



ETDA  
สทศ  
www.elda.or.th



กระทรวงดิจิทัล  
เพื่อเศรษฐกิจและสังคม

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยี  
สารสนเทศและการสื่อสารที่จำเป็นต่อ  
ธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วย

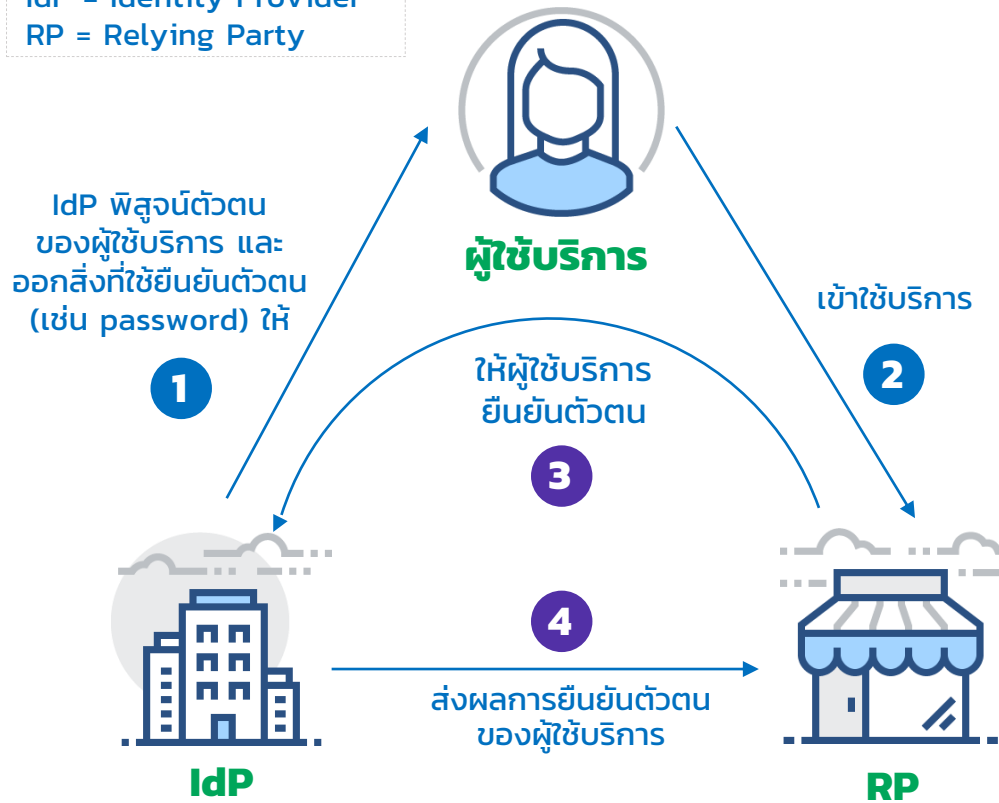
## โครงสร้างข้อมูลของเอกสารรับรอง และเอกสารสำแดง

(Data Structure of Verifiable Credentials and Presentations)

