ประกาศสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ที่ ม ๔/๒๕๖๙

เรื่อง มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ แนวปฏิบัติและหลักการพื้นฐานในการออกแบบ
มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านความหมายข้อมูล กรณีเอกสารรับรองดิจิทัล
และเอกสารสำแดงดิจิทัล

.....

ด้วยสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) มีภารกิจในการส่งเสริมและสนับสนุนการดำเนินงานของหน่วยงานของรัฐในการบริหารราชการแผ่นดินและการให้บริการประชาชนผ่านระบบดิจิทัล เพื่อให้กระบวนการหรือการดำเนินงานทางดิจิทัลในการขับเคลื่อนประเทศในด้านต่าง ๆ เป็นไปอย่างเต็มรูปแบบ ซึ่งเป็นกลไกสำคัญในการยกระดับการให้บริการประชาชนผ่านระบบดิจิทัลให้มีประสิทธิภาพยิ่งขึ้น โดยการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลระหว่างหน่วยงานของรัฐ และการบูรณาการข้อมูลร่วมกัน สพร. จึงได้จัดทำมาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ แนวปฏิบัติและหลักการพื้นฐานในการออกแบบ มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านความหมายข้อมูล กรณีเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล เพื่อยกระดับบริการภาครัฐสู่รูปแบบดิจิทัลและการออกแบบบริการแบบยึดประชาชนเป็นศูนย์กลาง ทำให้บทบาทของเอกสารดิจิทัลที่สามารถตรวจสอบได้ ซึ่งอยู่ในรูปแบบเอกสารรับรองดิจิทัล (Verifiable Credential: VC) และเอกสารสำแดงดิจิทัล (Verifiable Presentation: VP) รวมทั้งเพื่อให้เป็นมาตรฐานในการทำงานร่วมกัน (Interoperability) ระหว่างหน่วยงานของรัฐ และให้การทำงานมีประสิทธิภาพยิ่งขึ้น

อาศัยอำนาจตามความในมาตรา ๘ (๒) มาตรา ๒๙ และมาตรา ๓๐ แห่งพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) พ.ศ. ๒๕๖๑ จึงออกประกาศ เรื่อง มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ แนวปฏิบัติและหลักการพื้นฐานในการออกแบบ มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านความหมายข้อมูล กรณีเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล เลขที่ มสพร. ๑๙-๒๕๖๙ เพื่อยึดถือเป็นแนวทางปฏิบัติภายในของ สพร. และเป็นข้อเสนอแนะสำหรับหน่วยงานของรัฐต่อไป โดยมีรายละเอียดตามเอกสารแนบท้ายประกาศนี้

จึงประกาศให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่ ๘ กันยายน พ.ศ.๒๕๖๙

(นางไอรดา เหลืองวิไล)
รองผู้อำนวยการ รักษาการแทน
ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

DGA Community Standard

มสพร. 19-2569

DGA 19-2569

ว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ
แนวปฏิบัติและหลักการพื้นฐานในการออกแบบ
มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ
ด้านความหมายข้อมูล
กรณีเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล

THAILAND GOVERNMENT INFORMATION EXCHANGE
STANDARD VERIFIABLE CREDENTIALS AND PRESENTATIONS

เวอร์ชัน 1.0

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ แนวปฏิบัติและหลักการพื้นฐานในการออกแบบ มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านความหมายข้อมูล กรณีเอกสารรับรองดิจิทัล และเอกสารสำแดงดิจิทัล

มสพร. 19-2569

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
เลขที่ 120 อาคารศูนย์ราชการเฉลิมพระเกียรติฯ (อาคารซี) ชั้น 8 - 9
หมู่ 3 ซอยแจ้งวัฒนะ 7 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210
หมายเลขโทรศัพท์: (+66) 0 2612 6000 โทรสาร: (+66) 0 2612 6011

ประกาศโดย
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
กันยายน 2569

คณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

ที่ปรึกษา

ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

ประธานกรรมการ

ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูไพโรจน์	จุฬาลงกรณ์มหาวิทยาลัย

รองประธานกรรมการ

นายอาศิส อัญญะโพธิ์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

กรรมการ

นายมารุต บูรณรัช	ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
นางสาวขนิษฐ์ ผาทอง	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายชลอ อินทพันธุ์	สำนักบริหารการทะเบียน กรมการปกครอง
นางสาวดารารัตน์ โฆษิตพิพัฒน์	สำนักงานคณะกรรมการพัฒนาระบบราชการ
นางสาวพรพิมล อุ่นไพร	สำนักงานคณะกรรมการกฤษฎีกา
นายสันติ สิทธิเลิศพิศาล	สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม
นายวีระ วีระกุล	สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย
รองศาสตราจารย์เกริก ภิรมย์โสภา	ประธานคณะทำงานเทคนิคด้านมาตรฐานความมั่นคงปลอดภัยภาครัฐ
ศาสตราจารย์ธีรณี อจลากุล	ประธานคณะทำงานเทคนิคด้านมาตรฐานการบริหารจัดการข้อมูลภาครัฐ
ผู้ช่วยศาสตราจารย์มารอง ผดุงสิทธิ์	ประธานคณะทำงานเทคนิคด้านมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ

กรรมการและเลขานุการ

นางสาวอุรัชฎา เกตุพรหม	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะทำงานเทคนิคด้านมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ

ที่ปรึกษา

ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูไพโรจน์	จุฬาลงกรณ์มหาวิทยาลัย
นายอาศิส อัญญะโพธิ์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ประธานคณะทำงาน

ผู้ช่วยศาสตราจารย์มารอง ผดุงสิทธิ์	มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี

รองประธานคณะทำงาน

นางสาวยศวลัย โชติปทุมวรรณ	มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

คณะทำงาน

นายสรชา หิรัญวัฒน์	กรมการขนส่งทางบก
นางสาวสุชาดา คำวงษ์	กรมการปกครอง
นางสาวมนทิพา เข่งพิมล	กรมพัฒนาธุรกิจการค้า
นายบวร เรืองแรงสกุล	กรมศุลกากร
นางจันทร์เจริญ แบร์โรวส์	กรมสรรพากร
นางสาวอาวีวรรณ อินทกาญจน์	ธนาคารแห่งประเทศไทย
นางสุรีพร พรโสภณวิชญ์	สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ
นายสยาม ลววิโรจน์วงศ์	สำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ (องค์การมหาชน)
นายศุภโชค จันทรประทิน	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายกิตติ ขุนสนิท	สำนักงานส่งเสริมเศรษฐกิจดิจิทัล
นายอัครรัฐ หย่างไพบูลย์	สำนักงานหลักประกันสุขภาพแห่งชาติ

คณะทำงานและเลขานุการ

นางสาวอุรัชฎา เกตุพรหม	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ผู้ช่วยเลขานุการ

นายนพดล แก้วคำ	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

วิเคราะห์และจัดทำมาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล ว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ แนวปฏิบัติและหลักการพื้นฐานในการออกแบบ มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านความหมายข้อมูล กรณีเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล

นายนพดล แก้วคำ	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นายปราการ ศิริมา	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นายณัฐวัฒน์ วรสิทธิ์ตระกูล	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

มาตรฐานฉบับนี้จัดทำขึ้นเพื่อเป็นข้อกำหนดตามมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ (Thailand Government Information Exchange: TGIX) โดยอยู่ในกลุ่มมาตรฐานด้านความหมายข้อมูล ที่กล่าวถึงมาตรฐานการแลกเปลี่ยนข้อมูลกรณีเอกสารรับรองดิจิทัล (Verifiable Credential: VC) และเอกสารสำแดงดิจิทัล (Verifiable Presentation: VP) การจัดทำมาตรฐานนี้ได้ผ่านกระบวนการที่เข้มงวดและรอบด้าน โดยมีการจัดให้มีการประชาพิจารณ์รับฟังความคิดเห็นเป็นการทั่วไป รวมถึงรวบรวมข้อมูลและข้อคิดเห็นจากผู้ทรงคุณวุฒิและหน่วยงานที่เกี่ยวข้อง เพื่อนำมาปรับปรุงเนื้อหาให้สมบูรณ์ครบถ้วน นอกจากนี้ มาตรฐานฉบับนี้ยังได้รับการพิจารณากลั่นกรองจากคณะทำงานเทคนิคด้านมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ และได้รับความเห็นชอบจากคณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 เพื่อให้มั่นใจว่าข้อเสนอแนะเกี่ยวกับมาตรฐานนี้มีความสมบูรณ์ น่าเชื่อถือ และสามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพสูงสุด

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ แนวปฏิบัติและหลักการพื้นฐานในการออกแบบ มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐด้านความหมายข้อมูล กรณีเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล เวอร์ชัน 1.0 ฉบับนี้จัดทำโดยฝ่ายมาตรฐานดิจิทัลภาครัฐ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
เลขที่ 120 อาคารศูนย์ราชการเฉลิมพระเกียรติฯ (อาคารซี) ชั้น 8 - 9
หมู่ 3 ซอยแจ้งวัฒนะ 7 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210
E-mail: sd-g3_division@dga.or.th
Website: www.dga.or.th

คำนำ

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร. หรือ DGA) ได้ประกาศมาตรฐาน การเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ (TGIX) เริ่มตั้งแต่ส่วนที่เป็นกรอบมาตรฐานกลางของภาครัฐไทย ที่กำหนดแนวทางการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน เพื่อให้หน่วยงานสามารถพัฒนา และเชื่อมโยงระบบสารสนเทศได้อย่างมีมาตรฐานเดียวกัน โดยแบ่งออกเป็นกลุ่มมาตรฐานฯ ด้านการเชื่อมโยงข้อมูล (Linkage Standards) และกลุ่มมาตรฐานฯ ด้านความหมายข้อมูล (Semantic Standards) โดยเอกสารฉบับนี้อยู่ในกลุ่มมาตรฐานด้านความหมายข้อมูล มุ่งเน้นที่โครงสร้างและความหมายของข้อมูลที่ใช้ในเอกสารรับรองและเอกสารสำแดงดิจิทัล

ในช่วงไม่กี่ปีที่ผ่านมาการยกระดับบริการภาครัฐสู่รูปแบบดิจิทัลและการออกแบบบริการแบบยึดประชาชนเป็นศูนย์กลาง ทำให้บทบาทของเอกสารดิจิทัลที่สามารถตรวจสอบได้ เช่น เอกสารรับรองดิจิทัล (Verifiable Credential: VC) และเอกสารสำแดงดิจิทัล (Verifiable Presentation: VP) มีความสำคัญมากยิ่งขึ้น แนวคิดดังกล่าวเชื่อมโยงกับหลักการอัตลักษณ์ดิจิทัลที่ประชาชนควบคุมข้อมูลของตนเอง (Self-Sovereign Identity: SSI) ซึ่งช่วยลดภาระการเชื่อมต่อเพื่อยืนยันตัวบุคคลกับระบบส่วนกลาง เพิ่มความเชื่อมั่นและประสิทธิภาพในการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างระบบ

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ. หรือ ETDA) ได้วางรากฐานด้านโครงสร้างข้อมูล VC/VP ผ่านข้อเสนอแนะมาตรฐาน ขมธอ. 24-2563 'โครงสร้างข้อมูลของเอกสารรับรองและเอกสารสำแดง' และรายงานทางเทคนิคด้านสถาปัตยกรรมและกรอบความน่าเชื่อถือ เช่น Thai VC Architecture and Reference Framework และ VC Trust Model Framework เพื่อกำหนดภาพรวมสถาปัตยกรรมระบบนิเวศ และกลไกความเชื่อถือของระบบเอกสารรับรองดิจิทัล สพร. เห็นว่าหากต้องการให้ระบบภาครัฐสามารถใช้ VC/VP ได้จริง จำเป็นต้องมีแนวปฏิบัติด้าน "ความหมายข้อมูล" ที่ชัดเจนและใช้งานได้จริงสำหรับนักพัฒนาระบบของหน่วยงาน เอกสารฉบับนี้ จึงจัดทำขึ้นเพื่อเป็นคู่มือเชิงปฏิบัติในการออกแบบชุดคำศัพท์ (vocabularies) และแอตทริบิวต์ ของข้อมูลให้สอดคล้องกับมาตรฐาน TGIX และกรอบของ สพธอ. โดยเน้นตัวอย่างการประยุกต์ใช้ กับใบอนุญาตขับขี่ และขยายไปสู่กรณีใช้งานอื่น ๆ ที่หน่วยงานสามารถนำไปปรับใช้ได้ เอกสารฉบับนี้ มุ่งช่วยให้นักพัฒนาระบบสารสนเทศของหน่วยงานภาครัฐสามารถออกแบบโครงสร้างข้อมูล VC/VP ให้สอดคล้องกับมาตรฐานสากล (เช่น W3C VC และ Decentralized Identifiers) ควบคู่กับมาตรฐาน TGIX และกรอบของ ETDA ลดความคลุมเครือด้านความหมายข้อมูล ลดไซโลข้อมูล และสนับสนุนให้ระบบบริการภาครัฐเชื่อมโยงกัน ได้อย่างน่าเชื่อถือ มั่นคงปลอดภัย และคุ้มครองความเป็นส่วนตัวของประชาชน

สารบัญ

สารบัญตาราง

สารบัญภาพ

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล
ว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ แนวปฏิบัติและหลักการพื้นฐาน ในการออกแบบ มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านความหมายข้อมูล กรณีเอกสารรับรองดิจิทัล และเอกสารสำแดงดิจิทัล

1. มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ แนวปฏิบัติและหลักการพื้นฐานในการออกแบบ มาตรฐานการเชื่อมโยง และแลกเปลี่ยนข้อมูลภาครัฐ ด้านความหมายข้อมูล กรณีเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล

1.1 ความเป็นมา

เพื่อยกระดับการบริหารงานและการให้บริการภาครัฐให้อยู่ในระบบดิจิทัล อันจะนำไปสู่การเป็นรัฐบาลดิจิทัล ที่มีระบบการทำงานและข้อมูลเชื่อมโยงกันระหว่างหน่วยงานของรัฐอย่างมั่นคงปลอดภัย มีประสิทธิภาพ รวดเร็ว เปิดเผยและโปร่งใส รวมทั้งประชาชนได้รับความสะดวกในการรับบริการและสามารถตรวจสอบการดำเนินงานของหน่วยงานของรัฐได้

เอกสารฉบับนี้มุ่งช่วยให้นักพัฒนาระบบสารสนเทศของหน่วยงานภาครัฐ สามารถเข้าใจถึงโครงสร้างข้อมูล VC/VP ในส่วนที่จำเป็น และสอดคล้องกับมาตรฐานสากล (เช่น W3C Verifiable Credentials Data Model) และโดเมนข้อมูลที่เป็นกรณีศึกษาที่อยู่ในรูปแบบของ VC/VP นี้ และสามารถนำโดเมนข้อมูลที่เป็นกรณีศึกษาในฉบับนี้ ปรับให้อยู่ในรูปแบบมาตรฐาน TGIX ตามกรอบของ สพธอ. หรือ ETDA ลดความคลุมเครือด้านความหมายข้อมูล เพิ่มความเชื่อมโยงของข้อมูลระหว่างหน่วยงาน และสนับสนุนให้ระบบบริการภาครัฐเชื่อมโยงกันได้อย่างน่าเชื่อถือ มั่นคงปลอดภัย และคุ้มครองความเป็นส่วนตัวของประชาชน

มาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัล ว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านความหมายข้อมูล ประกาศเพื่อเป็นแนวทางและข้อเสนอแนะให้กับหน่วยงานภาครัฐ เพื่อเป็นมาตรฐานกลางด้านการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ โดยครอบคลุมทั้งมิติด้านช่องทางการเชื่อมโยงและมิติด้านความหมายของข้อมูลที่ต้องตีความร่วมกันได้ สพร. จึงได้นำข้อเสนอแนะมาตรฐานของ สพธอ. (ETDA) “โครงสร้างข้อมูลของเอกสารรับรองและเอกสารสำแดง” เพื่อกำหนดโครงสร้างข้อมูลพื้นฐานสำหรับ VC และ VP รวมถึงอธิบายความเชื่อมโยงในการใช้งานเอกสารดังกล่าวระหว่าง issuer, holder และ verifier ต่อมาได้มีการจัดทำกรอบ Thai VC Architecture and Reference Framework และ VC Trust Model Framework เพื่อวางสถาปัตยกรรมและกรอบธรรมาภิบาลสำหรับระบบเอกสารรับรองดิจิทัล และกระเป๋าเอกสารดิจิทัลของไทย และเป็นการต่อยอดจากกรอบเชิงสถาปัตยกรรมและ trust framework เหล่านี้มาสู่แนวปฏิบัติด้าน “ความหมายข้อมูล” ชุดคำศัพท์หรือแอตทริบิวต์ เพื่อให้หน่วยงานสามารถ นำไปใช้ในการออกแบบระบบจริง โดยเริ่มจากกรณีตัวอย่างใบอนุญาตขับขี่ และขยายสู่เอกสารประเภทอื่น ในอนาคตต่อไป

1.2 วัตถุประสงค์

เอกสารฉบับนี้มีวัตถุประสงค์หลัก ดังนี้

- กำหนดแนวปฏิบัติและหลักการพื้นฐานในการออกแบบโครงสร้างข้อมูลและความหมายข้อมูลสำหรับเอกสารรับรองและเอกสารสำแดงดิจิทัลภาครัฐ ตามกรอบ TGIX และอ้างอิงมาตรฐาน ETDA ที่เกี่ยวข้อง
- แสดงตัวอย่างการประยุกต์ใช้ VC/VP กับข้อมูลใบอนุญาตขับขี่ของไทย โดยเชื่อมโยงกับแอตทริบิวต์ในมาตรฐาน GDX และข้อกำหนดสากล เช่น ISO 18013-5 เพื่อให้นักพัฒนามองเห็นแนวทางการปรับข้อมูลไปสู่ VC credential Subject และ namespace ตามมาตรฐาน TGIX
- เสนอแนวทางเชิงปฏิบัติสำหรับการเลือกใช้รูปแบบข้อมูลตามมาตรฐาน W3C VC Data Model และ SD-JWT รวมถึงโปรโตคอลสื่อสารอย่าง OID4VC ในการออกเอกสารรับรอง และเอกสารสำแดงเพื่อให้หน่วยงานผู้ตรวจสอบเอกสารดำเนินการตรวจสอบเป็นเอกสารอ้างอิงสำหรับหน่วยงานภาครัฐในการออกแบบ สร้าง และตรวจสอบเอกสาร รับรองดิจิทัลอย่างมีมาตรฐานเดียวกัน ช่วยลดความซ้ำซ้อนของการพัฒนาและเพิ่มความสามารถในการทำงานร่วมกันของระบบ

1.3 ขอบข่าย

ฉบับนี้ครอบคลุมแนวทางการออกแบบสถาปัตยกรรมระบบสำหรับการออก จัดเก็บ นำเสนอ และตรวจสอบเอกสารรับรองและเอกสารสำแดงดิจิทัล (VC/VP) ให้สอดคล้องกับกรอบแนวคิด และมาตรฐาน TGIX รวมทั้งแนวทางเกี่ยวกับรูปแบบการรับ-ส่งข้อมูล และการประยุกต์ใช้รูปแบบของ VC/VP เข้ากับระบบงานเดิมของหน่วยงาน เพื่อให้ระบบต่าง ๆ สามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพ นอกจากนี้ ยังครอบคลุมตัวอย่างรูปแบบการนำไปใช้ที่มุ่งสนับสนุนนักพัฒนาระบบในการออกแบบและพัฒนาระบบที่รองรับการทำงานร่วมกัน แนวทางการอ้างอิงและประยุกต์ใช้ข้อกำหนดทางเทคนิคจากรายงานทางเทคนิคและมาตรฐานที่เกี่ยวข้องของ ETDA และมาตรฐานสากล ตลอดจนแนวทางด้านความมั่นคงปลอดภัย การคุ้มครองข้อมูลส่วนบุคคล และหลักการ Data Minimization ในการนำ VC/VP ไปใช้ในบริบทของบริการภาครัฐดิจิทัลอย่างเหมาะสม

ทั้งนี้ การจัดทำเอกสารฉบับนี้มิได้มีวัตถุประสงค์เพื่อกำหนดข้อกำหนดทางเทคนิคใหม่ หากแต่เป็นการสนับสนุนการนำมาตรฐานและรายงานทางเทคนิคที่หน่วยงานที่เกี่ยวข้อง โดยเฉพาะสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) ที่ได้จัดทำไว้แล้ว ไปประยุกต์ใช้ในบริบทของการพัฒนาระบบภาครัฐให้เกิดผลในทางปฏิบัติ

1.4 บทนิยาม

“เอกสารรับรองดิจิทัล (Verifiable Credential: VC)” หมายความว่า ชุดของข้อความยืนยันอย่างน้อยหนึ่งรายการที่ถูกรับรองโดยผู้ออกเอกสาร (Issuer) ทั้งนี้เอกสาร VC มีคุณสมบัติที่สามารถตรวจพบการเปลี่ยนแปลงใด ๆ ที่เกิดกับความถูกต้องครบถ้วนของข้อมูล และตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ของผู้ออกเอกสารได้ด้วยกระบวนการเข้ารหัสลับ

“เอกสารสำแดงดิจิทัล (Verifiable Presentation: VP)” หมายความว่า VC อย่างน้อยหนึ่งชุด ที่ผู้ถือเอกสาร (Holder) ใช้แสดงต่อผู้ตรวจสอบเอกสาร (Verifier) ทั้งนี้เอกสาร VP มีคุณสมบัติที่สามารถตรวจพบการเปลี่ยนแปลงใด ๆ ที่เกิดกับความถูกต้องครบถ้วนของข้อมูล และตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ของผู้ถือเอกสารและตรวจสอบ VC เกี่ยวข้องได้ด้วยกระบวนการเข้ารหัสลับ

“ผู้ออกเอกสาร (Issuer)” หมายความว่า เอนทิตีที่ทำหน้าที่รับรองข้อความยืนยันโดยออกเป็น VC ให้แก่ผู้ถือเอกสาร

“ผู้ถือเอกสาร (Holder)” หมายความว่า เอนทิตีที่เป็นเจ้าของ VC อย่างน้อยหนึ่งชุด โดยจัดเก็บไว้ในกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) และสามารถใช้ VC สร้างเป็น VP ทั้งนี้ ผู้ถือเอกสารมีอีกชื่อเรียกหนึ่งว่า ผู้ใช้งานกระเป๋าเอกสารดิจิทัล

“ผู้ตรวจสอบเอกสาร (Verifier)” หมายความว่า เอนทิตีที่สามารถตรวจสอบความถูกต้องครบถ้วนของ VC และ VP ด้วยกระบวนการเข้ารหัสลับ รวมถึงตรวจสอบสถานะการใช้งานและความสอดคล้องตามโครงสร้างข้อมูลของ VC และ VP

“กระเป๋าเอกสารดิจิทัล (Digital Document Wallet)” หมายความว่า โปรแกรมที่จัดเก็บและช่วยให้ผู้ถือเอกสารสามารถเข้าถึงและใช้งาน VC ได้อย่างมั่นคงปลอดภัย

