กรมสรรพากร
THE REVENUE DEPARTMENT

06

การสร้างลายมือชื่อดิจิทัล DIGITAL SIGNATURE

ใบกำกับภาษีอิเล็กทรอนิกส์และใบรับอิเล็กทรอนิกส์ในรูปแบบ XML

(สำหรับนักพัฒนาซอฟต์แวร์)

E-TAX
INVOICE & RECEIPT

06

DIGITAL SIGNATURE

การสร้างลายมือชื่อดิจิทัล ใบกำกับภาษีอิเล็กทรอนิกส์และใบรับอิเล็กทรอนิกส์ในรูปแบบ XML

คำนำ

ผู้ประกอบการที่ได้รับการประกาศรายชื่อให้เป็นผู้มีสิทธิจัดทำใบกำกับภาษีหรือใบรับโดยใช้ใบรับรองอิเล็กทรอนิกส์ในการลงลายมือชื่อตามที่กฎหมายกำหนด ทุกครั้งที่มีการออกใบกำกับภาษีอิเล็กทรอนิกส์ (e-Tax Invoice) และใบรับอิเล็กทรอนิกส์ (e-Receipt) มีหน้าที่นำส่งข้อมูลที่เกี่ยวข้องกับใบกำกับภาษีหรือใบรับให้แก่กรมสรรพากร โดยข้อมูลใบกำกับภาษีหรือใบรับที่นำส่งจะต้องจัดทำขึ้นเป็นข้อมูลอิเล็กทรอนิกส์แบบมีโครงสร้างโดยใช้ XML format ตามข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยข้อความอิเล็กทรอนิกส์สำหรับการซื้อขายสินค้าหรือบริการ (ขมธอ. 3-2560) ที่มีการลงลายมือชื่อดิจิทัล ในรูปแบบ XAdES ด้วยใบรับรองอิเล็กทรอนิกส์ที่ออกโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ซึ่งการลงลายมือชื่อดิจิทัลนั้นเป็นรูปแบบหนึ่งของลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้

เอกสารฉบับนี้ จึงได้จัดทำขึ้นเพื่อให้ผู้พัฒนาโปรแกรมใช้ศึกษาและเป็นแนวทางในการสร้างลายมือชื่อดิจิทัลในรูปแบบ XAdES ด้วยใบรับรองอิเล็กทรอนิกส์ ควบคู่กับการใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลที่เกี่ยวข้องกับใบกำกับภาษีและหรือใบรับระหว่างผู้ประกอบการกับกรมสรรพากร ตามข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ระหว่างหน่วยงาน (ขมธอ.14-2560) เพื่อให้ผู้ประกอบการสามารถสร้างลายมือชื่อดิจิทัลซึ่งเป็นองค์ประกอบสำคัญของการจัดทำข้อมูลที่เกี่ยวข้องกับใบกำกับภาษีอิเล็กทรอนิกส์ (e-Tax Invoice) และใบรับอิเล็กทรอนิกส์ (e-Receipt) ได้อย่างถูกต้อง

สารบัญ

1. ขั้นตอนการจัดทำและลงลายมือชื่อดิจิทัล ใบกำกับภาษีอิเล็กทรอนิกส์ และใบรับอิเล็กทรอนิกส์ 4

2. การสร้างลายมือชื่อดิจิทัล ในรูปแบบ XAdES 5
   - 2.1 โครงสร้างลายมือชื่อดิจิทัลแบบ XAdES 6
   - 2.2 กระบวนการสร้างลายมือชื่อดิจิทัล 10
   - 2.3 คำอธิบายตัวอย่างลายมือชื่อดิจิทัล 13

3. การตรวจสอบความถูกต้อง ของลายมือชื่อดิจิทัล 18

4. ข้อเสนอแนะอื่นๆ 21

เอกสารอ้างอิง 23

กองบริหารการเสียภาษีทางอิเล็กทรอนิกส์
กรมสรรพากร
90 ซอยพหลโยธิน 7 ถนนพหลโยธิน
แขวงพญาไท เขตพญาไท กรุงเทพฯ 10400

RD Intelligence Center 1161

e_taxinvoice@rdservice.rd.go.th

1 ขั้นตอนการจัดทำและลงลายมือชื่อดิจิทัล ใบกำกับภาษีอิเล็กทรอนิกส์ และใบรับอิเล็กทรอนิกส์

> สำหรับนักพัฒนาซอฟต์แวร์

1 **ศึกษาข้อเสนอแนะ**มาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยข้อความอิเล็กทรอนิกส์สำหรับการซื้อขายสินค้าและบริการ (ขมธอ. 3-2560)

2 **ศึกษาข้อเสนอแนะ**มาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ระหว่างหน่วยงาน (ขมธอ. 14-2560) ในส่วนของการสร้างลายมือชื่อดิจิทัล ประกอบกับคู่มือฉบับนี้ ได้แนะนำวิธีการสร้างลายมือชื่อดิจิทัล

3 **พัฒนาระบบ**ของผู้ประกอบการให้สามารถจัดทำข้อมูลใบกำกับภาษีหรือใบรับให้อยู่ในรูปข้อมูลอิเล็กทรอนิกส์แบบไฟล์ XML ตามมาตรฐานฯ ว่าด้วยข้อความอิเล็กทรอนิกส์สำหรับการซื้อขายสินค้าและบริการ (ขมธอ. 3-2560) และพัฒนาโปรแกรมลงลายมือชื่ออิเล็กทรอนิกส์โดยใช้ใบรับรองอิเล็กทรอนิกส์ในรูปแบบลายมือชื่อดิจิทัล ตามมาตรฐาน XAdES สำหรับนำส่งกรมสรรพากร รวมถึงวิธีการลงลายมือชื่อดิจิทัลอื่น ๆ สำหรับเอกสารที่ส่งมอบให้กับผู้ซื้อสินค้าหรือผู้รับบริการ

4 **จัดหาใบรับรองอิเล็กทรอนิกส์**จากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority) ที่มีความน่าเชื่อถือ ภายใต้การรับรองของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์แห่งชาติ (Thailand National Root Certification Authority) โดยมีมาตรฐานหรือมาตรการด้านความมั่นคงปลอดภัยตามที่สำนักพัฒนาธุรกรรมทางอิเล็กทรอนิกส์กำหนด

5 **ตรวจสอบโครงสร้างข้อมูล**ใบกำกับภาษีหรือใบรับที่ได้จัดทำขึ้นในรูปแบบไฟล์ XML ทำได้ 2 วิธี

วิธีที่ 1 ตรวจสอบผ่านโปรแกรม XML Validator Tools ที่ผู้ประกอบการจัดหาเช่น XMLSpy หรือ Oxygen xml editor เปรียบเทียบกับไฟล์ตรวจสอบโครงสร้างข้อมูล (Schema & Schematron) สามารถดาวน์โหลดไฟล์ได้ที่ https://etax.rd.go.th > เมนูสนับสนุน > ดาวนโหลดโปแกรม เลือก “ไฟล์ตรวจสอบโครงสร้างข้อมูล (Schema & Schematron)”

วิธีที่ 2 ตรวจสอบผ่านเว็บไซต์กรมสรรพากร ได้ที่ https://etax.rd.go.th > เมนูสนับสนุน > ตรวจสอบโครงสร้างข้อมูล โดยวิธีนี้สามารถตรวจสอบได้ทั้งโครงสร้างข้อมูล (Schema & Schematron) และโครงสร้างลายมือชื่อดิจิทัล (Digital Signature)

2 การสร้างลายมือชื่อดิจิทัล ในรูปแบบ XAdES

> เอกสารอิเล็กทรอนิกส์

ปัจจุบันเอกสารอิเล็กทรอนิกส์เข้ามามีบทบาทสำคัญในการทำธุรกรรมต่าง ๆ ในทางธุรกิจ ทำให้หลายองค์กร หลายบริษัท ต้องปรับการทำงานหรือเปลี่ยนระบบการทำงานให้สอดคล้องกับเทคโนโลยีที่เข้ามามากขึ้น เอกสารอิเล็กทรอนิกส์จึงเป็นส่วนสำคัญส่วนหนึ่งที่จะทำให้เกิดการพัฒนาและทำงานได้อย่างราบรื่น โดยมีสิ่งสำคัญที่ควรคำนึงถึงคือการมีกลไกในการดูแลรักษาความมั่นคงปลอดภัยของข้อมูลในเอกสารอิเล็กทรอนิกส์ที่เหมาะสม เพื่อให้ผู้ใช้งานมีความเชื่อมั่น และเอกสารอิเล็กทรอนิกส์มีความน่าเชื่อถือและมีผลผูกพันทางกฎหมาย เทคนิคที่ใช้ในการรักษาความถูกต้องครบถ้วนของข้อมูล รวมถึงใช้ในการพิสูจน์ตัวตนของผู้ลงลายมือชื่อได้คือการลงลายมือชื่ออิเล็กทรอนิกส์โดยใช้ใบรับรองอิเล็กทรอนิกส์ ซึ่งต่อไปนี้จะเรียกว่า “การลงลายมือชื่อดิจิทัล”

> การลงลายมือชื่อดิจิทัลแบบ Advanced Electronic Signatures (AdES) แบ่งออกเป็น 3 แบบ ได้แก่

