THE WORLD BANK | ETDA

VC Recommendation Policy

การยกระดับโครงสร้างพื้นฐานความเชื่อมั่นดิจิทัลของประเทศไทย

ผ่านการขยายผลการใช้งาน Digital ID และ Verifiable Credentials



BUILDING THAILAND'S DIGITAL TRUST INFRASTRUCTURE:
SCALING DIGITAL IDENTITY AND VERIFIABLE CREDENTIALS

JULY 2026 | VERSION 1.2

เอกสารข้อเสนอแนะเชิงนโยบาย

เรื่อง **การยกระดับโครงสร้างพื้นฐานความเชื่อมั่นดิจิทัลของประเทศไทยผ่านการขยายผลการใช้งาน Digital ID และ Verifiable Credentials**

Building Thailand's Digital Trust Infrastructure:
Scaling Digital Identity and Verifiable Credentials

กรกฎาคม 2569
เวอร์ชัน 1.2



THE WORLD BANK

1 บทสรุปผู้บริหาร 4

2 บทนำ 10

2.1 วัตถุประสงค์ 12

3 **ตัวอย่างกรณีการใช้งาน** 14

3.1 ความสำคัญและโอกาสในการประยุกต์ใช้เอกสารรับรองดิจิทัล (VC)เพื่อการยืนยันอัตลักษณ์พื้นฐาน 14

3.2 การยืนยันตัวตน ณ จุดให้บริการ (NFC / Bluetooth) 15

3.3 การยืนยันอายุออนไลน์โดยคุ้มครองความเป็นส่วนตัว 15

3.4 การเข้าถึงสินเชื่อ: เอกสารรับรองดิจิทัล (VC) สถานะทางการเงินและการสมัครสินเชื่อ MSME 16

3.5 สวัสดิการสังคม: การใช้สิทธิ์รับเงินชดเชยค่าน้ำมันแบบเฉพาะกลุ่มสำหรับแรงงานนอกระบบ 17

3.6 บริการแพทย์ทางไกลและใบสั่งยาดิจิทัล 18

3.7 การยื่นเอกสารรับรองดิจิทัล (VC) เพื่อการค้าในภูมิภาคอาเซียน (กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับ นิติบุคคล) 19

3.8 การตรวจสอบเอกสารรับรองดิจิทัล (VC) ทางการศึกษาและวิชาชีพ 19

3.9 การเช่ารถในต่างประเทศด้วยใบอนุญาตขับขี่ดิจิทัล 20

3.10 บัตรขาเข้าดิจิทัล (ใบตม.6) และการเช็คอินเข้าพักโรงแรม 20

3.11 การยืนยันตัวตนผู้ขายออนไลน์เพื่อป้องกันการฉ้อโกงบนแพลตฟอร์มดิจิทัล 21

4 **ผลสัมฤทธิ์เชิงประจักษ์** 23

4.1 การลดภาระต้นทุนการลงทะเบียนและการปฏิบัติตามกฎระเบียบ 23

4.2 การลดการฉ้อโกงและการเสริมสร้างยกระดับความมั่นคงปลอดภัย 23

4.3 ประสิทธิภาพการบริหารและการเพิ่มผลผลิต 24

4.4 ผลกระทบระดับเศรษฐกิจและประโยชน์ต่อภาคธุรกิจ 24

4.5 ผลกระทบต่อประเทศไทย 25

5 **ข้อเสนอแนะเชิงนโยบาย** 26

5.1 การจัดตั้งกรอบแนวทางการสร้างความเชื่อถือแห่งชาติสำหรับเอกสารรับรองดิจิทัล (VC) อย่างเป็นทางการ 26

5.2 พัฒนาและกำกับดูแลระบบนิเวศของกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ตามมาตรฐานและข้อกำหนดที่เกี่ยวข้อง 27

5.3 กำหนดให้มีการออกเอกสารรับรองดิจิทัล (VC) พื้นฐานและการยอมรับจากทุกภาคส่วนที่เกี่ยวข้อง 28

5.4 กำหนดลำดับความสำคัญกรณีการใช้งานที่มีผลกระทบสูง 5 ประการ 31

5.5 การเป็นผู้นำของอาเซียนในการพัฒนามาตรฐานระดับภูมิภาค 33

6 **กรอบแนวทางการขับเคลื่อนเพื่อพัฒนาระบบนิเวศของการใช้เอกสารรับรองดิจิทัลที่ตรวจสอบได้** . 34

6.1 ระยะที่ 1 (พ.ศ. 2569) : จัดทำกรอบอำนาจทางกฎหมายและระบบธรรมาภิบาลที่สามารถบังคับใช้ได้ 34

6.2 ระยะที่ 2 (พ.ศ. 2570) : กำหนดให้มีการออกเอกสารรับรองดิจิทัล (VC) ให้เป็นที่ยอมรับในภาครัฐและภาคส่วนที่อยู่ภายใต้การกำกับดูแล พร้อมนำกรณีการใช้งานที่มีความสำคัญสูงมาใช้งานจริง 36
6.3 ระยะที่ 3 (พ.ศ. 2571–2572) : ดำเนินการขยายการใช้งานสู่ระดับประเทศและส่งเสริมให้มีการรับรองซึ่งกันและกันในระดับอาเซียน 37
6.4 ระยะที่ 4 (พ.ศ. 2573–2575) : การสร้างความยั่งยืนและการนำไปใช้ในเชิงพาณิชย์ที่มีศักยภาพ 38
6.5 สรุปบทบาทและความรับผิดชอบ 39

7 **ประมาณการงบประมาณที่ต้องใช้จ่ายสำหรับการดำเนินงานระยะที่** 2 (**พ.ศ.** 2570) 43

ภาคผนวก ก – ภูมิหลัง 45
ก.1 ปัจจัยขับเคลื่อนเพื่อการเปลี่ยนแปลง 45
ก.2 ความจำเป็นในการกำกับดูแลที่เข้มแข็งและความรับผิดชอบที่ชัดเจน 46
ก.3 การสร้างโครงสร้างพื้นฐานดิจิทัลของประเทศที่สามารถขยายการใช้งานและมีความยืดหยุ่น 48
ก.4 ขอบเขตของกรอบการสร้างความน่าเชื่อถือของเอกสารรับรองและเอกสารสำแดง 51
ก.5 การสร้างความน่าเชื่อถือของเอกสารรับรองดิจิทัล (VC) และการรักษาความมั่นคงปลอดภัย 54
ก.6 การคัดเลือกกรณีการใช้งานระดับประเทศที่มีผลกระทบสูง 56
ก.7 การปรับปรุงการบูรณาการบริการและการแลกเปลี่ยนข้อมูลในภาครัฐ 57
ก.8 แหล่งข้อมูลทางการที่มีศักยภาพ 59
ก.9 หน่วยงานหลักของภาครัฐ 59

ภาคผนวก ข – การวิเคราะห์และประเด็นท้าทายสำคัญ 61
ข.1 การป้องกันความเสี่ยงจากการฉ้อโกงและการเสริมสร้างความมั่นคงปลอดภัยสาธารณะ 61
ข.2 กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับธุรกิจและผลกระทบทางเศรษฐกิจ 62
ข.3 การเพิ่มประสิทธิภาพและการเข้าถึงบริการภาครัฐ 65
ข.4 ความชัดเจนเกี่ยวกับผู้ให้บริการกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ของภาครัฐ 67
ข.5 ความสอดคล้องกับพระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. 2565 70
ข.6 ประโยชน์ของมาตรฐาน 70

1 บทสรุปผู้บริหาร

ตามที่ได้มีการประกาศนโยบายของรัฐบาลชุดใหม่ หนึ่งในนโยบายที่มีความสำคัญคือการปรับปรุงประสิทธิภาพการบริหารงานของภาครัฐโดยเฉพาะการปรับปรุงและพัฒนาโครงสร้างพื้นฐานด้านความน่าเชื่อถือทางดิจิทัล และวางบทบาทของประเทศอย่างเหมาะสมเพื่อรองรับการเติบโตทางเศรษฐกิจในอนาคต โดยเฉพาะภายใต้บริบทด้านการขยายตัวของบริการดิจิทัลและการค้าข้ามพรมแดน ซึ่งมีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่องตามกรอบการบูรณาการของอาเซียน (ASEAN) ในการนี้ระบบที่เกี่ยวข้องกับการยืนยันตัวตนดิจิทัล การรับรองความน่าเชื่อถือของข้อมูล และการแลกเปลี่ยนข้อมูลที่เป็นประโยชน์ระหว่างหน่วยงานต่างๆ ทั้งหน่วยงานภาครัฐและเอกชน จึงมีความสำคัญเชิงยุทธศาสตร์อย่างยิ่งต่อการยกระดับประสิทธิภาพการให้บริการภาครัฐ การสนับสนุนการดำเนินธุรกิจ และการสร้างความเชื่อมั่นในระบบเศรษฐกิจดิจิทัลของประเทศ

อย่างไรก็ดี ในปัจจุบันกระบวนการยืนยันตัวตนและการใช้เอกสารประกอบการให้บริการดิจิทัลยังคงประสบข้อจำกัดหลายประการ อาทิ การยื่นเอกสารซ้ำซ้อน การส่งภาพถ่ายบัตรประจำตัวประชาชน การใช้สำเนาเอกสารกระดาษและเอกสารอิเล็กทรอนิกส์ที่ยากต่อการตรวจสอบความถูกต้อง ซึ่งก่อให้เกิดต้นทุนในการดำเนินงานที่สูงขึ้น ส่งผลให้กระบวนการให้บริการมีความล่าช้า และเพิ่มความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูล นอกจากนี้สถานการณ์การฉ้อโกงทางออนไลน์ การแอบอ้างหรือปลอมแปลงตัวตน และการใช้เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) ในการสร้างข้อมูลหรือเอกสารปลอม มีแนวโน้มทวีความรุนแรงและซับซ้อนมากยิ่งขึ้นอย่างต่อเนื่อง จึงมีความจำเป็นที่ประเทศไทยจะต้องเร่งพัฒนาโครงสร้างพื้นฐานด้านความน่าเชื่อถือทางดิจิทัลให้มีความมั่นคง ปลอดภัย เชื่อมโยงกันได้ และรองรับการใช้งานในระดับประเทศและระดับภูมิภาคได้อย่างมีประสิทธิภาพ

ด้วยเหตุนี้การดำเนินการเพื่อยกระดับโครงสร้างพื้นฐานด้านความเชื่อมั่นดิจิทัลของประเทศไทยให้เกิดผลอย่างเป็นรูปธรรม จึงมีความจำเป็นอย่างยิ่ง โดยควรมุ่งเน้นการปรับเปลี่ยนแนวทางสำคัญในสามมิติ ได้แก่ 1) การเปลี่ยนผ่านจากการยื่นเอกสารประกอบการให้บริการ ไปสู่การแลกเปลี่ยนข้อมูลที่มีความน่าเชื่อถือ 2) การเปลี่ยนผ่านจากการยืนยันตัวตนด้วยวิธีการแบบพบเห็นหน้า ไปสู่การยืนยันตัวตนออนไลน์ที่มีความปลอดภัยด้วยวิทยาการเข้ารหัสลับ และ 3) การเปลี่ยนผ่านจากระบบดิจิทัลที่ต่างคนต่างให้บริการ ไปสู่ระบบที่สามารถเชื่อมโยงและบูรณาการข้อมูลร่วมกันเพื่อให้บริการได้อย่างมีประสิทธิภาพ

ในบริบทของการปรับเปลี่ยนแนวทางดังกล่าว การนำเอกสารรับรองดิจิทัล (Verifiable Credential: VC) มาใช้งาน จึงเป็นแนวทางสำคัญที่มีความปลอดภัย สามารถรองรับการขยายการใช้งานในวงกว้าง และได้รับการพัฒนาเป็นมาตรฐานสากลแล้ว โดยหลายประเทศได้เริ่มนำกรอบความเชื่อมั่นแห่งชาติสำหรับเอกสารรับรองดิจิทัลมาใช้ในการดำเนินงานจริง เพื่อสนับสนุนการยืนยันตัวตน การรับรองคุณสมบัติ และการแลกเปลี่ยนข้อมูลที่เชื่อถือได้ในระบบดิจิทัล นอกจากนี้การบูรณาการทางดิจิทัลภายใต้กรอบความตกลงเศรษฐกิจดิจิทัลอาเซียน (Digital Economy Framework Agreement: DEFA) อยู่ระหว่างการเร่งรัดพัฒนา

และมีแนวโน้มที่จะนำไปสู่การกำหนดมาตรฐานระดับภูมิภาคสำหรับการแลกเปลี่ยนข้อมูลที่น่าเชื่อถือ ดังนั้น จึงนับเป็นโอกาสสำคัญของประเทศไทยในการมีบทบาทเชิงรุกต่อการกำหนดทิศทาง มาตรฐาน และแนวทางการดำเนินงานด้านความเชื่อมั่นดิจิทัลในระดับภูมิภาค เพื่อเสริมสร้างขีดความสามารถในการแข่งขัน และรองรับการเชื่อมโยงบริการดิจิทัลและการค้าข้ามพรมแดนในอนาคต

ประเทศไทยมีความพร้อมในการดำเนินการเพื่อยกระดับโครงสร้างพื้นฐานด้านความเชื่อมั่นดิจิทัลได้อย่างรวดเร็ว เนื่องจากมีโครงสร้างพื้นฐานดิจิทัลที่สำคัญรองรับอยู่แล้วหลายประการ อาทิ แอปพลิเคชัน ThaID ซึ่งทำหน้าที่เป็นแอปพลิเคชันอัตลักษณ์ดิจิทัลแห่งชาติ และแพลตฟอร์ม “ทางรัฐ” ซึ่งเป็นแอปพลิเคชันสำหรับการให้บริการภาครัฐ โดยมีฐานผู้ใช้งานจำนวนหลายสิบล้านคน นอกจากนี้ ประเทศไทยยังมีฐานข้อมูลบัตรประจำตัวประชาชนและทะเบียนธุรกิจภายในประเทศ ซึ่งเป็นแหล่งข้อมูลทางการในรูปแบบดิจิทัลที่สามารถนำมาใช้สนับสนุนการให้บริการภาครัฐและภาคธุรกิจได้อย่างมีประสิทธิภาพ นอกจากนี้ในส่วนของการกำหนดแนวทางและมาตรฐานการเชื่อมโยงด้านเทคนิค สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ได้จัดทำรายงานกรอบแนวทางการทำงานร่วมกันสำหรับเอกสารรับรองดิจิทัล (Verifiable Credential: VC) ซึ่งสอดคล้องกับมาตรฐานสากล ประกอบกับการที่มีผู้ให้บริการพิสูจน์และยืนยันตัวตน (Identity Provider) ภาครัฐและภาคเอกชนที่ได้รับใบอนุญาตหลายรายอยู่ก่อนแล้ว ทำให้เป็นแรงขับเคลื่อนสำคัญที่ช่วยเสริมสร้างความเข้มแข็งให้แก่โครงสร้างพื้นฐานด้านความเชื่อมั่นดิจิทัลของประเทศอย่างมีนัยสำคัญ การดำเนินการดังกล่าวยังมีความสอดคล้องกับนโยบายของรัฐบาลและเจตนารมณ์ของพระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. 2565 ซึ่งมุ่งส่งเสริมให้หน่วยงานของรัฐให้บริการประชาชนในรูปแบบดิจิทัล และกำหนดให้มีการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานภาครัฐอย่างสอดคล้อง เชื่อมโยงกันได้ มีความมั่นคงปลอดภัย และประชาชนสามารถเข้าถึงได้โดยสะดวก ทั้งนี้ การนำเอกสารรับรองดิจิทัล (VC) มาใช้ จะช่วยสนับสนุนให้การให้บริการดังกล่าวสามารถขยายผลได้ในวงกว้างมากยิ่งขึ้น

จากข้อเท็จจริงที่ปรากฏในต่างประเทศ พบว่าการนำเอกสารรับรองที่ตรวจสอบได้ (VC) ในรูปแบบดิจิทัลมาใช้งาน ดังกล่าวสามารถก่อให้เกิดประโยชน์ทางเศรษฐกิจและสังคมอย่างมีนัยสำคัญ โดยคณะกรรมาธิการยุโรปประเมินว่า การใช้กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับประชาชนสามารถช่วยลดค่าใช้จ่ายในภาคบริการทางการเงินได้ประมาณ 0.68–1.36 พันล้านยูโรต่อปี และในระบบสุขภาพดิจิทัลประมาณ 1.26–2.51 พันล้านยูโรต่อปี จากการลดต้นทุนในกระบวนการลงทะเบียนเข้าใช้บริการและการยืนยันตัวตนเพียงอย่างเดียว นอกจากนี้ ยังสามารถลดต้นทุนจากภาระงานด้านการบริหารจัดการของประชาชนได้ประมาณ 350–400 ล้านยูโรต่อปี ผลการดำเนินโครงการนำร่องในต่างประเทศยังแสดงให้เห็นว่า ระยะเวลาในการลงทะเบียนเข้าใช้บริการสามารถลดลงจากหลายวันเหลือเพียงไม่กี่นาที ขณะที่ในระดับเศรษฐกิจโดยรวม หากมีการขยายการใช้งานกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับภาคธุรกิจอย่างเต็มรูปแบบ อาจก่อให้เกิดผลประโยชน์ทางเศรษฐกิจสูงถึง 116 พันล้านยูโรต่อปี โดยผลประโยชน์ดังกล่าวเกิดจากการลดความซ้ำซ้อนของกระบวนการ การให้บริการที่รวดเร็วขึ้น การลดความสูญเสียจากการฉ้อโกง และการโอนย้ายข้อมูลที่มีความปลอดภัยและน่าเชื่อถือ

ข้อเท็จจริงข้างต้นมีความเกี่ยวข้องโดยตรงกับแนวทางการดำเนินงานของประเทศไทย เนื่องจากในปัจจุบันการหลอกลวงทางออนไลน์และการฉ้อโกงสร้างความเสียหายคิดเป็นมูลค่าประมาณ 45,000 ล้านบาทต่อปี และมีการรายงานคดีจำนวนหลายร้อยคดีในแต่ละวัน โดยหลายกรณีอาศัยจุดอ่อนของระบบยืนยันตัวตนด้วยเอกสาร เช่น การใช้บัตรประจำตัวประชาชนปลอม เอกสารที่ถูกแก้ไข หรือการปลอมแปลงตัวตน แม้ว่าการนำเอกสารรับรองดิจิทัล (VC) มาใช้สนับสนุนการให้บริการ จะไม่สามารถขจัดการฉ้อโกงได้อย่างสิ้นเชิง แต่สามารถช่วยลดความเสี่ยงและความเสียหายจากการฉ้อโกงได้อย่างมีนัยสำคัญ ในขณะเดียวกัน ก็ให้ประโยชน์ต่อการลดอุปสรรคในกระบวนการลงทะเบียนเข้าใช้บริการ การออกใบอนุญาต และการปฏิบัติตามกฎระเบียบของภาคธุรกิจและเสริมสร้างขีดความสามารถในการแข่งขันของประเทศไทยในด้านการค้าดิจิทัลระดับภูมิภาค ทั้งนี้ในช่วงเวลาที่มาตรฐานระดับโลกและระดับภูมิภาคด้านความเชื่อมั่นดิจิทัลกำลังพัฒนาอย่างรวดเร็ว หากประเทศไทยดำเนินการล่าช้า อาจต้องปรับตัวตามกรอบด้านกฎระเบียบและมาตรฐานที่ประเทศอื่นหรือองค์กรระหว่างประเทศเป็นผู้กำหนด และอาจสูญเสียโอกาสในการมีบทบาทเชิงรุกในการกำหนดทิศทาง กรอบกติกา และมาตรฐานที่สอดคล้องกับบริบทและผลประโยชน์ของประเทศ

ข้อเสนอแนะเชิงวิชาการฉบับนี้จึงมีข้อเสนอเชิงนโยบายเกี่ยวกับการดำเนินการสำคัญ 5 ประการ โดยมีวัตถุประสงค์เพื่อยกระดับความน่าเชื่อถือด้านดิจิทัลของเศรษฐกิจไทยในระดับอาเซียน เสริมสร้างศักยภาพให้ประชาชนและผู้พำนักในประเทศสามารถแลกเปลี่ยนข้อมูลของตนได้ภายใต้เงื่อนไขที่กำหนด และวางรากฐานโครงสร้างพื้นฐานด้านความเชื่อมั่นดิจิทัลให้แก่ภาคธุรกิจ เพื่อสนับสนุนการเติบโตทั้งในระดับประเทศ ระดับภูมิภาค และระดับโลก

ภาครัฐของไทยจึงควรพิจารณาดำเนินการดังต่อไปนี้

- **จัดทำกรอบแนวทางทางการขับเคลื่อนเพื่อพัฒนาระบบนิเวศของการใช้เอกสารรับรองดิจิทัลที่ตรวจสอบได้** (Verifiable Credential Trust Framework) อย่างเป็นทางการ เพื่อกำหนดทิศทาง หลักเกณฑ์ และกลไกการดำเนินงานด้านเอกสารรับรองดิจิทัล (Verifiable Credential: VC) ของประเทศให้มีความเป็นเอกภาพ สอดคล้องกับมาตรฐานสากล และสามารถนำไปใช้ได้อย่างมั่นคง ปลอดภัยในวงกว้าง การดำเนินการดังกล่าวอาจพิจารณาขับเคลื่อนผ่านมติคณะรัฐมนตรี หรือกลไกของคณะกรรมการระดับชาติที่เกี่ยวข้อง เพื่อมอบหมายให้ สพธอ. ซึ่งมีอำนาจหน้าที่ในการกำกับดูแลการประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ตามพระราชกฤษฎีกาที่ออกตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ เป็นหน่วยงานหลักในการดำเนินการรับรองบริการด้านเอกสารรับรองดิจิทัล (VC)ให้มีความน่าเชื่อถือ นอกจากนี้ สพธอ. ควรมีบทบาทในการจัดทำข้อเสนอแนะ มาตรฐาน หลักเกณฑ์ หรือแนวทางปฏิบัติที่เกี่ยวข้อง เพื่อให้หน่วยงานภาครัฐ ภาคธุรกิจ และผู้ให้บริการที่เกี่ยวข้องสามารถใช้เทคโนโลยีดิจิทัลที่สอดคล้องกัน เชื่อมโยงและทำงานร่วมกันได้อย่างมั่นคงปลอดภัย มีความน่าเชื่อถือ มีกลไกรับผิดชอบที่ชัดเจน และสามารถขยายการใช้งานได้ในระดับประเทศ
- **พัฒนาและกำกับดูแลระบบนิเวศของกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ให้ได้มาตรฐานและข้อกำหนดที่เกี่ยวข้อง** กำหนดให้มีระบบการรับรองมาตรฐานกระเป๋าเอกสารดิจิทัล 2 ประเภท ได้แก่ (1) สำหรับบุคคลธรรมดา และ (2) สำหรับนิติบุคคล รวมถึงจำกัดจำนวนผู้ให้บริการกระเป๋าเอกสารดิจิทัลหลักของภาครัฐได้ไม่เกินประเภทละ 2 ราย ทั้งในส่วนของบุคคลธรรมดาและนิติบุคคล ดังกล่าวต้องรองรับการเชื่อมโยงข้อมูล การทำงานร่วมกัน (Interoperability) และการโอนย้ายข้อมูลระหว่างระบบได้อย่างปลอดภัยและมีประสิทธิภาพ ทั้งนี้สำหรับผู้ให้บริการภาคเอกชน จะไม่มีการจำกัดจำนวน เพื่อส่งเสริมการพัฒนานวัตกรรมและการแข่งขันอย่างเสรี แนวทางดังกล่าวจะช่วยสร้างสมดุลระหว่างการส่งเสริมนวัตกรรม กับความเป็นเอกภาพของระบบ ความสอดคล้องกับทิศทางนโยบายดิจิทัล และความสะดวกในการใช้งานสำหรับประชาชนและภาคธุรกิจ
- **กำหนดให้มีการออกเอกสารรับรองดิจิทัล (VC) พื้นฐานและให้มีการยอมรับจากทุกภาคส่วน** โดยให้หน่วยงานสำคัญที่เกี่ยวข้องกับการออกเอกสารรับรองดิจิทัล (VC) พื้นฐาน ดำเนินการให้สอดคล้องกับข้อกำหนดของ สพธอ. และหน่วยงานกำกับดูแลภาคธุรกิจเฉพาะต่างๆ เช่น ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ และสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ พร้อมทั้งกำหนดให้มีการยอมรับโดยทั่วไปในการให้บริการสาธารณะต่าง ๆ ทั้งนี้ ควรมีการจัดตั้งกองทุนเพื่อสนับสนุนการจัดทำเอกสารรับรองดิจิทัล (VC) และการพัฒนาขีดความสามารถในการออกเอกสารรับรองดิจิทัล (VC) ร่วมกัน โดยบูรณาการกับศูนย์แลกเปลี่ยนข้อมูลกลางภาครัฐ (Government Data Exchange: GDX) และระบบทะเบียนเอกสารรับรอง (verifiable data registry) รวมถึงการพัฒนา

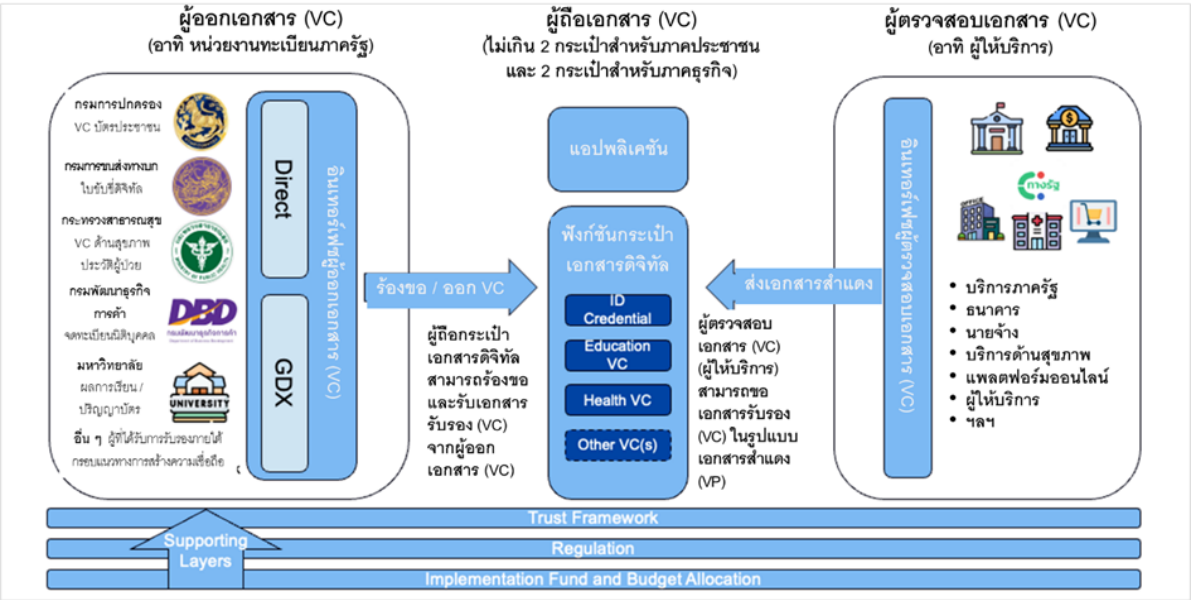
ขีดความสามารถในการตรวจสอบของแอปพลิเคชันทางรัฐ และการจัดชุดเครื่องมือพัฒนาซอฟต์แวร์สำหรับการตรวจสอบสากล (Universal Verifier SDK) เพื่อรองรับการให้บริการดิจิทัลของภาครัฐ

- **กำหนดลำดับความสำคัญของกรณีการใช้งานระดับประเทศที่มีผลกระทบสูง จำนวน 5 กรณี** เพื่อใช้เป็นแนวทางแสดงความคุ้มค่าและผลสัมฤทธิ์ของการดำเนินงานในระยะแรก อาทิ การเข้าถึงสินเชื่อของภาคธุรกิจ โดยเฉพาะวิสาหกิจรายย่อย ขนาดกลาง และขนาดย่อม (MSME) การยืนยันอายุผ่านช่องทางออนไลน์โดยคุ้มครองข้อมูลส่วนบุคคล การเข้าถึงสวัสดิการสังคม การโอนย้ายเอกสารรับรองดิจิทัล (VC) ด้านสุขภาพ และเอกสารรับรองดิจิทัล (VC) ด้านใบอนุญาตขับขี่ วิชาชีพ และการศึกษา ทั้งนี้ กรณีการใช้งานดังกล่าวมีความเหมาะสม สำหรับดำเนินการเป็นโครงการนำร่อง เนื่องจากมีปริมาณธุรกรรมสูง สามารถติดตามผล ได้อย่างชัดเจน และแสดงให้เห็นประโยชน์ต่อประชาชน ภาคธุรกิจ และภาครัฐได้อย่างเป็นรูปธรรม
- **เป็นผู้นำของอาเซียนในการพัฒนามาตรฐานระดับภูมิภาคภายใต้กรอบความตกลงเศรษฐกิจดิจิทัล (DEFA)** โดยดำเนินการผ่านกระบวนการการประชุมรัฐมนตรีดิจิทัลอาเซียน (ADGMIN) และการประชุมรัฐมนตรีเศรษฐกิจอาเซียน (AEM) พร้อมกับเป็นประเทศแรกในอาเซียนที่นำเอกสารรับรองดิจิทัล (VC) มาใช้จริงในระดับประเทศ และวางบทบาทประเทศไทยให้เป็นตัวเชื่อมระหว่างอาเซียนกับกรอบความน่าเชื่อถือทางดิจิทัลระดับโลก

การดำเนินการสามารถแบ่งออกเป็น 4 ระยะ ดังนี้

- **ระยะที่ 1 (พ.ศ. 2569)** จัดทำกรอบอำนาจทางกฎหมายและระบบธรรมาภิบาลที่สามารถบังคับใช้ได้
- **ระยะที่ 2 (พ.ศ. 2570)** กำหนดให้มีการออกเอกสารรับรองดิจิทัล (VC) ให้เป็นที่ยอมรับในภาครัฐและภาคส่วนที่อยู่ภายใต้การกำกับดูแล พร้อมนำกรณีการใช้งานที่มีความสำคัญสูงมาใช้งานจริง
- **ระยะที่ 3 (พ.ศ. 2571 – 2572)** ดำเนินการขยายการใช้งานสู่ระดับประเทศ และส่งเสริมให้มีการรับรองซึ่งกันและกันในระดับอาเซียน
- **ระยะที่ 4 (พ.ศ. 2573 – 2575)** การสร้างความยั่งยืนและการนำไปใช้ในเชิงพาณิชย์ที่มีศักยภาพ

ความต้องการงบประมาณในเบื้องต้นสำหรับการดำเนินการระยะที่ 2 เมื่อเทียบกับผลลัพธ์ของการดำเนินการอยู่ในระดับต่ำ สำหรับช่วง 1 ถึง 2 ปีงบประมาณ มีความจำเป็นในการใช้งบประมาณ จำนวน 490 - 1,160 ล้านบาท ครอบคลุมการพัฒนาโครงสร้างพื้นฐานร่วม การยกระดับกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) การบูรณาการระหว่างหน่วยงานที่มีความสำคัญสูง และการสนับสนุนการพัฒนาระบบนิเวศ รวมถึงแนวทางแบบรวมศูนย์ โดยเฉพาะการพัฒนาขีดความสามารถในการออกเอกสารรับรองดิจิทัล (VC) ร่วม โดยใช้ศูนย์แลกเปลี่ยนข้อมูลกลางภาครัฐ (GDX) เป็นฐาน ซึ่งจะสามารถลดความซ้ำซ้อนและต้นทุนของระบบโดยรวมได้อย่างมีนัยสำคัญ การให้ความสำคัญกับโครงสร้างพื้นฐานร่วมเป็นอันดับแรก และมุ่งเน้นการดำเนินการของหน่วยงานเฉพาะสำหรับกรณีการใช้งานที่มีผลกระทบสูงเป็นลำดับที่ 2 จะช่วยเพิ่มผลตอบแทนจากการลงทุนและเห็นผลลัพธ์อย่างเป็นรูปธรรม



รูปที่ 1 —ข้อเสนอสำหรับรูปแบบระบบนิเวศเอกสารรับรองดิจิทัล (VC) ของประเทศไทย

2 บทนำ

ปัจจุบันประเทศไทยอยู่ระหว่างการเปลี่ยนผ่านสู่เศรษฐกิจดิจิทัลอย่างเต็มรูปแบบ อย่างไรก็ตาม กระบวนการยืนยันตัวตนและวิธีการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานภาครัฐและภาคเอกชนยังคงมีข้อจำกัด ปัจจุบันการดำเนินการยืนยันตัวตนและการแลกเปลี่ยนข้อมูลส่วนใหญ่ยังคงใช้การยื่นเอกสารที่ซ้ำซ้อน การส่งภาพถ่ายบัตรประจำตัวประชาชน การตรวจสอบฐานข้อมูลด้วยตนเอง และการเชื่อมต่อระบบเฉพาะกิจระหว่าง หน่วยงาน กับผู้ให้บริการภาคเอกชนโดยที่ประชาชนและภาคธุรกิจมักถูกกำหนดให้ยื่นข้อมูลชุดเดิมหลายครั้งเนื่องจากข้อมูลหรือเอกสารที่ผ่านการยืนยันในระบบหนึ่งไม่สามารถนำไปใช้ซ้ำหรือได้รับการรับรองในอีกระบบหนึ่งได้ ความซ้ำซ้อนดังกล่าว ส่งผลให้เกิดภาระต้นทุนการบริหารเพิ่มขึ้น การให้บริการเกิดความล่าช้า และเกิดความเสี่ยงด้านความมั่นคงปลอดภัย โดยปัญหาดังกล่าวยังคงอยู่แม้จะมีพระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์จะกำหนดให้หน่วยงานของรัฐต้องให้บริการในรูปแบบดิจิทัลซึ่งสะท้อนให้เห็นถึงความจำเป็นอย่างมากในการพัฒนารูปแบบการแลกเปลี่ยนข้อมูลหน่วยงานที่มีความน่าเชื่อถือและสามารถทำงานร่วมกันได้

ในขณะเดียวกัน ประเทศไทยยังคงเผชิญกับปัญหาการหลอกลวงและการฉ้อโกงออนไลน์ในระดับสูง ซึ่งมาจากการหลอกลวงที่อาศัยการปลอมแปลงอัตลักษณ์และวิศวกรรมสังคม (Social Engineering) โดยมีมูลค่าความเสียหายหลายพันล้านบาทต่อปี ความก้าวหน้าอย่างรวดเร็วของปัญญาประดิษฐ์ (AI) ส่งผลให้การปลอมแปลงตัวตน และการฉ้อโกงที่อาศัยเทคโนโลยีดีปเฟก (Deepfake) รวมถึงการโจมตีแบบฟิชชิงโดยอัตโนมัติ (Automated Phishing Attacks) มีความซับซ้อนและแพร่หลายมากยิ่งขึ้น ซึ่งทำให้ความน่าเชื่อถือของระบบการยืนยันตัวตนด้วยเอกสารแบบดั้งเดิมลดลง ด้วยเหตุนี้ ระบบที่กำกับดูแลกระบวนการออก จัดเก็บ แบ่งปัน และตรวจสอบเอกสารรับรองดิจิทัล (VC) จึงได้กลายเป็นองค์ประกอบสำคัญของโครงสร้างพื้นฐานด้านความน่าเชื่อถือทางดิจิทัลของประเทศ

เอกสารรับรองดิจิทัล (VC) เป็นแนวทางแก้ไขปัญหาดังกล่าวได้อย่างเป็นรูปธรรม กล่าวคือ เอกสารรับรองดิจิทัล (VC) คือข้อความลงลายมือชื่อดิจิทัล (Digital Signature) ที่ออกโดยหน่วยงานที่มีอำนาจหน้าที่หรือองค์กรที่ได้รับความเชื่อถือ เช่น หน่วยงานภาครัฐ สถาบันการศึกษา หรือหน่วยงานกำกับดูแล ซึ่งสามารถจัดเก็บไว้ในกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ได้อย่างมั่นคงปลอดภัย และนำออกมาแสดงเพื่อการตรวจสอบได้ตามต้องการ เปรียบได้กับบัตรประจำตัวประชาชนที่พกพาไว้ในกระเป๋าสตางค์ เอกสารรับรองดิจิทัล (VC) ช่วยให้สามารถพกพาและใช้เอกสารที่น่าเชื่อถือได้ทุกที่ทุกเวลา โดยมีความสามารถเพิ่มเติมในการพิสูจน์ความถูกต้องและความสมบูรณ์ของเอกสารได้ทันทีผ่านวิทยาการเข้ารหัสลับ ทั้งนี้ เช่นเดียวกับที่การกำหนดขนาดมาตรฐานของบัตร ที่ทำให้บัตรทุกใบสามารถใส่ในกระเป๋าสตางค์ได้ กรอบความน่าเชื่อถือร่วม (Common Trust Framework) และมาตรฐานทางเทคนิคที่ใช้ร่วมกัน ก็ช่วยให้เอกสารรับรองดิจิทัล (VC) ที่ออกโดยหน่วยงานหนึ่ง สามารถจัดเก็บและใช้งานผ่านกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) และระบบต่าง ๆ บนมาตรฐานเดียวกันได้ ปัจจุบันมาตรฐานทางเทคนิคในระดับสากลสำหรับเอกสารรับรองดิจิทัล (VC) มีความสมบูรณ์และเสถียรแล้ว และเอกสารรับรองดิจิทัล (VC) ไม่ได้อยู่ในขั้นของการทดลองหรือโครงการนำร่องอีกต่อไป หากแต่กำลังก้าวขึ้นเป็นรากฐานสำคัญของ

ระบบอัตลักษณ์ดิจิทัลและการแลกเปลี่ยนข้อมูลที่น่าเชื่อถือในยุคต่อไปอย่างรวดเร็ว ด้วยเหตุนี้ เอกสารรับรองดิจิทัล (VC) จึงเป็นการเปลี่ยนแปลงที่มีนัยสำคัญสำหรับการแบ่งปันข้อมูลที่น่าเชื่อถือระหว่างภาครัฐ ประชาชน และภาคธุรกิจ แทนการใช้ฐานข้อมูลส่วนกลางของภาครัฐ โดยมุ่งเน้นไปที่การออกเอกสารรับรองดิจิทัล (VC) ที่ปลอดภัยสำหรับผู้ถือเอกสาร และสามารถแบ่งปันได้ทันทีโดยไม่ต้องผ่านระบบของภาครัฐ แนวทางการใช้เอกสารรับรองดิจิทัล (VC) ทำให้การบริการสาธารณะดิจิทัลเกิดการใช้งานได้ง่าย โดยไม่สร้างภาระที่ไม่จำเป็นต่อระบบของรัฐ อีกทั้งลดความซับซ้อนในการพัฒนาบริการดิจิทัลโดยลดความจำเป็นในการใช้ส่วนต่อประสานโปรแกรมประยุกต์ (Application Programming Interface: API) เพื่อเข้าถึงระบบของภาครัฐลงอย่างมาก

ประเทศไทยมีความคืบหน้าอย่างมากในด้านอัตลักษณ์ดิจิทัลและการวางรากฐานสำหรับเอกสารรับรองดิจิทัล (VC) โดยฐานข้อมูลของภาครัฐมีการเปลี่ยนแปลงเป็นดิจิทัล อาทิ การใช้งานแอปพลิเคชัน ThaID ทางรัฐ และเป๋าตัง พบว่าคนไทยมากกว่า 10 ล้านคนเข้าถึงบริการด้านอัตลักษณ์ดิจิทัล เพื่อการชำระเงิน และเข้าใช้แพลตฟอร์มบริการของภาครัฐ แพลตฟอร์ม National Digital ID (NDID) ใช้ระบบยืนยันตัวตนแบบรวมศูนย์ (Federated Identity Model: FIM) สำหรับภาคการเงิน ในส่วนของธนาคารแห่งประเทศไทยได้จัดโครงการ Your Data เพื่อช่วยส่งเสริมการโอนย้ายข้อมูลทางการเงินได้ตามความยินยอมของเจ้าของข้อมูลเป็นพื้นฐาน และกระทรวงสาธารณสุขได้เริ่มดำเนินการศึกษาการใช้เอกสารรับรองดิจิทัล (VC) ในบริบทด้านสุขภาพ รวมถึงการใช้งานผ่านแอปพลิเคชันหมอพร้อม นอกจากนี้ ผู้ให้บริการโทรคมนาคมได้นำ Mobile ID มาใช้ภายใต้การกำกับดูแลของคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) Mobile ID ในปัจจุบันดำเนินการโดย AIS, TRUE และบริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (National Telecom: NT) ซึ่งทั้งหมดล้วนเป็นผู้ให้บริการกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) จากภาคเอกชนในอนาคต สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ได้พัฒนาสถาปัตยกรรมและกรอบแนวทางการขับเคลื่อนเพื่อพัฒนาระบบนิเวศของการใช้เอกสารรับรองดิจิทัล (VC) สำหรับเอกสารรับรองดิจิทัล (VC) ของไทย อย่างไรก็ตาม โครงการเหล่านี้ได้รับการพัฒนาในช่วงเวลาและเพื่อวัตถุประสงค์ที่แตกต่างกัน ส่งผลให้การดำเนินงานขาดความเป็นเอกภาพและไม่เกิดการบูรณาการในรูปแบบระบบนิเวศเดียวกัน

ในระดับสากล ภาครัฐของประเทศต่าง ๆ ได้นำเอกสารรับรองดิจิทัล (VC) มาใช้งานอย่างจริงจัง เพื่อเสริมสร้างความน่าเชื่อถือทางดิจิทัลและปรับปรุงระบบอัตลักษณ์ดิจิทัลสำหรับการแบ่งปันข้อมูลที่ปลอดภัยและนำมาใช้ซ้ำได้ สหภาพยุโรป (EU) ได้นำ eIDAS 2.0 มาใช้ โดยกำหนดให้รัฐสมาชิกแต่ละรัฐต้องพัฒนา หรือได้รับใบอนุญาตสำหรับกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) อย่างน้อย 1 ใบ และบังคับให้ใช้การทำงานร่วมกันและการโอนย้ายข้อมูลได้ ภายใต้กรอบทางเทคนิคและธรรมาภิบาลร่วมกัน ประเทศ ออสเตรเลีย บราซิล แคนาดา อินเดีย เกาหลีใต้ สหราชอาณาจักร และสหรัฐอเมริกา เป็นตัวอย่างประเทศที่กำลังพัฒนาระบบนิเวศเอกสารรับรองดิจิทัล (VC) ในประเทศ ส่วนแพลตฟอร์มเทคโนโลยีรายใหญ่

อาทิ Apple และ Google ปัจจุบันสามารถรองรับเอกสารรับรองดิจิทัล (VC) โดยตรงภายในระบบปฏิบัติการสมาร์ตโฟน

ในระดับอาเซียน การบูรณาการทางดิจิทัลกำลังพัฒนาภายใต้กรอบความตกลงเศรษฐกิจดิจิทัล (DEFA) ซึ่งมุ่งหมายให้การค้าดิจิทัลสามารถเชื่อมโยงกันได้และให้บริการข้ามพรมแดนเป็นไปอย่างน่าเชื่อถือ เพื่อให้ประเทศไทยเข้าร่วมได้อย่างเต็มที่และมีความสามารถแข่งขัน เอกสารรับรองดิจิทัล (VC) จำเป็นต้องสามารถโอนย้ายได้ ตรวจสอบได้ และสอดคล้องกับมาตรฐานสากล กรณีดังกล่าวถือเป็นโอกาสเชิงยุทธศาสตร์ ประเทศไทยสามารถวางบทบาทตนเองเป็นผู้นำระดับภูมิภาคในเรื่องดังกล่าวได้ ด้วยการจัดตั้งกรอบแนวทางการสร้างความเชื่อถือแห่งชาติสำหรับเอกสารรับรองดิจิทัล (VC) อย่างเป็นทางการและชัดเจนในระยะแรก และอาจเป็นประเทศแรกในอาเซียนที่นำเอกสารรับรองดิจิทัล (VC) มาใช้จริงในระดับประเทศ โดยกำหนดมาตรฐานและมีอิทธิพลต่อการดำเนินการทั่วภูมิภาค แทนการปรับตัวให้เข้ากับกรอบที่กำหนดโดยประเทศอื่น

เอกสารรับรองดิจิทัล (VC) เปรียบเทียบกับ API เกี่ยวกับการเปลี่ยนแปลงกระบวนทัศน์ในการแบ่งปันข้อมูล

