

Digital Signature use case in Thailand

Paradorn Athichitsakul

Deputy Director One Authen company limited



One Authen

บริษัท วัน ออเท่น จำกัด (One Authen Co.,Ltd)

ผู้เชี่ยวชาญด้านการออกแบบและพัฒนาซอฟต์แวร์ด้าน

เทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure : PKI)



One Authen

บริษัท วัน ออเท่น จำกัด (One Authen) ผู้เชี่ยวชาญด้านการออกแบบและพัฒนาซอฟต์แวร์ด้านเทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure : PKI)



CERTIFICATE AUTHORITY SERVICE

CENTRALIZED LOG SERVICE



DIGITAL SIGNATURE SERVICE

E-STAMP SERVICE



E-TIMESTAMP SERVICE

E-VERIFIED SERVICE



คปท.
สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย(คปท.)



สมาคมอุตสาหกรรมซอฟต์แวร์ไทย
The Association of Thai Software Industry



ธนาคารแห่งประเทศไทย



DFT



สำนักงานคณะกรรมการวิจัยและพัฒนา
BRSRB THE CANE AND SUGAR BOARD

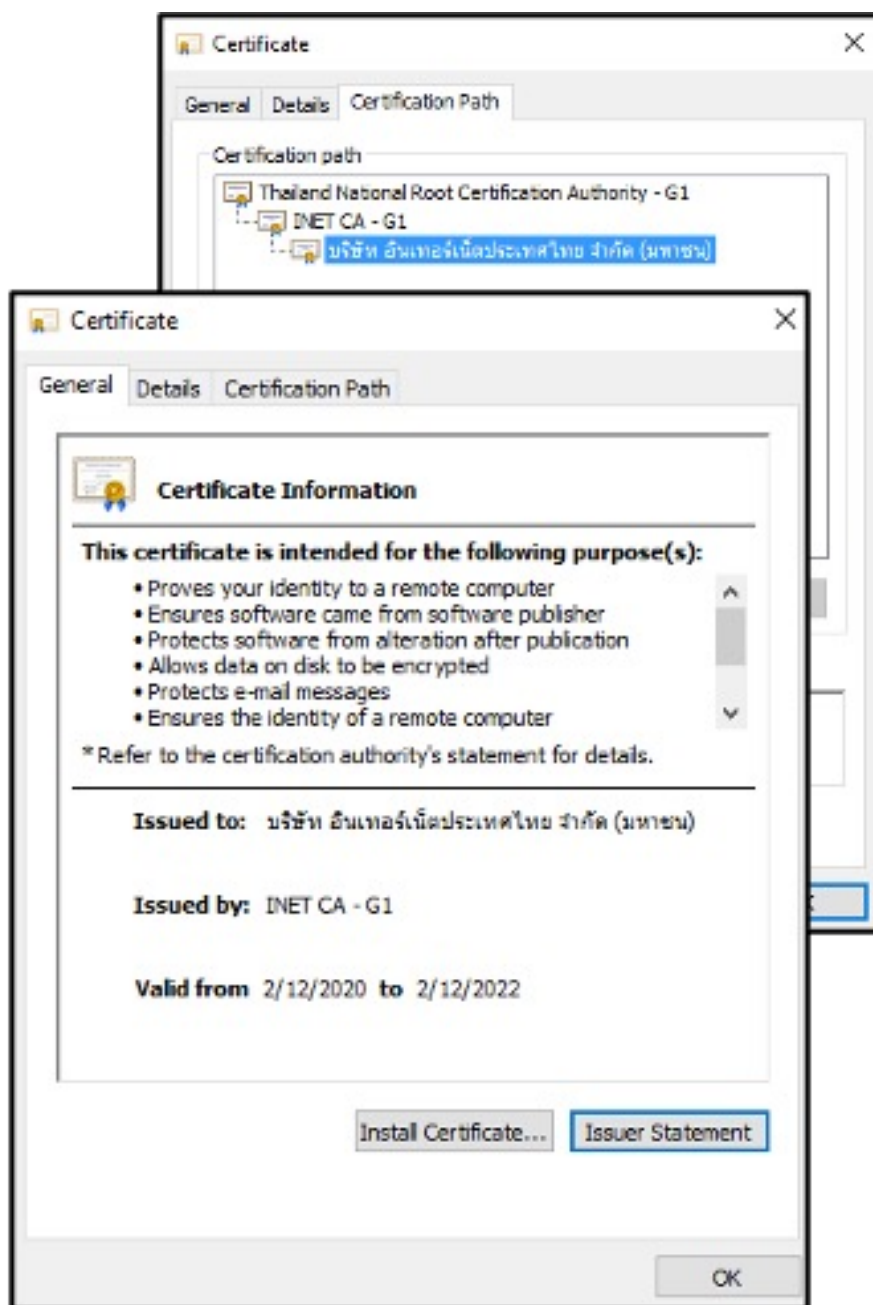
Agenda

- **Digital Certificate**
- **PKI based Digital Signature**
 - **Signature application**
 - **Security & Compliance & Legal**
- **Use case in Thailand**
 - **e-Tax invoice & e-Receipt**
 - **University and Education segment**
 - **Healthcare**
 - **Other**
 - **Recommendation**
- **Consideration & Future Challenge**
- **Q&A**

