ประกาศสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ที่ ม ๕/๒๕๖๙

เรื่อง มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ว่าด้วยแนวปฏิบัติกระบวนการทางดิจิทัลภาครัฐ - ส่วนที่ ๘ เรื่อง เอกสารใบอนุญาตอิเล็กทรอนิกส์ภาครัฐ
ในรูปแบบเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล

.....

ด้วยสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ได้ให้ความสำคัญกับการสนับสนุนการดำเนินการของหน่วยงานของรัฐในการบริหารราชการแผ่นดินและการให้บริการประชาชนผ่านระบบดิจิทัล เพื่อให้กระบวนการหรือการดำเนินงานทางดิจิทัลมีประสิทธิภาพและสามารถทำงานร่วมกันได้ตามมาตรฐาน ข้อกำหนด และหลักเกณฑ์ที่คณะกรรมการพัฒนารัฐบาลดิจิทัลกำหนด เพื่อให้มีความสอดคล้องและเชื่อมโยงระหว่างหน่วยงานของรัฐอื่นได้ ตามมาตรา ๑๒ (๒) แห่งพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ และเพื่อเป็นการสนับสนุนการจัดทำวิธีการทางอิเล็กทรอนิกส์ ตามมาตรา ๑๙ แห่งพระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๕

อาศัยอำนาจตามความในมาตรา ๘ (๒) มาตรา ๒๙ และมาตรา ๓๐ แห่งพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) พ.ศ. ๒๕๖๑ จึงออกประกาศ เรื่อง มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยแนวปฏิบัติกระบวนการทางดิจิทัลภาครัฐ - ส่วนที่ ๘ เรื่อง เอกสารใบอนุญาตอิเล็กทรอนิกส์ภาครัฐในรูปแบบเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัลฉบับนี้ เพื่อยึดถือเป็นแนวปฏิบัติในการดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) และเป็นข้อเสนอแนะสำหรับหน่วยงานของรัฐต่อไป โดยมีรายละเอียดปรากฏตามเอกสารแนบท้ายประกาศนี้

จึงประกาศให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่ ๑๐ กันยายน พ.ศ.๒๕๖๙

(นางไอรดา เหลืองวิไล)
รองผู้อำนวยการ รักษาการแทน
ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

DGA Community Standard

มสพร. 6-8 : 2569

DGA 6-8 : 2569

ว่าด้วยแนวปฏิบัติกระบวนการทางดิจิทัลภาครัฐ - ส่วนที่ 8
เรื่อง เอกสารใบอนุญาตอิเล็กทรอนิกส์ภาครัฐ
ในรูปแบบเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล

GUIDELINES FOR DIGITAL GOVERNMENT PROCESS – PART 8
VERIFIABLE CREDENTIALS AND PRESENTATIONS
LICENSE DOCUMENT

เวอร์ชัน 1.0

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ว่าด้วยแนวปฏิบัติกระบวนการทางดิจิทัลภาครัฐ - ส่วนที่ 8 เรื่อง เอกสารใบอนุญาตอิเล็กทรอนิกส์ภาครัฐในรูปแบบเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล

มสพร. 6-8 : 2569

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
เลขที่ 120 อาคารศูนย์ราชการเฉลิมพระเกียรติฯ (อาคารซี) ชั้น 8 – 9
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210
หมายเลขโทรศัพท์: (+66) 0 2612 6000 โทรสาร: (+66) 0 2612 601

ประกาศโดย
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
กันยายน 2569

คณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์
ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

ที่ปรึกษา

นางไอรดา เหลืองวิไล	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

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)

คณะทำงานเทคนิคด้านมาตรฐานกระบวนการและการดำเนินงานทางดิจิทัล

ที่ปรึกษา

นางไอรดา เหลืองวิไล	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูไพโรจน์	จุฬาลงกรณ์มหาวิทยาลัย
นายอาศิส อัญญะโพธิ์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ประธานคณะทำงาน

รองศาสตราจารย์เกริก ภิรมย์โสภา	จุฬาลงกรณ์มหาวิทยาลัย

รองประธานคณะทำงาน

ผู้ช่วยศาสตราจารย์กุลวดี ศรีพานิชกุลชัย	จุฬาลงกรณ์มหาวิทยาลัย

คณะทำงาน

นายสุภณ สยามบุญนัญ	กรมการปกครอง
นางวัลภา นุตโร	กรมบัญชีกลาง
นางสาวพณิชา เกื้อประจง	กรมพัฒนาธุรกิจการค้า
นายกำชัย จัตตานนท์	กรมศุลกากร
นางฤชาภร แบร์โรวส์	กรมสรรพากร
นายทรงวุฒิ โชติกาญจนวิทย	กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
นางสาวดารารัตน์ โฆษิตพิพัฒน์	สำนักงานคณะกรรมการพัฒนาระบบราชการ
พ.ต.ท.วรกร ทองสุข	สำนักงานตรวจคนเข้าเมือง
พล.อ.ต.จเด็ด คูหะก้องกิจ	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
นายชาลี วรกุลพิพัฒน์	ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
นางสาวขนิษฐ์ ผาทอง	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายเมธวิน กิติคุณ	สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย
นายคฑาวุธ ปาระมี	สมาคมไทยบล็อกเชน
นายอธิบดี ลิมสัมพันธ์สันติ	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นายอุสรา วิสารทานนท์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะทำงานและเลขานุการ

นางสาวอุรัชฎา เกตุพรหม	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ผู้ช่วยเลขานุการ

นายธีรวัฒน์ โรจนไพฑูรย์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

วิเคราะห์และจัดทำมาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยแนวปฏิบัติกระบวนการทางดิจิทัลภาครัฐ - ส่วนที่ 8 เรื่อง เอกสารใบอนุญาตอิเล็กทรอนิกส์ภาครัฐในรูปแบบเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

นายธีรวัฒน์ โรจนไพฑูรย์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นายธนัตถ์ โอมพรนุวัฒน์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นางสาวพิมพ์ชนก เจ็กภู่	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยแนวปฏิบัติกระบวนการทางดิจิทัลภาครัฐ - ส่วนที่ 8 เรื่อง เอกสารใบอนุญาตอิเล็กทรอนิกส์ภาครัฐในรูปแบบเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล เพื่อสร้างความเข้าใจที่ชัดเจน และกำหนดแนวทางในการพัฒนากระบวนการออกใบอนุญาตอิเล็กทรอนิกส์ของหน่วยงานภาครัฐ ให้สามารถตรวจสอบและแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ได้อย่างน่าเชื่อถือ มีความมั่นคงปลอดภัย และตรวจสอบได้ ตามหลักการของเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล โดยมาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยแนวปฏิบัติกระบวนการทางดิจิทัลภาครัฐ - ส่วนที่ 8 เรื่อง เอกสารใบอนุญาตอิเล็กทรอนิกส์ภาครัฐในรูปแบบเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล ฉบับนี้ได้จัดทำตามมาตรฐานและแนวทางแห่ง

1. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562
2. พระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. 2565

และได้มีการจัดงานประชาพิจารณ์เพื่อเปิดรับฟังความคิดเห็นเป็นการทั่วไป และนำข้อมูล ข้อสังเกต ข้อคิดเห็นจากผู้ทรงคุณวุฒิและจากหน่วยงานที่เกี่ยวข้อง เพื่อให้ข้อเสนอแนะเกี่ยวกับมาตรฐานฉบับนี้มีความสมบูรณ์ครบถ้วน และสามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพ

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยแนวปฏิบัติกระบวนการทางดิจิทัลภาครัฐ - ส่วนที่ 8 เรื่อง เอกสารใบอนุญาตอิเล็กทรอนิกส์ภาครัฐในรูปแบบเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล ฉบับนี้ จัดทำโดยฝ่ายมาตรฐานดิจิทัลภาครัฐ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
เลขที่ 120 อาคารศูนย์ราชการเฉลิมพระเกียรติฯ (อาคารซี)
ชั้น 8 – 9 หมู่ 3 ซอยแจ้งวัฒนะ 7 ถนนแจ้งวัฒนะ
แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210
หมายเลขโทรศัพท์: (+66) 0 2612 6000
E-mail: sd-g1_division@dga.or.th
Website: www.dga.or.th

คำนำ

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยแนวปฏิบัติกระบวนการทางดิจิทัลภาครัฐ – ส่วนที่ 8 เรื่องเอกสารใบอนุญาตอิเล็กทรอนิกส์ภาครัฐในรูปแบบเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล จัดทำขึ้นเพื่อสนับสนุนการดำเนินงานของหน่วยงานของรัฐให้เป็นไปตามพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 และพระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. 2565 รวมถึงมาตรฐานและแนวปฏิบัติที่เกี่ยวข้อง

เอกสารฉบับนี้มีวัตถุประสงค์เพื่อสร้างความเข้าใจที่ชัดเจน และกำหนดแนวทางในการพัฒนากระบวนการออกใบอนุญาตอิเล็กทรอนิกส์ของหน่วยงานภาครัฐ ให้สามารถตรวจสอบและแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ได้อย่างน่าเชื่อถือ มีความมั่นคงปลอดภัย และตรวจสอบย้อนกลับได้ ตามหลักการของเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล

นอกจากนี้ ยังมุ่งส่งเสริมให้หน่วยงานของรัฐนำรูปแบบเอกสารดังกล่าวไปประยุกต์ใช้จริง เพื่อเพิ่มประสิทธิภาพในการให้บริการและเสริมสร้างความน่าเชื่อถือของข้อมูลภาครัฐ ขณะเดียวกัน ประชาชนและผู้ประกอบการสามารถใช้ใบอนุญาตอิเล็กทรอนิกส์ได้อย่างสะดวก ปลอดภัย คุ้มครองความเป็นส่วนตัว และลดภาระในการติดต่อกับหน่วยงานของรัฐ และยังได้รวบรวมหลักการ แนวคิด ข้อเสนอแนะเชิงปฏิบัติ และตัวอย่างกรณีศึกษา เพื่อเป็นแนวทางให้หน่วยงานของรัฐสามารถนำไปปรับใช้ให้เหมาะสมกับบริบทของตนเอง โดยอ้างอิงกรอบแนวทางและมาตรฐานทางเทคนิคที่สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์กำหนด เพื่อให้การพัฒนาระบบมีความสอดคล้อง เชื่อมโยงกันได้ และรองรับการใช้งานในระดับประเทศอย่างเป็นระบบ

สารบัญ

คำนำ.....(7)
สารบัญ.....(8)
สารบัญตาราง.....(9)
สารบัญภาพ.....(10)
1. บทนำ.....1
1.1 ความเป็นมา.....1
1.2 วัตถุประสงค์.....2
1.3 ขอบข่าย.....2
1.4 บทนิยาม.....3
1.5 กฎหมายและแนวทางที่เกี่ยวข้อง.....4
2. กรอบแนวคิดและมาตรฐานสำหรับเอกสารรับรองดิจิทัล VC/VP.....5
2.1 แนวคิดหลักในการประยุกต์ใช้ VC/VP.....6
2.2 กรอบแนวทางด้านเอกสารรับรองดิจิทัลที่ประกาศโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์.....11
2.3 มาตรฐานที่เกี่ยวข้อง.....17
2.4 แนวทางการนำมาตรฐานสู่การดำเนินการของหน่วยงานของรัฐ.....19
3. แนวทางการดำเนินการสำหรับหน่วยงานของรัฐในการประยุกต์ใช้ VC/VP.....22
3.1 ปัญหาและข้อจำกัดของเอกสารอิเล็กทรอนิกส์แบบเดิม.....22
3.2 การเลือกเอกสารสำหรับการประยุกต์ใช้ในรูปแบบ VC/VP.....23
3.3 โครงสร้างบทบาท.....25
3.4 การวิเคราะห์ช่องว่าง (Gap Analysis).....28
3.5 การออกแบบและพัฒนากระบวนการตามมาตรฐาน (Design and Development).....31
3.6 ความพร้อมและการนำไปใช้งาน (Operational Readiness and Deployment).....33
3.7 การตรวจสอบและการประเมินความสอดคล้อง.....35
4. กรณีศึกษา.....37
4.1 กรณีศึกษาต่างประเทศ.....37
4.2 กรณีศึกษาในประเทศไทย.....42
บรรณานุกรม.....49

สารบัญตาราง

ตารางที่ 1 ตัวอย่างการกำหนดความรับผิดชอบของหน่วยงานของรัฐในการประยุกต์ใช้ VC/VP..... 27

สารบัญภาพ

ภาพที่ 1 ภาพรวมการใช้งานของเอกสารรับรองดิจิทัล.....5
ภาพที่ 2 บทบาทและการไหลของข้อมูลภายใต้มาตรฐาน W3C Verifiable Credentials Data Model.....6
ภาพที่ 3 องค์ประกอบภายใต้ระบบนิเวศเอกสารรับรองดิจิทัล 9
ภาพที่ 4 กระบวนการทำงานของระบบนิเวศเอกสารรับรองดิจิทัล 11
ภาพที่ 5 ตัวอย่างโครงสร้างข้อมูล VC/VP.....13
ภาพที่ 6 สถาปัตยกรรมซอฟต์แวร์ของกระเป๋าดิจิทัล.....14
ภาพที่ 7 บทบาทของผู้ที่เกี่ยวข้องกับการใช้งานเอกสารรับรองดิจิทัล.....15
ภาพที่ 8 กรอบแนวทางการสร้างความน่าเชื่อถือสำหรับระบบนิเวศเอกสารรับรอง (VC Trust Model Framework) อ้างอิงกรอบความน่าเชื่อถือของระบบนิเวศดิจิทัลโดย ToIP 16

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยแนวปฏิบัติกระบวนการทางดิจิทัลภาครัฐ - ส่วนที่ 8 เรื่อง เอกสารใบอนุญาตอิเล็กทรอนิกส์ภาครัฐในรูปแบบเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล

1. บทนำ

1.1 ความเป็นมา

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ได้จัดทำมาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัลว่าด้วยแนวปฏิบัติกระบวนการทางดิจิทัลภาครัฐ เพื่อเป็นแนวทางให้หน่วยงานของรัฐสามารถนำไปประยุกต์ใช้ในการพัฒนากระบวนการทำงานและการให้บริการในรูปแบบดิจิทัลได้อย่างเป็นระบบ โดยมาตรฐานดังกล่าวได้กำหนดแนวทางเป็นลำดับขั้น ตั้งแต่ส่วนที่ 1 ถึง 7 ครอบคลุมภาพรวมการจัดทำกระบวนการทางดิจิทัลสำหรับการ “ขออนุญาต” และรวบรวมมาตรฐานสำหรับใช้ศึกษาอ้างอิง รวมถึงวิธีการทางอิเล็กทรอนิกส์สำหรับหน่วยงานที่มีความพร้อมระดับเริ่มต้นและระดับมาตรฐาน ตลอดจนหลักเกณฑ์การประเมินระดับวิธีการทางอิเล็กทรอนิกส์ของหน่วยงานและวิธีการที่เหมาะสมสำหรับหน่วยงาน นอกจากนี้ ยังเพิ่มเติมในส่วนของการรับและจ่ายเงินด้วยวิธีการทางอิเล็กทรอนิกส์ และการจัดทำเอกสารใบอนุญาตอิเล็กทรอนิกส์ในรูปแบบเอกสารดิจิทัลที่มีการลงลายมือชื่ออิเล็กทรอนิกส์

อย่างไรก็ตาม แนวทางในส่วนที่ 7 ซึ่งเป็นการจัดทำเอกสารใบอนุญาตอิเล็กทรอนิกส์ในรูปแบบไฟล์เอกสาร (เช่น PDF) ที่มีการลงลายมือชื่ออิเล็กทรอนิกส์นั้น แม้จะช่วยให้เอกสารมีความน่าเชื่อถือในระดับหนึ่ง แต่ยังคงมีข้อจำกัดในด้านการตรวจสอบแบบอัตโนมัติ การใช้งานข้ามหน่วยงาน และการควบคุมการเปิดเผยข้อมูลตามความจำเป็น ดังนั้น มาตรฐานในส่วนที่ 8 นี้จึงถูกพัฒนาขึ้นเพื่อเป็นแนวทางในระดับที่สูงขึ้นของวิธีการทางอิเล็กทรอนิกส์ โดยมุ่งเน้นการออกเอกสารในรูปแบบที่สามารถตรวจสอบได้ และรองรับการใช้งานในลักษณะดิจิทัลอย่างเต็มรูปแบบผ่านเทคโนโลยี Verifiable Credentials : VC

ดังนั้น การยกระดับใบอนุญาตอิเล็กทรอนิกส์ภาครัฐไปสู่รูปแบบเอกสารรับรองดิจิทัล (Verifiable Credentials : VC) และเอกสารสำแดงดิจิทัล (Verifiable Presentations : VP) จึงมีความจำเป็น โดยเฉพาะสำหรับหน่วยงานของรัฐที่มีความพร้อมในระดับสูง เพื่อเพิ่มประสิทธิภาพในการให้บริการ และรองรับการตรวจสอบข้อมูลในรูปแบบดิจิทัลอย่างเป็นระบบ อีกทั้งยังช่วยให้สามารถใช้งานและตรวจสอบใบอนุญาตได้อย่างมีประสิทธิภาพระหว่างหน่วยงานภาครัฐและภาคเอกชน โดยลดข้อจำกัดของการพึ่งพาระบบของหน่วยงานผู้ออกและสนับสนุนการแลกเปลี่ยนข้อมูลในลักษณะที่ปลอดภัยและควบคุมได้

1.2 วัตถุประสงค์

1) เพื่อสร้างความเข้าใจเกี่ยวกับแนวคิดและหลักการของเอกสารรับรองดิจิทัล (Verifiable Credentials: VC) และเอกสารสำแดงดิจิทัล (Verifiable Presentations: VP) ในบริบทของการออกใบอนุญาตภาครัฐ
2) เพื่ออธิบายกรอบแนวทาง มาตรฐาน และโครงสร้างพื้นฐานด้านความน่าเชื่อถือที่เกี่ยวข้องในประเทศไทย เพื่อให้หน่วยงานของรัฐสามารถเข้าใจบริบทและข้อกำหนดที่เกี่ยวข้องได้อย่างเป็นระบบ
3) เพื่ออธิบายบทบาท หน้าที่ และความรับผิดชอบของผู้เกี่ยวข้องในระบบนิเวศของเอกสารรับรองดิจิทัล เพื่อให้หน่วยงานของรัฐสามารถมองเห็นภาพรวมของกระบวนการและความเชื่อมโยงระหว่างหน่วยงานได้อย่างชัดเจน
4) เพื่อเป็นข้อเสนอแนะแนวทางสำหรับหน่วยงานของรัฐในการปรับกระบวนการเดิมสู่การใช้งาน VC และ VP โดยคำนึงถึงโครงสร้างพื้นฐานด้านความน่าเชื่อถือ กลไกการตรวจสอบ และการทำงานร่วมกันระหว่างหน่วยงาน
5) เพื่อเป็นกรอบแนวคิดสำหรับการเตรียมความพร้อมและการนำไปใช้งานจริง โดยเฉพาะสำหรับหน่วยงานของรัฐที่มีระดับความพร้อมด้านดิจิทัลในระดับสูง ให้สามารถออกและให้บริการใบอนุญาตในรูปแบบดิจิทัลที่ตรวจสอบได้อย่างมั่นคงปลอดภัย

1.3 ขอบข่าย

เอกสารฉบับนี้จัดทำขึ้นเพื่อเสนอแนวทางและแนวปฏิบัติสำหรับหน่วยงานของรัฐในการพัฒนาและนำเอกสารในรูปแบบเอกสาร VC/VP ไปใช้ในบริบทของบริการภาครัฐ โดยครอบคลุมทั้งการอธิบายกรอบแนวทาง มาตรฐาน และโครงสร้างพื้นฐานด้านความน่าเชื่อถือที่เกี่ยวข้องในประเทศไทย รวมถึงแนวทางเชิงกระบวนการสำหรับการดำเนินงานของหน่วยงานที่เกี่ยวข้องในระบบนิเวศของ VC เพื่อสนับสนุนให้หน่วยงานของรัฐสามารถนำกรอบแนวทางที่มีอยู่มาประยุกต์ใช้ได้อย่างเหมาะสม โดยขอบข่ายของเอกสารครอบคลุมประเด็นสำคัญ ได้แก่

- กรอบแนวทาง มาตรฐาน และโครงสร้างพื้นฐานด้านความน่าเชื่อถือที่เกี่ยวข้องกับ VC/VP ในประเทศไทย
- บทบาทและความรับผิดชอบของหน่วยงานที่เกี่ยวข้องในระบบ VC/VP
- แนวทางสำหรับหน่วยงานของรัฐในการพัฒนาและปรับกระบวนการสู่การใช้งาน VC/VP
- แนวทางการเตรียมความพร้อม การทดสอบ และการนำระบบไปใช้งานจริง
- แนวทางการตรวจสอบและประเมินความพร้อมของระบบ
- มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ แนวปฏิบัติและหลักการพื้นฐานในการออกแบบมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านความหมายข้อมูล กรณีเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล (TGIX VC/VP)

เอกสารฉบับนี้มุ่งเน้นการนำเสนอแนวทางและแนวปฏิบัติสำหรับหน่วยงานของรัฐในการประยุกต์ใช้เทคโนโลยี VC/VP ในการพัฒนาบริการภาครัฐ โดยไม่ได้มีวัตถุประสงค์เพื่อกำหนดข้อกำหนดหรือมาตรฐานเชิงเทคนิคโดยตรง ทั้งนี้ หน่วยงานสามารถอ้างอิงมาตรฐานสากล กรอบแนวทางที่เกี่ยวข้อง และแนวทางตามมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ แนวปฏิบัติและหลักการพื้นฐานในการออกแบบมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านความหมายข้อมูล กรณีเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัลในการพัฒนาและดำเนินการได้ตามความเหมาะสม

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 ที่เกี่ยวข้องได้ด้วยกระบวนการเข้ารหัสลับ

“เอนทิตี (entity)” หมายความว่า สิ่งที่มีอยู่จริง เช่น บุคคล องค์กร หรืออุปกรณ์ซึ่งถูกกล่าวอ้างในการใช้งาน VC และ VP

“ผู้ออกเอกสาร (Issuer)” หมายความว่า เอนทิตีที่ทำหน้าที่รับรองข้อความยืนยันโดยออกเป็น VC ให้แก่ผู้ถือเอกสาร

“ผู้ถือเอกสาร (Holder)” หมายความว่า เอนทิตีที่เป็นเจ้าของ VC อย่างน้อยหนึ่งชุด โดยจัดเก็บไว้ในกระเป๋าดิจิทัล (Digital Wallet) และสามารถใช้ VC สร้างเป็น VP ทั้งนี้ ผู้ถือเอกสารมีอีกชื่อเรียกหนึ่งว่า ผู้ใช้งานกระเป๋าดิจิทัล

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

“กระเป๋าดิจิทัล (Digital Wallet)” หมายความว่า โปรแกรมที่จัดเก็บและช่วยให้ผู้ถือเอกสารสามารถเข้าถึงและใช้งานเอกสาร VC ได้อย่างมั่นคงปลอดภัย

