Digital Signature use case in Thailand

Paradorn Athichitsakul

Deputy Director One Authen company limited

One Authen

บริษัท วัน ออเทน จำกัด (One Authen Co.,Ltd)
ผู้เชี่ยวชาญด้านการออกแบบและพัฒนาซอฟต์แวร์ด้าน
เทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure : PKI)

One Authen

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

INET • CA

CERTIFICATE AUTHORITY SERVICE

CENTRALIZED LOG SERVICE

INET LOG

DIGITAL SIGNATURE SERVICE

E-STAMP SERVICE

STAMP DUTY

E-TIMESTAMP SERVICE

E-VERIFIED SERVICE

กรมศุลกากร

คปภ. สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย(คปภ.)

ITSI สมาคมอุตสาหกรรมซอฟต์แวร์ไทย The Association of Thai Software Industry

ธนาคารแห่งประเทศไทย

DFT

กสท

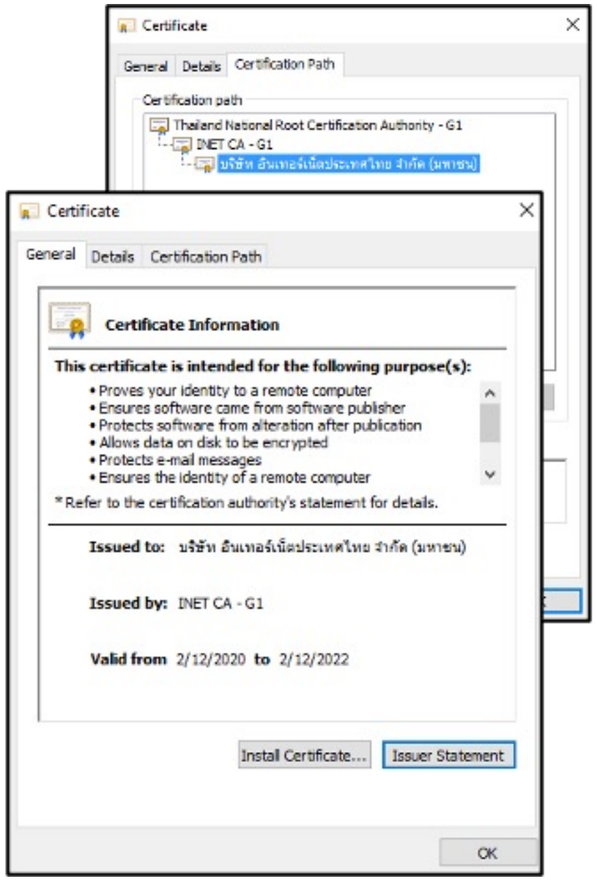
สำนักงานคณะกรรมการอ้อยและน้ำตาลทราย OFFICE THE CANE AND SUGAR BOARD

Agenda

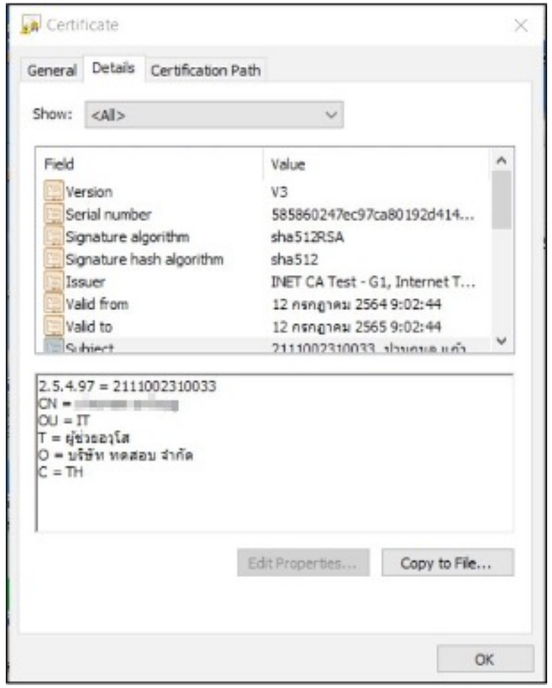
- Digital Certificate
- PKI based Digital Signature
  - Signature application
  - Security & Compliance & Legal
- Use case in Thailand
  - e-Tax invoice & e-Receipt
  - University and Education segment
  - Healthcare
  - Other
  - Recommendation
- Consideration & Future Challenge
- Q&A

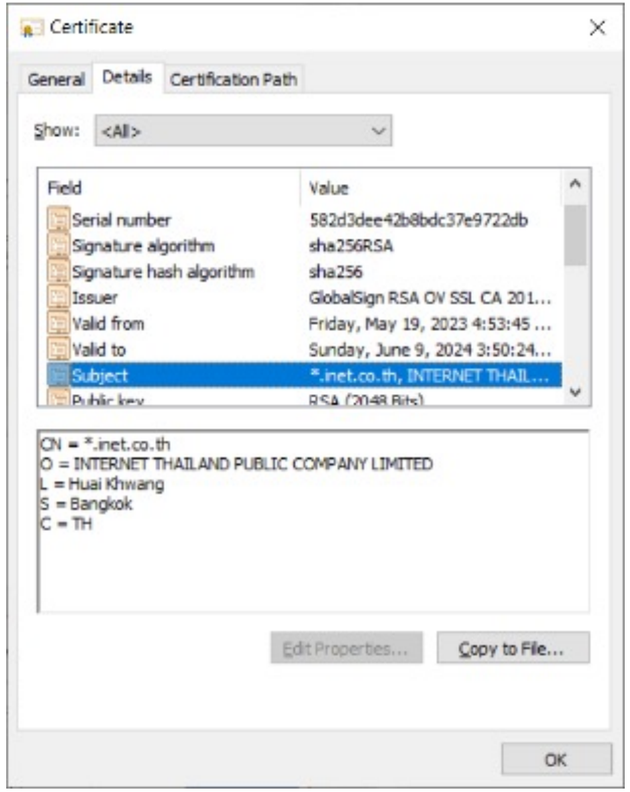
บริษัท วัน ออเทน จำกัด (One Authen) ผู้เชี่ยวชาญด้านการออกแบบและพัฒนาซอฟต์แวร์ ซึ่งเป็นบริษัทในเครือของบริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน)

Digital Certificate



Document Signing Certificate (17,285)



