ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ETDA Recommendation on ICT Standard for Electronic Transactions

ขมธอ. 11-2560

ว่าด้วยการจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์

ELECTRONIC CERTIFICATE

เวอร์ชัน 1.0

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ICS 35.240.30

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์

ขมธอ. 11-2560

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 20 มีนาคม พ.ศ. 2560

คณะทำงานจัดทำร่างข้อเสนอแนะเกี่ยวกับการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

ประธานคณะทำงาน

นายศุภโชค จันทรประทิน	รักษาการผู้อำนวยการสำนักมาตรฐาน สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ผู้ทำงาน

นายกำชัย จัตตานนท์	ผู้แทนกรมศุลกากร
นางสาวขนิษฐา สหเมธาพัฒน์	ผู้แทนกรมสรรพากร
นายธานินทร์ ตันกิติบุตร	บริษัท ไทยเทรดเน็ท จำกัด
นายธิติกร ตระกูลศิริศักดิ์	ผู้แทนสำนักโครงสร้างพื้นฐานสารสนเทศ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
นายพุทธิพร หงษ์สุรกุล	ผู้แทนสำนักวิจัยและพัฒนา สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ผู้ทำงานและเลขานุการ

นายเฉลิมชัย บวรนันท์	ผู้แทนสำนักมาตรฐาน สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อการทำธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ฉบับนี้ จัดทำขึ้นเพื่อกำหนดมาตรฐานและวางแนวทางการจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ให้มีความน่าเชื่อถือ มีผลผูกพันบังคับใช้ทางกฎหมาย และสามารถใช้งานได้เช่นเดียวกับการทำธุรกรรมโดยวิธีการทั่วไปที่เคยปฏิบัติอยู่เดิม โดยพัฒนาตามแนวมาตรฐาน

(1) ISO 19005-3: 2012, Document management -- Electronic document file format for long-term preservation -- Part 3: Use of ISO 32000-1 with support for embedded files (PDF/A-3)

(2) ETSI TS 102 778-2 V1.2.1, Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1

(3) ISO 16684-1:2012, Graphic technology -- Extensible metadata platform (XMP) specification -- Part 1: Data model, serialization and core properties

โดยมีการนำเสนอและรับฟังความคิดเห็นเป็นการทั่วไป ตลอดจนพิจารณาข้อมูล ข้อสังเกต ข้อคิดเห็นจากผู้ทรงคุณวุฒิและจากหน่วยงานที่เกี่ยวข้อง เพื่อปรับปรุงให้ข้อเสนอแนะเกี่ยวกับมาตรฐานฉบับนี้มีความสมบูรณ์ครบถ้วนยิ่งขึ้น รวมทั้งให้สามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพ

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ฉบับนี้ จัดทำขึ้นโดยสำนักวิจัยและพัฒนา ภายใต้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

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

คำนำ

หนังสือรับรองเป็นรูปแบบหนึ่งของหนังสือที่ทุกหน่วยงานทั้งภาครัฐและเอกชนต่างก็ต้องมีความจำเป็นในการออกหนังสือดังกล่าว ตัวอย่างเช่น หนังสือรับรองนิติบุคคลที่ออกโดยกระทรวงพาณิชย์ หนังสือรับรองการอนุญาตการผลิตและนำเข้าอาหารที่ออกโดยสำนักงานคณะกรรมการอาหารและยา หนังสือรับรองการทำงานที่ออกโดยนายจ้าง หนังสือรับรองฐานะทางการเงินที่ออกโดยธนาคารพาณิชย์ หนังสือรับรองการถือครองหลักทรัพย์ที่ออกโดยบริษัทหลักทรัพย์ เป็นต้น

โดยหนังสือรับรองที่ออกในปัจจุบันล้วนแล้วแต่ออกในรูปแบบกระดาษ ซึ่งจัดทำด้วยการพิมพ์ข้อความในคอมพิวเตอร์แล้วพิมพ์ออกในรูปแบบกระดาษ จากนั้นจึงทำการลงลายมือชื่อในหนังสือรับรองโดยผู้มีอำนาจกระทำการแทนหน่วยงานเพื่อรับรองเอกสารดังกล่าว สำหรับกรณีที่ต้องมีการออกหนังสือรับรองจำนวนมากในคราวเดียวอาจมีการใช้ภาพลายมือชื่อแทนการลงลายมือชื่อด้วยปากกาเพื่อลดเวลาในการดำเนินการออกหนังสือรับรอง จากนั้นจึงดำเนินการจัดส่งไปยังผู้ร้องขอหรือผู้รับปลายทางแล้วแต่กรณี ซึ่งในบางกรณีการดำเนินการดังกล่าวข้างต้นจำเป็นต้องมีค่าใช้จ่ายต่อหนังสือรับรองหนึ่งฉบับที่สูง เนื่องจากจำเป็นต้องใช้กระดาษที่มีคุณสมบัติพิเศษซึ่งมีมูลค่าสูงเพื่อป้องกันการปลอมแปลง อีกทั้งยังมีค่าใช้จ่ายในการร้องขอและจัดส่งหนังสือรับรองดังกล่าว นอกจากนี้ผู้รับปลายทางยังมีค่าใช้จ่ายแฝงในการเก็บรักษาหนังสือรับรองไว้ตามระยะเวลาที่กฎหมายกำหนด ซึ่งเป็นปัญหาใหญ่สำหรับหน่วยงานที่ต้องเกี่ยวข้องกับบุคคลภายนอกเป็นจำนวนมาก

จากปัญหาดังกล่าวข้างต้นจึงเป็นที่มาของการจัดทำเอกสารฉบับนี้ขึ้น เพื่อกำหนดมาตรฐานและวางแนวทางการจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ โดยจัดทำให้อยู่ในรูปแบบไฟล์เอกสาร Portable Document Format (PDF) ให้มีผลในทางกฎหมายเช่นเดียวกับการทำธุรกรรมโดยวิธีการทั่วไปที่เคยปฏิบัติอยู่เดิมตามเจตนารมณ์ของพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ที่รับรองสถานะทางกฎหมายของข้อมูลทางอิเล็กทรอนิกส์ให้เสมอกับการทำเป็นหนังสือ หรือหลักฐานเป็นหนังสือ การใช้ลายมือชื่ออิเล็กทรอนิกส์ตลอดจนการรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ เพื่อเป็นการส่งเสริมการทำธุรกรรมทางอิเล็กทรอนิกส์ให้น่าเชื่อถือ

นอกจากนี้ในการออกแบบหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ดังกล่าว ยังได้คำนึงถึงความสอดคล้องในการใช้งานจริงตลอดวงจรการใช้งานเอกสาร (Document Life Cycle) ของหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ตั้งแต่การจัดทำ การลงลายมือชื่ออิเล็กทรอนิกส์ การส่ง การรับ การตรวจสอบ การนำไปใช้งานหรือประมวลผลเพื่อใช้งาน การเก็บรักษา ตลอดไปจนถึงการยกเลิกหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์

สารบัญ

1. ขอบข่าย 1
2. บทนิยาม 2
3. ภาพรวมของหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ (Overview) 5
   3.1 หนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ (Electronic Certificate) 5
   3.2 การลงลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature) เพื่อรับรองข้อความที่ปรากฏในหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ 6
   3.3 วงจรการใช้งานหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ (Electronic Certificate Life Cycle) 6
   3.4 คุณสมบัติของหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ 9
4. การจัดทำหนังสือรับรองในรูปแบบไฟล์เอกสาร Portable Document Format (PDF) 13
   4.1 ไฟล์เอกสาร Portable Document Format (PDF) 13
   4.2 การจัดทำหนังสือรับรองในรูปแบบไฟล์เอกสาร Portable Document Format (PDF) 14
5. รายละเอียดทางเทคนิคในการจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ 16
   5.1 การจัดทำหนังสือรับรองนิติบุคคลในรูปแบบไฟล์เอกสาร PDF ประเภท PDF/A 18
   5.2 การแนบไฟล์เพื่อประโยชน์ในการแลกเปลี่ยนข้อความที่ปรากฏหรืออยู่ในหนังสือรับรอง 22
   5.3 การลงลายมือชื่ออิเล็กทรอนิกส์บนหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ 27
   5.4 การเพิ่มมาตรการด้านความมั่นคงปลอดภัย (Security Enhancement) 30
ภาคผนวก ก 31
ภาคผนวก ข 32
ภาคผนวก ค 33
บรรณานุกรม 34

สารบัญรูป

หน้า

รูปที่ 1 วงจรการใช้งานหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ (Electronic Certificate Life Cycle) 7

รูปที่ 2 คุณสมบัติของหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ 9

รูปที่ 3 องค์ประกอบต่างๆ ของหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ 16

รูปที่ 4 โครงสร้างไฟล์เอกสาร PDF/A ภายหลังจากแนบไฟล์ XML 23

รูปที่ 5 โครงสร้างไฟล์เอกสาร PDF/A ภายหลังจากแนบเอกสารอื่นเพิ่มเติม 26

สารบัญตาราง

หน้า

ตารางที่ 1 แสดงคุณสมบัติของหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ตามประเภทต่างๆ 9

ตารางที่ 2 แสดงความสัมพันธ์ระหว่างคุณสมบัติของหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์
และวงจรการใช้งานหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ 12

ตารางที่ 3 แสดงข้อดีและข้อเสียในการนำไฟล์เอกสาร PDF ประเภทต่างๆ มาใช้ในการจัดทำหนังสือรับรอง
ในรูปแบบอิเล็กทรอนิกส์ 14

ตารางที่ 4 แสดงเหตุผลและความจำเป็นในการจัดทำหนังสือรับรองในรูปแบบไฟล์ PDF ประเภท PDF/A
ให้สอดคล้องตามคุณสมบัติของหนังสือรับรองอิเล็กทรอนิกส์แต่ละข้อ 17

ตารางที่ 5 แสดงข้อมูลเมตาดาตา (Metadata) ที่เกี่ยวกับไฟล์เอกสารประเภท PDF/A 19

ตารางที่ 6 แสดงข้อมูลเมตาดาตา (Metadata) ที่เกี่ยวกับหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ 20

ตารางที่ 7 แสดงข้อมูลเมตาดาตา (Metadata) ของไฟล์ XML 24

ตารางที่ 8 แสดงอัลกอริทึมที่เสนอให้ใช้ในการลงลายมือชื่ออิเล็กทรอนิกส์ 30

ETDA
สพธอ
www.etda.or.th

ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

เรื่อง ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์

เพื่อกำหนดมาตรฐานและแนวทางการจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ให้มีความน่าเชื่อถือ และสามารถใช้งานโดยมีสถานะทางกฎหมายได้เช่นเดียวกับการทำธุรกรรมโดยวิธีการทั่วไปที่เคยปฏิบัติอยู่เดิม

อาศัยอำนาจตามความในมาตรา ๗ (๔) แห่งพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ. ๒๕๕๔ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) จึงประกาศข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ เลขที่ ขมธอ. ๑๑-๒๕๖๐ ปรากฏตามท้ายประกาศฉบับนี้

ประกาศ ณ วันที่ ๒๑ มีนาคม พ.ศ. ๒๕๖๐

(นางสุรางคณา วายุภาพ)
ผู้อำนวยการ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ว่าด้วยการจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์

1. ขอบข่าย

เพื่อให้หนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ที่จัดทำตามข้อเสนอแนะฯ ฉบับนี้มีความน่าเชื่อถือและสามารถใช้งานโดยมีสถานะทางกฎหมายได้เช่นเดียวกับการทำธุรกรรมโดยวิธีการทั่วไปที่เคยปฏิบัติอยู่เดิม จึงได้นำเสนอแนวทางการจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ให้อยู่ในรูปแบบของไฟล์เอกสาร Portable Document Format (PDF) ซึ่งถูกออกแบบมาเพื่อให้แสดงผลข้อความเสมือนกับการแสดงข้อความบนกระดาษ โดยแบ่งเนื้อหาออกเป็น 3 หัวข้อหลัก ได้แก่

(1) ภาพรวมของหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ (Overview)

(2) การจัดทำหนังสือรับรองในรูปแบบไฟล์เอกสาร Portable Document Format (PDF)

(3) รายละเอียดทางเทคนิคในการจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์

อย่างไรก็ตาม หนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ที่จัดทำขึ้นตามข้อเสนอแนะฯ ฉบับนี้ไม่ครอบคลุมไปถึง

(1) การพิมพ์ออกของหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ตามข้อเสนอแนะฯ ฉบับนี้ เพื่อมาใช้แทนต้นฉบับและใช้เป็นพยานหลักฐานในศาล

(2) การรับรองความถูกต้องของสำเนาเอกสาร (Certified True Copy) ที่แปลงให้อยู่ในรูปแบบของภาพในภายหลัง

(3) การนำหนังสือรับรองตามข้อเสนอแนะฯ ฉบับนี้ ไปใช้ในการสร้างหนังสือรับรองที่สามารถเปลี่ยนมือได้ (Transferable)

2. บทนิยาม

คำศัพท์	ความหมาย
หนังสือรับรอง	หนังสือที่หน่วยงานออกให้เพื่อรับรองแก่ บุคคล นิติบุคคล หรือหน่วยงาน เพื่อวัตถุประสงค์อย่างหนึ่งอย่างใดให้ปรากฏแก่บุคคลโดยทั่วไป
Portable Document Format (PDF)	รูปแบบไฟล์เอกสารประเภทหนึ่งซึ่งพัฒนาโดย บริษัท Adobe System Incorporated โดยมีวัตถุประสงค์เพื่อแสดงข้อความ รูปภาพ หรือสัญลักษณ์อื่นใด ให้มีลักษณะเหมือนกับการแสดงผลบนกระดาษ ปัจจุบันถูกประกาศให้เป็นมาตรฐานสากลเพื่อรองรับการแสดงผลได้ในทุกอุปกรณ์
Comma Separated Values (CSV)	เป็นรูปแบบของการเก็บข้อมูลทั้งที่เป็นตัวอักษร อักขระ และตัวเลข โดยในแต่ละบรรทัดจะประกอบไปด้วยหลายข้อมูล ซึ่งคั่นด้วยอักขระพิเศษ ตัวอย่างเช่น เครื่องหมายจุลภาค (Comma) เป็นต้น เพื่อประโยชน์ในการแลกเปลี่ยนข้อมูลระหว่างเครื่องคอมพิวเตอร์
Extensible Markup Language (XML)	เป็นภาษาที่ใช้สำหรับการแลกเปลี่ยนข้อมูลแบบมีโครงสร้างระหว่างเครื่องคอมพิวเตอร์ ซึ่งพัฒนาโดยหน่วยงาน World Wide Web Consortium (W3C)
ลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature)	อักษร อักขระ ตัวเลข เสียงหรือสัญลักษณ์อื่นใดที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์ซึ่งนำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้น และเพื่อแสดงว่าบุคคลดังกล่าวยอมรับข้อความในข้อมูลอิเล็กทรอนิกส์นั้น
กุญแจส่วนตัว (Private Key)	กุญแจที่ใช้ในการลงลายมือชื่ออิเล็กทรอนิกส์โดยใช้เทคโนโลยี PKI และเป็นกุญแจที่ใช้ในการถอดรหัสลับข้อมูล (Decryption)
กุญแจสาธารณะ (Public Key)	กุญแจที่ใช้ในการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์โดยใช้เทคโนโลยี PKI และเป็นกุญแจที่ใช้ในการเข้ารหัสลับข้อมูล (Encryption)
โครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure: PKI)	โครงสร้างพื้นฐานที่รับรองกุญแจสาธารณะ (Public Key) ว่าเป็นของบุคคล หน่วยงาน หรืออุปกรณ์ที่กล่าวอ้างถึงจริง ด้วยการออกใบรับรอง X.509 Certificate รวมถึงจัดเก็บ เผยแพร่ และเพิกถอนกุญแจสาธารณะ (Public Key) ที่รับรอง
ใบรับรอง X.509 Certificate	ใบรับรองตามมาตรฐาน X.509 ที่ใช้ในการรับรองกุญแจสาธารณะ (Public Key) ว่าเป็นของบุคคล หน่วยงาน หรืออุปกรณ์ใด ซึ่งกำหนดโดย International Telecommunication Union (ITU)

