ETDA สพธอ www.etda.or.th | กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วย

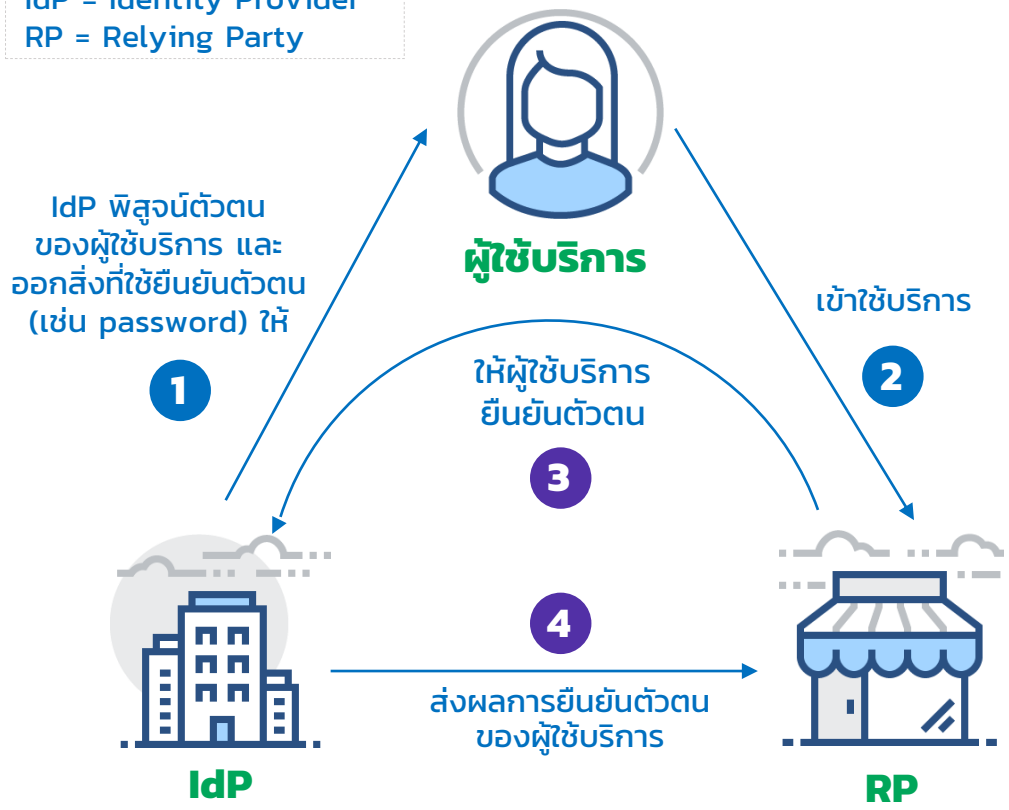
โครงสร้างข้อมูลของเอกสารรับรองและเอกสารสำแดง

(Data Structure of Verifiable Credentials and Presentations)

