ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ETDA Recommendation on ICT Standard

for Electronic Transactions

ขมธอ. 14-2560

ว่าด้วยการใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ระหว่างหน่วยงาน

USING XML MESSAGES FOR INTER-ORGANIZATIONAL DATA EXCHANGE

เวอร์ชัน 1.0

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ICS 35.240.30

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ระหว่างหน่วยงาน

ขมธอ. 14-2560

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 21
เลขที่ 33/4 ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
หมายเลขโทรศัพท์: 0 2123 1234 หมายเลขโทรสาร: 0 2123 1200

ประกาศโดย
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

วันที่ 23 พฤษภาคม พ.ศ. 2560

คณะทำงานจัดทำร่างข้อเสนอแนะเกี่ยวกับการจัดทำหรือแปลงเอกสารและข้อความ ให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

ประธานคณะทำงาน

นายศุภโชค จันทรประทิน	รักษาการผู้อำนวยการสำนักมาตรฐาน สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ผู้ทำงาน

นายกำชัย จัตตานนท์	ผู้แทนกรมศุลกากร
นางสาวขนิษฐา สหเมธาพัฒน์	ผู้แทนกรมสรรพากร
นายธานินทร์ ตันกิติบุตร	ผู้แทนบริษัท ไทยเทรดเน็ต จำกัด
นายธิติกร ตระกูลศิริศักดิ์	ผู้แทนสำนักโครงสร้างพื้นฐานสารสนเทศ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
นายชาณิน เลาหพันธ์	ผู้แทนสำนักวิจัยและพัฒนา สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ผู้ทำงานและเลขานุการ

นายเฉลิมชัย บวรนันท์	ผู้แทนสำนักมาตรฐาน สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อการทำธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ระหว่างหน่วยงานฉบับนี้ จัดทำขึ้นเพื่อสนับสนุนการใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัยและน่าเชื่อถือ รวมทั้งให้ผู้ประกอบการและหน่วยงานต่าง ๆ มีแนวทางในการสร้างเอกสารอิเล็กทรอนิกส์อยู่ในรูปแบบข้อความ XML ให้เป็นมาตรฐานเดียวกัน โดยข้อเสนอแนะฉบับนี้ได้พัฒนาตามแนวมาตรฐาน ดังนี้

- XML Naming and Design Rules Technical Specification Version 3, UN/CEFACT, 2009
- ISO 14533-2:2012, Processes, data elements and documents in commerce, industry and administration -- Long term signature profiles -- Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES)
- ISO/TS 15000-1:2004, Electronic business eXtensible Markup Language (ebXML) – Part 1: Collaboration-Protocol Profile and Agreement Specification (ebCPP)
- ISO/TS 15000-2:2004, Electronic business eXtensible Markup Language (ebXML) – Part 2: Message service specification (ebMS)

โดยได้มีการนำเสนอและรับฟังความคิดเห็นเป็นการทั่วไป ตลอดจนพิจารณาข้อมูล ข้อสังเกต ข้อคิดเห็น จากผู้ทรงคุณวุฒิและจากหน่วยงานที่เกี่ยวข้องเพื่อให้ข้อเสนอแนะมาตรฐานฉบับนี้มีความสมบูรณ์ครบถ้วนยิ่งขึ้น รวมทั้งสามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพ

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ระหว่างหน่วยงานฉบับนี้ จัดทำขึ้นโดยสำนักมาตรฐาน ภายใต้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 21 เลขที่ 33/4 ถนนพระราม 9
แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
โทรศัพท์: 0 2123 1234 โทรสาร: 0 2123 1200
E-mail: estandard.center@etda.or.th www.etda.or.th

คำนำ

ปัจจุบันการทำธุรกรรมทางอิเล็กทรอนิกส์ด้วยการรับส่งข้อความอิเล็กทรอนิกส์ถูกใช้อย่างแพร่หลายในด้านการค้าและการทำธุรกรรมภาครัฐระหว่างหน่วยงาน โดยเฉพาะการใช้ข้อความ XML (Extensible Markup Language Messages) อย่างไรก็ตาม การจัดทำและใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ในปัจจุบันมีรูปแบบการใช้งานที่หลากหลายตามความต้องการของแต่ละหน่วยงานโดยไม่มีแนวทางที่เป็นมาตรฐานเดียวกัน เช่น การจัดทำข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน และการใช้ลายมือชื่ออิเล็กทรอนิกส์กับข้อความ XML ที่ถูกต้องสอดคล้องกับมาตรฐานสากล

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. ได้เห็นถึงประโยชน์ของการใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ที่มีความมั่นคงปลอดภัยและสอดคล้องกับมาตรฐานสากล ข้อเสนอแนะมาตรฐานฉบับนี้จึงกล่าวถึงแนวทางในการสร้างข้อความ XML อย่างเป็นระบบทั้งในเชิงโครงสร้างและความหมายของข้อมูลในเอกสารเพื่อให้ผู้ใช้งานสามารถเข้าใจความหมายของข้อมูลตรงกัน ข้อแนะนำเกี่ยวกับการลงลายมือชื่ออิเล็กทรอนิกส์เพื่อรักษาความมั่นคงปลอดภัยของข้อมูลในข้อความ XML รวมถึงแนวทางการแลกเปลี่ยนข้อความ XML ระหว่างหน่วยงานที่เป็นมาตรฐานเดียวกัน

สารบัญ

สารบัญรูป

สารบัญตาราง

ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

เรื่อง ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ระหว่างหน่วยงาน

โดยที่เป็นการสมควรกำหนดแนวทางการสร้างและการใช้เอกสารอิเล็กทรอนิกส์ในรูปแบบข้อความ XML เพื่อสนับสนุนการใช้งานเอกสารอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย น่าเชื่อถือ และเป็นมาตรฐานเดียวกัน

อาศัยอำนาจตามความในมาตรา ๗ (๔) แห่งพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ. ๒๕๕๔ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) จึงประกาศข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ระหว่างหน่วยงาน เลขที่ ขมธอ. ๑๔-๒๕๖๐ ปรากฏตามท้ายประกาศฉบับนี้

ประกาศ ณ วันที่ ๒๗ พฤษภาคม ๒๕๖๐

(นางสุรางคณา วายุภาพ)
ผู้อำนวยการ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ว่าด้วยการใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ระหว่างหน่วยงาน

1. ขอบข่าย

เอกสารฉบับนี้ จัดทำขึ้นสำหรับผู้พัฒนาซอฟต์แวร์และพัฒนาข้อความ XML เพื่อแนะนำแนวทางการใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ให้สอดคล้องกับมาตรฐานสากล และเป็นไปตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. 2553 [1] อาทิ กระบวนการจัดทำเอกสารและข้อความอิเล็กทรอนิกส์และวิธีการที่น่าเชื่อถือในการระบุตัวตนของผู้จัดทำ รวมถึงกลไกในการรับรองความถูกต้องครบถ้วนของเอกสารอิเล็กทรอนิกส์ที่ถูกสร้างขึ้น

เอกสารฉบับนี้ แบ่งเนื้อหาออกเป็น 3 หัวข้อหลัก ได้แก่

(1) การจัดทำและออกแบบเอกสารให้อยู่ในรูปแบบข้อความ XML ซึ่งอ้างอิงแนวทางจากเอกสาร XML Schema Design and Management [2]

(2) การสร้างและการตรวจสอบความถูกต้องลายมือชื่ออิเล็กทรอนิกส์ โดยมีรายละเอียดของพื้นฐานและองค์ประกอบของลายมือชื่ออิเล็กทรอนิกส์แบบ Advanced Electronic Signature (AdES) รวมถึงแนวทางในการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์และข้อมูลอื่น ๆ ที่เกี่ยวข้อง เช่น เวลาที่ลงลายมือชื่อในเอกสาร และข้อมูลใบรับรองอิเล็กทรอนิกส์ทั้งหมดที่เกี่ยวข้อง โดยอ้างอิงแนวทางจากเอกสารมาตรฐาน ISO 14533-2:2012 [3]

(3) แนวทางการแลกเปลี่ยนข้อความ XML ซึ่งมีรายละเอียดของโครงสร้างและคุณลักษณะเฉพาะของ Electronic Business Extensible Markup Language (ebXML) โดยอ้างอิงแนวทางจากเอกสารมาตรฐาน ISO/TS 15000-1:2004 [5] และ ISO/TS 15000-2:2004 [6]

2. บทนิยาม

คำนิยามของศัพท์ที่ใช้กับมาตรฐานฉบับนี้

2.1 “ข้อความ” หมายถึง เรื่องราว หรือข้อเท็จจริง ไม่ว่าจะปรากฏในรูปแบบของตัวอักษร ตัวเลข เสียง ภาพ หรือรูปแบบอื่นใดที่สื่อความหมายได้โดยสภาพของสิ่งนั้นเองหรือโดย สภาพของสิ่งนั้นเองหรือโดยผ่านกิจการใดๆ

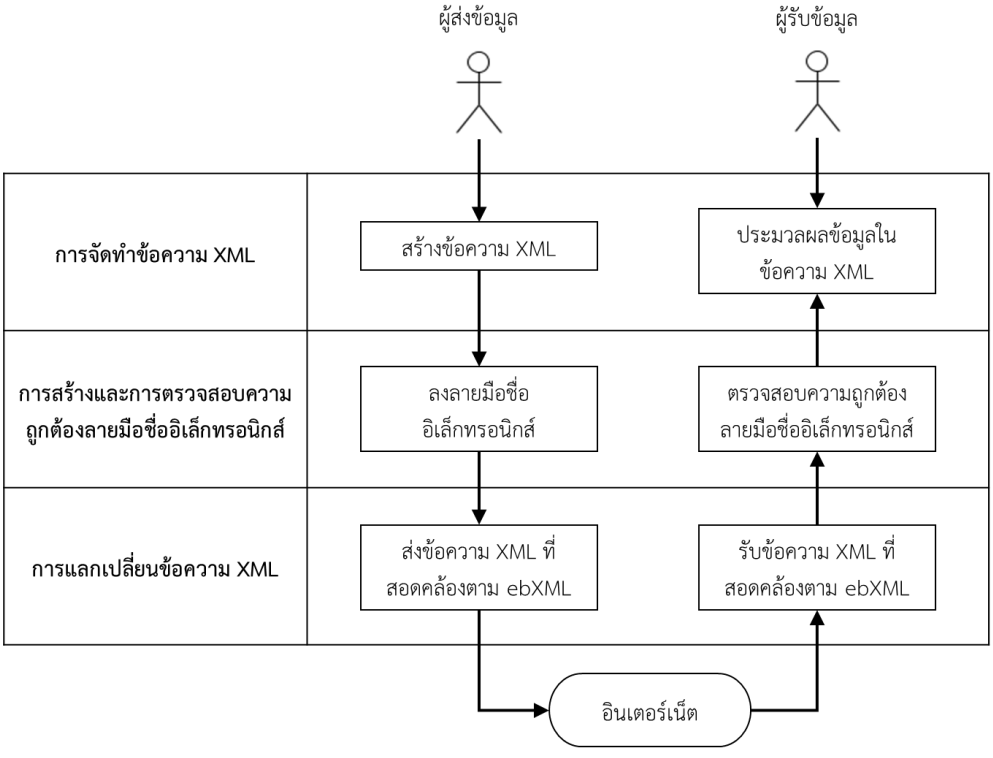
2.2 “ข้อมูลอิเล็กทรอนิกส์” หมายถึง ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือ ประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร

3. แนวคิดการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์โดยใช้ข้อความ XML

ปัจจุบันการแลกเปลี่ยนเอกสารระหว่างหน่วยงานต่าง ๆ โดยเฉพาะหน่วยงานภาครัฐ ส่วนใหญ่ยังใช้เอกสารกระดาษ เมื่อมีการส่งเอกสารถึงผู้รับแล้ว ผู้รับต้องนำข้อมูลในเอกสารดังกล่าวจัดเก็บเข้าระบบคอมพิวเตอร์อีกครั้งเพื่อนำไปประมวลผลต่อ ทำให้เกิดความผิดพลาดในการนำเข้าข้อมูลได้ง่าย ดังนั้นเพื่อให้เกิดความสะดวกในแลกเปลี่ยนเอกสารระหว่างระบบคอมพิวเตอร์ จึงมีการจัดทำเอกสารให้อยู่ในรูปแบบข้อความ XML ซึ่งถูกเขียนขึ้นด้วยภาษาคอมพิวเตอร์ที่เรียกว่าภาษา XML (Extensible Markup language) ใช้สำหรับการแสดงผลและจัดเก็บข้อมูลอิเล็กทรอนิกส์ รวมถึงนำไปใช้ในการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ในระบบคอมพิวเตอร์ของหน่วยงานที่มีความแตกต่างกัน ส่งผลให้การรับส่งและประมวลผลข้อมูลอิเล็กทรอนิกส์ในระบบคอมพิวเตอร์สามารถทำได้แบบอัตโนมัติ ลดข้อผิดพลาดที่เกิดจากการนำเข้าข้อมูลโดยมนุษย์ได้

นอกจากนี้ หน่วยงานผู้ส่งเอกสารหรือข้อมูลต้องมีการลงลายมือชื่อผู้จัดทำและผู้อนุมัติให้ออกเอกสารเพื่อเป็นการรับรองเอกสารที่จะส่งออก ทั้งนี้ การจัดทำข้อมูลอิเล็กทรอนิกส์ในรูปแบบข้อความ XML สามารถสร้างลายมือชื่ออิเล็กทรอนิกส์ได้ตามมาตรฐาน XAdES (XML Advanced Electronic Signatures) [3] เพื่อทำให้ข้อความ XML มีคุณสมบัติในการตรวจสอบความถูกต้องครบถ้วนของข้อมูลและสามารถพิสูจน์เวลาที่มีการลงลายมือชื่ออิเล็กทรอนิกส์ได้

สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ในรูปแบบข้อความ XML สามารถส่งกันได้หลากหลายวิธี ซึ่งแนวทางหนึ่งที่มีความมั่นคงปลอดภัย คือ การแลกเปลี่ยนข้อมูลด้วยมาตรฐาน ebXML (Electronic Business Extensible Markup Language) ซึ่งเป็นมาตรฐานเปิดสำหรับการแลกเปลี่ยนข้อมูลข้อมูลอิเล็กทรอนิกส์ที่เข้าใจตรงกันในระดับสากล นอกจากนี้ กรมศุลกากรของประเทศไทยมีการใช้มาตรฐาน ebXML ในการแลกเปลี่ยนข้อมูลใบอนุญาต/ใบรับรองกับหน่วยงานผู้ออกใบอนุญาต และแลกเปลี่ยนข้อมูลใบขนสินค้ากับผู้ประกอบการนำเข้าส่งออก



รูปที่ 1 กระบวนการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์โดยใช้ข้อความ XML

จากกระบวนการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์โดยใช้ข้อความ XML ที่กล่าวมาข้างต้น (ดังแสดงในรูปที่ 1) กระบวนการตั้งแต่การสร้างข้อความ XML จนถึงการส่งข้อความ XML นั้น ผู้ส่งข้อมูลอาจทำการส่งออกข้อมูล (export) ออกมาจากระบบงานของหน่วยงานให้อยู่ในรูปแบบข้อความ XML ตามโครงสร้างมาตรฐานที่กำหนด (รายละเอียด หัวข้อ 4) จากนั้นทำการลงลายมือชื่ออิเล็กทรอนิกส์บนข้อความ XML (รายละเอียด หัวข้อ 5) และส่งข้อความ XML ที่สอดคล้องตามข้อกำหนด ebXML ให้ผู้รับข้อมูล (รายละเอียด หัวข้อ 6)