- API (ระบบสู่ระบบ) ข้อมูลจะถูกแลกเปลี่ยนโดยตรงระหว่างระบบ ผ่านการเชื่อมต่อแบบจุดต่อจุด โดยแต่ละบริการต้องสร้างและบำรุงรักษาการเชื่อมต่อกับหน่วยงานหลายแห่ง ซึ่งนำไปสู่ความซับซ้อน ซ้ำซ้อน และต้นทุนที่สูงขึ้น
- เอกสารรับรองดิจิทัล (VC) (ที่ผู้ใช้บริการเป็นผู้ควบคุม) ข้อมูลจะถูกออกในรูปแบบเอกสารรับรองดิจิทัล (VC) ที่น่าเชื่อถือและจัดเก็บในกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ของผู้ใช้บริการ (ผ่านแอปพลิเคชันหรือคลาวด์) โดยผู้ใช้บริการสามารถแบ่งปันได้อย่างปลอดภัยกับหลายบริการ ซึ่งบริการเหล่านั้นสามารถตรวจสอบความถูกต้องได้ทันที (ผ่านการเข้ารหัสลับ) โดยไม่จำเป็นต้องมีการบูรณาการระบบโดยตรง และไม่ต้องร้องขอเอกสารรับรองดิจิทัล (VC) ซ้ำ เนื่องจากสามารถนำกลับมาใช้ได้หลายครั้ง เอกสารรับรองดิจิทัล (VC) นี้ ถูกใช้งานทั่วโลกในฐานะอนาคตของบริการดิจิทัล เนื่องจากช่วยลดต้นทุนการบูรณาการ เสริมสร้างความเป็นส่วนตัว มีความมั่นคงปลอดภัย และทำให้การแลกเปลี่ยนข้อมูลข้ามภาคส่วนและข้ามพรมแดนเป็นไปอย่างราบรื่นโดยไม่ต้องพึ่งพาโครงสร้างพื้นฐานแบบรวมศูนย์

2.1 วัตถุประสงค์

ข้อเสนอแนะเชิงวิชาการฉบับนี้มีวัตถุประสงค์เพื่อนำเสนอข้อเสนอแนะเชิงนโยบายที่ชัดเจนเกี่ยวกับแนวทางและเหตุผลความจำเป็นที่ประเทศไทยควรจัดทำกรอบแนวการขับเคลื่อนเพื่อพัฒนาระบบนิเวศของการใช้เอกสารรับรองดิจิทัล (VC) **เพื่อขยายการใช้งานอัตลักษณ์ดิจิทัลและเอกสารรับรองดิจิทัล (VC) ที่ใช้งานได้ทั้งภาครัฐและภาคเอกชน**

วัตถุประสงค์ที่สำคัญ การยกระดับความน่าเชื่อถือด้านดิจิทัลของเศรษฐกิจไทยในระดับอาเซียน โดยการสนับสนุนให้ประชาชนและผู้พำนักในประเทศ แลกเปลี่ยนข้อมูลของตนได้ภายใต้เงื่อนไขของตนเองกำหนด และวางครงสร้างพื้นฐานด้านความน่าเชื่อถือทางดิจิทัลสำหรับภาคธุรกิจ เพื่อส่งเสริมการเติบโตทั้งในประเทศ ระดับภูมิภาค และระดับโลก การดำเนินการดังกล่าวหมายถึงการทำให้ภาครัฐสามารถออกเอกสารรับรองดิจิทัล (VC) ได้สะดวก ปลอดภัย และเชื่อถือได้ โดยสามารถใช้งานได้ผ่านกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับบุคคลธรรมดาหรือนิติบุคคล เพื่อรับรองการให้บริการภาครัฐอย่างเท่าเทียมแก่ประชาชน ผู้พำนัก และภาคธุรกิจ ทั้ง หากนำรากฐานด้านดิจิทัลที่มีอยู่แล้วมาบูรณาการภายใต้ระบบธรรมาภิบาล ที่มีความสอดคล้องและชัดเจน และกำหนดให้มีการเชื่อมโยงทำงานร่วมกันได้อย่างมีผลบังคับใช้ ประเทศไทยจะสามารถเสริมสร้างโครงสร้างพื้นฐานด้านความน่าเชื่อถือทางดิจิทัลแห่งชาติ ลดความเสี่ยงจากการฉ้อโกง ทำให้การแลกเปลี่ยนข้อมูลมีความสะดวกและมั่นคงปลอดภัยยิ่งขึ้น ลดต้นทุนการปฏิบัติตามกฎระเบียบ เสริมสร้างการคุ้มครองข้อมูลส่วนบุคคล ตลอดจนวางบทบาทของประเทศให้เป็นผู้นำระดับภูมิภาคในการบูรณาการดิจิทัลของอาเซียนในระยะต่อไป

3 ตัวอย่างกรณีการใช้งาน

การประยุกต์ใช้เอกสารรับรองดิจิทัล (Verifiable Credentials: VC) ในหลากหลายภาคส่วน ช่วยรองรับรูปแบบการทำธุรกรรมที่ครอบคลุมทุกมิติ ทั้งการทำธุรกรรมออนไลน์ การทำธุรกรรม ณ จุดให้บริการ การใช้งานระหว่างประเทศ ตลอดจนการพัฒนาระบบกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับประชาชนและภาคธุรกิจ โดยคุณสมบัติสำคัญของ VC ได้แก่ การเปิดเผยข้อมูลแบบเลือกได้ (Selective Disclosure) การคุ้มครองข้อมูลส่วนบุคคล การมอบอำนาจ และความสามารถในการแลกเปลี่ยนข้อมูลได้อย่างมีประสิทธิภาพ ทั้งนี้ การนำ VC มาใช้จะช่วยลดความซับซ้อนของกระบวนการบริการ ป้องกันการฉ้อโกง ยกระดับความเป็นส่วนตัวของข้อมูล และส่งเสริมการทำงานร่วมกันระหว่างหน่วยงาน อันเป็นการอำนวยความสะดวกให้เกิดการแลกเปลี่ยนข้อมูลที่เชื่อมโยงกันระหว่างภาครัฐ ภาคธุรกิจ และบริบทระหว่างประเทศได้อย่างน่าเชื่อถือและมีประสิทธิภาพสูงสุด

3.1 ความสำคัญและโอกาสในการประยุกต์ใช้เอกสารรับรองดิจิทัล (VC)เพื่อการยืนยันอัตลักษณ์พื้นฐาน

ระบบนิเวศเอกสารรับรองดิจิทัล (Verifiable Credential Ecosystem) ของประเทศไทย มีเอกสารรับรองพื้นฐานด้านอัตลักษณ์เป็นองค์ประกอบสำคัญ 2 ประเภท ได้แก่ เอกสารรับรองดิจิทัลสำหรับบัตรประจำตัวประชาชน (VC) ซึ่งออกโดยกรมการปกครอง (DOPA) และเอกสารรับรองดิจิทัลสำหรับการจดทะเบียนธุรกิจ (VC) ซึ่งออกโดยกรมพัฒนาธุรกิจการค้า (DBD) ทั้งนี้ เอกสารรับรองดิจิทัล (VC) ประเภทอื่น ๆ ภายในระบบนิเวศล้วนถูกพัฒนาขึ้นโดยอ้างอิงและเชื่อมโยงกับเอกสารรับรองพื้นฐานทั้งสองประเภทดังกล่าว

เอกสารรับรองดิจิทัลสำหรับบัตรประจำตัวประชาชน (VC) มีบทบาทสำคัญในการยืนยันอัตลักษณ์บุคคล และสามารถเปิดการเข้าถึงบริการต่าง ๆ ได้ทันที อาทิ

- การเข้าถึงบริการของกรมสรรพากรและแอปพลิเคชันภาครัฐ อาทิ ทางรัฐ หรือ หมอพร้อม
- การยื่นขอใบอนุญาตขับขี่และบริการอื่น ๆ ของกรมการขนส่งทางบก
- การเข้าถึงบริการด้านสาธารณสุข ทั้งในสถานพยาบาลและผ่านระบบออนไลน์ทางไกล
- การสมัครงานหรือการลงทะเบียนเข้าศึกษา
- การเปิดกระเป๋าเงินดิจิทัลและบัญชีการเงินอื่น ๆ

เอกสารรับรองดิจิทัลสำหรับบัตรประจำตัวประชาชน (VC) ถือเป็นกลไกสำคัญที่ประชาชนใช้ในการขอรับเอกสารรับรองดิจิทัล (VC) เพิ่มเติมจากผู้ออกเอกสารอื่น ๆ โดยกรมการปกครองเป็นหน่วยงานที่ออกเอกสารรับรองดิจิทัล (VC) สำหรับทะเบียนบ้าน สูติบัตร มรณบัตร และทะเบียนสมรสในรูปแบบเอกสารรับรองดิจิทัล (VC) เพิ่มเติม ซึ่งครอบคลุมข้อมูลข้อมูลทะเบียนราษฎร์ที่จำเป็นต่อการให้บริการภาครัฐและภาคเอกชนจำนวนมาก

เอกสารรับรองดิจิทัลสำหรับการจดทะเบียนธุรกิจ (VC) มีบทบาทในการยืนยันตัวตนตามกฎหมายของบริษัทในลักษณะเดียวกับที่เอกสารรับรองดิจิทัล (VC) สำหรับบัตรประจำตัวประชาชน และสามารถเปิดให้เข้าถึงเอกสารรับรองดิจิทัล (VC) ในหลายด้าน อาทิ

- เอกสารรับรองแสดงสถานะทางภาษีและใช้สำหรับการยื่นแบบแสดงรายการภาษี
- เอกสารรับรองใบอนุญาตประกอบกิจการและการอนุญาตตามกฎระเบียบในแต่ละสาขา
- เอกสารรับรอง ในการส่งออกและนำเข้าสินค้า
- การเข้าถึงแหล่งเงินทุนทางธุรกิจและการค้ำประกันสินเชื่อ

ทั้งนี้ บุคลากรที่ได้รับอนุญาตสามารถดำเนินการแทนบริษัทได้โดยใช้เอกสารรับรองการมอบอำนาจ (Delegation Credential) ซึ่งจัดเก็บไว้ในกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับธุรกิจ (Business Wallet) ที่ทำหน้าที่เป็นคลังเอกสารรับรองร่วมของบริษัท และสามารถบริหารจัดการสิทธิในการนำเสนอเอกสารของบุคลากรภายในองค์กรได้อย่างเป็นระบบ

3.2 การยืนยันตัวตน ณ จุดให้บริการ (NFC / Bluetooth)

- มาลีไปที่สาขาธนาคารเพื่อเปิดบัญชีใหม่
- เจ้าหน้าที่ธนาคารร้องขอหลักฐานยืนยันตัวตน
- มาลีเปิดแอปพลิเคชันกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) และทำการยืนยันตัวตนด้วยข้อมูลชีวมิติ (Biometric)
- ธนาคารส่งคำร้องขอที่ปลอดภัยผ่านระบบ Near Field Communication (NFC) หรือ Bluetooth
- มาลีให้ความยินยอมแบ่งปันเอกสารรับรองดิจิทัล (VC) สำหรับบัตรประจำตัวประชาชนของเธอ
- กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ส่งเอกสารสำแดง (Verifiable Presentation: VP) โดยตรงไปยังอุปกรณ์ของธนาคาร
- ธนาคารตรวจสอบ
    - เอกสารรับรองดิจิทัล (VC) ออกโดยกรมการปกครอง
    - เอกสารรับรองดิจิทัล (VC) ไม่ได้ถูกแก้ไขหรือถูกเพิกถอน
    - เอกสารรับรองดิจิทัล (VC) เป็นของมาลีจริง
- ธนาคารดำเนินการเปิดบัญชีสำเร็จโดยไม่ต้องถ่ายสำเนาเอกสารหรือตรวจสอบข้อมูลด้วยระบบเอกสารแบบเดิม (Manual Process)

3.3 การยืนยันอายุออนไลน์โดยคุ้มครองความเป็นส่วนตัว

- อานันท์ต้องการซื้อสินค้าที่จำกัดอายุผ่านแอปพลิเคชันอีคอมเมิร์ซ
- อานันท์เลือกสินค้าและดำเนินการชำระเงิน
- แอปพลิเคชันร้องขอหลักฐานยืนยันว่าอานันท์มีอายุเกิน 20 ปีบริบูรณ์
- อานันท์เปิดแอปพลิเคชันกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) และยืนยันตัวตนด้วยข้อมูลชีวมิติ

- ระบบกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) จะแจ้งเตือนให้อานันท์ยืนยันการแลกเปลี่ยนข้อมูลหลักฐานการยืนยันอายุ
- อานันท์ให้ความยินยอมในการแลกเปลี่ยนข้อมูลหลักฐานที่ยืนยันได้ว่าเขามีอายุเกิน 20 ปี โดยอ้างอิงจากเอกสารรับรองดิจิทัลสำหรับบัตรประจำตัวประชาชน (VC)
- การแลกเปลี่ยนข้อมูลดังกล่าวใช้วิธีการเปิดเผยข้อมูลแบบเลือกได้ (Selective Disclosure) หรือเทคนิคการคุ้มครองความเป็นส่วนตัว (เช่น Zero-Knowledge Proof) โดยไม่มีการเปิดเผยวันเดือนปีเกิดหรือข้อมูลส่วนบุคคลอื่น ๆ ของผู้ใช้งาน
- แอปพลิเคชันอีคอมเมิร์ซทำการตรวจสอบลายเซ็นเข้าดิจิทัลของหลักฐาน
- แอปพลิเคชันยืนยันว่าหลักฐานถูกต้องและดำเนินการซื้อขายเสร็จสิ้น

3.4 การเข้าถึงสินเชื่อ: เอกสารรับรองดิจิทัลสถานะทางการเงิน (VC) และการสมัครสินเชื่อ MSME

- แดงประกอบกิจการร้านอาหารขนาดเล็ก และต้องการสมัครสินเชื่อเงินทุนหมุนเวียนจากธนาคารที่เข้าร่วมโครงการของบรรษัทประกันสินเชื่ออุตสาหกรรมขนาดย่อม (บสย.)
- ธนาคารกำหนดให้ผู้ขอสินเชื่อต้องส่งหลักฐานยืนยันตัวตน ข้อมูลสถานะทางการเงิน รายงานประวัติสินเชื่อ และเอกสารการค้ำประกันสินเชื่อ
- แดงเปิดแอปพลิเคชันกระเป๋าเอกสารดิจิทัลและยืนยันตัวตนด้วยข้อมูลชีวมิติ
- แดงได้รับการร้องขอเอกสารรับรองดิจิทัล (VC) ที่เกี่ยวข้อง
- แดงให้ความยินยอมในการแลกเปลี่ยนข้อมูล ดังนี้:
    - เอกสารรับรองดิจิทัลสำหรับบัตรประจำตัวประชาชน (VC) (ออกโดยกรมการปกครอง)
    - เอกสารรับรองดิจิทัลสถานะทางการเงิน (VC) หรือ Ari Score VC ที่ออกโดยสำนักงานเศรษฐกิจการคลัง โดยระบบจะดึงข้อมูลจากเอกสารรับรองดิจิทัล (VC) ที่น่าเชื่อถือจากหลายหน่วยงาน ดังนี้
        - ข้อมูลรายได้ประจำเดือนและการยื่นแบบภาษี (กรมสรรพากร)
        - วงเงินสินเชื่อรวมและจำนวนบัญชีสินเชื่อ (สถาบันการเงิน)
        - ยอดเงินฝากเฉลี่ยย้อนหลัง 3 เดือน (ธนาคาร)
        - ข้อมูลครอบครัว/ทะเบียนบ้าน (กรมการปกครอง)
    - เอกสารรับรองรายงานเครดิต (NCB Credit Report Credential) ซึ่งออกโดยบริษัทข้อมูลเครดิตแห่งชาติ (National Credit Bureau) ครอบคลุมประวัติการขอสินเชื่อและการชำระหนี้
    - เอกสารรับรองการค้ำประกันสินเชื่อ (Loan Guarantee Credential) ซึ่งออกโดยบรรษัทประกันสินเชื่ออุตสาหกรรมขนาดย่อม (บสย.) เพื่อยืนยันสิทธิในการได้รับการค้ำประกันสินเชื่อจากภาครัฐตามวงเงินที่กำหนด

- กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ส่งเอกสารสำแดง (VP) ซึ่งรวบรวมข้อมูลเอกสารรับรองดิจิทัล (VC) ทั้ง 4 รายการเข้าด้วยกัน ให้ธนาคารตรวจสอบเอกสาร
- ธนาคารทำการตรวจสอบ:
    - เอกสารยืนยันตัวตนออกโดยหน่วยงานที่เชื่อถือได้ (กรมการปกครอง)
    - เอกสาร Ari Score VC ออกโดยสำนักงานเศรษฐกิจการคลัง และจัดทำจากข้อมูลที่เชื่อถือได้ ไม่ใช่การรายงานด้วยตนเอง
    - เอกสารรับรองดิจิทัล (VC) ของบริษัท ข้อมูลเครดิตแห่งชาติ จำกัด (NCB) ที่เป็นปัจจุบัน ถูกต้อง และออกโดยบริษัทข้อมูลเครดิตแห่งชาติ
    - เอกสารรับรองการค้ำประกันสินเชื่อจากบรรษัทประกันสินเชื่ออุตสาหกรรมขนาดย่อม (บสย.) มีผลบังคับใช้และครอบคลุมวงเงินสินเชื่อที่ร้องขอ
- ธนาคารสามารถดำเนินการประเมินสินเชื่อได้ภายในไม่กี่นาที โดยที่แดงไม่ต้องจัดเตรียมเอกสารที่เป็นกระดาษจากหลายหน่วยงานหรือกรอกแบบสอบถามทางการเงินด้วยตนเอง
- สินเชื่อได้รับการอนุมัติและโอนเงินเข้าบัญชีที่ผูกกับพร้อมเพย์ (PromptPay) ของแดงโดยตรง

3.5 สวัสดิการสังคม: การใช้สิทธิ์รับเงินชดเชยค่าน้ำมันแบบเฉพาะกลุ่มสำหรับแรงงานนอกระบบ

- รัฐบาลประกาศมาตรการช่วยเหลือเร่งด่วนเพื่อบรรเทาภาระค่าใช้จ่ายด้านน้ำมันเชื้อเพลิงแก่แรงงานนอกระบบที่ได้รับผลกระทบโดยตรงจากราคาน้ำมันที่ปรับสูงขึ้น เช่น ผู้ขับขี่รถจักรยานยนต์รับจ้าง และผู้ขับขี่รถบริการผ่านแอปพลิเคชั่น
- อาทิตย์เป็นผู้ขับขี่รถบริการผ่านแพลตฟอร์ม และต้องการสมัครเข้าร่วมมาตรการดังกล่าวผ่านระบบออนไลน์ของรัฐบาล (แอปพลิเคชัน ทางรัฐ)
- ระบบพอร์ทัลร้องขอหลักฐานยืนยันสิทธิ์ในการเข้าร่วมมาตรการ
- อาทิตย์เปิดแอปพลิเคชันกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) และทำการยืนยันด้วยข้อมูลชีวมิติ
- อาทิตย์ให้ความยินยอมในการแลกเปลี่ยนข้อมูลเอกสารรับรองดิจิทัล (VC) ดังนี้
    - เอกสารรับรองดิจิทัล (VC) สำหรับบัตรประจำตัวประชาชน (ออกโดยกรมการปกครอง)
    - เอกสารรับรองดิจิทัล (VC) สำหรับใบอนุญาตขับขี่รถจักรยานยนต์รับจ้าง (ออกโดยกรมการขนส่งทางบก) เพื่อยืนยันว่าเป็นผู้ขับขี่ที่มีการจดทะเบียนและยังคงปฏิบัติหน้าที่อยู่
    - เอกสารรับรองดิจิทัล (VC) สรุปสถานการณ์ทำงานและสรุปรายได้ (ออกโดย Grab หรือ LINE MAN) เพื่อยืนยันว่าอาทิตย์กำลังทำงานอยู่บนแพลตฟอร์มและมีรายได้เฉลี่ยต่อเดือนอยู่ในช่วงที่มีสิทธิได้รับการช่วยเหลือ
- ระบบพอร์ทัลดำเนินการตรวจสอบเอกสารรับรองดังกล่าวเพื่อยืนยันสิทธิ์ของอาทิตย์ในการเข้าร่วมมาตรการชดเชยค่าเชื้อเพลิง

- เอกสารรับรองดิจิทัล (VC) ออกโดยหน่วยงานที่น่าเชื่อถือ (กรมการปกครอง กรมการขนส่งทางบก และแพลตฟอร์มที่จดทะเบียนภายใต้การรับรองของกระทรวงแรงงาน)
- เอกสารรับรองดิจิทัล (VC) ยังมีผลบังคับใช้และไม่ถูกเพิกถอน
- เอกสารรับรองดิจิทัล (VC) เป็นของอาทิตย์โดยแท้จริง

- ระบบตรวจสอบและยืนยันว่าอาทิตย์ยังไม่เคยได้รับเงินช่วยเหลือดังกล่าวภายในรอบระยะเวลาปัจจุบัน
- เมื่อสิทธิ์ได้รับการยืนยันโดยอัตโนมัติ ระบบจะดำเนินการจ่ายเงินชดเชยเข้าบัญชี PromptPay ของอาทิตย์โดยตรง

3.6 บริการแพทย์ทางไกลและใบสั่งยาดิจิทัล

- นรินทร์นัดหมายขอรับคำปรึกษาออนไลน์ผ่านแพลตฟอร์มบริการแพทย์ทางไกล (Telemedicine)
- ระบบต้องดำเนินการยืนยันตัวตนทั้งในส่วนของนรินทร์และบุคลากรทางการแพทย์
- นรินทร์เปิดใช้งานแอปพลิเคชันกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) และดำเนินการยืนยันตัวตนเข้าสู่ระบบ
- นรินทร์ยินยอมให้ส่งข้อมูลดังนี้:
  - เอกสารรับรองดิจิทัล (VC) สำหรับบัตรประจำตัวประชาชน
  - เอกสารรับรองดิจิทัล (VC) สำหรับประกันสุขภาพหรือสิทธิการรักษาพยาบาล
- แพลตฟอร์มตรวจสอบตัวตนและยืนยันสิทธิของนรินทร์
- ระบบจะดำเนินการส่งข้อมูลเอกสารรับรองดิจิทัล (VC) ของแพทย์ให้แก่นรินทร์ ได้แก่
  - เอกสารรับรองดิจิทัล (VC) สำหรับใบอนุญาตประกอบวิชาชีพเวชกรรมของบุคลากรทางการแพทย์
  - สังกัดโรงพยาบาลหรือสถาบัน
- นรินทร์ดำเนินการตรวจสอบความถูกต้องของใบอนุญาตประกอบวิชาชีพและสิทธิ์ในการให้บริการของแพทย์
- หลังการปรึกษา แพทย์ออกใบสั่งยาดิจิทัลในรูปแบบเอกสารรับรองดิจิทัล (VC)
- ใบสั่งยาถูกจัดเก็บอย่างปลอดภัยในแอปพลิเคชันกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ของนรินทร์
- นรินทร์สามารถนำใบสั่งยาไปแสดงที่ร้านขายยาในภายหลังได้
- ร้านขายยาตรวจสอบความถูกต้องและความสมบูรณ์ของใบสั่งยาก่อนจ่ายยา

3.7 การยื่นเอกสารรับรองดิจิทัล (VC) เพื่อการค้าในภูมิภาคอาเซียน (กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับ นิติบุคคล)

- บริษัท เจริญเอ็กซ์พอร์ต จำกัดมีความประสงค์ที่จะส่งออกสินค้าไปยังประเทศอื่นในภูมิภาคอาเซียน
- หน่วยงานศุลกากรของประเทศปลายทางกำหนดให้ต้องแสดงหลักฐานการจดทะเบียนธุรกิจ ใบอนุญาตส่งออก และใบรับรองผลิตภัณฑ์
- บุคลากรของบริษัทที่ได้รับมอบอำนาจเปิดแอปพลิเคชันกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ของบริษัท (กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับธุรกิจ) และดำเนินการยืนยันตัวตนเข้าสู่ระบบ
- บุคลากรของบริษัทดำเนินการภายใต้เอกสารรับรองดิจิทัล (VC) ที่ได้รับมอบอำนาจและตรวจสอบยืนยันสิทธิ์ได้ว่าเป็นตัวแทนบริษัทจริง
- บริษัทให้ความยินยอมในการแลกเปลี่ยนข้อมูลเอกสารรับรองดิจิทัล (VC) ดังนี้:
    - เอกสารรับรองดิจิทัล (VC) การจดทะเบียนนิติบุคคล/ธุรกิจ
    - เอกสารรับรองดิจิทัล (VC) ใบอนุญาตส่งออก
    - หนังสือรับรองแหล่งกำเนิดสินค้า
- ข้อมูลดังกล่าวจะถูกส่งต่อในรูปแบบเอกสารรับรองดิจิทัล (VC) ไปยังหน่วยงานศุลกากรต่างประเทศ
- หน่วยงานศุลกากรดำเนินการตรวจสอบความถูกต้อง
    - ความถูกต้องของเอกสารรับรองดิจิทัล (VC) และตรวจสอบลายมือชื่อดิจิทัล
    - เอกสารรับรองดิจิทัล (VC) ออกโดยหน่วยงานผู้ออกเอกสาร
    - บุคลากรของบริษัทแสดงเอกสารดิจิทัล (VC) ที่ได้รับมอบอำนาจ
- การขนส่งสินค้าจึงสามารถผ่านพิธีการศุลกากรได้โดยไม่ต้องจัดเตรียมเอกสารกระดาษหรือตรวจสอบข้อมูลด้วยระบบเอกสารแบบเดิม (Manual Process)

3.8 การตรวจสอบเอกสารรับรองดิจิทัล (VC) ทางการศึกษาและวิชาชีพ

- สุดายื่นสมัครงานในตำแหน่งที่กำหนดให้แสดงหลักฐานวุฒิการศึกษาและใบรับรองวิชาชีพ
- นายจ้างดำเนินการขอตรวจสอบคุณวุฒิของสุดา
- สุดาเปิดแอปพลิเคชันกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) และดำเนินการยืนยันตัวตนเข้าสู่ระบบ
- สุดาได้รับการร้องขอเอกสารรับรองดิจิทัล (VC) ที่เกี่ยวข้อง
- สุดาให้ความยินยอมในการแลกเปลี่ยนข้อมูลเอกสารรับรองดิจิทัล (VC) ดังนี้:
    - เอกสารรับรองดิจิทัล (VC) ปริญญาจากมหาวิทยาลัย
    - เอกสารรับรองดิจิทัล (VC) ใบอนุญาตประกอบวิชาชีพ

- กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สร้างเอกสารสำแดง (VP)
- มีการเปิดเผยเฉพาะข้อมูลที่จำเป็นเท่านั้น (เช่น วุฒิการศึกษา สถาบันผู้ออกเอกสาร และสถานะความมีผลของเอกสาร)
- นายจ้างดำเนินการตรวจสอบความถูกต้อง ดังนี้
    - เอกสารรับรองดิจิทัล (VC) ออกโดยสถาบันที่น่าเชื่อถือ (อาทิ มหาวิทยาลัย หน่วยงานกำกับดูแล)
    - เอกสารรับรองดิจิทัล (VC) สถานะยังมีผลและไม่ถูกเพิกถอน
    - เอกสารรับรองดิจิทัล (VC) เป็นของสุดาโดยแท้จริง
- นายจ้างสามารถตรวจสอบความถูกต้องของเอกสารได้ทันทีโดยไม่ต้องติดต่อสถาบันผู้ออกเอกสารโดยตรง

3.9 การเช่ารถในต่างประเทศด้วยใบอนุญาตขับขี่ดิจิทัล

- กิตติพงศ์เดินทางไปท่องเที่ยว ณ ประเทศญี่ปุ่น
- กิตติพงศ์มีความประสงค์เช่ารถยนต์และจำเป็นต้องแสดงใบอนุญาตขับขี่ที่ยังมีผลบังคับใช้
- ณ จุดให้บริการเช่ารถยนต์บริษัทผู้ให้บริการขอดำเนินการตรวจสอบหลักฐานยืนยันสิทธิ์ในการขับขี่
- กิตติพงศ์เปิดแอปพลิเคชันกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) และทำการยืนยันตัวตนด้วยข้อมูลชีวมิติ
- บริษัทเช่ารถส่งคำร้องขอเอกสารรับรองดิจิทัลใบอนุญาตขับขี่ (VC)
- กิตติพงศ์ให้ความยินยอมในการแลกเปลี่ยนข้อมูลใบอนุญาตขับขี่ดิจิทัลของเขาในรูปแบบเอกสารรับรองดิจิทัล (VC)
- กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สร้างเอกสารสำแดง (VP) โดยเปิดเผยเฉพาะข้อมูลที่จำเป็นเท่านั้นอาทิ สถานะของใบอนุญาตขับขี่ ประเภทรถที่ได้รับอนุญาตในการขับขี่
- บริษัทเช่ารถดำเนินการตรวจสอบความถูกต้อง ดังนี้:
    - ใบอนุญาตออกโดยหน่วยงานที่น่าเชื่อถือ (อาทิ กรมการขนส่งทางบก)
    - เอกสารรับรองดิจิทัล (VC) ยังมีผลบังคับใช้และไม่ถูกเพิกถอน
    - เอกสารรับรองดิจิทัล (VC) เป็นของกิตติพงศ์โดยแท้จริง
- การเช่าได้รับการอนุมัติทันทีโดยไม่ต้องใช้เอกสารจริงหรือกระบวนการตรวจสอบด้วยวิธีปกติ

3.10 บัตรขาเข้าดิจิทัล (ใบตม.6) และการเช็คอินเข้าพักโรงแรม

- มาเรียเดินทางมาถึงประเทศไทย และดำเนินการกรอกข้อมูลบัตรขาเข้าดิจิทัล(ใบตม.6)ก่อนเครื่องบินลงจอด
- ข้อมูลการเดินทางเข้าประเทศถูกออกเป็นเอกสารรับรองดิจิทัล (VC) และจัดเก็บไว้ในแอปพลิเคชันกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ของมาเรีย

- เมื่อเดินทางมาถึงประเทศไทย เจ้าหน้าที่ตรวจคนเข้าเมืองทำการตรวจสอบเอกสารรับรองดิจิทัล (VC) การเดินทางเข้าเมืองในรูปแบบดิจิทัล
- หลังจากนั้น นักท่องเที่ยวเดินทางไปยังโรงแรม
- ระหว่างการเช็คอินที่โรงแรม พนักงานต้อนรับดำเนินการตรวจสอบข้อมูล ดังนี้:
    - หลักฐานการยืนยันตัวตน (เช่น Passport)
    - สถานะการเดินทางเข้าประเทศหรือข้อมูลการตรวจคนเข้าเมือง
- มาเรียเปิดแอปพลิเคชันกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) และดำเนินการยืนยันตัวตนด้วยข้อมูลชีวมิติ
- เธอให้ความยินยอมในการแบ่งปัน:
    - เอกสารรับรองดิจิทัล (VC) หนังสือเดินทางหรือเอกสารยืนยันตัวตน
    - เอกสารรับรองดิจิทัล (VC) บัตรขาเข้าดิจิทัล
- กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สร้างเอกสารสำแดง (VP) โดยแบ่งปันเฉพาะข้อมูลที่จำเป็นเท่านั้น
- โรงแรมดำเนินการตรวจสอบความถูกต้อง ดังนี้:
    - ความถูกต้องของเอกสารรับรองดิจิทัล (VC) ที่ออกโดยหน่วยงานตรวจคนเข้าเมือง
    - สถานะการอนุญาตให้เข้าเมือง
    - ข้อมูลการยืนยันตัวตนตรงกับการจอง
- การเช็คอินเข้าที่พักเสร็จสิ้นทันทีโดยไม่ต้องถ่ายสำเนาหนังสือเดินทางหรือกรอกแบบฟอร์มด้วยวิธีปกติ

3.11 การยืนยันตัวตนผู้ขายออนไลน์เพื่อป้องกันการฉ้อโกงบนแพลตฟอร์มดิจิทัล

- พลอยมีความประสงค์สั่งซื้อสินค้าผ่านแพลตฟอร์มพาณิชย์ดิจิทัล แต่มีความกังวลเกี่ยวกับความเสี่ยงจากการฉ้อโกงและผู้ขายที่ไม่น่าเชื่อถือ
- แพลตฟอร์มดิจิทัลกำหนดให้ผู้ขายต้องแสดงเอกสารรับรองดิจิทัล (VC) เพื่อยืนยันสถานะทางธุรกิจ
- ผู้ขายดำเนินการส่งเอกสารรับรองดิจิทัล (VC) เพื่อยืนยันข้อมูล ดังนี้:
    - เอกสารรับรองการจดทะเบียนธุรกิจ
    - เอกสารยืนยันตัวตน

- พลอยสามารถตรวจสอบสัญลักษณ์ ผู้ขายที่ผ่านการรับรอง" (Verified Seller) ซึ่งได้รับการยืนยันความถูกต้องด้วยเทคโนโลยีการเข้ารหัส (ไม่ใช่เพียงการรับรองโดยแพลตฟอร์มเท่านั้น)
- เมื่อพลอยดำเนินการสั่งซื้อสินค้า
    - แพลตฟอร์มจะดำเนินการตรวจสอบความถูกต้องของเอกสารรับรองดิจิทัล (VC) ของผู้ขายแบบเรียลไทม์
    - ระบบยืนยันความน่าเชื่อถือของผู้ออกเอกสารว่าเป็นหน่วยงานภาครัฐที่มีอำนาจในการออกเอกสารดังกล่าว (เช่น กรมพัฒนาธุรกิจการค้า)
- พลอยสามารถทำธุรกรรมได้อย่างมั่นใจ เนื่องจากระบบสามารถยืนยันสถานะความเป็นผู้ประกอบการที่ถูกต้องตามกฎหมายของผู้ขายได้โดยสมบูรณ์

4 ผลสัมฤทธิ์เชิงประจักษ์

จากผลการดำเนินงานในต่างประเทศแสดงให้เห็นว่าการนำกระเป๋าเอกสารอัตลักษณ์ดิจิทัลและเอกสารรับรองดิจิทัล (VC) มาใช้ ก่อให้เกิดประโยชน์เชิงยุทธศาสตร์ทั้งในมิติเศรษฐกิจ การบริหารจัดการ และความมั่นคงปลอดภัยอย่างมีนัยสำคัญ จากการประเมินผลกระทบและการนำไปปฏิบัติจริงในหลายประเทศแสดงให้เห็นอย่างชัดเจนว่า การดำเนินการดังกล่าวจะช่วยลดต้นทุนการลงทะเบียนผู้ใช้บริการ เพิ่มประสิทธิภาพการให้บริการ และลดความสูญเสียจากการถูกฉ้อโกง ประโยชน์ดังกล่าวเป็นผลจากการปรับเปลี่ยนโครงสร้างพื้นฐานดิจิทัล จากเดิมที่ต้องตรวจสอบเอกสารซ้ำซ้อน ไปสู่การใช้ข้อมูลที่สามารถตรวจสอบความถูกต้องได้ด้วยเทคโนโลยีการเข้ารหัส ซึ่งช่วยให้สามารถนำข้อมูลกลับมาใช้ใหม่ได้อย่างปลอดภัยและมีประสิทธิภาพ

4.1 การลดภาระต้นทุนการลงทะเบียนและการปฏิบัติตามกฎระเบียบ

เอกสารรับรองดิจิทัล (VC) มีบทบาทสำคัญในการลดต้นทุน ลดความซับซ้อนในการยืนยันตัวตน และเพิ่มประสิทธิภาพในการลงทะเบียนผู้ใช้บริการได้อย่างมีนัยสำคัญ โดยสามารถออกเอกสารครั้งเดียวและนำกลับมาใช้ซ้ำได้ในหลายธุรกรรม ทั้งนี้ ผลการประเมินผลกระทบของคณะกรรมาธิการยุโรปสำหรับกรอบอัตลักษณ์ดิจิทัลของสหภาพยุโรป (eIDAS 2.0) พบว่า กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ทำให้ผู้ให้บริการลดต้นทุนในการระบุตัวตน และการลงทะเบียนผู้ใช้บริการในภาคการเงิน ประมาณ 0.68–1.36 พันล้านยูโร และในด้านสุขภาพดิจิทัล ประมาณ 1.26–2.51 พันล้านยูโร นอกจากนี้ ยังก่อให้เกิดการประหยัดต้นทุนเพิ่มเติมในพาณิชย์อิเล็กทรอนิกส์และการบิน[1]

หลักฐานเชิงประจักษ์สนับสนุนข้อค้นพบดังกล่าว กรณีศึกษาจากโครงการนำร่องของรัฐบาลรัฐควีนส์แลนด์ที่ใช้เอกสารรับรองดิจิทัล (VC) ในกระบวนการรับพนักงานใหม่สามารถลดระยะเวลาจากประมาณ 3 วัน เหลือ 30 นาที โดยลดขั้นตอนที่ซ้ำซ้อนในการยืนยันตัวตน การตรวจสอบคุณวุฒิ และการตรวจสอบประวัติ [2] ทั้งนี้ การปรับปรุงประเภทนี้มีความเกี่ยวข้องโดยตรงกับกระบวนการที่มีอุปสรรคและความซับซ้อนสูง อาทิ กระบวนการรู้จักลูกค้า (Know Your Customer: KYC), กระบวนการรู้จักธุรกิจ (Know Your Business: KYB) การออกใบอนุญาต และการเข้าถึงแหล่งเงินทุน

4.2 การลดการฉ้อโกงและการเสริมสร้างยกระดับความมั่นคงปลอดภัย

การเปลี่ยนผ่านจากการใช้เอกสารและภาพหน้าจอทั่วไป มาเป็นการใช้เอกสารรับรองดิจิทัล (VC) ที่ลงนามด้วยการเข้ารหัสลับ จะช่วยลดความเสี่ยงจากการถูกฉ้อโกง การปลอมแปลง และการแอบอ้างตัวตนได้อย่างมีนัยสำคัญ ทั้งนี้ คณะกรรมาธิการยุโรปประเมินว่า การนำกระเป๋าเอกสารอัตลักษณ์ดิจิทัล (Digital Identity Wallet) มาใช้ จะช่วยลดความสูญเสียจากการฉ้อโกงในภาคการเงินได้ประมาณ 0.85–1.4 พันล้านยูโรต่อปี และในภาคสุขภาพดิจิทัลประมาณ 0.3–0.6 พันล้านยูโร[3]

---

[1] European Commission (2021), *Impact Assessment Report accompanying the proposal for a European Digital Identity framework* (eIDAS 2.0).

[2] Meeco et al. (Queensland Government pilot), *Workplace Credentials Case Study*.

[3] European Commission (2021).

ประโยชน์ดังกล่าวมีความสำคัญอย่างยิ่งในสถานการณ์ปัจจุบันที่การฉ้อโกงทางดิจิทัลมีแนวโน้มทวีความรุนแรงและซับซ้อนยิ่งขึ้น โดยเอกสารรับรองดิจิทัล (VC) จะช่วยยกระดับความน่าเชื่อถือจากเดิมที่พึ่งพาเอกสารกระดาษดั้งเดิม ซึ่งมีความเปราะบางและเสี่ยงต่อการถูกปลอมแปลง ไปสู่การตรวจสอบความถูกต้องด้วยเทคโนโลยีการเข้ารหัส ซึ่งสามารถยืนยันข้อมูลได้อย่างรวดเร็ว แม่นยำ และมีความน่าเชื่อถือสูง

4.3 ประสิทธิภาพการบริหารและการเพิ่มผลผลิต

เอกสารรับรองดิจิทัล (VC) ช่วยลดภาระงานด้านการบริหารจัดการสำหรับผู้ใช้บริการและผู้ให้บริการ โดยการตัดกระบวนการที่ซ้ำซ้อนออก ทั้งนี้ คณะกรรมาธิการยุโรปประเมินว่า การนำระบบดังกล่าวมาใช้จะช่วยลดภาระงานด้านการบริหารของประชาชนที่ประมาณ 350–400 ล้านยูโรต่อปี[4]

ในส่วนของภาครัฐ ระบบ Digital Staff Passport ของสำนักงานบริการสุขภาพแห่งชาติ สหราชอาณาจักร (NHS) ได้แสดงให้เห็นถึงผลลัพธ์ที่ใกล้เคียงกัน โดยการเปิดโอกาสให้บุคลากรทางการแพทย์สามารถนำเอกสารรับรองดิจิทัล (VC) ที่ผ่านการตรวจสอบแล้วมาใช้ซ้ำได้ในหลายสถาบัน สามารถประหยัดเวลาการทำงานได้ถึง 100,000 วันต่อปี โดยการตัดขั้นตอนการตรวจสอบซ้ำในการเริ่มงานและการฝึกอบรม [5] ทั้งนี้ กรณีดังกล่าวแสดงให้เห็นถึงศักยภาพของรูปแบบการให้บริการภาครัฐแบบ "แจ้งข้อมูลครั้งเดียว" (Tell Us Once) ซึ่งช่วยลดความซ้ำซ้อนและเพิ่มความรวดเร็วในการให้บริการได้อย่างมีประสิทธิภาพ

4.4 ผลกระทบระดับเศรษฐกิจและประโยชน์ต่อภาคธุรกิจ

การนำเอกสารรับรองดิจิทัล (VC) มาประยุกต์ใช้โดยเฉพาะผ่านระบบกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับธุรกิจ (Business Wallet) จะก่อให้เกิดผลกระทบเชิงบวกอย่างมีนัยสำคัญ โดยผลการประเมินของคณะกรรมาธิการยุโรปคาดการณ์ว่าประโยชน์สุทธิต่อปีจากการใช้กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับธุรกิจอยู่ที่ประมาณ 46.9 พันล้านยูโรที่อัตราการนำไปใช้ร้อยละ 33 และเพิ่มสูงขึ้นเป็น 116.0 พันล้านยูโรที่อัตราการนำไปใช้ร้อยละ 75 ภายในปีแรกของการดำเนินงาน [6] ทั้งนี้ ธุรกิจขนาดกลางและขนาดย่อม (Small and Medium Enterprises: SME) จะได้รับประโยชน์สูงสุด โดยมีการประมาณการต้นทุนการดำเนินการเพียงร้อยละ 12–24 ของผลประโยชน์ทางตรง

ผลลัพธ์เหล่านี้สะท้อนถึงต้นทุนธุรกรรมที่ลดลง การเข้าถึงบริการที่รวดเร็วขึ้น และการเพิ่มประสิทธิภาพในการโอนย้ายข้อมูล โดยเฉพาะในด้านการเข้าถึงแหล่งเงินทุน การปฏิบัติตามข้อกำหนดทางกฎหมาย และการดำเนินการค้าข้ามพรมแดน

[4] ibid.
[5] NHS England, *Digital Staff Passport / Enabling Staff Movement Programme*.
[6] European Commission (2025), *Impact Assessment accompanying the proposal on European Business Wallets*.