เลขที่ ขมธอ. 24-2563

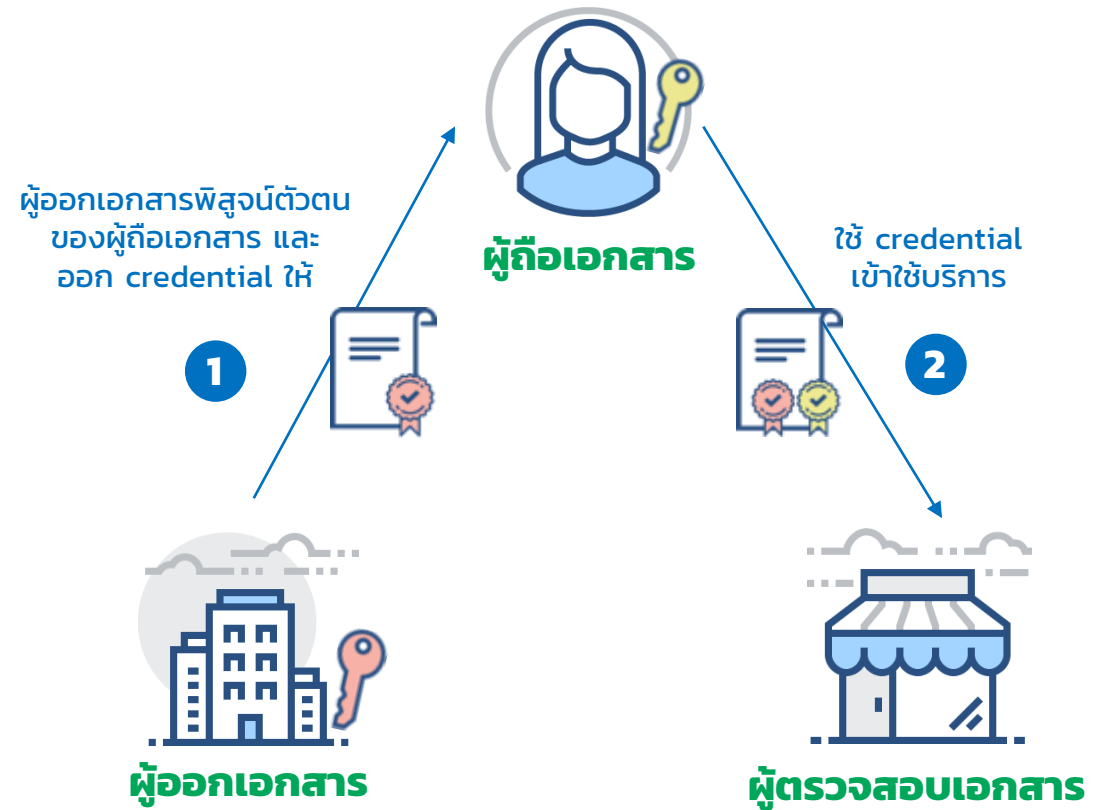
# IdP - Based Authentication

IdP = Identity Provider  
RP = Relying Party



RP ให้ผู้ให้บริการไปยืนยันตัวตนกับ IdP และ IdP จะส่งผลการยืนยันตัวตนกลับให้ RP

# Public Key - Based Authentication



ผู้ตรวจสอบเอกสารสามารถตรวจสอบและเชื่อถือคุณลักษณะใน credential ได้ **โดยไม่ต้องกลับไปให้ผู้ออกเอกสารยืนยัน**



