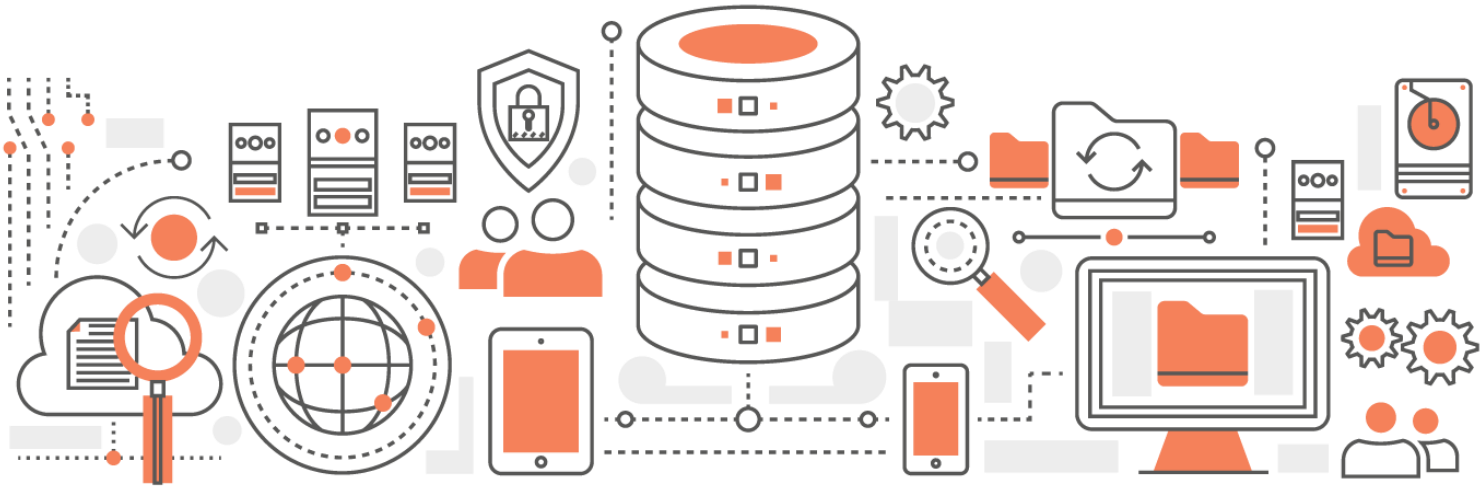
กรมอนามัย
DEPARTMENT OF HEALTH

มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน



สารบัญ

มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน 3

1. ขอบข่าย 3

2. นิยาม 3

3. กฎหมายและแนวปฏิบัติที่เกี่ยวข้อง 4

4. มาตรฐานการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน 4

5. แนวทางการพัฒนามาตรฐานฯ ด้านการเชื่อมโยงข้อมูล 7

6. แนวทางการพัฒนามาตรฐานฯ ด้านความหมายข้อมูล 10

บรรณานุกรม 13

เรื่อง ข้อกำหนดด้านความน่าเชื่อถือและความมั่นคงปลอดภัย 14

1. ขอบข่าย 14

2. นิยาม 14

3. กฎหมายและแนวปฏิบัติที่เกี่ยวข้อง 15

4. ข้อกำหนดด้านความน่าเชื่อถือและความมั่นคงปลอดภัย 15

บรรณานุกรม 22

เรื่อง ข้อกำหนดด้านโปรโตคอลระดับแอปพลิเคชันเอนพอยน์ และการจัดการโทเคนและเซสชัน 24

1. ขอบข่าย 24

2. นิยาม 24

3. กฎหมายและแนวปฏิบัติที่เกี่ยวข้อง 25

4. ข้อกำหนดด้านโปรโตคอลระดับแอปพลิเคชัน เอนพอยน์และการจัดการโทเคนและเซสชัน 25

บรรณานุกรม 32

เรื่อง ข้อกำหนดด้านการกำหนดชื่อและเนมสเปซ 33

1. ขอบข่าย 33

2. นิยาม 33

3. กฎหมายและแนวปฏิบัติที่เกี่ยวข้อง 33

4. ข้อกำหนดด้านการกำหนดชื่อและเนมสเปซ 34

บรรณานุกรม 36

เรื่อง ข้อกำหนดด้านการตรวจสอบระบบและการลงบันทึกล็อก 37

1. ขอบข่าย 37

2. นิยาม 37
3. กฎหมายและแนวปฏิบัติที่เกี่ยวข้อง 37
4. ข้อกำหนดด้านการตรวจสอบระบบและการลงบันทึกล็อก 38
บรรณานุกรม 40
เรื่อง ข้อกำหนดด้านการยืนยันตัวตน การควบคุมสิทธิ์และบัญชีการใช้งาน 41
1. ขอบข่าย 41
2. นิยาม 41
3. กฎหมายและแนวปฏิบัติที่เกี่ยวข้อง 41
4. ข้อกำหนดด้านการยืนยันตัวตน การควบคุมสิทธิ์และบัญชีการใช้งาน 42
บรรณานุกรม 47

มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน

1. ขอบข่าย

การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานเป็นพื้นฐานหลักที่จำเป็นต่อการพัฒนารัฐบาลดิจิทัลในปัจจุบันประเทศไทยมีแพลตฟอร์มการแลกเปลี่ยนข้อมูลที่ให้บริการอยู่หลายแห่ง แพลตฟอร์มแต่ละแห่งมีแนวทางและพันธกิจในการดำเนินงานเป็นของตนเอง เป็นผลให้การบูรณาการข้อมูลจำเป็นต้องขับเคลื่อนด้วยการสร้างมาตรฐานหรือข้อตกลงร่วมกันในการแลกเปลี่ยนข้อมูล กรมอนามัยจึงมีความจำเป็นต้องจัดทำมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลเพื่อใช้ในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน เพื่อให้เกิดการบูรณาการข้อมูลเกิดขึ้นอย่างเป็นรูปธรรม

เป้าประสงค์หลักของการใช้มาตรฐานฯ เป็นตัวขับเคลื่อนการบูรณาการข้อมูลหน่วยงาน คือ การให้หน่วยงานมีแนวทางในการพัฒนาระบบสารสนเทศเพื่อใช้ในการแลกเปลี่ยนข้อมูลที่ชัดเจน มีความสอดคล้องในการเชื่อมต่อระหว่างกันซึ่งจะทำให้ต้นทุนในการพัฒนาระบบสารสนเทศด้านการแลกเปลี่ยนข้อมูลน้อยลง ดังนั้น เพื่อให้บรรลุเป้าประสงค์หลักดังกล่าว เอกสารฉบับนี้จึงขอเสนอกรอบแนวทางในการพัฒนามาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานขึ้น เพื่อใช้เป็นกรอบอ้างอิงในการดำเนินการพัฒนามาตรฐานของกรมอนามัยเท่านั้น

2. นิยาม

นิยามคำศัพท์ที่เกี่ยวข้องกับกรอบแนวทางในการพัฒนามาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานที่ใช้ในเอกสารฉบับนี้มีดังนี้

2.1 ความสามารถในการทำงานร่วมกัน หรือ มาตรฐานการทำงานร่วมกัน (Interoperability) หมายความว่า การที่ระบบหรือหน่วยงานซึ่งมีความแตกต่างกันสามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพภายใต้ข้อมูลที่มีการแลกเปลี่ยนกัน

2.2 การเชื่อมโยงข้อมูล หมายความว่า การที่ระบบสารสนเทศตั้งแต่สองระบบขึ้นไป มีการเชื่อมต่อกันและรับส่งข้อมูลระหว่างกันผ่านการเรียกใช้ Application Programming Interface (API)

2.3 การแลกเปลี่ยนข้อมูล หมายความว่า การที่ระบบสารสนเทศตั้งแต่สองระบบขึ้นไป มีการเชื่อมโยงข้อมูลระหว่างกันและมีการนำข้อมูลที่รับส่งกันไปใช้ในการดำเนินงานขององค์กร (Organizational Process)

2.4 การแลกเปลี่ยนข้อมูลระดับเทคนิค (Technical Data Exchange) หมายความว่า ระบบสารสนเทศ ตั้งแต่สองระบบขึ้นไปสามารถแลกเปลี่ยนข้อมูลกันได้โดยมิได้คำนึงถึงความหมายของข้อมูลที่แลกเปลี่ยนกัน

2.5 การแลกเปลี่ยนความหมายข้อมูล (Semantic Meaning Exchange) หมายความว่า ระบบสารสนเทศ ตั้งแต่สองระบบขึ้นไปสามารถแลกเปลี่ยนข้อมูลกันได้และสามารถเข้าใจความหมายของข้อมูลที่แลกเปลี่ยนกัน

2.6 ข้อตกลงในขั้นตอนการดำเนินงานขององค์กร (Organizational Process Agreement) หมายความว่า องค์กรที่เกี่ยวข้องในข้อมูลที่แลกเปลี่ยนกันมีข้อตกลงในการดำเนินงานร่วมกันเมื่อเกิดการแลกเปลี่ยนข้อมูล

2.7 ศูนย์แลกเปลี่ยนข้อมูลกลาง (Data Exchange Center) หมายความว่า ศูนย์กลางในการแลกเปลี่ยนข้อมูลดิจิทัลและทะเบียนดิจิทัลระหว่างหน่วยงานของรัฐ เพื่อสนับสนุนการดำเนินการของหน่วยงานของรัฐในการให้บริการประชาชนผ่านระบบดิจิทัล

2.8 ผู้ให้บริการแลกเปลี่ยนข้อมูล (Data Exchange Provider) หมายความว่า หน่วยงานที่มีความรับผิดชอบในการดำเนินการศูนย์แลกเปลี่ยนข้อมูลกลาง

2.9 ผู้ให้บริการข้อมูล (Data Provider หรือ Service Provider) หมายความว่า บุคคลหรือหน่วยงานผู้เป็นเจ้าของข้อมูลที่ให้บริการอยู่ในศูนย์แลกเปลี่ยนข้อมูลกลาง

2.10 ผู้ใช้บริการข้อมูล (Data Consumer หรือ Service Consumer) หมายความว่า บุคคลหรือหน่วยงานผู้ใช้บริการข้อมูลจากหน่วยงานอื่นที่ให้บริการข้อมูลอยู่ในศูนย์แลกเปลี่ยนข้อมูลกลาง

2.11 รีซอร์สข้อมูล (Data Resource) หมายความว่า ระบบสารสนเทศที่เชื่อมต่อกับศูนย์แลกเปลี่ยนข้อมูลกลางในการให้บริการข้อมูล ผู้ให้บริการข้อมูลมีความรับผิดชอบต่อระบบสารสนเทศนี้

2.12 แอปพลิเคชัน (Application) หมายความว่า ระบบสารสนเทศที่เชื่อมต่อกับศูนย์แลกเปลี่ยนข้อมูลกลางใช้ข้อมูลจากรีซอร์สข้อมูลในการให้บริการประชาชน หน่วยงานของรัฐ หรือหน่วยงานเอกชน

2.13 ความหมายข้อมูล (Semantic) หมายความว่า วิธีการในตีความหมายจากข้อมูลที่มีการแลกเปลี่ยนกัน เช่น "Gender" = "M" หมายถึงเพศชาย "Gender" = "F" หมายถึง เพศหญิง เป็นต้น

2.14 กลุ่มข้อมูลหลัก (Core Data) หมายความว่า กลุ่มข้อมูลที่ไม่อ้างอิงกับโดเมนข้อมูล (Data Domain) ใด ๆ เช่น ข้อมูลบุคคล ข้อมูลสถานที่ ข้อมูลองค์กร เป็นต้น

2.15 กลุ่มข้อมูลอ้างอิงทั่วไป (Common Reference Data) หมายความว่า กลุ่มข้อมูลที่ใช้สำหรับการอ้างอิงจากกลุ่มข้อมูลอื่น เช่น ข้อมูลจังหวัด ข้อมูลอำเภอ ข้อมูลตำบล ข้อมูลถนน ข้อมูลเพศ ข้อมูลศาสนา เป็นต้น

2.16 กลุ่มข้อมูลขยาย (Extend Data) หมายความว่า กลุ่มข้อมูลเฉพาะทางโดเมนนั้น ๆ เช่น กลุ่มข้อมูลด้านการเกษตร กลุ่มข้อมูลด้านสาธารณะสุข กลุ่มข้อมูลด้านการเงิน เป็นต้น

2.17 กลุ่มข้อมูลอ้างอิงเฉพาะโดเมน (Domain Reference Data) หมายความว่า ข้อมูลอ้างอิงพื้นฐานที่ขึ้นกับความต้องการเฉพาะธุรกิจ (Business Data) เช่น ข้อมูลสถานะนิติบุคคล ข้อมูลรหัสวัตถุประสงค์นิติบุคคล เป็นต้น

2.18 ประเภทข้อมูล (Data Type) หมายความว่า คลาสข้อมูล (Data Class) หรือ อ็อบเจกต์ข้อมูล (Data Object) ที่มีการนิยามขึ้นมาสำหรับใช้ในการเก็บข้อมูล แบ่งเป็นสองประเภทคือ Simple Type และ Complex Type

2.19 รูปแบบข้อมูล (Data Format) หมายความว่า วิธีการนำเสนอข้อมูล (Data Representation) เพื่อให้แปลความหมายข้อมูลได้อย่างถูกต้อง

3. กฎหมายและแนวปฏิบัติที่เกี่ยวข้อง

การเชื่อมโยงและการแลกเปลี่ยนข้อมูลภาครัฐมีการบัญญัติไว้ในกฎหมายหรือแนวปฏิบัติที่เกี่ยวข้อง ดังนี้

3.1 รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 ในมาตรา 59 ระบุว่ารัฐต้องเปิดเผยข้อมูลหรือข่าวสารสาธารณะในครอบครองของหน่วยงานของรัฐที่มิใช่ข้อมูลเกี่ยวกับความมั่นคงของรัฐหรือเป็นความลับของทางราชการตามที่กฎหมายบัญญัติ และต้องจัดให้ประชาชนเข้าถึงข้อมูลหรือข่าวสารดังกล่าวได้โดยสะดวก

3.2 พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 ในมาตรา 13 ระบุว่าเพื่อประโยชน์ในการบริหารราชการแผ่นดินและการให้บริการประชาชนให้หน่วยงานของรัฐจัดให้มีการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลที่มีการจัดทำและครอบครองตามที่หน่วยงานของรัฐแห่งอื่นร้องขอที่จะเกิดการบูรณาการร่วมกันมาตรา 15 ระบุว่าให้มีศูนย์แลกเปลี่ยนข้อมูลกลางทำหน้าที่เป็นศูนย์กลางในการแลกเปลี่ยนข้อมูลดิจิทัลและทะเบียนดิจิทัลระหว่างหน่วยงานของรัฐ เพื่อสนับสนุนการดำเนินการของหน่วยงานของรัฐ ในการให้บริการประชาชนผ่านระบบดิจิทัล และดำเนินการในเรื่องดังต่อไปนี้

(1) กำหนดนโยบายและมาตรฐานเกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลเสนอต่อคณะกรรมการพัฒนารัฐบาลดิจิทัลให้ความเห็นชอบ

(2) ประสานและให้ความช่วยเหลือแก่หน่วยงานของรัฐในการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลระหว่างกัน รวมทั้งกำกับติดตามให้การดำเนินการดังกล่าวเป็นไปในแนวทางและมาตรฐานเดียวกันตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่กำหนด

(3) จัดทำคำอธิบายชุดข้อมูลดิจิทัลของภาครัฐ และจัดเก็บบันทึกหลักฐานของการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล

(4) เรื่องอื่น ๆ ตามที่หน่วยงานมอบหมาย

4. มาตรฐานการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน

มาตรฐานการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานของรัฐ คือ มาตรฐานการทำงานร่วมกันของหน่วยงานซึ่งมีความหลากหลายและความแตกต่างในเชิงพันธกิจสามารถทำงานร่วมกันได้อย่างมีปฏิสัมพันธ์กันเพื่อให้เกิดประโยชน์ร่วมกันและมุ่งสู่จุดมุ่งหมายร่วมกัน มาตรฐานดังกล่าวว่าด้วยการแบ่งปันสารสนเทศและองค์ความรู้ระหว่างองค์การผ่านทางกระบวนการทางธุรกิจขององค์กรเหล่านั้นโดยอาศัยการแลกเปลี่ยนข้อมูลผ่านทางเทคโนโลยีสารสนเทศและการสื่อสาร

การเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐเป็นหนึ่งในนโยบายหลักของรัฐบาลที่ต้องเร่งดำเนินการให้เกิดขึ้นเพื่อให้พร้อมต่อมาตรฐานการทำงานร่วมกันของหน่วยงานของรัฐเป็นที่สังเกตว่าปัญหาการแลกเปลี่ยนข้อมูลเป็นปัญหาที่เทียบเคียงได้กับปัญหามาตรฐานการทำงานร่วมกัน เนื่องจากปัญหาทั้งสองมีแนวทางและความต้องการเหมือนกัน ดังนั้นการพัฒนา

มาตรฐานการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานนั้นเราสามารถใช้ตัวแบบอ้างอิงมาตรฐานการทำงานร่วมกันของรัฐบาลดิจิทัล (Digital Government Interoperation Reference Model) เป็นกรอบแนวทางในการพัฒนามาตรฐานได้

4.1. ตัวแบบอ้างอิงมาตรฐานการทำงานร่วมกันสำหรับรัฐบาลดิจิทัล

ในการอธิบายถึงตัวแบบอ้างอิงมาตรฐานการทำงานร่วมกันสำหรับรัฐบาลดิจิทัลนั้น จะต้องเริ่มต้นจากจุดประสงค์ของมาตรฐานการทำงานร่วมกันก่อน จากนั้นจึงจะเชื่อมโยงจุดประสงค์เหล่านั้นไปเป็นมาตรฐานในระดับต่าง ๆ โดยที่จุดประสงค์ที่มีความซับซ้อนมากขึ้นก็จะเชื่อมกับมาตรฐานในระดับที่สูงขึ้น และท้ายสุดก็เข้าสู่บริบทที่เกี่ยวข้องเฉพาะกับหน่วยงานโดยการใส่ปัจจัยที่มีผลกระทบลงไปในตัวแบบ

4.1.1 จุดประสงค์ของมาตรฐานการทำงานร่วมกัน

ระหว่างระบบสารสนเทศใด ๆ ที่ใช้มาตรฐานการทำงานร่วมกันจะมีจุดประสงค์ของการทำงานร่วมกันอยู่สามประการ คือ เพื่อให้เกิดการแลกเปลี่ยนข้อมูล (Data Exchange) เพื่อให้เกิดการแลกเปลี่ยนความหมาย(Meaning Exchange) และเพื่อให้เกิดข้อตกลงในขั้นตอนการดำเนินงาน (Process Agreement)

(1) เพื่อให้เกิดการแลกเปลี่ยนข้อมูล: จุดประสงค์แรกของมาตรฐานการทำงานร่วมกัน คือ การแลกเปลี่ยนข้อมูลระหว่างกันในระดับพื้นฐาน (Basic Data Exchange) จุดประสงค์นี้ไม่ได้สนใจในความหมายของข้อมูลที่แลกเปลี่ยนกัน กำหนดเพียงแค่ให้มีการแลกเปลี่ยนข้อมูลกันได้เท่านั้น ตัวอย่างเช่น ระบบ สารสนเทศสองระบบสามารถแลกเปลี่ยนข้อมูลกันได้ภายใต้ข้อตกลงเรื่องขนาดของข้อมูลว่าเป็นข้อมูลตัวเลขที่มีทศนิยมสองตำแหน่ง โดยไม่ได้สนใจว่าข้อมูลนี้คือข้อมูลอะไร เป็นต้น

(2) เพื่อให้เกิดการแลกเปลี่ยนความหมาย : จุดประสงค์ที่สองนี้หมายถึงระบบสารสนเทศที่แลกเปลี่ยนข้อมูลกันเข้าใจถึงความหมายของข้อมูลนั้นร่วมกัน ตัวอย่างเช่น ตัวเลขทศนิยมสองตำแหน่งที่แลกเปลี่ยนกันคืออัตราการแลกเปลี่ยนระหว่างสกุลเงิน เป็นต้น การแลกเปลี่ยนความหมายมีความ แตกต่างจากการแลกเปลี่ยนข้อมูลตรงที่การแปลความหมายข้อมูลของผู้เกี่ยวข้องในระบบ ปัญหาของ การแลกเปลี่ยนข้อมูลก็เพียงแค่ข้อมูลเกิดการแลกเปลี่ยนหรือไม่เกิดการแลกเปลี่ยน แต่ปัญหาของการแลกเปลี่ยนความหมาย คือ ระบบไม่สามารถรับประกันได้ว่าผู้เกี่ยวข้องทั้งหมดจะเข้าใจความหมายได้ตรงกัน ตัวอย่างเช่น หน่วยวัดของข้อมูลที่แลกเปลี่ยนกันมีข้อกำหนดเหมือนกันในทุกหน่วยงานหรือไม่ เป็นต้น

(3) เพื่อให้เกิดข้อตกลงในด้านขั้นตอนการดำเนินงาน : จุดประสงค์ที่สามคือระบบจะปฏิบัติต่อสารสนเทศที่มีการแลกเปลี่ยนกันอย่างไร โดยผู้เกี่ยวข้องทั้งหมดจะต้องมีความเข้าใจตรงกันในการปฏิบัติต่อสารสนเทศที่มีการแลกเปลี่ยนกัน จุดประสงค์ที่สามนี้แตกต่างจากทั้งสองจุดประสงค์ที่ผ่านมาตรงที่ เปลี่ยนจากการให้ความสำคัญกับการแลกเปลี่ยนสารสนเทศไปเป็นแนวปฏิบัติของผู้เกี่ยวข้องที่มีการ แลกเปลี่ยนสารสนเทศกัน ในการที่จะบรรลุจุดประสงค์ในข้อนี้ ผู้เกี่ยวข้องในระบบจะต้องบรรลุ ข้อตกลงร่วมกันก่อนว่าจะทำอย่างไรกับสารสนเทศที่ได้รับ ข้อตกลงในด้านขั้นตอน การดำเนินงานเป็นสิ่งที่ซับซ้อนและมีความหลากหลาย ซึ่งหน่วยงานต้องใช้ความพยายามอย่างมากใน การดำเนินการเพื่อให้แนวคิด Once-only Principle [2] ให้เป็นรูปธรรม

4.1.2 ระดับของมาตรฐานการทำงานร่วมกัน ที่สอดคล้องกับจุดประสงค์เหล่านั้นได้ ดังนี้

(1) มาตรฐานการทำงานร่วมกันระดับเทคนิค (Technical Interoperability)

เชื่อมโยงกับจุดประสงค์เพื่อให้เกิดการแลกเปลี่ยนข้อมูลมาตรฐานระดับนี้เทคนิคเป็นพื้นฐานและจุดเริ่มต้นของการแลกเปลี่ยนข้อมูล ระหว่างกัน

(2) มาตรฐานการทำงานร่วมกันระดับความหมาย (Semantic Interoperability)

เชื่อมโยงกับจุดประสงค์เพื่อให้เกิดการแลกเปลี่ยนความหมายมาตรฐานระดับความหมายอยู่เหนือมาตรฐานระดับเทคนิค เพราะว่าการแลกเปลี่ยนความหมายจะเกิดขึ้นได้จำเป็นต้องมีการแลกเปลี่ยนข้อมูลให้ได้ก่อน

(3) มาตรฐานการทำงานร่วมกันระดับองค์กร (Organizational Interoperability)

