ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ETDA Recommendation on ICT Standard for Electronic Transactions

ขมธอ. 24-2563

ว่าด้วยโครงสร้างข้อมูลของเอกสารรับรองและเอกสารสำแดง

DATA STRUCTURE OF VERIFIABLE CREDENTIALS AND PRESENTATIONS

เวอร์ชัน 1.0

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ICS 35.240.30

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยโครงสร้างข้อมูลของเอกสารรับรองและเอกสารสำแดง

ขมธอ. 24-2563

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

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

ประกาศโดย
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

วันที่ 30 กันยายน พ.ศ. 2563

คณะทำงานจัดทำร่างข้อเสนอแนะมาตรฐานเกี่ยวกับธุรกิจบริการ
ด้านการทำธุรกรรมทางอิเล็กทรอนิกส์

ที่ปรึกษาคณะทำงาน

นายชัยชนะ มิตรพันธ์	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ประธานคณะทำงาน

นายศุภโชค จันทรประทิน	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ผู้ทำงาน

นางสาวสำรวย นุ่มศรี	กรมศุลกากร
นายกำชัย จัตตานนท์	
นายนิรันดร์ ประจวบเหมาะ	กรมสรรพากร
นางสุภิดา บรรเทาทุกข์	
นายคงฤทธิ์ จันทริก	สภาผู้ส่งสินค้าทางเรือแห่งประเทศไทย
นายภาวุธ พงษ์วิทยภานุ	สมาคมผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์ไทย
นายธานินทร์ ตันกิติบุตร	สมาคมผู้ให้บริการอินเทอร์เน็ตไทย
นายวรพจน์ ธาราศิริสกุล	สมาคมฟินเทคประเทศไทย
นายปกรณ์ ลี้สกุล	สมาคมอุตสาหกรรมซอฟต์แวร์ไทย
นางสาวขนิษฐ์ ผาทอง	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายพงษ์พันธ์ ศรีปาน	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ผู้ทำงานและเลขานุการ

นายณัฐฑพัฒน์ โรจนศุภมิตร	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ผู้ช่วยเลขานุการ

นายปัญจพร ทิพย์พิริยพงศ์	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

วิเคราะห์และจัดทำข้อเสนอแนะมาตรฐานฯ
ว่าด้วยโครงสร้างข้อมูลของเอกสารรับรองและเอกสารสำแดง

นายปกรณ์ ลี้สกุล	สมาคมอุตสาหกรรมซอฟต์แวร์ไทย
นายศราวุธ รุ่งเจริญกิจ	สมาคมอุตสาหกรรมซอฟต์แวร์ไทย
นายสัมโมทิก สวิชญาน	สมาคมอุตสาหกรรมซอฟต์แวร์ไทย
นายสุปวีณ์ สุวปรีชาภาส	สมาคมอุตสาหกรรมซอฟต์แวร์ไทย
นายณัฐฑพัฒน์ โรจนศุภมิตร	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายวีรศักดิ์ ดีอ่ำ	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายภูรินทร์ หวังกีรติกานต์	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายวรัชญ์ เฉลิมพรพงศ์	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยโครงสร้างข้อมูลของเอกสารรับรองและเอกสารสำแดงฉบับนี้ จัดทำขึ้นเพื่อกำหนดโครงสร้างข้อมูลสำหรับเอกสารรับรอง (verifiable credential: VC) และเอกสารสำแดง (verifiable presentation: VP) ซึ่งสามารถตรวจสอบที่มาและความถูกต้องครบถ้วนของข้อมูล รวมถึงอธิบายความเชื่อมโยงในการใช้งาน VC และ VP ระหว่างเอนทิตีที่เกี่ยวข้อง ซึ่งประกอบด้วยผู้ออกเอกสาร (issuer) ผู้ถือเอกสาร (holder) และผู้ตรวจสอบเอกสาร (verifier) โดยผู้ถือเอกสารสามารถใช้ VC และ VP ในการพิสูจน์และยืนยันตัวตน การให้ความยินยอม การมอบอำนาจ หรือการแสดงข้อมูลที่ถูกรับรองแก่ผู้อื่น ในรูปแบบอิเล็กทรอนิกส์ที่มีความมั่นคงปลอดภัย มีการรักษาความเป็นส่วนตัว สามารถตรวจสอบได้ด้วยกระบวนการเข้ารหัสลับ และสนับสนุนการแลกเปลี่ยนระหว่างกันตามมาตรฐานสากล โดยข้อเสนอแนะมาตรฐานฉบับนี้อ้างอิงมาตรฐาน Verifiable Credentials Data Model ของ World Wide Web Consortium (W3C) [1]

ข้อเสนอแนะมาตรฐานฉบับนี้มีการนำเสนอและรับฟังความคิดเห็นเป็นการทั่วไป ตลอดจนพิจารณาข้อมูล ข้อสังเกต ข้อคิดเห็นจากผู้ทรงคุณวุฒิและหน่วยงานที่เกี่ยวข้อง เพื่อปรับปรุงให้ข้อเสนอแนะมาตรฐานฉบับนี้มีความสมบูรณ์ครบถ้วนยิ่งขึ้น รวมทั้งให้สามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพ

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยโครงสร้างข้อมูลของเอกสารรับรองและเอกสารสำแดงฉบับนี้ จัดทำขึ้นโดยสำนักมาตรฐาน สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

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

คำนำ

เอกสารรับรอง (verifiable credential: VC) และเอกสารสำแดง (verifiable presentation: VP) สามารถนำไปใช้เป็นเอกสารอิเล็กทรอนิกส์ ตัวอย่างเช่น หนังสือให้ความยินยอม หนังสือมอบอำนาจ ใบปริญญาบัตรที่มหาวิทยาลัยออกให้แก่นักศึกษา หรือใบรับรองแพทย์ที่แพทย์ออกให้แก่ผู้ป่วย โดย VC และ VP จะมีคุณสมบัติที่สามารถตรวจสอบความถูกต้องครบถ้วนของข้อมูล และตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ของผู้ออกเอกสารและผู้ถือเอกสารได้ด้วยกระบวนการเข้ารหัสลับ

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์เห็นถึงประโยชน์จากการใช้งาน VC และ VP จึงจัดทำมาตรฐานโครงสร้างข้อมูลของเอกสารรับรองและเอกสารสำแดง โดยผู้ถือเอกสารสามารถใช้ VC และ VP ในการพิสูจน์และยืนยันตัวตน การให้ความยินยอม การมอบอำนาจ หรือการแสดงข้อมูลที่ถูกรับรองแก่ผู้อื่น ในรูปแบบอิเล็กทรอนิกส์ที่มีความมั่นคงปลอดภัย มีการรักษาความเป็นส่วนตัว สามารถตรวจสอบได้ด้วยกระบวนการเข้ารหัสลับ และสนับสนุนการแลกเปลี่ยนระหว่างเอนทิตีที่เกี่ยวข้องตามมาตรฐานสากล ซึ่งประกอบด้วยผู้ออกเอกสาร ผู้ถือเอกสาร และผู้ตรวจสอบเอกสาร

สารบัญ

สารบัญรูป

หน้า

สารบัญตาราง

หน้า

ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
เรื่อง ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์
ว่าด้วยโครงสร้างข้อมูลของเอกสารรับรองและเอกสารสำแดง

โดยที่เป็นการสมควรกำหนดโครงสร้างข้อมูลสำหรับเอกสารรับรอง (verifiable credential: VC) และเอกสารสำแดง (verifiable presentation: VP) ซึ่งสามารถตรวจสอบที่มาและความถูกต้องครบถ้วนของข้อมูล รวมถึงอธิบายความเชื่อมโยงในการใช้งาน VC และ VP ระหว่างเอนทิตีที่เกี่ยวข้อง ซึ่งประกอบด้วย ผู้ออกเอกสาร (issuer) ผู้ถือเอกสาร (holder) และผู้ตรวจสอบเอกสาร (verifier) เพื่อให้ผู้ถือเอกสารสามารถใช้ VC และ VP ในการพิสูจน์และยืนยันตัวตน การให้ความยินยอม การมอบอำนาจ หรือการแสดงข้อมูลที่ถูกรับรองแก่ผู้อื่น ในรูปแบบอิเล็กทรอนิกส์ที่มีความมั่นคงปลอดภัย มีการรักษาความเป็นส่วนตัว สามารถตรวจสอบได้ด้วยกระบวนการเข้ารหัสลับ และสนับสนุนการแลกเปลี่ยนระหว่างกันตามมาตรฐานสากล

อาศัยอำนาจตามความในมาตรา ๕ แห่งพระราชบัญญัติสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๒ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ จึงประกาศข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยโครงสร้างข้อมูลของเอกสารรับรองและเอกสารสำแดง เลขที่ ขมธอ. ๒๔-๒๕๖๓ ปรากฏตามท้ายประกาศฉบับนี้

ประกาศ ณ วันที่ ๓๐ กันยายน พ.ศ. ๒๕๖๓

(นายชัยชนะ มิตรพันธ์)
ผู้อำนวยการ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ว่าด้วยโครงสร้างข้อมูลของเอกสารรับรองและเอกสารสำแดง

1. ขอบข่าย

ข้อเสนอแนะมาตรฐานฉบับนี้ กำหนดโครงสร้างข้อมูลสำหรับเอกสารรับรอง (verifiable credential: VC) และเอกสารสำแดง (verifiable presentation: VP) ซึ่งสามารถตรวจสอบที่มาและความถูกต้องครบถ้วนของข้อมูล รวมถึงอธิบายความเชื่อมโยงในการใช้งาน VC และ VP ระหว่างเอนทิตีที่เกี่ยวข้อง ซึ่งประกอบด้วยผู้ออกเอกสาร (issuer) ผู้ถือเอกสาร (holder) และผู้ตรวจสอบเอกสาร (verifier) เพื่อให้ผู้ถือเอกสารสามารถใช้ VC และ VP ในการพิสูจน์และยืนยันตัวตน การให้ความยินยอม การมอบอำนาจ หรือการแสดงข้อมูลที่ถูกรับรองแก่ผู้อื่น ในรูปแบบอิเล็กทรอนิกส์ที่มีความมั่นคงปลอดภัย มีการรักษาความเป็นส่วนตัว สามารถตรวจสอบได้ด้วยกระบวนการเข้ารหัสลับ และสนับสนุนการแลกเปลี่ยนระหว่างกันตามมาตรฐานสากล

ข้อเสนอแนะมาตรฐานฉบับนี้จะแสดงตัวอย่างของโครงสร้างข้อมูลในรูปแบบ JSON (JavaScript Object Notation) และ JSON-LD (JavaScript Object Notation for Linked Data) อย่างไรก็ตาม โครงสร้างข้อมูลของ VC และ VP สามารถแสดงด้วยวากยสัมพันธ์ (syntax) รูปแบบอื่น ๆ ได้ เช่น XML (Extensible Markup Language)

ในข้อเสนอแนะมาตรฐานฉบับนี้ รูปแบบของคำที่ใช้แสดงออกถึงคุณลักษณะของเนื้อหาเชิงบรรทัดฐาน (normative) และเนื้อหาเชิงให้ข้อมูล (informative) มีดังต่อไปนี้

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

2. บทนิยาม

ความหมายของคำที่ใช้ในข้อเสนอแนะมาตรฐานฉบับนี้ มีดังต่อไปนี้

2.1 เจ้าของข้อความ (subject) หมายถึง เอนทิตีที่ถูกกล่าวอ้างถึงในข้อความยืนยัน (claim)

2.2 ข้อความยืนยัน (claim) หมายถึง ข้อความเกี่ยวกับเจ้าของข้อความ (subject) ที่จะถูกรับรองโดยผู้ออกเอกสาร (issuer)

2.3 เอกสารรับรอง (verifiable credential: VC) หมายถึง ชุดของข้อความยืนยันอย่างน้อยหนึ่งรายการที่ถูกรับรองโดยผู้ออกเอกสาร (issuer) ทั้งนี้ VC มีคุณสมบัติที่สามารถตรวจพบการเปลี่ยนแปลงใด ๆ ที่เกิดกับความถูกต้องครบถ้วนของข้อมูล และตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ของผู้ออกเอกสารได้ด้วยกระบวนการเข้ารหัสลับ

ข้อสังเกต: ข้อความยืนยันใน VC อาจเกี่ยวกับเจ้าของข้อความ (subject) ที่มากกว่าหนึ่งราย เช่น ข้อความยืนยันในทะเบียนสมรส

2.4 เอกสารสำแดง (verifiable presentation: VP) หมายถึง VC อย่างน้อยหนึ่งชุด ที่ผู้ถือเอกสาร (holder) ใช้แสดงต่อผู้ตรวจสอบเอกสาร (verifier) ทั้งนี้ VP มีคุณสมบัติที่สามารถตรวจพบการเปลี่ยนแปลงใด ๆ ที่เกิดกับความถูกต้องครบถ้วนของข้อมูล และตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ของผู้ถือเอกสารและตรวจสอบ VC ที่เกี่ยวข้องได้ด้วยกระบวนการเข้ารหัสลับ

2.5 เอนทิตี (entity) หมายถึง สิ่งที่มีอยู่จริง เช่น บุคคล องค์กร หรืออุปกรณ์ ซึ่งถูกกล่าวอ้างในการใช้งาน VC และ VP

2.6 ผู้ออกเอกสาร (issuer) หมายถึง เอนทิตีที่ทำหน้าที่รับรองข้อความยืนยันโดยออกเป็น VC ให้แก่ผู้ถือเอกสาร

