สัมมนาเผยแพร่ความรู้และผลการศึกษา

ลายมือชื่อดิจิทัล ครั้งที่ 1

กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม

ETDA

การยกระดับลายมือชื่อดิจิทัล ให้มีความน่าเชื่อถือในระยะยาว

(long-term digital signature)

วันศุกร์ที่ 21 มิถุนายน 2567 เวลา 9.30 - 12.00 น.

ผ่านโปรแกรม Microsoft teams

ลงทะเบียน

แบบฟอร์มลงทะเบียน

เพื่อรับ Link เข้าประชุม

http://bit.ly/3XmhVVQ

หัวข้อการสัมมนา

- กฎหมายไทยและกฎหมายต่างประเทศ ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล
- การวิเคราะห์พารามิเตอร์ทางธุรกิจ (BSP: Business Scoping Parameter) เพื่อเลือกใช้มาตรฐานทางเทคนิคที่เหมาะสมกับลายมือชื่อดิจิทัล
- ประเภทของลายมือชื่อ (signature class) และระดับความน่าเชื่อถือ
- แบบจำลองส่วนประกอบพื้นฐานและกรอบกระบวนทำงาน (building blocks and framework) ในการสร้าง (creation) การเพิ่มความน่าเชื่อถือ (augmentation) และการตรวจสอบความถูกต้อง (validation) ของลายมือชื่อดิจิทัล

หัวข้อการสัมมนา

- กฎหมายไทยและกฎหมายต่างประเทศ ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล
- การวิเคราะห์พารามิเตอร์ทางธุรกิจ (BSP: Business Scoping Parameter) เพื่อเลือกใช้มาตรฐานทางเทคนิคที่เหมาะสมกับลายมือชื่อดิจิทัล
- ประเภทของลายมือชื่อ (signature class) และระดับความน่าเชื่อถือ
- แบบจำลองส่วนประกอบพื้นฐานและกรอบกระบวนทำงาน (building blocks and framework) ในการสร้าง (creation) การเพิ่มความน่าเชื่อถือ (augmentation) และการตรวจสอบความถูกต้อง (validation) ของลายมือชื่อดิจิทัล

กฎหมายไทย

พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

พระราชบัญญัตินี้ใช้บังคับแก่ธุรกรรมในทางแพ่งและพาณิชย์ที่ดำเนินการโดยใช้ข้อมูลอิเล็กทรอนิกส์ ซึ่งประกอบด้วยทั้งหมด 6 หมวด

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 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	ลักษณะของ ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้
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.

การลงลายมือชื่อดิจิทัล

Local Signing *vs* Remote Signing

Local Signing

กุญแจสำหรับสร้างลายมือชื่อดิจิทัล ถูกเก็บไว้ที่เจ้าของลายมือชื่อ

โดยอาจเก็บในอุปกรณ์อิเล็คทรอนิกส์ (hardware) เช่น USB Token

หรือ ติดตั้งในรูปแบบซอฟต์แวร์ (software) บนอุปกรณ์คอมพิวเตอร์

VS

กุญแจสำหรับสร้างลายมือชื่อดิจิทัล มิได้เก็บไว้ที่เจ้าของลายมือชื่อ

แต่ถูกเก็บไว้บนระบบ โดยเรียกใช้งานผ่านระบบเครือข่ายคอมพิวเตอร์

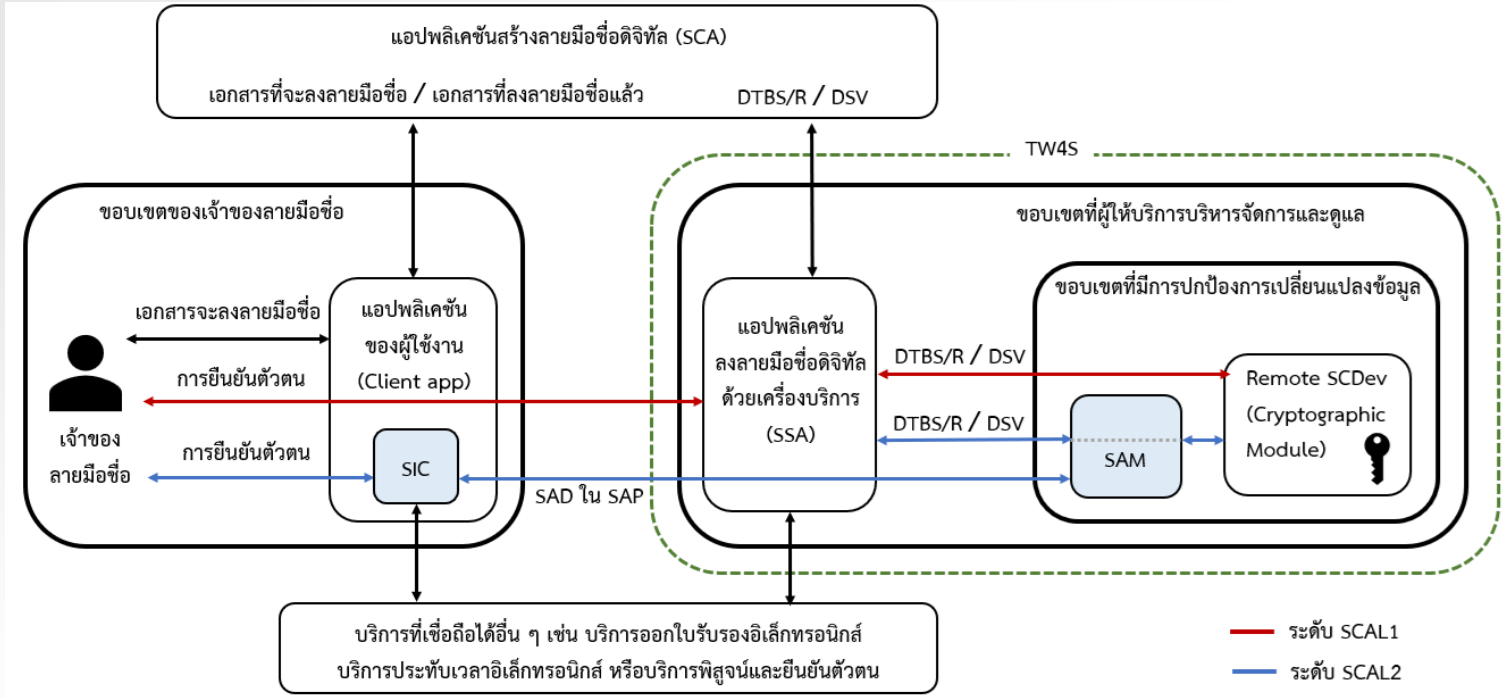
Remote Signing

การลงลายมือชื่อดิจิทัล

บริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล
(Remote Signing Service)

ข้อเสนอแนะมาตรฐานฯ
บริการลงลายมือชื่อดิจิทัล ที่ใช้การควบคุมจากระยะไกล (Remote Signing Service)

เลขที่ ขมธอ. 36-2566



- ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD)
- โมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM)
- โพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP)
- ระดับความเข้มงวดในการควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น (SCAL)
- อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote SCDev)
- ส่วนติดต่อของเจ้าของลายมือชื่อ (SIC)
- แบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R)
- ค่าลายมือชื่อดิจิทัล (DSV)

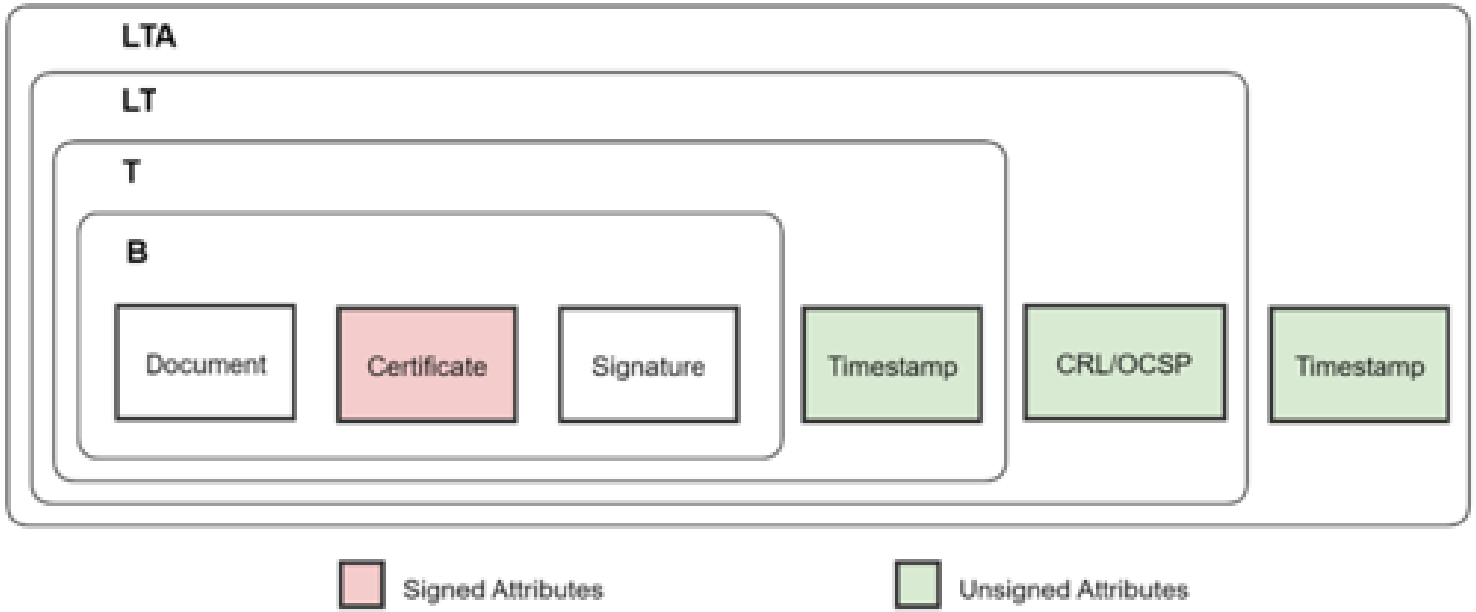
การลงลายมือชื่อดิจิทัล

3 + 1 องค์ประกอบสำคัญของลายมือชื่อดิจิทัล

การลงลายมือชื่อดิจิทัล

การเพิ่มความน่าเชื่อถือในระยะยาว
สำหรับลายมือชื่อดิจิทัล

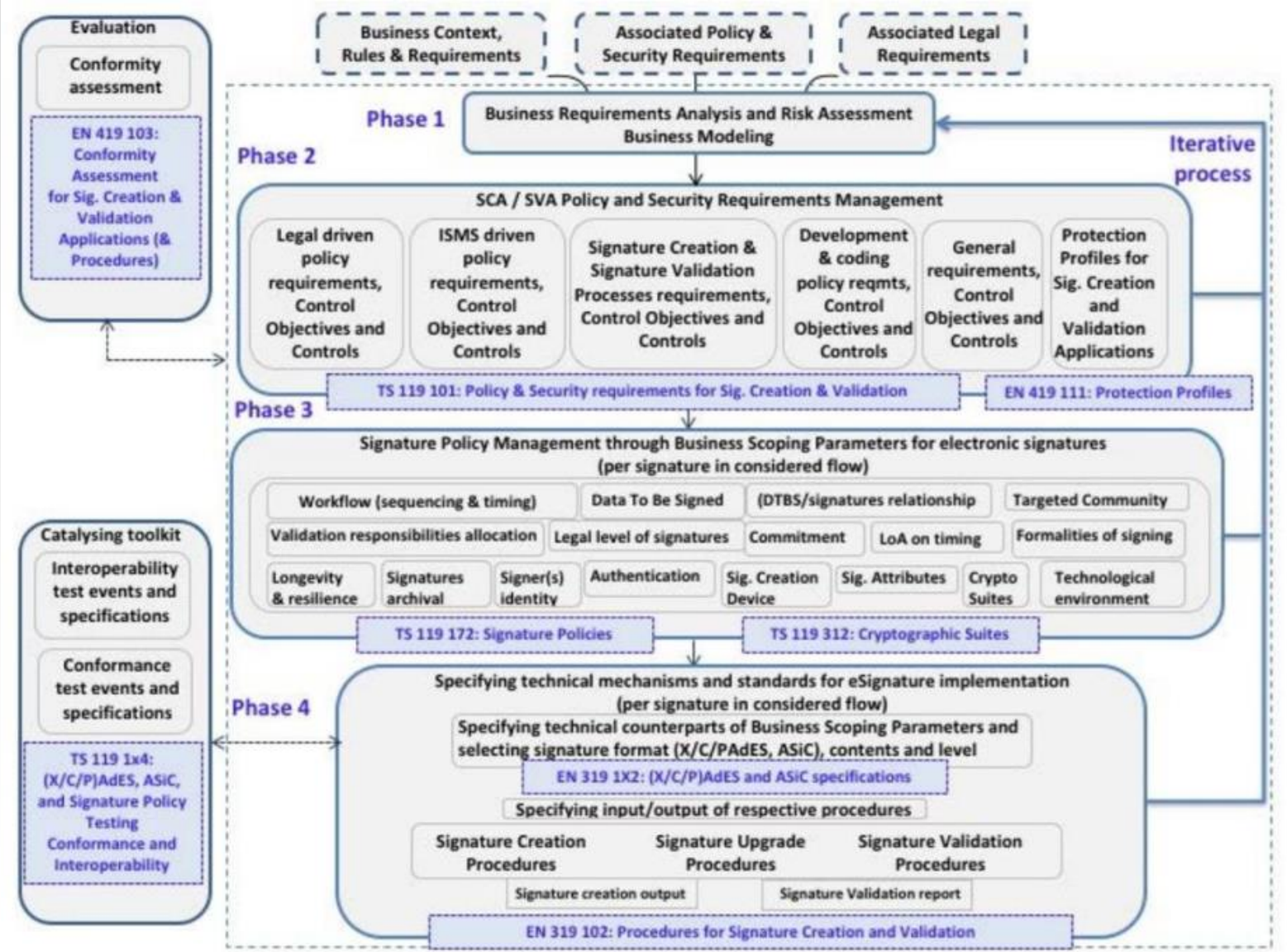
- **มาตรฐานประเภทของลายมือชื่อดิจิทัล (Signature Class)**
  - ระดับ B-B basic signature
  - ระดับ B-T signature with time
  - ระดับ B-LT signature with long-term validation material
  - ระดับ B-LTA signature with long-term availability and integrity of validation material



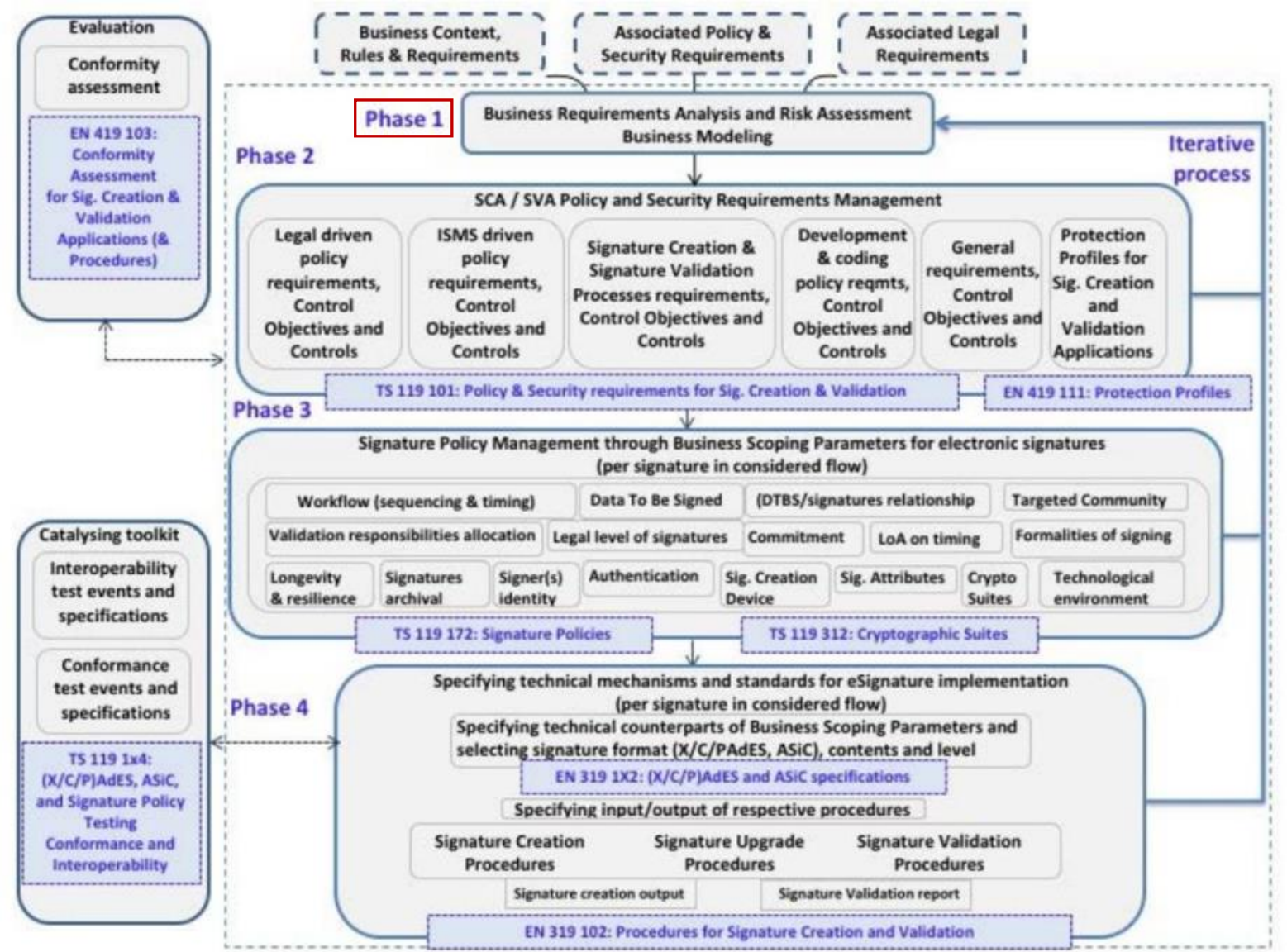
หัวข้อการสัมมนา

- กฎหมายไทยและกฎหมายต่างประเทศ ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล
- การวิเคราะห์พารามิเตอร์ทางธุรกิจ (BSP: Business Scoping Parameter) เพื่อเลือกใช้มาตรฐานทางเทคนิคที่เหมาะสมกับลายมือชื่อดิจิทัล
- ประเภทของลายมือชื่อ (signature class) และระดับความน่าเชื่อถือ
- แบบจำลองส่วนประกอบพื้นฐานและกรอบกระบวนทำงาน (building blocks and framework) ในการสร้าง (creation) การเพิ่มความน่าเชื่อถือ (augmentation) และการตรวจสอบความถูกต้อง (validation) ของลายมือชื่อดิจิทัล

กระบวนการประยุกต์ใช้มาตรฐานในการสร้างและตรวจสอบความถูกต้องของลายมือชื่อ (อ้างอิง ETSI TR 119 100 Guidance on the use of standards for signature creation and validation)



กระบวนการประยุกต์ใช้มาตรฐานในการสร้างและตรวจสอบความถูกต้องของลายมือชื่อ (อ้างอิง ETSI TR 119 100 Guidance on the use of standards for signature creation and validation)



