มาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำหรับธุรกรรมภาษีทางอิเล็กทรอนิกส์

ว่าด้วยการลงลายมือชื่ออิเล็กทรอนิกส์

RD ICT Standard for Electronic Tax Transactions

: Electronic Signature

RD STD. [05-2566]

กรมสรรพากร

Version 01.00.0000

คำนำ

ปัจจุบันความก้าวหน้าทางเทคโนโลยีสารสนเทศมีความสะดวก รวดเร็ว และเอื้ออำนวยต่อการทำธุรกรรมในรูปแบบของธุรกรรมทางอิเล็กทรอนิกส์มากขึ้น กรมสรรพากรจึงได้พัฒนาระบบงานและบริการ เพื่ออำนวยความสะดวกแก่ผู้เสียภาษีอย่างต่อเนื่อง และเพื่อให้การให้บริการเป็นไปอย่างมีประสิทธิภาพ กรมสรรพากรได้มีการเชื่อมโยงข้อมูลจากหน่วยงานที่เกี่ยวข้องทั้ง ข้อมูลจากหน่วยงานภายในและข้อมูลจากหน่วยงานภายนอก เพื่อนำมาพัฒนานวัตกรรมบริการและส่งมอบบริการได้อย่างสะดวก รวดเร็ว ครบวงจร และเป็นประโยชน์ต่อผู้เสียภาษี

ในขั้นตอนการรับ-ส่งข้อมูลจากหน่วยงานภายนอก หรือระบบงานของกรมสรรพากรที่มีการให้บริการข้อมูล รายงาน หรือเอกสารหลักฐานต่าง ๆ แก่ผู้เสียภาษี เพื่อให้การลงลายมือชื่ออิเล็กทรอนิกส์ของระบบงานที่เชื่อมโยงกับกรมสรรพากร และระบบงานของกรมสรรพากร มีการดำเนินการอย่างมีมาตรฐาน กรมสรรพากรจึงได้จัดทำมาตรฐานการลงลายมือชื่ออิเล็กทรอนิกส์ ฉบับนี้ขึ้น เพื่อให้ระบบงานที่ต้องใช้มาตรฐานการลงลายมือชื่ออิเล็กทรอนิกส์ มีมาตรฐานที่สามารถอ้างอิงเกี่ยวกับการลงลายมือชื่ออิเล็กทรอนิกส์ เพื่อให้สามารถพิจารณาเลือกใช้ได้อย่างเหมาะสมกับบริการต่าง ๆ

ประกอบกับ กฎกระทรวงฉบับที่ 384 (พ.ศ. 2565) ตามความในประมวลรัษฎากรว่าด้วยการดำเนินการเกี่ยวกับเอกสารอิเล็กทรอนิกส์ หลักฐานหรือหนังสือด้วยกระบวนการทางอิเล็กทรอนิกส์ และประกาศอธิบดีกรมสรรพากร (ฉบับที่ 48) เรื่อง กำหนดมาตรฐานเกี่ยวกับรูปแบบ วิธีการส่ง การเก็บรักษาเอกสารหลักฐานหรือหนังสือ และความมั่นคงปลอดภัยด้านสารสนเทศ สำหรับการดำเนินการที่เกี่ยวข้องกับกระบวนการทางอิเล็กทรอนิกส์ กำหนดให้ต้องมีการการลงลายมือชื่อ จึงจำเป็นต้องมีมาตรฐานการลงลายมือชื่ออิเล็กทรอนิกส์ฉบับนี้ ซึ่งจะครอบคลุมเนื้อหาเกี่ยวกับภาพรวมของลายมือชื่ออิเล็กทรอนิกส์ ประเภทและองค์ประกอบของลายมือชื่ออิเล็กทรอนิกส์ การเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์ และมาตรฐานการลงลายมือชื่อดิจิทัลตามประเภทเอกสารอิเล็กทรอนิกส์ อย่างไรก็ตามหากมีข้อกำหนดเกี่ยวกับการลงลายมือชื่ออิเล็กทรอนิกส์ ตามกฎหมายอื่นที่กำหนดไว้เป็นการเฉพาะ ระบบงานต่าง ๆ ควรมีการศึกษาข้อกฎหมายอื่น ๆ ที่เกี่ยวข้องประกอบด้วย

ประวัติการปรับปรุงเอกสาร

Version	รายละเอียด	วันที่
01.00.0000	เวอร์ชันแรก	23 สิงหาคม 2566

สารบัญ

เรื่อง **หน้าที่**

สารบัญตาราง

หน้าที่

สารบัญภาพ

หน้าที่

1. ขอบข่าย

มาตรฐานการลงลายมือชื่ออิเล็กทรอนิกส์ฉบับนี้ อธิบายภาพรวมของลายมือชื่ออิเล็กทรอนิกส์ ประเภทและองค์ประกอบของลายมือชื่ออิเล็กทรอนิกส์ การเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์ และมาตรฐานการลงลายมือชื่อดิจิทัลตามประเภทเอกสารอิเล็กทรอนิกส์ โดยเนื้อหาของมาตรฐานการลงลายมือชื่ออิเล็กทรอนิกส์ฉบับนี้จะครอบคลุมภาพรวมของลายมือชื่ออิเล็กทรอนิกส์ ประเภทและองค์ประกอบของลายมือชื่ออิเล็กทรอนิกส์ การเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์ และมาตรฐานการลงลายมือชื่อดิจิทัลตามประเภทเอกสารอิเล็กทรอนิกส์

อย่างไรก็ตามหากมีข้อกำหนดเกี่ยวกับการลงลายมือชื่ออิเล็กทรอนิกส์ ตามกฎหมายอื่นที่กำหนดไว้เป็นการเฉพาะ ระบบงานต่าง ๆ ควรมีการศึกษาข้อกฎหมายอื่น ๆ ที่เกี่ยวข้องประกอบด้วย

2. นิยาม

2.1 เอกสารอิเล็กทรอนิกส์ (Electronic Document) หมายถึง เอกสารในรูปแบบอิเล็กทรอนิกส์ที่ได้สร้าง ส่ง รับ เก็บรักษา หรือ ประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์

2.2 ลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature หรือ E-Signature) หมายถึง อักษร อักขระ ตัวเลข เสียง หรือสัญลักษณ์อื่นใดที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์ซึ่งนำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้นและเพื่อแสดงว่าบุคคลดังกล่าวยอมรับข้อความในข้อมูลอิเล็กทรอนิกส์นั้น

2.3 ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ หมายถึง ลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะตามที่กำหนดในมาตรา 26 แห่งกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

2.4 ลายมือชื่อดิจิทัล (Digital signature) หมายถึง ลายมือชื่ออิเล็กทรอนิกส์ที่ได้จากกระบวนการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ ซึ่งช่วยให้สามารถยืนยันตัวเจ้าของลายมือชื่อและตรวจพบการเปลี่ยนแปลงของข้อความและลายมือชื่ออิเล็กทรอนิกส์ได้ รวมถึงการทำให้เจ้าของลายมือชื่อไม่สามารถปฏิเสธความรับผิดจากข้อความที่ตนเองลงลายมือชื่อได้

2.5 เจ้าของลายมือชื่อ หมายถึง ผู้ซึ่งถือข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์และสร้างลายมือชื่ออิเล็กทรอนิกส์นั้นในนามตนเองหรือแทนบุคคลอื่น

2.6 โครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure: PKI) หมายถึง โครงสร้างพื้นฐานที่รับรองกุญแจสาธารณะ (Public Key) ว่าเป็นของบุคคลหน่วยงาน หรืออุปกรณ์ที่กล่าวอ้างถึงจริง ด้วยการออกใบรับรอง X.509 Certificate รวมถึงจัดเก็บ เผยแพร่ และเพิกถอนกุญแจสาธารณะ (Public Key) ที่รับรอง