เชื่อมโยงกับจุดประสงค์ เพื่อให้เกิดข้อตกลงในด้านขั้นตอนการดำเนินงาน มาตรฐานระดับองค์กรนี้จำเป็นต้องอาศัยมาตรฐานระดับความหมายและมาตรฐานระดับเทคนิคเป็นแกนขับเคลื่อนเพื่อให้เกิดขั้นตอนการทำงานร่วมกันระหว่างหน่วยงานได้

4.1.3 ปัจจัยที่มีผลต่อมาตรฐานการทำงานร่วมกันสำหรับหน่วยงาน

บริบทของหน่วยงานเป็นเรื่องที่ซับซ้อนเนื่องจากมีประเด็นที่เกี่ยวข้องอยู่มากไม่ว่าจะเป็นระเบียบกฎหมาย การเมืองและนโยบาย และวัฒนธรรมทางสังคม ปัจจัย (Influence Factors) ทั้งสามนี้ส่งผลต่อทุกระดับของตัวแบบอย่างหลีกเลี่ยงไม่ได้ [1] และให้ผลที่แตกต่างกันไปตามสถานการณ์จากมุมมองของนักพัฒนาระบบนั้นปัจจัยทั้งสามนี้เป็นสิ่งที่ต้อง

พิจารณาเพิ่มจากปัญหาด้านมาตรฐานการทำงานร่วมกัน การเข้าสู่ทุกระดับของมาตรฐานการทำงานร่วมกันจะต้องสอดคล้องกับปัจจัยทั้งสาม ดังต่อไปนี้

(1) ปัจจัยด้านระเบียบกฎหมาย: หนึ่งในข้อสังเกตทางด้านระเบียบกฎหมายคือการบังคับใช้กฎหมายกับบริการดิจิทัลของภาครัฐที่จะมาสนับสนุนหรือแทนที่บริการแบบเดิม การบังคับใช้กฎหมายต่อบริการภาครัฐนั้นไม่เพียงแค่ว่าจะต้องกำหนดให้มีบริการใดบ้าง แต่ยังรวมถึงบริการแบบใดที่ไม่ควรมี เช่น บริการที่ไม่สอดคล้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล เป็นต้น

(2) ปัจจัยด้านนโยบายการเมือง: ผู้บริหารจะต้องมีความมุ่งมั่นและอำนาจทางการเมืองอย่างแท้จริงในการผลักดันโครงการ ให้การสนับสนุนด้านการเงินในโครงการด้านมาตรฐานการทำงานร่วมกันของหน่วยงาน และจำเป็นต้องจัดการเรื่องความความสัมพันธ์ระหว่างหน่วยงานของรัฐเพื่อให้เกิดโอกาสแห่งความสำเร็จ ถ้าปราศจากการสนับสนุนด้านนี้แล้วเป็นเรื่องยากที่จะเชื่อได้ว่าหน่วยงานรัฐจะร่วมมือกันในการจัดการปัญหามาตรฐานการทำงานร่วมกันในระดับเทคนิค ระดับความหมาย และระดับองค์กร

(3) ปัจจัยด้านสังคมและวัฒนธรรม: อีกปัจจัยหนึ่งที่มีอิทธิพลกับนักออกแบบระบบที่จะต้องพิจารณ าคือ ด้านสังคมและวัฒนธรรม เช่น การระบุข้อมูลด้านศาสนาหรือข้อมูลด้านเพศ ระบบอาจจะต้องมีตัวเลือกเพิ่มเติมจากตัวเลือกที่มีอยู่เดิมเพื่อให้สอดคล้องกับการยอมรับทางสังคมที่มีการเปลี่ยนแปลงไป การออกแบบตัวประสาน (Interface) ระหว่างระบบกับผู้ใช้งานควรสอดคล้องกับลักษณะการใช้งานที่เปลี่ยนไปจากอดีต เช่น การใช้ระบบจอภาพระบบสัมผัสหรือแม้แต่การเลือกใช้ภาษาในระบบที่อาจเป็นที่ยอมรับในสังคมหนึ่งแต่ไม่เป็นที่ยอมรับในอีกสังคมหนึ่ง เป็นต้น

4.2 การพัฒนามาตรฐานการเชื่อมโยงและการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน

การจะพัฒนามาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐสำหรับหน่วยงานให้ประสบผลสำเร็จนั้นจำเป็นต้องมีกรอบแนวทางที่ชัดเจนในการดำเนินงานเนื่องจากการพัฒนามาตรฐานดังกล่าวเป็นงานที่ท้าทายอย่างมากเพราะต้องดำเนินการทั้งในระดับเทคนิคระดับความหมาย และระดับองค์กรในเวลาเดียวกัน นอกจากนี้ยังจำเป็นต้องมีหน่วยงานหลักในการขับเคลื่อนเพราะต้องจัดการกับปัญหาต่าง ๆ อันเนื่องมาจากปัจจัยด้านระเบียบกฎหมาย การเมืองและนโยบาย และวัฒนธรรมทางสังคม ซึ่งต้องใช้ความพยายามอย่างสูงในการผลักดัน

การพัฒนามาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานจำเป็นจะต้องดำเนินการไปพร้อมกันทั้งสามระดับ ได้แก่ มาตรฐานระดับเทคนิค มาตรฐานระดับความหมาย และมาตรฐานระดับองค์กร ดังนั้นการพัฒนามาตรฐานจึงเป็นการสร้างมาตรฐานทั้งสามระดับร่วมกันบนกรณีศึกษาที่เป็นรูปธรรมและเน้นไปทางด้านการใช้ในระดับต่าง ๆ กรอบแนวทางดังกล่าวได้จากการพิจารณาร่วมกันของด้านการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานของหน่วยงานภาครัฐที่เกี่ยวข้อง รายละเอียดของมาตรฐานแต่ละชุดมีดังต่อไปนี้

(1) มาตรฐานระดับเทคนิคมีการกำหนดชื่อเรียกในการพัฒนาว่า “มาตรฐานฯ ด้านการเชื่อมโยงข้อมูล” หรือ Linkage Standard มาตรฐานชุดนี้มุ่งเน้นให้เกิดข้อกำหนดร่วมกันทางเทคนิคเพื่อให้เกิดการ เชื่อมต่อระหว่างระบบสารสนเทศของผู้เกี่ยวข้อง มาตรฐานการเชื่อมโยงนี้แบ่งออกเป็นสองส่วน คือ สถาปัตยกรรมอ้างอิงของระบบ (Reference Architecture) และ ชุดมาตรฐานข้อกำหนดด้านเทคนิค (Technical Requirement Standard)

(2) มาตรฐานระดับความหมายมีการกำหนดชื่อในการพัฒนาว่า “มาตรฐานฯ ด้านความหมายข้อมูล” หรือ Semantic Standard มาตรฐานชุดนี้มุ่งเน้นให้หน่วยงานของรัฐมีการใช้ข้อมูลที่อ้างอิงบนสคีมา (Schema) เดียวกันและแปลความหมายข้อมูลแบบเดียวกัน ตัวอย่างเช่น ข้อมูลบุคคล (Person) จะอ้างอิงบนชื่อฟิลด์ข้อมูล (Data Field Name) และประเภทข้อมูล (Data Type) เดียวกันในการแลกเปลี่ยน นอกจากนี้ยังรวมถึงมาตรฐานข้อมูลอ้างอิงของประเทศเช่น รหัสประเทศ รหัสจังหวัด รหัสถนน เป็นต้น

(3) เพื่อที่จะผลักดันมาตรฐานระดับเทคนิคและระดับความหมายให้เกิดเป็นมาตรฐานระดับองค์กรและเกิดการใช้งานจริง จำเป็นที่จะต้องนำมาตรฐานทั้งสองไปทดสอบกับกระบวนการทางธุรกิจที่มีอยู่หรือที่กำลังจะเกิดขึ้น ด้วยเหตุนี้การพัฒนามาตรฐานระดับองค์กรนี้จะแตกต่างไปจากการพัฒนามาตรฐานทั้งสองก่อนหน้านี้

4.3 ข้อแนะนำสำหรับหน่วยงานภาครัฐในการปรับระบบเข้าสู่มาตรฐานฯ

ผลกระทบของหน่วยงานภาครัฐต่อมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลแบ่งออกได้ 3 กลุ่ม ได้แก่ กลุ่มผู้ให้บริการแพลตฟอร์มแลกเปลี่ยนข้อมูล กลุ่มผู้ให้บริการข้อมูลและกลุ่มผู้ใช้บริการข้อมูล ข้อเสนอแนะสำหรับแต่ละกลุ่มมีดังต่อไปนี้

กลุ่มที่ 1 : ผู้ให้บริการแพลตฟอร์มแลกเปลี่ยนข้อมูล (Exchange Platform Provider) เป็นกลุ่มผู้เกี่ยวข้องที่มีจำนวนน้อย ข้อเสนอแนะต่อผู้เกี่ยวข้องในกลุ่มนี้ มีดังนี้

(1) สำหรับหน่วยงานที่กำลังจะเป็นผู้ให้บริการแต่ยังไม่ได้พัฒนาระบบควรนำมาตรฐานฯ ด้านการเชื่อมโยงข้อมูล (Linkage Standard) เป็นข้อพิจารณาในการพัฒนาระบบหรือเป็นข้อกำหนดของการจัดซื้อจัดจ้าง (Term of Reference) เพื่อให้ระบบที่จะพัฒนามีการทำงานในระดับเทคนิคสอดคล้องกับมาตรฐานฯ ซึ่งนำไปสู่ความสะดวกในการเชื่อมต่อกับแพลตฟอร์มหรือระบบสารสนเทศในการแลกเปลี่ยนข้อมูลอื่น หน่วยงานกลุ่มนี้ได้รับผลกระทบจากมาตรฐานฯ ในระดับสูง

(2) สำหรับหน่วยงานที่ดำเนินการให้บริการอยู่ควรศึกษาตัวมาตรฐาน เพื่อประเมินข้อดีและข้อเสียความคุ้มค่าในการใช้มาตรฐาน มูลค่าการลงทุนในกรณีที่มีการปรับเปลี่ยนเมื่อถึงวงรอบอายุการใช้งานของระบบก็ควรจะนำผลการประเมินเป็นข้อพิจารณาในการปรับปรุงระบบต่อไป หน่วยงานกลุ่มนี้มีผลกระทบจากมาตรฐานในระดับสูงที่สุด

กลุ่มที่ 2 : ผู้ให้บริการข้อมูล (Data Provider) เป็นกลุ่มผู้เกี่ยวข้องที่มีจำนวนมากกว่ากลุ่มแรกมาก พิจารณาได้จากจำนวนหน่วยงานที่เป็นผู้ให้บริการข้อมูลในแพลตฟอร์มข้อเสนอแนะต่อผู้เกี่ยวข้องในกลุ่มนี้ มีดังนี้

(1) สำหรับหน่วยงานที่กำลังจะเป็นผู้ให้บริการข้อมูลแต่ยังไม่ได้พัฒนาระบบสารสนเทศเพื่อการเชื่อมต่อกับแพลตฟอร์มแลกเปลี่ยนข้อมูล ควรนำแนวทางของการแบ่งประเภทข้อมูลในมาตรฐานฯด้านความหมายข้อมูล (Semantic Standard) มาพิจารณาในการพัฒนาว่าข้อมูลของหน่วยงานท่านอยู่ในหมวดหมู่ใดและสามารถทำตามมาตรฐานได้หรือไม่ นอกจากนี้ยังควรนำมาตรฐานฯ ด้านการเชื่อมโยงข้อมูล (Linkage Standard) มาเป็นข้อพิจารณาในการพัฒนาระบบสารสนเทศของท่านเพื่อเป็นการสร้างทางเลือกในกรณีที่ต้องปรับปรุงระบบด้านเทคนิคให้เข้าสู่มาตรฐานนอกเหนือจากข้อกำหนดของแพลตฟอร์มที่หน่วยงานต้องการจะเชื่อมต่อ เช่น มาตรฐานด้านการยืนยันตัวตนต่อแพลตฟอร์ม มาตรฐานเรื่องโปรโตคอลในการเชื่อมต่อ เป็นต้น หน่วยงานกลุ่มนี้มีผลกระทบจากมาตรฐานในระดับต่ำ

(2) สำหรับหน่วยงานที่เป็นผู้ให้บริการข้อมูลอยู่แล้วในแพลตฟอร์มใด ๆ ที่ดำเนินการอยู่ควรนำแนวทางของการแบ่งประเภทข้อมูลในมาตรฐานฯ ด้านความหมายข้อมูล (Semantic Standard) มาพิจารณาว่าข้อมูลของหน่วยงานท่านอยู่ในหมวดหมู่ใด หน่วยงานกลุ่มนี้มีผลกระทบจากมาตรฐานในระดับปานกลาง

กลุ่มที่ 3 : ผู้ใช้บริการข้อมูล (Data Consumer) เป็นกลุ่มผู้เกี่ยวข้องที่มีจำนวนมากที่สุดข้อเสนอแนะต่อผู้เกี่ยวข้องในกลุ่มนี้มีดังนี้

(1) สำหรับหน่วยงานที่กำลังจะเป็นผู้ใช้บริการข้อมูลแต่ยังไม่ได้พัฒนาระบบสารสนเทศควรตรวจสอบว่าข้อมูลที่ต้องการจะใช้งานเป็นข้อมูลอะไร หน่วยงานใดเป็นเจ้าของข้อมูลและให้บริการอยู่ที่แพลตฟอร์มแลกเปลี่ยนข้อมูลใด เนื่องจากข้อมูลดังกล่าวอาจให้บริการทั้งในรูปแบบดั้งเดิมและรูปแบบมาตรฐาน ผู้พัฒนาระบบควรใช้มาตรฐานฯ ด้านความหมายข้อมูล (Sematic Standard) เป็นแนวปฏิบัติในการพัฒนาระบบในทำนองเดียวกันทางผู้พัฒนาระบบควรตรวจสอบว่าวิธีการเชื่อมต่อทางเทคนิคกับผู้ให้บริการแพลตฟอร์มสามารถดำเนินการด้วยมาตรฐานฯ ด้านการเชื่อมโยงข้อมูล (Linkage Standard) หรือวิธีการดั้งเดิมของแพลตฟอร์ม ซึ่งการเชื่อมต่อด้วยวิธีมาตรฐานจะเป็นทางเลือกที่สร้างความคุ้มค่าต่อต้นทุนในการพัฒนาระบบหน่วยงานกลุ่มนี้มีผลกระทบจากมาตรฐานในระดับต่ำ

(2) สำหรับหน่วยงานที่เป็นผู้ใช้บริการข้อมูลจะต้องพิจารณามาตรฐานด้านข้อมูลว่าข้อมูลที่ใช้งานมีการประกาศมาตรฐานไว้หรือไม่ ถ้ามีให้นำไปเป็นข้อพิจารณาในการปรับปรุงระบบเมื่อครบวงรอบอายุการใช้งานของระบบสารสนเทศ ส่วนในกรณีด้านการเชื่อมต่อก็ขึ้นอยู่กับผู้ให้บริการแลกเปลี่ยนข้อมูลว่ามีทางเลือกการเชื่อมต่อแบบมาตรฐานหรือไม่ ถ้ามีก็ควรปรับไปสู่ระบบการเชื่อมต่อแบบมาตรฐานหน่วยงานกลุ่มนี้มีผลกระทบจากมาตรฐานในระดับปานกลาง

5. แนวทางการพัฒนามาตรฐานฯ ด้านการเชื่อมโยงข้อมูล

การพัฒนามาตรฐานฯ ด้านการเชื่อมโยงข้อมูลมุ่งเน้นไปที่ (1) สถาปัตยกรรมอ้างอิงของระบบแลกเปลี่ยนข้อมูล และ (2) ข้อกำหนดด้านเทคนิคในการแลกเปลี่ยนข้อมูล อย่างไรก็ตามการพัฒนามาตรฐานดังกล่าวต้องพิจารณาถึงแพลตฟอร์มการแลกเปลี่ยนข้อมูลของหน่วยงานภาครัฐที่ดำเนินการอยู่ควบคู่ไปด้วยดังนั้นการศึกษาคุณลักษณะสำคัญของแพลตฟอร์มเหล่านั้นจึงมีความจำเป็น

5.1 สถาปัตยกรรมอ้างอิงเบื้องต้นของระบบแลกเปลี่ยนข้อมูล

สถาปัตยกรรมอ้างอิงเบื้องต้น (Initial Reference Architecture) ของมาตรฐานฯด้านการเชื่อมโยงข้อมูลองค์ประกอบ (Components) อินเตอร์เฟสและฟังก์ชัน (Interfaces and Functions) ของสถาปัตยกรรมอ้างอิงดังกล่าวมา

จากผลการสำรวจแพลตฟอร์มที่ให้บริการอยู่ในปัจจุบันของประเทศ ดังนั้นจึงกล่าวได้ว่าสถาปัตยกรรมอ้างอิงนี้เป็นข้อกำหนดขั้นต่ำที่แพลตฟอร์มการแลกเปลี่ยนข้อมูลภายใต้มาตรฐานฯ ต้องปฏิบัติตาม รายละเอียดของสถาปัตยกรรมอ้างอิงเบื้องต้นมีดังต่อไปนี้

(1) Central Data Exchange ทำหน้าที่เป็นศูนย์กลางควบคุมการแลกเปลี่ยนข้อมูลระหว่าง Provider และ Consumer มีหน้าที่ในการยืนยันตัวตน (Authentication) ตรวจสอบสิทธิการใช้ข้อมูลตามนโยบายที่กำหนดไว้ (Authorization) หรือตรวจสอบจำนวนการใช้งานข้อมูล (Accounting) หรือตรวจสอบสถานะของ Provider เป็นต้น

(2) Service Catalog ทำหน้าที่แสดงบัญชีรายการ Application Programming Interface (API) ที่ Provider ให้บริการข้อมูลในแพลตฟอร์ม รายการ API แต่ละชุด จะประกอบด้วยรายละเอียดต่าง ๆ เช่น คำอธิบายข้อมูล เมทาดาต้า วิธีการเรียกใช้ API และ Message Request เป็นต้น

(3) Monitoring and Logging ทำหน้าที่ตรวจสอบติดตามสภาวะการทำงาน (Operation) และสภาวะแวดล้อม (Environment) ของระบบ รวมถึงทำการบันทึกล็อค (Log) การทำงานของระบบบันทึกการแลกเปลี่ยนเพื่อใช้เป็นหลักฐานทางกฎหมาย รวมถึงเพื่อนำข้อมูลไปใช้ในการวิเคราะห์ต่อไป

(4) Certificate Authority ทำหน้าที่เป็นผู้รับลงทะเบียนสำหรับ Provider และ Consumer ของระบบเป็นผู้ออกใบรับรองดิจิทัล (Digital Certificate) หรือพารามิเตอร์ที่เป็นอัตลักษณ์ของผู้เกี่ยวข้องสำหรับการเชื่อมต่อกับแพลตฟอร์ม เช่น Public Key องค์ประกอบนี้ควรแยกออกจาก Central Data Exchange เนื่องจากอาจถูกใช้เป็น Certificate Authority ในระดับ Federation ได้ในอนาคต

(5) Time-Stamping และ Digital Signature เป็นองค์ประกอบมาตรฐานเวลาและมาตรฐานลายเซ็นดิจิทัลที่ใช้ยืนยันการแลกเปลี่ยน Message และใช้ในการบันทึก Log องค์ประกอบ Time-Stamping อาจทำงานประสานกับ Time-Stamping ของแพลตฟอร์มอื่นในกรณีที่ต้องแลกเปลี่ยนข้อมูลกับต่างประเทศหรือข้ามโซนเวลา องค์ประกอบทั้งสองนี้ควรแยกออกจาก Central Data Exchange ด้วยเหตุผลเดียวกับ Certificate Authority เนื่องจากอาจมีการทำงานเป็นแบบ Federation ในอนาคต

(6) Provider's Resource คือระบบสารสนเทศที่ให้บริการข้อมูลซึ่งอยู่ภายใต้การดูแลของ Provider (หน่วยงานหรือบุคคล) ซึ่งเป็นเจ้าของข้อมูลและเป็นผู้กำหนดสิทธิในการใช้ข้อมูลสำหรับ Consumer

(7) Consumer's Application คือระบบสารสนเทศที่ใช้บริการข้อมูลซึ่งอยู่ภายใต้การดูแลของ Consumer (หน่วยงานหรือบุคคล) ซึ่งเป็นเจ้าของแอปพลิเคชันและเป็นผู้ขอสิทธิการใช้ข้อมูลจาก Provider

อินเตอร์เฟส คือ จุดต่อเชื่อมระหว่างองค์ประกอบในระบบและจะต้องมีมาตรฐานโปรโตคอล (Protocol) ที่กำหนดไว้อย่างชัดเจน อินเตอร์เฟสในสถาปัตยกรรมอ้างอิงมีดังนี้

(1) Manage Authorization: ทำหน้าที่เป็นจุดเชื่อมต่อที่ให้ Provider ใช้ในการกำหนดสิทธิการใช้บริการข้อมูลของตนกับ Consumer อื่น ๆ อินเตอร์เฟสนี้อาจอยู่ในรูปแบบเว็บแอปพลิเคชันที่ผู้ให้บริการแพลตฟอร์มจัดเตรียมไว้ให้

(2) Resource: ทำหน้าที่เป็นจุดเชื่อมต่อเพื่อให้ Central Data Exchang ตรวจสอบสถานะการใช้งานของ Provider's Resource

(3) Authorization: ทำหน้าที่เป็นจุดเชื่อมต่อเพื่อให้ Central Data Exchange ตรวจสอบสิทธิในการใช้บริการข้อมูลของ Provider's Resource เมื่อมีการร้องขอจาก Consumer's Application รวมถึงการจัดการโทเคน (Token) และเซสชัน (Session) ในการติดต่อ

(4) Consent: ทำหน้าที่เป็นจุดเชื่อมต่อที่ให้ Provider ให้ความยินยอมในการให้บริการข้อมูลของตนกับ Consumer ในตอนต้น

(5) Discover: ทำหน้าที่เป็นจุดเชื่อมต่อที่ให้ Consumer เข้ามาค้นหาบริการข้อมูลในการพัฒนา Consumer's Application

(6) Manage Catalog: ทำหน้าที่เป็นจุดเชื่อมต่อที่ให้ Provider เข้ามาจัดการเมทาดาต้า (Service API) ของตน

(7) Identity: ทำหน้าที่เป็นจุดเชื่อมต่อที่ให้ Consumer และ Provider มาลงทะเบียนเพื่อกำหนดคีย์ (ไอดี) ให้กับ Consumer's Application และ Provider's Resource

(8) Logging: ทำหน้าที่เป็นจุดเชื่อมต่อ (ภายในระบบ) ที่ให้ Central Data Exchange ทำการบันทึกล็อคไฟล์

(9) TSP: ทำหน้าที่เป็นจุดเชื่อมต่อ (ภายในระบบ) ที่ให้ Central Data Exchange ดึงเวลามาใช้ในการบันทึกล็อคไฟล์ด้วย Time Stamp Protocol

(10) OCSP: ทำหน้าที่เป็นจุดเชื่อมต่อ (ภายในระบบ) ที่ให้ Central Data Exchange นำใบรับรอง (Certificate) มาใช้ในการบันทึกล็อคไฟล์ด้วย Online Certificate Status Protocol

