สัมมนาเผยแพร่ความรู้และผลการศึกษา
ลายมือชื่อดิจิทัล ครั้งที่ 3

การใช้ลายมือชื่อดิจิทัล ให้มีความปลอดภัย

วันอังคาร ที่ 23 กรกฎาคม 2567 เวลา 14.00 - 16.00 น.

ณ อาคารจามจุรี 9 จุฬาลงกรณ์มหาวิทยาลัย และผ่านโปรแกรม Microsoft teams

หัวข้อการสัมมนา

- กฎหมายที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์
- ภาพรวมของลายมือชื่ออิเล็กทรอนิกส์
- กรอบแนวปฏิบัติการลงลายมือชื่อดิจิทัล
- กรอบแนวทางการพัฒนาและส่วนประกอบที่เกี่ยวข้องกับระบบลงลายมือชื่อดิจิทัล

หัวข้อการสัมมนา

- กฎหมายที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์
- ภาพรวมของลายมือชื่ออิเล็กทรอนิกส์
- กรอบแนวปฏิบัติการลงลายมือชื่อดิจิทัล
- กรอบแนวทางการพัฒนาและส่วนประกอบที่เกี่ยวข้องกับระบบลงลายมือชื่อดิจิทัล

กฎหมายไทย

พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

พระราชบัญญัตินี้ใช้บังคับแก่ธุรกรรมในทางแพ่งและพาณิชย์ที่ดำเนินการโดยใช้ข้อมูลอิเล็กทรอนิกส์ ซึ่งประกอบด้วยทั้งหมด 7 หมวด

กฎหมายไทย

พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

หมวด 1 ธุรกรรมอิเล็กทรอนิกส์

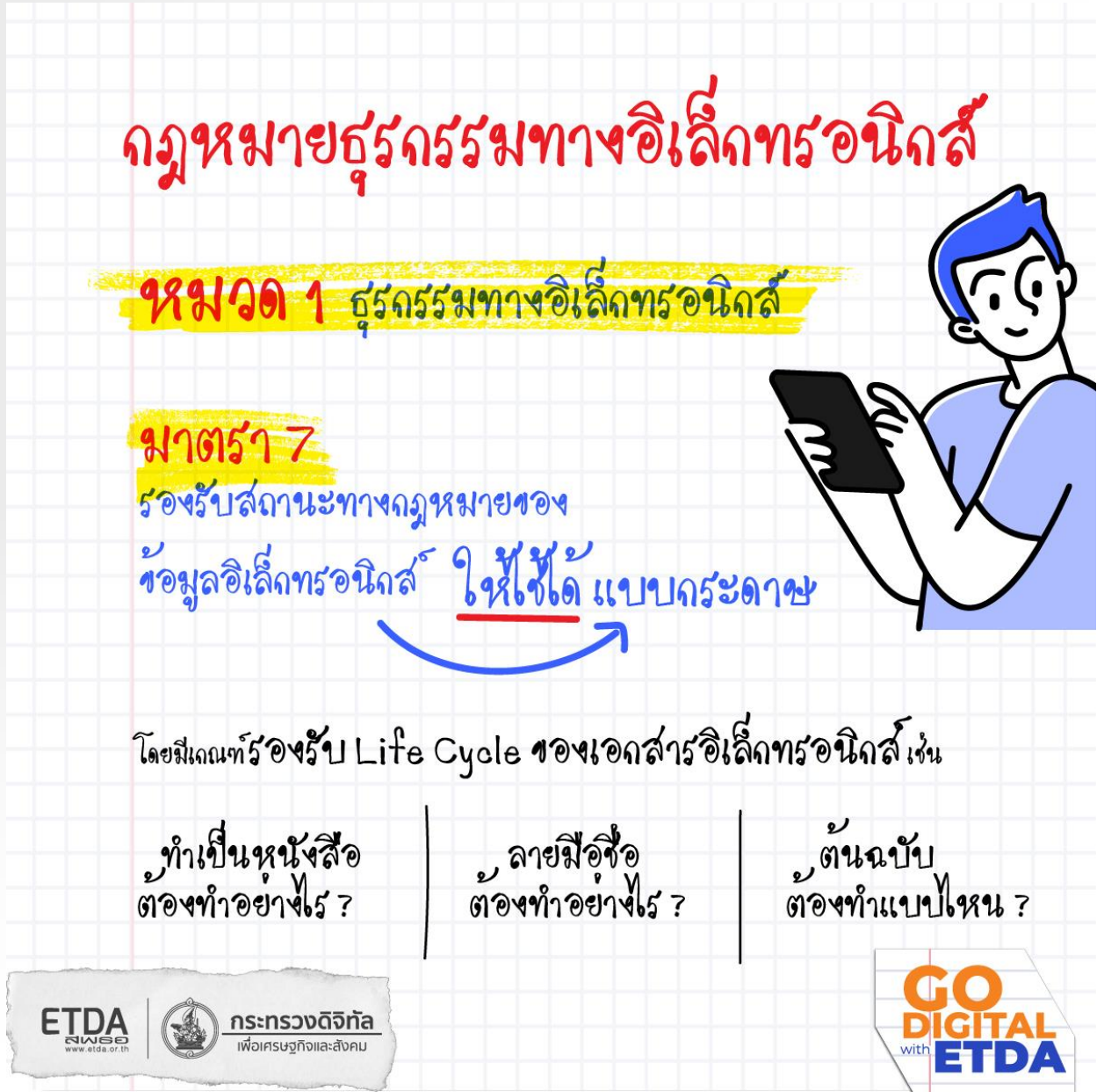
(มาตรา 7 - มาตรา 25)

กฎหมายไทย

พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

หมวด 1 ธุรกรรมอิเล็กทรอนิกส์

(มาตรา 7 - มาตรา 25)



กฎหมายไทย

พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

หมวด 1 ธุรกรรมอิเล็กทรอนิกส์

(มาตรา 7 - มาตรา 25)

กฎหมายไทย

พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

หมวด 1 ธุรกรรมอิเล็กทรอนิกส์

(มาตรา 7 - มาตรา 25)

มาตรา ๙[๑๑] ในกรณีที่กฎหมายกำหนดให้มีการลงลายมือชื่อ หรือกำหนดผลทางกฎหมาย กรณีที่ไม่มีการลงลายมือชื่อไว้ ให้ถือว่าได้มีการลงลายมือชื่อแล้ว ถ้า

(๑) ใช้วิธีการที่สามารถระบุตัวเจ้าของลายมือชื่อ และสามารถแสดงเจตนาของเจ้าของลายมือชื่อเกี่ยวกับข้อความในข้อมูลอิเล็กทรอนิกส์ และ

(๒) ใช้วิธีการในลักษณะอย่างใดอย่างหนึ่ง ดังต่อไปนี้

(ก) วิธีการที่เชื่อถือได้โดยเหมาะสมกับวัตถุประสงค์ของการสร้างหรือส่งข้อมูลอิเล็กทรอนิกส์ โดยคำนึงถึงพฤติการณ์แวดล้อมทั้งปวง รวมถึงข้อตกลงใด ๆ ที่เกี่ยวข้อง หรือ

(ข) วิธีการอื่นใดที่สามารถยืนยันตัวเจ้าของลายมือชื่อและสามารถแสดงเจตนาของเจ้าของลายมือชื่อ ตาม (๑) ได้ด้วยวิธีการนั้นเองหรือประกอบกับพยานหลักฐานอื่น

- การพิมพ์ชื่อไว้ท้ายเนื้อหาของอีเมล
- การใช้ระบบที่มีการยืนยันตัวตนผู้ใช้งาน
- การใช้ปากกาสไตลัสเขียนลายมือชื่อ
- การแปะภาพลายมือชื่อที่เขียนด้วยมือ

กฎหมายไทย

พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

หมวด 1 ธุรกรรมอิเล็กทรอนิกส์

(มาตรา 7 - มาตรา 25)

กฎหมายไทย

พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

หมวด 1 ธุรกรรมอิเล็กทรอนิกส์

(มาตรา 7 - มาตรา 25)

กฎหมายไทย

พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

หมวด 1 ธุรกรรมอิเล็กทรอนิกส์

(มาตรา 7 - มาตรา 25)

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเป็นมาตรการสำหรับใช้ในการควบคุมให้ระบบสารสนเทศมีความมั่นคงปลอดภัย ซึ่งครอบคลุมการรักษาความลับ (Confidentiality) การรักษาความครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้งาน (Availability) ของระบบสารสนเทศและสารสนเทศในระบบ นั้น โดยการทำธุรกรรมทางอิเล็กทรอนิกส์ด้วยระบบสารสนเทศ ต้องดำเนินการตามมาตรการที่เกี่ยวข้องตามบัญชีแนบท้ายนี้ และต้องพิจารณาให้สอดคล้องกับระดับความเสี่ยงที่ได้จากการประเมิน ทั้งนี้ มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ แบ่งออกเป็น ๑๑ ข้อ ได้แก่

๑. การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ
๒. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร
๓. การบริหารจัดการทรัพย์สินสารสนเทศ
๔. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร
๕. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม
๖. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ
๗. การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์
๘. การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ
๙. การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด
๑๐. การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง
๑๑. การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

กฎหมายไทย

พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

หมวด 2 ลายมือชื่ออิเล็กทรอนิกส์

(มาตรา 26 - มาตรา 31)

มาตรา ๒๖ ลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะดังต่อไปนี้ให้ถือว่าเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้

