ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ETDA Recommendation on ICT Standard

for Electronic Transactions

ขมธอ. 15-256x

ว่าด้วยข้อมูลในใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ

SUBSCRIBER CERTIFICATE PROFILE

เวอร์ชัน 0.2

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ICS 35.030

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยข้อมูลในใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ

ขมธอ. 15-256x

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 20-22
เลขที่ 33/4 ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
หมายเลขโทรศัพท์: 0 2123 1234 หมายเลขโทรสาร: 0 2123 1200

ประกาศโดย
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

วันที่ กรุณาเลือกวันที่ประกาศ

คณะทำงานจัดทำร่างข้อเสนอแนะมาตรฐานเกี่ยวกับธุรกิจบริการ
ด้านการทำธุรกรรมทางอิเล็กทรอนิกส์

ที่ปรึกษาคณะทำงาน

นายชัยชนะ มิตรพันธ์	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ประธานคณะทำงาน

นายศุภโชค จันทรประทิน	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ผู้ทำงาน

นางสาวสำรวย นุ่มศรี	กรมศุลกากร
นายกำชัย จัตตานนท์	
นางจันทร์เจริญ เทพสุธา	กรมสรรพากร
นายยุทธพล จินะสี	
นายคงฤทธิ์ จันทริก	สภาผู้ส่งสินค้าทางเรือแห่งประเทศไทย
นายภาวุธ พงษ์วิทยภานุ	สมาคมผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์ไทย
นายธานินทร์ ตันกิติบุตร	สมาคมผู้ให้บริการอินเทอร์เน็ตและคลาวด์ไทย
นายวรพจน์ ธาราศิริสกุล	สมาคมฟินเทคประเทศไทย
นายปกรณ์ ลี้สกุล	สมาคมอุตสาหกรรมซอฟต์แวร์ไทย
นายสันติ สิทธิเลิศพิศาล	สำนักมาตรฐานผลิตภัณฑ์อุตสาหกรรม
นางสาวธิดารัธ ธนภรรคภวิน	สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย
นายอิศร์ เตาลานนท์	
นางสาวขนิษฐ์ ผาทอง	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายพงษ์พันธ์ ศรีปาน	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ผู้ทำงานและเลขานุการ

นายณัฐฑพัฒน์ โรจนศุภมิตร	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ผู้ช่วยเลขานุการ

นายวีรศักดิ์ ดีอ่ำ	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยข้อมูลในใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการฉบับนี้ จัดทำขึ้นเพื่อกำหนดประเภทของใบรับรองและข้อมูลในใบรับรองของผู้ใช้บริการ (subscriber) สำหรับให้ผู้ให้บริการออกใบรับรอง (certification authority: CA) มีแนวทางในการออกใบรับรองของผู้ใช้บริการที่เป็นมาตรฐานเดียวกันและเป็นไปตามมาตรฐานสากล

โดยมีการนำเสนอและรับฟังความคิดเห็นเป็นการทั่วไป ตลอดจนพิจารณาข้อมูล ข้อสังเกต ข้อคิดเห็นจากผู้ทรงคุณวุฒิและจากหน่วยงานที่เกี่ยวข้อง เพื่อปรับปรุงให้ข้อเสนอแนะมาตรฐานฉบับนี้มีความสมบูรณ์ครบถ้วนยิ่งขึ้น รวมทั้งให้สามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพ

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยข้อมูลในใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการฉบับนี้ จัดทำขึ้นโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 20-22 เลขที่ 33/4 ถนนพระราม 9
แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
โทรศัพท์: 0 2123 1234 โทรสาร: 0 2123 1200
อีเมล: estandard.center@etda.or.th
เว็บไซต์: www.etda.or.th

คำนำ

ใบรับรอง (certificate) เป็นส่วนประกอบสำคัญสำหรับการตรวจสอบลายมือชื่อดิจิทัล โดยใบรับรองจะบันทึกข้อมูลอิเล็กทรอนิกส์ซึ่งยืนยันความเชื่อมโยงระหว่างเจ้าของลายมือชื่อกับข้อมูลสำหรับใช้สร้างลายมือชื่อดิจิทัลไว้ การกำหนดข้อมูลในใบรับรองให้สอดคล้องตามประเภทการใช้งานจะทำให้การตรวจสอบลายมือชื่อดิจิทัลมีความสะดวกต่อการใช้งานและเป็นมาตรฐานเดียวกัน

ในการนี้ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ได้จัดทำข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยข้อมูลในใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ (Subscriber Certificate Profile) เวอร์ชัน 2.0 (เลขที่ ขมธอ. 15-2566) ขึ้น เพื่อกำหนดประเภทของใบรับรองและข้อมูลในใบรับรองของผู้ใช้บริการ (subscriber) สำหรับให้ผู้ให้บริการออกใบรับรอง (certification authority: CA) มีแนวทางในการออกใบรับรองของผู้ใช้บริการที่เป็นมาตรฐานเดียวกันและเป็นไปตามมาตรฐานสากล

สารบัญ

สารบัญรูป

สารบัญตาราง

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ว่าด้วยข้อมูลในใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ

1. ขอบข่าย

ข้อเสนอแนะมาตรฐานฉบับนี้กำหนดประเภทของใบรับรองและข้อมูลในใบรับรองของผู้ใช้บริการ โดยข้อเสนอแนะมาตรฐานฉบับนี้กำหนดข้อมูลใบรับรองของผู้ใช้บริการ 3 ประเภท ได้แก่ ใบรับรองประเภทบุคคลธรรมดา (natural person certificate) ใบรับรองประเภทนิติบุคคล (juristic person certificate) และใบรับรองประเภทเจ้าหน้าที่นิติบุคคล (enterprise user certificate) สำหรับให้ผู้ให้บริการออกใบรับรอง (certification authority: CA) มีแนวทางในการออกใบรับรองของผู้ใช้บริการที่เป็นมาตรฐานเดียวกันและเป็นไปตามมาตรฐานสากล ทั้งนี้ ข้อมูลในใบรับรองของผู้ใช้บริการอ้างอิงตาม RFC 5280 และเพิ่มข้อกำหนดของข้อมูลในใบรับรองให้เหมาะสมกับประเทศไทย

ข้อเสนอแนะมาตรฐานฉบับนี้จะไม่ครอบคลุมถึง

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

2. บทนิยาม

ความหมายของคำที่ใช้ในข้อเสนอแนะมาตรฐานฉบับนี้ มีดังต่อไปนี้

2.1 บุคคล หมายถึง บุคคลธรรมดา หรือนิติบุคคล [1]

2.2 เอนทิตี (entity) หมายถึง บุคคลและรวมถึงเครื่องให้บริการ (server) หรือเว็บไซต์ หรือหน่วยปฏิบัติงาน (operation unit/site) หรือเครื่องมืออื่นใด (device) ที่อยู่ภายใต้ความควบคุมของบุคคล [1]

2.3 ลายมือชื่ออิเล็กทรอนิกส์ หมายถึง อักษร อักขระ ตัวเลข เสียงหรือสัญลักษณ์อื่นใดที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์ซึ่งนำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้น และเพื่อแสดงว่าบุคคลดังกล่าวยอมรับข้อความในข้อมูลอิเล็กทรอนิกส์นั้น [2]

2.4 ลายมือชื่อดิจิทัล (digital signature) หมายถึง ลายมือชื่ออิเล็กทรอนิกส์ที่ได้จากกระบวนการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ ซึ่งช่วยให้สามารถยืนยันตัวเจ้าของลายมือชื่อและตรวจพบการเปลี่ยนแปลงของข้อความ

และลายมือชื่ออิเล็กทรอนิกส์ได้รวมถึงการทำให้เจ้าของลายมือชื่อไม่สามารถปฏิเสธความรับผิดจากข้อความที่ตนเองลงลายมือชื่อได้ [3]

2.5 ใบรับรองอิเล็กทรอนิกส์ หรือใบรับรอง (certificate) หมายถึง ข้อมูลอิเล็กทรอนิกส์หรือการบันทึกอื่นใดซึ่งยืนยันความเชื่อมโยงระหว่างเจ้าของลายมือชื่อกับข้อมูลสำหรับใช้สร้างลายมือชื่อดิจิทัล

2.6 ผู้ให้บริการออกใบรับรอง (certification authority: CA) หมายถึง เอนทิตีที่รับรองกุญแจสาธารณะให้กับผู้ใช้บริการโดยการออกใบรับรองให้กับผู้ใช้บริการ และยังมีหน้าที่บริหารจัดการใบรับรองของผู้ใช้บริการ เช่น เผยแพร่ใบรับรอง เพิกถอนใบรับรอง และเผยแพร่ข้อมูลสำหรับตรวจสอบสถานะใบรับรอง

2.7 ผู้ใช้บริการ (subscriber) หมายถึง บุคคล หรือเอนทิตีใด ๆ ที่ได้รับใบรับรองจากผู้ให้บริการออกใบรับรอง [1]

