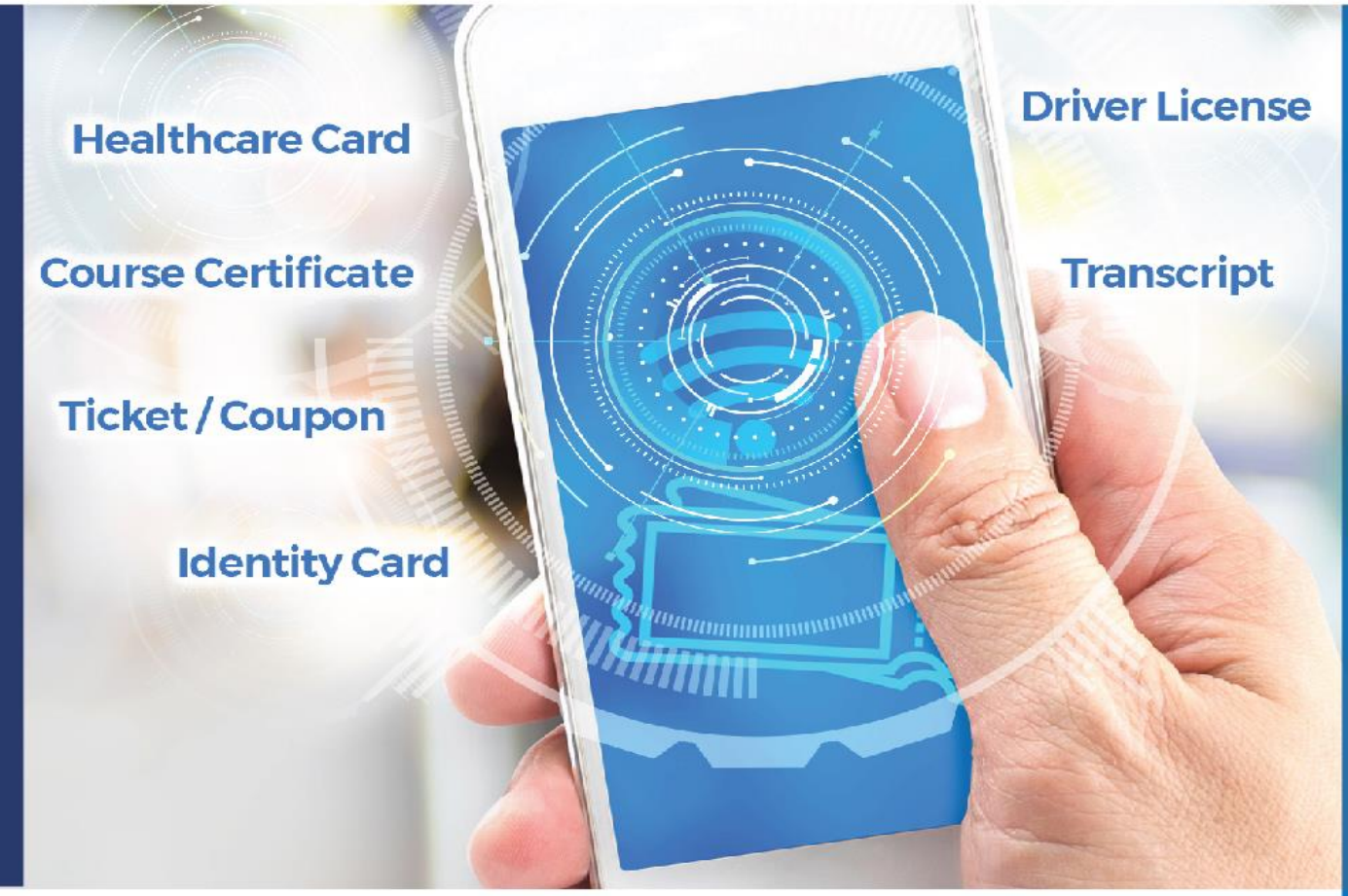


รายงานทางเทคนิค

Technical Report

กรอบการทำงานร่วมกัน ของกระเป๋าดิจิทัลสำหรับเอกสารรับรอง

Interoperable Framework of Digital Wallets
for Verifiable Credentials

เวอร์ชัน 1.0 - เมษายน 2566

รายงานทางเทคนิค

Technical Report

กรอบการทำงานร่วมกันของกระเป๋าดิจิทัลสำหรับเอกสารรับรอง

INTEROPERABLE FRAMEWORK OF DIGITAL WALLETS FOR VERIFIABLE CREDENTIALS

เวอร์ชัน 1.0

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

เมษายน 2566

คำนำ

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

ทั้งนี้ เพื่อให้การให้บริการกระเป๋าดิจิทัลมีความน่าเชื่อถือและเป็นที่ยอมรับ โดยเฉพาะอย่างยิ่ง การใช้เพื่อพิสูจน์และยืนยันตัวตนทางดิจิทัล ซึ่งเป็นบริการที่มีความสำคัญและช่วยสร้างความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์จึงได้จัดทำรายงานทางเทคนิค เรื่อง กรอบการทำงานร่วมกันของกระเป๋าดิจิทัลสำหรับเอกสารรับรอง เพื่ออธิบายหลักการทำงาน วงจรชีวิต องค์ประกอบ และข้อแนะนำของกระเป๋าดิจิทัลและเอกสารรับรอง (verifiable credential: VC) ที่จัดเก็บในกระเป๋าดิจิทัล เพื่อให้ผู้ให้บริการกระเป๋าดิจิทัล (digital wallet provider) และผู้พัฒนาที่เกี่ยวข้องมีแนวทางในการให้บริการที่มีความมั่นคงปลอดภัย คุ้มครองข้อมูลส่วนบุคคล และสามารถทำงานร่วมกันได้ รวมถึงช่วยส่งเสริมให้เกิดบริการกระเป๋าดิจิทัลสำหรับเอกสารรับรองในประเทศไทย

รายงานฉบับนี้มีวัตถุประสงค์เพื่อเป็นแนวทางอ้างอิงในการดำเนินการ (reference implementation) ให้กระเป๋าดิจิทัลในประเทศไทยสามารถทำงานร่วมกันได้ และช่วยจำกัดความซับซ้อนของรายละเอียดทางเทคนิค (technical solution) ที่แตกต่างกันจำนวนมาก ผู้ให้บริการกระเป๋าดิจิทัลสามารถนำรายงานฉบับนี้ไปปรับใช้เป็นแนวทางได้ตามความเหมาะสม อย่างไรก็ตาม รายงานฉบับนี้อาจมีการปรับปรุงเนื้อหาเพิ่มเติมตามลักษณะการใช้งานในประเทศไทยและการเปลี่ยนแปลงของเทคโนโลยีในอนาคต

สารบัญ

สารบัญรูป

สารบัญตาราง

รายงานทางเทคนิค

กรอบการทำงานร่วมกันของกระเป๋าดิจิทัลสำหรับเอกสารรับรอง

1. ขอบข่าย

รายงานทางเทคนิคฉบับนี้อธิบายหลักการทำงาน วงจรชีวิต องค์ประกอบ และข้อแนะนำของกระเป๋าดิจิทัลและเอกสารรับรอง (verifiable credential: VC) ที่จัดเก็บในกระเป๋าดิจิทัล เพื่อให้ผู้ให้บริการกระเป๋าดิจิทัล (digital wallet provider) และผู้พัฒนาที่เกี่ยวข้องมีแนวทางในการให้บริการที่มีความมั่นคงปลอดภัย คุ้มครองข้อมูลส่วนบุคคล และสามารถทำงานร่วมกันได้

รายงานฉบับนี้อ้างอิงเนื้อหาจากเอกสาร The European Digital Identity Wallet Architecture and Reference Framework [1] ของสหภาพยุโรป และเอกสารที่เกี่ยวข้องอื่น ๆ โดยมีวัตถุประสงค์เพื่อเป็นแนวทางอ้างอิงในการดำเนินการ (reference implementation) ให้กระเป๋าดิจิทัลในประเทศไทยสามารถทำงานร่วมกันได้ และช่วยจำกัดความซับซ้อนของรายละเอียดทางเทคนิค (technical solution) ที่แตกต่างกันจำนวนมาก ผู้ให้บริการกระเป๋าดิจิทัลสามารถนำรายงานฉบับนี้ไปปรับใช้เป็นแนวทางได้ตามความเหมาะสม อย่างไรก็ตาม รายงานฉบับนี้อาจมีการปรับปรุงเนื้อหาเพิ่มเติมตามลักษณะการใช้งานในประเทศไทยและการเปลี่ยนแปลงของเทคโนโลยีในอนาคต

รายงานฉบับนี้จำกัดนิยามของกระเป๋าดิจิทัลให้ครอบคลุมเฉพาะการใช้งานเอกสารรับรองและเอกสารสำแดงที่มีการลงลายมือชื่อดิจิทัล (digital signature) เท่านั้น แต่จะไม่ครอบคลุมถึง

- การใช้งานเอกสารอิเล็กทรอนิกส์ที่ไม่สามารถตรวจสอบได้ด้วยกระบวนการเข้ารหัสลับ (cryptography)
- กระเป๋าดิจิทัลประเภทอื่น ๆ เช่น กระเป๋าดิจิทัลสำหรับบริการเงินอิเล็กทรอนิกส์ (e-money wallet) หรือกระเป๋าดิจิทัลสำหรับการรับฝากหรือเก็บรักษาสินทรัพย์ดิจิทัล (digital asset wallet)

2. บทนิยาม

ความหมายของคำที่ใช้ในรายงานฉบับนี้ มีดังต่อไปนี้

2.1 กระเป๋าดิจิทัล (digital wallet) หมายถึง หมายถึง โปรแกรมที่จัดเก็บและช่วยให้ผู้ถือเอกสารสามารถเข้าถึงและใช้งานเอกสารรับรองได้อย่างมั่นคงปลอดภัย [2]

2.2 ผู้ให้บริการกระเป๋าดิจิทัล (digital wallet provider) หมายถึง เอนทิตีที่ทำหน้าที่พัฒนาและ/หรือดำเนินการเกี่ยวกับกระเป๋าดิจิทัล ให้แก่ผู้ออกเอกสาร ผู้ถือเอกสาร หรือผู้ตรวจสอบเอกสาร

2.3 เจ้าของข้อความ (subject) หมายถึง เอนทิตีที่ถูกกล่าวอ้างถึงในข้อความยืนยัน (claim) [2]

2.4 ข้อความยืนยัน (claim) หมายถึง ข้อความเกี่ยวกับเจ้าของข้อความ (subject) ที่จะถูกรับรองโดยผู้ออกเอกสาร (issuer) [2]