(๑) ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์นั้นได้เชื่อมโยงไปยังเจ้าของลายมือชื่อโดยไม่เชื่อมโยงไปยังบุคคลอื่นภายใต้สภาพที่นำมาใช้

(๒) ในขณะสร้างลายมือชื่ออิเล็กทรอนิกส์นั้น ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น

(๓) การเปลี่ยนแปลงใด ๆ ที่เกิดแก่ลายมือชื่ออิเล็กทรอนิกส์ นับแต่เวลาที่ได้สร้างขึ้นสามารถจะตรวจพบได้

(๔)[๑๙] ในกรณีที่กฎหมายกำหนดให้การลงลายมือชื่อเป็นไปเพื่อรับรองความครบถ้วนและไม่มีการเปลี่ยนแปลงของข้อความ การเปลี่ยนแปลงใดแก่ข้อความนั้นสามารถตรวจพบได้นับแต่เวลาที่ลงลายมือชื่ออิเล็กทรอนิกส์

- Uniquely Linked & Identification
- Sole Control
- Detectable Change

DIGITAL Signature

กฎหมายไทย

พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

หมวด 2 ลายมือชื่ออิเล็กทรอนิกส์

(มาตรา 26 - มาตรา 31)

มาตรา 26	ลักษณะของลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้
มาตรา 27	เจ้าของลายมือชื่อต้องดำเนินการอะไรบ้าง เพื่อให้ลายมือชื่ออิเล็กทรอนิกส์มีความน่าเชื่อถือ
มาตรา 28	ผู้ให้บริการออกใบรับรองต้องดำเนินการอะไรบ้าง เพื่อสนับสนุนลายมือชื่ออิเล็กทรอนิกส์ให้มีความน่าเชื่อถือ
มาตรา 29	ความเชื่อถือได้ของระบบ วิธีการ และบุคลากร ตามมาตรา 28 (6) ต้องคำนึงถึงสิ่งใดบ้าง
มาตรา 30	คู่กรณีที่เกี่ยวข้องต้องดำเนินการสิ่งใดบ้าง
มาตรา 31	ใบรับรองหรือลายมือชื่ออิเล็กทรอนิกส์ให้ถือว่ามีผลทางกฎมาย โดยไม่ต้องคำนึงถึงสถานที่ออกใบรับรอง และสถานที่ทำการของผู้ออกใบรับรอง

กฎหมาย eIDAS

(Electronic Identification, Authentication and Trust Services)

ข้อบังคับของสหภาพยุโรปเกี่ยวกับบริการระบุตัวตน
ทางอิเล็กทรอนิกส์และความน่าเชื่อถือ
สำหรับธุรกรรมทางอิเล็กทรอนิกส์

SIMPLE ELECTRONIC SIGNATURE ≈ พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ มาตรา 9

- ระบุตัวเจ้าของรายมือชื่อ
- แสดงเจตนาของเจ้าของรายมือชื่อ

ADVANCED ELECTRONIC SIGNATURE ≈ พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ มาตรา 26 (ถึง 31)

- Uniquely Linked & Identification
- Sole Control
- Detectable Change

QUALIFIED ELECTRONIC SIGNATURE ≈ **ADVANCED ELECTRONIC SIGNATURE**

- + Qualified Electronic Signature Creation Device
- + Qualified Certificate

QES shall have the equivalent legal effect of a handwritten signature.

หัวข้อการสัมมนา

- กฎหมายที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์
- ภาพรวมของลายมือชื่ออิเล็กทรอนิกส์
- กรอบแนวปฏิบัติการลงลายมือชื่อดิจิทัล
- กรอบแนวทางการพัฒนาและส่วนประกอบที่เกี่ยวข้องกับระบบลงลายมือชื่อดิจิทัล

e-Signature

ลายมือชื่ออิเล็กทรอนิกส์

ข้อเสนอแนะมาตรฐานฯ ว่าด้วยแนวทาง
การลงลายมือชื่ออิเล็กทรอนิกส์
เลขที่ ขมธอ. 23-2563

และ

มาตรฐานสำนักงานรัฐบาลดิจิทัล ว่าด้วยแนวปฏิบัติ
การลงลายมืออิเล็กทรอนิกส์สำหรับเจ้าหน้าที่
เลขที่ มพสร. 7/2565

3 องค์ประกอบสำคัญของลายมือชื่ออิเล็กทรอนิกส์ ได้แก่

- องค์ประกอบที่ 1 คือ การพิสูจน์และยืนยันตัวตน

ลายมือชื่ออิเล็กทรอนิกส์นำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์ เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยสามารถระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่อที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้นได้

- องค์ประกอบที่ 2 คือ เจตนาในการลงลายมือชื่อ

ลายมือชื่ออิเล็กทรอนิกส์ต้องสามารถแสดงเจตนาของเจ้าของลายมือชื่อเกี่ยวกับข้อความที่ตนเองลงลายมือชื่อได้ วิธีการลงลายมือชื่อต้องมีกระบวนการหรือหลักฐานที่แสดงได้ว่าบุคคลได้ยอมรับการแสดงเจตนาที่ตนได้ลงลายมือชื่ออย่างชัดเจน

- องค์ประกอบที่ 3 คือ การรักษาความครบถ้วนของข้อมูล

ข้อมูลที่ลงลายมือชื่อ ลายมือชื่ออิเล็กทรอนิกส์ และข้อมูลอื่น ๆ ที่เกี่ยวข้องจะต้องมีการเก็บรักษาข้อมูลให้มีความครบถ้วนและไม่มีการเปลี่ยนแปลงของข้อมูลตลอดระยะเวลาทั้งหมดของการเก็บรักษา

Digital Signature

ลายมือชื่อดิจิทัล

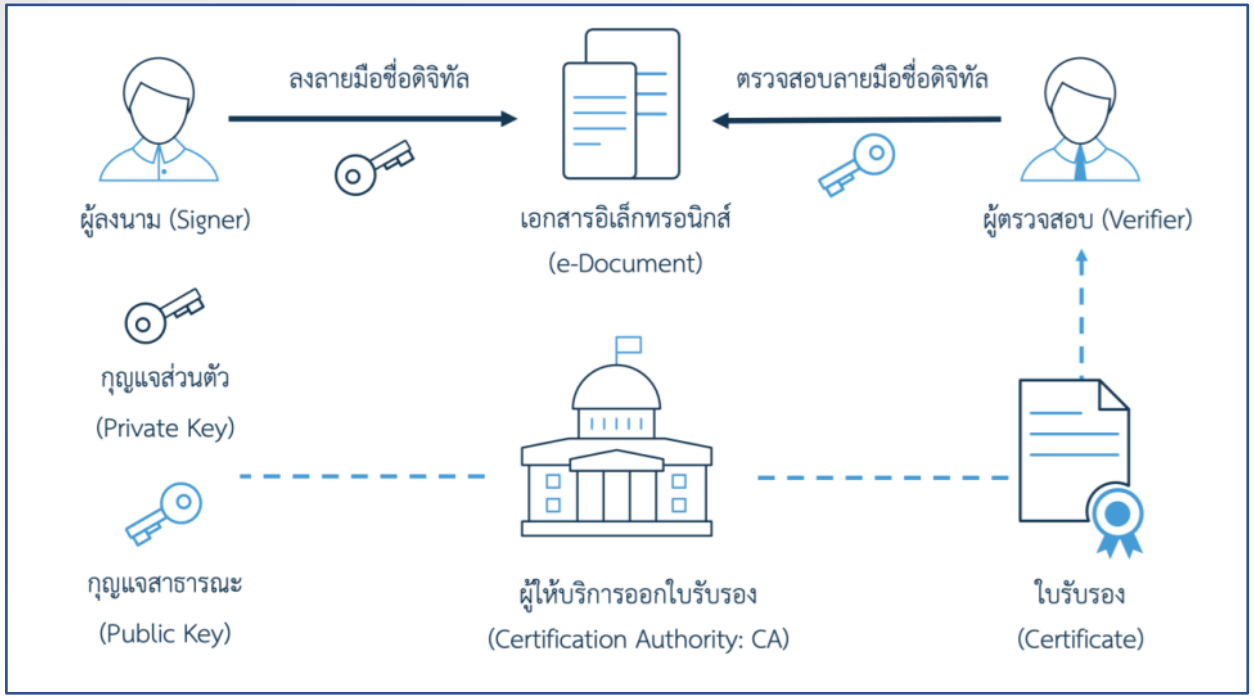
ข้อเสนอแนะมาตรฐานฯ ว่าด้วยแนวทาง
การลงลายมือชื่ออิเล็กทรอนิกส์
เลขที่ ขมธอ. 23-2563

และ

มาตรฐานสำนักงานรัฐบาลดิจิทัล ว่าด้วยแนวปฏิบัติ
การลงลายมืออิเล็กทรอนิกส์สำหรับเจ้าหน้าที่
เลขที่ มพสร. 7/2565

ลายมือชื่อดิจิทัล (digital signature)

ลายมือชื่อดิจิทัลเป็นลายมือชื่ออิเล็กทรอนิกส์ที่ได้จากกระบวนการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ด้วยกุญแจส่วนตัว (private key) ในระบบรหัสแบบอสมมาตร (asymmetric cryptography) ซึ่งมีคุณสมบัติด้านความมั่นคงปลอดภัยในการช่วยให้สามารถยืนยันตัวเจ้าของลายมือชื่อ (authentication) และตรวจพบการเปลี่ยนแปลงของข้อความและลายมือชื่ออิเล็กทรอนิกส์ได้ (data integrity) รวมถึงการทำให้เจ้าของลายมือชื่อไม่สามารถปฏิเสธความรับผิดจากข้อความที่ตนเองลงลายมือชื่อได้ (non-repudiation)