“ผู้ให้บริการกระเป๋าเอกสารดิจิทัล (Digital Document Wallet Provider)” หมายความว่า เอนทิตีที่ทำหน้าที่พัฒนาและ/หรือดำเนินการเกี่ยวกับกระเป๋าเอกสารดิจิทัล ให้แก่ผู้ออกเอกสาร ผู้ถือเอกสาร หรือผู้ตรวจสอบเอกสาร

“โครงสร้างพื้นฐานด้านความน่าเชื่อถือ (Trust Infrastructure)” หมายความว่า กลไกหรือระบบที่สนับสนุนการตรวจสอบความถูกต้องของเอกสารรับรอง เช่น ระบบทะเบียนผู้ออกเอกสาร ระบบบริหารกุญแจดิจิทัล หรือระบบตรวจสอบสถานะ

“การเลือกเปิดเผยข้อมูลบางส่วน (Selective Disclosure)” หมายความว่า กลไกที่เปิดโอกาสให้ผู้ถือเอกสารเปิดเผยเฉพาะข้อมูลที่จำเป็นต่อวัตถุประสงค์ของการตรวจสอบ โดยไม่ต้องเปิดเผยข้อมูลทั้งหมดในเอกสารรับรอง

“กลไกการตรวจสอบสถานะ (Credential Status Mechanism)” หมายความว่า กลไกสำหรับตรวจสอบว่าเอกสารรับรองยังมีผลบังคับใช้ ถูกระงับ หรือถูกเพิกถอน

“กรอบบริการเกี่ยวกับระบบเอกสารรับรอง (VC Trust Framework)” หมายความว่า ชุดข้อกำหนดที่กำหนด บทบาท หน้าที่ และกระบวนการปฏิบัติงาน (Operational Process) ที่จำเป็นในการสร้างความเชื่อมั่นในระบบนิเวศของเอกสารรับรอง (VC ecosystem) รวมถึงเทคนิคด้านความมั่นคงปลอดภัยสำหรับกระบวนการออกเอกสาร VC การใช้งานเอกสาร VP และการตรวจสอบความน่าเชื่อถือของเอกสาร

1.5 กฎหมายและแนวปฏิบัติที่เกี่ยวข้อง

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ แนวปฏิบัติและหลักการพื้นฐาน ในการออกแบบ มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านความหมายข้อมูล กรณีเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล มีความเกี่ยวข้องกับกฎหมายหรือแนวปฏิบัติ ดังนี้

1.5.1 พระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. 2565 และกฎหมายที่เกี่ยวข้อง

1.5.2 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม

1.5.3 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1.5.4 มาตรฐานรัฐบาลดิจิทัล ว่าด้วยกรอบแนวทางการพัฒนามาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ (Thailand Government Information eXchange :TGIX) (มรด. 2-1:2565)

1.5.5 มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านความหมายข้อมูล เรื่องข้อมูลบุคคล (มสพร. 4-2565) และเรื่องข้อมูลนิติบุคคล (มสพร.5-2565)

1.5.6 มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐด้านความหมายข้อมูล เรื่องข้อมูลสถานที่-ที่อยู่ (มสพร. 9-1:2566)

1.5.7 ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยโครงสร้างข้อมูลของเอกสารรับรองและเอกสารสำแดง (ขมธอ. 24-2563)

1.5.8 รายงานทางเทคนิค เรื่อง กรอบการทำงานร่วมกันของกระเป๋าเอกสารดิจิทัลสำหรับเอกสารรับรอง พ.ศ. 2566 สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

1.5.9 รายงานทางเทคนิค เรื่อง กรอบแนวทางการทำงานร่วมกันของเอกสารรับรองดิจิทัลสำหรับประเทศไทย พ.ศ. 2568 สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

1.5.10 รายงานทางเทคนิค เรื่อง กรอบการสร้างความน่าเชื่อถือของเอกสารรับรองและเอกสารสำแดง พ.ศ. 2568 สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

1.5.11 มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยแนวปฏิบัติกระบวนการทางดิจิทัลภาครัฐ - ส่วนที่ 8 เรื่องเอกสารใบอนุญาตอิเล็กทรอนิกส์ภาครัฐในรูปแบบเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล เวอร์ชัน 1.0

2. การประยุกต์ใช้ใบอนุญาตอิเล็กทรอนิกส์ในรูปแบบ VC/VP

จากใบอนุญาตอิเล็กทรอนิกส์ของหน่วยงานภาครัฐจากรูปแบบเอกสารดิจิทัลทั่วไป สู่รูปแบบเอกสารรับรองดิจิทัล (Verifiable Credential: VC) และเอกสารสำแดงดิจิทัล (Verifiable Presentation: VP) ถือเป็นการปรับเปลี่ยนแนวทางการจัดการข้อมูลใบอนุญาตให้สามารถตรวจสอบความถูกต้อง และแหล่งที่มาของข้อมูลได้ด้วยกลไกทางเทคโนโลยีที่น่าเชื่อถือ อีกทั้งยังรองรับการใช้งานในสภาพแวดล้อมดิจิทัลที่มีการเชื่อมโยงข้อมูลระหว่างหน่วยงานอย่างเป็นระบบ

แนวทางดังกล่าวมุ่งให้หน่วยงานของรัฐสามารถออกใบอนุญาตในรูปแบบที่มีโครงสร้างข้อมูลชัดเจน สามารถพิสูจน์แหล่งที่มา และสถานะของเอกสารได้ ขณะเดียวกันผู้ถือเอกสารใบอนุญาตสามารถเลือกเปิดเผยข้อมูลเฉพาะส่วนที่จำเป็นผ่านเอกสารสำแดง โดยไม่จำเป็นต้องเปิดเผยข้อมูลทั้งหมด อันเป็นการส่งเสริมทั้งความน่าเชื่อถือ ความมั่นคงปลอดภัย และการคุ้มครองข้อมูลส่วนบุคคล โดยในบทนี้จะนำเสนอแนวคิด มาตรฐาน และองค์ประกอบที่เกี่ยวข้อง เพื่อเป็นพื้นฐานให้ผู้พัฒนาระบบเข้าใจภาพรวมของกระบวนการ VC/VP และสามารถนำไปประยุกต์ใช้ได้จริงในบทถัดไป

2.1 แนวคิดในเอกสารกำหนดกรอบของเอกสารรับรองและเอกสารสำแดงที่ประกาศโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.)

ในการยกระดับเอกสารภาครัฐสู่รูปแบบอิเล็กทรอนิกส์ที่สามารถตรวจสอบความถูกต้อง และแหล่งที่มาได้ จำเป็นต้องอาศัยโครงสร้างพื้นฐานทางเทคนิคที่อยู่ในข้อกำหนด หรือกรอบมาตรฐานเดียวกัน ในช่วงเวลาที่ผ่านมาสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ได้จัดทำประกาศกรอบมาตรฐานและรายงานทางเทคนิคที่เกี่ยวข้องกับเอกสารรับรองดิจิทัลไว้ ซึ่งทำหน้าที่เป็นโครงสร้างพื้นฐานเชิงแนวคิด (Conceptual Foundation) และโครงสร้างพื้นฐานเชิงระบบ (Infrastructure Foundation) สำหรับการพัฒนา VC/VP ในระดับประเทศ ครอบคลุมมิติสำคัญ ดังนี้

- มิติโครงสร้างข้อมูลของเอกสารรับรองและเอกสารสำแดง
- มิติการทำงานร่วมกันของกระเป๋าเอกสารดิจิทัล
- มิติการทำงานร่วมกันของเอกสารรับรองในระดับประเทศ
- มิติการสร้างความน่าเชื่อถือและกลไกกำกับดูแล

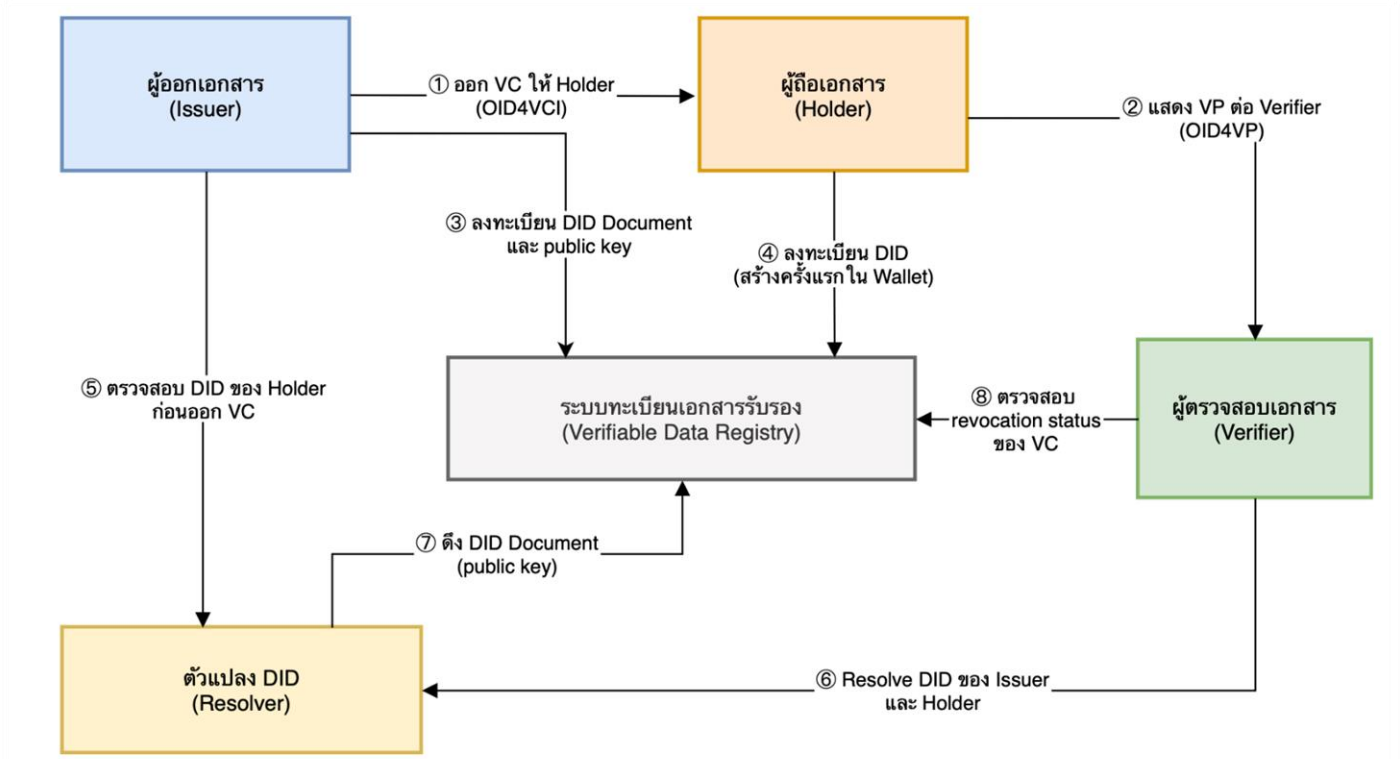
โดยกรอบดังกล่าวทำหน้าที่กำหนด “หลักการขั้นต่ำที่ระบบควรมี” เพื่อให้เอกสารรับรองดิจิทัลสามารถ

- ตรวจสอบความถูกต้องครบถ้วนได้ด้วยกระบวนการเข้ารหัสลับ
- ใช้งานข้ามหน่วยงานได้โดยไม่ต้องพัฒนาเชื่อมต่อแบบเฉพาะกิจ
- บริหารสถานะใบอนุญาตได้อย่างเป็นระบบ
- มีโครงสร้างพื้นฐานด้านความเชื่อถือรองรับในระดับระบบนิเวศ

ซึ่งได้ประกาศกรอบมาตรฐานและรายงานทางเทคนิคจำนวน 4 ฉบับ เอกสารมาตรฐานฉบับนี้จัดทำขึ้นโดยสนับสนุนการนำมาตรฐาน และรายงานทางเทคนิคที่หน่วยงานที่เกี่ยวข้อง ในข้อกำหนดและประกาศของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ได้แก่ ข้อเสนอแนะมาตรฐานว่าด้วยโครงสร้างข้อมูล

ของเอกสารรับรองและเอกสารสำแดง (ขมธอ. 24-2563) กรอบการทำงานร่วมกันของกระเป๋าเอกสารดิจิทัลสำหรับเอกสารรับรอง พ.ศ. 2566 และรายงานทางเทคนิคฉบับปี พ.ศ. 2568 ได้แก่ กรอบแนวทางการทำงานร่วมกันของเอกสารรับรองดิจิทัลสำหรับประเทศไทย (Thai VC ARF) และกรอบการสร้างความน่าเชื่อถือของเอกสารรับรองและเอกสารสำแดง (Trust Model Framework ซึ่งประกอบด้วย VCTF และ VCGF)

เพื่อให้นักพัฒนาระบบสารสนเทศของหน่วยงาน เข้าใจในภาพรวมของกระบวนการทำงาน และกลไกของเอกสารรับรอง/เอกสารสำแดง (VC/VP) มากขึ้น จึงขอนำเสนอถึงความเชื่อมโยงของกระบวนการ VC/VP ดังกล่าว



ภาพที่ 1 ภาพรวมของกระบวนการ VC และ VP โดยแยกในแต่ละส่วน

จากภาพที่ 1 อธิบายกระบวนการ VC และ VP ในแต่ละส่วน ตามแต่ละขั้นตอนดังนี้

กระบวนการออกเอกสารรับรอง (VC Issuance) : ขั้นตอน 1 --> 3 --> 4 --> 5 --> 7

กระบวนการแสดงและตรวจสอบเอกสาร (VP Verification) : ขั้นตอน 2 --> 6 --> 7 --> 8

1) ผู้ออกเอกสาร (Issuer) --> ผู้ถือเอกสาร (Holder) : **ออก VC**

   ผู้ออกเอกสาร (Issuer) ออกเอกสารรับรอง (VC) ซึ่งมีการลงลายมือชื่อดิจิทัล (Digital Signature) แล้วส่งให้ผู้ถือเอกสาร (Holder) ผ่านโปรโตคอล OID4VCI โดยผู้ถือเอกสารจะจัดเก็บ VC ไว้ในกระเป๋าเอกสารดิจิทัล (Digital Wallet)

2) ผู้ถือเอกสาร (Holder) --> ผู้ตรวจสอบเอกสาร (Verifier) : **แสดง VP**

   ผู้ถือเอกสารนำ VC มาสร้างเป็นเอกสารสำแดง (VP) โดยลงลายมือชื่อดิจิทัลด้วยกุญแจส่วนตัว (private key) ของตนเอง เพื่อยืนยันความเป็นเจ้าของ (Proof of Possession) และส่งให้ผู้ตรวจสอบเอกสาร (Verifier) ผ่านโปรโตคอล OID4VP

3) ผู้ออกเอกสาร (Issuer) --> ระบบทะเบียนเอกสารรับรอง (VDR) : **ลงทะเบียน DID Document**

   ผู้ออกเอกสารลงทะเบียน DID Document (Decentralized Identifier Document) พร้อม public key ของตนในระบบทะเบียนเอกสารรับรอง (Verifiable Data Registry: VDR) เพื่อให้สามารถนำไปใช้ตรวจสอบลายมือชื่อดิจิทัลได้ในภายหลัง

4) ผู้ถือเอกสาร (Holder) --> ระบบทะเบียนเอกสารรับรอง (VDR) : **ลงทะเบียน DID**

   ผู้ถือเอกสารสร้าง DID (Decentralized Identifier) เมื่อเริ่มใช้งาน Wallet

   - กรณี did:web ต้องลงทะเบียน DID Document กับ VDR
   - กรณี did:key ไม่ต้องลงทะเบียน เนื่องจาก public key ถูกฝังอยู่ใน DID แล้ว

5) ผู้ออกเอกสาร (Issuer) --> Resolver : **ตรวจสอบ DID ของผู้ถือเอกสาร (Holder)**

   ก่อนออก VC ผู้ออกเอกสารต้องตรวจสอบ DID ของผู้ถือเอกสาร โดยใช้ Resolver เพื่อทำการ resolve DID และดึง DID Document เพื่อตรวจสอบ public key และยืนยันความเป็นเจ้าของกุญแจ (Proof of Possession)

6) ผู้ตรวจสอบเอกสาร (Verifier) --> Resolver : **Resolve DID ของทั้ง Issuer และ Holder**

   ผู้ตรวจสอบเอกสารใช้ Resolver เพื่อดึงข้อมูล (resolve) DID ของทั้ง Issuer และ Holder ซึ่งจะได้ public key มาใช้ตรวจสอบลายมือชื่อดิจิทัลทั้งสองส่วน ได้แก่

   - ลายมือชื่อของ VC (จาก Issuer)
   - ลายมือชื่อของ VP (จาก Holder)

7) Resolver --> ระบบทะเบียนเอกสารรับรอง (VDR) : **ดึง DID Document**

Resolver ทำหน้าที่แปลง DID ให้เป็น DID Document โดยไปดึงข้อมูลจาก VDR ซึ่งอาจมีหลายรูปแบบ เช่น

- Blockchain HTTPS
- Endpoint
- DNS

จะเห็นได้ว่า Resolver จะเป็นตัวกลางที่รู้วิธีเข้าถึง VDR ในแต่ละรูปแบบ

8) ผู้ตรวจสอบเอกสาร (Verifier) --> ระบบทะเบียนเอกสารรับรอง (VDR) : **ตรวจสถานะการยกเลิก (revocation status)**

ผู้ตรวจสอบเอกสารตรวจสอบสถานะของ VC โดยตรงกับ VDR ว่าเอกสารถูกเพิกถอน (revoked) หรือไม่ ผ่านกลไก เช่น StatusList2021 โดยขั้นตอนนี้ไม่ต้องผ่าน Resolver เนื่องจากเป็นการเรียกใช้ HTTP endpoint โดยตรง

จากกระบวนการดังกล่าวจะเห็นได้ว่า การทำงานของเอกสารรับรอง (Verifiable Credential: VC) และเอกสารสำแดง (Verifiable Presentation: VP) อาศัยการทำงานร่วมกันของหลายองค์ประกอบ ทั้งผู้ออกเอกสาร ผู้ถือเอกสาร ผู้ตรวจสอบเอกสาร ตลอดจนกลไกสนับสนุน เช่น DID, Resolver และระบบทะเบียนเอกสารรับรอง (Verifiable Data Registry: VDR) ซึ่งทำหน้าที่ในการสร้างความน่าเชื่อถือให้กับข้อมูลผ่านการพิสูจน์ตัวตน การลงลายมือชื่อดิจิทัล และการตรวจสอบสถานะของเอกสาร

เพื่อให้หน่วยงานภาครัฐสามารถนำแนวทางดังกล่าวไปประยุกต์ใช้ได้อย่างถูกต้องและสอดคล้องกับมาตรฐาน จำเป็นต้องทำความเข้าใจมาตรฐานที่เกี่ยวข้อง ตลอดจนโครงสร้างของข้อมูลและรายการแอตทริบิวต์ ที่ใช้ในการพิสูจน์ตัวตนและออกเอกสารรับรอง ดังนั้น ในหัวข้อถัดไปจะนำเสนอรายละเอียดของมาตรฐานที่เกี่ยวข้อง รวมถึงแนวทางการกำหนดรายการข้อมูลสำหรับการพิสูจน์ตัวตนตามมาตรฐานดังกล่าว

2.2 มาตรฐานที่เกี่ยวข้อง

เพื่อให้หน่วยงานภาครัฐสามารถนำกรอบแนวคิดดังกล่าวไปพัฒนาระบบสารสนเทศในเรื่องเอกสารรับรอง และเอกสารสำแดงได้จริง พร้อมทั้งสามารถนำมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ (TGIX) มาประยุกต์ใช้ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) จึงได้กำหนดแนวทางการปรับรูปแบบของชุดข้อมูลที่อยู่ในรูปแบบ JSON ของเอกสารรับรอง ให้อยู่ในโครงสร้างมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ (TGIX) โดยมีกรณีศึกษาคือ "ใบอนุญาตขับขี่ (รถยนต์)" ภายใต้เทคโนโลยี Verifiable Credential (VC) และโปรโตคอลการรับส่งข้อมูลที่สอดคล้องกับมาตรฐานสากล

การประยุกต์ใช้งานเอกสารรับรอง (Verifiable Credential: VC) และเอกสารสำแดง (Verifiable Presentation: VP) ตามแนวทางในเอกสารนี้ อ้างอิงมาตรฐานและเอกสารที่เกี่ยวข้องทั้งในระดับสากลและระดับประเทศไทย เพื่อให้การพัฒนาระบบสามารถทำงานร่วมกันได้ (Interoperability) และสอดคล้องกับกรอบการกำกับดูแลของภาครัฐ โดยมีรายละเอียดดังนี้

2.2.1 มาตรฐานระดับสากล (International Standards)

มาตรฐาน/เอกสาร	ปีที่ประกาศ	คำอธิบาย
W3C Verifiable Credentials Data Model 2.0[1]	พ.ศ. 2568 (ค.ศ. 2025)	มาตรฐานแกนหลักที่พัฒนาต่อยอดจาก v1.1 โดยปรับเปลี่ยนจากข้อบังคับเดิมที่ต้องใช้ JSON-LD และ @context มาเป็นการรองรับข้อมูลแบบ Multi-format ผ่าน Media Types (เช่น JWT, CBOR)
OpenID for Verifiable Credential Issuance (OID4VCI) / VP[2]	พ.ศ. 2568 (ค.ศ. 2025)	โปรโตคอลมาตรฐานบนพื้นฐานของ OAuth 2.0 และ OpenID Connect ที่ใช้สำหรับการออกเอกสาร (Issuance) และการสำแดงเอกสาร (Presentation)
Decentralized Identifiers (DID)[3]	พ.ศ. 2565 (ค.ศ. 2022)	มาตรฐาน W3C สำหรับตัวระบุดิจิทัลแบบกระจายศูนย์ที่ใช้ระบุเอนทิตี เช่น บุคคล องค์กร หรือระบบ
Trust over IP (ToIP)[4]	เวอร์ชัน 1.0 พ.ศ. 2565 (ค.ศ. 2022)	กรอบการทำงานความน่าเชื่อถือดิจิทัลแบบ 4 ชั้น (Four-layer stack) ซึ่งเป็นสถาปัตยกรรมอ้างอิงในการออกแบบทั้งด้านเทคนิคและธรรมาภิบาล เพื่อสร้างระบบนิเวศความเชื่อมั่น (Digital Trust Ecosystem)
ISO/IEC 18013-5	พ.ศ. 2564 (ค.ศ. 2021)	มาตรฐานเฉพาะสำหรับการออกใบอนุญาตขับขี่บนอุปกรณ์พกพา (Mobile Driving License: mDL) โดยเน้นกระบวนการตรวจสอบข้อมูลในระยะใกล้ (Offline/Proximity Verification)

ตารางที่ 1 ตารางมาตรฐานสากลที่เกี่ยวข้องกับเอกสารรับรอง และเอกสารสำแดง

[1] https://www.w3.org/TR/vc-data-model/

[2] ttps://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html

[3] https://www.w3.org/TR/did-1.0/

[4] https://trustoverip.org

2.2.2 มาตรฐานและข้อเสนอแนะระดับประเทศไทย (Thai ETDA Standards)