1 XML
Advanced Electronic Signatures (XAdES)

ใช้ลงลายมือชื่อดิจิทัล สำหรับไฟล์แบบ XML

2 PDF
Advanced Electronic Signatures (PAdES)

ใช้ลงลายมือชื่อดิจิทัล สำหรับไฟล์แบบ PDF

3 CMS
Advanced Electronic Signatures (CAdES)

ใช้ลงลายมือชื่อดิจิทัล สำหรับไฟล์แบบอื่นๆ

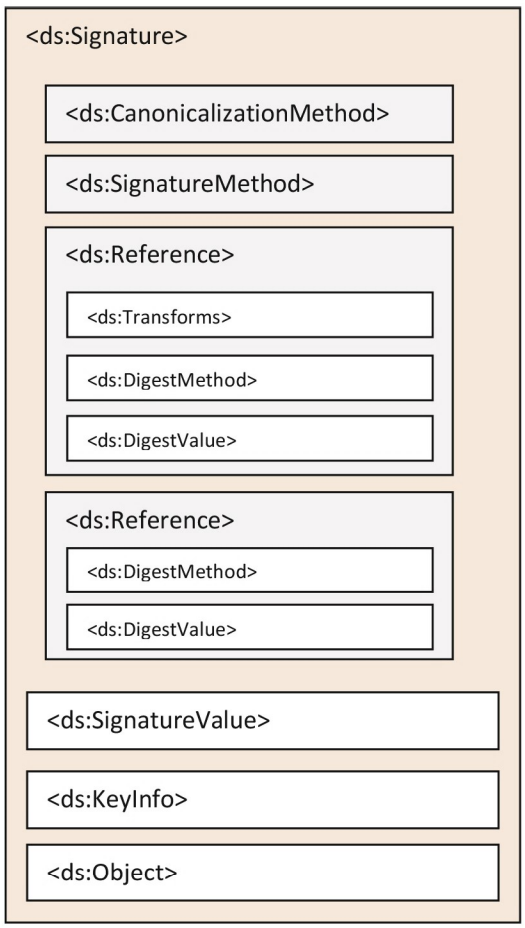
การลงลายมือชื่อดิจิทัลเพื่อจัดทำใบกำกับภาษีหรือใบรับในรูปข้อมูลอิเล็กทรอนิกส์โดยใช้ใบรับรองอิเล็กทรอนิกส์ในการลงลายมือชื่อ ภายใต้โครงการ e-Tax Invoice & e-Receipt ของกรมสรรพากร ประกอบด้วย

1. การลงลายมือชื่อดิจิทัลในใบกำกับภาษีอิเล็กทรอนิกส์ และใบรับอิเล็กทรอนิกส์ เพื่อส่งมอบให้ผู้ซื้อสินค้าหรือผู้รับบริการ ซึ่งวิธีการลงลายมือชื่อดิจิทัลจะขึ้นอยู่กับประเภทเอกสารอิเล็กทรอนิกส์ที่ผู้ประกอบการจัดทำขึ้น

2. การลงลายมือชื่อดิจิทัลในข้อมูลที่เกี่ยวข้องกับใบกำกับภาษีหรือใบรับเพื่อส่งให้กรมสรรพากร ซึ่งข้อมูลจัดทำขึ้นในรูปแบบไฟล์ XML ตามข้อเสนอแนะมาตฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยข้อความอิเล็กทรอนิกส์สำหรับการซื้อขายสินค้าและบริการ (ขมธอ. 3-2560) จะใช้วิธีการลงลายมือชื่อดิจิทัล แบบ XAdES ซึ่งเป็นมาตรฐานในการลงลายมือชื่ออิเล็กทรอนิกส์บนเอกสาร XML

> การสร้างลายมือชื่อดิจิทัล แบบ XAdES สำหรับไฟล์ XML (ภายใต้โครงการ e-Tax Invoice & e-Receipt)

2.1 โครงสร้างลายมือชื่อดิจิทัล แบบ XAdES สำหรับไฟล์ XML มีองค์ประกอบหลักดังนี้



รูปที่ 2.1 โครงสร้างการลงลายมือชื่อดิจิทัลแบบ XMLDSIG

1 **SignedInfo element** ประกอบด้วยข้อมูล algorithms หรือขั้นตอนในการลงลายมือชื่ออิเล็กทรอนิกส์ในชื่อเอกสาร ประกอบด้วย

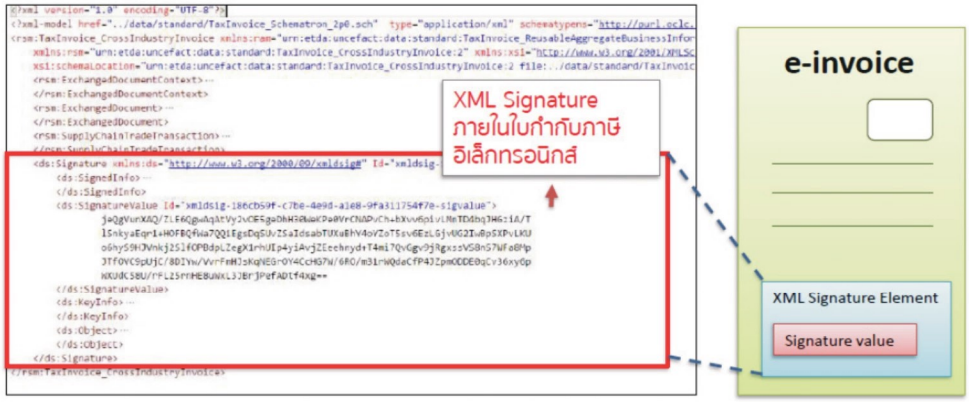
1.1 Canonicalization Method หรือขั้นตอนการจัดโครงสร้างของ XML ก่อนทำการลงลายมือชื่อ โดย W3C กำหนดให้ XML-C14N (http://www.w3.org/TR/2001/REC-xml-c14n-20010315) สำหรับ Canonical XML 1.0 และ XML-C14N11 สำหรับ Canonical XML 1.1 (http://www.w3.org/2006/12/xml-c14n11)

1.2 Signature Method หรือ Algorithms ที่ใช้ในการ สร้าง Digital Signature เป็นค่าการเข้ารหัส Hash Value และ DigestValue แบบ Private Key ของผู้ลงลายมือชื่อดิจิทัล จะจัดให้อยู่ในรูปแบบ Base 64

1.3 Reference หรือข้อมูลอื่นๆ ที่ใช้ในการลงลายมือชื่อดิจิทัล

1.3.1 การ transform signature โดยข้อมูลใน transform element สามารถกำหนดได้ว่าจะให้ XMLDSIG อยู่ในรูปแบบ Enveloped (ลายมือชื่อภายในเนื้อหาเอกสาร)

โครงการนี้ใช้ Signature ประเภท Enveloped Signature XML Signature element จะอยู่ภายใต้ root ของ XML Document



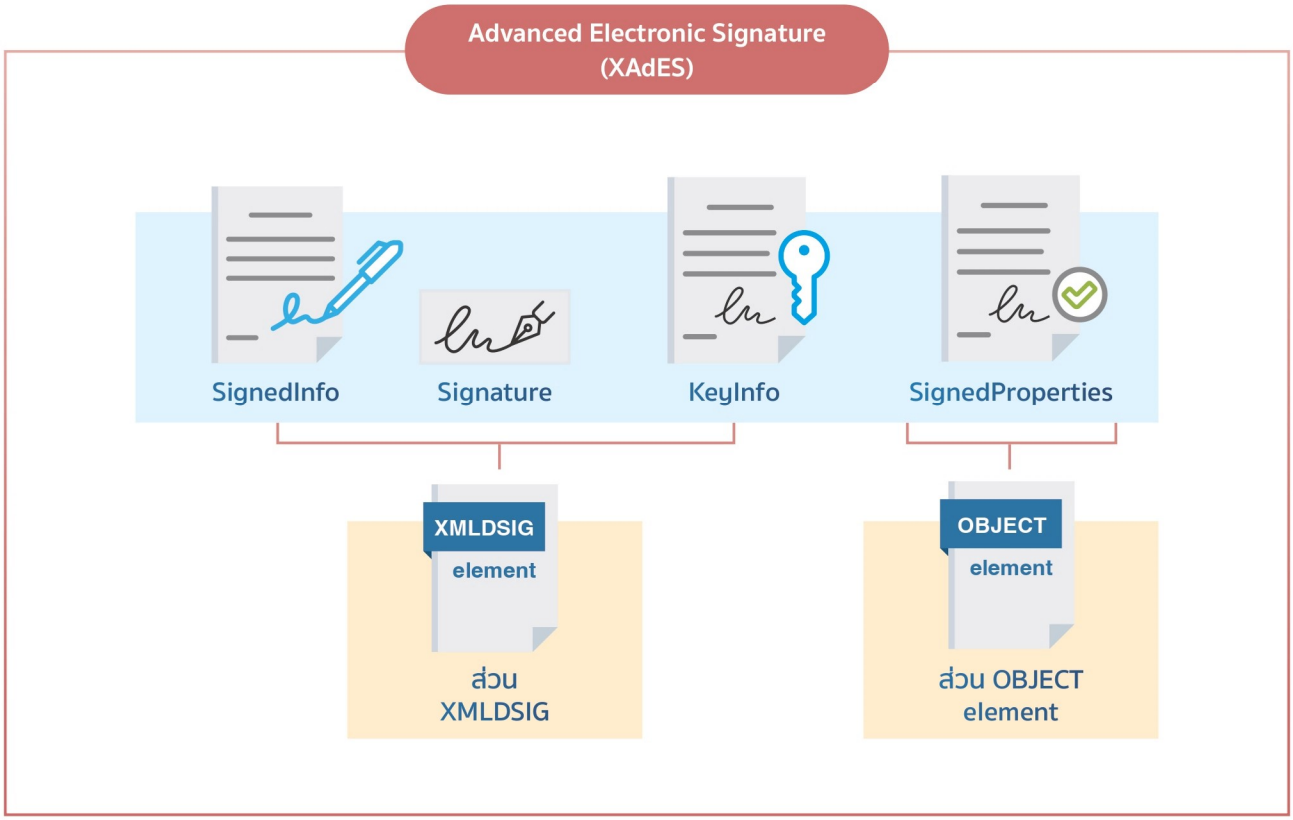
รูปที่ 2.2 Digital Signature จะแทรกอยู่ในข้อความภายใต้ root element