ETSI TR 119 100

Guidance on the use of standards for signature creation and validation

รูปแบบลายมือชื่อดิจิทัล (digital signature formats)

รูปแบบลายมือชื่อดิจิทัล (digital signature formats)

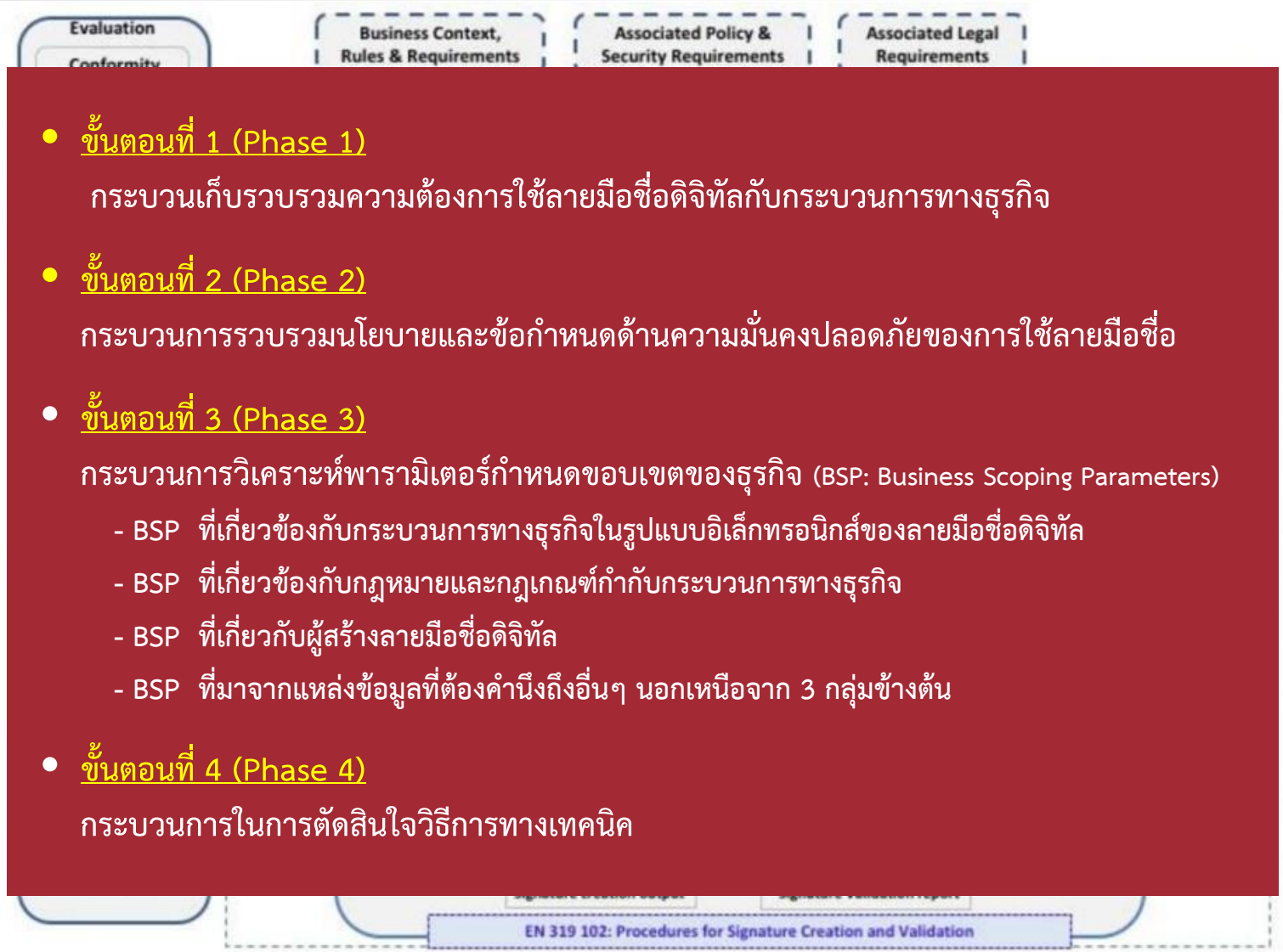
มาตรฐานลายมือชื่ออิเล็กทรอนิกส์ขั้นสูง (Advanced Electronic Signature: AdES) จากสถาบัน European Telecommunications Standards Institute (ETSI) อ้างอิงรายงานทางเทคนิค ETSI TR 119 100 Guidance on the use of standards for signature creation and validation มีมาตรฐานการกำหนดรูปแบบลายมือชื่อดิจิทัล (digital signature formats) ทั้งหมด 5 รูปแบบ ได้แก่

1. **CMS Advanced Electronic Signatures (CADES)**
   สำหรับเอกสารอิเล็กทรอนิกส์ในรูปแบบ Cryptographic Message Syntax (CMS)
   ETSI EN 319 122-1 CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures
2. **XML Advanced Electronic Signatures (XADES)**
   สำหรับเอกสารอิเล็กทรอนิกส์ในรูปแบบ Extensible Markup Language (XML)
   ETSI EN 319 132-1 XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures
3. **PDF Advanced Electronic Signatures (PADES)**
   สำหรับเอกสารอิเล็กทรอนิกส์ในรูปแบบ Portable Data Format (PDF)
   ETSI EN 319 142-1 PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures
4. **JSON Advanced Electronic Signatures (JADES)**
   สำหรับเอกสารอิเล็กทรอนิกส์ในรูปแบบ Javascript Object Notation (JSON)
   ETSI TS 119 182-1 JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures
5. **Associated Signature Containers (ASiC)**
   สำหรับการรวมเอกสารอิเล็กทรอนิกส์มากกว่าหนึ่งฉบับมาลงลายมือชื่อและประทับรับรองเวลาร่วมกัน
   ETSI EN 319 162-1 Associated Signature Containers (ASiC): Part 1: Building blocks and ASiC baseline containers

ETSI TR 119 100

Guidance on the use of standards for signature creation and validation

กระบวนการประยุกต์ใช้มาตรฐาน
สำหรับการสร้างและตรวจสอบความถูกต้องของลายมือชื่อ



- ขั้นตอนที่ 1 (Phase 1)
  กระบวนเก็บรวบรวมความต้องการใช้ลายมือชื่อดิจิทัลกับกระบวนการทางธุรกิจ
- ขั้นตอนที่ 2 (Phase 2)
  กระบวนการรวบรวมนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยของการใช้ลายมือชื่อ
- ขั้นตอนที่ 3 (Phase 3)
  กระบวนการวิเคราะห์พารามิเตอร์กำหนดขอบเขตของธุรกิจ (BSP: Business Scoping Parameters)
  - BSP ที่เกี่ยวข้องกับกระบวนการทางธุรกิจในรูปแบบอิเล็กทรอนิกส์ของลายมือชื่อดิจิทัล
  - BSP ที่เกี่ยวข้องกับกฎหมายและกฎเกณฑ์กำกับกระบวนการทางธุรกิจ
  - BSP ที่เกี่ยวกับผู้สร้างลายมือชื่อดิจิทัล
  - BSP ที่มาจากแหล่งข้อมูลที่ต้องคำนึงถึงอื่นๆ นอกเหนือจาก 3 กลุ่มข้างต้น
- ขั้นตอนที่ 4 (Phase 4)
  กระบวนการในการตัดสินใจวิธีการทางเทคนิค

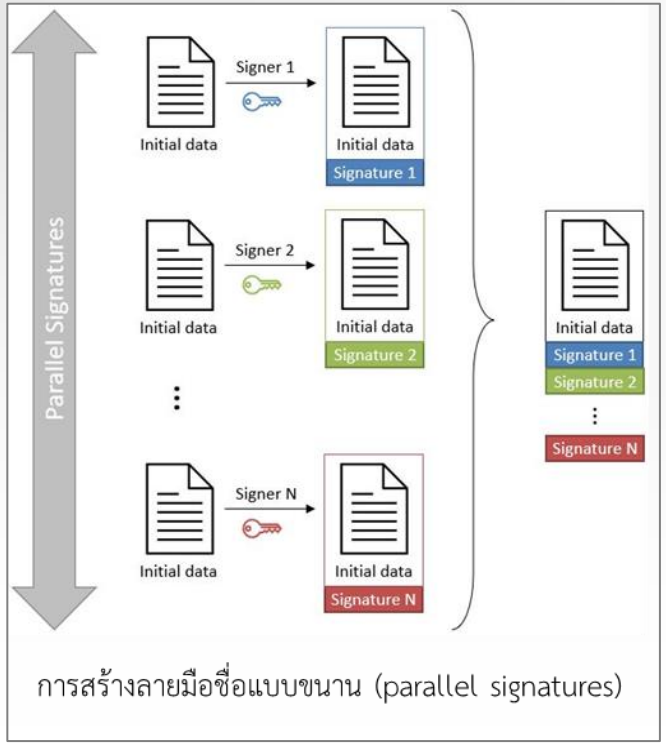
ETSI TR 119 100

Guidance on the use of standards for signature creation and validation

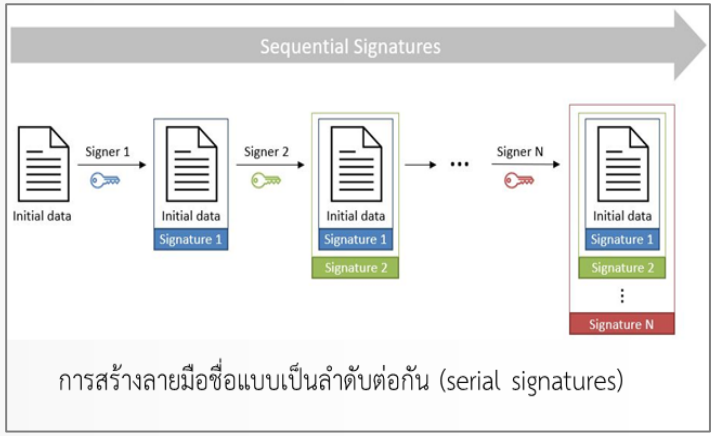
การวิเคราะห์พารามิเตอร์กำหนดขอบเขตของธุรกิจ (BSP: business scoping parameters)