คำศัพท์	ความหมาย
Distinguished Name	ชื่อที่ระบุถึงบุคคล หน่วยงาน หรืออุปกรณ์ที่เกี่ยวข้องกับใบรับรอง X.509 Certificate
ผู้ให้บริการออกใบรับรอง (Certification Authority: CA)	หน่วยงานหรือองค์กรที่มีหน้าที่ในการออกใบรับรอง X.509 Certificate เพื่อรับรองกุญแจสาธารณะ (Public Key)
ใบรับรองอิเล็กทรอนิกส์ระดับชั้นบนสุด (Root CA Certificate)	ใบรับรอง X.509 Certificate ที่ออกโดยผู้ให้บริการออกใบรับรอง (CA) ที่กำกับดูแลการออกใบรับรอง X.509 Certificate ที่อยู่ภายใต้ตนทั้งหมด
รายการเพิกถอนใบรับรอง (Certificate Revocation List: CRL)	รายการใบรับรอง X.509 Certificate ทั้งหมดที่ถูกเพิกถอนการใช้งาน ซึ่งสร้างและประกาศโดยผู้ให้บริการออกใบรับรอง (CA)
โปรโตคอลตรวจสอบสถานะของใบรับรองในรูปแบบออนไลน์ (Online Certificate Status Protocol: OCSP)	ช่องทางการให้บริการตรวจสอบสถานะของใบรับรอง X.509 Certificate อีกรูปแบบหนึ่ง ซึ่งผู้ให้บริการออกใบรับรอง (CA) ให้บริการตรวจสอบสถานะทางออนไลน์
Cryptographic Message Syntax (CMS)	ไวยกรณ์หรือโครงสร้างของข้อมูลสำหรับเก็บลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature) ที่สร้างด้วยเทคโนโลยี PKI และข้อมูลที่ถูกเข้ารหัสลับ (Encryption) เพื่อรักษาความมั่นคงปลอดภัยให้กับข้อมูล
การประทับรับรองเวลา (Time Stamping)	การรับรองความมีอยู่ของข้อมูลหรือเอกสารอิเล็กทรอนิกส์ ณ เวลาใดเวลาหนึ่งโดยบุคคลที่สามที่มีความน่าเชื่อถือ
เวลาที่ได้รับการประทับรับรอง (Time-Stamp Token)	ข้อมูลที่บุคคลที่สามออกให้เพื่อรับรองว่า ข้อมูลหรือเอกสารอิเล็กทรอนิกส์ที่ร้องขอการประทับเวลามีอยู่จริง ณ เวลาที่ประทับรับรอง โดยข้อมูลดังกล่าวสามารถใช้ในการตรวจสอบได้ว่าข้อมูลหรือเอกสารอิเล็กทรอนิกส์นั้นถูกแก้ไขภายหลังจากได้รับการประทับรับรองเวลาหรือไม่
อัลกอริทึมสำหรับเข้ารหัสลับด้วยกุญแจแบบอสมมาตร (Asymmetric Key Algorithm)	กระบวนการทางคณิตศาสตร์ที่ใช้ในการสร้างกุญแจส่วนตัว (Private Key) และกุญแจสาธารณะ (Public Key) รวมถึงการนำกุญแจดังกล่าวไปใช้ในการลงลายมือชื่ออิเล็กทรอนิกส์และเข้ารหัสลับ
อัลกอริทึมสำหรับสร้างค่าแฮช (Hash Algorightm)	กระบวนการทางคณิตศาสตร์ที่ประมวลผลข้อมูลหรือเอกสารอิเล็กทรอนิกส์ใดๆ ที่แตกต่างกันแล้วให้ผลลัพธ์ที่ไม่ซ้ำกัน ซึ่งเปรียบเสมือนเป็นตัวแทนหรือลายนิ้วมือ (fingerprint) ของข้อมูลหรือเอกสารอิเล็กทรอนิกส์นั้น โดยผลลัพธ์จากกระบวนการดังกล่าวจะถูกเรียกว่าค่าแฮช (Hash Value)
MIME Media Types	ประเภทของไฟล์ข้อมูลและเนื้อหาที่รับส่งผ่านเครือข่ายอินเทอร์เน็ตซึ่งประกาศโดย Internet Assigned Numbers Authority (IANA)

คำศัพท์	ความหมาย
Object Identifier (OID)	ชุดของหมายเลขที่ระบุถึงวัตถุที่เกี่ยวข้องกับสารสนเทศ (Information Object) ใดๆ โดยค่า OID ของแต่ละวัตถุจะไม่ซ้ำกับค่า OID ของ Object อื่น
Unicode	มาตรฐานอุตสาหกรรมที่กำหนดรหัสของตัวอักษร ตัวอักขระ และตัวเลขของภาษาส่วนใหญ่ในโลก อีกทั้งยังเป็นมาตรฐานในการกำหนดแนวทางการแสดงผลและการจัดการข้อความให้สอดคล้องกัน
ข้อความขนาดเล็ก (Micro Text)	เป็นเทคนิคในการแทรกข้อความขนาดเล็กบนเอกสารที่พิมพ์ออกมาเพื่อประโยชน์ในการตรวจสอบและป้องกันการปลอมแปลงเอกสาร

3. ภาพรวมของหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ (Overview)

3.1 หนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ (Electronic Certificate)

หนังสือรับรอง (Certificate) หรือหนังสืออื่นใดที่ถูกใช้งานเพื่อวัตถุประสงค์ในลักษณะเดียวกัน เช่น ใบสำคัญรับรอง หนังสือสำคัญรับรอง เป็นต้น ตามระเบียบสำนักนายกรัฐมนตรี ว่าด้วยงานสารบรรณ พ.ศ. 2526 [1] ได้มีการกำหนดความหมายและแบบของหนังสือรับรองไว้ กล่าวคือ หนังสือที่ส่วนงานราชการออกให้เพื่อรับรองแก่ บุคคล นิติบุคคล หรือหน่วยงาน เพื่อวัตถุประสงค์อย่างหนึ่งอย่างใดให้ปรากฏแก่บุคคลโดยทั่วไปไม่จำเพาะเจาะจง ใช้กระดาษตราครุฑ และให้จัดทำตามแบบที่ 10 ท้ายระเบียบ โดยกรอกข้อรายละเอียด เช่น เลขที่หนังสือรับรอง ส่วนราชการเจ้าของหนังสือ ข้อความที่ทางราชการรับรอง วันที่ให้ไว้ ลายมือชื่อหัวหน้าส่วนราชการหรือผู้ที่ได้รับมอบหมาย และชื่อเต็มของเจ้าของลายมือชื่อไว้ใต้ลายมือชื่อ เป็นต้น

ซึ่งจากความหมายของหนังสือรับรองดังกล่าวข้างต้นพบว่า ในทางปฏิบัติทั่วไปหนังสือรับรองที่ออกโดยเอกชนล้วนมีวัตถุประสงค์ในการออกไม่แตกต่างไปจากส่วนงานราชการ เช่น หนังสือรับรองฐานะทางการเงินที่ออกโดยธนาคารพาณิชย์ หนังสือรับรองการถือครองหลักทรัพย์ที่ออกโดยบริษัทหลักทรัพย์ หนังสือรับรองการทำงานที่ออกโดยนายจ้าง เป็นต้น นอกเหนือจากเลขที่หนังสือรับรอง ชื่อหน่วยงานเอกชนที่เป็นเจ้าของหนังสือ ข้อความที่รับรอง และวันที่ให้ไว้ ซึ่งเหมือนกันกับหนังสือรับรองที่ออกโดยส่วนงานราชการ หนังสือรับรองที่ออกโดยเอกชนยังคงมีความต้องการในการลงลายมือชื่อบุคคลที่มีอำนาจกระทำการเพื่อรับรองข้อความในหนังสือเช่นเดียวกัน

ทั้งนี้ในการใช้งานหนังสือรับรองเพื่อประกอบการทำธุรกรรมเรื่องใดเรื่องหนึ่งนั้น อาจมีการร้องขอหนังสือรับรองในรูปแบบต้นฉบับหรือสำเนาแล้วแต่กรณี เพื่อให้เกิดการทำธุรกรรมทางอิเล็กทรอนิกส์โดยสมบูรณ์ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 [2] จึงได้มีบทบัญญัติเพื่อรับรองสถานะทางกฎหมายของข้อมูลทางอิเล็กทรอนิกส์ให้เสมอกับการทำเป็นหนังสือหรือหลักฐานเป็นหนังสือ การใช้ลายมือชื่ออิเล็กทรอนิกส์ ตลอดจนการรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ โดยมีบทบัญญัติที่สำคัญเกี่ยวข้องกับการจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ดังต่อไปนี้

(1) มาตรา 7 ห้ามมิให้ปฏิเสธความมีผลผูกพันและการบังคับใช้ทางกฎหมายของข้อความใดเพียงเพราะเหตุที่ข้อความนั้นอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

(2) มาตรา 8 วรรคหนึ่ง ภายใต้บังคับบทบัญญัติแห่งมาตรา 9 การใดต้องทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดง ถ้าได้มีการจัดทำข้อความขึ้นเป็นข้อมูลอิเล็กทรอนิกส์ที่สามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง ให้ถือว่าข้อความนั้นได้ทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดงแล้ว

(3) มาตรา 9 วรรคหนึ่ง ในกรณีที่บุคคลพึงลงลายมือชื่อในหนังสือ ให้ถือว่าข้อมูลอิเล็กทรอนิกส์นั้นมีการลงลายมือชื่อแล้ว ถ้าได้มีการดำเนินการตามหลักเกณฑ์ที่กำหนด

(4) มาตรา 10 ในกรณีที่กฎหมายกำหนดให้นำเสนอหรือเก็บรักษาข้อความใดในสภาพที่เป็นมาแต่เดิมอย่างเอกสารต้นฉบับ ถ้าได้นำเสนอหรือเก็บรักษาในรูปข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์ที่กำหนด

(5) มาตรา 11 ห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในกระบวนการพิจารณาตามกฎหมายทั้งในคดีแพ่ง คดีอาญา หรือคดีอื่นใด เพียงเพราะเหตุว่าเป็นข้อมูลอิเล็กทรอนิกส์

(6) มาตรา 26 วรรคหนึ่ง ลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะดังต่อไปนี้ให้ถือว่าเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้

จากบทบัญญัติข้างต้นอาจกล่าวโดยสรุปได้ว่า พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 [2] รับรองสถานะทางกฎหมายของหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ว่าเป็นเอกสารต้นฉบับ และสามารถใช้เป็นพยานหลักฐานในศาลได้ หากหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ดังกล่าวสามารถเข้าถึง เก็บรักษา และสามารถนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลงตามหลักเกณฑ์ที่กฎหมายกำหนด นอกจากนี้ลายมือชื่ออิเล็กทรอนิกส์ที่ปรากฏในหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ ยังมีสถานะเทียบเท่าเสมือนหนึ่งว่าหนังสือรับรองดังกล่าวได้มีการลงลายมือชื่อโดยผู้มีอำนาจกระทำการแล้ว หากได้มีการดำเนินการตามหลักเกณฑ์ที่กฎหมายกำหนด

3.2 การลงลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature) เพื่อรับรองข้อความที่ปรากฏในหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์

การลงลายมือชื่อในหนังสือรับรองโดยบุคคลที่มีอำนาจกระทำการแทนหน่วยงานนั้น เป็นไปเพื่อรับรองข้อความที่ปรากฏในหนังสือว่าถูกต้องแท้จริงโดยหน่วยงานที่มีอำนาจรับรอง ด้วยเหตุนี้ เพื่อให้การลงลายมือชื่ออิเล็กทรอนิกส์มีสถานะทางกฎหมายเทียบเท่ากับการลงลายมือชื่อในหนังสือรับรองทั่วไป พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 [2] จึงได้มีบทบัญญัติเกี่ยวกับการลงลายมือชื่ออิเล็กทรอนิกส์ไว้ 2 มาตรา กล่าวคือ 1) ลายมือชื่ออิเล็กทรอนิกส์ ตามมาตรา 9 และ 2) ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ ตามมาตรา 26 แต่เนื่องด้วยการลงลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ ตามมาตรา 26 มีคุณสมบัติพิเศษที่นอกเหนือจากมาตรา 9 คือ ภายหลังจากลงลายมือชื่ออิเล็กทรอนิกส์บนหนังสือ การเปลี่ยนแปลงใดๆ ที่เกิดแก่ข้อความจะสามารถตรวจพบได้ทันทีโดยคอมพิวเตอร์ ซึ่งจะช่วยให้ผู้รับสามารถพิสูจน์ได้ว่าหนังสือรับรองดังกล่าว ออกโดยหน่วยงานที่มีอำนาจจริงและข้อความไม่ถูกเปลี่ยนแปลงแก้ไขหรือถูกปลอมแปลง

ด้วยคุณสมบัติดังกล่าวจึงทำให้ลายมือชื่ออิเล็กทรอนิกส์ตามมาตรา 26 นั้นเหมาะกับการลงลายมือชื่อบนหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ ซึ่งเทคโนโลยีการลงลายมือชื่ออิเล็กทรอนิกส์ที่สอดคล้องตามมาตรา 26 ในปัจจุบันคือ เทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure)

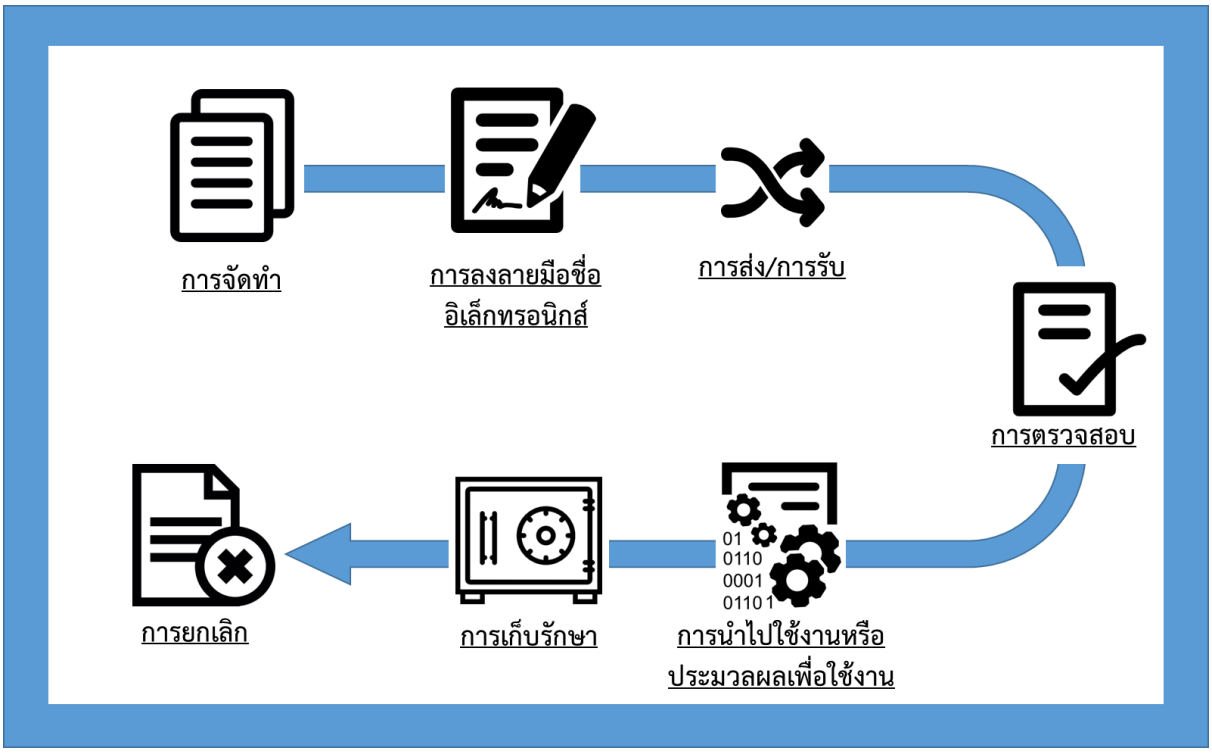
3.3 วงจรการใช้งานหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ (Electronic Certificate Life Cycle)

