เวอร์ชัน 1.0

รายงานทางเทคนิค

Technical Report

กรอบการสร้างความน่าเชื่อถือของเอกสารรับรองและเอกสารสำแดง

Trust Model Framework for Verifiable Credential (VC) and Verifiable Presentation (VP)

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ETDA
ธันวาคม 2568

รายงานทางเทคนิค

Technical Report

กรอบการสร้างความน่าเชื่อถือของเอกสารรับรองและเอกสารสำแดง

Trust Model Framework for Verifiable Credential (VC) and Verifiable Presentation (VP)

เวอร์ชัน 1.0

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ธันวาคม 2568

ตารางบันทึกประวัติการแก้ไข/ทบทวนเอกสาร

แก้ไขครั้งที่	วันที่	เวอร์ชันที่นำมาแก้ไข	รายละเอียดการแก้ไข/ทบทวนเอกสาร	เวอร์ชันหลังแก้ไข
-	1 ธ.ค. 68	-	- ต้นฉบับ	1.0

คำนำ

ในช่วงปีที่ผ่านมา สำนักงานพัฒนาธุรรมทางอิเล็กทรอนิกส์ (สพธอ.) ให้ความสำคัญกับการพัฒนาระบบกระเป๋าดิจิทัลสำหรับเอกสารรับรอง (Digital Wallet) และการใช้งานเอกสารรับรอง (Verifiable Credential: VC) และเอกสารสำแดง (Verifiable Presentation: VP) บนหลักการ Self-Sovereign Identity (SSI) โดยมีเป้าหมายเพื่อรองรับการใช้งานเอกสารดิจิทัลที่สามารถพิสูจน์และตรวจสอบความถูกต้องได้อย่างมีประสิทธิภาพภายใต้บริบทของความเป็นส่วนตัว ความมั่นคงปลอดภัย และความสามารถในการเชื่อมโยงข้ามระบบ (Interoperability)

เพื่อให้การนำระบบเอกสารรับรองไปใช้งานได้อย่างแพร่หลายและยั่งยืน สพธอ. จึงได้ออกแบบกรอบการทำงานเพื่อแลกเปลี่ยนเอกสารรับรองและเอกสารสำแดงที่เชื่อถือได้ (VC/VP Interoperability Framework) รวมถึงแต่งตั้งคณะทำงานร่วมกับหน่วยงานทั้งภาครัฐและภาคเอกชนเพื่อ พัฒนา ทดสอบ และเชื่อมโยงระบบเอกสารรับรองและเอกสารสำแดงต้นแบบให้สามารถใช้งานได้จริงในหลายบริบท

อย่างไรก็ตาม ความท้าทายสำคัญในการประยุกต์ใช้งานกับระบบเอกสารรับรอง (VC) คือ การสร้างความน่าเชื่อถือในระดับของระบบนิเวศของเอกสารรับรองและเอกสารสำแดงในภาพรวม โดยเฉพาะในกระบวนการรับรองและตรวจสอบผู้ออกเอกสารรับรองที่น่าเชื่อถือ (trust issuer) การออกเอกสารรับรอง การใช้งานเอกสารสำแดง และการตรวจสอบเอกสารว่ามาจากผู้ออกเอกสารรับรองที่น่าเชื่อถือซึ่งจำเป็นต้องมีกลไกทางเทคนิค และกรอบธรรมาภิบาลที่บูรณาการกันอย่างเป็นระบบ

สารบัญ

สารบัญรูป

หน้า

สารบัญตาราง

หน้า

กรอบการสร้างความน่าเชื่อถือของเอกสารรับรองและเอกสารสำแดง

TRUST MODEL FRAMEWORK FOR VERIFIABLE CREDENTIAL (VC) AND VERIFIABLE PRESENTATION (VP)

1. ขอบข่าย

รายงานฉบับนี้ อธิบายการพัฒนากรอบแนวทางการสร้างระบบนิเวศสำหรับเอกสารรับรองและเอกสารสำแดงที่เชื่อถือได้ (Trust Model Framework) โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ได้ทำการศึกษาและวิเคราะห์กรอบความน่าเชื่อถือ ที่เกี่ยวข้องกับการทำงานของการประยุกต์ใช้งานเอกสารรับรองและเอกสารสำแดงจากองค์กรสากลหรือแหล่งข้อมูลที่ได้รับการยอมรับ เช่น รายงานเทคนิคกรอบการทำงานร่วมกันของกระเป๋าดิจิทัลสำหรับเอกสารรับรอง (interoperable framework for digital wallets for verifiable credentials) โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ [8] และเอกสารอื่น ๆ ที่เกี่ยวข้อง

กรอบแนวทางการสร้างระบบนิเวศสำหรับเอกสารรับรองและเอกสารสำแดงที่เชื่อถือได้ (Trust Model Framework) สำหรับระบบนิเวศของเอกสารรับรอง (VC ecosystem) ฉบับนี้ประกอบด้วยข้อกำหนดด้านเทคนิค ธรรมาภิบาล กระบวนการรับรอง และการตรวจสอบความน่าเชื่อถือของผู้เกี่ยวข้อง อันได้แก่ ผู้ออกเอกสารรับรอง (issuer) ผู้ถือเอกสารรับรอง (holder) ผู้ตรวจสอบเอกสารสำแดง (verifier) ระบบทะเบียนเอกสารรับรอง (verifiable data registry: VDR) และหน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VC Governance Authority หรือ VCGA) เพื่อให้การประยุกต์ใช้เอกสารรับรองและเอกสารสำแดงมีความมั่นคงปลอดภัย มีการกำกับดูแลที่ชัดเจน และสามารถนำไปประยุกต์ใช้งานได้ในบริบทสากล

รายงานฉบับนี้มุ่งเน้นให้เกิดความเชื่อมโยงระหว่างภาคนโยบาย ภาคเทคนิค และภาคปฏิบัติการอย่างเป็นรูปธรรม โดยจะเป็นรากฐานสำหรับการกำกับ ส่งเสริม และผลักดันการนำเอกสารรับรองและเอกสารสำแดงมาใช้ในประเทศไทยอย่างมั่นคงและยั่งยืน

2. บทนิยามและอักษรย่อ

การกำหนดคำนิยามและอักษรย่อของคำเฉพาะทางเทคนิค และใช้อ้างอิงในกรอบแนวทางการสร้างระบบนิเวศสำหรับเอกสารรับรองและเอกสารสำแดงที่เชื่อถือได้ (Trust Model Framework) ให้สอดคล้องในรายงานฉบับนี้ จะสามารถสื่อสารคำแนะนำและข้อกำหนดต่าง ๆ ให้ผู้อ่านและผู้นำกรอบแนวทางการสร้างระบบนิเวศสำหรับเอกสารรับรองและเอกสารสำแดงที่เชื่อถือได้ (Trust Model Framework) ไปประยุกต์ใช้ได้อย่างถูกต้องและมีความเข้าใจที่ตรงกัน ได้รวบรวมและกำหนดคำนิยาม และอักษรย่อจากเอกสารอ้างอิงประกอบด้วย

2.1 บทนิยาม

คำนิยามในภาษาไทย เป็นการเสนอความเห็นถึงคำอธิบายของคำศัพท์เฉพาะตามบริบทคำอธิบายจากภาษาอังกฤษ แต่ไม่ใช่เป็นการแปลคำศัพท์คำต่อคำ หรือการอ้างอิงถึงคำศัพท์ทางวิชาการจากราชบัณฑิตสภา ความหมายของคำที่ใช้ มีดังต่อไปนี้

1) **ผู้ตรวจประเมิน (auditor)** หมายถึง บุคคลที่ประเมินความสอดคล้องกับข้อกำหนดตามที่ระบุไว้ในเอกสารข้อกำหนดที่กำหนด

2) **แอตทริบิวต์ (attribute)** หมายถึง คุณลักษณะหรือคุณสมบัติที่เกี่ยวข้องกับผู้ให้บริการและเอนทิตี และสามารถบันทึกลงในเอกสารรับรอง (VC) หรือเอกสารสำแดง (VP) ได้

3) **ข้อความยืนยัน (claim)** หมายถึง ข้อความเกี่ยวข้องกับเอนทิตีของข้อความ (subject) ที่ผู้ออกเอกสารรับรอง (issuer) ให้การรับรอง

4) **การตรวจประเมินความสอดคล้อง (conformity assessment)** หมายถึง กระบวนการที่แสดงให้เห็นว่าข้อกำหนดที่เกี่ยวข้องกับผลิตภัณฑ์ กระบวนการ บริการ ระบบ บุคคล หรือหน่วยงานได้ดำเนินการครบถ้วน

5) **ข้อมูลรับรอง (credential)** หมายถึง ข้อมูลดิจิทัลที่ใช้เป็นสิ่งยืนยันความถูกต้องของชุดข้อความยืนยัน (claim) เกี่ยวกับเอนติที (entity) และออกโดยผู้มีอำนาจ (authority)

6) **ชุดการเข้ารหัสลับ (cryptographic suite)** หมายถึง การรวมกันของรูปแบบลายมือชื่อกับกระบวนวิธีการเติม (padding) และฟังก์ชันแฮชด้วยการเข้ารหัสลับ (cryptographic hash function)

7) **การตรวจสอบแหล่งที่มาของข้อมูล (data origin authentication)** หมายถึง การยืนยันว่าแหล่งที่มาของข้อมูลที่ได้รับเป็นไปตามที่อ้าง

8) **เค้าร่างโครงสร้างข้อมูล (data schema)** หมายถึง ข้อมูลที่กำหนดโครงสร้าง (structure) และรูปแบบ (format) ของเอกสารรับรอง (VC) และ/หรือเอกสารสำแดง (VP) โดยสามารถแบ่งออกเป็น 2 ประเภท ได้แก่ (1) เค้าร่างสำหรับการตรวจสอบยืนยันโครงสร้างข้อมูล (data verification schema) สำหรับตรวจสอบโครงสร้างและรูปแบบของข้อมูลอิเล็กทรอนิกส์ และ (2) เค้าร่างสำหรับการเข้ารหัสข้อมูล (data

encoding schema) สำหรับการแปลงข้อมูลอิเล็กทรอนิกส์จากรูปแบบ (format) หนึ่งไปยังอีกรูปแบบหนึ่ง

9) **ดีไอดี (Decentralized identifier หรือ DID)** หมายถึง ตัวระบุ (identifier) ที่ไม่ซ้ำกันและไม่ขึ้นกับหน่วยงานกลางที่มีอำนาจหน้าที่ในการขึ้นทะเบียน โดยตัวระบุนี้มันถูกสร้างขึ้นโดยการกระบวนการเข้ารหัสลับ (cryptography)

10) **ดีไอดีดอคคิวเมนต์ (DID document)** หมายถึง ชุดข้อมูลที่ใช้อธิบายถึงเอนทิตีของดีไอดี (DID subject) ซึ่งรวมถึงข้อมูลที่ระบุถึงกลไกการยืนยันตัวตน (authentication) หรือการพิสูจน์ความเกี่ยวข้องของเอนทิตีที่เกี่ยวข้องกับดีไอดี เช่น อัลกอริทึมการเข้ารหัสลับ (cryptography algorithm) และกุญแจสาธารณะ (public keys) ที่เกี่ยวข้องกับดีไอดีนั้น

11) **ดีไอดีเมธอด (Decentralized Identifiers Methodologies หรือ DID method)** หมายถึง ชุดข้อกำหนดที่ใช้ในการสร้าง จัดการ แก้ไข และยกเลิก ดีไอดี (DID) และดีไอดีดอคคิวเมนต์ (DID document) หรือ กลไกเฉพาะสำหรับแต่ละ DID ที่ใช้ในการสร้าง ดึงข้อมูล (resolve) อัปเดต และระงับการใช้งาน DID รวมไปถึง DID document ที่เกี่ยวข้องกับ DID นั้น

12) **ลายมือชื่อดิจิทัล (Digital Signature)** หมายถึง ลายมือชื่ออิเล็กทรอนิกส์ที่ได้จากกระบวนการเข้ารหัสลับ (cryptography) ซึ่งมีคุณสมบัติที่สามารถตรวจพบการเปลี่ยนแปลงใด ๆ ที่เกิดกับความครบถ้วนของข้อมูลได้

13) **กระเป๋าดิจิทัล (Digital Wallet)** หมายถึง โปรแกรมที่จัดเก็บและช่วยให้ผู้ถือเอกสารรับรอง (holder) สามารถเข้าถึงและใช้งานเอกสารรับรองได้อย่างมั่นคงปลอดภัย

14) **ผู้ให้บริการกระเป๋าดิจิทัล (Digital Wallet Provider)** หมายถึง ผู้ให้บริการที่ทำหน้าที่พัฒนาและ/หรือให้บริการที่เกี่ยวข้องกับกระเป๋าดิจิทัล ให้แก่ผู้ออกเอกสารรับรอง (issuer) ผู้ถือเอกสารรับรอง (holder) หรือผู้ตรวจสอบเอกสารสำแดง (verifier)

15) **เอนทิตี (Entity)** หมายถึง สิ่งที่มีอยู่จริง เช่น บุคคล องค์กร ระบบซอฟต์แวร์ หรืออุปกรณ์ ซึ่งถูกกล่าวอ้างถึงในเอกสารรับรอง (VC) หรือเอกสารสำแดง (VP)

16) **หลักฐาน (Evidence)** หมายถึง ข้อมูลที่สามารถใช้เพื่อพิสูจน์ข้อพิพาทเกี่ยวกับประเด็นความถูกต้อง

17) **ฟังก์ชันแฮช (Hash Function)** หมายถึง คำนิยามตามที่กำหนดไว้ใน ISO/IEC 10118-3

18) **ผู้ถือเอกสารรับรอง (Holder)** หมายถึง เอนทิตีที่เป็นเจ้าของเอกสารรับรองอย่างน้อยหนึ่งชุด โดยจัดเก็บไว้ในกระเป๋าดิจิทัล (digital wallet) และสามารถใช้เอกสารรับรอง (VC) เพื่อสร้างเป็นเอกสารสำแดง (VP) ได้

19) **ตัวระบุ (Identifier)** หมายถึง uniform resource identifier (URI) ที่ระบุถึงเอนทิตี หรือข้อมูลอิเล็กทรอนิกส์ที่เกี่ยวข้อง

20) **ผู้ให้บริการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Identity Provider)** หมายถึง นิติบุคคลที่ให้บริการข้อมูลตัวตน

21) **ผู้ออกเอกสารรับรอง (Issuer)** หมายถึง ผู้ให้บริการที่ทำหน้าที่รับรองข้อความยืนยัน (claim) โดยออกเป็นเอกสารรับรอง (VC) ให้แก่ผู้ถือเอกสารรับรอง (holder)

22) **ข้อมูลเมตา (Metadata)** หมายถึง ข้อมูลที่อธิบายบริบท เนื้อหา และโครงสร้างของอ็อบเจกต์ข้อมูลและการจัดการในช่วงเวลาที่กำหนด

23) **อุปกรณ์โทรศัพท์เคลื่อนที่ (Mobile Device)** หมายถึง อุปกรณ์ส่วนบุคคลที่สามารถสื่อสารผ่านเครือข่ายโทรศัพท์เคลื่อนที่ โดยปกติจะเป็นอุปกรณ์ที่เหมาะสำหรับพกพา กระเป๋าถือ หรือกระเป๋าเสื้อ เช่น โทรศัพท์มือถือหรือสมาร์ทโฟน

24) **กุญแจส่วนตัว (Private Key)** หมายถึง กุญแจที่เป็นคู่ของอีกกุญแจในระบบการเข้ารหัสลับกุญแจสาธารณะ ซึ่งถูกถือครองและเข้าถึงได้โดยบุคคลหนึ่งบุคคลใดเท่านั้น

25) **กุญแจสาธารณะ (Public Key)** หมายถึง กุญแจที่เป็นคู่ของอีกกุญแจในระบบการเข้ารหัสลับกุญแจสาธารณะ ซึ่งเปิดเผยต่อสาธารณะ

26) **การตรวจสอบลายมือชื่อ (Signature Verification)** หมายถึง กระบวนการตรวจสอบค่าการเข้ารหัสลับของลายมือชื่อโดยใช้ข้อมูลการตรวจสอบลายมือชื่อ

27) **ผู้ให้บริการที่เชื่อถือได้ (Trust Service Provider)** หมายถึง บุคคลหรือนิติบุคคลที่ให้บริการที่เชื่อถือได้ตั้งแต่หนึ่งบริการขึ้นไป

28) **ผู้ตรวจสอบเอกสารสำแดง (Verifier)** หมายถึง ผู้ให้บริการที่สามารถตรวจสอบความถูกต้องของเอกสารรับรองและเอกสารสำแดงได้ด้วยกระบวนการเข้ารหัสลับ (cryptography) รวมถึงสามารถตรวจสอบสถานะความพร้อมใช้งาน/สถานะถูกเพิกถอน และตรวจสอบความสอดคล้องโครงสร้างข้อมูลของเอกสารรับรองและเอกสารสำแดง

29) **เอกสารรับรองดิจิทัล (Verifiable Credential หรือ VC)** หมายถึง ชุดของข้อความยืนยัน (claim) อย่างน้อยหนึ่งรายการที่ถูกรับรองโดยผู้ออกเอกสารรับรอง (issuer) ทั้งนี้ เอกสารรับรองนี้มีคุณสมบัติที่สามารถตรวจพบการเปลี่ยนแปลงใด ๆ ที่เกิดกับความครบถ้วนของข้อมูล และสามารถตรวจสอบความถูกต้องแท้จริงของลายมือชื่อดิจิทัลของผู้ออกเอกสารรับรอง (issuer) ได้ด้วยกระบวนการเข้ารหัสลับ (cryptography)

30) **เอกสารสำแดง (Verifiable Presentation หรือ VP)** หมายถึง เอกสารรับรองอย่างน้อยหนึ่งชุด ที่ผู้ถือเอกสารรับรอง (holder) ใช้แสดงต่อผู้ตรวจสอบเอกสารสำแดง (verifier) ทั้งนี้ เอกสารสำแดงมีคุณสมบัติที่สามารถตรวจพบการเปลี่ยนแปลงใด ๆ ที่เกิดกับความครบถ้วนของข้อมูล และสามารถตรวจสอบความถูกต้องแท้จริงของลายมือชื่อดิจิทัลของผู้ออกเอกสารรับรอง (issuer) และผู้ถือเอกสารรับรอง (holder) ได้ด้วยกระบวนการเข้ารหัสลับ (cryptography)

31) **ระบบทะเบียนเอกสารรับรอง (Verifiable Data Registry หรือ Credential Registry)** หมายถึง ระบบสนับสนุนการสร้างและตรวจสอบความถูกต้องของเอกสารรับรองและเอกสารสำแดงโดยข้อมูลที่อาจมีการจัดเก็บในระบบนี้เพื่อสนับสนุนการตรวจสอบความถูกต้อง เช่น ตัวระบุ (identifier) กุญแจสาธารณะ (public key) ของเอนทิตีที่เกี่ยวข้อง รายการเพิกถอน (revocation list) และเค้าร่างโครงสร้างข้อมูล (data schema) ของเอกสารรับรอง (VC) หรือเอกสารสำแดง (VP)

32) **กรอบแนวทางการสร้างระบบนิเวศสำหรับเอกสารรับรองและเอกสารสำแดงที่เชื่อถือได้ (Trust Model Framework)** หมายถึง ชุดแนวทาง หลักการ และข้อกำหนดที่จัดทำขึ้นเพื่อกำหนดกลไกความเชื่อมั่นทั้งในด้านเทคนิค (technical trust) และด้านธรรมาภิบาล (governance trust) สำหรับการดำเนินงานภายในระบบนิเวศของเอกสารรับรอง (VC ecosystem) โดยมีเป้าหมายเพื่อสร้างความเชื่อมั่นระหว่างผู้มีส่วนได้ส่วนเสียในระบบ เช่น ผู้ออกเอกสารรับรอง (issuer) ผู้ถือเอกสารรับรอง (holder) ผู้ตรวจสอบเอกสารสำแดง (verifier) และหน่วยควบคุมดูแลบริการเกี่ยวกับเอกสารรับรอง (VC Governance Authority) ให้สามารถแลกเปลี่ยนข้อมูลที่พิสูจน์ได้ มีความมั่นคงปลอดภัย สอดคล้องกับหลักการคุ้มครองข้อมูลส่วนบุคคล โปร่งใส่และสามารถตรวจสอบย้อนกลับได้ และเป็นที่ยอมรับในระดับสากล

33) **กรอบเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VC Trust Framework)** หมายถึง ชุดข้อกำหนดทางเทคนิคด้านความมั่นคงปลอดภัยสำหรับกระบวนการออกเอกสารรับรอง (VC) การใช้งานเอกสารสำแดง (VP) และการตรวจสอบความน่าเชื่อถือของเอกสาร

34) **กรอบธรรมาภิบาลบริการเกี่ยวกับระบบเอกสารรับรอง (VC Governance Framework)** หมายถึง ชุดข้อกำหนดที่กำหนด บทบาท หน้าที่ และกระบวนการปฏิบัติงาน (operational process) ที่จำเป็นในการสร้างความเชื่อมั่นในระบบนิเวศของเอกสารรับรอง (VC ecosystem)

35) **หน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VC Governance Authority หรือ VCGA)** หมายถึง หน่วยงานที่มีหน้าที่และความรับผิดชอบในการกำหนด กำกับดูแล และบังคับใช้กรอบธรรมาภิบาล (governance framework) ในระบบนิเวศของเอกสารรับรอง (VC ecosystem) เพื่อให้แน่ใจว่ากรอบแนวทางการสร้างความเชื่อถือ (trust framework) ดำเนินการได้อย่างมีประสิทธิภาพและสอดคล้องตามข้อกำหนดที่กำหนดไว้

36) **Universal Resolver** หมายถึง เครื่องมือหรือบริการที่ใช้สนับสนุนการทำงานร่วมกันระหว่างหลาย DID method ในกระบวนการร้องขอข้อมูล DID (DID Resolution) และการดึงข้อมูล (Resolve) DID Document

37) **DID resolver** หมายถึง ส่วนประกอบที่เป็นซอฟต์แวร์หรือฮาร์ดแวร์ที่ใช้ในกระบวนการร้องขอข้อมูล DID (DID Resolution) ซึ่งทำงานโดยใช้ DID เป็นอินพุต และได้เอาต์พุตเป็น DID document

2.2 อักษรย่อ

คำภาษาไทยที่แสดงคำเต็มภาษาอังกฤษของอักษรย่อบางส่วน เป็นคำศัพท์จากบริบทของคำเต็มภาษาอังกฤษ หรือนำคำภาษาไทยที่ได้ระบุไว้ในมาตรฐานหรือรายงานทางเทคนิคของ สพธอ. แต่ไม่ใช่เป็นการแปลคำศัพท์คำต่อคำ หรือการอ้างอิงถึงคำศัพท์ทางวิชาการจากราชบัณฑิตสภา และในส่วนที่เห็นว่าควรใช้คำภาษาไทยทับศัพท์คำภาษาอังกฤษ รายงานฉบับนี้จะระบุไว้ว่า “ทับศัพท์คำภาษาอังกฤษ” ประกอบด้วย

อักษรย่อ	คำเต็ม	คำภาษาไทย
DID	Decentralized Identifier	ดีไอดี (ทับศัพท์คำภาษาอังกฤษ)
DID Document	Decentralized Identifier Document	ดีไอดีดอคคิวเมนต์ (ทับศัพท์คำภาษาอังกฤษ)
DID Method	Decentralized Identifier Method	ดีไอดีเมธอด (ทับศัพท์คำภาษาอังกฤษ)
ECC	Elliptic Curve Cryptography	กระบวนการเข้ารหัสลับด้วยกระบวนวิธีเส้นโค้งเชิงวงรี หรือ เส้นโค้งเอลลิปติค
EdDSA	Edwards-Curve Digital Signature Algorithm	อัลกอริทึมลายมือชื่อดิจิทัลแบบสมัยใหม่ที่สร้างบนโครงสร้างคณิตศาสตร์ของ Edwards-curve elliptic curves
ENISA	European Union Agency for Network and Information Security Agency	สำนักงานความมั่นคงปลอดภัยระบบเครือข่ายและสารสนเทศสหภาพยุโรป
ETSI	European Telecommunications Standards Institute	องค์กรด้านมาตรฐานโทรคมนาคมของสหภาพยุโรป
e-POA	Electronic Power of Attorney	เอกสารมอบอำนาจอิเล็กทรอนิกส์
HTML	HyperText Markup Language	เอชทีเอ็มแอล (ทับศัพท์คำภาษาอังกฤษ)
HTTP	HyperText Transfer Protocol	โพรโทคอลเอชทีทีพี (ทับศัพท์คำภาษาอังกฤษ)

อักษรย่อ	คำเต็ม	คำภาษาไทย
IdP	Identity Provider	ผู้ให้บริการพิสูจน์และยืนยันตัวตนทางดิจิทัล
ISO/IEC	International Organization for Standardization/ International Electrotechnical Commission	องค์การระหว่างประเทศว่าด้วยการมาตรฐาน/ คณะกรรมาธิการระหว่างประเทศว่าด้วยมาตรฐานสาขาอิเล็กทรอนิกส์
JSON	JavaScript Object Notation	เจสัน (ทับศัพท์คำภาษาอังกฤษ)
NIST	National Institute of Standards and Technology	สถาบันมาตรฐานและเทคโนโลยีแห่งชาติสหรัฐอเมริกา
OID	Object Identifier	โอไอดี (ทับศัพท์คำภาษาอังกฤษ)
RFC	Request For Comments	เอกสารหรือบันทึกเพื่อขอรับความเห็นใช้ในการบันทึกการประชุมและเผยแพร่ขอรับความเห็นของ IETF
TEE/ SE	Trusted Execution Environment/ Secure Element	ส่วนมั่นคงของอุปกรณ์โทรศัพท์เคลื่อนที่
TMF	Trust Model Framework	กรอบแนวทางการสร้างระบบนิเวศสำหรับเอกสารรับรองและเอกสารสำแดงที่เชื่อถือได้
SHA	Secure Hash Algorithm	อัลกอริทึมแฮชที่มีความมั่นคง
TLS/SSL	Transport Layer Security/Secure Socket Layer protocol	โพรโทคอลทีแอลเอส/เอสเอสแอล (ทับศัพท์คำภาษาอังกฤษ) - การเข้ารหัสลับเพื่อรักษาความมั่นคงปลอดภัยให้กับข้อมูลรับส่งระหว่างเครื่องบริการและเครื่องลูกข่าย
URI	Uniform Resource Identifier	ยูอาร์ไอ (ทับศัพท์คำภาษาอังกฤษ)
URL	Uniform Resource Locator	ยูอาร์แอล (ทับศัพท์คำภาษาอังกฤษ)
URN	Uniform Resource Name	ยูอาร์เอ็น (ทับศัพท์คำภาษาอังกฤษ)
UTF	Unicode Transformation Format	รูปแบบการเข้ารหัสอักษรยูนิโคด
VC	Verifiable Credential	เอกสารรับรอง

อักษรย่อ	คำเต็ม	คำภาษาไทย
VP	Verifiable Presentation	เอกสารสำแดง
VCGA	Verifiable Credential Governance Authority	หน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล
VCGF	Verifiable Credential Governance Framework	กรอบธรรมาภิบาลบริการเกี่ยวกับระบบเอกสารรับรอง
VCTF	Verifiable Credential Trust Framework	กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้
XML	eXtensible Markup Language	เอ็กซ์เอ็มแอล (ทับศัพท์คำภาษาอังกฤษ)

3. ข้อมูลทั่วไปและวัตถุประสงค์ของกรอบแนวทางการสร้างระบบนิเวศสำหรับเอกสารรับรองและเอกสารสำแดงที่เชื่อถือได้ (Trust Model Framework)