เมื่อผู้รับข้อมูลได้รับข้อความ XML แล้ว สามารถตรวจสอบว่าข้อความที่ได้รับมาจากหน่วยงานใดและมีข้อกำหนดต่าง ๆ อย่างไร ตามโครงสร้างของ ebXML (รายละเอียด หัวข้อ 6) จากนั้นทำการตรวจสอบความถูกต้องลายมือชื่ออิเล็กทรอนิกส์ในข้อความ XML (รายละเอียด หัวข้อ 5) และสุดท้าย ผู้รับข้อมูลสามารถนำข้อมูลในข้อความ XML ไปประมวลผลต่อหรือจัดเก็บ (รายละเอียด หัวข้อ 4) ซึ่งรายละเอียดในแต่ละกระบวนการจะกล่าวในหัวข้อต่อไป

4. การจัดทำข้อความ XML

หัวข้อนี้จะอธิบายการจัดทำข้อความ XML สำหรับใช้ในการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ให้สอดคล้องตาม World Wide Web Consortium (W3C) XML Schema Recommendation

ทั้งนี้ สิ่งที่ต้องคำนึงถึงในการจัดทำข้อความ XML คือ การตรวจสอบความถูกต้องของโครงสร้างข้อมูลและประเภทของข้อมูลที่มาตรฐานกำหนด ซึ่งจำเป็นต้องมีการอ้างอิงถึงที่อยู่ที่จัดเก็บ XML Schema และ Namespace (รายละเอียดในหัวข้อ 4.2) นอกจากนี้ การส่งข้อความ XML สามารถทำได้ทีละหลายรายการโดยจำเป็นต้องมี Business Header เพื่อกำกับข้อมูลในข้อความ XML

4.1 Extensible Markup Language

Extensible Markup Language (XML) คือ ภาษาที่ใช้ในการแลกเปลี่ยนข้อมูล โดยผู้ใช้งานสามารถกำหนดโครงสร้างข้อมูลอิเล็กทรอนิกส์ที่จะใช้ในการรับส่งข้อมูล และสามารถนำไปใช้งานได้ในทุกแพลตฟอร์ม นอกจากนี้ ข้อความ XML ยังง่ายต่อการนำข้อมูลไปประมวลผล ในปัจจุบัน มีการนำข้อความ XML ไปใช้ในการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์อย่างกว้างขวาง เช่น ใบแจ้งหนี้อิเล็กทรอนิกส์ ข้อความการชำระเงินทางอิเล็กทรอนิกส์ เป็นต้น โดยข้อความ XML มีโครงสร้างและไวยากรณ์ตามตารางที่ 1 ดังนี้ [9]

ตารางที่ 1 ตัวอย่างข้อความ XML

บรรทัด	ตัวอย่างข้อความ XML
1	<?xml version="1.0" encoding="UTF-8"?>
2	<!-- This is a comment -->
3	<note>
4	<to gender="female">Tove</to>
5	<from><Name>Jani</Name></from>
6	<heading>Reminder</heading>
7	<body>Don't forget me this weekend!</body>
8	</note>

(1) ส่วนนำของ XML (XML prolog) ถูกกำหนดให้อยู่บรรทัดแรกสุดของข้อความ XML ใช้ในการอธิบายคุณลักษณะของ XML เช่น เวอร์ชันของ XML การเข้ารหัสอักขระ (character encoding) เป็นต้น (ตารางที่ 1 บรรทัดที่ 1)

(2) คำอธิบายข้อมูล (Comment) จะไม่ถูกนำไปประมวลผลโดยแอปพลิเคชันหรือเว็บเบราว์เซอร์ (ตารางที่ 1 บรรทัดที่ 2)

(3) ข้อความ XML ต้องประกอบด้วยรายการข้อมูลลำดับชั้นบนสุด (Root Element) ซึ่งทุกรายการข้อมูลจะอยู่ภายใต้ Root Element (ตารางที่ 1 บรรทัดที่ 3)

(4) ทุกรายการข้อมูล (Element) ในข้อความ XML ต้องประกอบด้วย Tag เปิด และ Tag ปิด โดยค่าของ Tag นั้นๆ จะอยู่ระหว่าง Tag เปิด และ Tag ยกเว้น prolog และ Comment

(5) รายการข้อมูลในข้อความ XML สามารถซ้อนกันได้ และต้องมีการจัดลำดับ Tag เปิด และ Tag ปิดที่เหมาะสม (ตารางที่ 1 บรรทัดที่ 5)

(6) XML เป็นภาษาที่เป็น Case Sensitive (มีความแตกต่างระหว่างการใช้ตัวใหญ่และตัวเล็กของตัวอักษรในภาษาอังกฤษ)

(7) รายการข้อมูลอิเล็กทรอนิกส์ในข้อความ XML สามารถมี attribute ได้ดังที่แสดงในตารางที่ 1 บรรทัดที่ 4 รายการข้อมูล to ที่มี attribute ชื่อ gender ซึ่งมีค่าเท่ากับ female

สำหรับข้อมูลในรูปแบบ XML มีข้อกำหนดเกี่ยวกับสัญลักษณ์ที่ห้ามใช้งานในข้อความ XML ซึ่งหากต้องการใช้งานสัญลักษณ์ดังกล่าว ควรใช้ชุดอักขระดังต่อไปนี้แทน ดังตัวอย่างในตารางที่ 2

ตารางที่ 2 ตัวอย่างการสัญลักษณ์ที่ห้ามในข้อความ XML และ ชุดอักขระที่ใช้แทน

สัญลักษณ์	ชุดอักขระที่ใช้แทน	รายละเอียด
<	&lt;	น้อยกว่า
>	&gt;	มากกว่า
&	&amp;	และ
'	&apos;	อัญประกาศเดี่ยว
"	&quot;	อัญประกาศ

4.2 การกำหนด Namespace ในข้อความ XML

Namespace เป็นชื่อกลุ่มของ XML element หรือ Datatype โดยที่อยู่ของ Namespace จะถูกกำหนดไว้เป็น attribute บน Root element ทั้งนี้ ชื่อ Namespace จะถูกกำหนดให้ไม่ซ้ำกัน เพื่อป้องกันความสับสนในการใช้งาน XML element

4.2.1 ประเภทของ Attribute เพื่อใช้ระบุ Namespace

(1) targetNamespace เป็น attribute เพื่อใช้กำหนด Namespace ของไฟล์ XML Schema เพื่อให้ XML ไฟล์อื่น อ้างอิงถึง
รูปแบบการกำหนด : targetNamespace = “[Namespace]”

(2) xmlns เป็น attribute เพื่อใช้กำหนด Default Namespace ในไฟล์ XML ในกรณีที่ชื่อ XML element ไม่มีการกำหนด prefix
รูปแบบการกำหนด : xmlns = “[Namespace]”

(3) xmlns:[prefix] เป็น attribute เพื่อใช้กำหนด Namespace ในไฟล์ XML ด้วย prefix
รูปแบบการกำหนด : xmlns:[prefix] = “[Namespace]”

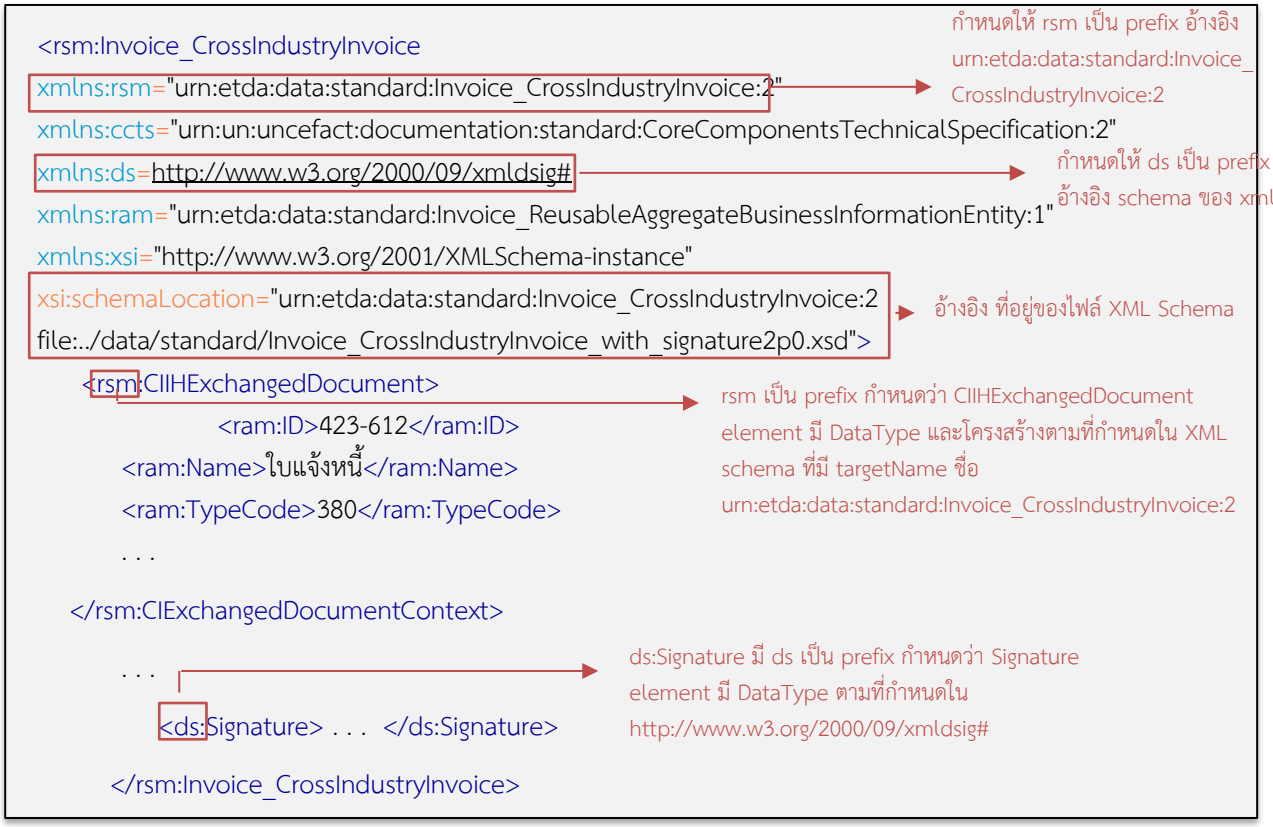
```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:ccts="urn:un:unece:uncefact:documentation:standard:CoreComponentsTechnicalSpecification:2"

targetNamespace="urn:etda:data:standard:Invoice_CrossIndustryInvoice:2" >

        . . .

  </xsd:schema>
```

รูปที่ 2 ตัวอย่างการกำหนด Namespace ใน XML Schema



รูปที่ 3 ตัวอย่างการกำหนด Namespace ในข้อความ XML

4.2.2 รูปแบบการระบุ Namespace

Namespace ที่กำหนดในข้อความ XML สามารถระบุได้ในรูปแบบ URI ซึ่ง URI สามารถแบ่งออกได้ 2 รูปแบบ ได้แก่ กำหนดในรูปแบบ URN (Uniform Resource Name) และ URL (Uniform Resource Locator)

4.2.2.1 การระบุ Namespace ในรูปแบบ URN

UN/CEFACT (United Nations Centre for Trade Facilitation and Electronic Business) ได้เสนอแนะการกำหนดชื่อ URN ตามโครงสร้างดังต่อไปนี้ [10]

```
urn:<organization>:<organizationhierarchy>[:<organizationhierarchylevel>]* :
<schematype>>[:<package>]+:<major>:<status>
```

รูปที่ 4 รูปแบบ Namespace แบบ URN ที่ UN/CEFACT เสนอแนะ

โดยที่

<organization> คือหน่วยงานจัดทำมาตรฐาน

<organizationhierarchy> คือ ส่วนงานลำดับแรกภายใต้หน่วยงานที่จัดทำมาตรฐาน

<organizationhierarchylevel> คือ ส่วนงานลำดับถัดมาภายใต้หน่วยงานที่จัดทำมาตรฐาน

<schematype> คือ ประเภทของ schema ได้แก่ data codelist identifierscheme documentation

<package> คือ ชื่อ package ตามที่มาตรฐานกำหนด

<version> คือ ตัวเลขเป็น major version

<status> คือ สถานะของ schema ได้แก่ standard draft

4.2.2.2 การระบุ Namespace ในรูปแบบ URL

UN/CEFACT ได้เสนอแนะการกำหนดชื่อ URL ตามโครงสร้างดังต่อไปนี้ [10]

```
http://<organization>/<organization hierarchy>[/<organizationhierarchy
level>]*/<schematype>[/<package>]+/<major> /<status>
```

รูปที่ 5 รูปแบบ Namespace แบบ URL ที่ UN/CEFACT เสนอแนะ

โดยที่

<organization> คือ Domain ของหน่วยงานจัดทำมาตรฐาน

<organizationhierarchy> คือ ส่วนงานลำดับแรกภายใต้หน่วยงานที่จัดทำมาตรฐาน

<organizationhierarchylevel> คือ ส่วนงานลำดับถัดมาภายใต้หน่วยงานที่จัดทำมาตรฐาน

<schematype> คือ ประเภทของ schema

<package> คือ ชื่อ package ตามที่มาตรฐานกำหนด

<version> คือ ตัวเลขเป็น major version

<status> คือ สถานะของ schema ได้แก่ standard draft

สำหรับโครงสร้างมาตรฐานกลางของ XML Schema ของข้อความอิเล็กทรอนิกส์ ยกตัวอย่างจากกระบวนการขออนุญาตส่งออกน้ำตาลทรายออกนอกราชอาณาจักรถูกจัดเก็บและถูกแบ่งปันจากระบบ CMR (Code and Message Repository) ในเบื้องต้นสามารถอ้างอิงเพื่อระบุ XML Schema ที่ต้องการใช้งานจากระบบ CMR ด้วย Namespace ในรูปแบบ URL ดังต่อไปนี้

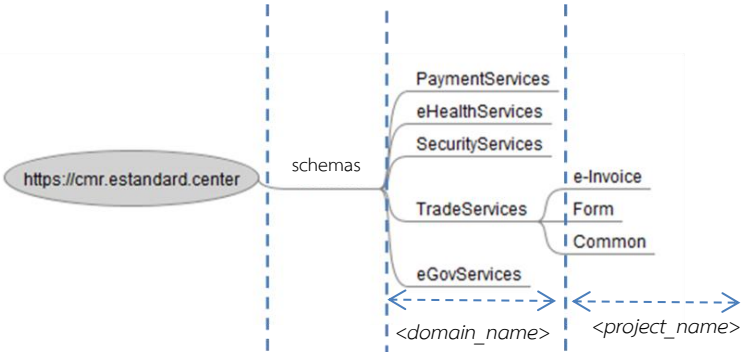
https://cmr.estandard.center/schemas/*<domain_name>*/*<project_name>*

รูปที่ 6 ตัวอย่างรูปแบบ Namespace แบบ URL ที่ UN/CEFACT เสนอแนะ

โดยที่

<domain_name> คือ ชื่อกลุ่ม Service ของมาตรฐาน เช่น PaymentServices, TradeServices, eHealthServices, eGovServices เป็นต้น

<project_name> คือ ชื่อของโปรเจ็ค (ในแต่ละกลุ่ม Service ของมาตรฐาน) เช่น e-Invoice
เป็นต้น



