สพธอ./ PRD

สิงหาคม 2563

ข้อเสนอแนะมาตรฐานอยู่ระหว่างการจัดทำ ห้ามใช้หรือยึดร่างนี้เป็นข้อเสนอแนะมาตรฐาน

ข้อเสนอแนะมาตรฐานฉบับสมบูรณ์จะมีประกาศโดย
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ร่าง

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร
ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์
ETDA Recommendation on ICT Standard for Electronic Transactions

ว่าด้วยโครงสร้างข้อมูลของสารรับรองและสารสำแดงที่ตรวจสอบได้

DATA STRUCTURE OF VERIFIABLE CREDENTIAL AND PRESENTATION

สำหรับเวียนขอข้อคิดเห็นจากหน่วยงานต่างๆ ที่เกี่ยวข้อง

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

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ETDA Recommendation on ICT Standard

for Electronic Transactions

ขมธอ. [x-xxxx]

ว่าด้วยโครงสร้างข้อมูลของสารรับรองและสารสำแดงที่ตรวจสอบได้

DATA STRUCTURE OF VERIFIABLE CREDENTIAL AND PRESENTATION

เวอร์ชัน 0.3

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ICS [xxx.xxx.xxx]

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยโครงสร้างข้อมูลของสารรับรองและสารสำแดงที่ตรวจสอบได้

ขมธอ. [x-xxxx]

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

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

ประกาศโดย
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

วันที่ กรุณาเลือกวันที่ประกาศ

คณะทำงานจัดทำร่างข้อเสนอแนะมาตรฐานเกี่ยวกับธุรกิจบริการ
ด้านการทำธุรกรรมทางอิเล็กทรอนิกส์

ที่ปรึกษาคณะทำงาน

นายชัยชนะ มิตรพันธ์	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ประธานคณะทำงาน

นายศุภโชค จันทรประทิน	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ผู้ทำงาน

นางสาวสำรวย นุ่มศรี	กรมศุลกากร
นายกำชัย จัตตานนท์	
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
ว่าด้วยโครงสร้างข้อมูลของสารรับรองและสารสำแดงที่ตรวจสอบได้

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 ว่าด้วยโครงสร้างข้อมูลของสารรับรองและสารสำแดงที่ตรวจสอบได้ ฉบับนี้ จัดทำขึ้นเพื่อกำหนดโครงสร้างข้อมูลสำหรับสารรับรองที่ตรวจสอบได้ (verifiable credential) และสารสำแดงที่ตรวจสอบได้ (verifiable presentation) และอธิบายความสัมพันธ์ระหว่างบทบาทที่เกี่ยวข้องกับระบบการใช้งานของสารรับรองที่ตรวจสอบได้ เพื่อให้ผู้ใช้งานสามารถใช้สารรับรองที่ตรวจสอบได้ในการแสดงเอกสารหรือข้อมูลประจำตัวต่าง ๆ บนโลกออนไลน์ในลักษณะที่มีความมั่นคงปลอดภัย มีการรักษาความเป็นส่วนตัว สามารถตรวจสอบได้ด้วยกระบวนการเข้ารหัสลับ และสนับสนุนการแลกเปลี่ยนระหว่างกันตามมาตรฐานสากล โดยข้อเสนอแนะมาตรฐานฉบับนี้อ้างอิงมาตรฐาน Verifiable Credentials Data Model ของ World Wide Web Consortium (W3C) [1]

โดยมีการนำเสนอและรับฟังความคิดเห็นเป็นการทั่วไป ตลอดจนพิจารณาข้อมูล ข้อสังเกต ข้อคิดเห็นจากผู้ทรงคุณวุฒิและจากหน่วยงานที่เกี่ยวข้อง เพื่อปรับปรุงให้ข้อเสนอแนะมาตรฐานฉบับนี้มีความสมบูรณ์ครบถ้วนยิ่งขึ้น รวมทั้งให้สามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพ

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยโครงสร้างข้อมูลของสารรับรองและสารสำแดงที่ตรวจสอบได้ ฉบับนี้ 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

การให้บริการแก่ประชาชนทั้งจากภาครัฐและภาคเอกชนโดยทั่วไปอาจมีการออกเอกสารที่ใช้รับรองข้อมูลบางอย่างแก่ประชาชนผู้เป็นเจ้าของข้อมูลในเอกสาร ตัวอย่างเช่น ใบขับขี่ที่ออกเพื่อรับรองว่าบุคคลมีความสามารถในการขับขี่รถยนต์ ใบปริญญาบัตรที่ออกโดยมหาวิทยาลัยให้แก่นักศึกษาเพื่อรับรองวุฒิการศึกษา ใบรับรองแพทย์ที่ออกโดยแพทย์เพื่อรับรองว่าผู้ป่วยมีอาการตามที่ระบุในเอกสาร

เมื่อการทำธุรกรรมมีแนวโน้มมาอยู่ในรูปแบบอิเล็กทรอนิกส์มากขึ้น หน่วยงานทั้งภาครัฐและภาคเอกชนอาจมีการออกเอกสารรับรองข้อมูลในรูปของสารรับรองที่ตรวจสอบได้ (verifiable credential: VC) ซึ่งเป็นวิธีการตามมาตรฐานของ World Wide Web Consortium (W3C) โดยสารรับรองที่ตรวจสอบได้ดังกล่าวเป็นเอกสารรับรองข้อมูลในรูปแบบอิเล็กทรอนิกส์ที่มีคุณสมบัติช่วยให้สามารถตรวจพบการปลอมแปลงและตรวจสอบผู้เขียนข้อมูลได้ด้วยกระบวนการเข้ารหัสลับ

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์เล็งเห็นถึงประโยชน์จากการใช้งานสารรับรองที่ตรวจสอบได้ จึงได้จัดทำมาตรฐานรายการข้อมูลของสารรับรองและสารสำแดงที่ตรวจสอบได้ เพื่อให้ผู้ใช้งานสามารถใช้สารรับรองที่ตรวจสอบได้ในการแสดงเอกสารหรือข้อมูลประจำตัวต่าง ๆ บนโลกออนไลน์ในลักษณะที่มีความมั่นคงปลอดภัย มีการรักษาความเป็นส่วนตัว สามารถตรวจสอบได้ด้วยกระบวนการเข้ารหัสลับ และสนับสนุนการแลกเปลี่ยนระหว่างกันตามมาตรฐานสากล

สารบัญ

สารบัญรูป

หน้า

สารบัญตาราง

หน้า

ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยโครงสร้างข้อมูลของสารรับรองและสารสำแดงที่ตรวจสอบได้

เพื่อกำหนดโครงสร้างข้อมูลสำหรับสารรับรองที่ตรวจสอบได้ (verifiable credential) และสารสำแดงที่ตรวจสอบได้ (verifiable presentation) และอธิบายความสัมพันธ์ระหว่างบทบาทที่เกี่ยวข้องกับระบบการใช้งานของสารรับรองที่ตรวจสอบได้ เพื่อให้ผู้ใช้งานสามารถใช้สารรับรองที่ตรวจสอบได้ในการแสดงเอกสารหรือข้อมูลประจำตัวต่าง ๆ บนโลกออนไลน์ในลักษณะที่มีความมั่นคงปลอดภัย มีการรักษาความเป็นส่วนตัว สามารถตรวจสอบได้ด้วยกระบวนการเข้ารหัสลับ และสนับสนุนการแลกเปลี่ยนระหว่างกันตามมาตรฐานสากล

อาศัยอำนาจตามความในมาตรา ๕ (๕) แห่งพระราชบัญญัติสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๒ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ จึงประกาศข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยโครงสร้างข้อมูลของสารรับรองและสารสำแดงที่ตรวจสอบได้ เลขที่ ขมธอ. [x-xxxx] ปรากฏตามท้ายประกาศฉบับนี้

ประกาศ ณ วันที่ [กรุณาระบุวันที่ประกาศ]

( )

ผู้อำนวยการ

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ว่าด้วยโครงสร้างข้อมูลของสารรับรอง และสารสำแดงที่ตรวจสอบได้

1. ขอบข่าย

ข้อเสนอแนะมาตรฐานฉบับนี้ กำหนดโครงสร้างข้อมูลสำหรับสารรับรองที่ตรวจสอบได้ (verifiable credential) และสารสำแดงที่ตรวจสอบได้ (verifiable presentation) และอธิบายความสัมพันธ์ระหว่างบทบาทที่เกี่ยวข้องกับระบบการใช้งานของสารรับรองที่ตรวจสอบได้ ซึ่งประกอบด้วยผู้ออกสาร (issuer) ผู้ถือสาร (holder) และผู้ตรวจสอบสาร (verifier) เพื่อให้ผู้ใช้งานสามารถใช้สารรับรองที่ตรวจสอบได้ในการแสดงเอกสารหรือข้อมูลประจำตัวต่าง ๆ บนโลกออนไลน์ในลักษณะที่มีความมั่นคงปลอดภัย มีการรักษาความเป็นส่วนตัว สามารถตรวจสอบได้ด้วยกระบวนการเข้ารหัสลับ และสนับสนุนการแลกเปลี่ยนระหว่างกันตามมาตรฐานสากล

โครงสร้างข้อมูลของสารรับรองที่ตรวจสอบได้สามารถแสดงด้วยวากยสัมพันธ์ (syntax) ได้หลายรูปแบบ อย่างไรก็ตาม ข้อเสนอแนะมาตรฐานฉบับนี้จะแสดงตัวอย่างของโครงสร้างข้อมูลในรูปแบบ JSON (JavaScript Object Notation) และ JSON-LD (JavaScript Object Notation for Linked Data)

2. บทนิยาม

ความหมายของคำที่ใช้ในข้อเสนอแนะมาตรฐานฉบับนี้ มีดังต่อไปนี้

2.1 ข้อกล่าวอ้าง (claim) หมายถึง ลักษณะ (characteristic) หรือข้อความ (statement) เกี่ยวกับเจ้าของข้อมูล (subject)

2.2 สารรับรองที่ตรวจสอบได้ (verifiable credential: VC) หมายถึง ชุดของข้อกล่าวอ้างอย่างน้อยหนึ่งรายการที่ออกโดยผู้ออกสาร (issuer) โดยสารรับรองที่ตรวจสอบได้มีคุณสมบัติที่สามารถตรวจพบการปลอมแปลง (tamper-evident) และตรวจสอบผู้เขียนข้อมูล (authorship) ได้ด้วยกระบวนการเข้ารหัสลับ (cryptographic verification)

<u>ข้อสังเกต</u>: ข้อกล่าวอ้างที่อยู่ในสารรับรองที่ตรวจสอบได้อาจเกี่ยวกับเจ้าของข้อมูล (subject) ที่แตกต่างกัน

2.3 สารสำแดงที่ตรวจสอบได้ (verifiable presentation: VP) หมายถึง ข้อมูลที่ประกอบด้วยสารรับรองที่ตรวจสอบได้อย่างน้อยหนึ่งชุดที่ออกโดยผู้ออกสาร (issuer) จำนวนตั้งแต่หนึ่งคน สำหรับใช้แสดงต่อผู้ตรวจสอบสาร (verifier) โดยสารสำแดงที่ตรวจสอบได้มีคุณสมบัติที่สามารถตรวจพบการปลอมแปลง (tamper-evident) และตรวจสอบผู้เขียนข้อมูล (authorship) ได้ด้วยกระบวนการเข้ารหัสลับ (cryptographic verification)

<u>ข้อสังเกต</u>: สารสำแดงที่ตรวจสอบได้บางประเภทอาจไม่ได้ประกอบด้วยข้อมูลต้นฉบับของสารรับรองที่ตรวจสอบได้ทั้งหมด แต่เป็นข้อมูลที่สังเคราะห์จากข้อมูลต้นฉบับของสารรับรองที่ตรวจสอบได้ (เช่น zero-knowledge proof)

2.4 เอนทิตี (entity) หมายถึง สิ่งใดสิ่งหนึ่งที่มีสภาพดำรงอยู่อย่างชัดเจน เช่น บุคคล องค์กร หรืออุปกรณ์ ซึ่งทำหน้าที่อย่างน้อยหนึ่งบทบาท (role) ในระบบการทำงานของสารรับรองที่ตรวจสอบได้

2.5 เจ้าของข้อมูล (subject) หมายถึง เอนทิตีที่ถูกกล่าวอ้างถึงในข้อกล่าวอ้าง

2.6 ผู้ถือสาร (holder) หมายถึง บทบาทของเอนทิตีที่ทำหน้าที่ถือครองสารรับรองที่ตรวจสอบได้อย่างน้อยหนึ่งชุด เก็บไว้ในกระเป๋าดิจิทัล (credential repository) และใช้สารรับรองที่ตรวจสอบได้นั้นสร้างเป็นสารสำแดงที่ตรวจสอบได้

