สมอ./ศอ.พว./FDNS (1)
มีนาคม 2558

ห้ามใช้หรือยึดร่างนี้เป็นมาตรฐาน
มาตรฐานฉบับสมบูรณ์จะมีประกาศในราชกิจจานุเบกษา

ร่าง

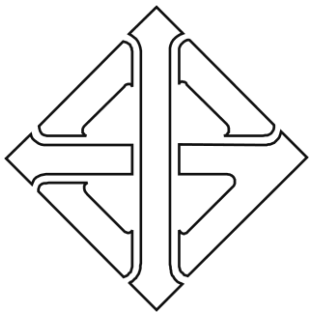
มาตรฐานผลิตภัณฑ์อุตสาหกรรม

สิ่งพิมพ์อิเล็กทรอนิกส์
เล่ม 3 ข้อกำหนดรูปแบบโอเพ่นคอนเทนเนอร์

ELECTRONIC PUBLICATION
PART 3: OPEN CONTAINER FORMAT

สำหรับเสนอคณะกรรมการพิจารณาร่างมาตรฐานผลิตภัณฑ์อุตสาหกรรม

สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม
กระทรวงอุตสาหกรรม ถนนพระรามที่ 6 กรุงเทพฯ 10400
โทรศัพท์ 0 2202-33XX



มาตรฐานผลิตภัณฑ์อุตสาหกรรม

THAI INDUSTRIAL STANDARD

มอก. XXXX–25YY

สิ่งพิมพ์อิเล็กทรอนิกส์

เล่ม 3 ข้อกำหนดรูปแบบโอเพ่นคอนเทนเนอร์

ELECTRONIC PUBLICATION

PART 3: OPEN CONTAINER FORMAT

สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม

กระทรวงอุตสาหกรรม ICS 91.160.10 ISBN

มาตรฐานผลิตภัณฑ์อุตสาหกรรม

สิ่งพิมพ์อิเล็กทรอนิกส์

เล่ม 3 ข้อกำหนดรูปแบบโอเพ่นคอนเทนเนอร์

มอก. XXXX–25YY

สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม
กระทรวงอุตสาหกรรม ถนนพระรามที่ 6 กรุงเทพฯ 10400
โทรศัพท์ 0 2202 3300

ประกาศในราชกิจจานุเบกษา ฉบับประกาศและงานทั่วไป เล่ม ตอนพิเศษ
วันที่ พุทธศักราช 25YY

คณะผู้จัดทำร่างมาตรฐาน
มาตรฐานสิ่งพิมพ์อิเล็กทรอนิกส์

ประธาน

นางสาววันทนีย์ พันธชาติ	ผู้ทรงคุณวุฒิ

กรรมการ

นายธรรม จตุนาม	วิทยาลัยราชสุดา มหาวิทยาลัยมหิดล
นายบุญเลิศ อรุณพิบูลย์	สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
นางสมศรี หอกันยา	กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
นางสาวนิติมา จิตต์จำนงค์	สำนักงานคณะกรรมการการอุดมศึกษา
นายจตุพล หนูท่าทอง	สมาคมคนตาบอดแห่งประเทศไทย
นายดนุพล กิ่งสุคนธ์	สมาคมผู้จัดพิมพ์และผู้จำหน่ายหนังสือแห่งประเทศไทย
นายประสิทธิ์ คล่องงูเหลือม	ชมรมการจัดพิมพ์อิเล็กทรอนิกไทย
นายพิสิษฐ์ วงษ์พิไลวัฒน์	
นายสุรพันธ์ เมฆนาวิน	ผู้ทรงคุณวุฒิ
นายณัฐนันท์ ทัดพิทักษ์กุล	ผู้ทรงคุณวุฒิ
นายธนาคม ตาฬวัฒน์	ผู้ทรงคุณวุฒิ
นายน้ำหนึ่ง มิตรสมาน	ผู้ทรงคุณวุฒิ
นายธนวัฒน์ ภูลายเหลือง	สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม

กรรมการและเลขานุการ

นางกมลพรรณ พันพึ่ง	ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
นางสาวสุภาพันธุ์ เกตุคำ	
นางกุลธิดา เอื้อมลฉัตร	

เทคโนโลยีมีการเปลี่ยนแปลงไปอย่างรวดเร็ว การจัดทำรูปแบบข้อมูลข่าวสารได้ปรับตัวให้เป็นไปตามเทคโนโลยีใหม่ๆ มากขึ้น รวมถึงหนังสือ ซึ่งแต่เดิมเป็นรูปแบบของกระดาษ ได้เปลี่ยนมาเป็นระบบอิเล็กทรอนิกส์กันมากขึ้น เพื่อความสะดวก รวดเร็วในการเข้าถึงข้อมูลด้วยอุปกรณ์พกพาแบบต่างๆ เพื่อให้สามารถใช้งานหนังสืออิเล็กทรอนิกส์ร่วมกันได้กับอุปกรณ์แบบต่างๆ ได้ ดังนั้นเพื่อเป็นการส่งเสริมอุตสาหกรรมประเภทนี้ และเพื่อให้ผลิตภัณฑ์นี้มีคุณลักษณะและคุณสมบัติถูกต้องตามหลักวิชาการ จึงกำหนดมาตรฐานผลิตภัณฑ์อุตสาหกรรมสิ่งพิมพ์อิเล็กทรอนิกส์ขึ้น

มาตรฐานผลิตภัณฑ์อุตสาหกรรมนี้ จัดทำขึ้นตามความร่วมมือด้านการกำหนดมาตรฐานระหว่างสำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรมกับศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ที่ตั้งอยู่เลขที่ 112 อุทยานวิทยาศาสตร์ประเทศไทย ถนนพหลโยธิน ตำบลคลองหนึ่ง อำเภอคลองหลวง จังหวัดปทุมธานี 12120 โทรศัพท์ 0 2564 6900 www.nectec.or.th และใช้ข้อมูลจากผู้ทำ ผู้ใช้ และเอกสารต่อไปนี้ เป็นแนวทาง

เอกสาร EPUB Open Container Format 3.0.1 โดยองค์กร International Digital Publishing Forum (IDPF) ปี 2014

มาตรฐานผลิตภัณฑ์อุตสาหกรรมนี้เป็นเล่มหนึ่งในอนุกรมมาตรฐานสิ่งพิมพ์อิเล็กทรอนิกส์ โดยสามารถอ่านและเข้าใจได้ เมื่อใช้ประกอบกันในอนุกรมมาตรฐานสิ่งพิมพ์อิเล็กทรอนิกส์ ประกอบด้วย

1. มาตรฐานผลิตภัณฑ์อุตสาหกรรมสิ่งพิมพ์อิเล็กทรอนิกส์ เล่ม 1 ข้อกำหนดการจัดทำสิ่งพิมพ์อิเล็กทรอนิกส์
2. มาตรฐานผลิตภัณฑ์อุตสาหกรรมสิ่งพิมพ์อิเล็กทรอนิกส์ เล่ม 2 ข้อกำหนดการจัดเอกสารเนื้อหาสิ่งพิมพ์อิเล็กทรอนิกส์
3. มาตรฐานผลิตภัณฑ์อุตสาหกรรมสิ่งพิมพ์อิเล็กทรอนิกส์ เล่ม 3 ข้อกำหนดรูปแบบโอเพ่นคอนเทนเนอร์
4. มาตรฐานผลิตภัณฑ์อุตสาหกรรมสิ่งพิมพ์อิเล็กทรอนิกส์ เล่ม 4 ข้อกำหนดการซ้อนทับของสื่อ

คณะกรรมการมาตรฐานผลิตภัณฑ์อุตสาหกรรมได้พิจารณามาตรฐานนี้แล้ว เห็นสมควรเสนอรัฐมนตรีประกาศตามมาตรา 15 แห่งพระราชบัญญัติมาตรฐานผลิตภัณฑ์อุตสาหกรรม พ.ศ. 2511

สารบัญ

	หน้า
1. ขอบข่าย	1
2. บทนิยาม	1
3. ภาพรวม	1
4. คอนเทนเนอร์แอบสแตรคท์ของโอซีเอฟ	2
5. คอนเทนเนอร์ซิปของโอซีเอฟ	14
6. การพรางทรัพยากร	16
ภาคผนวก ก. ผังเอกสาร	19
ภาคผนวก ข. ตัวอย่าง	21
ภาคผนวก ค. ชนิดสื่อ application/epub+zip	28

ประกาศกระทรวงอุตสาหกรรม

ฉบับที่ (พ.ศ. 2554)

ออกตามความในพระราชบัญญัติมาตรฐานผลิตภัณฑ์อุตสาหกรรม

พ.ศ. 2511

เรื่อง กำหนดมาตรฐานผลิตภัณฑ์อุตสาหกรรม

สิ่งพิมพ์อิเล็กทรอนิกส์ เล่ม 3 ข้อกำหนดรูปแบบโอเพ่นคอนเทนเนอร์

อาศัยอำนาจตามความในมาตรา 15 แห่งพระราชบัญญัติมาตรฐานผลิตภัณฑ์อุตสาหกรรม พ.ศ. 2511 รัฐมนตรีว่าการกระทรวงอุตสาหกรรมออกประกาศกำหนดมาตรฐานผลิตภัณฑ์อุตสาหกรรม สิ่งพิมพ์อิเล็กทรอนิกส์ เล่ม 3 ข้อกำหนดรูปแบบคอนเทนเนอร์เปิด มาตรฐานเลขที่ มอก. XXXX-25YY ไว้ ดังมีรายละเอียดต่อท้ายประกาศนี้

ประกาศ ณ วันที่ พ.ศ. 2559

รัฐมนตรีว่าการกระทรวงอุตสาหกรรม

มาตรฐานผลิตภัณฑ์อุตสาหกรรม
สิ่งพิมพ์อิเล็กทรอนิกส์ เล่ม 3
ข้อกำหนดรูปแบบคอนเทนเนอร์เปิด

1. ขอบข่าย

มาตรฐานผลิตภัณฑ์อุตสาหกรรมนี้กำหนดรูปแบบไฟล์ (file format) และรูปแบบการประมวลผลสำหรับห่อหุ้มชุดทรัพยากรที่เกี่ยวข้องซึ่งประกอบเป็นสิ่งพิมพ์อิเล็กทรอนิกส์ เข้าเป็นคอนเทนเนอร์ไฟล์เดียว

2. บทนิยาม

ความหมายของคำที่ใช้ในมาตรฐานผลิตภัณฑ์อุตสาหกรรมนี้ ให้เป็นไปตาม มอก. XXXX-25YY เล่ม 1 และ มอก. XXXX-25YY เล่ม 2 และดังต่อไปนี้

2.1 ตัวประมวลผลโอซีเอฟ (OCF processor) หมายถึง โปรแกรมประยุกต์ที่ประมวลผลคอนเทนเนอร์สิ่งพิมพ์อิเล็กทรอนิกส์ตามที่กำหนดในมาตรฐานผลิตภัณฑ์อุตสาหกรรมนี้

2.2 ไดเรกทอรี่ราก (root directory) หมายถึง ไดเรกทอรี่ที่เป็นฐานของระบบไฟล์คอนเทนเนอร์แอบสแตรคท์ ไดเรกทอรี่นี้มีลักษณะเป็นไดเรอทอรี่เสมือนจริง กล่าวคือระบบการอ่านอาจสร้างหรือไม่สร้างไดเรกทอรี่รากเชิงกายภาพสำหรับเนื้อหาของคอนเทนเนอร์แอบสแตรคท์ถ้าเนื้อหานั้นไม่ได้ถูกซิป