2.7 กุญแจส่วนตัว (Private Key) หมายถึง กุญแจที่ใช้ในการลงลายมือชื่ออิเล็กทรอนิกส์โดยใช้เทคโนโลยี PKI ระบบรหัสแบบอสมมาตรและเป็นกุญแจที่ใช้ในการถอดรหัสลับข้อมูล (Decryption)

2.8 กุญแจสาธารณะ (Public Key) หมายถึง กุญแจที่ใช้ในการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์โดยใช้เทคโนโลยี PKI ระบบรหัสแบบอสมมาตรและเป็นกุญแจที่ใช้ในการเข้ารหัสลับข้อมูล (Encryption)

2.9 ใบรับรอง (Certificate) หมายถึง ข้อมูลอิเล็กทรอนิกส์หรือการบันทึกอื่นใด ซึ่งยืนยันความเชื่อมโยงระหว่างเจ้าของลายมือชื่อกับข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์

2.10 ใบรับรอง X.509 Certificate หมายถึง ใบรับรองตามมาตรฐาน X.509 ที่ใช้ในการรับรองกุญแจสาธารณะ (Public Key) ว่าเป็นของบุคคล หน่วยงาน หรืออุปกรณ์ใด ซึ่งกำหนดโดย International Telecommunication Union (ITU)

2.11 ผู้ให้บริการออกใบรับรอง (Certification Authority: CA) หมายถึง บุคคล หน่วยงาน หรือเครื่องให้บริการ (Server) ที่ให้บริการรับรองกุญแจสาธารณะให้กับผู้ใช้บริการโดยการออกใบรับรองให้กับผู้ใช้บริการ และยังมีหน้าที่บริหารจัดการใบรับรองของผู้ใช้บริการ เช่น เผยแพร่ใบรับรอง เพิกถอนใบรับรอง และเผยแพร่ข้อมูลสำหรับตรวจสอบสถานะใบรับรอง

2.12 Cryptographic Message Syntax (CMS) หมายถึง ไวยกรณ์ หรือโครงสร้างของข้อมูลสำหรับเก็บลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature) ที่สร้างด้วยเทคโนโลยี PKI และข้อมูลที่ถูกเข้ารหัสลับ (Encryption) เพื่อรักษาความมั่นคงปลอดภัยให้กับข้อมูล

2.13 อัลกอริทึมสำหรับเข้ารหัสลับด้วยกุญแจแบบอสมมาตร (Asymmetric Key Algorithm) หมายถึง กระบวนการทางคณิตศาสตร์ที่ใช้ในการสร้างกุญแจส่วนตัว (Private Key) และกุญแจสาธารณะ (Public Key) รวมถึงการนำกุญแจดังกล่าวไปใช้ในการลงลายมือชื่ออิเล็กทรอนิกส์และเข้ารหัสลับ

3. ภาพรวมของลายมือชื่ออิเล็กทรอนิกส์

เมื่อบุคคลต้องการแสดงเจตนาที่จะเชื่อมโยงตนเองเข้ากับข้อความเพื่อให้เกิดผลผูกพัน เช่น ยอมรับเงื่อนไขตามข้อความที่ปรากฏในข้อตกลง หรือรับรองความถูกต้องของข้อความที่ตนเองให้ไว้ บุคคลดังกล่าวสามารถกระทำได้โดยการลงลายมือชื่อบนเอกสารกระดาษซึ่งเป็นวิธีการทั่วไปที่ปฏิบัติอยู่ในปัจจุบัน หรือการลงลายมือชื่ออิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ก็ได้ สิ่งสำคัญของการลงลายมือชื่อ คือ การทำให้เกิดหลักฐานที่สามารถระบุตัวเจ้าของลายมือชื่อ และสามารถแสดงเจตนาของเจ้าของลายมือชื่อเกี่ยวกับข้อความที่ตนเองลงลายมือชื่อได้ ทั้งนี้ บุคคลจะมีวัตถุประสงค์หรือเหตุผลของการลงลายมือชื่อที่แตกต่างกันตามการทำธุรกรรมแต่ละประเภท เช่น

– การอนุมัติ เห็นชอบ หรือยอมรับข้อความ เช่น การลงลายมือชื่อเพื่อยอมรับข้อกำหนดที่ปรากฏในสัญญา

– การรับรองหรือยืนยันความถูกต้องของข้อความ เช่น การลงลายมือชื่อเพื่อรับรองว่าข้อความในแบบแสดงรายการภาษีเงินได้เป็นรายการที่ถูกต้องสมบูรณ์และเป็นความจริง

– การตอบแจ้งการเข้าถึงหรือการรับข้อความ (Acknowledgement) เช่น การลงลายมือชื่อเพื่อตอบแจ้งการรับเอกสาร

– การเป็นพยานให้กับการลงลายมือชื่อหรือการทำธุรกรรมของบุคคลอื่น เช่น การลงลายมือชื่อเพื่อรับรองเอกสารหรือรับรองลายมือชื่อ (Notarization)

3.1 ลายมือชื่ออิเล็กทรอนิกส์

กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์รองรับการลงลายมือชื่ออิเล็กทรอนิกส์ให้มีผลทางกฎหมายเช่นเดียวกับการลงลายมือชื่อบนเอกสารกระดาษ กฎหมายดังกล่าวไม่ได้กำหนดเทคโนโลยีที่ใช้ในการลงลายมือชื่ออย่างเฉพาะเจาะจง ลายมือชื่ออิเล็กทรอนิกส์จึงมีความเป็นกลางทางเทคโนโลยี (Technology neutrality) และสามารถสร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์ใด ๆ ก็ได้ หากลายมือชื่ออิเล็กทรอนิกส์นั้นมีคุณสมบัติเป็นไปตามที่กฎหมายกำหนด

ตัวอย่างของรูปแบบของลายมือชื่ออิเล็กทรอนิกส์มีดังนี้

– การพิมพ์ชื่อไว้ท้ายเนื้อหาของอีเมล
– การสแกนภาพของลายมือชื่อที่เขียนด้วยมือและแนบไปกับเอกสารอิเล็กทรอนิกส์
– การใช้สไตลัส (Stylus) เขียนลายมือชื่อด้วยมือลงบนหน้าจอและบันทึกไว้ในรูปแบบอิเล็กทรอนิกส์
– การคลิกปุ่มแสดงการยอมรับหรือตกลง
– การทำเครื่องหมายในช่องแสดงการยอมรับ
– การใช้ลายมือชื่อดิจิทัล

ทั้งนี้ รูปแบบของลายมือชื่ออิเล็กทรอนิกส์ข้างต้นสามารถนำมาใช้ประกอบในกระบวนการลงลายมือชื่ออิเล็กทรอนิกส์ในระบบงานอัตโนมัติ (Automated workflow system) ซึ่งจะมีการควบคุมการเข้าถึงการยืนยันตัวตน และการตรวจสอบสิทธิของผู้ใช้งาน ก่อนอนุญาตให้ผู้ใช้งานดำเนินการลงลายมือชื่ออิเล็กทรอนิกส์

ตัวอย่างของระบบงานอัตโนมัติ เช่น ระบบอีเมลที่มีการยืนยันความถูกต้องของผู้ส่งอีเมลและการส่งอีเมลระบบอนุมัติเอกสารภายในหน่วยงานที่มีการเก็บรักษาบันทึกธุรกรรม (Transaction record) ไว้ในระบบการจัดการเอกสารที่เหมาะสม

3.2 ลายมือชื่อดิจิทัล

ลายมือชื่อดิจิทัลเป็นรูปแบบหนึ่งของลายมือชื่ออิเล็กทรอนิกส์ และสามารถถือเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้หากมีลักษณะตามที่กำหนดในมาตรา 26 แห่งกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