“ผู้ให้บริการกระเป๋าดิจิทัล (Digital Wallet Provider)” หมายความว่า เอนทิตีที่ทำหน้าที่พัฒนาและ/หรือดำเนินการเกี่ยวกับกระเป๋าดิจิทัล ให้แก่ผู้ออกเอกสาร ผู้ถือเอกสาร หรือผู้ตรวจสอบเอกสาร

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

“การเลือกเปิดเผยข้อมูลบางส่วน (Selective Disclosure)” หมายความว่า กลไกที่เปิดโอกาสให้ผู้ถือเปิดเผยเฉพาะข้อมูลที่จำเป็นต่อวัตถุประสงค์ของการตรวจสอบ 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

“EUDI ARF (European Digital Identity Wallet Architecture and Reference Framework)” หมายความว่า กรอบสถาปัตยกรรมและเอกสารอ้างอิงสำหรับระบบนิเวศของสหภาพยุโรป ซึ่งกำหนดแนวทางร่วมด้านบทบาท องค์ประกอบ มาตรฐาน โปรโตคอล และรูปแบบการแลกเปลี่ยนข้อมูล เพื่อให้ระบบนิเวศสามารถทำงานร่วมกันได้อย่างมีความน่าเชื่อถือ ปลอดภัย และคุ้มครองความเป็นส่วนตัวของผู้ใช้

1.5 กฎหมายและแนวทางที่เกี่ยวข้อง

การพัฒนาและใช้งานใบอนุญาตอิเล็กทรอนิกส์ภาครัฐในรูปแบบ VC/VP ต้องดำเนินการให้สอดคล้องกับกฎหมาย ระเบียบ และแนวทางที่เกี่ยวข้อง ดังต่อไปนี้

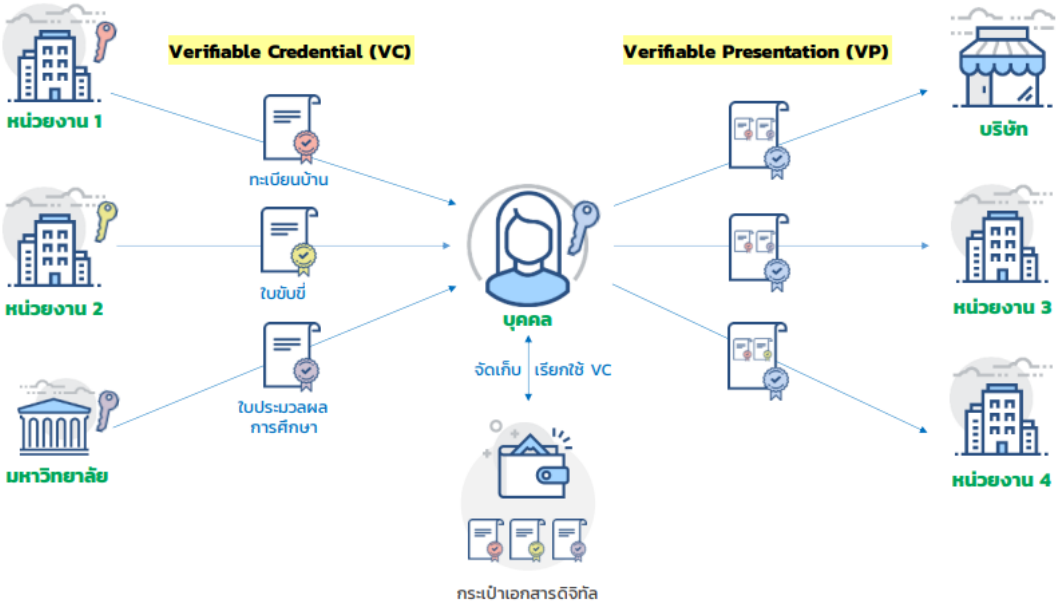
1) พระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. 2565
2) พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม
3) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
4) มาตรฐานรัฐบาลดิจิทัล ว่าด้วยแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – ภาพรวม (มรด. 1-1 : 2564) และ – การพิสูจน์และยืนยันตัวตนทางดิจิทัลสำหรับบุคคลธรรมดาที่มีสัญชาติไทย (มรด. 1-2 : 2564)
5) ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยโครงสร้างข้อมูลของเอกสารรับรองและเอกสารสำแดง (ขมธอ. 24-2563)
6) รายงานทางเทคนิค เรื่อง กรอบการทำงานร่วมกันของกระเป๋าดิจิทัลสำหรับเอกสารรับรอง พ.ศ. 2566 สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
7) รายงานทางเทคนิค เรื่อง กรอบแนวทางการทำงานร่วมกันของเอกสารรับรองดิจิทัลสำหรับประเทศไทย พ.ศ. 2568 สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
8) รายงานทางเทคนิค เรื่อง กรอบการสร้างความน่าเชื่อถือของเอกสารรับรองและเอกสารสำแดง พ.ศ. 2568 สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

2. กรอบแนวคิดและมาตรฐานสำหรับเอกสารรับรองดิจิทัล VC/VP

การยกระดับใบอนุญาตอิเล็กทรอนิกส์ภาครัฐจากเอกสารดิจิทัลทั่วไปสู่รูปแบบที่สามารถพิสูจน์ความถูกต้องได้ (Verifiable Credentials: VC) และการนำเสนอข้อมูลอย่างปลอดภัย (Verifiable Presentations: VP) สะท้อนถึงการปรับเปลี่ยนกระบวนทัศน์จากการจัดการข้อมูลแบบรวมศูนย์ ไปสู่รูปแบบที่ให้ความสำคัญกับการให้ประชาชนเป็นผู้ถือครองและสามารถควบคุมการเปิดเผยข้อมูลของตนเองได้ตามความจำเป็น

ภายใต้แนวทางดังกล่าว เมื่อหน่วยงานภาครัฐออกใบอนุญาตในรูปแบบดิจิทัลที่สามารถพิสูจน์ความถูกต้องได้ ประชาชนจะสามารถจัดเก็บเอกสารไว้ในอุปกรณ์ส่วนบุคคล และเลือกส่งต่อข้อมูลไปยังหน่วยงานปลายทางได้โดยตรง โดยไม่จำเป็นต้องพึ่งพาการเชื่อมโยงข้อมูลแบบจุดต่อจุด (Point-to-Point) ซึ่งมีความซับซ้อนและมีต้นทุนสูง แนวทางนี้อาศัยกลไกทางเทคโนโลยี เช่น ลายมือชื่อดิจิทัลและโครงสร้างข้อมูลที่สามารถตรวจสอบย้อนกลับได้เพื่อสร้างความน่าเชื่อถือของข้อมูลระหว่างหน่วยงาน

เพื่อให้การดำเนินงานดังกล่าวสามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพในระดับประเทศ หน่วยงานของรัฐจำเป็นต้องพิจารณาทั้งในมิติของแนวคิดและองค์ประกอบของระบบ VC/VP กรอบแนวทางและมาตรฐานที่เกี่ยวข้อง ตลอดจนแพลตฟอร์มและโครงสร้างพื้นฐานที่รองรับการให้บริการดิจิทัลของภาครัฐ โดยควรสอดคล้องกับกรอบรายงานทางเทคนิคและมาตรฐานที่เกี่ยวข้องทั้งในระดับประเทศและระดับสากล



ภาพที่ 1 ภาพรวมการใช้งานของเอกสารรับรองดิจิทัล[1]

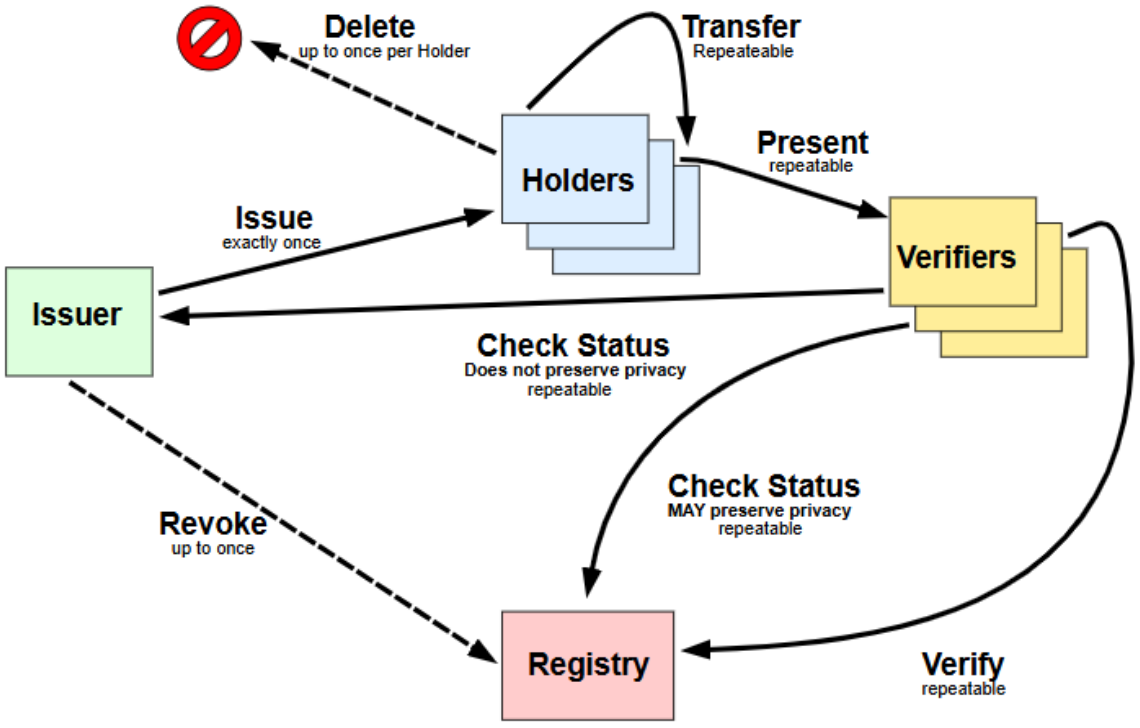
การดำเนินงานภายใต้แนวทางดังกล่าวจะช่วยยกระดับความยืดหยุ่นในการใช้งานเอกสารดิจิทัล รองรับการตรวจสอบสถานะได้อย่างมีประสิทธิภาพ และสร้างรากฐานสำคัญสำหรับการพัฒนาระบบนิเวศดิจิทัลภาครัฐภายใต้หลักการคุ้มครองข้อมูลส่วนบุคคลและความน่าเชื่อถือของแหล่งที่มาของข้อมูล

[1] อ้างอิงภาพมาจากเอกสาร ETDA รายงานทางเทคนิคกรอบแนวทางการทำงานร่วมกันของเอกสารรับรองดิจิทัลสำหรับประเทศไทย เวอร์ชัน 1.1 มกราคม 2568

2.1 แนวคิดหลักในการประยุกต์ใช้ VC/VP

เอกสารรับรองดิจิทัลในรูปแบบ VC/VP เป็นรูปแบบข้อมูลดิจิทัลที่ออกโดยหน่วยงานที่มีอำนาจ และสามารถตรวจสอบความถูกต้องได้จากตัวเอกสารเองโดยไม่ต้องพึ่งพาการเชื่อมต่อกับผู้ออกเอกสาร โดยเอกสารรับรอง (Verifiable Credential: VC) คือ ข้อมูลดิจิทัลที่มีการลงลายมือชื่ออิเล็กทรอนิกส์เพื่อรับรองแหล่งที่มาและความครบถ้วนของข้อมูล ส่วนเอกสารสำแดง (Verifiable Presentation: VP) คือ รูปแบบการนำ VC มาแสดงต่อผู้ตรวจสอบตามวัตถุประสงค์ที่กำหนด

ตัวอย่างเช่น ผู้ถือใบอนุญาตสามารถจัดเก็บเอกสารไว้ในแอปพลิเคชัน และเลือกแสดงเฉพาะข้อมูลที่จำเป็นต่อผู้ตรวจสอบ ซึ่งสามารถตรวจสอบได้ทันทีว่าเอกสารดังกล่าวออกโดยหน่วยงานที่เชื่อถือได้ และยังมีสถานะใช้งานอยู่ การดำเนินการดังกล่าวอาศัยเทคนิคกระบวนการเข้ารหัสลับในการรับรองความถูกต้องครบถ้วนของข้อมูล ทำให้ผู้ตรวจสอบสามารถตรวจสอบเอกสารได้โดยอิสระ ทั้งนี้ แนวคิดดังกล่าวสอดคล้องกับมาตรฐาน W3C Verifiable Credentials Data Model ซึ่งกำหนดกลไกการรับรองข้อมูลและบทบาทของผู้เกี่ยวข้องในระบบไว้อย่างชัดเจน



[2]

ภาพที่ 2 บทบาทและการไหลของข้อมูลภายใต้มาตรฐาน W3C Verifiable Credentials Data Model

[2] อ้างอิงภาพมาจากเอกสาร W3C Verifiable Credentials Data Model v1.1 มีนาคม 2563

2.1.1 แนวคิดหลักของการทำงานในระบบ VC/VP

การดำเนินการในลักษณะดังกล่าวจำเป็นต้องอาศัยแนวคิดหลักของระบบเอกสารรับรองดิจิทัล ดังนี้

1) การรับรองข้อมูลโดยผู้ออกเอกสาร

ผู้ออกเอกสารทำหน้าที่รับรองข้อความยืนยันเกี่ยวกับผู้ถือเอกสารหรือเรื่องที่เกี่ยวข้อง และออกเป็นเอกสารรับรองดิจิทัล (Verifiable Credential: VC) โดยมีกลไกการพิสูจน์ความถูกต้องของแหล่งที่มาและความครบถ้วนของข้อมูลด้วยกระบวนการเข้ารหัสลับ เช่น ลายมือชื่อดิจิทัล หรือ Proof ตามมาตรฐานที่เกี่ยวข้อง

2) การควบคุมข้อมูลโดยผู้ถือเอกสาร

ผู้ถือเอกสารสามารถจัดเก็บ VC ไว้ในกระเป๋าดิจิทัล และสามารถนำ VC ไปสร้างเป็นเอกสารสำแดง (Verifiable Presentation: VP) เพื่อแสดงต่อผู้ตรวจสอบเอกสารได้ตามวัตถุประสงค์ของการใช้งาน

3) การตรวจสอบด้วยกระบวนการเข้ารหัสลับ

ผู้ตรวจสอบเอกสารสามารถตรวจสอบได้ว่า VC หรือ VP มาจากผู้ออกเอกสารที่ระบุจริง ข้อมูลไม่ถูกแก้ไขเปลี่ยนแปลง และในกรณีที่เกี่ยวข้องยังสามารถตรวจสอบสถานะของเอกสาร เช่น การเพิกถอนหรือระงับการใช้งาน ผ่านกลไกตรวจสอบสถานะตามที่ระบบกำหนด

4) การเลือกเปิดเผยข้อมูลบางส่วน

ระบบ VC/VP รองรับแนวคิดให้ผู้ถือเอกสารเปิดเผยเฉพาะข้อมูลที่จำเป็นต่อวัตถุประสงค์ของการตรวจสอบได้ โดยไม่จำเป็นต้องเปิดเผยข้อมูลทั้งหมดของเอกสารเสมอไป ทั้งนี้ขึ้นอยู่กับรูปแบบเทคโนโลยีและกลไก Proof ที่เลือกใช้

5) การสนับสนุนด้วยโครงสร้างพื้นฐานด้านความน่าเชื่อถือ

การทำงานของระบบ VC/VP ในทางปฏิบัติยังต้องอาศัยองค์ประกอบสนับสนุนด้านความน่าเชื่อถือ เช่น กลไกเผยแพร่ข้อมูลของผู้ออกเอกสารที่เชื่อถือได้ กลไกจัดการกุญแจดิจิทัล กลไกตรวจสอบสถานะเอกสาร ตลอดจนกรอบธรรมาภิบาลและข้อกำหนดที่เกี่ยวข้อง เพื่อให้การออก การแสดง และการตรวจสอบเอกสารเป็นไปอย่างน่าเชื่อถือและทำงานร่วมกันได้ในระดับระบบนิเวศ

2.1.2 แนวคิดสำคัญที่ทำให้ระบบ VC/VP มีความน่าเชื่อถือ ความปลอดภัย และความเป็นส่วนตัว

ความน่าเชื่อถือของระบบ VC/VP ไม่ได้เกิดจากรูปแบบเอกสารเพียงอย่างเดียว แต่เกิดจากการออกแบบระบบที่รองรับการยืนยันตัวตน การพิสูจน์ความถูกต้องของเอกสาร การคุ้มครองความเป็นส่วนตัว และการลดการพึ่งพาตัวกลางเกินจำเป็น โดยแนวคิดสำคัญ ได้แก่

1) การมีรากฐานการยืนยันตัวตนที่เชื่อถือได้ (Root of Trust)

ความน่าเชื่อถือของ VC เริ่มต้นจากการอ้างอิงข้อมูลยืนยันตัวตนหลักที่เชื่อถือได้ เช่น PID (Person Identification Data) ซึ่งในบริบทสากลสอดคล้องกับแนวทางของ EUDI ARF ที่ใช้ PID เป็นรากฐานของเอกสารประเภทอื่นต่อไป

2) การใช้กลไกตัวระบุและกุญแจดิจิทัลที่เหมาะสมกับบทบาท (DID Method)

การกำหนดตัวระบุและข้อมูลกุญแจดิจิทัลให้เหมาะสมกับบทบาทของผู้ออก ผู้ถือ และผู้ตรวจสอบ เพื่อให้สามารถตรวจสอบแหล่งที่มาและความถูกต้องของเอกสารได้ โดยแนวคิดนี้เชื่อมโยงกับ DID Method ตามมาตรฐาน W3C DID Core และแนวทางของ EUDI ARF ในการใช้ข้อมูลยืนยันตัวตนและข้อมูลสำหรับการตรวจสอบที่เชื่อถือได้

3) การตรวจสอบได้โดยไม่ต้องพึ่งพาการเรียกกลับไปยังระบบกลางทุกครั้ง (Local Resolution)

ระบบ VC/VP สามารถออกแบบให้ผู้ตรวจสอบตรวจสอบ Proof ที่มีอยู่แล้วในฝั่ง Wallet หรือในข้อมูลอ้างอิงที่เข้าถึงได้ โดยลดการพึ่งพาการเรียกไปยังส่วนกลางทุกครั้ง เพื่อลดการจราจร ทั้งนี้แนวคิดดังกล่าวสอดคล้องกับหลักการของ W3C ที่มุ่งให้เอกสารสามารถตรวจสอบได้ด้วยกระบวนการรหัสลับและรองรับการทำงานแบบ Local Resolution ในบางรูปแบบการนำไปใช้.

4) การพิสูจน์การครอบครองกุญแจของผู้แสดงเอกสาร (Proof of Possession – PoP)

ระบบ VC/VP สามารถมีกลไก Proof of Possession เพื่อพิสูจน์ว่าผู้แสดงเอกสารเป็นผู้ครอบครองกุญแจส่วนตัว (Private Key) ที่เกี่ยวข้องจริง เช่น ระบบ Wallet สามารถให้ผู้ตรวจสอบส่งค่า Challenge หรือ Nonce แบบสุ่ม แล้วให้ผู้ถือเอกสารใช้กุญแจส่วนตัวลงนามหรือสร้าง Proof เพื่อตอบกลับมาให้ตรวจสอบได้ แนวคิดนี้สอดคล้องกับกลไก Challenge-Response ตามมาตรฐาน OID4VCI และ OID4VP

5) การลดการติดตามจากการตรวจสอบโดยไม่จำเป็น (Anti-Tracking)

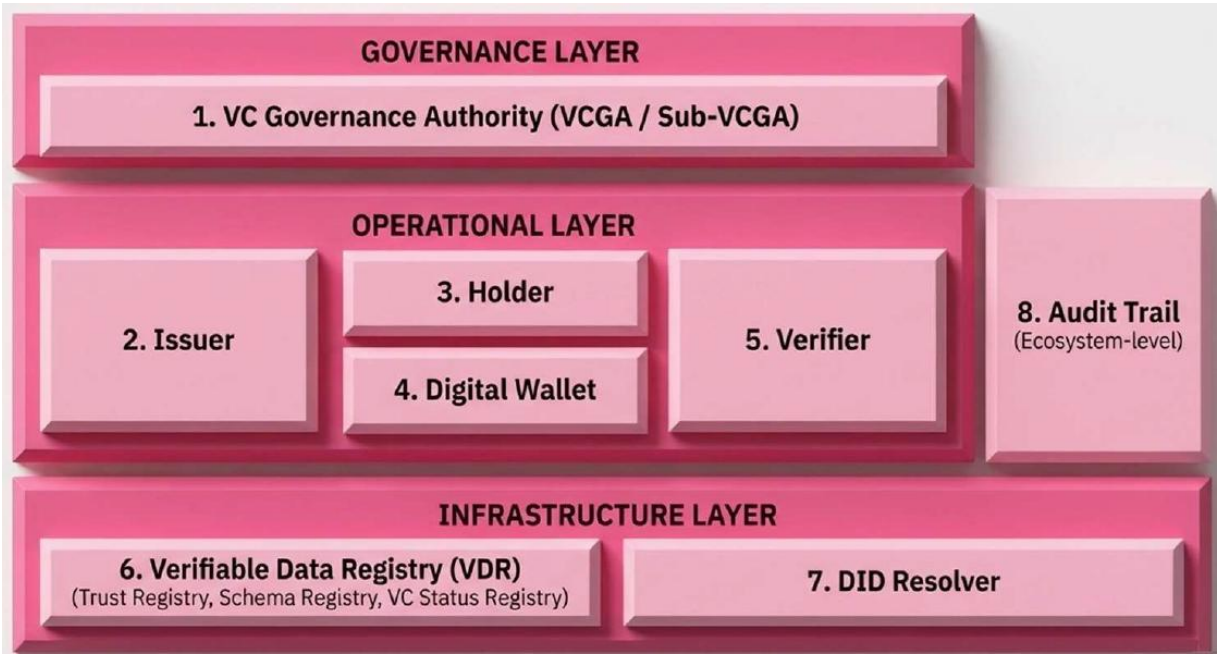
ความเป็นส่วนตัวของผู้ถือเอกสารจะมีมากยิ่งขึ้นเมื่อระบบลดการตรวจสอบย้อนกลับไปยังผู้ออกเอกสารระหว่างการสำแดงเอกสาร เพราะหากต้องเรียกกลับผู้ออกเอกสารบ่อยครั้ง อาจทำให้ผู้ออกเอกสารทราบได้ว่าผู้ถือเอกสารไปทำธุรกรรมที่ใดและเมื่อใด แนวคิดนี้จึงเป็น Anti-Tracking หรือการลดความสามารถในการเชื่อมโยงพฤติกรรมของผู้ถือเอกสาร และสอดคล้องกับแนวคิด Selective Disclosure ตาม W3C และ EUDI ARF

