เวอร์ชัน 1.1

รายงานทางเทคนิค

Technical Report

กรอบแนวทางการทำงานร่วมกันของเอกสารรับรองดิจิทัลสำหรับประเทศไทย

THAI VC ARCHITECTURE AND REFERENCE FRAMEWORK

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ETDA
มกราคม 2568

รายงานทางเทคนิค

Technical Report

กรอบแนวทางการทำงานร่วมกันของเอกสารรับรองดิจิทัลสำหรับประเทศไทย

THAI VC ARCHITECTURE AND REFERENCE FRAMEWORK

เวอร์ชัน 1.1

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

มกราคม 2568

ตารางบันทึกประวัติการแก้ไข/ทบทวนเอกสาร

แก้ไขครั้งที่	วันที่	เวอร์ชันที่นำมาแก้ไข	รายละเอียดการแก้ไข/ทบทวนเอกสาร	เวอร์ชันหลังแก้ไข
-	2 ม.ค. 68	-	- ต้นฉบับ	1.0
1	6 ม.ค. 68	1.0	- เพิ่มรายละเอียดกระบวนการทำงาน OID4VCI บทที่ 5 เช่น คำอธิบายค่าพารามิเตอร์ ตัวอย่างการส่ง HTTP Request - เพิ่มรายละเอียดกระบวนการทำงาน OID4VP บทที่ 5 เช่น คำอธิบายค่าพารามิเตอร์ ตัวอย่างการส่ง HTTP Request	1.1

คำนำ

ปัจจุบันการใช้งานกระเป๋าเอกสารดิจิทัล (digital document wallet) ได้เข้ามามีบทบาทในการทำธุรกรรมทางอิเล็กทรอนิกส์ โดยกระเป๋าเอกสารดิจิทัลจะมีคุณสมบัติในการจัดเก็บกุญแจเข้ารหัส (cryptographic keys) เอกสารรับรองดิจิทัล (verifiable credentials: VC) ข้อมูลเกี่ยวกับอัตลักษณ์ (identity attributes) และข้อมูลส่วนบุคคลต่าง ๆ อย่างมั่นคงปลอดภัย และสามารถนำมาใช้ในการรับส่งเอกสารรับรองดิจิทัล เอกสารสำแดงดิจิทัล (verifiable presentation: VP) ที่สามารถตรวจสอบความถูกต้อง เพื่อเข้าถึงบริการทั้งจากภาครัฐและภาคเอกชน นอกจากนี้ กระเป๋าเอกสารดิจิทัลสามารถนำมาใช้ในการทำธุรกรรมออนไลน์ เช่น การลงทะเบียนขอใช้บริการบนเว็บไซต์ และรูปแบบออฟไลน์ เช่น การเข้ารับการรักษาในโรงพยาบาล รวมถึงใช้ในการสร้างลายมือชื่อดิจิทัล (digital signature) บนเอกสารหรือข้อมูลอิเล็กทรอนิกส์

เพื่อให้การให้บริการกระเป๋าเอกสารดิจิทัลและเอกสารรับรองดิจิทัลมีความน่าเชื่อถือและเป็นที่ยอมรับ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ จึงได้จัดทำรายงานทางเทคนิค เรื่อง กรอบแนวทางการทำงานร่วมกันของเอกสารรับรองดิจิทัลสำหรับประเทศไทย หรือ THAI VC ARCHITECTURE AND REFERENCE FRAMEWORK เพื่ออธิบายหลักการทำงาน วงจรชีวิต องค์ประกอบ และข้อแนะนำของเอกสารรับรองดิจิทัล และเอกสารสำแดงดิจิทัล เพื่อให้ผู้ให้บริการในระบบนิเวศของเอกสารรับรองดิจิทัล และผู้พัฒนาที่เกี่ยวข้องมีแนวทางที่สามารถนำไปปรับใช้ในการให้บริการและการพัฒนาระบบให้มีความมั่นคงปลอดภัย มีการคุ้มครองข้อมูลส่วนบุคคล และสามารถทำงานร่วมกันได้อย่างไร้รอยต่อ

รายงานฉบับนี้มีวัตถุประสงค์เพื่อเป็นแนวทางอ้างอิงในการดำเนินการให้ระบบการใช้งานเอกสารรับรองดิจิทัล และเอกสารสำแดงดิจิทัลในประเทศไทยสามารถทำงานร่วมกันได้ และช่วยลดความซับซ้อนของการพัฒนาเชิงเทคนิคที่อาจมีความแตกต่างกัน โดยได้รับการสนับสนุนข้อมูลจากการทำงานร่วมกันของคณะทำงานส่งเสริมการพัฒนาระบบเพื่อรองรับการใช้งาน Document Wallet และ Verifiable Credentials และผู้ที่เกี่ยวข้อง ที่ได้ร่วมกันศึกษาและหาแนวทางมาตรฐานที่จะใช้รับส่งข้อมูล ตลอดจนร่วมกันทดสอบการใช้งาน Document Wallet และ Verifiable Credentials เพื่อให้สามารถทำงานร่วมกันได้ และสามารถแลกเปลี่ยนข้อมูลได้อย่างปลอดภัยและน่าเชื่อถือ อย่างไรก็ตาม รายงานฉบับนี้อาจมีการปรับปรุงเนื้อหาเพิ่มเติมตามลักษณะการใช้งานและบริบทของระบบนิเวศในประเทศไทยและการเปลี่ยนแปลงของเทคโนโลยีในอนาคต

สารบัญ

สารบัญรูป

หน้า

กรอบแนวทางการทำงานร่วมกันของเอกสารรับรองดิจิทัลสำหรับประเทศไทย
(THAI VC ARCHITECTURE AND REFERENCE FRAMEWORK)

1. ขอบข่าย

รายงานฉบับนี้อธิบายหลักการทำงาน วงจรชีวิต องค์ประกอบของระบบการใช้งานเอกสารรับรองดิจิทัล (verifiable credential: VC) และเอกสารสำแดงดิจิทัล (verifiable presentation: VP) โดยมีวัตถุประสงค์เพื่อเป็นแนวทางอ้างอิงในการดำเนินการ (reference implementation) และช่วยลดความซับซ้อนของการพัฒนาเชิงเทคนิค ที่อาจมีความแตกต่างกัน เพื่อให้ผู้ให้บริการระบบและผู้พัฒนาที่เกี่ยวข้องสามารถนำไปปรับใช้ในการให้บริการและการพัฒนาระบบให้มีความมั่นคงปลอดภัย มีการคุ้มครองข้อมูลส่วนบุคคลและสามารถทำงานร่วมกันได้ระหว่างระบบการใช้งานเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัลในประเทศไทย

รายงานฉบับนี้**ไม่ครอบคลุม**ถึงขั้นตอนการพิสูจน์และยืนยันตัวตนของบุคคลธรรมดาและนิติบุคคล การสร้างตัวระบุแบบกระจายศูนย์ (Decentralized Identifiers: DID) สำหรับบุคคลธรรมดาและนิติบุคคล แต่ให้ความสำคัญในส่วนขั้นตอนการทำงานร่วมกัน (Interoperability) ของ ผู้ออกเอกสาร (issuer) ผู้ถือเอกสาร (holder) และผู้ตรวจสอบเอกสาร (verifier) ซึ่งทั้งสามเป็นส่วนประกอบสำคัญ (component) ในระบบนิเวศของเอกสารรับรองดิจิทัล (VC Ecosystem)

2. บทนิยาม

ความหมายของคำที่ใช้ในรายงานฉบับนี้ มีดังต่อไปนี้

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

2.2 กระเป๋าเอกสารดิจิทัล (digital document wallet) หมายถึง โปรแกรมที่จัดเก็บและช่วยให้ผู้ถือเอกสารสามารถเข้าถึงและใช้งาน VC ได้อย่างมั่นคงปลอดภัย [2]

2.3 ผู้ให้บริการกระเป๋าเอกสารดิจิทัล (digital document wallet provider) หมายถึง เอนทิตีที่ทำหน้าที่พัฒนาและ/หรือดำเนินการเกี่ยวกับกระเป๋าเอกสารดิจิทัล ให้แก่ผู้ออกเอกสาร ผู้ถือเอกสาร หรือผู้ตรวจสอบเอกสาร

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

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

2.6 เอกสารรับรองดิจิทัล (verifiable credential: VC) หมายถึง ชุดของข้อความยืนยันอย่างน้อยหนึ่งรายการที่ถูกรับรองโดยผู้ออกเอกสาร (issuer) ทั้งนี้ VC มีคุณสมบัติที่สามารถตรวจพบการเปลี่ยนแปลงใด ๆ ที่เกิดกับความถูกต้องครบถ้วนของข้อมูล และตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ของผู้ออกเอกสารได้ด้วยกระบวนการเข้ารหัสลับ [2]

<u>ข้อสังเกต:</u> ข้อความยืนยันใน VC อาจเกี่ยวกับเจ้าของข้อความ (subject) ที่มากกว่าหนึ่งราย เช่น ข้อความยืนยันในทะเบียนสมรส

2.7 เอกสารสำแดงดิจิทัล (verifiable presentation: VP) หมายถึง VC อย่างน้อยหนึ่งชุด ที่ผู้ถือเอกสาร (holder) ใช้แสดงต่อผู้ตรวจสอบเอกสาร (verifier) ทั้งนี้ VP มีคุณสมบัติที่สามารถตรวจพบการเปลี่ยนแปลงใด ๆ ที่เกิดกับความถูกต้องครบถ้วนของข้อมูล และตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ของผู้ถือเอกสารและตรวจสอบ VCเกี่ยวข้องได้ด้วยกระบวนการเข้ารหัสลับ [2]

2.8 เอนทิตี (entity) หมายถึง สิ่งที่มีอยู่จริง เช่น บุคคล องค์กร หรืออุปกรณ์ ซึ่งถูกกล่าวอ้างในการใช้งาน VC และ VP [2]

2.9 ผู้ออกเอกสาร (issuer) หมายถึง เอนทิตีที่ทำหน้าที่รับรองข้อความยืนยันโดยออกเป็น VC ให้แก่ผู้ถือเอกสาร [2]

2.10 ผู้ถือเอกสาร (holder) หมายถึง เอนทิตีที่เป็นเจ้าของ VC อย่างน้อยหนึ่งชุด โดยจัดเก็บไว้ในกระเป๋าเอกสารดิจิทัล (digital document wallet) และสามารถใช้ VC สร้างเป็น VP [2] ทั้งนี้ ผู้ถือเอกสารมีอีกชื่อเรียกหนึ่งว่า ผู้ใช้งานกระเป๋าเอกสารดิจิทัล

2.11 ผู้ตรวจสอบเอกสาร (verifier) หมายถึง เอนทิตีที่สามารถตรวจสอบความถูกต้องครบถ้วนของ VC และ VP ด้วยกระบวนการเข้ารหัสลับ รวมถึงตรวจสอบสถานะการใช้งานและความสอดคล้องตามโครงสร้างข้อมูลของ VC และ VP [2]

2.12 ระบบทะเบียนเอกสารรับรอง (verifiable data registry) หมายถึง ระบบที่ช่วยสนับสนุนการสร้างและการตรวจสอบความถูกต้องครบถ้วนของ VC และ VP โดยข้อมูลที่มีการจัดเก็บในระบบนี้ เช่น ตัวระบุ (identifier) และกุญแจสาธารณะ (public key) ของเอนทิตีที่เกี่ยวข้อง รวมถึงรายการเพิกถอน (revocation list) และเค้าร่าง (schema) ของ VC หรือ VP [2]

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

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

2.15 ตัวระบุแบบกระจายศูนย์ (decentralized identifier: DID) หมายถึง ตัวระบุ (identifier) ที่มีความคงอยู่ถาวร (persistence) ที่มีเอกลักษณ์เฉพาะในระดับสากล ซึ่งไม่จำเป็นต้องอาศัยหน่วยงานกลางผู้รับผิดชอบในการลงทะเบียน และมักถูกสร้างขึ้นและ/หรือลงทะเบียนโดยใช้วิธีการเข้ารหัสลับ [4]

2.16 DID subject หมายถึง เอนทิตีที่ถูกระบุโดย DID และถูกอธิบายไว้ใน DID Document [4]

2.17 DID document หมายถึง ชุดข้อมูลที่ใช้ในการอธิบาย DID subject รวมไปถึงกลไกที่เกี่ยวข้องกับ DID subject นั้น เช่น กุญแจสาธารณะที่ DID subject สามารถใช้ในการยืนยันตัวตนหรือพิสูจน์ความเกี่ยวข้องกับ DID นั้น [4]

2.18 DID method (Decentralized Identifiers Methodologies) หมายถึง กลไกเฉพาะสำหรับแต่ละ DID ที่ใช้ในการสร้าง ดึงข้อมูล (resolve) อัปเดต และระงับการใช้งาน DID รวมไปถึง DID document ที่เกี่ยวข้องกับ DID นั้น [4]

2.19 DID resolver หมายถึง ส่วนประกอบที่เป็นซอฟต์แวร์หรือฮาร์ดแวร์ที่ใช้ในกระบวนการ DID resolution ซึ่งทำงานโดยใช้ DID เป็นอินพุต และได้เอาต์พุตเป็น DID document [4]

2.20 Universal Resolver หมายถึง เครื่องมือหรือบริการที่ใช้สนับสนุนการทำงานร่วมกันระหว่างหลาย DID method ในกระบวนการ DID resolution และการดึงข้อมูล (resolve) DID Document

2.21 เค้าร่าง (schema) หมายถึง ข้อมูลที่กำหนดโครงสร้าง (structure) และรูปแบบ (format) ของ VC และ/หรือ VP โดยสามารถแบ่งออกเป็น 2 ประเภท ได้แก่ (1) เค้าร่างสำหรับการตรวจสอบข้อมูล (data verification schema) สำหรับตรวจสอบโครงสร้างและเนื้อหาของ VC และ (2) เค้าร่างสำหรับการเข้ารหัสข้อมูล (data encoding schema) สำหรับการแปลงเนื้อของ VC จากรูปแบบ (format) หนึ่งไปยังอีกรูปแบบหนึ่ง [5]

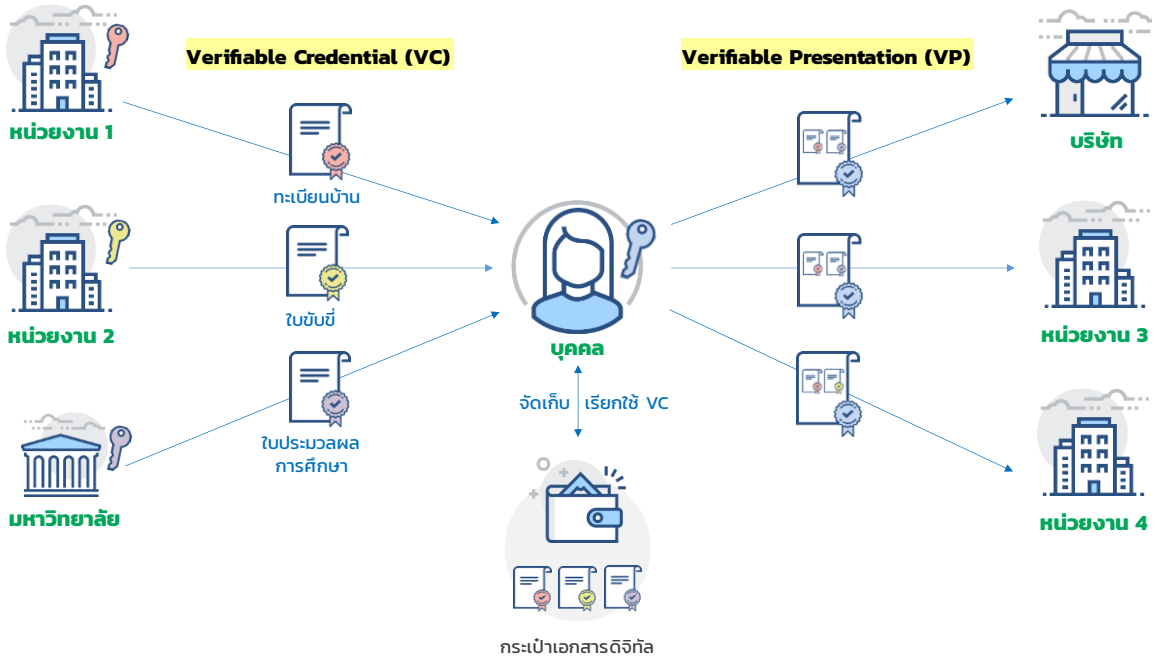
2.22 การทำงานร่วมกัน (interoperability) หมายถึง ความสามารถ (ทางเทคนิค) ในการแลกเปลี่ยนและใช้ข้อมูลระหว่างระบบ/ส่วนประกอบตั้งแต่สองระบบขึ้นไป ซึ่งทำงานร่วมกันได้โดยผู้ดำเนินการไม่จำเป็นต้องแทรกแซงการดำเนินการในแต่ละครั้ง [IEEE+ eHealth Governance Initiative]

3. ภาพรวมการใช้งาน

ในปัจจุบันเอกสารในรูปแบบของข้อมูลอิเล็กทรอนิกส์เริ่มมีการใช้งานแพร่หลายมากยิ่งขึ้น แต่การใช้งานยังคงถูกจำกัดอยู่ในแค่บางกรณี เนื่องจากการออกหนังสือหรือเอกสารบางส่วนยังคงอยู่ในรูปแบบกระดาษ ส่วนเอกสารอิเล็กทรอนิกส์ที่มีใช้งานอยู่นั้นก็มีรูปแบบและมาตรฐานที่หลากหลาย เอกสารที่ออกโดยหน่วยงานหนึ่งอาจต้องใช้วิธีการในการจัดเก็บและวิธีการในการตรวจสอบที่แตกต่างกันไปตามเทคโนโลยีที่ใช้งาน

การใช้งานเอกสารอิเล็กทรอนิกส์ในระยะหลัง เริ่มมีแนวคิดของการนำเอกสารรับรองดิจิทัล (verifiable credential: VC) และเอกสารสำแดงดิจิทัล (verifiable presentation: VP) มาใช้งาน โดยเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัลนั้น มีคุณสมบัติที่ช่วยให้สามารถตรวจสอบความถูกต้องของเอกสารได้ว่าเอกสารดังกล่าวออกโดยหน่วยงานนั้นจริง และบุคคลที่ยื่นเอกสารเป็นเจ้าของเอกสารนั้นจริง นอกจากนั้น ยังช่วยเพิ่มความเป็นส่วนตัวให้กับผู้ใช้งาน เนื่องจากในบางกรณี ผู้ใช้งานสามารถเลือกแสดงข้อมูลในเอกสารบางส่วนได้

อย่างไรก็ตาม การนำ VC และ VP มาใช้งานนั้น ระบบที่ให้บริการแต่ละระบบจำเป็นต้องมีความสามารถในการทำงานร่วมกัน (interoperability) เพื่อให้สามารถเชื่อมต่อกันได้และสามารถตรวจสอบข้อมูลข้ามระบบได้อย่างมีประสิทธิภาพ เนื่องจากเอกสารบางประเภทอาจมีความเกี่ยวข้องกับหลายหน่วยงานไม่ว่าจะเป็นองค์กรภาครัฐ บริษัทเอกชน สถาบันการศึกษา หรือบริการออนไลน์ต่าง ๆ



รูปที่ 1 ภาพรวมการใช้งานของเอกสารรับรองดิจิทัล

3.1 บทบาทและระบบที่เกี่ยวข้องกับการใช้งานเอกสารรับรองดิจิทัล

(1) ผู้สมัคร (applicant) และ ผู้ถือเอกสาร (holder)

