαση.

Η εφαρμογή σας θα πρέπει να στείλει ένα POST request (Content-Type: application/x-www-form-urlencoded) στο 'https://login.it.teithe.gr/token' συμπεριλαμβάνοντας:

client_id : Client ID της εφαρμογής. Δημιουργείται από το μενού "Οι εφαρμογές μου". | Υποχρεωτική παράμετρος

client_secret : Client Secret της εφαρμογής. | Υποχρεωτική παράμετρος

grant_type : Για το Refresh Token θα πρέπει να έχει την τιμή "refresh_token". | Υποχρεωτική παράμετρος

code : Το Refresh Token που λάβατε με το Access Token. | Υποχρεωτική παράμετρος

B. Access Token

Αν όλα τα στοιχεία ήταν σωστά τότε η απάντηση θα είναι σε μορφή JSON ως εξής:

```
{
  "access_token": "ACCESS_TOKEN_VALUE",
  "user": "USER_ID",
  "refresh_token": NEW_REFRESH_TOKEN
}
```

access_token : Το Access Token λήγει σε 2 λεπτά.

user : Μοναδικό αναγνωριστικό χρήστη.

refresh_token : Το καινούργιο Refresh Token.

Αν υπήρξε κάποιο σφάλμα η απάντηση είναι πάλι ένα JSON object ως εξής:

```
{
  "error": {
    "message": "Human readable message.",
    "code": CODE_NUMBER
  }
}
```

message : Κείμενο με την περιγραφή του σφάλματος.

code : Κωδικός σφάλματος.

C. Απάντηση

Αν ο χρήστης δεχτεί την πρόσβαση που ζηται η εφαρμογή τότε θα μεταφερθεί στο URL επιστροφής με μια παράμετρο `access_token` που η τιμή της θα χρησιμοποιηθεί στο βήμα Γ για την απόκτηση Access Token.

```
http://your-redirect-uri#access_token=ACCESS_TOKEN
```

access_token : Το Access Token λήγει σε 2 λεπτά από την έκδοση του.

Αν ο χρήστης απορρίψει την πρόσβαση στην εφαρμογή τότε θα μεταφερθεί πάλι στο URL επιστροφής με τις παραμέτρους `error,error_reason,error_description`.

```
http://your-redirect-uri#error=access_denied&error_reason=user_denied&error_description=Permission+Denied
```

Θα πρέπει να διαχειριστείτε στην εφαρμογή σας αυτή την κατάσταση.

Αν ο χρήστης δεν δεχτεί να δώσει πρόσβαση στην εφαρμογή, τότε δεν θα μπορέσετε να αποκτήσετε πρόσβαση στο Access Token.

D. Api Call

Με το Access Token που λάβατε στο προηγούμενο βήμα μέσω του url κάντε αιτήσεις στο <https://api.it.teithe.gr>. Για περισσότερες πληροφορίες πατήστε εδώ (https://github.com/apavliidi/IT_API/wiki/API-Documentation).

Παράδειγμα:

```
curl -X GET \  
  -H "x-access-token: ACCESS_TOKEN" \  
  -H "Content-Type:application/json" \  
  api.it.teithe.gr/profile
```

E. Απάντηση

Αν το Access Token ισχύει τότε θα λάβετε ως απάντηση ένα JSON Object ως εξής:

Επιστρέφει τα στοιχεία του χρήστη.

Αν το Access Token δεν ισχύει τότε θα λάβετε ως απάντηση ένα JSON Object ως εξής:

```
{  
  "error": {  
    "message": "Human readable message.",  
    "type": "ERRORTYPE"  
    "code": CODE NUMBER  
  }  
}
```

4. Client credentials

```

+-----+
|          |--(A)- Αίτημα Εξουσιοδότησης ->| login.it.  |
|          |                               | teithe.gr/  |
|          |<-(B)-- Απάντηση Token      ---| authorization |
|          |                               +-----+
| Εφαρμογή|
| Χρήστη  |                               +-----+
|          |--(C)----- API Call  ----->| api.it.    |
|          |                               | teithe.gr/  |
|          |<-(D)-- Protected Resource  --| profile    |
+-----+                               +-----+