2.5 เอกสารรับรอง (verifiable credential: VC) หมายถึง ชุดของข้อความยืนยันอย่างน้อยหนึ่งรายการที่ถูกรับรองโดยผู้ออกเอกสาร (issuer) ทั้งนี้ เอกสารรับรองมีคุณสมบัติที่สามารถตรวจพบการเปลี่ยนแปลงใด ๆ ที่เกิดกับความถูกต้องครบถ้วนของข้อมูล และตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ของผู้ออกเอกสารได้ด้วยกระบวนการเข้ารหัสลับ [2]

2.6 เอกสารสำแดง (verifiable presentation: VP) หมายถึง เอกสารรับรองอย่างน้อยหนึ่งชุด ที่ผู้ถือเอกสาร (holder) ใช้แสดงต่อผู้ตรวจสอบเอกสาร (verifier) ทั้งนี้ เอกสารสำแดงมีคุณสมบัติที่สามารถตรวจพบการเปลี่ยนแปลงใด ๆ ที่เกิดกับความถูกต้องครบถ้วนของข้อมูล และตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ของผู้ถือเอกสารและตรวจสอบเอกสารรับรองที่เกี่ยวข้องได้ด้วยกระบวนการเข้ารหัสลับ [2]

2.7 เอนทิตี (entity) หมายถึง สิ่งที่มีอยู่จริง เช่น บุคคล องค์กร หรืออุปกรณ์ ซึ่งถูกกล่าวอ้างในการใช้งานเอกสารรับรองและเอกสารสำแดง [2]

2.8 ผู้ออกเอกสาร (issuer) หมายถึง เอนทิตีที่ทำหน้าที่รับรองข้อความยืนยันโดยออกเป็นเอกสารรับรองให้แก่ผู้ถือเอกสาร [2]

2.9 ผู้สมัคร (applicant) หมายถึง เอนทิตีที่ยื่นขอเอกสารรับรองจากผู้ออกเอกสาร (issuer) โดยผู้สมัครอาจจะเป็นเจ้าของข้อความ (subject) ในเอกสารรับรองหรือไม่ก็ได้

2.10 ผู้ถือเอกสาร (holder) หมายถึง เอนทิตีที่เป็นเจ้าของเอกสารรับรองอย่างน้อยหนึ่งชุด โดยจัดเก็บไว้ในกระเป๋าดิจิทัล (digital wallet) และสามารถใช้เอกสารรับรองสร้างเป็นเอกสารสำแดง ทั้งนี้ ผู้ถือเอกสารมีอีกชื่อเรียกหนึ่งว่า ผู้ใช้งานกระเป๋าดิจิทัล

2.11 ผู้ตรวจสอบเอกสาร (verifier) หมายถึง เอนทิตีที่สามารถตรวจสอบความถูกต้องครบถ้วนของเอกสารรับรองและเอกสารสำแดงด้วยกระบวนการเข้ารหัสลับ รวมถึงตรวจสอบสถานะการใช้งานและความสอดคล้องตามโครงสร้างข้อมูลของเอกสารรับรองและเอกสารสำแดง [2]

2.12 ระบบทะเบียนเอกสารรับรอง (verifiable data registry) หมายถึง ระบบที่ช่วยสนับสนุนการสร้างและการตรวจสอบความถูกต้องครบถ้วนของเอกสารรับรองและเอกสารสำแดง โดยข้อมูลที่มีการจัดเก็บในระบบนี้ เช่น ตัวระบุ (identifier) และกุญแจสาธารณะ (public key) ของเอนทิตีที่เกี่ยวข้อง รวมถึงรายการเพิกถอน (revocation list) และเค้าร่าง (schema) ของเอกสารรับรองหรือเอกสารสำแดง [2]

2.13 ลายมือชื่อดิจิทัล (digital signature) หมายถึง ลายมือชื่ออิเล็กทรอนิกส์ (electronic signature) ที่ได้จากกระบวนการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ ซึ่งช่วยให้สามารถยืนยันตัวเจ้าของลายมือชื่อและตรวจพบการเปลี่ยนแปลงของข้อความและลายมือชื่ออิเล็กทรอนิกส์ได้ รวมถึงการทำให้เจ้าของลายมือชื่อไม่สามารถปฏิเสธความรับผิดจากข้อความที่ตนเองลงลายมือชื่อได้ [3]

2.14 ตัวระบุ (identifier) หมายถึง Uniform Resource Identifier (URI) ที่ระบุถึงเอนทิตี เอกสารรับรอง หรือข้อมูลอื่น ๆ ที่เกี่ยวข้อง [4]

2.15 เค้าร่าง (schema) หมายถึง ข้อมูลที่กำหนดโครงสร้าง (structure) และรูปแบบ (format) ของเอกสารรับรองและ/หรือเอกสารสำแดง โดยสามารถแบ่งออกเป็น 2 ประเภท ได้แก่ (1) เค้าร่างสำหรับการตรวจสอบข้อมูล (data verification schema) สำหรับตรวจสอบโครงสร้างและเนื้อหาของเอกสารรับรอง และ (2) เค้าร่างสำหรับการเข้ารหัสข้อมูล (data encoding schema) สำหรับการแปลงเนื้อของเอกสารรับรองจากรูปแบบ (format) หนึ่งไปยังอีกรูปแบบหนึ่ง [5]

3. ภาพรวมของกระเป๋าดิจิทัลสำหรับเอกสารรับรอง

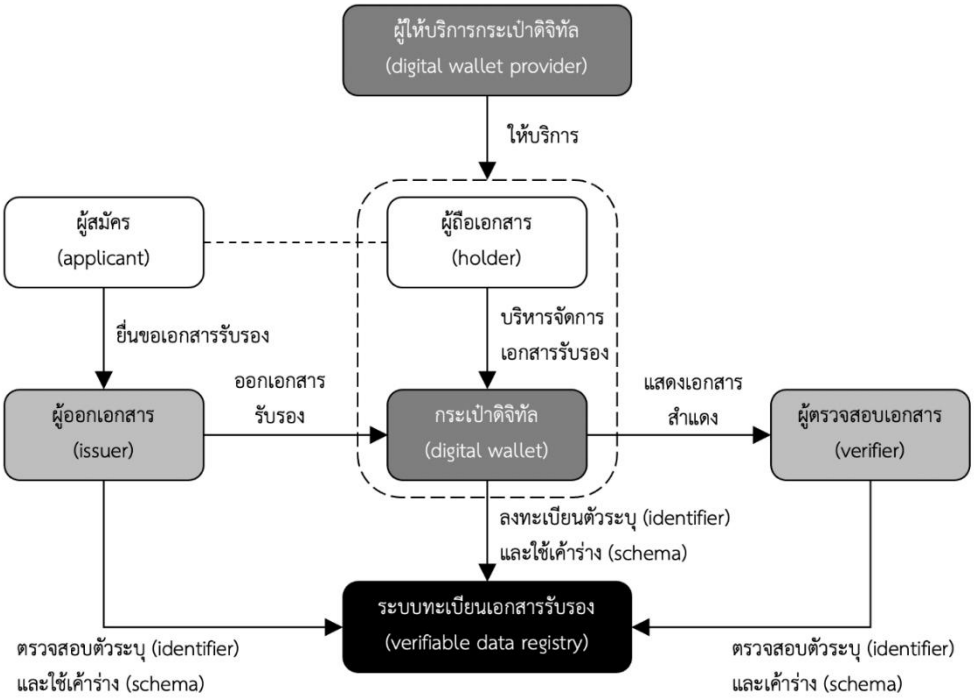
การแลกเปลี่ยนเอกสารในรูปแบบกายภาพ (physical document) เป็นส่วนหนึ่งของการทำธุรกรรมในชีวิตประจำวัน โดยมีการใช้งานมาเป็นเวลายาวนานก่อนที่อินเทอร์เน็ตจะถูกใช้งานอย่างแพร่หลาย ตัวอย่างเช่น ผู้ขับรถแสดงใบอนุญาตขับขี่ที่ได้รับจากกรมการขนส่งทางบกต่อเจ้าพนักงานจราจร นักศึกษาแสดงปริญญาบัตรจากมหาวิทยาลัยต่อผู้ว่าจ้างเพื่อสมัครเข้าทำงาน และผู้โดยสารแสดงหนังสือเดินทางต่อเจ้าหน้าที่ตรวจคนเข้าเมืองเพื่อเดินทางไปต่างประเทศ

ในยุคของอินเตอร์เน็ต ได้มีการใช้งานและแลกเปลี่ยนเอกสารบนเว็บไซต์และแอปพลิเคชันอย่างแพร่หลาย อย่างไรก็ตาม เอกสารข้างต้นมักถูกใช้ในรูปแบบสำเนาอิเล็กทรอนิกส์ของเอกสารในรูปแบบกายภาพ (electronic copy of physical document) เช่น การสแกนบัตรประชาชนให้เป็นไฟล์เอกสารอิเล็กทรอนิกส์ประเภท portable document format (PDF) ซึ่งเอกสารอิเล็กทรอนิกส์ในรูปแบบนี้ส่วนมากยังใช้บุคคลในการตรวจสอบความถูกต้องครบถ้วนของเอกสาร

การพัฒนาเทคโนโลยีและมาตรฐานของเอกสารในรูปแบบข้อมูลอิเล็กทรอนิกส์ (electronic document) ที่มีความน่าเชื่อถือ จะช่วยเพิ่มประสิทธิภาพและความมั่นคงปลอดภัยในการทำธุรกรรมออนไลน์ จึงเป็นที่มาของเอกสารรับรอง (verifiable credential: VC) ซึ่งเป็นเอกสารอิเล็กทรอนิกส์ที่มีคุณสมบัติด้านความมั่นคงปลอดภัยที่สามารถตรวจสอบได้ด้วยกระบวนการเข้ารหัสลับ (cryptography) [2] [5] และถูกออกแบบมาเพื่อให้สามารถใช้งานบนโลกออนไลน์ ทั้งนี้ โปรแกรมหรือซอฟต์แวร์สำหรับการบริหารจัดการ การจัดเก็บ และการแลกเปลี่ยนเอกสารรับรอง รวมถึงข้อมูลอื่น ๆ ที่เกี่ยวข้องจะเรียกว่า กระเป๋าดิจิทัล (digital wallet)

3.1 บทบาทและความสัมพันธ์ของเอนทิตีที่เกี่ยวข้อง

การใช้งานกระเป๋าดิจิทัลสำหรับเอกสารรับรอง ประกอบด้วยเอนทิตีต่าง ๆ ที่เกี่ยวข้อง 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 โดยผู้ออกเอกสารมีหน้าที่ตรวจสอบความถูกต้องของข้อมูลนั้น

