[2018]

ข้อกำหนดทางเทคนิค (Technical Specification)

ในส่วนของการเชื่อมต่อด้วย WEB API สำหรับ RELYING PARTY

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

API DOCUMENT FOR RELYING PARTY

วัตถุประสงค์ (**Objective**)	เพื่อเป็นคู่มือที่ใช้สำหรับการเชื่อมต่อ Application Programming Interface (API) ของ Relying Party
เจ้าของโครงการ (**Ownership**)	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
วันที่เริ่มโครงการ (**Start Date**)	1 มกราคม 2561
วันที่สิ้นสุดโครงการ (**Completion Date**)	
ประกาศโครงการ (**Important Notice**)	

ข้อมูลเอกสาร (DOCUMENT INFORMATION)

วัตถุประสงค์ (Objective)	เพื่อเป็นแนวทางของ RP ในการเตรียมการเชื่อมต่อกับระบบ Federation Proxy 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 และรายละเอียด เพิ่มเติมเกี่ยวกับ ID Token
1.0	22 พ.ค. 2561	ETDA	- ปรับปรุงรายละเอียดคำอธิบายขั้นตอน และ Web API ในหัวข้อที่ 1.4 - เปลี่ยน Error code ของ invalid_request_uri จาก 302 เป็น 400 - เพิ่มภาคผนวก ก. การเรียกดูข้อมูลการเชื่อมต่อผ่าน Discovery Endpoint
1.0	26 พ.ค. 2561	ETDA	- ปรับปรุง post reqeust เป็น json body

สารบัญ

1. การเชื่อมต่อ RP กับระบบ FEDERATION PROXY

1.1 การเตรียมข้อมูลสำหรับเชื่อมต่อกับระบบ Federation Proxy

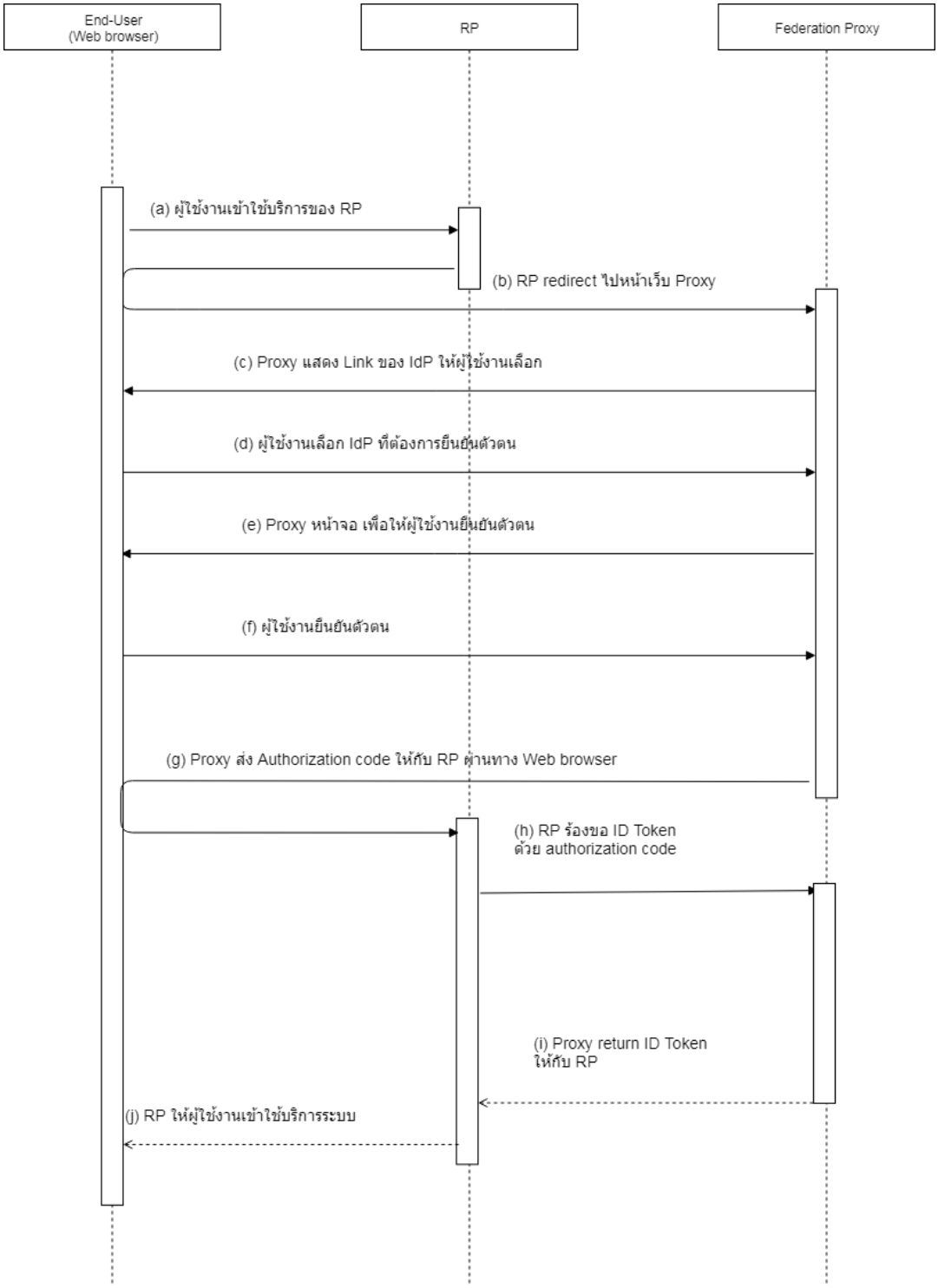
ในการเชื่อมต่อระหว่าง IdP และ RP นั้น ระบบ Federation Proxy จะเป็นตัวกลางในการเชื่อมต่อผ่านโปรโตคอล OpenID Connect 1.0 โดยก่อนเริ่มการเชื่อมต่อกับระบบ Federation Proxy นั้น RP จะต้องเตรียมข้อมูลเบื้องต้นและกำหนดช่องทาง (ในรูปแบบ URL) ในการร้องข้อมูลการตามที่โปรโตคอล OpenID Connect 1.0 กำหนดและส่งให้กับ Federation s ดังรายละเอียดต่อไปนี้

