กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม

ETDA

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วย

ข้อมูลในใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ

(Subscriber Certificate Profile)

เลขที่ ขมธอ. 15-2566

เวอร์ชัน 2.0

การเปลี่ยนแปลงโครงสร้างของเอกสาร

ขมธอ. 15-2560 version 1.0 การกำหนดข้อมูลในใบรับรองและรายการเพิกถอนใบรับรอง **(ยกเลิก)**
ขมธอ. 15-2566 version 2.0 ข้อมูลในใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ **(ประกาศใช้งาน)**

ขมธอ. 15-2560 version 1.0	ขมธอ. 15-2566 version 2.0
นำออก 3. ข้อมูลในใบรับรองและรายการเพิกถอนใบรับรอง	3. ข้อมูลในใบรับรอง
4. การกำหนดข้อมูลในใบรับรอง	นำออก รายละเอียดของข้อมูลในใบรับรอง
4.1 โครงสร้างของใบรับรอง/4.2 ข้อมูลในใบรับรอง	4. ข้อมูลในใบรับรองของผู้ใช้บริการ
4.3 ข้อแนะนำในการกำหนดข้อมูลในใบรับรอง	แก้ 4.1 ใบรับรองประเภทบุคคลธรรมดา
นำออก 4.3.1/4.3.2 ใบรับรองของ sub-CA ชั้นที่ 1 และชั้นที่ 2	แก้ 4.2 ใบรับรองประเภทนิติบุคคล
4.3.3 ใบรับรองของผู้ใช้บริการ	เพิ่ม 4.3 ใบรับรองประเภทเจ้าหน้าที่นิติบุคคล
• ใบรับรองสำหรับบุคคลธรรมดา	เพิ่ม 4.4 หมายเลขโอไอดี (Object Identifier: OID) ของ Certificate Policy Identifier
• ใบรับรองสำหรับนิติบุคคล	เพิ่ม ภาคผนวก ก. ตัวย่อ หมายเลขโอไอดี (OID) และความจำเป็นของคุณลักษณะภายใต้ฟิลด์ subject
นำออก • ใบรับรองสำหรับลงลายมือชื่อดิจิทัลโดยระบบให้บริการ	ภาคผนวก ข.โครงสร้างความสัมพันธ์ของใบรับรองในประเทศไทย
นำออก • ใบรับรองสำหรับ SSL	
นำออก 5. การกำหนดข้อมูลในรายการเพิกถอนใบรับรอง	
ภาคผนวก ก. โครงสร้างความสัมพันธ์ของใบรับรองในประเทศไทย	

รายละเอียดที่เกี่ยวข้องสำหรับข้อมูลที่นำออก

ลำดับ	หัวข้อในขมธอ. 15-2560 version 1.0 ที่นำออก	รายละเอียดที่เกี่ยวข้อง
1.	**4. การกำหนดข้อมูลในใบรับรอง** • นำรายละเอียดข้อมูลในใบรับรองออก	รายละเอียดที่นำออกเป็นไปตาม RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
2.	**4.3.1 และ 4.3.2 ใบรับรองของ sub-CA ชั้นที่ 1 และชั้นที่ 2**	หัวข้อที่นำออกเป็นเนื้อหาสำหรับ NRCA ใช้ในการออกใบรับรองให้ sub-CA
3.	**4.3.3 ใบรับรองของผู้ใช้บริการ** • ใบรับรองสำหรับลงลายมือชื่อดิจิทัลโดยระบบให้บริการ	ขมธอ. 15-2566 version 2.0 จัดให้เป็นใบรับรองประเภทที่ CA ออกโดยมีวัตถุประสงค์เฉพาะเจาะจงต่อการใช้งาน CA ตามหัวข้อ 4.4 หมายเลขโอไอดี (OID) ของ Certificate Policy
4.	**4.3.3 ใบรับรองของผู้ใช้บริการ** • ใบรับรองสำหรับ SSL	หัวข้อที่นำออกเป็นไปตาม Baseline Requirement Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates ของ CA/Browser Forum
5.	**5. การกำหนดข้อมูลในรายการเพิกถอนใบรับรอง**	หัวข้อที่นำออกเป็นไปตาม RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

ข้อมูลในใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ

(Subscriber Certificate Profile)

ขอบข่าย

ข้อเสนอแนะมาตรฐานฉบับนี้กำหนดประเภทของใบรับรองและข้อมูลในใบรับรองของผู้ใช้บริการ

3 ประเภท ได้แก่

- **ใบรับรองประเภทบุคคลธรรมดา** (natural person certificate)
- **ใบรับรองประเภทนิติบุคคล** (juristic person certificate) และ
- **ใบรับรองประเภทเจ้าหน้าที่นิติบุคคล** (enterprise user certificate)

สำหรับให้ผู้ให้บริการออกใบรับรอง (certification authority: CA) มีแนวทางในการออกใบรับรองของผู้ใช้บริการที่เป็นมาตรฐานเดียวกันและเป็นไปตามมาตรฐานสากล