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

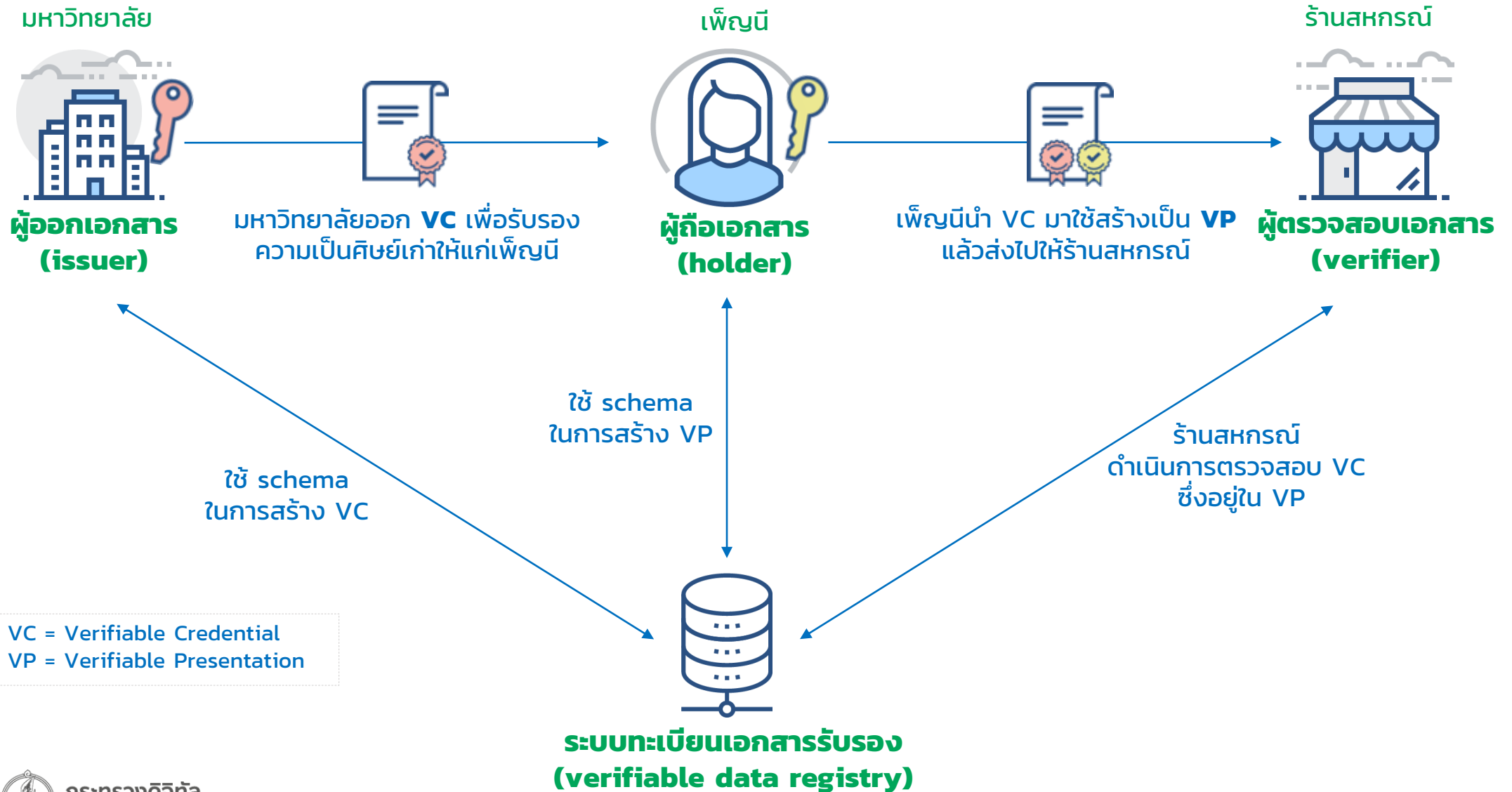
ตัวอย่างเช่น

- หนังสือให้ความยินยอม
- หนังสือมอบอำนาจ
- ใบปริญญาบัตรที่มหาวิทยาลัยออกให้แก่นักศึกษา
- ใบรับรองแพทย์ที่แพทย์ออกให้แก่ผู้ป่วย

