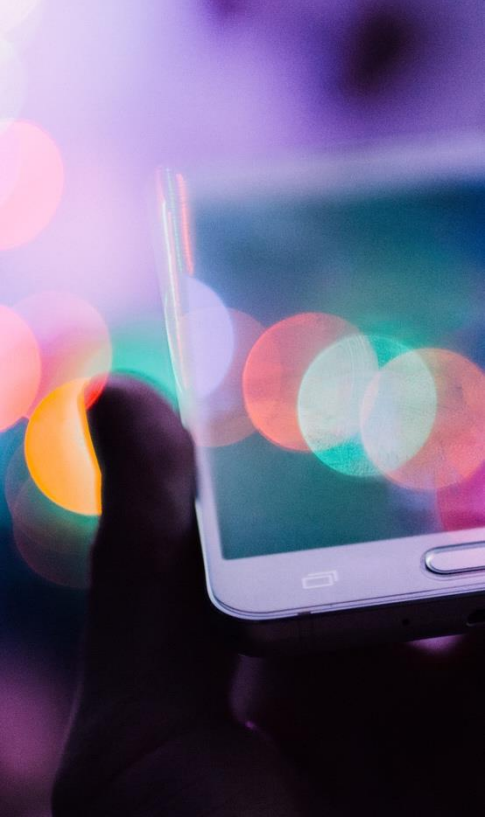


สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
Electronic Transactions Development Agency

กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม

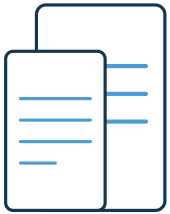
ETDA

เอกสารนำเสนอ
ความรู้พื้นฐานและรายงานทางเทคนิคของ

กรอบการทำงานร่วมกัน ของกระเป๋าดิจิทัลสำหรับเอกสารรับรอง

(Interoperable Framework of Digital Wallets for Verifiable Credentials)

วิวัฒนาการของเอกสารรับรอง

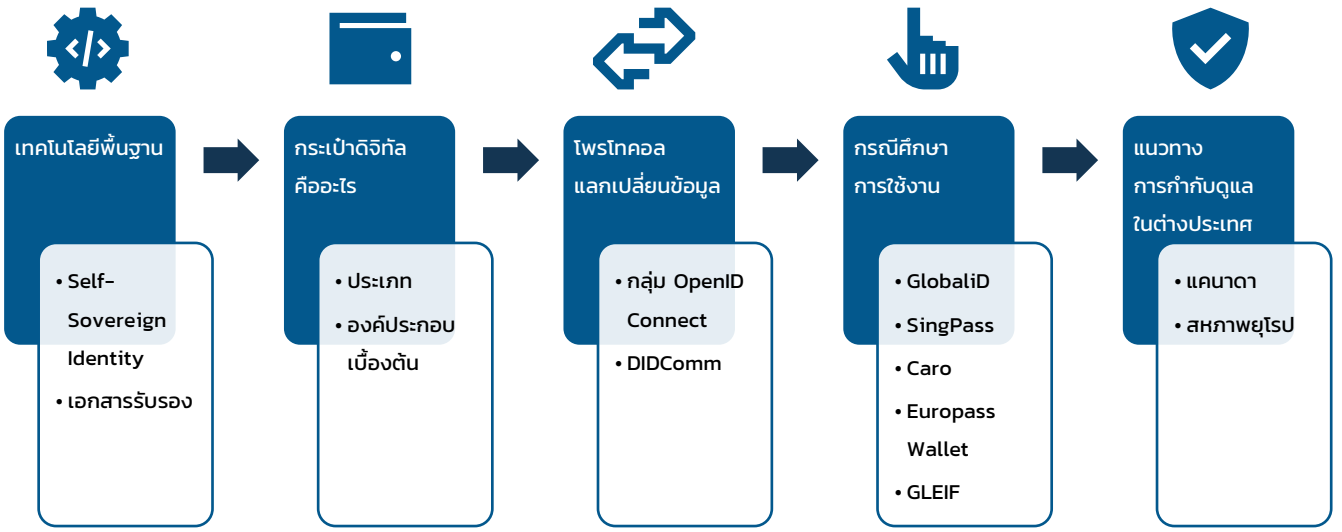


เอกสารรับรองกระดาษ
(Paper Credentials)

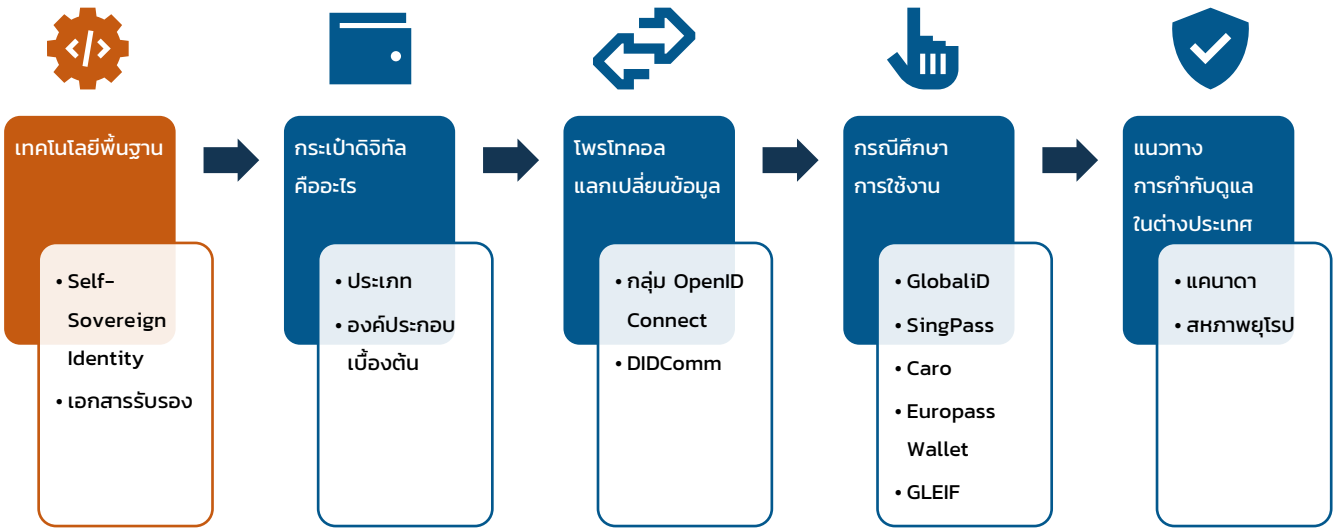
สำเนาอิเล็กทรอนิกส์ของ
เอกสารรับรองกระดาษ
(e-Copy of Paper Credentials)

เอกสารรับรองดิจิทัล
(Digital Credentials
หรือ Verifiable Credential)

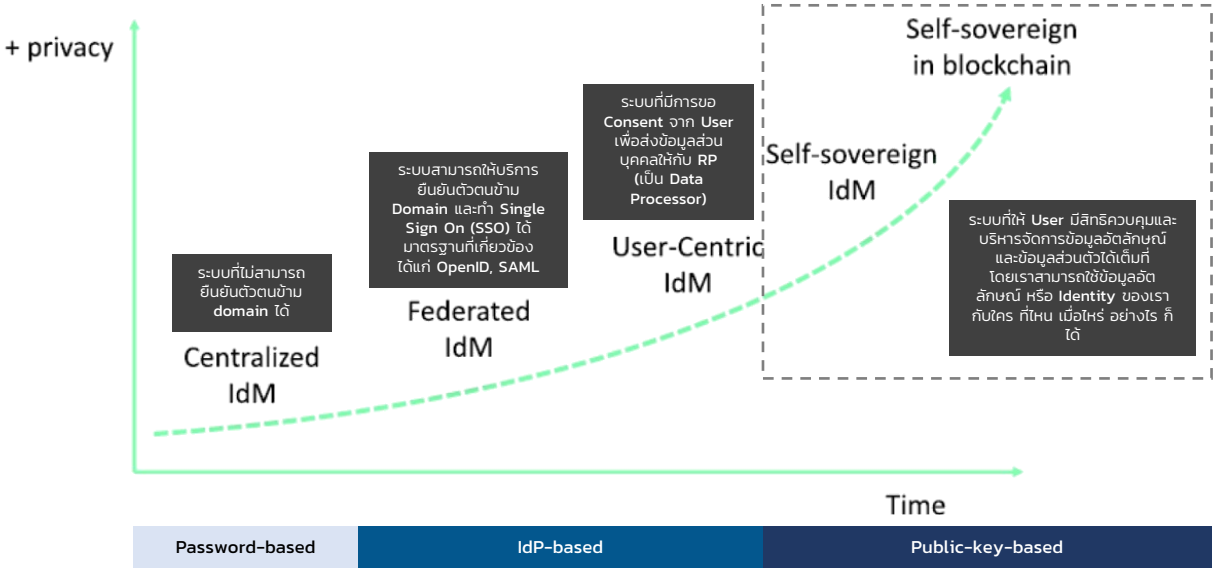
โครงร่างการนำเสนอ



โครงร่างการนำเสนอ

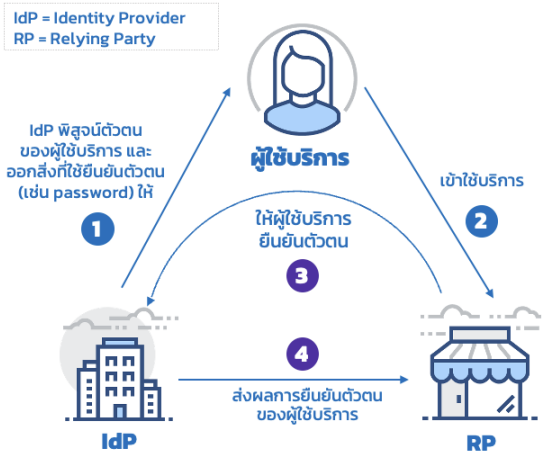


วิวัฒนาการของระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล



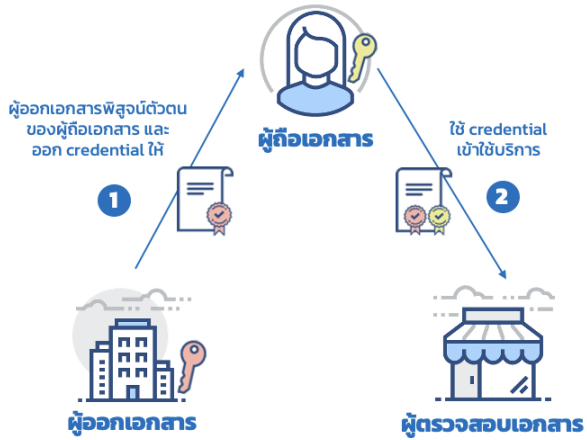
ที่มา J. Bernal Bernabe et al.: Privacy-Preserving Solutions for Blockchain: Review and Challenges

IdP – based Authentication



RP ให้ผู้ใช้บริการไปยืนยันตัวตนกับ IdP และ
IdP จะส่งผลการยืนยันตัวตนกลับให้ RP

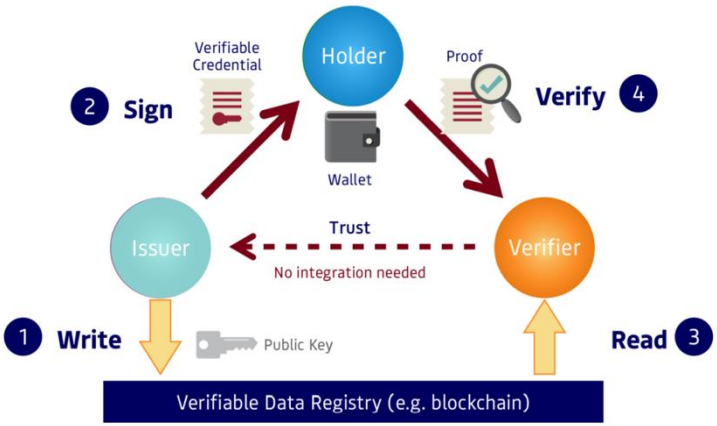
Public-key-based Authentication



ผู้ตรวจสอบเอกสารสามารถตรวจสอบและเชื่อถือคุณลักษณะ
ใน credential ได้ **โดยไม่ต้องกลับไปให้ผู้ออกเอกสารยืนยัน**