เลขที่ ขมธอ. 24-2563

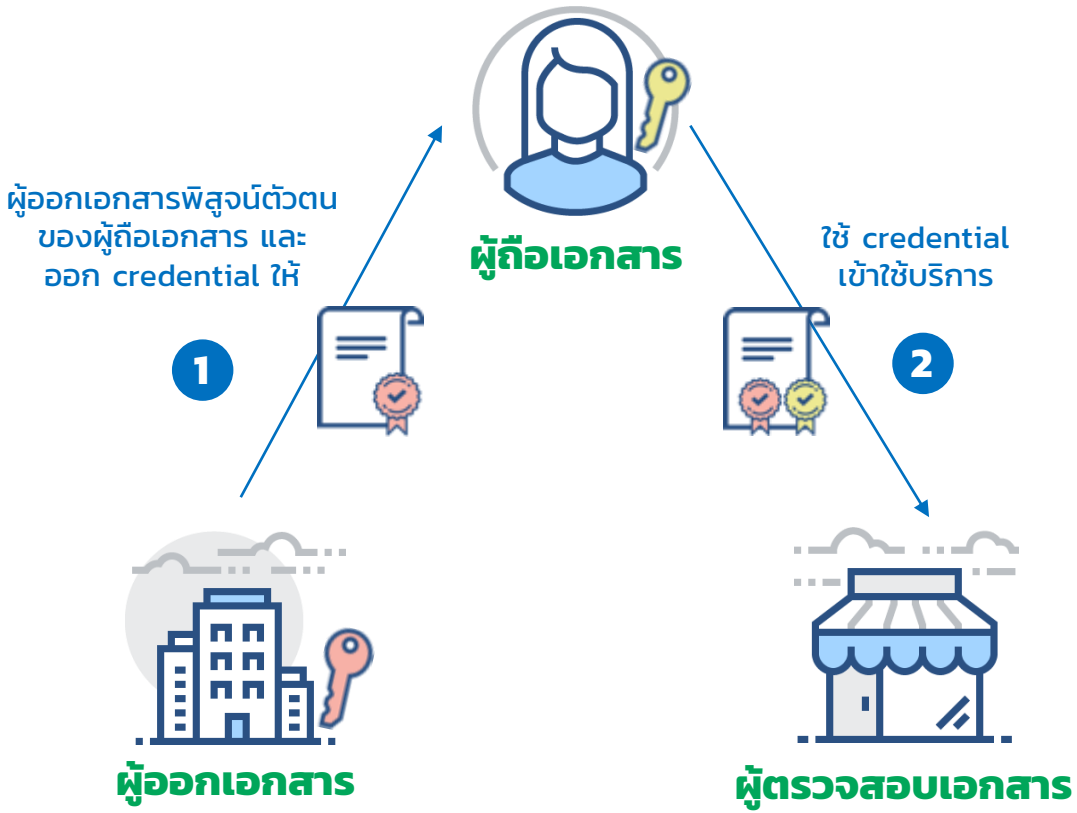
TRANSACTION
BASED AUTHENTICATION

IdP = Identity Provider
RP = Relying Party



RP ให้ผู้ใช้บริการไปยืนยันตัวตนกับ IdP และ IdP จะส่งผลการยืนยันตัวตนกลับให้ RP

CREDENTIAL
BASED AUTHENTICATION



ผู้ตรวจสอบเอกสารสามารถตรวจสอบและเชื่อถือคุณลักษณะใน credential ได้ **โดยไม่ต้องกลับไปให้ผู้ออกเอกสารยืนยัน**

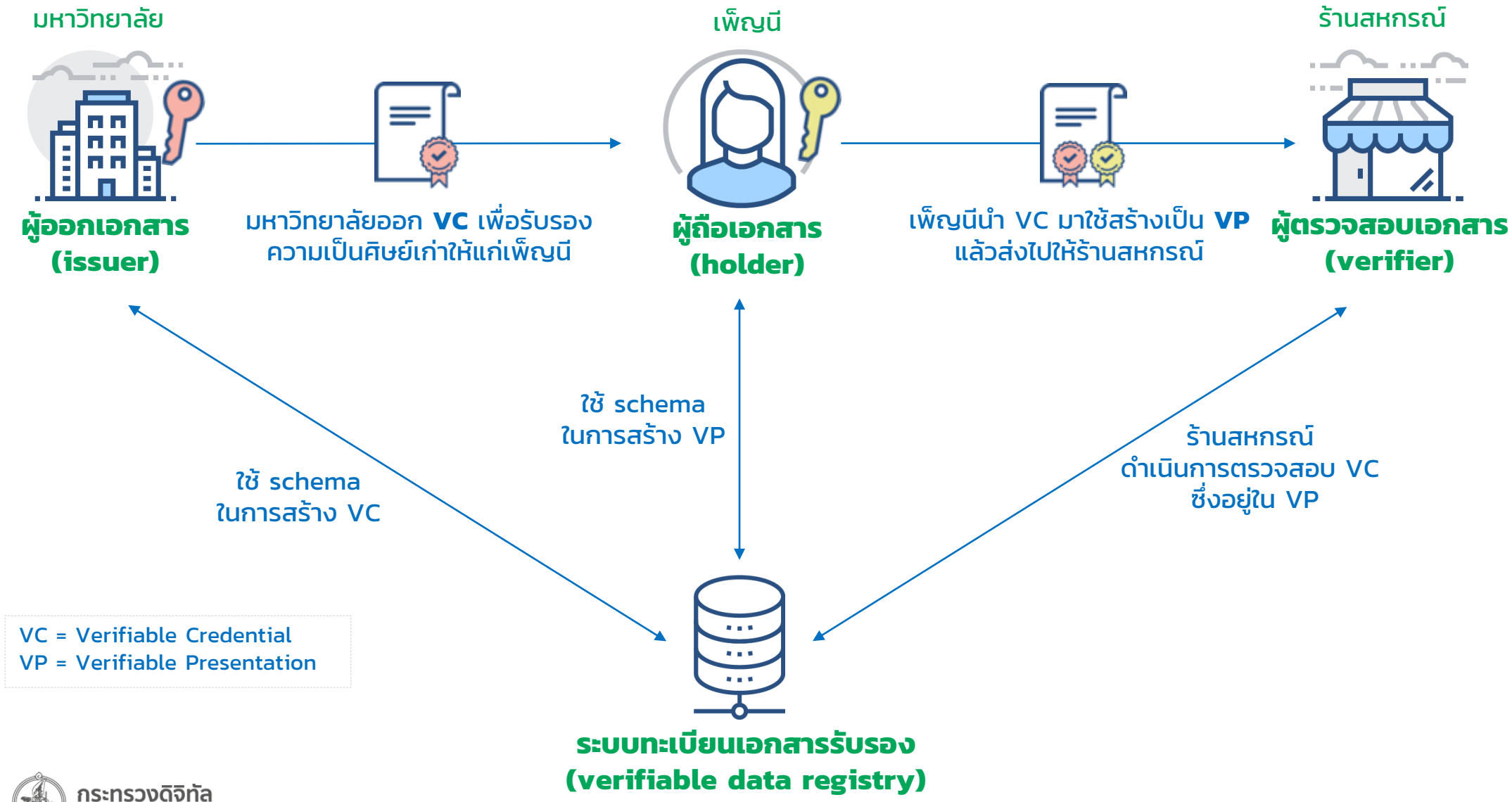
เอกสารรับรอง (verifiable credential: VC) และ
เอกสารสำแดง (verifiable presentation: VP)
สามารถนำไปใช้เป็นเอกสารอิเล็กทรอนิกส์

