**PHỤ LỤC  
HƯỚNG DẪN TÍCH HỢP SSO   
VỚI HỆ THỐNG ĐĂNG NHẬP TẬP TRUNG BỘ GIÁO DỤC**

**I. Quy trình tích hợp**

***1. Thực hiện tích hợp trên hệ thống thử nghiệm:***

- Hệ thống thử nghiệm: [**https://dangnhap.moet.gov.vn**](https://dangnhap.moet.gov.vn)

- Các ứng dụng gửi thông tin callbackUrl (login, logout)

- Hệ thống xác thực tập trung tạo service provider và cung cấp lại bộ key cho các ứng dụng

- Các ứng dụng thực hiện gọi API để xác thực, đăng nhập tập trung

- Đầu mối hệ thống đăng nhập tập trung kiểm tra xác nhận ứng dụng đã hoàn thành tích hợp SSO thử nghiệm

**II. Các bước tích hợp**

1. **Thông tin API kết nối**

|  |  |  |
| --- | --- | --- |
| **STT** | **EndPoint** | **Mô tả** |
| 1 | https://dangnhap.moet.gov.vn/oauth2/authorize | Gửi yêu cầu xác thực tài khoản |
| 2 | https://dangnhap.moet.gov.vn/oauth2/token | Lấy accessToken |
| 3 | https://dangnhap.moet.gov.vn/oauth2/userinfo | Lấy thông tin người dùng |
| 4 | https://dangnhap.moet.gov.vn/oidc/logout | Logout |
| 5 | https://dangnhap.moet.gov.vn/oauth2/revoke | Thu hồi access token |
| 6 | https://dangnhap.moet.gov.vn/oauth2/token | Refresh token |

1. **Client đăng ký dịch vụ SSO**

- Cung cấp callback url

- Lấy thông tin bộ key bảo mật

1. **Khi cần xác thực người dùng sẽ redirect tới trang xác thực của tỉnh**

**- Đường dẫn**: https://dangnhap.moet.gov.vn/oauth2/authorize

**- Method**: GET

**- Input**: Request Param

* + - response\_type=code : (Required) Mô tả loại ủy quyền nào. ở đây là authorization code. Hoặc **token** đối với implicit.
    - client\_id : (Required)định danh cho 1 ứng dụng
    - redirect\_uri : (Required) url callback sau khi người dùng chấp nhận ủy quyền thành công
    - scope : (Required) Danh sách các quyền mà ứng dụng yêu cầu. Bắt buộc phải có openid.
    - state : (optional) ứng dụng gửi lên 1 mã random. Mã này sẽ được gửi lại trong step url callback để ứng dụng xác nhận đúng server mình gửi yêu cầu (CSRF attack)

VD:

https://dangnhap.moet.gov.vn/oauth2/authorize?response\_type=code&client\_id=29352915982374239857&redirect\_uri=https%3A%2F%2Fexample-app.com%2Fcallback&scope=openid

* **Chú ý:** Nếu muốn thêm nhiều scope thì các scope cách nhau dấu +.

VD: scope=openid+email+…

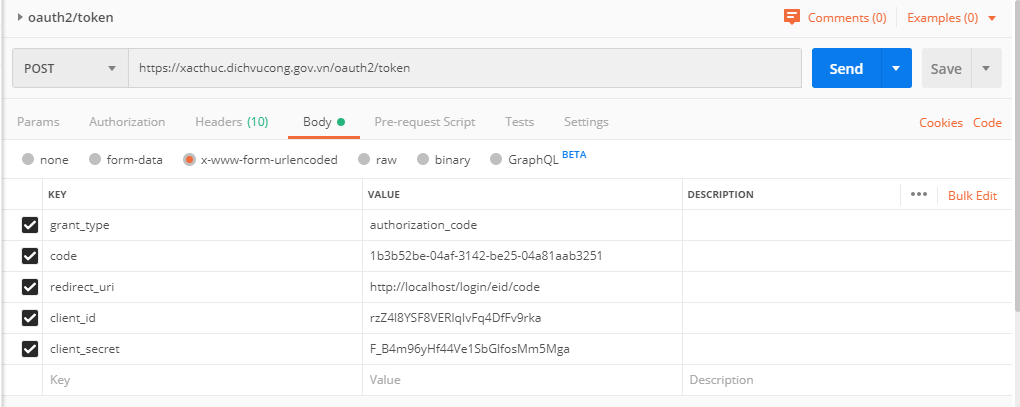
#### Sau khi nhận được Auth Code, thực hiện gọi API Get access token