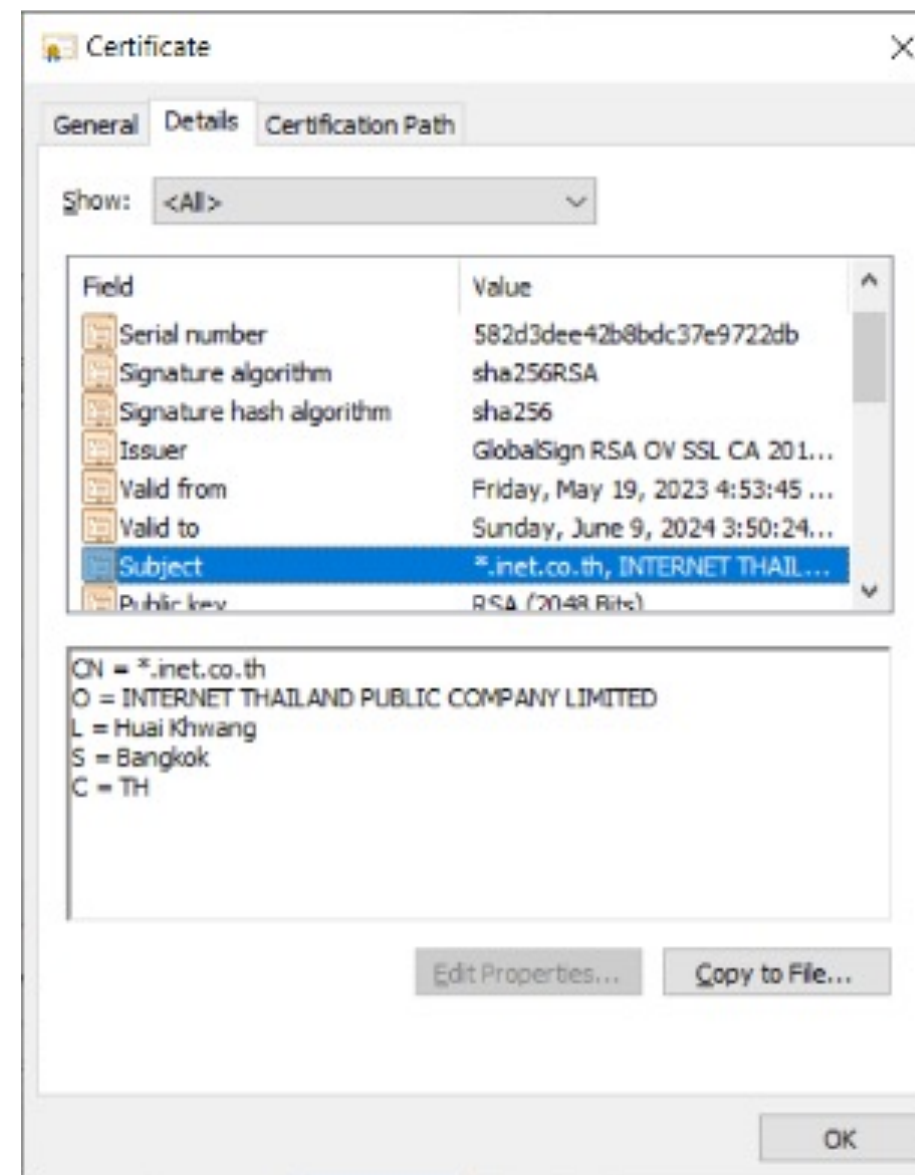
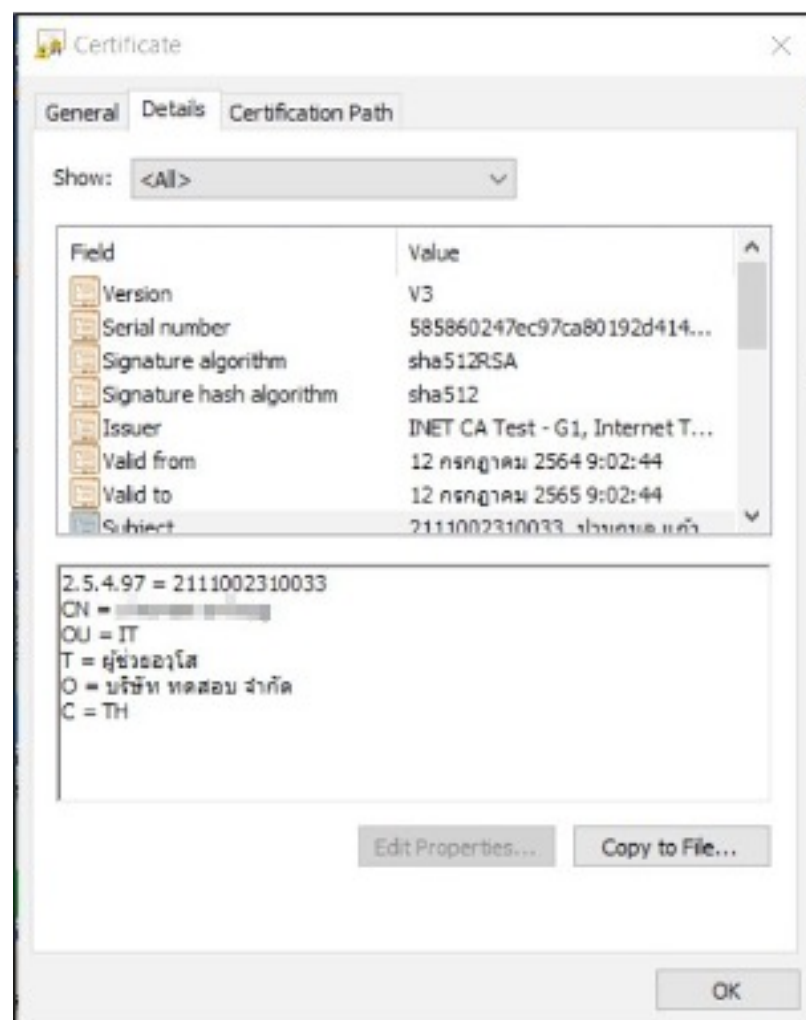
One Authen

บริษัท วัน ออเท่น จำกัด (One Authen) ผู้เชี่ยวชาญด้าน
การออกแบบและพัฒนาซอฟต์แวร์ ซึ่งเป็นบริษัทในเครือของ
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน)

Digital Certificate



Document Signing Certificate (17,285)



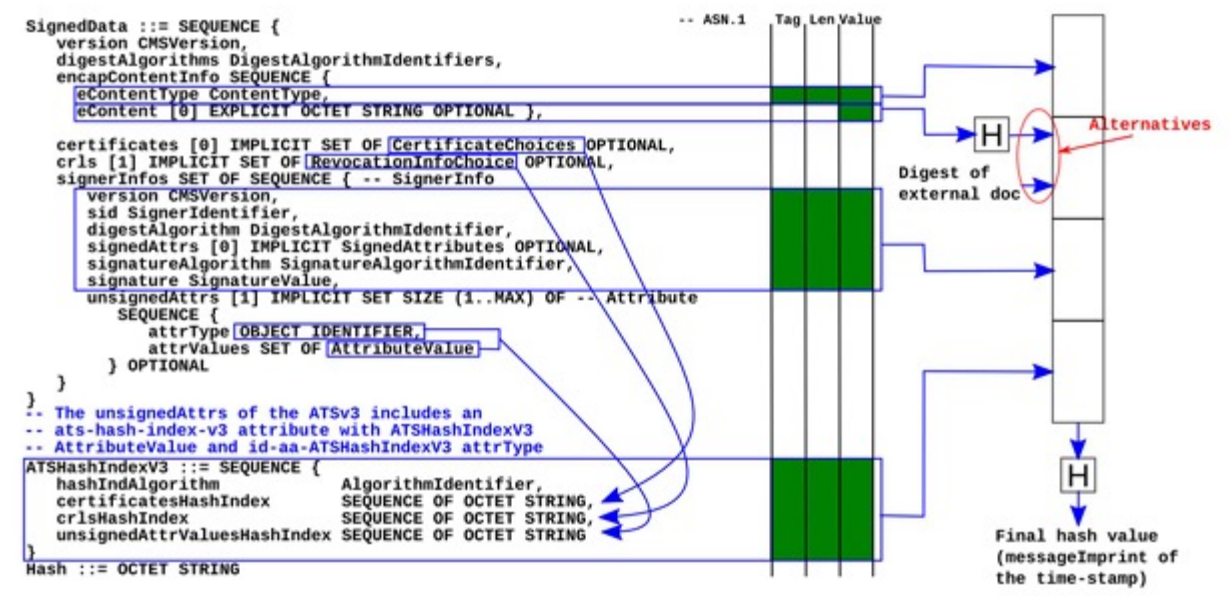
SSL Certificate (23)