ตัวอย่างเช่น

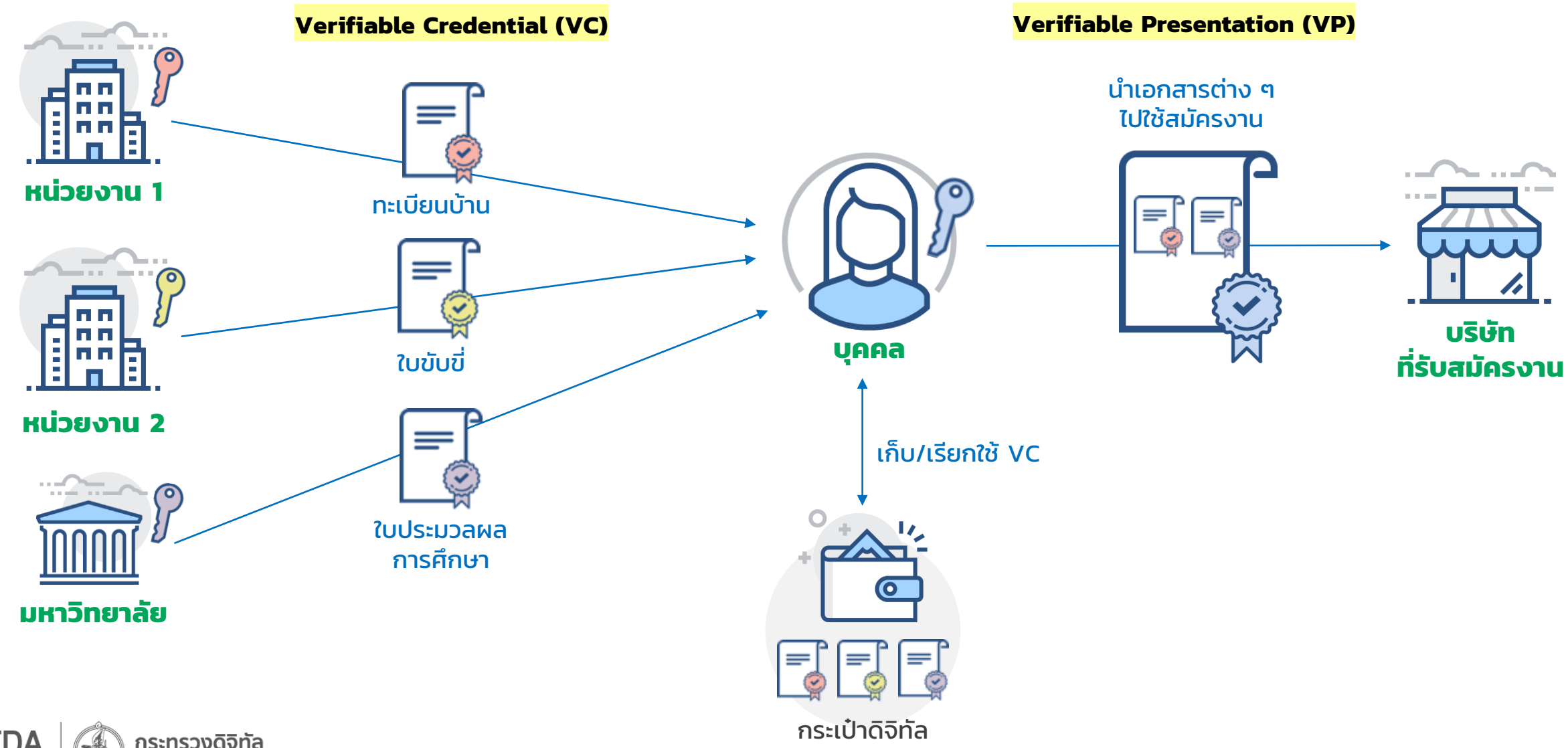
- หนังสือให้ความยินยอม
- หนังสือมอบอำนาจ
- ใบปริญญาบัตรที่มหาวิทยาลัยออกให้แก่นักศึกษา
- ใบรับรองแพทย์ที่แพทย์ออกให้แก่ผู้ป่วย