เทคโนโลยีพื้นฐาน

เอกสารรับรอง (verifiable credential: VC) และเอกสารสำแดง (verifiable presentation: VP)



ขั้นตอนที่ 1 : issuer จัดเก็บ public key บน verifiable data registry

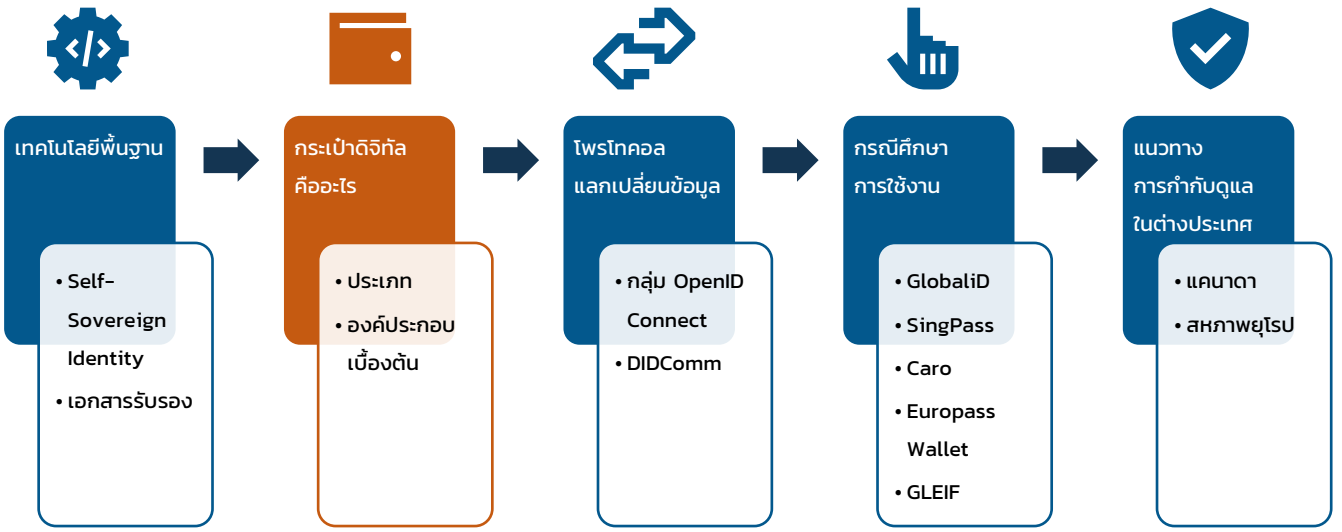
ขั้นตอนที่ 2 : issuer ลงลายมือชื่อดิจิทัลบน VC เพื่อออกให้ holder

ขั้นตอนที่ 3 : holder จะสร้าง VP (Proof) ให้ verifier และ verifier สามารถดึงกุญแจสาธารณะจาก verifiable data registry

ขั้นตอนที่ 4 : verifier จะใช้กุญแจสาธารณะของ issuer ในการตรวจสอบ VP

ที่มา https://trustoverip.org/wp-content/uploads/Introduction-to-ToIP-V2.0-2021-11-17.pdf

โครงร่างการนำเสนอ



กระเป๋าดิจิทัล (Digital Wallet)

กระเป๋าดิจิทัล (digital wallet) คือ ซอฟต์แวร์ที่ให้ผู้ใช้งานสร้าง (generate) จัดเก็บ (store) จัดการ (manage) และเก็บรักษา (protect) กุญแจเข้ารหัส (cryptographic key) ข้อมูลลับ (secret) และข้อมูลส่วนตัวอื่น ๆ ที่มีความอ่อนไหว เช่น เอกสารรับรองที่ตรวจสอบได้ (verifiable credential) และสำเนาอิเล็กทรอนิกส์ของเอกสารรับรองแบบกระดาษ (อาทิ หนังสือเดินทาง)

กระเป๋าดิจิทัลที่จะกล่าวถึงในที่นี้ ครอบคลุมเฉพาะกระเป๋าดิจิทัลสำหรับการเก็บเอกสารรับรองเท่านั้น (credentials) **ไม่**รวมถึงกระเป๋าดิจิทัลสำหรับการแลกเปลี่ยนเงินอิเล็กทรอนิกส์ หรือ สินทรัพย์ดิจิทัล (digital asset)

ที่มา Alex Preukschat and Drummond Reed, "Self-Sovereign Identity", Manning Publications, 2021

กระเป๋าดิจิทัล – ประเภท

Edge Wallet

มีองค์ประกอบทั้งหมดจัดเก็บอยู่ในอุปกรณ์ของผู้ใช้งาน (edge) สำหรับกระเป๋าดิจิทัลประเภทนี้ ผู้ใช้งานจะสามารถจัดเก็บข้อมูลของตนได้ แต่มีข้อจำกัดที่ผู้ใช้งานจะไม่สามารถซิงค์ ข้อมูลระหว่างอุปกรณ์

Hybrid Wallet

เป็นกระเป๋าดิจิทัลแบบผสม ผู้ใช้งานกระเป๋าดิจิทัลรูปแบบนี้ มีทางเลือกในการเลือกจัดเก็บองค์ประกอบในที่ต่าง ๆ ทั้งบนระบบคลาวด์ของผู้ให้บริการ (cloud) หรือในอุปกรณ์ของผู้ใช้งานเอง (edge)

Cloud Wallet

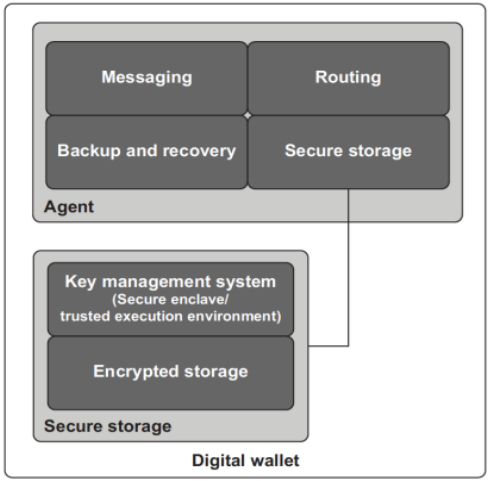
มีองค์ประกอบทั้งหมดจัดเก็บอยู่กับผู้ให้บริการ (cloud) โดยผู้ใช้งานสามารถบริหารจัดการกระเป๋าดิจิทัลของตน ที่อยู่กับผู้ให้บริการผ่านทางอินเทอร์เน็ต ข้อดีของกระเป๋าดิจิทัลประเภทนี้ คือ ระบบมีกลไกการกู้คืนข้อมูล และการซิงค์ข้อมูล

กระเป๋าดิจิทัล – องค์ประกอบและฟังก์ชันการทำงาน

โปรแกรมเอเยนต์ (Agent)

โปรแกรมเอเยนต์ หรือตัวแทนดิจิทัล คือ software module ที่ขับเคลื่อนการใช้งานและรักษาความปลอดภัยของกระเป๋าดิจิทัล

เฉพาะผู้ที่เป็นเจ้าของเอกสารรับรองและกุญแจเข้ารหัสเท่านั้น ที่จะใช้งานกระเป๋าดิจิทัลได้



พื้นที่จัดเก็บข้อมูลอย่างมั่นคงปลอดภัย (Secure Storage)

พื้นที่จัดเก็บข้อมูล แบ่งเป็นสองส่วนหลัก ๆ คือ

1. พื้นที่จัดเก็บข้อมูลสนับสนุนการใช้งานโดยทั่วไป (เช่น Wallet API) และ
2. พื้นที่จัดเก็บข้อมูลอย่างมั่นคงปลอดภัย ซึ่งประกอบไปด้วยสองส่วนย่อยคือ พื้นที่จัดเก็บข้อมูลแบบเข้ารหัส (encrypted storage) และพื้นที่ที่จัดไว้สำหรับดำเนินการเกี่ยวกับข้อมูลอย่างมั่นคงปลอดภัย (เช่น trusted execution environment)

ที่มา Alex Preukschat and Drummond Reed, "Self-Sovereign Identity", Manning Publications, 2021

กระเป๋าดิจิทัล – ลักษณะการใช้งาน

การใช้งานของบุคคลธรรมดาโดยทั่วไป แบบพื้นฐาน

ผู้ใช้งานติดต่อสื่อสารกับกับกระเป๋าดิจิทัลอื่น โดยใช้กุญแจส่วนตัวในการสร้างช่องทางสื่อสารที่มีความมั่นคงปลอดภัย โดยการสร้างการเชื่อมต่อใหม่ ๆ ด้วยการสแกน QR code หรือคลิกลิงก์ จากนั้นยอมรับการสร้างการเชื่อมต่อ เลือกเอกสารรับรองที่ต้องการแลกเปลี่ยนในการปฏิสัมพันธ์ดังกล่าว รวมไปถึงมีข้อดี ต่าง ๆ อาทิ เช่น การจดจำการเชื่อมต่อโดยอัตโนมัติ ไม่ต้องมีตัวกลางในการเชื่อมต่อ และทุกข้อความจะถูกเข้ารหัสทั้งกระบวนการ

ผู้ใช้งานรับ ส่ง และสำแดงเอกสารอิเล็กทรอนิกส์ โดยเฉพาะเอกสารรับรองและเอกสารสำแดง โดยเมื่อมีการสร้างการเชื่อมต่อแล้ว จะสามารถแลกเปลี่ยนเอกสารรับรองได้ทั้งทิศทางเดียว (กำหนดตายตัวว่าฝ่ายใดเป็นผู้ส่งเท่านั้น และฝ่ายใดเป็นผู้รับเท่านั้น) และสองทิศทาง (ทั้งสองฝ่ายเป็นได้ทั้งผู้ส่งและผู้รับ) เพื่อออกเอกสารรับรองใหม่ หรือตรวจสอบเอกสารรับรองที่ถูกออกมาแล้ว

การเพิกถอนเอกสารรับรอง โดยใช้ลายมือชื่อดิจิทัลเพื่อการยืนยันการเพิกถอนเอกสาร สามารถเพิกถอนเอกสารรับรองที่หมดอายุได้หลากหลายวิธี

ผู้ใช้งานยืนยันตัวตน ด้วยกระบวนการระบบรหัส ซึ่งใช้กุญแจส่วนตัวเป็นปัจจัยในการยืนยันตัวตน สามารถทำได้ 2 วิธี วิธีแรกคือ การยืนยันตัวตนอัตโนมัติ ทำให้ไม่จำเป็นต้องมีการ “ล็อกอิน” ด้วยการกรอก username และ password แบบเดิม ช่วยประหยัดเวลาและเพิ่มความสะดวกในการเข้าสู่ระบบ วิธีที่สองคือ ยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication: MFA) ซึ่งถูกรวมเข้าด้วยกันในแนวคิด SSI ที่เพิ่มความปลอดภัยในการรักษาข้อมูลของผู้ใช้งานยิ่งขึ้น

ตัวแทนดิจิทัลและกระเป๋าดิจิทัล **สามารถลงลายมือชื่อในเอกสารอิเล็กทรอนิกส์**ที่กำหนดให้ใช้ลายมือชื่อได้

กระเป๋าดิจิทัล – ลักษณะการใช้งาน

การใช้งานของบุคคลธรรมดาโดยทั่วไป แบบขั้นสูง

กระเป๋าสามารถ**รองรับอุปกรณ์ได้หลายเครื่องและสามารถเชื่อมต่อระหว่างกันได้** ซึ่งจะก่อให้เกิดประสบการณ์การใช้งานที่ต่อเนื่องบนอุปกรณ์ทั้งหมดของผู้ใช้งาน อย่างไรก็ตาม ต้องคำนึงถึงความมั่นคงปลอดภัย การทำงานร่วมกันของกระเป๋าดิจิทัล การโยกย้ายถ่ายโอนข้อมูลเนื่องจากต้องทำให้ข้อมูลบนอุปกรณ์ทุกเครื่องตรงกัน

กระเป๋าสามารถ**ทำงานแบบออฟไลน์** สามารถตรวจสอบเอกสารรับรองได้โดยไม่ต้องมีการเชื่อมต่อกับอินเตอร์เน็ต ซึ่งสอดคล้องกับความต้องการของหน่วยงานภาครัฐหลายแห่ง ทั้งนี้ต้องมีการจัดทำมาตรฐาน และการทดสอบความสามารถในการทำงานร่วมกัน

