

 **เผยแพร่ประกาศ**

มาตรฐานสำนักงาน พัฒนารัฐบาลดิจิทัล

มสพร. 6-8 : 2569

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ว่าด้วยแนวปฏิบัติกระบวนการทางดิจิทัลภาครัฐ - ส่วนที่ 8

เรื่อง เอกสารใบอนุญาตอิเล็กทรอนิกส์ภาครัฐ
ในรูปแบบเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล

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

 ใบอนุญาตภาครัฐ
ดิจิทัล

 **VC/VP**

 ความน่าเชื่อถือ
ปลอดภัย

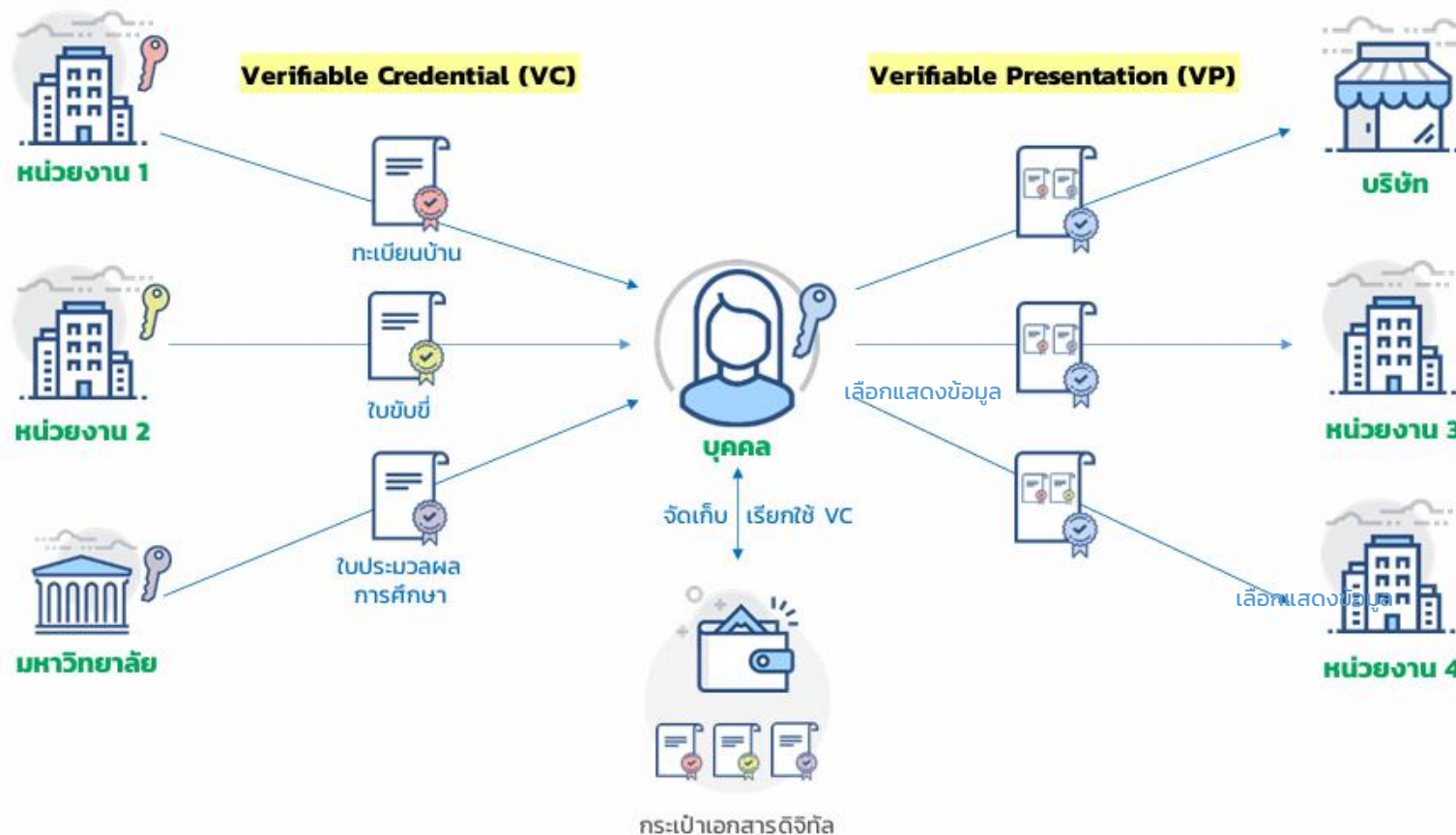
 เชื่อมโยงข้อมูล
อย่างมั่นใจ

 เอกสารรับรอง
ดิจิทัล

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล

ว่าด้วยแนวปฏิบัติกระบวนการทางดิจิทัลภาครัฐ – ส่วนที่ 8 เรื่อง เอกสารใบอนุญาตอิเล็กทรอนิกส์ภาครัฐในรูปแบบเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล

เอกสารรับรองดิจิทัล (Verifiable Credential: VC) และเอกสารสำแดงดิจิทัล (Verifiable Presentation: VP)



เอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล

- ❑ สามารถ**ตรวจสอบความถูกต้อง**ของเอกสารได้ว่าเอกสารดังกล่าวออกโดยหน่วยงานนั้นจริง
- ❑ บุคคลที่ยื่นเอกสาร**เป็นเจ้าของเอกสาร**นั้นจริง
- ❑ ช่วยเพิ่ม**ความเป็นส่วนตัว**ให้กับผู้ใช้งาน (สามารถเลือกแสดงข้อมูลในเอกสารบางส่วนได้)

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล

ว่าด้วยแนวปฏิบัติกระบวนการทางดิจิทัลภาครัฐ – ส่วนที่ 8 เรื่อง เอกสารใบอนุญาตอิเล็กทรอนิกส์ภาครัฐในรูปแบบเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล



1. บทนำ

1.1 ความเป็นมา / 1.2 วัตถุประสงค์

ยกระดับใบอนุญาตดิจิทัลภาครัฐ: จาก PDF สู่มาตรฐาน VC/VP (มสพร. 6 ส่วนที่ 8)

สำนักงานพัฒนารัฐบาลดิจิทัล (DGA) พัฒนามาตรฐานเพื่อยกระดับใบอนุญาตอิเล็กทรอนิกส์สู่เทคโนโลยี Verifiable Credentials (VC) รองรับการตรวจสอบอัตโนมัติและเพิ่มความเป็นส่วนตัว

มสพร. ส่วนที่ 7 (รูปแบบเดิม)



ก้าวข้ามข้อจำกัดของไฟล์ PDF

แม้ PDF จะนำเชื่อถือแต่ยังตรวจสอบแบบอัตโนมัติและใช้งานข้ามหน่วยงานได้ยาก

คุณลักษณะ:

- รูปแบบเอกสาร: ไฟล์เอกสาร (เช่น PDF)
- การตรวจสอบ: ตรวจสอบผ่านระบบผู้ออก
- การประมวลผล: มนุษย์อ่านเป็นหลัก



ลดการพึ่งพาฐานข้อมูลส่วนกลาง
ช่วยให้หน่วยงานปลายทางตรวจสอบใบอนุญาตได้
แม้ระบบของผู้ออกจะขัดข้อง



ประโยชน์หลักสำหรับการเป็นรัฐบาลดิจิทัล

ประยุกต์ใช้ได้ในทุกมิติ
ครอบคลุมทั้งใบขับขี่ดิจิทัล, ปริญญาบัตร
(Digital Transcript) และใบอนุญาตประกอบธุรกิจ



มาตรฐานสากลระดับโลก

อ้างอิงมาตรฐาน W3C ทำให้สามารถเชื่อมโยง
ข้อมูลข้ามเครือข่ายได้อย่างไร้รอยต่อ

NotebookLM

มสพร. ส่วนที่ 8 (ระดับสูง)



ยกระดับสู่มาตรฐาน VC/VP

รองรับการตรวจสอบความถูกต้องได้ทันทีโดยไม่ต้องพึ่งพาฐานข้อมูลกลางตลอดเวลา



สู่ความปลอดภัย
และคล่องตัว



Issuer
(หน่วยงานรัฐ)

VC

Issues digital
credential (VC)



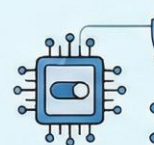
Holder
(ประชาชน/Wallet)

VP

Selectable
presentation (VP)



Verifier
(หน่วยงานตรวจสอบ)



Selective Disclosure: เปิดเผยเท่าที่จำเป็น
ผู้ถือเอกสารสามารถเลือกสำแดงเฉพาะข้อมูลที่ต้องการ (VP)
เพื่อรักษาความเป็นส่วนตัวสูงสุด

รูปแบบเอกสาร: ข้อมูลดิจิทัล (VC/VP)
การตรวจสอบ: ตรวจสอบได้โดยอิสระ (Decentralized)
การประมวลผล: เครื่องคอมพิวเตอร์ประมวลผลได้ทันที

- 1) เพื่อสร้างความเข้าใจเกี่ยวกับแนวคิดและหลักการ **VC/VP**
- 2) เพื่ออธิบายกรอบแนวทาง มาตรฐาน และโครงสร้างพื้นฐานด้านความน่าเชื่อถือที่เกี่ยวข้องใน**ประเทศไทย**
- 3) เพื่ออธิบายบทบาท **หน้าที่** และความรับผิดชอบ**ของผู้เกี่ยวข้อง**ในระบบนิเวศของ VC/VP
- 4) เพื่อเป็นข้อเสนอแนะแนวทางสำหรับหน่วยงานของรัฐในการ**ปรับกระบวนการเดิม**สู่การใช้งาน VC /VP
- 5) เพื่อเป็นกรอบแนวคิดสำหรับการเตรียมความพร้อมและการนำไปใช้งานจริง โดยเฉพาะสำหรับหน่วยงานของรัฐที่มีระดับความพร้อมด้านดิจิทัลในระดับสูง ให้สามารถออกและให้บริการใบอนุญาตในรูปแบบดิจิทัลที่ตรวจสอบได้อย่างมั่นคงปลอดภัย

มาตรฐานหรือข้อกำหนดสากล (VC /VP)