ข้อสังเกต: ในหลายกรณี ผู้ถือสารจะเป็นเจ้าของข้อมูลของสารรับรองที่ตรวจสอบได้ที่ตนเองถือครองอยู่ เช่น บุคคลถือครองบัตรประจำตัวของตนเอง แต่ในบางกรณี ผู้ถือสารอาจไม่ใช่เจ้าของข้อมูลของสารรับรองที่ตรวจสอบได้ เช่น ผู้ปกครอง (holder) อาจถือครองสารรับรองที่ตรวจสอบได้ของเด็ก (subject) หรือเจ้าของสัตว์เลี้ยง (holder) อาจถือครองสารรับรองที่ตรวจสอบได้ของสัตว์เลี้ยง (subject)

2.7 ผู้ออกสาร (issuer) หมายถึง บทบาทของเอนทิตีที่ทำหน้าที่ยืนยันข้อกล่าวอ้างเกี่ยวกับเจ้าของข้อมูล เพื่อนำข้อกล่าวอ้างนั้นมาสร้างเป็นสารรับรองที่ตรวจสอบได้ และส่งสารรับรองที่ตรวจสอบได้นั้นให้กับผู้ถือสาร

2.8 ผู้ตรวจสอบสาร (verifier) หมายถึง บทบาทของเอนทิตีที่ทำหน้าที่รับสารรับรองที่ตรวจสอบได้อย่างน้อยหนึ่งชุดซึ่งอาจอยู่ในรูปของสารสำแดงที่ตรวจสอบได้เพื่อนำมาประมวลผล

2.9 ระบบจัดเก็บข้อมูล (verifiable data registry) หมายถึง บทบาทของระบบที่ทำหน้าที่เป็นสื่อกลางในการสร้างและตรวจสอบข้อมูลที่จำเป็นต่อการใช้งานสารรับรองที่ตรวจสอบได้ เช่น ตัวระบุ (identifier) กุญแจสาธารณะ (public key) รายการเพิกถอน (revocation registry) และโครงสร้างข้อมูล (schema)

ข้อสังเกต: ตัวอย่างของระบบจัดเก็บข้อมูล เช่น ฐานข้อมูลแบบรวมศูนย์หรือฐานข้อมูลแบบกระจายศูนย์ ทั้งนี้ การใช้งานสารรับรองที่ตรวจสอบได้อาจประกอบด้วยระบบจัดเก็บข้อมูลมากกว่าหนึ่งประเภทก็ได้

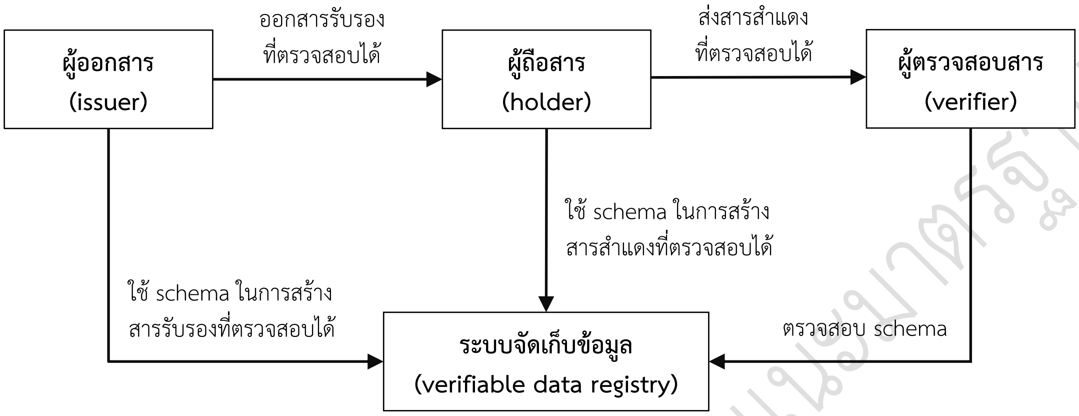
2.10 กระเป๋าดิจิทัล (credential repository) หมายถึง โปรแกรมที่เก็บรักษาและควบคุมการเข้าถึงข้อมูลสารรับรองที่ตรวจสอบได้ของผู้ถือสาร

2.11 การตรวจสอบ (verification) หมายถึง การตรวจสอบความแท้จริง (authenticity) และสถานะการใช้งาน (validity) ของสารรับรองที่ตรวจสอบได้หรือสารสำแดงที่ตรวจสอบได้ และรวมถึงการตรวจสอบความสอดคล้อง (conformance) ตามข้อกำหนดหรือมาตรฐาน

3. ภาพรวมของสารรับรองที่ตรวจสอบได้และสารสำแดงที่ตรวจสอบได้

3.1 หลักการทำงานของสารรับรองที่ตรวจสอบได้

ระบบการใช้งานสารรับรองที่ตรวจสอบได้ ประกอบด้วยบทบาทของเอนทิตีและการปฏิสัมพันธ์ระหว่างกันตามรูปที่ 1



รูปที่ 1 บทบาทและการปฏิสัมพันธ์ในระบบการใช้งานสารรับรองที่ตรวจสอบได้

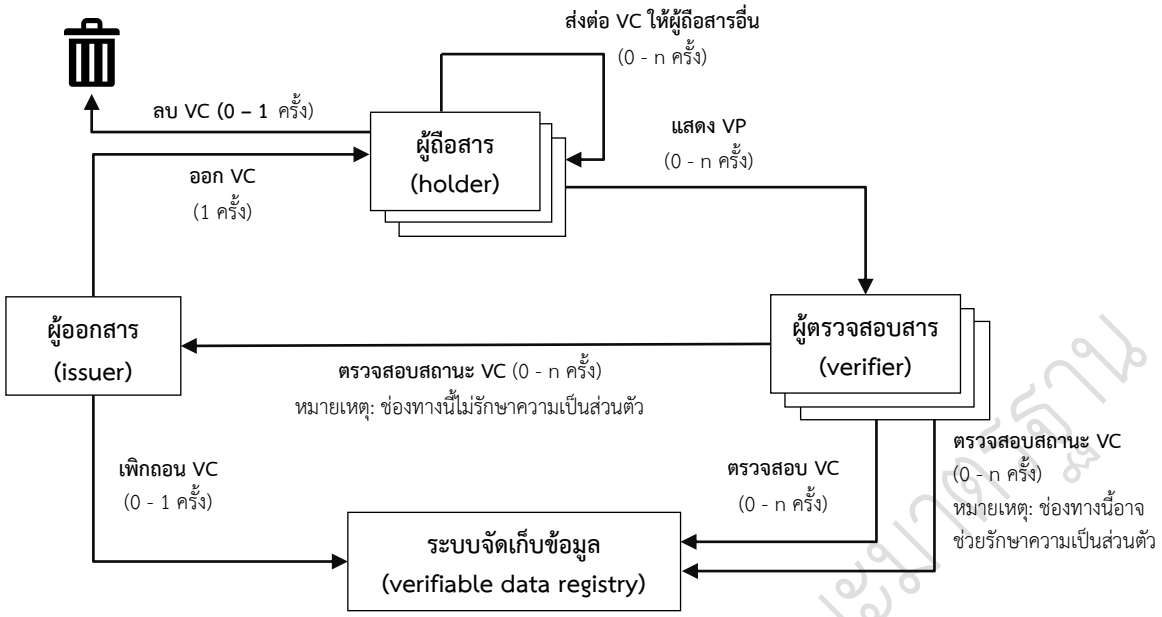
– ผู้ออกสาร (issuer) คือ บทบาทของเอนทิตีที่ทำหน้าที่ยืนยันข้อกล่าวอ้างเกี่ยวกับเจ้าของข้อมูลเพื่อนำข้อกล่าวอ้างนั้นมาสร้างเป็นสารรับรองที่ตรวจสอบได้ และส่งสารรับรองที่ตรวจสอบได้นั้นให้กับผู้ถือสาร

– ผู้ถือสาร (holder) คือ บทบาทของเอนทิตีที่ทำหน้าที่ถือครองสารรับรองที่ตรวจสอบได้ และใช้สารรับรองที่ตรวจสอบได้นั้นสร้างเป็นสารสำแดงที่ตรวจสอบได้

– ผู้ตรวจสอบสาร (verifier) คือ บทบาทของเอนทิตีที่ทำหน้าที่รับสารรับรองที่ตรวจสอบได้ ซึ่งอาจอยู่ในรูปของสารสำแดงที่ตรวจสอบได้เพื่อนำมาประมวลผล

– ระบบจัดเก็บข้อมูล (verifiable data registry) คือ บทบาทของระบบที่ทำหน้าที่เป็นสื่อกลางในการสร้างและตรวจสอบข้อมูลที่จำเป็นต่อการใช้งานสารรับรองที่ตรวจสอบได้และสารสำแดงที่ตรวจสอบได้ เช่น
   - ตัวระบุ (identifier) ของสารรับรองที่ตรวจสอบได้ สารสำแดงที่ตรวจสอบได้ ผู้ออกสาร ผู้ถือสาร หรือผู้ตรวจสอบสาร
   - กุญแจสาธารณะ (public key) ของผู้ออกสาร ผู้ถือสาร หรือผู้ตรวจสอบสาร
   - รายการเพิกถอน (revocation registry) ของสารรับรองที่ตรวจสอบได้หรือสารสำแดงที่ตรวจสอบได้
   - โครงสร้างข้อมูล (schema) ของสารรับรองที่ตรวจสอบได้หรือสารสำแดงที่ตรวจสอบได้

ทั้งนี้ กิจกรรมที่แต่ละบทบาทดำเนินการต่อสารรับรองที่ตรวจสอบได้สามารถแสดงเป็นแผนภาพวัฏจักรข้อมูลตามรูปที่ 2



รูปที่ 2 แผนภาพแสดงวัฏจักรข้อมูลในระบบการใช้งานสารรับรองที่ตรวจสอบได้

- ผู้ออกสารออกสารรับรองที่ตรวจสอบได้ให้แก่ผู้ถือสาร ซึ่งกิจกรรมนี้จะเกิดขึ้นก่อนกิจกรรมอื่น ๆ ของสารรับรองที่ตรวจสอบได้
- ผู้ถือสารอาจส่งต่อสารรับรองที่ตรวจสอบได้อย่างน้อยหนึ่งชุดให้แก่ผู้ถือสารอื่นได้
- ผู้ถือสารแสดงสารรับรองที่ตรวจสอบได้อย่างน้อยหนึ่งชุดให้แก่ผู้ตรวจสอบสาร ซึ่งอาจแสดงอยู่ในรูปของสารสำแดงที่ตรวจสอบได้
- ผู้ตรวจสอบสารตรวจสอบความถูกต้องของสารสำแดงที่ตรวจสอบได้และสารรับรองที่ตรวจสอบได้ที่นำมาแสดง และควรรวมถึงการตรวจสอบสถานะการเพิกถอนของสารรับรองที่ตรวจสอบได้นั้นด้วย
- ผู้ออกสารอาจเพิกถอนสารรับรองที่ตรวจสอบได้
- ผู้ถือสารอาจลบสารรับรองที่ตรวจสอบได้

อย่างไรก็ตาม กิจกรรมต่าง ๆ ข้างต้นไม่จำเป็นต้องเกิดขึ้นตามลำดับ และกิจกรรมบางอย่างอาจเกิดขึ้นมากกว่าหนึ่งครั้ง โดยอาจเกิดขึ้นทันทีหรือในภายหลัง

3.2 ข้อกำหนดการใช้งานสารรับรองที่ตรวจสอบได้

<u>ข้อกำหนดของผู้ออกสาร (issuer)</u> มีดังต่อไปนี้

- ผู้ออกสารสามารถออกสารรับรองที่ตรวจสอบได้เกี่ยวกับเจ้าของข้อมูลใด ๆ
- สารรับรองที่ตรวจสอบได้ใช้แสดงข้อความที่สร้างขึ้นโดยผู้ออกสารในรูปแบบที่สามารถตรวจพบการปลอมแปลงและมีการรักษาความเป็นส่วนตัว
- ผู้ออกสารสามารถออกสารรับรองที่ตรวจสอบได้ที่สามารถเพิกถอนในภายหลังได้
- การเพิกถอนสารรับรองที่ตรวจสอบได้โดยผู้ออกสารไม่ควรเปิดเผยข้อมูลใด ๆ ที่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูล ผู้ถือสาร ผู้ตรวจสอบสาร หรือสารรับรองที่ตรวจสอบได้อันใดอันหนึ่ง
- ผู้ออกสารสามารถเปิดเผยเหตุผลในการเพิกถอนสารรับรองที่ตรวจสอบได้

- การเพิกถอนสารรับรองที่ตรวจสอบได้โดยผู้ออกสารควรแบ่งแยกระหว่างการเพิกถอนที่เกิดจากปัญหาด้านความสมบูรณ์ของการเข้ารหัสลับ (cryptographic integrity) กับการเพิกถอนที่เกิดจากการเปลี่ยนสถานะของสารรับรองที่ตรวจสอบได้
- ผู้ออกสารอาจมีบริการต่ออายุหรือปรับสารรับรองที่ตรวจสอบได้ให้เป็นปัจจุบัน

