API เชื่อมต่อระบบยืนยันตัวตนแบบรวมศูนย์

e-Authentication แบบ Single Sign-On ของสปสช.

(Version 2.5 08/05/2025)

การเชื่อมต่อ e-Authentication (SSO) ด้วย OpenID Configuration

การเชื่อมต่อ SSO (Single Sign-On) โดยใช้ OpenID Configuration สามารถพัฒนาระบบเพื่อทำการเชื่อมต่อได้ตามขั้นตอนต่างๆ ดังนี้

1. ขั้นตอนการเชื่อมต่อ SSO ด้วย OpenID Configuration

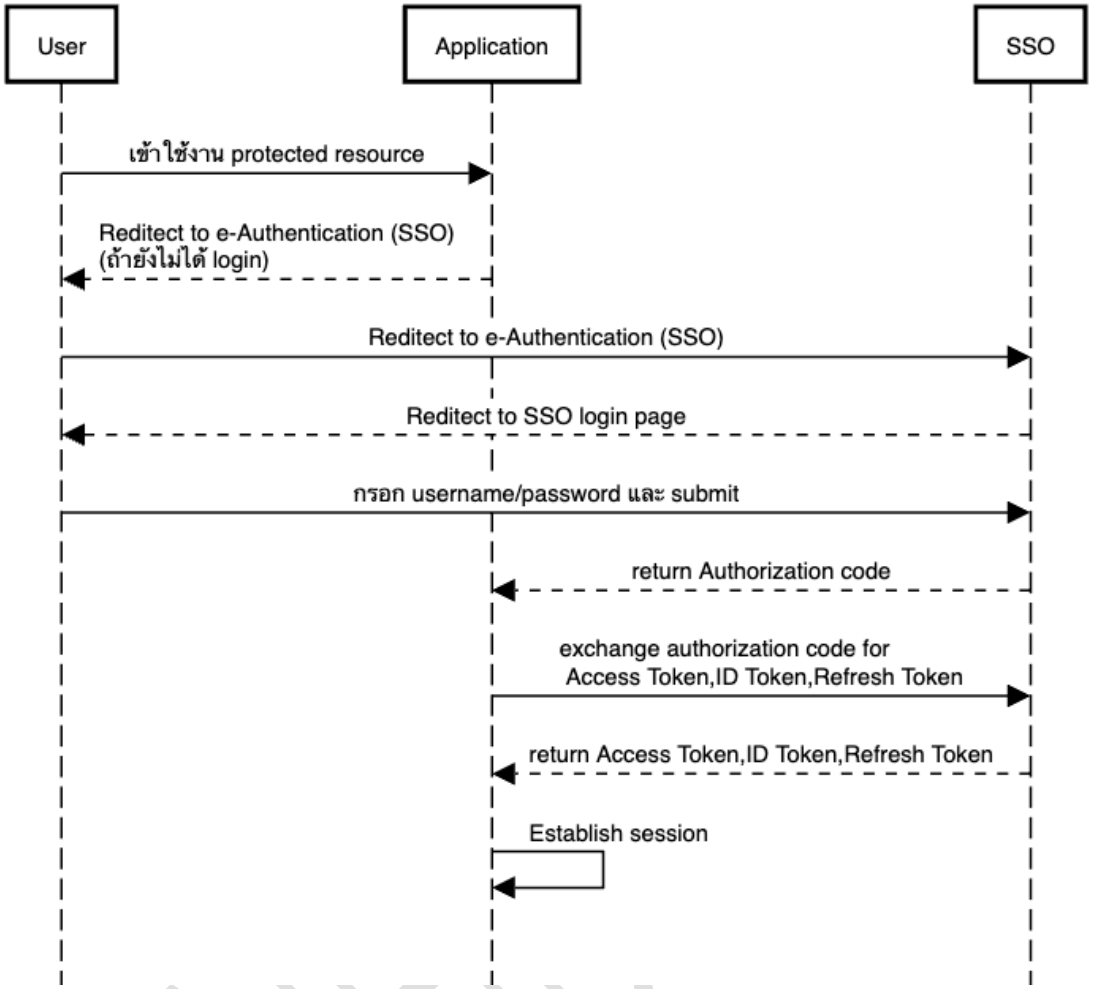
1.1 ตรวจสอบ OpenID Configuration

OpenID Connect Well-Known Configuration https://iam.nhso.go.th/realms/nhso/.well-known/openid-configuration เพื่อดูรายละเอียดการตั้งค่าต่าง ๆ ที่จำเป็นต้องใช้ในการเชื่อมต่อ

1.2 ตั้งค่าไคลเอนต์ (Client Setup)