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

(4) ผู้ถือเอกสารสามารถสร้างเอกสารสำแดงโดยใช้ข้อมูลจากเอกสารรับรอง จากนั้นแสดงเอกสารสำแดงต่อผู้ตรวจสอบเอกสาร (verifier) ซึ่งทำหน้าที่ตรวจสอบความถูกต้องครบถ้วนของเอกสารสำแดงนั้น

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

ทั้งนี้ ผู้ออกเอกสารและผู้ตรวจสอบเอกสารอาจเป็นบุคคลซึ่งใช้งานกระเป๋าดิจิทัลเช่นเดียวกันกับผู้ถือเอกสาร หรืออาจเป็นระบบขององค์กรที่ทำหน้าที่ออกเอกสารรับรองหรือตรวจสอบเอกสารรับรองโดยอัตโนมัติ ในกรณีนี้ ระบบขององค์กรจะถือเป็นกระเป๋าดิจิทัลขององค์กร (enterprise digital wallet) ซึ่งทำหน้าที่บริหารจัดการเอกสารรับรองสำหรับองค์กรนั้น

3.2 เอกสารรับรองและเอกสารสำแดง

ในรายงานฉบับนี้ เอกสารรับรองจะไม่จำกัดความหมายเฉพาะเอกสารรับรองที่ออกโดยหน่วยงานของรัฐให้แก่บุคคล แต่มีความหมายรวมถึงเอกสารอิเล็กทรอนิกส์ใด ๆ ซึ่งยืนยัน (assert) ข้อความยืนยัน (claims) เกี่ยวกับเจ้าของข้อความ (subject) โดยสามารถตรวจสอบได้ว่าเอกสารรับรองนั้นไม่ถูกเปลี่ยนแปลง (integrity) และสามารถยืนยันตัวผู้ออกเอกสารได้ (authenticity) โดยเอกสารรับรองมีองค์ประกอบ ดังนี้

(1) คำอธิบายข้อมูล (metadata) ของเอกสารรับรอง ซึ่งอาจรวมถึงตัวระบุ (identifier) ของเอนทิตีที่เกี่ยวข้อง ข้อมูลของผู้ออกเอกสาร หรือวันหมดอายุของเอกสารรับรอง

(2) ข้อความยืนยัน (claim) ซึ่งอาจมีเพียงข้อความยืนยันเดียวหรือหลายข้อความยืนยันก็ได้ โดยเป็นข้อมูลที่ยืนยันเกี่ยวกับเจ้าของข้อความ ซึ่งอาจเป็นบุคคลธรรมดา นิติบุคคล สิ่งของ หรือซอฟต์แวร์ โดยมีข้อความยืนยัน 2 ประเภท ได้แก่ คุณลักษณะ (attribute) ของเจ้าของข้อความ และความสัมพันธ์ (relationship) ของเจ้าของข้อความต่อเอนทิตีอื่น

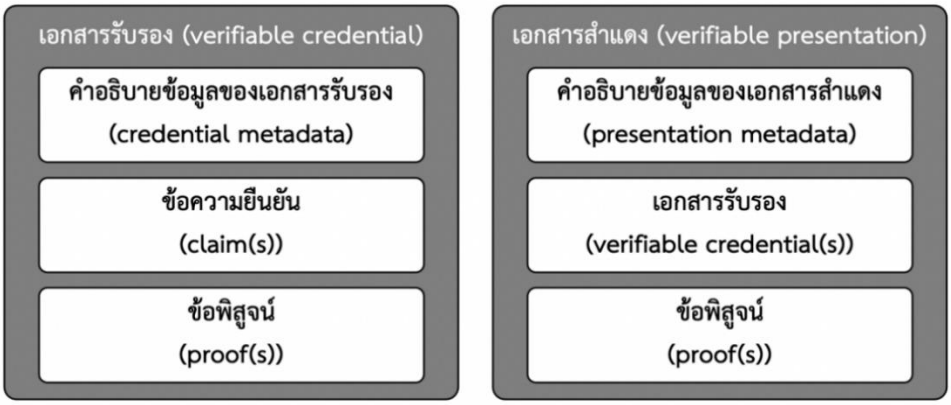
(3) ข้อพิสูจน์ (proof) ของเอกสารรับรอง ซึ่งอาจมีข้อพิสูจน์เดียวหรือหลายข้อพิสูจน์ก็ได้ โดยเป็นข้อมูลที่สร้างขึ้นจากลายมือชื่อดิจิทัลของผู้ออกเอกสาร

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

(1) คำอธิบายข้อมูล (metadata) ของเอกสารสำแดง

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

(3) ข้อพิสูจน์ (proof) ของเอกสารสำแดง ซึ่งอาจมีข้อพิสูจน์เดียวหรือหลายข้อพิสูจน์ก็ได้ โดยเป็นข้อมูลที่สร้างขึ้นจากลายมือชื่อดิจิทัลของผู้ถือเอกสาร



รูปที่ 2 องค์ประกอบพื้นฐานของเอกสารรับรองและเอกสารสำแดง

ปัจจุบันมีมาตรฐานเกี่ยวกับเอกสารรับรองและเอกสารสำแดงจากองค์กรกำหนดมาตรฐานสากลหลายองค์กร เช่น มาตรฐาน Verifiable Credentials Data Model จากองค์กร World Wide Web Consortium (W3C) [5] และมาตรฐาน ISO/IEC 18013-5 ซึ่งเกี่ยวกับใบขับขี่บนอุปกรณ์เคลื่อนที่ (mobile driving

license: mDL) [6] ทั้งนี้ รายงานฉบับนี้จะระบุถึงเอกสารรับรองและเอกสารสำแดง โดยไม่เจาะจงระบุถึงมาตรฐานหรือเทคโนโลยีที่ใช้ เว้นแต่จะมีการระบุไว้เป็นอย่างอื่น

3.3 ระบบทะเบียนเอกสารรับรอง (verifiable data registry)

ในการใช้งานกระเป๋าดิจิทัลสำหรับเอกสารรับรอง เอนทิตีที่เกี่ยวข้องจะใช้งานกระเป๋าดิจิทัลร่วมกับระบบทะเบียนเอกสารรับรอง ซึ่งทำหน้าที่สนับสนุนการออกเอกสารรับรองและการตรวจสอบเอกสารสำแดง โดยมีองค์ประกอบหลัก 3 องค์ประกอบเป็นอย่างน้อย ดังนี้

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

นอกจากนี้ ระบบทะเบียนเอกสารรับรองอาจมีองค์ประกอบเพิ่มเติมเพื่อทำหน้าที่เป็นทะเบียนรายชื่อที่เชื่อถือได้ (trusted lists) ของเอนทิตีต่าง ๆ เช่น

- รายชื่อผู้ให้บริการกระเป๋าดิจิทัลที่ได้รับการรับรอง (qualified digital wallet providers)
- รายชื่อผู้ออกเอกสารที่ได้รับการรับรอง (qualified issuers)
- รายชื่อผู้ตรวจสอบเอกสาร (verifiers)
- รายชื่อผู้ให้บริการออกใบรับรอง (certification authorities: CA)

ทั้งนี้ ระบบทะเบียนเอกสารรับรองสามารถพัฒนาได้ด้วยเทคโนโลยีหลากหลายรูปแบบ ทั้งในรูปแบบรวมศูนย์ (centralized) ด้วยระบบฐานข้อมูล หรือรูปแบบกระจายศูนย์ (decentralized) ด้วยเทคโนโลยีบล็อกเชน (blockchain) หรือโครงสร้างพื้นฐานใบรับเหตุการณ์กุญแจ (key event receipt infrastructure: KERI) [7] หรือรูปแบบผสม

หน้าที่ของระบบทะเบียนเอกสารรับรองในการสนับสนุนการออกเอกสารรับรองและการตรวจสอบเอกสารสำแดง สามารถสรุปได้ ดังนี้

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

(2) ผู้ออกเอกสารใช้เค้าร่างของเอกสารรับรอง (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) ผู้ถือเอกสารสามารถแปลงเอกสารรับรองให้เป็นเอกสารสำแดงได้ โดยการลงลายมือชื่อดิจิทัลด้วยกุญแจส่วนตัวของผู้ถือเอกสาร 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 แต่มีข้อเสียคือ กระเป๋าดิจิทัลจะอยู่ในความรับผิดชอบของผู้ถือเอกสารโดยสมบูรณ์ และมีความไม่สะดวกในการสำรองข้อมูลและการเชื่อมโยงข้อมูล (synchronization) ระหว่างกระเป๋าดิจิทัลของผู้ถือเอกสารคนเดียวกัน

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

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

ทั้งนี้ กระเป๋าดิจิทัลแต่ละประเภทมีข้อดีข้อเสียที่แตกต่างกัน โดยควรพิจารณาเลือกประเภทตามความเหมาะสมของธุรกรรมที่จะนำกระเป๋าดิจิทัลไปใช้งาน เช่น เลือกกระเป๋าดิจิทัลแบบคลาวด์สำหรับธุรกรรมที่มีความเสี่ยงต่ำ และเลือกกระเป๋าดิจิทัลแบบเอดจ์สำหรับธุรกรรมที่มีความเสี่ยงสูง

3.5 การสำรองและกู้คืนข้อมูลความลับ

กระเป๋าดิจิทัลมีหน้าที่สำคัญในการจัดเก็บและบริหารจัดการข้อมูลลับสำหรับการเข้ารหัส (cryptographic secret) เช่น กุญแจส่วนตัว โดยผู้ใช้งานมีความเสี่ยงที่จะสูญเสียการเข้าถึงข้อมูลความลับ ซึ่งอาจทำให้ผู้ใช้งานไม่สามารถใช้งานกระเป๋าดิจิทัลได้อีกต่อไป เช่น ในกรณีที่อุปกรณ์จัดเก็บกุญแจส่วนตัวสูญหายหรือชำรุด ทำให้ผู้ใช้งานไม่สามารถใช้กุญแจส่วนตัวในการลงลายมือชื่อเพื่อสร้างเอกสารสำแดงได้

ผู้ให้บริการกระเป๋าดิจิทัลสามารถบรรเทาความเสี่ยงที่ข้อมูลความลับจะสูญหายได้โดยมีแนวทางการสำรอง (backup) และกู้คืน (recovery) ข้อมูลความลับ ดังนี้