2.7 ผู้ถือเอกสาร (holder) หมายถึง เอนทิตีที่เป็นเจ้าของ VC อย่างน้อยหนึ่งชุด โดยจัดเก็บไว้ในกระเป๋าดิจิทัล (credential wallet) และสามารถใช้ VC สร้างเป็น VP

2.8 ผู้ตรวจสอบเอกสาร (verifier) หมายถึง เอนทิตีที่สามารถตรวจสอบความถูกต้องครบถ้วนของ VC และ VP ด้วยกระบวนการเข้ารหัสลับ รวมถึงตรวจสอบสถานะการใช้งานและความสอดคล้องตามโครงสร้างข้อมูลของ VC และ VP

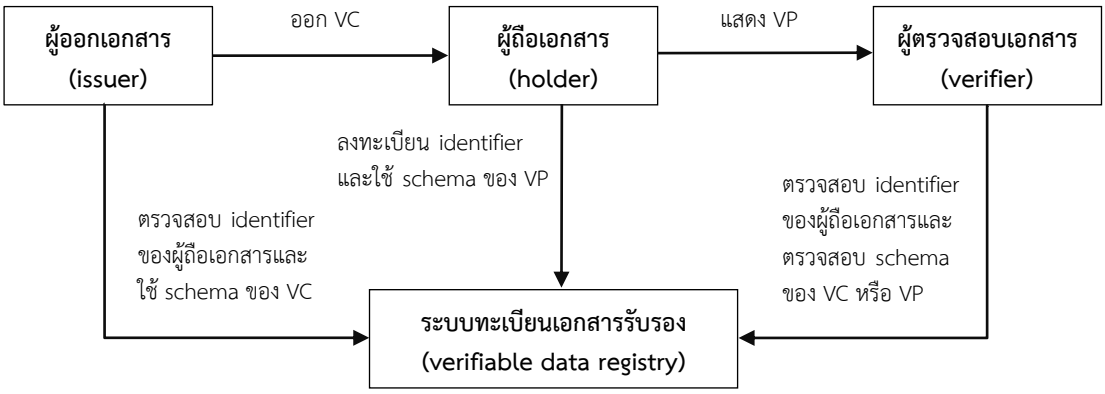
2.9 ระบบทะเบียนเอกสารรับรอง (verifiable data registry) หมายถึง ระบบที่ช่วยสนับสนุนการสร้างและการตรวจสอบความถูกต้องครบถ้วนของ VC และ VP โดยข้อมูลที่มีการจัดเก็บในระบบนี้ เช่น ตัวระบุ (identifier) และกุญแจสาธารณะ (public key) ของเอนทิตีที่เกี่ยวข้อง รวมถึงรายการเพิกถอน (revocation list) และเค้าร่าง (schema)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

2.10 กระเป๋าดิจิทัล (credential wallet หรือ credential repository) หมายถึง โปรแกรมที่จัดเก็บและช่วยให้ผู้ถือเอกสารสามารถเข้าถึงและใช้งาน VC ได้อย่างมั่นคงปลอดภัย

3. ภาพรวมของ VC และ VP

3.1 การใช้งาน VC และ VP

ระบบที่มีการใช้งาน VC และ VP จะประกอบด้วยความเชื่อมโยงระหว่างเอนทิตีที่เกี่ยวข้อง ตามรูปที่ 1 (ตัวอย่างกรณีศึกษาการใช้งาน VC และ VP สามารถดูในภาคผนวก ค.) ซึ่งมีรายละเอียดดังต่อไปนี้



รูปที่ 1 ความเชื่อมโยงในการใช้งาน VC และ VP ระหว่างเอนทิตีที่เกี่ยวข้อง

จากรูปที่ 1 ผู้ออกเอกสาร (issuer) ออกเอกสารรับรอง (VC) ให้แก่ผู้ถือเอกสาร (holder) จัดเก็บไว้ในกระเป๋าดิจิทัลและสามารถนำ VC สร้างเป็น VP เพื่อส่งให้กับผู้ตรวจสอบเอกสาร (verifier) ได้ ทั้งนี้การเชื่อมโยงการทำงานของผู้เกี่ยวข้องข้างต้นจำเป็นต้องมีระบบทะเบียนเอกสารรับรอง

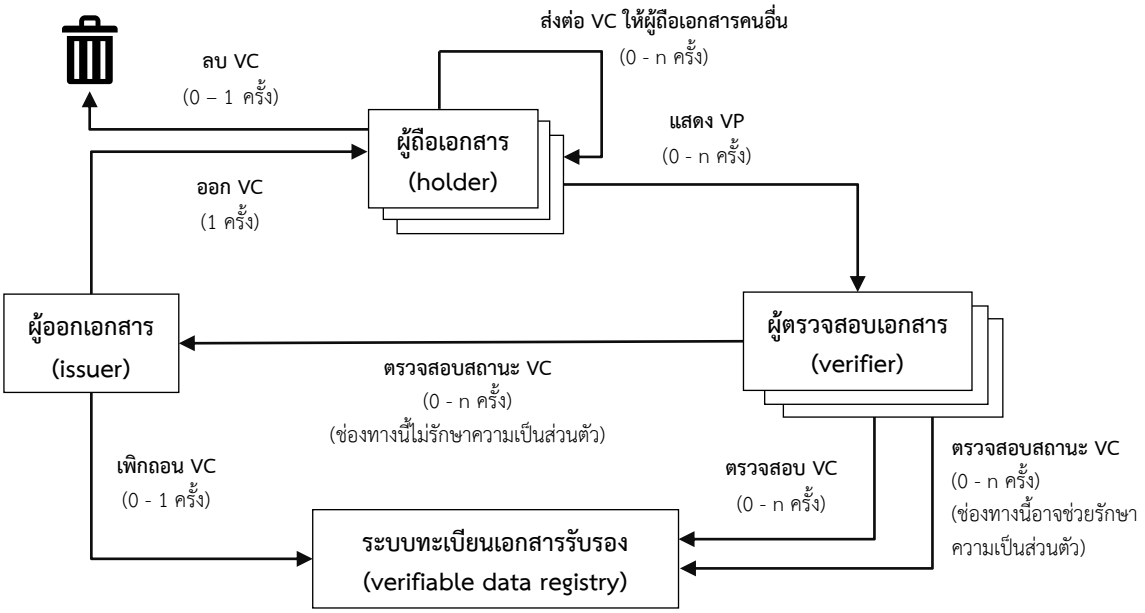
ระบบทะเบียนเอกสารรับรอง (verifiable data registry) คือ ระบบที่ช่วยสนับสนุนการสร้างและการตรวจสอบความถูกต้องครบถ้วนของ VC และ VP โดยข้อมูลที่มีการจัดเก็บในระบบนี้ เช่น

- ตัวระบุ (identifier) ของ VC หรือ VP ผู้ออกเอกสาร ผู้ถือเอกสาร หรือผู้ตรวจสอบเอกสาร
- กุญแจสาธารณะ (public key) ของผู้ออกเอกสาร ผู้ถือเอกสาร หรือผู้ตรวจสอบเอกสาร
- รายการเพิกถอน (revocation list) ของ VC หรือ VP
- เค้าร่าง (schema) ของ VC หรือ VP

หลักการที่สำคัญของการใช้งาน VC และ VP ควรมีดังต่อไปนี้ [2]

(1) ผู้ถือเอกสารสามารถควบคุมและเข้าถึงข้อความยืนยันใน VC ของตนเองได้
(2) หากเป็นไปได้ การนำข้อความยืนยันของเจ้าของข้อความไปใช้งานควรได้รับความยินยอมจากเจ้าของข้อความ
(3) รองรับการเปิดเผยข้อความยืนยันเท่าที่จำเป็น (minimization)
(4) ระบบและอัลกอริทึมในการใช้งาน VC และ VP ต้องมีความโปร่งใส (transparency)
(5) รองรับการย้าย VC จากกระเป๋าดิจิทัลเดิมไปยังกระเป๋าดิจิทัลใหม่ได้ (portability)

ทั้งนี้ กิจกรรมที่แต่ละเอนทิตีดำเนินการต่อ VC และ VP สามารถแสดงเป็นแผนภาพตามรูปที่ 2



รูปที่ 2 แผนภาพการใช้งาน VC และ VP

(1) ผู้ออกเอกสารออก VC ให้แก่ผู้ถือเอกสาร ซึ่งกิจกรรมนี้จะเกิดขึ้นก่อนกิจกรรมอื่น ๆ
(2) ผู้ถือเอกสารอาจถือไว้หรือส่งต่อ VC ให้แก่ผู้ถือเอกสารคนอื่นมากกว่าหนึ่งคนได้ (0 - n ครั้ง)
(3) ผู้ถือเอกสารอาจใช้ VC สร้างเป็น VP และแสดง VP ให้แก่ผู้ตรวจสอบเอกสารมากกว่าหนึ่งเอนทิตีได้ (0 - n ครั้ง)

(4) ผู้ตรวจสอบเอกสารอาจตรวจสอบความถูกต้องของ VC และ VP กับระบบทะเบียนเอกสารรับรอง (0 - n ครั้ง) และอาจตรวจสอบสถานะการเพิกถอนของ VC นั้นด้วย (0 - n ครั้ง)

(5) ผู้ออกเอกสารอาจเพิกถอน VC (0 - 1 ครั้ง)

(6) ผู้ถือเอกสารอาจลบ VC ออกจากกระเป๋าดิจิทัล (0 - 1 ครั้ง)

อย่างไรก็ตาม กิจกรรมข้อ (2) – (6) ไม่จำเป็นต้องเกิดขึ้นตามลำดับ และอาจเกิดขึ้นมากกว่าหนึ่งครั้ง โดยอาจเกิดขึ้นทันทีหรือในภายหลัง

3.2 ข้อกำหนดการใช้งาน VC และ VP

ข้อกำหนดของผู้ออกเอกสาร (issuer)

(1) ผู้ออกเอกสารสามารถออก VC ให้แก่เจ้าของข้อความ (subject) คนใดก็ได้

(2) VC ใช้แสดงข้อความที่สร้างขึ้นโดยผู้ออกเอกสารในรูปแบบที่สามารถตรวจพบการเปลี่ยนแปลงใด ๆ ที่เกิดกับความถูกต้องครบถ้วนของข้อมูล

(3) ผู้ออกเอกสารสามารถออก VC ที่สามารถเพิกถอนในภายหลังได้

(4) ในการเพิกถอน VC ผู้ออกเอกสารไม่ควรเปิดเผยข้อมูลที่สามารถระบุตัวบุคคลของเจ้าของข้อความ ผู้ถือเอกสาร ผู้ตรวจสอบเอกสาร หรือ VC อันใดอันหนึ่ง

(5) ผู้ออกเอกสารสามารถเปิดเผยเหตุผลในการเพิกถอน VC

(6) ในการเพิกถอน VC ผู้ออกเอกสารควรระบุเหตุผลในการเพิกถอนว่าเกิดจากปัญหาด้านความสมบูรณ์ของการเข้ารหัสลับ (cryptographic integrity) หรือเกิดจากการเปลี่ยนสถานะของ VC

ข้อกำหนดของผู้ถือเอกสาร (holder)

(1) ผู้ถือเอกสารสามารถรับ VC จากผู้ออกเอกสารหรือผู้ถือเอกสารคนอื่นได้ ทั้งนี้ ในบางกรณี ผู้ถือเอกสารอาจไม่ใช่เจ้าของข้อความ เช่น ผู้ปกครอง (ผู้ถือเอกสาร) อาจถือครอง VC ของบุตร (เจ้าของข้อความ)

(2) รายละเอียดการจัดเก็บและการใช้งาน VC และ VP เช่น การใช้กับใคร ที่ไหน เมื่อไหร่ อย่างไร เป็นข้อมูลส่วนบุคคลของผู้ถือเอกสาร ไม่จำเป็นต้องแจ้งให้ผู้ออกเอกสารทราบ

(3) ผู้ถือเอกสารสามารถใช้งาน VC ผ่านโปรแกรมที่อำนวยความสะดวกในการติดต่อ (user agent) กับผู้ออกเอกสารและผู้ตรวจสอบเอกสาร เช่น web application หรือ mobile application

(4) ผู้ถือเอกสารสามารถสร้าง VP โดยใช้ VC มากกว่าหนึ่งชุดซึ่งออกโดยผู้ออกเอกสารที่แตกต่างกัน

(5) การแสดง VP ต่อผู้ตรวจสอบเอกสาร ของผู้ถือเอกสารจะไม่ส่งผลกระทบต่อความถูกต้องแท้จริงของข้อความยืนยันซึ่งถูกรับรองโดยผู้ออกเอกสาร

ข้อกำหนดของผู้ตรวจสอบเอกสาร (verifier)

(1) ผู้ตรวจสอบเอกสารสามารถตรวจสอบความยินยอมในการแสดง VP จากผู้ถือเอกสารได้

(2) ผู้ตรวจสอบเอกสารสามารถตรวจสอบความถูกต้องแท้จริงของ VC ซึ่งถูกรับรองโดยผู้ออกเอกสารได้

(3) ผู้ตรวจสอบเอกสารสามารถตรวจสอบ VC และ VP ได้ โดยไม่จำเป็นต้องพึ่งพาผู้ออกเอกสาร และไม่จำเป็นต้องเปิดเผยรายละเอียดการตรวจสอบให้แก่ผู้ออกเอกสาร