ระบบนิเวศของเอกสารรับรอง (VC ecosystem) เป็นโครงสร้างสำคัญของการพัฒนาระบบดิจิทัลที่เชื่อถือได้ (trustworthy digital systems) โดยเปิดโอกาสให้หน่วยงานต่าง ๆ ทั้งภาครัฐและภาคเอกชนสามารถแลกเปลี่ยนข้อมูลและพิสูจน์ตัวตนผ่านเทคโนโลยีที่มีความมั่นคงปลอดภัย โปร่งใส และตรวจสอบได้ โดยไม่ต้องอาศัยตัวกลางแบบรวมศูนย์ (centralized trust authority) และยังมีข้อได้เปรียบอย่างชัดเจนเมื่อเทียบกับระบบแลกเปลี่ยนเอกสารอิเล็กทรอนิกส์แบบเดิมหลายประการ ได้แก่

- ความสามารถในการตรวจสอบความถูกต้องของเอกสารรับรองและเอกสารสำแดงมีระดับความมั่นคงปลอดภัยสูงด้วยการลงลายมือชื่อดิจิทัล (digital signature) ของเอนติทีที่เกี่ยวข้องในระบบนิเวศของเอกสารรับรอง (VC ecosystem) ซึ่งมีกลไกการป้องกันการปลอมแปลงและการแก้ไขเอกสารด้วยกระบวนการเข้ารหัสลับ (cryptography) และการเชื่อมโยงข้อมูลเข้ากับดีไอดี (DID) ของผู้ให้บริการและเอนทิตี ทำให้สามารถตรวจสอบความน่าเชื่อถือของเอกสารได้ในทั้งวงจรชีวิตของเอกสาร
- ความสามารถในการคุ้มครองข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล (data privacy) โดยผู้ถือเอกสารรับรอง (holder) สามารถควบคุมได้เองว่าจะแสดงข้อมูลใดแก่ผู้ตรวจสอบเอกสารสำแดง (verifier) และเลือกเปิดเผยข้อมูลเฉพาะส่วน (selective disclosure) ได้ เมื่อใช้โครงสร้างข้อมูลและแอพพลิเคชันที่รองรับ
- ความสามารถในการใช้งานข้ามระบบและข้ามหน่วยงาน (interoperability) ผ่านมาตรฐานเปิดที่ได้รับการยอมรับในระดับสากล เช่น W3C Verifiable Credentials [2] [3]

เมื่อเทียบกับการใช้งานและแลกเปลี่ยนเอกสารอิเล็กทรอนิกส์ในรูปแบบเดิม ซึ่งมักเป็นไฟล์แนบ เช่น ไฟล์ในรูปแบบ PDF ซึ่งแม้ว่าจะรองรับการลงลายมือชื่อดิจิทัลเพื่อรับรองข้อมูลและข้อความในไฟล์เอกสารได้ แต่ก็จะมีข้อจำกัดในบางกรณีที่ผู้รับเอกสารไม่สามารถตรวจสอบแหล่งที่มาหรือความสมบูรณ์ของเอกสารว่าเป็นเอกสารที่สร้างจากผู้ออกเอกสารหรือแหล่งข้อมูลที่เชื่อถือได้ (authoritative source) ได้อย่างน่าเชื่อถือหรือไม่ ซึ่งกลไกของระบบเอกสารรับรองช่วยให้ผู้รับเอกสารสามารถมั่นใจได้ว่าเอกสารนั้นมาจากแหล่งที่เชื่อถือได้ แม้ผู้รับเอกสารจะไม่รู้จักหรือมีการเชื่อมโยงระบบกับผู้ออกเอกสารรับรอง (issuer) และสามารถดำเนินการตรวจสอบเอกสารได้เองแบบอัตโนมัติได้โดยไม่ต้องพึ่งพาการตรวจสอบจากผู้ให้บริการรายใดรายหนึ่งเป็นเฉพาะ

ในระดับสากล มีหลายประเทศและองค์กรระดับสากลที่ได้ประยุกต์ใช้งานระบบเอกสารรับรองและเอกสารสำแดง (VC/VP) ระบบบริการจริงอย่างประสบความสำเร็จ เช่น

- สหภาพยุโรป (European Union) โครงการ “EU Digital Identity Wallet” ภายใต้ European Digital Identity Framework ได้ริเริ่มการออกใบรับรองแบบเอกสารรับรองสำหรับใบขับขี่ บัตรนักศึกษา ใบรับรองทางวิชาชีพ และข้อมูลสุขภาพที่สามารถแสดงได้ผ่านกระเป๋าดิจิทัล (digital wallet) ซึ่งผู้ถือสามารถควบคุมการเปิดเผยข้อมูลได้ตามความเหมาะสม

- หน่วยงานด้านการพัฒนาเทคโนโลยีดิจิทัลสำหรับภาครัฐ หรือ GovTech สาธารณรัฐสิงคโปร์ ได้เปิดตัวบริการ “Singpass Verifiable Credential (VC) Attestation Service” ภายใต้โครงการ National Digital Identity (NDI) เพื่อออกเอกสารรับรอง เช่น ใบรับรองการเป็นพลเมือง การเป็นเจ้าของที่อยู่ หรือคุณวุฒิทางวิชาชีพ โดยสามารถแสดงผ่านแอป Singpass และตรวจสอบความถูกต้องโดยผู้ตรวจสอบเอกสารสำแดง (verifier) ได้ทันทีผ่านลายมือชื่อดิจิทัลและ ดีไอดี (DID) โดยระบบนี้ยังรองรับการเชื่อมต่อกับแพลตฟอร์มภาคเอกชน โดยไม่ต้องลงทะเบียนผู้ใช้งานใหม่อีกครั้งเพื่อใช้บริการ
- กระทรวงวิทยาศาสตร์และเทคโนโลยีสารสนเทศ (Korean MSIT) สาธารณรัฐเกาหลี ได้ร่วมมือกับบริษัทเอกชนพัฒนาระบบการออกใบรับรองผลตรวจ COVID-19 ในรูปแบบเอกสารรับรอง โดยใช้ ดีไอดี (DID) และลายมือชื่อดิจิทัล เพื่อให้สามารถแสดงผลตรวจได้แบบปลอดภัยผ่านสมาร์ตโฟน โดยไม่เปิดเผยข้อมูลส่วนบุคคลที่ไม่จำเป็น
- หน่วยงานเทคโนโลยีสารสนเทศแห่งชาติ หรือ RIA ประเทศเอสโตเนีย ได้นำแนวคิดดิจิทัลไอดี (e-ID) และบริการภาครัฐแบบไร้กระดาษมาใช้เป็นประเทศแรกๆ ของโลก โดยปัจจุบันได้ขยายไปสู่การใช้เอกสารรับรอง ในงานบริการภาครัฐ เช่น ใบขับขี่ดิจิทัลและบัตรประจำตัวประชาชนดิจิทัล โดยอิงตามหลักการของ W3C Verifiable Credentials และใช้ลายมือชื่อดิจิทัลสำหรับการพิสูจน์ความถูกต้องของเอกสาร

ในประเทศไทย โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ได้เล็งเห็นถึงศักยภาพของเทคโนโลยีนี้ในการยกระดับการให้บริการสาธารณะและบริการทางธุรกิจดิจิทัล จึงได้พัฒนากรอบแนวทางการแลกเปลี่ยนเอกสารรับรองและเอกสารสำแดง และส่งเสริมการใช้กระเป๋าดิจิทัล (digital wallet) สำหรับผู้ถือเอกสารรับรอง (holder) เพื่อจัดเก็บและแสดงเอกสารเหล่านี้อย่างมั่นคงปลอดภัย

อย่างไรก็ตาม เพื่อให้การประยุกต์ใช้งานระบบเอกสารับรองและเอกสารสำแดง (VC/VP) สามารถนำไปใช้อย่างแพร่หลายและเป็นที่ยอมรับ การสร้างความน่าเชื่อถือในระบบนิเวศของเอกสารรับรอง (VC ecosystem) จึงเป็นเรื่องสำคัญและจำเป็นต้องมีกลไกการกำกับดูแลที่สามารถตรวจสอบได้ ทั้งในด้านเทคนิค เช่น การใช้ลายมือชื่อดิจิทัล (digital signature) และ ดีไอดี (decentralized identifier: DID) และในด้านธรรมาภิบาล เช่น การรับรองผู้ออกเอกสารรับรอง (issuer) และการกำกับดูแลผู้ตรวจสอบเอกสารสำแดง (verifier) โดยสรุปเป็นวัตถุประสงค์หลักของการจัดทำกรอบแนวทางการสร้างระบบนิเวศสำหรับเอกสารรับรองและเอกสารสำแดงที่เชื่อถือได้ (trust model framework) สำหรับเอกสารรับรองและเอกสารสำแดง ดังต่อไปนี้

1. กำหนดหลักการพื้นฐานและข้อกำหนดทั่วไป สำหรับระบบเอกสารรับรองและเอกสารสำแดง โดยมุ่งเน้นให้เกิดความเชื่อมั่นระหว่างผู้มีส่วนได้ส่วนเสียผ่านการกำหนดบทบาท หน้าที่ และเกณฑ์การประเมินความน่าเชื่อถือของแต่ละฝ่ายในระบบนิเวศของเอกสารรับรอง (VC ecosystem)
2. ส่งเสริมการใช้เทคโนโลยีตามมาตรฐานสากล เช่น W3C Verifiable Credentials Data Model [2] [3], DID Core [1], และแนวทางการแลกเปลี่ยนเอกสารรับรองและเอกสารสำแดง ตามกรอบของ Trust over IP (ToIP) [4] และ Sovrin Trust Assurance Framework [6] เพื่อให้สามารถเชื่อมโยงกับระบบในต่างประเทศได้อย่างมั่นคงปลอดภัย

3. กำหนดแนวทางการรับรองและการตรวจสอบ สำหรับผู้ออกเอกสารรับรอง (issuer) และผู้ตรวจสอบเอกสารสำแดง (verifier) เพื่อให้สามารถเข้าร่วมในระบบนิเวศของเอกสารรับรอง (VC ecosystem) ได้อย่างเป็นทางการ พร้อมกลไกในการจัดการสถานภาพของผู้ให้บริการและเอนทิตีในระบบนิเวศเมื่อเกิดการละเมิดข้อกำหนด

4. กำหนดระดับความน่าเชื่อถือ (Level of Assurance) สำหรับแต่ละประเภทของเอกสารรับรอง และการพิสูจน์และยืนยันตัวตนทางดิจิทัล เพื่อรองรับการใช้งานในหลายบริบท ตั้งแต่การยืนยันตัวตนเพื่อเข้าถึงบริการพื้นฐาน ไปจนถึงการใช้งานในภาคการเงิน ภาคแรงงาน และภาคการศึกษา

5. ส่งเสริมการนำเอกสารรับรอง ไปประยุกต์ใช้ในลักษณะที่การคุ้มสิทธิและเสรีภาพของเจ้าของข้อมูล โดยเปิดโอกาสให้ผู้ถือเอกสารรับรอง (holder) เป็นผู้ควบคุมข้อมูลของตนเอง สามารถเลือกเปิดเผยเฉพาะข้อมูลที่จำเป็น (selective disclosure) ให้แก่ผู้ตรวจสอบเอกสารสำแดง (verifier) ได้ตามวัตถุประสงค์ที่ชัดเจน และสอดคล้องกับหลักการคุ้มครองข้อมูลส่วนบุคคล (data privacy by design)

4. กรอบแนวทางการสร้างความน่าเชื่อถือสำหรับระบบนิเวศเอกสารรับรอง (VC Trust Model Framework)

กรอบแนวทางการสร้างความน่าเชื่อถือสำหรับระบบนิเวศเอกสารรับรอง (VC Trust Model Framework: TMF) แสดงดังรูปที่ ถูกออกแบบตามหลักการของกรอบแนวทางสร้างความน่าเชื่อถือที่เป็นมาตรฐานสากล โดยจัดโครงสร้างหน้าที่ในระบบนิเวศของเอกสารรับรองเป็น 4 ชั้น (four-layer stack) ตามสถาปัตยกรรมมาตรฐานระดับโลกสำหรับการสร้างความเชื่อถือดิจิทัล (Digital Trust Framework) ตาม ToIP [4] และจัดทำข้อกำหนดต่าง ๆ ในโครงสร้างคู่ขนาน (dual framework) ซึ่งประกอบด้วย

- **กรอบธรรมาภิบาลบริการเกี่ยวกับระบบเอกสารรับรอง (VC Governance Framework: VCGF)** ชุดของกฎเกณฑ์ นโยบาย และกระบวนการดำเนินงานที่จัดทำขึ้นเพื่อกำหนดกลไกในการควบคุม กำกับดูแล ตรวจสอบ และบังคับใช้กับหน่วยงานที่มีบทบาทในระบบนิเวศของเอกสารรับรอง (VC ecosystem) ทั้งนี้เพื่อให้แน่ใจว่าข้อกำหนดต่าง ๆ ภายใต้กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF) จะสามารถถูกนำไปใช้ได้อย่างมีประสิทธิภาพ โปร่งใส และเป็นไปตามมาตรฐานสากล โดยมีหลักการสำคัญ ได้แก่
    - ความโปร่งใสและการตรวจสอบได้ (transparency and accountability) กำหนดให้มีการเปิดเผยข้อมูลและกระบวนการกำกับดูแลที่ชัดเจน มีหลักฐานเอกสารที่สามารถตรวจสอบย้อนกลับได้
    - ความชัดเจนในบทบาทและหน้าที่ (clear roles and responsibilities) กำหนดหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในระบบนิเวศของเอกสารรับรอง (VC ecosystem) อย่างชัดเจน
    - การจัดการความเสี่ยงอย่างมีประสิทธิภาพ (effective risk management) สร้างกลไกการบริหารความเสี่ยงอย่างเป็นระบบ และใช้เป็นเครื่องมือในการพิจารณาหรือเพิกถอนการรับรองผู้ให้บริการและเอนทิตีต่างๆ เพื่อสร้างความเชื่อมั่นให้กับผู้มีส่วนได้ส่วนเสียภายใต้ระบบนิเวศของเอกสารรับรอง (VC ecosystem)
    - ความสอดคล้องกับมาตรฐานในระดับสากล (International recognition) สนับสนุนการใช้มาตรฐานและกระบวนการที่สอดคล้องกับแนวทางสากล เพื่อให้ได้รับการยอมรับและใช้งานข้ามระบบและข้ามประเทศได้
- **กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VC Technical Framework: VCTF)** ชุดข้อกำหนดทางเทคนิคและข้อกำหนดมาตรฐานที่ออกแบบมาเพื่อให้เอนทิตีต่าง ๆ ภายในระบบนิเวศของเอกสารรับรอง (VC ecosystem) สามารถเชื่อถือซึ่งกันและกันได้อย่างมั่นใจ เช่น ข้อกำหนดทางเทคนิคที่เกี่ยวข้องกระบวนการออกเอกสาร การจัดการ การพิสูจน์และยืนยันตัวตนดิจิทัล และการพิสูจน์ความ

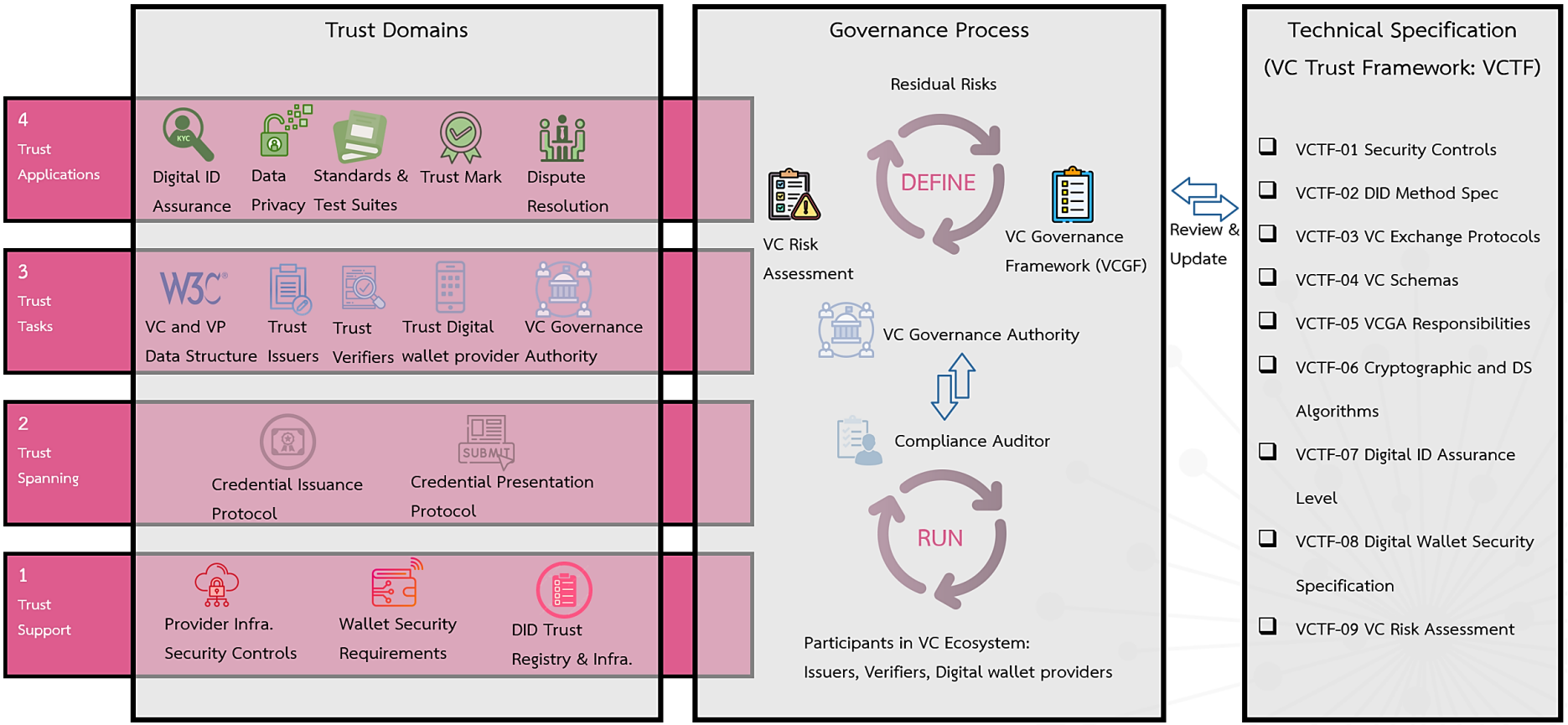
น่าเชื่อถือของเอกสารรับรอง โดยครอบคลุมตั้งแต่มาตรฐานเทคนิคด้านการเข้ารหัสลับข้อมูล มาตรการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กระบวนการประเมินและจัดการความเสี่ยง โพรโทคอลการแลกเปลี่ยนข้อมูล ไปจนถึงโครงสร้างของเอกสารรับรองและเอกสารสำแดง เป็นต้น

VC Trust Model Framework เกี่ยวข้องกับผู้มีส่วนได้ส่วนเสียหรือผู้ให้บริการและเอนทิตีภายใต้ระบบนิเวศของเอกสารรับรองหลายกลุ่ม ดังต่อไปนี้

- **หน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA)** ทำหน้าที่จัดทำและเผยแพร่กรอบแนวทางสร้างความน่าเชื่อถือ ข้อกำหนดและมาตรฐานทางเทคนิค กำกับดูแล ตรวจสอบ และรับรองผู้ให้บริการ
- **ผู้ออกเอกสารรับรอง (issuer)** เช่น หน่วยงานภาครัฐ สถาบันการศึกษา สถาบันการเงิน และองค์กรธุรกิจที่ได้รับการรับรองให้สามารถออกเอกสารรับรองที่เชื่อถือได้
- **ผู้ตรวจสอบเอกสารสำแดง (verifier)** คือ หน่วยงานหรือองค์กรที่ใช้บริการตรวจสอบข้อมูลจากผู้ถือเอกสารรับรอง เพื่อตรวจสอบความถูกต้องของข้อมูล
- **ผู้ให้บริการระบบดิจิทัล (service providers)** รวมถึงผู้ให้บริการด้านเทคนิคที่เกี่ยวข้องกับเอกสารรับรอง เช่น ผู้ให้บริการกระเป๋าดิจิทัล (digital wallet provider) ผู้ให้บริการทะเบียนข้อมูลที่เชื่อถือได้ (trust registry provider) เป็นต้น

กระบวนการกำกับดูแลกรอบแนวทางการสร้างความน่าเชื่อถือสำหรับระบบนิเวศเอกสารรับรอง (VC TMF) จะอยู่ภายใต้การดำเนินงานของหน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) โดยหน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) ต้องจัดเตรียมกลไกต่าง ๆ ที่จำเป็นในการสร้างความน่าเชื่อถือให้ระบบนิเวศของเอกสารรับรอง (VC ecosystem) เช่น การกำหนดกระบวนการตรวจประเมินที่ชัดเจนเพื่อรองรับการรับรอง (certification) ของผู้ให้บริการและเอนทิตีตามวิธีปฏิบัติและมาตรฐานสากล การจัดเตรียมบุคลากรหรือแต่งตั้งมอบหมายให้หน่วยงานทำหน้าที่เป็นผู้ตรวจประเมิน (auditor) เป็นต้น

นอกจากนี้ หน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) ยังมีหน้าที่ต้องนำกรอบแนวทางการสร้างความน่าเชื่อถือสำหรับระบบนิเวศเอกสารรับรองนี้มาทบทวน ปรับปรุงและพัฒนาอย่างสม่ำเสมอเพื่อให้สามารถตอบสนองต่อการเปลี่ยนแปลงของเทคโนโลยี นโยบายสาธารณะ และมาตรฐานสากล โดยกระบวนการปรับปรุงจะดำเนินการผ่านคณะกรรมการผู้เชี่ยวชาญจากทุกฝ่ายที่เกี่ยวข้อง ทั้งภาครัฐและเอกชน เพื่อให้มั่นใจว่ากรอบแนวทางนี้ยังคงมีความทันสมัย และมีประสิทธิภาพในการสนับสนุนการใช้งานระบบเอกสารรับรองได้อย่างยั่งยืน



รูปที่ 1 กรอบแนวทางการสร้างความน่าเชื่อถือสำหรับระบบนิเวศเอกสารรับรอง (VC Trust Model Framework)

อ้างอิงกรอบความน่าเชื่อถือของระบบนิเวศดิจิทัลโดย ToIP

4.1 คำที่ใช้แสดงออกถึงคุณลักษณะของเนื้อหาเชิงบรรทัดฐาน

กรอบแนวทางการสร้างความน่าเชื่อถือสำหรับระบบนิเวศเอกสารรับรอง ในรายงานฉบับนี้ มีรูปแบบของคำที่ใช้แสดงออกถึงคุณลักษณะของเนื้อหาเชิงบรรทัดฐาน (normative) และเนื้อหาเชิงให้ข้อมูล (informative) ดังต่อไปนี้

– "**ต้อง**" หรือ "**MUST**" ใช้ระบุสิ่งที่เป็นข้อกำหนด ซึ่งต้องปฏิบัติตาม

– "**ควร**" หรือ "**SHOULD**" ใช้ระบุสิ่งที่เป็นข้อแนะนำ

– "**อาจ**" หรือ "**MAY**" ใช้ระบุสิ่งที่ยินยอมหรืออนุญาตให้ทำได้

4.2 แนวทางการดำเนินการตามกรอบธรรมาภิบาลบริการเกี่ยวกับระบบเอกสารรับรอง (VC Governance Framework)

แนวทางการดำเนินการตามกรอบธรรมาภิบาลบริการเกี่ยวกับระบบเอกสารรับรอง (VC Governance Framework) เป็นกรอบแนวปฏิบัติกลางสำหรับหน่วยงานภายในระบบนิเวศของเอกสารรับรอง (VC ecosystem) อันประกอบด้วย ผู้ออกเอกสารรับรอง (issuer) ผู้ให้บริการกระเป๋าดิจิทัล (digital wallet provider) ผู้ตรวจสอบเอกสารสำแดง (verifier) ผู้ให้บริการทะเบียนข้อมูล (verifiable data registry provider) และหน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VC Governance Authority หรือ VCGA) เพื่อให้สามารถดำเนินงานให้สอดคล้องกับข้อกำหนดด้านการรับประกันธรรมาภิบาล (Governance Assurance Requirements) ได้อย่างเป็นระบบ มีประสิทธิภาพ และสามารถตรวจสอบได้ พร้อมส่งเสริมความเชื่อมั่น ความมั่นคงปลอดภัย และความน่าเชื่อถือของบริการในระบบนิเวศของเอกสารรับรอง (VC ecosystem) ทั้งยังเป็นเครื่องมือช่วยเตรียมความพร้อมสำหรับการตรวจประเมินความสอดคล้อง การตรวจสอบจากภายนอก และการรับรองตามระดับความน่าเชื่อถือ (level of assurance – LoA) ที่หน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) กำหนดไว้

แนวทางนี้ครอบคลุมกระบวนการสำคัญ ได้แก่ การจัดตั้งระบบควบคุมภายใน การกำหนดบทบาทและความรับผิดชอบ การตรวจประเมินความสอดคล้องด้วยตนเองและการตรวจสอบภายใน การพัฒนาและปรับปรุงอย่างต่อเนื่อง และการจัดทำรายงานเพื่อการกำกับดูแล โดยผู้ให้บริการและเอนทิตีในระบบนิเวศของเอกสารรับรองสามารถนำไปประยุกต์ใช้ให้เหมาะสมกับบริบทของตนเอง ทั้งในระดับการเริ่มต้นดำเนินงาน (initial implementation) จนถึงระดับการพัฒนาอย่างยั่งยืน (continuous improvement) เพื่อให้มั่นใจว่าการใช้งานเอกสารรับรองนั้นเป็นไปตามมาตรฐานทางเทคนิค กฎหมาย และข้อกำหนดด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง

4.2.1 การจัดตั้งการดำเนินการตามกรอบธรรมาภิบาล (Plan)

(1) ผู้ให้บริการและเอนทิตี ต้อง กำหนดบทบาทและความรับผิดชอบที่ชัดเจนในการดำเนินการตามข้อกำหนดของกรอบธรรมาภิบาลบริการเกี่ยวกับระบบเอกสารรับรอง (VCGF) และแต่งตั้งผู้รับผิดชอบด้านการดำเนินการตามกรอบธรรมภิบาล (VCGF Representative)

(2) ผู้ให้บริการและเอนทิตีในระบบนิเวศของเอกสารรับรอง (VC ecosystem) ต้อง ตรวจสอบข้อกำหนดตามกรอบธรรมาภิบาลบริการเกี่ยวกับระบบเอกสารรับรอง (VCGF) ที่เกี่ยวข้องกับบทบาทหน้าที่ของตน เช่น ผู้ออกเอกสารรับรอง (issuer) หรือผู้ให้บริการกระเป๋าดิจิทัล (digital wallet provider) จัดตั้งและดำเนินการให้เป็นกระบวนการที่สามารถปฏิบัติได้ และจัดทำเอกสารเชิงนโยบายหรือมาตรฐานภายสนับสนุนการปฏิบัติงานของผู้ที่เกี่ยวข้องให้ชัดเจน

(3) ผู้ให้บริการและเอนทิตีในระบบนิเวศของเอกสารรับรอง (VC ecosystem) ควร ดำเนินการตรวจประเมินความสอดคล้อง (gap analysis) ในการปฏิบัติกับข้อกำหนดของกรอบธรรมาภิบาลบริการเกี่ยวกับระบบเอกสารรับรอง (VCGF) และจัดทำแผนการดำเนินการปรับปรุงให้เป็นไปตามข้อกำหนด

4.2.2 การดำเนินการควบคุมภายใน (Do)

(1) ผู้ให้บริการและเอนทิตี ต้อง ดำเนินการตามข้อกำหนดของกรอบธรรมาภิบาลบริการเกี่ยวกับระบบเอกสารรับรอง (VCGF) พร้อมจัดทำรายงานผลการดำเนินการหรือเอกสารหลักฐานตามที่หน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) กำหนดอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการร้องขอ

