06

การสร้างลายมือชื่อดิจิทัล DIGITAL SIGNATURE

ใบกำกับภาษีอิเล็กทรอนิกส์และใบรับอิเล็กทรอนิกส์ในรูปแบบ XML

(สำหรับนักพัฒนาซอฟต์แวร์)

E-TAX
INVOICE & RECEIPT



กรมสรรพากร
กองบริหารการเสียภาษีทางอิเล็กทรอนิกส์

06

DIGITAL SIGNATURE

การสร้างลายมือชื่อดิจิทัล ใบกำกับภาษีอิเล็กทรอนิกส์และใบรับอิเล็กทรอนิกส์ในรูปแบบ XML

คำนำ

การจัดทำใบกำกับภาษีอิเล็กทรอนิกส์และใบรับอิเล็กทรอนิกส์ (e-Tax Invoice & e-Receipt) ผู้ประกอบการต้องจัดทำใบกำกับภาษี ใบเพิ่มหนี้ ใบลดหนี้ และใบรับ ให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ซึ่งต้องมีการลงลายมือชื่อดิจิทัล (Digital Signature) ที่ข้อมูลอิเล็กทรอนิกส์สร้างขึ้น เพื่อให้ข้อมูลนั้นมีความน่าเชื่อถือ และมีผลผูกพันทางกฎหมาย ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

เอกสารฉบับนี้ จึงได้จัดทำขึ้นเพื่อใช้เป็นแนวทางในการสร้างลายมือชื่อดิจิทัล (Digital Signature) ในรูปแบบ XAdES ที่ใช้ลงลายมือชื่อดิจิทัลสำหรับข้อมูลอิเล็กทรอนิกส์ที่จัดทำขึ้นในรูปแบบ XML File ตามข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ระหว่างหน่วยงานของสำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ (ขมธอ.14-2560) เพื่อให้ผู้ประกอบการสามารถสร้างลายมือชื่อดิจิทัลซึ่งเป็นองค์ประกอบที่สำคัญของการจัดทำใบกำกับภาษีอิเล็กทรอนิกส์และใบรับอิเล็กทรอนิกส์ได้อย่างถูกต้องตามที่กฎหมายกำหนด

กองบริหารการเสียภาษีทางอิเล็กทรอนิกส์
กรมสรรพากร
ธันวาคม 2562

สารบัญ

1. ขั้นตอนการจัดทำและลงลายมือชื่อดิจิทัล ใบกำกับภาษีอิเล็กทรอนิกส์ และใบรับอิเล็กทรอนิกส์ 4

2. การสร้างลายมือชื่อดิจิทัล แบบ XAdES 5
   - 2.1 โครงสร้างและการลงลายมือชื่อดิจิทัล แบบ XAdES 6
   - 2.2 กระบวนการสร้างลายมือชื่อที่ใช้ในโครงการ 10
   - 2.3 คำอธิบายตัวอย่างลายมือชื่อดิจิทัล 13

3. การตรวจสอบความถูกต้องของลายมือชื่อดิจิทัล 18

4. ข้อเสนอแนะอื่นๆ 21

เอกสารอ้างอิง 23

กองบริหารการเสียภาษีทางอิเล็กทรอนิกส์
กรมสรรพากร
90 ซอยพหลโยธิน 7 ถนนพหลโยธิน
แขวงพญาไท เขตพญาไท กรุงเทพฯ 10400

RD Intelligence Center 1161 กด 48

e_taxinvoice@rdserver.rd.go.th

© ขอสงวนสิทธิตามกฎหมาย ห้ามมิให้นำไปตีพิมพ์เป็นหนังสือหรืออื่นใด เพื่อแสวงหาผลประโยชน์ทางพาณิชย์ทั้งทางตรงและทางอ้อมโดยมิได้รับอนุญาต



1 ขั้นตอนการจัดทำและลงลายมือชื่อดิจิทัล

ใบกำกับภาษีอิเล็กทรอนิกส์และใบรับอิเล็กทรอนิกส์

> สำหรับนักพัฒนาซอฟต์แวร์

1 **ศึกษาข้อเสนอแนะ**มาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยข้อความอิเล็กทรอนิกส์สำหรับการซื้อขายสินค้าและบริการ (ขมธอ.3-2560) เวอร์ชัน 2.0

2 **ศึกษาข้อเสนอแนะ**มาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ระหว่างหน่วยงาน (ขมธอ.14-2560) ในส่วนของวิธีการสร้างลายมือชื่อดิจิทัลประกอบกับคู่มือฉบับนี้ ได้แนะนำวิธีการสร้างลายมือชื่อดิจิทัลสำหรับที่ใช้ในโครงการ

3 **พัฒนาระบบ**ของผู้ประกอบการให้สามารถจัดทำข้อมูลใบกำกับภาษีอิเล็กทรอนิกส์และใบรับอิเล็กทรอนิกส์ ให้อยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์ XML File ตามมาตรฐานฯ ว่าด้วยข้อความอิเล็กทรอนิกส์สำหรับการซื้อขายสินค้าและบริการ เวอร์ชัน 2.0 (ขมธอ.3-2560) และพัฒนาโปรแกรมลงลายมือชื่อดิจิทัล (Digital Signature) ที่ใบกำกับภาษีอิเล็กทรอนิกส์และใบรับอิเล็กทรอนิกส์ตามมาตรฐาน XAdES สำหรับนำส่งกรมสรรพากร รวมถึงวิธีการลงลายมือชื่อดิจิทัลอื่นๆ สำหรับเอกสารที่ส่งมอบให้กับผู้ซื้อสินค้าและบริการ

4 **จัดหาใบรับรองอิเล็กทรอนิกส์**จากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certifitcation Authority: CA) ที่มีความน่าเชื่อถือ ภายใต้การรับรองของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์แห่งชาติ (Thailand National Root Certification Authority หรือ Thailand NRCA) และของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

5 **ไฟล์ข้อมูล XML** ที่ได้สร้างขึ้นและลงลายมือชื่อแล้วให้ทำการตรวจสอบโครงสร้างข้อมูล XML และการลงลายมือชื่อดิจิทัล (Digital Signature) ทำได้ 2 วิธี

วิธีที่ 1 ดาวน์โหลดไฟล์สำหรับตรวจสอบโครงสร้างข้อมูล ผ่านเว็บไซต์กรมสรรพากร https://etax.rd.go.th ที่เมนู สนับสนุน > ดาวน์โหลดโปรแกรม และเลือกดาวน์โหลดไฟล์สำหรับตรวจสอบโครงสร้างข้อมูล (Schema & Schematron) โดยนำไฟล์ XML ที่จัดทำขึ้นตรวจสอบกับไฟล์ XML Schema และ Schematron (XSD File และ SCH File) ด้วยโปรแกรม XML Validator Tools เช่น XMLSpy Oxygen xml editor เป็นต้น

วิธีที่ 2 นำไฟล์ XML ที่จัดทำขึ้นตรวจสอบผ่านเว็บไซต์ https://etax.rd.go.th ที่เมนู สนับสนุน เลือก ตรวจสอบโครงสร้างข้อมูล (วิธีนี้ตรวจสอบทั้งโครงสร้าง XML และ Digital Signature)

2 การสร้างลายมือชื่อดิจิทัล
ในรูปแบบ XAdES

> ปัจจุบันเอกสารอิเล็กทรอนิกส์เข้ามามีบทบาทสำคัญและถูกใช้อย่างแพร่หลาย

ในการค้าขายสินค้าระหว่างบริษัท และการทำธุรกรรมต่างๆ ระหว่างหน่วยงาน หรือแม้แต่ภายในหน่วยงานเอง เอกสารอิเล็กทรอนิกส์ก็มีส่วนสำคัญที่จะทำให้หน่วยงานเกิดการพัฒนาและทำงานไปได้อย่างราบรื่น อย่างไรก็ตาม สิ่งสำคัญที่ควรคำนึงถึง คือ การมีกลไกในการดูแลรักษาความมั่นคงปลอดภัยของข้อมูลในเอกสารอิเล็กทรอนิกส์ที่เหมาะสม เพื่อผู้ใช้งานมีความเชื่อมั่นและเอกสารอิเล็กทรอนิกส์เองมีความน่าเชื่อถือ ทั้งนี้ เทคนิคที่ใช้ในการรักษาความถูกต้องครบถ้วน รวมถึงใช้ในการพิสูจน์ตัวตนของผู้ลงลายมือชื่อได้ คือ การใช้ลายมือชื่ออิเล็กทรอนิกส์ หรือลายมือชื่อดิจิทัล

