

[2018]

# ข้อกำหนดทางเทคนิค (Technical Specification)

ในส่วนของการเชื่อมต่อด้วย WEB API  
สำหรับ RELYING PARTY



สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ELECTRONIC  
TRANSACTIONS DEVELOPMENT AGENCY (PUBLIC ORGANIZATION) |

|  |   |
|--|---|
| <b>วัตถุประสงค์</b><br>(Objective)               | เพื่อเป็นคู่มือที่ใช้สำหรับการเชื่อมต่อ Application Programming Interface (API) ของ Relying Party |
| <b>เจ้าของโครงการ</b><br>(Ownership)             | สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)  |
| <b>วันที่เริ่มโครงการ</b><br>(Start Date)        | 1 มกราคม 2561   |
| <b>วันที่สิ้นสุดโครงการ</b><br>(Completion Date) | 30 มิถุนายน 2561  |
| <b>ประกาศโครงการ</b><br>(Important Notice)       |   |

ข้อมูลเอกสาร (DOCUMENT INFORMATION)

|                                 |   |
|---------------------------------|---|
| <b>วัตถุประสงค์ (Objective)</b> | เพื่อเป็นแนวทางของ RP ในการเตรียมการเชื่อมต่อกับระบบ ETDA Connect สำหรับการยืนยันตัวตนเพื่อใช้บริการภาครัฐและบริการอื่นที่ต้องการเชื่อมต่อกับภาครัฐ |
|---------------------------------|---|

| การปรับปรุงเอกสาร (DOCUMENT VERSION HISTORY) |               |                          |   |
|--|---------------|--------------------------|---|
| เลขที่ รุ่น (Version No.)                    | วันที่ (Date) | ผู้ปรับปรุง (Revised By) | เหตุผลการเปลี่ยนแปลง (Reason for Change)  |
| 1.0  | 30 มี.ค. 2561 | ETDA                     | สร้างเอกสาร   |
| 1.0  | 11 เม.ย. 2561 | ETDA                     | ปรับปรุง Parameter และรายละเอียดเพิ่มเติมเกี่ยวกับ ID Token   |
| 1.0  | 22 พ.ค. 2561  | ETDA                     | <ul style="list-style-type: none"> <li>- ปรับปรุงรายละเอียดคำอธิบายขั้นตอน และ Web API ในหัวข้อที่ 1.4</li> <li>- เปลี่ยน Error code ของ invalid_request_uri จาก 302 เป็น 400</li> <li>- เพิ่มภาคผนวก ก. การเรียกดูข้อมูลการเชื่อมต่อผ่าน Discovery Endpoint</li> </ul> |
| 1.0  | 26 พ.ค. 2561  | ETDA                     | - ปรับปรุง post request เป็น json body  |
|  |               |                          |   |

## สารบัญ

---

|   |    |
|---|----|
| 1. การเชื่อมต่อ RP กับระบบ ETDA Connect.....                                  | 5  |
| 1.1 การเตรียมข้อมูลสำหรับเชื่อมต่อกับระบบ ETDA Connect.....                   | 5  |
| 1.2 กระบวนการทำงานของการยืนยันตัวตนทางอิเล็กทรอนิกส์โดยมี ETDA Connect.....   | 6  |
| 1.3 ขั้นตอนการทำงานของการยืนยันตัวตนทางอิเล็กทรอนิกส์โดยมี ETDA Connect ..... | 7  |
| .14 รายละเอียดของขั้นตอนและการเชื่อมต่อ RP กับ ETDA Connect ด้วย Web API..... | 8  |
| .14.1 ขั้นตอน 1RP Request ขอนำจอของแสดงรายการ IdP โดยมี Message ดังนี้.....   | 8  |
| .14.2 ระบบ ETDA Connect ส่ง Authorization Code ให้กับ RP .....                | 10 |
| .14.3 ขั้นตอนการขอข้อมูล 3ID Token .....                                      | 11 |
| 1.5 ขอบเขตของข้อมูล (scope).....  | 13 |
| ขอบเขตของข้อมูลประเภท profile_kyc.....  | 14 |
| 1.6 ข้อมูลผลการยืนยันตัวตนและข้อมูลผู้ใช้งาน (ID Token).....                  | 16 |
| 1.6.1 ส่วนของ Header .....  | 16 |
| 1.6.2 ส่วนของ Payload.....  | 16 |
| 1.6.3 ส่วนของ Signature.....  | 18 |
| 1.6.4 ตัวอย่าง 4ID Token.....   | 18 |
| 1.6.5 การตรวจสอบความถูกต้องของข้อมูล ID Token .....                           | 20 |
| 2. ข้อความแจ้งกลับข้อผิดพลาด ERROR RESPONSE.....                              | 22 |
| ภาคผนวก ก. การร้องขอข้อมูลการเชื่อมต่อผ่าน Discovery Endpoint.....            | 25 |