3. ภาพรวม

เนื้อหาส่วนนี้เป็นข้อแนะนำ

รูปแบบคอนเทนเนอร์เปิด (Open Container Format: OCF) ต่อไปนี้จะเรียกว่า โอซีเอฟ ซึ่งเป็นเทคโนโลยีคอนเทนเนอร์ที่จำเป็นสำหรับสิ่งพิมพ์อิเล็กทรอนิกส์ โอซีเอฟอาจมีบทบาทในขั้นตอนงานต่อไปนี้

- ระหว่างขั้นตอนเตรียมการในการผลิตสิ่งพิมพ์อิเล็กทรอนิกส์ อาจมีการใช้โอซีเอฟเป็นรูปแบบคอนเทนเนอร์เมื่อแลกเปลี่ยนสิ่งพิมพ์ที่อยู่ระหว่างการจัดทำระหว่างบุคคลและ/หรือองค์กรต่าง ๆ
- เมื่อมอบสิ่งพิมพ์อิเล็กทรอนิกส์จากผู้จัดพิมพ์หรือผู้แปลงให้กับช่องทางแจกจ่ายหรือจัดจำหน่าย โอซีเอฟคือรูปแบบคอนเทนเนอร์ที่แนะนำให้ใช้เป็นรูปแบบการขนส่ง
- เมื่อส่งมอบสิ่งพิมพ์ฉบับสมบูรณ์ให้กับระบบการอ่านสิ่งพิมพ์อิเล็กทรอนิกส์หรือผู้ใช้ โอซีเอฟคือรูปแบบที่จำเป็นสำหรับคอนเทนเนอร์ซึ่งเก็บสินทรัพย์ทั้งหมดที่ประกอบขึ้นเป็นสิ่งพิมพ์อิเล็กทรอนิกส์

ข้อกำหนดโอซีเอฟอธิบายกฎสำหรับการวางโครงสร้างชุดรวมไฟล์ในแอบสแตรคท์ ซึ่งเรียกว่า"คอนเทนเนอร์แอบสแตรคท์" และกำหนดกฎสำหรับการแสดงของคอนเทนเนอร์แอบสแตรคท์นี้ภายในอาร์ไคฝ์ซิป (ZIP archive) ซึ่งเรียกว่า “คอนเทนเนอร์กายภาพ" กฎสำหรับคอนเทนเนอร์กายภาพแบบซิปสร้างขึ้นโดยใช้เทคโนโลยีซิปซึ่งนำมาใช้ในมาตรฐานโอดีเอฟโอเพ่นด็อกคูเม้นฟอร์แมท **[ODF]** โอซีเอฟกำหนดวิธีการมาตรฐานในการพรางทรัพยากรแบบฝัง เช่น ฟอนต์ สำหรับสิ่งพิมพ์อิเล็กทรอนิกส์ที่ต้องการฟังก์ชันนี้ด้วย

3.1 การปฏิบัติตามข้อกำหนดสำหรับเนื้อหา

- คอนเทนเนอร์แอบสแตรคท์ของโอซีเอฟต้องเป็นไปตามข้อบังคับที่อธิบายในหัวข้อ 3. คอนเทนเนอร์แอบสแตรคท์ของโอซีเอฟ
- คอนเทนเนอร์ซิปของโอซีเอฟ (OCF ZIP container) (หรือที่เรียกว่าคอนเทนเนอร์ของสิ่งพิมพ์อิเล็กทรอนิกส์) ต้องเป็นไปตามข้อบังคับที่อธิบายในหัวข้อ 4. คอนเทนเนอร์ซิปของโอซีเอฟ

3.2 การปฏิบัติตามข้อกำหนดสำหรับระบบการอ่าน

- ต้องประมวลผลคอนเทนเนอร์ซิปของโอซีเอฟตามที่กำหนดตามข้อบังคับสำหรับระบบการอ่านในหัวข้อ 4. คอนเทนเนอร์ซิปของโอซีเอฟ
- ถ้ามีวิวพอร์ตต้องรองรับการลบการพรางทรัพยากรตามที่ระบุในหัวข้อ 5. การพรางทรัพยากร

4. คอนเทนเนอร์แอบสแตรคท์ของโอซีเอฟ

4.1 ภาพรวม

เนื้อหาส่วนนี้เป็นข้อแนะนำ

คอนเทนเนอร์แอบสแตรคท์ของโอซีเอฟกำหนดรูปแบบระบบไฟล์สำหรับเนื้อหาของคอนเทนเนอร์ รูปแบบระบบไฟล์ใช้ไดเรกทอรี่รากร่วมเพียงไดเรกทอรี่เดียวสำหรับเนื้อหาทั้งหมดของคอนเทนเนอร์ ทรัพยากรทั้งหมดที่ไม่ใช่แบบระยะไกล (non-remote) สำหรับเรนดิชั่นแบบฝังจะถูกจัดเก็บอยู่ภายในไดเรกทอรี่ที่ตั้งต้นจากไดเรกทอรี่รากของคอนเทนเนอร์ แม้ว่าไม่มีโครงสร้างระบบไฟล์ที่เป็นข้อบังคับโดยเฉพาะรูปแบบระบบไฟล์ยังมีไดเรกทอรี่บังคับชื่อ ***META-INF*** ด้วย ซึ่งเป็นลูกโดยตรงของไดเรกทอรี่รากของคอนเทนเนอร์ และใช้เพื่อจัดเก็บไฟล์พิเศษดังต่อไปนี้

container.xml [ต้องมี]	ระบุไฟล์ที่เป็นจุดเริ่มต้นของเรนดิชั่นแบบฝังของสิ่งพิมพ์อิเล็กทรอนิกส์แต่ละรายการ
signatures.xml [ทางเลือก]	บรรจุลายเซ็นอิเล็กทรอนิกส์สำหรับสินทรัพย์ต่างๆ
encryption.xml [ทางเลือก]	บรรจุข้อมูลเกี่ยวกับการเข้ารหัสของทรัพยากรสิ่งพิมพ์อิเล็กทรอนิกส์ (ต้องมีไฟล์นี้ถ้ามีการใช้การพราง)
metadata.xml [ทางเลือก]	ใช้เพื่อจัดเก็บเมทาดาตาเกี่ยวกับคอนเทนเนอร์ของสิ่งพิมพ์อิเล็กทรอนิกส์
rights.xml [ทางเลือก]	ใช้เพื่อจัดเก็บข้อมูลเกี่ยวกับสิทธิทางดิจิทัล
manifest.xml [ยินยอม]	รายชื่อแฟ้มของเนื้อหาคอนเทนเนอร์ตามที่ฟอร์แมทเอกสารแบบเปิด **[ODF]** อนุญาต

ข้อกำหนดการปฏิบัติทั้งหมดสำหรับไฟล์รูปแบบหลากหลายใน ***META-INF*** ปรากฏในหัวข้อ 4.5 ไดเรกทอรี่ META-INF

4.2 โครงสร้างไดเรกทอรี่และไฟล์

ระบบไฟล์เสมือนสำหรับคอนเทนเนอร์แอบสแตรคท์ของโอซีเอฟต้องมีไดเรกทอรี่รากร่วมเพียงไดเรกทอรี่เดียวสำหรับเนื้อหาทั้งหมดของคอนเทนเนอร์

คอนเทนเนอร์แอบสแตรคท์ของโอซีเอฟต้องรวมไดเรกทอรี่ชื่อ ***META-INF*** ซึ่งเป็นลูกโดยตรงของไดเรกทอรี่รากของคอนเทนเนอร์ ข้อกำหนดสำหรับเนื้อหาของไดเรกทอรี่อธิบายอยู่ในหัวข้อ 4.5 ไดเรกทอรี่ META-INF ชื่อไฟล์ ***minetype*** ในไดเรกทอรี่รากถูกสงวนไว้ใช้โดยคอนเทนเนอร์ซิปของโอซีเอฟ ดังอธิบายในหัวข้อ 4. คอนเทนเนอร์ซิปของโอซีเอฟ

ไฟล์อื่นทั้งหมดในคอนเทนเนอร์แอบสแตรคท์ของโอซีเอฟอาจอยู่ในตำแหน่งใดก็ได้ที่เป็นทายาทของไดเรกทอรี่รากของคอนเทนเนอร์ ยกเว้นภายในไดเรกทอรี่ ***META-INF***

เนื้อหาของสิ่งพิมพ์อิเล็กทรอนิกส์แต่ละชิ้นควรเก็บไว้ภายในไดเรกทอรี่ที่จัดไว้โดยเฉพาะของตนเองภายใต้รากของคอนเทนเนอร์

4.3 ไออาร์ไอสัมพัทธ์สำหรับอ้างอิงส่วนประกอบอื่น

ไฟล์ภายในคอนเทนเนอร์แอบสแตรคท์ของโอซีเอฟต้องอ้างอิงซึ่งกันและกันผ่านการอ้างอิงไออาร์ไอสัมพัทธ์ (ข้อกำหนดตัวระบุทรัพยากรที่เป็นสากล **[RFC3987]** และข้อกำหนดตัวระบุทรัพยากรยูนิฟอร์ม: ไวยากรณ์ทั่วไป **[RFC3986]**) ตัวอย่างเช่น ถ้าไฟล์ชื่อ chapter1.html อ้างถึงไฟล์รูปภาพชื่อ image1.jpg ที่อยู่ในไดเรกทอรี่เดียวกัน ดังนั้น chapter1.html อาจบรรจุ <img src="image1.jpg" alt="..." / > เป็นส่วนหนึ่งของเนื้อหา

สำหรับการอ้างอิงไออาร์ไอสัมพัทธ์ ไออาร์ไอฐาน **[RFC3986]** ถูกกำหนดโดยคุณลักษณะเฉพาะของภาษาที่เกี่ยวข้องสำหรับฟอร์แมทไฟล์ที่กำหนด ดังตัวอย่างคุณลักษณะเฉพาะซีเอสเอสระบุวิธีการที่การอ้างอิงไออาร์ไอสัมพัทธ์ทำงานในบริบทของสไตล์ชีทซีเอสเอสและการประกาศคุณสมบัติ สังเกตว่าคุณลักษณะเฉพาะของภาษาบางอย่างอ้างอิง RFC ที่เก่ากว่า **[RFC3987]** ซึ่งในกรณีเช่นนั้น จะปรับใช้ RFC ที่เก่ากว่าสำหรับเนื้อหาในภาษานั้น ๆ

ต่างกับคุณลักษณะเฉพาะทางภาษาส่วนใหญ่ ไออาร์ไอฐานสำหรับไฟล์ทั้งหมดภายในไดเรกทอรี่ ***META-INF*** ใช้ไดเรกทอรี่รากสำหรับคอนเทนเนอร์แอบสแตรคท์เป็นไออาร์ไอฐานโดยปริยาย ดังตัวอย่าง หาก META-INF/container.xml มีเนื้อหาต่อไปนี้

```
<?xml version="1.0"?>

<container version="1.0" xmlns="urn:oasis:names:tc:opendocument:xmlns:container">

        <rootfiles>

                <rootfile full-path="EPUB/Great Expectations.opf"

                        media-type="application/oebps-package+xml" />

        </rootfiles>

</container>
```

เส้นทาง EPUB/Great Expectations.opf สัมพันธ์กับไดเรกทอรี่รากของคอนเทนเนอร์แอบสแตรคท์ของโอซีเอฟและไม่สัมพันธ์กับไดเรกทอรี่ ***META-INF***

4.4 ชื่อไฟล์

คำศัพท์ชื่อไฟล์ (File Name) หมายถึง ชื่อของไฟล์ประเภทใดก็ได้ ไม่ว่าจะเป็นไดเรกทอรี่หรือไฟล์ทั่วไปภายในไดเรกทอรี่ภายในคอนเทนเนอร์แอบสแตรคท์ของโอซีเอฟ