4.5 ผลกระทบต่อประเทศไทย

การนำเอกสารรับรองดิจิทัล (VC) มาประยุกต์ใช้ จะช่วยลดต้นทุน ยกระดับความมั่นคงปลอดภัย และเพิ่มประสิทธิภาพการดำเนินงานทั้งในภาครัฐและภาคเอกชน โดยผลลัพธ์ที่จะเกิดขึ้นนั้นขึ้นอยู่กับรูปแบบและระดับความพร้อมในการนำไปปฏิบัติจริง ทั้งนี้ ด้วยรากฐานทางดิจิทัลที่แข็งแกร่งและอัตราการเข้าถึงบริการดิจิทัลที่สูงของประเทศไทย จึงมีความเป็นไปได้สูงที่จะเกิดผลลัพธ์เชิงบวกในทิศทางเดียวกันกับที่ปรากฏในระดับสากล

จากการประมาณการเบื้องต้นโดยเปรียบเทียบกับข้อมูลข้างต้น คาดการณ์ว่าการนำระบบดังกล่าวมาใช้ลดต้นทุนการลงทะเบียนผู้ใช้บริการ การยืนยันตัวตน และภาระงานด้านการบริหารจัดการ คิดเป็นมูลค่ารวมหลายหมื่นล้านบาทต่อปี โดยเฉพาะอย่างยิ่งในภาคการเงิน ภาคสาธารณสุข และการให้บริการภาครัฐ

นอกจากนี้ เมื่อพิจารณาจากมูลค่าความสูญเสียจากการฉ้อโกงออนไลน์ในปัจจุบันที่สูงถึง 45,000 ล้านบาทต่อปี การนำเอกสารรับรองดิจิทัล (VC) มาใช้แม้เพียงบางส่วน จะช่วยลดความสูญเสียดังกล่าวได้หลายพันล้านบาทต่อปี

จากผลการวิเคราะห์ข้างต้น ชี้ให้เห็นว่าผลประโยชน์ทางเศรษฐกิจที่จะได้รับจากเอกสารรับรองดิจิทัล (VC) มาใช้ มีแนวโน้มสูงกว่างบประมาณการลงทุนภาครัฐอย่างมีนัยสำคัญ โดยเฉพาะเมื่อพิจารณาถึงผลประโยชน์ในภาพรวม ทั้งการเพิ่มผลผลิต การยกระดับคุณภาพการให้บริการ และการเสริมสร้างความเชื่อมั่นต่อระบบเศรษฐกิจดิจิทัลของประเทศ

5 ข้อเสนอแนะเชิงนโยบาย

ข้อเสนอแนะสำคัญ 5 ประการต่อไปนี้ เป็นแนวทางการดำเนินงานที่มีความจำเป็นต่อการบรรลุวัตถุประสงค์ในการยกระดับความน่าเชื่อถือด้านดิจิทัลของเศรษฐกิจไทยในระดับอาเซียน โดยมุ่งเสริมสร้างศักยภาพให้ประชาชนและผู้พำนักในประเทศไทยสามารถแลกเปลี่ยนข้อมูลของตนเองได้ภายใต้เงื่อนไขที่กำหนดอย่างปลอดภัย โปร่งใส และน่าเชื่อถือ ตลอดจนวางรากฐานโครงสร้างพื้นฐานด้านความน่าเชื่อถือทางดิจิทัลให้แก่ภาคธุรกิจ เพื่อสนับสนุนการเติบโตทางเศรษฐกิจทั้งในระดับประเทศ ระดับภูมิภาค และระดับโลก

5.1 การจัดตั้งกรอบแนวทางการสร้างความเชื่อถือแห่งชาติสำหรับเอกสารรับรองดิจิทัล (VC) อย่างเป็นทางการ

บริบท: ที่ผ่านมาประเทศไทยได้มีการพัฒนาขีดความสามารถด้านเทคโนโลยี ตลอดจนการออกแบบและพัฒนากลไกเชิงสถาบันที่เกี่ยวข้องกับสถาปัตยกรรมด้านอัตลักษณ์ดิจิทัลและเอกสารรับรองดิจิทัล (VC) มาอย่างต่อเนื่อง ซึ่งเป็นพื้นฐานสำคัญในการยกระดับโครงสร้างพื้นฐานด้านความเชื่อมั่นดิจิทัลของประเทศให้มีความเข้มแข็งมากยิ่งขึ้น อย่างไรก็ดี หากขีดความสามารถดังกล่าวยังคงดำเนินการภายใต้การกำกับดูแลที่แยกส่วน และขับเคลื่อนด้วยการนำไปใช้โดยความสมัครใจเป็นหลัก อาจไม่เพียงพอต่อการรองรับการขยายการใช้งานในวงกว้าง โดยเฉพาะเมื่อมีการนำไปใช้เพิ่มมากขึ้น การทำงานร่วมกันระหว่างระบบ การโอนย้ายข้อมูล และการยอมรับเอกสารรับรองดิจิทัล (VC) ข้ามหน่วยงานหรือข้ามบริการ ย่อมไม่สามารถเกิดขึ้นได้อย่างสมบูรณ์หากปราศจากหลักเกณฑ์และมาตรฐานที่มีผลบังคับใช้อย่างชัดเจน ดังนั้นการปฏิรูปในระยะต่อไปจึงควรมุ่งเน้นการจัดให้มีฐานอำนาจทางกฎหมาย มาตรฐานที่มีผลบังคับใช้ และกลไกการกำกับดูแลที่มีการประสานงานกันอย่างเป็นระบบ เพื่อให้การพัฒนาและการใช้งานอัตลักษณ์ดิจิทัลและเอกสารรับรองดิจิทัล (VC) ของประเทศไทยสามารถดำเนินไปในทิศทางเดียวกัน มีความมั่นคงปลอดภัย เชื่อมโยงและทำงานร่วมกันได้อย่างมีประสิทธิภาพ ตลอดจนสามารถขยายการใช้งานได้ในระดับประเทศอย่างเป็นรูปธรรม

แนวทางดำเนินการ: รัฐบาลควรจัดทำกรอบแนวทางการสร้างความเชื่อถือแห่งชาติสำหรับเอกสารรับรองดิจิทัล (VC) อย่างเป็นทางการ ผ่านมติคณะรัฐมนตรี โดยกำหนดให้เกิดการมีส่วนร่วมจากหลายกระทรวง ในการนี้ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) เป็นหน่วยงานที่เหมาะสมที่สุดในการบริหารและกำกับดูแลกรอบดังกล่าว รวมถึงการตรวจรับรองตามมาตรฐานที่กำหนดให้แก่หน่วยงานที่เข้าร่วม อาทิ ผู้ออกเอกสารรับรองดิจิทัล (Issuer)[7] กระเป๋าเอกสารดิจิทัล (Digital Document Wallet)[8] และผู้ตรวจสอบ (Verifier)[9] ซึ่งในอนาคต บทบาทของ สพธอ. ตามกรอบดังกล่าว อาจถูกบัญญัติไว้ในกฎหมายโดยการปรับปรุงพระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งใช้แนวทางตามกฎหมายแม่แบบของคณะกรรมาธิการสหประชาชาติว่าด้วยกฎหมายการค้าระหว่างประเทศ (UNCITRAL) ว่าด้วยการใช้และการยอมรับข้ามพรมแดน

[7] ผู้ออกเอกสาร (Issuer) คือหน่วยงานภาครัฐหรือองค์กรที่ได้รับอนุญาตซึ่งออกเอกสารรับรองดิจิทัล (VC) ดิจิทัลที่ลงนามด้วยการเข้ารหัสลับให้แก่ประชาชนหรือภาคธุรกิจ ตัวอย่างเช่น กรมการปกครองออกเอกสารรับรองดิจิทัล (VC) บัตรประชาชน หรือกรมพัฒนาธุรกิจการค้าออกเอกสารรับรองดิจิทัล (VC) การจดทะเบียนนิติบุคคล

[8] กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) คือแอปพลิเคชันดิจิทัลที่ได้รับการรับรองซึ่งประชาชนและภาคธุรกิจใช้ในการจัดเก็บ บริหารจัดการ และนำเสนอเอกสารรับรองดิจิทัล (VC) ของตน ตัวอย่างเช่น ThaID หรือทางรัฐ

[9] ผู้ตรวจสอบเอกสาร (Verifier) คือบริการของภาครัฐหรือภาคเอกชนที่ร้องขอและตรวจสอบเอกสารรับรองดิจิทัล (VC) ที่ประชาชนหรือภาคธุรกิจนำเสนอด้วยการเข้ารหัสลับ ตัวอย่างเช่น ธนาคารตรวจสอบอัตลักษณ์ของลูกค้า หรือหน่วยงานภาครัฐตรวจสอบใบอนุญาตประกอบธุรกิจ

ของการจัดการอัตลักษณ์ดิจิทัลและบริการความน่าเชื่อถือ[10] เป็นกรอบอ้างอิงในการพัฒนากฎหมายและมาตรฐานที่เกี่ยวข้องให้สอดคล้องกับแนวปฏิบัติสากล

กรอบแนวทางการขับเคลื่อนฯ ควรประกอบด้วย:

- การกำหนดบทบาทและความรับผิดชอบของหน่วยงานที่เกี่ยวข้องในด้านนโยบาย การกำกับดูแล การตรวจรับรองและการสนับสนุนเพื่อขับเคลื่อนตามนโยบาย
- การกำหนดแผนการทำงานร่วมกันที่สอดคล้องกับนโยบายระดับประเทศของทุกหน่วยงาน
- การจัดทำข้อกำหนดและมาตรฐานที่เกี่ยวข้องในการรับรองกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) และระบบอื่น ๆ
- การจัดทำข้อกำหนดให้มีการเชื่อมโยงการทำงานของระบบที่เกี่ยวข้องร่วมกัน รวมถึงการโอนย้ายข้อมูลได้ในระบบที่ได้รับการรับรอง
- การกำหนดระดับความน่าเชื่อถือสำหรับการออกเอกสารรับรองดิจิทัล (VC)
- การมอบหมายให้มีการกำกับดูแลด้านนโยบายและการขับเคลื่อนผ่านคณะกรรมการเฉพาะกิจภายใต้คณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ
- กำหนดบทบาท หน้าที่ และความรับผิดชอบ การชดเชยค่าเสียหาย และกระบวนการระงับข้อพิพาทของหน่วยงาน ผู้ให้บริการ และผู้ใช้บริการที่เกี่ยวข้อง

5.2 พัฒนาและกำกับดูแลระบบนิเวศของกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ตามมาตรฐานและข้อกำหนดที่เกี่ยวข้อง

บริบท: ประเทศไทยประสบความสำเร็จในการนำระบบอัตลักษณ์ดิจิทัล ระบบการชำระเงินดิจิทัล และแอปพลิเคชันบริการดิจิทัลมาใช้งานในวงกว้าง ซึ่งสะท้อนให้เห็นถึงศักยภาพด้านนวัตกรรมของประเทศ ตลอดจนความเชื่อมั่นของประชาชนและผู้ใช้บริการต่อโครงสร้างพื้นฐานดิจิทัลที่มีอยู่ อย่างไรก็ดีการมีฟังก์ชันด้านอัตลักษณ์ดิจิทัลของประชาชนและกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ที่ซ้อนทับกันในหลายแอปพลิเคชัน โดยเฉพาะแอปพลิเคชันที่ได้รับการสนับสนุนโดยภาครัฐ อาจเพิ่มความซับซ้อนต่อการบูรณาการระบบในภาพรวม และก่อให้เกิดความเสี่ยงต่อการลงทุนของภาครัฐที่ซ้ำซ้อน หากไม่มีการกำหนดหลักเกณฑ์ด้านการทำงานร่วมกันและการโอนย้ายข้อมูลที่ชัดเจน เอกสารรับรองดิจิทัล (VC) อาจถูกจำกัดการใช้งานอยู่ภายในระบบนิเวศแบบปิด ส่งผลให้ไม่สามารถขยายการใช้ประโยชน์ในระดับประเทศได้อย่างเต็มประสิทธิภาพ ปัจจุบันประเทศไทยยังไม่มีกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับภาคธุรกิจหรือนิติบุคคลที่ทำหน้าที่เป็นทั้งอัตลักษณ์ดิจิทัลขององค์กร และเป็นช่องทางในการจัดเก็บเอกสารรับรองดิจิทัล (VC) ที่สำคัญ เช่น ใบอนุญาตประกอบธุรกิจ หนังสือรับรอง หรือเอกสารสิทธิและคุณสมบัติอื่นที่เกี่ยวข้อง ซึ่งถือเป็นช่องว่างสำคัญต่อการพัฒนาโครงสร้างพื้นฐานด้านความเชื่อมั่นดิจิทัลสำหรับภาคธุรกิจในระยะต่อไป

[10] UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services (MLIT). See: https://uncitral.un.org/en/mlit.

แนวทางการดำเนินงาน: หน่วยงานกำกับดูแลควรจัดระบบการรับรองมาตรฐานกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) โดยแบ่งเป็น 2 ประเภท ได้แก่ (1) สำหรับบุคคลธรรมดา และ (2) สำหรับนิติบุคคล เพื่อประสิทธิภาพในการลงทุนภาครัฐ กำหนดให้มีผู้ให้บริการกระเป๋าเอกสารดิจิทัลที่เป็นหน่วยงานของรัฐ มีไม่เกินประเภทละ 2 ราย ทั้งนี้ กระเป๋าดังกล่าวต้องรองรับการเชื่อมโยงข้อมูล การทำงานร่วมกัน (Interoperability) และการโอนย้ายข้อมูลระหว่างระบบได้อย่างปลอดภัยและมีประสิทธิภาพ

สำหรับผู้ให้บริการภาคเอกชนรายอื่น ๆ สามารถขอรับการรับรองเพื่อให้บริการในระบบนิเวศได้โดยไม่จำกัดจำนวน เพื่อส่งเสริมนวัตกรรมและการแข่งขันอย่างเสรี ทั้งนี้ ฟังก์ชันการทำงานของกระเป๋าเอกสารดิจิทัลอาจบูรณาการเป็นส่วนหนึ่งของแอปพลิเคชันบนโทรศัพท์เคลื่อนที่ที่ได้รับความนิยมอยู่เดิมได้ โดยไม่จำเป็นต้องพัฒนาแอปพลิเคชันขึ้นใหม่เป็นการเฉพาะ

ระบบการรับรองกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) :

- กำหนดให้แอปพลิเคชันใด ๆ ที่จัดเก็บหรือแสดงเอกสารรับรองดิจิทัล (VC) ที่ภาครัฐรับรอง ต้องปฏิบัติตามมาตรฐานและได้รับการตรวจรับรอง
- กำหนดให้มีการเชื่อมโยงการทำงานร่วมกัน (interoperability) และการโอนย้ายข้อมูลได้ในกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ที่ได้รับการรับรอง
- กำหนดกระบวนการยืนยันตัวตนและกฎเกณฑ์การออกเอกสารรับรองดิจิทัล (VC) อัตลักษณ์ดิจิทัลที่สอดคล้องกับกรอบแนวทางการขับเคลื่อนฯ และมาตรฐานที่เกี่ยวข้อง
- พัฒนาขีดความสามารถและกลไกในการทดสอบความสอดคล้องร่วมกันระหว่างหน่วยงานที่เกี่ยวข้องเพื่อสนับสนุนกระบวนการตรวจรับรองกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) และการทำงานของระบบอื่นๆ ที่เกี่ยวข้อง
- กำหนดให้มีกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับประชาชนที่รัฐบาลสนับสนุนได้สูงสุด 2 ใบ[11] และกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับธุรกิจที่รัฐบาลสนับสนุนได้สูงสุด 2 ใบ เพื่อให้การลงทุนภาครัฐมีประสิทธิภาพ
- กรณีกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับธุรกิจ ควรรองรับการใช้หนังสือมอบอำนาจ และหนังสือรับรองนิติบุคคลในรูปแบบ VC รวมถึงหนังสือรับรองฐานะทางการเงินของนิติบุคคล เพื่อรองรับการทำธุรกรรมนิติบุคคลของบริษัทได้อย่างปลอดภัย

5.3 กำหนดให้มีการออกเอกสารรับรองดิจิทัลพื้นฐาน (VC) และการยอมรับจากทุกภาคส่วนที่เกี่ยวข้อง

บริบท: ในปัจจุบันฐานข้อมูลของภาครัฐส่วนใหญ่ได้รับการแปลงให้อยู่ในรูปแบบดิจิทัลแล้ว และมีคุณภาพของข้อมูลที่สามารถใช้เป็นแหล่งข้อมูลทางการได้อย่างน่าเชื่อถือ อย่างไรก็ดี การขยายการใช้งานเอกสารรับรองดิจิทัล (VC) ให้เกิดผลอย่างเต็มรูปแบบ ยังจำเป็นต้องแก้ไขความท้าทายเชิงโครงสร้างสำคัญ 2 ประการ

[11] ตัวเลือกหนึ่งน่าจะเป็นทางรัฐ เนื่องจากมีการนำมาใช้อย่างแพร่หลายและมีบทบาทในปัจจุบันในฐานะ "ซูเปอร์แอปพลิเคชัน" ของภาครัฐ ทั้งนี้ ตัวเลือกอื่น ๆ ที่อาจได้รับการพิจารณา ได้แก่ ThaID และเป๋าตัง

ประการแรก การใช้เอกสารรับรองดิจิทัล (VC) ที่ตรวจสอบได้ยังมิได้ถูกกำหนดให้เป็นเป็นที่ยอมรับอย่างชัดเจน หากบริการสาธารณะของรัฐมิได้ถูกกำหนดให้ยอมรับการใช้เอกสารรับรองดิจิทัล (VC) ที่ตรวจสอบได้ รวมถึงการยอมรับเฉพาะรายการข้อมูลที่เป็นส่วนหนึ่งของเอกสารรับรอง (VC) การนำไปใช้ในวงกว้างอาจหยุดชะงักหรือไม่สามารถขยายผลได้อย่างมีประสิทธิภาพ โดยเฉพาะกรณีที่มีการกำหนดไว้ในระเบียบหรือข้อกฎหมายที่เกี่ยวข้องกับการยื่นเอกสารรับรองว่าจะต้องเป็นการยื่นเอกสารรับรองทั้งเอกสารที่มีข้อมูลครบถ้วนสมบูรณ์ทั้ง ๆ ที่หน่วยงานอาจจะมีการใช้รายการข้อมูลบางรายการเพื่อตรวจสอบเท่านั้น

ประการที่สอง จำเป็นต้องเสริมสร้างขีดความสามารถในการดำเนินงานของหน่วยงานภาครัฐส่วนใหญ่ เนื่องจากบางหน่วยงานยังมีข้อจำกัดด้านงบประมาณ บุคลากร ความพร้อมของระบบ หรือโครงสร้างพื้นฐานที่จำเป็นต่อการออกเอกสารรับรองดิจิทัล (VC) ดังนั้น จึงควรมีแนวทางสนับสนุนที่เป็นระบบ เพื่อให้หน่วยงานที่เกี่ยวข้องสามารถดำเนินการออก ใช้ และยอมรับเอกสารรับรองดิจิทัล (VC) อย่างมั่นคง ปลอดภัย และสอดคล้องกับมาตรฐานที่กำหนด

แนวทางดำเนินการ: เพื่อให้การดำเนินการเกี่ยวกับเอกสารรับรองดิจิทัล (VC) เป็นไปอย่างมีประสิทธิภาพ รัฐบาลควรกำหนดให้มีการออกเอกสารและการยอมรับเอกสารรับรองดิจิทัล (VC) ตลอดจนจัดสรรงบประมาณเฉพาะและโครงสร้างพื้นฐานร่วมเพื่อรองรับการดำเนินการ

โดยเฉพาะภาครัฐควรดำเนินการ ดังนี้:

- เสนอคณะรัฐมนตรีให้มอบหมายหน่วยงานที่รับผิดชอบในการออกเอกสารรับรองดิจิทัลพื้นฐาน (VC) ที่มีปริมาณธุรกรรมสูง อาทิ กรมการปกครอง (อัตลักษณ์ดิจิทัล) กรมพัฒนาธุรกิจการค้า (การจดทะเบียนนิติบุคคล) กรมการขนส่งทางบก (ใบอนุญาตขับขี่) กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม (เอกสารการศึกษา) และกระทรวงสาธารณสุข (เอกสารรับรองดิจิทัลด้านสุขภาพ (VC)) ให้จัดลำดับความสำคัญการออกเอกสารรับรองดิจิทัล (VC) ที่สอดคล้องกับกรอบการสร้างความน่าเชื่อถือ เอกสารรับรองดิจิทัล (VC) เนื่องจากมีปริมาณธุรกรรมสูงและสามารถนำมาใช้ซ้ำได้ในหลายบริการ
- เสนอคณะรัฐมนตรีมอบหมายให้สำนักงบประมาณ สำนักงานพัฒนารัฐบาลดิจิทัล และหน่วยงานที่เกี่ยวข้องสนับสนุนกรมการปกครองในการดำเนินการเกี่ยวกับการออกข้อมูลระบุตัวบุคคล (PID Issuer) เพื่อใช้เป็นเอกสารรับรองดิจิทัล (VC) อัตลักษณ์ดิจิทัลหลักในกรอบการสร้างความน่าเชื่อถือ ซึ่งอาจรวมถึงการจัดลำดับความสำคัญเกี่ยวกับงบประมาณเพิ่มเติมสำหรับการดำเนินการในระบบออกข้อมูลระบุตัวบุคคล (PID Issuer)

- เสนอคณะรัฐมนตรีให้กำหนดให้หน่วยงานภาครัฐที่เกี่ยวข้องยอมรับเอกสารรับรองดิจิทัล (VC) ซึ่งสอดคล้องกับมาตรฐานที่กำหนด ให้มีผลเทียบเท่ากับเอกสารรับรองในรูปแบบกระดาษ เพื่อให้มีผลในทางปฏิบัติ นอกจากนี้ ควรกำหนดให้มีการรับรองอย่างเป็นทางการว่าเอกสารรับรองดิจิทัล (VC) ซึ่งออกจากหน่วยงานที่ได้รับการรับรองตามมาตรฐาน เป็นเอกสารอิเล็กทรอนิกส์ที่มีความถูกต้องและมีผลตามกฎหมาย โดยเฉพาะอย่างยิ่งสำหรับการนำไปใช้ในภาคเอกชน เพื่อสร้างความเชื่อมั่นในการใช้ การยอมรับ และการตรวจสอบเอกสารรับรองดิจิทัล (VC) ระหว่างหน่วยงานภาครัฐ ภาคธุรกิจ และผู้ใช้บริการที่เกี่ยวข้อง
- มีกระบวนการติดตามผลการขับเคลื่อนตามกรอบการสร้างความน่าเชื่อถืออย่างเป็นทางการ เพื่อดำเนินการติดตาม ให้คำแนะนำ และ ขับเคลื่อนโครงการของหน่วยงานต่าง ๆ ให้เป็นไปตาม กรอบการสร้างความน่าเชื่อถือซึ่งอาจอยู่ภายใต้การกำกับดูแลของคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมภายใต้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยอาจจัดตั้ง "คณะอนุกรรมการขับเคลื่อนการใช้เอกสารรับรอง VC" เป็นการเฉพาะ

- ประสานงานกับธนาคารแห่งประเทศไทยและหน่วยงานกำกับดูแลภาคส่วนอื่น ๆ เพื่อให้การยอมรับตามมาตรฐานในภาคส่วนที่กำกับดูแล อาทิ การเงิน สาธารณสุข การศึกษา และการออกใบอนุญาตวิชาชีพ

- สำหรับหน่วยงานขนาดใหญ่ที่มีสมรรถนะสูง ให้จัดตั้งกองทุนสนับสนุนการจัดทำเอกสารรับรองดิจิทัลเฉพาะด้าน (VC) บริหารจัดการโดยสำนักงานพัฒนารัฐบาลดิจิทัล เพื่อจัดสรรงบประมาณสำหรับการบูรณาการระบบ การเตรียมข้อมูล การสอดคล้องทางกฎหมาย และการเปลี่ยนแปลงเชิงโครงสร้างที่จำเป็นภายใต้กรอบการสร้างความน่าเชื่อถือ สำหรับการออกเอกสารและการยืนยันเอกสารรับรองดิจิทัล (VC) งบประมาณเฉพาะด้านมีความจำเป็นอย่างยิ่ง เนื่องจากในปัจจุบันหน่วยงานส่วนใหญ่ขาดงบประมาณเกี่ยวกับโครงสร้างพื้นฐานและความสามารถในการออกเอกสารและยืนยันเอกสารรับรองดิจิทัล (VC)

- สำหรับหน่วยงานขนาดเล็กที่มีข้อจำกัดด้านความสามารถทางเทคนิค ต้องผลักดันให้มีการพัฒนาความสามารถในการออกเอกสารรับรองดิจิทัล (VC) ระดับประเทศ ศูนย์แลกเปลี่ยนข้อมูลกลางภาครัฐ (GDX) โดยใช้ประโยชน์จากการเชื่อมต่อที่มีอยู่ของข้อมูลกลางภาครัฐ (GDX) กับทุกหน่วยงานภาครัฐ เพื่อให้หน่วยงานสามารถออกเอกสารรับรองดิจิทัล (VC) โดยไม่ต้องสร้างระบบเฉพาะ

- พัฒนา SDK หรือแอปพลิเคชันสำหรับการตรวจสอบสากล (Universal Verifier) สำหรับหน่วยงานภาครัฐ เพื่อให้สามารถยืนยันเอกสารรับรองดิจิทัล (VC) ที่สอดคล้องในบริการสาธารณะและการปฏิสัมพันธ์กับภาครัฐทั้งหมดได้ในวงกว้าง

- เผยแพร่สถาปัตยกรรมสำหรับการอ้างอิงเพื่อพัฒนาระบบแบบเปิดและเครื่องมือทดสอบความสอดคล้อง เพื่อให้หน่วยงานต่าง ๆ สามารถพัฒนาแอปพลิเคชันสำหรับการตรวจสอบที่สอดคล้องกับมาตรฐานของตนเองตามมาตรฐานที่กำหนด

5.4 กำหนดลำดับความสำคัญกรณีการใช้งานที่มีผลกระทบสูง 5 ประการ

บริบท: เพื่อสร้างแรงขับเคลื่อนการนำไปใช้ ในระยะแรกควรมุ่งเน้นไปที่การใช้งานที่เป็นที่ประจักษ์และสามารถวัดผลกระทบได้ การส่งมอบกรณีการใช้งานเหล่านี้จึงจำเป็นต้องอาศัยการปรับนโยบายและกฎระเบียบให้สอดคล้องกัน มีเป้าหมายสำหรับการลงทุน และการมีส่วนร่วมกับผู้มีส่วนเกี่ยวข้องทั้งภาครัฐและภาคเอกชน ผลสำเร็จในระยะแรกจึงเป็นปัจจัยสำคัญในการแสดงคุณค่า เพื่อเป็นเหตุผลในการจัดสรรงบประมาณ และขับเคลื่อนการดำเนินการในวงกว้าง

แนวทางดำเนินการ: รัฐบาลควรกำหนดกรณีการใช้งานที่มีลำดับความสำคัญสูงสุดไม่เกิน 5 กรณี เพื่อเร่งรัดการดำเนินการภายใต้กรอบการสร้างความน่าเชื่อถือ โดยต้องมีการกำหนดความรับผิดชอบของหน่วยงานที่เกี่ยวข้องให้ชัดเจน กรอบเวลาในการดำเนินการ และตัวชี้วัดที่สามารถวัดผลการดำเนินงานได้ การคัดเลือกและการดำเนินการกรณีการใช้งานตามลำดับความสำคัญ ควรประเมินผลกระทบด้านการมีส่วนร่วมและความเสมอภาคอย่างชัดเจน โดยเฉพาะสำหรับสตรีและประชากรที่มีข้อจำกัดด้านการเชื่อมต่ออินเทอร์เน็ตและ/หรือมีความรู้เท่าทันดิจิทัลต่ำ รวมทั้งต้องมีตัวชี้วัดเพื่อติดตามการนำไปใช้และผลลัพธ์ในกลุ่มประชากรเหล่านี้ กรณีการใช้งานที่มีความสำคัญสูงสุดเหล่านี้ ควรยึดโยงกับเอกสารรับรองดิจิทัล (VC) พื้นฐานที่จัดลำดับความสำคัญภายใต้ข้อเสนอแนะ 3.3 ในแต่ละกรณีการใช้งานควรมีหน่วยงานหลักเพียงแห่งเดียวรับผิดชอบในการดำเนินการ โดยสำนักงานคณะกรรมการพัฒนาระบบราชการ (ก.พ.ร.) ทำหน้าที่ประสานการดำเนินงานระหว่างหน่วยงาน และ สพธอ. ให้การกำกับดูแลด้านเทคนิค เพื่อความสอดคล้องกับกรอบการสร้างความน่าเชื่อถือ

กรณีการใช้งานที่สำคัญ ได้แก่

- **การเข้าถึงสินเชื่อและบริการทางการเงินสำหรับภาคธุรกิจ**: สนับสนุนให้ภาคธุรกิจ รวมถึง MSME สามารถแปลงการจดทะเบียนนิติบุคคล ข้อมูลภาษี ใบอนุญาต และข้อมูลทางการเงินที่ผ่านการตรวจแล้ว ให้เป็นเอกสารรับรองดิจิทัล (VC) ที่นำมาใช้ซ้ำได้ ซึ่งรองรับการประเมินความน่าเชื่อถือทางการเงิน ลดต้นทุนการตรวจสอบธุรกิจ และเร่งการเข้าถึงแหล่งเงินทุน
    - หน่วยงานหลัก: กระทรวงพาณิชย์
    - เอกสารรับรองดิจิทัล (VC) สำคัญ: หนังสือรับรองการจดทะเบียนธุรกิจ (กรมพัฒนาธุรกิจการค้า) ใบรับรองการปฏิบัติตามกฎหมายภาษี (กรมสรรพากร) ใบอนุญาตประกอบธุรกิจ (หน่วยงานกำกับดูแลภาคส่วน อาทิ สำนักงานคณะกรรมการอาหารและยา สำนักงานคณะกรรมการส่งเสริมการลงทุน) งบการเงิน (ธนาคาร/นิติบุคคลที่ธนาคารแห่งประเทศไทยกำกับดูแล)

- **การตรวจสอบอายุโดยคุ้มครองความเป็นส่วนตัว**: สนับสนุนให้มีการพิสูจน์อายุอย่างปลอดภัย สำหรับบริการที่อยู่ภายใต้การกำกับดูแลและบริการออนไลน์ (อาทิ การจำหน่ายสุรา) เพื่อลดการฉ้อโกงและความเสี่ยงด้านกฎระเบียบ พร้อมทั้งคุ้มครองข้อมูลส่วนบุคคล
    - **หน่วยงานหลัก**: กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
    - **เอกสารรับรองดิจิทัล (VC) สำคัญ**: เอกสารรับรองดิจิทัล (VC) สำหรับบัตรประจำตัวประชาชน (กรมการปกครอง)
- **การเข้าถึงสวัสดิการสังคม**: สนับสนุนให้ประชาชนที่มีสิทธิ์สามารถการแสดงเอกสารรับรองดิจิทัล (VC) ที่ยืนยันรายได้ ที่พักอาศัย ความพิการ สถานะครัวเรือน และข้อมูลอื่น ๆ เพื่อเพิ่มประสิทธิภาพการลงทะเบียนในโครงการสวัสดิการสังคมของภาครัฐ ลดภาระงานด้านการบริหาร ปรับปรุงความแม่นยำในการกำหนดเป้าหมาย และลดการลงทะเบียนซ้ำซ้อนในโครงการต่าง ๆ
    - **หน่วยงานหลัก**: กระทรวงการคลัง
    - **เอกสารรับรองดิจิทัล (VC) สำคัญ**: เอกสารรับรองดิจิทัล (VC) บัตรสวัสดิการ/สิทธิประโยชน์ (กระทรวงการคลัง) การตรวจสอบรายได้ (กรมสรรพากร) ทะเบียนบ้าน (กรมการปกครอง) และอื่น ๆ
- **การโอนย้ายเอกสารรับรองดิจิทัล (VC) ด้านสุขภาพ**: สนับสนุนให้มีเอกสารรับรองดิจิทัล (VC) ด้านสุขภาพที่ปลอดภัยซึ่งผู้ป่วยควบคุมได้เอง เพื่อลดภาระงานด้านการบริหารและปรับปรุงความต่อเนื่องในการรักษาพยาบาลระหว่างผู้ให้บริการหลายราย
    - **หน่วยงานหลัก**: กระทรวงสาธารณสุข
    - **เอกสารรับรองดิจิทัล (VC) สำคัญ**: สิทธิประกันสุขภาพ (สำนักงานหลักประกันสุขภาพแห่งชาติ) บันทึกการฉีดวัคซีนและภูมิคุ้มกัน (กระทรวงสาธารณสุข) สรุปประวัติทางการแพทย์ (โรงพยาบาล/ผู้ให้บริการที่กระทรวงสาธารณสุขรับรอง)
- **ใบอนุญาตขับขี่ ใบอนุญาตวิชาชีพ และเอกสารรับรองดิจิทัล (VC) ทางวิชาการ** : สนับสนุนให้มีใบอนุญาตขับขี่ดิจิทัล ใบอนุญาตวิชาชีพดิจิทัล และคุณวุฒิทางการศึกษาดิจิทัล ที่ข้อมูลสามารถเชื่อมโยงกันได้ เพื่อรองรับการจ้างงาน การเดินทาง และการรับรองข้ามพรมแดน ตัวอย่างเช่น การยืนยันใบอนุญาตวิชาชีพเวชกรรมในระหว่างบริการแพทย์ทางไกล และการใช้ใบอนุญาตขับขี่เพื่อเช่ารถยนต์ในต่างประเทศ
    - **หน่วยงานหลัก :** กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
    - **เอกสารรับรองดิจิทัล (VC) สำคัญ** : ใบอนุญาตขับขี่ (กรมการขนส่งทางบก) ใบอนุญาตประกอบวิชาชีพ อาทิ แพทย์ พยาบาล วิศวกรรม (สภาวิชาชีพที่เกี่ยวข้อง) ใบแสดงผลการศึกษา (มหาวิทยาลัย/กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม)

5.5 การเป็นผู้นำของอาเซียนในการพัฒนามาตรฐานระดับภูมิภาค

บริบท: การบูรณาการด้านดิจิทัลของอาเซียนภายใต้กรอบความตกลงเศรษฐกิจดิจิทัลอาเซียน (Digital Economy Framework Agreement: DEFA) มีแนวโน้มเร่งตัวขึ้นอย่างต่อเนื่อง อย่างไรก็ดี มาตรฐานระดับภูมิภาคที่เกี่ยวข้องกับอัตลักษณ์ดิจิทัลที่น่าเชื่อถือ และการแลกเปลี่ยนข้อมูลข้ามพรมแดน ยังคงอยู่ในระยะเริ่มต้นของการพัฒนา ในบริบทดังกล่าว ประเทศที่สามารถจัดตั้งกรอบการกำกับดูแลระดับประเทศที่มีผลบังคับใช้อย่างชัดเจนได้ก่อน ย่อมมีโอกาสในการมีบทบาทสำคัญต่อการกำหนดมาตรฐานทางเทคนิค แนวทางการดำเนินงาน และข้อตกลงการรับรองร่วมกันในระดับภูมิภาค ดังนั้นการดำเนินการเชิงรุกตั้งแต่ระยะเริ่มต้นจะช่วยให้ประเทศไทยสามารถมีส่วนร่วมในการกำหนดบรรทัดฐานระดับภูมิภาคด้านอัตลักษณ์ดิจิทัลและการแลกเปลี่ยนข้อมูลที่น่าเชื่อถือ เพื่อสนับสนุนเป้าหมายด้านการค้า เสริมสร้างการบูรณาการทางเศรษฐกิจดิจิทัล ดึงดูดการลงทุน และวางตำแหน่งของประเทศไทยให้เป็นศูนย์กลางด้านความเชี่ยวชาญและโครงสร้างพื้นฐานด้านความเชื่อมั่นดิจิทัลในระดับอาเซียน

แนวทางดำเนินการ: รัฐบาลควรผลักดันการพัฒนาเอกสารรับรองดิจิทัล (VC) ให้เป็นวาระสำคัญในระดับภูมิภาค ผ่านกลไกความร่วมมือดิจิทัลและเศรษฐกิจของอาเซียน

ข้อเสนอแนะเฉพาะสำหรับประเทศไทย:

- ดำเนินโครงการนำร่องแบบทวิภาคีและไตรภาคีกับประเทศสมาชิกอาเซียน ในกรณีการใช้งานที่มีผลสาธิตสูง อาทิ ใบอนุญาตขับขี่ร่วมกับมาเลเซียและสิงคโปร์
- ผลักดันการเอกสารรับรองดิจิทัล (VC) ผ่านการประชุมรัฐมนตรีดิจิทัลอาเซียน (ADGMIN) การประชุมรัฐมนตรีเศรษฐกิจอาเซียน (AEM) และคณะทำงานที่เกี่ยวข้อง โดยเสนอให้มีการรับรองอย่างเป็นทางการภายใต้เสาหลัก ได้แก่ อัตลักษณ์ดิจิทัล การยืนยันตัวตน และการแลกเปลี่ยนข้อมูล พร้อมทั้งผลักดันการรับรองร่วมกันสำหรับเอกสารรับรองดิจิทัล (VC) ที่ออกภายใต้กรอบแนวทางการสร้างความเชื่อถือแห่งชาติสำหรับเอกสารรับรองดิจิทัล (VC)
- เสนอโครงการนำร่องระดับภูมิภาคในพื้นที่ที่มีมูลค่าสูง ซึ่งสอดคล้องกับเสาหลักกรอบความตกลงเศรษฐกิจดิจิทัล (DEFA) และกรอบแนวทางการสร้างความเชื่อถือแห่งชาติสำหรับเอกสารรับรองดิจิทัล (VC)อาทิ การทำให้เอกสารทางการค้าเป็นดิจิทัล การสร้างอัตลักษณ์ดิจิทัลธุรกิจข้ามพรมแดน (ระบบเลขทะเบียนนิติบุคคลเดียวของอาเซียน หรือ ASEAN Unique Business Identification Number: UBIN) การรับรองเอกสารรับรองดิจิทัลวิชาชีพ (VC) และการโอนย้ายเอกสารรับรองดิจิทัลด้านสุขภาพ (VC) สำหรับการเดินทางและการท่องเที่ยว
- เสนอให้ประเทศไทยเป็นศูนย์กลางความเชี่ยวชาญระดับภูมิภาค โดยแบ่งปันความเชี่ยวชาญด้านเทคนิคและสถาปัตยกรรมอ้างอิงกับประเทศสมาชิกอาเซียน และสร้างโอกาสให้บริษัทเทคโนโลยีไทยสามารถส่งออกโซลูชันและบริการทั่วภูมิภาค
- เป็นผู้นำในการหารือด้านการทำงานร่วมกันข้ามพรมแดนกับประเทศและกลุ่มเศรษฐกิจนอกอาเซียน อาทิ สหภาพยุโรป สหราชอาณาจักร และเกาหลีใต้ เพื่อวางบทบาทประเทศไทยให้เป็นสะพานเชื่อมระหว่างอาเซียนและกรอบความเชื่อมั่นระดับโลก

6 กรอบแนวทางการขับเคลื่อนเพื่อพัฒนาระบบนิเวศของการใช้เอกสารรับรองดิจิทัลที่ตรวจสอบได้

กรอบแนวทางการขับเคลื่อนเพื่อพัฒนาระบบนิเวศของการใช้เอกสารรับรองดิจิทัลที่ตรวจสอบได้ของประเทศไทย ควรมีการแบ่งการดำเนินการออกเป็นช่วงระยะเวลาโดยต่อยอดจากผลการดำเนินงานที่สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) และคณะทำงานส่งเสริมการพัฒนาระบบเพื่อรองรับการใช้งานเอกสารรับรองดิจิทัล (Verifiable Credentials) และกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ได้ดำเนินการไว้ ทั้งนี้ เป้าหมายของการดำเนินการ คือ การพัฒนาและทดสอบกรอบการทำงานเชิงเทคนิคร่วมกันและออกแบบการกำกับดูแลที่สามารถบังคับใช้ได้จริงและนำไปใช้งานในระดับประเทศได้อย่างเหมาะสม

6.1 ระยะที่ 1 (พ.ศ. 2569) : จัดทำกรอบอำนาจทางกฎหมายและระบบธรรมาภิบาลที่สามารถบังคับใช้ได้

ประเด็นหลัก คือ การออกคำสั่งหรือกฎระเบียบทางกฎหมายที่ชัดเจน ตลอดจนเกิดการบังคับใช้งานจริง รวมถึงการขยายผลการใช้งานกระบวนการและองค์ประกอบทางเทคนิคที่มีอยู่ โดยต่อยอดจากการพัฒนาของ สพธอ. อาทิ ข้อเสนอแนะมาตรฐานโครงสร้างข้อมูลเอกสารรับรองและเอกสารสำแดง รายงานทางเทคนิคกรอบการทำงานร่วมกันของกระเป๋าดิจิทัลสำหรับเอกสารรับรอง ผลการดำเนินงานของคณะทำงานฯ และเครื่องมือทดสอบที่เกี่ยวข้อง ทั้งนี้ ในระยะที่ 1 ควรมุ่งเน้นการออกคำสั่งหรือกฎระเบียบทางกฎหมายที่ชัดเจน เพื่อบังคับใช้และกำหนดให้หน่วยงานภาครัฐต้องปฏิบัติตาม

แนวทางดำเนินการสำคัญ ดังนี้

- เสนอคณะรัฐมนตรีให้มีมติรับรองกรอบแนวทางการสร้างความเชื่อถือแห่งชาติสำหรับเอกสารรับรองดิจิทัล (VC) และเกิดการบูรณาการจากการทำงานร่วมกันของหน่วยงานภาครัฐ และออกคำสั่งหรือกฎระเบียบทางกฎหมายว่าเอกสารรับรองดิจิทัล (VC) ที่ออกภายใต้กรอบแนวทางการขับเคลื่อนดังกล่าว เป็นเอกสารอิเล็กทรอนิกส์ที่มีผลและสามารถใช้งานได้ตามกฎหมาย
- เผยแพร่และทำให้เกิดแนวปฏิบัติการทำงานร่วมกันระดับประเทศ โดยอิงจากกรอบการทำงานร่วมกันของกระเป๋าดิจิทัลสำหรับเอกสารรับรอง และกระบวนการทดสอบความสอดคล้องของระบบที่ สพธอ. มีอยู่แล้ว
- เปิดใช้งานกระบวนการรับรองกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) และผู้ออกเอกสารดิจิทัล รวมถึงกลไกการตรวจสอบก่อนระบบจะมีการให้บริการเป็นสาธารณะ ที่พัฒนาไว้แล้ว อาทิ กรอบการสร้างความน่าเชื่อถือของเอกสารรับรองและเอกสารสำแดง ข้อกำหนดหรือหลักเกณฑ์เกี่ยวกับบริการที่จำเป็นในระบบนิเวศของกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) พร้อมรายการตรวจประเมินที่จะแล้วเสร็จภายในเดือนกันยายน พ.ศ. 2569
- จัดตั้งกองทุนเพื่อสนับสนุนการพัฒนาเอกสารรับรองดิจิทัล (VC) ภายใต้การบริหารงานของสำนักงานพัฒนารัฐบาลดิจิทัล (สพร.) เพื่อจัดสรรงบประมาณให้แก่หน่วยงานภาครัฐ โดยเริ่มตั้งแต่ปีงบประมาณ พ.ศ. 2570

- พัฒนาขีดความสามารถในการออกเอกสารรับรองดิจิทัล (VC) ระดับประเทศ ภายใต้ศูนย์แลกเปลี่ยนข้อมูลกลางภาครัฐ (GDX) และระบบทะเบียนเอกสารรับรอง (verifiable data registry) สำหรับหน่วยงานภาครัฐ
- พัฒนาแอปพลิเคชัน “ทางรัฐ” ให้เป็นกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับประชาชน และพัฒนาชุดเครื่องมือพัฒนาซอฟต์แวร์สำหรับผู้ตรวจสอบเอกสารสำแดง (Universal Verifier SDK) เพื่อให้สามารถยืนยันว่าเอกสารรับรองดิจิทัล (VC) สอดคล้องข้อกำหนดทางมาตรฐาน ครอบคลุมในทุกบริการของภาครัฐพร้อมทั้งเริ่มการประสานงานกับธนาคารแห่งประเทศไทยและหน่วยงานกำกับดูแลอื่น ๆ เพื่อให้เกิดความสอดคล้องและการยอมรับของแต่ละภาคส่วน
- กำหนดเกณฑ์การคัดเลือกกรณีการใช้งานเอกสารรับรองดิจิทัลระดับประเทศที่มีความสำคัญและผลกระทบสูง โดยพิจารณาจากปริมาณการใช้งาน ความต้องการของผู้ใช้บริการ ลักษณะการให้บริการแบบครบวงจร ที่มีความจำเป็นต้องใช้ข้อมูลการยืนยันตัวตน เช่น ข้อมูลส่วนบุคคล ข้อมูลประจำตัวตามบัตรประชาชน และที่สามารถลดกระบวนการที่ซับซ้อนหรือลดการฉ้อโกงลงได้
- ดำเนินโครงการนำร่องแบบทวิภาคีและไตรภาคีกับประเทศสมาชิกอาเซียน ในกรณีการใช้งานที่มีที่สามารถแสดงให้เห็นผลสัมฤทธิ์สูง อาทิ ใบอนุญาตขับขี่ร่วมกับมาเลเซียและสิงคโปร์
- สร้างการมีส่วนร่วมของภาคประชาชน เพื่อสร้างความตระหนักรู้เกี่ยวกับเอกสารรับรองดิจิทัล (VC)
- ผลักดันให้หน่วนงานภาครัฐทั้งส่วนกลางและส่วนท้องถิ่น เกิดองค์ความรู้และความเข้าใจเกี่ยวกับเอกสารรับรองดิจิทัล (VC) และเพื่อให้แน่ใจว่าหน่วยงานภาครัฐทุกแห่งเตรียมพร้อมสำหรับการยอมรับเอกสารรับรองดิจิทัล (VC) ที่อาจเกิดขึ้นในอนาคต
- จัดตั้งคณะกรรมการขับเคลื่อนและพัฒนาระบบนิเวศของการใช้เอกสารรับรองดิจิทัลที่ตรวจสอบได้ของประเทศไทยภายใต้คณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ รับผิดชอบการกำกับดูแลและติดตามแผนการดำเนินงาน รวมถึงการตัดสินใจด้านนโยบายที่จำเป็น คณะกรรมการฯ ควรประกอบด้วย ผู้มีส่วนเกี่ยวข้องในนโยบายดังกล่าว โดยให้ สพธอ. ทำหน้าที่เป็นฝ่ายเลขานุการของคณะกรรมการฯ