## 1. การเชื่อมต่อ RP กับระบบ ETDA CONNECT

### 1.1 การเตรียมข้อมูลสำหรับเชื่อมต่อกับระบบ ETDA Connect

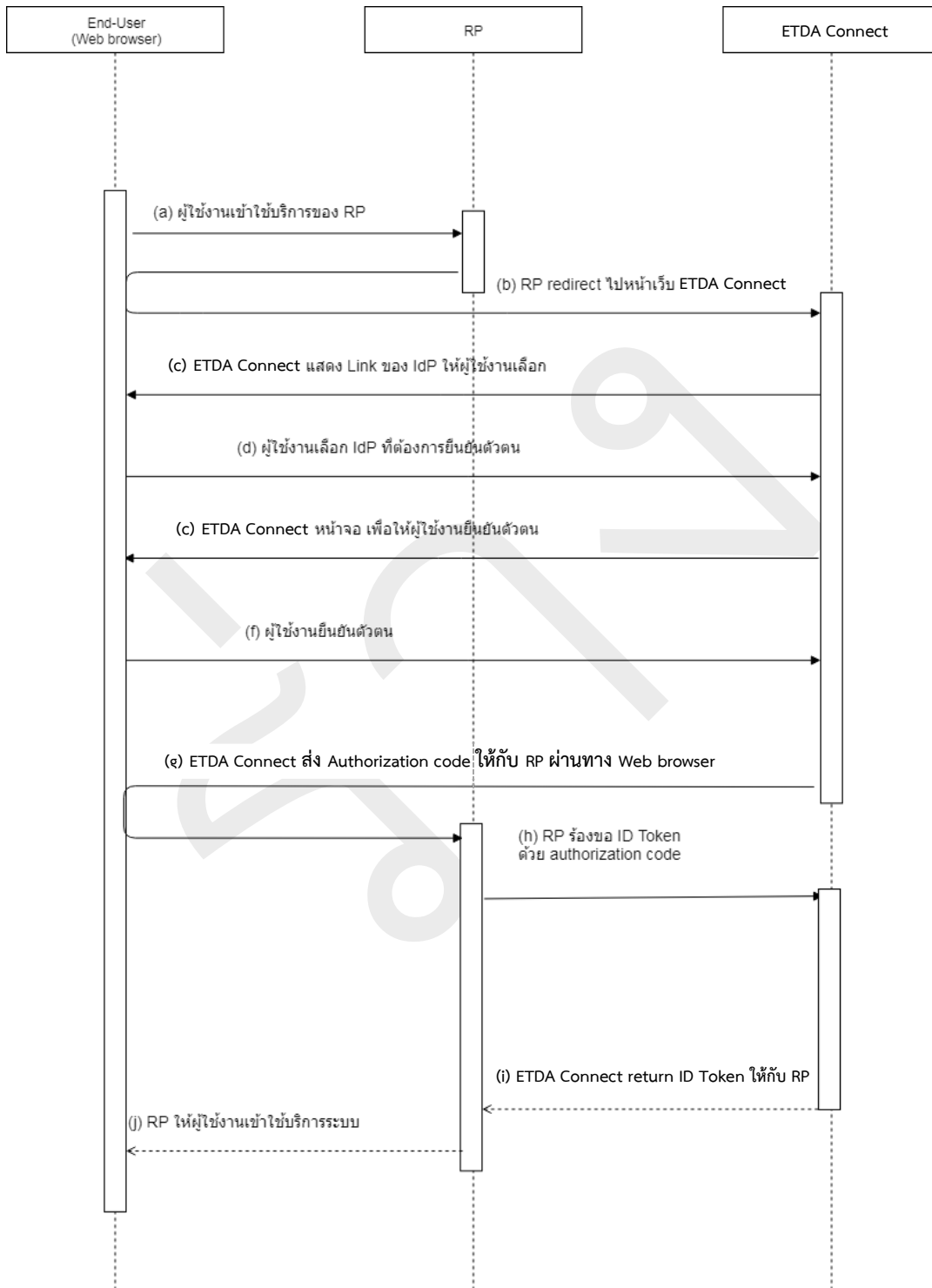
ในการเชื่อมต่อระหว่าง IdP และ RP นั้น ระบบ ETDA Connect จะเป็นตัวกลางในการเชื่อมต่อผ่าน โพรโตคอล OpenID Connect 1.0 โดยก่อนเริ่มการเชื่อมต่อกับระบบ ETDA Connect นั้น RP จะต้องเตรียมข้อมูลเบื้องต้นและกำหนดช่องทาง (ในรูปแบบ URL) ในการร้องขอผลการตามที่โปรโตคอล OpenID Connect 1.0 กำหนดและส่งให้กับ Federation s ดังรายละเอียดต่อไปนี้

- 1) Redirect URL: URL สำหรับรับ Response ของ authentication request จาก ETDA Connect
- 2) ข้อมูลเพื่อใช้ในการลงทะเบียนกับ ETDA Connect มีดังต่อไปนี้

| พารามิเตอร์   | พารามิเตอร์ (ภาษาไทย)  | คำอธิบาย                                  |
|---------------|------------------------|---|
| RP Name (TH)  | ชื่อหน่วยงาน (ไทย)     | ชื่อของ RP ภาษาไทย (ห้ามมีอักขระพิเศษ)    |
| RP Name (EN)  | ชื่อหน่วยงาน (English) | ชื่อของ RP ภาษาอังกฤษ (ห้ามมีอักขระพิเศษ) |
| RP Short Name | ชื่อย่อ                | ชื่อย่อหน่วยงาน RP                        |
| Sector        | ประเภทหน่วยงาน         | ประเภทหน่วยงานของ RP                      |
| Address       | ที่อยู่                | บ้านเลขที่ ชื่ออาคาร ถนน                  |
| Sub-District  | ตำบล                   | แขวง/ตำบล                                 |
| District      | อำเภอ                  | เขต/อำเภอ                                 |
| City          | จังหวัด                | จังหวัด                                   |
| Post Code     | รหัสไปรษณีย์           | รหัสไปรษณีย์                              |
| Mobile        | โทรศัพท์เคลื่อนที่     | เบอร์โทรศัพท์เคลื่อนที่ของ RP             |
| Phone         | โทรศัพท์สำนักงาน       | เบอร์โทรศัพท์สำนักงานของ RP               |

สำหรับ RP ที่ต้องการพัฒนา OpenID Connect เพื่อเชื่อมต่อกับ ETDA Connect สามารถใช้งาน Library ที่ผ่านการรับรองจาก OpenID Foundation ซึ่งผู้พัฒนาสามารถหา Library ตามความเหมาะสมกับภาษาที่ใช้พัฒนา โดยข้อมูลของ Library ที่ใช้พัฒนาสามารถหาได้จาก URL : <http://openid.net/developers/certified>