มาตรฐาน/เอกสาร	ปีที่ประกาศ	คำอธิบาย
ขมธอ. 24-2563[5]	พ.ศ. 2563 (ค.ศ. 2020)	ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยโครงสร้างข้อมูลของเอกสารรับรองและเอกสารสำแดง
INTEROPERABLE FRAMEWORK OF DIGITAL WALLETS FOR VERIFIABLE CREDENTIALS	พ.ศ. 2566	กรอบการทำงานร่วมกันของกระเป๋าเอกสารดิจิทัลสำหรับเอกสารรับรอง พ.ศ. 2566 สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
THAI VC ARCHITECTURE AND REFERENCE FRAMEWORK	มกราคม พ.ศ. 2568	กรอบแนวทางการทำงานร่วมกันของเอกสารรับรองดิจิทัลสำหรับประเทศไทย พ.ศ. 2568 สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
Trust Model Framework for Verifiable Credential (VC) and Verifiable Presentation (VP)	ธันวาคม พ.ศ. 2568	กรอบการสร้างความน่าเชื่อถือของเอกสารรับรองและเอกสารสำแดง พ.ศ. 2568 สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ตารางที่ 2 ตารางมาตรฐานและข้อเสนอแนะระดับประเทศไทย

เมื่อนำมาพัฒนาระบบนิเวศเอกสารรับรองดิจิทัล (VC Ecosystem) ภาครัฐ จะเกิดการทำงานร่วมกันผ่านมาตรฐานทางเทคนิคที่สำคัญ ดังนี้

1) มาตรฐานโครงสร้างข้อมูล (Data Model & Schema): อ้างอิงมาตรฐาน W3C Verifiable Credentials Data Model (v1.1 และ v2.0) ซึ่งรองรับการเข้ารหัสข้อมูลในรูปแบบ JSON-LD (JavaScript Object Notation for Linked Data) และ JWT (JSON Web Token) รวมถึงเทคโนโลยี SD-JWT (Selective Disclosure JWT) ที่ช่วยให้ผู้ใช้งานสามารถเลือกเปิดเผยข้อมูลเฉพาะบางส่วนได้ เพื่อการคุ้มครองข้อมูลส่วนบุคคล (Privacy by Design)
2) กรอบสถาปัตยกรรมอ้างอิง (Architecture and Reference Framework - ARF): อ้างอิงตามรายงานทางเทคนิคของ สพธอ. ปี 2568 ในการกำหนดโครงสร้างการทำงานร่วมกันระหว่าง ผู้ออกเอกสาร (Issuer) ผู้ถือเอกสาร (Holder) และผู้ตรวจสอบเอกสาร (Verifier)
3) กรอบความน่าเชื่อถือ (VC Trust Model Framework): อ้างอิงกรอบด้านเทคนิค (VCTF) และกรอบด้านธรรมาภิบาล (VCGF) เพื่อใช้กำหนดเกณฑ์ความมั่นคงปลอดภัย การจัดการตัวระบุแบบกระจายศูนย์ (DID) และรายการเพิกถอน (Revocation Registry)

[5] https://www.etda.or.th/getattachment/Our-Service/Standard/ETDA-Recommendation/Information/ดาวนโหลดมาตรฐาน/ETDA-Recommendation-(1)/แสดงเอกสารทงหมด/ขมธอ-24-2563/20200914-DataStructure-VC-VP_V08-1.pdf.aspx

2.3 รายการข้อมูลสำหรับการพิสูจน์ตัวตนตามมาตรฐานที่เกี่ยวข้อง

ในการประยุกต์ใช้เอกสารรับรอง (VC) และเอกสารสำแดง (VP) จำเป็นต้องเข้าใจข้อกำหนดของโปรโตคอล OID4VCI และ OID4VP ซึ่งเป็นส่วนขยายที่พัฒนาต่อยอดจาก OpenID Connect (OIDC) โดยมาตรฐานดังกล่าวกำหนดกลไกการสื่อสาร และรูปแบบการรับ-ส่งข้อมูลในกระบวนการออกรับรองและเอกสารสำแดงอย่างเป็นระบบ ขณะเดียวกันรายการข้อมูล และแอตทริบิวต์ที่ใช้ในการพิสูจน์ตัวตน ยังคงอ้างอิงจากแนวคิดของ OIDC ซึ่งทำงานร่วมกันกับโครงสร้างข้อมูลของ VC เพื่อให้สามารถแลกเปลี่ยนและตรวจสอบข้อมูลได้ ดังนั้นในหัวข้อนี้จะนำเสนอแนวทางการใช้แอตทริบิวต์ตามมาตรฐานดังกล่าว โดยจะอธิบายในรายละเอียดในหัวข้อถัดไป

2.3.1 OpenID Connect (OIDC) และบทบาทในระบบ VC/VP

OpenID Connect (OIDC) เป็นมาตรฐานข้อกำหนดสำหรับการพิสูจน์ตัวตน (Authentication) ที่พัฒนาบนพื้นฐานของ OAuth 2.0 โดยใช้ในการพิสูจน์ตัวตนระหว่างผู้ให้บริการพิสูจน์ตัวตน (Identity Provider: IdP) และผู้ให้บริการ (Relying Party: RP) ซึ่งโดยทั่วไปมีลักษณะการทำงานแบบรวมศูนย์หรืออาศัยตัวกลาง OIDC ยังเป็นแหล่งกำเนิดของข้อมูลแอตทริบิวต์ (Claims) ที่ใช้ในการพิสูจน์ตัวตน โดยข้อมูลดังกล่าวมักเป็นข้อมูลพื้นฐานของผู้ใช้ เช่น sub name given_name family_name email phone_number birthdate และ address ซึ่งสามารถนำไปใช้เป็นข้อมูลตั้งต้นในกระบวนการออกเอกสารรับรอง (VC) ได้

2.3.2 OID4VCI และ OID4VP (OpenID for VC Issuance / VP Exchange)

OID4VCI และ OID4VP[6] เป็นข้อกำหนดที่พัฒนาต่อยอดจาก OIDC เพื่อรองรับการทำงานในบริบทของ VC โดยอาศัยโครงสร้างพื้นฐานของ OAuth 2.0 และ JSON Web Token (JWT) เช่นเดียวกับ OIDC

- OID4VCI ใช้ในฝั่งผู้ออกเอกสาร (Issuer) เพื่อกำหนดกระบวนการยืนยันสิทธิ และการออกเอกสารรับรอง (VC) ไปยังกระเป๋าเอกสารดิจิทัล (Wallet) ของผู้ใช้งาน
- OID4VP ใช้ในฝั่งผู้ตรวจสอบเอกสาร (Verifier) เพื่อกำหนดกระบวนการร้องขอ และรับเอกสารสำแดง (VP) จากผู้ใช้งานผ่าน Wallet

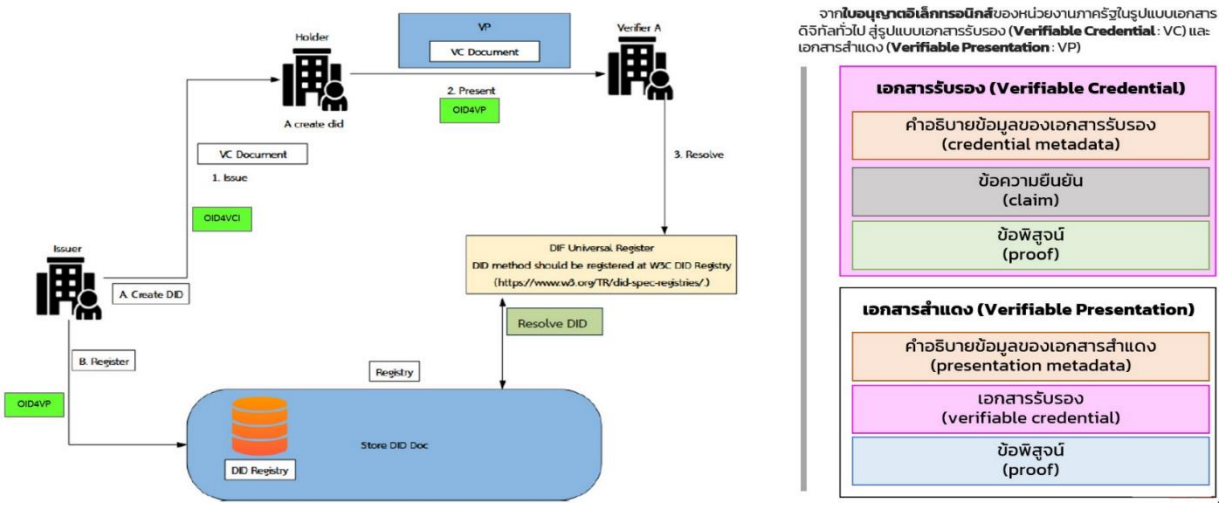
แนวทางดังกล่าวสะท้อนการเปลี่ยนแปลงจากรูปแบบการพึ่งพาผู้ให้บริการพิสูจน์ตัวตนส่วนกลางไปสู่รูปแบบที่ผู้ใช้งานสามารถควบคุม และนำเสนอข้อมูลของตนเองได้ (User-centric) โดยยังคงสามารถตรวจสอบความถูกต้องของข้อมูลได้ผ่านกลไกของ VC/VP

[6] OpenID Foundation, "OpenID for Verifiable Credential Issuance 1.0", September 2025

ด้านที่เปรียบเทียบ	OIDC	OID4VCI / OID4VP	หมายเหตุ
วัตถุประสงค์	ยืนยันตัวตน ส่ง ID Token (JWT)	ออกเอกสารรับรองและสำแดง VC/VP	ขยายขีดความสามารถ
ผู้กำหนดมาตรฐาน	OpenID Foundation (OIDF)	OpenID Foundation (OIDF) ส่วนขยาย	ต่อยอดจาก OIDC
รูปแบบข้อมูล	JWT ID Token และ Claims	JWT-VC, JSON-LD, SD-JWT	หลายรูปแบบ
โฟล์วหลัก	Authorization Code Flow	Credential Issuance/Presentation	ใช้ OAuth 2.0 ร่วม

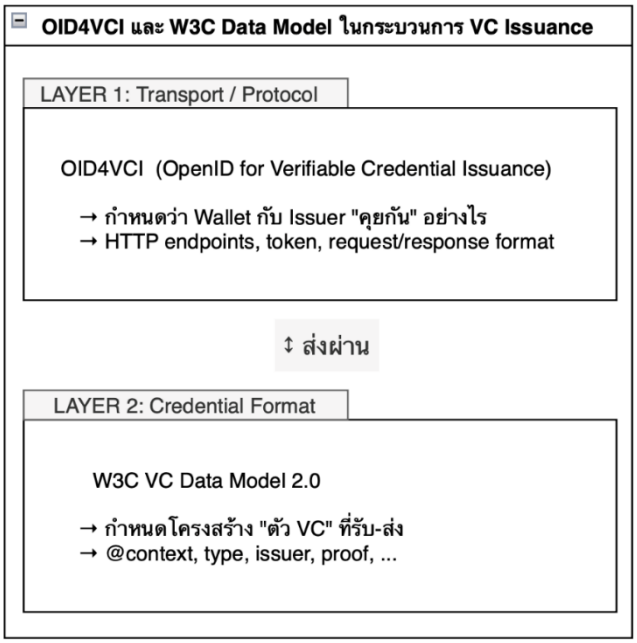
ตารางที่ 3 การเปรียบเทียบ OIDC กับ OID4VCI / OID4VP

OID4VCI และ OID4VP เป็นการขยายความสามารถของมาตรฐาน OpenID Connect เพื่อรองรับการออกเอกสารรับรอง (VC) และเอกสารสำแดง (VP) ในบริบทของระบบนิเวศตัวตนดิจิทัล โดย OID4VCI ทำหน้าที่กำหนดรูปแบบ และขั้นตอนการสื่อสารระหว่างผู้ออกเอกสาร (Issuer) และผู้ถือเอกสาร (Holder) ในกระบวนการออก VC ขณะที่ OID4VP ใช้สำหรับกำหนดกลไกการร้องขอ และการแสดง VP ระหว่างผู้ถือเอกสาร (Holder) และผู้ตรวจสอบเอกสาร (Verifier) ซึ่งทั้งสองส่วนนี้ยังคงอาศัยแนวคิดพื้นฐานของข้อกำหนด OIDC เช่น การใช้โทเคน (token), เอนพอยท์ (endpoint) และรูปแบบการร้องขอ (request)/การตอบกลับ (response) เพื่อให้สามารถนำไปประยุกต์ใช้ร่วมกับระบบเดิมได้อย่างต่อเนื่อง เมื่อพิจารณาร่วมกับโครงสร้างข้อมูลของ W3C Verifiable Credentials Data Model



ภาพที่ 2 แสดงถึงโปรโตคอล OID4VCI และ OID4VP และ W3C VC ในกระบวนการการทำงานของ VC/VP

จะเห็นได้ว่า OID4VCI และ OID4VP ทำหน้าที่ในระดับโปรโตคอลการสื่อสาร (Transport / Protocol) ขณะที่ W3C VC Data Model ทำหน้าที่กำหนดโครงสร้างของข้อมูลภายในเอกสารรับรอง ซึ่งสอดคล้องกับภาพไดอะแกรม โดยเป็นไปตามกรอบแนวทางการทำงานร่วมกันของเอกสารรับรองดิจิทัลสำหรับประเทศไทย (THAI VC ARCHITECTURE AND REFERENCE FRAMEWORK) เวอร์ชัน 1.1 (ภาพที่ 3)



ภาพที่ 3 OID4VCI และ W3C Data Model ในกระบวนการ VC Issuance

จากภาพจะแสดงให้เห็นการทำงานในส่วนของโปรโตคอล OID4VCI และ W3C VC Data Model โดย **OID4VCI เปรียบได้กับระบบไปรษณีย์ที่กำหนดวิธีการส่งพัสดุ** ตั้งแต่รูปแบบการรับ-ส่ง การพิสูจน์ตัวตน ไปจนถึงขั้นตอนการสื่อสารระหว่างผู้ส่งและผู้รับ ขณะที่ **W3C Verifiable Credentials Data Model หรือ VC เปรียบเสมือนตัวพัสดุ**ข้างใน ซึ่งกำหนดโครงสร้าง และเนื้อหาของข้อมูลที่ถูกบรรจุและส่งออกไป ดังนั้น แม้ว่าวิธีการจัดส่งจะเป็นไปตามมาตรฐานเดียวกัน แต่ความหมายของข้อมูลจะขึ้นอยู่กับโครงสร้างของ “พัสดุ” ที่ถูกกำหนดไว้อย่างเป็นระบบภายในนั้น

- OID4VCI = ระบบไปรษณีย์ (วิธีส่งพัสดุ)
- W3C VC หรือ VC = ตัวพัสดุข้างใน (เนื้อหาที่ส่ง) ความหมายของข้อมูลจะขึ้นอยู่กับโครงสร้างของ “พัสดุ” เช่น ข้อมูลใบอนุญาตขับขี่ ข้อมูลใบประมวลผลการศึกษา เป็นต้น

ทั้งนี้เพื่อให้ข้อมูลภายในเอกสารสามารถนำไปใช้ร่วมกันได้อย่างมีประสิทธิภาพในระดับภาครัฐ จำเป็นต้องเข้าใจถึงชุดแอตทริบิวต์และข้อมูลยืนยันตัวตนที่เป็นมาตรฐานร่วมกัน ซึ่งจะกล่าวถึงในหัวข้อถัดไป

2.3.3 แอตทริบิวต์และข้อมูลยืนยันตัวตนที่ใช้ร่วมกัน

ในมาตรฐาน OpenID Connect (OIDC) รายการข้อมูลสำหรับการพิสูจน์ตัวตน (Claims) ถูกกำหนดผ่านทั้ง ID Token และ UserInfo Endpoint ซึ่งใช้สำหรับถ่ายทอดข้อมูลเกี่ยวกับผู้ใช้งานจาก ผู้ให้บริการพิสูจน์ตัวตน (Identity Provider :IdP) ไปยัง ระบบที่นำผลการพิสูจน์ตัวตนไปใช้ (Relying Party :RP) เมื่อมีการประยุกต์ใช้ในบริบทของเอกสารรับรอง (VC) และเอกสารสำแดง (VP) ข้อมูลดังกล่าวสามารถนำมาใช้เป็นข้อมูลตั้งต้น โดยแอตทริบิวต์จะถูกนำไปจัดโครงสร้างใหม่ภายใต้ credentialSubject ของ VC ตามรูปแบบของ W3C Verifiable Credentials Data Model ดังแสดงในตารางที่ 4

OIDC Claim	ตัวอย่างการใช้ใน VC (credentialSubject)	ความหมาย	หมายเหตุ
sub	id / identifier	ตัวระบุผู้ถือเอกสาร	ใช้เป็น subject identifier
given_name	givenName	ชื่อบุคคล	ใช้เก็บชื่อจริงของผู้ถือเอกสารรับรอง
family_name	familyName	ชื่อสกุล	ใช้เก็บชื่อสกุลของผู้ถือเอกสารรับรอง
birthdate	birthDate	วันเกิด	ใช้ตรวจสอบอายุหรือคุณสมบัติของผู้ถือเอกสารใบอนุญาต
gender	gender	เพศสภาพ	ใช้ระบุเพศสภาพ (ข้อมูลประกอบ)
address	address	ข้อมูลที่อยู่ของบุคคล	ใช้เก็บข้อมูลที่อยู่ (ข้อมูลประกอบ)
phone_number	phoneNumber	โทรศัพท์ของบุคคล	ใช้สำหรับการติดต่อหรือยืนยันตัวตนเพิ่มเติม
email	email	ที่อยู่อีเมลของบุคคล	ใช้สำหรับการติดต่อหรือใช้เป็นตัวระบุดิจิทัลเพิ่มเติม
iss	issuer	ตัวระบุผู้ออกเอกสารข้อมูล	เป็นข้อมูลเมตาดาตาของ VC
exp	expirationDate	วันหมดอายุของ token หรือ credential	ใช้กำหนดอายุของเอกสารรับรอง

ตารางที่ 4 แสดงการเชื่อมโยงรายการข้อมูลจาก OIDC ไปสู่เอกสารรับรอง (VC)

ทั้งนี้ มาตรฐาน OID4VCI และ OID4VP ไม่ได้กำหนดชุดแอตทริบิวต์ใหม่โดยตรง แต่ทำหน้าที่กำหนดกลไกการรับ-ส่ง และการใช้งานข้อมูลดังกล่าวในกระบวนการออกและแสดงเอกสารรับรอง ดังนั้น เมื่อผู้พัฒนาระบบมีความเข้าใจในข้อมูลยืนยัน (Claims) ของ OIDC และโครงสร้างของ VC แล้ว จะสามารถนำแอตทริบิวต์ดังกล่าวไปใช้สร้างและแลกเปลี่ยน VC และ VP ได้อย่างถูกต้องและเป็นมาตรฐานต่อไป

2.4 การจัดเตรียมชุดคำศัพท์หรือแอตทริบิวต์ของชุดข้อมูลตามมาตรฐาน TGIX และเอกสารรับรอง

ในหัวข้อนี้จะเป็นการเตรียมชุดคำศัพท์ หรือแอตทริบิวต์ของโครงสร้างข้อมูลของ "ชุดข้อมูลโดเมน" ซึ่งเป็นข้อมูลที่มีความเฉพาะเจาะจง หรือเฉพาะกลุ่ม เช่น ข้อมูลใบอนุญาตขับขี่ และทำการปรับโครงสร้างของชุดคำศัพท์หรือแอตทริบิวต์ให้เป็นไปตามมาตรฐานฯ ด้านความหมาย (TGIX Semantic) เพื่อให้ข้อมูลสามารถแลกเปลี่ยน และตีความร่วมกันได้ระหว่างหน่วยงานได้อย่างมีประสิทธิภาพ

2.4.1 การปรับเปลี่ยนชุดคำศัพท์หรือแอตทริบิวต์ให้เป็นไปตามมาตรฐาน TGIX

ในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานภาครัฐ จำเป็นต้องกำหนดชุดแอตทริบิวต์ที่สามารถใช้ร่วมกันได้ เพื่อให้การตีความข้อมูลเป็นไปในทิศทางเดียวกัน และสามารถนำข้อมูลไปใช้งานข้ามระบบได้อย่างมีประสิทธิภาพ ทาง สพร. จึงขอเสนอการประยุกต์มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐด้านความหมายข้อมูล (TGIX Semantic)[7]

เพื่อให้ระบบภาครัฐสามารถใช้ข้อมูลร่วมกันได้อย่างมีประสิทธิภาพ ผู้พัฒนาระบบสารสนเทศหน่วยงาน สามารถเลือกใช้กลุ่มข้อมูลจากมาตรฐาน TGIX Semantic ที่สำคัญจากกลุ่มข้อมูลดังนี้

- กลุ่มข้อมูลหลัก (Core Data) ซึ่งเป็นกลุ่มข้อมูลพื้นฐานที่สามารถนำไปใช้ซ้ำได้ในหลายบริบทของบริการภาครัฐ โดย สพร. ได้ประกาศเป็นมาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัล (มสพร.) ที่สำคัญ ๆ เช่น มาตรฐานฯ ข้อมูลบุคคล (มสพร. 4-2565)[8] มาตรฐานฯ ข้อมูลนิติบุคคล (มสพร.5-2565)[9] และ มาตรฐานฯ ข้อมูลสถานที่-ที่อยู่ (มสพร. 9-1:2566)[10] ข้อมูลประเภทนี้สามารถพบได้ในเอกสารหรือบริการภาครัฐหลายประเภท เช่น บัตรประจำตัวประชาชน ใบอนุญาตขับขี่ ใบอนุญาตอื่น ๆ ของบริการภาครัฐ
- กลุ่มข้อมูลขยาย (Extend Data) เป็นกลุ่มข้อมูลที่มีความเฉพาะเจาะจง หรือเฉพาะกลุ่ม (Domain) กับบริการหรือประเภทเอกสารนั้น ๆ เช่น ในกรณีของใบอนุญาตขับขี่ ข้อมูลในกลุ่มนี้มักถูกกำหนดภายใต้ namespace เฉพาะของหน่วยงานหรือโดเมนข้อมูล เช่น namespace "dlt" สำหรับข้อมูลที่เกี่ยวข้องกับกรมการขนส่งทางบก

โดยในขั้นตอนนี้จะมุ่งเน้นเฉพาะการปรับโครงสร้างข้อมูลของ ชุดข้อมูลหลัก ที่อยู่ในส่วน Credential Subject เท่านั้น เช่น ข้อมูลใบอนุญาตขับขี่ ***โดยแอตทริบิวต์ที่มาจากมาตรฐานสากล เช่น OIDC หรือ***

[7] สพร., มาตรฐาน TGIX (Thailand Government Information Exchange), https://standard.dga.or.th

[8] สพร., มาตรฐาน ฯ ข้อมูลบุคคล มสพร. 4-2565 (https://standard.dga.or.th/ตัวอย่าง-มาตรฐานการเชื่/)

[9] สพร., มาตรฐาน ฯ ข้อมูลนิติบุคคล มสพร. 5-2565 (https://standard.dga.or.th/มาตรฐานของสำนักงานพัฒน/)