ข้อกำหนดของระบบทะเบียนเอกสารรับรอง (verifiable data registry)

(1) ระบบทะเบียนเอกสารรับรองทำหน้าที่บริหารจัดการความน่าเชื่อถือของระบบด้วยการจัดเก็บข้อมูลที่เชื่อมโยงไปยังแต่ละเอนทิตี โดยสามารถตรวจพบการเปลี่ยนแปลงใด ๆ ที่เกิดกับความถูกต้องครบถ้วนของข้อมูลนั้นได้

(2) ระบบทะเบียนเอกสารรับรองมีการจัดเก็บ schema ของ VC และ VP สำหรับนำไปใช้งานในกรณีดังต่อไปนี้

(2.1) ผู้ออกเอกสารใช้ schema ในการสร้าง VC

(2.2) ผู้ถือเอกสารใช้ schema ในการสร้าง VP

(2.3) ผู้ตรวจสอบเอกสารใช้ schema ในการตรวจสอบโครงสร้างข้อมูลของ VC หรือ VP

(3) ระบบทะเบียนเอกสารรับรองมีการจัดเก็บรายการเพิกถอน เพื่อให้ผู้ตรวจสอบเอกสารสามารถตรวจสอบสถานะการใช้งานของ VC หรือ VP ได้

(4) ระบบทะเบียนเอกสารรับรองอาจเป็นฐานข้อมูลแบบรวมศูนย์หรือฐานข้อมูลแบบกระจายศูนย์ก็ได้ ทั้งนี้ในบางกรณี ระบบทะเบียนเอกสารรับรองอาจมีมากกว่าหนึ่งระบบ โดยทำหน้าที่แตกต่างกันเพื่อสนับสนุนการใช้งาน VC และ VP เช่น ระบบหนึ่งทำหน้าที่จัดเก็บ schema ในขณะที่อีกระบบหนึ่งทำหน้าที่จัดเก็บรายการเพิกถอน

3.3 รูปแบบความไว้วางใจ (trust model)

รูปแบบความไว้วางใจของการใช้งาน VC และ VP อาศัยความสัมพันธ์หรือความไว้วางใจกันระหว่างเอนทิตีตามรูปที่ 3

(1) ผู้ตรวจสอบเอกสารเชื่อถือผู้ออกเอกสารในการออก VC ซึ่งอาศัยกระบวนการเข้ารหัสลับที่ตรวจสอบได้ว่าผู้ออกเอกสารสร้าง VC ดังกล่าวจริง

(2) ผู้ถือเอกสารและผู้ตรวจสอบเอกสารเชื่อถือว่า ผู้ออกเอกสารสามารถออก VC ที่มีความถูกต้องแท้จริงเกี่ยวกับเจ้าของข้อความ และสามารถเพิกถอน VC ในภายหลังอย่างเหมาะสม

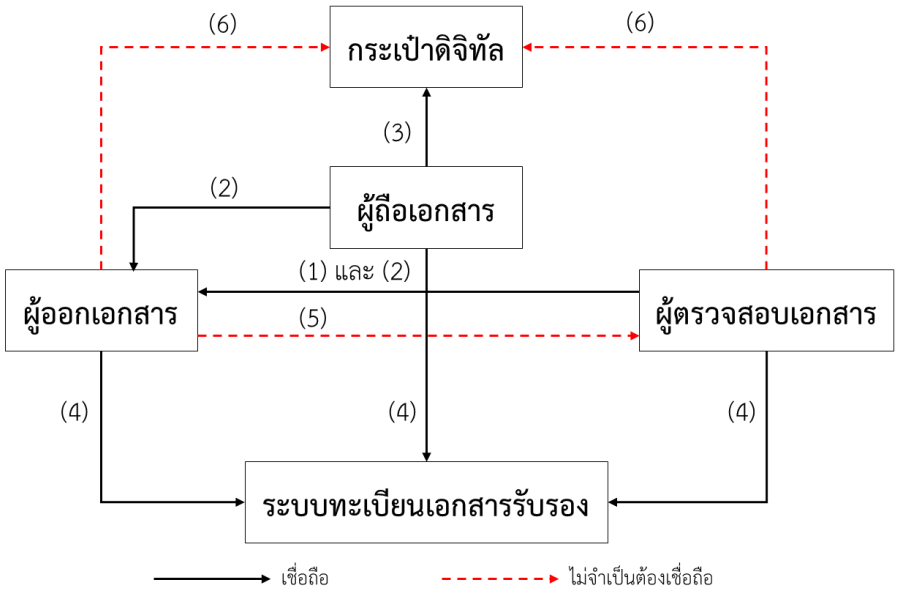
(3) ผู้ถือเอกสารเชื่อถือกระเป๋าดิจิทัลว่ามีการจัดเก็บ VC อย่างมั่นคงปลอดภัย ไม่เปิดเผย VC แก่บุคคลอื่นและไม่ทำให้ VC เปลี่ยนแปลงหรือสูญหายขณะที่จัดเก็บอยู่ในกระเป๋าดิจิทัล

(4) เอนทิตีทั้งหมดเชื่อถือระบบทะเบียนเอกสารรับรองว่ามีการจัดเก็บข้อมูลที่เชื่อมโยงไปยังแต่ละเอนทิตีอย่างถูกต้องและสามารถตรวจพบการเปลี่ยนแปลงของข้อมูลที่จัดเก็บได้

รูปแบบความไว้วางใจของการใช้งาน VC และ VP แตกต่างจากรูปแบบความไว้วางใจทั่วไปที่อาศัยการติดต่อโดยตรงระหว่างผู้ออกเอกสารและผู้ตรวจสอบเอกสาร กล่าวคือ

(5) ผู้ออกเอกสารไม่จำเป็นต้องรู้จักหรือเชื่อถือผู้ตรวจสอบเอกสาร

(6) ผู้ออกเอกสารและผู้ตรวจสอบเอกสารไม่จำเป็นต้องเชื่อถือกระเป๋าดิจิทัลที่จัดเก็บ VC

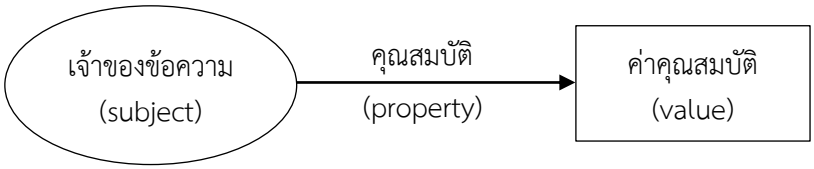


รูปที่ 3 รูปแบบความไว้วางใจในการใช้งาน VC และ VP ระหว่างเอนทิตี

3.4 แบบจำลองข้อมูลของ VC และ VP

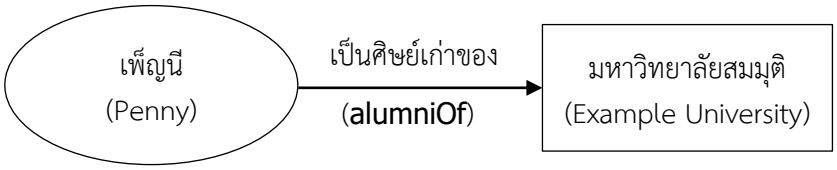
3.4.1 ข้อความยืนยัน (claim)

ข้อความยืนยัน (claim) คือ ข้อความเกี่ยวกับเจ้าของข้อความ โดยแบบจำลองข้อมูลของข้อความยืนยันสามารถแสดงด้วยความสัมพันธ์ในรูปแบบ เจ้าของข้อความ (subject) – คุณสมบัติ (property) – ค่าคุณสมบัติ (value) ตามรูปที่ 4



รูปที่ 4 แบบจำลองข้อมูลของข้อความยืนยัน

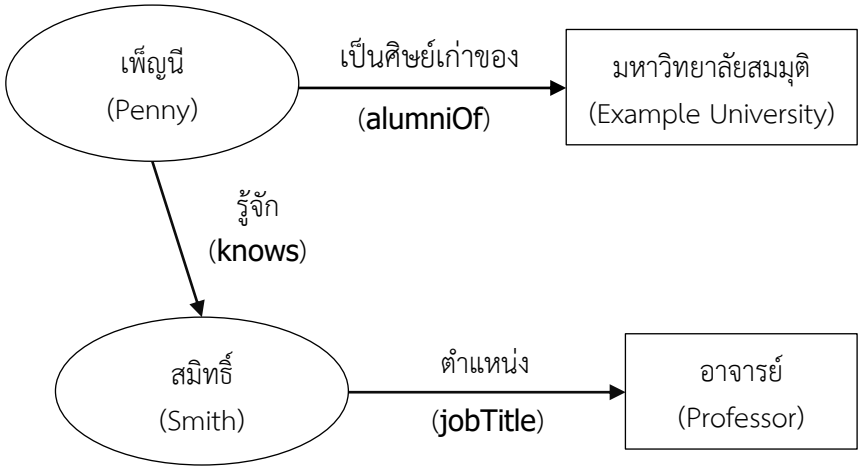
ตัวอย่างของข้อความยืนยันแสดงข้อความ “เพ็ญนีเป็นศิษย์เก่าของมหาวิทยาลัยสมมุติ” (“Penny is an alumna of Example University.”) สามารถแสดงตามแบบจำลองข้างต้นได้ตามรูปที่ 5



รูปที่ 5 ข้อความยืนยันแสดงข้อความ “เพ็ญนีเป็นศิษย์เก่าของมหาวิทยาลัยสมมุติ”

ทั้งนี้ ข้อความยืนยันสามารถนำมาเชื่อมโยงกันเป็นกราฟ (graph) สำหรับใช้แสดงความสัมพันธ์ของข้อมูลต่าง ๆ กับเจ้าของข้อความ ตัวอย่างเช่น การเชื่อมโยงข้อความยืนยันก่อนหน้าในรูปที่ 5 กับ

ข้อความยืนยันที่แสดงข้อความ “เพ็ญนีรู้จักสมิทธิ์” (“Penny knows Smith.”) และ “สมิทธิ์มีตำแหน่งเป็นอาจารย์” (“Smith is a professor.”) ตามรูปที่ 6

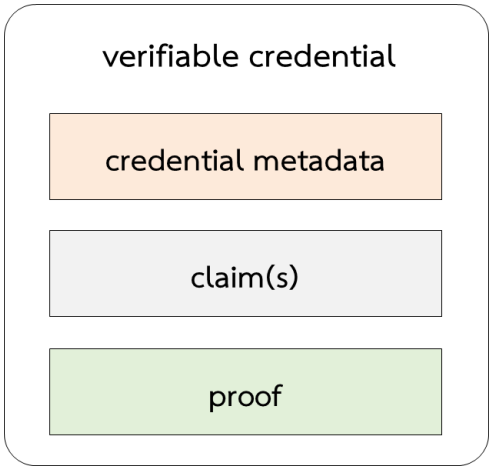


รูปที่ 6 การเชื่อมโยงกันระหว่างข้อความยืนยันเพื่อสร้างเป็นกราฟข้อมูล

3.4.2 เอกสารรับรอง (VC)

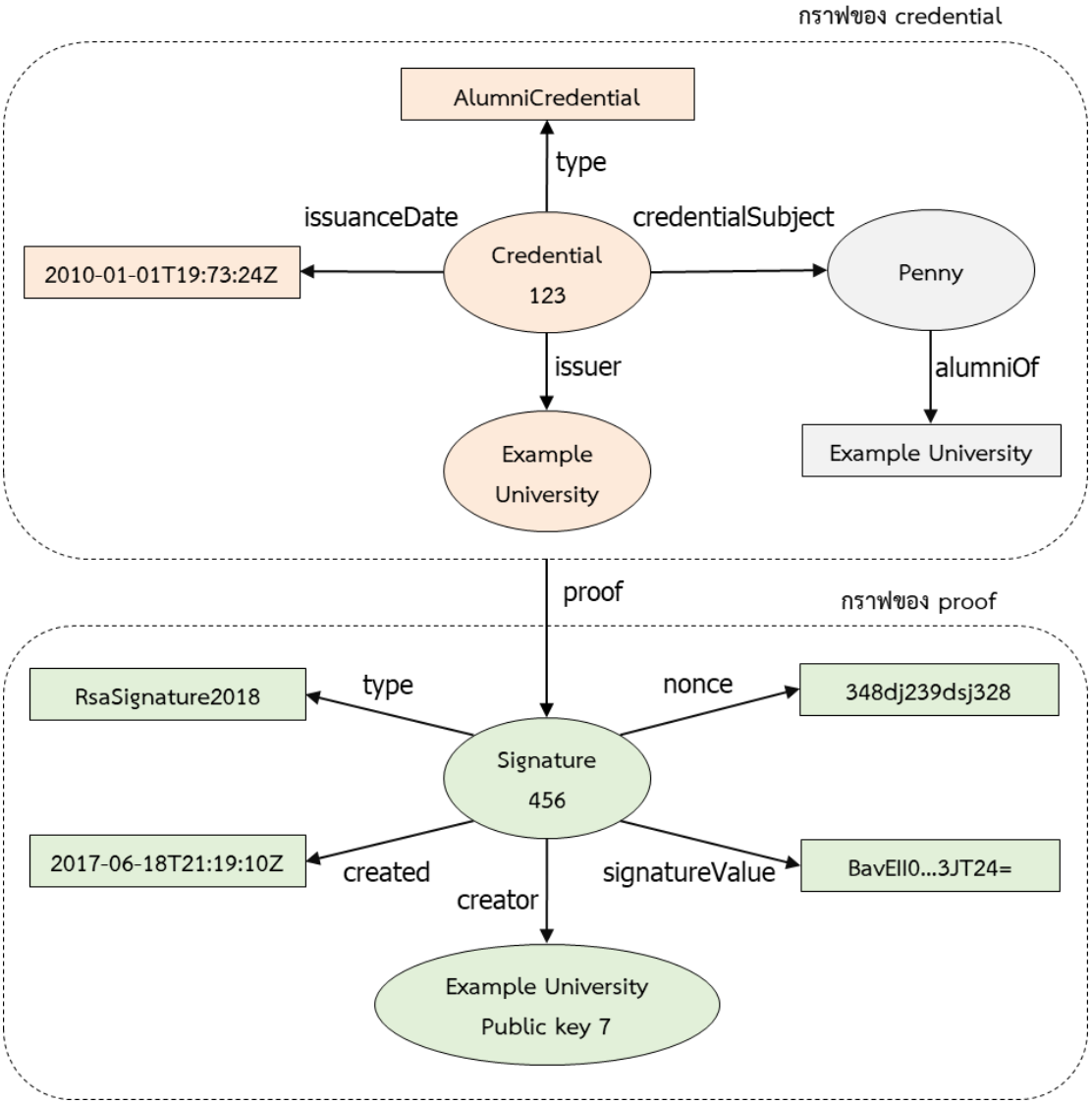
VC คือ ชุดของข้อความยืนยันอย่างน้อยหนึ่งรายการที่ถูกรับรองโดยผู้ออกเอกสาร ทั้งนี้ VC มีคุณสมบัติที่สามารถสามารถตรวจพบการเปลี่ยนแปลงใด ๆ ที่เกิดกับความถูกต้องครบถ้วนของข้อมูล และตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ของผู้ออกเอกสารได้ด้วยกระบวนการเข้ารหัสลับ VC อาจประกอบด้วย identifier และคำอธิบายข้อมูล (metadata) เช่น ผู้ออกเอกสาร วันและเวลาเมื่อ VC เริ่มมีผลผูกพันและสิ้นผลผูกพัน