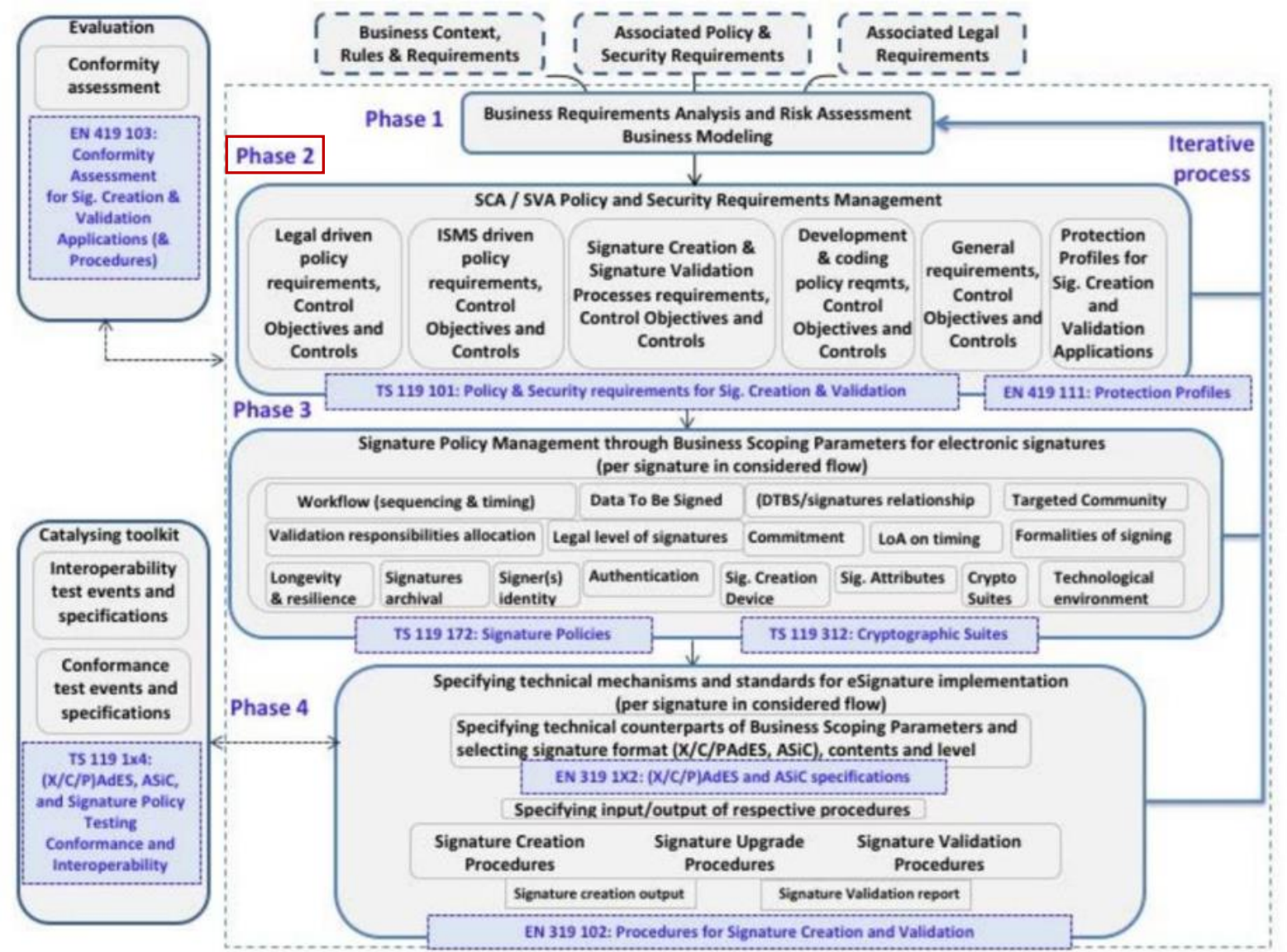
ขั้นตอนที่ 1 (Phase 1)

กระบวนเก็บรวบรวมความต้องการใช้ลายมือชื่อดิจิทัลกับกระบวนการทางธุรกิจ

เป็นขั้นตอนเริ่มต้นของกระบวนการประยุกต์ใช้ลายมือชื่อดิจิทัลกับกระบวนการทางธุรกิจในรูปแบบอิเล็กทรอนิกส์ เพื่อนำมาวิเคราะห์เป็นแบบจำลองทางธุรกิจ และประเด็นความเสี่ยงของธุรกิจที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

ในมาตรฐานฉบับนี้ไม่ได้เสนอวิธีการหรือกระบวนการในการวิเคราะห์ความเสี่ยง (risk assessment methodology) หรือจัดทำแบบจำลองทางธุรกิจ (business modelling) แต่มีการอ้างถึงเครื่องมือที่มีและได้รับการยอมรับ เช่น UML (Unified Modelling Language) และ BPMN (Business Process Management and Notation

กระบวนการประยุกต์ใช้มาตรฐานในการสร้างและตรวจสอบความถูกต้องของลายมือชื่อ (อ้างอิง ETSI TR 119 100 Guidance on the use of standards for signature creation and validation)



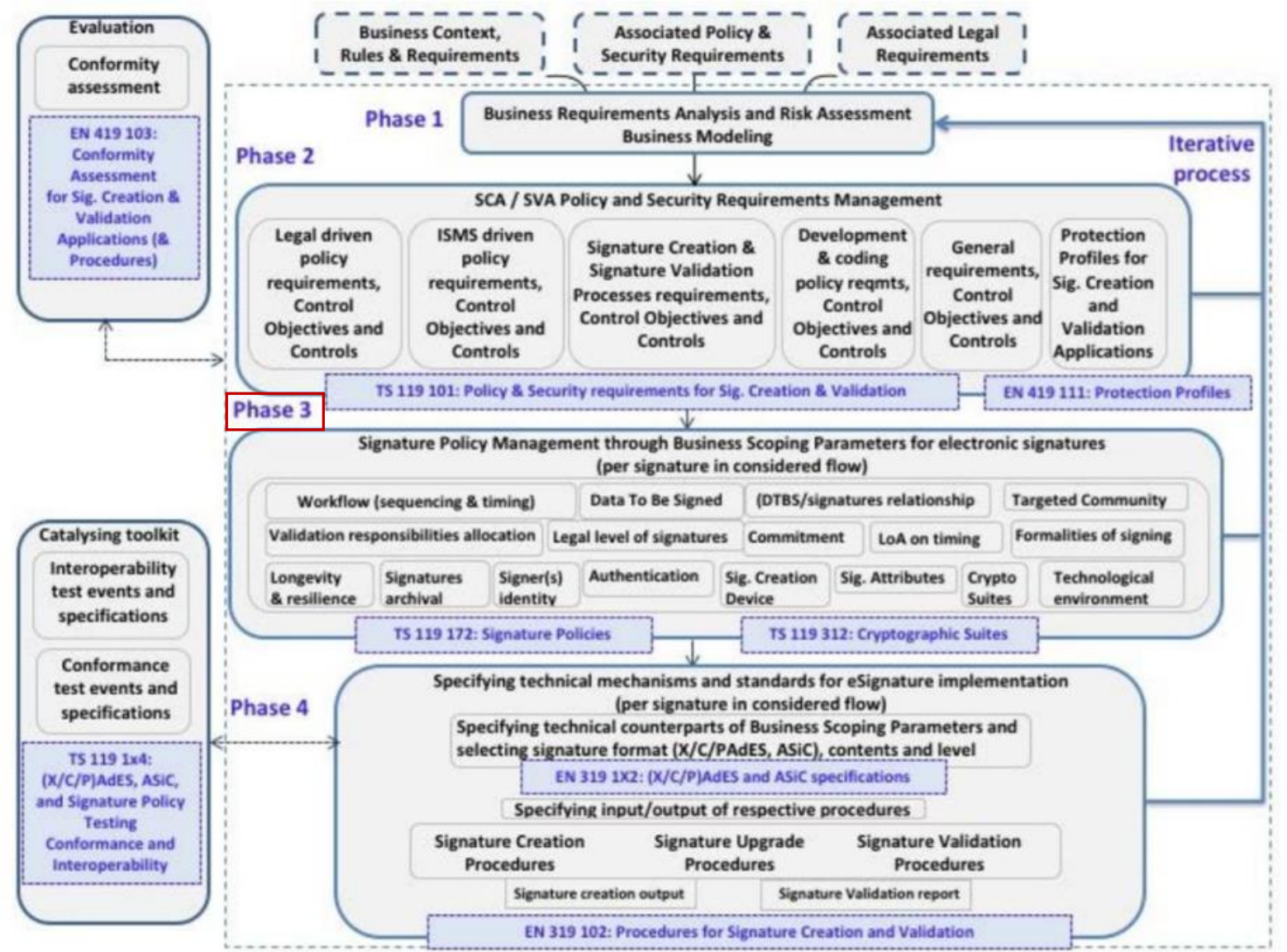
ขั้นตอนที่ 2 (Phase 2)

กระบวนการรวบรวมนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยของการใช้ลายมือชื่อ

เป็นกระบวนการที่จัดทำข้อกำหนดที่ต้องปฏิบัติและวัตถุประสงค์ในการปฏิบัติขึ้น โดยพิจารณาจากนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัย ข้อปฏิบัติในการขั้นตอนนี้ ประกอบด้วย

- ระบุข้อกำหนดที่เกี่ยวข้องจากแหล่งข้อมูลต่างๆ ที่เกี่ยวข้องกับบริบทในทางธุรกิจ อาทิ นโยบายที่เกี่ยวข้องกับกฎเกณฑ์กำกับและกรอบกฎหมายที่เกี่ยวข้อง เป็นต้น
- กำหนดวัตถุประสงค์และเป้าหมายของข้อกำหนดที่ต้องปฏิบัติ
- เลือกข้อกำหนดที่ต้องปฏิบัติมาปฏิบัติเพื่อให้บรรลุเป้าหมายที่ต้องการ

กระบวนการประยุกต์ใช้มาตรฐานในการสร้างและตรวจสอบความถูกต้องของลายมือชื่อ (อ้างอิง ETSI TR 119 100 Guidance on the use of standards for signature creation and validation)

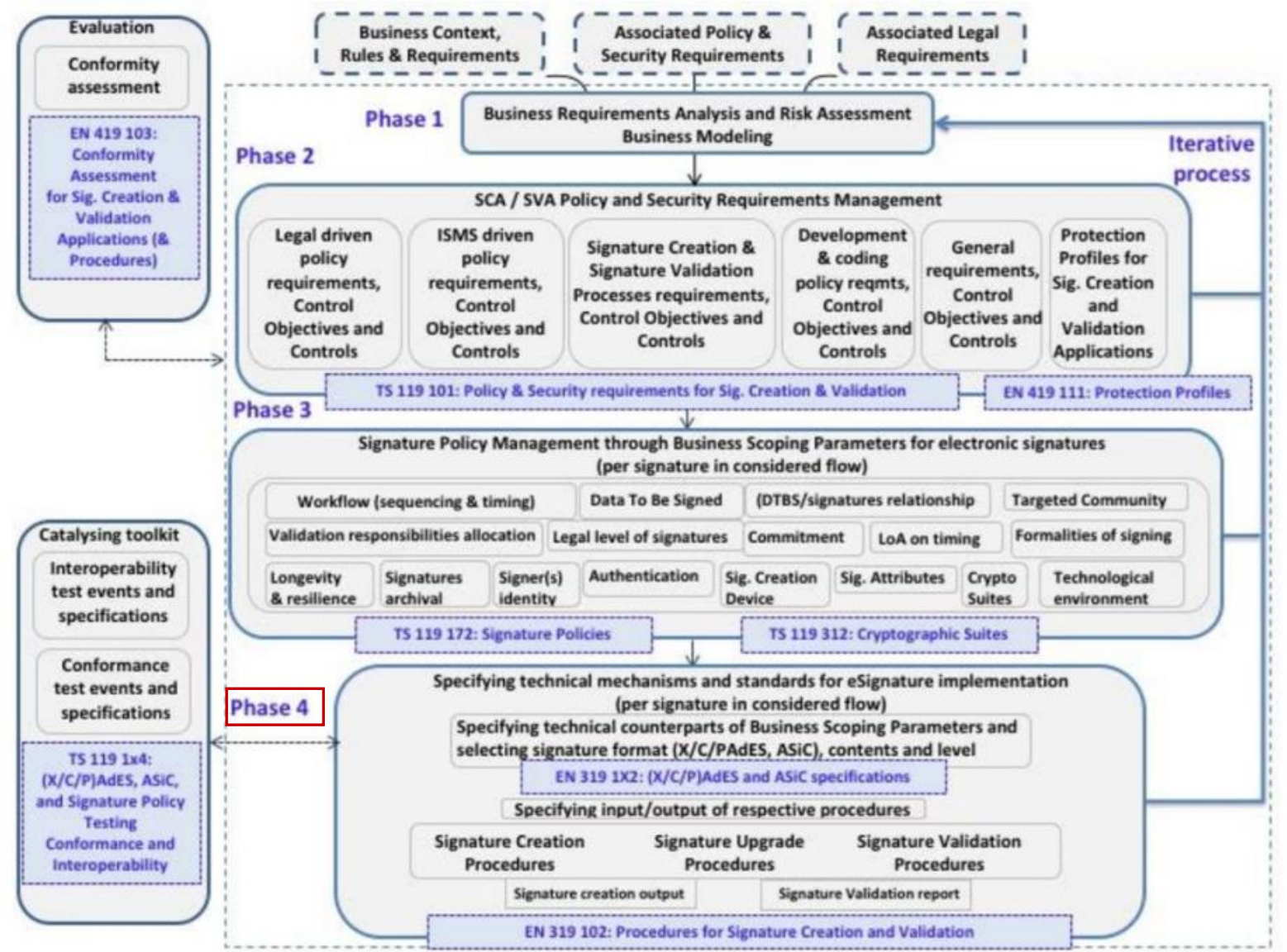


ขั้นตอนที่ 3 (Phase 3)

กระบวนการวิเคราะห์พารามิเตอร์กำหนดขอบเขตของธุรกิจ

เป็นกระบวนการที่มุ่งเน้นการวิเคราะห์พารามิเตอร์กำหนดขอบเขตของธุรกิจ (business scoping parameters) ในบริการของการประยุกต์ใช้ลายมือชื่อดิจิทัลในกระบวนการทางธุรกิจ ซึ่งจะมีขอบเขตตั้งแต่การเริ่มสร้างลายมือชื่อ การนำไปใช้งาน และการดูแลความน่าเชื่อถือของลายมือชื่อดิจิทัล

กระบวนการประยุกต์ใช้มาตรฐานในการสร้างและตรวจสอบความถูกต้องของลายมือชื่อ (อ้างอิง ETSI TR 119 100 Guidance on the use of standards for signature creation and validation)



ขั้นตอนที่ 4 (Phase 4)

กระบวนการในการตัดสินใจวิธีการทางเทคนิค

เพื่อตอบสนองต่อพารามิเตอร์กำหนดขอบเขตของธุรกิจ (business scoping parameters) ซึ่งเป็นผลลัพธ์ของการวิเคราะห์ความต้องการทางธุรกิจใน 3 ขั้นตอนแรก ข้อแนะนำในขั้นตอนนี้ จะช่วยให้ผู้ดำเนินการในการสร้างลายมือชื่อ (implementer) สามารถตัดสินในประเด็นต่างๆ ที่เกี่ยวข้องกับการเลือกมาตรฐานและกลไกทางเทคนิคที่เหมาะสม ประกอบด้วย

- มาตรฐานที่กำหนดรูปแบบ (formats) เนื้อความ (contents) และระดับ/ประเภทของลายมือชื่อดิจิทัล (levels of signature)

- ขั้นตอนปฏิบัติในเชิงเทคนิคในการสร้าง (generating) การเพิ่มความน่าเชื่อถือ (augmenting) และการตรวจสอบความถูกต้อง (validating) ให้กับลายมือชื่อดิจิทัล

- โปรไฟล์การป้องกัน (protection profiles) เป็นข้อกำหนดเทคนิคในด้านการรักษาความมั่นคงปลอดภัยสำหรับอุปกรณ์สร้างลายมือชื่อดิจิทัล แอปพลิเคชันตามแบบแสดงการทำงาน (functional model) ที่ต้องพัฒนาให้สอดคล้อง

ขั้นตอนที่ 3 (Phase 3) กระบวนการวิเคราะห์พารามิเตอร์กำหนดขอบเขตของธุรกิจ (BSP: Business Scoping Parameters)

1. BSP ที่เกี่ยวข้องกับกระบวนการทางธุรกิจในรูปแบบอิเล็กทรอนิกส์ของลายมือชื่อดิจิทัล
2. BSP ที่เกี่ยวข้องกับกฎหมายและกฎเกณฑ์กำกับกระบวนการทางธุรกิจ
3. BSP ที่เกี่ยวกับผู้สร้างลายมือชื่อดิจิทัล
4. BSP ที่มาจากแหล่งข้อมูลที่ต้องคำนึงถึงอื่นๆ นอกเหนือจาก 3 กลุ่มข้างต้น

ขั้นตอนที่ 3 (Phase 3) กระบวนการวิเคราะห์พารามิเตอร์กำหนดขอบเขตของธุรกิจ (BSP: Business Scoping Parameters)

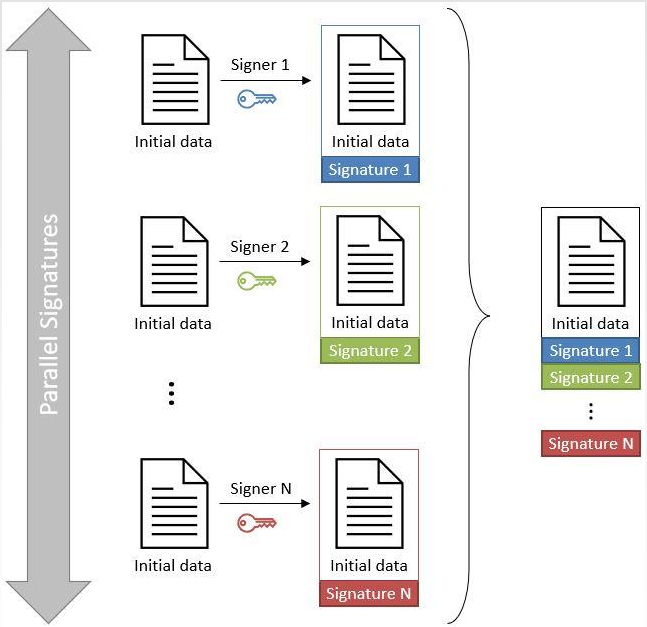
1. BSP ที่เกี่ยวข้องกับกระบวนการทางธุรกิจในรูปแบบอิเล็กทรอนิกส์ของลายมือชื่อดิจิทัล
2. BSP ที่เกี่ยวข้องกับกฎหมายและกฎเกณฑ์กำกับกระบวนการทางธุรกิจ
3. BSP ที่เกี่ยวกับผู้สร้างลายมือชื่อดิจิทัล
4. BSP ที่มาจากแหล่งข้อมูลที่ต้องคำนึงถึงอื่นๆ นอกเหนือจาก 3 กลุ่มข้างต้น

ขั้นตอนที่ 3 (Phase 3) กระบวนการวิเคราะห์พารามิเตอร์กำหนดขอบเขตของธุรกิจ (BSP: Business Scoping Parameters)

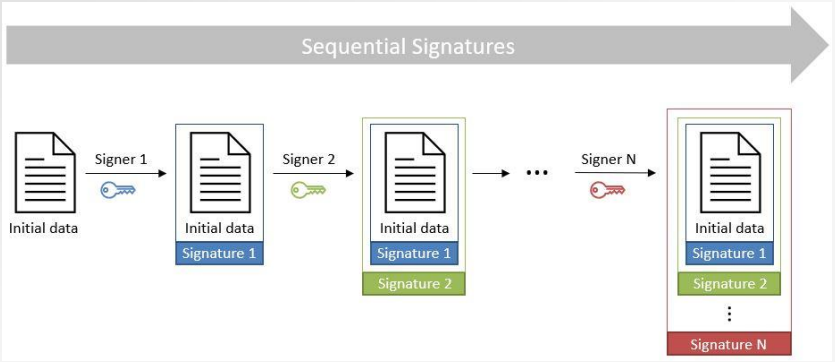
1. BSP ที่เกี่ยวข้องกับกระบวนการทางธุรกิจในรูปแบบอิเล็กทรอนิกส์ของลายมือชื่อดิจิทัล