[10] สพร., มาตรฐาน ฯ ข้อมูลสถานที่-ที่อยู่ มสพร. 9-1:2566 (https://standard.dga.or.th/มาตรฐานสำนักงานพัฒนารั-3/)

OID4VCI จะไม่ถูกแปลงเป็น TGIX เนื่องจากถือเป็นโครงสร้างมาตรฐานสากลอยู่แล้ว ซึ่งกระบวนการจัดเตรียมข้อมูลตามมาตรฐาน TGIX สามารถอธิบายได้เป็นขั้นตอนหลักดังนี้

(1) ข้อมูลต้นทางของระบบ

ในกระบวนการพัฒนาเอกสารรับรองดิจิทัล หน่วยงานมักมีข้อมูลต้นทางอยู่แล้วในระบบสารสนเทศของหน่วยงาน เช่น ฐานข้อมูลใบอนุญาตขับขี่ของบุคคล โดยข้อมูลดังกล่าวมักอยู่ในรูปแบบ JSON หรือโครงสร้างข้อมูลของระบบเดิม เช่น ข้อมูลใบอนุญาตขับขี่ (ใบอนุญาตขับขี่) ของศูนย์กลางแลกเปลี่ยนข้อมูลภาครัฐ (GDX) ประกอบไปด้วยแอตทริบิวต์ docNo, docType, excFee, expDate, issDate, addrNo

(2) การกำหนด Namespace และ Prefix

ในขั้นตอนนี้จะกำหนด namespace ตามมาตรฐาน TGIX เพื่อให้ข้อมูลมีความหมายเชิงมาตรฐาน เช่น

cd: (Core Data) สำหรับกลุ่มข้อมูลหลัก ตามมาตรฐานฯ ด้านความหมายข้อมูล TGIX Semantic ที่ สพร. ประกาศไว้ เช่น cd:Person (มาตรฐานฯ ข้อมูลบุคคล) cd:OrganizationJuristicPerson (มาตรฐานฯ ข้อมูลนิติบุคคล) และ cd:Address (มาตรฐานฯ ข้อมูลสถานที่-ที่อยู่) เป็นต้น

dlt: (Department of Land Transport) ในที่นี้ได้ยกกรณีศึกษาหลัก เป็นข้อมูลโดเมนของกรมการขนส่งทางบก ซึ่งได้ใช้ชุดคำศัพท์หรือแอตทริบิวต์ ศูนย์กลางแลกเปลี่ยนข้อมูลภาครัฐ (GDX) ซึ่งทาง สพร. ได้ร่วมมือกับกรมการขนส่งทางบก นำบริการข้อมูลใบอนุญาตขับขี่ (ใบอนุญาตขับขี่) มาวางไว้ที่ GDX นี้

การกำหนด ค่า Namespace หรือ prefix ดังกล่าวช่วยให้สามารถระบุได้ชัดเจนว่าข้อมูลแต่ละส่วนอยู่ในหมวดข้อมูลใด และทราบได้ว่าแต่ละส่วนหรือแอตทริบิวต์ข้อมูลเหล่านั้นมาจากหน่วยงานใด

(3) การแปลงแอตทริบิวต์ของระบบกับ TGIX Semantic

จากขั้นตอนที่ 2 ที่กำหนด Namespace หรือ Prefix ของกลุ่มข้อมูลหลัก (cd:) และกลุ่มข้อมูลเฉพาะ ซึ่งในที่นี้คือใบอนุญาตขับขี่ ซึ่งกำหนดเป็น ‘dlt’ เรียบร้อยแล้ว ก็สามารถเติมเข้าไปข้างหน้า (Prefix) ตามความสัมพันธ์ระหว่างแอตทริบิวต์ของระบบเดิมกับแอตทริบิวต์ตามมาตรฐาน TGIX เช่น

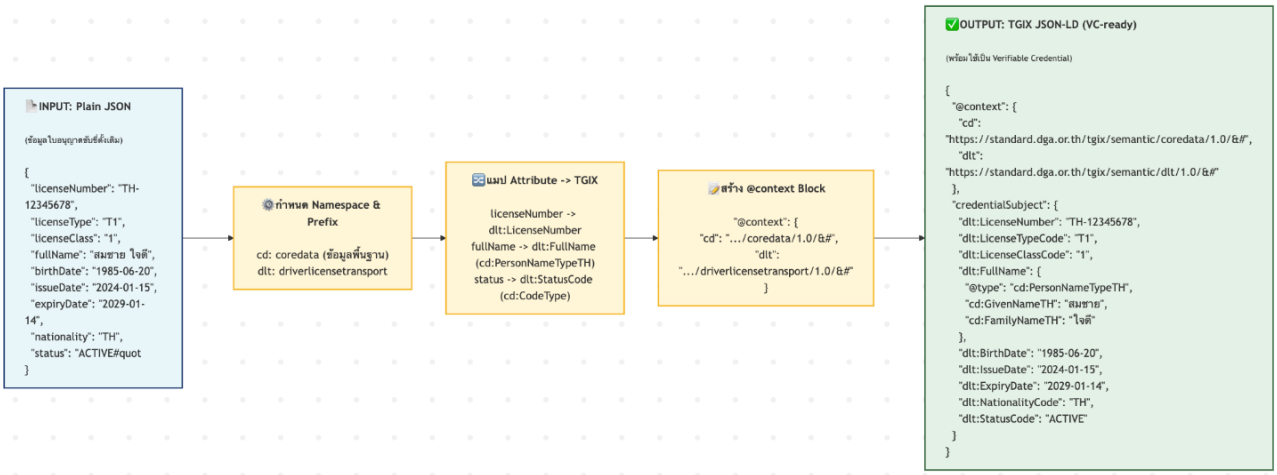
licenseNumber --> dlt:licenseNumber

docType --> dlt:LicenseTypeCode

excFee --> dlt:excFee

fName --> dlt:FullName

ในบางกรณี แอตทริบิวต์หนึ่งอาจต้องถูกแปลงเป็นโครงสร้างข้อมูลที่ซับซ้อนมากขึ้น เช่น การแยกชื่อและนามสกุลให้สอดคล้องกับโครงสร้าง cd:PersonNameTypeTH



ภาพที่ 4 ตัวอย่างการแยกชื่อและนามสกุลให้สอดคล้องกับโครงสร้าง cd:PersonNameTypeTH

2.4.2 การปรับเปลี่ยนชุดคำศัพท์และแอตทริบิวต์ให้อยู่ในรูปแบบเอกสารรับรอง (VC)

ในหัวข้อนี้จะอธิบายแนวทางการจัดโครงสร้างข้อมูลให้อยู่ในรูปแบบเอกสารรับรอง (Verifiable Credential: VC) เพื่อให้นักพัฒนาระบบสารสนเทศของหน่วยงานสามารถเข้าใจองค์ประกอบของ VC และสามารถนำชุดข้อมูลที่ผ่านการจัดเตรียมตามมาตรฐาน TGIX ไปประยุกต์ใช้ได้อย่างถูกต้อง ทั้งนี้ การจัดทำ VC จะต้องคำนึงถึงทั้งโครงสร้างข้อมูลตามมาตรฐานสากล และความสอดคล้องของข้อมูลเชิงบริบทของหน่วยงานภาครัฐ โดยแนวทางการดำเนินการสามารถอธิบายได้ดังนี้

1. กำหนดโครงสร้าง VC ตามแบบจำลองที่เกี่ยวข้อง
    - ระบุ @context ที่อ้างถึงทั้งเนมสเปซมาตรฐานของ W3C Verifiable Credentials Data Model หรือของ TGIX ที่เกี่ยวข้อง
    - ระบุ type ของเอกสาร เช่น ["VerifiableCredential", "ThaiDrivingLicenseCredential"]
    - กำหนดข้อมูลเมตาดาตา เช่น issuer, issuanceDate และ expirationDate ตามเงื่อนไขของการใช้งาน
2. กำหนดส่วน credentialSubject
    - จัดวางข้อมูลภายใน credentialSubject ให้สอดคล้องกับโครงสร้างของข้อมูล
    - สำหรับข้อมูลยืนยันตัวตนที่อ้างอิงจากมาตรฐานสากล เช่น OIDC Claims หรือแอตทริบิวต์ที่ใช้ในบริบทของ OID4VCI ควรคงชื่อหรือความหมายตามมาตรฐานเดิม
    - สำหรับข้อมูลเชิงบริบทของหน่วยงาน เช่น ข้อมูลใบอนุญาตขับขี่ ให้ทำการแมปไปยังคำศัพท์ตามมาตรฐาน TGIX ภายใต้ namespace ที่เกี่ยวข้อง

- ตัวอย่างการแมปข้อมูลสามารถแสดงได้ในตาราง เช่น licenseNumber -> dlt:LicenseNumber และ fullName -> cd:PersonNameTypeTH

Attribute ใบอนุญาตขับขี่	TGIX (แนะนำ)	ตัวอย่างการจัดวางข้อมูลใน VC
licenseNumber	dlt:LicenseNumber	driverLicense.licenseNumber
fullName	dlt:FullName -> cd:PersonNameTypeTH	name.given / name.family
licenseClass	dlt:LicenseClassCode	driverLicense.licenseClass
issueDate	dlt:IssueDate	driverLicense.issueDate
expiryDate	dlt:ExpiryDate	driverLicense.expiryDate
status	dlt:StatusCode	driverLicense.status

ตารางที่ 5 ตัวอย่างการแมปข้อมูลใบอนุญาตขับขี่ไปสู่ TGIX และการจัดวางใน credentialSubject ของ VC

หมายเหตุ: คอลัมน์ “ตัวอย่างการจัดวางข้อมูลใน VC” เป็นการแสดงตำแหน่งข้อมูลในเชิงแนวคิดเพื่ออธิบายการนำข้อมูลไปวางภายใน credentialSubject ไม่ใช่ข้อกำหนดตายตัวของชื่อฟิลด์ใน JSON-LD VC ซึ่งในการใช้งานจริงอาจต้องกำหนดโครงสร้างให้สอดคล้องกับ credential profile หรือโครงสร้างข้อมูลหรือสคีมาที่หน่วยงานใช้

3. รองรับรูปแบบของ VC ตามบริบทการใช้งาน
    - ในกรณี JSON-LD VC ควรเน้นการใช้ @context และการอ้างอิงคำศัพท์ผ่าน URL ของคำศัพท์อย่างชัดเจน
    - ในกรณี JWT-based VC สามารถใช้แอตทริบิวต์ข้อมูลยืนยันตัวตน ตามโครงสร้างที่กำหนด แต่ยังคงอ้างอิงแนวทางการแมปข้อมูลเดียวกัน
    - ในกรณี SD-JWT VC ควรพิจารณาการออกแบบสคีมาเพื่อรองรับการเปิดเผยข้อมูลแบบเลือกได้ (Selective Disclosure) ตั้งแต่ต้น
4. ทดสอบและตรวจสอบความสอดคล้อง
    - ตรวจสอบว่า VC ที่สร้างขึ้นสามารถผ่านกระบวนการตรวจสอบความถูกต้องได้ตามแนวทางของระบบนิเวศ VC/VP ที่เกี่ยวข้อง
    - ตรวจสอบความสอดคล้องของ namespace และโครงสร้างข้อมูล เพื่อให้สามารถทำงานร่วมกับระบบอื่นที่ใช้มาตรฐาน TGIX เดียวกันได้
    - ตรวจสอบว่าการแมปข้อมูลจากส่วนของแอตทริบิวต์ยืนยันตัวตนและข้อมูลเชิงบริบทไม่ก่อให้เกิดความคลาดเคลื่อนของความหมายข้อมูล

```
{
  "@context": [
    "https://www.w3.org/ns/credentials/v2",
    {
      "dlt": "https://standard.dga.or.th/tgix/semantic/dlt/1.0/#",
      "cd": "https://standard.dga.or.th/tgix/semantic/coredata/1.0/#"
    }
  ],
  "type": [
    "VerifiableCredential",
    "ThaiDrivingLicenseCredential"
  ],
  "issuer": "https://issuer.example.go.th/dlt",
  "issuanceDate": "2025-03-23T00:00:00Z",
  "expirationDate": "2030-03-22T23:59:59Z",
  "credentialSubject": {
    "id": "did:key:z6Mk...holderKey",
    "driverLicense": {
      "licenseNumber": "TH-12345678",
      "licenseClass": "1",
      "issueDate": "2024-01-15",
      "expiryDate": "2029-01-14",
      "status": "ACTIVE"
    },
    "name": {
      "given": "สมชาย",
      "family": "ใจดี"
    },
    "dlt:LicenseNumber": "TH-12345678",
    "dlt:LicenseClassCode": "1",
    "dlt:IssueDate": "2024-01-15",
    "dlt:ExpiryDate": "2029-01-14",
    "dlt:StatusCode": "ACTIVE",
    "dlt:FullName": {
      "cd:Person": {
          "cd:PersonNameTH": {
            "cd:PersonFirstNameTH": "สมชาย",
            "cd:PersonLastNameTH": "ใจดี"
          }
        }
    }
  },
  "proof": {
    "type": "Ed25519Signature2020",
    "created": "2025-03-23T00:00:00Z",
    "verificationMethod": "did:web:issuer.example.go.th#key-1",
    "proofPurpose": "assertionMethod",
    "proofValue": "z3Z...signature"
  }
}
```


ตัวอย่างผลลัพธ์ในรูปแบบ VC (JSON-LD)

ตัวอย่างนี้แสดงการจัดวางข้อมูลภายในเอกสารรับรอง (VC) โดยใช้แอตทริบิวต์ตัวอย่างจากตารางการแมปข้อมูลใบอนุญาตขับขี่ และแสดงให้เห็นการใช้งานร่วมกันระหว่างโครงสร้างมาตรฐานสากลของ VC กับข้อมูลเชิงบริบทที่ถูกแมปไปยังคำศัพท์ตามมาตรฐาน TGIX โดยมีโครงสร้างของ VC ดังนี้

คำอธิบายแอตทริบิวต์สำคัญของ VC

1. @context
   - เจ้าของ: Issuer (กำหนดตามมาตรฐาน)
   - ความหมาย: ระบุบริบทและ namespace ของคำศัพท์ที่ใช้ในเอกสาร
   - ใช้ทำอะไร: ทำให้ข้อมูลเป็น JSON-LD และเชื่อมโยงคำศัพท์ไปยัง URL ของมาตรฐาน
   - หมายเหตุ: ต้องมีทั้ง W3C VC และ TGIX (ถ้ามีการใช้แอตทริบิวต์ TGIX)
2. type
   - เจ้าของ: Issuer
   - ความหมาย: ระบุประเภทของเอกสาร
   - ใช้ทำอะไร: บอกว่าเป็น VC และเป็น credential ประเภทใด เช่น ใบอนุญาตขับขี่
3. issuer
   - เจ้าของ: Issuer
   - ความหมาย: ตัวระบุของผู้ออกเอกสาร (อาจเป็น DID หรือ URL)
   - ใช้ทำอะไร: ใช้ตรวจสอบลายมือชื่อดิจิทัล
   - หมายเหตุ: แนะนำใช้ DID เพื่อรองรับระบบ VC/VP
4.issuanceDate / expirationDate
   - เจ้าของ: Issuer
   - ความหมาย: วันที่ออกและวันหมดอายุของเอกสาร
   - ใช้ทำอะไร: ใช้กำหนดช่วงเวลาที่ VC มีผลใช้งาน
5.credentialSubject.id
   - เจ้าของ: Holder
   - ความหมาย: ตัวระบุของผู้ถือเอกสาร (DID)
   - ใช้ทำอะไร: ใช้ผูก VC กับตัวผู้ถือเอกสาร และใช้ในกระบวนการพิสูจน์ตัวตน
   - หมายเหตุ: อาจเป็น did:key, did:web หรือวิธีอื่นตามที่ระบบรองรับ
6.credentialSubject (data)
   - เจ้าของ: Issuer (เป็นผู้บรรจุข้อมูล), Holder (เป็นเจ้าของข้อมูล)
   - ความหมาย: ชุดข้อมูลของเอกสาร เช่น ข้อมูลใบอนุญาตขับขี่
   - ใช้ทำอะไร: เป็นเนื้อหาหลักของ VC
   - หมายเหตุ: ส่วนนี้สามารถใช้ TGIX ในการจัดโครงสร้างข้อมูลได้
7. proof
   - เจ้าของ: Issuer
   - ความหมาย: ลายมือชื่อดิจิทัลของ VC
   - ใช้ทำอะไร: ใช้ยืนยันว่า VC ถูกออกโดย issuer และไม่ถูกแก้ไข
   - องค์ประกอบภายใน proof:

- type: ประเภทลายมือชื่อ
- created: เวลาที่ลงนาม
- verificationMethod: public key (อ้างอิงผ่าน DID)
- proofPurpose: วัตถุประสงค์ของลายมือชื่อ (เช่น assertionMethod)
- proofValue: ค่าลายมือชื่อ

8. DID (Decentralized Identifier)

- เจ้าของ: ทั้ง Issuer และ Holder
- ความหมาย: ตัวระบุแบบกระจายศูนย์ที่ใช้แทนตัวบุคคลหรือหน่วยงาน
- ใช้ทำอะไร: ใช้เชื่อมโยงกับ public key สำหรับการตรวจสอบลายมือชื่อ
- หมายเหตุ: ใช้ร่วมกับ DID Document และอาจมี Resolver ในการดึงข้อมูล

หมายเหตุ: ตัวอย่างนี้เป็นเพียงแนวทาง โครงสร้างจริงอาจขึ้นอยู่กับ credential profile การเลือกวิธีลงนาม (เช่น Ed25519Signature2020 หรือ JWS) ขึ้นอยู่กับการประยุกต์ใช้ และมาตรฐานที่หน่วยงานเลือกใช้

- ส่วน driverLicense และ name แสดงตัวอย่างการจัดวางข้อมูลในเชิงโครงสร้างภายใน credentialSubject เพื่อให้นักพัฒนาระบบเข้าใจการใช้งานในระดับแอปพลิเคชัน
- ส่วนที่ใช้ prefix เช่น dlt: และ cd: แสดงตัวอย่างการแมปข้อมูลเชิงบริบทไปยัง TGIX Semantic Element ตามแนวทางของมาตรฐาน TGIX
- ในการนำไปใช้งานจริง หน่วยงานสามารถปรับรายละเอียดของ @context, type, และโครงสร้างภายใน credentialSubject ให้สอดคล้องกับ credential profile หรือ schema ที่กำหนดไว้ในระบบนิเวศของหน่วยงานได้

ตัวอย่างแนวทางการเก็บรักษากุญแจส่วนตัว (Private Key) และความมั่นคงปลอดภัย สำหรับการใช้งานเอกสารรับรองและเอกสารสำแดงทุกบทบาทเกี่ยวข้องกับกุญแจส่วนตัวที่ใช้ลงลายมือชื่อดิจิทัล โดยหลักการฝั่งผู้ถือเอกสารให้จัดเก็บกุญแจส่วนตัวในพื้นที่ปลอดภัยของอุปกรณ์ (เช่น Trusted Execution Environment: TEE หรือ Secure Element) ส่วนกรณีจัดเก็บบนเครื่องแม่ข่ายของผู้ออกเอกสารหรือผู้ให้บริการ ให้จัดเก็บใน Hardware Security Module (HSM) และไม่ส่งออกหรือสำรองกุญแจส่วนตัวในรูปแบบที่ไม่เข้ารหัสลับ ทั้งนี้ มาตรฐานฉบับนี้ไม่กำหนดข้อกำหนดทางเทคนิคในเรื่องดังกล่าวขึ้นใหม่ โดยรายละเอียด บทนิยาม ตลอดจนแนวทางการสำรอง กู้คืน และเพิกถอนกุญแจ ให้เป็นไปตามรายงานทางเทคนิคของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง กรอบการสร้างความน่าเชื่อถือของเอกสารรับรองและเอกสารสำแดง (Trust Model Framework) โดยเฉพาะข้อกำหนด VCTF-08 และ VCGF-1.2 และเรื่อง กรอบการทำงานร่วมกันของกระเป๋าดิจิทัลสำหรับเอกสารรับรอง

3. การประยุกต์ใช้เอกสารรับรองและเอกสารสำแดงกับชุดข้อมูลใบอนุญาตขับขี่ตามมาตรฐาน TGIX

ในบทนี้จะนำเสนอแนวทางการประยุกต์ใช้เอกสารรับรอง (Verifiable Credential: VC) และเอกสารสำแดง (Verifiable Presentation: VP) กับชุดข้อมูลใบอนุญาตขับขี่ โดยใช้แบบจำลองข้อมูลเชิงความหมายตามมาตรฐาน TGIX เป็นพื้นฐานในการออกแบบโครงสร้างข้อมูล

ตัวอย่างในบทนี้มีวัตถุประสงค์เพื่อช่วยให้นักพัฒนาระบบของหน่วยงานภาครัฐเข้าใจแนวทางการออกแบบข้อมูล การสร้างเอกสารรับรอง และการตรวจสอบข้อมูล โดยอาศัยเทคโนโลยีตามมาตรฐาน W3C VC และแนวทาง OpenID Connect for Verifiable Credential Issuance (OID4VCI)

3.1 แนวทางการออกแบบสคีมาของใบอนุญาตขับขี่

เพื่อให้สามารถนำชุดข้อมูลใบอนุญาตขับขี่มาประยุกต์ใช้ในรูปแบบเอกสารรับรอง (VC) และเอกสารสำแดง (VP) ได้อย่างถูกต้อง จำเป็นต้องทำความเข้าใจโครงสร้างของชุดคำศัพท์หรือแอตทริบิวต์ที่ใช้ในกรณีศึกษานี้ ตลอดจนแนวทางในการปรับโครงสร้างข้อมูลดังกล่าวให้สอดคล้องกับแบบจำลองข้อมูลเชิงความหมายตามมาตรฐาน TGIX

ในหัวข้อนี้จึงนำเสนอแนวทางการออกแบบสคีมาของข้อมูลใบอนุญาตขับขี่ โดยเริ่มจากการพิจารณารายการแอตทริบิวต์ของข้อมูลต้นทาง และนำไปสู่การปรับเปลี่ยนชุดคำศัพท์หรือแอตทริบิวต์ให้เป็นไปตามมาตรฐาน TGIX ซึ่งมีรายละเอียดดังนี้

3.1.1 เปรียบเทียบรายการชุดคำศัพท์หรือแอตทริบิวต์ในกรณีศึกษาใบอนุญาตขับขี่

เพื่อให้ข้อมูลใบอนุญาตภาครัฐมีความหมายที่เข้าใจตรงกันระหว่างหน่วยงาน กรณีศึกษาหลักในเอกสารฉบับนี้คือใบอนุญาตขับขี่ยนต์ (Driver's License) โดยได้นำชุดแอตทริบิวต์ของข้อมูลใบอนุญาตขับขี่ (ใบอนุญาตขับขี่) ของศูนย์กลางแลกเปลี่ยนข้อมูลภาครัฐ (GDX) เทียบกับแอตทริบิวต์จากมาตรฐานใบอนุญาตขับขี่สากลบนอุปกรณ์พกพา (ISO/IEC 18013-5: mDL) ดังตาราง