ทั้งนี้ องค์ประกอบพื้นฐานของ VC สามารถแสดงตามรูปที่ 7 ซึ่งประกอบด้วย 3 ส่วน ได้แก่ (1) คำอธิบายข้อมูลของ VC (credential metadata) (2) ข้อความยืนยัน (claim) และ (3) ข้อพิสูจน์ (proof) ซึ่งโดยทั่วไปจะเป็นลายมือชื่อดิจิทัลของผู้ออกเอกสาร



รูปที่ 7 องค์ประกอบพื้นฐานของ VC

นอกจากนี้ VC สามารถแสดงเป็นกราฟข้อมูลได้ตามรูปที่ 8



รูปที่ 8 กราฟข้อมูลของ VC

ตัวอย่างกรณีศึกษาของ VC แสดงกรณีศึกษาเมื่อเพ็ญนีไปซื้อสินค้าจากร้านสหกรณ์มหาวิทยาลัยสมมุติ โดยจะได้รับส่วนลดเมื่อเพ็ญนีพิสูจน์ได้ว่าตนเองเคยศึกษา ณ มหาวิทยาลัยดังกล่าว ซึ่งทางมหาวิทยาลัยได้ออก VC เพื่อรับรองความเป็นศิษย์เก่าให้แก่เพ็ญนี และเพ็ญนีจัดเก็บ VC นั้นไว้ในกระเป๋าดิจิทัลของตนเอง ตัวอย่างของ VC ข้างต้นในรูปแบบ JSON-LD แสดงตามตัวอย่างที่ 1

หมายเหตุ: ข้อเสนอแนะมาตรฐานฉบับนี้ จะใช้รูปแบบอักขระ Tahoma สำหรับแสดงคุณสมบัติ (property) และค่าคุณสมบัติ (property value)

ตัวอย่างที่ 1 ตัวอย่างของ VC ในรูปแบบ JSON-LD

```
{
 // @context ซึ่งประกาศนิยามของสมนาม (alias) เช่น issuer และ alumniOf
 "@context": [
   "https://www.w3.org/2018/credentials/v1",
   "https://www.w3.org/2018/credentials/examples/v1"
 ],
```

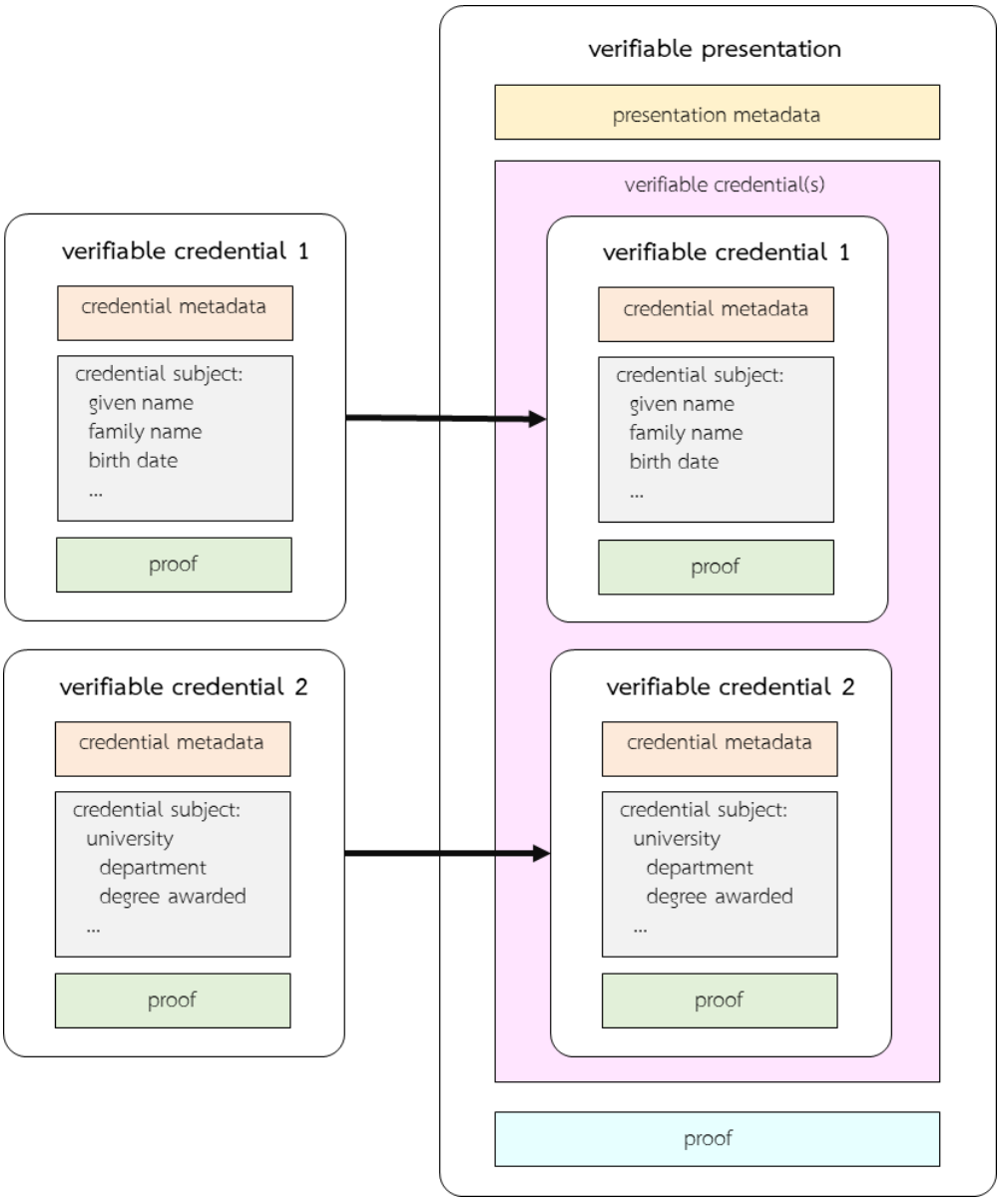
```
 "id": "http://example.edu/credentials/1872",              // id ของเอกสาร
 "type": ["VerifiableCredential", "AlumniCredential"],    // ประเภทของเอกสาร
 "issuer": "https://example.edu/issuers/565049",          // ผู้ออกเอกสาร
 "issuanceDate": "2010-01-01T19:73:24Z",                  // วันและเวลาเมื่อ VC เริ่มมีผลผูกพัน
 // เจ้าของข้อความใน VC  โดยในกรณีนี้มีเพียงเอนทิตีเดียว
 "credentialSubject": {
  // id ของเจ้าของข้อความ โดยในกรณีนี้ใช้ DID [1]
  "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
  // ข้อความยืนยันเกี่ยวกับเจ้าของข้อความ
   "alumniOf": {
    "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",
    "name": [{
     "value": "Example University",
     "lang": "en"
    }, {
     "value": "มหาวิทยาลัยสมมุติ",
     "lang": "th"
    }]
   }
 },
 // ลายมือชื่อดิจิทัล ซึ่งช่วยให้สามารถตรวจพบการเปลี่ยนแปลงของ VC
 "proof": {
  // กระบวนการเข้ารหัสลับที่ใช้ในการลงลายมือชื่อ
   "type": "RsaSignature2018",
  // วันที่ลงลายมือชื่อ
   "created": "2017-06-18T21:19:10Z",
  // วัตถุประสงค์ของการลงลายมือชื่อ
   "proofPurpose": "assertionMethod",
  // id ของกุญแจสาธารณะที่ใช้ในการตรวจสอบลายมือชื่อ
   "verificationMethod": "https://example.edu/issuers/keys/1",

  // ค่าของลายมือชื่อดิจิทัล
   "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..TCYt5XsITJX
     1CxPCT8yAV-TVkIEq_PbChOMqsLfRoPsnsgw5WEuts01mq-pQy7UJiN5mgRxD-WUcX
     16dUEMGlv50aqzpqh4Qktb3rk-BuQy72IFLOqV0G_zS245-kronKb78cPN25DGlcTwLtjP
     AYuNzVBAh4vGHSrQyHUdBBPM"
  }
}
```

[1] decentralized identifier (DID) เป็น identifier บนระบบทะเบียนเอกสารรับรอง (verifiable data registry) แบบกระจายศูนย์ที่ใช้ URL ในการเชื่อมโยงกับเอนทิตี โดยทั่วไป DID จะนำมาใช้ใน VC เพื่อแสดงความเชื่อมโยงไปยังเจ้าของข้อความ ซึ่งทำให้สามารถส่งต่อหรือโอนย้าย VC จากกระเป๋าดิจิทัลหนึ่งไปยังกระเป๋าดิจิทัลอีกอันหนึ่งได้โดยไม่จำเป็นต้องออก VC ชุดใหม่ อย่างไรก็ตาม VC ไม่จำเป็นต้องใช้ identifier เป็น DID ก็ได้

3.4.3 เอกสารสำแดง (VP)

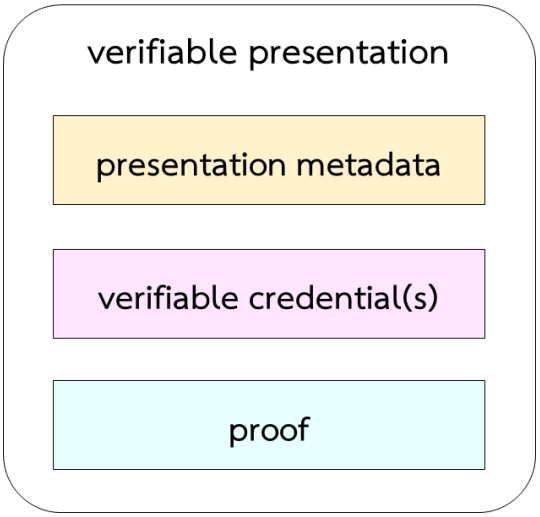
VP คือ ข้อมูลที่ประกอบด้วย VC อย่างน้อยหนึ่งชุด ซึ่งอาจเป็นข้อมูลต้นฉบับตามที่ปรากฏใน VC หรือเป็นข้อมูลที่สังเคราะห์จาก VC ก็ได้ โดย VP จะมีคุณสมบัติที่สามารถตรวจพบการเปลี่ยนแปลงใด ๆ ที่เกิดกับความถูกต้องครบถ้วนของข้อมูล และตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ของผู้ถือเอกสารและตรวจสอบ VC ที่เกี่ยวข้องได้ด้วยกระบวนการเข้ารหัสลับ