2.8 หมายเลขโอไอดี (object identifier: OID) หมายถึง ค่าสัมพันธ์ซึ่งบ่งบอกถึงข้อมูลสารสนเทศของวัตถุ (information object) ใด ๆ โดยเป็นค่าที่สามารถบ่งชี้ได้ถึงความเป็นหนึ่งเดียวของ object นั้น ๆ [1]

2.9 กุญแจสาธารณะ (public key) หมายถึง กุญแจที่ใช้ตรวจสอบลายมือชื่อดิจิทัล และสามารถนำไปใช้เข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ เพื่อมิให้สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ที่มีการเข้ารหัสลับนั้นได้ เพื่อประโยชน์ในการรักษาความลับของข้อมูลอิเล็กทรอนิกส์นั้น [1]

2.10 กุญแจส่วนตัว (private key) หมายถึง กุญแจที่ใช้สร้างลายมือชื่อดิจิทัล และสามารถนำไปใช้ในการถอดรหัสลับเมื่อมีการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ เพื่อให้สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ที่มีการเข้ารหัสลับนั้นได้ [1]

2.11 คู่กุญแจ (key pair) หมายถึง กุญแจส่วนตัวและกุญแจสาธารณะในระบบการเข้ารหัสลับแบบอสมมาตรที่สร้างขึ้นโดยวิธีการที่ทำให้กุญแจส่วนตัวมีความสัมพันธ์ในทางคณิตศาสตร์กับกุญแจสาธารณะในลักษณะที่สามารถใช้กุญแจสาธารณะตรวจสอบได้ว่าลายมือชื่อดิจิทัลได้สร้างขึ้นโดยใช้กุญแจส่วนตัวนั้นหรือไม่ และสามารถนำกุญแจสาธารณะไปใช้ในการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ ทำให้ไม่สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ได้เพื่อประโยชน์ในการรักษาความลับของข้อมูลอิเล็กทรอนิกส์ เว้นแต่บุคคลที่ถือกุญแจส่วนตัวซึ่งสามารถนำกุญแจส่วนตัวของตนใช้ในการถอดรหัสลับของข้อมูลอิเล็กทรอนิกส์ เพื่อให้เจ้าของกุญแจส่วนตัวสามารถอ่านหรือเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์นั้นได้ [1]

2.12 แนวนโยบายของผู้ให้บริการออกใบรับรอง (certificate policy: CP) หมายถึง นโยบายที่ระบุแนวทางการใช้งานใบรับรองสำหรับกลุ่มการใช้งานที่เฉพาะหรือตามแต่ละประเภทของแอปพลิเคชัน ซึ่งรวมถึงข้อกำหนดด้านความมั่นคงปลอดภัยทั่วไป ตัวอย่างเช่น CP ที่ระบุแนวทางการใช้งานใบรับรองสำหรับยืนยันตัวตนผู้ที่เกี่ยวข้องกับธุรกรรมระหว่างธุรกิจกับธุรกิจในการการซื้อขายสินค้าหรือบริการภายในช่วงราคาที่กำหนด

2.13 แนวปฏิบัติของผู้ให้บริการออกใบรับรอง (certification practice statement: CPS) หมายถึง แนวปฏิบัติที่ผู้ให้บริการออกใบรับรองใช้ในการออก จัดการ เพิกถอน และต่ออายุหรือเปลี่ยนกุญแจใหม่สำหรับใบรับรอง

2.14 รายการเพิกถอนใบรับรอง (certificate revocation list: CRL) หมายถึง รายการใบรับรองที่ถูกเพิกถอนการใช้งาน [1]

2.15 เกณฑ์วิธีการตรวจสอบสถานะของใบรับรอง (online certificate status protocol: OCSP) หมายถึง เกณฑ์วิธี (protocol) สำหรับตรวจสอบสถานะของการเพิกถอนใบรับรอง หรือวันเวลาที่เริ่มต้นและสิ้นสุดการใช้ใบรับรอง [1]

3. ข้อมูลในใบรับรอง

มาตรฐาน RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile อธิบายข้อมูลในใบรับรอง X.509 เวอร์ชัน 3 โดยใบรับรองจะประกอบด้วยฟิลด์ข้อมูล 3 ฟิลด์ ดังนี้

(1) ฟิลด์ tbsCertificate: แสดงข้อมูลในใบรับรอง ซึ่งแบ่งเป็น 2 ส่วน

- ฟิลด์พื้นฐาน (basic fields) เช่น ชื่อของเจ้าของใบรับรองและผู้ออกใบรับรอง กุญแจสาธารณะของผู้เป็นเจ้าของใบรับรอง ช่วงเวลาที่ใบรับรองสามารถใช้งานได้ รายละเอียดตามหัวข้อ 3.1
- ฟิลด์เพิ่มเติม (extension fields) สำหรับบรรจุข้อมูลอื่น ๆ ที่อยู่นอกเหนือจากฟิลด์พื้นฐาน รายละเอียดตาม 3.2 โดย RFC 5280 ได้กำหนดฟิลด์เพิ่มเติมหลายชนิดให้เลือกใช้งาน ทั้งฟิลด์เพิ่มเติมแบบมาตรฐาน (standard extensions) และฟิลด์เพิ่มเติมที่กำหนดขึ้นเพื่อใช้งานตามวัตถุประสงค์เฉพาะ (private internet extensions) ทั้งนี้ หากมีความจำเป็นต้องใช้ฟิลด์เพิ่มเติมที่นอกเหนือจากรายการตามตารางที่ 1 ในหัวข้อ 3.2 CA สามารถกำหนดฟิลด์เพิ่มเติมได้โดยวิธีการกำหนดข้อมูลให้อ้างอิงตาม ISO/IEC 9594-8 : 2020 หรือ RFC 5280

(2) ฟิลด์ signatureAlgorithm: แสดงข้อมูลอัลกอริทึมที่ผู้ให้บริการออกใบรับรองใช้ลงลายมือชื่อดิจิทัลเพื่อรับรองข้อมูลในใบรับรอง โดยอัลกอริทึมที่ใช้ต้องเป็นชนิดเดียวกับอัลกอริทึมที่ระบุในฟิลด์ signature ของ tbsCertificate (ข้อ 3.1 ข้อ (3))

(3) ฟิลด์ signatureValue: แสดงลายมือชื่อดิจิทัลที่สร้างขึ้นโดยผู้ให้บริการออกใบรับรองเพื่อรับรองความถูกต้องของข้อมูลในฟิลด์ tbsCertificate ซึ่งหมายความว่า ผู้ให้บริการออกใบรับรองได้รับรองข้อมูลของเจ้าของใบรับรอง และความเชื่อมโยงระหว่างข้อมูลดังกล่าวกับกุญแจสาธารณะ ที่ระบุในใบรับรอง

3.1 ฟิลด์พื้นฐาน (basic fields) ของ tbsCertificate

(1) version: แสดงข้อมูลเวอร์ชันของใบรับรอง โดยกำหนดให้ใช้เฉพาะใบรับรองเวอร์ชัน 3 (ระบุค่าเป็น 2) เพื่อให้ใบรับรองรองรับการใช้งานฟิลด์เพิ่มเติมได้

(2) serialNumber: แสดงข้อมูลหมายเลขใบรับรอง (certificate serial number) ซึ่งมีค่าเป็นจำนวนเต็มบวก ขนาดไม่เกิน 20 octets (160 บิต) และไม่ซ้ำกับหมายเลขใบรับรองอื่นที่ออกโดยผู้ให้บริการออกใบรับรองรายเดียวกัน

(3) signature: แสดง algorithm identifier ซึ่งประกอบด้วยหมายเลขโอไอดี (OID) ของอัลกอลิทึมและค่าพารามิเตอร์ (ถ้ามี) ที่ผู้ให้บริการออกใบรับรองใช้ลงลายมือชื่อดิจิทัลเพื่อรับรองข้อมูลในใบรับรอง

(4) issuer: แสดงข้อมูลระบุผู้ให้บริการออกใบรับรองที่ออกใบรับรองนี้

(5) validity: แสดงช่วงเวลาที่สามารถใช้ใบรับรองได้ โดยประกอบด้วยข้อมูลวันและเวลาที่ใบรับรองเริ่มต้นใช้งานได้ (not before) และวันและเวลาที่ใบรับรองหมดอายุ (not after)

(6) subject: แสดงข้อมูลระบุเอนทิตีที่ผู้ให้บริการออกใบรับรองได้รับรองว่าเป็นเจ้าของกุญแจส่วนตัวซึ่งเป็นคู่กับกุญแจสาธารณะที่อยู่ในใบรับรอง