- **BSP (a) เวิร์คโฟล (ช่วงเวลาและลำดับ)**

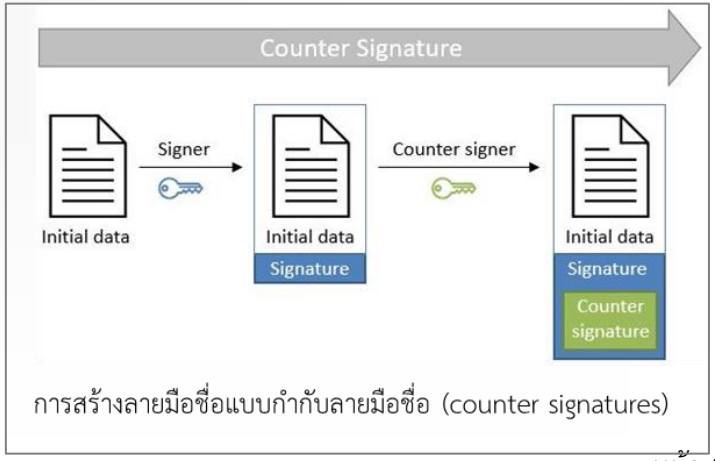
พารามิเตอร์ที่เกี่ยวข้องกับเวลาจะมีความสัมพันธ์กับการลงลายมือชื่อหรือไม่ และในกรณีที่มีการลงลายมือชื่อมากกว่าหนึ่งเจ้าของลายมือชื่อ พารามิเตอร์ที่เกี่ยวกับลำดับลายมือชื่อจะมีความสัมพันธ์กับการลงลายมือชื่อหรือไม่



การสร้างลายมือชื่อแบบขนาน (parallel signatures)



การสร้างลายมือชื่อแบบเป็นลำดับต่อกัน (serial signatures)



การสร้างลายมือชื่อแบบกำกับลายมือชื่อ (counter signatures)

ETSI TR 119 100

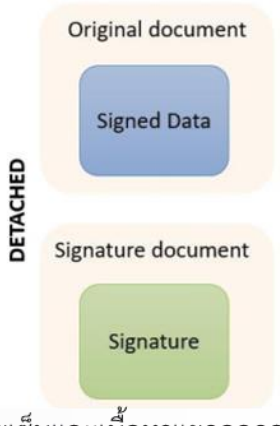
Guidance on the use of standards for signature creation and validation

การวิเคราะห์พารามิเตอร์กำหนดขอบเขตของธุรกิจ (BSP: business scoping parameters)

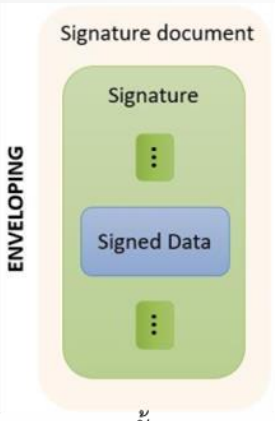
- **BSP (c): ความสัมพันธ์ระหว่างลายมือชื่อดิจิทัลกับอ็อบเจกต์ข้อมูลที่ถูกลงลายมือชื่อ**

ข้อแนะนำของตำแหน่งของข้อมูลที่ลงลายมือชื่อและข้อมูลลายมือชื่อ จะมี 3 แบบ ประกอบด้วย

ลายเซ็นและเนื้อหาอยู่ในไฟล์เดียวกัน
เช่น ใบรับรองแพทย์ในรูปแบบ PDF



ลายเซ็นและเนื้อหาแยกออกจากกัน
เช่น ไฟล์ PDF ขนาดใหญ่, ไฟล์มัลติมีเดีย



ลายเซ็นครอบคลุมเนื้อหาเอกสารทั้งหมด เหมาะสำหรับเอกสารที่ต้องการ
ความปลอดภัยสูง เช่น เอกสารทางกฎหมายที่ต้องลงนามทุกหน้า

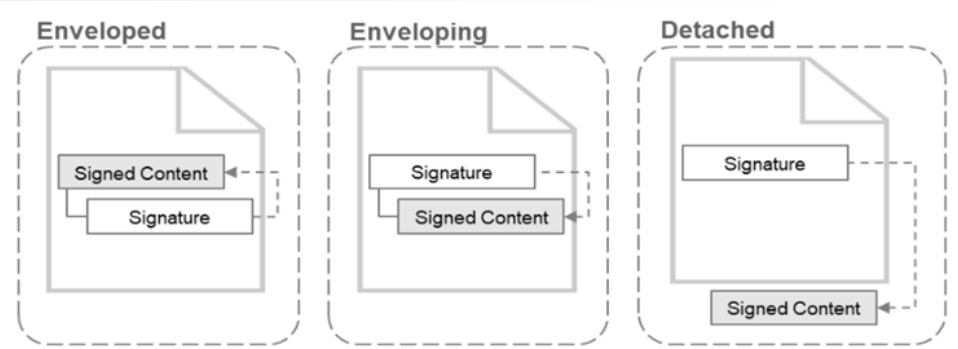
ETSI TR 119 100

Guidance on the use of standards for signature creation and validation

การวิเคราะห์พารามิเตอร์กำหนดขอบเขตของธุรกิจ (BSP: business scoping parameters)

- **BSP (c): ความสัมพันธ์ระหว่างลายมือชื่อดิจิทัลกับอ็อบเจกต์ข้อมูลที่ถูกลงลายมือชื่อ**

  ข้อแนะนำของตำแหน่งของข้อมูลที่ลงลายมือชื่อและข้อมูลลายมือชื่อ จะมี 3 แบบ ประกอบด้วย



	Enveloped	Enveloping	Detached
CAdES		X	X
XAdES	X	X	X
PAdES	X		
JAdES		X	X
ASiC			X

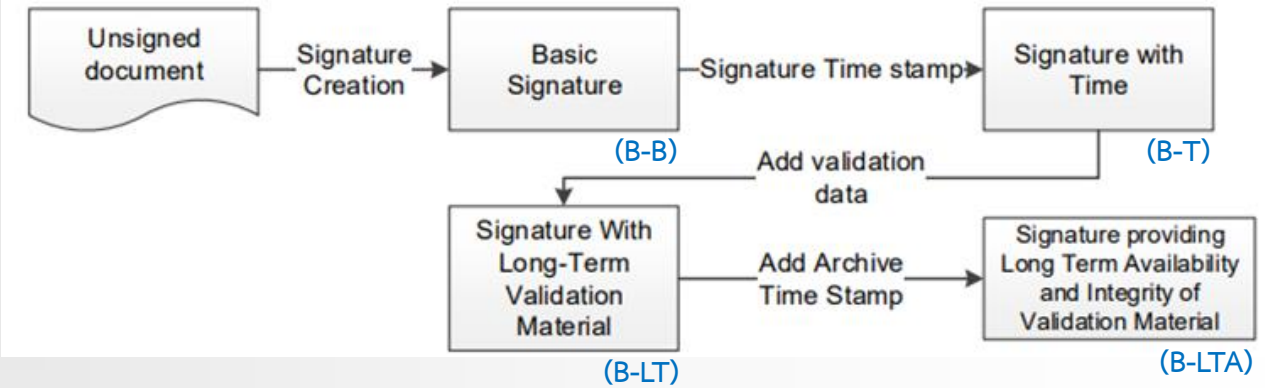
Compatibility of the packaging with the AdES formats

ETSI EN 319 102-1

Security requirements for signature creation applications and signature validation applications

การเพิ่มความน่าเชื่อถือให้กับลายมือชื่อ (Signature Augmentation)

กระบวนการในการสร้างและเพิ่มความน่าเชื่อถือให้กับลายมือชื่อ (signature creation and augmentation process)

