(ร่าง) ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร
ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วย

โครงสร้างข้อมูลของสารรับรองและสารสำแดงที่ตรวจสอบได้

(Data Structure of Verifiable Credential and Presentation)

โครงสร้างข้อมูลของสารรับรองและสารสำแดงที่ตรวจสอบได้ (Data Structure of Verifiable Credential and Presentation)

การให้บริการแก่ประชาชนทั้งจาก**ภาครัฐและภาคเอกชนอาจมีการออกเอกสารที่ใช้รับรองข้อมูลบางอย่างแก่ประชาชนผู้เป็นเจ้าของข้อมูลในเอกสาร** ตัวอย่างเช่น

- ใบขับขี่ ที่ออกเพื่อรับรองว่าบุคคลมีความสามารถในการขับขี่รถยนต์
- ใบปริญญาบัตร ที่ออกโดยมหาวิทยาลัยให้แก่นักศึกษาเพื่อรับรองวุฒิการศึกษา
- ใบรับรองแพทย์ ที่ออกโดยแพทย์เพื่อรับรองว่าผู้ป่วยมีอาการตามที่ระบุในเอกสาร

หน่วยงานอาจมีการออกเอกสารรับรองข้อมูลในรูปของ

“สารรับรองที่ตรวจสอบได้ (verifiable credential: VC)”

ซึ่งเป็นตามมาตรฐานของ World Wide Web Consortium (W3C)

สารรับรองที่ตรวจสอบได้ดังกล่าวเป็นเอกสารรับรองข้อมูลในรูปแบบอิเล็กทรอนิกส์ที่**มีคุณสมบัติช่วยให้สามารถตรวจพบการปลอมแปลงและตรวจสอบผู้เขียนข้อมูลได้ด้วยกระบวนการเข้ารหัสลับ**

ขอบข่าย

กำหนด**โครงสร้างข้อมูลสำหรับสารรับรองที่ตรวจสอบได้ (verifiable credential) และสารสำแดงที่ตรวจสอบได้ (verifiable presentation)** และอธิบาย**ความสัมพันธ์ระหว่างบทบาทที่เกี่ยวข้องกับระบบการใช้งานของสารรับรองที่ตรวจสอบได้** ซึ่งประกอบด้วยผู้ออกสาร (issuer) ผู้ถือสาร (holder) และผู้ตรวจสอบสาร (verifier) เพื่อให้ผู้ใช้งานสามารถใช้สารรับรองที่ตรวจสอบได้ในการแสดงเอกสารหรือข้อมูลประจำตัวต่าง ๆ บนโลกออนไลน์ในลักษณะที่มีความมั่นคงปลอดภัย มีการรักษาความเป็นส่วนตัว สามารถตรวจสอบได้ด้วยกระบวนการเข้ารหัสลับ และสนับสนุนการแลกเปลี่ยนระหว่างกันตามมาตรฐานสากล

โครงสร้างของเอกสาร

1. **ขอบข่าย**
2. **บทนิยาม**
3. **ภาพรวมของสารรับรองที่ตรวจสอบได้และสารสำแดงที่ตรวจสอบได้**
   - 3.1 หลักการทำงานของสารรับรองที่ตรวจสอบได้
   - 3.2 ข้อกำหนดการใช้งานสารรับรองที่ตรวจสอบได้
   - 3.3 รูปแบบการรับรองความน่าเชื่อถือ (trust model)
   - 3.4 แบบจำลองข้อมูลของสารรับรองที่ตรวจสอบได้และสารสำแดงที่ตรวจสอบได้
     - 3.4.1 ข้อกล่าวอ้าง (claim)
     - 3.4.2 สารรับรองที่ตรวจสอบได้ (verifiable credential)
     - 3.4.3 สารสำแดงที่ตรวจสอบได้ (verifiable presentation)
4. **โครงสร้างข้อมูลของสารรับรองที่ตรวจสอบได้และสารสำแดงที่ตรวจสอบได้**
   - 4.1 คุณสมบัติพื้นฐานของสารรับรองที่ตรวจสอบได้
     - 4.1.1 บริบท (context)
     - 4.1.2 ตัวระบุ (identifier)
     - 4.1.3 ประเภท (type)
     - 4.1.4 ผู้ออกสาร (issuer)
     - 4.1.5 วันที่ออกสาร (issuance date) และวันที่สารสิ้นอายุ (expiration date)
     - 4.1.6 เจ้าของข้อมูล (subject) และข้อกล่าวอ้าง (claim)
     - 4.1.7 สถานะ (credential status)
     - 4.1.8 ข้อพิสูจน์ (proof) หรือลายมือชื่อ (signature)
     - 4.1.9 โครงสร้างข้อมูลแสดงคุณสมบัติพื้นฐานของสารรับรองที่ตรวจสอบได้
   - 4.2 คุณสมบัติของสารสำแดงที่ตรวจสอบได้
     - 4.2.1 โครงสร้างข้อมูลแสดงคุณสมบัติของสารสำแดงที่ตรวจสอบได้