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

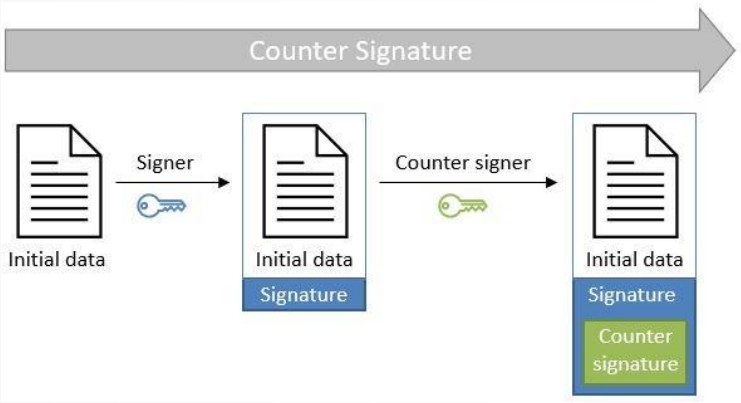
พารามิเตอร์ที่เกี่ยวข้องกับเวลาจะมีความสัมพันธ์กับการลงลายมือชื่อหรือไม่ และในกรณีที่มีการลงลายมือชื่อมากกว่าหนึ่งเจ้าของลายมือชื่อ พารามิเตอร์ที่เกี่ยวกับลำดับลายมือชื่อจะมีความสัมพันธ์กับการลงลายมือชื่อหรือไม่



การสร้างลายมือชื่อแบบขนาน (parallel signatures)



การสร้างลายมือชื่อแบบเป็นลำดับต่อกัน (serial signatures)



การสร้างลายมือชื่อแบบกำกับลายมือชื่อ (counter signatures)

ขั้นตอนที่ 3 (Phase 3) กระบวนการวิเคราะห์พารามิเตอร์กำหนดขอบเขตของธุรกิจ (BSP: Business Scoping Parameters)

1. BSP **ที่เกี่ยวข้องกับกระบวนการทางธุรกิจในรูปแบบอิเล็กทรอนิกส์ของลายมือชื่อดิจิทัล** *(ต่อ...)*

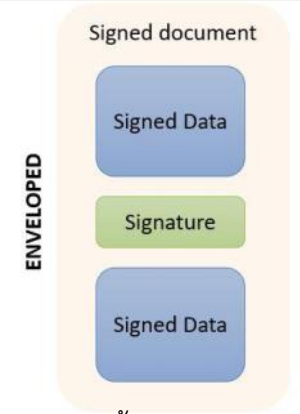
- **BSP (b): อ็อบเจกต์ข้อมูลที่ลงลายมือชื่อ (data object(s) to be signed)**

การระบุถึงขอบเขตของข้อมูลที่ลงลายมือชื่อ (data object to be signed) ว่า การลงลายมือชื่อจะครอบคลุมข้อมูลทั้งหมด หรือบางส่วนของข้อมูลที่ลงลายมือชื่อ ประเด็นนี้ใช้ในการพิจารณาถึงการเลือกรูปแบบลายมือชื่อ (digital signature format)

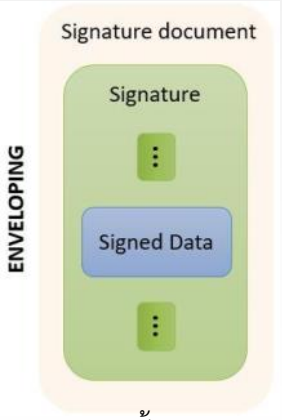
- **BSP (c): ความสัมพันธ์ระหว่างลายมือชื่อดิจิทัลกับอ็อบเจกต์ข้อมูลที่ถูกลงลายมือชื่อ**

ให้ความสำคัญต่อความสัมพันธ์ระหว่างลายมือชื่อดิจิทัลในแต่ละลายมือชื่อกับอ็อบเจกต์ข้อมูลในประเด็นดังต่อไปนี้

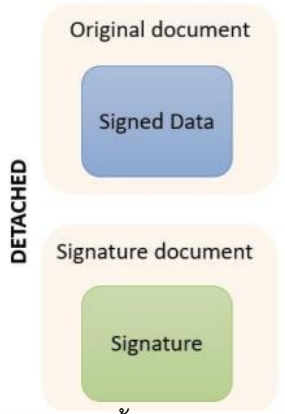
- การสร้างลายมือชื่อดิจิทัลต่ออ็อบเจกต์ข้อมูลในแต่ละรูปแบบจะมีวิธีการจัดการหรือจัดเตรียมอ็อบเจกต์ข้อมูลที่ลงลายมือชื่อ มีความสะดวกหรือยากง่ายที่แตกต่างกัน ประเด็นนี้จึงเป็นประเด็นที่ใช้ในการพิจารณาในการเลือกรูปแบบลายมือชื่อ
- การลงลายมือชื่อครั้งละหลายรายการ (bulk signature) ในบางรูปแบบลายมือชื่อจะมีกลไกสนับสนุนการลงลายมือชื่อในรูปแบบนี้ได้โดยสะดวก เช่น รูปแบบลายมือชื่อ XAdES
- ข้อแนะนำของตำแหน่งของข้อมูลที่ลงลายมือชื่อและข้อมูลลายมือชื่อ จะมี 3 แบบ ประกอบด้วย



ลายเซ็นและเนื้อหาอยู่ในไฟล์เดียวกัน
เช่น ใบรับรองแพทย์ในรูปแบบ PDF



ลายเซ็นครอบคลุมเนื้อหาเอกสารทั้งหมด เหมาะสำหรับเอกสารที่ต้องการความปลอดภัยสูง เช่น เอกสารทางกฎหมายที่ต้องลงนามทุกหน้า

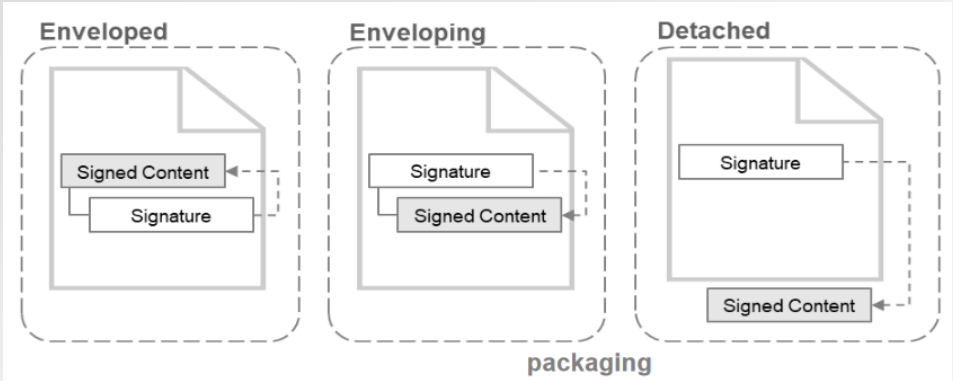


ลายเซ็นและเนื้อหาแยกออกจากกัน
เช่น ไฟล์ PDF ขนาดใหญ่, ไฟล์มัลติมีเดีย

ขั้นตอนที่ 3 (Phase 3) กระบวนการวิเคราะห์พารามิเตอร์กำหนดขอบเขตของธุรกิจ (BSP: Business Scoping Parameters)

1. BSP ที่เกี่ยวข้องกับกระบวนการทางธุรกิจในรูปแบบอิเล็กทรอนิกส์ของลายมือชื่อดิจิทัล *(ต่อ...)*

   - BSP (c): ความสัมพันธ์ระหว่างลายมือชื่อดิจิทัลกับอ็อบเจกต์ข้อมูลที่ถูกลงลายมือชื่อ



	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

ขั้นตอนที่ 3 (Phase 3) กระบวนการวิเคราะห์พารามิเตอร์กำหนดขอบเขตของธุรกิจ (BSP: Business Scoping Parameters)

1. BSP ที่เกี่ยวข้องกับกระบวนการทางธุรกิจในรูปแบบอิเล็กทรอนิกส์ของลายมือชื่อดิจิทัล *(ต่อ...)*

- **BSP (d) ข้อกำหนดเฉพาะกลุ่ม ในกรณีการประยุกต์ใช้ลายมือชื่อถูกนำไปใช้ภายใต้กลุ่มเฉพาะ**

  ผู้ประยุกต์ใช้มาตรฐานฯ จำเป็นต้องพิจารณาถึงข้อกำหนดถึงคุณสมบัติ รูปแบบ และกฎเกณฑ์ที่เกี่ยวข้องกับลายมือชื่อได้กำหนดไว้ เพื่อประกอบการพิจารณาเลือกใช้ข้อกำหนดของมาตรฐานฯ

- **BSP (e): ความรับผิดชอบในการตรวจสอบความถูกต้องลายมือชื่อดิจิทัล**

  - **คู่กรณีของลายมือชื่อ**
    โดยปกติการตรวจสอบความถูกต้องลายมือชื่อจะเป็นความรับผิดชอบของคู่กรณีของลายมือชื่อ แต่การสันนิษฐานว่าคู่กรณีของลายมือชื่อจะสามารถตรวจสอบความถูกต้องลายมือชื่อได้ อาจเป็นเรื่องที่ปฏิบัติไม่ได้จริง
  - **ผู้ให้บริการตรวจสอบความถูกต้องลายมือชื่อ**
    เป็นทางเลือกของการถ่ายโอนความรับผิดชอบในการตรวจสอบความถูกต้องลายมือชื่อ ซึ่งมีความซับซ้อนในเชิงเทคนิคและกระบวนการไปให้กับผู้ให้บริการที่ถูกกำกับหรือผ่านการรับรอง เพื่อให้แน่ใจว่าเป็นบริการตรวจสอบความถูกต้องลายมือชื่อดิจิทัลเป็นที่เชื่อถือได้
  - **การเพิ่มความน่าเชื่อถือให้กับลายมือชื่อดิจิทัล**
    เป็นกระบวนการที่เพิ่มข้อมูลเฉพาะ (เช่น ข้อมูลประทับเวลา ข้อมูลตรวจสอบความถูกต้อง และข้อมูลเกี่ยวกับการเก็บไว้เป็นหลักฐานในระยะยาว) เพิ่มลงในข้อมูลลายมือชื่อดิจิทัลเพื่อทำให้ลายมือชื่อดิจิทัลมีความทนทานต่อการแก้ไขเปลี่ยนแปลง หรือเป็นการเพิ่มช่วงระยะเวลาการใช้งานของลายมือชื่อดิจิทัลให้ยาวนานขึ้น

ขั้นตอนที่ 3 (Phase 3) กระบวนการวิเคราะห์พารามิเตอร์กำหนดขอบเขตของธุรกิจ (BSP: Business Scoping Parameters)

1. BSP ที่เกี่ยวข้องกับกระบวนการทางธุรกิจในรูปแบบอิเล็กทรอนิกส์ของลายมือชื่อดิจิทัล
2. **BSP ที่เกี่ยวข้องกับกฎหมายและกฎเกณฑ์กำกับกระบวนการทางธุรกิจ**
3. BSP ที่เกี่ยวกับผู้สร้างลายมือชื่อดิจิทัล
4. BSP ที่มาจากแหล่งข้อมูลที่ต้องคำนึงถึงอื่นๆ นอกเหนือจาก 3 กลุ่มข้างต้น

ขั้นตอนที่ 3 (Phase 3) กระบวนการวิเคราะห์พารามิเตอร์กำหนดขอบเขตของธุรกิจ (BSP: Business Scoping Parameters)

2. BSP ที่เกี่ยวข้องกับกฎหมายและกฎเกณฑ์กำกับกระบวนการทางธุรกิจ

- **BSP (f) ผลในทางกฎหมายของลายมือชื่อ**
  พารามิเตอร์ในด้านนี้จะมีผลต่อการกำหนดระดับความเข้มงวดของการยืนยันตัวตนของบุคคลที่สร้างลายมือชื่อดิจิทัล การกำหนดนโยบายและข้อกำหนดสำหรับผู้ให้บริการที่เชื่อถือได้ที่ให้บริการภายใต้ระดับความเข้มงวดที่กำหนด การกำหนดประเภทของอุปกรณ์ที่ใช้สร้างลายมือชื่อ

- **BSP (g) ความรับผิดชอบของเจ้าของลายมือชื่อ (Commitment)**
  ผู้ดำเนินการในการสร้างลายมือชื่อควรระบุถึงวัตถุประสงค์และความรับผิดชอบที่เกิดขึ้นเมื่อมีการลงลายมือชื่อในกระบวนการธุรกิจ ซึ่งการกำหนดรายละเอียดส่วนนี้ให้มีความชัดเจนจะทำให้การประยุกต์ใช้ลายมือชื่อดิจิทัลในกระบวนการทางธุรกิจไม่เกิดความคลุมเครือของวัตถุประสงค์ในการลงลายมือชื่อในรูปแบบดิจิทัล
  อาทิ เพื่อรับรองร่างเอกสาร, เพื่อยืนยันว่าได้รับข้อมูล, เพื่ออนุมัติในกระบวนการพิจารณาต่างๆ, เพื่อแสดงความเป็นผู้มีสิทธิ์ (authorship) หรือความรับผิดชอบในเอกสาร, เพื่อแสดงว่าเอกสารได้ผ่านการทบทวน, เพื่อแสดงความเป็นต้นฉบับของเอกสาร, เพื่อเป็นพยานต่อลายมือชื่อของผู้อื่นบนเอกสาร เป็นต้น

- **BSP (h) ระดับความเข้มงวดของเวลาที่ใช้อ้างอิงเป็นพยานหลักฐาน (Level of assurance of timing evidences)**
  ผู้ดำเนินการในการสร้างลายมือชื่อควรระบุถึงระดับความเข้มงวดที่ต้องการของเวลาที่ใช้อ้างอิงเป็นพยานหลักฐาน ข้อมูลเวลาที่อ้างขึ้นเอง (claimed information) จะแตกต่างจากข้อมูลเวลาที่เชื่อถือได้ (trusted time) ซึ่งเป็นข้อมูลเวลาที่ได้รับจากผู้ให้บริการประทับเวลาที่เชื่อถือได้

- **BSP (i) ระเบียบวิธีการการลงลายมือชื่อ แสดงถึงความรับผิดชอบที่เกิดขึ้นเมื่อมีการสร้างลายมือชื่อของเจ้าของลายมือชื่อ**
  วิธีการหรือการกระทำในการลงลายมือชื่อของเจ้าของลายมือชื่อ เพื่อให้เกิดความตระหนักถึงความรับผิดชอบที่เกิดขึ้นภายหลังกระบวนการลงลายมือชื่อเสร็จสิ้น ข้อกำหนดเหล่านี้จะเกี่ยวข้องกับการออกแบบส่วนการติดต่อหรือรูปแบบการติดต่อกับเจ้าของลายมือชื่อ อาทิ What You See Is What You Sign

- **BSP (j) การรักษาอายุของลายมือชื่อให้ยาวนานขึ้นและความทนทานต่อการเปลี่ยนแปลง**
  สถานการณ์ที่จะส่งผลกระทบต่อความน่าเชื่อถือของลายมือชื่อดิจิทัลซึ่งจำเป็นต้องมีกระบวนการรักษาอายุของลายมือชื่อให้ยาวนานขึ้น คือ เมื่อข้อมูลที่ใช้ในการตรวจสอบความถูกต้องลายมือชื่อดิจิทัล (ใบรับรอง) หมดอายุลงหรือไม่สามารถเข้าถึงหรือใช้งานได้ต่อไป หรือเมื่ออัลกอริทึมการเข้ารหัสลับไม่ปลอดภัยสำหรับการใช้งานต่อไป ผู้ดำเนินการในการสร้างลายมือชื่อจำเป็นต้องใช้ข้อมูลในส่วนนี้ดำเนินการเพื่อรักษาอายุของลายมือชื่อให้ยาวนานขึ้นได้ตามความต้องการ

ขั้นตอนที่ 3 (Phase 3) กระบวนการวิเคราะห์พารามิเตอร์กำหนดขอบเขตของธุรกิจ (BSP: Business Scoping Parameters)

2. **BSP ที่เกี่ยวข้องกับกฎหมายและกฎเกณฑ์กำกับกระบวนการทางธุรกิจ** *(ต่อ...)*

- **BSP (k) การจัดเก็บไว้เป็นหลักฐานในระยะยาว (Archival)**
  ผู้ดำเนินการในการสร้างลายมือชื่อควรพิจารณาถึงข้อกำหนดของกฎหมายหรือกฎเกณฑ์กำกับที่เกี่ยวข้อง เพื่อให้ข้อมูลที่จัดเก็บไว้เป็นหลักฐานในระยะยาวมีผลและชอบโดยกฎหมาย

ขั้นตอนที่ 3 (Phase 3) กระบวนการวิเคราะห์พารามิเตอร์กำหนดขอบเขตของธุรกิจ (BSP: Business Scoping Parameters)

1. BSP ที่เกี่ยวข้องกับกระบวนการทางธุรกิจในรูปแบบอิเล็กทรอนิกส์ของลายมือชื่อดิจิทัล
2. BSP ที่เกี่ยวข้องกับกฎหมายและกฎเกณฑ์กำกับกระบวนการทางธุรกิจ
3. **BSP ที่เกี่ยวกับผู้สร้างลายมือชื่อดิจิทัล**
4. BSP ที่มาจากแหล่งข้อมูลที่ต้องคำนึงถึงอื่นๆ นอกเหนือจาก 3 กลุ่มข้างต้น

ขั้นตอนที่ 3 (Phase 3) กระบวนการวิเคราะห์พารามิเตอร์กำหนดขอบเขตของธุรกิจ (BSP: Business Scoping Parameters)

3. BSP ที่เกี่ยวกับผู้สร้างลายมือชื่อดิจิทัล

- **BSP (l) ไอเดนทิตี (บทบาทและแอตทริบิวต์) ของเจ้าของลายมือชื่อ**

  ผู้ดำเนินการในการสร้างลายมือชื่อ ควรระบุประเภทของหลักฐานที่ใช้ในการพิสูจน์ตัวบุคคลของเจ้าของลายมือชื่อจากหน่วยงานที่เกี่ยวข้องที่ยอมรับได้ ซึ่งอาจประกอบด้วยหลักฐานว่าพนักงานหรือตัวแทนได้รับอนุญาตให้ทำธุรกรรมเกินมูลค่าที่ระบุ และ หลักฐานการมอบอำนาจให้ลงลายมือชื่อได้

- **BSP (m) ระดับของความเข้มงวดที่จำเป็นสำหรับการยืนยันตัวตนของเจ้าของลายมือชื่อ**

  ผู้ดำเนินการในการสร้างลายมือชื่อ ควรระบุระดับความเข้มงวดที่จำเป็นสำหรับการยืนยันตัวตนของเจ้าของลายมือชื่อในแต่ละลายมือชื่อที่จะสร้างภายในกระบวนการทางธุรกิจ เช่น เกณฑ์ความน่าเชื่อถือที่คาดหวังในการระบุตัวตนของเจ้าของลายมือชื่อ (เช่น ระดับคุณภาพของใบรับรอง) ข้อกำหนดในส่วนนี้จะไม่ส่งผลกระทบต่อเนื้อหาของลายมือชื่อ แต่การไม่ปฏิบัติตามข้อกำหนดนี้ อาจส่งผลกระทบต่อการถูกปฏิเสธผลทางกฎหมายของลายมือชื่อ เมื่อมีการตรวจสอบหรือข้อพิพาทเกิดขึ้น

- **BSP (n) อุปกรณ์สร้างลายมือชื่อ**

  ผู้ดำเนินการในการสร้างลายมือชื่อ ควรระบุข้อกำหนดเกี่ยวกับอุปกรณ์สร้างลายมือชื่อ (เช่น การควบคุมโดยเจ้าของลายมือชื่อโดยไม่อยู่ภายใต้การควบคุมของผู้อื่น) ที่จะใช้ในการสร้างลายมือชื่อภายในกระบวนการทางธุรกิจ เพื่อให้มั่นใจว่าจะปฏิบัติตามได้ การไม่ปฏิบัติตามข้อกำหนดนี้ อาจส่งผลกระทบต่อการถูกปฏิเสธผลทางกฎหมายของลายมือชื่อ เมื่อมีการตรวจสอบหรือข้อพิพาทเกิดขึ้น

