ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
เรื่อง ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์
ว่าด้วยบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล

โดยที่เป็นการสมควรอธิบายส่วนประกอบและหลักการทำงานที่เกี่ยวข้องกับการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote signing) โดยอาศัยระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (trustworthy systems supporting server signing: TW4S) ในการสร้างลายมือชื่อดิจิทัล เพื่อรับประกันว่ากุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น (sole control) รวมทั้งระบุข้อกำหนดด้านความมั่นคงปลอดภัยของ TW4S เพื่อให้หน่วยงานต่าง ๆ ในประเทศไทยสามารถใช้บริการหรือให้บริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกลได้โดยมีความน่าเชื่อถือและเป็นมาตรฐานเดียวกัน

อาศัยอำนาจตามความในมาตรา ๕ แห่งพระราชบัญญัติสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๒ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ จึงประกาศข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล เลขที่ ขมธอ. ๓๖-๒๕๖๖ ปรากฏตามท้ายประกาศฉบับนี้

ประกาศ ณ วันที่ ๓๐ มิถุนายน พ.ศ. ๒๕๖๖

(นายชาติชาย สุทธาเวศ)
รองผู้อำนวยการ
ปฏิบัติการแทนผู้อำนวยการ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ETDA Recommendation on ICT Standard

for Electronic Transactions

ขมธอ. 36-2566

ว่าด้วยบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล

REMOTE SIGNING SERVICE

เวอร์ชัน 1.0

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ICS 35.030

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล

ขมธอ. 36-2566

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 30 มิถุนายน พ.ศ. 2566

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

วิเคราะห์และจัดทำข้อเสนอแนะมาตรฐานฯ
ว่าด้วยบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล

นายณัฐฑพัฒน์ โรจนศุภมิตร	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายจิรายุ ภูโต	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายวรัชญ์ เฉลิมพรพงศ์	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายพงษ์พันธ์ ศรีปาน	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายวีรศักดิ์ ดีอ่ำ	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นางสาววราภรณ์ หลีสกุล	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายรุ่งโรจน์ กิตติถาวรกุล	จุฬาลงกรณ์มหาวิทยาลัย
นายสรณันท์ จิวะสุรัตน์	จุฬาลงกรณ์มหาวิทยาลัย
นายสาวจินตนา ชูพันธ์	จุฬาลงกรณ์มหาวิทยาลัย
นางสาวชัชยาวรรณ คูเมืองแมนสิริ	จุฬาลงกรณ์มหาวิทยาลัย

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกลฉบับนี้ จัดทำขึ้นเพื่ออธิบายส่วนประกอบและหลักการทำงานที่เกี่ยวข้องกับการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote signing) โดยอาศัยระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (trustworthy systems supporting server signing: TW4S) ในการสร้างลายมือชื่อดิจิทัล เพื่อรับประกันว่ากุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น (sole control) รวมทั้งระบุข้อกำหนดด้านความมั่นคงปลอดภัยของ TW4S เพื่อให้หน่วยงานต่าง ๆ ในประเทศไทยสามารถใช้บริการหรือให้บริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกลได้โดยมีความน่าเชื่อถือและเป็นมาตรฐานเดียวกัน

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 และการบริหารจัดการกุญแจส่วนตัวเพื่อนำมาใช้ลงลายมือชื่อดิจิทัลได้อย่างสะดวกนั้นไม่ใช่สิ่งที่ผู้ใช้งานทั่วไปจะกระทำเองได้โดยง่าย การลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote signing) จึงเป็นวิธีการที่เป็นทางเลือกและได้รับการยอมรับในหลายประเทศ เช่น สหภาพยุโรป เนื่องจากสามารถอำนวยความสะดวกให้กับผู้ใช้งานในการเก็บรักษาและเรียกใช้งานกุญแจส่วนตัวผ่านระบบเครือข่ายคอมพิวเตอร์ เมื่อได้ดำเนินการด้วยวิธีการที่เชื่อถือได้และมีความมั่นคงปลอดภัย

ด้วยเหตุนี้ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์จึงได้จัดทำข้อเสนอแนะมาตรฐาน ฯ ว่าด้วยบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล เพื่ออธิบายส่วนประกอบและหลักการทำงานที่เกี่ยวข้องกับการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote signing) โดยอาศัยระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (trustworthy systems supporting server signing: TW4S) ในการสร้างลายมือชื่อดิจิทัล เพื่อรับประกันว่ากุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น (sole control) รวมทั้งระบุข้อกำหนดด้านความมั่นคงปลอดภัยของ TW4S เพื่อให้หน่วยงานต่าง ๆ ในประเทศไทยสามารถใช้บริการหรือให้บริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกลได้โดยมีความน่าเชื่อถือและเป็นมาตรฐานเดียวกัน โดยข้อเสนอแนะมาตรฐานฉบับนี้มีการอ้างอิงข้อกำหนดจากมาตรฐานของสหภาพยุโรป

สารบัญ

สารบัญรูป

หน้า

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ว่าด้วยบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล

1. ขอบข่าย

ข้อเสนอแนะมาตรฐานฉบับนี้อธิบายส่วนประกอบและหลักการทำงานที่เกี่ยวข้องกับการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote signing) โดยอาศัยระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (trustworthy systems supporting server signing: TW4S) ในการสร้างลายมือชื่อดิจิทัล เพื่อรับประกันว่ากุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น (sole control) รวมทั้งระบุข้อกำหนดด้านความมั่นคงปลอดภัยของ TW4S เพื่อให้หน่วยงานต่าง ๆ ในประเทศไทยสามารถใช้บริการหรือให้บริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกลได้โดยมีความน่าเชื่อถือและเป็นมาตรฐานเดียวกัน

ข้อเสนอแนะมาตรฐานฉบับนี้สามารถใช้ได้ในกรณีดังนี้

- การสร้างลายมือชื่อดิจิทัลครั้งละหลายรายการ (bulk/batch signing) ซึ่งเป็นการสร้างลายมือชื่อดิจิทัลภายในช่วงระยะเวลาที่กำหนดไว้ช่วงหนึ่ง หรือการสร้างลายมือชื่อดิจิทัลที่กำหนดไว้จำนวนหนึ่ง ในนามของเจ้าของลายมือชื่อหลังการยืนยันตัวตนเจ้าของลายมือชื่อเป็นผลสำเร็จ อย่างไรก็ตาม การพิจารณาใช้รูปแบบการสร้างลายมือชื่อดิจิทัลครั้งละหลายรายการควรคำนึงถึงข้อกำหนดทางกฎหมายที่เกี่ยวข้องด้วยว่าอนุญาตให้เจ้าของลายมือชื่อดำเนินการได้หรือไม่
- การลงลายมือชื่ออิเล็กทรอนิกส์ (electronic signature) ของบุคคล หรือการประทับตราอิเล็กทรอนิกส์ (electronic seal) ของนิติบุคคล ดังนั้น คำนิยามที่กำหนดไว้เกี่ยวกับเจ้าของลายมือชื่อจะมีความหมายครอบคลุมถึงนิติบุคคลที่เป็นเจ้าของตราอิเล็กทรอนิกส์ด้วย

ทั้งนี้ ข้อเสนอแนะมาตรฐานฉบับนี้จะไม่ครอบคลุมถึง

- รายละเอียดของสถาปัตยกรรมระบบสารสนเทศสำหรับระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) เช่น จำนวนเครื่องบริการที่จำเป็นต้องใช้
- รายละเอียดของส่วนประกอบที่เกี่ยวข้องกับการสร้างลายมือชื่อดิจิทัล ซึ่งอยู่นอกขอบเขตของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) เช่น แอปพลิเคชันสร้างลายมือชื่อดิจิทัล (signature creation application: SCA) หรือแอปพลิเคชันของผู้ใช้งาน (client application)
- รายละเอียดของบริการสนับสนุนอื่น ๆ ที่ใช้ประกอบกับบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล เช่น บริการออกใบรับรอง บริการประทับเวลาอิเล็กทรอนิกส์ หรือบริการพิสูจน์และยืนยันตัวตน

ข้อเสนอแนะมาตรฐานฉบับนี้อ้างอิงข้อกำหนดจากมาตรฐานของสหภาพยุโรป [1]

ข้อเสนอแนะมาตรฐานฉบับนี้มีรูปแบบของคำที่ใช้แสดงออกถึงคุณลักษณะของเนื้อหาเชิงบรรทัดฐาน (normative) และเนื้อหาเชิงให้ข้อมูล (informative) ดังต่อไปนี้

- “ต้อง” ใช้ระบุสิ่งที่เป็นข้อกำหนด (requirement) ซึ่งต้องปฏิบัติตาม
- “ควร” ใช้ระบุสิ่งที่เป็นข้อแนะนำ (recommendation)
- “อาจ” ใช้ระบุสิ่งที่ยินยอมหรืออนุญาตให้ทำได้ (permission)

2. บทนิยาม

ความหมายของคำที่ใช้ในข้อเสนอแนะมาตรฐานฉบับนี้ มีดังต่อไปนี้

2.1 ลายมือชื่อดิจิทัล (digital signature) หมายถึง ลายมือชื่ออิเล็กทรอนิกส์ที่ได้จากกระบวนการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ ซึ่งช่วยให้สามารถยืนยันตัวเจ้าของลายมือชื่อและตรวจพบการเปลี่ยนแปลงของข้อความและลายมือชื่ออิเล็กทรอนิกส์ได้ รวมถึงการทำให้เจ้าของลายมือชื่อไม่สามารถปฏิเสธความรับผิดจากข้อความที่ตนเองลงลายมือชื่อได้ [2]

2.2 กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) หมายถึง กุญแจส่วนตัว (private key) ในระบบการเข้ารหัสลับแบบอสมมาตร (asymmetric cryptography) สำหรับใช้สร้างลายมือชื่อดิจิทัล

2.3 เจ้าของลายมือชื่อ (signer) หมายถึง ผู้ซึ่งถือกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) และสร้างลายมือชื่อดิจิทัลนั้นในนามตนเองหรือแทนบุคคลอื่น

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

2.5 บริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote signing service) หรือ บริการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (server signing service) หมายถึง บริการสร้างลายมือชื่อดิจิทัล ที่มีระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) เพื่อให้เจ้าของลายมือชื่อสามารถควบคุมกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) และรับประกันว่ากุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลนั้นอยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น (sole control)

2.6 ผู้ให้บริการ หมายถึง หน่วยงานที่ให้บริการระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S)

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

2.8 การยืนยันตัวตน (authentication) หมายถึง กระบวนการยืนยันอัตลักษณ์ของบุคคลด้วยการตรวจสอบสิ่งที่ใช้ยืนยันตัวตนของบุคคลนั้น [3]

2.9 แบบแสดงข้อมูลเพื่อลงลายมือชื่อ (data to be signed representation: DTBS/R) หมายถึง ข้อมูลที่ถูกจัดรูปแบบเพื่อนำมาคำนวณในการสร้างค่าลายมือชื่อดิจิทัล (digital signature value)

2.10 ใบรับรอง (certificate) หมายถึง ข้อมูลอิเล็กทรอนิกส์หรือการบันทึกอื่นใด ซึ่งยืนยันความเชื่อมโยงระหว่างเจ้าของลายมือชื่อกับข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์ [4]

2.11 ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (signature activation data: SAD) หมายถึง ชุดข้อมูลที่รวบรวมโดยโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) เพื่อใช้ในการควบคุมด้วยความเชื่อมั่นในระดับสูงว่าการดำเนินการสร้างลายมือชื่อดิจิทัล (signature operation) อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น

2.12 โพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (signature activation protocol: SAP) หมายถึง โพรโทคอลที่รวบรวมข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) เพื่อใช้ในการควบคุมการดำเนินการสร้างลายมือชื่อดิจิทัล (signature operation) ต่อแบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R) โดยอาศัยกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) ของเจ้าของลายมือชื่อ

2.13 อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (signature creation device: SCDev) หมายถึง ซอฟต์แวร์หรือฮาร์ดแวร์ที่ออกแบบให้ใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) ในการสร้างค่าลายมือชื่อดิจิทัล (digital signature value) ด้วยโมดูลเข้ารหัสลับ (cryptographic module)

2.14 อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote signature creation device: remote SCDev) หมายถึง อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) ที่เจ้าของลายมือชื่อสามารถควบคุมการดำเนินการสร้างลายมือชื่อดิจิทัล (signature operation) จากระยะไกล และรับประกันด้วยความเชื่อมั่นในระดับสูงว่ากุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น

2.15 โมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (signature activation module: SAM) หมายถึง ซอฟต์แวร์ที่ออกแบบให้ใช้ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) เพื่อรับประกันด้วยความเชื่อมั่นในระดับสูงว่าการใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น

2.16 แอปพลิเคชันสร้างลายมือชื่อดิจิทัล (signature creation application: SCA) หมายถึง แอปพลิเคชันที่ใช้ลงลายมือชื่อในเอกสารอิเล็กทรอนิกส์ด้วยลายมือชื่อดิจิทัลที่สร้างจากอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev)

2.17 แอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (server signing application: SSA) หมายถึง แอปพลิเคชันที่ใช้อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote SCDev) ในการสร้างค่าลายมือชื่อดิจิทัล (digital signature value) ในนามของเจ้าของลายมือชื่อ

2.18 ส่วนติดต่อของเจ้าของลายมือชื่อ (signer's interaction component: SIC) หมายถึง ส่วนประกอบในรูปแบบซอฟต์แวร์และ/หรือฮาร์ดแวร์ที่เจ้าของลายมือชื่อใช้ในการทำงานร่วมกับโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP)

3. อักษรย่อ

อักษรย่อที่ใช้ในข้อเสนอแนะมาตรฐานฉบับนี้ มีดังต่อไปนี้

อักษรย่อ	คำเต็ม	คำภาษาไทย
AAL	Authentication Assurance Level	ระดับความน่าเชื่อถือของการยืนยันตัวตน
CA	Certificate Authority	ผู้ให้บริการออกใบรับรอง
CC	Common Criteria	เกณฑ์ประเมินทั่วไปด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ [5] [6] [7]
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
IAL	Identity Assurance Level	ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน
IdP	Identity Provider	ผู้พิสูจน์และยืนยันตัวตน
ISO/IEC	International Organization for Standardization/ International Electrotechnical Commission	องค์การระหว่างประเทศว่าด้วยการมาตรฐาน/ คณะกรรมาธิการระหว่างประเทศว่าด้วยมาตรฐานสาขาอิเล็กทรอนิกส์
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
SIC	Signer’s Interaction Component	ส่วนติดต่อของเจ้าของลายมือชื่อ
SSA	Server Signing Application	แอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ
TSA	Time-stamping Authority	ผู้ให้บริการประทับเวลา
TW4S	Trustworthy System Supporting Server Signing	ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้