PKI Based Digital Signature

- Image

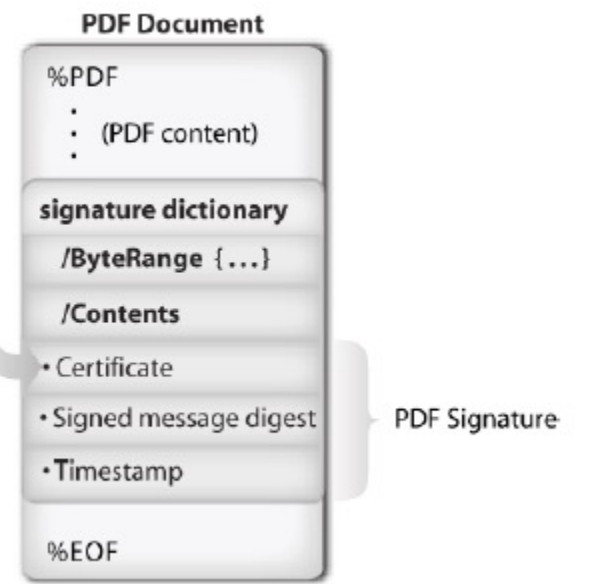
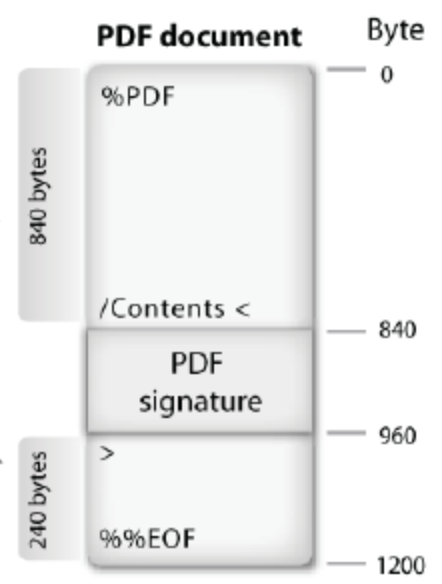


- Cryptography



Example:
/ByteRange
[0, 840, 960, 240]

Signature hash value computed for these bytes



Security & Compliance & Legal

- Asymmetric key cryptography & Cryptographic Hashing
- NIST
 - FIPS-186-5: ref: <https://csrc.nist.gov/pubs/fips/186-5/final>



- ETSI: ESI: ref: <https://www.etsi.org/committee/esi>



Security & Compliance & Legal

- **Legal**

- **United States : UETA & E-Sign Act**

- **The European Union : EU Regulation (No 910/2014):**

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910>

28.8.2014	EN	Official Journal of the European Union	L 257/73
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			

- **Another country:**

<https://helpx.adobe.com/search.html?q=Electronic+Signature+Laws>

- **Thailand : Thailand Electronic Transaction Act:**

1
<i>ELECTRONIC TRANSACTIONS ACT</i> <i>B.E. 2544 (2001)</i> -----
<i>BHUMIBOL ADULYADEJ, REX.</i> <i>Given on the 2nd day of December B.E. 2544</i> <i>Being the 56th year of the Present Reign</i>
<i>His Majesty King Bhumibol Adulyadej is graciously pleased to proclaim that,</i> <i>Whereas it is deemed expedient to have a law on electronic transactions,</i> <i>And whereas this Act contains certain provisions relating to the restriction of</i> <i>personal rights and freedom, for which Section 29 incorporating Section 50 of the</i> <i>Constitution of the Kingdom of Thailand provides that it can be made by virtue of the</i> <i>provisions of a law.</i> <i>Be it therefore enacted by H. M. the King an Act, by and with the advice and</i> <i>consent of the Parliament, as follows:</i>

Electronic Signature Laws & Regulations - Indonesia

Aug 2022 | <https://helpx.adobe.com/legal/esignatures/regulations/indonesia.html>

Electronic Signature Laws & Regulations - Indonesia

Electronic Signature Laws & Regulations - India

May 2024 | <https://helpx.adobe.com/legal/esignatures/regulations/india.html>

Electronic Signature Laws & Regulations - India

Electronic Signature Laws & Regulations - Brazil

Aug 2022 | <https://helpx.adobe.com/legal/esignatures/regulations/brazil.html>

Electronic Signature Laws & Regulations - Brazil

Electronic Signature Laws & Regulations - The European Union

Oct 2023 | <https://helpx.adobe.com/legal/esignatures/regulations/european-union.html>

Electronic Signature Laws & Regulations - The European Union

Electronic Signature Laws & Regulations - Turkey

Aug 2022 | <https://helpx.adobe.com/legal/esignatures/regulations/turkey.html>

Electronic Signature Laws & Regulations - Turkey

Electronic Signature Laws & Regulations - Thailand

Aug 2022 | <https://helpx.adobe.com/legal/esignatures/regulations/thailand.html>

Electronic Signature Laws & Regulations - Thailand

Electronic Signature Laws & Regulations - Bangladesh

Aug 2022 | <https://helpx.adobe.com/legal/esignatures/regulations/bangladesh.html>

Electronic Signature Laws & Regulations - Bangladesh

Electronic Signature Laws & Regulations - Ireland

Feb 2024 | <https://helpx.adobe.com/legal/esignatures/regulations/ireland.html>

Electronic Signature Laws & Regulations - Ireland

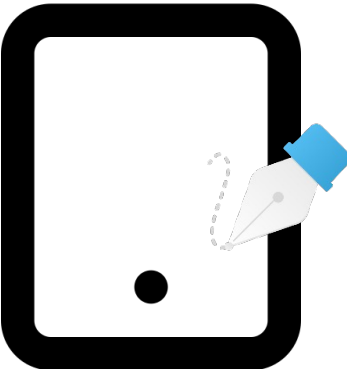
Electronic Signature Laws & Regulations - Ukraine

Nov 2023 | <https://helpx.adobe.com/legal/esignatures/regulations/ukraine.html>

Electronic Signature Laws & Regulations - Ukraine

Security & Compliance & Legal

- **Thailand : Thailand Electronic Transaction Act:**
 - **Regular electronic signature:**



- **Reliable Electronic Signatures**

(1) **the signature creation data** are, within the context in which they are used, **linked to the signatory and to no other person;**

(2) **the signature creation data** were, at the time of signing, **under the control of the signatory and of no other person;**