- **OpenID for Verifiable Credential Issuance (OID4VCI)/VP (2568):**
โปรโตคอลมาตรฐานบนพื้นฐานของ OAuth 2.0 และ OpenID Connect ที่ใช้สำหรับการออก **เอกสาร** (Issuance) และ**การสำแดงเอกสาร** (Presentation)
- **Architecture Reference Framework (2564):**
กำหนดภาพรวมสถาปัตยกรรม บทบาท (Role) ต่าง ๆ (**Issuer**, **Holder** และ **Verifier**) และ Trust model
- **W3C Verifiable Credentials Data Model 2.0 (2568):**
มาตรฐานแกนหลักที่พัฒนาต่อยอดจาก v1.1 โดยปรับเปลี่ยนจากข้อบังคับเดิมที่ต้องใช้ JSON-LD และ @context มาเป็น**การรองรับข้อมูลแบบ Multi-format** ผ่าน Media Types (เช่น JWT)

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA)

- **THAI VC ARCHITECTURE AND REFERENCE FRAMEWORK (2568):**
กรอบแนวทางการทำงานร่วมกันของ**เอกสารรับรองดิจิทัล**สำหรับประเทศไทย พ.ศ. 2568 สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
- **INTEROPERABLE FRAMEWORK OF DIGITAL WALLETS FOR VERIFIABLE CREDENTIALS (2566):**
กรอบการทำงานร่วมกันของ**กระเป๋าดิจิทัลสำหรับเอกสารรับรอง** พ.ศ. 2566 สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
- **Trust Model Framework for Verifiable Credential (VC) and Verifiable Presentation (VP) (2568):**
กรอบการ**สร้างความน่าเชื่อถือของเอกสารรับรองและเอกสารสำแดง** พ.ศ. 2568 สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์



สำนักงานพัฒนารัฐบาลดิจิทัล (DGA)

- (ร่าง) มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัลว่าด้วยแนวปฏิบัติกระบวนการทางดิจิทัลภาครัฐ ส่วนที่ 8 เรื่อง เอกสารใบอนุญาตอิเล็กทรอนิกส์ภาครัฐในรูปแบบเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล เวอร์ชัน 1.0 :
สร้างความเข้าใจที่ชัดเจนตามกรอบของ ETDA และนำมาเป็นแนวทางในการพัฒนากระบวนการออกใบอนุญาตอิเล็กทรอนิกส์ของหน่วยงานภาครัฐ ให้สามารถตรวจสอบและแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ได้อย่างน่าเชื่อถือ และปลอดภัย
- (ร่าง) มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ แนวปฏิบัติและหลักการพื้นฐานในการออกแบบ มาตรฐานการเชื่อมโยง และแลกเปลี่ยนข้อมูลภาครัฐ ด้านความหมายข้อมูลกรณีเอกสารรับรอง และเอกสารสำแดงอิเล็กทรอนิกส์ภาครัฐ :
มุ่งช่วยให้นักพัฒนาระบบสารสนเทศของหน่วยงานภาครัฐ สามารถเข้าใจถึงโครงสร้างข้อมูล VC/VP ในส่วนที่จำเป็น และสอดคล้องกับมาตรฐานสากล (เช่น W3C Verifiable Credentials Data Model) และโดเมนข้อมูลที่เป็นกรณีศึกษา (ใบอนุญาตขับขี่)



2. กรอบแนวคิดและมาตรฐานสำหรับเอกสารรับรองดิจิทัล VC/VP

2.1 แนวคิดในการประยุกต์ใช้ VC/VP

2.1.1 แนวคิดหลักของการทำงานในระบบ VC/VP

1. การรับรองข้อมูลโดยผู้ออกเอกสาร

ผู้ออกเอกสารทำหน้าที่รับรองข้อความยืนยันและออกเป็น VC พร้อมลงลายมือชื่ออิเล็กทรอนิกส์

2. การควบคุมข้อมูลโดยผู้ถือเอกสาร

ผู้ถือเอกสารจัดเก็บ VC ไว้ในกระเป๋าดิจิทัล และสามารถนำ VC สร้างเป็น VP เพื่อแสดงต่อผู้ตรวจสอบเอกสาร

3. การตรวจสอบด้วยกระบวนการเข้ารหัสลับ

ผู้ตรวจสอบเอกสารสามารถตรวจสอบความถูกต้องครบถ้วนของ VC และ VP รวมถึงตรวจสอบสถานการณ์ใช้งานได้ผ่านกลไกการตรวจสอบสถานะ

4. การเลือกเปิดเผยข้อมูลบางส่วน

ผู้ถือเอกสารสามารถเปิดเผยเฉพาะข้อมูลที่จำเป็นต่อวัตถุประสงค์ของการตรวจสอบ โดยไม่ต้องเปิดเผยข้อมูลทั้งหมด

5. การสนับสนุนด้วยโครงสร้างพื้นฐานด้านความน่าเชื่อถือ

ระบบทะเบียนผู้ออก ระบบบริหารกุญแจดิจิทัล และกลไกการตรวจสอบสถานะ ทำหน้าที่สนับสนุนความเชื่อมั่นของทั้งระบบ

2.1.2 แนวคิดสำคัญที่ทำให้ระบบ VC/VP มีความน่าเชื่อถือ ปลอดภัย และความเป็นส่วนตัว



หลักการที่ 1:
PID VC คือ
รากฐานการ
ยืนยันตัวตน
(root of trust)



