ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
เรื่อง ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์
ว่าด้วยข้อมูลในใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ

โดยที่เป็นการสมควรปรับปรุงข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ เพื่อให้การกำหนดข้อมูลในใบรับรองสอดคล้องกับการกำหนดประเภทของใบรับรองและข้อมูลในใบรับรองของผู้ใช้บริการ ๓ ประเภท ได้แก่ ใบรับรองประเภทบุคคลธรรมดา (natural person certificate) ใบรับรองประเภทนิติบุคคล (juristic person certificate) และใบรับรองประเภทเจ้าหน้าที่นิติบุคคล (enterprise user certificate) สำหรับให้ผู้ให้บริการออกใบรับรอง (certification authority: CA) มีแนวทางในการออกใบรับรองของผู้ใช้บริการที่เป็นมาตรฐานเดียวกันและเป็นไปตามมาตรฐานสากล รวมถึงเหมาะสมกับบริบทการใช้งานของประเทศไทย

อาศัยอำนาจตามความในมาตรา ๕ แห่งพระราชบัญญัติสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๒ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ จึงให้ยกเลิกประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการกำหนดข้อมูลในใบรับรองและรายการเพิกถอนใบรับรอง เลขที่ ขมธอ. ๑๕-๒๕๖๐ เวอร์ชัน ๑.๐ ลงวันที่ ๑๕ สิงหาคม พ.ศ. ๒๕๖๐ และประกาศข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยข้อมูลในใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ เลขที่ ขมธอ. ๑๕-๒๕๖๖ เวอร์ชัน ๒.๐ ปรากฏตามท้ายประกาศฉบับนี้

ประกาศ ณ วันที่ ๔ ตุลาคม พ.ศ. ๒๕๖๖

(นายมีธรรม ณ ระนอง)
รองผู้อำนวยการ
ปฏิบัติการแทนผู้อำนวยการ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ETDA Recommendation on ICT Standard for Electronic Transactions

ขมธอ. 15-2566

ว่าด้วยข้อมูลในใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ

SUBSCRIBER CERTIFICATE PROFILE

เวอร์ชัน 2.0

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ICS 35.030

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยข้อมูลในใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ

ขมธอ. 15-2566

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 4 ตุลาคม พ.ศ. 2566

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 3 ประเภท ได้แก่ ใบรับรองประเภทบุคคลธรรมดา (natural person certificate) ใบรับรองประเภทนิติบุคคล (juristic person certificate) และใบรับรองประเภทเจ้าหน้าที่นิติบุคคล (enterprise user certificate) สำหรับให้ผู้ให้บริการออกใบรับรอง (certification authority: CA) มีแนวทางในการออกใบรับรองของผู้ใช้บริการที่เป็นมาตรฐานเดียวกันและเป็นไปตามมาตรฐานสากล รวมถึงเหมาะสมกับบริบทการใช้งานของประเทศไทย

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

ใบรับรองอิเล็กทรอนิกส์ หรือใบรับรอง (certificate) เป็นส่วนประกอบสำคัญสำหรับการตรวจสอบลายมือชื่อดิจิทัล โดยใบรับรองจะบันทึกข้อมูลอิเล็กทรอนิกส์ซึ่งยืนยันความเชื่อมโยงระหว่างเจ้าของลายมือชื่อกับข้อมูลสำหรับใช้สร้างลายมือชื่อดิจิทัลไว้ การกำหนดข้อมูลในใบรับรองให้สอดคล้องตามประเภทการใช้งานจะทำให้การตรวจสอบลายมือชื่อดิจิทัลมีความสะดวกต่อการใช้งานและเป็นมาตรฐานเดียวกัน

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

สารบัญ

สารบัญรูป

สารบัญตาราง

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ว่าด้วยข้อมูลในใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ

1. ขอบข่าย

ข้อเสนอแนะมาตรฐานฉบับนี้กำหนดประเภทของใบรับรองและข้อมูลในใบรับรองของผู้ใช้บริการ 3 ประเภท ได้แก่ ใบรับรองประเภทบุคคลธรรมดา (natural person certificate) ใบรับรองประเภทนิติบุคคล (juristic person certificate) และใบรับรองประเภทเจ้าหน้าที่นิติบุคคล (enterprise user certificate) สำหรับให้ผู้ให้บริการออกใบรับรอง (certification authority: CA) มีแนวทางในการออกใบรับรองของผู้ใช้บริการที่เป็นมาตรฐานเดียวกันและเป็นไปตามมาตรฐานสากล ทั้งนี้ ข้อมูลในใบรับรองของผู้ใช้บริการอ้างอิงตาม RFC 5280 [1] และเพิ่มข้อกำหนดของข้อมูลในใบรับรองให้เหมาะสมกับบริบทการใช้งานของประเทศไทย

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

ใบรับรองของผู้ใช้บริการ (subscriber certificate) สามารถนำไปใช้งานสำหรับการยืนยันตัวตน (authentication) การเข้ารหัสลับ (encryption) และการตรวจสอบลายมือชื่อดิจิทัล (digital signature verification) ทั้งนี้ ในกรณีของบุคคลธรรมดาและเจ้าหน้าที่นิติบุคคล ลายมือชื่อดิจิทัลจะใช้เป็นลายมือชื่ออิเล็กทรอนิกส์ (e-signature) ของบุคคลธรรมดา ซึ่งมีวัตถุประสงค์เพื่อระบุตัวบุคคลธรรมดาผู้เป็นเจ้าของลายมือชื่อและแสดงเจตนาของบุคคลนั้นที่มีต่อข้อความ แต่ในกรณีของนิติบุคคล ลายมือชื่อดิจิทัลจะใช้เป็นตราอิเล็กทรอนิกส์ (e-seal) ของนิติบุคคล ซึ่งมีวัตถุประสงค์เพื่อยืนยันแหล่งที่มาของข้อความว่ามาจากนิติบุคคลนั้น

2. บทนิยาม

ความหมายของคำที่ใช้ในข้อเสนอแนะมาตรฐานฉบับนี้ มีดังต่อไปนี้

2.1 บุคคล หมายถึง บุคคลธรรมดา หรือนิติบุคคล [2]

2.2 เอนทิตี (entity) หมายถึง บุคคลและรวมถึงเครื่องให้บริการ (server) หรือเว็บไซต์ หรือหน่วยปฏิบัติงาน (operation unit/site) หรือเครื่องมืออื่นใด (device) ที่อยู่ภายใต้ความควบคุมของบุคคล [2]

2.3 ลายมือชื่ออิเล็กทรอนิกส์ หมายถึง อักษร อักขระ ตัวเลข เสียงหรือสัญลักษณ์อื่นใดที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์ซึ่งนำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้น และเพื่อแสดงว่าบุคคลดังกล่าวยอมรับข้อความในข้อมูลอิเล็กทรอนิกส์นั้น [3]

