ยกเลิกการใช้งานข้อเสนอแนะมาตรฐานฯ ฉบับนี้

ข้อเสนอแนะมาตรฐานฯ ที่ประกาศยกเลิก

เลขที่	ขมธอ. 15-2560 เวอร์ชัน 1.0
ชื่อเอกสาร	การกำหนดข้อมูลในใบรับรองและรายการเพิกถอนใบรับรอง (Certificate and Certificate Revocation List (CRL) Profile)
วันที่ประกาศใช้	15 สิงหาคม พ.ศ. 2560
วันที่ประกาศยกเลิก	4 ตุลาคม พ.ศ. 2566

ข้อเสนอแนะมาตรฐานฯ ที่ประกาศใช้แทนฉบับเดิม

เลขที่	ขมธอ. 15-2566 เวอร์ชัน 2.0
ชื่อเอกสาร	ข้อมูลในใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ (Subscriber Certificate Profile)
วันที่ประกาศใช้	4 ตุลาคม พ.ศ. 2566

ETDA สพธอ
www.etda.or.th

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ETDA Recommendation on ICT Standard for Electronic Transactions

ขมธอ. 15-2560

ว่าด้วยการกำหนดข้อมูลในใบรับรองและรายการเพิกถอนใบรับรอง

CERTIFICATE AND CERTIFICATE REVOCATION LIST (CRL) PROFILE

เวอร์ชั่น 1.0

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ICS 35.100.70

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการกำหนดข้อมูลในใบรับรองและรายการเพิกถอนใบรับรอง

ขมธอ. 15-2560

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 21
เลขที่ 33/4 ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
หมายเลขโทรศัพท์: 0 2123 1234 หมายเลขโทรสาร: 0 2123 1200

ประกาศโดย
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

วันที่ 15 สิงหาคม พ.ศ. 2560

คณะทำงานจัดทำร่างข้อเสนอแนะเกี่ยวกับการจัดทำหรือแปลงเอกสารและข้อความ
ให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

ประธานคณะทำงาน

นายศุภโชค จันทรประทิน	รักษาการผู้อำนวยการสำนักมาตรฐาน สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ผู้ทำงาน

นายกำชัย จัตตานนท์	ผู้แทนกรมศุลกากร
นางสาวขนิษฐา สหเมธาพัฒน์	ผู้แทนกรมสรรพากร
นายธานินทร์ ตันกิติบุตร	ผู้แทนบริษัท ไทยเทรดเน็ต จำกัด
นายธิติกร ตระกูลศิริศักดิ์	ผู้แทนสำนักบริการโครงสร้างพื้นฐาน สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
นายณธรรม ธรรมาณิชานนท์	ผู้แทนสำนักพัฒนาธุรกิจ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ผู้ทำงานและเลขานุการ

นายเฉลิมชัย บวรนันท์	ผู้แทนสำนักมาตรฐาน สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

วิเคราะห์และจัดทำข้อเสนอแนะมาตรฐานฯ
ว่าด้วยการกำหนดข้อมูลในใบรับรองและรายการเพิกถอนใบรับรอง

นายโสพส พานิชปรีชา	ที่ปรึกษา สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
นายนครินทร์ ลิ้มรังษี	สำนักมาตรฐาน สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
นายธวัชชัย พริ้งพร้อม	สำนักสารสนเทศ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการกำหนดข้อมูลในใบรับรองและรายการเพิกถอนใบรับรองฉบับนี้ จัดทำขึ้นเพื่อเป็นแนวทางการกำหนดข้อมูลในใบรับรองสำหรับผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา (Subordinate CA) ใบรับรองสำหรับผู้ใช้บริการ และรายการเพิกถอนใบรับรอง ซึ่งจะช่วยให้รูปแบบของใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรองรายต่าง ๆ มีความสอดคล้องกันและเป็นไปตามมาตรฐานสากล ข้อเสนอแนะมาตรฐานฉบับนี้อ้างอิงเอกสารและมาตรฐานดังต่อไปนี้

1. IETF RFC 5280 (2008), Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
2. Recommendation ITU-T X.509 (2016) | ISO/IEC 9594-8 : 2017, Information Technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks
3. Recommendation ITU-T X.520 (2012) | ISO/IEC 9594-6 : 2014, Information Technology - Open Systems Interconnection – The Directory: Selected attribute types
4. Recommendation ITU-T X.680 (2015) | ISO/IEC 8824-1 : 2015, Information Technology - Abstract Syntax Notation One (ASN.1) : Specification of basic notation
5. Baseline Requirement Certificate Policy for the Issuance and Management of Publicly - Trusted Certificates, Version 1.4.2

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการกำหนดข้อมูลในใบรับรองและรายการเพิกถอนใบรับรองฉบับนี้ จัดทำขึ้นตามความร่วมมือด้านมาตรฐานระหว่าง สำนักมาตรฐาน และสำนักบริการโครงสร้างพื้นฐาน ภายใต้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 21 เลขที่ 33/4 ถนนพระราม 9
แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
โทรศัพท์: 0 2123 1234 โทรสาร: 0 2123 1200
E-mail: estandard.center@etda.or.th, www.etda.or.th

คำนำ

ใบรับรองเป็นส่วนประกอบสำคัญสำหรับการตรวจสอบลายมือชื่อดิจิทัล โดยในใบรับรองบันทึกข้อมูลอิเล็กทรอนิกส์ซึ่งยืนยันความเชื่อมโยงระหว่างเจ้าของลายมือชื่อกับข้อมูลสำหรับใช้สร้างลายมือชื่อดิจิทัล ในปัจจุบันผู้ให้บริการออกใบรับรองในประเทศไทยบางรายออกใบรับรองที่ไม่เหมาะสม เช่น กำหนดข้อมูลเจ้าของใบรับรองไม่ตรงตามนิยามของคุณลักษณะ (Attribute) ใช้งานคู่กุญแจที่มีขนาดไม่เหมาะสม และใช้อัลกอริทึมที่ไม่เหมาะสมกับการใช้งานในปัจจุบัน เป็นต้น ซึ่งใบรับรองที่ไม่เหมาะสมนี้อาจก่อให้เกิดปัญหากับการใช้ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้

เพื่อแก้ไขปัญหาการออกใบรับรองที่ไม่เหมาะสม สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. ในฐานะหน่วยงานที่ได้รับมอบหมายจากรัฐบาลให้เป็นผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์แห่งชาติ (Thailand National Root Certification Authority) ได้จัดทำข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยการกำหนดข้อมูลในใบรับรองและรายการเพิกถอนใบรับรองฉบับนี้ขึ้น เพื่อกำหนดประเภทของใบรับรอง ฟิลด์และข้อมูลที่จำเป็นต้องระบุในใบรับรองและรายการเพิกถอนใบรับรอง ทั้งนี้ เพื่อให้การใช้งานใบรับรองมีความสอดคล้องกันระหว่างผู้ที่เกี่ยวข้องและเป็นไปตามมาตรฐานสากล

สารบัญ

สารบัญรูป

หน้า

สารบัญตาราง

หน้า

ETDA
สพธอ
www.etda.or.th

ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
เรื่อง ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์
ว่าด้วยการกำหนดข้อมูลในใบรับรองและรายการเพิกถอนใบรับรอง

เพื่อเป็นข้อเสนอแนะสำหรับการกำหนดข้อมูลที่เหมาะสมในใบรับรองในประเทศไทยให้มีรูปแบบเป็นมาตฐานกลางเดียวกัน และเพื่อสนับสนุนการใช้ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ตามมาตรา ๒๖ แห่งกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

อาศัยอำนาจตามความในมาตรา ๗ (๔) แห่งพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ. ๒๕๕๔ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) จึงประกาศข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการกำหนดข้อมูลในใบรับรองและรายการเพิกถอนใบรับรอง เลขที่ ขมธอ. ๑๕ – ๒๕๖๐ ปรากฏตามท้ายประกาศฉบับนี้

ประกาศ ณ วันที่ ๑๕ สิงหาคม ๒๕๖๐

(นางสุรางคณา วายุภาพ)
ผู้อำนวยการ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ว่าด้วยการกำหนดข้อมูลในใบรับรอง และรายการเพิกถอนใบรับรอง

1. ขอบข่าย

ข้อเสนอแนะมาตรฐานฯ ฉบับนี้นำเสนอแนวทางการกำหนดข้อมูลในใบรับรอง และรายการเพิกถอนใบรับรอง ประเภท X.509 เพื่อสนับสนุนการใช้งานลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ โดยครอบคลุมเนื้อหา ดังนี้

(1) รายละเอียดข้อมูลในแต่ละฟิลด์ของใบรับรอง และรายการเพิกถอนใบรับรอง

(2) การกำหนดข้อมูลในใบรับรองของผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา ชั้นที่ 1 และ 2

(3) การกำหนดข้อมูลในใบรับรองของผู้ใช้บริการ ซึ่งแบ่งออกเป็น 4 ประเภท ได้แก่

(3.1) ใบรับรองสำหรับบุคคลธรรมดา

(3.2) ใบรับรองสำหรับนิติบุคคล

(3.3) ใบรับรองสำหรับลงลายมือชื่อดิจิทัลโดยระบบให้บริการ

(3.4) ใบรับรองสำหรับโปรโตคอล SSL/TLS หรือโปรโตคอลอื่น ๆ

(4) การกำหนดข้อมูลในรายการเพิกถอนใบรับรอง

2. บทนิยาม

คำนิยามและคำย่อเพื่อกำหนดความหมายให้กับคำที่ใช้ในเอกสารนี้เข้าใจได้ถูกต้องตรงกัน

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 หมายถึง ลายมือชื่ออิเล็กทรอนิกส์ประเภทหนึ่งที่ใช้รับรองตัวตนของเอนทิตี ด้วยการประยุกต์ใช้เทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure : PKI) [1]

2.5 ใบรับรอง (Certificate) หมายถึง ข้อมูลอิเล็กทรอนิกส์หรือการบันทึกอื่นใดซึ่งยืนยันความเชื่อมโยงระหว่างเจ้าของลายมือชื่อกับข้อมูลสำหรับใช้สร้างลายมือชื่อดิจิทัล [2]

2.6 รายการเพิกถอนใบรับรอง (Certificate Revocation List : CRL) หมายถึง รายการใบรับรองที่ถูกเพิกถอนการใช้งาน [1]

2.7 ผู้ให้บริการออกใบรับรอง (Certification Authority : CA) หมายถึง เอนทิตีที่รับรองกุญแจสาธารณะให้กับผู้ใช้บริการโดยการออกใบรับรองให้กับผู้ใช้บริการ และยังมีหน้าที่บริหารจัดการใบรับรองของผู้ใช้บริการ เช่น เผยแพร่ใบรับรอง เพิกถอนใบรับรอง และเผยแพร่ข้อมูลสำหรับตรวจสอบสถานะใบรับรอง

2.8 เจ้าของใบรับรอง หมายถึง เอนทิตีซึ่งถือข้อมูลสำหรับใช้สร้างลายมือชื่อดิจิทัลและสร้างลายมือชื่อดิจิทัลนั้นในนามตนเองหรือแทนบุคคลอื่น

2.9 ผู้ใช้บริการ (Subscriber) หมายถึง บุคคล หรือเอนทิตีใด ๆ ที่ได้รับใบรับรองจากผู้ให้บริการออกใบรับรอง

2.10 โปรโตคอลตรวจสอบสถานะของใบรับรอง (Online Certificate Status Protocol : OCSP) หมายถึง โปรโตคอลสำหรับตรวจสอบสถานะของใบรับรองว่าใบรับรองถูกเพิกถอนหรือไม่

2.11 Object Identifier (OID) หมายถึง ค่าสัมพันธ์ซึ่งบ่งบอกถึงข้อมูลสารสนเทศของวัตถุ (Information Object) ใด ๆ โดยเป็นค่าที่สามารถบ่งชี้ได้ถึงความเป็นหนึ่งเดียวของ Object นั้น ๆ [1]

2.12 กุญแจสาธารณะ (Public Key) หมายถึง กุญแจที่ใช้ตรวจสอบลายมือชื่อดิจิทัล และสามารถนำไปใช้เข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ เพื่อมิให้สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ที่มีการเข้ารหัสลับนั้นได้ เพื่อประโยชน์ในการรักษาความลับของข้อมูลอิเล็กทรอนิกส์นั้น [1]

2.13 กุญแจส่วนตัว (Private Key) หมายถึง กุญแจที่ใช้สร้างลายมือชื่อดิจิทัล และสามารถนำไปใช้ในการถอดรหัสลับเมื่อมีการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ เพื่อให้สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ที่มีการเข้ารหัสลับนั้นได้ [1]

2.14 คู่กุญแจ (Key Pair) หมายถึง กุญแจส่วนตัวและกุญแจสาธารณะในระบบการเข้ารหัสลับแบบอสมมาตรที่สร้างขึ้นโดยวิธีการที่ทำให้กุญแจส่วนตัวมีความสัมพันธ์ในทางคณิตศาสตร์กับกุญแจสาธารณะในลักษณะที่สามารถใช้กุญแจสาธารณะตรวจสอบได้ว่าลายมือชื่อดิจิทัลได้สร้างขึ้นโดยใช้กุญแจส่วนตัวนั้นหรือไม่ และสามารถนำกุญแจสาธารณะไปใช้ในการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ ทำให้ไม่สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ได้เพื่อประโยชน์ในการรักษาความลับของข้อมูลอิเล็กทรอนิกส์ เว้นแต่บุคคลที่ถือกุญแจส่วนตัวซึ่งสามารถนำกุญแจส่วนตัวของตนใช้ในการถอดรหัสลับของข้อมูลอิเล็กทรอนิกส์ เพื่อให้เจ้าของกุญแจส่วนตัวสามารถอ่านหรือเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์นั้นได้ [1]

3. ข้อมูลในใบรับรองและรายการเพิกถอนใบรับรอง

3.1 เกี่ยวกับตารางการกำหนดข้อมูลในใบรับรองและรายการเพิกถอนใบรับรอง

ในตารางการกำหนดข้อมูลในใบรับรองและรายการเพิกถอนใบรับรอง ประกอบด้วยสดมภ์ ซึ่งจะมีข้อมูลอยู่ในแนวตั้ง ดังต่อไปนี้

Index	Item	M	C	Value	Guide No.