GDX	mDL (ISO 18013-5)	ความหมาย	หมายเหตุ
docNo	-	เลขที่เอกสาร	-
docType	-	ประเภทเอกสาร	GDX มีเพิ่มเติม, mDL ใช้ DocType ระดับ mdoc แทน
excFee	-	ค่าธรรมเนียม	GDX มีเพิ่มเติม; ไม่มีใน mDL
expDate	expiry_date	วันหมดอายุ	GDX ใช้ String, mDL ใช้ (ISO 8601) ค่าเกิน 5 ปี = ตลอดชีพ
issDate	issue_date	วันที่ออกใบอนุญาต	GDX ใช้ String, mDL ใช้ (ISO 8601)
addrNo	-	เลขที่บ้าน	GDX แยก address เป็น field ย่อย mDL รวมใน resident_address

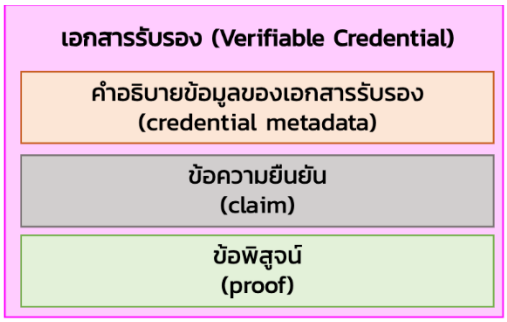
GDX	mDL (ISO 18013-5)	ความหมาย	หมายเหตุ
locCode	-	เขต/อำเภอ	ส่วนหนึ่งของที่อยู่, mDL รวมใน resident_address
locDesc	-	แขวง/ตำบล	ส่วนหนึ่งของที่อยู่, mDL รวมใน resident_address
locFullDesc	-	ชื่อเต็มจังหวัด/อำเภอ/ตำบล	ส่วนหนึ่งของที่อยู่, mDL รวมใน resident_address
natCode	nationality	รหัสสัญชาติ	GDX แยก code/desc; mDL ใช้ตัวเดียว (ISO 3166-1 alpha-2)
natDesc	-	ชื่อสัญชาติ	GDX มีเพิ่มเติม, mDL ใช้รหัสเดียว
offLocCode	-	จังหวัด	ส่วนหนึ่งของที่อยู่, mDL รวมใน resident_address
pcNo	-	หมายเลขเครื่อง	GDX มีเพิ่มเติม, ไม่มีใน mDL
pltCode	vehicle_category_code	รหัสชนิดใบอนุญาตขับขี่	ความหมายเดียวกัน
pltDesc	-	ชื่อชนิดใบอนุญาตขับขี่	GDX มี description แยก, mDL ใช้รหัสเป็นหลัก
pltNo	document_number	เลขที่ใบอนุญาต	pltNo ตรงกับ driving licence number มากกว่า docNo
sex	sex	เพศ	GDX ใช้ 1/2, mDL ใช้เลขจำนวนเต็มแบบไม่ระบุเครื่องหมาย (ISO 5218: 1= ชาย 2=หญิง)
titleDesc	-	คำนำหน้าชื่อ (ไทย)	ไม่มีใน mDL
titleEngDesc	-	คำนำหน้าชื่อ (อังกฤษ)	ไม่มีใน mDL
villageNo	-	บ้านเลขที่	รวมใน resident_address ของ mDL
fName	-	ชื่อ (ภาษาไทย)	mDL ไม่มี Thai-specific field, ใช้ domestic namespace แทน
fNameEng	given_name	ชื่อ (ภาษาอังกฤษ)	ความหมายตรงกัน
lName	-	นามสกุล (ภาษาไทย)	mDL ไม่มี Thai-specific field, ใช้ domestic namespace แทน
lNameEng	family_name	นามสกุล (ภาษาอังกฤษ)	ความหมายตรงกัน

GDX	mDL (ISO 18013-5)	ความหมาย	หมายเหตุ
-	resident_address	ที่อยู่ (รวม)	mDL รวม address เป็น String เดียว, GDX แยกเป็น field ย่อยหลายตัว
pic	portrait	รูปภาพ	-
-	birth_date	วันเกิด	mDL มี
-	issuing_authority	หน่วยงานออกใบอนุญาต	mDL บังคับ, GDX ไม่มี field ตรง
-	issuing_country	ประเทศที่ออกใบอนุญาต	mDL มีเนื่องจากใช้ในกรณีข้ามประเทศในกลุ่มประเทศที่ตกลงกัน, GDX ไม่มี

ตารางที่ 6 การเปรียบเทียบแอตทริบิวต์ใบอนุญาตขับขี่ระหว่าง GDX และ mDL (ISO / IEC 18013-5)

3.1.2 การปรับเปลี่ยนชุดคำศัพท์หรือแอตทริบิวต์ให้เป็นไปตามมาตรฐาน TGIX

การออกแบบสคีมาของใบอนุญาตขับขี่ในรูปแบบ Verifiable Credential (VC) ประกอบไปด้วยโครงสร้างข้อมูลหลัก 3 ส่วน ได้แก่



(1) Meta data ของเอกสารรับรอง

(2) ข้อมูลของผู้ถือเอกสาร และข้อมูลเฉพาะของใบอนุญาตขับขี่

(3) ข้อมูลพิสูจน์

ภาพที่ 5 รูปแบบเอกสารรับรอง

ในการออกแบบข้อมูลภายใต้ credentialSubject ข้อมูลพื้นฐานของบุคคลควรอ้างอิงโครงสร้าง Core Data ตามมาตรฐาน TGIX เช่น cd:Person และ cd:PersonIdentifier เพื่อให้เกิดความสอดคล้องด้านความหมายข้อมูลระหว่างหน่วยงานภาครัฐ ขณะที่ข้อมูลเฉพาะของใบอนุญาตขับขี่ควรถูกจัดกลุ่มภายใต้ namespace ของโดเมน เช่น dlt: เพื่อสะท้อนบริบทของข้อมูลและรองรับการขยายในอนาคต

ตัวอย่างโครงสร้าง JSON ของ Verifiable Credential สำหรับใบอนุญาตขับขี่

```
{ "@context": [
  "https://www.w3.org/2018/credentials/v1",
    { "cd": "http://standard.dga.or.th/tgix/semantic/core-data/1.0/#",
      "dlt": "https://standard.dga.or.th/tgix/semantic/dlt/1.0/#" } ],
 "type": ["VerifiableCredential", "ThaiDrivingLicenseCredential"],
 "issuer": "https://issuer.dlt.go.th",
 "issuanceDate": "2025-01-01T00:00:00Z",
 "credentialSubject": { "cd:Person": {
                          "cd:PersonID": "1234567890123",
                          "cd:PersonNameTH": {
                            "cd:PersonFirstNameTH": "สมชาย",
```

```
                    "cd:PersonLastNameTH": "ใจดี"},
                },
                "dlt:DrivingLicense": {
                    "dlt:licenseNumber": "DL12345678",
                    "dlt:licenseType": "B",
                    "dlt:issueDate": "2025-01-01",
                    "dlt:expiryDate": "2030-01-01" }
                }
    }
```

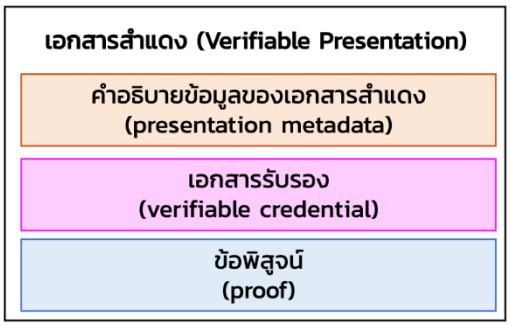
โครงสร้างดังกล่าวเป็นไปตามหลักการแบ่งกลุ่มข้อมูลระหว่าง กลุ่มข้อมูลหลัก (Core Data) และกลุ่มข้อมูลเฉพาะโดเมน (Domain Data) ซึ่งช่วยให้สามารถนำข้อมูลไปใช้ซ้ำ (Reusability) และเชื่อมโยงข้อมูลระหว่างระบบได้อย่างมีประสิทธิภาพ

ตัวอย่างโครงสร้าง VC แบบสมบูรณ์ (รวมส่วน proof สำหรับการลงลายมือชื่อดิจิทัล)

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    {
      "cd": "http://standard.dga.or.th/tgix/semantic/core-data/1.0/#",
      "dlt": "https://standard.dga.or.th/tgix/semantic/dlt/1.0/#"
    }
  ],
  "id": "http://dlt.go.th/credentials/dl-6500001",
  "type": [
    "VerifiableCredential",
    "ThaiDrivingLicenseCredential"
  ],
  "issuer": "did:tbsi:dlt-agency-id",
  "issuanceDate": "2024-05-20T10:00:00Z",
  "expirationDate": "2029-05-20T10:00:00Z",
  "credentialSubject": {
    "id": "did:key:holder-did-id",
    "dlt:DrivingLicense": {
      "dlt:LicenseNumber": "6500001",
      "dlt:LicenseType": "ใบอนุญาตขับขี่ยนต์ส่วนบุคคล",
      "dlt:IssueDate": "2024-05-20",
      "dlt:ExpiryDate": "2029-05-20",
      "dlt:IssuingAgency": "กรมการขนส่งทางบก",
      "dlt:LicenseStatus": "Active",
      "dlt:LicenseHolder": {
        "cd:Person": {
          "cd:PersonID": "1234567890123",
          "cd:PersonNameTH": {
            "cd:PersonFirstNameTH": "สมชาย",
            "cd:PersonLastNameTH": "ใจดี" },
          "cd:PersonBirthDate": "1990-01-01"
        }
      }
    }
  },
```

```
  "proof": {
    "type": "Ed25519Signature2018",
    "created": "2024-05-20T10:05:00Z",
    "proofPurpose": "assertionMethod",
    "verificationMethod": "did:tbsi:dlt-agency-id#key-1",
    "jws": "eyJhbGciOiJFZERTQSIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..."
  }
}
```

ในส่วนการออกแบบเอกสารสำแดงในรูปแบบ Verifiable Presentation (VP) เป็นกระบวนการที่ผู้ถือเอกสาร (Holder) ใช้ในการรวบรวมและส่งต่อข้อมูลจาก Verifiable Credential (VC) ที่ตนถือครองไปยังผู้ตรวจสอบเอกสาร (Verifier) โดยมีวัตถุประสงค์เพื่อยืนยันข้อมูลตามบริบทของการใช้งานโครงสร้างของ Verifiable Presentation ประกอบด้วยส่วนสำคัญ ได้แก่



(1) ข้อมูลเมตาดาตาของเอกสารสำแดง

(2) ชุดของเอกสารรับรอง (Verifiable Credential (VC))

(3) ข้อมูลพิสูจน์ (Proof) ของผู้ถือเอกสาร (Holder)

ภาพที่ 6 รูปแบบเอกสารสำแดง

ในกระบวนการสำแดง ผู้ถือเอกสารสามารถเลือกเปิดเผยเฉพาะข้อมูลที่จำเป็นตามวัตถุประสงค์ของผู้ตรวจสอบเอกสาร (Selective Disclosure) โดยเฉพาะในกรณีที่ใช้รูปแบบเอกสารรับรองที่รองรับกลไกดังกล่าว เช่น SD-JWT VC ซึ่งช่วยลดการเปิดเผยข้อมูลเกินความจำเป็น และสอดคล้องกับหลักการคุ้มครองข้อมูลส่วนบุคคล

ทั้งนี้ในกรณีที่ต้องการให้เอกสารรับรอง (VC) รองรับชุดแอตทริบิวต์ตามมาตรฐาน ISO / IEC 18013-5 หรือ mDL นั้นสามารถกำหนด Verifiable Credential Type หรือประเภทของของเอกสารรับรองเข้าไปที่ VDR (Verifiable Data Registry) ของผู้ออกเอกสาร (Issuer) เพื่อที่ใช้อ้างอิงใน VC ได้ เช่น ***"type": ["VerifiableCredential", "mDLCredential"]*** ทำให้การออกเอกสารรับรอง และการตรวจสอบเอกสารรับรองเป็นไปตามข้อกำหนดใน mDL ตามมาตรฐานสากลได้

ตัวอย่างโครงสร้าง VP แบบสมบูรณ์ (รวมส่วน proof สำหรับการลงลายมือชื่อดิจิทัล)

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

  // 1. ส่วนของเอกสารรับรอง (VC) ต้นฉบับที่นำมาสำแดง
  "verifiableCredential": [
    {
      "@context": [
        "https://www.w3.org/2018/credentials/v1",
        {
          "cd": "http://standard.dga.or.th/tgix/semantic/core-data/1.0/#",
          "dlt": "http://standard.dga.or.th/tgix/semantic/landtransport/1.0/#"
        }
      ],
      "id": "http://dlt.go.th/credentials/dl-6500001",
      "type": [
        "VerifiableCredential",
        "ThaiDrivingLicenseCredential"
      ],
      "issuer": "did:tbsi:dlt-agency-id",
      "issuanceDate": "2024-05-20T10:00:00Z",
      "expirationDate": "2029-05-20T10:00:00Z",
      "credentialSubject": {
        "id": "did:key:holder-did-id",
        "dlt:DrivingLicense": {
          "dlt:LicenseNumber": "6500001",
          "dlt:LicenseType": "ใบอนุญาตขับขี่ยนต์ส่วนบุคคล",
          "cd:Person": {
            "cd:PersonNameTH": {
              "cd:PersonFirstNameTH": "สมชาย",
              "cd:PersonLastNameTH": "ใจดี"
            }
          }
        }
      },
      "proof": {
        "type": "Ed25519Signature2018",
        "created": "2024-05-20T10:05:00Z",
        "proofPurpose": "assertionMethod",
        "verificationMethod": "did:tbsi:dlt-agency-id#key-1",
        "jws": "eyJhbGciOiJFZERTQSIsIml... (ลายมือชื่อของกรมการขนส่งฯ)"
      }
    }
  ],
```

```
// 2. ส่วนข้อพิสูจน์ (Proof) และลายมือชื่อของผู้ถือเอกสาร (Holder)
"proof": {
  "type": "Ed25519Signature2018",
  "created": "2024-05-25T08:30:00Z",
  "proofPurpose": "authentication",
  "verificationMethod": "did:key:holder-did-id#key-1",
  "challenge": "1f44d55f-f161-4938-a659-f8026467f126",
  "domain": "verifier.example.com",
  "jws": "eyJhbGciOiJFZERTQSIsIml... (ลายมือชื่อของนายสมชาย ผู้ถือเอกสาร)"
}
```

จากการดำเนินการปรับเปลี่ยนชุดคำศัพท์และแอตทริบิวต์ให้เป็นไปตามมาตรฐาน TGIX ในหัวข้อก่อนหน้า ส่งผลให้โครงสร้างข้อมูลของเอกสารรับรองมีความสอดคล้องทั้งในเชิงความหมายและโครงสร้างข้อมูล อันเอื้อต่อการนำไปใช้ในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน

หัวข้อถัดไปจะแสดงตัวอย่างการประยุกต์ใช้โครงสร้างข้อมูลดังกล่าวในเชิงเทคนิค ครอบคลุมกระบวนการสร้างเอกสารรับรอง (VC) การลงลายมือชื่อดิจิทัล และการสำแดงข้อมูลในรูปแบบเอกสารสำแดง (VP) เพื่อใช้เป็นแนวทางสำหรับนักพัฒนาระบบ

3.2 การเขียนชุดคำสั่งในสคีมาของใบอนุญาตขับขี่

หัวข้อนี้นำเสนอการประยุกต์ใช้สคีมาข้อมูลของใบอนุญาตขับขี่ในการพัฒนาระบบออกเอกสารรับรอง (VC) โดยมุ่งเน้นการอธิบายองค์ประกอบและขั้นตอนการดำเนินการในเชิงเทคนิค ได้แก่ การจัดโครงสร้างข้อมูลตาม credentialSubject การสร้างเอกสารรับรองในรูปแบบ VC การลงลายมือชื่อดิจิทัล และการสำแดงข้อมูลในรูปแบบ VP ทั้งนี้ เพื่อใช้เป็นแนวทางสำหรับการพัฒนาระบบให้สอดคล้องกับมาตรฐานที่เกี่ยวข้อง

โดยตัวอย่างชุดคำสั่งที่แสดงในหัวข้อย่อยถัดไปจัดทำขึ้นเพื่อประกอบความเข้าใจในเชิงแนวคิดและลำดับการประมวลผลเท่านั้น โดยอาจใช้ภาษาโปรแกรมหรือกรอบงานใดกรอบงานหนึ่งเป็นตัวแทนในการอธิบาย ทั้งนี้ มิได้มีวัตถุประสงค์เพื่อกำหนดข้อบังคับด้านเทคโนโลยี และหน่วยงานสามารถเลือกใช้ภาษาโปรแกรม เครื่องมือ หรือสถาปัตยกรรมที่เหมาะสมกับบริบทของตนได้

3.2.1 รูปแบบและกลไกของเอกสารรับรองดิจิทัล

การพัฒนาระบบออกและใช้งานเอกสารรับรองดิจิทัล (Verifiable Credential) สามารถดำเนินการได้โดยอาศัยรูปแบบของเอกสารรับรอง (Credential Format) ที่แตกต่างกัน ซึ่งแต่ละรูปแบบจะใช้กลไกในการจัดโครงสร้างข้อมูล การลงลายมือชื่อ และการสำแดงข้อมูลที่แตกต่างกัน โดยไม่ผูกกับไลบรารีหรือเครื่องมือเฉพาะใด ทั้งนี้ รูปแบบที่พบโดยทั่วไปสามารถแบ่งได้ดังนี้

(1) รูปแบบ JWT-based Verifiable Credential

เป็นรูปแบบที่เอกสารรับรองถูกจัดเก็บและลงลายมือชื่อในรูปแบบ JSON Web Token (JWT) โดยอาศัยมาตรฐานในกลุ่ม JOSE (JSON Object Signing and Encryption) เช่น JWS และ JWK เหมาะสำหรับกรณีที่ต้องการความเรียบง่าย และสามารถทำงานร่วมกับระบบที่ใช้ OAuth 2.0 หรือ OpenID Connect ได้โดยตรง

(2) รูปแบบ JSON-LD Verifiable Credential

เป็นรูปแบบที่สอดคล้องกับแบบจำลองข้อมูลของ W3C VC โดยใช้ JSON-LD เป็นโครงสร้างข้อมูล และใช้กลไก Data Integrity สำหรับการลงลายมือชื่อ เหมาะสำหรับกรณีที่ต้องการรักษาความหมายของข้อมูล (semantic interoperability) และรองรับการเชื่อมโยงข้อมูล (Linked Data) โดยเฉพาะในบริบทที่ต้องอ้างอิง ontology หรือ schema กลาง เช่น TGIX Semantic

(3) รูปแบบ SD-JWT Verifiable Credential

เป็นรูปแบบที่พัฒนาต่อยอดจาก JWT โดยรองรับกลไกการเปิดเผยข้อมูลแบบเลือกได้ (Selective Disclosure) ทำให้ผู้ถือเอกสารสามารถเลือกเปิดเผยเฉพาะข้อมูลที่จำเป็นในขั้นตอนการสำแดง (Verifiable Presentation) ได้ เหมาะสำหรับกรณีใช้งานที่ต้องคำนึงถึงหลักการคุ้มครองข้อมูลส่วนบุคคล (Data Minimization) และ ออกแบบโดยคำนึงถึงการคุ้มครองข้อมูลส่วนบุคคลตั้งแต่ต้น (Privacy by Design) โดยรูปแบบดังกล่าวสามารถทำงานร่วมกับโปรโตคอล เช่น OID4VCI และ OID4VP ได้

นอกจากรูปแบบของเอกสารรับรองที่กล่าวข้างต้น ยังมีรูปแบบอื่นที่ถูกใช้งานในบางบริบทเฉพาะ เช่น รูปแบบ Mobile Document (mDoc) ตามมาตรฐาน ISO/IEC 18013-5 ซึ่งใช้โครงสร้างข้อมูลแบบ CBOR และกลไกการลงลายมือชื่อแบบ COSE สำหรับกรณีใช้งาน เช่น ใบอนุญาตขับขี่ดิจิทัล (Mobile Driving

License: mDL) อย่างไรก็ตาม เอกสารฉบับนี้มุ่งเน้นรูปแบบที่สอดคล้องกับมาตรฐาน W3C VC และ OpenID ecosystem เป็นหลัก เพื่อให้สามารถนำไปใช้งานร่วมกับระบบภาครัฐได้อย่างกว้างขวางและสอดคล้องกับแนวโน้มสากล

3.2.2 ชุดคำสั่งการออกเอกสารรับรองรูปแบบ JWT

ตัวอย่างต่อไปนี้เป็นเพียงตัวอย่างประกอบเพื่อแสดงลำดับการทำงานของระบบ โดยใช้ภาษาโปรแกรมหนึ่งเป็นตัวแทน ทั้งนี้ โครงสร้างตรรกะและขั้นตอนสามารถนำไปประยุกต์ใช้กับภาษาโปรแกรมหรือกรอบงานอื่นได้ตามความเหมาะสม โดยเป็นการแสดงแนวทางการพัฒนาส่วนบริการ สำหรับรับคำร้องขอออกเอกสารรับรองใบอนุญาตขับขี่ในรูปแบบ JWT โดยมีการลงลายมือชื่อดิจิทัลด้วยอัลกอริทึม EdDSA (Ed25519)

ตัวอย่างรหัสที่ 3.2 API Route สำหรับออกเอกสารรับรองรูปแบบ JWT

```
// ไฟล์: app/api/credentials/issue/route.ts
// API Route สำหรับออกเอกสารรับรอง (Verifiable Credential) ในรูปแบบ JWT
import { NextRequest, NextResponse } from 'next/server';
import * as jose from 'jose';
// กำหนดชนิดข้อมูลสำหรับข้อมูลใบอนุญาตขับขี่
interface ThaiDLData {
  document_number: string;
  family_name: string;
  given_name: string;
  family_name_thai: string;
  given_name_thai: string;
  birth_date: string;
  national_id: string;
  issuing_country: string;
  driving_privileges: Array<{
    vehicle_category_code: string;
    issue_date: string;
    expiry_date: string;
  }>;
  [key: string]: unknown;
}
export async function POST(req: NextRequest) {
  // รับข้อมูลจากคำร้องขอ
  const { subjectDid, licenseData } = await req.json() as {
    subjectDid: string;
    licenseData: ThaiDLData;
  };
  // นำเข้ากุญแจส่วนตัวของผู้ออกเอกสาร (Issuer Private Key)
```

```
const privateKey = await jose.importPKCS8(
  process.env.ISSUER_PRIVATE_KEY!,
  'EdDSA'
);

const now = Math.floor(Date.now() / 1000);
const FIVE_YEARS = 5 * 365 * 24 * 60 * 60;
// สร้าง Payload ของ Verifiable Credential
const vcPayload = {
  iss: 'did:web:dlt.go.th',           // DID ของผู้ออกเอกสาร
  sub: subjectDid,                     // DID ของผู้ถือเอกสาร
  nbf: now,                           // เริ่มมีผลบังคับใช้
  exp: now + FIVE_YEARS,              // วันหมดอายุ
  vc: {
    '@context': [
      'https://www.w3.org/ns/credentials/v2',
      'https://w3id.org/vdl/v2',
      'https://dlt.go.th/credentials/v1'
    ],
    type: [
      'VerifiableCredential',
      'ThaiDrivingLicenseCredential'
    ],
    credentialSubject: {
      id: subjectDid,
      driversLicense: {
        type: 'ThaiDrivingLicenseCredential',
        ...licenseData
      }
    }
  }
};
// ลงนามด้วย EdDSA (Ed25519)
const jwt = await new jose.SignJWT(vcPayload)
  .setProtectedHeader({
    alg: 'EdDSA',
    typ: 'JWT',
    kid: 'did:web:dlt.go.th#key-1'
```

```
    })
    .setIssuedAt()
    .sign(privateKey);

  return NextResponse.json({
    verifiableCredential: jwt,
    format: 'jwt_vc'
  });
}
```