ข้อกำหนดของผู้ถือสาร (holder) มีดังต่อไปนี้

- ผู้ถือสารสามารถรับสารรับรองที่ตรวจสอบได้จากเอนทิตีใด ๆ
- ผู้ถือสารสามารถจัดเก็บสารรับรองที่ตรวจสอบได้ไว้ที่ใดก็ได้ โดยจะไม่ส่งผลกระทบต่อการตรวจสอบและไม่จำเป็นต้องให้ผู้ออกสารทราบถึงข้อมูลใด ๆ เกี่ยวกับสถานที่จัดเก็บข้อมูลหรือเวลาที่มีการเข้าถึงข้อมูลของสารรับรองที่ตรวจสอบได้
- ผู้ถือสารสามารถติดต่อกับผู้ออกสารและผู้ตรวจสอบสารผ่านโปรแกรม (user agent) ที่เป็นสื่อกลางในการติดต่อสื่อสารระหว่างผู้ถือสาร ผู้ออกสาร และผู้ตรวจสอบสาร
- ผู้ถือสารสามารถรวบรวมสารรับรองที่ตรวจสอบได้หลายชุดจากผู้ออกสารที่แตกต่างกันและสร้างเป็นสารสำแดงที่ตรวจสอบได้
- ผู้ถือสารสามารถแสดงสารสำแดงที่ตรวจสอบได้ให้ผู้ตรวจสอบสารตรวจสอบได้โดยไม่ต้องเปิดเผยตัวตนของผู้ตรวจสอบสารต่อผู้ออกสาร
- ผู้ถือสารสามารถแสดงสารสำแดงที่ตรวจสอบได้ต่อผู้ตรวจสอบสารใด ๆ โดยไม่ส่งผลกระทบต่อความถูกต้องแท้จริงของข้อกล่าวอ้างและไม่ต้องเปิดเผยการกระทำดังกล่าวต่อผู้ออกสาร

ข้อกำหนดของผู้ตรวจสอบสาร (verifier) มีดังต่อไปนี้

- ผู้ตรวจสอบสารสามารถตรวจสอบสารสำแดงที่ตรวจสอบได้จากผู้ถือสารใด ๆ
- ผู้ตรวจสอบสารสามารถตรวจสอบความถูกต้องแท้จริงของสารรับรองที่ตรวจสอบได้ที่ออกโดยเจ้าของข้อมูลใด ๆ ได้
- การตรวจสอบสารรับรองที่ตรวจสอบได้และสารสำแดงที่ตรวจสอบได้ไม่ควรจะอาศัยการติดต่อกันโดยตรงระหว่างเจ้าของข้อมูลและผู้ตรวจสอบสาร
- การตรวจสอบสารรับรองที่ตรวจสอบได้และสารสำแดงที่ตรวจสอบได้ไม่ควรจะเปิดเผยตัวตนของผู้ตรวจสอบสารต่อผู้ออกสาร

ข้อกำหนดของการเลือกเปิดเผยข้อมูลบางส่วน (selective disclosure) มีดังต่อไปนี้

- ผู้ออกสารสามารถออกสารรับรองที่ตรวจสอบได้ที่รองรับการเลือกเปิดเผยข้อมูลบางส่วนได้
- หากเป็นสารรับรองที่ตรวจสอบได้ที่รองรับการเลือกเปิดเผยข้อมูลบางส่วน ผู้ถือสารจะสามารถแสดงการพิสูจน์ให้ทราบข้อเท็จจริงเกี่ยวกับข้อกล่าวอ้างได้ โดยไม่ต้องเปิดเผยข้อกล่าวอ้างทั้งหมดที่อยู่ในสารรับรองที่ตรวจสอบได้
- สารสำแดงที่ตรวจสอบได้อาจอยู่ในรูปแบบการเปิดเผยค่าคุณสมบัติที่แท้จริงของสารรับรองที่ตรวจสอบได้ หรือรูปแบบการแสดงค่าความจริง (boolean) ที่ใช้ยืนยันค่าคุณสมบัติโดยไม่ต้องเปิดเผยค่าคุณสมบัติที่แท้จริงของสารรับรองที่ตรวจสอบได้ (เช่น ค่าความจริงที่ใช้ยืนยันว่าเจ้าของข้อมูลมีอายุมากกว่า 20 ปีบริบูรณ์โดยไม่ต้องเปิดเผยอายุที่แท้จริงของเจ้าของข้อมูล)

3.3 รูปแบบการรับรองความเชื่อถือ (trust model)

รูปแบบการรับรองความเชื่อถือของระบบการใช้งานสารรับรองที่ตรวจสอบได้แตกต่างจากรูปแบบการรับรองความเชื่อถืออื่น ๆ ที่อาศัยความไว้วางใจกันระหว่างผู้ออกสารและผู้ตรวจสอบสาร เนื่องจากในการใช้งานสารรับรองที่ตรวจสอบได้นั้น ผู้ออกสารไม่จำเป็นต้องรู้หรือเชื่อถือเกี่ยวกับผู้ตรวจสอบสาร รวมถึงผู้ออกสารและผู้ตรวจสอบสารไม่จำเป็นต้องเชื่อถือกระเป๋าดิจิทัลที่เก็บรักษาสารรับรองที่ตรวจสอบได้

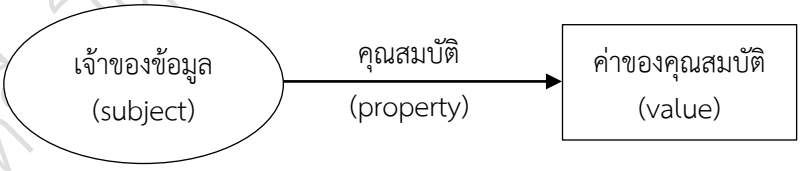
รูปแบบการรับรองความเชื่อถือของระบบการใช้งานสารรับรองที่ตรวจสอบได้อาศัยความสัมพันธ์หรือความไว้วางใจกันระหว่างบทบาทของเอนทิตี ดังนี้

- ผู้ตรวจสอบสารเชื่อถือผู้ออกสารในการออกสารรับรองที่ตรวจสอบได้ โดยอาศัยวิธีการที่แสดงและตรวจสอบได้ว่าผู้ออกสารเป็นผู้สร้างสารรับรองที่ตรวจสอบได้ดังกล่าวจริง หรืออาศัยวิธีการอื่นที่น่าเชื่อถือและเหมาะสมกับความเสี่ยงที่ผู้ตรวจสอบสารยอมรับ
- เอนทิตีทั้งหมดเชื่อถือระบบจัดเก็บข้อมูลว่ามีการจัดเก็บข้อมูลของแต่ละเอนทิตีอย่างถูกต้องและสามารถตรวจพบการปลอมแปลงของข้อมูลที่บันทึกได้
- ผู้ถือสารและผู้ตรวจสอบสารเชื่อถือผู้ออกสารว่าออกสารรับรองที่ตรวจสอบได้ที่มีความถูกต้องแท้จริงเกี่ยวกับเจ้าของข้อมูลและสามารถเพิกถอนสารรับรองที่ตรวจสอบได้ในภายหลังได้ตามความเหมาะสม
- ผู้ถือสารเชื่อถือกระเป๋าดิจิทัลว่ามีการเก็บรักษาสารรับรองที่ตรวจสอบได้อย่างมั่นคงปลอดภัย ไม่เปิดเผยสารรับรองที่ตรวจสอบได้แก่บุคคลอื่น และไม่ทำให้สารรับรองที่ตรวจสอบได้เสียหายหรือสูญหายขณะที่มีการเก็บรักษาในกระเป๋าดิจิทัล

3.4 แบบจำลองข้อมูลของสารรับรองที่ตรวจสอบได้และสารสำแดงที่ตรวจสอบได้

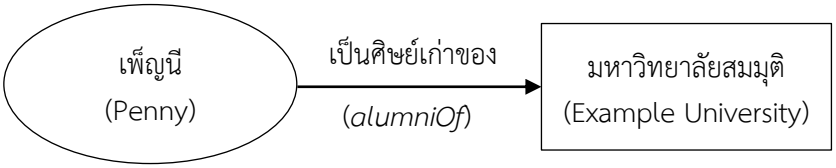
3.4.1 ข้อกล่าวอ้าง (claim)

ข้อกล่าวอ้าง (claim) คือ ลักษณะหรือข้อความเกี่ยวกับเจ้าของข้อมูล โดยแบบจำลองข้อมูลของข้อกล่าวอ้างสามารถแสดงด้วยความสัมพันธ์ในรูปแบบ เจ้าของข้อมูล (subject) – คุณสมบัติ (property) – ค่าของคุณสมบัติ (value) ตามรูปที่ 3



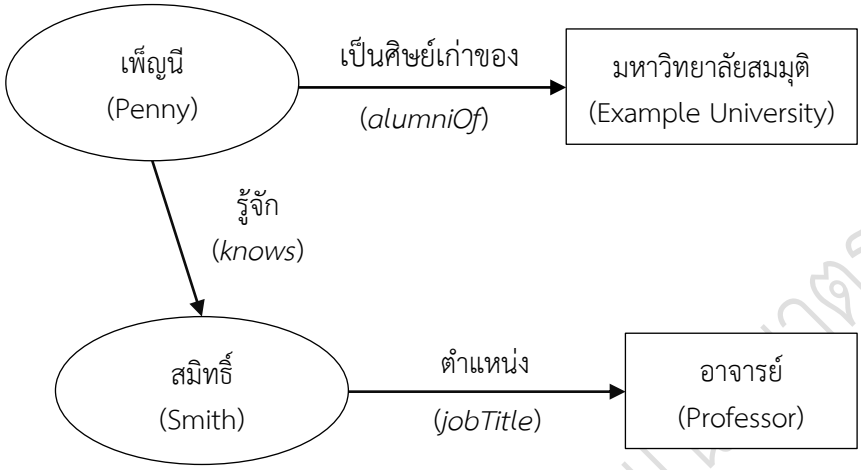
รูปที่ 3 แบบจำลองข้อมูลของข้อกล่าวอ้าง

ตัวอย่างของข้อกล่าวอ้างแสดงข้อความ “เพ็ญนีเป็นศิษย์เก่าของมหาวิทยาลัยสมมุติ” (“Penny is an alumna of Example University.”) สามารถแสดงตามแบบจำลองข้างต้นได้ตามรูปที่ 4



รูปที่ 4 ข้อกล่าวอ้างแสดงข้อความ “เพ็ญนีเป็นศิษย์เก่าของมหาวิทยาลัยสมมุติ”

ทั้งนี้ ข้อกล่าวอ้างสามารถนำมาเชื่อมโยงกันเป็นกราฟ (graph) สำหรับใช้แสดงความสัมพันธ์ของข้อมูลต่าง ๆ กับเจ้าของข้อมูล ตัวอย่างเช่น การเชื่อมโยงข้อกล่าวอ้างก่อนหน้าในรูปที่ 4 กับข้อกล่าวอ้างที่แสดงข้อความ “เพ็ญนีรู้จักสมิทธิ์” (“Penny knows Smith.”) และ “สมิทธิ์มีตำแหน่งเป็นอาจารย์” (“Smith is a professor.”) ตามรูปที่ 5

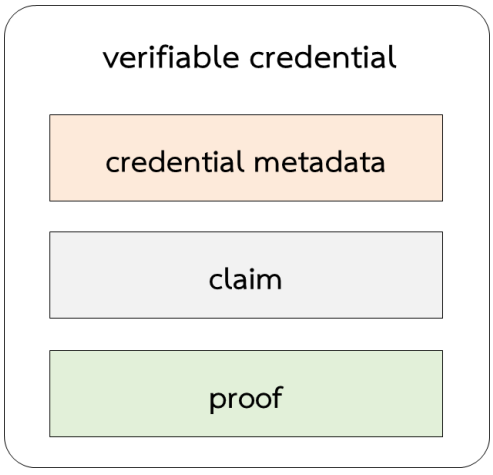


รูปที่ 5 การเชื่อมโยงกันระหว่างข้อกล่าวอ้างเพื่อสร้างเป็นกราฟข้อมูล

3.4.2 สารรับรองที่ตรวจสอบได้ (verifiable credential)