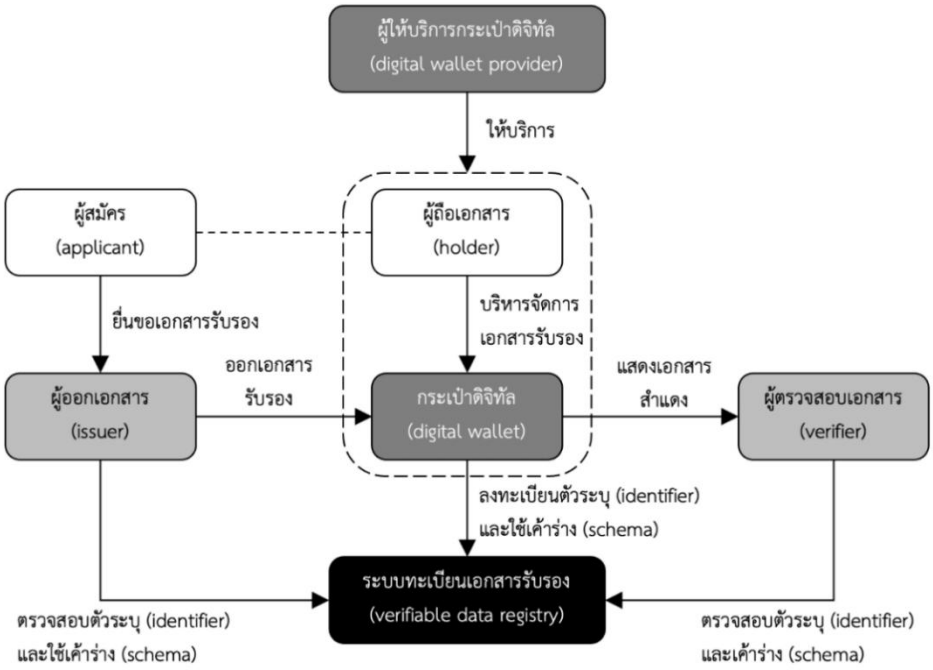
(2) ผู้ออกเอกสาร (issuer)

(3) ผู้ตรวจสอบเอกสาร (verifier)

(4) ผู้ให้บริการกระเป๋าเอกสารดิจิทัล (digital document wallet provider)

(5) ระบบทะเบียนเอกสารรับรอง (verifiable data registry)

การใช้งานกระเป๋าเอกสารดิจิทัลสำหรับเอกสารรับรองดิจิทัล ประกอบด้วยเอนทิตีและระบบที่เกี่ยวข้อง ได้แก่ ผู้สมัคร (applicant) ผู้ถือเอกสาร (holder) ผู้ออกเอกสาร (issuer) ผู้ตรวจสอบเอกสาร (verifier) ผู้ให้บริการกระเป๋าเอกสารดิจิทัล (digital document wallet provider) รวมไปถึงระบบทะเบียนเอกสารรับรอง (verifiable data registry) โดยบทบาทและความสัมพันธ์ของเอนทิตีที่เกี่ยวข้องเป็นไปตามรูปที่ 22



รูปที่ 2 บทบาทของผู้ที่เกี่ยวข้องกับการใช้งานเอกสารรับรองดิจิทัล

(1) ผู้สมัคร (applicant) ยื่นขอเอกสารรับรองดิจิทัลจากผู้ออกเอกสาร (issuer) พร้อมทั้งกำหนดให้จัดส่ง VC มายังกระเป๋าเอกสารดิจิทัลของผู้ถือเอกสาร (holder) ทั้งนี้ ผู้ออกเอกสารอาจกำหนดให้ผู้สมัครกรอกข้อมูลที่เกี่ยวข้องหรือแนบเอกสารเพิ่มเติม เพื่อให้ผู้ออกเอกสารตรวจสอบความถูกต้องก่อนออกเอกสารรับรองดิจิทัล

(2) ผู้ถือเอกสาร (holder) ใช้งานและควบคุมการทำงานกระเป๋าเอกสารดิจิทัลที่ให้บริการโดยผู้ให้บริการกระเป๋าเอกสารดิจิทัล (digital document wallet provider) โดยกระเป๋าเอกสารดิจิทัลนั้นอาจอยู่ในรูปแบบแอปพลิเคชันบนอุปกรณ์เคลื่อนที่หรือเว็บไซต์

<u>ข้อสังเกต:</u> ผู้สมัคร ผู้ถือเอกสาร และเจ้าของข้อความ (subject) อาจเป็นบุคคลเดียวกันหรือไม่ก็ได้ ตัวอย่างเช่น บิดาเป็นผู้สมัครยื่นขอเอกสารรับรองดิจิทัลซึ่งมีบุตรเป็นเจ้าของข้อความ จากนั้นจัดเก็บ VC เอกสารรับรอง ในกระเป๋าเอกสารดิจิทัลของมารดาซึ่งมีบทบาทเป็นผู้ถือเอกสาร

(3) ผู้ถือเอกสารสามารถสร้าง VP โดยใช้ข้อมูลจาก VC จากนั้นแสดง VP ต่อผู้ตรวจสอบเอกสาร (verifier) ซึ่งผู้ตรวจสอบเอกสารสามารถตรวจสอบความถูกต้องครบถ้วนของ VP ดังกล่าวได้ โดยอาศัยข้อมูลในระบบทะเบียนเอกสารรับรอง (verifiable data registry)

(4) ระบบทะเบียนเอกสารรับรอง (verifiable data registry) เป็นตัวกลางในการสนับสนุนการสร้างและตรวจสอบเอกสารรับรอง โดยทำหน้าที่ลงทะเบียนตัวระบุ (identifier) รวมไปถึงกุญแจสาธารณะ (public key) ของแต่ละเอนทิตี และเค้าร่าง (schema) ของ VC และ VP

ทั้งนี้ ผู้ออกเอกสารและผู้ตรวจสอบเอกสารอาจเป็นบุคคลซึ่งใช้งานกระเป๋าเอกสารดิจิทัลเช่นเดียวกันกับผู้ถือเอกสาร หรืออาจเป็นระบบขององค์กรที่ทำหน้าที่ออก VC เอกสารรับรองดิจิทัลหรือตรวจสอบ VP ในกรณีนี้ ระบบขององค์กรจะถือเป็นกระเป๋าเอกสารดิจิทัลขององค์กร (enterprise digital wallet) ซึ่งทำหน้าที่บริหารจัดการเอกสารรับรองดิจิทัลสำหรับองค์กรนั้น

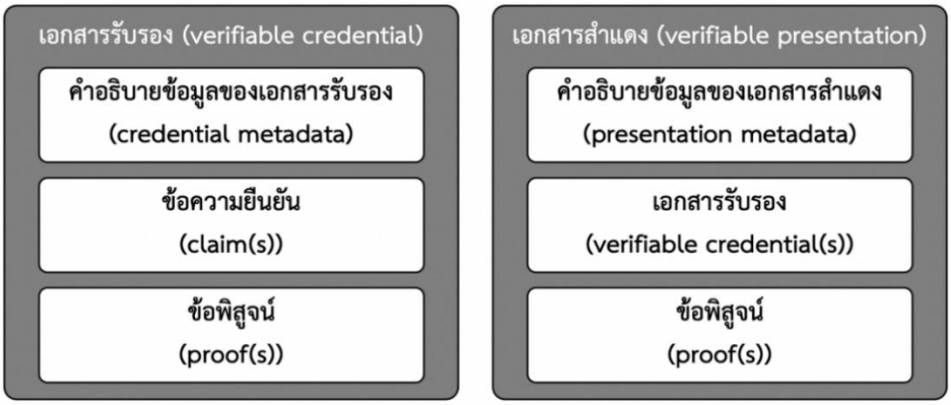
3.2 เอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล

เอกสารรับรองดิจิทัล (verifiable credential: VC) อาจเป็นเอกสารที่ออกโดยหน่วยงานของรัฐหรือเอกสารอิเล็กทรอนิกส์ใด ๆ ที่ออกให้เพื่อรับรองข้อความที่เกี่ยวข้องกับเจ้าของข้อความ (subject) ซึ่งเอกสารรับรองดิจิทัลนี้จะมีคุณสมบัติที่สามารถตรวจสอบได้ว่าเอกสารนั้นไม่ถูกเปลี่ยนแปลง และสามารถยืนยันตัวบุคคลผู้ออกเอกสารได้ ทั้งนี้ เมื่อพิจารณาตาม Verifiable Credentials Data Model ของ W3C จะสามารถสรุปองค์ประกอบของ VC ได้ ดังนี้

(1) คำอธิบายข้อมูล (metadata) ของ VC ซึ่งอาจรวมถึงตัวระบุ (identifier) ของเอนทิตีที่เกี่ยวข้อง ข้อมูลของผู้ออกเอกสาร หรือวันหมดอายุของเอกสารรับรอง
(2) ข้อความยืนยัน (claim) ซึ่งอาจมีเพียงข้อความยืนยันเดียวหรือหลายข้อความ โดยเป็นข้อมูลที่ยืนยันเกี่ยวกับเจ้าของข้อความ ซึ่งอาจเป็นบุคคลธรรมดา นิติบุคคล สิ่งของ หรือซอฟต์แวร์
(3) ข้อพิสูจน์ (proof) ของ VC ซึ่งอาจมีข้อพิสูจน์เดียวหรือหลายข้อพิสูจน์ โดยเป็นข้อมูลที่เป็นลายมือชื่อดิจิทัลของผู้ออกเอกสาร

เอกสารสำแดงดิจิทัล (verifiable presentation: VP) คือ ชุดข้อมูลที่ผู้ถือเอกสารสร้างขึ้นจาก VC โดย VP นั้นจะมีคุณสมบัติที่สามารถตรวจสอบได้ว่าเอกสารนั้นไม่ถูกเปลี่ยนแปลง (integrity) และสามารถยืนยันตัวผู้ถือเอกสารได้ (authenticity) ทั้งนี้ เมื่อพิจารณาตาม Verifiable Credentials Data Model ของ W3C จะสามารถสรุปองค์ประกอบของ VP ได้ ดังนี้

(1) คำอธิบายข้อมูล (metadata) ของ VP
(2) เอกสารรับรอง (verifiable credential: VC) ซึ่งอาจมี VC เดียวหรือหลาย VCก็ได้ ทั้งนี้ VP อาจไม่ใช้ข้อมูลจาก VC โดยตรง แต่อาจใช้ข้อมูลซึ่งสร้าง (derived) มาจาก VC อีกที
(3) ข้อพิสูจน์ (proof) ของ VP ซึ่งอาจมีข้อพิสูจน์เดียวหรือหลายข้อพิสูจน์ก็ได้ โดยเป็นข้อมูลที่เป็นลายมือชื่อดิจิทัลของผู้ถือเอกสาร



รูปที่ 3 องค์ประกอบพื้นฐานของเอกสารรับรองและเอกสารสำแดง

3.3 ระบบทะเบียนเอกสารรับรอง (verifiable data registry)

ในการใช้งานเอกสารรับรองดิจิทัล เอนทิตีที่เกี่ยวข้องจะใช้งานกระเป๋าเอกสารดิจิทัลร่วมกับระบบทะเบียนเอกสารรับรอง โดยระบบทะเบียนเอกสารรับรองจะถูกนำมาใช้สนับสนุนการทำงานและจัดเก็บข้อมูลต่าง ๆ เช่น

- ทะเบียนตัวระบุ (identifier) หรือตัวระบุแบบกระจายศูนย์ (decentralized identifier: DID) รวมไปถึง DID Document ของผู้ที่เกี่ยวข้อง เช่น ผู้ถือเอกสาร ผู้ออกเอกสาร หรือผู้ตรวจสอบเอกสาร

  ข้อสังเกต: การตรวจสอบ VC หรือ VP สามารถทำได้โดยการนำ DID ของ issuer หรือ holder มาใช้ในการดึงข้อมูล (resolve) DID Document ที่ถูกลงทะเบียนไว้ในระบบทะเบียนเอกสารรับรอง เพื่อนำ public key มาใช้ตรวจสอบลายมือชื่อดิจิทัล

- ทะเบียนเค้าร่างของเอกสารรับรอง (credential schema)

  ข้อสังเกต: เพื่อให้ผู้ออกเอกสาร (issuer) สามารถเลือกใช้งานเค้าร่างของเอกสารรับรองได้ เมื่อต้องมีการออกเอกสารรับรองในลักษณะเดียวกัน โดยเอกสารรับรองที่ออกตาม credential schema เดียวกัน จะมีโครงสร้าง (structure) เนื้อหา (content) และรูปแบบ (format) ที่สอดคล้องกัน

- ทะเบียนรายการเพิกถอนเอกสารรับรอง (revocation registry)

นอกจากนี้ ระบบทะเบียนเอกสารรับรองอาจถูกนำมาใช้เป็นทะเบียนรายชื่อของเอนทิตีต่าง ๆ ในระบบได้ เช่น

- รายชื่อผู้ให้บริการกระเป๋าเอกสารดิจิทัล (digital document wallet providers)
- รายชื่อผู้ออกเอกสาร (issuers)
- รายชื่อผู้ตรวจสอบเอกสาร (verifiers)
- รายชื่อผู้ให้บริการออกใบรับรอง (certification authorities: CA)

ทั้งนี้ ระบบทะเบียนเอกสารรับรองสามารถพัฒนาได้หลากหลายรูปแบบ เช่น รูปแบบรวมศูนย์ (centralized) ด้วยระบบฐานข้อมูล หรือรูปแบบกระจายศูนย์ (decentralized) ด้วยเทคโนโลยีบล็อกเชน (blockchain) หรือโครงสร้างพื้นฐานใบรับเหตุการณ์กุญแจ (key event receipt infrastructure: KERI) หรือรูปแบบผสม

4. องค์ประกอบที่ส่งเสริมให้เกิดการทำงานร่วมกัน (Interoperability)

เนื่องด้วยการใช้งานเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัลยังอยู่ในระยะเริ่มต้น การให้บริการในปัจจุบันจึงมีความหลากหลายทั้งในมิติเชิงธุรกิจและการพัฒนาระบบที่อ้างอิงกระบวนการทางเทคนิคหรือมาตรฐานที่แตกต่างกัน ในกรณีที่ต้องมีการขยายการใช้งานไปในวงกว้างหรือต้องการใช้งานเอกสารดังกล่าวข้ามระบบนิเวศ (Ecosystem) ก็อาจไม่สามารถทำงานร่วมกันได้ ดังนั้น ในการพัฒนาระบบเกี่ยวกับเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล ผู้พัฒนาควรให้ความสำคัญในรายละเอียดของเรื่องดังต่อไปนี้

- **มาตรฐานเกี่ยวกับ VC และ VP** เนื่องจากเอกสารรับรองดิจิทัลหรือเอกสารสำแดงดิจิทัลเป็นเอกสารที่ต้องมีการส่งต่อหรือแลกเปลี่ยนระหว่างหลายหน่วยงาน หากเอกสารดังกล่าวมีรูปแบบที่แตกต่างกัน เช่น หน่วยงาน A และ หน่วยงาน B ใช้เอกสารที่มีโครงสร้างข้อมูลที่แตกต่างกัน ก็อาจส่งผลต่อการประมวลผลแบบอัตโนมัติของระบบ หรือทำให้ไม่สามารถตรวจสอบเอกสารดังกล่าวได้
- **เค้าร่าง (schema)** เอกสารรับรองที่ออกโดยหน่วยงานต่าง ๆ อาจถูกออกแบบและใช้โครงสร้างข้อมูลที่แตกต่างกัน เมื่อต้องมีการส่งเอกสารข้ามหน่วยงาน หากเอกสารดังกล่าวไม่ได้ใช้เค้าร่างข้อมูลเดียวกัน ก็อาจส่งผลให้มีโครงสร้าง (structure) เนื้อหา (content) และรูปแบบ (format) ที่แตกต่างกัน ซึ่งส่งผลต่อประมวลผลแบบอัตโนมัติของระบบ หรือทำให้ไม่สามารถตรวจสอบเอกสารดังกล่าวได้
- **มาตรฐานเกี่ยวกับ Protocol สำหรับการออก VC** เพื่อให้การเชื่อมต่อในขั้นตอนของการออก VC โดยผู้ออกเอกสาร (issuer) มีความมั่นคงและปลอดภัย และระบบต่าง ๆ สามารถเชื่อมต่อกันได้ด้วยวิธีการที่เป็นมาตรฐานเดียวกัน
- **มาตรฐานเกี่ยวกับ Protocol สำหรับการใช้งาน VP** เพื่อให้การเชื่อมต่อในขั้นตอนของการใช้งาน VP ระหว่าง Digital Document Wallet และผู้ตรวจสอบเอกสาร รวมไปถึงผู้ถือเอกสารมีความมั่นคงและปลอดภัย และระบบต่าง ๆ สามารถเชื่อมต่อกันได้ด้วยวิธีการที่เป็นมาตรฐานเดียวกัน
- **มาตรฐานเกี่ยวกับตัวระบุ (identifier) ตัวระบุแบบกระจายศูนย์ (decentralized identifier: DID) และ DID Method** เนื่องจากเป็นส่วนสำคัญเกี่ยวกับการระบุตัวบุคคลที่เกี่ยวข้องและการตรวจสอบ VC และ VP ดังนั้น identifier รวมไปถึงในส่วนของ DID Document ควรมีฟังก์ชันและการบริหารจัดการต่าง ๆ ที่มีความมั่นคงปลอดภัย ไม่ถูกแก้ไขโดยไม่ได้รับอนุญาต และสามารถดึงข้อมูล (resolve) มาใช้เมื่อต้องการตรวจสอบ VC หรือ VP ได้
- **Universal Resolver** เนื่องจากในการตรวจสอบ VC และ VP นั้นต้องมีการดึงข้อมูล DID Document ที่ถูกจัดเก็บไว้ใน registry ของแต่ละ DID Method โดยการดึงข้อมูลดังกล่าว ส่วนใหญ่จะเป็นการดำเนินการผ่านช่องทาง resolver ของแต่ละ DID Method ดังนั้น ในกรณีที่มีการใช้งานหลาย DID Method ร่วมกัน ย่อมต้องมีการใช้ resolver หลายอัน หากมี Universal resolver ที่เป็นเสมือนศูนย์รวมของ resolver ก็จะช่วยให้สามารถเข้าใช้งานและดึงข้อมูล DID Document ได้ที่จุดเดียว

5. มาตรฐานและข้อปฏิบัติสำหรับเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล (Standards and Compliance for Verifiable Credentials and Presentations)

เมื่อการทำธุรกรรมมีแนวโน้มมาอยู่ในรูปแบบอิเล็กทรอนิกส์มากขึ้น หน่วยงานทั้งภาครัฐและภาคเอกชนอาจมีการออกเอกสารรับรองข้อมูลในรูปของเอกสารรับรองดิจิทัลที่ตรวจสอบได้ (verifiable credential: VC) ซึ่งเป็นวิธีการตามมาตรฐานของ World Wide Web Consortium (W3C) [5] โดยเอกสารรับรองดิจิทัลที่ตรวจสอบได้ดังกล่าวเป็นเอกสารรับรองข้อมูลในรูปแบบอิเล็กทรอนิกส์ที่มีคุณสมบัติช่วยให้สามารถตรวจพบการปลอมแปลงและตรวจสอบผู้เขียนข้อมูลได้ด้วยการกระบวนการเข้ารหัสลับ (Cryptography)

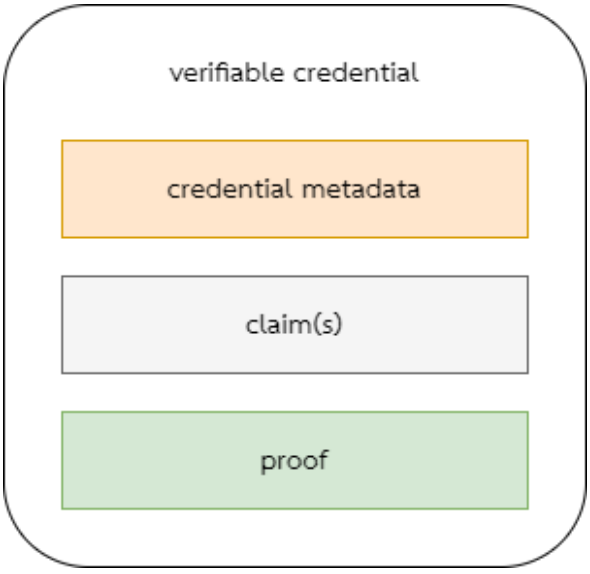
ในรายงานฉบับนี้ จะอ้างอิงรูปแบบเอกสารรับรองตามโครงสร้าง W3C VC Data Model v1.0 [5] โดยรูปแบบจะประกอบด้วย 2 ส่วนดังนี้

- เอกสารรับรองดิจิทัล (verifiable credential: VC)
- เอกสารสำแดงดิจิทัล (verifiable presentation: VP)

5.1 เอกสารรับรองดิจิทัล (verifiable credential: VC)