(1) สดมภ์ Index แสดงดัชนีรายการฟิลด์ข้อมูล ฟิลด์เพิ่มเติม (Extension Field) หรือคุณลักษณะ (Attribute)

(2) สดมภ์ Item แสดงชื่อฟิลด์ข้อมูล ฟิลด์เพิ่มเติม หรือคุณลักษณะ

(3) สดมภ์ M แสดงความจำเป็นของข้อมูลในฟิลด์ข้อมูล ฟิลด์เพิ่มเติม หรือคุณลักษณะ

(4) สดมภ์ C แสดงความสำคัญของข้อมูลในฟิลด์เพิ่มเติม

(5) สดมภ์ Value แสดงข้อมูลหรือวิธีการกำหนดข้อมูลในฟิลด์ข้อมูล ฟิลด์เพิ่มเติม หรือคุณลักษณะ

(6) สดมภ์ Guide No. แสดงเลขที่ข้อซึ่งอธิบายรายละเอียดการกำหนดข้อมูลในฟิลด์ข้อมูล ฟิลด์เพิ่มเติม หรือคุณลักษณะ

3.2 ความจำเป็นของข้อมูล (Mandatory : M)

ในตารางการกำหนดข้อมูลในใบรับรองและรายการเพิกถอนใบรับรอง จะระบุค่าความจำเป็นของข้อมูล ดังต่อไปนี้

(1) m (mandatory) : ฟิลด์ข้อมูล ฟิลด์เพิ่มเติม หรือคุณลักษณะ ที่ต้องระบุข้อมูล

(2) o (optional) : ฟิลด์ข้อมูล ฟิลด์เพิ่มเติม หรือคุณลักษณะ ที่สามารถเลือกระบุหรือไม่ระบุข้อมูล ขึ้นอยู่กับความต้องการใช้งาน

(3) nu (not used) : ห้ามมีฟิลด์ข้อมูล ฟิลด์เพิ่มเติม หรือคุณลักษณะนี้

3.3 ความสำคัญของข้อมูล (Criticality: C)

ในตารางการกำหนดข้อมูลในใบรับรองและรายการเพิกถอนใบรับรอง จะระบุค่าความสำคัญของข้อมูลในฟิลด์เพิ่มเติม ดังต่อไปนี้

(1) T (True) : ฟิลด์เพิ่มเติมที่สำคัญ โดยซอฟต์แวร์จะต้องปฏิเสธการใช้งานใบรับรอง หากไม่เข้าใจความหมายหรือไม่สามารถประมวลผลข้อมูลในฟิลด์เพิ่มเติมได้

(2) F (False) : ฟิลด์เพิ่มเติมทั่วไป โดยซอฟต์แวร์สามารถใช้งานใบรับรองได้ แม้ไม่เข้าใจความหมายของฟิลด์เพิ่มเติม ทั้งนี้ หากซอฟต์แวร์เข้าใจความหมายของฟิลด์เพิ่มเติม ซอฟต์แวร์ต้องประมวลผลข้อมูลในฟิลด์เพิ่มเติมด้วย

4. การกำหนดข้อมูลในใบรับรอง

คณะทำงาน Public-Key Infrastructure (X.509) หรือ PKIX ถูกตั้งขึ้นเพื่อพัฒนามาตรฐานที่เกี่ยวข้องกับการใช้งานโครงสร้างพื้นฐานกุญแจสาธารณะที่อยู่บนพื้นฐานของ X.509 [3] ในอินเทอร์เน็ต โดยคณะทำงาน PKIX ได้จัดทำเอกสาร RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” [4] เพื่อนำเสนอมาตรฐานข้อมูลที่ใช้ในใบรับรอง X.509 เวอร์ชัน 3 และรายการเพิกถอนใบรับรอง X.509 เวอร์ชัน 2 สำหรับการใช้งานในอินเทอร์เน็ต โดยปัจจุบัน RFC 5280 มีการอ้างอิงเพื่อใช้งานอย่างแพร่หลาย

การกำหนดข้อมูลในใบรับรองตามข้อเสนอแนะมาตรฐานฉบับนี้อ้างอิงกับ RFC 5280 โดยมีรายละเอียดดังนี้

4.1 โครงสร้างของใบรับรอง

RFC 5280 กำหนดโครงสร้างพื้นฐานของใบรับรอง X.509 เวอร์ชัน 3 ในรูปแบบ ASN.1 [5] ดังนี้

```
Certificate ::= SEQUENCE {
    tbsCertificate          TBSCertificate,
    signatureAlgorithm      AlgorithmIdentifier,
    signatureValue          BIT STRING }
```

โครงสร้างพื้นฐานข้างต้นแสดงให้เห็นว่าใบรับรองประกอบด้วยฟิลด์ข้อมูล 3 ฟิลด์ คือ

(1) ฟิลด์ tbsCertificate : แสดงข้อมูลในใบรับรอง ซึ่งประกอบด้วย ข้อมูลของเจ้าของใบรับรอง ข้อมูลของผู้ออกใบรับรอง กุญแจสาธารณะของผู้เป็นเจ้าของใบรับรอง ช่วงเวลาที่ใบรับรองสามารถใช้งานได้ และฟิลด์เพิ่มเติมสำหรับบรรจุข้อมูลอื่น ๆ ที่อยู่นอกเหนือจากฟิลด์พื้นฐาน

(2) ฟิลด์ signatureAlgorithm : แสดงข้อมูลอัลกอริทึมที่ผู้ให้บริการออกใบรับรองใช้ลงลายมือชื่อดิจิทัลเพื่อรับรองข้อมูลในใบรับรอง โดยอัลกอริทึมที่ใช้ต้องเป็นชนิดเดียวกับอัลกอริทึมที่ระบุในฟิลด์ signature ของ tbsCertificate (ข้อ 4.2.3)

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

4.2 ข้อมูลในใบรับรอง

ข้อมูลในใบรับรอง ถูกบรรจุอยู่ในฟิลด์ที่ชื่อว่า “tbsCertificate” ซึ่งเป็นฟิลด์ที่ประกอบด้วยข้อมูลพื้นฐานที่จำเป็นต้องปรากฏในใบรับรองทุกใบ และฟิลด์เพิ่มเติม โดยโครงสร้างข้อมูลในใบรับรอง หรือ ฟิลด์ประเภท TBSCertificate ตาม RFC 5280 มีดังนี้

```
TBSCertificate ::= SEQUENCE {
    version             [0]   EXPLICIT Version DEFAULT v1,
    serialNumber              CertificateSerialNumber,
```

signature *AlgorithmIdentifier,*
issuer *Name,*
validity *Validity,*
subject *Name,*
subjectPublicKeyInfo *SubjectPublicKeyInfo,*
issuerUniqueID *[1]* *IMPLICIT UniqueIdentifier OPTIONAL,*
-- If present, version MUST be v2 or v3
subjectUniqueID *[2]* *IMPLICIT UniqueIdentifier OPTIONAL,*
-- If present, version MUST be v2 or v3
extensions *[3]* *EXPLICIT Extensions OPTIONAL*
-- If present, version MUST be v3 }

Version ::= INTEGER { v1(0), v2(1), v3(2) }

CertificateSerialNumber ::= INTEGER

Validity ::= SEQUENCE {
notBefore *Time,*
notAfter *Time }*

Time ::= CHOICE {
utcTime *UTCTime,*
generalTime *GeneralizedTime }*

SubjectPublicKeyInfo ::= SEQUENCE {
algorithm *AlgorithmIdentifier,*
subjectPublicKey *BIT STRING }*

Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension

Extension ::= SEQUENCE {
extnID *OBJECT IDENTIFIER,*
critical *BOOLEAN DEFAULT FALSE,*
extnValue *OCTET STRING }*

รายละเอียดของแต่ละฟิลด์มีดังนี้

4.2.1 version

ฟิลด์ version แสดงข้อมูลเวอร์ชันของใบรับรอง ซึ่ง RFC 5280 นิยามชนิดข้อมูล Version ดังนี้

Version ::= INTEGER { v1(0), v2(1), v3(2) }

ทั้งนี้ เพื่อให้ใบรับรองรองรับการใช้งานฟิลด์เพิ่มเติม จึงกำหนดให้ใช้เฉพาะใบรับรองเวอร์ชัน 3 (ระบุค่าเป็น 2)

4.2.2 serialNumber

ฟิลด์ serialNumber แสดงข้อมูลหมายเลขใบรับรอง (Certificate Serial Number) ซึ่งมีค่าเป็นจำนวนเต็มบวก ขนาดไม่เกิน 20 octets (160 บิต) และไม่ซ้ำกับหมายเลขใบรับรองอื่นที่ออกโดยผู้ให้บริการออกใบรับรองรายเดียวกัน

RFC 5280 นิยามชนิดข้อมูล CertificateSerialNumber ดังนี้

CertificateSerialNumber ::= INTEGER

4.2.3 signature

ฟิลด์ signature แสดง Algorithm Identifier ซึ่งประกอบด้วยหมายเลข Object Identifier (OID) ของอัลกอลิทึมและค่าพารามิเตอร์ (ถ้ามี) ที่ผู้ให้บริการออกใบรับรองใช้ลงลายมือชื่อดิจิทัลเพื่อรับรองข้อมูลในใบรับรองนี้

RFC 5280 นิยามชนิดข้อมูล AlgorithmIdentifier ดังนี้

AlgorithmIdentifier ::= SEQUENCE {

algorithm *OBJECT IDENTIFIER,*

parameters *ANY DEFINED BY algorithm OPTIONAL }*

ทั้งนี้ อัลกอริทึมที่ระบุจะต้องเลือกจากรายการอัลกอริทึมในตารางที่ 1

ตารางที่ 1 อัลกอริทึมที่ใช้ในการลงลายมือชื่อดิจิทัลบนใบรับรอง

ลำดับ	อัลกอริทึมที่ใช้ในการลงลายมือชื่อดิจิทัล	Object Identifier (OID)
1	sha256WithRSAEncryption	1.2.840.113549.1.1.11
2	sha384WithRSAEncryption	1.2.840.113549.1.1.12
3	sha512WithRSAEncryption	1.2.840.113549.1.1.13

4.2.4 issuer

ฟิลด์ issuer แสดงข้อมูลระบุผู้ให้บริการออกใบรับรองที่ออกใบรับรองนี้ โดยใช้ชนิดข้อมูลตาม ITU-T X.501 “Name” [6] ซึ่งมีโครงสร้าง ASN.1 ดังนี้

Name ::= CHOICE { -- only one possibility for now --

rdnSequence RDNSequence }

RDNSequence ::= SEQUENCE OF RelativeDistinguishedName

RelativeDistinguishedName ::= *SET SIZE (1..MAX) OF AttributeTypeAndValue*

AttributeTypeAndValue ::= SEQUENCE {

Type AttributeType,
Value AttributeValue }

AttributeType ::= OBJECT IDENTIFIER

AttributeValue *::= ANY -- DEFINED BY AttributeType*

-- For many of the attribute types defined in X.520 [7]*,*
-- the AttributeValue uses the DirectoryString type.
DirectoryString ::= CHOICE {

teletexString TeletexString (SIZE (1..MAX)),
printableString PrintableString (SIZE (1..MAX)),
universalString UniversalString (SIZE (1..MAX)),
utf8String UTF8String (SIZE (1..MAX)),
bmpString BMPString (SIZE (1..MAX)) }

ทั้งนี้ ข้อมูลในฟิลด์ issuer จะใช้การเข้ารหัส (Encoding) แบบ PrintableString[1] และประกอบด้วยคุณลักษณะตามตารางที่ 2

[1] PrintableString ประกอบด้วยอักขระดังนี้ a-z A-Z 0-9 ' ( ) + , - . ? : / = และ space

ตารางที่ 2 คุณลักษณะของฟิลด์ issuer ในใบรับรอง

คุณลักษณะ	ความหมาย
commonName (cn)	ชื่อของผู้ให้บริการออกใบรับรอง และอาจระบุข้อมูลบ่งบอกถึงระบบบริการ เป็นภาษาอังกฤษ เช่น “ABC CA-G2”
organizationalUnitName (ou)	ชื่อหน่วยงานย่อยในองค์กรของผู้ให้บริการออกใบรับรอง เป็นภาษาอังกฤษ เช่น “ABC Certification Authority”
organizationName (o)	ชื่อองค์กรของผู้ให้บริการออกใบรับรอง เป็นภาษาอังกฤษ เช่น “ABC Company Limited”
countryName (c)	รหัสประเทศ อยู่ในรูปแบบ 2 ตัวอักษรตามที่กำหนดใน ISO 3166-1 คือ “TH”

4.2.5 validity

ฟิลด์ validity แสดงช่วงเวลาที่สามารถใช้ใบรับรองได้ โดยประกอบด้วยข้อมูลวันและเวลาที่ใบรับรองเริ่มต้นใช้งานได้ (notBefore) และวันและเวลาที่ใบรับรองหมดอายุ (notAfter) โดยข้อมูลวันและเวลาสามารถระบุได้ 2 รูปแบบ คือ UTCTime และ GeneralizedTime

ทั้งนี้ ใบรับรองที่หมดอายุก่อนปี ค.ศ. 2050 ต้องระบุข้อมูลในฟิลด์ validity เป็น UTCTime และใบรับรองที่หมดอายุในปี ค.ศ. 2050 เป็นต้นไป ต้องระบุข้อมูลในฟิลด์ validity เป็น GeneralizedTime [4]

RFC 5280 นิยามชนิดข้อมูล Validity ดังนี้

```
Validity ::= SEQUENCE {
        notBefore       Time,
        notAfter        Time }

Time ::= CHOICE {
        utcTime         UTCTime,
        generalTime     GeneralizedTime }
```

รูปแบบของ UTCTime และ GeneralizedTime มีรายละเอียดดังนี้

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 ตัวอักษร ‘Z’ ซึ่งแสดงว่า เวลาที่ระบุเป็นเวลากลางของโลก หรือ Greenwich Mean Time (Zulu)

4.2.6 subject

ฟิลด์ subject แสดงข้อมูลระบุเอนทิตีที่ผู้ให้บริการออกใบรับรองได้รับรองว่าเป็นเจ้าของกุญแจส่วนตัว ซึ่งเป็นคู่กับกุญแจสาธารณะที่อยู่ในใบรับรอง โดยข้อมูลในฟิลด์ subject เป็นข้อมูลชนิด ITU-T X.501 “Name” ซึ่งโครงสร้าง ASN.1 เป็นไปตามข้อ 4.2.4

รายการคุณลักษณะที่ใช้ทั่วไปในฟิลด์ subject เป็นไปตามตารางที่ 3 ทั้งนี้ การกำหนดข้อมูลคุณลักษณะในฟิลด์ subject ของใบรับรองแต่ละประเภทเป็นไปตามข้อ 0

ตารางที่ 3 คุณลักษณะของฟิลด์ subject ในใบรับรอง

คุณลักษณะ	ความหมาย
commonName (cn)	ชื่อทั่วไป
givenName	ชื่อจริง
surname (sn)	นามสกุล
serialNumber	หมายเลขที่ใช้ระบุตัวตนของเอนทิตีซึ่งเป็นเจ้าของใบรับรอง
title	ตำแหน่ง
organizationalUnitName (ou)	ชื่อหน่วยงานย่อยในองค์กร
organizationName (o)	ชื่อองค์กร
organizationIdentifier	หมายเลขระบุองค์กร
localityName (l)	ชื่ออำเภอ หรือ ชื่อเขต
stateOrProvinceName (s)	ชื่อจังหวัด
country (c)	รหัสประเทศ อยู่ในรูปแบบ 2 ตัวอักษรตามที่กำหนดใน ISO 3166-1

4.2.7 subjectPublicKeyInfo

ฟิลด์ subjectPublicKeyInfo แสดงข้อมูลกุญแจสาธารณะ และอัลกอริทึมของกุญแจสาธารณะ ซึ่ง RFC 5280 นิยามชนิดข้อมูล SubjectPublicKeyInfo ดังนี้

SubjectPublicKeyInfo ::= SEQUENCE {

algorithm AlgorithmIdentifier,
subjectPublicKey BIT STRING }

ทั้งนี้ หมายเลข OID ของอัลกอลิทึมที่ใช้ต้องเป็น 1.2.840.113549.1.1.1 ซึ่งหมายถึง RSA encryption และ subjectPublicKey ต้องมีขนาด 4096 บิตเป็นอย่างน้อยสำหรับใบรับรองของผู้ให้บริการออกใบรับรอง และ 2048 บิตเป็นอย่างน้อยสำหรับใบรับรองของผู้ใช้บริการ

4.2.8 extensions

ใบรับรองเวอร์ชัน 3 รองรับการใช้งานฟิลด์ extensions ซึ่งเป็นฟิลด์สำหรับแสดงข้อมูลเพิ่มเติมเกี่ยวกับเจ้าของใบรับรอง กุญแจสาธารณะ และการจัดการใบรับรอง

RFC 5280 นิยามชนิดข้อมูล Extensions ดังนี้

Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension

Extension ::= SEQUENCE {

extnID	*OBJECT IDENTIFIER,*
critical	*BOOLEAN DEFAULT FALSE,*
extnValue	*OCTET STRING }*

โครงสร้างข้างต้นแสดงให้เห็นว่าฟิลด์ Extension มีส่วนประกอบ 3 ส่วน คือ

(1) extnID : หมายเลข OID ที่บ่งบอกถึงประเภทของฟิลด์เพิ่มเติมตัวอย่างเช่น หมายเลข OID เป็น 2.5.29.32 บ่งบอกว่าฟิลด์เพิ่มเติมนี้บรรจุข้อมูลเกี่ยวกับแนวนโยบายของผู้ให้บริการออกใบรับรอง (Certificate Policy : CP) ทั้งนี้ หมายเลข OID ที่บ่งบอกประเภทของฟิลด์เพิ่มเติมตามมาตรฐาน ITU-T X. 509 (Standard Extensions) จะอยู่ภายใต้หมายกิ่ง 2.5.29