2.1.3 องค์ประกอบของระบบนิเวศ

ภายใต้ระบบนิเวศเอกสารรับรองดิจิทัล VC/VP ประกอบด้วยองค์ประกอบสำคัญ 8 ส่วน ดังนี้

1) กรอบบริการและหน่วยงานกำกับดูแลระบบเอกสารรับรอง (VC Trust Framework and Governance Authority: VCGA / Sub-VCGA)
2) ผู้ออกเอกสารรับรอง (Issuer)
3) ผู้ถือเอกสารรับรอง (Holder)
4) ผู้ให้บริการกระเป๋าดิจิทัล (Digital Wallet Provider)
5) ผู้ตรวจสอบเอกสาร (Verifier)
6) ระบบทะเบียนข้อมูลที่ตรวจสอบได้ (Verifiable Data Registry: VDR) เช่น Trust Registry, Schema Registry และ VC Status Registry
7) ระบบสืบค้นข้อมูลตัวระบุแบบกระจายศูนย์ (DID Resolver)
8) การตรวจสอบ (Audit Trail: Ecosystem-level)

องค์ประกอบทั้ง 8 ส่วนดังกล่าวทำงานร่วมกันภายใต้ 3 ชั้นหลัก ได้แก่ ชั้นการกำกับดูแล (Governance Layer) ชั้นการดำเนินงาน (Operational Layer) และชั้นโครงสร้างพื้นฐาน (Infrastructure Layer) เพื่อรองรับการออก การถือครอง การสำแดง และการตรวจสอบเอกสารรับรองดิจิทัลให้มีความน่าเชื่อถือ มั่นคงปลอดภัย และสามารถตรวจสอบย้อนหลังได้



ภาพที่ 3 องค์ประกอบภายใต้ระบบนิเวศเอกสารรับรองดิจิทัล[3]

[3] อ้างอิงภาพมาจากเอกสาร ETDA การประชุมเชิงปฏิบัติการ เรื่อง การออกแบบกระบวนการทางเทคนิคการใช้เอกสารดิจิทัล มีนาคม 2569

2.1.4 กระบวนการทำงานของระบบนิเวศเอกสารรับรองดิจิทัล

กระบวนการทำงานของระบบเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัลโดยทั่วไป สามารถอธิบายได้เป็น 7 กระบวนการ ดังนี้

1) **P0 การกำกับดูแลและขึ้นทะเบียนความน่าเชื่อถือ** (Ecosystem Governance & Trust Registry)

เป็นกระบวนการกำหนดกฎเกณฑ์ การกำกับดูแล และการขึ้นทะเบียนผู้ที่เกี่ยวข้องในระบบนิเวศ เพื่อสร้างฐานความน่าเชื่อถือร่วมกันของทั้งระบบ

2) **P1 การเตรียมพร้อมกระเป๋าดิจิทัลและการออกเอกสารยืนยันตัวตนหลัก** (Wallet Provisioning & PID VC Issuance)

เป็นกระบวนการเตรียมความพร้อมของกระเป๋าดิจิทัล การสร้างและจัดการกุญแจที่เกี่ยวข้อง ตลอดจนการออกเอกสารยืนยันตัวตนหลัก เพื่อใช้เป็นรากฐานของความน่าเชื่อถือในการทำธุรกรรมต่อไป

3) **P2 การออกเอกสารรับรองดิจิทัลประเภทต่าง ๆ** (Standard VC Issuance)

เป็นกระบวนการที่ผู้ออกเอกสารออกเอกสารรับรองดิจิทัลให้แก่ผู้ถือเอกสารตามเงื่อนไขหรือคุณสมบัติที่กำหนด

4) **P3 การถือครอง จัดการเอกสาร และบริหารกุญแจ** (VC Holding & Lifecycle Management)

เป็นกระบวนการที่ผู้ถือเอกสารจัดเก็บ ดูแล และบริหารวงจรชีวิตของเอกสารรับรองดิจิทัลและกุญแจที่เกี่ยวข้องภายในกระเป๋าดิจิทัล

5) **P4 การสำแดงเอกสาร** (VP Presentation)

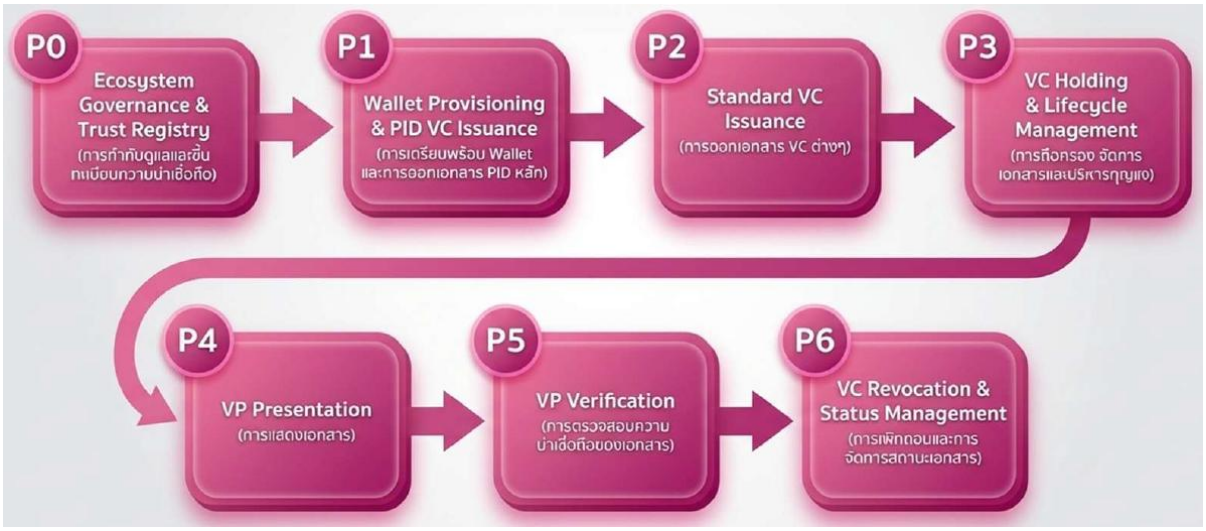
เป็นกระบวนการที่ผู้ถือเอกสารนำข้อมูลจากเอกสารรับรองดิจิทัลมาสร้างและแสดงเป็นเอกสารสำแดงดิจิทัลแก่ผู้ตรวจสอบตามวัตถุประสงค์ของการใช้งาน

6) **P5 การตรวจสอบความน่าเชื่อถือของเอกสาร** (VP Verification)

เป็นกระบวนการที่ผู้ตรวจสอบเอกสารตรวจสอบความถูกต้อง ความสมบูรณ์ สถานะ และความน่าเชื่อถือของเอกสารสำแดงดิจิทัลตามกฎเกณฑ์ที่ระบบกำหนด

7) **P6 การเพิกถอนและการจัดการสถานะเอกสาร** (VC Revocation & Status Management)

เป็นกระบวนการจัดการสถานะของเอกสารรับรองดิจิทัล เช่น การพักใช้ การเพิกถอน หรือการเปลี่ยนแปลงสถานะ เพื่อให้การตรวจสอบเอกสารเป็นปัจจุบันและน่าเชื่อถืออยู่เสมอ



ภาพที่ 4 กระบวนการทำงานของระบบนิเวศเอกสารรับรองดิจิทัล[4]

โดยลำดับการทำงานดังกล่าวสะท้อนให้เห็นว่า ระบบ VC/VP มิได้เป็นเพียงรูปแบบข้อมูลของเอกสารเท่านั้น แต่เป็นระบบนิเวศที่ครอบคลุมตั้งแต่การกำกับดูแล การออกเอกสาร การถือครอง การสำแดง การตรวจสอบ ไปจนถึงการจัดการสถานะของเอกสารอย่างเป็นวงจรครบถ้วน

2.2 กรอบแนวทางด้านเอกสารรับรองดิจิทัลที่ประกาศโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ในบริบทของประเทศไทย สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) ได้จัดทำและประกาศกรอบมาตรฐานและรายงานทางเทคนิคที่เกี่ยวข้องกับเอกสารรับรองดิจิทัล (Verifiable Credentials: VC) และเอกสารสำแดงดิจิทัล (Verifiable Presentations: VP) เพื่อสนับสนุนการนำแนวคิดตามมาตรฐานสากลไปสู่การใช้งานจริงในระดับประเทศ

โดยในขณะที่มาตรฐานสากล เช่น W3C Verifiable Credentials Data Model มุ่งเน้นการกำหนดรูปแบบข้อมูลและหลักการพื้นฐานของเอกสารรับรองดิจิทัล กรอบแนวทางของ ETDA ได้ขยายแนวคิดดังกล่าวไปสู่การกำหนดองค์ประกอบที่จำเป็นต่อการใช้งานจริงในระดับระบบนิเวศของภาครัฐ ทั้งในด้านการเชื่อมโยงระบบ การทำงานร่วมกัน และการสร้างความน่าเชื่อถือระหว่างหน่วยงาน

[4] อ้างอิงภาพมาจาก ETDA เอกสารการประชุมเชิงปฏิบัติการ เรื่อง การออกแบบกระบวนการทางเทคนิคการใช้เอกสารดิจิทัล มีนาคม 2569

กรอบดังกล่าวจึงทำหน้าที่เป็นทั้งโครงสร้างพื้นฐานเชิงแนวคิด (Conceptual Foundation) และโครงสร้างพื้นฐานเชิงระบบ (Infrastructure Foundation) สำหรับการพัฒนาและใช้งาน VC/VP ในระดับประเทศ โดยครอบคลุมองค์ประกอบสำคัญ 4 ด้าน ดังนี้

- **ด้านโครงสร้างข้อมูล (Data Model):** การกำหนดรูปแบบและโครงสร้างข้อมูลของ VC และ VP ให้สามารถระบุผู้ออก ผู้ถือ และข้อความยืนยันได้อย่างชัดเจน รวมถึงรองรับการลงลายมือชื่ออิเล็กทรอนิกส์
- **ด้านการทำงานของกระเป๋าดิจิทัล (Wallet):** การจัดเก็บ การนำเสนอ และการควบคุมการเปิดเผยข้อมูลของผู้ถือเอกสาร รวมถึงกลไกการเลือกเปิดเผยข้อมูลบางส่วน (Selective Disclosure)
- **ด้านการทำงานร่วมกัน (Interoperability):** การกำหนดแนวทางการแลกเปลี่ยนและยอมรับเอกสาร VC/VP ระหว่างหน่วยงาน เพื่อลดการพัฒนาแบบจุดต่อจุด
- **ด้านความน่าเชื่อถือและการกำกับดูแล (Trust and Governance):** การกำหนดโครงสร้างพื้นฐานด้านความเชื่อถือ กลไกการตรวจสอบสถานะ และหลักเกณฑ์ด้านการกำกับดูแล

โดยกรอบดังกล่าวมีบทบาทในการกำหนด “หลักการขั้นต่ำที่ระบบควรมี” เพื่อให้เอกสารรับรองดิจิทัลสามารถรองรับการใช้งานในระดับระบบนิเวศได้อย่างมีประสิทธิภาพ โดยมีคุณลักษณะสำคัญ ได้แก่

- สามารถตรวจสอบความถูกต้องและความครบถ้วนของข้อมูลได้ด้วยกระบวนการเข้ารหัสลับ
- สามารถใช้งานข้ามหน่วยงานได้ โดยลดความจำเป็นในการพัฒนาเชื่อมต่อแบบเฉพาะโครงการ
- รองรับการบริหารสถานะของใบอนุญาตหรือเอกสารได้อย่างเป็นระบบ
- มีโครงสร้างพื้นฐานด้านความน่าเชื่อถือรองรับในระดับประเทศ

เพื่อให้ครอบคลุมองค์ประกอบดังกล่าว ETDA ได้จัดทำกรอบมาตรฐานและรายงานทางเทคนิคที่เกี่ยวข้อง จำนวน 4 ฉบับ ดังนี้

1) ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยโครงสร้างข้อมูลของเอกสารรับรองและเอกสารสำแดง (ขมธอ. 24-2563)

เอกสารฉบับนี้กำหนดโครงสร้างข้อมูลพื้นฐานของเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล เพื่อให้สามารถ

- ระบุผู้ออก (Issuer) และผู้ถือ (Holder/Subject) ได้อย่างชัดเจน
- กำหนดข้อความยืนยัน (Claims) ในรูปแบบข้อมูลเชิงโครงสร้าง
- รองรับการลงลายมือชื่ออิเล็กทรอนิกส์
- ตรวจสอบความถูกต้องครบถ้วนของข้อมูลด้วยกระบวนการเข้ารหัสลับ

กรอบดังกล่าวเป็นรากฐานด้าน Data Model สำหรับการออกแบบ Schema ของ VC ในประเทศไทย และช่วยให้การพัฒนามีความสอดคล้องกับมาตรฐานสากล เช่น W3C Verifiable Credentials Data Model โดยไม่ขัดกับบริบทกฎหมายไทย

ภาพที่ 5 ตัวอย่างโครงสร้างข้อมูล VC/VP[5]

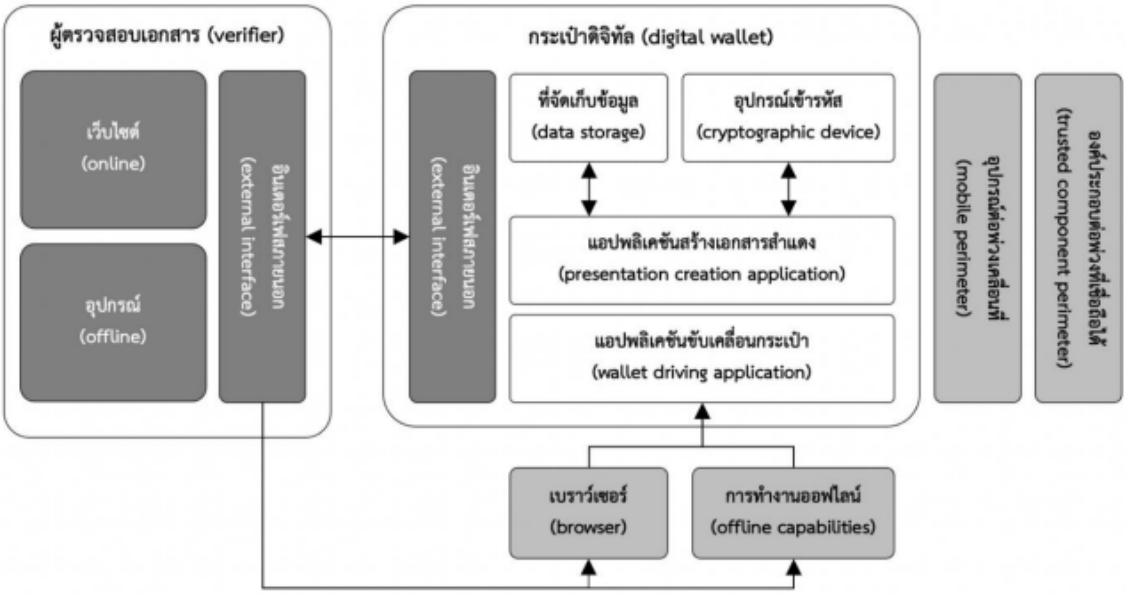
[5] อ้างอิงภาพมาจากเอกสาร ETDA ขมธอ. 24-2563 ว่าด้วยโครงสร้างข้อมูลของเอกสารรับรองและเอกสารสำแดง เวอร์ชัน 1.1 กันยายน 2563

2) รายงานทางเทคนิค เรื่อง กรอบการทำงานร่วมกันของกระเป๋าดิจิทัลสำหรับเอกสารรับรอง (พ.ศ. 2566)

เอกสารฉบับนี้กำหนดหลักการและแนวทางให้กระเป๋าดิจิทัล (Digital Wallet) สามารถทำงานร่วมกันได้ในระดับประเทศ โดยมีสาระสำคัญ ได้แก่

- การจัดเก็บ VC อย่างมั่นคงปลอดภัย
- การสร้างและส่ง Verifiable Presentation (VP)
- การรองรับกลไกการเลือกเปิดเผยข้อมูลบางส่วน (Selective Disclosure)
- การทำงานร่วมกับผู้ออกเอกสารและผู้ตรวจสอบหลายหน่วยงาน

กรอบนี้มีความสำคัญต่อการพัฒนา Wallet ให้เป็นมาตรฐานเดียวกัน และสนับสนุนให้เกิดระบบนิเวศที่เปิดกว้างและทำงานร่วมกันได้ (Interoperable Ecosystem)



ภาพที่ 6 สถาปัตยกรรมซอฟต์แวร์ของกระเป๋าดิจิทัล[6]

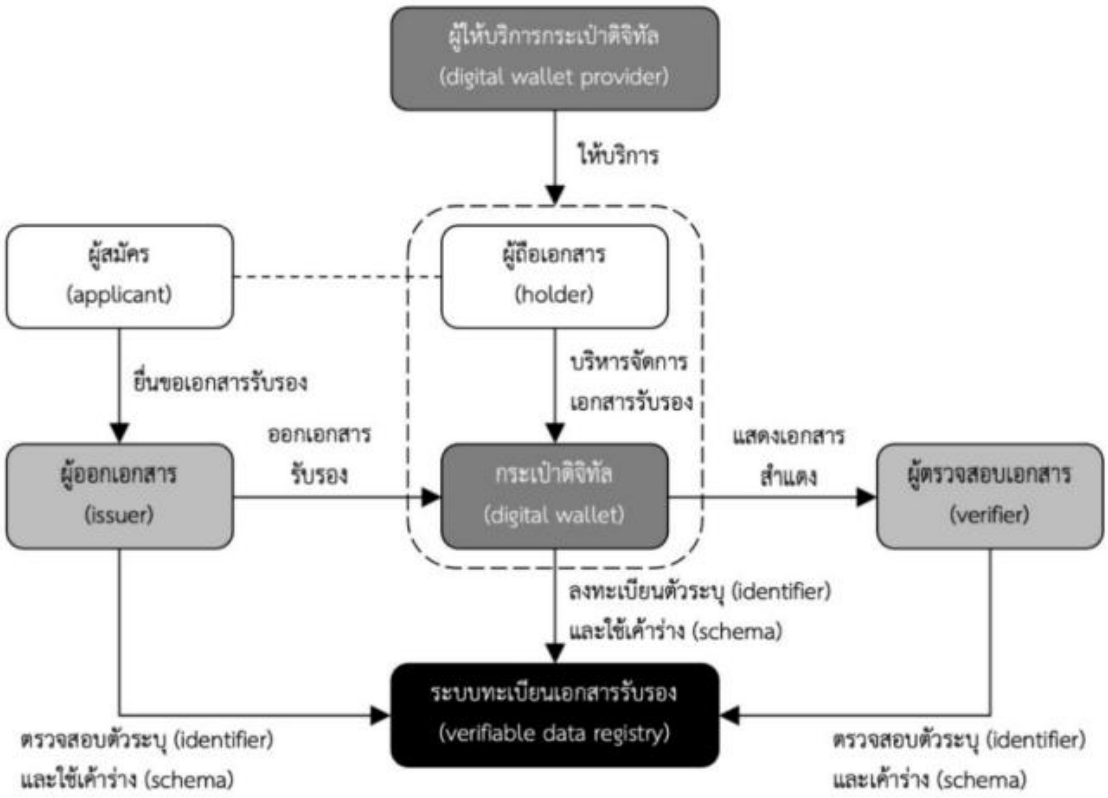
[6] อ้างอิงภาพมาจากเอกสาร ETDA รายงานทางเทคนิคกรอบการทำงานร่วมกันของกระเป๋าดิจิทัลสำหรับเอกสารรับรอง เวอร์ชัน 1.0 เมษายน 2566

3) รายงานทางเทคนิค เรื่อง กรอบแนวทางการทำงานร่วมกันของเอกสารรับรองดิจิทัลสำหรับประเทศไทย (พ.ศ. 2568)

เอกสารฉบับนี้กำหนดหลักการด้าน Interoperability ของเอกสารรับรองดิจิทัลในระดับประเทศ ครอบคลุม

- การกำหนดบทบาทของ Issuer, Holder และ Verifier
- แนวทางการแลกเปลี่ยนและยอมรับเอกสาร VC/VP ข้ามหน่วยงาน
- หลักการลดการเชื่อมต่อแบบจุดต่อจุด (Point-to-Point Integration)
- การสนับสนุนการใช้งานเอกสารในหลายบริบทโดยไม่ต้องพึ่งพาฐานข้อมูลต้นทางทุกครั้ง

กรอบดังกล่าวทำให้ VC/VP สามารถทำหน้าที่เป็น “เอกสารดิจิทัลที่ใช้ร่วมกันได้ในระดับประเทศ” แทนการเป็นเอกสารเฉพาะระบบของหน่วยงานใดหน่วยงานหนึ่ง



ภาพที่ 7 บทบาทของผู้ที่เกี่ยวข้องกับการใช้งานเอกสารรับรองดิจิทัล[7]

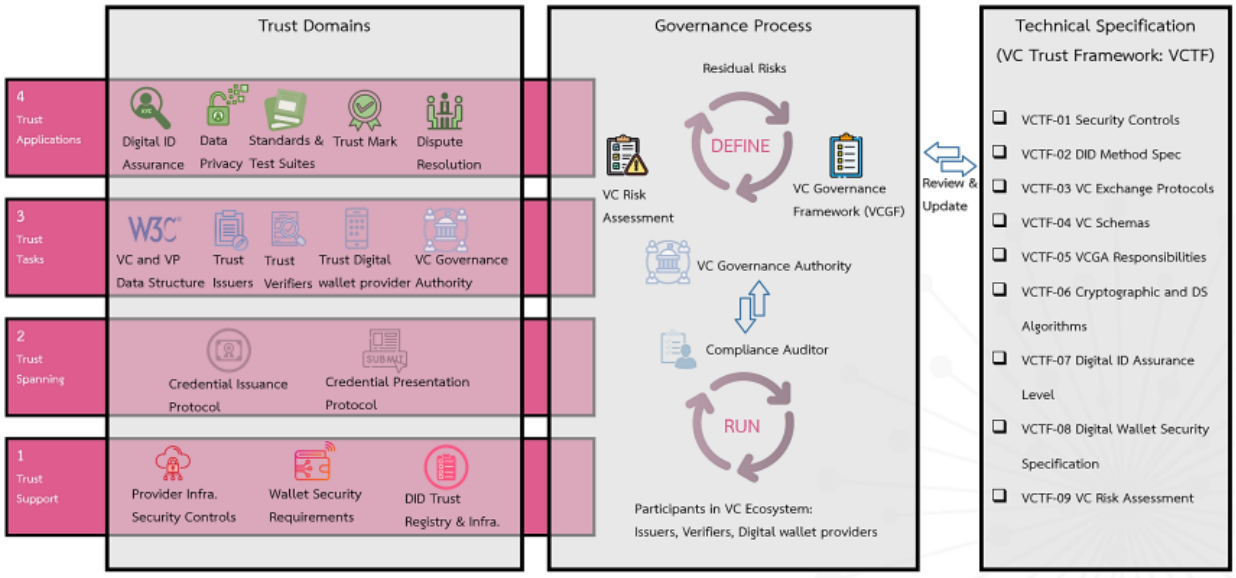
[7] อ้างอิงภาพมาจากเอกสาร ETDA รายงานทางเทคนิคกรอบแนวทางการทำงานร่วมกันของเอกสารรับรองดิจิทัลสำหรับประเทศไทย เวอร์ชัน 1.1 มกราคม 2568

4) รายงานทางเทคนิค เรื่อง กรอบการสร้างความน่าเชื่อถือของเอกสารรับรองและเอกสารสำแดง (พ.ศ. 2568)