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

4.1 สถาปัตยกรรมแนวคิดของการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล

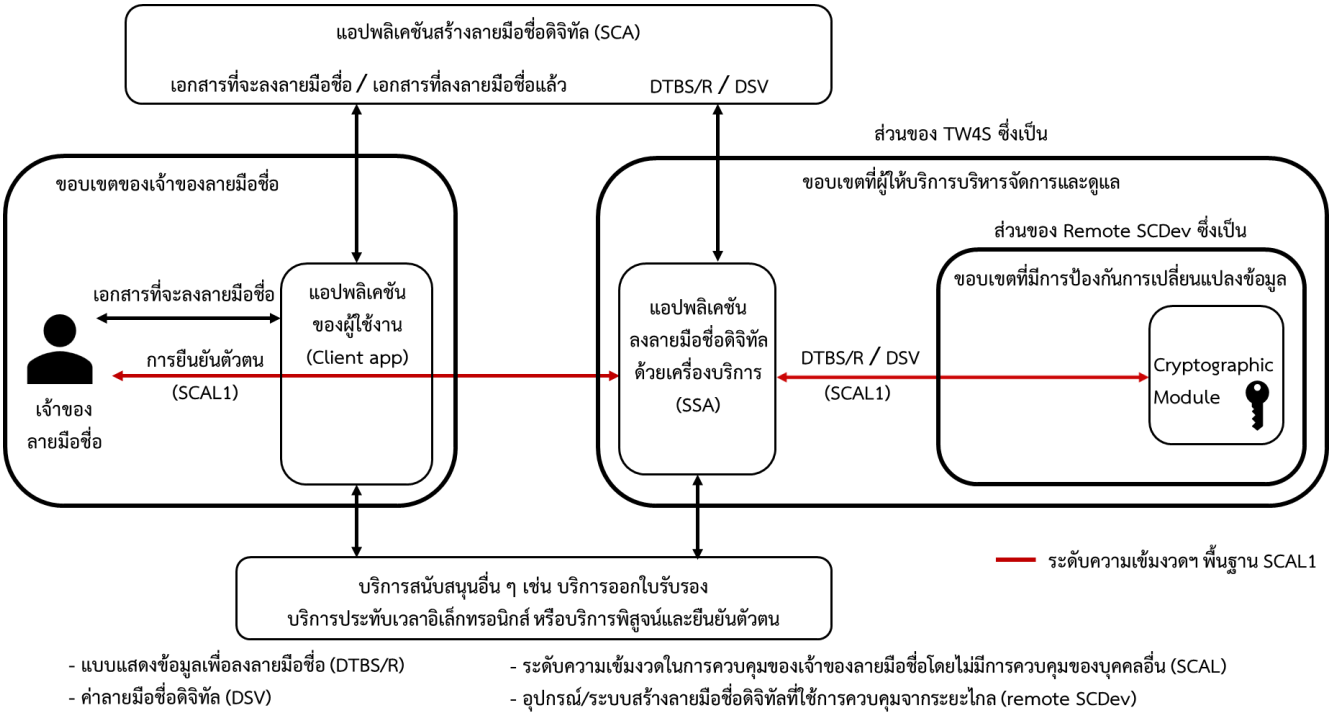
สถาปัตยกรรมแนวคิด (conceptual architecture) ของการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote signing) อาศัยการทำงานร่วมกันระหว่างแอปพลิเคชันสร้างลายมือชื่อดิจิทัล (signature creation application: SCA) และแอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (server signing application: SSA) ที่ใช้อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote signature creation device: remote SCDev) รวมถึงองค์ประกอบหรือบริการสนับสนุนอื่น ๆ ที่เกี่ยวข้อง โดยคำนึงถึงความมั่นใจของการควบคุมกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล

หมายเหตุ: บริการสนับสนุนอื่น ๆ ที่ใช้ประกอบกับบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล เช่น บริการออกใบรับรอง บริการประทับเวลาอิเล็กทรอนิกส์ หรือบริการพิสูจน์และยืนยันตัวตน จะไม่อยู่ในขอบข่ายของข้อเสนอแนะมาตรฐานฉบับนี้

องค์ประกอบหลักสององค์ประกอบของสถาปัตยกรรมแนวคิดข้างต้น ซึ่งได้แก่ แอปพลิเคชันสร้างลายมือชื่อดิจิทัล (SCA) และแอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) มีหลักการทำงาน ดังนี้

- แอปพลิเคชันสร้างลายมือชื่อดิจิทัล (SCA) ทำหน้าที่สร้างลายมือชื่อดิจิทัลให้กับเอกสารที่จะลงลายมือชื่อและจัดรูปแบบเป็นเอกสารที่ลงลายมือชื่อแล้ว โดยมีข้อมูลเข้าหลัก (main input) ที่รับมาจากแอปพลิเคชันของผู้ใช้งาน (client application) คือ เอกสารหรือค่าแฮชของเอกสารที่จะลงลายมือชื่อ (และพารามิเตอร์อื่น ๆ) และมีข้อมูลออกหลัก (main output) ที่ส่งกลับไปยังแอปพลิเคชันของผู้ใช้งาน (client application) คือ เอกสารที่ลงลายมือชื่อแล้ว
- แอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) ทำหน้าที่ใช้อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote SCDev) ในการสร้างค่าลายมือชื่อดิจิทัล (digital signature value: DSV) โดยมีข้อมูลเข้าหลัก (main input) ที่รับมาจากแอปพลิเคชันสร้างลายมือชื่อดิจิทัล (SCA) คือ แบบแสดงข้อมูลเพื่อลงลายมือชื่อ (data to be signed representation: DTBS/R) (และพารามิเตอร์อื่น ๆ) และมีข้อมูลออกหลัก (main output) ที่ส่งกลับไปยังแอปพลิเคชันสร้างลายมือชื่อดิจิทัล (SCA) คือ ค่าลายมือชื่อดิจิทัล (DSV)

ข้อเสนอแนะมาตรฐานฉบับนี้กำหนดความมั่นใจของการควบคุมกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลเป็นระดับ ที่เรียกว่า “ระดับความเข้มงวดในการควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น (sole control assurance level: SCAL)” ทั้งนี้ สถาปัตยกรรมแนวคิดของการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล ที่ระดับความเข้มงวดฯ พื้นฐาน SCAL1 และระดับความเข้มงวดฯ ขั้นสูง SCAL2 สามารถแสดงเป็นแผนภาพตามรูปที่ 1 และรูปที่ 2 ตามลำดับ



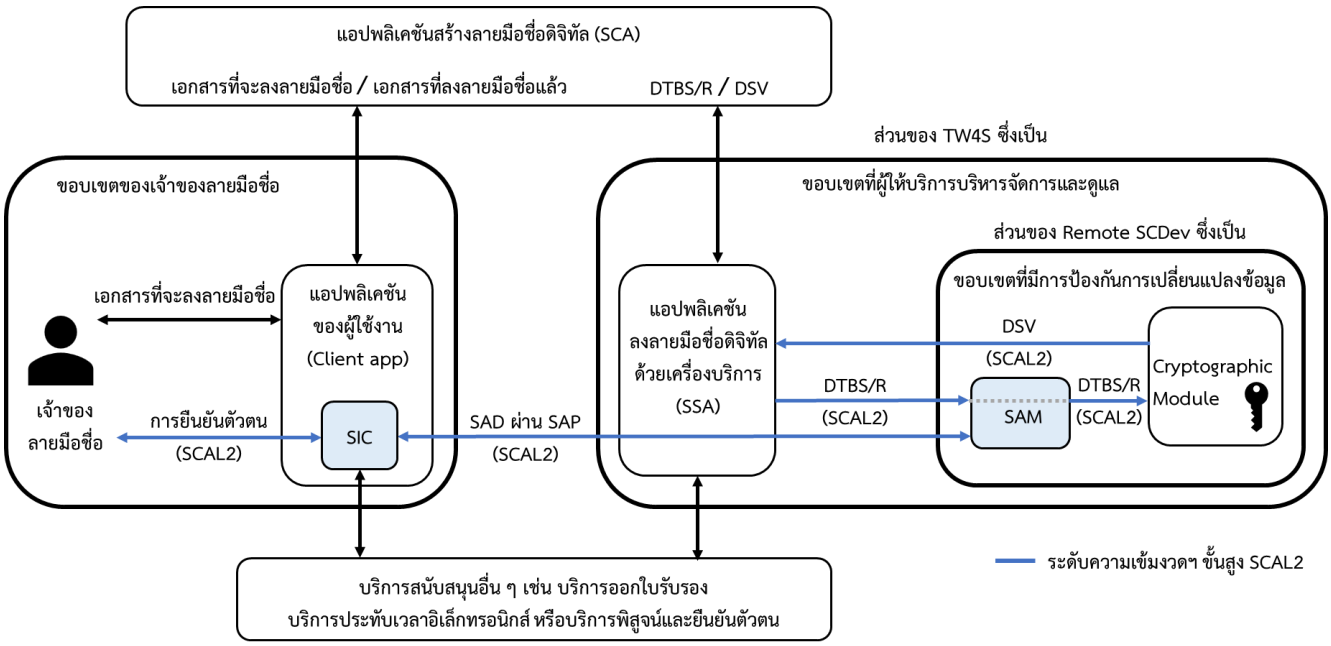
รูปที่ 1 สถาปัตยกรรมแนวคิดของการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล ที่ระดับ SCAL1

ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (trustworthy system supporting server signing: TW4S) เป็นระบบที่มีสถาปัตยกรรมในรูปแบบเครื่องขอใช้บริการและเครื่องบริการ (client-server system) ที่ออกแบบเพื่อให้เจ้าของลายมือชื่อสามารถควบคุมกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) และรับประกันว่ากุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลนั้นอยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น

โดยทั่วไป ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) จะถูกใช้งานโดยเจ้าของลายมือชื่อหลายคน และเจ้าของลายมือชื่อแต่ละคนอาจจะเป็นเจ้าของหรือผู้ควบคุมกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลหนึ่งกุญแจหรือหลายกุญแจก็ได้ ทั้งนี้ TW4S จะประกอบด้วยแอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) และอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote SCDev) ซึ่งทำให้เจ้าของลายมือชื่อสามารถควบคุมกุญแจจากระยะไกล (remote control) ได้

หมายเหตุ: รายละเอียดของแอปพลิเคชันสร้างลายมือชื่อดิจิทัล (SCA) จะไม่อยู่ในขอบข่ายของข้อเสนอแนะมาตรฐานฉบับนี้ เนื่องจากแอปพลิเคชันสร้างลายมือชื่อดิจิทัล (SCA) ไม่ถือเป็นส่วนประกอบที่อยู่ใน TW4S

ในกรณีที่เป็นระดับ SCAL2 อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote SCDev) จะมีโมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (signature activation module: SAM) ที่ติดตั้งภายในขอบเขตที่มีการป้องกันการเปลี่ยนแปลงข้อมูล มาทำหน้าที่สนับสนุนการควบคุมกุญแจจากระยะไกล (remote control) นอกจากนี้ ในขอบเขตของเจ้าของลายมือชื่อ ส่วนติดต่อของเจ้าของลายมือชื่อ (signer's interaction component: SIC) จะทำหน้าที่ยืนยันตัวตนเจ้าของลายมือชื่อ สร้างข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (signature activation data: SAD) และส่งไปยังโมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM)



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

รูปที่ 2 สถาปัตยกรรมแนวคิดของการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล ที่ระดับ SCAL2

กระบวนการทำงานและข้อมูลที่สำคัญของแอปพลิเคชันสร้างลายมือชื่อดิจิทัล (SCA) และแอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) มีรายละเอียด ดังนี้

4.1.1 แอปพลิเคชันสร้างลายมือชื่อดิจิทัล (signature creation application: SCA)

กระบวนการสร้างลายมือชื่อดิจิทัลด้วยแอปพลิเคชันสร้างลายมือชื่อดิจิทัล (SCA) ประกอบด้วยขั้นตอนที่สำคัญ ดังนี้

(1) แอปพลิเคชันสร้างลายมือชื่อดิจิทัล (SCA) รับเอกสารหรือค่าแฮชของเอกสารที่จะลงลายมือชื่อในกรณีที่ผู้ใช้งานนำเข้าข้อมูลเป็นเอกสาร แอปพลิเคชันสร้างลายมือชื่อดิจิทัล (SCA) จะคำนวณค่าแฮชของเอกสารนั้น

(2) แอปพลิเคชันสร้างลายมือชื่อดิจิทัล (SCA) นำค่าแฮชของเอกสารที่จะลงลายมือชื่อ และค่าแฮชของรายการข้อมูลที่จะลงลายมือชื่อ (signed attributes) ทั้งหมด (เช่น หมายเลขใบรับรอง) มาจัดองค์ประกอบ จัดรูปแบบ และคำนวณค่าแฮชออกมาเป็นแบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R) จากนั้น แอปพลิเคชันสร้างลายมือชื่อดิจิทัล (SCA) จะส่งแบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R) ไปยังแอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) ของ TW4S เพื่อสร้างค่าลายมือชื่อดิจิทัล (DSV) (รายละเอียดตามหัวข้อ 4.1.2)

(3) แอปพลิเคชันสร้างลายมือชื่อดิจิทัล (SCA) จะรับค่าลายมือชื่อดิจิทัล (DSV) ที่สร้างจากแอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) ของ TW4S มารวมกับพารามิเตอร์อื่น ๆ และจัดรูปแบบเป็นเอกสารที่ลงลายมือชื่อแล้วตามรูปแบบที่ผู้ใช้งานร้องขอ เช่น เอกสาร XML ที่ลงลายมือชื่อดิจิทัล