(2) ผู้ให้บริการและเอนทิตี ต้อง เก็บรักษาหลักฐานและบันทึกผลการดำเนินการ เช่น รายงานการตรวจประเมินความสอดคล้องด้วยตนเอง รายงานการตรวจสอบ และเอกสารการแก้ไขปัญหา ให้สามารถตรวจสอบย้อนหลังได้ตามระยะเวลาที่กฎหมายหรือกรอบการประเมินหรือรับรองที่กำหนดโดยผู้ตรวจสอบ (auditor) กำหนด

4.2.3 การทบทวนและประเมินการดำเนินการ (Check)

(1) ผู้ให้บริการและเอนทิตี ต้อง จัดทำการประเมินความเสี่ยงประจำปี (Risk assessment) และ/หรือการตรวจสอบภายในเพื่อตรวจสอบความสอดคล้องของกระบวนการต่าง ๆ กับข้อกำหนดของกรอบธรรมาภิบาลบริการเกี่ยวกับระบบเอกสารรับรอง (VCGF)

(2) ผู้ให้บริการและเอนทิตี ต้อง ทบทวนกระบวนการดำเนินการตามกรอบธรรมาภิบาลบริการเกี่ยวกับระบบเอกสารรับรอง (VCGF) หลังจากเกิดเหตุการณ์สำคัญ เช่น การเปลี่ยนแปลงระบบ การเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย หรือการปรับเปลี่ยนความต้องการทางธุรกิจหรือข้อกำหนดตามกฎหมาย เพื่อใช้เป็นข้อมูลปรับปรุงและพัฒนากรอบธรรมาภิบาลบริการเกี่ยวกับระบบเอกสารรับรอง (VCGF)

4.2.4 การปรับปรุงและพัฒนาอย่างต่อเนื่อง (Act)

(1) ผู้ให้บริการและเอนทิตี ต้อง จัดทำแผนและปรับปรุงกระบวนการอย่างต่อเนื่องเพื่อแก้ไขการดำเนินงานที่มีความเสี่ยงต่อความน่าเชื่อถือของบริการในระบบนิเวศของเอกสารรับรอง (VC ecosystem)

(2) ผู้ให้บริการและเอนทิตี ต้อง จัดการเอกสารหลักฐานตามกรอบธรรมาภิบาลบริการเกี่ยวกับระบบเอกสารรับรอง (VCGF) เพื่อให้มีความทันสมัยและรองรับติดตามการเปลี่ยนแปลงที่สามารถตรวจสอบย้อนกลับได้ (change traceability)

ตารางที่ 1 การตรวจประเมินความสอดคล้องตามแนวทางการดำเนินการตามกรอบธรรมาภิบาลบริการเกี่ยวกับระบบเอกสารรับรอง (VC Governance Framework)

รายการ	แนวทางการดำเนินการ	สถานภาพ (ดำเนินการแล้ว/ ไม่ได้ดำเนินการ/อยู่ระหว่างดำเนินการ)
4.2.1 การจัดตั้งการดำเนินการตามกรอบธรรมาภิบาล (Plan)		
(1)	กำหนดบทบาทและความรับผิดชอบของผู้เกี่ยวข้อง และแต่งตั้งผู้รับผิดชอบด้านการดำเนินการตามกรอบธรรมภิบาล (VCGF Representative)	
(2)	ตรวจสอบข้อกำหนดตามกรอบธรรมาภิบาลบริการเกี่ยวกับระบบเอกสารรับรอง (VCGF) ที่เกี่ยวข้องกับบทบาทหน้าที่ของตน และจัดตั้งกระบวนการที่สามารถปฏิบัติได้	
(3)	ดำเนินตรวจประเมินความสอดคล้อง (gap analysis) กับข้อกำหนดของกรอบธรรมาภิบาลบริการเกี่ยวกับระบบเอกสารรับรอง (VCGF) และจัดทำแผนการดำเนินการให้เป็นไปตามข้อกำหนด	
4.2.2 การดำเนินการควบคุมภายใน (Do)		
(1)	ดำเนินการตามข้อกำหนดของกรอบธรรมาภิบาลบริการเกี่ยวกับระบบเอกสารรับรอง (VCGF) พร้อมจัดทำรายงานผลการดำเนินการหรือเอกสารหลักฐาน	
(2)	เก็บรักษาหลักฐานและบันทึกผลการดำเนินการ เช่น รายงานการตรวจประเมินความสอดคล้องด้วยตนเอง รายงานการตรวจสอบ และเอกสารการแก้ไขปัญหา ให้สามารถตรวจสอบย้อนกลับได้	
5.2.3 การทบทวนและประเมินการดำเนินการ (Check)		

รายการ	แนวทางการดำเนินการ	สถานภาพ (ดำเนินการแล้ว/ ไม่ได้ดำเนินการ/อยู่ระหว่างดำเนินการ)
(1)	จัดทำการประเมินความเสี่ยงประจำปี (risk assessment)	
(2)	ทบทวนกระบวนการดำเนินการตามกรอบธรรมาภิบาลบริการเกี่ยวกับระบบเอกสารรับรอง (VCGF) หลังจากเกิดเหตุการณ์สำคัญ	
4.2.4 การปรับปรุงและพัฒนาอย่างต่อเนื่อง (Act)		
(1)	จัดทำแผนและปรับปรุงกระบวนการอย่างต่อเนื่องเพื่อแก้ไขการดำเนินงานที่มีความเสี่ยง	
(2)	จัดการเอกสารหลักฐานตามกรอบธรรมาภิบาลบริการเกี่ยวกับระบบเอกสารรับรอง (VCGF) เพื่อให้สามารถตรวจสอบย้อนกลับได้ (change traceability)	

5. กรอบธรรมาภิบาลบริการเกี่ยวกับระบบเอกสารรับรอง (Verifiable Credential Governance Framework: VCGF)

กรอบธรรมาภิบาลบริการเกี่ยวกับระบบเอกสารรับรอง (VCGF) มีการจัดโครงสร้างเนื้อหาให้สามารถนำไปปฏิบัติ วัดผล รวมถึงใช้สร้างระบบประเมินตนเอง (self-assessment tools) หรือระบบตรวจประเมิน (audit) ได้ โดยในแต่ละข้อกำหนดจะมีรหัสควบคุมเฉพาะที่ใช้ระบุข้อกำหนดในรูปแบบ ***VCGF A.B.C*** โดย

- *A* สื่อถึงระดับชั้นของ ToIP (ToIP layer) ของข้อกำหนดนั้นมีค่าระหว่าง 1-4
- *B* สื่อถึงลำดับขอบเขตของข้อกำหนด (trust domain) และ
- *C* สื่อถึงลำดับของข้อกำหนดภายใต้ระดับชั้นของ ToIP *A* และลำดับขอบเขตของข้อกำหนด *B*

ข้อกำหนด VCGF แต่ละข้อกำหนดมีองค์ประกอบสำคัญ ประกอบด้วย

- **ชั้นของ ToIP (ToIP layer)** ระบุระดับของ ToIP stack ที่ข้อกำหนดนี้สอดคล้อง
- **ขอบเขตของข้อกำหนด (trust domain)** ระบุถึงระบบ พื้นที่ สิ่งแวดล้อม ประเด็น หรือวิธีการที่เฉพาะเจาะจง ซึ่งอาจจะมีข้อกำหนดได้หลายข้อที่อยู่ภายใต้ขอบเขตของข้อกำหนด (trust domain) นั้น
- **วัตถุประสงค์ของข้อกำหนด (assurance objective)** ระบุถึงวัตถุประสงค์หรือจุดมุ่งหมายของการควบคุมภายใต้ข้อกำหนดนั้น เช่น การกำหนดให้ผู้ให้บริการกระเป๋าดิจิทัลต้องมีกลไกในการป้องกันการเข้าถึงเอกสารรับรองโดยผู้ใดที่ไม่ได้รับอนุญาต เพื่อรักษาความมั่นคงปลอดภัยและความเป็นส่วนตัวของเอกสารับรองของผู้ถือเอกสารรับรอง
- **ข้อเสนอแนะในการปฏิบัติตามข้อกำหนด (governance guidance)** ระบุถึงขั้นตอน กระบวนการ หรือวิธีปฏิบัติที่เกี่ยวข้องเพื่อให้ได้ผลลัพธ์ตามจุดหมายของข้อกำหนด (assurance objective)
- **ตัวอย่างหลักฐานแสดง (evidence example)** แสดงตัวอย่างที่สามารถนำมาอ้างอิงเป็นหลักฐานเพื่อแสดงว่าได้ดำเนินการตามข้อกำหนด

ทั้งนี้ กรอบธรรมาภิบาลบริการเกี่ยวกับระบบเอกสารรับรอง (VCGF) ได้มีการจัดแบ่งเนื้อหาของข้อกำหนดโดยอ้างอิงตามโครงสร้างระดับชั้นของ ToIP (ToIP stack) ได้แก่

- **ชั้นที่ 1 trust support** ข้อกำหนดเกี่ยวกับโครงสร้างพื้นฐานของความน่าเชื่อถือ แสดงรายละเอียดในข้อ 5.1
- **ชั้นที่ 2 trust spanning** ข้อกำหนดเกี่ยวกับโพรโทคอลการแลกเปลี่ยนข้อมูล แสดงรายละเอียดในข้อ 5.2
- **ชั้นที่ 3 trust tasks** ข้อกำหนดด้านความน่าเชื่อถือกับเอกสารรับรอง แสดงรายละเอียดในข้อ 5.3
- **ชั้นที่ 4 trust applications** ข้อกำหนดที่เกี่ยวข้องกับกฎเกณฑ์ทางธุรกิจและการธรรมาภิบาลของระบบนิเวศของเอกสารับรอง แสดงรายละเอียดในข้อ 5.4

5.1 ข้อกำหนดเกี่ยวกับโครงสร้างพื้นฐานของความน่าเชื่อถือ (VCGF-1 trust support)

5.1.1 ข้อกำหนดการบริหารจัดการความมั่นคงปลอดภัยของโครงสร้างพื้นฐาน (Security controls and Technical Infrastructure) (VCGF-1.1)

- ข้อกำหนด VCGF 1.1 เป็นข้อกำหนดด้านมาตรการรักษาความมั่นคงปลอดภัยของโครงสร้างพื้นฐานและระบบสารสนเทศของผู้ให้บริการและเอนทิตีสำคัญของผู้ให้บริการในระบบนิเวศของเอกสารรับรอง ประกอบด้วย ผู้ออกเอกสารรับรอง ผู้ให้บริการกระเป๋าดิจิทัล และผู้ตรวจสอบเอกสาร

5.1.1.1 การบริหารจัดการความมั่นคงปลอดภัยของผู้ออกเอกสารรับรอง (VCGF-1.1.1)

(1) วัตถุประสงค์ของข้อกำหนด (assurance objective)

- ผู้ออกเอกสารรับรอง **ต้อง** มั่นใจว่าได้ออกแบบและมีมาตรการรักษาความมั่นคงปลอดภัยในทุกส่วนของซอฟต์แวร์และโครงสร้างพื้นฐานของบริการเอกสารรับรอง เพื่อรักษาความน่าเชื่อถือของบริการ ป้องกันความผิดพลาดหรือการโจมตีที่อาจส่งผลกระทบต่อความถูกต้องของการประมวลผลเอกสารรับรอง

(2) ข้อเสนอแนะในการปฏิบัติตามข้อกำหนด (governance guidance):

- ผู้ออกเอกสารรับรองต้องปฏิบัติตามแนวทางการรักษาความมั่นคงปลอดภัยและการดำเนินงานของผู้ให้บริการ ตามข้อเสนอแนะของ สพธอ. เช่น ขมธอ. 21-2562 และ ขมธอ. 35-2567 เพื่อให้ระบบมีความมั่นคงปลอดภัย มีความน่าเชื่อถือ และเป็นไปตามมาตรฐานที่กำหนด

(3) กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF)

- VCTF-01 Security Requirements for IT Infrastructure in the Thai VC ecosystem

(4) ตัวอย่างหลักฐานแสดง (evidence example)

- รายงานตรวจสอบหรือประเมินระบบความมั่นคงปลอดภัย (Security and Compliance Assurance) หลักฐานแสดงว่าได้นำแนวทางตามข้อเสนอแนะของ สพธอ. (เช่น ขมธอ. 21-2562 และ ขมธอ. 35-2567) มาปฏิบัติจริง เช่น รายงานการตรวจประเมิน (audit) หรือเอกสารสรุปมาตรการควบคุมที่ได้ปฏิบัติ โดยในรายงานได้แสดงว่าระบบมีการดำเนินการมาตรการควบคุมที่เหมาะสม มีการจัดการข้อมูลอย่างมั่นคงปลอดภัย และเป็นไปตามมาตรฐานด้านเทคนิค

5.1.1.2 การบริหารจัดการความมั่นคงปลอดภัยของผู้ให้บริการกระเป๋าดิจิทัล (VCGF-1.1.2)

(1) วัตถุประสงค์ของข้อกำหนด (assurance objective)

- ผู้ให้บริการกระเป๋าดิจิทัล **ต้อง** มั่นใจว่าได้ออกแบบและมีมาตรการรักษาความมั่นคงปลอดภัยในทุกส่วนของซอฟต์แวร์และโครงสร้างพื้นฐานของบริการเอกสารรับรอง เพื่อรักษาความน่าเชื่อถือบริการ

ป้องกันความผิดพลาดหรือการโจมตีที่อาจส่งผลกระทบต่อความถูกต้องของการประมวลผลเอกสารรับรอง

(2) ข้อเสนอแนะในการปฏิบัติตามข้อกำหนด (governance guidance):

- ผู้ให้บริการกระเป๋าดิจิทัลต้องปฏิบัติตามแนวทางการรักษาความมั่นคงปลอดภัยและการดำเนินงานของผู้ให้บริการ ตามข้อเสนอแนะของ สพธอ. เช่น ขมธอ. 21-2562 และ ขมธอ. 35-2567 เพื่อให้ระบบมีความมั่นคงปลอดภัย มีความน่าเชื่อถือ และเป็นไปตามมาตรฐานที่กำหนด

(3) กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF)

- VCTF-01 ข้อกำหนดด้านความมั่นคงปลอดภัยของโครงสร้างพื้นฐานไอทีสำหรับระบบนิเวศของเอกสารรับรอง

(4) ตัวอย่างหลักฐานแสดง (evidence example)

- รายงานตรวจสอบหรือประเมินระบบความมั่นคงปลอดภัย (Security and Compliance Assurance) หลักฐานแสดงว่าได้นำแนวทางตามข้อเสนอแนะของ สพธอ. (เช่น ขมธอ. 21-2562 และ ขมธอ. 35-2567) มาปฏิบัติจริง เช่น รายงานการตรวจประเมิน (audit) หรือเอกสารสรุปมาตรการควบคุมที่ได้ปฏิบัติ โดยในรายงานได้แสดงว่าระบบมีการดำเนินการมาตรการควบคุมที่เหมาะสม มีการจัดการข้อมูลอย่างมั่นคงปลอดภัย และเป็นไปตามมาตรฐานด้านเทคนิค

5.1.1.3 การบริหารจัดการความมั่นคงปลอดภัยของผู้ตรวจสอบเอกสารสำแดง (VCGF-1.1.3)

(1) วัตถุประสงค์ของข้อกำหนด (assurance objective)

- ผู้ตรวจสอบเอกสารสำแดง **ต้อง** มั่นใจว่าได้ออกแบบและมีมาตรการรักษาความมั่นคงปลอดภัยในทุกส่วนของซอฟต์แวร์และโครงสร้างพื้นฐานของบริการเอกสารรับรอง เพื่อรักษาความน่าเชื่อถือบริการป้องกันความผิดพลาดหรือการโจมตีที่อาจส่งผลกระทบต่อความถูกต้องของการประมวลผลเอกสารรับรอง

(2) ข้อเสนอแนะในการปฏิบัติตามข้อกำหนด (governance guidance):

- ผู้ตรวจสอบเอกสารสำแดงต้องปฏิบัติตามแนวทางการรักษาความมั่นคงปลอดภัยและการดำเนินงานของผู้ให้บริการ ตามข้อเสนอแนะของ สพธอ. เช่น ขมธอ. 21-2562 และ ขมธอ. 35-2567 เพื่อให้ระบบมีความมั่นคงปลอดภัย มีความน่าเชื่อถือ และเป็นไปตามมาตรฐานที่กำหนด

(3) กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF)

- VCTF-01 ข้อกำหนดด้านความมั่นคงปลอดภัยของโครงสร้างพื้นฐานไอทีสำหรับระบบนิเวศของเอกสารรับรอง

(4) ตัวอย่างหลักฐานแสดง (evidence example)

- รายงานตรวจสอบหรือประเมินระบบความมั่นคงปลอดภัย (Security and Compliance Assurance) หลักฐานแสดงว่าได้นำแนวทางตามข้อเสนอแนะของ สพธอ. (เช่น ขมธอ. 21-2562 และ ขมธอ. 35-2567) มาปฏิบัติจริง เช่น รายงานการตรวจประเมิน (audit) หรือเอกสารสรุปมาตรการควบคุมที่ได้ปฏิบัติ โดยในรายงานได้แสดงว่าระบบมีการดำเนินการมาตรการควบคุมที่เหมาะสม มีการจัดการข้อมูลอย่างมั่นคงปลอดภัย และเป็นไปตามมาตรฐานด้านเทคนิค

5.1.2 ข้อกำหนดด้านความมั่นคงปลอดภัยของกระเป๋าเอกสารดิจิทัล (Digital Wallet Security Requirements) (VCGF-1.2)

- ข้อกำหนด VCGF 1.2 เป็นข้อกำหนดด้านความมั่นคงปลอดภัยของระบบกระเป๋าดิจิทัล

5.1.2.1 ความมั่นคงปลอดภัยของกระเป๋าเอกสารดิจิทัล (VCGF-1.2.1)

(1) วัตถุประสงค์ของข้อกำหนด (assurance objective)

- ผู้ให้บริการกระเป๋าดิจิทัล **ต้อง** ใช้การจัดเก็บข้อมูลที่มั่นคง เพื่อปกป้องข้อมูลรับรองและกุญแจเข้ารหัสลับที่จัดเก็บอยู่ภายในระบบจากการเข้าถึงหรือการถูกเปิดเผยโดยมิชอบ หรือการถูกโจมตี กลไกปกป้องดังกล่าว **อาจ** รวมถึงการใช้ฮาร์ดแวร์ที่มั่นคงปลอดภัย (hardware-backed security elements) ส่วนมั่นคงของอุปกรณ์โทรศัพท์เคลื่อนที่ (secure enclave) หรืออยู่ในสภาพแวดล้อมการประมวลผลที่เชื่อถือได้

(2) ข้อเสนอแนะในการปฏิบัติตามข้อกำหนด (governance guidance):

- ผู้ให้บริการกระเป๋าดิจิทัลต้องใช้ฮาร์ดแวร์ที่ได้รับการรับรองตามมาตรฐานสากล หรืออุปกรณ์ที่มีคุณสมบัติต้านทานการแก้ไขดัดแปลง (tamper-resistant components) สำหรับการจัดเก็บข้อมูลรับรองหรือข้อมูลที่มีความอ่อนไหวของผู้ถือเอกสารรับรอง

(3) กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF)

- VCTF-08 การจัดการความมั่นคงปลอดภัยของกุญแจเข้ารหัสและการจัดเก็บเอกสารรับรองสำหรับระบบกระเป๋าดิจิทัล

(4) ตัวอย่างหลักฐานแสดง (evidence example)

- รายงานตรวจสอบการจัดเก็บข้อมูลปลอดภัย (Secure Storage Audit) แสดงรายงานการตรวจสอบหรือประเมินระบบ ที่ระบุว่ามีการใช้อุปกรณ์จัดเก็บข้อมูลที่มั่นคงในระดับฮาร์ดแวร์ ซึ่งเป็นไปตามหรือสูงกว่ามาตรฐานด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง เช่น FIPS 140-3 [12] ISO/IEC 19790 [13] หรือข้อเสนอแนะทางเทคนิคที่ สพธอ. กำหนด

- เอกสารการบริหารจัดการกุญแจเข้ารหัส (Cryptographic Key Management

Documentation) แสดงเอกสารกระบวนการบริหารจัดการวงจรชีวิตของกุญแจเข้ารหัสลับที่ออกแบบให้มีความมั่นคงปลอดภัย ครอบคลุมถึงขั้นตอนการสร้าง การจัดเก็บ การสำรอง การหมุนเวียน และการลบกุญแจ โดยต้องสอดคล้องกับมาตรฐานความมั่นคงปลอดภัยที่เกี่ยวข้อง เช่น ข้อเสนอแนะทางเทคนิคที่ สพธอ. กำหนด มาตรฐาน NIST SP 800-57 Part 1 Rev.5 (Recommendation for Key Management: Part 1 – General) หรือ FIPS 140-3 [12] อย่างเคร่งครัด

5.1.2.2 กลไกการยืนยันตัวตนสำหรับเข้าถึงเอกสารรับรองในกระเป๋าเอกสารดิจิทัล (VCGF-1.2.2)

(1) วัตถุประสงค์ของข้อกำหนด (assurance objective)

- ผู้ให้บริการกระเป๋าดิจิทัล **ต้อง** ใช้วิธีการยืนยันตัวตนมาใช้ให้สอดคล้องกับระดับความน่าเชื่อถือการยืนยันตัวตน (AAL) ที่เหมาะสม โดยต้องสอดคล้องกับระดับเข้มงวดสูงสุดของข้อมูลรับรองที่จัดเก็บไว้ภายในกระเป๋าดิจิทัล

(2) ข้อเสนอแนะในการปฏิบัติตามข้อกำหนด (governance guidance):

- ผู้ให้บริการกระเป๋าดิจิทัลต้องนำกลไกการยืนยันตัวตนที่สามารถรองรับระดับความเข้มงวดสูงสุดของข้อมูลรับรองที่จัดเก็บมาใช้ โดยวิธีการดังกล่าว ต้อง เป็นไปตามเกณฑ์ที่ สพธอ. กำหนด หรือเทียบเท่ากับเกณฑ์ของมาตรฐานระดับประเทศ เช่น NIST SP 800-63B [14] หรือ FIPS 140-3 [12]

(3) กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF)

- VCTF-07 ระดับความเข้มงวดของการพิสูจน์และยืนยันตัวตนดิจิทัล

(4) ตัวอย่างหลักฐานแสดง (evidence example)

- เอกสารการประเมินความสอดคล้องของกลไกการยืนยันตัวตน (Authentication Assurance Compliance) แสดงรายงานการทดสอบหรือการประเมินทางเทคนิคที่แสดงให้เห็นว่าวิธีการยืนยันตัวตนที่ผู้ให้บริการกระเป๋าดิจิทัลนำมาใช้ มีความสอดคล้องกับเกณฑ์ที่ สพธอ. กำหนด หรือ มาตรฐานสากลที่ได้รับการยอมรับ เช่น NIST SP 800-63B [14]

5.1.3 ข้อกำหนดความน่าเชื่อถือของโครงสร้างพื้นฐานและการเข้ารหัสลับข้อมูล (Cryptographic Integrity and Trust Infrastructure) (VCGF-1.3)

- ข้อกำหนด VCGF 1.3 เป็นข้อกำหนดเกี่ยวกับชุดการเข้ารหัสลับ (cryptographic suites) ของเอกสารรับรองซึ่งเป็นโครงสร้างพื้นฐานที่สร้างความน่าเชื่อถือให้กับระบบนิเวศของเอกสารรับรอง (VC ecosystem)

5.1.3.1 ความมั่นคงปลอดภัยของระบบทะเบียนเอกสารรับรอง (Verifiable Data Registry) (VCGF-1.3.1)

(1) วัตถุประสงค์ของข้อกำหนด (assurance objective)

- ระบบทะเบียนเอกสารรับรอง (VDR) **ต้อง** มีมาตรการรักษาความมั่นคงปลอดภัย ให้มีความพร้อมใช้ (availability) และมีคุณสมบัติต้านทานการแก้ไขดัดแปลง (tamper-resistant) เพื่อใช้จัดเก็บและบริหารจัดการข้อมูลสนับสนุนการตรวจสอบยืนยันความถูกต้อง (verification material) สำหรับผู้มีส่วนได้ส่วนเสียในระบบนิเวศของเอกสารรับรอง (VC ecosystem)

(2) ข้อเสนอแนะในการปฏิบัติตามข้อกำหนด (governance guidance):

- ระบบทะเบียนเอกสารรับรอง (VDR) ต้องเป็นแหล่งข้อมูลที่เชื่อถือได้ (authoritative source) สำหรับการตรวจสอบความน่าเชื่อถือและแสดงข้อมูลที่เกี่ยวกับเอกสารรับรอง เช่น การดึงกุญแจสาธารณะ (public key) จากดีไอดี (DID) ของผู้ออกเอกสารรับรองและผู้ตรวจสอบเอกสารสำแดงจากการตรวจสอบสถานการณ์เพิกถอนจากรหัสของเอกสารรับรอง เป็นต้น

- ระบบทะเบียนเอกสารรับรอง (VDR) ต้องมีมาตรการรักษาความมั่นคงปลอดภัยกับข้อมูลที่เหมาะสม เช่น การใช้ลายมือชื่อดิจิทัล การใช้แฮช เพื่อยืนยันว่าเป็นข้อมูลมาจากแหล่งที่เชื่อถือได้และไม่ได้ถูกแก้ไขข้อมูลโดยมิชอบ

- ระบบทะเบียนเอกสารรับรอง (VDR) ต้องเปิดให้เอนทิตีที่ได้รับอนุญาตเข้าถึงบริการตรวจสอบดีไอดี (DID) ของผู้ออกเอกสารรับรอง/ผู้ตรวจสอบเอกสารสำแดง หรือตรวจสอบสถานะการเพิกถอนของเอกสารรับรองได้ทางออนไลน์

- ระบบทะเบียนเอกสารรับรอง (VDR) ต้องปฏิบัติตามแนวทางการรักษาความมั่นคงปลอดภัยและการดำเนินงานของผู้ให้บริการ ตามข้อเสนอแนะของ สพธอ. เช่น ขมธอ. 21-2562 และ ขมธอ. 35-2567 เพื่อให้ระบบมีความมั่นคงปลอดภัย มีความน่าเชื่อถือ และเป็นไปตามมาตรฐานที่กำหนด

(3) กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF)

- VCTF-01 ข้อกำหนดด้านความมั่นคงปลอดภัยของโครงสร้างพื้นฐานไอทีสำหรับระบบนิเวศของเอกสารรับรอง

- VCTF-04 โมเดลข้อมูลและโครงสร้างข้อมูลของเอกสารรับรองและข้อความยืนยัน

(4) ตัวอย่างหลักฐานแสดง (evidence example)

- หลักฐานการเข้าถึงและความมั่นคงปลอดภัยของระบบทะเบียน (Registry Accessibility and Integrity) แสดงเอกสารหรือหลักฐานที่แสดงว่าระบบทะเบียนเอกสารรับรอง (VDR) เปิดบริการทางออนไลน์ให้เข้าถึงได้อย่างมั่นคงปลอดภัย และมีการจัดเก็บเอกสารสำคัญ เช่น ดีไอดีดอคคูเมนต์ (DID document) กุญแจสาธารณะ (public key) ของผู้ออกเอกสารรับรอง และรายการเพิกถอน (revocation list) ไว้อย่างมั่นคงปลอดภัยและต้านทานการแก้ไขดัดแปลงโดยกระบวนวิธีเข้ารหัสลับข้อมูล เช่น ลายมือชื่อดิจิทัล หรือแฮช ในการรักษาความครบถ้วนสมบูรณ์ของข้อมูล

- การปฏิบัติตามมาตรฐาน DID และระบบทะเบียน (Conformance to DID and Registry Standards) แสดงรายงานประเมินความสอดคล้องของโครงสร้างพื้นฐานระบบสารสนเทศของระบบทะเบียนเอกสารรับรอง (VDR) ว่าสอดคล้องกับข้อกำหนดของ W3C DID Core Specification และ W3C VC Status List Specification Conformance to DID and Registry Standards