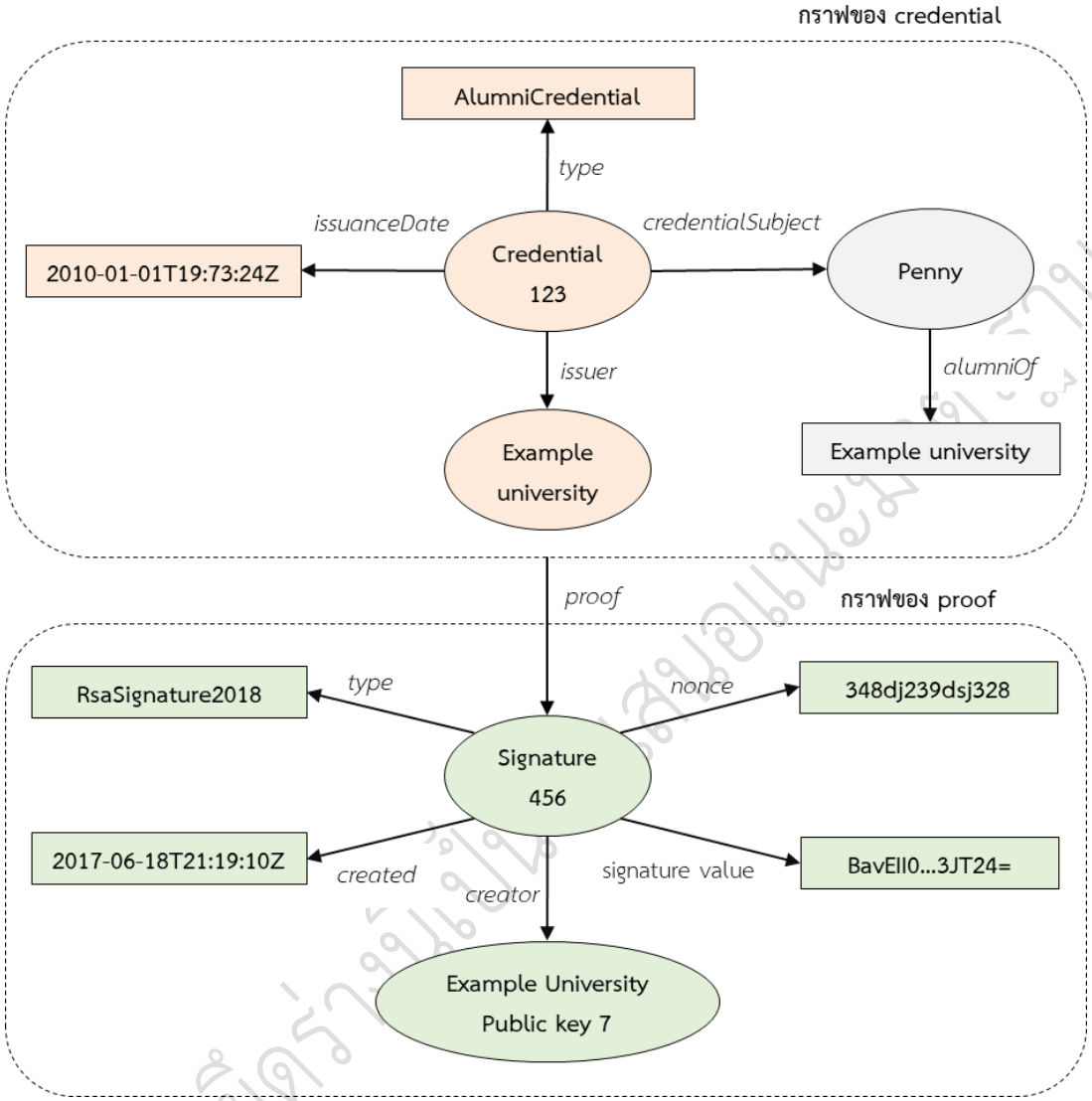
สารรับรองที่ตรวจสอบได้ (verifiable credential: VC) คือ ชุดของข้อกล่าวอ้างอย่างน้อยหนึ่งรายการที่ออกโดยผู้ออกสารเดียวกัน โดยสารรับรองที่ตรวจสอบได้จะมีคุณสมบัติที่สามารถตรวจพบการปลอมแปลงและตรวจสอบผู้เขียนข้อมูลได้ด้วยกระบวนการเข้ารหัสลับ สารรับรองที่ตรวจสอบได้อาจประกอบด้วยตัวระบุ (identifier) และคำอธิบายข้อมูล (metadata) เช่น ผู้ออกสาร วันที่ออกสาร และวันที่สารสิ้นอายุ ซึ่งคำอธิบายข้อมูลอาจมีการลงลายมือชื่อโดยผู้ออกสารก็ได้

ทั้งนี้ องค์ประกอบพื้นฐานของสารรับรองที่ตรวจสอบได้สามารถแสดงตามรูปที่ 6 ซึ่งประกอบด้วย 3 ส่วน ได้แก่ (1) คำอธิบายข้อมูลของสารรับรองที่ตรวจสอบได้ (credential metadata) (2) ข้อกล่าวอ้าง (claim) และ (3) ข้อพิสูจน์ (proof) ซึ่งโดยทั่วไปจะเป็นลายมือชื่อดิจิทัลของผู้ออกสาร



รูปที่ 6 องค์ประกอบพื้นฐานของสารรับรองที่ตรวจสอบได้

นอกจากนี้ สารรับรองที่ตรวจสอบได้สามารถแสดงเป็นกราฟข้อมูลได้ตามรูปที่ 7



รูปที่ 7 กราฟข้อมูลของสารรับรองที่ตรวจสอบได้

ตัวอย่างของสารรับรองที่ตรวจสอบได้แสดงกรณีศึกษาเมื่อเพ็ญนีไปซื้อสินค้าจากร้านสหกรณ์มหาวิทยาลัยสมมุติ โดยจะได้รับส่วนลดเมื่อเพ็ญนีพิสูจน์ได้ว่าตนเองเคยศึกษา ณ มหาวิทยาลัยดังกล่าว ซึ่งทางมหาวิทยาลัยได้ออกสารรับรองที่ตรวจสอบได้เพื่อรับรองความเป็นศิษย์เก่าให้แก่เพ็ญนี และเพ็ญนีเก็บสารรับรองที่ตรวจสอบได้นั้นไว้ในกระเป๋าดิจิทัลของตนเอง ตัวอย่างของสารรับรองที่ตรวจสอบได้ข้างต้นในรูปแบบ JSON-LD เป็นดังนี้

ตัวอย่างที่ 1 ตัวอย่างของสารรับรองที่ตรวจสอบได้ในรูปแบบ JSON-LD

```
{
 // บริบท ซึ่งประกาศนิยามของสมนามที่จะใช้ 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",              // ตัวระบุของ credential
 "type": ["VerifiableCredential", "AlumniCredential"],    // ประเภทของ credential
 "issuer": "https://example.edu/issuers/565049",          // ผู้ออกสาร
 "issuanceDate": "2010-01-01T19:73:24Z",                  // วันที่ออกเอกสาร
 // เจ้าของข้อมูลในสารรับรองที่ตรวจสอบได้ โดยในกรณีนี้มีเพียงเอนทิตีเดียว
 "credentialSubject": {
  // ตัวระบุของเจ้าของข้อมูล โดยในกรณีนี้ใช้ DID [1]
  "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
  // ข้อกล่าวอ้างเกี่ยวกับเจ้าของข้อมูล
  "alumniOf": {
   "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",
   "name": [{
    "value": "Example University",
    "lang": "en"
   }, {
    "value": "มหาวิทยาลัยสมมุติ",
    "lang": "th"
   }]
  }
 },
 // ลายมือชื่อดิจิทัล ซึ่งช่วยให้สามารถตรวจพบการปลอมแปลงของสารรับรองที่ตรวจสอบได้
 "proof": {
  // กระบวนการเข้ารหัสลับที่ใช้ในการลงลายมือชื่อ
  "type": "RsaSignature2018",
  // วันที่ลงลายมือชื่อ
  "created": "2017-06-18T21:19:10Z",
  // วัตถุประสงค์ของการลงลายมือชื่อ
  "proofPurpose": "assertionMethod",
  // ตัวระบุของกุญแจสาธารณะที่ใช้ในการตรวจสอบลายมือชื่อ
  "verificationMethod": "https://example.edu/issuers/keys/1",
  // ค่าของลายมือชื่อดิจิทัล
  "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..TCYt5XsITJX
  1CxPCT8yAV-TVkIEq_PbChOMqsLfRoPsnsgw5WEuts01mq-pQy7UJiN5mgRxD-WUcX
  16dUEMGlv50aqzpqh4Qktb3rk-BuQy72IFLOqV0G_zS245-kronKb78cPN25DGlcTwLtjP
  AYuNzVBAh4vGHSrQyHUdBBPM"
 }
}
```

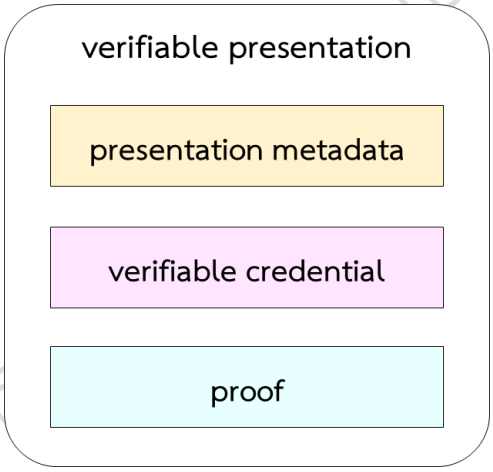
[1] decentralized identifier (DID) เป็นตัวระบุที่ใช้ URL ในการเชื่อมโยงกับเอนทิตี โดยทั่วไป DID จะนำมาใช้ในสารรับรองที่ตรวจสอบได้เพื่อแสดงความเชื่อมโยงไปยังเจ้าของข้อมูลที่เกี่ยวข้อง ซึ่งทำให้สามารถส่งต่อหรือโอนย้ายสารรับรองที่ตรวจสอบได้จากกระเป๋าดิจิทัลหนึ่งไปยังกระเป๋าดิจิทัลอีกอันหนึ่งได้โดยไม่จำเป็นต้องออกสารรับรองที่ตรวจสอบได้ชุดใหม่ อย่างไรก็ตาม สารรับรองที่ตรวจสอบได้ไม่จำเป็นต้องใช้ตัวระบุเป็น DID ก็ได้

3.4.3 สารสำแดงที่ตรวจสอบได้ (verifiable presentation)

สารสำแดงที่ตรวจสอบได้ (verifiable presentation: VP) คือ ข้อมูลที่รวบรวมจากสารรับรองที่ตรวจสอบได้อย่างน้อยหนึ่งชุด ซึ่งอาจเป็นข้อมูลต้นฉบับตามที่ปรากฏในสารรับรองที่ตรวจสอบได้ หรือเป็นข้อมูลที่สังเคราะห์จากสารรับรองที่ตรวจสอบได้เพื่อรักษาความเป็นส่วนตัว โดยสารสำแดงที่ตรวจสอบได้จะมีคุณสมบัติที่สามารถตรวจพบการปลอมแปลงและตรวจสอบผู้เขียนข้อมูลได้ด้วยกระบวนการเข้ารหัสลับ