Sau khi đăng nhập và đồng ý chấp nhận chia sẻ thuộc tính thành công thì Hệ thống SSO sẽ gọi lại url callback của ứng dụng để trả lại authorization code,

Ứng dụng sử dụng authorization code để call API lấy access token:

* **Input:**
* **Đường dẫn:** [https://dangnhap.moet.gov.vn/oauth2/token](https://xacthuc.daklak.gov.vn/oauth2/token)
* **Method**: POST
* **Header**:
  + Content-Type: application/x-www-form-urlencoded
* **Body**: Query Params
  + grant\_type=authorization\_code
  + code : Mã authorization code
  + redirect\_uri :
  + client\_id: client id của ứng dụng
  + client\_secret : là key bí mật của ứng dụng. Giá trị này được gửi lên để server xác thực có chính xác là ứng dụng đó hay không hay. Phòng tránh kẻ tấn công có được authorization code ở bước trước đó

VD:



* **Output**:

HTTP/1.1 200 OK

{

"access\_token": "11e6bccd-e16a-35a6-98d2-c7fe594e0045",

"refresh\_token": "0d41ffa7-f942-38fa-94cf-25a2cc60cd5e",

"scope": "openid",

"id\_token": "eyJ4NXQiOiJOVGhsWm1GaE4yTmpZamt4TmpoalpEVmxOekZsTURReE9UZGpZelUzTkRVM05UaGpNelF6WkEiLCJraWQiOiJOVGhsWm1GaE4yTmpZamt4TmpoalpEVmxOekZsTURReE9UZGpZelUzTkRVM05UaGpNelF6WkEiLCJhbGciOiJSUzI1NiJ9.eyJhdF9oYXNoIjoiVkVVVlZaTjh1TURsby1nWmVuMlJIdyIsImF1ZCI6Inp1SDlqRXJtZVZmajlxS0p1cmhWMV9XUmg4Y2EiLCJzdWIiOiJhZG1pbiIsIm5iZiI6MTU2MjkyMjg4NywiYXpwIjoienVIOWpFcm1lVmZqOXFLSnVyaFYxX1dSaDhjYSIsImFtciI6WyJwYXNzd29yZCJdLCJpc3MiOiJodHRwczpcL1wvbWNhLnZucHQtY2Eudm46OTQ0M1wvb2F1dGgyXC90b2tlbiIsImV4cCI6MTU2MjkyNjQ4NywiaWF0IjoxNTYyOTIyODg3fQ.HvoJ5OzOy4FnEkqY2YSjr5trG19UYz2D8izHuvSu5l0ywiQOEuVjZU3fxF9m4QcIMArRLyGO97JWAyZIBiuL1-uwJNvqLdqbh8PCuSrPIErfy19oXzNpStSMgIzEi4ky1VRodt\_KmjnUIA0cBzrE1-IQycy8H9fNnUzUjG3qzxg",

"token\_type": "Bearer",

"expires\_in": 3600

}

Note:

* id\_token là dạng JWT. Để đảm bảo tính bảo mật các ứng dụng cần xác thực lại id\_token dựa vào public key của server xác thực cung cấp trong đường dẫn lấy jwks
* Trong id\_token phần payload có chứa thông tin người dùng trả về. Decode base64 để thấy rõ

#### Hệ thống gọi API Get user info (tùy chọn, nếu muốn lấy dữ liệu thông tin người dùng từ Hệ thống SSO)

* **Mục đích**: dùng accsess token mục 4 gọi api Get userinfo để lấy thông tin tài khoản
* **Đường dẫn**: [https://dangnhap.moet.gov.vn/oauth2/userinfo](https://xacthuc.daklak.gov.vn/oauth2/userinfo)
* **Method**: GET
* **Header**:
* **Authorization: Bearer <access token>**
* **Output**: thông tin người dùng, định dạng.