1.3.2 Digest Method เป็น algorithms ที่ใช้ในการทำ Digest Message (Hash value ของเนื้อหาเอกสาร) โครงการนี้ให้ใช้ Digest Method ในกลุ่ม SHA-2 (SHA-512)

1.3.3 Digest Value เป็น Digest Message หรือ ค่า Hash ของเอกสาร XML โดยค่า Hash ดังกล่าวจะอยู่ในรูปแบบ Base 64 (ตามข้อกำหนด W3C Recommendation on XML Signature Syntax and Processing [1])

2 **SignatureValue** เป็นค่าของลงลายมือชื่อดิจิทัลถูกเข้ารหัสในรูปแบบ Base 64

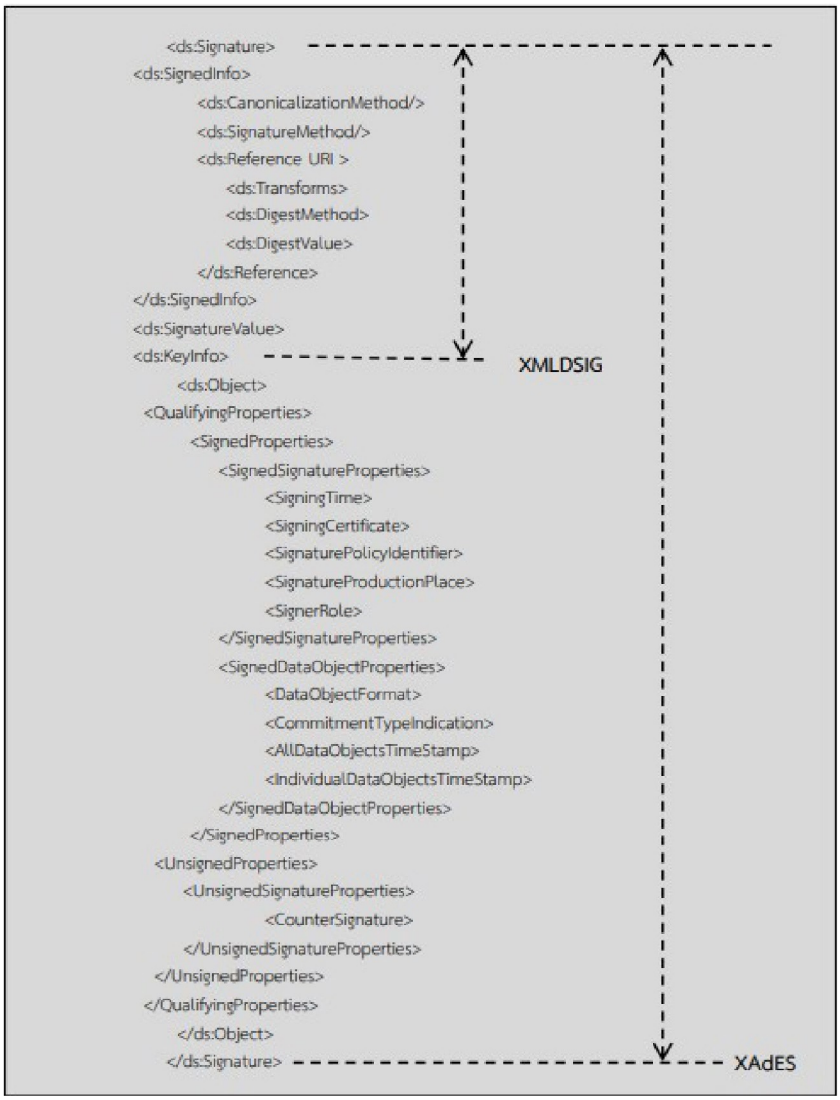
3 **KeyInfo** ให้ข้อมูลใบรับรองอิเล็กทรอนิกส์ของผู้ลงลายมือชื่อ X509 SubjectName ประกอบด้วย element ซึ่งระบุ Distinguished Name ของเจ้าของใบรับรองอิเล็กทรอนิกส์ X509 และ Certificate ระบุ Certificate ถูกเข้ารหัสแบบ Base 64



รูปที่ 2.3 โครงสร้างการลงลายมือชื่อดิจิทัลในรูปแบบ XAdES

4 **SignedProperties** เป็น element ภายใต้ Signature/ Object/ QualifyingProperties ประกอบด้วย element ต่างๆ ที่จะถูกลงลายมือชื่อในขั้นตอนการสร้าง XMLDISG ซึ่ง element ที่อยู่ภายใต้ SignedProperties ตัวอย่างเช่น SigningTime, SigningCertificate, SignatureProductionPlace และ SignaturePolicy

ทั้งนี้ โครงการจัดทำใบกำกับภาษีอิเล็กทรอนิกส์และใบรับอิเล็กทรอนิกส์จะใช้การลงลายมือชื่อดิจิทัล (Digital Signature) แบบ Basic Signature เท่านั้น โดยกระบวนการสร้างลงลายมือชื่อดิจิทัลแบบ XAdES จะกล่าวถึงในหัวข้อ 2.2 และการตรวจสอบความถูกต้องของลงลายมือชื่อดิจิทัล จะกล่าวถึงในหัวข้อที่ 3



รูปที่ 2.4 แสดง SignedProperties ภายใต้ XAdES

> การสร้างลายมือชื่อดิจิทัลแบบ XAdES

การสร้างลายมือชื่อดิจิทัลเบื้องต้น (Basic Signature) ใช้ข้อมูลนำเข้าซอฟต์แวร์สร้างลายมือชื่อ ดังนี้

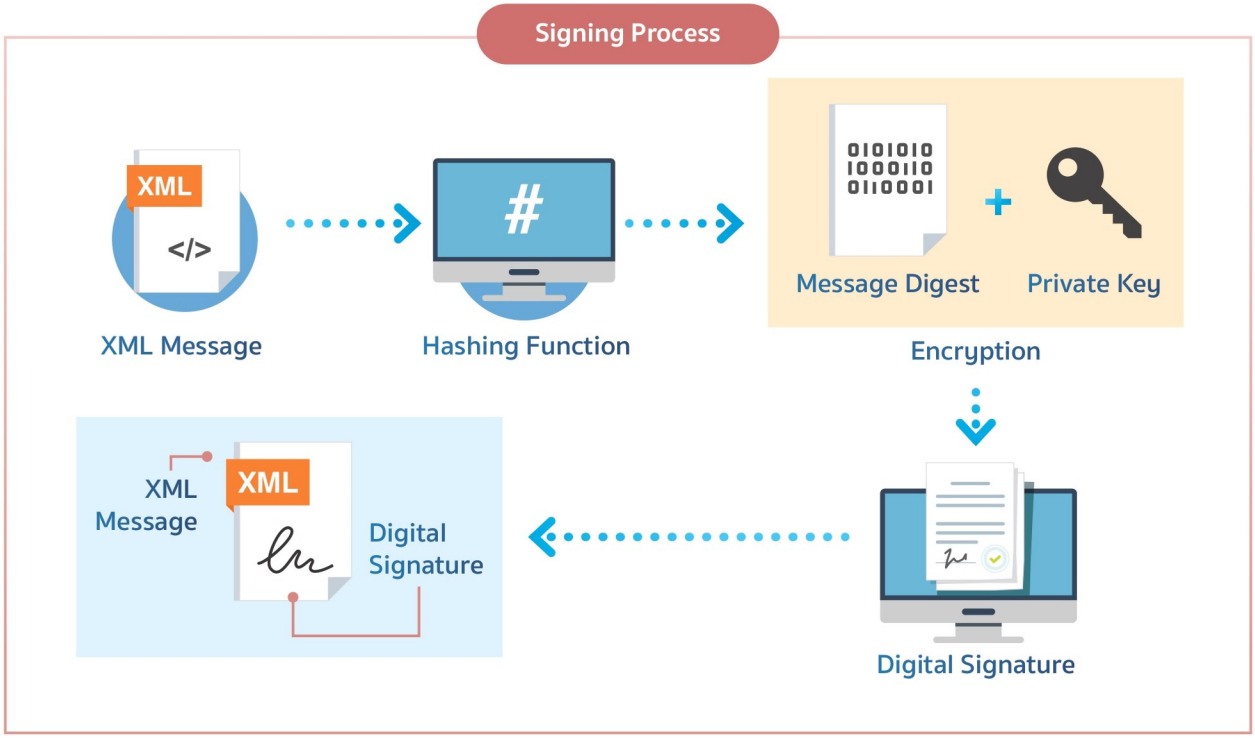
ข้อมูลนำเข้า	จำเป็น/ ไม่ใช้
เอกสารอิเล็กทรอนิกส์ (Document)	จำเป็นต้องมี
ใบรับรองอิเล็กทรอนิกส์ของเจ้าของลายมือชื่อ (Certificate)	จำเป็นต้องมี
รายการข้อมูลของลงลายมือชื่อดิจิทัล (Signature Attributes)	จำเป็นต้องมี