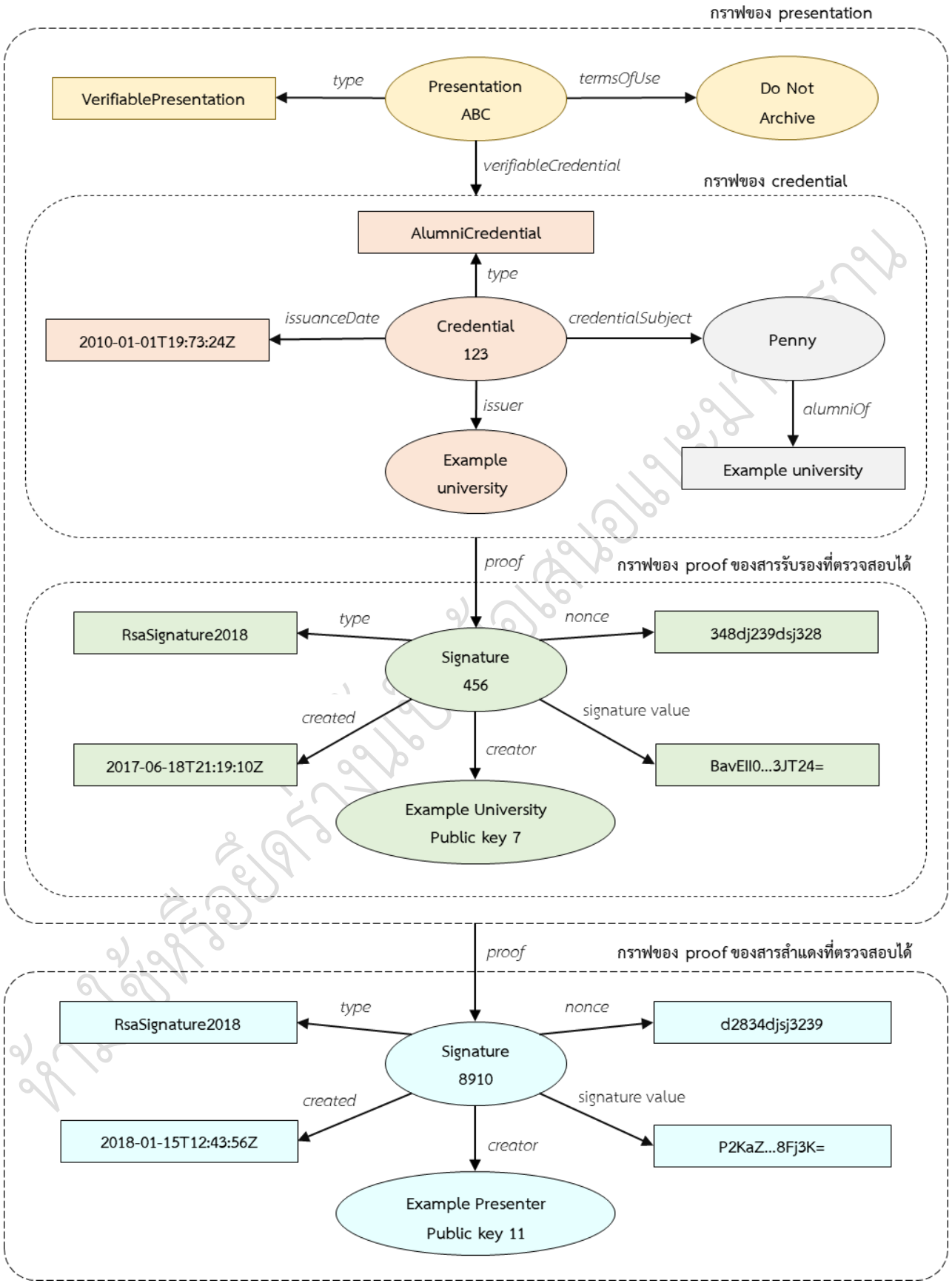
โดยทั่วไป ข้อมูลในสารสำแดงที่ตรวจสอบได้ชุดหนึ่งจะเป็นข้อมูลเกี่ยวกับเจ้าของข้อมูลเดียวกัน แต่อาจมีการออกให้โดยผู้ออกสารหลายราย อย่างไรก็ตาม ในกรณีของเอนทิตีที่เป็นองค์กร สารสำแดงที่ตรวจสอบได้อาจประกอบด้วยสารรับรองที่ตรวจสอบได้หลายชุดของเจ้าของข้อมูลที่แตกต่างกัน ซึ่งเจ้าของข้อมูลเหล่านั้นอาจจะมีความเกี่ยวข้องกันหรือไม่เกี่ยวข้องกันก็ได้

ทั้งนี้ องค์ประกอบพื้นฐานของสารสำแดงที่ตรวจสอบได้สามารถแสดงตามรูปที่ 8 ซึ่งประกอบด้วย 3 ส่วน ได้แก่ (1) คำอธิบายข้อมูลของสารสำแดงที่ตรวจสอบได้ (presentation metadata) (2) สารรับรองที่ตรวจสอบได้ (verifiable credential) และ (3) ข้อพิสูจน์ (proof) ซึ่งโดยทั่วไปจะเป็นลายมือชื่อดิจิทัลของผู้ถือสาร



รูปที่ 8 องค์ประกอบพื้นฐานของสารสำแดงที่ตรวจสอบได้

นอกจากนี้ สารสำแดงที่ตรวจสอบได้สามารถแสดงเป็นกราฟข้อมูลได้ตามรูปที่ 9 ซึ่งมีคุณสมบัติชื่อ *verifiableCredential* ที่ใช้อ้างอิงถึงสารรับรองที่ตรวจสอบได้อย่างน้อยหนึ่งชุด โดยสารรับรองที่ตรวจสอบได้แต่ละชุดจะประกอบด้วยคำอธิบายข้อมูลของสารรับรองที่ตรวจสอบได้ (credential metadata) ข้อกล่าวอ้าง (claim) และข้อพิสูจน์ (proof)



รูปที่ 9 กราฟข้อมูลของสารสำแดงที่ตรวจสอบได้

จากกรณีศึกษาในตัวอย่างที่ 1 เมื่อเพ็ญนีได้รับสารรับรองที่ตรวจสอบได้มาเก็บไว้ในกระเป๋าดิจิทัลของตนเองแล้ว ต่อมาจะขอรับส่วนลดจากร้านสหกรณ์มหาวิทยาลัยสมมุติซึ่งเป็นผู้ตรวจสอบสาร ร้านสหกรณ์จะส่งคำร้องขอสารรับรองที่ตรวจสอบได้ที่ออกโดยมหาวิทยาลัยผ่านไปยังกระเป๋าดิจิทัลของเพ็ญนี และกระเป๋าดิจิทัลจะถามเพ็ญนีว่าต้องการใช้สารรับรองที่ตรวจสอบได้ที่มีอยู่หรือไม่ เมื่อเพ็ญนีตอบตกลง สารรับรองที่ตรวจสอบได้จะถูกนำมาใช้สร้างเป็นสารสำแดงที่ตรวจสอบได้แล้วส่งต่อไปให้ร้านสหกรณ์ดำเนินการตรวจสอบ ตัวอย่างของสารสำแดงที่ตรวจสอบได้ข้างต้นในรูปแบบ JSON-LD เป็นดังนี้

ตัวอย่างที่ 2 ตัวอย่างของสารสำแดงที่ตรวจสอบได้ในรูปแบบ JSON-LD

```
{
 "@context": [
  "https://www.w3.org/2018/credentials/v1",
  "https://www.w3.org/2018/credentials/examples/v1"
 ],
 "type": "VerifiablePresentation",
 // สารรับรองที่ตรวจสอบได้ 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 ซึ่งเป็นผู้ถือสารรับรองที่ตรวจสอบได้และเป็นผู้ออกสารสำแดงที่ตรวจสอบได้
```

```
  "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"
  }
}
```

216

4. โครงสร้างข้อมูลของสารรับรองที่ตรวจสอบได้และสารสำแดงที่ตรวจสอบได้

โครงสร้างข้อมูลของสารรับรองที่ตรวจสอบได้และสารสำแดงที่ตรวจสอบได้ ประกอบด้วยคุณสมบัติต่าง ๆ (property) ซึ่งจะแบ่งออกเป็นคุณสมบัติพื้นฐาน (รายละเอียดตามหัวข้อ 4.1 และ 4.2) และคุณสมบัติเพิ่มเติม (รายละเอียดตามภาคผนวก ก.)

4.1 คุณสมบัติพื้นฐานของสารรับรองที่ตรวจสอบได้

4.1.1 บริบท (context)

@context คือ คุณสมบัติที่ใช้เชื่อมโยงชื่อคุณสมบัติต่าง ๆ ในสารรับรองที่ตรวจสอบได้หรือสารสำแดงที่ตรวจสอบได้เข้ากับ URI เพื่อให้ระบบคอมพิวเตอร์สามารถแลกเปลี่ยนข้อมูลและเข้าใจความหมายหรือบริบทของคุณสมบัติต่าง 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 10 การเปรียบเทียบระหว่างการใช้ @context กับการใช้ URI แบบเต็มรูป

ข้อกำหนดของคุณสมบัติ *@context*

- สารรับรองที่ตรวจสอบได้และสารสำแดงที่ตรวจสอบได้ต้องมีคุณสมบัติ *@context*
- *@context* ต้องมีค่าเป็น URI หรือรายการของ URI แบบมีลำดับ (ordered) โดยมี URI ลำดับแรกเป็นบริบทพื้นฐาน (base context) คือ https://www.w3.org/2018/credentials/v1 ส่วน URI ลำดับถัดมาเป็นข้อมูลบริบทที่มีคุณสมบัติอื่นนอกเหนือจากคุณสมบัติในบริบทพื้นฐาน
- URI แต่ละรายการใน *@context* ควรเชื่อมโยงไปยังเอกสารที่มีข้อมูลในรูปแบบที่คอมพิวเตอร์สามารถนำไปประมวลผลได้

ตัวอย่างที่ 3 การใช้งานของคุณสมบัติ *@context*

```
{
  "@context": [
    // URI ของบริบทพื้นฐาน
    "https://www.w3.org/2018/credentials/v1",
    // URI ของบริบทที่มีคุณสมบัติอื่นนอกเหนือจากคุณสมบัติในบริบทพื้นฐาน
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  "id": "http://example.edu/credentials/58473",
```

```
  "type": ["VerifiableCredential", "AlumniCredential"],
  "credentialSubject": { ... },
  "proof": { ... }
}
```

4.1.2 ตัวระบุ (identifier)

id คือ คุณสมบัติที่ใช้แสดงตัวระบุสำหรับอ้างอิงวัตถุที่เฉพาะเจาะจงในสารรับรองที่ตรวจสอบได้ เช่น บุคคล ผลิตภัณฑ์ หรือองค์กร เพื่อให้สามารถกล่าวถึงถึงวัตถุอันเดียวกันได้อย่างชัดเจน

ข้อกำหนดของคุณสมบัติ *id*

- สารรับรองที่ตรวจสอบได้อาจมี *id* หรือไม่ก็ได้ และถ้ามี *id* ต้องมีเพียงค่าเดียวเท่านั้น
- *id* ต้องใช้แสดงตัวระบุที่คาดว่าบุคคลอื่นจะนำไปใช้เมื่อต้องการอ้างอิงถึงวัตถุที่ถูกระบุด้วยตัวระบุดังกล่าว
- ค่าของ *id* ต้องเป็น URI และ URI ใน *id* นี้ควรเชื่อมโยงไปยังเอกสารที่มีข้อมูลในรูปแบบที่คอมพิวเตอร์สามารถนำไปประมวลผลได้เกี่ยวกับ *id*

ตัวอย่างที่ 4 การใช้งานของคุณสมบัติ *id*

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

4.1.3 ประเภท (type)

type คือ คุณสมบัติที่ใช้แสดงประเภทของชุดข้อมูล (object) เพื่อพิจารณาว่าข้อมูลมีความเหมาะสมหรือไม่ โดยชุดข้อมูลที่ต้องระบุคุณสมบัติ *type* จะแสดงตามตารางที่ 1

ข้อกำหนดของคุณสมบัติ *type*

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

ตัวอย่างที่ 5 การใช้งานของคุณสมบัติ *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 ข้อมูลที่ต้องระบุคุณสมบัติ *type*

ชื่อชุดข้อมูล (object)	ประเภทของชุดข้อมูล
verifiable credential	สารรับรองที่ตรวจสอบได้ และประเภทเฉพาะของสารรับรองที่ตรวจสอบได้ (ถ้ามี) "type": ["VerifiableCredential", "UniversityDegreeCredential"]
verifiable presentation	สารสำแดงที่ตรวจสอบได้ และประเภทเฉพาะของสารสำแดงที่ตรวจสอบได้ (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 ผู้ออกสาร (issuer)

issuer คือ คุณสมบัติที่ใช้แสดงผู้ออกสารของสารรับรองที่ตรวจสอบได้

ข้อกำหนดของคุณสมบัติ *issuer*

- สารรับรองที่ตรวจสอบได้ต้องมี *issuer*
- ค่าของ *issuer* ต้องเป็น URI หรือชุดข้อมูลที่มีคุณสมบัติ *id*

- URI ใน *issuer* หรือ *id* ของ *issuer* ควรเชื่อมโยงไปยังเอกสารที่มีข้อมูลในรูปแบบที่คอมพิวเตอร์สามารถนำไปประมวลผลได้เกี่ยวกับ *issuer*

ตัวอย่างที่ 6 การใช้งานของคุณสมบัติ *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 สามารถเชื่อมโยงชุดข้อมูลกับคุณสมบัติ *issuer* เพื่อแสดงข้อมูลเพิ่มเติมเกี่ยวกับผู้ออกสารดังนี้

ตัวอย่างที่ 7 การใช้งานของคุณสมบัติ *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 วันที่ออกสาร (issuance date) และวันที่สารสิ้นอายุ (expiration date)

issuanceDate และ *expirationDate* คือ คุณสมบัติที่ใช้แสดงวันและเวลาเมื่อสารรับรองที่ตรวจสอบได้เริ่มมีผลผูกพันและสิ้นผลผูกพัน ตามลำดับ

ข้อกำหนดของคุณสมบัติ *issuanceDate* และ *expirationDate*

- สารรับรองที่ตรวจสอบได้ต้องมี *issuanceDate*
- ค่าของ *issuanceDate* ต้องเป็น string ที่แสดงวันและเวลาตามรูปแบบของ RFC 3339 ซึ่งเป็นวันและเวลาที่สารรับรองที่ตรวจสอบได้เริ่มมีผลผูกพัน โดยอาจเป็นวันและเวลาในอนาคตก็ได้
- สารรับรองที่ตรวจสอบได้อาจมี *expirationDate* หรือไม่ก็ได้
- ค่าของ *expirationDate* ต้องเป็น string ที่แสดงวันและเวลาตามรูปแบบของ RFC 3339 ซึ่งเป็นวันและเวลาที่สารรับรองที่ตรวจสอบได้สิ้นผลผูกพัน
- ผู้ตรวจสอบสารอาจทำการตรวจสอบค่าของ *issuanceDate* และ *expirationDate* ว่าอยู่ในช่วงวันและเวลาที่ผู้ตรวจสอบสารกำหนดหรือไม่ เช่น *issuanceDate* ไม่เป็นวันและเวลาในอนาคต และ *expirationDate* ไม่เป็นวันและเวลาในอดีต