สำหรับไดเรกทอรี่ภายในคอนเทนเนอร์แอบสแตรคท์ของโอซีเอฟ ชื่อเส้นทาง (Path Name) คือสายอักขระที่มีชื่อไฟล์ไดเรกทอรี่ทั้งหมดแบบเต็มเชื่อมต่อกับอักขระ / (U+002F) ซึ่งแบ่งชื่อไฟล์ไดเรกทอรี่ สำหรับไฟล์ภายในคอนเทนเนอร์แอบสแตรคท์ ชื่อเส้นทางคือสายอักขระที่มีชื่อไฟล์ไดเรกทอรีทั้งหมดที่เชื่อมต่อกันด้วยอักขระ / ซึ่งแบ่งชื่อไฟล์ไดเรกทอรี่ตามด้วยอักขระ / จากนั้นตามด้วยชื่อไฟล์ของไฟล์นั้น

ข้อจำกัดของชื่อไฟล์ที่บรรยายไว้ด้านล่างนี้อนุญาตให้ใช้ชื่อเส้นทางและชื่อไฟล์โดยไม่มีการดัดแปลงบนระบบปฏิบัติการที่มีการใช้งานอยู่ทั่วไป มาตรฐานผลิตภัณฑ์อุตสาหกรรมนี้ไม่ระบุว่าตัวประมวลผลโอซีเอฟซึ่งไม่สามารถแสดงชื่อไฟล์และเส้นทางของโอซีเอฟจะชดเชยความไม่เข้ากันนี้ได้อย่างไร

ในบริบทของคอนเทนเนอร์แอบสแตรคท์ของโอซีเอฟ ชื่อไฟล์และเส้นทางต้องเป็นไปตามเกณฑ์ ต่อไปนี้

- ชื่อไฟล์ต้องเข้ารหัสเป็นยูทีเอฟ-8 ตามมาตรฐานยูนิโค้ด รุ่น 5.0.0 **[Unicode]**
- ชื่อไฟล์ต้องไม่เกิน 255 ไบท์
- ชื่อเส้นทางสำหรับไดเรกทอรี่หรือไฟล์ภายในคอนเทนเนอร์แอบสแตรคท์ต้องไม่เกิน 65535 ไบท์
- ชื่อไฟล์ต้องไม่ใช้ตัวอักขระยูนิโค้ดต่อไปนี้ เนื่องจากอักขระเหล่านี้อาจไม่ได้การรองรับจากบางระบบปฏิบัติการที่มีใช้ทั่วไป
    - เครื่องหมายทับ: / (U+002F)
    - อัญประกาศ: " (U+0022)
    - ดอกจัน: * (U+002A)
    - มหัพภาค เมื่อใช้เป็นอักขระสุดท้าย: . (U+002E)
    - ทวิภาค: : (U+003A)
    - เครื่องหมายน้อยกว่า: < (U+003C)
    - เครื่องหมายมากกว่า: > (U+003E)
    - ปรัศนี: ? (U+003F)
    - เครื่องหมายทับกลับหลัง: \ (U+005C)
    - DEL (U+007F)
    - ช่วง C0 (U+0000 … U+001F)
    - ช่วง C1 (U+0080 … U+009F)

- บริเวณใช้งานส่วนตัว (U+E000 ... U+F8FF)
- ไม่ใช่อักขระในรูปแบบการนำเสนอภาษาอารบิก-A (U+FDDO ... U+FDEF)
- พิเศษ (U+FFF0 ... U+FFFF)
- แท็กและตัวเลือกตัวแปรเพิ่มเติม (U+E0000 ... U+E0FFF)
- บริเวณใช้งานส่วนตัวเพิ่มเติม-A (U+F0000 ... U+FFFFF)
- บริเวณใช้งานส่วนตัวเพิ่มเติม-B (U+100000 ... U+10FFFF)

- ตัวอักษรพิมพ์เล็กหรือตัวอักษรพิมพ์ใหญ่มีผลต่อชื่อไฟล์
- ชื่อไฟล์ทั้งหมดภายในไดเรกทอรี่เดียวกันต้องไม่ซ้ำกัน ภายหลังการทำตัวอักษรให้มีลักษณะตัวพิมพ์เดียวกัน (case normalization) ดังอธิบายในหัวข้อ 3.13 ของ **[Unicode]**
- ชื่อไฟล์ทั้งหมดภายในไดเรกทอรี่เดียวกันควรไม่ซ้ำกันภายหลังการทำให้เป็นมาตรฐานแบบ NFC หรือ NFD (NFC, NFD normalization) **[TR15]**

หมายเหตุ บางเครื่องมือชิปที่จำหน่ายในท้องตลาดไม่รองรับช่วงยูนิโค้ดทั้งหมด และอาจรองรับเพียงช่วงแอสกี้เป็นชื่อไฟล์ ผู้สร้างเนื้อหาที่ต้องการใช้เครื่องมือชิปซึ่งมีข้อจำกัดเหล่านี้อาจพบว่าการจำกัดชื่อไฟล์ให้อยู่ในช่วงแอสกี้เป็นสิ่งที่ดีที่สุด หากไม่สามารถรักษาชื่อของไฟล์ได้ระหว่างกระบวนการคลายซิป จำเป็นต้องชดเชยการแปลชื่อใดๆ ที่เกิดขึ้นเมื่อไฟล์ถูกอ้างอิงโดยยูอาร์ไอจากภายในเนื้อหา

4.5 ไดเรกทอรี่ META-INF

คอนเทนเนอร์แอบสแตรคท์โอซีเอฟทั้งหมดต้องมีไดเรกทอรี่เรียกว่า ***META-INF*** ไดเรกทอรี่นี้บรรจุไฟล์ตามระบุด้านล่างนี้ ไฟล์อื่นที่นอกเหนือจากที่กำหนดนี้อาจมีอยู่ในไดเรกทอรี่ ***META-INF*** โดยตัวประมวลผลโอซีเอฟต้องดำเนินการไม่ล้มเหลวเมื่อพบกับไฟล์เหล่านั้น

4.5.1 คอนเทนเนอร์ - META-INF/container.xml

คอนเทนเนอร์โอซีเอฟทั้งหมดต้องมีไฟล์เรียกว่า container.xml ภายในไดเรกทอรี่ ***META-INF*** ไฟล์ container.xml ต้องระบุชนิดสื่อของไฟล์รากและเส้นทางไปยังไฟล์รากสำหรับแต่ละเรนดิชั่นสิ่งพิมพ์อิเล็กทรอนิกส์ที่อยู่ในคอนเทนเนอร์

ไฟล์ container.xml ต้องไม่เข้ารหัส

ผังเอกสารสำหรับไฟล์ container.xml ปรากฏในหัวข้อผังเอกสารสำหรับ container.xml ไฟล์ container.xml ต้องถูกต้องตามผังเอกสารนี้หลังจากนำเอลิเมนต์และแอตทริบิวส์ทั้งหมดออกไปจากเนมสเปซอื่นแล้ว (รวมถึงแอตทริบิวส์และเนื้อหาทั้งหมดของเอลิเมนต์ดังกล่าว)

เอลิเมนต์ ***rootfiles*** ต้องมีเอลิเมนต์ ***rootfile*** หนึ่งเอลิเมนต์ขึ้นไป แต่ละเอลิเมนต์ต้องอ้างอิงเอกสารแพ็คเกจที่แสดงถึงเรนดิชั่นของสิ่งพิมพ์อิเล็กทรอนิกส์หนึ่งฉบับที่ไม่ซ้ำกัน ถ้าเรนดิชั่นมากกว่าหนึ่งเรนดิชั่นถูกจัดเก็บในโอซีเอฟ แต่ละเรนดิชั่นต้องเป็นการประมวลการแสดงผลที่แตกต่างกันของสิ่งพิมพ์อิเล็กทรอนิกส์เดียวกัน

ตัวประมวลผลโอซีเอฟต้องถือว่าเอลิเมนต์ ***rootfile*** ตัวแรกภายในเอลิเมนต์ ***rootfiles*** แสดงถึงเรนดิชั่นโดยปริยายสำหรับสิ่งพิมพ์อิเล็กทรอนิกส์ที่มีอยู่ไม่จำเป็นต้องมีระบบการอ่านเพื่อใช้เรนดิชั่นใดๆ ยกเว้นเรนดิชั่นโดยปริยาย

ตัวอย่างต่อไปนี้แสดง container.xml ตัวอย่างสำหรับสิ่งพิมพ์อิเล็กทรอนิกส์ที่มีไฟล์ราก EPUB/My Crazy Life.opf (เอกสารแพ็คเกจ)

```
<?xml version="1.0"?>
<container version="1.0" xmlns="urn:oasis:names:tc:opendocument:xmlns:container">
    <rootfiles>
        <rootfile full-path="EPUB/My Crazy Life.opf"
            media-type="application/oebps-package+xml" />
    </rootfiles>
</container>
```

ตัวอย่างต่อไปนี้แสดงเรนดิชั่นของเอสวีจีและเอ็กซ์เอชทีเอ็มแอลของรามเกียรติ์ (Ramayana) ที่อยู่ในคอนเทนเนอร์เดียวกัน

```
<?xml version="1.0"?>
<container version="1.0" xmlns="urn:oasis:names:tc:opendocument:xmlns:container">
    <rootfiles>
        <rootfile full-path="SVG/ Ramayana.opf"
            media-type="application/oebps-package+xml" />
        <rootfile full-path="XHTML/ Ramayana.opf"
            media-type="application/oebps-package+xml" />
    </rootfiles>
</container>
```

เอลิเมนต์ ***manifest*** ที่อยู่ภายในเอกสารแพ็คเกจระบุถึงรายชื่อแฟ้มเพียงหนึ่งเดียวที่ใช้สำหรับการประมวลผลเรนดิชั่นที่ให้มา ข้อมูลแมนิเฟสประกอบที่อยู่ในอาร์ไคฝ์ซิปหรือในไฟล์ทางเลือก manifest.xml ต้องไม่ถูกใช้เพื่อประมวลผลเรนดิชั่น ไฟล์เพิ่มเติมใดในอาร์ไคฝ์ซิปต้องไม่ถูกใช้ในการประมวลผลเรนดิชั่น (นั่นคือ ไฟล์ภายในอาร์ไคฝ์ซิปที่ไม่ได้แสดงรายการภายในเอลิเมนต์ ***manifest*** ของเอกสารแพ็คเกจ เช่น ไฟล์ ***META-INF*** หรือทรัพยากรเฉพาะกับเรนดิชั่นอื่นของสิ่งพิมพ์อิเล็กทรอนิกส์)

ไฟล์ container.xml อาจรวมเอลิเมนต์ ***links*** ตามหลังเอลิเมนต์ ***rootfiles*** ซึ่ง (ถ้ามี) ต้องมีเอลิเมนต์ ***link*** หนึ่งตัวขึ้นไป เอลิเมนต์ ***link*** แต่ละเอลิเมนต์ต้องรวมแอตทริบิวส์ ***href*** ซึ่งมีค่าที่ระบุถึงตำแหน่งของทรัพยากรที่จำเป็นสำหรับการประมวลผลคอนเทนเนอร์ของสิ่งพิมพ์อิเล็กทรอนิกส์ เอลิเมนต์ ***link*** แต่ละ

เอลิเมนต์ต้องรวมแอตทริบิวส์ ***rel*** ซึ่งมีค่าที่ระบุความสัมพันธ์ของทรัพยากรและอาจรวมแอตทริบิวส์ ***media-type*** ซึ่งค่าของแอตทริบิวส์ต้องเป็นชนิดสื่อ **[RFC2046]** ที่ระบุชนิดและฟอร์แมทของทรัพยากรที่อ้างอิงโดยเอลิเมนต์ ***link***