ผลลัพธ์ของระยะที่ 1 คือ กรอบแนวทางการขับเคลื่อนเพื่อพัฒนาระบบนิเวศของการใช้เอกสารรับรองดิจิทัลที่ตรวจสอบได้ประเทศไทย ที่มีผลบังคับใช้ตามกฎหมาย ซึ่งจัดทำขึ้นบนพื้นฐานทางเทคนิคที่ สพธอ. ออกแบบและพัฒนาไว้ โดยมีผู้เข้าร่วมที่ได้รับการรับรอง มาตรฐานที่ได้รับการยอมรับ ผู้ให้บริการกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ที่ได้รับการขึ้นทะเบียน และความสามารถในการออกเอกสารรับรองดิจิทัล (VC) ที่สามารถทำงานร่วมกันได้ พร้อมสำหรับการนำไปขยายผลการใช้งานในระดับประเทศ

6.2 ระยะที่ 2 (พ.ศ. 2570) : กำหนดให้มีการออกเอกสารรับรองดิจิทัล (VC) ให้เป็นที่ยอมรับในภาครัฐและภาคส่วนที่อยู่ภายใต้การกำกับดูแล พร้อมนำกรณีการใช้งานที่มีความสำคัญสูงมาใช้งานจริง

ประเด็นหลัก คือ การออกเอกสารรับรองดิจิทัล (VC) ตามข้อกำหนด การยอมรับตามข้อกำหนด และนำไปใช้งานได้ในระดับปฏิบัติการ

แนวทางดำเนินการสำคัญ ดังนี้

- ยืนยันกรณีการใช้งานระดับประเทศที่มีผลกระทบสูงตามลำดับความสำคัญ โดยอิงจากเกณฑ์ที่ถูกกล่าวถึงในระยะที่ 1
- กำหนดให้หน่วยงานที่มีหน้าที่ออกเอกสารรับรองที่สำคัญ ได้แก่ กรมการปกครอง กรมพัฒนาธุรกิจการค้า กรมการขนส่งทางบก กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม และกระทรวงสาธารณสุข ออกเอกสารรับรองดิจิทัล (VC) ที่สอดคล้องกับกรอบการสร้างความน่าเชื่อถือของเอกสารรับรองและเอกสารสำแดง
- ดำเนินการบังคับการใช้งานและการยอมรับเอกสารรับรองดิจิทัล (VC) ในบริการสาธารณะ โดยเริ่มจากกรณีการใช้งานที่มีความสำคัญ พร้อมกำหนดระยะเวลาที่มีผลบังคับใช้ที่ชัดเจนเพื่อให้ผู้ให้บริการภาครัฐรายอื่นสามารถนำไปใช้ได้ในระยะที่ 3
- จัดเตรียมเครื่องมือเพื่อสนับสนุนผู้ให้บริการและผู้ออกเอกสารรับรองสำหรับการพัฒนาและปรับปรุงระบบ รวมถึงคู่มือหรือแนวทางการพัฒนาที่ชัดเจน สถาปัตยกรรมอ้างอิงแบบโอเพนซอร์ส (open source) และสภาพแวดล้อมจำลองสำหรับการทดสอบ (sandbox) สำหรับผู้ออกเอกสารรับรองดิจิทัล (Issuer) รายใหม่ และผู้ให้บริการที่ต้องใช้งาน VC รายใหม่
- ดำเนินการให้ภาคการเงินยอมรับเอกสารรับรองดิจิทัล (VC) โดยการประสานงานกับธนาคารแห่งประเทศไทย
- นำกรณีศึกษาที่มีผลกระทบสูงตามที่กำหนดไว้ไปใช้งานจริง ได้แก่ การเข้าถึงสินเชื่อและบริการทางการเงินของธุรกิจ การยืนยันอายุแบบรักษาความเป็นส่วนตัว เอกสารรับรองการค้าอาเซียน และการรับรองทางการแพทย์หรือการส่งตัวไปยังสถานพยาบาลอื่น ใบอนุญาตขับขี่ และใบประกอบวิชาชีพ
- ขยายขอบเขตการทดสอบความสอดคล้องและกลไกการตรวจสอบ เพื่อให้มั่นใจว่ามีการปฏิบัติตามข้อกำหนด
- จัดทำโครงการสร้างการรับรู้แก่สาธารณะและการมีส่วนร่วมของผู้มีส่วนเกี่ยวข้อง มุ่งเน้นกรณีการใช้งานระดับประเทศที่มีผลกระทบสูง
- กำหนดตัวชี้วัด (KPIs) ของหน่วยงาน เรื่อง การยอมรับเอกสารรับรองดิจิทัล (VC) และการลดระยะเวลาดำเนินการให้บริการ โดยให้รายงานต่อคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ เพื่อสร้างความมั่นใจและความรับผิดชอบว่าเป้าหมายจะถูกนำไปปฏิบัติจริง

- ผลักดันโครงการนำร่องระดับอาเซียนภายใต้กรอบความตกลงเศรษฐกิจดิจิทัล (DEFA) ในด้านการค้า การเงิน การเดินทาง และการท่องเที่ยว
- สนับสนุนและผลักดันให้เกิดการยอมรับเอกสารรับรองดิจิทัล (VC) ร่วมกันทั่วทั้งภูมิภาคอาเซียน

ผลลัพธ์ของระยะที่ 2 คือ เอกสารรับรองดิจิทัล (VC) จะถูกนำไปใช้จริงในระดับปฏิบัติการกับภาคส่วนที่มีความสำคัญ และประเทศไทยมีบทบาทเป็นผู้นำในการกำหนดรูปแบบการยืนยันตัวตนทางดิจิทัลและกรอบการแลกเปลี่ยนข้อมูลที่น่าเชื่อถือของอาเซียน

6.3 ระยะที่ 3 (พ.ศ. 2571–2572) : ดำเนินการขยายการใช้งานสู่ระดับประเทศ และส่งเสริมให้มีการรับรองซึ่งกันและกันในระดับอาเซียน

ประเด็นหลัก คือ การใช้งานเต็มรูปแบบ การบังคับใช้ ความยั่งยืน และการดำเนินการระดับภูมิภาค

แนวทางดำเนินการสำคัญ ดังนี้

- ขยายการออกเอกสารและการยอมรับเอกสารรับรองดิจิทัล (VC) ไปยังหน่วยงานและภาคส่วนที่อยู่ภายใต้การกำกับดูแลเพิ่มเติม
- ควบคุมและติดตามการปฏิบัติตามข้อกำหนดเป็นระยะ และบังคับใช้ข้อกำหนดการทำงานร่วมกันและข้อกำหนดในการรับรองระบบงาน
- ขยายผลแพลตฟอร์มการออกเอกสารรับรองดิจิทัล (VC) ที่บูรณาการกับศูนย์แลกเปลี่ยนข้อมูลกลางภาครัฐ (GDX) เพื่อให้เกิดการใช้งานระดับประเทศ
- ใช้รูปแบบดำเนินงานเชิงพาณิชย์ที่มีความยั่งยืนและรูปแบบการรับรองสำหรับการกำกับดูแลระบบนิเวศในระยะยาว
- ขยายการบูรณาการกับภาคเอกชนให้ครอบคลุมถึงด้านการเงิน โทรคมนาคม การศึกษา และบริการดิจิทัลปริมาณสูง
- นำข้อตกลงการยอมรับร่วมกันในระดับอาเซียนมาปฏิบัติ และบูรณาการเอกสารรับรองดิจิทัล (VC) เข้ากับระบบการค้าและระบบการเดินทางข้ามพรมแดน
- ดำเนินกิจกรรมเพื่อการสร้างการรับรู้แก่สาธารณะและส่งเสริมการนำไปใช้ระดับประเทศ

ผลลัพธ์ของระยะที่ 3 คือ ประเทศไทยมีระบบนิเวศเอกสารรับรองดิจิทัล (VC) ที่บังคับใช้ได้อย่างเต็มรูปแบบและทำงานร่วมกันได้ในระดับประเทศ พร้อมการกำกับดูแลที่ยั่งยืนและการยอมรับการใช้งานข้ามพรมแดนได้อย่างเป็นรูปธรรมภายในภูมิภาคอาเซียน

6.4 ระยะที่ 4 (พ.ศ. 2573–2575) : การสร้างความยั่งยืนและการนำไปใช้ในเชิงพาณิชย์ที่มีศักยภาพ

ประเด็นหลัก คือ กรอบการสร้างความน่าเชื่อถือของเอกสารรับรองและเอกสารสำแดงจะมีความยั่งยืนและสามารถใช้งานในระยะยาวได้อย่างสมบูรณ์แบบ โดยมีการประกอบธุรกิจที่เกี่ยวข้องกับการออกเอกสารและการใช้งานเอกสารรับรองดิจิทัล (VC) นอกเหนือหน่วยงานภาครัฐ

แนวทางดำเนินการสำคัญ ดังนี้

- พิจารณาเรียกเก็บค่าธรรมเนียมหรือค่าบำรุงรักษาจากหน่วยงานภาครัฐ หรือการเรียกเก็บค่าบริการระหว่างหน่วยงานสำหรับการเข้าถึงกรอบการสร้างความน่าเชื่อถือของเอกสารรับรองและเอกสารสำแดงของภาครัฐ
- สร้างความสมดุลระหว่างผู้มีส่วนเกี่ยวข้อง ด้วยการกำหนดแนวทางคืนค่าใช้จ่าย (Cost Recovery) แบบผสมผสานสำหรับการดำเนินการตามกรอบการสร้างความน่าเชื่อถือโดยยังคงสร้างแรงจูงใจให้มีการผลิตข้อมูลคุณภาพสูง และคงระดับการมีส่วนร่วมในงานบริการ เช่น
    - ผู้ออกเอกสาร — ได้รับแรงจูงใจจากการคืนค่าใช้จ่ายหรือรายได้ใหม่สำหรับการให้ข้อมูลที่มีคุณภาพสูงและข้อมูลที่ผ่านการรับรอง
    - ผู้ใช้งาน / ภาคธุรกิจ — ได้รับแรงจูงใจจากการได้รับบริการที่ดีขึ้นและภาระงานด้านธุรการที่ลดลง
    - ผู้ตรวจสอบเอกสารดิจิทัล หรือหน่วยงานที่ใช้ข้อมูลการยืนยันตัวตน — ได้รับแรงจูงใจจากการลดการฉ้อโกง สามารถดำเนินการ KYC/KYB ได้โดยอัตโนมัติ และลดต้นทุนการปฏิบัติงาน
- การติดตามตัวชี้วัดด้านความยั่งยืนเพื่อติดตามประสิทธิภาพของการดำเนินการเชิงพาณิชย์ เช่น ตัวชี้วัดเรื่องต้นทุนต่อการยืนยัน 1 ครั้ง (Cost per Verification) ตัวชี้วัดจำนวนครั้งที่ใช้เอกสารรับรองดิจิทัล (VC) ฉบับเดิมซ้ำ (Credential Velocity) โดยจำนวนครั้งที่มากขึ้น หมายถึงอัตราผลตอบแทนต่อการลงทุนการผลิตข้อมูลที่สูงขึ้น และตัวชี้วัดจำนวนผู้ตรวจสอบในระบบ (Verifier Onboarding)
- การมีระบบเรียกเก็บค่าธรรมเนียมที่คำนึงถึงความเป็นส่วนตัว (Privacy-first Billing) โดยหลีกเลี่ยงความเสี่ยงที่กลไกการเรียกเก็บค่าธรรมเนียมจะกลายเป็นกลไกการติดตามข้อมูล

ผลลัพธ์ของระยะที่ 4 คือ กรอบการสร้างความน่าเชื่อถือของเอกสารรับรองและเอกสารสำแดงที่มีความยั่งยืนและสามารถใช้งานในระยะยาวได้อย่างสมบูรณ์แบบ และสามารถรองรับการขยายตัวของการใช้งานเอกสารรับรองดิจิทัล (VC) ในภาครัฐและภาคเอกชน

6.5 สรุปบทบาทและความรับผิดชอบ

การดำเนินการตามกรอบแนวทางการขับเคลื่อนเพื่อพัฒนาระบบนิเวศของการใช้เอกสารรับรองดิจิทัลที่ตรวจสอบได้นี้ให้ประสบความสำเร็จจำเป็นต้องอาศัยความร่วมมือระหว่างหน่วยงาน อย่างน้อยจากหน่วยงานดังนี้

- กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม: กำหนดทิศทางนโยบายโดยรวมและกำกับดูแลเชิงนโยบายสำหรับระบบนิเวศของเอกสารรับรองดิจิทัล (VC) รวมถึงการนำเสนอเรื่องดังกล่าวต่อคณะรัฐมนตรี รวมถึงดำเนินการให้สอดคล้องกับยุทธศาสตร์เศรษฐกิจดิจิทัลแห่งชาติ และประสานงานระหว่างหน่วยงานที่ดำเนินการ
- สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์: เป็นหน่วยงานผู้นำในการออกแบบ กำกับดูแล และบังคับใช้กรอบการสร้างความน่าเชื่อถือของเอกสารรับรองและเอกสารสำแดงในระดับประเทศ รวมถึงมาตรฐาน การรับรอง การทำงานร่วมกัน และการประสานงานข้ามพรมแดน
- สำนักงาน ก.พ.ร.: ประสานการดำเนินงานระหว่างหน่วยงานภาครัฐ ผ่านการระบุบริการที่มีความสำคัญสอดคล้องระหว่างหน่วยงาน และให้การรับรองเอกสารรับรองดิจิทัล (VC) ภายใต้พระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. 2565 สามารถสนับสนุนการใช้งานภาครัฐได้จริง
- สำนักงานพัฒนารัฐบาลดิจิทัล: ส่งเสริมการนำไปใช้และขยายผลในภาครัฐ โดยการบูรณาการเอกสารรับรองดิจิทัล (VC) เข้าสู่บริการสาธารณะ พัฒนาขีดความสามารถด้านการออกเอกสารรับรองดิจิทัล (VC) ร่วมกันภายในศูนย์แลกเปลี่ยนข้อมูลกลางภาครัฐ (GDX) บริหารจัดการกองทุนสนับสนุนการพัฒนาเอกสารรับรองดิจิทัล (VC) และพัฒนาแอปพลิเคชัน “ทางรัฐ” เป็นกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) และระบบตรวจสอบที่รัฐบาลรับรอง โดยมีสำนักงานพัฒนารัฐบาลดิจิทัลทำหน้าที่เป็นผู้ให้บริการระบบออกเอกสารรับรองดิจิทัล (VC) ผ่าน GDX สำหรับการออกเอกสารรับรองดิจิทัล (VC) จากชุดข้อมูลภาครัฐ และ Universal Verifier ผ่าน “ทางรัฐ” เพื่อให้ผู้ใช้แอปพลิเคชันทุกคนสามารถตรวจสอบเอกสารรับรองดิจิทัล (VC) ที่ออกภายใต้กรอบการสร้างความน่าเชื่อถือของเอกสารรับรองและเอกสารสำแดง รวมถึงชุดเครื่องมือพัฒนาซอฟต์แวร์สำหรับการตรวจสอบ (Universal Verifier SDK) ซึ่งจะช่วยลดภาระของหน่วยงานภาครัฐที่บูรณาการกับแอปพลิเคชัน “ทางรัฐ” ในการออกเอกสารรับรองดิจิทัล (VC) อย่างมีนัยสำคัญ
- กรมการปกครอง: ออกเอกสารรับรองดิจิทัล (VC) อัตลักษณ์พื้นฐานสำหรับบุคคลธรรมดา โดยอ้างอิงจากข้อมูลฐานทะเบียนราษฎร และสนับสนุนการจัดเก็บและนำไปใช้งานผ่านกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) บนแอปพลิเคชัน “ThaID” ซึ่งทำหน้าที่เป็นรากฐานของความเชื่อถือสำหรับข้อมูลประจำตัวของบุคคลธรรมดา
- กรมพัฒนาธุรกิจการค้า: ออกเอกสารรับรองดิจิทัลของข้อมูลนิติบุคคล (VC) ที่มีระดับความน่าเชื่อถือสูงสำหรับบริษัทจดทะเบียน รวมถึงสถานะทางกฎหมาย ข้อมูลการจดทะเบียน และผู้แทนที่ได้รับมอบอำนาจ

- กรมสรรพากร: ขยายขอบเขตความครอบคลุมเอกสารรับรองดิจิทัล (VC) ของข้อมูลนิติบุคคล และการออกเอกสารรับรองดิจิทัล (VC) ที่เกี่ยวกับเศรษฐกิจและภาษี รวมถึงสำหรับ SME และประเภทนิติบุคคลอื่นที่ไม่ได้จดทะเบียนกับกรมพัฒนาธุรกิจการค้า

ตารางต่อไปนี้ อธิบายเพิ่มเติมถึงบทบาทที่หน่วยงานต่าง ๆ จะรับผิดชอบตามระยะที่ 1-3

ความรับผิดชอบ	**ระยะที่ 1 (พ.ศ. 2569) : จัดทำกรอบอำนาจทางกฎหมายและระบบธรรมาภิบาลที่สามารถบังคับใช้ได้**	**ระยะที่ 2 (พ.ศ. 2570) : กำหนดให้มีการออกเอกสารรับรองดิจิทัล (VC) ให้เป็นที่ยอมรับในภาครัฐและภาคส่วนที่อยู่ภายใต้การกำกับดูแล และใช้งานจริง**	**ระยะที่ 3 (พ.ศ. 2571-2572) : ดำเนินการขยายการใช้งานสู่ระดับประเทศ และส่งเสริมให้มีการรับรองซึ่งกันและกันในระดับอาเซียน**
ผู้ออกเอกสารรับรองดิจิทัลขั้นพื้นฐาน	- กรมการปกครอง - กรมพัฒนาธุรกิจการค้า - กรมสรรพากร - กรมการขนส่งทางบก		
การคัดเลือกกรณีการใช้งานที่มีความสำคัญ	- สพธอ. - สำนักงาน ก.พ.ร. สำนักงานพัฒนารัฐบาลดิจิทัล		
การบำรุงรักษาโครงสร้างข้อมูลเอกสารรับรอง	- สพธอ. - สำนักงานพัฒนารัฐบาลดิจิทัล	- สพธอ. - สำนักงานพัฒนารัฐบาลดิจิทัล	- สพธอ. - สำนักงานพัฒนารัฐบาลดิจิทัล
ผู้ออกเอกสารรับรองดิจิทัลรายอื่น		- กระทรวงสาธารณสุข - กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม	- กระทรวงสาธารณสุข - กรมการขนส่งทางบก - กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม และอื่น ๆ ตามที่จะกำหนดต่อไป

ความรับผิดชอบ	ระยะที่ 1 (พ.ศ. 2569) : จัดทำกรอบอำนาจทางกฎหมายและระบบธรรมาภิบาลที่สามารถบังคับใช้ได้	ระยะที่ 2 (พ.ศ. 2570) : กำหนดให้มีการออกเอกสารรับรองดิจิทัล (VC) ให้เป็นที่ยอมรับในภาครัฐและภาคส่วนที่อยู่ภายใต้การกำกับดูแล และใช้งานจริง	ระยะที่ 3 (พ.ศ. 2571-2572) : ดำเนินการขยายการใช้งานสู่ระดับประเทศ และส่งเสริมให้มีการรับรองซึ่งกันและกันในระดับอาเซียน
ผู้ให้บริการ (ผู้ตรวจสอบรับรองดิจิทัล)	- กรมการปกครอง - สำนักงานพัฒนารัฐบาลดิจิทัล	กรณีการใช้งานที่มีความสำคัญ	- กรณีการใช้งานที่มีความสำคัญ - หน่วยงานภาครัฐอื่น ๆ - ธนาคาร (สำหรับ KYC) - ภาคเอกชน
ผู้ให้บริการที่สนับสนุนโครงสร้างพื้นฐาน	- สำนักงานพัฒนารัฐบาลดิจิทัล – ผู้ให้บริการระบบออกเอกสารรับรองดิจิทัลผ่าน ข้อมูลกลางภาครัฐ (GDX) - สำนักงานพัฒนารัฐบาลดิจิทัล – Universal Verifier, ทางรัฐ - สำนักงานพัฒนารัฐบาลดิจิทัล/สพธอ. – โครงสร้างพื้นฐานความเชื่อถือร่วม	- สำนักงานพัฒนารัฐบาลดิจิทัล – ผู้ให้บริการระบบออกเอกสารรับรองดิจิทัลผ่าน ข้อมูลกลางภาครัฐ (GDX) - สำนักงานพัฒนารัฐบาลดิจิทัล – Universal Verifier, ทางรัฐ - สำนักงานพัฒนารัฐบาลดิจิทัล/สพธอ. – โครงสร้างพื้นฐานความเชื่อถือร่วม	- สำนักงานพัฒนารัฐบาลดิจิทัล – ผู้ให้บริการระบบออกเอกสารรับรองดิจิทัลผ่าน ข้อมูลกลางภาครัฐ (GDX) - สำนักงานพัฒนารัฐบาลดิจิทัล – Universal Verifier, ทางรัฐ - สำนักงานพัฒนารัฐบาลดิจิทัล/สพธอ. – โครงสร้างพื้นฐานความเชื่อถือร่วม

ความรับผิดชอบ	ระยะที่ 1 (พ.ศ. 2569) : จัดทำกรอบอำนาจทางกฎหมายและระบบธรรมาภิบาลที่สามารถบังคับใช้ได้	ระยะที่ 2 (พ.ศ. 2570) : กำหนดให้มีการออกเอกสารรับรองดิจิทัล (VC) ให้เป็นที่ยอมรับในภาครัฐและภาคส่วนที่อยู่ภายใต้การกำกับดูแล และใช้งานจริง	ระยะที่ 3 (พ.ศ. 2571-2572) : ดำเนินการขยายการใช้งานสู่ระดับประเทศ และส่งเสริมให้มีการรับรองซึ่งกันและกันในระดับอาเซียน
การกำกับดูแล	- คณะรัฐมนตรี – มติคณะรัฐมนตรี (เสนอโดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม) - สพธอ. - ธนาคารแห่งประเทศไทย – การยอมรับในระดับภาคส่วน	- สพธอ. - ธนาคารแห่งประเทศไทย (ภาคการเงิน) - สำนักงาน ก.พ.ร. (ภาครัฐ) - กระทรวงสาธารณสุข (ภาคสุขภาพ)	- สพธอ. - ธนาคารแห่งประเทศไทย (ภาคการเงิน) -สำนักงาน ก.พ.ร. (ภาครัฐ) - กระทรวงสาธารณสุข (ภาคสุขภาพ) และอื่น ๆ ตามที่จะกำหนดต่อไป
การสร้างความตระหนักรู้ของประชาชน	- สำนักงาน ก.พ.ร. - สพธอ. - หน่วยงานกำกับดูแลในแต่ละภาคส่วน	- สำนักงาน ก.พ.ร. - สพธอ. - หน่วยงานกำกับดูแลในแต่ละภาคส่วน	- สำนักงาน ก.พ.ร. - สพธอ. - หน่วยงานกำกับดูแลในแต่ละภาคส่วน
การสร้างความตระหนักรู้ของภาครัฐ	- สำนักงาน ก.พ.ร. - สพธอ.	- สำนักงาน ก.พ.ร. - สพธอ.	- สำนักงาน ก.พ.ร. - สพธอ.
กลไกการเยียวยา (Redress Mechanism)	- สำนักงาน ก.พ.ร. - สพธอ.	- สำนักงาน ก.พ.ร. - สพธอ.	- สำนักงาน ก.พ.ร. - สพธอ.

7 ประมาณการงบประมาณที่ต้องใช้จ่ายสำหรับการดำเนินงานระยะที่ 2 (พ.ศ. 2570)

ความต้องการด้านงบประมาณสำหรับระยะที่ 2 นั้นถือว่าไม่สูงมากเมื่อเทียบกับผลลัพธ์ที่จะเกิดขึ้น สามารถดำเนินการได้ด้วยการพัฒนาโครงสร้างพื้นฐานร่วมกัน และการลงทุนในระดับหน่วยงานที่มีเป้าหมายชัดเจน

ปัจจัยที่เป็นต้นทุนการดำเนินงานที่สำคัญ ได้แก่ การพัฒนาขีดความสามารถในการออกเอกสารรับรองดิจิทัล (VC) ระดับประเทศ การบูรณาการแหล่งข้อมูลในหน่วยงานที่มีความสำคัญ และการขับเคลื่อนระบบนิเวศ ซึ่งรวมถึงการบูรณาการเครื่องมือทดสอบความสอดคล้องของเอกสารรับรองดิจิทัล (Conformance test tool)การสร้างความตระหนักรู้ และการพัฒนาศักยภาพของหน่วยงาน ทั้งนี้ แนวทางการออกเอกสารรับรองดิจิทัล (VC) แบบรวมศูนย์ โดยให้หน่วยงานขนาดเล็กสามารถใช้แพลตฟอร์มกลางเพื่อปรับเปลี่ยนข้อมูลและเอกสารให้เป็นเอกสารรับรองดิจิทัล (VC) ที่สอดคล้องมาตรฐานร่วมกัน ซึ่งจะลดความซ้ำซ้อนและต้นทุนโดยรวมได้อย่างมีนัยสำคัญ ดังนั้น ในระยะการดำเนินงานที่ 2 นี้ จะใช้งบประมาณอยู่ที่จำนวน 430 - 1.1 พันล้านบาท สามารถจัดสรรให้ทยอยจ่ายในช่วง 1–2 ปีงบประมาณ อย่างไรก็ตาม **จำนวนเงินดังกล่าวครอบคลุมแกนหลักของระบบนิเวศและผู้ออกเอกสารจำนวนจำกัด โดยไม่ได้ครอบคลุมต้นทุนทั้งหมดของระบบนิเวศ โดยเฉพาะในกรณีที่มีหน่วยงานผู้ออกเอกสารจำนวนมาก** สำหรับหน่วยงานผู้ออกเอกสารเพิ่มเติมส่วนใหญ่ ต้นทุนการดำเนินงานคาดว่าจะอยู่ในระดับน้อยมาก โดยเฉพาะเมื่อมีการใช้โครงสร้างพื้นฐานและบริการออกเอกสารรับรองดิจิทัล (VC) ร่วมกัน และเน้นไปที่การบูรณาการเครื่องมือที่มีอยู่ การปรับมาตรฐานข้อมูล และการปรับกระบวนการเล็กน้อย ซึ่งโดยทั่วไปสามารถจะอยู่ภายในงบประมาณประจำปีของหน่วยงาน

ส่วนประกอบ	รายละเอียด	งบประมาณ (บาท)
โครงสร้างพื้นฐานร่วม (ใช้งานร่วมกันได้ที่ระบบกลาง)	แพลตฟอร์มออกเอกสารรับรองดิจิทัลกลาง ที่บูรณาการเข้ากับระบบกับศูนย์แลกเปลี่ยนข้อมูลกลางภาครัฐ (GDX) การบูรณาการ trust registry การทดสอบความสอดคล้องและเครื่องมือสำหรับนักพัฒนา	180 - 360 ล้านบาท
การพัฒนาหรือปรับปรุงกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) [12]	การจัดเก็บเอกสารรับรองดิจิทัล การสำแดงเอกสาร กระบวนการให้ความยินยอม ส่วนติดต่อสำหรับผู้ตรวจสอบ และการเพิ่มความมั่นคงปลอดภัย	40 - 120 ล้านบาท
กรมการปกครอง (เอกสารรับรองดิจิทัลข้อมูลทะเบียนราษฎร์)	การออกเอกสารรับรองดิจิทัล ID หลัก การบูรณาการกับทะเบียนราษฎร์และ ThaID โดยมีข้อกำหนดด้านการความน่าเชื่อถือสูงสุดและการรองรับการใช้งานในวงกว้าง	60 - 140 ล้านบาท

[12] การพัฒนาหรือปรับปรุงกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ที่กำหนดสูงสุด 2 กระเป๋าสำหรับภาคประชาชน และสูงสุด 2 กระเป๋าสำหรับภาคธุรกิจ พร้อมทั้งการสนับสนุนการรับรองกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) เพิ่มเติมของภาคเอกชน โดยค่าใช้จ่ายครอบคลุมการจัดเก็บเอกสารรับรองดิจิทัล (VC) การสำแดงเอกสารรับรองดิจิทัล กระบวนการยินยอม อินเทอร์เฟซผู้ตรวจสอบ และการเพิ่มความปลอดภัย เป็นต้น

ส่วนประกอบ	รายละเอียด	งบประมาณ (บาท)
หน่วยงานออกเอกสารรับรองดิจิทัลที่มีความสำคัญอื่น ๆ (4-5 หน่วยงาน)	การบูรณาการกับฐานข้อมูล การสร้างมาตรฐานข้อมูล การออกแบบกระบวนการใหม่ ความปลอดภัย และการปฏิบัติตามข้อกำหนด	140 - 360 ล้านบาท (ยอดรวม)
การสร้างระบบนิเวศ	การสนับสนุนการบูรณาการสำหรับผู้ตรวจสอบ การรณรงค์สร้างความตระหนักรู้ ความช่วยเหลือทางเทคนิคและการพัฒนาศักยภาพของหน่วยงาน	70 - 180 ล้านบาท
	วงเงินรวมโดยประมาณ	**490 ล้านบาท - 1.16 พันล้านบาท**

การประมาณการงบประมาณข้างต้น เป็นเพียงข้อมูลเบื้องต้นและมีวัตถุประสงค์เพื่อแสดงกรอบความต้องการทรัพยากรในภาพรวมมากกว่าการระบุตัวเลขงบประมาณที่แน่ชัด ต้นทุนที่แท้จริงจะขึ้นอยู่กับปัจจัยหลายประการ รวมถึงขอบเขตขั้นสุดท้ายของการใช้งาน ความสมบูรณ์ คุณภาพของระบบที่หน่วยงานมีอยู่ แนวทางการจัดซื้อจัดจ้าง และระดับการใช้โครงสร้างพื้นฐานร่วมกันเมื่อเทียบกับการพัฒนาเฉพาะของแต่ละหน่วยงาน ด้วยเหตุนี้ การประมาณการงบประมาณ จึงควรได้รับการปรับปรุงในระหว่างดำเนินการในระยะที่ 1 ผ่านการประเมินทางเทคนิคเชิงลึก การวางแผนการดำเนินงาน การมีส่วนร่วมกับหน่วยงานหลัก และผู้ให้บริการเทคโนโลยี รวมถึงการตรวจสอบความต้องการการบูรณาการระบบของแต่ละหน่วยงาน ความพร้อมของข้อมูล และข้อกำหนดเชิงปฏิบัติการ

ภาคผนวก ก – ภูมิหลัง

ก.1 ปัจจัยขับเคลื่อนเพื่อการเปลี่ยนแปลง

มีหลายระบบที่ไม่สามารถทำงานร่วมกันได้หรือไม่ปฏิบัติตามมาตรฐานที่ได้รับการยอมรับ ปัจจุบันมีกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ของรัฐบาลและการใช้งานระบบดิจิทัลไอดีที่มีความหลากหลาย อย่างไรก็ดี เอกสารรับรองดิจิทัล (VC) ไม่สามารถโอนย้ายจากระบบหนึ่งไปยังอีกระบบหนึ่งได้ ในเชิงเทคนิคระบบเหล่านี้ทำงานร่วมกันได้ไม่ดีเท่าที่ควร ส่งผลให้ประชาชนต้องใช้หลายระบบ

การฉ้อโกงและการหลอกลวงยังคงสร้างความเดือดร้อนให้กับประชาชนและภาครัฐ การฉ้อโกง การหลอกลวง และอาชญากรรมทางไซเบอร์ยังคงเป็นภัยต่อประชาชนและภาคธุรกิจของไทย ในช่วงปี พ.ศ. 2566 และ 6 เดือนแรกของปี พ.ศ. 2567 การโจมตีออนไลน์ได้สร้างความสูญเสียทางการเงินโดยรวม ประมาณ 45,000 ล้านบาท อีกทั้งการโจรกรรมข้อมูลอัตลักษณ์ที่ใช้เทคโนโลยีปัญญาประดิษฐ์ ส่งผลให้ความเสี่ยงนี้ทวีความรุนแรงมากขึ้น

โอกาสที่สูญเสียไป ระบบดิจิทัลไอดีและเอกสารรับรองดิจิทัล (VC) ที่เชื่อถือได้ถูกใช้งานน้อย เนื่องจากขาดแรงจูงใจในการใช้งาน แต่ในอีกด้านหนึ่ง ยังคงใช้สำเนาเอกสารบัตรประจำตัวประชาชนแบบกระดาษซึ่งเป็นกระบวนการที่ไม่มีประสิทธิภาพและอาจไม่ปลอดภัย ทั้งที่การใช้เอกสารรับรองดิจิทัล (VC) สามารถช่วยประหยัดเวลาและทรัพยากรได้ ดังนั้น จึงควรระบุกรณีการใช้งานที่มีความสำคัญเพื่อให้การใช้งานเป็นประโยชน์มากขึ้น เช่น

- ***การอำนวยความสะดวกทางธุรกิจ*** – การทำให้กระบวนการกำกับดูแลสำหรับการจัดตั้งและดำเนินธุรกิจง่ายขึ้น โดยไม่ลดระดับความน่าเชื่อถือ
- ***การปฏิบัติตามกฎระเบียบ*** – การจัดให้มีวิธีการที่เชื่อถือได้และปลอดภัยสำหรับประชาชนในการพิสูจน์อายุ ตัวอย่างเช่น การสนับสนุนการขายสินค้าที่จำกัดอายุทางออนไลน์
- ***การสาธารณสุข*** – การสนับสนุนการโอนย้ายประวัติสุขภาพเมื่อมีความจำเป็นต้องย้ายการรับบริการจากสถานพยาบาลแห่งหนึ่งไปยังอีกแห่งหนึ่ง โดยการรวมศูนย์ประวัติข้อมูลไว้ที่ตัวผู้ป่วยแทนการมีระบบของรายโรงพยาบาลที่ไม่เชื่อมโยงกันหรือแยกออกจากกัน
- ***ความร่วมมือระดับภูมิภาค*** – อำนวยความสะดวกให้ประชาชนสามารถพิสูจน์สิทธิการขับขี่ในประเทศอาเซียนอื่น ๆ การสมัครงานหรือเข้าศึกษาในระดับอุดมศึกษา โดยใช้เอกสารรับรองดิจิทัลด้านการศึกษา (VC) รวมถึงการเข้าร่วมการค้าข้ามพรมแดนในรูปแบบดิจิทัล

การแข่งขันระดับภูมิภาคและนโยบายอาเซียนบ่งชี้ถึงความร่วมมือดิจิทัลที่เข้มแข็งยิ่งขึ้น การจัดเตรียมเครื่องมือเพื่อให้ธุรกิจไทยสามารถแข่งขันได้ทั้งในระดับภูมิภาคและระดับนานาชาติเป็นสิ่งสำคัญต่อการเติบโตทางการค้าในอนาคต กรณีการใช้งานข้ามพรมแดนจะเปิดโอกาสให้ประชาชนไทยสามารถทำงาน ศึกษา และเดินทางได้อย่างเสรีมากขึ้นในภูมิภาค

กรอบการสร้างความน่าเชื่อถือของเอกสารรับรองและเอกสารสำแดง มีความสำคัญสำหรับความร่วมมือระหว่างประเทศ แนวโน้มระหว่างประเทศและการใช้เอกสารรับรองดิจิทัล (VC) ที่ตรวจสอบได้ซึ่งหลายประเทศกำลังตั้งคาดหวังไว้ เช่น สหภาพยุโรป บราซิล เกาหลี ภูฏาน และสหรัฐอเมริกา และกรอบความน่าเชื่อถือสำหรับการค้าและข้อมูลนิติบุคคลระหว่างประเทศก็กำลังมีบทบาทมากขึ้น เช่น สหภาพแอฟริกา สหภาพยุโรป และในอนาคตอาจรวมถึงอาเซียนด้วย

ก.2 ความจำเป็นในการกำกับดูแลที่เข้มแข็งและความรับผิดชอบที่ชัดเจน

เพื่อรักษาความเชื่อมั่นในระบบนิเวศเอกสารรับรองดิจิทัล (VC) จำเป็นต้องมีระบบการกำกับดูแลที่เข้มแข็ง เพื่อให้มั่นใจว่ามาตรฐาน นโยบาย และขั้นตอนถูกนำไปปฏิบัติและบำรุงรักษาอย่างถูกต้อง ผ่านกิจกรรมต่าง ๆ เช่น การกำกับดูแล การตรวจสอบการปฏิบัติตามข้อกำหนด การรับรองคุณภาพหรือการรับรองมาตรฐาน การบังคับใช้ และการระงับข้อพิพาท

ควรจัดตั้ง**กรอบแนวทางการขับเคลื่อนเพื่อพัฒนาระบบนิเวศของการใช้เอกสารรับรองดิจิทัลที่ตรวจสอบได้** ที่กำหนดบทบาทและความรับผิดชอบของหน่วยงานที่เข้าร่วม กำหนด สภาพแวดล้อมทางกฎหมายที่กรอบการสร้างความน่าเชื่อถือของเอกสารรับรองและเอกสารสำแดงดำเนินการอยู่ และข้อกำหนดเฉพาะและข้อกำหนดทางเทคนิคที่ใช้กับหน่วยงานและองค์ประกอบเชิงหน้าที่ของระบบนิเวศความเชื่อถือ ซึ่งอาจรวมถึงข้อกำหนดด้านการรับรองหรือระบบการประเมินทางเทคนิคที่บางหน่วยงานต้องปฏิบัติตาม เพื่อให้สามารถดำเนินการและได้รับความเชื่อถือจากหน่วยงานอื่นในระบบนิเวศ

หน่วยงาน	ความรับผิดชอบหลัก
หน่วยงานกำกับดูแลกรอบการสร้างความน่าเชื่อถือ (Trust Framework Authority)	หน่วยงานที่กำหนดและบำรุงรักษากรอบแนวทางการขับเคลื่อนฯ รวมถึงการกำหนดขอบเขต กฎเกณฑ์การเข้าร่วม ระดับความเชื่อมั่น เกณฑ์การรับรอง ข้อกำหนดด้านการทำงานร่วมกัน กฎเกณฑ์ความรับผิดชอบ และมาตรฐานที่เกี่ยวข้อง หน่วยงานดังกล่าวมีหน้าที่กำหนดนโยบาย กฎหมาย และข้อกำหนดภายใต้ซึ่งหน่วยงานผู้ออกเอกสาร ผู้ให้บริการกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ผู้ตรวจสอบ และองค์กรรับรอง สามารถดำเนินงานได้อย่างถูกต้องตามมาตรฐาน โดยพิจารณาจากบทบาทและหน้าที่ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.)ตามพระราชบัญญัติสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2562 **จึงขอเสนอแนะให้** สพธอ. **รับบทบาทเป็นหน่วยงานกำกับดูแลกรอบการสร้างความน่าเชื่อถือของเอกสารรับรองและเอกสารสำแดง**
องค์กรรับรองที่เชื่อถือได้	หน่วยงานดังกล่าวมีหน้าที่ในการรับรองหรือให้การรับรองแก่หน่วยงานอื่นเพื่อแสดงให้เห็นว่าหน่วยงานนั้นเป็นผู้ออกเอกสารรับรองที่เชื่อถือได้ใน

หน่วยงาน	ความรับผิดชอบหลัก
	บางประเภทของเอกสาร เช่น กระทรวงศึกษาธิการอาจทำหน้าที่รับรองมหาวิทยาลัยแห่งหนึ่งว่าได้รับอนุญาตให้ออกใบแสดงผลการศึกษาทางการศึกษาในรูปแบบเอกสารรับรองดิจิทัล (VC Transcript) ได้อย่างถูกต้องตามมาตรฐาน
ผู้ตรวจประเมิน / หน่วยงานประเมินความสอดคล้อง	หน่วยงานอิสระที่รับผิดชอบในการประเมินว่าผู้ให้บริการกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ผู้ออกเอกสาร ผู้ตรวจสอบ และองค์กรรับรองได้ปฏิบัติตามข้อกำหนดของกรอบการสร้างความน่าเชื่อถือ ผู้ตรวจประเมินดำเนินการประเมินความสอดคล้องตามเกณฑ์และมาตรฐาน และส่งรายงานประกันคุณภาพให้กับหน่วยงานกำกับดูแล ผู้ตรวจประเมินต้องได้รับการรับรองภายใต้การจัดการรับรองที่เป็นที่ยอมรับและดำเนินการอย่างอิสระจากหน่วยงานที่ตนประเมิน สพธอ. ทำหน้าที่เป็นหน่วยงานรับรองหลักในการตรวจสอบความน่าเชื่อถือขององค์กรรับรอง ผู้ให้บริการกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ผู้ออกเอกสาร และผู้ตรวจสอบ โดยในอนาคตสามารถนำผู้ตรวจประเมินจากภาคเอกชนเข้ามาเพิ่มเติมได้
หน่วยงานกำกับดูแล	หน่วยงานกำกับดูแลรับผิดชอบในการกำกับดูแลการทำงานที่เหมาะสมของระบบนิเวศเอกสารรับรองดิจิทัล (VC) และบังคับใช้การปฏิบัติตามกรอบการสร้างความน่าเชื่อถือ รวมถึงการติดตามผู้เข้าร่วมที่ได้รับการรับรอง การทบทวนผลการตรวจสอบ การจัดการการไม่ปฏิบัติตาม การใช้มาตรการแก้ไขหรือการลงโทษ และการประสานงานกลไกการระงับข้อพิพาทและการเยียวยา โดยพิจารณาจากบทบาทและหน้าที่ของ สพธอ. ตามพระราชบัญญัติสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2562 **จึงขอเสนอแนะให้** สพธอ. **รับบทบาทหน่วยงานกำกับดูแล**

ก.3 การสร้างโครงสร้างพื้นฐานดิจิทัลของประเทศที่สามารถขยายการใช้งานและมีความยืดหยุ่น

อัตลักษณ์ดิจิทัลและโครงสร้างพื้นฐานด้านความเชื่อถือที่จำเป็นต่อการออกและการตรวจสอบเอกสารรับรองดิจิทัล (VC) เมื่อจัดตั้งขึ้นแล้ว จะกลายเป็นโครงสร้างพื้นฐานสำคัญระดับประเทศ หากระบบหยุดทำงานหรือสูญเสียความน่าเชื่อถือ บริการทั้งหมดที่พึ่งพาระบบดังกล่าวก็จะหมดความเชื่อถือตามไปด้วย

การนำแนวทางแบบกระจายศูนย์มาใช้ในการออกและการใช้เอกสารรับรองดิจิทัล (VC) จะช่วยลดการพึ่งพาการใช้งานข้อมูลภาครัฐแบบรวมศูนย์ขนาดใหญ่ เพิ่มการควบคุมข้อมูลส่วนบุคคลให้แก่ประชาชน ลดความจำเป็นที่ผู้ให้บริการที่ต้องตรวจสอบเอกสารรับรองดิจิทัล (VC) ต้องเชื่อมต่อโดยตรงกับระบบของภาครัฐ

ผู้ออกเอกสารจำเป็นต้องจัดทำข้อมูลที่เชื่อถือได้ มีความปลอดภัย และเป็นที่ได้รับการยอมรับ และเมื่อออกเอกสารรับรองดิจิทัล (VC) ผู้ออกเอกสารจำเป็นต้องสร้างความมั่นใจว่าเอกสารรับรองดิจิทัล (VC) เหล่านั้นได้รับการลงนามด้วยการเข้ารหัสลับ เพื่อยืนยันว่าเอกสารไม่ได้ถูกแก้ไขดัดแปลง และเพื่อพิจารณาว่าเอกสารนั้นถูกสร้างขึ้นโดยหน่วยงานที่เป็นผู้ออกเอกสารจริง นอกจากนี้ ผู้ตรวจสอบเอกสารจำเป็นต้องรู้ว่าผู้ออกเอกสารรายใดน่าเชื่อถือ และจำเป็นต้องเข้าถึงข้อมูลที่สามารถอธิบายประเภทข้อมูลที่ร้องขอจากผู้ถือเอกสารที่ออกภายใต้ระบบนิเวศ ผู้ตรวจสอบเอกสารจำเป็นต้องเข้าถึงเครื่องมือที่ช่วยตรวจสอบความถูกต้องและความสมบูรณ์ของเอกสารรับรองดิจิทัล (VC) เพื่อให้สามารถระบุได้ว่าหน่วยงานใดที่เป็นผู้ออกเอกสารนั้น

ดังนั้น โครงสร้างพื้นฐานความน่าเชื่อถือไม่ได้ประกอบด้วยกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) และผู้ออกเอกสารเท่านั้น แต่เป็นหน่วยงานหรือผู้ที่เกี่ยวข้องหลักและหน่วยงานสนับสนุนทั้งหมดในระบบนิเวศ ตัวอย่างเช่น