แบบ XAdES (XML Advanced Electronic Signature) เอกสาร PDF ที่ลงลายมือชื่อดิจิทัลแบบ PAdES (PDF Advanced Electronic Signature) หรือเอกสารที่บรรจุเอกสารต้นฉบับพร้อมลายมือชื่อดิจิทัลแบบ CAdES (CMS Advanced Electronic Signature)

4.1.2 แอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (server signing application: SSA)

กระบวนการเรียกใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key activation) และการสร้างค่าลายมือชื่อดิจิทัล (DSV creation) ด้วยแอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) ประกอบด้วยขั้นตอนที่สำคัญ ดังนี้

(1) แอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) ใช้อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote SCDev) เพื่อสร้าง เก็บรักษา และใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลภายใต้การควบคุมของเจ้าของลายมือชื่อที่ได้รับอนุญาต ทั้งนี้ เจ้าของลายมือชื่อที่ได้รับอนุญาตสามารถควบคุมกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลได้จากระยะไกลด้วยระดับความเข้มงวดในการควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น (SCAL) ซึ่งแบ่งออกเป็น 2 ระดับ ดังนี้ (รายละเอียดตามหัวข้อ 4.2)

- ระดับความเข้มงวดฯ พื้นฐาน SCAL1

  ที่ระดับ SCAL1 การใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลจะถูกควบคุมโดยแอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) ซึ่งจะทำหน้าที่ยืนยันตัวตนเจ้าของลายมือชื่อ

- ระดับความเข้มงวดฯ ขั้นสูง SCAL2

  ที่ระดับ SCAL2 การใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลจะถูกควบคุมโดยโมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) ซึ่งจะทำหน้าที่ตรวจสอบความถูกต้องของข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ที่มาจากการยืนยันตัวตนเจ้าของลายมือชื่อ

ทั้งนี้ การยืนยันตัวตนเจ้าของลายมือชื่อจะช่วยทำให้มีความมั่นใจว่ากุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลอยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น

(2) อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote SCDev) ใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลเพื่อสร้างค่าลายมือชื่อดิจิทัล (DSV) กับแบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R) ภายหลังจากแอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) ยืนยันตัวตนเจ้าของลายมือชื่อ (signer authentication) จนเป็นผลสำเร็จ (ในกรณีของระดับ SCAL1) หรือภายหลังจากโมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) ตรวจสอบความถูกต้องของข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD verification) จนเป็นผลสำเร็จ (ในกรณีของระดับ SCAL2)

4.2 ระดับความเข้มงวดในการควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น (sole control assurance level: SCAL)

ระดับความเข้มงวดในการควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น (SCAL) ของ TW4S แบ่งออกเป็น 2 ระดับ ดังนี้

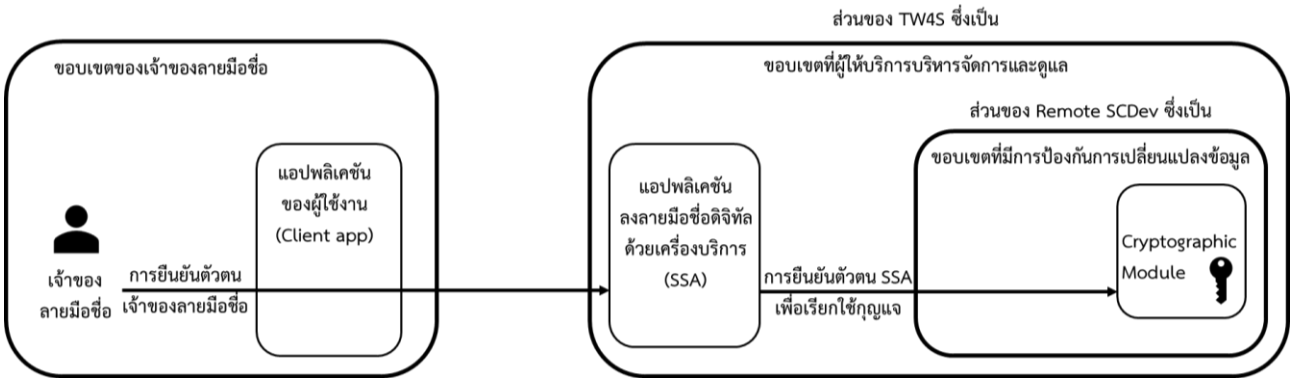
4.2.1 ระดับความเข้มงวดฯ พื้นฐาน SCAL1

ระดับ SCAL1 มีคุณสมบัติ ดังนี้ (ตามรูปที่ 3)

(1) ระดับ SCAL1 รับประกันความเชื่อมั่นในระดับพื้นฐานว่าการใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น จึงอาจใช้กับธุรกรรมที่ไม่ได้มีมูลค่าสูงหรือไม่ได้มีความสำคัญ

(2) การรักษาความลับและความครบถ้วนสมบูรณ์ของกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลได้รับการดูแลโดยอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote SCDev) ซึ่งสามารถเปิดใช้งานได้โดยแอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA)

(3) แอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) จะทำหน้าที่ยืนยันตัวตนเจ้าของลายมือชื่อจนเป็นผลสำเร็จก่อน จึงจะเรียกใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลเพื่อดำเนินการสร้างลายมือชื่อดิจิทัลในนามของเจ้าของลายมือชื่อ



รูปที่ 3 การยืนยันตัวตนและการเรียกใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล ที่ระดับ SCAL1

4.2.2 ระดับความเข้มงวดฯ ขั้นสูง SCAL2

ระดับ SCAL2 มีคุณสมบัติ ดังนี้ (ตามรูปที่ 4)

(1) ระดับ SCAL2 รับประกันความเชื่อมั่นในระดับสูงว่าการใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น จึงอาจใช้กับธุรกรรมที่มีมูลค่าสูงหรือมีความสำคัญ

(2) การรักษาความลับและความครบถ้วนสมบูรณ์ของกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลได้รับการดูแลโดยอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote SCDev) ซึ่งจะอยู่ภายใต้การควบคุมของแอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA)

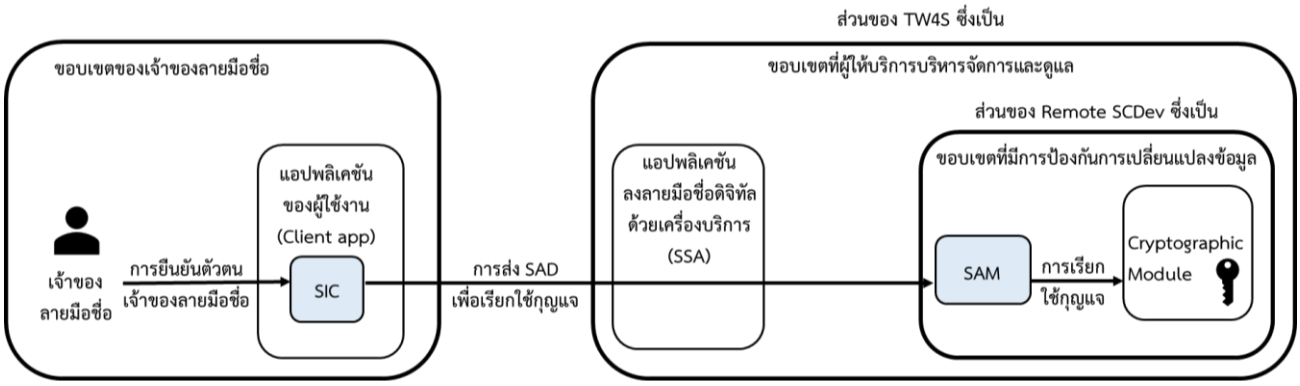
(3) แอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) ประสานกับโมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) ซึ่งเป็นซอฟต์แวร์ภายในอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote SCDev) ผ่านช่องทางการสื่อสารที่มีความมั่นคงปลอดภัย

(4) โมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) จะทำหน้าที่ตรวจสอบความถูกต้องของข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ที่มาจากการยืนยันตัวตนเจ้าของลายมือชื่อ จนเป็นผลสำเร็จก่อน จึงจะเรียกใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลเพื่อดำเนินการสร้างลายมือชื่อดิจิทัลในนามของ

เจ้าของลายมือชื่อ

(5) ส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) จะทำหน้าที่ยืนยันตัวตนเจ้าของลายมือชื่อ และสร้างข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ที่เชื่อมโยงการยืนยันตัวตนเจ้าของลายมือชื่อ เข้ากับกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล และแบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R)

(6) ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ต้องถูกส่งผ่านช่องทางการสื่อสารที่มีความมั่นคงปลอดภัยจากส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) ไปยังโมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) เพื่อตรวจสอบความถูกต้อง



รูปที่ 4 การยืนยันตัวตนและการเรียกใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล ที่ระดับ SCAL2

ทั้งนี้ การเลือกระดับ SCAL สามารถพิจารณาใช้งานให้เหมาะสมกับลักษณะ ประเภท หรือขนาดของธุรกรรมที่ทำ หรือเป็นไปตามที่กฎหมายกำหนด

4.3 การพิสูจน์และยืนยันตัวตนของเจ้าของลายมือชื่อ

4.3.1 การพิสูจน์ตัวตน

ระดับ SCAL1: การพิสูจน์ตัวตนของเจ้าของลายมือชื่อต้องมีความเข้มงวดที่ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน IAL1 ขึ้นไป [8]

ระดับ SCAL2: การพิสูจน์ตัวตนของเจ้าของลายมือชื่อต้องมีความเข้มงวดที่ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน IAL2 ขึ้นไป [8]

4.3.2 การยืนยันตัวตน

ระดับ SCAL1: การยืนยันตัวตนของเจ้าของลายมือชื่อต้องมีความเข้มงวดที่ระดับความน่าเชื่อถือของการยืนยันตัวตน AAL1 ขึ้นไป [9]

ระดับ SCAL2: การยืนยันตัวตนของเจ้าของลายมือชื่อต้องมีความเข้มงวดที่ระดับความน่าเชื่อถือของการยืนยันตัวตน AAL2 ขึ้นไป [9]

4.3.3 เป้าหมายของการยืนยันตัวตน

4.3.3.1 ระดับ SCAL1

(1) เจ้าของลายมือชื่อต้องยืนยันตัวตนกับแอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) จนสำเร็จก่อน จึงจะอนุญาตให้เข้าถึงการดำเนินการสร้างลายมือชื่อดิจิทัล

(2) แอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) ต้องเชื่อมโยงกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) ของเจ้าของลายมือชื่อไปยังสิ่งที่ใช้ยืนยันตัวตน (authenticator) ของเจ้าของลายมือชื่อ

4.3.3.2 ระดับ SCAL2

(1) ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ต้องถูกสร้างขึ้นหรือเป็นผลลัพธ์ที่เกิดจากการทำงานร่วมกันที่มีความมั่นคงปลอดภัยระหว่างโมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) กับส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) ผ่านแอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) เพื่ออนุญาตให้สร้างลายมือชื่อดิจิทัลภายในอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev)

(2) ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ต้องถูกส่งไปยังโมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) ผ่านแอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) เพื่อจะอนุญาตให้อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) สร้างลายมือชื่อดิจิทัลกับแบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R) ที่ระบุไว้

4.3.4 การพิสูจน์และยืนยันตัวตนจากบุคคลภายนอก

การพิสูจน์และยืนยันตัวตนของ TW4S อาจใช้บริการพิสูจน์และยืนยันตัวตนจากบุคคลภายนอกที่เป็นผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP)

4.3.4.1 ระดับ SCAL1

ผู้ให้บริการต้องทำให้มีความมั่นใจว่าการพิสูจน์และยืนยันตัวตนจากบุคคลภายนอกเป็นไปตามข้อกำหนดที่ระบุไว้ในหัวข้อ 5.2.2.1(1)

4.3.4.2 ระดับ SCAL2

ผู้ให้บริการต้องทำให้มีความมั่นใจว่าการพิสูจน์และยืนยันตัวตนจากบุคคลภายนอกเป็นไปตามข้อกำหนดที่ระบุไว้ในหัวข้อ 5.3.1.1(1) และต้องทำให้มีความมั่นใจว่าคุณสมบัติของบุคคลภายนอกหรือการพิสูจน์และยืนยันตัวตนจากบุคคลภายนอก เป็นไปตามที่กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์กำหนด [4]

4.4 กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) และโมดูลเข้ารหัสลับ (cryptographic module)

ในการสร้างลายมือชื่อดิจิทัลที่ระดับ SCAL1 กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) ไม่จำเป็นต้องถูกสร้าง จัดเก็บ และใช้งานภายในโมดูลเข้ารหัสลับ (cryptographic module) เช่น อุปกรณ์ hardware security module (HSM) หรือสมาร์ทการ์ด (smart card) ดังนั้น กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลอาจถูกจัดเก็บในรูปแบบไฟล์ข้อมูล และอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) อาจเป็นซอฟต์แวร์ที่นำกุญแจในรูปแบบไฟล์ข้อมูลนั้นมาใช้งาน

ทั้งนี้ หากกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลอยู่ในรูปแบบไฟล์ข้อมูล ผู้ให้บริการควรจัดให้มีมาตรการด้านความมั่นคงปลอดภัยเพิ่มเติมนอกเหนือจากการป้องกันการเปลี่ยนแปลงไฟล์ข้อมูล

อย่างไรก็ตาม ข้อเสนอแนะมาตรฐานฉบับนี้แนะนำให้ TW4S ใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) ที่จัดเก็บภายในขอบเขตที่มีการป้องกันการเปลี่ยนแปลงข้อมูล (รายละเอียดตามหัวข้อ 4.9.1)

หรือกล่าวคือ อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) ควรเป็นโมดูลเข้ารหัสลับ (cryptographic module) ที่มีการรับรองตามมาตรฐานด้านความมั่นคงปลอดภัยที่ได้รับการยอมรับในระดับสากล เช่น CEN EN 419221-5 [10]

4.5 ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (signature activation data: SAD)

ในการเรียกใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลที่ระดับ SCAL2 โมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) ต้องใช้ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) เพื่อรับประกันว่ากุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อ และต้องเป็นไปตามเงื่อนไขและข้อกำหนดต่าง ๆ เช่น การยืนยันตัวตนเจ้าของลายมือชื่อ และการตรวจสอบความถูกต้องของคำขอสร้างลายมือชื่อดิจิทัลจากเจ้าของลายมือชื่อ (รายละเอียดตามหัวข้อ 4.3)