ในการขอเข้าใช้งานระบบแลกเปลี่ยนข้อมูล Provider และ/หรือ Consumer ลงทะเบียนกับ Certificate Authority (Identity) เพื่อขอชุดไอดี (ID) หรือสิ่งที่ใช้ยืนยันตัวตน ในด้านของ Provider นั้นจะเริ่มจากการจัดเตรียม Provider's Resource (ข้อมูล) และเชื่อมต่อกับ Central Data Exchange แล้วProvider ต้องทำการกำหนดกำหนดเมทาดาตาใน Service Catalog (Manage Metadata) และนโยบายในการให้บริการข้อมูล (Manage Authorization) ในระหว่างที่ระบบดำเนินงานจริง Central Data Exchange จะทำการตรวจสอบ Provider's Resource ว่ามีสถานะพร้อมใช้หรือไม่ (Resource) ในด้านของ Consumerนั้นจะเริ่มจากการที่นักพัฒนาระบบสารเทศมาค้นหาข้อมูลที่ต้องการใน Service Catalog (Discover) โดย Consumer จะต้องมีการขอความยินยอม (Consent) จาก Provider (Consent) และทำการพัฒนา Consumer's Application

ในขั้นตอนการดำเนินงาน Consumer's Application จะทำการร้องขอใช้บริการ Provider's Resource ผ่าน Central Data Exchange (Authorize) Central Data Exchange จะทำการตรวจสอบสิทธิการใช้งาน เมื่อสิทธิการใช้งานถูกต้องการแลกเปลี่ยนข้อมูลจึงเกิดขึ้น อย่างไรก็ตามลักษณะการแลกเปลี่ยนข้อมูลนั้นมีทั้งแบบ Centralized Model และ Decentralized Model ซึ่งมีความแตกต่างกัน ซึ่งในแต่ละแบบมีข้อดีข้อเสียแตกต่างกันไป เช่น ในรูปแบบ Centralized Model ข้อมูลจะแลกเปลี่ยนผ่าน Central Data Exchange ทำให้เหมาะสมกับการทำ Adapter สำหรับแปลงข้อมูลที่แตกต่างกันระหว่างหน่วยงานให้อยู่ในรูปแบบมาตรฐาน แต่อาจทำให้เกิดปัญหาความล่าช้าในการแลกเปลี่ยนได้ (Single Point Problem) ส่วนรูปแบบ Decentralized Model การส่งผ่านข้อมูลจะไม่เกิดปัญหา Single Point การส่งผ่านข้อมูลเกิดระหว่างหน่วยงานโดยตรงและรวดเร็ว แต่ยากต่อการทำ Adapter เพื่อแก้ปัญหาความแตกต่างของข้อมูล

อย่างไรก็ตามเนื้อหาที่กล่าวมาในส่วนนี้เป็นเพียงสถาปัตยกรรมอ้างอิงเบื้องต้นที่ได้จากการสำรวจคุณลักษณะแพลตฟอร์มแลกเปลี่ยนข้อมูลของภาครัฐที่ดำเนินการอยู่อาจมีการปรับเปลี่ยนไปตามความเหมาะสมระหว่างดำเนินการพัฒนามาตรฐานฯ

5.2 โครงสร้างของชุดมาตรฐานฯ ด้านการเชื่อมโยงข้อมูล

ประเด็นที่ต้องพิจารณาในการพัฒนามาตรฐานฯ ด้านการเชื่อมโยงข้อมูลประกอบด้วยสองประเด็นหลัก คือ (1) ประเด็นด้านสถาปัตยกรรมและโปรโตคอล (Architecture and Protocol Issue) และ (2) ประเด็นด้านความน่าเชื่อถือและความมั่นคงปลอดภัย (Trust and Security Issue)

(1) ประเด็นด้านสถาปัตยกรรมและโปรโตคอล: เป็นข้อกำหนดที่แสดงถึงองค์ประกอบของระบบอินเตอร์เฟสและฟังก์ชันขององค์ประกอบเหล่านั้น ข้อกำหนดโปรโตคอลที่ใช้ในการทำงานสถาปัตยกรรมจะเป็นตัวกำหนดบทบาทและหน้าที่ของระบบสารสนเทศของหน่วยงานที่เชื่อมต่อกับแพลตฟอร์มแลกเปลี่ยนข้อมูล โดยทั่วไปสถาปัตยกรรมระบบจะมีสองลักษณะ คือ Centralized Modelและ Decentralized Model ที่กล่าวไว้ก่อนหน้านี้ความแตกต่างของสถาปัตยกรรมทำให้เกิดความแตกต่างของโปรโตคอล

โปรโตคอล (หรือ Message Transfer) นั้นเป็นข้อกำหนดรายละเอียดของการแลกเปลี่ยน Information Message ระหว่างหน่วยงานภาครัฐหรือผู้เกี่ยวข้องว่าเกิดขึ้นได้อย่างไร (Consumer's Application และ Consumer's Resource) ระบบสารสนเทศจะต้องมีพฤติกรรมการทำงานอย่างไรในการเชื่อมต่อ มีการจัดการเซสชัน (Session) และโทเคน (Token) อย่างไร ในการแลกเปลี่ยนข้อมูลหรือกล่าวได้ว่ามีผลกระทบโดยตรงต่อหน่วยงานของรัฐในการออกแบบระบบสารสนเทศในการแลกเปลี่ยนข้อมูล

(2) ประเด็นด้านชุดมาตรฐานด้านความน่าเชื่อถือและความมั่นคงปลอดภัย: เป็นประเด็นที่สำคัญเพื่อให้มั่นใจได้ว่าการแลกเปลี่ยนข้อมูลที่เกิดขึ้นมีความน่าเชื่อถือมีความมั่นคงปลอดภัยและถูกต้องตามระเบียบ ข้อกำหนดของภาครัฐ ซึ่งจะแบ่งเป็นประเด็นย่อย ดังนี้

(2.1) Identification เพื่อที่จะบ่งชี้เอนทิตี้ (บุคคลหรือระบบ) ที่มีการส่งหรือรับข้อมูล (Message)

(2.2) Authentication เพื่อที่จะยืนยันเอนทิตี้ (บุคคลหรือระบบ) นั้น ๆ ว่าเป็นตัวจริงตามที่อ้าง

(2.3) Certification เพื่อที่จะรับรอง message ที่มีการส่งหรือการรับ (Message Authentication)

(2.4) Encryption เพื่อให้มั่นใจว่าไม่มีใครสามารถอ่านหรือแก้ไข message ระหว่างการรับส่ง

(2.5) Non-repudiation เพื่อให้มั่นใจว่าเอนทิตี้ไม่สามารถปฏิเสธตัวตนในเอกสารที่ได้ลงนามหรือใน message ที่มาต้นทางจากเอนทิตี้นั้น

(2.6) Logging เพื่อใช้เก็บหลักฐานทางกฎหมายของ Message ที่แลกเปลี่ยนกันอาจเป็นตัว Messageเอง หรือค่าแฮช (Hash) ของ Message

การพัฒนาชุดมาตรฐานด้านนี้ต้องทำการออกแบบตัวแบบความน่าเชื่อถือ (Trust Model) ก่อน จากนั้นจะนำไปสู่การออกแบบ Security หรือการเลือกชุดการเข้ารหัส (Cypher Suite)ที่จะนำไปใช้ในมาตรฐานต่อไป

จากประเด็นดังกล่าวข้างต้นเป็นผลให้ชุดมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน ประกอบด้วย

(1) สถาปัตยกรรมอ้างอิงระบบการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Reference Architecture)

(2) ข้อกำหนดด้านการยืนยันตัวตน การกำหนดสิทธิ์และบัญชีการใช้งาน (Authentication, Authorization and Accounting Requirement)

(3) ข้อกำหนดของโปรโตคอลระดับแอปพลิเคชัน เอนพอยน์และการจัดการโทเคนและเซสชัน (Application Protocol, End-Point, Token and Session Management Requirement)

(4) ข้อกำหนดด้านความน่าเชื่อถือและความมั่นคงปลอดภัย (Trust and Security Requirement)

(5) ข้อกำหนดของการตรวจสอบระบบและการลงบันทึกล็อค (Monitoring and Logging Requirement)

6. แนวทางการพัฒนามาตรฐานฯ ด้านความหมายข้อมูล

มาตรฐานฯ ด้านความหมายข้อมูล มุ่งเน้นไปที่การสร้างข้อตกลงร่วมกันระหว่างหน่วยงานในการกำหนดคำศัพท์ (Vocabulary) รูปแบบ โครงสร้าง และความหมายของข้อมูลที่ใช้แลกเปลี่ยนกัน ในสภาพความเป็นจริงข้อมูลเดียวกันอาจมีโครงสร้างและความหมายเหมือนกันหรือต่างกันในแต่ละหน่วยงาน ในการที่จะทำให้หน่วยงานภาครัฐมีการแลกเปลี่ยนข้อมูลกันได้อย่างมีประสิทธิภาพนั้นการกำหนดมาตรฐานด้านความหมายข้อมูลเป็นสิ่งจำเป็นเพื่อแก้ปัญหาความแตกต่างเหล่านี้

จากสภาพความแตกต่างในการกำหนดโครงสร้างและความหมายข้อมูลของหน่วยงานภาครัฐในปัจจุบันวิธีการในการกำหนดมาตรฐานฯ ด้านความหมายข้อมูลที่สามารถดำเนินการได้อย่างมีประสิทธิภาพ คือ การกำหนดแบบจำลองข้อมูลขึ้นจากมาตรฐานข้อมูลที่มีการใช้งานในระดับสากลเพื่อให้หน่วยงานเข้าใจความหมายของข้อมูลตรงกัน เกิดการยอมรับและนำไปสู่มาตรฐานการทำงานร่วมกันอย่างเต็มรูปแบบรวมถึงสามารถแลกเปลี่ยนข้อมูลได้ในระดับสากล

แนวทางการสร้างมาตรฐานการแลกเปลี่ยนข้อมูลด้านความหมาย (Semantic Exchange) สำหรับประเทศไทยนั้นไม่ใช่เรื่องใหม่ ก่อนหน้านี้ได้มีการนำเสนอแนวทางดังกล่าวไว้ใน “กรอบแนวทางในการเชื่อมโยงรัฐบาลอิเล็กทรอนิกส์แห่งชาติ (Thailand e-Government Interoperability Framework, TH eGIF) ” [6] ดังนั้นการพัฒนามาตรฐานฯ ด้านความหมายข้อมูลนี้จึงขอรับแนวทางที่นำเสนอไว้มาเป็นแนวคิดเริ่มต้นแนวคิดในการพัฒนามาตรฐานต่อไป

6.1 กรอบแนวทางการเชื่อมโยงรัฐบาลอิเล็กทรอนิกส์แห่งชาติ

ในเอกสาร TH e-GIF เวอร์ชั่น 2.0 ได้ให้แนวทางในการนำเอาสถาปัตยกรรมทางด้านเทคโนโลยีสารสนเทศมาประยุกต์ใช้ในการปฏิบัติงานเพื่อให้เกิดการเชื่อมโยงข้อมูลไว้อย่างชัดเจน โดยมีจำแนกสถาปัตยกรรมฯ ออกเป็น 4 ด้าน ดังนี้

- สถาปัตยกรรมด้านธุรกิจ (Business Architecture)
- สถาปัตยกรรมด้านข้อมูล (Data Architecture)
- สถาปัตยกรรมด้านระบบงาน (Application Architecture)
- สถาปัตยกรรมด้านเทคโนโลยี (Technology Architecture)

จากสถาปัตยกรรมทั้งสี่ด้านนี้จะเห็นได้ว่าสถาปัตยกรรมด้านข้อมูล (Data Architecture) มีความเกี่ยวพันกับการพัฒนามาตรฐานฯ ด้านความหมายข้อมูลโดยตรง สถาปัตยกรรมด้านข้อมูลอธิบายเกี่ยวกับกลุ่มของข้อมูล โครงสร้างข้อมูลและลักษณะข้อมูล การหาข้อตกลงในการปรับลดชื่อรายการข้อมูลที่มีความหมายเหมือนกันให้เหลือเพียงชื่อเดียวและสร้างความสอดคล้องกับเงื่อนไขการจัดเก็บข้อมูลของแต่ละหน่วยงานซึ่งช่วยให้เกิดการใช้ข้อมูลร่วมกันระหว่างหน่วยงาน และสามารถนำเอาข้อมูลที่มีรูปแบบแตกต่างกันไปใช้ในการพัฒนาระบบงานได้

กรอบแนวทาง TH e-GIF ได้ให้คำแนะนำในการสร้างมาตรฐานด้านข้อมูลไว้หลายประเด็น ยกตัวอย่าง เช่น วิธีการกำหนดมาตรฐาน สร้างความสอดคล้อง และลดความซ้ำซ้อนรายการข้อมูล (Data Simplification,Harmonization and Standardization) ตามคำแนะนำของร่างข้อเสนอหมายเลข 34 ของศูนย์อำนวยความสะดวกด้านการค้าและธุรกรรมอิเล็กทรอนิกส์แห่งสหประชาชาติ (UN/CEFACT) [7] ที่ว่าด้วยการกำหนดมาตรฐาน ชื่อรายการข้อมูลด้านการค้าระหว่างประเทศ การรวบรวม และปรับลด ชื่อรายการข้อมูลที่ใช้ทั่วไปในการทำธุรกรรมที่มาจากต่างเอกสาร

อย่างไรก็ตามกรอบแนวทางที่ TH e-GIF ได้วางไว้เป็นระเบียบวิธีหรือเป็นข้อแนะนำของขั้นตอนต่าง ๆ ในการสร้างมาตรฐานด้านข้อมูลสำหรับหน่วยงานหนึ่งๆ ของรัฐ แต่ไม่ได้ทำให้เห็นภาพรวมของข้อมูลของหน่วยงานภาครัฐทั้งหมด (Bird's-eye View) ดังนั้นมาตรฐานฯ ด้านความหมายข้อมูลนี้จึงจำเป็นที่จะต้องหาตัวแบบที่เหมาะสมเพื่อที่มาเสริมกรอบแนวทางที่ TH e-GIF ได้วางเอาไว้

6.2 National Information Exchange Model

National Information Exchange Model หรือ NIEM[2] [9] เป็นมาตรฐานการแลกเปลี่ยนข้อมูลแห่งชาติโดยแรกเริ่มใช้สำหรับการแลกเปลี่ยนข้อมูลที่สำคัญในกระบวนการยุติธรรมของประเทศสหรัฐอเมริกาและต่อมาได้ถูกพัฒนาขึ้นเป็นมาตรฐานแห่งชาติเพื่อให้สามารถแลกเปลี่ยนข้อมูลในหน่วยงานทั้งภาครัฐและเอกชน โดยมาตรฐาน NIEM ได้มีการจัดแบ่งรายการข้อมูล (Data Domain) ของข้อมูลที่ต้องการแลกเปลี่ยนระหว่างหน่วยงานออกเป็นกลุ่มรายการข้อมูลโดยมีองค์ประกอบ ดังนี้

(1) NIEM Core หมายถึง กลุ่มรายการข้อมูลพื้นฐานทั่วไปที่จำเป็นต้องมีและสามารถเข้าใจได้ระหว่างกลุ่มรายการข้อมูลอื่น ๆ เพื่อเป็นหลักใช้ในการอ้างอิงระหว่างรายการข้อมูล สามารถใช้ร่วมกันได้กับทุกกลุ่มรายการข้อมูล (NIEM Domain) เช่น องค์ประกอบข้อมูลที่เกี่ยวกับบุคคล (Person Data) ประกอบด้วย ชื่อ เพศ วันเกิด เป็นต้น

(2) NIEM Domain หมายถึง กลุ่มรายการข้อมูลที่จำแนกตามประเภทของข้อมูลและวัตถุประสงค์ในการใช้งานในแต่ละศาสตร์ เช่น ข้อมูลด้านธุรกิจ ข้อมูลด้านสุขภาพ เป็นกลุ่มรายการข้อมูลที่มีเป้าหมายหรือภารกิจการทำงานที่สอดคล้องกัน

(3) Future Domain หมายถึง กลุ่มรายการข้อมูลที่อาจเกิดขึ้นได้ในอนาคต โดยในปัจจุบัน NIEM มีเนื้อหาแบบจำลองข้อมูลสำหรับ 15 โดเมน แต่ NIEM ได้เปิดโอกาสในการสร้างโดเมนใหม่เพิ่มเติมได้ในอนาคตได้ โดยขึ้นอยู่กับความต้องการทางธุรกิจและเนื้อหาของโมเดล โดยในการใช้งานมาตรฐาน NIEM ของประเทศสหรัฐอเมริกานั้นได้มีการจัดกลุ่มของรายการข้อมูลของประเทศใน NIEM Core และ NIEM Domains

ในมาตรฐาน NIEM กำหนดให้มีการนำเสนอข้อมูล (Data Representation) ได้ทั้ง Extensible Markup Language (XML) และ JavaScript Object Notation (JSON) โดย ณ ปัจจุบัน NIEM มีการเผยแพร่ในรูปแบบของ XSD, Microsoft Excel และ UML (Unified Modeling Language) ซึ่งเวอร์ชั่นที่มีการเผยแพร่และใช้งานอยู่ในปัจจุบัน คือ NIEM 4.23 และกำลังพัฒนาเวอร์ชั่น NIEM 5.0 อยู่ ซึ่งได้มีการเพิ่ม Uniform Resource Identifier เพื่อช่วยในการจับคู่ Namespace (NIEM JSON-LD) ในการส่ง JSON Message

มาตรฐาน NIEM ทำให้เราสามารถตอบคำถามต่อจาก TH e-GIF ได้ กล่าวคือ เราสามารถสร้างภาพรวม (Bird's-eye view) ของข้อมูลสำหรับประเทศได้ โดยที่มาตรฐาน NIEM ได้สร้างกลุ่มข้อมูลไว้ 3 กลุ่มดังนี้

(1) กลุ่มข้อมูลหลัก (Core Data) หมายถึง กลุ่มของรายการข้อมูลพื้นฐานทั่วไปที่จำเป็นต้องมีเพื่อเป็นหลักใช้ในการอ้างอิงระหว่างกลุ่มข้อมูล (Domain) เช่น ข้อมูลบุคคล (Person) หรือข้อมูลนิติบุคคล (Juristic Person) เป็นต้น

(2) กลุ่มข้อมูลส่วนขยาย (Extend Data) หมายถึง กลุ่มของรายการข้อมูล (Domain) ที่เฉพาะเจาะจงตามความต้องการทางธุรกิจ หรือมีวัตถุประสงค์ในการใช้งาน เฉพาะทางในแต่ละธุรกิจ เช่น ข้อมูลที่ดินข้อมูลภาษี ข้อมูลการลงทุน ข้อมูลสหกรณ์ หรือกลุ่มข้อมูลที่อาจเกิดขึ้นได้ในอนาคต เป็นต้น

(3) กลุ่มข้อมูลอ้างอิง (Reference Data) จะเป็นการกำหนดรูปแบบของข้อมูลทั่วไป แยกเป็น 2 ประเภท คือ

(3.1) ข้อมูลอ้างอิงทั่วไป (Common Reference Data) หมายถึง ข้อมูลอ้างอิงพื้นฐานทั่วไป ที่ไม่ขึ้นกับความต้องการเฉพาะทางธุรกิจ เช่น ข้อมูลจังหวัด (Province) หรือข้อมูลสัญชาติ (Nationality) เป็นต้น

(3.2) ข้อมูลอ้างอิงพื้นฐานทั่วไปที่ขึ้นกับความต้องการเฉพาะธุรกิจ (Domain Reference Data) หมายถึง ข้อมูลอ้างอิงพื้นฐานทั่วไปที่ขึ้นกับความต้องการเฉพาะธุรกิจ (Business Data) เช่น ข้อมูลสถานะนิติบุคคล ข้อมูลรหัสวัตถุประสงค์นิติบุคคล เป็นต้น โดยข้อมูลในแต่ละประเภทจะมีองค์ประกอบสามอย่างคือ

(1) Data Element หมายถึง องค์ประกอบของกลุ่มข้อมูล (Domain) เช่น ข้อมูลบุคคล (Person) จำเป็นต้องประกอบไปด้วย ข้อมูลหมายเลขบัตรประจำตัวประชาชน ข้อมูลชื่อต้น ชื่อรอง ชื่อสกุล หรือที่อยู่ ฯลฯ

(2) Data Format หมายถึง รูปแบบของข้อมูลในรายการข้อมูล เช่น ตัวอักษร ตัวอักษรที่มีรูปแบบเป็นตัวเลข Code Set (รหัสอ้างอิง) ที่สามารถอ้างอิงได้กับ Domain อื่น Data Format อื่น ๆ ที่กำหนดในเอกสาร เช่น รูปแบบข้อมูลวันที่ (Date Format) กำหนดให้มีรูปแบบเป็น YYYYMMDD เป็นต้น

(3) Data Type หมายถึง ประเภทของข้อมูล โดยแบ่งเป็น 2 ประเภทคือ

(3.1) Complex Type เป็นประเภทข้อมูลที่มีการนิยามขึ้นมาใหม่ ประกอบจากประเภทข้อมูลพื้นฐาน (Simple Type) เช่น ข้อมูลชื่อของบุคคล (Person Name) ต้องมีการนิยามประเภทข้อมูล PersonNameType ขึ้นมารองรับ ซึ่งประกอบด้วย คำนำหน้าชื่อ ชื่อต้น ชื่อกลาง ชื่อสกุล และตัวย่อลงท้ายนาม เป็นต้น

(3.2) Reference Type เป็นประเภทข้อมูลที่อ้างอิงผ่าน Primary Key ยกตัวอย่าง เช่น ใช้การระบุรหัสประเทศ (Country Code) เพื่ออ้างอิงข้อมูลประเทศ เป็นต้น ซึ่งในการกำหนดรหัสของข้อมูลอ้างอิงนั้น ควรจะยึดหลักตามมาตรฐานสากลเพื่อให้สะดวกต่อการแลกเปลี่ยนข้อมูลระหว่างประเทศ

6.3 โครงสร้างชุดของมาตรฐานฯ ด้านความหมายข้อมูล

มาตรฐานฯ ด้านความหมายข้อมูล (Semantic Standard) มีความแตกต่างจากมาตรฐานฯ ด้านการเชื่อมโยงข้อมูล (Linkage Standard) ในจุดที่มีขอบเขตเนื้อหาที่กว้างและต้องอาศัยความร่วมมือจากหน่วยงานเจ้าของข้อมูลและผู้เกี่ยวข้องในข้อมูลนั้น ทำให้การพัฒนามาตรฐานเป็นเรื่องที่ต้องอาศัยเวลาและความต่อเนื่องในการดำเนินการ ดังนั้นในการพัฒนามาตรฐานฯด้านความหมายข้อมูลนี้จะใช้กรณีศึกษาเป็นตัวขับเคลื่อน

ตามแผนการดำเนินงานในหัวข้อที่ 4 จะเริ่มจากกรณีศึกษาที่สำคัญก่อน เช่น มาตรฐานข้อมูลบุคคลมาตรฐานข้อมูลนิติบุคคล มาตรฐานข้อมูลสถานที่ เป็นต้น ในการทำมาตรฐานในแต่ละเรื่องนั้นจะมีชุดมาตรฐานข้อมูลเกิดขึ้นกลุ่มหนึ่ง ยกตัวอย่างเช่น การทำมาตรฐานข้อมูลบุคคล (Person) จะมีชุดข้อมูลที่เกี่ยวข้องกับข้อมูลบุคคล ได้แก่ ข้อมูลเพศ ข้อมูลสถานะ ข้อมูลศาสนา เป็นต้น ซึ่งชุดข้อมูลเหล่านี้จะตกอยู่ในหมวดข้อมูลต่อไปนี้