(7) subjectPublicKeyInfo: แสดงข้อมูลกุญแจสาธารณะและอัลกอริทึมของกุญแจสาธารณะ

รายละเอียดฟิลด์พื้นฐานเป็นไปตาม RFC 5280 ข้อ 4.1 Basic Certificate Fields

3.2 ฟิลด์เพิ่มเติม (extensions fields) ของ tbsCertificate

ใบรับรอง X.509 เวอร์ชัน 3 รองรับการใช้งานฟิลด์เพิ่มเติม ซึ่งแสดงข้อมูลเพิ่มเติมเกี่ยวกับเจ้าของใบรับรอง กุญแจสาธารณะ โดยฟิลด์เพิ่มเติมที่สำคัญสำหรับการใช้งานร่วมกันของซอฟต์แวร์ในประเทศไทยมีดังนี้

(1) authority key identifier: เป็นฟิลด์เพิ่มเติมที่ระบุค่าอ้างอิงถึงกุญแจสาธารณะที่เป็นคู่กับกุญแจส่วนตัวซึ่งผู้ให้บริการออกใบรับรองใช้ลงลายมือชื่อดิจิทัลเพื่อรับรองใบรับรองนี้

(2) subject key identifier: เป็นฟิลด์เพิ่มเติมที่ระบุค่าอ้างอิงถึงกุญแจสาธารณะของเจ้าของใบรับรอง

(3) key usage: เป็นฟิลด์เพิ่มเติมที่ใช้ระบุถึงวัตถุประสงค์ของการใช้กุญแจสาธารณะซึ่งอยู่ในใบรับรอง อาทิ การเข้ารหัสลับข้อมูล และการตรวจสอบลายมือชื่อดิจิทัล โดยการกำหนดวัตถุประสงค์ของการใช้กุญแจสาธารณะสามารถกำหนดวัตถุประสงค์ได้มากกว่า 1 วัตถุประสงค์ตามความเหมาะสมของการใช้งานและความปลอดภัยในการดูแลรักษากุญแจส่วนตัว

(4) certificate policies: เป็นฟิลด์เพิ่มเติมที่แสดงข้อมูลนโยบาย (policy information) ที่เกี่ยวข้องกับการออกใบรับรองและวัตถุประสงค์ของการใช้ใบรับรองที่กำหนดโดยผู้ให้บริการออกใบรับรอง ซึ่งแต่ละนโยบายประกอบด้วยหมายเลขโอไอดี (OID) ของนโยบายและอาจมีข้อมูลเพิ่มเติม (qualifier)

(5) subject alternative name: เป็นฟิลด์เพิ่มเติมที่ใช้ระบุข้อมูลเกี่ยวกับเอนทิตีที่เป็นเจ้าของใบรับรองเพิ่มเติมจากฟิลด์ subject โดยสามารถกำหนดได้หลายรูปแบบ เช่น e-mail address, Domain Name, IP Address และ URI

(6) basic constraints: เป็นฟิลด์เพิ่มเติมที่ใช้ระบุว่าใบรับรองนี้เป็นใบรับรองของผู้ให้บริการออกใบรับรองหรือไม่ พร้อมทั้งระบุจำนวนชั้นของใบรับรองของ CA ที่มากที่สุดที่อนุญาตให้อยู่ในชั้นถัดลงมาจากใบรับรองใบนี้ใน certification path

(7) extended key usage: เป็นฟิลด์เพิ่มเติมที่ใช้ระบุถึงวัตถุประสงค์ของการใช้กุญแจสาธารณะในใบรับรองที่เพิ่มเติมจากฟิลด์ keyUsage

(8) CRL distribution points: เป็นฟิลด์เพิ่มเติมที่ใช้ระบุวิธีการเข้าถึงรายการเพิกถอนใบรับรอง โดยแสดงเป็นลำดับของแหล่งเผยแพร่รายการเพิกถอนใบรับรอง

(9) authority information access: เป็นฟิลด์เพิ่มเติมที่ระบุวิธีการเข้าถึงข้อมูล และบริการต่าง ๆ ของผู้ให้บริการออกใบรับรองที่ออกใบรับรองนี้

ทั้งนี้ ฟิลด์เพิ่มเติมจะมีการกำหนดค่า critical ซึ่งใช้แสดงค่าความสำคัญของข้อมูลในฟิลด์เพิ่มเติมในรูปแบบ Boolean โดยมีรายละเอียดดังนี้

- ค่า critical เป็น True (T) หมายถึง ซอฟต์แวร์จะต้องปฏิเสธการใช้งานใบรับรองหากไม่สามารถเข้าใจความหมายหรือไม่สามารถประมวลผลข้อมูลในฟิลด์เพิ่มเติมได้
- ค่า critical เป็น False (F) หมายถึง ซอฟต์แวร์สามารถใช้งานใบรับรองได้ แม้ไม่เข้าใจความหมายของฟิลด์เพิ่มเติม ทั้งนี้ หากซอฟต์แวร์เข้าใจความหมายของฟิลด์เพิ่มเติม ซอฟต์แวร์ต้องประมวลผลข้อมูลในฟิลด์เพิ่มเติมด้วย

ทั้งนี้ ชื่อฟิลด์เพิ่มเติม ชื่อฟิลด์เพิ่มเติมในใบรับรอง หมายเลขโอไอดี (OID) และ ค่า critical เป็นไปตามตารางที่ 1 โดยรายละเอียดอื่น ๆ ของฟิลด์เพิ่มเติมเป็นไปตาม RFC 5280 ข้อ 4.2 Certificate Extensions

ตารางที่ 1 รายการฟิลด์เพิ่มเติมในใบรับรอง

Index	ชื่อฟิลด์เพิ่มเติม	ชื่อฟิลด์เพิ่มเติมในใบรับรอง	หมายเลขโอไอดี (OID)	ค่า critical
	ฟิลด์เพิ่มเติมแบบมาตรฐาน (standard extensions) ที่เป็นไปตาม ITU-T X. 509			
(1)	authority key identifier	authorityKeyIdentifier	2.5.29.35	F
(2)	subject key identifier	subjectKeyIdentifier	2.5.29.14	F
(3)	key usage	keyUsage	2.5.29.15	T
(4)	certificate policies	certificatePolicies	2.5.29.32	F
(5)	subject alternative name	subjectAltName	2.5.29.17	F
(6)	basic constraints	basicConstraints	2.5.29.19	T
(7)	extended key usage	extKeyUsage	2.5.29.37	F
(8)	CRL distribution points	cRLDistributionPoints	2.5.29.31	F
	ฟิลด์เพิ่มเติมที่กำหนดขึ้นเพื่อใช้งานตามวัตถุประสงค์เฉพาะ (private internet extensions)			
(9)	authority information access	authorityInfoAccess	1.3.6.1.5.5.7.1.1	F

4. การกำหนดข้อมูลในใบรับรองของผู้ใช้บริการ

ข้อมูลในใบรับรองของผู้ใช้บริการมีรายละเอียดสอดคล้องตาม RFC 5280 [4] และเพิ่มข้อกำหนดของข้อมูลในใบรับรองให้เหมาะสมกับประเทศไทย โดยข้อมูลในใบรับรองจะแสดงเป็นตารางรายการข้อมูล ซึ่งประกอบด้วยสดมภ์ต่าง ๆ ดังต่อไปนี้

(1) สดมภ์ Index แสดงดัชนีของฟิลด์พื้นฐาน ฟิลด์เพิ่มเติม หรือคุณลักษณะ (attribute)

(2) สดมภ์ Item แสดงชื่อฟิลด์พื้นฐาน ฟิลด์เพิ่มเติม หรือคุณลักษณะ

(3) สดมภ์ mandatory แสดงความจำเป็นของข้อมูลในฟิลด์พื้นฐาน ฟิลด์เพิ่มเติม หรือคุณลักษณะ

- m (mandatory): ฟิลด์พื้นฐาน ฟิลด์เพิ่มเติม หรือคุณลักษณะ ที่ต้องระบุข้อมูล
- o (optional): ฟิลด์พื้นฐาน ฟิลด์เพิ่มเติม หรือคุณลักษณะ ที่สามารถเลือกระบุหรือไม่ระบุก็ได้ ขึ้นอยู่กับความต้องการใช้งาน
- nu (not used): ห้ามมีฟิลด์พื้นฐาน ฟิลด์เพิ่มเติม หรือคุณลักษณะนี้

การกำหนดค่าความจำเป็นของข้อมูลในเพิ่มเติมเป็นไปตามการใช้งานร่วมกันของซอฟต์แวร์ในประเทศไทย

(4) สดมภ์ Value แสดงข้อมูลหรือวิธีการกำหนดข้อมูลในฟิลด์พื้นฐาน ฟิลด์เพิ่มเติม หรือคุณลักษณะ

ทั้งนี้ รายละเอียดของข้อมูลในใบรับรองของผู้ใช้บริการซึ่งแบ่งออกเป็น 3 ประเภท ได้แก่

(1) ใบรับรองประเภทบุคคลธรรมดา (natural person certificate) รายละเอียดตามหัวข้อ 4.1

(2) ใบรับรองประเภทเจ้าหน้าที่นิติบุคคล (enterprise user certificate) รายละเอียดตามหัวข้อ 4.2

(3) ใบรับรองประเภทนิติบุคคล (juristic person certificate) รายละเอียดตามหัวข้อ 4.3