หน่วยงาน	หน้าที่ / ความรับผิดชอบ
ผู้ใช้งานกระเป๋าเอกสารดิจิทัล (Digital Document Wallet)	ประชาชนและผู้พำนักถาวรซึ่งมีการควบคุมกระเป๋าเอกสารดิจิทัลที่ได้รับการรับรอง มีหน้าที่รับผิดชอบในการแบ่งปันเอกสารรับรองดิจิทัล (VC) ที่อยู่ในกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ดังกล่าวแก่หน่วยงานที่ต้องการข้อมูล
ผู้ให้บริการกระเป๋าเอกสารดิจิทัล (Digital Document Wallet)	องค์กรที่ได้รับมอบหมายหรือได้รับการยอมรับจากภาครัฐให้พัฒนาและจัดหาโซลูชันกระเป๋าเอกสารดิจิทัล (เช่น แอปพลิเคชัน) และผู้ให้บริการกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) มีหน้าที่ในการจัดเก็บป้องกัน และนำเสนอเอกสารรับรองดิจิทัล (VC) อย่างปลอดภัย รวมถึงการจัดการกุญแจและการผูกโยงกับผู้ถือเอกสาร ทั้งนี้ ต้องเป็นไปตามข้อกำหนดของกรอบแนวทางการขับเคลื่อนฯ หมายเหตุ: กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) อาจต้องได้รับการรับรองหากมีการกำหนดไว้ในกรอบแนวทางการขับเคลื่อนฯ

หน่วยงาน	หน้าที่ / ความรับผิดชอบ
ผู้ออกเอกสารรับรองดิจิทัล (Issuer) ที่เกี่ยวข้องกับข้อมูลอัตลักษณ์ (Identity Credential Provider)	หน่วยงานที่เชื่อถือได้ซึ่งได้รับอนุญาตภายใต้กรอบการสร้างความน่าเชื่อถือสำหรับการออกเอกสารรับรองดิจิทัล (VC) รับผิดชอบในการ: ● ยืนยันตัวตนของผู้ใช้ที่ร้องขอเอกสารรับรองดิจิทัล (VC) ● ออกเอกสารรับรองดิจิทัล (VC) ให้กับกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) (ของผู้ใช้บริการนั้น) และ ● การจัดให้มีข้อมูลสำหรับหน่วยงานที่อาศัยข้อมูล เพื่อใช้ในการตรวจสอบความถูกต้องของเอกสารแสดงตน โดยต้องดำเนินการในลักษณะที่คุ้มครองความเป็นส่วนตัว
ผู้รับขึ้นทะเบียนหน่วยงาน (Entity Registrar)	ช่วยให้หน่วยงานอื่นที่มีส่วนร่วมในระบบนิเวศสามารถลงทะเบียนอย่างเป็นทางการ และทำให้ข้อมูลเกี่ยวกับหน่วยงานเหล่านั้นพร้อมใช้งานทางออนไลน์ในรูปแบบที่มนุษย์และเครื่องอ่านได้ หน่วยงานที่ลงทะเบียนจะถูกจัดอยู่ในลำดับความเชื่อถือที่เกี่ยวข้องภายใต้กรอบแนวทางการขับเคลื่อนฯ
ผู้ขึ้นทะเบียนหน่วยงานที่น่าเชื่อถือในระบบนิเวศ VC (Trusted List Provider)	หน่วยงานที่รับผิดชอบในการบำรุงรักษา จัดการ และเผยแพร่รายการความเชื่อถือของหน่วยงาน เช่น ผู้ให้บริการเอกสารรับรองดิจิทัล (VC) ผู้ให้บริการกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สถานะของหน่วยงานในฐานะหน่วยงาน "ที่น่าเชื่อถือ" สามารถตรวจสอบได้โดยการตรวจสอบว่าหน่วยงานนั้นปรากฏอยู่ในรายการความเชื่อถือหรือไม่
ผู้ออกเอกสารรับรอง (Issuers of Credentials)	หน่วยงานที่ได้รับอนุญาตให้ออกเอกสารรับรองดิจิทัล (VC) ให้กับผู้ใช้บริการที่ระบุตัวตนแล้ว ภายใต้กฎระเบียบของกรอบแนวทางการขับเคลื่อนฯผู้ออกเอกสาร (VC) อาจใช้แหล่งข้อมูลทางการจากภาครัฐหรือนำข้อมูลจากแหล่งอื่นที่เชื่อถือภายใต้ข้อตกลงได้เช่นเดียวกัน
ทะเบียน (แหล่งข้อมูลทางการ) หรือ Registries (Authoritative Sources)	คลังข้อมูลหรือระบบสาธารณะหรือเอกชนที่ได้รับการรับรองหรือกำหนดโดยกฎหมาย ซึ่งมีข้อมูลเกี่ยวกับบุคคลหรือหน่วยงาน เช่น สถานะทางแพ่ง องค์ประกอบครอบครัว สัญชาติ คุณสมบัติทางการศึกษา/การฝึกอบรม ใบอนุญาตวิชาชีพ ใบอนุญาตสาธารณะ ข้อมูลการจดทะเบียนธุรกิจ
ผู้อาศัยการยืนยันตัวตน (บริการ) หรือ Relying Parties	ผู้ให้บริการ (ทั้งในรูปแบบบุคคลหรือผ่านบริการดิจิทัล) ซึ่งร้องขอข้อมูลคุณลักษณะเฉพาะที่บรรจุอยู่ในเอกสารรับรองดิจิทัล (VC) 1 รายการหรือมากกว่าที่ผู้ถือเอกสารแบ่งปัน (ภายใต้ความยินยอมที่บังคับใช้) จากกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ที่ได้รับการรับรอง หน่วยงานที่อาศัยข้อมูลมีหน้าที่รับผิดชอบในการตรวจสอบความถูกต้อง ความ

หน่วยงาน	หน้าที่ / ความรับผิดชอบ
	สมบูรณ์ และสถานะความน่าเชื่อถือของผู้ออกเอกสาร และการเชื่อมโยงกับผู้ถือเอกสาร โดยใช้โครงสร้างพื้นฐานด้านความเชื่อถือ
หน่วยงานกำกับดูแล (Supervisory Body)	หน่วยงานกำกับดูแลการทำงานที่เหมาะสมของระบบนิเวศเอกสารรับรองดิจิทัล (VC) และการบังคับใช้การปฏิบัติตามกรอบแนวทางการขับเคลื่อนฯ รวมถึงการติดตามผู้เข้าร่วมที่ได้รับการรับรอง การทบทวนผลการตรวจสอบ การจัดการการไม่ปฏิบัติตาม การใช้มาตรการแก้ไขหรือการลงโทษ และการประสานงานกลไกการระงับข้อพิพาทและการเยียวยา
ผู้ให้บริการ Attribute Schema	การเผยแพร่แบบแผนคุณลักษณะที่อธิบายโครงสร้างของเอกสารรับรองดิจิทัล (VC) และวิธีการที่หน่วยงานที่อาศัยข้อมูลสามารถนำไปใช้

ก.4 ขอบเขตของกรอบการสร้างความน่าเชื่อถือของเอกสารรับรองและเอกสารสำแดง

ข้อกำหนดด้านธรรมาภิบาลและโครงสร้างพื้นฐานดิจิทัลแห่งชาติที่อ้างอิงจากการดำเนินการระบบนิเวศของเอกสารรับรองดิจิทัล (VC) ที่อธิบายไว้ในส่วนก่อนหน้า แสดงให้เห็นถึงความจำเป็นในการมีกรอบการสร้างความน่าเชื่อถือที่ครอบคลุม ซึ่งกรอบดังกล่าวมีบทบาทในการสร้างความเชื่อถือระหว่างผู้มีส่วนเกี่ยวข้องในระบบนิเวศ โดยการกำหนดกฎเกณฑ์และการจัดการด้านธรรมาภิบาลที่ทุกฝ่ายตกลงปฏิบัติตาม

เพื่ออำนวยความสะดวกในการทำงานร่วมกัน หน่วยงานหนึ่งต้องสามารถเชื่อถืออีกหน่วยงานหนึ่งได้ ไม่เพียงแต่ในด้านความถูกต้องของกระบวนการทางเทคนิค แต่ยังรวมถึงแหล่งที่มาของข้อมูลที่ถูกแบ่งปัน (เช่น กระบวนการในการเก็บรวบรวม และการกำหนดบันทึกให้กับบุคคลใดบุคคลหนึ่ง) กรอบการสร้างความน่าเชื่อถือเหล่านี้จึงมุ่งเน้นไปที่การกำกับดูแล กระบวนการ และความรับผิดชอบมากกว่าด้านเทคโนโลยี โดยเทคโนโลยีเป็นเพียงเครื่องมือสนับสนุนเท่านั้น ด้วยเหตุนี้ กรอบการสร้างความน่าเชื่อถือที่เข้มแข็งควรกำหนดข้อกำหนดด้านธุรกิจอย่างชัดเจน (เช่น ขอบเขต บริการที่จัดให้ ข้อกำหนดสำหรับการมีส่วนร่วม รวมถึงเกณฑ์คุณสมบัติ เกณฑ์และกระบวนการประเมิน และพันธกรณีการปฏิบัติตามอย่างต่อเนื่องสำหรับผู้ให้บริการกระเป๋าเอกสารดิจิทัล (Digital Document Wallet)) ด้านเทคนิค (เช่น รูปแบบข้อมูล ส่วนเชื่อมโยง มาตรฐาน) ด้านปฏิบัติการ (เช่น วิธีการตรวจสอบและยืนยันตัวตน การสนับสนุน การสื่อสาร) และด้านกฎหมาย (เช่น ระดับการให้บริการ ความรับผิดชอบ การระงับข้อพิพาท) สำหรับระบบอัตลักษณ์และองค์ประกอบการแบ่งปันข้อมูล

กรอบการสร้างความน่าเชื่อถือของเอกสารรับรองและเอกสารสำแดง ต้องสนับสนุนรูปแบบการเข้าถึงที่ครอบคลุม เพื่อให้มั่นใจว่าการไม่มีอุปกรณ์หรือโทรศัพท์มือถือ การเชื่อมต่ออินเทอร์เน็ต หรือการรู้เท่าทันดิจิทัลจะไม่เป็นอุปสรรคต่อการเข้าถึงบริการสาธารณะ

กรอบการสร้างความน่าเชื่อถือของเอกสารรับรองและเอกสารสำแดง ต้องกำหนดวิธีการที่อำนาจทางกฎหมาย คำสั่ง และการมอบหมายอำนาจจะถูกแสดงและจัดการโดยใช้เอกสารรับรองที่สามารถตรวจสอบได้ รวมถึงกฎเกณฑ์ในการออก มอบหมาย จำกัด และเพิกถอนอำนาจสำหรับนิติบุคคลที่ดำเนินการผ่านบุคคลธรรมดา

บทบาทภายในกรอบการสร้างความน่าเชื่อถือของเอกสารรับรองและเอกสารสำแดง

บทบาทภายในกรอบการสร้างความน่าเชื่อถือครอบคลุมตั้งแต่ผู้บัญญัติกฎหมายไปจนถึงผู้ใช้ปลายทางและบุคคลอื่น ๆ ที่อาจทำหน้าที่ด้านการกำกับดูแล นโยบาย การประกันคุณภาพ และการปฏิบัติงาน ในกรอบความน่าเชื่อถือที่กำหนดไว้ในเอกสารฉบับนี้ บทบาทและความรับผิดชอบระดับสูงที่คาดหวัง มีดังต่อไปนี้

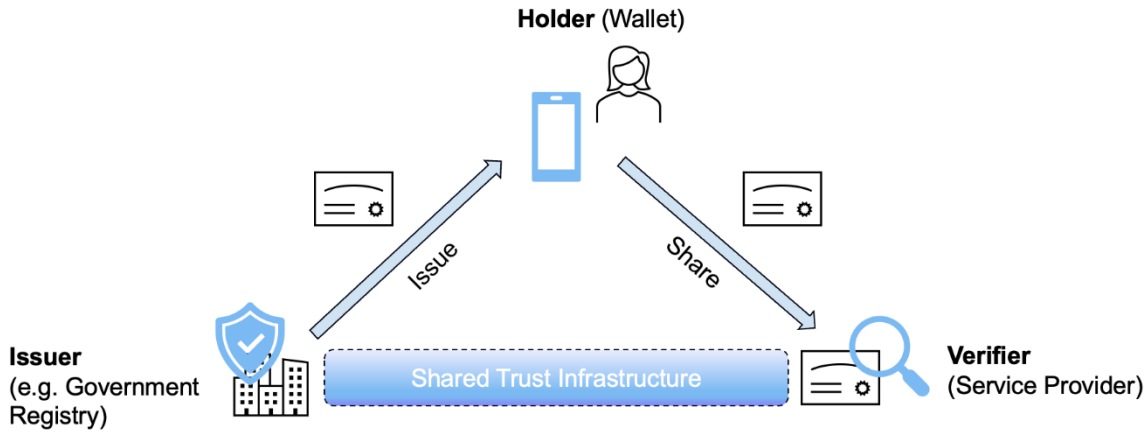
บทบาท / หน่วยงาน	ความรับผิดชอบ
ผู้ดำเนินการกรอบการสร้างความน่าเชื่อถือ (Framework Operator)	• กำหนดและบำรุงรักษากรอบการสร้างความน่าเชื่อถือ รวมถึงกฎสำหรับการมีส่วนร่วม ข้อกำหนดการประกันคุณภาพ และการจัดการกำกับดูแล • กำกับดูแลและบังคับใช้การปฏิบัติตามการสร้างความน่าเชื่อถือ รวมถึงการใช้บทลงโทษหรือการจำกัดสิทธิที่หน่วยงานที่เกี่ยวข้องละเมิดข้อตกลงกรอบแนวทาง
ผู้ออกเอกสารรับรองดิจิทัล (Issuer)	• ออกเอกสารรับรองดิจิทัล (VC) ที่สามารถตรวจสอบได้ตามข้อกำหนดและมาตรฐานของกรอบความน่าเชื่อถือ • รับรองว่าผู้รับเอกสารได้รับการตรวจสอบก่อนการออกเอกสารและข้อมูลที่แบ่งปันในเอกสารรับรองดิจิทัล (VC) เหล่านั้นได้รับการระบุอย่างน่าเชื่อถือแก่หน่วยงานที่ทำการร้องขอ • ใช้กุญแจส่วนตัวที่เชื่อมโยงกับผู้ออกเอกสาร เพื่อวัตถุประสงค์ในการลงนามเอกสารรับรองดิจิทัล (VC) และปรับปรุงโครงสร้างพื้นฐานด้านความเชื่อมั่นที่ใช้ร่วมกัน (ตามที่กำหนดโดยกรอบการสร้างความน่าเชื่อถือ) เพื่อให้สามารถตรวจสอบเอกสารได้เมื่อมีการออกเอกสารแล้ว
ผู้ให้บริการกระเป๋าเอกสารดิจิทัล (Digital Document Wallet)	• รับรองว่าแอปพลิเคชันกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ที่ได้รับการรับรองยังคงปฏิบัติตามข้อกำหนดของกรอบการสร้างความน่าเชื่อถือ • รับรองว่าแอปพลิเคชันกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) พร้อมใช้งาน เข้าถึงได้ และน่าเชื่อถือ
ผู้ให้บริการ (ผู้ตรวจสอบเอกสารรับรองดิจิทัล)	• ปฏิบัติตามหลักการลดการใช้ข้อมูล โดยร้องขอเฉพาะเอกสารรับรองดิจิทัล (VC) ที่จำเป็นสำหรับการให้บริการที่ร้องขอ • ตรวจสอบความสมบูรณ์ของเอกสารรับรองดิจิทัล (VC) ที่ได้รับโดยการตรวจสอบหลักฐานการเข้ารหัสลับที่บรรจุอยู่ในเอกสารรับรองดิจิทัล (VC) เหล่านั้น และความถูกต้องของเอกสารรับรองดิจิทัล (VC) ตามข้อมูลเมตาและกลไกการเพิกถอนที่เกี่ยวข้อง • ปฏิบัติตามกฎหมายระดับประเทศและนานาชาติที่บังคับใช้เกี่ยวกับการคุ้มครองข้อมูลและความมั่นคงปลอดภัยทางไซเบอร์

บทบาท / หน่วยงาน	ความรับผิดชอบ
ผู้ดำเนินการโครงสร้างพื้นฐานความเชื่อถือ (Trust Infrastructure Operator)	● เมื่อดำเนินการองค์ประกอบสำคัญของโครงสร้างพื้นฐานด้านความเชื่อถือ เช่น องค์กรผู้ออกใบรับรอง (CA) บัญชีรายชื่อที่เชื่อถือได้ หรือทะเบียนข้อมูลที่สามารถตรวจสอบได้ ต้องรับรองว่าสินทรัพย์ดังกล่าวได้รับการคุ้มครอง สามารถใช้งานได้ และมีความน่าเชื่อถือภายใต้ขอบเขตของกรอบความเชื่อถือ
ผู้ใช้งาน เช่น ประชาชน	● มีหน้าที่ในการคุ้มครองกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) และเอกสารรับรองดิจิทัล (VC) ที่บรรจุอยู่ โดยการรักษาการยืนยันตัวตนที่เข้มแข็งสำหรับกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) และอุปกรณ์ที่ติดตั้งกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) นั้น ● มีหน้าที่ในการให้ความยินยอมสำหรับการแบ่งปันข้อมูลจากเอกสารรับรองดิจิทัล (VC) แก่ผู้ให้บริการที่ได้รับการรับรอง

ก.5 การสร้างความน่าเชื่อถือของเอกสารรับรองดิจิทัล (VC) และการรักษาความมั่นคงปลอดภัย

การสร้างความปลอดภัยและความมั่นคงของระบบนิเวศเอกสารรับรองดิจิทัล (VC) จำเป็นต้องใช้แนวทางหลายขั้นตอนซึ่งครอบคลุมความเชื่อถือทางเทคนิค (หลักฐานการเข้ารหัส) ความมั่นคงปลอดภัยของข้อมูล (รวมถึงความสมบูรณ์ของข้อมูลและข้อกังวลด้านความเป็นส่วนตัว) และความมั่นคงปลอดภัยทางไซเบอร์ (การสร้างความมั่นใจในการป้องกันและความยืดหยุ่นของระบบ)

เอกสารรับรองดิจิทัล (VC) โดยทั่วไปมีอยู่ในระบบนิเวศที่สนับสนุนการออก การแบ่งปัน และการตรวจสอบเอกสารรับรองดิจิทัล (VC) โดยหน่วยงานที่เรียกว่า “ผู้ออกเอกสาร ผู้ถือเอกสาร และผู้ตรวจสอบเอกสาร” แผนภาพต่อไปนี้ได้อธิบายรูปแบบและบทบาทสำคัญที่กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ทำหน้าที่เป็น "ผู้ถือเอกสาร" เอกสารรับรองดิจิทัล (VC) และศูนย์กลางประสานงานสำหรับการแบ่งปันเอกสารรับรองดิจิทัล (VC) โดยผู้ใช้บริการ



รูปที่ 2 – รูปแบบแบบกระจายศูนย์สำหรับเอกสารรับรองดิจิทัล (VC)

ความเชื่อถือทางเทคนิค – เอกสารรับรองดิจิทัล (VC) ที่สามารถตรวจสอบได้ ประกอบด้วย หลักฐานการเข้ารหัสที่สร้างโดยผู้ออกเอกสาร ซึ่งควรนำมาใช้ตรวจสอบว่าเอกสารรับรองดิจิทัล (VC) ไม่ได้ถูกแก้ไขดัดแปลง และเพื่อยืนยันว่าเอกสารรับรองดิจิทัล (VC) ดังกล่าวไม่ถูกเพิกถอน เมื่อมีการแบ่งปันจากกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ที่น่าเชื่อถือ จะมีการสร้างเอกสารสำแดง (VP) ซึ่งรวมถึงหลักฐานการเชื่อมโยงกับผู้ถือเอกสาร เพื่อให้ผู้ตรวจสอบสามารถตรวจสอบได้ว่าเอกสารที่ได้รับถูกนำเสนอโดยเจ้าของที่แท้จริง (กล่าวคือ หน่วยงานที่เอกสารรับรองดิจิทัล (VC) ออกให้)

ภายใต้สถาปัตยกรรมกรอบการสร้างความน่าเชื่อถือของเอกสารรับรองและเอกสารสำแดง สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์เป็นผู้จัดการและบำรุงรักษาสิ่งนี้ในฐานะ "รายการความเชื่อถือ" ผ่าน "Universal Resolver"

ความมั่นคงปลอดภัยของข้อมูล – มุ่งเน้นการรักษาความลับ ความถูกต้องสมบูรณ์ และความพร้อมใช้งาน (CIA) ของข้อมูลตลอดวงจรชีวิตเอกสารรับรองดิจิทัล (VC) รวมถึงเมื่อเอกสารรับรองดิจิทัล (VC) ถูกร้องขอ จัดเก็บ และแบ่งปันโดยผู้ถือเอกสาร ตลอดจนการปฏิบัติตามข้อกำหนดการคุ้มครองข้อมูลและความเป็นส่วนตัว เอกสารรับรองดิจิทัล (VC) ที่อยู่ระหว่างการส่งผ่านจะถูกส่งผ่านช่องทางที่ปลอดภัยเสมอ (เช่น HTTPS) เพื่อรักษาความลับ ในขณะที่เอกสารรับรองดิจิทัล (VC) เอง จะถูกลงนามด้วยการเข้ารหัสเพื่อรับรองความสมบูรณ์และความถูกต้องของข้อมูล

ความมั่นคงปลอดภัยทางไซเบอร์ – ผู้ออกเอกสาร ผู้ตรวจสอบ และผู้ให้บริการโครงสร้างพื้นฐานความเชื่อมั่นมีหน้าที่รับผิดชอบในการปกป้องระบบและสินทรัพย์จากการถูกโจมตี และเพื่อให้มั่นใจในความยืดหยุ่น แอปพลิเคชันกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) และกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับธุรกิจบนคลาวด์ควรใช้การจัดการกุญแจที่เหมาะสมและการป้องกันด้วยพื้นที่ปลอดภัย (secure enclave) หรือระบบ HSM (Hardware Security Module) ตามที่ระดับความน่าเชื่อถือกำหนด รวมทั้งต้องมั่นใจว่ากลไกการควบคุมการเข้าถึงและการยืนยันตัวตนของผู้ใช้มีความเหมาะสมกับความอ่อนไหวของเอกสารรับรองดิจิทัล (VC) และข้อมูลที่ได้รับการคุ้มครอง

ความรับผิดและความรับผิดชอบ – ภายใต้กรอบการสร้างความน่าเชื่อถือ ผู้ออกเอกสารมีหน้าที่รับผิดชอบต่อความถูกต้อง การออกอย่างถูกต้องตามกฎหมาย และการจัดการสถานะอย่างทันท่วงที (รวมถึงการเพิกถอนหรือการระงับชั่วคราว) ของเอกสารรับรองดิจิทัล (VC) สำหรับผู้ให้บริการกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) มีหน้าที่รับผิดชอบต่อการจัดเก็บอย่างปลอดภัย การคุ้มครอง และการออกเอกสารสำแดง (VP) อย่างถูกต้อง รวมถึงการผูกโยงกับผู้ถือเอกสารและการยืนยันตัวตน แต่ไม่ต้องรับผิดชอบต่อความถูกต้องของเนื้อหาสาระภายในเอกสารรับรองดิจิทัล (VC) และหน้าที่ของผู้ตรวจสอบและผู้อาศัยการยืนยันตัวตนต้องรับผิดชอบต่อการใช้ข้อมูลเอกสารรับรองดิจิทัล (VC) อย่างถูกต้องตามกฎหมาย มีความเหมาะสมตามสัดส่วน และจำกัดตามวัตถุประสงค์ รวมถึงการปฏิบัติตามข้อกำหนดด้านการคุ้มครองข้อมูลและความมั่นคงปลอดภัยทางไซเบอร์ กรอบการสร้างความน่าเชื่อถือต้องกำหนดกลไกการเยียวยาและการระงับข้อพิพาท และให้อำนาจแก่หน่วยงานกำกับดูแลในการสอบสวนเหตุการณ์ กำหนดมาตรการแก้ไข และบังคับใช้การปฏิบัติตามในกรณีที่เกิดความล้มเหลวหรือการใช้งานที่ไม่ถูกต้อง

ก.6 การคัดเลือกกรณีการใช้งานระดับประเทศที่มีผลกระทบสูง

การคัดเลือกกรณีการใช้งานระดับประเทศที่มีผลกระทบสูง ไม่ควรพิจารณาเพียงแค่ความสำคัญที่เห็นได้ชัดหรือการใช้งานในปริมาณมาก (การแบ่งปันเอกสารรัฐที่ใช้งานบ่อย อาทิ บัตรประจำตัวประชาชน และใบอนุญาตขับขี่) แต่ยังต้องพิจารณาถึงความต้องการที่คำนึงถึงผู้ใช้ การเข้าถึงที่ครอบคลุม และศักยภาพสำหรับการเปลี่ยนแปลงบริการดิจิทัลที่สร้างบริการสาธารณะที่ดียิ่งขึ้น ใช้งานได้จริง และดึงดูดผู้ใช้มากขึ้น

เกณฑ์	แนวทาง
ผลกระทบจากปริมาณการใช้งานสูง	ให้ความสำคัญกับบริการที่มีจำนวนผู้ใช้หรือธุรกรรมมากที่สุด เพื่อเพิ่มผลกระทบสูงสุดจากการเปลี่ยนผ่านสู่ระบบดิจิทัล
การวิจัยที่มุ่งเน้นผู้ใช้เป็นศูนย์กลาง	การใช้ข้อมูลและข้อเสนอแนะของผู้ใช้บริการ เพื่อระบุบริการที่ต้องการใช้งาน แทนการอ้างอิงสมมติฐานภายใน
แนวทาง “แก้ปัญหาทั้งระบบ”	การคัดเลือกบริการที่สามารถออกแบบใหม่ได้แบบครบวงจร เพื่อตอบสนองความต้องการทั้งหมดของผู้ใช้บริการ เช่น การเริ่มและดำเนินธุรกิจ หรือการมีบุตร
การเปลี่ยนแปลงเชิงยุทธศาสตร์	การมุ่งเน้นการบริการที่แสดงให้เห็นถึงคุณค่าของแพลตฟอร์มระหว่างหน่วยงานภาครัฐ เช่น ศูนย์แลกเปลี่ยนข้อมูลกลางภาครัฐ (GDX)
การเปลี่ยนแปลงบริการ	การทำงานร่วมกับหน่วยงานภาครัฐและผู้ให้บริการ เพื่อระบุพื้นที่ที่มีอัตราการละทิ้งสูงหรือพื้นที่ที่จะได้รับประโยชน์สูงสุดจากการออกแบบบริการใหม่หรือการปรับปรุงกระบวนการ

การให้บริการที่อาจพิจารณาเพิ่มเติมจากที่ระบุไว้ในข้อ 5.4 (กำหนดลำดับความสำคัญกรณีการใช้งานที่มีผลกระทบสูง 5 ประการ) ได้แก่:

- การวิเคราะห์บริการเอกสารอิเล็กทรอนิกส์มากกว่า 100 รายการของสำนักงานพัฒนารัฐบาลดิจิทัล
- Biz Portal ของกรมพัฒนาธุรกิจการค้าและบริการที่เกี่ยวข้องกับการจัดตั้งและบริหารธุรกิจ
- โครงการสวัสดิการสังคม

ยกตัวอย่าง หากพิจารณาศักยภาพของเอกสารรับรองดิจิทัล (VC) ในการส่งผลกระทบต่อโครงการสวัสดิการสังคม จะสามารถเห็นข้อได้เปรียบที่ครอบคลุมหลายด้าน

รากฐานการบริหารของระบบสวัสดิการสังคมจำนวนมากถูกพัฒนาในโลกที่พึ่งพากระดาษเป็นหลัก ซึ่งต้องอาศัยเอกสารหลายรูปแบบและการให้บริการในพื้นที่ เมื่อระบบเหล่านี้ย้ายเข้าสู่ระบบออนไลน์ มักยังคงรักษากระบวนการที่ล้าสมัยและมีคลังข้อมูลแบบแยกส่วน ซึ่งส่งผลให้เกิดค่าใช้จ่ายด้านการดำเนินงานและภาระทางการบริหารที่มากสำหรับผู้มีสิทธิ์ได้รับประโยชน์

การเปลี่ยนผ่านจากฐานข้อมูลแบบรวมศูนย์และแยกส่วนไปสู่รูปแบบที่กระจายศูนย์และมุ่งเน้นผู้ใช้เป็นศูนย์กลาง เช่น กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) และเอกสารรับรองดิจิทัล (VC) ส่งผล

ให้โครงการสวัสดิการสังคมสามารถบรรลุระดับประสิทธิภาพ ความเป็นส่วนตัว และการมีส่วนร่วมที่ไม่เคยมีมาก่อน รูปแบบเหล่านี้ควรสนับสนุนการตรวจสอบแบบออฟไลน์ การใช้ QR code ที่ตรวจสอบได้ และการให้บริการที่ผ่านตัวแทนอย่างชัดเจน เพื่อให้มั่นใจได้ว่าการเข้าถึงจะไม่ถูกจำกัดด้วยการมีสมาร์ทโฟน การเชื่อมต่อ หรือทักษะดิจิทัล เอกสารรับรองดิจิทัล (VC) ได้มีวิธีการที่เป็นมาตรฐานและปลอดภัยด้วยการเข้ารหัสสำหรับการยืนยันข้อมูลส่วนบุคคล เช่น อัตลักษณ์ รายได้ สถานะความพิการ หรือประวัติการจ้างงาน โดยไม่จำเป็นต้องมีกระบวนการยืนยันด้วยตนเอง

การเปลี่ยนจาก "การพึ่งพาความน่าเชื่อถือของสถาบัน" ไปสู่ "หลักฐานทางการเข้ารหัส" ช่วยสร้างระบบนิเวศที่มุ่งเน้นผู้ใช้โดยไร้รอยต่อ ซึ่งประชาชนสามารถควบคุมข้อมูลของตนเองได้ และรัฐสามารถมุ่งเน้นทรัพยากรไปยังผู้ที่ต้องการความช่วยเหลือมากที่สุด

ก.7 การปรับปรุงการบูรณาการบริการและการแลกเปลี่ยนข้อมูลในภาครัฐ

เอกสารรับรองดิจิทัล (VC) และกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) เป็นรากฐานของระบบนิเวศแบบกระจายศูนย์ ที่เปลี่ยนแปลงความสัมพันธ์ระหว่างหน่วยงานภาครัฐกับบริการอื่น ๆ ทั้งภายในและภายนอกรัฐบาลที่ใช้ข้อมูลของตนอย่างมีนัยสำคัญ หน่วยงานที่เคยมีการเปิดการเข้าถึงข้อมูลให้กับระบบอื่นผ่าน API เพื่อวัตถุประสงค์ เช่น การตรวจสอบ การตรวจสอบคุณสมบัติ หรือการเริ่มต้นบริการ (เช่น KYC) สามารถมุ่งเน้นการออกข้อมูลสำคัญในรูปแบบเอกสารรับรองดิจิทัล (VC) ที่ผู้ใช้บริการถือครอง แทนการให้บริการแก่ระบบบุคคลที่สามที่หลากหลาย

การเปลี่ยนแปลงจุดมุ่งเน้นของหน่วยงานภาครัฐ จากผู้ให้บริการเป็นผู้ให้ข้อมูล มีข้อได้เปรียบหลายประการสำหรับการขยายขอบเขตการใช้งานและความยั่งยืน ได้แก่

การเปลี่ยนแปลงแนวทาง	ประโยชน์
ความต้องการข้อมูลสามารถขยายตัวได้ทั้งในเชิงปริมาณและขอบเขต โดยไม่จำเป็นต้องมีข้อกำหนดด้านโครงสร้างพื้นฐานเพิ่มเติมสำหรับผู้ออกข้อมูล	• ผู้ใช้บริการสามารถแบ่งปันข้อมูลของตนเองโดยตรงกับผู้ให้บริการอื่น ๆ ภายใต้การควบคุมและความยินยอมของตนเอง โดยไม่ต้องเรียก API กลับไปยังระบบของหน่วยงานผู้ออกข้อมูลสำหรับทุกธุรกรรม • การเชื่อมโยงระหว่างผู้ใช้ข้อมูลของหน่วยงานและระบบ IT ของหน่วยงานถูกยกเลิก ซึ่งหมายความว่าการที่ผู้ให้บริการที่ใช้ข้อมูลสามารถขยายบริการของตนได้ โดยไม่ทำให้หน่วยงานภาครัฐต้องขยายระบบของตนตามไปด้วย
ปริมาณการใช้งานสูงสุดมีความราบเรียบมากขึ้น และไม่ได้ถูกขับเคลื่อนโดยบริการที่ต้องพึ่งพาข้อมูลจากหน่วยงาน	• เมื่อผู้ใช้บริการแบ่งปันข้อมูลโดยตรงมากขึ้น ปริมาณการใช้งานสูงสุดจะเกิดขึ้นที่ระบบของผู้ให้บริการ ไม่ใช่ที่ผู้ออกข้อมูล

การเปลี่ยนแปลงแนวทาง	ประโยชน์
	• ความต้องการใช้ระบบหลังบ้านราบเรียบขึ้น และต้องการเวลาประมวลผลน้อยลง ลดปัญหาที่เกี่ยวข้องกับความพร้อมใช้งาน เนื่องจากผู้ใช้ไม่ต้องร้องขอข้อมูลบ่อยครั้ง (เอกสารรับรองถูกเก็บไว้ในกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) และสามารถนำไปใช้ซ้ำได้หลายครั้งกับหลายบริการ)
ข้อจำกัดที่เกิดจากระบบหลังบ้านที่เป็นกรรมสิทธิ์หรือซับซ้อนลดลง	• การพัฒนาและบำรุงรักษา API อาจมีค่าใช้จ่ายสูงเมื่อมีระบบหลังบ้านเก่า เป็นกรรมสิทธิ์ หรือซับซ้อน การออกเอกสารรับรองดิจิทัล (VC) ตามมาตรฐานสากลเป็นแนวทางที่ง่ายกว่า และสามารถดำเนินการได้ด้วยการลงทุนที่น้อยลงเนื่องจากความซับซ้อนลดลง • เมื่อความซับซ้อนในการประมวลผลข้อมูลอยู่ที่ผู้ใช้ปลายทางหรือผู้ให้บริการ ไม่ใช่หน่วยงานผู้ออกเอกสาร
ปัญหาการทำงานร่วมกันลดลงเนื่องจากการใช้มาตรฐานแบบเปิด	• บริการที่ต้องพึ่งพาข้อมูลของหน่วยงานสามารถเชื่อมต่อกับผู้ใช้บริการและกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) โดยตรง เพื่อร้องขอข้อมูลสำคัญ ซึ่งช่วยลดปัญหาการสนับสนุนและการทำงานร่วมกัน รวมถึงการเริ่มต้นใช้งานของผู้ใช้บริการ API • หน่วยงานสามารถใช้เครื่องมือ ไลบรารีโค้ด และผลิตภัณฑ์หลายประเภท (ซึ่งหลายรายการเป็น open source) พื่อออกเอกสารรับรองดิจิทัล (VC) ไปยังกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ที่สอดคล้องตามมาตรฐานได้

ก.8 แหล่งข้อมูลทางการที่มีศักยภาพ

แหล่งข้อมูลทางการในภาครัฐควรได้รับการยืนยัน และผู้ดำเนินการชุดข้อมูลดังกล่าว ควรได้รับการสนับสนุน เพื่อให้ประชาชนเข้าถึงข้อมูลในรูปแบบเอกสารรับรองดิจิทัล (VC) ที่กำหนดไว้

ประเภท	ชุดข้อมูล	เจ้าของ
ขั้นพื้นฐาน	บัตรประจำตัวประชาชน ทะเบียนบ้าน ใบสำคัญการจดทะเบียนธุรกิจ	กรมการปกครอง กรมพัฒนาธุรกิจการค้า
การเดินทางและแรงงาน	ใบอนุญาตขับขี่ ใบอนุญาตวิชาชีพ ปริญญาบัตร	กรมการขนส่งทางบก สภาวิชาชีพ มหาวิทยาลัย
การเงินและกฎหมาย	การยื่นภาษี ประวัติเครดิต โฉนดที่ดิน	กรมสรรพากร บริษัท ข้อมูลเครดิตแห่งชาติ จำกัด กรมที่ดิน
สุขภาพและการเดินทาง	ใบรับรองแพทย์ การส่งต่อผู้ป่วย สถานะวีซ่า บัตรขาเข้า	กระทรวงสาธารณสุข สำนักงานตรวจคนเข้าเมือง

ก.9 หน่วยงานหลักของภาครัฐ

ความสำเร็จของระบบนิเวศเอกสารรับรองดิจิทัล (VC) ระดับประเทศขึ้นอยู่กับการมีส่วนร่วมของหน่วยงานภาครัฐที่ดูแลแหล่งข้อมูลที่เป็นทางการ เช่น ทะเบียนฐานข้อมูลสำคัญ ชุดข้อมูลที่เชื่อถือได้เหล่านี้ให้ผลทางกฎหมายแก่เอกสารรับรองดิจิทัล (VC) เพื่อให้มั่นใจว่าเอกสารได้รับการยอมรับในทุกภาคส่วนของสังคม

กรมการปกครอง

ในฐานะผู้ดูแลข้อมูลทะเบียนราษฎรและเอกสารการทะเบียนราษฎร กรมการปกครองมีหน้าที่รับผิดชอบชุดข้อมูลขั้นพื้นฐานสำคัญในระบบนิเวศ แอปพลิเคชัน ThaID ซึ่งพัฒนาโดยสำนักบริหารการทะเบียน (BORA) ได้สร้างระบบบัตรประชาชนดิจิทัลในระดับประชากรแล้ว ThaID ช่วยให้ประชาชนสามารถแสดงบัตรประจำตัวประชาชนและทะเบียนบ้านในรูปแบบดิจิทัล ซึ่งได้รับการรับรองทางกฎหมายว่าเทียบเท่ากับเอกสารจริงตามกฎหมายการทะเบียนราษฎรที่มีอยู่

สำนักงานพัฒนารัฐบาลดิจิทัล

ผ่านแอปพลิเคชัน “ทางรัฐ” สำนักงานพัฒนารัฐบาลดิจิทัลได้สร้างบริการแบบรวมศูนย์ เพื่อให้ประชาชนในการเข้าถึงบริการภาครัฐ ทั้งนี้ ความรับผิดชอบของสำนักงานพัฒนารัฐบาลดิจิทัลยังรวมถึงการพัฒนาและดำเนินการศูนย์แลกเปลี่ยนข้อมูลกลางภาครัฐ (GDX) และการกำหนดมาตรฐานกลาง เพื่อให้มั่นใจว่าเอกสารรับรองดิจิทัล (VC) ที่ออกโดยหน่วยงานหนึ่งสามารถอ่านและตรวจสอบโดยหน่วยงานอื่นได้

บริษัท ไปรษณีย์ไทย จำกัด

บริษัท ไปรษณีย์ไทย จำกัด อยู่ในฐานะที่เป็นตัวกลางที่น่าเชื่อถือระหว่างโลกกายภาพและดิจิทัล แอปพลิเคชัน "Prompt Post" ทำหน้าที่เป็นกล่องจดหมายดิจิทัลที่ปลอดภัยและแพลตฟอร์มการจัดการเอกสาร ช่วยให้สามารถส่งและรับเอกสารอิเล็กทรอนิกส์ได้อย่างมีความน่าเชื่อถือ การบูรณาการลายเซ็นอิเล็กทรอนิกส์ของ Prompt Post และแพลตฟอร์มปิดสำหรับผู้ใช้ที่ผ่านการ KYC ทำให้เป็นผู้ให้บริการกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ที่มีศักยภาพ โดยเฉพาะสำหรับเอกสารทางกฎหมายและการติดต่อทางธุรกิจที่ต้องการหลักฐานการส่งที่มีความน่าเชื่อถือสูง

กรมพัฒนาธุรกิจการค้า

ในส่วนของกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับนิติบุคคลซึ่งเป็นองค์ประกอบสำคัญของระบบนิเวศ กรมพัฒนาธุรกิจการค้าเป็นผู้ออกหนังสือรับรองนิติบุคคลซึ่งเป็นเอกสารที่สำคัญในภาคธุรกิจ และการเปลี่ยนผ่านไปสู่แพลตฟอร์ม "DBD Biz Regist" ภายในเดือนกรกฎาคม 2568 กำหนดให้การจดทะเบียนนิติบุคคลและการดาวน์โหลดเอกสารที่รับรองทั้งหมดต้องดำเนินการในรูปแบบอิเล็กทรอนิกส์ แพลตฟอร์มนี้จัดเตรียมข้อมูลที่เครื่องสามารถอ่านได้เพื่อใช้ในการออกเอกสารรับรองดิจิทัล (VC) ข้อมูลของนิติบุคคล ช่วยให้ธุรกิจทุกขนาดสามารถพิสูจน์สถานะทางกฎหมาย อำนาจของกรรมการ และฐานะทางการเงินได้

กรมการขนส่งทางบก

กรมการขนส่งทางบกรับผิดชอบในการกำกับดูแลการขนส่งทางถนน การจดทะเบียนยานพาหนะ และการออกใบอนุญาตขับขี่ ซึ่งถือว่าเป็นเอกสารรับรองที่มีการใช้งานมากที่สุดในระบบเศรษฐกิจไทย ทั้งนี้ใบอนุญาตขับขี่มีศักยภาพที่จะเป็นเอกสารรับรองดิจิทัล (VC) หลักที่สามารถตรวจสอบได้ เช่น การพิสูจน์อายุ และหากสอดคล้องกับมาตรฐานสากล จะเป็นพื้นฐานสำหรับการทำงานร่วมกันข้ามพรมแดนสำหรับผู้ขับขี่ไทยเมื่อเดินทางไปยังประเทศอื่น ๆ ในภูมิภาคและอาจรวมถึงนอกภูมิภาคด้วย

ภาคผนวก ข – การวิเคราะห์และประเด็นท้าทายสำคัญ

ข.1 การป้องกันความเสี่ยงจากการฉ้อโกงและการเสริมสร้างความมั่นคงปลอดภัยสาธารณะ

การแทนที่เอกสารทางกายภาพและฐานข้อมูลแยกส่วนด้วยหลักฐานทางการเข้ารหัส ทำให้การบริการภาครัฐและภาคเอกชนสามารถเปลี่ยนจากการ "คาดการณ์" ว่าผู้ใช้บริการถูกต้องตามกฎหมายไปสู่การ "รู้" ด้วยความแน่นอนทางคณิตศาสตร์

ในระบบดั้งเดิม การฉ้อโกงมักเริ่มต้นด้วยการปลอมแปลงบัตรประจำตัวประชาชนหรือเอกสารทางราชการที่ถูกแก้ไข (เช่น PDF ที่ถูกตกแต่งด้วย Photoshop) การใช้เอกสารรับรองดิจิทัล (VC) จะช่วยลดความเสี่ยงนี้ เนื่องจากถูกลงนามด้วยการเข้ารหัสโดยผู้ออกเอกสาร (หน่วยงานรัฐบาล) ภายใต้การควบคุมที่เข้มงวด เพื่อให้มั่นใจว่าผู้ถือเอกสารได้รับการยืนยันตัวตนก่อนการออก และสามารถตรวจพบความพยายามในการแก้ไขข้อมูลภายในเอกสารรับรองดิจิทัล (VC) เมื่อนำไปแบ่งปันในภายหลัง

การหลอกลวงและการฉ้อโกงออนไลน์เป็นปัญหาสำคัญในหลายประเทศ โดยเฉพาะอย่างยิ่งในประเทศไทย เช่น การปลอมแปลงเอกสารในภาคสาธารณสุขที่นำไปสู่การใช้การยืนยันด้วยข้อมูลชีวมิติ (Biometric) [13] การหลอกลวงในชีวิตประจำวัน และการฉ้อโกงอัตลักษณ์ที่ใช้ AI

ตามรายงานของกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (สำนักงานตำรวจแห่งชาติ) ในปี 2566 - 2567 มีคดีหลอกลวงและฉ้อโกงเกิดขึ้นประมาณ 700 คดีต่อวัน โดยการหลอกลวงผ่านพาณิชย์อิเล็กทรอนิกส์พบมากที่สุด โดยคิดเป็นร้อยละ 40 ของอาชญากรรมทางไซเบอร์ การฉ้อโกงออนไลน์เหล่านี้ก่อให้เกิดความเสียหายทางการเงินประมาณ 45,000 ล้านบาทในช่วงปี พ.ศ. 2566 และครึ่งแรกของปี พ.ศ. 2567