(2) critical : ค่าความสำคัญของข้อมูลในฟิลด์เพิ่มเติม ในรูปแบบ Boolean

ก. ค่า critical เป็น True หมายถึง ซอฟต์แวร์จะต้องปฏิเสธการใช้งานใบรับรองหากไม่สามารถเข้าใจความหมายหรือไม่สามารถประมวลผลข้อมูลในฟิลด์เพิ่มเติมได้

ข. ค่า critical เป็น False หมายถึง ซอฟต์แวร์สามารถใช้งานใบรับรองได้ แม้ไม่เข้าใจความหมายของฟิลด์เพิ่มเติม ทั้งนี้ หากซอฟต์แวร์เข้าใจความหมายของฟิลด์เพิ่มเติม ซอฟต์แวร์ต้องประมวลผลข้อมูลในฟิลด์เพิ่มเติมด้วย

(3) extnValue : ข้อมูลในฟิลด์เพิ่มเติม

RFC 5280 ได้กำหนดฟิลด์เพิ่มเติมหลายชนิดให้เลือกใช้งาน ทั้งฟิลด์เพิ่มเติมที่เป็นไปตามมาตรฐาน ITU-T X. 509 (Standard Extensions) และฟิลด์เพิ่มเติมที่กำหนดขึ้นเพื่อใช้งานตามวัตถุประสงค์เฉพาะ (Private Internet Extensions) ทั้งนี้ ข้อเสนอแนะมาตรฐานฉบับนี้จะกล่าวถึงเฉพาะฟิลด์เพิ่มเติมที่สำคัญสำหรับการใช้งานร่วมกันของซอฟต์แวร์ในประเทศไทย ดังรายละเอียดในตารางที่ 4

ตารางที่ 4 รายการฟิลด์เพิ่มเติมในใบรับรอง

ฟิลด์เพิ่มเติม	Object Identifier (OID)	M	C
ฟิลด์เพิ่มเติมที่เป็นไปตามที่มาตรฐาน ITU-T X. 509 (Standard Extensions)			
authorityKeyIdentifier	2.5.29.35	m	F
subjectKeyIdentifier	2.5.29.14	m	F

ฟิลด์เพิ่มเติม	Object Identifier (OID)	M	C
keyUsage	2.5.29.15	m	T
certificatePolicies	2.5.29.32	m	F
subjectAltName	2.5.29.17	o	F
basicConstraints	2.5.29.19	m	T
extKeyUsage	2.5.29.37	o	F
cRLDistributionPoints	2.5.29.31	m	F
ฟิลด์เพิ่มเติมที่กำหนดขึ้นเพื่อใช้งานตามวัตถุประสงค์เฉพาะ (Private Internet Extensions)			
authorityInfoAcess	1.3.6.1.5.5.7.1.1	m	F

หมายเหตุ : 1. คำอธิบายค่าของสดมภ์ M และ C อ้างอิงตามรายละเอียดในข้อ 3.1, 3.2 และ 3.3
2. ในกรณีที่มีความจำเป็นต้องใช้ฟิลด์เพิ่มเติมที่นอกเหนือจากรายการในตารางที่ 4 ผู้ให้บริการออกใบรับรองสามารถกำหนดฟิลด์เพิ่มเติมได้โดยวิธีการกำหนดข้อมูลให้อ้างอิงตาม ISO/IEC 9594-8 : 2017 หรือ RFC 5280

4.2.8.1 authorityKeyIdentifier

authorityKeyIdentifier เป็นฟิลด์เพิ่มเติมที่ระบุค่าอ้างอิงถึงกุญแจสาธารณะที่เป็นคู่กับกุญแจส่วนตัวซึ่งผู้ให้บริการออกใบรับรองใช้ลงลายมือชื่อดิจิทัลเพื่อรับรองใบรับรองนี้ โดย authorityKeyIdentifier มีประโยชน์ในกรณีที่ผู้ให้บริการออกใบรับรองมีกุญแจส่วนตัวสำหรับลงลายมือชื่อดิจิทัลมากกว่า 1 อัน

RFC 5280 นิยามฟิลด์ authorityKeyIdentifier ดังนี้

id-ce-authorityKeyIdentifier OBJECT IDENTIFIER ::= { id-ce 35 }

AuthorityKeyIdentifier ::= SEQUENCE {

keyIdentifier	*[0]*	*KeyIdentifier*	*OPTIONAL,*
authorityCertIssuer	*[1]*	*GeneralNames*	*OPTIONAL,*
authorityCertSerialNumber	*[2]*	*CertificateSerialNumber*	*OPTIONAL }*

KeyIdentifier ::= OCTET STRING

ทั้งนี้ ให้ระบุเฉพาะค่าของ KeyIdentifier ซึ่งเป็นค่าของฟังก์ชัน SHA-1 Hash ของกุญแจสาธารณะของผู้ให้บริการออกใบรับรอง

4.2.8.2 subjectKeyIdentifier

subjectKeyIdentifier เป็นฟิลด์เพิ่มเติมที่ระบุค่าอ้างอิงถึงกุญแจสาธารณะของเจ้าของใบรับรอง โดย RFC 5280 นิยามฟิลด์ subjectKeyIdentifier ดังนี้

id-ce-subjectKeyIdentifier OBJECT IDENTIFIER ::= { id-ce 14 }

SubjectKeyIdentifier ::= KeyIdentifier

KeyIdentifier ::= OCTET STRING

ทั้งนี้ ค่าของ KeyIdentifier ให้ระบุเป็นค่าของฟังก์ชัน SHA-1 Hash ของกุญแจสาธารณะที่อยู่ในใบรับรองใบนี้ (กุญแจสาธารณะ คือข้อมูลในฟิลด์ subjectPublicKey ซึ่งอยู่ภายใต้ฟิลด์ subjectPublicKeyInfo ดังรายละเอียดในข้อ 4.2.7)

4.2.8.3 keyUsage

keyUsage เป็นฟิลด์เพิ่มเติมที่ใช้ระบุถึงวัตถุประสงค์ของการใช้กุญแจสาธารณะซึ่งอยู่ในใบรับรอง อาทิ การเข้ารหัสลับข้อมูล และการตรวจสอบลายมือชื่อดิจิทัล โดยการกำหนดวัตถุประสงค์ของการใช้กุญแจสาธารณะสามารถกำหนดวัตถุประสงค์ได้มากกว่า 1 วัตถุประสงค์ตามความเหมาะสมของการใช้งานและความปลอดภัยในการดูแลรักษากุญแจส่วนตัว

RFC 5280 นิยามฟิลด์ keyUsage ดังนี้

id-ce-keyUsage OBJECT IDENTIFIER ::= { id-ce 15 }

KeyUsage ::= BIT STRING {

digitalSignature	*(0),*
contentCommitment	*(1),*
keyEncipherment	*(2),*
dataEncipherment	*(3),*
keyAgreement	*(4),*
keyCertSign	*(5),*
cRLSign	*(6),*
encipherOnly	*(7),*
decipherOnly	*(8) }*

บิตใน keyUsage บ่งบอกถึงวัตถุประสงค์ของการใช้งานกุญแจสาธารณะในใบรับรอง ดังนี้

(0) digitalSignature	มีค่าเป็น 1 เมื่อใช้สำหรับตรวจสอบลายมือชื่อดิจิทัลที่ใช้เพื่อการยืนยันตัวตนของผู้ลงลายมือชื่อ การยืนยันแหล่งที่มาของข้อมูล และ/หรือ ความครบถ้วนสมบูรณ์ (Integrity) ของข้อมูล
(1) contentCommitment	มีค่าเป็น 1 เมื่อใช้สำหรับตรวจสอบลายมือชื่อดิจิทัลที่ใช้เพื่อการรับรองว่าผู้ลงลายมือชื่อได้รับรองเนื้อหาที่ตนลงนามและยินยอมให้มีผลผูกพันกับตน หรือผู้ลงลายมือชื่อได้ทบทวนและเห็นชอบในเนื้อหา
(2) keyEncipherment	มีค่าเป็น 1 เมื่อใช้สำหรับการเข้ารหัสลับกุญแจ หรือข้อมูลด้านความปลอดภัย เช่น การแลกเปลี่ยนกุญแจ (Key Transport)

(3) dataEncipherment มีค่าเป็น 1 เมื่อใช้สำหรับการเข้ารหัสลับข้อมูลของผู้ใช้บริการ

(4) keyAgreement มีค่าเป็น 1 เมื่อใช้สำหรับกระบวนการ key agreement

(5) keyCertSign มีค่าเป็น 1 เมื่อใช้สำหรับตรวจสอบลายมือชื่อดิจิทัลของผู้ให้บริการออกใบรับรอง

(6) cRLSign มีค่าเป็น 1 เมื่อใช้สำหรับตรวจสอบลายมือชื่อดิจิทัลของผู้ออกรายการเพิกถอนใบรับรอง

(7) encipherOnly มีค่าเป็น 1 เมื่อใช้สำหรับเข้ารหัสลับข้อมูลในกระบวนการ key agreement โดยต้องใช้ร่วมกับ keyAgreement

(8) decipherOnly มีค่าเป็น 1 เมื่อใช้สำหรับถอดรหัสลับข้อมูลในกระบวนการ key agreement โดยต้องใช้ร่วมกับ keyAgreement

ทั้งนี้ ใบรับรองของผู้ใช้บริการ จะเลือกตั้งค่าเฉพาะบิต (0) (1) (2) และ (3) โดยบิตอื่น ๆ มีค่าเป็น 0

4.2.8.4 certificatePolicies

certificatePolicies เป็นฟิลด์เพิ่มเติมที่แสดงข้อมูลนโยบาย (Policy information) ที่เกี่ยวข้องกับการออกใบรับรองและวัตถุประสงค์ของการใช้ใบรับรองที่กำหนดโดยผู้ให้บริการออกใบรับรอง ซึ่งแต่ละนโยบายประกอบด้วยหมายเลข OID ของนโยบายและอาจมีข้อมูลเพิ่มเติม (Qualifier)

RFC 5280 นิยามฟิลด์ certificatePolicies ดังนี้

```
id-ce-certificatePolicies OBJECT IDENTIFIER ::=  { id-ce 32 }

CertificatePolicies ::= SEQUENCE SIZE (1..MAX) OF PolicyInformation

PolicyInformation ::= SEQUENCE {
    policyIdentifier        CertPolicyId,
    policyQualifiers        SEQUENCE SIZE (1..MAX) OF
                                PolicyQualifierInfo OPTIONAL }

CertPolicyId ::= OBJECT IDENTIFIER

PolicyQualifierInfo ::= SEQUENCE {
    policyQualifierId       PolicyQualifierId,
    qualifier               ANY DEFINED BY policyQualifierId }

-- policyQualifierIds for Internet policy qualifiers
id-qt          OBJECT IDENTIFIER ::= { id-pkix 2 }
id-qt-cps      OBJECT IDENTIFIER ::= { id-qt 1 }
```

id-qt-unotice OBJECT IDENTIFIER ::= { id-qt 2 }

PolicyQualifierId ::= OBJECT IDENTIFIER (id-qt-cps | id-qt-unotice)

Qualifier ::= CHOICE {

cPSuri	*CPSuri,*
userNotice	*UserNotice }*

CPSuri ::= IA5String

UserNotice ::= SEQUENCE {

noticeRef	*NoticeReference OPTIONAL,*
explicitText	*DisplayText OPTIONAL }*

NoticeReference ::= SEQUENCE {

Organization	*DisplayText,*
noticeNumbers	*SEQUENCE OF INTEGER }*

DisplayText ::= CHOICE {

ia5String	*IA5String*	*(SIZE (1..200)),*
visibleString	*VisibleString*	*(SIZE (1..200)),*
bmpString	*BMPString*	*(SIZE (1..200)),*
utf8String	*UTF8String*	*(SIZE (1..200)) }*

จากโครงสร้างข้างต้น ข้อมูลนโยบาย (Policy Information) แบ่งออกเป็น 2 ส่วน ได้แก่

(1) PolicyIdentifier : ข้อมูลระบุหมายเลข OID ของแนวนโยบาย (Certificate Policy) ที่เกี่ยวข้องกับการออกใบรับรองและวัตถุประสงค์ของการใช้ใบรับรอง

(2) PolicyQualifiers : ข้อมูลเพิ่มเติมจากแนวนโยบายที่กำหนดใน PolicyIdentifier ซึ่งเป็นไปได้ 2 รูปแบบ คือ

(2.1) CPS Pointer {OID = 1.3.6.1.5.5.7.2.1} : ตัวบ่งชี้ไปยังแนวปฏิบัติของผู้ให้บริการออกใบรับรอง (Certification Practice Statement : CPS) สำหรับการให้บริการออกใบรับรอง ในรูปแบบ Uniform Resource Identifier (URI)

(2.2) User notice {OID = 1.3.6.1.5.5.7.2.2} : -ข้อความที่แสดงต่อผู้ใช้บริการและผู้ที่เกี่ยวข้อง (Relying Party) เมื่อใช้ใบรับรอง โดยซอฟต์แวร์ควรจะแสดงข้อความนี้เมื่อใช้ใบรับรอง

4.2.8.5 subjectAltName

subjectAltName เป็นฟิลด์เพิ่มเติมที่ใช้ระบุข้อมูลเกี่ยวกับเอนทิตีที่เป็นเจ้าของใบรับรอง เพิ่มเติมจากฟิลด์ subject โดยสามารถกำหนดได้หลายรูปแบบ เช่น e-mail address, Domain Name, IP Address และ URI เป็นต้น

RFC 5280 นิยามฟิลด์ subjectAltName ดังนี้

id-ce-subjectAltName OBJECT IDENTIFIER ::= { id-ce 17 }

SubjectAltName ::= GeneralNames

GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName

GeneralName ::= CHOICE {

otherName	*[0]*	*OtherName,*
rfc822Name	*[1]*	*IA5String,*
dNSName	*[2]*	*IA5String,*
x400Address	*[3]*	*ORAddress,*
directoryName	*[4]*	*Name,*
ediPartyName	*[5]*	*EDIPartyName,*
uniformResourceIdentifier	*[6]*	*IA5String,*
iPAddress	*[7]*	*OCTET STRING,*
registeredID	*[8]*	*OBJECT IDENTIFIER }*

OtherName ::= SEQUENCE {

type-id		*OBJECT IDENTIFIER,*
value	*[0]*	*EXPLICIT ANY DEFINED BY type-id }*

EDIPartyName ::= SEQUENCE {

nameAssigner	*[0]*	*DirectoryString OPTIONAL,*
partyName	*[1]*	*DirectoryString }*

4.2.8.6 basicConstraints

basicConstraints เป็นฟิลด์เพิ่มเติมที่ใช้ระบุว่าใบรับรองนี้เป็นใบรับรองของผู้ให้บริการออกใบรับรองหรือไม่ พร้อมทั้งจำนวนใบรับรองลำดับชั้นถัดลงมา (Subordinate CA Certificate) ที่มากที่สุดที่อนุญาตให้อยู่ในลำดับชั้นถัดลงมาจากใบรับรองใบนี้ใน certification path

RFC 5280 นิยามฟิลด์ basicConstraints ดังนี้

id-ce-basicConstraints OBJECT IDENTIFIER ::= { id-ce 19 }

BasicConstraints ::= SEQUENCE {

cA *BOOLEAN DEFAULT FALSE,*

pathLenConstraint *INTEGER (0..MAX) OPTIONAL }*

basicConstraints extension สามารถใช้ระบุข้อจำกัดพื้นฐานได้ 2 รายการ คือ

(1) cA คือ ค่าชนิด Boolean ที่แสดงว่าใบรับรองนี้เป็นใบรับรองของผู้ให้บริการออกใบรับรองหรือไม่ โดย

(1.1) cA มีค่าเป็น True หมายถึง ใบรับรองของผู้ให้บริการออกใบรับรอง

(1.2) cA มีค่าเป็น False หมายถึง ใบรับรองของผู้ใช้งาน

(2) pathLenConstraint จะมีความหมายก็ต่อเมื่อ cA มีค่าเป็น True โดย pathLenConstraint แสดงจำนวนใบรับรองลำดับชั้นถัดลงมา (Subordinate CA Certificate) ที่มากที่สุดที่อนุญาตให้อยู่ในลำดับชั้นถัดจากใบรับรองใบนี้ใน certification path