VC และ VP จะ**มีคุณสมบัติที่สามารถตรวจสอบความถูกต้องครบถ้วนของข้อมูล**และ**ตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ของผู้ออกเอกสาร**และ**ผู้ถือเอกสาร**ได้ด้วย**กระบวนการเข้ารหัสลับ**

ความเชื่อมโยงในการใช้งาน VC และ VP ระหว่างเอนทิตีที่เกี่ยวข้อง

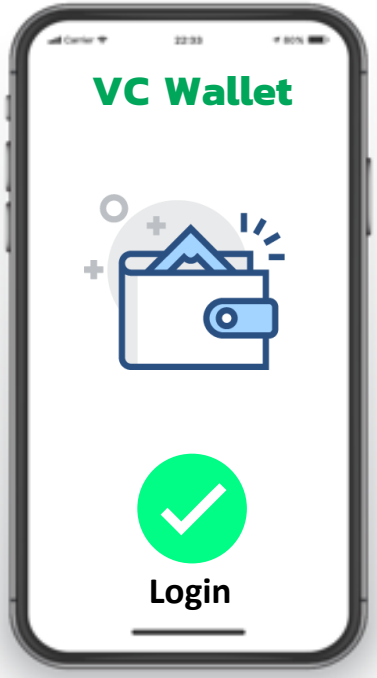


ตัวอย่างการใช้งาน VC และ VP



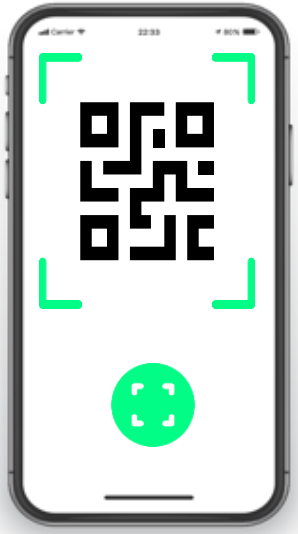
ตัวอย่าง User Journey ขั้นตอนการรับ VC

- ผู้ถือเอกสารยื่นขอ VC จากผู้ออกเอกสาร
- และ ผู้ออกเอกสารจะพิสูจน์ตัวตนของผู้ถือเอกสารก่อนออก VC ให้