1) Redirect URL: URL สำหรับรับ Response ของ authentication request จาก Federation Proxy
2) ข้อมูลเพื่อใช้ในการลงทะเบียนกับ Federation Proxy 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 Federation Proxy สามารถใช้งาน Library ที่ผ่านการรับรองจาก OpenID Foundation ซึ่งผู้พัฒนาสามารถหา Library ตามความเหมาะสมกับภาษาที่ใช้พัฒนา โดยข้อมูลของ Library ที่ใช้พัฒนาสามารถหาได้จาก URL : http://openid.net/developers/certified

1.2 กระบวนการทำงานของการยืนยันตัวตนทางอิเล็กทรอนิกส์โดยมี Federation Proxy



1.3 ขั้นตอนการทำงานของการยืนยันตัวตนทางอิเล็กทรอนิกส์โดยมี Federation Proxy

1. ผู้ใช้งานพิมพ์ URL ของ Relying Party เพื่อเข้าใช้งานระบบผ่านทาง Web Browser
2. Relying Party ทำการร้องขอการยืนยันตัวตนผู้ใช้งานไปยังระบบ Federation Proxy 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 พร้อมทั้งให้ผู้ใช้ยืนยันความถูกต้องของข้อมูลและยินยอม (Consent) ในการเปิดเผยข้อมูลแก่ Relying Party
6. เมื่อผู้ใช้งานยืนยันความถูกต้องของข้อมูลและยินยอมเปิดเผยข้อมูลแล้ว ผู้ใช้งานถูก redirect ไปยัง Federation Proxy พร้อมผลการยืนยันตัวตน ซึ่งเรียกว่า Authentication code ให้กับ Proxy
7. Proxy ทำการส่ง Authentication code ให้กับ Relying Party ผ่านทาง Web Browser
8. Relying Party ทำการขอข้อมูลจาก Identity Provider โดยการส่ง Authentication code ไปยัง Proxy
9. Proxy นำ Authentication Code ที่ได้รับจาก Relying Party ตรวจสอบ Authentication Code หาก Authentication Code ถูกต้อง Proxy จะส่ง Assertion กลับมายัง RP โดยการระบุข้อมูลไว้ใน ID Token ซึ่ง Assertion ต้องถูกลงลายมือชื่ออิเล็กทรอนิกส์ด้วยกุญแจส่วนตัว (Private key) Proxy ด้วย
10. Relying Party ทำการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ที่ลงใน ID Token ว่าถูกส่งมาจาก Federation Proxy หากลายมือชื่ออิเล็กทรอนิกส์ถูกต้อง Relying Party ก็สามารถเชื่อถือได้ว่าผู้ใช้งานได้ทำการยืนยันตัวตนแล้วกับ Identity Provider ที่น่าเชื่อถือตามระดับ LoA ที่กำหนดไว้และอนุญาตให้ผู้ใช้งานเข้าใช้ระบบได้