เอกสารฉบับนี้กำหนดโครงสร้างพื้นฐานด้านความน่าเชื่อถือ (Trust Infrastructure) สำหรับระบบเอกสารรับรองดิจิทัล โดยครอบคลุมองค์ประกอบสำคัญ เช่น

- ระบบทะเบียนผู้ออกเอกสาร (Issuer Registry)
- การบริหารจัดการกุญแจดิจิทัล
- กลไกการตรวจสอบสถานะ (Credential Status / Revocation Mechanism)
- หลักเกณฑ์ด้านการกำกับดูแลและการประเมินความสอดคล้อง

กรอบนี้มีบทบาทสำคัญในการทำให้ระบบ VC/VP มีความน่าเชื่อถือในระดับระบบนิเวศ (Ecosystem-Level Trust) มิใช่อาศัยเพียงกลไกการเข้ารหัสในระดับเอกสารเท่านั้น



ภาพที่ 8 กรอบแนวทางการสร้างความน่าเชื่อถือสำหรับระบบนิเวศเอกสารรับรอง (VC Trust Model Framework) อ้างอิงกรอบความน่าเชื่อถือของระบบนิเวศดิจิทัลโดย ToIP[8]

โดยภาพรวม กรอบมาตรฐานและรายงานทางเทคนิคดังกล่าวทำหน้าที่เป็นรากฐานสำคัญในการพัฒนาระบบเอกสารรับรองดิจิทัลของประเทศ ทั้งในด้านโครงสร้างข้อมูล การทำงานร่วมกัน และโครงสร้างพื้นฐานด้านความน่าเชื่อถือ ซึ่งหน่วยงานของรัฐควรนำไปใช้เป็นแนวทางอ้างอิงในการออกแบบและพัฒนาระบบ VC/VP ให้สามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพในระดับประเทศ

[8] อ้างอิงภาพมาจากเอกสาร ETDA รายงานทางเทคนิคกรอบการสร้างความน่าเชื่อถือของเอกสารรับรองและเอกสารสำแดง เวอร์ชัน 1.0 ธันวาคม 2568

2.3 มาตรฐานที่เกี่ยวข้อง

ปัจจุบันมีมาตรฐานสากลที่รองรับการพัฒนาเอกสารในรูปแบบ VC/VP ซึ่งถูกนำไปใช้งานจริงในหลายประเทศ การพัฒนาใบอนุญาตภาครัฐในรูปแบบดังกล่าวจึงควรอ้างอิงมาตรฐานที่เกี่ยวข้อง เพื่อให้ระบบสามารถทำงานร่วมกัน (Interoperability) ได้ในระยะยาว และรองรับการเชื่อมโยงกับระบบของหน่วยงานอื่นทั้งในและต่างประเทศ

ทั้งนี้ การจัดกลุ่มมาตรฐานตามลำดับการใช้งานของเอกสารในหัวข้อนี้ เป็นการสรุปเชิงแนวปฏิบัติโดยอ้างอิงจากมาตรฐานสากลร่วมกับกรอบมาตรฐานและรายงานทางเทคนิคของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) ซึ่งครอบคลุมทั้งด้านโครงสร้างข้อมูล การทำงานร่วมกัน และโครงสร้างพื้นฐานด้านความน่าเชื่อถือ

เพื่อให้เข้าใจง่าย มาตรฐานที่เกี่ยวข้องสามารถพิจารณาตาม “ลำดับการใช้งานของเอกสาร” ได้ดังนี้

1) การกำหนดรูปแบบข้อมูล (Data Model)

เป็นการกำหนดว่า “เอกสาร VC/VP มีโครงสร้างอย่างไร และประกอบด้วยข้อมูลอะไรบ้าง”

ควรอ้างอิง:

1.1) W3C Verifiable Credentials Data Model 2.0

1.2) แนวทางการกำหนดโครงสร้างข้อมูลภาครัฐ เช่น TGIX VC/VP

1.3) ข้อเสนอแนะมาตรฐานด้านโครงสร้างข้อมูลของเอกสารรับรองและเอกสารสำแดง (ขมธอ. 24-2563)

มาตรฐานในส่วนนี้ช่วยกำหนดเรื่อง เช่น

- การระบุผู้ออกเอกสาร (Issuer) และผู้ถือเอกสาร (Subject)
- การกำหนดข้อความยืนยัน (Claims) ในรูปแบบข้อมูลเชิงโครงสร้าง
- การลงลายมือชื่ออิเล็กทรอนิกส์เพื่อรับรองความถูกต้องของข้อมูล

2) การออกเอกสาร (Issuance)

เป็นขั้นตอนที่หน่วยงานออก VC ให้กับประชาชนหรือผู้ประกอบการ

ควรอ้างอิง:

2.1) OpenID for Verifiable Credential Issuance (OID4VCI)

2.2) แนวทางการพิสูจน์และยืนยันตัวตนดิจิทัล

ในบริบทประเทศไทย การออกเอกสารควรเชื่อมโยงกับระบบ Digital ID ที่ได้รับการยอมรับ เพื่อให้สามารถยืนยันตัวตนของผู้รับเอกสารได้อย่างถูกต้องและมีความน่าเชื่อถือ ซึ่งสอดคล้องกับแนวทางด้านการทำงานร่วมกันของเอกสารรับรองดิจิทัลตามกรอบของ ETDA

3) การนำเอกสารไปแสดง (Presentation)

เป็นขั้นตอนที่ผู้ถือเอกสารนำ VC ไปแสดงต่อหน่วยงานปลายทางในรูปแบบ VP

ควรอ้างอิง:

3.1) OpenID for Verifiable Presentations (OID4VP)

มาตรฐานในส่วนนี้ช่วยให้

- ผู้ถือเอกสารสามารถเลือกเปิดเผยเฉพาะข้อมูลที่จำเป็น (Selective Disclosure)
- รองรับการนำเสนอข้อมูลในหลายบริบท โดยไม่ต้องเปิดเผยข้อมูลทั้งหมด

4) การตรวจสอบความถูกต้อง (Verification)

เป็นขั้นตอนที่หน่วยงานปลายทางตรวจสอบว่าเอกสารที่ได้รับ “ถูกต้องและยังใช้งานได้”

การตรวจสอบความถูกต้องของ VC/VP อาศัยมาตรฐานและกลไกหลายส่วนร่วมกัน เช่น

- การตรวจสอบลายมือชื่อดิจิทัลตาม W3C Verifiable Credentials Data Model 2.0
- การตรวจสอบตัวตนของผู้ออกเอกสารผ่านกลไก DID หรือ Trust Registry
- การตรวจสอบสถานะของเอกสาร (Credential Status / Revocation)

องค์ประกอบดังกล่าวสอดคล้องกับกรอบการสร้างความน่าเชื่อถือของเอกสารรับรองและเอกสารสำแดงของ ETDA ซึ่งกำหนดกลไกในการตรวจสอบในระดับระบบนิเวศ

5) การจัดเก็บเอกสาร (Wallet)

เป็นการจัดเก็บเอกสารในรูปแบบกระเป๋าดิจิทัล (Digital Wallet) แม้ยังไม่มีมาตรฐานสากลเพียงหนึ่งเดียวที่กำหนดรูปแบบการทำงานทั้งหมดของ Wallet แต่มีแนวทางและข้อกำหนดที่เกี่ยวข้องจากหลายมาตรฐาน เช่น VC, DID และเทคโนโลยีด้านกระบวนการเข้ารหัสลับ รวมถึงกรอบการพัฒนา Wallet ในระดับสากล (เช่น European Digital Identity Wallet)

ในบริบทประเทศไทย แนวทางดังกล่าวถูกนำมาประยุกต์ผ่านรายงานทางเทคนิคของ ETDA โดยเฉพาะกรอบการทำงานร่วมกันของกระเป๋าดิจิทัลสำหรับเอกสารรับรอง เพื่อกำหนดข้อแนะนำด้านความมั่นคงปลอดภัย การจัดการกุญแจ และการทำงานร่วมกันของระบบ

โดยระบบในส่วนนี้ควร:

- มีความมั่นคงปลอดภัย
- รองรับการใช้งานร่วมกับหลายหน่วยงาน
- สามารถเรียกใช้งานเอกสารเพื่อสร้างและแสดงผล VP ได้อย่างสะดวก

2.4 แนวทางการนำมาตรฐานสู่การดำเนินการของหน่วยงานของรัฐ

จากการศึกษามาตรฐานสากลและกรอบแนวทางที่เกี่ยวข้อง รวมถึงกรอบมาตรฐานและรายงานทางเทคนิคของประเทศไทย หน่วยงานของรัฐสามารถนำแนวคิดดังกล่าวมาประยุกต์ใช้ในการพัฒนาระบบเอกสารรับรองดิจิทัลในรูปแบบ VC/VP ได้ โดยพิจารณาองค์ประกอบสำคัญอย่างน้อยใน 4 ด้าน ดังนี้

1) ด้านโครงสร้างข้อมูล (Data Model)

หน่วยงานควรกำหนดโครงสร้างข้อมูลของเอกสารรับรองดิจิทัล (VC) ให้สอดคล้องกับมาตรฐานที่เกี่ยวข้อง เช่น W3C Verifiable Credentials Data Model และแนวทางโครงสร้างข้อมูลภาครัฐ เพื่อให้สามารถตรวจสอบความถูกต้องของข้อมูล และรองรับการใช้งานร่วมกันระหว่างหน่วยงานได้

2) ด้านกระบวนการ (Process Integration)

หน่วยงานควรกำหนดกระบวนการออก การนำเสนอ การบริหารสถานะ และการตรวจสอบเอกสาร VC/VP ให้สอดคล้องกับกระบวนการทางดิจิทัลภาครัฐตามมาตรฐาน มสพร 6-1 โดยเฉพาะในขั้นตอนการจัดทำและส่งมอบเอกสาร

3) ด้านเทคโนโลยีและโครงสร้างพื้นฐาน (Technology and Infrastructure)

หน่วยงานควรออกแบบและพัฒนาระบบโดยคำนึงถึงการใช้โครงสร้างพื้นฐานร่วมในระดับประเทศ เพื่อให้สามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพ ลดความซ้ำซ้อนในการลงทุน และรองรับการขยายผลในระยะยาว

โดยควรพิจารณาแนวทางดังต่อไปนี้

3.1) หลีกเลี่ยงการพัฒนาแบบแยกส่วน (Silo)

การพัฒนาโครงสร้างพื้นฐานแยกตามหน่วยงานอาจก่อให้เกิดความซ้ำซ้อน ขาด interoperability และเพิ่มภาระในการเชื่อมโยงระบบในอนาคต

3.2) ใช้โครงสร้างพื้นฐานที่มีอยู่แล้วเป็นลำดับแรก (Reuse-First Principle)

ควรสำรวจและเลือกใช้แพลตฟอร์มหรือโครงสร้างพื้นฐานที่มีอยู่แล้ว ทั้งในระดับหน่วยงานและระดับประเทศ ก่อนพัฒนาระบบใหม่ โดยเฉพาะในกรณีที่เกี่ยวข้องกับกระเป๋าดิจิทัล หน่วยงานควรพิจารณาความเป็นไปได้ในการเชื่อมโยงหรือบูรณาการกับแพลตฟอร์มกลางของรัฐที่มีอยู่หรือที่ได้รับการกำหนดในอนาคต เพื่อหลีกเลี่ยงการพัฒนาแอปพลิเคชันหรือกระเป๋าดิจิทัลแยกตามหน่วยงานโดยไม่จำเป็น และลดภาระของประชาชนในการใช้งานหลายระบบ

3.3) ออกแบบให้รองรับการใช้งานร่วมกัน (Reusable by Design)

ในกรณีที่จำเป็นต้องพัฒนาระบบใหม่ ควรออกแบบให้สามารถนำไปใช้ซ้ำหรือขยายผลได้ โดยใช้มาตรฐานกลาง และรองรับการเชื่อมโยงผ่าน API

3.4) ออกแบบให้สามารถพัฒนาเป็นแพลตฟอร์มร่วม (Shared Platform)

ระบบที่มีแนวโน้มใช้งานในหลายหน่วยงาน ควรออกแบบให้สามารถพัฒนาเป็นแพลตฟอร์มกลางหรือรองรับการใช้งานในวงกว้าง ทั้งนี้ ในกรณีของกระเป๋าดิจิทัล ควรออกแบบให้รองรับการทำงานร่วมกันกับหลายหน่วยงาน หลายผู้ออกเอกสาร และหลายผู้ตรวจสอบเอกสาร โดยใช้มาตรฐานกลางที่เกี่ยวข้อง เพื่อให้ประชาชนสามารถจัดเก็บ แสดง และใช้เอกสารรับรองดิจิทัลได้อย่างต่อเนื่องในระบบนิเวศเดียวกันหรือระบบที่สามารถทำงานร่วมกันได้

3.5) ประเภทโครงสร้างพื้นฐานที่ควรพิจารณาใช้ร่วมกัน
ตัวอย่างโครงสร้างพื้นฐานสำคัญ ได้แก่

- ระบบทะเบียนผู้ออกเอกสาร (Issuer Registry)
- ระบบเผยแพร่ข้อมูลความเชื่อถือและกุญแจสาธารณะ (Trust Registry / PKI)
- ระบบบัญชีรายชื่อหน่วยงานที่ได้รับความเชื่อถือ (Trust List)
- ระบบระบุตัวตนดิจิทัลและ DID/Resolver
- กลไกการตรวจสอบสถานะ (Credential Status)
- ระบบตรวจสอบ VC/VP ข้ามหน่วยงาน
- กลไกการเชื่อมโยงข้อมูล (Interoperability / Protocol Layer)
- กระเป๋าดิจิทัล (Digital Wallet)

3.6) แนวทางการพัฒนาแพลตฟอร์มในระดับประเทศ (โดยสรุป)
ในกรณีที่หน่วยงานมีความประสงค์จะพัฒนาแพลตฟอร์มที่มีศักยภาพเป็นแพลตฟอร์มกลาง ควรดำเนินการโดยสรุป ดังนี้

3.6.1) จัดทำรายละเอียดแพลตฟอร์ม
ระบุวัตถุประสงค์ ขอบเขตการใช้งาน กลุ่มผู้ใช้ โครงสร้างการเชื่อมโยง มาตรการด้านความมั่นคงปลอดภัย และเหตุผลความจำเป็น

3.6.2) ยื่นคำขอขึ้นทะเบียนต่อหน่วยงานรับผิดชอบด้านมาตรฐานดิจิทัลภาครัฐ
เพื่อพิจารณาความครบถ้วน ความซ้ำซ้อน และความสอดคล้องกับกรอบโครงสร้างพื้นฐานกลาง

3.6.3) การกลั่นกรองโดยคณะอนุกรรมการที่เกี่ยวข้อง
ประเมินความเหมาะสม ผลกระทบ และความสอดคล้องกับยุทธศาสตร์ดิจิทัลภาครัฐ

3.6.4) เสนอคณะกรรมการพัฒนารัฐบาลดิจิทัลเพื่อพิจารณา
หากเห็นชอบ จะมีการประกาศรับรองเป็นแพลตฟอร์มกลางภาครัฐตามกระบวนการที่กำหนด

3.6.5) ดำเนินการตามเงื่อนไขที่กำหนด
หน่วยงานควรปฏิบัติตามข้อกำหนดด้านมาตรฐาน ความมั่นคงปลอดภัย และการเชื่อมโยงข้อมูลอย่างต่อเนื่อง

4) ด้านความน่าเชื่อถือและการกำกับดูแล (Trust and Governance)
หน่วยงานควรกำหนดกลไกด้านความน่าเชื่อถือและการกำกับดูแล เช่น

- การลงลายมือชื่ออิเล็กทรอนิกส์
- การบริหารจัดการกุญแจดิจิทัล
- การตรวจสอบสถานะเอกสาร (เช่น การระงับหรือเพิกถอน)
- การกำหนดบทบาทและความรับผิดชอบของผู้ที่เกี่ยวข้อง

เพื่อสร้างความเชื่อมั่นในการใช้งานในระดับระบบนิเวศ

แนวทางทั้ง 4 ด้านดังกล่าวเป็นกรอบสำหรับหน่วยงานของรัฐในการวางแผนและดำเนินการพัฒนาระบบเอกสาร VC/VP อย่างเป็นระบบ โดยครอบคลุมทั้งมิติของข้อมูล กระบวนการ เทคโนโลยี และการกำกับดูแล

ทั้งนี้ ในทางปฏิบัติ การดำเนินการควรเริ่มจากการวิเคราะห์ปัญหาและข้อจำกัดของระบบเดิม รวมถึงการเลือกเอกสารที่เหมาะสม ก่อนเข้าสู่ขั้นตอนการออกแบบและพัฒนาระบบในบทถัดไป

3. แนวทางการดำเนินการสำหรับหน่วยงานของรัฐในการประยุกต์ใช้ VC/VP

บทนี้มุ่งเน้นการนำเสนอแนวทางการดำเนินการสำหรับหน่วยงานของรัฐในการประยุกต์ใช้เอกสารรับรองดิจิทัล VC/VP โดยมีวัตถุประสงค์เพื่อให้หน่วยงานสามารถนำแนวคิดและกรอบมาตรฐานที่เกี่ยวข้องไปใช้ในการพัฒนาและปรับปรุงกระบวนการออกใบอนุญาตและเอกสารภาครัฐได้อย่างเป็นรูปธรรม

แม้ว่าปัจจุบันหน่วยงานของรัฐได้มีการจัดทำเอกสารในรูปแบบอิเล็กทรอนิกส์แล้ว โดยเฉพาะเอกสารใบอนุญาตในรูปแบบไฟล์ดิจิทัลที่มีการลงลายมือชื่ออิเล็กทรอนิกส์ แต่รูปแบบดังกล่าวยังมีข้อจำกัดในด้านการตรวจสอบแบบอัตโนมัติ การใช้งานข้ามหน่วยงาน และการควบคุมการเปิดเผยข้อมูลตามความจำเป็น ซึ่งส่งผลให้การให้บริการดิจิทัลยังไม่สามารถดำเนินการได้อย่างเต็มประสิทธิภาพ

การนำ VC/VP มาใช้จึงเป็นแนวทางในการยกระดับรูปแบบเอกสารภาครัฐให้สามารถตรวจสอบได้ด้วยกลไกทางเทคโนโลยี ลดการพึ่งพาการเชื่อมต่อระบบแบบเฉพาะโครงการ และสนับสนุนการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานได้อย่างมีประสิทธิภาพมากยิ่งขึ้น อย่างไรก็ตาม การดำเนินการดังกล่าวจำเป็นต้องอาศัยการวางแผนและดำเนินการอย่างเป็นระบบ โดยครอบคลุมตั้งแต่การวิเคราะห์ปัญหา การเลือกเอกสารที่เหมาะสม การกำหนดบทบาทของหน่วยงานที่เกี่ยวข้อง การประเมินความพร้อม ไปจนถึงการออกแบบ พัฒนา และนำระบบไปใช้งานจริง

ดังนั้น บทนี้จึงนำเสนอแนวทางการดำเนินการในลำดับขั้นที่หน่วยงานของรัฐสามารถนำไปประยุกต์ใช้ได้จริง โดยเริ่มจากการวิเคราะห์ปัญหาและอุปสรรคของรูปแบบเอกสารในปัจจุบัน และต่อเนื่องไปสู่การกำหนดแนวทางในการพัฒนาและนำ VC/VP ไปใช้งานในระดับหน่วยงาน

3.1 ปัญหาและข้อจำกัดของเอกสารอิเล็กทรอนิกส์แบบเดิม

แม้ใบอนุญาตภาครัฐจำนวนมากได้พัฒนาในรูปแบบอิเล็กทรอนิกส์แล้ว แต่การตรวจสอบและการใช้งานยังมีข้อจำกัดในเชิงกระบวนการและโครงสร้างพื้นฐาน โดยสามารถพิจารณาได้ทั้งในมุมของหน่วยงานของรัฐ และในมุมของประชาชนหรือผู้ประกอบการ ดังนี้

1) ในมุมของหน่วยงานของรัฐ

1.1) ความท้าทายในการตรวจสอบความถูกต้องของเอกสาร
หน่วยงานผู้ตรวจสอบเอกสารมักต้องพึ่งพาการพิจารณาด้วยสายตา การตรวจสอบกับฐานข้อมูลภายใน หรือการสอบถามกลับไปยังผู้ออกเอกสาร ทำให้กระบวนการตรวจสอบขาดความคล่องตัว และไม่สามารถตรวจสอบความถูกต้องครบถ้วนของข้อมูลด้วยกระบวนการเข้ารหัสลับได้โดยตรง

1.2) ข้อจำกัดในการบริหารสถานะใบอนุญาต
เมื่อมีการระงับหรือเพิกถอนใบอนุญาต การเปลี่ยนแปลงสถานะอาจไม่สะท้อนถึงผู้ตรวจสอบในทันที หากไม่มีกลไกการตรวจสอบสถานะที่เป็นมาตรฐานเดียวกัน ส่งผลให้เกิดช่องว่างระหว่างคำสั่งทางปกครองกับการบังคับใช้

1.3) ความซ้ำซ้อนของระบบและการพัฒนาเฉพาะหน่วยงาน
การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานมักต้องพัฒนาเชื่อมโยงแบบเฉพาะโครงการ ทำให้เกิดภาระในการพัฒนาระบบซ้ำซ้อน และขาดโครงสร้างพื้นฐานด้านความน่าเชื่อถือที่ใช้ร่วมกัน

1.4) ความท้าทายด้านการกำกับดูแลและความมั่นคงปลอดภัย
หน่วยงานต้องรับผิดชอบความถูกต้องของใบอนุญาต แต่ในรูปแบบเอกสารทั่วไป อาจไม่สามารถตรวจพบการแก้ไขข้อมูลได้โดยอัตโนมัติ ส่งผลต่อความน่าเชื่อถือของระบบโดยรวม

2) ในมุมของประชาชนและผู้ประกอบการ

2.1) ภาระในการแสดงเอกสารและยืนยันความถูกต้อง
ประชาชนหรือผู้ประกอบการต้องแสดงเอกสารในรูปแบบไฟล์หรือสำเนา ซึ่งผู้ตรวจสอบอาจต้องสอบถามกลับผู้ออกเอกสาร ทำให้กระบวนการใช้สิทธิหรือประกอบกิจการเกิดความล่าช้า

2.2) การเปิดเผยข้อมูลเกินความจำเป็น
การแสดงใบอนุญาตในรูปแบบเอกสารทั่วไปมักเปิดเผยข้อมูลทั้งหมด แม้ว่าผู้ตรวจสอบต้องการเพียงบางส่วน ทำให้ไม่สอดคล้องกับหลักการคุ้มครองข้อมูลส่วนบุคคล และไม่รองรับการเลือกเปิดเผยข้อมูลบางส่วน

2.3) ความไม่ชัดเจนของสถานะเอกสาร
ในกรณีที่ใบอนุญาตหมดอายุหรือถูกระงับ ผู้ถือเอกสารอาจไม่ทราบว่าการแสดงเอกสารเดิมยังมีผลหรือไม่ และผู้ตรวจสอบอาจไม่สามารถตรวจสอบสถานะได้ทันที