หลักการที่ 2:
มาตรฐานการใช้
DID (DID
Method)



หลักการที่ 3:
การทำงานแบบ
ขจัดคอขวด
(Local
Resolution)



หลักการที่ 4:
การพิสูจน์ความ
เป็นเจ้าของกุญแจ
(Proof of
Possession -
PoP)



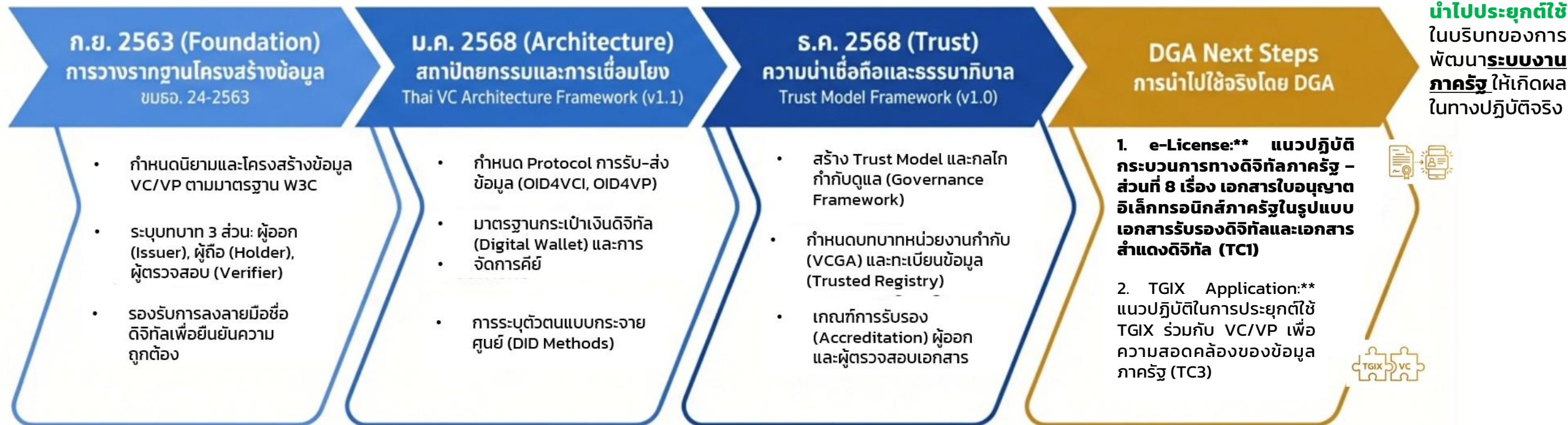
หลักการที่ 5:
เคารพความเป็นส่วนตัว
(Anti-Tracking)

ที่มา: การประชุมเชิงปฏิบัติการ เรื่อง การออกแบบกระบวนการทางเทคนิคการใช้เอกสารดิจิทัล มีนาคม 2569, ETDA



2. กรอบแนวคิดและมาตรฐานสำหรับเอกสารรับรองดิจิทัล VC/VP

2.2 กรอบแนวทางด้านเอกสารรับรองดิจิทัลที่ประกาศโดยสำนักงานพัฒนารัฐธรรมทางอิเล็กทรอนิกส์



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



3. แนวทางการดำเนินการสำหรับหน่วยงานของรัฐในการประยุกต์ใช้ VC/VP

3.1 ปัญหาและข้อจำกัดของเอกสารอิเล็กทรอนิกส์แบบเดิม

มุมมองของหน่วยงานของรัฐ (The Government's Perspective)



ตรวจสอบความถูกต้องได้ยากและล่าช้า
มักต้องใช้สำเนาพิจารณาหรือสอบถามกลับไปซึ่งผู้ออกเอกสารไม่สามารถตรวจสอบผ่านกระบวนการเข้ารหัสลับได้โดยตรง

การบริหารสถานะใบอนุญาตขาดมาตรฐาน

เมื่อมีการระงับหรือเพิกถอนข้อมูลมักไม่สะท้อนถึงผู้ตรวจสอบทันที ทำให้เกิดช่องว่างในการบังคับใช้กฎหมาย



ระบบเข้าซื้อและขาดความมั่นคงปลอดภัย

การเชื่อมโยงข้อมูลมักทำแบบเฉพาะโครงการ และตรวจพบการแก้ไขข้อมูลได้ยากหากเป็นรูปแบบเอกสารทั่วไป



การสื่อสารกับหน่วยงานของรัฐ

- สามารถตรวจสอบเอกสารได้สะดวกและเชื่อถือได้มากขึ้น
- ไม่ได้ต้องรู้ระบบเดิมทั้งหมดในทันที
- หน่วยงานสามารถพิจารณาจากปัญหาและความจำเป็นของเอกสารแต่ละประเภท
- เน้นการเชื่อมโยงระหว่างหน่วยงาน และหลีกเลี่ยงการพัฒนาแบบแยกส่วน
- เน้นการใช้บริการแพลตฟอร์มกลาง

มุมมองของประชาชนและผู้ประกอบการ (Citizen & Entrepreneur Perspective)