1.4 รายละเอียดของขั้นตอนและการเชื่อมต่อ RP กับ Proxy ด้วย Web API

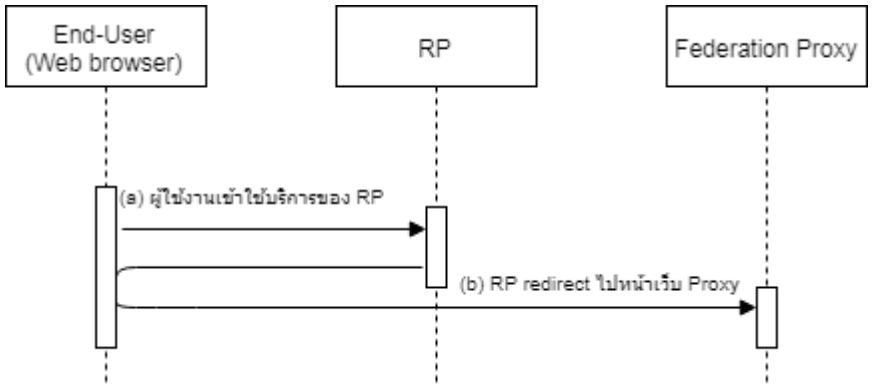
ขั้นตอนการยืนยันตัวตนทางอิเล็กทรอนิกส์กับระบบ Federation Proxy ประกอบด้วย 3 ขั้นตอนหลัก ดังต่อไปนี้

ขั้นตอนหลักที่ 1: RP ร้องขอการยืนยันตัวตน ผ่าน Authorization Endpoint

ขั้นตอนหลักที่ 2: ระบบ Federation Proxy ส่ง Authorization Code ให้กับ RP

ขั้นตอนหลักที่ 3: RP ร้องขอ Access Token และ ID Token ผ่าน Token Endpoint

1.4.1 ขั้นตอน RP Request ขอหน้าจอของแสดงรายการ IdP โดยมี Message ดังนี้



Request

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

พารามิเตอร์

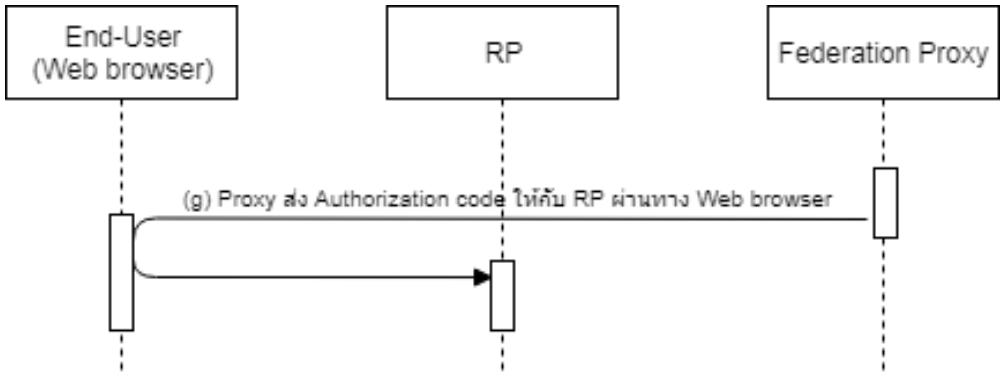
พารามิเตอร์	Required	รายละเอียด
response_type	Required	กำหนดค่าเป็น “code”
client_id	Required	identifier ที่ใช้ระบุ RP