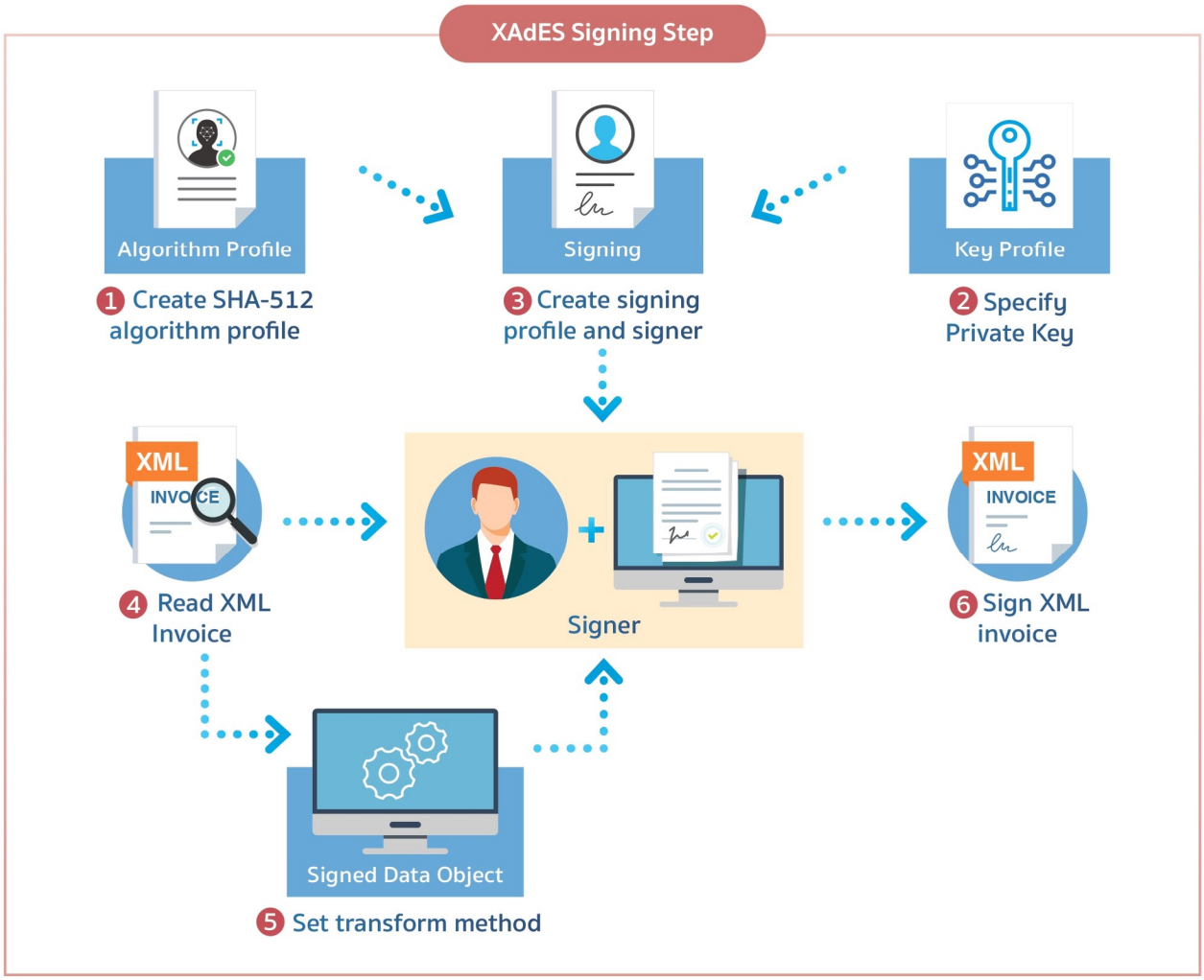
ค่ากำหนดของซอฟต์แวร์

1) ค่าของการลงลายมือชื่อดิจิทัล (Signature Value)
2) รายการข้อมูลใน element SignedProperties

2.2 กระบวนการสร้างลายมือชื่อดิจิทัล

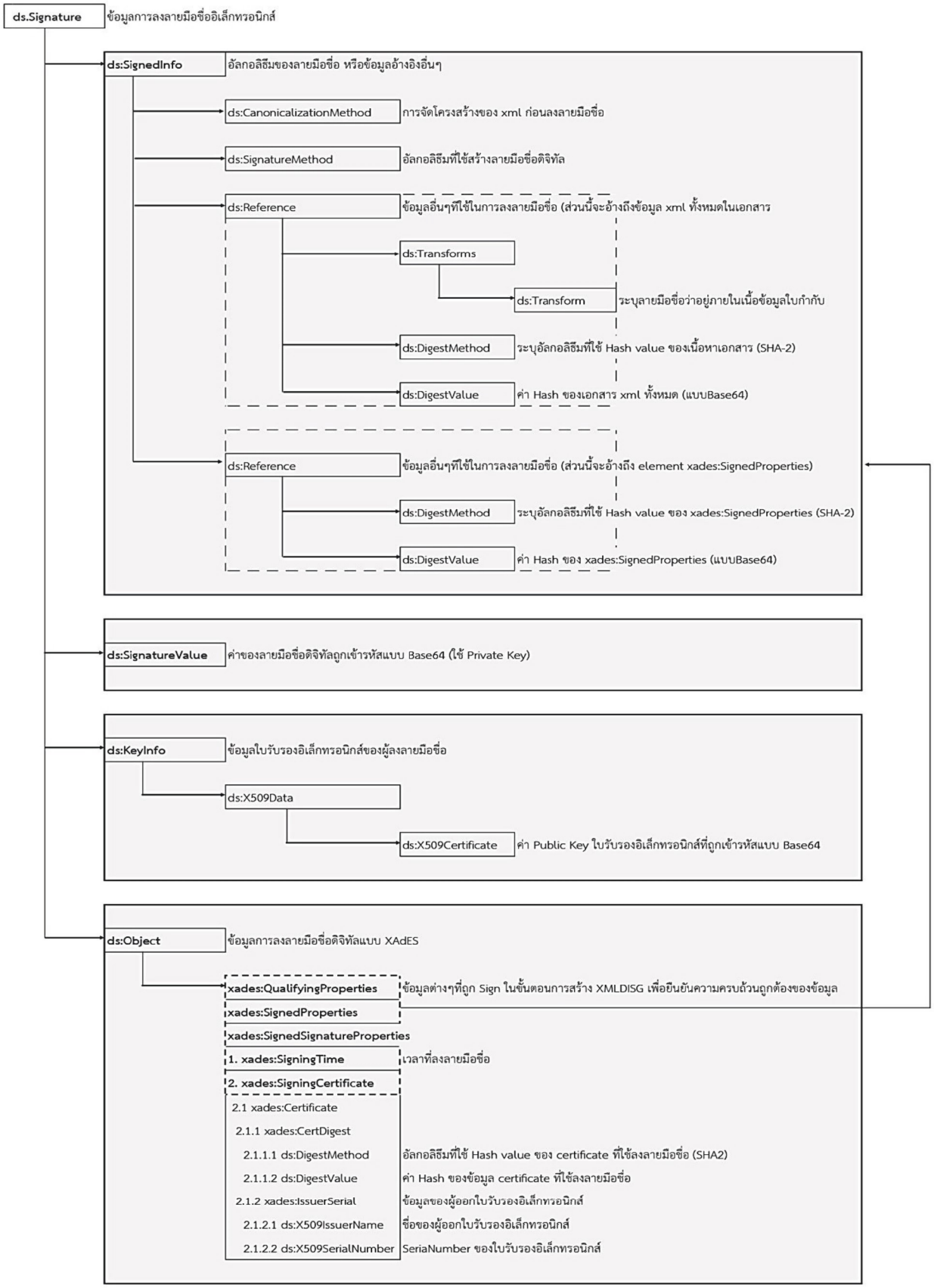
1. จัดหาหรือพัฒนาซอฟต์แวร์ที่ใช้ลงลายมือชื่อ จะต้องมีความสามารถในการให้ผู้ใช้งานสามารถลงลายมือชื่อดิจิทัลกำกับทั้งเอกสาร ซึ่งในโครงการนี้ใช้รูปแบบการลงลายชื่อดิจิทัลทั้งเอกสาร
2. นำข้อมูล XML มาทำขั้นตอนการจัดโครงสร้างของ XML (Canonicalization Method) อ้างอิงจากเว็บไซต์ https://www.w3.org/TR/xml-c14n/
3. กำหนดฟอร์แมตของการลงลายมือชื่อดิจิทัลแบบ XAdES คลาสของการลงลายมือชื่อดิจิทัล BasicSignature และรูปแบบของการลงลายมือชื่อเป็น Enveloped
4. ในกระบวนการที่ใช้ในการลงลายมือชื่อต้องมีกลไกในการแจ้งเตือนผู้ใช้งานว่าจะมีการลงลายมือชื่อเพื่อใช้ในการรับการยินยอม (Consent) จากเจ้าของลายมือชื่อ
5. กระบวนการจะทำการสร้างลายมือชื่อต้องตรวจสอบใบรับรองอิเล็กทรอนิกส์ของเจ้าของลายมือชื่อก่อนว่ายังไม่ถูกเพิกถอนหรือหมดอายุ
6. ในการลงลายมือชื่ออาจมีกระบวนการตรวจสอบตัวตนของผู้ลงลายมือชื่อด้วย เช่น การขอให้ผู้ลงลายมือชื่อระบุรหัสผ่าน (ของ Private Key)
7. ทำการสร้างลงลายมือชื่อดิจิทัลโดยใช้ Digest Method เป็น algorithms ที่ใช้ในการทำ Digest Message โครงการนี้ให้ใช้ Digest Method ในกลุ่ม SHA-2 (SHA-512) และทำให้อยู่ในรูปแบบ Base 64
8. นำลงลายมือชื่อดิจิทัลที่ได้จากกระบวนการขั้นต้น มาประกอบเข้ากับเอกสารอิเล็กทรอนิกส์





รูปที่ 2.5 แผนภาพขั้นตอนการลงลายมือชื่อดิจิทัลแบบ XAdES

โครงสร้างของลายมือชื่อดิจิทัลที่ใช้ในโครงการ



2.3 คำอธิบายตัวอย่างลายมือชื่อดิจิทัล

> ds:Signature คือ Element ข้อมูลของการลงลายมือชื่อดิจิทัล

1 **ds:Signedinfo** คือ Element ที่ระบุอัลกอริทึมแบบ canonicalizationMethod, อัลกอริทึมของลายมือชื่อ หรือข้อมูลอ้างอิงอื่นๆ หรืออาจจะระบุ ID ที่ใช้อ้างอิงโดยลายมือชื่ออื่นๆ หรือ Object