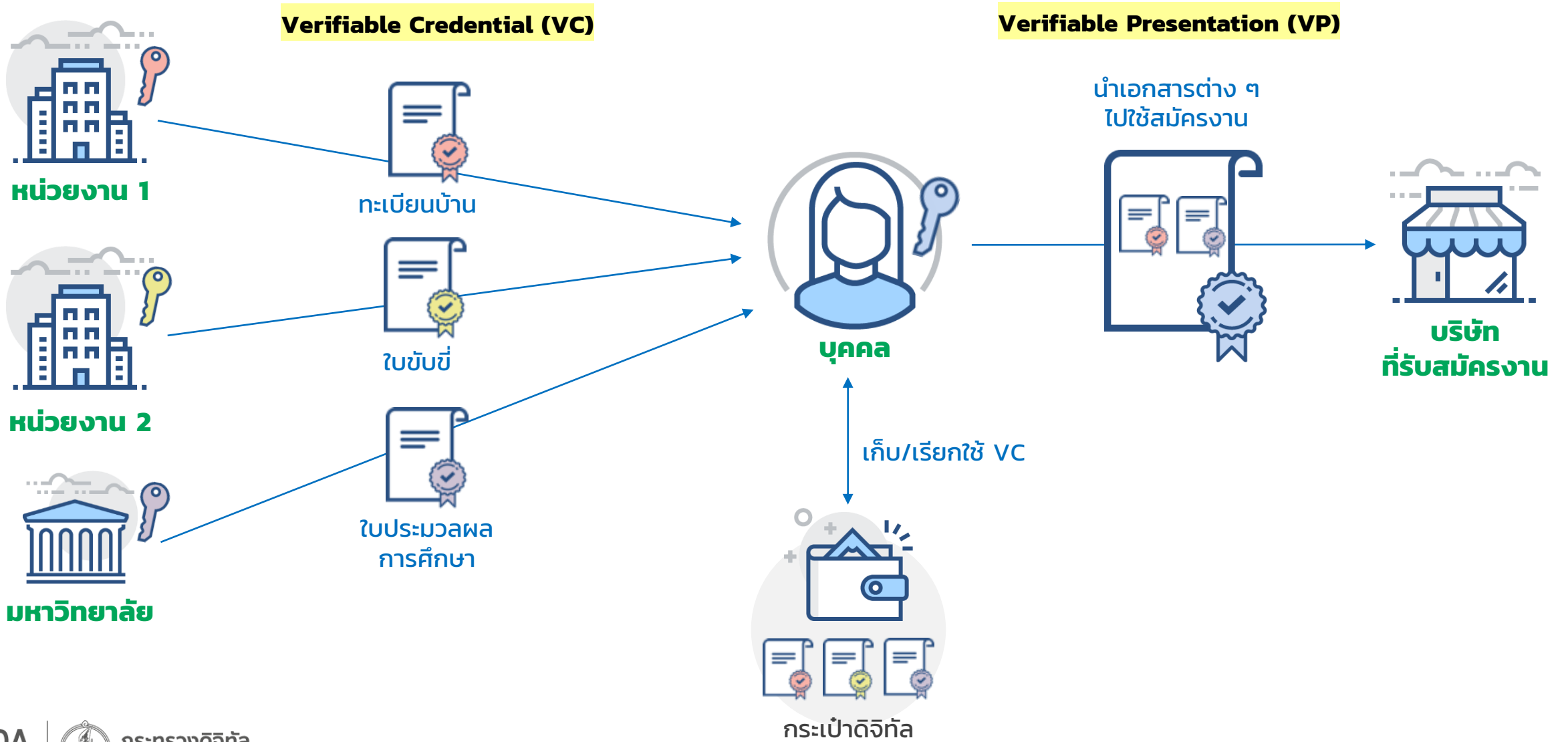


VC และ VP จะมีคุณสมบัติที่สามารถตรวจสอบความถูกต้องครบถ้วนของข้อมูล  
และตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ของผู้ออกเอกสารและผู้ถือเอกสารได้ด้วย  
กระบวนการเข้ารหัสลับ

# ความเชื่อมโยงในการใช้งาน VC และ VP ระหว่างเอนทิตีที่เกี่ยวข้อง



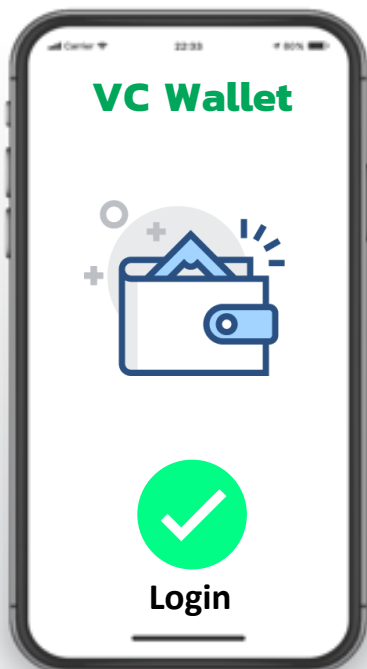
# ตัวอย่างการใช้งาน VC และ VP



# ตัวอย่าง User Journey ขั้นตอนการรับ VC

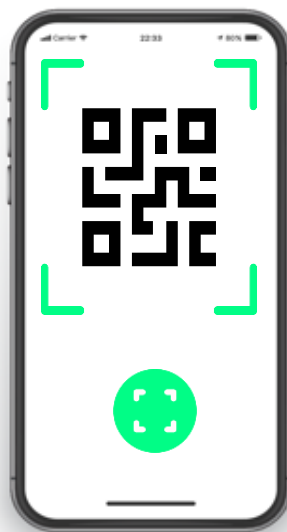


- ผู้ถือเอกสารยื่นขอ VC จากผู้ออกเอกสาร
- และ ผู้ออกเอกสารจะ พิสูจน์ตัวตนของผู้ถือเอกสารก่อนออก VC ให้