ขั้นตอนที่ 3 (Phase 3) กระบวนการวิเคราะห์พารามิเตอร์กำหนดขอบเขตของธุรกิจ (BSP: Business Scoping Parameters)

1. BSP ที่เกี่ยวข้องกับกระบวนการทางธุรกิจในรูปแบบอิเล็กทรอนิกส์ของลายมือชื่อดิจิทัล
2. BSP ที่เกี่ยวข้องกับกฎหมายและกฎเกณฑ์กำกับกระบวนการทางธุรกิจ
3. BSP ที่เกี่ยวกับผู้สร้างลายมือชื่อดิจิทัล
4. **BSP ที่มาจากแหล่งข้อมูลที่ต้องคำนึงถึงอื่นๆ นอกเหนือจาก 3 กลุ่มข้างต้น**

ขั้นตอนที่ 3 (Phase 3) กระบวนการวิเคราะห์พารามิเตอร์กำหนดขอบเขตของธุรกิจ (BSP: Business Scoping Parameters)

4. BSP **ที่มาจากแหล่งข้อมูลที่ต้องคำนึงถึงอื่นๆ นอกเหนือจาก 3 กลุ่มข้างต้น**

- **BSP (o) ข้อมูลอื่นที่ใส่รวมไว้กับลายมือชื่อ**

  ข้อมูลคุณลักษณะลายมือชื่ออื่นๆ ที่เกี่ยวข้อง หากพิจารณาว่าจำเป็น เช่น สถานที่ที่สร้างลายมือชื่อ เวลาที่สร้างลายมือชื่อจากเจ้าของลายมือชื่อโทเค็นการประทับเวลาจากผู้ให้บริการ และรูปแบบของอ็อบเจกต์ที่ลงลายมือชื่อ (signed data object) ในรูปแบบที่มนุษย์สามารถอ่านและเข้าใจได้ และไม่มีความคลุมเครือ

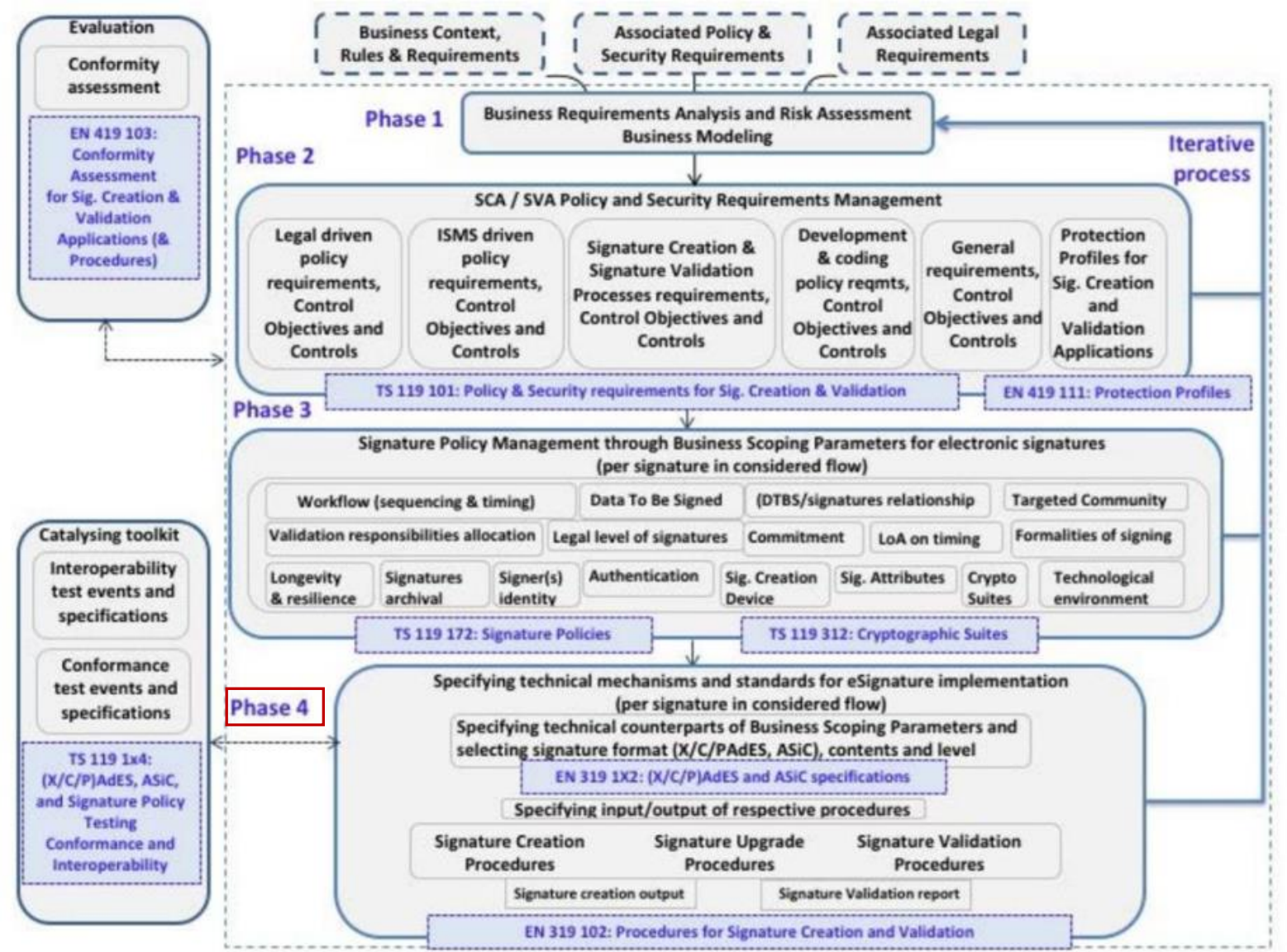
- **BSP (p) ชุดการเข้ารหัสลับ**

  ผู้ดำเนินการในการสร้างลายมือชื่อ ควรระบุข้อกำหนดเกี่ยวกับความแข็งแรงและพร้อมใช้ของชุดการเข้ารหัสที่ใช้ในการสร้าง (generate) หรือเพิ่มความน่าเชื่อถือ (augment) ให้กับลายมือชื่อดิจิทัลในกระบวนการทางธุรกิจที่เกี่ยวข้อง

- **BSP (q) สภาพแวดล้อมทางเทคนิค**

  ผู้ดำเนินการในการสร้างลายมือชื่อ ควรให้ความสำคัญกับสภาพแวดล้อมทางเทคโนโลยีที่อ็อบเจกต์ข้อมูลที่ลงลายมือชื่อและลายมือชื่อได้มีการบริหารจัดการอย่างเหมาะสม

กระบวนการประยุกต์ใช้มาตรฐานในการสร้างและตรวจสอบความถูกต้องของลายมือชื่อ (อ้างอิง ETSI TR 119 100 Guidance on the use of standards for signature creation and validation)



ขั้นตอนที่ 4 (Phase 4)

กระบวนการในการตัดสินใจวิธีการทางเทคนิค

เพื่อตอบสนองต่อพารามิเตอร์กำหนดขอบเขตของธุรกิจ (business scoping parameters) ซึ่งเป็นผลลัพธ์ของการวิเคราะห์ความต้องการทางธุรกิจใน 3 ขั้นตอนแรก ข้อแนะนำในขั้นตอนนี้ จะช่วยให้ผู้ดำเนินการในการสร้างลายมือชื่อ (implementer) สามารถตัดสินในประเด็นต่างๆ ที่เกี่ยวข้องกับการเลือกมาตรฐานและกลไกทางเทคนิคที่เหมาะสม ประกอบด้วย

- มาตรฐานที่กำหนดรูปแบบ (formats) เนื้อความ (contents) และระดับ/ประเภทของลายมือชื่อดิจิทัล (levels of signature)

- ขั้นตอนปฏิบัติในเชิงเทคนิคในการสร้าง (generating) การเพิ่มความน่าเชื่อถือ (augmenting) และการตรวจสอบความถูกต้อง (validating) ให้กับลายมือชื่อดิจิทัล

- โปรไฟล์การป้องกัน (protection profiles) เป็นข้อกำหนดเทคนิคในด้านการรักษาความมั่นคงปลอดภัยสำหรับอุปกรณ์สร้างลายมือชื่อดิจิทัล แอปพลิเคชันตามแบบแสดงการทำงาน (functional model) ที่ต้องพัฒนาให้สอดคล้อง

ขั้นตอนที่ 4 (Phase 4) กระบวนการในการตัดสินใจวิธีการทางเทคนิค

1. มาตรฐานที่กำหนดรูปแบบ (formats) เนื้อความ (contents) และ ระดับ/ประเภทของลายมือชื่อดิจิทัล (levels of signature)

2. ขั้นตอนปฏิบัติในเชิงเทคนิคในการสร้าง (generating) การเพิ่มความน่าเชื่อถือ (augmenting) และการตรวจสอบความถูกต้อง (validating) ให้กับลายมือชื่อดิจิทัล

3. โปรไฟล์การป้องกัน (protection profiles) ของแอปพลิเคชันของการสร้าง และการตรวจสอบความถูกต้องลายมือชื่อดิจิทัล

ขั้นตอนที่ 4 (Phase 4) กระบวนการในการตัดสินใจวิธีการทางเทคนิค

1. มาตรฐานที่กำหนดรูปแบบ (formats) เนื้อความ (contents) และ ระดับ/ประเภทของลายมือชื่อดิจิทัล (levels of signature)

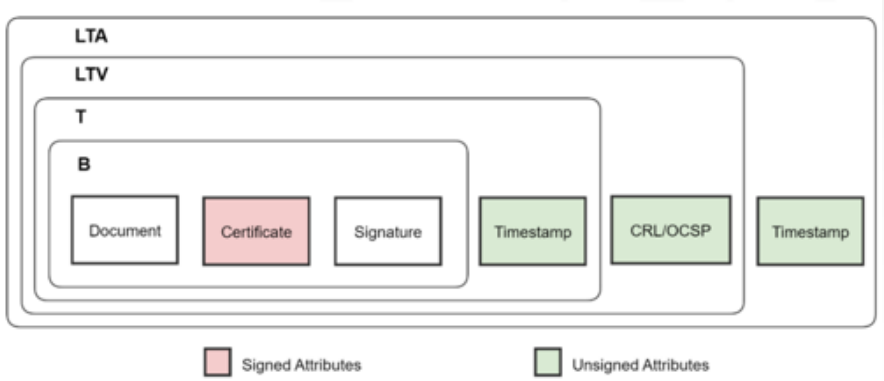
2. ขั้นตอนปฏิบัติในเชิงเทคนิคในการสร้าง (generating) การเพิ่มความน่าเชื่อถือ (augmenting) และการตรวจสอบความถูกต้อง (validating) ให้กับลายมือชื่อดิจิทัล

3. โปรไฟล์การป้องกัน (protection profiles) ของแอปพลิเคชันของการสร้าง และการตรวจสอบความถูกต้องลายมือชื่อดิจิทัล

ขั้นตอนที่ 4 (Phase 4) กระบวนการในการตัดสินใจวิธีการทางเทคนิค

1. **มาตรฐานที่กำหนดรูปแบบ (formats) เนื้อความ (contents) และ ระดับ/ประเภทของลายมือชื่อดิจิทัล (levels of signature)**

- **มาตรฐานที่กำหนดรูปแบบของลายมือชื่อดิจิทัล**
  - ASN.1: CAdES (ETSI EN 319 122-1 และ ETSI EN 319 122-2) มีโครงสร้างอ้างอิงมาตรฐาน CMS IETF RFC 5652
  - XML: XAdES (ETSI EN 319 132-1 และ ETSI EN 319 132-2) มีโครงสร้างอ้างอิง W3C XML signatures
  - PDF: PAdES (ETSI EN 319 142-1 และ ETSI EN 319 142-2) มีโครงสร้างอ้างอิง PDF signatures
  - ASiC: มาตรฐานรูปแบบลายมือชื่อดิจิทัลในรูปแบบโครงสร้างข้อมูลแบบคอนเทนเนอร์ที่สามารถใส่อ็อบเจกต์ข้อมูลได้หลายรายการ และสามารถใส่ลายมือชื่อดิจิทัลที่เลือกลงลายมือชื่อกับอ็อบเจกต์ข้อมูลได้ (ETSI EN 319 162-1 และ ETSI EN 319 162-2])
- **มาตรฐานประเภทของลายมือชื่อดิจิทัล (signature class)**
  - ระดับ B-B basic signature
  - ระดับ B-T signature with time
  - ระดับ B-LT signature with long-term validation material
  - ระดับ B-LTA signature with long-term availability and integrity of validation material



ขั้นตอนที่ 4 (Phase 4) กระบวนการในการตัดสินใจวิธีการทางเทคนิค

1. มาตรฐานที่กำหนดรูปแบบ (formats) เนื้อความ (contents) และ ระดับ/ประเภทของลายมือชื่อดิจิทัล (levels of signature)

2. **ขั้นตอนปฏิบัติในเชิงเทคนิคในการสร้าง (generating) การเพิ่มความน่าเชื่อถือ (augmenting) และการตรวจสอบความถูกต้อง (validating) ให้กับลายมือชื่อดิจิทัล**

3. โปรไฟล์การป้องกัน (protection profiles) ของแอปพลิเคชันของการสร้าง และการตรวจสอบความถูกต้องลายมือชื่อดิจิทัล

ขั้นตอนที่ 4 (Phase 4) กระบวนการในการตัดสินใจวิธีการทางเทคนิค

2. ขั้นตอนปฏิบัติในเชิงเทคนิคในการสร้าง (generating) การเพิ่มความน่าเชื่อถือ (augmenting) และการตรวจสอบความถูกต้อง (validating) ให้กับลายมือชื่อดิจิทัล

- มาตรฐาน ETSI EN 319 102-1 กำหนดขั้นตอนกระบวนการสร้าง และเพิ่มความน่าเชื่อถือให้กับลายมือชื่อดิจิทัลในกระบวนการทั่วไปโดยไม่ขึ้นกับรูปแบบลายมือชื่อรูปแบบใดรูปแบบหนึ่ง การสร้างลายมือชื่อดิจิทัลภายใต้ชุดมาตรฐานนี้ เป็นการสร้างลายมือชื่อดิจิทัลด้วยการเข้ารหัสลับด้วยเทคโนโลยีกุญแจสาธารณะ และมีใบรับรองกุญแจสาธารณะเป็นส่วนประกอบในการสร้างลายมือชื่อ และฟังก์ชันที่เกี่ยวข้องเมื่อสร้างและเพิ่มความน่าเชื่อถือให้กับลายมือชื่อ ยังได้กำหนดกระบวนการสร้างที่เกี่ยวข้องกับการสร้างลายมือชื่อดิจิทัลในแต่ประเภท/ระดับ (B-B, B-T, B-LT, B-LTA) เพื่อรองรับการขยายอายุการใช้งานของลายมือชื่อดิจิทัลให้ยาวนานขึ้น ในส่วนของนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยของแอปพลิเคชันที่เกี่ยวข้องกับการสร้างลายมือชื่อดิจิทัล ถูกกำหนดไว้ในมาตรฐาน ETSI TS 119 101 มาตรฐานที่กำหนดรูปแบบของลายมือชื่อดิจิทัล
- กระบวนการตรวจสอบความถูกต้องลายมือชื่อดิจิทัล ซึ่งจะมีแอปพลิเคชันตรวจสอบความถูกต้องลายมือชื่อ (SVA) เป็นองค์ประกอบหลัก

ขั้นตอนที่ 4 (Phase 4) กระบวนการในการตัดสินใจวิธีการทางเทคนิค

1. มาตรฐานที่กำหนดรูปแบบ (formats) เนื้อความ (contents) และ ระดับ/ประเภทของลายมือชื่อดิจิทัล (levels of signature)

2. ขั้นตอนปฏิบัติในเชิงเทคนิคในการสร้าง (generating) การเพิ่มความน่าเชื่อถือ (augmenting) และการตรวจสอบความถูกต้อง (validating) ให้กับลายมือชื่อดิจิทัล

3. **โปรไฟล์การป้องกัน (protection profiles) ของแอปพลิเคชันของการสร้าง และการตรวจสอบความถูกต้องลายมือชื่อดิจิทัล**

ขั้นตอนที่ 4 (Phase 4) กระบวนการในการตัดสินใจวิธีการทางเทคนิค

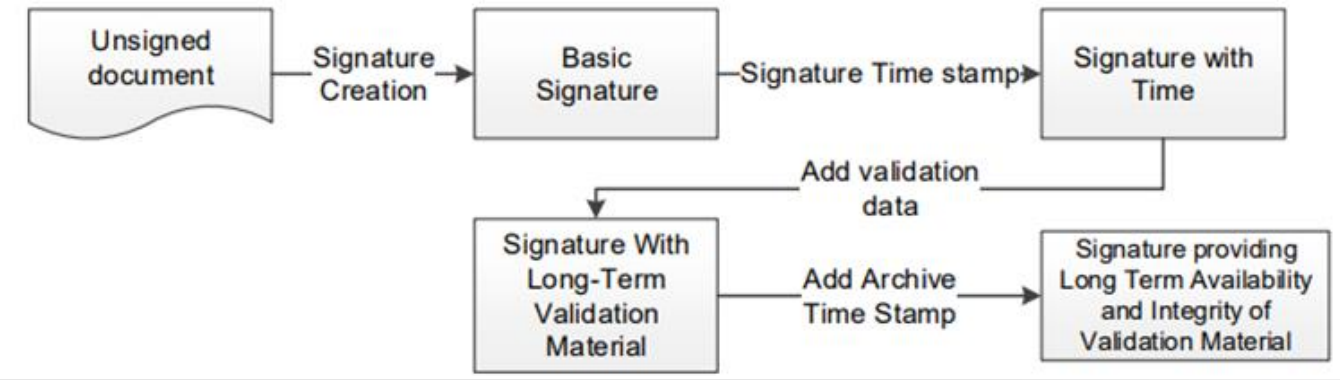
3. โปรไฟล์การป้องกัน (protection profiles) ของแอปพลิเคชันของการสร้าง และการตรวจสอบความถูกต้องลายมือชื่อดิจิทัล

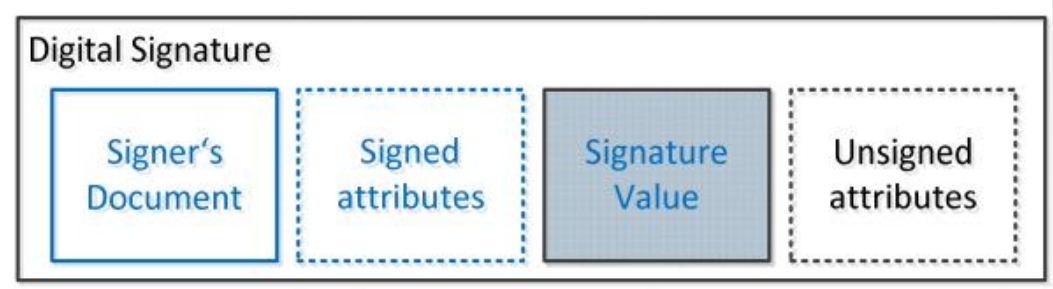
โปรไฟล์การป้องกัน (protection profiles) เป็นข้อกำหนดเทคนิคในด้านการรักษาความมั่นคงปลอดภัยสำหรับอุปกรณ์สร้างลายมือชื่อดิจิทัล

หัวข้อการสัมมนา

- กฎหมายไทยและกฎหมายต่างประเทศ ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล
- การวิเคราะห์พารามิเตอร์ทางธุรกิจ (BSP: Business Scoping Parameter) เพื่อเลือกใช้มาตรฐานทางเทคนิคที่เหมาะสมกับลายมือชื่อดิจิทัล
- ประเภทของลายมือชื่อ (signature class) และระดับความน่าเชื่อถือ
- แบบจำลองส่วนประกอบพื้นฐานและกรอบกระบวนทำงาน (building blocks and framework) ในการสร้าง (creation) การเพิ่มความน่าเชื่อถือ (augmentation) และการตรวจสอบความถูกต้อง (validation) ของลายมือชื่อดิจิทัล