สำหรับใบรับรองภายใต้ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์แห่งชาตินั้น มีการกำหนดค่า cA และ pathLenConstraint เป็นไปตามตารางที่ 5

ตารางที่ 5 ค่า cA และ pathLenConstraint ในใบรับรองแต่ละประเภท

ประเภทของใบรับรอง	ค่า cA	ค่า pathLenConstraint
1. ใบรับรองของผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา ชั้นที่ 1	True	1
2. ใบรับรองของผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา ชั้นที่ 2	True	0
3. ใบรับรองของผู้ใช้บริการ (Subscriber Certificate)	False	ห้ามมีฟิลด์นี้

4.2.8.7 extKeyUsage

extKeyUsage เป็นฟิลด์เพิ่มเติมที่ใช้ระบุถึงวัตถุประสงค์ของการใช้กุญแจสาธารณะในใบรับรองที่เพิ่มเติมจากฟิลด์ keyUsage ในข้อ 4.2.8.3

RFC 5280 นิยามฟิลด์ extKeyUsage ดังนี้

id-ce-extKeyUsage OBJECT IDENTIFIER ::= { id-ce 37 }

ExtKeyUsageSyntax ::= SEQUENCE SIZE (1..MAX) OF KeyPurposeId

KeyPurposeId ::= OBJECT IDENTIFIER

RFC 5280 กำหนดวัตถุประสงค์ของการใช้งานไว้ดังนี้

anyExtendedKeyUsage OBJECT IDENTIFIER ::= { id-ce-extKeyUsage 0 }

id-kp *OBJECT IDENTIFIER ::= { id-pkix 3 }*

id-kp-serverAuth OBJECT IDENTIFIER ::= { id-kp 1 }

-- ใช้สำหรับยืนยันตัวตน Server (Server authentication)

id-kp-clientAuth OBJECT IDENTIFIER ::= { id-kp 2 }

-- ใช้สำหรับยืนยันตัวตนผู้ใช้บริการ (Client authentication)

id-kp-codeSigning OBJECT IDENTIFIER ::= { id-kp 3 }

-- ใช้สำหรับรับรองที่มาของโค้ด (Signing of downloadable executable code)

id-kp-emailProtection OBJECT IDENTIFIER ::= { id-kp 4 }

-- ใช้สำหรับป้องกันจดหมายอิเล็กทรอนิกส์ (Email protection)

id-kp-timeStamping OBJECT IDENTIFIER ::= { id-kp 8 }

-- ใช้สำหรับประทับรับรองเวลา (Time Stamping)

id-kp-OCSPSigning OBJECT IDENTIFIER ::= { id-kp 9 }

-- ใช้สำหรับลงลายมือชื่อบน OCSP Reponse

ทั้งนี้ สำหรับการใช้งานใบรับรองร่วมกับ Microsoft Root Certificate Program [8] ใบรับรองจะต้องระบุค่า extKeyUsage ที่ไม่ใช่ anyExtendedKeyUsage ซึ่ง Microsoft ได้เพิ่มหมายเลข OID สำหรับกำหนดวัตถุประสงค์ของการใช้งานเพิ่มเติมจาก RFC 5280 คือ Encrypting File System {1.3.6.1.4.1.311.10.3.4} และ Document Signing {1.3.6.1.4.1.311.10.3.12}

รายการวัตถุประสงค์ของการใช้งานกุญแจสาธารณะที่ระบุฟิลด์ extKeyUsage ที่สำคัญเป็นไปตามตารางที่ 6

ตารางที่ 6 วัตถุประสงค์ของการใช้งานกุญแจสาธารณะในฟิลด์ extKeyUsage

วัตถุประสงค์ของการใช้งาน	Object Identifier (OID)	วัตถุประสงค์
id-kp-serverAuth	1.3.6.1.5.5.7.3.1	การยืนยันตัวตน Server (Server Authentication) ผ่านโปรโตคอล SSL หรือ TLS
id-kp-clientAuth	1.3.6.1.5.5.7.3.2	การยืนยันตัวตนผู้ใช้บริการ (Client Authentication) ผ่านโปรโตคอล SSL หรือ TLS
id-kp-codeSigning	1.3.6.1.5.5.7.3.3	การลงลายมือชื่อดิจิทัลรับรองที่มาของโค้ด
id-kp-emailProtection	1.3.6.1.5.5.7.3.4	การป้องกันจดหมายอิเล็กทรอนิกส์ (Email protection)
id-kp-timeStamping	1.3.6.1.5.5.7.3.8	การประทับรับรองเวลา (Time Stamping)
id-kp-OCSPSigning	1.3.6.1.5.5.7.3.9	การลงลายมือชื่อสำหรับ OCSP Reponse

วัตถุประสงค์ของการใช้งาน	Object Identifier (OID)	วัตถุประสงค์
szOID_EFS_CRYPTO	1.3.6.1.4.1.311.10.3.4	การเข้ารหัสลับ File System (Encrypting File System)
szOID_KP_DOCUMENT_SIGNING	1.3.6.1.4.1.311.10.3.12	การลงลายมือชื่อบนเอกสาร (Document Signing)

4.2.8.8 cRLDistributionPoints

cRLDistributionPoints เป็นฟิลด์เพิ่มเติมที่ใช้ระบุวิธีการเข้าถึงรายการเพิกถอนใบรับรอง โดยแสดงเป็นลำดับของแหล่งเผยแพร่รายการเพิกถอนใบรับรอง

RFC 5280 นิยามฟิลด์ cRLDistributionPoints ดังนี้

id-ce-cRLDistributionPoints OBJECT IDENTIFIER ::= { id-ce 31 }

CRLDistributionPoints ::= SEQUENCE SIZE (1..MAX) OF DistributionPoint

DistributionPoint ::= SEQUENCE {

distributionPoint [0] DistributionPointName OPTIONAL,
reasons [1] ReasonFlags OPTIONAL,
cRLIssuer [2] GeneralNames OPTIONAL }

DistributionPointName ::= CHOICE {

fullName [0] GeneralNames,
nameRelativeToCRLIssuer [1] RelativeDistinguishedName }

ReasonFlags ::= BIT STRING {

unused (0),
keyCompromise (1),
cACompromise (2),
affiliationChanged (3),
superseded (4),
cessationOfOperation (5),
certificateHold (6),
privilegeWithdrawn (7),
aACompromise (8) }

ผู้ให้บริการออกใบรับรองสามารถระบุแหล่งเผยแพร่รายการเพิกถอนใบรับรอง (DistributionPoint) ได้มากกว่า 1 แหล่ง โดยแต่ละแหล่งสามารถระบุข้อมูลดังนี้

(1) distributionPoint : แหล่งเผยแพร่รายการเพิกถอนใบรับรอง โดยให้กำหนดเป็น URI ของรายการเพิกถอนใบรับรองปัจจุบัน โดยใบรับรองแต่ละใบจะต้องมีข้อมูล DistributionPointName อย่างน้อย 1 แหล่ง

(2) reason : เหตุผลในการเพิกถอนใบรับรอง

(3) cRLIssuer : Distinguished name (DN) ของผู้ออกรายการเพิกถอนใบรับรอง ใช้ในกรณีที่ผู้ให้บริการออกใบรับรองไม่ได้เป็นผู้ออกรายการเพิกถอนใบรับรองเอง

4.2.8.9 authorityInfoAccess

authorityInfoAccess เป็นฟิลด์เพิ่มเติมที่ระบุวิธีการเข้าถึงข้อมูล และบริการต่าง ๆ ของผู้ให้บริการออกใบรับรองที่ออกใบรับรองนี้

RFC 5280 นิยามฟิลด์ authorityInfoAccess ดังนี้

id-pe-authorityInfoAccess OBJECT IDENTIFIER ::= { id-pe 1 }

AuthorityInfoAccessSyntax ::=

SEQUENCE SIZE (1..MAX) OF AccessDescription

AccessDescription ::= SEQUENCE {

accessMethod OBJECT IDENTIFIER,

accessLocation GeneralName }

ทั้งนี้ RFC 5280 นิยามวิธีการเข้าถึงข้อมูลและบริการของผู้ให้บริการออกใบรับรอง 2 วิธี คือ id-ad-calssuers และ id-ad-ocsp รายละเอียดตามตารางที่ 7

ตารางที่ 7 วิธีการเข้าถึงข้อมูลและบริการของผู้ให้บริการออกใบรับรอง

วิธีการเข้าถึง (accessMethod)	Object Identifier (OID)	รายละเอียด
id-ad-ocsp	1.3.6.1.5.5.7.48.1	การเข้าถึงสถานะการเพิกถอนใบรับรองใบนี้ ผ่านโปรโตคอล Online Certificate Status Protocol (OCSP)
id-ad-calssuers	1.3.6.1.5.5.7.48.2	การเข้าถึงรายการใบรับรองของผู้ให้บริการออกใบรับรองที่ออกใบรับรองนี้ ผ่านชื่อ directory หรือ LDAP หรือ HTTP หรือ FTP

4.3 ข้อแนะนำในการกำหนดข้อมูลในใบรับรอง

4.3.1 ใบรับรองของผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา (Subordinate CA Certificate) ชั้นที่ 1

ใบรับรองของผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา ชั้นที่ 1 คือ ใบรับรองที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์แห่งชาติ ออกให้กับผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา (รายละเอียดตามภาคผนวก ก.)

การกำหนดข้อมูลในใบรับรองของผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา ชั้นที่ 1 มีรายละเอียดตามตารางที่ 8 โดยข้อมูลในฟิลด์ issuer และฟิลด์ subject ใช้การเข้ารหัสแบบ PrintableString เท่านั้น

ตารางที่ 8 การกำหนดข้อมูลในใบรับรองของผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา ชั้นที่ 1

Index	Item	M	C	Value	Guide No.
ฟิลด์พื้นฐาน (Basic Fields)					
1	version	m		2 (Version 3)	4.2.1
2	serialNumber	m		ตัวเลขที่ไม่ซ้ำกันระหว่างใบรับรองภายใต้ผู้ให้บริการออกใบรับรองรายเดียวกัน โดยเป็นตัวเลขแบบสุ่มและไม่เรียงกันเมื่อเทียบกับใบรับรองที่ออกก่อนหน้าและต่อจากใบนี้ (randomized and non-sequential) ทั้งนี้ จะต้องมีค่ามากกว่า 0 และขนาดไม่น้อยกว่า 64 บิต [9]	4.2.2
3	signature	m		OID={1.2.840.113549.1.1.13} (sha512WithRSAEncryption)	4.2.3
4	issuer	m			4.2.4
4.1	commonName (cn)	m		ชื่อผู้ให้บริการออกใบรับรองลำดับชั้นบนสุด และข้อมูลบ่งบอกถึงระบบบริการ เป็นภาษาอังกฤษ เช่น “Thailand National Root Certification Authority - G1”	
4.2	organizationalUnitName (ou)	o		ชื่อหน่วยงานย่อยในองค์กรของผู้ให้บริการออกใบรับรองลำดับชั้นบนสุด เป็นภาษาอังกฤษ เช่น “Thailand National Root Certification Authority”	
4.3	organizationName (o)	m		ชื่อองค์กรของผู้ให้บริการออกใบรับรองลำดับชั้นบนสุด เป็นภาษาอังกฤษ เช่น “Electronic Transactions Development Agency (Public Organization)”	
4.4	countryName (c)	m		“TH”	
5	validity	m			4.2.5
5.1	notBefore	m		วันและเวลาที่ใบรับรองเริ่มใช้งานได้	
5.2	notAfter	m		วันและเวลาที่ใบรับรองสิ้นสุดการใช้งาน	
6	subject	m			4.2.6

Index	Item	M	C	Value	Guide No.
6.1	commonName (cn)	m		ชื่อผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา ชั้นที่ 1 และข้อมูลบ่งบอกถึงระบบบริการ เป็นภาษาอังกฤษ เช่น “ABC Certification Authority - G1”	
6.2	organizationalUnitName (ou)	o		ชื่อหน่วยงานย่อยในองค์กรของผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา ชั้นที่ 1 เป็นภาษาอังกฤษ เช่น “ABC Certification Authority”	
6.3	organizationName (o)	m		ชื่อองค์กรของผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา ชั้นที่ 1 เป็น ภาษาอังกฤษ เช่น “ABC Corporation”	
6.4	countryName (c)	m		“TH”	
7	subjectPublicKeyInfo	m			4.2.7
7.1	algorithm	m		OID = {1.2.840.113549.1.1.1} (RSA encryption)	
7.2	subjectPublicKey	m		กุญแจสาธารณะชนิด RSA ความยาวอย่างน้อย 4096 บิต	
ฟิลด์เพิ่มเติม (Extension Fields)					
8	authorityKeyIdentifier	m	F	keyIdentifier บรรจุค่าของฟังก์ชัน SHA-1 Hash ของกุญแจสาธารณะที่เป็นคู่กับกุญแจส่วนตัวซึ่งผู้ให้บริการออกใบรับรองลำดับชั้นบนสุดใช้ลงลายมือชื่อดิจิทัลเพื่อรับรองใบรับรองนี้	4.2.8.1
9	subjectKeyIdentifier	m	F	keyIdentifier บรรจุค่าของฟังก์ชัน SHA-1 Hash ของ subjectPublicKey ซึ่งอยู่ในฟิลด์ subjectPublicKeyInfo	4.2.8.2
10	keyUsage	m	T	- ตั้งค่า keyCertSign และ cRLSign เป็น 1 - สามารถเลือกตั้งค่า digitalSignature เป็น 1 - ค่าอื่น ๆ เป็น 0	4.2.8.3
11	certificatePolicies	m	F		4.2.8.4
11.1	policyIdentifier	m		OID ของ Certificate Policy	
11.2	policyQualifiers	m		ระบุอย่างน้อย 1 PolicyQualifierInfo	
11.2.1	PolicyQualifierInfo [1]	m			
11.2.1.1	policyQualifierId	m		OID = {1.3.6.1.5.5.7.2.1}	
11.2.1.2	qualifier	m		cPSuri = HTTP URL ของ Certification Practice Statement	
12	basicConstraints	m	T		4.2.8.6
12.1	cA	m		True	
12.2	pathLenConstraint	m		1	
13	cRLDistributionPoints	m	F	ระบุอย่างน้อย 1 DistributionPoint	4.2.8.8
13.1	DistributionPoint [1]	m			
13.1.1	distributionPoint	m		HTTP URL ที่สามารถเข้าถึงรายการเพิกถอนใบรับรอง	
13.1.2	reason	nu		ห้ามมีฟิลด์นี้	
13.1.3	cRLIssuer	nu		ห้ามมีฟิลด์นี้	

Index	Item	M	C	Value	Guide No.
14	authorityInfoAccess	m	F	ระบุ 2 AccessDescription	4.2.8.9
14.1	AccessDescription [1]	m			
14.1.1	accessMethod	m		OID = {1.3.6.1.5.5.7.48.1}	
14.1.2	accessLocation	m		HTTP URL สำหรับเข้าถึงบริการ OCSP	
14.2	AccessDescription [2]	m			
14.2.1	accessMethod	m		OID = {1.3.6.1.5.5.7.48.2}	
14.2.2	accessLocation	m		HTTP URL สำหรับเข้าถึงรายการใบรับรองของผู้ให้บริการออกใบรับรองลำดับชั้นบนสุด	

4.3.2 ใบรับรองของผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา ชั้นที่ 2

ใบรับรองของผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา ชั้นที่ 2 คือ ใบรับรองสำหรับผู้ให้บริการออกใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา ชั้นที่ 1 (รายละเอียดตาม ภาคผนวก ก.)

