ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ETDA Recommendation on ICT Standard

for Electronic Transactions

ขมธอ. [x-xxxx]

ว่าด้วยกระเป๋าดิจิทัลสำหรับการแลกเปลี่ยนเอกสารรับรอง

DIGITAL WALLET FOR VERIFIABLE CREDENTIALS

เวอร์ชัน 0.2

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ICS 35.030

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยกระเป๋าดิจิทัลสำหรับการแลกเปลี่ยนเอกสารรับรอง

ขมธอ. [x-xxxx]

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

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

ประกาศโดย
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

วันที่ กรุณาเลือกวันที่ประกาศ

คณะทำงานจัดทำร่างข้อเสนอแนะมาตรฐานเกี่ยวกับธุรกิจบริการ
ด้านการทำธุรกรรมทางอิเล็กทรอนิกส์

ที่ปรึกษาคณะทำงาน

นายชัยชนะ มิตรพันธ์	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ประธานคณะทำงาน

นายศุภโชค จันทรประทิน	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ผู้ทำงาน

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

ผู้ทำงานและเลขานุการ

นายณัฐฑพัฒน์ โรจนศุภมิตร	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ผู้ช่วยเลขานุการ

นายวีรศักดิ์ ดีอ่ำ	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยกระเป๋าดิจิทัลสำหรับการแลกเปลี่ยนเอกสารรับรองฉบับนี้ จัดทำขึ้นเพื่ออธิบายหลักการและองค์ประกอบที่เกี่ยวข้องกับการใช้งานและการให้บริการกระเป๋าดิจิทัลเพื่อแลกเปลี่ยนเอกสารรับรอง (verifiable credential: VC) และเอกสารสำแดง (verifiable presentation: VP) รวมถึงระบุข้อกำหนดสำหรับผู้ที่เกี่ยวข้องกับการใช้งานและการให้บริการกระเป๋าดิจิทัล เพื่อให้ผู้ที่เกี่ยวข้องมีความเข้าใจตรงกัน เกิดเป็นแบบแผนการใช้งานกระเป๋าดิจิทัลในประเทศไทยที่มีความมั่นคงปลอดภัย คุ้มครองข้อมูลส่วนบุคคล และสามารถทำงานร่วมกันได้

โดยมีการนำเสนอและรับฟังความคิดเห็นเป็นการทั่วไป ตลอดจนพิจารณาข้อมูล ข้อสังเกต ข้อคิดเห็นจากผู้ทรงคุณวุฒิและจากหน่วยงานที่เกี่ยวข้อง เพื่อปรับปรุงให้ข้อเสนอแนะมาตรฐานฉบับนี้มีความสมบูรณ์ครบถ้วนยิ่งขึ้น รวมทั้งให้สามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพ

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยกระเป๋าดิจิทัลสำหรับการแลกเปลี่ยนเอกสารรับรอง ฉบับนี้ จัดทำขึ้นโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

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

คำนำ

ปัจจุบันการใช้งานกระเป๋าดิจิทัล (digital wallet) ได้เข้ามามีบทบาทในการทำธุรกรรมทางอิเล็กทรอนิกส์ โดยกระเป๋าดิจิทัลจะมีคุณสมบัติในการจัดเก็บกุญแจเข้ารหัสลับ (cryptographic keys) เอกสารรับรอง (verifiable credentials) ข้อมูลเกี่ยวกับอัตลักษณ์ (identity attributes) และข้อมูลส่วนบุคคลต่าง ๆ อย่างมั่นคงปลอดภัย และสามารถนำมาใช้ในการพิสูจน์และยืนยันตัวตนทางดิจิทัลเพื่อเข้าถึงบริการทั้งจากภาครัฐและภาคเอกชน นอกจากนี้กระเป๋าดิจิทัลสามารถนำมาใช้ในการพิสูจน์และยืนยันตัวตนได้ทั้งในรูปแบบแบบออนไลน์ เช่น การลงทะเบียนขอใช้บริการบนเว็บไซต์ และรูปแบบออฟไลน์ เช่น การเข้ารับการรักษาในโรงพยาบาล รวมถึงใช้ในการสร้างลายมือชื่อดิจิทัล (digital signature) บนเอกสารหรือข้อมูลอิเล็กทรอนิกส์

ทั้งนี้ เพื่อให้การให้บริการกระเป๋าดิจิทัลมีความน่าเชื่อถือและเป็นที่ยอมรับ โดยเฉพาะอย่างยิ่ง การใช้เพื่อพิสูจน์และยืนยันตัวตนทางดิจิทัล ซึ่งเป็นบริการที่มีความสำคัญและช่วยสร้างความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์จึงได้จัดทำข้อเสนอแนะมาตรฐานฯ ว่าด้วยกระเป๋าดิจิทัลสำหรับการแลกเปลี่ยนเอกสารรับรอง เพื่ออธิบายหลักการและองค์ประกอบที่เกี่ยวข้องกับการใช้งานและให้บริการกระเป๋าดิจิทัลเพื่อแลกเปลี่ยนเอกสารรับรอง (verifiable credential: VC) และเอกสารสำแดง (verifiable presentation: VP) รวมถึงระบุข้อกำหนดสำหรับผู้ที่เกี่ยวข้องกับการใช้งานและให้บริการกระเป๋าดิจิทัล เพื่อให้ผู้ที่เกี่ยวข้องมีความเข้าใจตรงกัน เกิดเป็นแบบแผนการใช้งานกระเป๋าดิจิทัลในประเทศไทยที่มีความมั่นคงปลอดภัย คุ้มครองข้อมูลส่วนบุคคล และสามารถทำงานร่วมกันได้ รวมถึงช่วยส่งเสริมให้เกิดบริการกระเป๋าดิจิทัลสำหรับการแลกเปลี่ยนเอกสารรับรองในประเทศไทย

สารบัญ

สารบัญรูป

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ว่าด้วยกระเป๋าดิจิทัลสำหรับการแลกเปลี่ยนเอกสารรับรอง

1. ขอบข่าย

ข้อเสนอแนะมาตรฐานฉบับนี้อธิบายหลักการ กรอบการทำงาน องค์ประกอบที่สำคัญ และโพรโทคอลการแลกเปลี่ยนข้อมูลสำหรับกระเป๋าดิจิทัลเพื่อแลกเปลี่ยนเอกสารรับรอง (verifiable credential: VC) และเอกสารสำแดง (verifiable presentation: VP) โพรโทคอลการแลกเปลี่ยนข้อมูลระหว่างกระเป๋าดิจิทัลกับผู้ที่เกี่ยวข้อง รวมทั้งกำหนดข้อกำหนดพื้นฐานที่จำเป็นสำหรับการให้บริการกระเป๋าดิจิทัล เพื่อให้ผู้ให้บริการกระเป๋าดิจิทัล (digital wallet provider) และผู้ออกเอกสารรับรอง (verifiable credential issuer) มีแนวทางในการให้บริการที่มีความน่าเชื่อถือ มั่นคงปลอดภัย คุ้มครองข้อมูลส่วนบุคคล และสามารถทำงานร่วมกันได้

ข้อเสนอแนะมาตรฐานฉบับนี้สามารถใช้เป็นแนวทางได้กับทั้งผู้ออกเอกสาร (issuer) ผู้ถือเอกสาร (holder) และผู้ตรวจสอบเอกสาร (verifier) สำหรับการใช้งานประเภทต่าง ๆ เช่น การพิสูจน์และยืนยันตัวตน การบริหารจัดการเอกสารรับรอง การบริหารจัดการกุญแจเข้ารหัสลับ การลงลายมือชื่อดิจิทัล และการเลือกเปิดเผยข้อมูลบางส่วน (selective disclosure)

ทั้งนี้ ข้อเสนอแนะมาตรฐานฉบับนี้จำกัดนิยามของกระเป๋าดิจิทัลให้ครอบคลุมเฉพาะการใช้งานเอกสารรับรองและเอกสารสำแดงที่มีการลงลายมือชื่อดิจิทัล (digital signature) เท่านั้น แต่จะไม่ครอบคลุมถึงการใช้งานเอกสารอิเล็กทรอนิกส์ที่ไม่สามารถตรวจสอบได้ด้วยกระบวนการระบบรหัส (cryptography) และไม่ครอบคลุมการใช้งานกระเป๋าดิจิทัลประเภทอื่น ๆ เช่น กระเป๋าดิจิทัลสำหรับบริการเงินอิเล็กทรอนิกส์ (e-money wallet) หรือกระเป๋าดิจิทัลสำหรับการแลกเปลี่ยนสินทรัพย์ดิจิทัล (cryptocurrency/cryptoasset wallet)

ข้อเสนอแนะมาตรฐานฉบับนี้มีรูปแบบของคำที่ใช้แสดงออกถึงคุณลักษณะของเนื้อหาเชิงบรรทัดฐาน (normative) และเนื้อหาเชิงให้ข้อมูล (informative) ดังต่อไปนี้

– "ต้อง" (shall) ใช้ระบุสิ่งที่เป็นข้อกำหนด (requirement)
– "ควร" (should) ใช้ระบุสิ่งที่เป็นข้อแนะนำ (recommendation)
– "อาจ" (may) ใช้ระบุสิ่งที่ยินยอมหรืออนุญาตให้ทำได้ (permission)

2. บทนิยาม

ความหมายของคำที่ใช้ในข้อเสนอแนะมาตรฐานฉบับนี้ มีดังต่อไปนี้

2.1 เจ้าของข้อความ (subject) หมายถึง เอนทิตีที่ถูกกล่าวอ้างถึงในข้อความยืนยัน (claim) [1]

2.2 ข้อความยืนยัน (claim) หมายถึง ข้อความเกี่ยวกับเจ้าของข้อความ (subject) ที่จะถูกรับรองโดยผู้ออกเอกสาร (issuer) [1]

2.3 เอกสารรับรอง (verifiable credential: VC) หมายถึง ชุดของข้อความยืนยันอย่างน้อยหนึ่งรายการที่ถูกรับรองโดยผู้ออกเอกสาร (issuer) ทั้งนี้ เอกสารรับรองมีคุณสมบัติที่สามารถตรวจพบการเปลี่ยนแปลงใด ๆ ที่

เกิดกับความถูกต้องครบถ้วนของข้อมูล และตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ของผู้ออกเอกสารได้ด้วยกระบวนการเข้ารหัสลับ [1]

2.4 เอกสารสำแดง (verifiable presentation: VP) หมายถึง เอกสารรับรองอย่างน้อยหนึ่งชุด ที่ผู้ถือเอกสาร (holder) ใช้แสดงต่อผู้ตรวจสอบเอกสาร (verifier) ทั้งนี้ เอกสารสำแดงมีคุณสมบัติที่สามารถตรวจพบการเปลี่ยนแปลงใด ๆ ที่เกิดกับความถูกต้องครบถ้วนของข้อมูล และตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ของผู้ถือเอกสารและตรวจสอบเอกสารรับรองที่เกี่ยวข้องได้ด้วยกระบวนการเข้ารหัสลับ [1]

2.5 เอนทิตี (entity) หมายถึง สิ่งที่มีอยู่จริง เช่น บุคคล องค์กร หรืออุปกรณ์ ซึ่งถูกกล่าวอ้างในการใช้งานเอกสารรับรองและเอกสารสำแดง [1]

2.6 ผู้ออกเอกสาร (issuer) หมายถึง เอนทิตีที่ทำหน้าที่รับรองข้อความยืนยันโดยออกเป็นเอกสารรับรองให้แก่ผู้ถือเอกสาร [1]