ภาคผนวก ก. คุณสมบัติเพิ่มเติมของสารรับรองที่ตรวจสอบได้

- ก.1 เค้าร่างข้อมูล (credential schema)
- ก.2 การต่ออายุหรือปรับให้เป็นปัจจุบัน (refreshing)
- ก.3 ข้อกำหนดการใช้งาน (terms of use)
- ก.4 หลักฐาน (evidence)
- ก.5 การโต้แย้ง (disputes)

ภาคผนวก ข. ความสามารถในการเพิ่มคุณสมบัติ (extensibility)

ภาคผนวก ค. กรณีศึกษาการใช้งานสารรับรองที่ตรวจสอบได้

บรรณานุกรม

หลักการทำงานของสารรับรองที่ตรวจสอบได้

ผู้ออกสาร (issuer)

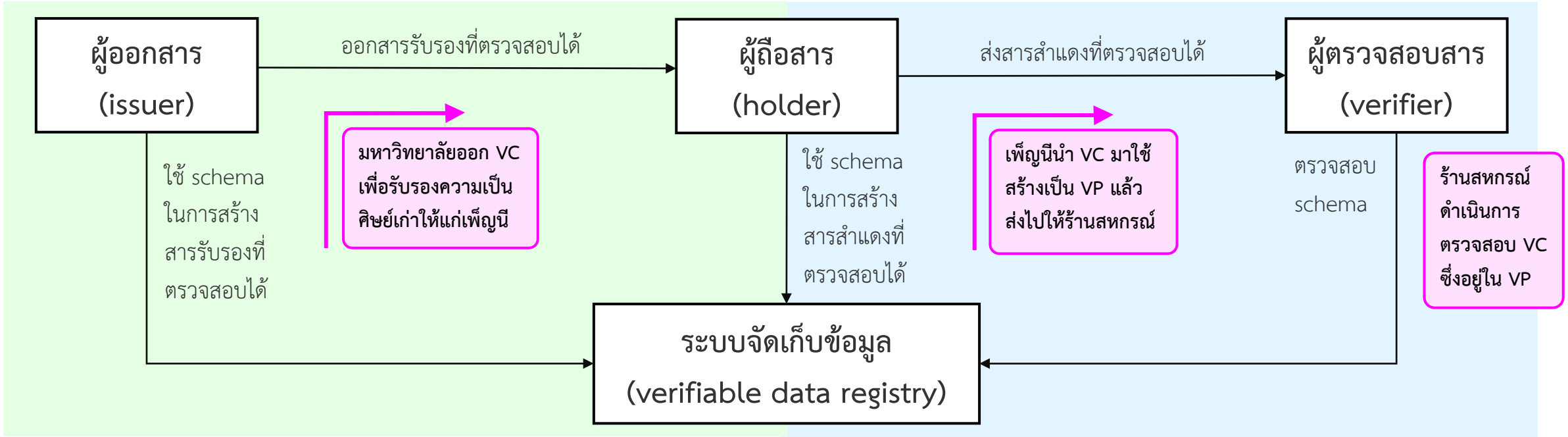
บทบาทที่ทำหน้าที่**ยืนยันข้อกล่าวอ้างเกี่ยวกับเจ้าของข้อมูล** เพื่อนำข้อกล่าวอ้างนั้นมา**สร้างเป็นสารรับรองที่ตรวจสอบได้** และส่งสารรับรองที่ตรวจสอบได้นั้นให้กับผู้ถือสาร