4.1 ใบรับรองประเภทบุคคลธรรมดา

ใบรับรองประเภทบุคคลธรรมดา คือ ใบรับรองที่ใช้สำหรับสนับสนุนลายมือชื่ออิเล็กทรอนิกส์ (e-signature) เพื่อระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่อและแสดงเจตนาของบุคคลดังกล่าวเกี่ยวกับข้อความ โดยมีรายละเอียดข้อมูลในฟิลด์ต่าง ๆ เป็นไปตามตารางที่ 2

ตารางที่ 2 ข้อมูลในใบรับรองประเภทบุคคลธรรมดา

Index	Item	mandatory	Value
1.	version	m	2 (Version 3)
2.	serialNumber	m	ตัวเลขที่ไม่ซ้ำกันระหว่างใบรับรองภายใต้ผู้ให้บริการออกใบรับรองรายเดียวกัน โดยเป็นตัวเลขแบบสุ่มและไม่เรียงกันเมื่อเทียบกับใบรับรองที่ออกก่อนหน้าและต่อจากใบนี้ (randomized and non-sequential) ทั้งนี้ จะต้องมีค่ามากกว่า 0 และขนาดไม่น้อยกว่า 64 บิต [5]
3.	signature	m	หมายเลขโอไอดี (OID) ของอัลกอริทึมจากตัวเลือกดังนี้ — {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)} — {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha384WithRSAEncryption(12)} — {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512WithRSAEncryption(13)} — iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)} — {iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)} — {iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA512(4)} ทั้งนี้ ผู้ให้บริการออกใบรับรองควรติดตามการอัปเดตอัลกอริทึมของ signature จากมาตรฐานที่เกี่ยวข้อง เช่น RFC 3279 และมาตรฐานเวอร์ชันที่อัปเดต
4.	issuer	m	
4.1	commonName (cn)	m	ชื่อผู้ให้บริการออกใบรับรองและข้อมูลบ่งบอกถึงระบบบริการ เป็นภาษาอังกฤษ เช่น “XYZ Certification Authority - G1”
4.2	organizationalUnitName (ou)	o	ชื่อหน่วยงานย่อยในองค์กรของผู้ให้บริการออกใบรับรอง เป็นภาษาอังกฤษ เช่น “XYZ Certification Authority”

Index	Item	mandatory	Value
4.3	organizationName (o)	m	ชื่อองค์กรของผู้ให้บริการออกใบรับรองที่ใช้จดทะเบียนกับหน่วยงานที่เป็นนายทะเบียน เป็นภาษาอังกฤษ เช่น “XYZ Company Limited”
4.4	countryName (c)	m	ระบุรหัสประเทศที่ตั้งของนิติบุคคลให้เป็นไปตาม ISO 3166-1 alpha-2 code เช่น “ประเทศไทย” ให้ใช้รหัส “TH”
4.5	organizationIdentifier	o	เลขประจำตัวผู้เสียภาษีอากรของผู้ให้บริการออกใบรับรองที่ออกใบรับรองนี้ เช่น “1234567890123”
5.	validity	m	
5.1	notBefore	m	วันและเวลาที่ใบรับรองเริ่มใช้งานได้
5.2	notAfter	m	วันและเวลาที่ใบรับรองสิ้นสุดการใช้งาน
6.	subject	m	
6.1	commonName (cn)	m	— ระบุชื่อตัว-ชื่อสกุลของเจ้าของใบรับรองในรูปแบบ “ชื่อตัว ชื่อสกุล” โดยเป็นภาษาไทยหรือภาษาอังกฤษก็ได้ เช่น “สมชาย รักดี” หรือ “Somchai Rakdee” — ในกรณีบุคคลที่มีชื่อรอง ให้ระบุชื่อตัว-ชื่อรอง-ชื่อสกุลของเจ้าของใบรับรองในรูปแบบ “ชื่อตัว ชื่อรอง ชื่อสกุล” โดยเป็นภาษาไทยหรือภาษาอังกฤษก็ได้ ทั้งนี้ CA สามารถพิจารณาใส่คำนำหน้าชื่อด้วยก็ได้ตามความเหมาะสม
6.2	givenName	m	— ระบุชื่อตัวของเจ้าของใบรับรองตามเอกสารที่ออกโดยหน่วยงานที่เป็นนายทะเบียนในรูปแบบ “ชื่อตัว” โดยเป็นภาษาไทยหรือภาษาอังกฤษก็ได้ เช่น “สมชาย” หรือ “Somchai” — ในกรณีบุคคลที่มีชื่อรอง ให้ระบุชื่อตัว-ชื่อรองของเจ้าของใบรับรองตามเอกสารที่ออกโดยหน่วยงานที่เป็นนายทะเบียนในรูปแบบ “ชื่อตัว ชื่อรอง” โดยเป็นภาษาไทยหรือภาษาอังกฤษก็ได้ ทั้งนี้ ชื่อตัวและชื่อรองของบุคคลสัญชาติไทยควรใช้เป็นภาษาไทยตามบัตรประจำตัวประชาชน ส่วนชื่อตัวและชื่อรองของบุคคลต่างด้าวให้ใช้เป็นภาษาอังกฤษตามหนังสือเดินทางหรือเอกสารสำคัญประจำตัวอื่นที่หน่วยงานของรัฐเจ้าของสัญชาติออกให้
6.3	surname (sn)	m	ระบุชื่อสกุลของเจ้าของใบรับรองตามเอกสารที่ออกโดยหน่วยงานที่เป็นนายทะเบียน โดยเป็นภาษาไทยหรือภาษาอังกฤษก็ได้ ทั้งนี้ ชื่อสกุลของบุคคลสัญชาติไทยควรใช้เป็นภาษาไทยตามบัตรประจำตัวประชาชน ส่วนชื่อสกุลของบุคคลต่างด้าวให้ใช้เป็นภาษาอังกฤษตามหนังสือเดินทางหรือเอกสารสำคัญประจำตัวอื่นที่หน่วยงานของรัฐเจ้าของสัญชาติออกให้

Index	Item	mandatory	Value
6.4	serialNumber	o	ข้อมูลที่เชื่อมโยงไปยังเจ้าของใบรับรอง โดยไม่เชื่อมโยงไปยังบุคคลอื่น เช่น เลขประจำตัวประชาชน เลขที่หนังสือเดินทาง หรือตัวเลขที่สร้างด้วยวิธีการสุ่ม ทั้งนี้ อาจใช้ค่าแฮชของเลขประจำตัวประชาชนหรือเลขที่หนังสือเดินทางก็ได้
6.5	title	nu	-
6.6	organizationalUnitName (ou)	nu	-
6.7	organizationName (o)	nu	-
6.8	organizationIdentifier	nu	-
6.9	country (c)	m	ระบุรหัสประเทศที่ตั้งของนิติบุคคลให้เป็นไปตาม ISO 3166-1 alpha-2 code เช่น “ประเทศไทย” ให้ใช้รหัส “TH”
7.	subjectPublicKeyInfo	m	
7.1	algorithm	m	หมายเลขโอไอดี (OID) ของอัลกอริทึมของกุญแจสาธารณะ OID = {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}
7.2	subjectPublicKey	m	กุญแจสาธารณะชนิด RSA ความยาวอย่างน้อย 2048 บิต
8.	authorityKeyIdentifier	m	keyIdentifier บรรจุค่าของฟังก์ชัน SHA-1 Hash ของกุญแจสาธารณะที่เป็นคู่กับกุญแจส่วนตัวซึ่งผู้ออกใบรับรองนี้ใช้ลงลายมือชื่อดิจิทัลเพื่อรับรองใบรับรอง
9.	subjectKeyIdentifier	m	keyIdentifier บรรจุค่าของฟังก์ชัน SHA-1 Hash ของ subjectPublicKey ซึ่งอยู่ในฟิลด์ subjectPublicKeyInfo
10.	keyUsage	m	ตั้งค่าตามวัตถุประสงค์ของการใช้งาน ทั้งนี้ สำหรับการใช้งานทั่วไปแนะนำให้ตั้งค่า ดังนี้ (1) สำหรับการลงลายมือชื่อดิจิทัล ให้ตั้งค่าบิต digitalSignature = 1 และ contentCommitment = 1 (2) สำหรับการเข้ารหัสลับ ให้ตั้งค่าบิต keyEncipherment = 1 และ/หรือ dataEncipherment = 1
11.	certificatePolicies	m	
11.1	policyIdentifier	m	หมายเลขโอไอดี (OID) ของ certificate policy
11.2	policyQualifiers	m	ระบุอย่างน้อย 1 PolicyQualifierInfo
11.2.1	PolicyQualifierInfo [1]	m	
11.2.1.1	policyQualifierId	m	หมายเลขโอไอดี (OID) ของประเภท qualifier เป็น certification practice statement OID = {iso(1) org(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) qt(2) cps(1)}
11.2.1.2	qualifier	m	cPSuri = HTTP URL ของ certification practice statement
11.2.2	PolicyQualifierInfo [2]	o	

