ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ETDA Recommendation on ICT Standard

for Electronic Transactions

ขมธอ. [x-xxxx]

ว่าด้วยบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล

REMOTE SIGNING SERVICE

เวอร์ชัน 0.2

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ICS 35.030

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล

ขมธอ. [x-xxxx]

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 20-22
เลขที่ 33/4 ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
หมายเลขโทรศัพท์: 0 2123 1234 หมายเลขโทรสาร: 0 2123 1200

ประกาศโดย
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

วันที่ กรุณาเลือกวันที่ประกาศ

คณะทำงานจัดทำร่างข้อเสนอแนะมาตรฐานเกี่ยวกับธุรกิจบริการ
ด้านการทำธุรกรรมทางอิเล็กทรอนิกส์

ที่ปรึกษาคณะทำงาน

นายชัยชนะ มิตรพันธ์	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ประธานคณะทำงาน

นายศุภโชค จันทรประทิน	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ผู้ทำงาน

นางสาวสำรวย นุ่มศรี	กรมศุลกากร
นายกำชัย จัตตานนท์	
นางจันทร์เจริญ เทพสุธา	กรมสรรพากร
นายยุทธพล จินะสี	
นายคงฤทธิ์ จันทริก	สภาผู้ส่งสินค้าทางเรือแห่งประเทศไทย
นายภาวุธ พงษ์วิทยภานุ	สมาคมผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์ไทย
นายธานินทร์ ตันกิติบุตร	สมาคมผู้ให้บริการอินเทอร์เน็ตและคลาวด์ไทย
นายวรพจน์ ธาราศิริสกุล	สมาคมฟินเทคประเทศไทย
นายปกรณ์ ลี้สกุล	สมาคมอุตสาหกรรมซอฟต์แวร์ไทย
นายสันติ สิทธิเลิศพิศาล	สำนักมาตรฐานผลิตภัณฑ์อุตสาหกรรม
นางสาวธิดารัธ ธนภรรคภวิน	สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย
นายอิศร์ เตาลานนท์	
นางสาวขนิษฐ์ ผาทอง	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายพงษ์พันธ์ ศรีปาน	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ผู้ทำงานและเลขานุการ

นายณัฐฑพัฒน์ โรจนศุภมิตร	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ผู้ช่วยเลขานุการ

นายวีรศักดิ์ ดีอ่ำ	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกลฉบับนี้ จัดทำขึ้นเพื่ออธิบายส่วนประกอบและหลักการทำงานของการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกลด้วยระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (trustworthy systems supporting server signing) รวมถึงกำหนดรูปแบบในการบริหารจัดการกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) และกระบวนการสั่งให้สร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกลซึ่งสามารถรับประกันความเชื่อมั่นในระดับสูงได้ว่ากุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลอยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น (sole control)

โดยมีการนำเสนอและรับฟังความคิดเห็นเป็นการทั่วไป ตลอดจนพิจารณาข้อมูล ข้อสังเกต ข้อคิดเห็นจากผู้ทรงคุณวุฒิและจากหน่วยงานที่เกี่ยวข้อง เพื่อปรับปรุงให้ข้อเสนอแนะมาตรฐานฉบับนี้มีความครบถ้วนสมบูรณ์ยิ่งขึ้น รวมทั้งให้สามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพ

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกลฉบับนี้ จัดทำขึ้นโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 20-22 เลขที่ 33/4 ถนนพระราม 9
แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
โทรศัพท์: 0 2123 1234 โทรสาร: 0 2123 1200
อีเมล: estandard.center@etda.or.th
เว็บไซต์: www.etda.or.th

คำนำ

ปัจจุบันการใช้งานลายมือชื่อดิจิทัลยังมีอุปสรรคที่ทำให้การประยุกต์ใช้งานยังไม่เป็นที่แพร่หลายอยู่ที่การเก็บรักษากุญแจส่วนตัวให้มั่นคงปลอดภัย และการบริหารจัดการกุญแจส่วนตัวเพื่อนำมาใช้ลงลายมือชื่อดิจิทัลได้อย่างสะดวกนั้นไม่ใช่สิ่งที่ผู้ใช้งานทั่วไปพึงจะกระทำเองได้โดยง่าย การลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote signing) จึงเป็นวิธีการที่เป็นทางเลือกและได้รับการยอมรับในหลายประเทศ เช่น สหภาพยุโรป เนื่องจากสามารถอำนวยความสะดวกให้กับผู้ใช้งานในการเก็บรักษาและเรียกใช้งานกุญแจส่วนตัวผ่านระบบเครือข่ายคอมพิวเตอร์ เมื่อได้ดำเนินการด้วยวิธีการที่เชื่อถือได้และมีความมั่นคงปลอดภัย

ด้วยเหตุนี้ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์จึงได้จัดทำข้อเสนอแนะมาตรฐาน ฯ ว่าด้วยบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote singing service) เพื่ออธิบายส่วนประกอบและหลักการทำงานของการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกลด้วยระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (trustworthy systems supporting server signing: TW4S) รวมถึงกำหนดรูปแบบในการบริหารจัดการกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) และกระบวนการสั่งให้สร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกลซึ่งสามารถรับประกันความเชื่อมั่นในระดับสูงได้ว่ากุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลอยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น (sole control) โดยข้อเสนอแนะมาตรฐานฉบับนี้เป็นข้อเสนอแนะสำหรับหน่วยงานต่างที่ต้องการใช้ และ/หรือให้บริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล ด้วยรูปแบบที่มีมาตรฐานและมีความน่าเชื่อถืออ้างอิงตามมาตรฐานของสหภาพยุโรป

สารบัญ

หน้า

1. ขอบข่าย **7**

2. บทนิยาม **8**

3. อักษรย่อ **10**

4. ภาพรวมของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (trustworthy system supporting server signing: TW4S) **11**

4.1 ภาพรวมของกระบวนการสร้างลายมือชื่อดิจิทัล 11

4.1.1 แอปพลิเคชันสร้างลายมือชื่อดิจิทัล (signature creation application: SCA) 12

4.1.2 แอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (server signing application: SSA) 13

4.2 ระดับความเข้มงวดในการควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น (sole control assurance level: SCAL) 14

4.2.1 ระดับความเข้มงวดฯ พื้นฐาน SCAL1 14

4.2.2 ระดับความเข้มงวดฯ ขั้นสูง SCAL2 15

4.3 การพิสูจน์และยืนยันตัวตนเจ้าของลายมือชื่อ 16

4.3.1 การพิสูจน์ตัวตน 16

4.3.2 การยืนยันตัวตน 16

4.3.3 เป้าประสงค์ของการยืนยันตัวตน 17

4.3.4 การพิสูจน์และยืนยันตัวตนจากผู้ให้บริการภายนอก 17

4.4 กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) และโมดูลเข้ารหัสลับ (cryptographic module) 18

4.5 ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (signature activation data: SAD) 18

4.6 โพรโทคอลเพื่อสั่งให้สร้างลายมือชื่อดิจิทัล (signature activation protocol: SAP) 19

4.7 ส่วนติดต่อของเจ้าของลายมือชื่อ (signer’s interaction component: SIC) 19

4.8 โมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (signature activation module: SAM) 20

4.9 ขอบเขตสภาพแวดล้อม 20

4.9.1 ขอบเขตที่มีการป้องกันการเปลี่ยนแปลงข้อมูล (tamper protected environment) 20

4.9.2 ขอบเขตที่ผู้ให้บริการที่เชื่อถือได้บริหารจัดการและดูแล (TSP protected environment) 21

4.9.3 ขอบเขตของเจ้าของลายมือชื่อ (signer’s environment) 21

5. ข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ **22**

5.1 ข้อกำหนดด้านความมั่นคงปลอดภัยพื้นฐานที่จำเป็น (general security requirements: SRG) 22

5.1.1 การบริหารจัดการ (SRG_M) 22

5.1.2 ระบบและการปฏิบัติงาน (SRG_SO) 24

5.1.3 การระบุและยืนยันตัวตน (SRG_IA) 25

5.1.4 การควบคุมและจำกัดการเข้าถึงระบบ (SRG_SA) 26

5.1.5 การบริหารจัดการกุญแจ (SRG_KM) 26

5.1.6 การตรวจสอบ (SRG_AA) 30

5.1.7 การจัดเก็บข้อมูลไว้เป็นหลักฐานในระยะยาว (SRG_AR) 33

5.1.8 การสำรองและกู้คืนข้อมูล (SRG_BK) 33

5.2 ข้อกำหนดด้านความมั่นคงปลอดภัยของส่วนประกอบหลักของระบบ (core component security requirements: SRC) 34
5.2.1 การตั้งค่ากุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล และกุญแจระบบรหัสลับ (SRC_SKS.1) 34
5.2.2 การยืนยันตัวตนเจ้าของลายมือชื่อ (SRC_SA) 34
5.2.3 การสร้างลายมือชื่อดิจิทัล และกระบวนการระบบรหัสลับ (SRC_DSC) 35
5.3 ข้อกำหนดด้านความมั่นคงปลอดภัยเพิ่มเติมสำหรับระดับความเข้มงวดฯ ขั้นสูง SCAL2 (additional security requirements: SRA) 36
5.3.1 โพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัลและข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SRA_SAP) 36
5.3.2 การบริหารจัดการกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (SRA_SKM) 38
5.4 ข้อกำหนดมาตรฐานความมั่นคงปลอดภัยสำหรับระบบ TW4S 40
บรรณานุกรม **41**

สารบัญรูป

หน้า

รูปที่ 1 ภาพรวมกระบวนการและข้อมูลในการสร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล 12
รูปที่ 2 การยืนยันตัวตนเพื่อสั่งให้สร้างลายมือชื่อดิจิทัลระดับความเข้มงวดฯ พื้นฐาน SCAL1 15
รูปที่ 3 การยืนยันตัวตนเพื่อสั่งให้สร้างลายมือชื่อดิจิทัลระดับความเข้มงวดฯ ขั้นสูง SCAL2 16

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ว่าด้วยบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล

1. ขอบข่าย

ข้อเสนอแนะมาตรฐานฉบับนี้อธิบายส่วนประกอบและหลักการทำงานของการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกลด้วยระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (trustworthy systems supporting server signing: TW4S) รวมถึงกำหนดรูปแบบในการบริหารจัดการกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) และกระบวนการสั่งให้สร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกลซึ่งสามารถรับประกันความเชื่อมั่นในระดับสูงได้ว่ากุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลอยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น (sole control) โดยข้อเสนอแนะมาตรฐานฉบับนี้เป็นข้อเสนอแนะสำหรับหน่วยงานต่าง ๆ ทั้งภาครัฐและเอกชนในประเทศไทย ที่ต้องการใช้ และ/หรือให้บริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล ด้วยรูปแบบที่มีมาตรฐานและมีความน่าเชื่อถืออ้างอิงตามมาตรฐานของสหภาพยุโรป [1]

ข้อเสนอแนะมาตรฐานฉบับนี้สามารถใช้เป็นวิธีการสร้างลายมือชื่อดิจิทัลได้ ดังนี้

- การสร้างลายมือชื่อดิจิทัลของบุคคล (digital signature) หรือใช้เป็นวิธีการสร้างตราประทับอิเล็กทรอนิกส์ของนิติบุคคล (electronic seal) [2] ดังนั้น คำนิยามที่กำหนดไว้เกี่ยวกับ เจ้าของลายมือชื่อ (signer) จะมีความหมายครอบคลุมถึงนิติบุคคลที่เป็นเจ้าของตราประทับอิเล็กทรอนิกส์
- การสร้างลายมือชื่อดิจิทัลครั้งละหลายรายการ (bulk/batch signing) เช่น การสร้างชุดลายมือชื่อดิจิทัลสำหรับการลงนามในชุดเอกสารในคราวเดียวแทนการสั่งให้สร้างลายมือชื่อสำหรับเอกสารทีละฉบับ อย่างไรก็ตาม การพิจารณาใช้รูปแบบการสร้างลายมือชื่อดิจิทัลครั้งละหลายรายการควรคำนึงถึงข้อกำหนดทางกฎหมายที่เกี่ยวข้องด้วยว่าอนุญาตให้เจ้าของลายมือชื่อดำเนินการได้หรือไม่

ทั้งนี้ ข้อเสนอแนะมาตรฐานฉบับนี้จะไม่ครอบคลุมถึง

- โครงสร้างสถาปัตยกรรมของระบบสารสนเทศ และจำนวนเครื่องบริการที่จำเป็นต้องใช้สำหรับระบบการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่ใช้การควบคุมจากระยะไกล
- รายละเอียดของส่วนประกอบต่าง ๆ ที่เกี่ยวข้องกับการสร้างลายมือชื่อดิจิทัล หรือส่วนประกอบที่อยู่นอกขอบเขตของระบบการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่ใช้การควบคุมจากระยะไกล เช่น ข้อกำหนดเกี่ยวกับแอปพลิเคชันสร้างลายมือชื่อดิจิทัล (SCA) ซึ่งเป็นแอปพลิเคชันที่เจ้าของลายมือชื่อใช้เพื่อลงลายมือชื่อดิจิทัลในเอกสาร
- ข้อกำหนดเกี่ยวกับบริการที่เชื่อถือได้ต่าง ๆ ที่เกี่ยวข้องกับการลงลายมือชื่อดิจิทัล เช่น ข้อกำหนดของระบบและผู้ให้บริการออกใบรับรอง (CA) ข้อกำหนดของระบบและผู้ให้บริการประทับเวลา (TSA)

ข้อเสนอแนะมาตรฐานฉบับนี้ประยุกต์จากข้อกำหนดและชุดมาตรฐานด้านเทคนิคว่าด้วยการลงลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ที่ใช้การควบคุมจากระยะไกลของสหภาพยุโรป

ข้อเสนอแนะมาตรฐานฉบับนี้มีรูปแบบของคำที่ใช้แสดงออกถึงคุณลักษณะของเนื้อหาเชิงบรรทัดฐาน (normative) และเนื้อหาเชิงให้ข้อมูล (informative) ดังต่อไปนี้

- “ต้อง” ใช้ระบุสิ่งที่เป็นข้อกำหนด ซึ่งต้องปฏิบัติตาม
- “ควร” ใช้ระบุสิ่งที่เป็นข้อแนะนำ
- “อาจ” ใช้ระบุสิ่งที่ยินยอมหรืออนุญาตให้ทำได้

2. บทนิยาม

ความหมายของคำที่ใช้ในข้อเสนอแนะมาตรฐานฉบับนี้ มีดังต่อไปนี้

2.1 การลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote signing หรือ server signing) หมายถึง การสร้างลายมือชื่อดิจิทัล โดยเจ้าของลายมือชื่ออาศัยระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ในการควบคุมกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) และสามารถรับรองได้ว่ากุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) นั้นอยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น (sole control)

2.2 การยืนยันตัวตน (authentication) หมายถึง กระบวนการตรวจสอบสิ่งที่ใช้ยืนยันตัวตน เพื่อยืนยันอัตลักษณ์ของบุคคลที่ใช้สิ่งที่ใช้ยืนยันตัวตนนั้น [3]

2.3 ปัจจัยของการยืนยันตัวตน (authentication factor) หมายถึง ข้อมูลและ/หรือวิธีการที่ใช้แสดงความเชื่อมโยงระหว่างตัวบุคคลกับอัตลักษณ์ของบุคคลในกระบวนการยืนยันตัวตน

2.4 สิ่งที่ใช้ยืนยันตัวตน (authenticator) หมายถึง สิ่งที่ใช้เชื่อมโยงอัตลักษณ์กับบุคคล ซึ่งบุคคลนั้นครอบครองและควบคุมเพื่อใช้ในการยืนยันตัวตน เช่น รหัสผ่าน ข้อมูลชีวภาพ [3]

2.5 แบบแสดงข้อมูลเพื่อลงลายมือชื่อ (data to be signed representation: DTBS/R) หมายถึง ข้อมูลที่ส่งให้กับระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ในรูปแบบที่ใช้คำนวณสร้างลายมือชื่อดิจิทัล เช่น ข้อมูลค่าแฮชของเอกสารและข้อมูลพารามิเตอร์อื่นสำหรับการสั่งให้สร้างลายมือชื่อดิจิทัล