2.4) ความซับซ้อนในการใช้งานข้ามหน่วยงาน
เมื่อจำเป็นต้องใช้ใบอนุญาตกับหลายหน่วยงาน ผู้ถือเอกสารอาจต้องส่งสำเนาหลายครั้ง หรืออัปโหลดข้อมูลซ้ำซ้อน เนื่องจากไม่มีระบบที่รองรับการแสดงเอกสารสำแดงดิจิทัลอย่างเป็นมาตรฐานเดียวกัน

จากปัญหาและอุปสรรคทั้งสองมุมมองดังกล่าว จึงเห็นความจำเป็นในการพัฒนาแนวทางที่ช่วยให้เอกสารสามารถตรวจสอบความถูกต้องได้ด้วยกระบวนการเข้ารหัสลับ รองรับการเลือกเปิดเผยข้อมูลบางส่วน และเชื่อมโยงกับโครงสร้างพื้นฐานด้านความน่าเชื่อถือที่ใช้ร่วมกันระหว่างหน่วยงาน

3.2 การเลือกเอกสารสำหรับการประยุกต์ใช้ในรูปแบบ VC/VP

การนำใบอนุญาตภาครัฐมาจัดทำในรูปแบบเอกสารรับรองดิจิทัล VC/VP ภายใต้มาตรฐานฉบับนี้ มิได้มีวัตถุประสงค์เพื่อปรับเปลี่ยนโครงสร้างกระบวนการอนุญาตของหน่วยงานโดยสิ้นเชิง หากแต่เป็นการยกระดับ “รูปแบบของผลลัพธ์เอกสาร” (Output Layer) ให้สอดคล้องกับแนวคิดเอกสารรับรองดิจิทัล

ตามมาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล ว่าด้วยแนวปฏิบัติกระบวนการทางดิจิทัลภาครัฐ – ส่วนที่ 1 (มสพร 6-1) ได้กำหนดกรอบกระบวนการทางดิจิทัลภาครัฐไว้จำนวน 8 กระบวนการ ซึ่งครอบคลุมวงจรชีวิตการให้บริการภาครัฐตั้งแต่ต้นจนจบ โดยมาตรฐานฉบับนี้ไม่ได้กำหนดให้หน่วยงานต้องปรับเปลี่ยนกระบวนการดังกล่าว หน่วยงานยังสามารถดำเนินการตามกรอบเดิมได้ เช่น

- การรับคำขอผ่านช่องทางดิจิทัล
- การพิสูจน์และยืนยันตัวตน
- การตรวจสอบคุณสมบัติและพิจารณาอนุมัติ
- การชำระเงิน

อย่างไรก็ตาม ในขั้นตอน “การจัดทำและส่งมอบเอกสารใบอนุญาต” หน่วยงานสามารถกำหนดให้มีการออกเอกสารในรูปแบบ VC เป็นทางเลือกเพิ่มเติมจากรูปแบบเอกสารดิจิทัลทั่วไป เช่น ไฟล์ PDF หรือเอกสารอิเล็กทรอนิกส์ตามแนวทางเดิม

การนำ VC/VP มาใช้จึงเป็นการปรับปรุงเฉพาะส่วนของผลลัพธ์เอกสาร โดยมีวัตถุประสงค์เพื่อเพิ่มศักยภาพของเอกสารดิจิทัลในประเด็นสำคัญ ได้แก่

- เพิ่มความสามารถในการตรวจสอบความถูกต้องด้วยกระบวนการเข้ารหัสลับ
- เพิ่มความสามารถในการบริหารสถานะใบอนุญาตอย่างเป็นระบบ
- รองรับการใช้งานข้ามหน่วยงานโดยไม่ต้องพัฒนาเชื่อมต่อแบบเฉพาะโครงการ
- สนับสนุนการคุ้มครองข้อมูลส่วนบุคคลผ่านกลไก Selective Disclosure

ทั้งนี้ แม้การปรับเปลี่ยนจะอยู่ในช่วงท้ายของกระบวนการ แต่การออกเอกสารในรูปแบบ VC จำเป็นต้องมีการออกแบบระบบและกลไกที่รองรับอย่างเหมาะสม เช่น

- โครงสร้างข้อมูลของ VC ที่สอดคล้องกับมาตรฐาน
- การลงลายมือชื่ออิเล็กทรอนิกส์ของผู้ออก
- กลไกการบริหารสถานะ (ระงับ เพิกถอน หมดอายุ)
- ความสามารถของผู้ตรวจสอบในการตรวจสอบ VC/VP ได้โดยอิสระ

ดังนั้น หน่วยงานควรพิจารณาเลือกเอกสารหรือใบอนุญาตที่เหมาะสมสำหรับการจัดทำในรูปแบบ VC อย่างเป็นระบบ โดยพิจารณาจากระดับความเสี่ยง ผลกระทบเชิงกำกับดูแล และลักษณะการใช้งาน มิใช่พิจารณาเพียงความสะดวกด้านเทคโนโลยี

เอกสารที่ควรได้รับการพิจารณาเป็นลำดับแรก ได้แก่ เอกสารที่มีคุณลักษณะอย่างน้อยหนึ่งในประเด็นต่อไปนี้

1) มีความสำคัญตามกฎหมายและการกำกับดูแล โดยเอกสารควรได้รับการพิจารณา หาก
   - มีผลทางกฎหมายต่อสิทธิหรือหน้าที่ของบุคคล
   - มีโอกาสถูกระงับหรือเพิกถอนระหว่างอายุใบอนุญาต
   - ต้องใช้ในการกำกับดูแลเชิงรุก

   เหตุผลเนื่องจาก VC รองรับกลไกการตรวจสอบสถานะ ซึ่งเหมาะกับเอกสารที่ “สถานะเปลี่ยนแปลงได้”

2) มีความเสี่ยงด้านความถูกต้องและการปลอมแปลง โดยเอกสารควรได้รับการพิจารณา หาก
   - มีความเสี่ยงต่อการปลอมแปลงสูง
   - มีมูลค่าทางเศรษฐกิจ
   - มีผลกระทบต่อความปลอดภัยสาธารณะ

   เหตุผลเนื่องจาก VC ช่วยตรวจสอบความครบถ้วนของข้อมูลด้วยกระบวนการเข้ารหัสลับ

3) ความจำเป็นในการทำงานร่วมกัน (Interoperability Impact) โดยเอกสารควรได้รับการพิจารณา หาก

- ต้องใช้ข้ามหน่วยงาน
- ต้องใช้กับทั้งภาครัฐและเอกชน
- ปัจจุบันต้องพัฒนา API หรือระบบเชื่อมต่อเฉพาะโครงการจำนวนมาก

เหตุผลเนื่องจาก VC ช่วยลดภาระการเชื่อมต่อแบบจุดต่อจุด (Point-to-Point Integration)

4) หลักการคุ้มครองข้อมูลส่วนบุคคล โดยเอกสารควรได้รับการพิจารณา หาก

- มีข้อมูลหลายประเภทในเอกสารเดียว
- ไม่จำเป็นต้องเปิดเผยข้อมูลทั้งหมดทุกครั้ง
- มีข้อกำหนดด้าน Data Minimization

เหตุผลเนื่องจาก VC รองรับการเปิดเผยข้อมูลเฉพาะส่วน (Selective Disclosure)

3.3 โครงสร้างบทบาท

การพัฒนาใบอนุญาตภาครัฐในรูปแบบเอกสาร VC/VP จำเป็นต้องกำหนดบทบาทของผู้เกี่ยวข้องในระบบนิเวศของเอกสารรับรองให้ชัดเจน เพื่อให้การดำเนินงานเป็นไปอย่างมีความรับผิดชอบ โปร่งใส และสอดคล้องกับกรอบบริการเกี่ยวกับระบบเอกสารรับรอง (VC Trust Framework) โดยบทบาทหลักในระบบ ได้แก่

1) ผู้ออกเอกสาร (Issuer)

ผู้ออกเอกสาร คือ เอนทิตีที่มีอำนาจตามกฎหมายในการรับรองข้อความยืนยัน และออกเป็นเอกสารรับรองดิจิทัล (VC) ให้แก่ผู้ถือเอกสาร ซึ่งมีความรับผิดชอบหลักคือ

1.1) กำหนดโครงสร้างข้อมูลและข้อความยืนยันของ VC

1.2) ตรวจสอบคุณสมบัติของผู้ขอใบอนุญาตตามกฎหมาย

1.3) ออก VC พร้อมลงลายมือชื่ออิเล็กทรอนิกส์

1.4) บริหารจัดการสถานะของใบอนุญาตผ่านกลไกการตรวจสอบสถานะ

1.5) เก็บรักษาหลักฐานการดำเนินการตามกระบวนการ

ผู้ออกเอกสารเป็นผู้รับผิดชอบสูงสุดต่อความถูกต้องของข้อมูลใน VC

2) ผู้ถือเอกสาร (Holder)

ผู้ถือเอกสาร คือ เอนทิตีที่เป็นเจ้าของ VC อย่างน้อยหนึ่งชุด และจัดเก็บไว้ในกระเป๋าดิจิทัล (Digital Wallet) ซึ่งมีความรับผิดชอบหลักคือ

2.1) จัดเก็บ VC อย่างมั่นคงปลอดภัย

2.2) ใช้ VC สร้างเอกสารสำแดงดิจิทัล (VP)

2.3) ควบคุมการเลือกเปิดเผยข้อมูลบางส่วน

2.4) ปฏิบัติตามเงื่อนไขของใบอนุญาต

ผู้ถือเอกสารมีบทบาทสำคัญในการควบคุมข้อมูลของตนเองตามหลัก Holder-Controlled Model

3) ผู้ตรวจสอบเอกสาร (Verifier)

ผู้ตรวจสอบเอกสาร คือ เอนทิตีที่ทำหน้าที่ตรวจสอบความถูกต้องครบถ้วนของ VC และ VP ด้วยกระบวนการเข้ารหัสลับ ซึ่งมีความรับผิดชอบหลักคือ

3.1) ตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ของผู้ออกเอกสารและผู้ถือเอกสาร

3.2) ตรวจสอบความครบถ้วนของข้อมูลตามโครงสร้าง VC และ VP

3.3) ตรวจสอบสถานะผ่านกลไกการตรวจสอบสถานะ

3.4) บันทึกผลการตรวจสอบตามแนวปฏิบัติที่กำหนด

ผู้ตรวจสอบเอกสารเป็นผู้ตัดสินใจยอมรับหรือปฏิเสธเอกสารในทางปฏิบัติ

4) ผู้ให้บริการกระเป๋าดิจิทัล (Digital Wallet Provider)

ผู้ให้บริการกระเป๋าดิจิทัล คือ เอนทิตีที่พัฒนาและ/หรือดำเนินการเกี่ยวกับกระเป๋าดิจิทัลให้แก่ผู้ออกเอกสาร ผู้ถือเอกสาร หรือผู้ตรวจสอบเอกสาร ซึ่งมีความรับผิดชอบหลักคือ

4.1) พัฒนาและดูแลระบบให้สอดคล้องกับมาตรฐานที่เกี่ยวข้อง

4.2) จัดเก็บ VC อย่างมั่นคงปลอดภัย

4.3) รองรับการสร้าง VP ตามมาตรฐาน

4.4) ป้องกันการเข้าถึงหรือแก้ไขข้อมูลโดยไม่ได้รับอนุญาต

ผู้ให้บริการกระเป๋าดิจิทัลเป็นผู้สนับสนุนกลไกทางเทคนิค แต่ไม่เป็นเจ้าของข้อมูลใน VC

5) ผู้ให้บริการโครงสร้างพื้นฐานด้านความน่าเชื่อถือ (Trust Infrastructure Provider)

ผู้ให้บริการโครงสร้างพื้นฐานด้านความน่าเชื่อถือ หมายถึง ผู้ให้บริการกลไกหรือระบบที่สนับสนุนการตรวจสอบความถูกต้องของเอกสารรับรองดิจิทัล โดยอาจมีองค์ประกอบ ได้แก่

5.1) ระบบทะเบียนผู้ออกเอกสาร

5.2) ระบบบริหารกุญแจดิจิทัล

5.3) กลไกการตรวจสอบสถานะ

5.4) ระบบเผยแพร่ข้อมูลที่เกี่ยวข้องกับความเชื่อถือ

โครงสร้างพื้นฐานดังกล่าวทำหน้าที่สนับสนุนการตรวจสอบ แต่ไม่เกี่ยวข้องกับสาระของใบอนุญาตโดยตรง

6) หน่วยงานกำหนดกรอบบริการเกี่ยวกับระบบเอกสารรับรอง (VC Trust Framework Agency)

หน่วยงานกำหนดกรอบบริการเกี่ยวกับระบบเอกสารรับรอง กำหนดบทบาท หน้าที่ และกระบวนการปฏิบัติงานที่จำเป็นในการสร้างความเชื่อมั่นในระบบนิเวศของเอกสารรับรอง โดยกรอบดังกล่าวช่วยกำหนด

6.1) แนวทางการทำงานร่วมกันระหว่างบทบาทต่าง ๆ

6.2) หลักเกณฑ์การขึ้นทะเบียนหรือรับรองหน่วยงาน

6.3) แนวทางด้านความมั่นคงปลอดภัย

6.4) แนวทางการประเมินความสอดคล้องเพื่อให้การดำเนินงานเกี่ยวกับเอกสาร VC/VP มีความชัดเจนในเชิงบทบาทและความรับผิดชอบ มาตรฐานฉบับนี้กำหนดกรอบการจัดสรรหน้าที่ระหว่างหน่วยงานของรัฐที่ทำหน้าที่เป็น ผู้ออกเอกสาร (Issuer) และหน่วยงานของรัฐที่ทำหน้าที่เป็นผู้ตรวจเอกสารสำแดง (Verifier) โดยการกำหนดความรับผิดชอบดังกล่าวมุ่งเน้นเฉพาะกระบวนการตามวงจรชีวิตของ VC/VP ได้แก่ การออกเอกสาร การบริหารสถานะ และการตรวจสอบเอกสาร โดยไม่ครอบคลุมบทบาทอื่นในระบบนิเวศ

ตารางต่อไปนี้แสดงตัวอย่างการจัดสรรความรับผิดชอบ โดยกำหนดให้ R (Responsible) คือ ผู้ปฏิบัติงาน หรือผู้ดำเนินการ และ A (Accountable) คือ ผู้รับผิดชอบผลลัพธ์หรือผู้มีอำนาจตัดสินใจ เพื่อให้เห็นความแตกต่างระหว่าง

- ความรับผิดชอบในการ “สร้างและรับรองเอกสาร” ซึ่งอยู่ภายใต้ผู้ออก VC
- ความรับผิดชอบในการ “ตรวจสอบและตัดสินใจยอมรับเอกสาร” ซึ่งอยู่ภายใต้ผู้ตรวจสอบ VP

การกำหนดบทบาทอย่างชัดเจนช่วยลดความกำกวมในการปฏิบัติ เสริมความโปร่งใสในการกำกับดูแล และรองรับการตรวจสอบย้อนกลับในบริบทภาครัฐ

ตารางที่ 1 ตัวอย่างการกำหนดความรับผิดชอบของหน่วยงานของรัฐในการประยุกต์ใช้ VC/VP

กิจกรรม	**หน่วยงานของรัฐ ผู้ออกเอกสาร VC**	**หน่วยงานของรัฐ ผู้ตรวจสอบเอกสาร VP**
1. กำหนดรูปแบบและข้อมูลของ VC	R/A	-
2. ตรวจสอบคุณสมบัติและอนุมัติการออกใบอนุญาต	R/A	-
3. ออก VC และลงลายมือชื่ออิเล็กทรอนิกส์	R/A	-
4. บริหารจัดการสถานะ (ระงับ / เพิกถอน / หมดอายุ)	R/A	-
5. รับเอกสารสำแดงดิจิทัล VP จากผู้ถือเอกสาร เพื่อการตรวจสอบ	-	R
6. ตรวจสอบลายมือชื่อและความครบถ้วนของ VP	-	R
7. ตรวจสอบสถานะใบอนุญาตผ่านกลไกที่กำหนด	-	R
8. ตัดสินใจยอมรับหรือปฏิเสธเอกสาร	-	R/A
9. บันทึกผลการตรวจสอบตามกระบวนการ	-	R

3.4 การวิเคราะห์ช่องว่าง (Gap Analysis)

เมื่อหน่วยงานได้กำหนดบทบาทและความรับผิดชอบของผู้ที่เกี่ยวข้องในระบบเอกสารรับรองดิจิทัลแล้ว ขั้นตอนถัดไปคือการดำเนินการพัฒนาและนำระบบไปใช้งานอย่างเป็นระบบตามหลักการพัฒนาระบบสารสนเทศ (System Development Life Cycle: SDLC)

การพัฒนาในระยะนี้ครอบคลุมตั้งแต่การวิเคราะห์ช่องว่างของระบบเดิม การออกแบบและพัฒนาระบบให้รองรับการออกและตรวจสอบเอกสารในรูปแบบ VC/VP ตลอดจนการทดสอบ การเตรียมความพร้อม และการนำไปใช้งานจริงในระดับหน่วยงาน

แนวทางดังกล่าวมีวัตถุประสงค์เพื่อให้หน่วยงานสามารถยกระดับใบอนุญาตภาครัฐสู่รูปแบบเอกสารรับรองดิจิทัลได้อย่างเป็นระบบ โดยยังคงสอดคล้องกับกรอบกระบวนการทางดิจิทัลภาครัฐตามมาตรฐาน มสพร 6-1 และกรอบมาตรฐานที่เกี่ยวข้องในระดับประเทศ

ในส่วนนี้จึงนำเสนอแนวทางการดำเนินการในลำดับขั้นของการพัฒนา ได้แก่ การวิเคราะห์ช่องว่าง (Gap Analysis) การออกแบบและพัฒนา (Design and Development) และการเตรียมความพร้อมและการนำไปใช้งาน (Operational Readiness and Deployment) เพื่อให้หน่วยงานสามารถนำไปประยุกต์ใช้ได้อย่างเป็นรูปธรรม

การวิเคราะห์ช่องว่างมีวัตถุประสงค์เพื่อให้หน่วยงานเข้าใจว่า “ต้องปรับอะไร” ก่อนนำ VC และ VP มาใช้จริง โดยสามารถพิจารณาตามกรณีที่พบบ่อยดังต่อไปนี้

1) กรณีผู้ออกเอกสารที่ยังใช้ไฟล์เอกสารทั่วไป (เช่น PDF)

สภาพปัจจุบัน (AS-IS)

- ออกใบอนุญาตในรูปแบบไฟล์เอกสาร
- การตรวจสอบต้องอาศัยการพิจารณาด้วยสายตา หรือสอบถามกลับ
- ไม่มีระบบตรวจสอบสถานะแบบเรียลไทม์

ช่องว่าง (GAP)

- ไม่สามารถตรวจสอบความถูกต้องครบถ้วนด้วยกระบวนการเข้ารหัสลับ (Cryptographic Verification)
- ไม่มีโครงสร้างข้อมูล (Structured Data) ที่เป็นมาตรฐาน
- ไม่รองรับการเลือกเปิดเผยข้อมูลบางส่วน (Selective Disclosure)

แนวทางปรับเปลี่ยน (TO-BE)

- ออกเอกสารในรูปแบบ VC
- จัดให้มีกลไกการตรวจสอบสถานะ (Revocation/Status Check)
- กำหนด Schema ที่สอดคล้องกับมาตรฐาน
- เชื่อมโยงกับโครงสร้างพื้นฐานด้านความน่าเชื่อถือของประเทศ

2) กรณีผู้ออกเอกสารที่มีระบบ Digital ID และ Wallet แล้ว แต่ยังไม่เป็น VC

สภาพปัจจุบัน (AS-IS)

- มีระบบพิสูจน์และยืนยันตัวตนดิจิทัล
- มีระบบจัดเก็บเอกสารในลักษณะคล้าย wallet
- เอกสารยังไม่อยู่ในรูปแบบ VC ตามมาตรฐานสากล

ช่องว่าง (GAP)

- โครงสร้างข้อมูลไม่สอดคล้องกับ W3C VC Data Model
- ไม่รองรับการสร้าง VP ตามมาตรฐาน
- การตรวจสอบยังต้องเชื่อมต่อ API เฉพาะของแต่ละหน่วยงาน

แนวทางปรับเปลี่ยน (TO-BE)

- ปรับโครงสร้างข้อมูลให้สอดคล้องกับมาตรฐาน VC
- รองรับการสร้าง VP เพื่อการแสดงเอกสารสำแดง
- ใช้กลไกตรวจสอบสถานะที่เป็นมาตรฐานเดียวกัน

3) กรณีผู้ตรวจสอบเอกสารที่รับเอกสารในรูปแบบไฟล์

สภาพปัจจุบัน (AS-IS)

- รับเอกสารเป็นไฟล์แนบหรือสำเนา
- ต้องสอบถามกลับผู้ออกเอกสารในบางกรณี

ช่องว่าง (GAP)

- ไม่สามารถตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ของ VC ได้โดยอัตโนมัติ
- ไม่มีระบบตรวจสอบสถานะโดยตรง

แนวทางปรับเปลี่ยน (TO-BE)

- พัฒนาระบบรองรับการตรวจสอบ VC และ VP
- เชื่อมต่อกับกลไกการตรวจสอบสถานะ
- กำหนดแนวทางยอมรับเอกสารสำแดงดิจิทัลอย่างเป็นทางการ

4) กรณีผู้ตรวจสอบที่มี API เชื่อมฐานข้อมูลเดิมอยู่แล้ว

สภาพปัจจุบัน (AS-IS)

- ตรวจสอบผ่าน API ของผู้ออกเอกสาร
- ผูกติดกับระบบเฉพาะหน่วยงาน

ช่องว่าง (GAP)

- ไม่สามารถทำงานแบบกระจายศูนย์ (Decentralized Verification)
- ต้องพัฒนา integration เฉพาะโครงการสำหรับแต่ละหน่วยงาน

แนวทางปรับเปลี่ยน (TO-BE)

- รองรับการตรวจสอบ VC โดยไม่ต้องเรียก API ต้นทางทุกครั้ง
- ใช้กลไกการตรวจสอบสถานะร่วม
- ลดการพัฒนา Integration แบบ Point-to-Point

5) ช่องว่างระดับโครงสร้างพื้นฐานของประเทศ ในระดับประเทศ อาจพบว่า

สภาพปัจจุบัน (AS-IS)

- ไม่มีระบบทะเบียนผู้ออก (Issuer Registry) ที่ใช้ร่วมกัน
- ไม่มี Credential Status Mechanism กลาง
- wallet หลายรูปแบบและไม่ทำงานร่วมกัน

ช่องว่าง (GAP)

- การทำงานร่วมกันข้ามหน่วยงานมีข้อจำกัด
- ความเชื่อมั่นในระบบโดยรวมยังไม่เป็นมาตรฐานเดียว

แนวทางปรับเปลี่ยน (TO-BE)

- พัฒนาโครงสร้างพื้นฐานด้านความน่าเชื่อถือที่ใช้ร่วมกัน (Trust Infrastructure)
- กำหนดแนวทางขึ้นทะเบียนผู้ออกและผู้ให้บริการ
- สนับสนุน Wallet ที่ทำงานร่วมกันได้ตามมาตรฐานเดียวกัน

3.5 การออกแบบและพัฒนากระบวนการตามมาตรฐาน (Design and Development)