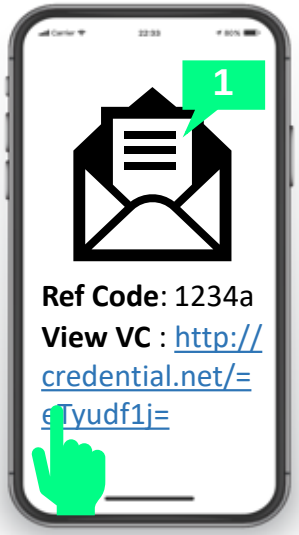
ผู้ถือเข้าแอป VC wallet

การรับ VC แบบ On-site

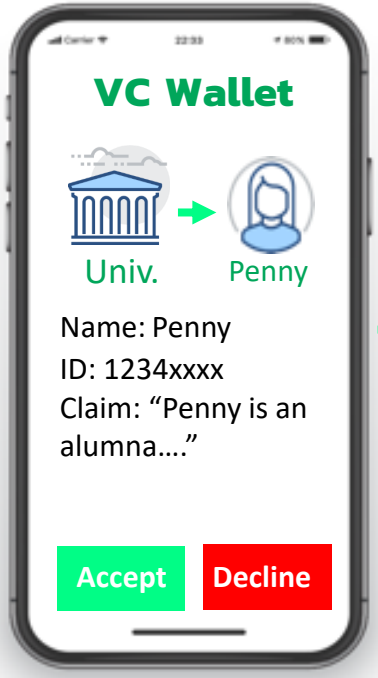


ผู้ถือเอกสารสแกน QR code ที่ผู้ออกเอกสารออกให้

การรับ VC แบบ Online



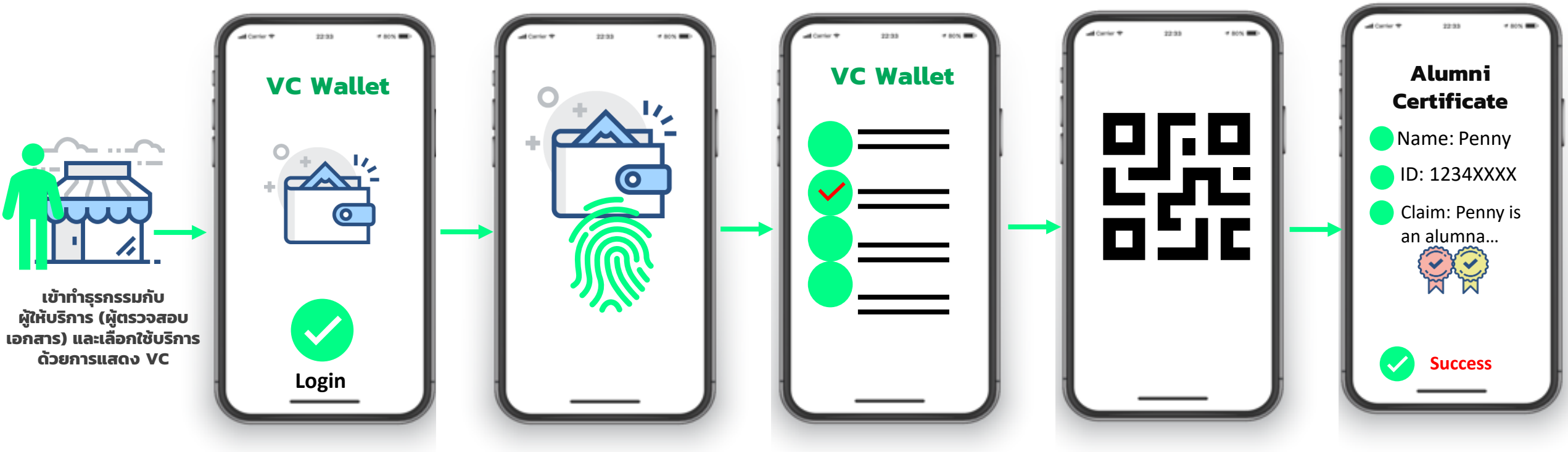
ผู้ถือเอกสารได้รับอีเมล ตรวจสอบ Ref code และคลิกดู VC



ผู้ถือเอกสารตรวจสอบความถูกต้องของ VC และกดยอมรับ

VC ถูกเพิ่มเข้ามาใน VC wallet

ตัวอย่าง User Journey
ขั้นตอนการใช้ VC แบบ On-site



เข้าทำธุรกรรมกับผู้ให้บริการ (ผู้ตรวจสอบเอกสาร) และเลือกใช้บริการด้วยการแสดง VC

เข้าแอป wallet

ผู้ถือเอกสารปลดล็อก wallet ตามวิธีการที่เลือกไว้ เช่น Fingerprint

เลือก VC เพื่อสร้าง VP

ผู้ให้บริการ (ผู้ตรวจสอบเอกสาร) สแกน QR ของผู้ถือเอกสารเพื่อรับ VP

ผู้ตรวจสอบเอกสารได้รับ VP

ตัวอย่าง User Journey ขั้นตอนการใช้ VC แบบ Online

เข้าทำธุรกรรมกับแอปพลิเคชันของผู้ให้บริการ (ผู้ตรวจสอบเอกสาร) และเลือกใช้บริการด้วยการแสดง VC

ผู้ให้บริการ redirect ให้เข้าแอป wallet

ผู้ถือสารปลดล็อก wallet ตามวิธีการที่เลือกไว้ เช่น Fingerprint

เลือก VC เพื่อสร้าง VP

ผู้ตรวจสอบเอกสารได้รับ VP

โครงสร้างข้อมูลของเอกสารรับรองและเอกสารสำแดง
(Data Structure of Verifiable Credentials and Presentations)

ขอบข่าย

- กำหนด**โครงสร้างข้อมูล**สำหรับ**เอกสารรับรอง (Verifiable Credential: VC)** และ**เอกสารสำแดง (Verifiable Presentation: VP)**
- และอธิบาย**ความเชื่อมโยง**ในการใช้งาน VC และ VP ระหว่างเอนทิตีที่เกี่ยวข้อง ซึ่งประกอบด้วยผู้ออกเอกสาร (issuer) ผู้ถือเอกสาร (holder) และผู้ตรวจสอบเอกสาร (verifier)