รูปที่ 7 รูปแบบของ Namespace แบบ URL สำหรับอ้างอิงถึง schema

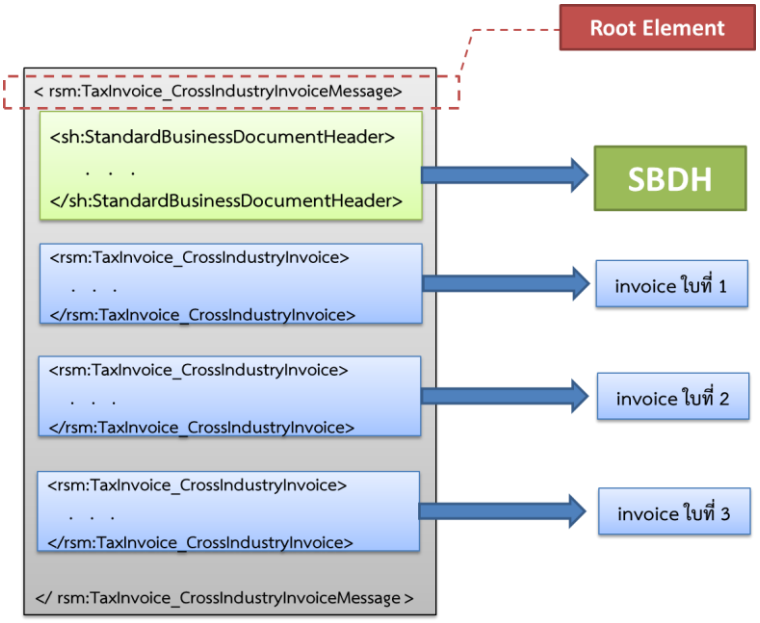
4.3 การกำหนด Standard Business Document Header (SBDH) [11]

SBDH เป็นชุดรายการข้อมูลสำหรับกำหนดรายละเอียดของเอกสารอิเล็กทรอนิกส์ที่จะทำการจัดส่ง แบ่งออกข้อมูลภายใน SBDH ออกได้เป็น 3 กลุ่ม ดังนี้

(1) ข้อมูลการกำหนดเส้นทางเอกสาร เป็นข้อมูลระบุผู้ส่งและผู้รับ โดยอาจใช้ตัวเลขระบุหน่วยงาน รวมถึงข้อมูลที่ติดต่อเพิ่มเติม

(2) ข้อมูลระบุเอกสาร เป็นข้อมูลที่ใช้ระบุเอกสารอิเล็กทรอนิกส์ที่อยู่ภายใต้ SBDH โดยข้อมูลดังกล่าวจะถูกใช้ในการระบุหรือกำหนดเส้นทางสำหรับเอกสารอิเล็กทรอนิกส์ เพื่อส่งต่อไปให้แอปพลิเคชันที่เหมาะสม โดยไม่ต้องตรวจสอบข้อมูลภายในเอกสารอิเล็กทรอนิกส์

(3) ข้อมูลบริบทของกระบวนการเอกสาร เป็นข้อมูลภายในใต้รายการข้อมูล BusinessScope ใช้เพื่อบันทึกพารามิเตอร์สำหรับกระบวนการประมวลผลเอกสารอิเล็กทรอนิกส์



รูปที่ 8 โครงสร้างข้อความแบบ XML ที่ใช้ SBDH

UN/ CEFACT ได้กำหนด Standard Business Document Header (SBDH) Technical Specification มีตัวอย่างข้อมูลเพื่อใช้ในการใช้งาน ดังต่อไปนี้

4.3.1 *<HeaderVersion>* ระบุเวอร์ชันของ SBDH ซึ่งปัจจุบันมีค่า 1.0 ทั้งนี้ ค่าของเวอร์ชันอาจเปลี่ยนไปตาม Schema ของ SBDH

4.3.2 *<Sender>* ระบุหน่วยงานที่เป็นผู้ส่งเอกสารอิเล็กทรอนิกส์ (Standard Business Document : SBD) โดย <Sender> สามารถมีมากกว่า 1 รายการ มีรายการข้อมูลย่อยต่อไปนี้

4.3.2.1 *<Idenfication>* เป็น element ภายใต้ <Sender> ระบุค่าเป็น ID ของผู้ส่งอาจอยู่ในรูปแบบ GLN

4.3.2.2 *<Authority>* เป็นข้อมูลอธิบายหน่วยงานผู้กำหนด Identification sheme เช่น EAN.UCC (European Article Numbering-Uniform Code Council)

4.3.2.3 *<ContactInformation>* เป็นข้อมูลของบุคคลที่สามารถติดต่อได้ ประกอบด้วย Contact (ชื่อบุคคลที่ที่สามารถติดต่อได้) *EmailAddress*, *FaxNumber*, *PhoneNumber*, *ContactTypeIdentifier*

4.3.3 *<Receiver>* ระบุหน่วยงานที่เป็นผู้รับ message ขึ้นมา โดย <Receiver> สามารถมีมากกว่า 1 รายการ มีรายการข้อมูลย่อยต่อไปนี้

4.3.3.1 *<Idenfication>* เป็น element ภายใต้ <Receiver> ระบุค่าเป็น ID ของผู้รับอาจอยู่ในรูปแบบ GLN

4.3.3.2 *<Authority>* เป็นข้อมูลอธิบายหน่วยงานผู้กำหนด Identification sheme เช่น EAN.UCC (European Article Numbering-Uniform Code Council)

4.3.3.3 *<ContactInformation>* เป็นข้อมูลของบุคคลที่สามารถติดต่อได้ ประกอบด้วยดังต่อไปนี้ Contact (ชื่อบุคคลที่สามารถติดต่อได้) EmailAddress, FaxNumber, PhoneNumber, ContactTypeIdentifier

4.3.4 *<DocumentIdentification>* ระบุคุณลักษณะของเอกสารอิเล็กทรอนิกส์ ภายใต้ SBDH

4.3.4.1 *<Standard>* เป็นชื่อมาตรฐานที่ใช้สำหรับ ID ของ message เช่น SWIFT, OAG, UCC, EDIFACT, X12 เป็นต้น

4.3.4.2 *<TypeVersion>* เป็นข้อมูลเวอร์ชันของ Standard element (ข้อ 1)

4.3.4.3 *<InstanceIdentifier>* เป็น ID ระบุ โดยจะมี InstanceIdentifier ต่อ 1 Business Header

4.3.4.4 *<Type* ประเภทของเอกสาร เช่น order, invoice

4.3.4.5 *<MultipleType>* เป็นค่า TRUE หรือ FALSE เพื่อระบุว่าใน message มีประเภทของ Document หลายแบบหรือไม่

4.3.4.6 *<CreationDateTime>* ระบุวันเวลาที่ SBDH ถูกสร้างขึ้น

4.3.5 *<Manifest>* มีรายการข้อมูลดังต่อไปนี้

4.3.5.1 <NumberOfItems> เป็นเลขจำนวนเต็มบวกแสดงจำนวนเอกสารอิเล็กทรอนิกส์ภายใต้ SBDH

4.3.5.2 <ManifestItem> มีข้อมูล ดังนี้

(1) <MimeTypeQualifierCode> แสดงประเภทของเอกสารอิเล็กทรอนิกส์ (Media Type) เช่น XML EDIFACT X12 เป็นต้น

(2) <UniformResourceIdentifier> เป็น URI แสดง Globally Unique ID ซึ่งบอกที่มาของ Content (RFC 2392)

(3) <Description> คำอธิบายที่เกี่ยวกับเอกสารอิเล็กทรอนิกส์

(4) <LanguageCode> รหัสภาษากำหนดใน ISO 639

4.3.6 *<BusinessScope>* ประกอบด้วย <Type>, <InstanceIdentifier>, <Identifier> โดยข้อมูลภายใต้ <BusinessScope> ระบุประเภทของขอบข่ายทางธุรกิจ (Scope) ตัวอย่างเช่น UN/CEFACT

Transaction, UMM: BusinessCollaboration, BusinessProcess, ebXML: BusinessService, BusinessServiceAction, BCF:AuthorizedRole, หรือ Role Party

4.3.7 *<BusinessService>* ข้อมูลภายใต้ Tag นี้อธิบาย Service ที่ผู้รับ message (Receiver) จะต้องเตรียมเพื่อดำเนินการจัดการเอกสารอิเล็กทรอนิกส์ โดย <BusinessService> มี element ลูกประกอบด้วย

4.3.7.1 <ServiceName> บอกชื่อของ Service Protocol ที่ใช้สำหรับ message

4.3.7.2 <ServiceTransaction> บอกคุณลักษณะที่ message ที่ถูกจัดการภายใต้ ServiceName ที่ระบุไว้ข้างต้น มี element ลูก ได้แก่

(1) <TypeOfServiceTransaction> บอกประเภท service transaction ที่กำหนดไว้ UMM เช่น “Requesting Service Transaction” หรือ “Responding Service Transaction”

(2) <IsNonRepudiationRequired> ค่า TRUE/FALSE มีความหมายบอกว่าผู้ส่งมีการลงลายมือชื่ออิเล็กทรอนิกส์หรือไม่

(3) <IsAuthenticationRequired> ค่า TRUE/FALSE บอกว่า identity ของผู้ส่งได้รับการ Verify ว่าผ่านการยืนยันตัวตนแล้ว ทั้งนี้ หาก IsNonRepudiationRequired เป็นค่า TRUE แล้ว tag นี้ก็อาจไม่จำเป็นต้องใช้

(4) <IsNonRepudiationOfReceiptRequired> ค่า TRUE/FALSE ต้องมีการ Verify ว่าผู้รับได้รับข้อความแล้ว

(5) <IsIntelligibleCheckRequired> ค่า TRUE/FALSE บอกว่าทั้งผู้รับ-ส่งข้อความมีการตรวจสอบแล้วว่า message ที่ได้รับถูกต้องครบถ้วน ไม่มีการบิดเบือน (โดยการตรวจสอบค่า Document Integrity)

(6) <IsApplicationErrorResponseRequested> ค่า TRUE/FALSE บอกว่ามีการตรวจสอบความผิดพลาดของแอปพลิเคชันหรือไม่

(7) <TimeToAcknowledgeAcceptance> ระบุช่วงเวลาที่ยอมรับได้ ในการส่ง acknowledge กลับว่าได้รับข้อความแล้ว

(8) <TimeToPerform> ระบุช่วงเวลาที่ message ที่ได้รับ ที่ต้องถูกดำเนินการให้เสร็จสิ้น (นับเวลาจาก จุดเวลาที่ Receiver ได้รับ message)

(9) <Recurrence> เป็นค่าของเลขจำนวนเต็มไม่มีเครื่องหมาย (Unsigned Integer)

4.3.8 *<CorrelationInformation>* บอกข้อมูลความสัมพันธ์ระหว่าง การร้องขอและการตอบกลับตามข้อกำหนดกระบวนการทางธุรกิจ UN/CEFACT Business Process Specification Schema (BPSS) มีการกำหนดความสัมพันธ์ของข้อมูลในระดับ transaction level โดยทั้งผู้รับ-ส่ง message ต้องมีการร่วมกันกำหนด โดยการใช้ <CorrelationInformation> มี element ลูกประกอบด้วย

4.3.8.1 <RequestingDocumentCreationDateTime> ข้อมูลวันเวลา SBDH ถูกสร้าง และเอกสารอิเล็กทรอนิกส์ถูกบรรจุภายใต้ SBDH นั้น

4.3.8.2 <RequestingDocumentInstanceIdentifier> Identifier ของ requesting SBDH หากเอกสารมีการ request และ respond หลายครั้งในการติดต่อทางธุรกิจ ข้อความแรกสุด (ซึ่งส่วนใหญ่เป็น requesting message) จะมี /CorrelationInformation/ RequestingDocumentInstance Identifier เป็นค่าเดียวกันกับ/DocumentIdentification/InstanceIdentifier

ส่วน responding SBDH จะมีค่าของ RequestingDocumentInstanceIdentifier เดียวกับค่าของ RequestingDocumentInstanceIdentifier ของ requesting SBDH

4.3.8.3 <ExpectedResponseDateTime> ข้อมูลวันเวลาที่คาดหวังในการ respond กลับ ExpectedResponseDateTime จะถูกกำหนดตอนสร้าง requesting message จากนั้นถูกคัดลอกและใส่ข้อมูลกลับขา responding message

5. การสร้างและการตรวจสอบความถูกต้องลายมือชื่ออิเล็กทรอนิกส์สำหรับข้อความ XML

ปัจจุบันเอกสารอิเล็กทรอนิกส์เข้ามามีบทบาทสำคัญและถูกใช้อย่างแพร่หลายในการค้าขายสินค้าระหว่างบริษัทและการทำธุรกรรมต่างๆ ระหว่างหน่วยงาน หรือแม้แต่ภายในหน่วยงานเอง เอกสารอิเล็กทรอนิกส์ก็มีส่วนสำคัญที่จะทำให้หน่วยงานเกิดการพัฒนาและทำงานไปได้อย่างราบรื่น อย่างไรก็ตาม สิ่งสำคัญที่ควรคำนึงถึงคือการมีกลไกในการดูแลรักษาความมั่นคงปลอดภัยของข้อมูลในเอกสารอิเล็กทรอนิกส์ที่เหมาะสม เพื่อผู้ใช้งานมีความเชื่อมั่นและเอกสารอิเล็กทรอนิกส์มีความน่าเชื่อถือ เทคนิคที่ใช้ในการรักษาความถูกต้องครบถ้วนของข้อมูล รวมถึงใช้ในการพิสูจน์ตัวตนของผู้ลงลายมือชื่อได้คือการใช้ลายมือชื่ออิเล็กทรอนิกส์

ลายมือชื่ออิเล็กทรอนิกส์แบบ Advanced Electronic Signature (AdES) ซึ่งแบ่งออกเป็น 3 แบบ ได้แก่

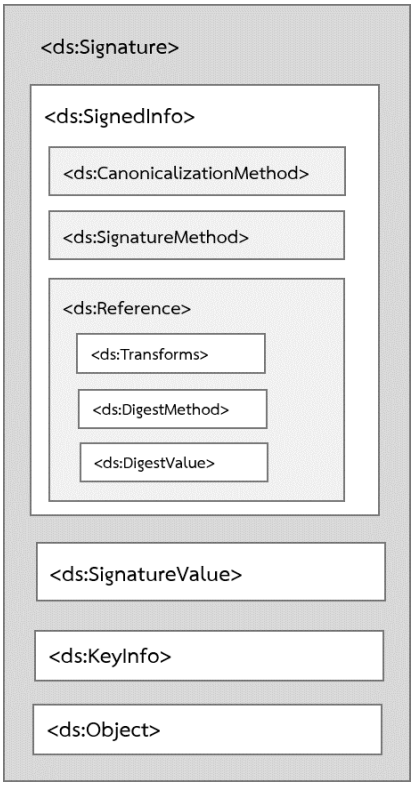
(1) XML Advanced Electronic Signatures (XAdES) ใช้ลงลายมือชื่ออิเล็กทรอนิกส์สำหรับไฟล์ XML

(2) PDF Advanced Electronic Signatures (PAdES) ใช้ลงลายมือชื่ออิเล็กทรอนิกส์สำหรับไฟล์ PDF

(3) CMS Advanced Electronic Signatures (CAdES) ใช้ลงลายมือชื่ออิเล็กทรอนิกส์สำหรับไฟล์ทุกแบบ

นอกเหนือจากที่ลายมือชื่ออิเล็กทรอนิกส์แบบ AdES สามารถตรวจสอบความถูกต้องครบถ้วนของข้อมูลในเอกสาร และสามารถระบุตัวตนของผู้ลงลายมือชื่อได้แล้ว ยังเพิ่มกลไกและรายการข้อมูลเพิ่มเติมลงในลายมือชื่ออิเล็กทรอนิกส์ เช่น เวลาในการลงลายมือชื่อ ข้อมูลที่จะใช้ในการตรวจสอบลายมือชื่อและจัดเก็บเอกสารในระยะยาว เป็นต้น