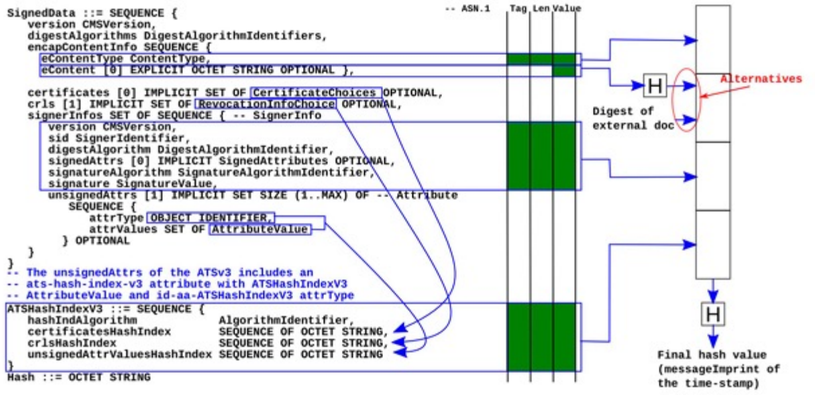


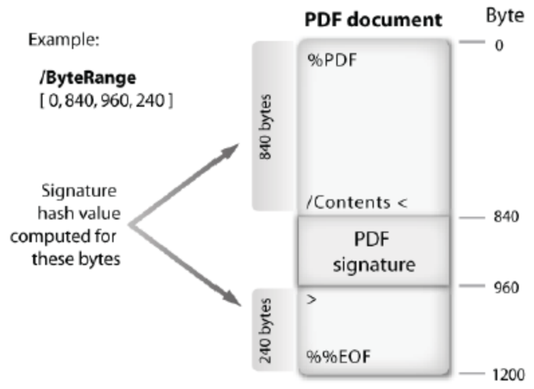
SSL Certificate (23)