การเปิดเผยข้อมูลเกินความจำเป็น
เอกสารทั่วไปมักแสดงข้อมูลทั้งหมด ไม่รองรับการเลือกเปิดเผยข้อมูลบางส่วนตามหลักความเป็นส่วนตัว



ภาระในการแสดงเอกสารและอัปเดตข้อมูล

ต้องส่งสำเนาหลายครั้งหรืออัปเดตข้อมูลเดิมซ้ำๆ เมื่อต้องติดต่อกับหลายหน่วยงานที่ระบบไม่เชื่อมกัน



ความไม่ชัดเจนของสถานะเอกสาร

ผู้ถือเอกสารและผู้ตรวจสอบมักไม่ทราบสถานะล่าสุดกับที่ในกรณีใบอนุญาตหมดอายุหรือถูกระงับการใช้งาน



การสื่อสารกับประชาชน

- ไม่ได้ทำให้การใช้งานยุ่งยากขึ้น แต่มีเป้าหมายเพื่อให้ใช้งานสะดวกและปลอดภัยกว่าเดิม
- ประชาชนควรเข้าใจว่าจะรับเอกสาร เก็บเอกสาร และแสดงเอกสารอย่างไร
- ประชาชนควรมั่นใจได้ว่าข้อมูลส่วนบุคคลจะถูกเปิดเผยเท่าที่จำเป็น
- มีคู่มือ คำอธิบาย หรือช่องทางช่วยเหลือที่ชัดเจน เพื่อไม่ให้รู้สึกว่าเป็นภาระ

“ข้อจำกัดของเอกสารอิเล็กทรอนิกส์แบบเดิมไม่ได้อยู่ที่การเป็นดิจิทัลหรือไม่เท่านั้น แต่อยู่ที่ความสามารถในการตรวจสอบสถานะ ความน่าเชื่อถือ และการใช้งานร่วมกันระหว่างหน่วยงาน ดังนั้น การพัฒนาในระยะต่อไปควรมุ่งแก้ปัญหาเชิงระบบ มากกว่าการเพิ่มช่องทางออกเอกสารเพียงอย่างเดียว”

“การพัฒนาเอกสารภาครัฐในรูปแบบใหม่มีเป้าหมายเพื่อให้ประชาชนใช้งานเอกสารได้สะดวก ปลอดภัย และตรวจสอบได้มากขึ้น โดยภาครัฐต้องสื่อสารวิธีใช้งานอย่างชัดเจน และต้องไม่ทำให้ประชาชนที่ยังไม่พร้อมด้านดิจิทัลเสียสิทธิในการเข้าถึงบริการ”



3. แนวทางการดำเนินการสำหรับหน่วยงานของรัฐในการประยุกต์ใช้ VC/VP

3.2 การเลือกเอกสารสำหรับการประยุกต์ใช้ในรูปแบบ VC/VP



VC/VP DIGITAL CREDENTIAL TRANSFORMATION



4 เกณฑ์ตัดสินใจเลือกเอกสารเพื่อทำ VC/VP



ความสำคัญตามกฎหมาย และการกำกับดูแล

เหมาะสำหรับเอกสารที่สถานะเปลี่ยนแปลงได้ เช่น มีโอกาสถูกระงับหรือเพิกถอน ระหว่างอายุใบอนุญาต



ความจำเป็นในการทำงานร่วมกัน (Interoperability)

ช่วยลดภาระการพัฒนาระบบเชื่อมต่อ (API) แบบจุดต่อจุด เมื่อต้องใช้งานข้ามหน่วยงานหรือภาคเอกชน



ความเสี่ยงด้านความถูกต้อง และการปลอมแปลง

เลือกเอกสารที่มีมูลค่าทางเศรษฐกิจสูง หรือหากปลอมแปลงแล้วจะกระทบต่อความปลอดภัยสาธารณะ



หลักการคุ้มครองข้อมูลส่วนบุคคล

เหมาะสำหรับเอกสารที่มีข้อมูลหลายประเภท แต่ต้องการเปิดเผยเฉพาะส่วนที่จำเป็น (Selective Disclosure)

จุดเด่นที่เหนือกว่าเอกสารดิจิทัลแบบเดิม (เช่น PDF)



vs



การบริหารสถานะแบบทันที (Real-Time Status)

ตรวจสอบสถานะ: เพิกถอน หรือระงับ ได้ทันทีโดยไม่ต้องเรียกคืนเอกสารตัวจริง



vs

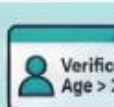


ตรวจสอบความถูกต้องได้โดยอิสระ

ผู้ตรวจสอบสามารถยืนยันความแท้จริงได้ด้วยเทคโนโลยีเข้ารหัสลับ โดยไม่ต้องสอบถามกลับไปยังผู้ออกเอกสารทุกครั้ง