ทั้งนี้ **ข้อมูลในใบรับรองของผู้ใช้บริการอ้างอิงตาม RFC 5280 และเพิ่มข้อกำหนดของข้อมูลในใบรับรองให้เหมาะสมกับบริบทการใช้งานของประเทศไทย**

ข้อเสนอแนะมาตรฐานฉบับนี้จะ**ไม่ครอบคลุม**ถึง

- **ใบรับรองของผู้ให้บริการออกใบรับรอง** (CA certificate) ภายใต้ผู้ให้บริการออกใบรับรองลำดับชั้นบนสุด (Root CA)
- **ใบรับรองของผู้ใช้บริการประเภทอื่น ๆ** นอกเหนือจากใบรับรองประเภทบุคคลธรรมดา ใบรับรองประเภทนิติบุคคล และใบรับรองประเภทเจ้าหน้าที่นิติบุคคล โดยที่ **ใบรับรองประเภทโปรโตคอล SSL/TLS** ให้มีรายละเอียดของข้อมูลเป็นไปตาม Baseline Requirement Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates ของ CA/Browser Forum

แนวทางการใช้งาน

ใบรับรองของผู้ใช้บริการ (subscriber certificate) สามารถนำไปใช้งานสำหรับ

การยืนยันตัวตน (authentication)

การเข้ารหัสลับ (encryption)

การตรวจสอบลายมือชื่อดิจิทัล
(digital signature verification)

โดยการใช้ลายมือชื่อดิจิทัล มีรายละเอียดดังต่อไปนี้

ในกรณีของ**บุคคลธรรมดา**และ**เจ้าหน้าที่นิติบุคคล ลายมือชื่อดิจิทัล จะใช้เป็นลายมือชื่ออิเล็กทรอนิกส์ (e-signature) ของบุคคลธรรมดา** ซึ่งมีวัตถุประสงค์เพื่อระบุตัวบุคคลธรรมดาผู้เป็นเจ้าของลายมือชื่อ และแสดงเจตนาของบุคคลนั้นที่มีต่อข้อความ

บุคคลธรรมดา

เจ้าหน้าที่นิติบุคคล

ลายมือชื่ออิเล็กทรอนิกส์
(e-signature)

ในกรณีของ**นิติบุคคล ลายมือชื่อดิจิทัลจะใช้เป็นตราอิเล็กทรอนิกส์ (e-seal) ของนิติบุคคล** ซึ่งมีวัตถุประสงค์เพื่อยืนยันแหล่งที่มาของข้อความ ว่ามาจากนิติบุคคลนั้น

นิติบุคคล

ตราอิเล็กทรอนิกส์
(e-seal) ของนิติบุคคล

การเปรียบเทียบข้อมูลในใบรับรองแต่ละประเภท

ตัวย่อ (descriptor) และหมายเลขโอไอดี (OID) ของคุณลักษณะภายใต้ฟิลด์ subject ซึ่งอ้างอิงจาก RFC 4519 และ ITU-T X.520 รวมถึงการเปรียบเทียบความจำเป็น (mandatory) ของคุณลักษณะภายใต้ฟิลด์ subject ที่กำหนดในใบรับรองแต่ละประเภท แสดงดังตาราง

ชื่อฟิลด์	ตัวย่อ (descriptor)	หมายเลขโอไอดี (OID)	ใบรับรองประเภทบุคคลธรรมดา	ใบรับรองประเภทเจ้าหน้าที่นิติบุคคล	ใบรับรองประเภทนิติบุคคล
subject			M	M	M
commonName	cn	2.5.4.3	M	M	M
givenName	-	2.5.4.42	M	M	NU
surname	sn	2.5.4.4	M	M	NU
serialNumber	-	2.5.4.5	O	O	NU
title	-	2.5.4.12	NU	O	NU
organizationalUnitName	ou	2.5.4.11	NU	O	O
organizationName	o	2.5.4.10	NU	M	M
organizationIdentifier	-	2.5.4.97	NU	M	M
localityName	l	2.5.4.7	NU	O	O
stateOrProvinceName	st	2.5.4.8	NU	O	O
countryName	c	2.5.4.6	M	M	M