เงื่อนไขและข้อกำหนดข้างต้นอาจกำหนดไว้ในข้อมูลสั่งให้ลายมือชื่อดิจิทัล (SAD) นอกจากนี้ การยืนยันตัวตนเจ้าของลายมือชื่ออาจจะเกิดขึ้นก่อนการสร้างข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) เช่น การใช้บริการยืนยันตัวตนจากบุคคลภายนอก

ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) อาจเป็นชุดข้อมูลหรือผลลัพธ์จากการเข้ารหัสลับข้อมูล (รายละเอียดตามหัวข้อ 5.3.1.2) โดยข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) จะเป็นข้อมูลที่เกี่ยวข้องกับการยืนยันตัวตนเจ้าของลายมือชื่อโดยทางตรงหรือทางอ้อม

ในกรณีที่การยืนยันตัวตนเจ้าของลายมือชื่อเกิดขึ้นก่อนการสร้างข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ข้อมูลสั่งให้ลายมือชื่อดิจิทัล (SAD) ต้องมีผลการยืนยันตัวตน (assertion) ที่ระบุตัวเจ้าของลายมือชื่อ โดยผลการยืนยันตัวตนอาจเป็นข้อมูลที่ได้รับจากส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) หรือจากผู้พิสูจน์และยืนยันตัวตน (IdP) ทั้งนี้ แหล่งที่มาของผลการยืนยันตัวตนต้องมีการตรวจสอบความถูกต้องด้วย

4.6 โพรโทคอลเพื่อสั่งให้สร้างลายมือชื่อดิจิทัล (signature activation protocol: SAP)

โพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) ต้องถูกออกแบบให้สามารถใช้งานกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลได้อย่างมั่นคงปลอดภัย เพื่อดำเนินการสร้างลายมือชื่อดิจิทัลในนามของเจ้าของลายมือชื่อด้วยโมดูลเข้ารหัสลับ (cryptographic module)

โพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) เป็นโพรโทคอลที่เจ้าของลายมือชื่อผ่านส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) และ TW4S ใช้สื่อสารระหว่างกันเพื่อสร้างข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD)

การออกแบบโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) ต้องมีการตรวจสอบอย่างน้อย ดังนี้

(1) การยืนยันตัวตนเจ้าของลายมือชื่อเมื่อมีการเรียกใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล
(2) ความถูกต้องของคำขอสร้างลายมือชื่อดิจิทัล ในข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD)
(3) ความถูกต้องและความพร้อมใช้งานของกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลที่ถูกเรียกใช้
(4) ความมั่นคงปลอดภัยของการส่งรายการข้อมูลทั้งหมดของข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD)

ในกรณีที่กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลไม่ได้ถูกใช้ลงลายมือชื่อในกระบวนการขอออกใบรับรอง โพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) ควรตรวจสอบความถูกต้องของใบรับรองที่เชื่อมโยงกับกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล

4.7 ส่วนติดต่อของเจ้าของลายมือชื่อ (signer's interaction component: SIC)

ส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) เป็นซอฟต์แวร์และ/หรือฮาร์ดแวร์ที่ถูกใช้งานภายในขอบเขตของเจ้าของลายมือชื่อ (รายละเอียดตามหัวข้อ 4.9.3) ซึ่งอยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น

การใช้งานส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) นี้มีความสำคัญในโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) และในกระบวนการสร้างลายมือชื่อดิจิทัลด้วยอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev)

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

(1) ส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) สามารถสร้างข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ได้โดยตรง หรือ
(2) ส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) สามารถใช้ยืนยันตัวตนเจ้าของลายมือชื่อ และผลการยืนยันตัวตน (assertion) ที่ระบุตัวเจ้าของลายมือชื่อจะถูกนำไปใช้สร้างข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD)

ส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) สามารถอยู่ในรูปแบบต่าง ๆ เช่น

(1) แอปพลิเคชันบนเว็บบราวเซอร์ เช่น เว็บในรูปแบบ POST และมีการรักษาความมั่นคงปลอดภัยของข้อมูลด้วย TLS (transport layer security)
(2) แอปพลิเคชันบนอุปกรณ์เคลื่อนที่ เช่น โทรศัพท์สมาร์ทโฟน หรือแท็บเล็ต
(3) ที่จัดเก็บที่ปลอดภัยของโทรศัพท์เคลื่อนที่ เช่น ชิป secure element ของโทรศัพท์เคลื่อนที่
(4) อุปกรณ์เข้ารหัสลับ (cryptographic device) ของเจ้าของลายมือชื่อ เช่น โทเคนแบบ FIDO หรือโทเคนอิเล็กทรอนิกส์ (e-Token)

ทั้งนี้ ส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) ทำให้เกิดการเชื่อมโยงระหว่างเจ้าของลายมือชื่อกับการดำเนินการสร้างลายมือชื่อดิจิทัลภายในโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP)

4.8 โมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (signature activation module: SAM)

โมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) เป็นซอฟต์แวร์ที่ใช้ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) เพื่อรับประกันด้วยความเชื่อมั่นในระดับสูงหรือที่ระดับ SCAL2 ว่าการใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลอยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น ทั้งนี้ โมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) กำหนดให้ใช้งานภายในขอบเขตที่มีการป้องกันการเปลี่ยนแปลงข้อมูล (รายละเอียดตามหัวข้อ 4.9.1)

ในกรณีที่โมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) ไม่ได้ติดตั้งและใช้งานภายในขอบเขตที่มีการป้องกันการเปลี่ยนแปลงข้อมูล เดียวกันกับขอบเขตที่มีการป้องกันการเปลี่ยนแปลงข้อมูลของอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) นั้น การสื่อสารข้อมูลระหว่างโมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) และอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) ซึ่งอยู่คนละขอบเขตที่มีการป้องกันการเปลี่ยนแปลงข้อมูลให้ดำเนินการผ่านช่องทางสื่อสารที่มีความมั่นคงปลอดภัย

4.9 ขอบเขตสภาพแวดล้อม

4.9.1 ขอบเขตที่มีการป้องกันการเปลี่ยนแปลงข้อมูล (tamper protected environment)

ขอบเขตที่มีการป้องกันการเปลี่ยนแปลงข้อมูล (tamper protected environment) ทำงานอยู่ภายในขอบเขตที่ผู้ให้บริการบริหารจัดการและดูแล (service provider protected environment) และมีการปิดกั้นไม่ให้เข้าถึงได้โดยตรงจากเครือข่ายอินเทอร์เน็ต เพื่อให้สามารถรักษาความครบถ้วนสมบูรณ์ของชุดคำสั่งที่ทำงานอยู่ภายในขอบเขตนี้

ชุดคำสั่งภายในขอบเขตนี้จะปกป้องการใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล และควบคุมการดำเนินการสร้างลายมือชื่อดิจิทัล ให้อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อ

นอกจากนี้ ขอบเขตที่มีการป้องกันการเปลี่ยนแปลงข้อมูลจะปกป้องข้อมูลเชื่อมโยงระหว่างกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลกับเจ้าของลายมือชื่อ (ข้อมูลเชื่อมโยงนี้จะถูกสร้างและตรวจสอบเมื่อจำเป็นสำหรับการสร้างลายมือชื่อดิจิทัล)

สำหรับระดับ SCAL1 แนะนำให้สร้างและใช้งานกุญแจส่วนตัวหรือกุญแจลับภายในขอบเขตที่มีการป้องกันการเปลี่ยนแปลงข้อมูล

สำหรับระดับ SCAL2 กำหนดให้สร้างและใช้งานกุญแจส่วนตัวหรือกุญแจลับภายในขอบเขตที่มีการป้องกันการเปลี่ยนแปลงข้อมูล นอกจากนี้ กำหนดให้การใช้งานซอฟต์แวร์ของโมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) อยู่ภายในขอบเขตที่มีการป้องกันการเปลี่ยนแปลงข้อมูลด้วย

4.9.2 ขอบเขตที่ผู้ให้บริการบริหารจัดการและดูแล (service provider protected environment)

ขอบเขตที่ผู้ให้บริการบริหารจัดการและดูแล (service provider protected environment) เป็นส่วนที่ป้องกันการโจมตีจากเครือข่ายอินเทอร์เน็ต และจัดการการเชื่อมต่ออินเทอร์เน็ตกับระบบภายนอกต่าง ๆ เช่น แอปพลิเคชันของผู้ใช้งาน (client application) แอปพลิเคชันสร้างลายมือชื่อดิจิทัล (SCA) ระบบของผู้ให้บริการออกใบรับรอง (certificate authority: CA) หรือระบบของผู้ให้บริการรับลงทะเบียนใบรับรอง (registration authority: RA)

ขอบเขตนี้สามารถจัดเก็บกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล และข้อมูลเชื่อมโยงระหว่างกุญแจกับเจ้าของลายมือชื่อ ในรูปแบบที่มีการปกป้องเพื่อรักษาความมั่นคงปลอดภัย

ผู้ให้บริการจะปกป้องขอบเขตนี้เพื่อให้เป็นไปตามข้อกำหนดด้านความมั่นคงปลอดภัยของข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) และโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) รวมถึงกำหนดภาระหน้าที่ให้กับผู้ให้บริการรับลงทะเบียนใบรับรอง (RA) ในการลงทะเบียนใบรับรองให้อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น

4.9.3 ขอบเขตของเจ้าของลายมือชื่อ (signer’s environment)

ขอบเขตของเจ้าของลายมือชื่อ (signer’s environment) เป็นส่วนทางฝั่งเจ้าของลายมือชื่อโดยเจ้าของลายมือชื่อมีหน้าที่รับผิดชอบในการปกป้องขอบเขตของตนเอง ทั้งนี้ หากเจ้าของลายมือชื่อใช้ขอบเขตสภาพแวดล้อมที่บริหารจัดการโดยบุคคลที่สาม บุคคลที่สามนั้นจะมีหน้าที่รับผิดชอบในการปกป้องขอบเขตของเจ้าของลายมือชื่อ

ขอบเขตของเจ้าของลายมือชื่อประกอบด้วยส่วนประกอบทั่วไปที่อาจใช้ในการเตรียมเอกสารที่จะลงลายมือชื่อ การจัดรูปแบบของเอกสารที่ลงลายมือชื่อแล้ว และการใช้งานส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) โดยเจ้าของลายมือชื่อจะใช้ส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) เพื่อสร้างการเชื่อมโยงระหว่างเจ้าของลายมือชื่อกับการดำเนินการสร้างลายมือชื่อดิจิทัลที่เปิดใช้งานผ่านโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP)

การออกแบบและพัฒนาส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) จำเป็นต้องพิจารณาข้อกำหนดเกี่ยวกับการสร้างและการส่งข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) การทำงานร่วมกันระหว่างส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) กับโมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) ผ่านโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) และรวมถึงการยืนยันตัวตนเจ้าของลายมือชื่อ

5. ข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S)

บริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote signing service) ด้วย TW4S ทำให้มีความมั่นใจได้ว่ากุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลอยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น ตามข้อกำหนดลายมือชื่ออิเล็กทรอนิกส์ของกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

ทั้งนี้ ข้อกำหนดด้านความมั่นคงปลอดภัยที่จำเป็นของ TW4S ประกอบด้วย

- ข้อกำหนดด้านความมั่นคงปลอดภัยทั่วไป (หัวข้อ 5.1)
- ข้อกำหนดด้านความมั่นคงปลอดภัยของส่วนประกอบหลักของระบบ (หัวข้อ 5.2)
- ข้อกำหนดด้านความมั่นคงปลอดภัยเพิ่มเติมสำหรับระดับ SCAL2 (หัวข้อ 5.3)
- ข้อกำหนดมาตรฐานความมั่นคงปลอดภัยสำหรับผลิตภัณฑ์ TW4S (หัวข้อ 5.4)

5.1 ข้อกำหนดด้านความมั่นคงปลอดภัยทั่วไป (general security requirements: SRG)

5.1.1 การบริหารจัดการ (management: SRG_M)

ผู้ให้บริการมีการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยที่เหมาะสมสำหรับบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote signing service) ด้วย TW4S เช่น ข้อกำหนดด้านความมั่นคงปลอดภัยทางกายภาพ ข้อกำหนดสำหรับเจ้าหน้าที่หรือบุคลากรของผู้ให้บริการ และข้อกำหนดด้านความมั่นคงปลอดภัยอื่น ๆ เพื่อให้การให้บริการลงลายมือชื่อดิจิทัลมีความน่าเชื่อถือและอ้างอิงได้ตามข้อกำหนดด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับผู้ให้บริการในระดับสากล เช่น มาตรฐาน ETSI EN 319401 [11] หรือข้อเสนอแนะหรือประกาศของหน่วยงานในระดับประเทศที่รับผิดชอบ

5.1.1.1 การบริหารจัดการระบบและความมั่นคงปลอดภัยของระบบ

(1) TW4S ต้องรองรับการแบ่งแยกบทบาทผู้ใช้งานที่มีสิทธิเข้าถึงระบบที่แตกต่างกัน

(2) TW4S ต้องรองรับการกำหนดบทบาทผู้ใช้งานที่มีสิทธิสูง (privileged role) อย่างน้อย ดังนี้

- เจ้าหน้าที่รักษาความมั่นคงปลอดภัยระบบ (security officer) ซึ่งมีหน้าที่รับผิดชอบในการบริหารจัดการมาตรการด้านความมั่นคงปลอดภัยของ TW4S ให้สอดคล้องกับแนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยที่กำหนดไว้ และสามารถเข้าถึง

ข้อมูลที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบได้

- เจ้าหน้าที่ดูแลระบบ (system administrator) ซึ่งได้รับมอบหมายให้สามารถติดตั้ง ตั้งค่า และบำรุงรักษา TW4S แต่ถูกควบคุมการเข้าถึงข้อมูลที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบ
- เจ้าหน้าที่ผู้ปฏิบัติงาน (system operator) ซึ่งมีหน้าที่ปฏิบัติงานประจำวันบน TW4S และได้รับอนุญาตให้ปฏิบัติงานสำรองหรือกู้คืนข้อมูลของระบบ
- ผู้ตรวจสอบระบบ (system auditor) ซึ่งได้รับมอบหมายให้เข้าถึงข้อมูลที่เก็บไว้เพื่อเป็นหลักฐานในระยะยาว (archive) และข้อมูลบันทึกกิจกรรมสำหรับตรวจสอบ (audit log) ของ TW4S เพื่อวัตถุประสงค์ในการตรวจสอบการปฏิบัติงานและการบริหารจัดการระบบตามแนวนโยบายการรักษาความมั่นคงปลอดภัย