Index	Item	mandatory	Value
11.2.2.1	policyQualifierId	o	หมายเลขโอไอดี (OID) ของประเภท qualifier เป็น user notice OID = {iso(1) org(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) qt(2) unotice(2)}
11.2.2.2	qualifier	o	userNotice = ข้อความที่แสดง เมื่อใช้ใบรับรอง
12.	subjectAltName	o	
12.1	directoryName	o	ข้อมูลเกี่ยวกับเจ้าของใบรับรอง โดยใช้ชนิดข้อมูลตาม ITU-T X.501 “Name”
12.2	rfc822Name	o	อีเมลของเจ้าของใบรับรอง
13.	basicConstraints	m	
13.1	cA	m	False
13.2	pathLenConstraint	nu	-
14.	extKeyUsage	o	ใช้เมื่อซอฟต์แวร์ที่ใช้ใบรับรองต้องการใช้ค่าในฟิลด์นี้เท่านั้น
15.	cRLDistributionPoints	m	ระบุอย่างน้อย 1 DistributionPoint
15.1	DistributionPoint [1]	m	
15.1.1	distributionPoint	m	HTTP URL ที่สามารถเข้าถึงรายการเพิกถอนใบรับรอง
15.1.2	reason	nu	-
15.1.3	cRLIssuer	nu	-
16.	authorityInfoAccess	m	ระบุ 2 AccessDescription
16.1	AccessDescription [1]	m	
16.1.1	accessMethod	m	OID = {iso(1) org(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) ocsp(1)}
16.1.2	accessLocation	m	HTTP URL สำหรับเข้าถึงบริการ OCSP
16.2	AccessDescription [2]	m	
16.2.1	accessMethod	m	OID = {iso(1) org(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) calssuers(2)}
16.2.2	accessLocation	m	HTTP URL สำหรับเข้าถึงรายการใบรับรองของผู้ให้บริการออกใบรับรอง

4.2 ใบรับรองประเภทนิติบุคคล

ใบรับรองประเภทนิติบุคคล คือ ใบรับรองที่ใช้สำหรับสนับสนุนตราอิเล็กทรอนิกส์ (e-seal) เพื่อรับรองแหล่งที่มาของข้อมูลและความครบถ้วนของข้อความที่มาจากนิติบุคคล โดยมีรายละเอียดของข้อมูลในฟิลด์ต่าง ๆ เป็นไปตามตารางที่ 3

ตารางที่ 3 ข้อมูลในใบรับรองประเภทนิติบุคคล

Index	Item	mandatory	Value
1.	Version	m	2 (Version 3)
2.	serialNumber	m	ตัวเลขที่ไม่ซ้ำกันระหว่างใบรับรองภายใต้ผู้ให้บริการออกใบรับรองรายเดียวกัน โดยเป็นตัวเลขแบบสุ่มและไม่เรียงกันเมื่อเทียบกับ

Index	Item	mandatory	Value
			ใบรับรองที่ออกก่อนหน้าและต่อจากใบนี้ (randomized and non-sequential) ทั้งนี้ จะต้องมีค่ามากกว่า 0 และขนาดไม่น้อยกว่า 64 บิต [5]
3.	signature	m	หมายเลขโอไอดี (OID) ของอัลกอริทึมจากตัวเลือกดังนี้ – {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)} – {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha384WithRSAEncryption(12)} – {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512WithRSAEncryption(13)} – iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)} – {iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)} – {iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA512(4)} ทั้งนี้ ผู้ให้บริการออกใบรับรองควรติดตามการอัปเดตอัลกอริทึมของ signature จากมาตรฐานที่เกี่ยวข้อง เช่น RFC 3279 และมาตรฐานเวอร์ชันที่อัปเดต
4.	issuer	m	
4.1	commonName (cn)	m	ชื่อผู้ให้บริการออกใบรับรองและข้อมูลบ่งบอกถึงระบบบริการ เป็นภาษาอังกฤษ เช่น “XYZ Certification Authority - G1”
4.2	organizationalUnitName (ou)	o	ชื่อหน่วยงานย่อยในองค์กรของผู้ให้บริการออกใบรับรอง เป็นภาษาอังกฤษ เช่น “XYZ Certification Authority”
4.3	organizationName (o)	m	ชื่อองค์กรของผู้ให้บริการออกใบรับรองที่ใช้จดทะเบียนกับหน่วยงานที่เป็นนายทะเบียน เป็นภาษาอังกฤษ เช่น “XYZ Company Limited”
4.4	countryName (c)	m	ระบุรหัสประเทศที่ตั้งของนิติบุคคลให้เป็นไปตาม ISO 3166-1 alpha-2 code เช่น “ประเทศไทย” ให้ใช้รหัส “TH”
4.5	organizationIdentifier	o	เลขทะเบียนนิติบุคคล หรือ เลขประจำตัวผู้เสียภาษีอากรของนิติบุคคลของผู้ให้บริการออกใบรับรอง เช่น “1234567890123”
5.	validity	m	
5.1	notBefore	m	วันและเวลาที่ใบรับรองเริ่มใช้งานได้
5.2	notAfter	m	วันและเวลาที่ใบรับรองสิ้นสุดการใช้งาน
6.	subject	m	

Index	Item	mandatory	Value
6.1	commonName (cn)	m	ชื่อนิติบุคคลโดยทั่วไปของเจ้าของใบรับรอง ให้เป็นภาษาไทยหรือภาษาอังกฤษก็ได้ โดย CA ต้องไม่ระบุเพียงอักษรย่อของนิติบุคคลหรือชื่อส่วนงานย่อยหรือชื่อหน่วยงานย่อยในนิติบุคคลเพียงอย่างเดียว เนื่องจากอาจซ้ำหรือทำให้เข้าใจว่าเป็นนิติบุคคลอื่นได้ ทั้งนี้สามารถระบุ commonName (cn) ได้ในรูปแบบดังต่อไปนี้ — ระบุชื่อนิติบุคคลที่ใช้จดทะเบียนกับหน่วยงานที่เป็นนายทะเบียน เช่น “บริษัท ทดสอบเซอร์วิส จำกัด” หรือ “Todsob Service Company Limited” — ระบุชื่อนิติบุคคลพร้อมอักษรย่อ ในรูปแบบ “ชื่อนิติบุคคล (อักษรย่อ)” เช่น “บริษัท ทดสอบเซอร์วิส จำกัด (ท.ซ.)” หรือ“Todsob Service Company Limited (T.S.)” — ชื่อนิติบุคคลพร้อมระบุวัตถุประสงค์การใช้งาน ในรูปแบบ “ชื่อนิติบุคคล (วัตถุประสงค์การใช้งาน)” เช่น “บริษัท ทดสอบเซอร์วิส จำกัด (สำหรับธุรกรรมเกี่ยวกับภาษี)” หรือ “Todsob Service Company Limited (for tax transaction)” — ชื่อนิติบุคคลพร้อมระบุชื่อส่วนงานย่อยหรือชื่อหน่วยงานย่อยในนิติบุคคล ในรูปแบบ “ชื่อนิติบุคคล (ชื่อส่วนงานย่อยหรือชื่อหน่วยงานย่อยในนิติบุคคล)” เช่น “มหาวิทยาลัยทดสอบ (คณะแพทยศาสตร์)” หรือ “Todsob University (Faculty of Medicine,)”
6.2	givenName	nu	-
6.3	surname (sn)	nu	-
6.4	serialNumber	nu	-
6.5	title	nu	-
6.6	organizationalUnitName (ou)	o	ชื่อของหน่วยงานย่อยของนิติบุคคลที่สอดคล้องกับเจ้าของใบรับรอง เช่น “ฝ่ายบริหาร”
6.7	organizationName (o)	m	ชื่อนิติบุคคลของเจ้าของใบรับรองที่ใช้จดทะเบียนกับหน่วยงานที่เป็นนายทะเบียน โดยเป็นภาษาไทยหรือภาษาอังกฤษก็ได้ เช่น “บริษัท เอเอเอ จำกัด” หรือ “AAA Company Limited”
6.8	organizationIdentifier	m	ข้อมูลที่เชื่อมโยงไปยังนิติบุคคลที่เป็นเจ้าของใบรับรอง โดยไม่เชื่อมโยงไปยังนิติบุคคลอื่น เช่น เลขทะเบียนนิติบุคคล เลขประจำตัวผู้เสียภาษีอากรของนิติบุคคลที่เจ้าของใบรับรองสังกัด นอกจากนี้ กลุ่มหน่วยงานที่มีการออกหมายเลขเฉพาะเจาะจงสามารถใช้หมายเลขเหล่านั้นได้ ตัวอย่างเช่น — สถานพยาบาลเอกชนที่ได้รับอนุญาต ให้ใช้หมายเลขใบอนุญาต — สถานพยาบาลของรัฐให้ใช้รหัส 9 หลักของสถานพยาบาล