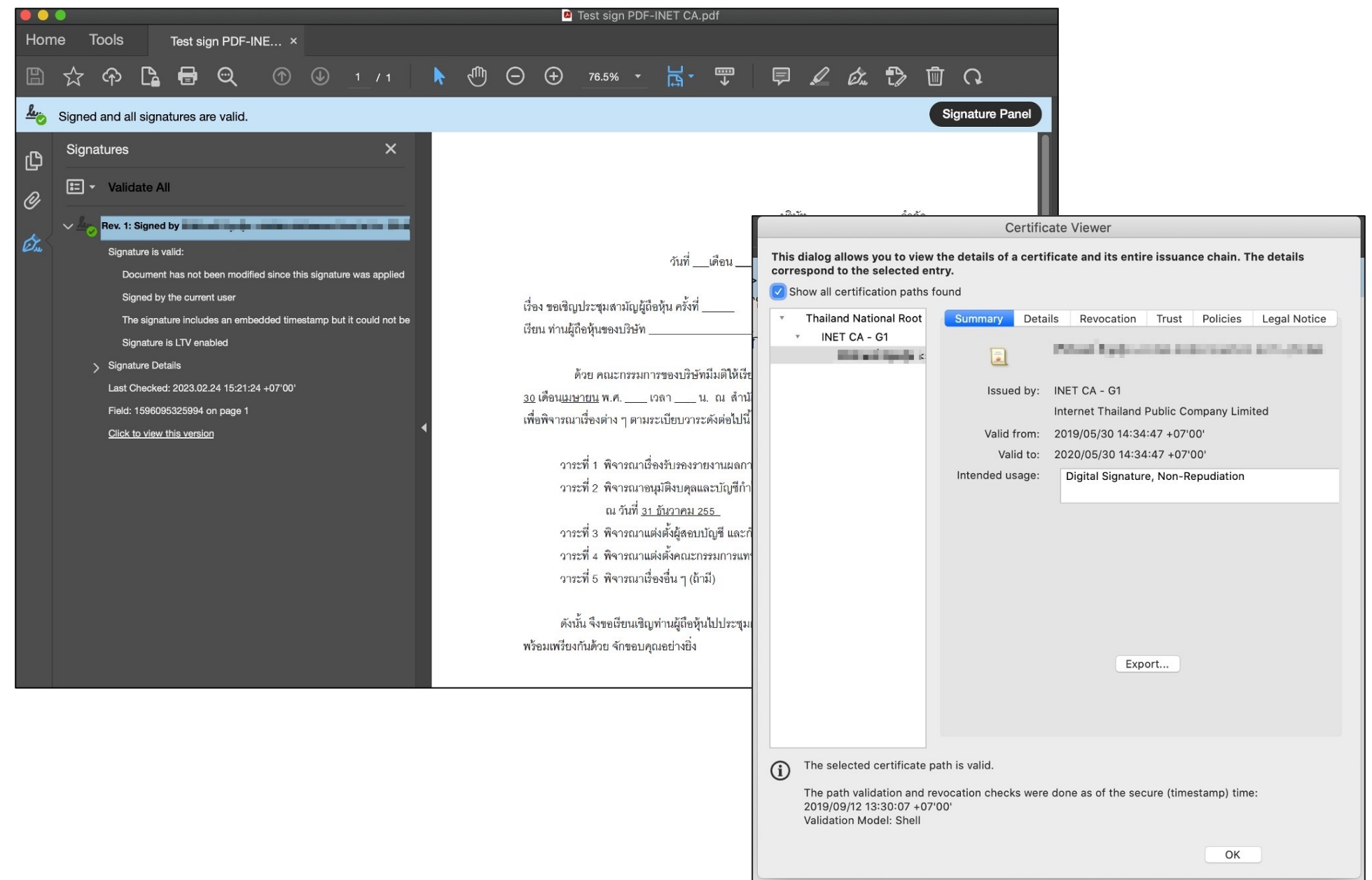
(3) **any alteration to the electronic signature**, made after the time of signing, is **detectable;**

(4) where a purpose of the legal requirement for a signature is to **provide assurance** as to the **completeness and integrity of the information** and any **alteration made** to that information after the time of signing is **detectable.**



Use case in Thailand

- e-Tax invoice & e-Receipt
- University and Education segment
- Healthcare
- Other
- Recommendation



e-Tax invoice & e-Receipt

- ใบกำกับภาษีตามมาตรา 86/4
- ใบกำกับภาษีอย่างย่อตามมาตรา 86/6
- ใบเพิ่มหนี้ตามมาตรา 86/9
- ใบลดหนี้ตามมาตรา 86/10
- ใบรับตามมาตรา 105 ทวิ แห่งประมวลรัษฎากร



Standard & Recommendation

- **พ.ร.อ. 3-2560 :**
ข้อความอิเล็กทรอนิกส์สำหรับการซื้อขายสินค้าและบริการ (Trade Services Message Standard)
- **พ.ร.อ. 14-2560 :**
การใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ (Using XML Messages for Inter-Organizational Data Exchange)

ส่งมอบให้ผู้ซื้อสินค้า หรือ ผู้รับบริการ

นำส่งสรรพากร

```
<?xml version='1.0' encoding='UTF-8' standalone='no'?>
<rsim:TaxInvoice_CrossIndustryInvoice xmlns:ram="urn:etda:uncefact:data:standard:TaxInvoice_ReusableAggregateBusinessProcessDocument:2.0" xmlns:rsm="urn:etda:uncefact:data:standard:TaxInvoice_CrossIndustryInvoice:2.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:etda:uncefact:data:standard:TaxInvoice_CrossIndustryInvoice:2.0 urn:etda:uncefact:data:standard:TaxInvoice_2p0.xsd">
  <ram:ExchangedDocumentContext>
    <ram:GuidelineSpecifiedDocumentContextParameter>
      <ram:ID>ETDA</ram:ID>
      <ram:SchemeAgencyID>ETDA</ram:SchemeAgencyID>
      <ram:SchemeVersionID>v2.0</ram:SchemeVersionID>
    </ram:GuidelineSpecifiedDocumentContextParameter>
    <ram:ExchangedDocument>
      <ram:ID>RDTIV0575526000058001</ram:ID>
      <ram:Name>ใบกำกับ</ram:Name>
      <ram:TypeCode>388</ram:TypeCode>
      <ram:IssueDateTime>2016-09-12T19:19:25.0</ram:IssueDateTime>
      <ram:CreationDateTime>2016-09-12T15:51:26.0</ram:CreationDateTime>
      <ram:IncludedNote>
        <ram:Subject>ใบกำกับ</ram:Subject>
      </ram:IncludedNote>
    </ram:ExchangedDocument>
    <ram:SupplyChainTradeTransaction>
      <ram:ApplicableHeaderTradeAgreement>
```

Transaction ID	File Name
17957675WUw0X	xml_sig.xml
ขนาดไฟล์ (File Size)	29.71 kb
วันที่ (Date)	23 มิ.ย. 2567 22:47:55 น. (เวลาประเทศไทย)
การตรวจสอบ XML-Digital Signature (XML-Digital Signature Result)	✓ ผ่าน
การตรวจสอบ XML-Schema and Schematron (XML-Schema and Schematron Result)	✓ ผ่าน
สถานะ (Status)	Active

University and Education segment

Standard & Recommendation

• VNO. 11-2560 :

การจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์

(Electronic Certificate)

• VNO. 14-2560 :

การใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์

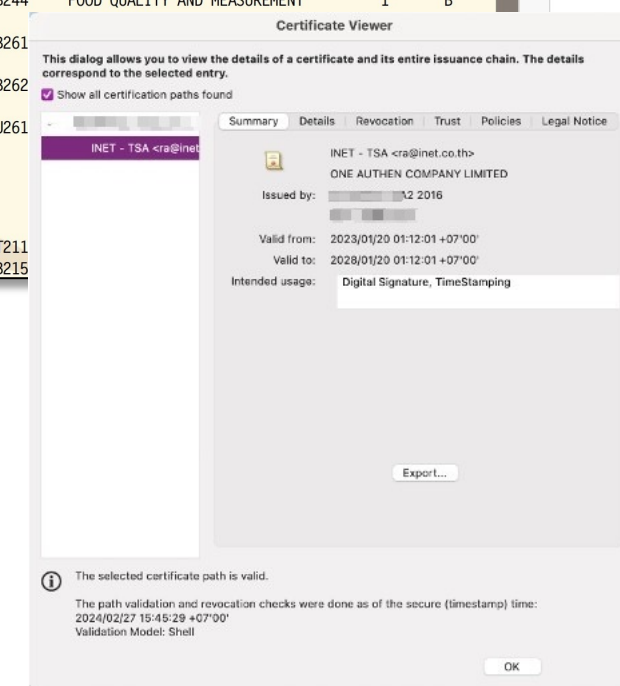
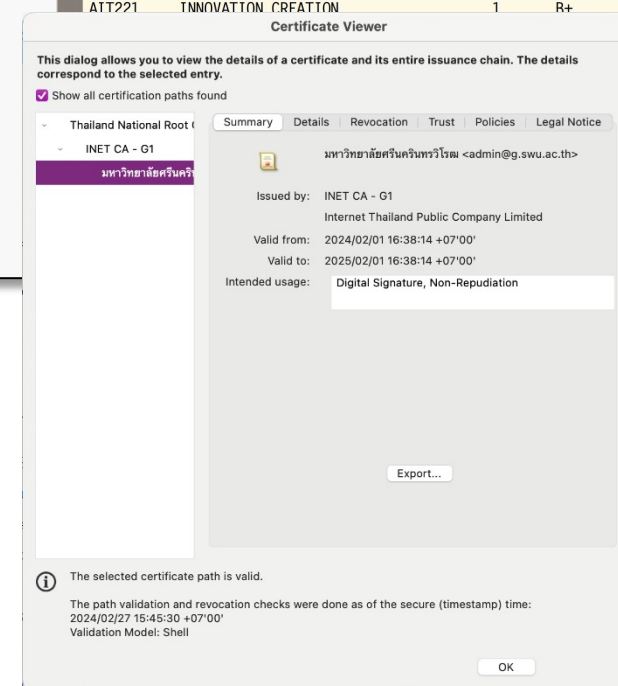
(Using XML Messages for Inter-Organizational Data Exchange)

• VNO. 25-2563 :

ข้อความอิเล็กทรอนิกส์สำหรับใบประมวลผลการศึกษา

(Message Standard for Academic Transcript)

```
<?xml-model href="..\schematron/DigitalTranscript_Schematron.sch" type="application/xml">
<?xml-stylesheet href="..\schematron/DigitalTranscript_Schematron.xsl" type="text/xsl" />
<ct:Transcript xmlns:ccts="urn:un:unece:uncefact:documentation:standard:CoreComponentsTechnicalSpecifi
xmlns:qt="urn:etda:teda:data:QualifiedDataType:1"
xmlns:tc="urn:etda:teda:documentation:Transcript:1"
xmlns:udt="urn:un:unece:uncefact:data:standard:UnqualifiedDataType:16"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:etda:teda:documentation:Transcript:1
file:..\schema\data\standard\Transcript.xsd">
  <tc:TranscriptContext>
    <tc:OID>2.16.764.1.4.1.1.8.1.1</tc:OID>
    <tc:Version>2.0</tc:Version>
    <tc:TranscriptID>ETRS73020</tc:TranscriptID>
    <tc:Name>Digital Transcript (EN)</tc:Name>
    <tc:TypeCode>01</tc:TypeCode>
    <tc:IssueDateTime>2021-10-08T15:36:54</tc:IssueDateTime>
    <tc:Language>EN</tc:Language>
    <tc:Status>TRANSCRIPT_CLOSED</tc:Status>
  </tc:TranscriptContext>
  <tc:Student>
    <tc:DataSubjectID schemeID="StudenID">57</tc:DataSubjectID>
    <tc:DataSubjectID schemeID="NIDN">140990</tc:DataSubjectID>
    <tc>NamePrefix languageID="th"></tc>NamePrefix>
    <tc>NamePrefix languageID="en"></tc>NamePrefix>
    <tc:GivenName languageID="th"></tc:GivenName>
    <tc:GivenName languageID="en"></tc:GivenName>
    <tc:FamilyName languageID="th"></tc:FamilyName>
    <tc:FamilyName languageID="en"></tc:FamilyName>
    <tc:Gender>1</tc:Gender>
    <tc:BirthDate>1996-04-19T00:00:00</tc:BirthDate>
    <tc:Nationality>TH</tc:Nationality>
    <tc:ResidentCountryOrTerritoryCode>TH</tc:ResidentCountryOrTerritoryCode>
    <tc:DateOfAdmission>2020-05-04T18:13:51.0</tc:DateOfAdmission>
    <tc:FacultyName>Science</tc:FacultyName>
  </tc:Student>
  <tc:ProgramContext>
    <tc:ProgramID>310208102154</tc:ProgramID>
    <tc:ProgramName>Information and Communication Technology</tc:ProgramName>
    <tc:Major>Information and Communication Technology</tc:Major>
    <tc:Degree>Bachelor Degree</tc:Degree>
  </tc:ProgramContext>
  <tc:CreditsTranferred>0</tc:CreditsTranferred>
  <tc:PreviousCertificate></tc:PreviousCertificate>
</ct:Transcript>
```



Healthcare

ETDA
www.eta.go.th

ผลการตรวจสอบเอกสาร
รายละเอียดผลการตรวจสอบเอกสาร

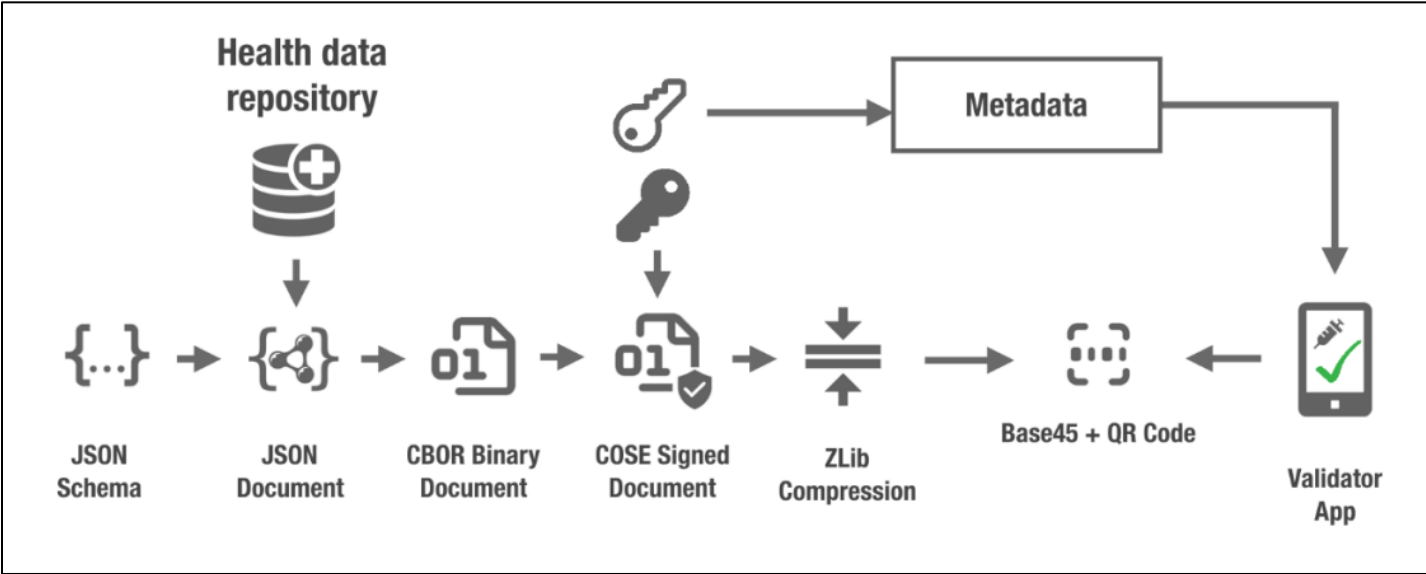
Transaction ID 1634461157raR16p1D

ชื่อไฟล์ (File Name) DHPv1.pdf

ขนาดไฟล์ (File Size) 313.50 kb

วัน - เวลาที่ทำการตรวจสอบ (Processing Date Time) 17 ต.ค. 2564 15:59:17 น. (เวลาประเทศไทย)