2.6 ลายมือชื่อดิจิทัล (digital signature) หมายถึง ลายมือชื่ออิเล็กทรอนิกส์ที่ได้จากกระบวนการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ ซึ่งช่วยให้สามารถยืนยันตัวเจ้าของลายมือชื่อและตรวจพบการเปลี่ยนแปลงของข้อความและลายมือชื่ออิเล็กทรอนิกส์ได้รวมถึงการทำให้เจ้าของลายมือชื่อไม่สามารถปฏิเสธความรับผิดจากข้อความที่ตนเองลงลายมือชื่อได้ [4]

2.7 ใบรับรอง (certificate) หมายถึง ข้อมูลอิเล็กทรอนิกส์หรือการบันทึกอื่นใด ซึ่งยืนยันความเชื่อมโยงระหว่างเจ้าของลายมือชื่อกับข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์ [5]

2.8 กฎหมายเอดาส (eIDAS Regulation) หมายถึง กฎหมายในระดับ Regulation ของสหภาพยุโรปหมายเลข 910/2014 เกี่ยวกับการระบุตัวตนทางอิเล็กทรอนิกส์และการให้บริการที่เชื่อถือได้ [6]

2.9 ผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) หมายถึง หน่วยงานที่ให้บริการแก่บุคคลภายนอกเกี่ยวกับการพิสูจน์ตัวตน การออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน หรือการยืนยันตัวตน ทั้งนี้ ผู้พิสูจน์และยืนยันตัวตนอาจมอบหมายงานบางส่วนให้ผู้ให้บริการภายนอก (outsourcing) หรือตัวแทนของผู้พิสูจน์และยืนยันตัวตน (agent) โดยผู้พิสูจน์และยืนยันตัวตนรับผิดชอบเสมือนเป็นผู้ดำเนินการเอง [3]

2.10 อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote signature creation device: remote SCDev) หมายถึง อุปกรณ์หรือซอฟต์แวร์สำหรับสร้างลายมือชื่อดิจิทัลที่เจ้าของลายมือชื่อสามารถควบคุมได้จากระยะไกลผ่านโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) ที่สามารถรับประกันความเชื่อมั่นในระดับสูงได้ว่ากุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) นั้นอยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น

2.11 ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (signature activation data: SAD) หมายถึง ชุดของข้อมูลที่นำมาใช้ในโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) และสามารถรับประกันความเชื่อมั่นในระดับสูงได้ว่าการสร้างลายมือชื่อดิจิทัลด้วยโมดูลเข้ารหัสลับ (cryptographic module) นั้นเป็นการสั่งการในนามของเจ้าของลายมือชื่อ (signer) และเป็นการดำเนินการที่อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น (sole control)

2.12 โมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (signature activation module: SAM) หมายถึง ซอฟต์แวร์ที่ใช้ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ซึ่งสามารถรับประกันความเชื่อมั่นในระดับสูงได้ว่าการใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น

2.13 โพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (signature activation protocol: SAP) หมายถึง โพรโทคอลที่ใช้ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) เพื่อการควบคุมหรือสั่งให้สร้างลายมือชื่อดิจิทัลจากชุดแบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R)

2.14 แอปพลิเคชันสร้างลายมือชื่อดิจิทัล (signature creation application: SCA) หมายถึง แอปพลิเคชันที่ใช้ลงนามในเอกสารอิเล็กทรอนิกส์ด้วยลายมือชื่อดิจิทัลที่สร้างจากอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev)

2.15 บริการสร้างลายมือชื่อดิจิทัล (signature creation service: SCS) หมายถึง บริการของซอฟต์แวร์หรือฮาร์ดแวร์ของโมดูลเข้ารหัสลับ (cryptographic module) สำหรับใช้สร้างลายมือชื่อดิจิทัล

2.16 เจ้าของลายมือชื่อ (signer) หมายถึง ผู้ซึ่งถือข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์และสร้างลายมือชื่ออิเล็กทรอนิกส์นั้นในนามตนเองหรือแทนบุคคลอื่น [5]

2.17 ส่วนติดต่อของเจ้าของลายมือชื่อ (signer's interaction component: SIC) หมายถึง ส่วนประกอบในรูปแบบซอฟต์แวร์ และ/หรือฮาร์ดแวร์ที่ทำงานร่วมกับโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) โดยเจ้าของลายมือชื่อเป็นผู้สั่งการใช้งาน

2.18 กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) หมายถึง กุญแจส่วนตัว (private key) ในกระบวนวิธีเข้ารหัสลับแบบอสมมาตร เพื่อใช้สำหรับสร้างลายมือชื่อดิจิทัล

2.19 ผู้ให้บริการที่เชื่อถือได้ (trust service provider: TSP) หมายถึง บุคคลหรือนิติบุคคลที่ให้บริการต่าง ๆ ที่เกี่ยวข้องกับสร้างลายมือชื่อดิจิทัล ตามกฎหมายกำหนด

2.20 ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (trustworthy system supporting server signing: TW4S) หมายถึง ระบบที่มีสถาปัตยกรรมในรูปแบบเครื่องขอใช้บริการและเครื่องบริการ (client-server) ที่ใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) ภายใต้การควบคุมของเจ้าของลายมือชื่อ เพื่อสร้างลายมือชื่อดิจิทัล

99 ## 3. อักษรย่อ

100 อักษรย่อที่ใช้ในข้อเสนอแนะมาตรฐานฉบับนี้ มีดังต่อไปนี้

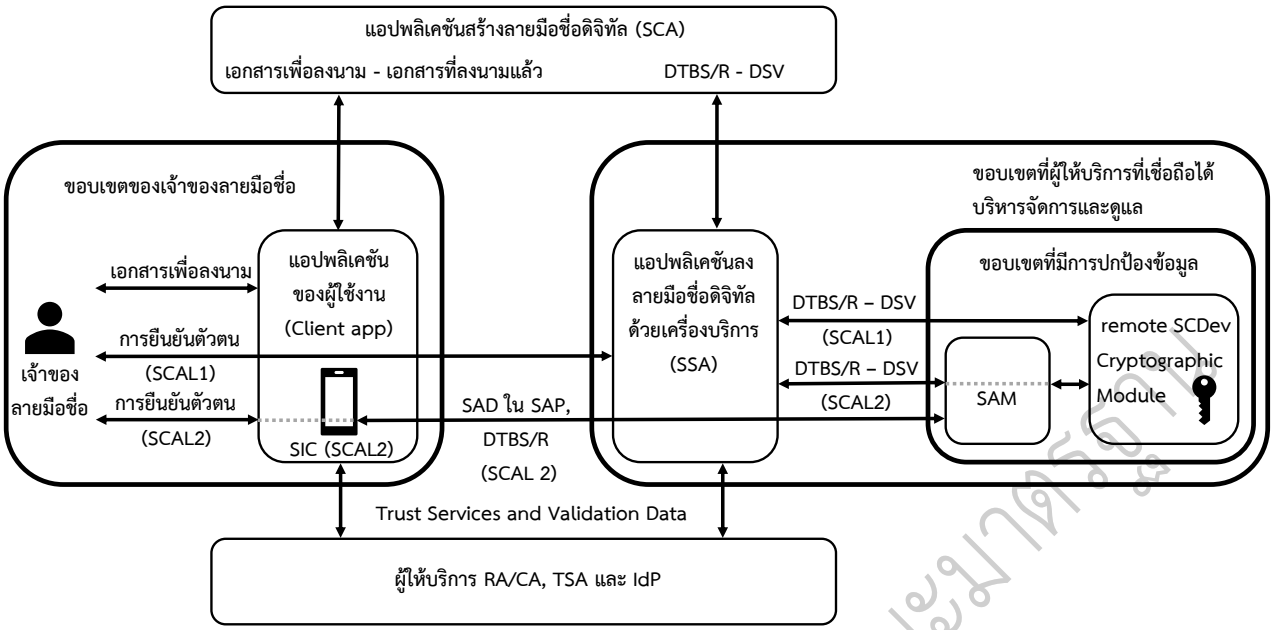
อักษรย่อ	คำเต็ม	คำภาษาไทย
CA	Certificate Authority	ผู้ให้บริการออกใบรับรอง
CC	Common Criteria	เกณฑ์ประเมินทั่วไปด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ [7] [8] [9]
CEN	European Committee for Standardization	คณะกรรมการด้านมาตรฐานของสหภาพยุโรป
DTBS/R	Data to Be Signed Representation	แบบแสดงข้อมูลเพื่อลงลายมือชื่อ
DSV	Digital Signature Value	ค่าลายมือชื่อดิจิทัล
EAL	Evaluation Assurance Level	ระดับความเข้มงวดในการประเมินตามเกณฑ์ประเมินทั่วไปด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ
ETSI	European Telecommunications Standards Institute	องค์กรด้านมาตรฐานโทรคมนาคมของสหภาพยุโรป
ISO/IEC	International Organization for Standardization/ International Electrotechnical Commission	องค์การระหว่างประเทศว่าด้วยการมาตรฐาน/ คณะกรรมาธิการระหว่างประเทศว่าด้วยมาตรฐานสาขาอิเล็กทรอนิกส์
IdP	Identity Provider	ผู้พิสูจน์และยืนยันตัวตน
RA	Registration Authority	ผู้ให้บริการรับลงทะเบียนใบรับรอง
SAD	Signature Activation Data	ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล
SAM	Signature Activation Module	โมดูลสั่งให้สร้างลายมือชื่อดิจิทัล
SAP	Signature Activation Protocol	โพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล
SCA	Signature Creation Application	แอปพลิเคชันสร้างลายมือชื่อดิจิทัล
SCAL	Sole Control Assurance Level	ระดับความเข้มงวดในการควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น
SCDev	Signature Creation Device	อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล
SCS	Signature Creation Service	บริการสร้างลายมือชื่อดิจิทัล
SIC	Signer’s Interaction Component	ส่วนติดต่อของเจ้าของลายมือชื่อ
SRA	Additional Security Requirements	ข้อกำหนดด้านความมั่นคงปลอดภัยเพิ่มเติม
SRC	Core Component Security Requirements	ข้อกำหนดด้านความมั่นคงปลอดภัยของส่วนประกอบหลัก

อักษรย่อ	คำเต็ม	คำภาษาไทย
SRG	General Security Requirements	ข้อกำหนดด้านความมั่นคงปลอดภัยทั่วไป
SSA	Server Signing Application	แอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ
SSASP	Server Signing Application Service Provider	ผู้ให้บริการแอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ
TSA	Time-stamping Authority	ผู้ให้บริการประทับเวลา
TSP	Trust Service Provider	ผู้ให้บริการที่เชื่อถือได้
TW4S	Trustworthy System Supporting Server Signing	ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้

4. ภาพรวมของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (trustworthy system supporting server signing: TW4S)

4.1 ภาพรวมของกระบวนการสร้างลายมือชื่อดิจิทัล

ผู้ใช้งานซึ่งเป็นเจ้าของลายมือชื่อที่ประสงค์จะลงลายมือชื่อดิจิทัลในเอกสารที่ต้องการลงนามทำงานผ่านแอปพลิเคชันของผู้ใช้งาน (client application) เพื่อติดต่อกับแอปพลิเคชันสร้างลายมือชื่อดิจิทัล (SCA) ซึ่งทำหน้าที่รับเอกสาร (document) และ/หรือค่าแฮชของเอกสาร (hash) และค่าพารามิเตอร์ที่เกี่ยวข้องกับการสร้างลายมือชื่อดิจิทัล และส่งต่อให้กับแอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) ซึ่งเป็นส่วนประกอบของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ที่อยู่ภายใต้ขอบเขตที่ผู้ให้บริการที่เชื่อถือได้บริหารจัดการและดูแล รูปที่ 1 แสดงขั้นตอนและข้อมูลที่เกี่ยวข้องในกระบวนการสร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกลที่เกิดขึ้นในส่วนประกอบต่าง ๆ ของระบบในภาพรวม



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

รูปที่ 1 ภาพรวมกระบวนการและข้อมูลในการสร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล

หมายเหตุ 1: กระบวนการสร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกลดังแสดงในรูปที่ 1 ไม่ได้แสดงรายละเอียดขั้นตอนของส่วนประกอบที่อยู่นอกขอบเขตของมาตรฐานฉบับนี้ เช่น ขั้นตอนการยืนยันตัวตนของเจ้าของลายมือชื่อ ขั้นตอนการอนุญาตให้เข้าถึงและใช้งานกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) หรือขั้นตอนการตรวจสอบความพร้อมใช้งานของใบรับรอง

หมายเหตุ 2: โมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) เป็นส่วนประกอบของระบบเฉพาะในกรณีที่บริการสร้างลายมือชื่อดิจิทัลในระดับความเข้มงวดฯ ขั้นสูง SCAL2 อ้างอิงตามข้อกำหนดระดับความเข้มงวดในการควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่นในข้อกำหนด 4.2

ขั้นตอนและข้อมูลในกระบวการสร้างลายมือชื่อดิจิทัลของแอปพลิเคชันสร้างลายมือชื่อดิจิทัล (SCA) และแอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) มีรายละเอียด ดังนี้

4.1.1 แอปพลิเคชันสร้างลายมือชื่อดิจิทัล (signature creation application: SCA)

กระบวนการสร้างลายมือชื่อดิจิทัลที่เกี่ยวข้องกับแอปพลิเคชันสร้างลายมือชื่อดิจิทัล (SCA) ประกอบด้วย 3 กิจกรรม

(1) แอปพลิเคชันสร้างลายมือชื่อดิจิทัล (SCA) รับเอกสาร และ/หรือ ค่าแฮชของเอกสารของผู้ใช้งานที่ประสงค์จะลงลายมือชื่อดิจิทัล ในกรณีที่ผู้ใช้งานนำเข้าข้อมูลในรูปแบบเอกสาร แอปพลิเคชันสร้างลายมือชื่อดิจิทัล (SCA) จะคำนวณค่าแฮชของเอกสารและจัดเตรียมให้อยู่ในรูปแบบข้อมูลเพื่อลงลายมือชื่อ (DTBS)

(2) แอปพลิเคชันสร้างลายมือชื่อดิจิทัล (SCA) นำค่าแฮชของเอกสารและค่าพารามิเตอร์ที่เกี่ยวข้องกับการสร้างลายมือชื่อดิจิทัล เช่น ตัวระบุใบรับรอง (certificate identifier) ข้อมูลคุณลักษณะการสร้าง

ลายมือชื่อ (attribute) มาจัดเตรียมเป็นข้อมูลในแบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R) เพื่อส่งข้อมูลต่อให้กับแอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) ของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) เพื่อสร้างลายมือชื่อดิจิทัล

(3) แอปพลิเคชันสร้างลายมือชื่อดิจิทัล (SCA) จะรับค่าลายมือชื่อดิจิทัล (DSV) ที่สร้างจากระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) มาเพื่อสร้างเอกสารที่ลงลายมือชื่อดิจิทัลตามรูปแบบที่ผู้ใช้งานร้องขอ เช่น การสร้างเอกสาร XML ที่ลงลายมือชื่อดิจิทัลด้วยรูปแบบ XAdES (XML Advanced Electronic Signature) การสร้างเอกสาร PDF ที่ลงลายมือชื่อดิจิทัลด้วยรูปแบบ PAdES (PDF Advanced Electronic Signature) การสร้างเอกสารที่บรรจุเอกสารต้นฉบับพร้อมค่าลายมือชื่อดิจิทัลด้วยรูปแบบ CAdES (CMS Advanced Electronic Signature) หรือการสร้างเอกสารสำหรับใส่ข้อมูลค่าลายมือชื่อดิจัทัลแยกออกจากเอกสารต้นฉบับ ในขั้นตอนนี้แอปพลิเคชันสร้างลายมือชื่อดิจิทัล (SCA) จะเรียกใช้บริการจากผู้ให้บริการภายนอกอื่นที่จำเป็นต่อการสร้างลายมือชื่อดิจิทัล เช่น การตรวจสอบความถูกต้องและสมบูรณ์ของใบรับรอง การตรวจสอบสถานะการพักใช้หรือการเพิกถอนใบรับรองจากผู้ให้บริการออกใบรับรอง (CA) หรือการขอโทเคนประทับเวลา (time-stamp token) จากผู้ให้บริการประทับเวลา (TSA)

4.1.2 แอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (server signing application: SSA)