(1) การกู้คืนข้อมูลแบบออนไลน์ (online recovery) เป็นการสำรองข้อมูลความลับบนระบบคลาวด์ โดยกระเป๋าดิจิทัลควรเลือกใช้บริการจากผู้ให้บริการคลาวด์ที่น่าเชื่อถือ และควรจัดเก็บข้อมูลความลับที่ถูกเข้ารหัสลับโดยอัตโนมัติ (automatic encrypted) ด้วยกุญแจส่วนตัวหรือใช้รหัสผ่านตามมาตรฐานสากล เช่น มาตรฐาน PKCS #12 [8]

(2) การกู้คืนข้อมูลแบบออฟไลน์ (offline recovery) เป็นการสำรองข้อมูลความลับภายในอุปกรณ์ซึ่งไม่ได้เชื่อมต่อกับเครือข่ายอินเทอร์เน็ต โดยอุปกรณ์ที่ใช้สำรองข้อมูลควรมีอายุการใช้งานยาวนานเพียงพอต่ออายุการใช้งานของข้อมูลความลับ (cryptoperiod)

(3) การกู้คืนข้อมูลแบบสังคม (social recovery) เป็นการสำรองข้อมูลความลับกับบุคคลหรือองค์กรอื่นที่ผู้ใช้งานเชื่อถือ (trustees) โดยใช้กระบวนการ key sharding เพื่อแบ่งข้อมูลความลับออกเป็นหลายส่วน และให้ trustee เป็นผู้จัดเก็บ เช่น การฝากส่วนกุญแจ (key shards) กับญาติ เพื่อการกู้คืนข้อมูลกุญแจส่วนตัวในอนาคต

(4) การกู้คืนข้อมูลด้วยหลายอุปกรณ์ (multi-device recovery) มีลักษณะคล้ายกับการกู้คืนข้อมูลแบบสังคม แต่ใช้อุปกรณ์จัดเก็บข้อมูลความลับหลายอุปกรณ์เพื่อแบ่งการจัดเก็บข้อมูลออกเป็นหลายส่วนแทนการใช้ trustee

ทั้งนี้ การสำรองข้อมูลความลับเป็นการส่งข้อมูลออกไปจากอุปกรณ์ที่ใช้ดำเนินการกระเป๋าดิจิทัล ทำให้มีความเสี่ยงที่ผู้ไม่หวังดีอาจทำการดักฟังเพื่อขโมยข้อมูลความลับดังกล่าว ดังนั้น การสำรองข้อมูลอาจไม่เหมาะสมกับการทำธุรกรรมที่มีความเสี่ยงสูง เช่น การทำธุกรรมที่อาศัยข้อมูลระบุตัวตนบุคคล (person identification data) โดยผู้ออกเอกสารอาจพิจารณาไม่ออกเอกสารรับรองให้กับกระเป๋าดิจิทัลที่สามารถสำรองข้อมูลความลับได้

3.6 การคุ้มครองข้อมูลส่วนบุคคลของผู้ถือเอกสาร

เอกสารรับรองอาจมีข้อมูลส่วนบุคคลที่อ่อนไหว (sensitive personal information) ดังนั้น กระบวนการหรือกลไกการคุ้มครองข้อมูลส่วนบุคคลของผู้ถือเอกสารจึงมีความสำคัญ ผู้ออกเอกสารและผู้ให้บริการกระเป๋าดิจิทัลสามารถดำเนินการได้หลายวิธี เพื่อลดการเปิดเผยข้อมูลส่วนบุคคลให้น้อยที่สุด (data minimization) โดยเฉพาะในระหว่างการแสดงเอกสารสำแดงต่อผู้ตรวจสอบเอกสาร

ตัวอย่างของกลไกการคุ้มครองข้อมูลส่วนบุคคล (privacy-preserving mechanism) ที่เป็นทางเลือกในการนำไปใช้งาน มีดังนี้

(1) การเลือกเปิดเผยข้อมูลบางส่วน (selective disclosure) เป็นกระบวนการที่ผู้ถือเอกสารสามารถเลือกเปิดเผยหรือปกปิดข้อมูลบางส่วนในเอกสารรับรองได้ โดยให้ข้อมูลกับผู้ตรวจสอบเอกสารเท่าที่จำเป็นกับการทำธุรกรรมนั้น ๆ เช่น การเลือกเปิดเผยข้อมูลชื่อและนามสกุล แต่ไม่เปิดเผยข้อมูลวันเดือนปีเกิดบนเอกสารรับรอง

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

(3) การใช้ตัวระบุแบบนามแฝง (pseudonymous identifier) เป็นกระบวนการใช้นามแฝง (pseudonym) เป็นตัวระบุในการทำธุรกรรมกับเอนทิตีอื่น เพื่อหลีกเลี่ยงการใช้ตัวระบุเดิมซ้ำในการทำธุรกรรมหลายครั้ง ทำให้ผู้ตรวจสอบเอกสารหนึ่ง ๆ ไม่สามารถเชื่อมโยงได้ (unlinkability) ว่าเป็นผู้ถือเอกสารคนเดิมที่ทำธุรกรรม รวมทั้งป้องกันการที่ผู้ตรวจสอบเอกสารอาจทำการแลกเปลี่ยนข้อมูลระหว่างกันเพื่อใช้ติดตามการใช้งานของผู้ถือเอกสารนั้น

3.7 กลไกการเชื่อมโยงผู้ถือเอกสารต่อเอกสารรับรอง

ในกรณีที่ผู้ตรวจสอบเอกสารมีความจำเป็นต้องตรวจสอบว่าผู้ถือเอกสารนั้นเป็นบุคคลคนเดียวกันกับเจ้าของข้อความ (subject) ในเอกสารรับรอง เอกสารรับรองต้องมีข้อมูลที่สามารถเชื่อมโยงผู้ถือเอกสารต่อเอกสารรับรองนั้นได้ (holder binding) โดยมีแนวทางเบื้องต้น ดังนี้

(1) การเชื่อมโยงกับอุปกรณ์ของผู้ใช้งาน (device binding) เป็นการระบุข้อมูลในเอกสารรับรอง ซึ่งสามารถเชื่อมโยงกับอุปกรณ์ที่ผู้ใช้งานครอบครองแต่เพียงผู้เดียว โดยอาจเชื่อมโยงกับกุญแจเข้ารหัส (cryptographic binding) ภายในอุปกรณ์ ทำให้ผู้ใช้งานสามารถพิสูจน์การเชื่อมโยงด้วยกระบวนการเข้ารหัสลับ (cryptographic proof)

(2) การเชื่อมโยงกับข้อมูลชีวมิติของผู้ใช้งาน (biometric binding) เป็นการระบุข้อมูลในเอกสารรับรอง ซึ่งสามารถเชื่อมโยงกับข้อมูลชีวมิติของผู้ใช้งาน เช่น การระบุรูปภาพใบหน้าของผู้ถือเอกสารในเอกสารรับรอง

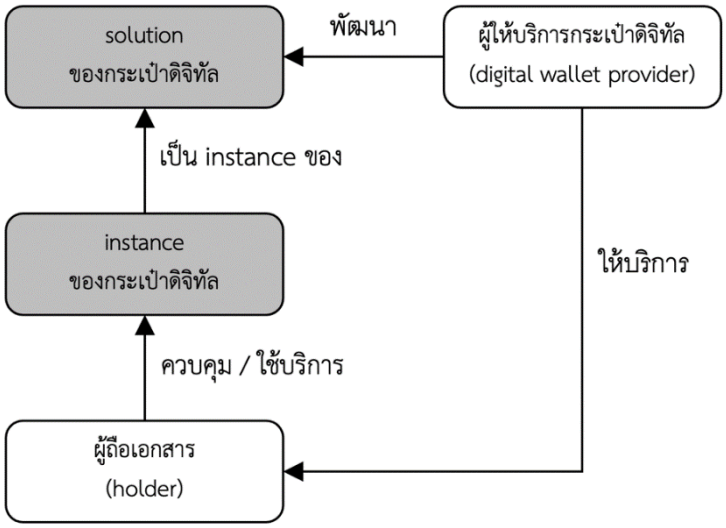
ทั้งนี้ การเชื่อมโยงกับอุปกรณ์ของผู้ใช้งานถือว่าเป็นปัจจัยของการยืนยันตัวตน (authentication factor) ประเภทสิ่งที่คุณมี (something you have) ส่วนการเชื่อมโยงกับข้อมูลชีวมิติของผู้ใช้งานถือว่าเป็นปัจจัยการยืนยันตัวตนประเภทสิ่งที่คุณเป็น (something you are) โดยการเชื่อมโยงผู้ถือเอกสารต่อเอกสารรับรองอาจใช้ปัจจัยของการยืนยันตัวตนประเภทอื่น หรือการผสมผสานหลายปัจจัย ก็เป็นได้ [9]

4. วงจรชีวิตของกระเป๋าดิจิทัลและเอกสารรับรอง

ผลิตภัณฑ์ของกระเป๋าดิจิทัลสามารถแบ่งออกเป็นโซลูชัน (solution) และอินสแตนซ์ (instance) ซึ่งมีความหมายดังนี้

- โซลูชัน (solution) หมายถึง ผลิตภัณฑ์ของกระเป๋าดิจิทัล ซึ่งเป็นผลิตภัณฑ์และบริการทั้งหมดที่เป็นของผู้ให้บริการกระเป๋าดิจิทัล และอาจรวมถึง ลิขสิทธ์ เครื่องหมายการค้า source code และโครงสร้างพื้นฐานอื่น ๆ ที่ทำหน้าที่สนับสนุนการให้บริการของกระเป๋าดิจิทัล
- อินสแตนซ์ (instance) หมายถึง ผลิตภัณฑ์ของกระเป๋าดิจิทัลเฉพาะส่วนที่ควบคุมโดยผู้ใช้งาน โดยอาจติดตั้งและดำเนินการภายในอุปกรณ์ของผู้ใช้งานเองหรือให้บริการผ่านทางอินเตอร์เน็ต

ความสัมพันธ์ระหว่างผู้ถือเอกสารหรือผู้ใช้งานกระเป๋าดิจิทัล ผู้ให้บริการกระเป๋าดิจิทัล โซลูชัน และอินสแตนซ์ของกระเป๋าดิจิทัล สามารถแสดงตามรูปที่ 3