ผลการตรวจสอบ PDF-Digital Signature (PDF-Digital Signature Result) ✓ นำเชื่อถือ



Standard & Recommendation

- **พ.ร.บ. 11-2560 :**
การจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์
(Electronic Certificate)
- **พ.ร.บ. 34-2566:**
ใบรับรองแพทย์อิเล็กทรอนิกส์
(Electronic Medical Certificate)
- **Technical Specifications for EU Digital COVID Certificates**

FR
MINISTÈRE DE LA SANTÉ ET DE LA PRÉVENTION
Liberté, Égalité, Fraternité

PARADORN AT

```

    {
      "ver": "1.3.0",
      "nam": {
        "fn": "กรรณ",
        "fnt": "P",
        "gn": "ธชิต",
        "gnt": "A"
      },
      "dob": "1987-04-30",
      "v": [
        {
          "tg": "8405",
          "vp": "J07B",
          "mp": "EU/1",
          "ma": "ORG-",
          "dn": 2,
          "sd": 2,
          "dt": "2021-02-18",
          "co": "SE",
          "is": "Swedish eHealth Agency",
          "ci": "URN:UVCI:01:SE:EHRM/V100000024GI5HM"
        }
      ]
    }
  
```

SAVE THE PASS TO YOUR PHONE
No need to print the pass, just present it on your mobile device.

Save to iPhone
Save to Android device

Other

- eStamp Duty
- ePolicy
- Timestamp Authority (TSA)

e-TIMESTAMP

- Paperless System
- eSarabun
- NSW National Single Window

e-Stamp Duty
มาตรการstampแบบใหม่ ติดได้ทุกที่ รองรับทุกตราสาร
 เทคโนโลยีที่ช่วยให้การชำระอากรแสตมป์เป็นเรื่องง่าย สะดวกรวดเร็ว ลดต้นทุน เพิ่มความสามารถในการแข่งขัน

ทำไมต้องใช้ e-TIMESTAMP

- สร้างความเชื่อมั่น**: เพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยน่าเชื่อถือ เทียบเท่ากับการประทับตราของบริษัท
- อ้างอิงเวลาประทับตามสากล**: เอกสารอิเล็กทรอนิกส์จะถูกเชื่อมโยงค่าเวลาที่อ้างอิงตามเวลาสากล และได้รับรองจาก สถาบันมาตรวิทยาแห่งชาติ
- ช่วยป้องกันการปลอมแปลงเอกสาร**: ตรวจสอบได้ว่าเอกสารอิเล็กทรอนิกส์ที่ได้รับการประทับรับรองเวลาแล้วมีการถูกแก้ไขเอกสารหรือไม่
- Adobe Trust List Member**: อยู่ภายใต้ Adobe Approved Trust List (AATL) ทำให้อเอกสาร PDF แสดงสัญลักษณ์ Green Mark และเกิดความน่าเชื่อถือ

Private and Confidential - Prepared by One Authen

BEFORE

ปิดอากรแสตมป์/สลักหลังลงบนกระดาษ

AFTER

แบบหลักฐานการชำระอากรแสตมป์ในรูปแบบอิเล็กทรอนิกส์

Recommendation

ข้อเสนอแนะมาตรฐานฯ (ETDA Recommendation)

Ref: <https://www.eta.or.th/th/Our-Service/Recommendation.aspx>

- **วรสอ. 11-2560 :**
การจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ (Electronic Certificate)
- **วรสอ. 15-2566 :**
ข้อมูลในใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ (Subscriber Certificate Profile)
- **วรสอ. 23-2563 :**
แนวทางการลงลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature Guideline)
- **วรสอ. 33-2566 :**
การประทับเวลาอิเล็กทรอนิกส์ (Electronic Time-Stamping)
- **วรสอ. 36-2566 :**
บริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (Remote Signing Service)



ประเภทของลายมือชื่ออิเล็กทรอนิกส์

ประเภทที่ 1
ลายมือชื่ออิเล็กทรอนิกส์ทั่วไป

เป็นลายมือชื่ออิเล็กทรอนิกส์ในรูปแบบใด ๆ (เป็นอักษร อักษรตัวเลข เสียงหรือสัญลักษณ์อื่นใดที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์) ที่มีลักษณะตามที่กำหนดใน **มาตรา 9** แห่งกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

ประเภทที่ 2
ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้

เป็นลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะตามที่กำหนดใน **มาตรา 26** แห่งกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

เช่น ลายมือชื่อดิจิทัลที่อาศัยโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure: PKI)

ประเภทที่ 3
ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ซึ่งใช้ใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรอง

เป็นลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะตามที่กำหนดใน **มาตรา 26** และอาศัยใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรองเพื่อสนับสนุนลายมือชื่ออิเล็กทรอนิกส์ตามที่กำหนดใน **มาตรา 28** แห่งกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

เช่น ลายมือชื่อดิจิทัลที่อาศัยโครงสร้างพื้นฐานกุญแจสาธารณะ (PKI) และใช้ใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรอง

องค์ประกอบของลายมือชื่ออิเล็กทรอนิกส์

	การพิสูจน์และยืนยันตัวตน ¹	เจตนาในการลงลายมือชื่อ	การรักษาความครบถ้วนของข้อมูล
ประเภทที่ 1 ลายมือชื่ออิเล็กทรอนิกส์ทั่วไป	มีการพิสูจน์และยืนยันตัวตนที่ น่าเชื่อถือ และเหมาะสมกับความเสี่ยงของธุรกรรม	มีกระบวนการหรือหลักฐานที่แสดงได้ว่าบุคคลได้ยอมรับการแสดงเจตนาที่ตนได้ลงลายมือชื่ออย่างชัดเจน	ใช้หลักฐานหรือบุคคลที่ สามที่เชื่อถือได้ เพื่อแสดงว่าไม่มีการเปลี่ยนแปลงความหมายของข้อความที่ลงลายมือชื่อ และรับรองความครบถ้วนของข้อมูล
ประเภทที่ 2 ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้	มีการพิสูจน์ตัวตนที่ น่าเชื่อถือ และเหมาะสมกับความเสี่ยงของธุรกรรมหรือระดับ IAL2 ขึ้นไป ²	ใช้ลายมือชื่อดิจิทัลในการลงลายมือชื่อต่อข้อความที่ตนแสดงเจตนา	ใช้ลายมือชื่อดิจิทัลในการลงลายมือชื่อต่อข้อความ
ประเภทที่ 3 ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ซึ่งใช้ใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรอง	มีการพิสูจน์ตัวตนที่ น่าเชื่อถือ และเหมาะสมกับความเสี่ยงของธุรกรรมหรือระดับ IAL2 ขึ้นไป	ใช้ลายมือชื่อดิจิทัลซึ่งใช้ใบรับรองที่ออกโดย CA ในการลงลายมือชื่อต่อข้อความที่ตนแสดงเจตนา	ใช้ลายมือชื่อดิจิทัลซึ่งใช้ใบรับรองที่ออกโดย CA ในการลงลายมือชื่อต่อข้อความ