กระบวนการสร้างลายมือชื่อดิจิทัลที่เกี่ยวข้องกับแอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) ซึ่งเป็นส่วนประกอบหนึ่งของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) และอยู่ภายใต้ขอบเขตที่ผู้ให้บริการที่เชื่อถือได้บริหารจัดการและดูแล (TSP protected environment) คือ การนำข้อมูลในแบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R) ไปสร้างลายมือชื่อดิจิทัลด้วยกุญแจส่วนตัวภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น กุญแจส่วนตัวหรือกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) นี้ ถูกจัดเก็บหรือรักษาความมั่นคงปลอดภัยของกุญแจไว้ด้วยอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote SCDev) ซึ่งเป็นอีกส่วนประกอบหนึ่งของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ที่ทำหน้าที่สร้างลายมือชื่อดิจิทัล โดยกระบวนการสร้างลายมือชื่อดิจิทัลผ่านแอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) ประกอบด้วย 2 กิจกรรม

(1) การสั่งให้สร้างลายมือชื่อดิจิทัล (signature activation) แอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) ใช้อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote SCDev) เพื่อสร้าง เก็บรักษา และใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) ภายใต้การควบคุมของเจ้าของลายมือชื่อที่ได้รับอนุญาต และทำการยืนยันตัวตนเจ้าของลายมือชื่อเพื่อสั่งให้สร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยไกลสำหรับแบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R) ด้วยกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) กระบวนการนี้ทำให้มีความมั่นใจว่ากุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อ

ระดับความมั่นใจว่าการควบคุมกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลอยู่ภายใต้เจ้าของลายมือชื่อหรือระดับความเข้มงวดในการควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น (ระดับความเข้มงวดฯ) กำหนดไว้เป็น 2 ระดับ ประกอบด้วย

- ระดับความเข้มงวดฯ พื้นฐาน SCAL1 เจ้าของลายมือชื่อ (signer) ยืนยันตัวตนกับแอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) และ
- ระดับความเข้มงวดฯ ขั้นสูง SCAL2 เจ้าของลายมือชื่อ (signer) ยืนยันตัวตนกับโมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM)

กระบวนการยืนยันตัวตนนี้เป็นการยืนยันและทำให้มีความมั่นใจว่ากุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น (sole control) อ้างอิงตามข้อกำหนดระดับความเข้มงวดในการควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่นในข้อกำหนด 4.2

(2) การสร้างลายมือชื่อดิจิทัล (signature creation) ลายมือชื่อดิจิทัลถูกสร้างขึ้นในอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote SCDev) หลังจากขั้นตอนการสั่งให้สร้างลายมือชื่อดิจิทัล (signature activation) เมื่อแอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) สามารถยืนยันตัวตน (authentication) เจ้าของลายมือชื่อ (signer) ได้เป็นผลสำเร็จแล้ว หรือโมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) ได้ทวนสอบข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ได้ผลถูกต้องแล้ว จึงจะอนุญาต (authorization) ให้อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote SCDev) เข้าถึงกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) เพื่อใช้สร้างลายมือชื่อดิจิทัลด้วยโมดูลเข้ารหัสลับ (cryptographic module) จากแบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R)

4.2 ระดับความเข้มงวดในการควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น (sole control assurance level: SCAL)

ข้อเสนอแนะมาตรฐานฉบับนี้แบ่งระดับความเข้มงวดในการควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น (SCAL) ของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) เป็น 2 ระดับ ดังนี้

4.2.1 ระดับความเข้มงวดฯ พื้นฐาน SCAL1

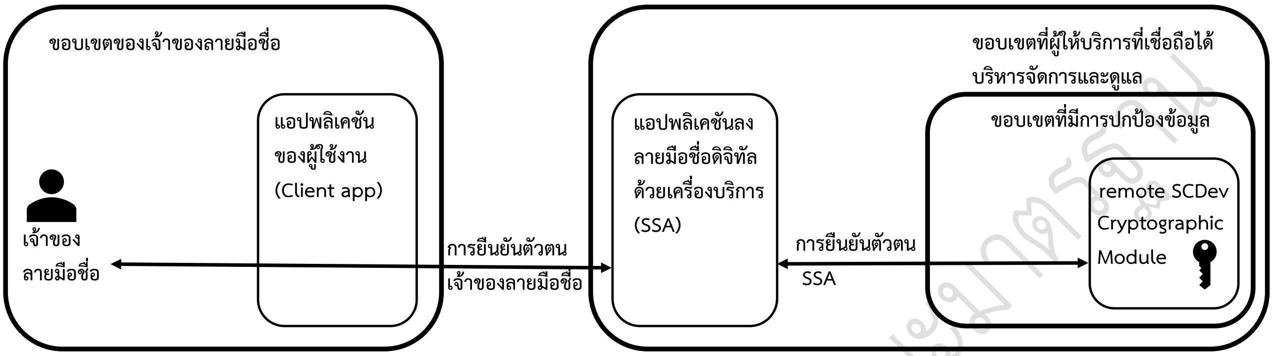
ระดับความเข้มงวดฯ พื้นฐาน SCAL1 มีคุณสมบัติ ดังนี้

(1) ความน่าเชื่อถือในการควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่นของการใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) อยู่ในระดับพื้นฐาน อาจใช้กับธุรกรรมที่ทำที่ไม่ได้มีมูลค่าสูง หรือไม่ได้มีความสำคัญ

(2) ความลับและความครบถ้วนสมบูรณ์ของกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) ได้รับการรักษาไว้โดยอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote SCDev)

(3) แอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) ซึ่งเป็นซอฟต์แวร์ที่อยู่ภายใต้ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ทำหน้าที่ยืนยันตัวตนเจ้าของลายมือชื่อ (signer) จนเป็นผลสำเร็จก่อน ถึงจะสั่งให้สร้างลายมือชื่อดิจิทัลได้ด้วยกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) ของเจ้าของลายมือชื่อ

(4) แอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) สามารถสั่งให้อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote SCDev) สร้างลายมือชื่อดิจิทัลได้โดยตรง โดยคำสั่งการสร้างลายมือชื่อดิจิทัลหนึ่งหลังการยืนยันตัวตนจนเป็นผลสำเร็จ อาจมีผลให้สามารถใช้งานได้อยู่ในช่วงระยะเวลาที่กำหนดไว้ช่วงหนึ่งหรือใช้สร้างลายมือชื่อดิจิทัลที่กำหนดไว้จำนวนหนึ่ง เพื่อให้รองรับการสร้างลายมือชื่อดิจิทัลครั้งละหลายรายการได้



รูปที่ 2 การยืนยันตัวตนเพื่อสั่งให้สร้างลายมือชื่อดิจิทัลระดับความเข้มงวดฯ พื้นฐาน SCAL1

4.2.2 ระดับความเข้มงวดฯ ขั้นสูง SCAL2

ระดับความเข้มงวดฯ ขั้นสูง SCAL2 มีคุณสมบัติ ดังนี้

(1) ความน่าเชื่อถือในการควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่นของการใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) อยู่ในระดับสูง อาจใช้กับธุรกรรมที่ทำธุรกรรมที่ทำที่มีมูลค่าสูง หรือมีความสำคัญ

(2) อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยไกล (remote SCDev) ทำงานร่วมกับโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) เพื่อยืนยันด้วยความมั่นใจในระดับสูงได้ว่ากิจกรรมต่าง ๆ กับลายมือชื่อดิจิทัลนั้นอยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อ

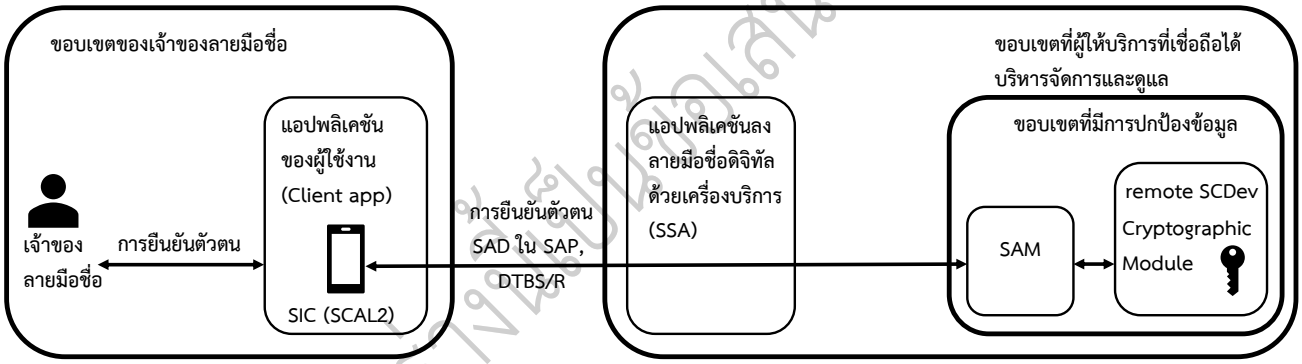
(3) แอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) ติดต่อกับโมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) ซึ่งเป็นส่วนประกอบภายในของอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยไกล (remote SCDev) ผ่านช่องทางการสื่อสารที่มั่นคงปลอดภัย และโมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) ทำหน้าที่ยืนยันตัวตนเจ้าของลายมือชื่อด้วยโพรโทคอลสร้างลายมือชื่อดิจิทัล (SAP) ซึ่งใช้ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) จากเจ้าของลายมือชื่อโดยตรง และพิจารณาเลือกกุญแจที่เชื่อมโยงกับเจ้าของลายมือชื่อเพื่อใช้สร้างลายมือชื่อดิจิทัล

(4) เมื่อการยืนยันตัวตนเจ้าของลายมือชื่อ (signer) จนเป็นผลสำเร็จ อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote SCDev) จะอนุญาตให้ใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) เพื่อสร้างลายมือชื่อดิจิทัลได้อยู่ในช่วงระยะเวลาที่กำหนดไว้ช่วงหนึ่งหรือใช้สร้างลายมือชื่อดิจิทัลที่กำหนดไว้จำนวนหนึ่งได้ แต่ในทุกรายการที่สร้างลายมือชื่อดิจิทัล ต้องมีการสร้างข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) สำหรับทุกคำสั่งสร้างลายมือชื่อดิจิทัล โดยข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) อาจเชื่อมโยงกับชุดแบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R) ได้หลายข้อมูลเพื่อให้รองรับการสร้างลายมือชื่อดิจิทัลครั้งละหลายรายการได้

(5) การยืนยันตัวตนเจ้าของลายมือชื่อ (signer) สามารถทำได้ผ่านส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) เพื่อสร้างความเชื่อมโยงระหว่างเจ้าของลายมือชื่อ (signer) กับลายมือชื่อดิจิทัลที่สร้างตามข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD)

(6) โมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) ทำหน้าที่ตรวจสอบความถูกต้องของข้อมูลในข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) โดย

- ถ้าข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ถูกสร้างขึ้นจากส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ต้องถูกส่งผ่านช่องทางสื่อสารที่มั่นคงปลอดภัยด้วยโพรโทคอลสร้างลายมือชื่อดิจิทัล (SAP) จากส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) ไปยังโมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) เพื่อทวนสอบความถูกต้อง
- ถ้าข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ไม่ได้ถูกสร้างขึ้นจากส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ต้องถูกสร้างในขณะที่เจ้าของลายมือชื่อยืนยันตัวตนเป็นผลสำเร็จด้วยส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) และถูกส่งผ่านช่องทางสื่อสารที่มั่นคงปลอดภัยด้วยโพรโทคอลสร้างลายมือชื่อดิจิทัล (SAP) ไปยังโมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) เพื่อทวนสอบความถูกต้อง



รูปที่ 3 การยืนยันตัวตนเพื่อสั่งให้สร้างลายมือชื่อดิจิทัลระดับความเข้มงวดฯ ขั้นสูง SCAL2

การเลือกระดับความเข้มงวดในการควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่นสามารถพิจารณาใช้งานให้เหมาะสมกับลักษณะ ประเภท หรือขนาดของธุรกรรมที่ทำ หรือเป็นไปตามที่กฎหมายกำหนดไว้

4.3 การพิสูจน์และยืนยันตัวตนเจ้าของลายมือชื่อ

4.3.1 การพิสูจน์ตัวตน

ระดับความเข้มงวดฯ พื้นฐาน SCAL1: การพิสูจน์ตัวตนของเจ้าของลายมือชื่อ ต้องมีความเข้มงวดของการพิสูจน์ตัวตนที่ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน IAL1 ขึ้นไป อ้างอิง ขมธอ. 19 [10]

ระดับความเข้มงวดฯ ขั้นสูง SCAL2: การพิสูจน์ตัวตนของเจ้าของลายมือชื่อ ต้องมีความเข้มงวดของการพิสูจน์ตัวตนที่ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน IAL2 ขึ้นไป อ้างอิง ขมธอ. 19 [10]

4.3.2 การยืนยันตัวตน

ระดับความเข้มงวดฯ พื้นฐาน SCAL1: การยืนยันตัวตนเจ้าของลายมือชื่อ ต้องใช้วิธีการยืนยันตัวตนที่มีความเข้มงวดในการยืนยันตัวตนที่ระดับความน่าเชื่อถือของการยืนยันตัวตน AAL1 ขึ้นไป อ้างอิง ขมธอ. 20 [11]

ระดับความเข้มงวดฯ ขั้นสูง SCAL2: การยืนยันตัวตนเจ้าของลายมือชื่อ ต้องใช้วิธีการยืนยันตัวตนที่มีความเข้มงวดในการยืนยันตัวตนที่ระดับความน่าเชื่อถือของการยืนยันตัวตน AAL2 ขึ้นไป อ้างอิง ขมธอ. 20 [11]

4.3.3 เป้าประสงค์ของการยืนยันตัวตน

4.3.3.1 ระดับความเข้มงวดฯ พื้นฐาน SCAL1

(1) เจ้าของลายมือชื่อต้องยืนยันตัวตนกับแอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) จนสำเร็จก่อน จึงจะได้รับอนุญาตให้เข้าถึงส่วนปฏิบัติงานเกี่ยวข้องกับลายมือชื่อดิจิทัล

(2) แอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) ต้องเชื่อมโยงกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) ของเจ้าของลายมือชื่อไปยังปัจจัยของการยืนยันตัวตน (authentication factor) ของเจ้าของลายมือชื่อ

4.3.3.2 ระดับความเข้มงวดฯ ขั้นสูง SCAL2

(1) ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ต้องถูกสร้างขึ้น หรือเป็นผลลัพธ์ที่เกิดจากการติดต่อที่มีความมั่นคงปลอดภัยระหว่างโมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) กับส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) ผ่านแอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) เพื่ออนุญาตให้สร้างลายมือชื่อดิจิทัลในอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev)

(2) ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ต้องถูกส่งให้กับโมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) ผ่านแอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) เพื่ออนุญาตให้อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) สร้างลายมือชื่อดิจิทัลกับแบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R) เฉพาะที่ระบุไว้

4.3.4 การพิสูจน์และยืนยันตัวตนจากผู้ให้บริการภายนอก

การพิสูจน์และยืนยันตัวตนต่าง ๆ ของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) อาจใช้บริการพิสูจน์และยืนยันตัวตนจากผู้พิสูจน์และยืนยันตัวตน (IdP) ซึ่งเป็นผู้ให้บริการภายนอกได้

ผู้ให้บริการที่เชื่อถือได้ต้องทำให้มีความมั่นใจว่ากระบวนการพิสูจน์และยืนยันตัวตนที่ใช้บริการจากผู้ให้บริการภายนอกสอดคล้องตามข้อกำหนดด้านความมั่นคงปลอดภัยของข้อเสนอแนะมาตรฐานฉบับนี้

4.3.4.1 ระดับความเข้มงวดฯ พื้นฐาน SCAL1

ผู้ให้บริการที่เชื่อถือได้ ต้องทำให้มีความมั่นใจว่าผู้ให้บริการภายนอกได้ปฏิบัติตามข้อกำหนดต่าง ๆ เกี่ยวกับการพิสูจน์และยืนยันตัวตนที่สอดคล้องตามรายละเอียดที่ระบุไว้ในข้อกำหนด 5.2.2.1(1)