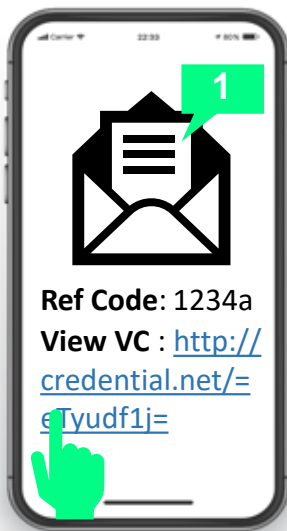
ผู้ถือเข้าแอป VC wallet

การรับ VC  
แบบ On-site

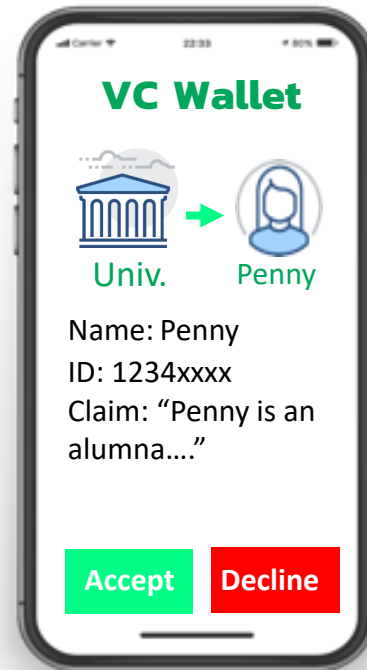


ผู้ถือเอกสารสแกน QR code ที่ผู้ออกเอกสารออกให้

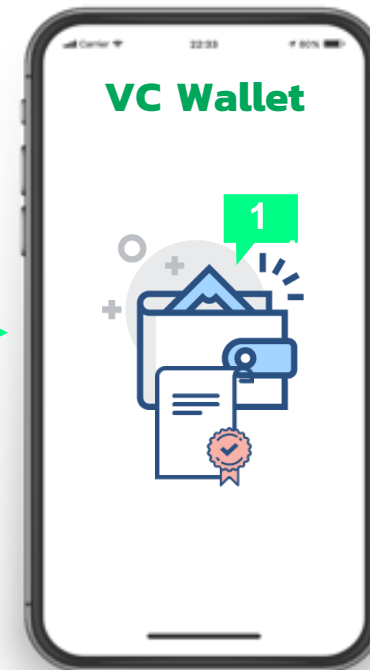
การรับ VC  
แบบ Online



ผู้ถือเอกสารได้รับอีเมล ตรวจสอบ Ref code และคลิกดู VC



ผู้ถือเอกสารตรวจสอบความถูกต้องของ VC และกดยอมรับ

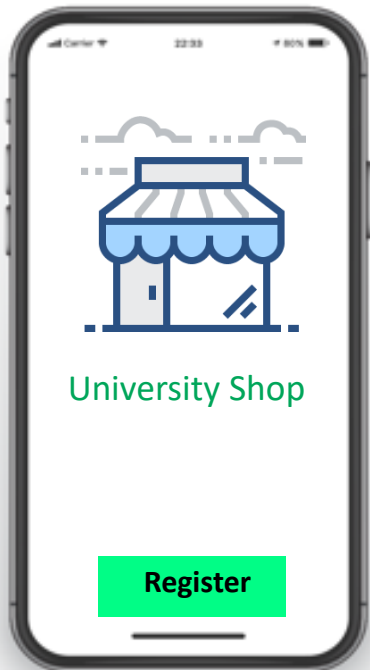


VC ถูกเพิ่มเข้ามาใน VC wallet

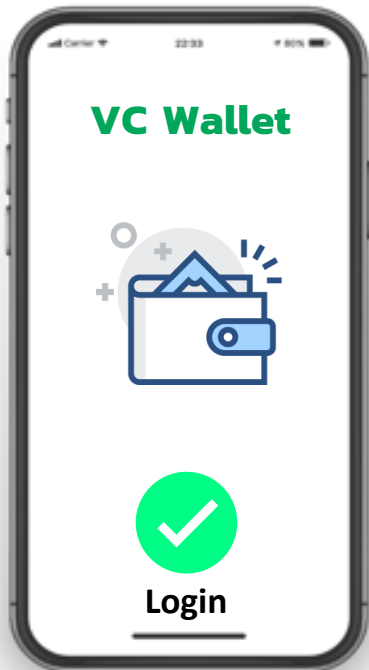
# ตัวอย่าง User Journey ขั้นตอนการใช้ VC แบบ On-site



# ตัวอย่าง User Journey ขั้นตอนการใช้ VC แบบ Online



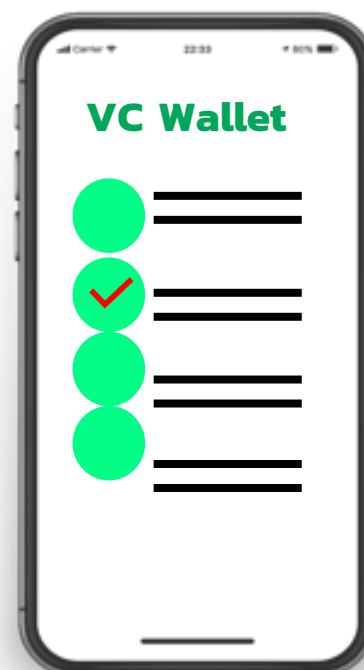
เข้าทำธุรกรรมกับแอปพลิเคชันของ  
ผู้ให้บริการ (ผู้ตรวจสอบเอกสาร) และ  
เลือกใช้บริการด้วยการแสดง VC