Consideration & Future Challenge

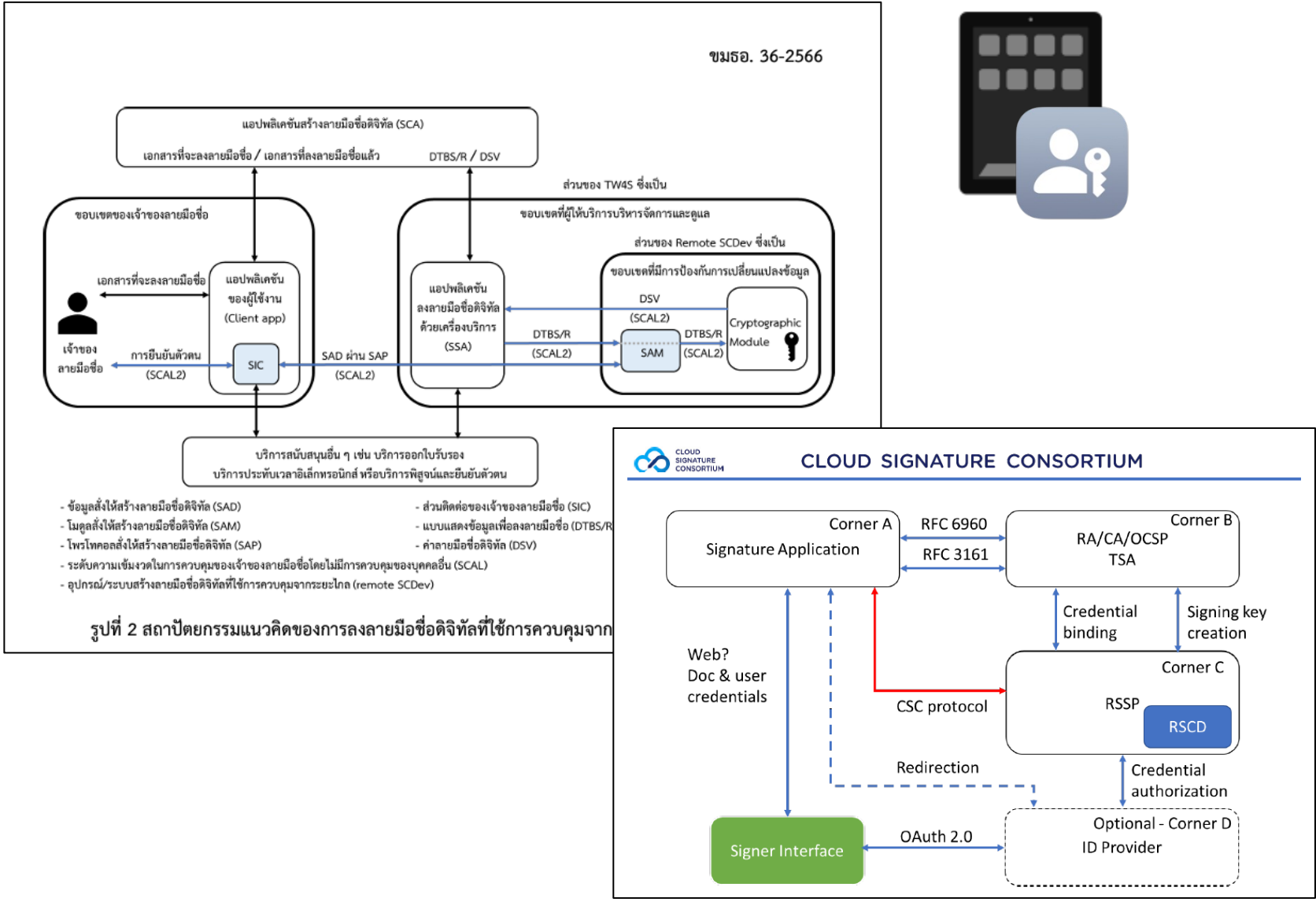
• Traditional Signing & Remote Signing

(2) the signature creation data were, at the time of signing, under the control of the signatory and of no other person;