กระเป๋าสามารถ**ตรวจสอบผู้ตรวจสอบเอกสาร** ว่ามีสิทธิ์ในการร้องขอให้ผู้ถือเอกสาร (holder) แสดงข้อความรับรอง (claim) หรือ เอกสารรับรอง (credential) เพื่อที่จะรับบริการหรือไม่ ผู้ตรวจสอบเอกสารต้องได้รับอนุญาต (authorized) ภายใต้กรอบการกำกับดูแล ในการเรียกขอหลักฐานต่าง ๆ

กระเป๋าสามารถ**เก็บรักษาบันทึกการตรวจสอบ**ที่สามารถตรวจสอบได้ด้วยการเข้ารหัส (cryptographically verifiable audit logs) เพื่อใช้ในการวิเคราะห์หลักฐาน ในกรณีที่เกิดปัญหาขึ้น

กระเป๋า**สนับสนุนพื้นที่จัดเก็บข้อมูลแบบมั่นคงปลอดภัย หรือ ห้องนิรภัย** (secure data storage [vault] support) มีความสามารถในการจัดเก็บบันทึกข้อมูลได้ทุกแบบ โดยเฉพาะที่มีการเข้ารหัสเอาไว้

ในกรณีฉุกเฉิน (emergencies) กระเป๋ายังสามารถ**ให้เข้าถึงข้อมูลได้อย่างง่าย** เช่น ในกรณีที่เกิดภาวะฉุกเฉินทางการแพทย์ รวมถึงมีบริการที่ใช้ในสถานการณ์ฉุกเฉินอื่น ๆ

ในด้านประกัน (insurance) ผู้ผลิตกระเป๋าสามารถวิเคราะห์ความเสี่ยงที่อาจเกิดขึ้นจากการใช้งานกระเป๋าดิจิทัล และมีการประกันที่สามารถบรรเทาความเสี่ยงดังกล่าวได้

กระเป๋าดิจิทัล – ลักษณะการใช้งาน

การใช้งานขององค์กร

องค์กรสามารถแต่งตั้งตัวแทน (delegation) ซึ่งหมายถึงการที่ "ผู้ถือไอเดนทิตี" ผู้หนึ่ง (หรือองค์กรหนึ่ง) อนุญาตให้ผู้อื่น กระทำการบางอย่างแทนตัวเองได้

กระเป๋าดิจิทัลแบบองค์กร ต้องสามารถมอบอำนาจในการทำธุรกรรมให้กับบุคคล

องค์กรอาจต้องการใช้กระเป๋าดิจิทัลและตัวแทนดิจิทัลแบบเฉพาะทาง (specialized wallets and agents) ที่เหมาะสมกับงานเฉพาะทาง ตัวอย่างเช่น การบัญชี การเงิน, การให้ความยินยอม, ข่าว เป็นต้น

องค์กรสามารถเพิ่มปริมาณการใช้งาน (scale) ของกระเป๋าดิจิทัล และเพิ่มจำนวนตัวแทนดิจิทัลได้

หน่วยงานที่เกี่ยวข้องกับองค์กร ต้องสามารถนำไปใช้งานได้ในวงกว้าง (large scale)

องค์กรมีสิทธิเพิกถอนเอกสารรับรอง (credential revocation) และออกเอกสารรับรองที่สามารถเพิกถอนในภายหลังได้ (revocable verifiable credentials)

กระเป๋าดิจิทัล – ลักษณะการใช้งาน

การใช้งานของบุคคลธรรมดา ในกรณีที่เป็นผู้ปกครอง (Guardian) หรือผู้แทน (Delegate)

ผู้ปกครองหรือผู้แทน (guardian/delegate) สามารถกระทำแทนผู้อยู่ในอุปการะ

เสมือนกับกรณีของการที่บุคคลทำหน้าที่ในฐานะผู้แทนขององค์กร

โดยต้องมีเอกสารรับรองที่ถูกออกโดยผู้มีอำนาจ ที่บ่งบอกอย่างเป็นทางการว่าได้แต่งตั้งบุคคลดังกล่าวเป็นผู้ปกครอง/ผู้แทน

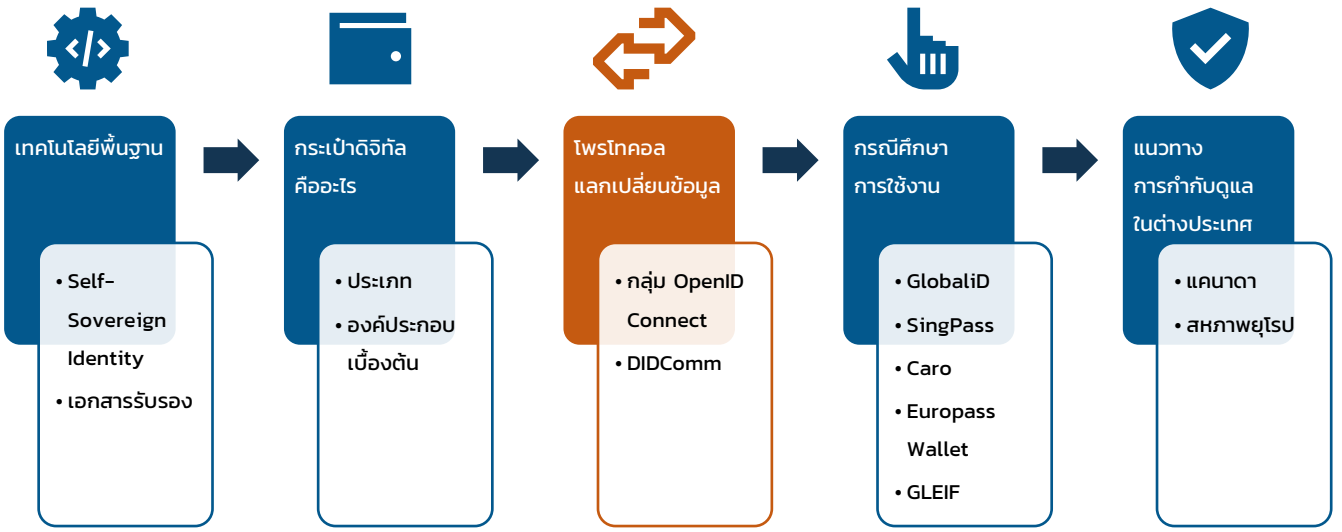
กระเป๋าดิจิทัลสำหรับผู้ปกครองหรือผู้แทน (guardian/delegate wallets) เป็นกระเป๋าที่ผู้ปกครองสามารถยืนยันสิทธิ์ของผู้อยู่ในอุปการะ

อีกทั้งสามารถเรียกขอเอกสารรับรองในฐานะของผู้อยู่ในอุปการะ

หรือเมื่อต้องแสดงเอกสารรับรองให้กับผู้ตรวจสอบเอกสาร ในฐานะของผู้อยู่ในอุปการะ

ตัวอย่างเช่น ผู้ปกครองกระทำการแทนที่บุตรที่อายุน้อย หรือบุตรที่อายุมากกระทำแทนผู้ปกครอง

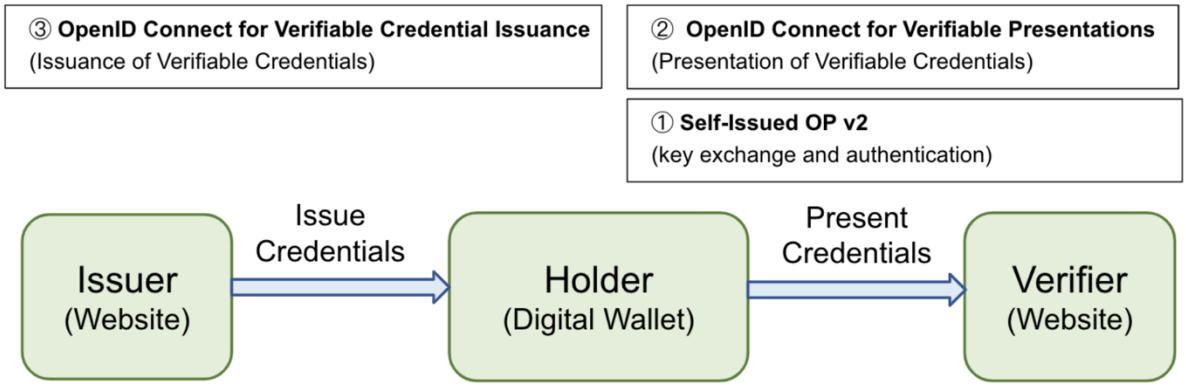
โครงร่างการนำเสนอ



โพรโทคอลในกลุ่ม OpenID

ภาพรวม

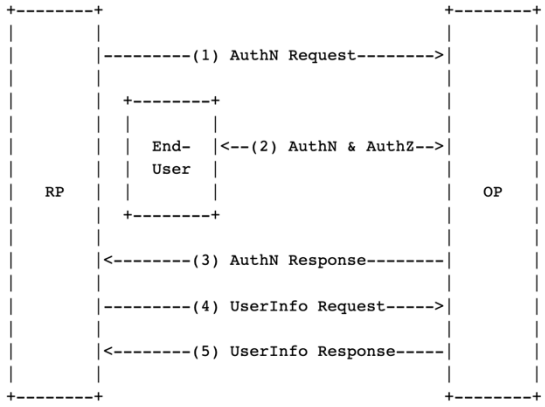
OpenID Foundation เป็นองค์กรไม่แสวงหาผลกำไร ที่มีพันธกิจในการจัดทำมาตรฐานสากลสำหรับเทคโนโลยีต่าง ๆ ที่เกี่ยวของกับการใช้งานโพรโทคอล OpenID โดยประกอบไปด้วยมาตรฐาน 3 ฉบับ



ที่มา K. Yasuda, T. Lodderstedt, D. Chadwick, K. Nakamura, and J. Vercammen "OpenID for Verifiable Credentials", https://openid.net/wordpress-content/uploads/2022/06/OIDF-Whitepaper_OpenID-for-Verifiable-Credentials-V2_2022-06-23.pdf

โพรโทคอลในกลุ่ม OpenID

OpenID Connect โดยทั่วไป



โพรโทคอล OpenID Connect (OIDC) เป็นโพรโทคอลสำหรับการยืนยันตัวตน (authentication) แบบสหพันธ์ (federated) โดยถือว่าเป็น "identity layer" ที่สร้างขึ้นบนโพรโทคอล Open Authorization (OAuth) 2.0 ซึ่งเป็นกรอบการทำงานสำหรับการมอบอำนาจการเข้าถึงข้อมูล (access delegation)

โพรโทคอล OIDC มีลำดับการทำงานโดยสังเขป ดังนี้

1. RP ส่งข้อมูลร้องขอการยืนยันตัวตนของ end-user จาก OP (OpenID Provider)

2. OP ดำเนินการยืนยันตัวตนและขอความยินยอมจาก end-user

3. OP ตอบรับคำร้องขอข้อมูลจาก RP โดยส่ง ID Token และ Access Token

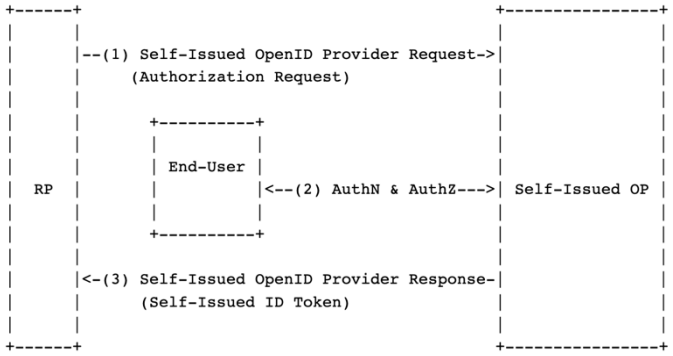
4. RP สามารถขอเข้าถึงข้อมูลของ end-user จาก OP โดยใช้ Access Token

5. OP ส่งข้อมูลข้อความยืนยัน (claims) เกี่ยวกับ end-user ให้กับ RP

ที่มา K. Yasuda, T. Lodderstedt, D. Chadwick, K. Nakamura, and J. Vercammen "OpenID for Verifiable Credentials", https://openid.net/wordpress-content/uploads/2022/06/OIDF-Whitepaper_OpenID-for-Verifiable-Credentials-V2_2022-06-23.pdf

โพรโทคอลในกลุ่ม OpenID

Self-Issued OpenID Provider v2 (SIOP v2)