เอกสารรับรองดิจิทัล ประกอบด้วย identifier และคำอธิบายข้อมูล (metadata) เช่น ผู้ออกเอกสาร วันและเวลาเมื่อ VC เริ่มมีผลผูกพันและสิ้นผลผูกพัน

โครงสร้างของเอกสารรับรองดิจิทัลในรายงานทางเทคนิคฉบับนี้ ได้อ้างอิงโครงสร้างตาม World Wide Web Consortium (W3C) [5] สามารถแสดงตามรูปที่ 5 ซึ่งประกอบด้วย 3 ส่วน ได้แก่ (1) คำอธิบายข้อมูลของ VC (credential metadata) (2) ข้อความยืนยัน (claim) และ (3) ข้อพิสูจน์ (proof)



รูปที่ 4 โครงสร้างเอกสารรับรอง (VC)

ในรายงานฉบับนี้ ได้ยกตัวอย่างกรณีศึกษาของ VC ที่แสดงกรณีศึกษา เรื่องการขอใบประมวลผลการศึกษา (Transcript) ตามรูปที่ 6 จากมหาวิทยาลัย โดยเอกสารจะออกให้เมื่อนักศึกษาพิสูจน์ได้ว่าตนเองเคยศึกษา ณ มหาวิทยาลัยดังกล่าว ซึ่งทางมหาวิทยาลัยได้ออก VC เพื่อรับรองการสำเร็จการศึกษา และนักศึกษาจัดเก็บ VC นั้นไว้ในกระเป๋าเอกสารดิจิทัลของตนเอง ตัวอย่างของ VC ข้างต้นในรูปแบบ JSON-LD ตามตัวอย่างที่ 1 โดยในการทำระบบทดสอบ จะใช้ JWT Format ในการสร้างข้อมูล VC และ VP

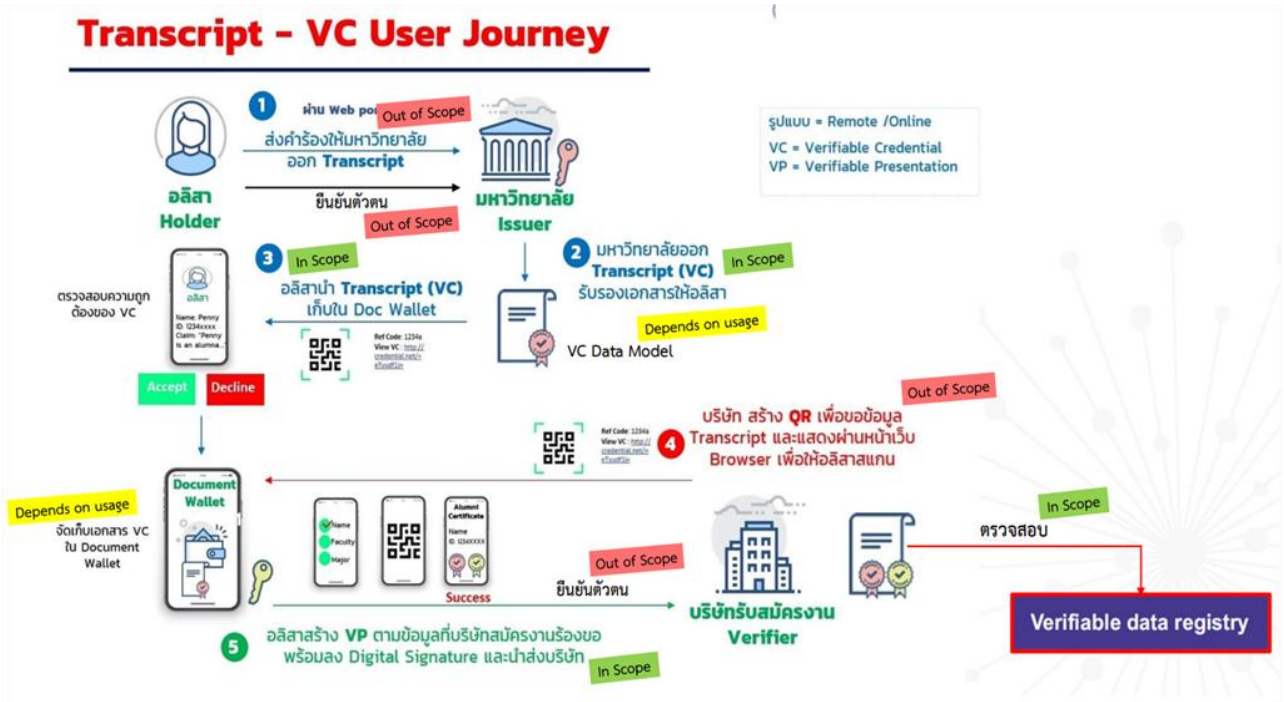
รูปที่ 5 VC JWT Format

โดย VC JWT Format จะแบ่งออกเป็น 3 ส่วน ซึ่งแต่ละส่วนจะใช้สัญลักษณ์ “.” ในการแยก ในรายละเอียดของแต่ละส่วนมีดังนี้

(1) ส่วนที่ 1 จะเป็นส่วนของการแสดงประเภทเอกสาร ID ของเอกสาร และ ID ผู้ที่ทำการออกเอกสาร

(2) ส่วนที่ 2 จะเป็นส่วนของ credentialSubject โดยจะมีรายละเอียดข้อมูลที่ทาง Wallet Holder ร้องขอ

(3) ส่วนที่ 3 จะเป็นส่วนของ proof คือลายมือชื่อดิจิทัลของผู้ที่ทำการออก VC รวมไปถึง ID ของกุญแจสาธารณะ ที่ใช้ในการตรวจสอบลายมือชื่อ



รูปที่ 6 กรณีศึกษา VC การขอใบประมวลผลการศึกษา (Transcript)

ขั้นตอนการออกใบประมวลผลการศึกษามีกระบวนการ (User Journey) ดังนี้

(1) นักศึกษาหรือผู้ที่ต้องการหลักฐานการศึกษาส่งคำร้อง (request) ให้กับทางมหาวิทยาลัย ผ่านช่องทางที่เป็น web application และมีการยืนยันตัวตน (user authentication)

(2) เมื่อนักศึกษาร้องขอเอกสารใบประมวลผลการศึกษา (Transcript) ไปยังมหาวิทยาลัย จากนั้นมหาวิทยาลัยจะดำเนินการสร้างคิวอาร์โคด (QR code) สำหรับรายละเอียดการเชื่อมต่อกับ wallet รับเอกสาร นักศึกษาสแกนคิวอาร์โคด (QR code) เพื่อขอรับเอกสารและมหาวิทยาลัยจัดเตรียมข้อมูลสำหรับใบประมวลผลการศึกษา (Transcript) ในรูปแบบเอกสารรับรองดิจิทัล (VC) และทำการลงลายมือชื่ออิเล็กทรอนิกส์

(3) เมื่อนักศึกษาได้รับใบประมวลผลการศึกษา (Transcript) ในรูปแบบเอกสารรับรองดิจิทัล (VC) แล้วจึงนำเอกสารที่ได้รับไปจัดเก็บในกระเป๋าเอกสารดิจิทัลของนักศึกษา (digital document wallet)

(4) เมื่อนักศึกษาต้องการไปสมัครงานกับบริษัทสมมติเป็นผู้ตรวจสอบเอกสาร ทางบริษัทจะส่งคำร้องขอ VC ที่ออกโดยมหาวิทยาลัยมายังกระเป๋าเอกสารดิจิทัลของนักศึกษา และกระเป๋าเอกสารดิจิทัลจะถามนักศึกษาว่าต้องการใช้ VC ที่มีอยู่หรือไม่ เมื่อนักศึกษาตอบตกลง VC จะถูกนำมาใช้สร้างเป็นเอกสารสำแดงดิจิทัล (VP) และส่งต่อไปให้บริษัทดำเนินการตรวจสอบ

ตัวอย่างที่ 1 โครงสร้าง VC ที่ใช้ในโครงการ แสดงรูปแบบ JSON-LD

```
{
  //@context ประกาศนิยามของสมนาม (alias)
  "@context": [
    "https://www.w3.org/ns/credentials/v2",
    "https://www.w3.org/ns/credentials/examples/v2"
  ],
  "id": "did:tbsi:zv8fVB1i6S7MLMZX8wd3Ayo", //id ของเอกสาร
  //ประเภทของเอกสาร
  "type": [
    "VerifiableCredential",
    "TranscriptCredential"
  ],
  //ผู้ออกเอกสาร
  "issuer": {
    "id": "did:demo:zv8fVB1i6S7MLMZX8wd3Ayo", //id ของเอกสาร
    "name": "University A" //ชื่อผู้ออกเอกสาร
  },
  "issuanceDate": "20/08/2024 3:09:51 PM", //วันและเวลาที่สร้าง VC
  "expireDate": "20/08/2024 3:14:51 PM", //วันและเวลาที่ VC หมดอายุ
  //เจ้าของข้อความใน VC
  "credentialSubject": {
    "id": "did:key:Nj+3XqFr2jwFsZiQ5YS+YgdnwXnRfW9rxSJxlvUO7H8=", //id เจ้าของข้อความ
    "student": "Nattapong Methawon", //ชื่อเจ้าของข้อความ
    "gpa": "3.71" //ข้อมูล GPA
  },
  //ลายมือชื่อดิจิทัล ซึ่งช่วยให้สามารถตรวจพบการเปลี่ยนแปลงของ VC
  "proof": {
    "type": "EdDSA", //กระบวนการเข้ารหัสลับที่ใช้ในการลงลายมือชื่อ
    "created": "8/20/2024 3:09:51 PM", // วันที่ลงลายมือชื่อ
    "proofPurpose": "assertionMethod", // วัตถุประสงค์ของการลงลายมือชื่อ
  //id ของกุญแจสาธารณะที่ใช้ในการตรวจสอบลายมือชื่อ
    "verificationMethod":
"did:demo:zv8fVB1i6S7MLMZX8wd3Ayo#1XmYo2EnZwAL0giRxBWMADGk2Zei+TD2VKx7aWgWWAo=",
    //ค่าของลายมือชื่อดิจิทัล
    "jws": "4BV4NWu5hRuWL52mBIUunAozKIiQzKuhYFaWj3oNDVwer78ZrHZD98uOUrv86B0_rZ4Sgh-4tJ95nA1c26yADg"
  }
}
```

5.2 เอกสารสำแดงดิจิทัล (verifiable presentation: VP)

เอกสารสำแดงข้อมูลที่ประกอบด้วย VC อย่างน้อยหนึ่งชุด ตามรูปที่ 4 ซึ่งอาจเป็นข้อมูลต้นฉบับตามที่ปรากฏใน VC หรือเป็นข้อมูลที่สังเคราะห์จาก VC ก็ได้ โดย VP จะมีคุณสมบัติที่สามารถตรวจพบการเปลี่ยนแปลงใด ๆ ที่เกิดกับความถูกต้องครบถ้วนของข้อมูล และตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ของผู้ถือเอกสารและตรวจสอบ VC ที่เกี่ยวข้องได้ด้วยกระบวนการเข้ารหัสลับ

การสังเคราะห์ข้อมูลจาก VC เพื่อสร้างเป็น VP สามารถใช้วิธีการที่รองรับการเลือกเปิดเผยข้อมูลบางส่วน (selective disclosure) กล่าวคือ ผู้ถือเอกสารสามารถแสดงการพิสูจน์ให้ทราบข้อเท็จจริงเกี่ยวกับข้อความยืนยันได้ โดยไม่ต้องแสดงข้อความยืนยันทั้งหมดที่อยู่ใน VC ก็ได้ เช่น เลือกแสดงเฉพาะชื่อและนามสกุลจากข้อมูลทั้งหมดตามหน้าบัตรประชาชน ทั้งนี้ VP อาจอยู่ในรูปแบบที่แสดงเฉพาะค่าความจริง (Boolean) ของข้อความยืนยัน โดยไม่ต้องแสดงค่าที่แท้จริงของข้อความยืนยันก็ได้ เช่น ค่าความจริงที่ยืนยันว่าเจ้าของข้อความมีอายุมากกว่า 20 ปีบริบูรณ์ โดยไม่ต้องเปิดเผยอายุที่แท้จริงของเจ้าของข้อความ

โครงสร้างของเอกสารสำแดงดิจิทัลในรายงานทางเทคนิคฉบับนี้ ได้อ้างอิงโครงสร้างตาม World Wide Web Consortium (W3C) [4] สามารถแสดงตามรูปที่ 7 ซึ่งประกอบด้วย 3 ส่วน ได้แก่ (1) คำอธิบายข้อมูลของ VP (presentation metadata) (2) เอกสารรับรองดิจิทัล (VC) และ (3) ข้อพิสูจน์ (proof) ซึ่งโดยทั่วไปจะเป็นลายมือชื่อดิจิทัลของผู้ถือเอกสาร

สำหรับในรายงานฉบับนี้การตรวจสอบเอกสารสำแดงดิจิทัล มีขั้นตอนการตรวจสอบดังนี้

(1) ตรวจสอบความถูกต้องของเอกสารสำแดงดิจิทัล โดยการตรวจสอบความถูกต้อง ที่ข้อมูลอยู่ในรูปแบบ JWT ที่มีการลงลายมือชื่อมาอย่างน่าเชื่อถือ

(2) ตรวจสอบความสอดคล้องของเอกสารสำแดงดิจิทัล โดยการตรวจสอบว่าลายมือชื่ออิเล็กทรอนิกส์ที่ถูกลงชื่อมานั้น มาจาก Private Key ของผู้ถือเอกสารหรือไม่ โดยใช้ Key จากเอกสารสำแดงดิจิทัล ในส่วน ข้อพิสูจน์ (proof) ในหัวข้อ verficationMethod ซึ่งจะมีข้อมูล DID ของผู้ถือเอกสารอยู่ เนื่องจาก DID ของผู้ถือเอกสารเป็น Method key ซึ่งระบุ Public key มาด้วย จึงสามารถใช้ Public key ของผู้ถือเอกสารมาตรวจสอบกับลายมือชื่ออิเล็กทรอนิกส์ที่ถูกลงชื่อ มาได้ว่าเป็นการลงชื่อ จากผู้ถือเอกสารจริงหรือไม่

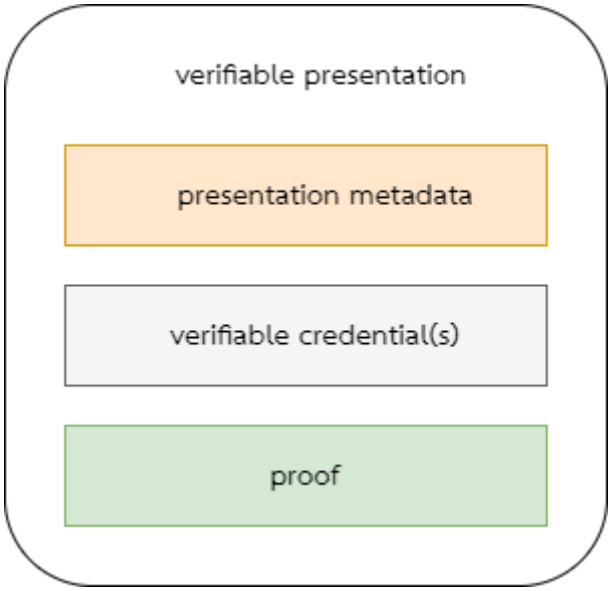
(3) ตรวจสอบผู้ออกเอกสาร (Issuer) เป็น Legal Entity หรือไม่ โดยการร้องขอ DID Document จาก Registry ผ่าน DIF Universal Resolver

(4) ตรวจสอบว่าข้อมูลภายในเอกสารรับรองดิจิทัล มีความสอดคล้องกับ Holder หรือไม่ โดยการตรวจสอบ DID ของ Holder ในเอกสารสำแดงดิจิทัล และ id ของ Holder ที่ Issuer ออกให้ โดยจะถูกระบุอยู่ที่ส่วน credentialSubject ในหัวข้อ id ซึ่ง DID ของทั้งสองส่วนนี้ต้องตรงกัน

(5) ตรวจสอบความถูกต้องของเอกสารรับรองดิจิทัล ว่าได้ออกมาอย่างถูกต้องผ่าน Issuer นั้นจริง โดยการตรวจสอบเอกสารรับรองดิจิทัล ที่มีการพิสูจน์ (Proof) โดย Signature ว่าเอกสารรับรองดิจิทัลฉบับนี้ถูกลงนาม (Sign) มาอย่างถูกต้อง

(6) ตรวจสอบความสอดคล้องของเอกสารรับรองดิจิทัล โดยการตรวจสอบว่า Signature ที่ถูกลงนาม (Sign) มานั้น มาจาก Private Key ของผู้ออกเอกสารรับรอง (Issuer) จริงหรือไม่ โดยใช้ Key ที่ได้จาก DID Document มาทำการตรวจสอบกับ Signature ที่ถูกลงนาม (Sign) มาได้ว่าเป็นการลงนาม (Sign) จาก Issuer นั้นจริงหรือไม่

เมื่อทำการตรวจสอบทั้ง 6 ขั้นตอนแล้วถูกต้องทั้งหมด จึงจะยอมรับว่า VP ที่ได้รับมา ถูกสร้างออกมาอย่างถูกต้อง จึงจะนำไปใช้งานหรือดำเนินการอื่นต่อไปได้



รูปที่ 7 โครงสร้างเอกสารสำแดงดิจิทัล VP

จากกรณีศึกษาในตัวอย่างที่ 1 เมื่อนักศึกษาได้รับ VC มาจัดเก็บไว้ในกระเป๋าเอกสารดิจิทัลของตนเองแล้วต่อมาจะนำเอกสารไปทำการสมัครงานจากบริษัทสมมติซึ่งเป็นผู้ตรวจสอบเอกสาร บริษัทที่รับสมัครจะส่งคำร้องขอ VC ที่ออกโดยมหาวิทยาลัยผ่านไปยังกระเป๋าเอกสารดิจิทัลของนักศึกษา และกระเป๋าเอกสารดิจิทัลจะถามนักศึกษาว่าต้องการใช้ VC ที่มีอยู่หรือไม่ เมื่อนักศึกษาตอบตกลง VC จะถูกนำมาใช้สร้างเป็น VP แล้วส่งต่อไปให้บริษัททำการตรวจสอบ ตัวอย่างของ VP ข้างต้นในรูปแบบ JSON-LD เป็นดังนี้

ตัวอย่างที่ 2 โครงสร้าง VP ที่ใช้ในโครงการ แสดงรูปแบบ JSON-LD

```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/suites/jws-2020/v1"
  ],
  "type": [
    "VerifiablePresentation",
    "TranscriptCredential"
  ],
  //ข้อมูล VC จากตัวอย่างที่ 1
  "verifiableCredential": {
    "@context": [
      "https://www.w3.org/ns/credentials/v2",
      "https://www.w3.org/ns/credentials/examples/v2"
    ],
    "id": "did:demo:zv8fVB1i6S7MLMZX8wd3Ayo",
    "type": [
      "VerifiableCredential",
      "TranscriptCredential"
    ],
    "issuer": {
      "id": "did:demo:zv8fVB1i6S7MLMZX8wd3Ayo",
      "name": "University A"
    },
    "issuanceDate": "14/08/2024 10:29:37 AM",
    "expireDate": "14/08/2024 10:34:37 AM",
    "credentialSubject": {
      "id": "did:key:Nj+3XqFr2jwFsZiQ5YS+YgdnwXnRfW9rxSJxlvUO7H8=",
      "student": "Nattapong Methawon",
      "gpa": "3.71"
    },
    "proof": {
      "type": "EdDSA",
      "created": "8/14/2024 10:29:37 AM",
      "proofPurpose": "assertionMethod",
      "verificationMethod":
"did:tbsi:zv8fVB1i6S7MLMZX8wd3Ayo#1XmYo2EnZwAL0giRxBWMADGk2Zei+TD2VKx7aWgWWAo=",
      "jws": "4TOgXBp-WoyhB3rqmccyT96iuJaeyDiTKwSP6rxqqx5402rdbBwd3OMmpT9TPDSZTTPBUPdpULaPd0nOMB7uBQ"
    }
  },
  //Digital Signature ของ Hollder
  "proof": {
    "type": "EdDSA",
    "created": "8/21/2024 5:26:44 AM",
    "proofPurpose": "assertionMethod",
    "verificationMethod": "did:key:Nj+3XqFr2jwFsZiQ5YS+YgdnwXnRfW9rxSJxlvUO7H8=",
    "jws": "JatBA5HBioSBsXQPpq1ueN22IU-wghszE9il8QFLrjdkU4MpLFJKioLP8oMXwMBt6t4kdn29Bj2qMxJWXmusAg"
  }
}
```