2.4 ลายมือชื่อดิจิทัล (digital signature) หมายถึง ลายมือชื่ออิเล็กทรอนิกส์ที่ได้จากกระบวนการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ ซึ่งช่วยให้สามารถยืนยันตัวเจ้าของลายมือชื่อและตรวจพบการเปลี่ยนแปลงของข้อความ และลายมือชื่ออิเล็กทรอนิกส์ได้รวมถึงการทำให้เจ้าของลายมือชื่อไม่สามารถปฏิเสธความรับผิดจากข้อความที่ตนเองลงลายมือชื่อได้ [4]

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 [2]

2.8 หมายเลขโอไอดี (object identifier: OID) หมายถึง ค่าสัมพันธ์ซึ่งบ่งบอกถึงข้อมูลสารสนเทศของวัตถุ (information object) ใด ๆ โดยเป็นค่าที่สามารถบ่งชี้ได้ถึงความเป็นหนึ่งเดียวของ object นั้น ๆ [2]

2.9 กุญแจสาธารณะ (public key) หมายถึง กุญแจที่ใช้ตรวจสอบลายมือชื่อดิจิทัล และสามารถนำไปใช้เข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ เพื่อมิให้สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ที่มีการเข้ารหัสลับนั้นได้ เพื่อประโยชน์ในการรักษาความลับของข้อมูลอิเล็กทรอนิกส์นั้น [2]

2.10 กุญแจส่วนตัว (private key) หมายถึง กุญแจที่ใช้สร้างลายมือชื่อดิจิทัล และสามารถนำไปใช้ในการถอดรหัสลับเมื่อมีการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ เพื่อให้สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ที่มีการเข้ารหัสลับนั้นได้ [2]

2.11 คู่กุญแจ (key pair) หมายถึง กุญแจส่วนตัวและกุญแจสาธารณะในระบบการเข้ารหัสลับแบบอสมมาตรที่สร้างขึ้นโดยวิธีการที่ทำให้กุญแจส่วนตัวมีความสัมพันธ์ในทางคณิตศาสตร์กับกุญแจสาธารณะในลักษณะที่สามารถใช้กุญแจสาธารณะตรวจสอบได้ว่าลายมือชื่อดิจิทัลได้สร้างขึ้นโดยใช้กุญแจส่วนตัวนั้นหรือไม่ และสามารถนำกุญแจสาธารณะไปใช้ในการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ ทำให้ไม่สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ได้เพื่อประโยชน์ในการรักษาความลับของข้อมูลอิเล็กทรอนิกส์ เว้นแต่บุคคลที่ถือกุญแจส่วนตัวซึ่งสามารถนำกุญแจส่วนตัวของตนใช้ในการถอดรหัสลับของข้อมูลอิเล็กทรอนิกส์ เพื่อให้เจ้าของกุญแจส่วนตัวสามารถอ่านหรือเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์นั้นได้ [2]

2.12 แนวนโยบายของผู้ให้บริการออกใบรับรอง (certificate policy: CP) หมายถึง นโยบายที่ระบุแนวทางการใช้งานใบรับรองตามประเภทการใช้งานหรือตามกลุ่มการใช้งานที่มีวัตถุประสงค์เฉพาะเจาะจง และระบุข้อกำหนดด้านความมั่นคงปลอดภัยทั่วไป

2.13 แนวปฏิบัติของผู้ให้บริการออกใบรับรอง (certification practice statement: CPS) หมายถึง แนวปฏิบัติสำหรับให้ผู้ให้บริการออกใบรับรองใช้ในการออก การจัดการ การเพิกถอน และการต่ออายุใบรับรอง ซึ่งรวมถึงการเปลี่ยนกุญแจสาธารณะใหม่สำหรับใบรับรอง

2.14 รายการเพิกถอนใบรับรอง (certificate revocation list: CRL) หมายถึง รายการใบรับรองที่ถูกเพิกถอนการใช้งาน

2.15 เกณฑ์วิธีการตรวจสอบสถานะของใบรับรอง (online certificate status protocol: OCSP) หมายถึง เกณฑ์วิธี (protocol) สำหรับตรวจสอบสถานะของการเพิกถอนใบรับรอง

3. ข้อมูลในใบรับรอง

ใบรับรอง X.509 เวอร์ชัน 3 ซึ่งเป็นไปตามมาตรฐาน RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile จะประกอบด้วยฟิลด์ข้อมูล 3 ฟิลด์ ดังนี้

(1) ฟิลด์ tbsCertificate: แสดงข้อมูลในใบรับรอง ซึ่งแบ่งเป็น 2 ส่วน

- ฟิลด์พื้นฐาน (basic fields) เช่น ข้อมูลของเจ้าของใบรับรอง ข้อมูลของผู้ให้บริการออกใบรับรอง กุญแจสาธารณะของเจ้าของใบรับรอง ช่วงเวลาที่สามารถใช้ใบรับรองได้ รายละเอียดตามหัวข้อ 3.1
- ฟิลด์เพิ่มเติม (extension fields) สำหรับบรรจุข้อมูลอื่น ๆ ที่อยู่นอกเหนือจากฟิลด์พื้นฐาน รายละเอียดตามหัวข้อ 3.2 โดย RFC 5280 ได้กำหนดฟิลด์เพิ่มเติมหลายชนิดให้เลือกใช้งาน ทั้งฟิลด์เพิ่มเติมแบบมาตรฐาน (standard extensions) และฟิลด์เพิ่มเติมที่กำหนดขึ้นเพื่อใช้งานตามวัตถุประสงค์เฉพาะ (private internet extensions) ทั้งนี้ หากมีความจำเป็นต้องใช้ฟิลด์เพิ่มเติมที่นอกเหนือจากรายการตามตารางที่ 1 ในหัวข้อ 3.2 ผู้ให้บริการออกใบรับรองสามารถกำหนดฟิลด์เพิ่มเติมได้โดยวิธีการกำหนดข้อมูลให้อ้างอิงตาม 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) โดยข้อมูลวันและเวลาสามารถระบุได้ 2 รูปแบบ คือ UTCTime และ GeneralizedTime ทั้งนี้ ใบรับรองที่หมดอายุก่อนปี ค.ศ. 2050 ต้องระบุข้อมูลในฟิลด์ validity เป็น UTCTime และใบรับรองที่หมดอายุในปี ค.ศ. 2050 เป็นต้นไป ต้อง ระบุข้อมูลในฟิลด์ validity เป็น GeneralizedTime โดยมีรูปแบบดังนี้

- UTCTime มีรูปแบบคือ YYMMDDhhmmssZ
- GeneralizedTime มีรูปแบบคือ YYYYMMDDhhmmssZ

โดย

YYYY	คือ ปีคริสต์ศักราชในรูปแบบตัวเลข 4 หลัก
YY	คือ ปีคริสต์ศักราชในรูปแบบตัวเลข 2 หลักหลัง
MM	คือ เดือนในรูปแบบตัวเลข 2 หลัก (01-12)
DD	คือ วันในรูปแบบตัวเลข 2 หลัก (01-31)
hh	คือ ชั่วโมงในรูปแบบตัวเลข 2 หลัก (00-23)
mm	คือ นาทีในรูปแบบตัวเลข 2 หลัก (00-59)
ss	คือ วินาทีในรูปแบบตัวเลข 2 หลัก (00-59)
Z	คือ ตัวอักษร ‘Z’ ซึ่งแสดงว่า เวลาที่ระบุเป็นเวลากลางของโลก หรือ Greenwich Mean Time (Zulu)