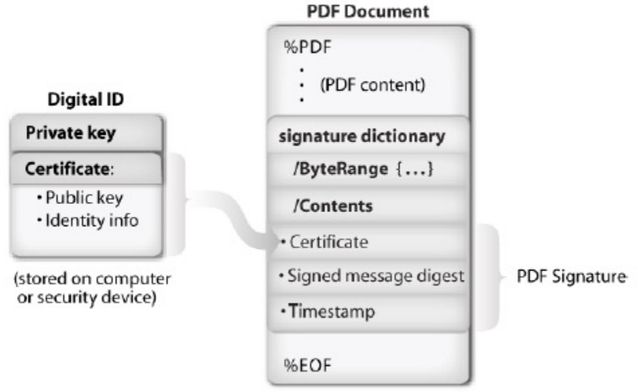
PKI Based Digital Signature

- **Image**

- **Cryptography**

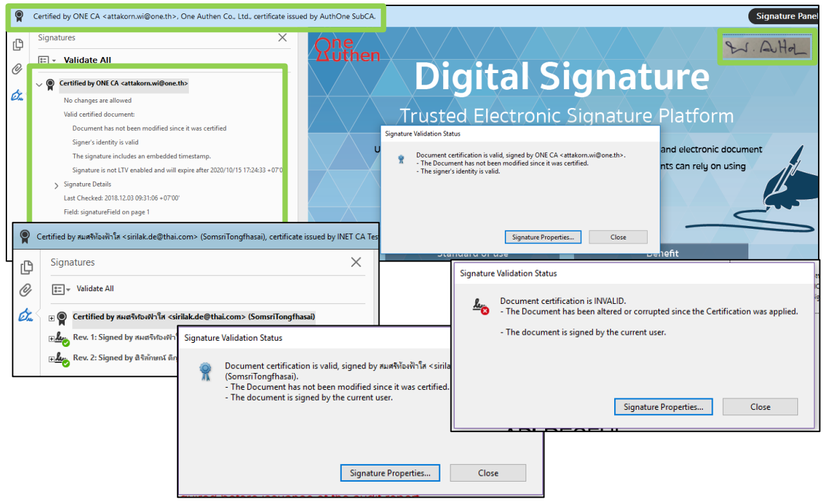




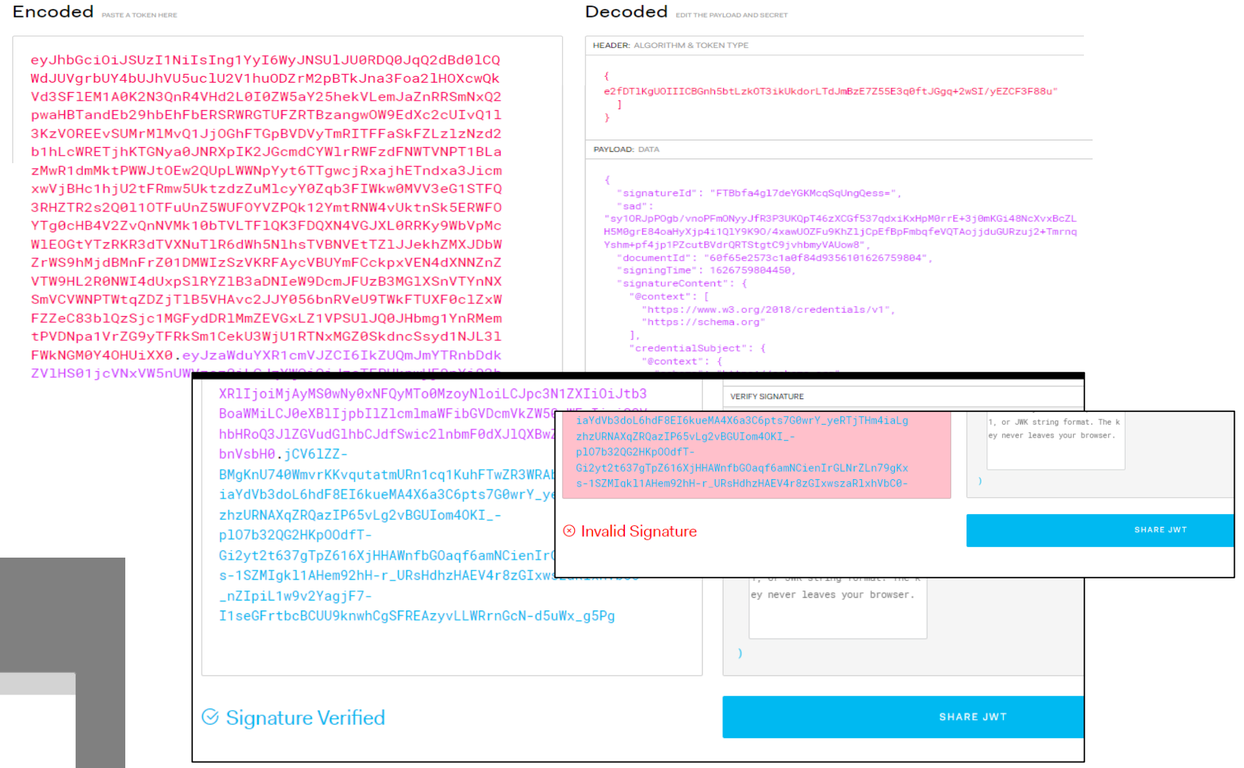


Signature application

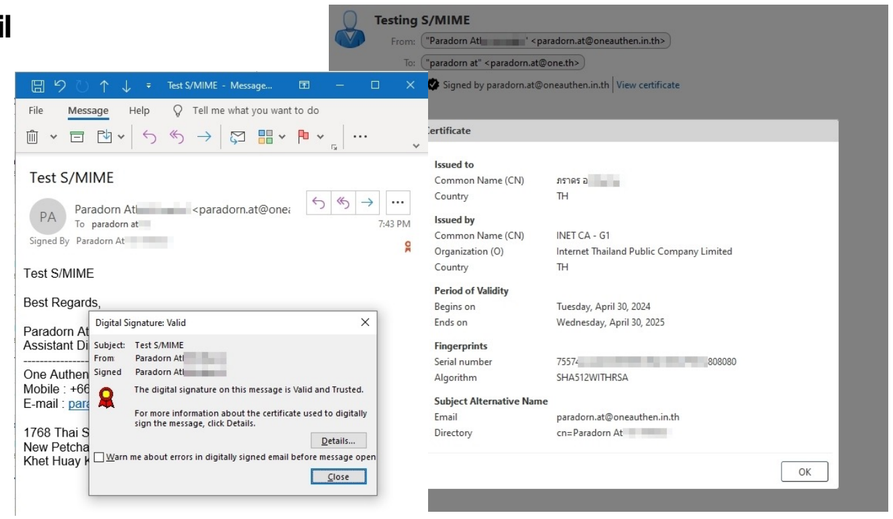
PDF



JSON



E-Mail

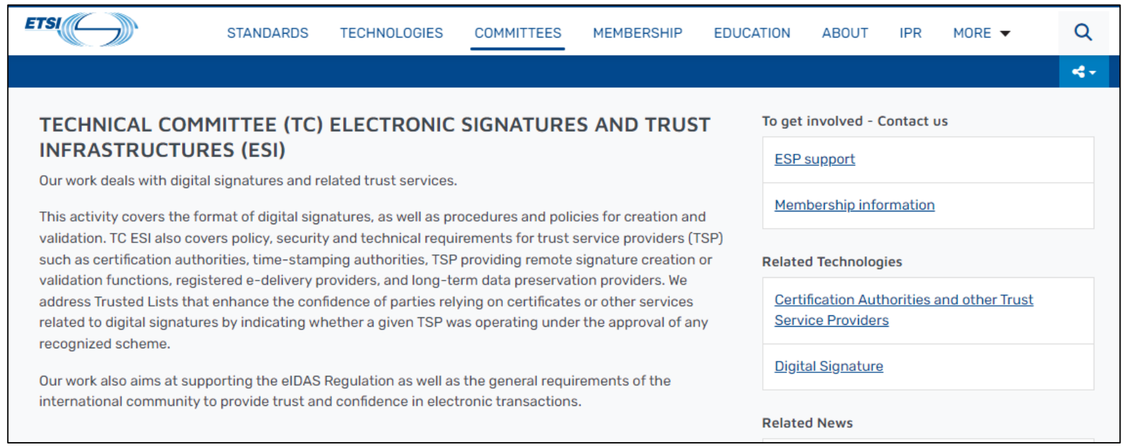


- **XML & OOXML**
- **BINARY**

Security & Compliance & Legal

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

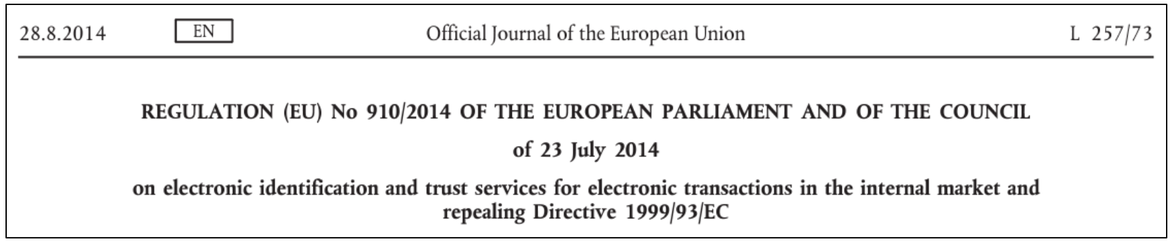
- ETSI: ESI: ref: https://www.etsi.org/committee/esi



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

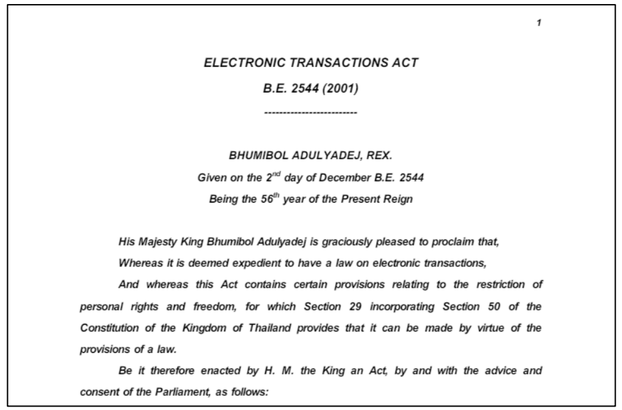
of 23 July 2014

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

ELECTRONIC TRANSACTIONS ACT

B.E. 2544 (2001)

BHUMIBOL ADULYADEJ, REX.

Given on the 2nd day of December B.E. 2544

Being the 56th year of the Present Reign

His Majesty King Bhumibol Adulyadej is graciously pleased to proclaim that,

Whereas it is deemed expedient to have a law on electronic transactions,

And whereas this Act contains certain provisions relating to the restriction of personal rights and freedom, for which Section 29 incorporating Section 50 of the Constitution of the Kingdom of Thailand provides that it can be made by virtue of the provisions of a law.

Be it therefore enacted by H. M. the King an Act, by and with the advice and consent of the Parliament, as follows:

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

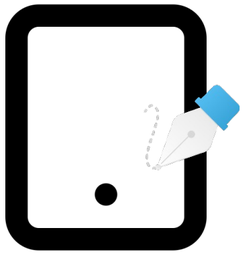
Electronic Signature Laws & Regulations - Ireland
Feb 2024 | https://helpx.adobe.com/legal/esignatures/regulations/ireland.html
Electronic Signature Laws & Regulations - Ireland

Electronic Signature Laws & Regulations - Ukraine
Nov 2023 | https://helpx.adobe.com/legal/esignatures/regulations/ukraine.html
Electronic Signature Laws & Regulations - Ukraine

One Authen

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**;