ผู้ถือสาร (holder)

บทบาทที่ทำหน้าที่**ถือครองสารรับรองที่ตรวจสอบได้** และใช้สารรับรองที่ตรวจสอบได้นั้น**สร้างเป็นสารสำแดงที่ตรวจสอบได้**

ผู้ตรวจสอบสาร (verifier)

บทบาทที่ทำหน้าที่รับสารรับรองที่ตรวจสอบได้ ซึ่งอาจอยู่ในรูปของ**สารสำแดงที่ตรวจสอบได้เพื่อนำมาประมวลผล**



ระบบจัดเก็บข้อมูล (verifiable data registry)

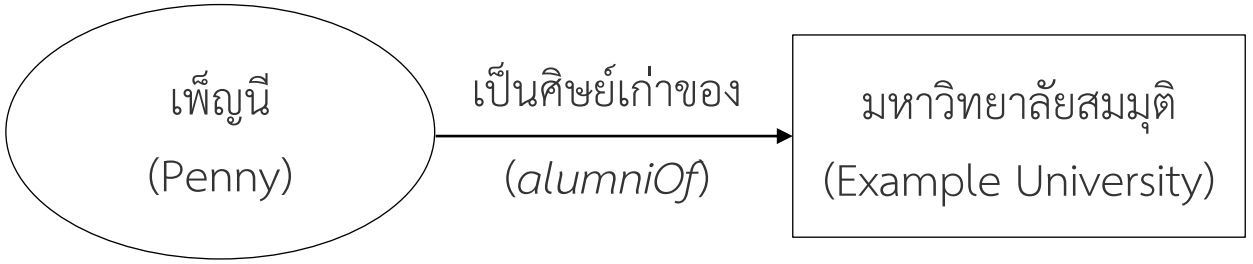
บทบาทของระบบที่ทำหน้าที่เป็น**สื่อกลางในการสร้างและตรวจสอบข้อมูลที่จำเป็น**ต่อการใช้งานสารรับรองที่ตรวจสอบได้ เช่น ตัวระบุ (identifier) กุญแจสาธารณะ (public key) รายการเพิกถอน (revocation registry) และโครงสร้างข้อมูล (schema)

ข้อกล่าวอ้าง (claim)

ข้อกล่าวอ้าง (claim) หมายถึง ลักษณะ (characteristic) หรือข้อความ (statement) เกี่ยวกับเจ้าของข้อมูล (subject)

ข้อกล่าวอ้าง สามารถแสดงด้วยความสัมพันธ์ในรูปแบบ **“เจ้าของข้อมูล (subject) – คุณสมบัติ (property) – ค่าของคุณสมบัติ (value)”**

ตัวอย่างของข้อกล่าวอ้าง แสดงข้อความ **“เพ็ญนีเป็นศิษย์เก่าของมหาวิทยาลัยสมมุติ” (“Penny is an alumna of Example University.”)**



สารรับรองที่ตรวจสอบได้ (verifiable credential: VC)