- Client ID: ได้รับจากผู้ให้บริการ (NHSO)
- Client Secret: ได้รับจากผู้ให้บริการ (NHSO)

2. การเชื่อมต่อด้วย Authorization Code Flow



2.1 การขอ Authorization Code

Redirect ผู้ใช้งานไปยังหน้าล็อกอินของ NHSO โดยใช้ URL ดังนี้ :

https://iam.nhso.go.th/realms/nhso/protocol/openid-connect/auth

โดยมีพารามิเตอร์ดังนี้:

- client_id: ID ของไคลเอนต์ที่ได้รับ
- redirect_uri: URL ที่จะรับการตอบกลับ
- response_type: code
- scope: openid
- state: ค่าที่ใช้เพื่อตรวจสอบการตอบกลับ

ตัวอย่าง URL:

https://iam.nhso.go.th/realms/nhso/protocol/openid-connect/auth?client_id=YOUR_CLIENT_ID&redirect_uri=YOUR_REDIRECT_URI&response_type=code&scope=openid&state=YOUR_STATE

2.2 แลกเปลี่ยน Authorization Code เป็น Access Token

เมื่อผู้ใช้ทำการล็อกอินสำเร็จ NHSO จะส่ง authorization code กลับไปยัง redirect URI ที่กำหนดไว้ในพารามิเตอร์ code ทำการส่ง request ไปยัง URL:

https://iam.nhso.go.th/realms/nhso/protocol/openid-connect/token

โดยมีพารามิเตอร์ดังนี้:

- grant_type: authorization_code
- code: authorization code ที่ได้รับ
- redirect_uri: URL ที่ตรงกับที่ระบุในขั้นตอนก่อนหน้า
- client_id: ID ของไคลเอนต์
- client_secret: Secret ของไคลเอนต์

ตัวอย่าง request:

```
POST /realms/nhso/protocol/openid-connect/token
Content-Type: application/x-www-form-urlencoded
grant_type=authorization_code
code=YOUR_AUTHORIZATION_CODE
redirect_uri=YOUR_REDIRECT_URI
client_id=YOUR_CLIENT_ID
client_secret=YOUR_CLIENT_SECRET
```

2.3 ตรวจสอบ Access Token

เมื่อได้รับ access token สามารถใช้ token นี้ในการเรียก API อื่น ๆ ที่ต้องการ authentication ด้วย access token เช่น:

```
GET /realms/nhso/protocol/openid-connect/userinfo
Authorization: Bearer ${YOUR_ACCESS_TOKEN}
```

ตัวอย่างการทำงานทั้งหมดด้วย curl

ตัวอย่างนี้จะใช้ curl สำหรับการขอ authorization code และแลกเปลี่ยนเป็น access token:

 # Step 1: Request Authorization Code

Open the following URL in your browser to get the authorization code:

```
https://iam.nhso.go.th/realms/nhso/protocol/openid-
connect/auth?client_id=YOUR_CLIENT_ID&redirect_uri=YOUR_REDIRECT_URI&response_type=co
de&scope=openid&state=YOUR_STATE
```

 # Step 2: Exchange Authorization Code for Access Token

Enter the authorization code: "code”

```
curl -X POST "https://iam.nhso.go.th/realms/nhso/protocol/openid-connect/token" \
-H "Content-Type: application/x-www-form-urlencoded" \
-d "grant_type=authorization_code" \
-d "code=$code" \
-d "redirect_uri=YOUR_REDIRECT_URI" \
-d "client_id=YOUR_CLIENT_ID" \
-d "client_secret=YOUR_CLIENT_SECRET"
```

Response


```
{
  "access_token":
"eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJIR0VyRHZwVVV0Wk5GU0ZWT3NEellhR3BVM
ThuOXNLY1l1b2s5emdjNjZJIn...",
  "expires_in": 1800,
  "refresh_expires_in": 7181,
  "refresh_token":
"eyJhbGciOiJIUzUxMiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJmZTBhYzM1Zi1mZjVhLTQ4MTAtYTBkMS1k
MmJlYmZlMmUyNzMifQ...",
  "token_type": "Bearer",
  "id_token":
"eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJIR0VyRHZwVVV0Wk5GU0ZWT3NEellhR3BVM
ThuOXNLY1l1b2s5emdjNjZJIn...",
  "not-before-policy": 1697652439,
  "session_state": "503ac775-a75c-4115-a2e3-937b29857edb",
  "scope": "openid email profile"
}
```

Response

Key	Description
access_token	The token used to access resources
expires_in	Time in seconds until the token expires
refresh_expires_in	Time in seconds until the refresh token expires
refresh_token	Token used to obtain a new access token when the current one expires
token_type	Type of token
id_token	Token that contains identity information about the user
session_state	State of the session
scope	Scope of the access request