Self-issued OpenID Provider (SIOP) เป็นโพรโทคอลที่พัฒนาโดย OpenID Foundation เพื่อต่อยอดจากโพรโทคอล OpenID Connect (OIDC) ให้สามารถใช้ในการยืนยันตัวตนทางดิจิทัลแบบกระจายศูนย์ได้

ในโพรโทคอล SIOP ผู้ใช้งานเป็นผู้บริหารจัดการข้อมูลเกี่ยวกับอัตลักษณ์ของตนเอง โดยยืนยันตัวตนกับ RP ด้วย identity token (ID token) ที่สร้างขึ้นจากกุญแจและข้อมูลประกอบต่าง ๆ ภายใต้การควบคุมของผู้ใช้งานเอง (ผู้ใช้งานเป็น OP เอง)

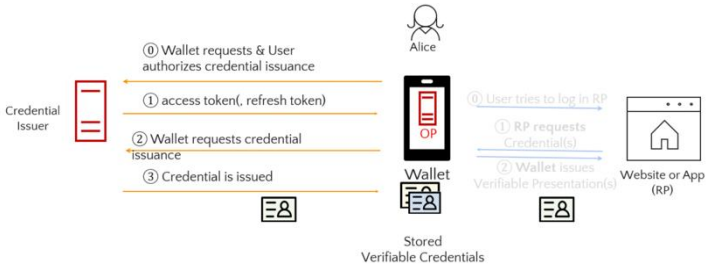
โพรโทคอล SIOP v2 มีลำดับการทำงานโดยสังเขป ดังนี้

1. RP ส่งข้อมูลร้องขอการยืนยันตัวตนของ end-user จาก SIOP บนอุปกรณ์ของ end-user เอง
2. end-user ดำเนินการยืนยันตัวตน (authentication: AuthN) และมอบอำนาจ (authorization: AuthZ)
3. SIOP ตอบรับคำร้องขอข้อมูลจาก RP โดยส่ง self-issued ID token

ที่มา K. Yasuda, M. Jones, and T. Lodderstedt, "Self-issued OPenID Provider v2", https://openid.net/specs/openid-connect-self-issued-v2-1_0.html

โพรโทคอลในกลุ่ม OpenID

OpenID Connect for Verifiable Credential Issuance (OIDC4VCI)



โพรโทคอล OIDC4VCI เป็นโพรโทคอลสำหรับการออกเอกสารรับรองผ่านทาง API โดยรองรับมาตรฐานเอกสารรับรองหลากหลายรูปแบบ รวมถึง W3C Verifiable Credentials และ ISO/IEC 18013-5 mDL

โดยมีลำดับการทำงานโดยสังเขป ดังนี้

0. end-user เริ่มต้นปฏิสัมพันธ์กับผู้ออกเอกสารเพื่อร้องขอเอกสารรับรอง

1. ผู้ออกเอกสารส่ง access token กลับมาให้อุปกรณ์ของ end-user

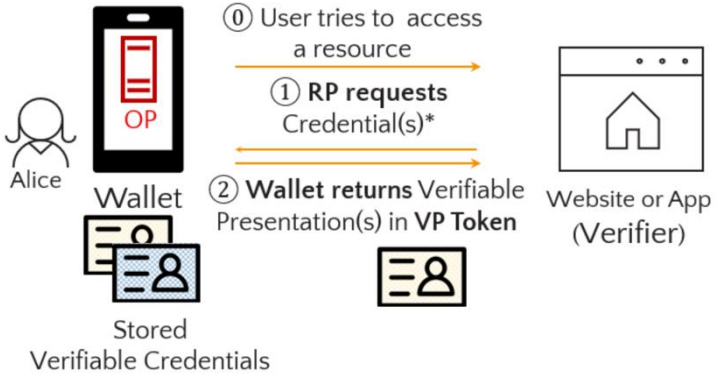
2. อุปกรณ์ของ end-user ดำเนินการร้องขอเอกสารรับรอง

3. ผู้ออกเอกสารออกและส่งเอกสารรับรองให้ end-user

ที่มา T. Lodderstedt, K. Yasuda, and T. Looker, "OpenID for Verifiable Credential Issuance", https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html

โพรโทคอลในกลุ่ม OpenID

OpenID Connect for Verifiable Presentations (OIDC4VP)



โพรโทคอล OIDC4VP ต่อยอดจากโพรโทคอล OIDC4VCI โดยมีลำดับการทำงานโดยสังเขป ดังนี้

0. end-user ประสงค์จะใช้บริการจากผู้ตรวจสอบเอกสาร (ซึ่งมีบทบาทเป็น RP)

1. ผู้ตรวจสอบเอกสารร้องขอเอกสารสำแดง

2. ผู้ถือเอกสารตอบรับการร้องขอข้อมูลในรูปแบบ VP token

จากนั้นผู้ตรวจสอบเอกสาร จะตรวจสอบว่า (ก) end-user เป็นเจ้าของเอกสารสำแดงจริง (holder binding) (ข) เอกสารสำแดงมีความครบถ้วนสมบูรณ์ (integrity) และ (ค) เอกสารสำแดงมีที่มาจากผู้ออกเอกสารจริง (authenticity)

ที่มา T. Lodderstedt, K. Yasuda, and T. Looker, "OpenID for Verifiable Credential Issuance", https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html

OpenID Connect ใน ISO/IEC 18013-5:2021

Data retrieval method	Transmission technology	Support			Reference
		mDL	mDL reader	issuing authority infrastructure	
Device retrieval	BLE	C [a]	M	N/A	8.3.3.1.1
	NFC	C [a]	M	N/A	8.3.3.1.2
	Wi-Fi Aware	O	R	N/A	8.3.3.1.3
Server retrieval	WebAPI	O	R	O	8.3.3.2.1
	OIDC	O	R	O	8.3.3.2.2

Key

M mandatory
C conditional
R recommended
O optional
N/A not applicable
[a] Support for at least one of these methods is mandatory.

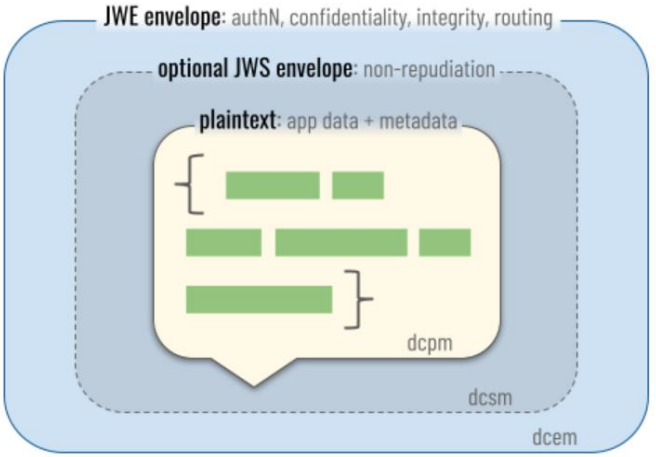
ISO/IEC 18013-5:2021 เป็นมาตรฐานใบขับขี่ดิจิทัลบนอุปกรณ์เคลื่อนที่ (mobile driving license)

OpenID Connect เป็นส่วนหนึ่งของข้อกำหนดสำหรับการสำแดงใบขับขี่ดิจิทัล ในกรณีที่ต้องดึงจากเซิร์ฟเวอร์ขององค์กรผู้ออกใบขับขี่โดยตรง

ที่มา ISO/IEC 18013-5:2021 Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application

โพรโทคอล – DIDComm

โครงสร้างข้อความ



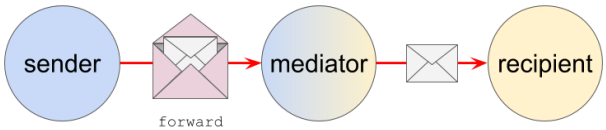
ข้อความที่ถูกส่งด้วย DIDComm จะประกอบไปด้วยข้อมูล 3 ชั้น ดังนี้

- **DIDComm plaintext message** : เป็นข้อความในรูปแบบ plaintext ที่อยู่ชั้นในสุด
- **DIDComm signed message** : เป็นชั้นถัดมาซึ่งอาจมีหรือไม่ก็ได้ (optional) ทำหน้าที่ลงลายมือชื่อดิจิทัลในรูปแบบ JSON Web Signature (JWS) เพื่อตรวจสอบที่มาของข้อความ
- **DIDComm encrypted message** : เป็นชั้นนอกสุดเป็นชั้นที่ทำการเข้ารหัส (encryption) ในรูปแบบ JSON Web Encryption (JWE) โดยทำหน้าที่รับรองความสมบูรณ์ (integrity) ของข้อความ

ที่มา DIF, "DIDComm Messaging", https://identity.foundation/didcomm-messaging/spec

โพรโทคอล – DIDComm

การค้นหาเส้นทางส่งข้อมูล



โปรโตคอล DIDcomm ประกอบไปด้วย 3 บทบาท ได้แก่

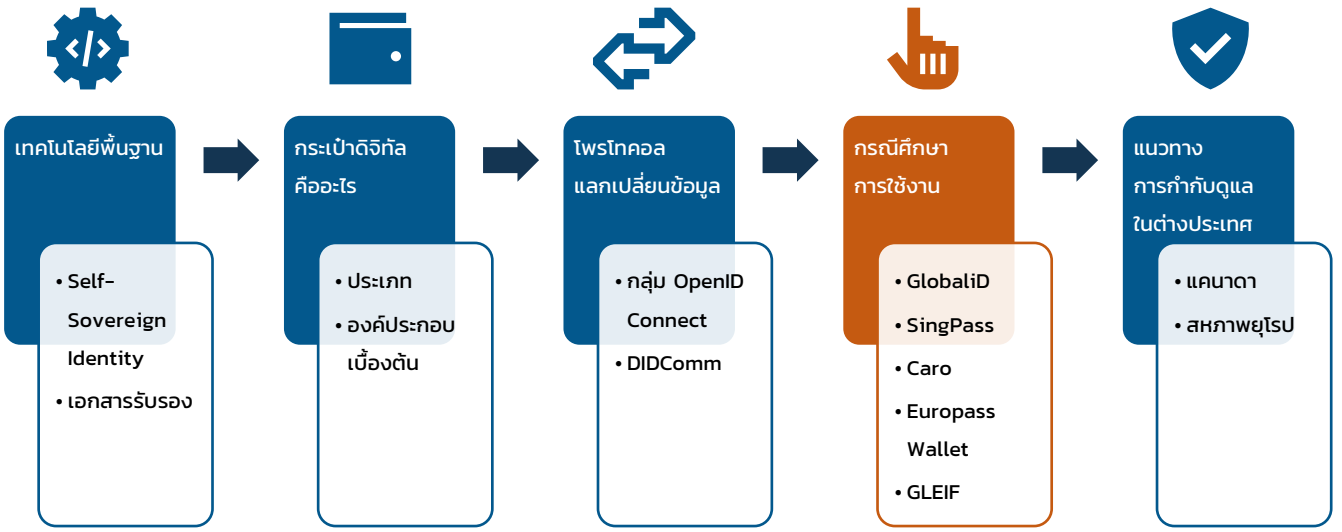
- ผู้ส่ง (sender)
- คนกลาง (mediator)
- และผู้รับ (recipient)

โดย sender ส่งข้อความประเภทส่งต่อไปยัง mediator ซึ่งทำการถอดรหัส payload ของข้อความ จากนั้นส่งต่อข้อความให้กับ recipient

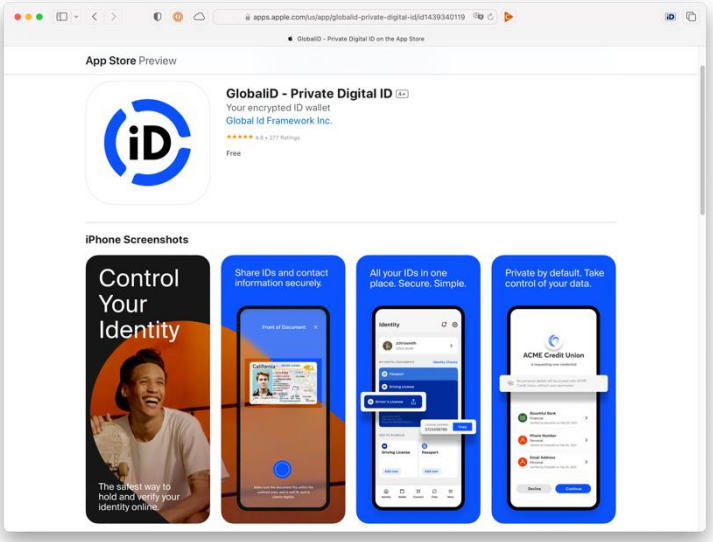
ทั้งนี้โปรโตคอลอาจเป็นแบบทางเดียว (one-way) ไม่มีการส่งข้อความกลับ หรือ ในกรณีที่มีการส่งข้อความกลับ sender และ recipient จะสลับบทบาทกัน โดยอาจใช้ mediator เดิม หรือ mediator อื่น หรือ ไม่ใช้ mediator เลยก็ได้