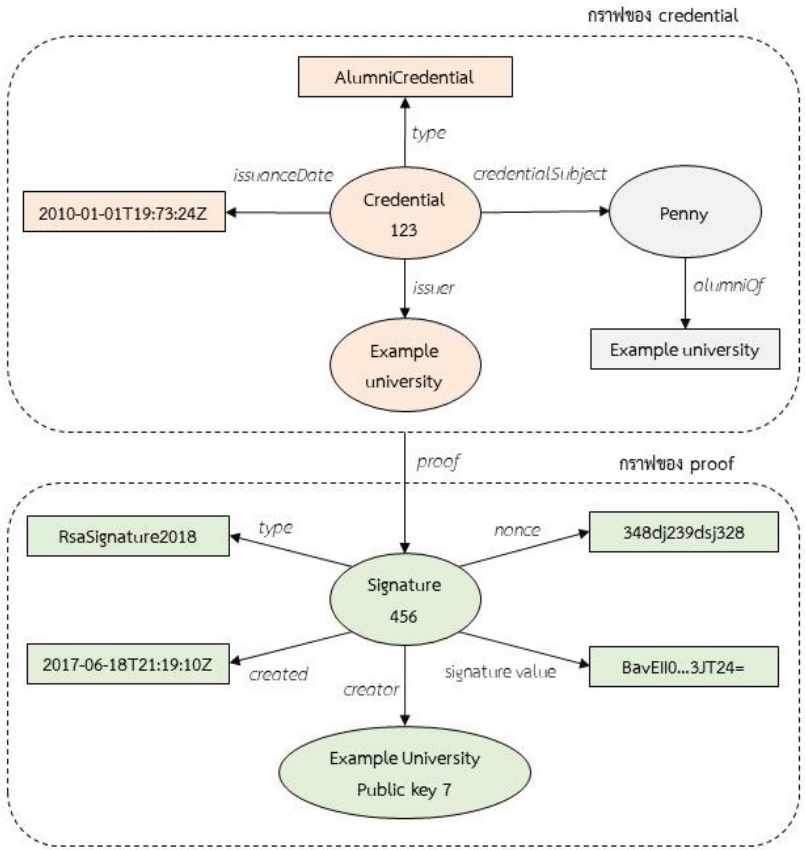
หมายถึง **ชุดของข้อกล่าวอ้าง**อย่างน้อยหนึ่งรายการที่ออกโดย**ผู้ออกสาร (issuer)** โดยสารรับรองที่ตรวจสอบได้มีคุณสมบัติที่สามารถตรวจพบการปลอมแปลง (tamper-evident) และตรวจสอบผู้เขียนข้อมูล (authorship) ได้ด้วยกระบวนการเข้ารหัสลับ (cryptographic verification)

Data model

verifiable credential

- credential metadata
- claim
- proof

Graph of information



JSON-LD file

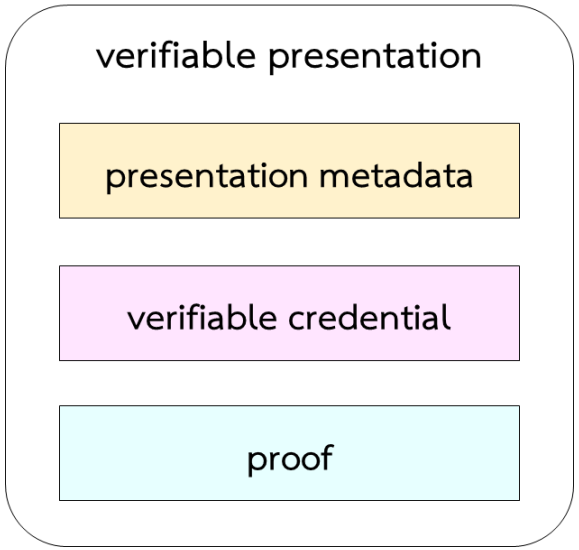
```
{
 "@context": [
  "https://www.w3.org/2018/credentials/v1",
  "https://www.w3.org/2018/credentials/examples/v1"],
 "id": "http://example.edu/credentials/1872"
  "type": ["VerifiableCredential",  "AlumniCredential"],
  "issuer": "https://example.edu/issuers/565049",
  "issuanceDate": "2010-01-01T19:73:24Z",
 "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..."
  }
}
```

ตัวอย่าง: มหาวิทยาลัยออก VC **เพื่อรับรองความเป็นศิษย์เก่า**ให้แก่เพ็ญนี และเพ็ญนีเก็บ VC นั้นไว้ในกระเป๋าดิจิทัลของตนเอง

สารสำแดงที่ตรวจสอบได้ (verifiable presentation: VP)