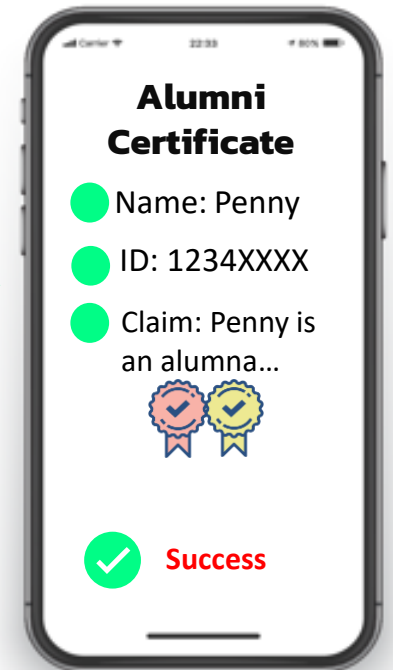
ผู้ให้บริการ redirect  
ให้เข้าแอป wallet



ผู้ถือสารปลดล็อก wallet  
ตามวิธีการที่เลือกไว้  
เช่น Fingerprint



เลือก VC เพื่อสร้าง VP



ผู้ตรวจสอบเอกสารได้รับ VP





## โครงสร้างข้อมูลของเอกสารรับรองและเอกสารสำแดง (Data Structure of Verifiable Credentials and Presentations)

### ขอบข่าย

- กำหนดโครงสร้างข้อมูลสำหรับเอกสารรับรอง (Verifiable Credential: VC) และเอกสารสำแดง (Verifiable Presentation: VP)
- และอธิบายความเชื่อมโยงในการใช้งาน VC และ VP ระหว่างเอนทิตีที่เกี่ยวข้อง ซึ่งประกอบด้วยผู้ออกเอกสาร (issuer) ผู้ถือเอกสาร (holder) และผู้ตรวจสอบเอกสาร (verifier)

เพื่อให้ผู้ถือเอกสารสามารถใช้ VC และ VP ในการพิสูจน์และยืนยันตัวตน การให้ความยินยอม การมอบอำนาจ หรือการแสดงข้อมูลที่ถูกรับรองแก่ผู้อื่น ในรูปแบบอิเล็กทรอนิกส์ที่

- มีความมั่นคงปลอดภัย
- มีการรักษาความเป็นส่วนตัว
- สามารถตรวจสอบได้ด้วยกระบวนการเข้ารหัสลับ และ
- สนับสนุนการแลกเปลี่ยนระหว่างกันตามมาตรฐานสากล

### โครงสร้างของเอกสาร

1. ขอบข่าย
2. บทนิยาม
3. ภาพรวมของ VC และ VP
  - 3.1 การใช้งาน VC และ VP
  - 3.2 ข้อกำหนดการใช้งาน VC และ VP
  - 3.3 รูปแบบความไว้วางใจ (trust model)
  - 3.4 แบบจำลองข้อมูลของ VC และ VP
    - 3.4.1 ข้อความยืนยัน (claim)
    - 3.4.2 เอกสารรับรอง (VC)
    - 3.4.3 เอกสารสำแดง (VP)

#### 4. โครงสร้างข้อมูลของ VC และ VP

- 4.1 คุณสมบัติพื้นฐานของ VC
- 4.2 คุณสมบัติของ VP

ภาคผนวก ก. คุณสมบัติเพิ่มเติมของ VC

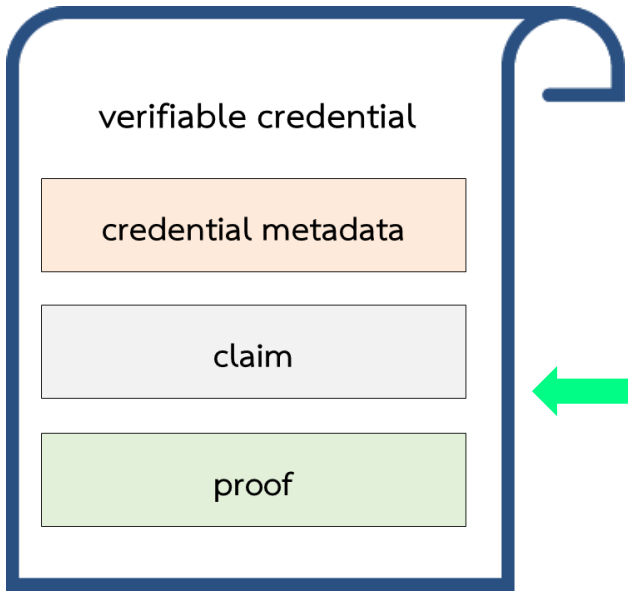
ภาคผนวก ข. การเพิ่มคุณสมบัติ (extensibility)