(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 ซึ่งแสดงข้อมูลเพิ่มเติมเกี่ยวกับเจ้าของใบรับรองและกุญแจสาธารณะ 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) ที่เกี่ยวข้องกับการออกใบรับรองและวัตถุประสงค์ของการใช้งานใบรับรอง 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 พร้อมทั้งระบุจำนวนชั้นของใบรับรองของผู้ให้บริการออกใบรับรอง ที่มากที่สุดที่อนุญาตให้อยู่ในชั้นถัดลงมาจากใบรับรองใบนี้ใน certification path

(7) extended key usage: เป็นฟิลด์เพิ่มเติมที่ใช้ระบุถึงวัตถุประสงค์ของการใช้กุญแจสาธารณะในใบรับรองที่เพิ่มเติมจากฟิลด์ keyUsage

(8) CRL distribution points: เป็นฟิลด์เพิ่มเติมที่ใช้ระบุวิธีการเข้าถึงรายการเพิกถอนใบรับรอง (CRL) โดยแสดงเป็นลำดับของแหล่งเผยแพร่รายการเพิกถอนใบรับรอง

(9) authority information access: เป็นฟิลด์เพิ่มเติมที่ระบุวิธีการเข้าถึงข้อมูล และบริการต่าง ๆ ของผู้ให้บริการออกใบรับรองที่ออกใบรับรองนี้

ทั้งนี้ ฟิลด์เพิ่มเติมจะมีการกำหนดค่าความสำคัญ (critical) ในรูปแบบ Boolean โดยมีรายละเอียดดังนี้

- ค่าความสำคัญเป็น True (T) หมายถึง ฟิลด์เพิ่มเติมที่มีความสำคัญ (critical extension) ทั้งนี้ หากระบบที่ใช้ใบรับรองไม่รู้จักฟิลด์เพิ่มเติมนั้นหรือไม่สามารถประมวลผลข้อมูลในฟิลด์เพิ่มเติมนั้นได้ ระบบดังกล่าวจะต้องปฏิเสธการใช้งานใบรับรอง
- ค่าความสำคัญเป็น False (F) หมายถึง ฟิลด์เพิ่มเติมที่ไม่มีความสำคัญ (non-critical extension) ทั้งนี้ หากระบบที่ใช้ใบรับรองไม่รู้จักฟิลด์เพิ่มเติมนั้น ระบบดังกล่าวอาจละเว้นการประมวลผลข้อมูลในฟิลด์เพิ่มเติมนั้น

ทั้งนี้ ชื่อฟิลด์เพิ่มเติม ชื่อฟิลด์เพิ่มเติมในรูป ASN.1 หมายเลขโอไอดี (OID) และค่าความสำคัญเป็นไปตามตารางที่ 1 โดยรายละเอียดอื่น ๆ ของฟิลด์เพิ่มเติมเป็นไปตาม RFC 5280 ข้อ 4.2 Certificate Extensions

ตารางที่ 1 รายการฟิลด์เพิ่มเติมในใบรับรอง

Index	ชื่อฟิลด์เพิ่มเติม	ชื่อฟิลด์เพิ่มเติมในรูป ASN.1	หมายเลขโอไอดี (OID)	ค่าความสำคัญ
	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

Index	ชื่อฟิลด์เพิ่มเติม	ชื่อฟิลด์เพิ่มเติมในรูป ASN.1	หมายเลขโอไอดี (OID)	ค่าความสำคัญ
(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 [1] 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): ต้องระบุข้อมูลนี้
- O (optional): เลือกระบุข้อมูลนี้หรือไม่ก็ได้ ขึ้นอยู่กับความต้องการใช้งาน
- NU (not used): ไม่ต้องระบุข้อมูลนี้

(4) สดมภ์ Value แสดงข้อมูลหรือวิธีการกำหนดข้อมูลในฟิลด์พื้นฐาน ฟิลด์เพิ่มเติม หรือคุณลักษณะ

ทั้งนี้ รายละเอียดของข้อมูลในใบรับรองของผู้ใช้บริการซึ่งแบ่งออกเป็น 3 ประเภท ได้แก่

(1) ใบรับรองประเภทบุคคลธรรมดา (natural person certificate) รายละเอียดตามหัวข้อ 4.1
(2) ใบรับรองประเภทนิติบุคคล (juristic person certificate) รายละเอียดตามหัวข้อ 4.2
(3) ใบรับรองประเภทเจ้าหน้าที่นิติบุคคล (enterprise user certificate) รายละเอียดตามหัวข้อ 4.3

4.1 ใบรับรองประเภทบุคคลธรรมดา

ใบรับรองประเภทบุคคลธรรมดา (natural person certificate) มีรายละเอียดข้อมูลในฟิลด์ต่าง ๆ เป็นไปตามตารางที่ 2

ตารางที่ 2 ข้อมูลในใบรับรองประเภทบุคคลธรรมดา

Index	Item	Mandatory	Value
1.	version	M	2 (Version 3)
2.	serialNumber	M	ตัวเลขที่ไม่ซ้ำกันระหว่างใบรับรองภายใต้ผู้ให้บริการออกใบรับรอง (CA) รายเดียวกัน โดยเป็นตัวเลขแบบสุ่มและไม่เรียงกันเมื่อเทียบกับใบรับรองที่ออกก่อนหน้าและต่อจากใบนี้ (randomized and non-sequential) ทั้งนี้ จะต้องมีค่ามากกว่า 0 และขนาดไม่น้อยกว่า 64 บิต [5]
3.	signature	M	หมายเลขโอไอดี (OID) ของอัลกอริทึมจากตัวเลือกดังนี้

Index	Item	Mandatory	Value
			– {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 CA ควรติดตามการอัปเดตอัลกอริทึมจากมาตรฐานที่เกี่ยวข้อง
4.	issuer	M	ข้อมูลในฟิลด์ issuer ทั้งหมด ให้ระบุโดยใช้การเข้ารหัสแบบ PrintableString เท่านั้น
4.1	commonName (cn)	M	ชื่อ CA และข้อมูลบ่งบอกถึงระบบบริการ เป็นภาษาอังกฤษ เช่น “XYZ Certification Authority - G1”
4.2	organizationalUnitName (ou)	O	ชื่อหน่วยงานย่อยในองค์กรของ CA เป็นภาษาอังกฤษ เช่น “XYZ Certification Authority”
4.3	organizationName (o)	M	ชื่อ CA ตามที่จดทะเบียนกับกรมพัฒนาธุรกิจการค้าหรือที่ระบุในเอกสารสำคัญอื่น เป็นภาษาอังกฤษ เช่น “XYZ Company Limited”
4.4	countryName (c)	M	รหัสประเทศที่ตั้งของ CA ให้เป็นไปตาม ISO 3166-1 alpha-2 code เช่น “ประเทศไทย” ให้ใช้รหัส “TH”
4.5	organizationIdentifier	O	รหัสที่เชื่อมโยงไปยัง CA ที่ออกใบรับรองนี้เท่านั้น ตัวอย่างเช่น CA ที่มีเลขประจำตัวผู้เสียภาษีอากร (tax identification number: TIN) ให้ใช้รูปแบบที่มีตัวอักษรนำหน้า “TIN” คั่นด้วยเครื่องหมาย “-” และตามด้วยเลขประจำตัวผู้เสียภาษีอากร 13 หลัก เช่น “TIN-1234567890123”
5.	validity	M	
5.1	notBefore	M	วันและเวลาที่ใบรับรองเริ่มใช้งานได้
5.2	notAfter	M	วันและเวลาที่ใบรับรองสิ้นสุดการใช้งาน
6.	subject	M	– ข้อมูล serialNumber และ countryName ในฟิลด์ subject ใช้การเข้ารหัสแบบ PrintableString เท่านั้น – ข้อมูลอื่นในฟิลด์ subject สามารถใช้การเข้ารหัสแบบ PrintableString หรือ UTF8String