หมวด 1. กลุ่มข้อมูลอ้างอิงทั่วไป (Common Reference Data) หมายถึง กลุ่มข้อมูลอ้างอิงพื้นฐานที่ไม่ขึ้นกับความต้องการเฉพาะทางธุรกิจ เช่น ข้อมูลรหัสเขตการปกครอง ข้อมูลรหัสสัญชาติบุคคล หรือข้อมูลรหัสศาสนา เป็นต้น

หมวด 2. กลุ่มข้อมูลหลัก (Core Data : CD) หมายถึง กลุ่มข้อมูลพื้นฐานทั่วไปที่จำเป็นต้องมีเพื่อใช้เป็นหลักในการอ้างอิงกับกลุ่มข้อมูลในโดเมนอื่น ๆ เช่น ข้อมูลบุคคล ข้อมูลนิติบุคคล ข้อมูลที่ดิน เป็นต้น

หมวด 3. กลุ่มข้อมูลขยาย (Extend Data : ED) หมายถึง กลุ่มข้อมูลที่เฉพาะเจาะจงตามความต้องการทางธุรกิจหรือมีวัตถุประสงค์ในการใช้งานเฉพาะทางในแต่ละธุรกิจ เช่น ข้อมูลทะเบียนบ้าน ข้อมูลใบกำกับภาษีข้อมูลใบรับรองผลการศึกษา เป็นต้น

หมวด 4. ข้อมูลอ้างอิงเฉพาะธุรกิจ (Domain Reference Data: DR) หมายถึง กลุ่มข้อมูลอ้างอิงที่ขึ้นกับความต้องการเฉพาะธุรกิจ (Domain) เช่น ข้อมูลประเภทนิติบุคคล ข้อมูลสถานะนิติบุคคล เป็นต้น

ในข้อมูลทุกตัวจะมีส่วนประกอบสำคัญอยู่ 3 อย่างคือ องค์ประกอบข้อมูล ประเภทข้อมูล และรูปแบบข้อมูล รายละเอียดดังนี้

• องค์ประกอบข้อมูล (Data Element) หมายถึง ข้อมูลย่อยที่นำมาประกอบกันเป็นข้อมูลนั้น เช่น ข้อมูลบุคคล จะมีองค์ประกอบย่อยคือ ชื่อ เพศ สัญชาติ ศาสนา วันเดือนปีเกิด

• ประเภทข้อมูล (Data Type) หมายถึง วิธีการอ้างอิงประเภทของข้อมูล ซึ่งแบ่งเป็น 2 ประเภท ดังนี้

• การอ้างอิงจาก Complex Type หมายถึง การกำหนดชุดองค์ประกอบของข้อมูล (Data Element) ขึ้นมาใหม่เพิ่มเติมจากประเภทข้อมูลพื้นฐาน (Simple Type)

• การอ้างอิงจาก Reference Data หมายถึง การอ้างอิงข้อมูลจากหมวด 1 หรือ หมวด 4 ผ่าน Primary Key

• รูปแบบข้อมูล (Data Format) หมายถึง การอธิบายรูปแบบของข้อมูลตัวหนังสือหรือข้อมูลใดที่ต้องมีการแปลความหมายเพื่อนำไปใช้งาน เช่น รูปแบบข้อมูลวันที่ จะกำหนดรูปแบบเป็นตัวอักษรที่มีรูปแบบเป็นตัวเลข และกำหนดรูปแบบเป็น YYYYMMDD เป็นต้น เพื่อให้การระบุข้อมูลของทุกหน่วยงานเป็นไปในทิศทางและรูปแบบเดียวกัน สามารถนำไปใช้งานได้ทันทีโดยไม่จำเป็นต้องทำการปรับเปลี่ยนรูปแบบ

บรรณานุกรม

[1] Interoperability in the e-Government Context. (2012). Software Engineering Institute,Carnegie Mellon University. Retrieved from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9869.

[2] Once-only principle. Retrieved from https://en.wikipedia.org/wiki/Once-only_principle.

[3] Exchange Patterns. (2021). Project Interoperability. Retrieved from http://projectinteroperability.github.io/exchange-patterns/.

[4] India Urban Data Exchange. (2021). Retrieved from https://iudx.org.in/.

[5] X-Road Global. (2021). Retrieved from https://x-road.global/.

[6] กรอบแนวทางในการเชื่อมโยงรัฐบาลอิเล็กทรอนิกส์แห่งชาติ (Thailand e-Government Interoperability Framework, Th e-GIF). Retrieved from http://www.goforit.co.th/upload/1469603297.pdf.

[7] Data Simplification and Standardization for International Trade Recommendation No. 34, first edition, adopted by the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT). (2010). Retrieved from https://unece.org/fileadmin/DAM/cefact/recommendations/rec34/ECE_TRADE_400_DataSimplificationand_Rec34E.pdf.

[8] ISO/IEC 11179-5:2015(en) Information technology — Metadata registries (MDR) — Part5: Naming principles Retrieved from https://www.iso.org/obp/ui/fr/#iso:std:iso-iec:11179:-5:ed-3:v1:en.

[9] NIEM. (2019). The National Information Exchange Model. Retrieved from https://www.niem.gov/.

[10] ประกาศข้อเสนอแนะมาตรฐานฯ ว่าด้วยข้อความอิเล็กทรอนิกส์สำหรับใบประมวลผล การศึกษา เลขที่ขมธอ. 25-2563. (2021). Retrieved from https://standard.etda.or.th/?p=11889.

[11] Data Exchange Framework: A Reference Architecture for the India Urban Data eXchange (IUDX). (2019). Retrieved from https://aml.ece.iisc.ac.in/images/4/43/Tech_Report_Data_Exhange_Reference_Architecture_v0.9.pdf.

[12] X-Road Architecture Technical Specification. (2021). Retrieved from https://github.com/nordic-institute/X-Road/blob/develop/doc/Architecture/arc-g_xroad_arhitecture.md.

มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน
เรื่อง ข้อกำหนดด้านความน่าเชื่อถือและความมั่นคงปลอดภัย

1. ขอบข่าย

การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานเป็นพื้นฐานหลักที่จำเป็นต่อการพัฒนารัฐบาลดิจิทัลในปัจจุบันประเทศไทยมีแพลตฟอร์มการแลกเปลี่ยนข้อมูลที่ให้บริการอยู่หลายแห่ง แพลตฟอร์มแต่ละแห่งมีแนวทางและพันธกิจในการดำเนินงานเป็นของตนเอง เป็นผลให้การบูรณาการข้อมูลจำเป็นต้องขับเคลื่อนด้วยการสร้างมาตรฐานหรือข้อตกลงร่วมกันในการแลกเปลี่ยนข้อมูล กรมอนามัยจึงมีความจำเป็นต้องจัดทำมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูล เพื่อใช้ในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน เพื่อให้เกิดการบูรณาการข้อมูลเกิดขึ้นอย่างเป็นรูปธรรม

เป้าประสงค์หลักของการใช้มาตรฐานฯ เป็นตัวขับเคลื่อนการบูรณาการข้อมูลหน่วยงาน คือ การให้หน่วยงานมีแนวทางในการพัฒนาสถาปัตยกรรมระบบสารสนเทศเพื่อใช้ในการแลกเปลี่ยนข้อมูลที่ชัดเจนมีความสอดคล้องในการเชื่อมต่อระหว่างกัน

ดังนั้นเพื่อให้บรรลุเป้าประสงค์หลักดังกล่าวจึงมีข้อกำหนดด้านความน่าเชื่อถือและความมั่นคงปลอดภัย สำหรับทำมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน เรื่องมาตรฐานสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐระดับการเชื่อมโยงข้อมูลที่เหมาะสมกับบริบทของกรมอนามัยเท่านั้น

2. นิยาม

นิยามคำศัพท์ที่เกี่ยวข้องกับมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน เรื่อง ข้อกำหนดด้านความน่าเชื่อถือและความมั่นคงปลอดภัยที่ใช้ มีดังนี้

2.1. โปรโตคอล HTTP หมายความว่า โปรโตคอลในระดับชั้นโปรแกรมประยุกต์ (Application Layer) ย่อมาจาก Hypertext Transfer Protocol ใช้สื่อสารผ่านระบบเครือข่ายคอมพิวเตอร์ในการรับและส่งข้อมูล ในการแลกเปลี่ยนข้อมูลระหว่างเครื่องลูกข่ายและเครื่องแม่ข่าย

2.2. โปรโตคอล HTTPS หมายความว่า เป็นส่วนขยายของโปรโตคอล HTTP ย่อมาจาก Hypertext Transfer Protocol Secure ใช้สื่อสารผ่านระบบเครือข่ายคอมพิวเตอร์ในการรับและส่งข้อมูลแบบปลอดภัย ที่ช่วยรักษาความสมบูรณ์ของข้อมูลในการแลกเปลี่ยนข้อมูลระหว่างเครื่องลูกข่ายและเครื่องแม่ข่าย รวมทั้งเก็บข้อมูลนั้นไว้เป็นความลับ

2.3. Transport Layer Security (TLS) หมายความว่า โปรโตคอลที่ใช้เข้ารหัสข้อมูลที่ส่งในเครือข่ายคอมพิวเตอร์ ซึ่งทำงานควบคู่กับโปโตคอล TCP

2.4. Public Key Infrastructure (PKI) หมายความว่า เทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ เป็นเทคโนโลยีที่ใช้ในการรักษาความมั่นคงปลอดภัยของข้อมูล ประกอบด้วยกุญแจที่ใช้ในการเข้ารหัส 2 ประเภท คือ กุญแจส่วนตัว (Private Key) และ กุญแจสาธารณะ (Public Key)

2.5. Certification Authority (CA) หมายความว่า บริการของผู้ให้บริการ Platform ทำหน้าที่ออกใบรับรองอิเล็กทรอนิกส์ (Digital Certificate)

2.6. ใบอนุญาต (Certificates) หมายความว่า เอกสารอิเล็กทรอนิกส์ที่ใช้บ่งบอกถึงความมีตัวตนที่แท้จริงของเจ้าของกุญแจสาธารณะ ซึ่งออกโดยผู้ให้บริการออกใบรับรอง (Certification Authority : CA)

2.7. การเข้ารหัสแฮชฟังก์ชัน (Hash Functions) หมายความว่า อัลกอริทึมสำหรับเข้ารหัสข้อมูลแบบทางเดียวเพื่อใช้ในกระบวนการสร้างและตรวจสอบลายมือชื่อดิจิทัล ซึ่งข้อมูลที่เข้ารหัสจะมีลักษณะเป็นข้อความที่มีความยาวคงที่และมีเอกลักษณ์สามารถใช้เป็นตัวแทนของข้อความตั้งต้นได้

2.8. การเข้ารหัสแบบสมมาตร (Symmetric Encryption) หมายความว่า อัลกอริทึมสำหรับเข้ารหัสข้อมูลที่มีความสำคัญและต้องการปกปิดเป็นความลับ โดยมีลักษณะการเข้ารหัสแบบใช้กุญแจที่เหมือนกันทั้งในขั้นตอนเข้ารหัสและขั้นตอนถอดรหัส

2.9. การเข้ารหัสแบบอสมมาตร (Asymmetric Encryption) หมายความว่า อัลกอริทึมสำหรับเข้ารหัสข้อมูลที่ใช้ในกระบวนการลงลายมือชื่อดิจิทัล ซึ่งมีลักษณะการเข้ารหัสแบบใช้กุญแจที่แตกต่างกันในขั้นตอน

3. กฎหมายและแนวปฏิบัติที่เกี่ยวข้อง

การเชื่อมโยงและการแลกเปลี่ยนข้อมูลภาครัฐมีการบัญญัติไว้ในกฎหมายหรือแนวปฏิบัติที่เกี่ยวข้อง ดังนี้

3.1 รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 ในมาตรา 59 ระบุว่ารัฐต้องเปิดเผยข้อมูลหรือข่าวสารสาธารณะในครอบครองของหน่วยงานของรัฐที่มิใช่ข้อมูลเกี่ยวกับความมั่นคงของรัฐหรือเป็นความลับของทางราชการตามที่กฎหมายบัญญัติ และต้องจัดให้ประชาชนเข้าถึงข้อมูลหรือข่าวสารดังกล่าวได้โดยสะดวก

3.2 พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 ในมาตรา 13 ระบุว่าเพื่อประโยชน์ในการบริหารราชการแผ่นดินและการให้บริการประชาชนให้หน่วยงานของรัฐจัดให้มีการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลที่มีการจัดทำและครอบครองตามที่หน่วยงานของรัฐแห่งอื่นร้องขอที่จะเกิดการบูรณาการร่วมกันมาตรา 15 ระบุว่าให้มีศูนย์แลกเปลี่ยนข้อมูลกลางทำหน้าที่เป็นศูนย์กลางในการแลกเปลี่ยนข้อมูลดิจิทัลและทะเบียนดิจิทัลระหว่างหน่วยงานของรัฐ เพื่อสนับสนุนการดำเนินการของหน่วยงานของรัฐในการให้บริการประชาชนผ่านระบบดิจิทัล และดำเนินการในเรื่องดังต่อไปนี้

(1) กำหนดนโยบายและมาตรฐานเกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลเสนอต่อคณะกรรมการพัฒนารัฐบาลดิจิทัลให้ความเห็นชอบ

(2) ประสานและให้ความช่วยเหลือแก่หน่วยงานของรัฐในการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลระหว่างกัน รวมทั้งกำกับติดตามให้การดำเนินการดังกล่าวเป็นไปในแนวทางและมาตรฐานเดียวกันตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่คณะกรรมการพัฒนารัฐบาลดิจิทัลกำหนด

(3) จัดทำคำอธิบายชุดข้อมูลดิจิทัลของภาครัฐ และจัดเก็บบันทึกหลักฐานของการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล

(4) เรื่องอื่น ๆ ตามที่หน่วยงานมอบหมาย

4. ข้อกำหนดด้านความน่าเชื่อถือและความมั่นคงปลอดภัย

มาตรฐานการเชื่อมโยงและการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานระดับการเชื่อมโยงข้อมูลมีความมุ่งเน้นและให้ความสำคัญในเรื่องของความปลอดภัยและการเข้ารหัสของการแลกเปลี่ยนข้อมูลระหว่างผู้ใช้บริการ API (Consumer System) และผู้ให้บริการ API (Provider System) การกำหนดมาตรฐานในด้านความปลอดภัยและการเข้ารหัสข้อมูลที่มีการรับส่งระหว่างกันจึงเป็นสิ่งจำเป็นที่จะช่วยการลดความเสี่ยงในด้านความปลอดภัยลงได้

ในส่วนนี้จะอธิบายหลักการขั้นพื้นฐานของมาตรฐานความปลอดภัยของมาตรฐานการเชื่อมโยงและการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานระดับการเชื่อมโยงข้อมูลที่กำหนดขึ้นเพื่อให้เป็นมาตรฐานความน่าเชื่อถือและความมั่นคงปลอดภัยการเชื่อมโยงและแลกเปลี่ยนข้อมูล โดยอ้างอิงจากหลักการในเรื่องความปลอดภัยสารสนเทศ (Information Security: InfoSec) ซึ่งประกอบไปด้วยส่วนสำคัญ 3 เรื่องคือ Confidentiality, Integrity และ Availability หรือที่รู้จักกันคือ CIA Triad

4.1. จุดประสงค์ของข้อกำหนดพื้นฐานด้านความน่าเชื่อถือและความมั่นคงปลอดภัย

4.1.1. การรักษาความลับของข้อมูล (Confidentiality)

การรักษาความลับของข้อมูล คือการเก็บรักษาข้อมูลให้เป็นความลับและอนุญาตให้เฉพาะผู้ที่ได้รับอนุญาตเข้าถึงข้อมูลได้โดยการจำกัดสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานในระบบ (ผู้ที่มีส่วนเกี่ยวข้องในการเชื่อมโยงและการแลกเปลี่ยนข้อมูล) ด้วยการยืนยันตัวตน (Authentication) และการตรวจสอบสิทธิ์ (Authorization) ในการเข้าถึงทรัพยากรเพื่อให้มั่นใจได้ว่าจะไม่มีการเข้าถึงข้อมูลจากผู้ที่ไม่ได้รับอนุญาตมาตรฐานการเชื่อมโยงและการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานระดับการเชื่อมโยงข้อมูล ใช้การส่งผ่านข้อมูลในระบบที่อาจผ่านเครือข่ายสาธารณะ เช่น Internet จึงมีการกำหนดให้ใช้วิธีการส่งข้อมูลด้วยกระบวนการที่มีความปลอดภัยสูง เช่น Digital Signature และการเข้ารหัสข้อมูล (Data Encryption) ซึ่งข้อมูลจะต้องถูกส่งผ่านโปรโตคอล HTTPS บน Transport Layer Security (TLS) ที่จะช่วยป้องกันการดักฟังและป้องกันการโจรกรรมข้อมูล โดยจะทำให้มั่นใจได้ว่าการแลกเปลี่ยนข้อมูลผ่านมาตรฐานจะรักษาความลับ และความเป็นส่วนตัวของข้อมูลได้ซึ่งได้มีข้อกำหนดที่เกี่ยวข้องดังต่อไปนี้

(1) ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security)

(2) ข้อกำหนดการเข้ารหัส (Encryption)

(3) ข้อกำหนดด้าน Authentication Access Control และ Accounting ซึ่งกล่าวในมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานด้านการเชื่อมโยงข้อมูล เรื่อง ข้อกำหนดด้านการยืนยันตัวตน การกำหนดสิทธิ์ และบัญชีการใช้งาน

(4) ข้อกำหนดด้านการบริหารจัดการ Token และ Session ซึ่งกล่าวในมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานด้านการเชื่อมโยงข้อมูล เรื่อง ข้อกำหนดของโปรโตคอลระดับแอบพลิเคชันเอนพอยน์และการจัดการโทเคนและเซสชัน

4.1.2. ความถูกต้องของข้อมูล (Integrity)

ความถูกต้องของข้อมูล คือ การตรวจสอบและทำให้มั่นใจว่าข้อมูลที่มีการแลกเปลี่ยนกันภายในมาตรฐานมีความถูกต้องและสมบูรณ์ครบถ้วน ไม่ถูกแก้ไขหรือทำให้ได้รับความเสียหายแก่ข้อมูลที่แลกเปลี่ยนกัน ซึ่งได้มีข้อกำหนดที่เกี่ยวข้องดังต่อไปนี้

(1) ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security)

(2) ข้อกำหนดการจำกัดอัตราการเข้าถึงบริการและใช้ทรัพยากร (Resource and Rate Limit)

(3) ข้อกำหนดการบันทึกกิจกรรมและข้อมูลจราจรคอมพิวเตอร์และการสอดส่อง (Logging & Monitoring)

(4) ข้อกำหนดการจัดการความผิดพลาด (Error handling)

(5) ข้อกำหนดการตรวจสอบข้อมูลนำเข้า (Input Validation)

4.1.3. ความพร้อมให้บริการ (Availability)

ความพร้อมให้บริการ คือ ความพร้อมใช้งานหรือให้บริการของระบบได้อย่างต่อเนื่องเพื่อทำให้มั่นใจว่าองค์ประกอบต่างๆ มีความพร้อมให้บริการกับองค์ประกอบอื่นที่มีความเกี่ยวข้องกันและเพื่อบรรเทาผลกระทบจากการไม่สามารถให้บริการได้จนนำไปสู่ผลกระทบกับผู้ใช้บริการ ซึ่งได้มีข้อกำหนดที่เกี่ยวข้องดังต่อไปนี้

(1) ข้อกำหนดเกี่ยวกับการป้องกันการโจมตี

(2) ข้อกำหนดการจำกัดอัตราการเข้าถึงบริการและใช้ทรัพยากร (Resource and Rate Limit)

(3) ข้อกำหนดการตรวจสอบข้อมูลนำเข้า (Input Validation)

จากหลักการขั้นพื้นฐานทั้ง 3 ข้างต้น คือ การรักษาความลับ (Confidentiality) ความถูกต้องของข้อมูล (Integrity) และความพร้อมให้บริการ (Availability) โดยมาตรฐานการเชื่อมโยงและการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานระดับการเชื่อมโยงข้อมูลจัดให้มีข้อกำหนดเพื่อเป็นกรอบแนวทางการปฏิบัติตามแนวทางการปฏิบัติที่ดี โดยจะครอบคลุมผู้ให้บริการ ผู้ใช้บริการและองค์ประกอบอื่น ๆ สามารถแบ่งข้อกำหนดเป็น 4 ส่วนดังนี้

(1) ข้อกำหนดด้านความปลอดภัยของผู้ให้บริการ ประกอบด้วย

- ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security)
- ข้อกำหนดการเข้ารหัส (Encryption)
- ข้อกำหนดการจ ากัดอัตราการเข้าถึงบริการและใช้ทรัพยากร
- ข้อกำหนดการบันทึกกิจกรรมและข้อมูลจราจรคอมพิวเตอร์และการตรวจสอบ (Logging & Monitoring)
- ข้อกำหนดการจัดการความผิดพลาด (Error handling)
- ข้อกำหนดการตรวจสอบข้อมูลนำเข้า (Input Validation)
- ข้อกำหนดเกี่ยวกับการป้องกันการโจมตี

(2) ข้อกำหนดด้านความปลอดภัยของผู้ใช้บริการ ประกอบด้วย

- ข้อกำหนดด้านความมั่นคงปลอดภัยของการส่งข้อมูล (Transport Security)
- ข้อกำหนดการเข้ารหัส (Encryption)
- ข้อกำหนดการบันทึกกิจกรรมและข้อมูลจราจรคอมพิวเตอร์และการตรวจสอบ (Logging & Monitoring)

(3) ข้อกำหนดด้านความปลอดภัยขององค์ประกอบอื่น ๆ ตามมาตรฐานประกอบด้วย

- ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security)
- ข้อกำหนดการเข้ารหัส (Encryption)
- ข้อกำหนดการบันทึกกิจกรรมและข้อมูลจราจรคอมพิวเตอร์และการตรวจสอบ (Logging & Monitoring)

- ข้อกำหนดการจัดการความผิดพลาด (Error handling)

(4) ข้อกำหนดด้านความปลอดภัยที่เกี่ยวข้องกับกฎหมาย ประกอบด้วย

- ข้อกำหนดที่เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- ข้อกำหนดที่เกี่ยวกับพระราชบัญญัติว่าด้วยการกระท าความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560
- ข้อกำหนดที่เกี่ยวกับหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564

4.2. ข้อกำหนดด้านความปลอดภัยของผู้ให้บริการ (Provider)

4.2.1. ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security)

ความปลอดภัยของการส่งข้อมูล (Transport Security) ของมาตรฐานของผู้ให้บริการจะมุ่งเน้นไปการส่งข้อความในระดับ Session ของผู้ให้บริการ ในองค์ประกอบของการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานของผู้ให้บริการ

เพื่อให้การรับส่งข้อมูลสำหรับบริการการแลกเปลี่ยนข้อมูลมีความปลอดภัยและเป็นไปตามข้อกำหนดพื้นฐานด้านความปลอดภัย การสื่อสารเพื่อรับส่งข้อมูลของมาตรฐานของผู้ให้บริการจะต้องเป็นไปตามข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security) ของผู้ให้บริการโดยมีรายละเอียดดังนี้

1. การส่งข้อมูลจะต้องดำเนินการบน HTTPS โดยใช้ TLS 1.2 เป็นอย่างน้อย

2. ใบรับรอง (Certificates) จะต้องมีการเข้ารหัสแฮชฟังก์ชัน (Hash Functions) แบบ SHA-2 (Secure Hash Algorithm 2) ด้วยความยาวกุญแจ (Key size) อย่างน้อย 2048 bits