พารามิเตอร์	Required	รายละเอียด
scope	Required	ขอบเขตหรือชุดของข้อมูลที่ร้องขอ ค่าของ scope ให้กำหนดเป็น และตามด้วย profile หรือ profile_kyc ในกรณีที่ต้องการเชื่อมต่อ ndid ให้ใช้ ndid
redirect_uri	Required	กำหนดค่าเป็น HTTP endpoint (url) ของ RP ใช้สำหรับ redirect กลับไปยัง เว็บไซต์ของ RP เมื่อการยืนยันตัวตนเสร็จสิ้น ซึ่งค่าของ redirect_url ต้องเป็น url ที่ได้ลงทะเบียนไว้กับ Proxy
state	Required	string ใช้ในการตรวจสอบความสัมพันธ์ระหว่าง request (จาก RP) กับ response (ของ Proxy) เพื่อป้องกันการโจมตีแบบ Cross-Site Request Forgery (CSRF, XSRF) โดยค่าของ state อาจทำได้โดย encode ค่า hash ของ browser cookie เพื่อตรวจสอบว่า request ที่เกิดขึ้น และ callback ที่ส่งกลับมาที่ browser เดียวกัน
prompt	Required	ให้กำหนดค่าเป็น “login consent”
acr_values	Optional	เป็นค่าที่ระบุเพื่อขอให้ RP แสดงรายการ IdP ที่เกี่ยวข้อง โดยเกณฑ์การเลือกแสดง IdP โดยให้ระบุค่า ดังต่อไปนี้ (สามารถระบุได้มากกว่า 1) - ระบุ IAL โดยมีรูปแบบ urn:did:ial:[ระดับของ ial] ตัวอย่าง การระบุ IAL ระดับ 2.1 ขึ้นไป : urn:did:ial:2_1 - ระบุ AAL โดยมีรูปแบบ urn:did:ial:[ระดับของ aal] ตัวอย่าง การระบุ AAL ระดับ 2.1 ขึ้นไป : urn:did:aal:2_1 - ระบุ sector คือการระบุ IdP ที่ให้บริการสำหรับเฉพาะกลุ่มธุรกิจ โดยมีรูปแบบ urn:did:sector:[sector short name] ตัวอย่าง ระบุ IdP สำหรับภาครัฐ: urn:did:sector:government - ระบุชื่อ IdP มีรูปแบบ urn:did:idp:[idp short name] ตัวอย่าง ระบุชื่อของ IdP : urn:did:idp:idp001

ตัวอย่าง HTTP Request

```
GET  https://openid1.digitalidproxy.or.th/oauth2/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 Federation Proxy ส่ง Authorization Code ให้กับ RP



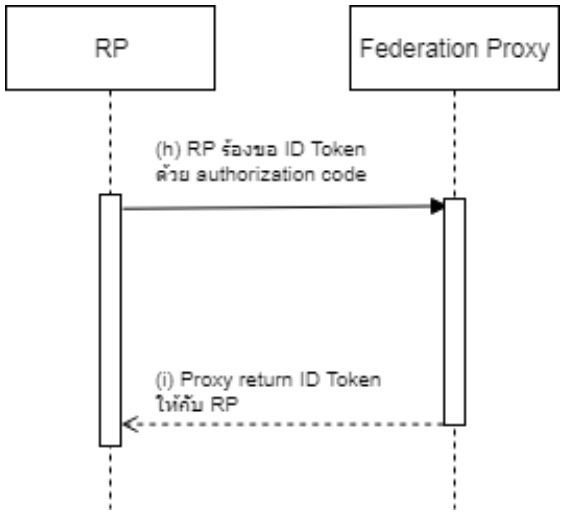
ระบบ Federation Proxy จะทำการส่ง Authorization Code ให้กับ RP ด้วย HTTP GET โดยมีพารามิเตอร์ดังต่อไปนี้