ทั้งนี้ เจ้าหน้าที่รักษาความมั่นคงปลอดภัยระบบ (security officer) และเจ้าหน้าที่ดูแลระบบ (system administrator) เป็นผู้ใช้งานที่มีสิทธิสูง (privileged user) ในขณะที่เจ้าหน้าที่ผู้ปฏิบัติงาน (system operator) และผู้ตรวจสอบระบบ (auditor) เป็นผู้ใช้งานที่มีสิทธิสูงแต่ไม่สามารถบริหารจัดการหรือตั้งค่าต่าง ๆ ใน TW4S

(3) TW4S ต้องรองรับการกำหนดบทบาทผู้ใช้งานที่มีสิทธิพื้นฐาน (non-privileged role) อย่างน้อยดังนี้

- เจ้าของลายมือชื่อซึ่งได้รับอนุญาตใช้ TW4S ด้วยการส่งข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ซึ่งเป็นส่วนหนึ่งของโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) เพื่อสั่งให้ลงลายมือชื่อดิจิทัลในเอกสารหรือสร้างลายมือชื่อดิจิทัลกับแบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R)
- แอปพลิเคชันสร้างลายมือชื่อดิจิทัล (SCA) ซึ่งได้รับอนุญาตให้ส่งคำขอแบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R) กับ TW4S เพื่อลงลายมือชื่อของเจ้าของลายมือชื่อ
- ผู้ให้บริการรับลงทะเบียนใบรับรอง (RA) ซึ่งได้รับอนุญาตให้ส่งใบรับรองให้กับ TW4S ตามคำขอลงลายมือชื่อในใบรับรอง (certificate signing request: CSR)

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

(5) ผู้ใช้งานที่มีบทบาทเป็นผู้ใช้งานที่มีสิทธิสูงต้องไม่มีบทบาทเป็นผู้ใช้งานที่มีสิทธิพื้นฐาน และผู้ใช้งานที่มีบทบาทเป็นผู้ใช้งานที่มีสิทธิพื้นฐานต้องไม่มีบทบาทเป็นผู้ใช้งานที่มีสิทธิสูง

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

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

(8) บุคคลที่อยู่ในกลุ่มผู้ใช้งานที่มีสิทธิสูงต้องมีการระบุชื่อและเป็นบุคคลที่ผ่านการอบรมที่จำเป็น

(9) ผู้ใช้งานที่เข้าถึงฮาร์ดแวร์ทางกายภาพและบริหารจัดการ TW4S ต้องเป็นผู้ใช้งานที่มีสิทธิสูงของระบบเท่านั้น

(10) ผู้ใช้งานที่มีสิทธิในการบริหารจัดการทุกส่วนประกอบของ TW4S ต้องเป็นผู้ใช้งานที่มีสิทธิสูงของระบบเท่านั้น

5.1.2 ระบบและการปฏิบัติงาน (systems and operations: SRG_SO)

5.1.2.1 การบริหารงานการปฏิบัติงาน

ผู้ให้บริการที่ให้บริการ TW4S ต้องทำให้มีความมั่นใจว่าการบริหารจัดการในการปฏิบัติงานในส่วนต่าง ๆ มีความมั่นคงปลอดภัยในระดับที่เหมาะสม

(1) ผู้ผลิตหรือผู้พัฒนา TW4S ต้องจัดให้มีคู่มือการปฏิบัติงาน เพื่อแสดงให้เห็นว่าการปฏิบัติงานที่เกี่ยวข้องกับ TW4S นั้น

- เป็นการให้บริการที่ถูกต้องและมั่นคงปลอดภัย
- เป็นบริการที่ผ่านการบรรเทาหรือแก้ไขความเสี่ยงจากความขัดข้องของบริการให้ลดลงเหลือน้อยเท่าที่เป็นไปได้
- สามารถป้องกันการโจมตีจากโปรแกรมประสงค์ร้าย เพื่อทำให้มีความมั่นใจในการรักษาความครบถ้วนสมบูรณ์ของ TW4S และข้อมูลที่ผ่านการประมวลผลของระบบ

(2) ผู้ผลิตหรือผู้พัฒนา TW4S ต้องจัดให้มีคู่มือการบริหารจัดการระบบสำหรับผู้ใช้งานที่มีสิทธิสูงในทั้ง 4 บทบาทตามรายละเอียดที่ระบุไว้ในหัวข้อ 5.1.1.1(2) และควรประกอบด้วยเอกสาร ดังนี้

- คู่มือหรือข้อแนะนำการติดตั้งระบบ
- คู่มือหรือข้อแนะนำการบริหารจัดการระบบ
- คู่มือหรือข้อแนะนำสำหรับผู้ใช้งาน

5.1.2.2 การประสานเวลาให้ตรงและถูกต้อง

การสร้างลายมือชื่อดิจิทัลและการตรวจสอบลายมือชื่อดิจิทัลเป็นกระบวนการที่เกี่ยวข้องกับเวลาในขณะดำเนินการสร้างและตรวจสอบลายมือชื่อดิจิทัล ดังนั้น จึงมีความจำเป็นต้องทำให้มีความมั่นใจว่า TW4S ได้รับการประสานเวลา (time synchronization) ให้สอดคล้องกับมาตรเวลาของแหล่งเวลาอ้างอิง ข้อกำหนดนี้เป็นคนละส่วนกับข้อกำหนดเกี่ยวกับการประทับเวลาอิเล็กทรอนิกส์ที่กำหนดไว้โดยผู้ให้บริการประทับเวลา (time-stamping authority: TSA)

(1) ผู้ผลิตหรือผู้พัฒนา TW4S ต้องระบุค่าความแม่นยำของค่าเวลาของ TW4S และกลไกที่ทำให้มีความมั่นใจว่านาฬิกาของ TW4S มีค่าความแม่นยำตามที่กำหนดไว้

(2) แหล่งเวลาของ TW4S ควรมีการประสานเวลากับมาตรเวลาของแหล่งเวลาอ้างอิง เพื่อให้มีความมั่นใจว่าเวลาของบันทึกกิจกรรมสำหรับตรวจสอบมีความแม่นยำ

(3) การตรวจสอบว่าใบรับรองหมดอายุหรือไม่ แหล่งเวลาของ TW4S ต้องมีการประสานเวลากับมาตรเวลาร่วมสากล (UTC)

5.1.3 การระบุและยืนยันตัวตน (identification and authentication: SRG_IA)

TW4S ใช้กลไกการระบุและยืนยันตัวตนเพื่อป้องกันการเข้าถึงและใช้งานโดยผู้ที่ไม่ได้รับอนุญาต และเพื่อป้องกันการเข้าถึงและใช้งานในทุกส่วนประกอบสำหรับการบริหารจัดการ TW4S ทั้งนี้ กลไกการระบุและยืนยันตัวตนอาจเป็นกลไกของซอฟต์แวร์ระบบปฏิบัติการที่ TW4S ติดตั้งอยู่ หรือเป็นระบบระบุและยืนยันตัวตนที่แยกออกเป็นการเฉพาะก็ได้

5.1.3.1 การยืนยันตัวตนผู้ใช้งานที่มีสิทธิสูงและผู้ใช้งานที่มีสิทธิพื้นฐานซึ่งไม่ใช่เจ้าของลายมือชื่อ

(1) TW4S ต้องกำหนดให้ผู้ใช้งานทุกคนแสดงตัวตนและผ่านการยืนยันตัวตนจนสำเร็จก่อน จึงจะอนุญาตให้เข้าถึงและใช้งาน TW4S ตามสิทธิและบทบาทของผู้ใช้งานนั้น

(2) TW4S ต้องยืนยันตัวตนผู้ใช้งานที่ได้ยุติการใช้งานหรือลงชื่อออกจากระบบ (log out) แล้วจนสำเร็จก่อน จึงจะอนุญาตให้เข้าถึงและใช้งาน TW4S ได้อีกครั้ง

(3) คุณสมบัติของข้อมูลที่ใช้ในกลไกการยืนยันตัวตนต้องเป็นข้อมูลที่ยากต่อการคาดเดา

(4) สำหรับการใช้งานของผู้ใช้งานที่มีสิทธิสูง TW4S ต้องมีมาตรการลดความเสี่ยงจากการถูกลักลอบเข้าถึงและใช้งานในบทบาทของผู้ใช้งานที่มีสิทธิสูงผ่านอุปกรณ์ของผู้ใช้งานนั้นในขณะที่ไม่มีการใช้งาน เช่น ยุติการใช้งานระบบ (session termination) หากไม่มีการใช้งานเป็นระยะเวลา (idle period) ตามที่กำหนดไว้

5.1.3.2 การยืนยันตัวตนที่ไม่สำเร็จ

(1) TW4S ต้องระงับการยืนยันตัวตนผู้ใช้งานซึ่งได้ยืนยันตัวตนเพื่อเข้าถึงระบบไม่สำเร็จเกินจำนวนครั้งสูงสุดที่กำหนดไว้ ผู้ใช้งานนั้นจะสามารถยืนยันตัวตนได้อีกครั้งหลังพ้นกรอบเวลาการระงับการยืนยันตัวตนที่กำหนดไว้ หรือจนกว่าผู้ดูแลระบบจะยกเลิกการระงับการยืนยันตัวตนของผู้ใช้งานนั้น

5.1.4 การควบคุมและจำกัดการเข้าถึงระบบ (system access control: SRG_SA)

TW4S ใช้กลไกการควบคุมและจำกัดการเข้าถึงระบบเพื่อป้องกันการเข้าถึงและใช้งานข้อมูลและส่วนประกอบสำคัญทั้งหมดของระบบโดยผู้ที่ไม่ได้รับอนุญาต กลไกการควบคุมและจำกัดการเข้าถึงระบบนี้ใช้กับผู้ใช้งานที่มีสิทธิสูงเท่านั้น ส่วนการควบคุมและจำกัดการเข้าถึงระบบของเจ้าของลายมือชื่อให้ปฏิบัติตามรายละเอียดที่ระบุไว้ในหัวข้อ 0

การควบคุมและจำกัดการเข้าถึงระบบอาจเป็นกลไกของซอฟต์แวร์ในระบบปฏิบัติการที่ TW4S ติดตั้งอยู่ หรือเป็นส่วนควบคุมและจำกัดการเข้าถึงระบบที่แยกออกเป็นการเฉพาะก็ได้ เจ้าของหรือผู้รับผิดชอบต่อข้อมูลในระบบนั้นจะเป็นผู้กำหนดสิทธิการเข้าถึงข้อมูลหรือส่วนประกอบเฉพาะของ TW4S โดยขึ้นอยู่กับอัตลักษณ์หรือข้อมูลระบุตัวตนของบุคคลที่พยายามเข้าถึงข้อมูลหรือส่วนประกอบของระบบนั้น และ

(1) สิทธิการเข้าถึงข้อมูลหรือส่วนประกอบของระบบที่มอบให้กับบุคคลนั้น หรือ

(2) สิทธิการเข้าถึงข้อมูลหรือส่วนประกอบของระบบตามบทบาทที่บุคคลนั้นถือครอง

5.1.4.1 การบริหารสิทธิการเข้าถึงระบบ

(1) TW4S ต้องมีความสามารถในการควบคุมและจำกัดผู้ใช้งานที่ระบุไว้ในการเข้าถึงข้อมูลที่ผู้ใช้งานเป็นเจ้าของ หรือส่วนประกอบของระบบที่ผู้ใช้งานเป็นผู้รับผิดชอบ

(2) TW4S ต้องทำให้มีความมั่นใจว่าสามารถควบคุมและจำกัดการเข้าถึงข้อมูลสำคัญที่เก็บไว้ในระบบ

5.1.5 การบริหารจัดการกุญแจ (key management: SRG_KM)

TW4S สามารถใช้กุญแจเข้ารหัสลับเพื่อการรักษาความครบถ้วนสมบูรณ์ (integrity) การรักษาความลับ (confidentiality) และการยืนยันตัวตน (authentication) ภายในระบบย่อยและระหว่างระบบย่อยต่าง ๆ ของ TW4S ดังนั้น การใช้กุญแจโดยไม่ได้รับอนุญาต การเปิดเผยกุญแจโดยไม่ได้รับอนุญาต การแก้ไขกุญแจ หรือการออกกุญแจแทนที่กุญแจเดิมเหล่านี้จะส่งผลให้เกิดการสูญเสียคุณสมบัติด้านความมั่นคงปลอดภัยของ TW4S จึงมีความจำเป็นต้องจัดการกุญแจเหล่านี้ด้วยความมั่นคงปลอดภัยตลอดวงจรชีวิตของกุญแจ

เนื่องจากมีภัยคุกคามหลายรูปแบบที่ส่งผลกระทบต่อกุญแจต่าง ๆ ที่ใช้ใน TW4S จึงมีความจำเป็นต้องจัดประเภทของกุญแจต่าง ๆ ตามความเสี่ยงหรือภัยคุกคามที่ส่งผลกระทบต่อกุญแจ สำหรับข้อเสนอแนะมาตรฐานฉบับนี้ กุญแจที่ใช้ใน TW4S สามารถแบ่งเป็นประเภท ดังนี้

- กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อ (signer's signing keys) คือ กุญแจที่อยู่ภายใต้การควบคุมและใช้งานโดยเจ้าของลายมือชื่อสำหรับสร้างลายมือชื่อดิจิทัล
- กุญแจโครงสร้างพื้นฐาน (infrastructure keys) คือ กุญแจที่ใช้งานโดย TW4S สำหรับกระบวนการต่าง ๆ เช่น การแลกและตกลงกุญแจ (key agreement) การยืนยันตัวตนของระบบย่อย (subsystem authentication) การลงลายมือชื่อในบันทึกกิจกรรมสำหรับตรวจสอบ (audit log signing) และการเข้ารหัสลับข้อมูลที่นำส่งและเก็บรักษา ทั้งนี้ กุญแจต่าง ๆ ที่มีอายุใช้งานในช่วงเวลาสั้น ๆ ใน TW4S ก็ถูกจัดอยู่ในประเภทกุญแจโครงสร้างพื้นฐานนี้
- กุญแจควบคุม (control keys) คือ กุญแจที่ใช้งานโดยบุคลากรหรือเจ้าหน้าที่ที่ได้รับมอบหมายให้เป็นผู้บริหารจัดการหรือใช้งาน TW4S และบุคคลซึ่งมีโอกาสจะใช้กุญแจควบคุมนี้สำหรับการยืนยันตัวตน การลงลายมือชื่อ หรือเพื่อวัตถุประสงค์ในการรักษาความลับของข้อมูล

ในด้านความมั่นคงปลอดภัยของกุญแจ กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อจัดเป็นกุญแจที่มีความสำคัญ และควรมีมาตรการในการบริหารความเสี่ยงที่จะส่งผลกระทบต่อกุญแจอย่างเหมาะสม กุญแจโครงสร้างพื้นฐานจัดเป็นกุญแจที่มีความสำคัญเช่นเดียวกัน แต่เนื่องจากรูปแบบหรือลักษณะการใช้งานกุญแจซึ่งจำเป็นต้องถูกเผยแพร่หรือจัดเก็บอยู่ในหลายแหล่ง จึงทำให้กุญแจโครงสร้างพื้นฐานนี้มีความสำคัญต่ำกว่ากุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อ

กุญแจที่มีความสำคัญต่ำที่สุด คือกุญแจควบคุมที่ใช้งานโดยบุคลากรหรือเจ้าหน้าที่ในการควบคุมหรือบริหารจัดการ TW4S เนื่องจากเป็นกุญแจที่ใช้งานโดยบุคคลที่เชื่อถือได้และมักจะมีอายุกุญแจในช่วงเวลาสั้น ๆ นอกจากนี้ กุญแจเซสชัน (session keys) ที่ใช้อ้างอิงถึงผู้ใช้งานภายหลังการยืนยันตัวตน

ผู้ใช้งานเป็นผลสำเร็จเพื่อทำธุรกรรมครั้งเดียวหรือหลายธุรกรรมภายในกำหนดเวลาสั้น ๆ จัดเป็นกุญแจที่มีความสำคัญ แต่จะมีข้อกำหนดด้านความมั่นคงปลอดภัยต่ำกว่าข้อกำหนดของกุญแจประเภทอื่น ๆ ที่กล่าวมาก่อนหน้านี้

ทั้งนี้ กุญแจโครงสร้างพื้นฐานและกุญแจควบคุมอาจเป็นกุญแจส่วนตัวหรือกุญแจลับก็ได้

5.1.5.1 การสร้างกุญแจ

(1) กุญแจส่วนตัวหรือกุญแจลับควรถูกสร้างขึ้นและใช้งานภายในอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) ทั้งนี้ อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) ควรเป็นอุปกรณ์/ระบบที่เชื่อถือได้และผ่านการตรวจรับรองเกณฑ์ประเมินทั่วไปด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ (common criteria: CC) ตามมาตรฐาน ISO/IEC 15408 [5] [6] [7] ในระดับความเข้มงวดในการประเมินตามเกณฑ์ประเมินทั่วไปด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ (evaluation assurance level: EAL) ที่ระดับ 4 ขึ้นไป หรือมาตรฐานอื่นในระดับประเทศที่เกี่ยวข้องกับการประเมินด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศของผลิตภัณฑ์ตามข้อกำหนดในข้อเสนอแนะมาตรฐานฉบับนี้

ตัวอย่างมาตรฐานด้านความมั่นคงปลอดภัยของโมดูลเข้ารหัสลับ (cryptographic module) ที่มีการรับรองตามมาตรฐาน ISO/IEC 15408 ประกอบด้วย CEN EN 419221-5 [10] หรือ ISO/IEC 19790 [12] หรือ FIPS PUB 140-2 level 3 [13]

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

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

เมื่อมีความจำเป็นต้องรักษาความลับและความครบถ้วนสมบูรณ์ของข้อมูลสำคัญ เช่น การสำรองข้อมูลกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล อัลกอริทึมการเข้ารหัสลับและค่าพารามิเตอร์ที่เกี่ยวข้องต้องมีระดับความมั่นคงปลอดภัยที่เทียบเท่าหรือสูงกว่าข้อกำหนดนี้เท่านั้น

(3) เมื่อกุญแจส่วนตัวหรือกุญแจลับ ซึ่งครอบคลุมถึงกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อ กุญแจโครงสร้างพื้นฐาน และกุญแจควบคุม ถูกถือครองหรือจัดเก็บภายนอกอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) กุญแจเหล่านี้ต้องได้รับการปกป้องเพื่อทำให้มีความมั่นใจว่ามีการรักษาความลับและความครบถ้วนสมบูรณ์ของกุญแจ

(4) อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) ต้องถูกตั้งค่าเริ่มต้นการใช้งานด้วยกลไกทางเทคนิคในอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) โดยอาศัยผู้ปฏิบัติงานอย่างน้อยสองคนก่อนจะใช้อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) ในการสร้างหรือจัดเก็บกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล

5.1.5.2 การจัดเก็บ สำรอง และกู้คืนกุญแจ

(1) กุญแจส่วนตัวและกุญแจลับทั้งหมด ซึ่งครอบคลุมถึงกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อ กุญแจโครงสร้างพื้นฐาน และกุญแจควบคุม ต้องมีการจัดเก็บอย่างมั่นคงปลอดภัย โดยไม่เก็บรักษาไว้ในรูปแบบที่ไม่มีการปกป้อง

(2) ถ้ามีกุญแจส่วนตัวหรือกุญแจลับ ซึ่งครอบคลุมถึงกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อ กุญแจโครงสร้างพื้นฐาน และกุญแจควบคุม ถูกนำออกจากอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) กุญแจนั้นต้องได้รับการปกป้องเพื่อทำให้มีความมั่นใจว่าการรักษาความลับและความครบถ้วนสมบูรณ์ของกุญแจนั้นยังมีระดับความมั่นคงปลอดภัยเทียบเท่าหรือสูงกว่าการจัดเก็บภายในอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev)

เมื่อมีการปกป้องกุญแจส่วนตัวหรือกุญแจลับด้วยการเข้ารหัสลับ ต้องใช้อัลกอริทึมการเข้ารหัสลับและค่าพารามิเตอร์ที่มีระดับความมั่นคงปลอดภัยเทียบเท่าหรือสูงกว่าที่อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) ใช้เท่านั้น

(3) TW4S ต้องทำให้มีความมั่นใจว่าการจัดเก็บ สำรอง และกู้คืนกุญแจส่วนตัวหรือกุญแจลับ ซึ่งครอบคลุมถึงกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อ กุญแจโครงสร้างพื้นฐาน และกุญแจควบคุม ดำเนินการโดยเจ้าหน้าที่ที่ได้รับอนุญาตเท่านั้น กุญแจมาสเตอร์ (master keys) ที่ใช้ปกป้องกุญแจผู้ใช้งาน (user keys) และกุญแจที่ใช้งานในระบบ (working keys) ต้องได้รับการจัดเก็บ สำรอง และนำเข้าหรือกู้คืนภายใต้การควบคุมการปฏิบัติงานที่อาศัยสองบุคคลหรือสองกระบวนการ (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) การเข้าถึงและการใช้กุญแจต่าง ๆ ซึ่งครอบคลุมถึงกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อ กุญแจโครงสร้างพื้นฐาน และกุญแจควบคุม ต้องผ่านกลไกการควบคุมและจำกัดการเข้าถึงเพื่ออนุญาตให้เฉพาะผู้ใช้งานที่มีสิทธิเท่านั้น

(4) กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อต้องเชื่อมโยงไปยังเจ้าของลายมือชื่อเพียงผู้เดียว และเชื่อมโยงกับใบรับรองเพียงใบรับรองเดียว

5.1.5.4 การเผยแพร่กุญแจ

(1) เมื่อจำเป็นต้องมีการจัดส่งกุญแจส่วนตัวหรือกุญแจลับ ซึ่งครอบคลุมถึงกุญแจโครงสร้างพื้นฐาน

และกุญแจควบคุม ต้องจัดส่งด้วยวิธีการที่มีการรักษาความมั่นคงปลอดภัยให้กับกุญแจ

(2) กุญแจทั้งหมดที่ใช้ในการรักษาความมั่นคงปลอดภัยให้กับกุญแจส่วนตัวหรือกุญแจลับในระหว่างการจัดส่ง ต้องมีความแข็งแกร่งของกุญแจไม่ต่ำกว่าความแข็งแกร่งของกุญแจที่ถูกจัดส่ง

5.1.5.5 การต่ออายุ ปรับปรุง และเปลี่ยนกุญแจ

(1) กุญแจโครงสร้างพื้นฐานและกุญแจควบคุมควรถูกเปลี่ยนอยู่เสมอตามระยะเวลาที่เหมาะสมตามผลประเมินความเสี่ยง

(2) เมื่อพบว่าอัลกอริทึมการเข้ารหัสลับหรือความยาวของกุญแจไม่เหมาะสมหรือไม่มั่นคงปลอดภัย กุญแจต่าง ๆ ที่อาศัยอัลกอริทึมการเข้ารหัสลับนี้ต้องถูกเปลี่ยนในทันที

(3) เมื่อพบว่ากุญแจถูกละเมิดหรือสงสัยว่าจะถูกละเมิด กุญแจเหล่านี้ควรถูกเปลี่ยนในทันที

5.1.5.6 การเก็บรักษากุญแจไว้เป็นหลักฐานในระยะยาว

(1) กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลต้องไม่ถูกเก็บรักษาไว้เป็นหลักฐานในระยะยาว

5.1.5.7 การลบกุญแจ

(1) กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลต้องถูกทำลายหลังจากที่ใบรับรองที่เชื่อมโยงกับกุญแจนั้นหมดอายุการใช้งาน หรือเมื่อเจ้าของลายมือชื่อไม่ต้องการใช้งานกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลนั้นอีกต่อไป

(2) เมื่อพบว่ากุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลขาดความเชื่อมโยงกับเจ้าของลายมือชื่อภายหลังกระบวนการลงลายมือชื่อใด กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลนั้นต้องถูกทำลายเมื่อสิ้นสุดกระบวนการลงลายมือชื่อนั้น

(3) ขั้นตอนการปฏิบัติงานและกลไกการทำลายกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลควรทำให้มีความมั่นใจว่าข้อมูลสำรองทุกสำเนาของกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลได้ถูกทำลายด้วย และไม่มีข้อมูลใดที่หลงเหลืออยู่สามารถใช้สร้างกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลนั้นกลับมาได้

5.1.6 การตรวจสอบ (auditing: SRG_AA)

5.1.6.1 การจัดทำข้อมูลสำหรับตรวจสอบ (audit data)

(1) เหตุการณ์ต่อไปนี้ต้องมีการบันทึกเป็นข้อมูลสำหรับตรวจสอบ (audit data) เป็นอย่างน้อย

- เหตุการณ์สำคัญของ TW4S ที่เกี่ยวข้องกับการบริหารจัดการกุญแจ (เช่น การสร้าง การใช้งาน และการทำลาย)
- เหตุการณ์การลงลายมือชื่อของผู้ใช้งาน เช่น เหตุการณ์การสร้างลายมือชื่อด้วยกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อ และเหตุการณ์การบริหารจัดการกับคำขอในแบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R)
- การยืนยันตัวตนผู้ใช้งานที่เกิดขึ้นภายในโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP)
- การจัดการข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ของเจ้าของลายมือชื่อโดย TW4S
- การเปิดและปิดฟังก์ชันการจัดทำข้อมูลสำหรับตรวจสอบ

– การเปลี่ยนค่าพารามิเตอร์ที่เกี่ยวข้องกับการจัดทำข้อมูลสำหรับตรวจสอบ

เหตุการณ์การลงลายมือชื่อของเจ้าของลายมือชื่อต้องบันทึกข้อมูลใบรับรองที่เชื่อมโยงกับกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลนั้นด้วย

เหตุการณ์การเข้าถึงหรือพยายามเข้าถึง TW4S ควรถูกบันทึกเป็นข้อมูลสำหรับตรวจสอบ

(2) ผู้ให้บริการต้องระบุกิจกรรมที่ได้ดำเนินการไปแล้ว ในกรณีที่เกิดความผิดพลาดในการส่งข้อมูลสำหรับตรวจสอบไปยังสื่อบันทึกข้อมูลภายนอก

5.1.6.2 การรักษาความพร้อมใช้งานของข้อมูลสำหรับตรวจสอบ

(1) TW4S ต้องดูแลรักษาข้อมูลสำหรับตรวจสอบ และทำให้มีความมั่นใจว่ามีการดำเนินมาตรการดูแลรักษาข้อมูลสำหรับตรวจสอบทั้งหมดที่จัดเก็บไว้

(2) ฟังก์ชันการบันทึกข้อมูลสำหรับตรวจสอบต้องเป็นรูปแบบการบันทึกข้อมูลเพิ่มต่อท้ายจากข้อมูลเดิมเท่านั้น

(3) TW4S ต้องปกป้องรายการข้อมูลสำหรับตรวจสอบ (audit records) ที่จัดเก็บไว้จากการถูกลบโดยผู้ที่ไม่ได้รับอนุญาต

(4) รายการข้อมูลสำหรับตรวจสอบอาจถูกลบได้เมื่อมีการเก็บรักษาข้อมูลไว้เป็นหลักฐานในระยะยาวที่สื่อบันทึกข้อมูลภายนอก

5.1.6.3 พารามิเตอร์ของข้อมูลสำหรับตรวจสอบ

(1) รายการข้อมูลสำหรับตรวจสอบทั้งหมดต้องประกอบด้วยพารามิเตอร์ต่าง ๆ ดังนี้

– วันและเวลาของเหตุการณ์
– ประเภทของเหตุการณ์
– อัตลักษณ์หรือข้อมูลระบุตัวตนของผู้รับผิดชอบหรือดำเนินการที่เกี่ยวข้องกับเหตุการณ์ (เช่น ผู้ใช้งาน ผู้ดูแลระบบ และกระบวนการของระบบ)
– สถานะของเหตุการณ์ เช่น สำเร็จหรือไม่สำเร็จ