 # Save the access token from the response to use in the next step

 # Step 3: Verify Access Token UserInfo

Enter the access token: "access_token"

```
curl -X GET "https://iam.nhso.go.th/realms/nhso/protocol/openid-connect/userinfo" \
-H "Authorization: Bearer $access_token"
```

Response


```
{
  "nameTh": "สมชาย ใจดี",
  "sub": "f:09ea7733-e40f-461c-a658-a4f67f35d25b:preferred_username",
  "personalId": "1350100xxxxxx",
  "resource_access": {
    "reghosp": {
      "roles": [
        "admin"
      ]
    },
    "e-portal": {
      "roles": [
        "admin"
      ]
    },
    "account": {
      "roles": [
        "manage-account",
        "manage-account-links",
```

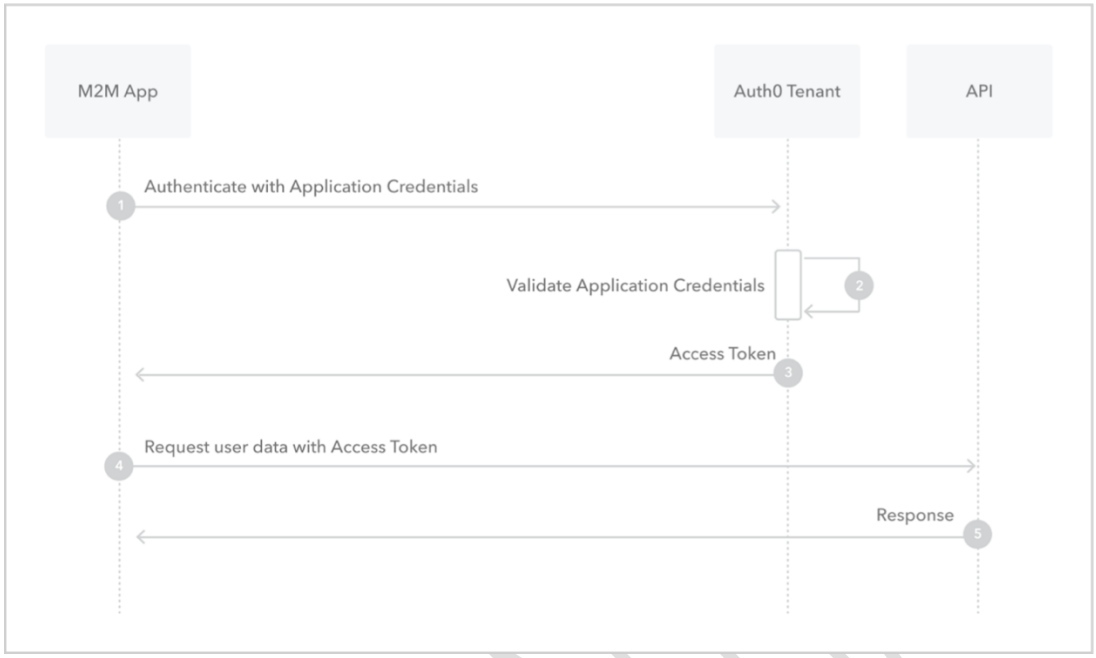
```
        "view-profile"
      ]
    }
  },
  "email_verified": true,
  "staffUserType": "43",
  "preferred_username": "preferred_username",
  "source": "DC",
  "given_name": "สมชาย",
  "middle_name": "",
  "userId": 56,
  "titleName": "นาย",
  "realm_access": {
    "roles": [
      "nhso",
      "hra",
      "offline_access",
      "uma_authorization"
    ]
  },
  "organization": {
    "id": "NHSO3",
    "orgType": "GOV",
    "name": "สำนักบริหารสารสนเทศการประกัน",
    "fromType": "O"
  },
  "name": "สมชาย ใจดี",
  "family_name": "ใจดี",
  "staffId": 10746322,
  "email": "email@nhso.go.th",
  "mobile": "08xxxxxxxx"
}
```