เมื่อหน่วยงานพิจารณาแล้วว่าเอกสารมีความเหมาะสมต่อการจัดทำในรูปแบบเอกสารรับรองดิจิทัล (VC) ขั้นตอนถัดไปคือการออกแบบและพัฒนาระบบให้รองรับการออก การบริหารสถานะ และการตรวจสอบ VC/VP อย่างเป็นระบบ ภายใต้กรอบแนวคิด SDLC

การพัฒนาในส่วนนี้ควรมุ่งเน้นประเด็นสำคัญดังต่อไปนี้

1) แนวทางการพัฒนาแยกตามบทบาท

1.1) ผู้ออกเอกสาร (Issuer) ควรดำเนินการดังนี้

1.1.1) กำหนดโครงสร้างข้อมูล (Schema) ของ VC
โดยอ้างอิง W3C Verifiable Credentials Data Model และแนวทางการออกแบบ Schema ที่สอดคล้องกับบริบทการแลกเปลี่ยนข้อมูลภาครัฐ เช่น มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ แนวปฏิบัติและหลักการพื้นฐานในการออกแบบมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านความหมายข้อมูล กรณีเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล โดยกำหนดรายการข้อมูล ข้อความยืนยัน (Claims) และคำอธิบายข้อมูล (Metadata) เท่าที่จำเป็นและเหมาะสมกับวัตถุประสงค์ของการออก การถือครอง การสำแดง และการตรวจสอบเอกสาร ทั้งนี้ ควรคำนึงถึงหลักการเปิดเผยข้อมูลเท่าที่จำเป็น การลดการประมวลผลข้อมูลส่วนบุคคลเกินจำเป็น และความสามารถในการเลือกเปิดเผยข้อมูลบางส่วน (Selective Disclosure) เพื่อสนับสนุนการคุ้มครองข้อมูลส่วนบุคคลและลดความเสี่ยงจากการเปิดเผยข้อมูลเกินวัตถุประสงค์

1.1.2) กำหนดกระบวนการออก VC
รองรับมาตรฐานที่เกี่ยวข้องกับการออกเอกสาร เช่น OpenID for Verifiable Credential Issuance (OID4VCI)

1.1.3) กำหนดกลไกการตรวจสอบสถานะ
เช่น Credential Status List เพื่อรองรับการระงับหรือเพิกถอนใบอนุญาต

1.1.4) เชื่อมโยงกับโครงสร้างพื้นฐานด้านความน่าเชื่อถือ
เช่น ระบบทะเบียนผู้ออกและการเผยแพร่กุญแจสาธารณะ

1.2) ผู้ตรวจสอบเอกสาร (Verifier) ควรดำเนินการดังนี้

1.2.1) พัฒนาความสามารถในการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ของ VC และ VP โดยอ้างอิงมาตรฐานด้าน Data Integrity

1.2.2) รองรับการรับ VP ผ่านมาตรฐานการส่งเอกสารสำแดง เช่น OpenID for Verifiable Presentations (OID4VP)

1.2.3) เชื่อมต่อกับกลไกการตรวจสอบสถานะ เพื่อยืนยันว่าใบอนุญาตยังมีผลบังคับใช้

1.2.4) กำหนดแนวทางการยอมรับเอกสาร

ควรกำหนดแนวปฏิบัติภายในสำหรับการรับ ตรวจสอบ และยอมรับหรือปฏิเสธเอกสารสำแดงดิจิทัล (VP) อย่างเป็นทางการ โดยกำหนดขั้นตอนการตรวจสอบ เงื่อนไขการยอมรับหรือปฏิเสธเอกสาร ผู้มีอำนาจตัดสินใจ และการบันทึกผลการตรวจสอบ เพื่อให้เจ้าหน้าที่สามารถปฏิบัติงานได้อย่างสอดคล้องกันและตรวจสอบย้อนหลังได้

1.2.5) กำหนดแนวทางการตรวจสอบ

ผู้ตรวจสอบเอกสารควรกำหนดแนวทางรองรับการตรวจสอบในกรณีออฟไลน์หรือพื้นที่สัญญาณต่ำ โดยอาจพิจารณาการตรวจสอบลายมือชื่อดิจิทัลจากข้อมูลในเอกสาร การใช้ข้อมูลสถานะหรือรายการเพิกถอนที่มีการซิงค์ไว้ล่วงหน้า และการตรวจสอบซ้ำเมื่อสามารถเชื่อมต่อระบบได้ ทั้งนี้ ควรกำหนดเงื่อนไขการยอมรับเอกสารให้เหมาะสมกับระดับความเสี่ยงของบริการ

1.3) ผู้ให้บริการกระเป๋าดิจิทัล (Digital Wallet Provider) ควรดำเนินการดังนี้

1.3.1) รองรับการจัดเก็บ VC อย่างมั่นคงปลอดภัย

1.3.2) รองรับการสร้าง VP และการเลือกเปิดเผยข้อมูลบางส่วน

1.3.3) สอดคล้องกับมาตรฐานการออกและการแสดง VC/VP

1.3.4) รองรับการทำงานร่วมกับหลายหน่วยงาน

1.3.5) ผู้ให้บริการกระเป๋าดิจิทัลควรกำหนดมาตรการคุ้มครองกุญแจส่วนตัว (Private Key) และข้อมูลที่ใช้ในการสร้างลายมือชื่อดิจิทัลหรือข้อพิสูจน์ (Proof) ของผู้ถือเอกสารอย่างเหมาะสม โดยครอบคลุมการจัดเก็บอย่างมั่นคงปลอดภัย การควบคุมการเข้าถึง การป้องกันการใช้งานโดยไม่ได้รับอนุญาต และการบริหารจัดการกุญแจตลอดวงจรชีวิต ทั้งนี้ ควรสอดคล้องกับมาตรฐานหรือแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้อง รวมถึงรายงานทางเทคนิคของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง กรอบการสร้างความน่าเชื่อถือของเอกสารรับรองและเอกสารสำแดง (Trust Model Framework) โดยเฉพาะข้อกำหนด VCTF-08 และ VCGF-1.2 ตลอดจนกรอบการทำงานร่วมกันของกระเป๋าดิจิทัลสำหรับเอกสารรับรองที่เกี่ยวข้อง

1.4) โครงสร้างพื้นฐานด้านความน่าเชื่อถือ (Trust Infrastructure) ควรดำเนินการดังนี้

1.4.1) มีระบบทะเบียนผู้ออก

1.4.2) มีกลไกการตรวจสอบสถานะที่ใช้ร่วมกัน

1.4.3) มีแนวทางการกำกับดูแลตามกรอบบริการเกี่ยวกับระบบเอกสารรับรอง

2) การเชื่อมโยงกับมาตรฐานและกรอบในประเทศ

แม้มาตรฐานหลักจะอ้างอิงจากมาตรฐานสากล เช่น W3C และ OpenID Foundation การพัฒนาควรสอดคล้องกับแนวทางที่หน่วยงานกำกับในประเทศกำหนด รวมถึงแนวทางการออกแบบข้อมูลที่เชื่อมโยงกับโครงสร้างการแลกเปลี่ยนข้อมูลภาครัฐ ซึ่งการดำเนินการดังกล่าวจะช่วยให้เอกสารรับรองดิจิทัลสามารถทำงานร่วมกันได้ทั้งภายในประเทศ และรองรับการพัฒนาในอนาคต

หมายเหตุ: ในการออกแบบและพัฒนาระบบเพื่อรองรับการออกเอกสารรับรองดิจิทัล หน่วยงานต้องกำหนดขอบเขตอำนาจหน้าที่และกลไกควบคุมภายในให้ชัดเจน โดยอย่างน้อยต้องกำหนดผู้มีอำนาจในการออก VC และผู้มีอำนาจในการเปลี่ยนแปลงสถานะของ VC อย่างเป็นทางการ รวมทั้งกำหนดเงื่อนไขและขั้นตอนการดำเนินการดังกล่าวให้สอดคล้องกับอำนาจตามกฎหมายและโครงสร้างการกำกับดูแลของหน่วยงาน นอกจากนี้ ต้องออกแบบกลไกป้องกันการออกหรือเปลี่ยนแปลงสถานะเอกสารโดยมิชอบ ตลอดจนกำหนดหลักเกณฑ์ที่ผู้ตรวจ (Verifier) ต้องใช้ในการพิจารณายอมรับหรือปฏิเสธ VC/VP เพื่อให้การดำเนินการเป็นไปตามหลักความถูกต้อง ความสม่ำเสมอ และสามารถตรวจสอบความสอดคล้องเชิงกระบวนการได้ในระดับระบบนิเวศ

3.6 ความพร้อมและการนำไปใช้งาน (Operational Readiness and Deployment)

ภายหลังจากการวิเคราะห์ช่องว่างและการออกแบบกระบวนการตามหลักการที่กำหนดแล้ว หน่วยงานควรดำเนินการเตรียมความพร้อมและนำระบบเอกสารรับรองดิจิทัลเข้าสู่การใช้งานจริงอย่างเป็นขั้นตอน เพื่อให้มั่นใจว่าการดำเนินงานสามารถให้บริการได้อย่างต่อเนื่อง มีเสถียรภาพ และสอดคล้องกับบทบาทของหน่วยงานในระบบนิเวศเอกสารรับรองดิจิทัล

การดำเนินการในระยะนี้มุ่งเน้นการยืนยันความพร้อมเชิงปฏิบัติ (operational readiness) มิใช่การรับรองเชิงมาตรฐานหรือการตรวจประเมินเชิงหลักฐาน

1) การทดสอบความพร้อมเชิงปฏิบัติการ

ก่อนเปิดใช้งานจริง หน่วยงานควรดำเนินการทดสอบกระบวนการที่เกี่ยวข้องกับวงจรชีวิตของเอกสารอย่างน้อยในประเด็นดังต่อไปนี้

1.1) การทดสอบการออกเอกสาร (Issuance)
- 1.1.1) ทดสอบการสร้าง VC จากข้อมูลตามกระบวนการปกติ
- 1.1.2) ตรวจสอบความครบถ้วนของข้อมูลและความสามารถในการตรวจสอบลายมือชื่อดิจิทัล

1.2) การทดสอบการแสดงเอกสาร (Presentation)
- 1.2.1) ทดสอบการสร้าง Verifiable Presentation (VP)
- 1.2.2) ทดสอบการเปิดเผยข้อมูลตามเงื่อนไขที่ออกแบบไว้

1.3) การทดสอบการตรวจสอบและสถานะ (Verification & Status)
- 1.3.1) ทดสอบการตรวจสอบความถูกต้องของ VC/VP
- 1.3.2) ทดสอบกลไกการตรวจสอบสถานะ เช่น การหมดอายุ การระงับ หรือการเพิกถอน

1.4) การทดสอบกรณีเหตุการณ์ผิดปกติ

1.4.1) กรณีสถานะถูกเพิกถอน

1.4.2) กรณีระบบบางส่วนไม่พร้อมใช้งาน

1.4.3) กรณีข้อมูลไม่ครบถ้วน

1.4.4) กรณีไม่สามารถเชื่อมต่อระบบตรวจสอบสถานะหรือระบบทะเบียนเอกสารรับรองได้ในขณะตรวจสอบ

1.4.5) กรณีพื้นที่ปฏิบัติงานมีสัญญาณอินเทอร์เน็ตต่ำหรือไม่เสถียร

การทดสอบดังกล่าวควรครอบคลุมทั้งกรณีปกติและกรณีข้อผิดพลาด เพื่อประเมินความสามารถของกระบวนการในการรองรับสถานการณ์จริง

2) การนำร่องในขอบเขตจำกัด (Pilot Implementation)

เพื่อบริหารความเสี่ยงและปรับปรุงกระบวนการก่อนเปิดใช้งานเต็มรูปแบบ หน่วยงานควรพิจารณาดำเนินโครงการนำร่องในขอบเขตจำกัด เช่น

- เลือกประเภทใบอนุญาตเฉพาะกลุ่ม
- จำกัดจำนวนผู้ถือเอกสารในระยะเริ่มต้น
- ทดลองใช้งานร่วมกับหน่วยงานผู้ตรวจสอบบางแห่ง

การนำร่องมีวัตถุประสงค์เพื่อ

- ประเมินความเข้าใจของเจ้าหน้าที่ผู้ปฏิบัติงาน
- ประเมินประสบการณ์ของผู้ถือเอกสาร
- ประเมินการทำงานร่วมกันระหว่างหน่วยงาน
- ระบุประเด็นที่ต้องปรับปรุงก่อนขยายผล

ผลจากการนำร่องควรถูกนำมาปรับปรุงกระบวนการและแนวปฏิบัติภายใน ก่อนเข้าสู่การเปิดใช้งานเต็มรูปแบบ

3) การประเมินความพร้อมก่อนเปิดใช้งาน (Go-Live Readiness)

ก่อนการเปิดใช้งานอย่างเป็นทางการ หน่วยงานควรพิจารณาความพร้อมในมิติต่อไปนี้

3.1) ความพร้อมด้านบทบาทและความรับผิดชอบ

- มีการกำหนดผู้รับผิดชอบในแต่ละช่วงของวงจรชีวิตเอกสาร
- มีผู้มีอำนาจในการเพิกถอนหรือระงับเอกสาร

3.2) ความพร้อมด้านกระบวนการ

- มีกลไกบริหารสถานะที่สามารถใช้งานได้จริง
- มีแนวปฏิบัติภายในและจัดให้มีการสื่อสารแก่เจ้าหน้าที่ผู้ตรวจสอบเกี่ยวกับกระบวนการ รับ ตรวจสอบ ยอมรับ ปฏิเสธ และบันทึกผลการตรวจสอบเอกสารสำแดงดิจิทัล (VP) เพื่อให้การปฏิบัติงานเป็นไปอย่างสอดคล้องกัน รวมทั้งกำหนดแนวทางดำเนินการในกรณีที่ผลการตรวจสอบไม่สมบูรณ์ ไม่สามารถยืนยันสถานะของเอกสารได้ หรือพบเหตุขัดข้องระหว่างการตรวจสอบ

3.3) ความพร้อมด้านโครงสร้างพื้นฐาน

- มีการเผยแพร่ข้อมูลความเชื่อถือที่จำเป็นต่อการตรวจสอบ
- มีกลไกบริหารกุญแจดิจิทัลที่เหมาะสม รวมถึงมาตรการคุ้มครองกุญแจส่วนตัว การควบคุมสิทธิการเข้าถึง การหมุนเวียน การระงับหรือเพิกถอนกุญแจ และการบันทึกเหตุการณ์ที่เกี่ยวข้อง

การประเมินดังกล่าวเป็นการพิจารณาภายในเพื่อยืนยันความสามารถในการให้บริการ มิใช่การรับรองความสอดคล้องตามเกณฑ์ภายนอก

4) การนำไปใช้งานและติดตามผล (Deployment and Monitoring)

เมื่อหน่วยงานพิจารณาว่ามีความพร้อมครบถ้วนแล้ว จึงสามารถดำเนินการเปิดใช้งานอย่างเป็นทางการ โดยควร

- ประกาศแนวปฏิบัติการใช้เอกสาร VC อย่างชัดเจน
- สื่อสารให้ผู้ถือเอกสารและผู้ตรวจสอบรับทราบ
- จัดเตรียมช่องทางรองรับข้อสงสัยหรือเหตุการณ์ผิดปกติ

หลังการเปิดใช้งาน ควรมีการติดตามผลการใช้งานอย่างต่อเนื่อง และทบทวนกระบวนการตามความเหมาะสม เพื่อให้สอดคล้องกับบริบทการใช้งานจริงและการเปลี่ยนแปลงของมาตรฐานที่เกี่ยวข้อง

3.7 การตรวจสอบและการประเมินความสอดคล้อง

การนำเอกสาร VC/VP มาใช้ในบริบทภาครัฐ จำเป็นต้องมีกลไกในการสร้างความน่าเชื่อถือของระบบ โดยแนวทางดังกล่าวไม่จำกัดเฉพาะการตรวจสอบระบบเชิงเทคนิค แต่ครอบคลุมถึงการกำกับดูแล (Governance) และการประเมินความสอดคล้อง (Conformity Assessment) ของผู้มีบทบาทในระบบเอกสารรับรองดิจิทัล

ทั้งนี้ แนวทางดังกล่าวสามารถอ้างอิงได้จากกรอบการสร้างความน่าเชื่อถือของเอกสารรับรองและเอกสารสำแดง (Trust Framework) ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) ซึ่งกำหนดหลักการเกี่ยวกับบทบาทของผู้มีส่วนเกี่ยวข้อง และแนวทางในการสร้างความเชื่อมั่นในระดับระบบนิเวศ

1) การกำกับดูแลและบทบาทในระบบ (Governance and Roles)

การดำเนินงานในระบบ VC/VP ควรมีการกำหนดบทบาทและความรับผิดชอบของผู้มีส่วนเกี่ยวข้องอย่างชัดเจน เช่น

- ผู้ออกเอกสาร (Issuer)
- ผู้ถือเอกสาร (Holder)
- ผู้ตรวจสอบเอกสาร (Verifier)
- ผู้ให้บริการกระเป๋าดิจิทัล (Wallet Provider)
- ผู้ให้บริการโครงสร้างพื้นฐานด้านความน่าเชื่อถือ

โดยแนวทางการกำหนดบทบาทดังกล่าวสอดคล้องกับกรอบ Trust Framework และแนวคิดที่เกี่ยวข้อง เช่น Trust Over IP ซึ่งใช้เป็นพื้นฐานในการกำหนดความสัมพันธ์และความรับผิดชอบในระบบ

2) การประเมินความสอดคล้องของหน่วยงาน (Organizational Conformity)

หน่วยงานของรัฐควรพิจารณาประเมินความสอดคล้องของการดำเนินงานของตนกับข้อกำหนดที่เกี่ยวข้อง โดยอาจพิจารณาประเด็น เช่น

- ความสอดคล้องของกระบวนการออกเอกสารกับอำนาจตามกฎหมาย
- การกำหนดและบริหารกลไกการตรวจสอบสถานะของเอกสาร
- การบริหารจัดการกุญแจดิจิทัลและการลงลายมือชื่ออิเล็กทรอนิกส์
- การจัดทำบันทึกหรือหลักฐานที่เกี่ยวข้องกับการดำเนินงาน
- การออกแบบ VC Schema มีการกำหนดข้อมูลเท่าที่จำเป็นต่อวัตถุประสงค์ของการใช้งาน และรองรับการลดการเปิดเผยข้อมูลเกินจำเป็นหรือการเลือกเปิดเผยข้อมูลบางส่วน (Selective Disclosure) ตามความเหมาะสม

โดยแนวทางดังกล่าวสอดคล้องกับหลักการด้านการกำกับดูแลการดำเนินงาน (Operational Governance) ตามกรอบของ ETDA

3) การประเมินความสามารถในการทำงานร่วมกัน (Interoperability Considerations)

หน่วยงานควรพิจารณาความสามารถของระบบในการทำงานร่วมกับหน่วยงานอื่น โดยอาจอ้างอิงแนวทางจากกรอบ VCGF ซึ่งมุ่งเน้นการสนับสนุนการทำงานร่วมกันในระดับระบบนิเวศ เช่น

- การรองรับมาตรฐานที่เกี่ยวข้องกับ VC และ VP
- ความสามารถในการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์
- ความสอดคล้องของกลไกการตรวจสอบสถานะของเอกสาร
- การเชื่อมโยงกับโครงสร้างพื้นฐานด้านความน่าเชื่อถือ

4) การประเมินในระดับผู้ให้บริการในระบบ (Ecosystem Considerations)

ในระดับระบบนิเวศ แนวทางของ ETDA กำหนดให้ผู้มีบทบาทในระบบควรสามารถแสดงความสอดคล้องกับข้อกำหนดที่เกี่ยวข้อง เพื่อสร้างความเชื่อมั่นในการใช้งานโดยอาจครอบคลุมผู้ให้บริการประเภทต่าง ๆ เช่น

- ผู้ออกเอกสาร (Issuer)
- ผู้ตรวจสอบเอกสาร (Verifier)
- ผู้ให้บริการกระเป๋าดิจิทัล
- ผู้ให้บริการโครงสร้างพื้นฐานด้านความน่าเชื่อถือ

โดยรายละเอียดของกลไกการประเมินความสอดคล้อง อาจเป็นไปตามกรอบและแนวทางที่กำหนดโดยหน่วยงานที่เกี่ยวข้องในระดับประเทศ

แนวทางการตรวจสอบในระบบ VC/VP ตามกรอบของ ETDA มีลักษณะเป็นการกำกับดูแลและการประเมินความสอดคล้องของผู้มีบทบาทในระบบ มากกว่าการตรวจสอบระบบสารสนเทศในรูปแบบดั้งเดิม โดยมุ่งเน้นให้เกิดความน่าเชื่อถือและการทำงานร่วมกันในระดับระบบนิเวศ

4. กรณีศึกษา

การพัฒนาใบอนุญาตภาครัฐในรูปแบบเอกสารรับรองดิจิทัล VC/VP เป็นแนวทางที่หลายประเทศได้เริ่มดำเนินการแล้ว ภายใต้กรอบมาตรฐานสากลและโครงสร้างพื้นฐานด้านความเชื่อถือของตนเอง การศึกษาแนวปฏิบัติจากต่างประเทศจึงมีความสำคัญ เพื่อทำความเข้าใจรูปแบบการกำกับดูแล กลไกความน่าเชื่อถือ และแนวทางการทำงานร่วมกันในระดับระบบนิเวศ

บทนี้จึงเริ่มต้นด้วยการนำเสนอกรอบแนวคิดและกรณีศึกษาจากต่างประเทศ ซึ่งสะท้อนให้เห็นแนวโน้มการกำหนดบทบาทของผู้ออกเอกสาร ผู้ถือเอกสาร และผู้ตรวจสอบ ตลอดจนการจัดตั้งโครงสร้างพื้นฐานด้านความน่าเชื่อถือในระดับชาติ จากนั้นจึงนำเสนอพัฒนาการและแนวทางดำเนินงานในประเทศไทย เพื่อเปรียบเทียบวิเคราะห์ และสังเคราะห์ประเด็นที่เหมาะสมต่อการประยุกต์ใช้ในบริบทภาครัฐไทย

การจัดลำดับเนื้อหาในลักษณะดังกล่าวมีวัตถุประสงค์เพื่อให้เห็นทั้งภาพรวมระดับสากลและบริบทเชิงระบบของประเทศไทยอย่างเชื่อมโยงกัน ไม่ใช่ในลักษณะการนำมาตรฐานต่างประเทศมาปรับใช้โดยตรง แต่เป็นการพิจารณาแนวคิด โครงสร้าง และกลไกที่สามารถปรับใช้ได้อย่างเหมาะสมกับกรอบกฎหมายและโครงสร้างการกำกับดูแลของประเทศ

4.1 กรณีศึกษาต่างประเทศ

4.1.1 กรณีศึกษา: สหภาพยุโรป (European Union Digital Identity Wallet: EUDI Wallet)

สหภาพยุโรปได้กำหนดกรอบการจัดการตัวตนดิจิทัลและเอกสารรับรองในรูปแบบดิจิทัลภายใต้กฎหมาย eIDAS 2.0 โดยมีเป้าหมายเพื่อให้ประชาชนในประเทศสมาชิกสามารถเข้าถึงและใช้บริการดิจิทัลได้อย่างปลอดภัย เชื่อถือได้ และสามารถใช้งานข้ามประเทศได้