4.3.4.2 ระดับความเข้มงวดฯ ขั้นสูง SCAL2

ผู้ให้บริการที่เชื่อถือได้ ต้องทำให้มีความมั่นใจว่าผู้ให้บริการภายนอกได้ปฏิบัติตามข้อกำหนดต่าง ๆ เกี่ยวกับการพิสูจน์และยืนยันตัวตนที่สอดคล้องตามรายละเอียดที่ระบุไว้ในข้อกำหนด 5.3.1.1(1) และต้องทำให้มีความมั่นใจว่า ทั้งกระบวนการพิสูจน์และยืนยันตัวตนและคุณสมบัติของผู้ให้บริการภายนอกนั้นเป็นไปตามที่กฎหมายธุรกรรมทางอิเล็กทรอนิกส์กำหนด [5]

4.4 กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) และโมดูลเข้ารหัสลับ (cryptographic module)

การสร้างลายมือชื่อดิจิทัลในระดับความเข้มงวดฯ พื้นฐาน SCAL1 ไม่ได้มีข้อกำหนดเกี่ยวกับกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) หรือกุญแจส่วนตัว (private key) ในกระบวนวิธีเข้ารหัสลับแบบอสมมาตร (asymmetric cryptography) ว่าต้องสร้าง เก็บรักษา หรือใช้งานภายในโมดูลเข้ารหัสลับ (cryptographic module) เช่น อุปกรณ์ฮาร์ดแวร์ HSM หรือ smart card ดังนั้น กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลสามารถถูกจัดเก็บได้ในรูปแบบไฟล์ข้อมูล และสามารถใช้อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) ในรูปแบบระบบซอฟต์แวร์เพื่อนำกุญแจในรูปแบบไฟล์ข้อมูลนั้นมาสร้างลายมือชื่อดิจิทัลก็ได้

เมื่อกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลอยู่ในรูปแบบไฟล์ข้อมูล ผู้ให้บริการระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ควรจัดให้มีมาตรการด้านความมั่นคงปลอดภัยเพื่อรักษาความพร้อมใช้งานและความครบถ้วนสมบูรณ์ของไฟล์ไม่ให้ถูกเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต

อย่างไรก็ตาม ข้อเสนอแนะมาตรฐานฉบับนี้เสนอแนะให้จัดเตรียมอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) ติดตั้งในขอบเขตที่มีการป้องกันการเปลี่ยนแปลงข้อมูล (tamper protected environment) ตามรายละเอียดที่ได้ระบุไว้ในข้อกำหนด 4.9.1 และควรเป็นอุปกรณ์/ระบบในรูปแบบฮาร์ดแวร์สำหรับโมดูลเข้ารหัสลับ (cryptographic module) เพื่อรักษาความมั่นคงปลอดภัยของกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) และเป็นอุปกรณ์/ระบบที่มีการรับรองตามมาตรฐานด้านความมั่นคงปลอดภัยของระบบสารสนเทศที่ได้รับการยอมรับในระดับสากล เช่น CEN EN 419211-5 [12]

4.5 ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (signature activation data: SAD)

ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ในระดับความเข้มงวดฯ ขั้นสูง SCAL2 โมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) ต้องใช้ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) เพื่อรับประกันว่ากุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อและการสั่งให้สร้างลายมือชื่อดิจิทัลในระดับความเข้มงวดฯ ขั้นสูง SCAL2 เป็นไปตามเงื่อนไขและข้อกำหนดในส่วนการยืนยันตัวตนเจ้าของลายมือชื่อ ตามรายละเอียดที่ได้ระบุไว้ในข้อกำหนด 5.3.1.2

เงื่อนไขและข้อกำหนดข้างต้น อาจกำหนดไว้ในข้อมูลสั่งให้ลายมือชื่อดิจิทัล (SAD) และมีความเป็นไปได้ว่าการยืนยันตัวตนเจ้าของลายมือชื่อ จะเกิดขึ้นก่อนการสร้างข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) เช่น การยืนยันตัวตนจากผู้ให้บริการภายนอก

ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) เป็นชุดข้อมูลหรือผลลัพธ์จากการเข้ารหัสลับข้อมูล ตามรายละเอียดที่ได้ระบุไว้ในข้อกำหนด 5.3.1.2

ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) เป็นข้อมูลสนับสนุนในการยืนยันตัวตนของเจ้าของลายมือชื่อทางตรงหรือทางอ้อม

เมื่อการยืนยันตัวตนเจ้าของลายมือชื่อเกิดขึ้นก่อนการสร้างข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ข้อมูลสั่งให้ลายมือชื่อดิจิทัล (SAD) ควรมีข้อมูลผลการยืนยันตัวตนเพื่อใช้ระบุหรือเชื่อมโยงไปยังเจ้าของลายมือชื่อดิจิทัล ข้อมูลผลการยืนยันตัวตนอาจเป็นข้อมูลที่ได้รับจากส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) หรือจากผู้พิสูจน์และยืนยันตัวตน (idP) ที่เชื่อถือได้ และแหล่งข้อมูลของข้อมูลผลการยืนยันตัวตน ต้องมีการยืนยันได้ว่าแหล่งข้อมูลนั้นมีความถูกต้องด้วย

4.6 โพรโทคอลเพื่อสั่งให้สร้างลายมือชื่อดิจิทัล (signature activation protocol: SAP)

โพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) ต้องถูกออกแบบให้สามารถใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลด้วยโมดูลเข้ารหัสลับ (cryptographic module) ได้อย่างมั่นคงปลอดภัยสำหรับการสั่งให้สร้างลายมือชื่อดิจิทัลจากเจ้าของลายมือชื่อ

โพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) เป็นโพรโทคอลที่เจ้าของลายมือชื่อใช้ส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) สื่อสารกับระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) เพื่อสร้างข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD)

การออกแบบโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) ต้องมีการตรวจสอบ อย่างน้อย ดังนี้

(1) การยืนยันตัวตนเจ้าของลายมือชื่อเมื่อมีการเรียกใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล

(2) ความถูกต้องแท้จริงของคำร้องการสร้างลายมือชื่อดิจิทัลในข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD)

(3) กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลที่ถูกเรียกใช้มีความถูกต้องและสมบูรณ์ของการใช้สร้างลายมือชื่อดิจิทัล

(4) การสื่อสารข้อมูลระหว่างส่วนประกอบต่าง ๆ ที่เกี่ยวข้องกับข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) มีความมั่นคงปลอดภัย

ในกรณีที่กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล ไม่ได้ใช้ลงนามในกระบวนการขอออกใบรับรอง โพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) ควรตรวจสอบความเชื่อมโยงและความถูกต้องของใบรับรองกับกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล

4.7 ส่วนติดต่อของเจ้าของลายมือชื่อ (signer's interaction component: SIC)

ส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) เป็นส่วนประกอบของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ในระดับความเข้มงวดฯ ขั้นสูง SCAL2 ในรูปแบบซอฟต์แวร์ และ/หรือ ฮาร์ดแวร์ ที่อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อในขอบเขตของเจ้าของลายมือชื่อตามรายละเอียดที่ระบุไว้ในข้อกำหนด 4.9.3

การใช้งานส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) นี้มีความจำเป็นในโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) และมีความเป็นจำเป็นในกระบวนการสร้างลายมือชื่อดิจิทัลด้วยอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev)

ส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) จะทำงานร่วมกับโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) เพื่อยืนยันตัวตนเจ้าของลายมือชื่อและสร้างข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) โดยมีรายละเอียด ดังนี้

(1) ส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) สามารถสร้างข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ได้เองโดยตรง หรือ

(2) ส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) สามารถใช้เพื่อยืนยันตัวตนเจ้าของลายมือชื่อ (signer) และผลการยืนยันตัวตน (assertion) ที่ระบุเจ้าของลายมือชื่อจะถูกนำไปใช้สร้างข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD)

ส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) สามารถอยู่ในรูปแบบต่าง ๆ เช่น

(1) แอปพลิเคชันบนเว็บบราวเซอร์ เช่น เว็บในรูปแบบ POST และมีการรักษาความมั่นคงปลอดภัยของข้อมูลด้วย TLS (transport layer security)

(2) แอปพลิเคชันบนอุปกรณ์เคลื่อนที่ เช่น โทรศัพท์สมาร์ทโฟน หรือ แท็บเล็ต

(3) ส่วนประกอบที่มีความมั่นคงของข้อมูลของโทรศัพท์เคลื่อนที่ เช่น ชิป Secure Element ของโทรศัพท์เคลื่อนที่

(4) อุปกรณ์เข้ารหัสลับ (cryptographic device) เช่น โทเคนแบบ FIDO หรือ โทเคนอิเล็กทรอนิกส์ (e-Token)

ส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) เป็นส่วนทำให้เกิดการเชื่อมโยงเจ้าของลายมือชื่อกับกระบวนการสร้างลายมือชื่อดิจิทัลในโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP)

4.8 โมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (signature activation module: SAM)

โมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) เป็นซอฟต์แวร์ที่ใช้ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ที่สามารถรับประกันได้ว่า กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลถูกใช้งานในระดับความเข้มงวดฯ ขั้นสูง SCAL2

โมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) กำหนดให้ใช้งานภายใต้ขอบเขตที่มีการป้องกันการเปลี่ยนแปลงข้อมูล (tamper protected environment) ตามรายละเอียดที่ระบุไว้ในข้อกำหนด 4.9.1

ในกรณีที่โมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) ติดตั้งและใช้งานภายใต้ขอบเขตที่มีการป้องกันการเปลี่ยนแปลงข้อมูลที่อยู่คนละพื้นที่กับอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) การสื่อสารข้อมูลระหว่างโมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) และอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) ที่อยู่คนละพื้นที่ให้ดำเนินการผ่านช่องทางสื่อสารที่มีความมั่นคงปลอดภัย

4.9 ขอบเขตสภาพแวดล้อม

4.9.1 ขอบเขตที่มีการป้องกันการเปลี่ยนแปลงข้อมูล (tamper protected environment)

ขอบเขตที่มีการป้องกันการเปลี่ยนแปลงข้อมูล เป็นพื้นที่ที่ผู้ให้บริการที่เชื่อถือได้บริหารจัดการและดูแล และมีการปิดกั้นไม่ให้เข้าถึงได้โดยตรงจากเครือข่ายอินเทอร์เน็ต และสามารถยืนยันความครบถ้วนสมบูรณ์ของการทำงานของชุดคำสั่งที่อยู่ในพื้นที่นี้ได้

ชุดคำสั่งของส่วนประกอบในพื้นที่นี้ ปกป้องการใช้งานของกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) และควบคุมการสั่งให้สร้างลายมือชื่อให้อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อ

ขอบเขตที่มีการป้องกันการเปลี่ยนแปลงข้อมูล ปกป้องข้อมูลเชื่อมโยงระหว่างกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลกับเจ้าของลายมือชื่อ (ข้อมูลเชื่อมโยงนี้ถูกสร้างและตรวจสอบได้เมื่อจำเป็นสำหรับการสร้างลายมือชื่อดิจิทัล)

สำหรับระดับความเข้มงวดฯ พื้นฐาน SCAL1 แนะนำให้สร้างและใช้งานกุญแจส่วนตัวหรือกุญแจลับภายในขอบเขตที่มีการป้องกันการเปลี่ยนแปลงข้อมูลนี้

สำหรับระดับความเข้มงวดฯ ขั้นสูง SCAL2 กำหนดให้สร้างและใช้งานกุญแจส่วนตัวหรือกุญแจลับภายในขอบเขตที่มีการป้องกันการเปลี่ยนแปลงข้อมูลนี้ นอกจากนั้น ยังกำหนดให้การใช้งานซอฟต์แวร์ของโมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) อยู่ภายในขอบเขตที่มีการป้องกันการเปลี่ยนแปลงข้อมูลนี้ด้วย

4.9.2 ขอบเขตที่ผู้ให้บริการที่เชื่อถือได้บริหารจัดการและดูแล (TSP protected environment)

ขอบเขตที่ผู้ให้บริการที่เชื่อถือได้ควบคุมหรือบริหารจัดการเป็นพื้นที่มีมาตรการปกป้องการโจมตีจากเครือข่ายอินเทอร์เน็ต และสามารถรับการเชื่อมต่อจากระบบภายนอกต่าง ๆ เช่น แอปพลิเคชันของผู้ใช้งาน (client application) แอปพลิเคชันสร้างลายมือชื่อดิจิทัล (SCA) ระบบของผู้ให้บริการออกใบรับรอง (CA) และระบบของผู้ให้บริการลงทะเบียนใบรับรอง (RA) เป็นต้น

ขอบเขตนี้สามารถจัดเก็บข้อมูลในรูปแบบที่มีการรักษาความมั่นคงปลอดภัยอย่างเหมาะสมได้ เช่น กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล และข้อมูลเชื่อมโยงระหว่างกุญแจกับเจ้าของลายมือชื่อ

ผู้ให้บริการที่เชื่อถือได้ปกป้องขอบเขตนี้เพื่อปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยของข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) และโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) และสร้างข้อผูกพันให้กับผู้ให้บริการลงทะเบียนใบรับรอง (RA) ว่าการลงทะเบียนใบรับรองนั้นอยู่ให้อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่อยู่ภายใต้การควบคุมของผู้อื่น

4.9.3 ขอบเขตของเจ้าของลายมือชื่อ (signer's environment)

ขอบเขตของเจ้าของลายมือชื่อเป็นพื้นที่ที่เจ้าของลายมือชื่อเข้าถึงเจ้าของลายมือชื่อรับผิดชอบต่อการปกป้องพื้นที่นี้ เมื่อเจ้าของลายมือชื่อใช้พื้นที่ที่ให้บริการโดยบุคคลที่สาม ผู้ให้บริการนั้นมีความรับผิดชอบต่อการปกป้องพื้นที่นี้

ขอบเขตของเจ้าของลายมือชื่อประกอบด้วยส่วนประกอบทั่วไปที่อาจถูกนำไปใช้เพื่อจัดเตรียมเอกสารสำหรับนำไปลงลายมือชื่อ จัดรูปแบบของลายมือชื่อที่ต้องการลงนามในเอกสาร และใช้งานส่วนติดต่อของเจ้าของลายมือชื่อ (SIC)

ส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) ถูกใช้งานโดยเจ้าของลายมือชื่อเพื่อสร้างข้อมูลเชื่อมโยงระหว่างเจ้าของลายมือชื่อและการสั่งให้สร้างลายมือชื่อผ่านโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP)

ถึงแม้ว่าจะไม่มีข้อกำหนดในข้อเสนอแนะมาตรฐานฉบับนี้ ที่ระบุให้ตรวจรับรอง (certification) ส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) อย่างไรก็ตาม การออกแบบและการพัฒนาส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) จำเป็นต้องพิจารณาข้อกำหนดต่าง ๆ ในการจัดส่ง/ประมวลผลข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) และการทำงานร่วมกันระหว่างส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) กับโมดูลสั่งให้

สร้างลายมือชื่อดิจิทัล (SAM) ผ่านโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) และรวมถึงการยืนยันตัวตนเจ้าของลายมือชื่อ

5. ข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้

การลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote signing หรือ server signing) ด้วยระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ทำให้มีความมั่นใจได้ว่ากุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น (sole control) ตามข้อกำหนดลายมือชื่ออิเล็กทรอนิกส์ของกฎหมายธุรกรรมทางอิเล็กทรอนิกส์

ทั้งนี้ ข้อเสนอแนะมาตรฐานฉบับนี้กำหนดข้อกำหนดด้านความมั่นคงปลอดภัยที่จำเป็นต่อการให้บริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (ข้อกำหนด 5.1) ข้อกำหนดด้านความมั่นคงปลอดภัยของส่วนประกอบหลักของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) (ข้อกำหนด 5.2) ข้อกำหนดด้านความมั่นคงปลอดภัยเพิ่มสำหรับระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ในระดับความเข้มงวดฯ ขั้นสูง SCAL2 (ข้อกำหนด 5.3) และข้อกำหนดมาตรฐานความมั่นคงปลอดภัยสำหรับระบบ/อุปกรณ์ของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) (ข้อกำหนด 5.4)

5.1 ข้อกำหนดด้านความมั่นคงปลอดภัยพื้นฐานที่จำเป็น (general security requirements: SRG)

5.1.1 การบริหารจัดการ (SRG_M)

กำหนดแนวทางในการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยที่เหมาะสมของผู้ให้บริการที่เชื่อถือได้สำหรับบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote siging หรือ server signing) ด้วยระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) เช่น ข้อกำหนดด้านความมั่นคงปลอดภัยทางกายภาพ ข้อกำหนดสำหรับเจ้าหน้าที่หรือบุคลากรของผู้ให้บริการ และข้อกำหนดด้านความมั่นคงปลอดภัยอื่น ๆ เพื่อให้การให้บริการลงลายมือชื่อดิจิทัลมีคามน่าเชื่อถือและอ้างอิงได้ตามข้อกำหนดด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับผู้ให้บริการที่เชื่อถือได้ในระดับสากล เช่น มาตรฐาน EN 319401 [13]

5.1.1.1 การบริหารจัดการระบบและความมั่นคงปลอดภัยของระบบ (SRG_M.1)

(1) ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องรองรับการแบ่งแยกผู้ใช้งานที่มีสิทธิเข้าถึงระบบที่แตกต่างกัน

(2) ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องรองรับการกำหนดบทบาทผู้ใช้งานที่มีสิทธิสูง (privilege role) อย่างน้อย ดังนี้

- เจ้าหน้าที่รักษาความมั่นคงปลอดภัยระบบ (security officer) ซึ่งมีหน้าที่รับผิดชอบในการจัดเตรียมมาตรการด้านความมั่นคงปลอดภัยของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ให้สอดคล้องกับแนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยที่กำหนดไว้ และสามารถเข้าถึงข้อมูลที่เกี่ยวข้องกับมาตรการด้านความมั่นคงปลอดภัยทั้งหมดได้

- เจ้าหน้าที่ผู้ดูแลระบบ (system administrator) ซึ่งได้รับมอบหมายให้สามารถติดตั้ง ตั้งค่า และซ่อมบำรุงระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) แต่ถูกควบคุมการเข้าถึงข้อมูลที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบ
- เจ้าหน้าที่ผู้ปฏิบัติงาน (system operator) ซึ่งมีหน้าที่ปฏิบัติงานประจำวันบนระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) และได้รับอนุญาตให้ปฏิบัติงานสำรองหรือกู้คืนข้อมูลของระบบ
- ผู้ตรวจสอบระบบ (system auditor) ซึ่งได้รับมอบหมายให้เข้าถึงข้อมูลที่เก็บไว้เพื่อเป็นหลักฐานในระยะยาว (archive) และข้อมูลบันทึกกิจกรรมสำหรับตรวจสอบ (audit log) ของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) เพื่อวัตถุประสงค์ในการตรวจสอบการปฏิบัติงานและการบริหารจัดการระบบตามแนวนโยบายการรักษาความมั่นคงปลอดภัย

เจ้าหน้าที่รักษาความมั่นคงปลอดภัยระบบ (security officer) และเจ้าหน้าที่ดูแลระบบ (system administrator) เป็นผู้ใช้งานที่มีสิทธิสูงของระบบ (privilege system user)

เจ้าหน้าที่ผู้ปฏิบัติงาน (system operator) และผู้ตรวจสอบระบบ (auditor) เป็นผู้ใช้งานที่มีสิทธิสูงของระบบ แต่ไม่สามารถบริหารจัดการหรือตั้งค่าต่าง ๆ ในระบบ

(3) ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องรองรับการกำหนดบทบาทผู้ใช้งานที่มีสิทธิพื้นฐาน (non-privilege role) อย่างน้อย ดังนี้

- เจ้าของลายมือชื่อ (signer) ซึ่งได้รับอนุญาตใช้ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ด้วยการส่งข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ซึ่งเป็นส่วนหนึ่งของโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) เพื่อสั่งให้ลงลายมือชื่อดิจิทัลในเอกสารหรือสร้างลายมือชื่อดิจิทัลจากแบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R)
- แอปพลิเคชันสร้างลายมือชื่อดิจิทัล (SCA) ซึ่งได้รับอนุญาตให้ส่งคำขอแบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R) กับระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) เพื่อลงลายมือชื่อของเจ้าของลายมือชื่อ
- ผู้ให้บริการรับลงทะเบียนใบรับรอง (RA) ซึ่งได้รับอนุญาตให้ส่งใบรับรองให้กับระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) จากคำขอลงนามในใบรับรอง (certificate siging request: CSR)

(4) ผู้ใช้งานที่มีสิทธิสูง (privilege user) ต้องไม่ถูกมอบหมายให้มีบทบาทเป็นผู้ใช้งานที่มีสิทธิสูงทั้งหมด และ ไม่ควรถูกมอบหมายให้มีบทบาทผู้ใช้งานที่มีสิทธิสูงอื่น ๆ มากกว่าหนึ่งบทบาท

(5) ผู้ใช้งานที่มีบทบาทเป็นผู้ใช้งานที่มีสิทธิสูง ต้องไม่มีบทบาทเป็นผู้ใช้งานที่มีสิทธิพื้นฐาน และผู้ใช้งานที่มีบทบาทเป็นผู้ใช้งานที่มีสิทธิพื้นฐาน ต้องไม่มีบทบาทเป็นผู้ใช้งานที่มีสิทธิสูง

(6) ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องสามารถจำกัดผู้ใช้งานในบทบาทเจ้าหน้าที่รักษาความมั่นคงปลอดภัยระบบ (security officer) ให้ไม่ถูกมอบหมายเป็นผู้ใช้งานในบทบาทผู้ตรวจสอบระบบ (system auditor)

(7) ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องสามารถจำกัดผู้ใช้งานในบทบาทเจ้าหน้าที่ดูแลระบบ (system administrator) และ/หรือในบทบาทเจ้าหน้าที่ผู้ปฏิบัติงาน (system operator) ให้ไม่ถูกมอบหมายเป็นผู้ใช้งานในบทบาทผู้ตรวจสอบระบบ (system auditor) และ/หรือในบทบาทเจ้าหน้าที่รักษาความมั่นคงปลอดภัยระบบ (security officer)

(8) บุคคลใดที่เป็นสมาชิกของกลุ่มผู้ใช้งานที่มีสิทธิสูง ต้องมีการระบุชื่อและเป็นบุคคลที่ผ่านการอบรมที่จำเป็น

(9) ผู้ใช้งานที่เข้าถึงฮาร์ดแวร์ทางกายภาพและบริหารจัดการระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องเป็นผู้ใช้งานที่มีสิทธิสูงของระบบฯ เท่านั้น

(10) ผู้ใช้งานที่มีสิทธิสูงสุดเพื่อบริหารจัดการทุกส่วนประกอบของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องเป็นผู้ใช้งานที่มีสิทธิสูงของระบบฯ เท่านั้น

5.1.2 ระบบและการปฏิบัติงาน (SRG_SO)

5.1.2.1 การบริหารงานการปฏิบัติงาน

ผู้ให้บริการที่เชื่อถือได้ที่ให้บริการระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องทำให้มีความมั่นใจว่าการบริหารจัดการในการปฏิบัติงานในส่วนต่าง ๆ มีความมั่นคงปลอดภัยในระดับที่เหมาะสม

(1) ผู้ผลิตระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องจัดให้มีคู่มือการปฏิบัติงานเพื่อแสดงให้เห็นว่าการปฏิบัติงานที่เกี่ยวข้องกับระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) นั้น

- เป็นการให้บริการที่ถูกต้องและมั่นคงปลอดภัย
- เป็นบริการที่ผ่านการบรรเทาหรือแก้ไขความเสี่ยงจากความขัดข้องของบริการให้ลดลงเหลือน้อยเท่าที่เป็นไปได้
- สามารถป้องกับหรือทนต่อการโจมตีจากโปรแกรมประสงค์ร้าย เพื่อทำให้มีความมั่นใจในการรักษาความครบถ้วนสมบูรณ์ของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) และข้อมูลที่ผ่านการประมวลผลของระบบฯ

(2) ผู้ผลิตหรือผู้พัฒนาระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องจัดให้มีคู่มือการบริหารจัดการระบบสำหรับผู้ใช้งานที่มีสิทธิสูงในทั้ง 4 บทบาทตามรายละเอียดที่ระบุไว้ในข้อกำหนด 5.1.1.1 (2) และควรประกอบด้วยเอกสาร ดังนี้

- คู่มือหรือข้อแนะนำในการติดตั้งระบบ
- คู่มือหรือข้อแนะนำการบริหารจัดการดูแลระบบ
- คู่มือหรือข้อแนะนำสำหรับผู้ปฏิบัติงาน

5.1.2.2 การตั้งค่าเวลาให้ตรงและถูกต้อง

การสร้างลายมือชื่อดิจิทัลและการตรวจสอบความถูกต้องของลายมือชื่อเป็นกระบวนการที่เกี่ยวข้องกับเวลาในขณะดำเนินการ ดังนั้น จึงมีความจำเป็นต้องทำให้มีความมั่นใจว่าระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ได้รับการตั้งค่าเวลาให้ตรงและถูกต้องเทียบกับแหล่งเวลาอ้างอิงที่เชื่อถือได้ ข้อกำหนดนี้เป็นคนละส่วนกับข้อกำหนดที่เกี่ยวข้องกับประทับเวลาทางอิเล็กทรอนิกส์ที่กำหนดไว้โดยผู้ให้บริการประทับเวลา (TSA)

(1) ผู้ผลิตหรือผู้พัฒนาระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องระบุค่าความแม่นยำของค่าเวลาของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) และกลไกที่ทำให้มีความมั่นใจว่านาฬิกาของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) มีค่าความแม่นยำตามที่กำหนดนี้ได้

(2) เพื่อให้มีความมั่นใจว่าเวลาของการบันทึกกิจกรรมสำหรับการตรวจสอบมีความแม่นยำแหล่งเวลาอ้างอิงของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ควรมีการประสานเวลากับมาตรเวลาของแหล่งเวลาอ้างอิง

(3) การตรวจสอบว่าใบรับรองหมดอายุหรือไม่ แหล่งเวลาอ้างอิงของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องมีการประสานเวลากับมาตรเวลาร่วมสากล (UTC)

5.1.3 การระบุและยืนยันตัวตน (SRG_IA)

ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ใช้กลไกการระบุและยืนยันตัวตนเพื่อป้องกันการเข้าถึงและใช้งานโดยผู้ที่ไม่ได้รับอนุญาต และเพื่อป้องกันการเข้าถึงและใช้งานในทุกส่วนประกอบสำหรับการบริหารจัดการระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) กลไกการระบุและยืนยันตัวตน อาจเป็นกลไกของซอฟต์แวร์ระบบปฏิบัติการที่ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ติดตั้งอยู่ หรือเป็นระบบระบุและยืนยันตัวตนแยกออกเป็นเฉพาะก็ได้

5.1.3.1 การยืนยันตัวตนผู้ใช้งานที่มีสิทธิสูงและผู้ใช้งานที่มีสิทธิพื้นฐานซึ่งไม่ใช่เจ้าของลายมือชื่อ

(1) ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องกำหนดให้ผู้ใช้งานทุกคนแสดงตัวตนและผ่านการยืนยันตัวตนจนสำเร็จก่อน จึงจะอนุญาตให้เข้าถึงและใช้งานระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ตามสิทธิและบทบาทของผู้ใช้งานนั้น

(2) ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องยืนยันตัวตนผู้ใช้งานที่ได้ยุติการใช้งานหรือลงชื่อออกจากระบบ (log out) แล้วจนสำเร็จก่อน จึงจะอนุญาตให้เข้าถึงและใช้งานระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ได้อีกครั้ง

(3) คุณสมบัติของข้อมูลที่ใช้ในกลไกการยืนยันตัวตน ต้องเป็นข้อมูลที่ยากต่อการคาดเดา

(4) สำหรับการใช้งานของผู้ใช้งานที่มีสิทธิสูง ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วย

เครื่องบริการที่เชื่อถือได้ (TW4S) ต้องจำกัดระยะเวลาการเชื่อมต่อกับระบบหรือยุติการใช้งานระบบหากไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนดไว้เพื่อลดความเสี่ยงจากการถูกลักลอบเข้าถึงและใช้งานในบทบาทของผู้ใช้งานที่มีสิทธิสูงผ่านอุปกรณ์ของผู้ใช้งานนั้นในขณะที่ไม่มีการใช้งานหรือดูแล

5.1.3.2 การยืนยันตัวตนที่ไม่สำเร็จ

(1) ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องระงับการยืนยันตัวตนผู้ใช้งานซึ่งได้ยืนยันตัวตนเพื่อเข้าถึงระบบไม่สำเร็จหรือเกิดความผิดพลาดเกินกว่าจำนวนครั้งสูงสุดที่ได้กำหนดไว้ ผู้ใช้งานนั้นจะสามารถยืนยันตัวตนได้อีกครั้งหลังพ้นกรอบเวลาการระงับการยืนยันตัวตนที่กำหนดไว้ หรือจนกว่าผู้ใช้งานในบทบาทผู้ดูแลระบบจะได้ยกเลิกการระงับการยืนยันตัวตนนั้น

5.1.4 การควบคุมและจำกัดการเข้าถึงระบบ (SRG_SA)

ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ใช้กลไกการควบคุมและจำกัดการเข้าถึงระบบเพื่อป้องกันการเข้าถึงและใช้งานข้อมูลและส่วนประกอบสำคัญทั้งหมดของระบบโดยผู้ไม่ได้รับอนุญาต กลไกการควบคุมและจำกัดการเข้าถึงระบบนี้ใช้กับผู้ใช้งานที่มีสิทธิสูงเท่านั้น ส่วนการควบคุมและจำกัดการเข้าถึงระบบของเจ้าของลายมือชื่อ ให้ปฏิบัติตามรายละเอียดที่ระบุไว้ในข้อกำหนด 5.2.2

การควบคุมและจำกัดการเข้าถึงระบบ อาจเป็นกลไกของซอฟต์แวร์ระบบปฏิบัติการที่ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ติดตั้งอยู่ หรือเป็นส่วนควบคุมและจำกัดการเข้าถึงระบบแยกออกเป็นเฉพาะก็ได้ โดยเจ้าของหรือผู้รับผิดชอบต่อข้อมูลในระบบนั้นจะเป็นผู้กำหนดสิทธิการเข้าถึงข้อมูลหรือส่วนประกอบเฉพาะของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ด้วยไอเดนทิตี้หรือข้อมูลระบุตัวตนของผู้ที่พยายามเข้าถึงข้อมูลหรือส่วนประกอบของระบบนั้น และ

(1) ผู้ที่พยายามเข้าถึงได้รับมอบสิทธิการเข้าถึงข้อมูลหรือส่วนประกอบของระบบ หรือ

(2) ผู้ที่พยายามเข้าถึงถือครองสิทธิการเข้าถึงข้อมูลหรือส่วนประกอบของระบบเอง

5.1.4.1 การบริหารสิทธิการเข้าถึงระบบ

(1) ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องมีความสามารถในการควบคุมและจำกัดผู้ใช้งานที่ระบุไว้ในการเข้าถึงข้อมูลที่ผู้ใช้งานเป็นเจ้าของ หรือส่วนประกอบของระบบที่ผู้ใช้งานเป็นผู้รับผิดชอบ

(2) ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องทำให้มีความมั่นใจว่าสามารถควบคุมและจำกัดการเข้าถึงข้อมูลสำคัญที่เก็บไว้บนระบบ

5.1.5 การบริหารจัดการกุญแจ (SRG_KM)

ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) สามารถใช้กุญแจเข้ารหัสลับเพื่อรักษาความครบถ้วนสมบูรณ์และความลับ และเพื่อใช้เป็นฟังก์ชันยืนยันตัวตนกับระบบย่อยของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) และกับระบบย่อย

อื่น ๆ ดังนั้น การใช้งานกุญแจโดยไม่ได้รับอนุญาต การเปิดเผยกุญแจโดยไม่ได้รับอนุญาต หรือการแก้ไขหรือการออกกุญแจแทนที่กุญแจเดิมเหล่านี้จะส่งผลให้เกิดสูญเสียคุณสมบัติด้านความมั่นคงปลอดภัยของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) จึงมีความจำเป็นต้องจัดการกุญแจเหล่านี้ด้วยความมั่นคงปลอดภัยตลอดวงจรชีวิตของกุญแจ