จากตัวอย่างที่ 1 และ 2 โครงสร้างข้อมูลของ VC และ VP ประกอบด้วยคุณสมบัติต่าง ๆ (property) ซึ่งจะแบ่งออกเป็นคุณสมบัติพื้นฐาน ดังนี้

(1) **@context** เป็นคุณสมบัติที่ใช้เชื่อมโยงชื่อคุณสมบัติต่าง ๆ ใน VC หรือ VP เข้ากับ URI เพื่อให้ระบบคอมพิวเตอร์สามารถแลกเปลี่ยนข้อมูลและเข้าใจความหมายของคุณสมบัติต่าง ๆ ด้วยสมนาม (alias) ซึ่งกะทัดรัดและบุคคลอ่านเข้าใจได้

(2) **id** เป็นคุณสมบัติที่ใช้แสดง identifier สำหรับอ้างอิงวัตถุที่เฉพาะเจาะจงใน VC เช่น บุคคล ผลิตภัณฑ์ หรือองค์กร เพื่อให้สามารถกล่าวถึงวัตถุเดียวกันได้อย่างชัดเจน

(3) **type** เป็นคุณสมบัติที่ใช้แสดงประเภทของชุดข้อมูล (object) เพื่อพิจารณาว่าข้อมูลมี ความเหมาะสมหรือไม่

(4) **issuer** เป็นคุณสมบัติที่ใช้แสดงถึงผู้ออกเอกสารรับรอง (VC)

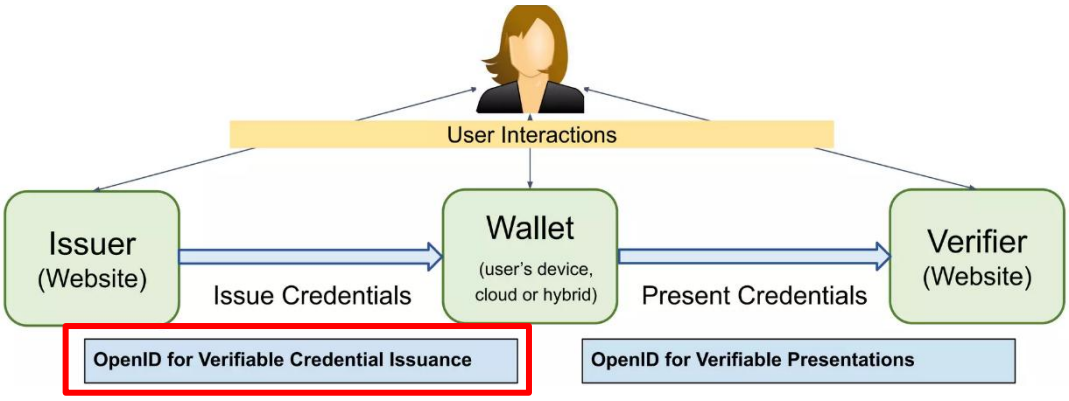
(5) **issuanceDate และ expirationDate** คุณสมบัติที่ใช้แสดงวันและเวลาเมื่อ VC เริ่มมีผลผูกพัน (issuance date) และสิ้นผลผูกพัน (expiration date) ตามลำดับ

(6) **credentialSubject** เป็นคุณสมบัติที่ใช้แสดงข้อความยืนยัน (claim) เกี่ยวกับเจ้าของข้อความ (subject) อย่างน้อยหนึ่งเอนทิต

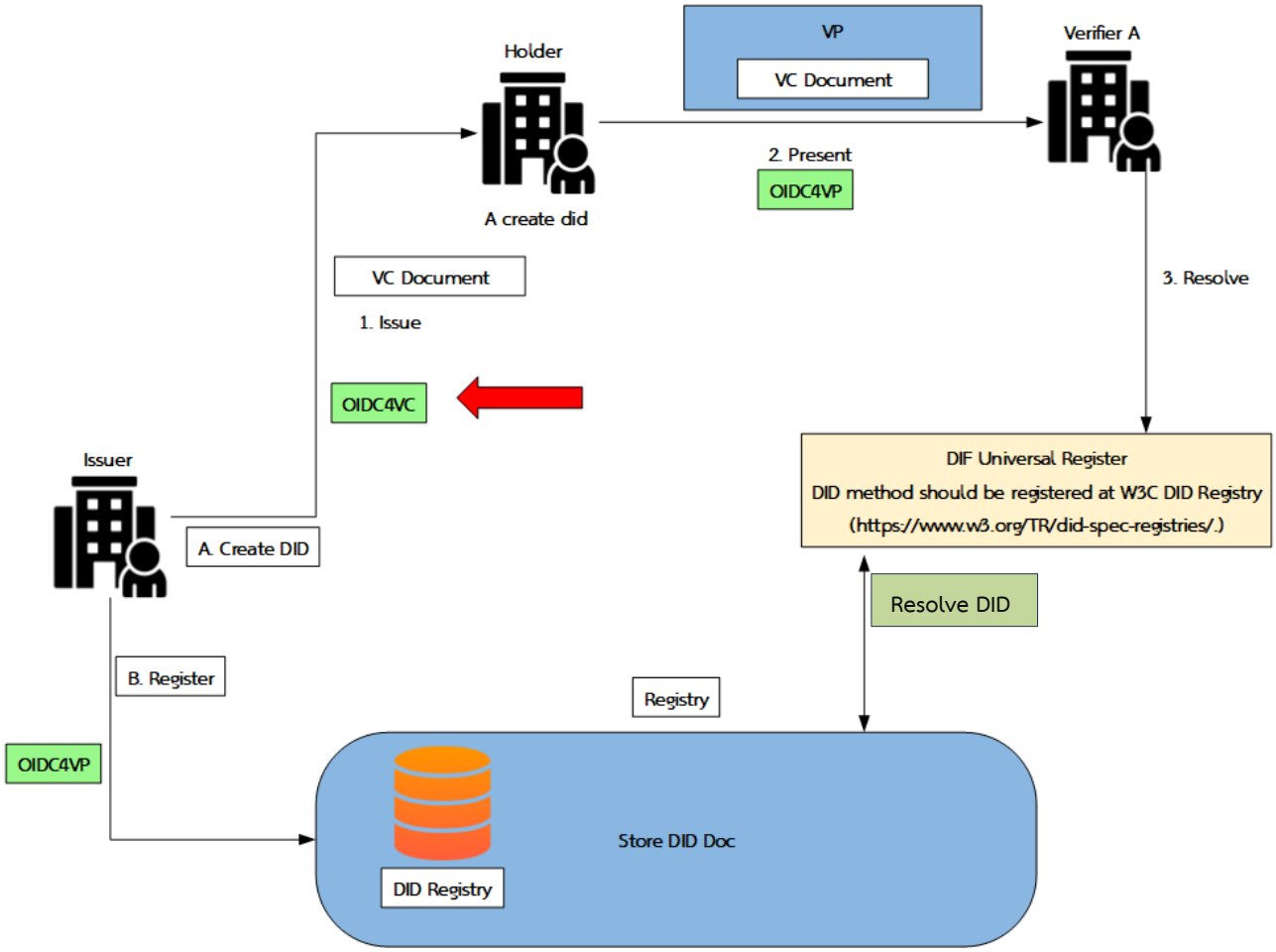
(7) **proof** เป็นคุณสมบัติที่ใช้แสดงข้อพิสูจน์ (proof) โดยข้อพิสูจน์คือวิธีการที่ทำให้ VC หรือ VP สามารถถูกตรวจพบการเปลี่ยนแปลงใด ๆ ที่เกิดกับความถูกต้องครบถ้วนของข้อมูล และตรวจสอบ ลายมือชื่ออิเล็กทรอนิกส์ของผู้ออกเอกสารและผู้ถือเอกสาร

5.3 Protocol สำหรับการออก VC

โพรโทคอล OpenID Connect for Verifiable Credentials Protocol (OID4VC) Draft Version 13 เป็นโพรโทคอลที่อยู่ในกลุ่ม OpenID ใช้สำหรับการออกเอกสารรับรองดิจิทัลผ่านทาง API โดยรองรับมาตรฐานเอกสารรับรองหลากหลายรูปแบบ รวมถึง W3C Verifiable Credentials เพื่อจัดการข้อมูลตัวตนดิจิทัลและการยืนยันตัวตนอย่างมั่นใจสำหรับ web application และ mobile application



รูปที่ 8 การใช้งาน OID4VC



รูปที่ 9 ขั้นตอนการทำ OID4VCI

5.3.1 กระบวนการทำงาน OID4VCI

การออกเอกสารรับรองดิจิทัล (VC) ของใบประมวลผลการศึกษา จะใช้โพรโทคอล OID4VCI draft Version 13 Pre-Authorized Code Flow มีขั้นตอนการทำงานดังนี้

(1) การให้ความยินยอมและการรวบรวมข้อมูล

(2) การสร้าง Credential Offer

(3) การดึงข้อมูล Metadata ผู้ออกเอกสาร

(4) การร้องขอ Token

(5) การร้องขอและการออก Credential Request

(1) การให้ความยินยอมและการรวบรวมข้อมูล

ผู้ออกเอกสาร (Credential Issuer) ต้องได้รับการยินยอมจากผู้ถือเอกสารและรวบรวมข้อมูลที่จำเป็นของผู้ถือเอกสารสำหรับการออกเอกสารรับรองดิจิทัลผ่านกระบวนการเฉพาะเช่น การยืนยันตัวตน (Authentication) และการอนุญาต (Authorization) ของผู้ถือเอกสาร โดยกระบวนการนี้ไม่อยู่ในของเขตของ OID4VCI

(2) การสร้าง Credential Offer

ผู้ออกเอกสารสร้าง Credential Offer สำหรับเอกสารรับรองที่จะทำการออกและส่งไปยังกระเป๋าเอกสารดิจิทัลโดยมีวิธีส่งได้หลายวิธีแต่ในการศึกษาครั้งนี้ผู้ออกเอกสารจะสร้าง QR Code ให้กระเป๋าเอกสารแสกนหรือคัดลอก URI ส่งให้ผ่านช่องทางอื่น Credential Offer ประกอบด้วย URL ของ ผู้ออกเอกสาร, ข้อมูลเกี่ยวกับเอกสารรับรอง, Pre-Authorized Code

ตัวอย่าง credential offer

```
{
   "credential_issuer":"https://credential-issuer.example.com",
   "credential_configuration_ids":["VerifiableCredential","TranscriptCredential"],
   "grants":{
      "urn:ietf:params:oauth:grant-type:pre-authorized_code":
      {
         "pre-authorized_code":"sX2CpoKx",
         "tx_code":{
            "length": 4,
            "input_mode": "numeric",
            "description": "Please provide the one-time code that was sent via e-mail"
          }
      }
   }
}
```

คำอธิบายพารามิเตอร์ (Pre-Authorized Code)

พารามิเตอร์	Required	Type	รายละเอียด
credential_issuer	Required	URL	URL ของผู้ออกเอกสารที่คำนึงถึงตัวพิมพ์เล็ก-ใหญ่ ใช้โปรโตคอล https และต้องประกอบด้วย scheme และ host รวมถึง port number และ path components ได้ตามต้องการ แต่ ต้องไม่มี ส่วนประกอบ query หรือ fragment
credential_configuration_ids	Required	Array	อาร์เรย์ของข้อความที่ไม่ซ้ำกัน โดยแต่ละข้อความคือชนิดของเอกสารรับรองที่ของผู้ออกเอกสารสามารถออกให้ได้สำหรับ Credential Offer ครั้งนี้
grants	Optional	Grant Type	ระบุ Grant Types ที่ Authorization Server ของผู้ออกเอกสารใช้สำหรับ Credential Offer ครั้งนี้ โดยในการศึกษาใช้เป็น urn:ietf:params:oauth:grant-type:pre-authorized_code

พารามิเตอร์	Required	Type	รายละเอียด
pre-authorized_code	Required	String	รหัสที่แสดงถึงการอนุญาตของผู้ออกเอกสารให้ผู้ถือเอกสารใช้ขอรับเอกสารรับรองประเภทใดประเภทหนึ่ง รหัสนี้ต้องมีอายุสั้นและใช้ได้เพียงครั้งเดียว หากเลือกใช้ Pre-Authorized Code Flow ต้องมีพารามิเตอร์นี้
tx_code	Optional	Object	ใช้ระบุว่า Authorization Server ต้องการ Transaction Code จากผู้ถือเอกสารพร้อมกับ Token Request ใน Pre-Authorized Code Flow หรือไม่ หาก Authorization Server ไม่ต้องการ Transaction Code วัตถุนี้จะไม่พารามิเตอร์นี้จะไม่ถูกใส่เข้ามา Transaction Code มีวัตถุประสงค์เพื่อเชื่อมโยง Pre-Authorized Code กับธุรกรรมที่เฉพาะเจาะจง เพื่อป้องกันการใช้รหัสซ้ำโดยผู้โจมตี เช่น การสแกน QR code โดยไม่ได้รับอนุญาต แนะนำให้ส่ง Transaction Code โดยผ่านช่องทางอื่น
Input_mode	Optional	String	กำหนดชุดตัวอักษรที่สามารถป้อนข้อมูลได้ ค่าเลือกที่เป็นไปได้คือเฉพาะตัวเลขหรือเฉพาะตัวอักษร ค่าเริ่มต้นคือตัวเลข
length	Optional	Integer	กำหนดความยาวของ Transaction Code ช่วยให้กระเป๋าเอกสารแสดงหน้าจอสำหรับป้อนข้อมูลได้ดีขึ้นและช่วยเพิ่มประสบการณ์การใช้งานของผู้ใช้
description	Optional	String	คำแนะนำแก่ผู้ถือกระเป๋าเอกสาร เกี่ยวกับวิธีการรับรหัสธุรกรรม เช่น การบอกว่ารหัสจะถูกส่งผ่านช่องทางการสื่อสารใด แนะนให้แสดงคำอธิบายนี้ถัดจากหน้าจอป้อน Transaction Code เพื่อปรับปรุงประสบการณ์การใช้งาน ข้อความนี้ต้องไม่เกิน 300 ตัวอักษรและไม่รองรับการแปลหลายภาษา

(3) การดึงข้อมูล Metadata ผู้ออกเอกสาร

เพื่อดึง Metadata กระเป๋าเอกสารจะต้องส่ง HTTP GET ไปที่ URL ของผู้ออกเอกสารต่อด้วย/.well-known/openid-credential-issuer เช่น https://credential-issuer.example.com/.well-known/openid-credential-issuer หาก URL ของผู้ออกเอกสารมี path component (/) ที่อยู่ท้ายสุดจะต้องถูกลบออกก่อนที่จะเพิ่ม /.well-known/openid-credential-issuer

Metadata จะเป็น JSON ประกอบด้วย ประเภทและรูปแบบของเอกสารรับรองทั้งหมดที่ผู้ออกเอกสารสามารถออกได้, Token Endpoint, Credential Endpoint และอื่น ๆ

ตัวอย่าง Metadata

```
{
   "credential_issuer": "https://credential-issuer.example.com",
   "authorization_servers": [ "https://server.example.com" ],
   "credential_endpoint": "https://credential-issuer.example.com",
   "batch_credential_endpoint": "https://credential-issuer.example.com/batch_credential",
   "deferred_credential_endpoint": "https://credential-issuer.example.com/deferred_credential",
   "credential_response_encryption": {
      "alg_values_supported" : [
         "ECDH-ES"
      ],
      "enc_values_supported" : [
         "A128GCM"
      ],
      "encryption_required": false
   },
```

```
  "display": [
    {
      "name": "Example University",
      "locale": "en-US"
    },
    {
      "name": "Example Université",
      "locale": "fr-FR"
    }
  ],
  "credential_configurations_supported": {
    "UniversityDegreeCredential": {
      "format": "jwt_vc_json",
      "scope": "UniversityDegree",
      "cryptographic_binding_methods_supported": [
        "did:example"
      ],
      "credential_signing_alg_values_supported": [
        "ES256"
      ],
      "credential_definition":{
        "type": [
          "VerifiableCredential",
          "UniversityDegreeCredential"
        ],
        "credentialSubject": {
          "given_name": {
            "display": [
              {
                "name": "Given Name",
                "locale": "en-US"
              }
            ]
          },
          "family_name": {
            "display": [
              {
                "name": "Surname",
                "locale": "en-US"
              }
            ]
          },
          "degree": {},
          "gpa": {
            "display": [
              {
                "name": "GPA"
              }
            ]
          }
        }
      },
      "proof_types_supported": {
        "jwt": {
          "proof_signing_alg_values_supported": [
            "ES256"
          ]
        }
      },
      "display": [
        {
```

```
                "name": "University Credential",
                "locale": "en-US",
                "logo": {
                    "url": "https://university.example.edu/public/logo.png",
                    "alt_text": "a square logo of a university"
                },
                "background_color": "#12107c",
                "text_color": "#FFFFFF"
            }
        ]
    }
  }
}
```

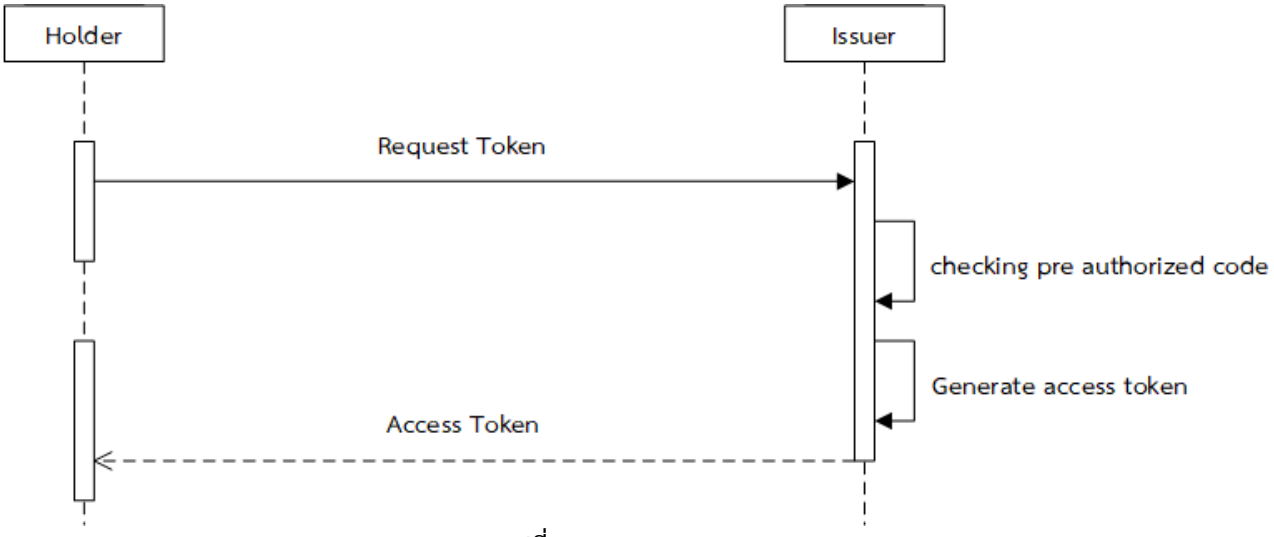

คำอธิบายค่าพารามิเตอร์

พารามิเตอร์	Required	Type	รายละเอียด
credential_issuer	Required	URL	URL ของผู้ออกเอกสารที่คำนึงถึงตัวพิมพ์เล็ก-ใหญ่ ใช้โปรโตคอล https และต้องประกอบด้วย scheme และ host รวมถึง port number และ path components ได้ตามต้องการ แต่ต้องไม่มีส่วนประกอบ query หรือ fragment
authorization_servers	Optional	Array of strings	อาร์เรย์ของสตริง ซึ่งแต่ละสตริงเป็นตัวระบุของ OAuth 2.0 Authorization Server ที่ผู้ออกเอกสารอ้างอิงเพื่อใช้ในการอนุมัติ หากไม่มีการระบุพารามิเตอร์นี้ผู้ออกเอกสารจะทำหน้าที่เป็น Authorization Server ด้วย โดยใช้ตัวระบุของผู้ออกเอกสารเพื่อดึงข้อมูล Metadata ของ Authorization Server
credential_endpoint	Required	URL	URL ของ Credential Endpoint ของผู้ออกเอกสาร URL นี้ต้องใช้โปรโตคอล HTTPS
batch_credential_endpoint	Optional	URL	URL ของ Batch Credential Endpoint ของผู้ออกเอกสารหากไม่มีการระบุพารามิเตอร์นี้ แสดงว่าผู้ออกเอกสารไม่รองรับ Batch Credential Endpoint
deferred_credential_endpoint	Optional	URL	URL ของ Deferred Credential Endpoint ของ ผู้ออกเอกสาร URL นี้ต้องใช้โปรโตคอล HTTPS หากไม่มีการระบุพารามิเตอร์นี้ แสดงว่าผู้ออกเอกสารไม่รองรับ Deferred Credential Endpoint
notification_endpoint	Optional	URL	URL ของ Notification Endpoint ผู้ออกเอกสารต้องใช้โปรโตคอล HTTPS หากไม่มีการระบุพารามิเตอร์นี้ แสดงว่า ผู้ออกเอกสารไม่รองรับ Notification Endpoint
credential_response_encryption	Optional	Object	แสดงข้อมูลว่าผู้ออกเอกสารรองรับการเข้ารหัส Credential และ Batch Credential Response เพิ่มเติมจาก TLS หรือไม่
alg_values_supported	Required*	Array	เป็นอาร์เรย์ที่ประกอบด้วยรายการของอัลกอริทึมการเข้ารหัส JWE ([RFC7516]) ที่ได้รับการสนับสนุนโดย Credential Endpoint และ Batch Credential Endpoint เพื่อเข้ารหัสข้อมูล Credential หรือ Batch Credential Response ในรูปแบบ JWT ([RFC7519]) ตามที่กำหนดไว้ใน [RFC7518]