ภายใต้กรอบดังกล่าว ได้มีการกำหนดให้ประเทศสมาชิกต้องจัดให้มี “กระเป๋าดิจิทัล” (Digital Identity Wallet หรือ EUDI Wallet) ซึ่งทำหน้าที่เป็นเครื่องมือสำหรับผู้ถือเอกสาร (Holder) ในการจัดเก็บและนำเสนอเอกสารรับรองในรูปแบบดิจิทัล เช่น บัตรประจำตัวประชาชน ใบอนุญาตขับขี่ ใบรับรองทางการศึกษา และเอกสารอื่นที่ออกโดยหน่วยงานภาครัฐหรือหน่วยงานที่ได้รับอนุญาต

1) ลักษณะทางสถาปัตยกรรม

EUDI Wallet ถูกออกแบบในลักษณะของ ecosystem ที่มีการกำหนดบทบาทของผู้มีส่วนเกี่ยวข้องอย่างชัดเจน ได้แก่

1.1) ผู้ออกเอกสาร (Issuer)
1.2) ผู้ถือเอกสาร (Holder)
1.3) ผู้ตรวจสอบเอกสาร (Verifier)
1.4) ผู้ให้บริการกระเป๋าดิจิทัล (Wallet Provider)
1.5) ผู้ให้บริการโครงสร้างพื้นฐานด้านความน่าเชื่อถือ (Trust Infrastructure Provider)

โดยการออกแบบดังกล่าวสอดคล้องกับแนวคิดของ VC ecosystem ที่แยกบทบาทหน้าที่อย่างชัดเจน และรองรับการทำงานร่วมกันระหว่างหลายหน่วยงาน

2) การใช้มาตรฐานสากล

ระบบ EUDI Wallet อ้างอิงมาตรฐานสากลที่เกี่ยวข้อง เช่น

2.1) W3C Verifiable Credentials Data Model

2.2) OpenID for Verifiable Credentials (OID4VCI / OID4VP)

2.3) มาตรฐานด้านการพิสูจน์ตัวตนและลายมือชื่อดิจิทัล

การใช้มาตรฐานดังกล่าวช่วยให้สามารถพัฒนาและใช้งานระบบได้โดยไม่ผูกติดกับเทคโนโลยีเฉพาะ (technology-agnostic) และรองรับการเชื่อมโยงกับระบบของประเทศอื่น

3) ความสามารถสำคัญของระบบ

ระบบ EUDI Wallet มีความสามารถที่สำคัญ ได้แก่

3.1) การออกเอกสารในรูปแบบ Verifiable Credential ที่สามารถตรวจสอบความถูกต้องได้

3.2) การนำเสนอข้อมูลผ่าน Verifiable Presentation โดยผู้ถือสามารถควบคุมข้อมูลที่เปิดเผยได้ (Selective Disclosure)

3.3) การรองรับการใช้งานข้ามประเทศ (Cross-border interoperability)

3.4) การตรวจสอบสถานะของเอกสาร เช่น การหมดอายุ การระงับ หรือการเพิกถอน

4) โครงสร้างพื้นฐานด้านความน่าเชื่อถือ

EUDI Wallet มีการกำหนดโครงสร้างพื้นฐานด้านความน่าเชื่อถือในระดับภูมิภาค เช่น

4.1) การเผยแพร่ข้อมูลผู้ออกเอกสารที่เชื่อถือได้ (Trusted Issuer Registry)

4.2) การจัดการกุญแจสาธารณะ (Public Key Infrastructure)

4.3) กลไกตรวจสอบสถานะของเอกสาร (Status/Revocation Mechanism)

องค์ประกอบดังกล่าวช่วยให้ผู้ตรวจสอบสามารถตรวจสอบความถูกต้องของเอกสารได้โดยไม่ต้องติดต่อผู้ออกเอกสารโดยตรง

5) บทเรียนที่สำคัญ

กรณีศึกษานี้แสดงให้เห็นถึงแนวทางการพัฒนาระบบในระดับประเทศและระดับภูมิภาคที่มีการกำหนดทั้งมาตรฐานทางเทคนิคและกรอบกำกับดูแลควบคู่กัน เพื่อสร้างความเชื่อมั่นในการใช้งาน และรองรับการขยายผลในวงกว้าง

4.1.2 กรณีศึกษา: ใบอนุญาตขับขี่ดิจิทัลบน EUDI Wallet

หนึ่งในกรณีใช้งานที่สำคัญภายใต้กรอบ EUDI Wallet คือ ใบอนุญาตขับขี่ดิจิทัล (Digital Driving License) ซึ่งเป็นตัวอย่างที่มีความเกี่ยวข้องโดยตรงกับบริบทของมาตรฐานฉบับนี้ เนื่องจากเป็นเอกสารภาครัฐที่มีผลทางกฎหมาย มีการใช้งานจริงในชีวิตประจำวัน ต้องมีการแสดงต่อเจ้าหน้าที่หรือหน่วยงานที่เกี่ยวข้อง และอาจมีการตรวจสอบสถานะของเอกสารระหว่างอายุการใช้งานได้

1) ลักษณะของกรณีใช้งาน

กรณีใบอนุญาตขับขี่ดิจิทัลบน EUDI Wallet สะท้อนลักษณะสำคัญของ VC/VP ได้อย่างชัดเจน กล่าวคือ

1.1) หน่วยงานผู้ออกออกเอกสารในรูปแบบดิจิทัลที่ตรวจสอบได้

1.2) ผู้ถือเก็บเอกสารไว้ใน wallet ที่ควบคุมโดยตนเอง

1.3) เมื่อต้องแสดงเอกสาร ผู้ถือสามารถสร้าง Verifiable Presentation เพื่อแสดงต่อผู้ตรวจสอบ

1.4) ผู้ตรวจสอบสามารถตรวจสอบลายมือชื่อและสถานะของเอกสารได้ทันที โดยไม่จำเป็นต้องพึ่งพาการตรวจสอบด้วยสายตาเพียงอย่างเดียว

2) ตัวอย่าง scenario การใช้งาน

ตัวอย่าง scenario ในเอกสารเดิมอธิบายไว้ในลักษณะเข้าใจง่าย ได้แก่

2.1) ประชาชนเก็บใบอนุญาตขับขี่ไว้ใน Wallet

2.2) เมื่อถูกตรวจโดยเจ้าหน้าที่

2.3) สร้าง Verifiable Presentation

2.4) เปิดเผยเฉพาะข้อมูลที่จำเป็น

2.5) เจ้าหน้าที่ตรวจสอบลายมือชื่อและสถานะ

2.6) ได้ผลการตรวจสอบทันที

จุดสำคัญของกรณีนี้คือ การตรวจสอบไม่จำเป็นต้องเข้าถึงฐานข้อมูลกลางทุกครั้ง แต่ใช้กลไกการพิสูจน์ตามมาตรฐาน VC ซึ่งสะท้อนหลักการสำคัญของการทำงานแบบ Interoperable และลดการเชื่อมต่อแบบเฉพาะโครงการ

3) ความสอดคล้องกับแนวคิด Selective Disclosure

กรณีใบอนุญาตขับขี่บน EUDI Wallet ยังเป็นตัวอย่างที่ดีของการนำแนวคิด Selective Disclosure มาใช้ในทางปฏิบัติ กล่าวคือ ผู้ถืออาจไม่จำเป็นต้องเปิดเผยข้อมูลทั้งหมดในใบอนุญาตขับขี่ทุกครั้ง แต่สามารถเปิดเผยเฉพาะข้อมูลที่จำเป็นต่อวัตถุประสงค์ของการตรวจสอบ เช่น การยืนยันว่ามีสิทธิขับขี่ หรือการยืนยันอายุในบางบริบท ทั้งนี้ หลักการดังกล่าวสอดคล้องกับความสามารถหลักของ EUDI Wallet ที่ให้ผู้ถือควบคุมข้อมูลที่เปิดเผยได้

4) ความสำคัญต่อการออกแบบ use case ของไทย

กรณีใบอนุญาตขับขี่ดิจิทัลบน EUDI Wallet มีความสำคัญต่อบริบทของประเทศไทยอย่างยิ่ง เพราะเป็นตัวอย่างของเอกสารภาครัฐที่

4.1) มีผลทางกฎหมาย

4.2) มีการตรวจสอบภาคสนาม

4.3) มีอายุเอกสารและสถานะการใช้งาน

4.4) ต้องรองรับทั้งการใช้งานกับหน่วยงานรัฐและบางบริบทของภาคเอกชน

ด้วยเหตุนี้ กรณีศึกษาดังกล่าวจึงสามารถใช้เป็นกรอบอ้างอิงเชิงแนวคิดสำหรับการพัฒนา ใบอนุญาตขับขี่ในรูปแบบ VC ของประเทศไทย ซึ่งในมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ แนวปฏิบัติและหลักการพื้นฐานในการออกแบบมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านความหมายข้อมูล กรณีเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล ได้กำหนดรายละเอียดด้าน Semantic Mapping และโครงสร้างข้อมูลสำหรับกรณีศึกษานี้ไว้แล้ว โดยมีการเปรียบเทียบข้อมูลจาก GDX กับมาตรฐาน mDL ตาม ISO/IEC 18013-5 และยกตัวอย่างโครงสร้าง VC สำหรับใบอนุญาตขับขี่ไว้อย่างเป็นรูปธรรม

4.1.3 กรณีศึกษา: Digital Passport และ Vaccine Certificate

ในบริบทของการเดินทางระหว่างประเทศ โดยเฉพาะในช่วงสถานการณ์การแพร่ระบาดของโรค COVID-19 หลายประเทศได้พัฒนาเอกสารรับรองในรูปแบบดิจิทัล เช่น ใบรับรองการฉีดวัคซีน (Digital Vaccine Certificate) และเอกสารการเดินทาง (Digital Passport) เพื่อรองรับการตรวจสอบข้อมูลของผู้เดินทางอย่างรวดเร็วและเชื่อถือได้

1) ลักษณะของเอกสาร

เอกสารดังกล่าวมีลักษณะเป็นเอกสารดิจิทัลที่มีการลงลายมือชื่อดิจิทัลโดยหน่วยงานที่เกี่ยวข้อง เช่น หน่วยงานสาธารณสุข หรือหน่วยงานตรวจคนเข้าเมือง เพื่อยืนยันความถูกต้องของข้อมูล

ในหลายกรณีมีการใช้โครงสร้างข้อมูลที่สอดคล้องกับแนวคิดของ Verifiable Credential แม้จะไม่ได้ใช้คำว่า VC โดยตรง

2) รูปแบบการใช้งาน

การใช้งานโดยทั่วไปประกอบด้วย

2.1) การออกเอกสารให้แก่ผู้ถือ (เช่น ผู้เดินทาง)

2.2) การจัดเก็บเอกสารในรูปแบบดิจิทัล เช่น QR Code หรือ mobile application

2.3) การนำเสนอเอกสารต่อผู้ตรวจสอบ เช่น สายการบิน หรือด่านตรวจคนเข้าเมือง

2.4) การตรวจสอบความถูกต้องของเอกสารผ่านกลไกการตรวจสอบลายมือชื่อดิจิทัล

3) การกำหนดมาตรฐานกลาง

หลายประเทศและองค์กรระหว่างประเทศได้กำหนดรูปแบบข้อมูลและมาตรฐานกลาง เช่น

3.1) รูปแบบข้อมูลสำหรับ QR Code

3.2) แนวทางการจัดการกุญแจและการตรวจสอบลายมือชื่อดิจิทัล

3.3) กลไกการแลกเปลี่ยนข้อมูลระหว่างประเทศ

การกำหนดมาตรฐานกลางช่วยให้เอกสารสามารถใช้งานร่วมกันได้ในหลายประเทศ และลดความซ้ำซ้อนในการพัฒนาระบบ

4) ความสามารถด้านการตรวจสอบ

ระบบดังกล่าวรองรับการตรวจสอบในลักษณะ offline หรือ near real-time โดยผู้ตรวจสอบสามารถตรวจสอบความถูกต้องของเอกสารได้โดยใช้กุญแจสาธารณะที่เผยแพร่ไว้ล่วงหน้า

5) บทเรียนที่สำคัญ

กรณีศึกษานี้แสดงให้เห็นถึงความสำคัญของ

5.1) การกำหนดรูปแบบข้อมูลและมาตรฐานร่วมกัน

5.2) การออกแบบระบบให้รองรับการตรวจสอบในหลายบริบท

5.3) การสร้างความเชื่อมั่นผ่านกลไกการลงลายมือชื่อดิจิทัล

4.1.4 การวิเคราะห์เปรียบเทียบและข้อสังเกตเชิงนโยบาย

เมื่อพิจารณากรณีศึกษาข้างต้น สามารถสรุปประเด็นเชิงนโยบายและเชิงออกแบบที่สำคัญได้ ดังนี้

1) การพัฒนาโดยอ้างอิงมาตรฐานสากล

ทั้งกรณี EUDI Wallet, ใบอนุญาตขับขี่ดิจิทัลบน EUDI Wallet และกรณี Digital Passport/Vaccine Certificate ต่างมีการอ้างอิงมาตรฐานสากลเป็นพื้นฐาน ซึ่งเป็นปัจจัยสำคัญในการรองรับการทำงานร่วมกันในระยะยาว

2) การออกแบบให้ผู้ถือเอกสารมีอำนาจควบคุมข้อมูล

แนวทางสมัยใหม่ให้ความสำคัญกับการที่ผู้ถือเอกสารสามารถควบคุมข้อมูลของตนเอง และเปิดเผยเฉพาะข้อมูลที่จำเป็น โดยเฉพาะกรณีใบอนุญาตขับขี่ดิจิทัลซึ่งมีความจำเป็นต้องแสดงข้อมูลตามบริบทที่แตกต่างกัน เช่น การตรวจโดยเจ้าหน้าที่ หรือการใช้เพื่อยืนยันคุณสมบัติบางประการ

3) การมีโครงสร้างพื้นฐานด้านความน่าเชื่อถือ

การตรวจสอบเอกสารจำเป็นต้องอาศัยโครงสร้างพื้นฐานที่รองรับ เช่น Registry, Public Key และ Status Mechanism ซึ่งเห็นได้ชัดจากกรณี EUDI Wallet และกรณีใบอนุญาตขับขี่ดิจิทัลที่ต้องรองรับการตรวจสอบแหล่งที่มาและสถานะของเอกสารอย่างเป็นระบบ

4) การรองรับการใช้งานในหลายบริบท

ระบบควรสามารถรองรับการใช้งานได้ทั้งในระดับหน่วยงาน ระดับประเทศ และระดับระหว่างประเทศ โดยกรณีใบอนุญาตขับขี่ดิจิทัลเป็นตัวอย่างที่ดีของเอกสารที่ใช้งานได้ทั้งในบริบทการกำกับดูแล การตรวจสอบภาคสนาม และบริการดิจิทัลอื่นที่เกี่ยวข้อง

5) การกำหนดกรอบกำกับดูแลควบคู่กับเทคโนโลยี

การนำเทคโนโลยี VC/VP ไปใช้จำเป็นต้องมีกรอบกำกับดูแลที่ชัดเจน เพื่อกำหนดบทบาท ความรับผิดชอบ และแนวทางการดำเนินงานของหน่วยงานที่เกี่ยวข้อง ทั้งนี้ กรณีของ European Digital Identity Wallet แสดงให้เห็นอย่างชัดเจนว่าแนวคิดเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัลในรูปแบบ VC/VP สามารถนำไปใช้งานจริงได้ในระดับภูมิภาค ทั้งในบริบทของการแสดงใบอนุญาต การยืนยันคุณวุฒิ และการทำธุรกรรมข้ามหน่วยงาน โดยมีการส่ง VP ในหลายกรณีศึกษาอย่างเป็นรูปธรรม ความสำเร็จดังกล่าวเกิดจากการบูรณาการด้านกฎหมาย มาตรฐานเทคนิค และโครงสร้างพื้นฐานความเชื่อถือที่ทำงานสอดประสานกันในระดับระบบนิเวศ สำหรับประเทศไทย มีพื้นฐานด้าน Digital ID และแนวคิดกรอบความเชื่อถือรองรับอยู่แล้ว หากสามารถพัฒนา Digital Wallet ที่ใช้งานได้จริง ควบคู่กับการจัดตั้ง Trust Infrastructure กลาง และกำหนดแนวปฏิบัติให้หน่วยงานของรัฐยอมรับเอกสารดิจิทัลร่วมกันอย่างเป็นระบบ ก็จะมีศักยภาพในการขับเคลื่อนการใช้งาน VC/VP ในระดับประเทศได้ในลักษณะเดียวกัน

4.2 กรณีศึกษาในประเทศไทย

จากกรณีศึกษาต่างประเทศในหัวข้อ 4.1 จะเห็นได้ว่าเอกสารในรูปแบบ VC/VP สามารถนำไปประยุกต์ใช้ได้กับเอกสารภาครัฐหลายประเภท ทั้งเอกสารเพื่อการยืนยันตัวตน เอกสารคุณวุฒิ และเอกสารใบอนุญาต โดยเฉพาะกรณี ใบอนุญาตขับขี่ดิจิทัลบน EUDI Wallet ซึ่งสะท้อนให้เห็นว่าเอกสารที่มีผลทางกฎหมาย มีการใช้งานจริง และต้องมีการตรวจสอบในหลากหลายบริบท สามารถพัฒนาให้อยู่ในรูปแบบที่ตรวจสอบได้อย่างเป็นระบบภายใต้โครงสร้างพื้นฐานด้านความน่าเชื่อถือที่เหมาะสม

ในบริบทของประเทศไทย แนวคิดดังกล่าวสามารถนำมาประยุกต์ใช้ได้เช่นเดียวกัน โดยเฉพาะกับเอกสารภาครัฐที่มีลักษณะเป็นเอกสารรับรองหรือใบอนุญาต ซึ่งมีความจำเป็นต้องแสดงต่อหน่วยงานหรือเจ้าหน้าที่ผู้ตรวจสอบ อาจมีการหมดอายุ ระงับ หรือเพิกถอนระหว่างวงจรชีวิตของเอกสาร และมีความจำเป็นต้องรองรับการใช้งานข้ามหน่วยงานได้อย่างมีประสิทธิภาพ ลักษณะดังกล่าวสอดคล้องกับคุณสมบัติของเอกสารที่เหมาะสมต่อการพัฒนาในรูปแบบ VC/VP ตามแนวทางของมาตรฐานฉบับนี้

หัวข้อนี้จึงนำเสนอกรณีศึกษาในประเทศไทยเพื่อให้เห็นพัฒนาการของการประยุกต์ใช้ VC/VP ตั้งแต่กรณีนำร่องด้านเอกสารการศึกษา ไปจนถึงการประยุกต์ใช้กับเอกสารภาครัฐประเภทใบอนุญาต ซึ่งรวมถึงกรณีใบอนุญาตขับขี่ ที่สามารถใช้เป็นกรณีศึกษาสำคัญในการเชื่อมโยงบทเรียนจากต่างประเทศเข้ากับแนวทางการพัฒนาเชิงโครงสร้างข้อมูลและความหมายข้อมูลของประเทศไทยได้อย่างเป็นรูปธรรม

4.2.1 กรณีนำร่อง Digital Transcript โดย ETDA และมหาวิทยาลัยขอนแก่น

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) ได้ดำเนินโครงการนำร่องด้าน Digital Transcript ร่วมกับมหาวิทยาลัยขอนแก่น โดยมีวัตถุประสงค์เพื่อทดสอบการออกและการตรวจสอบใบแสดงผลการศึกษาในรูปแบบ VC กรณีศึกษานี้มีความสำคัญในฐานะหลักฐานเชิงประจักษ์ว่าแนวคิด VC/VP สามารถนำมาใช้กับเอกสารที่มีความสำคัญสูงและต้องการความน่าเชื่อถือได้จริงในบริบทประเทศไทย

1) กระบวนการทดสอบนำร่อง

การนำร่องประกอบด้วยขั้นตอนสำคัญ ได้แก่

1.1) กำหนด Schema ของ Transcript ให้สอดคล้องกับมาตรฐานสากล

1.2) พัฒนากระบวนการออกเอกสารในรูปแบบ VC

1.3) ผูกกระบวนการออกกับการพิสูจน์ตัวตนของผู้สำเร็จการศึกษา

1.4) ทดสอบการจัดเก็บ VC ใน Digital Wallet

1.5) ทดสอบการสร้าง Verifiable Presentation (VP)

1.6) ทดสอบการตรวจสอบโดยหน่วยงานปลายทาง

กระบวนการดังกล่าวครอบคลุมบทบาทสำคัญครบถ้วน ได้แก่ Issuer คือมหาวิทยาลัย Holder คือผู้สำเร็จการศึกษา และ Verifier คือหน่วยงานปลายทาง เช่น นายจ้างหรือสถาบันการศึกษาอื่น รวมถึงมีองค์ประกอบของโครงสร้างพื้นฐานด้านความเชื่อถือเข้ามารองรับการตรวจสอบด้วย

2) สิ่งที่ได้จากการนำร่อง

ผลจากการทดสอบนำร่องสะท้อนประโยชน์ของ VC/VP อย่างชัดเจน ได้แก่

2.1) เอกสารสามารถตรวจสอบความถูกต้องได้โดยไม่ต้องสอบถามกลับผู้ออก

2.2) ลดระยะเวลาการตรวจสอบ Transcript

2.3) รองรับการเปิดเผยข้อมูลเฉพาะส่วน (Selective Disclosure)

2.4) ลดความเสี่ยงจากการปลอมแปลง

2.5) แสดงให้เห็นความเป็นไปได้ในการทำงานร่วมกันตามมาตรฐานสากล

3) ข้อสังเกตจากกรณีนำร่อง

กรณี Digital Transcript แสดงให้เห็นว่า แม้จะเริ่มต้นจากบริบทของเอกสารการศึกษา แต่โครงสร้างความคิดและกระบวนการที่ใช้ สามารถนำไปประยุกต์กับเอกสารภาครัฐประเภทอื่นได้ โดยเฉพาะเอกสารที่มีความจำเป็นต้องพิสูจน์ความถูกต้องของแหล่งที่มา ลดการปลอมแปลง และรองรับการใช้งานข้ามหน่วยงานในอนาคต

4.2.2 การประยุกต์ใช้ในบริบทใบอนุญาตจำหน่ายสุรา ไพ่ และยาสูบ

จากกรณีศึกษาในประเทศไทยข้างต้น โดยเฉพาะแนวทางการจัดทำเอกสารใบอนุญาตอิเล็กทรอนิกส์ตามมาตรฐาน มสพร 6-7 ซึ่งได้กำหนดรูปแบบการจัดทำและการให้บริการเอกสารใบอนุญาตในรูปแบบดิจิทัลสำหรับหน่วยงานของรัฐไว้แล้ว สามารถต่อยอดและยกระดับไปสู่การใช้เอกสารในรูปแบบ VC/VP

การยกระดับดังกล่าวเป็นการพัฒนาจากเอกสารอิเล็กทรอนิกส์แบบเดิม ซึ่งอาจอยู่ในรูปแบบไฟล์ดิจิทัลหรือการแสดงผลผ่านระบบ ไปสู่เอกสารที่มีคุณสมบัติในการตรวจสอบความถูกต้องได้ (Verifiable) โดยไม่ต้องพึ่งพาการตรวจสอบด้วยสายตาเพียงอย่างเดียว และสามารถรองรับการใช้งานข้ามหน่วยงานได้อย่างมีประสิทธิภาพ