Index	Item	Mandatory	Value
6.1	commonName (cn)	M	ชื่อตัว ชื่อรอง (ถ้ามี) ชื่อสกุล ให้ระบุตามหลักฐานแสดงตน เช่น บัตรประจำตัวประชาชน หรือหนังสือเดินทาง ซึ่งสามารถมีรูปแบบได้ดังนี้ — ระบุ “ชื่อตัว ชื่อรอง (ถ้ามี) ชื่อสกุล” เป็นอักษรภาษาหลักที่ไม่ใช่อักษรภาษาอังกฤษ คั่นด้วย “/” และตามด้วย “ชื่อตัว ชื่อรอง (ถ้ามี) ชื่อสกุล” เป็นอักษรภาษาอังกฤษ เช่น “สมชาย รักดี/Somchai Rakdee” — ระบุ “ชื่อตัว ชื่อรอง (ถ้ามี) ชื่อสกุล” เป็นอักษรภาษาอังกฤษ เช่น “Somchai Rakdee” ทั้งนี้ CA อาจพิจารณาใส่คำนำหน้าชื่อด้วยก็ได้ตามความเหมาะสม
6.2	givenName	M	ชื่อตัว ชื่อรอง (ถ้ามี) ให้ระบุตามหลักฐานแสดงตน เช่น บัตรประจำตัวประชาชน หรือหนังสือเดินทาง ในรูปแบบ “ชื่อตัว ชื่อรอง (ถ้ามี)” โดยเป็นภาษาไทยหรือภาษาอังกฤษก็ได้ เช่น “สมชาย” หรือ “Somchai” ทั้งนี้ ชื่อตัวของบุคคลสัญชาติไทยควรใช้เป็นภาษาไทยตามบัตรประจำตัวประชาชน ในขณะเดียวกันชื่อตัวของบุคคลต่างด้าวให้ใช้เป็นภาษาอังกฤษตามหนังสือเดินทางหรือเอกสารสำคัญประจำตัวอื่นที่หน่วยงานของรัฐออกให้
6.3	surname (sn)	M	ชื่อสกุล ให้ระบุตามหลักฐานแสดงตน เช่น บัตรประจำตัวประชาชน หรือหนังสือเดินทาง ในรูปแบบ “ชื่อสกุล” โดยเป็นภาษาไทยหรือภาษาอังกฤษก็ได้ เช่น “รักดี” หรือ “Rakdee” ทั้งนี้ ชื่อสกุล ของบุคคลสัญชาติไทยควรใช้เป็นภาษาไทยตามบัตรประจำตัวประชาชน ส่วนชื่อตัวและชื่อรองของบุคคลต่างด้าวให้ใช้เป็นภาษาอังกฤษตามหนังสือเดินทางหรือเอกสารสำคัญประจำตัวอื่นที่หน่วยงานของรัฐออกให้
6.4	serialNumber	O	รหัสที่เชื่อมโยงไปยังเจ้าของใบรับรองเท่านั้น โดยมีรูปแบบดังต่อไปนี้ — เลขประจำตัวประชาชน (identity card number: IDC) ให้ใช้รูปแบบที่มีตัวอักษรนำหน้า “IDC” คั่นด้วยเครื่องหมาย “-” และตามด้วยเลขประจำตัวประชาชน 13 หลัก เช่น “IDC-1234567890123” — เลขที่หนังสือเดินทาง (passport number: PAS) ให้ใช้รูปแบบที่มีตัวอักษรนำหน้า “PAS” คั่นด้วยเครื่องหมาย “-” และตามด้วยเลขที่หนังสือเดินทาง ทั้งนี้ หากรหัสที่เชื่อมโยงไปยังเจ้าของใบรับรองเป็นข้อมูลส่วนบุคคล ผู้ใช้งานต้องคำนึงถึงข้อกำหนดในการใช้งานข้อมูลส่วนบุคคลที่เกี่ยวข้องด้วย
6.5	title	NU	-

Index	Item	Mandatory	Value
6.6	organizationalUnitName (ou)	NU	-
6.7	organizationName (o)	NU	-
6.8	organizationIdentifier	NU	-
6.9	localityName (l)	NU	-
6.10	stateOrProvinceName (st)	NU	-
6.11	countryName (c)	M	รหัสประเทศที่อยู่ของเจ้าของใบรับรองให้เป็นไปตาม ISO 3166-1 alpha-2 code เช่น “ประเทศไทย” ให้ใช้รหัส “TH” ทั้งนี้ countryName ให้ CA พิจารณาจากหลักฐานแสดงตนตามความเหมาะสม ตัวอย่างเช่น — หลักฐานแสดงตนเป็นบัตรประจำตัวประชาชน ให้ใช้ “TH” — หลักฐานแสดงตนเป็นหนังสือเดินทาง ให้ใช้รหัสประเทศของสัญชาติที่ระบุในหนังสือเดินทาง — ในกรณีบุคคลต่างด้าวมีทะเบียนบ้าน (ท.ร.13 หรือ ท.ร.14) เพื่อยืนยันว่าอยู่ในประเทศไทย ให้ใช้ “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 ของกุญแจสาธารณะที่เป็นคู่กับกุญแจส่วนตัวซึ่ง CA ใช้ลงลายมือชื่อดิจิทัลเพื่อรับรองใบรับรองนี้
9.	subjectKeyIdentifier	M	keyIdentifier บรรจุค่าของฟังก์ชัน SHA-1 Hash ของ subjectPublicKey ซึ่งอยู่ในฟิลด์ subjectPublicKeyInfo
10.	keyUsage	M	ค่าที่แสดงวัตถุประสงค์ของการใช้งาน 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	
11.2.1	PolicyQualifierInfo [1]	M	

Index	Item	Mandatory	Value
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 โดยใช้ชนิดข้อมูล ตาม 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	
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	
16.1	AccessDescription [1]	M	
16.1.1	accessMethod	M	หมายเลขโอไอดี (OID) ของเกณฑ์วิธีสำหรับตรวจสอบสถานะของการเพิกถอนใบรับรอง (OCSP) โดยมีรายละเอียดดังนี้ 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 สำหรับเข้าถึงรายการใบรับรองของ CA