Local Signing



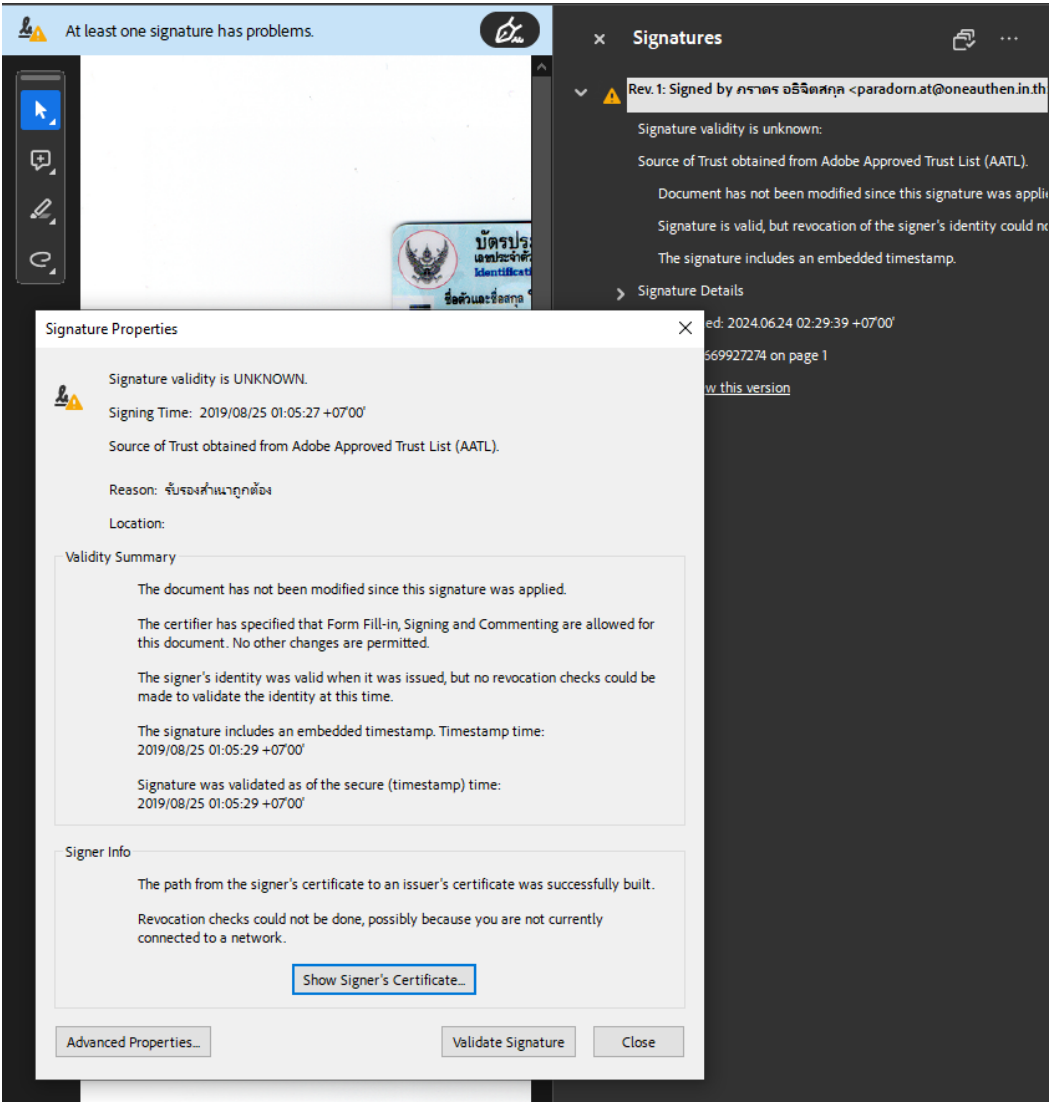
Remote Signing



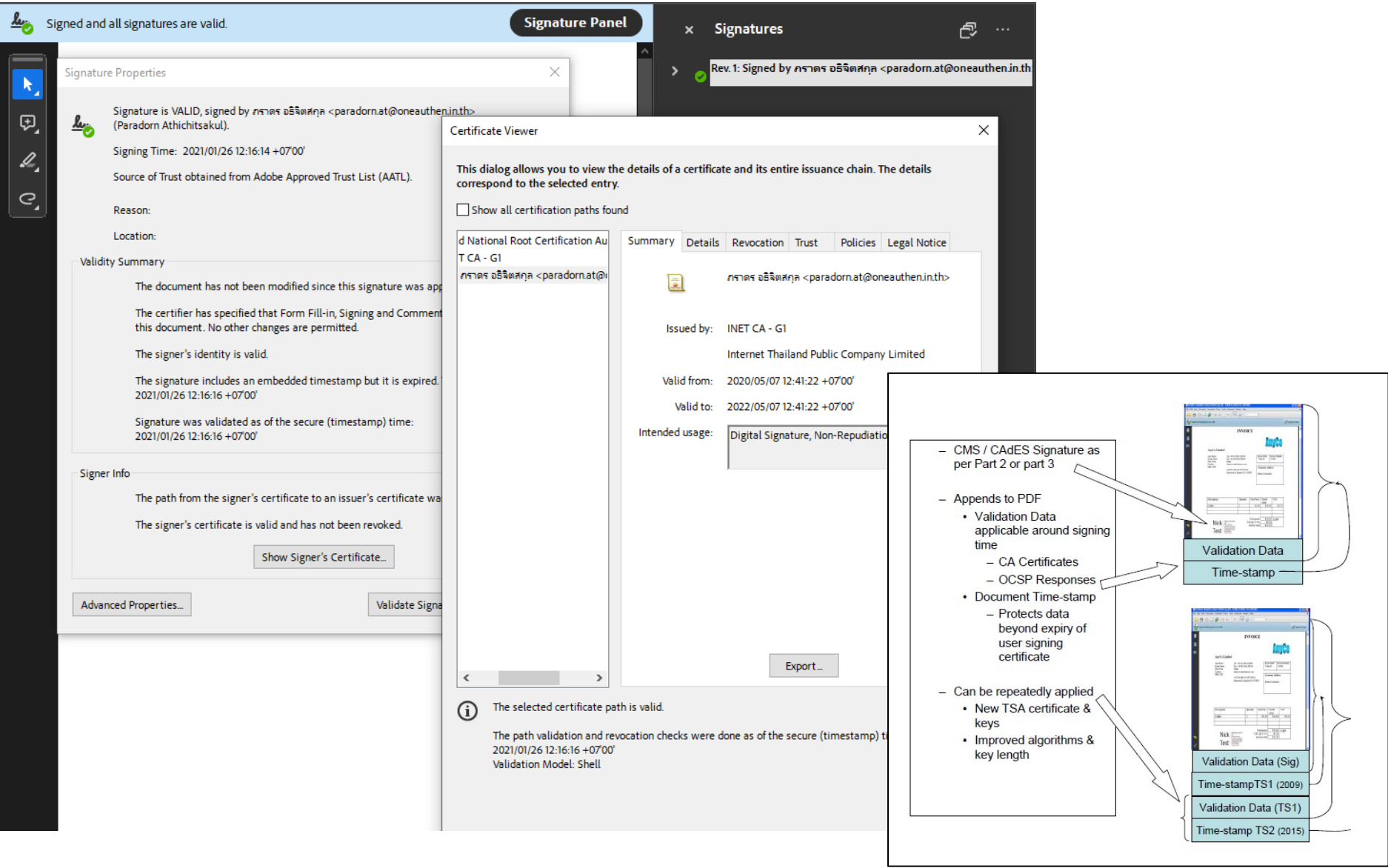
Consideration & Future Challenge

Document Archive & Digital Signature Validation

Simple digital signed document



Simple digital signed document with LTV related attribute



Consideration & Future Challenge

- Quantum Cryptography & AI-driven cryptography

The screenshot shows the top navigation bar of the NIST CSRC website. It includes the NIST logo, a search bar labeled 'Search CSRC', and a 'CSRC MENU' button. Below this is a blue banner with the text 'Information Technology Laboratory' and 'COMPUTER SECURITY RESOURCE CENTER'.

PROJECTS

Post-Quantum Cryptography PQC

f t in e

PROJECT LINKS

[Overview](#)

[FAQs](#)

[News & Updates](#)

[Events](#)

[Publications](#)

[Presentations](#)

Overview

Public comments are available for [Draft FIPS 203](#), [Draft FIPS 204](#) and [Draft FIPS 205](#), which specify algorithms derived from CRYSTALS-Dilithium, CRYSTALS-KYBER and SPHINCS*. The public comment period closed November 22, 2023.

The screenshot shows the top navigation bar of the NIST CSRC website. It includes the NIST logo, a search bar labeled 'Search CSRC', and a 'CSRC MENU' button. Below this is a blue banner with the text 'Information Technology Laboratory' and 'COMPUTER SECURITY RESOURCE CENTER'.

PRESENTATIONS 2024

Presentation

Synergies between AI and Cryptography: Challenges and Research Directions

January 10, 2024

f t in e

PRESENTERS

Luca Mariot - University of Twente, Netherlands

DESCRIPTION

Abstract. The interplay between Artificial Intelligence (AI) and cryptography has been a fruitful one for many years, although it became quite prominent only recently due to the success of deep learning. In this talk, we give a broad overview of the research at the intersection of AI and cryptography, considering both directions: how to use AI techniques to design and cryptanalyze cryptographic primitives, and how cryptography can help in building secure and private AI models. For the first direction, we survey AI-based optimization methods and computational models to optimize low-level cryptographic primitives, and how deep neural networks have been successfully trained as differential distinguishers for small symmetric ciphers. In the other direction, we mention a few applications of privacy enhancing technologies applied to machine learning models. Next, we highlight some recent ideas for detecting text generated by large language models via statistical watermarking, and how to inject cryptographic backdoors in neural networks. We also take the chance to advertise the AICrypt 2024 workshop (affiliated with Eurocrypt), which is focused on these topics.

Suggested readings: <https://aicrypt2024.aisylab.com>; ia.cr/2021/1092; [arXiv:2301.08012](https://arxiv.org/abs/2301.08012); [doi:10.1007/978-3-030-98795-4_1](https://doi.org/10.1007/978-3-030-98795-4_1)

Thank you