vs



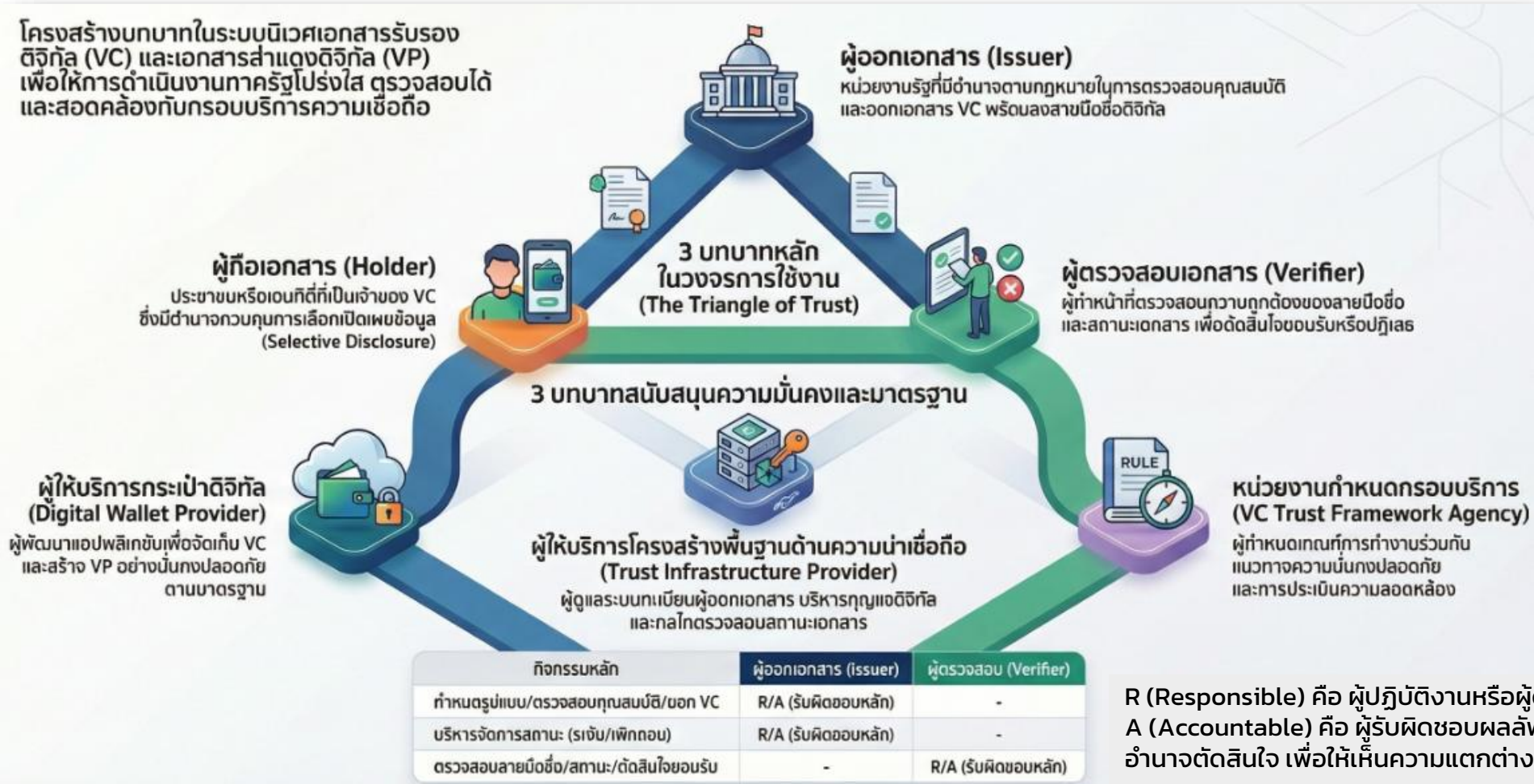
การเปิดเผยข้อมูลเท่าที่จำเป็น

เช่น การยืนยันว่าอายุเกิน 20 ปี โดยไม่ต้องเปิดเผยวันเดือนปีเกิดหรือเลขบัตรประชาชน



3. แนวทางการดำเนินการสำหรับหน่วยงานของรัฐในการประยุกต์ใช้ VC/VP

3.3 โครงสร้างบทบาท





3. แนวทางการดำเนินการสำหรับหน่วยงานของรัฐในการประยุกต์ใช้ VC/VP

3.4 – 3.7 กระบวนการพัฒนาและนำระบบไปใช้งานอย่างเป็นระบบตามหลักการพัฒนาระบบสารสนเทศ (SDLC)

3.4 การวิเคราะห์ช่องว่าง (Gap Analysis) — จุดเริ่มต้นสำคัญ

เริ่มจากเข้าใจ "ฐานเดิม" เพื่อต่อยอด "ระบบใหม่"

วิเคราะห์ว่าหน่วยงานมีอะไรอยู่แล้วและควรปรับปรุงส่วนใดโดยไม่ต้องรื้อระบบเดิมทั้งหมด

“Gap Analysis คือจุดเริ่มต้นของการเปลี่ยนผ่าน ไม่ใช่การเริ่มระบบใหม่ทั้งหมด”

5 ประเด็นวิเคราะห์เพื่อปิดช่องว่างสู่ VC/VP



3.5 การออกแบบและพัฒนา (Design & Development)



ผังโครงสร้างข้อมูล และกลไกควบคุมตามมาตรฐาน
กำหนดโครงสร้างข้อมูลตามมาตรฐานสากล และวางบทบาทกลไกควบคุมภายในให้ชัดเจน

3.6 ความพร้อมและการนำไปใช้งาน (Readiness & Deployment)