Index	Item	mandatory	Value
6.9	localityName (L)	o	ระบุรหัสอำเภอหรือเขตที่ตั้งของนิติบุคคลให้เป็นไปตามรหัสของกรมการปกครอง ซึ่งเป็นเลข 4 หลัก เช่น “หลักสี่” ให้ใช้ “1041”
6.10	stateOrProvinceName (S)	o	ระบุรหัสจังหวัดที่ตั้งของนิติบุคคลให้เป็นไปตาม ISO 3166-2 code (ดูได้จาก https://www.iso.org/obp/ui/en/#iso:code:3166:TH) เช่น “กรุงเทพ” ให้ใช้ “TH-10”
6.11	country (c)	m	ระบุรหัสประเทศที่ตั้งของนิติบุคคลให้เป็นไปตาม ISO 3166-1 alpha-2 code เช่น “ประเทศไทย” ให้ใช้รหัส “TH”
7.	subjectPublicKeyInfo	m	
7.1	algorithm	m	หมายเลขโอไอดี (OID) ของอัลกอริทึมของกุญแจสาธารณะ OID = {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}
7.2	subjectPublicKey	m	กุญแจสาธารณะชนิด RSA ความยาวอย่างน้อย 2048 บิต
8.	authorityKeyIdentifier	m	keyIdentifier บรรจุค่าของฟังก์ชัน SHA-1 Hash ของกุญแจสาธารณะที่เป็นคู่กับกุญแจส่วนตัวซึ่งผู้ออกใบรับรองนี้ ใช้ลงลายมือชื่อดิจิทัลเพื่อรับรองใบรับรองนี้
9.	subjectKeyIdentifier	m	keyIdentifier บรรจุค่าของฟังก์ชัน SHA-1 Hash ของ subjectPublicKey ซึ่งอยู่ในฟิลด์ subjectPublicKeyInfo
10.	keyUsage	m	ตั้งค่าตามวัตถุประสงค์ของการใช้งาน ทั้งนี้ สำหรับการใช้งานทั่วไปแนะนำให้ตั้งค่า ดังนี้ (1) สำหรับการลงลายมือชื่อดิจิทัล ให้ตั้งค่าบิต digitalSignature = 1 และ contentCommitment = 1 (2) สำหรับการเข้ารหัสลับ ให้ตั้งค่าบิต keyEncipherment = 1 และ/หรือ dataEncipherment = 1
11.	certificatePolicies	m	
11.1	policyIdentifier	m	หมายเลขโอไอดี (OID) ของ certificate policy
11.2	policyQualifiers	m	ระบุอย่างน้อย 1 PolicyQualifierInfo
11.2.1	PolicyQualifierInfo [1]	m	
11.2.1.1	policyQualifierId	m	หมายเลขโอไอดี (OID) ของประเภท qualifier เป็น certification practice statement OID = {iso(1) org(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) qt(2) cps(1)}
11.2.1.2	qualifier	m	cPSuri = HTTP URL ของ certification practice statement
11.2.2	PolicyQualifierInfo [2]	o	
11.2.2.1	policyQualifierId	o	หมายเลขโอไอดี (OID) ของประเภท qualifier เป็น user notice OID = {iso(1) org(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) qt(2) unotice(2)}

Index	Item	mandatory	Value
11.2.2.2	qualifier	o	userNotice = ข้อความที่แสดง เมื่อใช้ใบรับรอง
12.	subjectAltName	o	
12.1	directoryName	o	ข้อมูลเกี่ยวกับเจ้าของใบรับรอง โดยใช้ชนิดข้อมูลตาม ITU-T X.501 “Name”
12.2	rfc822Name	o	อีเมลของเจ้าของใบรับรอง
13.	basicConstraints	m	
13.1	cA	m	False
13.2	pathLenConstraint	nu	-
14.	extKeyUsage	o	ใช้เมื่อซอฟต์แวร์ที่ใช้ใบรับรองต้องการใช้ค่าในฟิลด์นี้เท่านั้น
15.	cRLDistributionPoints	m	ระบุอย่างน้อย 1 DistributionPoint
15.1	DistributionPoint [1]	m	
15.1.1	distributionPoint	m	HTTP URL ที่สามารถเข้าถึงรายการเพิกถอนใบรับรอง
15.1.2	reason	nu	-
15.1.3	cRLIssuer	nu	-
16.	authorityInfoAccess	m	ระบุ 2 AccessDescription
16.1	AccessDescription [1]	m	
16.1	accessMethod	m	OID = {iso(1) org(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) ocsp(1)}
16.1.2	accessLocation	m	HTTP URL สำหรับเข้าถึงบริการ OCSP
16.2	AccessDescription [2]	m	
16.2.1	accessMethod	m	OID = {iso(1) org(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) calssuers(2)}
16.2.2	accessLocation	m	HTTP URL สำหรับเข้าถึงรายการใบรับรองของผู้ให้บริการออกใบรับรอง

4.3 ใบรับรองประเภทเจ้าหน้าที่นิติบุคคล

ใบรับรองประเภทเจ้าหน้าที่นิติบุคคล คือ ใบรับรองที่ใช้สำหรับสนับสนุนลายมือชื่ออิเล็กทรอนิกส์ (e-signature) เพื่อระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่อและเป็นเจ้าหน้าที่ของนิติบุคคล ทั้งนี้ อาจแสดงตำแหน่งของเจ้าหน้าที่ด้วย โดยมีรายละเอียดของข้อมูลในฟิลด์ต่าง ๆ เป็นไปตามตารางที่ 4

ตารางที่ 4 ข้อมูลในใบรับรองประเภทเจ้าหน้าที่นิติบุคคล

Index	Item	mandatory	Value
1.	version	m	2 (Version 3)
2.	serialNumber	m	ตัวเลขที่ไม่ซ้ำกันระหว่างใบรับรองภายใต้ผู้ให้บริการออกใบรับรองรายเดียวกัน โดยเป็นตัวเลขแบบสุ่มและไม่เรียงกันเมื่อเทียบกับใบรับรองที่ออกก่อนหน้าและต่อจากใบนี้ (randomized and non-sequential) ทั้งนี้ จะต้องมีค่ามากกว่า 0 และขนาดไม่น้อยกว่า 64 บิต [5]

Index	Item	mandatory	Value
3.	signature	m	หมายเลขโอไอดี (OID) ของอัลกอริทึมจากตัวเลือกดังนี้ — {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)} — {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha384WithRSAEncryption(12)} — {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512WithRSAEncryption(13)} — iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)} — {iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)} — {iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA512(4)} ทั้งนี้ ผู้ให้บริการออกใบรับรองควรติดตามการอัปเดตอัลกอริทึมของ signature จากมาตรฐานที่เกี่ยวข้อง เช่น RFC 3279 และมาตรฐานเวอร์ชันที่อัปเดต
4.	issuer	m	
4.1	commonName (cn)	m	ชื่อผู้ให้บริการออกใบรับรองและข้อมูลบ่งบอกถึงระบบบริการ เป็นภาษาอังกฤษ เช่น “XYZ Certification Authority - G1”
4.2	organizationalUnitName (ou)	o	ชื่อหน่วยงานย่อยในองค์กรของผู้ให้บริการออกใบรับรอง เป็นภาษาอังกฤษ เช่น “XYZ Certification Authority”
4.3	organizationName (o)	m	ชื่อองค์กรของผู้ให้บริการออกใบรับรองที่ใช้จดทะเบียนกับหน่วยงานที่เป็นนายทะเบียน เป็นภาษาอังกฤษ เช่น “XYZ Company Limited”
4.4	countryName (c)	m	ระบุรหัสประเทศที่ตั้งของนิติบุคคลให้เป็นไปตาม ISO 3166-1 alpha-2 code เช่น “ประเทศไทย” ให้ใช้รหัส “TH”
4.5	organizationIdentifier	o	เลขประจำตัวผู้เสียภาษีอากรของผู้ให้บริการออกใบรับรอง เช่น “1234567890123”
5.	validity	m	
5.1	notBefore	m	วันและเวลาที่ใบรับรองเริ่มใช้งานได้
5.2	notAfter	m	วันและเวลาที่ใบรับรองสิ้นสุดการใช้งาน
6.	subject	m	
6.1	commonName (cn)	m	— ระบุชื่อตัว-ชื่อสกุลของเจ้าของใบรับรองในรูปแบบ “ชื่อตัว ชื่อสกุล” โดยเป็นภาษาไทยหรือภาษาอังกฤษก็ได้ เช่น