1.1 **ds:Canonicalization Method** คือ ขั้นตอนการจัดโครงสร้างของข้อความเนื้อ xml ก่อนทำการลงลายมือชื่อดิจิทัล เพื่อแก้ไขปัญหา XML ที่ถูกสร้างจากระบบปฏิบัติการ UNIX และ Windows จะมีอักขระในการตัดบรรทัดใหม่ที่แตกต่างกัน กระบวน Canonicalization จะแปลงให้อยู่ในระบบกลาง ทำให้สามารถอ่านในระบบปฏิบัติการ UNIX กับ Windows ได้ และความหมายเหมือนกัน

1.2 **ds:SignatureMethod** คือ element ที่จัดเก็บ Algorithms SHA-512 ที่ใช้ในการลงลายมือชื่อ

1.3 **ds:Reference** หรือข้อมูลอื่นๆ ที่ใช้ในการลงลายมือชื่อดิจิทัล ซึ่ง element นี้ จัดเก็บ URI เท่ากับค่าว่าง (URI="") หมายถึงอ้างอิงถึงข้อมูล xml ทั้งหมดในเอกสารนี้

- 1.3.1 **ds:Transforms** คือ element ที่กำหนดว่า XMLDSIG อยู่ในรูปแบบไหน ซึ่งในโครงการใช้รูปแบบ Enveloped คือ XMLDSIG อยู่ในเนื้อข้อมูลเอกสาร XML
- 1.3.2 **ds:DigestMethod** เป็น element ระบุ Algorithms ที่ใช้ในการทำ Digest Message (Hash value ของเนื้อหาเอกสาร) โครงการนี้ให้ใช้ Digest Method ในกลุ่ม SHA-2 (SHA-512)
- 1.3.3 **ds:DigestValue** เป็น Digest Message หรือค่า Hash ของเอกสาร XML ทั้งหมด โดยค่า Hash ดังกล่าวจะอยู่ในรูปแบบ Base 64

1.4 **ds:Reference** คือข้อมูลที่ใช้ในการลงลายมือชื่อดิจิทัล ซึ่ง element นี้อ้างอิงถึงข้อมูล element xades:SignedProperties ในเอกสารนี้

จาก element ตามตัวอย่างข้อมูลเป็นค่า URI="#xmldsig-522d79b4-afac-421e-a47d-5df812053914-signedprops"

- 1.4.1 **ds:DigestMethod** เป็น element ระบุ algorithms ที่ใช้ในการทำ Digest Message (Hash value ของข้อมูล element xades:SignedProperties) โครงการนี้ให้ใช้ Digest Method ในกลุ่ม SHA-2 (SHA-512)
- 1.4.2 **ds:DigestValue** เป็น Digest Message คือค่า Hash ของข้อมูล XML ที่อ้างอิง element xades:SignedProperties ตาม Id="#xmldsig-522d79b4-afac-421e-a47d-5df812053914-signedprops" โดยค่า Hash ดังกล่าวจะอยู่ในรูปแบบ Base 64

2 **ds:SignatureValue** เป็นค่าการเข้ารหัสของ element ds:SignedInfo ด้วย Private Key ของผู้ลงลายมือชื่อดิจิทัลจะอยู่ในรูปแบบ Base 64

3 **ds:KeyInfo** คือ element ข้อมูลใบรับรองอิเล็กทรอนิกส์ของผู้ลงลายมือชื่อ

3.1 ds:X509Data

- 3.1.1 **ds:Transforms** คือ element ที่กำหนดว่า XMLDSIG อยู่ในรูปแบบไหน ซึ่งในโครงการใช้รูปแบบ Enveloped คือ XMLDSIG อยู่ในเนื้อข้อมูลเอกสาร XML

4 **vds:Object** คือ element ระบุข้อมูลของการลงลายมือชื่ออิเล็กทรอนิกส์แบบ XAdES

4.1 **xades:QualifyingProperties** คือ ระบุข้อมูลรูปแบบการลงลายมือชื่ออิเล็กทรอนิกส์ของ XAdES ซึ่งโครงการจะเป็นรูปแบบ Signed Properties

- 4.1.1 **xades:SignedProperties** คือ element ต่างๆ ที่จะถูก sign ในขั้นตอนการสร้าง XMLDISG เพื่อยืนยันความถูกต้องครบถ้วนของข้อมูลที่อยู่ภายใต้ SignedProperties element นี้

1. **xades:SigningTime** คือ element ระบุเวลาลงลายมือชื่อดิจิทัล
2. **xades:SigningCertificate**

2.1 xades:Cert

2.1.1 xades:CertDigest

- 2.1.1.1 xades:DigestMethod เป็น element ระบุ algorithms ที่ใช้ในการทำ Digest Message (Hash value ของ certificate ที่ใช้ลงลายมือชื่อ) โครงการนี้ให้ใช้ Digest Method ในกลุ่ม SHA-2 (SHA-512)
- 2.1.1.2 xades:DigestValue เป็น Digest Message หรือค่า Hash ของ certificate ที่ใช้ลงลายมือชื่อ

2.1.1 xades:CertDigest

- 2.1.2.1 xades:X509IssuesName คือ ระบุชื่อของผู้ออกใบรับรองอิเล็กทรอนิกส์
- 2.1.2.2 xades:X509SerialNumber คือ เลขที่ Serial Number ของใบรับรองอิเล็กทรอนิกส์