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

1 XML
Advanced Electronic Signatures (XAdES)



ใช้ลงลายมือชื่อดิจิทัลสำหรับไฟล์แบบ XML

2 PDF
Advanced Electronic Signatures (PAdES)



ใช้ลงลายมือชื่อดิจิทัลสำหรับไฟล์แบบ PDF

3 CMS
Advanced Electronic Signatures (CAdES)



ใช้ลงลายมือชื่อดิจิทัลสำหรับไฟล์แบบอื่นๆ

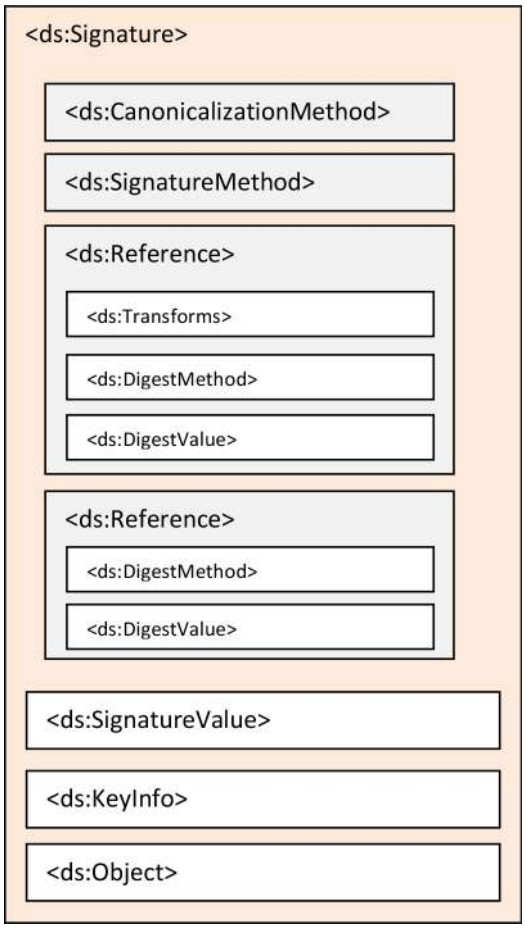
นอกเหนือจากที่ลงลายมือชื่อดิจิทัลแบบ AdES สามารถตรวจสอบความถูกต้องครบถ้วนของข้อมูลในเอกสาร และสามารถระบุตัวตนของผู้ลงลายมือชื่อได้แล้ว ยังเพิ่มกลไกและรายการข้อมูลเพิ่มเติม ลงในลายมือชื่อดิจิทัล เช่น เวลาในการลงลายมือชื่อ ข้อมูลที่จะใช้ในการตรวจสอบลายมือชื่อ และจัดเก็บเอกสารในระยะยาว เป็นต้น

การจัดทำใบกำกับภาษีอิเล็กทรอนิกส์และใบรับอิเล็กทรอนิกส์ ที่กรมสรรพากรกำหนดจะแยกการลงลายมือชื่อออกเป็น 2 ส่วนคือ

1. การลงลายมือชื่อใบกำกับภาษีอิเล็กทรอนิกส์และใบรับอิเล็กทรอนิกส์ เพื่อส่งมอบให้ผู้ซื้อสินค้าหรือผู้รับบริการ ซึ่งวิธีการลงลายมือชื่อดิจิทัลจะขึ้นอยู่กับประเภทเอกสารอิเล็กทรอนิกส์ที่ผู้ประกอบการจัดทำขึ้น
2. การลงลายมือชื่อในข้อมูลอิเล็กทรอนิกส์ในรูปแบบ XML File (ขมธอ. 3-2560) ที่นำส่งข้อมูลให้กรมสรรพากร

การสร้างเอกสารอิเล็กทรอนิกส์เพื่อใช้ รับ-ส่งข้อมูล XML File จะใช้รูปแบบของลายมือชื่อดิจิทัลแบบ XAdES โดยสิ่งที่ได้จากการลงลายมือชื่อดิจิทัลในรูปแบบ XML จะมีข้อมูลที่เกี่ยวกับการลงลายมือชื่อต่อไปนี้

2.1 โครงสร้างและการลงลายมือชื่อดิจิทัล แบบ XAdES ที่ใช้ในโครงการ



รูปที่ 2.1 โครงสร้างการลงลายมือชื่อดิจิทัลแบบ XMLDSIG

1 **SignedInfo element** ประกอบด้วยข้อมูล algorithms หรือขั้นตอนในการลงลายมือชื่ออิเล็กทรอนิกส์ในชื่อเอกสาร ประกอบด้วย

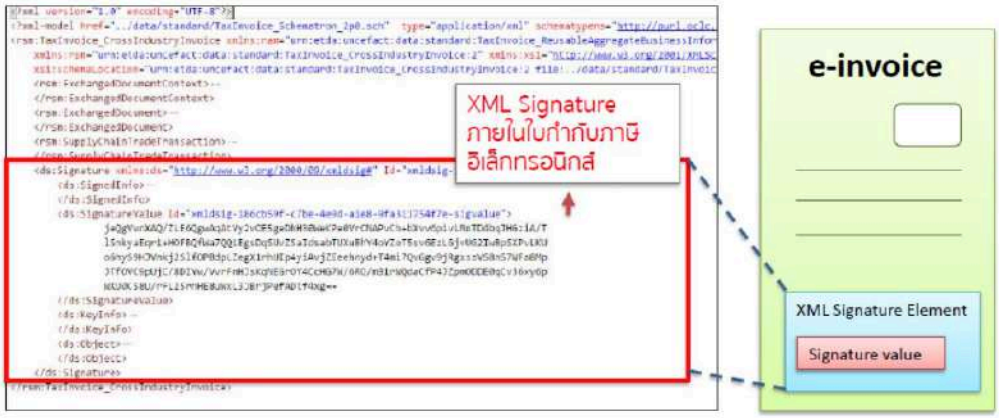
1.1 Canonicalization Method หรือขั้นตอนการจัดโครงสร้างของ XML ก่อนทำการลงลายมือชื่อ โดย W3C กำหนดให้ XML-C14N (http://www.w3.org/TR/2001/REC-xml-c14n-20010315) สำหรับ Canonical XML 1.0 และ XML-C14N11 สำหรับ Canonical XML 1.1 (http://www.w3.org/2006/12/xml-c14n11)