เพื่อให้การจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ให้มีสถานะเป็นเอกสารต้นฉบับ และสามารถใช้เป็นพยานหลักฐานในศาลได้ ตามมาตรา 10 แห่งพระราชบัญญัติ ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 [2] ซึ่งได้มีการกำหนดหลักเกณฑ์ของเอกสารที่มีสถานะเป็นต้นฉบับตามกฎหมาย ดังนี้

(1) ข้อมูลอิเล็กทรอนิกส์ได้ใช้วิธีการที่เชื่อถือได้ในการรักษาความถูกต้องของข้อความตั้งแต่การสร้างข้อความเสร็จสมบูรณ์ และ

(2) สามารถแสดงข้อความนั้นในภายหลังได้

จากบทบัญญัติดังกล่าวข้างต้น หนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ที่จัดทำขึ้นจะต้องเป็นเอกสารที่สามารถแสดงตัวอักษร ตัวเลข ภาพ หรือรูปแบบอื่นใดในภายหลังได้โดยความหมายไม่เปลี่ยนแปลง ตั้งแต่ขั้นตอนการจัดทำไปจนตลอดวงจรการใช้งานเอกสาร (Document Life Cycle) ซึ่งได้แก่การจัดทำ การลงลายมือชื่ออิเล็กทรอนิกส์ การส่ง การรับ การตรวจสอบ การนำไปใช้งานหรือประมวลผลเพื่อใช้งาน การเก็บรักษา และการยกเลิก



รูปที่ 1 วงจรการใช้งานหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ (Electronic Certificate Life Cycle)

3.3.1 การจัดทำและการลงลายมือชื่ออิเล็กทรอนิกส์

การออกหนังสือรับรองโดยหน่วยงานไม่ว่าจะโดยส่วนงานราชการหรือเอกชน จะมีกระบวนการในการจัดทำรวมถึงการเลือกใช้วัสดุที่เหมาะสมกับวัตถุประสงค์ของการใช้งาน ตั้งแต่การเลือกใช้กระดาษ การจัดพิมพ์ การออกเลขที่หนังสือรับรอง การจัดทำต้นขั้วของหนังสือรับรอง การควบคุมกระบวนการจัดทำ และการเพิ่มมาตรการด้านความมั่นคงปลอดภัย เช่น การลงลายน้ำ การวางลวดลายที่เป็นเอกลักษณ์เฉพาะตัว การแทรกข้อความหรือคุณสมบัติพิเศษบางประการเพื่อสร้างเอกลักษณ์ให้แก่กระดาษ เป็นต้น ซึ่งมาตรการดังกล่าวข้างต้นเป็นไปเพื่อป้องกันการปลอมแปลง สามารถตรวจสอบความแท้จริง และใช้เป็นพยานหลักฐานในกรณีที่เกิดข้อพิพาทขึ้นได้

เพื่อให้หนังสือรับรองในรูปแบบอิเล็กทรอนิกส์มีความน่าเชื่อถือและสามารถตรวจสอบความแท้จริง อีกทั้งยังสามารถใช้เป็นพยานหลักฐานได้เช่นเดียวกันกับหนังสือรับรองในรูปแบบกระดาษ การลงลายมือชื่ออิเล็กทรอนิกส์ตามมาตรา 26 จึงเป็นมาตรการหนึ่งที่ช่วยในการป้องกันการเปลี่ยนแปลงแก้ไขและการปลอมแปลง ซึ่งเป็นความสามารถที่นอกเหนือไปจากการรับรองว่าหนังสือรับรองดังกล่าวออกโดยหน่วยงานที่มีอำนาจจริง อย่างไรก็ตามหน่วยงานที่ออกหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์อาจมีการพิจารณานำมาตรการด้านความมั่นคงปลอดภัยอื่นมาประยุกต์ใช้ได้ เช่น การจัดทำหมายเลขอ้างอิง

ในลักษณะเดียวกันกับหมายเลขต้นขั้วเพื่อยืนยันความมีอยู่ของหนังสือรับรอง การลงลายน้ำ การแทรกข้อความขนาดเล็ก (Micro Text) เป็นต้น

3.3.2 การส่งและการรับหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์

เนื่องด้วยบทบัญญัติแห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 [2] ไม่ได้มีการกำหนดวิธีการส่งและวิธีการรับข้อมูลอิเล็กทรอนิกส์ไว้ วิธีการส่งและการรับจึงเป็นไปตามที่ผู้ส่งข้อมูลและผู้รับข้อมูลตกลงกันหรือเป็นไปตามมาตรฐานซึ่งใช้บังคับอยู่

3.3.3 การตรวจสอบและนำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ไปใช้งานหรือประมวลผลเพื่อใช้งาน

ภายหลังจากที่หนังสือรับรองถูกส่งไปยังผู้รับปลายทาง เช่น การยื่นหนังสือรับรับรองนิติบุคคลเพื่อประกอบการการพิจารณาแก่หน่วยงานราชการ การยื่นหนังสือรับรองการทำงานเพื่อการตรวจลงตรา (VISA) เป็นต้น ผู้รับจำเป็นต้องตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ในหนังสือรับรองดังกล่าวว่า ออกโดยหน่วยงานที่มีอำนาจ ข้อความในหนังสือรับรองดังกล่าวไม่ได้ถูกเปลี่ยนแปลงแก้ไข นอกจากนี้อาจจำเป็นต้องตรวจสอบเพิ่มเติม ในกรณีที่มีการเพิ่มมาตรการด้านความมั่นคงปลอดภัยในหนังสือรับรองดังกล่าวเสียก่อน จึงจะสามารถนำไปใช้งานต่อได้ ทั้งนี้การใช้งานข้อความในหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ อาจดำเนินการได้ใน 2 ลักษณะ กล่าวคือ

(1) การนำไปใช้งานโดยบุคคล

ในกรณีพื้นฐานทั่วไป เมื่อผู้รับได้รับหนังสือรับรองจะทำการพิจารณาข้อความตามที่ปรากฏในหนังสือ ซึ่งในการใช้งานลักษณะดังกล่าว หนังสือรับรองในรูปแบบอิเล็กทรอนิกส์จำเป็นต้องอยู่ในสภาพที่สามารถอ่านเข้าใจได้โดยบุคคล (Human Readable)

(2) การนำไปใช้งานด้วยการประมวลผลโดยคอมพิวเตอร์

ในกรณีที่หนังสือรับรองอยู่ในรูปแบบอิเล็กทรอนิกส์ได้ถูกออกแบบและสร้างให้อยู่ในรูปแบบที่คอมพิวเตอร์สามารถประมวลผลข้อความนั้นได้ ภายหลังจากที่ได้รับหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ดังกล่าวคอมพิวเตอร์ก็จะสามารถนำข้อความไปประมวลผลเพื่อพิจารณาข้อความได้โดยอัตโนมัติ ซึ่งในปัจจุบันรูปแบบของข้อความที่นิยมใช้เพื่อให้คอมพิวเตอร์สามารถประมวลผลได้ (Machine Processable) มีอยู่หลายรูปแบบ เช่น Extensible Markup Language (XML) และ Comma Separated Values (CSV) เป็นต้น ซึ่งประโยชน์ของการทำให้ข้อความอยู่ในรูปแบบดังกล่าว คือ ผู้ส่งและผู้รับสามารถแลกเปลี่ยนข้อความที่ปรากฏหรืออยู่ในหนังสือรับรองได้ (Exchangeable) ได้ไม่ต้องใช้บุคคลในการพิจารณาข้อความ อีกทั้งยังช่วยลดเวลาในการดำเนินงาน ลดความผิดพลาดที่เกิดจากคน และลดค่าใช้จ่ายในการดำเนินการได้อีกด้วย

3.3.4 การเก็บรักษาและการยกเลิก

เมื่อหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ถูกใช้งานตามวัตถุประสงค์เป็นที่เรียบร้อยแล้ว ผู้รับอาจทำการเก็บรักษาไฟล์เอกสารตามระยะเวลาที่กฎหมายกำหนด พร้อมข้อมูลเมตาดาตา (Metadata) ซึ่งเป็นข้อมูลเกี่ยวกับไฟล์เอกสารดังกล่าวเพื่อประโยชน์ในการสืบค้นและอ้างอิงภายหลัง

ในบางกรณีการเก็บรักษาหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์อาจมีความจำเป็นในการเก็บรักษาเกินกว่า 10 ปี ก่อนที่จะถูกยกเลิกการใช้งานหรือถูกทำลาย เพื่อให้หนังสือดังกล่าวยังคงสถานะ

ความเป็นต้นฉบับตามหลักเกณฑ์ของกฎหมายและสามารถใช้เป็นพยานหลักฐานในศาลได้ การเก็บรักษาหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ให้อยู่ในสภาพที่สามารถแสดงข้อความได้ในภายหลังโดยความหมายไม่เปลี่ยนแปลงแม้จะถูกเก็บรักษาไว้เป็นระยะเวลานานจึงมีความสำคัญเป็นอย่างยิ่ง

3.4 คุณสมบัติของหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์

จากวงจรการใช้งานหนังสือรับรองอิเล็กทรอนิกส์ (Electronic Certificate Life Cycle) ที่กล่าวมาข้างต้น เพื่อให้หนังสือรับรองในรูปแบบอิเล็กทรอนิกส์มีคุณสมบัติเทียบเท่าหนังสือรับรองในรูปแบบกระดาษและสอดคล้องกับการใช้งานจริง หนังสือรับรองในรูปแบบอิเล็กทรอนิกส์จึงควรมีคุณสมบัติดังปรากฏตามด้านล่างนี้

ตารางที่ 1 แสดงคุณสมบัติของหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ตามประเภทต่างๆ

ประเภทคุณสมบัติ	คุณสมบัติของหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์
คุณสมบัติด้านกฎหมาย	(1) ความเป็นต้นฉบับและสามารถใช้เป็นพยานหลักฐานในศาลได้ (Original Document)
คุณสมบัติด้านการใช้งาน	(2) สามารถอ่านเข้าใจได้โดยบุคคล (Human Readable) (3) สามารถแลกเปลี่ยนข้อความที่ปรากฏหรืออยู่ในหนังสือรับรองได้ (Exchangeable)
คุณสมบัติด้านความน่าเชื่อถือ	(4) การลงลายมือชื่ออิเล็กทรอนิกส์บนหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ (Electronic Signature) (5) การเพิ่มมาตรการด้านความมั่นคงปลอดภัย (Security Enhancement)

รูปที่ 2 คุณสมบัติของหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์

3.4.1 คุณสมบัติข้อที่ 1 ความเป็นต้นฉบับและสามารถใช้เป็นพยานหลักฐานในศาลได้ (Original Document)

เนื่องจากการรับฟังพยานเอกสารในศาล จะรับฟังเฉพาะพยานเอกสารที่มีสถานะเป็นต้นฉบับเท่านั้น การจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ให้มีสถานะเป็นต้นฉบับตามหลักเกณฑ์ที่กฎหมายกำหนดจึงมีความสำคัญเป็นอย่างยิ่ง หนังสือรับรองในรูปแบบอิเล็กทรอนิกส์จึงจำเป็นต้องสามารถรักษาความถูกต้องของข้อความ และแสดงข้อความในภายหลังได้โดยความหมายไม่เปลี่ยนแปลง

3.4.2 คุณสมบัติข้อที่ 2 สามารถอ่านเข้าใจได้โดยบุคคล (Human Readable)

คุณสมบัติในข้อนี้คือ การทำให้คอมพิวเตอร์สามารถแสดงผลหนังสือรับรองให้ปรากฏเป็นเอกสารที่มีรูปแบบของตัวอักษร ตัวเลข ภาพ หรือรูปแบบอื่นใดบนหน้าจอคอมพิวเตอร์ได้โดยความหมายไม่เปลี่ยนแปลง และเพื่อให้บุคคลสามารถเข้าใจความหมายของข้อความที่แสดงนั้นได้ ซึ่งคุณสมบัติในข้อที่ 2 นี้ถูกกำหนดไว้เพื่อรองรับการใช้งานส่วนใหญ่ที่ยังคงต้องอาศัยบุคคลในการดำเนินงาน รวมถึงรองรับการพิมพ์ออกมาใช้งานในรูปแบบกระดาษสำหรับกรณีจำเป็น

3.4.3 คุณสมบัติข้อที่ 3 สามารถแลกเปลี่ยนข้อความที่ปรากฏหรืออยู่ในหนังสือรับรองได้ (Exchangeable)

ในกรณีที่ต้องการให้คอมพิวเตอร์ดำเนินงานบางอย่างแทนบุคคล เช่น การพิจารณาคำขอใช้บริการแบบอัตโนมัติ การนำเข้าข้อความที่ปรากฏหรืออยู่ในหนังสือรับรองสู่ระบบโดยอัตโนมัติ เป็นต้น เพื่อลดเวลาในการดำเนินงาน ความผิดพลาดที่เกิดจากคน และค่าใช้จ่ายในการดำเนินงาน ด้วยเหตุนี้ข้อความที่ปรากฏหรืออยู่ในหนังสือรับรองจึงควรถูกจัดเก็บในรูปแบบที่คอมพิวเตอร์สามารถนำไปประมวลผลได้ (Machine Processable) เช่น Extensible Markup Language (XML) หรือ Comma Separated Values (CSV) เป็นต้น

3.4.4 คุณสมบัติข้อที่ 4 การลงลายมือชื่ออิเล็กทรอนิกส์บนหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ (Electronic Signature)

คุณสมบัติในข้อนี้เป็นหนึ่งในคุณสมบัติที่สำคัญสำหรับการจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ เนื่องจากเป็นสิ่งที่ใช้ในการตรวจสอบข้อความที่ปรากฏหรือยู่ในหนังสือรับรองว่า ได้รับรองโดยหน่วยงานที่มีอำนาจจริง ไม่ถูกเปลี่ยนแปลงแก้ไข และสามารถนำข้อความดังกล่าวไปใช้ในการอ้างอิงได้

ซึ่งในข้อเสนอแนะมาตรฐานนี้ได้นำแนวคิดของเทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure) หรือ เทคโนโลยี PKI เข้ามาประยุกต์ใช้งานในการลงลายมือชื่ออิเล็กทรอนิกส์ เนื่องจากเป็นเทคโนโลยีที่พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 [2] รับรองสถานะทางกฎหมาย นอกจากนี้ สหประชาชาติและสหภาพยุโรปยังได้มีการประกาศกฎหมายเพื่อรับรองสถานะทางกฎหมายของลายมือชื่ออิเล็กทรอนิกส์โดยใช้เทคโนโลยี PKI เพื่อสนับสนุนให้เกิดการใช้ลายมือชื่ออิเล็กทรอนิกส์สำหรับการทำธุรกรรมระหว่างประเทศสมาชิก ซึ่งประกอบด้วย

(1) UNCITRAL Model Law on Electronic Signature ซึ่งเป็นกฎหมายต้นแบบที่ประกาศโดย United Nations Commission on International Trade Law สำหรับเป็นแนวทางในการยกร่างกฎหมายของประเทศสมาชิกภายใต้สหประชาชาติ และสนับสนุนให้เกิดการใช้งานลายมือชื่ออิเล็กทรอนิกส์มีสถานะทางกฎหมายเทียบเท่าการลงลายมือชื่อด้วยปากกา