1.2 กระบวนการทำงานของการยืนยันตัวตนทางอิเล็กทรอนิกส์โดยมี ETDA Connect



### 1.3 ขั้นตอนการทำงานของการทำงานการยืนยันตัวตนทางอิเล็กทรอนิกส์โดยมี ETDA Connect

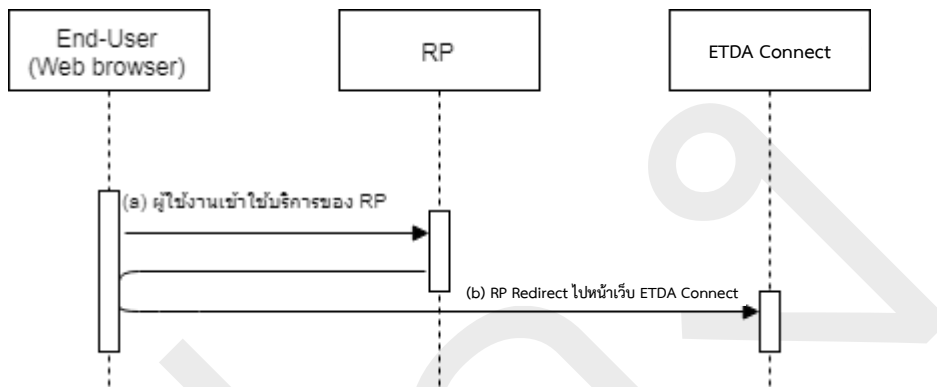
1. ผู้ใช้งานพิมพ์ URL ของ Relying Party เพื่อเข้าใช้งานระบบผ่านทาง Web Browser
2. Relying Party ทำการร้องขอการยืนยันตัวตนผู้ใช้งานไปยังระบบ ETDA Connect พร้อมทั้งกำหนด
  - เงื่อนไขในการแสดง IdP List เช่น Level of Assurance (LoA) เป็นต้น และ
  - รายละเอียดข้อมูลที่ Relying Party ต้องการ เช่น ชื่อ นามสกุล และหมายเลขประจำตัวประชาชน (ในกรณีที่ต้องการข้อมูลเพื่อระบุได้ว่าเป็นบุคคลใด) หรือ ข้อมูลประกอบการดำเนินการรู้จักลูกค้า (Know Your Customer: KYC) เป็นต้น ทั้งนี้ อาจมีการเพิ่มเติมรายละเอียดเพิ่มเติมได้
3. ผู้ใช้งานทำการเลือก Identity Provider ที่ต้องการยืนยันตัวตน
4. Identity Provider ทำการยืนยันตัวตนผู้ใช้งาน
5. ผู้ใช้งานทำการยืนยันตัวตน หากการยืนยันตัวตนสำเร็จ Identity Provider จะต้องแสดงข้อมูลของผู้ใช้งานบนหน้าจอ พร้อมทั้งให้ผู้ยืนยันความถูกต้องของข้อมูลและยินยอม (Consent) ในการเปิดเผยข้อมูลแก่ Relying Party
6. เมื่อผู้ใช้งานยืนยันความถูกต้องของข้อมูลและยินยอมเปิดเผยข้อมูลแล้ว ผู้ใช้งานถูก redirect ไปยัง ETDA Connect พร้อมผลการยืนยันตัวตน ซึ่งเรียกว่า Authentication code ให้กับ ETDA Connect
7. ETDA Connect ทำการส่ง Authentication code ให้กับ Relying Party ผ่านทาง Web Browser
8. Relying Party ทำการขอข้อมูลจาก Identity Provider โดยการส่ง Authentication code ไปยัง ETDA Connect
9. ETDA Connect นำ Authentication Code ที่ได้รับจาก Relying Party ตรวจสอบ Authentication Code หาก Authentication Code ถูกต้อง ETDA Connect จะส่ง Assertion กลับมายัง RP โดยการระบุข้อมูลไว้ใน ID Token ซึ่ง Assertion ต้องถูกลบลงเมื่อชื่ออิเล็กทรอนิกส์ด้วยกุญแจส่วนตัว (Private key) ETDA Connect ด้วย
10. Relying Party ทำการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ที่ลงใน ID Token ว่าถูกส่งมาจาก ETDA Connect หากลายมือชื่ออิเล็กทรอนิกส์ถูกต้อง Relying Party ก็สามารถเชื่อถือได้ว่าผู้ใช้งานได้ทำการยืนยันตัวตนแล้วกับ Identity Provider ที่น่าเชื่อถือตามระดับ LoA ที่กำหนดไว้และอนุญาตให้ผู้ใช้งานเข้าใช้ระบบได้

### 1.4 รายละเอียดของขั้นตอนและการเชื่อมต่อ RP กับ ETDA Connect ด้วย Web API

ขั้นตอนการยืนยันตัวตนทางอิเล็กทรอนิกส์กับระบบ ETDA Connect ประกอบด้วย 3 ขั้นตอนหลักดังต่อไปนี้

- ขั้นตอนหลักที่ 1: RP ร้องขอการยืนยันตัวตน ผ่าน Authorization Endpoint
- ขั้นตอนหลักที่ 2: ระบบ ETDA Connect ส่ง Authorization Code ให้กับ RP
- ขั้นตอนหลักที่ 3: RP ร้องขอ Access Token และ ID Token ผ่าน Token Endpoint

#### 1.4.1 ขั้นตอน RP Request ขอนำจอของแสดงรายการ IdP โดยมี Message ดังนี้



#### Request

| Method | URL  |
|--------|--|
| GET    | https://example.digitalidproxy.or.th/authorize |

#### พารามิเตอร์

| พารามิเตอร์   | Required | รายละเอียด   |
|---------------|----------|--|
| response_type | Required | กำหนดค่าเป็น “code”  |
| client_id     | Required | identifier ที่ใช้ระบุ RP   |
| scope         | Required | ขอบเขตหรือชุดของข้อมูลที่ร้องขอ ค่าของ scope ให้กำหนดเป็น และตามด้วย profile หรือ profile_kyc                    |
| redirect_uri  | Required | กำหนดค่าเป็น HTTP endpoint (url) ของ RP ใช้สำหรับ redirect กลับไปยัง เว็บไซต์ของ RP เมื่อการยืนยันตัวตนเสร็จสิ้น |