5.1.6.4 การเรียกแสดงข้อมูลสำหรับตรวจสอบ

(1) TW4S ต้องสามารถค้นหาเหตุการณ์จากข้อมูลสำหรับตรวจสอบ (audit data) ด้วยวันที่ของเหตุการณ์ที่เกิดขึ้น ด้วยประเภทของเหตุการณ์ หรือด้วยอัตลักษณ์หรือข้อมูลระบุตัวตนของผู้ใช้งาน

(2) รายการข้อมูลสำหรับตรวจสอบ (audit records) ต้องสามารถนำไปประมวลผลข้อมูลหรือแสดงในรูปแบบที่เหมาะสมสำหรับผู้ตรวจสอบระบบ (system auditor) ในการตีความข้อมูล

5.1.6.5 การจำกัดการเข้าถึงข้อมูลสำหรับตรวจสอบ

(1) TW4S ต้องปฏิเสธการเข้าถึงเพื่ออ่านข้อมูลสำหรับตรวจสอบจากผู้ใช้งานทั้งหมด ยกเว้นสำหรับผู้ใช้งานที่ได้รับสิทธิการเข้าถึงเพื่ออ่านอย่างชัดเจน เช่น ผู้ใช้งานในบทบาทผู้ตรวจสอบระบบ (system auditor)

5.1.6.6 การสร้างข้อความแจ้งเตือน

(1) TW4S ต้องสร้างข้อความแจ้งเตือนเหตุการณ์ความผิดปกติซึ่งอาจส่งผลกระทบต่อความสามารถด้านความมั่นคงปลอดภัยของระบบ ภายในเวลาที่เหมาะสม

TW4S ควรมีกลไกการแจ้งเตือนต่อเจ้าหน้าที่ดูและระบบที่เกี่ยวข้องเมื่อตรวจพบเหตุการณ์ความผิดปกติ ทั้งนี้ กลไกการแจ้งเตือนอาจเป็นเครื่องมือสั่งการให้ดำเนินการเพื่อตอบสนองต่อเหตุการณ์ที่อาจเป็นการโจมตีต่อระบบ เช่น การสั่งให้ตัดเส้นทางการเชื่อมต่อของการโจมตีที่อาจเกิดขึ้น

ตัวอย่างของเหตุการณ์ความผิดปกติที่เกี่ยวข้องกับกิจกรรมของผู้ใช้งาน เช่น การใช้งานของผู้ใช้งานนอกเวลาใช้งานปกติ การสั่งงานของผู้ใช้งานจำนวนมากจนผิดปกติ (ตรวจจับการสั่งงานจากโปรแกรมหรือซอฟต์แวร์) หรือการมีเซสชันใช้งานของผู้ใช้งานมากกว่าหนึ่งเซสชัน

5.1.6.7 การรักษาความครบถ้วนสมบูรณ์ของข้อมูลสำหรับตรวจสอบ

(1) TW4S ต้องทำให้มีความมั่นใจว่าสามารถรักษาความครบถ้วนสมบูรณ์ของข้อมูลสำหรับตรวจสอบ

(2) TW4S ต้องมีฟังก์ชันสำหรับการตรวจสอบความครบถ้วนสมบูรณ์ของข้อมูลสำหรับตรวจสอบ

5.1.6.8 ความแม่นยำของเวลาของข้อมูลสำหรับตรวจสอบ

(1) เพื่อทำให้มีความมั่นใจว่าข้อมูลเวลาของเหตุการณ์ในข้อมูลสำหรับตรวจสอบมีความแม่นยำของเวลา ให้ปฏิบัติตามข้อกำหนดที่ระบุไว้ในหัวข้อ 5.1.2.2(2)

5.1.7 การเก็บรักษาข้อมูลไว้เป็นหลักฐานในระยะยาว (archiving: SRG_AR)

5.1.7.1 การสร้างข้อมูลไว้เป็นหลักฐานในระยะยาว

(1) ผู้ให้บริการต้องสามารถเก็บรักษาข้อมูลไว้เป็นหลักฐานในระยะยาวบนสื่อบันทึกข้อมูลภายนอก สื่อบันทึกข้อมูลนี้ควรมีการจัดเก็บอย่างเหมาะสมให้สามารถนำมาใช้ได้ในภายหลัง และสามารถใช้แสดงหลักฐานทางกฎหมายที่จำเป็นเพื่อสนับสนุนลายมือชื่อดิจิทัลที่สร้างขึ้นใน TW4S

(2) บันทึกกิจกรรมสำหรับตรวจสอบ (audit log) ทั้งหมดต้องมีการเก็บรักษาไว้เป็นหลักฐานในระยะยาว

(3) ข้อมูลที่เก็บรักษาไว้เป็นหลักฐานในระยะยาวแต่ละรายการต้องประกอบด้วยเวลาที่ทำการสร้างข้อมูลที่เก็บรักษาไว้เป็นหลักฐานในระยะยาว

(4) ข้อมูลที่เก็บรักษาไว้เป็นหลักฐานในระยะยาวต้องไม่จัดเก็บพารามิเตอร์ที่สำคัญต่อความมั่นคงปลอดภัย เช่น รหัสผ่านของผู้ใช้งานใน TW4S

5.1.7.2 การรักษาความครบถ้วนสมบูรณ์ของข้อมูลที่เก็บรักษาไว้เป็นหลักฐานในระยะยาว

(1) ข้อมูลที่เก็บรักษาไว้เป็นหลักฐานในระยะยาวต้องมีการป้องกันการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต และต้องจัดให้มีกลไกการตรวจสอบความครบถ้วนสมบูรณ์เพื่อตรวจหาการเปลี่ยนแปลงที่ไม่ได้รับอนุญาตใด ๆ ที่เกิดแก่ข้อมูลที่เก็บรักษาไว้เป็นหลักฐานในระยะยาวนับแต่เวลาที่ได้สร้างขึ้น

5.1.8 การสำรองและกู้คืนข้อมูล (backup and recovery: SRG_BK)

ข้อกำหนดนี้จะครอบคลุมเฉพาะข้อมูลระบบ ข้อมูลผู้ใช้งาน และข้อมูลอื่น ๆ ทั้งหมดที่จำเป็นต่อการกู้คืนระบบหลังจากระบบล้มเหลวหรือเกิดเหตุภัยพิบัติต่อระบบ แต่ไม่ครอบคลุมถึงการสำรองและกู้คืนกุญแจต่าง ๆ ซึ่งมีข้อกำหนดที่ระบุไว้ในหัวข้อ 5.1.5.2

5.1.8.1 การรักษาความลับและความครบถ้วนสมบูรณ์ของข้อมูลสำรอง

(1) ข้อมูลสำรองต้องได้รับการปกป้องไม่ให้มีการแก้ไขเปลี่ยนแปลง โดยมีกลไกการตรวจสอบความครบถ้วนสมบูรณ์ของข้อมูลสำรอง

(2) พารามิเตอร์ที่สำคัญต่อความมั่นคงปลอดภัยและข้อมูลลับต้องมีการจัดเก็บไว้ในรูปแบบที่มีการปกป้องเพื่อรักษาความลับและความครบถ้วนสมบูรณ์ของข้อมูล

5.1.8.2 การกู้คืนข้อมูล

(1) TW4S ต้องมีฟังก์ชันสำหรับการกู้คืนข้อมูลระบบจากข้อมูลสำรอง

(2) ผู้ใช้งานที่เชื่อมโยงกับบทบาทผู้ใช้งานที่มีสิทธิสูงเพียงพอต้องสามารถสั่งการฟังก์ชันสำหรับการกู้คืนข้อมูลจากข้อมูลสำรองได้ตามที่ต้องการ

5.2 ข้อกำหนดด้านความมั่นคงปลอดภัยของส่วนประกอบหลักของระบบ (core component security requirements: SRC)

5.2.1 การตั้งค่ากุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key setup: SRC_SKS)

(1) ค่าพารามิเตอร์ของอัลกอริทึมที่ใช้สำหรับการสร้างลายมือชื่อด้วย TW4S ต้องถูกกำหนดให้มีความมั่นคงปลอดภัยเพียงพอในตลอดช่วงอายุของใบรับรองของเจ้าของลายมือชื่อ

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

(2) TW4S ต้องเชื่อมโยงกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อกับใบรับรองของเจ้าของลายมือชื่อนั้น

(3) กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่ออาจถูกสร้างขึ้นไว้ล่วงหน้าก่อนจะมีการเชื่อมโยงกับใบรับรองก็ได้

(4) กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลไม่ควรถูกนำไปใช้งานก่อนจะมีการเชื่อมโยงกุญแจนั้นกับใบรับรองด้วย TW4S

หมายเหตุ: ข้อกำหนดนี้ไม่ครอบคลุมถึงการใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลในการลงลายมือชื่อเพื่อเป็นหลักฐานแสดงการครอบครองกุญแจในกระบวนการขอใบรับรอง

(5) TW4S ต้องรักษาความครบถ้วนสมบูรณ์ของข้อมูลการเชื่อมโยงกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อกับใบรับรอง

5.2.2 การยืนยันตัวตนเจ้าของลายมือชื่อ (signer authentication: SRC_SA)

5.2.2.1 การยืนยันตัวตนเจ้าของลายมือชื่อสำหรับระดับ SCAL1

(1) การพิสูจน์ตัวตนเจ้าของลายมือชื่อต้องมีความเข้มงวดที่ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน IAL1 ขึ้นไป และการยืนยันตัวตนเจ้าของลายมือชื่อต้องมีความเข้มงวดที่ระดับความน่าเชื่อถือของการยืนยันตัวตน AAL1 ขึ้นไป

(2) แอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) ต้องกำหนดให้เจ้าของลายมือชื่อพิสูจน์และยืนยันตัวตนจนสำเร็จแล้ว จึงจะอนุญาตให้ใช้งานกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลซึ่งอยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น

(3) โพรโทคอลที่ใช้ในการยืนยันตัวตนต้องสามารถปกป้องการโจมตีโดยคนกลาง (man-in-the-middle attack) การโจมตีแบบส่งข้อมูลซ้ำ (reply attack) และการโจมตีรูปแบบอื่น ๆ ที่ผู้ไม่ประสงค์ดีสามารถใช้สิ่งที่ใช้ยืนยันตัวตนของผู้อื่นมายืนยันตัวตนเข้าระบบได้

(4) มาตรการควบคุมการเข้าถึงระบบต้องทำให้มีความมั่นใจว่าเจ้าของลายมือชื่อไม่สามารถเข้าถึงข้อมูลหรือฟังก์ชันสำคัญของ TW4S เพื่อควบคุมกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของบุคคลอื่น

(5) TW4S ต้องทำให้มีความมั่นใจว่าแบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R) ที่ได้รับมาซึ่งอยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อนั้น ถูกลงลายมือชื่อด้วยกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อเท่านั้น

5.2.2.2 การจัดการเมื่อมีการยืนยันตัวตนไม่สำเร็จ

(1) TW4S ต้องสามารถตรวจพบเหตุการณ์การยืนยันตัวตนไม่สำเร็จต่อเนื่องของเจ้าของลายมือชื่อแต่ละรายที่เกิดขึ้นเกินจำนวนครั้งที่กำหนดไว้ได้

(2) เมื่อเกิดเหตุการณ์การยืนยันตัวตนไม่สำเร็จต่อเนื่องของเจ้าของลายมือชื่อแต่ละรายที่เกิดขึ้นเกินจำนวนครั้งที่กำหนดไว้แล้ว TW4S ต้องระงับการเข้าถึงระบบของผู้ใช้งานนั้นเป็นระยะเวลาที่เหมาะสม หรือจนกว่าผู้ดูแลระบบจะยกเลิกการระงับการเข้าถึงระบบของผู้ใช้งานนั้น

5.2.2.3 การพิสูจน์และยืนยันตัวตนจากบุคคลภายนอก

(1) ในกรณีที่มีการใช้บริการพิสูจน์และยืนยันตัวตนจากบุคคลภายนอก ผู้ให้บริการต้องทำให้มีความมั่นใจว่าบุคคลภายนอกนั้นมีคุณสมบัติตามรายละเอียดที่ระบุไว้ในหัวข้อ 5.2.2.1 และ 5.2.2.2

5.2.3 การสร้างลายมือชื่อดิจิทัล (digital signature creation: SRC_DSC)

(1) ค่าพารามิเตอร์ของอัลกอริทึมที่ใช้สำหรับการสร้างลายมือชื่อด้วย TW4S ต้องถูกกำหนดให้มีความมั่นคงปลอดภัยเพียงพอในตลอดช่วงอายุของใบรับรอง

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

5.3 ข้อกำหนดด้านความมั่นคงปลอดภัยเพิ่มเติมสำหรับระดับ SCAL2 (additional security requirements: SRA)

ข้อกำหนดด้านความมั่นคงปลอดภัยในหัวข้อนี้ใช้สำหรับ TW4S ที่ระดับ SCAL2 เท่านั้น โดยโมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) จะทำหน้าที่ยืนยันตัวตนเจ้าของลายมือชื่อทางตรงหรือทางอ้อม และข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) จะถูกเก็บรวบรวมภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่นด้วยความเชื่อมั่นในระดับสูง เพื่อทำให้มีความมั่นใจว่ากุญแจที่ระบุไว้ในข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ถูกใช้กับแบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R) โดยเจ้าของลายมือชื่อที่ผ่านการยืนยันตัวตนจนสำเร็จ

5.3.1 โพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัลและข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (signature activation protocol and signature activation data: SRA_SAP)

5.3.1.1 การต้านทานต่อภัยคุกคาม

(1) การพิสูจน์ตัวตนเจ้าของลายมือชื่อต้องมีความเข้มงวดที่ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน IAL2 ขึ้นไป และการยืนยันตัวตนเจ้าของลายมือชื่อต้องมีความเข้มงวดที่ระดับความน่าเชื่อถือของการยืนยันตัวตน AAL2 ขึ้นไป

(2) โพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) ต้องมีมาตรการควบคุมตามที่จำเป็นตามระดับความเสี่ยง เพื่อรับมือกับภัยคุกคามต่อไปนี้ที่จะส่งผลต่อการใช้ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD)