```
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 Proxy ด้วย authoruzation code

RP ขอข้อมูล ID Token ผ่าน Proxy โดยการส่ง Reqeust เป็น HTTP Post ไปยัง Proxy 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://example.digitalidproxy.or.th/authorize

พารามิเตอร์

พารามิเตอร์	Required	รายละเอียด
grant_type	Required	ใช้ค่า “authorization_code”
Code	Required	Authentication Code ที่ได้รับจาก Proxy
redirect_uri	Required	URI ที่ใช้ในการ Call Back ซึ่งถูกระบุไว้กับทาง Proxy

ตัวอย่างการส่ง HTTP Request

ส่ง Request ไปยังด้วย Http Post ไปยัง Proxy โดยมี พารามิเตอร

```
POST  https://openid1.digitalidproxy.or.th/oauth2/token HTTP/1.1
      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 Proxy ตรวจสอบ code และ redirect_uri ว่าถูกต้องแล้ว Proxy จะส่ง Access Token และ ID Token กลับมายัง RP ดังต่อไปนี้

ตัวอย่างการส่ง HTTP Response ของ Proxy 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 ...I6IjlifX0.DeWt4Qu ... ZXso"
  "Id_token": "eyJraWQiOiJkZWZhdWx0IiwiYWxnIjo....",
  "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) ถูกลงลายมือดิจิทัลด้วย Proxy (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 Federation Proxy สามารถรองรับการร้องขอขอบเขตของข้อมูล 3 ประเภท ได้แก่

1) openid คือขอบเขตของข้อมูลพื้นฐานที่มาตรฐาน OpenID Connect 1.0 กำหนดให้มีในทุกคำรองขอการยืนยันตัวตน ดังรายละเอียดใน*หัวข้อ 4.3 ข้อมูลผลการยืนยันตัวตนและข้อมูลผู้ใช้งาน (ID Token) ในส่วนของ Payload*
2) profile คือ ขอบเขตของข้อมูลเพื่อวัตถุประสงค์ในการยืนยันตัวตน (Authentication)
3) profile_kyc คือ ขอบเขตของข้อมูลเพื่อวัตถุประสงค์ในการรู้จักลูกค้า (Know Your Customer: KYC)
4) ndid คือ ขอบเขตของข้อมูลเพื่อวัตถุประสงค์ในการเชื่อมต่อเพื่อขอยืนยันตัวตนไปยังระบบ NDID Platform

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)

No.	Short Name	Type	คำอธิบาย	Required / Optional
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	ที่อยู่ที่อาศัย	Required
6.1	formatted	string	ที่อยู่แบบไม่มีโครงสร้าง สามารถใส่ข้อมูลมากกว่า 1 บรรทัด โดยใช้เครื่องหมาย “\n” แทนการขึ้นบรรทัดใหม่	Optional
6.2	street_address	string	บ้านเลขที่ ถนน ตำบล	Optional

No.	Short Name	Type	คำอธิบาย	Required / 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	สถานทำงาน	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

รายการข้อมูลใน ID Token เมื่อกำหนดค่า scope เป็น ndid

No.	Short Name	Type	คำอธิบาย	Required / Optional
1	request_id	string	ข้อมูล request id ที่เรียกไปยัง ndid	Required
3	national_id	string	หมายเลขประจำตัวประชาชน	Required (กรณีบุคคลที่มีสัญชาติไทย)

1.6 ข้อมูลผลการยืนยันตัวตนและข้อมูลผู้ใช้งาน (ID Token)

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

1.6.1 ส่วนของ Header

ข้อมูล ID Token ในส่วนของ Header นี้ เป็นรายการข้อมูลที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์ที่ถูกสร้างจาก IdP และระบบ Federation Proxy โดยรายการดังกล่าวจะแสดงเฉพาะรายการข้อมูลที่จำเป็นสำหรับการเชื่อมต่อกับระบบ Federation Proxy เท่านั้น ซึ่งประกอบด้วย

พารามิเตอร์	Required	รายละเอียด