ในเอกสารฉบับนี้ กล่าวถึงการสร้างเอกสารอิเล็กทรอนิกส์สำหรับแลกเปลี่ยนข้อมูลโดยใช้ข้อความ XML ซึ่งรูปแบบของลายมือชื่อสำหรับไฟล์ XML ที่เหมาะสมคือ XAdES ซึ่งมีองค์ประกอบหลักต่อไปนี้



รูปที่ 9 โครงสร้างลายมือชื่ออิเล็กทรอนิกส์แบบ XMLDSIG

(1) SignedInfo element ประกอบด้วยข้อมูล algorithms หรือขั้นตอนในการลงลายมือชื่ออิเล็กทรอนิกส์ในเอกสาร 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

(1.3) Reference หรือข้อมูลอื่นๆ ที่ใช้ในการลงลายมือชื่ออิเล็กทรอนิกส์

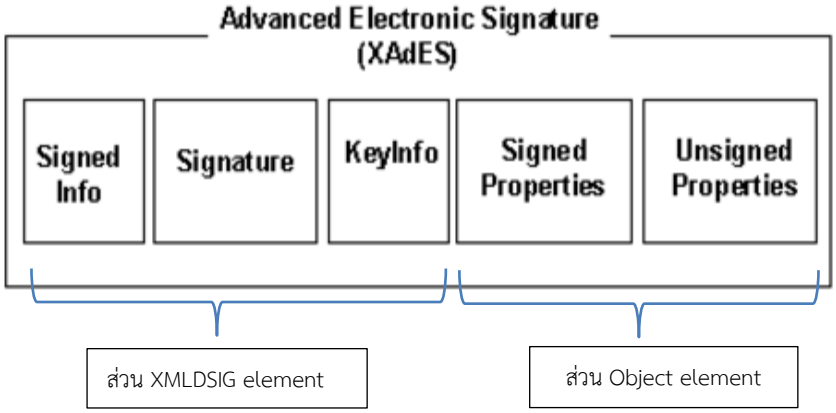
(ก) การ transform signature โดยข้อมูลใน transform element สามารถกำหนดได้ว่าจะให้ XMLDSIG อยู่ในรูปแบบ Enveloping (ลายมือชื่อจะครอบส่วนของเนื้อหาเอกสาร) หรือ Enveloped (ลายมือภายในเนื้อหาเอกสาร)

(ข) Digest Method เป็น algorithms ที่ใช้ในการทำ Digest Message (Hash value ของเนื้อหาเอกสาร) เอกสารฉบับนี้เสนอแนะให้ใช้ Digest Method ในกลุ่ม SHA-2 (เช่น SHA-256 SHA-512 เป็นต้น) และ SHA-3 (เช่น SHA3-256 SHA3-512 เป็นต้น)

(ค) Digest Value เป็น Digest Message หรือ ค่า Hash ของเอกสาร XML โดยค่า Hash ดังกล่าวจะอยู่ในรูปแบบ Base 64 (ตามข้อกำหนด W3C Recommendation on XML Signature Syntax and Processing [12])

(2) SignatureValue เป็นค่าของลายมือชื่ออิเล็กทรอนิกส์ถูกเข้ารหัสในรูปแบบ Base 64

(3) KeyInfo มีข้อมูลใบรับรองอิเล็กทรอนิกส์ของผู้ลงลายมือชื่อ ประกอบด้วย X509SubjectName element ซึ่งระบุ Distinguished Name ของเจ้าของใบรับรองอิเล็กทริกนิกส์ และ X509Certificate ระบุ Certificate ถูกเข้ารหัสแบบ Base 64)

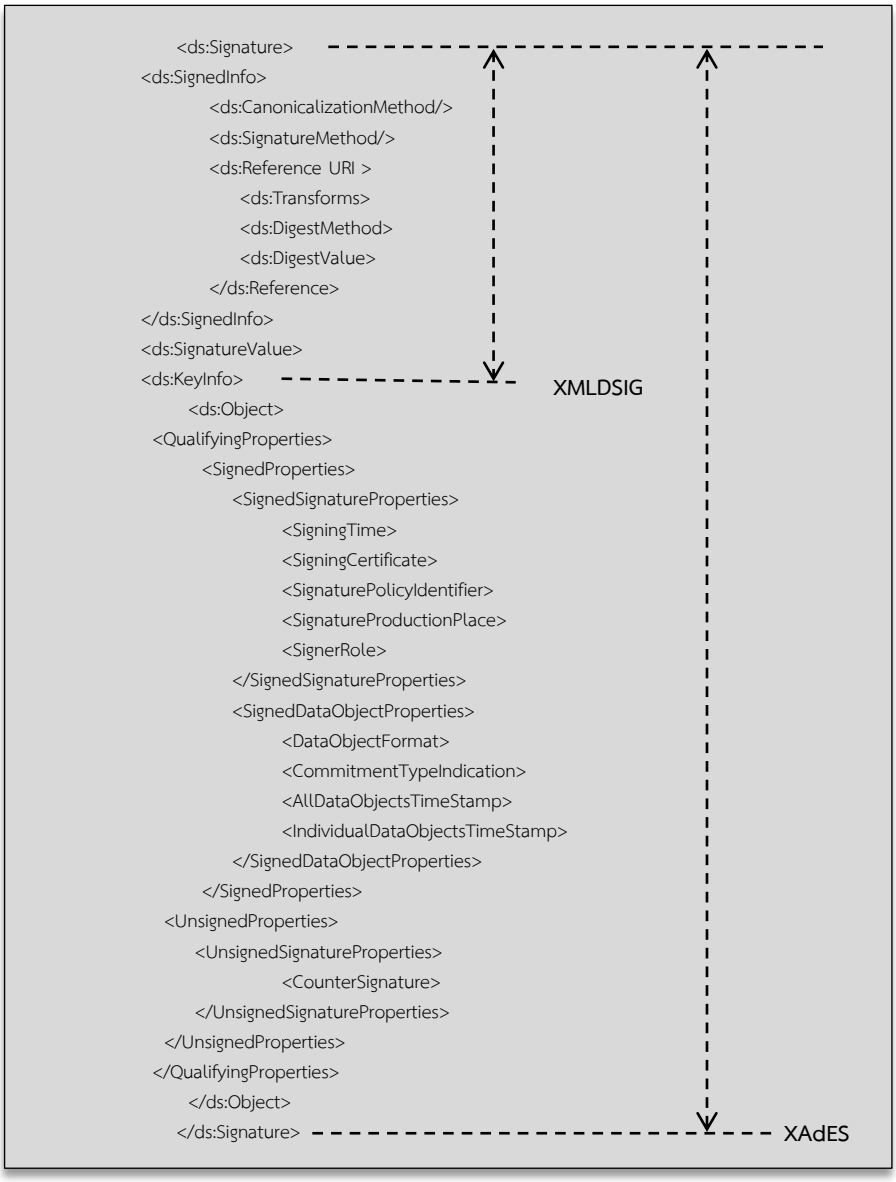


รูปที่ 10 โครงสร้างลายมือชื่ออิเล็กทรอนิกส์ XAdES

(4) SignedProperties เป็น element ภายใต้ Signature/Object/QualifyingProperties ประกอบด้วย element ต่างๆ ที่จะถูกลงลายมือชื่อในขั้นตอนการสร้างลายมือชื่อ element ที่อยู่ภายใต้ SignedProperties ตัวอย่างเช่น SigningTime SigningCertificate SignatureProductionPlace และ SignaturePolicy

(5) UnsignedProperties เป็น element ภายใต้ Signature/Object/QualifyingProperties ประกอบด้วย element ต่างๆ โดย จะไม่ถูกลงลายมือชื่อในขั้นตอนการสร้างลายมือชื่อ โดย element ภายใต้ UnsignedProperties จะถูกรวมเข้ามาภายหลังการลงลายมือชื่ออิเล็กทรอนิกส์ ด้วย XMLDSIG แล้ว เช่น SignatureTimeStamp ซึ่งเป็น Time-Stamp ที่ออกโดย TSA (Time Stamping Authority) เพื่อยืนยันเวลาที่ลายมือชื่ออิเล็กทรอกนิกส์ถูกสร้างขึ้น

ลายมือชื่ออิเล็กทรอนิกส์แบบ AdES แต่ละประเภท ได้แก่ Basic Signature, Signature with Time, Signatures With Long-Term Validation Data, Signatures With Archival Data มีรายการข้อมูลเพิ่มเติมในลายมือชื่อต่างกันออก ทำให้มีคุณสมบัติแตกต่างกันออกไป และความซับซ้อนในการใช้งานมากขึ้นตามลำดับ ทั้งนี้ เอกสารฉบับนี้ จะเสนอแนะลายมือชื่ออิเล็กทรอนิกส์แบบ Basic Signature, Signature with Time เท่านั้น โดยกระบวนการสร้างลายมือชื่ออิเล็กทรอนิกส์แบบ XAdES (กล่าวถึงในหัวข้อ 5.1) และการตรวจสอบความถูกต้องของลายมือชื่ออิเล็กทรอนิกส์ (กล่าวถึงในหัวข้อ 5.2)



รูปที่ 11 แสดง SignedProperties และ UnSignedProperties ภายใต้ XAdES

5.1 การสร้างลายมือชื่ออิเล็กทรอนิกส์แบบ AdES

5.1.1 การสร้างลายมือชื่ออิเล็กทรอนิกส์เบื้องต้น (Basic Signature)

ข้อมูลนำเข้ากระบวนการสร้างลายมือชื่อ

ข้อมูลนำเข้า	จำเป็น/ทางเลือก
เอกสารอิเล็กทรอนิกส์ (Document)	จำเป็นต้องมี
ใบรับรองของเจ้าของลายมือชื่อ (Certificate)	จำเป็นต้องมี
รายการข้อมูลของลายมือชื่ออิเล็กทรอนิกส์ที่ต้องการลงลายมือชื่อ (Signature Attributes)	ทางเลือก
แนวนโยบายในการสร้างลายมือชื่ออิเล็กทรอนิกส์ (Signature Creation Policy)	ทางเลือก

ผลลัพธ์จากกระบวนการ

(1) ค่าของลายมือชื่ออิเล็กทรอนิกส์ (Signature Value)

(2) รายการข้อมูลที่ใน UnSignedProperties และรายการข้อมูลใน SignedProperties

กระบวนการในการสร้างลายมือชื่อ

(1) ซอฟต์แวร์ที่ใช้ลงลายมือชื่ออิเล็กทรอนิกส์จะต้องมีความสามารถในการลงลายมือชื่อกำกับเฉพาะบางส่วนของเอกสารได้ด้วย เช่น เอกสารฉบับหนึ่งมี 10 หน้า ซอฟต์แวร์จะต้องมีความสามารถในการลงลายมือชื่อครอบคลุม 5 หน้าแรก หรือ 3 หน้าสุดท้ายของเอกสารได้ เป็นต้น

(2) เลือกรายการข้อมูล (Attributes) เช่น ใบรับรองอิเล็กทรอนิกส์ที่เกี่ยวข้องกับลายมือชื่อและพารามิเตอร์ที่จะทำการลงลายมือชื่อโดยพิจารณาจาก ฟอร์แมตของลายมือชื่ออิเล็กทรอนิกส์ (CAdES, XAdES, PAdES) คลาสของลายมือชื่ออิเล็กทรอนิกส์ (Basic Signature, Signature with Time) และรูปแบบของลายลงลายมือชื่อ (Detached, Enveloping, Enveloped)

(3) ในกระบวนการที่ใช้ในการลงลายมือชื่อต้องมีกลไกในการแจ้งเตือนผู้ใช้งานว่าจะมีการลงลายมือชื่อเพื่อใช้ในการรับการยินยอม (Consent) จากเจ้าของลายมือชื่อ

(4) กระบวนการจะทำการสร้างลายมือชื่อต้องตรวจสอบใบรับรองอิเล็กทรอนิกส์ของเจ้าของลายมือชื่อก่อนว่ายังไม่ถูกเพิกถอน (Revoke) หรือหมดอายุ (Expire)

(5) ในการลงลายมือชื่ออาจมีกระบวนการตรวจสอบตัวตนของผู้ลงลายมือชื่อด้วย เช่น การขอให้ผู้ลงลายมือชื่อใส่รหัสผ่าน (ของ Private Key)

(6) ทำการสร้างลายมือชื่ออิเล็กทรอนิกส์

(7) นำลายมือชื่ออิเล็กทรอนิกส์ที่ได้จากกระบวนการขั้นต้น มาประกอบเข้ากับเอกสารอิเล็กทรอนิกส์

5.1.2 การสร้างลายมือชื่ออิเล็กทรอนิกส์แบบมีประทับเวลา (Signature with Time)

ลายมือชื่ออิเล็กทรอนิกส์แบบมีประทับเวลาใช้พิสูจน์ว่าลายมือชื่ออิเล็กทรอนิกส์เกิดขึ้น ณ เวลาที่ประทับเวลาในลายมือชื่ออิเล็กทรอนิกส์ได้ระบุไว้

ข้อมูลนำเข้ากระบวนการสร้างลายมือชื่อ

ข้อมูลนำเข้า	จำเป็น/ทางเลือก
ลายมือชื่ออิเล็กทรอนิกส์ขั้นต้น (Basic Signature)	จำเป็นต้องมี
รายการข้อมูลเพิ่มเติมสำหรับประทับเวลา	มีหรือไม่มีก็ได้

ผลลัพธ์จากกระบวนการ

ได้ลายมือชื่ออิเล็กทรอนิกส์ที่มีข้อมูลการประทับเวลา (time-stamp token) อยู่ภายใต้รายการข้อมูล UnsigneProperties

กระบวนการสร้างลายมือชื่อ

(1) ทำการส่งข้อความเพื่อร้องขอประทับเวลาจาก TSA โดยประทับเวลาต้องมีการลงลายมือชื่ออิเล็กทรอนิกส์จาก TSA ด้วย

(2) สร้างรายการข้อมูลของลายมืออิเล็กทรอนิกส์เพื่อเก็บประทับเวลา (ในข้อ 1)

(3) เพิ่มรายการข้อมูลในข้อที่ 2 ลงในลายมือชื่ออิเล็กทรอนิกส์ขั้นต้น ในส่วนรายการข้อมูล UnsigneProperties

5.2 การตรวจสอบความถูกต้องลายมือชื่ออิเล็กทรอนิกส์

ในการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์จำเป็นต้องอาศัยซอฟต์แวร์ในการทำงาน ซึ่งซอฟต์แวร์ดังกล่าวต้องมีความสามารถตรวจสอบข้อกำหนดต่างๆ ที่กำหนดในแนวนโยบายในการตรวจสอบลายมือชื่อ (Signature validation policy) ได้แก่

(1) ข้อกำหนดเกี่ยวกับการเข้ารหัสลับ (Cryptographic Constraints)

(2) ข้อกำหนดในการตรวจสอบรายการข้อมูล X.509 (X.509 Validation Constraints)

(3) ข้อกำหนดเกี่ยวกับรายการข้อมูลของลายมือชื่ออิเล็กทรอนิกส์ (Signature Elements Constraints)

(4) ข้อกำหนดหรือเงื่อนไขอื่นๆ ที่กำหนดขึ้น (Other Constraints)

ทั้งนี้ ลักษณะของซอฟต์แวร์ที่ใช้ในการตรวจสอบความถูกต้องลายมือชื่ออิเล็กทรอนิกส์ (Signature Validation Application) อาจจะเป็นไปได้หลายรูปแบบ เช่น