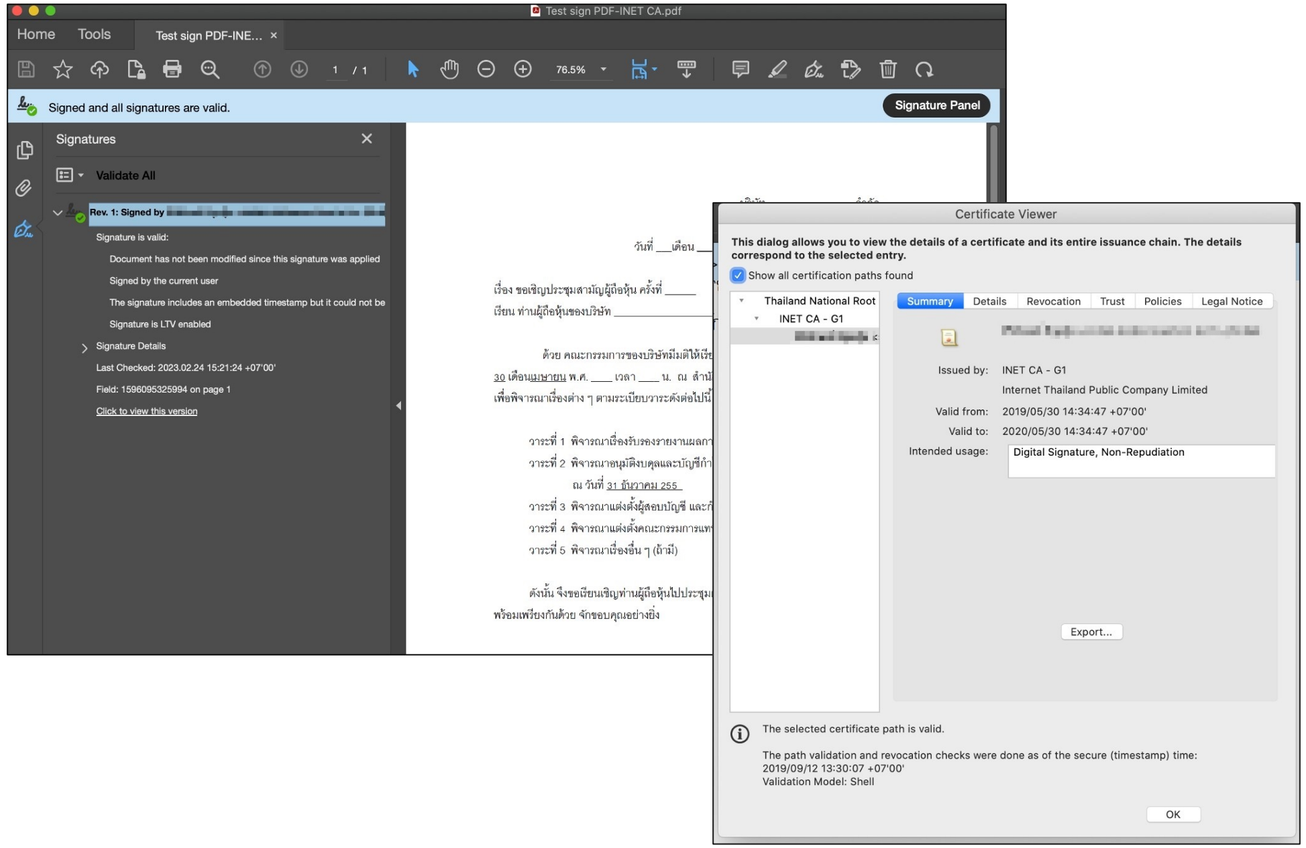
(2) **the signature creation data** were, at the time of signing, **under the control of the signatory and of no other person**;