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



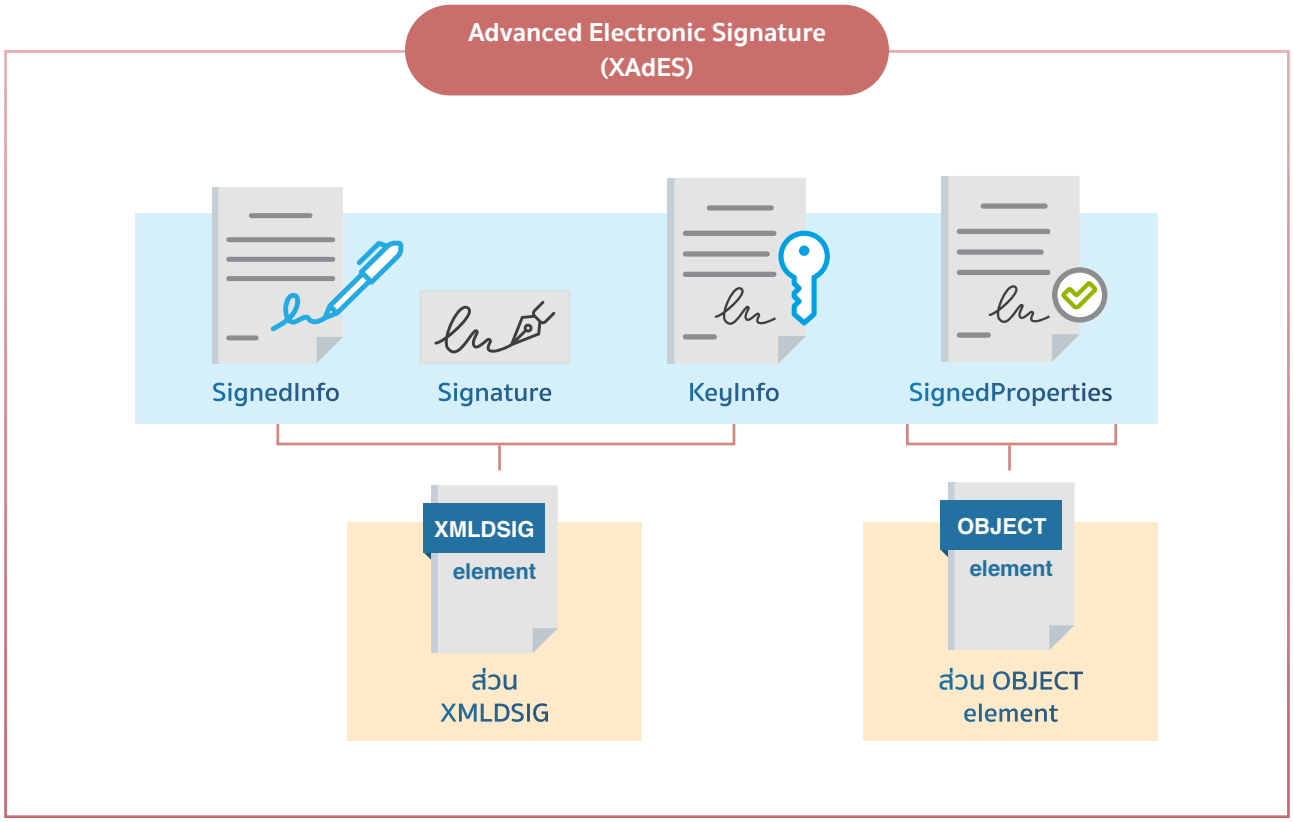
รูปที่ 2.2 Digital Signature จะแทรกอยู่ในข้อความภายใต้ root element

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

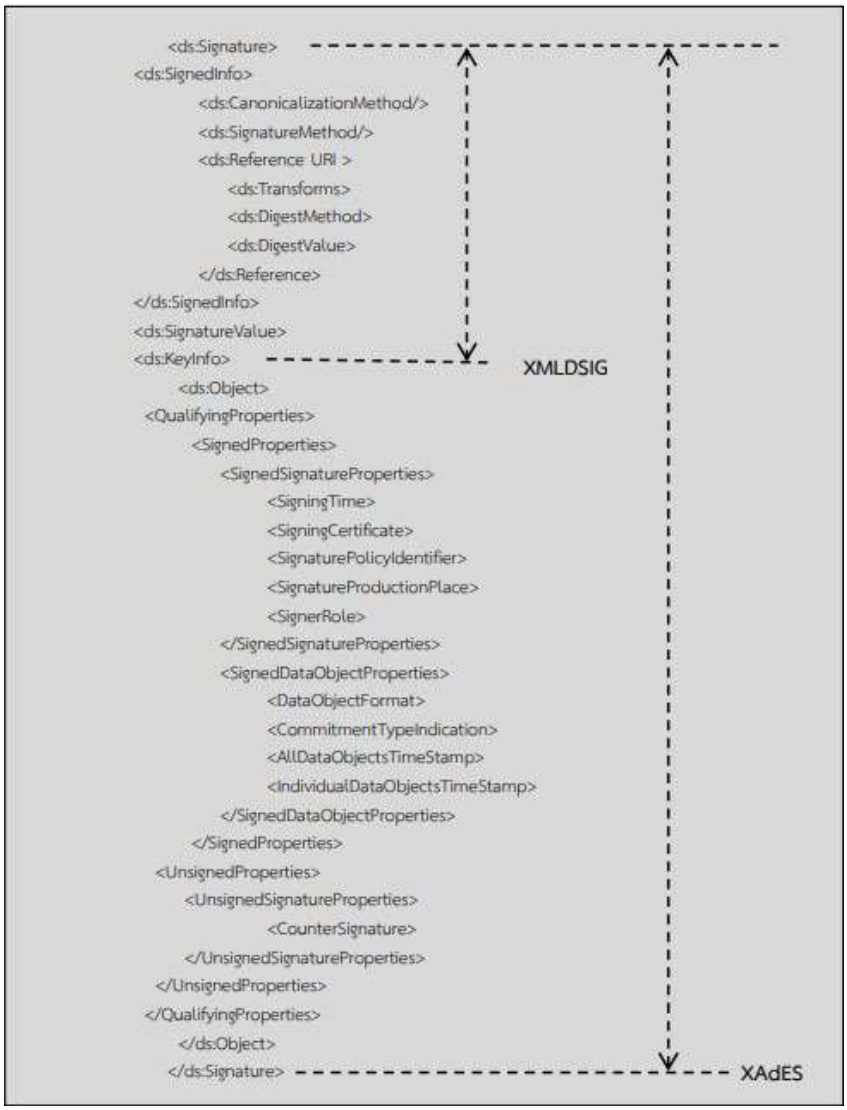
3 **KeyInfo** ให้ข้อมูลใบรับรองอิเล็กทรอนิกส์ของผู้ลงลายมือชื่อ X509 SubjectName ประกอบด้วย element ซึ่งระบุ Distinguished Name ของเจ้าของใบรับรองอิเล็กทรอนิกส์ X509 และ Certificate ระบุ Certificate ถูกเข้ารหัสแบบ Base 64



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

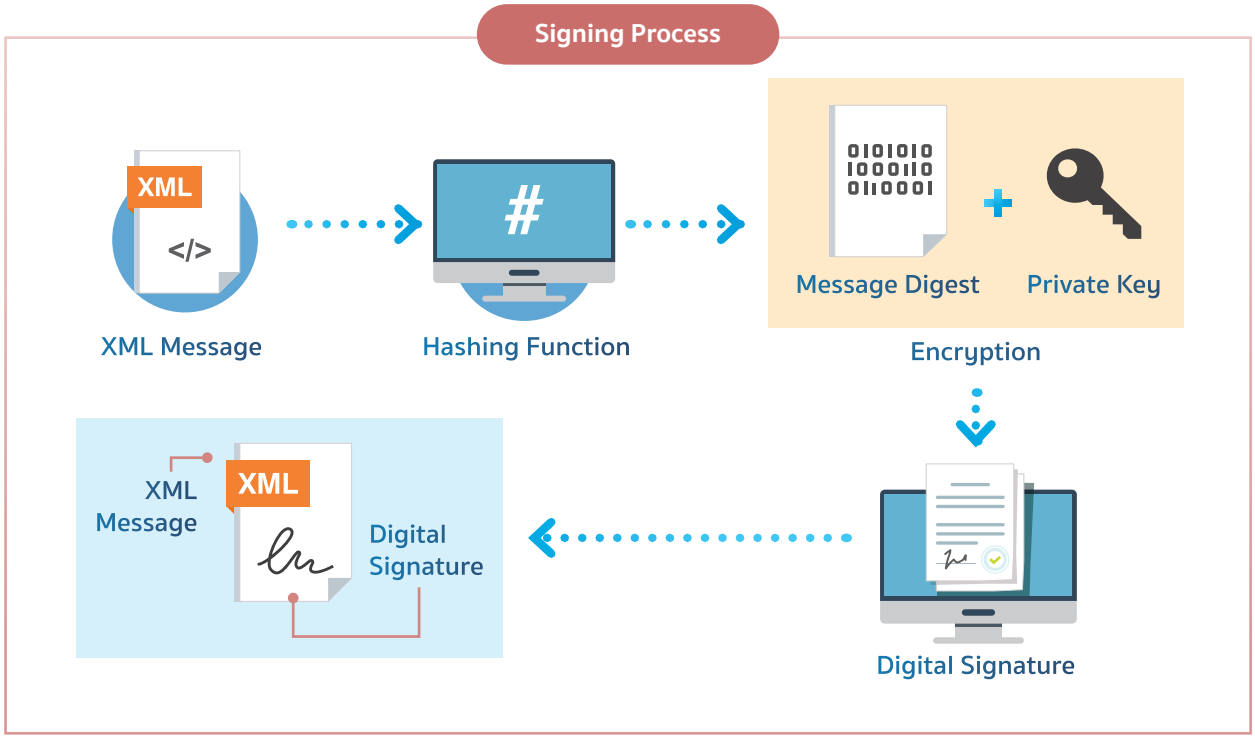
ข้อมูลนำเข้า	จำเป็น/ ไม่ใช้
เอกสารอิเล็กทรอนิกส์ (Document)	จำเป็นต้องมี
ใบรับรองอิเล็กทรอนิกส์ของเจ้าของลายมือชื่อ (Certificate)	จำเป็นต้องมี
รายการข้อมูลของลงลายมือชื่อดิจิทัล (Signature Attributes)	จำเป็นต้องมี