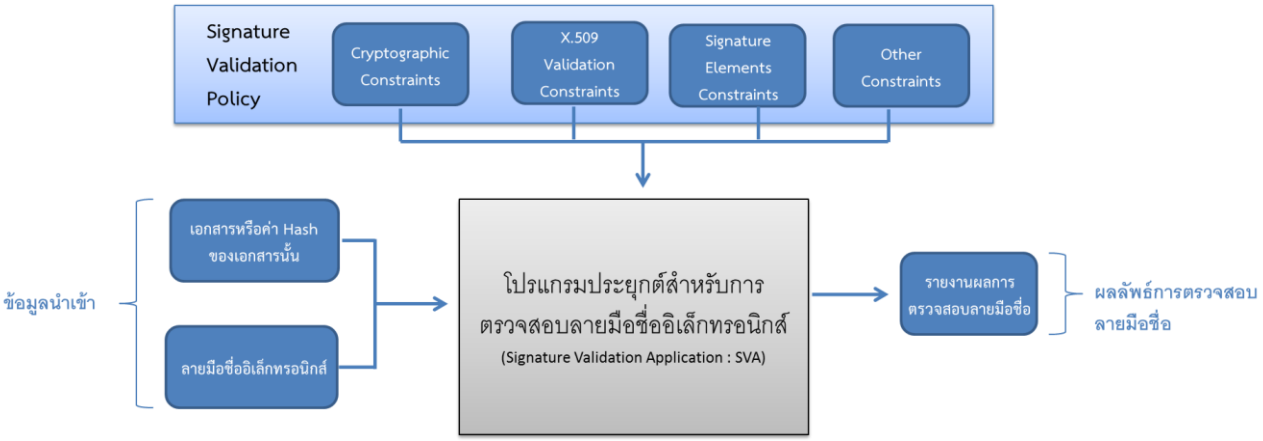
(1) โปรแกรมประยุกต์สำหรับใช้งานใน PC

(2) Web Service

(3) Web Application

(4) โปรแกรมในรูปแบบ Command Line

(5) Integrated library หรือ Middleware หรือโปรแกรมประยุกต์ในรูปแบบอื่นๆ



รูปที่ 12 แบบจำลองการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์

ในการตรวจสอบความถูกต้องของลายมือชื่ออิเล็กทรอนิกส์แบบ AdES จะให้ผลลัพธ์เป็นสถานะการตรวจสอบความถูกต้องของลายมือชื่อดังต่อไปนี้

PASSED หมายความว่า ลายมือชื่ออิเล็กทรอนิกส์ถูกต้องตามข้อกำหนดของ Signature Validation Policy

FAILED หมายความว่า ลายมือชื่ออิเล็กทรอนิกส์ไม่ถูกต้องตามข้อกำหนดของ Signature Validation Policy เนื่องจาก พบว่าข้อมูลที่เกี่ยวกับการเข้ารหัสลับของลายมือชื่ออิเล็กทรอนิกส์ (รวมถึงค่า hash ของเอกสารและ ค่า hash ของ object ที่อยู่ภายในลายมือชื่ออิเล็กทรอนิกส์) ไม่ถูกต้อง หรือตรวจสอบแล้วพบว่าลายมือชื่ออิเล็กทรอนิกส์ถูกสร้างขึ้นภายหลังใบรับรองอิเล็กทรอนิกส์ถูกยกเลิกไปแล้ว

ทั้งนี้ การตรวจสอบลายมือชื่ออิเล็กทรอนิกส์แบบ AdES ในแต่ละคลาสมีรายละเอียดที่แตกต่างกันไปตามรายการข้อมูลที่เกี่ยวข้อง และเทคนิคการสร้างที่ดังกล่าวข้างต้น โดยมีรายละเอียดดังต่อไปนี้

5.2.1 ขั้นการตรวจสอบความถูกต้องลายมือชื่ออิเล็กทรอนิกส์แบบขั้นต้น (Validation of Basic Signature)

ขั้นตอนตรวจสอบความถูกต้องของลายมือชื่ออิเล็กทรอนิกส์ในหัวข้อนี้กล่าวถึง ขั้นตอนตรวจสอบความถูกต้องของลายมือชื่ออิเล็กทรอนิกส์ที่สร้างขึ้นในหัวข้อ 5.2.1

ข้อมูลนำเข้าสำหรับกระบวนการตรวจสอบความถูกต้องของลายมือชื่อ

ข้อมูลนำเข้า	จำเป็น/ทางเลือก
ลายมือชื่ออิเล็กทรอนิกส์ (Signature Value)	จำเป็นต้องมี
เอกสารที่ถูกลงลายมือชื่อ หรือค่า hash ของเอกสาร	จำเป็นต้องมี
ใบรับรองอิเล็กทรอนิกส์ (Certificate)	ทางเลือก
Signature Validation Policies	ทางเลือก
Trust anchor list	ทางเลือก
Certificate Validation Data	ทางเลือก

ผลลัพธ์ที่ได้จากกระบวนการ

ผลของการตรวจสอบความถูกต้องสำหรับ ลายมือชื่ออิเล็กทรอนิกส์แบบ Basic Signature เป็น PASSED ก็ต่อเมื่อตรวจสอบกระบวนการด้านล่างแล้วถูกต้องทั้งหมด นอกนั้น ผลจะได้เป็น FAILED

กระบวนการตรวจสอบความถูกต้องของลายมือชื่อ

(1) ตรวจสอบความถูกต้องของ Format ลายมือชื่ออิเล็กทรอนิกส์ เช่น Format แบบ XAdES, Format ของ XMLDSIG เป็นต้น

(2) ตรวจสอบความถูกต้องของ Reference ที่ใช้ระบุใบรับรองอิเล็กทรอนิกส์ ทั้งหมดในลายมือชื่ออิเล็กทรอนิกส์

(3) ตรวจสอบความครบถ้วนขององค์ประกอบในที่ใช้ในการตรวจสอบความถูกต้องของลายมือชื่อ ได้แก่ เงื่อนไขการตรวจสอบความถูกต้องของลายมือชื่อ (chain contraints, cryptographic constraints, signature constraints)

(4) ตรวจสอบความถูกต้องของ Cryptographic Verification โดยใช้ใบรับรองอิเล็กทรอนิกส์ตรวจสอบกับลายมือชื่อที่ลงไว้ในเอกสาร ในกรณีนี้ ไม่ได้ใช้ใบรับรองอิเล็กทรอนิกส์ทั้งหมดใน Certificate Chain ใช้เพียงใบรับรองอิเล็กทรอนิกส์ของเจ้าของลายมือชื่อเท่านั้น

(5) ตรวจสอบความถูกต้องของความถูกต้องของใบรับรองอิเล็กทรอนิกส์ (X.509 Certificate)

(ก) ตรวจสอบว่าปัจจุบันใบรับรองอิเล็กทรอนิกส์ต้องยังไม่หมดอายุ หรือยังไม่ถูกเพิกถอน

(ข) ตรวจสอบความถูกต้องของความสัมพันธ์ของใบรับรองอิเล็กทรอนิกส์ใน Certificate Chain

(ค) ใบรับรองอิเล็กทรอนิกส์ทั้งหมดใน Certificate Chain ต้องยังไม่หมดอายุ หรือยังไม่ถูกเพิกถอน

5.2.2 การตรวจสอบความถูกต้องลายมือชื่ออิเล็กทรอนิกส์ที่มีประทับเวลา (Validation process for time-stamps)

ข้อมูลนำเข้าสำหรับกระบวนการตรวจสอบความถูกต้องของลายมือชื่อ

ข้อมูลนำเข้า	จำเป็น/ทางเลือก
Time-stamp token	จำเป็นต้องมี
Trust anchor list	ทางเลือก
แนวนโยบายการตรวจสอบความถูกต้องลายมือชื่ออิเล็กทรอนิกส์	ทางเลือก
ใบรับรองอิเล็กทรอนิกส์ (Certificate) ของ Time-stamp	ทางเลือก

ผลลัพธ์ที่ได้จากกระบวนการ

ผลของการตรวจสอบความถูกต้องสำหรับ Signature with Time คือ สถานะเป็น PASSED หากการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ Basic Signature ถูกต้อง และ Time-stamp token ถูกตรวจสอบแล้วว่าถูกต้อง นอกนั้นจะได้ผลเป็น FAILED

กระบวนการตรวจสอบความถูกต้องของลายมือชื่อ

ตรวจสอบความถูกต้องของลายมือชื่ออิเล็กทรอนิกส์ขั้นต้น (Basic Signature) รวมถึงต้องพิจารณาความถูกต้องของ Time-stamp token ด้วย หากผลการตรวจสอบเป็น PASSED แล้ว แต่หากผลการตรวจสอบไม่ถูกต้องซอฟต์แวร์ต้องคืนสถานะการตรวจสอบความถูกต้องเป็น FAILED

6. แนวทางการแลกเปลี่ยนข้อความ XML

การแลกเปลี่ยนข้อมูลในรูปแบบอิเล็กทรอนิกส์ เป็นการช่วยลดการใช้เอกสารกระดาษ ลดค่าใช้จ่าย และเพิ่มประสิทธิภาพการทำงานร่วมกันทางธุรกิจให้กับหน่วยงาน อย่างไรก็ตาม การที่หน่วยงานต่าง ๆ มีแนวทางการแลกเปลี่ยนข้อมูลด้วยรูปแบบหรือข้อกำหนดที่แตกต่างกันถือเป็นอุปสรรคของการติดต่อสื่อสารระหว่างกัน ด้วยเหตุนี้ มาตรฐาน Electronic Business using eXtensible Markup Language (ebXML) ซึ่งอาศัยการแลกเปลี่ยนข้อมูลในรูปแบบข้อความ XML ซึ่งเป็นภาษาที่มีโครงสร้างที่สามารถรองรับความต้องการในการแลกเปลี่ยนข้อมูล

ระหว่างหน่วยงานที่หลากหลายได้เป็นอย่างดี จึงถูกพัฒนาขึ้น โดยมาตรฐาน ebXML มีเป้าหมายหลักเพื่อเป็นโครงสร้างพื้นฐานของมาตรฐานเปิดสำหรับการแลกเปลี่ยนข้อมูลทางธุรกิจที่เข้าใจตรงกันในระดับสากล ภายใต้พื้นฐานของการทำงานข้ามระบบ ความมั่นคงปลอดภัย และความถูกต้องระหว่างหน่วยงานหรือองค์กรทางธุรกิจต่าง ๆ

เอกสารฉบับนี้จะอธิบาย ebXML ซึ่งเป็นกรอบแนวทางที่สำคัญในการใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ระหว่างหน่วยงานในหัวข้อ 6.1 โดยสถาปัตยกรรมของ ebXML จะประกอบด้วยข้อกำหนดทางเทคนิคต่างๆ แบ่งเป็น 5 ระดับ ซึ่งจะกล่าวถึงในหัวข้อ 6.2 นอกจากนี้ จะอธิบายข้อกำหนดของ ebXML ในส่วนของความตกลงของการทำงานร่วมกัน หรือ ebXML Collaboration-Protocol Profile and Agreement Specification ที่อ้างอิงตามมาตรฐาน ISO/TS 15000-1:2004 ในหัวข้อ 6.3 และข้อกำหนดของ ebXML เฉพาะในส่วนของการรับส่งข้อความ หรือ ebXML Message Service Specification ที่อ้างอิงตามมาตรฐาน ISO/TS 15000-2:2004 ในหัวข้อ 6.4

6.1 Electronic Business Extensible Markup Language (ebXML)

มาตรฐาน ebXML เป็นชุดข้อกำหนดทางเทคนิคที่จะทำให้หน่วยงานหรือองค์กรไม่ว่าจะเป็นขนาดใดหรือมีสถานที่ทางภูมิศาสตร์ตั้งอยู่ที่ใดก็ตาม สามารถดำเนินธุรกิจระหว่างกันผ่านอินเตอร์เน็ตได้ด้วยการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ในรูปแบบข้อความ XML ทั้งนี้ การใช้งาน ebXML จะทำให้หน่วยงานต่างๆ มีวิธีการที่เป็นมาตรฐานเดียวกันสำหรับการแลกเปลี่ยนข้อมูลทางธุรกิจ การกำหนดกระบวนการทางธุรกิจ การจัดทำความตกลงในการแลกเปลี่ยนข้อมูลร่วมกัน และการติดต่อสื่อสารด้วยข้อกำหนดที่เข้าใจตรงกัน

มาตรฐาน ebXML เริ่มดำเนินการในปี 1999 ซึ่งเป็นการประสานความร่วมมือระหว่างสองหน่วยงาน ได้แก่ OASIS (Organization for the Advancement of Structured Information Standards) ซึ่งเป็นสมาคมระหว่างประเทศที่ไม่แสวงหากำไร ทำหน้าที่ขับเคลื่อนให้เกิดการพัฒนา ความสอดคล้อง และการใช้งานมาตรฐานต่างๆ ที่เกี่ยวข้องกับการดำเนินธุรกิจผ่านสื่ออิเล็กทรอนิกส์ (e-business) และ UN/CEFACT (United Nations Centre for Trade Facilitation and Electronic Business) ซึ่งเป็นหน่วยงานสหประชาชาติ ทำหน้าที่พัฒนาการทำงานเพื่อให้การประสานและความร่วมมือทั่วโลกในด้านการอำนวยความสะดวกทางการค้าและธุรกิจอิเล็กทรอนิกส์เป็นไปในทางที่ดีขึ้น ซึ่งจะส่งเสริมให้เกิดการเติบโตของการค้าระหว่างประเทศและบริการต่างๆ ที่เกี่ยวข้อง [13] [14]

6.2 สถาปัตยกรรมของ ebXML

สถาปัตยกรรมของมาตรฐาน ebXML ประกอบด้วยข้อกำหนดทางเทคนิคซึ่งเป็นรูปแบบข้อความ XML จำนวน 5 ระดับ ดังนี้

(1) กระบวนการทางธุรกิจ (Business processes)

ซึ่งอธิบายไว้ในมาตรฐาน OASIS standard, ebXML Business Process Specification Schema Technical Specification (ebBPSS) v2.0.4 [15]

(2) ชุดข้อมูลร่วม (Core data components)

ซึ่งอธิบายไว้ในมาตรฐาน ISO 15000-5:2014, ebXML – Part 5: Core Components Specification (CCS) [16]

(3) ความตกลงของการทำงานร่วมกัน (Collaboration protocol agreements)

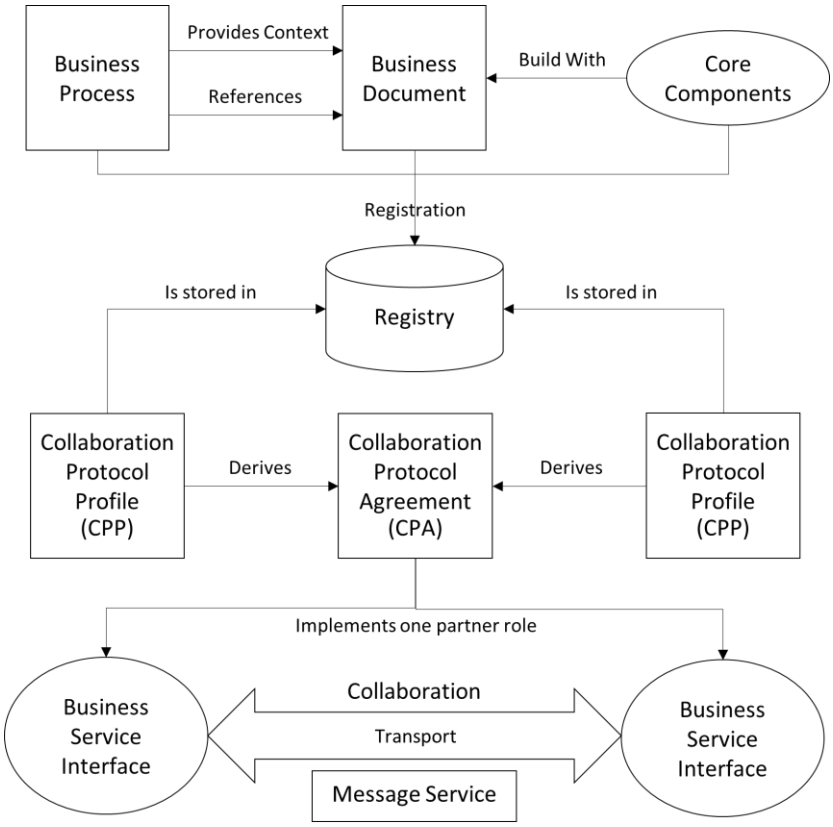
ซึ่งอธิบายไว้ในมาตรฐาน ISO/TS 15000-1:2004, ebXML – Part 1: Collaboration-Protocol Profile and Agreement Specification (ebCPP) [5]