2.7 ผู้สมัคร (applicant) หมายถึง เอนทิตีที่ยื่นขอเอกสารรับรอง แต่ยังไม่ได้รับเอกสารรับรองนั้น โดยผู้สมัครอาจจะเป็นเจ้าของข้อความ (subject) ในเอกสารรับรองหรือไม่ก็ได้

2.8 ผู้ถือเอกสาร (holder) หมายถึง เอนทิตีที่เป็นเจ้าของเอกสารรับรองอย่างน้อยหนึ่งชุด โดยจัดเก็บไว้ในกระเป๋าดิจิทัล (credential wallet) และสามารถใช้เอกสารรับรองสร้างเป็นเอกสารสำแดง ทั้งนี้ ผู้ถือเอกสารมีอีกชื่อเรียกหนึ่งว่า ผู้ใช้งานกระเป๋าดิจิทัล (user) [1]

2.9 ผู้ตรวจสอบเอกสาร (verifier) หมายถึง เอนทิตีที่สามารถตรวจสอบความถูกต้องครบถ้วนของเอกสารรับรองและเอกสารสำแดงด้วยกระบวนการเข้ารหัสลับ รวมถึงตรวจสอบสถานะการใช้งานและความสอดคล้องตามโครงสร้างข้อมูลของเอกสารรับรองและเอกสารสำแดง ทั้งนี้ ผู้ตรวจสอบเอกสารมีอีกชื่อเรียกหนึ่งว่า ผู้อาศัยการยืนยันตัวตน (relying party: RP) [1]

2.10 ระบบทะเบียนเอกสารรับรอง (verifiable data registry) หมายถึง ระบบที่ช่วยสนับสนุนการสร้างและการตรวจสอบความถูกต้องครบถ้วนของเอกสารรับรองและเอกสารสำแดง โดยข้อมูลที่มีการจัดเก็บในระบบนี้ เช่น ตัวระบุ (identifier) และกุญแจสาธารณะ (public key) ของเอนทิตีที่เกี่ยวข้อง รวมถึงรายการเพิกถอน (revocation list) และเค้าร่าง (schema) ของเอกสารรับรองหรือเอกสารสำแดง [1]

2.11 ลายมือชื่อดิจิทัล (digital signature) หมายถึง ลายมือชื่ออิเล็กทรอนิกส์ (electronic signature) ที่ได้จากกระบวนการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ ซึ่งช่วยให้สามารถยืนยันตัวเจ้าของลายมือชื่อและตรวจพบการเปลี่ยนแปลงของข้อความและลายมือชื่ออิเล็กทรอนิกส์ได้ รวมถึงการทำให้เจ้าของลายมือชื่อไม่สามารถปฏิเสธความรับผิดจากข้อความที่ตนเองลงลายมือชื่อได้ [2]

2.12 ตัวระบุ (identifier) หมายถึง Uniform Resource Identifier (URI) ที่ระบุถึงเอนทิตี เอกสารรับรอง หรือข้อมูลอื่น ๆ ที่เกี่ยวข้อง

2.13 ตัวระบุแบบกระจายศูนย์ (decentralized identifier) หมายถึง ตัวระบุ (identifier) ที่ถูกสร้าง บริหารจัดการและควบคุมโดยเอนทิตีต่าง ๆ ในรูปแบบกระจายศูนย์ กล่าวคือไม่มีบุคคลที่สามที่เชื่อถือได้ (trusted third party) เป็นผู้ดำเนินการแทน

2.14 เค้าร่าง (schema) หมายถึง ข้อมูลที่กำหนดโครงสร้าง (structure) เนื้อหา (content) และรูปแบบ (format) ของเอกสารรับรองและ/หรือเอกสารสำแดง โดยสามารถแบ่งออกเป็น 2 ประเภท ได้แก่ เค้าร่างสำหรับการ

ตรวจสอบข้อมูล (data verification schema) และเค้าร่างสำหรับการเข้ารหัสข้อมูล (data encoding schema)

2.15 กระเป๋าดิจิทัล (digital wallet) หมายถึง หมายถึง โปรแกรมที่จัดเก็บและช่วยให้ผู้ถือเอกสารสามารถเข้าถึงและใช้งานเอกสารรับรองได้อย่างมั่นคงปลอดภัย [1]

2.16 ผู้ให้บริการกระเป๋าดิจิทัล (digital wallet provider) หมายถึง เอนทิตีที่ทำหน้าที่เป็นผู้พัฒนาและ/หรือผู้ให้บริการกระเป๋าดิจิทัลแก่ผู้ออกเอกสาร ผู้ถือเอกสาร หรือผู้ตรวจสอบเอกสาร

3. ภาพรวมของกระเป๋าดิจิทัล

การแลกเปลี่ยนเอกสารในรูปแบบกายภาพ (physical document) เป็นส่วนหนึ่งของการทำธุรกรรมในชีวิตประจำวัน โดยมีการใช้งานเป็นเวลายาวนานก่อนที่อินเทอร์เน็ตจะถูกใช้งานอย่างแพร่หลาย ยกตัวอย่างเช่น ผู้ขับรถแสดงใบอนุญาตขับขี่ที่ได้รับจากกรมการขนส่งทางบกต่อเจ้าพนักงานจราจร นักศึกษาแสดงปริญญาบัตรจากมหาวิทยาลัยต่อผู้ว่าจ้างเพื่อสมัครเข้าทำงาน และผู้โดยสารแสดงหนังสือเดินทางต่อเจ้าหน้าที่ตรวจคนเข้าเมืองเพื่อเดินทางไปต่างประเทศ

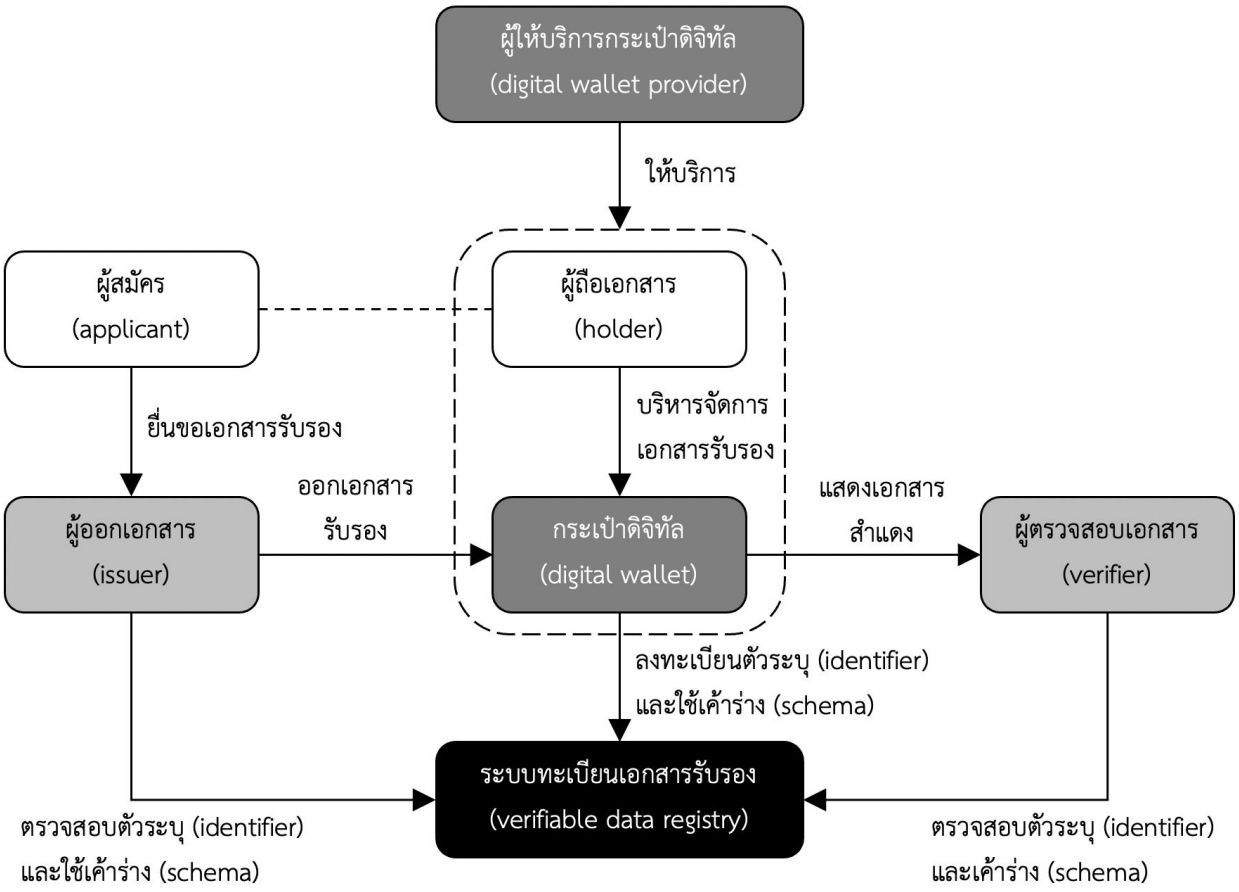
ในยุคของอินเตอร์เน็ต ได้มีการใช้งานและแลกเปลี่ยนเอกสารบนเว็บไซต์และแอปพลิเคชันอย่างแพร่หลาย อย่างไรก็ตาม เอกสารข้างต้นมักถูกใช้ในรูปแบบสำเนาอิเล็กทรอนิกส์ของเอกสารในรูปแบบกายภาพ (electronic copy of physical document) เช่น การสแกนบัตรประชาชนให้เป็นไฟล์เอกสารอิเล็กทรอนิกส์ประเภท Portable Document Format (PDF) ซึ่งเอกสารอิเล็กทรอนิกส์ในรูปแบบนี้ไม่ได้ใช้ศักยภาพของเทคโนโลยีสารสนเทศอย่างเต็มรูปแบบ และส่วนมากยังต้องใช้บุคคลในการตรวจสอบความถูกต้องครบถ้วนของเอกสาร

การพัฒนาเทคโนโลยีและมาตรฐานของเอกสารรูปแบบดิจิทัล (digital document) ที่มีความน่าเชื่อถือ จะช่วยเพิ่มประสิทธิภาพและความมั่นคงปลอดภัยในการทำธุรกรรมออนไลน์ จึงเป็นที่มาของการพัฒนามาตรฐานของเอกสารรับรอง (verifiable credential: VC) ที่มีคุณสมบัติสามารถตรวจสอบได้ด้วยกระบวนการระบบรหัส (cryptography) ซึ่งถูกออกแบบมาเพื่อให้สามารถใช้งานบนโลกออนไลน์ได้เหมือนกับเอกสารรับรองในรูปแบบกายภาพ [1] [3]

ซอฟต์แวร์สำหรับการบริหารจัดการ การจัดเก็บ และการแลกเปลี่ยนเอกสารรับรอง รวมถึงข้อมูลอื่น ๆ ที่เกี่ยวข้องจะถูกเรียกว่า "กระเป๋าดิจิทัล" (digital wallet)