ลายมือชื่อดิจิทัลเป็นลายมือชื่ออิเล็กทรอนิกส์ที่ได้จากกระบวนการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์หรือแฮชของข้อมูลอิเล็กทรอนิกส์ด้วยกุญแจส่วนตัว (Private key) ในระบบรหัสแบบอสมมาตร (Asymmetric cryptography) ซึ่งมีคุณสมบัติด้านความมั่นคงปลอดภัยในการช่วยให้สามารถยืนยันตัวเจ้าของลายมือชื่อ (Authentication) และตรวจพบการเปลี่ยนแปลงของข้อความและลายมือชื่ออิเล็กทรอนิกส์ได้ (Data integrity) รวมถึงการทำให้เจ้าของลายมือชื่อไม่สามารถปฏิเสธความรับผิดจากข้อความที่ตนเองลงลายมือชื่อได้ (Non-repudiation) ตัวอย่างของลายมือชื่อดิจิทัล เช่น ลายมือชื่อดิจิทัลแบบ XML Advanced Electronic Signatures (XAdES) ตามมาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยแนวปฏิบัติการลงลายมือชื่ออิเล็กทรอนิกส์สำหรับเจ้าหน้าที่ของรัฐ มสพร. (7-2565) ลงวันที่ 1 ตุลาคม พ.ศ. 2565 ซึ่งใช้ในการลงลายมือชื่ออิเล็กทรอนิกส์สำหรับไฟล์ XML ตามข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการลงลายมือชื่ออิเล็กทรอนิกส์ (ขมธอ. 23-2563) ลงวันที่ 29 พฤษภาคม พ.ศ. 2563

หากกฎหมายไม่ได้กำหนดให้ธุรกรรมต้องมีการลงลายมือชื่อ ผู้ใช้งานอาจพิจารณาความจำเป็นของลายมือชื่ออิเล็กทรอนิกส์จาก

(1) ความต้องการในการเน้นความสำคัญของธุรกรรม เพื่อให้ผู้ที่เกี่ยวข้องตระหนักถึงความสำคัญของธุรกรรม เช่น การลงลายมือชื่อที่ช่วยให้ผู้กรอกข้อมูลตระหนักถึงความสำคัญของข้อมูลที่นำส่งและผลที่จะเกิดขึ้นหากกรอกข้อมูลเท็จ หรือ

(2) ความต้องการในการสร้างหลักฐานที่ชัดเจนในการแสดงเจตนาของเจ้าของลายมือชื่อ (เช่น การอนุมัติ การยอมรับ การตอบแจ้ง การรับทราบ การเป็นพยาน) ซึ่งจะช่วยลดความกังวลเกี่ยวกับปัญหาการปฏิเสธในภายหลัง เช่น การปฏิเสธว่าไม่รับทราบเงื่อนไขการใช้งาน การปฏิเสธว่าไม่ได้ตกลงกันไว้

4. ประเภทของลายมือชื่ออิเล็กทรอนิกส์

4.1 ประเภทที่ 1 ลายมือชื่ออิเล็กทรอนิกส์ทั่วไป

ลายมือชื่ออิเล็กทรอนิกส์ทั่วไป เป็นลายมือชื่ออิเล็กทรอนิกส์ในรูปแบบใด ๆ (กล่าวคือ เป็นอักษร อักขระ ตัวเลข เสียงหรือสัญลักษณ์อื่นใดที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์) ที่มีลักษณะตามที่กำหนดในมาตรา 9 แห่งกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

ตัวอย่างของรูปแบบของลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ 1 เช่น การพิมพ์ชื่อไว้ท้ายเนื้อหาของอีเมล การสแกนภาพของลายมือชื่อที่เขียนด้วยมือและแนบไปกับเอกสารอิเล็กทรอนิกส์ การใช้สไตลัส (Stylus) เขียนลายมือชื่อด้วยมือลงบนหน้าจอและบันทึกไว้ในรูปแบบอิเล็กทรอนิกส์ การคลิกปุ่มแสดง การยอมรับหรือตกลง การทำเครื่องหมายในช่องแสดงการยอมรับ ทั้งนี้ รวมถึงการใช้ระบบงานอัตโนมัติ (Automated workflow system) ที่มีการยืนยันตัวผู้ใช้งานมาประกอบกับรูปแบบของลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ 1 ข้างต้นด้วย

4.2 ประเภทที่ 2 ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้

ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ เป็นลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะตามที่กำหนดในมาตรา 26 แห่งกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ตัวอย่างของรูปแบบของลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ 2 เช่น ลายมือชื่อดิจิทัลที่อาศัยโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure: PKI)

4.3 ประเภทที่ 3 ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ซึ่งใช้ใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรอง

ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ซึ่งใช้ใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรอง เป็นลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะตามที่กำหนดในมาตรา 26 และอาศัยใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรองเพื่อสนับสนุนลายมือชื่ออิเล็กทรอนิกส์ตามที่กำหนดในมาตรา 28 แห่งกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

ตัวอย่างของรูปแบบของลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ 3 เช่น ลายมือชื่อดิจิทัลที่อาศัยโครงสร้างพื้นฐานกุญแจสาธารณะและใช้ใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรอง

5. องค์ประกอบของลายมือชื่ออิเล็กทรอนิกส์

5.1 องค์ประกอบที่ 1: การพิสูจน์และยืนยันตัวตน

ลายมือชื่ออิเล็กทรอนิกส์นำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยสามารถระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่อที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้น ดังนั้น ความน่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์จะเชื่อมโยงกันกับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนของบุคคล กล่าวคือ ความน่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์ส่วนหนึ่งจะพิจารณาจากระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตน ซึ่งประกอบด้วย ระดับความน่าเชื่อถือของไอเดนทิตี (IAL) ในกระบวนการพิสูจน์ตัวตน และระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (AAL) ในกระบวนการยืนยันตัวตน

ทั้งนี้ ลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ 2 และ 3 จะต้องอาศัยการยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) ตามข้อกำหนดของการยืนยันตัวตนที่ระดับ AAL2 ขึ้นไป และจะต้องมีสิ่งที่ใช้ยืนยันตัวตนปัจจัยหนึ่งเป็นกุญแจเข้ารหัส (cryptographic key) (ซึ่งได้แก่ ซอฟต์แวร์เข้ารหัสลับ (cryptographic software) หรืออุปกรณ์เข้ารหัสลับ (cryptographic device)) เนื่องจากกุญแจเข้ารหัสดังกล่าวจะเป็นข้อมูลสำหรับใช้สร้างลายมือชื่อดิจิทัล

5.2 องค์ประกอบที่ 2: เจตนาในการลงลายมือชื่อ

ลายมือชื่ออิเล็กทรอนิกส์ต้องสามารถแสดงเจตนาของเจ้าของลายมือชื่อเกี่ยวกับข้อความที่ตนเองลงลายมือชื่อได้ วิธีการลงลายมือชื่อต้องมีกระบวนการหรือหลักฐานที่แสดงได้ว่าบุคคลได้ยอมรับการแสดงเจตนาที่ตนได้ลงลายมือชื่ออย่างชัดเจน หรือใช้ลายมือชื่อดิจิทัลในการลงลายมือชื่อต่อข้อความที่ตนแสดงเจตนา

นอกจากนี้ วิธีการลงลายมือชื่อควรมีการออกแบบให้บุคคลเข้าใจอย่างชัดเจนว่ากำลังลงลายมือชื่อกับข้อมูลอิเล็กทรอนิกส์ และมีการบ่งบอกวัตถุประสงค์หรือเหตุผลของการลงลายมือชื่อในรูปแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ว่า ลายมือชื่อนำมาใช้เพื่อวัตถุประสงค์ใด เช่น อนุมัติ ยอมรับ รับรองหรือยืนยันความถูกต้อง ตอบแจ้งการรับข้อความ เป็นพยาน หรือเพื่อวัตถุประสงค์อื่น ๆ รวมทั้งใช้ภาษาที่อ่านง่ายและไม่เป็นการหลอกลวงหรือทำให้เข้าใจผิดในวัตถุประสงค์ดังกล่าว