4.2 ใบรับรองประเภทนิติบุคคล

ใบรับรองประเภทนิติบุคคล (juristic person certificate) มีรายละเอียดของข้อมูลในฟิลด์ต่าง ๆ เป็นไปตามตารางที่ 3

ตารางที่ 3 ข้อมูลในใบรับรองประเภทนิติบุคคล

Index	Item	Mandatory	Value
1.	version	M	2 (Version 3)
2.	serialNumber	M	ตัวเลขที่ไม่ซ้ำกันระหว่างใบรับรองภายใต้ผู้ให้บริการออกใบรับรอง (CA) รายเดียวกัน 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 CA ควรติดตามการอัปเดตอัลกอริทึมจากมาตรฐานที่เกี่ยวข้อง
4.	issuer	M	ข้อมูลในฟิลด์ issuer ทั้งหมด ให้ระบุโดยใช้การเข้ารหัสแบบ PrintableString เท่านั้น
4.1	commonName (cn)	M	ชื่อ CA และข้อมูลบ่งบอกถึงระบบบริการ เป็นภาษาอังกฤษ เช่น “XYZ Certification Authority - G1”
4.2	organizationalUnitName (ou)	O	ชื่อหน่วยงานย่อยในองค์กรของ CA เป็นภาษาอังกฤษ เช่น “XYZ Certification Authority”
4.3	organizationName (o)	M	ชื่อ CA ตามที่จดทะเบียนกับกรมพัฒนาธุรกิจการค้าหรือที่ระบุในเอกสารสำคัญอื่น เป็นภาษาอังกฤษ เช่น “XYZ Company Limited”

Index	Item	Mandatory	Value
4.4	countryName (c)	M	รหัสประเทศที่ตั้งของ CA ให้เป็นไปตาม ISO 3166-1 alpha-2 code เช่น “ประเทศไทย” ให้ใช้รหัส “TH”
4.5	organizationIdentifier	O	รหัสที่เชื่อมโยงไปยัง CA ที่ออกใบรับรองนี้เท่านั้น ตัวอย่างเช่น CA ที่มีเลขประจำตัวผู้เสียภาษีอากร (tax identification number: TIN) ให้ใช้รูปแบบที่มีตัวอักษรนำหน้า “TIN” คั่นด้วยเครื่องหมาย “-” และตามด้วยเลขประจำตัวผู้เสียภาษีอากร 13 หลัก เช่น “TIN-1234567890123”
5.	validity	M	
5.1	notBefore	M	วันและเวลาที่ใบรับรองเริ่มใช้งานได้
5.2	notAfter	M	วันและเวลาที่ใบรับรองสิ้นสุดการใช้งาน
6.	subject	M	— ข้อมูล serialNumber และ countryName ในฟิลด์ subject ใช้การเข้ารหัสแบบ PrintableString เท่านั้น — ข้อมูลอื่นในฟิลด์ subject สามารถใช้การเข้ารหัสแบบ PrintableString หรือ UTF8String
6.1	commonName (cn)	M	ชื่อทั่วไปของนิติบุคคลซึ่งเป็นเจ้าของใบรับรอง ให้เป็นภาษาไทยหรือภาษาอังกฤษก็ได้ โดย CA ต้องไม่ระบุเพียงอักษรย่อของนิติบุคคลหรือชื่อหน่วยงานย่อยของนิติบุคคลเพียงอย่างเดียว เนื่องจากอักษรย่อหรือชื่อหน่วยงานย่อยอาจทำให้เข้าใจผิดว่าเป็นนิติบุคคลอื่นหรือละเมิดทรัพย์สินทางปัญญาของบุคคลอื่น ทั้งนี้ สามารถระบุ commonName (cn) ได้ในรูปแบบดังต่อไปนี้ — ระบุชื่อนิติบุคคล ตามที่จดทะเบียนกับกรมพัฒนาธุรกิจการค้าหรือที่ระบุในเอกสารสำคัญอื่น เช่น “บริษัท ทดสอบ เซอร์วิส จำกัด” หรือ “Todsob Service Company Limited” — ระบุชื่อนิติบุคคล ตามที่จดทะเบียนกับกรมพัฒนาธุรกิจการค้าหรือที่ระบุในเอกสารสำคัญอื่น ตามด้วยอักษรย่อในรูปแบบ “ชื่อนิติบุคคล (อักษรย่อ)” เช่น “บริษัท ทดสอบเซอร์วิส จำกัด (ท.ซ.)” หรือ“Todsob Service Company Limited (T.S.)” — ระบุชื่อนิติบุคคล ตามที่จดทะเบียนกับกรมพัฒนาธุรกิจการค้าหรือที่ระบุในเอกสารสำคัญอื่น ตามด้วยระบุชื่อหน่วยงานย่อยของนิติบุคคล ในรูปแบบ “ชื่อนิติบุคคล (ชื่อหน่วยงานย่อยของนิติบุคคล)” เช่น “มหาวิทยาลัยทดสอบ (คณะแพทยศาสตร์)” หรือ “Todsob University (Faculty of Medicine)”

Index	Item	Mandatory	Value
			— ระบุชื่อนิติบุคคล ตามที่จดทะเบียนกับกรมพัฒนาธุรกิจการค้าหรือที่ระบุในเอกสารสำคัญอื่น ตามด้วยวัตถุประสงค์การใช้งาน ในรูปแบบ “ชื่อนิติบุคคล (วัตถุประสงค์การใช้งาน)” เช่น “บริษัท ทดสอบเซอร์วิส จำกัด (สำหรับธุรกรรมภาษี)” หรือ “Todsob Service Company Limited (for tax transactions)”
6.2	givenName	NU	-
6.3	surname (sn)	NU	-
6.4	serialNumber	NU	-
6.5	title	NU	-
6.6	organizationalUnitName (ou)	O	ชื่อของหน่วยงานย่อยของนิติบุคคลที่สอดคล้องกับเจ้าของใบรับรอง โดยเป็นภาษาไทยหรือภาษาอังกฤษก็ได้ เช่น “คณะแพทยศาสตร์” หรือ “Faculty of Medicine”
6.7	organizationName (o)	M	ชื่อนิติบุคคล ตามที่จดทะเบียนกับกรมพัฒนาธุรกิจการค้าหรือที่ระบุในเอกสารสำคัญอื่น โดยเป็นภาษาไทยหรือภาษาอังกฤษก็ได้ เช่น “บริษัท ทดสอบเซอร์วิส จำกัด” หรือ “Todsob Service Company Limited”
6.8	organizationIdentifier	M	รหัสที่เชื่อมโยงไปยังนิติบุคคลที่เป็นเจ้าของใบรับรองเท่านั้น โดยมีรูปแบบดังต่อไปนี้ — หน่วยงานที่มีเลขประจำตัวผู้เสียภาษีอากร (tax identification number: TIN) ให้ใช้รูปแบบที่มีตัวอักษรนำหน้า “TIN” คั่นด้วยเครื่องหมาย “-” และตามด้วยเลขประจำตัวผู้เสียภาษีอากร 13 หลัก เช่น “TIN-1234567890123” ทั้งนี้ อาจระบุด้วยรหัสอื่นที่เฉพาะเจาะจงตามประเภทหน่วยงาน เช่น — หน่วยงานบริการสุขภาพภาคเอกชนที่มีเลขที่ใบอนุญาตให้ประกอบกิจการสถานพยาบาล (license number: LIN) ให้ใช้รูปแบบที่มีตัวอักษรนำหน้า “LIN” คั่นด้วยเครื่องหมาย “-” และตามด้วยหมายเลขใบอนุญาต 11 หลัก เช่น “LIN-12345678901” — หน่วยงานบริการสุขภาพภาครัฐที่มีรหัสหน่วยงานบริการสุขภาพ (hospital code: HOC) ให้ใช้รูปแบบที่มีตัวอักษรนำหน้า “HOC” คั่นด้วยเครื่องหมาย “-” และตามด้วยรหัสหน่วยงานบริการสุขภาพ 9 หลัก เช่น “HOC-123456789” — หน่วยงานภาครัฐที่มีรหัสองค์กรปกครองท้องถิ่น (code of local administration: CLA) ให้ใช้รูปแบบที่มีตัวอักษรนำหน้า “CLA” คั่นด้วยเครื่องหมาย “-” และตามด้วยรหัสองค์กรปกครองท้องถิ่น 8 หลัก เช่น “CLA-12345678”