ค่าของแอตทริบิวส์ ***full-path*** ของเอลิเมนต์ ***rootfile*** และแอตทริบิวส์ ***href*** ของเอลิเมนต์ ***link*** ต้องมีคอมโพเน้นท์เส้นทาง (path component) ตามอธิบายใน **[RFC 3986]** ซึ่งต้องอยู่ในรูปแบบของ path-rootless เท่านั้น อธิบายใน **[RFC 3986]** เช่นกัน คอมโพเน้นท์เส้นทางสัมพันธ์กับรากของคอนเทนเนอร์ที่ใช้คอมโพเน้นท์เส้นทางนั้น

ตัวประมวลผลโอซีเอฟต้องไม่สนใจเอลิเมนต์และแอตทริบิวส์แปลกปลอมภายในไฟล์ container.xml

4.5.2 การเข้ารหัส – META-INF/encryption.xml

ไฟล์ทางเลือก encryption.xml ภายในไดเรกทอรี่ ***META-INF*** ที่ระดับรากของระบบไฟล์คอนเทนเนอร์มีข้อมูลการเข้ารหัสทั้งหมดของเนื้อหาของคอนเทนเนอร์ ถ้าทรัพยากรใดภายในคอนเทนเนอร์ถูกเข้ารหัสต้องมีไฟล์ encryption.xml เพื่อแสดงว่าทรัพยากรนั้นถูกเข้ารหัสและให้ข้อมูลว่าวิธีการเข้ารหัสเป็นอย่างไร

ไฟล์นี้เป็นเอกสารเอ็กซ์เอ็มแอลซึ่งเอลิเมนต์รากคือ ***encryption*** เอลิเมนต์ ***encryption*** บรรจุเอลิเมนต์ลูกชนิด ***EncryptedKey*** และ ***EncryptedData*** ตามที่อธิบายในข้อกำหนดไวยากรณ์และการประมวลผลการเข้ารหัสเอ็กซ์เอ็มแอล รุ่น 1.1 **[XML ENC Core]** เอลิเมนต์ ***EncryptedKey*** อธิบายกุญแจการเข้ารหัสแต่ละอันที่ใช้ในคอนเทนเนอร์ ขณะที่เอลิเมนต์ ***EncryptedData*** อธิบายไฟล์ที่เข้ารหัสแต่ละไฟล์ เอลิเมนต์ ***EncryptedData*** แต่ละเอลิเมนต์อ้างถึงเอลิเมนต์ ***EncryptedKey*** ดังที่กล่าวถึงในการเข้ารหัสเอ็กซ์เอ็มแอล

ผังเอกสารสำหรับไฟล์ encryption.xml มีแสดงอยู่ในภาคผนวกหัวข้อ ก.2 ผังเอกสารสำหรับไฟล์ encryption.xml โดยไฟล์ encryption.xml ต้องถูกต้องตามที่กำหนดในผังเอกสาร

โอซีเอฟเข้ารหัสไฟล์แต่ละไฟล์อย่างเป็นอิสระต่อกัน โดยแลกความปลอดภัยบางส่วนกับประสิทธิภาพที่ดีขึ้น ทำให้สามารถถอดรหัสเนื้อหาของคอนเทนเนอร์แบบเพิ่มขึ้นทีละส่วนได้ ซึ่งการเข้ารหัสด้วยวิธีนี้เปิดเผยโครงสร้างไดเรกทอรี่และการตั้งชื่อไฟล์ของทั้งแพ็คเกจ

โอซีเอฟใช้การเข้ารหัสเอ็กซ์เอ็มแอล **[XML ENC Core]** เพื่อจัดให้มีกรอบการทำงานสำหรับการเข้ารหัสทำให้สามารถใช้ชุดคำสั่งได้หลากหลาย การเข้ารหัสเอ็กซ์เอ็มแอลระบุกระบวนการในการเข้ารหัสข้อมูลที่กำหนดขึ้นเองและแสดงผลลัพธ์เป็นเอ็กซ์เอ็มแอล แม้ว่าคอนเทนเนอร์แอบสแตรคท์ของโอซีเอฟอาจมีข้อมูลที่ไม่ใช่เอ็กซ์เอ็มแอล แต่สามารถใช้การเข้ารหัสเอ็กซ์เอ็มแอลเพื่อเข้ารหัสข้อมูลทั้งหมดในคอนเทนเนอร์แอบสแตรคท์ของโอซีเอฟได้เช่นกัน การเข้ารหัสโอซีเอฟรองรับเพียงการเข้ารหัสทั้งไฟล์ภายในคอนเทนเนอร์เท่านั้น ไม่ใช่บางส่วนของไฟล์ ไฟล์ encryption.xml (ถ้ามี) ต้องไม่เข้ารหัส

ข้อมูลที่เข้ารหัสแทนที่ข้อมูลที่ไม่ได้เข้ารหัสในคอนเทนเนอร์แอบสแตรคท์ของโอซีเอฟ ตัวอย่างเช่น ถ้ารูปภาพชื่อ photo.jpeg ถูกเข้ารหัส เนื้อหาของทรัพยากร photo.jpeg ควรถูกแทนที่ด้วยเนื้อหาที่เข้ารหัสแล้ว เมื่อข้อมูลถูกเก็บในคอนเทนเนอร์ซิปต้องบีบอัดกระแสของข้อมูลก่อนเข้ารหัส และต้องใช้

การบีบอัดแบบดีเฟลท (deflate compression) ภายในไดเรกทอรี่ซิปควรจัดเก็บไฟล์ที่เข้ารหัสไม่ใช่ไฟล์ที่บีบอัดแบบดีเฟลท

สังเกตว่าบางสถานการณ์ต้องการการพรางการจัดเก็บทรัพยากรแบบฝังที่อ้างอิงโดยเรนดิชั่นเพื่อผูกเข้ากับสิ่งพิมพ์อิเล็กทรอนิกส์ และทำให้แยกเพื่อนำไปใช้โดยไม่มีข้อจำกัดได้ยากขึ้น (เช่น ฟอนต์) แม้ว่าการพรางฟอนต์จะไม่ใช่การเข้ารหัสให้ใช้ไฟล์ encryption.xml ร่วมกับชุดคำสั่งการพรางทรัพยากรของ IDPF เพื่อบ่งชี้ถึงทรัพยากรที่จำเป็นต้องยกเลิกการพรางก่อนที่จะสามารถถูกนำใช้ได้

ไฟล์ต่อไปนี้ต้องไม่ถูกเข้ารหัสไม่ว่าจะมีการร้องขอการเข้ารหัสโดยปริยายหรือเฉพาะเจาะจง

- mimetype
- META-INF/container.xml
- META-INF/encryption.xml
- META-INF/manifest.xml
- META-INF/metadata.xml
- META-INF/rights.xml
- META-INF/signatures.xml
- EPUB rootfile (เอกสารแพ็คเกจ)

ทรัพยากรที่เซ็นชื่อแล้วในภายหลังอาจถูกเข้ารหัสโดยใช้การแปลงการถอดรหัส (decryption transform) สำหรับลายเซ็นเอ็กซ์เอ็มแอลตามข้อกำหนดการแปลงการถอดรหัสสำหรับลายเซ็นเอ็กซ์เอ็มแอล **[XML SIG Decrypt]** คุณลักษณะนี้ทำให้โปรแกรมประยุกต์ใช้ เช่น โอซีเอฟเอเจ้นท์ (OCF agent) สามารถแยกข้อมูลที่เข้ารหัสก่อนเซ็นชื่อออกจากข้อมูลที่เข้ารหัสภายหลังจากเซ็นชื่อได้ เฉพาะข้อมูลที่เข้ารหัสภายหลังการเซ็นชื่อเท่านั้นที่ต้องถอดรหัสก่อนการประมวลผลข้อมูลไดเจสท์ (digest) เพื่อใช้พิสูจน์ลายเซ็น

ตัวอย่างต่อไปนี้ ดัดแปลงจาก หัวข้อ 2.2.1 ของ **[XML ENC Core]** ทรัพยากร image.jpeg ถูกเข้ารหัสโดยใช้ชุดคำสั่งกุญแจสมมาตร (AES) และกุญแจสมมาตรถูกเข้ารหัสต่อโดยใช้ชุดคำสั่งกุญแจอสมมาตร (RSA) ที่มีกุญแจคือ John Smith

```
<encryption
    xmlns ="urn:oasis:names:tc:opendocument:xmlns:container"
    xmlns:enc="http://www.w3.org/2001/04/xmlenc#"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <enc:EncryptedKey Id="EK">
        <enc:EncryptionMethodAlgorithm="http://www.w3.org/2001/04/xmlenc#rsa
        - 1_5"/>
```

```
            <ds:KeyInfo>
                <ds:KeyName>John Smith</ds:KeyName>
            </ds:KeyInfo>
            <enc:CipherData>
                <enc:CipherValue>xyzabc</enc:CipherValue>
            </enc:CipherData>
        </enc:EncryptedKey>
        <enc:EncryptedData Id="ED1">
            <enc:EncryptionMethod  Algorithm="http://www.w3.org/2001/04/xmlenc#kw-
            aes128"/>
            <ds:KeyInfo>
                <ds:RetrievalMethod URI="#EK"
                    Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"/>
            </ds:KeyInfo>
            <enc:CipherData>
                <enc:CipherReference URI="image.jpeg"/>
            </enc:CipherData>
        </enc:EncryptedData>
    </encryption>
```

4.5.3 รายชื่อแฟ้ม - META-INF/manifest.xml

ไฟล์ทางเลือกที่สงวนการใช้ชื่อว่า manifest.xml อาจรวมอยู่ภายในไดเรกทอรี่ ***META-INF*** ที่ระดับรากของระบบไฟล์ของคอนเทนเนอร์

ไฟล์ manifest.xml (ถ้ามี) ต้องไม่เข้ารหัส

4.5.4 เมทาดาตา - META-INF/metadata.xml

ไฟล์ทางเลือกที่สงวนการใช้ชื่อว่า metadata.xml อาจรวมอยู่ภายในไดเรกทอรี่ ***META-INF*** ที่ระดับรากของระบบไฟล์ของคอนเทนเนอร์ไฟล์นี้ (ถ้ามี) ต้องใช้กับเมทาดาตาระดับคอนเทนเนอร์

หากมีไฟล์ META-INF/metadata.xml เนื้อหาควรเป็นเพียงเอลิเมนต์ที่ผ่านคุณสมบัติของเนมสเปซ (namespace-qualified) ตามข้อกำหนดเนมสเปซในเอ็กซ์เอ็มแอล (ปรับปรุงครั้งที่ 3) **[XMLNS]** ไฟล์ควรบรรจุเอลิเมนต์ราก ***metadata*** ในเนมสเปซ http://www.idpf.org/2013/metadata แต่เอลิเมนต์

รากอื่นๆ อนุญาตสำหรับการเข้ากันได้กับรุ่นที่สูงกว่าระบบการอ่านควรละเลยไฟล์ metadata.xml ที่เอลิเมนต์รากไม่รู้จัก

ข้อกำหนดโอซีเอฟรุ่นนี้ไม่ได้อธิบายเมทาดาตาสำหรับใช้ในไฟล์ metadata.xml เมทาดาตาระดับคอนเทนเนอร์อาจถูกระบุในข้อกำหนดนี้ในรุ่นอนาคต และในข้อกำหนดส่วนขยายของสิ่งพิมพ์อิเล็กทรอนิกส์ของ IDPF