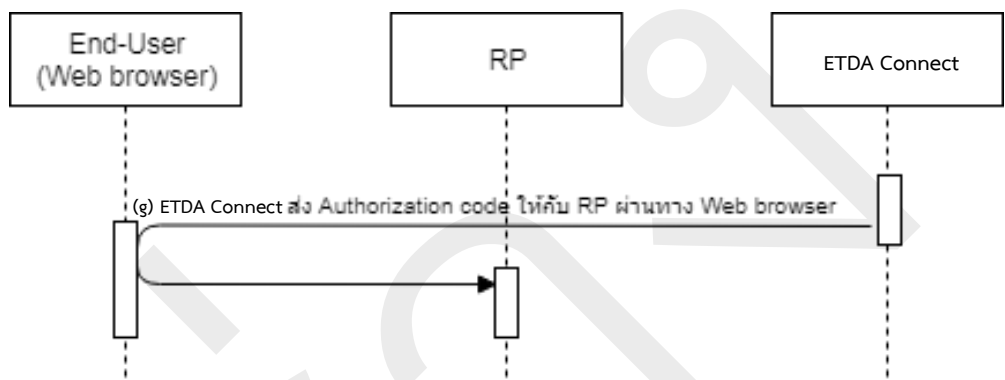
| พารามิเตอร์ | Required | รายละเอียด   |
|-------------|----------|--|
|             |          | ซึ่งค่าของ redirect_url ต้องเป็น url ที่ได้ลงทะเบียนไว้กับ ETDA Connect  |
| state       | Required | string ใช้ในการตรวจสอบความสัมพันธ์ระหว่าง request (จาก RP) กับ response (ของ ETDA Connect) เพื่อป้องกันการโจมตีแบบ Cross-Site Request Forgery (CSRF, XSRF) โดยค่าของ state อาจทำได้โดย encode ค่า hash ของ browser cookie เพื่อตรวจสอบว่า request ที่เกิดขึ้น และ callback ที่ส่งกลับมาจาก browser เดียวกัน  |
| prompt      | Required | ให้กำหนดค่าเป็น “login consent”  |
| acr_values  | Optional | เป็นค่าที่ระบุเพื่อขอให้ RP แสดงรายการ IdP ที่เกี่ยวข้อง โดยเกณฑ์การเลือกแสดง IdP โดยให้ระบุค่า ดังต่อไปนี้ (สามารถระบุได้มากกว่า 1)<br>- ระบุ IAL โดยมีรูปแบบ urn:did:ial:[ระดับของ ial]<br>ตัวอย่าง การระบุ IAL ระดับ 2.1 ขึ้นไป : urn:did:ial:2_1<br>- ระบุ AAL โดยมีรูปแบบ urn:did:ial:[ระดับของ aal]<br>ตัวอย่าง การระบุ AAL ระดับ 2.1 ขึ้นไป : urn:did:aal:2_1<br>- ระบุ sector คือการระบุ IdP ที่ให้บริการสำหรับเฉพาะกลุ่มธุรกิจ โดยมีรูปแบบ urn:did:sector:[sector short name]<br>ตัวอย่าง ระบุ IdP สำหรับภาครัฐ: urn:did:sector:government<br>- ระบุชื่อ IdP มีรูปแบบ urn:did:idp:[idp short name]<br>ตัวอย่าง ระบุชื่อของ IdP : urn:did:idp:idp001 |

ตัวอย่าง HTTP Request

```
GET https://proxy1.auth.teda.th/proxy/v1/authorize?
response_type=code
&client_id=ba2fdDyiE3SsbQTUt9UWZu6
&redirect_uri=https://rp.example.com/callback
&scope=openid%20profile
&state=af0ifjsldkj
&prompt=login%20consent
```

```
&acr_values=urn:did:ial:2_1%20urn:did:aal:3%20urn:did:sector:financial
```

1.4.2 ระบบ ETDA Connect ส่ง Authorization Code ให้กับ RP



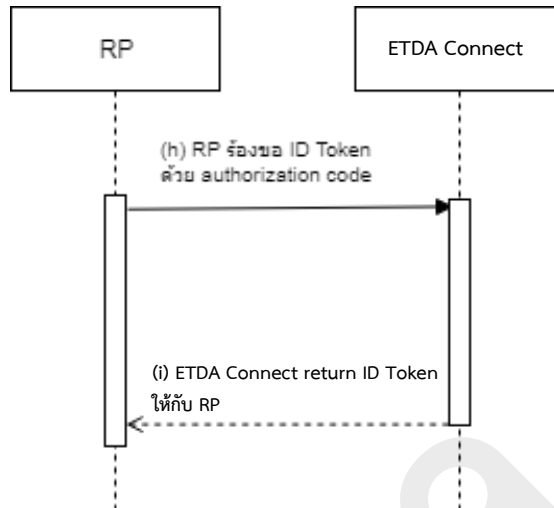
ระบบ ETDA Connect จะทำการส่ง Authorization Code ให้กับ RP ด้วย HTTP GET โดยมีพารามิเตอร์ดังต่อไปนี้

```
GET https://rp.example.org/callback?
code=nnqtYcoik7cjtHQYyn3Af8uk4LG3rYYh
&state=af0ifjsldkj
```

คำอธิบายพารามิเตอร์

| พารามิเตอร์ | Required | รายละเอียด  |
|-------------|----------|---|
| code        | Required | Authorization Code ที่ใช้ในการร้องขอ ID Token   |
| state       | Required | ค่า state ที่ RP ส่งมาพร้อมกับ Authentication Request ในขั้นตอน (b) เพื่อยืนยันว่า response ที่ได้รับเป็น response ที่เกิดจาก request ของ RP จริง |

### 1.4.3 ขั้นตอนการขอข้อมูล ID Token



#### RP ขอข้อมูล ID Token จาก ETDA Connect ด้วย authorization code

RP ขอข้อมูล ID Token ผ่าน ETDA Connect โดยการส่ง Request เป็น HTTP Post ไปยัง ETDA Connect ทั้งนี้ ในส่วนของ HTTP Header ให้กำหนดพารามิเตอร์ “Authorization” ซึ่งค่าของ Authorization ถูก Encode ด้วย Base64(client\_id +”:” + client\_secret) ตามที่ระบุในมาตรฐาน [HTTP Basic Authentication](#) และ [Oauth 2.0 section 2.1.1](#) ซึ่งมีพารามิเตอร์ ดังต่อไปนี้

#### Request

| Method | URL  |
|--------|--|
| POST   | https://proxy1.auth.teda.th/proxy/v1/token |

#### พารามิเตอร์

| พารามิเตอร์  | Required | รายละเอียด  |
|--------------|----------|---|
| grant_type   | Required | ใช้ค่า “authorization_code”                                 |
| Code         | Required | Authentication Code ที่ได้รับจาก ETDA Connect               |
| redirect_uri | Required | URI ที่ใช้ในการ Call Back ซึ่งถูกระบุไว้กับทาง ETDA Connect |

### ตัวอย่างการส่ง HTTP Request

ส่ง Request ไปยังด้วย Http Post ไปยัง ETDA Connect โดยมี พารามิเตอร์

```
POST https://proxy1.auth.teda.th/proxy/v1/token
Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW
Content-Type: application/x-www-form-urlencoded

grant_type=authorization_code
code=SplxlOBeZQQYbYS6WxSbIA
redirect_uri= https://rp.example.com/callback
```

### Response

หลังจากที่ ETDA Connect ตรวจสอบ code และ redirect\_uri ว่าถูกต้องแล้ว ETDA Connect จะส่ง Access Token และ ID Token กลับมายัง RP ดังต่อไปนี้

### ตัวอย่างการส่ง HTTP Response ของ ETDA Connect ไปยัง RP

Status : 200

```
Content-Type: application/json
Cache-Control: no-cache, no-store
Pragma: no-cache
{
  "access_token": "SlAV32hkKG",
  "token_type": "Bearer",
  "expires_in": 3600,
  "idp_token": "eyJ0 ... NiJ9.eyJ1c ... l6ljlfX0.DeWt4Qu ... ZXso"
  "id_token": "eyJraWQiOiJkZWZhdWx0IiwiaWF0IjoiYXNjaWkiLCJ0eSI6ImF0ifj",
  "state": "af0ifjsldkj"
}
```