3.2.3 ชุดคำสั่งการออกเอกสารรับรองรูปแบบ SD-JWT VC

SD-JWT VC เป็นรูปแบบของเอกสารรับรองที่รองรับกลไกการเปิดเผยข้อมูลแบบเลือกได้ (Selective Disclosure) ซึ่งเอื้อต่อการควบคุมการเปิดเผยข้อมูลของผู้ถือเอกสารในขั้นตอนการสำแดง (Verifiable Presentation) โดยผู้ออกเอกสารสามารถกำหนดแอตทริบิวต์ที่อนุญาตให้เปิดเผยหรือปกปิดได้ ทั้งนี้ ตัวอย่างต่อไปนี้แสดงการประยุกต์ใช้รูปแบบ SD-JWT VC ในการออกเอกสารรับรอง โดยกำหนดให้ข้อมูลส่วนบุคคลที่มีความอ่อนไหว เช่น ชื่อ-สกุล วันเกิด เลขประจำตัวประชาชน และหมู่เลือด ถูกจัดเก็บในลักษณะที่รองรับการเปิดเผยแบบเลือก เพื่อให้สอดคล้องกับหลักการคุ้มครองข้อมูลส่วนบุคคลและการใช้ข้อมูลเท่าที่จำเป็น

ตัวอย่างรหัสที่ 3.3 การออกเอกสารรับรอง SD-JWT VC

```
// ไฟล์: app/api/credentials/issue-sdjwt/route.ts
// API Route สำหรับออกเอกสารรับรองในรูปแบบ SD-JWT VC
import { SDJwtVcInstance } from '@sd-jwt/sd-jwt-vc';
import { digest, generateSalt } from '@sd-jwt/crypto-nodejs';
import type { DisclosureFrame } from '@sd-jwt/types';
import Crypto from 'node:crypto';
// สร้างคู่กุญแจ Ed25519 สำหรับผู้ออกเอกสาร
const { privateKey, publicKey } = Crypto.generateKeyPairSync('ed25519');
// กำหนดฟังก์ชันลงนามและตรวจสอบ
const signer = async (data: string) =>
  Buffer.from(
    Crypto.sign(null, Buffer.from(data), privateKey)
  ).toString('base64url');
const verifier = async (data: string, sig: string) =>
  Crypto.verify(
    null,
    Buffer.from(data),
    publicKey,
    Buffer.from(sig, 'base64url')
  );
// สร้างอินสแตนซ์ SD-JWT VC
const sdjwt = new SDJwtVcInstance({
  signer,
  signAlg: 'EdDSA',
  verifier,
  hasher: digest,
  hashAlg: 'sha-256',
  saltGenerator: generateSalt,
});
```

```
// ข้อมูลใบอนุญาตขับขี่ (Claims)
const claims = {
  document_number: '12345678',
  family_name: 'SMITH',
  given_name: 'JOHN',
  family_name_thai: 'สมิท',
  given_name_thai: 'จอห์น',
  title_thai: 'นาย',
  birth_date: '1990-05-15',
  national_id: '1100400123456',
  blood_type: 'O',
  issuing_country: 'TH',
  license_type_code: 'car_private_5yr',
  driving_privileges: [
    {
      vehicle_category_code: 'B',
      issue_date: '2020-01-01',
      expiry_date: '2029-01-01',
    },
  ],
};
// กำหนดฟิลด์ที่สามารถเปิดเผยแบบเลือกได้
// ฟิลด์ที่อยู่ใน _sd จะถูกแฮชและซ่อนไว้
// ฟิลด์ที่ไม่อยู่ใน _sd จะเปิดเผยเสมอ
const disclosureFrame: DisclosureFrame<typeof claims> = {
  _sd: [
    'family_name',
    'given_name',
    'family_name_thai',
    'given_name_thai',
    'title_thai',
    'birth_date',
    'national_id',
    'blood_type',
  ],
};
// document_number, issuing_country, license_type_code,
// driving_privileges จะเปิดเผยเสมอ
```

```
// ออกเอกสารรับรอง SD-JWT VC
const credential = await sdjwt.issue(
  {
    iss: 'did:web:dlt.go.th',
    iat: Math.floor(Date.now() / 1000),
    vct: 'ThaiDrivingLicenseCredential',
    ...claims,
  },
  disclosureFrame
);
console.log(credential);
// ผลลัพธ์: <JWT>~<Disclosure1>~<Disclosure2>~...
```

หมายเหตุ: ในตัวอย่างนี้ ฟิลด์ document_number, issuing_country, license_type_code และ driving_privileges ไม่ได้อยู่ใน _sd จึงเปิดเผยเสมอทุกครั้งที่มีการสำแดง ขณะที่ฟิลด์อื่น ๆ เช่น national_id และ blood_type ถูกซ่อนเป็นค่าแฮช SHA-256 และจะเปิดเผยได้ ก็ต่อเมื่อ ผู้ถือเอกสารเลือกที่จะเปิดเผย

3.3 การเขียนชุดคำสั่งในการยืนยันและตรวจสอบ

การยืนยันและตรวจสอบเอกสารรับรองดิจิทัล (Verification) เป็นกระบวนการที่ผู้ตรวจสอบเอกสาร (Verifier) ดำเนินการเพื่อให้มั่นใจว่าเอกสารรับรองที่ได้รับนั้นเป็นของจริง ไม่ถูกดัดแปลง ยังไม่หมดอายุ และยังไม่ถูกเพิกถอน กระบวนการนี้ประกอบด้วยขั้นตอนหลัก 5 ขั้นตอน ดังนี้

ขั้นตอนที่ 1: ถอดรหัส VP Token เพื่อดึงข้อมูล payload ของเอกสารสำแดง

ขั้นตอนที่ 2: ตรวจสอบค่า nonce เพื่อป้องกันการโจมตีแบบ replay attack

ขั้นตอนที่ 3: แก้ไข DID (Decentralized Identifier) ของผู้ออกเอกสารเพื่อดึงกุญแจสาธารณะจาก DID Document

ขั้นตอนที่ 4: ตรวจสอบลายมือชื่อดิจิทัลของ VP และ VC แต่ละฉบับ

ขั้นตอนที่ 5: ตรวจสอบวันหมดอายุ และสถานะการเพิกถอน

3.3.1 ชุดคำสั่งการตรวจสอบเอกสารสำแดงรูปแบบ JWT

ตัวอย่างต่อไปนี้แสดง API Route ใน Next.js สำหรับรับและตรวจสอบ VP Token ในรูปแบบ JWT พร้อมตรวจสอบ VC แต่ละฉบับที่อยู่ภายในเอกสารสำแดง

ตัวอย่างรหัสที่ 3.4 API Route สำหรับตรวจสอบเอกสารสำแดง

```
// ไฟล์: app/api/verify/route.ts
// API Route สำหรับตรวจสอบเอกสารสำแดง (Verifiable Presentation)
import { NextRequest, NextResponse } from 'next/server';
import * as jose from 'jose';
export async function POST(req: NextRequest) {
```

```
const { vpToken, nonce } = await req.json();
try {
  // ขั้นตอนที่ 1: ถอดรหัส VP Token
  const vpPayload = jose.decodeJwt(vpToken);
  // ขั้นตอนที่ 2: ตรวจสอบ nonce ป้องกันการโจมตีแบบ replay
  if (vpPayload.nonce !== nonce) {
    return NextResponse.json(
      { valid: false, error: 'nonce ไม่ตรงกัน' },
      { status: 400 }
    );
  }
  // ขั้นตอนที่ 3: ดึงกุญแจสาธารณะของผู้ออกเอกสารจาก DID Document
  const issuerDid = vpPayload.iss as string;
  const issuerPublicKey = await resolveIssuerKey(issuerDid);
  // ขั้นตอนที่ 4: ตรวจสอบลายเซ็นของ VP
  const { payload: verifiedVP } = await jose.jwtVerify(
    vpToken,
    issuerPublicKey
  );
  // ขั้นตอนที่ 5: ตรวจสอบ VC แต่ละฉบับภายใน VP
  const credentials = verifiedVP.vp?.verifiableCredential || [];
  const vcResults = [];
  for (const vcJwt of credentials) {
    const vcPayload = jose.decodeJwt(vcJwt);
    const vcIssuerKey = await resolveIssuerKey(vcPayload.iss);
    // ตรวจสอบลายเซ็น
    await jose.jwtVerify(vcJwt, vcIssuerKey);
    // ตรวจสอบวันหมดอายุ
    const now = Math.floor(Date.now() / 1000);
    if (vcPayload.exp && vcPayload.exp < now) {
      vcResults.push({
        valid: false,
        error: 'เอกสารรับรองหมดอายุแล้ว'
      });
      continue;
    }
    // ตรวจสอบว่ายังไม่ถูกเพิกถอน
    const isRevoked = await checkRevocation(vcPayload);
```

```
      if (isRevoked) {
        vcResults.push({
          valid: false,
          error: 'เอกสารรับรองถูกเพิกถอนแล้ว'
        });
        continue;
      }
      vcResults.push({
        valid: true,
        credential: vcPayload.vc
      });
    }
    return NextResponse.json({
      valid: true,
      verifiedCredentials: vcResults
    });
  } catch (error) {
    return NextResponse.json(
      { valid: false, error: 'การตรวจสอบล้มเหลว' },
      { status: 400 }
    );
  }
}
// ฟังก์ชันช่วย: แก้ไข DID เพื่อดึงกุญแจสาธารณะ
async function resolveIssuerKey(did: string) {
  // ตัวอย่าง: did:web:dlt.go.th ⟶ GET https://dlt.go.th/.well-known/did.json
  const url = did.replace('did:web:', 'https://') + '/.well-known/did.json';
  const res = await fetch(url);
  const didDoc = await res.json();
  const keyJwk = didDoc.verificationMethod[0].publicKeyJwk;
  return jose.importJWK(keyJwk, 'EdDSA');
}
// ฟังก์ชันช่วย: ตรวจสอบสถานะการเพิกถอน
async function checkRevocation(payload: any): Promise<boolean> {
  // ใช้ Status List 2021 หรือ Bitstring Status List
  if (!payload.vc?.credentialStatus) return false;
  const statusUrl = payload.vc.credentialStatus.statusListCredential;
  const res = await fetch(statusUrl);
```

```
  const statusList = await res.json();
  const idx = payload.vc.credentialStatus.statusListIndex;
  return checkBit(statusList, idx);
}
```

3.3.2 การตรวจสอบผ่านโปรโตคอล OID4VP

OpenID for Verifiable Presentations (OID4VP) เวอร์ชัน 1.0 เป็นโปรโตคอลมาตรฐานที่พัฒนาโดย OpenID Foundation สำหรับการร้องขอและสำแดงเอกสารรับรอง (Verifiable Presentation) ผ่านช่องทางออนไลน์ โดยมีรากฐานจากมาตรฐาน OpenID Connect และสามารถนำไปใช้ร่วมกับรูปแบบเอกสารรับรองที่หลากหลาย ทั้งนี้ มาตรฐาน ISO/IEC TS 18013-7:2024 ได้นำโปรโตคอลดังกล่าวไปประยุกต์ใช้เป็นหนึ่งในแนวทางสำหรับการสำแดงใบอนุญาตขับขี่อิเล็กทรอนิกส์ผ่านช่องทางระยะไกล อย่างไรก็ดี โปรโตคอล OID4VP มิได้มีที่มาจากมาตรฐาน ISO ดังกล่าวโดยตรง แต่เป็นมาตรฐานสากลที่สามารถนำไปใช้ในหลายบริบทนอกเหนือจากกรณีใบอนุญาตขับขี่อิเล็กทรอนิกส์ได้ โดยในภาพรวม หน่วยงานผู้ตรวจสอบเอกสารสามารถร้องขอข้อมูลจากผู้ถือเอกสาร และผู้ถือเอกสารสามารถสำแดงข้อมูลที่เกี่ยวข้องเพื่อตอบสนองต่อคำร้องขอดังกล่าวได้ตามวัตถุประสงค์ของการใช้งาน

3.3.3 การออกเอกสารรับรองผ่านโปรโตคอล OID4VCI

OpenID for Verifiable Credential Issuance (OID4VCI) เวอร์ชัน 1.0 เป็นโปรโตคอลมาตรฐานที่พัฒนาโดย OpenID Foundation สำหรับการออกเอกสารรับรองดิจิทัลผ่านช่องทางออนไลน์ โดยอาศัยกลไกด้านความปลอดภัยจาก OAuth 2.0 เพื่อควบคุมการเข้าถึงและยืนยันสิทธิของผู้ขอรับเอกสาร ทั้งนี้ โปรโตคอลดังกล่าวสามารถนำไปใช้ร่วมกับรูปแบบเอกสารรับรองที่หลากหลาย และมิได้มีที่มาจากมาตรฐาน ISO โดยตรง แม้ว่าในบางกรณี เช่น การออกใบอนุญาตขับขี่อิเล็กทรอนิกส์ อาจมีการนำไปประยุกต์ใช้ร่วมกับมาตรฐานที่เกี่ยวข้อง

ในภาพรวม กระบวนการทำงานเริ่มจากผู้ถือเอกสารยืนยันตัวตนกับผู้ออกเอกสาร จากนั้นจะได้รับข้อมูลหรือรหัสสำหรับใช้ยืนยันสิทธิในการขอรับเอกสารรับรองผ่านกระเป๋าเอกสารดิจิทัล (Digital Wallet) โดยกระเป๋าดังกล่าวจะติดต่อกับระบบของผู้ออกเอกสารเพื่อขอรับเอกสารรับรอง และดำเนินการตามขั้นตอนที่กำหนดในโปรโตคอล ก่อนจัดเก็บเอกสารรับรองไว้ใช้งานต่อไป ทั้งนี้ อาจมีการใช้กลไกเพิ่มเติมเพื่อยืนยันความเป็นเจ้าของของผู้ถือเอกสาร เช่น การผูกเอกสารกับกุญแจดิจิทัลของอุปกรณ์ เพื่อเพิ่มความมั่นคงปลอดภัยในการใช้งาน

3.4 การเขียนชุดคำสั่งในการยืนยันและตรวจสอบ โดยไม่เปิดเผยแอตทริบิวต์สำคัญอื่น ๆ

การเปิดเผยข้อมูลแบบเลือกได้ (Selective Disclosure) เป็นกลไกสำคัญ ในการรักษาความเป็นส่วนตัวของผู้ถือเอกสารรับรอง โดยช่วยให้ผู้ถือเอกสารสามารถเลือกเปิดเผยเฉพาะแอตทริบิวต์ที่จำเป็นต่อการตรวจสอบในแต่ละกรณีใช้งาน (Use Case) เท่านั้น เช่น การเช่ารถ อาจต้องการเพียงยืนยันว่ามีใบอนุญาตขับขี่ประเภทที่ถูกต้องและยังไม่หมดอายุ โดยไม่จำเป็นต้องเปิดเผยเลขบัตรประชาชน หรือหมู่เลือด

3.4.1 หลักการทำงานของ SD-JWT (RFC 9901)

SD-JWT (Selective Disclosure for JWTs) เป็นมาตรฐานระดับ RFC (RFC 9901 เผยแพร่เมื่อเดือนพฤศจิกายน พ.ศ. 2568) ที่กำหนดกลไกการเปิดเผยข้อมูลแบบเลือกได้ (Selective Disclosure) สำหรับ JSON Web Token (JWT) โดยแนวคิดหลักคือการไม่เก็บค่าข้อมูลสำคัญไว้ในรูปแบบเปิดเผยโดยตรง แต่แทนที่ด้วยค่าแฮช (Hash) เช่น SHA-256 เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ในขั้นตอนการออกเอกสาร (Issuance) ผู้ออกเอกสารจะกำหนดแอตทริบิวต์ที่สามารถเปิดเผยแบบเลือกได้ โดยค่าจริงของแอตทริบิวต์เหล่านี้จะถูกจัดเก็บในรูปแบบที่เรียกว่า Disclosure ซึ่งประกอบด้วยข้อมูล เช่น salt (ค่าข้อมูลสุ่มที่ใช้ร่วมกับการแฮชเพื่อป้องกันการคาดเดาค่าเดิม), ชื่อแอตทริบิวต์ (claim name) และค่าของแอตทริบิวต์ (claim value) ก่อนนำไปเข้ารหัสแบบ base64url และสร้างค่าแฮช (SHA-256) เพื่อบันทึกไว้ในโครงสร้าง JWT (เช่น ในฟิลด์ _sd) โดยไม่เปิดเผยค่าจริงในตัวโทเคน ผลลัพธ์โดยรวมจะอยู่ในรูปแบบที่ประกอบด้วย JWT และชุดของ Disclosure ที่เกี่ยวข้อง

ในขั้นตอนการสำแดง (Presentation) ผู้ถือเอกสารสามารถเลือกส่งเฉพาะ Disclosure ที่ต้องการเปิดเผยให้แก่ผู้ตรวจสอบเอกสาร (Verifier) โดย Disclosure ที่ไม่ได้ส่งจะไม่สามารถถูกนำไปใช้เพื่อคำนวณย้อนกลับเป็นค่าจริงได้ นอกจากนี้ อาจมีการใช้ Key Binding JWT (KB-JWT) เพื่อยืนยันว่าผู้ที่นำเสนอข้อมูลเป็นเจ้าของเอกสารรับรองตัวจริง ซึ่งช่วยเพิ่มความมั่นคงปลอดภัยในการใช้งาน

3.4.2 ชุดคำสั่งการสำแดงแบบเปิดเผยเลือกด้วย SD-JWT

ตัวอย่างต่อไปนี้แสดงการใช้งาน SD-JWT ใน 3 กรณี ได้แก่ การตรวจสอบใบอนุญาตขับขี่ โดยไม่เปิดเผยข้อมูลส่วนบุคคล การพิสูจน์ตัวตนทั่วไปที่เปิดเผยเฉพาะชื่อและวันเกิด และการพิสูจน์ตัวตนเต็มรูปแบบที่เปิดเผยรวมถึงเลขบัตรประชาชน

ตัวอย่างรหัสที่ 3.5 การสำแดงแบบเปิดเผยเลือกด้วย SD-JWT

```
// ไฟล์: lib/sd-jwt-present.ts
// ฟังก์ชันสำหรับผู้ถือเอกสาร (Holder) สร้างเอกสารสำแดง SD-JWT
import { SDJwtVcInstance } from '@sd-jwt/sd-jwt-vc';
import { digest, generateSalt } from '@sd-jwt/crypto-nodejs';
// ... (ตั้งค่า sdjwt instance เหมือนในหัวข้อ 3.2) ...
// ===== กรณีที่ 1: ตรวจสอบประเภทใบอนุญาตขับขี่เท่านั้น =====
// เปิดเผยเฉพาะ driving_privileges (เปิดเผยเสมอ)
// ไม่เปิดเผยข้อมูลส่วนบุคคลใด ๆ
const licenseCheckOnly = await sdjwt.present(
  credential,
  {} // ไม่เลือกเปิดเผยฟิลด์ที่ซ่อนไว้
);
// ===== กรณีที่ 2: ยืนยันตัวตนทั่วไป =====
// เปิดเผยชื่อ-สกุล + วันเกิด
const identityCheck = await sdjwt.present(
  credential,
  {
    family_name: true,
    given_name: true,
    birth_date: true,
  }
);
// ===== กรณีที่ 3: ยืนยันตัวตนเต็มรูปแบบ =====
// เปิดเผยชื่อ-สกุล + วันเกิด + เลขบัตรประชาชน
const fullIdentityCheck = await sdjwt.present(
  credential,
  {
    family_name: true,
    given_name: true,
    family_name_thai: true,
    given_name_thai: true,
    birth_date: true,
```

```
    national_id: true,
  }
);
// ===== ผู้ตรวจสอบเอกสาร (Verifier): ตรวจสอบเอกสารสำแดง =====
const result = await sdjwt.verify(identityCheck);
console.log(result.payload);
// ผลลัพธ์ที่ได้:
// {
//   iss: 'did:web:dlt.go.th',
//   iat: 1710000000,
//   vct: 'ThaiDrivingLicenseCredential',
//   document_number: '12345678',        // เปิดเผยเสมอ
//   issuing_country: 'TH',              // เปิดเผยเสมอ
//   license_type_code: 'car_private_5yr', // เปิดเผยเสมอ
//   driving_privileges: [...],          // เปิดเผยเสมอ
//   family_name: 'SMITH',               // เปิดเผยตามที่เลือก
//   given_name: 'JOHN',                 // เปิดเผยตามที่เลือก
//   birth_date: '1990-05-15',           // เปิดเผยตามที่เลือก
//   // national_id: ไม่แสดง (ถูกซ่อนไว้)
//   // blood_type: ไม่แสดง (ถูกซ่อนไว้)
// }
```

3.4.3 ทางเลือก: BBS+ Signatures (bbs-2023)

มาตรฐาน BBS+ Signatures เป็นอีกแนวทางหนึ่งที่รองรับการเปิดเผยข้อมูลแบบเลือกได้ (Selective Disclosure) โดยอาศัยหลักการ Zero-Knowledge Proof (ZKP) (การพิสูจน์ข้อมูลโดยไม่ต้องเปิดเผยค่าจริงทั้งหมด) จุดเด่นสำคัญเมื่อเทียบกับ SD-JWT คือคุณสมบัติ Unlinkability (ความสามารถในการป้องกันการเชื่อมโยงข้อมูลระหว่างการใช้งานแต่ละครั้ง) กล่าวคือ หลักฐาน ZKP ที่สร้างขึ้นจากลายเซ็นเดียวกันในแต่ละครั้งจะไม่สามารถเชื่อมโยงกลับไปยังลายเซ็นต้นฉบับ หรือเชื่อมโยงกันระหว่างการสำแดงหลายครั้งได้ ซึ่งช่วยลดความเสี่ยงในการติดตามพฤติกรรมของผู้ถือเอกสารข้ามผู้ตรวจสอบเอกสารหลายราย

ปัจจุบัน มาตรฐาน BBS+ อยู่ในสถานะ IETF Internet-Draft (draft-irtf-cfrg-bbs-signatures-09 เมื่อเดือนกรกฎาคม พ.ศ. 2568) และมีการกำหนด cryptosuite ที่เกี่ยวข้องใน W3C เช่น bbs-2023 สำหรับการใช้งานร่วมกับ Verifiable Credentials ทั้งนี้ แนวทางการทำงานของ BBS+ แตกต่างจาก SD-JWT ในเชิงสถาปัตยกรรม โดยผู้ออกเอกสารจะลงนามข้อมูลหลายแอตทริบิวต์พร้อมกันด้วยลายเซ็น BBS เดียว จากนั้นผู้ถือเอกสารสามารถสร้างหลักฐาน ZKP เพื่อเปิดเผยเฉพาะแอตทริบิวต์ที่ต้องการ และผู้ตรวจสอบเอกสารจะทำการตรวจสอบหลักฐานดังกล่าวโดยไม่สามารถเชื่อมโยงกลับไปยังลายเซ็นต้นฉบับได้