ภาคผนวก ค. ตัวอย่างกรณีศึกษาการใช้งาน VC และ VP  
บรรณานุกรม

# เอกสารรับรอง (verifiable credential: VC)

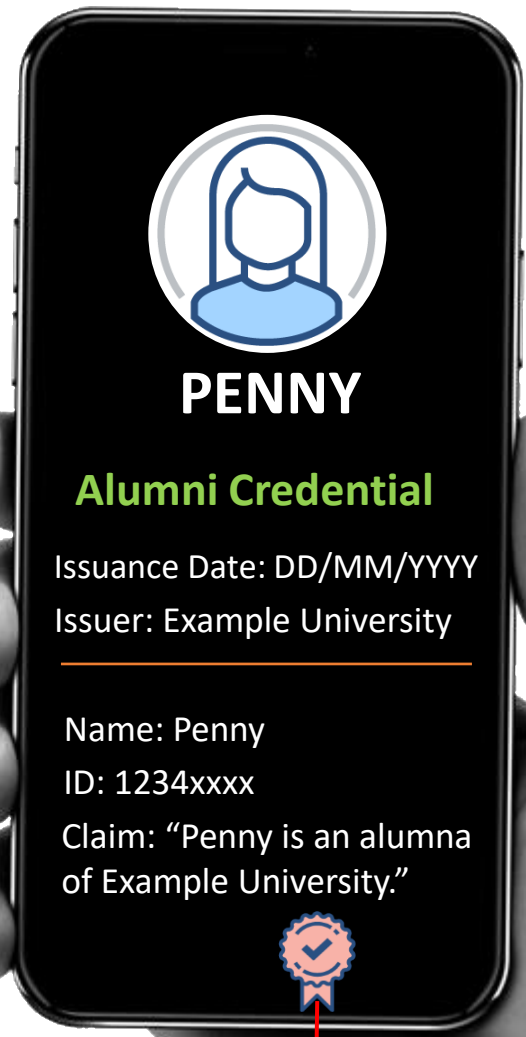
หมายถึง **ชุดของข้อความยืนยัน (claim)** อย่างน้อยหนึ่งรายการที่ถูกรับรองโดย**ผู้ออกเอกสาร (issuer)** ทั้งนี้ VC มีคุณสมบัติที่สามารถตรวจพบการเปลี่ยนแปลงใด ๆ ที่เกิดกับความถูกต้องครบถ้วนของข้อมูล และตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ของผู้ออกเอกสารได้ด้วยกระบวนการเข้ารหัสลับ