### คำอธิบายค่าพารามิเตอร์

| พารามิเตอร์  | Required | รายละเอียด  |
|--------------|----------|---|
| access_token | Required | เป็น token ที่ใช้ในการเข้าถึงบริการหรือข้อมูลจากผู้ให้บริการต่างๆ ที่เชื่อถือ access_token นั้น ออกให้โดย Authorization Server      |
| token_type   | Required | ชนิดของ Token Openid connect กำหนดค่าเป็น Bearer เสมอ   |
| expires_in   | Required | อายุการใช้งานของ access_token มีระยะเวลาเป็นวินาทีนับจากเวลาของการเริ่มสร้าง access_token   |
| id_token     | Required | ข้อมูลอัตลักษณ์ของผู้ใช้งานอยู่ในรูปแบบ JWT (Json Web Token) ถูกแปลงลายมือดิจิทัลด้วย ETDA Connect (ภายในมี id_token ที่ได้จาก IdP) |

ทั้งนี้หากมีการกำหนด **scope** เป็น “profile” รายการข้อมูลของผู้ใช้งานใน id\_token จะถูกกำหนดตาม ตารางที่ 1.5.1

กรณี กำหนด **scope** เป็น “openid profile\_kyc” เพื่อใช้ในการรู้จักลูกค้า (KYC) รายการข้อมูลของผู้ใช้งานใน id\_token จะถูกกำหนดตาม ตารางที่ 1.5.2

### 1.5 ขอบเขตของข้อมูล (scope)

ปัจจุบันระบบ ETDA Connect สามารถรองรับการร้องขอขอบเขตของข้อมูล 3 ประเภท ได้แก่

- 1) openid คือขอบเขตของข้อมูลพื้นฐานที่มาตรฐาน OpenID Connect 1.0 กำหนดให้มีในทุกคำร้องขอการยืนยันตัวตน ดังรายละเอียดในหัวข้อ 4.3 ข้อมูลผลการยืนยันตัวตนและข้อมูลผู้ใช้งาน (ID Token) ในส่วนของ Payload
- 2) profile คือ ขอบเขตของข้อมูลเพื่อวัตถุประสงค์ในการยืนยันตัวตน (Authentication)
- 3) profile\_kyc คือ ขอบเขตของข้อมูลเพื่อวัตถุประสงค์ในการรู้จักลูกค้า (Know Your Customer: KYC)

#### ขอบเขตของข้อมูลประเภท profile

profile เป็นขอบเขตของข้อมูลที่ตอบกลับข้อมูลคุณลักษณะ (Attribute) พื้นฐานของผู้ใช้งาน ที่สามารถระบุได้ว่าผู้ใช้งานเป็นบุคคลใด ซึ่งถูกออกแบบมาเพื่อวัตถุประสงค์ในการยืนยันตัวตน (Authentication) เข้าใช้บริการของ RP

#### รายการข้อมูลใน ID Token เมื่อกำหนดค่า scope เป็น profile

| No. | Short Name      | Type   | คำอธิบาย               | Required / Optional                 |
|-----|-----------------|--------|------------------------|-------------------------------------|
| 1   | given_name      | string | ชื่อ                   | Required                            |
| 2   | family_name     | string | นามสกุล                | Required                            |
| 3   | national_id     | string | หมายเลขประจำตัวประชาชน | Required (กรณีบุคคลที่มีสัญชาติไทย) |
| 4   | passport_number | string | หมายเลขหนังสือเดินทาง  | Required (กรณีบุคคลต่างชาติ)        |

ขอบเขตของข้อมูลประเภท profile\_kyc

profile\_kyc เป็นขอบเขตของข้อมูลที่ตอบกลับข้อมูลคุณลักษณะ (Attribute) ของผู้ใช้งาน ที่ออกแบบมาเพื่อให้ RP ร้องขอข้อมูลเพื่อวัตถุประสงค์ในการรู้จักลูกค้า (Know Your Customer: KYC)

รายการข้อมูลใน ID Token เมื่อกำหนดค่า scope เป็น profile\_kyc

| No. | Short Name      | Type        | คำอธิบาย   | Required / Optional                 |
|-----|-----------------|-------------|--|-------------------------------------|
| 1   | given_name      | string      | ชื่อ   | Required                            |
| 2   | family_name     | string      | นามสกุล  | Required                            |
| 3   | national_id     | string      | หมายเลขประจำตัวประชาชน   | Required (กรณีบุคคลที่มีสัญชาติไทย) |
| 4   | passport_number | string      | หมายเลขหนังสือเดินทาง  | Required (กรณีบุคคลต่างชาติ)        |
| 5   | birthdate       | string      | วัน เดือน ปีเกิด   | Required                            |
| 6   | address         | JSON object | ที่อยู่ที่สำคัญ  | Required                            |
| 6.1 | formatted       | string      | ที่อยู่แบบไม่มีโครงสร้าง สามารถใส่ข้อมูลมากกว่า 1 บรรทัด โดยใช้เครื่องหมาย “\n” แทนการขึ้นบรรทัดใหม่ | Optional                            |

| No. | Short Name       | Type        | คำอธิบาย   | Required / Optional |
|-----|------------------|-------------|--|---------------------|
| 6.2 | street_address   | string      | บ้านเลขที่ ถนน ตำบล  | Optional            |
| 6.3 | locality         | string      | เขต/อำเภอ  | Required            |
| 6.4 | region           | string      | จังหวัด  | Required            |
| 6.5 | postal_code      | string      | รหัสไปรษณีย์   | Optional            |
| 6.6 | country          | string      | ประเทศ   | Optional            |
| 7   | career           | string      | อาชีพ  | Required            |
| 8   | business_address | JSON object | สถานที่ทำงาน   | Required            |
| 8.1 | formatted        | string      | ที่อยู่แบบไม่มีโครงสร้าง สามารถใส่ข้อมูลมากกว่า 1 บรรทัด โดยใช้เครื่องหมาย “\n” แทนการขึ้นบรรทัดใหม่ | Optional            |
| 8.2 | street_address   | string      | บ้านเลขที่ ถนน ตำบล  | Optional            |
| 8.3 | locality         | string      | เขต/อำเภอ  | Required            |
| 8.4 | region           | string      | จังหวัด  | Required            |
| 8.5 | postal_code      | string      | รหัสไปรษณีย์   | Optional            |
| 8.6 | country          | string      | ประเทศ   | Optional            |
| 9   | phone_number     | string      | หมายเลขโทรศัพท์  | Required            |
| 10  | email            | string      | อีเมล  | Required            |