การกำหนดข้อมูลในใบรับรองของผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา ชั้นที่ 2 มีรายละเอียดตามตารางที่ 9 โดยข้อมูลในฟิลด์ issuer และฟิลด์ subject ใช้การเข้ารหัสแบบ PrintableString เท่านั้น

ตารางที่ 9 การกำหนดข้อมูลในใบรับรองของผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา ชั้นที่ 2

Index	Item	M	C	Value	Guide No.
ฟิลด์พื้นฐาน (Basic Fields)					
1	version	m		2 (Version 3)	4.2.1
2	serialNumber	m		ตัวเลขที่ไม่ซ้ำกันระหว่างใบรับรองภายใต้ผู้ให้บริการออกใบรับรองรายเดียวกัน โดยเป็นตัวเลขแบบสุ่มและไม่เรียงกันเมื่อเทียบกับใบรับรองที่ออกก่อนหน้าและต่อจากใบนี้ (randomized and non-sequential) ทั้งนี้ จะต้องมีค่ามากกว่า 0 และขนาดไม่น้อยกว่า 64 บิต [9]	4.2.2
3	signature	m		OID={1.2.840.113549.1.1.13} (sha512WithRSAEncryption)	4.2.3
4	issuer	m			4.2.4
4.1	commonName (cn)	m		ชื่อผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา ชั้นที่ 1 และข้อมูลบ่งบอกถึงระบบบริการ เป็นภาษาอังกฤษ เช่น “ABC Certification Authority - G1”	
4.2	organizationalUnitName (ou)	o		ชื่อหน่วยงานย่อยในองค์กรของผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา ชั้นที่ 1 เป็นภาษาอังกฤษ เช่น “ABC Certification Authority”	
4.3	organizationName (o)	m		ชื่อองค์กรของผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา ชั้นที่ 1 เป็นภาษาอังกฤษ เช่น “ABC Corporation”	

Index	Item	M	C	Value	Guide No.
4.4	countryName (c)	m		"TH"	
5	validity	m			4.2.5
5.1	notBefore	m		วันและเวลาที่ใบรับรองเริ่มใช้งานได้	
5.2	notAfter	m		วันและเวลาที่ใบรับรองสิ้นสุดการใช้งาน	
6	subject	m			4.2.6
6.1	commonName (cn)	o		ชื่อผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา ชั้นที่ 2 และข้อมูลบ่งบอกถึงระบบบริการ เป็นภาษาอังกฤษ เช่น "XYZ Certification Authority - G1"	
6.2	organizationalUnitName (ou)	m		ชื่อหน่วยงานย่อยในองค์กรของผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา ชั้นที่ 2 เป็นภาษาอังกฤษ เช่น "XYZ Certification Authority"	
6.3	organizationName (o)	m		ชื่อองค์กรของผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา ชั้นที่ 2 เป็นภาษาอังกฤษ เช่น "XYZ Corporation"	
6.4	countryName (c)	m		"TH"	
7	subjectPublicKeyInfo	m			4.2.7
7.1	algorithm	m		OID = {1.2.840.113549.1.1.1} (RSA encryption)	
7.2	subjectPublicKey	m		กุญแจสาธารณะชนิด RSA ความยาวอย่างน้อย 4096 บิต	
ฟิลด์เพิ่มเติม (Extension Fields)					
8	authorityKeyIdentifier	m	F	keyIdentifier บรรจุค่าของฟังก์ชัน SHA-1 Hash ของกุญแจสาธารณะที่เป็นคู่กับกุญแจส่วนตัวซึ่งผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา ชั้นที่ 1 ใช้ลงลายมือชื่อดิจิทัลเพื่อรับรองใบรับรองนี้	4.2.8.1
9	subjectKeyIdentifier	m	F	keyIdentifier บรรจุค่าของฟังก์ชัน SHA-1 Hash ของ subjectPublicKey ซึ่งอยู่ในฟิลด์ subjectPublicKeyInfo	4.2.8.2
10	keyUsage	m	T	- ตั้งค่า keyCertSign และ cRLSign เป็น 1 - สามารถเลือกตั้งค่า digitalSignature เป็น 1 - ค่าอื่น ๆ เป็น 0	4.2.8.3
11	certificatePolicies	m	F		4.2.8.4
11.1	policyIdentifier	m		OID ของ Certificate Policy	
11.2	policyQualifiers	m		ระบุอย่างน้อย 1 PolicyQualifierInfo	
11.2.1	PolicyQualifierInfo [1]	m			
11.2.1.1	policyQualifierId	m		OID = {1.3.6.1.5.5.7.2.1}	
11.2.1.2	qualifier	m		cPSuri = HTTP URL ของ Certification Practice Statement	

Index	Item	M	C	Value	Guide No.
12	basicConstraints	m	T		4.2.8.6
12.1	cA	m		True	
12.2	pathLenConstraint	m		0	
13	cRLDistributionPoints	m	F	ระบุอย่างน้อย 1 DistributionPoint	4.2.8.8
13.1	DistributionPoint [1]	m			
13.1.1	distributionPoint	m		HTTP URL ที่สามารถเข้าถึงรายการเพิกถอนใบรับรอง	
13.1.2	reason	nu		ห้ามมีฟิลด์นี้	
13.1.3	cRLIssuer	nu		ห้ามมีฟิลด์นี้	
14	authorityInfoAccess	m	F	ระบุ 2 AccessDescription	4.2.8.9
14.1	AccessDescription [1]	m			
14.1.1	accessMethod	m		OID = {1.3.6.1.5.5.7.48.1}	
14.1.2	accessLocation	m		HTTP URL สำหรับเข้าถึงบริการ OCSP	
14.2	AccessDescription [2]	m			
14.2.1	accessMethod	m		OID = {1.3.6.1.5.5.7.48.2}	
14.2.2	accessLocation	m		HTTP URL สำหรับเข้าถึงรายการใบรับรองของผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา ชั้นที่ 1	

4.3.3 ใบรับรองของผู้ใช้บริการ

ใบรับรองของผู้ใช้บริการ ตามข้อเสนอแนะมาตรฐานฉบับนี้ แบ่งออกเป็น 4 ประเภท ได้แก่ ใบรับรองสำหรับบุคคลธรรมดา ใบรับรองสำหรับนิติบุคคล ใบรับรองสำหรับลงลายมือชื่อดิจิทัลโดยเครื่องให้บริการ และใบรับรองสำหรับโปรโตคอล SSL/TLS หรือโปรโตคอลอื่น ๆ

การระบุข้อมูลในฟิลด์ issuer ทั้งหมด และข้อมูล serialNumber และ countryName ในฟิลด์ subject ใช้การเข้ารหัสแบบ PrintableString เท่านั้น ในขณะที่ข้อมูลส่วนอื่น สามารถใช้การเข้ารหัสแบบ PrintableString หรือ UTF8String

4.3.3.1 ใบรับรองสำหรับบุคคลธรรมดา

ใบรับรองสำหรับบุคคลธรรมดา คือ ใบรับรองที่ใช้ในกรณีผู้รับผิดชอบทางธุรกรรมเป็นบุคคลธรรมดา มีรายละเอียดการกำหนดข้อมูลตามตารางที่ 10

ตารางที่ 10 การกำหนดข้อมูลในใบรับรองสำหรับบุคคลธรรมดา

Index	Item	M	C	Value	Guide No.
ฟิลด์พื้นฐาน (Basic Fields)					
1	version	m		2 (Version 3)	4.2.1
2	serialNumber	m		ตัวเลขที่ไม่ซ้ำกันระหว่างใบรับรองภายใต้ผู้ให้บริการออกใบรับรองรายเดียวกัน โดยเป็นตัวเลขแบบสุ่มและไม่เรียงกันเมื่อเทียบกับใบรับรองที่ออกก่อนหน้าและต่อจากใบนี้ (randomized and non-sequential) ทั้งนี้ จะต้องมีค่ามากกว่า 0 และขนาดไม่น้อยกว่า 64 บิต [9]	4.2.2
3	signature	m		OID ของอัลกอริทึมจากตัวเลือกดังนี้ ● sha256WithRSAEncryption {1.2.840.113549.1.1.11} ● sha384WithRSAEncryption {1.2.840.113549.1.1.12} ● sha512WithRSAEncryption {1.2.840.113549.1.1.13}	4.2.3
4	issuer	m			4.2.4
4.1	commonName (cn)	m		ชื่อผู้ให้บริการออกใบรับรอง และข้อมูลบ่งบอกถึงระบบบริการ เป็นภาษาอังกฤษ เช่น “XYZ Certification Authority - G1”	
4.2	organizationalUnitName (ou)	o		ชื่อหน่วยงานย่อยในองค์กรของผู้ให้บริการออกใบรับรอง เป็นภาษาอังกฤษ เช่น “XYZ Certification Authority”	
4.3	organizationName (o)	m		ชื่อองค์กรของผู้ให้บริการออกใบรับรอง เป็นภาษาอังกฤษ เช่น “XYZ Corporation”	
4.4	countryName (c)	m		“TH”	
5	validity	m			4.2.5
5.1	notBefore	m		วันและเวลาที่ใบรับรองเริ่มใช้งานได้	
5.2	notAfter	m		วันและเวลาที่ใบรับรองสิ้นสุดการใช้งาน	
6	subject	m			4.2.6
6.1	commonName (cn)	m		ชื่อ เว้นวรรค นามสกุล ของเจ้าของใบรับรอง เป็นภาษาไทย เช่น “สมชาย รักดี” *ยกเว้น ชาวต่างชาติสามารถใช้ชื่อเป็นภาษาอังกฤษได้*	
6.2	givenName	o		ชื่อของเจ้าของใบรับรอง เป็นภาษาอังกฤษ เช่น “Somchai” *กรณีข้อมูลใน commonName เป็นภาษาอังกฤษ ห้ามใช้งานคุณลักษณะนี้*	
6.3	surname (sn)	o		นามสกุลของเจ้าของใบรับรอง เป็นภาษาอังกฤษ เช่น “Rakdee” *กรณีข้อมูลใน commonName เป็นภาษาอังกฤษ ห้ามใช้งานคุณลักษณะนี้*	

Index	Item	M	C	Value	Guide No.
6.4	serialNumber	o		ข้อมูลที่เชื่อมโยงไปยังเจ้าของใบรับรอง โดยไม่เชื่อมโยงไปยังบุคคลอื่น	
6.5	title	o		ตำแหน่งของเจ้าของใบรับรองในองค์กรที่เจ้าของใบรับรองสังกัด เช่น “ผู้จัดการ” หรือ “Manager”	
6.6	organizationalUnitName (ou)	o		ชื่อของหน่วยงานย่อยในองค์กรที่เจ้าของใบรับรองสังกัด เช่น “แผนกไอที” หรือ “IT Division”	
6.7	organizationName (o)	o		ชื่อองค์กรที่เจ้าของใบรับรองสังกัด เช่น “บริษัท เอเอเอ จำกัด” หรือ “AAA Company Limited”	
6.8	organizationIdentifier	o		เลขประจำตัวผู้เสียภาษีอากรขององค์กรที่เจ้าของใบรับรองสังกัด เช่น “1234567890123”	
6.9	country (c)	m		“TH”	
7	subjectPublicKeyInfo	m			4.2.7
7.1	algorithm	m		OID = {1.2.840.113549.1.1.1} (RSA encryption)	
7.2	subjectPublicKey	m		กุญแจสาธารณะชนิด RSA ความยาวอย่างน้อย 2048 บิต	
ฟิลด์เพิ่มเติม (Extension Fields)					
8	authorityKeyIdentifier	m	F	keyIdentifier บรรจุค่าของฟังก์ชัน SHA-1 Hash ของกุญแจสาธารณะที่เป็นคู่กับกุญแจส่วนตัวซึ่งผู้ให้บริการออกใบรับรองใช้ลงลายมือชื่อดิจิทัลเพื่อรับรองใบรับรองนี้	4.2.8.1
9	subjectKeyIdentifier	m	F	keyIdentifier บรรจุค่าของฟังก์ชัน SHA-1 Hash ของ subjectPublicKey ซึ่งอยู่ในฟิลด์ subjectPublicKeyInfo	4.2.8.2
10	keyUsage	m	T	ตั้งค่าตามวัตถุประสงค์ของการใช้งาน ทั้งนี้ สำหรับการใช้งานทั่วไปแนะนำให้ตั้งค่า ดังนี้ (1) สำหรับการลงลายมือชื่อดิจิทัล ให้ตั้งค่าบิต • digitalSignature = 1 และ contentCommitment = 1 (2) สำหรับการเข้ารหัสลับ ให้ตั้งค่าบิต • keyEncipherment = 1 และ/หรือ • dataEncipherment = 1	4.2.8.3
11	certificatePolicies	m	F		4.2.8.4
11.1	policyIdentifier	m		OID ของ Certificate Policy	
11.2	policyQualifiers	m		ระบุอย่างน้อย 1 PolicyQualifierInfo	
11.2.1	PolicyQualifierInfo [1]	m			
11.2.1.1	policyQualifierId	m		OID = {1.3.6.1.5.5.7.2.1}	
11.2.1.2	qualifier	m		cPSuri = HTTP URL ของ Certification Practice Statement	

Index	Item	M	C	Value	Guide No.
11.2.2	PolicyQualifierInfo [2]	o			
11.2.2.1	policyQualifierId	o		OID = {1.3.6.1.5.5.7.2.2}	
11.2.2.2	qualifier	o		userNotice = ข้อความที่แสดง เมื่อใช้ใบรับรอง	
12	subjectAltName	o	F		4.2.8.5
12.1	directoryName	o		ข้อมูลเกี่ยวกับเจ้าของใบรับรอง โดยใช้ชนิดข้อมูลตาม ITU-T X.501 “Name”	
12.2	rfc822Name	o		อีเมลของเจ้าของใบรับรอง	
13	basicConstraints	m	T		4.2.8.6
13.1	cA	m		False	
13.2	pathLenConstraint	nu		ห้ามมีฟิลด์นี้	
14	extKeyUsage	o	F	ใช้เมื่อซอฟต์แวร์ที่ใช้ใบรับรองต้องการใช้ค่าในฟิลด์นี้เท่านั้น	4.2.8.7
15	cRLDistributionPoints	m	F	ระบุอย่างน้อย 1 DistributionPoint	4.2.8.8
15.1	DistributionPoint [1]	m			
15.1.1	distributionPoint	m		HTTP URL ที่สามารถเข้าถึงรายการเพิกถอนใบรับรอง	
15.1.2	reason	nu		ห้ามมีฟิลด์นี้	
15.1.3	cRLIssuer	nu		ห้ามมีฟิลด์นี้	
16	authorityInfoAccess	m	F	ระบุ 2 AccessDescription	4.2.8.9
16.1	AccessDescription [1]	m			
16.1.1	accessMethod	m		OID = {1.3.6.1.5.5.7.48.1}	
16.1.2	accessLocation	m		HTTP URL สำหรับเข้าถึงบริการ OCSP	
16.2	AccessDescription [2]	m			
16.2.1	accessMethod	m		OID = {1.3.6.1.5.5.7.48.2}	
16.2.2	accessLocation	m		HTTP URL สำหรับเข้าถึงรายการใบรับรองของผู้ให้บริการออกใบรับรอง	

4.3.3.2 ใบรับรองสำหรับนิติบุคคล

ใบรับรองสำหรับนิติบุคคล คือ ใบรับรองที่ใช้ในกรณีผู้รับผิดชอบทางธุรกรรมเป็นนิติบุคคล มีรายละเอียดการกำหนดข้อมูลตามตารางที่ 11