ไฟล์ metadata.xml (ถ้ามี) ต้องไม่เข้ารหัส

4.5.5 การจัดการสิทธิ - META-INF/rights.xml

ไฟล์ทางเลือกที่สงวนการใช้ชื่อว่า rights.xml อาจรวมอยู่ภายในไดเรกทอรี่ ***META-INF*** ที่ระดับรากของระบบไฟล์ของคอนเทนเนอร์ ไฟล์นี้สงวนไว้สำหรับข้อมูลการจัดการสิทธิทางดิจิทัล (digital rights management: DRM) ในการแลกเปลี่ยนสิ่งพิมพ์อิเล็กทรอนิกส์ที่เชื่อถือได้ระหว่างผู้ถือสิทธิคนกลางและผู้ใช้ข้อกำหนดโอซีเอฟรุ่นนี้ไม่ได้ระบุรูปแบบไฟล์สำหรับข้อมูลการจัดการสิทธิทางดิจิทัลที่ต้องการ แต่ข้อกำหนดรุ่นในอนาคตอาจระบุรูปแบบเฉพาะสำหรับข้อมูลการจัดการสิทธิทางดิจิทัล

หากมีไฟล์ META-INF/rights.xml เนื้อหาไฟล์ควรเป็นเพียงเอลิเมนต์ที่ผ่านคุณสมบัติของเนมสเปซ **[XMLNS]** เพื่อเลี่ยงการขัดแย้งกับโอซีเอฟรุ่นในอนาคตที่อาจระบุรูปแบบเฉพาะสำหรับไฟล์นี้

ไฟล์ rights.xml ต้องไม่เข้ารหัส

เมื่อไม่มีไฟล์ rights.xml คอนเทนเนอร์โอซีเอฟจะไม่ให้ข้อมูลที่แสดงว่าส่วนใดของคอนเทนเนอร์ถูกปกป้องสิทธิ

4.5.6 ลายเซ็นอิเล็กทรอนิกส์ - META-INF/signatures.xml

ไฟล์ทางเลือก signatures.xml ภายในไดเรกทอรี่ ***META-INF*** ที่ระดับรากของระบบไฟล์ของคอนเทนเนอร์จัดเก็บลายเซ็นดิจิทัลของคอนเทนเนอร์ และเนื้อหาของลายเซ็นไฟล์นี้เป็นเอกสารเอ็กซ์เอ็มแอล ซึ่งเอลิเมนต์รากคือ ***signatures*** เอลิเมนต์ ***signatures*** บรรจุเอลิเมนต์ลูกชนิด ***Signature*** ตามที่อธิบายในข้อกำหนดไวยากรณ์และการประมวลผลลายเซ็นเอ็กซ์เอ็มแอล **[XML DSIG Core]** ลายเซ็นสามารถประยุกต์ใช้กับเรนดิชั่นใดๆ ของสิ่งพิมพ์อิเล็กทรอนิกส์ได้ทั้งหมดหรือบางส่วนของเรนดิชั่น ลายเซ็นเอ็กซ์เอ็มแอลสามารถระบุการเซ็นของข้อมูลชนิดใดก็ได้ ไม่ใช่เพียงเอ็กซ์เอ็มแอล

ไฟล์ signatures.xml ต้องไม่เข้ารหัส

เมื่อไม่มีไฟล์ signatures.xml คอนเทนเนอร์โอซีเอฟจะไม่ให้ข้อมูลที่แสดงว่าส่วนใดของคอนเทนเนอร์มีการเซ็นอิเล็กทรอนิกส์ที่ระดับคอนเทนเนอร์ อย่างไรก็ตามเป็นไปได้ว่าการเซ็นอิเล็กทรอนิกส์มีอยู่ภายในเรนดิชั่นที่บรรจุอยู่ใดก็ได้

ผังเอกสารสำหรับไฟล์ signatures.xml มีแสดงอยู่ในภาคผนวกหัวข้อ ก.3 ผังเอกสารสำหรับไฟล์ signatures.xml โดยไฟล์ signatures.xml ต้องถูกต้องตามผังเอกสารนี้

เมื่อโอซีเอฟเอเจ้นท์สร้างลายเซ็นของข้อมูลในคอนเทนเนอร์ ควรเพิ่มลายเซ็นใหม่เป็นเอลิเมนต์ลูกลำดับสุดท้ายของเอลิเมนต์ ***Signature*** ของเอลิเมนต์ ***signatures***ในไฟล์ signatures.xml

หมายเหตุ เอลิเมนต์ ***Signature*** แต่ละเอลิเมนต์ในไฟล์ signatures.xml ระบุว่าลายเซ็นเป็นของข้อมูลใดโดยไออาร์ไอโดยใช้เอลิเมนต์ ***Manifest*** ของลายเซ็นเอ็กซ์เอ็มแอล และเอลิเมนต์ย่อย ***Reference*** แต่ละไฟล์ที่บรรจุอยู่อาจเซ็นแยกกันหรือรวมกันได้ การเซ็นแต่ละไฟล์แยกกันจะสร้างค่าข้อมูลไดเจสท์ของทรัพยากรที่สามารถพิสูจน์ความถูกต้องอย่างเป็นอิสระจากกัน วิธีการนี้อาจทำให้เอลิเมนต์ ***signature*** ขนาดใหญ่ขึ้นหากเซ็นไฟล์รวมด้วยกันสามารถแสดงรายการชุดของไฟล์ที่เซ็นในเอลิเมนต์ ***Manifest*** ของลายเซ็นเอ็กซ์เอ็มแอลเอลิเมนต์เดียวและอ้างอิงโดยเอลิเมนต์ ***Signature*** ตั้งแต่หนึ่งเอลิเมนต์ขึ้นไปได้

ไฟล์ใดหรือไฟล์ทั้งหมดในคอนเทนเนอร์สามารถถูกเซ็นได้โดยยกเว้นไฟล์ signatures.xml เนื่องจากไฟล์จะมีข้อมูลลายเซ็นที่ถูกประมวลผลแล้ว ไฟล์ signatures.xml ควรถูกเซ็นหรือไม่อย่างไรขึ้นอยู่กับวัตถุประสงค์ของผู้ลงลายเซ็น

หากผู้เซ็นต้องการอนุญาตให้เพิ่มหรือลบลายเซ็นในคอนเทนเนอร์ได้โดยไม่ทำให้ลายเซ็นของผู้เซ็นไม่ถูกต้องไม่ควรเซ็นไฟล์ signatures.xml

หากผู้เซ็นต้องการให้การเพิ่มหรือลบลายเซ็นในคอนเทนเนอร์ทำให้ลายเซ็นของผู้เซ็นไม่ถูกต้อง การแปลงลายเซ็นแบบเอ็นวีลอปด์ (enveloped signature transform) (อธิบายในหัวข้อ 6.6.4 ของ **[XML DSIG Core]**) สามารถใช้เพื่อเซ็นไฟล์ลายเซ็นทั้งหมดที่มีอยู่ก่อนทั้งหมดได้ยกเว้น ***Signature*** ที่กำลังสร้างขึ้น การแปลงนี้จะเซ็นลายเซ็นก่อนหน้าทั้งหมด และเปลี่ยนสถานะเป็นไม่ถูกต้องหากมีการเพิ่มลายเซ็นลงในแพ็คเกจหลังจากนั้น

ไฟล์ใดหรือไฟล์ทั้งหมดในคอนเทนเนอร์สามารถถูกเซ็นได้โดยยกเว้นไฟล์ signatures.xml เนื่องจากไฟล์จะมีข้อมูลลายเซ็นที่ถูกประมวลผลแล้ว ไฟล์ signatures.xml ควรถูกเซ็นหรือไม่อย่างไรขึ้นอยู่กับวัตถุประสงค์ของผู้ลงลายเซ็น

หากผู้เซ็นต้องการอนุญาตให้เพิ่มหรือลบลายเซ็นในคอนเทนเนอร์ได้โดยไม่ทำให้ลายเซ็นของผู้เซ็นไม่ถูกต้องไม่ควรเซ็นไฟล์ signatures.xml

หากผู้เซ็นต้องการให้การเพิ่มหรือลบลายเซ็นในคอนเทนเนอร์ทำให้ลายเซ็นของผู้เซ็นไม่ถูกต้อง การแปลงลายเซ็นแบบเอ็นวีลอปด์ (enveloped signature transform) (อธิบายในหัวข้อ 6.6.4 ของ **[XML DSIG Core]**) สามารถใช้เพื่อเซ็นไฟล์ลายเซ็นทั้งหมดที่มีอยู่ก่อนทั้งหมดได้ ยกเว้น ***Signature*** ที่กำลังสร้างขึ้น การแปลงนี้จะเซ็นลายเซ็นก่อนหน้าทั้งหมดและเปลี่ยนสถานะเป็นไม่ถูกต้องหากมีการเพิ่มลายเซ็นลงในแพ็คเกจหลังจากนั้น

ถ้าผู้ลงลายเซ็นต้องการให้การเอาลายเซ็นที่มีอยู่ออกทำให้ลายเซ็นของผู้ลงลายเซ็นไม่ถูกต้อง แต่ต้องการอนุญาตให้มีการเพิ่มลายเซ็นใหม่ด้วยสามารถใช้การแปลงแบบเอ็กซ์พาธ (XPath transform) เพื่อเซ็นเฉพาะลายเซ็นที่มีอยู่แล้ว (ส่วนนี้เป็นเพียงข้อแนะนำ การแปลงแบบเอ็กซ์พาธไม่ได้เป็นส่วนหนึ่งของข้อกำหนดโอซีเอฟนี้)

ลายเซ็นเอ็กซ์เอ็มแอลไม่ได้เชื่อมโยงความหมายใดกับลายเซ็นเอเจ้นท์อาจมีข้อมูลเชิงความหมายดังตัวอย่าง การเพิ่มข้อมูลลงในเอลิเมนต์ ***Signature*** ที่อธิบายลายเซ็น ลายเซ็นเอ็กซ์เอ็มแอลอธิบายวิธีการเพิ่มข้อมูลลงในลายเซ็น (เช่น โดยการใช้เอลิเมนต์ ***SignatureProperties***)

นิพจน์เอ็กซ์เอ็มแอลต่อไปนี้แสดงเนื้อหาของไฟล์ signautres.xml ตัวอย่างและอิงจากตัวอย่างที่พบในส่วนที่ 2 ของ **[XML DSIG Core]** ซึ่งมีหนึ่งลายเซ็นและลายเซ็นนั้นปรับใช้กับทรัพยากรสองรายการในคอนเทนเนอร์ ได้แก่ OEBFPS/book.html และ OEBFPS/images/cover.jpeg

```
<signatures xmlns="urn:oasis:names:tc:opendocument:xmlns:container">
    <Signature Id="sig" xmlns="http://www.w3.org/2000/09/xmldsig#">
 <SignedInfo>
       <CanonicalizationMethod
            Algorithm="http://www.w3.org/TR/2001/REC-xmlc14n- 20010315"/>
       <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
       <Reference URI="#Manifest1">
            <DigestMethodAlgorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</DigestValue>
       </Reference>
 </SignedInfo>
 <SignatureValue>...</SignatureValue>
 <KeyInfo>
       <KeyValue>
            <DSAKeyValue>
                 <P>...</P><Q>...</Q><G>...</G><Y>...</Y>
            </DSAKeyValue>
       </KeyValue>
 </KeyInfo>

 <Object>
       <Manifest Id="Manifest1">
            <Reference URI="OEBFPS/book.xml">
                 <Transforms>
                      <Transform
                        Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
                 </Transforms>
                 <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                 <DigestValue></DigestValue>
            </Reference>
            <Reference URI="OEBFPS/images/cover.jpeg">
                 <Transforms>
```

```
                        <Transform
                          Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
                    </Transforms>
                    <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                    <DigestValue></DigestValue>
                </Reference>
            </Manifest>
        </Object>
    </Signature>
</signatures>
```