พารามิเตอร์	Required	Type	รายละเอียด
enc_values_supported	Required*	Array	เป็นอาร์เรย์ที่ประกอบด้วยรายการของอัลกอริทึมการเข้ารหัส JWE ([RFC7516]) (ค่า enc) ที่ได้รับการสนับสนุนโดย Credential Endpoint และ Batch Credential Endpoint เพื่อเข้ารหัสข้อมูล Credential หรือ Batch Credential Response ในรูปแบบ JWT ([RFC7519]) ตามที่กำหนดไว้ใน [RFC7518]
encryption_required	Required*	Boolean	เป็นค่าบูลีนที่ระบุว่าผู้ออกเอกสาร ต้องการการเข้ารหัสเพิ่มเติมนอกเหนือจาก TLS สำหรับ Credential Response หรือไม่ หากค่าเป็น true แสดงว่าผู้ออกเอกสารต้องการการเข้ารหัสสำหรับ Credential Response ทุกครั้ง และกระเป๋าเอกสารจะต้องให้คีย์การเข้ารหัสในคำขอ Credential Request หากค่าเป็น false กระเป๋าเอกสารอาจเลือกได้ว่าจะให้คีย์การเข้ารหัสหรือไม่
credential_identifiers_supported	Optional	Boolean	ค่า Boolean ที่ระบุว่าผู้ออกเอกสารรองรับการส่งคืนพารามิเตอร์ credential_identifiers ในพารามิเตอร์ authorization_details ของ Token Response หรือไม่ หากค่าเป็น true แสดงว่ารองรับ หากไม่มีการระบุคือ false
signed_metadata	Optional	String	สตริงที่เป็น JWT ที่ลงนามแล้วซึ่งมี Metadata ของผู้ออกเอกสารในรูปของ claims เมทาดาทาที่ลงนามนี้ต้องใช้ JSON Web Signature (JWS)
display	Optional	Array of objects	อาร์เรย์ทีมีคุณสมบัติการแสดงผลของผู้ออกเอกสารในแต่ละภาษา
credential_configurations_supported	Required	Object	วัตถุที่อธิบายรายละเอียดของเอกสารรับรองที่ผู้ออกเอกสารรองรับ โดยมีพารามิเตอร์

*ต้องใส่เมื่อมี credential_response_encryption

(4) การร้องขอ Token



รูปที่ 10 Token Exchange

- กระเป๋าเอกสารส่ง Pre-Authorized Code ที่ได้รับในขั้นตอนที่ 3 ไปยัง Token Endpoint หากผู้ออกเอกสารกำหนดให้ต้องใช้ Transaction Code กระเป๋าเอกสารจะส่งไปด้วย
- ผู้ออกเอกสารรับคำร้องขอโทเคนและทำการตรวจสอบสิทธิ์การเข้าถึงข้อมูล หากถูกต้องผู้ออกเอกสารจะดำเนินการสร้าง Access Token และส่ง Token กลับไปให้กระเป๋าเอกสาร

ตัวอย่างการส่ง Token Request ของกระเป๋าเอกสาร (Pre-Authorized Code)

```
POST /token HTTP/1.1
Host: server.example.com
Content-Type: application/x-www-form-urlencoded
grant_type=urn:ietf:params:oauth:grant-type:pre-authorized_code
&pre-authorized_code=SplxlOBeZQQYbYS6WxSbIA
&tx_code=493536
```

คำอธิบายค่าพารามิเตอร์ (Pre-Authorized Code)

พารามิเตอร์	Required	type	รายละเอียด
grant_type	Required	String	ระบุ Grant Types ที่ Authorization Server ของผู้ออกเอกสารใช้สำหรับ Credential Offer ครั้งนี้ โดยในการศึกษาใช้เป็น urn:ietf:params:oauth:grant-type:pre-authorized_code
pre-authorized_code	Required	String	รหัสที่ได้จากผู้ออกเอกสารที่แสดงถึงการอนุญาตเพื่อขอรับเอกสารรับรองประเภทใดประเภทหนึ่ง
tx_code	Optional	String	Transaction Code ที่ได้จากผู้ออกเอกสาร

Issuer ดำเนินการสร้าง Access Token ตามรูปที่ 14 และส่ง Token กลับไปให้ Holder ระบุ parameter ดังนี้

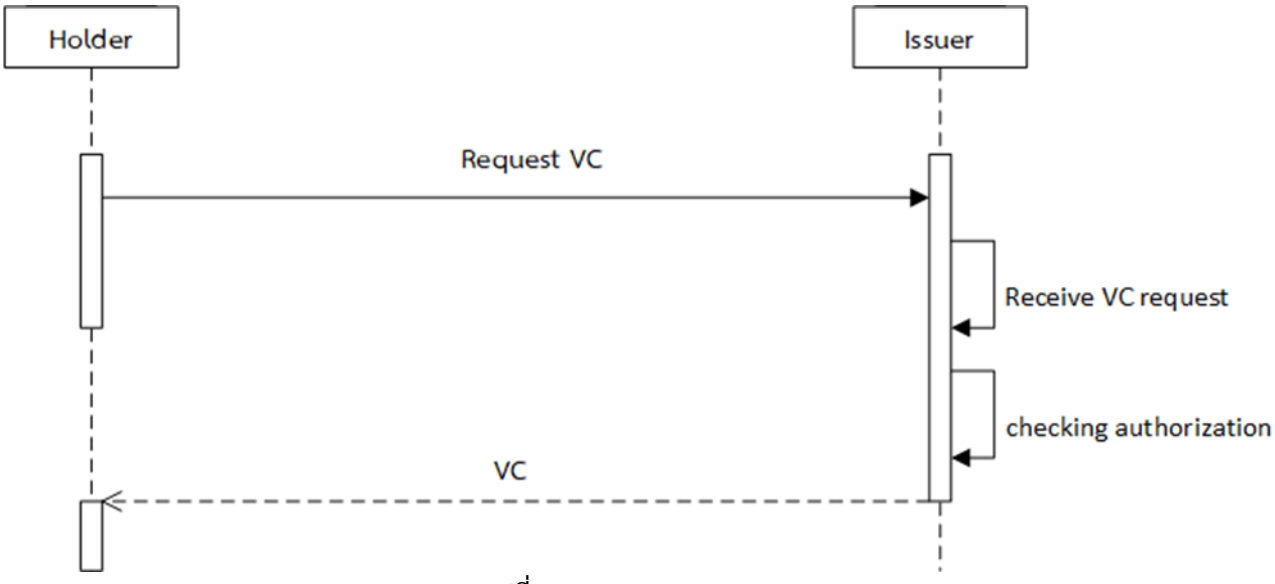
ตัวอย่างการส่ง HTTP Response ของผู้ออกเอกสาร (Pre-Authorized Code)

```
HTTP/1.1 200 OK
Content-Type: application/json
 {
   "access_token": "eyJhbGciOiJSUzI1NiIsInR5cCI6Ikp..sHQ",
   "token_type": "bearer",
   "expires_in": 86400,
   "c_nonce": "tZignsnFbp",
   "c_nonce_expires_in": 86400
   }
```

คำอธิบายค่าพารามิเตอร์

พารามิเตอร์	**Required**	**Type**	**รายละเอียด**
access_token	Required	String	เป็น token ที่ใช้ในการเข้าถึงบริการหรือข้อมูลจากผู้ให้บริการต่างๆ ที่เชื่อถือ access_token นั้น ออกให้โดย Authorization Server
token_type	Required	String	ชนิดของ Token
expires_in	Required	Number	อายุการใช้งานของ access_token มีระยะเวลาเป็นวินาทีนับจากเวลาของการเริ่มสร้าง access_token
c_nonce	Optional	String	ค่าประเภทสตริงที่มี nonce ใช้ในการสร้าง proof of possession สำหรับ key proof
c_nonce_expires_in	Optional	Number	จำนวนที่ระบุอายุของ c_nonce เป็นวินาที

(5) การร้องขอและการออกเอกสารรับรอง



รูปที่ 11 Credential Request

- กระเป๋าเอกสารส่ง Credential Request ไปยัง Credential Endpoint ของผู้ออกเอกสารโดยแนบ Access Token และ Proof of Possession (ถ้ามี) ของคู่คีย์ที่ผู้ออกเอกสารจะผูกไว้กับเอกสารรับรองที่จะออก
- ผู้ออกเอกสารตรวจสอบ Access Token และ Proof of Possession (ถ้ามี)
- เมื่อผ่านการตรวจสอบผู้ออกเอกสารจะส่งเอกสารรับรองกลับไปยังกระเป๋าเอกสารใน Credential Response

ตัวอย่างการส่ง HTTP Request

```
METHOD: HttpMethod(value=POST)
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJFZERTQSJ9.eyJzdWIiOiJhN2MwODczZS02Y2IxLTRjYmMtYWM2OS1hYTM3YWZlNzgwNTQiLCJpc3MiOiJodHRwczovL2lzc3Vlci1hcGktdGVzdC5ldGRhLm9yLnRoIiwiYXVkIjoiQUNDRVNTIn0.dH8bufDYHuMagSi3IpnUUcscYcZDtYgygFaDX5xY-LBSVM4eUpUj-a50rd9tFo4mMMHMo1OiPvFHguMV1KiSBw
BODY Content-Type: application/json
{
      "format":"jwt_vc_json",
       "proof":{
           "proof_type":"jwt",
            "jwt":"eyJhbGciOiJFZERTQSIsInR5cCI6IkpXVCIsImtpZC
I6ImRpZDpqd2s6ZXlKcmRIa2lPaUpQUzFBaUxDSmpjbllpT2lKRlpESTFOVEU1SWl3aWEybGtJam9pZUhaVmNYZDR
hbTQyYjBsdGNsVXROWGxETUZCdWFHOVZaa1pHZEhObFRGTTRNRmR6Wm5KcVJEWnNOQ0lzSW5naU9pSkNRME
poV0RoM1drNURXamxGVm04eE5XMXJZVTVoVWs5V2RqRXhhRmcyVFZCM2VYVmZTVWR2T0VOWkluMCMwIn0.e
```

```
yJhdWQiOiJodHRwczovL2lzc3Vlci1hcGktdGVzdC5ldGRhLm9yLnRoIiwiaWF0IjoxNzM2MDYwMTQ0LCJub25jZSI6Im
ZiMWQ1NDdlLWUwYTEtNDY4Ny05NTY2LWRkYTQxNzJlYmU1OCJ9.tUM4POiJf-mzAW3w-
rcJVGUwR8lWsYjMubD2ZRRGOqGPRupfetJdzmdUmersj1Tw88unGYKW-h2KcZEUBVADQ"
    }
}
```

คำอธิบายค่าพารามิเตอร์

พารามิเตอร์	Required	Type	รายละเอียด
format	Required	String	เป็นค่าประเภทสตริงที่กำหนดรูปแบบเอกสารรับรองที่จะออก ซึ่งอาจระบุประเภทและข้อมูลอื่น ๆ ที่มีความสัมพันธ์กับเอกสารรับรองที่ออก
proof	Optional	Object	proof of possession ของคีย์เข้ารหัสที่เอกสารรับรองที่ออกจะถูกผูกมัดไว้ จำเป็นหากมี proof_types_supported ใน credential_configurations_supported ของ metadata ของผู้ออกเอกสาร สำหรับเอกสารรับรองที่ขอ
proof_type	Required*	String	ค่าประเภทสตริงที่ระบุประเภทของ proof สำหรับคีย์ ค่าของพารามิเตอร์นี้กำหนดพารามิเตอร์อื่น ๆ ในวัตถุ proof ของคีย์ และกฎการประมวลผลที่เกี่ยวข้อง
credential_response_encryption	Optional	Object	ข้อมูลสำหรับเข้ารหัส Credential Response หากไม่มีพารามิเตอร์นี้ Credential Response ที่ส่งกลับมาจะไม่ถูกเข้ารหัส

Credential Response อาจเป็นแบบทันทีหรือแบบรอการดำเนินการ:

- กรณีตอบกลับทันที: ผู้ออกเอกสารออกเอกสารรับรองที่ร้องขอได้ทันทีและส่งไปยังกระเป๋าเอกสาร
- กรณีรอตอบกลับ (Deferred Response): ผู้ออกเอกสารอาจไม่สามารถออกเอกสารรับรองที่ร้องขอได้ทันที และจะส่งพารามิเตอร์ transaction_id ให้กับ กระเป๋าเอกสารเพื่อใช้ขอรับเอกสารรับรองเมื่อพร้อม รหัสสถานะ HTTP ต้องเป็น 202

การเข้ารหัสข้อมูล Credential Response:

- กรณีไม่มีการเข้ารหัส สื่อประเภทของคำตอบ (media type) ต้องถูกตั้งค่าเป็น application/json
- หากผู้ถือเอกสารร้องขอการเข้ารหัส Credential Response โดยส่ง credential_response_encryption ในคำขอ ผู้ออกเอกสารต้องเข้ารหัสข้อมูลใน Credential Response เป็น JWT โดยใช้พารามิเตอร์จาก credential_response_encryption และสื่อประเภทของคำตอบ (media type) ต้องถูกตั้งค่าเป็น application/jwt
- หากมีการร้องขอให้เข้ารหัสใน Credential Request แต่ Credential Response ไม่ได้ถูกเข้ารหัส กระเป๋าเอกสารควรปฏิเสธ Credential Response

ตัวอย่างการส่ง HTTP Response ของผู้ออกเอกสาร (ไม่ได้เข้ารหัส)

```
Content-Type: application/json
{
  "credential": "LUpixVCWJk0eOt4CXQe1NXK....WZwmhmn9OQp6YxX0a2L",
  "c_nonce": "fGFF7UkhLa",
  "c_nonce_expires_in": 86400
}
```

คำอธิบายค่าพารามิเตอร์

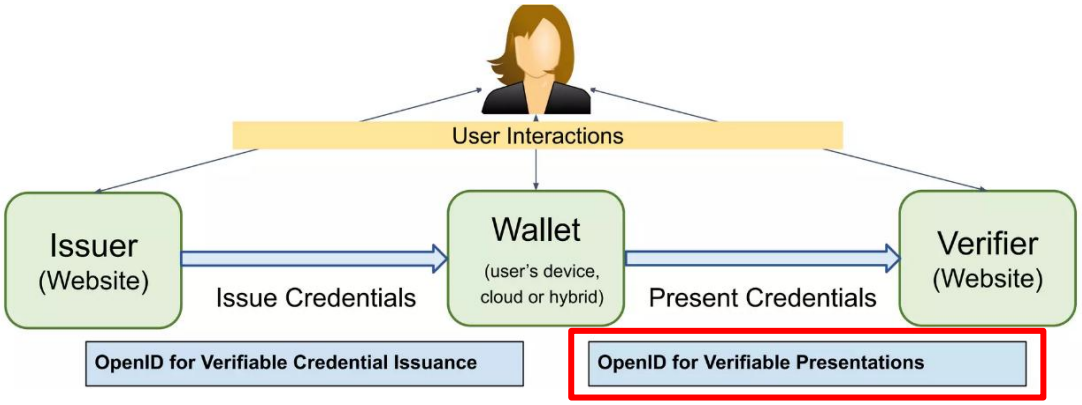
พารามิเตอร์	Required		รายละเอียด
credential	Optional	String	ข้อมูลของเอกสารรับรองที่ออกให้ อาจเป็นค่าแบบสตริงหรือออบเจ็กต์ ขึ้นอยู่กับรูปแบบของเอกสารรับรอง
transaction_id	Optional	String	เป็นค่าประเภทสตริงที่ระบุการออกเอกสารรับรองแบบ Deferred หากผู้ออกเอกสารไม่สามารถออกเอกสารรับรองได้ทันที โดยใช้ค่านี้ขอเอกสารรับรองในภายหลัง ค่านี้จะต้องถูกยกเลิกหลังจากที่กระเป๋าเอกสารได้รับเอกสารรับรองที่เกี่ยวข้องเรียบร้อยแล้ว
c_nonce	Optional	String	ค่าประเภทสตริงที่มี nonce ใช้ในการสร้าง proof of possession สำหรับ key proof
c_nonce_expires_in	Optional	Number	ระบุอายุการใช้งานของ c_nonce ในหน่วยวินาที

5.4 Protocol สำหรับการใช้งาน VP

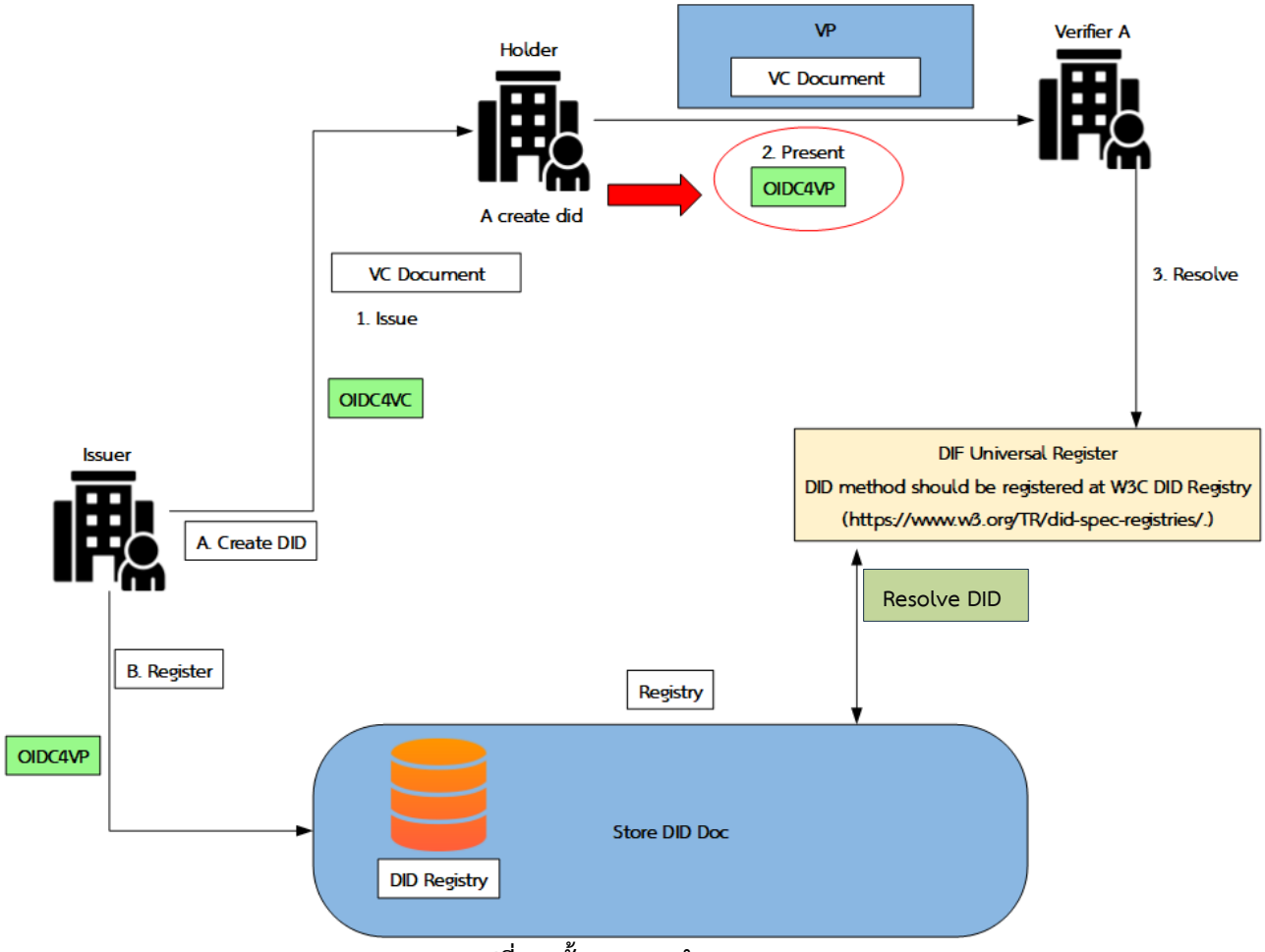
โพรโทคอล OpenID Connect for Verifiable Presentation Protocol (OID4VP) Draft Version 20 ต่อยอดจากโพรโทคอล OID4VC โดยมีการนำโพรโทคอล OpenID Connect (OIDC) มาใช้งานร่วมกันกับ เอกสารสำแดงดิจิทัล (VP)