ตารางที่ 11 การกำหนดข้อมูลในใบรับรองสำหรับนิติบุคคล

Index	Item	M	C	Value	Guide No.
ฟิลด์พื้นฐาน (Basic Fields)					
1	version	m		2 (Version 3)	4.2.1
2	serialNumber	m		ตัวเลขที่ไม่ซ้ำกันระหว่างใบรับรองภายใต้ผู้ให้บริการออกใบรับรองรายเดียวกัน โดยเป็นตัวเลขแบบสุ่มและไม่เรียงกันเมื่อเทียบกับใบรับรองที่ออกก่อนหน้าและต่อจากใบนี้ (randomized and non-sequential) ทั้งนี้ จะต้องมีค่ามากกว่า 0 และขนาดไม่น้อยกว่า 64 บิต [9]	4.2.2
3	signature	m		OID ของอัลกอริทึมจากตัวเลือกดังนี้ ● sha256WithRSAEncryption {1.2.840.113549.1.1.11} ● sha384WithRSAEncryption {1.2.840.113549.1.1.12} ● sha512WithRSAEncryption {1.2.840.113549.1.1.13}	4.2.3
4	issuer	m			4.2.4
4.1	commonName (cn)	m		ชื่อผู้ให้บริการออกใบรับรอง และข้อมูลบ่งบอกถึงระบบบริการ เป็นภาษาอังกฤษ เช่น “XYZ Certification Authority - G1”	
4.2	organizationalUnitName (ou)	o		ชื่อหน่วยงานย่อยในองค์กรของผู้ให้บริการออกใบรับรอง เป็นภาษาอังกฤษ เช่น “XYZ Certification Authority”	
4.3	organizationName (o)	m		ชื่อองค์กรของผู้ให้บริการออกใบรับรอง เป็นภาษาอังกฤษ เช่น “XYZ Corporation”	
4.4	countryName (c)	m		“TH”	
5	validity	m			4.2.5
5.1	notBefore	m		วันและเวลาที่ใบรับรองเริ่มใช้งานได้	
5.2	notAfter	m		วันและเวลาที่ใบรับรองสิ้นสุดการใช้งาน	
6	subject	m			4.2.6
6.1	commonName (cn)	m		ชื่อนิติบุคคล เป็นภาษาไทย เช่น “บริษัท เอเอเอ จำกัด” *ยกเว้น นิติบุคคลต่างชาติสามารถใช้ชื่อเป็นภาษาอังกฤษได้*	
6.2	givenName	o		ชื่อของผู้แทนของนิติบุคคลหรือผู้มีอำนาจทำการแทนนิติบุคคล เช่น “สมชาย” หรือ “Somchai”	
6.3	surname (sn)	o		นามสกุลของผู้แทนของนิติบุคคลหรือผู้มีอำนาจทำการแทนนิติบุคคล เช่น “รักดี” หรือ “Rakdee”	
6.4	serialNumber	o		ข้อมูลที่เชื่อมโยงไปยังเจ้าของใบรับรอง โดยไม่เชื่อมโยงไปยังบุคคลอื่น	
6.5	title	o		ตำแหน่งของผู้แทนของนิติบุคคลหรือผู้มีอำนาจทำการแทนนิติบุคคล เช่น “กรรมการผู้จัดการ” หรือ “Managing Director”	

Index	Item	M	C	Value	Guide No.
6.6	organizationalUnitName (ou)	o		ชื่อของหน่วยงานย่อยของนิติบุคคลที่ผู้แทนของนิติบุคคลหรือผู้มีอำนาจทำการแทนนิติบุคคลสังกัด เช่น “ฝ่ายบริหาร”	
6.7	organizationName (o)	o		ชื่อนิติบุคคล เป็นภาษาอังกฤษ เช่น “AAA Company Limited” *กรณีข้อมูลใน commonName เป็นภาษาอังกฤษ ห้ามใช้งานคุณลักษณะนี้*	
6.8	organizationIdentifier	m		เลขประจำตัวผู้เสียภาษีอากรของนิติบุคคล เช่น “1234567890123”	
6.9	localityName (L)	o		อำเภอหรือเขตที่อยู่ของนิติบุคคล เช่น “หลักสี่” หรือ “Lak Si”	
6.10	stateOrProvinceName (S)	o		จังหวัดที่อยู่ของนิติบุคคล เช่น “กรุงเทพ” หรือ “Bangkok”	
6.11	country (c)	m		“TH”	
7	subjectPublicKeyInfo	m			4.2.7
7.1	Algorithm	m		OID = {1.2.840.113549.1.1.1} (RSA encryption)	
7.2	subjectPublicKey	m		กุญแจสาธารณะชนิด RSA ความยาวอย่างน้อย 2048 บิต	
ฟิลด์เพิ่มเติม (Extension Fields)					
8	authorityKeyIdentifier	m	F	keyIdentifier บรรจุค่าของฟังก์ชัน SHA-1 Hash ของกุญแจสาธารณะที่เป็นคู่กับกุญแจส่วนตัวซึ่งผู้ให้บริการออกใบรับรองใช้ลงลายมือชื่อดิจิทัลเพื่อรับรองใบรับรองนี้	4.2.8.1
9	subjectKeyIdentifier	m	F	keyIdentifier บรรจุค่าของฟังก์ชัน SHA-1 Hash ของ subjectPublicKey ซึ่งอยู่ในฟิลด์ subjectPublicKeyInfo	4.2.8.2
10	keyUsage	m	T	ตั้งค่าตามวัตถุประสงค์ของการใช้งาน ทั้งนี้ สำหรับการใช้งานทั่วไปแนะนำให้ตั้งค่า ดังนี้ (1) สำหรับการลงลายมือชื่อดิจิทัล ให้ตั้งค่าบิต • digitalSignature = 1 และ contentCommitment = 1 (2) สำหรับการเข้ารหัสลับ ให้ตั้งค่าบิต • keyEncipherment = 1 และ/หรือ • dataEncipherment = 1	4.2.8.3
11	certificatePolicies	m	F		4.2.8.4
11.1	policyIdentifier	m		OID ของ Certificate Policy	
11.2	policyQualifiers	m		ระบุอย่างน้อย 1 PolicyQualifierInfo	
11.2.1	PolicyQualifierInfo [1]	m			
11.2.1.1	policyQualifierId	m		OID = {1.3.6.1.5.5.7.2.1}	
11.2.1.2	qualifier	m		cPSuri = HTTP URL ของ Certification Practice Statement	

Index	Item	M	C	Value	Guide No.
11.2.2	PolicyQualifierInfo [2]	o			
11.2.2.1	policyQualifierId	o		OID = {1.3.6.1.5.5.7.2.2}	
11.2.2.2	qualifier	o		userNotice = ข้อความที่แสดง เมื่อใช้ใบรับรอง	
12	subjectAltName	o	F		4.2.8.5
12.1	directoryName	o		ข้อมูลเกี่ยวกับนิติบุคคลซึ่งเป็นเจ้าของใบรับรอง โดยใช้ชนิดข้อมูลตาม ITU-T X.501 “Name”	
12.2	rfc822Name	o		อีเมลสำหรับติดต่อนิติบุคคล	
13	basicConstraints	m	T		4.2.8.6
13.1	cA	m		False	
13.2	pathLenConstraint	nu		ห้ามมีฟิลด์นี้	
14	extKeyUsage	o	F	ใช้เมื่อซอฟต์แวร์ที่ใช้ใบรับรองต้องการใช้ค่าในฟิลด์นี้เท่านั้น	4.2.8.7
15	cRLDistributionPoints	m	F	ระบุอย่างน้อย 1 DistributionPoint	4.2.8.8
15.1	DistributionPoint [1]	m			
15.1.1	distributionPoint	m		HTTP URL ที่สามารถเข้าถึงรายการเพิกถอนใบรับรอง	
15.1.2	Reason	nu		ห้ามมีฟิลด์นี้	
15.1.3	cRLIssuer	nu		ห้ามมีฟิลด์นี้	
16	authorityInfoAccess	m	F	ระบุ 2 AccessDescription	4.2.8.9
16.1	AccessDescription [1]	m			
16.1.1	accessMethod	m		OID = {1.3.6.1.5.5.7.48.1}	
16.1.2	accessLocation	m		HTTP URL สำหรับเข้าถึงบริการ OCSP	
16.2	AccessDescription [2]	m			
16.2.1	accessMethod	m		OID = {1.3.6.1.5.5.7.48.2}	
16.2.2	accessLocation	m		HTTP URL สำหรับเข้าถึงรายการใบรับรองของผู้ให้บริการออกใบรับรอง	

4.3.3.3 ใบรับรองสำหรับลงลายมือชื่อดิจิทัลโดยระบบให้บริการ

ใบรับรองสำหรับลงลายมือชื่อดิจิทัลโดยระบบให้บริการ คือ ใบรับรองที่ผู้ให้บริการออกใบรับรองออกให้กับนิติบุคคลเพื่อใช้สำหรับลงลายมือชื่อดิจิทัลโดยระบบให้บริการ ทั้งนี้ นิติบุคคลจะต้องจัดเก็บข้อมูลผู้รับผิดชอบกุญแจส่วนตัวของระบบให้บริการ

ใบรับรองสำหรับลงลายมือชื่อดิจิทัลโดยระบบให้บริการ มีรายละเอียดการกำหนดข้อมูลตามตารางที่ 12

ตารางที่ 12 การกำหนดข้อมูลในใบรับรองสำหรับลงลายมือชื่อดิจิทัลโดยระบบให้บริการ

Index	Item	M	C	Value	Guide No.
ฟิลด์พื้นฐาน (Basic Fields)					
1	version	m		2 (Version 3)	4.2.1
2	serialNumber	m		ตัวเลขที่ไม่ซ้ำกันระหว่างใบรับรองภายใต้ผู้ให้บริการออกใบรับรองรายเดียวกัน โดยเป็นตัวเลขแบบสุ่มและไม่เรียงกันเมื่อเทียบกับใบรับรองที่ออกก่อนหน้าและต่อจากใบนี้ (randomized and non-sequential) ทั้งนี้ จะต้องมีค่ามากกว่า 0 และขนาดไม่น้อยกว่า 64 บิต [9]	4.2.2
3	signature	m		OID ของอัลกอริทึมจากตัวเลือกดังนี้ ● sha256WithRSAEncryption {1.2.840.113549.1.1.11} ● sha384WithRSAEncryption {1.2.840.113549.1.1.12} ● sha512WithRSAEncryption {1.2.840.113549.1.1.13}	4.2.3
4	issuer	m			4.2.4
4.1	commonName (cn)	m		ชื่อผู้ให้บริการออกใบรับรอง และข้อมูลบ่งบอกถึงระบบบริการ เป็นภาษาอังกฤษ เช่น “XYZ Certification Authority - G1”	
4.2	organizationalUnitName (ou)	o		ชื่อหน่วยงานย่อยในองค์กรของผู้ให้บริการออกใบรับรอง เป็นภาษาอังกฤษ เช่น “XYZ Certification Authority”	
4.3	organizationName (o)	m		ชื่อองค์กรของผู้ให้บริการออกใบรับรอง เป็นภาษาอังกฤษ เช่น “XYZ Corporation”	
4.4	countryName (c)	m		“TH”	
5	validity	m			4.2.5
5.1	notBefore	m		วันและเวลาที่ใบรับรองเริ่มใช้งานได้	
5.2	notAfter	m		วันและเวลาที่ใบรับรองสิ้นสุดการใช้งาน	
6	subject	m			4.2.6
6.1	commonName (cn)	m		ชื่อของระบบให้บริการ เช่น “Tax Invoice Service” หรือ “บริการใบกำกับภาษี”	
6.2	serialNumber	o		ตัวเลขที่ไม่ซ้ำกันระหว่างใบรับรองอิเล็กทรอนิกส์ที่ใช้งานภายใต้ระบบให้บริการเดียวกัน	
6.3	organizationalUnitName (ou)	o		ชื่อของหน่วยงานย่อยของนิติบุคคลที่ให้บริการระบบ เช่น “สำนักทะเบียน” หรือ “Office of the Registrar”	
6.4	organizationName (o)	m		ชื่อนิติบุคคลที่ให้บริการระบบ เป็นภาษาไทย เช่น “บริษัท เอเอเอ จำกัด”	
6.5	organizationIdentifier	m		เลขประจำตัวผู้เสียภาษีอากรของนิติบุคคลที่ให้บริการระบบ เช่น “1234567890123”	
6.6	localityName (L)	o		อำเภอหรือเขตที่อยู่ของนิติบุคคลที่ให้บริการระบบ เช่น “หลักสี่” หรือ “Lak Si”	

Index	Item	M	C	Value	Guide No.
6.7	stateOrProvinceName (S)	o		จังหวัดที่อยู่ของนิติบุคคลที่ให้บริการระบบ เช่น “กรุงเทพ” หรือ “Bangkok”	
6.8	country (c)	m		“TH”	
7	subjectPublicKeyInfo	m			4.2.7
7.1	Algorithm	m		OID = {1.2.840.113549.1.1.1} (RSA encryption)	
7.2	subjectPublicKey	m		กุญแจสาธารณะชนิด RSA ความยาวอย่างน้อย 2048 บิต	
ฟิลด์เพิ่มเติม (Extension Fields)					
8	authorityKeyIdentifier	m	F	keyIdentifier บรรจุค่าของฟังก์ชัน SHA-1 Hash ของกุญแจสาธารณะที่เป็นคู่กับกุญแจส่วนตัวซึ่งผู้ให้บริการออกใบรับรองใช้ลงลายมือชื่อดิจิทัลเพื่อรับรองใบรับรองนี้	4.2.8.1
9	subjectKeyIdentifier	m	F	keyIdentifier บรรจุค่าของฟังก์ชัน SHA-1 Hash ของ subjectPublicKey ซึ่งอยู่ในฟิลด์ subjectPublicKeyInfo	4.2.8.2
10	keyUsage	m	T	digitalSignature = 1 และ contentCommitment = 1	4.2.8.3
11	certificatePolicies	m	F		4.2.8.4
11.1	policyIdentifier	m		OID ของ Certificate Policy	
11.2	policyQualifiers	m		ระบุอย่างน้อย 1 PolicyQualifierInfo	
11.2.1	PolicyQualifierInfo [1]	m			
11.2.1.1	policyQualifierId	m		OID = {1.3.6.1.5.5.7.2.1}	
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		OID = {1.3.6.1.5.5.7.2.2}	
11.2.2.2	qualifier	o		userNotice = ข้อความที่แสดง เมื่อใช้ใบรับรอง	
12	subjectAltName	o	F		4.2.8.5
12.1	rfc822Name	o		อีเมลสำหรับติดต่อเจ้าหน้าที่ของระบบให้บริการ	
13	basicConstraints	m	T		4.2.8.6
13.1	cA	m		False	
13.2	pathLenConstraint	nu		ห้ามมีฟิลด์นี้	
14	extKeyUsage	o	F	ใช้เมื่อซอฟต์แวร์ที่ใช้ใบรับรองต้องการใช้ค่าในฟิลด์นี้เท่านั้น	4.2.8.7
15	cRLDistributionPoints	m	F	ระบุอย่างน้อย 1 DistributionPoint	4.2.8.8
15.1	DistributionPoint [1]	m			
15.1.1	distributionPoint	m		HTTP URL ที่สามารถเข้าถึงรายการเพิกถอนใบรับรอง	
15.1.2	Reason	nu		ห้ามมีฟิลด์นี้	
15.1.3	cRLIssuer	nu		ห้ามมีฟิลด์นี้	

Index	Item	M	C	Value	Guide No.
16	authorityInfoAccess	m	F	ระบุ 2 AccessDescription	4.2.8.9
16.1	AccessDescription [1]	m			
16.1.1	accessMethod	m		OID = {1.3.6.1.5.5.7.48.1}	
16.1.2	accessLocation	m		HTTP URL สำหรับเข้าถึงบริการ OCSP	
16.2	AccessDescription [2]	m			
16.2.1	accessMethod	m		OID = {1.3.6.1.5.5.7.48.2}	
16.2.2	accessLocation	m		HTTP URL สำหรับเข้าถึงรายการใบรับรองของผู้ให้บริการออกใบรับรอง	

4.3.3.4 ใบรับรองสำหรับโปรโตคอล SSL/TLS หรือโปรโตคอลอื่น ๆ

ใบรับรองสำหรับโปรโตคอล SSL/TLS หรือโปรโตคอลอื่น ๆ คือ ใบรับรองที่ผู้ให้บริการออกใบรับรองออกให้กับบุคคลธรรมดาหรือนิติบุคคลเพื่อใช้รักษาความปลอดภัยในการเข้าถึงระบบให้บริการ ด้วยโปรโตคอล SSL/TLS หรือโปรโตคอลอื่น ๆ การกำหนดข้อมูลของใบรับรองประเภทนี้จะอ้างอิงตาม Baseline Requirement ของ CA/Browser Forum [9]

การกำหนดข้อมูลในใบรับรองสำหรับโปรโตคอล SSL/TLS หรือโปรโตคอลอื่น ๆ มีรายละเอียดตามตารางที่ 13 โดยข้อมูลในฟิลด์ issuer และฟิลด์ subject ใช้การเข้ารหัสแบบ PrintableString เท่านั้น