- ความพร้อมใช้งานและการอัปเดตข้อมูลในระบบทะเบียน (Timeliness and Availability of Registry Data) แสดงผลการตรวจสอบหรือรายงานความพร้อมใช้งาน (uptime) ที่พิสูจน์ได้ว่าข้อมูลในระบบทะเบียนเอกสารรับรอง (VDR) เช่น กุญแจสาธารณะ (public key) ดีไอดีดอคคูเมนต์ (DID document) และสถานการณ์เพิกถอน (revocation list) เป็นข้อมูลที่เป็นปัจจุบันและสามารถเข้าถึงได้ต่อเนื่องตาม SLA ที่กำหนด

- รายงานตรวจสอบหรือประเมินระบบความมั่นคงปลอดภัย (Security and Compliance Assurance) หลักฐานแสดงว่าได้นำแนวทางตามข้อเสนอแนะของ สพธอ. (เช่น ขมธอ. 21-2562 และ ขมธอ. 35-2567) มาปฏิบัติจริง เช่น รายงานการตรวจประเมิน (audit) หรือเอกสารสรุปมาตรการควบคุมที่ได้ปฏิบัติ โดยในรายงานได้แสดงว่าระบบมีการดำเนินการมาตรการควบคุมที่เหมาะสม มีการจัดการข้อมูลอย่างมั่นคงปลอดภัย และเป็นไปตามมาตรฐานด้านเทคนิค รวมถึงแสดงรายงานการตรวจสอบหรือการประเมินระบบ ที่แสดงให้เห็นว่ามีการใช้งานอุปกรณ์จัดเก็บข้อมูลแบบฮาร์ดแวร์ที่มั่นคงปลอดภัย (hardware-based secure storage) ซึ่งเป็นไปตามหรือสูงกว่าข้อกำหนดด้านความมั่นคงปลอดภัยตามมาตรฐานที่เกี่ยวข้อง เช่น FIPS 140-3 [12] ISO/IEC 19790 [13] หรือแนวทางที่ สพธอ. กำหนด

5.1.3.2 ข้อกำหนดลายมือชื่อดิจิทัลและอัลกอริทึมเข้ารหัสลับสำหรับเอกสารรับรอง (VCGF-1.3.2)

(1) วัตถุประสงค์ของข้อกำหนด (assurance objective)

- ลายมือชื่อดิจิทัลที่ใช้ในเอกสารรับรอง (VC) **ต้อง** สร้างขึ้นด้วยอัลกอริทึมและค่าพารามิเตอร์ที่ผ่านการรับรองตามข้อกำหนดของ สพธอ. หรือมาตรฐานสากลที่ได้รับการยอมรับ เช่น ETSI TS 119 312 [15] เพื่อให้มั่นใจว่าสามารถตรวจสอบย้อนกลับได้ ทำงานร่วมกับระบบอื่นได้ และมีความมั่นคงปลอดภัยเพียงพอในระดับระบบนิเวศของเอกสารรับรอง (VC ecosystem)

(2) ข้อเสนอแนะในการปฏิบัติตามข้อกำหนด (governance guidance):

- ลายมือชื่อดิจิทัลที่ปรากฏในส่วนข้อพิสูจน์ (proof) ของเอกสารรับรองหรือเอกสารสำแดง ต้องใช้อัลกอริทึมเข้ารหัสลับ ขนาดกุญแจ และฟังก์ชันแฮชที่สอดคล้องกับรายการอัลกอริทึมที่ สพธอ. กำหนด หรือเทียบเคียงได้ตามมาตรฐานสากลที่เชื่อถือได้ เช่น ETSI TS 119 312 [15]

- การใช้งานลายมือชื่อดิจิทัลในระบบต้องปฏิบัติตามมาตรฐานเทคโนโลยีที่เป็นที่ยอมรับ เช่น JSON Web Signature (JWS) [16] JSON Web Key (JWK) [17] หรือ JSON-LD Proofs ซึ่งถูกกำหนดไว้ใน W3C Verifiable Credential Data Model [2] [3]

(3) กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF)

- VCTF-06 อัลกอริทึมการเข้ารหัสลับและลายมือชื่อดิจิทัล

(4) ตัวอย่างหลักฐานแสดง (evidence example)

- ความสอดคล้องกับมาตรฐานอัลกอริทึมและลายมือชื่อ (Algorithm and Signature Specification Compliance) แสดงรายงานหรือหลักฐานผลการทดสอบหรือเอกสารตรวจสอบที่แสดงว่าลายมือชื่อดิจิทัลในส่วนข้อพิสูจน์ (proof) ของเอกสารรับรองใช้อัลกอริทึมตามที่ สพธอ. กำหนด หรือเป็นไปตามมาตรฐานสากล ETSI TS 119 312 [15] โดยสามารถอ้างอิงผลจากเครื่องมือทดสอบเช่น OpenSSL หรือระบบทดสอบอื่นที่เชื่อถือได้

- การตรวจสอบส่วนข้อพิสูจน์ (proof) และวิธีการตรวจสอบยืนยัน (Proof Section and Verification Method Compliance) แสดงเอกสารหรือหลักฐานที่แสดงว่าข้อมูลในส่วนข้อพิสูจน์ (proof) ของเอกสารรับรองมีการเชื่อมโยงกับ ดีไอดี (DID) ของผู้ออกเอกสารรับรองอย่างถูกต้อง มีการกำหนดวิธีการตรวจสอบยืนยัน (verificationMethod) ที่สามารถใช้ตรวจสอบลายมือชื่อดิจิทัลได้จริงจากกุญแจสาธารณะ (public key) ที่ขึ้นทะเบียนไว้

5.2 ข้อกำหนดเกี่ยวกับโพรโทคอลการแลกเปลี่ยนข้อมูล (VCGF-2 trust spanning)

5.2.1 ข้อกำหนดโพรโทคอลการออกเอกสารรับรอง (Protocol for Credential Issuance) (VCGF-2.1)

- ข้อกำหนด VCGF 2.1 เป็นข้อกำหนดเชิงเทคนิคที่เกี่ยวข้องกับการแลกเปลี่ยนข้อมูลเอกสารรับรองระหว่างผู้ให้บริการและเอนทิตีในระบบนิเวศของเอกสารรับรองด้วยโพรโทคอลมาตรฐาน

5.2.1.1 โพรโทคอลออกเอกสารรับรอง (VCGF-2.1.1)

(1) วัตถุประสงค์ของข้อกำหนด (assurance objective)

- ผู้ออกเอกสารรับรองและผู้ให้บริการกระเป๋าดิจิทัล **ต้อง** ใช้โพรโทคอลที่ได้การรับรองจาก สพธอ. อย่างเคร่งครัด เพื่อให้การออกเอกสารรับรองจากผู้ออกเอกสารรับรองไปยังแอปพลิเคชันกระเป๋าดิจิทัลเป็นไปอย่างมั่นคงปลอดภัยและเป็นมาตรฐานเดียวกัน

(2) ข้อเสนอแนะในการปฏิบัติตามข้อกำหนด (governance guidance)

- ผู้ออกเอกสารรับรองและผู้ให้บริการกระเป๋าดิจิทัลต้องปฏิบัติตามโพรโทคอลการออกเอกสารรับรองที่ได้รับการรับรองจาก สพธอ. เช่น OIDC4VC (OpenID for Verifiable Credentials) ผ่านช่องทางสื่อสารที่มั่นคงปลอดภัย เช่น TLS 1.2 หรือสูงกว่า และต้องดำเนินกระบวนการออกเอกสารให้ครบถ้วนถูกต้องตามขั้นตอนที่กำหนดอย่างเคร่งครัด

- แอปพลิเคชันกระเป๋าดิจิทัลต้องตรวจสอบสถานะการลงทะเบียนของดีไอดี (DID) ของผู้ออก

เอกสารรับรองจากระบบทะเบียนเอกสารรับรอง (VDR) เพื่อยืนยันว่าผู้ออกเอกสารรับรองมีความน่าเชื่อถือและอยู่ภายใต้การกำกับดูแลของหน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) ก่อนรับเอกสารเข้าสู่ระบบ

(3) กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF)

- VCTF-03 โพรโทคอลการแลกเปลี่ยนเอกสารรับรอง

(4) ตัวอย่างหลักฐานแสดง (evidence example)

- รายงานการทดสอบความสอดคล้องกับโพรโทคอล (Protocol Conformance and Interoperability Testing) แสดงรายงานผลการทดสอบที่ยืนยันว่าการดำเนินงานตามโพรโทคอล OIDC4VC เป็นไปตามข้อกำหนด เช่น การพิสูจน์ตัวตนของผู้ออกเอกสารรับรอง กลไกการแลกเปลี่ยนโทเค็น และการออกเอกสารรับรองไปยังแอปพลิเคชันกระเป๋าดิจิทัลสำเร็จตามลำดับ

- การตรวจสอบยืนยันผู้ออกเอกสารรับรองผ่านระบบ VDR (Issuer Verification via VDR) แสดงหลักฐาน เช่น log หรือรายงานการตรวจสอบ ที่แสดงว่าแอปพลิเคชันกระเป๋าดิจิทัลได้ตรวจสอบสถานะการลงทะเบียนของดีไอดี (DID) ของผู้ออกเอกสารรับรองจากระบบทะเบียนเอกสารรับรอง (VDR) ก่อนยอมรับเอกสารรับรองเข้าระบบ

- รายงานการตรวจสอบความมั่นคงปลอดภัยของช่องทางสื่อสาร (Secure Communication Audit) แสดงรายงานการตรวจสอบความมั่นคงปลอดภัยที่แสดงให้เห็นว่า กระบวนการตรวจสอบผู้ออกเอกสารรับรองและขั้นตอนการออกเอกสารรับรอง ดำเนินการผ่านช่องทางสื่อสารที่มั่นคงปลอดภัย (เช่น TLS 1.2 หรือสูงกว่า)

5.2.1.2 การยืนยันตัวตนของผู้ถือเอกสารก่อนออกเอกสารรับรอง (VCGF-2.1.2)

(1) วัตถุประสงค์ของข้อกำหนด (assurance objective)

- ผู้ออกเอกสารรับรอง **ควร** เชื่อมต่อกับผู้ให้บริการยืนยันตัวตนที่เชื่อถือได้ (Trust IdP) ภายนอกเพื่อยืนยันตัวตนของผู้ถือเอกสารรับรองได้อย่างถูกต้องก่อนการออกเอกสารรับรอง

(2) ข้อเสนอแนะในการปฏิบัติตามข้อกำหนด (governance guidance)

- ผู้ออกเอกสารรับรองควรยืนยันตัวตนของผู้ถือเอกสารรับรองก่อนออกเอกสารรับรอง โดยใช้บริการจากผู้ให้บริการยืนยันตัวตนที่เชื่อถือได้ (Digital Identities Provider) ภายนอกที่ได้รับการรับรองจาก สพธอ. และต้องตรวจสอบให้แน่ใจว่าผู้ให้บริการยืนยันตัวตนดังกล่าวมีความเข้มงวดของการยืนยันตัวตนสอดคล้องหรือสูงกว่าระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL) และระดับความน่าเชื่อถือของการยืนยันตัวตน (AAL) ตามที่กำหนดไว้ในมาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัลของ สพธอ.

(3) กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF)

- VCTF-07 ระดับความเข้มงวดของการพิสูจน์และยืนยันตัวตนดิจิทัล

(4) ตัวอย่างหลักฐานแสดง (evidence example)

- หลักฐานการปฏิบัติตามกรอบมาตรฐานการพิสูจน์และยืนยันตัวตนดิจิทัลของ สพธอ. (Digital ID Framework Compliance Verification) แสดงเอกสารหรือรายงานรับรองที่แสดงว่าผู้ให้บริการยืนยันตัวตน (IDP) ภายนอก มีระดับความเข้มงวดการพิสูจน์และยืนยันตัวตนตามข้อกำหนดของ สพธอ.

5.2.2 ข้อกำหนดโพรโทคอลการสำแดงเอกสาร (Protocol for Presentation Exchange) (VCGF-2.2)

- ข้อกำหนด VCGF 2.2 เป็นข้อกำหนดเชิงเทคนิคที่เกี่ยวข้องกับการแลกเปลี่ยนข้อมูลเอกสารรับรองระหว่างผู้ให้บริการและเอนทิตีในระบบนิเวศของเอกสารรับรองด้วยโพรโทคอลมาตรฐาน

5.2.2.1 โพรโทคอลแลกเปลี่ยนเอกสารสำแดง (VCGF-2.2.1)

(1) วัตถุประสงค์ของข้อกำหนด (assurance objective)

- ผู้ห้บริการกระเป๋าดิจิทัลและผู้ตรวจสอบเอกสารสำแดง **ต้อง** ใช้โพรโทคอลที่ได้การรับรองจาก สพธอ. อย่างเคร่งครัด เพื่อให้การแลกเปลี่ยนเอกสารสำแดงจากแอปพลิเคชันกระเป๋าดิจิทัลไปยังผู้ตรวจสอบเอกสารสำแดงเป็นไปอย่างมั่นคงปลอดภัยและเป็นมาตรฐานเดียวกัน

(2) ข้อเสนอแนะในการปฏิบัติตามข้อกำหนด (governance guidance)

- แอปพลิเคชันกระเป๋าดิจิทัลและผู้ตรวจสอบเอกสารสำแดงต้องปฏิบัติตามโพรโทคอลการแลกเปลี่ยนเอกสารสำแดงที่ได้รับการรับรองจาก สพธอ. เช่น OIDC4VP (OpenID for Verifiable Presentations) ผ่านช่องทางสื่อสารที่มั่นคงปลอดภัย เช่น TLS 1.2 หรือสูงกว่า และดำเนินกระบวนการให้ครบถ้วนถูกต้องตามขั้นตอนที่กำหนดอย่างเคร่งครัด

- แอปพลิเคชันกระเป๋าดิจิทัลต้องตรวจสอบสถานะการลงทะเบียนของดีไอดี (DID) ของผู้ตรวจสอบเอกสารสำแดงจากระบบทะเบียนเอกสารรับรอง (VDR) เพื่อยืนยันว่าผู้ตรวจสอบเอกสารสำแดงดังกล่าวได้รับการรับรองและได้รับความเชื่อถือจากหน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) ก่อนที่จะทำการส่งเอกสารสำแดงให้

(3) กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF)

- VCTF-03 โพรโทคอลการแลกเปลี่ยนเอกสารรับรอง

(4) ตัวอย่างหลักฐานแสดง (evidence example)

- รายงานการทดสอบความสอดคล้องกับโพรโทคอล (Protocol Conformance and Interoperability Testing) แสดงรายงานผลการทดสอบที่ยืนยันว่ากระบวนการแลกเปลี่ยนเอกสาร

สำแดงตามโพรโทคอล OIDC4VP ดำเนินการได้อย่างถูกต้อง เช่น การพิสูจน์ตัวตนของผู้ตรวจสอบเอกสารสำแดง กลไกการแลกเปลี่ยนโทเค็น และการส่งเอกสารสำแดงไปยังผู้ตรวจสอบเอกสารสำแดงได้สำเร็จ

- การตรวจสอบยืนยันผู้ตรวจสอบเอกสารผ่านระบบ VDR (Verifier Verification via VDR) แสดงหลักฐาน เช่น log หรือรายงานการตรวจสอบ ที่แสดงว่าแอปพลิเคชันกระเป๋าดิจิทัลได้ตรวจสอบสถานะการลงทะเบียนดีไอดี (DID) ของผู้ตรวจสอบเอกสารผ่านระบบทะเบียนเอกสารรับรอง (VDR) ก่อนส่งเอกสารสำแดง

- รายงานการตรวจสอบความมั่นคงปลอดภัยของช่องสื่อสาร (Secure Communication Audit) แสดงรายงานการตรวจสอบความมั่นคงปลอดภัยที่แสดงให้เห็นว่า กระบวนการตรวจสอบผู้ตรวจสอบเอกสารสำแดงและขั้นตอนการแลกเปลี่ยนเอกสารสำแดง ดำเนินการผ่านช่องทางสื่อสารที่มั่นคงปลอดภัย เช่น TLS 1.2 หรือสูงกว่า

5.3 ข้อกำหนดเกี่ยวกับข้อมูลรับรอง (VCGF-3 trust tasks)

5.3.1 ข้อกำหนดโครงสร้างข้อมูลของเอกสารรับรองและเอกสารสำแดง (Verifiable Credential and Presentation Structure) (VCGF-3.1)

- ข้อกำหนด VCGF 3.1 เป็นข้อกำหนดเชิงเทคนิคที่เกี่ยวข้องกับเค้าโครงร่างและแบบข้อมูลมาตรฐานของเอกสารรับรองและเอกสารสำแดง

5.3.1.1 แบบข้อมูลสำหรับเอกสารรับรองและเอกสารสำแดง (VCGF-3.1.1)

(1) วัตถุประสงค์ของข้อกำหนด (assurance objective)

- เอกสารรับรองและเอกสารสำแดง **ต้อง** เป็นไปตามแบบข้อมูลของ W3C Verifiable Credential Data Model ที่ สพธอ. เห็นชอบให้นำมาใช้ในระบบนิเวศของเอกสารรับรอง (VC ecosystem) โดยมีโครงสร้างข้อมูลที่อิงตาม JSON Schema ซึ่งประกอบด้วยชนิดข้อมูลและโครงสร้างที่กำหนดชัดเจน

- แบบข้อมูลที่ใช้ในระบบนิเวศของเอกสารรับรอง (VC ecosystem) **ต้อง** สามารถเข้าถึงได้ผ่านระบบคลังโครงสร้างข้อมูลที่เชื่อถือได้ (trust Schema Repository) และ **ต้อง** ระบุที่อยู่ของคลังโครงสร้างข้อมูลในเอกสารรับรองและเอกสารสำแดงด้วยข้อมูลคุณสมบัติ "credentialSchema"

(2) ข้อเสนอแนะในการปฏิบัติตามข้อกำหนด (governance guidance)

- เมทาดาทาในเอกสารรับรองและเอกสารสำแดง ต้อง ระบุคุณสมบัติ "credentialSchema" ซึ่งอธิบายชนิดของสคีมา (schema type) และตำแหน่งการอ้างอิง (URI) อย่างชัดเจน

- สคีมาของ W3C VC ที่ สพธอ. เห็นชอบต้องมีนิยามองค์ประกอบข้อมูล ชนิดข้อมูล และเงื่อนไขการตรวจสอบ (validation rules) อย่างชัดเจน เพื่อให้สามารถตรวจสอบความถูกต้องเอกสารได้แบบอัตโนมัติ

- ผู้ออกเอกสารรับรองต้องรับรองว่าข้อความยืนยัน (claim) ทุกรายการในเอกสารรับรองเป็นไปตามแบบข้อมูลที่อ้างอิงไว้ เพื่อให้มั่นใจว่าสามารถทำงานร่วมกัน (interoperability) ได้กับเอนติทีอื่นในระบบนิเวศของเอกสารรับรอง (VC ecosystem) และมีความสอดคล้องกับข้อกำหนดตามมาตรฐาน W3C VC Data Model

(3) กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF)

- VCTF-04 โมเดลข้อมูลและโครงสร้างข้อมูลของเอกสารรับรองและข้อความยืนยัน

(4) ตัวอย่างหลักฐานแสดง (evidence example)

- การตรวจสอบยืนยันคุณสมบัติมาตรฐาน (Standard Properties Verification) แสดงหลักฐานว่าคุณสมบัติพื้นฐานที่กำหนดใน W3C VC Data Model เช่น @context, type, issuer, issuanceDate ได้รับการกำหนดและใช้งานอย่างถูกต้อง และมีการตรวจสอบความถูกต้องของชนิดข้อมูลและข้อจำกัดของค่าข้อมูล (value constraints) เป็นไปตามโครงสร้างข้อมูลที่ สพธอ. กำหนด

- การอ้างอิงโครงสร้างข้อมูลและการเข้าถึงแบบสาธารณะ (Schema Identification and Public Accessibility) แสดงหลักฐานว่าในเอกสารรับรองและเอกสารสำแดง มีการระบุข้อมูลคุณสมบัติ "credentialSchema" ที่ชี้ไปยังตำแหน่งการอ้างอิง (URI) สาธารณะของคลังโครงสร้างข้อมูลที่ สพธอ. เห็นชอบ และโครงสร้างข้อมูลที่อ้างอิงมีโครงสร้างที่ถูกต้องตามมาตรฐาน JSON Schema

5.3.1.2 โครงสร้างข้อมูลของข้อมูลรับรอง (VCGF-3.1.2)

(1) วัตถุประสงค์ของข้อกำหนด (assurance objective)

- เอกสารรับรอง **ต้อง** มีโครงสร้างข้อมูลที่สอดคล้องกับแบบข้อมูลและข้อกำหนดของข้อมูลรับรองและข้อความยืนยันตามที่ระบุในโครงสร้างข้อมูลอ้างอิง เพื่อให้มั่นใจว่าสามารถทำงานร่วมกันระหว่างระบบของเอนทิตีต่าง ๆ ได้

(2) ข้อเสนอแนะในการปฏิบัติตามข้อกำหนด (governance guidance)

- ข้อมูลรับรองและข้อความยืนยันในเอกสารต้องมีโครงสร้างตามแบบโครงสร้างข้อมูลที่กำหนดไว้ โดยสอดคล้องกับแบบข้อมูลและข้อกำหนดของคุณสมบัติ (attribute) ต่าง ๆ

- แบบข้อมูลและโครงสร้างต้องตรงตามข้อกำหนดในโครงสร้างข้อมูลอ้างอิง เพื่อให้สามารถตรวจสอบความถูกต้องได้ และเพื่อให้ข้อมูลในเอกสารรับรองสามารถทำงานร่วมกันระหว่างระบบของเอนทิตีต่าง ๆ ในระบบนิเวศของเอกสารรับรอง (VC ecosystem) ได้อย่างมีประสิทธิภาพ

(3) กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF)

- VCTF-04 โมเดลข้อมูลและโครงสร้างข้อมูลของเอกสารรับรองและข้อความยืนยัน

(4) ตัวอย่างหลักฐานแสดง (evidence example)

- การตรวจสอบความสอดคล้องของโครงสร้างข้อมูล (Schema Conformance Validation) แสดงหลักฐานว่าเอกสารรับรองมีแบบและโครงสร้าง ชนิดข้อมูล และข้อมูลคุณสมบัติที่ถูกต้องตรงตามโครงสร้างข้อมูลอ้างอิง

- รายงานผลการตรวจสอบอัตโนมัติจากเครื่องมือ (Automated Schema Validation Report) แสดงรายงานจากเครื่องมือการตรวจสอบความถูกต้องของโครงสร้างข้อมูล (schema validator) ที่ยืนยันว่าเอกสารรับรองมีรูปแบบและโครงสร้างข้อมูลที่ถูกต้องตามโครงสร้างข้อมูลอ้างอิง

- บันทึกการทำงานของระบบผู้ออกเอกสารรับรอง (Issuer Implementation Logs) จัดเก็บ log หรือ audit trail ของระบบที่แสดงว่าได้มีการตรวจสอบความสอดคล้องของเอกสารรับรองกับโครงสร้างข้อมูลอ้างอิงระหว่างกระบวนการออกเอกสารรับรอง

5.3.1.3 ข้อพิสูจน์ของเอกสารรับรองและเอกสารสำแดง (VCGF-3.1.3)

(1) วัตถุประสงค์ของข้อกำหนด (assurance objective)

- เอกสารรับรองและเอกสารสำแดง **ต้อง** ประกอบด้วยส่วนข้อพิสูจน์ (proof) ที่ระบุวิธีการตรวจสอบยืนยันความน่าเชื่อถือของลายมือชื่อ (verification method) อย่างชัดเจน เพื่อให้ผู้ตรวจสอบเอกสารสำแดงสามารถตรวจสอบความถูกต้องของข้อมูลและยืนยันความแท้จริงของเอกสารได้ผ่านกระบวนการตรวจสอบยืนยันด้วยการเข้ารหัสลับ (cryptography verification)

(2) ข้อเสนอแนะในการปฏิบัติตามข้อกำหนด (governance guidance)

- เอกสารรับรองและเอกสารสำแดงต้องมีส่วนข้อพิสูจน์ (proof) ที่สามารถยืนยันความครบถ้วนสมบูรณ์ของข้อมูล (integrity) และความถูกต้องแท้จริง (authenticity) ด้วยกระบวนการตรวจสอบยืนยันด้วยการเข้ารหัสลับ (cryptography verification) เพื่อป้องกันการปลอมแปลงหรือการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต

- ส่วนข้อพิสูจน์ (proof) ต้องใช้อัลกอริทึมเข้ารหัสลับที่ได้รับการรับรองจาก สพธอ. หรือเป็นไปตามรายการอัลกอริทึมตามมาตรฐาน ETSI TS 119 312 [15] เพื่อให้สอดคล้องกับแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัย

(3) กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF)

- VCTF-04 โมเดลข้อมูลและโครงสร้างข้อมูลของเอกสารรับรองและข้อความยืนยัน

- VCTF-06 อัลกอริทึมการเข้ารหัสลับและลายมือชื่อดิจิทัล

(4) ตัวอย่างหลักฐานแสดง (evidence example)

- ข้อพิสูจน์ (Proof Mechanism) แสดงหลักฐานว่าเอกสารรับรองหรือเอกสารสำแดงมีลายมือชื่อดิจิทัลที่สร้างขึ้นด้วยอัลกอริทึมเข้ารหัสลับที่ได้รับการรับรองจาก สพธอ. หรือเป็นไปตาม ETSI TS 119 312 [15] และระบุดีไอดี (DID) ของเจ้าของลายมือชื่อในส่วนข้อพิสูจน์ (proof) อย่างถูกต้อง

- กระบวนการตรวจสอบลายมือชื่อ (Proof Validation Process) แสดงการตรวจสอบความถูกต้องของลายมือชื่อด้วยกุญแจสาธารณะ (public key) ของผู้ออกเอกสารรับรองจากดีไอดีดอคคูเมนต์ (DID Document) หรือกลไกการตรวจสอบที่เชื่อถือได้อื่น

- รายงานการตรวจสอบความมั่นคงปลอดภัยของกระบวนการเข้ารหัสลับ (Cryptographic Compliance Audit) แสดงรายงานหรือผลการทดสอบที่แสดงว่ากลไกการพิสูจน์ความถูกต้องที่ใช้มีความมั่นคงปลอดภัย และสามารถตรวจสอบลายมือชื่อดิจิทัลได้อย่างถูกต้อง เช่น การใช้กุญแจสาธารณะ (public key) จากดีไอดีดอคคูเมนต์ (DID Document) หรือ ทะเบียนข้อมูลที่เชื่อถือได้ (trust registry)

5.3.1.4 การตรวจสอบการเพิกถอนและการระงับเอกสารรับรอง (VCGF-3.1.4)

(1) วัตถุประสงค์ของข้อกำหนด (assurance objective)

- เอกสารรับรอง **ต้อง** มีกลไกการตรวจสอบสถานะของเอกสาร เช่น การระบุข้อมูลคุณสมบัติ "credentialStatus" เพื่อให้ผู้ตรวจสอบสำแดงสามารถตรวจสอบสถานะการเพิกถอนหรือการระงับของเอกสารรับรองได้ในขณะตรวจสอบ

(2) ข้อเสนอแนะในการปฏิบัติตามข้อกำหนด (governance guidance)

- เอกสารรับรองต้องมีข้อมูลคุณสมบัติ "credentialStatus" ที่ระบุตำแหน่งการอ้างอิง (URI) สำหรับการตรวจสอบสถานะและระบุวิธีการตรวจสอบสถานะเอกสาร เพื่อให้สามารถตรวจสอบได้ว่าเอกสารยังใช้ได้ ถูกเพิกถอน หรือถูกระงับ