เพื่อให้ผู้ถือเอกสารสามารถใช้ VC และ VP ใน**การพิสูจน์และยืนยันตัวตน การให้ความยินยอม การมอบอำนาจ** หรือ**การแสดงข้อมูลที่ถูกรับรองแก่ผู้อื่น** ในรูปแบบอิเล็กทรอนิกส์ที่

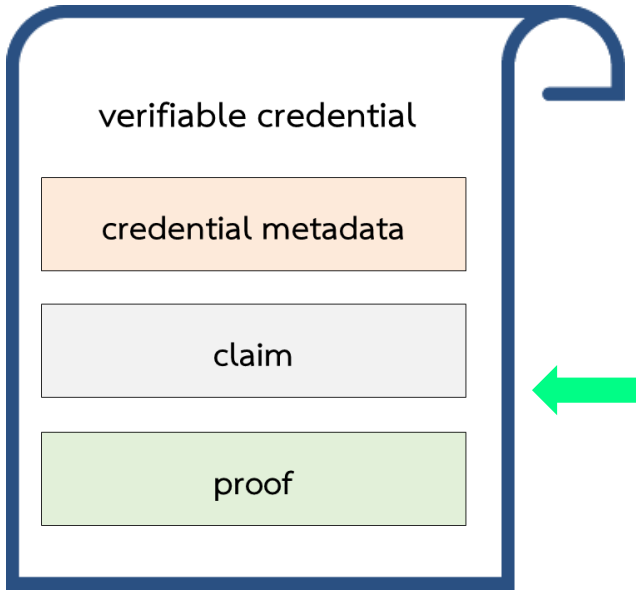
- มีความมั่นคงปลอดภัย
- มีการรักษาความเป็นส่วนตัว
- สามารถตรวจสอบได้ด้วยกระบวนการเข้ารหัสลับ และ
- สนับสนุนการแลกเปลี่ยนระหว่างกันตามมาตรฐานสากล

โครงสร้างของเอกสาร

เอกสารรับรอง
(verifiable credential: VC)

หมายถึง **ชุดของข้อความยืนยัน (claim)** อย่างน้อยหนึ่งรายการที่ถูกรับรองโดย**ผู้ออกเอกสาร (issuer)** ทั้งนี้ VC มีคุณสมบัติที่สามารถตรวจพบการเปลี่ยนแปลงใด ๆ ที่เกิดกับความถูกต้องครบถ้วนของข้อมูล และตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ของผู้ออกเอกสารได้ด้วยกระบวนการเข้ารหัสลับ