รูปที่ 9 ตัวอย่างความสัมพันธ์ระหว่าง VC และ VP

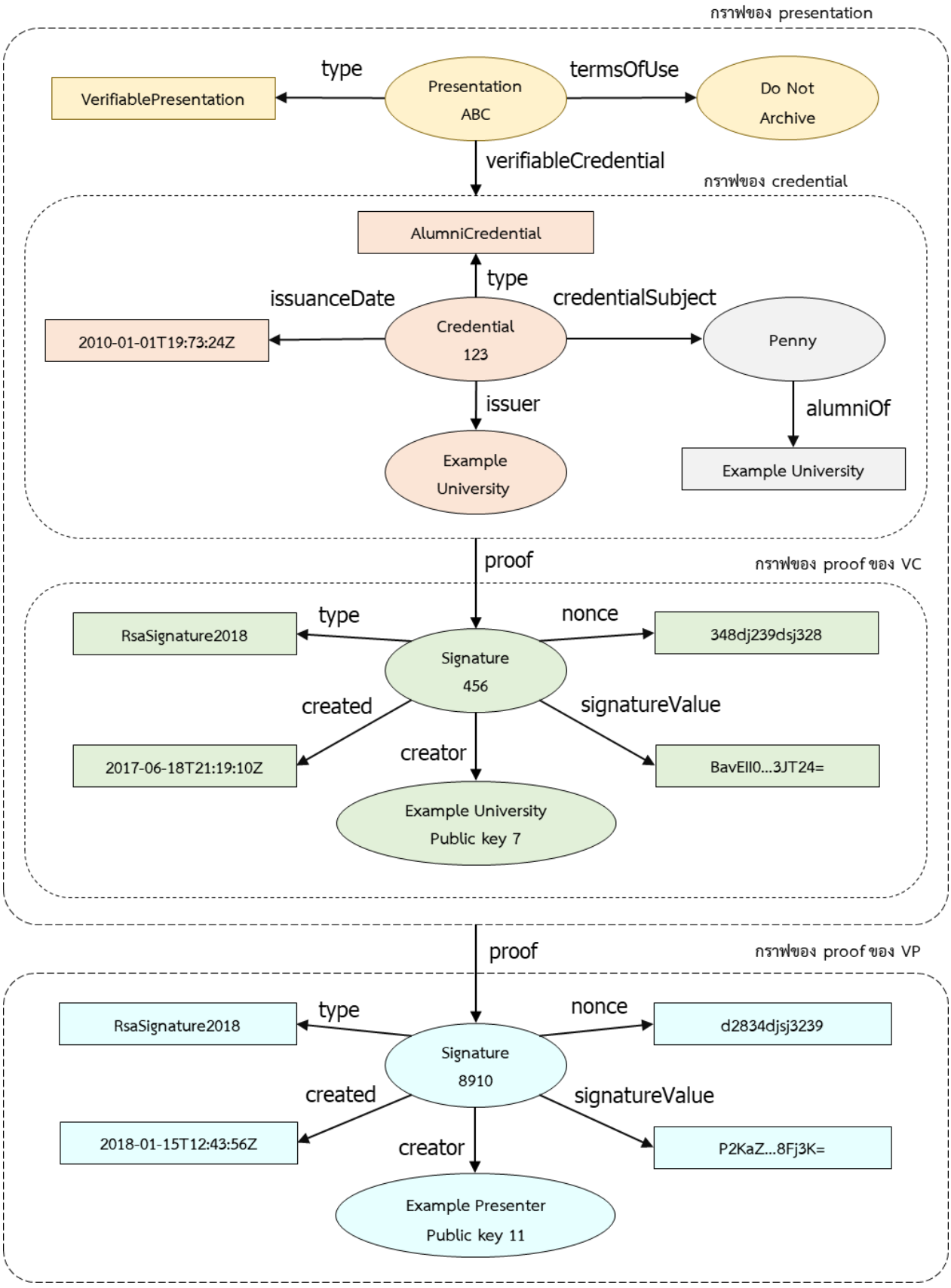
การสังเคราะห์ข้อมูลจาก VC เพื่อสร้างเป็น VP สามารถใช้วิธีการที่รองรับการเลือกเปิดเผยข้อมูลบางส่วน (selective disclosure) กล่าวคือ ผู้ถือเอกสารสามารถแสดงการพิสูจน์ให้ทราบข้อเท็จจริงเกี่ยวกับข้อความยืนยันได้ โดยไม่ต้องแสดงข้อความยืนยันทั้งหมดที่อยู่ใน VC ก็ได้ ทั้งนี้ VP อาจอยู่ในรูปแบบที่แสดงเฉพาะค่าความจริง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

ทั้งนี้ องค์ประกอบพื้นฐานของ VP สามารถแสดงตามรูปที่ 10 ซึ่งประกอบด้วย 3 ส่วน ได้แก่ (1) คำอธิบายข้อมูลของ VP (presentation metadata) (2) VC และ (3) ข้อพิสูจน์ (proof) ซึ่งโดยทั่วไปจะเป็นลายมือชื่อดิจิทัลของผู้ถือเอกสาร



รูปที่ 10 องค์ประกอบพื้นฐานของ VP

นอกจากนี้ VP สามารถแสดงเป็นกราฟข้อมูลได้ตามรูปที่ 11 โดย VP จะมีคุณสมบัติชื่อ **verifiableCredential** ที่ใช้อ้างอิงถึง VC อย่างน้อยหนึ่งชุด ซึ่ง VC แต่ละชุดจะประกอบด้วยคำอธิบายข้อมูลของ VC (credential metadata) ข้อความยืนยัน (claim) และข้อพิสูจน์ (proof)



รูปที่ 11 กราฟข้อมูลของ VP

จากกรณีศึกษาในตัวอย่างที่ 1 เมื่อเพ็ญนีได้รับ VC มาจัดเก็บไว้ในกระเป๋าดิจิทัลของตนเองแล้ว ต่อมาจะขอรับส่วนลดจากร้านสหกรณ์มหาวิทยาลัยสมมุติซึ่งเป็นผู้ตรวจสอบเอกสาร ร้านสหกรณ์จะส่งคำร้องขอ VC ที่ออกโดยมหาวิทยาลัยผ่านไปยังกระเป๋าดิจิทัลของเพ็ญนี และกระเป๋าดิจิทัลจะถามเพ็ญนีว่าต้องการใช้ VC ที่มีอยู่หรือไม่ เมื่อเพ็ญนีตอบตกลง VC จะถูกนำมาใช้สร้างเป็น VP แล้วส่งต่อไปให้ร้านสหกรณ์ดำเนินการตรวจสอบ ตัวอย่างของ VP ข้างต้นในรูปแบบ JSON-LD เป็นดังนี้

ตัวอย่างที่ 2 ตัวอย่างของ VP ในรูปแบบ JSON-LD

```
{
 "@context": [
   "https://www.w3.org/2018/credentials/v1",
   "https://www.w3.org/2018/credentials/examples/v1"
 ],
 "type": "VerifiablePresentation",
 // VC จากตัวอย่างที่ 1
 "verifiableCredential": [{
   "@context": [
     "https://www.w3.org/2018/credentials/v1",
     "https://www.w3.org/2018/credentials/examples/v1"],
   "id": "http://example.edu/credentials/1872",
   "type": ["VerifiableCredential", "AlumniCredential"],
   "issuer": "https://example.edu/issuers/565049",
   "issuanceDate": "2010-01-01T19:73:24Z",
   "credentialSubject": {
     "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
     "alumniOf": {
       "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",
       "name": [{
         "value": "Example University",
         "lang": "en"},
        {"value": "มหาวิทยาลัยสมมุติ",
         "lang": "th"}]
     }
   },
   "proof": {
     "type": "RsaSignature2018",
     "created": "2017-06-18T21:19:10Z",
     "proofPurpose": "assertionMethod",
     "verificationMethod": "https://example.edu/issuers/keys/1",
     "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..TCYt5X
       sITJX1CxPCT8yAV-TVkIEq_PbChOMqsLfRoPsnsgw5WEuts01mq-pQy7UJiN
       5mgRxD-WUcX16dUEMGlv50aqzpqh4Qktb3rk-BuQy72IFLOqV0G_zS245-
       kronKb78cPN25DGlcTwLtjPAYuNzVBAh4vGHSrQyHUdBBPM"
   }
 }],
// ลายมือชื่อดิจิทัลของเพ็ญนี ซึ่งเป็นผู้ถือ VC และเป็นผู้ออก VP
 "proof": {
   "type": "RsaSignature2018",
   "created": "2018-09-14T21:19:10Z",
```

```
    "proofPurpose": "authentication",
    "verificationMethod": "did:example:ebfeb1f712ebc6f1c276e12ec21#keys-1",
    // คุณสมบัติ challenge และ domain ใช้ในการป้องกัน replay attack
    "challenge": "1f44d55f-f161-4938-a659-f8026467f126",
    "domain": "4jt78h47fh47",
    "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..kTCYt5XsITJ
      X1CxPCT8yAV-TVIw5WEuts01mqpQy7UJiN5mgREEMGlv50aqzpqh4Qq_PbChOMqs
      LfRoPsnsgxD-WUcX16dUOqV0G_zS245-kronKb78cPktb3rk-BuQy72IFLN25DYuNzVB
      Ah4vGHSrQyHUGlcTwLtjPAnKb78"
  }
}
```

4. โครงสร้างข้อมูลของ VC และ VP

โครงสร้างข้อมูลของ VC และ VP ประกอบด้วยคุณสมบัติต่าง ๆ (property) ซึ่งจะแบ่งออกเป็นคุณสมบัติพื้นฐาน (รายละเอียดตามหัวข้อ 4.1 และ 4.2) และคุณสมบัติเพิ่มเติม (รายละเอียดตามภาคผนวก ก.)

4.1 คุณสมบัติพื้นฐานของ VC

4.1.1 @context

@context คือ คุณสมบัติที่ใช้เชื่อมโยงชื่อคุณสมบัติต่าง ๆ ใน VC หรือ VP เข้ากับ URI เพื่อให้ระบบคอมพิวเตอร์สามารถแลกเปลี่ยนข้อมูลและเข้าใจความหมายของคุณสมบัติต่าง ๆ ด้วยสมนาม (alias) ซึ่งกะทัดรัดและบุคคลอ่านเข้าใจได้

ไฟล์แบบมีการใช้ **@context**

```
{
  "@context":
["http://schema.org"],
  "type": "Person",
  "address": {
    "type": "PostalAddress",
    "streetAddress": "123 Main St.",
    "addressLocality": "Blacksburg",
    "postalCode": "24060"
  }
}
```

ไฟล์แบบมีการใช้ URI แบบเต็มรูป

```
{
  "@type": "http://schema.org/Person",
  "http://schema.org/address": {
    "@type": "http://schema.org/PostalAddress",
    "http://schema.org/streetAddress": "123 Main St.",
    "http://schema.org/addressLocality": "Blacksburg",
    "http://schema.org/postalCode": "24060"
  }
}
```

รูปที่ 12 การเปรียบเทียบระหว่างการใช้ @context กับการใช้ URI แบบเต็มรูป

ข้อกำหนดทางเทคนิค

- VC และ VP ต้องมี @context
- @context ต้องมีค่าเป็น URI หรือรายการของ URI ที่กำหนดให้ URI ลำดับแรกเป็น base context คือ https://www.w3.org/2018/credentials/v1 ตามตัวอย่างที่ 3
- URI แต่ละรายการใน @context ควรเชื่อมโยงไปยังแหล่งข้อมูลในรูปแบบที่คอมพิวเตอร์สามารถนำไปประมวลผลได้

ตัวอย่างที่ 3 วิธีใช้ @context

```
{
 "@context": [
   // URI ของ base context
   "https://www.w3.org/2018/credentials/v1",
   // URI ที่มีคุณสมบัติอื่นนอกเหนือจากคุณสมบัติใน base context
   "https://www.w3.org/2018/credentials/examples/v1"
 ],
 "id": "http://example.edu/credentials/58473",
 "type": ["VerifiableCredential", "AlumniCredential"],
 "credentialSubject": { ... },
 "proof": { ... }
}
```

4.1.2 id

id คือ คุณสมบัติที่ใช้แสดง identifier สำหรับอ้างอิงวัตถุที่เฉพาะเจาะจงใน VC เช่น บุคคล ผลิตภัณฑ์ หรือองค์กร เพื่อให้สามารถกล่าวถึงวัตถุเดียวกันได้อย่างชัดเจน

ข้อกำหนดทางเทคนิค

- VC อาจมี id หรือไม่ก็ได้ และถ้ามี id ต้องมีเพียงค่าเดียวสำหรับแต่ละวัตถุใน VC
- id ต้องใช้แสดง identifier ของวัตถุสำหรับนำไปใช้อ้างอิง
- ค่าของ id ต้องเป็น URI และ URI ใน id นี้ควรเชื่อมโยงไปยังแหล่งข้อมูลในรูปแบบที่คอมพิวเตอร์สามารถนำไปประมวลผลได้

ตัวอย่างที่ 4 วิธีใช้ id

```
{
 "@context": [ ... ],
 // id สำหรับ VC ซึ่งใช้เป็น URL รูปแบบ HTTP
 "id": "http://example.edu/credentials/3732",
 "type": ["VerifiableCredential", "UniversityDegreeCredential"],
 "credentialSubject": {
  // id สำหรับเจ้าของข้อความ ซึ่งใช้เป็น decentralized identifier (DID)
   "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
   "degree": { ... }
 },
 "proof": { ... }
}
```

4.1.3 type

type คือ คุณสมบัติที่ใช้แสดงประเภทของชุดข้อมูล (object) เพื่อพิจารณาว่าข้อมูลมีความเหมาะสมหรือไม่ โดยชุดข้อมูลที่ต้องระบุคุณสมบัติ type จะแสดงตามตารางที่ 1

ข้อกำหนดทางเทคนิค

- VC ต้องมี type

- ค่าของ **type** ต้องเป็น URI หรือเชื่อมโยงไปยัง URI (ผ่านการใช้ **@context**) อย่างน้อยหนึ่งรายการ ทั้งนี้ หากมี URI มากกว่าหนึ่งรายการ ค่าของ **type** ต้องเป็นรายการของ URI แบบไม่มีลำดับ (unordered)
- URI แต่ละรายการใน **type** ควรเชื่อมโยงไปยังแหล่งข้อมูลในรูปแบบที่เครื่องคอมพิวเตอร์สามารถนำไปประมวลผลได้