## 1.6 ข้อมูลผลการยืนยันตัวตนและข้อมูลผู้ใช้งาน (ID Token)

ข้อมูลผลการยืนยันตัวตนและข้อมูลผู้ใช้งาน หรือ ID Token ตามมาตรฐาน OpenID Connect 1.0 นั้น จะอยู่ในรูปแบบ JSON Web Token (JWT) ซึ่งถูกแปลงเป็นชื่ออิเล็กทรอนิกส์เพื่อรับรองความถูกต้องครบถ้วน ของข้อมูลตามรูปแบบ JSON Web Signature (JWS) โดยจะประกอบด้วยข้อมูล 3 ส่วน ได้แก่ Header, Payload และ Signature ดังรายละเอียดต่อไปนี้

### 1.6.1 ส่วนของ Header

ข้อมูล ID Token ในส่วนของ Header นี้ เป็นรายการข้อมูลที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์ที่ถูก สร้างจาก IdP และระบบ ETDA Connect โดยรายการดังกล่าวจะแสดงเฉพาะรายการข้อมูลที่เป็นสำหรับการ เชื่อมต่อกับระบบ ETDA Connect เท่านั้น ซึ่งประกอบด้วย

| พารามิเตอร์ | Required | รายละเอียด   |
|-------------|----------|--|
| typ         | Required | กำหนดเป็น “JWT” เสมอ   |
| alg         | Required | พารามิเตอร์ที่ระบุอัลกอริทึมที่ใช้ในการแปลงลายมือชื่ออิเล็กทรอนิกส์ ตามหัวข้อ 4.5 ข้อกำหนดการใช้งานเทคโนโลยีระบบรหัส (Cryptographic Requirement)   |
| x5c         | Required | พารามิเตอร์ที่เก็บใบรับรองอิเล็กทรอนิกส์ตามมาตรฐาน X.509 ที่ เกี่ยวข้องกับการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ทั้งหมด (X.509 Certificate Chain) โดยข้อมูล x5c นี้ถูกกำหนดให้ระบุในส่วนของ Header เพื่อประโยชน์ในการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ได้ ภายหลัง (Long-term Validation) |
| kid         | Required | Identifier ของ key ที่ใช้ในการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์  |

### 1.6.2 ส่วนของ Payload

ข้อมูล ID Token ในส่วนของ Payload นี้ คือรายการข้อมูลผลการยืนยันตัวตนและข้อมูลผู้ใช้งานที่ IdP และระบบ ETDA Connect สร้างขึ้น โดยรายการดังกล่าวจะแสดงเฉพาะรายการข้อมูลที่เป็นสำหรับการ เชื่อมต่อกับระบบ ETDA Connect เท่านั้น ซึ่งประกอบด้วย



| พารามิเตอร์   | Required | รายละเอียด   |
|---------------|----------|--|
| iss           | Required | Identifier ของผู้สร้าง ID Token โดยกำหนดรูปแบบเป็น HTTPS URL<br><i>หมายเหตุ:</i> สำหรับ ID Token ที่สร้างโดย IdP จะระบุเป็น HTTPS URL ของ IdP แต่สำหรับ ID Token ที่สร้างโดยระบบ ETDA Connect จะระบุเป็น HTTPS URL ของระบบ ETDA Connect  |
| sub           | Required | Identifier ที่ IdP ออกให้กับผู้ใช้งานที่ยืนยันตัวตน<br><i>หมายเหตุ:</i> ID Token ที่สร้างโดย IdP และระบบ ETDA Connect จะมีค่าเดียวกัน  |
| aud           | Required | Identifier ของ RP ที่ร้องขอการยืนยันตัวตน (client_id) ที่ IdP หรือระบบ ETDA Connect ออกให้กับ RP<br><i>หมายเหตุ:</i> สำหรับ ID Token ที่สร้างโดย IdP จะระบุเป็นค่า client_id ของระบบ ETDA Connect แต่สำหรับ ID Token ที่สร้างโดยระบบ ETDA Connect จะระบุเป็นค่า client_id ของ RP |
| exp           | Required | เวลาที่ ID Token หมดอายุ โดยอยู่ในรูปแบบของ UNIX timestamp   |
| iat           | Required | เวลาที่ ID Token ถูกสร้างขึ้น โดยอยู่ในรูปแบบของ UNIX timestamp  |
| acr           | Required | ระบุเฉพาะระดับความน่าเชื่อถือ IAL และ AAL ที่ IdP ให้บริการ<br><i>หมายเหตุ:</i> จะปรากฏเฉพาะ ID Token ที่สร้างโดย ระบบ ETDA Connect เท่านั้น   |
| idp_shortname | Required | String ระบุชื่อของ IdP ผู้ออก ID Token<br><i>หมายเหตุ:</i> จะปรากฏเฉพาะ ID Token ที่สร้างโดย ระบบ ETDA Connect เท่านั้น  |
| idp_id_token  | Required | ID Token ที่ระบบ ETDA Connect ได้รับจาก IdP<br><i>หมายเหตุ:</i> จะปรากฏเฉพาะ ID Token ที่สร้างโดย ระบบ ETDA Connect เท่านั้น   |

\*\*\* **หมายเหตุ** นอกเหนือจากรายการพารามิเตอร์ตามตารางด้านบน ยังมีรายการพารามิเตอร์อื่นปรากฏใน ID Token ได้ เช่น ชื่อ ที่อยู่ อีเมลของผู้ใช้งาน ขึ้นอยู่กับการกำหนดพารามิเตอร์ scope ในขั้นตอน (b) ดังรายละเอียดในหัวข้อ 4.4 ขอบเขตของข้อมูล (Scope)

### 1.6.3 ส่วนของ Signature

ข้อมูล ID Token ในส่วนของ Signature นี้ เป็นส่วนสำคัญที่ใช้ในการตรวจสอบความถูกต้องครบถ้วนของ ID Token ซึ่งจะมีรูปแบบที่แตกต่างกันไปขึ้นอยู่กับอัลกอริทึม (Algorithm) ที่ IdP และระบบ ETDA Connect ใช้ในการลงลายมือชื่ออิเล็กทรอนิกส์