วงจรชีวิตของลายมือชื่อ และการเพิ่มความน่าเชื่อถือ กับประเภทของลายมือชื่อ (signature class)



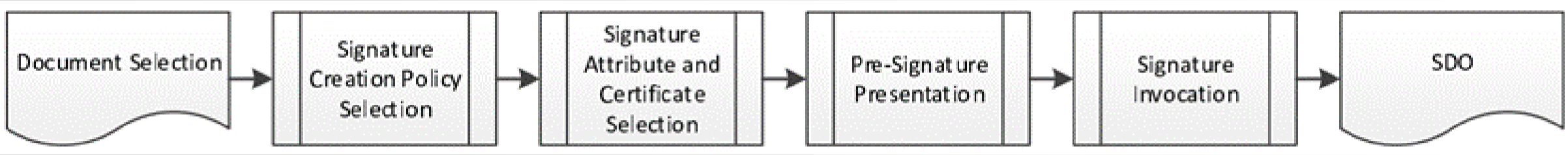


หมายเหตุ การเพิ่มความน่าเชื่อถือให้กับลายมือชื่อ หมายถึง การเพิ่มข้อมูลแอตทริบิวต์ที่ไม่ถูกลงลายมือชื่อ

- **ลายมือชื่อพื้นฐาน (basic signature)**
  ลายมือชื่อที่สามารถตรวจสอบความถูกต้องของลายมือชื่อได้ ตราบเท่าที่ใบรับรองยังไม่หมดอายุ หรือไม่ถูกเพิกถอน (B-B)
- **ลายมือชื่อที่มีข้อมูลเวลา (signature with time)**
  ลายมือชื่อที่สามารถพิสูจน์ได้ว่าคงอยู่ ณ เวลาที่กำหนด (B-T)
- **ลายมือชื่อที่มีข้อมูลตรวจสอบความถูกต้องในระยะยาว (signature with long-term validation material)**
  ลายมือชื่อที่ข้อมูลตรวจสอบความถูกต้องลายมือชื่อมีความพร้อมใช้ในระยะยาว ด้วยการรวมข้อมูลที่จำเป็นหรือข้อมูลอ้างอิงกับข้อมูลตรวจสอบความถูกต้องลายมือชื่อทั้งหมดเข้าไว้ด้วยกัน (B-LT)
- **ลายมือชื่อที่มีความพร้อมใช้ในระยะยาวและมีความสมบูรณ์ครบถ้วนของข้อมูลตรวจสอบความถูกต้องลายมือชื่อ (signature providing long term availability and integrity of validation material)**
  ลายมือชื่อที่ต้องการให้มีความพร้อมใช้งานในระยะยาว ซึ่งเกินระยะเวลาที่สามารถใช้งานได้ เช่น เมื่อพบความไม่แข็งแรงเพียงพอของอัลกอริทึมที่ใช้งาน หรือ เมื่อข้อมูลตรวจสอบความถูกต้องลายมือชื่อหมดอายุการใช้งาน (B-LTA)

Ref: ETSI EN 319 102-1 Security requirements for signature creation applications and signature validation applications

กระบวนการสร้างลายมือชื่อพื้นฐาน (creation of the basic signature (B-B))



1. การเลือกเอกสารที่จะลงลายมือชื่อ (selection of documents to sign)
   - อาจกำหนดให้ลงลายมือชื่อเพียงบางส่วนในเอกสารก็ได้
   - ควรตรวจความถูกต้องของลายมือชื่อ หากมีลายมือชื่อในเอกสารที่เลือกก่อนการลงนาม
2. การเลือกแอตทริบิวต์ลายเซ็นและพารามิเตอร์ (signature attribute and parameters selection)
   ข้อมูลที่ระบุตัวตนในใบรับรองต้องรวมอยู่ในข้อมูลที่จะลงลายมือชื่อในส่วน signed หรือ unsigned attributes ก็ได้
3. การแสดงเอกสารก่อนลงลายมือชื่อ (pre-signature presentation)
   แอพพลิเคชั่นต้องนำเสนอเอกสารที่จะลงลายมือชื่อ หรือเปิดให้เจ้าของลายมือชื่อสามารถทบทวน (inspect) เอกสารที่จะลงลายมือชื่อได้ และนำเสนอผลการตรวจสอบความถูกต้องของลายมือชื่อที่มีอยู่ในเอกสารก่อนลงลายมือชื่อ
4. การเรียกสร้างลายมือชื่อ (signature invocation)
   การเรียกสร้างลายมือชื่อต้องได้รับความยินยอมจากเจ้าของลายมือชื่อก่อนการลงลายมือชื่อ แอพพลิเคชั่นต้องมี pre-signature presentation แจ้งให้ทราบถึง commitment และได้รับความยินยอม
5. การลงลายมือชื่อ (signing)
   ต้องตรวจสอบความถูกต้องของใบรับรอง และตรวจสอบความถูกต้องของลายมือชื่อที่สร้างกับใบรับรอง
6. การยืนยันตัวตนเจ้าของลายมือชื่อ (singer authentication)
   กำหนดให้เจ้าของลายมือชื่อต้องผ่านการยืนยันตัวตนเสียก่อน
7. การสร้างอ็อบเจกต์ข้อมูลที่ลงลายมือชื่อ (signed data object หรือ SDO)
   ต้องสร้าง SDO จากค่าลายมือชื่อจาก SCDev และตามรูปแบบที่กำหนดไว้ พร้อมส่งผลลัพธ์ของการสร้างลายมือชื่อและสถานภาพให้กับแอพพลิเคชั่น

กระบวนการสร้างลายมือชื่อพื้นฐาน (creation of the basic signature (B-B))

Table 1: Inputs to the Basic Signature Creation process

Input	Requirement
Signer's Document or Signer's Document Representation	Mandatory
Signing Certificate	Mandatory
Other Signature Attributes	Optional
Signature Creation Policy	Optional
NOTE: A signature can also contain the time when the signature has been created. It is assumed that the current time is accurately available to the SCA. It is not listed as an input to avoid giving the impression that this time value can be selected at will.	

Figure 6: Basic Signature

กระบวนการสร้างลายมือชื่อที่มีข้อมูลเวลา (creation of signature with time (B-T))

Table 2: Inputs to the creation process for Signatures with Time

Input	Requirement
Basic Signature	Mandatory
Signature Augmentation Policy	Optional

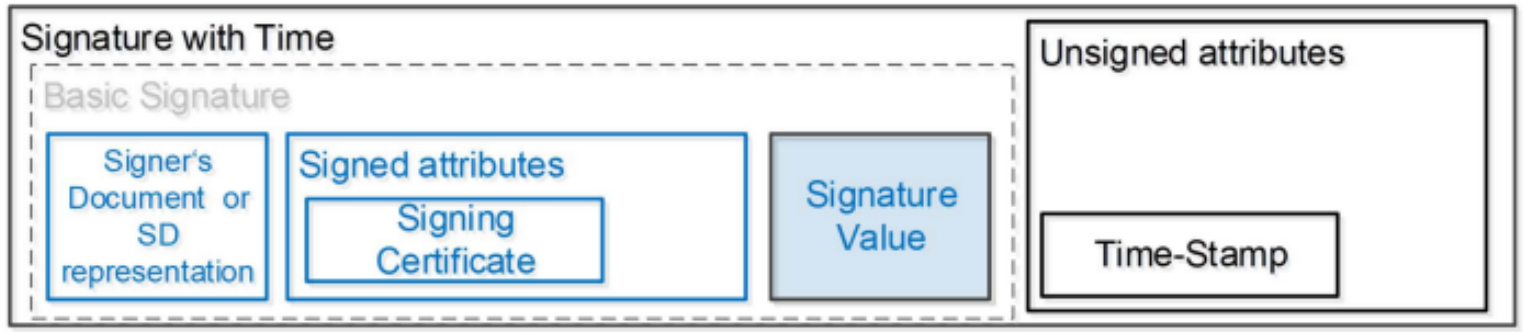


Figure 7: Signature with Time

กระบวนการสร้างลายมือชื่อที่มีข้อมูลตรวจสอบความถูกต้องในระยะยาว (creation of signature with long-term validation material (B-LT))

Table 3: Inputs to the creation process for Signatures with Long Term Validation Material

Input	Requirement
Signature with Time	Mandatory
Signature Augmentation Policy	Optional

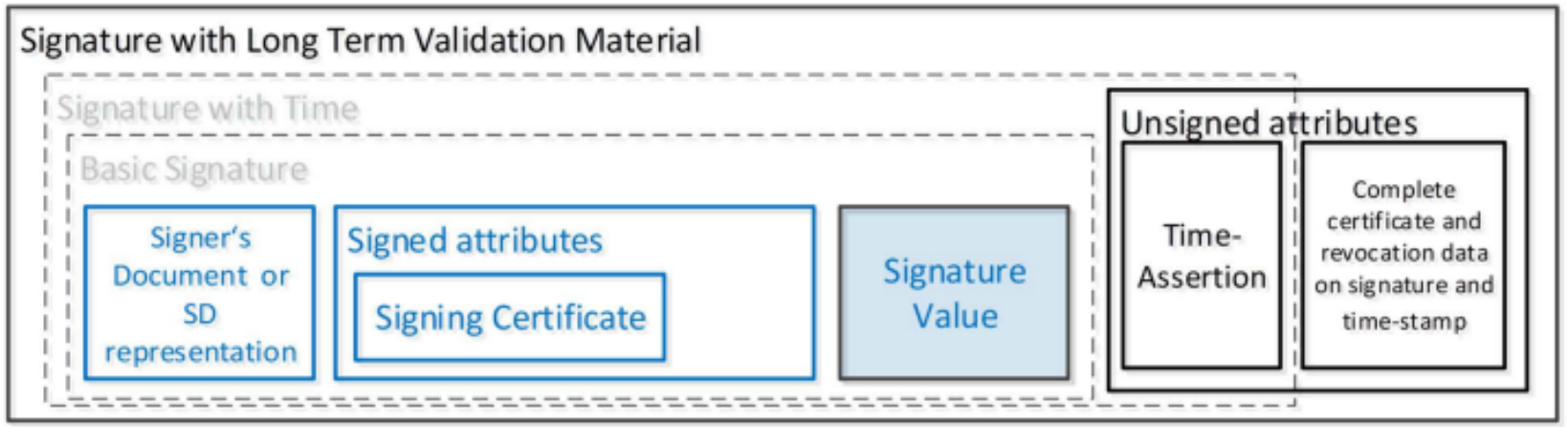


Figure 8: Signature with Long Term Validation Material

กระบวนการสร้างลายมือชื่อที่มีความพร้อมใช้ในระยะยาว และมีความสมบูรณ์ครบถ้วนของข้อมูลตรวจสอบความถูกต้องลายมือชื่อ (signature providing long term availability and integrity of validation material (B-LTA))

Table 4: Inputs to the creation process for Signatures providing Long Term Availability and Integrity of Validation Material

Input	Requirement
Signature with Long Term Validation Material or Signature providing Long Term Availability and Integrity of Validation Material	Mandatory
Signature Augmentation Policy	Optional

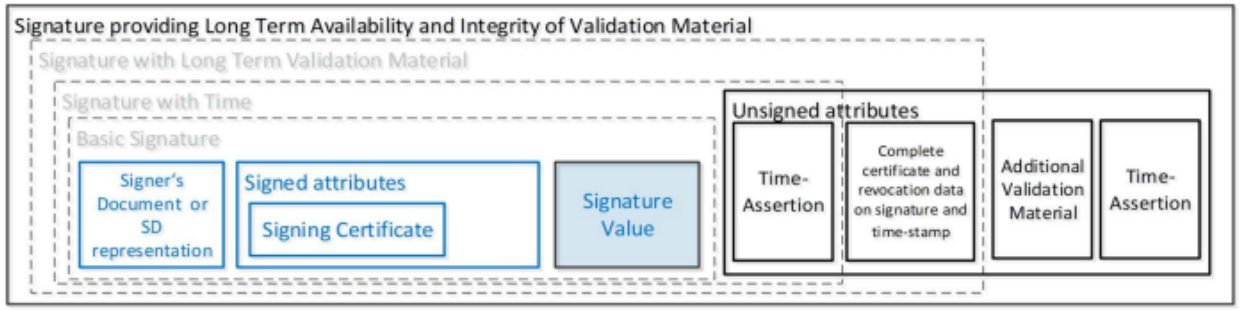


Figure 9: Signature providing Long Term Availability and Integrity of Validation Material

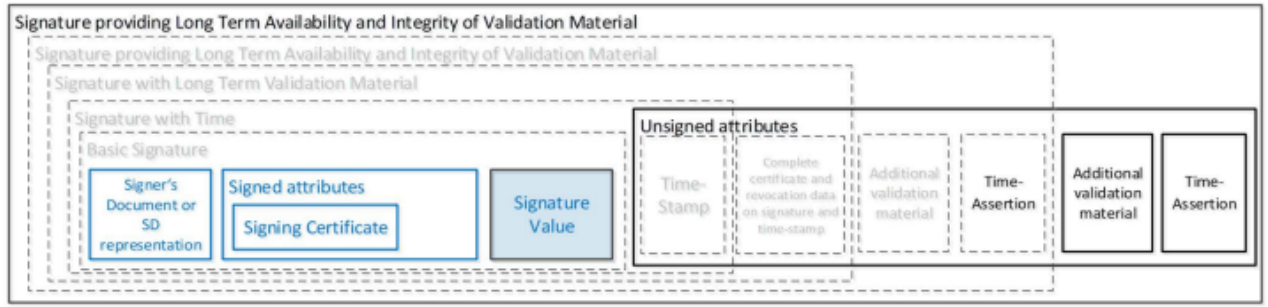
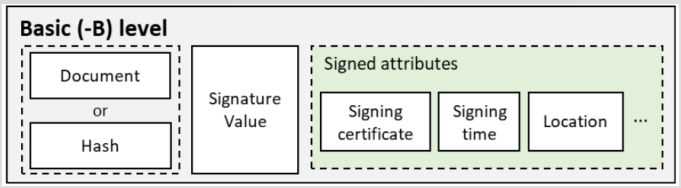
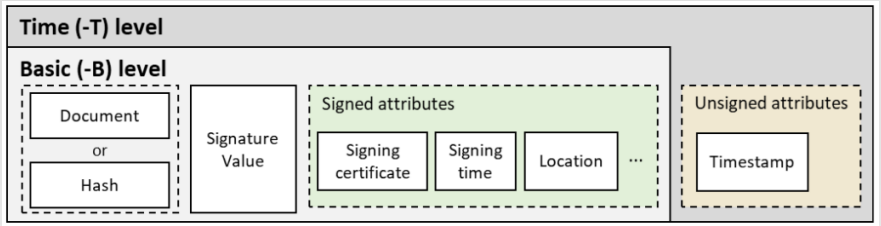
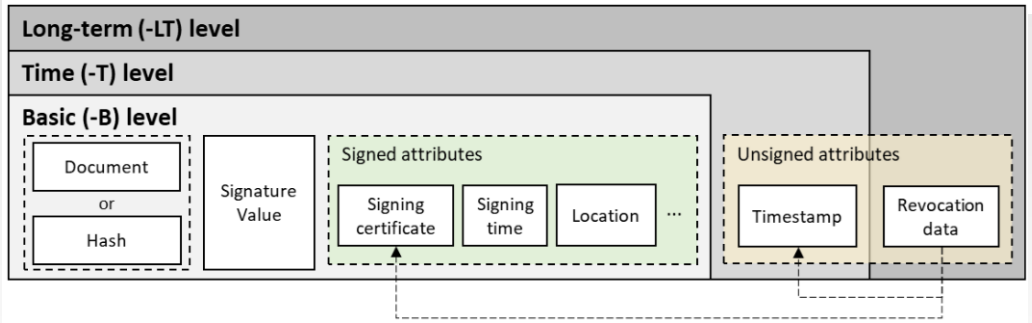


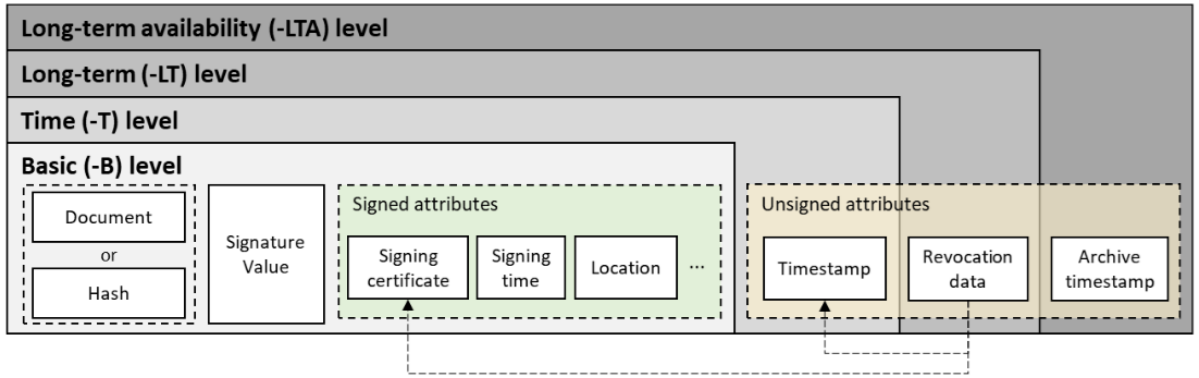
Figure 10: Signature providing Long Term Availability and Integrity of Validation Material after repetition

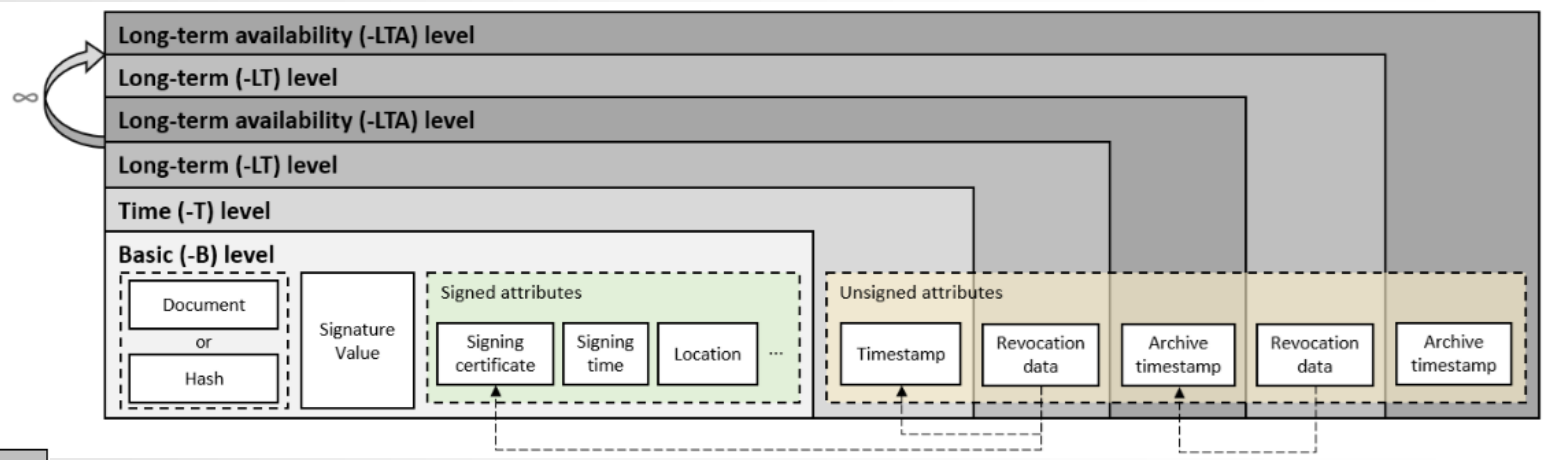
สรุปกระบวนการสร้างลายมือชื่อ B-B / B-T / B-LT / B-LTA