Index	Item	mandatory	Value
			“สมชาย รักดี” หรือ “Somchai Rakdee” — ในกรณีบุคคลที่มีชื่อรอง ให้ระบุชื่อตัว-ชื่อรอง-ชื่อสกุลของเจ้าของใบรับรองในรูปแบบ “ชื่อตัว ชื่อรอง ชื่อสกุล” โดยเป็นภาษาไทยหรือภาษาอังกฤษก็ได้ ทั้งนี้ CA สามารถพิจารณาใส่คำนำหน้าชื่อด้วยก็ได้ตามความเหมาะสม
6.2	givenName	m	— ระบุชื่อตัวของเจ้าของใบรับรองตามเอกสารที่ออกโดยหน่วยงานที่เป็นนายทะเบียนในรูปแบบ “ชื่อตัว” โดยเป็นภาษาไทยหรือภาษาอังกฤษก็ได้ เช่น “สมชาย” หรือ “Somchai” — ในกรณีบุคคลที่มีชื่อรอง ให้ระบุชื่อตัว-ชื่อรองของเจ้าของใบรับรองตามเอกสารที่ออกโดยหน่วยงานที่เป็นนายทะเบียนในรูปแบบ “ชื่อตัว ชื่อรอง” โดยเป็นภาษาไทยหรือภาษาอังกฤษก็ได้ ทั้งนี้ ชื่อตัวและชื่อรองของบุคคลสัญชาติไทยควรใช้เป็นภาษาไทยตามบัตรประจำตัวประชาชน ส่วนชื่อตัวและชื่อรองของบุคคลต่างด้าวให้ใช้เป็นภาษาอังกฤษตามหนังสือเดินทางหรือเอกสารสำคัญประจำตัวอื่นที่หน่วยงานของรัฐเจ้าของสัญชาติออกให้
6.3	surname (sn)	m	ระบุชื่อสกุลของเจ้าของใบรับรองตามเอกสารที่ออกโดยหน่วยงานที่เป็นนายทะเบียน โดยเป็นภาษาไทยหรือภาษาอังกฤษก็ได้ ทั้งนี้ ชื่อสกุลของบุคคลสัญชาติไทยควรใช้เป็นภาษาไทยตามบัตรประจำตัวประชาชน ส่วนชื่อสกุลของบุคคลต่างด้าวให้ใช้เป็นภาษาอังกฤษตามหนังสือเดินทางหรือเอกสารสำคัญประจำตัวอื่นที่หน่วยงานของรัฐเจ้าของสัญชาติออกให้
6.4	serialNumber	o	ข้อมูลที่เชื่อมโยงไปยังเจ้าของใบรับรอง โดยไม่เชื่อมโยงไปยังบุคคลอื่น เช่น เลขประจำตัวประชาชน เลขที่หนังสือเดินทาง หรือตัวเลขที่สร้างด้วยวิธีการสุ่ม ทั้งนี้ อาจใช้ค่าแฮชของเลขประจำตัวประชาชนหรือเลขที่หนังสือเดินทางก็ได้
6.5	title	o	ตำแหน่งของเจ้าของใบรับรองในนิติบุคคลที่เจ้าของใบรับรองสังกัด เช่น “ผู้จัดการ” หรือ “Manager”
6.6	organizationalUnitName (ou)	o	ชื่อของหน่วยงานย่อยในนิติบุคคลที่เจ้าของใบรับรองสังกัด เช่น “แผนกไอที” หรือ “IT Division”
6.7	organizationName (o)	m	ชื่อนิติบุคคลที่เจ้าของใบรับรองสังกัด เช่น “บริษัท เอเอเอ จำกัด” หรือ “AAA Company Limited”
6.8	organizationIdentifier	m	ข้อมูลที่เชื่อมโยงไปยังนิติบุคคลที่เป็นเจ้าของใบรับรอง โดยไม่เชื่อมโยงไปยังนิติบุคคลอื่น เช่น เลขประจำตัวผู้เสียภาษีอากรของนิติบุคคลที่เจ้าของใบรับรองสังกัด เช่น “1234567890123”

Index	Item	mandatory	Value
6.9	country (c)	m	ระบุรหัสประเทศที่ตั้งของนิติบุคคลให้เป็นไปตาม ISO 3166-1 alpha-2 code เช่น “ประเทศไทย” ให้ใช้รหัส “TH”
7.	subjectPublicKeyInfo	m	
7.1	algorithm	m	หมายเลขโอไอดี (OID) ของอัลกอริทึมของกุญแจสาธารณะ OID = {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}
7.2	subjectPublicKey	m	กุญแจสาธารณะชนิด RSA ความยาวอย่างน้อย 4096 บิต
8.	authorityKeyIdentifier	m	keyIdentifier บรรจุค่าของฟังก์ชัน SHA-1 Hash ของกุญแจสาธารณะที่เป็นคู่กับกุญแจส่วนตัวซึ่งผู้ออกใบรับรองนี้ ใช้ลงลายมือชื่อดิจิทัลเพื่อรับรองใบรับรองนี้
9.	subjectKeyIdentifier	m	keyIdentifier บรรจุค่าของฟังก์ชัน SHA-1 Hash ของ subjectPublicKey ซึ่งอยู่ในฟิลด์ subjectPublicKeyInfo
10.	keyUsage	m	ตั้งค่าตามวัตถุประสงค์ของการใช้งาน ทั้งนี้ สำหรับการใช้งานทั่วไปแนะนำให้ตั้งค่า ดังนี้ (1) สำหรับการลงลายมือชื่อดิจิทัล ให้ตั้งค่าบิต digitalSignature = 1 และ contentCommitment = 1 (2) สำหรับการเข้ารหัสลับ ให้ตั้งค่าบิต keyEncipherment = 1 และ/หรือ dataEncipherment = 1
11.	certificatePolicies	m	
11.1	policyIdentifier	m	หมายเลขโอไอดี (OID) ของ certificate policy
11.2	policyQualifiers	m	ระบุอย่างน้อย 1 PolicyQualifierInfo
11.2.1	PolicyQualifierInfo [1]	m	
11.2.1.1	policyQualifierId	m	หมายเลขโอไอดี (OID) ของประเภท qualifier เป็น certification practice statement OID = {iso(1) org(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) qt(2) cps(1)}
11.2.1.2	qualifier	m	cPSuri = HTTP URL ของ certification practice statement
11.2.2	PolicyQualifierInfo [2]	o	
11.2.2.1	policyQualifierId	o	หมายเลขโอไอดี (OID) ของประเภท qualifier เป็น user notice OID = {iso(1) org(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) qt(2) unotice(2)}
11.2.2.2	qualifier	o	userNotice = ข้อความที่แสดง เมื่อใช้ใบรับรอง
12.	subjectAltName	o	
12.1	directoryName	o	ข้อมูลเกี่ยวกับเจ้าของใบรับรอง โดยใช้ชนิดข้อมูลตาม ITU-T X.501 “Name”
12.2	rfc822Name	o	อีเมลของเจ้าของใบรับรอง
13.	basicConstraints	m	

Index	Item	mandatory	Value
13.1	cA	m	False
13.2	pathLenConstraint	nu	-
14.	extKeyUsage	o	ใช้เมื่อซอฟต์แวร์ที่ใช้ใบรับรองต้องการใช้ค่าในฟิลด์นี้เท่านั้น
15.	cRLDistributionPoints	m	ระบุอย่างน้อย 1 DistributionPoint
15.1	DistributionPoint [1]	m	
15.1.1	distributionPoint	m	HTTP URL ที่สามารถเข้าถึงรายการเพิกถอนใบรับรอง
15.1.2	reason	nu	-
15.1.3	cRLIssuer	nu	-
16.	authorityInfoAccess	m	ระบุ 2 AccessDescription
16.1	AccessDescription [1]	m	
16.1.1	accessMethod	m	OID = {iso(1) org(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) ocsp(1)}
16.1.2	accessLocation	m	HTTP URL สำหรับเข้าถึงบริการ OCSP
16.2	AccessDescription [2]	m	
16.2.1	accessMethod	m	OID = {iso(1) org(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) calssuers(2)}
16.2.2	accessLocation	m	HTTP URL สำหรับเข้าถึงรายการใบรับรองของผู้ให้บริการออกใบรับรอง

4.4 หมายเลขโอไอดี (OID) ของ Certificate Policy

ในการออกใบรับรองให้ผู้ใช้บริการ CA จะระบุหมายเลขโอไอดี (OID) ของ CP ใน policyIdentifier ซึ่งอยู่ภายใต้ฟิลด์ certificatePolicies ด้วยเพื่อระบุประเภทของใบรับรอง หมายเลขโอไอดี (OID) ของ CP ดังกล่าวมีไว้สำหรับให้คู่กรณีที่เกี่ยวข้อง (relying parties) ใช้ในการพิจารณาความเหมาะสมและขอบเขตการใช้งานของใบรับรอง ทั้งนี้ หมายเลขโอไอดี (OID) ของ CP แต่ละประเภทใบรับรอง มีดังนี้

4.4.1 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

4.4.2 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

4.4.3 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-User

ทั้งนี้ หมายเลขโอไอดี (OID) ของ CP สำหรับใบรับรองประเภทอื่น ๆ ที่ CA ออกโดยมีวัตถุประสงค์เฉพาะเจาะจงต่อการใช้งาน CA สามารถกำหนดหมายเลขโอไอดี (OID) สำหรับการใช้งานดังกล่าวเพิ่มเติมและแจ้งหมายเลขโอไอดี (OID) กับ NRCA ตัวอย่างเช่น ใบรับรองสำหรับแพทย์ ใบรับรองสำหรับลงลายมือชื่อดิจิทัลโดยระบบให้บริการ ใบรับรองที่ระบุความน่าเชื่อถือของการพิสูจน์ตัวตน