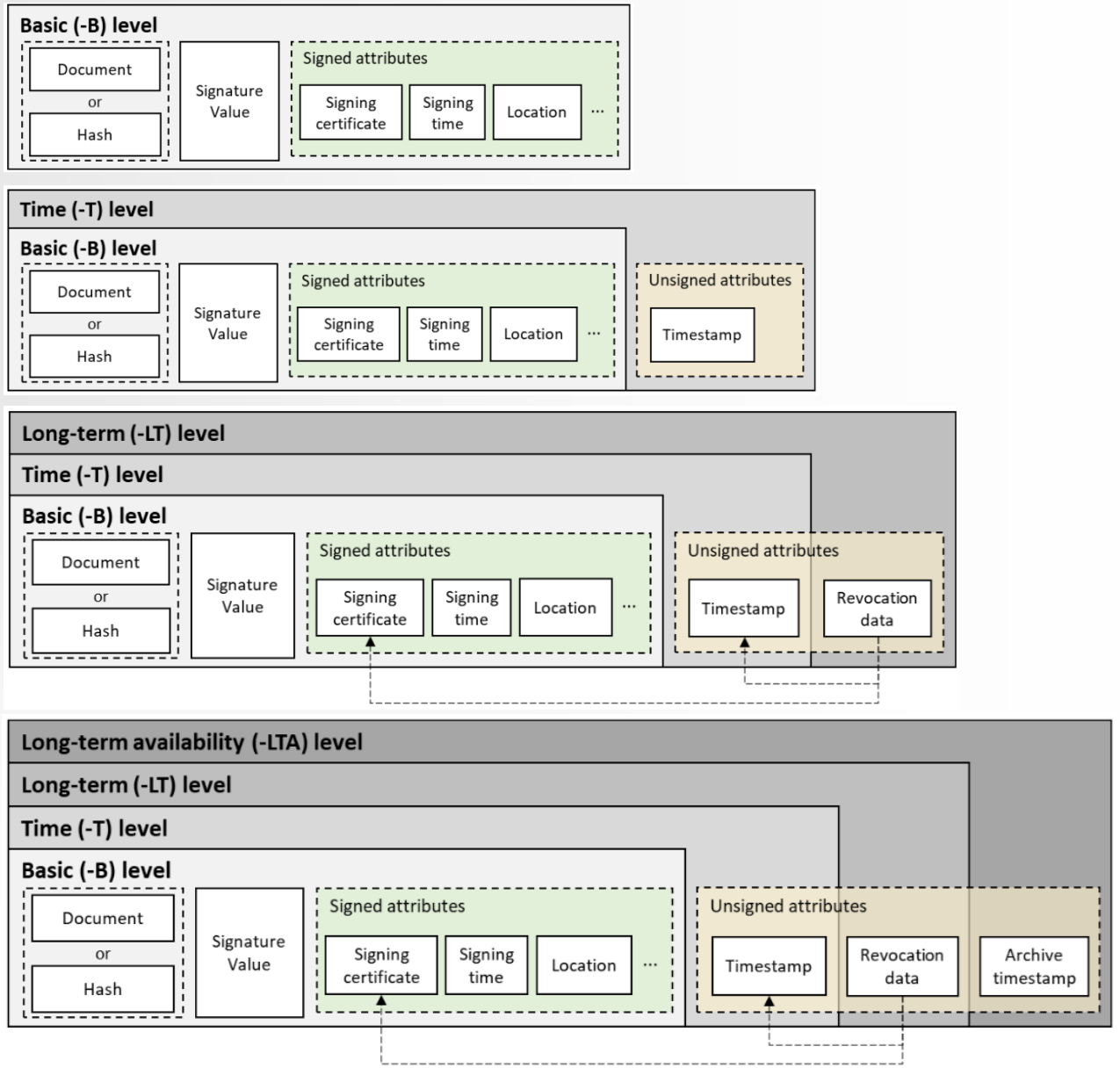


- **ลายมือชื่อพื้นฐาน (basic signature)**
  ลายมือชื่อที่สามารถตรวจสอบความถูกต้องของลายมือชื่อได้ ตราบเท่าที่ใบรับรองยังไม่หมดอายุหรือไม่ถูกเพิกถอน (B-B)
- **ลายมือชื่อที่มีข้อมูลเวลา (signature with time)**
  ลายมือชื่อที่สามารถพิสูจน์ได้ว่าคงอยู่ ณ เวลาที่กำหนด (B-T)
- **ลายมือชื่อที่มีข้อมูลตรวจสอบความถูกต้องในระยะยาว (signature with long-term validation material)**
  ลายมือชื่อที่ข้อมูลตรวจสอบความถูกต้องลายมือชื่อมีความพร้อมใช้ในระยะยาว
- **ลายมือชื่อที่มีความพร้อมใช้ในระยะยาวและมีความสมบูรณ์ครบถ้วนของข้อมูลตรวจสอบความถูกต้องลายมือชื่อ (signature providing long term availability and integrity of validation material)**
  ลายมือชื่อที่ต้องการให้มีความพร้อมใช้งานในระยะยาว ซึ่งเกินระยะเวลาที่สามารถใช้งานได้ (B-LTA)

ETSI EN 319 102-1

Security requirements for signature creation applications and signature validation applications

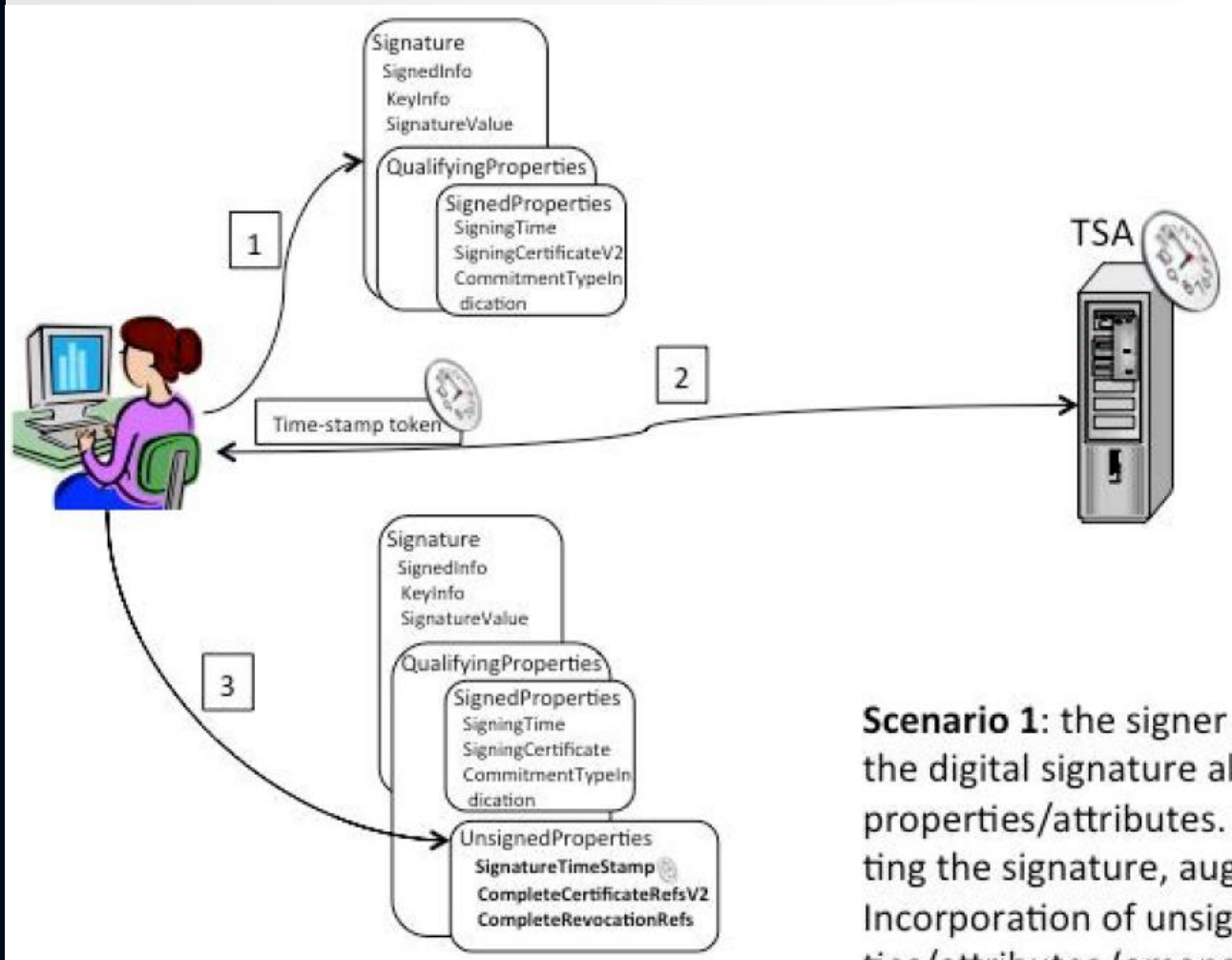
การเพิ่มความน่าเชื่อถือให้กับลายมือชื่อ (Signature Augmentation)



ตัวอย่างการเพิ่มความน่าเชื่อถือให้กับลายมือชื่อ

การเพิ่มความน่าเชื่อถือให้กับลายมือชื่อ

(Signature Augmentation)