(2) Directive on Electronic Signatures (1999/93/EC) ซึ่งเป็นกฎหมายกลางของสหภาพยุโรปที่รับรองสถานะทางกฎหมายของลายมือชื่ออิเล็กทรอนิกส์ให้เทียบเท่ากับการลงลายมือชื่อด้วยปากกา ซึ่งกำหนดแนวทางให้ประเทศสมาชิกประกาศกฎหมายของตนให้สอดคล้องตามกฎหมายกลางดังกล่าว

ซึ่งจะส่งผลให้ประเทศที่มีกฎหมายรับรองสถานะของลายมือชื่ออิเล็กทรอนิกส์โดยใช้เทคโนโลยี PKI สามารถแลกเปลี่ยนหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ระหว่างประเทศได้ โดยไม่จำเป็นต้องใช้หนังสือรับรองในรูปแบบกระดาษอีกต่อไป

นอกจากนี้การลงลายมือชื่ออิเล็กทรอนิกส์ด้วยเทคโนโลยี PKI ยังมีความน่าเชื่อถือมากว่าการลงลายมือชื่อด้วยปากกา เนื่องจากบุคคลที่ครอบครองกุญแจส่วนตัว (Private Key) ที่ใช้ในการลงลายมือชื่ออิเล็กทรอนิกส์คือเจ้าของลายมือชื่อเท่านั้น จึงทำให้การลงลายมือชื่อปลอมในเอกสารจึงไม่สามารถทำได้ด้วยเทคโนโลยีดังกล่าว อีกทั้ง หากเกิดการเปลี่ยนแปลงใดๆ แก่ข้อความที่ปรากฏหรืออยู่ในหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ คอมพิวเตอร์จะสามารถตรวจพบและแจ้งแก่บุคคลที่ใช้หนังสือรับรองดังกล่าวได้ทันที

3.4.5 คุณสมบัติข้อที่ 5 การเพิ่มมาตรการด้านความมั่นคงปลอดภัย (Security Enhancement)

การเพิ่มมาตรการด้านความมั่นคงปลอดภัยตามคุณสมบัติข้อที่ 5 นี้ เป็นการเพิ่มมาตรการที่ช่วยเพิ่มความน่าเชื่อถือแก่หนังสือรับรองอิเล็กทรอนิกส์ ซึ่งเป็นสิ่งที่หน่วยงานสามารถดำเนินการเพิ่มเติมได้ แต่ไม่เป็นการจำกัดให้หนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ต้องดำเนินการเพิ่มมาตรการดังกล่าวทุกฉบับ ทั้งนี้ หน่วยงานอาจพิจารณาเพิ่มเติมมาตรการให้เหมาะสมกับการใช้งานจริงหรือความต้องการเฉพาะของแต่ละหน่วยงานได้ ตัวอย่างเช่น

(1) การจัดทำหมายเลขอ้างอิงในลักษณะเดียวกันกับหมายเลขต้นขั้วเช็ค และเก็บรักษาหมายเลขอ้างอิงดังกล่าวพร้อมกับค่าแฮช (Hash Value) โดยบุคคลที่สาม (Third Party) หรือหน่วยงานที่กำกับดูแล เพื่อเป็นหลักฐานยืนยันความมีอยู่ของหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์และสามารถตรวจสอบความถูกต้องครบถ้วนของข้อความในภายหลังได้ ซึ่งเป็นการประยุกต์แนวคิดของการตรวจสอบความมีอยู่ของเอกสารที่มีความสำคัญ เช่น เช็ค หนังสือรับรองที่ออกโดยหน่วยงานรัฐ เป็นต้น มาประยุกต์ใช้ในรูปแบบอิเล็กทรอนิกส์

(2) การแสดงลายน้ำ (Watermark) ในรูปแบบข้อความหรือรูปภาพให้ปรากฏบนหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ เพื่อให้ข้อความหรือรูปภาพนั้นปรากฏบนหนังสือรับรองที่ถูกพิมพ์ออก ตัวอย่างเช่น

(2.1) การแสดงข้อความวัตถุประสงค์ของการใช้งาน

(2.2) การแสดงข้อความเพื่อบ่งบอกสถานะของเอกสาร เช่น “คู่ฉบับ” “สำเนา” เป็นต้น

(2.3) การแสดงรูปภาพที่มีลวดลายเป็นเอกลักษณ์เฉพาะตัวซึ่งยากต่อการปลอมแปลง เช่น ลวดลายบนธนบัตร หรือหนังสือเดินทาง เป็นต้น

(2.4) การแทรกข้อความขนาดเล็ก (Micro Text) บนหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ เพื่อประโยชน์ในการตรวจสอบว่าหนังสือรับรองที่ถูกพิมพ์ออกมีการใช้งานซ้ำหรือไม่ ซึ่งข้อความดังกล่าวจะยังคมชัดเมื่อพิมพ์ออกในครั้งแรกและเลือนหายไปเมื่อมีการทำสำเนา

จากคุณสมบัติทั้ง 5 ข้อของหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ข้างต้น เกี่ยวข้องกับวงจรการใช้งานหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ ได้ดังตารางดังต่อไปนี้

ตารางที่ 2 แสดงความสัมพันธ์ระหว่างคุณสมบัติของหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์และวงจรการใช้งานหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์

	คุณสมบัติที่เกี่ยวข้อง	ขั้นตอนในวงจรการใช้งาน
1.	ความเป็นต้นฉบับและสามารถใช้เป็นพยานหลักฐานในศาลได้ (Original Document)	● ตลอดวงจรการใช้งาน
2.	สามารถอ่านเข้าใจได้โดยบุคคล (Human Readable)	● การจัดทำ ● การนำไปใช้งานหรือการประมวลผลเพื่อใช้งาน
3.	สามารถแลกเปลี่ยนข้อความที่ปรากฏหรืออยู่ในหนังสือรับรองได้ (Exchangeable)	● การจัดทำ ● การนำไปใช้งานหรือการประมวลผลเพื่อใช้งาน
4.	การลงลายมือชื่ออิเล็กทรอนิกส์บนหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ (Electronic Signature)	● การลงลายมือชื่ออิเล็กทรอนิกส์ ● การตรวจสอบ
5.	การเพิ่มมาตรการด้านความมั่นคงปลอดภัย (Security Enhancement)	● การตรวจสอบ

4. การจัดทำหนังสือรับรองในรูปแบบไฟล์เอกสาร Portable Document Format (PDF)

4.1 ไฟล์เอกสาร Portable Document Format (PDF)

ไฟล์เอกสารในรูปแบบ Portable Document Format หรือ PDF เป็นไฟล์เอกสารที่ถูกออกแบบเพื่อให้สามารถแสดงผลข้อความในรูปแบบของตัวอักษร ตัวเลข ภาพ หรือรูปแบบอื่นใดเสมือนการแสดงข้อความบนกระดาษ ซึ่งปัจจุบันไฟล์เอกสาร PDF มีการใช้งานใน 2 รูปแบบกล่าวคือ

4.1.1 ไฟล์เอกสาร PDF เพื่อการแสดงข้อความ ซึ่งได้แก่

(1) PDF ตามมาตรฐาน ISO 32000-1 หรือไฟล์เอกสาร PDF ที่ใช้งานกันอยู่ทั่วไปในปัจจุบัน

(2) PDF/A เป็นไฟล์เอกสาร PDF ที่ออกแบบมาเพื่อการเก็บรักษาในระยะยาว (Long-term Preservation) ตามมาตรฐาน ISO 19005-1 ถึง ISO 19005-3 ตามลำดับ

(3) PDF/X เป็นไฟล์เอกสาร PDF ที่ออกแบบมาเพื่องานสิ่งพิมพ์ ตามมาตรฐาน ISO 15930-1 ถึง ISO 15930-8 ตามลำดับ

(4) PDF/E เป็นไฟล์เอกสาร PDF ที่ออกแบบมาเพื่องานออกแบบด้านวิศวกรรม ตามมาตรฐาน ISO 24517-1

(5) PDF/VT เป็นไฟล์เอกสาร PDF ที่ออกแบบมาเพื่อรองรับงานพิมพ์ในรูปแบบดิจิทัล ตามมาตรฐาน ISO 16612-1 ถึง ISO 16612-2

(6) PDF/UA เป็นไฟล์เอกสาร PDF ที่ออกแบบมาเพื่อให้ผู้พิการสามารถเข้าถึงข้อความได้โดยไม่มีข้อจำกัด ตามมาตรฐาน ISO 14289-1

4.1.2 ไฟล์เอกสาร PDF เพื่อรองรับการกรอกข้อความในแบบฟอร์ม ซึ่งได้แก่

(1) AcroForm เป็นไฟล์เอกสาร PDF ตามมาตรฐาน ISO 32000-1 ที่รองรับการกรอกข้อมูลและจัดเก็บข้อมูลลงในไฟล์เอกสาร เพื่อทดแทนกรอกข้อความบนแบบฟอร์มบนกระดาษ

(2) XML Forms Architecture (XFA) เป็นไฟล์เอกสาร PDF อีกรูปแบบหนึ่งที่รองรับการใช้งานในรูปแบบฟอร์ม โดยมีคุณสมบัติที่เหนือกว่า AcroFrom ในด้านการรองรับการแสดงผลโดยไม่จำกัดจำนวนหน้า กล่าวคือ XFA สามารถเพิ่มหน้าแบบฟอร์มได้โดยอัตโนมัติตามจำนวนข้อความที่กรอกลงในแบบฟอร์ม (Dynamic Form) ซึ่ง AcroForm ไม่สามารถเพิ่มจำนวนหน้าแบบฟอร์มได้ (Static Form) เช่นเดียวกันกับ XFA อย่างไรก็ตาม ไฟล์เอกสาร PDF ในรูปแบบ XFA นี้ ยังไม่ถูกประกาศเป็นมาตรฐานสากลจึงทำให้มีเพียงแอปพลิเคชั่นของบริษัท Adobe Systems Incorporated เท่านั้น ที่สามารถแสดงผลไฟล์เอกสารในรูปแบบดังกล่าวได้

4.2 การจัดทำหนังสือรับรองในรูปแบบไฟล์เอกสาร Portable Document Format (PDF)

จากคุณสมบัติของไฟล์เอกสาร PDF ในรูปแบบต่างๆ ข้างต้น พบว่าไฟล์เอกสาร PDF บางประเภทถูกออกแบบมาเพื่องานเฉพาะด้าน จึงทำให้มีคุณสมบัติที่มากเกินกว่าความต้องการสำหรับการสร้างหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ อีกทั้งยังเป็นภาระแก่ผู้พัฒนาในการจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ให้สอดคล้องตามมาตรฐานดังกล่าว ด้วยเหตุนี้จึงเหลือไฟล์เอกสาร PDF ที่เหมาะสมกับการใช้งานเพียง 4 ประเภทตามตารางด้านล่าง พร้อมทั้งเปรียบเทียบข้อดีและข้อเสียในการนำไฟล์เอกสาร PDF ประเภทต่างๆ มาใช้ในการจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ ดังนี้

ตารางที่ 3 แสดงข้อดีและข้อเสียในการนำไฟล์เอกสาร PDF ประเภทต่างๆ มาใช้ในการจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์

ประเภทของไฟล์เอกสาร PDF	ข้อดี	ข้อเสีย
PDF ที่ใช้งานทั่วไป	● ถูกประกาศให้เป็นมาตรฐานสากล ● แอปพลิเคชั่นแสดงผลทั่วไปไม่สามารถเปลี่ยนแปลงแก้ไขได้ ● รองรับการแนบไฟล์ที่คอมพิวเตอร์สามารถประมวลได้ เพื่อให้มีความสามารถในการแลกเปลี่ยนข้อความที่ปรากฏหรืออยู่ในหนังสือรับรองได้ ● รองรับการลงลายมือชื่ออิเล็กทรอนิกส์ด้วยเทคโนโลยี PKI	● การแสดงผลอาจมีความหมายเปลี่ยนแปลงไปจากเดิมเมื่อมีการจัดเก็บไว้เป็นระยะเวลานาน
PDF/A [3]	● ถูกประกาศให้เป็นมาตรฐานสากล ● แอปพลิเคชั่นแสดงผลทั่วไปไม่สามารถเปลี่ยนแปลงแก้ไขได้ ● PDF/A เวอร์ชัน 2 และ 3 รองรับการแนบไฟล์ที่คอมพิวเตอร์สามารถประมวลได้ เพื่อให้มีความสามารถในการแลกเปลี่ยนข้อความที่ปรากฏหรืออยู่ในหนังสือรับรองได้ ● ถูกออกแบบมาเพื่อการเก็บรักษาเป็นระยะยาว (Long-term Preservation) ทำให้มั่นใจได้ว่าข้อความที่ปรากฏบนหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์จะสามารถแสดงผลได้โดยความหมายไม่เปลี่ยนแปลงไปจากเดิม ● รองรับการลงลายมือชื่ออิเล็กทรอนิกส์ด้วยเทคโนโลยี PKI	● ต้องแนบสิ่งที่จำเป็นต้องใช้ในการแสดงผลหรือประมวลผลทั้งหมดในไฟล์เอกสาร PDF เพื่อให้สามารถแสดงผลได้ถูกต้องอย่างต้นฉบับ

ประเภทของไฟล์เอกสาร PDF	ข้อดี	ข้อเสีย
AcroForm	● ถูกประกาศให้เป็นมาตรฐานสากล ● คอมพิวเตอร์สามารถประมวลข้อความที่ปรากฏหรืออยู่ในหนังสือรับรองได้ ● รองรับการลงลายมือชื่ออิเล็กทรอนิกส์ด้วยเทคโนโลยี PKI	● การแสดงผลอาจมีความหมายเปลี่ยนแปลงไปจากเดิมเมื่อมีการจัดเก็บไว้เป็นระยะเวลานาน ● แอปพลิเคชั่นแสดงผลทั่วไปสามารถเปลี่ยนแปลงแก้ไขได้โดยง่าย หากไม่มีการควบคุม ● ไม่รองรับการแสดงผลเกินกว่าจำนวนหน้าที่ออกแบบไว้
XML Forms Architecture (XFA)	● คอมพิวเตอร์สามารถประมวลข้อความที่ปรากฏหรืออยู่ในหนังสือรับรองได้ ● รองรับการแสดงผลข้อมูลโดยไม่จำกัดจำนวนหน้า ซึ่งเหมาะกับการใช้งานเพื่อเป็นแบบฟอร์มกรอกข้อมูล ● รองรับการลงลายมือชื่ออิเล็กทรอนิกส์ด้วยเทคโนโลยี PKI	● การแสดงผลอาจมีความหมายเปลี่ยนแปลงไปจากเดิมเมื่อมีการจัดเก็บไว้เป็นระยะเวลานาน ● สามารถเปลี่ยนแปลงแก้ไขได้ง่ายโดยแอปพลิเคชั่น หากไม่มีการควบคุม ● ยังไม่ถูกประกาศเป็นมาตรฐานสากลจึงทำให้แอปพลิเคชั่นทั่วไปไม่สามารถเปิดได้
<u>หมายเหตุ</u>: ไฟล์เอกสาร PDF อาจมีโอกาสแสดงผลที่มีความหมายเปลี่ยนแปลงไปจากเดิมเมื่อมีการจัดเก็บไว้เป็นระยะเวลานาน เนื่องจากแอปพลิเคชั่นที่แสดงผลมีข้อมูลไม่เพียงพอที่จะแสดงผลให้ถูกต้อง หรือไม่สามารถแสดงผลสิ่งที่แนบบนหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ได้ถูกต้องอย่างต้นฉบับ เช่น ไม่มีรูปแบบตัวอักษร (Font) แนบมากับหนังสือรับรอง มีการแนบไฟล์ที่ต้องการแอปพลิเคชั่นพิเศษในการแสดงผลซึ่งถูกการยกเลิกการใช้งานไปแล้ว หรือมีการแนบโปรแกรมประยุกต์ (เช่น JavaScript) เพื่อให้ไฟล์เอกสารแสดงผลแตกต่างกันไปตามพฤติกรรมของผู้ใช้ เป็นต้น		