ตัวอย่าง ใบกำกับภาษีอิเล็กทรอนิกส์ที่อยู่ในรูปแบบ xml และมีลายมือชื่อดิจิทัลแทรกอยู่ในข้อความ

```
<rsm:TaxInvoice_CrossIndustryInvoice
    xmlns:ram="urn:etda:uncefact:data:standard:TaxInvoice_ReusableAggregateBusinessInformationEntity:2"
    xmlns:rsm="urn:etda:uncefact:data:standard:TaxInvoice_CrossIndustryInvoice:2"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <rsm:ExchangedDocumentContext>
        <ram:GuidelineSpecifiedDocumentContextParameter>
            <ram:ID schemeAgencyID="ETDA" schemeVersionID="v2.0">ER3-2560</ram:ID>
        </ram:GuidelineSpecifiedDocumentContextParameter>
    </rsm:ExchangedDocumentContext>
    <rsm:ExchangedDocument>
        <ram:ID>E0015665457</ram:ID>
        <ram:Name>ใบกำกับภาษี</ram:Name>
        <ram:TypeCode>388</ram:TypeCode>
        <ram:IssueDateTime>2023-06-11T10:24:00.100</ram:IssueDateTime>
        <ram:CreationDateTime>2023-06-11T10:20:04.999</ram:CreationDateTime>
    </rsm:ExchangedDocument>
    <rsm:SupplyChainTradeTransaction>
        <ram:ApplicableHeaderTradeAgreement>
            <ram:SellerTradeParty>
            <ram:Name>บริษัท ทดสอบ จำกัด</ram:Name>
            <ram:SpecifiedTaxRegistration>
                <ram:ID schemeID="TXID">3333333333333000000</ram:ID>
            </ram:SpecifiedTaxRegistration>
            <ram:PostalTradeAddress>
                <ram:PostcodeCode>10310</ram:PostcodeCode>
                <ram:CityName>1017</ram:CityName>
                <ram:CitySubDivisionName>101701</ram:CitySubDivisionName>
                <ram:CountryID schemeID="3166-1 alpha-2">TH</ram:CountryID>
                <ram:CountrySubDivisionID>10</ram:CountrySubDivisionID>
                <ram:BuildingNumber>1234</ram:BuildingNumber>
            </ram:PostalTradeAddress>
        </ram:SellerTradeParty>
        <ram:BuyerTradeParty>
            <ram:Name>นายภาษี เที่ยงตรง</ram:Name>
            <ram:SpecifiedTaxRegistration>
                <ram:ID schemeID="NIDN">1234567890123</ram:ID>
            </ram:SpecifiedTaxRegistration>
            <ram:PostalTradeAddress>
                <ram:PostcodeCode>10330</ram:PostcodeCode>
                <ram:LineThree>จุฬาซอย 10</ram:LineThree>
                <ram:StreetName>พระราม 6</ram:StreetName>
                <ram:CityName>1004</ram:CityName>
                <ram:CitySubDivisionName>100402</ram:CitySubDivisionName>
                <ram:CountryID schemeID="3166-1 alpha-2">TH</ram:CountryID>
                <ram:CountrySubDivisionID>10</ram:CountrySubDivisionID>
                <ram:BuildingNumber>66/999</ram:BuildingNumber>
            </ram:PostalTradeAddress>
        </ram:BuyerTradeParty>
    </ram:ApplicableHeaderTradeAgreement>
    <ram:ApplicableHeaderTradeDelivery>
        <ram:ShipToTradeParty>
            <ram:PostalTradeAddress>
                <ram:PostcodeCode>10330</ram:PostcodeCode>
                <ram:LineThree>จุฬาซอย 10</ram:LineThree>
                <ram:StreetName>พระราม 6</ram:StreetName>
                <ram:CityName>1004</ram:CityName>
                <ram:CitySubDivisionName>100402</ram:CitySubDivisionName>
                <ram:CountryID schemeID="3166-1 alpha-2">TH</ram:CountryID>
                <ram:CountrySubDivisionID>10</ram:CountrySubDivisionID>
                <ram:BuildingNumber>66/999</ram:BuildingNumber>
            </ram:PostalTradeAddress>
        </ram:ShipToTradeParty>
    </ram:ApplicableHeaderTradeDelivery>
    <ram:ApplicableHeaderTradeSettlement>
        <ram:InvoiceCurrencyCode listID="ISO 4217 3A">THB</ram:InvoiceCurrencyCode>
        <ram:ApplicableTradeTax>
            <ram:TypeCode>VAT</ram:TypeCode>
            <ram:CalculatedRate>7</ram:CalculatedRate>
            <ram:BasisAmount>700</ram:BasisAmount>
            <ram:CalculatedAmount currencyID="THB">700</ram:CalculatedAmount>
        </ram:ApplicableTradeTax>
        <ram:SpecifiedTradeAllowanceCharge>
            <ram:ChargeIndicator>false</ram:ChargeIndicator>
            <ram:ActualAmount currencyID="THB">1000</ram:ActualAmount>
            <ram:TypeCode>95</ram:TypeCode>
        </ram:SpecifiedTradeAllowanceCharge>
```

```
            <ram:SpecifiedTradeSettlementHeaderMonetarySummation>
                <ram:LineTotalAmount currencyID="THB">11000</ram:LineTotalAmount>
                <ram:AllowanceTotalAmount currencyID="THB">1000</ram:AllowanceTotalAmount>
                <ram:TaxBasisTotalAmount currencyID="THB">10000</ram:TaxBasisTotalAmount>
                <ram:TaxTotalAmount currencyID="THB">700</ram:TaxTotalAmount>
                <ram:GrandTotalAmount currencyID="THB">10700</ram:GrandTotalAmount>
            </ram:SpecifiedTradeSettlementHeaderMonetarySummation>
        </ram:ApplicableHeaderTradeSettlement>
        <ram:IncludedSupplyChainTradeLineItem>
            <ram:AssociatedDocumentLineDocument>
                <ram:LineID>1</ram:LineID>
            </ram:AssociatedDocumentLineDocument>
            <ram:SpecifiedTradeProduct>
                <ram:ID>8119US</ram:ID>
                <ram:Name>เครื่องฟอกอากาศ</ram:Name>
            </ram:SpecifiedTradeProduct>
            <ram:SpecifiedLineTradeAgreement>
                <ram:GrossPriceProductTradePrice>
                    <ram:ChargeAmount>11000</ram:ChargeAmount>
                </ram:GrossPriceProductTradePrice>
            </ram:SpecifiedLineTradeAgreement>
            <ram:SpecifiedLineTradeDelivery>
                <ram:BilledQuantity unitCode="ชิ้น">1</ram:BilledQuantity>
            </ram:SpecifiedLineTradeDelivery>
            <ram:SpecifiedLineTradeSettlement>
                <ram:SpecifiedTradeSettlementLineMonetarySummation>
                    <ram:NetLineTotalAmount currencyID="THB">11000</ram:NetLineTotalAmount>
                    <ram:NetIncludingTaxesLineTotalAmount currencyID="THB">11000</ram:NetIncludingTaxesLineTotalAmount>
                </ram:SpecifiedTradeSettlementLineMonetarySummation>
            </ram:SpecifiedLineTradeSettlement>
        </ram:IncludedSupplyChainTradeLineItem>
    </rsm:SupplyChainTradeTransaction>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="xmldsig-c827c554-0264-40d2-8aca-a486b40cee21">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"></ds:CanonicalizationMethod>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha512"></ds:SignatureMethod>
            <ds:Reference Id="xmldsig-c827c554-0264-40d2-8aca-a486b40cee21-ref0" URI="">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"></ds:Transform>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></ds:Transform>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha512"></ds:DigestMethod>
                <ds:DigestValue>rAkqKrn0qamf6pGPaN7NSKpCret0g1wWUPfjTdjnrkOtF5usbpO91527n31UGKP9Gz80eAiKUaUQB5RYmo/2Mg==</ds:DigestValue>
            </ds:Reference>
            <ds:Reference Type="http://uri.etsi.org/01903#SignedProperties" URI="#xmldsig-c827c554-0264-40d2-8aca-a486b40cee21-signedprops">
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha512"></ds:DigestMethod>
                <ds:DigestValue>XccuZg85iVBxOHBH+AYmZiCtB8hZAUWuvhy4GVCCDpVdZUXh2maBHBpyR9h9PJPhk3gXrLEZgnGgy3178ouREA==</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue Id="xmldsig-c827c554-0264-40d2-8aca-a486b40cee21-sigvalue">
        HY0WhPIsD5DQYDRdwzWdq2u3EDXFL1IR0aAXLRR7QkIFfH5rPakXyqeADEVbzr0NenofJgKo4JsB
        8chKZFBGRBvX6Lo5perilwSUy6xXfzSXy0+e6yw+z1qatBrZqimBZi5MXTENUwniI4/hLYnlKg63
        Y6J+wedCXkBZDjf6/xsS6Xt9O5q7RB19Sqn1vjpt5smDSMMjbpor0gdX/buxX8Hcg0STZOdhaNpc
        WCSeJT3n5gtCepN4Pqfnn/l8cSQZoIlVeeeM29Zm70BtKbEnWnHrLRBsVj9zqKhuZ1k5D3sFtNbX
        NqQahhMzEIyRj8SiZC6EPNtxbesZajOSB0PCLg==
        </ds:SignatureValue>
        <ds:KeyInfo>
            <ds:X509Data>
                <ds:X509Certificate>
                MIIGzzCCBLegAwIBAgIQXR1ZrpOi3wXWmpzedbX68jANBgkqhkiG9w0BAQ0FADBcMQswCQYDVQQG
                EwJUSDExMC8GA1UECgwoSW50ZXJuZXQgVGhhaWxhbmQgUHVibGljIENvbXBhbnkgTGltaXRlZDEa
                MBgGA1UEAwwRSU5FVCBDQSBUZXN0ICOgRzEwHhcNMjIwOTE5MDgzNjM3WhcNMjQwOTE5MDgzNjM3
                WjCBhjELMAkGA1UEBhMCVEgxXzBdBgNVBAMMVuC4muC4o+C4tOC4qeC4seC41yDguJTguLUg4LmC
                4LiL4Li54LiK4Lix4LmI4LiZIOC4lOC4reC41yDguITguK3guKEg4LiI4Liz4LiB4Lix4LiU
                MRYwFAYDVQRhDA0wMTA1NTYwMDgyNDY0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
                vc91qAseExmmUIprrSQ/3UsBoTsxzIpzOpahHsl24wKLA1OhOy4XcMLUN1R44HhIOlJElFH+KWyW
                568deDMlWPK6yt9tmG+utidxYvChSffcLG4umB42Sd1poVfZ9mF4xQUOOmLonKUV+JgQdbCRnrsO
                HuIGXjd1EL1Dc591ZEzSBQpIMsr8PwzWFpkpX9XweUCQGFxhbJ7uSKyPlvklPfjuETTnJ3gRpaK
                /6TszuRUPgKiaL1Cw81ir8gn2bRKTIpy3k5GaZJG+XVhKGahCP87Gh52dRItPmFrvOa/o9MFG1Be
                J2qt9Sc+0UX+HXCuwHFlgXdtjS+T2BLokJI/IQIDAQABo4ICYDCCAlwwHwYDVR0jBBgwFoAUFY73
                T25hNvPD04eu/KWpECzMbvQwHQYDVR0OBBYEFJRf9StD0d77c3WvAtGaTBbhmnKBMA4GA1UdDwEB
                /wQEAwIGwDCBhgYDVR0gBH8wfTA2BgZghXwBAQEwLDAqBggrBgEFBQcCARYeaHR0cDovL25yY2Eu
                Z28udGgvoHVibGlzaC5odG1sMEMGB2CFfAEBAwEwODA2BggrBgEFBQcCARYqaHR0cHM6Ly9jYS5p
                bmV0LmNvLnRoL2luZXRjYS9kb2N1bWVudC5odG1sMIGYBgNVHR8EgZAwgY0wSKBGoESGQmh0dHA6
                Ly91YXQtY2EuaW51ldC5jby50aC9yZXBvc2l0b3J5L2NybC9pbmV0Y2EvMTAwLTEvcGFydGl0aW9u
                LmNybDBBoD+gPYY7aHR0cDovL3VhdC1jYS5pbmV0LmNvLnRoL3J1cG9zaXRvcnkvY3JsL2luZXRj
                YS9jb21wbGV0ZS5jcmwwgYYGCCsGAQUFBwEBBHoweDBJBggrBgEFBQcwAoY9aHR0cHM6Ly91YXQt
                Y2EuaW51ldC5jby50aC9yZXBvc2l0b3J5L2N1cnRzL01zc3VlZFRvVGhpc0NBLnA3YjArBggrBgEF
                BQcwAYYfaHR0cDovLzIwMy4xNTQuNTkuMTM0L09DU1Avb2NzcDBPBgNVHREESDBGgRNyZHRlc3Rl
                dGF4QHRoYWkuY29tpC8wLTErMCkGA1UEAwwiRCBTT0xVVElPTiBET1QgQ09NIENPTVBBTlkgTElN
                SVRFRDAMBgNVHRMBAf8EAjAAMA0GCSqGSIb3DQEBDQUAA4ICAQCb5KbAXw8819iQMvldrm8plr/6
                Mbf2kPyytJc34pm+kPsnDSg2sBQ4W1tNCKfgn8gQ2tvu1Z0pH7G/KuO4H0CDM/6HGdhVR1Kv0sLG
                hhmDiyrwGcKwaUliYJ83iN2DMCaYgeyxGXIdqf7VBmsJYPN2XhaYlm5d5Z9IBZ9jKQbBcN+b1q5c
                +CfDzPaAW2iJjT6mywlAnEqkkjg7ZZSn2aUqYoyKcohtvbRwotH80T9C6+SBDsZKXn+djtLeKmX1
                M5Uklm+YZvFVuFXV/idG6yUwqagSWuBHijZIZ+11wQ1NponBpgfPVviX650m4cFLAXvISRAvoPS5
                sA/UMdrq/S/mr1TT6i8FJqe6ZLhsoMEBcZQQ0CFehEoRM7aPBdnRsy13dYDc0yJff2eMAnP9sSeR
                dpwXLIB0U/54H54HWjd0Y+daqaU3SSyxmUkZC+u0Z+DBqExhPQn7MiYrlnoQmBJZSstww9RMCx+x
                FX8DxbFzsNDsfYXey7NhssYJTewTyxxI0zQihxd7MHKXAH1trErvQGjo2+YpafF0D2BBzjl/yp3f
                PJOxLS+emEuAvWYZhZ4gvLTZnBImkT4yCsFIdd4Mmuk6FxbHELz4k6lykUh+6F8KFtklUcBQFrb5
                qj5bIpeqFHOQnynbP1hte26/pFlbpZut2oaaWPgS/Uo2x10nXQ==
                </ds:X509Certificate>
            </ds:X509Data>
        </ds:KeyInfo>
```

```
        <ds:Object>
            <xades:QualifyingProperties xmlns:xades="http://uri.etsi.org/01903/v1.3.2#"
                xmlns:xades141="http://uri.etsi.org/01903/v1.4.1#" Target="#xmldsig-c827c554-0264-40d2-8aca-a486b40cee21">
                <xades:SignedProperties Id="xmldsig-c827c554-0264-40d2-8aca-a486b40cee21-signedprops">
                    <xades:SignedSignatureProperties>
                        <xades:SigningTime>2023-06-10T10:26:49.058+07:00</xades:SigningTime>
                        <xades:SigningCertificate>
                            <xades:Cert>
                                <xades:CertDigest>
                                    <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha512"></ds:DigestMethod>
                                    <ds:DigestValue>Gjw1aWtJfFVvhK7e+mEwdRrnD0CzODq4zlS+xd/c00as6yCiq+STBtKU8ytauPQVUl5myS2+7XEaV0QtNTX2Sg==</ds:DigestValue>
                                </xades:CertDigest>
                                <xades:IssuerSerial>
                                    <ds:X509IssuerName>C=TH,O=Thai Digital ID Company Limited,CN=Thai Digital ID CA G3</ds:X509IssuerName>
                                    <ds:X509SerialNumber>123770599182740884283882453659708422898</ds:X509SerialNumber>
                                </xades:IssuerSerial>
                            </xades:Cert>
                        </xades:SigningCertificate>
                    </xades:SignedSignatureProperties>
                </xades:SignedProperties>
            </xades:QualifyingProperties>
        </ds:Object>
    </ds:Signature>
</rsm:TaxInvoice_CrossIndustryInvoice>
```