5.3 องค์ประกอบที่ 3: การรักษาความครบถ้วนของข้อมูล

ข้อมูลที่ลงลายมือชื่ออิเล็กทรอนิกส์ และข้อมูลอื่น ๆ ที่เกี่ยวข้องจะต้องมีการเก็บรักษาข้อมูลให้มีความครบถ้วนและไม่มีการเปลี่ยนแปลงของข้อมูลตลอดระยะเวลาทั้งหมดของการเก็บรักษา ทั้งนี้ การรักษาความครบถ้วนของข้อมูลจะต้องมีหลักฐานแสดงได้ว่าไม่มีการเปลี่ยนแปลงความหมาย ของข้อความที่ลงลายมือชื่อหรือใช้บุคคลที่สามที่เชื่อถือได้เป็นเสมือนพยานในการรับรองความครบถ้วน ของข้อมูลด้วยการใช้ลายมือชื่อดิจิทัลของบุคคลดังกล่าว หรือใช้ลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อในการลงลายมือชื่อต่อข้อความ ซึ่งลายมือชื่อดิจิทัลมีคุณสมบัติด้านความมั่นคงปลอดภัยที่ช่วยให้สามารถตรวจพบการเปลี่ยนแปลงของข้อความและลายมือชื่ออิเล็กทรอนิกส์ได้

6. สรุปประเภทและองค์ประกอบของลายมือชื่ออิเล็กทรอนิกส์

ประเภทของลายมือชื่ออิเล็กทรอนิกส์ ตัวอย่างของรูปแบบของลายมือชื่ออิเล็กทรอนิกส์แต่ละประเภทและองค์ประกอบของลายมือชื่ออิเล็กทรอนิกส์ สามารถสรุปได้ตามตารางที่ 1

ตาราง 1 ประเภทและองค์ประกอบของลายมือชื่ออิเล็กทรอนิกส์

ประเภทของลายมือชื่ออิเล็กทรอนิกส์	ตัวอย่างของรูปแบบของลายมือชื่ออิเล็กทรอนิกส์	องค์ประกอบของลายมือชื่ออิเล็กทรอนิกส์		
		การพิสูจน์และยืนยันตัวตน	เจตนาในการลงลายมือชื่อ	การรักษาความครบถ้วนของข้อมูล
<u>ประเภทที่ 1</u> ลายมือชื่ออิเล็กทรอนิกส์ทั่วไป	– การพิมพ์ชื่อไว้ท้ายเนื้อหาของอีเมล – การสแกนภาพของลายมือชื่อที่เขียนด้วยมือและแนบไปกับเอกสาร – การใช้สไตลัส (stylus) เขียนลายมือชื่อด้วยมือลงบนหน้าจอและบันทึกไว้ – การใช้ระบบงานอัตโนมัติที่มีการยืนยันตัวผู้ใช้งานมาประกอบกับรูปแบบของลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ 1	มีการพิสูจน์และยืนยันตัวตนที่น่าเชื่อถือและเหมาะสมกับความเสี่ยงของธุรกรรม	มีกระบวนการหรือหลักฐานที่แสดงได้ว่าบุคคลได้ยอมรับการแสดงเจตนาที่ตนได้ลงลายมือชื่ออย่างชัดเจน	มีหลักฐานหรือใช้บุคคลที่สามที่เชื่อถือได้ เพื่อแสดงว่าไม่มีการเปลี่ยนแปลงความหมายของข้อความที่ลงลายมือชื่อ และรับรองความครบถ้วนของข้อมูล
<u>ประเภทที่ 2</u> ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้	– ลายมือชื่อดิจิทัลที่อาศัยโครงสร้างพื้นฐานกุญแจสาธารณะ (PKI)	– มีการพิสูจน์ตัวตนที่น่าเชื่อถือและเหมาะสมกับความเสี่ยงของธุรกรรม หรือมีการพิสูจน์ตัวตนที่ระดับ IAL2 ขึ้นไป	ใช้ลายมือชื่อดิจิทัลในการลงลายมือชื่อต่อข้อความที่ตนแสดงเจตนา	ใช้ลายมือชื่อดิจิทัลในการลงลายมือชื่อต่อข้อความ

ประเภทของลายมือชื่ออิเล็กทรอนิกส์	ตัวอย่างของรูปแบบของลายมือชื่ออิเล็กทรอนิกส์	องค์ประกอบของลายมือชื่ออิเล็กทรอนิกส์		
		การพิสูจน์และยืนยันตัวตน	เจตนาในการลงลายมือชื่อ	การรักษาความครบถ้วนของข้อมูล
		– มีการยืนยันตัวตนที่ระดับ AAL2 ขึ้นไป ซึ่งเป็นการยืนยันตัวตนแบบหลายปัจจัย และมีปัจจัยหนึ่งเป็นกุญแจเข้ารหัส		
<u>ประเภทที่ 3</u> **ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ซึ่งใช้ใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรอง**	– ลายมือชื่อดิจิทัลที่อาศัยโครงสร้างพื้นฐานกุญแจสาธารณะ (PKI) และใช้ใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรอง	– มีการพิสูจน์ตัวตนที่น่าเชื่อถือและเหมาะสมกับความเสี่ยงของธุรกรรมหรือมีการพิสูจน์ตัวตนที่ระดับ IAL2 ขึ้นไป – มีการยืนยันตัวตนที่ระดับ AAL2 ขึ้นไปซึ่งเป็นการยืนยันตัวตนแบบหลายปัจจัยและมีปัจจัยหนึ่งเป็นกุญแจเข้ารหัส	ใช้ลายมือชื่อดิจิทัลซึ่งใช้ใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรองในการลงลายมือชื่อต่อข้อความที่ตนแสดงเจตนา	ใช้ลายมือชื่อดิจิทัลซึ่งใช้ใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรองในการลงลายมือชื่อต่อข้อความ

7. การเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์

การเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์ที่มีความน่าเชื่อถือและความเหมาะสมกับวัตถุประสงค์ของการสร้างหรือส่งข้อมูลอิเล็กทรอนิกส์ จะช่วยจัดการความเสี่ยงหรือผลกระทบที่เป็นไปได้จากภัยคุกคามหรือเหตุการณ์ที่ลายมือชื่ออิเล็กทรอนิกส์จะไม่เป็นที่ยอมรับ ตัวอย่างเช่น

- การปลอมตัวเป็นผู้อื่น (Impersonation) เช่น ผู้ลงลายมือชื่อไม่ใช่เจ้าของลายมือชื่อ
- การปฏิเสธความรับผิด (Repudiation) เช่น ผู้ลงลายมือชื่อพยายามปฏิเสธว่าตนเองไม่ได้ลงลายมือชื่อ
- ข้อมูลไม่มีความครบถ้วน (Loss of data integrity) เช่น ข้อมูลมีการเปลี่ยนแปลงหลังจากที่ลงลายมือชื่อ
- การไม่มีอำนาจลงนาม (Exceeding authority) เช่น ผู้ลงลายมือชื่อไม่ได้รับอนุญาตให้ลงลายมือชื่อกับข้อมูลอิเล็กทรอนิกส์ที่เกี่ยวข้อง

ในการเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์แต่ละประเภท ผู้ใช้งานควรพิจารณาถึงปัจจัยเสี่ยงเพื่อจะนำไปวิเคราะห์ความเสี่ยงและวิธีการบรรเทาความเสี่ยงจากภัยคุกคามหรือเหตุการณ์ที่ลายมือชื่ออิเล็กทรอนิกส์จะไม่เป็นที่ยอมรับได้อย่างเหมาะสม ทั้งนี้ ผู้ใช้งานอาจพิจารณาปัจจัยเสี่ยงจากประเด็นด้านกฎหมาย ด้านการเงิน ด้านเทคนิคหรือประเด็นอื่น ๆ ที่เกี่ยวข้องกับการทำธุรกรรมนั้น โดยมีตัวอย่างของปัจจัยเสี่ยงในการเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์ ดังนี้