จากตารางเปรียบเทียบข้อดีและข้อเสียในการใช้ไฟล์เอกสาร PDF ประเภทต่างๆ ข้างต้นพบว่าไฟล์เอกสาร PDF ทุกประเภทรองรับคุณสมบัติทั้ง 5 ด้านของหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ คือ

(1) ความเป็นต้นฉบับและสามารถใช้เป็นพยานหลักฐานในศาลได้ (Original Document)

(2) สามารถอ่านเข้าใจได้โดยบุคคล (Human Readable)

(3) สามารถแลกเปลี่ยนข้อความที่ปรากฏหรืออยู่ในหนังสือรับรองได้ (Exchangeable)

(4) การลงลายมือชื่ออิเล็กทรอนิกส์บนหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ (Electronic Signature)

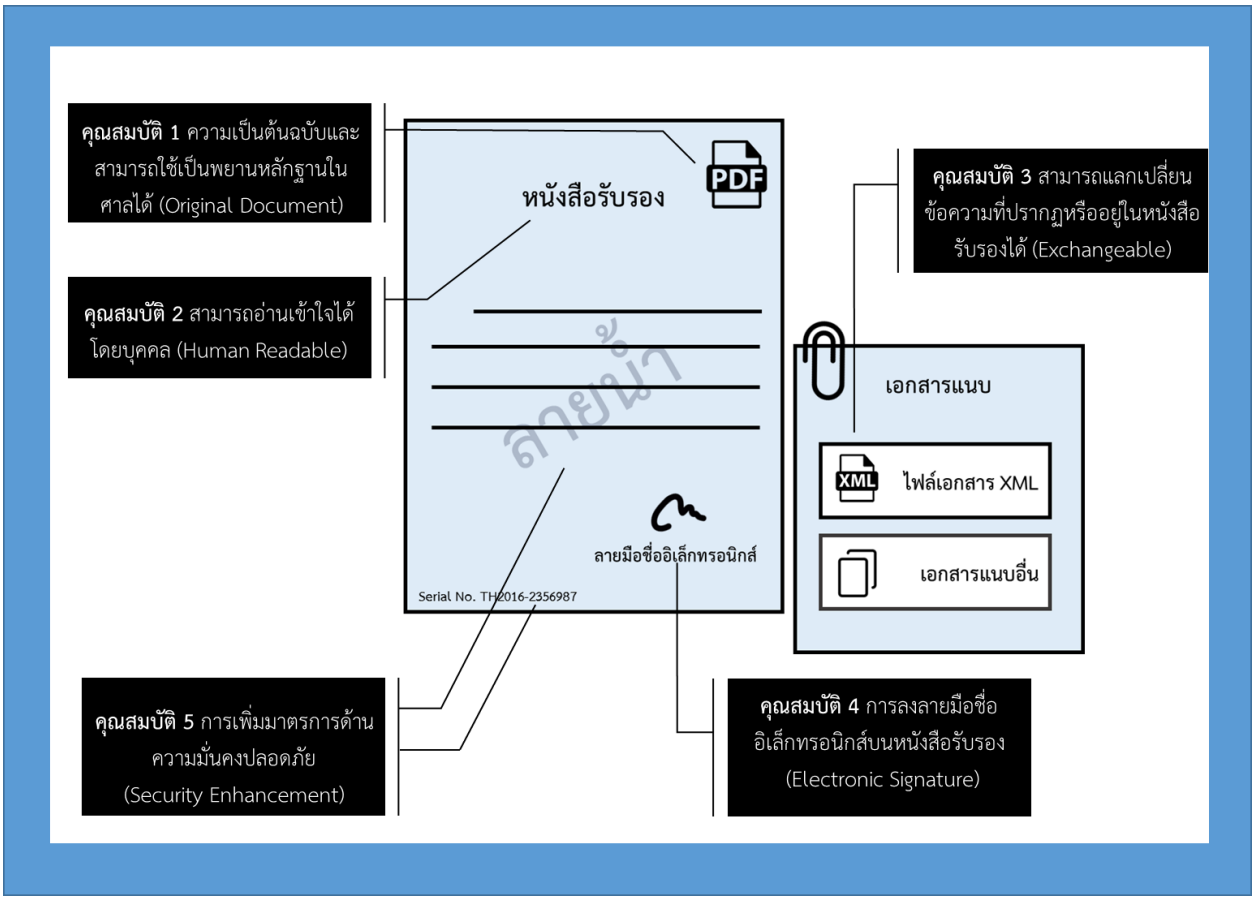
(5) การเพิ่มมาตรการด้านความมั่นคงปลอดภัย (Security Enhancement)

แต่ในการเก็บรักษาหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์เพื่อให้สามารถแสดงผลได้ถูกต้อง แม้จะถูกเก็บรักษาไว้เป็นระยะเวลานาน (Long-term Archive) การจัดทำหนังสือรับรองดังกล่าวให้อยู่ในรูปแบบไฟล์เอกสาร PDF ประเภท PDF/A จึงมีความเหมาะสมมากกว่า เนื่องจากหนังสือรับรองในบางประเภทมีความจำเป็นต้องเก็บรักษาเป็นระยะเวลานานเพื่อใช้เป็นหลักฐานในศาล เช่น ใบสำคัญแสดงการจดทะเบียนบริษัท หนังสือรับรองการจบการศึกษา หนังสือรับรองยอดบัญชีเงินฝาก เป็นต้น ด้วยเหตุนี้ข้อเสนอแนะมาตรฐาน

ฉบับนี้จึงกำหนดให้จัดทำหนังสือรับรองในรูปแบบไฟล์เอกสาร PDF ประเภท PDF/A [3] โดยมีรายละเอียดในทางเทคนิคตามหัวข้อที่จะกล่าวถึงถัดไป

5. รายละเอียดทางเทคนิคในการจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์

จากคุณสมบัติไฟล์เอกสาร PDF ประเภท PDF/A [3] ที่กล่าวถึงในบทที่ผ่านมา เมื่อนำมาจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ ให้สอดคล้องตามคุณสมบัติของหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ สามารถแสดงความสัมพันธ์ของคุณสมบัติดังรูปภาพต่อไปนี้



รูปที่ 3 องค์ประกอบต่างๆ ของหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์

อย่างไรก็ตาม การสร้างหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ อาจไม่จำเป็นต้องจัดทำให้สอดคล้องตามคุณสมบัติทุกข้อ เนื่องจากหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์บางประเภทไม่มีความต้องการนำข้อความที่ปรากฏหรืออยู่ในหนังสือรับรองไปประมวลผลต่อ รวมถึงไม่มีความต้องการมาตรการในการรักษาความมั่นคงปลอดภัยที่สูงเป็นพิเศษ ข้อเสนอแนะมาตรฐานฉบับนี้จึงได้เสนอเหตุผลและความจำเป็นในการพิจารณาว่าคุณสมบัติข้อใดมีความจำเป็นต่อการใช้งานจริง ดังตารางต่อไปนี้

ตารางที่ 4 แสดงเหตุผลและความจำเป็นในการจัดทำหนังสือรับรองในรูปแบบไฟล์ PDF ประเภท PDF/A ให้สอดคล้องตามคุณสมบัติของหนังสือรับรองอิเล็กทรอนิกส์แต่ละข้อ

	คุณสมบัติของหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์	ความจำเป็นในการจัดทำ	
		จำเป็นต้องมี	จำเป็นในบางกรณี
1.	ความเป็นต้นฉบับและสามารถใช้เป็นพยานหลักฐานในศาลได้ (Original Document) <u>เหตุผลและความจำเป็น:</u> ● เนื่องจากพยานเอกสารจำเป็นต้องใช้เอกสารที่มีสถานะเป็นต้นฉบับ การจัดทำหนังสือรับรองในรูปแบบไฟล์เอกสารประเภท PDF/A ทำให้มั่นใจได้ว่า ข้อความที่ปรากฏบนหนังสือรับรองจะสามารถแสดงผลได้ถูกต้องอย่างต้นฉบับ แม้จะถูกเก็บรักษาไว้เป็นระยะเวลานาน (Long-term Archive)	✓	
2.	สามารถอ่านเข้าใจได้โดยบุคคล (Human Readable) <u>เหตุผลและความจำเป็น</u>: ● เพื่อให้หนังสือรับรองในรูปแบบอิเล็กทรอนิกส์สามารถรองรับการใช้งานพื้นฐาน คือ การพิจารณาข้อความตามที่ปรากฏในหนังสือ หน่วยงานที่ออกหนังสือจึงควรจัดทำหนังสือรับรองที่ผู้รับปลายทางสามารถเข้าใจได้ ในกรณีที่หนังสือรับรองนั้นประกอบด้วยภาษาไทยหรือภาษาอื่นที่ไม่ใช่ภาษาอังกฤษ ไฟล์เอกสารประเภท PDF/A [3] ที่จัดทำจะต้องสอดคล้องในระดับ U (Level U Conformance) ซึ่งจัดทำในรูปแบบ Unicode เพื่อให้หนังสือรับรองในรูปแบบอิเล็กทรอนิกส์สามารถแสดงข้อความตัวอักษรได้ทุกภาษา	✓	
3.	สามารถแลกเปลี่ยนข้อความที่ปรากฏหรืออยู่ในหนังสือรับรองได้ (Exchangeable) <u>เหตุผลและความจำเป็น:</u> ● ในกรณีที่ผู้รับมีความต้องการนำข้อความที่ปรากฏหรืออยู่ในหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ไปประมวลผลต่อ หน่วยงานที่ออกหนังสือรับรองจำเป็นต้องจัดทำหนังสือรับรองในรูปแบบไฟล์ PDF/A-3 (PDF/A เวอร์ชัน 3 ตามมาตรฐาน ISO 19005-3) [3] เพื่อรองรับการแนบไฟล์ที่คอมพิวเตอร์สามารถประมวลผลได้ ● PDF/A-3 [3] รองรับการแนบไฟล์ตามรายการ MIME Media Types [4] ที่ประกาศโดย Internet Assigned Numbers Authority (IANA) ซึ่งไฟล์ Extensible Markup Language (XML) เป็นไฟล์หนึ่งที่อยู่ในรายการดังกล่าว		✓

	คุณสมบัติของหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์	ความจำเป็นในการจัดทำ	
		จำเป็นต้องมี	จำเป็นในบางกรณี
	ข้อเสนอแนะมาตรฐานนี้จึงเสนอให้แนบไฟล์ XML เนื่องจากเป็นไฟล์ที่นิยมใช้ในการแลกเปลี่ยนข้อมูลมากที่สุดในปัจจุบัน • ข้อมูลที่อยู่ในไฟล์ XML ที่ใช้ในการแลกเปลี่ยนข้อมูล ควรอยู่ในรูปแบบที่หน่วยงานที่ออกหนังสือรับรองและผู้รับปลายทางตกลงร่วมกัน เพื่อมิให้เกิดความผิดพลาดในการประมวลผล ทั้งนี้หน่วยงานที่ออกหนังสือรับรองอาจทำการแนบไฟล์อื่นนอกเหนือจากไฟล์ XML เพื่อเป็นข้อมูลเพิ่มเติมแก่ผู้รับปลายทางก็สามารถทำได้		
4.	การลงลายมือชื่ออิเล็กทรอนิกส์บนหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ (Electronic Signature) [5] <u>เหตุผลและความจำเป็น:</u> • เพื่อให้สามารถตรวจสอบได้ว่าหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ออกโดยหน่วยงานที่มีอำนาจและถูกเปลี่ยนแปลงแก้ไขหรือไม่ โดยคอมพิวเตอร์ของผู้รับปลายทางได้ทันที ด้วยเหตุนี้ หนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ทุกฉบับจึงควรมีการลงลายมือชื่ออิเล็กทรอนิกส์โดยหน่วยงานที่รับรอง	✓	
5.	การเพิ่มมาตรการด้านความมั่นคงปลอดภัย (Security Enhancement) <u>เหตุผลและความจำเป็น:</u> • ในการพิจารณามาตรการด้านความมั่นคงปลอดภัยที่จะเพิ่มเติมในหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์นั้นขึ้นอยู่กับหลายปัจจัย เช่น ข้อกำหนดด้านกฎหมาย ความต้องการที่หน่วยงานพิจารณาแล้วเห็นสมควรเพิ่มเติมโดยพิจารณาถึงผลกระทบที่อาจเกิดขึ้นหากมีการปลอมแปลงหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ เป็นต้น		✓

5.1 การจัดทำหนังสือรับรองนิติบุคคลในรูปแบบไฟล์เอกสาร PDF ประเภท PDF/A

เพื่อให้หนังสือรับรองในรูปแบบอิเล็กทรอนิกส์มีคุณสมบัติความเป็นต้นฉบับและสามารถใช้เป็นพยานหลักฐานในศาลได้ (Original Document) สามารถอ่านเข้าใจได้โดยบุคคล (Human Readable) และสามารถแลกเปลี่ยนข้อความที่ปรากฏหรืออยู่ในหนังสือรับรองได้ (Exchangeable) ข้อเสนอแนะมาตรฐานนี้จึงเสนอให้จัดทำหนังสือรับรองดังกล่าวให้อยู่ในรูปแบบไฟล์ PDF ประเภท PDF/A เวอร์ชัน 3 โดยในการออกหนังสือรับรองอิเล็กทรอนิกส์ที่มีภาษาไทยหรือภาษาอื่นที่ไม่ใช่ภาษาอังกฤษนั้น กำหนดให้ต้องจัดทำให้สอดคล้องในระดับ U (Level U Conformance) โดยในทางเทคนิคจะเรียกไฟล์เอกสาร PDF ประเภทนี้ว่า

PDF/A-3U ทั้งนี้หากหนังสือรับรองที่ออกมีเฉพาะตัวอักษรภาษาอังกฤษก็ไม่จำเป็นต้องจัดทำในรูปแบบ PDF/A-3U โดยสามารถจัดทำให้สอดคล้องในระดับ A (Level A Compliance) หรือ B (Level B Compliance) ตามความเหมาะสม ซึ่งในทางเทคนิคจะเรียกไฟล์เอกสารประเภทนี้ว่า PDF/A-3A หรือ PDF/A-3B ตามลำดับ โดยมีรายละเอียดในการจัดทำดังนี้

5.1.1 จัดเตรียมหนังสือรับรองให้อยู่ในรูปแบบ PDF/A-3

หนังสือรับรองที่อยู่ในรูปแบบ PDF/A-3 จะต้องสอดคล้องตามมาตรฐาน ISO 19005-3 ซึ่งเป็นมาตรฐานที่อ้างอิงจากมาตรฐาน ISO 32000-1 (เป็นมาตรฐานของไฟล์เอกสาร PDF ที่รู้จักกันทั่วไป ซึ่งเป็นไฟล์เอกสาร PDF เวอร์ชัน 1.7) และได้มีการพัฒนาต่อเนื่องมาจาก ISO 19005-1 (PDF/A เวอร์ชัน 1 หรือ PDF/A-1) และISO 19005-2 (PDF/A เวอร์ชัน 2 หรือ PDF/A-2) โดยมีรายละเอียดในการจัดทำดังต่อไปนี้

(1) ต้องมีการระบุข้อมูลเมตาดาตา (Metadata) ที่เกี่ยวกับไฟล์เอกสารประเภท PDF/A ในรูปแบบ Extensible Metadata Platform (XMP) [6] โดยต้องมีการระบุค่าดังต่อไปนี้