ตัวอย่างที่ 8 การใช้งานของคุณสมบัติ *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",  // สารรับรองที่ตรวจสอบได้มีอายุ 10 ปี
 "credentialSubject": { ... },
 "proof": { ... }
}
```

4.1.6 เจ้าของข้อมูล (subject) และข้อกล่าวอ้าง (claim)

credentialSubject คือ คุณสมบัติที่ใช้แสดงข้อกล่าวอ้างเกี่ยวกับเจ้าของข้อมูลอย่างน้อยหนึ่งเอนทิตี

ข้อกำหนดของคุณสมบัติ *credentialSubject*

- สารรับรองที่ตรวจสอบได้ต้องมี *credentialSubject*
- ค่าของ *credentialSubject* เป็นกลุ่มของชุดข้อมูลที่ประกอบด้วยคุณสมบัติอย่างน้อยหนึ่งรายการซึ่งจะเกี่ยวข้องกับเจ้าของข้อมูลของสารรับรองที่ตรวจสอบได้
- ชุดข้อมูลแต่ละรายการใน *credentialSubject* อาจประกอบด้วย *id*

ตัวอย่างที่ 9 การใช้งานของคุณสมบัติ *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 สารรับรองที่ตรวจสอบได้สามารถใช้แสดงข้อมูลเกี่ยวกับเจ้าของข้อมูลมากกว่าหนึ่งเอนทิตีได้โดยนำชุดข้อมูลมาเรียงกันเป็นแถวลำดับ (array) ภายในคุณสมบัติ *credentialSubject* ตัวอย่างเช่น สารรับรองที่ตรวจสอบได้ของทะเบียนสมรสที่ระบุว่าเจ้าของข้อมูลสองคน ได้แก่ เพ็ญนี (Penny) และใจเด่น (Jayden) เป็นคู่สมรสกัน โดยใช้คุณสมบัติ *spouse*

ตัวอย่างที่ 10 การใช้งานของคุณสมบัติ *credentialSubject* ที่ระบุเจ้าของข้อมูลมากกว่าหนึ่งเอนทิตี

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

4.1.7 สถานะ (credential status)

credentialStatus คือ คุณสมบัติที่ใช้แสดงสถานะปัจจุบันของสารรับรองที่ตรวจสอบได้ เพื่อให้ทราบได้ว่าสารรับรองที่ตรวจสอบได้ถูกระงับหรือเพิกถอนหรือไม่

ข้อกำหนดของคุณสมบัติ *credentialStatus*

- สารรับรองที่ตรวจสอบได้อาจมี *credentialStatus* หรือไม่ก็ได้
- *credentialStatus* ต้องประกอบด้วยคุณสมบัติต่อไปนี้
  - *id* ซึ่งต้องมีค่าเป็น URL
  - *type* ซึ่งระบุประเภทสถานะของสารรับรองที่ตรวจสอบได้ (credential status type) โดยค่านี้ควรแสดงข้อมูลที่เพียงพอสำหรับแสดงสถานะปัจจุบันของสารรับรองที่ตรวจสอบได้ เช่น การระบุ URL ที่เชื่อมไปยังเอกสารภายนอกที่ระบุสถานะของสารรับรองที่ตรวจสอบได้

ตัวอย่างที่ 11 การใช้งานของคุณสมบัติ *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 ข้อพิสูจน์ (proof) หรือลายมือชื่อ (signature)

proof คือ คุณสมบัติที่ใช้แสดงวิธีการพิสูจน์ (proof mechanism) เพื่อให้สารรับรองที่ตรวจสอบได้หรือสารสำแดงที่ตรวจสอบได้มีคุณสมบัติที่สามารถตรวจพบการปลอมแปลงและตรวจสอบผู้เขียนข้อมูลได้ด้วยกระบวนการเข้ารหัสลับ

วิธีการพิสูจน์สามารถแบ่งออกเป็น 2 ประเภท คือ (1) external proof ซึ่งเป็นวิธีการที่มีข้อพิสูจน์อยู่ภายนอกโครงสร้างข้อมูล เช่น JSON Web Token (JWT) และ (2) embedded proof ซึ่งเป็นวิธีการที่มีข้อพิสูจน์รวมอยู่ในโครงสร้างข้อมูล เช่น Linked Data Signature

ข้อกำหนดเกี่ยวกับคุณสมบัติ *proof*

- สารรับรองที่ตรวจสอบได้ต้องรองรับวิธีการพิสูจน์ที่อาศัยกระบวนการเข้ารหัสลับอย่างน้อยหนึ่งวิธี ไม่ว่าจะเป็น external proof หรือ embedded proof
- วิธีการ external proof อาจมีคุณสมบัติ *proof* หรือไม่ก็ได้
- วิธีการ embedded proof ต้องมีคุณสมบัติ *proof* และระบุชื่อวิธีการพิสูจน์ไว้ในคุณสมบัติ *type*

ตัวอย่างที่ 12 การใช้งานของคุณสมบัติ *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": "eyJhbGciOiJQUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19
    ..DJBMvvFAIC00nSGB6Tn0XKbbF9XrsaJZREWvR2aONYTQQxnyXirtXnlewJMB
    Bn2h9hfcGZrvnC1b6PgWmukzFJ1IiH1dWgnDIS81BH-IxXnPkbuYDeySorc4
    QU9MJxdVkY5EL4HYbcIfwKj6X4LBQ2_ZHZIu1jdqLcRZqHcsDF5KKylKc1TH
    n5VRWy5WhYg_gBnyWny8E6Qkrze53MR7OuAmmNJ1m1nN8SxDrG6a08L78J0-
    Fbas5OjAQz3c17GY8mVuDPOBIOVjMEghBlgl3nOi1ysxbRGhHLEK4s0KKbeR
    ogZdgt1DkQxDFxxn41QWDw_mmMCjs9qxg0zcZzqEJw"
 }
}
```

4.1.9 โครงสร้างข้อมูลแสดงคุณสมบัติพื้นฐานของสารรับรองที่ตรวจสอบได้

สารรับรองที่ตรวจสอบได้แต่ละชุดประกอบด้วยคุณสมบัติและค่าของคุณสมบัติ ผู้พัฒนาต้องตรวจสอบสารรับรองที่ตรวจสอบได้ให้สอดคล้องตามโครงสร้างข้อมูลของสารรับรองที่ตรวจสอบได้ ซึ่งรวมถึงชื่อคุณสมบัติ ชนิดของค่าคุณสมบัติ และจำนวนของค่าคุณสมบัติ โดยบางคุณสมบัติอาจเป็นคุณสมบัติบังคับ และบางคุณสมบัติอาจมีได้หลายรายการ

โครงสร้างข้อมูลที่มีรายการคุณสมบัติพื้นฐานสำหรับใช้ในการสร้างสารรับรองที่ตรวจสอบได้สามารถแสดงตามตารางที่ 2

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

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

334

ตารางที่ 2 โครงสร้างข้อมูลแสดงคุณสมบัติพื้นฐานของสารรับรองที่ตรวจสอบได้

คุณสมบัติ	ชื่อคุณสมบัติ	คำอธิบาย	จำนวน	ชนิดของค่าคุณสมบัติ	ตัวอย่างการใช้งาน
บริบท (context)	*@context*	ที่อยู่เอกสารที่เชื่อมโยงชื่อคุณสมบัติต่าง ๆ ในสารรับรองที่ตรวจสอบได้เข้ากับ URI ที่ระบุนิยามและโครงสร้างของคุณสมบัตินั้น	[1..n]	URI หรือรายการของ URI แบบมีลำดับ	*"@context": ["https://www.w3.org/2018/credentials/v1", "https://www.w3.org/2018/credentials/examples/v1"]*
ตัวระบุ (identifier)	*id*	ตัวระบุสารรับรองที่ตรวจสอบได้	[0..1]	URI	*"id": "http://example.edu/credentials/3732"*
ประเภท (type)	*type*	ประเภทสาร เพื่อให้ผู้รับพิจารณาความเหมาะสมของโครงสร้างข้อมูลได้ โดยในกรณีนี้ให้ระบุเป็น “*VerifiableCredential*” และอาจมีประเภทเฉพาะของสารด้วย	[1..n]	URI หรือรายการของ URI แบบไม่มีลำดับ	*"type": ["VerifiableCredential", "UniversityDegreeCredential"]*
ผู้ออกสาร (issuer)	*issuer*	ผู้ออกสารรับรองที่ตรวจสอบได้	[1..1]	URI	*"issuer": "https://example.edu/issuers/14"*
				ชุดข้อมูลที่มีคุณสมบัติ *id*	*"issuer": { "id": "did:example:76e12ec712ebc6f1c221ebfeb1f", "name": "Example University" }*
วันที่ออกสาร (issuance date) และวันที่สารสิ้นอายุ (expiration dates)	*issuanceDate* หรือ *validFrom*	วันและเวลาเมื่อสารรับรองที่ตรวจสอบได้เริ่มมีผลผูกพัน	[1..1]	string แสดงวันและเวลาตาม RFC 3339	*"issuanceDate": "2010-01-01T19:23:24Z"*
	expirationDate หรือ *validUntil*	วันและเวลาเมื่อสารรับรองที่ตรวจสอบได้สิ้นผลผูกพัน	[0..1]	string แสดงวันและเวลาตาม RFC 3339	*"expirationDate": "2016-01-01T00:00:00Z"*
เจ้าของข้อมูล (credential subject) และข้อกล่าวอ้าง (claim)	*credentialSubject*	เจ้าของข้อมูลที่ถูกกล่าวอ้างถึงในข้อกล่าวอ้าง	[1..n]		*"credentialSubject": { "id": "did:example:ebfeb1f712ebc6f1c276e12ec21", "alumniOf": { "id": "did:example:c276e12ec21ebfeb1f712ebc6f1", "name": [{ "value": "Example University", "language": "en" }, {*
	id	ตัวระบุเจ้าของข้อมูล	[0..1]	URI	
	ชื่อคุณสมบัติ[2] เช่น *name*, *alumniOf*, *degree* หรือ *spouse* โดยอาจอ้างอิง www.schema.org	คุณสมบัติและค่าคุณสมบัติของข้อกล่าวอ้างที่เกี่ยวกับเจ้าของข้อมูลนั้น	[1..n]	ประเภทข้อมูลที่เหมาะสมต่อคุณสมบัตินั้น ๆ หรือชุดข้อมูลซึ่งอาจมีคุณสมบัติ *id* หากกล่าวถึงเอนทิตีอื่น	

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

คุณสมบัติ	ชื่อคุณสมบัติ	คำอธิบาย	จำนวน	ชนิดของค่าคุณสมบัติ	ตัวอย่างการใช้งาน
					"value": "มหาวิทยาลัยสมมุติ", *"language": "th"* *}]* *}* *}*
สถานะ (credential status)	*credentialStatus*	สถานะปัจจุบันของสาร เช่น เพิกถอนแล้ว	[0..1]		*"credentialStatus": {*
	id	ตัวระบุเอกสารอ้างอิง	[1..1]	URL	*"id": "https://example.edu/status/24",*
	type	ประเภทสถานะสาร	[1..1]	string	*"type": "CredentialStatusList2017"* *}*
ข้อพิสูจน์ (proof)	*proof*	ข้อพิสูจน์หรือหลักฐานที่ใช้ในการตรวจสอบสาร 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":* *"eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..TCYt5XsITJX1CxPCT8yAV-TVkIEq_PbChOMqsLfRoPsnsgw5WEuts01mq-pQy7UJiN5mgRxD-WUcX16dUEMGlv50aqzpqh4Qktb3rk-BuQy72IFLOqV0G_zS 245-kronKb78cPN25DGlcTwLtjPAYuNzVBAh4vGHSrQy 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	

335

[3] สารรับรองที่ตรวจสอบได้จำเป็นต้องรองรับวิธีการพิสูจน์ ไม่ว่าจะเป็น external proof หรือ embedded proof ซึ่งหากสารรับรองที่ตรวจสอบได้ใดใช้ embedded proof จะต้องปรากฏคุณสมบัติ *proof* ด้วยเสมอ

4.2 คุณสมบัติของสารสำแดงที่ตรวจสอบได้

สารสำแดงที่ตรวจสอบได้ถูกสร้างขึ้นมาจากสารรับรองที่ตรวจสอบได้อย่างน้อยหนึ่งชุดโดยผู้ถือสาร เพื่อใช้แสดงข้อกล่าวอ้างภายในสารรับรองที่ตรวจสอบได้ในรูปแบบที่สามารถตรวจสอบผู้เขียนข้อมูลได้ โดยทั่วไปสารสำแดงที่ตรวจสอบได้จะประกอบไปด้วยคุณสมบัติตามตารางที่ 3