M = Mandatory

O = Optional

NU = Not Used

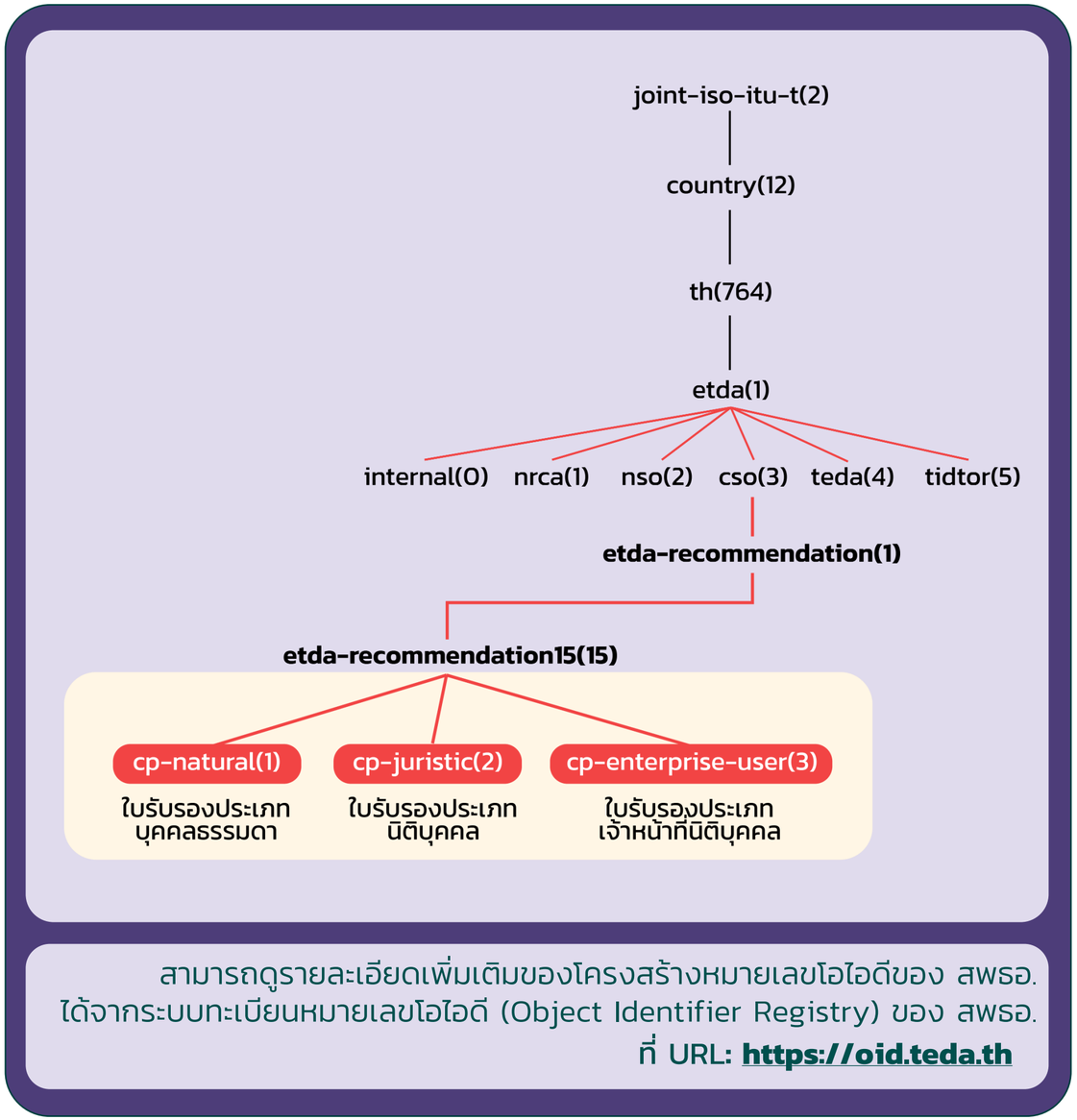
OID Structure ของ Certificate Policy Identifier สำหรับใบรับรองแต่ละประเภท

กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม ETDA

certificate policy identifier สำหรับใบรับรองประเภทบุคคลธรรมดา	
ASN.1 notation:	{join-iso-itu-t(2) country(16) th(764) etda(1) cso(3) etda-recommendation(1) etda-recommendation15(15) cp-natural(1)}
Dot notation:	2.16.764.1.3.1.15.1
OID-IRI notation:	/Joint-ISO-ITU-T/Country/764/ETDA/Community-Standard-Objects/ETDA-Recommendation/ETDA-Recommendation15/CP-Natural
Description:	Certificate policy identifier for certificates issued to natural persons

certificate policy identifier สำหรับใบรับรองประเภทนิติบุคคล	
ASN.1 notation:	{join-iso-itu-t(2) country(16) th(764) etda(1) cso(3) etda-recommendation(1) etda-recommendation15(15) cp-juristic(2)}
Dot notation:	2.16.764.1.3.1.15.2
OID-IRI notation:	/Joint-ISO-ITU-T/Country/764/ETDA/Community-Standard-Objects/ETDA-Recommendation/ETDA-Recommendation15/CP-Juristic
Description:	Certificate policy identifier for certificates issued to juristic persons

certificate policy identifier สำหรับใบรับรองประเภทเจ้าหน้าที่นิติบุคคล	
ASN.1 notation:	{join-iso-itu-t(2) country(16) th(764) etda(1) cso(3) etda-recommendation(1) etda-recommendation15(15) cp-enterprise-user(3)}
Dot notation:	2.16.764.1.3.1.15.3
OID-IRI notation:	/Joint-ISO-ITU-T/Country/764/ETDA/Community-Standard-Objects/ETDA-Recommendation/ETDA-Recommendation15/CP-Enterprise-User
Description:	Certificate policy identifier for certificates issued to enterprise users



สามารถดูรายละเอียดเพิ่มเติมของโครงสร้างหมายเลขโอไอดีของ สพธอ. ได้จากระบบทะเบียนหมายเลขโอไอดี (Object Identifier Registry) ของ สพธอ. ที่ URL: **https://oid.teda.th**