เนื่องจากมีภัยคุกคามหลายรูปแบบที่ส่งผลกระทบต่อกุญแจต่าง ๆ ที่ใช้ในระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) จึงมีความจำเป็นต้องจัดประเภทของกุญแจต่าง ๆ ตามประเภทภัยคุกคามที่ส่งผลกระทบต่อกุญแจ สำหรับข้อเสนอแนะมาตรฐานฉบับนี้ กุญแจที่ใช้ในระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) สามารถจัดแบ่งเป็นประเภท ดังนี้

- กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อ (signer's signing keys) คือ กุญแจหรือชุดกุญแจที่อยู่ภายใต้การควบคุมและใช้งานโดยเจ้าของลายมือชื่อสำหรับสร้างลายมือชื่อดิจิทัล
- กุญแจโครงสร้างพื้นฐาน (infrastructure keys) คือ กุญแจที่ใช้งานโดยระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) สำหรับประมวลผลกิจกรรมต่าง ๆ เช่น การแลกและตกลงกุญแจ (key agreement) การยืนยันตัวตนของส่วนประกอบย่อยของระบบ (subsystem authentication) การลงลายมือชื่อในบันทึกกิจกรรมสำหรับตรวจสอบ (audit log signing) และจัดเก็บหรือส่งข้อมูลที่มีรักษาความมั่นคงปลอดภัยด้วยการเข้ารหัสลับข้อมูล เป็นต้น ทั้งนี้ กุญแจต่าง ๆ ที่มีอายุใช้งานในช่วงเวลาสั้น ๆ ในระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ก็ถูกจัดให้อยู่ในประเภทกุญแจโครงสร้างพื้นฐานนี้
- กุญแจควบคุม (control keys) คือ กุญแจที่ใช้งานโดยบุคลากรหรือเจ้าหน้าที่ที่ได้รับมอบหมายให้เป็นผู้บริหารจัดการหรือใช้งานระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) และบุคคลซึ่งมีโอกาสจะใช้กุญแจควบคุมนี้สำหรับการยืนยันตัวตน การลงลายมือชื่อ หรือเพื่อวัตถุประสงค์ในการรักษาความลับของข้อมูล

(1) ข้อกำหนดด้านความมั่นคงปลอดภัยของกุญแจ กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อ ต้องจัดเป็นกุญแจที่มีความสำคัญและ ควรมีมาตรการในการรักษาความมั่นคงปลอดภัยต่อภัยคุกคามทั้งในแง่ปริมาณและระดับความเสี่ยงที่เหมาะสม กุญแจโครงสร้างพื้นฐานจัดเป็นกุญแจที่มีความสำคัญเช่นเดียวกัน แต่เนื่องจากรูปแบบหรือลักษณะการใช้งานกุญแจที่จำเป็นต้องถูกเผยแพร่หรือจัดเก็บอยู่ในหลายแหล่ง จึงทำให้กุญแจโครงสร้างพื้นฐานนี้มีความสำคัญต่ำกว่ากุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อ กุญแจที่มีความสำคัญต่ำที่สุด คือกุญแจควบคุมที่ใช้งานโดยบุคลากรหรือเจ้าหน้าที่ของผู้ให้บริการที่เชื่อถือได้ในการควบคุมหรือบริหารจัดการระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) และมักจะมีอายุกุญแจในช่วงเวลาสั้น ๆ กุญแจเซสชันที่ใช้อ้างอิงถึงผู้ใช้งานภายหลังการยืนยันตัวตนผู้ใช้งานเป็นผลสำเร็จเพื่อทำธุรกรรมเดียวหรือหลายธุรกรรมภายในกำหนดเวลาสั้น ๆ จัดเป็นกุญแจที่มีความสำคัญเช่นกัน แต่ข้อกำหนดด้านความมั่นคงปลอดภัยของกุญแจประเภทนี้จะต่ำกว่าข้อกำหนดสำหรับกุญแจประเภทอื่น ๆ ที่กล่าวถึงมาก่อนหน้านี้

(2) กุญแจโครงสร้างพื้นฐานและกุญแจควบคุมอาจเป็นกุญแจประเภทกุญแจส่วนตัวหรือกุญแจลับก็ได้

5.1.5.1 การสร้างกุญแจ

(1) กุญแจส่วนตัวหรือกุญแจลับ ควรถูกสร้างขึ้นและใช้งานภายในอุปกรณ์/ระบบสร้าง

ลายมือชื่อดิจิทัล (SCDev) โดยอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) ควรเป็นอุปกรณ์/ระบบที่เชื่อถือได้และผ่านการตรวจรับรองเกณฑ์ประเมินทั่วไปด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ (CC) ตามมาตรฐาน ISO/IEC 15408 [7] [8] [9] หรือมาตรฐานอื่นในระดับประเทศที่เกี่ยวข้องกับการประเมินด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศของผลิตภัณฑ์ตามข้อกำหนดด้านความมั่นคงปลอดภัยที่กำหนดไว้ในข้อเสนอแนะมาตรฐานฉบับนี้ ในระดับความเข้มงวดในการประเมินตามเกณฑ์ประเมินทั่วไปด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ (EAL) ที่ระดับ 4 ขึ้นไป

(2) อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) ต้องรองรับกระบวนวิธีเข้ารหัสลับ (cryptographic algorithms) และความยาวของกุญแจ (key lengths) ตามความเหมาะสมของระดับความมั่นคงปลอดภัยที่ต้องการตามรายละเอียดที่กำหนดไว้ในช่วงการออกแบบของระบบ

หมายเหตุ การเลือกใช้กระบวนวิธีเข้ารหัสลับ (cryptographic algorithms) ที่เหมาะสมให้เป็นไปตามข้อเสนอแนะหรือประกาศของหน่วยงานในระดับประเทศที่รับผิดชอบ โดยมีความสอดคล้องและได้รับการยอมรับในระดับสากล เช่น มาตรฐานเรื่องชุดกระบวนวิธีเข้ารหัสลับ (cryptographic suites) ETSI TS 119312 [14]

เมื่อมีความจำเป็นต้องรักษาความลับและความครบถ้วนสมบูรณ์ของข้อมูลสำคัญ เช่น การสำรองข้อมูลกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล กระบวนวิธีเข้ารหัสลับ (cryptographic algorithms) และพารามิเตอร์อื่นที่เกี่ยวข้อง ต้องมีระดับความมั่นคงปลอดภัยที่เทียบเท่าหรือสูงกว่าข้อกำหนดในข้อกำหนดนี้เท่านั้น

(3) เมื่อกุญแจส่วนตัวหรือกุญแจลับ ซึ่งครอบคลุมถึงกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อ กุญแจโครงสร้างพื้นฐาน และกุญแจควบคุม ที่ถือครองภายนอกอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) กุญแจเหล่านี้ ต้องได้รับการปกป้องเพื่อทำให้มีความมั่นใจว่ามีการรักษาความลับและความครบถ้วนสมบูรณ์ของกุญแจ

(4) อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) ต้องถูกตั้งค่าเริ่มต้นการใช้งานด้วยกลไกทางเทคนิคในอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) ด้วยผู้ปฏิบัติงานอย่างน้อย 2 คน ก่อนใช้สร้างหรือจัดเก็บกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล

5.1.5.2 การจัดเก็บ สำรอง และกู้คืนกุญแจ

(1) กุญแจส่วนตัวและกุญแจลับทั้งหมด ซึ่งครอบคลุมถึงกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อ กุญแจโครงสร้างพื้นฐาน และกุญแจควบคุม ต้องมีการจัดเก็บด้วยความมั่นคงปลอดภัยโดยไม่เก็บรักษาไว้ในรูปแบบที่ไม่มีปกป้อง

(2) ถ้ามีกุญแจส่วนตัวหรือกุญแจลับ ซึ่งครอบคลุมถึงกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อ กุญแจโครงสร้างพื้นฐาน และกุญแจควบคุม ถูกนำออกจากอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) กุญแจนั้น ต้องได้รับการปกป้องเพื่อทำให้มีความมั่นใจว่าการรักษาความลับและความครบถ้วนสมบูรณ์ของกุญแจนั้น

ยังมีระดับความมั่นคงปลอดภัยเทียบเท่าหรือสูงกว่าการจัดเก็บภายในอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev)

เมื่อมีการปกป้องกุญแจส่วนตัวหรือกุญแจลับด้วยการเข้ารหัสลับ ต้องใช้กระบวนวิธีการเข้ารหัสลับและค่าพารามิเตอร์ที่มีระดับความมั่นคงปลอดภัยเทียบเท่าหรือสูงกว่าที่อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) ใช้เท่านั้น

(3) อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) ต้องทำให้มีความมั่นใจว่าการจัดเก็บ สำรอง และกู้คืนกุญแจส่วนตัวหรือกุญแจลับ ซึ่งครอบคลุมถึงกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อ กุญแจโครงสร้างพื้นฐาน และกุญแจควบคุม ดำเนินการได้โดยเจ้าหน้าที่ที่ได้รับอนุญาตเท่านั้น กุญแจมาสเตอร์ (master keys) ที่ใช้ปกป้องกุญแจผู้ใช้งาน (user keys) และกุญแจที่ใช้งานในระบบ (working keys) ต้องได้รับการจัดเก็บ สำรอง และนำเข้าหรือกู้คืนภายใต้การควบคุมการปฏิบัติงานที่ใช้สองบุคคลหรือสองกระบวนการ (dual control) เป็นขั้นต่ำ กุญแจมาสเตอร์ (master keys) ที่จัดเก็บภายนอกอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) ต้องอยู่ในรูปแบบที่มีการปกป้องเพื่อรักษาความมั่นคงปลอดภัยให้กับกุญแจ

5.1.5.3 การใช้กุญแจ

(1) การใช้กุญแจส่วนตัวหรือกุญแจลับ ซึ่งครอบคลุมถึงกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อ กุญแจโครงสร้างพื้นฐาน และกุญแจควบคุม ต้องเป็นไปตามวัตถุประสงค์ที่กำหนดไว้สำหรับกุญแจนั้นเท่านั้น

(2) กุญแจส่วนตัวหรือกุญแจลับ ซึ่งครอบคลุมถึงกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อ กุญแจโครงสร้างพื้นฐาน และกุญแจควบคุม ต้องไม่ถูกส่งต่อหรือมอบให้ผู้อื่น เว้นแต่เป็นไปตามวัตถุประสงค์ที่กำหนดไว้สำหรับกุญแจนั้น

(3) การเข้าถึงและใช้งานกุญแจต่าง ๆ ซึ่งครอบคลุมถึงกุญแจโครงสร้างพื้นฐาน และกุญแจควบคุม ต้องผ่านกลไกควบคุมการเข้าถึงเพื่ออนุญาตให้เฉพาะผู้ใช้งานที่ได้รับสิทธิเท่านั้น

(4) กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อ ต้องถูกเชื่อมโยงไปยังเจ้าของลายมือชื่อเพียงผู้เดียว และเชื่อมโยงกับใบรับรองเพียงใบรับรองเดียว

5.1.5.4 การเผยแพร่กุญแจ

(1) เมื่อจำเป็นต้องมีการจัดส่งกุญแจส่วนตัวหรือกุญแจลับ ซึ่งครอบคลุมถึงกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อ กุญแจโครงสร้างพื้นฐาน และกุญแจควบคุม ต้องจัดส่งด้วยวิธีการที่มีการรักษาความมั่นคงปลอดภัยกับกุญแจ

(2) กุญแจทั้งหมดที่ใช้ในการรักษาความมั่นคงปลอดภัยในระหว่างการจัดส่งกุญแจส่วนตัวหรือกุญแจลับ ต้องมีความแข็งแกร่งของกุญแจไม่ต่ำกว่าความแข็งแกร่งของกุญแจที่ถูกจัดส่ง

5.1.5.5 การต่ออายุ ปรับปรุง และเปลี่ยนกุญแจ

(1) กุญแจโครงสร้างพื้นฐาน และกุญแจควบคุม ควรถูกเปลี่ยนอยู่เสมอตามระยะเวลาที่เหมาะสมตามผลประเมินความเสี่ยง

(2) เมื่อพบความไม่เหมาะสมหรือไม่มั่นคงปลอดภัยของกระบวนวิธีเข้ารหัสลับ (cryptographic algorithms) หรือความยาวของกุญแจ (key lengths) กุญแจต่าง ๆ ที่เกี่ยวกับกับกระบวนวิธีการรหัสลับนี้ ต้องถูกเปลี่ยนในทันที

(3) เมื่อพบว่ามีกุญแจถูกละเมิดหรือสงสัยว่าจะถูกละเมิด กุญแจเหล่านี้ ควรถูกเปลี่ยนในทันที

5.1.5.6 การจัดเก็บกุญแจเพื่อเป็นข้อมูลที่เก็บไว้เป็นหลักฐานในระยะยาว (**archive)**

(1) กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล ต้องไม่จัดเก็บไว้เป็นหลักฐานในระยะยาว

5.1.5.7 การลบกุญแจ

(1) กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล ต้องถูกทำลายหลังจากที่ใบรับรองที่เชื่อมโยงกับกุญแจนั้นหมดอายุการใช้งาน หรือเมื่อพบว่าเจ้าของลายมือชื่อไม่สามารถใช้งานกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลนั้นได้อีกต่อไป

(2) เมื่อพบว่ากุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลขาดความเชื่อมโยงกับเจ้าของลายมือชื่อภายหลังกระบวนการลงลายมือชื่อใด กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลนั้นต้องถูกทำลายเมื่อสิ้นสุดกระบวนการลงลายมือชื่อนั้น

(3) ขั้นตอนการปฏิบัติงานและกลไกในการทำลายกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลควรทำให้มีความมั่นใจว่าข้อมูลสำรองของกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลทุกสำเนาได้ถูกทำลายด้วย และไม่มีข้อมูลใดที่หลงเหลืออยู่สามารถใช้สร้างกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลนั้นกลับมาได้

5.1.6 การตรวจสอบ (SRG_AA)

5.1.6.1 การบันทึกข้อมูลสำหรับตรวจสอบ **(audit data)**

ในแต่ละบริการของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) มีข้อกำหนดเพิ่มเติมเป็นเฉพาะเพิ่มขึ้นจากข้อกำหนดทั่วไปที่ ต้องระบุไว้เป็นข้อกำหนด ดังนี้

(1) เหตุการณ์ที่ต้องมีการบันทึกข้อมูลสำหรับตรวจสอบ (audit data) ไว้ อย่างน้อย ดังนี้

- สถานการณ์แวดล้อมที่สำคัญของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) และเหตุการณ์ที่เกี่ยวข้องกับการบริหารจัดการกุญแจ (การสร้าง การใช้งาน และการทำลาย)
- เหตุการณ์การลงลายมือชื่อของผู้ใช้งาน เช่น เหตุการณ์การสร้างลายมือชื่อด้วยกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อ และเหตุการณ์ในการบริหารจัดการกับคำขอในแบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R)
- การยืนยันตัวตนผู้ใช้งานที่เกิดขึ้นภายในโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP)

- การจัดการข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ของเจ้าของลายมือชื่อด้วยระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S)
- การเปิดและปิดฟังก์ชันการสร้างข้อมูลสำหรับตรวจสอบ
- การเปลี่ยนพารามิเตอร์ที่เกี่ยวข้องกับการสร้างข้อมูลสำหรับตรวจสอบ

เหตุการณ์การลงลายมือชื่อของเจ้าของลายมือชื่อ ต้องบันทึกข้อมูลใบรับรองที่เชื่อมโยงกับกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลนั้นด้วย

เหตุการณ์เข้าถึงหรือพยายามเข้าถึงระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ควรถูกบันทึกเป็นข้อมูลสำหรับตรวจสอบ

(2) ผู้ให้บริการที่เชื่อถือได้ ต้องระบุกิจกรรมที่ได้ดำเนินการไปแล้ว เมื่อเกิดความผิดพลาดในการส่งข้อมูลสำหรับตรวจสอบ (audit data) ไปยังสื่อบันทึกข้อมูลภายในนอกระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้

5.1.6.2 การรักษาความพร้อมใช้งานของข้อมูลสำหรับตรวจสอบ

(1) ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องดูแลรักษาข้อมูลสำหรับตรวจสอบ (audit data) และทำให้มีความมั่นใจว่ามาตรการนี้ดูแลรักษาข้อมูลสำหรับตรวจสอบทั้งหมดที่จัดเก็บไว้