แนวทางการป้องกันการฉ้อโกงแบบบูรณาการ ที่ใช้ประโยชน์จากการเข้ารหัสและการใช้งานเอกสารรับรองดิจิทัล (VC) สามารถเพิ่มความปลอดภัยสาธารณะ ลดภาระทางการเงินจากการฉ้อโกงทั้งต่อรัฐและผู้เสียหาย และสนับสนุนการป้องกันเพิ่มเติมในอนาคต เช่น การยืนยันผู้ขายในพาณิชย์อิเล็กทรอนิกส์ การพิสูจน์อัตลักษณ์องค์กรและธุรกิจในธุรกรรมดิจิทัล สำหรับช่องทางการฉ้อโกงที่พบบ่อย คือ การใช้เอกสารที่ถูกขโมยมาเพื่อเปิดบัญชีธนาคารหรือสมัครผลิตภัณฑ์ทางการเงิน ซึ่งเกิดขึ้นได้จากกระบวนการสมัครที่ยังใช้เอกสารกระดาษและการขาดการตรวจสอบเอกสารยืนยันตัวตนโดยตรง การกำหนดให้มีหลักฐานอัตลักษณ์ดิจิทัลที่ได้รับจากเอกสารรับรองดิจิทัล (VC) จะช่วยยับยั้งผู้ฉ้อโกง ลดความเสี่ยงต่อผู้ให้บริการทางการเงิน และลดการเกิดการฉ้อโกงประเภทนี้สำหรับประชาชน

[13] ไทยนำระบบยืนยันตัวตนด้วยข้อมูลชีวมิติใบหน้ามาใช้ เพื่อต่อต้านการฉ้อโกงในภาคสาธารณสุข
https://www.biometricupdate.com/202601/thailand-introduces-face-biometrics-verification-to-fight-health-sector-fraud

ข.2 กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับธุรกิจและผลกระทบทางเศรษฐกิจ

แนวคิดหลักของกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับธุรกิจ

ขณะที่กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ส่วนบุคคลได้จัดเก็บหนังสือเดินทางหรือใบอนุญาตขับขี่ ในส่วนของกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับธุรกิจจะเก็บอัตลักษณ์ดิจิทัลของนิติบุคคล เพื่ออำนวยความสะดวกให้ธุรกิจสามารถพิสูจน์การมีอยู่ สถานะ และอำนาจในการดำเนินธุรกิจได้ทันที

กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับธุรกิจ ช่วยให้ธุรกิจสามารถเก็บข้อมูลของตนเองในรูปแบบเอกสารรับรองดิจิทัล (VC) ที่สามารถตรวจสอบได้ โดยปกติจะอยู่ในกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) บนคลาวด์ที่ปลอดภัย เช่นเดียวกับบุคคล นิติบุคคลจำเป็นต้องมีอัตลักษณ์ทางกฎหมายเพื่อให้กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ธุรกิจสามารถพิสูจน์ความเป็นเจ้าของเอกสารรับรองเหล่านั้นได้ ซึ่งในกรณีนี้ควรอ้างอิงจากชุดข้อมูลหลักที่ใช้ในการจดทะเบียนและดำเนินธุรกิจ เช่น *DBD Biz Regist*

ตัวอย่างการใช้งานกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับธุรกิจ

- **KYB (Know Your Business)**: ธนาคารสามารถรับลูกค้านิติบุคคลได้ภายในไม่กี่วินาที โดยการตรวจสอบเอกสารรับรองดิจิทัล (VC) แทนการตรวจสอบหนังสือบริคณห์สนธิด้วยตนเอง
- **การจัดซื้อจัดจ้างภาครัฐ**: ธุรกิจสามารถเข้าร่วมการจัดซื้อจัดจ้างในรูปแบบดิจิทัล โดยการส่งเอกสารรับรองดิจิทัล (VC) ที่ผ่านการตรวจสอบล่วงหน้าเกี่ยวกับความมั่นคงทางการเงินและขีดความสามารถทางเทคนิค
- **ห่วงโซ่อุปทาน/หนังสือเดินทางดิจิทัลของสินค้า**: ธุรกิจสามารถตรวจสอบเอกสารรับรองดิจิทัล (VC) ด้านแหล่งที่มาและความยั่งยืนของผู้จัดหาได้แบบเรียลไทม์

กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับธุรกิจควรสนับสนุนเอกสารรับรองดิจิทัล (VC) ที่แสดงการมอบอำนาจและอำนาจที่ได้รับมอบหมาย เพื่อให้บุคคลธรรมดาสามารถดำเนินการแทนนิติบุคคลในลักษณะที่ควบคุมและตรวจสอบได้ รวมถึงการสนับสนุนการมอบอำนาจที่จำกัดขอบเขตและระยะเวลา รวมถึงการเพิกถอน

กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับธุรกิจจะเก็บ "วัตถุ" ดิจิทัล 3 ประเภทหลัก เพื่อสนับสนุนการดำเนินงานของนิติบุคคล ได้แก่ หลักฐานดิจิทัล การมอบอำนาจดิจิทัล และลงลายมือชื่อดิจิทัล (Digital Signature):

หลักฐานดิจิทัล	หลักฐานดิจิทัลของข้อมูลเฉพาะที่ออกโดยหน่วยงานที่เป็นทางการ เช่น ใบอนุญาตค้า หรือใบอนุญาตด้านสิ่งแวดล้อม
การมอบอำนาจดิจิทัล	หลักฐานเพื่อแสดงว่าบุคคลธรรมดา มีอำนาจกระทำการแทนบริษัท เช่น หนังสือมอบอำนาจหรือสิทธิในการลงนามสำหรับบัญชีธนาคาร
ลงลายมือชื่อดิจิทัล (Digital Signature)	ลายมือชื่อดิจิทัลในรูปแบบนิติบุคคล เป็นการรับรองต้นทางและความถูกต้องที่ใช้ในการลงนามเอกสารอิเล็กทรอนิกส์ในนามของธุรกิจหรือองค์กร

ผลกระทบทางเศรษฐกิจ

กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับธุรกิจ ถือเป็นโอกาสสำคัญในการลดแรงเสียดทานเชิงโครงสร้างในเศรษฐกิจไทย วิสาหกิจขนาดกลางและขนาดย่อม (SME) ซึ่งคิดเป็นสัดส่วนส่วนใหญ่ของธุรกิจไทย มักเผชิญกับต้นทุนที่สูงเกินไปและขั้นตอนที่ซับซ้อนในการเข้าร่วมการค้าระหว่างประเทศหรือการสมัครขอสินเชื่อ[14]

ด้วยการจัดให้ทุกบริษัทไทยมีกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับธุรกิจ รัฐบาลจะสามารถเปิดใช้งาน KYB ที่สามารถตรวจสอบธุรกิจได้ทุกขนาด รวมถึง SME สิ่งนี้จะช่วยให้บริษัทไทยสามารถแบ่งปันสถานะการจดทะเบียน รายชื่อผู้ถือหุ้น และสถานะทางการเงินได้ทันทีกับธนาคารหรือพันธมิตร

การดำเนินการตามระบบเลขทะเบียนนิติบุคคลเดียวของอาเซียน (ASEAN Unique Business Identification Number : UBIN) จะช่วยสนับสนุนให้ธุรกิจไทยได้รับการยอมรับและความเชื่อถือในทุกประเทศสมาชิกอาเซียนทั้ง 10 ประเทศ โดยการประมาณการของ Boston Consulting Group ระบุว่าการดำเนินการ UBIN อย่างเต็มรูปแบบ สามารถสร้างมูลค่าทางเศรษฐกิจให้แก่อาเซียนได้ระหว่าง 110,000 - 300,000 ล้านดอลลาร์สหรัฐ ผ่านการลดต้นทุนทางธุรกรรมและดึงดูดการลงทุนจากต่างประเทศ

ประโยชน์ทางเศรษฐกิจที่มีศักยภาพ

	ประโยชน์ทางตรง	**ผลกระทบในระยะยาว**
SMEs/MSMEs	การลดเวลาการเริ่มต้นใช้งานสำหรับการส่งออกและการขอสินเชื่อ	การเพิ่มการมีส่วนร่วมในการค้าดิจิทัลระดับภูมิภาค
การบริหารราชการแผ่นดิน	การกำจัดการประมวลผลเอกสารบนกระดาษ	ดัชนีพัฒนาการรัฐบาลอิเล็กทรอนิกส์ (EGDI) มีอันดับที่สูงขึ้น

[14] ASEAN's Next Trade Breakthrough: Accelerating Cross-Border Growth Through Interoperable Identity - https://asean-bac.org/news-and-press-releases/asean%E2%80%99s-next-trade-breakthrough-accelerating-cross-border-growth-through-interoperable-identity

ภาคการเงิน	ต้นทุนการปฏิบัติตาม KYC/AML ลดลง	สามารถเข้าถึงสินเชื่อ และบริการทางการเงินอย่างทั่วถึง
ภาคการท่องเที่ยว	การตรวจสอบที่ไร้รอยต่อสำหรับผู้ประกอบอาชีพดิจิทัล (digital nomad) และผู้ถือวีซ่าพำนักระยะยาว (Long-Term Resident Visa: LTR)	รายได้จากการท่องเที่ยวและค่าใช้จ่ายของผู้เยี่ยมเยือนที่เพิ่มขึ้น

ผู้ให้บริการกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับธุรกิจที่มีศักยภาพ

ควรมีการหารือกับภาคเอกชน เพื่อให้มั่นใจว่าได้มีการพิจารณาโครงการที่มีอยู่แล้ว และกำหนดว่าบุคคลใดควรเป็นผู้ให้บริการกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ธุรกิจ ตัวอย่างเช่น Prompt Post ของไปรษณีย์ไทยมีแผนพัฒนากระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับองค์กรเพื่อจัดเก็บใบอนุญาตของภาครัฐ โดยมีการบูรณาการในอนาคตเข้ากับระบบ National Single Window (NSW) สำหรับกระบวนการนำเข้า-ส่งออก กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) นี้ได้รับการรับรองสำหรับใช้เป็นกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับธุรกิจระดับประเทศภายใต้เงื่อนไขของกรอบการสร้างความน่าเชื่อถือขั้นตอนเริ่มต้นสำหรับการดำเนินงานกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับธุรกิจ

เมื่อวางแผนการดำเนินงานกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับธุรกิจ ประเด็นสำคัญที่จำเป็นต้องพิจารณาคือบุคคลใดจะเป็นผู้ใช้งานกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) เอกสารรับรองดิจิทัล (VC) ประเภทใดที่กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) จะจัดเก็บ และกรณีการใช้งานใดที่กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ธุรกิจจะสร้างผลกระทบได้อย่างมีนัยสำคัญ ทั้งนี้ การดำเนินงานกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับธุรกิจมีแนวทางการดำเนินงานที่สำคัญดังต่อไปนี้

ระยะที่ 1: กรอบการทำงานและการปฏิบัติตามข้อกำหนด (ปีที่ 1)

- การปรับให้สอดคล้องกับกฎระเบียบ: ตรวจสอบสถาปัตยกรรมกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับธุรกิจให้ตรงตามข้อกำหนดของกรอบการสร้างความน่าเชื่อถือและมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ โดยขยายกรอบการสร้างความน่าเชื่อถือตามที่เหมาะสม
- การกำหนดการกำกับดูแล: กำหนดว่าใครเป็นผู้ออกกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับธุรกิจ (รัฐบาลหรือผู้ให้บริการที่มีคุณสมบัติจากภาคเอกชน) และจัดทำรายการความเชื่อถือสำหรับผู้ให้บริการที่ได้รับการรับรอง

- ระบุกรณีการใช้งานหลักเบื้องต้นสำหรับกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับธุรกิจ: ตัวอย่างเช่น การเป็นตัวแทนทางกฎหมาย การขอรับเงินสนับสนุนจากภาครัฐ การเข้าร่วมการจัดซื้อจัดจ้างภาครัฐ การสมัครหรือการแสดงใบอนุญาต

ระยะที่ 2: การพัฒนาหลักและการกำหนดมาตรฐาน (ปีที่ 1 – ควบคู่กับระยะที่ 1)

- เอกสารรับรองดิจิทัล (VC) สำหรับนิติบุคคล: พัฒนาเอกสารรับรองดิจิทัล (VC) อัตลักษณ์นิติบุคคลโดยเฉพาะสำหรับธุรกิจ เช่น หมายเลขภาษีมูลค่าเพิ่ม รหัส LEI และข้อมูลจากทะเบียนนิติบุคคลแห่งชาติ
- สนับสนุนหน่วยงานภาครัฐและสถาบันหลักในการออกเอกสารรับรองดิจิทัล (VC): ตัวอย่างเช่น ใบสำคัญการจดทะเบียนบริษัท หนังสือรับรองการเสียภาษี สถานะประกันสังคม และใบอนุญาตวิชาชีพ
- การกำหนดกฎเกณฑ์สำหรับการมอบอำนาจและหนังสือการมอบอำนาจ: เพื่อให้ธุรกิจ (นิติบุคคล) สามารถมอบหมายสิทธิเฉพาะให้พนักงานในการลงนามหรือแบ่งปันข้อมูลในนามองค์กรได้

ระยะที่ 3: การทดสอบนำร่องและการเชื่อมต่อระบบนิเวศ (ปีที่ 2)

- ดำเนินการทดสอบนำร่องกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ธุรกิจสำหรับกรณีการใช้งานหลัก
- การลงทะเบียนผู้ใช้บริการ: เชื่อมต่อผู้ใช้บริการ เช่น ธนาคาร หน่วยงานสาธารณูปโภค และหน่วยงานรัฐ เพื่อให้มีความพร้อมทางเทคนิคในการร้องขอและตรวจสอบข้อมูลจากกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ธุรกิจ

ระยะที่ 4: การขยายผลในวงกว้างและการบังคับใช้ (ปีที่ 3)

- การจัดการวงจรชีวิต: กำหนดขั้นตอนสำหรับการเพิกถอน (เช่น หากบริษัทหยุดดำเนินการค้าล้มละลาย หรือการมอบอำนาจถูกถอน)
- การขยายผลการใช้งานกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับธุรกิจ
- การพิจารณาข้อกำหนดของภาครัฐ: หน่วยงานภาครัฐต้องยอมรับการใช้กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับการยืนยันตัวตนและการยื่นเอกสาร ซึ่งอาจจำเป็นต้องมีการออกกฎระเบียบหรือกฎหมายเพิ่มเติมเพื่อรองรับการดำเนินการดังกล่าว

ข.3 การเพิ่มประสิทธิภาพและการเข้าถึงบริการภาครัฐ

กระบวนการของภาครัฐแบบดั้งเดิมมักต้องอาศัยการตรวจสอบเอกสารด้วยตนเอง โดยเจ้าหน้าที่ต้องตรวจสอบเอกสารจริง และบ่อยครั้งต้องตรวจสอบหลายเอกสารพร้อมกัน กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ดิจิทัลช่วยให้ประชาชนสามารถถือครองเอกสารดิจิทัลจากภาครัฐและเอกชนที่ได้รับการรับรองด้วยความเชื่อถือทางการเข้ารหัส ซึ่งไม่เพียงแต่ทำให้กระบวนการมีความคล่องตัวมากขึ้น แต่ยังช่วยลดภาระของประชาชนและเจ้าหน้าที่อย่างมีนัยสำคัญ

- เอกสารรับรองดิจิทัล (VC) สามารถตรวจสอบได้ทันทีทั้งแบบออนไลน์และออฟไลน์ (เช่น ใบอนุญาตขับขี่ดิจิทัลหรือบัตรประจำตัวประชาชน) ซึ่งจะได้รับการลงนามด้วยการเข้ารหัสโดยกระทรวงที่ออกเอกสาร บุคคลที่สามสามารถตรวจสอบความถูกต้องได้ทันทีโดยไม่จำเป็นต้องติดต่อกระทรวงต้นทางอีกครั้ง
- ประชาชนต้องพิสูจน์อัตลักษณ์หรือคุณสมบัติเพียงครั้งเดียว เมื่อเอกสารรับรองดิจิทัล (VC) อยู่ในกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) แล้ว สามารถนำมาใช้ซ้ำได้หลายครั้งกับผู้ให้บริการภาครัฐและภาคเอกชน โดยไม่จำเป็นต้องขอสำเนาเอกสารเพิ่มเติมหรือทำการตรวจสอบตัวตนด้วยตนเองหลายครั้ง
- เอกสารรับรองดิจิทัล (VC) ยังสามารถใช้ในการกรอกแบบคำขอที่ซับซ้อนสำหรับการขอรับสิทธิประโยชน์หรือการยื่นภาษี ซึ่งจะช่วยลดข้อผิดพลาดและระยะเวลาดำเนินการจากสัปดาห์เป็นวินาที อีกทั้งยังเปิดโอกาสให้ประชาชนสามารถเลือกแชร์ข้อมูลเฉพาะส่วนที่จำเป็นแทนการส่งเอกสารทั้งฉบับ ซึ่งช่วยเพิ่มความเป็นส่วนตัวและลดการร้องขอข้อมูลเกินความจำเป็นจากผู้ให้บริการ

การลดภัยคุกคามจากการรั่วไหลของข้อมูล

ภัยคุกคามที่พบบ่อยต่อประสิทธิภาพของภาครัฐคือความเสี่ยงจากการรั่วไหลของข้อมูล ซึ่งอาจนำไปสู่การสูญเสียหรือถูกละเมิดบริการของรัฐ การนำรูปแบบการจัดการแบบกระจายศูนย์มาใช้สำหรับอัตลักษณ์ดิจิทัลและข้อมูลสำคัญของรัฐบาล (ที่ใช้โดยประชาชนและธุรกิจ) จะช่วยลดความเสี่ยงจากการที่ฐานข้อมูลหรือระบบบริการแบบรวมศูนย์ถูกโจมตี เนื่องจากหน่วยงานสามารถมุ่งเน้นไปที่การออกเอกสารรับรองดิจิทัล (VC) อย่างปลอดภัย แทนการเปิดเผยการทำงานหรือข้อมูลไปยังระบบอื่น ๆ

ประชาชนที่ถือเอกสารรับรองดิจิทัล (VC) ในกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สามารถใช้ฟังก์ชันการเปิดเผยข้อมูลแบบเลือกได้ (Selective Disclosure) ซึ่งหมายความว่าสามารถเลือกแบ่งปันข้อมูลหรือการยืนยันข้อมูลเฉพาะบางส่วนจากเอกสารรับรองดิจิทัล (VC) แทนการใช้เอกสารดิจิทัลทั้งฉบับ ซึ่งช่วยบังคับใช้หลักการลดข้อมูลให้น้อยที่สุด ซึ่งลดความเสี่ยงจากการรั่วไหลของข้อมูลที่ผู้ให้บริการได้รับ เนื่องจากได้รับเฉพาะข้อมูลที่จำเป็นต่อการทำธุรกรรมเท่านั้น

เอกสารรับรองดิจิทัล (VC) ยังลดการถูกฉ้อโกงได้ เนื่องจากมีคุณสมบัติที่ไม่สามารถแก้ไขดัดแปลงได้ และกระบวนการตรวจสอบอัตลักษณ์ที่เข้มงวด เช่น การตรวจสอบด้วยข้อมูลชีวมิติ (Biometric) และการตรวจสอบการมีตัวตนจริง (Liveness Checking) ซึ่งทำให้การโจรกรรมอัตลักษณ์ทำได้ยากกว่าการใช้เอกสารกระดาษและกระบวนการแบบดั้งเดิมอย่างมาก

ข.4 ความชัดเจนเกี่ยวกับผู้ให้บริการกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ของภาครัฐ

ประเด็นสำคัญ คือ ประเทศไทยควรรับรองผู้ให้บริการกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) และอัตลักษณ์ดิจิทัลรายเดียวหรืออนุญาตให้มีผู้ให้บริการหลายราย แม้ว่าทั้งสองแนวทางสามารถดำเนินการได้ แต่จะส่งผลกระทบระยะยาวต่อระบบนิเวศที่แตกต่างกัน ซึ่งควรได้รับการพิจารณาอย่างรอบคอบ

การตัดสินใจเลือกระหว่างการกำหนดให้มีเพียงกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ที่จัดทำโดยภาครัฐ หรือการอนุญาตให้มีระบบนิเวศที่แข่งขันกันโดยมีผู้ให้บริการหลายราย ถือเป็นการตัดสินใจเชิงยุทธศาสตร์ที่สำคัญของรัฐบาลไทย การเลือกแนวทางนี้จะส่งผลอย่างลึกซึ้งต่อการยอมรับของผู้ใช้งาน นวัตกรรม และความยืดหยุ่นของระบบ

ระบบนิเวศกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ที่กระจัดกระจายในปัจจุบัน

สำหรับประชาชนไทยที่ทำธุรกรรมออนไลน์ อัตลักษณ์ดิจิทัลและกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) มีมาให้ใช้งานระยะหนึ่งแล้วในรูปแบบที่แยกส่วน โดยมุ่งเน้นการตอบสนองความต้องการของผู้ใช้งานเฉพาะกลุ่ม ปัจจุบัน ThaID (มีผู้ใช้งาน 30 ล้านคน) มักถูกใช้สำหรับการพิสูจน์อัตลักษณ์ ในขณะที่ทางรัฐ (มีผู้ใช้งาน 39 ล้านคน) ให้การเข้าถึงบริการภาครัฐผ่านอินเทอร์เฟซซูเปอร์แอปพลิเคชันเดียว ซึ่งทั้งสองแอปพลิเคชันได้รวมกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ในแผนการพัฒนาผลิตภัณฑ์ นอกจากนี้ยังมีซูเปอร์แอปพลิเคชัน “เป๋าตัง” ที่พัฒนาขึ้นโดยความร่วมมือระหว่างรัฐบาลไทยและธนาคารกรุงไทย ซึ่งกลายเป็นกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับชำระเงินรายใหญ่ที่มีผู้ใช้งานมากกว่า 40 ล้านคน นอกจากนี้ เป๋าตังยังช่วยลดต้นทุนการแจกจ่ายความช่วยเหลือและเพิ่มความโปร่งใสด้วยการสร้างเส้นทางการตรวจสอบดิจิทัลสำหรับการใช้จ่ายทุกบาท

แม้รูปแบบกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) เหล่านี้ประสบความสำเร็จ อย่างไรก็ดี ยังคงเป็นนวัตกรรมรูปแบบแยกส่วน และมีการทำงานร่วมกันน้อยมาก ซึ่งส่วนใหญ่มีสาเหตุจากการขาดกรอบความเชื่อมั่นและขาดการบังคับใช้ให้เป็นมาตรฐานการทำงานร่วมกัน ซึ่งนำไปสู่การใช้งานของผู้ใช้ที่ซับซ้อนและเกิดความสูญเสียสำหรับองค์กรภาครัฐและภาคเอกชนในการเพิ่มประสิทธิภาพหรือสร้างนวัตกรรมที่ก้าวหน้ามากขึ้น

จากมุมมองของผู้ใช้บริการ ความไม่สอดคล้องกันเหล่านี้แสดงออกมาในรูปแบบการใช้งานที่ยุ่งยากและความจำเป็นต้องใช้หลายแอปพลิเคชัน เพื่อทำธุรกรรมให้เสร็จสมบูรณ์ ขณะที่มุมมองของภาครัฐ ต้นทุนในการทำให้ระบบต่าง ๆ เชื่อมโยงกันมีมูลค่าสูง และความพยายามในการบูรณาการมักถูกทำซ้ำในหลายหน่วยงาน

ข้อสนับสนุนรูปแบบผู้ให้บริการรายเดียว

อาจมีการโต้แย้งได้ว่าผู้ให้บริการกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) รายเดียว เช่น ทางรัฐหรือ ThaID ที่ใช้แนวทางแบบรวมศูนย์ อาจสร้างความเชื่อมั่นสำหรับผู้ใช้งานได้อย่างสม่ำเสมอและสามารถลดภาระด้านกฎระเบียบได้ แอปพลิเคชันของรัฐเพียงหนึ่งเดียวที่ทำหน้าที่เป็น "บริการแบบครบวงจร" จะช่วยให้ทรัพยากรของภาครัฐมุ่งเน้นไปที่การรักษาความปลอดภัยของแพลตฟอร์มเดียวแทนการตรวจสอบหลายแพลตฟอร์ม[15]

ข้อสนับสนุนรูปแบบผู้ให้บริการหลายรายหรือระบบนิเวศ

แม้ประชาชนโดยทั่วไปจะไว้วางใจภาครัฐในการออกเอกสารอัตลักษณ์หลัก แต่ประชาชนมักนิยมนวัตกรรมจากภาคเอกชนสำหรับบริการเชิงพาณิชย์ ธนาคาร และการบูรณาการด้านไลฟ์สไตล์ รูปแบบผู้ให้บริการหลายรายที่ธนาคาร ผู้ให้บริการโทรคมนาคม และบริษัทเทคโนโลยีสามารถให้บริการกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ที่ได้รับการรับรอง จะช่วยส่งเสริมการแข่งขันในด้านคุณสมบัติความปลอดภัย การบูรณาการข้อมูลชีวมิติ และการออกแบบสำหรับผู้ใช้งาน

จากมุมมองด้านการดำเนินงาน ระบบนิเวศผู้ให้บริการหลายรายช่วยลดภาระของภาครัฐในการเป็นผู้ให้บริการกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) รายเดียว และอาจเพิ่มความยืดหยุ่นในระบบนิเวศ โดยลดความเสี่ยงจากการที่ผู้ให้บริการกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) รายเดียวหยุดให้บริการ จนทำให้ประชาชนไม่สามารถเข้าถึงบริการรัฐบาลที่สำคัญได้

ข้อเสนอแนะเชิงยุทธศาสตร์: รูปแบบระบบนิเวศแบบผสมผสาน

เมื่อพิจารณาบริบทในประเทศ ประเทศไทยควรนำระบบนิเวศกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) หลายรายที่อยู่ภายใต้การกำกับดูแลตามกรอบแนวทางการสร้างความเชื่อถือแห่งชาติสำหรับเอกสารรับรองดิจิทัล (VC) มาใช้ รูปแบบนี้สอดคล้องกับโครงสร้างหลายหน่วยงานของประเทศไทย รักษาการแข่งขันและนวัตกรรม และป้องกันการกระจัดกระจายของระบบผ่านมาตรฐานการทำงานร่วมกันที่บังคับใช้ได้

แทนที่จะกำหนดให้มีเพียงกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) แห่งชาติหนึ่งเดียว หรืออนุญาตให้มีการขยายตัวของแอปพลิเคชัน ที่แยกส่วนโดยไม่มีการควบคุม รัฐบาลควรกำหนดกฎเกณฑ์การทำงานร่วมกันที่บังคับใช้ได้ เพื่อให้กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ที่ได้รับการรับรองหลายรายสามารถดำเนินการภายใต้กรอบเดียวกัน แนวทางนี้จะรักษานวัตกรรมและทางเลือกของผู้ใช้งาน ขณะเดียวกันก็

[15] Thailand Digital Data Infrastructure Roadmap Report (World Bank) - https://thedocs.worldbank.org/en/doc/c9160dd8065d1300384d8ab790742165-0070012025/original/Deliverable-5-Final-DDIR-for-publication-June2025-final-revision.pdf

รับประกันความสามารถในการพกพา มาตรฐานที่สม่ำเสมอ และความสอดคล้องของระบบโดยรวม ภายใต้รูปแบบนี้

- สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.)จะเป็นผู้จัดตั้งและบริหารกรอบแนวทางการสร้างความเชื่อถือแห่งชาติสำหรับเอกสารรับรองดิจิทัล (VC) รวมถึงการรับรอง การทดสอบความสอดคล้อง และกลไกการกำกับดูแล
- กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ทั้งหมดที่ดำเนินการภายในระบบนิเวศจำเป็นต้องได้รับการรับรองภายใต้กรอบการสร้างความน่าเชื่อถือและต้องปฏิบัติตามแนวปฏิบัติการทำงานร่วมกันระดับประเทศ โดยการรับรองถือเป็นเกณฑ์พื้นฐานสำหรับผู้เข้าร่วมทั้งหมดภายในกรอบนี้ กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ที่ได้รับการกำหนดโดยภาครัฐจะได้รับสิทธิพิเศษเพิ่มเติมในการจัดเก็บเอกสารรับรองดิจิทัล (VC) ที่ออกโดยรัฐบาลอย่างเป็นทางการ และหน่วยงานภาครัฐจะต้องยอมรับการใช้งานดังกล่าว ส่วนกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ที่ได้รับการรับรอง แต่ไม่ได้ถูกกำหนดโดยภาครัฐสามารถดำเนินการได้เต็มรูปแบบภายในระบบนิเวศสำหรับเอกสารรับรองดิจิทัล (VC) ที่ไม่เป็นทางการ โดยไม่มีข้อจำกัดหรือการกีดกัน
- การทำงานร่วมกันและการโอนย้ายกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ที่ได้รับการรับรองถือเป็นข้อบังคับ และระบบเอกสารรับรองดิจิทัล (VC) ที่เป็นกรรมสิทธิ์ที่ดำเนินการนอกกรอบแนวทางจะไม่ได้รับการรับรองสำหรับการใช้งานของรัฐบาล
- เพื่อเพิ่มประสิทธิภาพการลงทุนภาครัฐและป้องกันการทำงานซ้ำซ้อน รัฐบาลควรกำหนดกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) ประชาชนที่รัฐบาลสนับสนุนได้สูงสุด 2 ราย และกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) สำหรับธุรกิจที่รัฐบาลสนับสนุนได้สูงสุด 2 ราย แอปพลิเคชันของภาครัฐที่มีการใช้งานในวงกว้างอยู่แล้ว เช่น ThaID และทางรัฐ ควรเป็นผู้ที่ได้รับการพิจารณาหลักสำหรับการกำหนดภายใต้การปฏิบัติตามข้อกำหนดของกรอบการสร้างความน่าเชื่อถือ
- กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) อื่นของภาครัฐ รัฐวิสาหกิจ และภาคเอกชนอื่น ๆ อาจดำเนินการภายใต้การรับรองได้ แต่จะไม่ได้รับสิทธิพิเศษด้านการบูรณาการ ข้อตกลงเฉพาะ หรือเงินทุนสาธารณะเพิ่มเติม

รูปแบบนี้สร้างความมั่นใจในการทำงานร่วมกันที่บังคับใช้ได้ การใช้ทรัพยากรสาธารณะอย่างมีวินัย และการนำไปใช้ในระดับประเทศที่ขยายการใช้งานได้ ขณะที่รักษาการแข่งขันและนวัตกรรมทางเทคโนโลยี

ข.5 ความสอดคล้องกับพระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. 2565

การใช้เอกสารรับรองดิจิทัล (VC) ไม่ได้ทำให้ผลบังคับใช้ของพระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. 2565 ภายใต้มาตรา 13 ลดลง หรือป้องกันไม่ให้หน่วยงานออก "ใบอนุญาต" ตามที่บัญญัติไว้ในพระราชบัญญัติ

อย่างไรก็ตาม สพธอ. ควรพยายามสื่อสารกับหน่วยงานอื่น ๆ ถึงวิธีที่เอกสารรับรองดิจิทัล (VC) สามารถและควรนำไปดำเนินการเพื่อตอบสนองความต้องการของหน่วยงานที่ต้องการจัดการราชการทางอิเล็กทรอนิกส์ในบริบทของพระราชบัญญัตินี้และกฎหมายที่มีอยู่อื่น ๆ

ข.6 ประโยชน์ของมาตรฐาน

ประโยชน์ของเอกสารรับรองดิจิทัล (VC) และรูปแบบแบบกระจายศูนย์

การนำมาตรฐานที่ได้รับการยอมรับในระดับสากลมาใช้สำหรับเอกสารรับรองดิจิทัล (VC) และการรับรองอัตลักษณ์ จะทำให้ประเทศไทยและประชาชนสามารถใช้ประโยชน์จากโอกาสในการเพิ่มผลิตภาพ ความสะดวกในการเข้าถึงบริการสาธารณะและภาคเอกชน และการทำงานร่วมกันในระดับสากล สำหรับการค้า การเดินทาง และพาณิชยกรรม

เอกสารรับรองดิจิทัล (VC) และแนวทางแบบกระจายศูนย์สำหรับการใช้งานเอกสารรับรองดิจิทัล (VC) เหล่านี้สำหรับประชาชนและธุรกิจ ยังมีข้อได้เปรียบในการเปลี่ยนบทบาทของรัฐบาลจากผู้ให้บริการหลักด้านอัตลักษณ์และข้อมูลไปสู่ผู้ออกเอกสารที่เชื่อถือได้ การทำงานร่วมกันและการแบ่งปันข้อมูลเกิดขึ้นโดยตรงระหว่างผู้ให้บริการและประชาชนสำหรับธุรกรรมที่พบบ่อยที่สุด ซึ่งช่วยลดภาระของระบบภาครัฐในการจัดหา API ที่สามารถขยายผลได้สำหรับการร้องขอข้อมูลจำนวนมาก หรือการตรวจสอบอัตลักษณ์ของผู้ใช้งาน

มาตรฐานสากลที่ได้รับการยอมรับอย่างกว้างขวางเป็นสิ่งจำเป็น

การเลือกใช้มาตรฐานและโปรโตคอลสำหรับอัตลักษณ์ดิจิทัลและการออกเอกสารรับรองดิจิทัล (VC) และการใช้งานต่อเนื่องในระบบนิเวศ ถือเป็นปัจจัยสำคัญต่อความยั่งยืนและการทำงานร่วมกันของระบบนิเวศ หลายประเทศกำลังดำเนินการใช้กระเป๋าเอกสารดิจิทัล (Digital Document Wallet) และออกเอกสารรับรองดิจิทัล (VC) ซึ่งส่งผลให้เกิดการขับเคลื่อนการพัฒนาและการยอมรับอย่างแพร่หลายของมาตรฐาน ข้อกำหนด และโปรโตคอลสำคัญบางประการ ตัวอย่างเช่น OpenID Foundation ได้พัฒนาโปรโตคอลสำหรับการออกแบบการออกเอกสารรับรองดิจิทัล (VC) และ การออกเอกสารสำแดง (VP) ซึ่งกำลังดำเนินการในสหภาพยุโรปภายใต้กรอบ European Digital Identity (EUDI) และในรัฐใกล้เคียงและประเทศที่สนใจทั่วโลก มาตรฐาน ISO/IEC 18013-5/7 ก็ได้รับความนิยมส่วนใหญ่จากการนำไปใช้เป็นพื้นฐานสำหรับการออกใบอนุญาตขับขี่แบบดิจิทัลในสหรัฐอเมริกา

มาตรฐานและโปรโตคอลจาก ISO, Open ID Foundation, World Wide Web Consortium (W3C) และ IETF (เช่น OpenID for Verifiable Credential issuance and presentation, SD-JWT และ ISO/IEC 18013-5/7) มีความสมบูรณ์ ผ่านการทดสอบอย่างครบถ้วน[16]และได้รับการรับรองเป็นกฎหมายโดยสหภาพยุโรปในฐานะมาตรฐานหลักสำหรับการออกและการใช้งานเอกสารรับรองดิจิทัล (VC) ที่มีความเชื่อถือสูง ทั้งในระดับประเทศและระดับสากล นอกจากนี้ยังนำไปสู่การพัฒนา OpenID4VC High Assurance Interoperability Profile (HAIP)[17] ซึ่งรวบรวมข้อกำหนดเหล่านี้สำหรับการดำเนินการในสหภาพยุโรปและนอกสหภาพยุโรป

ชั้น	มาตรฐานที่ใช้ (กระเป๋าเอกสารดิจิทัล EUDI / โปรไฟล์ OIDF HAIP)				
การยืนยันตัวตน	NIST 800.63A	eIDAS LoA	ISO/IEC 29115	National Derivatives...	
โปรโตคอลการออก	OpenID4VCI	ISO 23220-3	DIDComm		
รูปแบบเอกสารรับรอง	W3C VCDM	SD-JWT-VC	ISO mDoc	AnonCreds	
กระบวนการนำเสนอ	OpenID4VP	DIDComm	mDoc	QR	
การเรียกใช้	W3C DC API	QR Code	Deep Link	CHAPI	NFC (mDoc)
การส่งผ่าน	BLE (mDoc)	NFC (CTAP)	Camera (QR)	HTTP	BLE (OpenID4VP)
ความเชื่อถือทางเทคนิค	X509 / Trust Lists	OIDF Federation	vLEI	DID	
สถานะเอกสารรับรอง	IETF Status List	W3C Bitstring Status List			

รูปที่ 3 – มาตรฐานและโปรโตคอลตามที่กำหนดสำหรับการดำเนินการเป็นโปรไฟล์สำหรับกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) EUDI

การกำหนดระบบที่นำมาตรฐานที่ได้รับการยอมรับแล้วไปใช้ จะช่วยให้เกิดการทำงานร่วมกันและความสะดวกในการดำเนินการกับผู้ให้บริการหลายราย รวมถึงมีชุมชนนักพัฒนาที่พร้อมสนับสนุนระบบนิเวศของประเทศไทย นอกจากนี้ยังหมายความว่าการให้บริการของผู้ที่ยืนยันตัวตนและผู้ออกเอกสารที่มีศักยภาพจะสามารถปรับระบบของตนให้ทำงานร่วมกับระบบนิเวศของเอกสารรับรองที่สามารถตรวจสอบได้ง่ายขึ้น ลดอุปสรรคในการดำเนินการโดยหลีกเลี่ยงเทคโนโลยีเฉพาะกลุ่มหรือเทคโนโลยีที่เป็นกรรมสิทธิ์

จากการวิเคราะห์ข้างต้น จึงมีข้อเสนอแนะให้ระบบนิเวศเอกสารรับรองดิจิทัล (VC) ของไทยนำมาตรฐานที่กำลังกลายเป็นเกณฑ์มาตรฐานสำหรับการทำงานร่วมกันของกระเป๋าเอกสารดิจิทัล (Digital Document Wallet) มาใช้

[16] OpenID Foundation demonstrates real-world interoperability of new Digital Identity Issuance Standards - https://openid.net/oidf-demonstrates-interoperability-of-new-digital-identity-issuance-standards/

[17] OpenID4VC High Assurance Interoperability Profile 1.0 - https://openid.net/specs/openid4vc-high-assurance-interoperability-profile-1_0.html

มาตรฐานที่แนะนำตามพัฒนาการในประเทศอื่น ๆ:

- **Issuance Protocol** – OpenID4VCI โปรโตคอลการออก – OpenID4VCI
- **Credential Format** – SD-JWT-VC, ISO mDoc รูปแบบเอกสารรับรองดิจิทัล (VC) – SD-JWT-VC, ISO mDoc
- **Presentation Flow** – OpenID4VP กระบวนการนำเสนอ – OpenID4VP
- **Invocation** – W3C DC API, Deep Link การเรียกใช้ – W3C DC API, Deep Link
- **Transport** – HTTP, (optionally BLE OpenID4VP, or BLE mDoc) การส่งผ่าน – HTTP (ตัวเลือกเพิ่มเติม: Bluetooth Low Energy (BLE) OpenID4VP หรือ BLE mDoc)
- **Technical Trust** – x509 / Trust Lists ความเชื่อถือทางเทคนิค – x509 / รายการความเชื่อถือ
- **Credential Status** – IETF Status List สถานะเอกสารรับรองดิจิทัล (VC) – IETF Status List

Delivering Thailand's Digital Trust Infrastructure:
Scaling digital ID and verifiable credentials

July 2026

Version 1.2

THE WORLD BANK

1 Executive Summary 5

2 Introduction 9

2.1 Objective 11

3 Illustrative use cases 12

3.1 The importance and opportunities of foundational identity verifiable credentials 12

3.2 In-Person Identity Verification (NFC / Bluetooth) 13

3.3 Online Privacy-Preserving Age Verification 13

3.4 Access to Credit: Financial Health Credential and MSME Loan Application 14

3.5 Social Welfare: Targeted Fuel Subsidy Redemption for Informal Workers 15

3.6 Telemedicine Consultation and Digital Prescription 16

3.7 ASEAN Trade Credential Submission (Business Wallet) 17

3.8 Education and Professional Credential Verification 17

3.9 Renting a Car Overseas Using a Digital Driving License 18

3.10 Digital Arrival Card and Hotel Check-In 18

3.11 Verified Online Seller to Prevent Marketplace Fraud 19

4 Evidence of impact 21

4.1 Reduced onboarding and compliance costs 21

4.2 Reduced fraud and improved security 21

4.3 Administrative efficiency and productivity gains 22

4.4 Economy-wide impact and business benefits 22

4.5 Implications for Thailand 22

5 Policy Recommendations 24

5.1 Formally establish a National Verifiable Credential Trust Framework 24

5.2 Develop and rationalize the wallet ecosystem 25

5.3 Mandate issuance of foundational verifiable credentials and acceptance across government and regulated sectors 26

5.4 Prioritize five high-impact use cases 28

5.5 Lead ASEAN in Developing Regional Standards 29

6 High-level strategic plan 31

6.1 Phase 1 (2026): Formalization and Regulatory Consolidation 31

6.2 Phase 2 (2027): Institutional Adoption, Priority Use Cases, and ASEAN Leadership 32

6.3 Phase 3 (2028-2029): National Scale and ASEAN Implementation 33

6.4 Phase 4 (2030-2032): Sustainability and potential commercialization 34

6.5 Summary of roles and responsibilities 34

7 Estimated budget needs for Phase 2 (2027) 38

Annex A – Background 40

A.1 The drivers for change 40

A.2 The need for strong governance and clear accountability 41

A.3 Building scalable and resilient National Digital Infrastructure 42

A.4 Scope of the Trust Framework 45

A.5 Ensuring that credentials are trusted and that security is maintained 47

A.6 Selecting high-impact national use cases 48

A.7 Improving service integration and data sharing across government 49

A.8 Potential Authoritative Sources of data 51

A.9 Key Government Actors 51

Annex B - Key issues and analysis 53

B.1 Fraud mitigation and enhanced public security 53

B.2 Business wallets and economic impact 54

B.3 Improving efficiency and access to government services 57

B.4 Clarity over the government wallet provider 58

B.5 Alignment with the Act on Management of State Affairs by Electronic Means (B.E. 2565) 60

B.6 The benefits of standards 60

1 Executive Summary

Thailand’s new government has an opportunity to modernize the foundations of digital trust and position the country for the next phase of economic growth. As digital services expand and cross-border trade deepens under ASEAN integration, the systems that govern how identity is verified and how official data is shared have become strategically important. Today, verification often relies on repeated document submission, screenshots of ID cards, and bespoke system integrations. This increases cost, slows services, and creates security risks. At the same time, online fraud and AI-enabled impersonation are increasing in scale and sophistication.

What is needed is a fundamental shift: from submitting documents to sharing trusted data, from physical verification to cryptographic certainty, and from fragmented silos to an interoperable national ecosystem. Verifiable credentials offer a secure and scalable solution. International standards have matured, and governments worldwide are operationalizing national verifiable credential trust frameworks. Within ASEAN, digital integration under the Digital Economy Framework Agreement (DEFA) is accelerating, and regional standards for trusted data exchange are still forming—creating a critical window for Thailand to act and shape the agenda.

Thailand is well-positioned to move quickly. ThaID, Thailand's national digital identity application, and Thang Rath, the government services super app, are used by tens of millions of citizens. A universal national ID and business registry provide reliable and digitalized authoritative data, and ETDA has established a verifiable credentials architecture and reference framework compliant with global standards. A vibrant private sector—including licensed digital identity operators—further strengthens these foundations. This transformation is also aligned with the *Act on Carrying Out of Public Service via Electronic Means* B.E. 2565 (2022), which mandates that public services be delivered digitally and requires interoperable, secure, and accessible data exchange across government agencies—capabilities that verifiable credentials directly enable at scale.

At present, however, these capabilities operate as parallel systems rather than a unified ecosystem. Multiple wallets, identity solutions, and agency systems exist, but credentials are not portable, interoperability is not enforced, and users are required to repeatedly provide the same data across services. Without a clear national framework, Thailand risks further fragmentation, duplication of public investment, and the emergence of closed ecosystems that limit reuse and scale.

International evidence suggests that the benefits of this shift are significant. The European Commission estimates that digital identity wallets could generate annual savings of €0.68–€1.36 billion in financial services and €1.26-2.51 billion in eHealth from reduced onboarding and verification costs alone. Administrative burden reductions for citizens are estimated at €350-400 million annually. Pilots have shown onboarding time reductions from days to minutes. At the economy-wide level, business wallet adoption has been estimated to generate up to €116 billion in annual benefits at scale. These gains are driven by reduced duplication, faster service delivery, lower fraud losses, and improved data portability.