3. ทุกปลายทาง (Endpoint) จะต้องใช้ใบรับรองดิจิทัล (Digital Certificate) ที่ออกโดยหน่วยงานที่ดูแลใบรับรองดิจิทัลที่ได้รับอนุญาต

4. ห้ามทำการเปลี่ยนเส้นทาง HTTP ไปยัง HTTPS โดยให้ปฏิเสธการเปลี่ยนเส้นทางทุกกรณี

5. ให้ปิดการใช้งานเมธอด HTTP (HTTP Method) ที่ไม่ได้ใช้งานและส่งคืนค่า HTTP 405 ตามมาตรฐาน Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content: section- 6.5.5

6. ต้องมีการตรวจสอบ (Validate) ตามข้อกำหนดการตรวจสอบข้อมูลนำเข้า (Input Validation) ทุก ๆ การเรียกใช้งาน (Request)

4.2.2. ข้อกำหนดการเข้ารหัส (Encryption)

การเข้ารหัสข้อมูลของผู้ให้บริการในกรณีที่ต้องมีการเข้ารหัสข้อมูล เช่น ข้อมูลที่มีความสำคัญที่เป็นข้อมูลเชิงธุรกรรมที่ Payload ข้อมูลลายเซ็นในส่วน Signature หรือข้อมูล Token ที่อยู่ในส่วน Header เป็นต้น การเข้ารหัสข้อมูล (Encryption) ของมาตรฐาน จะมุ่งเน้นไปยังส่วน Presentation ของผู้ให้บริการ ในองค์ประกอบของการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานของผู้ให้บริการ

เพื่อให้เป็นไปตามข้อกำหนดพื้นฐานด้านความปลอดภัย การเข้ารหัสข้อมูล (Encryption) ของมาตรฐานของผู้ให้บริการจะต้องเป็นไปตามข้อกำหนดการเข้ารหัส (Encryption) ของผู้ให้บริการโดยมีรายละเอียดดังนี้

1. ในกรณีที่การส่งข้อมูลที่ผู้ให้บริการพิจารณาแล้วว่ามีข้อมูลที่มีความสำคัญที่เป็นข้อมูลเชิงธุรกรรมใน Payload หรือเป็นความลับที่ต้องการการเข้ารหัสจะต้องใช้การเข้ารหัสแบบสมมาตร (Symmetric Encryption) แบบ AES (Advanced Encryption Standard) [6] โดยมีความยาวของกุญแจอย่างน้อย 128 bits (AES-128) ซึ่งสามารถเข้ารหัสเฉพาะข้อมูลนั้นๆ ไม่จำเป็นต้องเข้ารหัสข้อมูลทั้ง Payload

2. สำหรับการลงลายมือชื่อดิจิทัล เพื่อการรับประกันการยืนยันตัวตนของต้นทางและความถูกต้องของข้อมูลจะต้องใช้อัลกอลิธึมแบบใดแบบหนึ่งดังต่อไปนี้

- อัลกอลิธึม DSA (Digital Signature Algorithm) โดยมีขนาดของ Security of strength มากกว่าหรือเท่ากับ 112 bits และ Domain Parameter อย่างน้อย (L, N) = (2048, 224)

- อัลกอลิธึม ECDSA (Elliptic Curve-based Digital Signature) โดยมีขนาดของ Security of strength อย่างน้อย 112 bits และ Domain Parameter อย่างน้อย 224 bits

- อัลกอลิธึม RSA (Rivest–Shamir–Adleman algorithm) โดยมีขนาดของ Security of strength อย่างน้อย 112 bits และ Domain Parameter อย่างน้อย 2048 bits ในกรณีที่พบปัญหาการถอดรหัส เช่น ผู้ให้บริการไม่สามารถถอดรหัสการตรวจสอบลายเซ็นของ JWT (JSON Web Token) ได้ ผู้ให้บริการสามารถตอบกลับด้วย error message

3. สำหรับการสร้างหรือตรวจสอบลายมือชื่อแบบดิจิทัลโดยใช้แฮชฟังก์ชัน (Hash Function) จะต้องใช้ฟังก์ชันแบบใดแบบหนึ่งดังต่อไปนี้

- SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 และ SHA-512/256)
- SHA-3 (SHA3-224, SHA3-256, SHA3-384 และ SHA3-512)

4. สำหรับการสร้างตัวเลขแบบสุ่ม (Random Bit Generation) เพื่อจุดประสงค์ต่าง ๆ เช่นการสร้างกุญแจ (keys) ตัวเลขแบบใช้ครั้งเดียว (Nonces) และ ค่าสุ่มเพื่อการยืนยันตัวตน (Authentication Challenges) จะต้องใช้อัลกอลิธึมแบบใดแบบหนึ่งดังต่อไปนี้

- Hash_DRBG และ HMAC_DRBG
- CRT_DRBG โดยใช้ AES-128, AES-192 และ AES-256

4.2.3. ข้อกำหนดการจำกัดอัตราการเข้าถึงบริการและใช้ทรัพยากร

การจำกัดอัตราการเข้าถึงบริการและใช้ทรัพยากรของมาตรฐานจะมุ่งเน้นไปยังส่วนของผู้ให้บริการ เพื่อให้เป็นไปตามข้อแนวทางการปฏิบัติที่ดีทางด้านความปลอดภัยของการให้บริการการแลกเปลี่ยนข้อมูล ผู้ให้บริการจะต้องจัดให้มีการควบคุมอัตราการเข้าถึงบริการและการใช้ทรัพยากรของระบบของผู้ให้บริการ โดยทั้งผู้ให้บริการจะต้องสามารถกำหนดการจำกัดได้อย่างน้อยดังนี้

1. สามารถจำกัดเวลาการทำงานของบริการได้ (Execution timeouts) โดยควรกำหนดค่าตั้งต้นของขนาดสูงสุดของเวลาการทำงาน (Execution timeout) ไว้ที่ 60 วินาทีหรือสามารถปรับเปลี่ยนได้ตามความเหมาะสมของการให้บริการ โดยสามารถเลือกดำเนินการได้จาก

- การพัฒนาด้วยภาษาโปรแกรมของ Provider System
- การระบุไว้ที่ Web Server หรือ Application Server ของ Provider System
- การใช้ API Gateway เข้ามาช่วยดำเนินการ
- อื่น ๆ ตามความเหมาะสม

2. สามารถจำกัดขนาดของข้อความในการร้องขอบริการได้ (Request payload size) โดยควรกำหนดค่าตั้งต้นของขนาดสูงสุดของข้อความร้องขอบริการ (Request payload size)ไว้ที่5 MB (Megabytes) หรือสามารถปรับเปลี่ยนได้ตามความเหมาะสมของการให้บริการโดยสามารถเลือกดำเนินการได้จาก

- การพัฒนาด้วยภาษาโปรแกรมของ Provider System
- การระบุไว้ที่ Web Server หรือ Application Server ของ Provider System
- การใช้ API Gateway เข้ามาช่วยดำเนินการ
- อื่น ๆ ตามความเหมาะสม

3. สามารถจำกัดจำนวนการร้องขอบริการต่อผู้ขอใช้บริการหรือบริการได้ (Number of requests per client/resource) โดยผู้ให้บริการทำการประเมินจากทรัพยากรและประสิทธิภาพที่จะให้บริการได้กับความต้องการใช้บริการของผู้ใช้บริการโดยสามารถเลือกดำเนินการได้จากตัวอย่างการ Implementation สามารถใช้เครื่องมือที่เป็นลักษณะ API Gateway ช่วยในการสามารถจำกัดเวลาการทำงานของบริการได้(Execution timeouts)

4. สามารถจำกัดจำนวนแถวข้อมูลต่อหน้าที่จะส่งกลับไปยังผู้ร้องขอบริการและตอบกลับต่อหนึ่งการร้องขอ (Number of records per page to return in a single request response)

4.2.4. ข้อกำหนดการบันทึกกิจกรรมและข้อมูลล็อกและการตรวจสอบ (Logging & Monitoring)

เพื่อให้เป็นไปตามแนวทางการปฏิบัติที่ดีทางด้านความปลอดภัยของการให้บริการการแลกเปลี่ยนข้อมูลผู้ให้บริการจะต้องจัดให้มีการบันทึกข้อมูลล็อกและการตรวจสอบโดยผู้ให้บริการจะต้องมีการปฏิบัติตามข้อกำหนด ซึ่งกล่าวในมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน ด้านการเชื่อมโยงข้อมูล เรื่องข้อกำหนดของการตรวจสอบระบบและการลงบันทึกล็อก

4.2.5. ข้อกำหนดการจัดการความผิดพลาด (Error handling)

เพื่อให้เป็นไปตามข้อแนวทางการปฏิบัติที่ดีทางด้านความปลอดภัยของการให้บริการการแลกเปลี่ยนข้อมูลเมื่อบริการที่เปิดให้บริการแสดงข้อความการท างานผิดพลาด จะต้องไม่เปิดเผยข้อมูลที่มีความเสี่ยงที่สามารถนำมาโจมตีระบบได้ โดยผู้ให้บริการจะต้องจัดให้มีการจัดการข้อผิดพลาดอย่างเหมาะสมอย่างน้อยดังนี้

1. บริการจะต้องปกปิดรหัสหรือข้อความแสดงข้อผิดพลาดอื่นใดนอกเหนือจากสถานะตอบกลับหรือข้อความแสดงข้อผิดพลาดของ HTTP (HTTP status responses และ HTTP error messages) เช่น ไม่ควรแสดงข้อมูลระดับระบบ (System level) ไปในข้อผิดพลาดที่ตอบกลับ

2. บริการจะต้องไม่ส่งรายละเอียดข้อผิดพลาดทางเทคนิคไปยังผู้ขอใช้บริการ เช่น ไม่ควรแสดงข้อความข้อผิดพลาดของลำดับการเรียกของระบบ (Call stacks) หรือข้อความข้อผิดพลาดของคำสั่งเรียกฐานข้อมูล

4.2.6. ข้อกำหนดการตรวจสอบข้อมูลนำเข้า (Input Validation)

เพื่อให้เป็นไปตามข้อแนวทางการปฏิบัติที่ดีทางด้านความปลอดภัยของการให้บริการการแลกเปลี่ยนข้อมูล การตรวจสอบข้อมูลที่จะนำเข้าสู่ระบบจะช่วยให้มั่นใจได้ว่าข้อมูลที่จะเข้าสู่ระบบอยู่ในรูปแบบที่เหมาะสม ซึ่งจะช่วยป้องกันการถูกโจมตีระบบได้ โดยผู้ให้บริการจะต้องจัดให้มีการตรวจสอบข้อมูลนำเข้าอย่างเหมาะสมอย่างน้อยดังนี้

1. การตรวจสอบข้อมูลนำเข้าควรจะกระทำเป็นลำดับแรกสุดเท่าที่จะทำได้นับตั้งแต่ได้รับข้อมูลเข้ามาจากระบบภายนอก

2. กำหนดการจำกัดขนาดของข้อมูลนำเข้าที่เหมาะสมและปฏิเสธข้อมูลนำเข้าที่มีขนาดเกินที่กำหนดไว้

3. ออกแบบและพัฒนาระบบให้ตรวจสอบข้อมูลนำเข้า โดยตรวจสอบ เช่น ขนาดความยาว ช่วงของข้อมูล รูปแบบข้อมูลและประเภทข้อมูล ให้ตรงตามข้อกำหนดทางเทคนิคของบริการนั้นที่กำหนดไว้

4. ออกแบบและพัฒนาระบบให้ตรวจสอบบันทึกกิจกรรมและข้อมูลจราจรคอมพิวเตอร์ที่ไม่ผ่านการตรวจสอบข้อมูลนำเข้า (Logging input validation) เพื่อเป็นการสอดส่องความพยายามตรวจสอบข้อมูลนำเข้าที่ไม่ผ่านและมีมากผิดปกติในช่วงเวลาสั้น ๆ ซึ่งอาจจะเป็นการพยายามโจมตีระบบ

5. จำกัดข้อมูลนำเข้าให้อยู่ในรูปแบบที่เหมาะสมกับประเภทข้อมูลตามข้อกำหนดทางเทคนิคของบริการนั้นด้วยการตรวจสอบด้วยนิพจน์ปกติ (Regular Expression)

4.2.7. ข้อกำหนดเกี่ยวกับการป้องกันการโจมตี

เพื่อให้เป็นไปตามข้อแนวทางการปฏิบัติที่ดีทางด้านความปลอดภัยของการให้บริการการแลกเปลี่ยนข้อมูล การป้องกันการโจมตีจะช่วยให้มั่นใจได้ว่าระบบจะมีความพร้อมให้บริการตามข้อตกลงบริการ (Service Agreement) และป้องกันความเสียหายจากข้อมูลที่รั่วไหล โดยผู้ให้บริการจะต้องจัดให้มีการดำเนินการป้องกันการโจมตีอย่างเหมาะสมอย่างน้อยดังนี้

1. จัดให้มี Endpoint Mapping โดยที่ผู้ให้บริการทำการเปิด Public Endpoint ของ API ให้ผู้ใช้บริการใช้งาน โดยที่ผู้ใช้บริการไม่ทราบ Endpoint ที่แท้จริงของ API ที่ Provider สร้างขึ้น โดยสามารถเลือกดำเนินการได้จากการใช้ API Gateway หรือสิ่งที่ทำหน้าที่ได้เทียบเท่าเข้ามาช่วยดำเนินการ

2. จัดทำ IP Access Control โดยการอนุญาตให้เฉพาะระบบของผู้ใช้บริการ หรือเฉพาะ IP Address หรือ Domain ที่กำหนดเท่านั้นที่เรียกใช้ API ได้ โดยสามารถเลือกดำเนินการได้จากการใช้ API Gateway หรือสิ่งที่ทำหน้าที่ได้เทียบเท่าเข้ามาช่วยดำเนินการ

3. จัดทำ Threat Protection เพื่อการป้องกันไม่ให้มีการโจมตี API จากผู้ใช้งานที่ไม่พึงประสงค์ก่อนที่ Request ไปถึงยังระบบของผู้ให้บริการ โดยสามารถเลือกดำเนินการได้จากการใช้ API Gateway หรือสิ่งที่ทำหน้าที่ได้เทียบเท่าเข้ามาช่วยดำเนินการ

4.3. ข้อกำหนดด้านความปลอดภัยของผู้ใช้บริการ (Consumer)

4.3.1. ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security)

ความปลอดภัยของการส่งข้อมูล (Transport Security) ของมาตรฐานของผู้ใช้บริการจะมุ่งเน้นไปการส่งข้อความในระดับ Session ของผู้ใช้บริการ ในองค์ประกอบของการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานของผู้ใช้บริการ

เพื่อให้การรับส่งข้อมูลสาหรับบริการการแลกเปลี่ยนข้อมูลมีความปลอดภัยและเป็นไปตามข้อกำหนดพื้นฐานด้านความปลอดภัย การสื่อสารเพื่อรับส่งข้อมูลของมาตรฐานของผู้ใช้บริการจะต้องเป็นไปตามข้อกำหนดโดยมีรายละเอียดดังนี้

1. การส่งข้อมูลจะต้องดาเนินการบน HTTPS โดยใช้ TLS 1.2 เป็นอย่างน้อย

2. ใบรับรอง (Certificates) จะต้องมีการเข้ารหัสแฮชฟังก์ชัน (Hash Functions) แบบ SHA-2 (Secure Hash Algorithm 2) ด้วยความยาวกุญแจ (Key size) อย่างน้อย 2048 bits

3. ทุกปลายทาง (Endpoint) จะต้องใช้ใบรับรองดิจิทัล (Digital Certificate) ที่ออกโดยหน่วยงานที่ดูแลใบรับรองดิจิทัลที่ได้รับอนุญาต

4.3.2. ข้อกำหนดการเข้ารหัส (Encryption)

การเข้ารหัสข้อมูลของผู้ใช้บริการในกรณีที่ต้องมีการเข้ารหัสข้อมูล เช่น ข้อมูลที่มีความสำคัญที่เป็นข้อมูลเชิงธุรกรรมที่ Payload ข้อมูลลายเซ็นในส่วน Signature หรือข้อมูล Token ที่อยู่ในส่วน Header เป็นต้น การเข้ารหัสข้อมูล (Encryption) ของมาตรฐานจะมุ่งเน้นไปยังส่วน Presentation ของผู้ใช้บริการ ในองค์ประกอบของการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานของผู้ใช้บริการ

เพื่อให้เป็นไปตามข้อกำหนดพื้นฐานด้านความปลอดภัย การเข้ารหัสข้อมูล (Encryption) ของมาตรฐานของผู้ใช้บริการจะต้องเป็นไปตามข้อกำหนดโดยมีรายละเอียดดังนี้

(1) ในกรณีการส่งข้อมูลที่มีความสำคัญเป็นข้อมูลเชิงธุรกรรมใน Payload หรือเป็นความลับที่ต้องการการเข้ารหัส ให้ดำเนินการตามข้อตกลงการใช้บริการ (Service Agreement) ที่ทำร่วมกับผู้ให้บริการ

(2) สำหรับการลงลายมือชื่อดิจิทัล เพื่อการรับประกันการยืนยันตัวตนของต้นทางและความถูกต้องของข้อมูลจะต้องใช้อัลกอลิธึมตามข้อตกลงการใช้บริการ (Service Agreement)ที่ทำร่วมกับผู้ให้บริการ

(3) สำหรับการสร้างหรือตรวจสอบลายมือชื่อแบบดิจิทัลโดยใช้แฮชฟังก์ชัน (Hash Function) จะต้องใช้ฟังก์ชันตามข้อตกลงการใช้บริการ (Service Agreement)ที่ทำร่วมกับผู้ให้บริการ

4.3.3. ข้อกำหนดการบันทึกกิจกรรมและข้อมูลล็อกและการตรวจสอบ (Logging & Monitoring)

เพื่อให้เป็นไปตามแนวทางการปฏิบัติที่ดีทางด้านความปลอดภัยของการใช้บริการการแลกเปลี่ยนข้อมูลผู้ใช้บริการจะต้องจัดให้มีการบันทึกข้อมูลล็อกและการตรวจสอบโดยผู้ใช้บริการจะต้องมีการปฏิบัติตามข้อกำหนดซึ่งกล่าวในมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน ด้านการเชื่อมโยงข้อมูล เรื่อง ข้อกำหนดของการตรวจสอบระบบและการลงบันทึกล็อก

4.4. ข้อกำหนดด้านความความปลอดภัยขององค์ประกอบอื่น ๆ

4.4.1. ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security)

ความปลอดภัยของการส่งข้อมูล (Transport Security) ของมาตรฐานของ Certification Authority จะทำหน้าที่ออกใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) ในองค์ประกอบของการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานของผู้ใช้บริการ

เพื่อให้การรับส่งข้อมูลสำหรับบริการการแลกเปลี่ยนข้อมูลมีความปลอดภัยและเป็นไปตามข้อกำหนดพื้นฐานด้านความปลอดภัย การสื่อสารเพื่อรับส่งข้อมูลของมาตรฐานของ Certification Authority จะต้องเป็นไปตามข้อกำหนดโดยมีรายละเอียดดังนี้

(1) การส่งข้อมูลจะต้องดำเนินการบน HTTPS โดยใช้ TLS 1.2 เป็นอย่างน้อย

(2) ใบรับรอง (Certificates) จะต้องมีการเข้ารหัสแฮชฟังก์ชัน (Hash Functions) แบบ SHA-2 (Secure Hash Algorithm 2) ด้วยความยาวกุญแจ (Key size) อย่างน้อย 2048 bits

(3) ห้ามทำการเปลี่ยนเส้นทาง HTTP ไปยัง HTTPS โดยให้ปฏิเสธการเปลี่ยนเส้นทางทุกกรณี

หมายเหตุ Certification Authority ทำหน้าที่ออกใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) ใน 2 กรณี

(1) เพื่อใช้เป็น Server Certificate (SSL) หรือ ใบรับรองอิเล็กทรอนิกส์สาหรับเครื่อง Server เพื่อให้สามารถใช้งานการเชื่อมต่อได้อย่างปลอดภัยด้วย HTTPS ซึ่งคือข้อกำหนดในข้อนี้

(2) เพื่อใช้ในการลงลายมือชื่อดิจิตอล (Digital Signature) หรือ การเข้ารหัส ถอดรหัส (Encryption) ลายมือชื่อที่ได้จากกระบวนการเข้ารหัสลับ (Encrypt) ซึ่งช่วยให้สามารถยืนยันตัวเจ้าของลายมือชื่อและตรวจพบการเปลี่ยนแปลงของข้อความและลายมือชื่อได้ จะกล่าวถึงในข้อกำหนดการเข้ารหัส

4.4.2. ข้อกำหนดการเข้ารหัส (Encryption)

การเข้ารหัสข้อมูลของ Certification Authority จะดำเนินการในส่วน การลงลายมือชื่อดิจิทัลหรือข้อมูล Token ที่อยู่ในส่วน Header เป็นต้น เพื่อให้เป็นไปตามข้อกำหนดพื้นฐานด้านความปลอดภัยการเข้ารหัสข้อมูล (Encryption) ของ Certification Authority จะต้องเป็นไปตามข้อกำหนดโดยมีรายละเอียดดังนี้

(1) สำหรับการลงลายมือชื่อดิจิทัล เพื่อการรับประกันการยืนยันตัวตนของต้นทางและความถูกต้องของข้อมูลจะต้องใช้อัลกอลิธึมแบบใดแบบหนึ่งดังต่อไปนี้

- อัลกอลิธึม DSA (Digital Siganture Algorithm) โดยมีขนาดของ Security of strength มากกว่าหรือเท่ากับ 112 bits และ Domain Parameter อย่างน้อย (L, N) = (2048, 224)
- อัลกอลิธึม ECDSA (Elliptic Curve-based Digital Signature) โดยมีขนาดของ Security of strength อย่างน้อย 112 bits และ Domain Parameter อย่างน้อย 224 bits
- อัลกอลิธึม RSA (Rivest-Shamir-Adelman algorithm) โดยมีขนาดของ Security of strength อย่างน้อย 112 bits และ Domain Parameter อย่างน้อย 2048 bits

(2) สำหรับการสร้างหรือตรวจสอบลายมือชื่อดิจิทัลโดยใช้แฮชฟังก์ชัน (Hash Function) จะต้องใช้ฟังก์ชันแบบใดแบบหนึ่งดังต่อไปนี้

- SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 และ SHA-512/256)
- SHA-3 (SHA3-224, SHA3-256, SHA3-384 และ SHA3-512)

(3) สำหรับการสร้างหรือตรวจสอบลายมือชื่อดิจิทัลโดยใช้แฮชฟังก์ชัน (Hash Function) จะต้องใช้ฟังก์ชันตามข้อตกลงการใช้บริการ (Service Agreement) ที่ทำร่วมกับผู้ให้บริการ

(4) สำหรับการสร้างตัวเลขแบบสุ่ม (Random Bit Generation) เพื่อจุดประสงค์ต่าง ๆ เช่นการสร้างกุญแจ (keys) ตัวเลขแบบใช้ครั้งเดียว (Nonces) และ ค่าสุ่มเพื่อการยืนยันตัวตน (Authentication Challenges) จะต้องใช้อัลกอลิธึมแบบใดแบบหนึ่งดังต่อไปนี้