ตารางที่ 13 การกำหนดข้อมูลในใบรับรองสำหรับโปรโตคอล SSL/TLS หรือโปรโตคอลอื่น ๆ

Index	Item	M	C	Value	Guide No.
ฟิลด์พื้นฐาน (Basic Fields)					
1	version	m		2 (Version 3)	4.2.1
2	serialNumber	m		ตัวเลขที่ไม่ซ้ำกันระหว่างใบรับรองภายใต้ผู้ให้บริการออกใบรับรองรายเดียวกัน โดยเป็นตัวเลขแบบสุ่มและไม่เรียงกันเมื่อเทียบกับใบรับรองที่ออกก่อนหน้าและต่อจากใบนี้ (randomized and non-sequential) ทั้งนี้ จะต้องมีค่ามากกว่า 0 และขนาดไม่น้อยกว่า 64 บิต [9]	4.2.2
3	signature	m		OID ของอัลกอริทึมจากตัวเลือกดังนี้ ● sha256WithRSAEncryption {1.2.840.113549.1.1.11} ● sha384WithRSAEncryption {1.2.840.113549.1.1.12} ● sha512WithRSAEncryption {1.2.840.113549.1.1.13}	4.2.3

Index	Item	M	C	Value	Guide No.
4	issuer	m			4.2.4
4.1	commonName (cn)	m		ชื่อผู้ให้บริการออกใบรับรอง และข้อมูลบ่งบอกถึงระบบบริการ เป็นภาษาอังกฤษ เช่น “XYZ Certification Authority - G1”	
4.2	organizationalUnitName (ou)	o		ชื่อหน่วยงานย่อยในองค์กรของผู้ให้บริการออกใบรับรอง เป็นภาษาอังกฤษ เช่น “XYZ Certification Authority”	
4.3	organizationName (o)	m		ชื่อองค์กรของผู้ให้บริการออกใบรับรอง เป็นภาษาอังกฤษ เช่น “XYZ Corporation”	
4.4	countryName (c)	m		“TH”	
5	validity	m			4.2.5
5.1	notBefore	m		วันและเวลาที่ใบรับรองเริ่มใช้งานได้	
5.2	notAfter	m		วันและเวลาที่ใบรับรองสิ้นสุดการใช้งาน	
6	subject	m			4.2.6
6.1	commonName (cn)	m		URL หรือ IP Address ของ server เช่น “www.aaa.com”	
6.2	organizationalUnitName (ou)	o		ชื่อของหน่วยงานย่อยในนิติบุคคลซึ่งเป็นเจ้าของ server เป็นภาษาอังกฤษ เช่น “IT Department”	
6.3	organizationName (o)	o		ชื่อนิติบุคคลซึ่งเป็นเจ้าของ server เป็นภาษาอังกฤษ เช่น “AAA Public Company Limited”	
6.4	localityName (L)	o		อำเภอหรือเขตที่อยู่ของเจ้าของ server เป็นภาษาอังกฤษ เช่น “Chatuchak”	
6.5	stateOrProvinceName (S)	m		จังหวัดที่อยู่ของเจ้าของ server เป็นภาษาอังกฤษ เช่น “Bangkok”	
6.6	country (c)	m		“TH”	
7	subjectPublicKeyInfo	m			4.2.7
7.1	Algorithm	m		OID = {1.2.840.113549.1.1.1} (RSA encryption)	
7.2	subjectPublicKey	m		กุญแจสาธารณะชนิด RSA ความยาวอย่างน้อย 2048 บิต	
ฟิลด์เพิ่มเติม (Extension Fields)					
8	authorityKeyIdentifier	m	F	keyIdentifier บรรจุค่าของฟังก์ชัน SHA-1 Hash ของกุญแจสาธารณะที่เป็นคู่กับกุญแจส่วนตัวซึ่งผู้ให้บริการออกใบรับรองใช้ลงลายมือชื่อดิจิทัลเพื่อรับรองใบรับรองนี้	4.2.8.1
9	subjectKeyIdentifier	m	F	keyIdentifier บรรจุค่าของฟังก์ชัน SHA-1 Hash ของ subjectPublicKey ซึ่งอยู่ในฟิลด์ subjectPublicKeyInfo	4.2.8.2
10	keyUsage	m	T	ตั้งค่าตามวัตถุประสงค์ของการใช้งาน ทั้งนี้ การใช้งานสำหรับเว็บไซต์ทั่วไปจะมีค่าบิต digitalSignature = 1 และ keyEncipherment = 1	4.2.8.3

Index	Item	M	C	Value	Guide No.
11	certificatePolicies	m	F		4.2.8.4
11.1	policyIdentifier	m		OID ของ Certificate Policy	
11.2	policyQualifiers	m		ระบุอย่างน้อย 1 PolicyQualifierInfo	
11.2.1	PolicyQualifierInfo [1]	m			
11.2.1.1	policyQualifierId	m		OID = {1.3.6.1.5.5.7.2.1}	
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		OID = {1.3.6.1.5.5.7.2.2}	
11.2.2.2	qualifier	o		userNotice = ข้อความที่แสดง เมื่อใช้ใบรับรอง	
12	subjectAltName	o	F		4.2.8.5
12.1	dNSName	o		ชื่อ Domain Name	
12.2	iPAddress	o		IP address	
13	basicConstraints	m	T		4.2.8.6
13.1	cA	m		False	
13.2	pathLenConstraint	nu		ห้ามมีฟิลด์นี้	
14	extKeyUsage	m	F	กำหนดค่าตามเงื่อนไข ดังนี้ [9] (1) ระบุค่าใดค่าหนึ่งของ id-kp-serverAuth หรือ id-kp-clientAuth หรือทั้งคู่ (2) id-kp-emailProtection สามารถเลือกใช้งานได้ (3) ค่าอื่น ๆ นอกเหนือจาก (1) และ (2) ไม่สามารถใช้งานได้ ทั้งนี้ การใช้งานสำหรับเว็บไซต์ทั่วไป แนะนำให้ระบุค่าเป็น id-kp-serverAuth และ id-kp-clientAuth	4.2.8.7
15	cRLDistributionPoints	m	F	ระบุอย่างน้อย 1 DistributionPoint	4.2.8.8
15.1	DistributionPoint [1]	m			
15.1.1	distributionPoint	m		HTTP URL ที่สามารถเข้าถึงรายการเพิกถอนใบรับรอง	
15.1.2	Reason	nu		ห้ามมีฟิลด์นี้	
15.1.3	cRLIssuer	nu		ห้ามมีฟิลด์นี้	
16	authorityInfoAccess	m	F	ระบุ 2 AccessDescription	4.2.8.9
16.1	AccessDescription [1]	m			
16.1.1	accessMethod	m		OID = {1.3.6.1.5.5.7.48.1}	
16.1.2	accessLocation	m		HTTP URL สำหรับเข้าถึงบริการ OCSP	
16.2	AccessDescription [2]	m			
16.2.1	accessMethod	m		OID = {1.3.6.1.5.5.7.48.2}	
16.2.2	accessLocation	m		HTTP URL สำหรับเข้าถึงรายการใบรับรองของผู้ให้บริการออกใบรับรอง	

5. การกำหนดข้อมูลในรายการเพิกถอนใบรับรอง

การกำหนดข้อมูลในรายการเพิกถอนใบรับรองตามข้อเสนอแนะมาตรฐานฉบับนี้อ้างอิงกับ RFC 5280 โดยมีรายละเอียดดังนี้

5.1 โครงสร้างของรายการเพิกถอนใบรับรอง

RFC 5280 กำหนดโครงสร้างของรายการเพิกถอนใบรับรอง X.509 เวอร์ชัน 2 ดังนี้

```
CertificateList  ::= SEQUENCE  {
    tbsCertList                 TBSCertList,
    signatureAlgorithm          AlgorithmIdentifier,
    signatureValue              BIT STRING }
```

โครงสร้างพื้นฐานข้างต้นแสดงให้เห็นว่ารายการเพิกถอนใบรับรอง (CertificateList) ประกอบด้วยฟิลด์ข้อมูล 3 ฟิลด์ คือ

(1) tbsCertList : แสดงข้อมูลในรายการเพิกถอนใบรับรอง ซึ่งประกอบด้วย ข้อมูลของผู้ออกรายการเพิกถอนใบรับรอง วันที่ออกรายการเพิกถอนใบรับรองนี้ วันที่จะออกรายการเพิกถอนใบรับรองครั้งต่อไป รายการใบรับรองที่ถูกเพิกถอน (ถ้ามี) และฟิลด์เพิ่มเติม (ถ้ามี)

(2) signatureAlgorithm : แสดงข้อมูลอัลกอริทึมที่ผู้ให้บริการออกใบรับรองใช้ลงลายมือชื่อดิจิทัลเพื่อรับรองข้อมูลใน tbsCertList

(3) signatureValue : แสดงลายมือชื่อดิจิทัลที่สร้างขึ้นโดยผู้ให้บริการออกใบรับรองเพื่อรับรองความถูกต้องของข้อมูลในฟิลด์ tbsCertList

5.2 ข้อมูลในรายการเพิกถอนใบรับรอง

ข้อมูลในรายการเพิกถอนใบรับรอง ถูกบรรจุอยู่ในฟิลด์ที่ชื่อว่า “TBSCertList” ซึ่งเป็นฟิลด์ที่มีข้อมูลเกี่ยวกับผู้ให้บริการออกใบรับรองที่ออกรายการเพิกถอนใบรับรองนี้ อัลกอริทึมที่ใช้ลงนามในรายการเพิกถอนใบรับรอง วันและเวลาที่ออกรายการเพิกถอนใบรับรองนี้ รวมถึงวันและเวลาที่จะออกรายการเพิกถอนใบรับรองครั้งต่อไป

โครงสร้างข้อมูลในรายการเพิกถอนใบรับรอง หรือ ฟิลด์ tbsCertList ตาม RFC 5280 มีดังนี้

```
TBSCertList  ::=  SEQUENCE  {
    version                     Version OPTIONAL,
                                -- if present, MUST be v2
    signature                   AlgorithmIdentifier,
    issuer                      Name,
    thisUpdate                  Time,
    nextUpdate                  Time OPTIONAL,
```

revokedCertificates *SEQUENCE OF SEQUENCE {*
userCertificate *CertificateSerialNumber,*
revocationDate *Time,*
crlEntryExtensions *Extensions OPTIONAL*
-- if present, version MUST be v2
} OPTIONAL,
crlExtensions *[0]* *EXPLICIT Extensions OPTIONAL*
-- if present, version MUST be v2 }

-- Version, Time, CertificateSerialNumber, และ Extensions

-- มีโครงสร้างข้อมูลตามรูปแบบ ASN.1 ในข้อ 5.1

-- AlgorithmIdentifier โครงสร้างข้อมูลตามรูปแบบ ASN.1 ในข้อ 5.2.2

5.2.1 version

ฟิลด์ version แสดงข้อมูลเวอร์ชันของรายการเพิกถอนใบรับรอง ซึ่งต้องระบุเป็นเวอร์ชัน 2 (ระบุค่าเป็น 1) เพื่อรองรับการใช้งานฟิลด์เพิ่มเติม ทั้งนี้ นิยามของชนิดข้อมูล Version เป็นไปตามข้อ 4.2.1

5.2.2 signature

ฟิลด์ signature แสดง Algorithm Identifier ซึ่งประกอบด้วยหมายเลข Object Identifier (OID) ของอัลกอลิทึมและค่าพารามิเตอร์ (ถ้ามี) ที่ผู้ให้บริการออกใบรับรองใช้ลงลายมือชื่อเพื่อรับรองข้อมูลในรายการเพิกถอนใบรับรอง ทั้งนี้ นิยามของชนิดข้อมูล AlgorithmIdentifier เป็นไปตามข้อ 4.2.3 และอัลกอริทึมที่ใช้จะต้องเลือกจากรายการอัลกอริทึมในตารางที่ 14

ตารางที่ 14 อัลกอริทึมที่ใช้ในการลงลายมือชื่อดิจิทัลบนรายการเพิกถอนใบรับรอง

ลำดับ	อัลกอริทึมที่ใช้ในการลงลายมือชื่อดิจิทัล	Object Identifier (OID)
1	sha256WithRSAEncryption	1.2.840.113549.1.1.11
2	sha384WithRSAEncryption	1.2.840.113549.1.1.12
3	sha512WithRSAEncryption	1.2.840.113549.1.1.13

5.2.3 issuer

ฟิลด์ issuer แสดงข้อมูลระบุเอนทิตีที่เป็นผู้ที่ออกรายการเพิกถอนใบรับรองรายการนี้ โดยใช้ชนิดข้อมูลตาม ITU-T X.501 “Name” [6] ทั้งนี้ ข้อมูลในฟิลด์ issuer ใช้การเข้ารหัสแบบ PrintableString โดยจะต้องประกอบด้วยคุณลักษณะตามตารางที่ 15

ตารางที่ 15 คุณลักษณะของฟิลด์ issuer ในรายการเพิกถอนใบรับรอง

คุณลักษณะ	คำอธิบาย
commonName (cn)	ชื่อผู้ให้บริการออกใบรับรอง และข้อมูลบ่งบอกถึงระบบบริการ เป็นภาษาอังกฤษ เช่น “ABC CA-G2”
organizationalUnitName (ou)	ชื่อหน่วยงานย่อยในองค์กรของผู้ให้บริการออกใบรับรอง เป็นภาษาอังกฤษ เช่น “ABC CA”
organizationName (o)	ชื่อองค์กรของผู้ให้บริการออกใบรับรอง เป็นภาษาอังกฤษ เช่น “ABC Corporation”
countryName (c)	รหัสประเทศ อยู่ในรูปแบบ 2 ตัวอักษรตามที่กำหนดใน ISO 3166-1 คือ “TH”

5.2.4 thisUpdate

ฟิลด์ thisUpdate แสดงข้อมูลวันและเวลาที่ออกรายการเพิกถอนใบรับรองนี้ โดยสามารถระบุได้ 2 แบบ คือ UTCTime และ GeneralizedTime (รายละเอียดตามข้อ 4.2.5) ทั้งนี้ ให้ระบุค่า thisUpdate เป็น UTCTime จนถึงปี ค.ศ. 2049 และเป็น GeneralizedTime สำหรับปี ค.ศ. 2050 เป็นต้นไป

5.2.5 nextUpdate

ฟิลด์ thisUpdate แสดงข้อมูลวันและเวลาที่รายการเพิกถอนใบรับรองจะถูกออกในครั้งถัดไป ซึ่งผู้ให้บริการออกใบรับรองจะต้องออกรายการเพิกถอนใบรับรองใหม่ก่อนถึงเวลาที่ระบุในฟิลด์นี้ โดยวันและเวลาสามารถระบุได้ 2 แบบคือ UTCTime และ GeneralizedTime (รายละเอียดตามข้อ 4.2.5) ทั้งนี้ ให้ระบุค่า nextUpdate เป็น UTCTime จนถึงปี ค.ศ. 2049 และเป็น GeneralizedTime สำหรับปี ค.ศ. 2050 เป็นต้นไป

5.2.6 revokedCertificates

ฟิลด์ revokedCertificates แสดงรายการใบรับรองที่ถูกเพิกถอน กรณีที่ไม่มีใบรับรองถูกเพิกถอน ฟิลด์นี้จะต้องไม่มีข้อมูล

การเพิกถอนใบรับรองทำได้โดยการระบุข้อมูลในฟิลด์ดังต่อไปนี้

5.2.6.1 userCertificate

ฟิลด์ userCertificae แสดงหมายเลข serialNumber ของใบรับรองที่ถูกเพิกถอน

5.2.6.2 revocationDate

ฟิลด์ revocationDate แสดงวันและเวลาที่ใบรับรองถูกเพิกถอนในรูปแบบ UTCTime หรือ GeneralizedTime โดยระบุเป็น UTCTime จนถึงปี ค.ศ. 2049 และเป็น GeneralizedTime สำหรับปี ค.ศ. 2050 เป็นต้นไป