These impacts are directly relevant to Thailand. Online scams and fraud already result in losses of approximately THB 45 billion annually, with hundreds of cases reported daily. Many of these rely on weaknesses in document-based verification, including fake IDs, altered documents, and impersonation. Moving to cryptographically verifiable credentials would not eliminate fraud, but would significantly reduce its feasibility and cost. At the same time, reducing friction in onboarding, licensing, and compliance processes would improve business productivity, support MSMEs, and strengthen Thailand’s competitiveness in regional digital trade.

This White Paper proposes five actions to realize the high-level objective of establishing Thailand as ASEAN's leading digital trust economy—empowering citizens and residents to share their data on their own terms, and giving businesses the digital trust infrastructure to grow at home, across the region, and globally. As global and regional standards rapidly converge, delay risks locking Thailand into externally defined frameworks rather than shaping them.

The Government should:

- **Formally establish a National Verifiable Credential Trust Framework** through Cabinet Resolution and Ministerial Regulation, designating ETDA which holds supervisory authority over electronic transaction services under the Royal Decree issued pursuant to the Electronic Transactions Act as the lead agency for certifying the trustworthiness of verifiable credential services.This will provide the legal and institutional foundation for the ecosystem, ensuring consistent rules, accountability, interoperability, and nationwide scale.

- **Develop and rationalize the digital wallet ecosystem** by implementing a two-tier accreditation system, categorized into (1) individual and (2) juristic business wallets. To optimize public investment, the number of government-designated wallet providers shall be limited to a maximum of two for each category ((1) individual wallets and (2) juristic business wallets). These designated wallets must ensure full interoperability and secure data portability. However, there will be no limitation on the number of private sector wallet providers, thereby fostering innovation and healthy market competition while maintaining system coherence and user-centric simplicity.

- **Mandate issuance of foundational verifiable credentials and acceptance across sectors**, requiring key agencies to issue foundational, high-volume credentials, mandating acceptance across public services, aligning with ETDA and relevant sector-specific regulators such as the Bank of Thailand, Securities and Exchange Commission (SEC) and Office of the National Broadcasting and Telecommunications Commission (NBTC) to establishing a Verifiable Credentials Issuance Fund, developing shared issuance capability integrated within the Government Data Exchange (GDX), National Verifiable Data Registry, and developing verification capabilities in Thang Rath and a universal verifier SDK for government digital services. This should drive end-to-end process re-engineering, eliminating redundant document requests, reducing

procedural steps, and minimizing administrative discretion in citizen-facing services.

- **Prioritize five high-impact national use cases** to demonstrate early value, including access to credit for businesses (particularly MSMEs), privacy-preserving age verification, social welfare access, health credential portability, and driving/professional/academic credentials. These use cases are selected for their high transaction volume, visibility, and ability to demonstrate clear benefits to citizens, businesses, and government.

- **Lead ASEAN in developing regional standards** under DEFA and through the ASEAN Digital Ministers' Meeting (ADGMIN) and ASEAN Economic Ministers (AEM) processes, while becoming the first ASEAN country to operationalize verifiable credentials at national scale and positioning Thailand as a connector between ASEAN and global digital trust frameworks.

Implementation should follow three phases:

- **Phase 1 (2026):** Establish legal framework and enforceable governance.

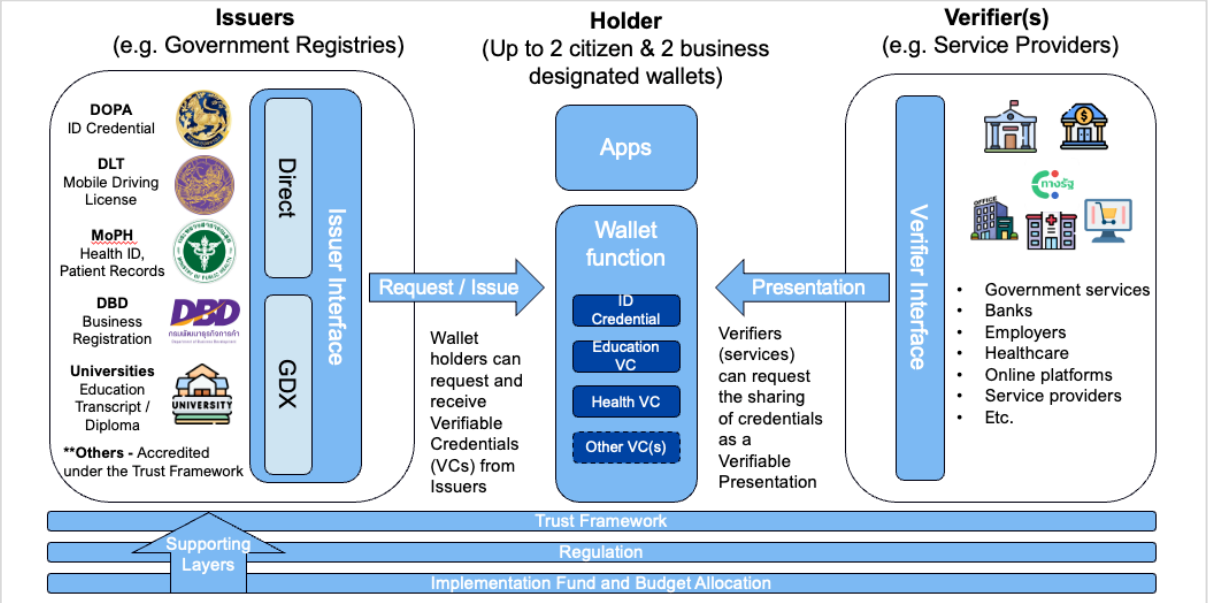
- **Phase 2 (2027):** Mandate issuance and acceptance across government and regulated sectors, while deploying priority use cases.

- **Phase 3 (2028-2029):** Scales nationally and advance ASEAN mutual recognition.

- **Phase 4 (2030-2032):** Sustainability and potential commercialization

Indicative financing requirements for Phase 2 are modest relative to the scale of impact. A financing envelope of approximately THB 490 million to THB 1.16 billion is estimated over one to two fiscal years, covering shared infrastructure, wallet enhancements, integration of priority agencies, and ecosystem enablement. A centralized approach—particularly through GDX-based shared issuance capability—can significantly reduce duplication and overall system cost. Prioritizing common infrastructure first, followed by targeted agency implementation for high-impact use cases, will maximize returns on investment and accelerate visible results.

Figure 1 — Illustration of the proposed verifiable credentials ecosystem in Thailand



2 Introduction

Thailand's new government has an opportunity to strengthen how identity is verified and how official data is shared across the digital economy. Today, much of this verification and data sharing still relies on repeated document submission, screenshots of ID cards, manual database checks, and application-specific integrations between agencies and private service providers. Citizens and businesses are frequently required to submit the same information multiple times because credentials verified in one system cannot be reused or recognized in another. This duplication increases administrative costs, slows service delivery, and creates security risks. This gap persists despite the Act on Carrying Out of Public Service via Electronic Means mandating digital service delivery, highlighting the need for a trusted and interoperable model for data sharing across agencies.

At the same time, Thailand continues to face high levels of scams and online fraud, with billions of baht lost annually through identity-based deception and social engineering. The rapid advancement of artificial intelligence is further increasing the scale and sophistication of impersonation, deepfake-enabled fraud, and automated phishing attacks, reducing the reliability of document-based verification. The systems that govern how credentials are issued, stored, shared, and verified have therefore become a critical component of national digital trust infrastructure.

Verifiable credentials provide a practical solution to these challenges. A verifiable credential is a digitally signed statement issued by an authoritative body or trusted entity — such as a government agency, university, or regulator — that can be securely stored in a digital wallet and presented for verification. Like physical ID cards carried in a wallet, they allow trusted documents to be carried and used when needed — but with the added ability to prove instantly that they are authentic and valid based on cryptographic proofs. Just as standardized card sizes allow any card to fit into any wallet, a common trust framework and shared technical standards ensure that digital credentials issued by one authority can be securely stored and used across different digital wallets and systems. International technical standards have matured and stabilized, and verifiable credentials are no longer pilots or experiments — they are rapidly becoming the foundation of the next generation of trusted digital identity and data exchange.

As such, verifiable credentials present a paradigm shift for the sharing of trusted data between government, citizens, and businesses. Rather than relying on centralized government databases and real-time access that requires significant investment to meet growing demand from digital services, governments are able to focus on the issuance of secure digital credentials that can be shared by the holders of those credentials without the intervention of government systems. This approach enables digital public service delivery to scale up and out without a disproportionate load being placed on government systems and simplifies digital service development by greatly reducing the need for APIs to access government systems.

Thailand has already made significant progress in digital identity and in laying the foundations for verifiable credentials. Government databases have been digitalized.

Applications such as ThaID, Thang Rath, and Paotang have achieved large-scale adoption, with tens of millions of Thais accessing identity services, government platforms, and payments. The National Digital ID (NDID) platform provides a federated model for identity verification in the financial sector. The Bank of Thailand's "Your Data" initiative is advancing consent-based financial data portability, and the Ministry of Public Health (MoPH) has begun exploring the use of verifiable credentials in health contexts, including through the Mor Prom application. Separately, the telecom providers have also implemented Mobile ID as supervised by the National Broadcasting and Telecommunication Commission (NBTC). Mobile ID is currently operated by AIS, TRUE, and NT, all of which could be future private sector wallet providers. ETDA has developed a Thai Verifiable Credential Architecture and Reference Framework. However, these initiatives were developed at different times and for different purposes, and they do not yet operate as a unified ecosystem.

Globally, governments are proactively operationalizing verifiable credentials to strengthen digital trust and modernize identity systems for secure, reusable data sharing. The European Union has adopted eIDAS 2.0, requiring each Member State to build or license at least one digital identity/document wallet and to enforce interoperability and portability under a common technical and governance framework. Australia, Brazil, Canada, India, South Korea, the United Kingdom, and the United States are just some of the countries developing national verifiable credential ecosystems. Major technology platforms such as Apple and Google now support verifiable credentials directly within smartphone operating systems.

Within ASEAN, digital integration is accelerating under the Digital Economy Framework Agreement (DEFA), which aims to enable interoperable digital trade and trusted cross-border services. For Thailand to participate fully and competitively, its digital credentials must be portable, verifiable, and aligned with global standards. This presents a strategic opportunity: by formalizing a national verifiable credential trust framework early and decisively, Thailand can position itself as a regional leader on this topic. With timely action, Thailand could become the first ASEAN country to operationalize verifiable credentials at national scale, shaping standards and influencing implementation across the region rather than adapting to frameworks defined elsewhere.

Verifiable credentials vs APIs: A paradigm shift in how data is shared

- **APIs (system-to-system):** Data is exchanged directly between systems through point-to-point integrations. Each service must build and maintain connections with multiple agencies, leading to complexity, duplication, and higher costs.
- **Verifiable Credentials (user-controlled):** Data is issued as a trusted digital credential and stored in a user's wallet (through an application or cloud). The user can securely share it across multiple services, which can instantly verify its authenticity (through cryptography) without needing direct system integration, or needing to repeatedly request credentials as they can be reused multiple times.

Verifiable credentials are emerging globally as the future of digital services, as they reduce integration costs, enhance privacy and security, and enable seamless cross-sector and cross-border data exchange without dependence on centralized infrastructure.

2.1 Objective

This White Paper sets out clear recommendations for how and why Thailand should formalize a National Trust Framework to scale digital identity and verifiable credential use across the public and private sectors.

High-Level Objective: Establish Thailand as ASEAN's leading digital trust economy—empowering citizens and residents to share their data on their own terms, and giving businesses the digital trust infrastructure to grow at home, across the region, and globally.

This means enabling government-recognized credentials to be issued easily, safely, and reliably—and usable through any accredited citizen or business wallet, across all government services, for citizens, residents, and businesses alike.

By aligning existing digital foundations under coherent governance and enforceable interoperability, Thailand can strengthen national digital trust infrastructure, reduce fraud, simplify and secure data sharing, lower compliance costs, enhance privacy protections, and position itself as a regional leader in ASEAN’s next phase of digital integration.

3 Illustrative use cases

This section presents a set of example use cases demonstrating how verifiable credentials can be applied across different sectors and interaction models in Thailand. These examples highlight the breadth of potential applications, including online and in-person transactions, cross-border use, citizen and business wallets, and multi-party interactions. They also demonstrate key features of verifiable credentials such as selective disclosure, privacy-preserving verification, delegation of authority, and the ability to share multiple trusted credentials seamlessly. Together, these use cases show how verifiable credentials can simplify service delivery, reduce fraud, enhance privacy, and enable interoperable, trusted data exchange across government, business, and international contexts.

3.1 The importance and opportunities of foundational identity verifiable credentials

The two foundational identity credentials underpinning Thailand's verifiable credential ecosystem are the national ID verifiable credential, issued by the Department of Provincial Administration (DOPA), and the business registration verifiable credential, issued by the Department of Business Development (DBD). All other credentials in the ecosystem build on one or both of these.

The **national ID verifiable credential** establishes who a person is and immediately unlocks a wide range of services, such as:

- Accessing Revenue Department services and government applications such as Thang Rath or MorProm
- Applying for driving licenses and other DLT services
- Accessing hospital and health services, both physically and remotely
- Applying for jobs or educational enrolment
- Opening payment wallets and other financial accounts

The national ID verifiable credential is also the key through which citizens acquire further credentials from other issuers. DOPA would additionally issue household registration and birth, death, and marriage certificates as verifiable credentials, covering the family and civil status data that many government and private sector services require.

The **business registration verifiable credential** establishes the legal identity of a company in the same way the national ID verifiable credential establishes the identity of an individual, and similarly unlocks downstream credentials including:

- Tax status and filing credentials
- Sector licenses and regulatory permits

- Export and import eligibility credentials
- Access to business finance and credit guarantees

Authorized employees can act on behalf of a company using a delegation credential stored in a business wallet — a shared credential store that holds the company's credentials and manages who within the organisation can present them. Together, these two credentials form the twin foundations on which every use case in this section is built.

3.2 In-Person Identity Verification (NFC / Bluetooth)

- Mali visits a bank branch to open a new account
- The bank officer requests proof of identity
- Mali opens her digital document wallet application and authenticates using biometrics
- The bank initiates a secure request via NFC or Bluetooth
- Mali consents to share her national ID credential
- The wallet transmits a verifiable presentation directly to the bank’s device
- The bank verifies:
    - The credential was issued by DOPA
    - The credential has not been altered or revoked
    - The credential belongs to Mali
- The bank completes onboarding without photocopying documents or manual verification

3.3 Online Privacy-Preserving Age Verification

- Anan wants to purchase an age-restricted product on an e-commerce application
- Anan selects the item and proceeds to checkout
- The application requests proof that Anan is over 20 years old
- Anan opens his digital document wallet application and authenticates using biometrics
- The wallet prompts Anan to approve sharing proof of age

- Anan consents to share a verifiable proof that he is over 20, derived from his national ID credential
- This proof is shared using selective disclosure or privacy-preserving techniques (e.g. zero-knowledge proof), without revealing his date of birth or other personal data
- The e-commerce application verifies the cryptographic signature of the proof
- The application confirms the proof is valid and completes the purchase

3.4 Access to Credit: Financial Health Credential and MSME Loan Application

- Daeng runs a small food stall and wants to apply for a working capital loan from a bank participating in the Thai Credit Guarantee Corporation (TCG) scheme
- The bank requires proof of identity, evidence of financial health, a credit history report, and a loan guarantee
- Daeng opens his digital document wallet application and authenticates using biometrics
- He receives a request for relevant credentials
- Daeng consents to share:
    - His national ID credential (issued by DOPA)
    - His financial health credential — an Ari Score VC issued by the Fiscal Policy Office, automatically pre-populated using trusted data from the following verifiable credentials:
        - Monthly income and tax filings (Revenue Department)
        - Total credit limit and number of credit accounts (his financial institutions)
        - Average deposits over the last 3 months (his banks)
        - Family/Household composition (DOPA)
    - His NCB credit report credential (issued by the National Credit Bureau), containing his credit history and repayment record
    - A loan guarantee credential issued by the Thai Credit Guarantee Corporation (TCG), confirming he qualifies for a government-backed guarantee on loans up to a specified amount

- The wallet generates a verifiable presentation combining all four credentials
- The bank verifies:
    - Identity was issued by a trusted authority (DOPA)
    - The Ari Score VC was issued by the Fiscal Policy Office and populated from authoritative data sources — not self-declared
    - The NCB credential is current, authentic, and issued by the National Credit Bureau
    - The TCG guarantee credential is valid and covers the requested loan amount
- The bank completes its credit assessment in minutes, without requiring Daeng to gather paper documents from multiple agencies or manually fill out financial questionnaires
- The loan is approved and disbursed to Daeng’s PromptPay-linked account

3.5 Social Welfare: Targeted Fuel Subsidy Redemption for Informal Workers

- The government announces an emergency fuel cost relief payment for informal workers most exposed to rising fuel prices, including motorcycle taxi drivers and ride-hailing drivers
- Arthit is a ride-hailing driver who wants to apply for the relief payment through the government's online portal (or Thang Rath)
- The portal requests proof of eligibility
- Arthit opens his digital document wallet application and authenticates using biometrics
- He consents to share:
    - His national ID credential (issued by DOPA)
    - His motorcycle taxi license credential (issued by DLT), confirming he is an active registered driver
    - His active driver and income summary credential (issued by Grab or LINE MAN), confirming he is currently working on the platform and his average monthly earnings fall within the eligible income band
- The portal verifies:

  - Credentials were issued by trusted authorities (DOPA, DLT, and a registered platform recognized by the Ministry of Labor)
  - Credentials are valid and not revoked
  - Credentials belong to Arthit
- The portal confirms Arthit has not previously received the payment in this period
- Eligibility is confirmed automatically and the relief payment is disbursed to Arthit's PromptPay account

3.6 Telemedicine Consultation and Digital Prescription

- Narin books an online consultation through a telemedicine platform
- The platform requires verification of both the patient and the medical professional
- Narin opens his digital document wallet application and authenticates
- He shares:
  - His national ID credential
  - His health insurance or eligibility credential
- The platform verifies Narin’s identity and eligibility
- The platform then shares the doctor’s credentials with Narin, including:
  - Medical license credential
  - Hospital or institutional affiliation
- Narin verifies that the doctor is licensed and authorized
- After consultation, the doctor issues a digital prescription as a verifiable credential
- The prescription is securely stored in Narin’s digital document wallet application
- Narin can later present the prescription at a pharmacy
- The pharmacy verifies the prescription’s authenticity and validity before dispensing medication

3.7 ASEAN Trade Credential Submission (Business Wallet)

- Charoen Export Co. Ltd. wants to export goods to another ASEAN country
- The importing country's customs authority requires proof of business registration, export license, and product certification
- An authorized employee opens the company's digital document wallet application (business wallet) and authenticates
- The employee acts under a verifiable mandate credential proving authority to represent the company
- The business consents to share:
    - Business registration credential
    - Export license credential
    - Certificate of origin
- These are shared as verifiable credentials with the foreign customs authority
- The customs authority verifies:
    - Authenticity of credentials (cryptographic signatures)
    - Issuing authorities (e.g. business registry, relevant ministries)
    - Delegated authority of the employee
- The shipment is cleared without paper documents or manual processing

3.8 Education and Professional Credential Verification

- Suda applies for a job requiring proof of her university degree and professional certification
- The employer requests verification of qualifications
- Suda opens her digital document wallet application and authenticates
- She receives a request for relevant credentials
- Suda consents to share:
    - University degree credential
    - Professional license credential
- The wallet generates a verifiable presentation

- Only required attributes are shared (e.g. qualification, issuing institution, validity)
- The employer verifies:
    - Credentials were issued by trusted institutions (e.g. university, regulator)
    - Credentials are valid and not revoked
    - Credentials belong to Suda
- The employer completes verification instantly without contacting issuing institutions

3.9 Renting a Car Overseas Using a Digital Driving License

- Kittipong travels to Japan for a holiday
- He wants to rent a car but must provide a valid driving license
- At the rental counter, the company requests proof of driving eligibility
- Kittipong opens his digital document wallet application and authenticates using biometrics
- The rental company sends a request for a driving license credential
- Kittipong consents to share his digital driving license as a verifiable credential
- The wallet generates a verifiable presentation, sharing only required information (e.g. license validity, vehicle class)
- The rental company verifies:
    - The license was issued by a trusted authority (e.g. Department of Land Transport)
    - The credential is valid and not revoked
    - The credential belongs to Kittipong
- The rental is approved instantly without requiring physical documents or manual checks

3.10 Digital Arrival Card and Hotel Check-In

- Maria, a tourist, arrives in Thailand and completes the Thailand Digital Arrival Card before landing

- Her arrival information is issued as a verifiable credential and stored in her digital document wallet application
- Upon arrival, immigration verifies her arrival credential digitally
- Maria proceeds to her hotel
- At hotel check-in, reception requests:
    - Proof of identity
    - Arrival or immigration status
- Maria opens her digital document wallet application and authenticates
- She consents to share:
    - Passport or identity credential
    - Digital arrival card credential
- The wallet generates a verifiable presentation, sharing only necessary details
- The hotel verifies:
    - Authenticity of the credentials (issued by immigration authorities)
    - Valid entry status
    - Identity matching the booking
- Check-in is completed instantly without photocopying passports or manual form filling

3.11 Verified Online Seller to Prevent Marketplace Fraud

- Ploy wants to buy a product from an online seller on a marketplace; she is concerned about scams and fake sellers
- The e-commerce platform requires sellers to present a verified business credential
- The seller shares a verifiable credential proving:
    - Business registration
    - Verified identity
- Ploy sees a "verified seller" badge backed by cryptographic verification (not just platform claims)

- When Ploy proceeds with the purchase:
    - The platform verifies the seller's credential in real time
    - Confirms it is issued by a trusted authority (e.g. DBD)
- Ploy completes the transaction with confidence that the seller is legitimate

4 Evidence of impact

International evidence shows that digital identity wallets and verifiable credentials can deliver substantial economic, administrative, and security benefits. Across jurisdictions, impact assessments and real-world implementations consistently demonstrate reduced onboarding costs, improved efficiency in service delivery, and lower fraud-related losses. These benefits arise from a fundamental shift from repeated document verification to reusable, cryptographically verifiable data.

4.1 Reduced onboarding and compliance costs

Verifiable credentials significantly reduce the cost and complexity of identity verification and onboarding by enabling data to be issued once and reused across multiple transactions. The European Commission's impact assessment for the European Digital Identity framework estimates that digital identity wallets could generate annual savings for service providers from reduced identification and onboarding costs of €0.68–€1.36 billion in financial services and €1.26–€2.51 billion in eHealth, with additional savings in eCommerce and aviation.[1]

Operational evidence reinforces these findings. A Queensland Government pilot using verifiable credentials for employee onboarding reduced onboarding time from approximately three days to 30 minutes by eliminating repeated verification of identity, qualifications, and background checks.[2] These types of gains are directly relevant to high-friction processes such as KYC, KYB, licensing, and access to finance.

4.2 Reduced fraud and improved security

By replacing documents and screenshots with cryptographically signed credentials, verifiable credentials materially reduce the risk of fraud, tampering, and impersonation. The European Commission estimates that adoption of digital identity wallets could reduce annual fraud-related losses by €0.85–€1.4 billion in financial services and €0.3–€0.6 billion in eHealth.[3]

These benefits are particularly relevant in environments where digital fraud is increasing in scale and sophistication. Verifiable credentials enable a transition from document-based trust—which is inherently vulnerable—to cryptographic verification, where authenticity can be confirmed instantly and reliably.

[1] European Commission (2021), *Impact Assessment Report accompanying the proposal for a European Digital Identity framework* (eIDAS 2.0).
[2] Meeco et al. (Queensland Government pilot), *Workplace Credentials Case Study*.
[3] European Commission (2021).

4.3 Administrative efficiency and productivity gains

Verifiable credentials also reduce administrative burden for both users and service providers by eliminating duplicate processes. The European Commission estimates €350–€400 million in annual savings for citizens from reduced administrative burden.[4]

In the public sector, the UK National Health Service (NHS) Digital Staff Passport demonstrates similar gains. By enabling healthcare workers to reuse verified credentials across institutions, it is estimated to save up to 100,000 days of staff time annually by eliminating repeated onboarding and training requirements.[5] This illustrates the potential for a "tell us once" model in public services, reducing duplication and improving service delivery speed.

4.4 Economy-wide impact and business benefits

At an economy-wide level, the impact of verifiable credentials—particularly through business wallets—can be substantial. A European Commission assessment of business wallets estimates annual net benefits of €46.9 billion at 33% adoption, rising to €116.0 billion at 75% adoption in the first year alone.[6] SMEs are expected to benefit disproportionately, with implementation costs estimated at only 12–24% of direct benefits.[7]

These gains reflect reduced transaction costs, faster access to services, and improved data portability—particularly in areas such as access to finance, regulatory compliance, and cross-border trade.

4.5 Implications for Thailand

While the scale of impact will depend on implementation and adoption, international evidence consistently shows that verifiable credentials reduce costs, improve security, and increase efficiency across both public and private sectors. Given Thailand's strong digital foundations and high adoption of digital services, similar categories of impact can be expected.

Based on rough proportional comparisons with the preceding estimates, annual savings from reduced onboarding, verification, and administrative costs could plausibly reach the tens of billions of THB, particularly across financial services, healthcare, and government service delivery.

[4] ibid.
[5] NHS England, *Digital Staff Passport / Enabling Staff Movement Programme*.
[6] European Commission (2025), *Impact Assessment accompanying the proposal on European Business Wallets*.
[7] Ibid.

In addition, given that online scams and fraud already result in losses of approximately THB 45 billion annually, even a modest reduction enabled by verifiable credentials could translate into several billion THB in avoided losses each year.

Taken together, these indicative estimates suggest that the economic benefits of verifiable credentials are likely to significantly exceed the required public investment, particularly when combined with broader productivity gains, improved service delivery, and increased trust in the digital economy.

5 Policy Recommendations

The following five recommendations set out the decisive steps needed to realize the High-level Objective of establishing Thailand as ASEAN's leading digital trust economy — empowering citizens and residents to share their data on their own terms and giving businesses the digital trust infrastructure to grow at home, across the region, and globally.

5.1 Formally establish a National Verifiable Credential Trust Framework

Context: Thailand has built strong technical and institutional capacity in digital identity and verifiable credential architecture. However, these capabilities operate under separate governance arrangements and rely largely on voluntary alignment. As adoption grows, interoperability, portability, and consistent acceptance cannot be guaranteed without enforceable rules. The next phase of reform must therefore focus on legal authority, mandated standards, and coordinated oversight to enable scalable, nationwide adoption.

Action: The Government should formally establish a National Verifiable Credential Trust Framework through a Cabinet Resolution, mandating cross-ministry participation.

ETDA is best placed to administer and supervise the framework including the assurance and accreditation of participating entities such as credential issuers,[8] wallets,[9] and verifiers[10].

In the future ETDA's roles may be enshrined in law through an update to the Electronic Transactions Act inspired by the UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services[11] serve as a reference framework for developing relevant laws and standards in alignment with international best practices.

The Trust Framework should:

- Define enforceable governance roles and responsibilities for relevant agencies, covering policy, oversight, certification, and implementation support.

[8] Credential issuers are government agencies or authorized organizations that issue cryptographically signed digital credentials to citizens or businesses. For example, DOPA issuing a national ID credential or DBD issuing a business registration credential.
[9] Wallets are accredited digital applications that citizens and businesses use to store, manage, and present their credentials. For example, ThaID or Thang Rath.
[10] Verifiers are public or private sector services that request and cryptographically verify credentials presented by a citizen or business. For example, a bank verifying a customer's identity or a government agency verifying a business license.
[11] UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services (MLIT). See: https://uncitral.un.org/en/mlit.

- Mandate adherence to a National Interoperability Profile.
- Establish wallet and other accreditation requirements.
- Require interoperability and portability across accredited systems.
- Define levels of assurance for credential issuance.
- Provide supervisory and enforcement authority, including through a dedicated committee under the National Board of Digital and Society.
- Define liabilities, redress and dispute resolution for all relevant agencies, service providers, and users.

5.2 Develop and rationalize the wallet ecosystem

Context: Thailand has achieved large-scale adoption of digital identity, payments, and service applications, demonstrating strong innovation and public trust. However, overlapping citizen identity and wallet functions across government-backed apps, financial institutions, SOEs, and private providers are increasing integration complexity and potentially duplicating public investment. Without enforceable interoperability and portability requirements, credentials risk remaining confined within closed ecosystems, limiting nationwide adoption and cross-sector reuse. Meanwhile, no business wallet currently exists for juristic persons, including to act as a digital identity and to store key credentials such as business licenses.

Action: The Government should introduce a two-tier wallet accreditation system as part of the Trust Framework, categorized into (1) individual wallets and (2) juristic business wallets. All wallets operating within the ecosystem must be accredited to meet technical, security, functionality, and governance standards.

To optimize public investment, the number of government-designated wallet providers shall be limited to a maximum of two for each category ((1) individual wallets and (2) juristic business wallets). This limitation ensures efficient use of public resources, maintains a consistent user experience, and preserves the integrity and public trust conferred by government endorsement. Designation of government-backed wallets does not preclude agencies from operating their own wallets for specific use cases.

All other accredited wallets may operate competitively within the ecosystem without preferential integration, encouraging private sector innovation, healthy competition, and a diverse range of wallet solutions. Furthermore, these wallet functions may be integrated into existing popular mobile applications, eliminating the need for standalone solutions.

The wallet accreditation system should:

- Require any application storing or presenting government-recognized credentials to comply with the Trust Framework and obtain accreditation.

- Mandate interoperability and portability across accredited wallets.
- Define clearly the process for identity verification and the rules for issuance of identity credentials under the Trust Framework.
- Develop a shared conformance testing capability to support wallet accreditation and interoperability.
- Designate up to two government-backed citizen document wallets[12] and up to two government-backed business wallets to ensure efficient public investment. Government agencies may also operate their own wallets for their own services or credentials.
- In the case of business wallets, these should support legal entity credentials, delegated authority models, and a broad set of business credentials—including licenses and financial standing—enabling secure representation of companies in digital transactions.

5.3 Mandate issuance of foundational verifiable credentials and acceptance across government and regulated sectors

Context: Government datasets are largely digitalized and of reliable quality. However, two structural challenges must be addressed to scale verifiable credentials.

First, acceptance of verifiable credentials is not mandated. Unless public services and regulated sectors are required to recognize compliant verifiable credentials including the selective disclosure of specific data attributes—implementation will remain fragmented, and adoption will likely stall. This is particularly critical in areas where existing regulations mandate the submission of full documents, even when only specific data points are required for verification.

Second, implementation capability needs to be built. Most agencies do not yet have the budget or infrastructure to issue verifiable credentials. Therefore, a systematic support mechanism must be established to enable relevant agencies to issue, utilize, and accept VCs in a secure, reliable, and standardized manner.

Action: The Government should mandate issuance and acceptance of verifiable credentials and establish dedicated funding and shared infrastructure to support implementation.

Specifically, the Government should:

- Propose that the Cabinet mandates agencies responsible for issuing foundational, high-volume verifiable credentials—including DOPA (identity), DBD (business registration), DLT (driving license), MHESI (higher education),

[12] One is likely to be Thang Rath, given its wide adoption and its current role as a government 'Super App'. Other candidates include ThaID and Pao Tang.

and MoPH (health credentials)—to prioritize issuance of verifiable credentials aligned with the Trust Framework. These foundational credentials should be prioritized due to their high transaction volume and ability to be reused across multiple services.

- Propose that the Cabinet designate the Bureau of the Budget, the Digital Government Development Agency (DGA), and other relevant agencies to provide necessary support to DOPA to implement the Person Identification Data (PID) Issuer for use as the primary identity credential in the Trust Framework. This may include prioritizing additional budget for the PID Issuer implementation.

- Propose that the Cabinet mandates all public agencies to accept compliant Verifiable Credentials (VC) as legally equivalent to physical documents. Furthermore, the Cabinet should formally recognize credentials issued under the Trust Framework as legally valid electronic documents, particularly for private sector adoption. This measure aims to foster trust, facilitate acceptance, and streamline the verification of digital credentials across public agencies, businesses, and all relevant service users.

- Establish a formal monitoring process to provide guidance and drive the implementation of agency projects in alignment with the national framework. This could be overseen by the Digital Infrastructure Committee under the Ministry of Digital Economy and Society (MDES), potentially by forming a dedicated "VC Sub-committee".

- Coordinate with the Bank of Thailand and other sector regulators to enable standards-based acceptance in regulated sectors, such as finance, healthcare, education, and professional licensing.

- For larger and higher capacity agencies, establish a dedicated Verifiable Credential Implementation Fund, managed by the Digital Government Development Agency (DGA), to allocate budget for system integration, data preparation, legal alignment, and operational changes required under the Trust Framework for issuance and verification. Dedicated funding is required as most agencies currently lack the infrastructure and capacity to issue and verify credentials at scale.

- For smaller and less technically capable agencies, develop a National Credential Issuance capability within the Government Data Exchange (GDX)—leveraging GDX's existing connections across government to enable agencies to issue verifiable credentials without building bespoke systems.

- Develop a universal verifier SDK or application for government agencies—enabling compliant verifiable credentials to be verified across all public services and government interactions at scale.

- Publish an open reference architecture and conformance testing tools to enable organizations to develop their own standards-compliant verifier applications under the Trust Framework.

5.4 Prioritize five high-impact use cases

Context: To generate momentum and drive adoption, early efforts should be concentrated on use cases with high visibility and measurable impact. Delivering these use cases will require coordinated policy and regulatory adjustments, targeted investment, and active engagement with public and private stakeholders. Clear early wins are essential to demonstrate value, justify funding, and accelerate broader implementation.

Action: The Government should designate up to five national priority use cases for accelerated implementation under the Trust Framework, with clear accountability, defined timelines, and measurable performance indicators. The selection and implementation of priority use cases should explicitly assess inclusion impacts, particularly for women and populations with limited connectivity and/or low digital literacy, and include indicators to monitor adoption and outcomes across these groups. These use cases should be anchored in the foundational verifiable credentials prioritized under recommendation 3.3. Each priority use case should have a single lead agency responsible for implementation, with OPDC coordinating cross-agency alignment and ETDA providing technical oversight of Trust Framework compliance.

Proposed priority use cases are:

- **Business Access to Credit and Financial Services:** Enable businesses—including MSMEs—to convert verified business registration, tax records, licenses, and financial data into reusable verifiable credentials that support creditworthiness assessment, reduce KYB costs, and accelerate access to finance.
    - **Lead agency:** Ministry of Commerce
    - **Key credentials:** Business registration certificate (DBD), tax compliance certificate (Revenue Department), business licenses (sector regulators e.g. FDA, BOI), financial statements (banks / BOT-regulated entities)
- **Privacy-Preserving Age Verification:** Enable secure proof of age for regulated and online services (e.g., alcohol sales), reducing fraud and regulatory exposure while protecting personal data.
    - **Lead agency:** MDES
    - **Key credentials:** National ID credential (DOPA)

- **Social Welfare Access:** Enable eligible citizens to present verifiable credentials attesting to income, residency, disability, household status, and other claims to streamline enrollment in government welfare programs, reduce administrative burden, improve targeting accuracy, and reduce duplicate enrollment across programs.
    - **Lead agency:** Ministry of Finance
    - **Key credentials:** Welfare card / entitlement credential (MOF), income verification (Revenue Department), household registration (DOPA), among others
- **Health Credential Portability:** Enable secure, patient-controlled health credentials to reduce administrative burden and improve continuity of care across providers.
    - **Lead agency:** MOPH
    - **Key credentials:** Health insurance entitlement (NHSO), vaccination and immunization records (MOPH), medical history summary (hospitals / MOPH-accredited providers)
- **Driving, Professional, and Academic Credentials:** Enable interoperable digital driving licenses, professional licenses, and educational qualifications to support employment, mobility, and cross-border recognition. For example, medical professional license verification during telemedicine services and using a driving license to rent a car overseas.
    - **Lead agency:** MDES
    - **Key credentials:** Driving license (DLT), professional licenses e.g. medical, nursing, engineering (relevant professional councils), academic transcripts and degree certificates (universities / MHESI)

5.5 Lead ASEAN in Developing Regional Standards

Context: ASEAN digital integration under DEFA will be accelerating, yet regional standards for trusted digital identity and cross-border data exchange are still emerging. Countries that establish enforceable national frameworks early will influence technical standards and mutual recognition arrangements. By moving early, Thailand can shape regional norms to support its trade priorities, strengthen integration, attract investment, and position itself as a provider of expertise and infrastructure across ASEAN.

Action: The Government should actively advance verifiable credentials as a regional priority through ASEAN digital and economic cooperation bodies.

Specifically, Thailand should:

- Pursue bilateral and trilateral pilot initiatives with ASEAN Member States (AMS) on use cases with high demonstration effect, such as driving licenses with Malaysia and Singapore.
- Champion verifiable credentials through ASEAN Digital Ministers’ Meetings (ADGMIN) ASEAN Economic Ministers (AEM) and related working bodies— — proposing formal recognition within DEFA's digital identity, authentication, and data sharing pillars, advocating for mutual recognition of credentials issued under aligned national trust frameworks, and promoting convergence on standards.
- Propose regional pilot initiatives in high-value areas aligned with DEFA pillars and Thailand's National Trust Framework—such as trade document digitalization, cross-border business identity (UBIN), professional credential recognition, and health credential portability for mobility and travel.
- Offer Thailand as a regional center of expertise—sharing technical expertise and reference architectures with AMS, and creating opportunities for Thai technology firms to export solutions and services across the region.
- Lead discussions on cross-border interoperability with countries and blocs beyond ASEAN—such as the European Union, the United Kingdom, and South Korea—positioning Thailand as a bridge between ASEAN and global trust frameworks.

6 High-level strategic plan

The Trust Framework should be implemented in phased manner and building on the work already undertaken by ETDA and its Verifiable Credentials Working Group. The objective is to move from technical framework development and testing to enforceable governance and national-scale deployment.

6.1 Phase 1 (2026): Formalization and Regulatory Consolidation

Focus: Formal legal establishment, enforceability, and scaling of existing technical foundations.

Building on ETDA's prior development of the VC data structure recommendations, interoperable wallet framework, working group outputs, and conformance testing tools, Phase 1 should focus on giving these foundations formal authority and cross-government mandate.

Key actions:

- Issue a Cabinet Resolution formally recognizing the National Verifiable Credential Trust Framework, mandating cross-ministry participation, and recognizing credentials issued under the framework as legally valid electronic documents.
- Publish and formalize the National Interoperability Profile based on ETDA's existing interoperability framework and conformance testing work.
- Operationalize wallet and issuer accreditation, including pre-release and audit mechanisms already developed, such as the audit checklist which will be completed by September 2026.
- Establish a Verifiable Credential Implementation Fund, managed by DGA, to provide budget to government agencies, beginning in 2027 as part of the annual budget setting process.
- Develop a National Credential Issuance capability within the Government Data Exchange (GDX) and Verifiable Data Registry (VDR) for government agencies.
- Develop Thang Rath as a national wallet for citizens and SDK for universal verifier enabling compliant verifiable credentials to be verified across all public services. Initiate coordination with the Bank of Thailand and other regulators to align sectoral acceptance frameworks.
- Define criteria for the selection of high-impact national use cases based on volume of use, user need, the end-to-end nature of services, how they demonstrate the value of core digital credentials (e.g. ID credential), and where complexity dropout rates or fraud can be reduced.

- Pursue bilateral and trilateral pilot initiatives with ASEAN Member States on high-demonstration use cases, such as driving license recognition with Malaysia and Singapore.
- Initiate public engagement to increase awareness of verifiable credentials and the opportunities that they present for citizens and businesses.
- Initiate central and local government engagement to increase awareness of verifiable credentials and to ensure that all government agencies are able to prepare for potential future acceptance of credentials.
- Establish a committee under the National Board of Digital and Society responsible for supervision and monitoring of the implementation plan, including making policy decisions required. The Committee should include stakeholders engaged in policy and implementation of the Trust Framework. ETDA would provide the secretariat for the Committee.

Outcome of Phase 1:

A legally enforceable trust framework built on ETDA's technical groundwork, with accredited participants, recognized standards, identified wallet providers, and shared issuance capability ready for scaled implementation.

6.2 Phase 2 (2027): Institutional Adoption, Priority Use Cases, and ASEAN Leadership

Focus: Mandated issuance, mandated acceptance, and operational deployment.

Key actions:

- Confirm priority high-impact national use cases based on criteria defined during Phase 1.
- Direct priority issuing agencies (DOPA, DBD, DLT, MHESI, MoPH) to issue verifiable credentials aligned with the Trust Framework.
- Implement mandated acceptance across public services starting with priority use cases and setting a deadline for acceptance to enable adoption by all other public sector service providers during phase 3.
- Provide tools to enable service providers and credential issuers to implement services, including clear guidance, open-source reference architectures, and compliance sandboxes (for the development of new issuers and relying party services).
- Operationalize financial sector acceptance through coordination with the Bank of Thailand.

- Deploy the designated high-impact national use cases: business access to credit and financial services, privacy-preserving age verification, ASEAN trade credentials, proof of medical certification or referral to another facility, and driving, professional, and academic credentials.
- Expand conformance testing and audit mechanisms to ensure compliance.
- Launch specific public awareness and stakeholder engagement initiatives including emphasis on high-impact national use cases.
- Establish agency-level KPIs for VC acceptance rates and service processing time reductions, reported to the National Board of Digital Economy and Society, to ensure accountability for adoption targets.
- Initiate ASEAN-level pilot programs under DEFA in trade, finance, mobility, and travel.
- Advocate for mutual recognition of credentials across ASEAN.

Outcome of Phase 2: Verifiable credentials move into live operational use across priority sectors and Thailand plays a leading role in shaping ASEAN digital identity and trusted data exchange frameworks.

6.3 Phase 3 (2028-2029): National Scale and ASEAN Implementation

Focus: Full deployment, enforcement, sustainability, and regional operationalization.

Key actions:

- Expand issuance and acceptance across additional agencies and regulated sectors.
- Conduct periodic compliance audits and enforce interoperability and accreditation requirements.
- Scale the GDX-integrated issuance platform for nationwide use.
- Operationalize a sustainable commercial and accreditation model for long-term ecosystem governance.
- Expand private-sector integration across finance, telecommunications, education, and high-volume digital services.
- Implement ASEAN-level mutual recognition arrangements and integrate verifiable credentials into cross-border trade and mobility systems.
- Conduct national public awareness and adoption campaigns.

Outcome of Phase 3: Thailand operates a fully enforceable, interoperable credential ecosystem at national scale, with sustainable governance and active cross-border recognition within ASEAN.

6.4 Phase 4 (2030-2032): Sustainability and potential commercialization

Focus: Ensuring that the trust framework is fully sustainable moving forward by implementing commercial models for credential issuance and use outside of the public sector.

Key actions:

- Consider charging support or maintenance fees for government agencies or cross-billing for government access to the trust framework.
- Define a hybrid approach for cost recovery of trust framework operation whilst incentivising high-quality data source and service participation. This should balance the requirements of the core participants, for example:
    - Issuers - motivated by cost recovery or new revenue for providing high-quality, "signed" data.
    - Users / Businesses - motivated by better service provision and reduced administrative burden.
    - Verifiers (Relying Party Services) - motivated by reduced fraud, automated KYC/B compliance, and lower operational costs.
- Implement monitoring of sustainability metrics to monitor the health of the commercial model. For example: Cost per Verification, Credential Velocity (how many times a single VC is reused - higher velocity = higher ROI for the Issuer), Verifier Onboarding (growth of private companies using the system).
- Implement privacy-first billing – that avoids the risk of billing mechanisms becoming a tracking mechanism.

Outcome of Phase 4: The trust framework becomes fully sustainable at national scale and is able to provide for growth in use of verifiable credentials within the public and private sectors.

6.5 Summary of roles and responsibilities

Successful implementation of this strategic plan requires cross-agency collaboration, at least among the following entities:

- **Ministry of Digital Economy and Society (MDES):** Provide overall policy direction and political oversight for the verifiable credential ecosystem, including representation at Cabinet level, ensuring alignment with national digital economy strategy and coordination across implementing agencies.
- **Electronic Transactions Development Agency (ETDA):** Lead the design, governance, and enforcement of the national verifiable credential trust framework, including standards, accreditation, interoperability, and cross-border alignment.
- **Office of the Public Sector Development Commission (OPDC):** Coordinate cross-government implementation by identifying priority services, aligning agencies, and ensuring verifiable credentials enable integrated digital public service delivery under the *Act on Carrying Out of Public Service via Electronic Means* B.E. 2565 (2022).
- **Digital Government Development Agency (DGA):** Enable adoption and scale across government by integrating verifiable credentials into public services, developing shared issuance capability within the Government Data Exchange (GDX), managing the Verifiable Credential Implementation Fund, and operating Thang Rath as a government-backed digital wallet and verifier. DGA has the capability to provide both a GDX Issuer for the issuance of Verifiable Credentials from government datasets, but also to provide a Universal Verifier through Thang Rath to enable anyone with the App to verify a verifiable credential issued under the Trust Framework, as well as a universal verifier software development kit (SDK). For many government agencies already integrated with Thang Rath this capability would also dramatically reduce the overhead of issuing VCs for those agencies.
- **Department of Provincial Administration (DOPA):** Issue foundational identity credentials for individuals based on the national population registry, and support storage and use through the ThaID wallet, serving as the root of trust for natural person identity.
- **Department of Business Development (DBD):** Issue high-assurance juristic person identity credentials for registered companies, including legal status, registration data, and authorized representatives.
- **Revenue Department (RD):** Extend coverage of juristic person identity credentials and issue economic and tax-related credentials, including for SMEs and unincorporated businesses not covered by DBD.