Data model

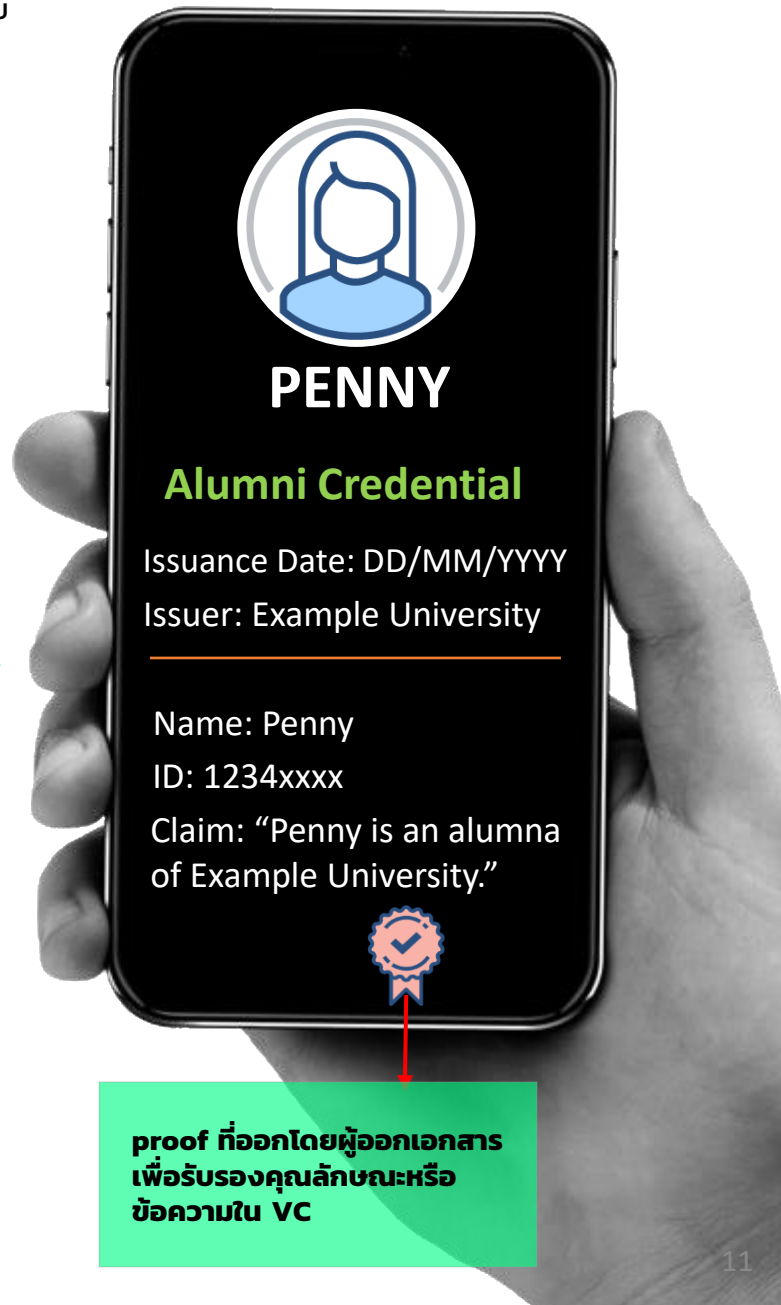


ตัวอย่าง:

มหาวิทยาลัยออก **VC เพื่อรับรองความเป็นศิษย์เก่า**ให้แก่เพ็ญนี และเพ็ญนีเก็บ VC นั้นไว้ในกระเป๋าดิจิทัลของตนเอง

JSON-LD file

```
{
 "@context": [
  "https://www.w3.org/2018/credentials/v1",
  "https://www.w3.org/2018/credentials/examples/v1"],
 "id": "http://example.edu/credentials/1872"
 "type": ["VerifiableCredential", "AlumniCredential"],
 "issuer": "https://example.edu/issuers/565049",
 "issuanceDate": "2010-01-01T19:73:24Z",
 "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "alumniOf": {
      "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",
      "name": [{
        "value": "Example University",
        "lang": "en"
      }, {
        "value": "มหาวิทยาลัยสมมุติ",
        "lang": "th"
      }]
    }
 },
 "proof": {
    "type": "RsaSignature2018",
    "created": "2017-06-18T21:19:10Z",
    "proofPurpose": "assertionMethod",
    "verificationMethod": "https://example.edu/issuers/keys/1",
    "jws": "eyJhb..."
 }
}
```



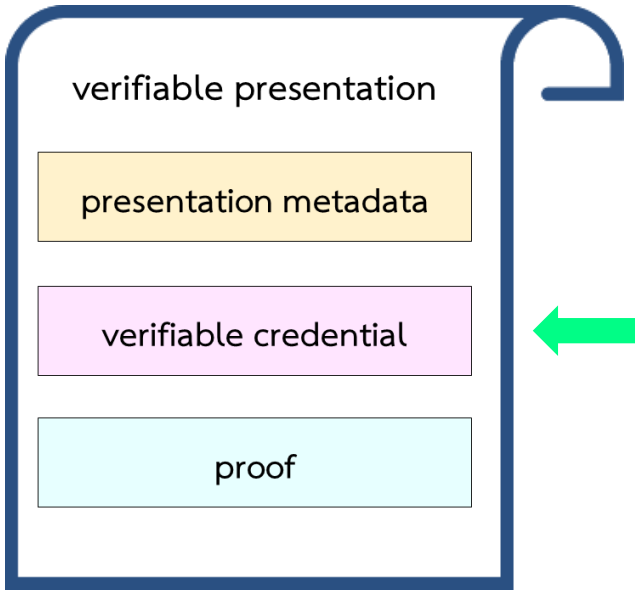
proof ที่ออกโดยผู้ออกเอกสารเพื่อรับรองคุณลักษณะหรือข้อความใน VC

เอกสารสำแดง
(verifiable presentation: VP)

หมายถึง **VC อย่างน้อยหนึ่งชุด** ที่**ผู้ถือเอกสาร (holder)** ใช้**แสดงต่อผู้ตรวจสอบเอกสาร (verifier)** ทั้งนี้ VP มีคุณสมบัติที่สามารถตรวจพบการเปลี่ยนแปลงใด ๆ ที่เกิดกับความถูกต้องครบถ้วนของข้อมูล และตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ของผู้ถือเอกสารและตรวจสอบ VC ที่เกี่ยวข้องได้ด้วยกระบวนการเข้ารหัสลับ