(1) **OpenID Connect (OIDC)**: เป็นโปรโตคอลที่ใช้ในการยืนยันตัวตนบนอินเทอร์เน็ต โดยสามารถใช้ในการลงชื่อเข้าใช้และรับรองตัวตนของผู้ใช้ได้ โดยมีการใช้ Access Token และ ID Token เพื่อยืนยันตัวตนและรับข้อมูลพื้นฐานของผู้ใช้

(2) **Verifiable Presentations (VP)**: เป็นรูปแบบการนำเสนอข้อมูลที่เชื่อถือได้ ที่สามารถใช้ในการยืนยันข้อมูลหรือข้อมูลตัวตนของบุคคลหรือองค์กร โดยมีการลงนามด้วยลายมือชื่อดิจิทัลและเข้ารหัสเพื่อให้มั่นใจได้ว่าข้อมูลมีความน่าเชื่อถือและไม่ได้ถูกแก้ไขโดยไม่ได้รับอนุญาต



รูปที่ 12 การใช้งาน OID4VP



รูปที่ 13 ขั้นตอนการทำ OID4VP

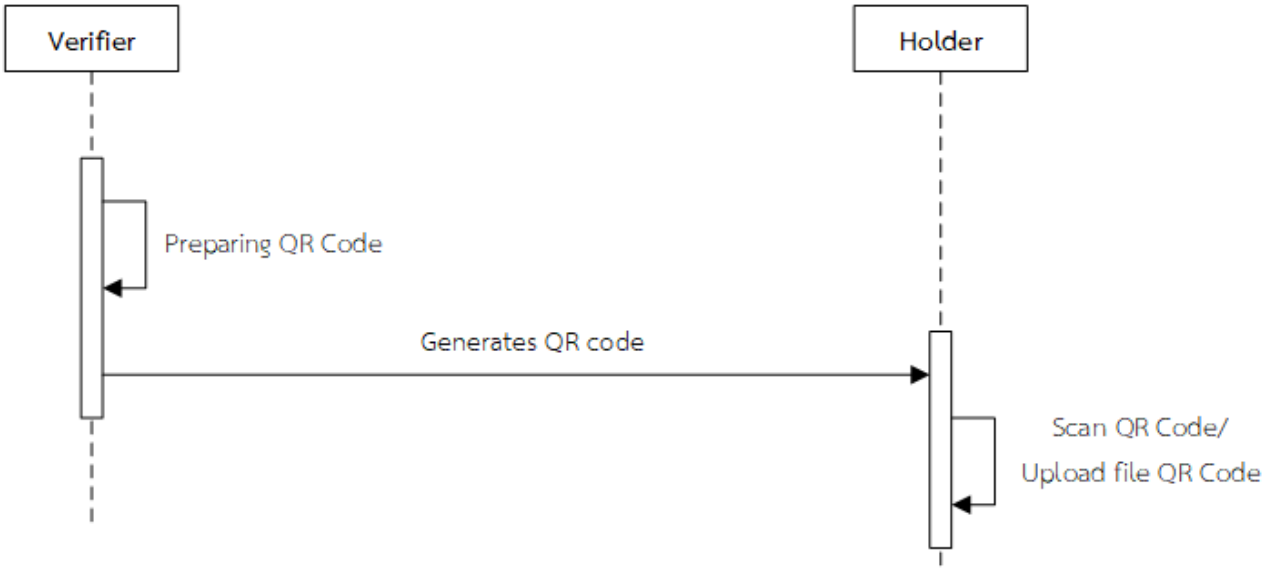
5.4.1 กระบวนการทำงาน OID4VP

การตรวจสอบข้อมูลเอกสารสำแดงดิจิทัล (VP) จะใช้โพรโทคอล OID4VP draft 20 มีขั้นตอนการทำงานดังนี้

(1) ผู้ตรวจสอบเอกสารส่ง Authorization Request ให้ผู้ถือเอกสาร

(2) ผู้ถือเอกสารส่ง VP ให้ผู้ตรวจสอบผ่าน Authorization Response

(1) ผู้ตรวจสอบเอกสารส่ง Authorization Request ให้ผู้ถือเอกสาร



รูปที่ 14 สร้าง Authorization QR Code

- Verifier สร้าง QR

- ผู้ถือเอกสารดำเนินการ Scan QR Code หรือ Upload QR Code

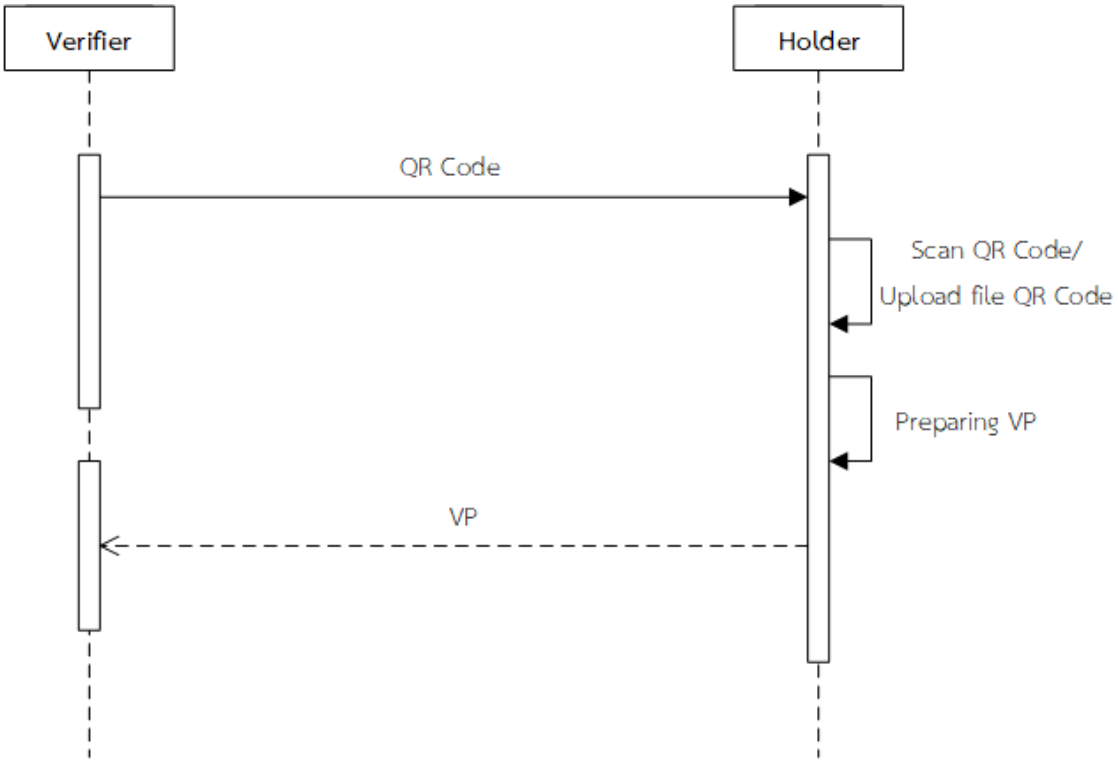
ตัวอย่างการ Decode QR ของ Verifier

```
{
    "client_id":"http://verifier.com/VP/callback",
    "client_id_scheme":"redirect_uri",
    "response_uri":"http://verifier.com/VP/callback",
    "response_type":"vp_token",
    "presentation_definition_uri": “https://verifier.com/openid4vc/pd/ijkguJGU”
    "nonce":"fa2450d7-8ca5-40d2-8832-b03891c355be"
}
```

คำอธิบายค่าพารามิเตอร์

พารามิเตอร์	**Required**		**รายละเอียด**
client_id	Required	String	ตัวระบุของผู้ตรวจสอบเอกสาร
client_id_scheme	Optional	String	รูปแบบของ client_id ที่ใช้
response_uri	Optional	String	URI ที่ใช้ในการ callback
response_type	Required	String	ประเภทของ Grant Type ที่ต้องตอบกลับ ในการศึกษากำหนดค่าเป็น “vp_token”
presentation_definition	Required*	String	สตริงที่มี Presentation Definition ในรูปแบบวัตถุ JSON ต้องมีหากไม่มีพารามิเตอร์ presentation_definition_uri หรือค่า scope
presentation_definition_uri	Required*	String	สตริงที่เป็น URL แบบ HTTPS ที่สามารถดึง JSON ของ Presentation Definition ได้ ในการศึกษาใช้พารามิเตอร์นี้ ต้องมีพารามิเตอร์นี้หากไม่มีพารามิเตอร์ presentation_definition หรือค่า scope
client_metadata	Optional	JSON	JSON ที่มีค่า Metadata ของผู้ตรวจสอบเอกสารซึ่งต้องเข้ารหัสเป็น UTF-8 และ ต้องไม่มีหากพารามิเตอร์ client_metadata_uri มีอยู่
client_metadata_uri	Optional	String	สตริงที่เป็น URL แบบ HTTPS ชี้ไปยัง JSON ที่มี Metadata ของผู้ตรวจสอบเอกสารได้ ต้องไม่มีหากพารามิเตอร์ client_metadata มีอยู่
nonce	Required	String	ใช้ผูก Verifiable Presentation(s) กับธุรกรรมนั้น ๆ เพื่อความปลอดภัย
state	Optional	String	ใช้เพื่อเชื่อมโยง Request กับ Response

(2) ผู้ถือเอกสารส่ง VP ให้ผู้ตรวจสอบผ่าน Authorization Response



รูปที่ 15 OID4VP Initiation

- Verifier สร้าง QR Code และส่งให้ Holder ทำการ Scan QR หรือ Upload file QR Code
- Holder ทำการสร้างข้อมูล VP ตามโครงสร้างในตัวอย่างที่ 2
- Holder ส่งข้อมูล VP ให้ทาง Verifier

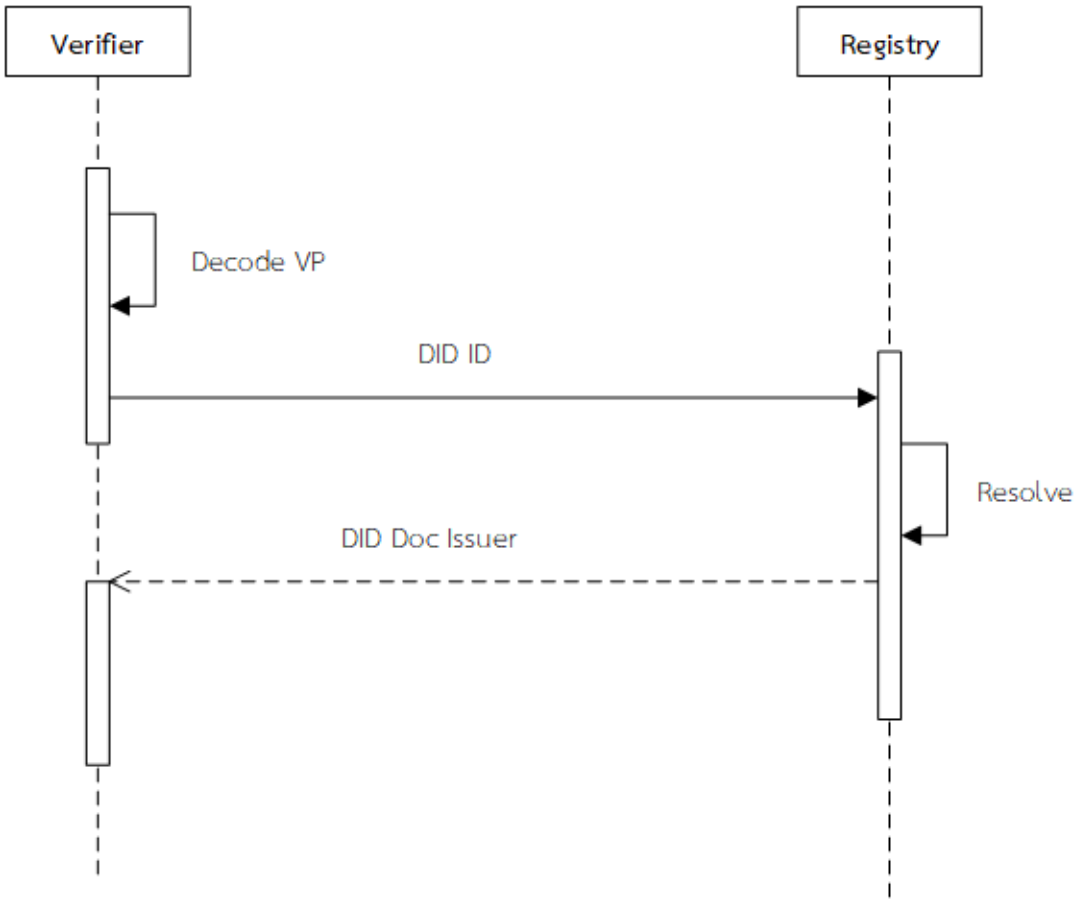
ตัวอย่างการส่ง HTTP Response VP

```
Content-Type: application/x-www-form-urlencoded
{
vp_token=eyJhbGciOiJFZ...ziRjjF8Z3V5QkHEhZTFplqnqfk2BxEtZDA
presentation_submission={"id":"qtxBFfOmPg7A","definition_id":"qtxBFfOmPg7A","descriptor_map":[{"id":"Transcript
Credential","format":"jwt_vp","path":"$","path_nested":{"id":"TranscriptCredential","format":"jwt_vc_json","path":"$.v
erifiableCredential[0]"}}]}
state=sIiRkOc7THO }
```

คำอธิบายค่าพารามิเตอร์

พารามิเตอร์	Required	Type	รายละเอียด
vp_token	Required	JSON String, JSON object	ข้อมูลเอกสารสำแดง
presentation_submission	Required	Array	การจับคู่ (Mappings) ระหว่างเอกสารรับรองที่ร้องขอและตำแหน่งที่สามารถพบได้ภายใน VP Token ที่ส่งกลับ

5.4.2 กระบวนการ Resolve DID เพื่อตรวจสอบ VP



รูปที่ 16 Resolve DID

- ผู้ตรวจสอบเอกสารรับข้อมูล VP จากผู้ถือเอกสาร ดำเนินการ Decode VP และตรวจสอบความถูกต้องของโครงสร้าง
- ผู้ตรวจสอบเอกสารทำการส่งข้อมูล DID ID ไปตรวจสอบข้อมูลใน Registry
  ข้อมูล DID => “did:tbsi:zv8fVB1i6S7MLMZX8wd3Ayo”
- การ Resolve ข้อมูลใน Registry มี 2 รูปแบบ
  - ทำการ Request ผ่าน DIF Universal Resolver
  - ทำการ Request ไปยัง Registry โดยตรง ซึ่งในรายงานฉบับนี้จะใช้วิธี “http get”
- ข้อมูลที่ได้จากการทำ Resolve คือข้อมูล DID Doc ของผู้ออกเอกสารและส่งข้อมูล DID Doc กลับมาให้ผู้ตรวจสอบเอกสาร

การตรวจสอบข้อมูลใน Registry ในรายงานฉบับนี้จะระบุพารามิเตอร์ดังนี้

ตัวอย่างการส่ง HTTP Request

```
GET ' http://example.verifier_url/GetDIDDoc?'
Id= did:tbsi:zv8fVB1i6S7MLMZX8wd3Ayo
```

คำอธิบายค่าพารามิเตอร์

พารามิเตอร์	Required	รายละเอียด
Id	Required	หมายเลข DID

ข้อมูลที่ได้จากการ Resolve และส่งกลับไปให้ Verifier

ตัวอย่างการส่ง HTTP Response ของ Registry ไปยัง Verifier


```
{
    "status": 200,
    "message": "Success",
    "data": {
        "@context": "https://www.context.org",
        "id": "did:tbsi:zv8fVB1i6S7MLMZX8wd3Ayo",
        "verificationMethod": [
            {
                "id":"did:tbsi:zv8fVB1i6S7MLMZX8wd3Ayo#1XmYo2EnZwAL0giRxBWMADGk2Zei\+TD2VKx7aWgWWAo
=",
                "type": "JsonWebKey2020",
                "publicKeyJwk": {
                    "kty": "OKP",
                    "crv": "Ed25519",
                    "alg": "EdDSA"
                }
            }
        ],
        "assertionMethod": []
    }
}
```


คำอธิบายค่าพารามิเตอร์

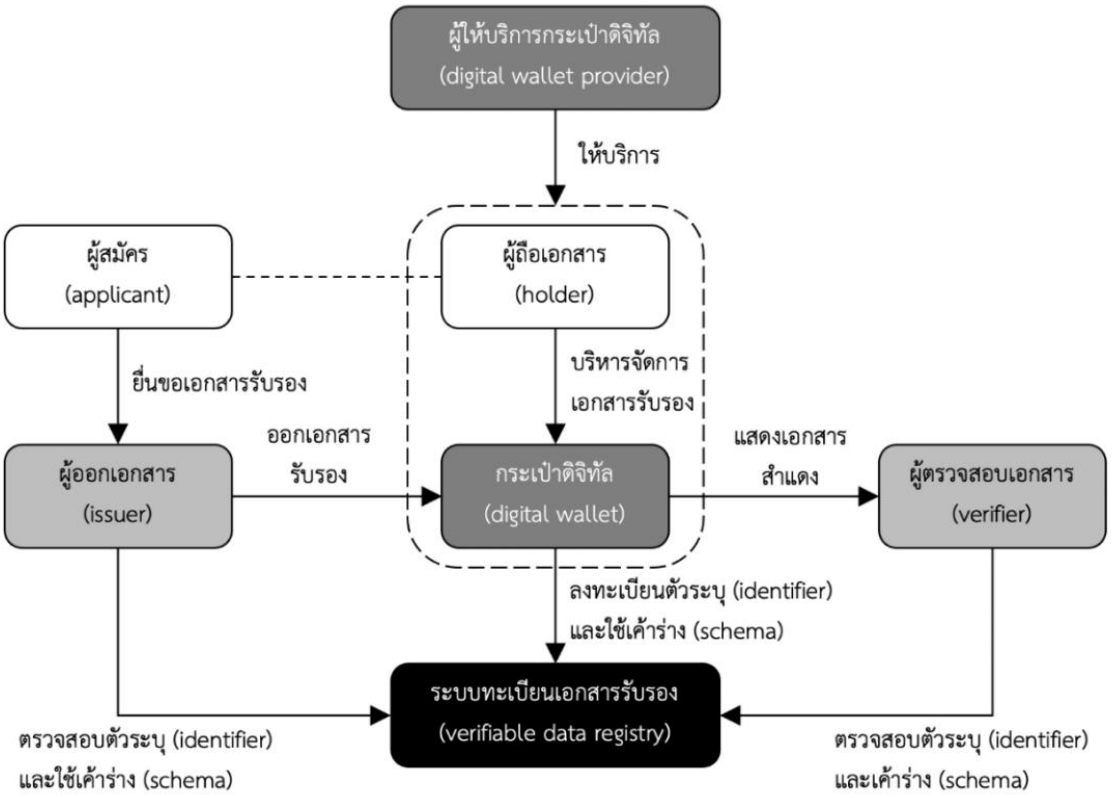
พารามิเตอร์	Required	Type	รายละเอียด
Status	Required	Nuber	สถานะการเรียกใช้งาน
Message	Required	String	คำอธิบาย status
Data	Required	JSON	ข้อมูล DID DOC