ตารางที่ 3 คุณสมบัติของสารสำแดงที่ตรวจสอบได้โดยทั่วไป

คุณสมบัติ	ข้อกำหนด
id	คุณสมบัติ *id* จะมีหรือไม่ก็ได้ และอาจใช้เป็นตัวระบุที่เฉพาะเจาะจงของสารสำแดงที่ตรวจสอบได้
type	คุณสมบัติ *type* ต้องมี และใช้แสดงประเภทของสารสำแดงที่ตรวจสอบได้ เช่น *VerifiablePresentation*
verifiableCredential	หากมีคุณสมบัติ *verifiableCredential* ค่าของคุณสมบัตินี้ต้องสร้างขึ้นจากสารรับรองที่ตรวจสอบได้อย่างน้อยหนึ่งชุด หรือเป็นข้อมูลที่สังเคราะห์จากสารรับรองที่ตรวจสอบได้ในรูปแบบที่สามารถตรวจสอบได้ด้วยกระบวนการเข้ารหัสลับ
holder	หากมีคุณสมบัติ *holder* ค่าของคุณสมบัตินี้ควรเป็น URI ของเอนทิตีที่มีบทบาทในการสร้างสารสำแดงที่ตรวจสอบได้
proof	หากมีคุณสมบัติ *proof* ค่าของคุณสมบัตินี้จะเป็นข้อพิสูจน์หรือหลักฐานที่ใช้ในการตรวจสอบสารสำแดงที่ตรวจสอบได้

ตัวอย่างที่ 13 สารสำแดงที่ตรวจสอบได้ที่ประกอบด้วยสารรับรองที่ตรวจสอบได้

```
{
  "@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 โครงสร้างข้อมูลแสดงคุณสมบัติของสารสำแดงที่ตรวจสอบได้

โครงสร้างข้อมูลที่มีรายการคุณสมบัติสำหรับใช้ในการสร้างสารสำแดงที่ตรวจสอบได้สามารถแสดงตามตารางที่ 4

346

ตารางที่ 4 โครงสร้างข้อมูลแสดงคุณสมบัติของสารสำแดงที่ตรวจสอบได้

คุณสมบัติ	ชื่อคุณสมบัติ	คำอธิบาย	จำนวน	ชนิดของค่าคุณสมบัติ	ตัวอย่างการใช้งาน
บริบท (context)	*@context*	ที่อยู่เอกสารที่เชื่อมโยงชื่อคุณสมบัติต่าง ๆ เข้ากับ URI ที่ระบุนิยามและโครงสร้างของคุณสมบัตินั้น	[1..n]	URI หรือรายการของ URI แบบมีลำดับ	*"@context": ["https://www.w3.org/2018/credentials/v1", "https://www.w3.org/2018/credentials/examples/v1"]*
ตัวระบุ (identifier)	*id*	ตัวระบุของสารสำแดงที่ตรวจสอบได้	[0..1]	URI	*"id": "urn:uuid:3978344f-8596-4c3a-a978-8fcaba3903c5"*
ประเภท (type)	*type*	ประเภทสาร เพื่อให้ผู้รับพิจารณาความเหมาะสมของโครงสร้างข้อมูลได้ โดยในกรณีนี้ ให้ระบุเป็น *"VerifiablePresentation"* และอาจมีประเภทเฉพาะของสารด้วย	[1..n]	URI หรือรายการของ URI แบบไม่มีลำดับ	*"type": ["VerifiablePresentation", "CredentialManagerPresentation"]*
ผู้ถือสาร (holder)	*holder*	ผู้ออกสารสำแดงที่ตรวจสอบได้ ซึ่งคือ ผู้ถือสารรับรองที่ตรวจสอบได้	[0..1]	URI	*"holder": "https://example.edu/issuers/14"*
ข้อกล่าวอ้าง (claim)	*verifiableCredential*	สารรับรองที่ตรวจสอบได้ซึ่งบรรจุข้อกล่าวอ้าง	[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": {...} }]*
ข้อพิสูจน์ (proof)	*proof*	ข้อพิสูจน์หรือข้อพิสูจน์ที่ใช้ในการตรวจสอบสาร 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",*
	type	ประเภทข้อพิสูจน์	[1..1]	string	
	created	วันและเวลาเมื่อลงข้อพิสูจน์	[1..1]	string แสดงวันและเวลาตาม RFC 3339	
	expires	วันและเวลาเมื่อข้อพิสูจน์สิ้นอายุ	[0..1]	string แสดงวันและเวลา	

[4] สารสำแดงที่ตรวจสอบได้จำเป็นต้องรองรับวิธีการพิสูจน์ ไม่ว่าจะเป็น external proof หรือ embedded proof ซึ่งหากสารสำแดงที่ตรวจสอบได้ใดใช้ embedded proof จะต้องปรากฏคุณสมบัติ *proof* ด้วยเสมอ

คุณสมบัติ	ชื่อคุณสมบัติ	คำอธิบาย	จำนวน	ชนิดของค่าคุณสมบัติ	ตัวอย่างการใช้งาน
				ตาม RFC 3339	*"challenge": "1f44d55f-f161-4938-a659-f8026467f126",* *"domain": "4jt78h47fh47",* *"jws":* *"eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..kTCYt5XsITJX1CxPCT8yAV-TVlw5WEuts01mq-pQy7UJiN5mgREEMGlv50aqzpqh4Qq_PbChOMqsLfRoPsnsgxD-WUcX16dUOqV0G_zS245-kronKb78cPktb3rk-BuQy72IFLN25DYuNzVBAh4vGHSrQyHUGlcTwLtjPAnKb78"* *}*
	proofPurpose	วัตถุประสงค์ของข้อพิสูจน์ โดยในกรณีนี้ ให้ระบุเป็น *"authentication"*	[0..1]	string	
	ชื่อคุณสมบัติทางความมั่นคงปลอดภัย เช่น *verificationMethod*, *jws*, *nonce*, *domain* หรือ *challenge* โดยอาจอ้างอิง w3c-ccg.github.io/security-vocab/	คุณสมบัติและค่าคุณสมบัติของข้อพิสูจน์นั้น	[0..1]	ประเภทข้อมูลที่เหมาะสมต่อคุณสมบัตินั้น ๆ	

347

ภาคผนวก ก. คุณสมบัติเพิ่มเติมของสารรับรองที่ตรวจสอบได้

ก.1 เค้าร่างข้อมูล (credential schema)

credentialSchema คือ คุณสมบัติที่ใช้กำหนดเค้าร่างของชุดข้อมูลในสาร ซึ่งอาจแบ่งออกเป็น 2 ประเภท คือ (1) data verification schema ซึ่งเป็นเค้าร่างที่ใช้ในการตรวจสอบโครงสร้างและเนื้อหาของสารรับรองที่ตรวจสอบได้ว่าสอดคล้องตามรูปแบบที่กำหนดไว้ และ (2) data encoding schema ซึ่งเป็นเค้าร่างที่ใช้ในการเข้ารหัสเนื้อหาของสารรับรองที่ตรวจสอบได้เพื่อแสดงในรูปแบบอื่น ๆ เช่น รูปแบบเลขฐานสอง (binary format) ที่ใช้สำหรับ zero-knowledge proof

ข้อกำหนดของคุณสมบัติ *credentialSchema*

- ค่าของ *credentialSchema* ต้องเป็นเค้าร่างข้อมูล (schema) อย่างน้อยหนึ่งรายการ เพื่อให้ผู้ตรวจสอบสารใช้ในการตรวจสอบข้อมูลว่าสอดคล้องตามเค้าร่างข้อมูลที่กำหนดไว้
- *credentialSchema* แต่ละรายการต้องระบุ *type* ซึ่งแสดงประเภทของเค้าร่างข้อมูล (เช่น JsonSchemaValidator2018) และ *id* ซึ่งต้องเป็น URI ที่เชื่อมโยงไปยังไฟล์เค้าร่างข้อมูล (schema file)

ตัวอย่างที่ 14 การใช้งานของคุณสมบัติ *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": { ... },
// ผู้ออกสารระบุ credentialSchema ที่เชื่อมโยงไปยังไฟล์ JSON schema เพื่อให้ผู้ตรวจสอบสารใช้ในการตรวจสอบสารรับรองที่ตรวจสอบได้ว่าสอดคล้องตามเค้าร่างข้อมูลที่กำหนดไว้
  "credentialSchema": {
    "id": "https://example.org/examples/degree.json",
    "type": "JsonSchemaValidator2018
  },
  "proof": { ... }
}
```

ตัวอย่างที่ 15 การใช้งานของคุณสมบัติ *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": { ... },
```

```
// ผู้ออกสารระบุ credentialSchema ที่เชื่อมโยงไปยัง binary format ที่ใช้ในการแปลงเนื้อหาสำหรับ zero-knowledge proof เพื่อให้ผู้ตรวจสอบสารใช้ในการตรวจสอบข้อพิสูจน์ของสารรับรองที่ตรวจสอบได้ว่าถูกต้องหรือไม่
  "credentialSchema": {
    "id": "https://example.org/examples/degree.zkp",
    "type": "ZkpExampleSchema2018"
  },
  "proof": { ... }
}
```

ก.2 การต่ออายุหรือปรับให้เป็นปัจจุบัน (refreshing)

refreshService คือ คุณสมบัติที่ใช้แสดงการต่ออายุหรือปรับให้เป็นปัจจุบัน (refreshing) ซึ่งผู้ออกสารสามารถระบุ URL ที่เชื่อมโยงไปยังบริการต่ออายุหรือปรับให้เป็นปัจจุบัน (refresh service) เพื่อให้ผู้รับ (ผู้ถือสารหรือผู้ตรวจสอบสาร) สามารถต่ออายุหรือปรับสารรับรองที่ตรวจสอบได้ให้เป็นปัจจุบันได้เอง ทั้งนี้ คุณสมบัติ *refreshService* ควรนำมาใช้ในกรณีที่สารรับรองที่ตรวจสอบได้นั้นสิ้นอายุ หรือกรณีที่ผู้ออกสารไม่ได้เปิดเผยข้อมูลสถานะของสารรับรองที่ตรวจสอบได้

ข้อกำหนดของคุณสมบัติ *refreshService*

- ค่าของ *refreshService* ต้องเป็นข้อมูลแสดงบริการต่ออายุหรือปรับให้เป็นปัจจุบันอย่างน้อยหนึ่งรายการ ซึ่งให้ข้อมูลที่เพียงพอสำหรับให้ผู้รับสามารถต่ออายุหรือปรับสารรับรองที่ตรวจสอบได้ให้เป็นปัจจุบันได้
- *refreshService* แต่ละรายการต้องระบุ *type* ซึ่งแสดงประเภทของบริการ (เช่น *ManualRefreshService2018*) และ *id* ซึ่งเป็น URL ของบริการนั้น

ตัวอย่างที่ 16 การใช้งานของคุณสมบัติ *refreshService*

```
{
  "@context": [ ... ],
  "id": "http://example.edu/credentials/3732",
  "type": ["VerifiableCredential", "UniversityDegreeCredential"],
  "issuer": "https://example.edu/issuers/14",
  "issuanceDate": "2010-01-01T19:23:24Z",
  "credentialSubject": { ... },
  "refreshService": {
    // URL ที่เชื่อมโยงผู้ถือสารหรือผู้ตรวจสอบสารไปยังบริการต่ออายุหรือปรับให้เป็นปัจจุบัน
    "id": "https://example.edu/refresh/3732"
    "type": "ManualRefreshService2018",
  },
  "proof": { ... }
}
```

ก.3 ข้อกำหนดการใช้งาน (terms of use)

termsOfUse คือ คุณสมบัติที่ใช้แสดงข้อกำหนดการใช้งาน (terms of use) ซึ่งผู้ออกสารหรือผู้ถือสารสามารถใช้สื่อสารไปยังผู้ตรวจสอบสารเกี่ยวกับสิ่งที่ต้องทำ (obligation) สิ่งที่ห้ามทำ (prohibition) และสิ่งที่สามารถทำได้ (permission) ทั้งนี้ ผู้ออกสารจะระบุข้อกำหนดการใช้งานไว้ในสารรับรองที่ตรวจสอบได้ ขณะที่ผู้ถือสารจะระบุข้อกำหนดการใช้งานไว้ในสารสำแดงที่ตรวจสอบได้

ข้อกำหนดของคุณสมบัติ *termsOfUse*

- ค่าของ *termsOfUse* ในสารรับรองที่ตรวจสอบได้หรือสารสำแดงที่ตรวจสอบได้ต้องเป็นข้อมูลแสดงข้อกำหนดการใช้งานอย่างน้อยหนึ่งรายการ
- *termsOfUse* แต่ละรายการต้องระบุ *type* ซึ่งแสดงประเภทของข้อกำหนด (เช่น *IssuerPolicy*) และอาจ ระบุ *id* หรือไม่ก็ได้

ตัวอย่างที่ 17 การใช้งานของคุณสมบัติ *termsOfUse* โดยผู้ออกสารในสารรับรองที่ตรวจสอบได้