รูปที่ 3 ความสัมพันธ์ระหว่างโซลูชันและอินสแตนซ์ของกระเป๋าดิจิทัล

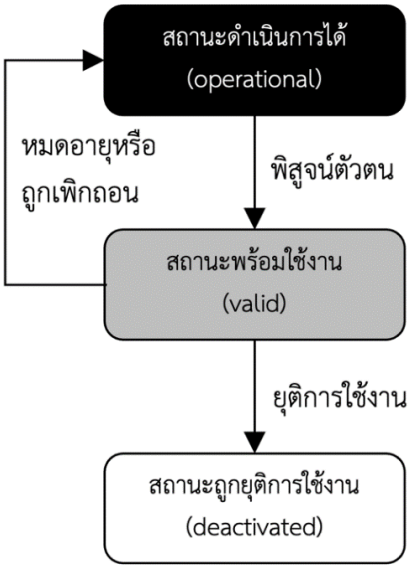
4.1 วงจรชีวิตการใช้งานอินสแตนซ์ของกระเป๋าดิจิทัล

เมื่อโซลูชันของกระเป๋าดิจิทัลพร้อมให้บริการ ผู้ใช้งานสามารถเริ่มการใช้งานอินสแตนซ์ของกระเป๋าดิจิทัลได้ โดยวงจรชีวิตการใช้งานจะเริ่มต้นในสถานะ “ดำเนินการได้” (operational) เมื่อผู้ใช้งานทำการติดตั้ง (install) และสั่งเริ่มการทำงาน (activate) อินสแตนซ์ของกระเป๋าดิจิทัล โดยในสถานะนี้ ผู้ใช้งานสามารถใช้งานอินสแตนซ์สำหรับการทำธุรกรรมที่มีความเสี่ยงต่ำ เช่น การใช้งานบัตรสะสมคะแนน ตั๋วโดยสารที่ไม่ระบุชื่อผู้ถือตั๋ว หรือเอกสารรับรองอื่นที่ไม่ได้กำหนดให้มีข้อมูลที่เชื่อมโยงผู้ถือเอกสารต่อเอกสารรับรองนั้น

จากนั้น ผู้ใช้งานสามารถพิสูจน์ตัวตน (identity proofing) กับผู้ให้บริการกระเป๋าดิจิทัลหรือหน่วยงานที่เกี่ยวข้อง เพื่อขอรับเอกสารรับรองที่สามารถนำไปใช้ระบุตัวตนผู้ใช้งาน โดยการพิสูจน์ตัวตนควรดำเนินการด้วยระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (Identity Assurance Level: IAL) ที่ระดับ IAL2 ขึ้นไป [10] การจัดเก็บเอกสารรับรองซึ่งรับรองการพิสูจน์ตัวตนของผู้ใช้งานในอินสแตนซ์ของกระเป๋าดิจิทัล จะเปลี่ยนสถานะของอินสแตนซ์เป็น “พร้อมใช้งาน” (valid)

ทั้งนี้ หากเอกสารรับรองดังกล่าวถูกเพิกถอนหรือหมดอายุ อินสแตนซ์ยังสามารถใช้งานต่อไปได้ แต่จะถูกลดสถานะกลับเป็น “ดำเนินการได้” (operational) โดยผู้ใช้งานสามารถดำเนินการพิสูจน์ตัวตนหรือยืนยันตัวตนกับหน่วยงานเดิม เพื่อขอเอกสารรับรองฉบับใหม่และเปลี่ยนสถานะของอินสแตนซ์เป็น “พร้อมใช้งาน” (valid) อีกครั้ง

นอกจากนี้ ผู้ใช้งานสามารถสั่งยุติการใช้งาน (deactivate) เพื่อเปลี่ยนสถานะของอินสแตนซ์ให้เป็น “ถูกยุติการใช้งาน” (deactivated) ทำให้อินสแตนซ์นั้นไม่สามารถใช้งานได้อีกต่อไป ทั้งนี้ การยุติการทำงานของอินสแตนซ์จะไม่เกี่ยวข้องกับการเพิกถอนเอกสารรับรอง โดยผู้ใช้งานอาจย้ายเอกสารรับรองไปยังอินสแตนซ์ของกระเป๋าดิจิทัลอื่นได้



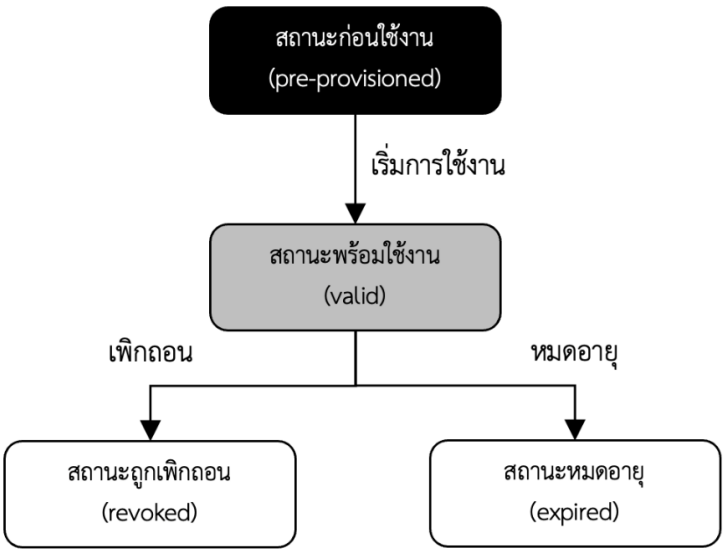
รูปที่ 4 วงจรชีวิตการใช้งานอินสแตนซ์ของกระเป๋าดิจิทัล

4.2 วงจรชีวิตการใช้งานเอกสารรับรอง

เอกสารรับรองเริ่มต้นวงจรชีวิตการใช้งานเมื่อผู้ออกเอกสารออกเอกสารรับรองให้ผู้ถือเอกสาร โดยอาจอยู่ในสถานะ “ก่อนใช้งาน” (pre-provisioned) หากยังไม่ถึงวันเวลาที่เอกสารรับรองสามารถใช้งานได้ (validity start date) ตามที่ระบุไว้ในเอกสารรับรอง ทำให้ยังไม่สามารถใช้งานเอกสารนั้นได้ทันที

เมื่อถึงวันเวลาที่เอกสารรับรองสามารถใช้งานได้ หรือในกรณีที่เอกสารรับรองสามารถใช้งานได้ทันที เอกสารรับรองจะอยู่ในสถานะ “พร้อมใช้งาน” (valid) โดยในสถานะนี้ ผู้ถือเอกสารสามารถสร้างเอกสารสำแดงจากเอกสารรับรองดังกล่าว เพื่อแสดงและขอใช้บริการจากผู้ตรวจสอบเอกสาร

จากนั้น เอกสารรับรองอาจเปลี่ยนสถานะเป็น “ถูกเพิกถอน” (revoked) ในกรณีที่ผู้ออกเอกสารเพิกถอนเอกสารรับรอง หรือเอกสารรับรองเปลี่ยนสถานะเป็น “หมดอายุ” (expired) โดยอัตโนมัติเมื่อผ่านวันเวลาที่เอกสารรับรองหมดอายุ (validity end date) ตามที่ระบุไว้ในเอกสารรับรอง ทำให้เอกสารรับรองไม่สามารถถูกนำไปใช้งานได้อีกต่อไป



รูปที่ 5 วงจรชีวิตการใช้งานเอกสารรับรอง

5. องค์ประกอบของกระเป๋าดิจิทัล

การกำหนดองค์ประกอบพื้นฐานและสถาปัตยกรรมซอฟต์แวร์ของกระเป๋าดิจิทัล รวมถึงช่องทางการแลกเปลี่ยนเอกสารรับรอง จะช่วยส่งเสริมให้เกิดการทำงานร่วมกันได้ (interoperability) ระหว่างกระเป๋าดิจิทัลจากผู้ให้บริการที่แตกต่างกัน และการแลกเปลี่ยนเอกสารรับรองระหว่างเอนทิตีต่าง ๆ เป็นไปอย่างสอดคล้องกัน

5.1 องค์ประกอบพื้นฐานของกระเป๋าดิจิทัล

กระเป๋าดิจิทัลมีองค์ประกอบพื้นฐาน (basic component) สำหรับการใช้งานเอกสารรับรอง ซึ่งรวมถึงการออกเอกสารรับรอง การจัดเก็บ จนถึงการแสดงเอกสารสำแดง ซึ่งผู้ให้บริการกระเป๋าดิจิทัลสามารถนำองค์ประกอบมาปรับใช้เพื่อพัฒนาโซลูชันของกระเป๋าดิจิทัลได้ตามความเหมาะสม ดังนี้

(1) **ระบบบริหารจัดการกุญแจเข้ารหัส (cryptographic key management system)** เป็นองค์ประกอบที่รับผิดชอบการบริหารจัดการและจัดเก็บข้อมูลที่เกี่ยวกับการเข้ารหัส (cryptographic information) เช่น กุญแจส่วนตัว

(2) **โพรโทคอลการแลกเปลี่ยนเอกสารสำแดง (attestation exchange protocol)** เป็นโพรโทคอลที่กำหนดขั้นตอนในการร้องขอ (request) และการแสดง (present) เอกสารรับรอง ที่มีความมั่นคงปลอดภัยและคุ้มครองข้อมูลส่วนบุคคล รวมถึงกำหนดขั้นตอนในการยืนยันตัวตนระหว่างผู้ถือเอกสารกับผู้ตรวจสอบเอกสาร

(3) **โพรโทคอลการออกเอกสารรับรอง (issuance protocol)** เป็นโพรโทคอลที่กำหนดขั้นตอนและรูปแบบ (format) ในการออกเอกสารรับรอง

(4) **โครงสร้างข้อมูลของเอกสารรับรอง (data model)** กำหนดและอธิบายรายการข้อมูล (data element) ความสัมพันธ์ระหว่างข้อมูล และคุณสมบัติของข้อมูล

(5) **เค้าร่างของเอกสารรับรอง (credential schema)** ประกอบด้วยโครงสร้างและการจัดกลุ่ม (logical organization) ของข้อมูลในเอกสารรับรอง ซึ่งระบุคุณสมบัติของเอกสารรับรอง คุณลักษณะของผู้ใช้งาน (user attributes) วิธีการตรวจสอบเอกสารรับรอง (verification mechanism) ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance) การพิสูจน์ว่าผู้ใช้งานเป็นผู้ครอบครองเอกสารรับรอง (proof of possession) และข้อมูลเพิ่มเติมอื่นๆ

(6) **รูปแบบของเอกสารรับรอง (credential format)** เป็นรูปแบบการแสดงผลข้อมูลของเอกสารรับรอง ซึ่งอาจรวมถึงลักษณะเฉพาะ (characteristic) คุณภาพ (quality) สิทธิ (right) หรือสิ่งที่ได้รับอนุญาต (permission) ของบุคคลธรรมดา นิติบุคคล หรือวัตถุใด ๆ ในรูปแบบที่มีการลงลายมือชื่อและสามารถตรวจสอบได้