typ	Required	กำหนดเป็น “JWT” เสมอ
alg	Required	พารามิเตอร์ที่ระบุอัลกอริทึมที่ใช้ในการลงลายมือชื่ออิเล็กทรอนิกส์ ตาม*หัวข้อ 4.5 ข้อกำหนดการใช้งานเทคโนโลยีระบบรหัส (Cryptographic Requirement)*
x5c	Required	พารามิเตอร์ที่เก็บใบรับรองอิเล็กทรอนิกส์ตามมาตรฐาน X.509 ที่เกี่ยวข้องกับการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ทั้งหมด (X.509 Certificate Chain) โดยข้อมูล x5c นี้ถูกกำหนดให้ระบุในส่วนของ

พารามิเตอร์	Required	รายละเอียด
		Header เพื่อประโยชน์ในการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ได้ภายหลัง (Long-term Validation)
kid	Required	Identifier ของ key ที่ใช้ในการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์

1.6.2 ส่วนของ Payload

ข้อมูล ID Token ในส่วนของ Payload นี้ คือรายการข้อมูลผลการยืนยันตัวตนและข้อมูลผู้ใช้งานที่ IdP และระบบ Federation Proxy สร้างขึ้น โดยรายการดังกล่าวจะแสดงเฉพาะรายการข้อมูลที่จำเป็นสำหรับการเชื่อมต่อกับระบบ Federation Proxy เท่านั้น ซึ่งประกอบด้วย

พารามิเตอร์	Required	รายละเอียด
iss	Required	Identifier ของผู้ที่สร้าง ID Token โดยกำหนดรูปแบบเป็น HTTPS URL *<u>หมายเหตุ:</u> สำหรับ ID Token ที่สร้างโดย IdP จะระบุเป็น HTTPS URL ของ IdP แต่สำหรับ ID Token ที่สร้างโดยระบบ Federation Proxy จะระบุเป็น HTTPS URL ของระบบ Federation Proxy*
sub	Required	Identifier ที่ IdP ออกให้กับผู้ใช้งานที่ยืนยันตัวตน *<u>หมายเหตุ:</u> ID Token ที่สร้างโดย IdP และระบบ Federation Proxy จะมีค่าเดียวกัน*
aud	Required	Identifier ของ RP ที่ร้องขอการยืนยันตัวตน (client_id) ที่ IdP หรือระบบ Federation Proxy ออกให้กับ RP *<u>หมายเหตุ:</u> สำหรับ ID Token ที่สร้างโดย IdP จะระบุเป็นค่า client_id ของระบบ Federation Proxy แต่สำหรับ ID Token ที่สร้างโดยระบบ Federation Proxy จะระบุเป็นค่า client_id ของ RP*
exp	Required	เวลาที่ ID Token หมดอายุ โดยอยู่ในรูปแบบของ UNIX timestamp

พารามิเตอร์	Required	รายละเอียด
iat	Required	เวลาที่ ID Token ถูกสร้างขึ้น โดยอยู่ในรูปแบบของ UNIX timestamp
acr	Required	ระบุเฉพาะระดับความน่าเชื่อถือ IAL และ AAL ที่ IdP ให้บริการ *<u>หมายเหตุ:</u> จะปรากฏเฉพาะ ID Token ที่สร้างโดย ระบบ Federation Proxy เท่านั้น*
idp_shortname	Required	String ระบุชื่อของ IdP ผู้ออก ID Token *<u>หมายเหตุ:</u> จะปรากฏเฉพาะ ID Token ที่สร้างโดย ระบบ Federation Proxy เท่านั้น*
idp_id_token	Required	ID Token ที่ระบบ Federation Proxy ได้รับจาก IdP *<u>หมายเหตุ:</u> จะปรากฏเฉพาะ ID Token ที่สร้างโดย ระบบ Federation Proxy เท่านั้น*

*** **<u>หมายเหตุ</u>** นอกเหนือจากรายการพารามิเตอร์ตามตารางด้านบน ยังมีรายการพารามิเตอร์อื่นปรากฏใน ID Token ได้ เช่น ชื่อ ที่อยู่ อีเมลของผู้ใช้งาน ขึ้นอยู่กับการกำหนดพารามิเตอร์ scope ในขั้นตอน **(b)** ดังรายละเอียดใน*หัวข้อ 4.4 ขอบเขตของข้อมูล (Scope)*

1.6.3 ส่วนของ Signature

ข้อมูล ID Token ในส่วนของ Signature นี้ เป็นส่วนสำคัญที่ใช้ในการตรวจความถูกต้องครบถ้วนของ ID Token ซึ่งจะมีรูปแบบที่แตกต่างกันไปขึ้นอยู่กับอัลกอริทึม (Algorithm) ที่ IdP และระบบ Federation Proxy ใช้ในการลงลายมือชื่ออิเล็กทรอนิกส์

1.6.4 ตัวอย่าง ID Token

ตัวอย่าง ID Token ที่ IdP ส่งให้ระบบ Federation Proxy

Header:

```
{
```

```
"alg": "RS256",
"typ": "JWT",
"kid": "3e0r02045mm5qlea56159fskd53ec1e9omg",
"x5c": ["OuH0aBDQjCCAiqgAwIBAu6/KgIGATz/FuSqGSIb3D ...
        BqLdElrRhjZkAzVvMIIb3dFUJheLiMA0GCBTWVU+4EjYx8sX=",
        "GA1UNAQ0wDQYJKoZIhTXMIIE+zCdMwzzvcBBGSgAwIBAgIC ...
        AwgbsxJDAAcTQsxjsvITmV0d29yazEXMBUCAQEFBQNliBgNVcn"]
}
```


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_
sj9fCmmiwHrXmWaQduS9ceSpRbdDngcjs8IOwTqoA4fqeI147Vzc6HFAvQ
```


ตัวอย่าง ID Token ที่ระบบ Federation Proxy ส่งให้ RP

Header:

```
{
"alg": "RS256",
"typ": "JWT",
"kid": "6b46020457cc1ea561f4ed53ec1e5ea",
"x5c": ["MIIDQjCCAiqgAwIBAgIGATz/FuLiMA0GCSqGSIb3D ...
        BqLdElrRhjZkAzVvb3du6/KFUJheqwNTrZEjYx8 OuH0aBsXBTWVU+4=",
        "MIIE+zCCBGSgAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQ ...
        AwgbsxJDAiBgNVBAcTTmV0d29yazEXMBUGA1UNlcnQsxTXdMwzzjsvI"]
}
```