5. คอนเทนเนอร์ซิปของโอซีเอฟ

5.1 ภาพรวม

เนื้อหาส่วนนี้เป็นข้อแนะนำ

คอนเทนเนอร์ซิปของโอซีเอฟเป็นแมนิเฟสเทชัน (manifestation) แบบไฟล์เดี่ยวเชิงกายภาพของคอนเทนเนอร์แอบสแตรคท์

5.2 ข้อกำหนดไฟล์ซิป

คอนเทนเนอร์ซิปของโอซีเอฟใช้รูปแบบซิปตามที่ระบุในข้อกำหนดของรูปแบบไฟล์ซิป **[ZIP APPNOTE 6.3.3]** โดยมีข้อบังคับและคำอธิบายดังต่อไปนี้

- เนื้อหาของคอนเทนเนอร์ซิปของโอซีเอฟต้องเป็นไปตามกฎเกณฑ์ของคอนเทนเนอร์แอบสแตรคท์
- คอนเทนเนอร์ซิปของโอซีเอฟต้องไม่ใช้คุณลักษณะในโปรแกรมการบันทึกซิปซึ่งอนุญาตให้แบ่งไฟล์ซิปลงในหลายสื่อเก็บข้อมูล ตัวประมวลผลโอซีเอฟต้องถือว่าไฟล์โอซีเอฟใดที่ระบุว่าไฟล์ซิปถูกแบ่งลงในสื่อเก็บข้อมูลหลายชิ้นว่าเป็นข้อผิดพลาด
- คอนเทนเนอร์ซิปของโอซีเอฟต้องมีเพียงรายการที่จัดเก็บโดยไม่บีบอัดและรายการที่บีบอัดแบบดีเฟลทภายในแฟ้มที่บีบอัดประเภทซิปเท่านั้น ตัวประมวลผลโอซีเอฟต้องถือว่าคอนเทนเนอร์ของโอซีเอฟที่ใช้เทคนิคการบีบอัดอื่นที่ไม่ใช่แบบดีเฟลทว่าเป็นข้อผิดพลาด
- คอนเทนเนอร์ซิปของโอซีเอฟอาจใช้ส่วนขยายซิป 64 ตามที่กำหนดเป็น “version 1” ในส่วนที่ 5 หัวข้อย่อย G ของโปรแกรมการบันทึกใน **[ZIP APPNOTE 6.3.3]** และควรใช้เพียงส่วนขยายเหล่านั้นเท่านั้นเมื่อเนื้อหาต้องการส่วนขยาย ตัวประมวลผลโอซีเอฟต้องรองรับส่วนขยายซิป 64 ตามที่กำหนดเป็น “version 1”
- คอนเทนเนอร์ซิปของโอซีเอฟต้องไม่ใช้คุณลักษณะการเข้ารหัสตามอธิบายในรูปแบบซิป การเข้ารหัสต้องใช้คุณลักษณะที่อธิบายในหัวข้อ 4.5.2 การเข้ารหัส – META-INF/encryption.xml แทนตัวประมวลผลโอซีเอฟต้องถือว่าคอนเทนเนอร์ซิปของโอซีเอฟซึ่งใช้คุณลักษณะการเข้ารหัสซิปเป็นข้อผิดพลาด
- ไม่บังคับให้ตัวประมวลผลโอซีเอฟต้องสงวนข้อมูลจากคอนเทนเนอร์ซิปของโอซีเอฟผ่านทางการรับข้อมูลเข้าและการบันทึกข้อมูลซึ่งไม่ได้ระบุภายในคอนเทนเนอร์แอบสแตรคท์ของโอซีเอฟ โดยเฉพาะอย่างยิ่งตัวประมวลผลโอซีเอฟไม่ต้องสงวนค่าซีอาร์ซี (CRC) ฟิลด์ข้อมูลความคิดเห็น (comment fields) หรือฟิลด์ที่เก็บข้อมูลระบบไฟล์ที่เฉพาะเจาะจงกับระบบปฏิบัติการหนึ่ง (เช่น แอตทริบิวส์ไฟล์ภายนอก (External file attributes) และฟิลด์พิเศษ (Extra field))
- คอนเทนเนอร์ซิปของโอซีเอฟต้องเข้ารหัสชื่อระบบไฟล์โดยใช้ยูทีเอฟ-8 **[Unicode]**

ข้อบังคับต่อไปนี้ใช้สำหรับฟิลด์เฉพาะในอาร์ไคฝ์คอนเทนเนอร์ซิปของโอซีเอฟ

- ในหัวตารางของไฟล์ภายในเครื่องคอนเทนเนอร์ซิปของโอซีเอฟต้องตั้งค่าฟิลด์รุ่นที่จำเป็นในการแยกฟิลด์เป็นค่า 10, 20 หรือ 45 เพื่อให้ตรงกับระดับรุ่นสูงสุดที่จำเป็นต่อไฟล์ที่กำหนดให้ (เช่น ค่า 20

หากต้องการดีเฟลท, ค่า 45 ถ้าต้องการซิป 64) ตัวประมวลผลโอซีเอฟต้องถือว่าค่าอื่นนอกจากนี้เป็นข้อผิดพลาด

- ในตารางหัวข้อของไฟล์ภายในเครื่องคอนเทนเนอร์ซิปของโอซีเอฟต้องตั้งค่าฟิลด์วิธีการบีบอัดข้อมูลเป็นค่า 0 หรือ 8 ตัวประมวลผลโอซีเอฟต้องถือว่าค่าอื่นนอกจากนี้เป็นข้อผิดพลาด
- ตัวประมวลผลโอซีเอฟต้องถือว่าคอนเทนเนอร์ซิปของโอซีเอฟที่มีส่วนหัวการถอดรหัสของอาร์ไคฝ์ (archive decryption header) หรือเรคอร์ดข้อมูลพิเศษของอาร์ไคฝ์ (archive extra data record) เป็นข้อผิดพลาด

5.3 การระบุชนิดสื่อของคอนเทนเนอร์ซิปของโอซีเอฟ

คอนเทนเนอร์ซิปของโอซีเอฟต้องมีไฟล์ ***mimetype*** เป็นไฟล์แรกในคอนเทนเนอร์ และเนื้อหาของไฟล์นี้ต้องเป็น ***application/epub+zip*** ซึ่งเป็นสายอักขระชนิดไมม์ เข้ารหัสเป็นยูเอส-แอสกี้ **[US-ASCII]**

เนื้อหาของไฟล์ ***mimetype*** ต้องไม่มีช่องว่างนำหน้าหรือเว้นวรรคและต้องไม่เริ่มต้นด้วยลายเซ็นยูนิโค้ด (หรือไบท์ออเดอร์มาร์ค (Byte Order Mark)) และในกรณีสายอักขระชนิดไมม์ต้องตรงกับที่แสดงไว้ข้างต้น ไฟล์ ***mimetype*** ที่เพิ่มเข้ามาต้องไม่ถูกบีบอัดหรือเข้ารหัส และต้องไม่เป็นฟิลด์พิเศษในส่วนหัวของซิป

หมายเหตุ อ้างอิงไปยังภาคผนวก ค. ชนิดสื่อ ***application/epub+zip*** สำหรับข้อมูลเพิ่มเติมเกี่ยวกับชนิดสื่อ ***application/epub+zip***

6. การพรางทรัพยากร

6.1 บทนำ

เนื้อหาส่วนนี้เป็นข้อแนะนำ

เนื่องจากคอนเทนเนอร์ซิปของโอซีเอฟโดยพื้นฐานเป็นไฟล์ซิป เครื่องมือซิปทั่วไปที่มีอยู่สามารถนำมาใช้เพื่อแตกเนื้อหาที่ไม่ได้เข้ารหัสจากแพ็คเกจได้ นอกจากนั้นเนื้อหาของไฟล์ซิปอาจมีลักษณะเหมือนคอนเทนเนอร์พื้นฐานอื่นที่อยู่บนบางระบบ (เช่น แฟ้มข้อมูล)

ขณะที่ความเรียบง่ายของไฟล์ซิปค่อนข้างเป็นประโยชน์ แต่ก็ทำให้เกิดปัญหาด้วยเมื่อการแตกข้อมูลทรัพยากรที่ง่ายไม่ใช่ผลกระทบข้างเคียงที่ต้องการของการไม่เข้ารหัส ตัวอย่างเช่น ผู้แต่งที่ต้องการรวมฟอนต์จากบุคคลที่สามโดยทั่วไปไม่ต้องการให้ฟอนต์ถูกแตกข้อมูลและนำกลับมาใช้ใหม่โดยผู้อื่น ฟอนต์ในท้องตลาดจำนวนมากยอมให้มีการฝัง แต่การฝังฟอนต์มีนัยยะว่าเป็นการทำให้ฟอนต์กลายเป็นส่วนหนึ่งของสิ่งพิมพ์อิเล็กทรอนิกส์ไม่ใช่มอบไฟล์ฟอนต์ต้นฉบับไปพร้อมกับเนื้อหา

เนื่องจากการรองรับการซิปตั้งแต่แรกเป็นสิ่งที่พบได้อย่างแพร่หลายในระบบปฏิบัติการสมัยใหม่ การใส่ฟอนต์ไว้ในอาร์ไคฝ์ซิปเพียงอย่างเดียวไม่เพียงพอที่จะบ่งชี้ได้ว่าฟอนต์นั้นไม่มีเจตนาให้นำไปใช้ซ้ำในบริบทอื่น ความไม่แน่นอนนี้ลดความสามารถในการฝังตัวฟอนต์ของสิ่งพิมพ์อิเล็กทรอนิกส์ ซึ่งมิฉะนั้นแล้วจะมีประโยชน์มาก

เพื่อไม่ส่งเสริมการนำฟอนต์ไปใช้ซ้ำ ผู้จำหน่ายฟอนต์บางรายอาจยอมให้ใช้ฟอนต์ของตนในสิ่งพิมพ์อิเล็กทรอนิกส์ถ้าฟอนต์เหล่านั้นถูกผูกไว้กับสิ่งพิมพ์อิเล็กทรอนิกส์ด้วยวิธีการบางอย่าง นั่นคือไฟล์ฟอนต์ไม่สามารถติดตั้งเพื่อใช้บนระบบปฏิบัติการได้โดยตรงด้วยเครื่องมือที่ติดมากับอุปกรณ์คอมพิวเตอร์นั้น และไม่สามารถใช้ได้โดยตรงกับสิ่งพิมพ์อิเล็กทรอนิกส์ฉบับอื่น

การจัดการสิทธิดิจิทัลหรือระบบการควบคุมสำหรับไฟล์ฟอนต์เป็นเรื่องอยู่นอกเหนือจากขอบเขตของข้อกำหนดฉบับนี้ ในส่วนหัวข้อนี้อธิบายถึงวิธีการพรางซึ่งผู้รับโอซีเอฟฉบับสมบูรณ์ต้องทำบางสิ่งเพิ่มเติมเพื่อให้เข้าถึงทรัพยากรที่พรางไว้

สังเกตว่าไม่มีการกล่าวอ้างในเอกสารมาตรฐานผลิตภัณฑ์อุตสาหกรรมฉบับนี้หรือโดยองค์กร IDPF ว่าการทำเช่นนี้เป็นการเข้ารหัส หรือการรับประกันว่าไฟล์ฟอนต์จะปลอดภัยจากการละเมิดลิขสิทธิ์ อย่างไรก็ดีองค์กร IDPF หวังว่าการทำเช่นนี้จะตอบสนองความต้องการของผู้จำหน่ายฟอนต์ส่วนใหญ่ ซึ่งต้องการความมั่นใจว่าทรัพยากรของตนจะไม่ถูกแตกข้อมูลได้อย่างง่ายโดยการคลายซิปคอนเทนเนอร์