(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



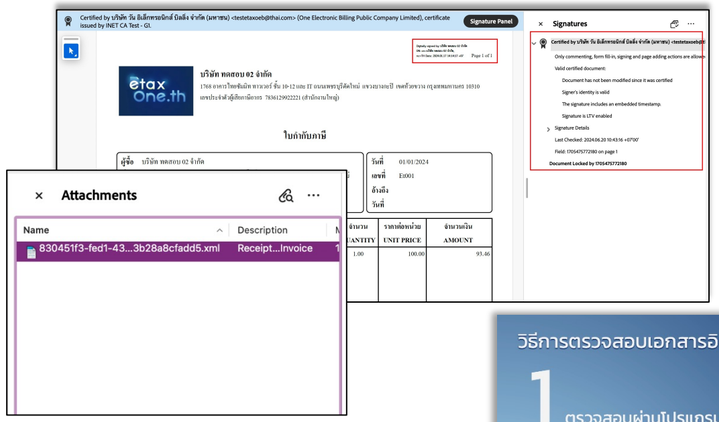
e-Tax invoice & e-Receipt

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

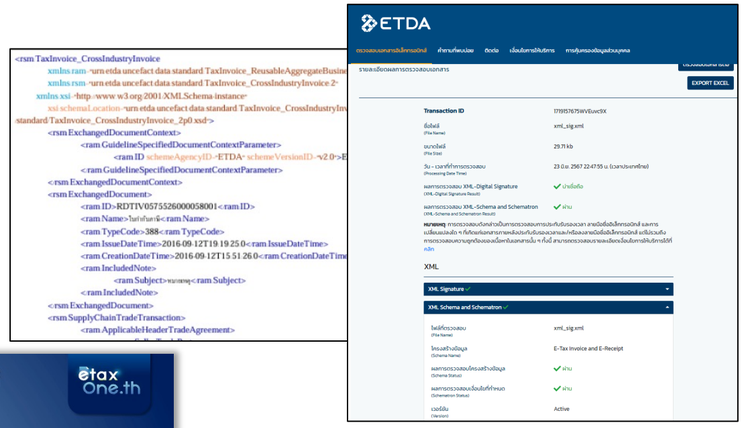
Standard & Recommendation

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

ส่งมอบให้ผู้ซื้อสินค้า หรือ ผู้รับบริการ



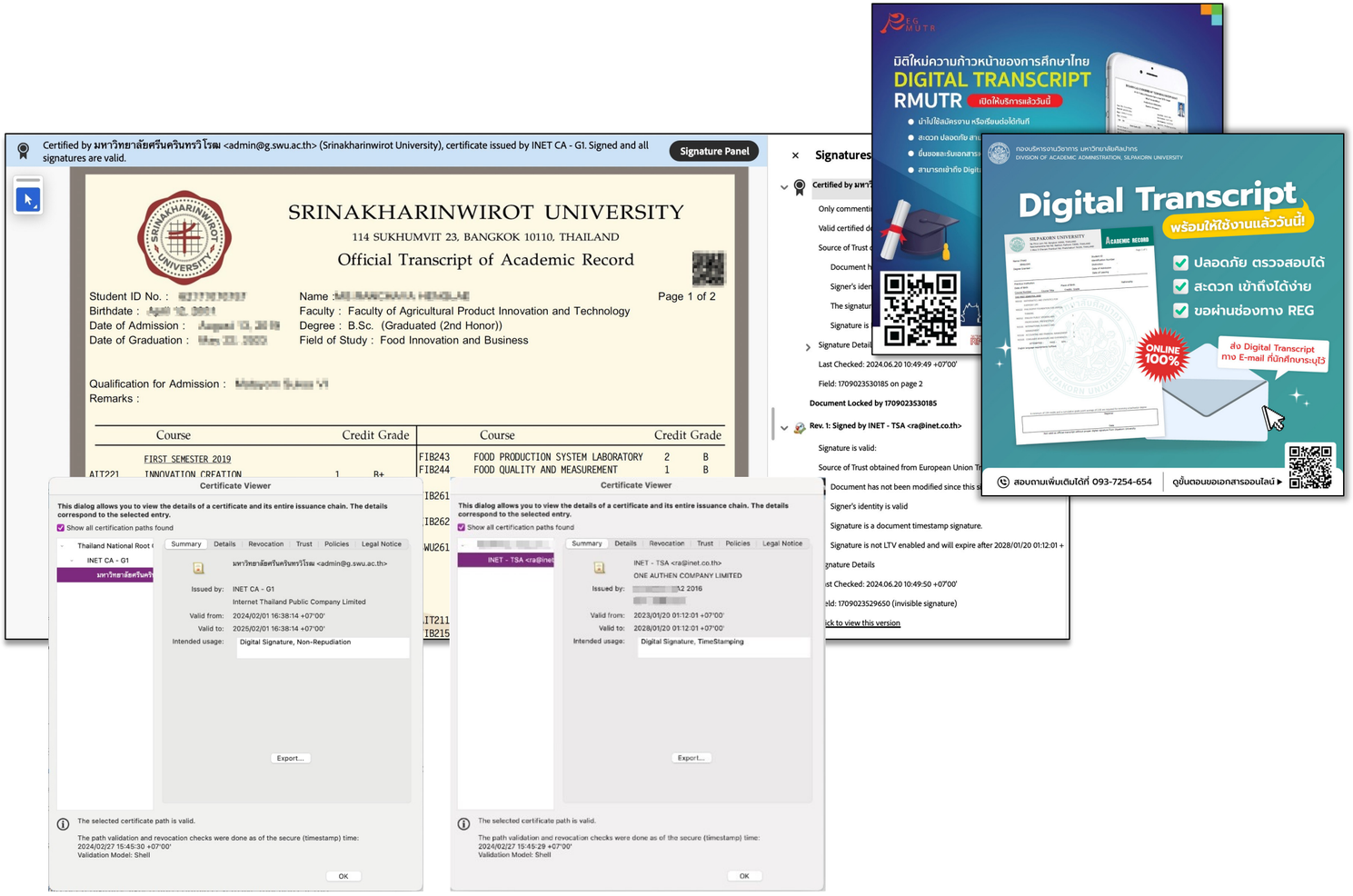
นำส่งสรรพากร



University and Education segment

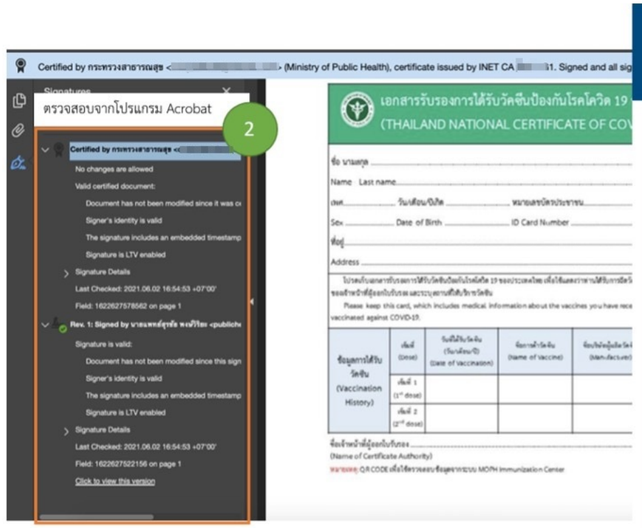
Standard & Recommendation

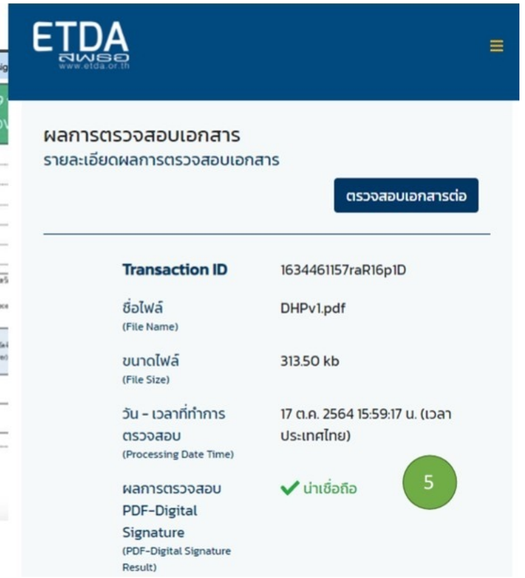
- **ขมธอ. 11-2560 :**
  การจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์
  (Electronic Certificate)
- **ขมธอ. 14-2560 :**
  การใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์
  (Using XML Messages for Inter-Organizational Data Exchange)
- **ขมธอ. 25-2563 :**
  ข้อความอิเล็กทรอนิกส์สำหรับใบประมวลผลการศึกษา
  (Message Standard for Academic Transcript)

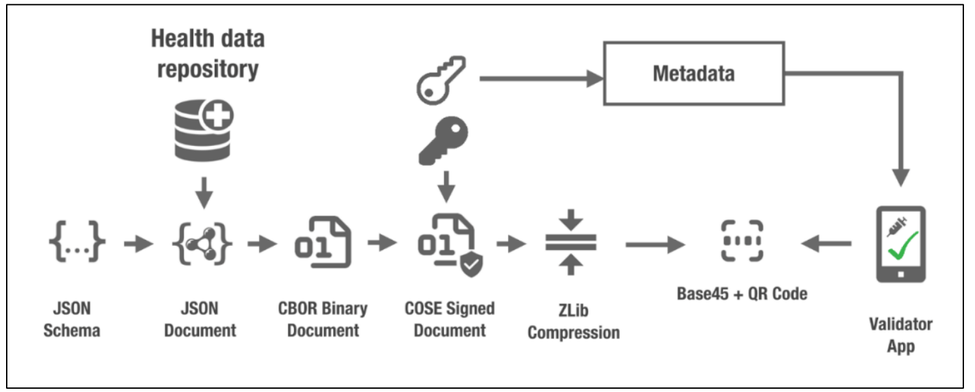



```
<?xml-model href="../schematron/DigitalTranscript_Schematron.sch" type="application/xml
<tc:Transcript
 xmlns:cct="urn:un:unece:uncefact:documentation:standard:CoreComponentsTechnicalSpecifi
 xmlns:qt="urn:etda:teda:data:QualifiedDataType:1"
 xmlns:tc="urn:etda:teda:documentation:Transcript:1"
 xmlns:udt="urn:un:unece:uncefact:data:standard:UnqualifiedDataType: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>ETR573020[redacted]</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[redacted]</tc:DataSubjectID>
    <tc:DataSubjectID schemeID="NIDN">140990[redacted]tc:DataSubjectID>
    <tc:NamePrefix languageID="th">[redacted]:NamePrefix>
    <tc:NamePrefix languageID="en">[redacted]amePrefix>
    <tc:GivenName languageID="th">[redacted]:GivenName>
    <tc:GivenName languageID="en">[redacted]:GivenName>
    <tc:FamilyName languageID="th">[redacted]:FamilyName>
    <tc:FamilyName languageID="en">[redacted]/tc:FamilyName>
    <tc:Gender>1</tc:Gender>
    <tc:BirthDate>1996-04-19T00:00:00.0</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: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>มัธยมศึกษาตอนปลาย</tc:PreviousCertificate>
```