3 การตรวจสอบความถูกต้องของลายมือชื่อดิจิทัล

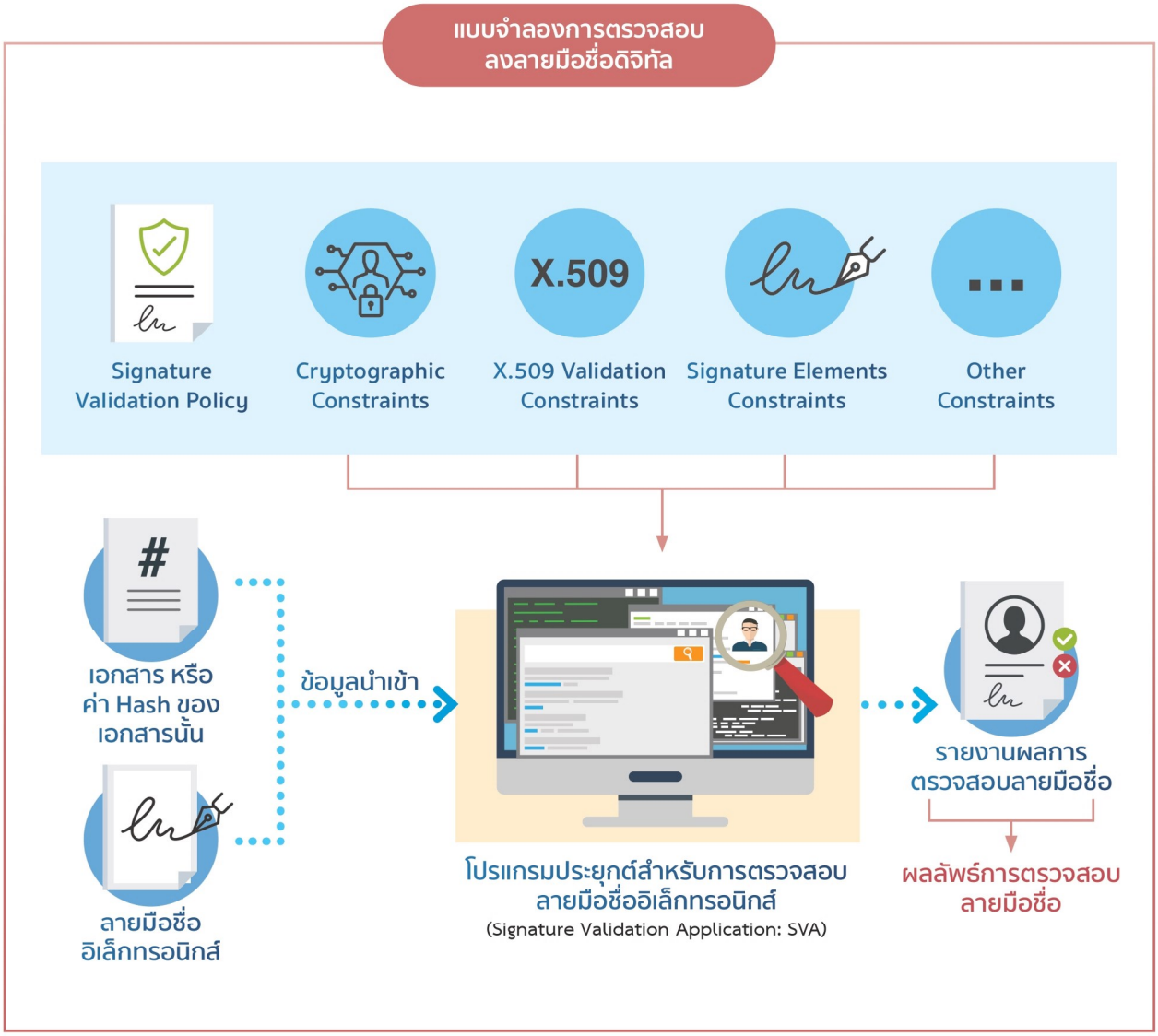
> การตรวจสอบลายมือชื่อดิจิทัล

จำเป็นต้องอาศัยซอฟต์แวร์ในการทำงานซึ่งซอฟต์แวร์ ดังกล่าวต้องมีความสามารถตรวจสอบข้อกำหนดต่างๆ ที่กำหนดในแนวนโยบายในการตรวจสอบลายมือชื่อ (Signature validation policy) ได้แก่

1. **ข้อกำหนดเกี่ยวกับการเข้ารหัสลับ** (Cryptographic Constraints)
2. **ข้อกำหนดในการตรวจสอบรายการข้อมูล** X.509 (X.509 Validation Constraints)
3. **ข้อกำหนดเกี่ยวกับรายการข้อมูลของการลงลายมือชื่อดิจิทัล** (Signature Elements Constraints)
4. **ข้อกำหนดหรือเงื่อนไขอื่นๆ ที่กำหนดขึ้น** (Other กำหนดขึ้น Constraints)

ทั้งนี้ ลักษณะของซอฟต์แวร์ที่ใช้ในการตรวจสอบความถูกต้องลงลายมือชื่อดิจิทัล (Signature Validation Application) อาจจะเป็นไปได้หลายรูปแบบ เช่น

1. โปรแกรมประยุกต์สำหรับใช้งานใน PC
2. Web Service
3. Web Application
4. โปรแกรมในรูปแบบ Command Line
5. Integrated library หรือ Middleware หรือโปรแกรมประยุกต์ในรูปแบบอื่นๆ



รูปที่ 3.1 แบบจำลองการตรวจสอบลายมือชื่อดิจิทัล

ในการตรวจสอบความถูกต้องของลงลายมือชื่อดิจิทัลแบบ XAdES จะให้ผลลัพธ์เป็นสถานะการตรวจสอบความถูกต้องของลายมือชื่อดังต่อไปนี้

- PASSED หมายความว่า ลงลายมือชื่อดิจิทัลถูกต้องตามข้อกำหนดของ Signature Validation Policy
- FAILED หมายความว่า ลงลายมือชื่อดิจิทัลไม่ถูกต้องตามข้อกำหนดของ Signature Validation Policy

เนื่องจากพบว่าข้อมูลที่เกี่ยวกับการเข้ารหัสลับของการลงลายมือชื่อดิจิทัล (รวมถึงค่า Hash ของเอกสาร และค่า Hash ของ object ที่อยู่ภายในการลงลายมือชื่อดิจิทัล) ไม่ถูกต้อง หรือตรวจสอบแล้วพบว่าการลงลายมือชื่อดิจิทัลถูกสร้างขึ้นภายหลังใบรับรองอิเล็กทรอนิกส์ถูกยกเลิกไปแล้ว

ทั้งนี้ การตรวจสอบการลงลายมือชื่อดิจิทัลแบบ XAdES ในแต่ละคลาสมีรายละเอียดที่แตกต่างกันไปตามรายการข้อมูลที่เกี่ยวข้อง และเทคนิคการสร้างที่ได้กล่าวไว้ในหัวข้อ 2. โดยมีรายละเอียดดังต่อไปนี้

การตรวจสอบความถูกต้องลงลายมือชื่อดิจิทัลแบบขั้นต้น (Validation of Basic Signature)

ขั้นตอนตรวจสอบความถูกต้องของลงลายมือชื่อดิจิทัลในหัวข้อนี้กล่าวถึง ความถูกต้องของลายมือชื่อดิจิทัล ข้อมูลนำเข้าสำหรับซอฟต์แวร์ตรวจสอบความถูกต้องของลายมือชื่อ