5.5 Universal Resolver

ในการที่จะให้ทุกระบบนิเวศน์ (ecosystem) ได้ทำงานร่วมกันได้ หรือการทำงานในรูปแบบ interoperability จำเป็นต้องมีตัวกลางในการเก็บรวบรวมข้อมูลที่ไว้สำหรับตรวจสอบและยืนยันความถูกต้องของข้อมูลสำคัญต้องเป็นรูปแบบมาตรฐานเดียวกัน จึงมีแนวคิดการใช้งาน DIF Universal Resolver เกิดขึ้น

โดย DIF Universal Resolver จะเปรียบเสมือนประตูที่จะนำไปสู่เส้นทางของแต่ละระบบนิเวศน์ (ecosystem) ดังนั้น เพื่อให้การทำงานในรูปแบบ Interoperability สมบูรณ์แบบ ในแต่ละ Ecosystem ต้องดำเนินการลงทะเบียนใช้งาน DIF Universal Resolver อย่างพร้อมเพียง ซึ่งข้อมูลจะอยู่ในรูปแบบอิเล็กทรอนิกส์ที่เป็น File format มาตรฐานเดียวกันทั้ง Ecosystem และเมื่อต้องการที่จะตรวจสอบความถูกต้องของข้อมูลที่มาจากแต่ละ Ecosystem ก็จะสามารถสอบถามไปที่ DIF Universal Resolver ได้ทันที ทำให้การดำเนินการในแต่ละขั้นตอน เป็นไปได้อย่างรวดเร็ว มีมาตรฐาน และแม่นยำมากยิ่งขึ้น

5.6 บทบาทและกระบวนการที่เกี่ยวข้องภายใต้ VC Ecosystem



รูปที่ 17 บทบาทของผู้ที่เกี่ยวข้องกับการใช้งานเอกสารรับรองดิจิทัล

a. ผู้ออกเอกสาร (Issuer) และกระบวนการที่เกี่ยวข้อง

(1) สร้าง DID Document ในรูปแบบ Legal Person

(2) ลงทะเบียนใน Registry

(3) เป็นผู้สร้าง VC

(4) ยึดมาตรฐานการส่ง VC ในรูปแบบ Protocol OID4VCI

(5) สร้างและแสดง QR Code เพื่อให้ Holder เข้ามาร้องขอข้อมูลที่ต้องการ

(6) ออก Token เพื่อใช้ในการยืนยันการส่ง VC

(7) ตรวจสอบความถูกต้องของข้อมูลร้องขอ VC ที่ได้รับจาก Holderส่งข้อมูล VC ในรูปแบบ JWT ให้กับทาง Holder

b. เจ้าของกระเป๋าเอกสารดิจิทัล (Wallet Holder) และกระบวนการที่เกี่ยวข้อง

(1) สร้าง DID Document ในรูปแบบ Natural Person

(2) ร้องขอข้อมูลที่ต้องการจาก Issuer

(3) Scan QR Code ที่ Issuer แสดงขึ้นมา เพื่อดำเนินการขอข้อมูล VC ในรูปแบบ Protocol OID4VCI

(4) ร้องขอ Token จาก Issuer เพื่อใช้ตรวจสอบการขอ VC

(5) จัดเก็บ VC ที่ได้จาก Issuer ใน Wallet สำเร็จ

(6) เลือก Verifier ที่ต้องการจะส่งต่อข้อมูล VC

(7) สร้างข้อมูล VC ให้อยู่ในรูปแบบ VP

(8) Scan QR Code ที่ Verifier แสดงขึ้นมา เพื่อดำเนินการส่งข้อมูล VP ในรูปแบบ Protocol OID4VP

(9) ร้องขอ Token จาก Verifier เพื่อใช้ตรวจสอบการส่ง VP

(10)ดำเนินการส่งข้อมูล VP ให้กับ Verifier สำเร็จ

c. ผู้ตรวจสอบเอกสาร (Verifier) และกระบวนการที่เกี่ยวข้อง

(1) ยึดมาตรฐานการรับ VP ในรูปแบบ Protocol OID4VP

(2) สร้างและแสดง QR Code เพื่อให้ Holder เข้ามาร้องขอการส่งข้อมูล

(3) ออก Token เพื่อใช้ในการยืนยันการรับ-ส่ง VP

(4) รับข้อมูล VP จาก Holder สำเร็จ

(5) ดึงข้อมูล (Resolve) จาก Registry จะดำเนินการผ่านขั้นตอน Decentralized Identity Foundation Universal Resolver (DIF Universal Resolver) เพื่อนำมาตรวจสอบความถูกต้องของผู้ออกข้อมูล VC

(6) ดำเนินการตรวจสอบความถูกต้องของข้อมูล VP ที่ได้รับมา โดยตรวจสอบรายละเอียด ดังนี้

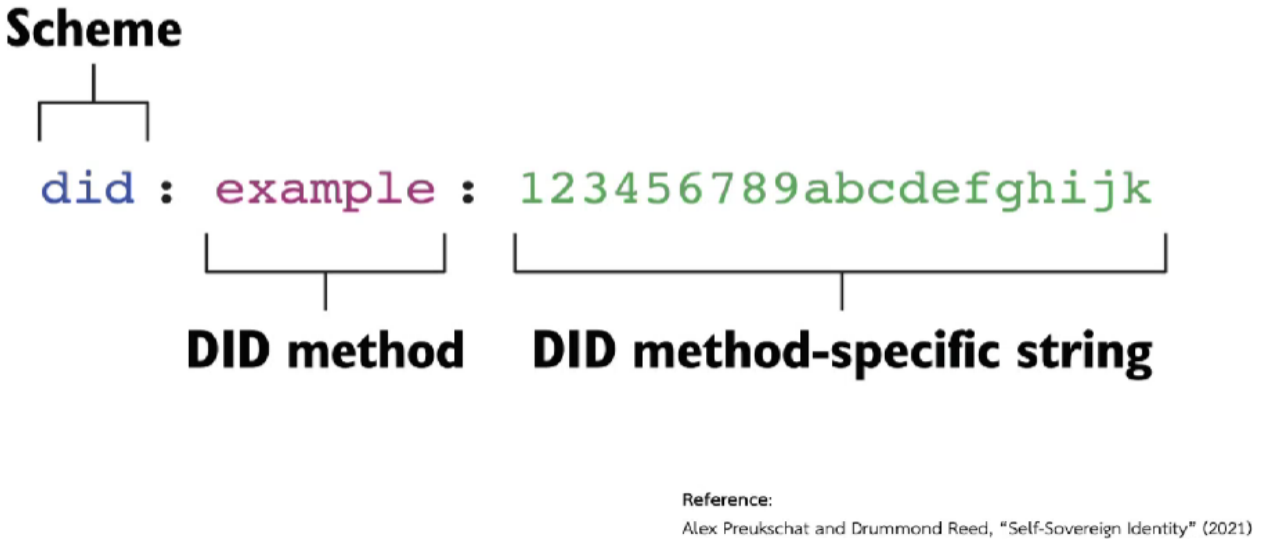
- ถอดรหัสข้อมูลเอกสารรับรองดิจิทัล (Decode the VC) เป็นการตรวจสอบโครงสร้างของเอกสารรับรองดิจิทัล ต้องประกอบด้วย
  - คำอธิบายข้อมูลของ VP (presentation metadata)
  - คำอธิบายข้อมูลของ VC (credential metadata)
  - ข้อพิสูจน์ (proof)
- ตรวจสอบลายมือชื่อดิจิทัล (Verify the Signature) จะตรวจสอบความถูกต้องของข้อมูลกุญแจสาธารณะของผู้ออกเอกสารรับรอง
- ตรวจสอบความถูกต้องของผู้ออกเอกสาร (Check Issuer's Credentials)
- ตรวจสอบความถูกต้องของโครงสร้างเอกสารรับรองดิจิทัล (Validate the Credential Schema)
- ตรวจสอบวันหมดอายุของเอกสารรับรองดิจิทัล (Validate the Credential Expiry)

6. Decentralized Identifiers Methodologies

เป็นตัวระบุ (identifier) บนระบบทะเบียนเอกสารรับรอง (verifiable data registry) แบบกระจายศูนย์ที่ใช้ URL ในการเชื่อมโยงกับเอนทิตี้ โดยทั่วไป DID จะนำมาใช้ใน VC เพื่อแสดงความเชื่อมโยงไปยังเจ้าของข้อความซึ่งทำให้สามารถส่งต่อหรือโอนย้าย VC จากกระเป๋าเอกสารดิจิทัลหนึ่งไปยังกระเป๋าเอกสารดิจิทัลอีกอันหนึ่งได้โดยไม่จำเป็นต้องออก VC ชุดใหม่อย่างไรก็ตาม VC ไม่จำเป็นต้องใช้ identifier เป็น DID ก็ได้

6.1 รูปแบบ DID

อ้างอิงตาม W3C โครงสร้างของ DID สามารถแสดงได้ตามรูปที่ ค ซึ่งประกอบด้วย 3 ส่วน ได้แก่ (1) scheme (2) DID method และ (3) DID method-specific string



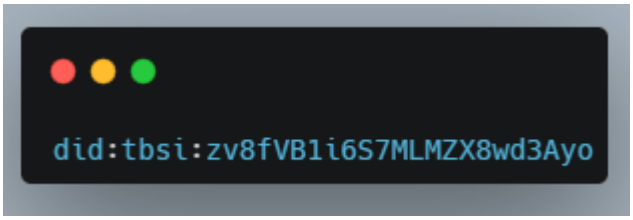
รูปที่ 18 โครงสร้าง DID

6.2 การสร้างและการทะเบียน DID Document

ยกตัวอย่างการทำ Digital Document โครงสร้างของ DID จะเป็นตามรูปที่ 19 ในส่วนของ DID method จะระบุเป็น “tbsi” และ DID method-specific ขึ้นต้นด้วยตัวอักษร “z” และชุดข้อความสุ่ม 16 ตัวอักษร

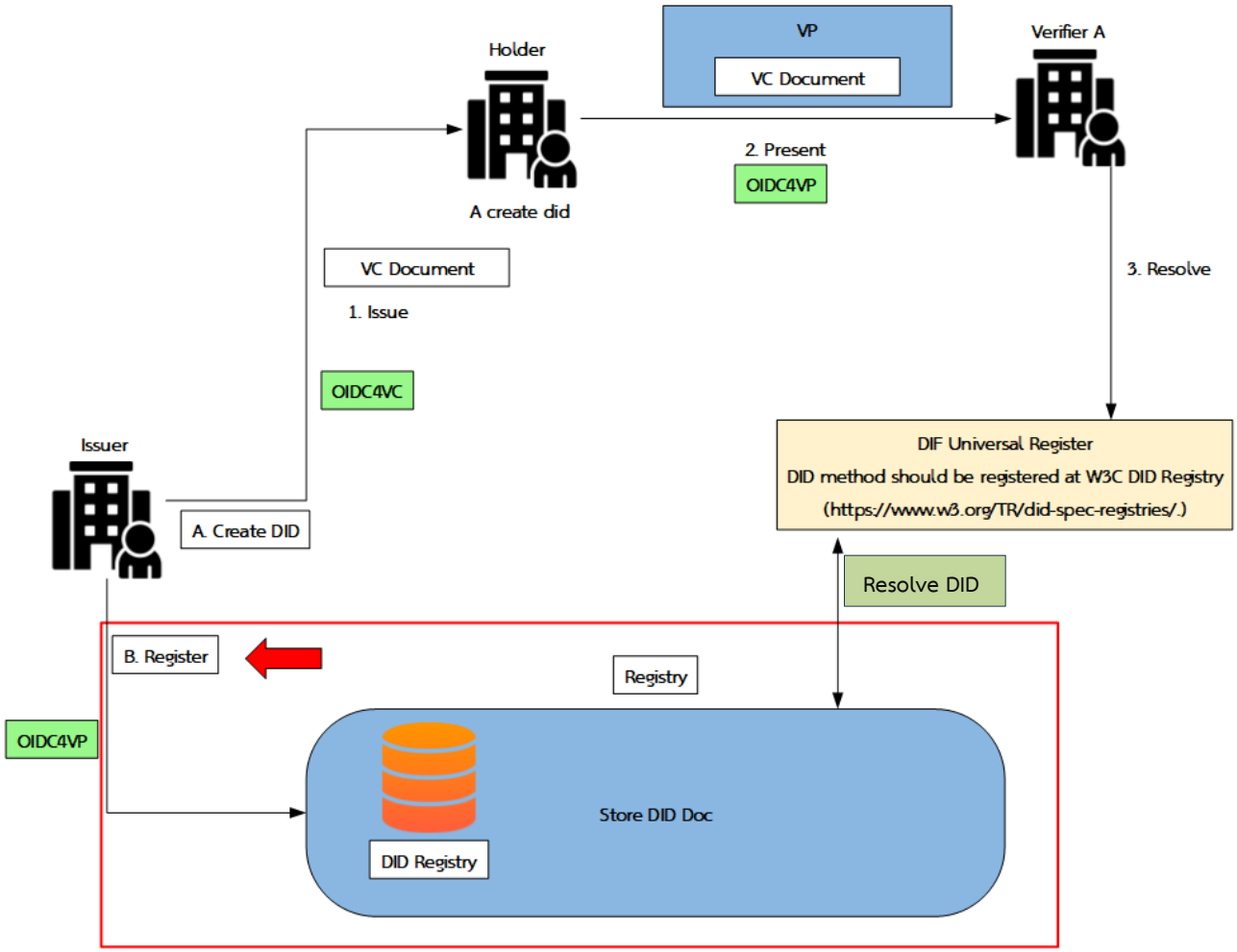
รูปที่ 19 โครงสร้าง DID Document

จากโครงสร้าง DID ข้างต้น เมื่อทำการสร้าง DID จะมีลักษณะองค์ประกอบ ตามรูปที่ 20



รูปที่ 20 DID ID

ข้อมูลที่ได้จากการสร้าง DID จะนำไปใช้ในการสร้าง DID Document เพื่อใช้ในการลงทะเบียน (Register) ในระบบ Registry ตามรูปที่ 21 การลงทะเบียนใน Registry จะทำโดยใช้โพโทคอล OID4VP ซึ่งข้อมูลที่นำมาใช้ในการลงทะเบียน คือ DID Document ในรายงานฉบับนี้จะเป็นการลงทะเบียนแบบออฟไลน์ (Offline)



รูปที่ 21 การลงทะเบียน DID Document

(1) DID Document

เป็นชุดข้อมูลที่อธิบาย DID ประกอบด้วยข้อมูลที่ใช้ในการเข้ารหัสลับ (encrypted data) และกุญแจสาธารณะ (public key) ดังแสดงตามรูปที่ 22

รูปที่ 22 โครงสร้าง DID Document

6.3 การดึงข้อมูล (Resolve) DID Document

DID Document ที่ได้ทำการลงทะเบียน (Register) ลงใน Registry ผ่านโพโทคอล OID4VP การดึงข้อมูล (Resolve) จาก Registry จะดำเนินการผ่านขั้นตอน Decentralized Identity Foundation Universal Resolver (DIF Universal Resolver) ซึ่งเป็นตัวกลางในการดึงข้อมูลจาก Registry ต่าง ๆ แสดงตามรูปที่ 21 โดยหากต้องการใช้ DIF Universal Resolver จำเป็นต้องมีผู้ให้บริการ และแต่ละระบบนิเวศน์ (Ecosystem) จะต้องทำการลงทะเบียนต่อผู้ให้บริการ โดยระบุรูปแบบ (pattern) ของ DID และ URL ของ Registry เพื่อทำการดึงข้อมูล (Resolve) และ ตัวอย่าง DID ที่ถูกต้องภายในระบบ ดังแสดงตามรูปที่ 25

สำหรับกรณีศึกษาในรายงานฉบับนี้จะใช้วิธีการดึงข้อมูลผ่าน “http get” ดังแสดงตามรูปที่ 24

การดึงข้อมูล (Resolve) ผ่าน “http get” จะเป็นขั้นตอนการตรวจสอบ DID ID ในเอกสารสำแดงดิจิทัล (VP) ข้อมูลที่ทำการดึงข้อมูลออกมาจะเป็นเอกสาร DID Document ดังแสดงตามรูปที่ 25 ข้อมูลที่ได้จะนำไปใช้ในการตรวจสอบความถูกต้องของเอกสารรับรองดิจิทัล (VC) และเอกสารสำแดงดิจทัล (VP) ดังนี้

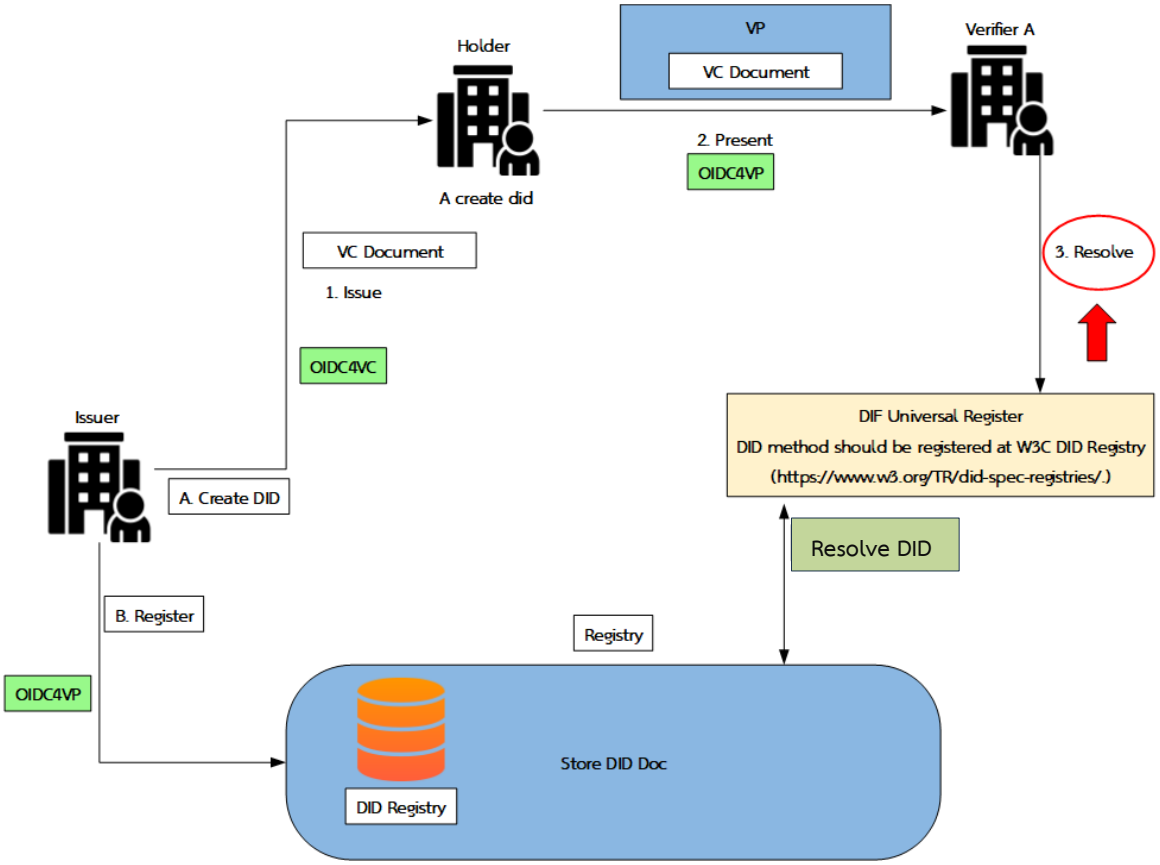
(1) ถอดรหัสข้อมูลเอกสารรับรองดิจิทัล (Decode the VC) เป็นการตรวจสอบโครงสร้างของเอกสารรับรองดิจิทัล ต้องประกอบด้วย (1) คำอธิบายข้อมูลของ VC (credential metadata) (2) ข้อความยืนยัน (claim) และ (3) ข้อพิสูจน์ (proof)