{

"firstName": "Văn",

"lastName": "Trần",

"sub": "tva@.daklak.gov.vn",

"zoneinfo": "Asia/Ho\_Chi\_Minh",

"mail": " tva@.daklak.gov.vn",

"middleName": "A",

"email": " tva@.daklak.gov.vn"

}

#### Logout

**- Đường dẫn**: [https://dangnhap.moet.gov.vn/oidc/logout](https://xacthuc.daklak.gov.vn/oidc/logout)

**- Method**: POST

**- Header**:

**- Input**: Query Params

* + id\_token\_hint: (required) id\_token được trả lại bởi identity provider
  + post\_logout\_redirect\_uri: (required) redirect URL được chuyển tới khi logout thành công
  + state: (optional)

**- Output**: redirect về uri redirect

#### Thu hồi access token

**- Đường dẫn**: [https://dangnhap.moet.gov.vn/oauth2](https://xacthuc.daklak.gov.vn/oidc/logout)/revoke

**- Method**: POST

**- Header**: **Content-Type: application/x-www-form-urlencoded**

**- Input**: Query Params

**+ token: token muốn hủy**

**+ token\_type\_hint = access\_token**

**+ client\_id: client id của ứng dụng**

**+ client\_secret : là key bí mật của ứng dụng**

**- Output**: redirect về uri redirect

#### Refresh token

**- Đường dẫn:** [**https://dangnhap.moet.gov.vn/oauth2/token**](https://xacthuc.daklak.gov.vn/oauth2/token)

**- Method: POST**

**- Header:**

- Content-Type: application/x-www-form-urlencoded

**- Body: Query Params**

- grant\_type = refresh\_token

- client\_id: client id của ứng dụng

- client\_secret : là key bí mật của ứng dụng.

- refresh\_token: refresh token đã lấy được tại bước lấy token

**- Output**

{

"access\_token": "1b2f1335-39a5-3318-8fd4-69520f3a3eab",

"refresh\_token": "deaf2825-73b6-396b-bf23-c72ee200d8e8",

"scope": "email openid profile",

"id\_token": "eyJ4NXQiOiJNell4TW1Ga09HWXdNV0kwWldObU5EY3hOR1l3WW1NNFpUQTNNV0kyTkRBelpHUXpOR00wWkdSbE5qSmtPREZrWkRSaU9URmtNV0ZoTXpVMlpHVmxOZyIsImtpZCI6Ik16WXhNbUZrT0dZd01XSTBaV05tTkRjeE5HWXdZbU00WlRBM01XSTJOREF6WkdRek5HTTBaR1JsTmpKa09ERmtaRFJpT1RGa01XRmhNelUyWkdWbE5nX1JTMjU2IiwiYWxnIjoiUlMyNTYifQ..CRWVNLJepUDHWQe2zS8kuIAmNiRiFh6kq1LuISByi3bQUux8d6Xfx8zUk1RDXohllVcl9qxu0NajdxsK9fRvUT4fUmGV1l4cu-cs12zzcOZXrZtYEn5CRV66dcYRmFOTsSTlovE83xcGbYqtatTki9RaS7Z-2nZJFMyxyYTqCC0yE\_z7eKhnkxoKP-00Iqb04Zd9Ryym8EOzN2zJqMx0Drvmv-8\_ip8NBqLyWyFpfNp0icvs1Q6hc829x3iUQHPH5hpHpf9bKJpzfX3rQ4hZkz7XDm0vqDtHsRWrfkJ7QJ0s\_F5eNIM822WVHEaOG9CCXWBfAfWAuOzw0qm1MHeF2g",

"token\_type": "Bearer",

"expires\_in": 3600

}