5.2.6.3 crlEntryExtensions

ฟิลด์ crlEntryExtensions แสดงข้อมูลเพิ่มเติมเกี่ยวกับใบรับรองที่ถูกเพิกถอน โดยประกอบด้วยฟิลด์เพิ่มเติมสำคัญ คือ reasonCode และ invalidityDate [4]

(1) reasonCode

reasonCode เป็นฟิลด์เพิ่มเติมที่ใช้ระบุข้อมูลสาเหตุการเพิกถอนใบรับรอง โดยใช้เป็นเลขรหัส (CRLReason) ซึ่ง RFC 5280 นิยามฟิลด์ reasonCode ไว้ดังนี้

id-ce-cRLReasons OBJECT IDENTIFIER ::= { id-ce 21 }
-- reasonCode ::= { CRLReason }

CRLReason ::= ENUMERATED {
unspecified (0),
keyCompromise (1),
cACompromise (2),
affiliationChanged (3),
superseded (4),
cessationOfOperation (5),
certificateHold (6),
-- value 7 is not used
removeFromCRL (8),
privilegeWithdrawn (9),
aACompromise (10)
weakAlgorithmOrKey (11) }

โดยคำอธิบายการระบุข้อมูลในฟิลด์ reasonCode เป็นไปตามตารางที่ 16

ตารางที่ 16 คำอธิบายสาเหตุของการเพิกถอนใบรับรอง

เหตุผลของการเพิกถอน	คำอธิบาย	reasonCode
unspecified	เหตุผลนอกเหนือจากรายการรหัส (Code) ที่มีอยู่	0
keyCompromise	รับรู้ หรือสงสัยว่ากุญแจส่วนตัวของผู้ใช้ถูกล่วงรู้โดยผู้ไม่ได้รับอนุญาต	1
cACompromise	รับรู้ หรือสงสัยว่ากุญแจส่วนตัวของผู้ให้บริการออกใบรับรองถูกล่วงรู้โดยผู้ไม่ได้รับอนุญาต	2
affiliationChanged	มีการเปลี่ยนแปลงข้อมูลในใบรับรอง โดยที่กุญแจส่วนตัวไม่ได้ถูกล่วงรู้โดยผู้ที่ไม่ได้รับอนุญาต	3
superseded	มีการสร้างใบรับรองใหม่แทนใบรับรองฉบับเดิม โดยที่กุญแจส่วนตัวไม่ได้ถูกล่วงรู้โดยผู้ที่ไม่ได้รับอนุญาต	4

เหตุผลของการเพิกถอน	คำอธิบาย	reasonCode
cessationOfOperation	ยกเลิกการใช้งานใบรับรอง โดยที่กุญแจส่วนตัวไม่ได้ถูกล่วงรู้โดยผู้ที่ไม่ได้รับอนุญาต	5
certificateHold	หยุดหรือพักใช้ใบรับรองชั่วคราว	6
removeFromCRL	ข้อมูลใบรับรองถูกเพิกถอนจากรายการเพิกถอนใบรับรอง เนื่องจากใบรับรองหมดอายุหรือยกเลิกการระงับใช้งาน และใช้เฉพาะใน delta CRL เท่านั้น	8
privilegeWithdrawn	สิทธิ์ของเจ้าของใบรับรองถูกถอดถอน	9
aACompromise	รับรู้ หรือสงสัยว่า ข้อมูลของ Attribute Authority ที่รับรอง attribute certificate ถูกล่วงรู้ โดยผู้ที่ไม่ได้รับอนุญาต	10
weakAlgorithmOrKey	คู่กุญแจ หรืออัลกอริทึมที่ใช้สร้างคู่กุญแจมีจุดอ่อน เช่น การสร้างคู่กุญแจไม่ปลอดภัย	11

(2) invalidityDate

invalidityDate เป็นฟิลด์เพิ่มเติมที่ใช้ระบุวันที่รับทราบ หรือเข้าใจว่ากุญแจส่วนตัวถูกล่วงรู้โดยผู้ที่ไม่ได้รับอนุญาต หรือวันที่ใบรับรองไม่สามารถใช้งานได้ โดยวันที่กำหนดในฟิลด์นี้อาจมาก่อนวันที่กำหนดใน revocationDate ของฟิลด์ revokedCertificates

RFC 5280 นิยามฟิลด์ InvalidityDate ดังนี้

id-ce-invalidityDate OBJECT IDENTIFIER ::= { id-ce 24 }

InvalidityDate ::= GeneralizedTime

5.2.7 crlExtensions

crlExtensions เป็นฟิลด์สำหรับแสดงข้อมูลเพิ่มเติมเกี่ยวกับรายการเพิกถอนใบรับรอง โดยฟิลด์เพิ่มเติมภายใต้ crlExtensions สามารถเป็นได้ทั้งฟิลด์เพิ่มเติมที่สำคัญ (critical) และฟิลด์เพิ่มเติมทั่วไป (non-critical) โดยซอฟต์แวร์จะไม่สามารถใช้งานรายการเพิกถอนใบรับรองได้หากพบฟิลด์เพิ่มเติมที่สำคัญ แต่ไม่เข้าใจความหมายหรือไม่สามารถประมวลผลข้อมูลในฟิลด์เพิ่มเติมได้

รายการเพิกถอนใบรับรอง เวอร์ชัน 2 ตาม RFC5280 มีฟิลด์เพิ่มเติมภายใต้ crlExtension ที่จำเป็นต้องระบุคือ authorityKeyIdentifier และ cRLNumber

5.2.7.1 authorityKeyIdentifier

authorityKeyIdentifier เป็นฟิลด์เพิ่มเติมที่ระบุค่าอ้างอิงถึงกุญแจสาธารณะที่เป็นคู่กับกุญแจส่วนตัวที่ผู้ให้บริการออกใบรับรองใช้ลงลายมือชื่อดิจิทัลเพื่อรับรองรายการเพิกถอนใบรับรองรายการนี้ โดย authorityKeyIdentifier มีประโยชน์ในกรณีที่ผู้ให้บริการออกใบรับรองมีกุญแจส่วนตัวสำหรับลงลายมือชื่อดิจิทัลมากกว่า 1 อัน ทั้งนี้ โครงสร้างของฟิลด์ authorityKeyIdentifier เป็นไปตามข้อ 4.2.8.1

5.2.7.2 cRLNumber

cRLNumber เป็นฟิลด์เพิ่มเติมที่แสดงลำดับเลขที่ของรายการเพิกถอนใบรับรอง โดยค่าของ cRLNumber จะเพิ่มขึ้นตามลำดับการออก CRL และมีค่าสูงสุด 20 octets ซึ่ง RFC 5280 นิยามฟิลด์ cRLNumber ดังนี้

id-ce-cRLNumber OBJECT IDENTIFIER ::= { id-ce 20 }

CRLNumber ::= INTEGER (0..MAX)

5.3 ข้อแนะนำในการกำหนดข้อมูลในรายการเพิกถอนใบรับรอง

การกำหนดข้อมูลในรายการเพิกถอนใบรับรองตามข้อเสนอแนะฉบับนี้เป็นไปตามตารางที่ 17 ทั้งนี้ ผู้ออกรายการเพิกถอนใบรับรองสามารถระบุรายละเอียดเพิ่มเติมจากข้อเสนอแนะมาตรฐานฉบับนี้ได้ตามความจำเป็น

ตารางที่ 17 การกำหนดข้อมูลในรายการเพิกถอนใบรับรอง

Index	Item	M	C	Value	Guide No.
ฟิลด์พื้นฐาน (Basic Fields)					
1	version	m		1 (Version 2)	5.2.1
2	signature	m		OID ของอัลกอริทึมจากตัวเลือกดังนี้ ● sha256WithRSAEncryption {1.2.840.113549.1.1.11} ● sha384WithRSAEncryption {1.2.840.113549.1.1.12} ● sha512WithRSAEncryption {1.2.840.113549.1.1.13}	5.2.2
3	issuer	m			5.2.3
3.1	commonName (cn)	m		ชื่อผู้ให้บริการออกใบรับรอง และข้อมูลบ่งบอกถึงระบบบริการ เป็นภาษาอังกฤษ เช่น “XYZ Certification Authority - G1”	
3.2	organizationalUnitName (ou)	o		ชื่อหน่วยงานย่อยในองค์กรของผู้ให้บริการออกใบรับรอง เป็นภาษาอังกฤษ เช่น “XYZ Certification Authority”	
3.3	organizationName (o)	m		ชื่อองค์กรของผู้ให้บริการออกใบรับรอง เป็นภาษาอังกฤษ เช่น “XYZ Corporation”	
3.4	countryName (c)	m		“TH”	
4	thisUpdate	m		วันและเวลาที่ออกรายการเพิกถอนใบรับรองนี้	5.2.4
5	nextUpdate	m		วันและเวลาที่จะออกรายการเพิกถอนใบรับรองครั้งถัดไป	5.2.5
6	revokedCertificate	m			5.2.6
6.1	userCertificate:	m		serialNumber ของใบรับรองที่ถูกเพิกถอน	5.2.6.1
6.2	revocationDate	m		วันและเวลาที่เพิกถอน	5.2.6.2

Index	Item	M	C	Value	Guide No.
6.3	crlEntryExtension				
6.3.1	reasonCode	m	F	ระบุเหตุผลในการเพิกถอนใบรับรองเป็นเลขรหัส	5.2.6.3 (1)(1)
6.3.2	invalidityDate	o	F	วันที่รับรู้หรือเข้าใจว่ากุญแจส่วนตัวถูกล่วงรู้โดยผู้ที่ไม่ได้รับอนุญาต โดยให้ระบุในกรณีที่ reasonCode เป็น keyCompromise หรือ cACompromise เท่านั้น	5.2.6.3 (2)(2)
crlExtensions					
7	authorityKeyIdentifier	m	F	keyIdentifier บรรจุค่าของฟังก์ชัน SHA-1 Hash ของกุญแจสาธารณะที่เป็นคู่กับกุญแจส่วนตัวซึ่งผู้ให้บริการออกใบรับรองใช้ลงลายมือชื่อดิจิทัลเพื่อรับรองรายการเพิกถอนใบรับรองนี้	5.2.7.1
8	cRLNumber	m	F	จำนวนเต็มบวกแสดงลำดับการออกรายการเพิกถอนใบรับรอง	5.2.7.2

ภาคผนวก ก. โครงสร้างความสัมพันธ์ของใบรับรองในประเทศไทย

ใบรับรองภายใต้ผู้ให้บริการออกใบรับรองในประเทศไทยสามารถแบ่งประเภทตามความสัมพันธ์ระหว่างผู้ให้บริการออกใบรับรองและผู้ใช้บริการเป็น 3 ประเภท ดังรูปที่ 1 โดยแต่ละประเภทมีรายละเอียดดังนี้

ก.1 ใบรับรองของผู้ให้บริการออกใบรับรองลำดับชั้นบนสุด (Root CA Certificate)

ใบรับรองของผู้ให้บริการออกใบรับรองลำดับชั้นบนสุด คือ ใบรับรองของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์แห่งชาติ (National Root CA Certificate) ซึ่งลงลายมือเพื่อรับรองตนเอง (Self-signed) ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์แห่งชาติมีหน้าที่ออกใบรับรองให้กับผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา (Subordinate Certification Authority) และมีหน้าที่กำหนดนโยบายการให้บริการของผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา

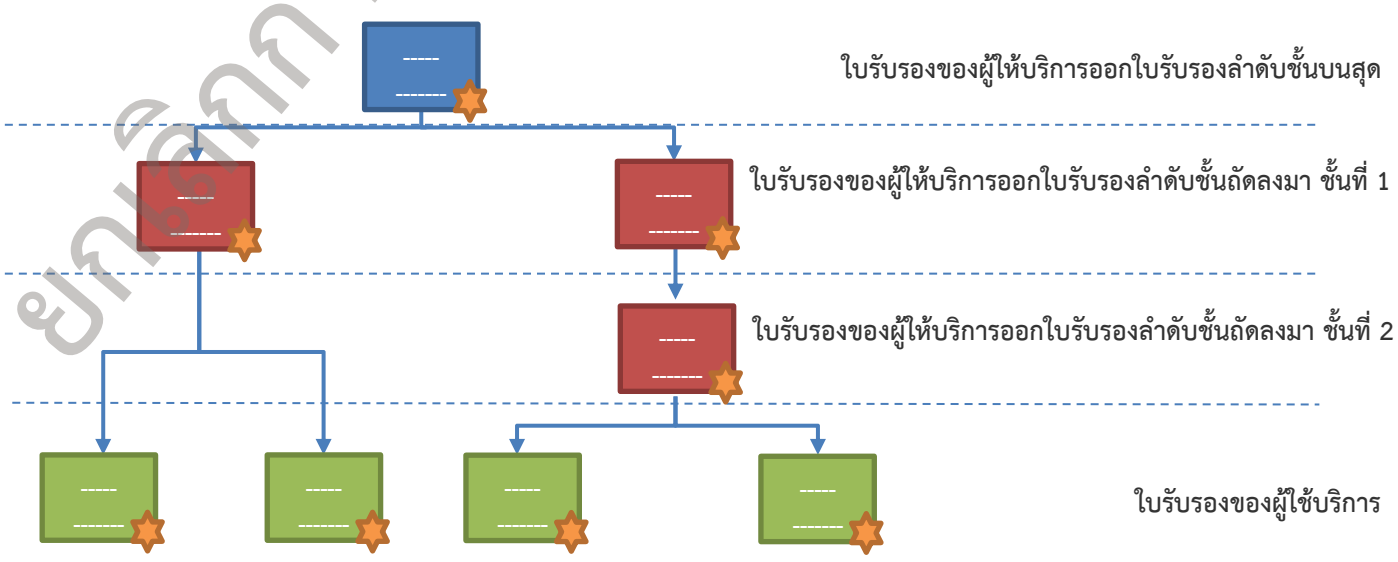
ก.2 ใบรับรองของผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา (Subordinate CA Certificate)

ใบรับรองของผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา คือ ใบรับรองของผู้ให้บริการออกใบรับรองที่ออกให้โดยผู้ให้บริการออกใบรับรองลำดับชั้นบนสุด โดยผู้ให้บริการออกใบรับรองประเภทนี้สามารถออกใบรับรองให้กับผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา หรือใบรับรองของผู้ใช้บริการ

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์แห่งชาติ มีนโยบายให้มีใบรับรองของผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมา ได้ไม่เกิน 2 ชั้น นับตั้งแต่ใบรับรองของผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมาที่ออกโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์แห่งชาติ

ก.3 ใบรับรองของผู้ใช้บริการ (Subscriber Certificate)

ใบรับรองของผู้ใช้บริการ คือ ใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรองลำดับชั้นถัดลงมาเพื่อรับรองข้อมูลตัวตนและความเป็นเจ้าของคู่กุญแจของเอนทิตี โดยใบรับรองของผู้ใช้บริการสามารถใช้งานได้ตามวัตถุประสงค์ที่กำหนดในใบรับรอง เช่น การลงลายมือชื่อดิจิทัล การเข้ารหัสลับ หรือการยืนยันตัวตน เป็นต้น



รูปที่ 1 โครงสร้างความสัมพันธ์ของใบรับรองในประเทศไทย

บรรณานุกรม

[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) พ.ศ. 2551

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

[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. Available: https://tools.ietf.org/html/rfc5280.

[5] Recommendation ITU-T X.680 (2015) | ISO/IEC 8824-1 : 2015 Information Technology - Abstract Syntax Notation One (ASN.1) : Specification of basic notation.

[6] Recommendation ITU-T X.501 (2012) | ISO/IEC 9594-2 : 2014 Information Technology - Open Systems Interconnection – The Directory: Models.

[7] Recommendation ITU-T X.520 (2012) | ISO/IEC 9594-6 : 2014 Information Technology - Open Systems Interconnection – The Directory: Selected attribute types.

[8] P. Geelen, "Microsoft Trusted Root Program Requirements," Microsoft, 16 11 2016. [Online]. Available: https://social.technet.microsoft.com/wiki/contents/articles/31633.microsoft-trusted-root-program-requirements.aspx#E_EKU_Requirements.

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