3.1 บทบาทและความสัมพันธ์ของเอนทิตีที่เกี่ยวข้อง

การใช้งานกระเป๋าดิจิทัล (digital wallet) สำหรับการแลกเปลี่ยนเอกสารรับรองประกอบด้วยเอนทิตีที่เกี่ยวข้อง ได้แก่ ผู้สมัคร (applicant) ผู้ออกเอกสาร (issuer) ผู้ถือเอกสาร (holder) ผู้ตรวจสอบเอกสาร (verifier) ผู้ให้บริการกระเป๋าดิจิทัล (digital wallet provider) และระบบทะเบียนเอกสารรับรอง (verifiable data registry) โดยบทบาทและความสัมพันธ์ของเอนทิตีที่เกี่ยวข้องเป็นไปตามรูปที่ 1 ซึ่งมีรายละเอียดดังนี้



รูปที่ 1 บทบาทและความสัมพันธ์เกี่ยวกับการใช้งานกระเป๋าดิจิทัล

(1) ผู้ถือเอกสาร (holder) ใช้งานและควบคุมการทำงานกระเป๋าดิจิทัลที่ให้บริการโดยผู้ให้บริการกระเป๋าดิจิทัล (digital wallet provider) โดยอาจใช้บริการในรูปแบบแอปพลิเคชันบนอุปกรณ์เคลื่อนที่หรือเว็บไซต์

(2) ผู้สมัคร (applicant) ยื่นขอเอกสารรับรองจากผู้ออกเอกสาร (issuer) พร้อมทั้งกำหนดให้จัดส่งเอกสารรับรองมายังกระเป๋าดิจิทัลของผู้ถือเอกสาร ทั้งนี้ ผู้ออกเอกสารอาจกำหนดให้ผู้สมัครกรอกข้อมูลที่เกี่ยวข้องหรือแนบเอกสารเพิ่มเติม โดยผู้ออกเอกสารมีหน้าที่ตรวจสอบความถูกต้องของข้อมูลดังกล่าว

(3) ผู้สมัคร ผู้ถือเอกสาร และเจ้าของข้อความ (subject) อาจเป็นบุคคลเดียวกันหรือไม่ก็ได้ ยกตัวอย่างเช่น บิดาเป็นผู้สมัครยื่นขอเอกสารรับรองซึ่งมีบุตรเป็นเจ้าของข้อความ จากนั้นจัดเก็บเอกสารรับรองในกระเป๋าดิจิทัลของมารดาซึ่งมีบทบาทเป็นผู้ถือเอกสาร

(4) ผู้ถือเอกสารสามารถสร้างเอกสารสำแดงโดยใช้ข้อมูลจากเอกสารรับรอง จากนั้นแสดงเอกสารสำแดงต่อผู้ตรวจสอบเอกสาร (verifier) ซึ่งทำหน้าที่ตรวจสอบความถูกต้องครบถ้วนของเอกสารสำแดงนั้น

(5) ระบบทะเบียนเอกสารรับรอง (verifiable data registry) เป็นตัวกลางในการสร้างและตรวจสอบเอกสารรับรอง โดยทำหน้าที่ลงทะเบียนตัวระบุ (identifier) และกุญแจสาธารณะ (public key) ของแต่ละเอนทิตี รวมถึงเค้าร่าง (schema) ของเอกสารรับรอง

ทั้งนี้ ผู้ออกเอกสารและผู้ตรวจสอบเอกสารอาจเป็นบุคคลซึ่งใช้งานกระเป๋าดิจิทัลเช่นเดียวกันกับผู้ถือเอกสาร โดยอาจใช้กระเป๋าดิจิทัลจากผู้ให้บริการกระเป๋าดิจิทัล หรืออาจเป็นระบบอัตโนมัติที่ทำหน้าที่เป็นกระเป๋าดิจิทัลขององค์กร (enterprise digital wallet)

3.2 เอกสารรับรองและเอกสารสำแดง

ในข้อเสนอแนะมาตรฐานฉบับนี้ เอกสารรับรอง (verifiable credential: VC) จะไม่ถูกจำกัดความหมายอยู่แค่เอกสารรับรองที่ออกโดยหน่วยงานรัฐให้แก่บุคคล แต่มีความหมายรวมถึงเอกสารอิเล็กทรอนิกส์ (electronic document) ใด ๆ ซึ่งยืนยัน (assert) ข้อความยืนยัน (claims) เกี่ยวกับเจ้าของข้อความ (subject) โดยสามารถตรวจสอบได้ว่าเอกสารรับรองนั้นไม่ถูกปลอมแปลงแก้ไข (integrity) และสามารถยืนยันตัวผู้ออกเอกสารได้ (authenticity) โดยเอกสารรับรองมีองค์ประกอบ ดังนี้

(1) คำอธิบายข้อมูล (metadata) ของเอกสารรับรอง ซึ่งอาจรวมตัวระบุ (identifier) ของเอนทิตีที่เกี่ยวข้องข้อมูลของผู้ออกเอกสาร วันหมดอายุของเอกสารรับรอง เป็นต้น

(2) ข้อความยืนยัน (claim) ซึ่งอาจมีเพียงข้อความยืนยันเดียวหรือหลายข้อความยืนยันก็ได้ โดยเป็นข้อมูลที่ยืนยัน (assert) เกี่ยวกับเจ้าของข้อความ (subject) ซึ่งอาจเป็นบุคคลธรรมดา นิติบุคคล สิ่งของ หรือซอฟต์แวร์ โดยมีข้อความยืนยัน 2 ประเภท ได้แก่ คุณลักษณะ (attribute) ของเจ้าของข้อความ และความสัมพันธ์ (relationship) ของเจ้าของข้อความต่อเอนทิตีอื่น

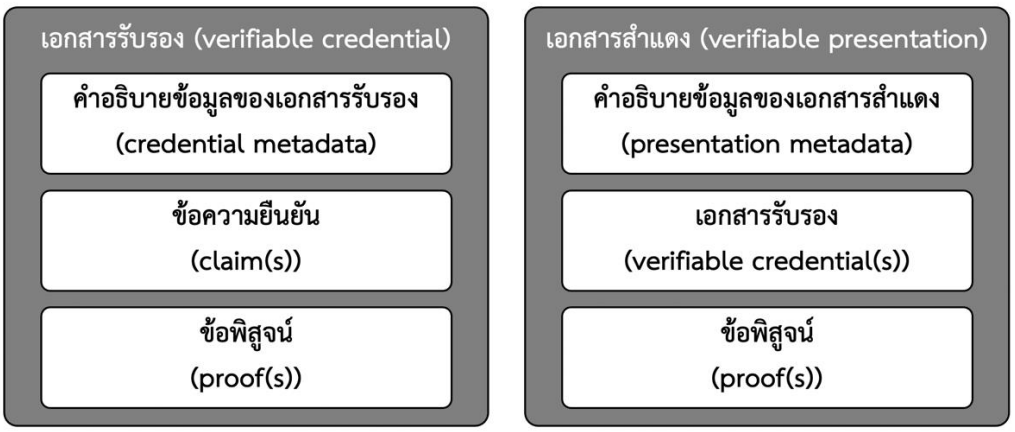
(3) ข้อพิสูจน์ (proof) ของเอกสารรับรอง ซึ่งอาจมีข้อพิสูจน์เดียวหรือหลายข้อพิสูจน์ก็ได้ โดยเป็นข้อมูลที่ถูกสร้างขึ้นจากลายมือชื่อดิจิทัล (digital signature) ของผู้ออกเอกสาร

เอกสารสำแดง (verifiable presentation: VP) คือ ชุดข้อมูลที่ผู้ถือเอกสารสร้างขึ้นจากเอกสารรับรอง โดยสามารถตรวจสอบได้ว่าเอกสารสำแดงนั้นไม่ถูกปลอมแปลงแก้ไข (integrity) และสามารถยืนยันตัวผู้ถือเอกสารได้ (authenticity) โดยเอกสารสำแดงมีองค์ประกอบ ดังนี้

(1) คำอธิบายข้อมูล (metadata) ของเอกสารสำแดง

(2) เอกสารรับรอง (verifiable credential) ซึ่งอาจมีเอกสารรับรองเดียวหรือหลายเอกสารรับรองก็ได้ ทั้งนี้เอกสารสำแดงอาจไม่ใช้เอกสารรับรองโดยตรง แต่อาจใช้ข้อมูลซึ่งสร้าง (derived) มาจากเอกสารรับรองอีกทีก็ได้

(3) ข้อพิสูจน์ (proof) ของเอกสารสำแดง ซึ่งอาจมีข้อพิสูจน์เดียวหรือหลายข้อพิสูจน์ก็ได้ โดยเป็นข้อมูลที่ถูกสร้างขึ้นจากลายมือชื่อดิจิทัล (digital signature) ของผู้ถือเอกสาร



รูปที่ 2 องค์ประกอบพื้นฐานของเอกสารรับรองและเอกสารสำแดง

ในปัจจุบัน มีมาตรฐานเกี่ยวกับเอกสารรับรองและเอกสารสำแดงจากองค์กรกำหนดมาตรฐานสากลหลายองค์กร เช่น มาตรฐาน Verifiable Credentials Data Model v1.1 จาก World Wide Web Consortium (W3C) [3] และมาตรฐาน ISO/IEC 18013-5 เกี่ยวกับใบขับขี่บนอุปกรณ์เคลื่อนที่ (mobile driving license: mDL) [4] ทั้งนี้ ข้อเสนอแนะมาตรฐานฉบับนี้จะระบุถึง "เอกสารรับรอง" และ "เอกสารสำแดง" โดยไม่เจาะจงระบุถึงมาตรฐานหรือเทคโนโลยีที่ใช้ เว้นแต่จะมีการระบุไว้เป็นอย่างอื่น

3.3 ระบบทะเบียนเอกสารรับรอง (verifiable data registry)

ในการใช้งานกระเป๋าดิจิทัลเพื่อการแลกเปลี่ยนเอกสารรับรอง เอนทิตีที่เกี่ยวข้องจะใช้งานกระเป๋าดิจิทัลร่วมกับระบบทะเบียนเอกสารรับรอง ซึ่งทำหน้าที่สนับสนุนการออกเอกสารรับรองและการตรวจสอบเอกสารสำแดง โดยมีองค์ประกอบหลัก 3 องค์ประกอบเป็นอย่างน้อย ดังนี้

- ทะเบียนตัวระบุ (identifier) และกุญแจสาธารณะ (public key)
- ทะเบียนเค้าร่างของเอกสารรับรอง (credential schema)
- ทะเบียนรายการเพิกถอนเอกสารรับรอง (revocation registry)

ทั้งนี้ ระบบทะเบียนเอกสารรับรองสามารถถูกพัฒนาและให้บริการได้ด้วยเทคโนโลยีหลากหลายรูปแบบ ทั้งในรูปแบบรวมศูนย์ (centralized) ด้วยระบบฐานข้อมูล หรือรูปแบบกระจายศูนย์ (decentralized) ด้วยเทคโนโลยีบล็อกเชน (blockchain) หรือโครงสร้างพื้นฐานใบรับเหตุการณ์กุญแจ (key event receipt infrastructure: KERI) [5] หรือให้บริการในรูปแบบผสม

หน้าที่ของระบบทะเบียนเอกสารรับรองในการสนับสนุนการออกเอกสารรับรองและการตรวจสอบเอกสารสำแดง สามารถสรุปได้ ดังนี้

(1) ผู้ถือเอกสารและผู้ออกเอกสารลงทะเบียนตัวระบุ (identifier) และกุญแจสาธารณะ (public key) ของตนเองในระบบทะเบียนเอกสารรับรอง

(2) ผู้ออกเอกสารใช้เค้าร่าง (credential schema) ที่ถูกลงทะเบียนไว้ในระบบทะเบียนเอกสารรับรองก่อนแล้ว หรือลงทะเบียนเค้าร่างใหม่