Index	Item	Mandatory	Value
6.9	localityName (l)	O	รหัสอำเภอหรือเขตที่ตั้งของนิติบุคคลให้เป็นไปตามรหัสของกรมการปกครอง ซึ่งเป็นเลข 4 หลัก เช่น “หลักสี่” ให้ใช้ “1041”
6.10	stateOrProvinceName (st)	O	รหัสจังหวัดที่ตั้งของนิติบุคคลให้เป็นไปตาม ISO 3166-2 code (ดูได้จาก https://www.iso.org/obp/ui/en/#iso:code:3166:TH) เช่น “กรุงเทพ” ให้ใช้ “TH-10”
6.11	countryName (c)	M	รหัสประเทศที่ตั้งของนิติบุคคลให้เป็นไปตาม 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 ของกุญแจสาธารณะที่เป็นคู่กับกุญแจส่วนตัวซึ่ง CA ใช้ลงลายมือชื่อดิจิทัลเพื่อรับรองใบรับรองนี้
9.	subjectKeyIdentifier	M	keyIdentifier บรรจุค่าของฟังก์ชัน SHA-1 Hash ของ subjectPublicKey ซึ่งอยู่ในฟิลด์ subjectPublicKeyInfo
10.	keyUsage	M	ค่าที่แสดงวัตถุประสงค์ของการใช้งาน ทั้งนี้ สำหรับการใช้งานทั่วไปแนะนำให้ตั้งค่า ดังนี้ (3) สำหรับการลงลายมือชื่อดิจิทัล ให้ตั้งค่าบิต digitalSignature = 1 และ contentCommitment = 1 (4) สำหรับการเข้ารหัสลับ ให้ตั้งค่าบิต keyEncipherment = 1 และ/หรือ dataEncipherment = 1
11.	certificatePolicies	M	
11.1	policyIdentifier	M	หมายเลขโอไอดี (OID) ของ certificate policy
11.2	policyQualifiers	M	
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	

Index	Item	Mandatory	Value
12.1	directoryName	O	ข้อมูลเกี่ยวกับเจ้าของใบรับรอง โดยใช้ชนิดข้อมูล ตาม ITU-T X.501 “Name”
12.2	rfc822Name	O	อีเมลของนิติบุคคล
13.	basicConstraints	M	
13.1	cA	M	False
13.2	pathLenConstraint	NU	-
14.	extKeyUsage	O	ใช้เมื่อซอฟต์แวร์ที่ใช้ใบรับรองต้องการใช้ค่าในฟิลด์นี้เท่านั้น
15.	cRLDistributionPoints	M	
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	
16.1	AccessDescription [1]	M	
16.1.1	accessMethod	M	หมายเลขโอไอดี (OID) ของเกณฑ์วิธีสำหรับตรวจสอบสถานะของการเพิกถอนใบรับรอง (OCSP) โดยมีรายละเอียดดังนี้ 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 สำหรับเข้าถึงรายการใบรับรองของ CA

4.3 ใบรับรองประเภทเจ้าหน้าที่นิติบุคคล

ใบรับรองประเภทเจ้าหน้าที่นิติบุคคล (enterprise user certificate) มีรายละเอียดของข้อมูลในฟิลด์ต่าง ๆ เป็นไปตามตารางที่ 4

ตารางที่ 4 ข้อมูลในใบรับรองประเภทเจ้าหน้าที่นิติบุคคล

Index	Item	Mandatory	Value
1.	version	M	2 (Version 3)
2.	serialNumber	M	ตัวเลขที่ไม่ซ้ำกันระหว่างใบรับรองภายใต้ผู้ให้บริการออกใบรับรอง (CA) รายเดียวกัน โดยเป็นตัวเลขแบบสุ่มและไม่เรียงกันเมื่อเทียบกับใบรับรองที่ออกก่อนหน้าและต่อจากใบนี้ (randomized and non-sequential) ทั้งนี้ จะต้องมีค่ามากกว่า 0 และขนาดไม่น้อยกว่า 64 บิต [5]
3.	signature	M	หมายเลขโอไอดี (OID) ของอัลกอริทึมจากตัวเลือกดังนี้

Index	Item	Mandatory	Value
			– {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 CA ควรติดตามการอัปเดตอัลกอริทึมจากมาตรฐานที่เกี่ยวข้อง
4.	issuer	M	ข้อมูลในฟิลด์ issuer ทั้งหมด ให้ระบุโดยใช้การเข้ารหัสแบบ PrintableString เท่านั้น
4.1	commonName (cn)	M	ชื่อ CA และข้อมูลบ่งบอกถึงระบบบริการ เป็นภาษาอังกฤษ เช่น “XYZ Certification Authority - G1”
4.2	organizationalUnitName (ou)	O	ชื่อหน่วยงานย่อยในองค์กรของ CA เป็นภาษาอังกฤษ เช่น “XYZ Certification Authority”
4.3	organizationName (o)	M	ชื่อ CA ตามที่จดทะเบียนกับกรมพัฒนาธุรกิจการค้าหรือที่ระบุในเอกสารสำคัญอื่น เป็นภาษาอังกฤษ เช่น “XYZ Company Limited”
4.4	countryName (c)	M	รหัสประเทศที่ตั้งของ CA ให้เป็นไปตาม ISO 3166-1 alpha-2 code เช่น “ประเทศไทย” ให้ใช้รหัส “TH”
4.5	organizationIdentifier	O	รหัสที่เชื่อมโยงไปยัง CA ที่ออกใบรับรองนี้เท่านั้น ตัวอย่างเช่น CA ที่มีเลขประจำตัวผู้เสียภาษีอากร (tax identification number: TIN) ให้ใช้รูปแบบที่มีตัวอักษรนำหน้า “TIN” คั่นด้วยเครื่องหมาย “-” และตามด้วยเลขประจำตัวผู้เสียภาษีอากร 13 หลัก เช่น “TIN-1234567890123”
5.	validity	M	
5.1	notBefore	M	วันและเวลาที่ใบรับรองเริ่มใช้งานได้
5.2	notAfter	M	วันและเวลาที่ใบรับรองสิ้นสุดการใช้งาน
6.	subject	M	– ข้อมูล serialNumber และ countryName ในฟิลด์ subject ใช้การเข้ารหัสแบบ PrintableString เท่านั้น – ข้อมูลอื่นในฟิลด์ subject สามารถใช้การเข้ารหัสแบบ PrintableString หรือ UTF8String