Healthcare







Standard & Recommendation

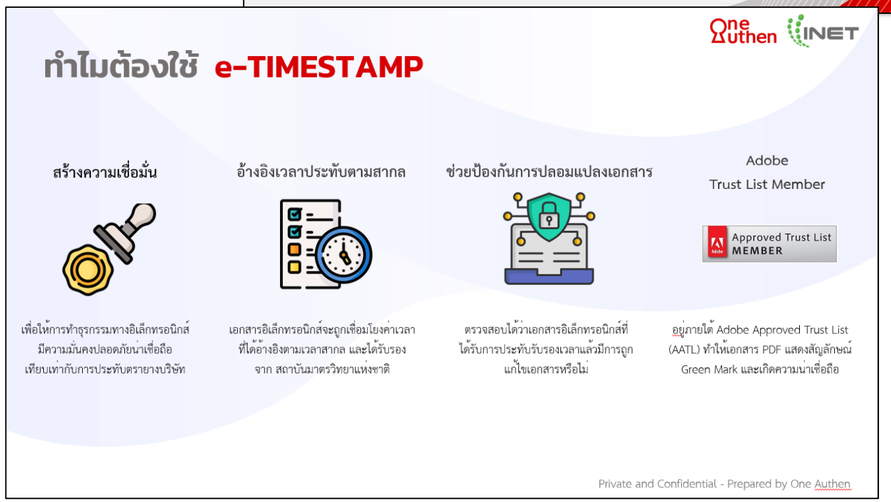
- **ขมธอ. 11-2560 :**
  การจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์
  (Electronic Certificate)
- **ขมธอ. 34-2566:**
  ใบรับรองแพทย์อิเล็กทรอนิกส์
  (Electronic Medical Certificate)
- **Technical Specifications for EU Digital COVID Certificates**

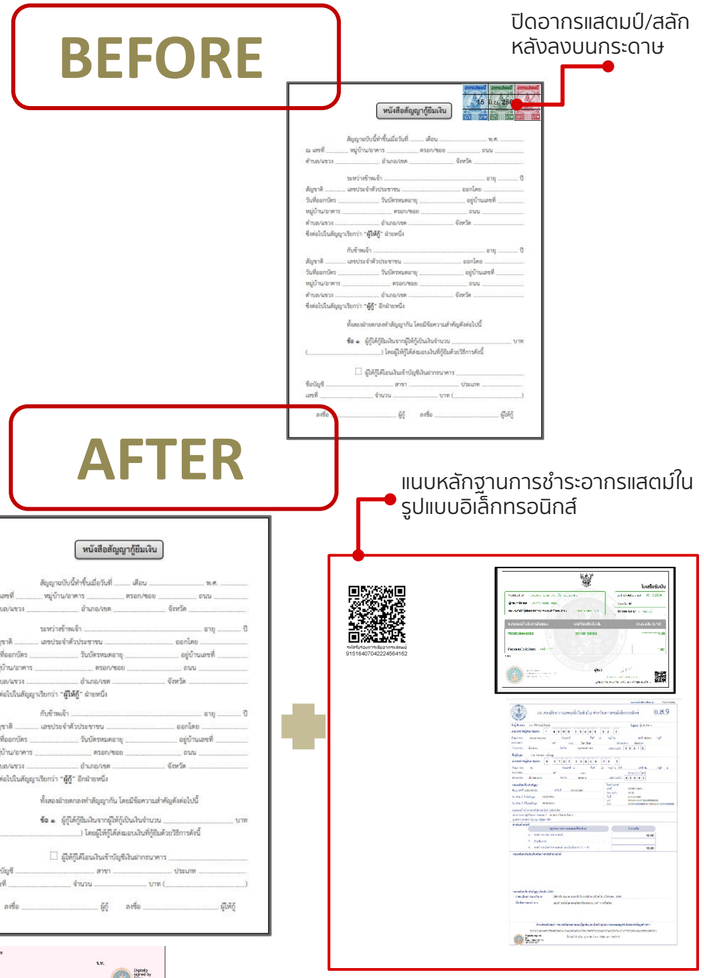
Other

- eStamp Duty
- ePolicy
- Timestamp Authority (TSA)

  e-TIMESTAMP
- Paperless System
- eSarabun
- NSW

  National Single Window





Recommendation

ข้อเสนอแนะมาตรฐานฯ (ETDA Recommendation)

Ref: https://www.etda.or.th/th/Our-Service/Recommendation.aspx

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

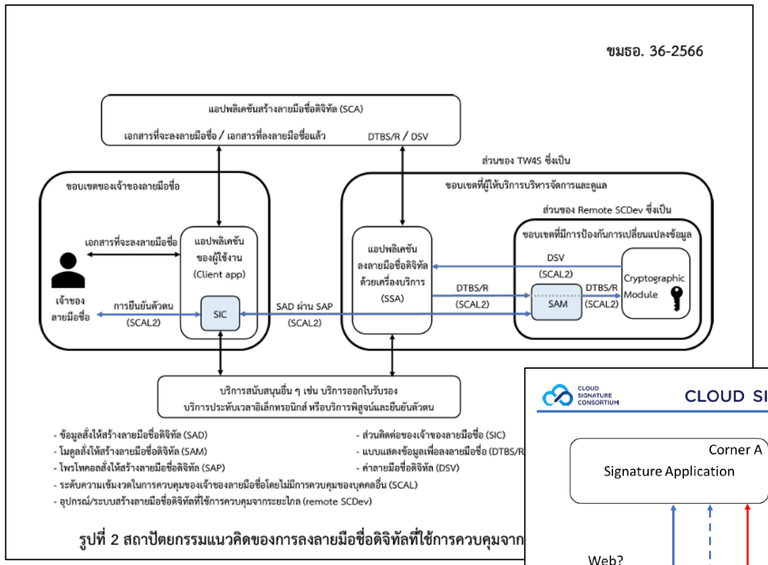
Consideration & Future Challenge

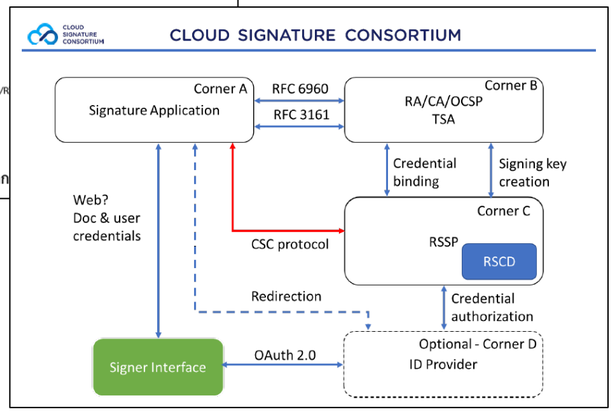
- **Traditional Signing & Remote Signing**