- กฎเกณฑ์เกี่ยวกับลายมือชื่อที่กำหนดไว้ในกฎหมาย
- การปฏิบัติตามประเพณีทางการค้าหรือทางปฏิบัติ
- ลักษณะ ประเภท หรือขนาดของธุรกรรมที่ทำ
- จำนวนครั้งหรือความสม่ำเสมอในการทำธุรกรรมระหว่างคู่กรณี
- ความสำคัญหรือมูลค่าของข้อความในข้อมูลอิเล็กทรอนิกส์
- ความมั่นคงและรัดกุมของอุปกรณ์ของคู่กรณีแต่ละฝ่ายและระบบการติดต่อสื่อสาร
- ระดับของการยอมรับหรือการไม่ยอมรับวิธีการที่ใช้ระบุตัวบุคคลในอุตสาหกรรมหรือสาขาที่เกี่ยวข้อง

อ้างอิงจากเอกสาร Security Guidelines On The Appropriate Use Of Qualified Electronic Signatures โดย European Union Agency For Network And Information Security (ENISA) ได้มีคำแนะนำการประเมินลักษณะของธุรกรรม โดยแบ่งตามระดับตามความวิกฤต (Criticality Levels) ได้แก่

(1) ระดับธรรมดา (Standard) หมายถึง ธุรกรรมทั่วไป กล่าวคือ การแลกเปลี่ยนหรือเข้าถึงข้อมูลอย่างจำกัดที่มีผลกระทบในระดับต่ำต่อองค์กร ซึ่งอาจรวมถึงการแลกเปลี่ยนข้อมูลภายในองค์กรที่อยู่ในลำดับชั้นข้อมูลที่ต่ำ เช่น ทั่วไป (Official) หรือเผยแพร่ได้ (Publish)

(2) ระดับขั้นสูง (Advanced) หมายถึง ธุรกรรมที่ต้องมีการพิจารณาอย่างรอบคอบถึงเงื่อนไขหรือข้อควรระวังเบื้องต้น อาจมีความเกี่ยวข้องกับความเสี่ยงทางด้านการเงินในระดับจำกัด หรืออาจมีการแลกเปลี่ยนข้อมูลในลำดับชั้นของข้อมูลที่สูงขึ้น เช่น ข้อมูลที่เป็นความลับ (Confidential) หรือใช้ภายใน (Internal Use)

(3) ระดับอ่อนไหว (Sensitive) หมายถึง ธุรกรรมที่เกี่ยวข้องกับข้อมูลที่มีความละเอียดอ่อนอาจมีความเสี่ยงทางด้านการเงินโดยตรง เช่น ธุรกรรมที่เกี่ยวข้องกับข้อมูลที่เป็นความลับขององค์กร (Secret หรือ Top Secret) รวมถึงธุรกรรมที่ก่อให้เกิดผลกระทบในวงกว้าง

ทั้งนี้ นอกเหนือจากการประเมินลักษณะของธุรกรรมจากด้านความเสี่ยงทางการเงินและลำดับชั้นของข้อมูล ENISA แนะนำให้พิจารณาถึงปัจจัยอื่น ซึ่งมีส่วนเกี่ยวข้องต่อการดำเนินงานขององค์กร โดยอาจมีปัจจัยเฉพาะสำหรับแต่ละธุรกิจ หรืออุตสาหกรรมที่ควรคำนึงถึงแตกต่างกันไป ซึ่งจากระดับของลักษณะธุรกรรมดังกล่าว นำมาประยุกต์ใช้เป็นแนวทางในการเลือกใช้ประเภทของลายมือชื่ออิเล็กทรอนิกส์ โดยสรุป ดังนี้

(1) ข้อเสนอแนะระดับทั่วไป (Basic) สำหรับธุรกรรมในระดับธรรมดา ควรเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์ที่ได้รับการยอมรับเทียบเท่ากับการลงลายมือชื่อบนกระดาษ โดยแนะนำให้ใช้ลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ 1

(2) ข้อเสนอแนะระดับแนะนำ (Recommended) สำหรับธุรกรรมขั้นสูง ควรเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์ที่มีคุณสมบัติเพิ่มเติมด้านการตรวจพบการเปลี่ยนแปลงของข้อมูล และการคงสภาพในระยะยาว เพื่อการตรวจสอบความถูกต้องของข้อมูลระยะยาว (Long-Term Validation) โดยแนะนำให้ใช้ลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ 2

(3) ข้อเสนอแนะในการยกระดับ (Enhanced) สำหรับธุรกรรมอ่อนไหว นอกเหนือจากการใช้ลายมือชื่ออิเล็กทรอนิกส์ที่ได้รับการยอมรับเทียบเท่าการลงลายมือชื่อบนกระดาษ และมีการตรวจสอบความถูกต้องของข้อมูลระยะยาว ควรเลือกใช้บริการที่ได้รับการรับรองคุณภาพ โดยแนะนำให้ใช้ลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ 3

ผู้ให้บริการออกใบรับรองสาธารณะในประเทศไทยควรอยู่ภายใต้การกำกับดูแลโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) โดยมีผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์แห่งชาติ (Thailand National Root Certification Authority: NRCA) เป็นผู้ให้บริการออกใบรับรองลำดับชั้นบนสุด (Root CA) ซึ่งรับรองผู้ให้บริการออกใบรับรองในลำดับชั้นถัดลงมา (Subordinate CA) สามารถศึกษารายละเอียดผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์แห่งชาติได้ที่ https://www.nrca.go.th/

อย่างไรก็ตาม ในกรณีของลายมือชื่ออิเล็กทรอนิกส์ที่มีผู้ลงลายมือชื่อหลายคนกับข้อมูลอิเล็กทรอนิกส์อันเดียวกัน (multiple signatures) เช่น การอนุมัติตามสายการบังคับบัญชา ลายมือชื่ออิเล็กทรอนิกส์ทั้งหมดควรใช้ลายมือชื่ออิเล็กทรอนิกส์ประเภทและรูปแบบเดียวกัน เพื่อช่วยให้การเก็บรักษาหลักฐานเกี่ยวกับการแสดงเจตนาการรักษาความครบถ้วน และข้อมูลที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์เป็นไปในทิศทางเดียวกัน

8. มาตรฐานการลงลายมือชื่อดิจิทัลตามประเภทเอกสารอิเล็กทรอนิกส์

ปัจจุบันเอกสารอิเล็กทรอนิกส์เข้ามามีบทบาทสำคัญและถูกใช้อย่างแพร่หลายในการค้าขายสินค้าระหว่างบริษัทและการทำธุรกรรมต่าง ๆ ระหว่างหน่วยงาน หรือแม้แต่ภายในหน่วยงานเอง เอกสารอิเล็กทรอนิกส์ก็มีส่วนสำคัญที่จะทำให้หน่วยงานเกิดการพัฒนาและทำงานไปได้อย่างราบรื่น อย่างไรก็ตาม สิ่งสำคัญที่ควรคำนึงถึงคือการมีกลไกในการดูแลรักษาความมั่นคงปลอดภัยของข้อมูลในเอกสารอิเล็กทรอนิกส์ที่เหมาะสม เพื่อผู้ใช้งานมีความเชื่อมั่นและเอกสารอิเล็กทรอนิกส์มีความน่าเชื่อถือ เทคนิคที่ใช้ในการรักษาความถูกต้องครบถ้วนของข้อมูล รวมถึงใช้ในการพิสูจน์ตัวตนของผู้ลงลายมือชื่อได้คือการใช้ลายมือชื่ออิเล็กทรอนิกส์

ลายมือชื่ออิเล็กทรอนิกส์แบบ Advanced Electronic Signature (AdES) แบ่งออกเป็น 4 แบบ ได้แก่

(1) XML Advanced Electronic Signatures (XAdES) ใช้ลงลายมือชื่ออิเล็กทรอนิกส์สำหรับไฟล์ XML