ตัวอย่างรหัสที่ 3.6 การใช้ BBS+ Signatures สำหรับ Selective Disclosure

```
// ไฟล์: lib/bbs-comparison.ts
// ตัวอย่างการใช้ BBS+ Signatures สำหรับ Selective Disclosure
// (ต้องติดตั้ง: npm install @digitalbazaar/bbs-2023-cryptosuite
//               @digitalbazaar/bls12-381-multikey)
import * as vc from '@digitalbazaar/vc';
import { DataIntegrityProof } from '@digitalbazaar/data-integrity';
import {
  createSignCryptosuite,
  createDiscloseCryptosuite
} from '@digitalbazaar/bbs-2023-cryptosuite';
import * as Bls12381Multikey from '@digitalbazaar/bls12-381-multikey';
// ขั้นตอนที่ 1: สร้างคู่กุญแจ BLS12-381
const keyPair = await Bls12381Multikey.generateBbsKeyPair({
  algorithm: 'BBS-BLS12-381-SHA-256',
});
// ขั้นตอนที่ 2: ผู้ออกเอกสาร - ลงนามเอกสารรับรองด้วย BBS+
const signSuite = new DataIntegrityProof({
  signer: keyPair.signer(),
  cryptosuite: createSignCryptosuite({
```

```
    mandatoryPointers: [
      // ฟิลด์ที่ต้องเปิดเผยเสมอ (Mandatory)
      '/issuer',
      '/validFrom',
      '/credentialSubject/driversLicense/document_number',
      '/credentialSubject/driversLicense/driving_privileges',
      '/credentialSubject/driversLicense/issuing_country',
    ],
  }),
});
const signedVC = await vc.issue({
  credential: thaiDLTCredential,  // VC แบบ JSON-LD
  suite: signSuite,
  documentLoader,
});
// ขั้นตอนที่ 3: ผู้ถือเอกสาร - สร้างหลักฐาน ZKP :: เลือกเปิดเผยเฉพาะชื่อ-สกุลและวันเกิด
const discloseSuite = new DataIntegrityProof({
  cryptosuite: createDiscloseCryptosuite({
    selectivePointers: [
      '/credentialSubject/driversLicense/family_name',
      '/credentialSubject/driversLicense/given_name',
      '/credentialSubject/driversLicense/birth_date',
    ],
  }),
});
const derivedVC = await vc.derive({
  verifiableCredential: signedVC,
  suite: discloseSuite,
  documentLoader,
});
// derivedVC มีเฉพาะฟิลด์ mandatory + selective ที่เลือก
// ลายเซ็นที่ได้เป็น ZKP - ไม่สามารถเชื่อมโยงกลับไปที่ต้นฉบับได้
```

3.4.4 การเปรียบเทียบเทคนิค Selective Disclosure

การเปรียบเทียบคุณสมบัติที่สำคัญระหว่าง 3 เทคนิคหลักสำหรับ Selective Disclosure ในระบบเอกสารรับรองดิจิทัล ดังแสดงในตารางที่ 3.5

คุณสมบัติ	**SD-JWT (RFC 9901)**	**BBS+ (bbs-2023)**
การเปิดเผยแบบเลือกได้	รองรับ (Hash-based)	รองรับ (Cryptographic)
ความไม่สามารถเชื่อมโยงได้ (Unlinkability)	ไม่รองรับ	รองรับ
การพิสูจน์เชิงเงื่อนไข (Predicate Proofs)	ไม่รองรับ	ไม่รองรับ (ต้องขยาย)
ผู้กำหนดฟิลด์ที่เปิดเผย	ผู้ออกเอกสาร (Issuer)	ผู้ถือเอกสาร (Holder)
ความซับซ้อนในการพัฒนา	ต่ำ	ปานกลาง-สูง
ความเร็วในการลงนาม	< 1 มิลลิวินาที	6-7.5 มิลลิวินาที
ความเร็วในการตรวจสอบ	< 1 มิลลิวินาที	~19 มิลลิวินาที
ระดับมาตรฐาน	RFC (สูงสุด)	IETF I-D และ W3C CR
ความเข้ากันได้กับ JWT/JOSE	รองรับ	ไม่รองรับ (JSON-LD)
การยอมรับในระบบนิเวศ	EU EUDI, 30และประเทศ	MATTR, Trinsic

ตารางที่ 7 เปรียบเทียบเทคนิค Selective Disclosure

3.4.5 ข้อเสนอแนะสำหรับกรอบมาตรฐาน TGIX

สำหรับการดำเนินการในระยะแรก สามารถพิจารณาใช้ SD-JWT (RFC 9901) เป็นกลไกหลักสำหรับการเปิดเผยข้อมูลแบบเลือกได้ (Selective Disclosure) เนื่องจากเป็นมาตรฐานระดับ RFC ที่มีความพร้อมในการใช้งานในปัจจุบัน มีความซับซ้อนไม่สูง และสามารถประยุกต์ใช้ร่วมกับโครงสร้างพื้นฐานแบบ JSON Web Token (JWT) ที่มีอยู่ได้ โดยแนวทางดังกล่าวได้รับการยอมรับในระบบนิเวศดิจิทัลระดับนานาชาติ เช่น โครงการ European Digital Identity Wallet (EUDI Wallet) และการนำไปใช้งานในหลายประเทศ ทั้งนี้ SD-JWT ยังสามารถทำงานร่วมกับโปรโตคอล OpenID Connect for Verifiable Credential Issuance (OID4VCI) และ OpenID Connect for Verifiable Presentations (OID4VP) ได้อย่างสอดคล้อง

อย่างไรก็ดี SD-JWT ยังไม่รองรับการพิสูจน์เชิงเงื่อนไข (Predicate Proof) โดยตรง (เช่น การพิสูจน์ว่าอายุเกินเกณฑ์ที่กำหนดโดยไม่เปิดเผยวันเกิดจริง) ซึ่งสามารถบรรเทาได้ในบางกรณีโดยการออกแบบแอตทริบิวต์เพิ่มเติม เช่น age_over_NN ตามแนวทางของมาตรฐาน ISO/IEC 18013-5

สำหรับการพัฒนาในระยะต่อไป หน่วยงานที่มีความต้องการด้านความเป็นส่วนตัวในระดับสูง เช่น การป้องกันการเชื่อมโยงข้อมูลการสำแดงของผู้ถือเอกสารข้ามผู้ตรวจสอบเอกสารหลายราย (Unlinkability) อาจพิจารณาใช้ BBS+ Signatures (bbs-2023) เป็นทางเลือกเพิ่มเติม ซึ่งอาศัยหลักการ Zero-Knowledge Proof อย่างไรก็ดี มาตรฐานดังกล่าวยังอยู่ในระยะพัฒนา (IETF Internet-Draft) และมีข้อจำกัดในด้านการรองรับโครงสร้างพื้นฐานบางประเภท เช่น Hardware Security Module (HSM) (อุปกรณ์สำหรับจัดเก็บกุญแจดิจิทัลอย่างปลอดภัย) รวมถึงการใช้เส้นโค้งเข้ารหัสเฉพาะ เช่น BLS12-381 ซึ่งอาจยังไม่รองรับอย่างแพร่หลายในบางระบบ

4 กรณีศึกษาอื่น ๆ

บทนี้นำเสนอกรณีศึกษาการประยุกต์ใช้เอกสารรับรองดิจิทัล (Verifiable Credential: VC) และเอกสารสำแดง (Verifiable Presentation: VP) ในบริบทที่หลากหลาย เพื่อใช้เป็นแนวทางอ้างอิงสำหรับการนำมาตรฐานไปประยุกต์ใช้ในทางปฏิบัติ โดยครอบคลุม 2 กรณีศึกษา ได้แก่ การใช้งานกับใบอนุญาตขับขี่อิเล็กทรอนิกส์ภายใต้กระเป๋าเอกสารดิจิทัลของสหภาพยุโรป (European Digital Identity Wallet: EUDI Wallet) และการใช้งานกับเอกสารทางการศึกษาในสถาบันอุดมศึกษาของประเทศไทย

4.1 แนวทางการใช้งานเอกสารรับรองและเอกสารสำแดงในต่างประเทศและตัวอย่างการใช้งาน

4.1.1 ภาพรวมของ EUDIW และกรอบสถาปัตยกรรม

กระเป๋าอัตลักษณ์ดิจิทัลของสหภาพยุโรป (European Digital Identity Wallet: EUDI Wallet) ถูกกำหนดภายใต้กรอบกฎหมาย eIDAS 2.0 โดยกำหนดให้ประเทศสมาชิกของสหภาพยุโรปต้องจัดหากระเป๋าเอกสารดิจิทัลให้แก่ประชาชนภายในเดือนธันวาคม พ.ศ. 2569 ทั้งนี้กรอบสถาปัตยกรรม (ARF) ได้กำหนดบทบาทของผู้มีส่วนเกี่ยวข้องไว้มากกว่า 18 บทบาท เช่น Wallet Provider, PID Provider, QEAA Provider และ Relying Party โดยความน่าเชื่อถือของระบบอาศัยกลไกที่เรียกว่า Trusted Lists ซึ่งใช้สำหรับยืนยันสถานะและความน่าเชื่อถือของหน่วยงานที่เกี่ยวข้องในระบบนิเวศ

4.1.2 กรณีศึกษา Mobile Driving Licence (mDL)

ในบริบทของกระเป๋าอัตลักษณ์ดิจิทัลของสหภาพยุโรป (EUDI Wallet) การนำใบอนุญาตขับขี่อิเล็กทรอนิกส์ (Mobile Driving Licence: mDL) มาใช้งานถือเป็นหนึ่งในกรณีศึกษาสำคัญ โดยโครงการนำร่องระยะที่ 1 ภายใต้ชื่อ POTENTIAL[11] ได้มีการทดสอบการใช้งานใน 4 สถานการณ์หลัก ครอบคลุมการใช้งานทั้งภายในประเทศและข้ามพรมแดน ซึ่งจากผลการดำเนินงานสามารถทดสอบได้มากกว่า 1,300 ครั้ง และมีธุรกรรมที่สำเร็จมากกว่า 1,000 รายการ รวมถึงกรณีการใช้งานข้ามพรมแดนจำนวน 249 กรณี แสดงให้เห็นถึงความเป็นไปได้ในการนำไปใช้งานจริงในระดับสหภาพยุโรป

สำหรับโครงการนำร่องระยะถัดไป (Large Scale Pilots) ได้มีการขยายความร่วมมือผ่านโครงการ เช่น APTITUDE[12] ซึ่งมีพันธมิตรเข้าร่วม 117 องค์กรจาก 11 ประเทศ และโครงการ WE BUILD ซึ่งมีผู้เข้าร่วม 197 หน่วยงาน เพื่อทดสอบการใช้งานในวงกว้างและหลากหลายบริบทมากยิ่งขึ้น

4.1.3 รูปแบบเอกสารรับรองที่บังคับใช้

สำหรับกรณีของใบอนุญาตขับขี่อิเล็กทรอนิกส์ (Mobile Driving Licence: mDL) ภายใต้มาตรฐานสหภาพยุโรป กำหนดให้ใช้รูปแบบ Mobile Document (mdoc) ตามมาตรฐาน ISO/IEC 18013-5 [13] เป็นรูปแบบหลักสำหรับการออกและสำแดงข้อมูล โดยไม่รองรับการใช้รูปแบบ SD-JWT VC สำหรับ mDL โดยตรง ทั้งนี้ ในกรณีของข้อมูลอัตลักษณ์พื้นฐาน (Person Identification Data: PID) อาจมีการออกเอกสาร

[11]POTENTIAL Large Scale Pilot, https://www.digital-identity-wallet.eu/use-case/mobile-driving-licence/

[12]APTITUDE LSP, https://aptitude.digital-identity-wallet.eu/

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

รับรองในหลายรูปแบบควบคู่กัน เช่น mdoc และ SD-JWT VC[14] เพื่อรองรับการใช้งานในบริบทที่หลากหลายและสอดคล้องกับระบบนิเวศดิจิทัลที่แตกต่างกัน

คุณสมบัติ	mdoc (ISO 18013-5)	SD-JWT VC
การเข้ารหัส	CBOR (RFC 8949)	JSON
ความปลอดภัย	COSE (RFC 9052)	JWS (RFC 7515)
Selective Disclosure	MSO salted hashes ในตัว	SD-JWT (RFC 9901)
การผูกอุปกรณ์	mdoc authentication	Key Binding JWT
รหัส DCQL	mso_mdoc	dc/sd-jwt
mDL ใน EUDIW	บังคับ (ใช้เฉพาะ mdoc)	ไม่บังคับสำหรับ mDL
PID ใน EUDIW	บังคับ	บังคับ
ใช้งานออฟไลน์	รองรับ	ไม่รองรับ

ตารางที่ 8 เปรียบเทียบ mdoc กับ SD-JWT VC

4.1.4 มาตรฐานที่เกี่ยวข้อง

การดำเนินงานของใบอนุญาตขับขี่อิเล็กทรอนิกส์ (mDL) ภายใต้กรอบของสหภาพยุโรปเกี่ยวข้องกับมาตรฐานหลายส่วนที่ทำงานร่วมกัน โดยในส่วนของการจัดเก็บและการแลกเปลี่ยนข้อมูลในระยะใกล้ (เช่น การแสดงผ่าน QR Code หรือการสื่อสารผ่าน NFC, Bluetooth Low Energy (BLE) และ Wi-Fi Aware) จะอ้างอิงมาตรฐาน ISO/IEC 18013-5 ซึ่งกำหนดรูปแบบ Mobile Document (mdoc) รวมถึงกลไกการเข้ารหัสระหว่างอุปกรณ์ (session encryption) เพื่อรักษาความปลอดภัยของข้อมูล

สำหรับการใช้งานผ่านช่องทางระยะไกล (Remote Presentation) จะอ้างอิงมาตรฐาน ISO/IEC 18013-7 ร่วมกับโปรโตคอล OpenID Connect for Verifiable Presentations (OID4VP) โดยผู้ตรวจสอบเอกสารสามารถร้องขอข้อมูลที่ต้องการผ่านกลไก เช่น Digital Credentials Query Language (DCQL) และผู้ถือเอกสารจะตอบกลับด้วยเอกสารสำแดงในรูปแบบที่กำหนดตามโปรโตคอล

ในส่วนของการออกเอกสารรับรอง (Issuance) สามารถใช้โปรโตคอล OpenID Connect for Verifiable Credential Issuance (OID4VCI v1.0[15]) เวอร์ชัน 1.0 เพื่อรองรับกระบวนการออกเอกสารรับรองในรูปแบบดิจิทัล โดยมาตรฐานต่าง ๆ เหล่านี้ทำงานร่วมกันเพื่อสนับสนุนการใช้งานทั้งในรูปแบบใกล้ตัวและระยะไกลอย่างครบวงจร

4.1.5 ซอฟต์แวร์โอเพนซอร์ส

ในบริบทของกระเป๋าอัตลักษณ์ดิจิทัลของสหภาพยุโรป (EUDI Wallet) คณะกรรมาธิการยุโรป (European Commission: EC[16]) ได้เผยแพร่ซอฟต์แวร์โอเพนซอร์สที่เกี่ยวข้องผ่านแพลตฟอร์ม GitHub เป็นจำนวนมาก โดยมีมากกว่า 70 โครงการ (repositories) ภายใต้สัญญาอนุญาตแบบเปิด เช่น Apache License 2.0 และ European Union Public Licence (EUPL) 1.2 เพื่อสนับสนุนการพัฒนา การทดสอบ และการนำไปใช้งานในประเทศสมาชิก

[14]IETF, "SD-JWT-based Verifiable Credentials (SD-JWT VC)", draft-ietf-oauth-sd-jwt-vc-15, 2025.

[15]OpenID Foundation, "OpenID for Verifiable Credential Issuance 1.0", September 2025.

[16]EU Digital Identity Wallet GitHub, https://github.com/eu-digital-identity-wallet — กว่า 76 repositories.

นอกจากนี้ ยังมีผู้ให้บริการภายนอก (Third-party Providers) ที่พัฒนาเครื่องมือและโซลูชันเพื่อรองรับการใช้งานในระบบนิเวศดังกล่าว เช่น walt.id[17], Sphereon[18], Authlete[19] และโครงการภายใต้ OWF[20] (React Native Wrapper) ซึ่งรวมถึงเครื่องมือสำหรับพัฒนาแอปพลิเคชันบนอุปกรณ์เคลื่อนที่ โดยองค์ประกอบเหล่านี้มีส่วนช่วยส่งเสริมให้เกิดการพัฒนาและการนำไปใช้งานในวงกว้างอย่างต่อเนื่อง

ส่วนประกอบ	Repository	ภาษา	หน้าที่
แอป Android	eudi-app-android-wallet-ui	Kotlin	กระเป๋าเอกสารดิจิทัล EUDI
แอป iOS	eudi-app-ios-wallet-ui	Swift	กระเป๋าเอกสารดิจิทัล EUDI
Core Android	eudi-lib-android-wallet-core	Kotlin	ไลบรารีหลักประสานงาน
OID4VCI Client	eudi-lib-jvm-openid4vci-kt	Kotlin	รับเอกสารรับรอง
OID4VP Client	eudi-lib-jvm-openid4vp-kt	Kotlin	สำแดงเอกสาร
ISO 18013-5	eudi-lib-android-iso18013-data-transfer	Kotlin	ถ่ายโอน mDL ใกล้ชิด
ผู้ออกเอกสาร (Kotlin)	eudi-srv-pid-issuer	Kotlin	ออก PID/mDL ผ่าน OID4VCI
ผู้ออกเอกสาร (Python)	eudi-srv-web-issuing-eudiw-py	Python	ออก PID/mDL/EAA
ผู้ตรวจสอบเอกสาร	eudi-srv-web-verifier-endpoint	Kotlin	ตรวจสอบ mDL ผ่าน OID4VP

ตารางที่ 9 Repositories หลักของ EUDI Wallet

[17]walt.id Identity Infrastructure, https://github.com/walt-id/waltid-identity

[18]Sphereon OID4VC Libraries, https://github.com/Sphereon-Opensource/OID4VC

[19]Authlete OID4VCI Demo, https://github.com/authlete/oid4vci-demo

[20]OpenWallet Foundation, eudi-wallet-kit-react-native.

4.2 แนวทางการใช้งานเอกสารรับรองและเอกสารสำแดงในประเทศและตัวอย่างการใช้งาน

การใช้งาน Verifiable Credentials (VC) และ Verifiable Presentations (VP) สำหรับ Transcript ในมหาวิทยาลัยไทยยังอยู่ในระยะวิจัยและนำร่อง (Pilot/PoC) โดยมีมหาวิทยาลัยมหิดลเป็นกรณีศึกษาหลักที่ทำวิจัยเชิงลึกเรื่อง VC Wallet สำหรับ Digital Transcript ร่วมกับสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) และบริษัท Finema รายงานนี้รวบรวมมาตรฐาน โปรโตคอล รูปแบบกระเป๋าเอกสารดิจิทัล และไลบรารีโอเพนซอร์สที่เกี่ยวข้อง รวมถึง Code implementation ที่สามารถนำไปใช้งานได้

4.2.1 สถานภาพปัจจุบัน

ปัจจุบันมหาวิทยาลัยในไทยกว่า 98 แห่งให้บริการ Digital Transcript แล้ว รวมถึงจุฬาลงกรณ์มหาวิทยาลัย มหาวิทยาลัยมหิดล มหาวิทยาลัยเชียงใหม่ มหาวิทยาลัยเกษตรศาสตร์ และมหาวิทยาลัยธรรมศาสตร์ อย่างไรก็ตาม Digital Transcript ที่ใช้งานอยู่ในปัจจุบันส่วนใหญ่ใช้เทคโนโลยี PKI (Public Key Infrastructure) พร้อม Digital Signature ในรูปแบบ PDF ซึ่งตรวจสอบผ่าน Adobe Acrobat Reader หรือเว็บไซต์ edocvalidation.digitalgov.go.th ไม่ใช่ W3C VC

มหาวิทยาลัยเชียงใหม่ (CMU) เป็นมหาวิทยาลัยแห่งแรกในไทยที่นำร่อง Digital Transcript ตั้งแต่ปี 2564 โดยใช้มาตรฐาน XML Schema ตาม ETDA Recommendation on "MESSAGE STANDARD FOR ACADEMIC TRANSCRIPT" แต่ยังไม่ใช่ VC ในรูปแบบ W3C

กรณีศึกษาหลัก: มหาวิทยาลัยมหิดล (Mahidol University)

ในงานวิจัย VC/VP สำหรับ Digital Transcript คณะเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) มหาวิทยาลัยมหิดล ภายใต้การดูแลของ อาจารย์ ดร. อิทธิพล รัศมีโรจน์ (Dr. Ittipon Rassameeroj) มีงานวิทยานิพนธ์ระดับปริญญาโท 2 เรื่องที่เกี่ยวข้องโดยตรง (สำเร็จการศึกษาปี 2024)

หัวข้อวิทยานิพนธ์	ผู้วิจัย	สาขา
Verifiable Credential Wallet for Digital Transcript	Tharathep (Fill) Klinla-or	M.S. in Computer Science
SSI for VC-Based Digital Transcript	Naphat (Third) Khajohn-udomrith	M.S. in Cyber Security

ตารางที่ 10 ตารางแสดงหัวข้อผลงาน

4.2.2 กลไกการตรวจสอบ Digital Signature ในไฟล์ PDF/A-3

ในทางปฏิบัติ หน่วยงานการศึกษาในประเทศไทยจำนวนหนึ่งใช้รูปแบบไฟล์ PDF/A-3 สำหรับการออกเอกสารรับรองดิจิทัล เช่น ใบรับรองหรือระเบียนผลการศึกษา โดยอาจมีการฝังข้อมูลเชิงโครงสร้างเพิ่มเติมในรูปแบบ XML และลงลายมือชื่อดิจิทัลตามมาตรฐาน PAdES ระดับ Long-Term Validation (PAdES-LTV) เพื่อรองรับการตรวจสอบในระยะยาว

โครงสร้างของเอกสารโดยทั่วไปประกอบด้วยองค์ประกอบหลัก ได้แก่ (1) ส่วนแสดงผล (Visual Layer) ในรูปแบบ PDF สำหรับการอ่านของผู้ใช้งาน (2) ส่วนข้อมูลที่ฝังภายใน (Embedded Data) เช่น XML Attachment ซึ่งใช้เก็บข้อมูลเชิงโครงสร้างของเอกสาร และ (3) ส่วนลายมือชื่อดิจิทัล (Signature Block) ซึ่งอาจรวมถึงใบรับรองดิจิทัล (X.509 Certificate) ข้อมูลสถานะใบรับรอง (เช่น CRL หรือ OCSP Response) และข้อมูลเวลาประทับ (Timestamp) เพื่อสนับสนุนการตรวจสอบในระยะยาว