ที่มา DIF, "DIDComm Messaging", https://identity.foundation/didcomm-messaging/spec

โครงร่างการนำเสนอ



กรณีศึกษา – GlobaliD



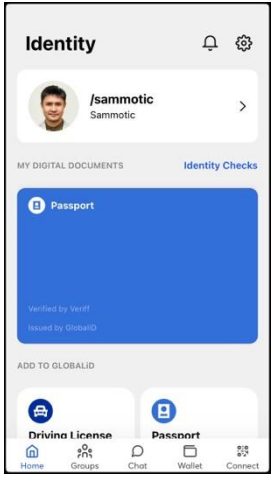
กระเป๋าดิจิทัล GlobaliD มีคุณสมบัติในการจัดเก็บและบริหารจัดการการพิสูจน์และยืนยันตัวตนของผู้ใช้บริการ

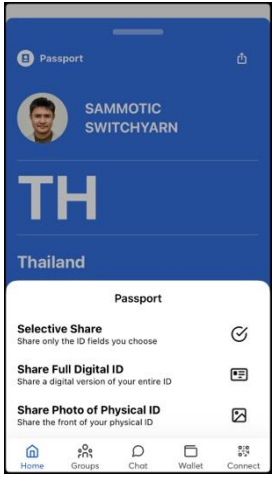
Global ID คือบริษัทด้านดิจิทัลไอดีที่มีสำนักงานใหญ่ตั้งอยู่ที่สหรัฐอเมริกา มีการให้บริการไอเดนทิตีกว่า 1.6 ล้านไอดี ครอบคลุมผู้ใช้งานกว่าหกแสนคน โดยให้บริการกระเป๋าดิจิทัล ที่พกพาสะดวกและสามารถทำงานร่วมกับกระเป๋าดิจิทัลอื่นได้ (portable, interoperable identiy wallet) ภายใต้มาตรฐานเปิด

GlobaliD จะออกเอกสารรับรองให้กับผู้ถือเอกสาร (holder) ซึ่งจะนำไปให้กับผู้รับรองเอกสาร (verifier) เพื่อยืนยันตัวตน

ที่มา https://apps.apple.com/us/app/globalid-private-digital-id/id1439340119

กรณีศึกษา – GlobaliD





GlobaliD ใช้บริการจากผู้ให้บริการ KYC ภายนอก (เช่น Veriff และ Twilio) ในการตรวจสอบเอกสาร เช่น หนังสือเดินทาง

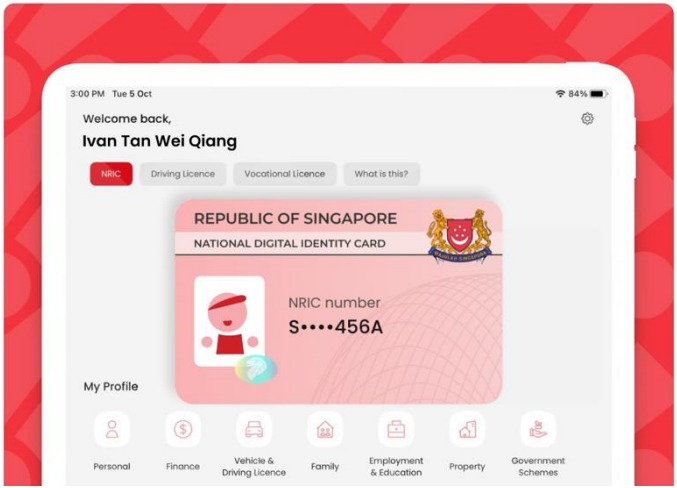
กระเป๋าดิจิทัล จะแปลงเอกสารดังกล่าวให้อยู่ในรูปแบบดิจิทัล และจัดเก็บและบนอุปกรณ์ของผู้ใช้งาน

ผู้ใช้งานสามารถแชร์เอกสารดังกล่าวให้กับผู้อื่นได้ โดยอาจแชร์แบบเต็ม หรือเพียงข้อมูลบางส่วน (ภาพซ้าย)

อย่างไรก็ดี ปัจจุบัน ยังไม่สนับสนุนการสำแดงเอกสารในรูปแบบ verifiable presentation แต่เป็นรูป jpeg (ภาพขวา)

ที่มา https://apps.apple.com/us/app/globalid-private-digital-id/id1439340119

กรณีศึกษา – SingPass ของสิงคโปร์



singpass

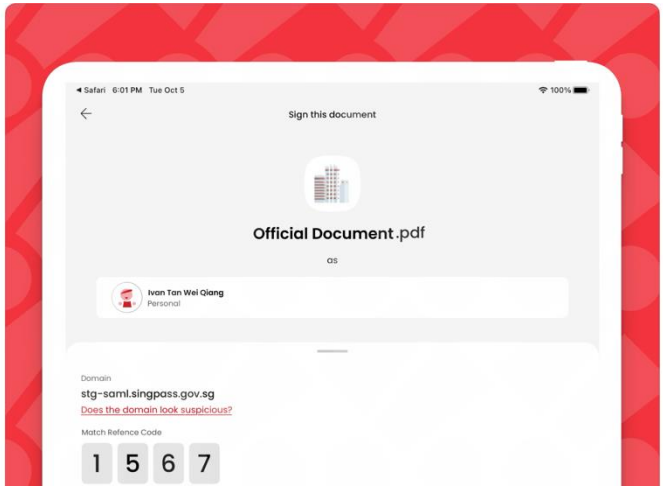
Singpass คือระบบการพิสูจน์และยืนยันตัวตนที่เชื่อถือได้ (trusted digital identity) สำหรับพลเมืองและผู้อยู่อาศัยในประเทศสิงคโปร์ แอปพลิเคชันดังกล่าวจะอาศัยการสร้างและยืนยันตัวตนผู้ใช้งานด้วยเทคโนโลยีต่าง ๆ อาทิ biometric verification เป็นต้น รวมถึงเชื่อมโยงข้อมูลเข้ากับภาครัฐ ทำให้ผู้ใช้งานสามารถใช้ SingPass ในการทำธุรกรรมและใช้บริการภาครัฐและภาคเอกชนทั่วสิงคโปร์อย่างปลอดภัยและสะดวกสบาย โดยมีตัวอย่างของบริการที่สามารถใช้งานได้ เช่น ธุรกรรมเกี่ยวกับที่ดิน ธุรกรรมเกี่ยวกับการประกัน เป็นต้น

ที่มา https://apps.apple.com/sg/app/singpass/id1340660807

กรณีศึกษา – SingPass ของสิงคโปร์

นอกเหนือไปจากการใช้เพื่อพิสูจน์และยืนยันตัวตน ผู้ใช้บริการ SingPass สามารถทำการลงลายมือชื่อดิจิทัล (digital signing) ผ่านแอปพลิเคชันดังกล่าวได้ โดยสามารถ

- ใช้ในการลงลายมือชื่อเอกสาร สัญญาทางกฎหมายต่าง ๆ ด้วยลายมือชื่อที่ได้รับการรับรองตามกฎหมาย
- ใช้ในการลงลายมือชื่อสำหรับการทำธุรกรรมอื่น ๆ กับทั้งภาครัฐและภาคเอกชน ผ่านทางแอปพลิเคชัน



ที่มา https://apps.apple.com/sg/app/singpass/id1340660807

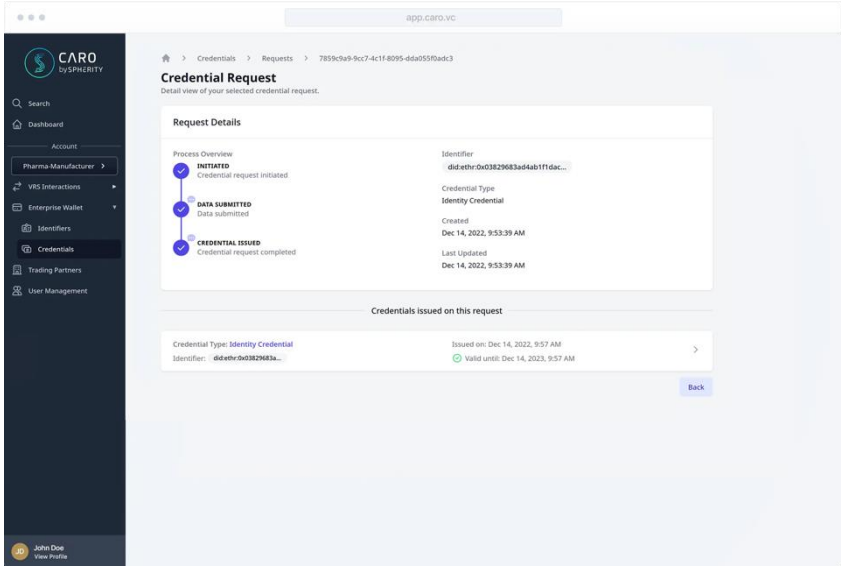
กรณีศึกษา – Caro

OPEN CREDENTIALING INITIATIVE ✖ SPHERITY

Caro คือเว็บแอปพลิเคชัน ที่ผู้ที่มีส่วนเกี่ยวข้องกับห่วงโซ่อุปทาน (supply chain) ของยารักษาโรค สามารถใช้เพื่อระบุตัวตนบริษัทคู่ค้า และตรวจสอบการเป็นพันธมิตรคู่ค้าที่ได้รับการรับรอง (Authorized Trading Partner: ATP) ตามข้อกำหนดของ Drug Supply Chain Security Act (DSCSA) ของสหรัฐอเมริกา

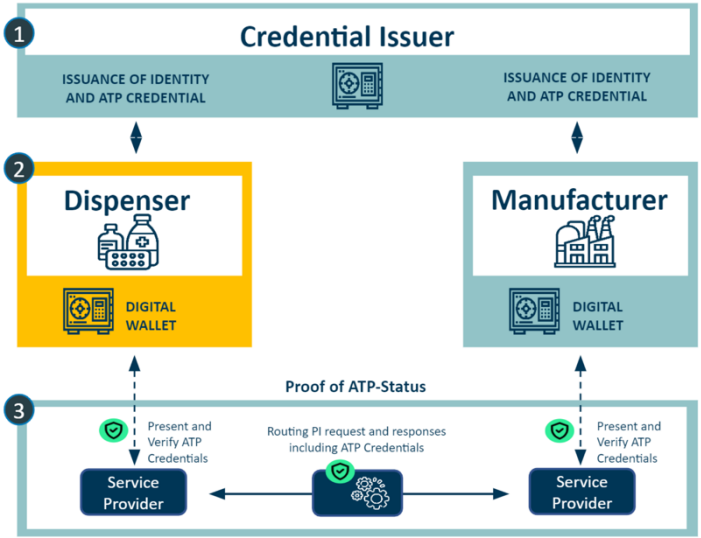
กระเป๋าดิจิทัลนี้ผลิตโดยบริษัท Spherity ภายใต้มาตรฐานที่กำหนดโดยการรวมกลุ่มกันของภาคเอกชน ในชื่อว่า Open Credentialing Initiative

จากภาพ เป็นตัวอย่างการทำงานของกระเป๋าดิจิทัลในส่วนของการขอเอกสารรับรองไอเดนทิตีของบริษัทคู่ค้า