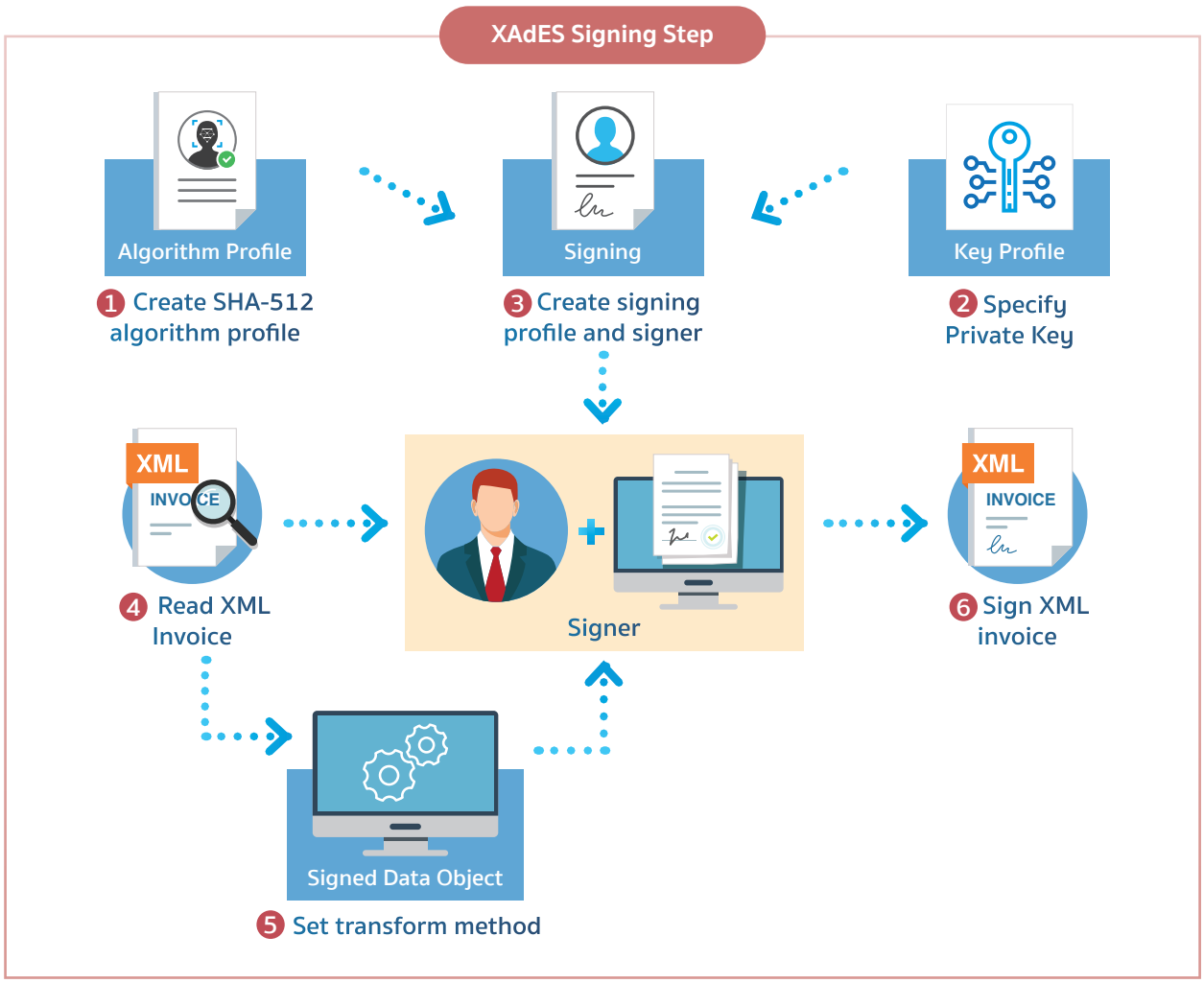
ค่ากำหนดของซอฟต์แวร์

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

2.2 กระบวนการในการสร้างลายมือชื่อดิจิทัลที่ใช้ในโครงการ

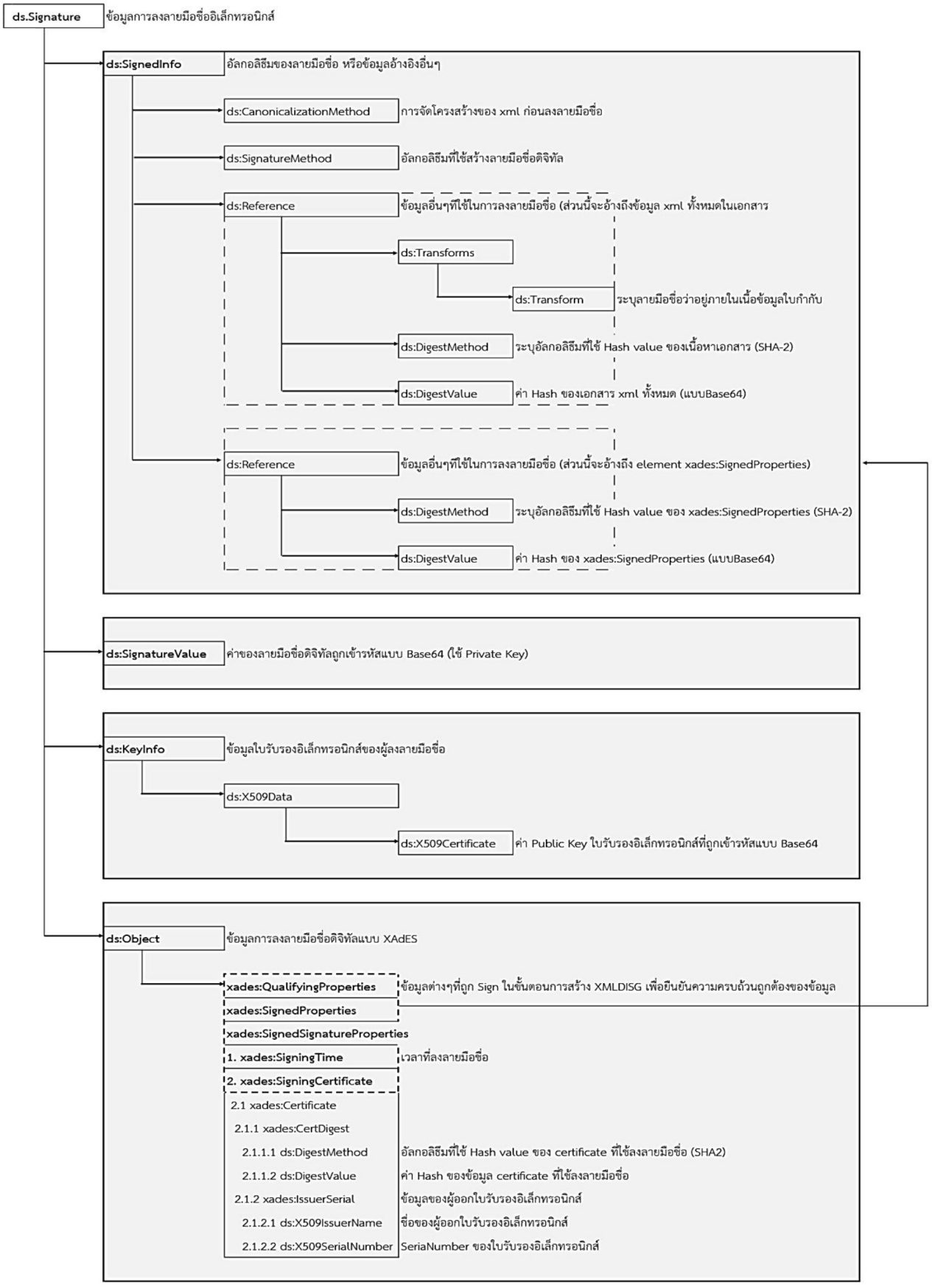
1. จัดหาหรือพัฒนาซอฟต์แวร์ที่ใช้ลงลายมือชื่อ จะต้องมีความสามารถในการให้ผู้ใช้งานสามารถลงลายมือชื่อดิจิทัลกำกับทั้งเอกสาร ซึ่งในโครงการนี้ใช้รูปแบบการลงลายชื่อดิจิทัลทั้งเอกสาร
2. นำข้อมูล XML มาทำขั้นตอนการจัดโครงสร้างของ XML (Canonicalization Method) อ้างอิงจากเว็บไซต์ https://www.w3.org/TR/xml-c14n/
3. กำหนดฟอร์แมตของการลงลายมือชื่อดิจิทัลแบบ XAdES คลาสของการลงลายมือชื่อดิจิทัล BasicSignature และรูปแบบของการลงลายมือชื่อเป็น Enveloped
4. ในกระบวนการที่ใช้ในการลงลายมือชื่อต้องมีกลไกในการแจ้งเตือนผู้ใช้งานว่าจะมีการลงลายมือชื่อเพื่อใช้ในการรับการยินยอม (Consent) จากเจ้าของลายมือชื่อ
5. กระบวนการจะทำการสร้างลายมือชื่อต้องตรวจสอบใบรับรองอิเล็กทรอนิกส์ของเจ้าของลายมือชื่อก่อนว่ายังไม่ถูกเพิกถอนหรือหมดอายุ
6. ในการลงลายมือชื่ออาจมีกระบวนการตรวจสอบตัวตนของผู้ลงลายมือชื่อด้วย เช่น การขอให้ผู้ลงลายมือชื่อ ระบุรหัสผ่าน (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