(3) ผู้ออกเอกสารออกเอกสารรับรอง ซึ่งมีโครงสร้าง (structure) เนื้อหา (content) และรูปแบบ (format) ตามเค้าร่าง โดยใช้กุญแจส่วนตัว (private key) ของผู้ออกเอกสารในการลงลายมือชื่อดิจิทัลในเอกสารรับรอง จากนั้นจัดส่งเอกสารรับรองให้กับผู้ถือเอกสาร

(4) ผู้ถือเอกสารใช้ตัวระบุของผู้ออกเอกสารในการค้นหากุญแจสาธารณะของผู้ออกเอกสารในระบบทะเบียนเอกสารรับรอง เพื่อนำมาตรวจสอบลายมือชื่อดิจิทัลของผู้ออกเอกสาร รวมทั้งตรวจสอบเอกสารรับรองว่ามีโครงสร้าง เนื้อหา และรูปแบบตามเค้าร่างหรือไม่

(5) ผู้ถือเอกสารสามารถแปลงเอกสารรับรองให้เป็นเอกสารสำแดงได้โดยการลงลายมือชื่อด้วยกุญแจส่วนตัวของผู้ถือเอกสาร จากนั้นแสดงเอกสารสำแดงต่อผู้ตรวจสอบเอกสาร

(6) ผู้ตรวจสอบเอกสารใช้ตัวระบุของผู้ออกเอกสารและตัวระบุของผู้ถือเอกสารในการค้นหากุญแจสาธารณะในระบบทะเบียนเอกสารรับรอง เพื่อนำมาตรวจสอบลายมือชื่อดิจิทัลของทั้งผู้ออกเอกสารและผู้ถือเอกสาร รวมทั้งตรวจสอบเอกสารรับรองว่ามีโครงสร้าง เนื้อหา และรูปแบบตามเค้าร่างหรือไม่

3.4 ประเภทกระเป๋าดิจิทัล

กระเป๋าดิจิทัลสามารถแบ่งประเภทตามลักษณะการจัดเก็บข้อมูล ออกเป็น 3 แบบ ดังนี้

(1) กระเป๋าดิจิทัลแบบเอดจ์ (edge wallet หรือ client-side wallet หรือ non-custodial wallet) คือ กระเป๋าดิจิทัลที่องค์ประกอบทั้งหมดจัดเก็บอยู่ในอุปกรณ์ของผู้ใช้งาน (edge device) โดยกระเป๋าดิจิทัลประเภทนี้ถือได้ว่าเป็นประเภทที่มีความมั่นคงปลอดภัยมากที่สุด แต่มีข้อเสียคือกระเป๋าดิจิทัลจะอยู่ในความรับผิดชอบของผู้ถือเอกสารโดยสมบูรณ์ และมีความไม่สะดวกในการสำรองข้อมูลและการเชื่อมโยงข้อมูล (synchronization) ระหว่างกระเป๋าดิจิทัลของผู้ถือเอกสารคนเดียวกัน

(2) กระเป๋าดิจิทัลแบบคลาวด์ (cloud wallet หรือ server-side wallet หรือ custodial wallet) คือ กระเป๋าดิจิทัลที่จัดเก็บข้อมูลทั้งหมดอยู่บนระบบคลาวด์ (cloud) ของผู้ให้บริการ โดยผู้ใช้งานสามารถบริหารจัดการกระเป๋าดิจิทัลของตนเองที่อยู่กับผู้ให้บริการผ่านทางอินเทอร์เน็ต กระเป๋าดิจิทัลประเภทนี้มีข้อดี คือ มีกลไกในการสำรองข้อมูล กู้คืนข้อมูล และเชื่อมโยงข้อมูล (synchronization) โดยอัตโนมัติ แต่มีข้อเสียในด้านความมั่นคงปลอดภัยซึ่งขึ้นอยู่กับความน่าเชื่อถือของผู้ให้บริการ

(3) กระเป๋าดิจิทัลแบบผสม (hybrid wallet) คือ กระเป๋าดิจิทัลที่จัดเก็บข้อมูลในรูปแบบผสม ภายในอุปกรณ์ของผู้ใช้งาน (edge device) และบนระบบคลาวด์ (cloud) ของผู้ให้บริการ ตัวอย่างเช่น ผู้ใช้งานสามารถจัดเก็บกุญแจส่วนตัวในอุปกรณ์ของผู้ใช้งาน และจัดเก็บข้อมูลอื่น ๆ เช่น เอกสารรับรองกับระบบคลาวด์ของผู้ให้บริการ

3.5 การสำรองและกู้คืนกุญแจเข้ารหัสลับ

กระเป๋าดิจิทัลมีหน้าที่ในการบริหารจัดการกุญแจส่วนตัวให้มีความมั่นคงปลอดภัย โดยผู้ใช้งานกระเป๋าดิจิทัลมีความเสี่ยงที่จะสูญเสียการเข้าถึงกุญแจส่วนตัว เช่น ในกรณีที่อุปกรณ์จัดเก็บกุญแจส่วนตัวสูญหายหรือชำรุด ทำให้ผู้ใช้งานไม่สามารถใช้กุญแจส่วนตัวดังกล่าวได้อีกต่อไป ดังนั้น กระเป๋าดิจิทัลจึงควรกำหนดมาตรการสำรอง (backup) และกู้คืน (recovery) ข้อมูลกุญแจส่วนตัว โดยมีแนวทางเบื้องต้น ดังนี้

(1) การกู้คืนข้อมูลแบบออนไลน์ (online recovery) เป็นการสำรองข้อมูลกุญแจส่วนตัวบนระบบคลาวด์ โดยกระเป๋าดิจิทัลควรเลือกใช้บริการจากผู้ให้บริการคลาวด์ที่น่าเชื่อถือ และควรจัดเก็บกุญแจส่วนตัวที่ถูกเข้ารหัสลับโดยอัตโนมัติ (automatic encrypted) ด้วยกุญแจส่วนตัวอื่นหรือใช้รหัสผ่านตามมาตรฐานสากล เช่น มาตรฐาน PKCS #12 [6]

(2) การกู้คืนข้อมูลแบบออฟไลน์ (offline recovery) เป็นการสำรองข้อมูลกุญแจส่วนตัวภายในอุปกรณ์ซึ่งไม่เชื่อมต่อกับเครือข่ายอินเทอร์เน็ต โดยอุปกรณ์ที่ใช้สำรองข้อมูลควรมีอายุการใช้งานยาวนานเพียงพอต่ออายุการใช้งานของกุญแจ (cryptoperiod)

(3) การกู้คืนข้อมูลแบบสังคม (social recovery) เป็นการสำรองกุญแจกับบุคคลหรือองค์กรอื่นที่ผู้ใช้งานเชื่อถือ (trustee) เช่น การใช้กระบวนการ key sharding เพื่อแบ่งข้อมูลกุญแจส่วนตัวออกเป็นหลายส่วน และให้ trustee เป็นผู้จัดเก็บ

(4) การกู้คืนข้อมูลด้วยหลายอุปกรณ์ (multi-device recovery) มีลักษณะคล้ายกับการกู้คืนกุญแจแบบสังคม แต่ใช้อุปกรณ์จัดเก็บกุญแจหลายอุปกรณ์เพื่อแบ่งการจัดเก็บข้อมูลกุญแจส่วนตัวหลายส่วน แทนการใช้ trustee

3.6 การคุ้มครองข้อมูลส่วนบุคคลของผู้ถือเอกสาร

เอกสารรับรองอาจมีข้อมูลส่วนบุคคลที่อ่อนไหว (sensitive personal information) ดังนั้น กระบวนการหรือกลไกในการคุ้มครองข้อมูลส่วนบุคคลของผู้ถือเอกสารจึงมีความสำคัญอย่างยิ่ง ผู้ออกเอกสารและผู้ให้บริการกระเป๋าดิจิทัลสามารถดำเนินการได้หลากหลายวิธีเพื่อลดการเปิดเผยข้อมูลส่วนบุคคลให้น้อยที่สุด (data minimization) โดยเฉพาะในระหว่างการแสดงเอกสารสำแดงต่อผู้ตรวจสอบเอกสาร

กลไกในการคุ้มครองข้อมูลส่วนบุคคล (privacy-preserving mechanism) ที่เป็นทางเลือกในการนำไปใช้งาน มีตัวอย่างดังนี้

(1) การเลือกเปิดเผยข้อมูลบางส่วน (selective disclosure) เป็นกระบวนการที่ผู้ถือเอกสารสามารถเลือกเปิดเผยหรือปกปิดข้อมูลบางส่วนในเอกสารรับรองได้ โดยให้ข้อมูลกับผู้ตรวจสอบเอกสารเท่าที่จำเป็นกับการทำธุรกรรมนั้น ๆ ตัวอย่างเช่น การเลือกเปิดเผยข้อมูลชื่อนามสกุล แต่ไม่เปิดเผยข้อมูลวันเดือนปีเกิดบนเอกสารรับรอง

(2) การพิสูจน์โดยไม่เปิดเผยข้อมูล (zero-knowledge proof) เป็นกระบวนการที่ผู้ถือเอกสารสามารถพิสูจน์กับผู้ตรวจสอบเอกสาร ว่าข้อความ (statement) หนึ่ง ๆ เป็นจริง โดยที่ผู้ถือเอกสารไม่ต้องเปิดเผยข้อมูลเพิ่มเติมใด ๆ นอกเหนือจากข้อเท็จจริงที่ว่าข้อความดังกล่าวนั้นเป็นความจริง เช่น การพิสูจน์ว่าผู้ใช้งานมีอายุมากกว่า 18 ปี โดยไม่จำเป็นต้องเปิดเผยวันเดือนปีเกิด

(3) การใช้ตัวระบุแบบนามแฝง (pseudonymous identifier) เป็นกระบวนการใช้นามแฝง (pseudonym) เป็นตัวระบุในการทำธุรกรรมกับเอนทิตีอื่น เพื่อหลีกเลี่ยงการใช้ตัวระบุเดิมซ้ำในการทำธุรกรรมหลายครั้ง ทำให้ผู้ตรวจสอบเอกสารหนึ่ง ๆ ไม่สามารถเชื่อมโยงได้ (unlinkability) ว่าเป็นผู้ถือเอกสารเดิมที่ทำธุรกรรม รวมทั้งป้องกันการที่ผู้ตรวจสอบเอกสารมาแลกเปลี่ยนข้อมูลกันเพื่อใช้ติดตามการใช้งานของผู้ถือเอกสารนั้น