ทั้งนี้ เอกสารประเภทใบอนุญาต เช่น ใบอนุญาตจำหน่ายสุรา ไพ่ และยาสูบ ถือเป็นกลุ่มเอกสารที่มีความเหมาะสมอย่างยิ่งในการยกระดับดังกล่าว เนื่องจากมีลักษณะเป็นเอกสารที่มีผลทางกฎหมาย อยู่ภายใต้การกำกับดูแลของรัฐ และมีความจำเป็นต้องแสดงต่อเจ้าหน้าที่ในการตรวจสอบ ณ จุดปฏิบัติงานจริง

1) ลักษณะสำคัญของเอกสาร

ใบอนุญาตประเภทดังกล่าวมีลักษณะสำคัญ ได้แก่

1.1) มีผลทางกฎหมายและอยู่ภายใต้การกำกับดูแลของรัฐ

1.2) มีอายุใบอนุญาต และอาจถูกระงับหรือเพิกถอนได้

1.3) ต้องมีการแสดงต่อเจ้าหน้าที่ระหว่างการตรวจสอบ ณ สถานประกอบการ

1.4) มีความเสี่ยงต่อการปลอมแปลงหรือใช้เอกสารที่หมดอายุ

ด้วยคุณลักษณะดังกล่าว เอกสารประเภทนี้จึงเหมาะสมต่อการนำมาพัฒนาในรูปแบบ VC เพราะสามารถเชื่อมโยงกับกลไกการตรวจสอบสถานะ และรองรับการตรวจสอบโดยเจ้าหน้าที่ได้อย่างเป็นระบบ

2) แนวทางการประยุกต์ใช้ VC/VP

ในเชิงการดำเนินงาน หน่วยงานผู้ออกสามารถออกใบอนุญาตในรูปแบบ VC ให้แก่ผู้ประกอบการหรือผู้ได้รับอนุญาต เพื่อให้เก็บรักษาในกระเป๋าดิจิทัล และใช้สร้าง VP เมื่อต้องแสดงต่อเจ้าหน้าที่ผู้ตรวจสอบ ณ จุดปฏิบัติงานจริง โดยผู้ตรวจสอบสามารถตรวจสอบได้ทั้ง

2.1) ความถูกต้องของแหล่งที่มา

2.2) ความครบถ้วนของข้อมูล

2.3) สถานะปัจจุบันของใบอนุญาต เช่น ยังมีผลใช้บังคับ ถูกระงับ หรือถูกเพิกถอน

แนวทางนี้ช่วยลดการพึ่งพาการตรวจสอบด้วยสายตาเพียงอย่างเดียว และลดความจำเป็นในการติดต่อกลับไปยังหน่วยงานต้นทางทุกครั้ง

3) ข้อพิจารณาในการออกแบบ

3.1) ด้านความเป็นส่วนตัว (Privacy)

ไม่ควรออกแบบระบบในลักษณะที่ทำให้หน่วยงานผู้ออกสามารถติดตามการใช้งานใบอนุญาตของผู้ถือได้ทุกครั้ง ควรใช้กลไกการตรวจสอบผ่านลายมือชื่อและสถานะของเอกสารแทนการเรียกข้อมูลกลับไปยังระบบต้นทางโดยตรงทุกครั้ง เพื่อให้สอดคล้องกับหลักการคุ้มครองข้อมูลส่วนบุคคลและลดการเปิดเผยข้อมูลเกินจำเป็น

3.2) ด้านการใช้งานภาคสนาม (Offline / Low Connectivity)

ควรออกแบบให้เจ้าหน้าที่สามารถตรวจสอบใบอนุญาตได้แม้ในสภาพแวดล้อมที่มีการเชื่อมต่อจำกัด เช่น ใช้ข้อมูลที่ฝังอยู่ใน VC ร่วมกับข้อมูลสถานะที่มีการซิงค์ล่วงหน้า แนวทางนี้เหมาะสมกับบริบทการตรวจสถานประกอบการ ซึ่งอาจไม่ได้อยู่ในสภาพแวดล้อมที่มีเครือข่ายเสถียรเสมอไป

3.3) ด้านการบูรณาการข้ามหน่วยงาน

ใบอนุญาตควรสามารถถูกตรวจสอบโดยหน่วยงานอื่นได้ โดยไม่ต้องพึ่งพาระบบเฉพาะของหน่วยงานผู้ออก และควรกำหนดรูปแบบข้อมูลและจุดตรวจสอบให้เป็นมาตรฐานกลาง เพื่อรองรับการทำงานร่วมกันระหว่างหน่วยงานในระยะยาว

3.4) สรุปประโยชน์ของกรณีนี้

การนำใบอนุญาตจำหน่ายสุรา ไพ่ และยาสูบ มาประยุกต์ใช้ในรูปแบบ VC/VP ช่วยให้สามารถ

- ลดการปลอมแปลงเอกสาร
- ตรวจสอบสถานะได้แบบทันสมัย
- เพิ่มความสะดวกในการแสดงและตรวจสอบ
- คุ้มครองข้อมูลส่วนบุคคลผ่านการเปิดเผยเท่าที่จำเป็น

อย่างไรก็ดี การออกแบบต้องคำนึงถึงความน่าเชื่อถือ ความปลอดภัย และความเป็นส่วนตัวควบคู่กัน เพื่อให้สามารถใช้งานได้จริงในบริบทภาครัฐ

4.2.3 การประยุกต์ใช้ในบริบทใบอนุญาตขับขี่

เมื่อพิจารณาต่อเนื่องจากกรณีศึกษาใบอนุญาตขับขี่ดิจิทัลบน EUDI Wallet ในข้อ 4.1 จะเห็นได้ว่าใบอนุญาตขับขี่เป็นเอกสารภาครัฐที่เหมาะสมอย่างยิ่งต่อการนำมาพัฒนาในรูปแบบ VC/VP ในบริบทของประเทศไทย เนื่องจากเป็นเอกสารที่มีผลทางกฎหมาย มีการใช้งานจริงอย่างแพร่หลาย ต้องมีการแสดงและตรวจสอบในภาคสนาม และอาจมีการเปลี่ยนแปลงสถานะระหว่างอายุการใช้งานได้ จึงเป็นกรณีใช้งานที่สะท้อนคุณลักษณะสำคัญของ VC/VP ได้อย่างชัดเจน ทั้งในด้านความน่าเชื่อถือ การตรวจสอบได้ และการคุ้มครองข้อมูลส่วนบุคคล

นอกจากนี้การเลือกยกบริบทใบอนุญาตขับขี่ขึ้นมาเป็นกรณีประยุกต์ใช้ ไม่ได้มีเหตุผลเพียงในเชิงแนวคิดเท่านั้น แต่ยังสอดคล้องกับทิศทางการพัฒนาเชิงนโยบายและโครงสร้างพื้นฐานดิจิทัลของประเทศไทย ซึ่ง ETDA ได้ผลักดันเรื่อง Verifiable Credentials และ Digital Wallet มาอย่างต่อเนื่อง และมีการเชื่อมโยงกับข้อเสนอเชิงนโยบายและการสนับสนุนด้านโครงสร้างพื้นฐานข้อมูลดิจิทัลในวงหารือร่วมกับธนาคารโลก (World Bank) ด้วย โดยรายงานของธนาคารโลกระบุถึงบทบาทของ ETDA ในการพัฒนามาตรฐาน VC เพื่อสร้างระบบนิเวศ Digital Identity ที่ทำงานร่วมกันได้ในประเทศไทย นอกจากนี้ การเลือกบริบทดังกล่าวยังมีน้ำหนักในทางปฏิบัติ เนื่องจาก ETDA ได้นำกรณีศึกษาใบอนุญาตขับขี่มาเป็นหนึ่งในกรณีศึกษา เพื่อใช้ในการประชุมเชิงปฏิบัติการเรื่องการออกแบบกระบวนการทางเทคนิคการใช้เอกสารรับรองดิจิทัลและกระเป๋าดิจิทัล เมื่อเดือน เมษายน 2569

อีกทั้งในเชิงข้อมูลและแบบจำลองเชิงความหมายตามมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ แนวปฏิบัติและหลักการพื้นฐานในการออกแบบมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านความหมายข้อมูล กรณีเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล ยังได้จัดทำรายละเอียดด้าน Semantic Mapping และตัวอย่างโครงสร้าง VC สำหรับใบอนุญาตขับขี่ไว้แล้ว จึงทำให้กรณีใบอนุญาตขับขี่เป็นกรณีศึกษาที่มีทั้งมิติด้านนโยบาย มาตรฐาน และความพร้อมเชิงปฏิบัติ รองรับการอธิบายต่อยอดจากระดับแนวคิดไปสู่การประยุกต์ใช้จริงในประเทศไทยได้อย่างเหมาะสม

1) เหตุผลที่ใบอนุญาตขับขี่เหมาะสมต่อการใช้ VC/VP

ใบอนุญาตขับขี่มีลักษณะที่สอดคล้องกับคุณสมบัติของเอกสารที่เหมาะกับ VC/VP ได้แก่

1.1) เป็นเอกสารที่มีผลทางกฎหมาย

1.2) มีข้อมูลประจำตัวและข้อมูลสิทธิในการขับขี่

1.3) มีวันออกและวันหมดอายุ

1.4) มีสถานะการใช้งานซึ่งอาจเปลี่ยนแปลงได้

1.5) ต้องใช้ในการตรวจสอบทั้งโดยหน่วยงานรัฐและในบางบริบทอาจเกี่ยวข้องกับภาคเอกชน

ในมุมเชิงระบบ เอกสารประเภทนี้จึงเหมาะทั้งต่อการออกเป็น VC และการแสดงผลในรูปแบบ VP เพื่อให้ผู้ถือสามารถควบคุมการเปิดเผยข้อมูลได้ตามความจำเป็น

2) การเชื่อมโยงกับมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ แนวปฏิบัติและหลักการพื้นฐานในการออกแบบมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านความหมายข้อมูล กรณีเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล

กรณีใบอนุญาตขับขี่เป็นกรณีศึกษาหลัก โดยมีการนำชุดแอตทริบิวต์ของข้อมูลใบอนุญาตขับขี่จาก GDX มาเปรียบเทียบกับแอตทริบิวต์ของมาตรฐาน mDL ตาม ISO/IEC 18013-5 เพื่อให้ข้อมูลมีความหมายที่เข้าใจตรงกันระหว่างหน่วยงาน และสามารถพัฒนาไปสู่โครงสร้างข้อมูลที่ทำงานร่วมกันได้

แนวทางดังกล่าวสะท้อนหลักสำคัญ 2 ประการ คือ

(1) การใช้ข้อมูลหลักร่วมกัน (Core Data) ตามมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ เช่น ข้อมูลบุคคล

(2) การแยกข้อมูลเชิงบริบทเฉพาะโดเมนของหน่วยงาน เช่น ข้อมูลใบอนุญาตขับขี่ ภายใต้ Namespace ที่เกี่ยวข้อง

3) แนวทางการจัดโครงสร้างข้อมูล

จากเอกสารมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ แนวปฏิบัติและหลักการพื้นฐานในการออกแบบมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านความหมายข้อมูล กรณีเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล มีตัวอย่างการจัดโครงสร้างข้อมูลใน VC โดยกำหนดให้ส่วน credentialSubject ประกอบด้วยข้อมูลผู้ถือเอกสารและข้อมูลใบอนุญาตขับขี่ เช่น เลขที่ใบอนุญาต ประเภทใบอนุญาต วันที่ออก วันหมดอายุ และสถานะการใช้งาน พร้อมทั้งแมปข้อมูลไปยังคำศัพท์ตามมาตรฐาน TGIX VC/VP เช่น dlt:LicenseNumber, dlt:LicenseClassCode, dlt:IssueDate, dlt:ExpiryDate และ dlt:StatusCode รวมทั้งใช้ข้อมูลหลักด้านบุคคลภายใต้โครงสร้างของ TGIX core data

แนวทางนี้มีความสำคัญ เพราะช่วยให้การออกแบบ VC ไม่ได้เป็นเพียงการสร้างเอกสารดิจิทัลที่ลงลายมือชื่อได้เท่านั้น แต่เป็นการกำหนด “ความหมายข้อมูล” ให้สามารถตีความร่วมกันได้ระหว่างระบบงานของภาครัฐ

4) บทบาทของผู้เกี่ยวข้อง

ในกรณีใบอนุญาตขับขี่ สามารถอธิบายบทบาทหลักได้ดังนี้

4.1) Issuer: หน่วยงานผู้ออกใบอนุญาตขับขี่

4.2) Holder: ประชาชนผู้ได้รับใบอนุญาต

4.3) Verifier: เจ้าหน้าที่รัฐหรือหน่วยงานที่มีหน้าที่ตรวจสอบ

4.4) Wallet: กระเป๋าดิจิทัลที่ผู้ถือใช้จัดเก็บ VC และสร้าง VP

4.5) Trust Infrastructure: กลไกตรวจสอบความน่าเชื่อถือ เช่น ระบบทะเบียนผู้ออก กุญแจสาธารณะ และกลไกตรวจสอบสถานะ

การกำหนดบทบาทเช่นนี้ทำให้กรณีใบอนุญาตขับขี่สามารถเชื่อมโยงกับกรอบภาพรวมของ VC ecosystem ได้โดยตรง

5) รูปแบบการใช้งาน

ในเชิงการใช้งาน สามารถอธิบายลำดับโดยสรุปได้ดังนี้

5.1) หน่วยงานผู้ออก ตรวจสอบคุณสมบัติและออกใบอนุญาตขับขี่ในรูปแบบ VC

5.2) ผู้ถือจัดเก็บ VC ไว้ในกระเป๋าดิจิทัล

5.3) เมื่อมีการตรวจสอบ ผู้ถือใช้ VC สร้างเป็น VP เพื่อแสดงต่อผู้ตรวจสอบ

5.4) ผู้ตรวจสอบตรวจสอบลายมือชื่อ ความครบถ้วนของข้อมูล และสถานะของใบอนุญาตผ่านกลไกที่กำหนด

แนวทางนี้ทำให้ผู้ถือไม่จำเป็นต้องแสดงข้อมูลทั้งหมดทุกครั้ง และผู้ตรวจสอบไม่จำเป็นต้องอาศัยการตรวจสอบด้วยสายตาเพียงอย่างเดียว

6) คุณค่าเชิงนโยบายและเชิงปฏิบัติ

กรณีใบอนุญาตขับขี่มีคุณค่าเชิงนโยบายหลายประการ ได้แก่

6.1) เป็น use case ที่ประชาชนเข้าใจง่ายและมีการใช้งานจริง

6.2) เหมาะกับการสื่อสารเรื่องการยกระดับจากเอกสารอิเล็กทรอนิกส์แบบเดิมไปสู่เอกสารที่ตรวจสอบได้

6.3) มีฐานข้อมูลและโครงสร้าง semantic รองรับตามรูปแบบ TGIX VC/VP

6.4) สามารถเป็นกรณีตัวอย่างสำหรับการพัฒนาเอกสารใบอนุญาตประเภทอื่นในอนาคต

ในเชิงปฏิบัติ กรณีนี้ยังช่วยให้เห็นภาพชัดเจนของการเชื่อมโยงระหว่างมาตรฐานโครงสร้างข้อมูล มาตรฐานด้านการออกและแสดงเอกสารดิจิทัล และแนวคิดเรื่องการคุ้มครองข้อมูลส่วนบุคคลผ่านการเปิดเผยเท่าที่จำเป็น

4.2.4 ข้อสรุปจากกรณีศึกษาในประเทศไทย

จากกรณีศึกษาในประเทศไทยทั้ง 3 กรณี จะเห็นได้ว่าแนวคิด VC/VP ไม่ได้เป็นเพียงรูปแบบเอกสารดิจิทัลรูปแบบใหม่ แต่เป็นแนวทางที่ช่วยตอบโจทย์ปัญหาและข้อจำกัดของเอกสารอิเล็กทรอนิกส์แบบเดิมที่กล่าวไว้ในข้อ 3.1 ได้อย่างเป็นรูปธรรม ทั้งในมุมของหน่วยงานของรัฐ และในมุมของประชาชนหรือผู้ประกอบการ

กรณี Digital Transcript แสดงให้เห็นว่าเอกสารสามารถออกและตรวจสอบได้ด้วยกระบวนการที่เป็นมาตรฐานและตรวจสอบได้ทางเทคนิค ช่วยลดการพึ่งพาการตรวจด้วยสายตาหรือการสอบถามกลับไปยังหน่วยงานผู้ออกโดยตรง และสะท้อนศักยภาพของ VC/VP ในการยกระดับความน่าเชื่อถือของเอกสารดิจิทัล

กรณี ใบอนุญาตจำหน่ายสุรา ไพ่ และยาสูบ แสดงให้เห็นความเหมาะสมของ VC/VP สำหรับเอกสารที่มีผลทางกฎหมาย ต้องมีการตรวจสอบภาคสนาม และต้องบริหารสถานะของเอกสารอย่างต่อเนื่อง โดยเฉพาะในกรณีที่มีการพักใช้ เพิกถอน หรือเปลี่ยนแปลงสถานะ ซึ่งช่วยลดช่องว่างระหว่างคำสั่งทางปกครองกับการบังคับใช้จริง

กรณี ใบอนุญาตขับขี่ ช่วยให้เห็นภาพการประยุกต์ใช้ VC/VP ในเอกสารที่มีการใช้งานอย่างแพร่หลาย มีการตรวจสอบข้ามหน่วยงานหรือข้ามบริบทการใช้งาน และสามารถเชื่อมโยงแนวปฏิบัติด้านกระบวนการเข้ากับแนวทางด้าน Semantic และ Schema ของ TGIX VC/VP ได้อย่างเป็นรูปธรรม

โดยภาพรวม กรณีศึกษาทั้ง 3 กรณีสะท้อนว่า VC/VP สามารถช่วยบรรเทาปัญหาสำคัญของเอกสารอิเล็กทรอนิกส์แบบเดิมได้ ได้แก่

- การตรวจสอบความถูกต้องของเอกสารที่ยังพึ่งพาการพิจารณาด้วยสายตาหรือการสอบถามกลับ
- ข้อจำกัดในการตรวจสอบสถานะเอกสารให้เป็นปัจจุบัน
- ความซ้ำซ้อนของการพัฒนาและการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน
- การเปิดเผยข้อมูลเกินความจำเป็น
- ภาระของประชาชนหรือผู้ประกอบการในการแสดงหรือส่งเอกสารซ้ำหลายครั้ง

ดังนั้น การเริ่มต้นนำ VC/VP มาใช้ในประเทศไทยจึงควรมุ่งไปที่เอกสารที่มีลักษณะดังต่อไปนี้ คือ เป็นเอกสารที่มีความสำคัญทางกฎหมาย มีความเสี่ยงต่อการปลอมแปลง มีการตรวจสอบภาคสนามหรือข้ามหน่วยงาน มีความจำเป็นต้องตรวจสอบสถานะของเอกสาร และมีประโยชน์จากการเปิดเผยข้อมูลเฉพาะส่วน แนวทางดังกล่าวจะช่วยให้การนำ VC/VP มาใช้สามารถตอบโจทย์ปัญหาที่มีอยู่จริง และขยายผลไปสู่ระบบนิเวศของเอกสารดิจิทัลภาครัฐได้อย่างเหมาะสม

บรรณานุกรม

[1] พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562. (2562, 22 พฤษภาคม). ราชกิจจานุเบกษา. เล่ม 136 ตอนที่ 67 ก. หน้า 1-13.

[2] พระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. 2565. (2565, 12 ตุลาคม). ราชกิจจานุเบกษา. เล่ม 139 ตอนที่ 63 ก. หน้า 1-14.

[3] พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544. (2544, 4 ธันวาคม). ราชกิจจานุเบกษา. เล่ม 118 ตอนที่ 112 ก. หน้า 1-24.

[4] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. (2562, 27 พฤษภาคม). ราชกิจจานุเบกษา. เล่ม 136 ตอนที่ 69 ก. หน้า 33-72.

[5] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2568). รายงานทางเทคนิค เรื่อง กรอบการสร้างความน่าเชื่อถือของเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล. สืบค้น 5 มีนาคม 2569, จาก 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?lang=th-TH

[6] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2568). รายงานทางเทคนิค เรื่อง กรอบแนวทางการทำงานร่วมกันของเอกสารรับรองดิจิทัลสำหรับประเทศไทย. สืบค้น 5 มีนาคม 2569, จาก 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?lang=th-TH

[7] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2566). รายงานทางเทคนิค เรื่อง กรอบการทำงานร่วมกันของกระเป๋าดิจิทัลสำหรับเอกสารรับรอง. สืบค้น 5 มีนาคม 2569, จาก https://www.etda.or.th/getattachment/4193e2fd-224a-44ce-b6c6-2e809d44a494/Technical-Report.aspx

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

[9] สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน). (2569). มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ แนวปฏิบัติและหลักการพื้นฐานในการออกแบบมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านความหมายข้อมูล กรณีเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล.

[10] European Commission. (2023). EU Digital COVID Certificate. Retrieved March 5, 2026, from https://commission.europa.eu/strategy-and-policy/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en

[11] European Commission. (2023). Architecture and Reference Framework for the European Digital Identity Wallet (ARF). Retrieved March 5, 2026, from https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework

[12] European Commission. (2023). eIDAS 2.0 Regulation and European Digital Identity Framework. Retrieved March 5, 2026, from https://www.european-digital-identity-regulation.com/

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

[14] International Air Transport Association. (2021). IATA Travel Pass Initiative. Retrieved March 5, 2026, from https://www.icao.int/sites/default/files/APAC/Meetings/2021/2021%20ACCRPG10/5-Presentations/4.2_IATA-Travel-Pass-introduction-ACCRPG-June-2021.pdf

[15] Internet Engineering Task Force. (2015). JSON Web Signature (JWS) (RFC No. 7515). Retrieved March 5, 2026, from https://www.rfc-editor.org/rfc/rfc7515.html

[16] Internet Engineering Task Force. (2012). The OAuth 2.0 Authorization Framework (RFC No. 6749). Retrieved March 5, 2026, from https://datatracker.ietf.org/doc/html/rfc6749

[17] OpenID Foundation. (2023). OpenID for Verifiable Credential Issuance (OpenID4VCI). Retrieved March 5, 2026, from https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html

[18] OpenID Foundation. (2023). OpenID for Verifiable Presentations (OpenID4VP). Retrieved March 5, 2026, from https://openid.net/specs/openid-4-verifiable-presentations-1_0.html

[19] OpenID Foundation. (2014). OpenID Connect Core 1.0. Retrieved March 5, 2026, from https://openid.net/specs/openid-connect-core-1_0-final.html

[20] World Wide Web Consortium. (2022). Decentralized Identifiers (DID) v1.0. Retrieved March 5, 2026, from https://www.w3.org/TR/did-1.0/

[21] World Wide Web Consortium. (2023). Verifiable Credentials Data Model v2.0. Retrieved March 5, 2026, from https://www.w3.org/TR/vc-data-model-2.0/