ตารางที่ 5 แสดงข้อมูลเมตาดาตา (Metadata) ที่เกี่ยวกับไฟล์เอกสารประเภท PDF/A

	ชื่อฟิลด์ข้อมูล	จำนวน	รายละเอียด	ประเภทข้อมูล	ตัวอย่าง
1.	<xmp:ModifyDate>	1..1	วันเวลาที่เกิดการปรับแก้ XMP Metadata	ISODatetime	2016-06-07T10:14:23+07:00
2.	<xmp:CreateDate>	1..1	วันเวลาที่สร้าง XMP Metadata	ISODatetime	2016-06-07T10:14:23+07:00
3.	<pdfaid:part>	1..1	เวอร์ชันของ PDF/A ที่จัดทำ ซึ่งหมายเลขเวอร์ชัน คือ หมายเลข Part ของมาตรฐาน ISO 19005 เช่น ISO 19005-3 หมายถึง PDF/A-3	Integer	3
4.	<pdfaid:conformance>	1..1	ระดับความสอดคล้อง (Level of Conformance) ที่ใช้ในการจัดทำ	String	U, B, A

หมายเหตุ : ในกรณีออกหนังสือรับรองที่ประกอบด้วยตัวอักษรภาษาไทยหรือภาษาอื่นที่ไม่ใช่ภาษาอังกฤษจำเป็นต้องกำหนดให้ระดับความสอดคล้องเป็น U แต่ในกรณีที่หนังสือรับรองมีเพียงตัวอักษรภาษาอังกฤษอาจกำหนดให้ระดับความสอดคล้องเป็น A หรือ B ได้ตามความเหมาะสมของลักษณะงาน ดังนี้

- Level B Compliance (Basic) ใช้ในลักษณะงานทั่วไปและมีเฉพาะตัวอักษรภาษาอังกฤษ

- Level A Compliance (Accessible) ใช้ในลักษณะช่วยให้เครื่องคอมพิวเตอร์สามารถเข้าใจในเนื้อหาของเอกสารได้ดีขึ้น เพื่อช่วยให้บุคคลที่มีข้อจำกัดด้านความพิการทางร่างกาย เช่น ความพิการในด้านการมองเห็นหรือด้านการได้ยิน เป็นต้น สามารถเข้าใจเนื้อหาในหนังสือรับรองได้
- Level U Compliance (Unicode) สำหรับกำหนดให้ข้อความทั้งหมดรองรับ Unicode Format

จากตารางแสดงข้อมูลเมตาดาตาดังกล่าว สามารถสร้างให้อยู่ในรูปแบบ Extensible Metadata Platform (XMP) [6] ได้ดังนี้

```
<?xpacket begin="" id="W5M0MpCehiHzreSzNTczkc9d"?>
<x:xmpmeta x:xmptk="Adobe XMP Core 5.1.0-jc003" xmlns:x="adobe:ns:meta/">
  <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">
    <rdf:Description rdf:about=""
      xmlns:dc="http://purl.org/dc/elements/1.1/"
      xmlns:pdf="http://ns.adobe.com/pdf/1.3/"
      xmlns:pdfaid="http://www.aiim.org/pdfa/ns/id/" xmlns:xmp="http://ns.adobe.com/xap/1.0/">
      <xmp:ModifyDate>2016-06-07T10:14:23+07:00</xmp:ModifyDate>
      <xmp:CreateDate>2016-06-07T10:14:23+07:00</xmp:CreateDate>
      <pdfaid:part>3</pdfaid:part>
  <pdfaid:conformance>U</pdfaid:conformance>
    </rdf:Description>
  </rdf:RDF>
</x:xmpmeta>
<?xpacket end="r"?>
```

(2) ต้องมีการระบุข้อมูลเมตาดาตา (Metadata) ซึ่งเป็นรายละเอียดของหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ ดังต่อไปนี้

ตารางที่ 6 แสดงข้อมูลเมตาดาตา (Metadata) ที่เกี่ยวกับหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์

	ชื่อฟิลด์ข้อมูล	จำนวน	รายละเอียด	ประเภทข้อมูล	ตัวอย่าง
1.	Title	1..1	ชื่อเอกสาร	String	หนังสือรับรองการทำงาน
2.	Author	1..n	ชื่อหน่วยงานที่ออกหนังสือรับรอง	String	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
3.	Subject	1..1	หัวข้อในหนังสือหรือคำอธิบายหนังสือรับรอง	String	หนังสือรับรองการทำงาน เพื่อรับรองการทำงานของ นายสมชาติ รักไทย
4.	Keywords	0..n	คำสำคัญ หรือ คำอธิบายโดยละเอียดเพื่อประโยชน์ในการค้นหาภายหลัง	String	หนังสือรับรองการทำงาน นายสมชาติ รักไทย

	ชื่อฟิลด์ข้อมูล	จำนวน	รายละเอียด	ประเภทข้อมูล	ตัวอย่าง
5.	CreationDate	1..1	วันที่สร้างเอกสาร	ISODateTime	สามารถเลือกรูปแบบให้เหมาะสมกับการใช้งานได้ โดยดูรูปแบบต่างๆ ได้จาก ภาคผนวก ก
6.	ModDate	1..1	วันที่แก้ไขเอกสาร	ISODateTime	

จากตารางแสดงข้อมูลเมตาดาตาดังกล่าว สามารถสร้างให้อยู่ในรูปแบบ Extensible Metadata Platform (XMP) ได้ดังนี้

```
<?xpacket begin="" id="W5M0MpCehiHzreSzNTczkc9d"?>
<x:xmpmeta x:xmptk="Adobe XMP Core 5.1.0-jc003" xmlns:x="adobe:ns:meta/">
  <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">
    <rdf:Description rdf:about=""
      xmlns:dc="http://purl.org/dc/elements/1.1/"
      xmlns:pdf="http://ns.adobe.com/pdf/1.3/"
      xmlns:pdfaid="http://www.aiim.org/pdfa/ns/id/" xmlns:xmp="http://ns.adobe.com/xap/1.0/">
      <dc:title>
        <rdf:Alt>
          <rdf:li xml:lang="x-default">หนังสือรับรองการผ่านการอบรมโครงการ TeDA</rdf:li>
        </rdf:Alt>
      </dc:title>
      <dc:creator>
        <rdf:Seq>
          <rdf:li>สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)</rdf:li>
        </rdf:Seq>
      </dc:creator>
      <dc:description>
        <rdf:Alt>
          <rdf:li xml:lang="x-default">หนังสือรับรองการผ่านการอบรม เพื่อนายสมชาติ รักไทย</rdf:li>
        </rdf:Alt>
      </dc:description>
      <pdf:Keywords>หนังสือรับรองการผ่านการอบรม โครงการ TeDA นายสมชาติ รักไทย </pdf:Keywords>
      <xmp:ModifyDate>2016-06-17T16:35:39+07:00</xmp:ModifyDate>
      <xmp:CreateDate>2016-06-17T16:35:39+07:00</xmp:CreateDate>
      <pdfaid:part>3</pdfaid:part>
      <pdfaid:conformance>U</pdfaid:conformance>
    </rdf:Description>
  </rdf:RDF>
</x:xmpmeta>
<?xpacket end="r"?>
```

(3) แนบรูปแบบตัวอักษร (Font) ที่ใช้งานทั้งหมดลงในไฟล์เอกสาร PDF/A เพื่อให้สามารถแสดงผลได้ถูกต้องอย่างต้นฉบับ แม้ถูกเก็บรักษาไว้เป็นระยะเวลานาน อย่างไรก็ตามเพื่อลดขนาดของไฟล์เอกสาร PDF/A อาจแนบรูปแบบตัวอักษร (Font) เฉพาะตัวอักษรหรือตัวเลขบางส่วนที่ใช้งานเท่านั้นก็ได้ ทั้งนี้ในการแนบรูปแบบตัวอักษร (Font) แนะนำให้ฝั่งผู้รับและผู้ส่งตกลงกันว่าจะแสดงผลด้วยรูปแบบตัวอักษร (Font) ใด

(4) ห้ามมิให้แนบไฟล์เสียงหรือภาพยนตร์ที่ต้องแสดงผลให้ปรากฏบนหนังสือรับรอง

(5) ห้ามมิให้แนบโปรแกรมประยุกต์ที่ทำให้การแสดงผลเปลี่ยนแปลงไปตามพฤติกรรมของผู้ใช้ เช่น JavaScript เป็นต้น

(6) รูปภาพที่ปรากฏบนเอกสารจำเป็นต้องอยู่ในรูปแบบ CCITT Group 3, CCITT Group 4, JPEG, JBIG2, JPEG2000 เท่านั้น เพื่อประโยชน์ในการเปิดใช้งานเอกสารในระยะยาวและเป็นรูปแบบเดียวกัน

(7) ในกรณีที่หน่วยงานไม่มีความต้องการพิเศษเกี่ยวกับสีของรูปภาพที่ปรากฏในหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ ควรกำหนดรูปแบบของสีที่ใช้กับรูปภาพ (Color Profile) ให้เป็น sRGB ซึ่งเป็นรูปแบบของสีที่เป็นมาตรฐาน

(8) ในกรณีที่มีความต้องการพิมพ์หนังสือรับรองในรูปแบบอิเล็กทรอนิกส์เพื่อใช้งานในรูปแบบกระดาษ รูปภาพที่ปรากฏในหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ควรมีความละเอียดของภาพ (Resolution) และความละเอียดของสี (Bit Depth) ขั้นต่ำ ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. 2553 หมวด 2 [7] ดังนี้

(8.1) ภาพลายเส้นหรือภาพขาวดำ ควรมีความละเอียดของภาพอย่างน้อย 150 จุดต่อนิ้ว (dot per inch หรือ dpi) และมีค่าความละเอียดของสีเท่ากับ 1 บิต (bit)

(8.2) ภาพสีเทา ควรมีความละเอียดของภาพอย่างน้อย 200 จุดต่อนิ้ว และมีค่าความละเอียดของสีเท่ากับ 8 บิต

(8.3) ภาพสี ควรมีความละเอียดของภาพอย่างน้อย 300 จุดต่อนิ้ว และมีค่าความละเอียดของสีเท่ากับ 24 บิต

5.2 การแนบไฟล์เพื่อประโยชน์ในการแลกเปลี่ยนข้อความที่ปรากฏหรืออยู่ในหนังสือรับรอง

5.2.1 การแนบไฟล์ XML ในไฟล์เอกสาร PDF/A

เพื่อให้สามารถแลกเปลี่ยนข้อความที่ปรากฏหรืออยู่ในหนังสือรับรองได้ (Exchangeable) ข้อเสนอแนะมาตรฐานนี้จึงเสนอให้แนบไฟล์ XML เนื่องจากเป็นไฟล์ที่คอมพิวเตอร์สามารถประมวลผลได้และนิยมใช้ในการแลกเปลี่ยนข้อมูลมากที่สุดในปัจจุบัน ดังนั้นข้อเสนอแนะมาตรฐานนี้จึงเสนอให้แนบไฟล์ XML พร้อมระบุรายละเอียดเกี่ยวกับไฟล์ XML ที่แนบ ดังต่อไปนี้

(1) ชื่อไฟล์ XML ที่แนบเพื่อแลกเปลี่ยนข้อความที่ปรากฏหรืออยู่ในหนังสือรับรอง จะต้องกำหนดชื่อให้เป็น ***ContentInformation.xml*** สำหรับการทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ประเภทต่างๆ ที่แตกต่างกันไป เช่น หนังสือรับรองฐานะทางการเงินที่ออกโดยธนาคารพาณิชย์ หนังสือรับรองการถือครองหลักทรัพย์ที่ออกโดยบริษัทหลักทรัพย์ หนังสือรับรองการทำงานที่ออกโดยนายจ้าง เป็นต้น จะมีชื่อไฟล์ที่เหมือนกัน คือ ContentInformation.xml แต่ข้อมูลที่เก็บในไฟล์จะมีความแตกต่างกันไปตามประเภทของหนังสือรับรอง

(2) ไฟล์ XML ที่แนบต้องแนบในระดับเอกสาร (Document Level) เนื่องจาก ไฟล์ XML แสดงถึงข้อความของหนังสือรับรองทั้งฉบับ (ไม่จำเพาะเจาะจงสำหรับหน้าใดหน้าหนึ่ง)

(3) ระบุชื่อไฟล์ ContentInformation.xml ในส่วนของ Names ภายใต้ Catalog Dictionary

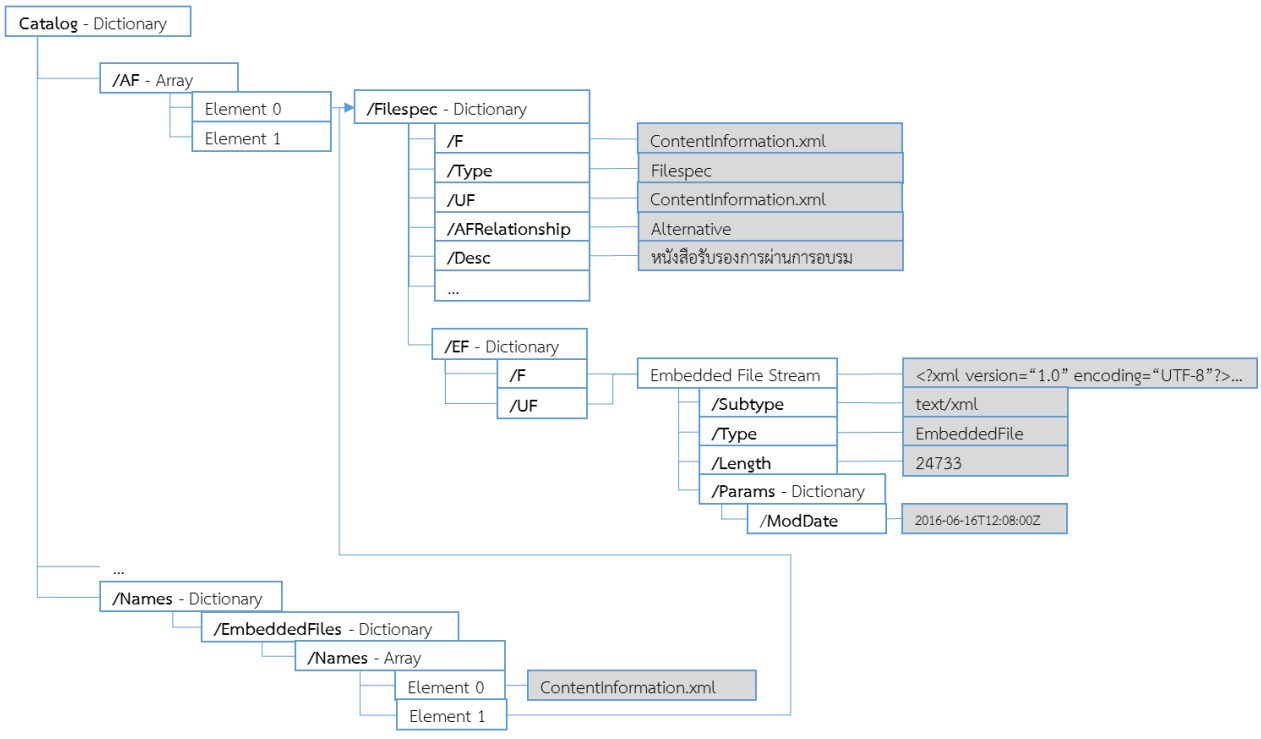
(4) ระบุข้อมูลเกี่ยวกับไฟล์ XML ที่แนบ ในส่วนของ File Specification Dictionary ภายใต้ Catalog Dictionary ดังต่อไปนี้

(4.1) AFRelationship: ระบุความสัมพันธ์ของไฟล์ (Associated file relationships) ที่แนบกับ PDF/A โดยระบุเป็น ***Alternative*** เพื่อบ่งบอกว่าไฟล์ XML ดังกล่าวเป็นรูปแบบหนึ่งของหนังสือรับรอง

(4.2) **Desc :** ระบุคำอธิบายของเนื้อหาไฟล์ XML เช่น ***หนังสือรับรองการผ่านการอบรม***