### 1.6.4 ตัวอย่าง ID Token

ตัวอย่าง ID Token ที่ IdP ส่งให้ระบบ ETDA Connect

Header:

```
{
  "alg": "RS256",
  "typ": "JWT",
  "kid": "3e0r02045mm5qlea56159fskd53ec1e9omg",
  "x5c": ["OuH0aBDQjCCAi9gAwlBAu6/KglGATz/FuSqGS1b3D ...
    BqLdElrRhjZkAzVvMI1b3dFUJheLiMA0GCBTWVU+4EjYx8sX=",
    "GA1UNAQ0wDQYJKoZIhTXMIIE+zCdMwzzvcBBGSgAwlBAglC ...
    AwgbsxJDAAcTQsxsjvITmV0d29yazEXMBUCAQEFBQNLiBgNVcn"]
}
```

Payload:

```
{
  "iss": " http://idp01.com",
  "sub": "114386995432676543513",
  "aud": "dcd27uq4nojetqu8e1kf8p8vatsbnd55",
  "exp": 1519798006,
  "iat": 1519794406,
  "given_name": "Somchai",
  "family_name": "Wahnpong",
  "national_id": "1724747767301",
  "passport_number": "AA7562739"
}
```

```
}

```

Signature:

```
dLP19D4HoJ_6E-0vAsufmli8C58LLSHpCO1VFOFknJe5rW20egUxnzWENA5Pxd2F5FHx7quOHTKV
zw1EtpQjGdAuaVAfl5e42vI8AnDPPMymcsLC2zKthDCnYud6cN7ciemI7vx9ysmyrmVRqT-
Jen9JRL6FTdv3QH_DQHLaAPclw-_fAFVYVz7k8pEGJ2wQL8RANMF2zil-bG8tZmAW4OwqZB_
sj9fCmmiwHrXmWaQduS9ceSpRbdDngcjs8IOwTqoA4fqel147Vzc6HFAvQ

```

**ตัวอย่าง ID Token ที่ระบบ ETDA Connect ส่งให้ RP**

Header:

```
{
  "alg": "RS256",
  "typ": "JWT",
  "kid": "6b46020457cc1ea561f4ed53ec1e5ea",
  "x5c": ["MIIDQjCCAiQgAwIBAgIGATz/FuLiMA0GCSqGSIb3D ...
    BqLdElrRhjZkAzVvb3du6/KFUJheqwNTrZEjYx8 OuH0aBsXBTWVU+4=",
    "MIIE+zCCBGsGAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQ ...
    AwgbsxJDAiBgNVBAcTTmV0d29yazEXMBUGA1UNlcnQsxTXdMwzzjsvl"]
}
```

Payload:

```
{
  "iss": " https://proxy1.auth.teda.th/proxy/v1",
  "sub": "114386995432663743513",
  "aud": "7e4ca2fa5d074543cf6a",
  "exp": 1519795196,
  "iat": 1519791596,
  "acr": "urn:did:ial:2 urn:did:aal:2",
  "idp_shortname": "idp01",
  "idp_id_token": "eyJhbGciOiJIY1OWYwNzM1OGZkZjgyODhjZTU5ZjE4OUM0MDI4ZjQifQ.eyJh
    enAiOiJhbnNzE2ODEwOHF1OG1CUWxtV2Q5cB2NhbGJ9.jdWoS3Dqan3Eg3EitHj
    -snhIBhlbePVrGcQqw148_-1rGtE1XJnk ... UhcigXM5JsW_b0Au7E- FzD3wVaa 2-
    R_hA",
  "given_name": "Somchai",
  "family_name": "Wahnpong",
}
```

```
"national_id": "1724747767301",  
"passport_number": "AA7562739"  
}
```

Signature:

```
dLP19D4HoJ_6E-0vAsufmli8C58LLSHpCO1VFOFKnJe5rW20egUxnzWENA5Pxd2F5FHx7quOHTKV  
zw1EtpQjGdAuaVAfl5e42vI8AnDPPMymcsLC2zKthDCnYud6cN7ciemI7vx9ysmyrmVRqT-  
Jen9JRL6FTdv3QH_DQHLAaPclw-_fAFVYVz7k8pEGJ2wQL8RANMF2zil-bG8tZmAW4OwqZB_  
sj9fCmmiwHrXmWaQduS9ceSpRbdDngcjs8IOwTqoA4fqel147Vzc6HFAvQ
```

### 1.6.5 การตรวจสอบความถูกต้องของข้อมูล ID Token

เมื่อ RP ได้รับ ID Token จาก ETDA Connect แล้ว RP จะต้องตรวจสอบความถูกต้องของข้อมูลใน ID Token มีรายละเอียดดังต่อไปนี้

#### ตรวจสอบความถูกต้องครบถ้วนของ ID Token

ID Token ที่ได้รับมา มีความถูกต้อง และข้อมูลภายใน ID Token ไม่ถูกเปลี่ยนแปลง

- ตรวจสอบความถูกต้องของลายมือชื่ออิเล็กทรอนิกส์ที่ลงบน ID Token ข้อกำหนด JWS โดยใช้อัลกอริทึมที่ระบุในรายการข้อมูล alg และใช้กุญแจสาธารณะที่ระบุใน JWKS endpoint ของ ETDA Connect

#### ตรวจสอบข้อมูลเวลา

- ตรวจสอบเวลาที่ ID Token หมดอายุ โดยตรวจสอบเวลาปัจจุบันจะต้องไม่เกินเวลาที่ระบุในรายการข้อมูล exp
- ตรวจสอบเวลาที่ ID Token ถูกสร้างขึ้น โดยตรวจสอบเวลาปัจจุบันจะต้องไม่เกินเวลาที่ระบุในรายการข้อมูล iat ไม่เกิน 5 นาที

#### ตรวจสอบความถูกต้องของข้อมูลอื่น ๆ

- ตรวจสอบความถูกต้องของ Client ID ในรายการข้อมูล aud ว่าถูกต้องตรงกับ Client ID ของหน่วยงานที่ลงทะเบียนไว้กับ ETDA Connect ทั้งนี้ aud อาจมีข้อมูลได้หลายรายการ RP ต้องตรวจสอบรายการข้อมูล aud ด้วย หากมีค่าของ aud ที่ไม่ถูกต้องและไม่น่าเชื่อถือ ถือว่า ID Token ที่รับมาน่าเชื่อถือ

- ตรวจสอบ Identifier ของผู้สร้าง ID Token โดยให้ตรวจสอบว่าค่าของ iss ต้องตรงกับค่าของ issuer ที่ระบุใน Discovery Endpoint
- ตรวจสอบรายการข้อมูล acr จะต้องมามีข้อมูลระดับของ IAL AAL และข้อมูล Sector ว่าตรงกับข้อมูลที่ร้องขอไปให้ ETDA Connect หรือไม่