(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

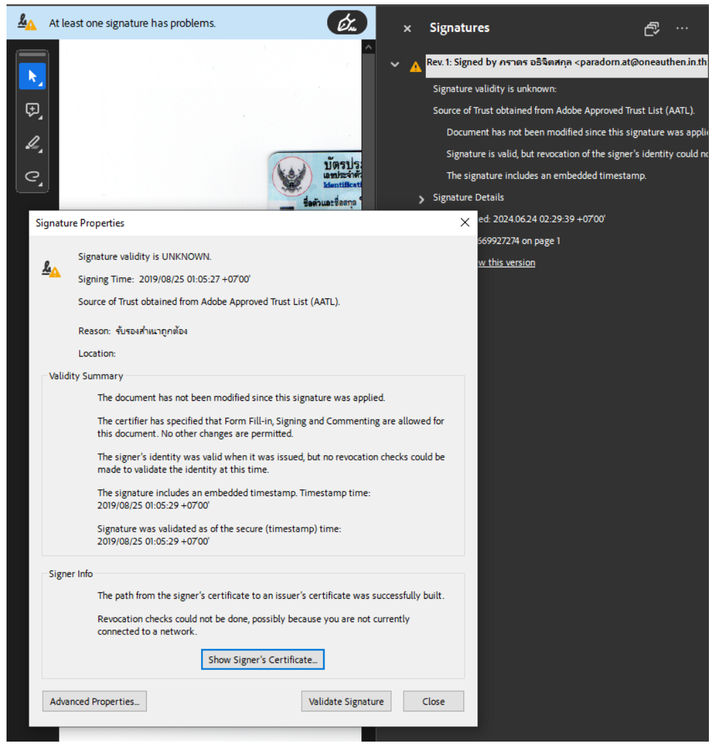




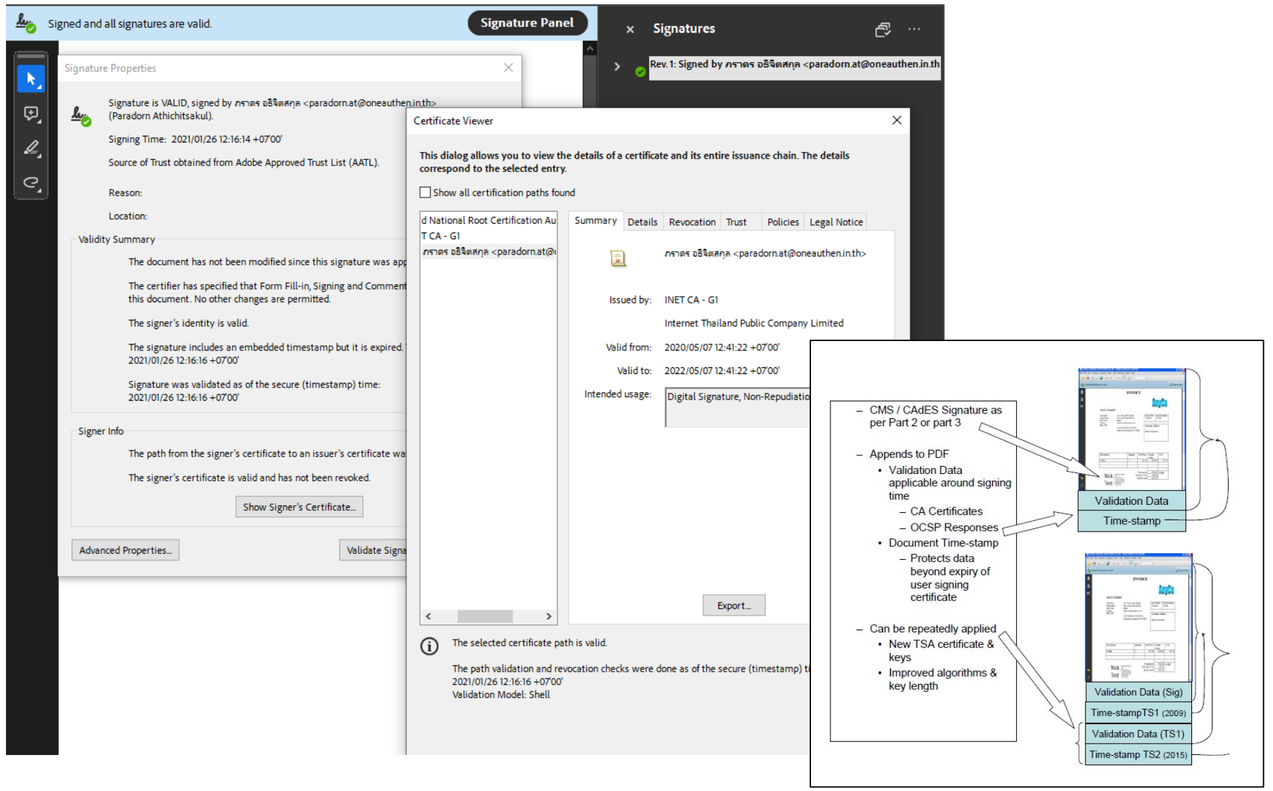
Consideration & Future Challenge

Document Archive & Digital Signature Validation

Simple digital signed document

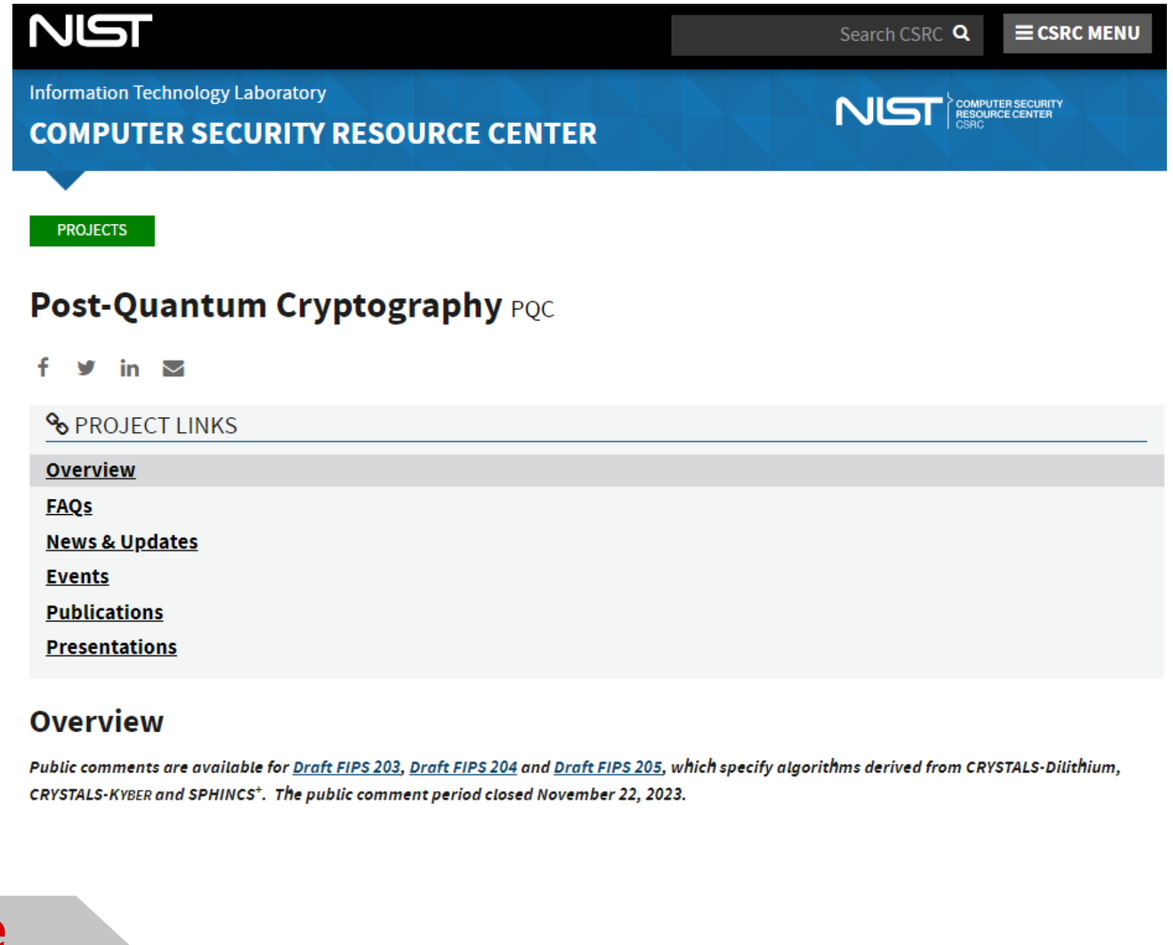


Simple digital signed document with LTV related attribute



Consideration & Future Challenge

- **Quantum Cryptography & AI-driven cryptography**



NIST Search CSRC CSRC MENU

Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER
NIST COMPUTER SECURITY RESOURCE CENTER CSRC

PROJECTS

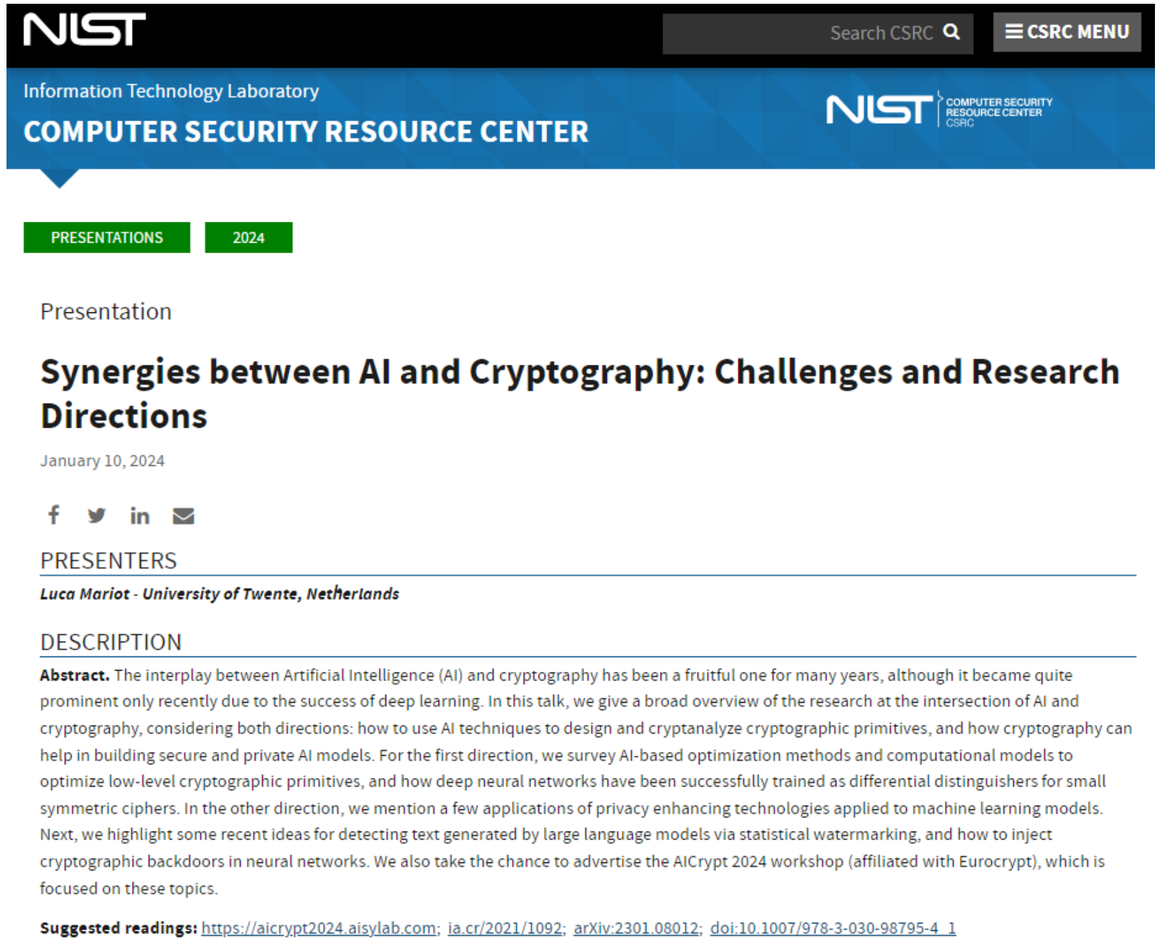
Post-Quantum Cryptography PQC

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.



NIST Search CSRC CSRC MENU

Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER
NIST COMPUTER SECURITY RESOURCE CENTER CSRC

PRESENTATIONS 2024

Presentation

Synergies between AI and Cryptography: Challenges and Research Directions

January 10, 2024

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; doi:10.1007/978-3-030-98795-4_1

Q&A

Thank you