(4.3) ในส่วนของ Embedded **File Stream** ให้ระบุรายละเอียดดังนี้

- **Subtype:** ระบุประเภทของไฟล์ XML ที่แนบเป็น ***text/xml*** (ตาม MIME Media type ที่ประกาศโดย IANA)
- **ModDate ในส่วนของ Params :** ระบุวันเวลาที่แก้ไขไฟล์ XML ล่าสุดในรูปแบบ *YYYY-MM-DDThh:mm:ssTZD*



รูปที่ 4 โครงสร้างไฟล์เอกสาร PDF/A ภายหลังจากแนบไฟล์ XML

5.2.2 การแนบข้อมูลเมตาดาตา (Metadata) ของไฟล์ XML

เพื่อคอมพิวเตอร์ของผู้รับสามารถรู้ได้ว่าหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ที่ได้รับเป็นหนังสือรับรองประเภทใด และทราบความหมายของข้อมูลที่อยู่ในไฟล์ XML ข้อเสนอแนะมาตรฐานนี้จึงเสนอให้ทำการแนบข้อมูลเมตาดาตา (Metadata) ของไฟล์ XML ในรูปแบบ Extensible Metadata Platform (XMP) ลงในไฟล์เอกสาร PDF/A โดยข้อมูลเมตาดาตาที่แนบประกอบด้วยข้อมูลดังต่อไปนี้

ตารางที่ 7 แสดงข้อมูลเมตาดาตา (Metadata) ของไฟล์ XML

	ชื่อฟิลด์ข้อมูล	จำนวน	รายละเอียด	ประเภทข้อมูล	ตัวอย่าง
1.	DocumentOID	1..1	หมายเลข OID ที่ระบุถึงประเภทหนังสือรับรอง	String	2.16.764.1.3.1000.1.1
2.	DocumentReferenceID	1..1	หมายเลขหนังสือรับรองที่ออกโดยหน่วยงาน	String	สพธอ. 1/2559
3.	DocumentVersion	1..1	หมายเลขเวอร์ชันของหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์	String	1.0
4.	DocumentFileName	1..1	ชื่อไฟล์ XML ที่แนบ	String	ContentInformation.xml

จากตารางแสดงข้อมูลเมตาดาตา (Metadata) ของไฟล์ XML ข้างต้น มีการกำหนดหมายเลข DocumentOID ซึ่งเป็นหมายเลข OID ที่ระบุถึงประเภทของหนังสือรับรอง อีกทั้งหมายเลขดังกล่าวยังสามารถใช้ในการอ้างอิงถึง XML Schema และเอกสารแนวทางการใช้งานข้อมูล XML (Message Usage Guide) ได้ ซึ่งในการใช้หมายเลข OID ดังกล่าวจะช่วยให้หน่วยงานปลายทางสามารถเข้าใจข้อมูลที่อยู่ในไฟล์ XML และสามารถประมวลผลข้อมูลได้อย่างถูกต้อง ซึ่งจากตารางแสดงข้อมูลเมตาดาตา (Metadata) ดังกล่าว สามารถสร้างให้อยู่ในรูปแบบ Extensible Metadata Platform (XMP) ได้ดังนี้

```
<rdf:Description rdf:about="" xmlns:ed="urn:etda:pdfa:ElectronicDocument:1p0:standard#">
   <ed:DocumentOID>2.16.764.1.3.1000.1.1</ed:DocumentOID>
   <ed:DocumentReferenceID>สพธอ 01/2559</ed:DocumentReferenceID>
   <ed:DocumentVersion>1.0</ed:DocumentVersion>
   <ed:DocumentFileName>ContentInformation.xml</ed:DocumentFileName>
</rdf:Description>
<rdf:Description rdf:about=""
      xmlns:pdfaExtension="http://www.aiim.org/pdfa/ns/extension/"
      xmlns:pdfaSchema="http://www.aiim.org/pdfa/ns/schema#"
      xmlns:pdfaProperty="http://www.aiim.org/pdfa/ns/property#">
<pdfaExtension:schemas>
   <rdf:Bag>
      <rdf:li rdf:parseType="Resource">
        <pdfaSchema:schema>Electronic Document PDFA Extension Schema
      </pdfaSchema:schema>
        <pdfaSchema:namespaceURI>urn:etda:pdfa:ElectronicDocument:1p0:standard#
           </pdfaSchema:namespaceURI>
        <pdfaSchema:prefix>ed</pdfaSchema:prefix>
        <pdfaSchema:property>
           <rdf:Seq>
             <rdf:li rdf:parseType="Resource">
                <pdfaProperty:name>DocumentOID</pdfaProperty:name>
                <pdfaProperty:valueType>Text</pdfaProperty:valueType>
                <pdfaProperty:category>external</pdfaProperty:category>
                <pdfaProperty:description>OID of Exchange Document Associated File
                  </pdfaProperty:description>
             </rdf:li>
```

```
            <rdf:li rdf:parseType="Resource">
               <pdfaProperty:name>DocumentReferenceID
               </pdfaProperty:name>
               <pdfaProperty:valueType>Text</pdfaProperty:valueType>
               <pdfaProperty:category>internal</pdfaProperty:category>
                  <pdfaProperty:description>Document Identification from document's
                     author</pdfaProperty:description>
            </rdf:li>
            <rdf:li rdf:parseType="Resource">
               <pdfaProperty:name>DocumentVersion</pdfaProperty:name>
               <pdfaProperty:valueType>Text</pdfaProperty:valueType>
               <pdfaProperty:category>external</pdfaProperty:category>
               <pdfaProperty:description>Version of document
                  </pdfaProperty:description>
            </rdf:li>
            <rdf:li rdf:parseType="Resource">
               <pdfaProperty:name>DocumentFileName</pdfaProperty:name>
               <pdfaProperty:valueType>Text</pdfaProperty:valueType>
               <pdfaProperty:category>external</pdfaProperty:category>
               <pdfaProperty:description>File name of Exchange Document Associated
                  File</pdfaProperty:description>
            </rdf:li>
         </rdf:Seq>
      </pdfaSchema:property>
   </rdf:li>
</rdf:Bag>
</pdfaExtension:schemas>
</rdf:Description>
```

5.2.3 การแนบเอกสารอื่นเพิ่มเติมในไฟล์เอกสาร PDF/A

ในกรณีที่ต้องการแนบไฟล์เอกสารอื่นเพิ่มเติมเพื่อประโยชน์ในการอ้างอิงเพิ่มเติม ข้อเสนอแนะมาตรฐานนี้ยินยอมให้มีการแนบเอกสารแนบอื่นได้ โดยไม่จำเป็นต้องแนบข้อมูลเมตาดาตา (Metadata) ของเอกสารแนบ แต่ยังคงต้องมีการระบุรายละเอียดเกี่ยวกับเอกสารแนบดังนี้

(1) ข้อเสนอแนะมาตรฐานนี้เสนอให้แนบเอกสารแนบเพิ่มเติมในระดับเอกสาร (Document Level) เท่านั้น เพื่อให้ง่ายต่อการเข้าถึงของผู้รับปลายทางในการค้นหา

(2) ระบุชื่อไฟล์เอกสารแนบในส่วนของ **Names** ภายใต้ **Catalog Dictionary** เช่น Syllabus.doc

(3) ระบุข้อมูลเกี่ยวกับไฟล์เอกสารแนบในส่วนของ **File Specification Dictionary** ภายใต้ **Catalog Dictionary** ดังต่อไปนี้

(3.1) **AFRelationship:** ระบุความสัมพันธ์ของไฟล์ (Associated file relationships) ที่แนบกับไฟล์เอกสาร PDF/A โดยค่าที่สามารถระบุใน AFRelationship นี้ได้ประกอบด้วย

- Source
- Data

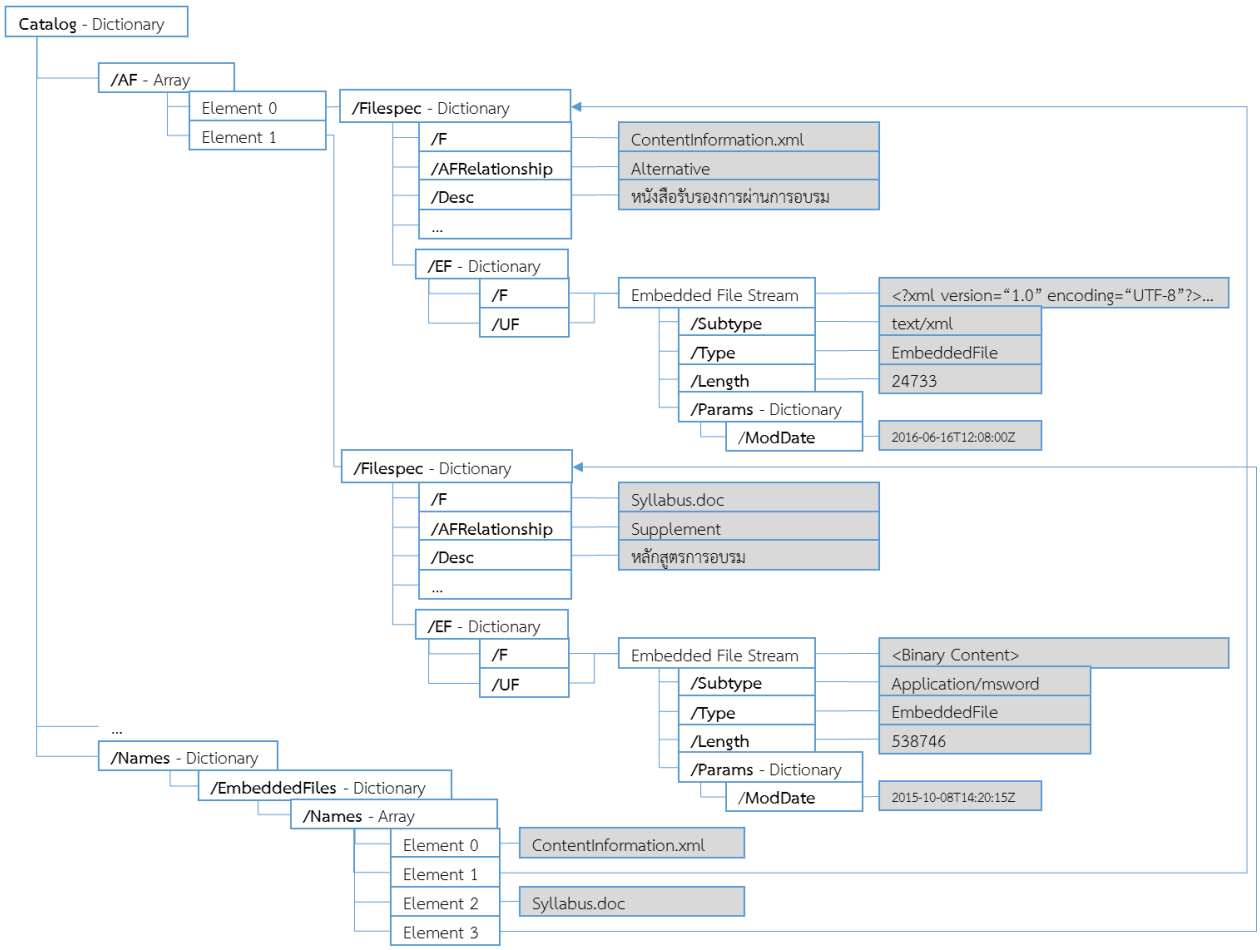
- Alternative
- Supplement
- Unspecified

โดยความหมายของแต่ละค่าเป็นไปตามข้อกำหนดของตามมาตรฐาน ISO 19005-3 ซึ่งสามารถดูรายละเอียดได้ตามภาคผนวก ค

(3.2) **Desc :** ระบุคำอธิบายของไฟล์เอกสารแนบ เช่น ***หลักสูตรการอบรม***

(3.3) ในส่วนของ **Embedded File Stream** ให้ระบุรายละเอียดดังนี้

- **Subtype:** ระบุประเภทของไฟล์เอกสารแนบตาม MIME Media type ที่ประกาศโดย IANA ในกรณีที่ไม่มีประเภทของไฟล์ที่ต้องการแนบในประกาศดังกล่าว ให้ระบุค่าเป็น **application/octet-stream**
- **ModDate ในส่วนของ Params :** ระบุวันเวลาที่แก้ไขไฟล์เอกสารแนบล่าสุดในรูปแบบ *YYYY-MM-DDThh:mm:ssTZD*



รูปที่ 5 โครงสร้างไฟล์เอกสาร PDF/A ภายหลังจากแนบเอกสารอื่นเพิ่มเติม

5.3 การลงลายมือชื่ออิเล็กทรอนิกส์บนหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์

5.3.1 การลงลายมือชื่ออิเล็กทรอนิกส์

เพื่อให้คอมพิวเตอร์ของผู้รับปลายทางสามารถตรวจสอบได้ว่าข้อความที่ปรากฏหรืออยู่ในหนังสือรับรองถูกรับรองโดยหน่วยงานที่มีอำนาจ ไม่ถูกเปลี่ยนแปลงแก้ไข และสามารถนำข้อความดังกล่าวไปใช้ในการอ้างอิงได้ ด้วยเหตุนี้หนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ทุกฉบับจึงควรมีการลงลายมือชื่ออิเล็กทรอนิกส์โดยหน่วยงานที่มีอำนาจและสอดคล้องตามมาตรฐานสากล ซึ่งมาตรฐานสากลที่ข้อเสนอแนะมาตรฐานนี้เสนอให้ใช้คือ ลายมือชื่ออิเล็กทรอนิกส์ในรูปแบบ PAdES Basic ตามมาตรฐาน ETSI TS 102 778-2 Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1 [5]

แต่อย่างไรก็ตาม เพื่อให้ลายมือชื่ออิเล็กทรอนิกส์มีความเหมาะสมกับการใช้งานบนหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ ข้อเสนอแนะมาตรฐานนี้จึงมีการกำหนดหลักเกณฑ์ในการลงลายมือชื่ออิเล็กทรอนิกส์เพิ่มเติม โดยมีรายละเอียดที่สำคัญดังต่อไปนี้

(1) ลายมือชื่ออิเล็กทรอนิกส์จะต้องอยู่ในรูปแบบ Cryptographic Message Syntax (CMS) ตามมาตรฐาน PKCS #7 เวอร์ชัน 1.5 (หรือตาม RFC 2315)

(2) มีการประทับรับรองเวลา (Time Stamping) ในขณะที่ลงลายมือชื่ออิเล็กทรอนิกส์
เนื่องจากในการลงลายมือชื่ออิเล็กทรอนิกส์ทุกครั้งจะมีการระบุวัน-เวลาที่ลงลายมือชื่ออิเล็กทรอนิกส์ โดยใช้เวลาของเครื่องคอมพิวเตอร์ที่ทำการลงลายมือชื่อ เพื่อเป็นการป้องกันปัญหาข้อพิพาทเกี่ยวกับเวลาในการจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ เช่น หนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ถูกจัดทำเมื่อใด ถูกจัดทำขึ้นในภายหลังโดยมีวัตถุประสงค์ที่มิชอบหรือไม่ เป็นต้น ข้อเสนอแนะมาตรฐานนี้จึงเสนอให้ทำการประทับรับรองเวลาที่สอดคล้องตาม RFC 3161 ณ ขณะที่ลงลายมือชื่ออิเล็กทรอนิกส์ทุกครั้ง โดยแนบเวลาที่ได้รับการประทับรับรอง (Time-Stamp Token) ในลายมือชื่ออิเล็กทรอนิกส์ตามรูปแบบที่ ISO 32000-1 กำหนด