ในกระบวนการตรวจสอบ ผู้ตรวจสอบเอกสารสามารถเปิดเอกสารด้วยโปรแกรมอ่าน PDF ที่รองรับ เช่น Adobe Acrobat Reader โดยระบบจะทำการตรวจสอบสายโซ่ใบรับรอง (Certificate Chain) ตั้งแต่ Root CA ไปยังใบรับรองของผู้ออกเอกสาร ตรวจสอบสถานะของใบรับรองว่าไม่ถูกเพิกถอน และตรวจสอบความถูกต้องของข้อมูล (Integrity) เพื่อยืนยันว่าเอกสารไม่ได้ถูกแก้ไขภายหลังการลงลายมือชื่อ

ทั้งนี้ แนวทางดังกล่าวอาศัยโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure: PKI) แบบดั้งเดิมเป็นหลัก และมีข้อจำกัดบางประการเมื่อเทียบกับแนวทาง Verifiable Credentials เช่น ไม่รองรับการเปิดเผยข้อมูลแบบเลือกได้ (Selective Disclosure) ไม่รองรับการสำแดงข้อมูลบางส่วน (Verifiable Presentation) และโดยทั่วไปต้องส่งเอกสารทั้งฉบับในการใช้งาน

4.2.3 บทบาทของ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ในการขับเคลื่อน W3C VC

สพธอ. ETDA ได้จัดทำ ขมธอ. 24-2563 (ETDA Recommendation 2020) เรื่อง "โครงสร้างข้อมูลของเอกสารรับรองและเอกสารสำแดง" (Data Structure of Verifiable Credentials and Presentations) ซึ่งอ้างอิงโดยตรงจาก W3C Verifiable Credentials Data Model ประกอบไปด้วยข้อกำหนดสำคัญ ๆ ดังนี้

- โครงสร้างข้อมูลในรูปแบบ JSON และ JSON-LD (JavaScript Object Notation for Linked Data)
- การใช้ @context โดย base context เป็น https://www.w3.org/2018/credentials/v1
- การใช้ DID (Decentralized Identifier) เป็น identifier ของเจ้าของข้อความ (subject)
- การใช้ Digital Signature ในรูปแบบ proof (เช่น RsaSignature2018)
- บทบาททั้ง 4 เอนทิตี: Issuer, Holder, Verifier และ Verifiable Data Registry

นอกจากนี้ สพธอ. ยังได้ออกออก Technical Report เรื่อง Interoperable Framework of Digital Wallets for Verifiable Credentials (เวอร์ชัน 1.0, เมษายน 2566) ซึ่งอ้างอิงจาก EUDI Wallet Architecture ของสหภาพยุโรป โดยแบ่งเอกสารรับรองเป็น 2 ประเภท:

- ประเภท 1 (ความเสี่ยงสูง เช่น บัตรประชาชน): ต้องรองรับมาตรฐานเข้มงวด
- ประเภท 2 (ความเสี่ยงต่ำ เช่น บัตรสะสมคะแนน, Transcript): มาตรฐานผ่อนปรนกว่า

องค์ประกอบ	มาตรฐาน/โปรโตคอล	ประเภท 1	ประเภท 2
โปรโตคอลออก VC	OID4VCI (OpenID for Verifiable Credential Issuance)	ต้อง	ต้อง
โปรโตคอลแสดง VP (Remote)	OID4VP (OpenID for Verifiable Presentations)	ต้อง	อาจ
Self-Issued OP	SIOPv2 (Self-Issued OpenID Provider v2)	ควร	ควร
โปรโตคอลแสดง VP (Proximity)	ISO/IEC 18013-5 (mDL)	ต้อง	อาจ
โครงสร้างข้อมูล	W3C VC Data Model v1.1	ต้อง	ควร
โครงสร้างข้อมูล	ISO/IEC 18013-5	ต้อง	ควร
รูปแบบ VC	JWT (JSON Web Token)	ต้อง	อาจ
Selective Disclosure	SD-JWT	ต้อง	อาจ
รูปแบบ VC	CBOR (Concise Binary Object Representation)	ต้อง	อาจ
รูปแบบ VC	JSON-LD with LD-Proof	อาจ	อาจ
Signature Format	JOSE (JSON Object Signing and Encryption)	ต้อง	อาจ
Signature Format	COSE (CBOR Object Signing and Encryption)	ต้อง	อาจ
Key Management	Secure Element / TEE / HSM	ต้อง	ควร

ตารางที่ 11 ตารางสรุปมาตรฐานและโปรโตคอลที่แนะนำ

ที่มา: ETDA Technical Report, เมษายน 2566[21]

4.2.4 กรอบอ้างอิงนานาชาติ

ในบริบทของการประยุกต์ใช้เอกสารรับรองดิจิทัลในภาคการศึกษา มีตัวอย่างการนำมาตรฐานสากลมาใช้งานในหลายประเทศและหลายแพลตฟอร์ม โดยในประเทศไทย สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง (สจล.) ได้มีการทดลองใช้มาตรฐาน W3C VC ร่วมกับ Open Badges 3.0 บนโครงข่าย Blockchain (เช่น Bitcoin Testnet) เพื่อรองรับการออกและตรวจสอบเอกสารรับรองดิจิทัล

ในระดับนานาชาติ โครงการ Digital Credentials Consortium (DCC) ซึ่งประกอบด้วยมหาวิทยาลัยชั้นนำ เช่น Massachusetts Institute of Technology (MIT) และเครือข่ายสถาบันการศึกษากว่า 16 แห่ง ได้พัฒนาแนวทางการใช้งานโดยอาศัยเทคโนโลยี เช่น did:web สำหรับตัวระบุแบบกระจายศูนย์ (Decentralized Identifier: DID), อัลกอริทึมลายมือชื่อดิจิทัลแบบ Ed25519 และกลไก Bitstring Status

[21] กรอบการทำงานร่วมกันของกระเป๋าดิจิทัลสำหรับเอกสารรับรอง https://www.etda.or.th/th/StandardNews/03042566.aspx

List สำหรับการตรวจสอบสถานะของเอกสารรับรอง รวมถึงมีการทดสอบการทำงานร่วมกันกับเครื่องมือสำหรับผู้ตรวจสอบเอกสาร เช่น VerifierPlus และ Learner Credential Wallet (LCW)

สำหรับสหภาพยุโรป แนวทางการพัฒนาในกรอบ European Blockchain Services Infrastructure (EBSI) ได้นำมาตรฐาน OpenID Connect for Verifiable Credential Issuance (OID4VCI) และ OpenID Connect for Verifiable Presentations (OID4VP) มาใช้ร่วมกับ DID ในรูปแบบ did:ebsi และ Open Badges 3.0 ซึ่งมีความสอดคล้องกับ W3C Verifiable Credentials Data Model เวอร์ชัน 2.0 เพื่อรองรับการใช้งานในระดับสหภาพยุโรป

ส่วนประกอบ	Repository	ภาษา	หน้าที่
ผู้ออกเอกสาร	issuer-coordinator	TypeScript	ประสานงานการออก VC
ลงนาม	sign-and-verify	TypeScript	ลงนาม/ตรวจสอบลายเซ็น
กระเป๋า	Learner Credential Wallet	React Native	แอปสำหรับผู้ถือเอกสาร
ตรวจสอบ	verifier-plus	TypeScript	ตรวจสอบ VC ผ่านเว็บ
LMS	lti-issuer	TypeScript	เชื่อมต่อระบบ LMS
ทะเบียน	community-registry	GitHub-based	รายชื่อผู้ออกเอกสารที่น่าเชื่อถือ

ตารางที่ 12 ซอฟต์แวร์โอเพนซอร์สของ DCC

4.2.5 ตัวอย่างโครงสร้างและชุดคำสั่ง

ตัวอย่างรหัสที่ 4.4 โครงสร้าง JSON-LD ของ VC ผลการเรียน (Open Badges 3.0)

```
{
 "@context": [
  "https://www.w3.org/ns/credentials/v2",
  "https://purl.imsglobal.org/spec/ob/v3p0/context-3.0.3.json"
 ],
 "type": ["VerifiableCredential", "OpenBadgeCredential"],
 "issuer": {
  "id": "did:web:reg.kmutt.ac.th",
  "name": "มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี"
 },
 "validFrom": "2026-03-01T00:00:00Z",
 "name": "ปริญญาวิศวกรรมศาสตรบัณฑิต",
 "credentialSubject": {
  "id": "did:key:z6Mk...",
  "type": "AchievementSubject",
  "achievement": {
   "name": "Bachelor of Engineering (Computer Engineering)",
   "description": "วิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมคอมพิวเตอร์"
  },
  "result": [
   { "type": "Result", "name": "GPA", "value": "3.45" },
   { "type": "Result", "name": "หน่วยกิตรวม", "value": "145" }
  ]
 }
}
```

ตัวอย่างรหัสที่ 4.5 เซิร์ฟเวอร์ออก VC ผลการเรียน (TypeScript)

```
// TypeScript — ออก VC ผลการเรียน ด้วย DCC Issuer Coordinator
import express from 'express';
import { issue } from '@digitalcredentials/vc';
import { Ed25519VerificationKey2020 }
  from '@digitalbazaar/ed25519-verification-key-2020';
import { Ed25519Signature2020 }
  from '@digitalbazaar/ed25519-signature-2020';
const app = express();
const keyPair = await Ed25519VerificationKey2020.generate();
keyPair.id = 'did:web:reg.kmutt.ac.th#key-1';
keyPair.controller = 'did:web:reg.kmutt.ac.th';
const suite = new Ed25519Signature2020({ key: keyPair });
app.post('/api/credentials/issue', async (req, res) => {
  const { studentDid, achievementData } = req.body;
  const credential = {
    '@context': ['https://www.w3.org/ns/credentials/v2',
      'https://purl.imsglobal.org/spec/ob/v3p0/context-3.0.3.json'],
    type: ['VerifiableCredential', 'OpenBadgeCredential'],
    issuer: { id: 'did:web:reg.kmutt.ac.th',
      name: 'มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี' },
    validFrom: new Date().toISOString(),
    credentialSubject: {
      id: studentDid, type: 'AchievementSubject',
      achievement: achievementData }
  };
  const signed = await issue({ credential, suite, documentLoader });
  res.json({ verifiableCredential: signed });
});
```

คำแนะนำสำหรับนักพัฒนา: นักพัฒนาสามารถดึงชุดคำสั่ง หรือซอร์สโคด ได้จาก issuer-coordinator ของ DCC จาก GitHub ซึ่งสามารถติดตั้งด้วย Docker Compose ทดสอบด้วย VerifierPlus

4.2.6 ช่องว่างทางมาตรฐาน

มาตรฐาน/โปรโตคอล	สถานะในไทย	แนวปฏิบัติสากล
W3C VC Data Model 2.0	สพธอ. พัฒนา, สจล. วิจัย	ใช้จริง (DCC, EBSI)
DID (did:web, did:key)	ยังไม่ใช้งาน	DCC ใช้ did:web และ did:key
SD-JWT	ยังไม่ใช้งาน	EUDI Wallet บังคับ
OID4VCI / OID4VP	ยังไม่ใช้งาน	EBSI + EUDI บังคับ
Open Badges 3.0	ยังไม่ใช้งาน	DCC, 1EdTech แพร่หลาย

ตารางที่ 13 เปรียบเทียบสถานะมาตรฐาน VC การศึกษาระหว่างไทยและสากล

ภาคผนวก

ตัวอย่างชุดคำสั่งในการประยุกต์ใช้ VC/VP จากต่างประเทศ

ตัวอย่างชุดคำสั่งของ Credential Endpoint ออก mDL (Kotlin)

```
// Kotlin — Credential Endpoint ออก mDL ผ่าน OID4VCI
// อ้างอิง: eudi-srv-pid-issuer (Spring Boot 3)
@RestController
@RequestMapping("/credential")
class MdlCredentialEndpoint(private val mdlIssuer: MdlIssuer) {
    @PostMapping
    suspend fun issueCredential(
        @RequestHeader("Authorization") token: String,
        @RequestBody request: CredentialRequest
    ): CredentialResponse {
        val accessToken = validateAccessToken(token)
        val holderKey = verifyProofOfPossession(request.proof)
        return when (request.format) {
            "mso_mdoc" -> {
                val mdoc = mdlIssuer.issueMdoc(
                    docType = "org.iso.18013.5.1.mDL",
                    nameSpace = "org.iso.18013.5.1",
                    claims = buildMdlClaims(accessToken),
                    deviceKey = holderKey)
                CredentialResponse("mso_mdoc", mdoc.toCBOR().toBase64Url())
            }
            "vc+sd-jwt" -> {
                val sdJwt = mdlIssuer.issueSdJwtVc(
                    vct = "urn:eu.europa.ec.eudi:mdl:1",
                    claims = buildMdlClaims(accessToken),
                    holderKey = holderKey,
                    disclosureFrame = listOf(
                        "family_name","given_name","birth_date","portrait"))
                CredentialResponse("vc+sd-jwt", sdJwt)
            }
            else -> throw UnsupportedFormatException()
        }
    }
}
```

ตัวอย่างชุดคำสั่งของ Verifier ร้องขอ mDL ผ่าน OID4VP (Kotlin)

```
// Kotlin — Verifier ร้องขอ mDL ผ่าน OID4VP + DCQL
@RestController
@RequestMapping("/api/verify")
class VerifierEndpoint(private val oid4vp: OID4VPService) {
    @PostMapping("/request")
    fun createRequest(): AuthorizationRequest {
        val dcql = DcqlQuery(credentials = listOf(
            DcqlCredential(id = "mdl_check",
                format = "mso_mdoc",
                meta = mapOf("doctype_value" to "org.iso.18013.5.1.mDL"),
                claims = listOf(
                    DcqlClaim("org.iso.18013.5.1","family_name"),
                    DcqlClaim("org.iso.18013.5.1","driving_privileges"),
                    DcqlClaim("org.iso.18013.5.1","portrait")))))
        return oid4vp.createAuthorizationRequest(
            responseType="vp_token", responseMode="direct_post",
            dcqlQuery=dcql, nonce=generateNonce())
    }
    @PostMapping("/response")
    fun verifyResponse(@RequestParam("vp_token") vp: String) =
        oid4vp.verify(vp)
}
```

โดยสามาถเข้าไปลองทดลองใช้งานของกรณีศึกษาของต่างประเทศ ซึ่งทำเป็นลักษณะสภาพแวดล้อมทดสอบ ตามตารางด้านล่างนี้

รายการลิงค์ของเว็บไซต์ข้อมูลและทดลองใช้ของระบบเอกสารรับรอง และเอกสารสำแดงของยุโรป: Issuer[22] และ Verifier[23] ของ EC หรือติดตั้ง Docker เอง เยอรมนีเปิด National Sandbox[24]

[22]EUDI Reference Issuer Demo, https://issuer.eudiw.dev/

[23]EUDI Reference Verifier Demo, https://verifier.eudiw.dev/

[24]Germany EUDI Wallet Sandbox, January 2026.

สภาพแวดล้อม	URL	คำอธิบาย
EC Issuer Demo	https://issuer.eudiw.dev/	ออก PID/mDL ทั้ง mdoc, SD-JWT
EC Verifier Demo	https://verifier.eudiw.dev/	ตรวจสอบ PID/mDL ผ่าน OID4VP
walt.id Wallet	https://wallet.demo.walt.id/	กระเป๋าเอกสารดิจิทัลเว็บ
VerifierPlus (DCC)	https://verifierplus.org/	ตรวจสอบ VC การศึกษา
DCC Badge Demo	https://badging.dcconsortium.org/	ทดลองออก Open Badge
Authlete OID4VCI	github.com/authlete/oid4vci-demo	ตัวอย่าง OID4VCI
Sphereon OID4VC	github.com/Sphereon-Opensource/OID4VC	OID4VCI และ VP (TypeScript)
Germany Sandbox	SPRIND National Sandbox	Sandbox เยอรมนี (ม.ค. 2569)

ตารางที่ 14 สภาพแวดล้อมทดสอบ

คำแนะนำสำหรับนักพัฒนา: เริ่มจาก issuer.eudiw.dev และ verifier.eudiw.dev ไม่ต้องติดตั้งโปรแกรม จากนั้นดาวน์โหลด EUDI Reference Wallet จาก GitHub Releases ทดสอบบนโทรศัพท์เคลื่อนที่จริง

ตัวอย่างชุดคำสั่ง (source code) ที่ปรากฏในเอกสารฉบับนี้ จัดทำขึ้นเพื่อแสดงแนวทางการพัฒนา ณ เวลาที่จัดทำเอกสาร ซึ่งเทคโนโลยี ไลบรารี และข้อกำหนดของมาตรฐานที่เกี่ยวข้องอาจมีการปรับปรุงเปลี่ยนแปลงได้ในภายหลัง เพื่อให้ผู้พัฒนาสามารถเข้าถึงตัวอย่างชุดคำสั่งฉบับล่าสุดที่ได้รับการปรับปรุงให้ทันสมัยอยู่เสมอ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) จึงจัดให้มีแหล่งรวมตัวอย่างชุดคำสั่ง (source code repository) ไว้ที่ https://standard.dga.or.th/34515/ ทั้งนี้ การแยกตัวอย่างชุดคำสั่งไว้ที่แหล่งภายนอกช่วยให้การปรับปรุงชุดคำสั่งในอนาคตดำเนินการได้โดยสะดวก

บรรณานุกรม

[1] ราชกิจจานุเบกษา. (2562). พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562. เล่ม 136 ตอนที่ 67 ก. วันที่ 22 พฤษภาคม 2562.

[2] ราชกิจจานุเบกษา. (2565). พระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. 2565. เล่ม 139 ตอนที่ 47 ก. วันที่ 12 ตุลาคม 2565.

[3] ราชกิจจานุเบกษา. (2544). พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544. เล่ม 118 ตอนที่ 112 ก. วันที่ 4 ธันวาคม 2544.

[4] ราชกิจจานุเบกษา. (2562). พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. เล่ม 136 ตอนที่ 69 ก. วันที่ 27 พฤษภาคม 2562.

[5] ราชกิจจานุเบกษา. (2562). ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานและหลักเกณฑ์การเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล ว่าด้วยเรื่อง กรอบแนวทางการพัฒนามาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ วันที่ 12 กันยายน พ.ศ. 2565

[6] มาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านความหมายข้อมูล เรื่องข้อมูลบุคคล (มสพร. 4-2565) และเรื่องข้อมูลนิติบุคคล (มสพร.5-2565) วันที่ 18 เมษายน พ.ศ. 2565

[7] มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐด้านความหมายข้อมูล เรื่องข้อมูลสถานที่-ที่อยู่ (มสพร. 9-1:2566) 14 มีนาคม พ.ศ. 2566

[8] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA). (2563). ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยโครงสร้างข้อมูลของเอกสารรับรองและเอกสารสำแดง (ขมธอ. 24-2563) สืบค้นจาก https://www.etda.or.th/getattachment/bafad651-864a-4f01-86ab-a2f39239d400/ขมธอ-24-2563.aspx ,เมื่อวันที่ 5 มีนาคม พ.ศ. 2569

[9] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA). (2566). รายงานทางเทคนิค เรื่อง กรอบการทำงานร่วมกันของกระเป๋าดิจิทัลสำหรับเอกสารรับรอง พ.ศ. 2566 สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ สืบค้นจาก https://www.etda.or.th/getattachment/newsevents/pr-news/news-standard/ประกาศขอเสนอแนะมาตรฐานฯ-วาดวยการพสจนและยนยนตวตนทาง/20230403_TR-Digital-Wallet_V01-10F.pdf.aspx ,เมื่อวันที่ 5 มีนาคม พ.ศ. 2569

[10] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA). (2568). รายงานทางเทคนิค เรื่อง กรอบแนวทางการทำงานร่วมกันของเอกสารรับรองดิจิทัลสำหรับประเทศไทย พ.ศ. 2568 สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ สืบค้นจาก https://www.etda.or.th/getattachment/Our-Service/Digital-Trusted-services-Infrastructure/VC-and-Digital-Document-Wallet/Technique-Report/รายงานทางเทคนค-Thai-VC-ARF-v1-1-(2).pdf.aspx ,เมื่อวันที่ 5 มีนาคม พ.ศ. 2569

[11] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA). (2568). รายงานทางเทคนิค เรื่อง กรอบการสร้างความน่าเชื่อถือของเอกสารรับรองและเอกสารสำแดง พ.ศ. 2568 สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ สืบค้นจาก https://www.etda.or.th/getattachment/Our-Service/Digital-Trusted-services-Infrastructure/VC-and-Digital-Document-Wallet/Technique-Report/รายงานทางเทคนค-VCGF-VCGF-v1-3.pdf.aspx ,เมื่อวันที่ 5 มีนาคม พ.ศ. 2569

[12] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA). (2567). Verifiable Credentials Data Model 2.0 และการประยุกต์ใช้กับ Digital Document Wallet. สืบค้นจาก https://www.etda.or.th/th/pr-news/VC-and-Digital-Document-Wallet/vd_model2.aspx, เมื่อวันที่ 5 มีนาคม 2569

[13] European Commission. (2023). Architecture and Reference Framework for the European Digital Identity Wallet (ARF), สืบค้นจาก https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework, เมื่อวันที่ 5 มีนาคม 2569

[14] European Commission. (2023). eIDAS 2.0 Regulation and European Digital Identity Framework, สืบค้นจาก https://www.european-digital-identity-regulation.com/

[15] Government of Singapore. (2022). Digital Service Standards (DSS). Retrieved February 13, 2026, สืบค้นจาก https://www.tech.gov.sg/products-and-services/for-government-agencies/digital-service-standards/, เมื่อวันที่ 5 มีนาคม 2569

[16] IETF. (2015). RFC 7515: JSON Web Signature (JWS). Internet Engineering Task Force. สืบค้นจาก https://www.rfc-editor.org/rfc/rfc7515.html, เมื่อวันที่ 5 มีนาคม 2569

[17] IETF. (2012). RFC 6749: The OAuth 2.0 Authorization Framework. Internet Engineering Task Force. สืบค้นจาก https://datatracker.ietf.org/doc/html/rfc6749, เมื่อวันที่ 5 มีนาคม 2569

[18] OpenID Foundation. (2023). OpenID for Verifiable Credential Issuance (OpenID4VCI), สืบค้นจาก https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html, เมื่อวันที่ 5 มีนาคม 2569

[19] OpenID Foundation. (2023). OpenID for Verifiable Presentations (OpenID4VP), สืบค้นจาก https://openid.net/specs/openid-4-verifiable-presentations-1_0.html, เมื่อวันที่ 5 มีนาคม 2569

[20] OpenID Foundation. (2014). OpenID Connect Core 1.0, สืบค้นจาก https://openid.net/specs/openid-connect-core-1_0-final.html, เมื่อวันที่ 5 มีนาคม 2569

[21] W3C. (2022). Decentralized Identifiers (DID) v1.0. World Wide Web Consortium, สืบค้นจาก https://www.w3.org/TR/did-1.0/, เมื่อวันที่ 5 มีนาคม 2569

[22] The Trust Over IP (ToIP) Foundation. (2021). Trust over IP ,สืบค้นจาก https://trustoverip.org/about/about/ ,เมื่อวันที่ 5 มีนาคม 2569