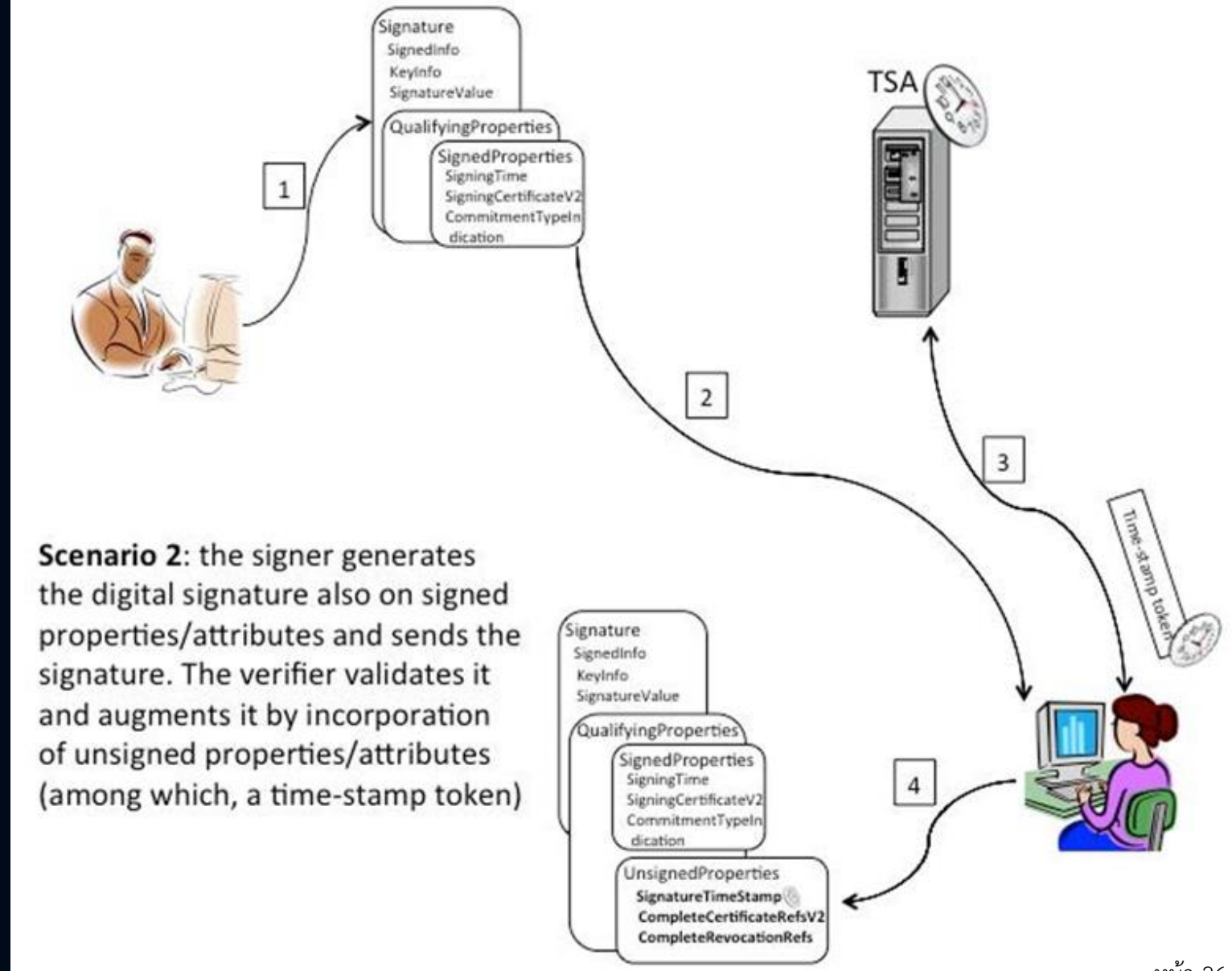


Scenario 1: the signer generates the digital signature also on signed properties/attributes. After generating the signature, augments it by Incorporation of unsigned properties/attributes (among which, in this picture, a time-stamp token.

ตัวอย่างการเพิ่มความน่าเชื่อถือให้กับลายมือชื่อ

การเพิ่มความน่าเชื่อถือให้กับลายมือชื่อ

(Signature Augmentation)



Scenario 2: the signer generates the digital signature also on signed properties/attributes and sends the signature. The verifier validates it and augments it by incorporation of unsigned properties/attributes (among which, a time-stamp token)

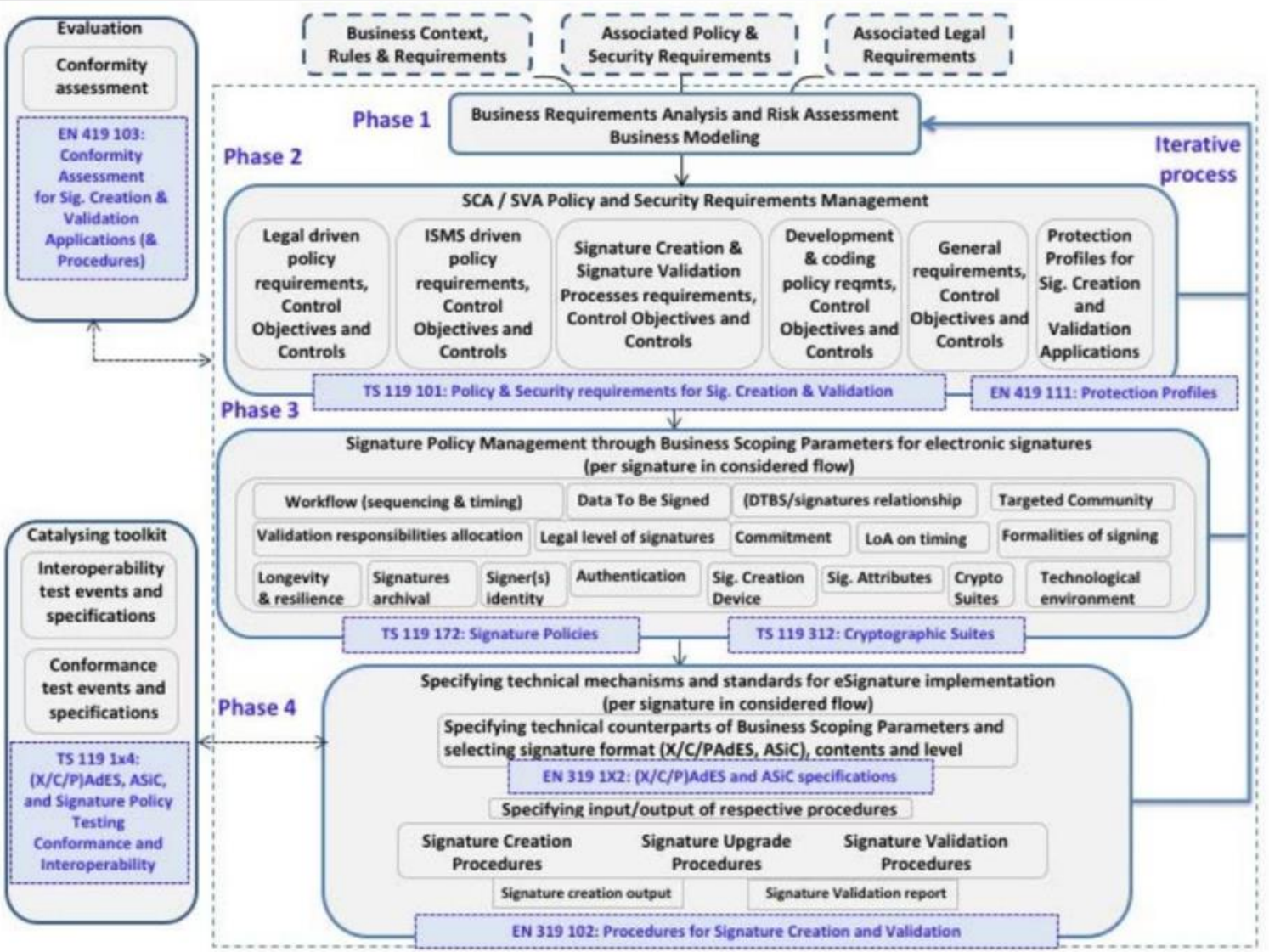
หัวข้อการสัมมนา

- กฎหมายที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์
- ภาพรวมของลายมือชื่ออิเล็กทรอนิกส์
- กรอบแนวปฏิบัติการลงลายมือชื่อดิจิทัล
- กรอบแนวทางการพัฒนาและส่วนประกอบที่เกี่ยวข้องกับระบบลงลายมือชื่อดิจิทัล