- Hash_DRBG และ HMAC_DRBG
- CRT_DRBG โดยใช้ AES-128, AES-192 และ AES-256

4.4.3. ข้อกำหนดการบันทึกกิจกรรมและข้อมูลล็อกและการตรวจสอบ (Logging & Monitoring)

เพื่อให้เป็นไปตามแนวทางการปฏิบัติที่ดีทางด้านความปลอดภัยของการให้บริการการแลกเปลี่ยนข้อมูล Certification Authority จะต้องจัดให้มีการบันทึกข้อมูลล็อกและการตรวจสอบ โดยของ Certification Authority จะต้องมีการปฏิบัติตามข้อกาหนดซึ่งกล่าวใน มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน เรื่องข้อกำหนดของการตรวจสอบระบบและการลงบันทึกล็อก

4.4.4. ข้อกำหนดการจัดการความผิดพลาด (Error handling)

เพื่อให้เป็นไปตามข้อแนวทางการปฏิบัติที่ดีทางด้านความปลอดภัยของการให้บริการการแลกเปลี่ยนข้อมูล เมื่อบริการที่เปิดให้บริการแสดงข้อความการทางานผิดพลาด จะต้องไม่เปิดเผยข้อมูลที่มีความเสี่ยงที่สามารถนามาโจมตีระบบได้ โดย ของ Certification Authority จะต้องจัดให้มีการจัดการข้อผิดพลาดอย่างเหมาะสมอย่างน้อยดังนี้ [3]

(1) บริการจะต้องปกปิดรหัสหรือข้อความแสดงข้อผิดพลาดอื่นใดนอกเหนือจากสถานะตอบกลับหรือข้อความแสดงข้อผิดพลาดของ HTTP (HTTP status responses และ HTTP error messages) เช่น ไม่ควรแสดงข้อมูลระดับระบบ (System level) ไปในข้อผิดพลาดที่ตอบกลับ

(2) บริการจะต้องไม่ส่งรายละเอียดข้อผิดพลาดทางเทคนิคไปยังผู้ขอใช้บริการ เช่น ไม่ควรแสดงข้อความข้อผิดพลาดของลำดับการเรียกของระบบ (Call stacks) หรือข้อความข้อผิดพลาดของคำสั่งเรียกฐานข้อมูล

บรรณานุกรม

[1] Wikipedia. (2021). Information security. [ออนไลน์]. เข้าถึงได้จาก: https://en.wikipedia.org/wiki/Information_security. (วันที่ค้นข้อมูล: 8 พฤศจิกายน 2021)

[2] Wikipedia. (2021). Key concepts. [ออนไลน์]. เข้าถึงได้จาก: https://en.wikipedia.org/wiki/Information_security#Key_concepts. (วันที่ค้นข้อมูล: 8 พฤศจิกายน 2021)

[3] Australian Government. (2021). API Security. [ออนไลน์]. เข้าถึงได้จาก: https://api.gov.au/standards/national_api_standards/api-security.html. (วันที่ค้นข้อมูล: 9 กันยายน 2021)

[4] R. Fielding. (2014, มิถุนายน) Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content: section-6.5.5. [ออนไลน์]. เข้าถึงได้จาก: https://datatracker.ietf.org/doc/html/rfc7231#section-6.5.5. (วันที่ค้นข้อมูล: 9 กันยายน 2021)

[5] E. Barker และ A. Roginsky. (2019, มีนาคม). NIST Special Publication 800-131A Revision 2 :Transitioning the Use of Cryptographic Algorithms and Key Lengths. [ออนไลน์]. เข้าถึง ได้จาก: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.**800-131**Ar**2.**pdf. (วันที่ค้นข้อมูล: 9 กันยายน 2021)

[6] ADVANCED ENCRYPTION STANDARD (AES). (2010, ธันวาคม). [ออนไลน์]. เข้าถึงได้จาก: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf. (วันที่ค้นข้อมูล: 9 กันยายน 2021)

[7] OWASP API Security Project. (2019). [ออนไลน์]. เข้าถึงได้จาก: https://owasp.org/www-project-api-security/.(วันที่ค้นข้อมูล: 9 กันยายน 2021)

[8] R. Fielding. (2014, มิถุนายน) Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content. [ออนไลน์]. เข้าถึงได้จาก: https://datatracker.ietf.org/doc/html/rfc7231. (วันที่ค้นข้อมูล: 9 กันยายน 2021)

[9] PauloASilva. (2019). API10:2019 Insufficient Logging & Monitoring. [ออนไลน์]. เข้าถึงได้จาก: https://github.com/OWASP/API-Security/blob/master/2019/en/src/0xaa-insufficient-logging-monitoring.md. (วันที่ค้นข้อมูล: 9 กันยายน 2021)

[10] ราชกิจจานุเบกษา. (2019, พฤษภาคม). พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒.[ออนไลน์]. เข้าถึงได้จาก: http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0052.PDF. (วันที่ค้นข้อมูล:9 กันยายน 2021)

[11] สำนักงานคณะกรรมการฤษฎีกา. (2017, มกราคม). พระราชบัญญัติว่าด้วยการกระท าความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. ๒๕๖๐. [ออนไลน์]. เข้าถึงได้จาก: http://www.ratchakitcha.soc.go.th/DATA/PDF/2560/A/010/24.PDF. (วันที่ค้นข้อมูล: 9 กันยายน 2021)

[12] ราชกิจจานุเบกษา. (2021, สิงหาคม). หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๖๔. [ออนไลน์]. Available: http://www.ratchakitcha.soc.go.th/DATA/PDF/2564/E/188/T_0009.PDF. (วันที่ค้นข้อมูล:9 กันยายน 2021)

[13] Charles Romine. (2013, กรกฎาคม). FIPS PUB 186-4 Digital Signature Standard (DSS).[ออนไลน์]. เข้าถึงได้จาก: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf.(วันที่ค้นข้อมูล: 9 กันยายน 2021)

[14] E. Barker และ J. Kelsey. (2015, มิถุนายน) NIST Special Publication 800-90A Revision 1 :Recommendation for Random Number Generation UsingDeterministic Random BitGenerators. [ออนไลน์]. เข้าถึงได้จาก: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf. (วันที่ค้นข้อมูล: 9 กันยายน 2021)

[15] The Cloud Connectivity Company. (2021). Request Size Limiting. [ออนไลน์]. เข้าถึงได้จาก: https://docs.konghq.com/hub/kong-inc/request-size-limiting/. (วันที่ค้นข้อมูล: 9กันยายน 2021)

[16] The Cloud Connectivity Company. (2021). Kong Gateway (OSS). [ออนไลน์]. เข้าถึงได้จาก: https://docs.konghq.com/gateway-oss/2.5.x/configuration/. (วันที่ค้นข้อมูล: 9 กันยายน 2021)

[17] Input Validation Cheat Sheet. (2021). [ออนไลน์]. เข้าถึงได้จาก: https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html.(วันที่ค้นข้อมูล: 9 กันยายน 2021)

มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน

เรื่องข้อกำหนดด้านโปรโตคอลระดับแอปพลิเคชันเอนพอยน์ และการจัดการโทเคนและเซสชัน

1. ขอบข่าย

การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานเป็นพื้นฐานหลักที่จำเป็นต่อการพัฒนารัฐบาลดิจิทัลในปัจจุบันประเทศไทยมีแพลตฟอร์มการแลกเปลี่ยนข้อมูลที่ให้บริการอยู่หลายแห่ง แพลตฟอร์มแต่ละแห่งมีแนวทางและพันธกิจในการดำเนินงานเป็นของตนเอง เป็นผลให้การบูรณาการข้อมูลจำเป็นต้องขับเคลื่อนด้วยการสร้างมาตรฐานหรือข้อตกลงร่วมกันในการแลกเปลี่ยนข้อมูล กรมอนามัยจึงมีความจำเป็นต้องจัดทำมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลเพื่อใช้ในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน เพื่อให้เกิดการบูรณาการข้อมูลเกิดขึ้นอย่างเป็นรูปธรรม

เป้าประสงค์หลักของการใช้มาตรฐานฯ เป็นตัวขับเคลื่อนการบูรณาการข้อมูลหน่วยงาน คือ การให้หน่วยงานมีแนวทางในการพัฒนาสถาปัตยกรรมระบบสารสนเทศเพื่อใช้ในการแลกเปลี่ยนข้อมูลที่ชัดเจนมีความสอดคล้องในการเชื่อมต่อระหว่างกัน

ดังนั้นเพื่อให้บรรลุเป้าประสงค์หลักดังกล่าวจึงมีข้อกำหนดาหนดด้านโปรโตคอลระดับแอปพลิเคชัน เอนพอยน์ และการจัดการโทเคนและเซสชัน สำหรับทำมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน เรื่องมาตรฐานสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐระดับการเชื่อมโยงข้อมูลที่เหมาะสมกับบริบทของกรมอนามัยเท่านั้น

2. นิยาม

นิยามคำศัพท์ที่เกี่ยวข้องกับมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน ด้านการเชื่อมโยงข้อมูล เรื่อง ข้อกำหนดด้านโปรโตคอลระดับแอปพลิเคชัน เอนพอยน์และการจัดการโทเคนและเซสชัน มีดังนี้

2.1 Hypertext Transfer Protocol (HTTP) หมายความว่า โปรโตคอลในระดับชั้นเซสชัน (SessionLayer) ของตัวแบบ OSI ทำหน้าที่สื่อสารผ่านระบบเครือข่ายคอมพิวเตอร์ใช้ในการรับและส่งข้อมูลในการแลกเปลี่ยนข้อมูลระหว่างเครื่องลูกข่ายและเครื่องแม่ข่าย

2.2 Hypertext Transfer Protocol Secure (HTTPS) หมายความว่า โปรโตคอลในระดับชั้นเซสชัน (Session Layer) ของตัวแบบ OSI ทำหน้าที่สื่อสารผ่านระบบเครือข่ายคอมพิวเตอร์ใช้ในการรับและส่งข้อมูล ที่ช่วยรักษาความสมบูรณ์ของข้อมูลในการแลกเปลี่ยนข้อมูลระหว่างเครื่องลูกข่ายและเครื่องแม่ข่าย รวมทั้งเก็บข้อมูลนั้นไว้เป็นความลับ

2.3 Transport Layer Security (TLS) หมายความว่า โปรโตคอลในระดับชั้นเซสชัน (Session Layer) ของตัวแบบ OSI ใช้เทคโนโลยีการเข้ารหัสข้อมูล เพื่อเพิ่มความปลอดภัยในการส่งข้อมูลบนเครือข่ายอินเทอร์เน็ตระหว่างเครื่องเซิร์ฟเวอร์กับเว็บเบราว์เซอร์หรือแอปพิเคชันที่ใช้งาน เพื่อให้ข้อมูลปลอดภัยจากการเข้าถึงโดยแฮกเกอร์ วิธีการเรียกใช้งานจะเรียกผ่านโปรโตคอล HTTPS หรือโปรโตคอลความปลอดภัยอื่น ๆ ตามแต่วิธีการใช้งาน

2.4 Transmission Control Protocol (TCP) หมายความว่า โปรโตคอลระดับชั้นทรานสปอร์ต(Transport Layer) ของตัวแบบ OSI ทำหน้าที่ควบคุมการรับส่งข้อมูลระหว่างผู้ส่งกับผู้รับ เพื่อใช้แลกเปลี่ยนข้อมูลระหว่างกัน โดยมีการตรวจสอบให้แน่ใจว่าทุกแพ็กเกจที่รับส่งมีความถูกต้อง

2.5 Application Programming Interface หรือ API หมายความว่า ช่องทางการเชื่อมโยงและการแลกเปลี่ยนข้อมูลภาครัฐระหว่างผู้ให้บริการและผู้ใช้บริการ

2.6 Representational State Transfer (REST API หรือ RESTful API) หมายความว่า ช่องทางการเชื่อมโยงและการแลกเปลี่ยนข้อมูลภาครัฐระหว่างผู้ให้บริการและผู้ใช้บริการตามมาตรฐาน

2.7 JavaScript Object Notation (JSON) หมายความว่า รูปแบบของโครงสร้างข้อมูลที่ใช้แลกเปลี่ยนผ่าน REST API

2.8 JSON Data Format หมายความว่า รูปแบบของมาตรฐานโครงสร้างข้อมูลที่ใช้แลกเปลี่ยนผ่าน REST API ตามมาตรฐาน

2.9 ผู้ให้บริการ API (Provider System) หมายความว่า ระบบสารสนเทศของหน่วยงานที่เปิดให้บริการ API สำหรับเชื่อมโยงและการแลกเปลี่ยนข้อมูลภายในแพลตฟอร์มที่ใช้มาตรฐาน

2.10 ผู้ใช้บริการ API (Consumer System) หมายความว่า ระบบสารสนเทศของหน่วยงานมีการใช้บริการ API สำหรับเชื่อมโยงและการแลกเปลี่ยนข้อมูลภายในแพลตฟอร์มที่ใช้มาตรฐาน

2.11 ผู้ให้บริการ Platform (Platform Provider) หมายความว่า ระบบสารสนเทศของหน่วยงานผู้ให้บริการ Platform เพื่อสนับสนุนดำเนินการเชื่อมโยงและการแลกเปลี่ยนข้อมูลให้เป็นไปตามมาตรฐาน

2.12 การบริการออกใบรับรอง (Certification Authority) หมายความว่า บริการของผู้ให้บริการ Platform ทำหน้าที่ออกใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) ให้แก่หน่วยงาน

2.13 การลงลายมือชื่อดิจิทัล (Digital Signature) หมายความว่า การลงลายมือชื่อดิจิทัลโดยใช้ใบรับรองอิเล็กทรอนิกส์ (Certificate) ที่ระบุตัวบุคคล หรือองค์กรผู้เป็นเจ้าของลายชื่อเพื่อแสดงว่าบุคคลหรือองค์กร ดังกล่าวยอมรับข้อความในข้อมูลอิเล็กทรอนิกส์นั้น

3. กฎหมายและแนวปฏิบัติที่เกี่ยวข้อง

การเชื่อมโยงและการแลกเปลี่ยนข้อมูลภาครัฐมีการบัญญัติไว้ในกฎหมายหรือแนวปฏิบัติที่เกี่ยวข้อง ดังนี้

3.1 รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 ในมาตรา 59 ระบุว่ารัฐต้องเปิดเผยข้อมูลหรือข่าวสารสาธารณะในครอบครองของหน่วยงานของรัฐที่มิใช่ข้อมูลเกี่ยวกับความมั่นคงของรัฐหรือเป็นความลับของทางราชการตามที่กฎหมายบัญญัติ และต้องจัดให้ประชาชนเข้าถึงข้อมูลหรือข่าวสารดังกล่าวได้โดยสะดวก

3.2 พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 ในมาตรา 13 ระบุว่าเพื่อประโยชน์ในการบริหารราชการแผ่นดินและการให้บริการประชาชนให้หน่วยงานของรัฐจัดให้มีการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลที่มีการจัดทำและครอบครองตามที่หน่วยงานของรัฐแห่งอื่นร้องขอที่จะเกิดการบูรณาการร่วมกันมาตรา 15 ระบุว่าให้มีศูนย์แลกเปลี่ยนข้อมูลกลางทำหน้าที่เป็นศูนย์กลางในการแลกเปลี่ยนข้อมูลดิจิทัลและทะเบียนดิจิทัลระหว่างหน่วยงานของรัฐ เพื่อสนับสนุนการดำเนินการของหน่วยงานของรัฐในการให้บริการประชาชนผ่านระบบดิจิทัล และดำเนินการในเรื่องดังต่อไปนี้

(1) กำหนดนโยบายและมาตรฐานเกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลเสนอต่อคณะกรรมการพัฒนารัฐบาลดิจิทัลให้ความเห็นชอบ

(2) ประสานและให้ความช่วยเหลือแก่หน่วยงานของรัฐในการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลระหว่างกัน รวมทั้งกำกับติดตามให้การดำเนินการดังกล่าวเป็นไปในแนวทางและมาตรฐานเดียวกันตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่คณะกรรมการพัฒนารัฐบาลดิจิทัลกำหนด

(3) จัดทำคำอธิบายชุดข้อมูลดิจิทัลของภาครัฐ และจัดเก็บบันทึกหลักฐานของการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล

(4) เรื่องอื่น ๆ ตามที่หน่วยงานมอบหมาย

4. ข้อกำหนดด้านโปรโตคอลระดับแอปพลิเคชัน เอนพอยน์และการจัดการโทเคนและเซสชัน

4.1 การทำงานของโปรโตคอล

การเชื่อมโยงและการแลกเปลี่ยนข้อมูลตามมาตรฐาน มีองค์ประกอบของสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน โดยมีการเชื่อมโยงข้อมูลจาก REST API Client ของผู้ใช้บริการ API (Consumer System) ไปยังเอนพอยน์(Endpoint URL) ของ REST API ของผู้ให้บริการ API (Provider System) ซึ่งเอนพอยน์ต้องมีโปรโตคอลเป็น Hypertext Transfer Protocol Secure (HTTPS) ใช้ร่วมกันกับโปรโตคอลสำหรับการรับรองความปลอดภัยในรูปแบบ Transport Layer Security (TLS) และ Secure Socket Layer (SSL) โดยขั้นตอนทั้งหมดที่กล่าวมาจะทำงานอยู่บน Transmission Control Protocol (TCP)

นอกจากนี้ข้อมูลที่ใช้ในการเชื่อมโยงและแลกเปลี่ยนทั้งหมดของ REST API ถูกรวมไว้ในรูปแบบ JSON Data Format ซึ่งประกอบด้วยข้อมูลเชิงธุรกรรม (Business Data) พร้อมทั้งข้อมูลที่เกี่ยวข้องกับความปลอดภัยเพิ่มเติม เช่น ลงลายมือชื่อดิจิทัล (Digital Signature) และ Online Certificate Status Protocol (OCSP) เพื่อใช้งานกับ Certification Authority เป็นต้น

4.2 ข้อกำหนดด้านโปรโตคอลที่เกี่ยวข้องกับเอนพอยน์

ข้อกำหนดด้านโปรโตคอลที่เกี่ยวข้องกับเอนพอยน์ (Endpoint URL) ในการเชื่อมโยงและแลกเปลี่ยนข้อมูลตามมาตรฐาน มีดังต่อไปนี้

(1) กำหนดให้ผู้ใช้บริการ API (Consumer System) มีการเรียกใช้งาน Endpoint URL ของผู้ให้บริการ (Provider System) ผ่านโปรโตคอล HTTPS เท่านั้น

(2) กำหนดให้ผู้ให้บริการ (Provider System) และ ผู้ใช้บริการ API (Consumer System) มีการใช้งาน TLS version 1.2 เป็นอย่างน้อยสำหรับการใช้งาน TLS/SSL

(3) กำหนดให้ผู้ให้บริการ (Provider System) และ ผู้ใช้บริการ API (Consumer System) ใช้งาน Transmission Control Protocol (TCP) ผ่าน TLS/SSL เท่านั้น

4.3 ข้อกำหนดด้านโครงสร้าง JSON Data Format ตามมาตรฐาน

การกำหนดโครงสร้าง JSON Data Format ตามมาตรฐาน เป็นการกำหนดรูปแบบโครงสร้างการรับส่งข้อมูลผ่าน REST API ระหว่างผู้ใช้บริการ API (Consumer System) และ ผู้ให้บริการ API (Provider System) โดยโครงสร้างของ JSON Data Format สามารถแบ่งตามประเภทการแลกเปลี่ยนข้อมูลดังตาราง

ประเภทการแลกเปลี่ยน		Content Type	รายละเอียด
การแลกเปลี่ยนข้อมูลเชิงธุรกรรม	ข้อมูลเชิงธุรกรรมที่กำหนดลักษณะ Payload เป็นรูปแบบ JSON	กำหนด Content Type ประเภท JSON	กำหนดข้อความมีลักษณะเป็น JSON ทั้งหมด
	ข้อมูลเชิงธุรกรรมที่กำหนดลักษณะ Payload ไม่ได้เป็นรูปแบบ JSON	กำหนด Content Type ประเภท Multipart	เพื่อรองรับการการแลกเปลี่ยนข้อมูล Format อื่น ๆ เช่น XML, ebXML เป็นต้น ทำให้มาตรฐาน สามารถทำงานร่วมกับ Data Format อื่น ๆ ได้
การแลกเปลี่ยนข้อมูลที่เป็น File	ขนาดของ File ไม่เกิน 5 MB	กำหนด Content Type ประเภท Multipart	เพื่อรองรับการแลกเปลี่ยนข้อมูลแบบ File ที่มีขนาดไม่เกิน 5 MB
	ขนาดของ File มากกว่า 5 MB ขึ้นไป	กำหนด Content Type ประเภท Multipart ร่วมกับ Resumable หากต้องการ	เพื่อรองรับการแลกเปลี่ยนข้อมูลแบบ File ที่มีขนาดเกิน 5MB รวมทั้งสามารถ Resume ได้กรณีการ Upload มีปัญหาตามมาตรฐาน Form-based File Upload in HTML: RFC-1867 และ Hypertext Transfer Protocol (HTTP/1.1): Range Requests: RFC-7233

4.3.1 ส่วน Message Headers

ในส่วนของ Message จะประกอบด้วย HTTP Header และ HTTP Body โดยมีรายละเอียดดังตาราง รายละเอียดโครงสร้างของ Message Headers ส่วน HTTP Header

พารามิเตอร์	ความจำเป็นต้องมี	รายละเอียด
HTTP Method	Required	กำหนด HTTP Method โดยรองรับ HTTP/1.1 และโดยรองรับกาหนดค่าเป็น POST, GET, DELETE, PUT, OPTIONS และ PATCH
Authorization	Required	กำหนดรหัสการยืนยันตนของผู้ใช้งาน โดยกำหนดค่าเป็น Bearer เสมอ
Accept-Encoding	Required	กำหนดการเข้ารหัสข้อมูล
Accept-Language	Required	กำหนดภาษาในการตอบรับ
Accept	Required	กำหนดประเภทของเนื้อหา

พารามิเตอร์	ความจำเป็นต้องมี	รายละเอียด
Host	Required	กำหนด URL ปลายทาง
Cache-Control	Required	กำหนดคำสั่งชี้แนะว่าจะต้องทำตามกลไกการเก็บแคชทั้งหมดโดยตลอดทั้งการร้องขอและการตอบรับ
Connection	Required	กำหนดวิธีการเชื่อมต่อ
Content-Type	Required	กำหนดชนิดของเนื้อหาที่ร้องขอ
Content-Length	Required	กำหนดความยาวของข้อมูลเนื้อหา
Origin	Required	กำหนด URL ต้นทาง
messageVersion	Required	กำหนดเวอร์ชั่นของ API
MessageId	Required	กำหนดรหัสของข้อความ
Timestamp	Required	กำหนดเวลาในการร้องขอ
clientId	Required	กำหนดรหัสของผู้ใช้บริการ
event	Required	กำหนดรายละเอียดการที่จะดำเนินการ (Action)