(3) แนบใบรับรองอิเล็กทรอนิกส์ตามมาตรฐาน X.509 ทุกใบที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์
ใบรับรองอิเล็กทรอนิกส์ตามมาตรฐาน X.509 หรือใบรับรอง X.509 Certificate เป็นข้อมูลสำคัญที่ใช้ในการตรวจสอบความน่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์ เนื่องจากใบรับรอง X.509 Certificate เป็นสิ่งที่ใช้ในการตรวจสอบว่า ลายมือชื่ออิเล็กทรอนิกส์บนหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์เป็นของหน่วยงานที่มีอำนาจรับรองหรือไม่ ด้วยการระบุชื่อผู้มีอำนาจลงนามและ/หรือหน่วยงานที่ออกหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ไว้ ด้วยเหตุนี้ในการลงลายมือชื่ออิเล็กทรอนิกส์ทุกครั้ง จึงควรมีการแนบใบรับรอง X.509 Certificate ทุกใบที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์ตามรูปแบบที่ ISO 32000-1 กำหนด ซึ่งประกอบด้วย

(3.1) ใบรับรอง X.509 Certificate ของหน่วยงานที่มีอำนาจออกหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์

(3.2) ใบรับรอง X.509 Certificte ของผู้ให้บริการออกใบรับรอง (Certification Authority: CA) ซึ่งเป็นใบรับรอง X.509 Certificate ของบุคคลที่สามที่รับรองว่า ใบรับรอง X.509 Certificate ของหน่วยงานที่ออกหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์มีตัวตนอยู่จริง ลายมือชื่ออิเล็กทรอนิกส์ที่เกิดจากใบรับรอง X.509 Certificate มีผลผูกพันกับหน่วยงานที่ออกหนังสือรับรองดังกล่าว

เพื่อให้สามารถตรวจสอบความน่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์แม้ว่าจะเก็บรักษาไว้เป็นระยะเวลานาน และมีผลผูกพันทางกฎหมายกับหน่วยงานที่มีอำนาจออกหนังสือรับรอง

(4) แนบข้อมูลเพื่อใช้ในการตรวจสอบสถานะของใบรับรอง X.509 Certificate
เพื่อให้สามารถตรวจสอบความน่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์บนหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ในภายหลังได้แม้จะเก็บไว้เป็นระยะเวลานาน ข้อเสนอแนะมาตรฐานนี้จึงเสนอให้ทำการแนบข้อมูลที่ใช้ในการตรวจสอบสถานะของใบรับรอง X.509 Certificate ที่ใช้ในการลงลายมือชื่ออิเล็กทรอนิกส์ว่าถูกเพิกถอนหรือไม่ ตามรูปแบบที่ ISO 32000-1 กำหนด ซึ่งในการแนบข้อมูลดังกล่าวสามารถแนบข้อมูลได้ 2 รูปแบบ คือ

(4.1) รายการเพิกถอนใบรับรอง (Certificate Revocation List: CRL)

(4.2) ข้อมูลสถานะของใบรับรองในรูปแบบ Online Certificate Status Protocol (OCSP)

โดยในการแนบข้อมูลดังกล่าวข้างต้นในลายมือชื่ออิเล็กทรอนิกส์ จำเป็นต้องแนบข้อมูลสำหรับตรวจสอบสถานะของใบรับรอง X.509 Certificate ทุกใบที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์ นอกจากนี้ก่อนการแนบข้อมูลดังกล่าวในลายมือชื่ออิเล็กทรอนิกส์ จำเป็นต้องใช้ข้อมูลดังกล่าวตรวจสอบสถานะของใบรับรอง X.509 Certificate ว่าถูกเพิกถอน ณ ขณะที่ลงลายมือชื่ออิเล็กทรอนิกส์หรือไม่

(5) แนบข้อมูลอื่นที่เกี่ยวข้องลายมือชื่ออิเล็กทรอนิกส์
มาตรฐาน ISO 32000-1 ได้ออกแบบให้ลายมือชื่ออิเล็กทรอนิกส์สามารถแนบข้อมูลอื่นที่เกี่ยวข้องได้ ได้แก่ วัตถุประสงค์หรือเหตุผล (Reason) ในการลงลายมือชื่ออิเล็กทรอนิกส์ สถานที่ (Location) ที่ลงลายมือชื่ออิเล็กทรอนิกส์ และข้อมูลสำหรับติดต่อ (Contact Info) เจ้าของลายมือชื่ออิเล็กทรอนิกส์ ซึ่งหน่วยงานอาจแนบข้อมูลดังกล่าวได้ตามความเหมาะสม

(6) กำหนดสถานะของหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ให้อยู่ในสถานะไม่สามารถแก้ไขได้ (Read Only)
ภายหลังแนบข้อมูลที่จำเป็นในการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์เรียบร้อยแล้ว จำเป็นต้องกำหนดให้หนังสือรับรองในรูปแบบอิเล็กทรอนิกส์อยู่ในสถานะที่ไม่สามารถแก้ไขได้ (Read Only) เพื่อป้องกันการเปลี่ยนแปลงแก้ไขโดยมิชอบอีกครั้ง

5.3.2 การตรวจสอบลายมือชื่ออิเล็กทรอนิกส์

เมื่อผู้รับปลายทางได้รับหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ ผู้รับปลายทางจะต้องทำการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ เพื่อให้มั่นใจได้ว่าข้อความที่ปรากฏหรืออยู่ในหนังสือรับรองได้รับรอง

โดยหน่วยงานที่มีอำนาจจริง ไม่ถูกเปลี่ยนแปลงแก้ไข และสามารถนำข้อความดังกล่าวไปใช้ในการอ้างอิงได้ ผู้รับปลายทางจะต้องทำการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ดังรายละเอียดต่อไปนี้

(1) ตรวจสอบค่าแฮช (Hash Value) ของหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ตามที่ ISO 32000-1 กำหนด

ค่าแฮช (Hash Value) เปรียบเสมือนตัวแทนของข้อมูลที่สร้างจากสมการทางคณิตศาสตร์ เมื่อข้อมูลหนึ่งถูกเปลี่ยนแปลงแก้ไขตัวแทนของข้อมูลดังกล่าวก็จะเปลี่ยนแปลงตามไปด้วย ซึ่งจากเทคนิคดังกล่าวข้างต้น หากค่าแฮชหรือตัวแทนข้อมูลของหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ ณ ขณะที่ผู้รับปลายทางเปิดอ่าน ไม่ตรงกันกับค่าแฮชของหนังสือรับรองดังกล่าวที่ถูกสร้างขึ้น ณ ขณะที่ลงลายมือชื่ออิเล็กทรอนิกส์ (ถูกแนบอยู่ในลายมือชื่ออิเล็กทรอนิกส์) นั้นหมายความว่าหนังสือรับรองดังกล่าวถูกเปลี่ยนแปลงแก้ไขภายหลังจากที่มีการลงลายมือชื่ออิเล็กทรอนิกส์โดยหน่วยงานที่มีอำนาจ

(2) ตรวจสอบว่าลายมือชื่ออิเล็กทรอนิกส์บนหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ เป็นของหน่วยงานที่มีอำนาจหรือไม่ โดยการตรวจสอบข้อมูล Distinguished Name ซึ่งระบุชื่อหน่วยงานที่ออกหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ (ระบุอยู่ในใบรับรอง X.509 Certificate) เพื่อให้มั่นใจได้ว่าลายมือชื่ออิเล็กทรอนิกส์เป็นของหน่วยงานที่มีอำนาจจริง

(3) ตรวจสอบความน่าเชื่อถือของใบรับรอง X.509 Certificate ทุกใบที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์ตาม RFC 5280

ในการตรวจสอบความน่าเชื่อถือดังกล่าว จะต้องตรวจสอบว่าใบรับรอง X.509 Certificate ทุกใบที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์มีความน่าเชื่อถือ ณ เวลาที่ได้รับการประทับรับรอง (Time Stamping) เพื่อให้มั่นใจได้ว่าใบรับรอง X.509 Certificate ที่ใช้ในการลงลายมือชื่ออิเล็กทรอนิกส์น่าเชื่อถือ และมีผลผูกพันกับหน่วยงานที่ออกหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์

(4) ตรวจสอบสถานะของใบรับรอง X.509 Certificate ทุกใบที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์ว่าถูกเพิกถอน ณ เวลาที่ได้รับการประทับรับรอง (Time Stamping) หรือไม่ เพื่อให้มั่นใจได้ว่าใบรับรอง X.509 Certificate มีผลผูกพันกับหน่วยงานที่ออกหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ ณ เวลาดังกล่าว อย่างไรก็ตาม ผู้รับปลายทางอาจตรวจสอบสถานะของใบรับรอง X.509 Certificate จากรายการเพิกถอนใบรับรอง (CRL) หรือข้อมูลสถานะของใบรับรอง X.509 Certificate ในรูปแบบ OCSP ที่แนบมากับลายมือชื่ออิเล็กทรอนิกส์ หรือจากแหล่งข้อมูลอื่นตามแนวปฏิบัติของผู้รับปลายทาง

5.3.3 อัลกอริทึมสำหรับลงลายมือชื่ออิเล็กทรอนิกส์

เพื่อให้ลายมือชื่ออิเล็กทรอนิกส์มีความน่าเชื่อถือ ข้อเสนอแนะมาตรฐานนี้จึงเสนอให้ใช้อัลกอริทึมในการลงลายมือชื่ออิเล็กทรอนิกส์ (Signature Algorithm) บนหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ดังต่อไปนี้

ตารางที่ 8 แสดงอัลกอริทึมที่เสนอให้ใช้ในการลงลายมือชื่ออิเล็กทรอนิกส์

ประเภทอัลกอริทึม (Algorithm)	ข้อเสนอแนะในการใช้งาน
อัลกอริทึมสำหรับสร้างค่าแฮช (Hash Algorightm)	SHA-224 SHA-256 SHA-384 SHA-512
อัลกอริทึมสำหรับเข้ารหัสลับด้วยกุญแจแบบอสมมาตร (Asymmetric Key Algorithm)	RSA ที่มีขนาดกุญแจ 2048 บิต

5.3.4 ใบรับรองอิเล็กทรอนิกส์ตามมาตรฐาน X.509 (X.509 Certificate) สำหรับลงลายมือชื่ออิเล็กทรอนิกส์

เพื่อให้คอมพิวเตอร์ของผู้รับปลายทางสามารถตรวจสอบลายมือชื่ออิเล็กทรอนิกส์บนหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ได้ ใบรับรอง X.509 Certificate ที่หน่วยงานใช้ลงลายมือชื่ออิเล็กทรอนิกส์ จะต้องออกโดยผู้ให้บริการออกใบรับรอง (Certification Authority: CA) ที่ผู้รับปลายทางเชื่อถือ (Trust) และติดตั้งใบรับรองอิเล็กทรอนิกส์ระดับชั้นบนสุด (Root CA Certificate) ในเครื่องคอมพิวเตอร์ของผู้รับปลายทาง

5.4 การเพิ่มมาตรการด้านความมั่นคงปลอดภัย (Security Enhancement)

การเพิ่มมาตรการด้านความมั่นคงปลอดภัยให้แก่หนังสือรับรองในรูปแบบอิเล็กทรอนิกส์เป็นสิ่งที่หน่วยงานสามารถดำเนินการเพิ่มเติมได้ เช่น การจัดทำหมายเลขอ้างอิงในลักษณะเดียวกันกับหมายเลขต้นขั้วเช็ค การแสดงลายน้ำ (Watermark) การแทรกข้อความขนาดเล็ก (Micro Text) เป็นต้น อย่างไรก็ตามในการเพิ่มมาตรการดังกล่าวจำเป็นต้องสอดคล้องตามข้อกำหนดของมาตรฐาน ISO 32000-1 และ ISO19005-3 [3] อีกทั้งยังต้องไม่ส่งผลกระทบต่อการแสดงผลและประมวลไฟล์เอกสาร PDF ของผู้รับปลายทาง

ภาคผนวก ก

รูปแบบของวันที่ที่ใช้ในหนังสือรับรองอิเล็กทรอนิกส์

รูปแบบของวันที่ ที่สามารถใช้ในการออกหนังสือรับรองอิเล็กทรอนิกส์ ได้แก่

1. YYYY
2. YYYY-MM
3. YYYY-MM-DD
4. YYYY-MM-DDThh:mmTZD
5. YYYY-MM-DDThh:mm:ssTZD
6. YYYY-MM-DDThh:mm:ss.sTZD

โดยมีความหมาย คือ

รูปแบบ	ความหมาย
YYYY	four-digit year
MM	two-digit month (01=January)
DD	two-digit day of month (01 to 31)
hh	two digits of hour (00 to 23)
mm	two digits of minute (00 to 59)
ss	two digits of second (00 to 59)
s	one or more digits representing a decimal fraction of a second
TZD	time zone designator (Z or +hh:mm or -hh:mm)

สามารถแสดงตัวอย่างการใช้งาน ดังนี้

(1) กรณีที่มีการชดเชยเวลา (time offset) จะมีการระบุเครื่องหมาย + หรือ – และตามด้วยเวลาที่ชดเชย เช่น 2004-10-23T12:00:00+07:00

(2) กรณีที่ไม่มีการชดเชยเวลา (time offset) จะถือว่าเวลาที่ระบุเป็นเวลากลางของโลก หรือ Coordinated Universal Time (UTC) ซึ่งจะมีการระบุตัวอักษร Z ในส่วนท้าย เช่น 2004-10-23T12:00:00Z

ภาคผนวก ข

ตารางที่ ข.1 การเปรียบข้อมูลเมตาดาตา (Metadata) ระหว่าง PDF และ XMP ตาม Dublin Core

PDF		XMP	
PDF Field	Data Type	XMP Property	Data Type
Title	Text String	dc:title[“x-default”]	Text
Author	Text String	dc:creator[0]	ProperName
Subject	Text String	dc:description[“x-deafult”]	Text
Keywords	Text String	pdf:Keywords	Text
CreationDate	Date	xmp:CreationDate	Date
ModDate	Date	xmp:ModifyDate	Date

ภาคผนวก ค

ตารางที่ ค.1 แสดงความหมายของค่า AFRelationship เพื่อระบุความสัมพันธ์ของไฟล์ (Associated file relationships) ที่แนบกับไฟล์เอกสาร PDF/A

AFRelationship	คำอธิบาย
Data	The embedded file contains data which is used for the visual representation in the PDF part, e.g. for a table or a graph.
Source	The embedded file contains the source data for the visual representation derived therefrom in the PDF part, e.g. a PDF file created via an XSL transformation from an (embedded) XML source file or the MS Word file from which the PDF file was created.
Alternative	This data relationship should be used if the embedded data are an alternative representation of the PDF contents.
Supplement	This data relationship is used if the embedded file serves neither as the source nor as the alternative representation, but the file contains additional information, e.g. on easier automatic processing.
Unspecified	If none of the data relationships above apply or there is an unknown data relationship, this data relationship is used.

บรรณานุกรม

[1] สำนักนายกรัฐมนตรี, ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ พ.ศ. 2526.

[2] พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาตรา 7, มาตรา 8 วรรค 1, มาตรา 9 วรรค 1, มาตรา 10, มาตรา 11, มาตรา 26 วรรค 1.

[3] ISO, Document management – Electronic document file format for long- term preservation - Part 3 : Use of ISO 32000-1 with support for embedded files (PDF/A-3), ISO 19005-3, 2012.

[4] Internet Assigned Numbers Authority, “Media Types,” Internet Assigned Numbers Authority (IANA), 20 06 2016. [ออนไลน์]. Available: http://www.iana.org/assignments/media-types/media-types.xhtml. [%1 ที่เข้าถึง27 06 2016].

[5] Electronic Signatures and Infrastructures (ESI), ETSI TS 102 778-2 PDF Advanced Electronic Signature Profiles;, FRANCE: ETSI, 2009.

[6] ISO, Graphic technology - Extensible metadata platform (XMP) specification - Part 1: Data model, serialization and core properties, ISO 16684-1, 2012.

[7] ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. 2553 หมวด 2.