ที่มา https://caro.vc

กรณีศึกษา – Caro

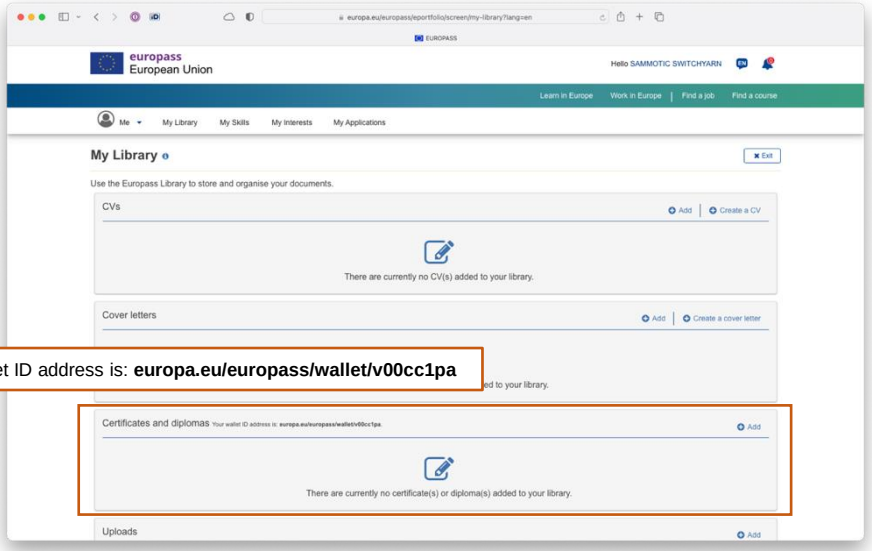


เพื่อความปลอดภัยของผู้ป่วย DSCSA กำหนดให้ผู้ที่เกี่ยวข้องกับห่วงโซ่อุปทานสำหรับยา ต้องทำธุรกรรมแลกเปลี่ยนกับ Authorized Trading Partners เท่านั้น ดังนั้น Caro จึงมีบทบาทในการช่วยสนับสนุน Verification Routing Service (VRS) สำหรับบริษัทที่ทำการแลกเปลี่ยนสินค้าได้ใช้ตรวจสอบที่มาของผลิตภัณฑ์

การออกเอกสารรับรอง มีการสร้างตัวระบุเฉพาะสำหรับองค์กร (unique enterprise identifier) และสร้างเอกสารรับรองสถานะ ATP ขององค์กร

ที่มา https://learn.caro.vc/docs/library/atp_credentialing_for_dispensers_poc.pdf

กรณีศึกษา – Europass Wallet



Your wallet ID address is: **europa.eu/europass/wallet/v00cc1pa**

Europass Wallet เป็นส่วนหนึ่งของ European Digital Credentials Infrastructure ที่จัดทำขึ้นโดยคณะกรรมาธิการยุโรป เพื่อเป็นแพลตฟอร์มกลางสำหรับเอกสารรับรองประเภท **ประกาศนียบัตรและวุฒิบัตร**

Europass Wallet เป็นกระเป๋าดิจิทัลแบบ**เว็บแอปพลิเคชัน**เท่านั้น ผู้ใช้งานจะได้รับแจ้ง service endpoint ของตนเองสำหรับแจ้งให้แก่ผู้ออกประกาศนียบัตรแบบเอกสารรับรองที่ตรวจสอบได้ (verifiable credential) ให้เข้ามาในกระเป๋าดิจิทัลของตนเองโดยตรง

กรณีศึกษา – GLEIF

GLEIF หรือ Global Legal Entity Identifier Foundation คือองค์กรไม่แสวงหาผลกำไรที่มีสำนักงานใหญ่อยู่ที่สวิตเซอร์แลนด์ ถูกจัดตั้งขึ้นเมื่อ ค.ศ. 2014 โดย Financial Stability Board ของ G20 Summit

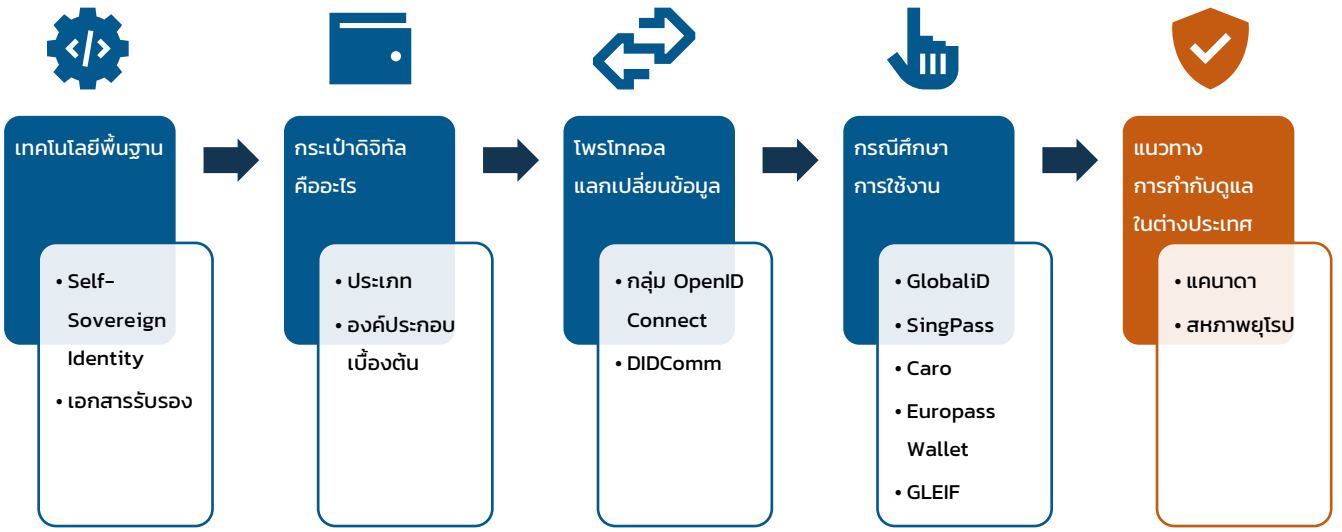
GLEIF มีจุดประสงค์ในการอำนวยความสะดวกให้ภาคธุรกิจและบุคคลทั่วไปสามารถทำธุรกรรมทางการเงินกับผู้อื่นได้อย่างมั่นใจ ด้วยการสนับสนุนการนำ Legal Entity Identifier (LEI) ซึ่งคือรหัสที่มีความยาว 20 ตัวอักษร (20-character code) ตามมาตรฐาน ISO 17442 ไปใช้เป็นไอเดนทิตีขององค์กร (organizational identity)

Verifiable LEI คือไอเดนทิตีองค์กรในรูปแบบดิจิทัล ที่ช่วยให้นิติบุคคลสามารถทำการยืนยันตัวตนและตรวจสอบเอกสารรับรองได้โดยอัตโนมัติภายใต้เทคโนโลยีกระจายศูนย์

โดย GLEIF ทำหน้าที่เป็น Root of Trust และกำหนดกรอบการกำกับดูแล (governance framework) สำหรับการออกเอกสารรับรอง และการผลิตกระเป๋าดิจิทัล เป็นต้น

ที่มา https://www.gleif.org/en/vlei/introducing-the-verifiable-lei-vlei

โครงร่างการนำเสนอ

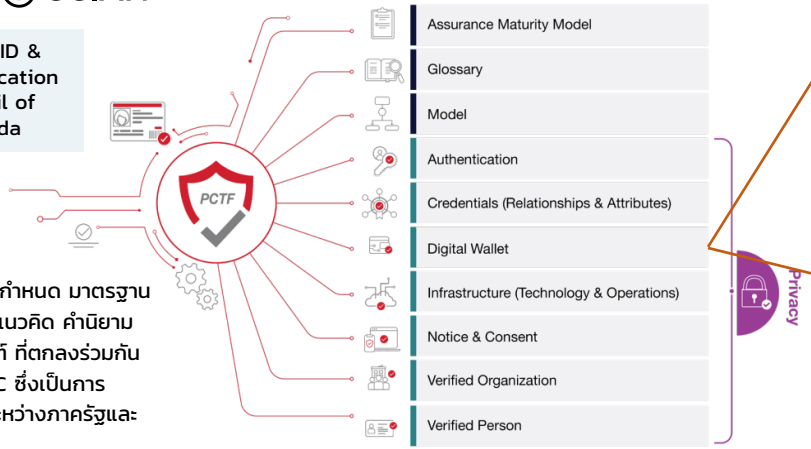


ตัวอย่างแนวทางการกำกับดูแล

แคนาดา – Pan-Canadian Trust Framework (PCTF)

DIACC CCIAN

Digital ID & Authentication Council of Canada



PCTF คือ ข้อกำหนด มาตรฐาน กระบวนการ แนวคิด คำนิยาม และหลักเกณฑ์ ที่ตกลงร่วมกันภายใน DIACC ซึ่งเป็นการรวมกลุ่มกันระหว่างภาครัฐและเอกชน

ข้อกำหนดเกี่ยวกับกระเป๋าดิจิทัล ประกอบด้วย 2 ส่วนคือ Component และ Conformance Profile


Pan-Canadian Trust Framework
PCTF Digital Wallet Component Overview Draft Recommendation V1.0
DIACC / PCTF12

DIACC CCIAN

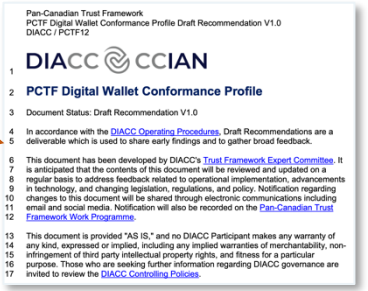
PCTF Digital Wallet Component Overview

Document Status: Draft Recommendation V1.0

In accordance with the DIACC Operating Procedures, Draft Recommendations are a deliverable which is used to share early findings and to gather broad feedback.

This document has been developed by DIACC's Trust Framework Expert Committee. It is anticipated that the contents of this document will be reviewed and updated on a regular basis to address feedback related to operational implementation, advancements in technology, and changing legislation, regulations, and policy. Notification regarding changes to this document will be shared through electronic communications including email and social media. Notification will also be recorded on the Pan-Canadian Trust Framework Work Programme.

This document is provided "AS IS," and no DIACC Participant makes any warranty of any kind, expressed or implied, including any implied warranties of merchantability, non-infringement of third party intellectual property rights, and fitness for a particular purpose. Those who are seeking further information regarding DIACC governance are invited to review the DIACC Controlling Policies.


Pan-Canadian Trust Framework
PCTF Digital Wallet Conformance Profile Draft Recommendation V1.0
DIACC / PCTF12

DIACC CCIAN

PCTF Digital Wallet Conformance Profile

Document Status: Draft Recommendation V1.0

In accordance with the DIACC Operating Procedures, Draft Recommendations are a deliverable which is used to share early findings and to gather broad feedback.

This document has been developed by DIACC's Trust Framework Expert Committee. It is anticipated that the contents of this document will be reviewed and updated on a regular basis to address feedback related to operational implementation, advancements in technology, and changing legislation, regulations, and policy. Notification regarding changes to this document will be shared through electronic communications including email and social media. Notification will also be recorded on the Pan-Canadian Trust Framework Work Programme.

This document is provided "AS IS," and no DIACC Participant makes any warranty of any kind, expressed or implied, including any implied warranties of merchantability, non-infringement of third party intellectual property rights, and fitness for a particular purpose. Those who are seeking further information regarding DIACC governance are invited to review the DIACC Controlling Policies.