ETSI TR 119 100

Guidance on the use of standards for signature creation and validation

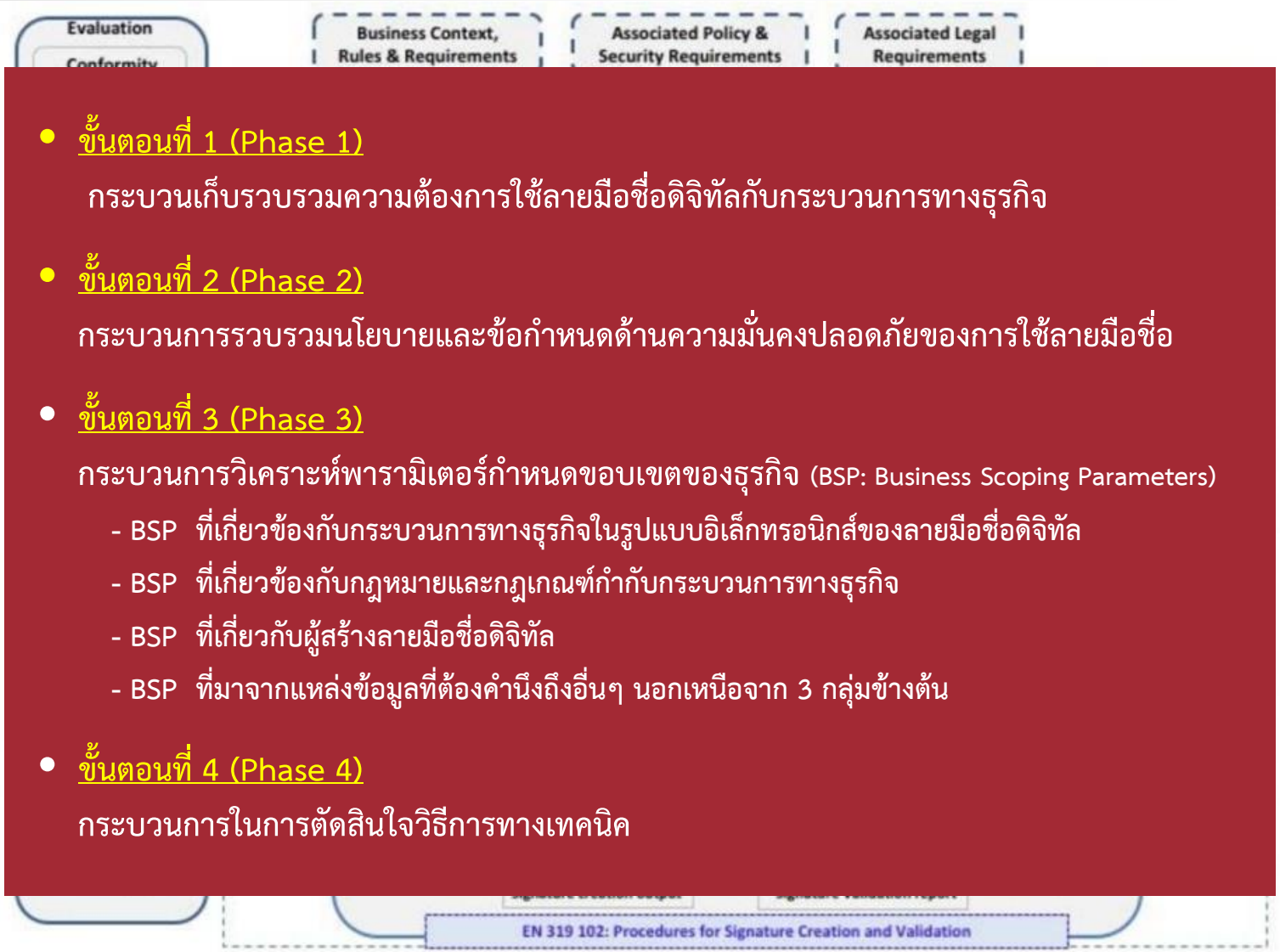
กระบวนการประยุกต์ใช้มาตรฐาน
สำหรับการสร้างและตรวจสอบความถูกต้องของลายมือชื่อ



ETSI TR 119 100

Guidance on the use of standards for signature creation and validation

กระบวนการประยุกต์ใช้มาตรฐาน
สำหรับการสร้างและตรวจสอบความถูกต้องของลายมือชื่อ



- ขั้นตอนที่ 1 (Phase 1)
  กระบวนเก็บรวบรวมความต้องการใช้ลายมือชื่อดิจิทัลกับกระบวนการทางธุรกิจ
- ขั้นตอนที่ 2 (Phase 2)
  กระบวนการรวบรวมนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยของการใช้ลายมือชื่อ
- ขั้นตอนที่ 3 (Phase 3)
  กระบวนการวิเคราะห์พารามิเตอร์กำหนดขอบเขตของธุรกิจ (BSP: Business Scoping Parameters)
  - BSP ที่เกี่ยวข้องกับกระบวนการทางธุรกิจในรูปแบบอิเล็กทรอนิกส์ของลายมือชื่อดิจิทัล
  - BSP ที่เกี่ยวข้องกับกฎหมายและกฎเกณฑ์กำกับกระบวนการทางธุรกิจ
  - BSP ที่เกี่ยวกับผู้สร้างลายมือชื่อดิจิทัล
  - BSP ที่มาจากแหล่งข้อมูลที่ต้องคำนึงถึงอื่นๆ นอกเหนือจาก 3 กลุ่มข้างต้น
- ขั้นตอนที่ 4 (Phase 4)
  กระบวนการในการตัดสินใจวิธีการทางเทคนิค

ENISA

Security guidelines on the appropriate use of qualified electronic signatures

มาตรฐานสำนักงานรัฐบาลดิจิทัล ว่าด้วยแนวปฏิบัติ
การลงลายมืออิเล็กทรอนิกส์สำหรับเจ้าหน้าที่
เลขที่ มพสร. 7/2565

การประเมินลักษณะของธุรกรรมตามระดับความวิกฤต (Criticality Levels)

- **ระดับธรรมดา (Standard)**

  ธุรกรรมทั่วไปการแลกเปลี่ยนหรือเข้าถึงข้อมูลอย่างจำกัดที่มีผลกระทบในระดับต่ำต่อองค์กร ซึ่งอาจรวมถึงการแลกเปลี่ยนข้อมูลภายในองค์กรที่อยู่ในลำดับชั้นข้อมูลที่ต่ำ

- **ระดับขั้นสูง (Advanced)**

  ธุรกรรมที่ต้องมีการพิจารณาอย่างรอบคอบถึงเงื่อนไขหรือข้อควรระวังเบื้องต้น อาจมีความเกี่ยวข้องกับความเสี่ยงทางด้านการเงินในระดับจำกัด หรืออาจมีการแลกเปลี่ยนข้อมูลในลำดับชั้นของข้อมูลที่สูงขึ้น เช่น ข้อมูลที่เป็นความลับ (Confidential)

- **ระดับอ่อนไหว (Sensitive)**

  ธุรกรรมที่เกี่ยวข้องกับข้อมูลที่มีความละเอียดอ่อน อาจมีความเสี่ยงทางด้านการเงินโดยตรง หรืออาจมีการแลกเปลี่ยนข้อมูลในลำดับชั้นของข้อมูลที่สูงมาก

ระดับความเสี่ยงของธุรกรรมและประเภทลายมือชื่ออิเล็กทรอนิกส์ที่แนะนำ

ระดับความเสี่ยงของธุรกรรม	แนวทางการเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์ ตาม ENISA
ระดับธรรมดา (Standard)	SES หรือ AdES ประเภท B-B
ระดับขั้นสูง (Advanced)	AdES ประเภท B-T เป็นอย่างน้อย และ B-LT / B-LTA หากจำเป็น
ระดับอ่อนไหว (Sensitive)	แนะนำให้ใช้ QES และบริการเสริมจาก Qualified Trust Services

การใช้ลายมือชื่อดิจิทัล ให้มีความปลอดภัย

4 องค์ประกอบสำคัญที่ต้องพิจารณา

หัวข้อการสัมมนา

- กฎหมายที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์
- ภาพรวมของลายมือชื่ออิเล็กทรอนิกส์
- กรอบแนวปฏิบัติการลงลายมือชื่อดิจิทัล
- กรอบแนวทางการพัฒนาและส่วนประกอบที่เกี่ยวข้องกับระบบลงลายมือชื่อดิจิทัล

ส่วนประกอบที่เกี่ยวข้องกับระบบลงลายมือชื่อดิจิทัล

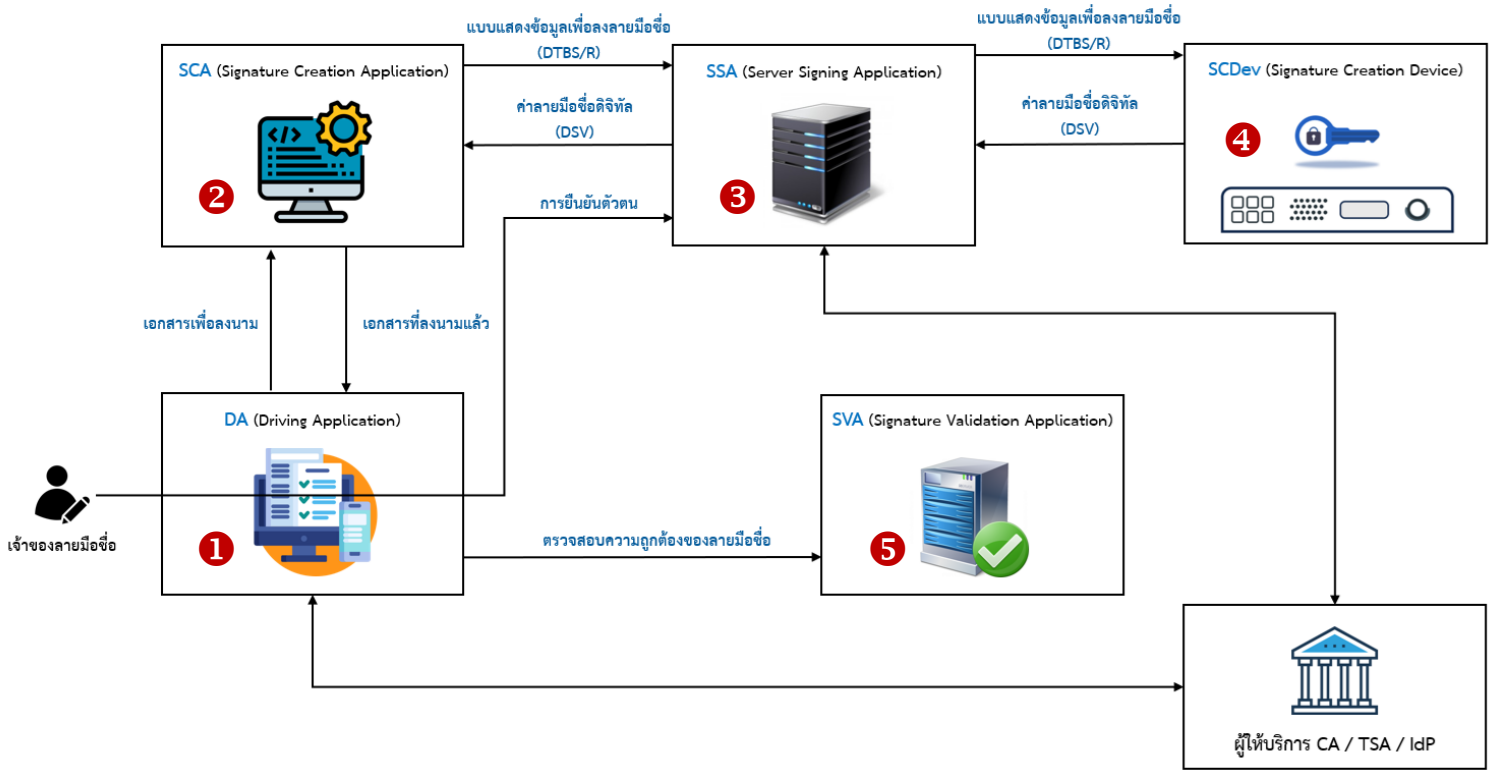
ข้อเสนอแนะมาตรฐานฯ ว่าด้วยบริการลงลายมือชื่อดิจิทัล
ที่ใช้การควบคุมจากระยะไกล
เลขที่ ขมธอ. 36-2566