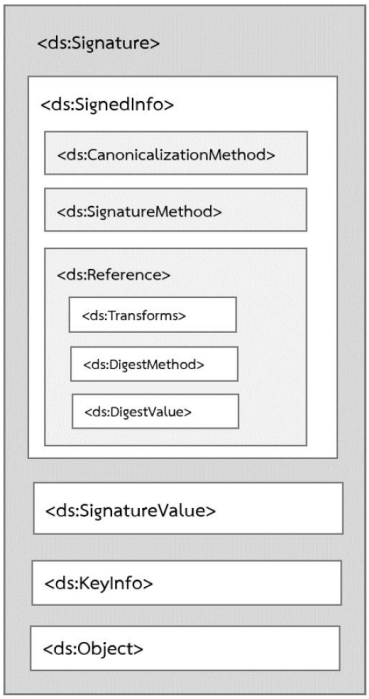
(2) PDF Advanced Electronic Signatures (PAdES) ใช้ลงลายมือชื่ออิเล็กทรอนิกส์สำหรับไฟล์ PDF

(3) JSON Advanced Electronic Signatures (JADES) ใช้ลงลายมือชื่ออิเล็กทรอนิกส์สำหรับรูปแบบ JSON

(4) CMS Advanced Electronic Signatures (CAdES) ใช้ลงลายมือชื่ออิเล็กทรอนิกส์สำหรับไฟล์ทุกแบบ

8.1 การลงลายมือชื่ออิเล็กทรอนิกส์สำหรับไฟล์ XML

มาตรฐานการลงลายมือชื่อดิจิทัล XML Advanced Electronic Signatures (XAdES) อ้างอิงตามข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ระหว่างหน่วยงาน (ขมธอ. 14-2560) ลงวันที่ 23 พฤษภาคม พ.ศ. 2560 โดยลงลายมือชื่อด้วยใบรับรองอิเล็กทรอนิกส์ของผู้นำส่งข้อมูล ที่ออกโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ตามข้อกำหนด W3C XML Advanced Electronic Signatures (XAdES) การสร้างเอกสารอิเล็กทรอนิกส์สำหรับแลกเปลี่ยนข้อมูลโดยใช้ข้อความ XML ซึ่งมีองค์ประกอบหลักต่อไปนี้



รูปที่ 1 โครงสร้างลายมือชื่ออิเล็กทรอนิกส์แบบ XMLDSIG

(1) Signed Info element ประกอบด้วยข้อมูล algorithms หรือขั้นตอนในการลงลายมือชื่ออิเล็กทรอนิกส์ในเอกสาร ประกอบด้วย

(1.1) Canonicalization Method หรือขั้นตอนการจัดโครงสร้างของ XML ก่อนทำการลงลายมือชื่อโดย W3C กำหนดให้ XML-C14N (http://www.w3.org/TR/2001/REC-xml-c14n-20010315) สำหรับ Canonical XML 1.0 และ XML-C14N11 สำหรับ Canonical XML 1.1 http://www.w3.org/2006/12/xmlc14n11)

(1.2) Signature Method หรือ Algorithms ที่ใช้ในการ สร้าง Digital Signature

(1.3) Reference หรือข้อมูลอื่น ๆ ที่ใช้ในการลงลายมือชื่ออิเล็กทรอนิกส์

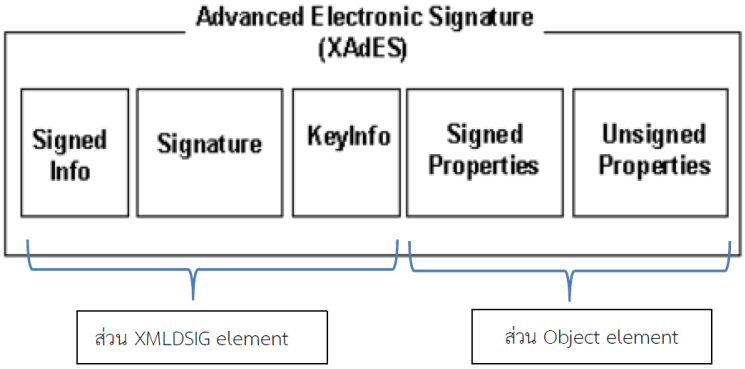
(ก) การ transform signature โดยข้อมูลใน transform element สามารถกำหนดได้ว่าจะให้ XMLDSIG อยู่ในรูปแบบ Enveloping (ลายมือชื่อจะครอบส่วนของเนื้อหาเอกสาร) หรือ Enveloped (ลายมือภายในเนื้อหาเอกสาร)

(ข) Digest Method เป็น algorithms ที่ใช้ในการทำ Digest Message (Hash value ของเนื้อหาเอกสาร) เอกสารฉบับนี้เสนอแนะให้ใช้ Digest Method ในกลุ่ม SHA-2 (เช่น SHA-256 SHA-512 เป็นต้น) และ SHA-3 (เช่น SHA3-256 SHA3-512 เป็นต้น)

(ค) Digest Value เป็น Digest Message หรือ ค่า Hash ของเอกสาร XML โดยค่า Hash ดังกล่าวจะอยู่ในรูปแบบ Base 64 (ตามข้อกำหนด W3C Recommendation on XML Signature Syntax and Processing)

(2) Signature Value เป็นค่าของลายมือชื่ออิเล็กทรอนิกส์ถูกเข้ารหัสในรูปแบบ Base 64

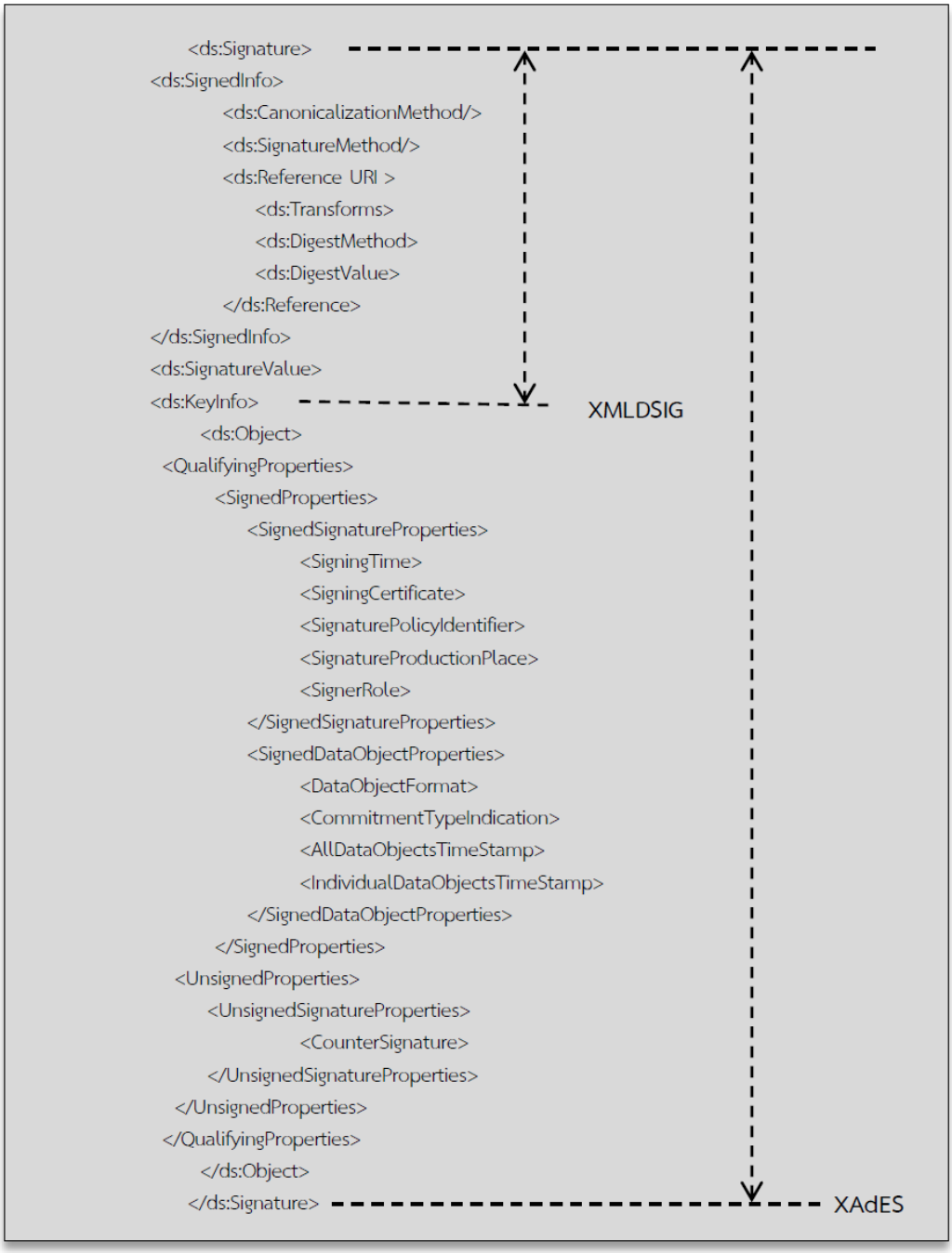
(3) Key Info มีข้อมูลใบรับรองอิเล็กทรอนิกส์ของผู้ลงลายมือชื่อ ประกอบด้วย X509SubjectName element ซึ่งระบุ Distinguished Name ของเจ้าของใบรับรองอิเล็กทรอนิกส์ และ X509Certificate ระบุ Certificate ถูกเข้ารหัสแบบ Base 64)