- กลไกการตรวจสอบสถานะเอกสารต้องเป็นไปตามมาตรฐานที่ได้รับการยอมรับ เช่น W3C Verifiable Credential Status List (vc-bitstring-status-list) เพื่อให้สามารถทำงานร่วมกัน (interoperability) กับเอนติทีอื่นได้อย่างมีประสิทธิภาพ

- บริการตรวจสอบสถานะของเอกสารรับรองต้องเป็นบริการสาธารณะที่สามารถเข้าถึงได้ทางออนไลน์ และต้องมีการป้องกันการแก้ไขข้อมูลโดยไม่ได้รับอนุญาต เพื่อป้องกันการปลอมแปลงสถานะของเอกสารรับรอง

(3) กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF)

- ข้อกำหนดด้านเทคนิคเกี่ยวกับบริการเพิกถอนเอกสารรับรอง (Revocation Service Specification) สามารถกำหนดเป็นส่วนหนึ่งของ VCTF-04 โมเดลข้อมูลและโครงสร้างข้อมูลของเอกสารรับรองและข้อความยืนยัน

(4) ตัวอย่างหลักฐานแสดง (evidence example)

- การระบุสถานะและการเข้าถึง (Status Identification and Accessibility) แสดงหลักฐานว่าเอกสารรับรองมีข้อมูลคุณสมบัติ "credentialStatus" ที่ชี้ไปยังแหล่งข้อมูลออนไลน์ที่เข้าถึงได้แบบสาธารณะ และแหล่งข้อมูลนั้นมีการป้องกันการแก้ไข เช่น ใช้ลายมือชื่อดิจิทัลหรือกลไกการเข้ารหัสด้วยฟังก์ชันแฮช

- ความสอดคล้องกับโครงสร้างคุณสมบัติสถานะ (Conformance to Status Property Structure and Content) แสดงว่าข้อมูลคุณสมบัติ "credentialStatus" ได้รับการจัดรูปแบบอย่างถูกต้องตามที่กำหนดใน W3C Status List Specification และมี ข้อมูลคุณสมบัติย่อย (sub-properties) เช่น "id" และ "type" ที่สอดคล้องกับมาตรฐานที่กำหนด

- ความทันต่อสถานะปัจจุบันของข้อมูล (Timeliness of Status Information) แสดงให้เห็นว่าข้อมูลสถานะของเอกสารได้รับการปรับปรุงให้สอดคล้องกับช่วงเวลาความถูกต้องของเอกสาร (validFrom และ validUntil) และมีการตรวจสอบสถานะเป็นระยะเพื่อให้แน่ใจว่าข้อมูลยังเป็นปัจจุบัน

- ความสอดคล้องของสถานะในเอกสารสำแดง (Consistency Across Credentials in a Verifiable Presentation) ในกรณีที่เอกสารสำแดงประกอบด้วยหลายเอกสารรับรอง แสดงหลักฐานว่าเอกสารรับรองแต่ละเอกสารมีข้อมูลคุณสมบัติ "credentialStatus" และกลไกการตรวจสอบสถานะเอกสารรับรองทั้งหมดมีความถูกต้อง

5.3.1.5 การสำแดงข้อมูลรับรองแบบเลือกได้ (VCGF-3.1.5)

(1) วัตถุประสงค์ของข้อกำหนด (assurance objective)

- เอกสารรับรอง **ต้อง** รองรับความสามารถในการสร้างข้อมูลรับรองอนุพันธ์ (derived credential) และการเปิดเผยข้อมูลบางส่วน (selective disclosure) เพื่อให้สามารถแสดงเอกสารรับรองโดยยังคงความเป็นส่วนตัวของผู้ถือเอกสาร และให้มีการเปิดเผยเฉพาะข้อมูลที่จำเป็นและได้รับความยินยอมจากผู้ถือเอกสารรับรองเท่านั้น

(2) ข้อเสนอแนะในการปฏิบัติตามข้อกำหนด (governance guidance)

- รูปแบบของข้อมูลรับรองต้องสนับสนุนกลไกการสร้างข้อมูลรับรองอนุพันธ์และการพิสูจน์แบบเปิดเผยข้อมูลบางส่วนโดยใช้กระบวนการเข้ารหัสลับ เช่น Zero-Knowledge Proof (ZKP) เพื่อให้สามารถปกป้องความเป็นส่วนตัวและลดการเปิดเผยข้อมูลที่ไม่จำเป็น

(3) กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF)

- ข้อกำหนดทางเทคนิคที่เกี่ยวข้องกับข้อมูลรับรองอนุพันธ์ (derived credential) ด้วยเทคนิค Zero-Knowledge Proof (ZKP) หรือข้อมูลรับรองแบบเลือกเปิดเผยบางส่วน (selective disclosure)

สามารถกำหนดเป็นส่วนหนึ่งของ VCTF-04 โมเดลข้อมูลและโครงสร้างข้อมูลของเอกสารรับรองและข้อความยืนยัน

(4) ตัวอย่างหลักฐานแสดง (evidence example)

- เอกสารแสดงวิธีการคุ้มครองข้อมูลส่วนบุคคล (Privacy Implementation Documentation) แสดงเอกสารด้านเทคนิคและรายงานผลการดำเนินการที่แสดงว่าระบบมีการนำกลไกการออกข้อมูลรับรองแบบคุ้มครองข้อมูลส่วนบุคคล เช่น การสร้างข้อมูลอนุพันธ์ และการเปิดเผยข้อมูลบางส่วนไปใช้

- รายงานการทดสอบการเลือกเปิดเผยบางส่วนหรือ ZKP และ (Selective Disclosure and ZKP Compliance Testing) แสดงรายงานผลการทดสอบที่แสดงว่าระบบทำงานด้วยกลไก ZKP ได้อย่างถูกต้องตามข้อกำหนด W3C หรือกระบวนการเข้ารหัสลับที่เทียบเท่า โดยไม่ต้องเปิดเผยข้อมูลต้นฉบับแก่ผู้ตรวจสอบเอกสารสำแดง

5.3.2 ข้อกำหนดความน่าเชื่อถือสำหรับผู้ออกเอกสารรับรอง (Trust Requirements for Issuers) (VCGF-3.2)

- ข้อกำหนด VCGF 3. เป็นข้อกำหนดที่เกี่ยวข้องกับคุณสมบัติของผู้ออกเอกสารรับรองที่เชื่อถือได้

5.3.2.1 คุณสมบัติของผู้ออกเอกสารรับรองที่เชื่อถือได้ (VCGF-3.2.1)

(1) วัตถุประสงค์ของข้อกำหนด (assurance objective)

- ผู้ออกเอกสารรับรองที่เชื่อถือได้ **ต้อง** ปฏิบัติตามข้อกำหนดที่ สพธอ. กำหนดไว้สำหรับผู้ออกเอกสารรับรอง ก่อนเริ่มดำเนินการออกเอกสารรับรองในระบบนิเวศของเอกสารรับรอง (VC ecosystem)

(2) ข้อเสนอแนะในการปฏิบัติตามข้อกำหนด (governance guidance)

- ผู้ออกเอกสารรับรองต้องปฏิบัติตามเกณฑ์การรับรองตามที่ สพธอ. กำหนด เพื่อให้มั่นใจว่าเป็นเอนติทีที่มีความน่าเชื่อถือ และดำเนินการได้สอดคล้องกับข้อกำหนดต่าง ๆ อย่างครบถ้วนก่อนเริ่มออกเอกสารรับรอง

(3) กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF)

- VCTF-05 บทบาทหน้าที่ของหน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA)

(4) ตัวอย่างหลักฐานแสดง (evidence example)

- การรับรองและการขึ้นทะเบียนผู้ออกเอกสารรับรอง (Issuer Onboarding and

Accreditation) แสดงหลักฐานในกระบวนการตรวจสอบและพิสูจน์ตัวตนของผู้ออกเอกสารรับรองโดยหน่วยงานกำกับดูแลที่เกี่ยวข้อง เพื่อรับรองเป็นผู้ออกเอกสารรับรองที่เชื่อถือได้ (trust issuer) และดำเนินการลงทะเบียนดีไอดี (DID) ของผู้ออกเอกสารรับรองไว้ในระบบทะเบียนข้อมูลที่เชื่อถือได้ (trust registry) เพื่อให้สามารถตรวจสอบย้อนกลับได้

- รายงานการทดสอบความสอดคล้องของฟังก์ชันการทำงาน (Functional Conformance Testing) แสดงรายงานผลการทดสอบบริการของผู้ออกเอกสารรับรอง เพื่อแสดงการเชื่อมต่อกับผู้ให้บริการกระเป๋าดิจิทัลในกระบวนการทดสอบการออกเอกสารรับรอง ตั้งแต่การสร้าง การลงลายมือชื่อ และการส่งเอกสารรับรองในรูปแบบที่เป็นไปตามข้อกำหนด

- รายงานตรวจสอบหรือประเมินระบบความมั่นคงปลอดภัย (Security and Compliance Assurance) เหมือนกับ VCGF 1.1.1

5.3.2.2 การเชื่อมโยงผู้ถือเอกสารรับรองกับดีไอดี (VCGF-3.2.2)

(1) วัตถุประสงค์ของข้อกำหนด (assurance objective)

- ผู้ออกเอกสารรับรอง **ต้อง** ดำเนินการตรวจสอบและยืนยันตัวตนของผู้ถือเอกสารรับรอง และเชื่อมโยงตัวตนดังกล่าวเข้ากับดีไอดี (DID) ของผู้ถือเอกสารรับรองอย่างเหมาะสม โดยอ้างอิงตามระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL) ที่กำหนดโดย สพธอ. หรือหน่วยงานกำกับดูแลที่เกี่ยวข้อง

(2) ข้อเสนอแนะในการปฏิบัติตามข้อกำหนด (governance guidance)

- ผู้ออกเอกสารรับรองต้องรับรองว่าผู้ถือเอกสารรับรองเชื่อมโยงกับดีไอดี (DID) ของผู้ถือเอกสารรับรองก่อนการออกเอกสารรับรอง

(3) กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF)

- VCTF-02 ดีไอดีเมธอดสำหรับระบบนิเวศของเอกสารรับรอง

- VCTF-07 ระดับความเข้มงวดของการพิสูจน์และยืนยันตัวตนดิจิทัล

(4) ตัวอย่างหลักฐานแสดง (evidence example)

- การพิสูจน์ตัวตนของผู้ถือเอกสารรับรอง (Holder Identity Proofing) แสดงให้เห็นว่ากระบวนการพิสูจน์ตัวตนที่ดำเนินการสำหรับผู้ถือเอกสารรับรองเป็นไปตามเกณฑ์ระดับความเข้มงวดการพิสูจน์และยืนยันตัวตน ที่กำหนดตามกรอบมาตรฐานการพิสูจน์และยืนยันตัวตน ของ สพธอ. โดยอาจแสดงหลักฐานที่เกี่ยวข้อง เช่น log การพิสูจน์ตัวตน บันทึกการพิสูจน์ตัวตนด้วยชีวมิติ รายงานตรวจสอบเอกสารแสดงตัวตน และแสดงให้เห็นว่ามีการเชื่อมโยงตัวตนที่ได้รับการยืนยันแล้วเข้ากับดีไอดี (DID) ของผู้ถือเอกสารรับรองอย่างมั่นคงปลอดภัย

5.3.2.3 การคุ้มครองข้อมูลส่วนบุคคลของผู้ออกเอกสารรับรอง (VCGF-3.2.3)

(1) วัตถุประสงค์ของข้อกำหนด (assurance objective)

- ผู้ออกเอกสารรับรอง **ต้อง** ปฏิบัติตามข้อกำหนดและกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องทั้งหมด

(2) ข้อเสนอแนะในการปฏิบัติตามข้อกำหนด (governance guidance)

- ผู้ออกเอกสารรับรองต้องจัดทำและเผยแพร่นโยบายหรือคำประกาศคุ้มครองข้อมูลส่วนบุคคลที่ชัดเจน ครอบคลุมถึงวัตถุประสงค์ วิธีการ เกณฑ์ระยะเวลาการจัดเก็บ และการเปิดเผยข้อมูลส่วนบุคคลของผู้ถือเอกสารรับรอง โดยต้องมีความสอดคล้องกับข้อกำหนดตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง

- ผู้ออกเอกสารรับรองต้องจัดให้มีระบบสารสนเทศที่มีการรักษามั่นคงปลอดภัยในการจัดเก็บข้อมูลส่วนบุคคล โดยใช้มาตรการควบคุมการเข้าถึงที่มีความมั่นคงปลอดภัยที่เข้มงวด เช่น การเข้ารหัสข้อมูลลับ การควบคุมสิทธิการเข้าถึง และการลบข้อมูลอย่างปลอดภัยเมื่อครบระยะเวลาที่กฎหมายหรือความจำเป็นทางปฏิบัติกำหนด

(3) กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF)

- กฎหมายและข้อกำหนดคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องทั้งหมด

(4) ตัวอย่างหลักฐานแสดง (evidence example)

- การเปิดเผยนโยบายคุ้มครองข้อมูลอย่างโปร่งใส (Transparency of Privacy Policies) แสดงนโยบายหรือคำประกาศคุ้มครองข้อมูลส่วนบุคคลที่เปิดเผยต่อสาธารณะ และอธิบายอย่างชัดแจ้งถึงวัตถุประสงค์ วิธีการ และเงื่อนไขในการประมวลผลข้อมูลส่วนบุคคลของผู้ถือเอกสารรับรอง ตลอดจนระบุสิทธิของเจ้าของข้อมูล เช่น สิทธิในการเข้าถึง แก้ไข ถอนความยินยอม และลบข้อมูล

- การจัดเก็บข้อมูลส่วนบุคคลอย่างมั่นคงปลอดภัยและการจัดการตามระยะเวลา (Secure Data Storage and Retention Compliance) แสดงรายงานการตรวจประเมินหรือการรับรอง ว่ามีการจัดเก็บข้อมูลส่วนบุคคลอย่างมั่นคงปลอดภัย โดยมีการเข้ารหัสลับข้อมูลและควบคุมการเข้าถึงอย่างเหมาะสม รวมถึงการจัดการข้อมูลส่วนบุคคลที่เกินระยะเวลาการจัดเก็บตามกฎหมายอย่างเป็นระบบ เช่น การลบข้อมูลหรือทำให้ไม่สามารถระบุตัวตนได้

- เอกสารแสดงการปฏิบัติตามข้อกำหนดด้านการคุ้มครองข้อมูล (Compliance Evidence Documentation) แสดงเอกสารการปฏิบัติตามข้อกำหนด เช่น รายงานการตรวจสอบความสอดคล้องข้อปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล หรือ log การดำเนินการที่แสดงให้เห็นถึงการปฏิบัติตามกฎหมายและข้อกำหนดการคุ้มครองข้อมูลส่วนบุคคล และแนวทางการจัดการข้อมูลที่มั่นคง

ปลอดภัยอย่างต่อเนื่อง

5.3.3 ข้อกำหนดความน่าเชื่อถือสำหรับผู้ตรวจสอบเอกสารสำแดง (Trust Requirements for Verifiers) (VCGF-3.3)

- ข้อกำหนด VCGF 3.3 เป็นข้อกำหนดที่เกี่ยวข้องกับคุณสมบัติของผู้ตรวจสอบเอกสารสำแดงที่เชื่อถือได้

5.3.3.1 คุณสมบัติของผู้ตรวจสอบเอกสารสำแดงที่เชื่อถือได้ (VCGF-3.3.1)

(1) วัตถุประสงค์ของข้อกำหนด (assurance objective)

- ผู้ตรวจสอบเอกสารสำแดงที่เชื่อถือได้ **ต้อง** ปฏิบัติตามข้อกำหนดที่ สพธอ. กำหนดไว้สำหรับผู้ตรวจสอบเอกสารสำแดง ก่อนเข้าร่วมในระบบนิเวศของเอกสารรับรอง (VC ecosystem)

(2) ข้อเสนอแนะในการปฏิบัติตามข้อกำหนด (governance guidance)

- ผู้ตรวจสอบเอกสารสำแดงต้องปฏิบัติตามเกณฑ์การรับรองตามที่ สพธอ. กำหนด เพื่อให้มั่นใจว่าเป็นเอนติทีที่มีความน่าเชื่อถือ และดำเนินการได้สอดคล้องกับข้อกำหนดต่าง ๆ อย่างครบถ้วนก่อนเข้าร่วมในระบบนิเวศของเอกสารรับรอง (VC ecosystem)

(3) กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF)

- VCTF-05 บทบาทหน้าที่ของหน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA)

(4) ตัวอย่างหลักฐานแสดง (evidence example)

- การรับรองและการขึ้นทะเบียนผู้ตรวจสอบเอกสารสำแดง (Verifier Onboarding and Accreditation) แสดงหลักฐานในกระบวนการตรวจสอบและพิสูจน์ตัวตนของผู้ตรวจสอบเอกสารสำแดง โดยหน่วยงานกำกับดูแลที่เกี่ยวข้อง เพื่อรับรองเป็นผู้ตรวจสอบเอกสารสำแดงที่เชื่อถือได้ (trust verifier) และดำเนินการลงทะเบียนดีไอดี (DID) ของผู้ตรวจสอบเอกสารสำแดงไว้ในทะเบียนข้อมูลที่เชื่อถือได้ (trust registry) เพื่อให้สามารถตรวจสอบย้อนกลับได้

- รายงานการทดสอบความสอดคล้องของฟังก์ชันการทำงาน (Functional Conformance Testing) แสดงรายงานผลการทดสอบบริการของผู้ตรวจสอบเอกสารสำแดง เพื่อแสดงการเชื่อมต่อกับผู้ให้บริการกระเป๋าดิจิทัลในกระบวนการทดสอบการแลกเปลี่ยนเอกสารสำแดง เป็นไปตามข้อกำหนดของ สพธอ.

- รายงานตรวจสอบหรือประเมินระบบความมั่นคงปลอดภัย (Security and Compliance

Assurance) เหมือนกับ VCGF 1.1.3

5.3.3.2 การคุ้มครองข้อมูลส่วนบุคคลของผู้ตรวจสอบเอกสารสำแดง (VCGF-3.3.2)

(1) วัตถุประสงค์ของข้อกำหนด (assurance objective)

- ผู้ตรวจสอบเอกสารสำแดง **ต้อง** ปฏิบัติตามข้อกำหนดและกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องทั้งหมด

(2) ข้อเสนอแนะในการปฏิบัติตามข้อกำหนด (governance guidance)

- ผู้ตรวจสอบเอกสารสำแดงต้องจัดทำและเผยแพร่นโยบายหรือคำประกาศคุ้มครองข้อมูลส่วนบุคคลที่ชัดเจน ครอบคลุมถึงวัตถุประสงค์ วิธีการ เกณฑ์ระยะเวลาการจัดเก็บ และการเปิดเผยข้อมูลส่วนบุคคลของผู้ถือเอกสารรับรอง โดยต้องมีความสอดคล้องกับข้อกำหนดตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง

- ผู้ตรวจสอบเอกสารสำแดงต้องจัดให้มีระบบสารสนเทศที่มีการรักษามั่นคงปลอดภัยในการจัดเก็บข้อมูลส่วนบุคคล โดยใช้มาตรการควบคุมการเข้าถึงที่มีความมั่นคงปลอดภัยที่เข้มงวด เช่น การเข้ารหัสข้อมูลลับ การควบคุมสิทธิการเข้าถึง และการลบข้อมูลอย่างปลอดภัยเมื่อครบระยะเวลาที่กฎหมายหรือความจำเป็นทางปฏิบัติกำหนด

(3) กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF)

- กฎหมายและข้อกำหนดคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องทั้งหมด

(4) ตัวอย่างหลักฐานแสดง (evidence example)

- การเปิดเผยนโยบายคุ้มครองข้อมูลอย่างโปร่งใส (Transparency of Privacy Policies) แสดงนโยบายหรือคำประกาศคุ้มครองข้อมูลส่วนบุคคลที่เปิดเผยต่อสาธารณะ และอธิบายอย่างชัดแจ้งถึงวัตถุประสงค์ วิธีการ และเงื่อนไขในการประมวลผลข้อมูลส่วนบุคคลของผู้ถือเอกสารรับรอง ตลอดจนระบุสิทธิของเจ้าของข้อมูล เช่น สิทธิในการเข้าถึง แก้ไข ถอนความยินยอม และลบข้อมูล

- การจัดเก็บข้อมูลส่วนบุคคลอย่างมั่นคงปลอดภัยและการจัดการตามระยะเวลา (Secure Data Storage and Retention Compliance) แสดงรายงานการตรวจประเมินหรือการรับรอง ว่ามีการจัดเก็บข้อมูลส่วนบุคคลอย่างมั่นคงปลอดภัย โดยมีการเข้ารหัสลับข้อมูลและควบคุมการเข้าถึงอย่างเหมาะสม รวมถึงการจัดการข้อมูลส่วนบุคคลที่เกินระยะเวลาการจัดเก็บตามกฎหมายอย่างเป็นระบบ เช่น การลบข้อมูลหรือทำให้ไม่สามารถระบุตัวตนได้

- เอกสารแสดงการปฏิบัติตามข้อกำหนดด้านการคุ้มครองข้อมูล (Compliance Evidence Documentation) แสดงเอกสารการปฏิบัติตามข้อกำหนด เช่น รายงานการตรวจสอบความสอดคล้องข้อปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล หรือ log การดำเนินการที่แสดงให้เห็นถึงการปฏิบัติ

ตามกฎหมายและข้อกำหนดการคุ้มครองข้อมูลส่วนบุคคล และแนวทางการจัดการข้อมูลที่มั่นคงปลอดภัยอย่างต่อเนื่อง

5.3.4 ข้อกำหนดความน่าเชื่อถือสำหรับผู้ให้บริการกระเป๋าดิจิทัล (Trust Requirements for Digital wallet providers) (VCGF-3.4)

- ข้อกำหนด VCGF 3.4 เป็นข้อกำหนดที่เกี่ยวข้องกับคุณสมบัติของผู้ตรวจสอบเอกสารสำแดงที่เชื่อถือได้

5.3.4.1 คุณสมบัติของผู้ให้บริการกระเป๋าดิจิทัลที่เชื่อถือได้ (VCGF-3.4.1)

(1) วัตถุประสงค์ของข้อกำหนด (assurance objective)

- ผู้ให้บริการกระเป๋าดิจิทัล **ต้อง** ปฏิบัติตามข้อกำหนดที่ สพธอ. กำหนดไว้สำหรับผู้ให้บริการกระเป๋าดิจิทัล ก่อนเริ่มให้บริการแอปพลิเคชันกระเป๋าดิจิทัลในระบบนิเวศของเอกสารรับรอง (VC ecosystem)

(2) ข้อเสนอแนะในการปฏิบัติตามข้อกำหนด (governance guidance)

- ผู้ให้บริการกระเป๋าดิจิทัลต้องดำเนินการให้แน่ใจว่าแอปพลิเคชันที่ให้บริการสอดคล้องกับมาตรฐาน โพรโทคอล และข้อกำหนดทางเทคนิคที่เกี่ยวข้องซึ่งระบุไว้ภายใต้กรอบเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VC Trust Framework)

(3) กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF)

- VCTF-01 ข้อกำหนดด้านความมั่นคงปลอดภัยของโครงสร้างพื้นฐานไอทีสำหรับระบบนิเวศของเอกสารรับรอง

- VCTF-03 โพรโทคอลการแลกเปลี่ยนเอกสารรับรอง

- VCTF-08 การจัดการความมั่นคงปลอดภัยของกุญแจเข้ารหัสและการจัดเก็บเอกสารรับรองสำหรับระบบกระเป๋าดิจิทัล

(4) ตัวอย่างหลักฐานแสดง (evidence example)

- รายงานผลการทดสอบการทำงานและการทำงานร่วมกันระหว่างระบบ (Functional and Interoperability Test Reports) แสดงรายงานผลการทดสอบของการทำงานร่วมกันระหว่างผู้ให้บริการกระเป๋าดิจิทัล ผู้ออกเอกสารรับรอง และผู้ตรวจสอบเอกสารสำแดง โดยการทดสอบต้องเป็นไปตามกรณีทดสอบที่ สพธอ. กำหนดไว้

- รายงานตรวจสอบหรือประเมินระบบความมั่นคงปลอดภัย (Security and Compliance Assurance) เหมือนกับ VCGF 1.1.3

5.3.4.2 ข้อกำหนดการยืนยันตัวตนและความมั่นคงปลอดภัยของกระเป๋าดิจิทัล (VCGF-3.4.2)

(1) วัตถุประสงค์ของข้อกำหนด (assurance objective)

- ผู้ให้บริการกระเป๋าดิจิทัล **ต้อง** ใช้กลไกการยืนยันตัวตนที่มีความมั่นคงปลอดภัยสูง และมีวิธีการจัดเก็บข้อมูลที่ปลอดภัย เพื่อปกป้องข้อมูลรับรองและกุญแจเข้ารหัสลับของผู้ใช้งานจากการเข้าถึงโดยไม่ได้รับอนุญาต

(2) ข้อเสนอแนะในการปฏิบัติตามข้อกำหนด (governance guidance)

- ผู้ให้บริการกระเป๋าดิจิทัลต้องใช้กลไกการยืนยันตัวตนสำหรับเข้าถึงข้อมูลรับรองภายในกระเป๋าดิจิทัลที่มีระดับความมั่นคงปลอดภัยเทียบเท่าหรือสูงกว่าข้อมูลรับรองที่จัดเก็บไว้ โดยต้องเป็นไปตามเกณฑ์ที่กำหนดโดย สพธอ. หรือมาตรฐานสากล เช่น NIST SP 800-63B [14] และ FIPS 140-3 [12]

- ผู้ให้บริการกระเป๋าดิจิทัลต้องใช้อุปกรณ์จัดเก็บที่ได้รับการรับรองความมั่นคงปลอดภัยในระดับสากล หรืออุปกรณ์ที่ต้านทานการแก้ไขดัดแปลง (tamper-resistant) สำหรับจัดเก็บข้อมูลรับรองหรือข้อมูลที่มีความอ่อนไหวของผู้ถือเอกสารรับรอง

(3) กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF)

- VCTF-07 ระดับความเข้มงวดของการพิสูจน์และยืนยันตัวตนดิจิทัล
- VCTF-08 การจัดการความมั่นคงปลอดภัยของกุญแจเข้ารหัสและการจัดเก็บเอกสารรับรองสำหรับระบบกระเป๋าดิจิทัล

(4) ตัวอย่างหลักฐานแสดง (evidence example)

- การปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัย (Security Compliance) แสดงรายงานผลการทดสอบกลไกการยืนยันตัวตนที่ผู้ให้บริการกระเป๋าดิจิทัลนำมาใช้ มีความสอดคล้องกับเกณฑ์ด้านความมั่นคงปลอดภัยของ สพธอ. หรือมาตรฐานสากล เช่น NIST SP 800-63B [14] และ FIPS 140-3 [12] สำหรับอุปกรณ์โมดูลเข้ารหัสลับ

- รายงานการตรวจสอบการจัดเก็บข้อมูลอย่างปลอดภัย (Secure Storage Audit) แสดงรายงานการตรวจประเมินอุปกรณ์จัดเก็บข้อมูลแบบฮาร์ดแวร์ที่ใช้ มีความมั่นคงปลอดภัยในระดับที่เป็นไปตามหรือสูงกว่ามาตรฐานที่เกี่ยวข้อง เช่น FIPS 140-3 [12] ISO/IEC 19790 [13] หรือเกณฑ์ที่ สพธอ. กำหนด

- เอกสารกระบวนการบริหารจัดการกุญแจเข้ารหัส (Cryptographic Key Management

Documentation) แสดงหลักฐานว่ามีการบริหารจัดการวงจรชีวิตของกุญแจเข้ารหัสลับอย่างมั่นคงปลอดภัย ครอบคลุมถึงการสร้าง จัดเก็บ สำรองข้อมูล หมุนเวียน และลบกุญแจ โดยเป็นไปตามมาตรฐานความมั่นคงปลอดภัยที่กำหนด เช่น ข้อเสนอแนะมาตรฐานทางเทคนิคของ สพธอ. NIST SP 800-63B [14] และ FIPS 140-3 [12]