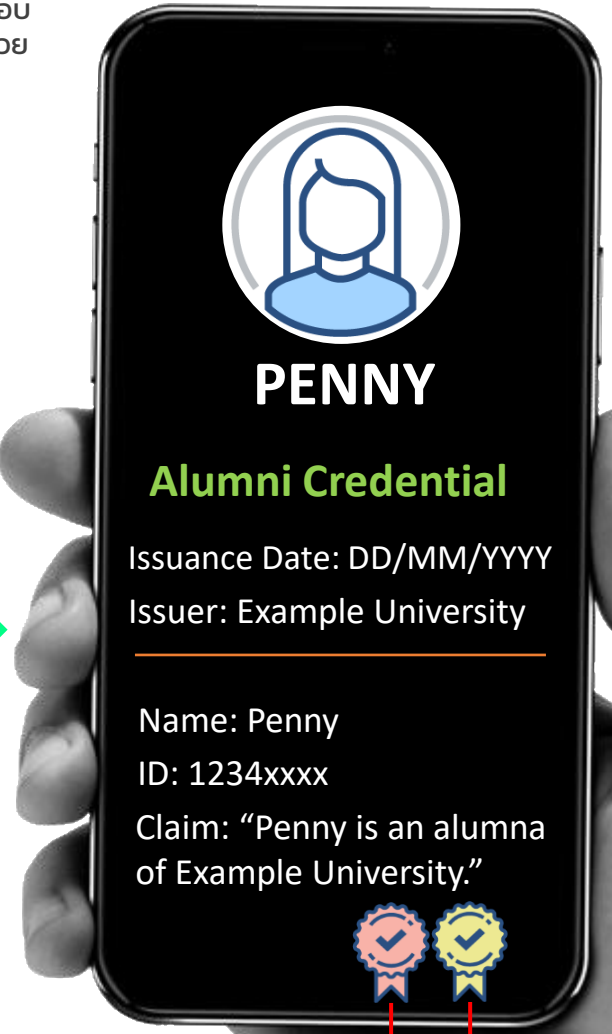
ETDA สพธอ www.etda.or.th | กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม

Data model



JSON-LD file

```
{
 "@context": [
  "https://www.w3.org/2018/credentials/v1",
  "https://www.w3.org/2018/credentials/examples/v1"],
 "type": "VerifiablePresentation",
 "verifiableCredential": [{
   "@context": [...],
   "id": "http://example.edu/credentials/1872",
   "type": ["VerifiableCredential", "AlumniCredential"],
   "issuer": "https://example.edu/issuers/565049",
   "issuanceDate": "2010-01-01T19:73:24Z",
   "credentialSubject": {...},
   "proof": {...}
 "proof": {
   "type": "RsaSignature2018",
   "created": "2018-09-14T21:19:10Z",
   "proofPurpose": "authentication",
   "verificationMethod": "did:example:ebf...e12ec21#keys-1",
   "challenge": "1f44d55f-f161-4938-a659-f8026467f126",
   "domain": "4jt78h47fh47",
   "jws": "eyJ..."
 }
}
```



ตัวอย่าง:

เพ็ญนีจะขอรับส่วนลดจากร้านสหกรณ์มหาวิทยาลัย เพ็ญนีจึงนำ **VC เพื่อรับรองความเป็นศิษย์เก่า มาใช้สร้างเป็น VP** แล้วส่งต่อไปให้ร้านสหกรณ์ดำเนินการตรวจสอบ

proof ที่ออกโดยผู้ออกเอกสาร เพื่อรับรองคุณลักษณะหรือข้อความใน VC

proof ที่ออกโดยผู้ถือเอกสาร เพื่อส่งให้กับผู้ตรวจสอบเอกสาร

หลักการที่สำคัญของการใช้งาน VC และ VP

Control and Access:
ผู้ถือเอกสารสามารถควบคุมและเข้าถึงข้อความยืนยันใน VC ของตนเองได้

Consent:
หากเป็นไปได้ การนำข้อความยืนยันของเจ้าของข้อความไปใช้งานควรได้รับความยินยอมจากเจ้าของข้อความ

Minimization:
รองรับการเปิดเผยข้อความยืนยันเท่าที่จำเป็น

Transparency:
ระบบและอัลกอริทึมในการใช้งาน VC และ VP ต้องมีความโปร่งใส

Portability:
รองรับการย้าย VC จากกระเป๋าดิจิทัลเดิมไปยังกระเป๋าดิจิทัลใหม่ได้

Reference: Christopher Allen, "The Path to Self-Sovereign Identity", April 2016 [Online]. Available: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.