และ

มาตรฐานสำนักงานรัฐบาลดิจิทัล ว่าด้วยแนวปฏิบัติ
การลงลายมืออิเล็กทรอนิกส์สำหรับเจ้าหน้าที่
เลขที่ มพสร. 7/2565

ส่วนประกอบที่เกี่ยวข้องกับระบบลงลายมือชื่อดิจิทัลที่แนะนำ

การพัฒนาระบบลงลายมือชื่อดิจิทัลให้มีคุณสมบัติสอดคล้องตาม พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และมาตรฐาน ETSI ของสหภาพยุโรป เพื่อให้ระบบได้มาตรฐานสากล มีความมั่นคงปลอดภัย และมีการบริหารจัดการข้อมูลส่วนบุคคลของผู้ใช้งานอย่างเหมาะสมนั้น ระบบลงลายมือชื่อดิจิทัลที่แนะนำ ควรมี 5 ส่วนประกอบหลักดังต่อไปนี้เป็นอย่างน้อย



ส่วนประกอบที่เกี่ยวข้องกับระบบลงลายมือชื่อดิจิทัล

ข้อเสนอแนะมาตรฐานฯ ว่าด้วยบริการลงลายมือชื่อดิจิทัล
ที่ใช้การควบคุมจากระยะไกล
เลขที่ ขมธอ. 36-2566

และ

มาตรฐานสำนักงานรัฐบาลดิจิทัล ว่าด้วยแนวปฏิบัติ
การลงลายมืออิเล็กทรอนิกส์สำหรับเจ้าหน้าที่
เลขที่ มพสร. 7/2565

ส่วนประกอบที่เกี่ยวข้องกับระบบลงลายมือชื่อดิจิทัลที่แนะนำ

1. **DA (Driving Application)**
   คือ แอปพลิเคชันที่ผู้ใช้โต้ตอบเพื่อเริ่มกระบวนการลงลายมือชื่อดิจิทัล เช่น ระบบที่ทำหน้าที่บริหารจัดการเอกสารอิเล็กทรอนิกส์และการลงนามลายมือชื่อดิจิทัล เป็นต้น

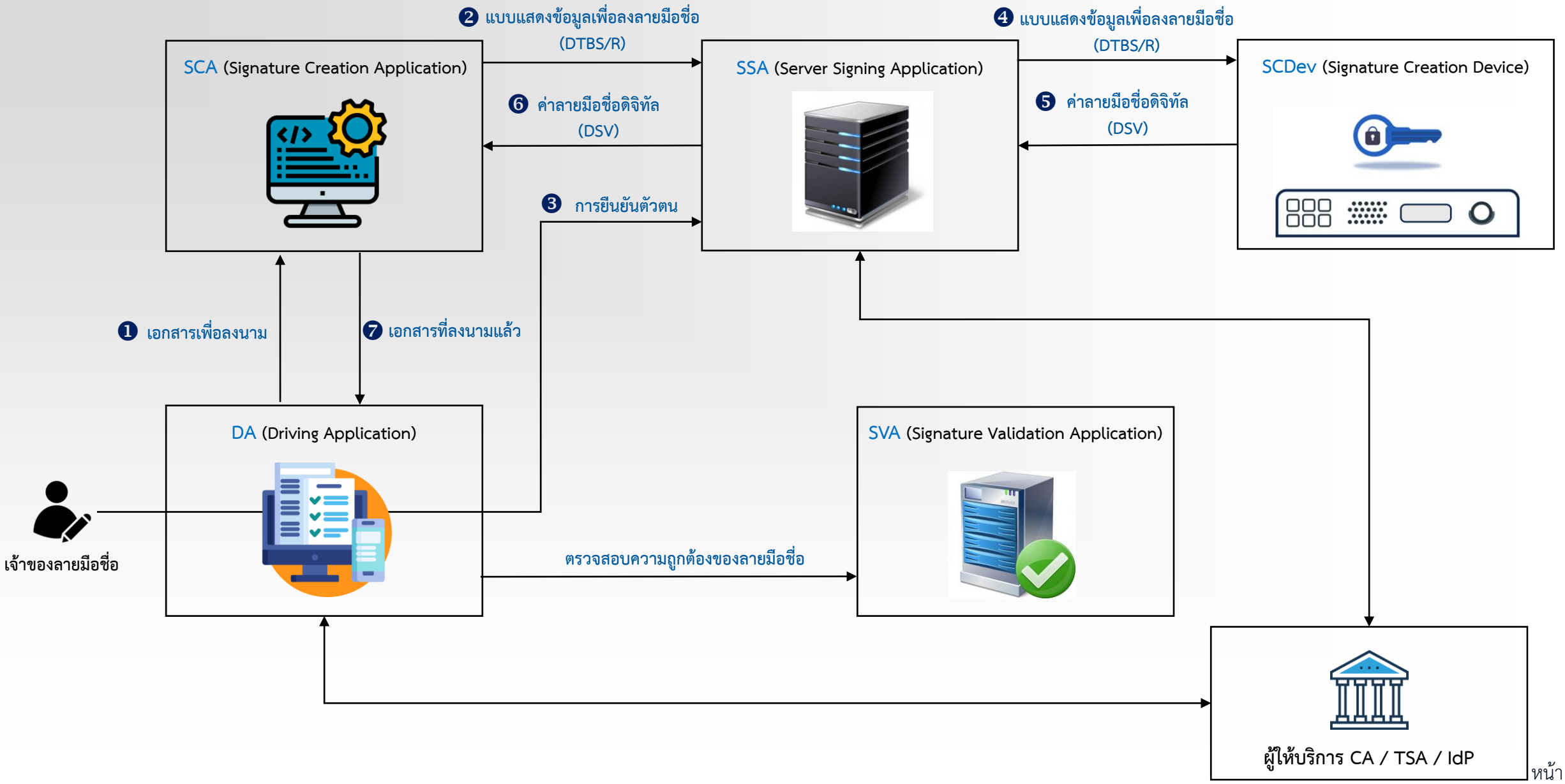
2. **SCA (Signature Creation Application)**
   2.1 ทำหน้าที่นำค่าแฮชของเอกสารที่จะลงลายมือชื่อ และค่าแฮชของรายการข้อมูลที่จะลงลายมือชื่อ (signed attributes) มาจัดองค์ประกอบ จัดรูปแบบ และคำนวณค่าแฮชออกมาเป็นแบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R)
   2.2 ทำหน้าที่รับค่าลายมือชื่อดิจิทัล (DSV) ที่สร้างจาก SSA มาจัดรูปแบบเป็นเอกสารที่ลงลายมือชื่อแล้วตามรูปแบบที่ผู้ใช้งานร้องขอ เช่น เอกสาร PDF ที่ลงลายมือชื่อดิจิทัล แบบ PAdES (PDF Advanced Electronic Signature) เป็นต้น

3. **SSA (Server Signing Application)**
   ทำหน้าที่เรียกใช้ SCDev เพื่อสร้างค่าลายมือชื่อดิจิทัล (DSV) ภายใต้การควบคุมของเจ้าของลายมือชื่อที่ได้รับอนุญาตเท่านั้น โดยจะต้องทำการยืนยันตัวตนก่อนทุกครั้ง

4. **SCDev (Signature Creation Device)**
   คือ อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล ทำหน้าที่บริหารจัดการกุญแจส่วนตัวให้มีความมั่นคงปลอดภัย เพื่อป้องกันไม่ให้ผู้อื่นซึ่งไม่ได้รับการอนุญาตลงลายมือชื่อแทน ซึ่ง SCDev นี้จะใช้กุญแจส่วนตัวนี้ ในการสร้างค่าลายมือชื่อดิจิทัล (DSV) จากแบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R)

5. **SVA (signature validation application)**
   ทำหน้าที่ในการตรวจสอบลายมือชื่อดิจิทัลว่าถูกต้องและเชื่อถือได้หรือไม่

ส่วนประกอบที่เกี่ยวข้องกับระบบลงลายมือชื่อดิจิทัลที่แนะนำ




Q&A