5.3.4.3 การคุ้มครองข้อมูลส่วนบุคคลของผู้ให้บริการกระเป๋าดิจิทัล (VCGF-3.4.3)

(1) วัตถุประสงค์ของข้อกำหนด (assurance objective)

- ผู้ให้บริการกระเป๋าดิจิทัล **ต้อง** ปฏิบัติตามข้อกำหนดและกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องทั้งหมด

(2) ข้อเสนอแนะในการปฏิบัติตามข้อกำหนด (governance guidance)

- ผู้ให้บริการกระเป๋าดิจิทัลต้องจัดทำและเผยแพร่นโยบายหรือคำประกาศคุ้มครองข้อมูลส่วนบุคคลที่ชัดเจน ครอบคลุมถึงวัตถุประสงค์ วิธีการ เกณฑ์ระยะเวลาการจัดเก็บ และการเปิดเผยข้อมูลส่วนบุคคลของผู้ถือเอกสารรับรอง โดยต้องมีความสอดคล้องกับข้อกำหนดตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง

- ผู้ให้บริการกระเป๋าดิจิทัลต้องจัดให้มีระบบสารสนเทศที่มีการรักษามั่นคงปลอดภัยในการจัดเก็บข้อมูลส่วนบุคคล โดยใช้มาตรการควบคุมการเข้าถึงที่มีความมั่นคงปลอดภัยที่เข้มงวด เช่น การเข้ารหัสข้อมูลลับ การควบคุมสิทธิการเข้าถึง และการลบข้อมูลอย่างปลอดภัยเมื่อครบระยะเวลาที่กฎหมายหรือความจำเป็นทางปฏิบัติกำหนด

(3) กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF)

- กฎหมายและข้อกำหนดคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องทั้งหมด

(4) ตัวอย่างหลักฐานแสดง (evidence example)

- การเปิดเผยนโยบายคุ้มครองข้อมูลอย่างโปร่งใส (Transparency of Privacy Policies) แสดงนโยบายหรือคำประกาศคุ้มครองข้อมูลส่วนบุคคลที่เปิดเผยต่อสาธารณะ และอธิบายอย่างชัดแจ้งถึงวัตถุประสงค์ วิธีการ และเงื่อนไขในการประมวลผลข้อมูลส่วนบุคคลของผู้ถือเอกสารรับรอง ตลอดจนระบุสิทธิของเจ้าของข้อมูล เช่น สิทธิในการเข้าถึง แก้ไข ถอนความยินยอม และลบข้อมูล

- การจัดเก็บข้อมูลส่วนบุคคลอย่างมั่นคงปลอดภัยและการจัดการตามระยะเวลา (Secure Data Storage and Retention Compliance) แสดงรายงานการตรวจประเมินหรือการรับรอง ว่ามีการจัดเก็บข้อมูลส่วนบุคคลอย่างมั่นคงปลอดภัย โดยมีการเข้ารหัสลับข้อมูลและควบคุมการเข้าถึงอย่างเหมาะสม รวมถึงการจัดการข้อมูลส่วนบุคคลที่เกินระยะเวลาการจัดเก็บตามกฎหมายอย่างเป็นระบบ เช่น การลบข้อมูลหรือทำให้ไม่สามารถระบุตัวตนได้

- เอกสารแสดงการปฏิบัติตามข้อกำหนดด้านการคุ้มครองข้อมูล (Compliance Evidence Documentation) แสดงเอกสารการปฏิบัติตามข้อกำหนด เช่น รายงานการตรวจสอบความสอดคล้องข้อปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล หรือ log การดำเนินการที่แสดงให้เห็นถึงการปฏิบัติตามกฎหมายและข้อกำหนดการคุ้มครองข้อมูลส่วนบุคคล และแนวทางการจัดการข้อมูลที่มั่นคงปลอดภัยอย่างต่อเนื่อง

5.3.5 ข้อกำหนดหน้าที่และรับความรับผิดชอบของหน่วยควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรอง (Responsibilities for the VC Governace Authority) (VCGF-3.5)

ข้อกำหนด VCGF 3.5 เป็นข้อกำหนดที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของหน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA)

5.3.5.1 การกำกับของหน่วยควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรอง (VCGF-3.5.1)

(1) วัตถุประสงค์ของข้อกำหนด (assurance objective)

- หน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) **ต้อง** กำกับดูแลเอนทิตีอย่างเคร่งครัด เพื่อให้มั่นใจได้ว่าการดำเนินงานภายในระบบนิเวศเอกสารรับรอง (VC ecosystem) มีความมั่นคงปลอดภัย และสามารถทำงานร่วมกันได้ (interoperability)

(2) ข้อเสนอแนะในการปฏิบัติตามข้อกำหนด (governance guidance)

- หน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) ต้องดูแลและเปิดเผยข้อมูลในทะเบียนข้อมูลที่เชื่อถือได้ (trust registry) ที่สามารถเข้าถึงได้โดยสาธารณะ โดยสามารถแสดงข้อมูลดีไอดี (DID) ที่ได้รับการตรวจสอบแล้วของเอนทิตีต่าง ๆ ที่ได้รับอนุญาตภายในระบบนิเวศของเอกสารรับรอง (VC ecosystem) เพื่อให้สามารถตรวจสอบสถานะความเชื่อถือได้อย่างมีประสิทธิภาพ

- หน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) ต้องมีกลไกการเพิกถอนข้อมูลรับรองและการอัปเดตสถานะของเอนทิตีในทะเบียนข้อมูลที่เชื่อถือได้ (trust registry) ให้เป็นปัจจุบัน

- หน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) ต้องแต่งตั้งและกำหนดบทบาทของหน่วยงานกำกับดูแลเฉพาะอุตสาหกรรม (Sector-Specific Authorities) เพื่อทำหน้าที่รับรองเอนทิตีในแต่ละภาคส่วน โดยหน่วยงานเหล่านี้ต้องรับผิดชอบในกระบวนการพิสูจน์ตัวตน การตรวจสอบ และการให้การรับรองผู้ออกเอกสารรับรองเข้าระบบนิเวศของเอกสารรับรอง (VC ecosystem) เพื่อให้มั่นใจว่ามีการปฏิบัติตามข้อกำหนดด้านธรรมาภิบาลและความมั่นคงปลอดภัยก่อนให้สิทธิการเป็นผู้ออกเอกสารรับรอง

- หน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) ต้อง

เผยแพร่และปรับปรุงข้อกำหนดทางเทคนิค แบบข้อมูลของเอกสารรับรอง โพรโทคอล และข้อกำหนดด้านการทำงานร่วมกัน (interoperability) ทั้งหมดที่จำเป็น เพื่อให้เอนทิตีในระบบนิเวศของเอกสารรับรองสามารถปฏิบัติตามข้อกำหนดได้อย่างถูกต้อง

(3) กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF)

- VCTF-05 บทบาทหน้าที่ของหน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA)

(4) ตัวอย่างหลักฐานแสดง (evidence example)

- หลักฐานการปฏิบัติตามเกณฑ์การรับรอง (Accreditation compliance) แสดงเอกสารหลักฐานการปฏิบัติตามเกณฑ์การรับรองหน่วยงานภายในระบบนิเวศ เช่น ผู้ออกเอกสารรับรอง ผู้ให้บริการกระเป๋าดิจิทัล และผู้ตรวจสอบเอกสารสำแดง มีการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัย ความสามารถในการทำงานร่วมกัน และการคุ้มครองข้อมูลส่วนบุคคล ตามที่กำหนดไว้ในกรอบธรรมาภิบาลฯ

- ระบบทะเบียนข้อมูลที่เชื่อถือได้ (Always-on Trust Registry) แสดงรายงานความพร้อมใช้งานของระบบทะเบียนข้อมูลที่เชื่อถือได้ที่เปิดให้บริการต่อสาธารณะ พร้อมข้อมูลล่าสุดของผู้ออกเอกสารรับรอง ผู้ตรวจสอบเอกสารสำแดง และระบบทะเบียนข้อมูลที่เชื่อถือได้ (trust registry) ที่ได้รับการรับรอง รวมถึงดีไอดี (DID) ที่ลงทะเบียนและเมตาดาตาที่เกี่ยวข้อง

- กลไกการเพิกถอนที่มีประสิทธิภาพ (Revocation mechanism) แสดงรายงานกระบวนการเพิกถอนเอกสารรับรองและการอัปเดตสถานะในระบบทะเบียนข้อมูลที่เชื่อถือได้ที่ดำเนินการได้อย่างมีประสิทธิภาพและทันท่วงที

- การทบทวนธรรมาภิบาล (Governance Reviews) แสดงหลักฐานการทบทวนด้านธรรมาภิบาลและความเสี่ยงอย่างสม่ำเสมอ การเปิดรับฟังความคิดเห็นจากผู้มีส่วนได้ส่วนเสีย และการปรับปรุงเอกสารตามสถานการณ์ เช่น การเปลี่ยนแปลงด้านภัยคุกคาม ข้อกำหนดด้านกฎหมาย หรือความก้าวหน้าทางเทคโนโลยี

- การเผยแพร่และบริหารจัดการข้อกำหนดทางเทคนิค (Publication and Management of Technical Specifications) แสดงบันทึกการเผยแพร่ข้อกำหนดทางเทคนิค เช่น แบบข้อมูลเอกสารรับรอง โพรโทคอลการแลกเปลี่ยนเอกสารรับรอง ข้อกำหนดด้านการทำงานร่วมกัน ที่เผยแพร่ผ่านช่องทางที่เป็นทางการ พร้อมระบบจัดการเวอร์ชัน เช่น บันทึกการแก้ไข การอัปเดต การเลิกใช้ และการแจ้งเตือนการเปลี่ยนแปลงต่อหน่วยงานในระบบนิเวศของเอกสารรับรอง

5.3.5.2 บริการตรวจสอบดีไอดีของเอกสารรับรอง (VCGF-3.5.2)

(1) วัตถุประสงค์ของข้อกำหนด (assurance objective)

- หน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) **ควร** มีระบบตัวกลาง (broker-based) เพื่อรองรับการตรวจสอบความถูกต้องของเอกสารรับรองกับเอนทิตีต่าง ๆ

(2) ข้อเสนอแนะในการปฏิบัติตามข้อกำหนด (governance guidance)

- หน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) ควรพัฒนาและดูแล API สำหรับระบบตัวกลางที่เชื่อถือได้ (trust broker API) เพื่อรองรับการตรวจสอบเอกสารรับรองที่ครอบคลุมหลายดีไอดีเมธอด (DID method)

- API สำหรับระบบตัวกลางที่เชื่อถือได้ต้องเชื่อมโยงกับระบบทะเบียนเอกสารรับรอง (VDR) และเครือข่ายดีไอดี (DID Networks) เพื่อยืนยันความถูกต้องและสถานะของเอกสารรับรอง

- API สำหรับระบบตัวกลางที่เชื่อถือได้ควรมีฟังก์ชันให้ผู้ตรวจสอบเอกสารสำแดงตรวจสอบสถานะของเอกสารรับรอง ข้อมูลการเพิกถอน ความน่าเชื่อถือของผู้ออกเอกสารรับรอง และความสอดคล้องกับระดับการรับรอง (Assurance Level) ที่กำหนด

(3) กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF)

-

(4) ตัวอย่างหลักฐานแสดง (evidence example)

- เอกสารทางเทคนิคของ API สำหรับระบบตัวกลางที่เชื่อถือได้ (Trust Broker API Documentation) แสดงเอกสารทางเทคนิคของ API สำหรับระบบตัวกลางที่เชื่อถือได้ Trust Broker API ที่อธิบายข้อกำหนด รูปแบบ แนวทางการเชื่อมต่อ และรูปแบบเอกสารรับรองที่รองรับ ตัวอย่างหนึ่งของ API สำหรับระบบตัวกลางที่เชื่อถือได้ ได้แก่ DIF Universal Resolver ซึ่งสนับสนุนการทำงานร่วมกันของหลายดีไอดีเมธอด (DID method)

- หลักฐานการใช้งาน (Implementation Evidence) แสดงกรณีศึกษา (use cases) หรือบันทึกการใช้งานที่แสดงให้เห็นว่า API สำหรับระบบตัวกลางที่เชื่อถือได้รับการนำไปใช้จริงโดยผู้ออกเอกสารรับรอง ผู้ให้บริการกระเป๋าดิจิทัล และผู้ตรวจสอบเอกสารสำแดง

5.4 ข้อกำหนดเกี่ยวกับแอพพลิเคชัน (VCGF-4 trust applications)

5.4.1 การพิสูจน์ยืนยันตัวตนของผู้ถือเอกสารรับรอง (Holder Onboarding and Digital Identity Assurance) (VCGF-4.1)

- ข้อกำหนด VCGF 4.1 เป็นข้อกำหนดเชิงเทคนิคที่เกี่ยวข้องกับการพิสูจน์ยืนยันตัวตนของผู้ถือเอกสารรับรองเพื่อรับประกันความน่าเชื่อถือของดีไอดีของผู้ถือเอกสารรับรอง

5.4.1.1 ข้อกำหนดการพิสูจน์ยืนยันตัวตนของผู้ถือเอกสารรับรอง (VCGF-4.1.1)

(1) วัตถุประสงค์ของข้อกำหนด (assurance objective)

- ผู้ให้บริการกระเป๋าดิจิทัล **ต้อง** มีกระบวนการพิสูจน์และยืนยันตัวตนของผู้ถือเอกสารรับรอง (holder) ที่มีความมั่นคงปลอดภัย เข้มงวด และเป็นไปตามมาตรฐานที่เกี่ยวข้องก่อนเริ่มใช้งานกระเป๋าดิจิทัล โดยกระบวนการดังกล่าว **ต้อง** สอดคล้องกับกรอบการพิสูจน์และยืนยันตัวตนดิจิทัลของ สพธอ. (ETDA Digital ID Framework) หรือมาตรฐานด้านการพิสูจน์ตัวตนอื่นที่เทียบเท่าที่กำหนดไว้

(2) ข้อเสนอแนะในการปฏิบัติตามข้อกำหนด (governance guidance)

- ผู้ให้บริการกระเป๋าดิจิทัล **ต้อง** ดำเนินการพิสูจน์ตัวตนของผู้ใช้งานกระเป๋าดิจิทัล (ผู้ถือเอกสารรับรอง) ตามเกณฑ์ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL) ที่กำหนดไว้ในกรอบการพิสูจน์และยืนยันตัวตนดิจิทัลของ สพธอ. หรือเกณฑ์ที่กำหนดโดยหน่วยงานกำกับดูแลเฉพาะอุตสาหกรรม

(3) กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF)

- VCTF-07 ระดับความเข้มงวดของการพิสูจน์และยืนยันตัวตนดิจิทัล

(4) ตัวอย่างหลักฐานแสดง (evidence example)

- ระดับความเข้มงวดการพิสูจน์ยืนยันตัวตนที่กำหนดไว้อย่างชัดเจน (Defined Levels of Identity Assurance) แสดงเอกสารที่กำหนดระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL) และระดับความน่าเชื่อถือของการยืนยันตัวตน (AAL) ที่กำหนดโดยหน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) หรือหน่วยงานกำกับเฉพาะอุตสาหกรรม โดยเกณฑ์การรับรองดังกล่าว ต้อง มีความสอดคล้องกับ หรือระดับความเข้มงวดการพิสูจน์และยืนยันตัวตน ที่กำหนดไว้ในกรอบการพิสูจน์และยืนยันตัวตนดิจิทัลของ สพธอ. เพื่อให้มั่นใจว่ามีการยืนยันตัวตนที่รัดกุม และสามารถใช้กลไกการยืนยันตัวตนที่มั่นคงปลอดภัยในระบบนิเวศของเอกสารรับรอง (VC ecosystem)

5.4.2 การคุ้มครองข้อมูลในข้อมูลรับรอง (Protection of accuracy data) (VCGF-4.2)

- ข้อกำหนด VCGF 4.2 เป็นข้อกำหนดเชิงเทคนิคที่เกี่ยวข้องกับความถูกต้องของข้อมูลรับรองและการคุ้มครองข้อมูลส่วนบุคคลในข้อมูลรับรอง

5.4.2.1 การคุ้มครองข้อมูลส่วนบุคคลของเอนทิตีในระบบนิเวศของเอกสารรับรอง (VCGF-4.2.1)

(1) วัตถุประสงค์ของข้อกำหนด (assurance objective)

- เอนทิตีในระบบนิเวศของเอกสารรับรอง (VC ecosystem) **ต้อง** ปฏิบัติตามข้อกำหนดและกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องทั้งหมด

(2) ข้อเสนอแนะในการปฏิบัติตามข้อกำหนด (governance guidance)

- ผู้ออกเอกสารรับรอง เหมือนกับ VCGF 3.2.3

- ผู้ตรวจสอบเอกสารสำแดง เหมือนกัน VCGF 3.3.2

- ผู้ให้บริการดิจิทัลกระเป๋าดิจิทัล เหมือนกัน VCGF 3.4.3

- หน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) ต้องกำหนดให้รูปแบบของเอกสารรับรองที่รองรับกระบวนการเข้ารหัสลับที่สามารถดำเนินการเปิดเผยข้อมูลแบบเลือกได้ (selective disclosure) โดยเปิดให้ผู้ถือเอกสารรับรองสามารถแสดงเฉพาะคุณลักษณะที่จำเป็น โดยไม่ต้องเปิดเผยข้อมูลทั้งหมดในเอกสารรับรอง ทั้งนี้ ต้องสอดคล้องตามข้อกำหนด VCGF-3.1.5

(3) กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF)

- กฎหมายและข้อกำหนดคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องทั้งหมด

(4) ตัวอย่างหลักฐานแสดง (evidence example)

-

5.4.3 การสร้างความน่าเชื่อถือกับระบบนิเวศของเอกสารรับรอง (Ecosystem technical trust) (VCGF-4.3)

- ข้อกำหนด VCGF 4.3 เป็นข้อกำหนดเชิงเทคนิคเพื่อสร้างความน่าเชื่อถือกับระบบนิเวศของเอกสารรับรองโดยหน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA)

5.4.3.1 มาตรฐานด้านเทคนิคและชุดการทดสอบความสอดคล้องทางเทคนิค (VCGF-4.3.1)

(1) วัตถุประสงค์ของข้อกำหนด (assurance objective)

- หน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) **ต้อง** กำหนดมาตรฐานด้านเทคนิคที่ครอบคลุม และจัดทำชุดทดสอบที่เป็นมาตรฐาน (standardized test suites) เพื่อให้เอนทิตีในระบบนิเวศของเอกสารรับรองสามารถประเมินความสอดคล้องทางเทคนิคและความสามารถในการทำงานร่วมกันได้ (interoperability) อย่างมีประสิทธิภาพ

(2) ข้อเสนอแนะในการปฏิบัติตามข้อกำหนด (governance guidance)

- เหมือนกันข้อเสนอแนะในการปฏิบัติตามข้อกำหนด 6 ของ VCGF 3.5 หน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) ต้องรับผิดชอบในการเผยแพร่และปรับปรุงข้อกำหนดทางเทคนิค แบบข้อมูลของเอกสารรับรอง โพรโทคอล และข้อกำหนดด้านการทำงานร่วมกันได้ (interoperability) ที่จำเป็น เพื่อให้เอนทิตีในระบบนิเวศของเอกสารรับรองสามารถปฏิบัติตามข้อกำหนดได้อย่างถูกต้อง

- หน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) ต้องพัฒนา เผยแพร่ และดูแลชุดทดสอบมาตรฐาน (standardized test suites) ที่มีชุดทดสอบที่เป็นมาตรฐาน (standardized test cases) สคริปต์ทดสอบ (test scripts) และสถานการณ์จำลองไว้อย่างชัดเจน เพื่อให้ผู้ออกเอกสารรับรอง ผู้ให้บริการกระเป๋าดิจิทัล ผู้ตรวจสอบเอกสารสำแดง และผู้ให้บริการระบบทะเบียนเอกสารรับรอง (VDR provider) สามารถนำไปใช้ทดสอบความสอดคล้องทางเทคนิคและความสามารถในการทำงานร่วมกันได้ (interoperability) อย่างมีประสิทธิภาพ

(3) กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF)

- VCTF-05 บทบาทหน้าที่ของหน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA)

(4) ตัวอย่างหลักฐานแสดง (evidence example)

- การเผยแพร่และจัดการข้อกำหนดทางเทคนิค (Publication and Management of Technical Specifications) แสดงการเผยแพร่ข้อกำหนดกรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF) และข้อกำหนดของแบบข้อมูลที่ใช้ในระบบนิเวศของเอกสารรับรอง เช่น โครงสร้างข้อมูลของ credential data โพรโทคอลการแลกเปลี่ยนเอกสารรับรอง รูปแบบข้อมูล ที่สามารถเข้าถึงได้ผ่านช่องทางอย่างเป็นทางการที่หน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) ดูแล พร้อมระบบจัดการเวอร์ชัน เช่น บันทึกการแก้ไข การอัปเดต การเลิกใช้ และการแจ้งเตือนการเปลี่ยนแปลง

- ชุดทดสอบมาตรฐานที่เป็นมาตรฐาน (Standardized Test Suites) แสดงชุดทดสอบที่เป็นมาตรฐาน (standardized test cases)ที่เผยแพร่โดยหน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) ซึ่งรวมถึงกรณีทดสอบ สคริปต์ และสิ่งแวดล้อมสำหรับการทดสอบ และแสดงเอกสารผลการทดสอบที่แสดงว่าหน่วยงานในระบบนิเวศของเอกสารรับรองได้ผ่านการทดสอบการทำงานและความสามารถในการทำงานร่วมกันได้ ในกระบวนการรับรองเอนทิตี

5.4.4 การกำกับและรับรองความน่าเชื่อถือกับเอนทิตีในระบบนิเวศของเอกสารรับรอง (Trust Assurance & Certification Governance) (VCGF-4.4)

- ข้อกำหนด VCGF 4.4 เป็นข้อเสนอแนะในเชิงกระบวนการรับรองเพื่อสร้างความน่าเชื่อถือกับเอนทิตีของระบบนิเวศของเอกสารรับรองโดยหน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA)

5.4.4.1 การรับรองผู้ให้บริการและเอนทิตีที่เชื่อถือได้ (VCGF-4.4.1)

(1) วัตถุประสงค์ของข้อกำหนด (assurance objective)

- หน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) **ต้อง** จัดให้มีกรอบการรับรอง (certification framework) ที่มีโครงสร้างชัดเจน โดยกำหนดระดับความน่าเชื่อถือ (LoA) เพื่อประเมินและรับรองความน่าเชื่อถือ ความมั่นคงปลอดภัย และการปฏิบัติตามข้อกำหนดของผู้เข้าร่วมในระบบนิเวศเอกสารรับรอง (VC ecosystem) ให้สอดคล้องกับกรอบธรรมาภิบาลและข้อกำหนดทางเทคนิค

(2) ข้อเสนอแนะในการปฏิบัติตามข้อกำหนด (governance guidance)

- หน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) ต้องกำหนดข้อปฏิบัติในการรับรองและการให้การรับรอง (certification & accreditation) สำหรับการพิจารณาเอนทิตีในการเข้าร่วมระบบนิเวศของเอกสารรับรอง (VC ecosystem) เช่น ผู้ออกเอกสารรับรอง ผู้ให้บริการกระเป๋าดิจิทัล และ ผู้ตรวจสอบเอกสารสำแดง อย่างชัดเจน

- แนวทางการรับรอง ต้องระบุเกณฑ์ขั้นต่ำที่ต้องปฏิบัติตาม เช่น มาตรฐานที่เกี่ยวข้อง แนวปฏิบัติด้านความมั่นคงปลอดภัย ขั้นตอนการดำเนินงาน และระดับความเข้มงวดการพิสูจน์ตัวตน เป็นต้น

- การตรวจประเมิน (audit) กับเอนทิตีต้องปฏิบัติตามรอบระยะเวลาที่กำหนดโดยหน่วยงานตรวจประเมินอิสระ (independent assessment bodies) ที่ได้รับการรับรอง เพื่อให้การประเมินความสอดคล้องกับกรอบธรรมาภิบาลและข้อกำหนดทางเทคนิค

- หน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) ต้องจัดให้มีเครื่องหมายแสดงความน่าเชื่อถือ (trustmark) สำหรับเอนทิตีที่ได้รับการรับรอง ซึ่งสามารถแสดงบนแพลตฟอร์มและบริการของตน เพื่อเพิ่มความน่าเชื่อถือและความมั่นใจแก่ผู้ใช้งานในระบบเอกสารรับรอง(VC ecosystem)

(3) กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF)

- VCTF-05 บทบาทหน้าที่ของหน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA)

(4) ตัวอย่างหลักฐานแสดง (evidence example)

- เอกสารการรับรองและการให้การรับรอง (Certification and Accreditation Documentation) แสดงรูปแบบของเอกสารทางการ เช่น หนังสือรับรอง รายงานการประเมิน หรือข้อตกลงสัญญาที่แสดงถึงการปฏิบัติตามข้อกำหนด และระดับความน่าเชื่อถือ (LoA) ที่เอนทิตีได้รับ

- เอกสารแสดงกระบวนการต่ออายุและการรักษาสถานะการรับรอง (Certification Renewal and Maintenance Records) แสดงหลักฐานว่ามีการดำเนินการทบทวนและรับรองซ้ำอย่างต่อเนื่อง เช่น ผลการตรวจสอบประจำปี เอกสารประเมินตามรอบ หรือรายงานการประเมินอัปเดต

- การบริหารจัดการระบบทะเบียนข้อมูลที่เชื่อถือได้ (Trust Registry Governance) หน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) แสดงว่ามีระบบทะเบียนข้อมูลที่เชื่อถือได้ (trust registry) ที่เปิดเผยต่อสาธารณะ พร้อมแสดงข้อมูลของเอนทิตีที่ได้รับการรับรองดีไอดี (DID) ระดับความน่าเชื่อถือ (LoA) และสถานะการรับรอง

- รายงานการตรวจสอบโดยหน่วยงานอิสระ (Independent Audit Reports) แสดงรายงานการตรวจสอบโดยผู้ตรวจประเมินอิสระที่ได้รับการรับรอง และแสดงผลการประเมินความสอดคล้องของเอนทิตีกับข้อกำหนดการรับรอง

- การแสดงเครื่องหมายแสดงความเชื่อถือ (Trustmark Display and Transparency Record) แสดงบันทึกการเผยแพร่ข้อมูลเอนทิตีที่ผ่านการรับรองเครื่องหมายแสดงความน่าเชื่อถือ (trustmark) ผ่านช่องทางสาธารณะ โดยเครื่องหมายแสดงความเชื่อถือ (trustmark) ต้อง ประกอบด้วยรหัสเฉพาะ หรือกลไกการตรวจสอบ เช่น QR code หรือลายมือชื่อดิจิทัล ที่สามารถเชื่อมโยงไปยังเอกสารรับรองในระบบทะเบียนข้อมูลที่เชื่อถือได้ (trust registry) ได้

5.4.4.2 การประเมินความเสี่ยงและการปรับปรุงกรอบแนวทางการสร้างระบบนิเวศที่เชื่อถือได้ (VCGF-4.4.2)

(1) วัตถุประสงค์ของข้อกำหนด (assurance objective)

- หน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) **ต้อง** จัดให้มีกระบวนการประเมินความเสี่ยง (risk assessment) และการปรับปรุงกรอบแนวทางการสร้างระบบนิเวศที่เชื่อถือได้ (Trust Model Framework) อย่างเป็นระบบและสม่ำเสมอ

(2) ข้อเสนอแนะในการปฏิบัติตามข้อกำหนด (governance guidance)