3.7 วงจรการใช้งานกระเป๋าดิจิทัล

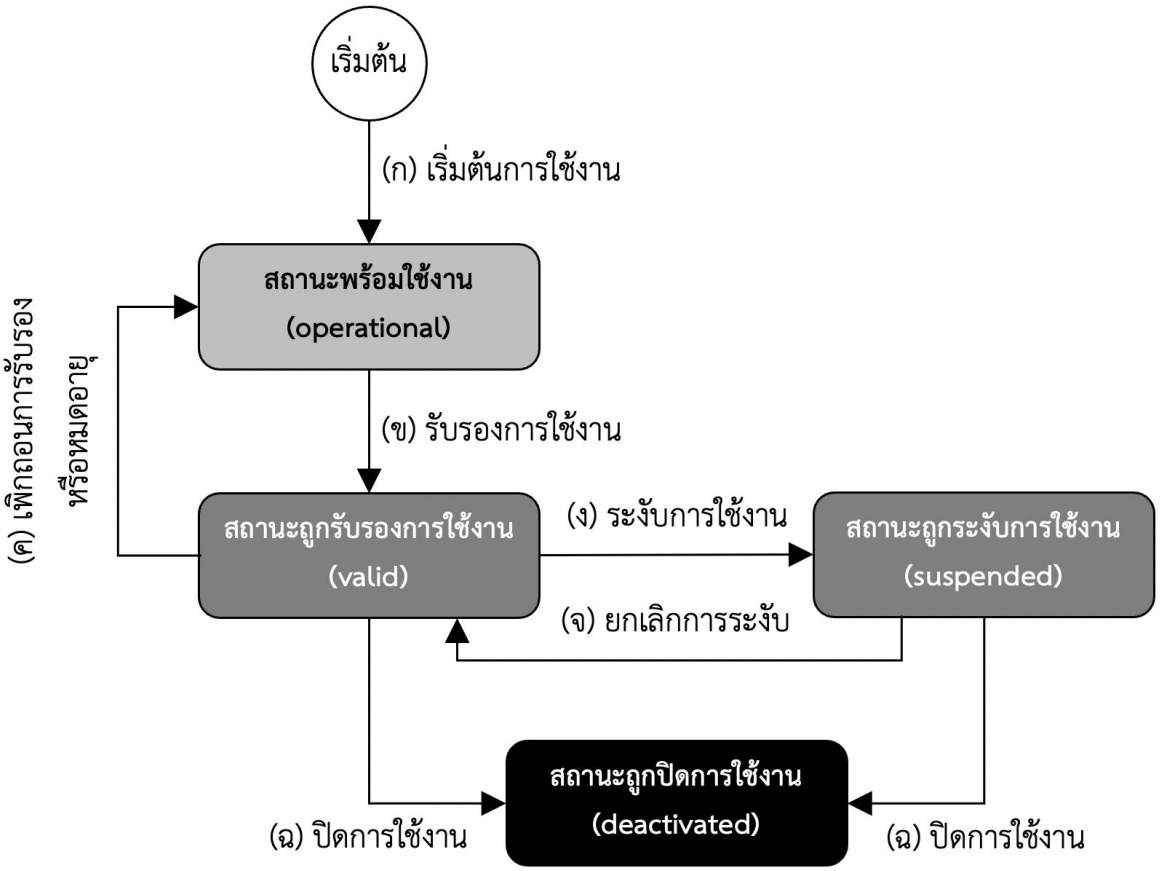
กระเป๋าดิจิทัลประกอบไปด้วยสถานะการใช้งานตลอดวงจรชีวิตการใช้งาน (life cycle) ทั้งหมด 4 สถานะ ได้แก่ สถานะพร้อมใช้งาน (operational) สถานะถูกรับรองการใช้งาน (valid) สถานะถูกระงับการใช้งาน (suspended) และ สถานะถูกปิดการใช้งาน (deactivated) โดยมีรายละเอียดตามรูปที่ 3 ดังนี้

(1) เมื่อผู้ให้บริการกระเป๋าดิจิทัลให้บริการแก่ผู้ใช้งาน กระเป๋าดิจิทัลของผู้ใช้งานนั้น (digital wallet instance) (ก) จะเริ่มต้นการใช้งานใน**สถานะพร้อมใช้งาน (operational)** โดยสามารถนำไปใช้ในการทำธุรกรรมพื้นฐานต่าง ๆ ได้ โดยเฉพาะกับธุรกรรมที่มีความเสี่ยงต่ำหรือธุรกรรมที่ไม่มีความจำเป็นต้องระบุตัวบุคคล เช่น การใช้งานสมัครสมาชิกร้านค้า และตั๋วรถโดยสารสาธารณะที่ไม่ระบุข้อมูลส่วนบุคคล

(2) เมื่อผู้ใช้งานที่เป็นเจ้าของกระเป๋าดิจิทัลได้รับการพิสูจน์ตัวตนโดยผู้ให้บริการกระเป๋าดิจิทัลหรือเอนทิตีอื่นที่เกี่ยวข้อง (ข) กระเป๋าดิจิทัลจะได้รับการรับรองและเปลี่ยนมาเป็น**สถานะถูกรับรองการใช้งาน (valid)** ทำให้กระเป๋าดิจิทัลมีความน่าเชื่อถือสำหรับการทำธุรกรรมที่มีความเสี่ยงสูงขึ้น เช่น การทำประกันภัย และ การทำธุรกรรมทางการเงิน ซึ่งสถานะถูกรับรองการใช้งานนั้นอาจ (ค) ถูกเพิกถอน (revoked) หรือหมดอายุ (expired) ทำให้กระเป๋าดิจิทัลเปลี่ยนกลับมาอยู่ในสถานะพร้อมใช้งานอีกครั้ง

(3) หากกระเป๋าดิจิทัลถูกโจรกรรมหรือสูญหาย (ง) ผู้ถือเอกสารอาจแจ้งผู้ให้บริการกระเป๋าดิจิทัลหรือเอนทิตีอื่นที่เกี่ยวข้อง เพื่อเปลี่ยนกระเป๋าดิจิทัลให้อยู่ใน**สถานะถูกระงับการใช้งาน (suspended)** ซึ่ง (จ) อาจถูกย้อนให้กลับมาอยู่ในสถานะถูกรับรองการใช้งานได้ ตามความเหมาะสม

(4) ในกรณีที่ผู้ถือเอกสารหยุดใช้บริการกระเป๋าดิจิทัล ซึ่งรวมถึงกรณีที่ผู้ถือเอกสารเสียชีวิต (ฉ) กระเป๋าดิจิทัลอาจถูกเปลี่ยนให้อยู่ใน**สถานะถูกปิดการใช้งาน (deactivated)** ทำให้กระเป๋าดิจิทัลไม่สามารถใช้งานได้อีกต่อไป



รูปที่ 3 วงจรการใช้งานกระเป๋าดิจิทัล

4. ข้อกำหนดการแลกเปลี่ยนและการใช้งานเอกสารรับรอง

การใช้งานกระเป๋าดิจิทัลให้มีความน่าเชื่อถือ ความมั่นคงปลอดภัย และการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้งานประเภทต่าง ๆ รวมถึงผู้สมัคร เจ้าของข้อความ ผู้ถือเอกสาร และผู้ตรวจสอบเอกสาร มีความจำเป็นต้องกำหนดคุณสมบัติพื้นฐานที่กระเป๋าดิจิทัลและเอกสารรับรองต้องมี ดังนี้

4.1 ช่องทางการแลกเปลี่ยนเอกสารรับรอง

กระเป๋าดิจิทัลต้องรองรับช่องทางการแลกเปลี่ยนเอกสารรับรองอย่างน้อย 1 ช่องทางจาก 4 ช่องทาง ดังนี้

(1) ช่องทางระยะใกล้โดยผู้ตรวจสอบเอกสารเป็นบุคคล (close proximity supervised flow)

(2) ช่องทางระยะใกล้โดยระบบอัตโนมัติ (close proximity unsupervised flow)

(3) ช่องทางระยะไกลข้ามอุปกรณ์ (remote cross-device flow)

(4) ช่องทางระยะไกลภายในอุปกรณ์เดียวกัน (remote same-device flow)

ช่องทางที่ (1) และ (2) เป็นช่องทางระยะใกล้ (close proximity) โดยผู้ถือเอกสารและผู้ตรวจสอบเอกสาร (human verifier) อยู่ใกล้กัน ทำให้สามารถแสดงเอกสารสำแดงได้โดยไม่จำเป็นต้องเชื่อมต่อกับอินเตอร์เน็ต เช่น การแลกเปลี่ยนเอกสารรับรองผ่าน Bluetooth หรือ Near-field communication (NFC)

โดยในช่องทางที่ (1) เป็นการแลกเปลี่ยนเอกสารรับรองกับผู้ตรวจสอบเอกสารที่เป็นบุคคล (human verifier) ส่วนในช่องทางที่ (2) เป็นการแลกเปลี่ยนเอกสารรับรองกับผู้ตรวจสอบเอกสารที่เป็นระบบอัตโนมัติ เช่น เครื่องให้บริการ (kiosk)

ช่องทางที่ (3) และ (4) เป็นช่องทางระยะไกล ซึ่งดำเนินการแลกเปลี่ยนเอกสารรับรองผ่านทางอินเทอร์เน็ต โดยในช่องทางที่ (3) ผู้ถือเอกสารใช้บริการดิจิทัลบนอุปกรณ์อื่นที่ไม่ใช่อุปกรณ์ที่กระเป๋าดิจิทัลดำเนินงานอยู่ ในกรณีนี้ กระเป๋าดิจิทัลทำหน้าที่พิสูจน์และยืนยันตัวตนผู้ถือเอกสารเพื่อใช้บริการดิจิทัลดังกล่าว เช่น การใช้กระเป๋าดิจิทัลบนอุปกรณ์เคลื่อนที่ สแกน QR code เพื่อเข้าใช้บริการเว็บไซต์บนเบราว์เซอร์ในเครื่องคอมพิวเตอร์ ส่วนในช่องทางที่ (4) ผู้ถือเอกสารใช้บริการดิจิทัลโดยใช้กระเป๋าดิจิทัลซึ่งดำเนินการภายในอุปกรณ์เครื่องเดียวกัน

4.2 ข้อกำหนดพื้นฐานที่จำเป็น

เอกสารรับรองและเอกสารสำแดงต้องมีคุณสมบัติพื้นฐานที่จำเป็น ดังนี้

(1) เอกสารรับรองและเอกสารสำแดงมีข้อมูลที่จำเป็นในการระบุและยืนยันตัวตนของผู้ออกเอกสาร (authenticity)

(2) เอกสารรับรองและเอกสารสำแดงมีข้อมูลที่จำเป็นในการตรวจสอบว่าข้อมูลในเอกสารรับรองไม่ถูกเปลี่ยนแปลง (data integrity)

(3) เอกสารรับรองและเอกสารสำแดงมีข้อมูลที่จำเป็นในการตัดสินช่วงเวลาที่สามารถใช้เอกสารรับรองได้ เช่น วันที่สามารถเริ่มใช้เอกสารรับรองได้ (validity start date) และวันหมดอายุ (expiry date)

(4) เอกสารรับรองและเอกสารสำแดงมีข้อมูลที่จำเป็นในการตรวจสอบสถานะของเอกสารรับรอง ว่าถูกยกเลิกหรือไม่

(5) เอกสารรับรองและเอกสารสำแดงมีข้อมูลที่จำเป็นในการระบุเค้าร่าง (schema) หรือข้อมูลอื่น ๆ ที่จำเป็นต่อการสร้างและตรวจสอบ

4.3 ข้อกำหนดเพิ่มเติมที่เป็นทางเลือก

เพื่อให้เอนทิตีต่าง ๆ สามารถแลกเปลี่ยนเอกสารรับรองและประมวลผลเอกสารรับรองร่วมกันได้ ผู้ออกเอกสารรับรองจำเป็นต้องรองรับการออกเอกสารรับรองที่มีความสอดคล้องกัน อีกทั้งสามารถรองรับกรณีการใช้งานที่หลากหลายและมีความยืดหยุ่นในการใช้งาน ดังนั้น ผู้ออกเอกสารควรพิจารณาออกเอกสารรับรองที่มีคุณสมบัติ ดังนี้