ข้อมูลนำเข้า	รายละเอียด
ลงลายมือชื่อดิจิทัล (Signature Value)	จำเป็นต้องมี
เอกสารที่ถูกลงลายมือชื่อ hash หรือค่าของเอกสาร	จำเป็นต้องมี
ใบรับรองอิเล็กทรอนิกส์ (Certificate)	จำเป็นต้องมี
Signature Validation Policies	จำเป็นต้องมี
Certificate Validation Data	จำเป็นต้องมี

ผลลัพธ์ที่ได้จากกระบวนการ

ผลของการตรวจสอบความถูกต้องสำหรับลงลายมือชื่อดิจิทัลแบบ Basic Signature เป็น PASSED ก็ต่อเมื่อตรวจสอบกระบวนการด้านล่างแล้วถูกต้องทั้งหมด นอกนั้น FAILED ผลจะได้เป็นกระบวนการตรวจสอบความถูกต้องของลายมือชื่อ

1. ตรวจสอบความถูกต้องของ Format ลงลายมือชื่อดิจิทัล Format เช่น แบบ XAdES Format ของ XMLDSIG เป็นต้น
2. ตรวจสอบความถูกต้องของ Reference ที่ใช้ระบุใบรับรองอิเล็กทรอนิกส์ทั้งหมดในลายมือชื่ออิเล็กทรอนิกส์
3. ตรวจสอบความครบถ้วนขององค์ประกอบที่ใช้ในการตรวจสอบความถูกต้องของลายมือชื่อ ได้แก่ เงื่อนไขการตรวจสอบความถูกต้องของลายมือชื่อ (chain contraints, cryptographic constraints, signature constraints)
4. ตรวจสอบความถูกต้องของ Cryptographic Verification โดยใช้ใบรับรองอิเล็กทรอนิกส์ตรวจสอบกับลายมือชื่อที่ลงไว้ในเอกสาร ในกรณีนี้ ไม่ได้ใช้ใบรับรองอิเล็กทรอนิกส์ทั้งหมดใน Certificate Chain ใช้เพียงใบรับรองอิเล็กทรอนิกส์ของเจ้าของลายมือชื่อเท่านั้น
5. ตรวจสอบความถูกต้องของใบรับรองอิเล็กทรอนิกส์ (X.509Certificate)
   (ก) ตรวจสอบว่าปัจจุบันใบรับรองอิเล็กทรอนิกส์ต้องยังไม่หมดอายุ หรือยังไม่ถูกเพิกถอน
   (ข) ตรวจสอบความถูกต้องของความสัมพันธ์ของใบรับรองอิเล็กทรอนิกส์ใน Certificate Chain และต้องยังไม่หมดอายุ หรือยังไม่ถูกเพิกถอน

4 ข้อเสนอแนะอื่นๆ

- ในการพัฒนาโปรแกรมหรือแอปพลิเคชันสำหรับลงลายมือชื่อดิจิทัลใบกำกับภาษีอิเล็กทรอนิกส์หรือใบรับอิเล็กทรอนิกส์ ผู้พัฒนาฯ ควรศึกษาทฤษฎี และรายการข้อมูลของ XAdES จากเอกสารข้อเสนอแนะฯ ขมธอ.14-2560 หรือ https://www.w3.org/TR/XAdES/ และทำความเข้าใจวิธีการสร้างลายมือชื่อดิจิทัลแบบ XAdES ตามรูปแบบที่กรมสรรพากรกำหนดในคู่มือฉบับนี้

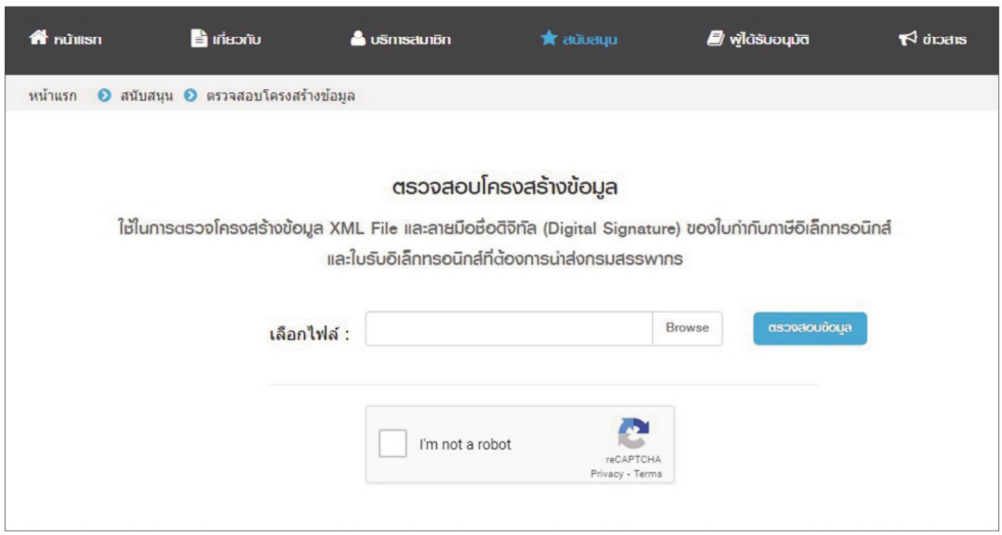
- ข้อมูลสำหรับช่วยในการพัฒนาโปรแกรมลงลายมือชื่อดิจิทัลในรูปแบบ XAdES
  1. เขียนโปรแกรมด้วย JAVA ดูข้อมูลที่ https://github.com/luisgoncalves/xades4j และ https://github.com/ETDA/etax-xades (XAdES signing sample code)
  2. เขียนโปรแกรมด้วย Node JS ดูข้อมูลที่ https://github.com/PeculiarVentures/xadesjs
  3. ข้อมูลสนับสนุนอื่นๆ https://github.com/ETDA/etax-xades

- การเขียนโปรแกรมด้วย JAVA ควรจะมีการระบุค่า NamespaceAware เป็น true เนื่องจากการตรวจสอบโครงสร้างข้อมูล XML และโครงสร้างลายมือชื่อดิจิทัล ต้องมีการระบุข้อมูล Namespace ของ XML ด้วย ตามตัวอย่าง ดังนี้

```
// Document to sign
dbf = DocumentBuilderFactory.newInstance();
dbf.setNamespaceAware(true);
Document doc = dbf.newDocumentBuilder()
```

- ในขั้นตอนการพัฒนาโปรแกรมลงลายมือชื่อดิจิทัล แนะนำให้ผู้ใช้งานขอใบรับรองอิเล็กทรอนิกส์สำหรับทดสอบจากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เพื่อใช้ในการทดสอบสร้างลายมือชื่อดิจิทัล

- ผู้ใช้งานทั่วไปสามารถตรวจสอบโครงสร้างข้อมูล และโครงสร้างลายมือชื่อดิจิทัลของข้อมูลใบกำกับภาษีหรือใบรับในรูปแบบไฟล์ XML ที่อยู่ระหว่างพัฒนาโปรแกรม ได้ที่เว็บไซต์ https://etax.rd.go.th > เมนูสนับสนุน > ตรวจสอบโครงสร้างข้อมูล



เมื่อทำการตรวจสอบไฟล์ XML ระบบจะตรวจสอบความถูกต้องของโครงสร้างข้อมูล XML ตามข้อเสนอแนะมาตฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยข้อความอิเล็กทรอนิกส์สำหรับการซื้อขายสินค้าและบริการ (ขมธอ. 3-2560) และตรวจสอบโครงสร้างลายมือชื่อดิจิทัล (Digital Signature) กรณีข้อมูลไม่ผ่านการตรวจสอบ ระบบจะมีข้อความแจ้งเตือนทันทีที่หน้าจอ ทั้งนี้ผู้ใช้งานสามารถศึกษารายละเอียดเพิ่มเติมได้ที่ คู่มือข้อความตอบกลับโครงสร้างข้อมูล (Response Error)

ข้อสังเกต : กรณีไฟล์ XML ที่จัดทำขึ้นและลงลายมือชื่อดิจิทัลโดยใช้ใบรับรองอิเล็กทรอนิกส์สำหรับทดสอบ เมื่อตรวจสอบโครงสร้างข้อมูลที่เว็บไซต์กรมสรรพากร ระบบจะปรากฏข้อความแจ้งเตือน “ECER : 010 ไม่ผ่านการตรวจสอบ เนื่องจากใบรับรองอิเล็กทรอนิกส์นี้ไม่ถูกรับรองโดยกรมสรรพากร” หมายความว่า วิธีการสร้างลายมือชื่อดิจิทัล แบบ XAdES เป็นไปตามเงื่อนไขที่กำหนดแล้ว เพียงแต่ผู้ใช้งานใช้ใบรับรองอิเล็กทรอนิกส์สำหรับทดสอบ หากใช้ใบรับรองอิเล็กทรอนิกส์สำหรับใช้งานจริงที่มีสถานะพร้อมใช้งาน ในส่วนของลายมือชื่อดิจิทัลจะมีสถานะผ่านการตรวจสอบ

เอกสารอ้างอิง

[1] “ETSI EN 319 102-1 v1.0.0 (2010-12) Electronic Signatures and Infrastructures Procedures for Creation and Validation,” ETSI (Electronic Telecommunications Standard Institute), 2010.

[2] “Schema Location” [ออนไลน์]. Available: http://www.w3.org/TR/2002/REC-xmldsig-core-v20020212/xmldsig-core-schema.xsd

[3] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยข้อความอิเล็กทรอนิกส์สำหรับการซื้อขายสินค้าและบริการ (ขมธอ.3-2560)

[4] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยการใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ระหว่างหน่วยงาน (ขมธอ.14-2560)

E-TAX
INVOICE & RECEIPT

ติดต่อสอบถามได้ที่นี่

1161 RD INTELLIGENCE CENTER
ศูนย์สารนิเทศสรรพากร

02 272 9771
https://etax.rd.go.th
e_taxinvoice@rdservice.rd.go.th