ที่มา https://diacc.ca/wp-content/uploads/2022/03/PCTF-Privacy-Component-Overview-Final-Recommendation-V1.2.pdf

ตัวอย่างแนวทางการกำกับดูแล

สหภาพยุโรป – ภาพรวม

ชื่อ	สถานะ	องค์กรหลักที่เกี่ยวข้องในการกำกับดูแล	กฎหมายที่เกี่ยวข้อง	กรอบการทำงานสำหรับกระเป๋าดิจิทัล
European Digital Credentials Infrastructure (EDCI) Wallet	มีการให้บริการแล้ว	คณะกรรมาธิการยุโรป (European Commission)	• **Decision (EU) 2018/646** of the European Parliament and of the Council of 18 April 2018 on a common framework for the provision of better services for skills and qualifications (Europass) and repealing Decision No 2241/2004/EC	ข้อกำหนดใน documentation ของ EDCI[1]
European Blockchain Services Infrastructure (EBSI)-Conformant Wallet	กำลังอยู่ระหว่างการทดสอบนำร่องการให้บริการ	European Blockchain Partnership	• **Decision (EU) 2022/2481** of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030	ข้อกำหนดใน documentation ของ EBSI[2]
European Digital Identity (EUDI) Wallet	กำลังอยู่ระหว่างการทดสอบนำร่องการให้บริการ	คณะกรรมาธิการยุโรป (European Commission)	• Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity • Commission Recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework	EUDI Architecture Reference Framework

[1] Europass, "European Digital Credentials for Learning Infrastructure : Information for Developers", europa.eu/europass/en/stakeholders/european-digital-credentials/interoperability

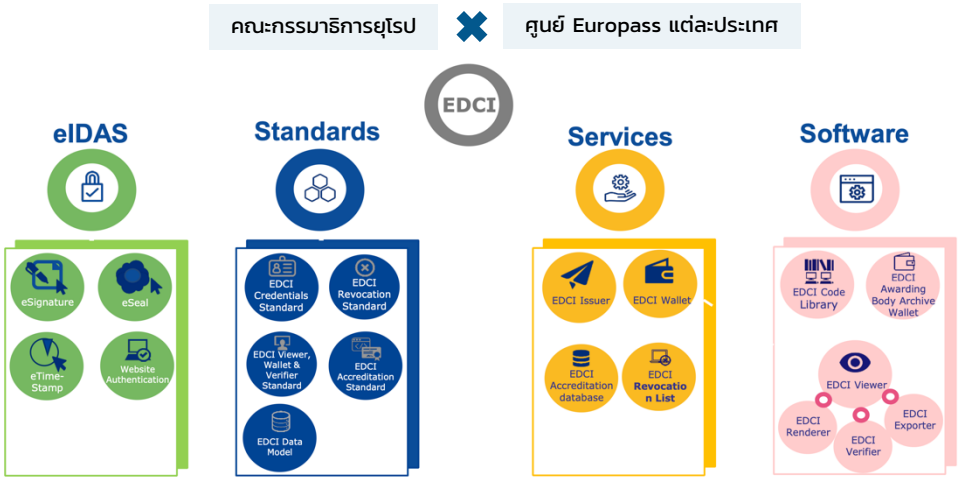
[2] EBSI, "EBSI developers hub", api-conformance.ebsi.eu/docs

ตัวอย่างแนวทางการกำกับดูแล

สหภาพยุโรป – European Digital Credentials Infrastructure (EDCI)

Decision (EU) 2018/646 of the European Parliament and of the Council of 18 April 2018 on a common framework for the provision of better services for skills and qualifications (Europass) and repealing Decision No 2241/2004/EC

การกำกับดูแลองค์ประกอบต่าง ๆ ของการให้บริการ อาทิ มาตรฐาน เอกสารรับรอง และการสร้างกระเป๋า ดำเนินการโดยคณะกรรมาธิการยุโรป โดยตรง ภายใต้ Decision (EU) 2018/646

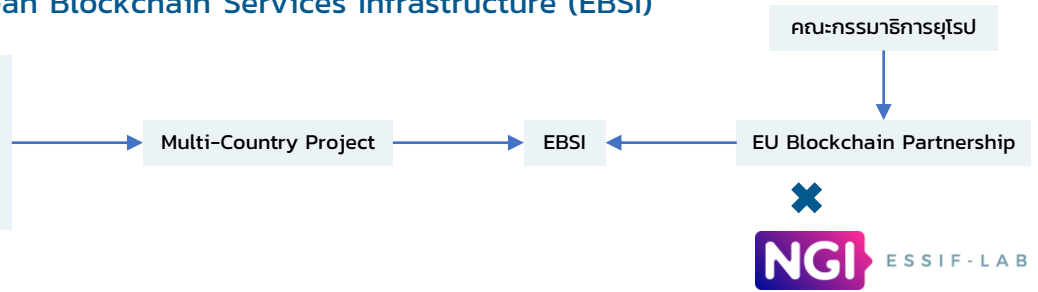


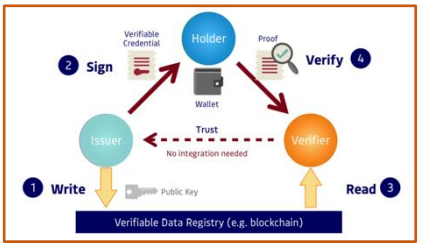
ที่มา https://microcredentials.eu/wp-content/uploads/sites/20/2019/10/Europass_Digital-Credentials-Masterclass_23-October-2019.pdf

ตัวอย่างแนวทางการกำกับดูแล

สหภาพยุโรป – European Blockchain Services Infrastructure (EBSI)

Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030





EBSI คือโครงสร้างพื้นฐานสำหรับการใช้งานเอกสารรับรองในกรณีที่ verifiable data registry เป็น blockchain

EBSI เป็นโครงการของ EU Blockchain Partnership ที่เรียกว่า "Multi-Country Project" ซึ่งเป็นโครงการชนิดพิเศษตาม Decision (EU) 2022/2481 ภายใต้แผนนโยบายระยะยาวที่มีชื่อว่า "Path to the Digital Decade" โดยใช้เงินสนับสนุนจาก Recovery and Resilience Facility ซึ่งเดิมสหภาพยุโรปจัดตั้งขึ้นเพื่อเป็นมาตรการชั่วคราวรองรับสถานการณ์โควิด-19

ที่มา https://trustoverip.org/wp-content/uploads/Introduction-to-ToIP-V2.0-2021-11-17.pdf

ตัวอย่างแนวทางการกำกับดูแล

สหภาพยุโรป – European Blockchain Services Infrastructure (EBSI)

Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030

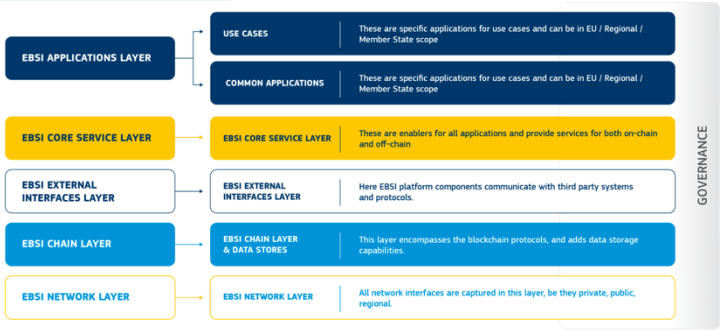
คณะกรรมาธิการยุโรป

EU Blockchain Partnership

EBSI

Multi-Country Project

NGI ESSIF-LAB



การกำกับดูแลไม่ได้มีข้อกำหนดจากส่วนกลางโดยตรง แต่ออกมาจาก EU Blockchain Partnership และกรอบการทำงาน European SSI Framework ซึ่งเป็นผลผลิตของโครงการวิจัย ESSIF-Lab ภายใต้โครงการ Next Generation Initiative (NGI) โดยคณะกรรมาธิการยุโรป

ที่มา European Commission, "Meet European Blockchain Services Infrastructure"

ตัวอย่างแนวทางการกำกับดูแล

สหภาพยุโรป – European Digital Identity (EUDI)

กฎหมายหลักที่กำกับดูแลบริการที่เชื่อถือได้ (trust service) ในสหภาพยุโรป คือกฎหมายที่มีชื่อเรียกโดยย่อว่า "eIDAS Regulation" ซึ่งไม่มีข้อกำหนดเกี่ยวกับการกำกับดูแลการให้บริการกระเป๋าดิจิทัลโดยตรง การกำกับดูแลการให้บริการกระเป๋าดิจิทัลเป็นเรื่องที่ประเทศสมาชิกแต่ละประเทศดำเนินการแยกกันเอง จนกระทั่งเมื่อมีการเสนอกฎหมายที่เรียกว่า "ร่าง eIDAS 2.0" จึงเรียกได้ว่าสหภาพยุโรปมี (หรือกำลังจะมี) กฎหมายกำกับดูแลการให้บริการกระเป๋าดิจิทัลโดยตรง

"Toolbox Recommendation" เป็นผลสืบเนื่องมาจาก "ร่าง eIDAS 2.0" โดยปัจจุบันมีผลทางกฎหมายแล้ว และนำมาสู่ EUDI Wallet ARF


The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework

The European Digital Identity Wallet Architecture and Reference Framework

January 2023

Version 1.0.0

eIDAS Regulation[1] → ร่าง eIDAS 2.0[2] → Toolbox Recommendation[3] → EUDI Wallet Architecture and Referencee Framework[4]

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[2] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity

[3] Commission Recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework

[4] digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework

ตัวอย่างแนวทางการกำกับดูแล

สหภาพยุโรป – สาระสำคัญบางส่วนเกี่ยวกับกระเป๋าฯ ในร่าง eIDAS 2.0

มาตรา	สรุปสาระสำคัญ
(Preamble ข้อ 36)	(ข้อนี้เป็นคำอธิบายเจตนารมณ์ของกฎหมาย ไม่ใช่ข้อบังคับ) จะมีการออก “Toolbox Recommendation”
1 ข้อ d	Regulation นี้จะกำหนดว่า การที่ประเทศสมาชิกจะออก EUDI Wallet ให้ประชาชนใช้งาน ต้องทำตามเงื่อนไขใดบ้าง
2 ข้อ 1	Regulation นี้ใช้กับ EUDI Wallet ที่ประเทศสมาชิกออกให้ประชาชนใช้งาน
3 ข้อ 2	ให้วลีว่า “electronic identification means” มีความหมายครอบคลุมถึง EUDI Wallet ด้วย
3 ข้อ 42	นิยามว่า EUDI Wallet คืออะไร
6a	ข้อกำหนดหลักของ EUDI Wallet
6b	ข้อกำหนดสำหรับผู้อาศัยการยืนยันตัวตน (relying party) ผ่าน EUDI Wallet
6c	การรับรองว่า EUDI Wallet เป็นไปตามข้อกำหนด
6d	การเผยแพร่รายการ EUDI Wallet ที่ได้รับการรับรองแล้ว
10a	มาตรการรองรับกรณีเกิดความไม่มั่นคงปลอดภัยในการใช้งาน EUDI Wallet
12b	กำหนดให้ใช้ EUDI Wallet สำหรับการยืนยันตัวตนข้ามประเทศได้
48a	การเก็บสถิติการใช้งาน EUDI Wallet เพื่อรายงานแก่คณะกรรมาธิการยุโรป

ตัวอย่างแนวทางการกำกับดูแล

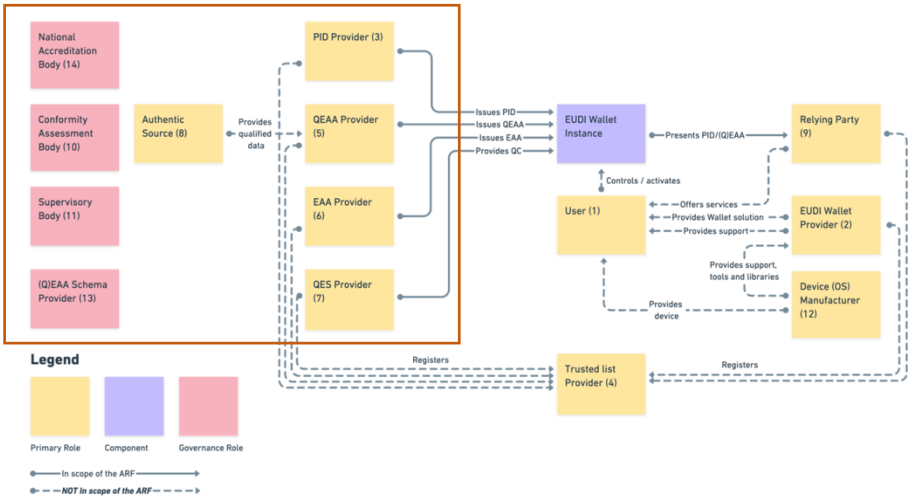
สหภาพยุโรป – European Digital Identity (EUDI) : โครงสร้างการกำกับดูแลคุณภาพการให้บริการ

ผู้ให้บริการต่าง ๆ ได้แก่

- PID provider (เอกสารรับรอง)
- [Q]EAA provider (เอกสารรับรอง)
- QES provider (ลายมือชื่ออิเล็กทรอนิกส์)
- EUDI wallet provider (กระเป๋าดิจิทัล)

อยู่ภายใต้โครงสร้างการกำกับดูแลคุณภาพการให้บริการ ที่ประกอบด้วยองค์กร 4 ประเภท ได้แก่

- supervisory body : กำหนดกรอบการกำกับดูแลคุณภาพ
- conformity assessment body (CAB) : ประเมินคุณภาพ
- national accreditation body : รับรอง CAB
- [Q]EAA schema provider : ประกาศใช้ schema/vocabulary มาตรฐาน



ที่มา EUDI Wallet Architecture and Referencee Framework, digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework

e-Standard

03 เม.ย. 66 | 548 | Share

เผยแพร่ ETDA Technical Report กรอบการทำงานร่วมกันของกระเป๋าดิจิทัลสำหรับเอกสารรับรอง (เวอร์ชัน 1.0 – เมษายน 2566)