ตัวอย่างที่ 5 วิธีใช้ type

```
{
  "@context": [ ... ],
  "id": "http://example.edu/credentials/3732",
  "type": ["VerifiableCredential", "UniversityDegreeCredential"],
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "degree": {
      "type": "BachelorDegree",
      "name": "Bachelor of Science and Arts"
    }
  },
  "proof": { ... }
}
```

ตารางที่ 1 ข้อมูลที่ต้องระบุ type

ชื่อชุดข้อมูล (object)	ประเภทของชุดข้อมูล
verifiable credential	VC และประเภทเฉพาะของ VC (ถ้ามี) "type": ["VerifiableCredential", "UniversityDegreeCredential"]
verifiable presentation	VP และประเภทเฉพาะของ VP (ถ้ามี) "type": ["VerifiablePresentation", "CredentialManagerPresentation"]

proof	"proof": {
	"type": "RsaSignature2018"
	}

credential status	"credentialStatus": {
	"type": "CredentialStatusList2017"
	}

terms of use	"termsOfUse": {
	"type": "OdrlPolicy2017"
	}

evidence	"evidence": {
	"type": "DocumentVerification2018"
	}

4.1.4 **issuer**

issuer คือ คุณสมบัติที่ใช้แสดงถึงผู้ออกเอกสารรับรอง (VC)

ข้อกำหนดทางเทคนิค

- VC ต้องมี **issuer**
- ค่าของ **issuer** ต้องเป็น URI (ตามตัวอย่างที่ 6) หรือเป็นชุดข้อมูลที่ประกอบด้วย **id** (ตามตัวอย่างที่ 7)
- ค่า URI ใน **issuer** ควรเชื่อมโยงไปยังแหล่งข้อมูลในรูปแบบที่คอมพิวเตอร์สามารถนำไปประมวลผลได้

ตัวอย่างที่ 6 วิธีใช้ issuer

```
{
  "@context": [ ... ],
  "id": "http://example.edu/credentials/3732",
  "type": ["VerifiableCredential", "UniversityDegreeCredential"],
  "issuer": "https://example.edu/issuers/14",
  "issuanceDate": "2010-01-01T19:23:24Z",
  "credentialSubject": { ... },
  "proof": { ... }
}
```

นอกจากนี้ ค่าของ **issuer** สามารถถูกกำหนดในรูปแบบของชุดข้อมูลที่ประกอบด้วย **id** ดังนี้

ตัวอย่างที่ 7 วิธีใช้ issuer ที่มีข้อมูลเพิ่มเติม

```
{
  "@context": [ ... ],
  "id": "http://example.edu/credentials/3732",
  "type": ["VerifiableCredential", "UniversityDegreeCredential"],
  "issuer": {
    "id": "did:example:76e12ec712ebc6f1c221ebfeb1f",
    "name": "Example University"
  },
  "issuanceDate": "2010-01-01T19:23:24Z",
  "credentialSubject": { ... },
  "proof": { ... }
}
```

4.1.5 **issuanceDate** และ **expirationDate**

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

ข้อกำหนดทางเทคนิค

- VC ต้องมี **issuanceDate**
- ค่าของ **issuanceDate** ต้องเป็น string ที่แสดงวันและเวลาตามรูปแบบที่กำหนดใน RFC 3339

ซึ่งเป็นวันและเวลาที่ VC เริ่มมีผลผูกพันตามตัวอย่างที่ 8 โดยอาจเป็นวันและเวลาในอนาคตก็ได้

- VC อาจมี **expirationDate** หรือไม่ก็ได้
- ค่าของ **expirationDate** ต้องเป็น string ที่แสดงวันและเวลาตามรูปแบบที่กำหนดใน RFC 3339 ซึ่งเป็นวันและเวลาที่ VC สิ้นผลผูกพันตามตัวอย่างที่ 8
- ผู้ตรวจสอบเอกสารอาจทำการตรวจสอบค่าของ **issuanceDate** และ **expirationDate** ว่าอยู่ในช่วงวันและเวลาที่ผู้ตรวจสอบเอกสารกำหนดหรือไม่ เช่น **issuanceDate** ไม่เป็นวันและเวลาในอนาคต และ **expirationDate** ไม่เป็นวันและเวลาในอดีต

ตัวอย่างที่ 8 วิธีใช้ issuanceDate และ expirationDate

```
{
 "@context": [ ... ],
 "id": "http://example.edu/credentials/3732",
 "type": ["VerifiableCredential", "UniversityDegreeCredential"],
 "issuer": "https://example.edu/issuers/14",
 "issuanceDate": "2010-01-01T19:23:24Z",
 "expirationDate": "2020-01-01T19:23:24Z",  // VC มีอายุ 10 ปี
 "credentialSubject": { ... },
 "proof": { ... }
}
```

4.1.6 credentialSubject

credentialSubject คือ คุณสมบัติที่ใช้แสดงข้อความยืนยัน (claim) เกี่ยวกับเจ้าของข้อความ (subject) อย่างน้อยหนึ่งเอนทิตี

ข้อกำหนดทางเทคนิค

- VC ต้องมี credentialSubject
- ค่าของ credentialSubject เป็นกลุ่มของชุดข้อมูลที่ประกอบด้วยคุณสมบัติอย่างน้อยหนึ่งรายการ ซึ่งจะเกี่ยวข้องกับเจ้าของข้อความของ VC
- ชุดข้อมูลแต่ละรายการใน credentialSubject อาจประกอบด้วย id

ตัวอย่างที่ 9 วิธีใช้ credentialSubject

```
{
 "@context": [ ... ],
 "id": "http://example.edu/credentials/3732",
 "type": ["VerifiableCredential", "UniversityDegreeCredential"],
 "credentialSubject": {
  "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
  "degree": {
   "type": "BachelorDegree",
   "name": "Bachelor of Science and Arts"
  }
 },
 "proof": { ... }
}
```

นอกจากนี้ VC สามารถใช้แสดงข้อมูลเกี่ยวกับเจ้าของข้อความมากกว่าหนึ่งเอนทิตีได้โดยนำชุดข้อมูลมาเรียงกันเป็นแถวลำดับ (array) ภายใน **credentialSubject** ตัวอย่างเช่น VC ของทะเบียนสมรสที่ระบุว่าเจ้าของข้อความสองคน ได้แก่ เพ็ญนี (Penny) และใจเด่น (Jayden) เป็นคู่สมรสกัน โดยใช้คุณสมบัติที่ชื่อว่า **spouse** ดังนี้

ตัวอย่างที่ 10 วิธีใช้ credentialSubject ที่ระบุเจ้าของข้อความมากกว่าหนึ่งเอนทิตี

```
{
 "@context": [ ... ],
 "id": "http://example.edu/credentials/3732",
 "type": [ ... ],
 "credentialSubject": [{    // ข้อความยืนยัน 1: เพ็ญนีมีคู่สมรสคือใจเด่น
  "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",    // id ของเพ็ญนี
  "name": "Penny",
  "spouse": "did:example:c276e12ec21ebfeb1f712ebc6f1"    // id ของใจเด่น
 }, {    // ข้อความยืนยัน 2: ใจเด่นมีคู่สมรสคือเพ็ญนี
  "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",    // id ของใจเด่น
  "name": "Jayden",
  "spouse": "did:example:ebfeb1f712ebc6f1c276e12ec21"    // id ของเพ็ญนี
 }],
 "proof": { ... }
}
```

4.1.7 credentialStatus

credentialStatus คือ คุณสมบัติที่ใช้แสดงสถานะปัจจุบันของ VC เพื่อให้ทราบได้ว่า VC ถูกระงับหรือเพิกถอนหรือไม่

ข้อกำหนดทางเทคนิค

- VC อาจมี credentialStatus หรือไม่ก็ได้
- credentialStatus ต้องประกอบด้วยคุณสมบัติต่อไปนี้
  - id ซึ่งต้องมีค่าเป็น URL
  - type ซึ่งระบุประเภทสถานะของ VC (credential status type) โดยค่านี้ควรแสดงข้อมูลที่เพียงพอสำหรับแสดงสถานะปัจจุบันของ VC เช่น การระบุ URL ที่เชื่อมไปยังเอกสารภายนอกที่ระบุสถานะของ VC ตามตัวอย่างที่ 11

ตัวอย่างที่ 11 วิธีใช้ credentialStatus

```
{
 "@context": [ ... ],
 "id": "http://example.edu/credentials/3732",
 "type": ["VerifiableCredential", "UniversityDegreeCredential"],
 "issuer": "https://example.edu/issuers/14",
 "issuanceDate": "2010-01-01T19:23:24Z",
 "credentialSubject": { ... },
 "credentialStatus": {
```

```
  "id": "https://example.edu/status/24",
  "type": "CredentialStatusList2017"
 },
 "proof": { ... }
}
```

4.1.8 proof

proof คือ คุณสมบัติที่ใช้แสดงข้อพิสูจน์ (proof) โดยข้อพิสูจน์คือวิธีการที่ทำให้ VC หรือ VP สามารถถูกตรวจพบการเปลี่ยนแปลงใด ๆ ที่เกิดกับความถูกต้องครบถ้วนของข้อมูล และตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ของผู้ออกเอกสารและผู้ถือเอกสาร ได้ด้วยกระบวนการเข้ารหัสลับตามตัวอย่างที่ 12

ข้อพิสูจน์สามารถแบ่งออกเป็นสองประเภท คือ (1) external proof เช่น JSON Web Token (JWT) (รายละเอียดเพิ่มเติมที่ [3] [4]) และ (2) embedded proof เช่น Linked Data Signature (รายละเอียดเพิ่มเติมที่ [5])

โดยทั่วไป ข้อพิสูจน์จะเป็นลายมือชื่อดิจิทัล ซึ่งจัดเป็นลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ 2 หรือ 3 ตามข้อเสนอแนะมาตรฐานฯ ว่าด้วยแนวทางการลงลายมือชื่ออิเล็กทรอนิกส์ [6] นอกจากนี้ การสร้างลายมือชื่อดิจิทัลสามารถใช้อัลกอริทึม DSA, ECDSA หรือ RSA ซึ่งกำหนดไว้ในมาตรฐาน FIPS PUB 186-4: Digital Signature Standard ของ NIST [7] รวมถึงอัลกอริทึมอื่น ๆ ซึ่งเป็นที่ยอมรับ เช่น BBS+

ข้อกำหนดทางเทคนิค

- VC ต้องรองรับข้อพิสูจน์ที่อาศัยกระบวนการเข้ารหัสลับอย่างน้อยหนึ่งวิธี ไม่ว่าจะเป็น external proof หรือ embedded proof
- วิธีการ external proof อาจมี **proof** หรือไม่ก็ได้
- วิธีการ embedded proof ต้องมี **proof** และระบุชื่อวิธีการไว้ใน **type**

ตัวอย่างที่ 12 วิธีใช้ proof

```
{
 "@context": [ ... ],
 "id": "http://example.gov/credentials/3732",
 "type": ["VerifiableCredential", "UniversityDegreeCredential"],
 "issuer": "https://example.edu",
 "issuanceDate": "2010-01-01T19:73:24Z",
 "credentialSubject": { ... },
 "proof": {
  "type": "RsaSignature2018",
  "created": "2018-06-18T21:19:10Z",
  "proofPurpose": "assertionMethod",
  "verificationMethod": "https://example.com/jdoe/keys/1",
  "jws": "eyJhbGciOiJQUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19DJBMvvFAIC00nS
   GB6Tn0XKbbF9XrsaJZREWvR2aONYTQQxnyXirtXnlewJMBBn2h9hfcGZrvnC1b6PgWmukzFJ1
   IiH1dWgnDIS81BHIxXnPkbuYDeySorc4QU9MJxdVkY5EL4HYbcIfwKj6X4LBQ2_ZHZIu1jdqLcRZ
   qHcsDF5KKylKc1THn5VRWy5WhYg_gBnyWny8E6Qkrze53MR7OuAmmNJ1m1nN8SxDrG6a08L7
   8J0Fbas5OjAQz3c17GY8mVuDPOBIOVjMEghBlgl3nOi1ysxbRGhHLEK4s0KKbeRogZdgt1DkQxDF
   xxn41QWDw_mmMCjs9qxg0zcZzqEJw"}
}
```

4.1.9 โครงสร้างข้อมูลแสดงคุณสมบัติพื้นฐานของ VC

VC แต่ละชุดประกอบด้วยคุณสมบัติ (property) และค่าคุณสมบัติ (property value) นักพัฒนาต้องตรวจสอบ VC ให้สอดคล้องตามโครงสร้างข้อมูลของ VC ซึ่งรวมถึงชื่อคุณสมบัติ ชนิดของค่าคุณสมบัติ และจำนวนของค่าคุณสมบัติ โดยบางคุณสมบัติอาจเป็นคุณสมบัติบังคับ และบางคุณสมบัติอาจมีได้หลายรายการ

โครงสร้างข้อมูลที่มีรายการคุณสมบัติพื้นฐานสำหรับใช้ในการสร้าง VC สามารถแสดงตามตารางที่ 2

ทั้งนี้ จำนวนของค่าคุณสมบัติ (multiplicity หรือ cardinality) ของคุณสมบัติหนึ่ง ๆ จะแสดงจำนวนต่ำสุดและจำนวนสูงสุดที่สามารถปรากฏใน VC โดยตัวเลขทางซ้ายคือจำนวนต่ำสุด และตัวเลขทางขวาคือจำนวนสูงสุด ดังนี้