- การคาดเดาแบบออนไลน์และออฟไลน์ (online and offline guessing)
- การทำซ้ำข้อมูลยืนยันตัวตน (credential duplication)
- การโจมตีแบบฟิชชิ่ง (phishing attack)
- การดักรับข้อมูล (eavesdropping)
- การโจมตีแบบส่งข้อมูลซ้ำ (replay attack)
- การโจรกรรมเซสชัน (session hijacking)
- การโจมตีโดยคนกลาง (man-in-the-middle attack)
- การโจรกรรมข้อมูลยืนยันตัวตน (credential theft)
- การปลอมแปลง (spoofing)
- การปลอมตัว (masquerading)

(3) โพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) ต้องใช้กลไกการเข้ารหัสลับเพื่อปกป้องสิ่งที่ใช้ยืนยันตัวตนจากภัยคุกคามต่อโพรโทคอลและการโจมตีด้วยการปลอมตัวเป็นบุคคลที่สามที่เชื่อถือได้

(4) โพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) ต้องถูกปกป้องจากการโจมตีด้วยการส่งข้อมูลซ้ำ (replay) การข้ามขั้นตอน (bypass) และการปลอมข้อมูล (forgery) ที่เกิดขึ้นระหว่างเจ้าของลายมือชื่อกับอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote SCDev) เช่น ปกป้องด้วยการใช้ค่า nonce การประทับเวลา (time-stamping) หรือโทเคนเซสชัน (session token)

(5) โมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) ต้องติดตั้งและใช้งานภายในขอบเขตที่มีการป้องกันการเปลี่ยนแปลงข้อมูล ซึ่งเป็นอุปกรณ์/ระบบที่เชื่อถือได้และผ่านการตรวจรับรองเกณฑ์ประเมินทั่วไปด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ (CC) ตามมาตรฐาน ISO/IEC 15408 [5] [6] [7] ในระดับความเข้มงวดในการประเมินตามเกณฑ์ประเมินทั่วไปด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ (EAL) ที่ระดับ 4 ขึ้นไป หรือมาตรฐานอื่นในระดับประเทศที่เกี่ยวข้องกับการประเมินด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศของผลิตภัณฑ์ตามข้อกำหนดในข้อเสนอแนะมาตรฐานฉบับนี้

ตัวอย่างมาตรฐานด้านความมั่นคงปลอดภัยของโมดูลเข้ารหัสลับ (cryptographic module) ที่มีการรับรองตามมาตรฐาน ISO/IEC 15408 ประกอบด้วย CEN EN 419221-5 [10] หรือ ISO/IEC 19790 [12] หรือ FIPS PUB 140-2 level 3 [13]

(6) โพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) ต้องถูกออกแบบให้ปกป้องการทำซ้ำ (duplication) หรือการเปลี่ยนแปลง (tampering) ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) จากผู้โจมตีที่มีศักยภาพในการโจมตีสูง

(7) โพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) ต้องถูกออกแบบให้เจ้าของลายมือชื่อสามารถปกป้องการเรียกใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key activation) ด้วยข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) จากผู้โจมตีที่มีศักยภาพในการโจมตีสูง

5.3.1.2 การจัดการข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล

(1) ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) อาจเป็นชุดข้อมูลหรือผลลัพธ์จากการเข้ารหัสลับข้อมูลโดยใช้พารามิเตอร์ที่จำเป็น (mandatory parameters) ตามรายการในข้อกำหนดถัดไป

(2) ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) อาจถูกรวบรวมหรือสร้างขึ้นภายในขอบเขตของเจ้าของลายมือชื่อ (signer's environment) ด้วยส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) หรือด้วยการสั่งการจากระยะไกลกับส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) ที่อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อ

(3) ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ต้องเชื่อมโยงด้วยความเชื่อมั่นในระดับสูงกับพารามิเตอร์ต่อไปนี้เป็นอย่างน้อย

- แบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R) หรือชุดของแบบแสดงข้อมูลเพื่อลงลายมือชื่อ
- ข้อมูลที่ใช้ระบุเจ้าของลายมือชื่อที่ผ่านการยืนยันตัวตน
- กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลที่ตั้งไว้เป็นค่าเริ่มต้นหรือที่ระบุไว้

ในกรณีที่รองรับ TW4S ต้องสามารถปิดการใช้งานแบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R) ที่มีจำนวนมากกว่าหนึ่งแบบข้อมูลได้ หากกฎหมายไม่อนุญาตให้สามารถทำได้

(4) ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ต้องถูกใช้ในการเรียกใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล ก็ต่อเมื่อการยืนยันตัวตนเจ้าของลายมือชื่อสำเร็จ

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

(6) ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ต้อง

- ถูกรวบรวมภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่นด้วยความเชื่อมั่นในระดับสูง
- ถูกปกป้องเพื่อให้กุญแจต่าง ๆ ที่จัดเก็บไว้ภายในอุปกรณ์/ระบบมีความมั่นคงปลอดภัย
- ปกป้องข้อมูลลับต่าง ๆ ทั้งแบบใช้ครั้งเดียวหรือแบบใช้ระยะยาว ตามรายละเอียดที่ระบุไว้ในหัวข้อ 5.3.1.1(4)

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

(8) ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ต้องถูกตรวจสอบให้เห็นว่ากิจกรรมที่เกี่ยวกับการโจมตีระบบ เช่น การคาดเดา (guessing) การดักรับข้อมูล (eavesdropping) การส่งข้อมูลซ้ำ (replay) การจัดการการสื่อสาร (manipulation of communication) จากผู้โจมตีที่มีศักยภาพในการโจมตีสูง แทบจะไม่มีโอกาสทำลายการยืนยันตัวตนเพื่อดำเนินการสร้างลายมือชื่อดิจิทัล

5.3.2 การบริหารจัดการกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key management: SRA_SKM)

5.3.2.1 การสร้างกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล

(1) กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อต้องถูกสร้างขึ้นและใช้งานภายในอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) ซึ่งเป็นอุปกรณ์/ระบบที่เชื่อถือได้และผ่านการตรวจรับรองเกณฑ์ประเมินทั่วไปด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ (CC) ตามมาตรฐาน ISO/IEC 15408 [5] [6] [7] ในระดับความเข้มงวดในการประเมินตามเกณฑ์ประเมินทั่วไปด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ (EAL) ที่ระดับ 4 ขึ้นไป หรือมาตรฐานอื่นในระดับประเทศที่เกี่ยวข้องกับการประเมินด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศของผลิตภัณฑ์ตามข้อกำหนดในข้อเสนอแนะมาตรฐานฉบับนี้

ตัวอย่างมาตรฐานด้านความมั่นคงปลอดภัยของโมดูลเข้ารหัสลับ (cryptographic module) ที่มีการรับรองตามมาตรฐาน ISO/IEC 15408 ประกอบด้วย CEN EN 419221-5 [10] หรือ ISO/IEC 19790 [12] หรือ FIPS PUB 140-2 level 3 [13]

(2) อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) ต้องใช้เฉพาะเพื่อสนับสนุนฟังก์ชันการเข้ารหัสลับของบริการสร้างลายมือชื่อดิจิทัล เช่น การสร้างหมายเลขสุ่ม (random number generation) และอาจรวมถึงการเข้ารหัสลับ (encryption) ของการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ

(3) เมื่ออุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) ที่ใช้สร้างกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล แตกต่างจากอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) ที่ใช้สร้างลายมือชื่อดิจิทัล การจัดส่งกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลต้องปฏิบัติตามข้อกำหนดที่ระบุไว้ในหัวข้อ 5.1.5.4(1)

(4) อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) อาจจัดเก็บกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลหลายกุญแจ สำหรับเจ้าของลายมือชื่อคนเดียวกันและสำหรับเจ้าของลายมือชื่อดิจิทัลที่แตกต่าง

กันได้ ทั้งนี้ ในกรณีที่มีการจัดเก็บกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลหลายกุญแจ สำหรับเจ้าของลายมือชื่อคนเดียวกันหรือสำหรับเจ้าของลายมือชื่อดิจิทัลที่แตกต่างกันอยู่ภายในอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) นั้น TW4S ต้องทำให้มีความมั่นใจว่าสามารถแบ่งแยกการควบคุมของเจ้าของลายมือชื่อเพื่อเข้าถึงและใช้กุญแจต่าง ๆ ออกจากกันได้

(5) กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อต้องเชื่อมโยงด้วยความเชื่อมั่นในระดับสูงกับเจ้าของลายมือชื่อนั้นด้วยวิธีการของโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP)

(6) กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อต้องไม่ถูกนำไปใช้งานก่อนจะมีการเชื่อมโยงกุญแจนั้นกับเจ้าของลายมือชื่อด้วย TW4S

(7) TW4S อาจรองรับโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) และข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ที่แตกต่างกันได้หลายกลไกเพื่อเรียกใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล อย่างไรก็ตาม กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลหนึ่ง ๆ ต้องเชื่อมโยงกับโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) และข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ของกลไกใดกลไกหนึ่งเท่านั้น

5.3.2.2 การเรียกใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล

(1) TW4S ต้องกำหนดให้เจ้าของลายมือชื่อแสดงข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) กับโมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) เพื่อยืนยันตัวตนและเรียกใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล

(2) โพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) ต้องจัดส่งข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ไปยังโมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) ในลักษณะที่สามารถรับประกันความเชื่อมั่นในระดับสูงได้ว่ากุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลอยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น

(3) กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลต้องถูกเรียกใช้เพื่อใช้งานในอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote SCDev) เท่านั้น

(4) กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลต้องถูกเรียกใช้โดยข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ที่สร้างขึ้นด้วยสิ่งที่ใช้ยืนยันตัวตนของเจ้าของลายมือชื่อกับข้อมูลที่ใช้ระบุถึงกุญแจนั้น

(5) กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลที่เรียกใช้ต้องถูกใช้เพื่อสร้างลายมือชื่อดิจิทัลกับแบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R) ที่ได้รับอนุญาตจากโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) เท่านั้น

(6) ในกรณีที่แบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R) สำหรับข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ได้รับมาจากแอปพลิเคชันสร้างลายมือชื่อดิจิทัล (SCA) TW4S ต้องยืนยันแหล่งที่มาของข้อมูล (source authentication) ว่าถูกต้องและแท้จริง

(7) ผู้ใช้งานที่มีสิทธิสูงต้องไม่สามารถเข้าถึงและใช้งานกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลที่จัดสรรให้กับเจ้าของลายมือชื่อได้

(8) หลังจากการเรียกใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลและการสร้างลายมือชื่อดิจิทัลแล้ว TW4S ต้องไม่จัดเก็บข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ของเจ้าของลายมือชื่อไว้ในรูปแบบที่ไม่มีการปกป้องเพื่อรักษาความมั่นคงปลอดภัยให้กับข้อมูล

5.4 ข้อกำหนดมาตรฐานความมั่นคงปลอดภัยสำหรับผลิตภัณฑ์ TW4S

เพื่อให้ TW4S มีความน่าเชื่อถือ ผู้ให้บริการต้องใช้ผลิตภัณฑ์ TW4S ที่ผ่านการตรวจรับรองเกณฑ์ประเมินทั่วไปด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ (common criteria: CC) ตามมาตรฐาน ISO/IEC 15408 [5] [6] [7] ด้วยข้อกำหนดป้องกันการดัดแปลงแก้ไข (protection profile) ในระดับความเข้มงวดในการประเมินตามเกณฑ์ประเมินทั่วไปด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ (EAL) ที่ระดับ 4 ขึ้นไป

ข้อกำหนดการป้องกันการดัดแปลงแก้ไข (protection profile) สำหรับ TW4S เพื่อใช้เป็นเกณฑ์ประเมินด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศของผลิตภัณฑ์ให้เป็นไปตามมาตรฐาน CEN EN 419241-2 [15] หรือข้อเสนอแนะหรือประกาศของหน่วยงานในระดับประเทศที่รับผิดชอบ

บรรณานุกรม

[1] European Telecommunications Standards Institute, "CEN EN 419241-1 - Trustworthy Systems Supporting Server Signing, Part 1 – General System Security Requirements", July 2018.

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

[3] พระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต พ.ศ. 2565.

[4] พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม.

[5] International Organization for Standardization, “ISO/IEC 15408-1:2022 - Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model”, August 2022.

[6] International Organization for Standardization, “ISO/IEC 15408-2:2022 - Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements”, August 2022.

[7] International Organization for Standardization, “ISO/IEC 15408-3:2022 - Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements”, August 2022.

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

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

[10] European Telecommunications Standards Institute, "CEN EN 419221-5 - Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services", May 2018.

[11] European Telecommunications Standards Institute, "ETSI EN 319401 V.2.3.1 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers", May 2021.

[12] International Organization for Standardization, “ISO/IEC 19790:2012 - Information technology – Security techniques – Security requirements for cryptographic modules”, August 2012.

[13] National Institute of Standards and Technology Federal Information Processing Standards Publication 140-2, "Security Requirements for Cryptographic Modules", May 2001.

[14] European Telecommunications Standards Institute, "ETSI TS 119312 V1.4.2 - Electronic Signatures and Infrastructures (ESI); Cryptographic Suites", February 2022.

[15] European Telecommunications Standards Institute, "CEN EN 419241-2 - Trustworthy Systems Supporting Server Signing; Part 2 - Protection profile for QSCD for Server Signing", March 2019.

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

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

[18] 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 repealing Directive 1999/93/EC.

[19] European Telecommunications Standards Institute, "ETSI TS 119432 V.1.1.1 - Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation", March 2019.

[20] Cloud Signature Consortium, "Cloud Signature Consortium Standard V 1.0.4.0 - Architectures and protocols for remote signature applications", June 2019.

[21] OASIS Open, "OASIS Standard: Advanced Electronic Signature Profiles of the OASIS Digital Signature Service Version 2.0", May 2018.

[22] OASIS Open, "OASIS Standard: Digital Signature Service Core Protocols, Elements, and Bindings Version 2.0", April 2019.

[23] European Telecommunications Standards Institute, "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", April 2020.

[24] European Telecommunications Standards Institute, "ETSI EN 319411-1 V1.3.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements " , May 2021.

[25] European Telecommunications Standards Institute, "ETSI TS 119431-1 V1.2.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev", May 2021.