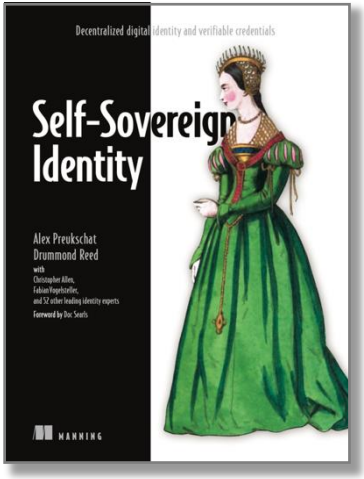
Technical Report
bit.ly/ETDA_DigitalWallet

โครงสร้างเอกสาร

1. **ขอบข่าย**
2. **บทนิยาม**
3. **ภาพรวมของกระเป๋าดิจิทัลสำหรับเอกสารรับรอง**
   - 3.1 บทบาทและความสัมพันธ์ของเอนทิตีที่เกี่ยวข้อง
   - 3.2 เอกสารรับรองและเอกสารสำแดง
   - 3.3 ระบบทะเบียนเอกสารรับรอง (verifiable data registry)
   - 3.4 ประเภทกระเป๋าดิจิทัล
   - 3.5 การสำรองและกู้คืนข้อมูลความลับ
   - 3.6 การคุ้มครองข้อมูลส่วนบุคคลของผู้ถือเอกสาร
   - 3.7 กลไกการเชื่อมโยงผู้ถือเอกสารต่อเอกสารรับรอง
4. **วงจรชีวิตของกระเป๋าดิจิทัลและเอกสารรับรอง**
   - 4.1 วงจรชีวิตการใช้งานอินสแตนซ์ของกระเป๋าดิจิทัล
   - 4.2 วงจรชีวิตการใช้งานเอกสารรับรอง
5. **องค์ประกอบของกระเป๋าดิจิทัล**
   - 5.1 องค์ประกอบพื้นฐานของกระเป๋าดิจิทัล
   - 5.2 สถาปัตยกรรมซอฟต์แวร์ของกระเป๋าดิจิทัล
   - 5.3 ช่องทางการแลกเปลี่ยนเอกสารรับรอง
6. **ข้อแนะนำของกระเป๋าดิจิทัลและเอกสารรับรอง**
   - 6.1 ประเภทของเอกสารรับรองตามความสำคัญของข้อมูล
   - 6.2 ข้อแนะนำของเอกสารรับรอง
   - 6.3 ข้อแนะนำการพัฒนาองค์ประกอบของกระเป๋าดิจิทัล

บรรณานุกรม

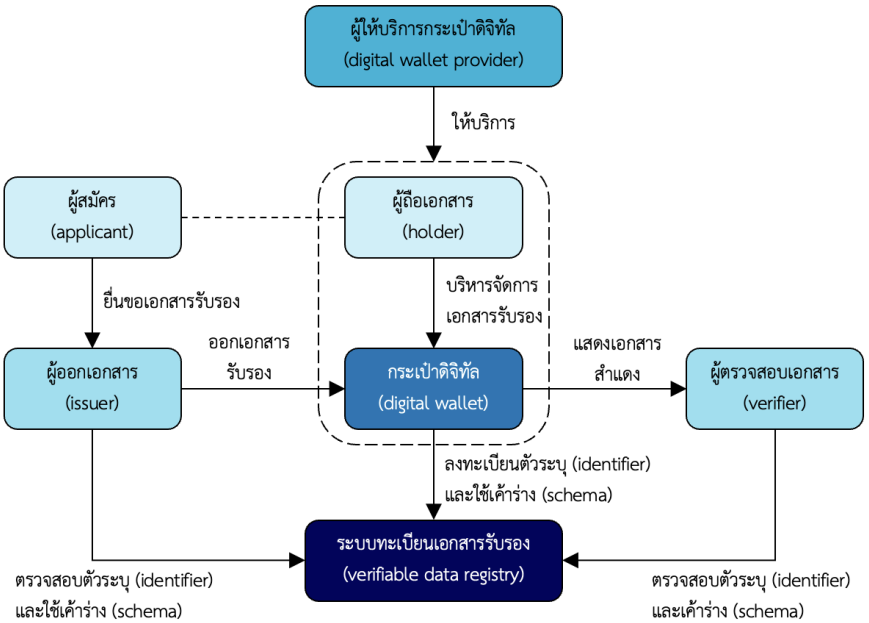
เอกสารอ้างอิงที่สำคัญ



Self-Sovereign Identity
Alex Preukschat and Drummond Reed
Manning Publications (2021)

The European Digital Identity Wallet Architecture and Reference Framework
European Commission (2023)

บทบาทและความสัมพันธ์



(1) ผู้ถือเอกสาร (holder) ใช้งานกระเป๋าดิจิทัล (digital wallet) ที่ให้บริการโดยผู้ให้บริการกระเป๋าดิจิทัล (digital wallet provider)

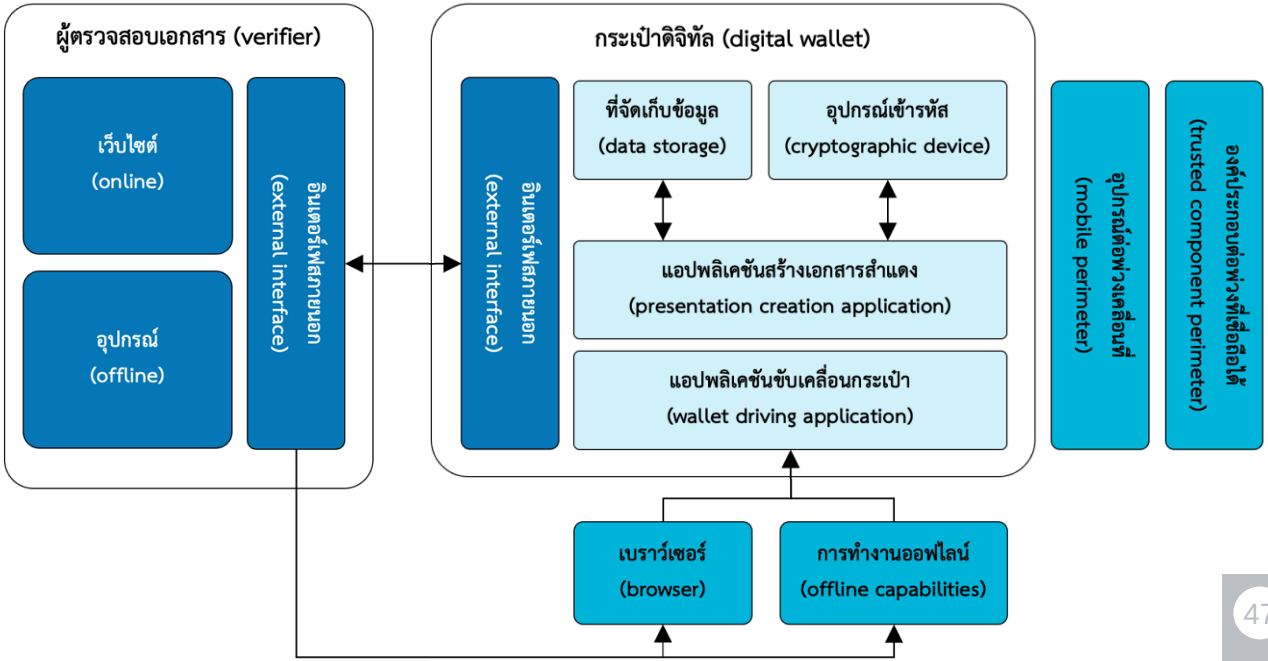
(2) ผู้สมัคร (applicant) ยื่นขอเอกสารรับรองจากผู้ออกเอกสาร (issuer)

(3) ผู้สมัคร ผู้ถือเอกสาร และเจ้าของข้อความ (subject) อาจเป็นบุคคลเดียวกันหรือไม่ก็ได้

(4) ผู้ถือเอกสารสามารถสร้างเอกสารสำแดงและแสดงต่อผู้ตรวจสอบเอกสาร (verifier)

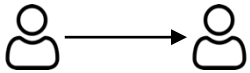
(5) ระบบทะเบียนเอกสารรับรอง (verifiable data registry) เป็นตัวกลางในการตรวจสอบเอกสารรับรองและเอกสารสำแดง

องค์ประกอบกระเป๋าดิจิทัล

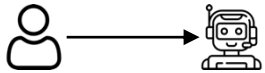


ช่องทางการแลกเปลี่ยนเอกสารรับรอง

ช่องทางระยะใกล้ โดยผู้ตรวจสอบเอกสารเป็นบุคคล
(Close Proximity Supervised Flow)

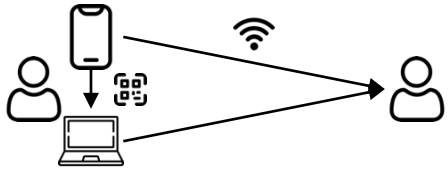


ช่องทางระยะใกล้ โดยระบบอัตโนมัติ
(Close Proximity Unsupervised Flow)



ช่องทางระยะไกลภายในอุปกรณ์เดียวกัน
(Remote Same-device Flow)

ช่องทางระยะไกล ข้ามอุปกรณ์
(Remote Cross-device Flow)



ข้อแนะนำของเอกสารรับรอง

Issuer Identification

สามารถระบุตัวตนของผู้ออกเอกสารได้

Data Integrity

สามารถตรวจพบการเปลี่ยนแปลงใด ๆ
ที่เกิดขึ้นต่อของเอกสารรับรองได้

Authenticity

สามารถตรวจสอบที่มาของเอกสารรับรองได้
ว่าออกโดยผู้ออกเอกสารตามที่ระบุจริง

Status Check

สามารถตรวจสอบสถานะของเอกสารรับรอง
ว่าถูกระงับหรือเพิกถอนหรือไม่

Holder Binding

สามารถตรวจสอบการเชื่อมโยงของผู้ถือเอกสาร
ต่อเอกสารรับรอง

ข้อแนะนำการพัฒนาองค์ประกอบของกระเป๋าดิจิทัล

Data Model

- W3C Verifiable Credentials Data Model 1.1
- ISO/IEC 18013-5:2021
- หรือมาตรฐานอื่น ๆ ซึ่งเป็นที่ยอมรับในระดับสากล

Data Format

- JSON Web Token (JWT)
- JSON for Linked Data (JSON-LD)
- Concise Binary Object Representation (CBOR)

Signature/Encryption Format

- Javascript Object Signing and Encryption (JOSE)
- Linked Data Proofs (LD-Proofs)
- CBOR Object Signing and Encryption (COSE)

Selective Disclosure

- ISO/IEC 18013-5:2021
- Selective Disclosure JWT (IETF SD-JWT Draft)

Holder Binding

- การเชื่อมโยงกับอุปกรณ์ของผู้ใช้งาน (device binding)
- การเชื่อมโยงกับข้อมูลชีวมิติของผู้ใช้งาน (biometric binding)

Transport Protocol

- OpenID for Verifiable Credential (OpenID4VCI)
- OpenID for Verifiable Presentations (OpenID4VP)
- Self-Issued OpenID Provider v2 (SIOPv2)

ประเภทของเอกสารรับรองตามความสำคัญของข้อมูล

เอกสารรับรองสามารถแบ่งออกเป็น 2 ประเภท ตามความสำคัญของข้อมูลในเอกสารรับรอง ดังนี้

(1) เอกสารรับรองประเภท 1: เป็นเอกสารรับรองที่มีข้อมูลสำคัญ ซึ่งเหมาะสำหรับการระบุตัวตนบุคคลในธุรกรรมที่มีความเสี่ยงสูง ตัวอย่างเช่น บัตรประจำตัวประชาชน ใบอนุญาตขับขี่

(2) เอกสารรับรองประเภท 2: เป็นเอกสารรับรองที่มีข้อมูลทั่วไป ซึ่งเหมาะสำหรับการใช้งานที่หลากหลายในธุรกรรมที่ไม่มีความเสี่ยงสูง ตัวอย่างเช่น บัตรสะสมคะแนน ตั๋วโดยสารที่ไม่ระบุชื่อผู้ถือตั๋ว

ภาพรวมของมาตรฐานของกระเป๋าดิจิทัล