1 **ds:Signature** คือ Element ข้อมูลของการลงลายมือชื่อดิจิทัล

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

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

1.1.2 ds:SignatureMethod คือ element ที่จัดเก็บ Algorithms SHA-512 ที่ใช้ในการลงลายมือชื่อ

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

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

1.1.4 ds:Reference คือข้อมูลที่ใช้ในการลงลายมือชื่อดิจิทัล ซึ่ง element นี้อ้างอิงถึงข้อมูล element xades:SignedProperties ในเอกสารนี้

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

- **1.1.4.1 ds:DigestMethod** เป็น element ระบุ algorithms ที่ใช้ในการทำ Digest Message (Hash value ของข้อมูล element xades:SignedProperties) โครงการนี้ให้ใช้ Digest Method ในกลุ่ม SHA-2 (SHA-512)
- **1.1.4.2 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

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

1.3 ds:KeyInfo คือ element ข้อมูลใบรับรองอิเล็กทรอนิกส์ของผู้ลงลายมือชื่อ

1.3.1 ds:X509Data

1.1.3.1 ds:Transforms คือ element ที่กำหนดว่า XMLDSIG อยู่ในรูปแบบไหน ซึ่งในโครงการใช้รูปแบบ Enveloped คือ XMLDSIG อยู่ในเนื้อข้อมูลเอกสาร XML

1.4 ds:Object คือ element ระบุข้อมูลของการลงลายมือชื่ออิเล็กทรอนิกส์แบบ XAdES

1.4.1 xades:QualifyingProperties คือ ระบุข้อมูลรูปแบบการลงลายมือชื่ออิเล็กทรอนิกส์ของ XAdES ซึ่งโครงการจะเป็นรูปแบบ Signed Properties

1.4.1.1 xades:SignedProperties คือ element ต่างๆ ที่จะถูก sign ในขั้นตอนการสร้าง XMLDISG เพื่อยืนยันความถูกต้องครบถ้วนของข้อมูลที่อยู่ภายใต้ SignedProperties element นี้

1. xades:SigningTime คือ element ระบุเวลาลงลายมือชื่อดิจิทัล
2. xades:SigninfCertificate

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"
    xsi:schemaLocation="urn:etda:uncefact:data:standard:TaxInvoice_CrossIndustryInvoice:2
    file:../data/standard/TaxInvoice_CrossIndustryInvoice_2p0.xsd">
    <rsm:ExchangedDocumentContext>
        <ram:GuidelineSpecifiedDocumentContextParameter>
            <ram:ID schemeAgencyID="ETDA" schemeVersionID="v1.0">ER3-2558</ram:ID>
        </ram:GuidelineSpecifiedDocumentContextParameter>
    </rsm:ExchangedDocumentContext>
    <rsm:ExchangedDocument>
        <ram:ID>RDTIV60060000002</ram:ID>
        <ram:Name>ใบเสร็จรับเงิน/ใบกำกับภาษี</ram:Name>
        <ram:TypeCode>T03</ram:TypeCode>
        <ram:IssueDateTime>2017-06-26T09:53:44.0</ram:IssueDateTime>
        <ram:CreationDateTime>2017-06-26T09:53:44.0</ram:CreationDateTime>
    </rsm:ExchangedDocument>
    <rsm:SupplyChainTradeTransaction>
        <ram:ApplicableHeaderTradeAgreement>
            <ram:SellerTradeParty>
                <ram:Name> บริษัท ตัวอย่าง (มหาชน)</ram:Name>
                <ram:SpecifiedTaxRegistration>
                    <ram:ID schemeAgencyID="RD" schemeID="TXID">0107557000101000000</ram:ID>
                </ram:SpecifiedTaxRegistration>
                <ram:DefinedTradeContact>
                    <ram:EmailURIUniversalCommunication>
                        <ram:URIID>test55555@gmail.com</ram:URIID>
                    </ram:EmailURIUniversalCommunication>
                    <ram:TelephoneUniversalCommunication>
                        <ram:CompleteNumber>+66-261230000</ram:CompleteNumber>
                    </ram:TelephoneUniversalCommunication>
                </ram:DefinedTradeContact>
                <ram:PostalTradeAddress>
                    <ram:PostcodeCode>10330</ram:PostcodeCode>
                    <ram:StreetName>พระรามที่6</ram:StreetName>
                    <ram:CityName>1007</ram:CityName>
                    <ram:CitySubDivisionName>100702</ram:CitySubDivisionName>
                    <ram:CountryID schemeID="3166-1 alpha-2">TH</ram:CountryID>
                    <ram:CountrySubDivisionID>10</ram:CountrySubDivisionID>
                    <ram:BuildingNumber>719/5,8-9</ram:BuildingNumber>
                </ram:PostalTradeAddress>
            </ram:SellerTradeParty>
            <ram:BuyerTradeParty>
                <ram:Name>สมชาย ใจดี</ram:Name>
                <ram:SpecifiedTaxRegistration>
                    <ram:ID schemeID="NIDN" schemeName="Tax Registration Number"
                        >1234567890123</ram:ID>
                </ram:SpecifiedTaxRegistration>
                <ram:PostalTradeAddress>
                    <ram:PostcodeCode>10330</ram:PostcodeCode>
                    <ram:StreetName>บรรทัดทอง</ram:StreetName>
                    <ram:CityName>1018</ram:CityName>
                    <ram:CitySubDivisionName>101804</ram:CitySubDivisionName>
                    <ram:CountryID schemeID="3166-1 alpha-2">TH</ram:CountryID>
                    <ram:CountrySubDivisionID>10</ram:CountrySubDivisionID>
                    <ram:BuildingNumber>48</ram:BuildingNumber>
                </ram:PostalTradeAddress>
            </ram:BuyerTradeParty>
        </ram:ApplicableHeaderTradeAgreement>
        <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>1200</ram:BasisAmount>
                <ram:CalculatedAmount>84</ram:CalculatedAmount>
            </ram:ApplicableTradeTax>
            <ram:SpecifiedTradeSettlementHeaderMonetarySummation>
                <ram:LineTotalAmount>1200</ram:LineTotalAmount>
                <ram:TaxBasisTotalAmount>1200</ram:TaxBasisTotalAmount>
                <ram:TaxTotalAmount>84</ram:TaxTotalAmount>
                <ram:GrandTotalAmount>1284</ram:GrandTotalAmount>
```