(1) ออกเอกสารรับรองที่มีแบบจำลองข้อมูล (data model) สอดคล้องตามมาตรฐาน W3C Verifiable Credentials Data Model 1.1 [3] หรือ ISO/IEC 18013-5:2021 [4] หรือมาตรฐานอื่น ๆ ซึ่งเป็นที่ยอมรับในระดับสากล

(2) ออกข้อความยืนยัน (claims) ซึ่งถูกเข้ารหัส (encode) ในรูปแบบมาตรฐาน Concise Binary Object Representation (CBOR) [7] หรือ JSON Web Token (JWT) [8] หรือ JSON for Linked Data (JSON-LD) [9]

(3) ออกเอกสารรับรองที่มีคุณสมบัติในการเลือกเปิดเผยข้อมูลบางส่วน (selective disclosure) ได้ โดยใช้กระบวนการที่ระบุในมาตรฐาน ISO/IEC 18013-5:2021 [4] หรือ ร่างมาตรฐาน Selective Disclosure JWT (SD-JWT) [10]

(4) สร้างลายมือชื่อดิจิทัล (digital signature) และดำเนินการเข้ารหัสลับ (encryption) ในรูปแบบมาตรฐาน Javascript Object Signing and Encryption (JOSE) [11] [12] หรือ CBOR Object Signing and Encryption (COSE) [13] หรือ Linked Data Proofs (LD-Proofs) [14]

ผู้ออกเอกสารอาจพิจารณาออกเอกสารรับรองที่มีคุณสมบัติเพิ่มเติม ดังนี้

(5) มีข้อมูลที่จำเป็นในการเชื่อมโยงเอกสารรับรองกับผู้ถือเอกสาร (holder binding) โดยอยู่ในรูปแบบข้อมูลคุณลักษณะ (attribute) ของผู้ถือเอกสารหรือข้อมูลอื่น เป็นต้น

(6) มีข้อมูลที่จำเป็นสำหรับผู้ถือเอกสารในการพิสูจน์ว่าเป็นเจ้าของเอกสารรับรองนั้นจริง

4.4 การประสานข้อมูลและการสำรองข้อมูล

กระเป๋าดิจิทัลอาจรองรับคุณสมบัติเกี่ยวกับการประสานข้อมูล (synchronization) ระหว่างอุปกรณ์ที่ใช้งานแอปพลิเคชันกระเป๋าดิจิทัลกับอุปกรณ์อื่น โดยมีจุดประสงค์ต่าง ๆ เช่น

- เพื่อการสำรองข้อมูล (backup) และการกู้คืนข้อมูล (recovery)
- เพื่อการย้ายข้อมูลไปยังกระเป๋าดิจิทัลอื่น (portability)
- เพื่อการใช้กระเป๋าดิจิทัลบนอุปกรณ์มากกว่า 1 เครื่อง (multi-device usage)

กระเป๋าดิจิทัลต้องมีคุณสมบัติเกี่ยวกับการประสานข้อมูลและการสำรองข้อมูล ดังนี้

(1) มีข้อมูลที่จำเป็นในการขอเอกสารรับรองใหม่ (re-issuance)

(2) ในกรณีที่รองรับการประสานข้อมูล เอกสารรับรองสามารถใช้งานได้ด้วยกระเป๋าดิจิทัลบนอุปกรณ์อื่น แม้ว่าผู้ถือเอกสารจะไม่สามารถเข้าถึงอุปกรณ์ดั้งเดิมที่ใช้รับการออกเอกสารรับรองนั้น

(3) ในกรณีที่รองรับการกู้คืนข้อมูล เอกสารรับรองสามารถถูกกู้คืนข้อมูลได้โดยเจ้าของข้อความ (subject) หรือตัวแทนที่ได้รับอนุญาตเท่านั้น

โดยเอกสารรับรองและกระเป๋าดิจิทัลอาจมีคุณสมบัติเพิ่มเติมตามความเหมาะสม ดังนี้

(4) สามารถส่งออกข้อมูลความลับ (secret material) เช่น กุญแจส่วนตัว (private key) หรือข้อมูลที่เชื่อมโยงกับผู้ถือเอกสาร (holder binding value) ซึ่งเกี่ยวข้องกับการประสานข้อมูลและการกู้คืนข้อมูล

ทั้งนี้ ในกรณีที่เอกสารรับรองมีจุดประสงค์ในการใช้งานกับธุรกรรมที่มีความเสี่ยงสูง ผู้ออกเอกสารอาจพิจารณาออกเอกสารรับรองให้กับอุปกรณ์หรือแอปพลิเคชันกระเป๋าดิจิทัลที่ไม่มีคุณสมบัติในการประสานข้อมูล ทำให้ไม่สามารถส่งออกข้อมูลเอกสารรับรองหรือข้อมูลความลับ (secret material) ที่เกี่ยวข้องกล่าวคือเอกสารรับรองนั้นถูกออกแบบให้ผูกติดกับอุปกรณ์ดั้งเดิมที่ใช้รับเอกสารรับรองดังกล่าว (device-bound credential)

5. องค์ประกอบพื้นฐานและตัวอย่างการดำเนินงาน

การกำหนดองค์ประกอบพื้นฐาน (basic components) และตัวอย่างการดำเนินงาน (reference implementation) ของกระเป๋าดิจิทัล จะช่วยส่งเสริมให้เกิดการทำงานร่วมกันได้ (interoperability) ระหว่างกระเป๋าดิจิทัลจากผู้ให้บริการที่แตกต่างกัน รวมถึงส่งเสริมให้การแลกเปลี่ยนเอกสารรับรองระหว่างเอนทิตีต่าง ๆ เป็นไปอย่างราบรื่น

5.1 องค์ประกอบพื้นฐาน

กระเป๋าดิจิทัลมีองค์ประกอบพื้นฐาน ซึ่งผู้ให้บริการกระเป๋าดิจิทัลสามารถเลือกองค์ประกอบมาพัฒนาแอปพลิเคชันกระเป๋าดิจิทัลได้ตามความเหมาะสม ดังต่อไปนี้

(1) **ที่จัดเก็บกุญแจเข้ารหัสลับ (cryptographic keys storage)** เป็นที่จัดเก็บของข้อมูลรหัสลับ (cryptographic secrets) รวมถึงกุญแจส่วนตัว (private key) และข้อมูลรหัสอื่นที่เกี่ยวกับเอกสารรับรองและการเชื่อมโยงกับตัวตนผู้ถือเอกสาร (holder binding)

(2) **อินเตอร์เฟสสำหรับผู้ตรวจสอบเอกสาร (verifier interface)** เป็นองค์ประกอบที่ทำหน้าที่อำนวยการแลกเปลี่ยนข้อมูลระหว่างผู้ถือเอกสารและผู้ตรวจสอบเอกสาร ซึ่งผู้ตรวจสอบสามารถร้องขอ (request) เอกสารรับรองจากกระเป๋าดิจิทัล โดยอาจแลกเปลี่ยนข้อมูลได้ทั้งในรูปแบบออนไลน์หรือออฟไลน์

(3) **โพรโทคอลการจัดส่งเอกสารรับรอง (credential transport protocol)** เป็นโพรโทคอลที่นิยามขั้นตอนการแลกเปลี่ยนข้อมูลระหว่างเอนทิตี รวมถึงรูปแบบ (format) ของข้อมูลร้องขอ (request) และข้อมูลตอบกลับ (response) ซึ่งอาจเกิดขึ้นระหว่างการยืนยันตัวตน (authentication) การออกเอกสารรับรอง (issuance) หรือการแสดงเอกสารสำแดง (presentation) ก็ได้ ยกตัวอย่างเช่น

- การใช้โพรโทคอลในกลุ่ม OpenID4VC ซึ่งประกอบไปด้วย 3 มาตรฐาน ได้แก่ SIOPv2 [15], OpenID4VP [16] และ OpenID4VCI [17]
- โพรโทคอลสำหรับการแลกเปลี่ยนเอกสารรับรองระยะใกล้ (close proximity) ที่ระบุใน ISO/IEC 18013-5:2021 [4]
- DIDComm Messaging v2 [18]
- โพรโทคอลการออกเอกสารรับรองและการแสดงเอกสารสำแดงใน (ร่าง) มาตรฐาน ISO/IEC 23220-3 [19] สำหรับ และ (ร่าง) มาตรฐาน ISO/IEC 23220-4 [20]

(4) **แบบจำลองข้อมูลของเอกสารรับรอง (credential data model)** นิยามและอธิบายคุณสมบัติและความสัมพันธ์ระหว่างข้อมูลองค์ประกอบภายในเอกสารรับรอง ยกตัวอย่างเช่น

- มาตรฐาน W3C VC Data Model v1.1 [3] ซึ่งรวมถึง (ร่าง) มาตรฐานเสริม IETF SD-JWT [10]
- มาตรฐานแบบจำลองข้อมูลที่ระบุใน ISO/IEC 18013-5:2021 [4]

ทั้งนี้ ทั้งสองตัวอย่างถูกรวมอยู่ภายใต้ (ร่าง) มาตรฐาน ISO/IEC 23220-2 [21]

(5) **เค้าร่างของเอกสารรับรอง (credential schemas)** ประกอบด้วยโครงสร้างและการจัดกลุ่มข้อมูลซึ่งนิยามคุณสมบัติของเอกสารรับรอง ทั้งนี้ เค้าร่างอาจมีข้อมูลเพิ่มเติมอื่น เช่น วิธีการตรวจสอบเอกสาร

รับรอง (verification mechanisms) ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance) การพิสูจน์ความเป็นเจ้าของ (proof of possession) ของผู้ใช้งาน

(6) **รูปแบบของเอกสารรับรอง (credentials formats)** ใช้ในการแสดงผลของเอกสารรับรองที่ได้รับการลงลายมือชื่อดิจิทัลและสามารถตรวจสอบได้ โดยอาจมีข้อมูลเพิ่มเติมอื่นเพื่อจุดประสงค์ในด้านการทำงานร่วมกัน (interoperability) ยกตัวอย่างเช่น

- JSON Web Token (JWT) [8]
- JSON for Linked Data (JSON-LD) [9]
- Concise Binary Object Representation (CBOR) [7]

(7) **รูปแบบการลงลายมือชื่อดิจิทัล (signature formats)** ใช้ในการแสดงผลลายมือชื่อดิจิทัล โดยขึ้นอยู่กับรายละเอียดทางเทคนิคและวิธีการทางคณิตศาสตร์ ยกตัวอย่างเช่น

- Javascript Object Signing and Encryption (JOSE) [11] [12]
- CBOR Object Signing and Encryption (COSE) [13]
- Linked Data Proofs (LD-Proofs) [14]

(8) **ชุดเครื่องมือและกลไกการเข้ารหัสลับ (cryptographic suites and mechanisms)** เป็นอัลกอริทึมและกระบวนการรักษาความมั่นคงปลอดภัยในการแลกเปลี่ยนข้อมูล ทั้งในด้านการรักษาความลับ (confidentiality) และความถูกต้องครบถ้วน (integrity) ของข้อมูล ยกตัวอย่างเช่น

- Edwards-curve Digital Signature Algorithm (EdDSA)
- Rivest–Shamir–Adleman (RSA) algorithm
- Hash-based Message Authentication Code (HMAC)