(4) การรับส่งข้อความ (Messaging)

ซึ่งอธิบายไว้ในมาตรฐาน ISO/TS 15000-2:2004, ebXML – Part 2: Message Service Specification (ebMS) [6]

(5) การลงทะเบียนและการจัดเก็บ (Registries and Repositories)

ซึ่งอธิบายไว้ในมาตรฐาน ISO/TS 15000-3:2004, ebXML – Part 3: Registry Information Model Specification (ebRIM) [17] และมาตรฐาน ISO/TS 15000-4:2004, ebXML – Part 4: Registry Services Specification (ebRS) [18]



รูปที่ 13 สถาปัตยกรรมของ ebXML [15]

จากสถาปัตยกรรมของ ebXML (ดังแสดงในรูปที่ 13) การแลกเปลี่ยนข้อมูลทางธุรกิจจะเริ่มต้นจากการกำหนดกระบวนการทางธุรกิจ (Business Process) ซึ่งจะระบุรายการเอกสารทางธุรกิจ (Business Document) ที่เกี่ยวข้องในกระบวนการนั้น โดยเอกสารทางธุรกิจแต่ละรายการอาจมีข้อกำหนดในการสร้างเอกสารอยู่แล้ว หรืออาจจะถูกประกอบขึ้นมาใหม่ด้วยข้อมูลในระดับเล็กลงมา เรียกว่า ชุดข้อมูลร่วม (Core components) ซึ่งนำมาประกอบกันเพื่อให้สอดคล้องตามบริบทการใช้งานที่กำหนดโดยกระบวนการ

ทางธุรกิจนั้น [15] ตัวอย่างเช่น ในกระบวนการทางธุรกิจของการสั่งซื้อสินค้า จะมีเอกสารทางธุรกิจเป็นคำขอซื้อสินค้า ที่ประกอบขึ้นมาจากชุดข้อมูลร่วมต่างๆ เช่น คน (party) ซึ่งหากทำให้สอดคล้องตามบริบทการใช้งานของการสั่งซื้อสินค้าจะเป็นผู้ซื้อและผู้ขาย

ทั้งนี้ คำอธิบายของกระบวนการทางธุรกิจ (Business Process Definition) และคำอธิบายของเอกสารทางธุรกิจ (Business Document Definition) สามารถจัดทำเป็นรูปแบบ XML และนำมาลงทะเบียนเพื่อจัดเก็บไว้ใน ebXML Registry/Repository สำหรับให้ผู้ใช้งานนำไปแลกเปลี่ยนข้อมูลทางธุรกิจร่วมกัน หรือนำกลับมาใช้งานในอนาคตได้ [15]

จากนั้น ผู้ใช้งานจะกำหนดสมรรถภาพในการแลกเปลี่ยนข้อความของหน่วยงานตนเอง เรียกว่า Collaboration-Protocol Profile (CPP) และผู้ใช้งานทั้งสองหน่วยงานจะจัดทำความตกลงในการแลกเปลี่ยนข้อความร่วมกัน เรียกว่า Collaboration Protocol Agreement (CPA) ทั้งนี้ CPA อาจถูกกำหนดขึ้นโดยการนำ CPP ของทั้งสองหน่วยงานมาประกอบกัน โดยการแลกเปลี่ยนข้อความระหว่างสองหน่วยงานนี้จะต้องใช้ CPA อันเดียวกันสำหรับการกำหนดค่าของระบบ (run-time system configuration) ซึ่งมี Business Service Interface เป็นซอฟต์แวร์ที่บริหารจัดการการทำงานร่วมกันทางธุรกิจ (Business Collaboration) เพื่อให้การแลกเปลี่ยนข้อความระหว่างหน่วยงานมีความสอดคล้องกันแม้ว่าจะเป็นระบบที่ไม่ได้มาจากผู้จำหน่ายรายเดียวกันก็ตาม [15]

ทั้งนี้ เพื่อให้หน่วยงานที่ต้องการแลกเปลี่ยนข้อความสามารถค้นหาคู่ค้าหรือหน่วยงานอื่นๆ ที่มีความเหมาะสมได้ หน่วยงานอาจจะนำ CPP ของตนเองมาลงทะเบียนเพื่อจัดเก็บไว้ใน ebXML Registry/Repository สำหรับให้ผู้ใช้งานค้นหาหน่วยงานที่จะทำงานร่วมกันทางธุรกิจ

สุดท้าย ระบบของหน่วยงานจะสามารถแลกเปลี่ยนข้อมูลหรือเอกสารทางธุรกิจเป็นข้อความระหว่างกันได้อย่างอัตโนมัติตามกระบวนการทางธุรกิจและความตกลงในการแลกเปลี่ยนข้อความที่มีการกำหนดไว้ก่อนหน้านี้ โดยกระบวนการแลกเปลี่ยนข้อความนี้จะเกิดขึ้นบนข้อกำหนดของ ebXML ที่เรียกว่า ebXML Message Service (ebMS) Specification ซึ่ง ebMS ถือว่าเป็นโครงสร้างพื้นฐานที่ทำให้การแลกเปลี่ยนข้อความระหว่างผู้ใช้งาน ebXML ผ่านโพรโทคอลการนำส่งข้อมูลต่างๆ เช่น HTTP/S, SMTP, FTP เป็นไปด้วยความเรียบร้อย มีความมั่นคงปลอดภัย และสอดคล้องตามกระบวนการหรือเงื่อนไขที่กำหนดไว้ [6]

6.3 ebXML Collaboration-Protocol Profile and Agreement Specification

ในการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ระหว่างสองหน่วยงาน แต่ละหน่วยงานจะต้องมีการทำงานร่วมกันทางธุรกิจ (Business Collaboration) กับอีกหน่วยงาน ทราบบทบาทของอีกหน่วยงานในการทำงานร่วมกัน และทราบรายละเอียดด้านเทคโนโลยีที่อีกหน่วยงานใช้ในการรับส่งข้อความ ซึ่งวิธีที่แต่ละหน่วยงานสามารถแลกเปลี่ยนข้อมูลในบริบทของการทำงานร่วมกันทางธุรกิจนั้นจะถูกอธิบายเป็น Collaboration-Protocol Profile (CPP) นอกจากนี้ ทั้งสองหน่วยงานอาจมีความจำเป็นที่จะต้องบรรลุข้อตกลงในรายละเอียดบางอย่าง ซึ่งความตกลงของการทำงานร่วมกันทางธุรกิจระหว่างหน่วยงานจะถูกอธิบายเป็น Collaboration-Protocol Agreement (CPA) [5]

ทั้งนี้ หน่วยงานหนึ่งอาจจะกำหนด CPP หนึ่งอันสำหรับตนเอง หรืออาจจะจัดทำ CPP หลายอันเพื่อใช้รองรับการทำงานร่วมกันทางธุรกิจที่มีความแตกต่างกัน ตัวอย่างเช่น ใช้ CPP หลายอันสำหรับการดำเนินการที่แตกต่างกันในภูมิภาคต่างๆ ของโลก หรือส่วนงานต่างๆ ของหน่วยงาน

ebXML Collaboration-Protocol Profile and Agreement Specification เป็นข้อกำหนดที่อธิบายคำศัพท์หรือรายการข้อมูลที่ใช้ในการจัดทำ CPP และ CPA รูปแบบอิเล็กทรอนิกส์ ซึ่ง CPP และ CPA นี้จะอยู่ในรูปแบบข้อความ XML โดย CPP จะอธิบายความสามารถของแต่ละหน่วยงาน ขณะที่ CPA จะอธิบายความสามารถในการที่สองหน่วยงานตกลงที่จะใช้ในการทำงานร่วมกันทางธุรกิจ ซึ่ง CPA จะถูกนำไปประมวลผลโดยคอมพิวเตอร์ของหน่วยงาน เพื่อใช้กำหนดค่าระบบ (Configuration) ให้สามารถแลกเปลี่ยนข้อความต่างๆ ระหว่างกันได้ [5]

ทั้งนี้ การจัดทำ CPA สามารถทำได้สองวิธี คือ การจัดทำ CPA จาก CPP ของสองหน่วยงาน และการจัดทำ CPA จากแม่แบบ (CPA template) โดยวิธีที่หนึ่ง หน่วยงานจะจัดทำ CPP แล้วนำมาจัดเก็บไว้ใน ebXML Registry จากนั้น อีกหน่วยงานหนึ่งจะสามารถค้นหา CPP ดังกล่าวจาก ebXML Registry และนำมารวมกับ CPP ของตนเองเพื่อจัดทำเป็น CPA ที่ตกลงร่วมกัน ขณะที่วิธีที่สอง หน่วยงานจะจัดทำ CPA template ซึ่งเป็นข้อเสนอ (Proposal) สำหรับการดำเนินการกระบวนการทางธุรกิจส่งให้อีกหน่วยงานหนึ่ง เพื่อให้หน่วยงานนั้นระบุลักษณะหรือความสามารถของตนเอง โดยการแทนที่ค่าว่าง (Placeholder values) ด้วยค่าที่เป็นจริง (Actual values) ใน CPA template เพื่อจัดทำเป็น CPA ที่ตกลงร่วมกัน [5]

6.3.1 ข้อกำหนดของ Collaboration-Protocol Profile (CPP)

CPP กำหนดความสามารถของหน่วยงานที่จะมีส่วนร่วมในการดำเนินธุรกิจแบบอิเล็กทรอนิกส์กับหน่วยงานอื่นๆ โดยความสามารถเหล่านี้ประกอบด้วยความสามารถทางเทคโนโลยี เช่น โพรโทคอลการติดต่อสื่อสารและการรับส่งข้อความที่ระบบของหน่วยงานรองรับ และความสามารถทางธุรกิจ ซึ่งเป็นลักษณะของการทำงานร่วมกันทางธุรกิจที่หน่วยงานรองรับ

ข้อกำหนดของ CPP หรือรายการข้อมูล CollaborationProtocolProfile สามารถแสดงได้เป็นรายการข้อมูล ดังนี้

ตารางที่ 3 รายการข้อมูลของ Collaboration-Protocol Profile

รายการข้อมูล	ความจำเป็นต้องมี	อ้างอิงรายละเอียด
PartyInfo	[1..n]	ISO/TS 15000-1:2004 หัวข้อ 8.4
SimplePart	[1..n]	ISO/TS 15000-1:2004 หัวข้อ 8.5
Packaging	[1..n]	ISO/TS 15000-1:2004 หัวข้อ 8.6
Signature	[0..1]	ISO/TS 15000-1:2004 หัวข้อ 8.7
Comment	[0..n]	ISO/TS 15000-1:2004 หัวข้อ 8.8

6.3.1.1 PartyInfo

PartyInfo เป็นรายการข้อมูลสำหรับระบุหน่วยงานและรายละเอียดเกี่ยวกับหน่วยงาน ซึ่งมีความสามารถตามที่กำหนดไว้ใน CPP ทั้งนี้ CPP อาจประกอบด้วยรายการข้อมูล PartyInfo มากกว่าหนึ่งรายการ หากหน่วยงานดังกล่าวเลือกจะแสดงหน่วยงานตนเองเป็นส่วนงานต่างๆ ที่มีลักษณะแตกต่างกัน โดย PartyInfo ประกอบด้วยรายการข้อมูลย่อยต่างๆ ดังนี้

รายการข้อมูลย่อยของ PartyInfo	ความจำเป็นต้องมี
PartyId	[1..n]
PartyRef	[1..n]
CollaborationRole	[1..n]
Certificate	[1..n]
SecurityDetails	[1..n]
DeliveryChannel	[1..n]
Transport	[1..n]
DocExchange	[1..n]
OverrideMshActionBinding	[0..n]

(1) PartyId เป็นรายการข้อมูลสำหรับระบุหมายเลขไอดี (Identifier) ของหน่วยงาน

(2) PartyRef เป็นรายการข้อมูลสำหรับอ้างอิงไปยังข้อมูลเพิ่มเติมเกี่ยวกับหน่วยงาน เช่น ชื่อหน่วยงาน ที่อยู่ หมายเลขโทรศัพท์ เป็นต้น ซึ่ง PartyRef กำหนดให้ระบุในรูปแบบ URI (Uniform Resource Identifier)

(3) CollaborationRole เป็นรายการข้อมูลสำหรับระบุบทบาทของหน่วยงานในบริบทของการทำงานร่วมกันทางธุรกิจ โดย CollaborationRole ประกอบด้วยรายการข้อมูลย่อย ดังนี้

รายการข้อมูลย่อยของ CollaborationRole	ความจำเป็นต้องมี
ProcessSpecification	[1..1]
Role	[1..1]
ApplicationCertificateRef	[0..1]
ApplicationSecurityDetailsRef	[0..1]
ServiceBinding	[1..1]

(3.1) ProcessSpecification สำหรับระบุการเชื่อมโยงไปยังเอกสารข้อกำหนดกระบวนการทางธุรกิจ (Process Specification document) ซึ่งกำหนดการปฏิสัมพันธ์ระหว่างสองหน่วยงาน

(3.2) Role สำหรับกำหนดบทบาทที่หน่วยงานสามารถรองรับได้ใน ProcessSpecification นั้นๆ

(3.3) ApplicationCertificateRef สำหรับระบุใบรับรองอิเล็กทรอนิกส์ที่จะใช้ในลายมือชื่ออิเล็กทรอนิกส์และการเข้ารหัสลับในระดับแอปพลิเคชัน (Application-level)

(3.4) ApplicationSecurityDetailsRef สำหรับระบุใบรับรองอิเล็กทรอนิกส์ที่ไว้วางใจ (Trust Anchors) และนโยบายความมั่นคงปลอดภัย (Security Policy) ที่จะนำไปใช้กับใบรับรองอิเล็กทรอนิกส์ระดับแอปพลิเคชันของอีกหน่วยงานหนึ่ง

(3.5) ServiceBinding ประกอบด้วยรายการข้อมูล Service สำหรับระบุบริการ (ต้องเป็นค่าเดียวกันกับค่า Service ใน ebXML Message Header ของ ebMS) และรายการข้อมูล CanSend และ CanReceive สำหรับระบุข้อความการดำเนินการ (Action Message) ที่หน่วยงานสามารถส่งได้ และข้อความการร้องขอให้ดำเนินการ (Action Invocation Message) ที่หน่วยงานสามารถรับได้ตามลำดับ รวมถึงระบุ DeliveryChannel ที่หน่วยงานจะใช้ส่งและรับข้อความข้างต้น ทั้งนี้ บริบทของ ServiceBinding จะต้องมีความสอดคล้องตามกระบวนการที่กำหนดไว้ใน ProcessSpecification และบทบาทที่กำหนดไว้ใน Role