รูปที่ 2 โครงสร้างลายมือชื่ออิเล็กทรอนิกส์ XAdES

(4) Signed Properties เป็น element ภายใต้ Signature/Object/Qualifying Properties ประกอบด้วย element ต่าง ๆ ที่จะถูกลงลายมือชื่อในขั้นตอนการสร้างลายมือชื่อ element ที่อยู่ภายใต้ Signed Properties ตัวอย่างเช่น Signing Time Signing Certificate Signature Production Place และ Signature Policy

(5) Unsigned Properties เป็น element ภายใต้ Signature/Object/Qualifying Properties ประกอบด้วยelement ต่าง ๆ โดย จะไม่ถูกลงลายมือชื่อในขั้นตอนการสร้างลายมือชื่อ โดย element ภายใต้ Unsigned Properties จะถูกรวมเข้ามาภายหลังการลงลายมือชื่ออิเล็กทรอนิกส์ด้วย XMLDSIG แล้ว เช่น Signature Time Stamp ซึ่งเป็น Time-Stamp ที่ออกโดย TSA (Time Stamping Authority) เพื่อยืนยันเวลาที่ลายมือชื่ออิเล็กทรอนิกส์ถูกสร้างขึ้น ลายมือชื่ออิเล็กทรอนิกส์แบบ AdES แต่ละประเภท ได้แก่ Basic Signature, Signature with Time, Signatures With Long-term Validation Data, Signatures With Archival Data มีรายการข้อมูลเพิ่มเติมในลายมือชื่อต่างกันออก ทำให้มีคุณสมบัติแตกต่างกันออกไป และความซับซ้อนในการใช้งานมากขึ้นตามลำดับ ทั้งนี้ เอกสารฉบับนี้จะเสนอแนะลายมือชื่ออิเล็กทรอนิกส์แบบ Basic Signature, Signature with Time เท่านั้น



รูปที่ 3 แสดง Signed Properties และ Un Signed Properties ภายใต้ XAdES

8.2 การลงลายมือชื่ออิเล็กทรอนิกส์สำหรับไฟล์ PDF

มาตรฐานการลงลายมือชื่อดิจิทัล PDF Advanced Electronic Signatures (PAdES) และอ้างอิงขั้นตอนการการจัดทำหนังสือรับรองในรูปแบบไฟล์เอกสาร Portable Document Format (PDF) ตามข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ (ขมธอ. 11-2560) ลงวันที่ 20 มีนาคม พ.ศ. 2560 และอ้างอิงข้อเสนอแนะมาตรฐานฯ ว่าด้วยการใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ระหว่างหน่วยงาน เลขที่ ขมธอ. 14-2560 โดยลงลายมือชื่อด้วยใบรับรองอิเล็กทรอนิกส์ของผู้นำส่งข้อมูล

ที่ออกโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ตามข้อกำหนด ETSI TS 102 778-1 Electronic Signatures and Infrastructures (ESI) PDF Advanced Electronic Signature Profiles และ 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

แต่อย่างไรก็ตาม เพื่อให้ลายมือชื่ออิเล็กทรอนิกส์มีความเหมาะสมกับการใช้งานบนเอกสารในรูปแบบอิเล็กทรอนิกส์ มาตรฐานนี้จึงมีการกำหนดหลักเกณฑ์ในการลงลายมือชื่ออิเล็กทรอนิกส์เพิ่มเติม โดยมีรายละเอียดที่สำคัญดังต่อไปนี้

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

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

(3) แนบใบรับรองอิเล็กทรอนิกส์ตามมาตรฐาน X.509 ทุกใบที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์ใบรับรองอิเล็กทรอนิกส์ตามมาตรฐาน X.509 หรือใบรับรอง X.509 Certificate เป็นข้อมูลสำคัญที่ใช้ในการตรวจสอบความน่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์ เนื่องจากใบรับรอง X.509 Certificate เป็นสิ่งที่ใช้ในการตรวจสอบว่า ลายมือชื่ออิเล็กทรอนิกส์บนเอกสารในรูปแบบอิเล็กทรอนิกส์เป็นของหน่วยงานที่มีอำนาจรับรองหรือไม่ ด้วยการระบุชื่อผู้มีอำนาจลงนามและ/หรือหน่วยงานที่ออกเอกสารในรูปแบบอิเล็กทรอนิกส์ไว้ ด้วยเหตุนี้ในการลงลายมือชื่ออิเล็กทรอนิกส์ทุกครั้ง จึงควรมีการแนบใบรับรอง X.509 Certificate ทุกใบที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์ตามรูปแบบที่ ISO 32000-1 กำหนด ซึ่งประกอบด้วย

(3.1) ใบรับรอง X.509 Certificate ของหน่วยงานที่มีอำนาจออกเอกสารในรูปแบบอิเล็กทรอนิกส์

(3.2) ใบรับรอง X.509 Certificate ของผู้ให้บริการออกใบรับรอง (Certification Authority: CA) ซึ่งเป็นใบรับรอง X.509 Certificate ของบุคคลที่สามที่รับรองว่า ใบรับรอง X.509 Certificate ของหน่วยงานที่ออกเอกสารในรูปแบบอิเล็กทรอนิกส์มีตัวตนอยู่จริงลายมือชื่ออิเล็กทรอนิกส์ที่เกิดจากใบรับรอง X.509 Certificate มีผลผูกพันกับหน่วยงานที่ออกเอกสารดังกล่าว เพื่อให้สามารถตรวจสอบความน่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์ แม้ว่าจะเก็บรักษาไว้เป็นระยะเวลานาน และมีผลผูกพันทางกฎหมายกับหน่วยงานที่มีอำนาจออกเอกสาร

(4) แนบข้อมูลเพื่อใช้ในการตรวจสอบสถานะของใบรับรอง X.509 Certificate เพื่อให้สามารถตรวจสอบความน่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์บนเอกสารในรูปแบบอิเล็กทรอนิกส์ในภายหลังได้แม้จะเก็บไว้เป็นระยะเวลานาน จึงเสนอให้ทำการแนบข้อมูลที่ใช้ในการตรวจสอบสถานะของใบรับรอง X.509 Certificate ที่ใช้ในการลงลายมือชื่ออิเล็กทรอนิกส์ว่าถูกเพิกถอนหรือไม่ ตามรูปแบบที่ ISO 32000-1 กำหนด ซึ่งในการแนบข้อมูลดังกล่าวสามารถแนบข้อมูลได้ 2 รูปแบบ

(4.1) รายการเพิกถอนใบรับรอง (Certificate Revocation List: CRL)