Response

Key	Description	Example Value
nameTh	ชื่อภาษาไทย	สมชาย ใจดี
sub	Subject Identifier	f:09ea7733-e40f-461c-a658-a4f67f35d25b: preferred_username
personalId	เลขประจำตัวประชาชน	1350100xxxxxx
resource_access	การเข้าถึงทรัพยากรที่ผู้ใช้สามารถเข้าถึงได้ แบ่งตามระบบต่างๆ	-
resource_access.reghosp	การเข้าถึงระบบ reghosp	-
resource_access.reghosp.roles	บทบาทของผู้ใช้ในระบบ reghosp	['admin']
resource_access.e-portal	การเข้าถึงระบบ e-portal	-
resource_access.e-portal.roles	บทบาทของผู้ใช้ในระบบ e-portal	['admin']
resource_access.account	การเข้าถึงระบบ account	-
resource_access.account.roles	บทบาทของผู้ใช้ในระบบ account	['manage-account', 'manage-account-links', 'view-profile']
email_verified	สถานะการยืนยันอีเมล	True
staffUserType	ประเภทผู้ใช้พนักงาน	ข้อมูลจากตาราง STAFF
preferred_username	ชื่อผู้ใช้งาน (Username)	
source	ประเภทผู้ใช้งาน	DC(Data Center) OSS(One Stop Service) LDAP(AD NHSO)
given_name	ชื่อจริง	
middle_name	ชื่อกลาง	
userId	รหัสผู้ใช้	
titleName	คำนำหน้าชื่อ	นาย
realm_access	บทบาทที่ผู้ใช้สามารถเข้าถึงในระบบต่าง ๆ	-
realm_access.roles	บทบาทใน realm	['nhso', 'hra', 'offline_access', 'uma_authorization']
organization	ข้อมูลองค์กร	-
organization.id	รหัสองค์กร	NHSO3
organization.orgType	ประเภทองค์กร	GOV
organization.name	ชื่อองค์กร	สำนักบริหารสารสนเทศการประกัน

Key	Description	Example Value
organization.fromType	ประเภทขององค์กร	- สปสช.ส่วนกลาง = ‘O’ - สปสช.เขต = ‘Z’ - หน่วยบริการ HOSPITAL = “H” - สสจ. PROVINCE =“P” - องค์บริหารส่วนจังหวัด = "C" - สสอ. AUMPHER = "A" - อปท DISTRICT = "D" - อปท TUMBON = "T"
name	ชื่อเต็ม	
family_name	นามสกุล	
staffId	รหัสพนักงาน	StaffId ตาราง Staff
email	อีเมล	email@nhso.go.th
mobile	เบอร์มือถือ	จะได้รับเมื่อขอ scope “mobile”
loginMethod	ช่องทางเข้าสู่ระบบ	- ThaiD = “thaiD” - SmartCard = “smartCard”

3. การเชื่อมต่อด้วย Client Credentials Flow



รูปภาพจาก auth0.com

3.1 การขอ Token ด้วย Client Credentials Flow

ขอ Token กับผู้ให้บริการ NHSO โดยใช้ URL ดังนี้ :

https://iam.nhso.go.th/realms/nhso/protocol/openid-connect/token

โดยมีพารามิเตอร์ดังนี้:

- Content-Type: application/x-www-form-urlencoded
- client_id: ID ของไคลเอนต์ที่ได้รับ
- client_secret: Secret ของไคลเอนต์ที่ได้รับ
- grant_type: client_credentials

ตัวอย่าง URL:

```
curl -X POST "https://iam.nhso.go.th/realms/nhso/protocol/openid-connect/token" \
    -H "Content-Type: application/x-www-form-urlencoded" \
    -d "grant_type=client_credentials" \
    -d "client_id=${client_id} " \
    -d "client_secret=${client_secret} "
```

Response


```
{
  "access_token": "eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6IC... ",
  "expires_in": 1800,
  "refresh_expires_in": 0,
  "token_type": "Bearer",
  "not-before-policy": 0,
  "scope": "email profile"
}
```


Response

Key	Description
access_token	The token used to access resources
expires_in	Time in seconds until the token expires
token_type	Type of token
scope	Scope of the access request

การเชื่อมต่อ SSO ด้วย Flow อื่นสามารถดูรายละเอียดได้ที่ https://auth0.com/docs/get-started/authentication-and-authorization-flow/authorization-code-flow

4. Log Users Out of SSO with OIDC Endpoint

Discovery metadata document URL : https://iam.nhso.go.th/realms/nhso/.well-known/openid-configuration

OIDC Logout endpoint :

"end_session_endpoint": "https://iam.nhso.go.th/realms/nhso/protocol/openid-connect/logout"

Call the OIDC Logout endpoint

Parameter	Description
id_token_hint	The ID Token previously issued to the user. This is used to identify the session to be logged out.
post_logout_redirect_uri	The URL to redirect the user to after a successful logout. Must be whitelisted in the OIDC provider settings.

ตัวอย่าง URL HTTP GET

https://iam.nhso.go.th/realms/nhso/protocol/openid-connect/logout?id_token_hint=eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkI...&post_logout_redirect_uri=https%3A%2F%2Fossregister.nhso.go.th

SSO NHSO Implements OpenID Connect's RP-Initiated Logout 1.0 : https://openid.net/specs/openid-connect-rpinitiated-1_0.html