Payload:


```
{
"iss": " https://proxy.digitalid.or.th",
"sub": "114386995432663743513",
"aud": "7e4ca2fa5d074543cf6a",
"exp": 1519795196,
"iat": 1519791596,
"acr": "urn:did:ial:2 urn:did:aal:2",
"idp_shortname": "idp01",
"idp_id_token": "eyJhbGciOiJY1OWYwNzM1OGZkZjgyODhjZTU5ZjE4OWM0MDI4ZjQifQ.eyJh
                enAiOiIyNjE5NzE2ODEwOHF1OG1CUWxtV2Q5cB2NhbGJ9.jdWoS3Dqan3Egj3EitHj
                -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_
sj9fCmmiwHrXmWaQduS9ceSpRbdDngcjs8lOwTqoA4fqeI147Vzc6HFAvQ

1.6.5 การตรวจสอบความถูกต้องของข้อมูล ID Token

เมื่อ RP ได้รับ ID Token จาก Federation Proxy แล้ว RP จะต้องตรวจสอบความถูกต้องของข้อมูลใน ID Token มีรายละเอียดดังต่อไปนี้

ตรวจสอบความถูกต้องครบถ้วนของ ID Token

ID Token ที่ได้รับมามีความถูกต้อง และข้อมูลภายใน ID Token ไม่ถูกเปลี่ยนแปลง

- ตรวจสอบความถูกต้องของลายมือชื่ออิเล็กทรอนิกส์ที่ลงบน ID Token ข้อกำหนด JWS โดยใช้อัลกอริทึมที่ระบุในรายการข้อมูล alg และใช้กุญแจสาธารณะที่ระบุใน JWKS endpoint ของ Federation Proxy

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 ของหน่วยงานที่ได้ลงทะเบียนไว้กับ Federation Proxy ทั้งนี้ aud อาจมีข้อมูลได้หลายรายการ RP ต้องตรวจสอบรายการข้อมูล aud ด้วย หากมีค่าของ aud ที่ไม่ถูกต้องและไม่น่าเชื่อถือ ถือว่า ID Token ที่รับมาไม่น่าเชื่อถือ

- ตรวจสอบ Identifier ของผู้ที่สร้าง ID Token โดยให้ตรวจสอบว่าค่าของ iss ต้องตรงกับค่าของ issuer ที่ระบุใน Discovery Endpoint
- ตรวจสอบรายการข้อมูล acr จะต้องมีข้อมูลระดับของ IAL AAL และข้อมูล Sector ว่าตรงกับข้อมูลที่ร้องขอไปให้ Federation Proxy หรือไม่

2. ข้อความแจ้งกลับข้อผิดพลาด ERROR RESPONSE

ในกระบวนการยืนยันตัวตนทางอิเล็กทรอนิกส์ด้วยโปรโตคอล OpenID กำหนดรายละเอียดในการแจ้งกลับข้อผิดพลาด (Error Response) โดยมีต้องกำหนดพารามิเตอร์ดังต่อไปนี้

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 (Return Error 500 Internal Server Error เนื่องจากไม่สามารถส่งพารามิเตอร์ให้ Client ผ่านทาง HTTP Redirect ได้)	500

temporarily_unavailable	พบข้อผิดพลาดของ Server เนื่องจาก Server ไม่สามารถรองรับภาระ Load ได้ หรืออยู่ระหว่างการปรับปรุง Server (Return Error 503 Service Unavailable เนื่องจากไม่สามารถส่งพารามิเตอร์ให้ Client ผ่านทาง HTTP Redirect ได้)	503
interaction_required	Authorization Server ต้องการให้ผู้ใช้บริการทำการยืนยันตัวตนผ่านแบบฟอร์ม หรือ หน้าจอ ข้อมูล Error นี้อาจถูกส่งกลับในกรณีที่ Parameter Prompt ถูกกำหนดเป็น none การยืนยันตัวตนจึงไม่สามารถดำเนินการต่อได้	302
login_required	Authorization Server ต้องการให้ผู้ใช้บริการทำการยืนยันตัวตน ข้อมูล Error นี้อาจถูกส่งกลับในกรณีที่ Parameter Prompt ถูกกำหนดเป็น none การยืนยันตัวตนจึงไม่สามารถดำเนินการต่อได้	302
consent_required	Authorization Server ต้องการให้ผู้ใช้บริการทำการยินยอมเพื่อให้ข้อมูล Error นี้อาจถูกส่งกลับในกรณีที่ Parameter Prompt ถูกกำหนดเป็น none การให้ข้อมูลจึงไม่สามารถดำเนินการต่อได้	302
invalid_request_uri	ข้อมูล request_uri ไม่ถูกต้อง	400
invalid_request_object	ข้อมูล request_object ไม่ถูกต้อง	302

ตัวอย่าง HTTP Response Error

```
HTTP/1.1 302 Found
  Location: https://rp.example.org/callback?
    error=invalid_request
    &error_description=
      Unsupported%20response_type%20value
    &state=af0ifjsldkj
```

ในกระบวนการยืนยันตัวตนทางอิเล็กทรอนิกส์ด้วยโปรโตคอล OpenID กำหนดรายละเอียดในการแจ้งกลับข้อผิดพลาด (Error Response) ของ Token Request โดยมีต้องกำหนดพารามิเตอร์ดังต่อไปนี้

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 ไม่ได้รับอนุญาตให้ร้องขอด้วยวิธีการที่ระบุ	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://{Proxy_URL}/.well-known/openid-configuration) เพื่อให้ RP ใช้เป็นข้อมูลในการเชื่อมต่อระบบ โดยปัจจุบัน Discovery Endpoint สามารถดูได้ที่ URL

- https://openid1.digitalid.or.th/proxy/.well-known/openid-configuration
- https://openid2.digitalid.or.th/proxy/.well-known/openid-configuration