- หน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) ต้องดำเนินการทบทวนความเสี่ยงอย่างสม่ำเสมอ และปรับปรุงกรอบเทคนิคสำหรับระบบเอกสารรับรองที่

เชื่อถือได้ (VCTF) ตามความเหมาะสม โดยต้องคำนึงถึงการเปลี่ยนแปลงของเทคโนโลยี ภัยคุกคามด้านความมั่นคงปลอดภัย และความเสี่ยงจากการฉ้อโกง เพื่อรักษาความน่าเชื่อถือในระบบนิเวศเอกสารรับรอง (VC ecosystem)

- การประเมินความเสี่ยง (risk assessment) ต้องครอบคลุมการประเมินเอนทิตีที่เกี่ยวข้องทั้งหมดภายในระบบนิเวศของเอกสารรับรอง (VC ecosystem) ได้แก่ ผู้ออกเอกสารรับรอง ผู้ให้บริการกระเป๋าดิจิทัล ผู้ตรวจสอบเอกสารสำแดง และผู้ให้บริการระบบทะเบียนเอกสารรับรอง เพื่อระบุจุดอ่อนที่อาจเกิดขึ้น และประเมินความสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัย การคุ้มครองข้อมูลส่วนบุคคล และข้อกำหนดต่าง ๆ

(3) กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF)

- VCTF-09 การประเมินความเสี่ยงสำหรับระบบนิเวศของเอกสารรับรอง

(4) ตัวอย่างหลักฐานแสดง (evidence example)

- รายงานการประเมินความเสี่ยงของหน่วยงานในระบบนิเวศ (Risk Assessment Reports for Ecosystem Participants) แสดงรายงานการประเมินความเสี่ยงที่ครอบคลุมผู้ออกเอกสารรับรอง ผู้ให้บริการกระเป๋าดิจิทัล ผู้ตรวจสอบเอกสารสำแดง และผู้ให้บริการระบบทะเบียนเอกสารรับรอง รายงานจะต้องแสดงรายการความเสี่ยง จุดอ่อนที่ตรวจพบ และแนวทางการจัดการความเสี่ยงอย่างชัดเจน โดยมีเป้าหมายหลักเพื่อประเมินภัยคุกคามด้านความมั่นคงปลอดภัยและการฉ้อโกงภายในระบบนิเวศของเอกสารรับรอง

- บันทึกการปรับปรุงกรอบเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VC Trust Model Framework) แสดงเอกสารอย่างเป็นทางการที่ระบุถึงการปรับปรุงกรอบแนวทางการสร้างระบบนิเวศที่เชื่อถือได้ (VC Trust Model Framework) โดยอิงตามผลการทบทวนความเสี่ยง รายงานการประเมินความมั่นคงปลอดภัย หรือข้อค้นพบเกี่ยวกับความก้าวหน้าทางเทคโนโลยีหรือภัยคุกคามใหม่

- บันทึกการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย (Incident Response and Handling Records) แสดงรายงานหรือหลักฐานการดำเนินการตอบสนองหรือการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย ภัยคุกคาม หรือเหตุการณ์ฉ้อโกง

- บันทึกการปรึกษาหารือกับผู้มีส่วนเกี่ยวข้อง (Stakeholder Risk Reviews and Consultation Records) แสดงรายงานการประชุม รายงานความคิดเห็นจากผู้มีส่วนเกี่ยวข้อง หรือข้อเสนอแนะจากคณะที่ปรึกษา ที่แสดงให้เห็นว่ามีการหารือร่วมกับหน่วยงานในระบบนิเวศของเอกสารรับรองอย่างต่อเนื่อง เพื่อทบทวนแนวโน้มความเสี่ยง ความกังวลด้านความมั่นคงปลอดภัย และแนวทางการปรับปรุงกรอบแนวทางการสร้างระบบนิเวศที่เชื่อถือได้ (VC Trust Model Framework)

5.4.5 ความรับผิดและการระงับข้อพิพาท (Liability & dispute resolution) (VCGF-4.5)

ข้อกำหนด VCGF 4.5 เป็นข้อเสนอแนะในเชิงกระบวนวางกรอบแนวทางความรับผิดชอบในบริการของผู้ให้บริการและเอนทิตีของระบบนิเวศของเอกสารรับรอง (VC ecosystem) และกลไกการระงับข้อพิพาทที่เกิดขึ้นโดยหน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA)

5.4.5.1 ความรับผิดชอบและแนวทางการระงับข้อพิพาทในกรณีใช้เอกสารรับรองโดยมิชอบ (VCGF-4.5.1)

(1) วัตถุประสงค์ของข้อกำหนด (assurance objective)

- หน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) **ต้อง** กำหนดกรอบความรับผิดชอบ (Liability Framework) ที่มีโครงสร้างชัดเจน เพื่อรองรับกรณีการใช้เอกสารรับรองโดยมิชอบ การฉ้อโกง และข้อพิพาทที่เกี่ยวข้อง โดยต้องกำหนดบทบาทและความรับผิดชอบของผู้มีส่วนร่วมทุกฝ่ายในระบบนิเวศเอกสารรับรองไว้อย่างชัดเจน

(2) ข้อเสนอแนะในการปฏิบัติตามข้อกำหนด (governance guidance)

- หน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) ต้องจัดทำและดำเนินการตามกรอบความรับผิดชอบที่ชัดเจน ซึ่งกำหนดหน้าที่ ความรับผิดชอบ มาตรการความรับผิด และภาระผูกพันทางกฎหมายของผู้ออกเอกสารรับรอง ผู้ให้บริการกระเป๋าดิจิทัล ผู้ตรวจสอบเอกสารสำแดง และผู้ให้บริการระบบทะเบียนเอกสารรับรอง ในกรณีที่เกิดการใช้เอกสารรับรองโดยมิชอบ การฉ้อโกง เอกสารถูกดัดแปลง หรือการทำธุรกรรมโดยไม่ได้รับอนุญาต

- หน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) ต้องจัดให้มีกลไกการระงับข้อพิพาทอย่างเป็นทางการ เพื่อใช้ในการจัดการกรณีที่เกี่ยวข้องกับการฉ้อโกง การแอบอ้างตัวตน ความล้มเหลวในการตรวจสอบความน่าเชื่อถือของเอนทิตี หรือการใช้งานเอกสารรับรองโดยไม่ได้รับอนุญาต เป็นต้น

- หน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) ต้องประสานกับหน่วยงานกำกับดูแลเฉพาะอุตสาหกรรม เพื่อจัดทำแนวทางความรับผิดที่เหมาะสมกับกรณีการใช้งานตามแต่ละอุตสาหกรรม เช่น ภาคการเงิน ภาคสาธารณสุข การศึกษา หรือการปฏิบัติราชการ

(3) กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF)

- กรอบความรับผิด (Liability Framework) และกลไกการระงับข้อพิพาท (Dispute Resolution Mechanism) สามารถกำหนดเป็นส่วนหนึ่งของ VCTF-05 บทบาทหน้าที่ของหน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA)

(4) ตัวอย่างหลักฐานแสดง (evidence example)

- กรอบความรับผิด (Liability Framework) เผยแพร่เอกสารกรอบความรับผิดชอบ ซึ่งอธิบายรายละเอียดเกี่ยวกับอำนาจ หน้าที่และความรับผิดชอบ การลงโทษ และแนวทางการลดความเสี่ยงในกรณีที่เกิดการฉ้อโกง การนำข้อมูลรับรองไปใช้ในทางที่ผิด หรือการเข้าถึงโดยไม่ได้รับอนุญาต

- กลไกการระงับข้อพิพาท (Dispute Resolution Mechanisms) เผยแพร่เอกสารที่กำหนดขั้นตอนการระงับข้อพิพาท ช่องทางการยกระดับข้อพิพาท (escalation flow) และระยะเวลาที่ใช้ในการดำเนินการสำหรับข้อพิพาทที่เกี่ยวข้องกับข้อมูลรับรอง (credential)

- การกำหนดความรับผิดเฉพาะกลุ่มอุตสาหกรรม (Sector-Specific Liability Designation) เผยแพร่แนวทางหรือข้อตกลงซึ่งเห็นชอบร่วมกับหน่วยงานกำกับดูแล โดยมีวัตถุประสงค์เพื่อกำหนดกรอบความรับผิดที่เหมาะสมเฉพาะที่นำเอกสารรับรองไปใช้งานในแต่ละกลุ่มอุตสาหกรรม

6. กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (Verifiable Credential Trust Framework: VCTF)

กรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF) มีบทบาทในการกำหนดมาตรฐานและแนวปฏิบัติทางเทคนิคที่เกี่ยวข้องกับระบบ VC/VP เช่น การออกแบบสถาปัตยกรรมระบบ การกำหนดมาตรการการรักษาความมั่นคงปลอดภัยของระบบ มาตรฐานเทคนิค และโพรโทคอลการแลกเปลี่ยนข้อมูลต่าง ๆ ทั้งนี้ รวมถึง กรอบการบริหารจัดการความเสี่ยงที่ส่งผลโดยตรงต่อความน่าเชื่อถือของระบบนิเวศของเอกสารรับรอง (VC ecosystem) หน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) ควรจัดทำและเผยแพร่เอกสารข้อกำหนดในเชิงเทคนิคที่สำคัญสำหรับบระนิเวศของเอกสารรับรอง (VC ecosystem) อย่างน้อย ประกอบด้วย

- **ข้อกำหนดด้านความมั่นคงปลอดภัยของโครงสร้างพื้นฐานไอทีสำหรับระบบนิเวศของเอกสารรับรอง** มีเนื้อหาเป็นข้อกำหนดพื้นฐานด้านความมั่นคงปลอดภัยของโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ (IT Infrastructure) ตามแนวทางมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ ตามวัตถุประสงค์ของ VCGF-1.1.1 การบริหารจัดการความมั่นคงปลอดภัยของผู้ออกเอกสารรับรอง VCGF-1.1.2 การบริหารจัดการความมั่นคงปลอดภัยของผู้ให้บริการกระเป๋าดิจิทัล VCGF-1.1.3 การบริหารจัดการความมั่นคงปลอดภัยของผู้ตรวจสอบเอกสารสำแดง และ VCGF-1.3.1 ความมั่นคงปลอดภัยของระบบทะเบียนเอกสารรับรอง (VDR)
- **ดีไอดีเมธอดสำหรับระบบนิเวศของเอกสารรับรอง** ระบุวิธีการจัดการดีไอดี (Decentralized Identifier: DID Method) สำหรับผู้เกี่ยวข้องในบริบทต่าง ๆ ของระบบนิเวศของเอกสารรับรอง (VC ecosystem) เช่น ดีไอดีบุคคลธรรมดาและดีไอดีนิติบุคคลในระบบนิเวศของเอกสารรับรอง (VC ecosystem) ตามวัตถุประสงค์ของ VCGF-3.2.1 คุณสมบัติของผู้ออกเอกสารรับรองที่เชื่อถือได้ VCGF-3.3.1 คุณสมบัติของผู้ตรวจสอบเอกสารสำแดงที่เชื่อถือได้ และ VCGF-3.4.1 คุณสมบัติของผู้ให้บริการกระเป๋าดิจิทัลที่เชื่อถือได้
- **โพรโทคอลการแลกเปลี่ยนเอกสารรับรอง** กำหนดโพรโทคอลทางเทคนิคสำหรับการออก (issuance) การแสดง (presentation) และการตรวจสอบยืนยัน (verification) เอกสารรับรองและเอกสารสำแดงภายในระบบนิเวศของเอกสารรับรอง (VC ecosystem) ตามวัตถุประสงค์ของ VCGF-2.1.1โพรโทคอลออกเอกสารรับรอง และ VCGF-2.2.1 โพรโทคอลออกเอกสารรับรอง
- **แบบข้อมูลและโครงสร้างข้อมูลของเอกสารรับรองและข้อความยืนยัน** ระบุโครงสร้าง โมเดลข้อมูล และแบบข้อมูล (schemas) สำหรับเอกสารรับรองและเอกสารสำแดงที่ใช้ภายในระบบนิเวศเอกสารรับรอง ตามวัตถุประสงค์ของ VCGF-3.1.1 แบบข้อมูลสำหรับเอกสารรับรองและเอกสารสำแดง และ VCGF-3.1.2 โครงสร้างข้อมูลข้อมูลรับรอง

- **บทบาทหน้าที่ของหน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA)** กำหนดหน้าที่ โครงสร้างการดำเนินงาน และกลไกการกำกับดูแลความสอดคล้องของหน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) ตามวัตถุประสงค์ของ VCGF-3.5.1 การกำกับของหน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) และ VCGF-4.4.1 การรับรองผู้ให้บริการและเอนทิตีที่เชื่อถือได้
- **อัลกอริทึมการเข้ารหัสลับและลายมือชื่อดิจิทัล (Digital Signature Algorithm)** กำหนดรายการอัลกอริทึมการเข้ารหัสลับและลายมือชื่อดิจิทัลที่หน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) เห็นชอบให้ใช้งานในระบบนิเวศของเอกสารรับรอง (VC ecosystem) ตามวัตถุประสงค์ของ VCGF-1.3.2 ข้อกำหนดลายมือชื่อดิจิทัลและอัลกอริทึมเข้ารหัสลับสำหรับเอกสารรับรอง
- **ระดับความน่าเชื่อถือของตัวตนดิจิทัล** กำหนดระดับความน่าเชื่อถือของตัวตนดิจิทัล (identity assurance level: IAL และ authentication assurance level: AAL) สำหรับการพิสูจน์และยืนยันบุคคลของเอนติทีต่าง ๆ ในระบบนิเวศของเอกสารรับรอง (VC ecosystem) ตามวัตถุประสงค์ของ VCGF-4.1.1 ข้อกำหนดการพิสูจน์ยืนยันตัวตนของผู้ถือเอกสารรับรอง
- **การจัดการความมั่นคงปลอดภัยของกุญแจเข้ารหัสและการจัดเก็บเอกสารรับรองสำหรับระบบกระเป๋าดิจิทัล** กำหนดข้อกำหนดทางเทคนิคและความมั่นคงปลอดภัยสำหรับการสร้างกุญแจเข้ารหัส การจัดเก็บกุญแจเข้ารหัสอย่างปลอดภัย และการปกป้องเอกสารรับรองในระบบกระเป๋าดิจิทัล (digital wallet) ตามวัตถุประสงค์ของ VCGF-3.4.2 ข้อกำหนดการยืนยันตัวตนและความมั่นคงปลอดภัยของกระเป๋าดิจิทัล โดยมีกรอบเนื้อหาตาม
- **การประเมินความเสี่ยงสำหรับระบบนิเวศของเอกสารรับรอง** กำหนดแนวทางมาตรฐานในการประเมินความเสี่ยงสำหรับหน่วยงานที่เข้าร่วมในระบบนิเวศของเอกสารรับรอง (VC ecosystem) เพื่อทบทวนระดับความมั่นคงปลอดภัยของเอนทิตีต่าง ๆ ในการรักษาความมั่นคงปลอดภัยให้กับข้อมูลสำคัญในระบบนิเวศของเอกสารรับรอง (VC ecosystem) ตามวัตถุประสงค์ของ VCGF-4.4.2 การประเมินความเสี่ยงและการปรับปรุงกรอบแนวทางการสร้างระบบนิเวศที่เชื่อถือได้ โดยมีกรอบเนื้อหาตาม

ทั้งนี้ สพธอ. ได้จัดทำตัวอย่างของชุดเอกสารกรอบด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF) สำหรับระบบนิเวศของเอกสารรับรอง (VC ecosystem) เพื่อใช้เป็นต้นแบบและกำหนดกรอบเนื้อหาข้อกำหนดทางเทคนิคดังแสดงในตารางที่ 2

ตารางที่ 2 ตัวอย่างเอกสารข้อกำหนดด้านเทคนิคสำหรับระบบเอกสารรับรองที่เชื่อถือได้ (VCTF)

ข้อกำหนดในเชิงเทคนิค	ชื่อเอกสาร/ กรอบเนื้อหา
ข้อกำหนดด้านความมั่นคงปลอดภัยของโครงสร้างพื้นฐานไอทีสำหรับระบบนิเวศของเอกสารรับรอง	VCTF-01 Security Requirements for IT Infrastructure in the Thai VC ecosystem/ หัวข้อ 1.1
ดีไอดีเมธอดสำหรับระบบนิเวศของเอกสารรับรอง	VCTF-02 DID Method Specification for Thai VC ecosystem/ หัวข้อ 1.16.2
โพรโทคอลการแลกเปลี่ยนเอกสารรับรอง	VCTF-03 Verifiable Credential Exchange Protocols/ หัวข้อ 6.3
แบบข้อมูลและโครงสร้างข้อมูลของเอกสารรับรองและข้อความยืนยัน	VCTF-04 Verifiable Credential and Claim Data Model & Schemas/ หัวข้อ 6.4
บทบาทหน้าที่ของหน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA)	VCTF-05 VC Governance Authority Responsibilities / หัวข้อ 7.5
อัลกอริทึมการเข้ารหัสลับและลายมือชื่อดิจิทัล	VCTF-06 Approval of Cryptographic and Digital Signature Algorithms / หัวข้อ 6.6
ระดับความเข้มงวดของการพิสูจน์และยืนยันตัวตนดิจิทัล	VCTF-07 Digital ID Assurance Level Requirements for VC Use Cases/ หัวข้อ 6.7
การจัดการความมั่นคงปลอดภัยของกุญแจเข้ารหัสและการจัดเก็บเอกสารรับรองสำหรับระบบกระเป๋าดิจิทัล	VCTF-08 Specification for Secure Key Management and Credential Storage in Digital Wallet Systems/ หัวข้อ 6.86.9
การประเมินความเสี่ยงสำหรับระบบนิเวศของเอกสารรับรอง	VCTF-09 VC Risk Assessment Guideline for the Thai VC Ecosystem/ หัวข้อ 7.9

6.1 VCGF-01 ข้อกำหนดด้านความมั่นคงปลอดภัยของโครงสร้างพื้นฐานไอทีสำหรับระบบนิเวศของเอกสารรับรอง

VCTF-01 Security Requirements for IT Infrastructure in the Thai VC ecosystem กำหนดข้อกำหนดความมั่นคงปลอดภัยพื้นฐาน (baseline security requirements) สำหรับระบบและบริการที่ดำเนินการโดยผู้ให้บริการและเอนทิตีทุกประเภทภายในระบบนิเวศของเอกสารรับรอง (VC ecosystem) มีเนื้อหาเป็นข้อกำหนดพื้นฐานด้านความมั่นคงปลอดภัยของโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ (IT infrastructure) ตามแนวทางมาตรฐานที่สอดคล้องกับข้อเสนอแนะมาตรฐาน ขมธอ. 21-2562 [18] (ระดับมาตรฐานอุตสาหกรรม) และ ขมธอ. 35-2567 [19] แบ่งออกเป็น 10 หมวดสำคัญ ดังนี้

- VCSec 1 นโยบายความมั่นคงสารสนเทศ กำหนดให้ผู้ให้บริการและเอนทิตีต้องจัดทำนโยบายความมั่นคงสารสนเทศที่ชัดเจน ครอบคลุมสินทรัพย์และกระบวนการสำคัญ และต้องมีการทบทวนและปรับปรุงนโยบายอย่างสม่ำเสมอเมื่อมีการเปลี่ยนแปลงหรือเกิดเหตุการณ์สำคัญ
- VCSec 2 โครงสร้างบทบาทและความรับผิดชอบด้านความมั่นคง กำหนดให้ผู้ให้บริการและเอนทิตีต้องแต่งตั้งบุคลากรที่รับผิดชอบด้านความมั่นคงโดยเฉพาะ กำหนดบทบาทหน้าที่อย่างชัดเจน และมีการทบทวนปรับปรุงโครงสร้างความรับผิดชอบเมื่อเกิดการเปลี่ยนแปลงที่สำคัญ
- VCSec 3 การจัดการและควบคุมสินทรัพย์ กำหนดให้ผู้ให้บริการและเอนทิตีต้องมีการบันทึกรายการสินทรัพย์สำคัญของระบบ มีการกำหนดเจ้าของสินทรัพย์ และมีมาตรการควบคุมการกำหนดค่าพื้นฐาน (baseline configuration) เพื่อรักษาความมั่นคงปลอดภัยของระบบ
- VCSec 4 ความมั่นคงปลอดภัยของบุคลากร กำหนดให้ผู้ให้บริการและเอนทิตีดำเนินการตรวจสอบประวัติบุคลากรที่มีบทบาทสำคัญก่อนการจ้างงาน และจัดทำกระบวนการรองรับการเปลี่ยนแปลงหน้าที่ หรือการสิ้นสุดการทำงาน เพื่อควบคุมสิทธิ์การเข้าถึงและสินทรัพย์ขององค์กรอย่างเหมาะสม
- VCSec 5 ความมั่นคงทางกายภาพและสิ่งแวดล้อม กำหนดให้ผู้ให้บริการและเอนทิตีต้องมีมาตรการควบคุมการเข้าถึงพื้นที่สำคัญ เช่น ศูนย์ข้อมูล พร้อมระบบเตือนภัย
- VCSec 6 การบริหารจัดการการสื่อสารและการดำเนินงาน กำหนดให้ผู้ให้บริการและเอนทิตีมีมาตรการปกป้องความสมบูรณ์ของเครือข่ายและระบบสารสนเทศ รวมถึงการจัดทำขั้นตอนปฏิบัติงานอย่างเป็นทางการ (standard operating procedures) สำหรับระบบสำคัญ
- VCSec 7 การควบคุมการเข้าถึงระบบ กำหนดให้ผู้ให้บริการและเอนทิตีจัดทำนโยบายและกลไกควบคุมการเข้าถึงระบบและเครือข่าย ทั้งในส่วนของผู้ใช้งานและผู้ดูแลระบบ เพื่อให้เฉพาะผู้มีสิทธิ์เท่านั้นที่สามารถเข้าถึงข้อมูลหรือระบบได้ และต้องมีการตรวจสอบทบทวนสิทธิ์อย่างสม่ำเสมอ

- VCSec 8 การพัฒนาระบบและการบำรุงรักษาอย่างมั่นคงปลอดภัย กำหนดให้ผู้ให้บริการและเอนทิตีต้องกำหนดแนวทางการพัฒนาซอฟต์แวร์ที่ปลอดภัย (secure software development) และเก็บรักษาหลักฐานการทดสอบความมั่นคงปลอดภัยในทุกขั้นตอนของวงจรการพัฒนา
- VCSec 9 การบริหารความต่อเนื่องทางธุรกิจ กำหนดให้ผู้ให้บริการและเอนทิตีต้องมีแผนรองรับเหตุฉุกเฉิน (contingency plan) และแผนกู้คืนระบบ (disaster recovery plan) สำหรับระบบที่สำคัญ เพื่อให้สามารถฟื้นฟูบริการได้รวดเร็วและลดผลกระทบจากเหตุการณ์ที่ไม่คาดคิด
- VCSec 10 การปฏิบัติตามข้อกำหนดกฎหมายและนโยบายความมั่นคงปลอดภัยขององค์กร กำหนดให้ผู้ให้บริการและเอนทิตีต้องมีการกำกับดูแลการปฏิบัติตามกฎหมาย มาตรการควบคุมภายใน และมาตรฐานสากลที่เกี่ยวข้อง โดยจัดให้มีขั้นตอนการตรวจสอบการปฏิบัติตาม (compliance monitoring and auditing) และต้องมีการทบทวนและปรับปรุงอย่างต่อเนื่อง

6.2 VCGF-02 ดีไอดีเมธอดสำหรับระบบนิเวศของเอกสารรับรองของไทย

VCTF-02 DID Method Specification for Thai VC ecosystem กำหนดวิธีการสร้าง บริหารจัดการและตรวจสอบตัวตนทางดิจิทัลแบบกระจายศูนย์สำหรับบุคคลธรรมดา โดยอิงตามมาตรฐาน W3C DID Core Specification และเสนอรูปแบบที่เหมาะสมกับบริบทของระบบนิเวศของเอกสารรับรองของไทย

เอกสารนี้นิยามรูปแบบดีไอดี (DID) สำหรับบุคคลธรรมดาในรูปแบบ did:key ซึ่งสามารถสร้างและบริหารจัดการได้แบบ self-sovereign ภายในกระเป๋าดิจิทัล (digital wallet) ของผู้ใช้เอง นอกจากนี้ยังกำหนดกระบวนการตรวจพิสูจน์และยืนยันตัวตน (DID resolution and verification) คุณสมบัติด้านความมั่นคงปลอดภัยของกระบวนการเข้ารหัสลับ (cryptographic compliance) และเสนอรูปแบบ API สำหรับการตรวจสอบข้อมูลตัวตนจากระบบทะเบียนข้อมูลตัวที่เชื่อถือได้ของ สพธอ. (ETDA-DIDR) เพื่อรองรับการพิสูจน์ความน่าเชื่อถือก่อนการใช้งานเอกสารรับรอง

6.3 VCTF-03 โพรโทคอลการแลกเปลี่ยนเอกสารรับรอง

VCTF-03 Verifiable Credential Exchange Protocols กำหนดกรอบกระบวนการมาตรฐานสำหรับการออก (issuance) การแลกเปลี่ยน (presentation) และการตรวจสอบยืนยัน (verification) สำหรับเอกสารรับรองและเอกสารสำแดงภายในระบบนิเวศของเอกสารรับรอง (VC ecosystem) ภายใต้การกำกับดูแลของหน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) โดยอิงตามมาตรฐานสากล เช่น W3C Verifiable Credentials Data Model 2.0 และ OpenID Connect for Verifiable Credentials/Presentations (OIDC4VC/VP)

เอกสารนี้กำหนดรายละเอียดของกระบวนการการออกเอกสารรับรองโดยใช้โพรโทคอล OIDC4VCI ซึ่งรองรับการพิสูจน์ตัวตนข้ามอุปกรณ์ผ่าน PKCE และการนำเสนอเอกสารสำแดงโดยใช้โพรโทคอล OIDC4VP พร้อมกำหนดข้อกำหนดการตรวจสอบความถูกต้องด้วยกระบวนการเข้ารหัสลับ (cryptographic

operations) และกระบวนการตรวจสอบความถูกต้องของเอกสาร นอกจากนี้ยังได้ระบุการตั้งค่าต่าง ๆ ที่เกี่ยวข้องกับกระบวนการแลกเปลี่ยนเอกสารรับรอง เช่น การจัดการอายุของโทเค็น และการตรวจสอบสถานะของผู้ออกและผู้ตรวจสอบเอกสารกับระบบทะเบียนข้อมูลตัวตนที่เชื่อถือได้ของ สพธอ. (ETDA-DIDR) เพื่อรักษาความน่าเชื่อถือและความมั่นคงปลอดภัยของเอกสารรับรอง

6.4 VCTF-04 แบบข้อมูลและโครงสร้างข้อมูลของเอกสารรับรองและข้อความยืนยัน

VCTF-04 Verifiable Credential and Claim Data Model & Schemas กำหนดแบบข้อมูล (data model) และเค้าร่างโครงสร้างข้อมูล (data schema) สำหรับการสร้างเอกสารรับรอง (VC) และเอกสารสำแดง (VP) ที่ใช้งานภายในระบบนิเวศของเอกสารรับรอง (VC ecosystem) ภายใต้การกำกับดูแลของหน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) เอกสารฉบับนี้อ้างอิงตามมาตรฐาน W3C Verifiable Credentials Data Model [2] [3]

เอกสารฉบับนี้ยังได้กำหนดการใช้ credentialSchema เพื่ออ้างอิงถึงเค้าร่างโครงสร้างข้อมูล (data schema) กลางที่หน่วยควบคุมดูแลบริการฯ เป็นผู้ดูแลในรูปแบบทะเบียนเค้าร่างโครงสร้างข้อมูล (schema registry) เพื่อให้การอ้างอิงและตรวจสอบความถูกต้องของข้อมูลที่ระบุในเอกสารรับรองมีความชัดเจน และรองรับการตรวจสอบความถูกต้องเชิงโครงสร้าง (structural validation) ของข้อมูล