(4) Certificate เป็นรายการข้อมูลสำหรับระบุข้อมูลใบรับรองอิเล็กทรอนิกส์ที่หน่วยงานใช้ในการรักษาความมั่นคงปลอดภัย

(5) SecurityDetails เป็นรายการข้อมูลสำหรับระบุรายการใบรับรองอิเล็กทรอนิกส์ที่ไว้วางใจ (Trust Anchors) และนโยบายความมั่นคงปลอดภัย (Security Policy) ที่หน่วยงานใช้ในการรักษาความมั่นคงปลอดภัย

(6) DeliveryChannel เป็นรายการข้อมูลสำหรับกำหนดลักษณะเฉพาะที่หน่วยงานสามารถใช้ในการส่งหรือรับข้อความ ซึ่งจะรวมทั้งโพรโทคอลการติดต่อสื่อสาร (Transport Protocol) เช่น HTTP และโพรโทคอลการรับส่งข้อความ (Messaging Protocol) เช่น ebXML Message Service (ebMS) ทั้งนี้ DeliveryChannel แต่ละรายการจะเป็นการรวมกันของ Transport หนึ่งลักษณะและ DocExchange หนึ่งลักษณะ เพื่อระบุลักษณะเฉพาะของช่องทางการส่งข้อความแต่ละช่องทาง

(7) Transport เป็นรายการข้อมูลสำหรับกำหนดลักษณะเฉพาะของโพรโทคอลการติดต่อสื่อสารต่าง ๆ ที่หน่วยงานสามารถรองรับในการส่งหรือรับข้อความ ทั้งนี้ Transport แต่ละรายการจะประกอบด้วย TransportSender สำหรับระบุวิธีการที่หน่วยงานใช้ส่งข้อความ หรือTransportReceiver สำหรับระบุวิธีการที่หน่วยงานใช้รับข้อความ หรือทั้งสองรายการ

(8) DocExchange เป็นรายการข้อมูลสำหรับกำหนดลักษณะเฉพาะของการแลกเปลี่ยนข้อความ เช่น โพรโทคอลเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์และการเข้ารหัสลับที่หน่วยงานสามารถรองรับ

(9) OverrideMshActionBinding เป็นรายการข้อมูลสำหรับระบุ DeliveryChannel ที่ใช้ส่งข้อความระดับ Message Service Handler แบบไม่ประสานเวลา (Asynchronous delivery)

6.3.1.2 SimplePart

SimplePart เป็นรายการข้อมูลสำหรับแสดงรายการขององค์ประกอบต่างๆ ซึ่งจะถูกระบุด้วยค่า MME content type

6.3.1.3 Packaging

Packaging เป็นรายการข้อมูลสำหรับระบุข้อมูลเฉพาะเกี่ยวกับวิธีการบรรจุ ebXML Message Header และ Payload ต่างๆ เพื่อนำส่งผ่านการติดต่อสื่อสาร รวมถึงข้อมูลสำคัญเกี่ยวกับการรักษาความมั่นคงปลอดภัยของเอกสาร และวิธีการในการนำคุณลักษณะด้านความมั่นคงปลอดภัยต่างๆ มาใช้

โดยทั่วไป รายการข้อมูล Packaging จะบ่งบอกแนวทางที่องค์ประกอบต่างๆ ประกอบกันเป็นข้อความ ebXML รวมถึงข้อมูลเกี่ยวกับ MIME processing capabilities, MIME content type, XML namespace, ตัวแปรด้านความมั่นคงปลอดภัย และ MIME structure ของข้อมูลที่จะแลกเปลี่ยนระหว่างหน่วยงาน

6.3.1.4 Signature

Signature เป็นรายการข้อมูลสำหรับการลงลายมือชื่ออิเล็กทรอนิกส์ใน CPA โดยใช้เทคโนโลยีที่สอดคล้องตามข้อกำหนด W3C Recommendation: XML Signature Syntax and Processing

6.3.1.5 Comment

Comment เป็นรายการข้อมูลสำหรับบรรยายข้อความ เพื่อผู้เขียนสามารถเพิ่มข้อความได้ตามวัตถุประสงค์ที่ต้องการ

6.3.2 ข้อกำหนดของ Collaboration-Protocol Agreement (CPA)

CPA กำหนดความสามารถที่สองหน่วยงานจำเป็นจะต้องตกลงร่วมกัน เพื่อให้ทั้งสองหน่วยงานสามารถดำเนินธุรกิจแบบอิเล็กทรอนิกส์ร่วมกันได้ตามวัตถุประสงค์ของ CPA นั้นๆ

ข้อกำหนดของ CPA หรือรายการข้อมูล CollaborationProtocolAgreement สามารถแสดงได้เป็นรายการข้อมูล ดังนี้

ตารางที่ 4 รายการข้อมูลของ Collaboration-Protocol Agreement

รายการข้อมูล	ความจำเป็นต้องมี	อ้างอิงรายละเอียด
Status	[1..1]	ISO/TS 15000-1:2004 หัวข้อ 9.3
Start	[1..1]	ISO/TS 15000-1:2004 หัวข้อ 9.4.1
End	[1..1]	ISO/TS 15000-1:2004 หัวข้อ 9.4.2
ConversationConstraints	[0..1]	ISO/TS 15000-1:2004 หัวข้อ 9.5
PartyInfo	[2..2]	ISO/TS 15000-1:2004 หัวข้อ 9.6
SimplePart	[1..n]	ISO/TS 15000-1:2004 หัวข้อ 9.7
Packaging	[1..n]	ISO/TS 15000-1:2004 หัวข้อ 9.8
Signature	[0..1]	ISO/TS 15000-1:2004 หัวข้อ 9.9
Comment	[0..n]	ISO/TS 15000-1:2004 หัวข้อ 9.10

6.3.2.1 Status

Status เป็นรายการข้อมูลสำหรับบันทึกสถานะของกระบวนการประกอบขึ้นหรือการเจรจาต่อรองที่ใช้ในการจัดทำ CPA โดยค่าของสถานะต่างๆ ประกอบด้วย proposed, agreed และ signed

6.3.2.2 Start

Start เป็นรายการข้อมูลสำหรับระบุวันและเวลาที่ CPA เริ่มมีผลบังคับใช้

6.3.2.3 End

End เป็นรายการข้อมูลสำหรับระบุวันและเวลาที่ CPA สิ้นสุด เมื่อ CPA ครบอายุการใช้งาน การทำธุรกรรม (Business Transactions) ใดๆ ที่ยังอยู่ระหว่างการดำเนินการจะอนุญาตให้ดำเนินการต่อจนเสร็จสมบูรณ์ ขณะที่การทำธุรกรรมใหม่จะไม่อนุญาตให้เริ่มดำเนินการ

6.3.2.4 ConversationConstraints

ConversationConstraints เป็นรายการข้อมูลสำหรับระบุข้อจำกัดเกี่ยวกับจำนวนของการสนทนา (conversation) ระหว่างสองหน่วยงาน ได้แก่ จำนวนสูงสุดของการสนทนาซึ่งสามารถประมวลผลได้ภายใต้ CPA และจำนวนสูงสุดของการสนทนาซึ่งสามารถอยู่ในกระบวนการประมวลผลในเวลาเดียวกันได้ภายใต้ CPA

6.3.2.5 PartyInfo

CPA ต้องประกอบด้วยรายการข้อมูล PartyInfo สองรายการ แต่ละรายการสำหรับระบุหน่วยงานที่เกี่ยวข้องกับ CPA โดยรายการข้อมูล PaytyInfo ใช้ระบุข้อตกลงที่ทั้งสองหน่วยงานจะนำมาทำงานร่วมกันตามกระบวนการทางธุรกิจที่อ้างอิงไว้ใน CPA ทั้งนี้ กรณีที่ CPP ประกอบด้วย PartyInfo มากกว่าหนึ่งรายการ จะต้องมีการเลือก PaytyInfo ที่เหมาะสมของ CPP นั้นมาจัดทำเป็น CPA

รายละเอียดของรายการ PartyInfo เช่นเดียวกับหัวข้อ 6.3.1.1

6.3.2.6 SimplePart

รายละเอียดของรายการ SimplePart เช่นเดียวกับหัวข้อ 6.3.1.2

6.3.2.7 Packaging

รายละเอียดของรายการ Packaging เช่นเดียวกับหัวข้อ 6.3.1.3

6.3.2.8 Signature

หน่วยงานมากกว่าหนึ่งหน่วยงานสามารถลงลายมือชื่ออิเล็กทรอนิกส์ในเอกสารความตกลงหรือ CPA ได้เพื่อเป็นการยืนยันความครบถ้วนของข้อมูล ทั้งนี้ ลายมือชื่ออิเล็กทรอนิกส์ที่จะใช้ลงลายมือชื่อใน CPA หรือ CPP จะต้องสอดคล้องตามข้อกำหนด W3C Recommendation: XML Signature Syntax and Processing

รายการข้อมูล Signature จะถูกสร้างขึ้นจากลายมือชื่อตั้งแต่หนึ่งถึงสามรายการ ซึ่ง CPA สามารถมีการลงลายมือชื่อโดยหนึ่งหน่วยงานหรือทั้งสองหน่วยงานก็ได้ อย่างไรก็ตาม แนะนำว่าควรมีการลงลายมือชื่อโดยหน่วยงานทั้งสองหน่วยงาน ซึ่งกระบวนการลงลายมือชื่อจะเริ่มจากหน่วยงานหนึ่งลงลายมือชื่อก่อน จากนั้นอีกหน่วยงานจะลงลายมือชื่อต่อจากลายมือชื่อของหน่วยงานแรก ทั้งนี้ CPA ที่เป็นผลลัพธ์จากการลงลายมือชื่อโดยทั้งสองหน่วยงานอาจจะมีการลงลายมือชื่อโดยหน่วยงานรับรอง (notary) อีกทีหนึ่ง

6.3.2.9 Comment

รายละเอียดของรายการ Packaging เช่นเดียวกับหัวข้อ 6.3.1.5

6.4 ebXML Message Service Specification

ebXML Message Service (ebMS) Specification มีวัตถุประสงค์หลักเพื่ออำนวยความสะดวกในการแลกเปลี่ยนข้อความภายใต้กรอบแนวทางของ XML โดยข้อความที่จะแลกเปลี่ยน ซึ่งเรียกว่า ‘payload’ นั้นไม่จำเป็นต้องอยู่ในรูปแบบข้อความ XML ดังนั้น ebMS จึงสามารถใช้นำส่งข้อความในรูปแบบใดๆ ก็ได้ นอกจากนี้ ebXML รองรับการแลกเปลี่ยนข้อความผ่านโพรโทคอลการติดต่อสื่อสารที่หลากหลาย (เช่น HTTP, SMTP, FTP เป็นต้น) [6]

ebMS เป็นการกำหนดชุดของส่วนขยาย (Extension) ที่มีการแบ่งเป็นชั้นๆ เพิ่มเติมจากส่วนฐานที่เป็นข้อกำหนดของ Simple Object Access Protocol (SOAP) และ SOAP Messages with Attachments นอกจากนี้ ebMS จะกำหนดคุณสมบัติด้านความมั่นคงปลอดภัยและความน่าเชื่อถือที่จำเป็นในการรับส่งข้อความ ซึ่งคุณสมบัติด้านความมั่นคงปลอดภัยและความน่าเชื่อถือเหล่านี้จะไม่มีอยู่ในข้อกำหนดของ SOAP [6]

6.4.1 ข้อกำหนดของ ebXML Message Service (ebMS)

ebMS กำหนดโครงสร้างข้อความ ebXML ที่ใช้บรรจุข้อความทางธุรกิจ (payload) สำหรับการรับส่งระหว่างหน่วยงานที่เกี่ยวข้อง และกำหนดพฤติกรรมของซอฟต์แวร์ที่ใช้ในการรับส่งข้อความ (Message Service Handler) ผ่านโพรโทคอลการติดต่อสื่อสาร ทั้งนี้ ข้อกำหนดของ ebMS สามารถแบ่งได้เป็น 2 ประเภท คือ ส่วนการทำงานหลัก (Core Functionality) และคุณสมบัติเพิ่มเติม (Additional Features) โดยมีรายละเอียดดังนี้

<u>ส่วนการทำงานหลัก (Core Functionality)</u>

6.4.1.1 Packaging Specification

Packaging Specification เป็นคำอธิบายวิธีการบรรจุข้อความ ebXML และส่วนประกอบที่เกี่ยวข้องในโครงสร้างข้อความที่สามารถส่งด้วยโพรโทคอลการติดต่อสื่อสารต่างๆ โดยสามารถดูตัวอย่างของข้อความ ebXML ที่ส่งผ่านโพรโทคอล HTTP ได้ที่หัวข้อ 6.4.2

รายละเอียดของ Packaging Specification เป็นไปตาม ISO/TS 15000-2:2004 หัวข้อ 2.1

6.4.1.2 ebXML SOAP Envelope Extension

ebXML SOAP Envelope Extension เป็นข้อกำหนดสำหรับชุดของส่วนขยาย (Extension) ให้กับข้อความ SOAP Message โดยข้อกำหนดของ ebMS ในส่วนการทำงานหลัก (Core Functionality) สามารถแสดงได้เป็นรายการข้อมูลของ ebXML SOAP Envelope Extension ดังนี้

ตารางที่ 5 รายการข้อมูลของ ebXML SOAP Envelope Extension

รายการข้อมูล	ความจำเป็นต้องมี	อ้างอิงรายละเอียด
MessageHeader	[1..1]	ISO/TS 15000-2:2004 หัวข้อ 3.1
Manifest	[0..1]	ISO/TS 15000-2:2004 หัวข้อ 3.2
Signature (ใน Security Module)	[0..n]	ISO/TS 15000-2:2004 หัวข้อ 4.1
ErrorList (ใน Error Handling Module)	[0..1]	ISO/TS 15000-2:2004 หัวข้อ 4.2
SyncReply (ใน Sync Reply Module)	[0..1]	ISO/TS 15000-2:2004 หัวข้อ 4.3

ebXML SOAP Envelope Extension แบ่งออกเป็น 2 ส่วน ได้แก่ ebXML SOAP Header Extension ซึ่งเป็นส่วนขยายของ SOAP Header และ ebXML SOAP Body Extension ซึ่งเป็นส่วนขยายของ SOAP Body โดยมีรายการข้อมูลที่สำคัญ ดังนี้

(1) ebXML SOAP Header Extension มีรายการข้อมูล MessageHeader ซึ่งประกอบด้วยรายการข้อมูลย่อยต่างๆ ดังนี้

รายการข้อมูลย่อยของ MessageHeader	ความจำเป็นต้องมี
From	[1..1]
To	[1..1]
CPAId	[1..1]
ConversationId	[1..1]
Service	[1..1]
Action	[1..1]
MessageData	[1..1]
DuplicateElimination	[0..1]
Description	[0..n]

(1.1) From เป็นรายการข้อมูลสำหรับระบุผู้ส่งข้อความ ประกอบด้วย PartyId และ Role ซึ่งจะมีค่าเหมือนกันกับค่าใน CPA

(1.2) To เป็นรายการข้อมูลสำหรับระบุผู้รับข้อความ ประกอบด้วย PartyId และ Role ซึ่งจะมีค่าเหมือนกันกับค่าใน CPA

(1.3) CPAId เป็นรายการข้อมูลสำหรับรหัสอ้างอิงของความตกลงในการแลกเปลี่ยนข้อความ (CPA)

(1.4) ConversationId เป็นรายการข้อมูลสำหรับรหัสอ้างอิงของชุดข้อความที่มีการสนทนา (conversation) หรือการแลกเปลี่ยนระหว่างสองหน่วยงาน