## 2. ข้อความแจ้งกลับข้อผิดพลาด ERROR RESPONSE

ในกระบวนการยืนยันตัวตนทางอิเล็กทรอนิกส์ด้วยโปรโตคอล OpenID กำหนดรายละเอียดในการแจ้งกลับข้อผิดพลาด (Error Response) โดยมีข้อกำหนดพารามิเตอร์ดังต่อไปนี้

| พารามิเตอร์       | Required | รายละเอียด  |
|-------------------|----------|---|
| error             | Required | Error code แจ้งสาเหตุของข้อผิดพลาดที่เกิดขึ้น   |
| error_description | Optional | ใช้ในการแสดงรายละเอียดข้อผิดพลาดของระบบ ในรูปแบบ text   |
| state             | Required | string ใช้ในการตรวจสอบความสัมพันธ์ระหว่าง request กับ response เพื่อป้องกันการโจมตีแบบ Cross-Site Request Forgery โดยค่า state ในการตอบกลับจะต้องเป็นค่าเดียวที่รับ |
| error_uri         | Optional | URI เพื่อแจ้งข้อมูลของ Error ที่ระบุ อาจเป็น Webpage  |

สำหรับพารามิเตอร์ error ของ error response สามารถระบุ Error code ได้ดังตารางต่อไปนี้

| Error code                | คำอธิบาย  | HTTP Return Code |
|---------------------------|---|------------------|
| invalid_request           | ข้อมูล request ไม่ถูกต้อง   | 302              |
| unauthorized_client       | Client ไม่ได้รับอนุญาตให้ร้องขอด้วยวิธีการที่ระบุ   | 302              |
| unsupported_response_type | Server ไม่รองรับการร้องขอตามที่ระบุ   | 302              |
| invalid_scope             | ข้อมูล Scope ที่ร้องขอไม่ถูกต้อง หรือขาดหาย   | 302              |
| server_error              | พบข้อผิดพลาดของ Server<br>(Return Error 500 Internal Server Error เนื่องจากไม่สามารถส่งพารามิเตอร์ให้ Client ผ่านทาง HTTP Redirect ได้)   | 500              |
| temporarily_unavailable   | พบข้อผิดพลาดของ Server เนื่องจาก Server ไม่สามารถรองรับภาระ Load ได้ หรืออยู่ระหว่างการปรับปรุง Server<br>(Return Error 503 Service Unavailable เนื่องจากไม่สามารถส่งพารามิเตอร์ให้ Client ผ่านทาง HTTP Redirect ได้) | 503              |

|                        |   |     |
|------------------------|---|-----|
| interaction_required   | Authorization Server ต้องการให้ ผู้ใช้บริการทำการยืนยันตัวตนผ่านแบบฟอร์ม หรือ หน้าจอ ข้อมูล Error นี้ อาจถูกส่งกลับในกรณี ที่ Parameter Prompt ถูกกำหนดเป็น none การยืนยันตัวตนจึงไม่สามารถ ดำเนินการต่อได้ | 302 |
| login_required         | Authorization Server ต้องการให้ ผู้ใช้บริการทำการยืนยันตัวตน ข้อมูล Error นี้ อาจถูกส่งกลับในกรณีที่ Parameter Prompt ถูกกำหนดเป็น none การยืนยันตัวตนจึงไม่ สามารถดำเนินการต่อได้                          | 302 |
| consent_required       | Authorization Server ต้องการให้ ผู้ใช้บริการทำการยินยอมเพื่อให้ข้อมูล Error นี้ อาจถูกส่งกลับในกรณีที่ Parameter Prompt ถูกกำหนดเป็น none การให้ข้อมูล จึงไม่สามารถดำเนินการต่อได้                          | 302 |
| invalid_request_uri    | ข้อมูล request_uri ไม่ถูกต้อง   | 400 |
| invalid_request_object | ข้อมูล request_object ไม่ถูกต้อง  | 302 |

ตัวอย่าง HTTP Response Error

|  |
|--|
| <p>HTTP/1.1 302 Found</p> <p>Location: <a href="https://rp.example.org/callback?error=invalid_request&amp;error_description=Unsupported%20response_type%20value&amp;state=af0ifjsldkj">https://rp.example.org/callback?error=invalid_request&amp;error_description=Unsupported%20response_type%20value&amp;state=af0ifjsldkj</a></p> |
|--|

ในกระบวนการยืนยันตัวตนทางอิเล็กทรอนิกส์ด้วยโปรโตคอล OpenID กำหนดรายละเอียดในการแจ้งกลับข้อผิดพลาด (Error Response) ของ Token Request โดยมีข้อกำหนดพารามิเตอร์ดังต่อไปนี้

| Error code             | คำอธิบาย   | HTTP Return Code |
|------------------------|--|------------------|
| invalid_request        | ข้อมูล request ไม่ถูกต้อง  | 400              |
| invalid_client         | ข้อมูล client ไม่ถูกต้อง หรือ ไม่รองรับการวิธีการร้องขอที่ client ระบุ | 401              |
| invalid_grant          | ข้อมูล authorization code ไม่ถูกต้องหรือหมดอายุ                        | 400              |
| unauthorized_client    | Client ไม่ได้ได้รับอนุญาตให้ร้องขอด้วยวิธีการที่ระบุ                   | 400              |
| unsupported_grant_type | Authorization Server ไม่รองรับ grant type ตามที่ระบุ                   | 400              |
| invalid_scope          | ข้อมูล Scope ที่ร้องขอไม่ถูกต้อง หรือขาดหาย                            | 400              |

#### ตัวอย่าง Error Response ของ Token Request

```
HTTP/1.1 400 Bad Request
Content-Type: application/json
Cache-Control: no-store
Pragma: no-cache
{
  "error": "invalid_request"
}
```



### ภาคผนวก ก. การร้องขอข้อมูลการเชื่อมต่อผ่าน DISCOVERY ENDPOINT

---

มาตรฐาน OpenID Connect 1.0 ได้มีการกำหนดรูปแบบการเผยแพร่ข้อมูลการเชื่อมต่อผ่าน Discovery Endpoint ในรูปแบบ URL ([https://{ETDA Connect\\_URL}/.well-known/openid-configuration](https://{ETDA Connect_URL}/.well-known/openid-configuration)) เพื่อให้ RP ใช้เป็นข้อมูลในการเชื่อมต่อระบบ โดยปัจจุบัน Discovery Endpoint สามารถดูได้ที่ URL

- <https://proxy1.auth.teda.th/proxy/v1/.well-known/openid-configuration>