(9) **ตัวระบุของเอนทิตี (entity identifiers)** ซึ่งเป็นตัวระบุเฉพาะที่ไม่ซ้ำกัน (globally unique identifiers) สำหรับทุก ๆ องค์ประกอบในแบบจำลองข้อมูล ยกตัวอย่างเช่น

- Uniform Resource Locator (URL)
- Decentralized Identifier (DID) [22]

(10) **กลไกการตรวจสถานะของเอกสารรับรอง (validity status check)** เป็นกลไกในการเผยแพร่ (publish) และรับข้อมูล (obtain) สถานะของเอกสารรับรอง เช่น สถานะการระงับหรือการเพิกถอนเอกสารรับรอง ยกตัวอย่างเช่น

- W3C Status List 2021 [23]
- Certificate revocation list (CRL)

5.2 ตัวอย่างการดำเนินการของกระเป๋าดิจิทัล

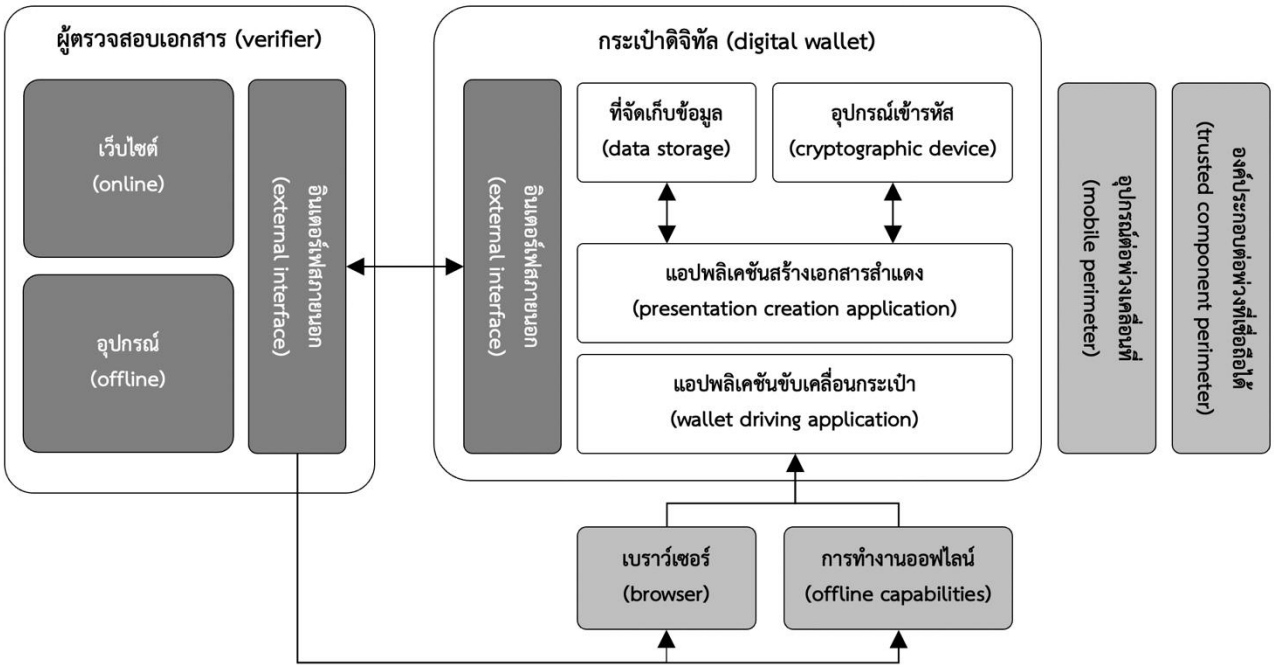
ตัวอย่างการดำเนินการ (reference Implementation) แสดงถึงตัวอย่างอ้างอิงสำหรับการออกแบบกระเป๋าดิจิทัล ซึ่งคำนึงถึงช่องทางการแลกเปลี่ยนข้อมูลทั้งระยะใกล้และไกล และคำนึงถึงสถานการณ์ที่

ผู้ใช้งานหรือผู้ตรวจสอบเอกสารอาจมีสถานะออฟไลน์ โดยที่ยังคงมีความยืดหยุ่นในการพัฒนาแอปพลิเคชันตามความเหมาะสมต่อกรณีการใช้งานที่หลากหลาย

ตัวอย่างเช่นในกรณีที่แอปพลิเคชันกระเป๋าดิจิทัลดำเนินการอยู่บนอุปกรณ์อุปกรณ์เคลื่อนที่ (mobile device) อาจมีความจำเป็นต้องใช้องค์ประกอบที่เชื่อถือได้ (trusted component) เพิ่มเติม ซึ่งไม่ใช่ส่วนหนึ่งของแอปพลิเคชันนั้น แต่ยังถือว่าเป็นส่วนหนึ่งของกระเป๋าดิจิทัล เช่น ฮาร์ดแวร์ภายนอกสำหรับการจัดเก็บข้อมูล (external trusted storage) หรือองค์ประกอบอื่นที่เชื่อมต่อกับอุปกรณ์มือถือจากทางไกล (remote components)

5.2.1 ภาพรวมและองค์ประกอบ

ตัวอย่างการดำเนินการอ้างอิงของกระเป๋าดิจิทัลมีภาพรวมและองค์ประกอบซึ่งจัดรวมกลุ่มโดยคำนึงถึงคุณสมบัติการใช้งาน (functional block) ตามที่แสดงในรูปที่ 4 ดังนี้



รูปที่ 4 ภาพรวมและองค์ประกอบ

(1) อุปกรณ์เข้ารหัสลับ (cryptographic device) ซึ่งมีองค์ประกอบย่อย ได้แก่

- กุญแจเข้ารหัสลับของผู้ใช้งาน (user keys) และใบรับรองอิเล็กทรอนิกส์ (digital certificate)
- อัลกอริทึมระบบรหัสลับ (cryptographic algorithms) รวมถึงอัลกอริทึมสำหรับระบบรหัสแบบสมมาตร (symmetric) ระบบรหัสแบบอสมมาตร (asymmetric) และฟังก์ชันแฮช (hash function) เป็นต้น
- อุปกรณ์ฮาร์ดแวร์ secure environment สำหรับกุญแจเข้ารหัสลับและข้อมูลรหัสลับ เช่น trusted platform module (TPM) และ hardware security module (HSM) ซึ่งอาจอยู่ภายในอุปกรณ์ที่ดำเนินการกระเป๋าดิจิทัลหรือเชื่อมต่อทางไกล

(2) ที่จัดเก็บข้อมูล (data storage) ซึ่งมีองค์ประกอบย่อย ได้แก่

- ตัวระบุเฉพาะ (unique identifier) ของผู้ใช้งาน
- เอกสารรับรอง (credentials)
- ข้อมูลอื่น ๆ สำหรับการยืนยันตัวตน เช่น เลขรหัสส่วนตัว (personal identification number: PIN) และ ข้อมูลชีวมิติ (biometrics)

(3) แอปพลิเคชันสร้างเอกสารสำแดง (presentation creation application) ซึ่งมีองค์ประกอบย่อย ได้แก่

- บันทึกเหตุการณ์ (logs) และประวัติการใช้งานกระเป๋าดิจิทัล
- ตัวระบุเฉพาะ (unique identifier) ของกระเป๋าดิจิทัล (wallet instance)
- ข้อมูลของแอปพลิเคชันกระเป๋าดิจิทัล เช่น การตั้งค่า (configuration) ข้อมูลของผู้ผลิต (manufacturer) และเวอร์ชันของกระเป๋าดิจิทัล

(4) แอปพลิเคชันสนับสนุนการใช้งานกระเป๋า (wallet driving application) ซึ่งมีองค์ประกอบย่อย ได้แก่

- หน้าจอหรืออินเตอร์เฟสอื่นสำหรับผู้ใช้งาน

(5) อินเตอร์เฟสภายนอก (external interface) ซึ่งมีองค์ประกอบย่อย ได้แก่

- อินเตอร์เฟสสำหรับแลกเปลี่ยนข้อมูลกับเอนทิตีอื่น
- ช่องทางแลกเปลี่ยนข้อมูล (communication channels) ซึ่งอาจเป็นช่องทางในรูปแบบออนไลน์หรือออฟไลน์

(6) อุปกรณ์ต่อพ่วงเคลื่อนที่ (mobile perimeter) ซึ่งมีองค์ประกอบย่อย ได้แก่

- ข้อมูลของอุปกรณ์ รวมถึง ประเภทอุปกรณ์ การตั้งค่า เวอร์ชันของเฟิร์มแวร์ (firmware)
- เซ็นเซอร์ของอุปกรณ์ รวมถึง กล้องถ่ายรูป เครื่องอ่าน NFC เครื่องอ่านลายนิ้วมือ มาตรวัดความเร่ง (accelerometer)

(7) องค์ประกอบต่อพ่วงที่เชื่อถือได้ (trusted components perimeter) ซึ่งมีองค์ประกอบย่อย ได้แก่

- ข้อมูลของอุปกรณ์ที่เชื่อมต่อ
- กุญแจเข้ารหัสลับของระบบ (system keys) และใบรับรองอิเล็กทรอนิกส์ (Certificates)
- ระบบ back-end เช่น เซิร์ฟเวอร์ฐานข้อมูล (database servers)

5.2.2 รายละเอียดตัวอย่างการดำเนินการ

(1) ที่จัดเก็บกุญแจเข้ารหัสลับ (cryptographic key storage) อาจรองรับการใช้งานร่วมกับ trusted execution environment (TEE) หรืออุปกรณ์ภายนอกอื่น เช่น สมาร์ทการ์ด รวมทั้งรองรับการเชื่อมต่อกับองค์ประกอบอื่นทางไกล เช่น การเชื่อมต่อกับ hardware security module (HSM) ทางไกล ทั้งนี้ อาจมีมาตรการความมั่นคงปลอดภัยเพื่อป้องกันการส่งออกข้อมูลการเข้ารหัสลับ (cryptographic secret) สำหรับธุรกรรมที่มีความเสี่ยงสูง

(2) กระเป๋าดิจิทัลแลกเปลี่ยนข้อมูลกับผู้ตรวจสอบเอกสาร โดยใช้ข้อมูลที่ถูกเข้ารหัส (encoded) ในรูปแบบ Uniform Resource Identifier (URI)

- ข้อมูลในคำร้องขอ (request) ต้องสอดคล้องตามมาตรฐาน OpenID4VP [17]
- ในกรณีที่ผู้ตรวจสอบเอกสารอนุญาตการแลกเปลี่ยนข้อมูลผ่านนามแฝง (pseudonymous identification) ข้อมูลในคำร้องขอ (request) ต้องสอดคล้องตามมาตรฐาน OpenID SIOPv2 [15]
- คำร้องขอการแสดงเอกสารสำแดง (presentation request) ควรถูกเข้ารหัส (encoded) ในรูปแบบ WWW URI
- เอกสารสำแดงต้องมีข้อมูลของคำร้องขอ (request object) ในรูปแบบ JWT ซึ่งลงลายมือชื่อดิจิทัลโดยผู้ส่งคำร้องขอ (requester) ด้วยกุญแจส่วนตัวอยู่ในความควบคุมของผู้ส่งคำร้องขอแต่เพียงผู้เดียว อีกทั้งใช้กลไกการลงลายมือชื่อดิจิทัลที่น่าเชื่อถือ

(3) ในระหว่างการแลกเปลี่ยนข้อมูล กระเป๋าดิจิทัลควรดำเนินการตรวจสอบเซสชันการสื่อสาร (session binding)