(7) **รูปแบบของลายมือชื่อดิจิทัลและการเข้ารหัสลับ (signature and encryption format)** เป็นรูปแบบการแสดงผลลายมือชื่อดิจิทัลและการเข้ารหัสลับ ซึ่งขึ้นอยู่กับรายละเอียดทางเทคนิคและวิธีการทางคณิตศาสตร์ที่เกี่ยวข้อง เพื่อให้สามารถตรวจสอบความถูกต้องครบถ้วนของข้อมูล (integrity) และสามารถระบุและยืนยันตัวตนของผู้ออกเอกสารและผู้ถือเอกสาร

(8) **รูปแบบความไว้วางใจ (trust model)** เป็นกฎเกณฑ์ (rule) ที่ใช้รับรองความน่าเชื่อถือหรือความถูกต้องตามกฎหมาย (legitimacy) ของเอนทิตีที่เกี่ยวข้อง ซึ่งอาจรวมถึงรายการดังนี้

- การยืนยันตัวตนผู้ใช้งาน
- การระบุตัวตนผู้เอกสาร
- การลงทะเบียนผู้ออกเอกสาร
- โครงสร้างข้อมูลและเค้าร่างของเอกสารรับรองที่ได้รับการยอมรับ
- การลงทะเบียนและยืนยันตัวตนผู้ตรวจสอบเอกสาร

รูปแบบความไว้วางใจช่วยทำให้สามารถระบุตัวตนของเอนทิตีต่าง ๆ ที่เกี่ยวข้องกับกระเป๋าดิจิทัล และสร้างความน่าเชื่อถือในการใช้งานเอกสารรับรอง

(9) **กลไกการเข้ารหัสลับ (cryptographic suite and mechanism)** เป็นอัลกอริทึมและกระบวนการรักษาความมั่นคงปลอดภัยในการแลกเปลี่ยนข้อมูล ในด้านการรักษาความลับ (confidentiality) และความถูกต้องครบถ้วน (integrity) ของข้อมูล

(10) **ตัวระบุของเอนทิตี (entity identifier)** เป็นตัวระบุเฉพาะที่ไม่ซ้ำกัน (unique identifier) สำหรับรายการข้อมูลต่าง ๆ ในโครงสร้างข้อมูลของเอกสารรับรอง

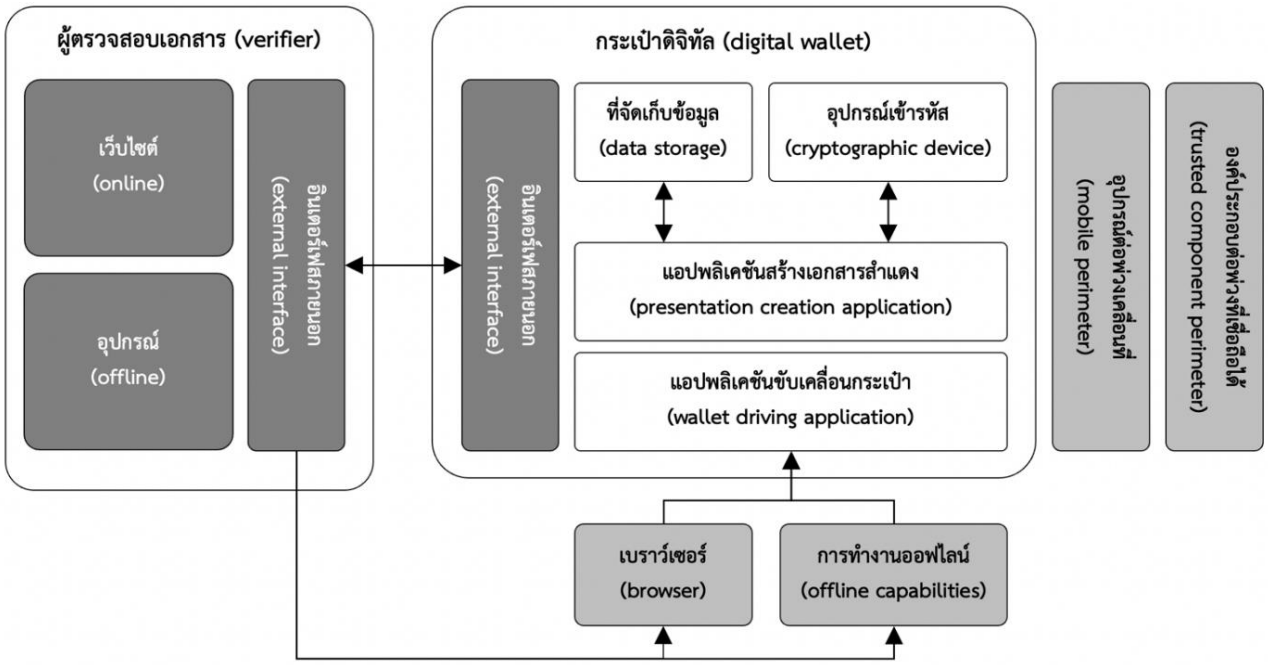
(11) **กลไกการตรวจสถานะของเอกสารรับรอง (validity status check)** เป็นกลไกในการเผยแพร่และรับข้อมูลสถานะ (validity status) ของเอกสารรับรอง เช่น สถานะพร้อมใช้งาน (valid) สถานะถูกเพิกถอน (revoked) และสถานะหมดอายุ (expired)

5.2 สถาปัตยกรรมซอฟต์แวร์ของกระเป๋าดิจิทัล

สถาปัตยกรรมซอฟต์แวร์ของกระเป๋าดิจิทัล เป็นตัวอย่างอ้างอิงสำหรับการออกแบบกระเป๋าดิจิทัลสำหรับเอกสารรับรอง ซึ่งคำนึงถึงช่องทางการแลกเปลี่ยนข้อมูลทั้งระยะใกล้และไกล และสถานการณ์ที่ผู้ใช้งานหรือผู้ตรวจสอบเอกสารอาจไม่ได้เชื่อมต่อกับอินเตอร์เน็ต โดยที่ยังคงมีความยืดหยุ่นในการออกแบบกระเป๋าดิจิทัลตามความเหมาะสมต่อกรณีการใช้งานที่หลากหลาย

ตัวอย่างเช่น กรณีที่กระเป๋าดิจิทัลเป็นแอปพลิเคชันบนอุปกรณ์เคลื่อนที่ (mobile application) อาจจำเป็นต้องใช้องค์ประกอบที่เชื่อถือได้ (trusted component) เพิ่มเติม ซึ่งไม่ใช่ส่วนหนึ่งของแอปพลิเคชันนั้น แต่ยังถือว่าเป็นส่วนหนึ่งของกระเป๋าดิจิทัล เช่น ฮาร์ดแวร์ภายนอกสำหรับการจัดเก็บข้อมูล (external trusted storage) หรือองค์ประกอบอื่นที่เชื่อมต่อกับอุปกรณ์เคลื่อนที่จากทางไกล (remote component)

สถาปัตยกรรมซอฟต์แวร์ของกระเป๋าดิจิทัล มีองค์ประกอบซึ่งจัดรวมกลุ่มโดยคำนึงถึงคุณสมบัติการใช้งาน (functional block) แสดงตามรูปที่ 6 ดังนี้



รูปที่ 6 สถาปัตยกรรมซอฟต์แวร์ของกระเป๋าดิจิทัล

(1) อุปกรณ์เข้ารหัสลับ (cryptographic device) ทำหน้าที่ดังนี้

- จัดเก็บและบริหารจัดการกุญแจเข้ารหัสของผู้ใช้งาน (user keys) และข้อมูลอื่น ๆ ที่เกี่ยวกับกระบวนการเข้ารหัสลับ เช่น ใบรับรอง (digital certificate) ที่ออกโดยผู้ให้บริการออกใบรับรอง (certification authority)
- จัดเก็บข้อมูลสำหรับการยืนยันตัวตนผู้ใช้งาน เช่น เลขรหัสส่วนตัว และข้อมูลชีวมิติ
- ดำเนินการอัลกอริทึมการเข้ารหัสลับ (cryptographic algorithm) เช่น อัลกอริทึมสำหรับระบบรหัสแบบสมมาตร (symmetric) ระบบรหัสแบบอสมมาตร (asymmetric) และฟังก์ชันแฮช (hash function)

อุปกรณ์เข้ารหัสลับอาจประกอบด้วยอุปกรณ์ฮาร์ดแวร์เฉพาะสำหรับกุญแจเข้ารหัสและข้อมูลรหัสลับ เช่น secure environment (SE), trusted execution environment (TEE) หรือ hardware security module (HSM) ซึ่งอาจอยู่ภายในอุปกรณ์ที่ดำเนินการกระเป๋าดิจิทัลหรือเชื่อมต่อทางไกล

(2) ที่จัดเก็บข้อมูล (data storage) ทำหน้าที่จัดเก็บข้อมูลต่าง ๆ เช่น ตัวระบุเฉพาะ (unique identifier) คุณลักษณะ (attribute) ข้อมูลส่วนบุคคล และเอกสารรับรอง (credential) ของผู้ใช้งาน

(3) แอปพลิเคชันสร้างเอกสารสำแดง (presentation creation application) ทำหน้าที่เชื่อมต่อกับองค์ประกอบอื่นภายในกระเป๋าดิจิทัล เพื่อนำข้อมูลที่เกี่ยวข้องมาสร้างเอกสารสำแดงตามคำสั่งของผู้ใช้งาน

(4) แอปพลิเคชันสนับสนุนการใช้งานกระเป๋าดิจิทัล (wallet driving application) ทำหน้าที่เป็นอินเตอร์เฟสให้กับผู้ใช้งาน (user interface) เพื่อการใช้งานและควบคุมการทำงานของกระเป๋าดิจิทัล และทำหน้าที่จัดเก็บบันทึกเหตุการณ์ (log) และประวัติการใช้งานของกระเป๋าดิจิทัล

(5) อินเตอร์เฟสภายนอก (external interface) ทำหน้าที่เชื่อมต่อและแลกเปลี่ยนข้อมูลกับเอนทิตีอื่น ซึ่งอาจเป็นช่องทางในรูปแบบออนไลน์หรือออฟไลน์

(6) อุปกรณ์ต่อพ่วงเคลื่อนที่ (mobile perimeter) เป็นอุปกรณ์เสริมที่เชื่อมต่อกับอุปกรณ์ที่ดำเนินการกระเป๋าดิจิทัล รวมถึงเซ็นเซอร์ของอุปกรณ์เคลื่อนที่ เช่น กล้องถ่ายรูป เครื่องอ่าน NFC หรือเครื่องอ่านลายนิ้วมือ