(1.5) Service เป็นรายการข้อมูลสำหรับระบุบริการ (Service) เพื่อให้ผู้ส่งข้อความและผู้รับข้อความใช้อ้างอิงตรงกัน เช่น SupplierOrderProcessing

(1.6) Action เป็นรายการข้อมูลสำหรับระบุการดำเนินการ (Action) ที่อยู่ในบริการ โดย Action จะมีความเอกลักษณ์ใน Service แต่ละบริการ เช่น NewOrder

(1.7) MessageData เป็นรายการข้อมูลสำหรับวิธีการในการระบุข้อความ XML ประกอบด้วย MessageId, Timestamp, RefToMessageId และ TimeToLive

(1.8) DuplicateElimination เป็นรายการข้อมูลสำหรับให้ Message Service Handler ของผู้ส่งข้อความแจ้งไปยัง Message Service Handler ของผู้รับข้อความ เพื่อให้ตรวจสอบความซ้ำซ้อนของข้อความที่ได้รับ

(1.9) Description เป็นรายการข้อมูลสำหรับคำอธิบายวัตถุประสงค์หรือเจตนาของข้อความที่สามารถอ่านเข้าใจได้โดยบุคคล

นอกจากรายการข้อมูล MessageHeader แล้ว ebXML SOAP Header Extension อาจจะมีรายการข้อมูลอื่นๆ ที่เป็นคุณสมบัติด้านความมั่นคงปลอดภัยและความน่าเชื่อถือที่จำเป็นในการรับส่งข้อความตามข้อกำหนดของของ ebMS ได้แก่ รายการข้อมูล Signature (ใน Security Module) ErrorList (ใน Error Handling Module) และ SyncReply (ใน Sync Reply Module)

(2) ebXML SOAP Body Extension มีรายการข้อมูล Manifest ที่ชี้ไปยังข้อมูลใดๆ ที่อยู่ใน ebXML Payload Container หรือที่อื่น เช่น บนเว็บไซต์

รายละเอียดของ ebXML SOAP Envelope Extension เป็นไปตาม ISO/TS 15000-2:2004 หัวข้อ 2.3

6.4.1.3 Security Module

Security Module เป็นข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับข้อความ ebXML ทั้งนี้ Security Module จะมีรายการข้อมูล Signature ซึ่งประกอบด้วยลายมือชื่ออิเล็กทรอนิกส์ที่สอดคล้องตามข้อกำหนด W3C Recommendation: XML Signature Syntax and Processing สำหรับใช้ลงลายมือชื่อในข้อมูลที่เกี่ยวข้องกับข้อความ ebXML เพื่อป้องกันความเสี่ยงด้านความมั่นคงปลอดภัยต่างๆ

6.4.1.4 Error Handling Module

Error Handling Module เป็นคำอธิบายวิธีการที่ Message Service Handler ใช้ในการรายงานข้อผิดพลาดที่ตรวจพบในข้อความ ebXML ไปยัง Message Service Handler อีกอันหนึ่ง ทั้งนี้ Error Handling Module จะมีรายการข้อมูล ErrorList ซึ่งประกอบด้วยรายการข้อผิดพลาดที่มีการตรวจพบในข้อความ ebXML ก่อนหน้านี้ เฉพาะกรณีที่มีการรายงานข้อผิดพลาดหรือคำเตือนของข้อความก่อนหน้าเท่านั้น

6.4.1.5 Sync Reply Module

Sync Reply Module เป็นการบ่งบอกไปให้ Message Service Handler อันถัดไปทราบว่าคำตอบกลับ (reply) จะถูกส่งกลับมาพร้อมกันหรือไม่ ทั้งนี้ Sync Reply Module จะมีรายการข้อมูล SyncReply ที่ผู้ส่งข้อความใช้บ่งบอกไปยังผู้รับข้อความเพื่อจะให้มีการตอบกลับสถานะของการส่งข้อมูล

<u>คุณสมบัติเพิ่มเติม (Additional Features)</u>

6.4.1.6 Reliable Messaging Module

Reliable Messaging Module เป็นการกำหนดโพรโทคอลการทำงานร่วมกัน เพื่อให้ Message Service Handler ของสองหน่วยงานสามารถแลกเปลี่ยนข้อความระหว่างกันได้อย่างน่าเชื่อถือ ด้วยการใช้ข้อความตอบรับ (acknowledgement) การส่งข้อความเดิมซ้ำ (retry) จนกว่าจะตอบรับ และวิธีการตรวจสอบและปฏิเสธความซ้ำซ้อนของข้อความ (duplicate detection and elimination) เพื่อให้หน่วยงานได้รับข้อความเพียงครั้งเดียวเท่านั้น

รายละเอียดของ Reliable Messaging Module เป็นไปตาม ISO/TS 15000-2:2004 หัวข้อ 6

6.4.1.7 Message Status Service

Message Status Service อธิบายบริการที่ส่งข้อความไปยัง Message Service Handler เพื่อขอทราบสถานะของข้อความที่ส่งไปก่อนหน้า ซึ่ง Message Status Service จะประกอบด้วยข้อความ Message Status Request สำหรับการขอทราบสถานะของข้อความใดๆ ที่ส่งไปก่อนหน้า และข้อความ Message Status Response สำหรับการตอบสถานะของข้อความตามที่ขอมา โดยมีสถานะของข้อความ ได้แก่ UnAuthorized, NotRecognized, Received, Processed และ Forwarded

รายละเอียดของ Message Status Service เป็นไปตาม ISO/TS 15000-2:2004 หัวข้อ 7

6.4.1.8 Message Service Handler Ping Service

Message Service Handler Ping Service อธิบายบริการที่ Message Service Handler อันหนึ่งใช้ตรวจสอบ Message Service Handler อีกอันหนึ่งว่ากำลังทำงานอยู่หรือไม่ โดย Message Service Handler จะส่งข้อความ Message Service Handler Ping ไปยัง Message Service Handler อีกอันหนึ่ง หาก Message Service Handler ที่ได้รับข้อความ Ping ดังกล่าวกำลังทำงานอยู่ก็จะส่งข้อความ Message Service Handler Pong ตอบกลับมา

รายละเอียดของ Message Service Handler Ping Service เป็นไปตาม ISO/TS 15000-2:2004 หัวข้อ 8

6.4.1.9 Message Order Module

Message Order Module ช่วยให้ข้อความที่ส่งมายังผู้รับข้อความมีการเรียงเป็นลำดับที่เฉพาะเจาะจง โดย Message Order Module จะใช้รายการข้อมูล MessageOrder ในการระบุลำดับของข้อความที่ส่งแต่ละข้อความ เพื่อให้ Message Service Handler ที่รับข้อความสามารถจัดลำดับก่อนหลังของข้อความทั้งหมดได้

รายละเอียดของ Message Order Module เป็นไปตาม ISO/TS 15000-2:2004 หัวข้อ 9

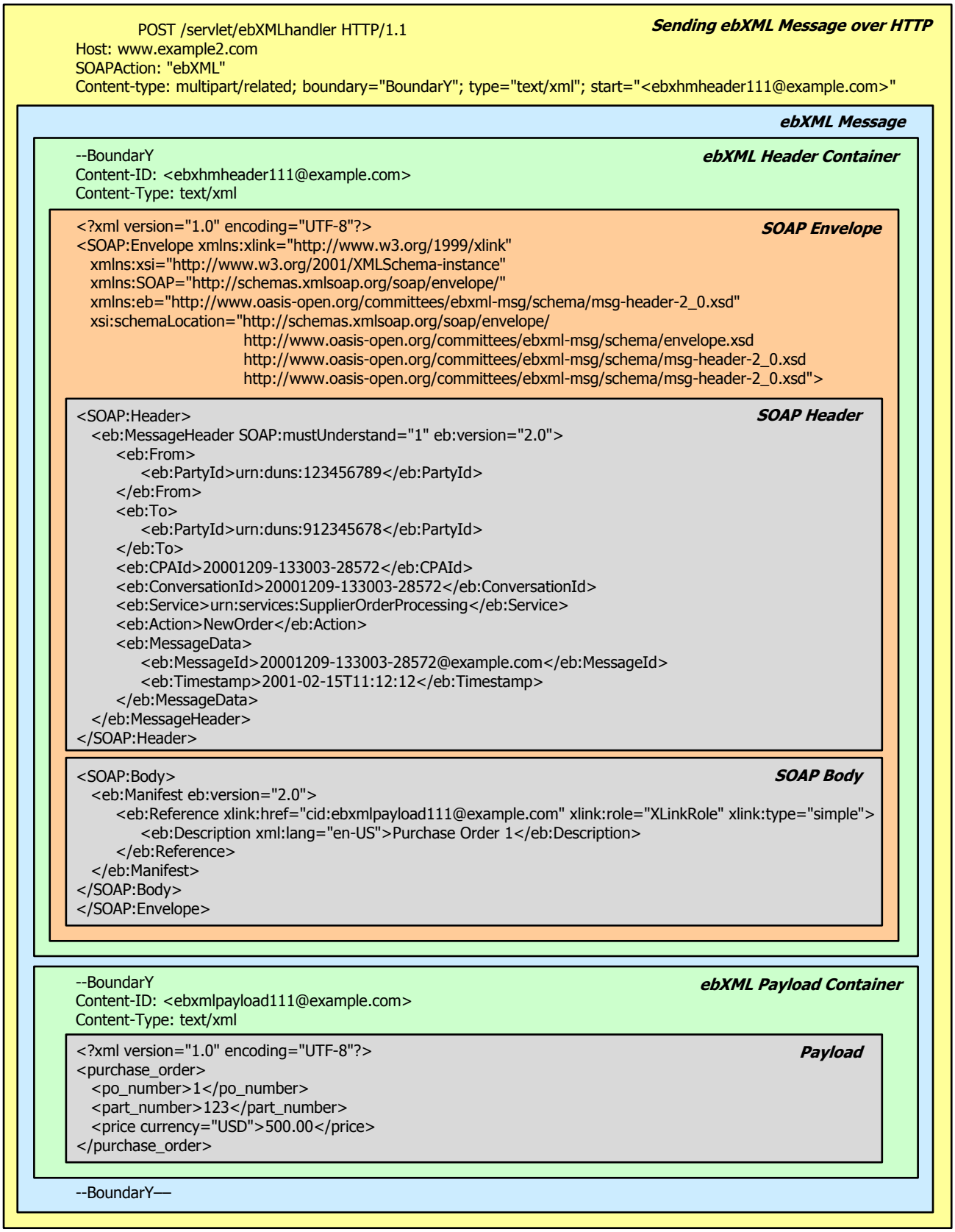
6.4.1.10 Multi-Hop Module

Multi-Hop Module เป็นกระบวนการในการนำส่งข้อความผ่าน Message Service Handler ที่อยู่ระหว่างกลางตั้งแต่หนึ่งอันขึ้นไป โดย Message Service Handler ที่อยู่ระหว่างกลางจะทำหน้าที่เก็บรักษาและส่งต่อข้อความ (Store-and-Forward) หรืออาจมีส่วนร่วมในการประมวลผลข้อมูล เช่น การลงประทับเวลาอิเล็กทรอนิกส์ (timestamp service) โดยผู้รับรองที่เชื่อถือได้

รายละเอียดของ Multi-Hop Module เป็นไปตาม ISO/TS 15000-2:2004 หัวข้อ 10

6.4.2 ตัวอย่างของข้อความ ebXML

ตัวอย่างของข้อความ ebXML ที่ส่งผ่านโพรโทคอลการติดต่อสื่อสารแบบ HTTP แสดงได้ตามนี้



รูปที่ 14 ตัวอย่างของข้อความ ebXML

เอกสารอ้างอิง

[1] “หลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของ,” ใน *ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ข้อมูลอิเล็กทรอนิกส์ พ.ศ. 2553*, 2553.

[2] “PART II: XML SCHEMA DESIGN GUIDE,” ใน *XML SCHEMA DESIGN AND MANAGEMENT GUIDE*, 1.4 บ.ก., The Government of the Hong Kong Special Administrative Region, 2015.

[3] “ISO 14533-2:2012, Processes, data elements and documents in commerce, industry and administration -- Long term signature profiles -- Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES),” *International Standard Organization,* 2012.

[4] “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.

[5] “ISO/TS 15000-1:2004, Electronic business eXtensible Markup Language (ebXML) – Part 1: Collaboration-Protocol Profile and Agreement Specification (ebCPP),” *ISO (International Organization for Standardization),* 2004.

[6] “ISO/TS 15000-2:2004, Electronic business eXtensible Markup Language (ebXML) – Part 2: Message service specification (ebMS),” *ISO (International Organization for Standardization),* 2004.

[7] “Introduction to XML,” W3Schools, [ออนไลน์]. Available: http://www.w3schools.com/xml/xml_whatis.asp.

[8] “ถาม-ตอบ,” สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) , [ออนไลน์]. Available: https://data.go.th/Faq.aspx?AspxAutoDetectCookieSupport=1.

[9] “XML Syntax Rules,” W3Schools, [ออนไลน์]. Available: http://www.w3schools.com/xml/xml_syntax.asp.

[10] “XML Naming and Design Rules Technical Specification Version 3,” *UN/CEFACT,* 2009.

[11] “UN/CEFACT STANDARD BUSINESS DOCUMENT HEADER Technical Specification,” UN/CEFACT, 2004.

[12] The World Wide Web Consortium (W3C), “XML Advanced Electronic Signatures (XAdES),” 20 February 2003. [ออนไลน์]. Available: https://www.w3.org/TR/XAdES/#Syntax_for_XAdES-L_form_The_CertificateValues_element.

[13] “About ebXML,” ebXML, [ออนไลน์]. Available: http://www.ebxml.org/geninfo.htm.

[14] “About CEFACT,” UN/CEFACT, [ออนไลน์]. Available: http://www.unece.org/cefact/.

[15] “ebXML Business Process Specification Schema Technical Specification v2.0.4,” ใน *OASIS Standard*, 2006.

[16] “ISO 15000-5:2014, Electronic business eXtensible Markup Language (ebXML) – Part 5: Core Components Specification (CCS),” *ISO (International Organization for Standardization),* 2014.

[17] “ISO/TS 15000-3:2004, Electronic business eXtensible Markup Language (ebXML) – Part 3: Registry Information Model Specification (ebRIM),” *ISO (International Organization for Standardization),* 2004.

[18] “ISO/TS 15000-4:2004, Electronic business eXtensible Markup Language (ebXML) – Part 4: Registry Services Specification (ebRS),” *ISO (International Organization for Standardization),* 2004.

[19] “PART I: OVERVIEW,” ใน *XML SCHEMA DESIGN AND MANAGEMENT GUIDE*, 1.4 บ.ก., The Government of the Hong Kong Special Administrative Region, 2015, p. March.

[20] “Electronic Signature and Infrastructures; XML Advanced Electronic Signature (XAdES) v1.4.2 (2010-12),” *ETSI (Electronic Telecommunications Standard Institute),* 2010.

[21] “RFC 4998: Evidence Record Syntax (ERS),” IETF (The Internet Engineering Task Force), 2007. [ออนไลน์]. Available: https://tools.ietf.org/html/rfc4998.

[22] “RFC5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,” IETF (The Internet Engineering Task Force), MAY 2008. [ออนไลน์]. Available: https://www.ietf.org/rfc/rfc5280.txt.

[23] “RFC 6283 Extensible Markup Language Evidence Record Syntax (XMLERS),” IETF (Internet Engineering Task Force), JULY 2011. [ออนไลน์]. Available: https://tools.ietf.org/html/rfc6283.

[24] “ebXML Technical Architecture Specification v1.0.4,” *ebXML Technical Architecture Project Team,* 2001.