ในกรณีของฟอนต์ ใช้หลักสำหรับการพราง กลไกนี้เป็นเพียงการขัดขวางผู้ที่ไม่ทราบรายละเอียดการอนุญาตไม่ให้ดำเนินการได้โดยง่าย กลไกไม่ได้ป้องกันผู้ใช้ที่มีเจตนาในการเข้าถึงฟอนต์ได้อย่างสมบูรณ์ มีความเป็นไปได้ที่จะใช้ขั้นตอนวิธีที่กำหนดเพื่อแตกไฟล์ฟอนต์ออกมา

6.2 กุญแจการพราง

กุญแจที่ใช้ในขั้นตอนวิธีการพรางสร้างมาจากตัวระบุเอกลักษณ์ของเรนดิชั่นโดยปริยาย

อักขระช่องว่างทั้งหมด ตามอธิบายในข้อกำหนดเอ็กซ์เอ็มแอล 1.0 **[XML]** หัวข้อ 2.3 ต้องถูกลบออกจากตัวระบุนี้ โดยเฉพาะอย่างยิ่งตำแหน่งรหัสยูนิโค้ด U+0020, U+0009, U+000D และ U+000A

ข้อมูลไดเจสท์เอสเอชเอ–1 (SHA-1) ของตัวแทนยูทีเอฟ–8 ของผลลัพธ์ที่เป็นสายอักขระควรถูกสร้างขึ้นโดยเฉพาะจากมาตรฐานแฮชแบบปลอดภัย **[SHA-1]** ข้อมูลไดเจสท์นี้ถูกนำไปใช้เป็นกุญแจสำหรับขั้นตอนวิธีต่อไป

6.3 ขั้นตอนวิธีการพราง

ขั้นตอนวิธีที่ถูกใช้เพื่อพรางทรัพยากร ประกอบด้วยการดัดแปลง 1040 ไบท์แรก (ประมาณ 1 กิโลไบท์) ของไฟล์ในกรณีที่มีขนาดน้อยกว่า 1040 ไบท์ ไฟล์ทั้งไฟล์จะถูกดัดแปลง

เพื่อพรางข้อมูลต้นฉบับ ผลลัพธ์ของการทำโลจิคัลเอ็กซ์คลูซีฟออ (logical exclusive or: XOR) ระหว่างไบท์แรกของไฟล์ดิบกับไบท์แรกของกุญแจการพรางถูกเก็บเป็นไบท์แรกของทรัพยากรแบบฝัง

กระบวนการนี้จะทำซ้ำกับไบท์ถัดไปของข้อมูลต้นทางและกุญแจ จนกระทั่งทุกไบท์ในกุญแจถูกใช้หมด เมื่อถึงจุดนี้ กระบวนการจะดำเนินการต่อโดยเริ่มจากไบท์แรกของกุญแจและไบท์ตัวที่ 21 ของข้อมูลต้นทาง เมื่อเข้ารหัส 1040 ไบท์ด้วยวิธีนี้แล้ว (หรือถึงจุดสิ้นสุดของข้อมูลต้นทาง) ข้อมูลที่เหลืออยู่ในข้อมูลต้นทางจะถูกคัดลอกโดยตรงไปยังปลายทาง

การพรางทรัพยากรต้องเกิดขึ้นก่อนที่ทรัพยากรจะถูกบีบอัดและเพิ่มเข้าไว้ในคอนเทนเนอร์ของโอซีเอฟ สังเกตว่าการพรางไม่ใช่การเข้ารหัส ข้อกำหนดนี้จึงไม่ละเมิดข้อกำหนดในหัวข้อ 4.5.2 การเข้ารหัส –META-INF/encryption.xml ในการบีบอัดทรัพยากรก่อนที่จะเข้ารหัส

รหัสเทียมต่อไปนี้เป็นตัวอย่างแสดงถึงขั้นตอนวิธีการพราง ดังนี้

```
set ocf to OCF container file
set source to file
set destination to obfuscated file
set keyData to key for file
set outer to 0
while outer < 52 and not (source at EOF)
    set inner to 0
    while inner < 20 and not (source at EOF)
        read 1 byte from source     //Assumes read advances file position
        set sourceByte to result of read
        set keyByte to byte inner of keyData
        set obfuscatedByte to (sourceByte XOR keyByte)
        write obfuscatedByte to destination
        increment inner
    end while
    increment outer
end while
if not (source at EOF) then
    read source to EOF
```

write result of read to destination
end if
Deflate destination
store destination as source in ocf

ในการนำข้อมูลฟอนต์ต้นฉบับกลับคืนมาให้ดำเนินกระบวนการย้อนกลับ นั่นคือไฟล์ต้นทางกลายเป็นข้อมูลที่ถูกพรางและไฟล์ปลายทางจะบรรจุข้อมูลดิบ

6.4 การระบุทรัพยากรการพราง

แม้ว่าทางเทคนิคแล้วทรัพยากรที่ถูกพรางจะไม่ใช่ข้อมูลที่ถูกเข้ารหัส แต่ทรัพยากรที่ถูกพรางทั้งหมดต้องปรากฏเป็นรายการอยู่ในไฟล์ encryption.xml ที่มากับสิ่งพิมพ์อิเล็กทรอนิกส์ (ดูที่หัวข้อ 4.5.2 การเข้ารหัส – META-INF/encryption.xml)

แต่ละทรัพยากรที่ถูกพรางต้องมีเอลิเมนต์ ***EncryptionMethod*** แต่ละทรัพยากรต้องมีเอลิเมนต์ลูก ***EncryptedData*** ของแอตทริบิวส์ ***Algorithm*** ที่ตั้งค่าเป็น http://www.idpf.org/2008/embedding การปรากฏของแอตทริบิวส์นี้ส่งสัญญาณถึงการใช้ขั้นตอนวิธีที่อธิบายไว้ในข้อกำหนดนี้ เส้นทางไปยังทรัพยากรที่ถูกพรางต้องถูกลงบัญชีรายการในเอลิเมนต์ลูก ***CipherReference*** ของเอลิเมนต์ ***CipherData***

ตัวอย่างต่อไปนี้แสดงรายการสำหรับฟอนต์ที่ถูกพรางในไฟล์ encryption.xml ดังนี้

```
<encryption
        xmlns="urn:oasis:names:tc:opendocument:xmlns:container"
        xmlns:enc="http://www.w3.org/2001/04/xmlenc#">
        <enc:EncryptedData>
                <enc:EncryptionMethod Algorithm="http://www.idpf.org/2008/embedding"/>
                <enc:CipherData>
                        <enc:CipherReference URI=" EPUB/Fonts/BKANT.TTF"/>
                </enc:CipherData>
        </enc:EncryptedData>
</encryption>
```

เพื่อป้องกันการคัดลอกฟอนต์แบบฝังบางส่วนไปยังสิ่งพิมพ์อิเล็กทรอนิกส์อื่น ต้องไม่ใส่กุญแจการพรางไว้ในไฟล์ encryption.xml

ภาคผนวก ก.

(ข้อแนะนำ)
ผังเอกสาร

(ข้อ 4.5.2 และ ข้อ 4.5.6)

ภาคผนวกนี้เป็นข้อแนะนำ

ก.1 ผังเอกสารสำหรับไฟล์ container.xml

ผังเอกสารสำหรับไฟล์ container.xml มีอยู่ที่

http://www.idpf.org/epub/301/schema/ocf-container-30.rnc

```
default namespace = "urn:oasis:names:tc:opendocument:xmlns:container"
  include "./mod/datatypes.rnc"

  start = ocf.container

  ocf.container =
    element container { ocf.container.attlist & ocf.container.content }
  ocf.container.attlist =
    attribute version { '1.0' }
  ocf.container.content = ocf.rootfiles, ocf.links?

  ocf.rootfiles =
    element rootfiles { ocf.rootfiles.attlist & ocf.rootfiles.content  }
  ocf.rootfiles.attlist = empty
  ocf.rootfiles.content = ocf.rootfile+

  ocf.rootfile  =
    element rootfile {ocf.rootfile.attlist & ocf.rootfile.content  }
  ocf.rootfile.attlist =
```

```
    attribute full-path { datatype.URI } &
    attribute media-type { 'application/oebps-package+xml' }
  ocf.rootfile.content = empty

 ocf.links =
   element links { ocf.links.attlist & ocf.links.content  }
 ocf.links.attlist = empty
 ocf.links.content = ocf.link+

 ocf.link =
   element link { ocf.link.attlist & ocf.link.content  }
 ocf.link.attlist =
     attribute href { datatype.URI } &
     attribute rel { datatype.space.separated.tokens } &
     attribute media-type { datatype.mimetype }?
 ocf.link.content = empty
```

การใช้งานได้ของการใช้ผังเอกสารนี้ต้องการตัวประมวลผลที่รองรับ **[RelaxNG]** และ **[XSD-DATATYPES]**

ก.2 ผังเอกสารสำหรับไฟล์ encryption.xml

ผังเอกสารสำหรับไฟล์ encryption.xml รวมอยู่ใน **[XML Sec RNG Schemas]**

ก.3 ผังเอกสารสำหรับไฟล์ signatures.xml

ผังเอกสารสำหรับไฟล์ signatures.xml รวมอยู่ใน **[XML Sec RNG Schemas]**

ภาคผนวก ข.

(ข้อแนะนำ)
ตัวอย่าง

(ข้อ 4.5)

ภาคผนวกนี้เป็นข้อแนะนำ

ตัวอย่างต่อไปนี้สาธิตการใช้รูปแบบโอซีเอฟเพื่อบรรจุสิ่งพิมพ์อิเล็กทรอนิกส์ที่มีลายเซ็นและเข้ารหัสภายในคอนเทนเนอร์ซิป

ตัวอย่าง ข.1 บัญชีรายการที่เรียงลำดับของไฟล์ในคอนเทนเนอร์ซิป

mimetype

META-INF/container.xml

META-INF/signatures.xml

META-INF/encryption.xml

OEBPS/As You Like It.opf

OEBPS/book.html

OEBPS/nav.html

OEBPS/toc.ncx

OEBPS/images/cover.png

ตัวอย่าง ข.2 เนื้อหาของไฟล์ ***mimetype***

application/epub+zip

ตัวอย่าง ข.3 เนื้อหาของไฟล์ META-INF/container.xml

```
<?xml version="1.0"?>
<container version="1.0"
xmlns="urn:oasis:names:tc:opendocument:xmlns:container">
        <rootfiles>
                <rootfile full-path=" EPUB/As You Like It.opf"
                        media-type="application/oebps-package+xml" />
        </rootfiles>
```

```
</container>
```