(2) ฟังก์ชันการบันทึกข้อมูลสำหรับตรวจสอบ ต้องอยู่ในรูปแบบการบันทึกข้อมูลเพิ่มต่อท้ายจากข้อมูลเดิมเท่านั้น

(3) ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องปกป้องข้อมูลสำหรับตรวจสอบ (audit data) ที่ถูกจัดเก็บไว้จากการถูกลบโดยผู้ที่ไม่ได้รับอนุญาต

(4) รายการข้อมูลสำหรับตรวจสอบ (audit records) อาจถูกลบได้เมื่อมีการจัดเก็บข้อมูลไว้เป็นหลักฐานในระยะยาวแล้ว

5.1.6.3 พารามิเตอร์ข้อมูลสำหรับตรวจสอบ

(1) ข้อมูลทั้งหมดสำหรับตรวจสอบ (รวมถึงข้อมูลเฉพาะของบริการบันทึกข้อมูลสำหรับตรวจสอบของบริการ) ต้องประกอบด้วยพารามิเตอร์ต่าง ๆ ดังนี้

- วันและเวลาของเหตุการณ์
- ประเภทของเหตุการณ์
- ไอเดนทิตี้หรือข้อมูลระบุตัวตน (เช่น ผู้ใช้งาน ผู้ดูแลระบบ และโพรเซสของระบบ) ที่เป็นผู้รับผิดชอบหรือดำเนินการที่เกี่ยวข้องกับเหตุการณ์
- สถานภาพของเหตุการณ์ เช่น สำเร็จหรือไม่สำเร็จ

5.1.6.4 การเรียกแสดงข้อมูลสำหรับตรวจสอบ

(1) ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้อง

สามารถค้นหาเหตุการณ์จากข้อมูลสำหรับตรวจสอบ (audit data) ด้วยวันที่ของเหตุการณ์ที่เกิดขึ้น หรือด้วยประเภทของเหตุการณ์ หรือด้วยไอเดนทิตี้หรือข้อมูลระบุตัวตนของผู้ใช้งาน

(2) รายการข้อมูลสำหรับตรวจสอบ (audit records) ต้องสามารถนำไปประมวลผลข้อมูลหรือแสดงในรูปแบบที่เหมาะสมกับผู้ตรวจสอบระบบ (system auditor) สามารถอ่านและเข้าใจได้

5.1.6.5 การจำกัดการเข้าถึงข้อมูลสำหรับตรวจสอบ

(1) ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องปฏิเสธการเข้าถึงเพื่ออ่านข้อมูลสำหรับตรวจสอบจากผู้ใช้งานทั้งหมด ยกเว้นสำหรับผู้ใช้งานที่มีสิทธิการเข้าถึงเพื่ออ่านอย่างชัดแจ้ง เช่น ผู้ใช้งานในบทบาทผู้ตรวจสอบระบบ (system auditor)

5.1.6.6 การสร้างข้อความแจ้งเตือน

(1) ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องสร้างข้อความและแจ้งเตือนทันต่อเวลาหรือภายในเวลาที่เหมาะสมกับสถานการณ์ความผิดปกติที่เกิดขึ้น

ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ควรมีกลไกการแจ้งเตือนต่อเจ้าหน้าที่ดูและระบบที่เกี่ยวข้องเมื่อตรวจพบสถานการณ์ความผิดปกติ

กลไกการแจ้งเตือนอาจเป็นเครื่องมือสั่งการให้ดำเนินการเพื่อตอบสนองต่อสถานการณ์ที่อาจเป็นการโจมตีต่อระบบ เช่น การสั่งให้ตัดเส้นทางการเชื่อมต่อที่พบสถานการณ์ที่อาจเป็นการโจมตีต่อระบบ ตัวอย่างสถานการณ์ผิดปกติที่เกี่ยวข้องกับกิจกรรมของผู้ใช้งาน เช่น การใช้งานของผู้ใช้งานนอกเวลาใช้งานปกติ การสั่งงานของผู้ใช้งานจำนวนมากจนผิดปกติ (ตรวจจับการสั่งงานจากโปรแกรมหรือซอฟต์แวร์) หรือ การมีเซสชันใช้งานของผู้ใช้งานมากกว่าหนึ่งเซสชัน เป็นต้น

5.1.6.7 การรักษาความครบถ้วนสมบูรณ์ของข้อมูลสำหรับตรวจสอบ

(1) ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องทำให้มีความมั่นใจว่าสามารถรักษาความครบถ้วนสมบูรณ์ของข้อมูลสำหรับตรวจสอบ (audit data)

(2) ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องมีฟังก์ชันสำหรับการตรวจสอบความครบถ้วนสมบูรณ์ของข้อมูลสำหรับตรวจสอบ (audit data)

5.1.6.8 ความแม่นยำของเวลาของข้อมูลสำหรับตรวจสอบ

(1) เพื่อทำให้มีความมั่นใจว่าข้อมูลเวลาของเหตุการณ์ในข้อมูลสำหรับตรวจสอบมีความแม่นยำของเวลา ให้ปฏิบัติตามข้อกำหนดในข้อกำหนดด้านความมั่นคงปลอดภัยทั่วใน

เรื่องระบบและการปฏิบัติงานในข้อกำหนด 5.1.2.2 (2)

5.1.7 การจัดเก็บข้อมูลไว้เป็นหลักฐานในระยะยาว (SRG_AR)

5.1.7.1 การสร้างข้อมูลไว้เป็นหลักฐานในระยะยาว

(1) ผู้ให้บริการที่เชื่อถือได้ ต้องสามารถจัดเก็บข้อมูลไว้เป็นหลักฐานในระยะยาวบนสื่อบันทึกข้อมูลภายนอก สื่อบันทึกข้อมูลนี้ ควรมีการจัดเก็บอย่างเหมาะสมให้สามารถนำมาใช้ได้ในภายหลัง และสามารถใช้เป็นหลักฐานในทางกฎหมายเพื่อรับรองลายมือชื่อดิจิทัลที่สร้างขึ้นในระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S)

(2) ข้อมูลสำหรับตรวจสอบทั้งหมด ต้องมีการจัดเก็บไว้เป็นหลักฐานในระยะยาว

(3) ข้อมูลที่เก็บไว้เป็นหลักฐานในระยะยาวในแต่ละรายการ ต้องประกอบด้วยเวลาที่ทำการสร้างข้อมูลที่เก็บไว้เป็นหลักฐานในระยะยาว

(4) ข้อมูลที่เก็บไว้เป็นหลักฐานในระยะยาว ต้องไม่จัดเก็บพารามิเตอร์ต่าง ๆ ที่สำคัญต่อความมั่นคงปลอดภัย เช่น รหัสผ่านของผู้ใช้งานระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S)

5.1.7.2 การรักษาความครบถ้วนสมบูรณ์ของข้อมูลที่เก็บไว้เป็นหลักฐานในระยะยาว

(1) ต้องมีการป้องกันการแก้ไขเปลี่ยนแปลงรายการข้อมูลที่เก็บไว้เป็นหลักฐานในระยะยาวโดยไม่ได้รับอนุญาต และ ต้องจัดให้มีกลไกการตรวจสอบความครบถ้วนสมบูรณ์เพื่อตรวจการเปลี่ยนแปลงที่ไม่ได้รับอนุญาตใด ๆ ที่เกิดแก่ข้อมูลที่เก็บไว้เป็นหลักฐานในระยะยาวนับแต่เวลาที่ได้สร้างขึ้น

5.1.8 การสำรองและกู้คืนข้อมูล (SRG_BK)

ขอบเขตของข้อกำหนดนี้ครอบคลุมถึงข้อมูลระบบ ข้อมูลผู้ใช้งาน และข้อมูลอื่นที่เกี่ยวข้องทั้งหมดที่จำเป็นต่อการกู้คืนระบบในภายหลังระบบล้มเหลวหรือเกิดเหตุภัยพิบัติต่อระบบ แต่ไม่รวมถึงข้อมูลสำรองและกู้คืนของกุญแจต่าง ๆ ซึ่งข้อกำหนดด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับกุญแจได้กำหนดไว้แล้วในข้อกำหนดด้านความมั่นคงปลอดภัยทั่วไปในเรื่องการบริหารจัดการกุญแจ ในข้อกำหนด 5.1.5.2

5.1.8.1 การรักษาความลับและความครบถ้วนสมบูรณ์ของข้อมูลสำรอง

(1) ข้อมูลสำรอง ต้องได้รับการปกป้องไม่ให้มีการแก้ไขเปลี่ยนแปลงจากกลไกในการตรวจสอบความครบถ้วนสมบูรณ์ของข้อมูลสำรอง

(2) พารามิเตอร์ต่างๆ ที่สำคัญต่อความมั่นคงปลอดภัยและข้อมูลลับ ต้องมีการจัดเก็บไว้ในรูปแบบที่มีความมั่นคงปลอดภัยเพื่อรักษาความลับและความครบถ้วนสมบูรณ์ของข้อมูล

5.1.8.2 การกู้คืนข้อมูล

(1) ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องมีฟังก์ชันสำหรับการกู้คืนข้อมูลระบบจากข้อมูลสำรอง

(2) ผู้ใช้งานใดที่เชื่อมโยงกับบทบาทผู้ใช้งานที่มีสิทธิสูงที่เหมาะสม ต้องสามารถสั่งการฟังก์ชันสำหรับการกู้คืนข้อมูลจากข้อมูลสำรองได้ตามที่ต้องการ

5.2 ข้อกำหนดด้านความมั่นคงปลอดภัยของส่วนประกอบหลักของระบบ (core component security requirements: SRC)

5.2.1 การตั้งค่ากุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล และกุญแจระบบรหัสลับ (SRC_SKS.1)

(1) พารามิเตอร์ของอัลกอริทึมที่ใช้สำหรับการสร้างลายมือชื่อด้วยระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องถูกกำหนดให้มีความมั่นคงปลอดภัยเพียงพอในตลอดช่วงอายุของใบรับรอง

หมายเหตุ: การเลือกใช้กระบวนวิธีเข้ารหัสลับ (cryptographic algorithm) ที่เหมาะสมให้เป็นไปตามข้อเสนอแนะหรือประกาศของหน่วยงานในระดับประเทศที่รับผิดชอบ โดยมีความสอดคล้องและได้รับการยอมรับในระดับสากล เช่น มาตรฐานเรื่องชุดกระบวนวิธีเข้ารหัสลับ (cryptographic suite) ETSI TS 119312 [14]

(2) ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องเชื่อมโยงกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อกับใบรับรองของเจ้าของลายมือชื่อนั้น

(3) กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อ อาจถูกสร้างขึ้นไว้ล่วงหน้า ก่อนจะมีการเชื่อมโยงกับใบรับรองก็ได้

(4) กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล ไม่ควรถูกนำไปใช้สร้างลายมือชื่อ ก่อนจะมีการเชื่อมโยงกับใบรับรองด้วยระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S)

หมายเหตุ: ข้อกำหนดด้านความมั่นคงปลอดภัยในข้อนี้ ไม่ครอบคลุมการใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลในการลงลายมือชื่อเพื่อใช้เป็นหลักฐานในการแสดงการครอบครองกุญแจในกระบวนการขอใบรับรอง

(5) ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องรักษาความครบถ้วนสมบูรณ์ของข้อมูลที่เกี่ยวข้องกับการเชื่อมโยงกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อกับใบรับรอง

5.2.2 การยืนยันตัวตนเจ้าของลายมือชื่อ (SRC_SA)

5.2.2.1 การยืนยันตัวตนเจ้าของลายมือชื่อสำหรับระดับความเข้มงวดฯ พื้นฐาน SCAL1

(1) การพิสูจน์ตัวตนเจ้าของลายมือชื่อ ต้องมีความเข้มงวดของการพิสูจน์ตัวตนที่ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน IAL1 ขึ้นไป

การยืนยันตัวตนเจ้าของลายมือชื่อ ต้องใช้วิธีการยืนยันตัวตนที่มีความเข้มงวดในการยืนยันตัวตนที่ระดับความน่าเชื่อถือของการยืนยันตัวตน AAL1 ขึ้นไป

(2) แอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) ต้องกำหนดให้เจ้าของลายมือชื่อพิสูจน์และยืนยันตัวตนจนสำเร็จแล้ว จึงจะอนุญาตให้ใช้งานกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลซึ่งอยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น

(3) โพรโทคอลที่ใช้ในการยืนยันตัวตน ต้องสามารถปกป้องการโจมตีแบบปรับเปลี่ยนข้อมูลในระหว่างสื่อสาร (man-in-the-middle attacks) การโจมตีแบบดักรับข้อมูลเพื่อใช้ซ้ำ (reply attacks) และรูปแบบการโจมตีทั่วไปอื่น ๆ ที่ผู้ประสงค์ร้ายสามารถใช้อัตลักษณ์หรือสิ่งที่ใช้ยืนยันตัวตนของผู้อื่นมายืนยันตัวตนเข้าระบบได้

(4) มาตการควบคุมการเข้าถึงระบบ ต้องทำให้มีความมั่นใจว่า เจ้าของลายมือชื่อไม่สามารถเข้าถึงข้อมูลหรือฟังก์ชันสำคัญของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) เพื่อควบคุมการเข้าถึงกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของบุคคลอื่น

(5) ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องทำให้มีความมั่นใจว่าแบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R) ที่ได้รับมาซึ่งอยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อนั้น ถูกลงนามด้วยกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อเท่านั้น

5.2.2.2 การจัดการเมื่อการยืนยันตัวตนเพื่อเข้าถึงระบบไม่สำเร็จหรือเกิดความผิดพลาด

(1) ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องสามารถตรวจพบเหตุการณ์การยืนยันตัวตนเจ้าของลายมือชื่อแต่ละรายที่เข้าถึงระบบไม่สำเร็จหรือเกิดความผิดพลาดและเกิดขึ้นต่อเนื่องเกินจำนวนครั้งที่กำหนดไว้ได้

(2) เมื่อเกิดเหตุการณ์การยืนยันตัวตนเจ้าของลายมือชื่อแต่ละรายที่เข้าถึงระบบไม่สำเร็จหรือเกิดความผิดพลาดและเกิดขึ้นต่อเนื่องเกินจำนวนครั้งที่กำหนดไว้แล้ว ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องระงับการเข้าถึงระบบของผู้ใช้งานนั้นเป็นระยะเวลาที่เหมาะสม หรือจนกว่าผู้ดูแลระบบจะยกเลิกการระงับการเข้าถึงระบบของผู้ใช้งานนั้น

5.2.2.3 การมอบหมายการยืนยันตัวตนเจ้าของลายมือชื่อให้กับระบบภายนอก

(1) ในกรณีที่มีการมอบหมายการยืนยันตัวตนเจ้าของลายมือชื่อให้กับระบบภายนอก ผู้ให้บริการที่เชื่อถือได้ ต้องทำให้มีความมั่นใจว่าระบบให้บริการภายนอกนั้นมีคุณสมบัติสอดคล้องตามรายละเอียดที่ระบุไว้ในข้อกำหนด 5.2.2.1 และข้อกำหนด 5.2.2.2

5.2.3 การสร้างลายมือชื่อดิจิทัล และกระบวนการระบบรหัสลับ (SRC_DSC)

(1) พารามิเตอร์ของอัลกอริทึมที่ใช้สำหรับการสร้างลายมือชื่อด้วยระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องถูกกำหนดให้มีความมั่นคงปลอดภัยเพียงพอในตลอดช่วงอายุของใบรับรอง

หมายเหตุ: การเลือกใช้กระบวนวิธีเข้ารหัสลับ (cryptographic algorithm) ที่เหมาะสมให้เป็นไปตามข้อเสนอแนะหรือประกาศของหน่วยงานในระดับประเทศที่รับผิดชอบ โดยมีความสอดคล้องและได้รับการยอมรับในระดับสากล เช่น มาตรฐานเรื่องชุดกระบวนวิธีเข้ารหัสลับ (cryptographic suite) ETSI TS 119312 [14]

5.3 ข้อกำหนดด้านความมั่นคงปลอดภัยเพิ่มเติมสำหรับระดับความเข้มงวดฯ ขั้นสูง SCAL2 (additional security requirements: SRA)

ข้อกำหนดด้านความมั่นคงปลอดภัยเพิ่มเติมในส่วนนี้สำหรับระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ในระดับความเข้มงวดฯ ขั้นสูง SCAL2

โมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) ทำหน้าที่ยืนยันตัวตนกับเจ้าของลายมือชื่อทั้งทางตรงหรือทางอ้อม

ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ถูกเก็บรวบรวมภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่นด้วยความเชื่อมั่นในระดับสูง เพื่อทำให้มีความมั่นใจว่ากุญแจที่ระบุไว้ในข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ถูกใช้ด้วยเจ้าของลายมือชื่อที่ผ่านการยืนยันตัวตนจนสำเร็จกับ (ชุด)แบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R) ที่ระบุไว้

5.3.1 โพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัลและข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SRA_SAP)

5.3.1.1 ความต้านทานต่อภัยคุกคาม

(1) การพิสูจน์ตัวตนเจ้าของลายมือชื่อ ต้องมีความเข้มงวดของการพิสูจน์ตัวตนที่ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน IAL2 ขึ้นไป

การยืนยันตัวตนเจ้าของลายมือชื่อ ต้องใช้วิธีการยืนยันตัวตนที่มีความเข้มงวดในการยืนยันตัวตนที่ระดับความน่าเชื่อถือของการยืนยันตัวตน AAL2 ขึ้นไป

(2) ต้องมีมาตรการควบคุมตามจำเป็นกับระดับความเสี่ยงเพื่อรับมือและโต้ตอบต่อภัยคุกคามกับโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) และข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ดังนี้ การคาดเดาทั้งออนไลน์และออฟไลน์ (online & offline guessing) การทำซ้ำข้อมูลตัวตน (credential duplication) ฟิชชิ่ง (phishing) การดักรับข้อมูล (eavesdropping) การดักรับข้อมูลเพื่อใช้ซ้ำ (reply) การโจรกรรมเซสชัน (session hijacking) การปรับเปลี่ยนข้อมูลในระหว่างสื่อสาร (man-in-the-middle attacks) การโจรกรรมตัวตน (credential theft) การปลอมแปลง (spoofing) และการปลอมตัว (masquerading)

(3) โพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) ต้องใช้กลไกการเข้ารหัสลับเพื่อปกป้องปัจจัยของการยืนยันตัวตน (authenticator) จากภัยคุกคามต่อโพรโทคอล และการโจมตีด้วยการปลอมตัวเป็นผู้อื่น

(4) โพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) ที่ใช้สื่อสารระหว่างเจ้าของลายมือชื่อกับอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) ต้องถูกปกป้องจากการโจมตีด้วยการดักรับข้อมูลเพื่อใช้ซ้ำ (reply) การโจมตีด้วยการข้ามขั้นตอน (bypass) และการโจมตีด้วยการปลอมข้อมูล (forgery) เช่น ปกป้องด้วยการใช้ค่า nonce การประทับเวลา (timestamp) หรือ โทเคนเซสชัน (session token)

(5) โมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) ต้องติดตั้งและใช้งานภายใต้ขอบเขตที่ผู้ให้บริการที่เชื่อถือได้บริหารจัดการและมีการป้องกันการเปลี่ยนแปลงข้อมูล ซึ่งเป็น

อุปกรณ์/ระบบที่เชื่อถือได้และผ่านการประเมินทั่วไปด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ (CC) ในระดับความเข้มงวดในการประเมินตามเกณฑ์ประเมินทั่วไปด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ (EAL) ที่ระดับ 4 ขึ้นไป ตามมาตรฐาน ISO/IEC 15408 หรือมาตรฐานอื่นในระดับประเทศที่เกี่ยวข้องกับการประเมินด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศของผลิตภัณฑ์ตามข้อกำหนดด้านความมั่นคงปลอดภัยที่กำหนดไว้ในข้อเสนอแนะมาตรฐานฉบับนี้

ตัวอย่างมาตรฐานด้านความมั่นคงปลอดภัยของโมดูลเข้ารหัสลับ (cryptographic module) ที่มีการรับรองตามมาตรฐาน ISO/IEC 15408 [7] [8] [9] ประกอบด้วย CEN EN 419221 [15] หรือ ISO/IEC 19790 [16] หรือ FIPS PUB 140-2 level 3 [17] เป็นต้น

(6) โพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) ต้องถูกออกแบบให้ปกป้องข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) จากการโจมตีด้วยการทำซ้ำข้อมูล หรือด้วยการเปลี่ยนแปลงแก้ไขข้อมูลได้จากผู้ที่มีศักยภาพในการโจมตีขั้นสูง

(7) โพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) ต้องถูกออกแบบให้เจ้าของลายมือชื่อสามารถปกป้องการสั่งให้สร้างลายมือชื่อด้วยข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) จากผู้ที่มีศักยภาพในการโจมตีขั้นสูง

5.3.1.2 การจัดการข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล

(1) ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) อาจเป็นชุดข้อมูล หรือผลลัพท์จากกระบวนการเข้ารหัสลับซึ่งใช้พารามิเตอร์ต่าง ๆ ที่แสดงไว้ในข้อกำหนดถัดไป

(2) ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) อาจถูกยกเลิกหรือสร้างขึ้นใหม่ภายในขอบเขตระบบงานในฝั่งของผู้ใช้งานด้วยส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) หรือด้วยการสั่งการจากระยะไกลกับส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) ที่อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อ

(3) ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ต้องเชื่อมโยงด้วยความเชื่อมั่นในระดับสูง กับพารามิเตอร์ต่าง ๆ ดังนี้

- แบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R) หรือ (ชุด) แบบแสดงข้อมูลเพื่อลงลายมือชื่อ
- ข้อมูลที่ใช้ระบุเจ้าของลายมือชื่อที่ผ่านการยืนยันตัวตน
- กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลที่ตั้งไว้เป็นค่าเริ่มต้นหรือที่ระบุไว้

ในกรณีที่เป็นไปได้ ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องปิดรับชุดแบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R) ที่มีจำนวนมากกว่าหนึ่งแบบข้อมูลเมื่อกฎหมายไม่ได้กำหนดให้สามารถทำได้หรือยังไม่มีกฎหมายรองรับ

(4) ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ต้องถูกใช้ในการสั่งให้สร้างลายมือชื่อดิจิทัลด้วยกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล ก็ต่อเมื่อการยืนยันตัวตนเจ้าของลายมือชื่อ

สำเร็จ

(5) ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ซึ่งอยู่ในโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) ต้องถูกจัดส่งให้โมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM)

(6) ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ต้อง

- ถูกเก็บรวบรวมภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่นด้วยความเชื่อมั่นในระดับสูง
- ถูกปกป้อง เพื่อรักษาความมั่นคงปลอดภัยของกุญใจใด ๆ ที่ถูกจัดเก็บไว้ในอุปกรณ์/ระบบ
- ปกป้องรักษาความลับทั้งแบบการใช้แบบครั้งเดียวหรือการใช้ในระยะเวลาตามรายละเอียดที่ระบุไว้ในข้อกำหนด 5.3.1.1(4)

(7) โพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) ต้องถูกออกแบบให้ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ที่ส่งให้กับโมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น

(8) ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ต้องถูกทวนสอบเพื่อพิจารณาว่ากิจกรรมที่เกี่ยวข้องกับการโจมตีระบบ เช่น การคาดการดักรับข้อมูล การดักรับและส่งข้อมูลซ้ำ การจัดการการสื่อสารข้อมูลจากผู้ที่มีศักยภาพในการโจมตีขั้นสูงไม่มีโอกาสในการทำลายส่วนการยืนยันตัวตนในการสั่งให้สร้างลายมือชื่อดิจิทัล

5.3.2 การบริหารจัดการกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (SRA_SKM)

5.3.2.1 การสร้างกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล

(1) กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล ต้องถูกสร้างขึ้นและใช้งานภายในอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) โดยอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) ต้องเป็นอุปกรณ์/ระบบที่เชื่อถือได้และผ่านการตรวจรับรองเกณฑ์ประเมินทั่วไปด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ (CC) ตามมาตรฐาน ISO/IEC 15408 [7] [8] [9] หรือมาตรฐานอื่นในระดับประเทศที่เกี่ยวข้องกับการประเมินด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศของผลิตภัณฑ์ตามข้อกำหนดด้านความมั่นคงปลอดภัยที่กำหนดไว้ในข้อเสนอแนะมาตรฐานฉบับนี้ ในระดับความเข้มงวดในการประเมินตามเกณฑ์ประเมินทั่วไปด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ (EAL) ที่ระดับ 4 ขึ้นไป

ตัวอย่างมาตรฐานด้านความมั่นคงปลอดภัยของโมดูลเข้ารหัสลับ (cryptographic module) ที่มีการรับรองตามมาตรฐาน ISO/IEC 15408 [7] [8] [9] ประกอบด้วย CEN EN 419221 [15] หรือ ISO/IEC 19790 [16] หรือ FIPS PUB 140-2 level 3 [17]

(2) อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) ต้องใช้เฉพาะเพื่อสนับสนุนฟังก์ชันเข้ารหัสลับของบริการสร้างลายมือชื่อดิจิทัล ซึ่งประกอบด้วยการสร้างหมายเลขสุ่มและอาจสนับสนุนกระบวนการรหัสลับของการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ

(3) เมื่ออุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) ที่ใช้สร้างกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล ไม่ได้เป็นอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) ที่ใช้สร้างลายมือชื่อดิจิทัล การจัดส่งกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล ต้องปฏิบัติตามข้อกำหนดในข้อกำหนดด้านความมั่นคงปลอดภัยทั่วในเรื่องการบริหารจัดการกุญแจ ในข้อกำหนด 5.1.5.4 (1)

(4) อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) อาจจัดเก็บกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลสำหรับเจ้าของลายมือชื่อคนเดียวและสำหรับเจ้าของลายมือชื่อดิจิทัลที่ต่างกันไว้หลายกุญแจได้ เมื่อมีการจัดเก็บกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลสำหรับเจ้าของลายมือชื่อคนเดียวและสำหรับเจ้าของลายมือชื่อดิจิทัลที่ต่างกันไว้หลายกุญแจในอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องทำให้มีความมั่นใจว่าสามารถแบ่งแยกการควบคุมของเจ้าของลายมือชื่อเพื่อเข้าถึงและใช้กุญแจของตนได้

(5) กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลต้องเชื่อมโยงกับเจ้าของลายมือชื่อเชื่อมโยงด้วยวิธีการภายใต้โพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) ด้วยความเชื่อมั่นในระดับสูง

(6) กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลต้องไม่ถูกใช้งานก่อนที่กุญแจนั้นจะถูกเชื่อมโยงกับเจ้าของลายมือชื่อด้วยระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S)

(7) ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) สามารถรองรับหรือสนับสนุนโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) และข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ได้หลายกลไกสำหรับสั่งให้สร้างลายมือชื่อด้วยกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล แต่กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลใด ๆ ต้องเชื่อมโยงกับโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) และข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ของกลไกใดกลไกหนึ่งเท่านั้น

5.3.2.2 การใช้งานกุญแจสำหรับใช้สร้างใช้ลายมือชื่อดิจิทัล

(1) ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องกำหนดให้เจ้าของลายมือชื่อแสดงข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) กับโมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) เพื่อยืนยันตัวตนและใช้งานกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล

(2) โพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) ต้องจัดส่งข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ให้โมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) ที่สามารถรับประกันความเชื่อมั่นในระดับสูงได้ว่ากุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลนั้นอยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น

(3) กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลต้องถูกสั่งให้ใช้สร้างลายมือชื่อที่ใช้การควบคุมจากระยะไกลเท่านั้น

(4) กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลต้องถูกสั่งให้ใช้สร้างลายมือด้วยข้อมูลสั่งให้สร้าง

ลายมือชื่อดิจิทัล (SAD) ที่สร้างขึ้นจากปัจจัยที่ใช้ยืนยันตัวตนของเจ้าของลายมือชื่อกับข้อมูลที่ใช้ระบุถึงกุญแจ

(5) กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลที่ถูกเรียกใช้ ต้องใช้สำหรับใช้สร้างลายมือชื่อดิจิทัลกับแบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R) ที่ถูกส่งโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) เท่านั้น

(6) เมื่อได้รับแบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R) สำหรับข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) จากแอปพลิเคชันสร้างลายมือชื่อดิจิทัล (SCA) ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องยืนยันแหล่งข้อมูลที่ส่งว่าถูกต้องและแท้จริง

(7) ผู้ใช้งานที่มีสิทธิสูงต้องไม่สามารถเข้าถึงและใช้งานกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อได้

(8) หลังจากการใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลแล้ว ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) ต้องไม่จัดเก็บข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) จากเจ้าของลายมือชื่อไว้ในรูปแบบที่ไม่มีการปกป้องเพื่อรักษาความมั่นคงปลอดภัยให้กับข้อมูล

5.4 ข้อกำหนดมาตรฐานความมั่นคงปลอดภัยสำหรับระบบ TW4S

เพื่อให้บริการระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) มีความน่าเชื่อถือ ผู้ให้บริการที่เชื่อถือได้ ต้องใช้ผลิตภัณฑ์ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) และผ่านการตรวจรับรองเกณฑ์ประเมินทั่วไปด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ (Common Criteria หรือ CC) ตามมาตรฐาน ISO/IEC 15408 [7] [8] [9] ด้วยข้อกำหนดป้องกันการดัดแปลงแก้ไข (Protection Profile) ในระดับความเข้มงวดในการประเมินตามเกณฑ์ประเมินทั่วไปด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ (EAL) ที่ระดับ 4 ขึ้นไป

ข้อกำหนดการป้องกันการดัดแปลงแก้ไข (Protection Profile) สำหรับระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) เพื่อใช้เป็นเกณฑ์ประเมินด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศของผลิตภัณฑ์ให้เป็นไปตามมาตรฐาน CEN EN 419241-2 [18] หรือข้อเสนอแนะหรือประกาศของหน่วยงานในระดับประเทศที่รับผิดชอบ

1049 **บรรณานุกรม**

1050

[1] CEN EN 419241-1 : 2018 Trustworthy Systems Supporting Server Signing, Part 1 – General System Security Requirements.

[2] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการมอบอำนาจทางอิเล็กทรอนิกส์ เลขที่ ขมธอ. 31-2565.

[3] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – กรอบการทำงาน เลขที่ ขมธอ. 18-2566 เวอร์ชัน 3.0.

[4] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการลงลายมือชื่ออิเล็กทรอนิกส์ เลขที่ ขมธอ. 23-2563, เวอร์ชัน 1.0.

[5] พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม.

[6] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and.

[7] ISO/IEC 15408-1:2022 - Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model.

[8] ISO/IEC 15408-2:2022 - Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements.

[9] ISO/IEC 15408-3:2022 - Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements.

[10] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล - ข้อกำหนดของการพิสูจน์ตัวตน เลขที่ ขมธอ. 19-2566 เวอร์ชัน 3.0.

[11] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการยืนยันตัวตน เลขที่ ขมธอ. 20-2566 เวอร์ชัน 3.0.

[12] CEN 419221-5:2018 Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services.

[13] ETSI TS 319401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers. v.2.3.1 (2021-05).

[14] ETSI TS 119312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites V1.4.2 (2022-02).

[15] CEN EN 419221-5:2018 Protection Profiles for TSP Cryptogrpahic Modules, Part 5 – Cryptographic Module for Trust Services.

[16] ISO/IEC 19790:2012 Information technology — Security techniques — Security requirements for cryptographic modules.

[17] FIPS PUB 140-2 Security Requirements for Cryptographic Modules.

[18] CEN EN 419241-2:2018 Trustworthy Systems Supporting Server Signing, Part 2 – Protection profile for QSCD for Server Signing.

[19] Cloud Signature Consortium Standard (Version 1.0.3.0): "Architectures and protocols for remote signature applications"..

[20] ETSI EN 319403-1 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers.

[21] ETSI EN 319411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements V1.3.1 (2021-05).

[22] ETSI TS 119431-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev. v1.2.1 (2021-05).

[23] OASIS Standard: "Advanced Electronic Signature Profiles of the OASIS Digital Signature Service Version 2.0", Working Draft 02..

[24] OASIS Standard: "Digital Signature Service Core Protocols, Elements, and Bindings Version 2.0", Committee Specification Draft 03 / Public Review Draft 03..

[25] ETSI TS 119432 Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation. v.1.1.1 (2019-03).

1051