หมายถึง ข้อมูลที่ประกอบด้วย**สารรับรองที่ตรวจสอบได้อย่างน้อยหนึ่งชุด**ที่ออกโดยผู้ออกสาร (issuer) จำนวนตั้งแต่หนึ่งคน สำหรับ**ใช้แสดงต่อผู้ตรวจสอบสาร (verifier)** โดยสารสำแดงที่ตรวจสอบได้มีคุณสมบัติที่สามารถตรวจพบการปลอมแปลง (tamper-evident) และตรวจสอบผู้เขียนข้อมูล (authorship) ได้ด้วยกระบวนการเข้ารหัสลับ (cryptographic verification)

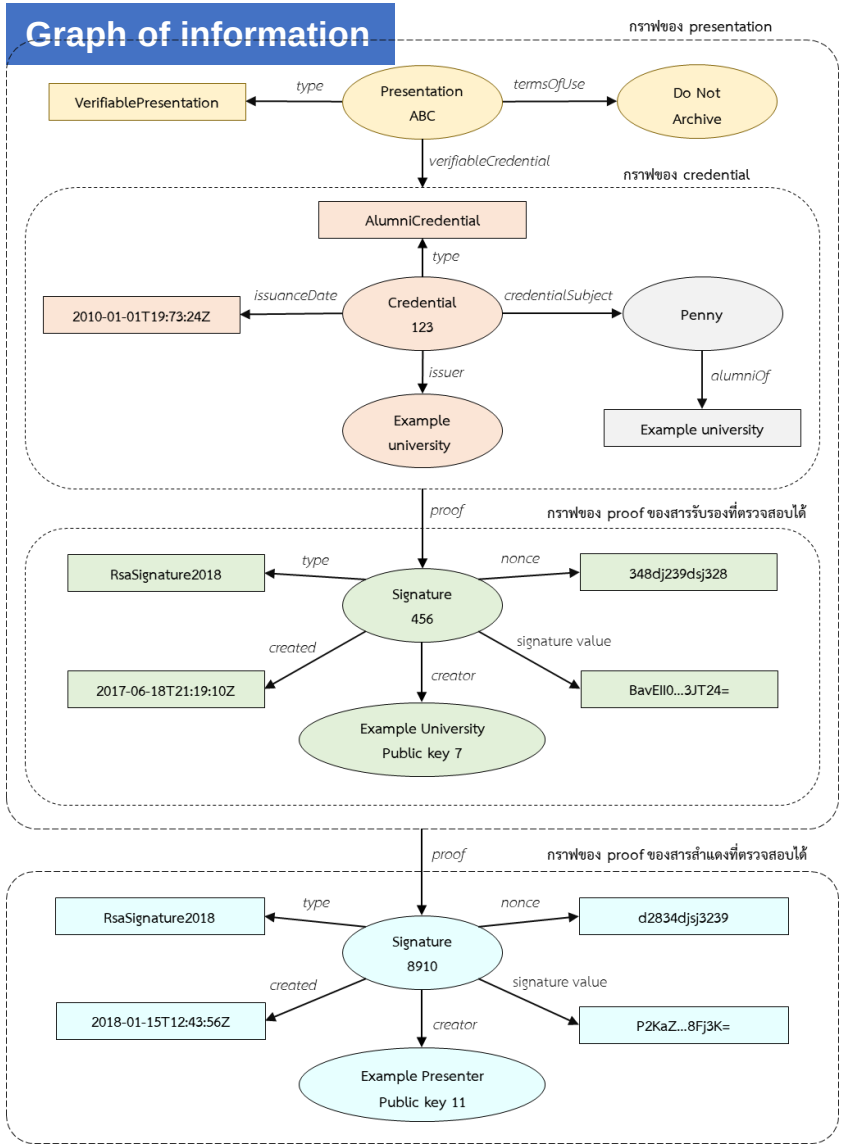
Data model



ตัวอย่าง:

เพ็ญนีจะขอรับส่วนลดจากร้านสหกรณ์มหาวิทยาลัย เพ็ญนีจึงนำ VC เพื่อรับรองความเป็นศิษย์เก่า มาใช้สร้างเป็น VP แล้วส่งต่อไปให้ร้านสหกรณ์ดำเนินการตรวจสอบ

Graph of information



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..."
 }
}
```