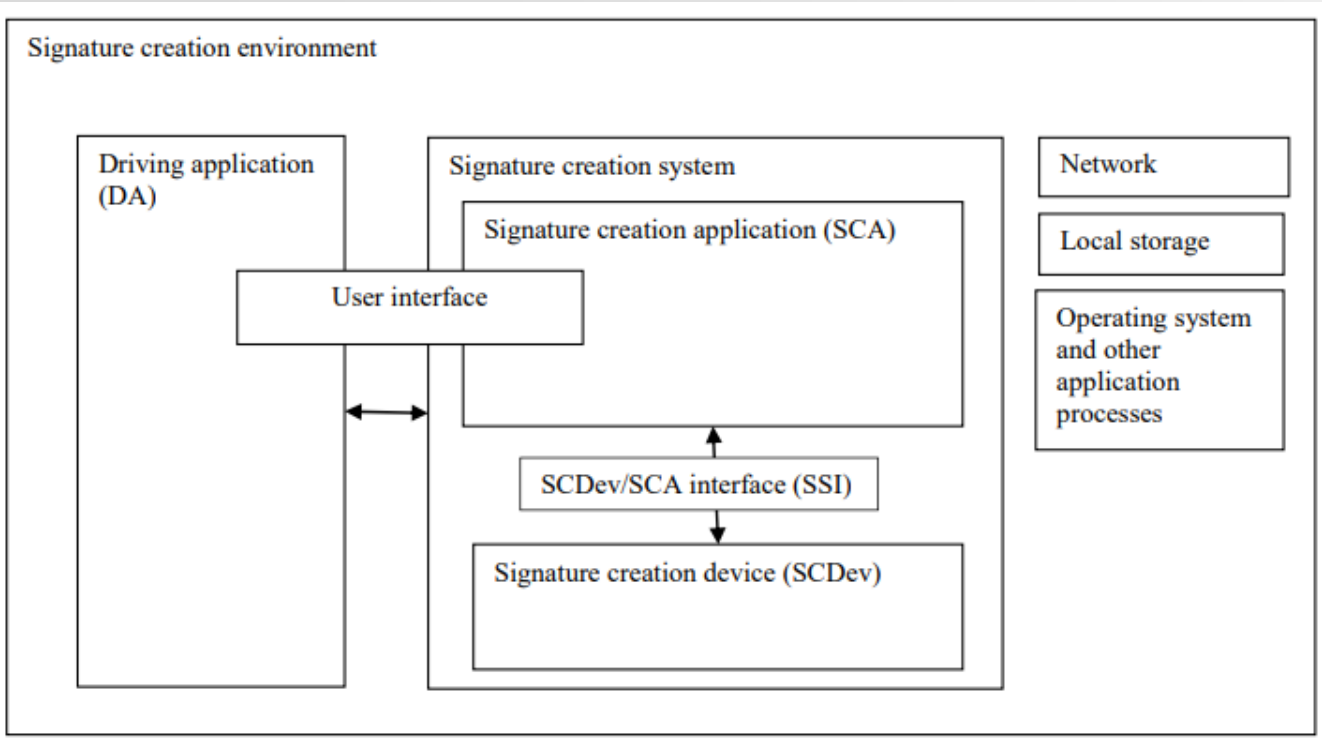




หัวข้อการสัมมนา

- กฎหมายไทยและกฎหมายต่างประเทศ ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล
- การวิเคราะห์พารามิเตอร์ทางธุรกิจ (BSP: Business Scoping Parameter) เพื่อเลือกใช้มาตรฐานทางเทคนิคที่เหมาะสมกับลายมือชื่อดิจิทัล
- ประเภทของลายมือชื่อ (signature class) และระดับความน่าเชื่อถือ
- แบบจำลองส่วนประกอบพื้นฐานและกรอบกระบวนทำงาน (building blocks and framework) ในการสร้าง (creation) การเพิ่มความน่าเชื่อถือ (augmentation) และการตรวจสอบความถูกต้อง (validation) ของลายมือชื่อดิจิทัล

ส่วนประกอบ (building blocks) ของแบบแสดงการทำงานของระบบการสร้างลายมือชื่อ



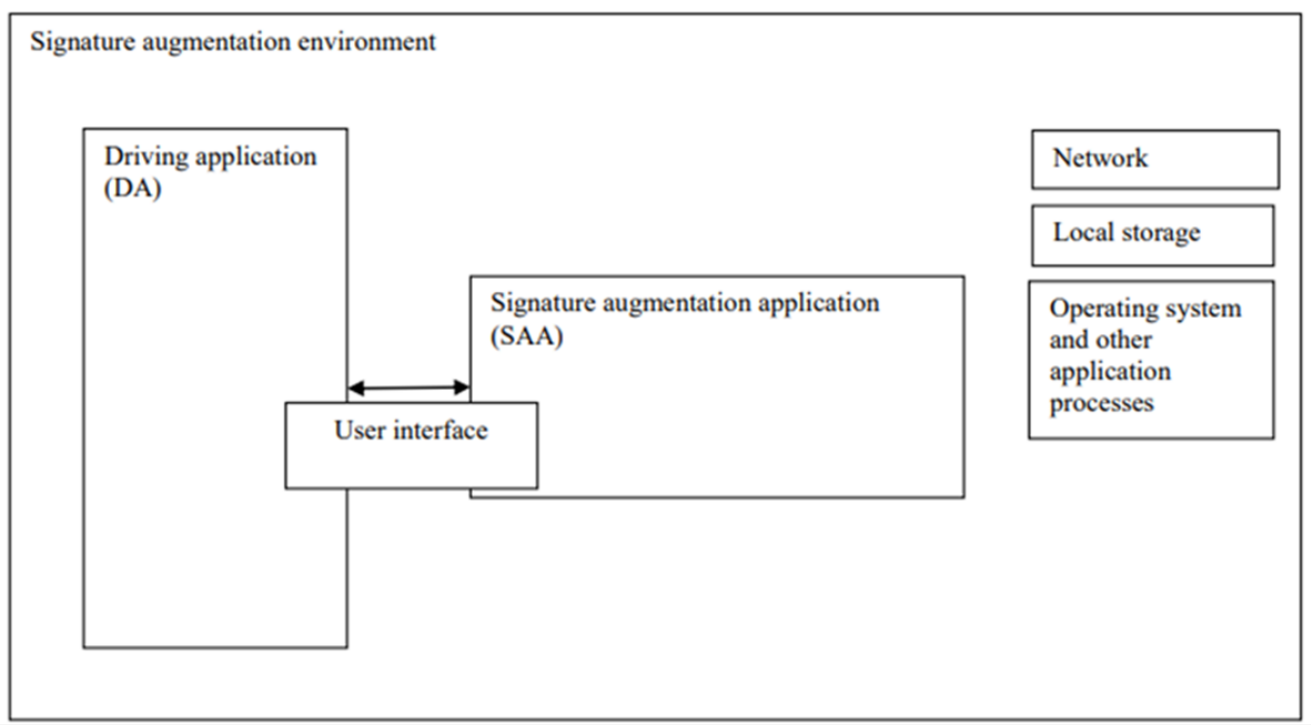
- ส่วนประกอบ (building blocks) ของแบบแสดงการทำงานในการสร้างลายมือชื่อทั้งหมดจะอยู่ในขอบเขตของการสร้างลายมือชื่อดิจิทัล ซึ่งถูกเรียกว่า สภาพแวดล้อมการสร้างลายมือชื่อ (signature creation environment) ซึ่งประกอบด้วย แอปพลิเคชันขับ (driving application หรือ DA), ระบบสร้างลายมือชื่อ (signature creation system) และระบบโครงสร้างพื้นฐานสารสนเทศที่สนับสนุนการทำงานของการสร้างลายมือชื่อ เช่น ระบบเครือข่าย ระบบการจัดเก็บข้อมูล และระบบปฏิบัติการและแอปพลิเคชันสารสนเทศต่าง ๆ

- ส่วนติดต่อผู้ใช้สามารถเป็นส่วนหนึ่งของแอปพลิเคชันขับ DA (บางส่วน) และ/หรือ (บางส่วน) ของ แอปพลิเคชันสร้างลายมือชื่อ (SCA) ก็ได้

- ส่วนสื่อสารข้อมูลระหว่าง แอปพลิเคชันสร้างลายมือชื่อ (SCA) กับ อุปกรณ์สร้างลายมือชื่อ (SCDev) เรียกว่า SCA and SCDev Interface หรือ SSI

Ref: ETSI TS 119 101 Security requirements for signature creation applications and signature validation applications

ส่วนประกอบ (building blocks) ของแบบแสดงการทำงานของการเพิ่มความน่าเชื่อถือให้กับลายมือชื่อ



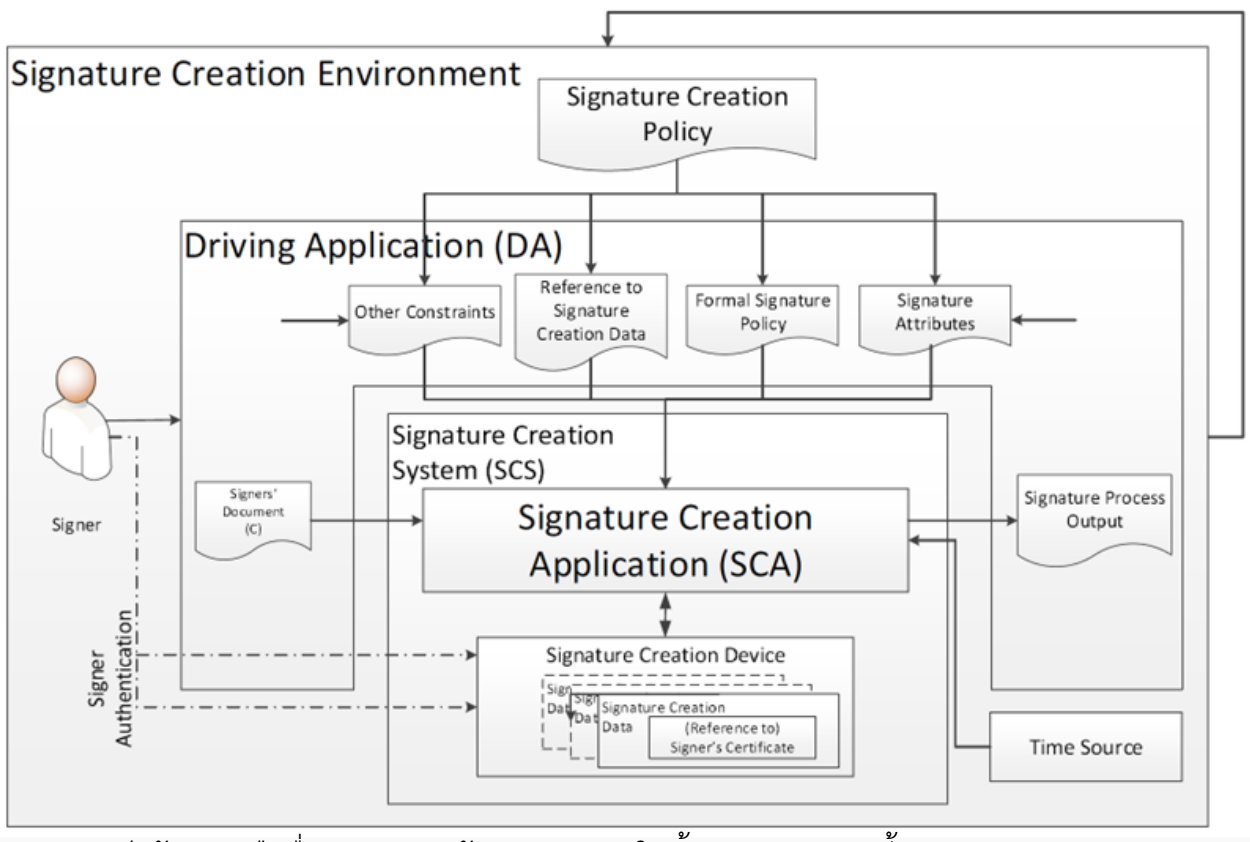
- สภาพแวดล้อมการเพิ่มความน่าเชื่อถือให้กับลายมือชื่อ (signature augmentation environment) ซึ่งประกอบด้วย แอปพลิเคชันขับ (driving application หรือ DA) แอปพลิเคชันเพิ่มความน่าเชื่อถือให้กับลายมือชื่อ (signature augmentation application หรือ SAA) และระบบโครงสร้างพื้นฐานสารสนเทศที่สนับสนุนการทำงานของการสร้างลายมือชื่อ เช่น ระบบเครือข่าย ระบบการจัดเก็บข้อมูล และระบบปฏิบัติการและแอปพลิเคชันสารสนเทศต่าง ๆ

- ตามข้อกำหนดในมาตรฐาน ETSI EN 319 102-1 การเพิ่มความน่าเชื่อถือให้กับลายมือชื่อดิจิทัล (augmentation) ถือเป็นส่วนหนึ่งของแอปพลิเคชันสร้างลายมือชื่อ (SCA)

- แอปพลิเคชันเพิ่มความน่าเชื่อถือให้กับลายมือชื่อ (SAA) สามารถเป็นส่วนหนึ่งของแอปพลิเคชันสร้างลายมือชื่อ (SCA) หรือ แอปพลิเคชันเพิ่มความน่าเชื่อถือให้กับลายมือชื่อ (SAA) อาจเป็นแอปพลิเคชันแบบสแตนด์อโลนแยกออกจากแอปพลิเคชันสร้างลายมือชื่อ (SCA) ก็ได้

Ref: ETSI TS 119 101 Security requirements for signature creation applications and signature validation applications

กระบวนการสร้างลายมือชื่อ (signing process)

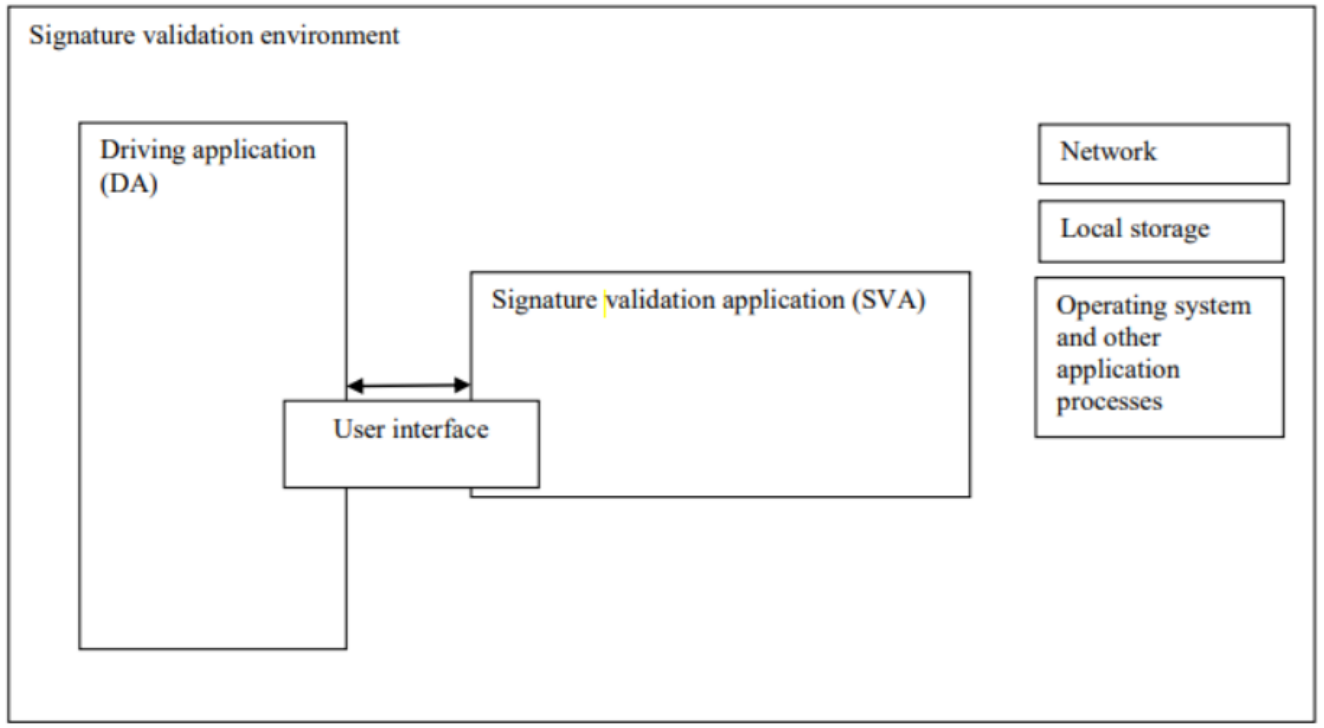


อุปกรณ์สร้างลายมือชื่อ (SCDev) ต้องดำเนินการในขั้นตอนต่างๆ ดังนี้

- ต้อง มีหรือครอบครองใบรับรองที่ใช้ลงลายมือชื่อ (หรือข้อมูลอ้างถึงใบรับรอง)
- ต้อง มีข้อมูลที่ใช้สร้างลายมือชื่อ (signature creation data)
- ต้อง สามารถยืนยันตัวตนเจ้าของลายมือชื่อ และ
- ต้อง สร้างข้อมูลลายมือชื่อ (signature value) ด้วยข้อมูลที่ใช้สร้างลายมือชื่อ (signature creation data) ของเจ้าของลายมือชื่อ (signer)

- ระบบสร้างลายมือชื่อ (SCS) รับเอกสารที่ต้องการลงลายมือชื่อ พร้อมด้วยข้อมูลอินพุตอื่นๆ จากแอปพลิเคชันขับ (DA)
- ระบบสร้างลายมือชื่อ (SCS) จัดเตรียมข้อมูลเพื่อลงลายมือชื่อ (data to be signed หรือ DTBS) จากเอกสารและข้อมูลอินพุตที่ได้รับ
- ระบบสร้างลายมือชื่อ (SCS) จัดรูปแบบข้อมูลเพื่อลงลายมือชื่อ (DTBS) ให้อยู่ในรูปแบบข้อมูลเพื่อลงลายมือชื่อ (DTBS formatted หรือ DTBSF)
- ระบบสร้างลายมือชื่อ (SCS) สร้างข้อมูลลายมือชื่อจากรูปแบบข้อมูลเพื่อลงลายมือชื่อ (DTBSF)
- ระบบสร้างลายมือชื่อ (SCS) จัดรูปแบบผลลัพธ์ของข้อมูลลายมือชื่อให้อยู่ในรูปแบบอ็อบเจกต์ข้อมูลที่ลงลายมือชื่อ (SDO) ที่สอดคล้องตามข้อกำหนดของรูปแบบลายมือชื่อที่ต้องการ (CAdES, XAdES, PAdES)
- ส่งอ็อบเจกต์ข้อมูลที่ลงลายมือชื่อ (SDO) และข้อมูลสถานภาพของการดำเนินการต่าง ๆ ให้กับแอปพลิเคชันขับ (DA)

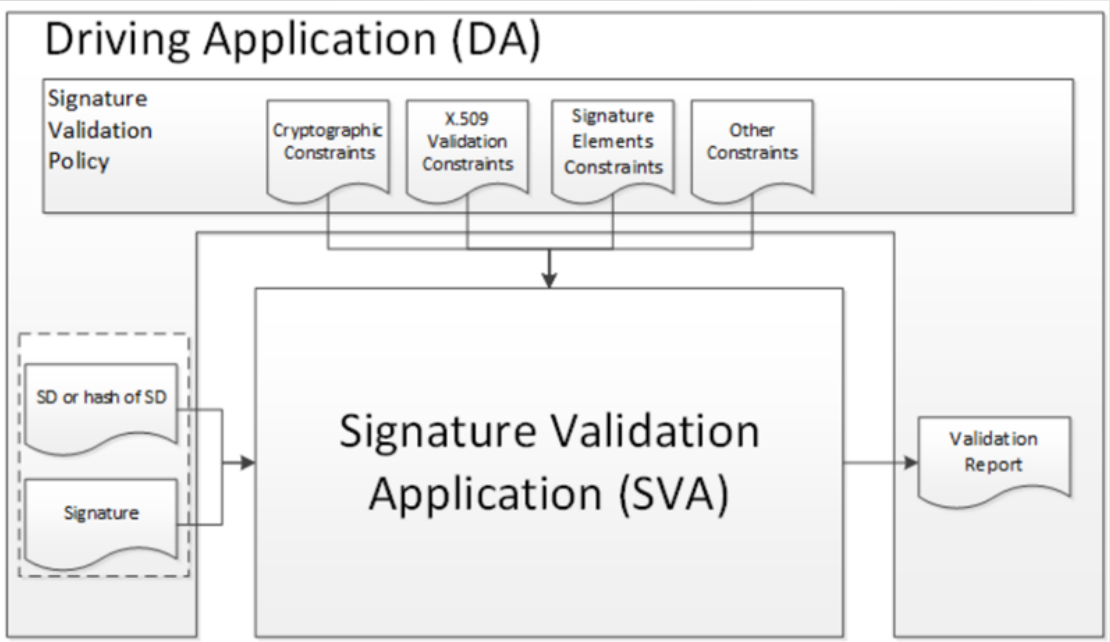
ส่วนประกอบ (building blocks) ของแบบแสดงการทำงานของระบบการตรวจสอบความถูกต้องของลายมือชื่อ