ตัวอย่าง ข.4 เนื้อหาของไฟล์ META-INF/signatures.xml

```
<signatures xmlns="urn:oasis:names:tc:opendocument:xmlns:container">
  <Signature Id="AsYouLikeItSignature" xmlns="http://www.w3.org/2000/09/xmldsig#">
    <!-- SignedInfo is the information that is actually signed. In this case -->
    <!-- the SHA1 algorithm is used to sign the canonical form of the XML -->
    <!-- documents enumerated in the Object element below -->
   <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
      20010315"/>
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
      <Reference URI="#AsYouLikeIt">
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
       <DigestValue>...</DigestValue>
      </Reference>
    </SignedInfo>
    <!-- The signed value of the digest above using the DSA algorithm -->
    <SignatureValue>...</SignatureValue>
    <!-- The key to use to validate the signature -->
    <KeyInfo>
      <KeyValue>
        <DSAKeyValue>
          <P>...</P>
       <Q>...</Q>
       <G>...</G>
       <Y>...</Y>
      </DSAKeyValue>
    </KeyValue>
   </KeyInfo>
<!-- The list documents to sign. Note that the canonical form of XML -->
```

```
        <!-- documents is signed while the binary form of the other documents -->
        <!-- is used -->
      <Object>
        <Manifest Id="AsYouLikeIt">
          <Reference URI="EPUB/As You Like It.opf">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue></DigestValue>
          </Reference>
          <Reference URI=" EPUB/book.html">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue></DigestValue>
          </Reference>
          <Reference URI=" EPUB/images/cover.png">
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue></DigestValue>
          </Reference>
        </Manifest>
      </Object>
    </Signature>
</signatures>

            <Object>
              <Manifest Id="AsYouLikeIt">
                <Reference URI="EPUB/As You Like It.opf">
                  <Transforms>
                    <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
                  </Transforms>
                  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                  <DigestValue></DigestValue>
```

```
            </Reference>
            <Reference URI=" EPUB/book.html">
                <Transforms>
                    <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
                </Transforms>
                <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <DigestValue></DigestValue>
            </Reference>
            <Reference URI=" EPUB/images/cover.png">
                <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <DigestValue></DigestValue>
            </Reference>
        </Manifest>
    </Object>
</Signature>
</signatures>
```

ตัวอย่าง ข.5 เนื้อหาของไฟล์ META-INF/encryption.xml

```
<?xml version="1.0"?>
<encryption xmlns="urn:oasis:names:tc:opendocument:xmlns:container"
    xmlns:enc=http://www.w3.org/2001/04/xmlenc#
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <!-- The RSA encrypted AES-128 symmetric key used to encrypt the data -->
   <enc:EncryptedKey Id="EK">
        <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
        <ds:KeyInfo>
            <ds:KeyName>John Smith</ds:KeyName>
        </ds:KeyInfo>
        <enc:CipherData>
            <enc:CipherValue>xyzabc...</enc:CipherValue>
        </enc:CipherData>
```

```
            </enc:EncryptedKey>
            <!-- Each EncryptedData block identifies a single document that has been -->
            <!-- encrypted using the AES-128 algorithm. The data remains stored in it's -->
            <!-- encrypted form in the original file within the container. -->
            <enc:EncryptedData Id="ED1">
                 <enc:EncryptionMethod    Algorithm="http://www.w3.org/2001/04/xmlenc#kw-
                aes128"/>
                <ds:KeyInfo>
                    <ds:RetrievalMethod URI="#EK"
 Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"/>
                </ds:KeyInfo>
                <enc:CipherData>
                    <enc:CipherReference URI=" EPUB/book.html"/>
                </enc:CipherData>
                </enc:EncryptedData>
                <enc:EncryptedData Id="ED2">
                        <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#kw-
aes128"/>
                <ds:KeyInfo>
                <ds:RetrievalMethod URI="#EK"
Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"/>
                </ds:KeyInfo>
                <enc:CipherData>
                     <enc:CipherReference URI=" EPUB/images/cover.png"/>
                </enc:CipherData>
              </enc:EncryptedData>
          </encryption>
```

ตัวอย่าง ข.6 เนื้อหาของไฟล์ EPUB/As You Like It.opf

```
<?xml version="1.0"?>
<package version="3.0"
        xml:lang="en"
        xmlns="http://www.idpf.org/2007/opf"
        unique-identifier="pub-id">
  <metadata xmlns:dc="http://purl.org/dc/elements/1.1/">
    <dc:identifier
      id="pub-id">urn:uuid:B9B412F2-CAAD-4A44-
B91FA375068478A0</dc:identifier>
    <meta refines="#pub-id"
      property="identifier-type"
      scheme="xsd:string">uuid</meta>
    <dc:language>en</dc:language>
    <dc:title>As You Like It</dc:title>
    <dc:creator id="creator">William Shakespeare</dc:creator>
    <meta refines="#creator"
      property="role"
      scheme="marc:relators">aut</meta>
    <meta property="dcterms:modified">2000-03-24T00:00:00Z</meta>
    <dc:publisher>Project Gutenberg</dc:publisher>
    <dc:date>2000-03-24</dc:date>
    <meta property="dcterms:dateCopyrighted">9999-01-01</meta>
    <dc:identifier
      id="isbn13">urn:isbn:9780741014559</dc:identifier>
    <meta refines="#isbn13"
      property="identifier-type"
      scheme="onix:codelist5">15</meta>
```

```
    <dc:identifier id="isbn10">0-7410-1455-6</dc:identifier>
    <meta refines="#isbn10"
        property="identifier-type"
       scheme="onix:codelist5">2</meta>
    <link rel="xml-signature"
         href="../META-INF/signatures.xml#AsYouLikeItSignature"/>
  </metadata>

  <manifest>
    <item id="r4915"
          href="book.html"
          media-type="application/xhtml+xml"/>
    <item id="r7184"
          href="images/cover.png"
          media-type="image/png"/>
    <item id="nav"
          href="nav.html"
          media-type="application/xhtml+xml"
          properties="nav"/>
    <item id="ncx"
          href="toc.ncx"
          media-type="application/x-dtbncx+xml"/>
  </manifest>
  <spine toc="ncx">
    <itemref idref="r4915"/>
  </spine>
</package>
```

ภาคผนวก ค.

(ข้อแนะนำ)

ชนิดสื่อ ***application/epub+zip***

(ข้อ 5.3)

ภาคผนวกนี้เป็นข้อแนะนำ

ภาคผนวกนี้แสดงชนิดสื่อ ***application/epub+zip*** สำหรับรูปแบบคอนเทนเนอร์เปิดของสิ่งพิมพ์อิเล็กทรอนิกส์ไฟล์โอซีเอฟเป็นเทคโนโลยีคอนเทนเนอร์ซึ่งเป็นรูปแบบอาร์ไคฝ์ซิป ใช้เพื่อห่อหุ้มเรนดิชั่นของสิ่งพิมพ์อิเล็กทรอนิกส์โอซีเอฟและมาตรฐานที่เกี่ยวข้องอยู่ในการดูแลและกำหนดโดยองค์กร IDPF

ชื่อชนิดสื่อไมม์:

application

ชื่อชนิดย่อยไมม์:

epub+zip

พารามิเตอร์ที่ต้องมี:

ไม่มี

พารามิเตอร์ทางเลือก:

ไม่มี

การพิจารณาด้านการเข้ารหัส:

ไฟล์โอซีเอฟเป็นไฟล์ไบนารีในรูปแบบซิป (http://www.iana.org/assignments/media-types/application/zip)

การพิจารณาด้านความปลอดภัย:

ตัวประมวลผลทั้งหมดที่อ่านไฟล์โอซีเอฟควรตรวจสอบขนาดและความถูกต้องของข้อมูลที่ค้นคืนมาอย่างเข้มงวด

นอกจากนั้นเนื่องจากมีเนื้อหาหลายชนิดที่สามารถฝังในไฟล์โอซีเอฟได้จึงเป็นไปได้ที่ ***application/epub+zip*** อาจอธิบายเนื้อหาที่มีข้อพิจารณาด้านความปลอดภัยนอกเหนือไปจากที่อธิบายไว้ในที่นี้อย่างไรก็ดีประเด็นด้านความปลอดภัยอาจเกิดขึ้นเฉพาะในกรณีที่ตัวประมวลผลรู้จำและประมวลผลเนื้อหาที่เพิ่มเติมเหล่านั้นหรือเมื่อการประมวลผลเนื้อหานั้นถูกส่งต่อให้กับตัวประมวลผลอื่นซึ่งในกรณีดังกล่าวจะอยู่นอกเหนือขอบเขตของเอกสารนี้

การพิจารณาด้านความปลอดภัยซึ่งใช้กับ ***application/zip*** จะใช้กับไฟล์โอซีเอฟด้วย

การพิจารณาด้านความสามารถในการทำงานร่วมกัน:

ไม่มี

โปรแกรมที่ใช้ชนิดสื่อนี้:

ชนิดสื่อนี้ถูกนำไปใช้อย่างกว้างขวางสำหรับแจกจ่ายหนังสืออิเล็กทรอนิกส์ในรูปแบบ EPUB บัญชีรายการของโปรแกรมต่อไปนี้ยังไม่ครอบคลุมทั้งหมด

- Adobe Digital Editions
- Aldiko
- Azardi
- Apple iBooks
- Barnes & Noble Nook
- Calibre
- Google Books
- Ibis Reader
- MobiPocket reader
- Sony Reader
- Stanza

ข้อมูลเพิ่มเติม:

เลขกล (Magic number(s)):

0: ***PK 0x03 0x04***, 30: ***mimetype***, 38: ***application/epub+zip***

นามสกุลไฟล์:

ส่วนใหญ่มักระบุไฟล์ OCF เป็นนามสกุล ***.epub***

รหัสชนิดไฟล์ Macintosh :

ZIP

ตัวระบุแฟรกเมนต์:

IDPF จัดเก็บทะเบียนผังที่เกี่ยวข้องไว้ที่ http://idpf.org/epub/linking/ บางส่วนของผังเหล่านี้กำหนดตัวระบุแฟรกเมนต์แบบกำหนดเองสำหรับแก้ไขเอกสาร ***application/epub+zip*** และ ***application/oebps-package+xml***

วัตถุประสงค์การใช้งาน:

ทั่วไป

ผู้แต่ง/ผู้ควบคุมการเปลี่ยนแปลง:

IDPF (http://www.idpf.org)

บรรณานุกรม

[ContentDocs30] *EPUB Content Documents 3.0*.

[HTML5] *HTML5: A vocabulary and associated APIs for HTML and XHTML*.

[MediaOverlays30] *EPUB Media Overlays 3.0.*

[OCF2] *Open Container Format 2.0.1.*

[OCF3] *Open Container Format 3.0*.

[Publications30] *EPUB Publication 3.0*.

[RFC2119] *Key words for use in RFCs to Indicate Requirement Levels (RFC 2119).* March 1997.

[RFC3986] *Uniform Resource Identifier (URI): Generic Syntax (RFC 3986).* Berners-Lee, et al. January 2005.

[RFC3987] *Internationalized Resource Identifiers (IRIs) (RFC 3987).* M Duerst, et al. January 2005.

[SHA-1] *Federal Information Processing Standards Publication 180-3: Secure Hash Standard (SHS)*. October 2008.

[TR15] *Unicode Normalization Forms*. Mark Davis, et al. 17 September 2010.

[Unicode] *The Unicode Consortium. The Unicode Standard, Version 5.0.0, defined by: The Unicode Standard, Version 5.0 (Boston, MA, Addison-Wesley, 2007. ISBN 0-321-48091-0)*.

[XML] *Extensible Markup Language (XML) 1.0 (Fifth Edition)*. T. Bray, et al. 26 November 2008.

[XML DSIG Core] *XML-Signature Syntax and Processing Version 1.1*. M. Bartel, et al. 3 March 2011.

[XML ENC Core] *XML Encryption Syntax and Processing Version 1.1.* D. Eastlake, et al. 3 March 2011.

[XML SIG Decrypt] *Decryption Transform for XML Signature*. M. Hughes, et al. 10 December 2002.

[XML Sec RNG Schemas] *XML Security RELAX NG Schemas*.

[XMLNS] *Namespaces in XML (Third Edition).* T. Bray, D. Hollander, A. Layman, R. Tobin. W3C. 8 December 2009.

[ZIP APPNOTE] *ZIP File Format Specification*. September 28, 2007. PKWARE, Inc..

ข้อมูลอ้างอิง (Informative References)

[EPUB3Changes] *EPUB 3 Differences from EPUB 2.0.1*. William McCoy, et al.

[EPUB3Overview] *EPUB 3 Overview*. Garth Conboy, et al.

[ODF] *ODF Open Document Format*.