(7) องค์ประกอบต่อพ่วงที่เชื่อถือได้ (trusted component perimeter) เป็นอุปกรณ์เสริมที่เชื่อมต่อกับอุปกรณ์ที่ดำเนินการกระเป๋าดิจิทัล ซึ่งทำหน้าที่เกี่ยวกับการเข้ารหัสลับ เช่น การใช้กุญแจรหัสลับโดยเชื่อมต่อกับระบบ back-end ผ่านช่องทางระยะไกล

5.3 ช่องทางการแลกเปลี่ยนเอกสารรับรอง

การแลกเปลี่ยนเอกสารรับรองในกรณีการใช้งานจริงสามารถทำได้หลากหลายรูปแบบ โดยกระเป๋าดิจิทัลควรรองรับช่องทางการแลกเปลี่ยนเอกสารรับรองอย่างน้อย 1 ช่องทางจาก 4 ช่องทาง ดังนี้

(1) ช่องทางระยะใกล้โดยผู้ตรวจสอบเอกสารเป็นบุคคล (proximity supervised flow)
(2) ช่องทางระยะใกล้โดยระบบอัตโนมัติ (proximity unsupervised flow)
(3) ช่องทางระยะไกลข้ามอุปกรณ์ (remote cross-device flow)
(4) ช่องทางระยะไกลภายในอุปกรณ์เดียวกัน (remote same-device flow)

ช่องทางที่ (1) และ (2) เป็นช่องทางระยะใกล้ โดยผู้ถือเอกสารและผู้ตรวจสอบเอกสารอยู่ในระยะที่ใกล้กัน ทำให้สามารถแสดงเอกสารสำแดงได้โดยไม่จำเป็นต้องเชื่อมต่อกับอินเตอร์เน็ต เช่น การแลกเปลี่ยนเอกสารรับรองผ่านโพรโทคอล 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) ผู้ถือเอกสารขอใช้บริการกับผู้ตรวจสอบเอกสารบนอุปกรณ์อื่นที่ไม่ใช่อุปกรณ์ที่กระเป๋าดิจิทัลดำเนินการอยู่ เช่น การใช้กระเป๋าดิจิทัลบนอุปกรณ์โทรศัพท์มือถือสแกน QR code ที่ปรากฏบนจอคอมพิวเตอร์แล็ปท็อป เพื่อจัดส่งเอกสารรับรองและขอเข้าใช้บริการเว็บไซต์บนเบราว์เซอร์ของคอมพิวเตอร์แล็ปท็อปนั้น ส่วนในช่องทางที่ (4) ผู้ถือเอกสารใช้บริการดิจิทัลโดยใช้กระเป๋าดิจิทัลซึ่งดำเนินการภายในอุปกรณ์เครื่องเดียวกัน

ทั้งนี้ การแลกเปลี่ยนเอกสารรับรองผ่านช่องทางต่าง ๆ ตามที่ระบุ อาจดำเนินการได้โดยมีการเชื่อมต่อกับอินเทอร์เน็ตหรือไม่ก็ได้ ดังนี้

- ผู้ถือเอกสารและผู้ตรวจสอบเอกสารเชื่อมต่อกับอินเทอร์เน็ต (both online)
- ผู้ถือเอกสารเท่านั้นที่เชื่อมต่อกับอินเทอร์เน็ต (only the user is online)
- ผู้ตรวจสอบเอกสารเท่านั้นที่เชื่อมต่อกับอินเทอร์เน็ต (only the verifier is online)
- ผู้ถือเอกสารและผู้ตรวจสอบเอกสารไม่ได้เชื่อมต่อกับอินเทอร์เน็ต (both offline)

6. ข้อแนะนำของกระเป๋าดิจิทัลและเอกสารรับรอง

ข้อแนะนำเบื้องต้นของกระเป๋าดิจิทัลและเอกสารรับรอง จะช่วยให้การให้บริการกระเป๋าดิจิทัลและการแลกเปลี่ยนเอกสารรับรองมีความมั่นคงปลอดภัยและคุ้มครองข้อมูลส่วนบุคคลของเอนทิตีต่าง ๆ ที่เกี่ยวข้อง รวมถึงช่วยจำกัดความซับซ้อนของรายละเอียดทางเทคนิค (technical solution) เพื่อให้กระเป๋าดิจิทัลและเอกสารรับรองสามารถทำงานร่วมกันได้

6.1 ประเภทของเอกสารรับรองตามความสำคัญของข้อมูล

เอกสารรับรองสามารถแบ่งออกเป็น 2 ประเภท ตามความสำคัญของข้อมูลในเอกสารรับรอง ดังนี้

(1) **เอกสารรับรองประเภท 1** เป็นเอกสารรับรองที่มีข้อมูลสำคัญ ซึ่งเหมาะสำหรับการระบุตัวตนบุคคลในธุรกรรมที่มีความเสี่ยงสูง ตัวอย่างเช่น บัตรประจำตัวประชาชน ใบอนุญาตขับขี่

(2) **เอกสารรับรองประเภท 2** เป็นเอกสารรับรองที่มีข้อมูลทั่วไป ซึ่งเหมาะสำหรับการใช้งานที่หลากหลายในธุรกรรมที่ไม่มีความเสี่ยงสูง ตัวอย่างเช่น บัตรสะสมคะแนน ตั๋วโดยสารที่ไม่ระบุชื่อผู้ถือตั๋ว

6.2 ข้อแนะนำของเอกสารรับรอง

ข้อแนะนำเบื้องต้นของเอกสารรับรอง มีรายละเอียดดังนี้

(1) เอกสารรับรองต้องมีข้อมูลที่จำเป็นในการระบุตัวตนของผู้ออกเอกสาร

(2) เอกสารรับรองต้องมีข้อมูลที่จำเป็นในการตรวจสอบความครบถ้วนสมบูรณ์ (data integrity) เพื่อให้สามารถตรวจพบการเปลี่ยนแปลงใด ๆ ที่เกิดกับความถูกต้องครบถ้วนของเอกสารรับรองได้

(3) เอกสารรับรองต้องมีข้อมูลที่จำเป็นในการตรวจสอบที่มา (authenticity) ของเอกสารรับรองว่าออกโดยผู้ออกเอกสารตามที่ระบุจริง

(4) เอกสารรับรองต้องมีข้อมูลที่จำเป็นในการตรวจสอบสถานะของเอกสารรับรอง

(5) เมื่อมีการแสดงเอกสารรับรองต่อผู้ตรวจสอบเอกสารในรูปแบบเอกสารสำแดง ผู้ตรวจสอบเอกสารสามารถตรวจสอบการเชื่อมโยงของผู้ถือเอกสารต่อเอกสารรับรอง (holder binding) ดังนี้

- เอกสารรับรองประเภท 1 ต้องมีข้อมูลที่จำเป็นในการตรวจสอบการเชื่อมโยงของผู้ถือเอกสารต่อเอกสารรับรอง
- เอกสารรับรองประเภท 2 ควรมีข้อมูลที่จำเป็นในการตรวจสอบการเชื่อมโยงของผู้ถือเอกสารต่อเอกสารรับรอง

6.3 ข้อแนะนำการพัฒนาองค์ประกอบของกระเป๋าดิจิทัล

ข้อแนะนำเบื้องต้นสำหรับการพัฒนาองค์ประกอบพื้นฐานของกระเป๋าดิจิทัล (หัวข้อ 5.1) เพื่อให้รองรับการใช้งานกับเอกสารรับรองประเภท 1 และ 2 มีรายละเอียดดังนี้

ตารางที่ 1 ข้อแนะนำการพัฒนาองค์ประกอบพื้นฐานของกระเป๋าดิจิทัล ให้รองรับเอกสารประเภท 1 และ 2

องค์ประกอบของกระเป๋าดิจิทัล	ข้อแนะนำ	ประเภท 1	ประเภท 2
ระบบบริหารจัดการกุญแจเข้ารหัส (cryptographic key management system)	กระเป๋าดิจิทัลใช้องค์ประกอบใดองค์ประกอบหนึ่ง จากรายการต่อไปนี้ ในการจัดเก็บและบริหารจัดการกุญแจเข้ารหัส – secure element หรือ trusted execution environment (TEE) ซึ่งอยู่ภายใน (embedded) อุปกรณ์ที่ดำเนินการกระเป๋าดิจิทัล – อุปกรณ์เชื่อมต่อจากภายนอก (external device) เช่น smart card – เชื่อมต่อกับ hardware security module (HSM) ผ่านระบบ backend จากทางไกล (remote)	ต้อง	ควร
	กระเป๋าดิจิทัลใช้มาตรการรักษาความมั่นคงปลอดภัยเพื่อป้องกันการส่งออก (export) ข้อมูลเข้ารหัส (cryptographic secret) เช่น กุญแจส่วนตัว	ต้อง	ควร
โพรโทคอลการแลกเปลี่ยนเอกสารสำแดง (attestation exchange protocol)	กระเป๋าดิจิทัลรองรับโพรโทคอล OpenID connect for verifiable presentation (OpenID4VP) [11] ในการแสดงเอกสารสำแดง สำหรับช่องทางระยะไกล (remote flow)	ต้อง	อาจ
	กระเป๋าดิจิทัลรองรับโพรโทคอล self-issued OpenID provider version 2 (SIOPv2) [12] ในกรณีที่ใช้การยืนยันตัวตนแบบอาศัยนามแฝง (pseudonymous authentication)	ควร	ควร
	กระเป๋าดิจิทัลรองรับโพรโทคอลตามที่กำหนดใน ISO/IEC 18013-5:2021 [6] ในการแสดงเอกสารสำแดง สำหรับช่องทางระยะใกล้ (proximity flow)	ต้อง	อาจ
	กระเป๋าดิจิทัลสามารถตรวจสอบว่าการทำธุรกรรมหนึ่ง ๆ เกิดขึ้นภายใน session เดียวกัน (session binding) เพื่อป้องกันไม่ให้ผู้อื่นที่ไม่ได้รับอนุญาตปลอมตัวเข้ามาทำธุรกรรมแทน	ควร	อาจ
	กระเป๋าดิจิทัลรองรับโพรโทคอลการแสดงเอกสารสำแดงอื่น ๆ	อาจ	อาจ
	กระเป๋าดิจิทัลสามารถพิสูจน์ว่าผู้ถือเอกสารเป็นผู้ครอบครองเอกสารรับรองจริง (proof of possession)	ต้อง	อาจ
	กระเป๋าดิจิทัลรองรับการเลือกเปิดเผยข้อมูล (selective disclosure) ในรูปแบบ mobile security object (MSO) ตามที่กำหนดใน ISO/IEC 18013-5:2021 [6]	ต้อง	อาจ