ทดสอบระบบและเริ่มจากโครงการนำร่อง (Pilot)
ทดสอบการออกและตรวจสอบเอกสารในขอบเขตจำกัดก่อนประเมินความพร้อมเพื่อเปิดใช้งานจริง

3.7 การตรวจสอบและความสอดคล้อง (Compliance & Governance)



เน้นความน่าเชื่อถือและการทำงานร่วมกัน (Interoperability)
กำหนดธรรมาภิบาลข้อมูลและประเมินความสอดคล้องของระบบเพื่อให้ใช้งานร่วมกับ Ecosystem

1) ศักยภาพของหน่วยงาน

หน่วยงานเริ่มใช้ VC/VP แบบ **ค่อยเป็นค่อยไป** โดยหลีกเลี่ยงการพัฒนา Wallet หรือโครงสร้างพื้นฐานเองทั้งหมดตั้งแต่ต้น แต่ให้เริ่มจากบทบาทที่จำเป็นก่อน เช่น ผู้ออกเอกสารหรือผู้ตรวจสอบเอกสาร

2) การเริ่มต้นดำเนินงาน

หน่วยงานเริ่มจาก **การเลือกเอกสารนำร่อง 1 ประเภท** ที่มีความเหมาะสมสูง และทำ Gap Analysis จากกระบวนการเดิมก่อน เพื่อให้การลงทุนและการออกแบบระบบสอดคล้องกับปัญหาจริง

3) ทรัพยากร

หน่วยงานเริ่มใช้วิธี **ต่อยอดจากระบบเดิม** เท่าที่ทำได้ และหลีกเลี่ยงการลงทุนสร้างระบบใหม่ทั้งชุดตั้งแต่ระยะแรก โดยเน้นการปรับกระบวนการ ข้อมูล และการเชื่อมต่อที่จำเป็นเป็นลำดับแรก

4) โครงสร้างพื้นฐานกลาง

ควรมีนโยบายสนับสนุน **แพลตฟอร์มกลาง** สำหรับองค์ประกอบที่ซับซ้อนและควรใช้ร่วมกัน เช่น กลไกความน่าเชื่อถือ การตรวจสอบสถานะ และข้อกำหนดร่วมด้านการเชื่อมโยง เพื่อไม่ให้เกิดภาระซ้ำซ้อนในแต่ละหน่วยงาน

5) การขยายผล

หน่วยงานสามารถเริ่มจาก **โครงการนำร่องในขอบเขตจำกัด** ก่อน แล้วจึงขยายผลเมื่อมีความพร้อมของมาตรฐาน กระบวนการ และโครงสร้างพื้นฐานกลางมากขึ้น

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล

ว่าด้วยแนวปฏิบัติกระบวนการทางดิจิทัลภาครัฐ – ส่วนที่ 8 เรื่อง เอกสารใบอนุญาตอิเล็กทรอนิกส์ภาครัฐในรูปแบบเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล



กรณีศึกษา

4.1 กรณีศึกษาต่างประเทศ

กรณีศึกษาที่สำคัญ (Key Case Studies)



European Digital Identity Wallet (EUDI Wallet)

การพัฒนาระบบนิเวศระบุตัวตนดิจิทัลและเอกสารรับรองที่ทำงานร่วมกันได้ข้ามพรมแดนในภูมิภาคยุโรป



ใบอนุญาตขับขี่ดิจิทัล (Digital Driving License)

การใช้ VC เพื่อออกใบอนุญาตที่ตรวจสอบสถานะได้แบบ Real-time และคุ้มครองข้อมูลส่วนบุคคล



Digital Passport และ Vaccine Certificate

การใช้มาตรฐานสากลเพื่อสร้างความปลอดภัยและความน่าเชื่อถือในการเดินทางระหว่างประเทศ

1. เริ่มจาก Use Case ที่มีความจำเป็นจริง



เน้นเอกสารมีผลทางกฎหมายใช้งานจริง และต้องมีการตรวจสอบข้ามหน่วยงานสม่ำเสมอ

2. ออกแบบ Ecosystem ไม่ใช่แค่ตัวเอกสาร



กำหนดบทบาท Issuer, Holder, Verifier และ Wallet ให้ทำงานร่วมกันอย่างเป็นระบบ

3. ยึดมาตรฐานสากลเพื่อ Interoperability



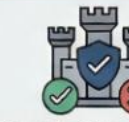
ใช้มาตรฐานกลาง (W3C, ISO) เพื่อลดการผูกขาดเทคโนโลยีและรองรับการใช้งานข้ามระบบ

4. ให้ผู้ถือเอกสารควบคุมข้อมูล (User-Centric)



รองรับ Selective Disclosure เพื่อให้ผู้ใช้งานเลือกเปิดเผยเฉพาะข้อมูลที่จำเป็นตามจริง