รายละเอียดโครงสร้างของ Message Headers ส่วน HTTP Body

พารามิเตอร์	ความจำเป็นต้องมี	รายละเอียด
ExpirationTime	Required	กำหนดเวลาที่หมดอายุของข้อความ
RequestId	Required	กำหนดรหัสของการร้องขอสำหรับตอบกลับ
Action: Method	Required	กำหนด HTTP Method ในการร้องขอ
Action: Path	Required	กำหนด Context Path ในการร้องขอ
Action: URL	Required	กำหนด URL ในการร้องขอ
Action: Parameter	Optional	กำหนดพารามิเตอร์ เพิ่มเติม โดยต้องกำหนด “parameterName”: “value” เสมอ
messageStatus	Required	กำหนดสถานะของข้อความ
messageStatus: status	Required	กำหนดสถานะตามมาตรฐาน HTTP Status
messageStatus: description	Required	กำหนดรายละเอียดสถานะ
messageStatus: error	Required	กำหนดรายละเอียดกรณีร้องขอไม่สำเร็จ โดยผู้ให้บริการเป็นผู้กำหนดเอง
error: code	Required	กำหนดรหัสของ Error
error: message	Required	กำหนดข้อความที่ต้องการแสดง Error
apiKey	Optional	กำหนดรหัสของ API
Headers	Optional	กำหนด Header เพิ่มเติมของข้อความ

4.3.2 ส่วน Message Payloads

ในส่วนของ Message ประกอบด้วย HTTP Body เป็นการกำหนดรูปแบบการรับส่งข้อมูลแบบ Multipart Content-Type เพื่อรองรับการรับส่งข้อมูลจากผู้ขอใช้บริการข้อมูลได้หลายรูปแบบ แต่อยู่ภายใต้ Header ที่เป็นเป็น JSON โดยมีรายละเอียดดังนี้

พารามิเตอร์	ความจำเป็นต้องมี	รายละเอียด
Content-Type	Required	กำหนด Body ของเนื้อหา โดยสามารถกำหนดได้หลายรูปแบบ (Any MimeType) เช่น JSON, XML และ File เป็นต้น

4.3.3 ส่วน Message Signature

ในส่วนของ Message จะประกอบด้วย HTTP Body เป็นการตรวจสอบความถูกต้องและครบถ้วนของข้อมูลที่รับส่งระหว่างผู้ใช้บริการและผู้ให้บริการ โดยการน าข้อมูล Header และ Payloads ที่ได้รับมาไปเข้ารหัสเทียบกับค่าของ sigValue ที่ถอดรหัสแล้ว ถ้าตรงกันจะถือว่าข้อมูลที่รับส่งนั้นครบถ้วนสมบูรณ์โดยมีรายละเอียดดังนี้

พารามิเตอร์	ความจำเป็นต้องมี	รายละเอียด
alg	Required	กำหนดอัลกอริธึมของกุญแจ เช่น RS256, RFC-7518
cert	Required	กำหนด Public Key ของลายมือชื่อดิจิทัล
sigValue	Required	กำหนดกุญแจที่ใช้ในการลงลายมือชื่อดิจิทัล

4.4 การบริหารจัดการ Session

4.4.1 การใช้งานเซสชัน (Session)

เซสชันตามมาตรฐาน คือ กลุ่มของข้อมูลใช้สำหรับการโต้ตอบระหว่างผู้ใช้บริการ (Consumer System) และผู้ให้บริการ (Provider System) ที่เกิดขึ้นภายในช่วงเวลาที่กำหนดเซสชัน (Session) เดียวสามารถมีได้หลายกิจกรรม ซึ่งเซสชันทั้งหมดเก็บไว้ชั่วคราวในขณะที่ผู้ใช้เชื่อมต่ออยู่ตามมาตรฐาน มีการกำหนดให้มีการใช้การยืนยันตัวตน ด้วย Open ID Connect 1.0 (OIDC) เมื่อผู้ใช้เข้าสู่ระบบจะมีการสร้างเซสชันสำหรับผู้ใช้ที่รับรองความถูกต้องผ่านแอปพลิเคชัน และเมื่อต้องการตรวจสอบสิทธิ์สามารถใช้ข้อมูลในเซสชันช่วยเป็นตัวกำหนดว่าผู้ใช้ต้องได้รับการตรวจสอบทุกครั้งที่มีการขอเพื่อเข้าใช้งานบริการข้อมูลของผู้ให้บริการ API (Provider System) โดยมีการใช้งานร่วมกับโทเค็น (Token) ที่มีการส่งไปพร้อมกับข้อมูลขอใช้บริการ รายละเอียดโทเค็นจะกล่าวถึงในส่วนการบริหารจัดการโทเค็นต่อไป เซสชันสามารถแบ่งออกได้เป็น 3 ส่วน คือ

(1) แอปพลิเคชันเซสชัน (Application Session) ส่วนนี้เป็นเซสชันภายในแอปพลิเคชัน ใช้สำหรับติดตามผู้ใช้งานมีการลงชื่อเข้าใช้งานหรือไม่ โดยการจัดเก็บข้อมูลไว้ในคุกกี้ (Cookie) หรือมีประโยชน์ในการเก็บข้อมูลกิจกรรมที่เกิดขึ้นในแอปพลิเคชันว่ามีการเข้าใช้งานระบบส่วนไหนบ้าง

(2) เซสชันการอนุญาต (Authorization Session) เซสชันการอนุญาต เป็นการเก็บเซสชันบนเซิร์ฟเวอร์การให้สิทธิ์สำหรับผู้ใช้และจัดเก็บข้อมูลผู้ใช้ไว้ในคุกกี้ เซสชันนี้ใช้เพื่อให้ครั้งต่อไปที่ผู้ใช้ถูกเปลี่ยนเส้นทาง (Redirect) ไปยังโปรแกรมบริการเพื่อเข้าสู่ระบบข้อมูลของผู้ใช้จะถูกจดจำสำหรับการใช้งานลงชื่อเพียงครั้งเดียว (SSO)

(3) เซสชันผู้ให้บริการข้อมูลประจำตัว (Identity Provider Session) เซสชันนี้เกิดขึ้นเมื่อผู้ใช้ลงชื่อเข้าใช้งานระบบโดยใช้ผู้ให้บริการข้อมูลประจำตัว เช่น Identity Provider Server และมีการลงชื่อเข้าใช้ถูกต้องอยู่แล้ว ผู้ให้บริการข้อมูลประจำตัวจะสร้างเซสชันขึ้นเพื่อเก็บข้อมูลประจำตัว เมื่อผู้ใช้มีการใช้งานข้อมูลประจำตัวจะไม่ได้รับแจ้งให้ลงชื่อเข้าใช้อีก

4.4.2 การกำหนดอายุของเซสชัน (Session Lifetime Limits)

แนะนำให้มีการกำหนดค่าในส่วนนี้ เพื่อเป็นการกำหนดว่าผู้ให้บริการควรจะเก็บเซสชันไว้นานเท่าไหร่ก่อนจะทำการออกจากระบบโดยอัตโนมัติ โดยผู้ให้บริการที่พัฒนาระบบตามมาตรฐาน OAuth 2.0 นั้นจะต้องมีการกำหนดค่าหมดเวลาไม่ใช้งาน (Inactivity timeout) คือกรอบเวลาหลังจากที่เซสชันของผู้ใช้จะหมดอายุหากไม่ได้โต้ตอบกับเซิร์ฟเวอร์การให้สิทธิ์ จะถูกทำให้ออกจากระบบหากเกินเวลาที่กำหนด และค่าต้องเข้าสู่ระบบหลังจากเวลาที่กำหนด (Require log in after) คือ กรอบเวลาที่กำหนดให้ผู้ใช้งานจะต้องเข้าสู่ระบบอีกครั้ง

4.4.3 การล้างเซสชัน

ส่วนของการล้างเซสชัน แนะนำให้ทำการล้างเซสชันเมื่อผู้ใช้งานออกจากระบบหรือแอบพลิเคชันนั้นๆ

4.4.3.1 การล้างเซสชันระดับแอปพลิเคชัน

เซสชันในส่วนปกติแล้วจะเกิดขึ้นเมื่อมีผู้ใช้งานเข้ามาใช้งานแอปพลิเคชันของผู้ขอใช้บริการ (Consumer) จะมีการสร้างเซสชันขึ้นมาเพื่อใช้งาน เมื่อผู้ใช้งานออกจากระบบ การล้างเซสชันในส่วนนี้จะต้องเป็นหน้าที่ของแอปพลิเคชันที่ต้องท าการล้างเซสชันทั้งหมดที่เกิดขึ้นโดยการบริหารจัดการในส่วนนี้สามารถทำได้ดังนี้

(1) การกำหนดอายุของเซสชัน (Session Expiration) เพื่อลดระยะเวลาที่ผู้โจมตีสามารถเริ่มการโจมตีในเซสชันที่ใช้งานอยู่และขโมยเซสชันเหล่านั้น จำเป็นต้องกำหนดอายุสำหรับทุกเซสชัน โดยกำหนดระยะเวลาที่เซสชันจะยังคงทำงานอยู่ การกำหนดอายุของเซสชันที่นานเกินความจำเป็นสำหรับเว็บแอปพลิเคชันจะเพิ่มช่องโหว่ของการโจมตีตามเซสชันได้โดยผู้โจมตีจะสามารถใช้ ID เซสชันที่ถูกต้องโจมตีซ้ำๆ ได้อยู่ ยิ่งการกำหนดช่วงเซสชันสั้นลงเท่าใด ผู้โจมตีก็จะมี

โอกาสใช้รหัสเซสชันที่ถูกต้องน้อยลงเท่านั้น ดังนั้นการกำหนดเวลาหมดอายุของเซสชันตามมาตรฐาน แนะนำมีการกำหนดค่าให้สอดคล้องกับวัตถุประสงค์และลักษณะการใช้งานหรือให้บริการของเว็บแอปพลิเคชัน โดยคำนึงถึงความปลอดภัยและการใช้งาน เพื่อให้ผู้ใช้สามารถดำเนินการภายในเว็บแอปพลิเคชันให้เสร็จสิ้นได้อย่างสะดวกสบายโดยที่เซสชันหมดอายุบ่อยครั้งจนเกินไป

เมื่อเซสชันหมดอายุ เว็บแอปพลิเคชันต้องดำเนินการเพื่อทำให้เซสชันเป็นโมฆะทั้งสองด้านทั้งไคลเอ็นต์และเซิร์ฟเวอร์

สำหรับกลไกการแลกเปลี่ยนเซสชันส่วนใหญ่ การดำเนินการฝั่งไคลเอ็นต์เพื่อทำให้ ID เซสชันใช้งานไม่ได้จะขึ้นอยู่กับการล้างค่าในโทเค็น ตัวอย่างเช่น หากต้องการทำให้คุกกี้ใช้งานไม่ได้ ข้อแนะนำคือ ให้ระบุค่าว่างสำหรับรหัสเซสชัน และตั้งค่าแอตทริบิวต์ Expires (หรือ Max-Age) เป็นวันที่ในอดีต

(2) การทำให้เซสชันหมดอายุอัตโนมัติ (Automatic Session Expiration) หมดเวลาที่ไม่ได้ใช้งาน (Idle Timeout) ข้อแนะนำคือ เซสชันทั้งหมดควรมีการกำหนดค่าหมดเวลาเมื่อไม่มีการใช้งานค่าหมดเวลานี้เป็นการกำหนดระยะเวลาที่เซสชันจะยังคงอยู่และสามารถใช้งานได้ ในกรณีที่ไม่มีกิจกรรมในเซสชันจะถูกทำให้เซสชันเป็นโมฆะเมื่อเลยช่วงเวลาที่กำหนดไว้โดยนับตั้งแต่คำร้องขอ HTTP ล่าสุดได้รับจากเว็บแอปพลิเคชัน การกำหนดค่าหมดเวลาเมื่อไม่มีการใช้งานจะเป็นการจำกัดโอกาสที่ผู้โจมตีใช้ ID เซสชันที่ถูกต้องในการโจมตี หากผู้โจมตีสามารถขโมยเซสชันได้ แนะนำให้มีการกำหนดค่าหมดเวลาของเซสชันและการหมดอายุในฝั่งเซิร์ฟเวอร์

(3) การทำให้หมดอายุของเซสชันด้วยตนเอง (Manual Session Expiration) เว็บแอปพลิเคชันจะต้องมีกลไกที่อนุญาตให้ผู้ใช้สามารถปิดเซสชันของตนได้เมื่อใช้งานเว็บแอปพลิเคชันเสร็จแล้ว โดยเว็บแอปพลิเคชันต้องมีปุ่มล็อกเอาต์ ออกจากระบบที่มองเห็นและเข้าถึงได้ง่าย ซึ่งอยู่ในส่วนหัวหรือเมนูของแอปพลิเคชันเว็บ และสามารถเข้าถึงได้จากทุกหน้า เพื่อให้ผู้ใช้สามารถปิดเซสชันด้วยตนเองเวลาใดก็ได้

4.4.3.2 การล้างเซสชันการอนุญาต

โดยปกติแอปพลิเคชันผู้ให้บริการให้สิทธิ์จะมี ฟังก์ชันให้เรียกใช้งานอยู่แล้วเพื่อล้างเซสชันชี้นอยู่กับเครื่องมือที่นำมาใช้ในการพัฒนาแอปพลิเคชัน การล้างเซสชันในส่วนนี้สามารถทำได้โดยจะต้องเรียกฟังก์ชันล้างเซสชันของแอปพลิเคชันผู้ให้บริการให้สิทธิ์

4.4.3.3 การล้างเซสชันผู้ให้บริการข้อมูลประจำตัว

สำหรับการล้างเซสชันในส่วนนี้ไม่มีความจำเป็นต้องดำเนินการใดสำหรับแอปพลิเคชันของผู้ขอใช้บริการ (Consumer) ตามมาตรฐาน แนะนำให้ปฏิบัติตามขั้นตอนการล้างเซสชันระดับแอปพลิเคชันและการล้างเซสชันการพิสูจน์ตัวตน ก็เพียงพอสำหรับการทำงาน ประกอบกับการกำหนดอายุของเซสชัน (Session Lifetime Limits) ผู้ให้บริการพิสูจน์และยืนยันตัวตน ในกรณีที่ผู้ใช้งานไม่ได้ทำการออกจากระบบ จะถูกทำให้ออกจากระบบโดยอัตโนมัติ เมื่อถึงเวลาที่กำหนด

4.4.4 การตรวจจับการโจมตีเซสชัน (Session Attacks Detection)

โดยปกติแอปพลิเคชันจะต้องมีการออกแบบ และพัฒนาโดยคำนึงถึงความปลอดภัยของแอปพลิเคชันดังนั้นฟังก์ชันการทำงานด้านความปลอดภัยพื้นฐานตามมาตรฐาน แนะนำควรจะมีดังต่อไปนี้

(1) การเดารหัสเซสชันและการตรวจจับการบังคับเซสชันที่ถูกต้อง (Session ID Guessing and Brute Force Detection) ในกรณีที่ผู้โจมตีพยายามคาดเดาหรือบังคับ ID เซสชันที่ถูกต้อง จำเป็นต้องเรียกใช้คำร้องขอจำนวนหลายรายการกับเว็บแอปพลิเคชันเป้าหมายโดยใช้ ID เซสชันที่แตกต่างกันจากที่อยู่ IP Address เดียว นอกจากนี้ ยังรวมถึงผู้โจมตีพยายามวิเคราะห์การคาดการณ์ของ ID เซสชัน เช่น การใช้การวิเคราะห์ทางสถิติก็จำเป็นต้องเรียกใช้คำร้องขอจำนวนหลายรายการจากที่อยู่ IP Address เดียวกันเพื่อนำข้อมูลมาเปรียบเทียบและรวบรวมข้อมูลให้เพียงพอสำหรับการสร้างเซสชัน ID ใหม่ที่ถูกต้อง

ข้อแนะนำเว็บแอปพลิเคชันต้องมีฟังก์ชันที่สามารถตรวจพบทั้งสองสถานการณ์ได้ โดยตรวจสอบจากตามจำนวนครั้งที่พยายามร้องขอข้อมูล จะต้องมีการแจ้งเตือนและบล็อกที่อยู่ IP Address ที่ละเมิดได้

(2) การตรวจจับความผิดปกติของรหัสเซสชัน (Detecting Session ID Anomalies) เว็บแอปพลิเคชันควรเน้นที่การตรวจจับความผิดปกติที่เกี่ยวข้องกับ ID เซสชัน แนะนำให้มีการพัฒนาเว็บแอปพลิเคชันโดยดูคำแนะน าจาก OWASP เป็นกรอบแนวทางและนำวิธีการต่างๆ มาปรับใช้เพื่อให้มีความสามารถในการตรวจจับการบุกรุก โดยเว็บแอปพลิเคชันควรเน้นไปที่การตรวจจับความผิดปกติและพฤติกรรมที่ไม่คาดคิด แทนที่จะใช้การป้องกันจากองค์ประกอบ

ภายนอกเช่น fire wall บางครั้งรายละเอียดข้อมูลต่างๆ ที่ได้จากภายในเว็บแอปพลิเคชันเท่านั้นที่จะสร้างจุดสังเกต และตรวจจับที่เกี่ยวข้องกับเซสชันได้หลายจุด เช่น เมื่อมีการแก้ไขคุกกี้สร้างคุกกี้ใหม่ การใช้รหัสเซสชันจากผู้ใช้รายอื่นซ้ำหรือเมื่อ User-Agent เปลี่ยนแปลงไปจากเดิมในช่วงระหว่างการสื่อสาร

(3) การผูก ID เซสชันกับคุณสมบัติผู้ใช้อื่น (Binding the Session ID to Other User Properties) ในการตรวจจับพฤติกรรมที่ไม่เหมาะสมของผู้ใช้และการขโมยเซสชัน ข้อแนะนำให้ผูก ID เซสชันกับผู้ใช้หรือคุณสมบัติของไคลเอ็นต์ เช่น IP Address ของไคลเอ็นต์, User-Agent, ใบรับรองดิจิทัล หากเว็บแอปพลิเคชันตรวจพบการเปลี่ยนแปลงหรือความผิดปกติของคุณสมบัติของไคลเอ็นต์ต่าง ๆ ในช่วงการสื่อสารของเซสชันที่สร้างขึ้นจะเป็นจุดสังเกตสำหรับการจัดการความพยายามในการขโมยบัญชีและสามารถใช้ข้อมูลนี้ เพื่อแจ้งเตือนและยุติเซสชันที่ไม่ถูกต้อง การใช้คุณสมบัติเหล่านี้เพื่อป้องกันการโจมตีเซสชันเป็นเพียงการเพิ่มความสามารถในการตรวจจับของเว็บแอปพลิเคชันเท่านั้น

4.4.5 การป้องกันและจัดการเซสชันโดยใช้ Web Application Firewalls

ในกรณีที่การตรวจจับการบุกรุก โดยเว็บแอปพลิเคชันยังไม่สามารถครอบคลุมได้เพื่อเป็นการเสริมการป้องกันเว็บแอปพลิเคชัน โดยมีเป้าหมายเพื่อให้เว็บแอปพลิเคชันมีความปลอดภัยมากขึ้น ข้อแนะนำให้ใช้การป้องกันภายนอก เช่น Web Application Firewalls (WAFs) ที่สามารถป้องกันภัยคุกคามการจัดการเซสชันที่อธิบายไว้แล้วข้างต้น โดยความสามารถในการตรวจจับ และป้องกันการโจมตีตามเซสชันสำหรับ WAF เป็นการบังคับให้มีการใช้แอตทริบิวต์ความปลอดภัยบนคุกกี้ เช่น แฟล็ก Secure และ HttpOnly โดยใช้เป็นกฎพื้นฐานบนส่วนหัว Set-Cookie สำหรับการตอบกลับของเว็บแอปพลิเคชันทั้งหมดจะต้องมีการใช้แอตทริบิวต์ความปลอดภัยบนคุกกี้ ความสามารถของ WAF สามารถติดตามเซสชันและ ID เซสชันที่เกี่ยวข้อง และใช้ป้องกันการแก้ไขเซสชัน โดยตรวจสอบความสัมพันธ์ระหว่าง ID เซสชันและคุณสมบัติของไคลเอ็นต์ เช่น IP Address หรือ User-Agent หรือจัดการการหมดอายุของเซสชัน โดยบังคับให้ไคลเอ็นต์และเว็บแอปพลิเคชันสิ้นสุดเซสชัน

4.4.6 การจัดการเซสชันในสถาปัตยกรรม Stateless

แนวคิดของสำหรับการจัดการเซสชันในสถาปัตยกรรม Stateless สำหรับนักพัฒนาที่ใช้เซสชันการเก็บสถานะ เพื่อให้เห็นประโยชน์และสามารถพัฒนาได้อย่างไร นอกจากนี้ยังอธิบายรายละเอียดของ JWT ตามมาตรฐาน OAuth 2.0 ซึ่งจะกล่าวถึงในหัวข้อถัดไป

เนื่องจากการรับรองความถูกต้องจะต้องมีการเก็บสถานะเป็นเวลานาน สำหรับกรณี stateful เมื่อผู้ใช้ทำการเข้าใช้งานจะต้องป้อนข้อมูลประจำตัว จากนั้นแอปพลิเคชันจะสร้าง ID เซสชันที่ไม่ซ้ำกันเก็บไว้ที่เซิร์ฟเวอร์ และส่งคืน ID เซสชันกลับให้ผู้ใช้ โดยข้อมูลรายละเอียดผู้ใช้ทั้งหมดจะถูกเก็บไว้ที่เซิร์ฟเวอร์ ทุกบริการที่ต้องใช้ข้อมูลบางอย่างเกี่ยวกับผู้ใช้จะต้องติดต่อกับฐานข้อมูลที่จัดเก็บข้อมูล ซึ่งวิธีการนี้มีข้อดีในกรณีที่ข้อมูลผู้ใช้ถูกรวมศูนย์ ทำให้ยากต่อการปลอมแปลงข้อมูลได้ และข้อมูลยังปรับปรุงให้ทันสมัยอยู่เสมอทุกอย่างถูกเก็บไว้ในฐานข้อมูลศูนย์กลาง สำหรับสถาปัตยกรรมรูปแบบ stateful การดึงข้อมูลจากส่วนกลางเพื่อดำเนินการบางอย่างอาจก่อให้เกิดปัญหา button neck ได้ในกรณีที่มีความต้องการในการเข้าถึงข้อมูลจำนวนมากการดำเนินการทั้งหมดที่กล่าวมาจะไม่เกิดปัญหา หากการพิสูจน์ตัวตนและการอนุญาตเป็นแบบ stateless เนื่องจากการร้องขอแต่ละครั้งจะมีข้อมูลที่จำเป็นทั้งหมดที่อยู่แล้ว โดยการสร้าง “รหัสเซสชัน” พิเศษซึ่งเป็นผลมาจากการเข้ารหัสข้อมูลด้วยรหัสลับที่เก็บไว้เซิร์ฟเวอร์ ทำให้สามารถส่งข้อมูลนั้นให้กับผู้ใช้งาน โดยไม่ต้องกังวลว่าจะถูกแก้ไขข้อมูล หรือกล่าวอีกนัยหนึ่งคือ สามารถรักษาคุณลักษณะของข้อมูลในรหัสเซสชันไว้เหมือนเดิมและในขณะเดียวกันก็สามารถที่จะเพิ่มข้อมูลต่าง ๆ เพิ่มเติมได้ซึ่งทำให้เข้าถึงข้อมูลฝั่งเซิร์ฟเวอร์ไม่จำเป็นต้องมีการดึงข้อมูลจากฐานข้อมูลหรือที่จัดเก็บข้อมูลอีก เซิร์ฟเวอร์ทำแค่ถอดรหัสข้อมูลที่มีอยู่ใน "รหัสเซสชัน" นั้น จากนี้ไปจะกล่าวถึงองค์ประกอบเหล่านี้ว่าเป็นโทเค็น ซึ่งจะกล่าวถึงในหัวข้อถัดไป