(2) ตรวจสอบลายมือชื่อดิจิทัล (Verify the Signature) จะตรวจสอบความถูกต้องของข้อมูลกุญแจสาธารณะของผู้ออกเอกสารรับรอง

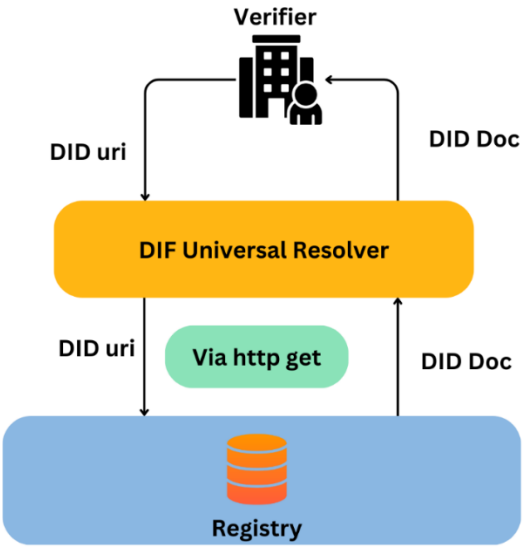
(3) ตรวจสอบความถูกต้องของผู้ออกเอกสาร (Check Issuer’s Credentials)

(4) ตรวจสอบความถูกต้องของโครงสร้างเอกสารรับรองดิจิทัล (Validate the Credential Schema)

(5) ตรวจสอบวันหมดอายุของเอกสารรับรองดิจิทัล (Validate Credential Expiration)

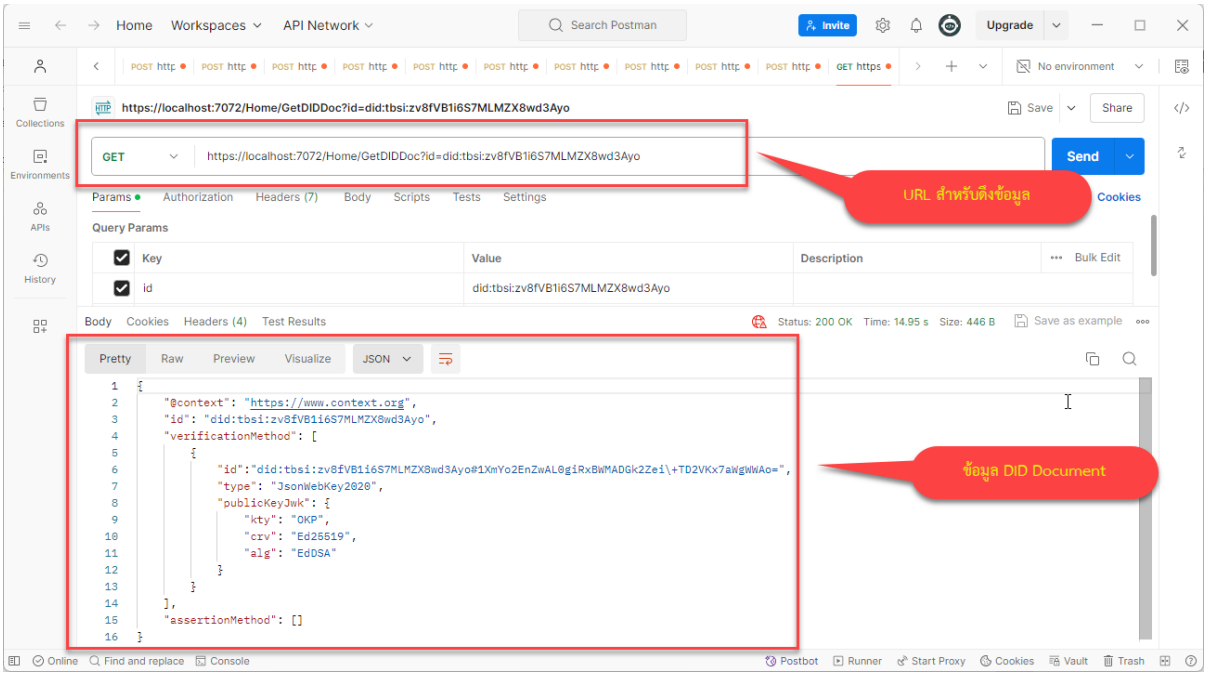


รูปที่ 23 ขั้นตอน Resolve DID Document



รูปที่ 24 การดึงข้อมูลผ่าน http get

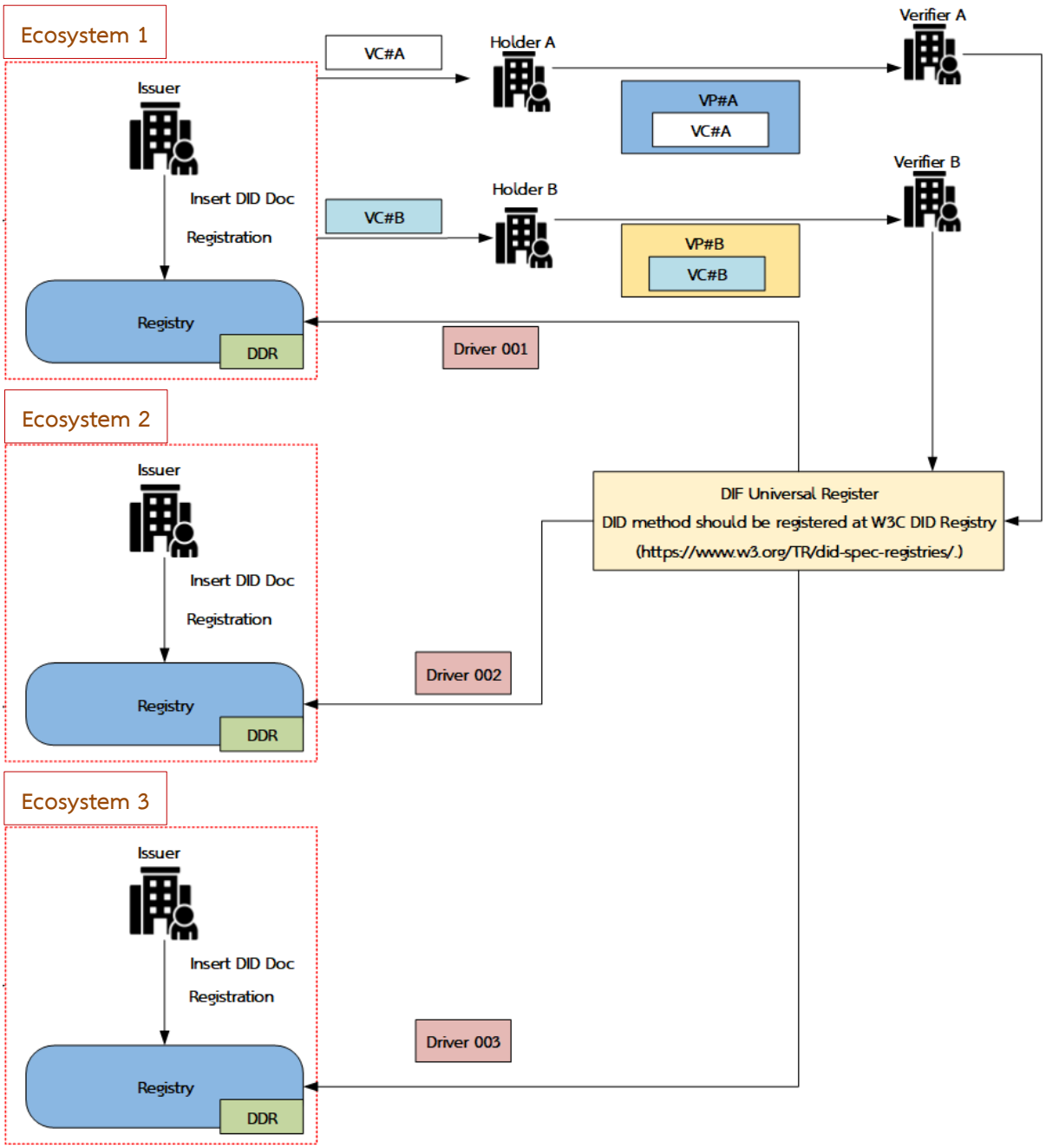
ในตัวอย่าง จะเป็นการแสดงถึงการเรียกในรูปแบบ http get โดย Key ที่ส่งไปพร้อมกับ URL คือ DID ของ Issuer ที่ได้มาจากข้อมูลของ VC และเมื่อส่งข้อมูลในรูปแบบ URL แล้วข้อมูลถูกต้อง ทาง Registry จะตอบกลับเป็น DID Document มาให้ โดย DID Document จะเป็นของ Issuer ที่ได้ทำการลงทะเบียนไว้กับ Registry



รูปที่ 25 ข้อมูลที่ผ่านการ resolve

รูปที่ 26 การตั้งค่า Registry สำหรับ DIF Universal Resolver

7. ภาพรวมการทำงานร่วมกัน (Interoperability) ข้ามระบบนิเวศ (Ecosystem)



รูปที่ 27 Interop. ระหว่าง Ecosystem

จากรูปที่ 27 จะเห็นว่ามี Ecosystem อยู่ทั้งหมด 3 Ecosystem โดย Holder สามารถขอข้อมูลจาก Ecosystem ใดก็ได้ขึ้นอยู่กับข้อมูลที่ต้องการ โดยจะอธิบายในแต่ละส่วน ดังนี้

1. ในแต่ละ Ecosystem ในส่วนของ Issuer ต้องสร้าง DID Document ในรูปแบบ Legal Person โดยต้องนำ DID Document ที่สร้าง ไป Register ลงใน Registry
2. Holder สามารถร้องขอข้อมูลจาก Ecosystem ใดก็ได้ ขึ้นอยู่กับข้อมูลในแต่ละ Ecosystem นั้น เป็นข้อมูลที่ทาง Holder ต้องการหรือไม่ โดยข้อมูล VC ที่ได้จาก Issuer แต่ละ Ecosystem จะถูกจัดเก็บไว้ใน Digital Wallet ของแต่ละ Holder

3. Holder สามารถส่งข้อมูลให้กับทาง Verifier ได้ โดยข้อมูลที่ทำการส่งให้นั้น ต้องดำเนินการจัดทำให้อยู่ในรูปแบบ VP ก่อนเสมอ
4. เมื่อ Verifier ต้องการจะตรวจสอบความถูกต้องของข้อมูลที่ได้รับมา จำเป็นต้องมีข้อมูล DID Document ของผู้ที่ออก VC ให้กับ Holder ก่อน ดังนั้นจึงต้องเรียกข้อมูล DID Document ของ Issuer ที่ได้ลงทะเบียนไว้ ผ่าน DIF Universal resolver
5. DIF Universal resolver จะส่งกลับ (Return) ข้อมูล DID Document ของ Issuer ที่ได้ทำการลงทะเบียนไว้ใน Registry กลับมาให้กับทาง Verifier เพื่อนำมาดำเนินการต่อ
6. Verifier นำ DID Document ที่ได้ ไปตรวจสอบความถูกต้องของข้อมูล VC ต่อไป

8. Implementation Guidelines

ข้อแนะนำเบื้องต้นการพัฒนาระบบจะช่วยให้การให้บริการและการแลกเปลี่ยนเอกสารรับรองดิจิทัลมีความมั่นคงปลอดภัยและช่วยคุ้มครองข้อมูลส่วนบุคคลของเอนทิตีต่าง ๆ ที่เกี่ยวข้อง รวมถึงช่วยจำกัดความซับซ้อนของแนวทางการพัฒนาเชิงเทคนิค (technical solution) เพื่อให้กระเป๋าเอกสารดิจิทัลและเอกสารรับรองสามารถทำงานร่วมกันได้

8.1 องค์ประกอบพื้นฐาน

ในรายงานนี้จะใช้กรณีศึกษา เรื่อง การออกใบประมวลผลการศึกษา (Transcript) ของสถาบันการศึกษาในประเทศไทย โดยมีการใช้ข้อมูล ดังนี้

(1) **พัฒนาโดยใช้ภาษาคอมพิวเตอร์ระดับสูง (High-Level Language)**

(2) **ข้อกำหนดทางเทคนิค** ประกอบไปด้วยดังนี้

- อัลกอริทึมสำหรับการทำลายมือชื่ออิเล็กทรอนิกส์ Edwards-Curve Digital Signature Algorithm (EdDSA)
- รูปแบบการเข้ารหัส Ed25519
- เค้าร่างของเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัลเป็นในรูปแบบ JSON-LD
- VC และ VP จะใช้งานในรูปแบบ JWT
- Protocol OID4VC draft 13 และ OID4VP draft 20
- Authorize code flow เป็นรูปแบบ pre-authorized code flow

8.2 กรณีศึกษาของคณะทำงานฯ

รายงานฉบับนี้ เป็นการศึกษาการออกเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล โดยใช้รูปแบบของการออกใบประมวลผลการศึกษา (Transcript) ของสถาบันการศึกษามาเป็นกรณีศึกษาตามรูปที่ 6 ซึ่งมีข้อกำหนดดังนี้

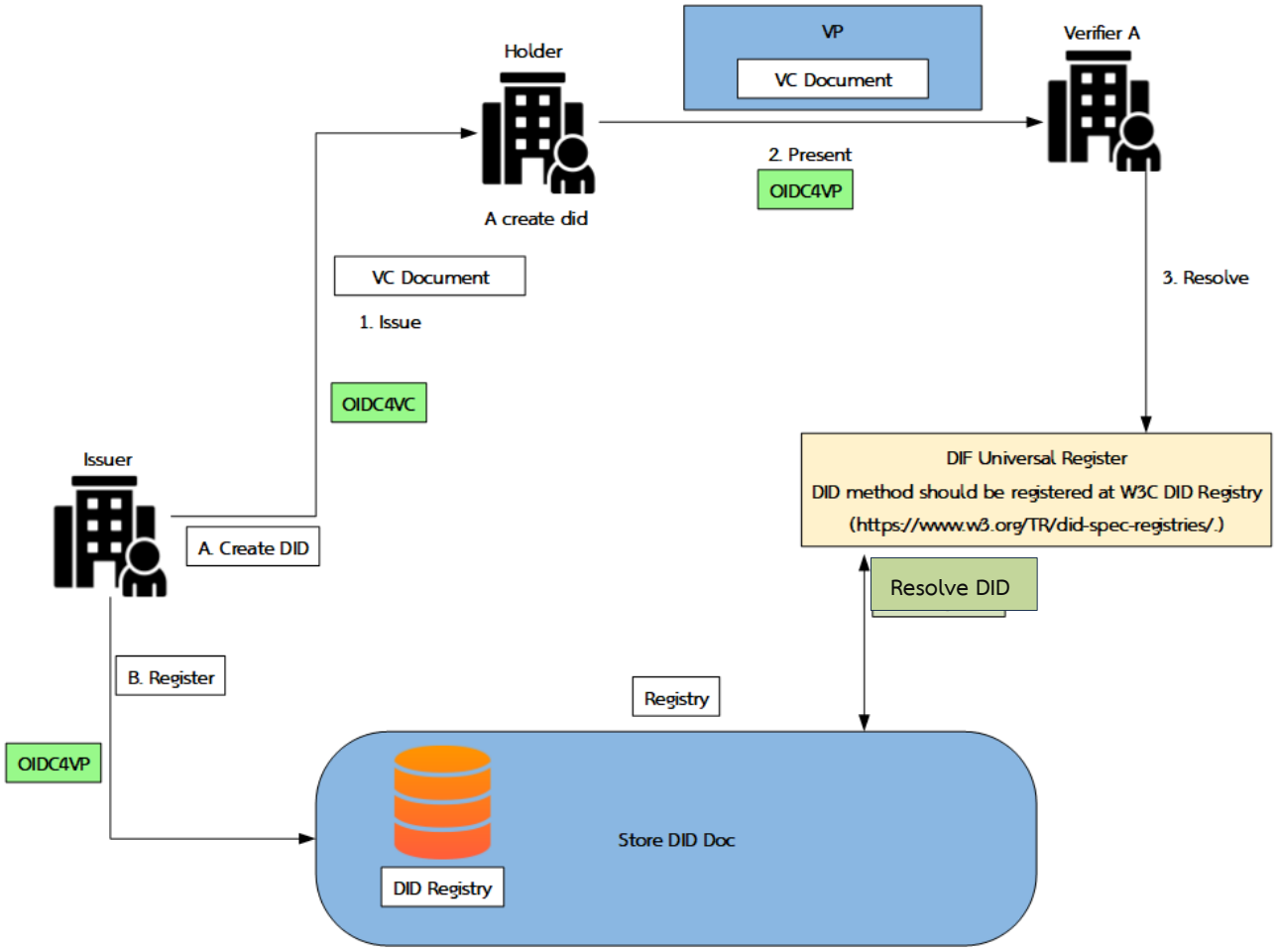
(1) การศึกษามุ่งเน้นไปที่ขั้นตอนการออกเอกสารรับรองดิจิทัล (VC) และเอกสารสำแดงดิจิทัล (VP)

(2) กระบวนการดึงข้อมูล (Resolve) DID Document ตามมาตรฐานของ W3C จะเป็นการใช้ DIF Universal Resolver ซึ่งในรายงานฉบับนี้จะเป็นการใช้ DIF Universal จำลองของสพธอ. (ETDA) ที่พัฒนาขึ้นเพื่อรองรับความพร้อมของการใช้งานของผู้ให้บริการในคณะทำงานส่งเสริมการพัฒนาเพื่อรองรับการใช้งาน Document Wallet และ Verifiable Credentials ก่อนเบื้องต้น เพื่อไปดึงข้อมูล DID Document จาก Registry

(3) ขั้นตอนการลงทะเบียน (Register) จะดำเนินการโดยใช้โพรโทคอล OpenID4VP ในรายงานฉบับนี้ทางคณะทำงานส่งเสริมการพัฒนาเพื่อรองรับการใช้งาน Document Wallet และ Verifiable Credentials ได้สร้าง DID Document แล้วบันทึกลง Registry เอง

ภาคผนวก

ภาคผนวก ก. การทำงานร่วมกัน (Interoperability) ระหว่าง Issuer และ Wallet Holder และ Verifier



รูปที่ 28 ภาพรวมของการศึกษา Digital Document

การออกแบบแนวทางการ Interoperability ระหว่าง Issuer และ Wallet Holder และ Verifier ในโครงการ มีขั้นตอน ดังนี้

(1) กำหนด Registry สำหรับการทดสอบขึ้นมา 1 Registry เพื่อให้ Issuer ทำการ Register

(2) กำหนด Issuer เพื่อใช้ในการทดสอบ โดย Issuer จะทำการสร้าง DID ไว้ เพื่อใช้สำหรับส่งข้อมูล และทำการ Register กับ Registry ที่ได้ทำการจัดเตรียมไว้

(3) กำหนด Holder เพื่อใช้ในการ Request ข้อมูลกับทาง Issuer และรับข้อมูล VC ที่จะได้จาก Issuer รวมถึงส่งข้อมูลในรูปแบบ VP ให้กับทาง Verifier

(4) กำหนด Verifier เพื่อใช้ในการรับข้อมูล VP จาก Holder พร้อมทั้งต้องตรวจสอบความถูกต้องของข้อมูล ตลอดจนการรับ-ส่ง ข้อมูลกับทาง DIF Universal Resolver

(5) สร้าง http get เพื่อใช้ในการเข้าถึง Registry พร้อมกับส่งข้อมูลให้กับทาง DIF Universal Resolver

บรรณานุกรม

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

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

[3] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการลงลายมือชื่ออิเล็กทรอนิกส์ 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] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการยืนยันตัวตน เลขที่ ขมธอ. 20-2566, เวอร์ชัน 3.0.

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

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

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