Index	Item	Mandatory	Value
6.1	commonName (cn)	M	ชื่อตัว ชื่อรอง (ถ้ามี) ชื่อสกุล ให้ระบุตามหลักฐานแสดงตน เช่น บัตรประจำตัวประชาชน หรือหนังสือเดินทาง ซึ่งสามารถมีรูปแบบได้ดังนี้ — ระบุ “ชื่อตัว ชื่อรอง (ถ้ามี) ชื่อสกุล” เป็นอักษรภาษาหลักที่ไม่ใช่อักษรภาษาอังกฤษ คั่นด้วย “/” และตามด้วย “ชื่อตัว ชื่อรอง (ถ้ามี) ชื่อสกุล” เป็นอักษรภาษาอังกฤษ เช่น “สมชาย รักดี/Somchai Rakdee” — ระบุ “ชื่อตัว ชื่อรอง (ถ้ามี) ชื่อสกุล” เป็นอักษรภาษาอังกฤษ เช่น “Somchai Rakdee” ทั้งนี้ CA อาจพิจารณาใส่คำนำหน้าชื่อด้วยก็ได้ตามความเหมาะสม
6.2	givenName	M	ชื่อตัว ชื่อรอง (ถ้ามี) ให้ระบุตามหลักฐานแสดงตน เช่น บัตรประจำตัวประชาชน หรือหนังสือเดินทาง ในรูปแบบ “ชื่อตัว ชื่อรอง (ถ้ามี)” โดยเป็นภาษาไทยหรือภาษาอังกฤษก็ได้ เช่น “สมชาย” หรือ “Somchai” ทั้งนี้ ชื่อตัวของบุคคลสัญชาติไทยควรใช้เป็นภาษาไทยตามบัตรประจำตัวประชาชน ในขณะเดียวกันชื่อตัวของบุคคลต่างด้าวให้ใช้เป็นภาษาอังกฤษตามหนังสือเดินทางหรือเอกสารสำคัญประจำตัวอื่นที่หน่วยงานของรัฐออกให้
6.3	surname (sn)	M	ชื่อสกุล ให้ระบุตามหลักฐานแสดงตน เช่น บัตรประจำตัวประชาชน หรือหนังสือเดินทาง ในรูปแบบ “ชื่อสกุล” โดยเป็นภาษาไทยหรือภาษาอังกฤษก็ได้ เช่น “รักดี” หรือ “Rakdee” ทั้งนี้ ชื่อสกุล ของบุคคลสัญชาติไทยควรใช้เป็นภาษาไทยตามบัตรประจำตัวประชาชน ส่วนชื่อตัวและชื่อรองของบุคคลต่างด้าวให้ใช้เป็นภาษาอังกฤษตามหนังสือเดินทางหรือเอกสารสำคัญประจำตัวอื่นที่หน่วยงานของรัฐออกให้
6.4	serialNumber	O	รหัสที่เชื่อมโยงไปยังเจ้าของใบรับรองเท่านั้น โดยมีรูปแบบดังต่อไปนี้ — เลขประจำตัวประชาชน (identity card number: IDC) ให้ใช้รูปแบบที่มีตัวอักษรนำหน้า “IDC” คั่นด้วยเครื่องหมาย “-” และตามด้วยเลขประจำตัวประชาชน 13 หลัก เช่น “IDC-1234567890123” — เลขที่หนังสือเดินทาง (passport number: PAS) ให้ใช้รูปแบบที่มีตัวอักษรนำหน้า “PAS” คั่นด้วยเครื่องหมาย “-” และตามด้วยเลขที่หนังสือเดินทาง ทั้งนี้ หากรหัสที่เชื่อมโยงไปยังเจ้าของใบรับรองเป็นข้อมูลส่วนบุคคล ผู้ใช้งานต้องคำนึงถึงข้อกำหนดในการใช้งานข้อมูลส่วนบุคคลที่เกี่ยวข้องด้วย

Index	Item	Mandatory	Value
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 โดยเป็นชื่อตามที่จดทะเบียนกับกรมพัฒนาธุรกิจการค้าหรือที่ระบุในเอกสารสำคัญอื่น โดยเป็นภาษาไทยหรือภาษาอังกฤษก็ได้ เช่น “บริษัท ทดสอบ เซอร์วิส จำกัด” หรือ “Todsob Service Company Limited”
6.8	organizationIdentifier	M	รหัสที่เชื่อมโยงไปยังนิติบุคคลที่เจ้าของใบรับรองสังกัดเท่านั้น โดยมีรูปแบบดังต่อไปนี้ — หน่วยงานที่มีเลขประจำตัวผู้เสียภาษีอากร (tax identification number: TIN) ให้ใช้รูปแบบที่มีตัวอักษรนำหน้า “TIN” คั่นด้วยเครื่องหมาย “-” และตามด้วยเลขประจำตัวผู้เสียภาษีอากร 13 หลัก เช่น “TIN-1234567890123” ทั้งนี้ อาจระบุด้วยรหัสอื่นที่เฉพาะเจาะจงตามประเภทหน่วยงาน เช่น — หน่วยงานบริการสุขภาพภาคเอกชนที่มีเลขที่ใบอนุญาตให้ประกอบกิจการสถานพยาบาล (license number: LIN) ให้ใช้รูปแบบที่มีตัวอักษรนำหน้า “LIN” คั่นด้วยเครื่องหมาย “-” และตามด้วยหมายเลขใบอนุญาต 11 หลัก เช่น “LIN-12345678901” — หน่วยงานบริการสุขภาพภาครัฐที่มีรหัสหน่วยงานบริการสุขภาพ (hospital code: HOC) ให้ใช้รูปแบบที่มีตัวอักษรนำหน้า “HOC” คั่นด้วยเครื่องหมาย “-” และตามด้วยรหัสหน่วยงานบริการสุขภาพ 9 หลัก เช่น “HOC-123456789” — หน่วยงานภาครัฐที่มีรหัสองค์กรปกครองท้องถิ่น (code of local administration: CLA) ให้ใช้รูปแบบที่มีตัวอักษรนำหน้า “CLA” คั่นด้วยเครื่องหมาย “-” และตามด้วยรหัสองค์กรปกครองท้องถิ่น 8 หลัก เช่น “CLA-12345678”
6.9	localityName (l)	O	รหัสอำเภอหรือเขตที่ตั้งของนิติบุคคลให้เป็นไปตามรหัสของกรมการปกครอง ซึ่งเป็นเลข 4 หลัก เช่น “หลักสี่” ให้ใช้ “1041”
6.10	stateOrProvinceName (st)	O	รหัสจังหวัดที่ตั้งของนิติบุคคลให้เป็นไปตาม ISO 3166-2 code (ดูได้จาก https://www.iso.org/obp/ui/en/#iso:code:3166:TH) เช่น “กรุงเทพ” ให้ใช้ “TH-10”
6.11	countryName (c)	M	รหัสประเทศที่ตั้งของนิติบุคคลให้เป็นไปตาม ISO 3166-1 alpha-2 code เช่น “ประเทศไทย” ให้ใช้รหัส “TH”
7.	subjectPublicKeyInfo	M	