The table below further describes the roles they would assume based on the 3 phases.

Responsibility	Phase 1 (2026): Formalization and Regulatory Consolidation	Phase 2 (2027): Institutional Adoption, Priority Use Cases, and ASEAN Leadership	Phase 3 (2028-2029): National Scale and ASEAN Implementation
Foundational credential issuer	DOPA DBD/RD DLT		
Priority Use Case Selection	ETDA OPDC DGA		
Credential Schema Maintenance	ETDA DGA	ETDA DGA	ETDA DGA
Other credential Issuer		MoPH MHESI MoPH	MoPH DLT MHESI MoPH + Others to be determined
Service Provider (Verifier)	DOPA DGA	Priority Use Cases	Priority Use Cases Other Government Agencies Banks (for KYC) Private Sector
Supporting Infrastructure Provider	DGA – GDX Issuer DGA – Thang Rath Universal Verifier DGA / ETDA – Common Trust Infrastructure	DGA – GDX Issuer DGA – Thang Rath Universal Verifier DGA / ETDA – Common Trust Infrastructure	DGA – GDX Issuer DGA – Thang Rath Universal Verifier DGA / ETDA – Common Trust Infrastructure
Governance	Council of Ministers – Cabinet Resolution (through the Ministry of Digital Economy and Society) ETDA BOT – sectoral acceptance	ETDA BOT (finance sector acceptance) OPDC (public sector acceptance) MoPH (health sector acceptance)	ETDA BOT (finance sector acceptance) OPDC (public sector acceptance) MoPH (health sector acceptance) + Others to be determined
Public Awareness	OPDC ETDA	OPDC ETDA	OPDC ETDA

	Sectoral Regulators	Sectoral Regulators	Sectoral Regulators
Government Awareness	OPDC ETDA	OPDC ETDA	OPDC ETDA
Redress Mechanism	OPDC ETDA	OPDC ETDA	OPDC ETDA

7 Estimated budget needs for Phase 2 (2027)

Indicative financing requirements for Phase 2 are modest relative to the scale of impact and can be delivered through a combination of shared infrastructure and targeted agency-level investments.

The primary cost drivers are the development of a national credential issuance capability, integration of authoritative data sources within priority agencies, and ecosystem enablement (including verifier integration, awareness, and capacity building). A centralized issuance approach—where smaller agencies leverage a shared platform for turning their data and documents into compliant verifiable credentials—can significantly reduce duplication and overall cost.

On this basis, a realistic financing envelope for Phase 2 is estimated at approximately THB 430 million to THB 1.1 billion, which can be sequenced over 1-2 fiscal years. **This amount covers the core of the ecosystem and a limited number of issuers—it doesn't represent the full costs of the whole ecosystem, particularly a large range of issuers.**

For most additional issuers, implementation costs are expected to be modest, primarily involving integration, data standardization, and minor process adjustments. These can typically be absorbed within existing agency budgets, particularly where shared infrastructure and common issuance services are leveraged.

Component	Description	Estimated Cost (THB)
Central shared infrastructure	National issuance platform (integrated into GDX), trust registry integration, conformance testing, developer tools	180 - 360 million
Wallet development or enhancement[13]	Credential storage, presentation, consent flows, verifier interface, security enhancements	40 - 120 million
DOPA (identity credentials)	Core ID credential issuance, integration with civil registry and ThaID, highest assurance and scale requirements	60 - 140 million

[13] Development or enhancement of up to two designated citizen wallets and up to two designated business wallets, alongside accreditation support for additional private sector wallets. Costs include credential storage, presentation, consent flows, verifier interface, and security enhancements, among others.

Other priority issuing agencies (4-5)	Integration with databases, data standardization, process redesign, security and compliance	140 - 360 million (total)
Ecosystem enablement	Verifier integration support, awareness campaigns, technical assistance and capacity building	70 - 180 million
	Total indicative envelope	**490 million - 1.16 billion**

These financing estimates are indicative and intended to provide an order-of-magnitude view of potential resource requirements rather than precise budget figures. Actual costs will depend on a range of factors, including the final scope of use cases, the maturity and quality of existing agency systems, procurement approaches, and the degree to which shared infrastructure is leveraged versus agency-specific development. These estimates should therefore be refined during Phase 1 through detailed technical assessments, implementation planning, and engagement with key agencies and technology providers, including validation of system integration needs, data readiness, and operational requirements.

Annex A – Background

A.1 The drivers for change

Multiple solutions that do not interoperate or follow recognized standards. There are currently multiple government wallets and multiple digital identity solutions, but credentials are not portable from one system to another, at a technical level they do not interoperate well, and citizens are left needing multiple solutions when one would suffice.

Fraud and scams continue to plague citizens and the state. Fraud, scams, and cybercrime continue to plague Thai citizens and businesses with online attacks amounting to substantial financial losses of approximately 45 billion baht over 2023 and the first half of 2024. The advent of AI-assisted identity theft is compounding this risk.

Opportunity is being missed. Digital ID and trusted credentials are being underutilized due to a lack of compelling use cases. Elsewhere inefficient and potentially unsafe processes remain reliant on paper copies of ID where digital equivalents would save time and resources. Priority use cases should be identified to realize this missed opportunity, for example:

- ***Ease of doing business*** – simplifying regulatory processes for business creation and operation without reducing trust.
- ***Regulatory compliance*** – providing reliable and safe methods for citizens to provide proof of age, for example, supporting the sale of age restricted goods online.
- ***Health Care*** – supporting the portability of health records when moving from one healthcare provider to another by centering records around the patient rather than embedding them in incompatible or siloed hospital system.
- ***Regional cooperation*** – enabling citizens to prove their ability to drive in other ASEAN countries, apply for jobs or attend higher education by providing digital proof of educational attainment, or to participate in digital cross-border trade.

Regional competition and ASEAN policy points towards greater digital collaboration. Providing the tools for Thai businesses to compete regionally and internationally is vital for future trade growth. Cross-border use cases provide opportunities for Thai citizens to work, be educated, and travel more freely across the region.

Trust frameworks for issuance and use of digital credentials are becoming increasingly important for international cooperation. International trends and the use of verifiable digital credentials in multiple jurisdictions are becoming an expectation rather than an aspiration (e.g. the EU, Brazil, Korea, Bhutan, and the USA). Trust frameworks for international trade and business identity are increasing in prominence e.g. African Union, EU, and potentially ASEAN.

A.2 The need for strong governance and clear accountability

In order to maintain trust in the Verifiable Credential ecosystem a robust governance regime will be required to ensure standards, policies and procedures are correctly implemented and maintained through activities such as: Oversight, Compliance & Audit, Organizational Certification or Accreditation, Enforcement, and Dispute Resolution.

A Trust Framework should be established that defines the roles and responsibilities of each participating entity, the legislative environment under which the trust framework operates, and specific requirements and technical specifications that apply to entities and functional elements of the trust ecosystem. This may include certification requirements or technical assessment regimes to which certain entities must comply in order to operate and be trusted by other entities in the ecosystem.

Entity	**Key Responsibilities**
Trust Framework Authority	The entity that defines and maintains the Trust Framework, including its scope, participation rules, assurance levels, accreditation criteria, interoperability requirements, liabilities rules and applicable standards. The Authority establishes the policy, legal and technical rules under which issuers, wallet providers, verifiers, and accreditation organizations may operate. Given ETDA's responsibilities under the Electronic Transactions Development Agency Act (2019) it is recommended that ETDA assume the role of Trust Framework Authority.
Trusted Accreditation Organization	An entity that accredits or certifies entities to denote that they are reliable issuers of certain credentials. For example, the Ministry of Education might certify that a specific university is authorized to issue Educational Transcripts as Verifiable Credentials.
Auditors / Conformity Assessment Bodies	Independent entities responsible for assessing whether wallet providers, issuers, verifiers, and accreditation organizations comply with the requirements of the Trust Framework. Auditors conduct conformity assessments against published criteria and standards and provide assurance reports to the Supervisory Body.

	Auditors must be accredited under recognized accreditation arrangements and operate independently of the entities they assess. ETDA could act as the primary certification body able to verify that Trusted Accreditation Organizations, Wallet Providers, Issuers, and Verifiers are following the rules laid out in the Trust Framework, with other private sector auditors being introduced in the future.
Supervisory Body	The Supervisory Body is responsible for overseeing the proper functioning of the verifiable credential ecosystem and enforcing compliance with the Trust Framework. This includes monitoring accredited participants, reviewing audit outcomes, handling non-compliance, applying corrective measures or sanctions, and coordinating dispute resolution and redress mechanisms. Given ETDA's responsibilities under the Electronic Transactions Development Agency Act (2019) it is recommended that ETDA assume the role of Supervisory Body.

A.3 Building scalable and resilient National Digital Infrastructure

Digital Identity and trust infrastructure required to issue and verify credentials once established will soon become critical national infrastructure: if it stops working or is no longer trusted then all of the services that rely upon it will cease to be trusted.

Adopting a decentralized approach to Digital Identity and Verifiable Credential issuance and use removes the reliance on monolithic centralized registries for government data, provides citizens with greater controls over the use of their data, and removes the need for relying party services providers to integrate directly with government systems.

Issuers of credentials need to provide high quality data that is trusted and secure from recognized registries. And when issuing verifiable credentials Issuers must ensure that those credentials are cryptographically signed to ensure transactional trust as well as organizational trust. Issuers must also ensure that credentials are issued to the correct entity by performing identity verification as needed.

Verifiers of credentials (relying party services or entities), need to understand which issuers are trusted (for example via a trust list), and have access to data schema that describe the type of data they may request from holders of credentials issued under

the ecosystem. Verifiers will also need access to tools to enable them to verify the validity and integrity of credentials, to check that they have not been tampered with, and to determine if they have been shared by an entity to which the credential was issued (e.g. Alice should only share credentials issued to Alice and not those issued to Bob).

All of this implies a trust infrastructure comprising of not just digital wallets and credential issuers but a whole ecosystem of supporting entities and functions to ensure that trust is maintained. For example:

Entity	**Function / Responsibility**
Users of Digital Wallets	Citizens and residents in control of a recognized digital wallet solution responsible for the sharing of credentials in those wallets with relying parties.
Wallet Provider(s)	Organizations either mandated or recognized by the State to develop and make available to Users a digital wallet solution (e.g. an App). Wallet Providers are responsible for the secure storage, protection, and presentation of credentials, including key management and holder binding, in accordance with Trust Framework requirements. Note: Wallets may be required to be accredited if specified in the Trust Framework.
Identity Credential Provider(s)	Trusted entity or entities authorized under the Trust Framework for the issuance of identity credentials responsible for: • verifying the identity of the User requesting an identity credential, • issuing an identity credential to a digital wallet (belonging to that user), and • making available, in a privacy-preserving way, information for Relying Parties to verify the validity of the identity credential.
Entity Registrar	Enables other entities participating in the ecosystem to register officially and have data about those entities made available online in human-readable and machine-readable format to any interested party. Registered entities will be placed on the relevant trusted list under the trust framework.

Trusted List Provider	A body responsible for maintaining, managing, and publishing a Trusted List of entities e.g. Identity Credential Providers, Wallet Providers. An entity's status as a ‘trusted’ entity can be verified by checking whether they are present on the relevant Trusted List.
Issuers of Credentials	Entities authorised to issue verifiable credentials to identified Users (and their wallets) under the rules of the trust framework. Issuers may be operated by an Authoritative Source or may simply issue credentials deriving data from authoritative sources under agreement.
Registries (Authoritative Sources)	Public or private repositories or systems, recognized or required by law, containing attributes about individual persons or entities. For example: civil status, family composition, nationality, education / training qualifications, professional licenses, public permits & licenses, business registration data.
Relying Parties (Services)	A service provider (in person or through a digital services) requesting specific attributes contained in one or more credentials shared by a Holder (under applicable consent) from a recognized wallet. Relying Parties are responsible for verifying credential authenticity, integrity, issuer trust status, and holder binding using the trust infrastructure.
Supervisory Body	The Supervisory Body is responsible for overseeing the proper functioning of the verifiable credential ecosystem and enforcing compliance with the Trust Framework. This includes monitoring accredited participants, reviewing audit outcomes, handling non compliance, applying corrective measures or sanctions, and coordinating dispute resolution and redress mechanisms.
Attribute Schema Providers	Publish attribute schemas describing the structure of Credentials and how they may be utilized by Relying Parties.

A.4 Scope of the Trust Framework

The requirements for Governance and National Digital Infrastructure based on the implementation of a verifiable credential ecosystem described in the preceding sections imply the need for an overarching Trust Framework.

Trust Frameworks enable trust to be fostered between the various parties in an ecosystem through the establishment of a set of rules and governance arrangements that all parties agree to observe.

To facilitate interoperability, one entity must be able to trust another entity based not just on the integrity of technical processes (e.g. cryptographic proof), but also regarding the provenance of the data being shared (e.g. the processes for its collection and for attributing a certain record to an individual). These trust frameworks focus more on governance, process and accountability than technology; technology is simply an enabler. Therefore, a robust trust framework should clearly define the Business (e.g. scope, services provided, requirements for participation, including the eligibility, criteria and assessment process, and ongoing compliance obligations for wallet providers, including differentiated requirements for accredited wallets and designated wallets); Technical (e.g. data formats, interfaces, standards); Operational (e.g. how identity proofing and authentication work, support, communications); and, Legal (e.g. service levels, liability, dispute resolution) requirements for the identity system and data sharing elements (e.g. verifiable credentials).

The Trust Framework shall explicitly support inclusive access models to ensure that lack of smartphones, connectivity, or digital literacy does not exclude individuals from accessing public services.

The Trust Framework shall also define how legal authority, mandate, and delegation are represented and managed using verifiable credentials, including the rules for issuing, delegating, limiting, and revoking authority for legal persons acting through natural persons.

A.4.1 Roles within the Trust Framework

The roles within a trust framework range from lawmakers to end users and others who may fulfil governance, policy, assurance and operational functions. In the trust framework envisaged in this white paper the following roles and high-level responsibilities would be expected.

Role / Entity	Responsibility
Framework Operator	• Defines and maintains the Trust Framework, including the rules for participation, assurance requirement, governance arrangement. • Oversees and enforces compliance with the Trust Framework, including the application of penalties or

	restrictions where participating entities are in breach of the framework agreement.
Credential Issuer	• Issues verifiable credentials in accordance with the trust framework specifications and standards. • Ensures that recipients of credentials are verified before issuance and that data shared in those credentials are attributed reliably to the entity making the request. • Utilizes a private key associated with the issuer for the purpose of signing credentials and that shared trust infrastructure (as defined by the trust framework) is updated to enable the verification of credentials once issued.
Wallet Provider	• Ensures that accredited wallet apps remain compliant with the requirements of the trust framework. • Ensures that wallet apps are available, accessible, and reliable.
Service Provider (credential Verifier)	• Follows the principles of data minimization by only requesting credentials that are required for the requested service delivery. • Verifies the integrity of received credentials by checking the cryptographic proof contained within those credentials, and the validity of the credential based on metadata and applicable revocation mechanisms (provided by the trust infrastructure). • Observes applicable national and international law with regards to data protection and cybersecurity.
Trust Infrastructure Operator	• Where operating a key element of the trust infrastructure such as a CA, Trust List, or Verifiable Data Registry, ensures that that asset is protected, available, and reliable in the scope of the trust framework.
End-User (e.g. Citizen)	• Is responsible for protecting the digital document wallet and the credentials it contains by maintaining strong authentication to the wallet and to the device where the wallet is installed. • Responsible for providing consent for the sharing of data from credentials with accredited Service Providers.

A.5 Ensuring that credentials are trusted and that security is maintained

Ensuring the safety and security of Verifiable Credential ecosystems requires a multi-layered approach that encompasses technical trust (cryptographic proof), information security (including data integrity, and privacy concerns), and cybersecurity (ensuring systemic defense and resilience).

Verifiable Credentials typically exist in an ecosystem that supports the issuance, sharing, and verification of those credentials by entities known as Issuers, Holders, and Verifiers (of credentials). The diagram below describes this model and the critical role that digital wallets play as the 'holders' of credentials and the orchestration point for the sharing of credentials by users.

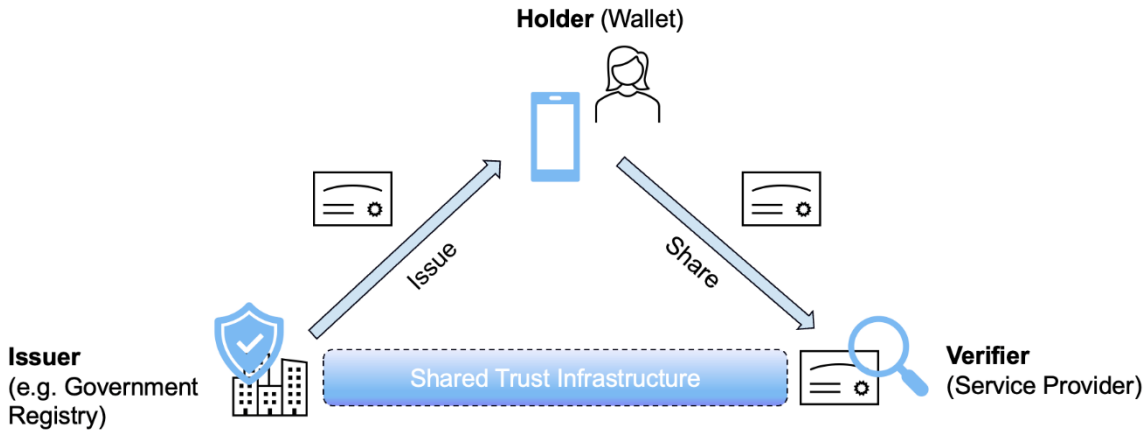


Figure 2 - the decentralised model for verifiable credentials

Technical Trust – Verifiable Credentials contain a cryptographic proof created by the Issuer of the credential that should be used to check that the credential has not been tampered with and (by means of revocation mechanisms or status lists) that the credential has not been revoked. When shared from a trusted wallet a Verifiable Presentation is also created that includes a Holder Binding Proof enabling the Verifier to also check that the credential(s) received have been presented by their legitimate owner (i.e. the entity to which they were issued).

Under the Trust Framework architecture this is to be managed and maintained by ETDA as the "Trust List," through a "Universal Resolver".

Information Security – Focuses on the Confidentiality, Integrity, and Availability (CIA) of data throughout the credential lifecycle, including when credentials are requested, stored, and shared by Holders, and with respect to data protection and privacy requirements. Credentials in transit are always transmitted over secure channels (e.g. HTTPS) to ensure confidentiality, whilst the credentials themselves are cryptographically signed to ensure integrity.

Cybersecurity – Issuers, Verifiers and trust infrastructure providers are individually responsible for protecting their systems and assets from compromise and for ensuring resilience. Wallet apps and cloud-based business wallets should utilize appropriate key-management and secure-enclave or HSM-based protections where required by assurance level and ensure that access controls and user authentication mechanism are appropriate for the sensitivity of the credentials and data they protect.

Liability and accountability - Under the Trust Framework, issuers are responsible for the accuracy, lawful issuance, and timely status management (including revocation or suspension) of credentials. Wallet providers are responsible for the secure storage, protection, and correct presentation of credentials, including holder binding and authentication, but are not responsible for the substantive correctness of credential content. Verifiers and relying parties are responsible for lawful, proportionate, and purpose limited use of credential data, including compliance with applicable data protection and cybersecurity obligations. The Trust Framework shall define redress and dispute resolution mechanisms and empower the Supervisory Body to investigate incidents, mandate corrective actions, and enforce compliance where failures or misuse occur.

A.6 Selecting high-impact national use cases

The selection of high-impact national use cases should be based not only on their obvious importance or high-volume use (e.g. sharing regularly used government documents such as national ID, and driving license), it is important to also consider user-centric needs, inclusive access, and the potential for digital service transformation creating better more usable and engaging public services.

Criteria	Approach
High-Volume Impact	Prioritizing services with the highest number of users or transactions to maximize the impact of digitization.
User-Centered Research	Using data and user feedback to identify which services were most needed, rather than relying on internal assumptions.
"Whole Problem" Approach	Selecting services that could be redesigned end-to-end to solve a user's entire need, such as "starting and sustaining a business" or "having a baby".
Strategic Transformation	Focusing on services that demonstrate the value of cross-government platforms e.g. GDX.
Service Transformation	Working with government agencies and their service providers to identify areas with high dropout rates or that would benefit most from service redesign or process re-engineering.

Candidate services that should be considered in additional to those already identified in section 5.4 include:

- Analysis of DGA's 100+ e-document services.
- DBD's Biz Portal and services related to business creation and administration
- Social welfare programmes

For example, if we examine the potential for verifiable credentials to have an impact on social welfare programmes we can already see cross-cutting advantages.

The administrative foundations of many social welfare systems were developed in a predominantly paper-based world reliant on multiple forms of documentation and localized service delivery. As these systems migrate online, they often retain these archaic processes and siloed data repositories which often results in operational overheads and a considerable administrative burden for potential beneficiaries.

By transitioning from centralized, siloed databases to decentralized, user-centric models (i.e. digital wallets and verifiable credentials), social welfare programs can achieve unprecedented levels of efficiency, privacy, and inclusion. These models should explicitly support offline verification, printed verifiable QR codes, and agent-assisted service delivery to ensure accessibility where smartphones, connectivity, or digital skills cannot be assumed. Verifiable credentials provide a standardized, cryptographically secure method for asserting personal attributes—such as identity, income, disability status, or employment history—without the need for intrusive, manual verification processes.

The shift from "institutional reputation" to "cryptographic proof" allows for a seamless, user-centric ecosystem where citizens control their own data and the state can focus its resources on those most in need.

A.7 Improving service integration and data sharing across government

Verifiable credentials and digital wallets are the cornerstones of decentralized ecosystems that change dramatically the relationship government agencies have with other services, inside or outside of government, that utilize their data. Agencies that previously exposed access to their data to other systems through APIs for purposes such as verification, eligibility checking, or service onboarding (e.g. KYC), can now focus on the issuance of key data in the form of verifiable credentials that are held by their customers rather than providing services to a variety of 3rd party systems.

This change in focus for government agencies, from service provider to data provider has a number of advantages for scalability and sustainability:

Change in approach	Benefit
Demand for data is able to scale up and out without additional infrastructure requirements for the data Issuer.	• Users share their data directly with other service providers, under their control and consent, without the need for API calls back to the issuing agency's systems for every transaction. • The link between consumers of agency data and the agency's IT systems is removed meaning that consuming service providers scaling their service dramatically does not mean that government agencies have to scale their systems in reply.
Peaks in load a flatter and not driven by services reliant on agency data.	• As users share more of their data directly peaks in load are seen at the delivery service's systems and not at the data issuer. • Demand on backend systems is flatter and requires less compute time reducing issues related to availability as users will not need to request data as often (as credentials are held in wallets and can be used multiple times with multiple services).
Fewer restrictions caused by proprietary or complex backend systems.	• Developing and maintaining APIs can be expensive where old, proprietary, or complex backend systems are involved. Issuing credentials based on international open standards is a simpler approach and can be achieved with minimal investment due to reduced complexity. • Once operational complexity for the processing of data sits with the end-user or service provider and not the issuing agency.
Interoperability issues are reduced due to the use of open standards.	• Services reliant on agency data integrate with users and their wallets directly to request key data thereby reducing support and interoperability issues as well as the onboarding of API users. • Multiple tools, code libraries, and products (many of which are opensource) can be utilized by the agency to issue credentials to compliant wallets.

A.8 Potential Authoritative Sources of data

The Authoritative Sources of data across government should be confirmed and the operators of these datasets enabled to provide citizens with access to their data in defined verifiable credential formats.

Type	Datasets	Owner
Foundational	National ID, Household Book, Business Certificate	DOPA, DBD
Mobility & Labor	Driving License, Professional License, Degree	DLT, Prof. Councils, Universities
Financial & Legal	Tax Submissions, Credit History, Land Titles	Revenue Dept, NCB, Land Dept
Health & Travel	Medical Certification, Healthcare Referral, Visa Status, Arrival Cards	MOPH, Immigration, SEC

A.9 Key Government Actors

The success of a national VC ecosystem is predicated on the active participation of the government agencies that maintain the authoritative sources of data such as foundational registries. These "authoritative datasets" provide the legal weight to digital credentials, ensuring they are accepted across all sectors of society.

A.9.1 Department of Provincial Administration (DOPA)

As the custodian of the national identity registry and civil registration documents, DOPA is responsible for key foundational datasets in the ecosystem. The ThaiD application, developed by the Bureau of Registration Administration (BORA), has already established a population-scale digital ID system. ThaiD allows citizens to present digital versions of their national ID cards and household books, which are legally recognized as equivalent to physical documents under existing civil registration laws.

A.9.2 Digital Government Development Agency (DGA)

Through the Thang Rath application, the DGA has created a unified portal for citizens to access public services. The DGA's responsibility also includes the development and operation of the Government Data Exchange (GDX) and the establishment of common standards that ensure credentials issued by one agency are readable and verifiable by others.

A.9.3. Thailand Post (Thai Post)

Thailand Post occupies a unique position as a trusted intermediary between the physical and digital worlds. The "Prompt Post" application functions as a secure digital mailbox and document management platform, enabling the trusted sending and receiving of electronic documents. Prompt Post’s integration of electronic signatures and its closed platform for KYC-verified users make it a potential wallet provider, especially for legal documents and business-related registered correspondence that requires high-assurance proof of delivery.

A.9.4 Department of Business Development (DBD)

For the "Business Wallet" component of the ecosystem, the DBD is the critical issuer of legal entity (business identity) credentials. The transition to the "DBD Biz Regist" platform by July 2025 mandates that all corporate registrations and certified document downloads occur digitally. This platform provides the machine-readable data needed to issue "Business Identity Credentials," allowing businesses of all sizes to prove their legal status, director authorizations, and financial standing.

A.9.5 Department of Land Transport (DLT)

The DLT is responsible for regulating road transport, vehicle registration, and issuing driving licenses meaning that it provides some of the most highly used credentials in the Thai economy. The Driving License alone has the potential to be a core verifiable credential (for example providing proof of age) and if aligned with international standards, the basis for cross-border interoperability for Thai drivers when visiting other countries in the region and potentially beyond.

Annex B - Key issues and analysis

B.1 Fraud mitigation and enhanced public security

By replacing physical documents and siloed databases with cryptographic proofs, public and private sector services can move from "guessing" if a user is legitimate to "knowing" with mathematical certainty.

In traditional systems, fraud often starts with a high-quality fake ID or an altered official document (e.g. a photoshopped PDF). Verifiable Credentials eliminate this risk as they are cryptographically signed by the issuer (e.g. a government ministry), issued under strict controls to ensure the holder of the credentials has their identity verified before issuance, and expose any attempts to alter the data within the credential when subsequently shared.

Scams and online fraud are a major issue in many countries, not least Thailand. This includes fraudulent claims in the health sector prompting the implementation of biometric verification[14], the high instance of scams occurring on a daily basis, and a growing trend in AI-assisted identity fraud.

According to reports by the High-Tech Crime Division at the Thai Cyber Crime Investigation Bureau, in 2023/24 there were around 700 scam and fraud cases occurring daily, with e-commerce scams being particularly prevalent, accounting for around 40% of Thai cybercrime. These online frauds resulted in substantial financial losses of approximately 45 billion baht over 2023 and the first half of 2024.

A coordinated approach to fraud prevention leveraging the cryptographic certainty and ease of use of the Verifiable Credential ecosystem could have a huge impact on public security, reduce the financial burden of fraud on the state and on the victims of fraud, and support additional protection in the future such as e-commerce seller verification and stronger proof of organization and business identity in digital transactions. For example, a common fraud vector is the use of stolen documentation to open a bank account, or apply for a financial product such as a loan, made possible by the paper-based nature of the application process and the lack of direct checking of identity documentation. Requiring a digital proof of identity as provided by a digital ID credential would serve as a deterrent to fraudsters, reduce risk for financial sector providers and reduce the incidence of this type of fraud for citizens.

[14] Thailand introduces face biometrics verification to fight health sector fraud - https://www.biometricupdate.com/202601/thailand-introduces-face-biometrics-verification-to-fight-health-sector-fraud

B.2 Business wallets and economic impact

B.2.1 The core concept of a Business Wallet

While a personal wallet holds a passport or driver's license, a Business Wallet holds the digital identity of a legal entity i.e. a business. It allows a business to prove its existence, status, and authority instantly.

Much like a personal wallet, a Business Wallet enables a business to hold its own data as verifiable credentials, typically within a secure Cloud-based wallet. Also, similarly to a person, a legal identity is required for the Business Wallet to prove ownership of those credentials. In this case this should be derived from core datasets used to register and operate businesses such as the DBD Biz Regist.

Example Business Wallet Use Cases:

- **KYB (Know Your Business):** Banks can onboard corporate clients in seconds by verifying credentials instead of manually reviewing articles of incorporation.
- **Public Procurement:** businesses can participate in procurements digitally by submitting pre-verified credentials regarding their solvency and technical capacity.
- **Supply Chain / Digital Product 'Passports':** businesses can verify the origin and sustainability credentials of suppliers in real-time.

Business Wallets should support verifiable credentials representing mandate and delegated authority, enabling natural persons to act on behalf of legal entities in a controlled and auditable manner, including support for scope limited and time bound delegation and revocation.

Business wallets will hold 3 main types of digital "objects" to support operations of a legal entity: digital proofs, digital mandates, and digital signatures:

Digital Proofs	Digital proofs of specific attributes issued by authoritative bodies. For example, trade licenses, or environmental permits.
Digital Mandates	Proof that a specific natural person (e.g., a CEO) has the authority to act on behalf of the company. For example, Power of attorney or "right to sign" for a specific bank account.
Digital Signature	The corporate version of a digital signature, ensuring the origin and integrity of a document used to sign electronic documents on behalf of the business or organization.

B.2.2 Economic impact

Business Wallets represent a significant opportunity to reduce structural friction in the Thai economy. Small and medium-sized enterprises (SMEs), which account for the vast majority of Thai businesses, often face prohibitive costs and complex procedures when participating in international trade or applying for credit[15].

By providing every Thai company with a Business Wallet, the government can enable Verifiable KYB (Know Your Business) capability for businesses of all sizes, including SMEs. This would allow Thai companies to share their registration status, shareholder lists, and financial health instantly with banks or partners.

Implementation of the ASEAN Unique Business Identification Number (UBIN) further enhances this by ensuring that Thai businesses are recognized and trusted across all ten ASEAN member states. Estimates (by the Boston Consulting Group) suggest that full implementation of the UBIN could generate between USD 110 billion and USD 300 billion in economic value for ASEAN by lowering transaction costs and attracting foreign investment.

Potential Economic Benefits:

	Direct Benefit	**Long Term Impact**
SMEs/MSMEs	Reduction in onboarding time for exports and loans.	Increased participation in regional digital trade.
Public Administration	Elimination of paper-based document processing.	Higher ranking in E-Government Development Index (EGDI).
Financial Sector	Lower KYC/AML compliance overhead.	Expanded credit access and financial inclusion.
Tourism Sector	Seamless verification for digital nomads and LTR visa holders.	Increased tourism revenue and visitor spending.

B.2.3 Potential providers of business wallets

The private sector should be consulted to ensure that existing initiatives are explored when determining who should provide the business wallets. For example, Thailand Post's "Prompt Post" has plans to develop a corporate wallet to store government licenses, with future integration into the National Single Window (NSW) for import-export processes. This wallet could be accredited for use as a national business wallet under the terms of the Trust Framework.

[15] ASEAN's Next Trade Breakthrough: Accelerating Cross-Border Growth Through Interoperable Identity - https://asean-bac.org/news-and-press-releases/asean%E2%80%99s-next-trade-breakthrough-accelerating-cross-border-growth-through-interoperable-identity

B.2.4 Initial steps for business wallet implementation

When planning implementation of business wallets, it is important to consider who will use the wallets, what credentials the wallets will hold, and the use cases for which business wallets will be impactful. The following high-level phases outline the key tasks to be addressed for bsuness wallet implementation.

Phase I: Framework & Compliance (Year 1)

- Regulatory Alignment: Ensure the business wallet architecture meets Trust Framework requirements and cybersecurity standards, extending the Trust Framework appropriately.
- Governance Setup: Define who issues the business wallets (Government vs. private-sector qualified providers) and establish a Trust List for certified providers.
- Identify initial set of core use cases for business wallets: For example, Legal representation, applying for public funding, participating in public procurement, applying for / presenting licenses.

Phase II: Core Development & Standards (Year 1 – in parallel to Phase I)

- ID Credentials for Legal Entities: Develop the business entity ID Verifiable Credential specific to businesses (e.g., VAT numbers, LEI, and National Registry data).
- Support government agencies and key institutions to issue digital credentials: for example, Company certificates of incorporation, Tax clearance and social security status, Professional licenses.
- Define rules for Delegation & Mandates: to allow a business (legal entity) to delegate specific permissions to employees to sign or share data on its behalf.

Phase III: Pilot Testing & Ecosystem Onboarding (Year 2)

- Pilot business wallets for key use cases.
- Relying Party Registration: Onboard "Relying Parties" (banks, utilities, govt agencies) so they are technically ready to request and verify wallet data.

Phase IV: Wider Rollout & Mandatory Acceptance (Year 3)

- Lifecycle Management: Establish protocols for revocation (e.g., if a company ceases trading, becomes bankrupt, or a mandate is withdrawn).

- Scale-up the rollout of business wallets beyond initial use cases.
- Consider Public Sector Mandate: Public bodies must accept the wallet for authentication and document submission. This may require additional regulation / legislation.

B.3 Improving efficiency and access to government services

Traditional government processes often require a manual verification process where an official must physically check a document, and often multiple documents. Digital wallets enable citizens to hold digital versions of government and private sector documentation backed by cryptographic trust, meaning that not only is the process streamlined but the burden on citizens and officials dramatically reduced.

- Credentials can be verified instantly either online or offline. A Verifiable Credential (like a digital driving license or ID card) is cryptographically signed by the issuing Ministry. A third party can verify its authenticity instantly without contacting the original Ministry again.
- Citizens only need to prove their identity or eligibility once. Once a credential is in their digital wallet, it can be reused multiple times across different public and private sector service providers without the need to request additional copies of documents or to complete multiple in-person verifications.
- Verifiable Credentials can also be used by citizens to automatically pre-fill complex applications for benefits or tax returns, reducing errors and processing times from weeks to seconds. They also have the opportunity to share specific data rather than entire documents, increasing privacy and reducing the over requesting if data by service providers.

B.3.1 Reducing the threat of data breaches

A common threat to government efficiency is the risk of data breach leading to loss or compromise of government services. Adopting a decentralized model for digital identity and key government data (as used by citizens and business) reduces dramatically the instance of centralized government database or service silos being compromised as they are able to focus more on the secure issuance of credentials rather than exposing their functionality or data to other systems.

Citizens holding credentials in their digital wallets are able to utilize functionality such as Selective Disclosure which means they are able to share specific data or confirmations from their credentials rather than the entire digital document. This helps to enforce the principle of data minimization which reduces the risk of a breach at a service provider as they only receive data needed to complete a transaction.

Verifiable Credentials also help to reduce fraud due to their tamper-proof nature and the strong identity verification processes such as biometrics verification and liveness

checking that make identity theft significantly harder compared to paper documents and traditional processes.

B.4 Clarity over the government wallet provider

A key question is whether Thailand should endorse a single digital identity and document wallet provider or multiple providers. Whilst both approaches will work, they will have a differing long-term effect on the ecosystem which should be considered.

The choice between mandating a single government-provided wallet or permitting a competitive ecosystem of multiple wallet providers is a key strategic decision for the Government of Thailand. This choice has profound implications for user adoption, innovation, and system resilience.

Today’s fragmented wallet ecosystem

For Thai citizens transacting online, digital identity and wallets have been available for some time but have evolved as siloed solutions focusing on specific user requirements. Currently ThaID (30 million users) is often used for proof of identity while Thang Rath (39 million users) provides access to government services through a single super app interface. Both applications have included a digital document wallet in their product roadmaps. Adjacent to this is Paotang, another ‘super app’ developed as a collaboration between the Thai government and Krungthai Bank which has become a major payment wallet solution with over 40 million users. Paotang has also helped to reduce the cost of distributing aid and increased transparency by creating a digital paper trail for every Baht spent.

All of these solutions have experienced successes but to date they remain separate pillars of innovation with little interoperability between them, largely due to the absence of a common trust framework and enforceable interoperability standards. This leads to complex user experiences for citizens and lost potential for public and private sector organizations to realize efficiencies or to build even more innovative solutions. Credentials in each system and wallet are incompatible, standards have not been imposed to ensure interoperability, and governance is fragmented.

From a user perspective these incompatibilities manifest themselves in cumbersome user journeys and the need for multiple apps to complete transactions. From the government perspective the cost of interoperability between systems is high, and integration effort is repeatedly duplicated across agencies.

B.4.1 The Case for a Single Provider Model

It could be argued that a single wallet provider, such as Thang Rath or ThaID, taking a centralized view may ensure a consistent user experience and could simplify the regulatory burden. A single government app acting as a unified "One-Stop Service,"

would concentrate government resources on securing one platform rather than auditing many[16].

B.4.2 The Case for Multiple Providers or Ecosystem Model

While citizens generally trust the state for core identity documents, they often prefer private-sector innovation for commercial services, banking, and lifestyle integrations. A multi-provider model where banks, telcos, and tech firms can offer certified wallets, encourages competition in security features, biometric integration, and user interface design.

From an operational perspective a multi-provider ecosystem reduces the burden on government to be the sole provider of digital wallets and may even increase resilience in the ecosystem by reducing the risk of wallet provider outages preventing citizens from accessing vital government services.

B.4.3 Strategic Recommendation: The Hybrid Ecosystem Model

Considering the local context, Thailand should adopt a governed multi-wallet ecosystem under the National Verifiable Credential Trust Framework. This model aligns with Thailand's multi-agency landscape, preserves competition and innovation, and prevents fragmentation through enforceable interoperability.

Rather than mandating a single national wallet or allowing uncontrolled proliferation of siloed applications, the Government should establish enforceable interoperability rules that enable multiple accredited wallets to operate within a common framework. This approach preserves innovation and user choice while ensuring portability, consistent standards, and system-wide coherence.

Under this model:

- ETDA establishes and administers the National Trust Framework, including accreditation, conformance testing, and supervisory mechanisms.
- All wallets operating within the ecosystem must be accredited under the Trust Framework and comply with the National Interoperability Profile—accreditation is the baseline for all participants. Within this, government-designated wallets receive the additional privilege of storing official government-issued credentials, and public agencies are mandated to accept them. Non-designated accredited wallets operate fully within the ecosystem for non-official credentials, without restriction or exclusion.
- Interoperability and portability across accredited wallets are mandatory, and proprietary credential systems operating outside the framework will not be recognized for government use.

[16] Thailand Digital Data Infrastructure Roadmap Report (World Bank) - https://thedocs.worldbank.org/en/doc/c9160dd8065d1300384d8ab790742165-0070012025/original/Deliverable-5-Final-DDIR-for-publication-June2025-final-revision.pdf

- To optimize public investment and prevent duplication, the Government should designate up to two government-backed citizen document wallets and up to two government-backed business wallets. Existing government applications with large-scale adoption — including ThaID and Thang Rath — should be primary contenders for designation, subject to compliance with Trust Framework requirements.
- Other public, SOE, and private sector wallets may operate under accreditation, but without preferential integration, exclusive arrangements, or additional public funding.

This model ensures enforceable interoperability, disciplined use of public resources, and scalable national adoption while maintaining competition and technological innovation.

B.5 Alignment with the Act on Management of State Affairs by Electronic Means (B.E. 2565)

The application of Verifiable Credentials does not compromise the effect of the Act on Management of State Affairs by Electronic Means (B.E. 2565) under section 13 or prevent agencies from issuing a "License" as described in the Act.

That said, ETDA should endeavor to communicate to other agencies how verifiable credentials can and should be implemented to meet the needs of agencies wishing to manage state affairs by electronic means in the context of this and other existing legislation.

B.6 The benefits of standards

B.6.1 The benefits of Verifiable Credentials and a decentralized model

Adopting internationally recognized standards for digital credentials and identity assurance will ensure that Thailand and its citizens can exploit opportunities for increased productivity, ease of access to public and private services, and international interoperability for trade, travel, and commerce.

Verifiable Credentials and a decentralized approach to utilizing these credentials for citizens and businesses also has the advantage of shifting the role of government from one of core service provider for identity and data to one of issuer of trusted credentials. Interoperability and data sharing happens directly between service providers and citizens for the most common transactions reducing the burden on government systems to provide scalable APIs for high volume data requests or to verify user identity.

B.6.2 Widely accepted international standards are essential

The choice of standards and protocols for digital identity and verifiable credential issuance and subsequent use in the ecosystem is critical to the sustainability and interoperability of the ecosystem. Many countries are now implementing digital credential wallets and issuing Verifiable Credentials and as a consequence have driven the development and widespread acceptance of certain key standards, specifications and protocols. For example, the OpenID Foundation has developed protocols for Verifiable Credential Issuance and Presentation which are being implemented across the European Union under the European Digital Identity (EUDI) framework and in neighboring states and interested counties globally. The ISO/IEC 18013-5/7 standards have also gained momentum largely due to their use as the basis for mobile driving license issuance in the USA.

These standards and protocols from ISO, the Open ID Foundation, W3C, and the IETF (e.g. OpenID for Verifiable Credential issuance and presentation, SD-JWT, and ISO/IEC 18013-5/7), are mature, extensively tested[17], and have been adopted into law by the European Union as the primary standards for high trust verifiable credential issuance and use nationally and internationally. This has also led to the development of the OpenID4VC High Assurance Interoperability Profile[18] (or HAIP) which encapsulates these requirements for implementation in the EU and beyond.

Layer	Available Standards (EUDI Wallet / OIDF HAIP Profile)				
Identity Verification	NIST 800.63A	eIDAS LoA	ISO/IEC 29115	National Derivatives...	
Issuance Protocol	OpenID4VCI	ISO 23220-3	DIDComm		
Credential Format	W3C VCDM	SD-JWT-VC	ISO mDoc	AnonCreds	
Presentation Flow	OpenID4VP	DIDComm	mDoc	QR	
Invocation	W3C DC API	QR Code	Deep Link	CHAPI	NFC (mDoc)
Transport	BLE (mDoc)	NFC (CTAP)	Camera (QR)	HTTP	BLE (OpenID4VP)
Technical Trust	X509 / Trust Lists	OIDF Federation	vLEI	DID	
Credential Status	IETF Status List	W3C Bitstring Status List			

Figure 3 - Standards and Protocols as specified for implementation as a profile for EUDI wallets

Defining systems that implement these already accepted standards will ensure interoperability and ease of implementation with multiple vendors and vibrant community of developers available to build and support the Thai ecosystem. It also

[17] OpenID Foundation demonstrates real-world interoperability of new Digital Identity Issuance Standards - https://openid.net/oidf-demonstrates-interoperability-of-new-digital-identity-issuance-standards/

[18] OpenID4VC High Assurance Interoperability Profile 1.0 - https://openid.net/specs/openid4vc-high-assurance-interoperability-profile-1_0.html

means that relying party services and potential issuers of credentials will find it easier to adapt their systems to interoperate with the VC ecosystem reducing barriers to implementation by avoiding niche or proprietary technologies.

Based on the above analysis it is recommended that the Thai VC ecosystem should adopt standards that are becoming the benchmark for digital wallet interoperability.

Recommended standards based on developments in other countries:

- **Issuance Protocol** – OpenID4VCI
- **Credential Format** – SD-JWT-VC, ISO mDoc
- **Presentation Flow** – OpenID4VP
- **Invocation** – W3C DC API, Deep Link
- **Transport** – HTTP, (optionally BLE OpenID4VP, or BLE mDoc)
- **Technical Trust** – x509 / Trust Lists
- **Credential Status** – IETF Status List



PUBLICATION DATE | JULY 2026
VERSION | 1.2

THE WORLD BANK