- [1..1] เป็นคุณสมบัติบังคับ และมีได้ไม่เกินหนึ่งค่า
- [1..n] เป็นคุณสมบัติบังคับ และมีได้ไม่จำกัดจำนวนสูงสุด
- [0..1] เป็นคุณสมบัติไม่บังคับ และหากมี จะมีได้ไม่เกินหนึ่งค่า
- [0..n] เป็นคุณสมบัติไม่บังคับ และหากมี จะมีได้ไม่จำกัดจำนวนสูงสุด

ตารางที่ 2 โครงสร้างข้อมูลแสดงคุณสมบัติพื้นฐานของ VC

คุณสมบัติ	ชื่อคุณสมบัติ	คำอธิบาย	จำนวน	ชนิดของค่าคุณสมบัติ	ตัวอย่างการใช้งาน
context	**@context**	ที่อยู่เอกสารที่เชื่อมโยงชื่อคุณสมบัติต่าง ๆ ใน VC เข้ากับ URI ที่ระบุนิยามและโครงสร้างของคุณสมบัตินั้น	[1..n]	URI หรือรายการของ URI	"@context": ["https://www.w3.org/2018/credentials/v1", "https://www.w3.org/2018/credentials/examples/v1"]
identifier	**id**	Identifier ของ VC	[0..1]	URI	"id": "http://example.edu/credentials/3732"
type	**type**	ประเภทเอกสาร เพื่อให้ผู้ถือเอกสารพิจารณาความเหมาะสมของโครงสร้างข้อมูลได้ โดยในกรณีนี้ ให้ระบุเป็น **"VerifiableCredential"** และอาจมีประเภทเฉพาะของเอกสารด้วย	[1..n]	URI หรือรายการของ URI	"type": ["VerifiableCredential", "UniversityDegreeCredential"]
issuer	**issuer**	ผู้ออก VC	[1..1]	URI	"issuer": "https://example.edu/issuers/14"

				ชุดข้อมูลที่มีคุณสมบัติ **id**	"issuer": {
					"id": "did:example:76e12ec712ebc6f1c221ebfeb1f",
					"name": "Example University"
					}

issuance date และ expiration dates	**issuanceDate** หรือ **validFrom**	วันและเวลาเมื่อ VC เริ่มมีผลผูกพัน	[1..1]	string แสดงวันและเวลาตาม RFC 3339	"issuanceDate": "2010-01-01T19:23:24Z"
	expirationDate หรือ **validUntil**	วันและเวลาเมื่อ VC สิ้นผลผูกพัน	[0..1]	string แสดงวันและเวลาตาม RFC 3339	"expirationDate": "2016-01-01T00:00:00Z"

credential subject และ claim	**credentialSubject**	เจ้าของข้อความที่ถูกกล่าวอ้างถึงในข้อความยืนยัน	[1..n]		"credentialSubject": {
					"id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
					"alumniOf": {
					"id": "did:example:c276e12ec21ebfeb1f712ebc6f1",
					"name": [{
					"value": "Example University",
					"language": "en"
					}, {
					"value": "**มหาวิทยาลัยสมมุติ**",
					"language": "th"

	id	identifier ของเจ้าของข้อความ	[0..1]	URI	
	ชื่อคุณสมบัติ[2] เช่น **name, alumniOf, degree** หรือ **spouse** โดยอาจอ้างอิง www.schema.org	คุณสมบัติและค่าคุณสมบัติของข้อความยืนยันที่เกี่ยวกับเจ้าของข้อความนั้น	[1..n]	ประเภทข้อมูลที่เหมาะสมต่อคุณสมบัตินั้น ๆ หรือชุดข้อมูลซึ่งอาจมี **id** หากกล่าวถึงเอนทิตีอื่น	

[2] โดยปกติให้ตั้งชื่อด้วย Lower Camel Case (LCC) กล่าวคือ แต่ละคำขึ้นต้นด้วยตัวพิมพ์ใหญ่ ยกเว้นคำแรกให้ขึ้นต้นด้วยตัวพิมพ์เล็ก และไม่เว้นวรรคระหว่างคำ

คุณสมบัติ	ชื่อคุณสมบัติ	คำอธิบาย	จำนวน	ชนิดของค่าคุณสมบัติ	ตัวอย่างการใช้งาน
					}] } }

credential status	credentialStatus	สถานะปัจจุบันของเอกสาร เช่น เพิกถอนแล้ว	[0..1]		"credentialStatus": {
					"id": "https://example.edu/status/24",
					"type": "CredentialStatusList2017"
					}

	id	identifier ของเอกสารอ้างอิง	[1..1]	URL	
	type	ประเภทสถานะเอกสาร	[1..1]	string	

proof	proof	ข้อพิสูจน์ที่ใช้ในการตรวจสอบเอกสาร เช่น ลายมือชื่อดิจิทัล หรือ JSON Web Token (JWT)	[0..n] [3]		"proof": {
					"type": "RsaSignature2018",
					"created": "2017-06-18T21:19:10Z",
					"proofPurpose": "assertionMethod",
					"verificationMethod": "https://example.edu/issuers/keys/1",
					"jws":
					"eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0II19..TCYt5XsITJX1CxPCT8yAV-TVkIEq_PbChOMqsLfRoPsnsg w5WEuts01mq-pQy7UJiN5mgRxD-WUcX16dUEMGlv50aqzp qh4Qktb3rk-BuQy72IFLOqV0G_zS 245-kronKb78cPN25DGlc TwLtjPAYuNzVBAh4vGHSrQy HUdBBPM"
					}

	type	ประเภทข้อพิสูจน์	[1..1]	string	
	created	วันและเวลาเมื่อลงข้อพิสูจน์	[1..1]	string แสดงวันและเวลาตาม RFC 3339	
	expires	วันและเวลาเมื่อข้อพิสูจน์สิ้นอายุ	[0..1]	string แสดงวันและเวลาตาม RFC 3339	
	proofPurpose	วัตถุประสงค์ของข้อพิสูจน์ โดยในกรณีนี้ ให้ระบุเป็น "assertionMethod"	[0..1]	string	
	ชื่อคุณสมบัติทางความมั่นคงปลอดภัย เช่น verificationMethod, jws, nonce หรือ domain โดยอาจอ้างอิง w3c-ccg.github.io/security-vocab/	คุณสมบัติและค่าคุณสมบัติของข้อพิสูจน์นั้น	[0..1]	ประเภทข้อมูลที่เหมาะสมต่อคุณสมบัตินั้น ๆ	

[3] VC จำเป็นต้องรองรับข้อพิสูจน์ (proof) ไม่ว่าจะเป็น external proof หรือ embedded proof ซึ่งหาก VC ใดใช้ embedded proof จะต้องปรากฏ **proof** ด้วยเสมอ

4.2 คุณสมบัติของ VP

VP ถูกสร้างขึ้นมาจาก VC อย่างน้อยหนึ่งชุดโดยผู้ถือเอกสาร ซึ่งผู้ถือเอกสาร (holder) ใช้แสดงข้อความยืนยันภายใน VC ในรูปแบบที่สามารถตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ของผู้ถือเอกสาร VP โดยทั่วไปจะประกอบไปด้วยคุณสมบัติตามตารางที่ 3

ตารางที่ 3 คุณสมบัติของ VP โดยทั่วไป

ชื่อคุณสมบัติ	ข้อกำหนด
id	id เป็นคุณสมบัติที่จะมีหรือไม่ก็ได้ และอาจใช้เป็น identifier ที่เฉพาะเจาะจงของ VP
type	type เป็นคุณสมบัติที่ต้องมี และใช้แสดงประเภทของ VP เช่น VerifiablePresentation
verifiableCredential	(ถ้ามี) ค่าของ verifiableCredential ต้องสร้างขึ้นจาก VC อย่างน้อยหนึ่งชุด หรือเป็นข้อมูลที่สังเคราะห์จาก VC ในรูปแบบที่สามารถตรวจสอบได้ด้วยกระบวนการเข้ารหัสลับ
holder	(ถ้ามี) ค่าของ holder ควรเป็น URI ของเอนทิตีที่สร้าง VP
proof	(ถ้ามี) ค่าของ proof จะเป็นข้อพิสูจน์หรือหลักฐานที่ใช้ในการตรวจสอบ VP

ตัวอย่างที่ 13 VP ที่ประกอบด้วย VC

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  "id": "urn:uuid:3978344f-8596-4c3a-a978-8fcaba3903c5",
  "type": ["VerifiablePresentation", "CredentialManagerPresentation"],
  "verifiableCredential": [{ ... }],
  "proof": [{ ... }]
}
```

4.2.1 โครงสร้างข้อมูลแสดงคุณสมบัติของ VP

โครงสร้างข้อมูลที่มีรายการคุณสมบัติสำหรับใช้ในการสร้าง VP สามารถแสดงตามตารางที่ 4

ตารางที่ 4 โครงสร้างข้อมูลแสดงคุณสมบัติของ VP

คุณสมบัติ	ชื่อคุณสมบัติ	คำอธิบาย	จำนวน	ชนิดของค่าคุณสมบัติ	ตัวอย่างการใช้งาน
context	**@context**	ที่อยู่เอกสารที่เชื่อมโยงชื่อคุณสมบัติต่าง ๆ เข้ากับ URI ที่ระบุนิยามและโครงสร้างของคุณสมบัตินั้น	[1..n]	URI หรือรายการของ URI	"@context": ["https://www.w3.org/2018/credentials/v1", "https://www.w3.org/2018/credentials/examples/v1"]
identifier	**id**	identifier ของ VP	[0..1]	URI	"id": "urn:uuid:3978344f-8596-4c3a-a978-8fcaba3903c5"
type	**type**	ประเภทเอกสาร เพื่อให้ผู้ตรวจสอบเอกสารพิจารณาความเหมาะสมของโครงสร้างข้อมูลได้ โดยในกรณีนี้ให้ระบุเป็น **"VerifiablePresentation"** และอาจมีประเภทเฉพาะของเอกสารด้วย	[1..n]	URI หรือรายการของ URI	"type": ["VerifiablePresentation", "CredentialManagerPresentation"]
holder	**holder**	ผู้ออก VP ซึ่งคือ ผู้ถือ VC	[0..1]	URI	"holder": "https://example.edu/issuers/14"
claim	**verifiableCredential**	VC ซึ่งบรรจุข้อความยืนยัน	[0..n]	ชุดข้อมูล verifiable credential	"verifiableCredential": [{ "@context": [...], "id": "http://example.edu/credentials/1872", "type": [...], "issuer": "https://example.edu/issuers/565049", "issuanceDate": "2010-01-01T19:73:24Z", "credentialSubject": {...}, "proof": {...} }]
proof	**proof**	ข้อพิสูจน์ที่ใช้ในการตรวจสอบเอกสาร เช่น ลายมือชื่อดิจิทัล หรือ JSON Web Token (JWT)	[0..n][4]		"proof": { "type": "RsaSignature2018", "created": "2018-09-14T21:19:10Z", "proofPurpose": "authentication", "verificationMethod": "did:example:ebfeb1f712ebc6f1c276e12ec21#keys-1", "challenge": "1f44d55f-f161-4938-a659-f8026467f126", "domain": "4jt78h47fh47",
	type	ประเภทข้อพิสูจน์	[1..1]	string	
	created	วันและเวลาเมื่อลงข้อพิสูจน์	[1..1]	string แสดงวันและเวลาตาม RFC 3339	
	expires	วันและเวลาเมื่อข้อพิสูจน์สิ้นอายุ	[0..1]	string แสดงวันและเวลาตาม RFC 3339	
	proofPurpose	วัตถุประสงค์ของข้อพิสูจน์ โดยในกรณีนี้ ให้ระบุเป็น **"authentication"**	[0..1]	string	

[4] VP จำเป็นต้องรองรับข้อพิสูจน์ (proof) ไม่ว่าจะเป็น external proof หรือ embedded proof ซึ่งหาก VP ใดใช้ embedded proof จะต้องปรากฏ **proof** ด้วยเสมอ

คุณสมบัติ	ชื่อคุณสมบัติ	คำอธิบาย	จำนวน	ชนิดของค่าคุณสมบัติ	ตัวอย่างการใช้งาน
	ชื่อคุณสมบัติทางความมั่นคงปลอดภัย เช่น verificationMethod, jws, nonce, domain หรือ challenge โดยอาจอ้างอิง w3c-ccg.github.io/security-vocab/	คุณสมบัติและค่าคุณสมบัติของข้อพิสูจน์นั้น	[0..1]	ประเภทข้อมูลที่เหมาะสมต่อคุณสมบัตินั้น ๆ	"jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..kTCYt5XsITJX1CxPCT8yAV-TVIw5WEuts01mq-pQ y7UJiN5mgREEMGlv50aqzpqh4Qq_PbChOMqsLfRoPsnsgxD-WUcX16dUOqV0G_zS245-kronKb78cPktb3rk-BuQy72IFLN25DYuNzVBAh4vGHSrQyHUGlcTwLtjPAnKb78" }

ภาคผนวก ก. คุณสมบัติเพิ่มเติมของ VC

ก.1 credentialSchema

credentialSchema คือ คุณสมบัติที่ใช้กำหนด schema ของเอกสาร ซึ่งอาจแบ่งออกเป็นสองประเภท คือ (1) data verification schema ซึ่งเป็น schema ที่ใช้ในการตรวจสอบโครงสร้างและเนื้อหาของ VC ว่าสอดคล้องตามรูปแบบที่กำหนดไว้ตามตัวอย่างที่ 14 และ (2) data encoding schema ซึ่งเป็น schema ที่ใช้ในการเข้ารหัสเนื้อหาของ VC เพื่อแสดงในรูปแบบอื่น ๆ เช่น รูปแบบเลขฐานสอง (binary format) ที่ใช้สำหรับ zero-knowledge proof ตามตัวอย่างที่ 15

ข้อกำหนดทางเทคนิค

- ค่าของ **credentialSchema** ต้องเป็น schema อย่างน้อยหนึ่งรายการ เพื่อให้ผู้ตรวจสอบเอกสารใช้ในการตรวจสอบข้อมูลว่าสอดคล้องตาม schema ที่กำหนดไว้
- **credentialSchema** แต่ละรายการต้องระบุ **type** ซึ่งแสดงประเภทของ schema และ **id** ซึ่งต้องเป็น URI ที่เชื่อมโยงไปยังไฟล์ schema

ตัวอย่างที่ 14 วิธีใช้ credentialSchema
เพื่อตรวจสอบโครงสร้างตามไฟล์ JSON schema