```
{
 "@context": [ ... ],
 "id": "http://example.edu/credentials/3732",
 "type": ["VerifiableCredential", "UniversityDegreeCredential"],
 "issuer": "https://example.edu/issuers/14",
 "issuanceDate": "2010-01-01T19:23:24Z",
 "credentialSubject": { ... },
 "termsOfUse": [{
  "type": "IssuerPolicy",
  "id": "http://example.com/policies/credential/4",
  "profile": "http://example.com/profiles/credential",
  // ผู้ออกสารห้ามไม่ให้ผู้ตรวจสอบสารจัดเก็บข้อมูลไว้ในระบบเก็บบันทึกถาวร
  "prohibition": [{
   "assigner": "https://example.edu/issuers/14",
   "assignee": "AllVerifiers",
   "target": "http://example.edu/credentials/3732",
   "action": ["Archival"]
  }]
 }],
 "proof": { ... }
}
```

ตัวอย่างที่ 18 การใช้งานของคุณสมบัติ *termsOfUse* โดยผู้ถือสารในสารสำแดงที่ตรวจสอบได้

```
{
 "@context": [ ... ],
 "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
 "type": ["VerifiablePresentation"],
 "verifiableCredential": { ... },
 "termsOfUse": [{
  "type": " HolderPolicy",
  "id": "http://example.com/policies/credential/6",
  "profile": "http://example.com/profiles/credential",
  // ผู้ถือสารซึ่งเป็นเจ้าของข้อมูลด้วย ห้ามไม่ให้ผู้ตรวจสอบสารส่งต่อข้อมูลให้แก่บุคคลที่สาม
  "prohibition": [{
   "assigner": "did:example:ebfeb1f712ebc6f1c276e12ec21",
   "assignee": "https://wineonline.example.org/",
   "target": "http://example.edu/credentials/3732",
   "action": ["3rdPartyCorrelation"]
  }]
 }],
 "proof": [ ... ]
}
```

ก.4 หลักฐาน (evidence)

evidence คือ คุณสมบัติที่ใช้แสดงข้อมูลหลักฐาน ซึ่งผู้ออกสารจัดทำเป็นข้อมูลสนับสนุนเพิ่มเติมในสารรับรองที่ตรวจสอบได้ เพื่อทำให้ผู้ตรวจสอบสารเกิดความเชื่อมั่นต่อข้อกล่าวอ้างที่อยู่ในสารรับรองที่ตรวจสอบได้ ตัวอย่างเช่น ผู้ออกสารอาจตรวจสอบเอกสารหลักฐานที่เป็นกระดาษหรือตรวจสอบประวัติของเจ้าของข้อมูลก่อนที่จะออกสารรับรองที่ตรวจสอบได้

evidence ต่างจาก *proof* ตรงที่คุณสมบัติ *evidence* ใช้แสดงข้อมูลสนับสนุนเพิ่มเติม เช่น หลักฐานที่เกี่ยวข้องกับความครบถ้วนของสารรับรองที่ตรวจสอบได้ ในขณะเดียวกัน *proof* ใช้แสดงข้อพิสูจน์ที่เกี่ยวข้องกับความครบถ้วนของสารรับรองที่ตรวจสอบได้และการตรวจสอบผู้ออกสารซึ่งเป็นผู้เขียนข้อมูล

ข้อกำหนดของคุณสมบัติ *evidence*

- ค่าของ *evidence* ต้องเป็นข้อมูลหลักฐานอย่างน้อยหนึ่งรายการ ซึ่งให้ข้อมูลที่เพียงพอตามข้อกำหนดของผู้ตรวจสอบสารเกี่ยวกับความน่าเชื่อถือของสารรับรองที่ตรวจสอบได้
- *evidence* แต่ละรายการต้องมี *type* ซึ่งแสดงประเภทของข้อมูลหลักฐาน
- *evidence* อาจมี *id* หรือไม่ก็ได้ และถ้ามี ควรเป็น URL ที่เชื่อมโยงไปยังแหล่งที่เก็บข้อมูลหลักฐาน

ตัวอย่างที่ 19 การใช้งานของคุณสมบัติ *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": { ... }
}
```

ก.5 การโต้แย้ง (disputes)

เอนทิตีอาจต้องการโต้แย้งข้อกล่าวอ้างในสารรับรองที่ตรวจสอบได้ที่ออกโดยผู้ออกสารในอย่างน้อย 2 กรณี คือ (1) เจ้าของข้อมูลโต้แย้งว่าข้อกล่าวอ้างเกี่ยวกับตนเองไม่ถูกต้อง (ตัวอย่างเช่น สารรับรองที่ตรวจสอบได้ของตนเองระบุหมายเลขประจำตัวประชาชนไม่ถูกต้อง) และ (2) เอนทิตีโต้แย้งว่าข้อกล่าวอ้าง

เกี่ยวกับเจ้าของข้อมูลอื่นไม่ถูกต้อง (ตัวอย่างเช่น สารรับรองที่ตรวจสอบได้ของผู้อื่นใช้หมายเลขประจำตัวประชาชนของตนเอง)

วิธีการออกสารรับรองสำหรับโต้แย้ง (dispute credential) เหมือนกับการออกสารรับรองที่ตรวจสอบได้แบบปกติ ยกเว้นตัวระบุในคุณสมบัติ *credentialSubject* ของสารรับรองสำหรับโต้แย้งจะเป็นตัวระบุของสารรับรองที่ตรวจสอบได้ที่ถูกโต้แย้ง

ตัวอย่างที่ 20 ตัวอย่างของสารรับรองสำหรับโต้แย้ง

```
{
  "@context": [ ... ],
  "id": "http://example.com/credentials/123",
  "type": ["VerifiableCredential", "DisputeCredential"],
  "credentialSubject": {
    "id": "http://example.com/credentials/245",  // ตัวระบุของสารรับรองที่ตรวจสอบได้ที่ถูกโต้แย้ง
    "currentStatus": "Disputed",
    "statusReason": {
      "value": "Address is out of date.",  // เจ้าของข้อมูลโต้แย้งว่าข้อมูลที่อยู่ไม่เป็นปัจจุบัน
      "lang": "en"
    },
  },
  "issuer": "https://example.com/people#me",
  "issuanceDate": "2017-12-05T14:27:42Z",
  "proof": { ... }
}
```

ทั้งนี้ เจ้าของข้อมูลสามารถออกสารรับรองสำหรับโต้แย้งตามตัวอย่างข้างต้นและนำไปแสดงต่อผู้ตรวจสอบสาร พร้อมกับสารรับรองที่ตรวจสอบได้ที่ถูกโต้แย้ง

ภาคผนวก ข. ความสามารถในการเพิ่มคุณสมบัติ (extensibility)

นักพัฒนาสามารถเพิ่มคุณสมบัติในโครงสร้างข้อมูลของสารรับรองที่ตรวจสอบได้ด้วยคำศัพท์ในรูปแบบที่คอมพิวเตอร์สามารถนำไปประมวลผลได้ โดยไม่จำเป็นต้องอาศัยระบบทะเบียนกลางก็ได้ ทั้งนี้ การเพิ่มคุณสมบัติของสารรับรองที่ตรวจสอบได้ดังกล่าวสามารถทำได้ด้วยการใช้ Linked data หรือ JSON-LD

ตัวอย่างของการเพิ่มคุณสมบัติในสารรับรองที่ตรวจสอบได้สามารถอธิบายโดยเริ่มต้นจากสารรับรองที่ตรวจสอบได้อย่างง่าย ดังนี้

ตัวอย่างที่ 21 สารรับรองที่ตรวจสอบได้อย่างง่าย

```
{
  "@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": { ... }
}
```

สารรับรองที่ตรวจสอบได้ข้างต้นระบุว่าเอนทิตีที่สัมพันธ์กับ did:example:abcdef1234567 มีคุณสมบัติ *name* ที่มีค่าเป็น Penny ทั้งนี้ หากนักพัฒนาต้องการเพิ่มคุณสมบัติใหม่ในสารรับรองที่ตรวจสอบได้ข้างต้นอีกสองรายการ คือ *referenceNumber* ซึ่งใช้แสดงหมายเลขอ้างอิงภายในองค์กร และ *favoriteFood* ซึ่งใช้แสดงอาหารจานโปรด นักพัฒนาต้องทำการสร้างบริบทในรูปแบบ JSON-LD (JSON-LD Context) ที่มีคุณสมบัติใหม่สองรายการนั้น ดังนี้

ตัวอย่างที่ 22 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 ข้างต้นไปเผยแพร่เพื่อให้ผู้ตรวจสอบสารสามารถเข้าถึงได้ ในที่นี้ คือ https://example.com/contexts/mycontext.jsonld หลังจากนั้นนักพัฒนาจะเพิ่มค่าของคุณสมบัติ *@context* และ *type* และสามารถเพิ่มคุณสมบัติใหม่สองรายการนั้นลงในสารรับรองที่ตรวจสอบได้ ดังนี้

ตัวอย่างที่ 23 สารรับรองที่ตรวจสอบได้ที่มีการเพิ่มคุณสมบัติใหม่

```
{
  "@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. กรณีศึกษาการใช้งานสารรับรองที่ตรวจสอบได้

กรณีศึกษาการใช้งานสารรับรองที่ตรวจสอบได้ พร้อมบทบาทของเอนทิตีต่าง ๆ มีตัวอย่างดังต่อไปนี้

ตารางที่ 5 ตัวอย่างกรณีศึกษาที่สามารถใช้สารรับรองที่ตรวจสอบได้

กรณีศึกษา	ผู้ออกสาร	ผู้ถือสาร	ผู้ตรวจสอบสาร
(1) ใบประมวลผลการศึกษา (transcript) หรือใบปริญญาบัตร มหาวิทยาลัยออกใบประมวลผลการศึกษาหรือใบปริญญาบัตรในรูปสารรับรองที่ตรวจสอบได้ให้แก่นักศึกษา เพื่อนำไปใช้สมัครเข้าทำงานกับบริษัทที่รับสมัครงาน บริษัทสามารถตรวจสอบได้ว่าเอกสารข้างต้นออกโดยมหาวิทยาลัยนั้นจริง ซึ่งช่วยป้องกันการนำเอกสารปลอมมาใช้ในการสมัครเข้าทำงาน	มหาวิทยาลัย	นักศึกษา	บริษัท
(2) หนังสือมอบอำนาจ ผู้มอบอำนาจออกหนังสือมอบอำนาจในรูปสารรับรองที่ตรวจสอบได้ให้แก่ผู้รับมอบอำนาจ เพื่อให้ดำเนินการแทนผู้มอบอำนาจตามรายละเอียดในหนังสือมอบอำนาจ ซึ่งเจ้าหน้าที่สามารถตรวจสอบได้ว่าผู้มอบอำนาจได้กระทำการมอบอำนาจนั้นจริง	ผู้มอบอำนาจ	ผู้รับมอบอำนาจ	เจ้าหน้าที่ตรวจสอบเอกสาร
(3) บัตรสมนาคุณ หรือบัตรสมาชิกสะสมแต้ม ผู้บริโภคใช้บริการของผู้ให้บริการตามเงื่อนไขที่กำหนด ผู้ให้บริการจึงออกบัตรสมนาคุณหรือบัตรสมาชิกสะสมแต้มในรูปสารรับรองที่ตรวจสอบได้ให้แก่ผู้บริโภค เพื่อนำไปใช้เป็นส่วนลดค่าบริการโดยอาจเป็นบริการของตนเองหรือบริการของผู้ให้บริการอื่นที่เป็นพันธมิตรก็ได้	ผู้ให้บริการ	ผู้บริโภค	ผู้ให้บริการอื่น
(4) ใบรับรองแพทย์ แพทย์ออกใบรับรองแพทย์ในรูปสารรับรองที่ตรวจสอบได้ให้แก่พนักงานบริษัท เพื่อรับรองว่ามีอาการป่วยจริง ซึ่งพนักงานสามารถนำเอกสารข้างต้นไปแสดงเป็นหลักฐานประกอบการลางานกับเจ้าหน้าที่ฝ่ายบุคคลของบริษัทได้	แพทย์	พนักงานบริษัท	เจ้าหน้าที่ฝ่ายบุคคลของบริษัท

438 **บรรณานุกรม**

439

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

[3] Internet Engineering Task Force, "RFC 7797 - JSON Web Signature (JWS) Unencoded Payload Option", February 2016 [Online]. Available: https://tools.ietf.org/html/rfc7797.

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

440