## Data model



## 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": "eyJhbGw..."
  }
}
```



**proof** ที่ออกโดยผู้ออกเอกสาร  
เพื่อรับรองคุณลักษณะหรือ  
ข้อความใน VC

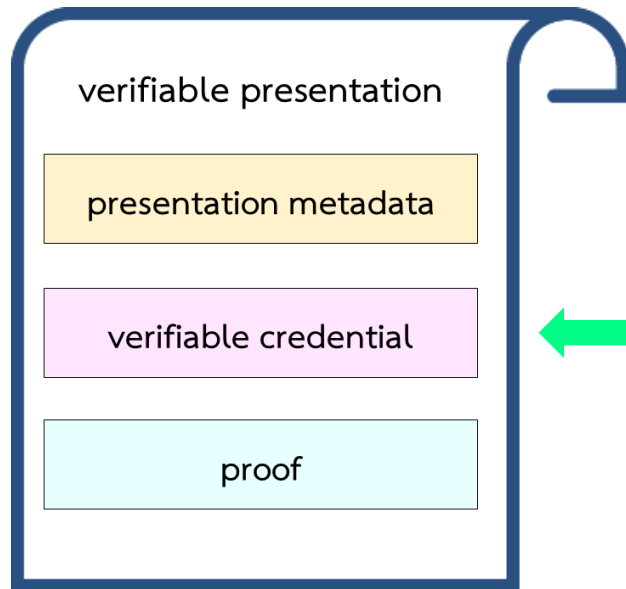
### ตัวอย่าง:

มหาวิทยาลัยออก **VC เพื่อรับรองความเป็นศิษย์** ให้แก่เพนนี่ และเพนนี่เก็บ VC นั้นไว้ในกระเป๋าดิจิทัลของเธอเอง

# เอกสารสำแดง (verifiable presentation: VP)

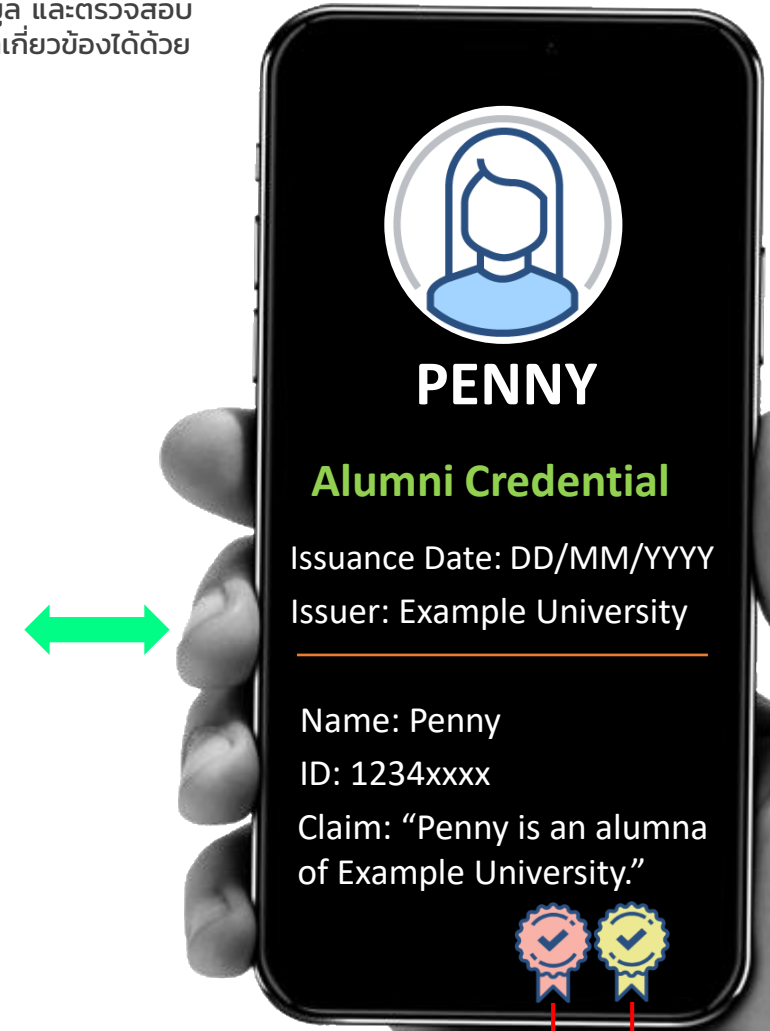
หมายถึง **VC อย่างน้อยหนึ่งชุด** ที่**ผู้ถือเอกสาร (holder)** ใช้แสดงต่อ**ผู้ตรวจสอบเอกสาร (verifier)** ทั้งนี้ VP มีคุณสมบัติที่สามารถตรวจพบการเปลี่ยนแปลงใด ๆ ที่เกิดกับความถูกต้องครบถ้วนของข้อมูล และตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ของผู้ถือเอกสารและตรวจสอบ VC ที่เกี่ยวข้องได้ด้วยกระบวนการเข้ารหัสลับ

## 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:

เพ็ญนิจะขอรับส่วนลดจากร้านสหกรณ์มหาวิทยาลัย เพ็ญนิจึงนำ **VC เพื่อรับรองความเป็นศิษย์เก่า** มาใช้สร้างเป็น **VP** แล้วส่งต่อไปให้ร้านสหกรณ์ ดำเนินการตรวจสอบ

proof ที่ออกโดยผู้ออกเอกสาร เพื่อรับรองคุณลักษณะหรือข้อมูลใน VC

proof ที่ออกโดยผู้ถือเอกสาร เพื่อส่งให้กับผู้ตรวจสอบเอกสาร



## **Control and Access:**

ผู้ถือเอกสารสามารถควบคุมและเข้าถึงข้อความยืนยันใน VC ของตนเองได้

## **Consent:**

หากเป็นไปได้ การนำข้อความยืนยันของเจ้าของข้อความไปใช้งานควรได้รับความยินยอมจากเจ้าของข้อความ

## **Minimization:**

รองรับการเปิดเผยข้อความยืนยันเท่าที่จำเป็น

## **Transparency:**

ระบบและอัลกอริทึมในการใช้งาน VC และ VP ต้องมีความโปร่งใส

## **Portability:**

รองรับการย้าย VC จากกระเป๋าดิจิทัลเดิมไปยังกระเป๋าดิจิทัลใหม่ได้