• ส่วนประกอบ (building blocks) ของแบบแสดงการทำงานในการตรวจสอบความถูกต้องของลายมือชื่อทั้งหมดจะอยู่ในขอบเขตของการตรวจสอบความถูกต้องของลายมือชื่อดิจิทัล ซึ่งถูกเรียกว่า สภาพแวดล้อมการตรวจสอบความถูกต้องของลายมือชื่อ (signature validation environment) ซึ่งประกอบด้วย แอปพลิเคชันขับ (driving application หรือ DA) แอปพลิเคชันตรวจสอบความถูกต้องของลายมือชื่อ (signature validation application หรือ SVA) และระบบโครงสร้างพื้นฐานสารสนเทศที่สนับสนุนการทำงานของการตรวจสอบลายมือชื่อ เช่น ระบบเครือข่าย ระบบการจัดเก็บข้อมูล และระบบปฏิบัติการและแอปพลิเคชันสารสนเทศต่างๆ

• ส่วนติดต่อผู้ใช้สามารถเป็นส่วนหนึ่งของแอปพลิเคชันขับ DA (บางส่วน) และ/หรือ (บางส่วน) ของ แอปพลิเคชันตรวจสอบความถูกต้องของลายมือชื่อ (SVA) ก็ได้

กระบวนการตรวจสอบความถูกต้องของลายมือชื่อ (validation process)



หมายเหตุ: SD คือ Signer ‘s document

- แอปพลิเคชันตรวจสอบความถูกต้องของลายมือชื่อ (SVA) รับเอกสารของเจ้าของลายมือชื่อ (SD) หรือค่าแฮชของ SD และข้อมูลลายมือชื่อ (signature) พร้อมด้วยข้อมูลอินพุตจากแหล่งต่าง ๆ เช่น ข้อจำกัดของการเข้ารหัสลับ (cryptographic constraints) ข้อจำกัดเกี่ยวกับใบรับรอง (X.509 constraints) ข้อจำกัดขององค์ประกอบลายมือชื่อ (signature element constraints) และข้อจำกัดอื่น ๆ จาก DA

- แอปพลิเคชันตรวจสอบความถูกต้องของลายมือชื่อ (SVA) ดำเนินการตรวจสอบความถูกต้องของลายมือชื่อตามข้อจำกัดต่าง ๆ และสร้างผลลัพธ์ของการตรวจสอบออกเป็นรายงาน (validation report)

- แอปพลิเคชันขับ (DA) ควรมีขั้นตอนกระบวนการทำงานเมื่อผลลัพธ์ของแอปพลิเคชันตรวจสอบความถูกต้องของลายมือชื่อ (SVA) ได้ผลลัพธ์ต่างๆ ดังนี้
  - ถ้า SVA ให้ผลลัพธ์ ผ่านทั้งหมด (TOTAL-PASSED) DA ควรพิจารณาว่าลายมือชื่อนั้นว่าเป็นถูกต้องเทคนิคบนข้อจำกัดในการตรวจสอบความถูกต้อง (validation constraints)
  - ถ้า SVA ให้ผลลัพธ์ ไม่ผ่านทั้งหมด (TOTAL-FAILED) DA ควรพิจารณาลายมือชื่อนั้นว่าไม่ถูกต้องทางเทคนิค
  - ถ้า SVA ให้ผลลัพธ์ ไม่ทราบแน่ชัด (INDETERMINATE) การยอมรับผลลัพธ์จะขึ้นกับ DA หรือขึ้นกับผู้ใช้งานก็ได้

การเลือกกระบวนการตรวจสอบความถูกต้องของลายมือชื่อ (validation process selection)

การเลือก SVA เพื่อใช้ตรวจสอบประเภทของลายมือชื่อต่าง ๆ โดยกระบวนการตรวจสอบลายมือชื่อประเภทที่มีความน่าเชื่อถือสูงกว่า ต้องรองรับการตรวจสอบลายมือชื่อประเภทที่มีความน่าเชื่อถือต่ำกว่าด้วย กระบวนการดำเนินการมีขั้นตอน ดังนี้

ขั้นตอนที่ 1 เลือกการตรวจสอบความถูกต้องของประเภทลายมือชื่อ

- Basic signature ..... ไปในขั้นตอนที่ 4
- Signature with T หรือ Signature with LT ..... ไปในขั้นตอนที่ 3
- Signature with LTA หรือ ไม่เลือก ..... ไปในขั้นตอนที่ 2

ขั้นตอนที่ 2 ตรวจสอบความถูกต้องของ Signature with LTA และข้ามไปในขั้นตอนที่ 5 หรือถ้าไม่รองรับการตรวจสอบ Signature with LTA ให้ดำเนินการในขั้นตอนถัดไป

ขั้นตอนที่ 3 ตรวจสอบความถูกต้องของ Signature with LT และข้ามไปในขั้นตอนที่ 5 หรือถ้าไม่รองรับการตรวจสอบ Signature with LT ให้ดำเนินการในขั้นตอนถัดไป

ขั้นตอนที่ 4 ตรวจสอบความถูกต้องของ Basic signature

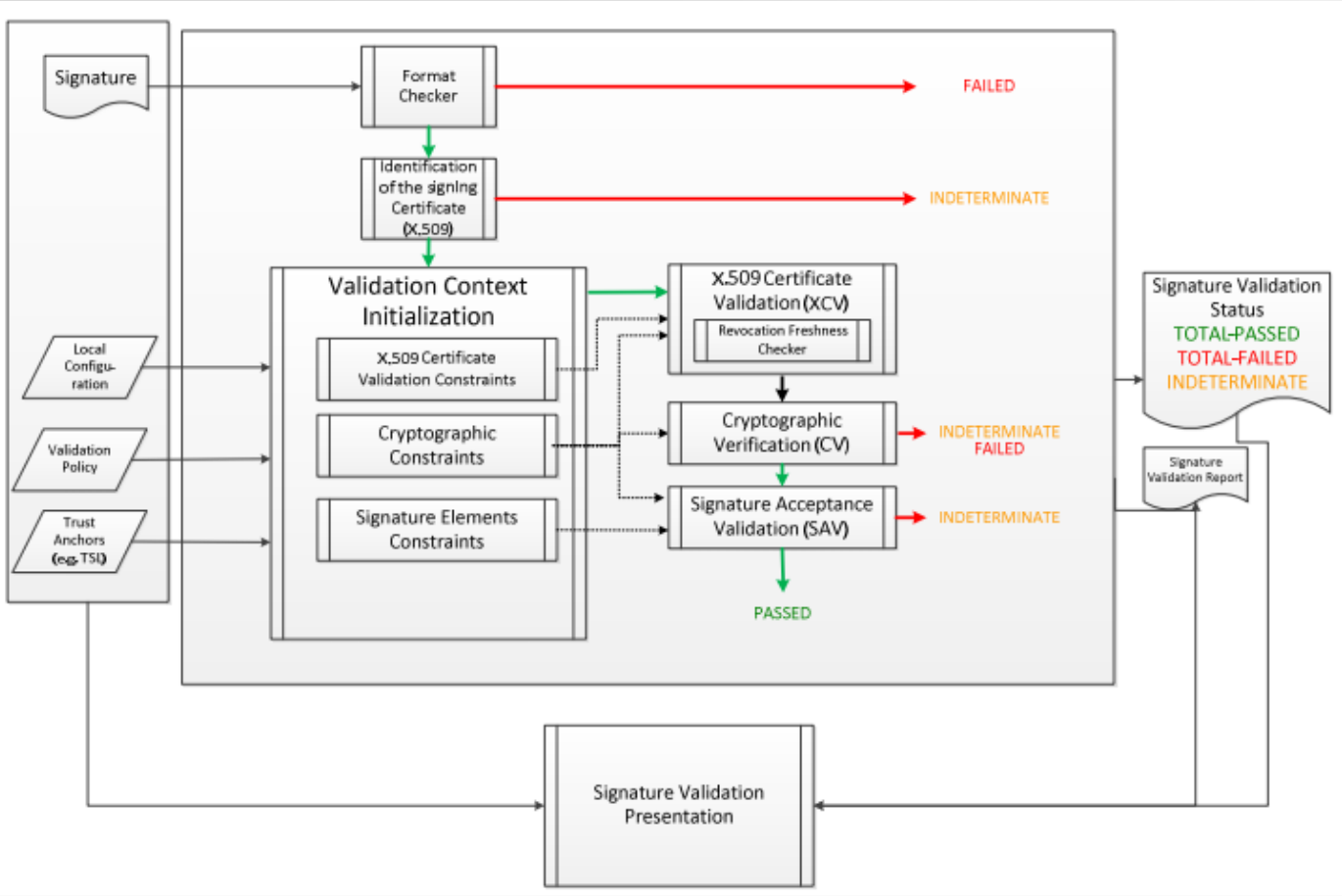
ขั้นตอนที่ 5 เมื่อได้ผลลัพธ์ของกระบวนการตรวจสอบความถูกต้องเป็น ผ่าน (PASSED) ส่งผลลัพธ์ ผ่านทั้งหมด (TOTAL PASSED) ให้ DA จบกระบวนการ

ขั้นตอนที่ 6 เมื่อได้ผลลัพธ์ของกระบวนการตรวจสอบความถูกต้องเป็น ไม่ผ่าน (FAILED) ส่งผลลัพธ์ ไม่ผ่านทั้งหมด (TOTAL FAILED) ให้ DA จบกระบวนการ

ขั้นตอนที่ 7 เมื่อได้ผลลัพธ์ของกระบวนการตรวจสอบความถูกต้องเป็น ไม่ทราบแน่ชัด (INDETERMINATE) ส่งผลลัพธ์นี้ให้ DA จบกระบวนการ

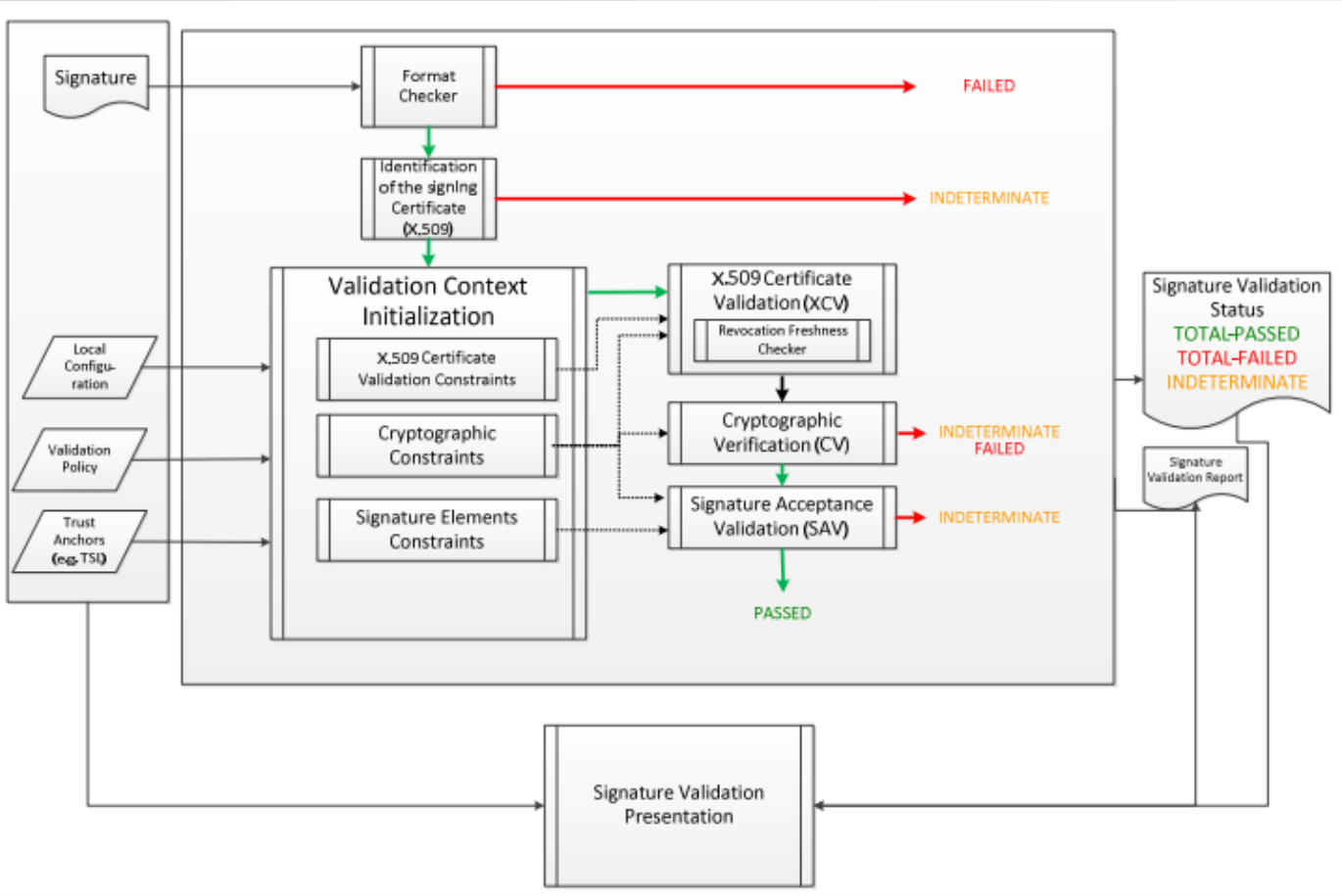
<u>หมายเหตุ</u> ในขั้นตอนที่ 5, 6, 7 SVA ต้องส่งข้อมูลผลลัพธ์สถานภาพย่อย (sub-indication) ให้กับ DA

ส่วนประกอบพื้นฐานของกระบวนการตรวจสอบความถูกต้องของลายมือชื่อพื้นฐาน (Basic building blocks for validation process)



1. การตรวจสอบรูปแบบของลายมือชื่อ (Format checking) ตรวจสอบข้อมูลลายมือชื่อว่ามีรูปแบบเป็นไปตามที่กำหนดและมีความถูกต้อง เช่น ความถูกต้องของการเข้ารหัสลับ (cryptographic verification)
2. การระบุใบรับรองของลายมือชื่อ (identification of the signing certificate X.509) ระบุใบรับรองที่ใช้เพื่อตรวจสอบความถูกต้องของลายมือชื่อ
3. การตั้งค่าการตรวจสอบความถูกต้องของลายมือชื่อ (validation context initialization) นำ validation constraints (ข้อมูลใน signature and validation policy) มาตั้งค่าในการดำเนินการตรวจสอบความถูกต้อง
4. การตรวจสอบความเป็นปัจจุบันของการเพิกถอนใบรับรอง (revocation freshness checker) ตรวจสอบความเป็นปัจจุบัน (fresh) ของข้อมูล revocation ในช่วงเวลาที่ validation
5. การตรวจสอบความถูกต้องของใบรับรอง (X.509 certificate validation) ตรวจสอบความถูกต้องของใบรับรอง X.509 ณ validation time (X.509 certificate validation)

ส่วนประกอบพื้นฐานของกระบวนการตรวจสอบความถูกต้องของลายมือชื่อพื้นฐาน (Basic building blocks for validation process)



6. การตรวจสอบด้วยกระบวนการเข้ารหัสลับ (cryptographic verification หรือ CV) ตรวจสอบ integrity ของ signed data ด้วยการตรวจสอบด้วยการเข้ารหัสลับ

7. การตรวจสอบเพิ่มเติมของลายมือชื่อ (Signature acceptance validation หรือ SAV) ตรวจสอบเพิ่มเติมของลายมือชื่อ หรือแอตทริบิวต์ของลายมือชื่อ (signature (elements) attributes) ซึ่งการตรวจสอบในขั้นตอนนี้สามารถรองรับการตรวจสอบอื่นๆ เพิ่มเติมที่ระบุไว้นโยบายการตรวจสอบความถูกต้องของลายมือชื่อ (signature validation policy

ผลลัพธ์หลักของกระบวนการตรวจสอบความถูกต้องของลายมือชื่อ

ข้อมูลรายงานสถานภาพการตรวจสอบความถูกต้อง		ความหมาย
ผลลัพธ์หลัก	รายงานการตรวจสอบความถูกต้อง	
TOTAL-PASSED	กระบวนการตรวจสอบความถูกต้องของลายมือชื่อ ต้องแสดงผลลัพธ์ของการตรวจสอบห่วงโซ่ใบรับรอง (certificate chain) ซึ่งรวมถึงใบรับรองที่ใช้สร้างลายมือชื่อ (signing certificate) นอกจากนั้น ต้องแสดงผลลัพธ์ตามข้อจำกัดของการตรวจสอบความถูกต้อง (validation constraints) กระบวนการตรวจสอบความถูกต้องของลายมือชื่อควรแอปพลิเคชันขับ (DA) เข้าถึงข้อมูลแอตทริบิวต์ที่ลงลายมือชื่อ (signed attributes) ข้อมูลระบุตัวตนของเจ้าของลายมือชื่อ และห่วงโซ่ใบรับรอง (signing certificate chain)	*TOTAL-PASSED* มีเงื่อนไขดังนี้ - ผลลัพธ์ของการตรวจสอบลายมือชื่อด้วยกระบวนการเข้ารหัสลับถูกต้อง - ผลลัพธ์ของการตรวจสอบตามข้อจำกัด (constraints) ที่เกี่ยวข้องกับการตรวจสอบใบรับรองของเจ้าของลายมือชื่อถูกต้อง - ผลลัพธ์ของการตรวจสอบตามข้อจำกัด (constraints) ที่เกี่ยวข้องกับลายมือชื่อถูกต้องหรือสอดคล้องตามข้อกำหนด
TOTAL-FAILED	กระบวนการตรวจสอบความถูกต้องของลายมือชื่อ ต้องให้ข้อมูลเพิ่มเติมเพื่ออธิบายในแต่ละสถานการณ์ที่ได้ผลลัพธ์หลักเป็น *TOTAL-FAILED*	ผลลัพธ์ *TOTAL-FAILED* เกิดขึ้นได้จากหลายสถานการณ์ เช่น พบว่ารูปแบบของลายมือชื่อไม่ถูกต้อง (format-check failed), การตรวจสอบลายมือชื่อด้วยกระบวนการเข้ารหัสลับ(cryptographic check) ได้ผลลัพธ์ไม่ถูกต้อง, หรือ พบว่าการสร้างลายมือชื่อเกิดขึ้นในภายหลังเวลาที่มีการเพิกถอนใบรับรองแล้ว
INDETERMINATE	กระบวนการตรวจสอบความถูกต้องของลายมือชื่อ ต้องให้ข้อมูลเพิ่มเติมเพื่ออธิบายในแต่ละสถานการณ์ที่ได้ผลลัพธ์หลักเป็น *INDETERMINATE* เพื่อช่วยให้กับผู้ตรวจสอบสามารถระบุได้ว่าข้อมูลใดที่ขาดหรือไม่ครบในการกระบวนตรวจสอบความถูกต้อง รวมถึงการระบุข้อจำกัด (constraints) ใดที่ใช้ในกระบวนการตรวจสอบที่ส่งผลให้ได้ผลลัพธ์นี้	ข้อมูลที่สนับสนุนในกระบวนการตรวจสอบความถูกต้องของลายมือชื่อมีไม่เพียงพอที่จะสามารถสรุปได้ว่าผลลัพธ์จะเป็น *TOTAL-PASSED* หรือ *TOTAL-FAILED*