ภาคผนวก ก.
การเปรียบเทียบข้อมูลในใบรับรองแต่ละประเภท

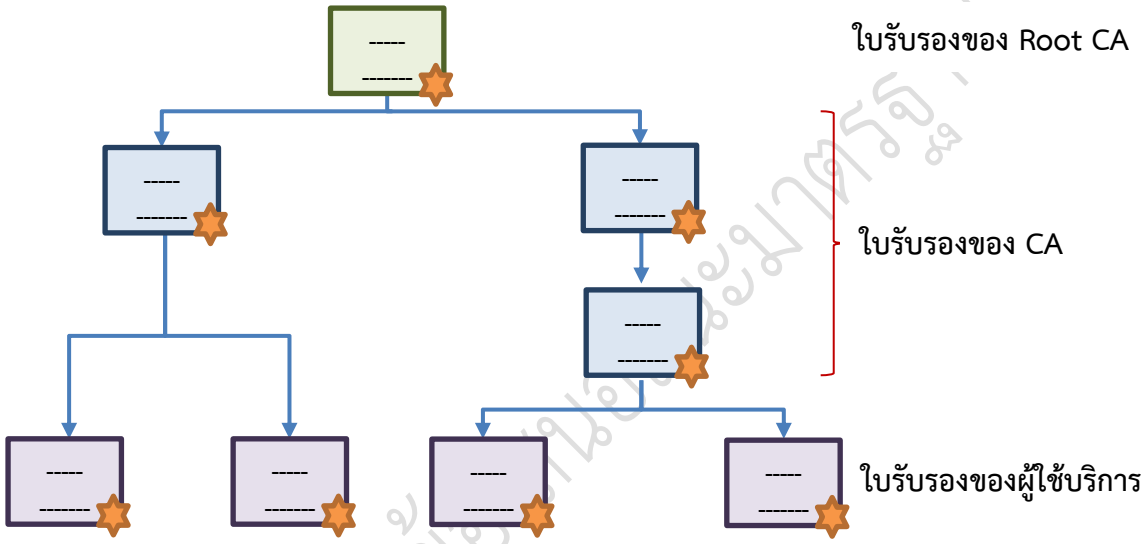
ตารางที่ 5 การเปรียบเทียบข้อมูลในใบรับรองแต่ละประเภท

ชื่อฟิลด์	บุคคลธรรมดา	เจ้าหน้าที่นิติบุคคล	นิติบุคคล
version	m	m	m
serialNumber	m	m	m
signature	m	m	m
issuer	m	m	m
commonName (cn)	m	m	m
organizationalUnitName (ou)	o	o	o
organizationName (o)	m	m	m
countryName (c)	m	m	m
organizationIdentifier	o	o	o
validity	m	m	m
notBefore	m	m	m
notAfter	m	m	m
subject	m	m	m
commonName (cn)	m	m	m
givenName	m	m	nu
surname (sn)	m	m	nu
serialNumber	o	o	nu
title	nu	o	nu
organizationalUnitName (ou)	nu	o	o
organizationName (o)	nu	m	m
organizationIdentifier	nu	m	m
country (c)	m	m	m
subjectPublicKeyInfo	m	m	m
algorithm	m	m	m
subjectPublicKey	m	m	m
authorityKeyIdentifier	m	m	m
subjectKeyIdentifier	m	m	m
keyUsage	m	m	m
certificatePolicies	m	m	m
policyIdentifier	m	m	m
policyQualifiers	m	m	m
PolicyQualifierInfo [1]	m	m	m
policyQualifierId	m	m	m
qualifier	m	m	m
PolicyQualifierInfo [2]	o	o	o
policyQualifierId	o	o	o

ชื่อฟิลด์	บุคคลธรรมดา	เจ้าหน้าที่นิติบุคคล	นิติบุคคล
qualifier	o	o	o
subjectAltName	o	o	o
directoryName	o	o	o
rfc822Name	o	o	o
basicConstraints	m	m	m
cA	m	m	m
pathLenConstraint	nu	nu	nu
extKeyUsage	o	o	o
cRLDistributionPoints	m	m	m
DistributionPoint [1]	m	m	m
distributionPoint	m	m	m
reason	nu	nu	nu
cRLIssuer	nu	nu	nu
authorityInfoAccess	m	m	m
AccessDescription [1]	m	m	m
accessMethod	m	m	m
accessLocation	m	m	m
AccessDescription [2]	m	m	m
accessMethod	m	m	m
accessLocation	m	m	m

ภาคผนวก ข.
โครงสร้างความสัมพันธ์ของใบรับรองในประเทศไทย

ใบรับรองภายใต้ผู้ให้บริการออกใบรับรองในประเทศไทยสามารถแบ่งระดับตามความสัมพันธ์ระหว่างผู้ให้บริการออกใบรับรองและผู้ใช้บริการเป็นไปตามรูปที่ 1 โดยมีรายละเอียดดังนี้



รูปที่ 1 โครงสร้างความสัมพันธ์ของใบรับรองในประเทศไทย

(1) ใบรับรองของผู้ให้บริการออกใบรับรองลำดับชั้นบนสุด (Root CA certificate)

ผู้ให้บริการออกใบรับรองลำดับชั้นบนสุดหรือ Root CA ซึ่งในที่นี้คือผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์แห่งชาติ (National Root CA Certificate: NRCA) จะลงลายมือประกอบกับใบรับรองของตนเพื่อรับรองตนเอง (self-signed)

NRCA มีหน้าที่ออกใบรับรองให้กับผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา (Subordinate CA) และมีหน้าที่กำหนดแนวนโยบาย (CP) ของผู้ให้บริการออกใบรับรองซึ่ง CA ต้องปฏิบัติให้สอดคล้อง

(2) ใบรับรองของผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา (Subordinate CA certificate)

Subordinate CA หรือ CA ที่มีใบรับรองที่ออกโดย Root CA โดย CA ประเภทนี้สามารถออกใบรับรองให้กับ Sub-CA หรือผู้ใช้บริการ ทั้งนี้ NRCA มีนโยบายให้มีใบรับรองของ CA ได้ไม่เกิน 2 ชั้น นับตั้งแต่ใบรับรองของ CA ที่ออกโดย NRCA

(3) ใบรับรองของผู้ใช้บริการ (Subscriber certificate)

ใบรับรองของผู้ใช้บริการ คือ ใบรับรองที่ออกโดย CA เพื่อรับรองข้อมูลตัวตนและความเป็นเจ้าของคู่กุญแจของเอนทิตี โดยใบรับรองของผู้ใช้บริการสามารถใช้งานได้ตามวัตถุประสงค์ที่กำหนดในใบรับรอง เช่น การลงลายมือชื่อดิจิทัล การเข้ารหัสลับ หรือการยืนยันตัวตน

211 **บรรณานุกรม**

212

[1] ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวทางการจัดทำแนวนโยบาย (Certificate Policy) และแนวปฏิบัติ (Certification Practice Statement) ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority) พ.ศ. 2552 ประกาศ ณ วันที่ 8 ตุลาคม พ.ศ. 2552.

[2] พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และฉบับแก้ไขเพิ่มเติม (ฉบับที่ 2).

[3] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วย แนวทางการลงลายมือชื่ออิเล็กทรอนิกส์ เลขที่ ขมธอ. 23-2563, เวอร์ชัน 1.0.

[4] D. Cooper, S. Santesson, S. Farrel, S. Boeyen, R. Housley, W. Polk, “IETF RFC 5280 (2008), Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,” IETF, May 2008. [ออนไลน์]. Available: https://tools.ietf.org/html/rfc5280.

[5] CA/Browser Forum, “Baseline Requirement Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates,” เล่มที่ Version 1.4.2, January 7, 2017.

[6] Recommendation ITU-T X.509 (2016) | ISO/IEC 9594-8 : 2017 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

[7] European Telecommunications Standards Institute, "(draft) ETSI EN 319412-3 V1.1.3 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons", April 2020.

[8] International Civil Aviation Organisation (ICAO), "Doc 9303 Machine Readable Travel Documents Part 3: Specifications Common to all MRTDs", 2021.

[9] Recommendation ITU-T X.520 (2019) | ISO/IEC 9594-6 : 2020 Information Technology - Open Systems Interconnection – The Directory: Selected attribute types.

[10] European Telecommunications Standards Institute, "EN 319411-2 V2.2.1: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons", July 2020.

[11] European Telecommunications Standards Institute, "ETSI EN 319411-1 V1.3.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements ", May 2021.

[12] International Organization for Standardization, "ISO/IEC 9594-8:2020: Information technology - Open systems interconnection -Part 8: The Directory: Public-key and attribute certificate frameworks", December 2020.

213

214