(4) โพรโทคอลการจัดส่งข้อมูล (transport protocols) สามารถแบ่งออกได้เป็นการจัดส่งสำหรับการออกเอกสารรับรอง (issuance transport) และการแสดงเอกสารสำแดง (presentation transport)

- การออกเอกสารรับรอง (issuance transport) ควรใช้ OpenID4VCI
- การแสดงเอกสารสำแดง (presentation transport) ต้องใช้ OpenID4VP สำหรับการแลกเปลี่ยนข้อมูลระยะไกล และใช้โพรโทคอลที่ระบุใน ISO/IEC 18013-5:2021 สำหรับการแลกเปลี่ยนข้อมูลระยะใกล้

(5) การใช้งานเอกสารรับรองและเอกสารสำแดงต้องสอดคล้องตามมาตรฐานแบบจำลองข้อมูลที่ระบุในมาตรฐาน W3C Verifiable Credentials Data Model 1.1 หรือ ISO/IEC 18013-5:2021

(6) ใช้รูปแบบของเอกสารรับรองตามมาตรฐาน JWT หรือ CBOR หรือ JSON-LD โดยอาจรองรับ (ร่าง) มาตรฐาน SD-JWT ร่วมด้วย

(7) ใช้รูปแบบของการลงลายมือชื่อดิจิทัลตามมาตรฐาน JOSE หรือ COSE หรือ LD-Proofs

(8) การเลือกเปิดเผยข้อมูลบางส่วน (selective disclosure) สามารถดำเนินการได้ด้วยการลงลายมือชื่อบนชุดข้อมูลที่ผ่านฟังก์ชันแฮชด้วย salt (signed logical grouping of salted hash digests) ตามที่ระบุในมาตรฐาน ISO/IEC 18013-5:2021 หรือ (ร่าง) มาตรฐาน SD-JWT

(9) ใช้ certificate revocation list (CRL) หรือ W3C Status List 2021 ในการตรวจสอบสถานะของใบรับรอง

6. ข้อกำหนดของโพรโทคอลการแลกเปลี่ยนข้อมูล

การแลกเปลี่ยนข้อมูลระหว่างกระเป๋าดิจิทัลของเอนทิตี ทั้งการออกเอกสารรับรองจากผู้ออกเอกสารไปยังผู้ถือเอกสาร และการแสดงเอกสารสำแดงจากผู้ถือเอกสารไปยังผู้ตรวจสอบเอกสารมีความจำเป็นต้องใช้โพรโทคอลการแลกเปลี่ยนข้อมูลเฉพาะที่มีความเหมาะสมกับลักษณะการใช้งานดังกล่าว

ปัจจุบัน โพรโทคอลการแลกเปลี่ยนข้อมูลยังเป็นเทคโนโลยีที่มีการเปลี่ยนแปลงอย่างรวดเร็ว มีมาตรฐานจาก

หลายองค์กรที่มีลักษณะการใช้งานที่คล้ายคลึงกัน เช่น โพรโทคอลในกลุ่ม OpenID4VC [15] [16] [17], ISO/IEC 18013-5:2021 [4] และ DIDComm Messaging v2 [18] ดังนั้น ข้อเสนอแนะมาตรฐานฉบับนี้จะไม่ระบุว่าผู้ให้บริการกระเป๋าดิจิทัลควรเลือกใช้มาตรฐานใด แต่จะระบุคุณสมบัติที่โพรโทคอลการแลกเปลี่ยนข้อมูลควรมี ดังนี้

6.1 คุณสมบัติพื้นฐานที่จำเป็น

โพรโทคอลการแลกเปลี่ยนข้อมูลระหว่างกระเป๋าดิจิทัล เช่น ระหว่างผู้ออกเอกสารและผู้ถือเอกสาร หรือระหว่างผู้ถือเอกสารและผู้ตรวจสอบเอกสาร มีคุณสมบัติพื้นฐานที่จำเป็นต้องมี ดังต่อไปนี้

(1) มีความมั่นคงปลอดภัย (secure) โดยการรักษาความถูกต้องครบถ้วนของข้อความ (integrity) สามารถตรวจสอบที่มาและยืนยันตัวตนผู้ส่งข้อความ (authenticity) และใช้ระบบรหัสที่ทันสมัยในการเข้ารหัสลับ (encryption) และการถอดรหัสลับ (decryption) เพื่อการรักษาความลับของข้อความ (confidentiality)

(2) รักษาความเป็นส่วนตัวของผู้ใช้งาน (private) โดยป้องกันบุคคลอื่นที่ไม่ได้รับอนุญาต (unauthorized third parties) ไม่ให้รู้ว่าผู้ส่งและผู้รับข้อความเป็นใคร กำลังสื่อสารเกี่ยวกับอะไร และสื่อสารเมื่อใด

(3) สามารถทำงานร่วมกันกับกระเป๋าดิจิทัลอื่นได้ (interoperable) โดยสามารถทำงานบนแพลตฟอร์มและระบบปฏิบัติการ (operating system: OS) ที่หลากหลาย เช่น Android, iOS, Windows และ Linux สามารถใช้งานได้ด้วยหลายภาษาโปรแกรม (programming language) รวมถึงสามารถทำงานร่วมกับระบบทะเบียนเอกสารรับรองที่หลากหลาย เช่น การใช้งานร่วมกับบล็อกเชนได้หลายเครือข่าย

6.2 คุณสมบัติเพิ่มเติมที่เป็นทางเลือก

โพรโทคอลการแลกเปลี่ยนข้อมูลระหว่างกระเป๋าดิจิทัลอาจมีคุณสมบัติเพิ่มเติมที่เป็นทางเลือก โดยผู้ให้บริการกระเป๋าดิจิทัลสามารถเลือกใช้ตามความเหมาะสมกับลักษณะการใช้งาน ดังนี้

(1) ผู้ถือเอกสารสามารถแสดงเอกสารสำแดงได้โดยไม่เปิดเผยตัวตนหรือชื่อได้ (anonymous) ในกรณีที่ผู้ตรวจสอบเอกสารไม่มีความจำเป็นต้องระบุตัวตนของผู้ถือเอกสาร

(2) ผู้ถือเอกสารสามารถเลือกเปิดเผยข้อมูลในเอกสารสำแดง (selective disclosure) ได้ โดยเปิดเผยข้อมูลแก่ผู้ตรวจสอบเอกสารเท่าที่จำเป็นต้องใช้

(3) ผู้ถือเอกสารสามารถเลือกไม่ให้ถูกติดตามการใช้งาน (unlinkability) จากการแสดงเอกสารสำแดงเดิมหลายครั้ง นั้นคือผู้ตรวจสอบเอกสารมากกว่าหนึ่งคนไม่สามารถแลกเปลี่ยนข้อมูลเพื่อติดตามการใช้งานของผู้ถือเอกสาร

(4) สามารถใช้งานได้กับการขนส่งข้อมูลหลากหลายรูปแบบ (transport-agnostic) เช่น สามารถใช้งานได้กับ HTTPS เวอร์ชัน 1.x และ 2.0, WebSockets, BlueTooth, Near-field Communication (NFC) รวมถึงรองกับการทำงานทั้งแบบออนไลน์ (online) และออฟไลน์ (offline) แบบ synchronous และแบบ asynchronous เป็นต้น

(5) มีความกระจายศูนย์ (decentralized) โดยเป็นการแลกเปลี่ยนข้อมูลในรูปแบบ end-to-end นั้นคือเป็นการแลกเปลี่ยนข้อมูลระหว่างข้อมูลระหว่างเอนทิตีโดยตรง และทำการเข้ารหัสข้อมูลก่อนการส่งทุกครั้งหากต้องอาศัยตัวกลางในการแลกเปลี่ยนข้อมูล

504 **บรรณานุกรม**

505

[1] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยโครงสร้างข้อมูลของเอกสารรับรองและเอกสารสำแดง เลขที่ ขมธอ. 24-2563, เวอร์ชัน 1.0.

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

[3] World Wide Web Consortium (W3C), "Verifiable Credentials Data Model) v1.1", 03 March 2022.

[4] ISO/IEC 18013-5:2021 Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application.

[5] Samuel M. Smith, "Key Event Receipt Infrastructure (KERI)", arXiv:1907.02143, 2021.

[6] Internet Engineering Task Force, RFC 7292, "PKCS #12: Personal Information Exchange Syntax v1.1", July 2014.

[7] Internet Engineering Task Force, RFC 8949, "Concise Binary Object Representation (CBOR)", December 2020.

[8] Internet Engineering Task Force, RFC 7519, "JSON Web Token (JWT)", May 2015.

[9] World Wide Web Consortium (W3C). "JSON-LD 1.1", 16 July 2020.

[10] Internet Engineering Task Force, "Selective Disclosure JWT (SD-JWT)", Internet-Draft, 11 July 2022.

[11] Internet Engineering Task Force, RFC 7515, "JSON Web Signature (JWS)", May 2015.

[12] Internet Engineering Task Force, RFC 7516, "JSON Web Encryption (JWE)", May 2015.

[13] Internet Engineering Task Force, RFC 8152, "CBOR Object Signing and Encryption (COSE)", July 2017.

[14] World Wide Web Consortium (W3C), "Verifiable Credential Data Integrity 1.0", First Draft, 10 November 2022..

[15] OpenID Foundation, "Self-Issued OpenID Provider v2", 1 January 2023..

[16] OpenID Foundation, "OpenID for Verifiable Credential Issuance", 30 December 2022.

[17] OpenID Foundation, "OpenID for Verifiable Presentations", 30 December 2022.

[18] Decentralized Identity Foundation, "DIDComm Messaging v2", Editor’s Draft.

[19] ISO/IEC AWI TS 23220-3 Cards and security devices for personal identification — Building blocks for identity management via mobile devices — Part 3: Protocols and services for issuing phase.

[20] ISO/IEC AWI TS 23220-4 Cards and security devices for personal identification — Building blocks for identity management via mobile devices — Part 4: Protocols and services for operational phase.

[21] ISO/IEC AWI TS 23220-2 Cards and security devices for personal identification — Building blocks for identity management via mobile devices — Part 2: Data objects and encoding rules for generic eID systems.

[22] World Wide Web Consortium (W3C), "Decentralized Identifiers (DIDs) v1.0", 19 July 2022.

[23] World Wide Web Consortium, "Status List 2021", W3C Editor's Draft, 08 January 2023.

[24] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ เลขที่ ขมธอ. 11-2560, เวอร์ชัน 1.0.

[25] World Wide Web Consortium, "Web Authentication: An API for accessing Public Key Credentials Level 2", 8 April 2021.

[26] Internet Engineering Task Force, "Authentic Chained Data Containers (ACDC)", Internet-Draft, 17 November 2022.

[27] International Civil Aviation Organization, "Doc 9303 Machine Readable Travel Documents", Eighth Edition, 2021.

[28] ISO 14641:2018 Electronic document management — Design and operation of an information system for the preservation of electronic documents — Specifications.

[29] National Institute of Standards and Technology Federal Information Processing Standards Publication 800-57 Part 1 Rev. 5, "Recommendation for Key Management", 2020.

[30] Alex Preukschat and Drummond Reed, "Self-Sovereign Identity", Manning Publications, 2021, Manning Publications, 2021.

[31] European Commission, "European Digital Identity Architecture and Reference Framework – Outline", 22 February 2022.

[32] Digital ID & Authentication Council of Canada, "Pan-Canadian Trust Framework Glossary", 2020.

506
507