```

A. Αίτημα Εξουσιοδότησης

Η εφαρμογή θα πρέπει να στείλει ένα POST request (Content-Type: application/x-www-form-urlencoded) στο 'https://login.it.teithe.gr/token' συμπεριλαμβάνοντας:

client_id : Client ID της εφαρμογής. Δημιουργείται από το μενού "Οι εφαρμογές μου". | Υποχρεωτική παράμετρος

client_secret : Client Secret της εφαρμογής. | Υποχρεωτική παράμετρος

grant_type : Για το Authorization code θα πρέπει να έχει την τιμή "client_credentials". | Υποχρεωτική παράμετρος

scope : Λίστα με τις διαθέσιμες τιμές μπορεί να βρεθεί εδώ. Μπορείτε να ορίσετε παραπάνω από μια πρόσβαση κάθε φορά, π.χ &scope=id,cn | Υποχρεωτική παράμετρος

B. Απάντηση

Αν όλα τα στοιχεία ήταν σωστά τότε η απάντηση θα είναι σε μορφή JSON ως εξής:

```

{
  "access_token": "ACCESS TOKEN VALUE",
  "user": "USER ID"
}

```

access_token : Το Access Token λήγει σε 2 λεπτά από την έκδοση του.

user : Μοναδικό αναγνωριστικό χρήστη. Προσοχή! Το Access Token που επιστρέφεται από την διαδικασία αυτή έχει πάντα ως user id το id του ιδιοκτήτη της εφαρμογής.

Αν υπήρξε κάποιο σφάλμα η απάντηση είναι πάλι ένα JSON object ως εξής:

```
{
  "error": {
    "message": "Human readable message.",
    "code": CODE_NUMBER
  }
}
```

message : Κείμενο με την περιγραφή του σφάλματος.

code : Κωδικός σφάλματος.

C. Api Call

Με το Access Token που λάβατε στο προηγούμενο βήμα μέσω του url κάντε αιτήσεις στο <https://api.it.teithe.gr>. Για περισσότερες πληροφορίες πατήστε εδώ (https://github.com/apavliidi/IT_API/wiki/API-Documentation).

Παράδειγμα:

```
curl -X GET \
  -H "x-access-token: ACCESS_TOKEN" \
  -H "Content-Type:application/json" \
  api.it.teithe.gr/profile
```

D. Απάντηση

Αν το Access Token ισχύει τότε θα λάβετε ως απάντηση ένα JSON Object ως εξής:

```
{
  "am": "123456",
  "regyear": "2012",
  "regsem": "2",
  "sem": "2",
  "givenName;lang-el": "ΓΕΩΡΓΙΟΣ",
  "sn;lang-el": "ΠΑΠΑΔΟΠΟΥΛΟΣ",
  "fathersname;lang-el": "ΙΩΑΝΝΗ",
  "eduPersonAffiliation": "student",
  "eduPersonPrimaryAffiliation": "it",
  "title": "Undergraduate Student",
  "title;lang-el": "Προπτυχιακός Φοιτητής",
  "cn;lang-el": "ΓΕΩΡΓΙΟΣ ΠΑΠΑΔΟΠΟΥΛΟΣ",
  "cn": "GEORGIOS PAPADOPOULOS",
  "sn": "PAPADOPOULOS",
  "givenName": "GEORGIOS",
  "fathersname": "IOANNH",
  "secondarymail": "-",
  "telephoneNumber": "0",
  "labeledURI": "-",
  "id": "1234",
  "mail": "mail@mail.com",
  "pwdChangedTime": "20180808152441Z",
  "socialMedia": {
    "socialMediaExtra": []
  },
  "profilePhoto": ""
}
```

Επιστρέφει τα στοιχεία του χρήστη.

Αν το Access Token δεν ισχύει τότε θα λάβετε ως απάντηση ένα JSON Object ως εξής:

```
{  
  "error": {  
    "message": "Human readable message.",  
    "type": "ERRORTYPE"  
    "code": CODE NUMBER  
  }  
}
```