```
{
  "@context": [ ... ],
  "id": "http://example.edu/credentials/3732",
  "type": ["VerifiableCredential", "UniversityDegreeCredential"],
  "issuer": "https://example.edu/issuers/14",
  "issuanceDate": "2010-01-01T19:23:24Z",
  "credentialSubject": { ... },
// ผู้ออกเอกสารระบุ credentialSchema ที่เชื่อมโยงไปยังไฟล์ JSON schema เพื่อให้ผู้ตรวจสอบเอกสารใช้ในการตรวจสอบ VC ว่าสอดคล้องตาม schema ที่กำหนดไว้
  "credentialSchema": {
    "id": "https://example.org/examples/degree.json",
    "type": "JsonSchemaValidator2018
  },
  "proof": { ... }
}
```

ตัวอย่างที่ 15 วิธีใช้ credentialSchema
เพื่อตรวจสอบการแปลงเนื้อหาสำหรับ zero-knowledge proof

```
{
  "@context": [ ... ],
  "id": "http://example.edu/credentials/3732",
  "type": ["VerifiableCredential", "UniversityDegreeCredential"],
  "issuer": "https://example.edu/issuers/14",
  "issuanceDate": "2010-01-01T19:23:24Z",
  "credentialSubject": { ... },
// ผู้ออกเอกสารระบุ credentialSchema ที่เชื่อมโยงไปยัง binary format ที่ใช้ในการแปลงเนื้อหาสำหรับ zero-knowledge proof เพื่อให้ผู้ตรวจสอบเอกสารใช้ในการตรวจสอบข้อพิสูจน์ของ VC ว่าถูกต้องหรือไม่
  "credentialSchema": {
```

```
  "id": "https://example.org/examples/degree.zkp",
  "type": "ZkpExampleSchema2018"
 },
 "proof": { ... }
}
```

ก.2 **evidence**

evidence คือ คุณสมบัติที่ใช้แสดงข้อมูลหลักฐาน ซึ่งผู้ออกเอกสารจัดทำเป็นข้อมูลสนับสนุนเพิ่มเติมใน VC เพื่อทำให้ผู้ตรวจสอบเอกสารเกิดความเชื่อมั่นต่อข้อความยืนยันที่อยู่ใน VC ตัวอย่างเช่น ผู้ออกเอกสารอาจตรวจสอบเอกสารหลักฐานที่เป็นกระดาษหรือตรวจสอบประวัติของเจ้าของข้อความก่อนที่จะออก VC ตามตัวอย่างที่ 16

evidence ต่างจาก proof ตรงที่ evidence ใช้แสดงข้อมูลสนับสนุนเพิ่มเติม เช่น หลักฐานที่เกี่ยวข้องกับความถูกต้องครบถ้วนของ VC ในขณะเดียวกัน proof ใช้แสดงข้อพิสูจน์ที่เกี่ยวข้องกับความถูกต้องครบถ้วนของ VC และการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ของผู้ออกเอกสาร

ข้อกำหนดทางเทคนิค

- ค่าของ evidence ต้องเป็นข้อมูลหลักฐานอย่างน้อยหนึ่งรายการ ซึ่งให้ข้อมูลที่เพียงพอตามข้อกำหนดของผู้ตรวจสอบเอกสารเกี่ยวกับความน่าเชื่อถือของ VC
- evidence แต่ละรายการต้องมี type ซึ่งแสดงประเภทของข้อมูลหลักฐาน
- evidence อาจมี id หรือไม่ก็ได้ และถ้ามี ควรเป็น URL ที่เชื่อมโยงไปยังแหล่งที่จัดเก็บข้อมูลหลักฐาน

ตัวอย่างที่ 16 วิธีใช้ evidence

```
{
 "@context": [ ... ],
 "id": "http://example.edu/credentials/3732",
 "type": ["VerifiableCredential", "UniversityDegreeCredential"],
 "issuer": "https://example.edu/issuers/14",
 "issuanceDate": "2010-01-01T19:23:24Z",
 "credentialSubject": { ... },
 "evidence": [{
  "id": "https://example.edu/evidence/f2aeec97-fc0d-42bf-8ca7-0548192d4231",
  "type": ["DocumentVerification"],
  "verifier": "https://example.edu/issuers/14",
  "evidenceDocument": "DriversLicense",
  "subjectPresence": "Physical",
  "documentPresence": "Physical"},
  {"id": "https://example.edu/evidence/f2aeec97-fc0d-42bf-8ca7-0548192dxyzab",
  "type": ["SupportingActivity"],
  "verifier": "https://example.edu/issuers/14",
  "evidenceDocument": "Fluid Dynamics Focus",
  "subjectPresence": "Digital",
  "documentPresence": "Digital"
 }],
 "proof": { ... }
}
```

ภาคผนวก ข. การเพิ่มคุณสมบัติ (extensibility)

นักพัฒนาสามารถเพิ่มคุณสมบัติในโครงสร้างข้อมูลของ VC ด้วยคำศัพท์ในรูปแบบที่คอมพิวเตอร์สามารถนำไปประมวลผลได้ โดยไม่จำเป็นต้องอาศัยระบบทะเบียนกลาง ทั้งนี้ การเพิ่มคุณสมบัติสามารถทำได้ด้วยการใช้ linked data หรือ JSON-LD

ตัวอย่างการเพิ่มคุณสมบัติใน VC สามารถอธิบายโดยเริ่มต้นจาก VC อย่างง่ายตามตัวอย่างที่ 17

ตัวอย่างที่ 17 VC อย่างง่าย

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  "id": "http://example.com/credentials/4643",
  "type": ["VerifiableCredential"],
  "issuer": "https://example.com/issuers/14",
  "issuanceDate": "2018-02-24T05:28:04Z",
  "credentialSubject": {
    "id": "did:example:abcdef1234567",
    "name": "Penny"
  },
  "proof": { ... }
}
```

VC ข้างต้นระบุว่าเอนทิตีที่สัมพันธ์กับ did:example:abcdef1234567 มี name ที่มีค่าเป็น Penny

หากนักพัฒนาต้องการเพิ่มคุณสมบัติใหม่เข้าไปใน VC ข้างต้นอีกสองรายการ คือ **referenceNumber** สำหรับใช้แสดงหมายเลขอ้างอิงภายในองค์กร และ **favoriteFood** สำหรับใช้แสดงอาหารจานโปรด นักพัฒนาต้องทำการสร้าง JSON-LD context ที่มีคุณสมบัติใหม่สองรายการตามตัวอย่างที่ 18

ตัวอย่างที่ 18 JSON-LD context

```
{
  "@context": {
    "referenceNumber": "https://example.com/vocab#referenceNumber",
    "favoriteFood": "https://example.com/vocab#favoriteFood"
  }
}
```

หลังจากสร้าง JSON-LD context แล้ว นักพัฒนาจะนำข้อมูล JSON-LD context ข้างต้นไปเผยแพร่ที่แหล่งที่ผู้ตรวจสอบเอกสารสามารถเข้าถึงได้ เช่น https://example.com/contexts/mycontext.jsonld ตามตัวอย่างที่ 19 จากนั้น นักพัฒนาจะอัปเดตค่าของ **@context** และ **type** และเพิ่มคุณสมบัติใหม่ลงใน VC

ตัวอย่างที่ 19 VC ที่มีการเพิ่มคุณสมบัติใหม่

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://example.com/contexts/mycontext.jsonld"],
// เพิ่ม URI ที่มีคุณสมบัติใหม่ใน @context
  "id": "http://example.com/credentials/4643",
  "type": ["VerifiableCredential", "CustomExt12"],   // เพิ่มค่า CustomExt12 ใน type
  "issuer": "https://example.com/issuers/14",
  "issuanceDate": "2018-02-24T05:28:04Z",
  "referenceNumber": 83294847,    // เพิ่มคุณสมบัติใหม่ คือ referenceNumber
  "credentialSubject": {
    "id": "did:example:abcdef1234567",
    "name": "Penny",
    "favoriteFood": "Som Tam"    // เพิ่มคุณสมบัติใหม่ คือ favoriteFood
  },
  "proof": { ... }
}
```

ภาคผนวก ค. ตัวอย่างกรณีศึกษาการใช้งาน VC และ VP

ตัวอย่างกรณีศึกษาการใช้งาน VC และ VP มีดังต่อไปนี้

กรณีศึกษา	ผู้ออกเอกสาร	ผู้ถือเอกสาร	ผู้ตรวจสอบเอกสาร
(1) ใบประมวลผลการศึกษา (transcript) หรือใบปริญญาบัตร มหาวิทยาลัยออกใบประมวลผลการศึกษาหรือใบปริญญาบัตรในรูป VC ให้แก่นักศึกษา เพื่อนำไปใช้สมัครเข้าทำงานกับหน่วยงานที่รับสมัครงาน หน่วยงานสามารถตรวจสอบได้ว่าเอกสารข้างต้นออกโดยมหาวิทยาลัยนั้นจริง ซึ่งช่วยป้องกันการนำเอกสารปลอมมาใช้ในการสมัครเข้าทำงาน	มหาวิทยาลัย	นักศึกษา	หน่วยงานที่รับสมัครงาน
(2) หนังสือมอบอำนาจ ผู้มอบอำนาจออกหนังสือมอบอำนาจในรูป VC ให้แก่ผู้รับมอบอำนาจ เพื่อให้ดำเนินการแทนผู้มอบอำนาจตามรายละเอียดในหนังสือมอบอำนาจ ซึ่งเจ้าหน้าที่สามารถตรวจสอบได้ว่าผู้มอบอำนาจได้กระทำการมอบอำนาจนั้นจริง	ผู้มอบอำนาจ	ผู้รับมอบอำนาจ	เจ้าหน้าที่ตรวจสอบเอกสาร
(3) บัตรสมนาคุณ หรือบัตรสมาชิกสะสมแต้ม ผู้บริโภคใช้บริการของผู้ให้บริการตามเงื่อนไขที่กำหนด ผู้ให้บริการจึงออกบัตรสมนาคุณหรือบัตรสมาชิกสะสมแต้มในรูป VC ให้แก่ผู้บริโภค เพื่อนำไปใช้เป็นส่วนลดค่าบริการ โดยอาจเป็นบริการของตนเองหรือบริการของผู้ให้บริการอื่นที่เป็นพันธมิตรก็ได้	ผู้ให้บริการ	ผู้บริโภค	ผู้ให้บริการอื่น
(4) ใบรับรองแพทย์ แพทย์/โรงพยาบาลออกใบรับรองแพทย์ในรูป VC ให้แก่ผู้ป่วย เพื่อรับรองอาการป่วย ซึ่งผู้ป่วยสามารถนำเอกสารข้างต้นไปแสดงเป็นหลักฐานประกอบการลางานกับฝ่ายบุคคลของหน่วยงานได้	แพทย์/โรงพยาบาล	หน่วยงาน	ฝ่ายบุคคลของหน่วยงาน

บรรณานุกรม

[1] W3C Recommendation, "Verifiable Credentials Data Model 1.0 - Expressing verifiable information on the Web", November 2019. Available: https://www.w3.org/TR/vc-data-model/.

[2] Christopher Allen, "The Path to Self-Sovereign Identity", April 2016 [Online]. Available: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.

[3] Internet Engineering Task Force, "RFC 7515 - JSON Web Signature (JWS)", May 2015 [Online]. Available: https://tools.ietf.org/html/rfc7515.

[4] Internet Engineering Task Force, "RFC 7519 - JSON Web Token (JWT)", May 2015 [Online]. Available: https://tools.ietf.org/html/rfc7519.

[5] W3C Working Group Note, "Linked Data Proofs 1.0", 03 March 2020. Available: https://w3c-ccg.github.io/ld-proofs/.

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

[7] National Institute of Standards and Technology, "FIPS PUB 186-4: Digital Signature Standard (DSS)", July 2013 [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf.

[8] W3C Working Group Note, "Verifiable Credentials Use Cases", September 2019. Available: https://www.w3.org/TR/vc-use-cases/.

[9] Internet Engineering Task Force, "RFC 3339 - Date and Time on the Internet: Timestamps", July 2002 [Online] . Available: https://tools.ietf.org/html/rfc3339.