6.5 VCTF-05 บทบาทหน้าที่ของหน่วยควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรอง

VCTF-05 VC Governance Authority Responsibilities กำหนดบทบาทหน้าที่ โครงสร้างการดำเนินงาน และกลไกการกำกับดูแลของหน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) ภายในระบบนิเวศของเอกสารรับรอง (VC ecosystem) โดยมีวัตถุประสงค์เพื่อสร้างความน่าเชื่อถือ ความมั่นคงปลอดภัย และการทำงานร่วมกันได้ของการออก การแลกเปลี่ยน การตรวจสอบ และการจัดการเอกสารรับรองและเอกสารสำแดง

เอกสารนี้ ยังได้เสนอโครงสร้างองค์กรของหน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) ซึ่งประกอบด้วยคณะกรรมการกำกับดูแล (VC governance board) คณะกรรมการตรวจสอบและประเมินความเชื่อมั่น (trust assurance committee) กลุ่มทำงานด้านเทคนิค (technical working group) และหน่วยรับเรื่องเหตุการณ์และข้อพิพาท (incident response and dispute resolution unit) ทั้งนี้ หน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) ยังมีหน้าที่และความรับผิดชอบหลักสำคัญใน 6 ด้าน เพื่อสร้างความเชื่อมั่นและความมั่นคงปลอดภัยให้กับการดำเนินงานของระบบเอกสารรับรอง ได้แก่

(1) การกำหนดนโยบายและกรอบการดำเนินงานสำหรับเอกสารรับรอง (governance and policy management) เพื่อให้เป็นไปตามมาตรฐานสากล

(2) การรับรองและกำกับดูแลหน่วยงานในระบบนิเวศ (accreditation and oversight) โดยการออกใบรับรอง การบำรุงรักษาทะเบียนหน่วยงานที่ได้รับการรับรอง และการตรวจสอบความสอดคล้อง

(3) การกำหนดมาตรฐานทางเทคนิคและการสร้างความสามารถในการทำงานร่วมกัน (Interoperability and Standardization)

(4) การวางนโยบายและควบคุมความเสี่ยงด้านความมั่นคงปลอดภัยและความน่าเชื่อถือ (security and trust assurance) รวมถึงการจัดการวงจรชีวิตของดีไอดี (DID) และเอกสารรับรอง

(5) การรับมือเหตุการณ์ความเสี่ยงและการระงับข้อพิพาท (incident handling and dispute resolution) และ

(6) การคุ้มครองข้อมูลส่วนบุคคลและการจัดการความเป็นส่วนตัวของผู้ใช้งาน (privacy and user data protection)

6.6 VCTF-06 การรับรองอัลกอริทึมการเข้ารหัสลับและลายมือชื่อดิจิทัล

VCTF-06 Approval of Cryptographic and Digital Signature Algorithms for the Thai VC ecosystem กำหนดอัลกอริทึมการเข้ารหัสลับ (cryptography) และลายมือชื่อดิจิทัล (digital signature) ที่ได้รับการอนุมัติสำหรับการใช้งานในระบบนิเวศของเอกสารรับรองภายใต้ สพธอ. เพื่อสร้างหลักประกันด้านความมั่นคงปลอดภัย ความถูกต้อง และความน่าเชื่อถือของเอกสารรับรอง

เอกสารนี้ระบุรายการอัลกอริทึมที่อนุมัติสำหรับการลงลายมือชื่อดิจิทัล เช่น EdDSA รวมถึงฟังก์ชันแฮชที่ได้รับอนุมัติ เช่น SHA-256 และ SHA-384 และอัลกอริทึมการเข้ารหัสลับเช่น AES-256 โดยอ้างอิงตามมาตรฐานสากล เช่น SOG-IS NIST และ ETSI ซึ่งเป็นอัลกอริทึมที่ยังคงมีความแข็งแกร่งในการประยุกต์ใช้งานและเป็นที่ยอมรับในระดับสากล เอกสารนี้ยังได้กำหนดแนวทางการทบทวนรายการอัลกอริทึมเข้ารหัสลับที่มีการใช้งานภายใต้ระบบนิเวศของเอกสารรับรองของไทยอย่างต่อเนื่องตามความก้าวหน้าทางเทคโนโลยี เพื่อรักษาความน่าเชื่อถือและความมั่นคงปลอดภัยในระบบนิเวศของเอกสารรับรอง

6.7 VCTF-07 ข้อกำหนดระดับความเข้มงวดของการพิสูจน์และยืนยันตัวตนดิจิทัล

VCTF-07 Digital ID Assurance Level Requirements for VC Use Cases กำหนดข้อกำหนดด้านระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL) และระดับความน่าเชื่อถือของการยืนยันตัวตน (AAL) สำหรับการออกเอกสารรับรอง ในกรณีการใช้งานภายใต้กรอบแนวทางการสร้างระบบนิเวศสำหรับเอกสารรับรองและเอกสารสำแดงที่เชื่อถือได้ (VCGF) โดยได้กำหนด IAL และ AAL ให้เหมาะสมตามความเสี่ยงของแต่ละประเภทเอกสาร

6.8 VCTF-08 ข้อกำหนดการจัดการกุญแจเข้ารหัสและการจัดเก็บเอกสารรับรองที่ปลอดภัยสำหรับระบบกระเป๋าดิจิทัล

VCTF-0 8 Specification for Secure Key Management and Credential Storage in Digital Wallet Systems เป็นข้อกำหนดทางเทคนิคและการรักษาความมั่นคงปลอดภัยสำหรับการสร้างกุญแจเข้ารหัส การเก็บรักษากุญแจส่วนตัว และการปกป้องข้อมูลเอกสารรับรอง (VCs) เอกสารสำแดง (VPs) และดีไอดี (DIDs) ภายในระบบกระเป๋าดิจิทัลที่ใช้ในระบบนิเวศของเอกสารรับรอง (VC ecosystem) โดยมีเป้าหมายเพื่อให้กระบวนการเข้ารหัสลับ (cryptography) และการจัดเก็บข้อมูลสำคัญเป็นไปตามระดับความน่าเชื่อถือ (level of assurance) ที่กำหนดไว้ VCTF-07 ข้อกำหนดระดับความน่าเชื่อถือของตัวตนดิจิทัลสำหรับกรณีใช้งานเอกสารรับรอง

เอกสารฉบับนี้ระบุข้อกำหนดหลักในสามส่วนสำคัญ ได้แก่ การสร้างกุญแจอย่างมั่นคง (secure key generation) การจัดเก็บกุญแจและข้อมูลอย่างมั่นคง (Secure Key Storage) และกระบวนการเข้ารหัสลับ (cryptographic operations) โดยกำหนดให้ใช้เทคโนโลยีเช่น Trusted Execution Environment/SE (TEE/ SE) หรือ Hardware Security Module (HSM) รวมทั้งกำหนดมาตรการต่าง ๆ ที่จำเป็นในการรักษาความมั่นคงปลอดภัยของกุญแจและข้อมูลสำคัญ เช่น การป้องกันการส่งออกกุญแจส่วนตัว และการตรวจสอบความสมบูรณ์ของอุปกรณ์ก่อนอนุญาตให้ดำเนินการที่เกี่ยวข้องกับกุญแจหรือข้อมูลรับรอง

6.9 VCTF-09 แนวทางการประเมินความเสี่ยงในระบบนิเวศของเอกสารรับรอง

VCTF-09 VC Risk Assessment Guideline กำหนดแนวทาง กระบวนการ และข้อกำหนดเชิงเทคนิคสำหรับการประเมินความเสี่ยงภายในระบบนิเวศสำหรับเอกสารรับรองและเอกสารสำแดงที่เชื่อถือได้ โดยมีวัตถุประสงค์เพื่อสนับสนุนเอนติทีต่าง ๆ เช่น ผู้ออกเอกสารรับรอง (issuer) ผู้ตรวจสอบเอกสารสำแดง (verifier) ผู้ให้บริการกระเป๋าดิจิทัล (digital wallet provider) ผู้ให้บริการระบบทะเบียนเอกสารรับรอง (verifiable data registry provider) ผู้ถือเอกสารรับรอง (holder) และหน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) ในการดำเนินการบริหารความเสี่ยงอย่างเป็นระบบและสอดคล้องกับกรอบแนวทางการสร้างระบบนิเวศสำหรับเอกสารรับรองและเอกสารสำแดงที่เชื่อถือได้ (trust model framework) แนวทางการจัดการความเสี่ยงในเอกสารนี้ได้นำแนวคิดและกระบวนการจากมาตรฐานสากล เช่น ISO/IEC 27005 [20] NIST SP 800-30 [21] และแนวทางของ Trust over IP Foundation มาใช้เพื่อระบุ วิเคราะห์ ประเมิน และกำหนดแผนการจัดการความเสี่ยงที่เกี่ยวข้องกับการดำเนินงานภายในระบบนิเวศของเอกสารรับรอง (VC ecosystem) ทั้งนี้ แนวทางการประเมินความเสี่ยงตามเอกสารฉบับนี้กำหนดให้กระบวนการเป็นแบบต่อเนื่องและมีการทบทวนสม่ำเสมอ รวมถึงให้ผู้ให้บริการและเอนทิตีต่าง ๆ ในระบบนิเวศต้องรายงานสถานะความเสี่ยงต่อหน่วยงานผู้มีอำนาจในการควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรองดิจิทัล (VCGA) เพื่อสนับสนุนความโปร่งใส การบริหารจัดการเชิงรุก และการรักษาความน่าเชื่อถือของระบบเอกสารรับรองอย่างยั่งยืน

ภาคผนวก

กรอบธรรมาภิบาลบริการเกี่ยวกับระบบเอกสารรับรอง (VCGF)

ก.1 ภาพรวมของกรอบธรรมาภิบาลเกี่ยวกับระบบเอกสารรับรอง (VCGF)

ขอบเขตของข้อกำหนด (trust domain)	ข้อกำหนดการสร้างความน่าเชื่อถือ (assurance governance)
VCGF-1 trust support ข้อกำหนดเกี่ยวกับโครงสร้างพื้นฐานของความน่าเชื่อถือ	
VCGF-1.1 ข้อกำหนดการบริหารจัดการความมั่นคงปลอดภัยของโครงสร้างพื้นฐาน (Security controls and Technical Infrastructure)	VCGF-1.1.1 การบริหารจัดการความมั่นคงปลอดภัยของผู้ออกเอกสารรับรอง
	VCGF-1.1.2 การบริหารจัดการความมั่นคงปลอดภัยของผู้ให้บริการกระเป๋าดิจิทัล
	VCGF-1.1.3 การบริหารจัดการความมั่นคงปลอดภัยของผู้ตรวจสอบเอกสารสำแดง
VCGF-1.2 ข้อกำหนดด้านความมั่นคงปลอดภัยของกระเป๋าเอกสารดิจิทัล (Digital Wallet Security Requirements)	VCGF-1.2.1 ความมั่นคงปลอดภัยของกระเป๋าเอกสารดิจิทัล
	VCGF-1.2.2 กลไกการยืนยันตัวตนสำหรับเข้าถึงเอกสารรับรองในกระเป๋าเอกสารดิจิทัล
VCGF-1.3 ข้อกำหนดความน่าเชื่อถือของโครงสร้างพื้นฐานและการเข้ารหัสลับข้อมูล (Cryptographic Integrity and Trust Infrastructure)	VCGF-1.3.1 ความมั่นคงปลอดภัยของระบบทะเบียนเอกสารรับรอง (Verifiable Data Registry)
	VCGF-1.3.2 ข้อกำหนดลายมือชื่อดิจิทัลและอัลกอริทึมเข้ารหัสลับสำหรับเอกสารรับรอง
VCGF-2 trust spanning ข้อกำหนดเกี่ยวกับโพรโทคอลการแลกเปลี่ยนข้อมูล	
VCGF-2.1 ข้อกำหนดโพรโทคอลการออกเอกสารรับรอง (Protocol for Credential Issuance)	VCGF-2.1.1 โพรโทคอลออกเอกสารรับรอง
	VCGF-2.1.2 การยืนยันตัวตนของผู้ถือเอกสารก่อนออกเอกสารรับรอง
VCGF-2.2 ข้อกำหนดโพรโทคอลการสำแดงเอกสาร (Protocol for Presentation Exchange)	VCGF-2.2.1 โพรโทคอลแลกเปลี่ยนเอกสารสำแดง

ขอบเขตของข้อกำหนด (trust domain)	ข้อกำหนดการสร้างความน่าเชื่อถือ (assurance governance)
VCGF-3 trust tasks ข้อกำหนดเกี่ยวกับข้อมูลรับรอง	
VCGF-3.1 ข้อกำหนดโครงสร้างข้อมูลของเอกสารรับรองและเอกสารสำแดง (Verifiable Credential and Presentation Structure)	VCGF-3.1.1 แบบข้อมูลสำหรับเอกสารรับรองและเอกสารสำแดง
	VCGF-3.1.2 โครงสร้างข้อมูลของข้อมูลรับรอง
	VCGF-3.1.3 ข้อพิสูจน์ของเอกสารรับรองและเอกสารสำแดง
	VCGF-3.1.4 การตรวจสอบการเพิกถอนและการระงับเอกสารรับรอง
	VCGF-3.1.5 การสำแดงข้อมูลรับรองแบบเลือกได้
VCGF-3.2 ข้อกำหนดความน่าเชื่อถือสำหรับผู้ออกเอกสารรับรอง (Trust Requirements for Issuers)	VCGF-3.2.1 คุณสมบัติของผู้ออกเอกสารรับรองที่เชื่อถือได้
	VCGF-3.2.2 การเชื่อมโยงผู้ถือเอกสารรับรองกับดีไอดี
	VCGF-3.2.3 การคุ้มครองข้อมูลส่วนบุคคลของผู้ออกเอกสารรับรอง
VCGF-3.3 ข้อกำหนดความน่าเชื่อถือสำหรับผู้ตรวจสอบเอกสารสำแดง (Trust Requirements for Verifiers)	VCGF-3.3.1 คุณสมบัติของผู้ตรวจสอบเอกสารสำแดงที่เชื่อถือได้
	VCGF-3.3.2 การคุ้มครองข้อมูลส่วนบุคคลของผู้ตรวจสอบเอกสารสำแดง
VCGF-3.4 ข้อกำหนดความน่าเชื่อถือสำหรับผู้ให้บริการกระเป๋าดิจิทัล (Trust Requirements for Digital wallet providers)	VCGF-3.4.1 คุณสมบัติของผู้ให้บริการกระเป๋าดิจิทัลที่เชื่อถือได้
	VCGF-3.4.2 ข้อกำหนดการยืนยันตัวตนและความมั่นคงปลอดภัยของกระเป๋าดิจิทัล
	VCGF-3.4.3 การคุ้มครองข้อมูลส่วนบุคคลของผู้ให้บริการกระเป๋าดิจิทัล
VCGF-3.5 ข้อกำหนดหน้าที่และรับความรับผิดชอบของหน่วยควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรอง (Responsibilities for the VC Governance Authority)	VCGF-3.5.1 การกำกับของหน่วยควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรอง
	VCGF-3.5.2 บริการตรวจสอบดีไอดีของเอกสารรับรอง
VCGF-4 trust applications ข้อกำหนดเกี่ยวกับแอพพลิเคชัน	
VCGF-4.1 การพิสูจน์ยืนยันตัวตนของผู้ถือเอกสารรับรอง (Holder Onboarding and Digital Identity Assurance)	VCGF-4.1.1 ข้อกำหนดการพิสูจน์ยืนยันตัวตนของผู้ถือเอกสารรับรอง

ขอบเขตของข้อกำหนด (trust domain)	ข้อกำหนดการสร้างความน่าเชื่อถือ (assurance governance)
VCGF-4.2 การคุ้มครองข้อมูลในข้อมูลรับรอง (Protection of accuracy data)	VCGF-4.2.1 การคุ้มครองข้อมูลส่วนบุคคลของเอนทิตีในระบบนิเวศของเอกสารรับรอง
VCGF-4.3 การสร้างความน่าเชื่อถือกับระบบนิเวศของเอกสารรับรอง (Ecosystem technical trust)	VCGF-4.3.1 มาตรฐานด้านเทคนิคและชุดการทดสอบความสอดคล้องทางเทคนิค
VCGF-4.4 การสร้างความน่าเชื่อถือกับระบบนิเวศของเอกสารรับรอง (Ecosystem technical trust)	VCGF-4.4.1 การรับรองผู้ให้บริการและเอนทิตีที่เชื่อถือได้
	VCGF-4.4.2 การประเมินความเสี่ยงและการปรับปรุงกรอบแนวทางการสร้างระบบนิเวศที่เชื่อถือได้
VCGF-4.5 ความรับผิดและการระงับข้อพิพาท (Liability & dispute resolution)	VCGF-4.5.1 ความรับผิดชอบและแนวทางการระงับข้อพิพาทในกรณีใช้เอกสารรับรองโดยมิชอบ

ก.2 กรอบธรรมาภิบาลเกี่ยวกับระบบเอกสารรับรอง (VCGF) สำหรับผู้ออกเอกสารรับรอง (issuer)

Layer	VCGF
Layer 1 trust support	- VCGF-1.1.1 การบริหารจัดการความมั่นคงปลอดภัยของผู้ออกเอกสารรับรอง - VCGF-1.3.2 ข้อกำหนดลายมือชื่อดิจิทัลและอัลกอริทึมเข้ารหัสลับสำหรับเอกสารรับรอง
Layer 2 trust spanning	- VCGF-2.1.1 โพรโทคอลออกเอกสารรับรอง - VCGF-2.1.2 การยืนยันตัวตนของผู้ถือเอกสารก่อนออกเอกสารรับรอง
Layer 3 trust tasks	- VCGF-3.1.1 แบบข้อมูลสำหรับเอกสารรับรองและเอกสารสำแดง - VCGF-3.1.2 โครงสร้างข้อมูลของข้อมูลรับรอง - VCGF-3.1.3 ข้อพิสูจน์ของเอกสารรับรองและเอกสารสำแดง - VCGF-3.1.4 การตรวจสอบการเพิกถอนและการระงับเอกสารรับรอง - VCGF-3.1.5 การสำแดงข้อมูลรับรองแบบเลือกได้ - VCGF-3.2.1 คุณสมบัติของผู้ออกเอกสารรับรองที่เชื่อถือได้

Layer	VCGF
	- VCGF-3.2.2 การเชื่อมโยงผู้ถือเอกสารรับรองกับดีไอดี - VCGF-3.2.3 การคุ้มครองข้อมูลส่วนบุคคลของผู้ออกเอกสารรับรอง
Layer 4 trust applications	- VCGF-4.2.1 การคุ้มครองข้อมูลส่วนบุคคลของเอนทิตีในระบบนิเวศของเอกสารรับรอง

ก.4 กรอบธรรมาภิบาลเกี่ยวกับระบบเอกสารรับรอง (VCGF) สำหรับผู้ตรวจสอบเอกสารสำแดง (verifier)

Layer	VCGF
Layer 1 trust support	- VCGF-1.1.3 การบริหารจัดการความมั่นคงปลอดภัยของผู้ตรวจสอบเอกสารสำแดง - VCGF-1.3.2 ข้อกำหนดลายมือชื่อดิจิทัลและอัลกอริทึมเข้ารหัสลับสำหรับเอกสารรับรอง
Layer 2 trust spanning	- VCGF-2.2.1 โพรโทคอลแลกเปลี่ยนเอกสารสำแดง
Layer 3 trust tasks	- VCGF-3.1.1 แบบข้อมูลสำหรับเอกสารรับรองและเอกสารสำแดง - VCGF-3.1.2 โครงสร้างข้อมูลของข้อมูลรับรอง - VCGF-3.1.3 ข้อพิสูจน์ของเอกสารรับรองและเอกสารสำแดง - VCGF-3.1.4 การตรวจสอบการเพิกถอนและการระงับเอกสารรับรอง - VCGF-3.1.5 การสำแดงข้อมูลรับรองแบบเลือกได้ - VCGF-3.3.1 คุณสมบัติของผู้ตรวจสอบเอกสารสำแดงที่เชื่อถือได้ - VCGF-3.3.2 การคุ้มครองข้อมูลส่วนบุคคลของผู้ตรวจสอบเอกสารสำแดง
Layer 4 trust applications	- VCGF-4.2.1 การคุ้มครองข้อมูลส่วนบุคคลของเอนทิตีในระบบนิเวศของเอกสารรับรอง

ก.3 กรอบธรรมาภิบาลเกี่ยวกับระบบเอกสารรับรอง (VCGF) สำหรับผู้ให้บริการกระเป๋าดิจิทัล (digital wallet provider)

Layer	VCGF
Layer 1 trust support	- VCGF-1.1.2 การบริหารจัดการความมั่นคงปลอดภัยของผู้ให้บริการกระเป๋าดิจิทัล - VCGF-1.2.1 ความมั่นคงปลอดภัยของกระเป๋าเอกสารดิจิทัล - VCGF-1.2.2 กลไกการยืนยันตัวตนสำหรับเข้าถึงเอกสารรับรองในกระเป๋าเอกสารดิจิทัล - VCGF-1.3.2 ข้อกำหนดลายมือชื่อดิจิทัลและอัลกอริทึมเข้ารหัสลับสำหรับเอกสารรับรอง
Layer 2 trust spanning	- VCGF-2.1.1 โพรโทคอลออกเอกสารรับรอง - VCGF-2.2.1 โพรโทคอลแลกเปลี่ยนเอกสารสำแดง
Layer 3 trust tasks	- VCGF-3.1.1 แบบข้อมูลสำหรับเอกสารรับรองและเอกสารสำแดง - VCGF-3.1.2 โครงสร้างข้อมูลของข้อมูลรับรอง - VCGF-3.1.3 ข้อพิสูจน์ของเอกสารรับรองและเอกสารสำแดง - VCGF-3.1.4 การตรวจสอบการเพิกถอนและการระงับเอกสารรับรอง - VCGF-3.1.5 การสำแดงข้อมูลรับรองแบบเลือกได้ - VCGF-3.4.1 คุณสมบัติของผู้ให้บริการกระเป๋าดิจิทัลที่เชื่อถือได้ - VCGF-3.4.2 ข้อกำหนดการยืนยันตัวตนและความมั่นคงปลอดภัยของกระเป๋าดิจิทัล - VCGF-3.4.3 การคุ้มครองข้อมูลส่วนบุคคลของผู้ให้บริการกระเป๋าดิจิทัล
Layer 4 trust applications	- VCGF-4.1.1 ข้อกำหนดการพิสูจน์ยืนยันตัวตนของผู้ถือเอกสารรับรอง - VCGF-4.2.1 การคุ้มครองข้อมูลส่วนบุคคลของเอนทิตีในระบบนิเวศของเอกสารรับรอง

ก.4 กรอบธรรมาภิบาลเกี่ยวกับระบบเอกสารรับรอง (VCGF) สำหรับหน่วยควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรอง (VCGA) และผู้ให้บริการระบบทะเบียนเอกสารรับรอง (VDR)

Layer	VCGF
Layer 1 trust support	- VCGF-1.3.1 ความมั่นคงปลอดภัยของระบบทะเบียนเอกสารรับรอง (Verifiable Data Registry) - VCGF-1.3.2 ข้อกำหนดลายมือชื่อดิจิทัลและอัลกอริทึมเข้ารหัสลับสำหรับเอกสารรับรอง
Layer 2 trust spanning	-
Layer 3 trust tasks	- VCGF-3.5.1 การกำกับของหน่วยควบคุมดูแลบริการเกี่ยวกับระบบเอกสารรับรอง - VCGF-3.5.2 บริการตรวจสอบดีไอดีของเอกสารรับรอง
Layer 4 trust applications	- VCGF-4.2.1 การคุ้มครองข้อมูลส่วนบุคคลของเอนทิตีในระบบนิเวศของเอกสารรับรอง - VCGF-4.3.1 มาตรฐานด้านเทคนิคและชุดการทดสอบความสอดคล้องทางเทคนิค - VCGF-4.4.1 การรับรองผู้ให้บริการและเอนทิตีที่เชื่อถือได้ - VCGF-4.4.2 การประเมินความเสี่ยงและการปรับปรุงกรอบแนวทางการสร้างระบบนิเวศที่เชื่อถือได้ - VCGF-4.5.1 ความรับผิดชอบและแนวทางการระงับข้อพิพาทในกรณีใช้เอกสารรับรองโดยมิชอบ

บรรณานุกรม

[1] W3C Recommendation - Decentralized Identifiers (DIDs) v1.0.

[2] W3C Recommendation - Verifiable Credentials Data Model v1.1.

[3] W3C Recommendation - Verifiable Credentials Data Model v2.0.

[4] Trust Over IP Foundation, Defining Digital Trust Ecosystems V 1.0, 13 October 2022.

[5] Sovrin Foundation, Sovrin Governance Framework V2 Master Document V1, 2019.

[6] Sovrin Foundation, Sovrin Trust Assurance Framework V1, 2021.

[7] World Bank Group Report: Verifiable Credentials Standards Evaluation Report v1, Electronic Transactions Development Agency, 2024.

[8] รายงานเทคนิคกรอบการทำงานร่วมกันของกระเป๋าดิจิทัลสำหรับเอกสารรับรอง (Interoperable framework for digital wallets for verifiable credentials), สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์.

[9] “EBSI VC Framework,” [ออนไลน์]. Available: https://hub.ebsi.eu/vc-framework.

[10] “OpenAttestation Document Endorser and Verification Framework,” [ออนไลน์]. Available: https://www.openattestation.com/.

[11] Open Identity Exchange (OIX), OIX Trust Frameworks for Smart Digital ID Version 1.2, Open Identity Exchange, 2020.

[12] FIPS 140-3 Security Requirements for Cryptographic Modules.

[13] ISO/IEC 19790:2025 Information technology — Security techniques — Security requirements for cryptographic modules

[14] NIST Special Publication 800-63B Digital Identity Guidelines: Authentication and Lifecycle Management.

[15] ETSI TS 119 312 ver 1.4.3 (2023-08) Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

[16] IETF RFC 7515: JSON Web Signature (JWS).

[17] IETF RFC 7638: JSON Web Key (JWK) Thumbprint.

[18] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับผู้ให้บริการจัดทำ ส่งมอบ และเก็บรักษาข้อมูลอิเล็กทรอนิกส์ เลขที่ ขมธอ. 21-2562, เวอร์ชัน 1.0.

[19] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ บริการจัดทำ นำส่ง หรือเก็บรักษาข้อมูลอิเล็กทรอนิกส์ เลขที่ ขมธอ. 35-2567, เวอร์ชัน 1.0.

[20] ISO/IEC 27005:2022 Information technology — Security techniques — Information security risk management.

[21] NIST SP 800-30 Guide for Conducting Risk Assessments.

[22] “ Digital Autralia - Power of Attorney Services,” [ออนไลน์]. Available: https://www.digitalaustria.gv.at/eng/insights/E-Gov-A-Z_EN/Digitally-networked-services/Power-of-Attorney-Service.html.

[23] “GOV.UK LPA,” [ออนไลน์]. Available: https://www.gov.uk/power-of-attorney.

[24] “ IRS Form 2848 Power of Attorney,” [ออนไลน์]. Available: https://www.irs.gov/forms-pubs/about-form-2848.

[25] ETSI TR 119 100 ver 1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI); Guidance on the use of standards for signature creation and validation.

[26] The JavaScript Object Notation (JSON) Data Interchange Format, [ออนไลน์]. Available: https://datatracker.ietf.org/doc/html/rfc8259.

[27] ETSI EN 319 122-1 ver 1.3.1 (2023-06) Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures.

[28] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการมอบอำนาจทางอิเล็กทรอนิกส เลขที่ ขมธอ. 31-2565, เวอร์ชัน 1.0.

[29] Trust Over IP Foundation, ToIP Risk Assessment Companion Guide Version 1.0, August 2021.