องค์ประกอบของกระเป๋าดิจิทัล	ข้อแนะนำ	ประเภท 1	ประเภท 2
	กระเป๋าดิจิทัลรองรับการเลือกเปิดเผยข้อมูล (selective disclosure) ตามที่กำหนดใน selective disclosure for JWT (SD-JWT) [13]	ต้อง	อาจ
โพรโทคอลการออกเอกสารรับรอง (issuance protocol)	กระเป๋าดิจิทัลรองรับโพรโทคอล OpenID connect for verifiable credential issuance (OpenID4VCI) [14] สำหรับการออกเอกสารรับรอง	ต้อง	ต้อง
	กระเป๋าดิจิทัลรองรับโพรโทคอลการออกเอกสารรับรองอื่น ๆ	อาจ	อาจ
โครงสร้างข้อมูลของเอกสารรับรอง (data model)	กระเป๋าดิจิทัลรองรับเอกสารที่มีโครงสร้างข้อมูลตามที่กำหนดใน ISO/IEC 18013-5:2021 [6]	ต้อง	ควร
	กระเป๋าดิจิทัลรองรับเอกสารที่มีโครงสร้างข้อมูลตามที่กำหนดใน W3C Verifiable Credentials Data Model 1.1 [5]	ต้อง	ควร
รูปแบบของเอกสารรับรอง (credential format)	กระเป๋าดิจิทัลรองรับเอกสารรับรองในรูปแบบ JSON web token (JWT) [15] และ SD-JWT [13]	ต้อง	อาจ
	กระเป๋าดิจิทัลรองรับเอกสารรับรองในรูปแบบ concise binary object representation (CBOR) [16]	ต้อง	อาจ
	กระเป๋าดิจิทัลรองรับเอกสารรับรองในรูปแบบ JSON for linked data (JSON-LD) [17]	อาจ	อาจ
รูปแบบของลายมือชื่อดิจิทัลและการเข้ารหัสลับ (signature and encryption format)	กระเป๋าดิจิทัลรองรับลายมือชื่อดิจิทัลและการเข้ารหัสลับในรูปแบบ JSON object signing and encryption (JOSE) [15]	ต้อง	อาจ
	กระเป๋าดิจิทัลรองรับลายมือชื่อดิจิทัลและการเข้ารหัสลับในรูปแบบ CBOR object signing and encryption (COSE) [18]	ต้อง	อาจ
	กระเป๋าดิจิทัลรองรับลายมือชื่อดิจิทัลและการเข้ารหัสลับในรูปแบบ linked data proof (LD-Proof) [19]	ต้องไม่	อาจ
กลไกการเข้ารหัสลับ (cryptographic suites and mechanism)	กระเป๋าดิจิทัลรองรับกลไกการเข้ารหัสลับตามที่กำหนดใน SOG-IS Agreed Cryptographic Mechanisms Version 1.2 [20]	ต้อง	ควร

ข้อแนะนำการพัฒนาองค์ประกอบพื้นฐานของกระเป๋าดิจิทัล สามารถสรุปเป็นภาพรวมตามรูปที่ 7 ดังนี้

(1) เอกสารรับรองประเภท 1 รองรับมาตรฐานทั้ง 2 รูปแบบ ดังนี้

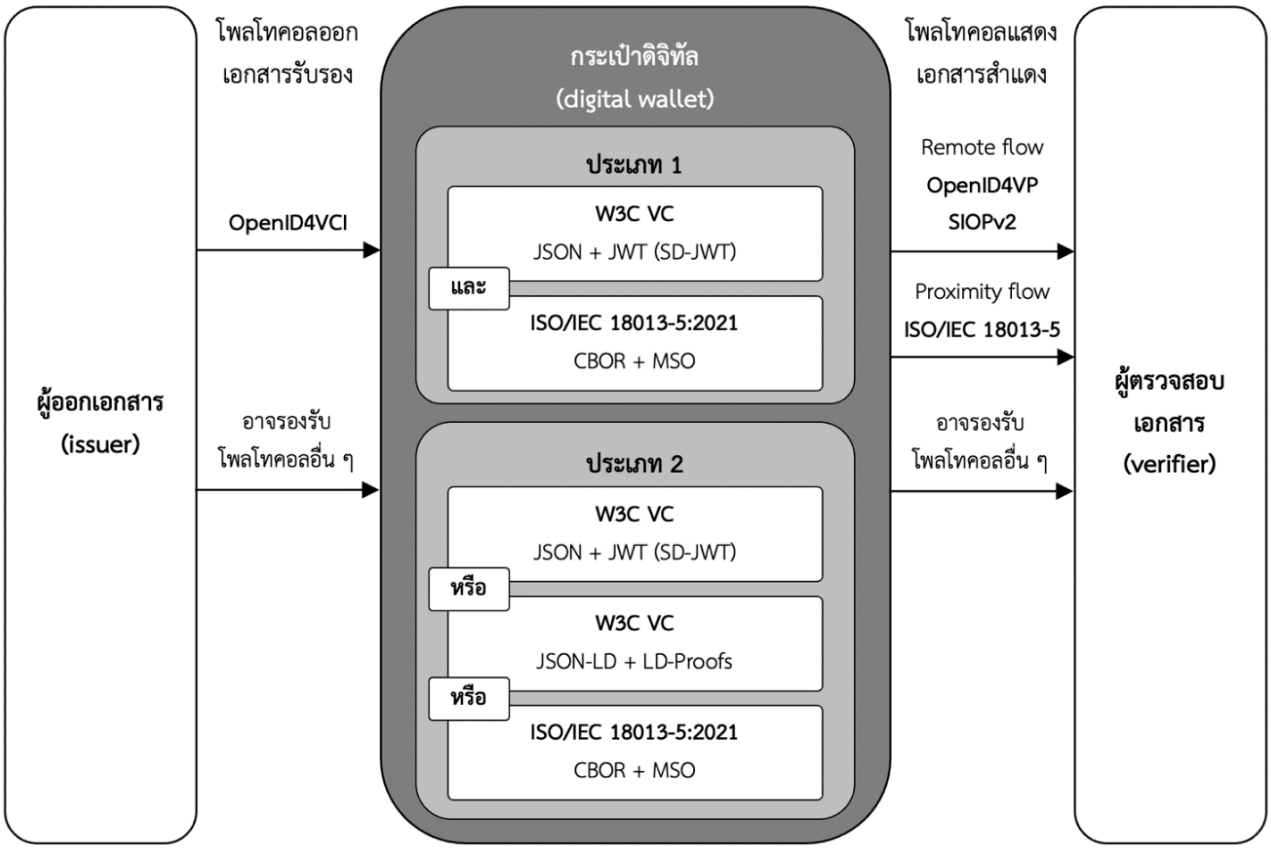
- โครงสร้างข้อมูล W3C VC ในรูปแบบ JWT ซึ่งใช้การเลือกเปิดเผยข้อมูลในรูปแบบ SD-JWT
- โครงสร้างข้อมูล ISO/IEC 18013-5 ในรูปแบบ CBOR ซึ่งใช้การเลือกเปิดเผยข้อมูลในรูปแบบ MSO

(2) เอกสารรับรองประเภท 2 รองรับมาตรฐานอย่างใดอย่างหนึ่งจาก 3 รูปแบบ ดังนี้
   - โครงสร้างข้อมูล W3C VC ในรูปแบบ JWT ซึ่งใช้การเลือกเปิดเผยข้อมูลในรูปแบบ SD-JWT
   - โครงสร้างข้อมูล W3C VC ในรูปแบบ JSON-LD และ LD-Proof
   - โครงสร้างข้อมูล ISO/IEC 18013-5 ในรูปแบบ CBOR ซึ่งใช้การเลือกเปิดเผยข้อมูลในรูปแบบ MSO

(3) กระเป๋าดิจิทัลรองรับโพรโทคอล OpenID4VCI ในการออกเอกสารรับรอง

(4) กระเป๋าดิจิทัลรองรับโพรโทคอล OpenID4VP และ SIOPv2 ในการแสดงเอกสารสำแดง สำหรับช่องทางระยะไกล (remote flow)

(5) กระเป๋าดิจิทัลรองรับโพรโทคอลตาม ISO/IEC 18013-5 ในการแสดงเอกสารสำแดง สำหรับช่องทางระยะใกล้ (proximity flow)



รูปที่ 7 ภาพรวมของข้อแนะนำการพัฒนาองค์ประกอบของกระเป๋าดิจิทัล

บรรณานุกรม

[1] European Commission, "The European Digital Identity Wallet Architecture and Reference Framework Version 1.0.0", January 2023.

[2] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วย โครงสร้างข้อมูลของเอกสารรับรองและเอกสารสำแดง เลขที่ ขมธอ. 24-2563, เวอร์ชัน 1.0.

[3] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วย แนวทางการลงลายมือชื่ออิเล็กทรอนิกส์ เลขที่ ขมธอ. 23-2563, เวอร์ชัน 1.0.

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

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

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

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

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

[9] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วย การพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการยืนยันตัวตน เลขที่ ขมธอ. 20-2566, เวอร์ชัน 3.0.

[10] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วย การพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการพิสูจน์ตัวตน เลขที่ ขมธอ. 19-2566, เวอร์ชัน 3.0.

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

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

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

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

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

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

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

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

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

[20] SOG-IS Crypto Working Group, "SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms Version 1.2", January 2020.

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

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

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

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

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

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

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

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

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

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

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

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

วิเคราะห์และจัดทำรายงานทางเทคนิค
กรอบการทำงานร่วมกันของกระเป๋าดิจิทัลสำหรับเอกสารรับรอง

นางสาวขนิษฐ์ ผาทอง	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายศุภโชค จันทรประทิน	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายณัฐฑพัฒน์ โรจนศุภมิตร	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นางสาววราภรณ์ หลีสกุล	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายวีรศักดิ์ ดีอ่ำ	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายพงษ์พันธ์ ศรีปาน	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายสมบัติ ชั้นอินทร์งาม	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายจิรายุ ภู่โต	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
บริษัท ฟินีม่า จำกัด	

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี)
ชั้น 20-22 เลขที่ 33/4 ถนนพระราม 9 แขวงห้วยขวาง
เขตห้วยขวาง กรุงเทพฯ 10310
โทรศัพท์ : 02 123 1234
โทรสาร : 02 123 1200