```
        </ram:SpecifiedTradeSettlementHeaderMonetarySummation>
    </ram:ApplicableHeaderTradeSettlement>
    <ram:IncludedSupplyChainTradeLineItem>
        <ram:AssociatedDocumentLineDocument>
            <ram:LineID>1</ram:LineID>
        </ram:AssociatedDocumentLineDocument>
        <ram:SpecifiedTradeProduct>
            <ram:ID>0001</ram:ID>
            <ram:Name>ผ้า</ram:Name>
        </ram:SpecifiedTradeProduct>
        <ram:SpecifiedLineTradeAgreement>
            <ram:GrossPriceProductTradePrice>
                <ram:ChargeAmount>100</ram:ChargeAmount>
            </ram:GrossPriceProductTradePrice>
        </ram:SpecifiedLineTradeAgreement>
        <ram:SpecifiedLineTradeDelivery>
            <ram:BilledQuantity unitCode="VLT">12</ram:BilledQuantity>
        </ram:SpecifiedLineTradeDelivery>
        <ram:SpecifiedLineTradeSettlement>
            <ram:SpecifiedTradeSettlementLineMonetarySummation>
                <ram:NetLineTotalAmount currencyID="THB">1200</ram:NetLineTotalAmount>
                <ram:NetIncludingTaxesLineTotalAmount currencyID="THB"
                    >1200</ram:NetIncludingTaxesLineTotalAmount>
            </ram:SpecifiedTradeSettlementLineMonetarySummation>
        </ram:SpecifiedLineTradeSettlement>
    </ram:IncludedSupplyChainTradeLineItem>
</rsm:SupplyChainTradeTransaction>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    Id="xmldsig-522d79b4-afac-421e-a47d-5df812053914">
    <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
        <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha512"/>
        <ds:Reference Id="xmldsig-522d79b4-afac-421e-a47d-5df812053914-ref0" URI="">
            <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"
                />
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha512"/>
            <ds:DigestValue>ECRMSeFxft9+/Qp/S0TBGwLPAx8vOF/Y6wMVyQaQvUG+Sz2wTNlmT+rBWNBuT4SocZqenNMal4OV
                SvNspV1y6g==</ds:DigestValue>
        </ds:Reference>
        <ds:Reference Type="http://uri.etsi.org/01903#SignedProperties"
            URI="#xmldsig-522d79b4-afac-421e-a47d-5df812053914-signedprops">
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha512"/>
            <ds:DigestValue>O5cEsbssGVoXkDhSAsoD7lHqr/ufsfxtIsDFj7Orp/yze4u9keNu9089SYSF/ETyw+ar8aFUFQTA
                C2fSzE04pw==</ds:DigestValue>
        </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue Id="xmldsig-522d79b4-afac-421e-a47d-5df812053914-sigvalue">
        Z5Q9TOTYGyNyAzrJfdoP2fGiK0Qkna5Ru0wQkfpAyVM9bJt+Au11Cu14R39xzih4eqZxGXsi5v1X
        nvrKFLR3wE/iNosIhMAjPW+PYvlbCmokhZffsWMDJGEuwyKsOWp0vxPgImhVEFOKVtTwHz7NctpV
        yOKjVzETOf1VpqPb/SiO7PArQbA3DaOU9aROELHSp1ipX9OWLr4qd+IGInW95Tb3tWvvZ3JEz7Ai
        71W0oEAnDuCOrv2oKP1C1N3+5wO5K0hy6qiN3F974BWiH/BlE1Ih/4C1Ksr5lLX8GuzYAl6P7ImZ
        0RZJhbB7b5EwZTwzqqXzHcHUEq9mofWykJMr2Q== </ds:SignatureValue>
    <ds:KeyInfo>
        <ds:X509Data>
            <ds:X509Certificate>
                MIIIFjCCBf6gAwIBAgIIU2lPz/hOgHAwDQYJKoZIhvcNAQELBQAwXDEjMCEGA1UEAwwaVGhhaSBE
                aWdpdGFsIElEIENBIEczIHRlc3QxKDAmBgNVBAoMH1RoYWkgRGlnaXRhbCBJRCBDb21wYW55IExp
                bWl0ZWQxCzAJBgNVBAYTAlRIMB4XDTE3MDYyMTA0NTIyMVoXDTE4MDYyMTA0NTIyMVowfDELMAkG
                A1UEBhMCVEgxFjAUBgNVBGEMDTAxMDc1NTcwMDAxMDExVTBTBgNVBAMMTOC4muC4o+C4tOC4qeC4
                seC4lyDguYDguJnguYfguJXguYDguJrguKLguYwg4LiI4Liz4LiB4Lix4LiUKOC4oeC4q+C4suC4
                iuC4mSkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDAoO2tpEA8fnDeti6IRZ5yyBpG
                ihbTHj+Ip0lcFP8QC3/1v2oVw3b2XTMdpDqKbip6ie/0ajDM+Gyd7K19CJYZP5qZrfzeo8AJeEly
                w8/bNG5coN9b82j8S0rSZX2wQir8HYf4+45xr2n04i07vCvDPhvV4f4bvRjVHmXo1LGLuCs1bYI1
                2vTPPlyiDGkpTrk5Xd+RnyeirLMZlCwYedCstrmkuw2zZjRw3kKRVIsCG/RCA4B0sZA2boPG2jKz
                eXqdKeJyL8SqvGsyeEcKA9JPBJ0EPbyLY0TAtO/YdmaT+ghXym26Ei6M2nX8nHKcAbwLrjUJeIJq
                AAuKGkg3KjgZAgMBAAGjggO6MIIDtjCCAQwGCCsGAQUFBwEBBIH/MIH8MIG0BggrBgEFBQcwAoaB
                p2h0dHA6Ly8yMDMuMTU1LjE1Ni4yMjM6ODA4MC9lamJjYS9wdWJsaWN3ZWIvd2ViZGlzdC9jZXJ0
                ZGlzdD9jbWQ9aWVjYWNlcnQmaXNzdWVyPUNOJTNkVGhhaStEaWdpdGFsK0lEK0NBK0czK3Rlc3Ql
                MmNPJTNkVGhhaStEaWdpdGFsK0lEK0NvbXBhbnkrTGltaXRlZCUyY0MlM2RUSCZsZXZlbD0wMEMG
                CCsGAQUFBzABhjdodHRwOi8vMjAzLjE1NS4xNTYuMjIzOjgwODAvZWpiY2EvcHVibGljd2ViL3N0
                YXR1cy9vY3NwMB0GA1UdDgQWBBSRQhwRwDPG6GcNCIye7lTXjz62eTAMBgNVHRMBAf8EAjAAMB8G
```