(4.2) ข้อมูลสถานะของใบรับรองในรูปแบบ Online Certificate Status Protocol (OCSP) โดยในการแนบข้อมูลดังกล่าวข้างต้นในลายมือชื่ออิเล็กทรอนิกส์ จำเป็นต้องแนบข้อมูลสำหรับตรวจสอบสถานะของใบรับรอง X.509 Certificate ทุกใบที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์ นอกจากนี้ก่อนการแนบข้อมูลดังกล่าวในลายมือชื่ออิเล็กทรอนิกส์จำเป็นต้องใช้ข้อมูลดังกล่าวตรวจสอบสถานะของใบรับรอง X.509 Certificate ว่าถูกเพิกถอน ณ ขณะที่ลงลายมือชื่ออิเล็กทรอนิกส์หรือไม่

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

(6) กำหนดสถานะของเอกสารในรูปแบบอิเล็กทรอนิกส์ให้อยู่ในสถานะไม่สามารถแก้ไขได้ (Read Only) ภายหลังแนบข้อมูลที่จำเป็นในการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์เรียบร้อยแล้วจำเป็นต้องกำหนดให้เอกสารในรูปแบบอิเล็กทรอนิกส์อยู่ในสถานะที่ไม่สามารถแก้ไขได้ (Read Only) เพื่อป้องกันการเปลี่ยนแปลงแก้ไขโดยมิชอบอีกครั้ง

8.3 การลงลายมือชื่ออิเล็กทรอนิกส์สำหรับไฟล์สำหรับรูปแบบ JSON

JSON Advanced Electronic Signatures (JAdES) เป็นมาตรฐานการลงลายมือชื่อดิจิทัลสำหรับไฟล์ JSON โดยใช้เทคโนโลยี Public Key Infrastructure (PKI) เพื่อให้มั่นใจได้ว่าไฟล์นั้นมีความถูกต้องและไม่ถูกแก้ไขในระหว่างการส่งผ่านเครือข่าย โดยสามารถนำมาใช้งานกับข้อมูลแบบ JSON Web Signature (JWS) หรือ JSON Web Token (JWT) ได้ [5]

การลงลายมือชื่อดิจิทัลแบบ JAdES จะช่วยให้มั่นใจว่าไฟล์ JSON ที่ใช้งานนั้นมีความถูกต้องและไม่ถูกแก้ไขโดยไม่ได้รับอนุญาต โดยสามารถใช้เครื่องมือที่รองรับ JAdES เพื่อตรวจสอบการลงลายมือชื่อดิจิทัลได้

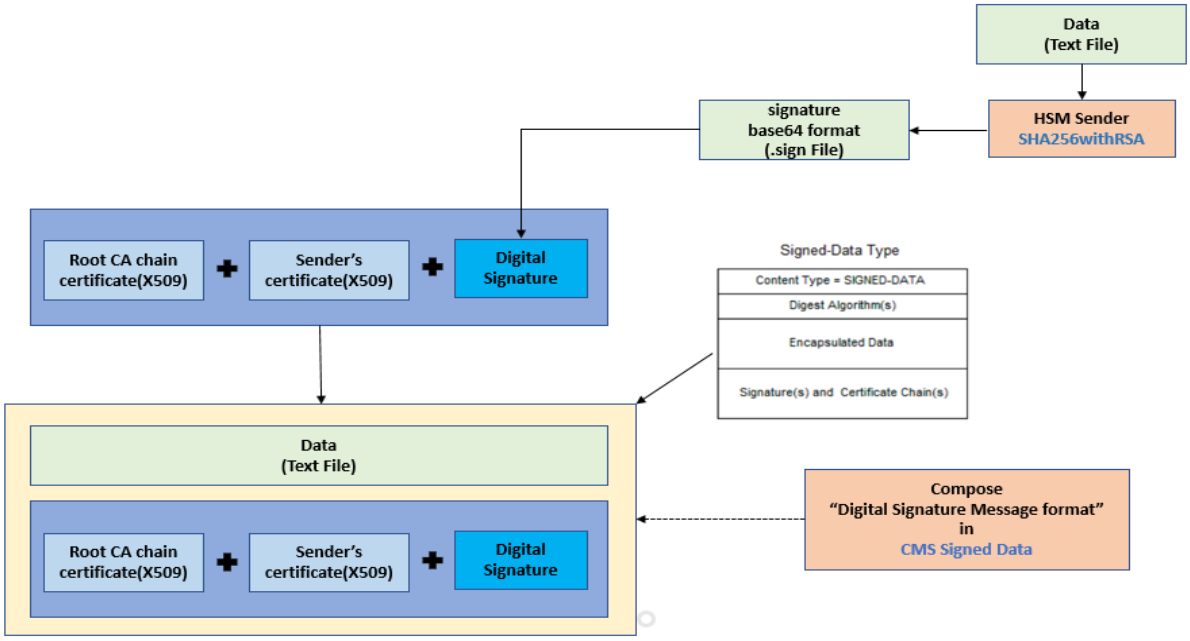
8.4 การลงลายมือชื่ออิเล็กทรอนิกส์สำหรับไฟล์ CMS

ใช้มาตรฐานการลงลายมือชื่อดิจิทัล CMS Advanced Electronic Signatures (CAdES) อ้างอิงจากข้อเสนอแนะมาตรฐานฯ ว่าด้วยการใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ระหว่างหน่วยงาน เลขที่ ขมธอ. 14-2560 โดยลงลายมือชื่อด้วยใบรับรองอิเล็กทรอนิกส์ของผู้นำส่งข้อมูล ที่ออกโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ตามข้อกำหนด RFC 5652 Cryptographic Message Syntax (CMS)

ตัวอย่างการลงลายมือชื่อดิจิทัลตามมาตรฐาน Cryptographic Message Syntax (CMS) สำหรับไฟล์ข้อมูล

1) นำไฟล์ข้อมูลเอกสารอิเล็กทรอนิกส์ (Data) ทำการลงลายมือชื่อดิจิทัล (Digital Signature) ด้วยอัลกอริทึมสำหรับเข้ารหัสลับข้อมูลด้วยกุญแจแบบอสมมาตร (Asymmetric Key Algorithm) SHA256withRSA โดยใช้กุญแจส่วนตัว (Private Key)

(2) นำไฟล์ข้อมูลที่ได้จากการลงลายมือชื่อดิจิทัลซึ่งจะอยู่ในรูปแบบ BASE64 (Digital Signature) รวมกับข้อมูลต้นฉบับ (Data) ใบรับรองของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Root CA Chain Certificate) และใบรับรองของผู้จัดทำข้อมูล (Sender's Certificate) โดยจัดรวม (Compose) ในรูปแบบ "Digital Signature Message Format" ในรูปแบบ CMS Signed Data ตามรูปที่ 4



รูปที่ 4 ตัวอย่างขั้นตอนการลงลายมือชื่อดิจิทัลสำหรับไฟล์ข้อมูล

บรรณานุกรม

[1] สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (2565) มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยแนวปฏิบัติการลงลายมือชื่ออิเล็กทรอนิกส์สำหรับเจ้าหน้าที่ของรัฐ มสพร. (7-2565) ลงวันที่ 1 ตุลาคม พ.ศ. 2565

[2] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (2563). ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการลงลายมือชื่ออิเล็กทรอนิกส์ (ขมธอ. 23-2563) ลงวันที่ 29 พฤษภาคม พ.ศ. 2563

[3] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (2560). ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ (ขมธอ. 11-2560) ลงวันที่ 20 มีนาคม พ.ศ. 2560

[4] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (2560). ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ระหว่างหน่วยงาน (ขมธอ. 14-2560) ลงวันที่ 23 พฤษภาคม พ.ศ. 2560

[5] ETSI TS 119 182-1 Electronic Signatures and Infrastructures (ESI); JAdES digital signatures https://www.etsi.org/deliver/etsi_ts/119100_119199/11918201/01.01.01_60/ts_11918201v010101p.pdf