โครงสร้างความสัมพันธ์ผลลัพธ์หลักและข้อมูลสถานภาพย่อย (sub-indication) สำหรับ TOTAL-FAILED และ INDETERMINATE

ข้อมูลรายงานสถานภาพการตรวจสอบความถูกต้อง			ความหมาย
ผลลัพธ์หลัก	สถานภาพย่อย	ข้อมูลรายงานของการตรวจสอบความถูกต้อง	
TOTAL-FAILED	*FORMAT_FAILURE*	ต้องให้ข้อมูลที่ระบุถึงสาเหตุที่ระบุว่ารูปแบบผิดพลาด	เมื่อรูปแบบลายมือชื่อไม่สอดคล้องตามข้อกำหนด ซึ่งรวมถึงพบว่าการตรวจสอบในกระบวนการเข้ารหัสลับไม่สามารถดำเนินการได้
	HASH_FAILURE	ต้องให้ข้อมูลตัวระบุองค์ประกอบของ SDO ใดที่ทำให้พบข้อผิดพลาด	เมื่อพบว่ามีอย่างน้อยหนึ่งข้อมูลแฮชของ SDO ที่มีค่าไม่เหมือนกับค่าแฮชที่แสดงไว้ในลายมือชื่อ
	SIG_CRYPTO_FAILURE	ต้องให้ข้อมูลระบุถึงใบรับรองที่พบให้ผลการตรวจสอบด้วยกระบวนการเข้ารหัสลับและได้ผลลัพธ์ไม่ถูกต้อง	เมื่อพบว่าค่าลายมือชื่อไม่สามารถตรวจสอบความถูกต้องด้วยกระบวนการเข้ารหัสลับด้วยกุญแจสาธารณะในใบรับรอง
	REVOKED	ต้องให้ข้อมูล certificate chain และเวลา (ถ้าระบุได้) และเหตุในการเพิกถอนใบรับรอง	เมื่อพบว่าใบรับรองถูกเพิกถอน และไม่มีหลักฐานยืนยันว่าลายมือชื่อถูกสร้างขึ้นในภายหลังเวลาที่เพิกถอนใบรับรอง

โครงสร้างความสัมพันธ์ผลลัพธ์หลักและข้อมูลสถานภาพย่อย (sub-indication) สำหรับ TOTAL-FAILED และ INDETERMINATE

ข้อมูลรายงานสถานภาพการตรวจสอบความถูกต้อง			ความหมาย
ผลลัพธ์หลัก	สถานภาพย่อย	ข้อมูลรายงานของการตรวจสอบความถูกต้อง	
INDETERMINATE	*SIG_CONSTRAINTS_FAILURE*	ต้องให้ข้อมูล ชุดรายการข้อจำกัด (constraints) ที่มีผลลัพธ์ไม่สอดคล้อง	เมื่อพบว่า มีอย่างน้อยหนึ่งรายการของแอตทริบิวต์ลายมือชื่อที่ไม่สอดคล้องกับข้อจำกัด (constraints)
	CHAIN_CONSTRAINTS_FAILURE	ต้องให้ข้อมูล ห่วงโซ่ใบรับรองที่ใช้ในกระบวนการตรวจสอบความถูกต้องและชุดของรายการข้อกำหนด (constraints) ที่ใช้ในกระบวนการตรวจสอบ	เมื่อพบว่า ห่วงโซ่ใบรับรองที่ใช้ในการตรวจสอบไม่สอดคล้องกับข้อจำกัดที่ระบุไว้ที่เกี่ยวข้องกับใบรับรองนั้น
	CERTIFICATE_CHAIN_GENERAL_FAILURE	ต้องให้ข้อมูลเพิ่มเติมที่เกี่ยวข้องกับความผิดพลาดของห่วงโซ่ใบรับรอง	เมื่อพบว่า ผลลัพธ์ของการตรวจสอบความถูกต้องของใบรับรองมีความผิดพลาดที่ไม่สามารถระบุเหตุผลได้
	CRYPTO_CONSTRANTS_FAILURE	ต้องให้ข้อมูลที่ใช้ในการตรวจสอบ (material) เช่น ลายมือชื่อหรือใบรับรอง ที่มีระดับความมั่นคงปลอดภัยต่ำกว่าข้อกำหนด และเวลาที่ระบุว่าอัลกอริทึมนั้นยังมีระดับความมั่นคงปลอดภัยที่ยังแข็งแรงหรือใช้งานได้อยู่ (ถ้าทราบ)	เมื่อพบว่า อัลกอริทึมหรือความยาวของกุญแจที่ใช้ในการตรวจสอบความถูกต้อง มีระดับความมั่นคงปลอดภัยต่ำกว่าข้อกำหนด และข้อมูลในการตรวจสอบนี้ถูกสร้างขึ้นภายหลังจากเวลาที่ระบุว่าอัลกอริทึมหรือความยาวกุญแจยังมีความแข็งแรงหรือยังใช้งานได้ และข้อมูลในการตรวจสอบนี้ ไม่ได้รับการปกป้องด้วยการประทับเวลาที่มีความแข็งแรงเพียงพอ
	EXPIRED	ต้องให้ข้อมูลห่วงโซ่ใบรับรอง	เมื่อพบว่ามีหลักฐานที่ยืนยันว่าลายมือชื่อถูกสร้างขึ้นในภายหลังเวลาที่ใบรับรองหมดอายุ
	NOT_YET_VALID	-	เมื่อพบว่า เวลาในการสร้างลายมือชื่อเกิดขึ้นก่อนวันที่จะออกใบรับรอง
	POLICY_PROCESSING_ERROR	ต้องให้ข้อมูลเพิ่มเติมที่เกี่ยวข้องกับข้อผิดพลาดที่พบ	เมื่อพบว่า นโยบายลายมือชื่อที่กำหนดไว้ไม่สามารถนำมาประมวลผลได้ อาจเกิดจากไม่สามารถเข้าถึงได้ หรือไม่สามารถประมวลข้อมูลได้ หรือค่าไดเจสต์ไม่ตรงกับที่ระบุไว้

โครงสร้างความสัมพันธ์ผลลัพธ์หลักและข้อมูลสถานภาพย่อย (sub-indication) สำหรับ TOTAL-FAILED และ INDETERMINATE

ข้อมูลรายงานสถานภาพการตรวจสอบความถูกต้อง			ความหมาย
ผลลัพธ์หลัก	สถานภาพย่อย	ข้อมูลรายงานของการตรวจสอบความถูกต้อง	
INDETERMINATE	*SIGNATURE_POLICY_NOT_AVAILABLE*	-	เมื่อพบว่า ไม่มีนโยบายลายมือชื่อที่กำหนดไว้
	TIMESTAMP_ORDER_FAILURE	ต้องให้ข้อมูลรายการ ข้อมูลประทับเวลาที่ไม่สอดคล้องกับข้อจำกัดที่ระบุ (constraints)	เมื่อพบว่ามีข้อจำกัด (constraints) ที่เกี่ยวข้องกับลำดับข้อมูลประทับเวลา หรือ SDO ไม่สอดคล้องกับข้อมูลที่พบ
	NO_SIGNING_CERTIFICATE_FOUND	-	เมื่อไม่พบใบรับรอง
	NO_CERTIFICATE_CHAIN_FOUND	-	เมื่อไม่พบห่วงโซ่ใบรับรอง (certificate chain)
	REVOKED_NO_POE	ต้องให้ข้อมูล ห่วงโซ่ใบรับรอง (certificate chain) และเวลาและเหตุผลในการเพิกถอนใบรับรอง	เมื่อ signing certificate ถูกเพิกถอน ก่อนเวลาตรวจสอบความถูกต้องของลายมือชื่อ แต่กระบวนการตรวจสอบความถูกต้องของลายมือชื่อไม่สามารถระบุได้แน่ชัดว่า เวลาการเพิกถอนเกิดขึ้นก่อนหรือหลังการสร้างลายมือชื่อ
	REVOKED_CA_NO_POE	ต้องให้ข้อมูล certificate chain ที่พบการเพิกถอนintermediate ca certificate และเวลาและเหตุผลในการเพิกถอน	เมื่อพบว่ามีอย่างน้อยหนึ่งข้อมูลห่วงโซ่ใบรับรอง ของ intermediate ca certificate ถูกเพิกถอน
	OUT_OF_BOUNDS_NO_POE	-	เมื่อพบว่า signing certificate หมดอายุหรือมีสถานภาพไม่สามารถใช้งานได้ ณ เวลาการตรวจสอบความถูกต้องของลายมือชื่อ และไม่สามารถระบุได้ว่าลายมือชื่อถูกสร้างในขณะที่ signing certificate ยังสามารถใช้งานได้หรือไม่

โครงสร้างความสัมพันธ์ผลลัพธ์หลักและข้อมูลสถานภาพย่อย (sub-indication) สำหรับ TOTAL-FAILED และ INDETERMINATE

ข้อมูลรายงานสถานภาพการตรวจสอบความถูกต้อง			ความหมาย
ผลลัพธ์หลัก	สถานภาพย่อย	ข้อมูลรายงานของการตรวจสอบความถูกต้อง	
INDETERMINATE	*CRYPTO_CONSTRAINTS_FAILURE_NO_POE*	ต้องให้ข้อมูลที่ใช้ในการตรวจสอบ (material) เช่น ลายมือชื่อ หรือ signing certificate ที่สร้างขึ้นจากอัลกอริทึมหรือความยาวของกุญแจที่มีระดับความมั่นคงปลอดภัยต่ำกว่าข้อกำหนด และเวลาที่ระบุว่าอัลกอริทึมหรือความยาวของกุญแจนั้นยังมีระดับความมั่นคงปลอดภัยที่ยังแข็งแรงหรือใช้งานได้อยู่ (ถ้าทราบ)	เมื่อพบว่า อัลกอริทึมหรือความยาวของกุญแจในการสร้างลายมือชื่อหรือใบรับรอง มีระดับความมั่นคงปลอดภัยต่ำกว่าข้อกำหนด และไม่หลักฐานที่สามารถระบุได้การสร้างลายมือชื่ออยู่ในช่วงเวลาที่กระบวนเข้ารหัสลับหรือความยาวของกุญแจยังมีความแข็งแรงเพียงพอหรือยังใช้งานได้
	NO_POE	ต้องระบุ signed object ที่หลักฐานการดำรงอยู่ (PoE) ขาดหรือไม่ครบถ้วน รวมถึงการให้ข้อมูลเพิ่มเติมที่เกี่ยวข้องกับปัญหานี้	เมื่อพบว่า หลักฐานการดำรงอยู่ (PoE) มีไม่ครบถ้วนเพื่อยืนยันว่าระบุ signed object ถูกสร้างก่อนเวลาที่จะพบปัญหา
	TRY_LATER	ต้องระบุเวลาที่คาดว่าจะมีข้อมูลการเพิกถอนใบรับรองเพื่อใช้ตรวจสอบความถูกต้อง	เมื่อพบว่า ข้อจำกัดของการตรวจสอบความถูกต้อง (constraints) ทั้งหมดสามารถตรวจสอบได้ และอาจสามารถดำเนินการตรวจสอบเพิ่มเติมได้ในภายหลัง
	SIGNED_DATA_NOT_FOUND	ควรให้ข้อมูล ตัวระบุตำแหน่ง (เช่น URI) ของ signed data ที่พบปัญหา	เมื่อพบว่า signed data ไม่มีให้นำมาใช้ตรวจสอบได้
	GENERIC	ต้องให้ข้อมูลเพิ่มเติมถึงสาเหตุที่ให้ผลลัพธ์ของการตรวจสอบเป็น ไม่ทราบแน่ชัด (INDETERMINATE)	เมื่อพบสาเหตุอื่นๆ นอกเหนือจากสาเหตุที่ระบุได้ในแน่ชัดข้างต้น

โครงสร้างความสัมพันธ์ผลลัพธ์หลักและข้อมูลสถานภาพย่อย (sub-indication) สำหรับ TOTAL-FAILED และ INDETERMINATE

ข้อมูลสถานภาพย่อย (sub-indication)	เงื่อนไข
CHAIN_CONSTRAINTS_FAILURE, *CERTIFICATE_CHAIN_GENERAL_FAILURE*	มีความเป็นไปได้ที่จะสร้างห่วงโซ่ใบรับรอง (certificate chain) ตัวอย่างเช่น การเพิ่มใบรับรองที่เป็น cross-certificate ซึ่งจะทำให้การสร้างห่วงโซ่ใบรับรองเชื่อมโยงขึ้นไปยังใบรับรองรูท (root certificate) อื่นได้
POLICY_PROCESSING_ERROR	พบว่าสามารถเข้าถึงนโยบายลายมือชื่อใหม่ที่สามารถนำมาประมวลผลได้
SIGNATURE_POLICY_NOT_AVAILABLE	พบว่ามีนโยบายลายมือชื่อใหม่
NO_SIGNING_CERTIFICATE_FOUND	พบว่ามีใบรับรองที่ใช้สร้างลายมือชื่อ (signing certificate)
NO_CERTIFICATE_CHAIN_FOUND	พบว่ามีใบรับรองของผู้ออกใบรับรอง (CA-certificate) เพื่อใช้ในการสร้างห่วงโซ่ใบรับรอง (certificate chain)
REVOKED_NO_POE, REVOKED_CA_NO_POE, *OUT_OF_BOUNDS_NOT_REVOKED,* *OUT_OF_BOUNDS_NO_POE,* *CRYPTO_CONSTRAINTS_FAILURE_NO_POE,* *NO_POE*	พบว่ามีข้อมูลเพิ่มเติมสำหรับการพิสูจน์หลักฐานการดำรงอยู่ (proof of existence (POE)) ในกรณีนี้จะเป็นกรณีเฉพาะลายมือชื่อที่มีความพร้อมใช้ในระยะยาวและมีความสมบูรณ์ครบถ้วนของข้อมูลตรวจสอบความถูกต้องลายมือชื่อ (signature providing long term availability and integrity of validation material)
TRY_LATER	พบว่ามีข้อมูลการเพิกถอนใบรับรองที่เป็นปัจจุบันเพียงพอเพื่อใช้ในการตรวจสอบความถูกต้องของลายมือชื่อ

ตัวอย่างการตรวจสอบความถูกต้องของลายมือชื่อ

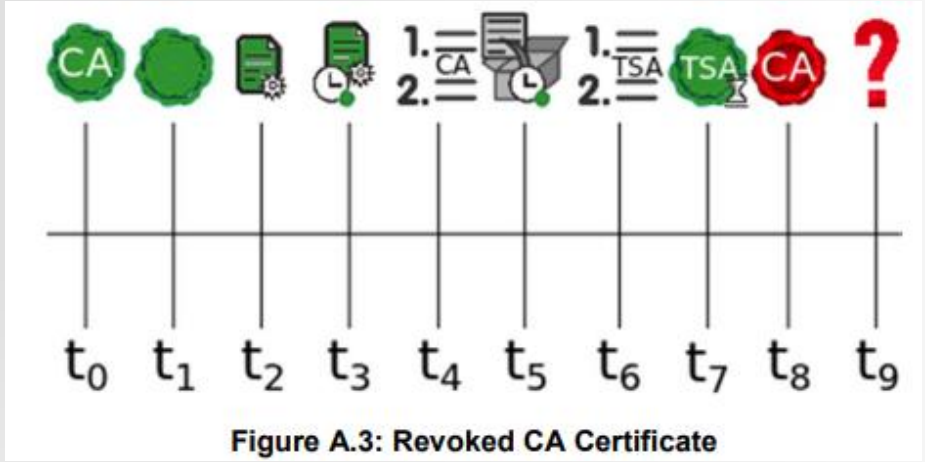
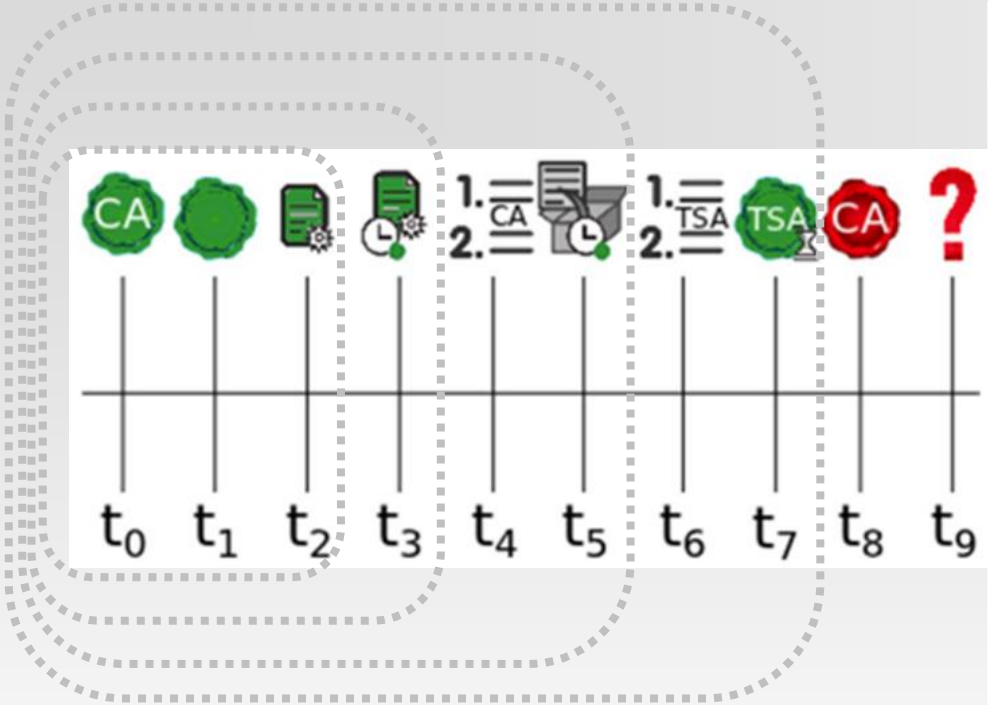


Figure A.3: Revoked CA Certificate

Validation Process	Expected Result	Rationale
Basic Sig. Validation	INDETERMINATE/REVOKED_CA_NO_POE	ไม่ทราบระบุได้ว่า signing time เกิดก่อนการเพิกถอนใบรับรองของ CA เนื่องจากไม่ได้ประมวลผลข้อมูลแอตทริบิวต์การเพิ่มความน่าเชื่อถือ (validation material)
Sig with Time Validation	INDETERMINATE/REVOKED_CA_NO_POE	ไม่สามารถสร้าง certificate chain ได้เนื่องจากใบรับรองของ intermediate CA ถูกเพิกถอนไป
Long-term validation	TOTAL-PASSED	เวลา t3 สร้างข้อมูลประทับเวลาและเวลา t5 สร้าง archive timestamp สำหรับ LT ซึ่งสามารถสร้าง POE และยืนยันได้ว่าใบรับรองของ certificate chain ทั้งหมดยังพร้อมใช้งานก่อนเวลา t7 และ t8 ณ เวลาตรวจสอบความถูกต้องของลายมือชื่อ t9

ตัวอย่างการตรวจสอบความถูกต้องของลายมือชื่อ



Time	Found	Result
t9 - Basic validation	Revoked CA certificate t8	Signature: INDETERMINATE/ REVOKED_CA_NO_POE
t9 – Time validation	Expired TSA certificate t7, only protect signature but not the signing certificate validation material	Signature: INDETERMINATE/REVOKED_CA_NO _POE, Time-stamp validation: INDETERMINATE/EXPIRED_NO_POE
t9 – LT validation	Step1: POE (5.6.3) validation signature	Archive time-stamp validation: PASSED -> extract POE at archive time-stamp t5 for signature and signature of time-stamp
t9 – LTA validation	Step4: time-stamp validation - time-stamp certificate expires t7 at the validation time t9 Past certificate validation for TSA certificate -> found valid TSA certificate chain at t5	Time-stamp Signature: INDETERMINATE/OUT_OF_BOUNDS _NO_POE


Q&A