```
                    A1UdIwQYMBaAFM3evfn1cLW16fXOqHEpBJD1NcnZMIG+BgNVHS4EgbYwgbMwgbCgga2ggaqGgado
                    dHRwOi8vMjAzLjE1NS4xNTYuMjIzOjgwODAvZWpiY2EvcHVibGljd2ViL3dlYmRpc3QvY2VydGRp
                    c3Q/Y21kPWRlbHRhY3JsJmlzc3Vlcj1DTj1UaGFpJTIwRGlnaXRhbCUyMElEJTIwQ0ElMjBHMyUy
                    MHRlc3QsTz1UaGFpJTIwRGlnaXRhbCUyMElEJTIwQ29tcGFueSUyMExpbWl0ZWQsQz1USDAXBgNV
                    HSAEEDAOMAwGCmCFfAEBAgHOEQEwggEeBgNVHR8EggEVMIIBETCCAQ2ggaiggaWGgaJodHRwOi8v
                    MjAzLjE1NS4xNTYuMjIzOjgwODAvZWpiY2EvcHVibGljd2ViL3dlYmRpc3QvY2VydGRpc3Q/Y21k
                    PWNybCZpc3N1ZXI9Q049VGhhaSUyMERpZZl0YWwlMjBJRCUyMENBJTIwRzMlMjB0ZXN0LE89VGhh
                    aSUyMERpZZl0YWwlMj8JRCUyMENvbXBhbnklMjBMaW1pdGVkLEM9VEiiYKReMFwxIzAhBgNVBAMM
                    GlRoYWkgRGlnaXRhbCBJRCBDQSBHMyB0ZXN0MSgwJgYDVQQKDB9UaGFpIERpZZl0YWwgSUQgQ29t
                    cGFueSBMaW1pdGVkMQswCQYDVQQGEwJUSDAOBgNVHQ8BAf8EBAMCBeAwSgYDVR0RBEMwQYETbmVh
                    Yi5uYjAyQGdtYWlsLmNvbaQqMCgxJjAkBgNVBAMMHU5ldGJheSBQdWJsaWMgQ29tcGFueSBMaW1p
                    dGVkMA0GCSqGSIb3DQEBCwUAA4ICAQB73lybVheJQq4t87ku8rh7YKQfUW+9n8qvqQIO6J+Ose10
                    s2dIIZH7WV2VifnI4nVIq8yX6KiC7EoF52oZ8SkCbWz9/VFAy2XpDVDwQMr9b9HdMRHok8pZ0kcv
                    LB3tqhWJa8SMBVrSI6HCy67DYTS3rUmCkAYSo4a4WGlj8QQOYbfrGkLPxZrhqFH4IIMWDlF7NgJp
                    zXZPp2HCZ61w3pRvSbnHL9rM++i7JkMIro3xGWWSZkb//3IKYpT/gpMZHvoL2DdfSFqFQBiPAGNV
                    bmzsLnLuAChaIdMUbBkvK4W+d4jI2XdfXGKKi/9/R5by63+Sgl88NciRDTnqgIp8lI0OuM55twIl
                    4o+G8mC1ZV3ZpkkLTh0Rxz0WU53xJf99ayb5C9YjlhmaW7nCXoKLSMWPZyskBbk+XAxqh+4LDpWP
                    EEOcMiOLLN56/rxHIGOS7vq6qFlXGJLm19ZmWoJAwb/K3UO5pJIRAzm1ZxCbRE4GX9r6HLYpf8Ff
                    F0IUj4VAoYcxpc9a9bTbX0EkaJXLaUwhJ25mccxoaKcjCwGM6Jpntf6jBYcsT2nV2LocMMizxOC+
                    xT/Cw4RXPFnP+oZ+wb4xG7GbZUpMYj6qpjps79QR40Ejag9eLQKTZ8D6mZxO1YW6E+t3MsBzphcs
                    Jtb4nQ+S7bBl/lDcHAZhbZJYlpe/WQ== </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-522d79b4-afac-421e-a47d-5df812053914">
                <xades:SignedProperties
                    Id="xmldsig-522d79b4-afac-421e-a47d-5df812053914-signedprops">
                    <xades:SignedSignatureProperties>
                        <xades:SigningTime>2017-06-26T09:52:17.474+07:00</xades:SigningTime>
                        <xades:SigningCertificate>
                            <xades:Cert>
                                <xades:CertDigest>
                                    <ds:DigestMethod
                                        Algorithm="http://www.w3.org/2001/04/xmlenc#sha512"/>
                                    <ds:DigestValue>x5081U7KRT5H800A1ioD+OPjB1pRpI93/CZr3kKIkszoLg/TztQG9lr5B62u/zT8z3g1l
                                        WAToUgsxTg==</ds:DigestValue>
                                </xades:CertDigest>
                                <xades:IssuerSerial>
                                    <ds:X509IssuerName>C=TH,O=Thai Digital ID Company
                                        Limited,CN=Thai Digital ID CA G3 test</ds:X509IssuerName>