5. จัดให้มี Trust Infrastructure ส่วนกลาง

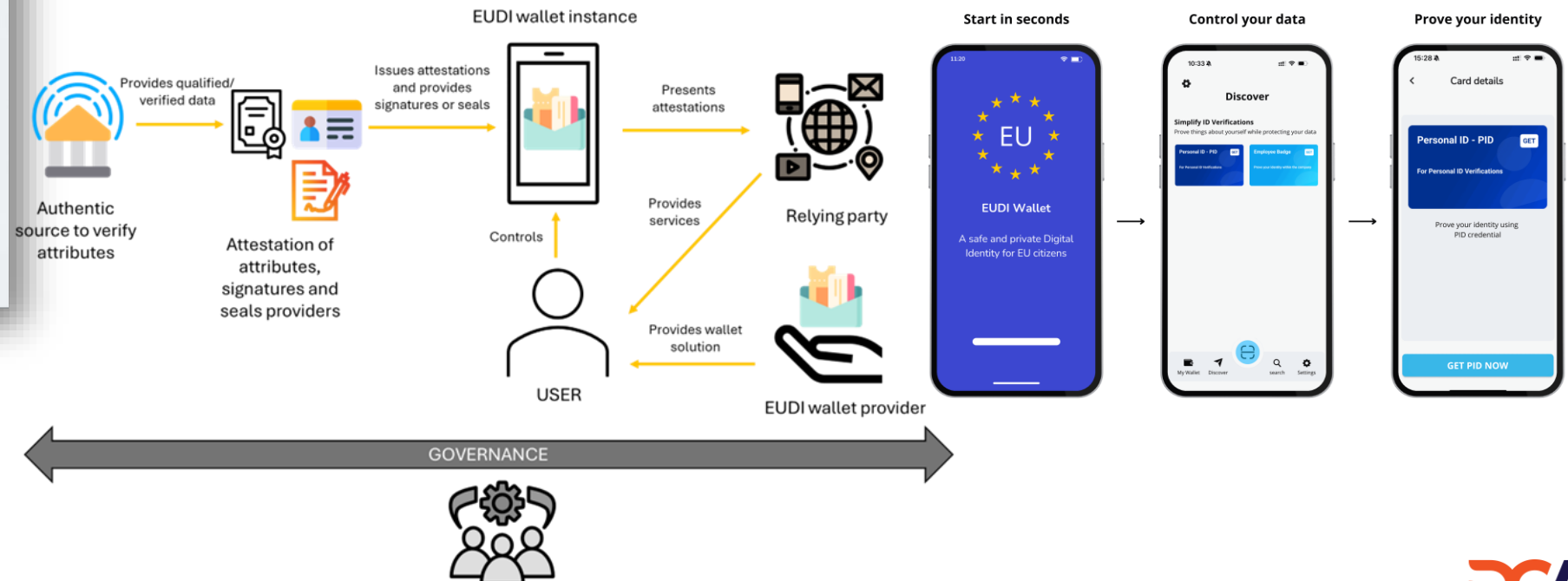


มีระบบ Registry และกลไกเพิกถอนที่ตรวจสอบได้กับที่โดยไม่ต้องสอบถามกลับทุกครั้ง

6. มีกลไกกำกับดูแลควบคู่กับเทคโนโลยี



กำหนดบทบาทความรับผิดชอบและเกณฑ์การยอมรับเอกสารให้ชัดเจนระดับระบบนิเวศ



มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล

ว่าด้วยแนวปฏิบัติกระบวนการทางดิจิทัลภาครัฐ – ส่วนที่ 8 เรื่อง เอกสารใบอนุญาตอิเล็กทรอนิกส์ภาครัฐในรูปแบบเอกสารรับรองดิจิทัลและเอกสารสำแดงดิจิทัล



กรณีศึกษา

4.2 กรณีศึกษาในประเทศไทย



ข้อค้นพบจากกรณีศึกษา



- ศักยภาพในการประยุกต์ใช้ที่หลากหลาย ประยุกต์ใช้ได้กับทั้งเอกสารทางการศึกษาและใบอนุญาตภาครัฐหลายประเภทอย่างเป็นรูปธรรม

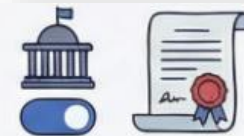


- มาตรฐานและความน่าเชื่อถือทางเทคนิค เอกสารออกและตรวจสอบได้ด้วยกระบวนการมาตรฐานที่เชื่อมโยง Semantic และ Schema ได้ชัดเจน



- แก้ปัญหาข้อจำกัดของเอกสารอิเล็กทรอนิกส์เดิม บรรเทาปัญหาการตรวจสอบด้วยสายตา การเชื่อมโยงข้อมูลซ้ำซ้อน และการเปิดเผยข้อมูลเกินความจำเป็น

สิ่งที่หน่วยงานของรัฐสามารถพิจารณาดำเนินการ



- การคัดเลือกเอกสารตามลำดับความสำคัญ เริ่มจากเอกสารที่มีความสำคัญทางกฎหมาย มีความเสี่ยงต่อการปลอมแปลง และต้องบริหารสถานะต่อเนื่อง



- เน้นการตรวจสอบข้ามหน่วยงานและภาคสนาม ให้ความสำคัญกับเอกสารที่ต้องใช้ตรวจสอบนอกสถานที่หรือมีการใช้งานร่วมกันระหว่างหลายหน่วยงาน



- การต่อยอดจากฐานความรู้เดิม ใช้กรณีศึกษาและแนวทางที่หน่วยงานนำร่อง (เช่น ETDA และมหาวิทยาลัย) จัดทำไว้เป็นแนวทางตั้งต้น