Index	Item	Mandatory	Value
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 ของกุญแจสาธารณะที่เป็นคู่กับกุญแจส่วนตัวซึ่ง CA ใช้ลงลายมือชื่อดิจิทัลเพื่อรับรองใบรับรองนี้
9.	subjectKeyIdentifier	M	keyIdentifier บรรจุค่าของฟังก์ชัน SHA-1 Hash ของ subjectPublicKey ซึ่งอยู่ในฟิลด์ subjectPublicKeyInfo
10.	keyUsage	M	ค่าที่แสดงวัตถุประสงค์ของการใช้งาน 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	
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	
13.1	cA	M	False
13.2	pathLenConstraint	NU	-
14.	extKeyUsage	O	ใช้เมื่อซอฟต์แวร์ที่ใช้ใบรับรองต้องการใช้ค่าในฟิลด์นี้เท่านั้น

Index	Item	Mandatory	Value
15.	cRLDistributionPoints	M	
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	
16.1	AccessDescription [1]	M	
16.1.1	accessMethod	M	หมายเลขโอไอดี (OID) ของเกณฑ์วิธีสำหรับตรวจสอบสถานะของการเพิกถอนใบรับรอง (OCSP) โดยมีรายละเอียดดังนี้ 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 สำหรับเข้าถึงรายการใบรับรองของ CA

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 ข้อเสนอแนะมาตรฐานฯ ฉบับนี้ กำหนดหมายเลขโอไอดี (OID) ของ CP แต่ละประเภทใบรับรอง ดังนี้[1]

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

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

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 users

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

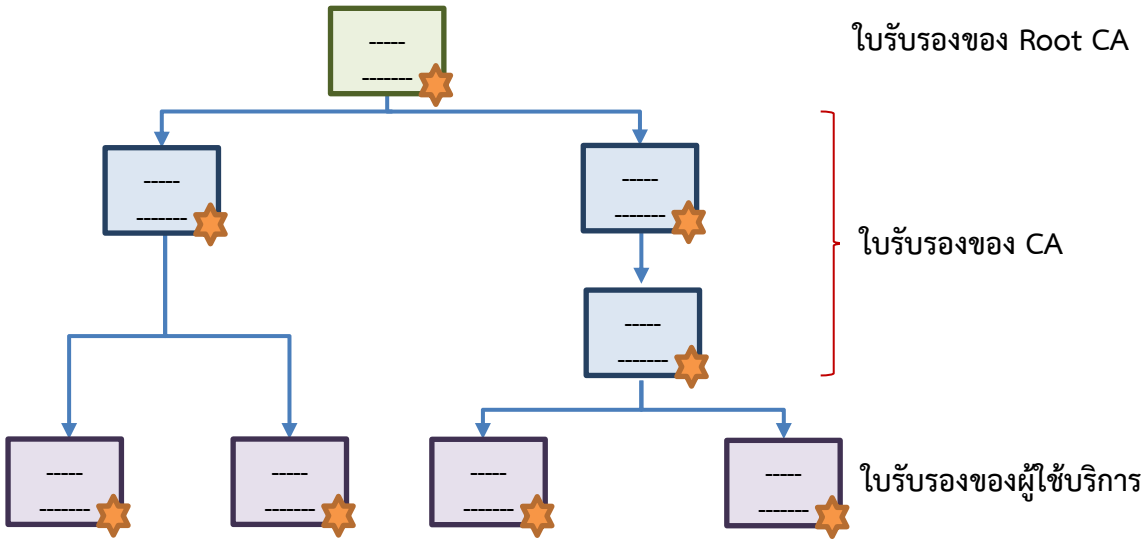
ภาคผนวก ก.
ตัวย่อ หมายเลขโอไอดี (OID) และความจำเป็นของคุณลักษณะภายใต้ฟิลด์ subject

ตัวย่อ (descriptor) และหมายเลขโอไอดี (OID) ของคุณลักษณะภายใต้ฟิลด์ **subject** ซึ่งอ้างอิงจาก RFC 4519 [6] และ ITU-T X.520 [7] 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

ภาคผนวก ข.
โครงสร้างความสัมพันธ์ของใบรับรองในประเทศไทย

ใบรับรองภายใต้ผู้ให้บริการออกใบรับรองในประเทศไทยสามารถแบ่งระดับตามความสัมพันธ์ระหว่างผู้ให้บริการออกใบรับรองและผู้ใช้บริการเป็นไปตามรูปที่ 1 โดยมีรายละเอียดดังนี้



รูปที่ 1 โครงสร้างความสัมพันธ์ของใบรับรองในประเทศไทย

(1) ใบรับรองของผู้ให้บริการออกใบรับรองลำดับชั้นบนสุด (Root CA certificate)

ใบรับรองของผู้ให้บริการออกใบรับรองลำดับชั้นบนสุด คือ ใบรับรองของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์แห่งชาติ (National Root CA: NRCA) โดย NRCA จะลงลายมือชื่อในใบรับรองของตนเพื่อรับรองตนเอง (self-signed)

ทั้งนี้ NRCA มีหน้าที่ออกใบรับรองให้กับผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา (Subordinate CA หรือ CA) และมีหน้าที่กำหนดแนวนโยบาย (CP) ของผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา

(2) ใบรับรองของผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา (Subordinate CA certificate)

ใบรับรองของผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา คือ ใบรับรองของ CA ที่ออกโดยผู้ให้บริการออกใบรับรองลำดับชั้นบนสุดหรือผู้ให้บริการออกใบรับรองอื่น

(3) ใบรับรองของผู้ใช้บริการ (Subscriber certificate)

ใบรับรองของผู้ใช้บริการ คือ ใบรับรองที่ออกโดย CA เพื่อรับรองข้อมูลตัวตนและความเป็นเจ้าของคู่กุญแจของเอนทิตีที่เป็นผู้ใช้บริการ โดยใบรับรองของผู้ใช้บริการสามารถใช้งานได้ตามวัตถุประสงค์ที่กำหนดในใบรับรอง เช่น การยืนยันตัวตน (authentication) การเข้ารหัสลับ (encryption) และการตรวจสอบลายมือชื่อดิจิทัล (digital signature verification)

บรรณานุกรม

[1] 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.

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

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

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

[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] A. Sciberras, Ed., “IETF RFC 4519 (2006), Lightweight Directory Access Protocol (LDAP): Schema for User Applications” IETF, June 2006. [ออนไลน์]. Available: https://datatracker.ietf.org/doc/html/rfc4519#page-9.

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

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

[9] 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.

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

[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.

[13] European Telecommunications Standards Institute, "EN 319412-2 V2.2.1: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons", July 2020.