                                    <ds:X509SerialNumber>6010422932345356400</ds:X509SerialNumber>
                                </xades:IssuerSerial>
                            </xades:Cert>
                        </xades:SigningCertificate>
                    </xades:SignedSignatureProperties>
                </xades:SignedProperties>
            </xades:QualifyingProperties>
        </ds:Object>
    </ds:Signature>
</rsm:TaxInvoice_CrossIndustryInvoice>
```

3 การตรวจสอบความถูกต้องของลายมือชื่อดิจิทัล

> การตรวจสอบลายมือชื่อดิจิทัล

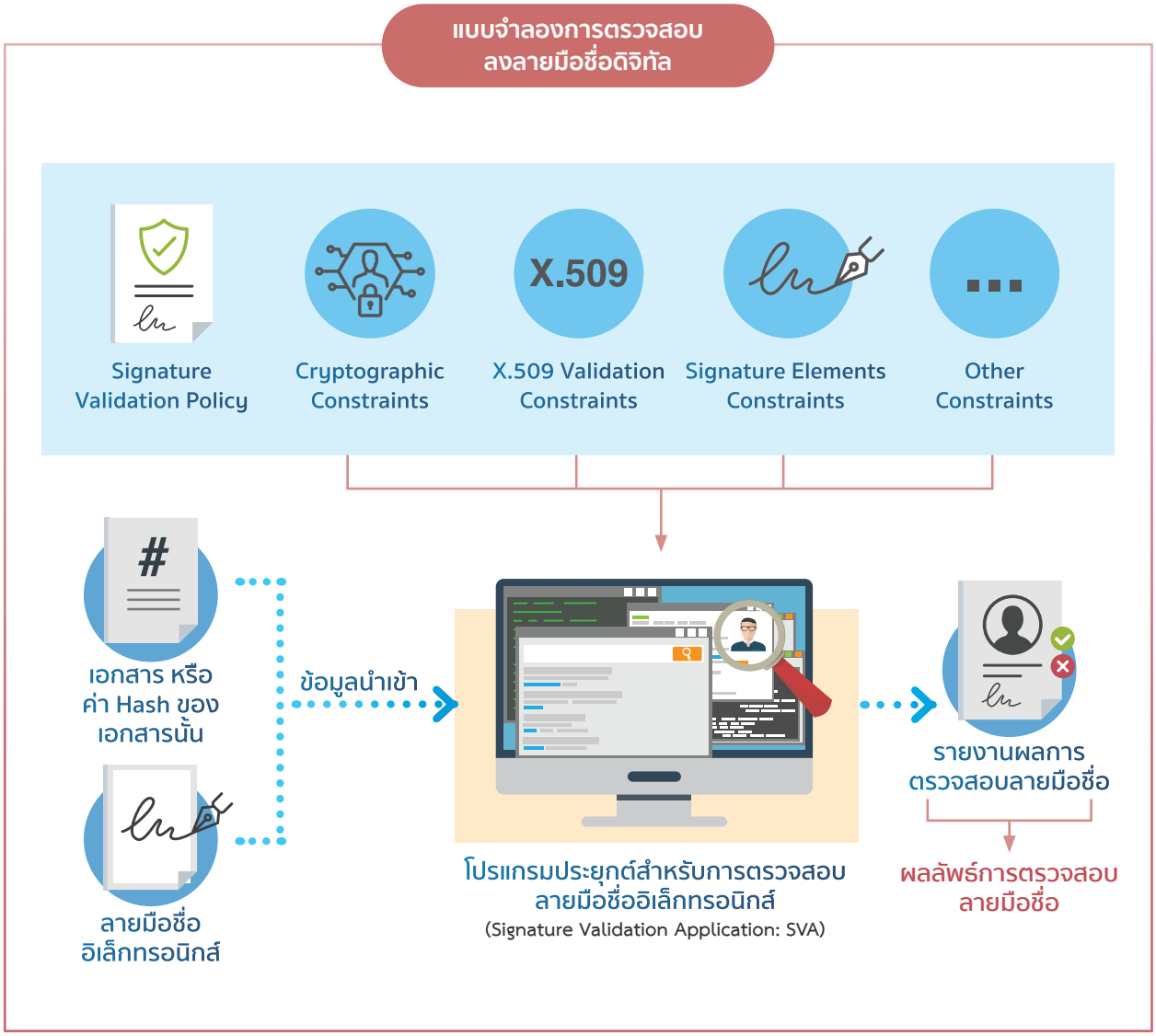
จำเป็นต้องอาศัยซอฟต์แวร์ในการทำงานซึ่งซอฟต์แวร์ ดังกล่าวต้องมีความสามารถตรวจสอบข้อกำหนดต่างๆ ที่กำหนดในแนวนโยบายในการตรวจสอบลายมือชื่อ (Signature validation policy) ได้แก่

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

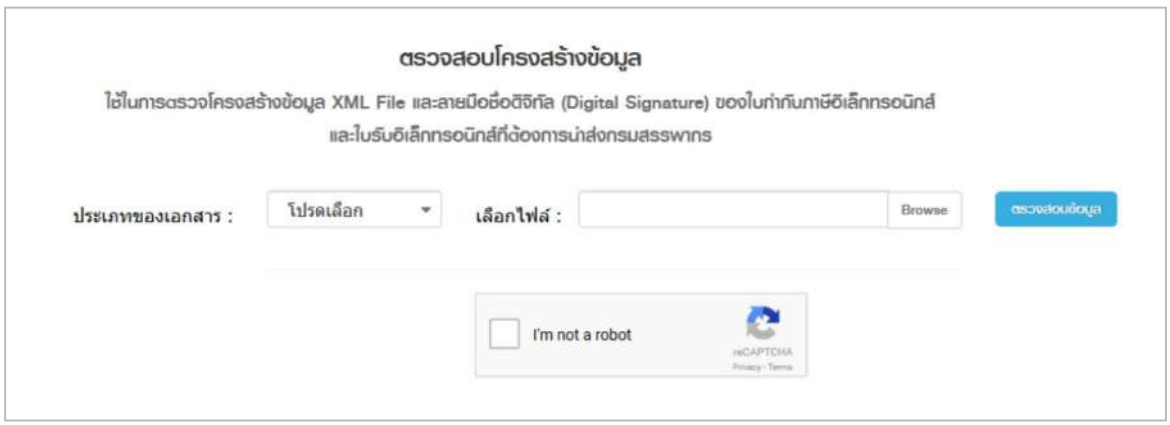
1. ตรวจสอบความถูกต้องของ Format ลงลายมือชื่อดิจิทัล Format เช่น แบบ XAdES Format ของ XMLDSIG เป็นต้น
2. ตรวจสอบความถูกต้องของ Reference ที่ใช้ระบุใบรับรองอิเล็กทรอนิกส์ทั้งหมดในลายมือชื่ออิเล็กทรอนิกส์
3. ตรวจสอบความครบถ้วนขององค์ประกอบที่ใช้ในการตรวจสอบความถูกต้องของลายมือชื่อ ได้แก่ เงื่อนไขการตรวจสอบความถูกต้องของลายมือชื่อ (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 เนื่องจากข้อมูลการตรวจสอบข้อมูลโครงสร้างข้อมูล XML และการลงลายมือชื่อดิจิทัล ต้องมีการระบุข้อมูล Namespace ของ XML ด้วย ตามตัวอย่าง ดังนี้

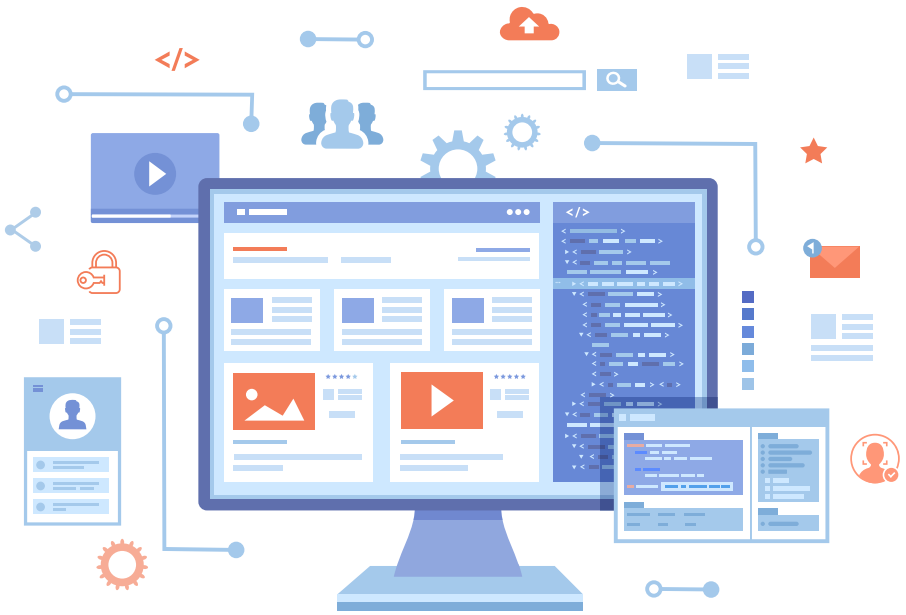
```
// Document to sign
dbf = DocumentBuilderFactory.newInstance();
dbf.setNamespaceAware(true);
Document doc = dbf.newDocumentBuilder()
```

- ในขั้นตอนการพัฒนาโปรแกรมลงลายมือชื่อดิจิทัล แนะนำให้ผู้ใช้งานขอใบรับรองอิเล็กทรอนิกส์สำหรับทดสอบจากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เพื่อใช้ในการทดสอบสร้างลายมือชื่อดิจิทัล
- ผู้ใช้งานทั่วไปสามารถตรวจสอบโครงสร้างข้อมูล XML และลายมือชื่อดิจิทัลที่อยู่ระหว่างพัฒนาโปรแกรมได้ที่เว็บไซต์ https://etax.rd.go.th เมนู สนับสนุน > ตรวจสอบโครงสร้างข้อมูล



ทั้งนี้ เมื่อทำการตรวจสอบโครงสร้างข้อมูล ระบบจะตรวจสอบโครงสร้างของ schema และ schematron ตามมาตรฐาน ขมธอ.3-2560 และตรวจสอบลายมือชื่อดิจิทัล (Digital Signature) กรณีข้อมูลไม่ผ่านการตรวจสอบ ระบบจะมีข้อความแจ้งเตือนทันทีที่หน้าจอ ผู้ใช้งานสามารถตรวจสอบข้อความแจ้งเตือน โดยศึกษารายละเอียดเพิ่มเติมได้ที่คู่มือ ข้อความตอบกลับการตรวจสอบโครงสร้างข้อมูล (Response Error)

- กรณีผู้พัฒนาใช้ใบรับรองอิเล็กทรอนิกส์สำหรับทดสอบสร้างลายมือชื่อดิจิทัล และนำไฟล์ดังกล่าวตรวจสอบโครงสร้างข้อมูลที่เว็บไซต์ จะปรากฏข้อความแจ้งเตือนว่า “Code : ECER010 ไม่ผ่านการตรวจสอบ เนื่องจากใบรับรองอิเล็กทรอนิกส์นี้ ไม่ถูกรับรองโดยกรมสรรพากร” หมายความว่า วิธีการสร้างลายมือชื่อดิจิทัลแบบ XAdES เป็นไปตามเงื่อนไขที่กำหนดแล้ว เพียงแต่ผู้ใช้งานใช้ใบรับรองอิเล็กทรอนิกส์สำหรับทดสอบ หากใช้ใบรับรองอิเล็กทรอนิกส์สำหรับใช้งานจริง ในส่วนของลายมือชื่อดิจิทัลจะมีสถานะผ่านการทดสอบ



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] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยข้อความอิเล็กทรอนิกส์สำหรับการซื้อขายสินค้าและบริการ เวอร์ชั่น 2.0 (ขมธอ.3-2560)

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

E-TAX
INVOICE & RECEIPT

ติดต่อสอบถามได้ที่

1161 RD INTELLIGENCE CENTER
ศูนย์สารนิเทศสรรพากร บริการด้วยใจ ใส่ใจทุกคำถาม

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