ข้อดีของ stateless คือ สามารถใช้ทั้งสองวิธีพร้อมกันได้ หากปัจจุบันสถาปัตยกรรมที่ใช้รหัสเซสชันสามารถเพิ่ม JWT ลงไปได้ หรือสามารถฝังรหัสเซสชันในโทเค็นและให้ API Gateway ทำการดึงข้อมูลเหล่านั้นแล้วส่งต่อไปยังผู้บริการต่อไปได้สามารถเพิ่มการรับรองความถูกต้องสมัยใหม่ให้กับแอปพลิเคชันรุ่นเก่าโดยการปรับให้มีการสร้าง JWT เป็นคุกกี้ กล่าวอีกนัยหนึ่ง คือการใช้ JWT เป็นรหัสเซสชันที่ไม่ซ้ำกันแทน ID เซสชันเดิม ในกรณีที่สถาปัตยกรรมอนุญาตให้ใช้รูปแบบ ID เซสชันได้หลากหลาย วิธีการนี้เป็นตัวเลือกที่ดีสำหรับนักพัฒนา

4.5 การบริหารจัดการ Token

4.5.1 มาตรฐานการสร้าง Token

การให้บริการข้อมูล ผู้ให้บริการจะต้องมีการกำหนดการรูปแบบการรักษาความปลอดภัยในการรับส่งข้อมูล ซึ่งมีมาตรฐานที่แตกต่างกันมาก ยกตัวอย่างเช่น การใช้การลงนามข้อความตาม OAuth 1.0การตรวจสอบสิทธิ์และการอนุญาตที่ใช้ OAuth 2.0 ซึ่งมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน ด้านการเชื่อมโยงข้อมูลได้กำหนดให้ใช้รูปแบบการตรวจสอบสิทธิ์และการอนุญาตที่ใช้ Open ID Connect 1.0 (OIDC) มาตรฐานดังกล่าวได้มีการกล่าวถึงโทเค็น และไอดีโทเค็น ซึ่งรายละเอียดของโทเค็นและไอดีโทเค็นได้อ้างถึงในมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน ด้านการเชื่อมโยงข้อมูล เรื่อง ข้อกำหนดด้านการยืนยันตัวตน การกำหนดสิทธิ์ และบัญชีการใช้งาน โดยทั้งโทเค็น และไอดีโทเค็นได้มีการกำหนดรูปแบบการรักษาความปลอดภัยสำหรับโทเค็น โดยอ้างอิงตามมาตรฐาน JSON Web Tokens (JWT): RFC-7519 [4]

มาตรฐาน JSON Web Token (JWT): RFC-7519 [4] ซึ่งมีข้อกำหนดที่กะทัดรัดและครอบคลุมเหมาะสำหรับการรับส่งข้อมูลเจสันออบเจ็ค เนื่องจากมีขนาดค่อนข้างเล็ก จึงสามารถส่งผ่านพารามิเตอร์ POST หรือสามารถส่งภายในส่วนหัว HTTP ได้ อีกทั้ง JWT มีข้อมูลที่จำเป็นเพียงพอที่ผู้รับตรวจสอบความถูกต้องของโทเค็นได้โดยไม่ต้องเรียกเซิร์ฟเวอร์ และเพื่อหลีกเลี่ยงการสืบค้นฐานข้อมูลมากกว่าหนึ่งครั้งสำหรับการเรียกดูข้อมูลที่เกี่ยวกับเอนติตี้ ประโยชน์ของการใช้งานมาตรฐาน JWT มีดังต่อไปนี้

(1) JWT มีขนาดที่เล็กกว่าเมื่อเทียบกับ โทเค็น SAML ซึ่งเป็นโทเค็นที่เกิดจากการนำ XML มาผ่านกระบวนการแฮชและการลงลายมือชื่อดิจิทัล เนื่องจาก JSON มีความละเอียดของส่วนขยายน้อยกว่า XMLดังนั้นเมื่อมีการเข้ารหัส JWT จะมีขนาดที่เล็กกว่าโทเค็น SAML สิ่งนี้ทำให้ JWT เป็นตัวเลือกที่ดีในการส่งผ่านโปรโตคอล Hyper Test Transfer Protocol

(2) มีความปลอดภัยสูง JWT สามารถใช้คู่คีย์สาธารณะ/ส่วนตัวในรูปแบบของใบรับรอง X.509 สำหรับการลงนาม JWT ยังสามารถเซ็นชื่อด้วยคีย์แบบสมมาตรโดยข้อมูลลับที่ใช้ร่วมกันโดยใช้อัลกอริธึม HMAC

(3) มีความนิยมใช้งานกันอย่างแพร่หลาย เนื่องจากภาษาที่ใช้ในการพัฒนาในปัจจุบันรองรับรูปแบบข้อมูลเจสันออบเจ็คอยู่แล้วจึงทำให้ใช้งานได้ง่ายกว่าเมื่อเทียบกับ XML

บรรณานุกรม

[1] E. Nebel. (1995,พฤศจิกายน). Form-based File Upload in HTML. [ออนไลน์]. เข้าถึงได้จาก: https://www.ietf.org/rfc/rfc1867.txt. (วันที่ค้นข้อมูล: 9 กันยายน 2021)

[2] R. Fielding. (2014, มิถุนายน). Hypertext Transfer Protocol (HTTP/1.1): Range Requests. [ออนไลน์]. เข้าถึงได้จาก: https://www.rfc-editor.org/rfc/rfc7233#section-4.2. (วันที่ ค้นข้อมูล: 9 กันยายน 2021)

[3] Hypertext Transfer Protocol -- HTTP/1.1. (1999, มิถุนายน). [ออนไลน์]. เข้าถึงได้จาก: https://www.w3.org/Protocols/rfc2616/rfc2616.html. (วันที่ค้นข้อมูล: 9 กันยายน 2021)

[4] M. Jones. (2015,พฤษภาคม) JSON Web Token (JWT). [ออนไลน์]. เข้าถึงได้จาก: https://datatracker.ietf.org/doc/html/rfc7519#section-7.2. (วันที่ค้นข้อมูล: 9 กันยายน 2021)

[5] M. Jones. (2015,พฤษภาคม) JSON Web Algorithms (JWA). [ออนไลน์]. เข้าถึงได้จาก: https://datatracker.ietf.org/doc/html/rfc7518. (วันที่ค้นข้อมูล: 9 กันยายน 2021)

[6] M. Jones. (2015, พฤษภาคม) JSON Web Signature (JWS). [ออนไลน์]. เข้าถึงได้จาก: https://datatracker.ietf.org/doc/html/rfc7515. (วันที่ค้นข้อมูล: 9 กันยายน 2021)

มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน

เรื่อง ข้อกำหนดด้านการกำหนดชื่อและเนมสเปซ

1. ขอบข่าย

การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานเป็นพื้นฐานหลักที่จำเป็นต่อการพัฒนารัฐบาลดิจิทัลในปัจจุบันประเทศไทยมีแพลตฟอร์มการแลกเปลี่ยนข้อมูลที่ให้บริการอยู่หลายแห่ง แพลตฟอร์มแต่ละแห่งมีแนวทางและพันธกิจในการดำเนินงานเป็นของตนเอง เป็นผลให้การบูรณาการข้อมูลจำเป็นต้องขับเคลื่อนด้วยการสร้างมาตรฐานหรือข้อตกลงร่วมกันในการแลกเปลี่ยนข้อมูล กรมอนามัยจึงมีความจำเป็นต้องจัดทำมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูล เพื่อใช้ในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน เพื่อให้เกิดการบูรณาการข้อมูลเกิดขึ้นอย่างเป็นรูปธรรม

เป้าประสงค์หลักของการใช้มาตรฐานฯ เป็นตัวขับเคลื่อนการบูรณาการข้อมูลหน่วยงาน คือ การให้หน่วยงานมีแนวทางในการพัฒนาสถาปัตยกรรมระบบสารสนเทศเพื่อใช้ในการแลกเปลี่ยนข้อมูลที่ชัดเจนมีความสอดคล้องในการเชื่อมต่อระหว่างกัน

ดังนั้นเพื่อให้บรรลุเป้าประสงค์หลักดังกล่าวจึงมีาเสนอข้อกำหนดด้านการกำหนดชื่อและเนมสเปซ สำหรับทำมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน เรื่องมาตรฐานสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐระดับการเชื่อมโยงข้อมูลที่เหมาะสมกับบริบทของกรมอนามัยเท่านั้น

2. นิยาม

นิยามคำศัพท์ที่เกี่ยวข้องกับมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน เรื่องข้อกำหนดด้านการกำหนดชื่อและเนมสเปซที่ใช้ในเอกสารฉบับนี้มีดังนี้

2.1 ผู้ให้บริการ API (Provider System) หมายความว่า ระบบสารสนเทศของหน่วยงานที่เปิดให้บริการ API สำหรับเชื่อมโยงและการแลกเปลี่ยนข้อมูลภายในแพลตฟอร์มใช้ตามมาตรฐาน

2.2 ผู้ใช้บริการ API (Consumer System) หมายความว่า ระบบสารสนเทศของหน่วยงานมีการใช้บริการ API สำหรับเชื่อมโยงและการแลกเปลี่ยนข้อมูลภายในแพลตฟอร์มที่ใช้ตามมาตรฐาน

2.3 REST (Representational State Transfer) หมายความว่า API ที่ใช้มาตรฐาน REST API เป็นรูปแบบสถาปัตยกรรมซอฟต์แวร์สำหรับสร้าง Web Service API ที่ทำงานผ่าน Hypertext Transfer Protocol (HTTP) โดยผู้ให้บริการ API สามารถรับคำขอและตอบกลับข้อมูลไปยังผู้ใช้บริการ (Consumer) ได้ตามมาตรฐาน REST API

2.4 Application Programming Interface (API) หมายความว่า ช่องทางการเชื่อมประสานระหว่างระบบสารสนเทศระหว่างผู้ให้บริการและผู้ใช้บริการในการแลกเปลี่ยนข้อมูลผ่านเครือข่ายคอมพิวเตอร์

2.5 ทรัพยากรข้อมูล (Data Resources) หมายความว่า ชุดข้อมูลที่ให้บริการ โดยสามารถแบ่งออกได้ 2 ประเภท คือ Instance Resource คือ ชุดข้อมูลที่มีจำนวนหนึ่งรายการและ Collections Resource คือ ชุดข้อมูลที่มีจำนวนมากกว่าหนึ่งรายการ

2.6 HTTP Header หมายความว่า ส่วนประกอบของโปรโตคอล HTTP ส่วนแรกที่ใช้สำหรับกำหนดลักษณะเฉพาะต่าง ๆ ของข้อมูลที่มีการร้องขอใช้บริการ

2.7 HTTP Body หมายความว่า ส่วนประกอบของโปรโตคอล HTTP ส่วนเนื้อหาที่อยู่ลำดับถัดจาก HTTP Header เป็นส่วนที่ใช้ระบุรายละเอียดเนื้อหาที่ต้องการส่งไปขอใช้บริการ

3. กฎหมายและแนวปฏิบัติที่เกี่ยวข้อง

การเชื่อมโยงและการแลกเปลี่ยนข้อมูลภาครัฐมีการบัญญัติไว้ในกฎหมายหรือแนวปฏิบัติที่เกี่ยวข้อง ดังนี้

3.1 รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 ในมาตรา 59 ระบุว่ารัฐต้องเปิดเผยข้อมูลหรือข่าวสารสาธารณะในครอบครองของหน่วยงานของรัฐที่มิใช่ข้อมูลเกี่ยวกับความมั่นคงของรัฐหรือเป็นความลับของทางราชการตามที่กฎหมายบัญญัติ และต้องจัดให้ประชาชนเข้าถึงข้อมูลหรือข่าวสารดังกล่าวได้โดยสะดวก

3.2 พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 ในมาตรา 13 ระบุว่าเพื่อประโยชน์ในการบริหารราชการแผ่นดินและการให้บริการประชาชนให้หน่วยงานของรัฐจัดให้มีการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลที่มีการจัดทำและครอบครองตามที่หน่วยงานของรัฐแห่งอื่นร้องขอที่จะเกิดการบูรณาการร่วมกันมาตรา 15 ระบุว่าให้มีศูนย์แลกเปลี่ยนข้อมูลกลางทำหน้าที่เป็นศูนย์กลางในการแลกเปลี่ยนข้อมูลดิจิทัลและทะเบียนดิจิทัลระหว่างหน่วยงานของรัฐ เพื่อสนับสนุนการดำเนินการของหน่วยงานของรัฐในการให้บริการประชาชนผ่านระบบดิจิทัล และดำเนินการในเรื่องดังต่อไปนี้

(1) กำหนดนโยบายและมาตรฐานเกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลเสนอต่อคณะกรรมการพัฒนารัฐบาลดิจิทัลให้ความเห็นชอบ

(2) ประสานและให้ความช่วยเหลือแก่หน่วยงานของรัฐในการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลระหว่างกัน รวมทั้งกำกับติดตามให้การดำเนินการดังกล่าวเป็นไปในแนวทางและมาตรฐานเดียวกันตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่คณะกรรมการพัฒนารัฐบาลดิจิทัลกำหนด

(3) จัดทำคำอธิบายชุดข้อมูลดิจิทัลของภาครัฐ และจัดเก็บบันทึกหลักฐานของการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล

(4) เรื่องอื่น ๆ ตามที่หน่วยงานมอบหมาย

4. ข้อกำหนดด้านการกำหนดชื่อและเนมสเปซ

การกำหนดเนมสเปซ เป็นข้อกำหนดการออกแบบและพัฒนาการให้บริการข้อมูลผ่าน API ประเภทREST ให้เป็นไปตามมาตรฐานการเชื่อมโยงและการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน ด้านการเชื่อมโยงข้อมูลสำหรับผู้ให้บริการ API (Provider System) เพื่อให้ผู้ใช้บริการ API (Consumer System) สามารถเข้าถึงเข้าถึงทรัพยากรข้อมูล (Data Resource) ที่ให้บริการได้อย่างถูกต้องและปลอดภัย

4.1 การกำหนดเนมสเปซของระบบ

การกำหนดเนมสเปซของระบบ ตามมาตรฐานการเชื่อมโยงและการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานด้านการเชื่อมโยงข้อมูลมีแนวทางดำเนินการ ดังนี้

4.1.1. การกำหนดโครงสร้างของ URI (Uniform Resource Identifier) เป็นการระบุที่อยู่ของทรัพยากรข้อมูล (Data Resource) ที่ให้บริการ โดยการกำหนดโครงสร้าง URI นั้นจะอ้างอิงตามมาตรฐานการกำหนด Uniform Resource Identifier (URI): Generic Syntax (RFC-3986) [1] ซึ่งผู้ให้บริการ API (Provider System) สามารถกำหนดรูปแบบโครงสร้างของ URI และรายละเอียดของแต่ละส่วนแสดง ดังนี้

พารามิเตอร์	รายละเอียด
scheme	เป็นการกำหนด Protocol สำหรับเรียกใช้งาน API เช่น https:// เป็นต้น
authority	เป็นการกำหนด Domain ของผู้ให้บริการตามมาตรฐานที่กำหนด เช่น ow.api.tgix.com เป็นต้น
path: API	เป็นการกำหนดชื่อการให้บริการ เช่น /namespace/project เป็นต้น
path: Version	เป็นการกำหนดเวอร์ชั่นของการให้บริการ เช่น /v1 /v2 เป็นต้น
path: Collections Data Resource	เป็นการกำหนดรูปแบบสำหรับการเข้าถึงชุดข้อมูลหลายรายการพร้อมกัน เช่น การเรียกข้อมูลสินค้าหลายรายการจะกำหนดเป็น /products เป็นต้น
path: Instance Data Resource	เป็นการกำหนดรูปแบบส าหรับการเข้าถึงข้อมูลรายการเดียว เช่น /products/0001 เป็นต้น
query	เป็นการกำหนดเงื่อนไขการเรียกข้อมูล เช่น ?itemname=abc หรือ ?itemname=abc&create_date=2021-10-24 เป็นต้น

4.1.2. การกำหนดรูปแบบชื่อของทรัพยากรข้อมูล (Data Resource) เป็นการกำหนดชื่อของชุดข้อมูลที่ให้บริการ โดยผู้ให้บริการ API (Provider System) สามารถกำหนดรูปแบบชื่อของทรัพยากรข้อมูล (Data Resource) ซึ่งมีแนวทางในการกำหนดดังนี้

(1) ควรเป็นคำนาม ไม่ควรใช้คำกริยาในการอธิบาย

(2) ควรเป็นเอกพจน์สำหรับแบบ Instance Data Resource

(3) ควรเป็นพหูพจน์สำหรับแบบ Collections Data Resource

(4) ควรกำหนดเป็นภาษาอังกฤษเท่านั้น

(5) ควรเป็นตัวพิมพ์เล็ก (Lower-case) และมีเครื่องหมาย - (Hyphen) ในการคั่นคำ

4.1.3. การกำหนดรูปแบบ Query ผู้ให้บริการ API (Provider System) สามารถกำหนดรูปแบบ Query ซึ่งมีแนวทางในการกำหนดดังนี้

(1) ควรใช้ (Underscore) ในการคั่นคำ

(2) ควรเป็นตัวพิมพ์เล็กทั้งหมด (Lower-case)

(3) ควรใช้ในกรณีการจัดเรียงข้อมูล (Sorting) หรือกรองข้อมูล (Filtering) เท่านั้น

(4) ควรกำหนดเป็นภาษาอังกฤษเท่านั้น

(5) ไม่ควรใช้ตัวอักษรที่เป็นข้อมูล Sensitive

4.1.4. การกำหนดเวอร์ชั่นของ API ผู้ให้บริการ API (Provider System) สามารถกำหนดโดยอ้างอิงตามมาตรฐาน Semantic Versioning [2] ซึ่งการปรับเปลี่ยนเวอร์ชั่นจะเปลี่ยนเมื่อมีการอัพเกรดของ API และเป็นการป้องกันการเกิดปัญหาการเรียกใช้บริการโดยไม่แจ้งการเปลี่ยนแปลงล่วงหน้า (Breaking API) โดยเวอร์ชั่นจะกำหนดเป็นส่วนหนึ่งใน URI

บรรณานุกรม

[1] T. Berners-Lee. (2005, มกราคม) Uniform Resource Identifier (URI): Generic Syntax (RFC-3986). [ออนไลน์]. เข้าถึงได้จาก: https://datatracker.ietf.org/doc/html/rfc3986. (วันที่ค้นข้อมูล: 9 กันยายน 2021)

[2] Tom Preston-Werner. Semantic Versioning 2.0.0. (2021). [ออนไลน์]. เข้าถึงได้จาก:https://semver.org/. (วันที่ค้นข้อมูล: 9 กันยายน 2021)

มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน

เรื่อง ข้อกำหนดด้านการตรวจสอบระบบและการลงบันทึกล็อก

1. ขอบข่าย

การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานเป็นพื้นฐานหลักที่จำเป็นต่อการพัฒนารัฐบาลดิจิทัลในปัจจุบันประเทศไทยมีแพลตฟอร์มการแลกเปลี่ยนข้อมูลที่ให้บริการอยู่หลายแห่ง แพลตฟอร์มแต่ละแห่งมีแนวทางและพันธกิจในการดำเนินงานเป็นของตนเอง เป็นผลให้การบูรณาการข้อมูลจำเป็นต้องขับเคลื่อนด้วยการสร้างมาตรฐานหรือข้อตกลงร่วมกันในการแลกเปลี่ยนข้อมูล กรมอนามัยจึงมีความจำเป็นต้องจัดทำมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลเพื่อใช้ในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน เพื่อให้เกิดการบูรณาการข้อมูลเกิดขึ้นอย่างเป็นรูปธรรม

เป้าประสงค์หลักของการใช้มาตรฐานฯ เป็นตัวขับเคลื่อนการบูรณาการข้อมูลหน่วยงาน คือ การให้หน่วยงานมีแนวทางในการพัฒนาสถาปัตยกรรมระบบสารสนเทศเพื่อใช้ในการแลกเปลี่ยนข้อมูลที่ชัดเจนมีความสอดคล้องในการเชื่อมต่อระหว่างกัน

ดังนั้นเพื่อให้บรรลุเป้าประสงค์หลักดังกล่าวจึงมีาเสนอข้อกำหนดด้านการาหนดด้านการตรวจสอบระบบและการลงบันทึกล็อก สำหรับทำมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน เรื่องมาตรฐานสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐระดับการเชื่อมโยงข้อมูลที่เหมาะสมกับบริบทของกรมอนามัยเท่านั้น

2. นิยาม

นิยามคำศัพท์ที่เกี่ยวข้องกับมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน เรื่อง ข้อกำหนดด้านการตรวจสอบระบบและการลงบันทึกล็อกที่ใช้ในเอกสารฉบับนี้มีดังนี้

2.1 ผู้ให้บริการ API (Provider System) หมายความว่า ระบบสารสนเทศของหน่วยงานที่เปิดให้บริการ API สำหรับให้บริการข้อมูลผ่านแพลตฟอร์มกลางการแลกเปลี่ยนข้อมูล

2.2 ผู้ใช้บริการ API (Consumer System) หมายความว่า ระบบสารสนเทศของหน่วยงานที่เรียกใช้บริการ API สำหรับใช้บริการข้อมูลผ่านแพลตฟอร์มกลางการแลกเปลี่ยนข้อมูล

2.3 การบันทึกล็อก (Logging) หมายความว่า การบันทึกข้อมูลที่ใช้ในการรับส่งระหว่างผู้ให้บริการและผู้ใช้บริการจากระบบเทคโนโลยีสารสนเทศที่ใช้งาน

2.4 ศูนย์ปฏิบัติการและให้บริการ (Service Operation Center: SOC) หมายความว่า ระบบสารสนเทศของผู้ให้บริการแพลตฟอร์มแลกเปลี่ยนข้อมูลสำหรับ เพื่อใช้ในการบริหารจัดการและกำกับดูแลการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างผู้ให้บริการและผู้ใช้บริการ

2.5 การติดตาม (Monitoring) หมายความว่า การนำข้อมูลเชิงเทคนิค และเชิงธุรกรรมที่บันทึกไว้มาประมวลผล เพื่อปรับปรุงและตรวจสอบ

3. กฎหมายและแนวปฏิบัติที่เกี่ยวข้อง

การเชื่อมโยงและการแลกเปลี่ยนข้อมูลภาครัฐมีการบัญญัติไว้ในกฎหมายหรือแนวปฏิบัติที่เกี่ยวข้อง ดังนี้

3.1 รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 ในมาตรา 59 ระบุว่ารัฐต้องเปิดเผยข้อมูลหรือข่าวสารสาธารณะในครอบครองของหน่วยงานของรัฐที่มิใช่ข้อมูลเกี่ยวกับความมั่นคงของรัฐหรือเป็นความลับของทางราชการตามที่กฎหมายบัญญัติ และต้องจัดให้ประชาชนเข้าถึงข้อมูลหรือข่าวสารดังกล่าวได้โดยสะดวก

3.2 พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 ในมาตรา 13 ระบุว่าเพื่อประโยชน์ในการบริหารราชการแผ่นดินและการให้บริการประชาชนให้หน่วยงานของรัฐจัดให้มีการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลที่มีการจัดทำและครอบครองตามที่หน่วยงานของรัฐแห่งอื่นร้องขอที่จะเกิดการบูรณาการร่วมกันมาตรา 15 ระบุว่าให้มีศูนย์แลกเปลี่ยนข้อมูลกลางทำหน้าที่เป็นศูนย์กลางในการแลกเปลี่ยนข้อมูลดิจิทัลและทะเบียนดิจิทัลระหว่างหน่วยงานของรัฐ เพื่อสนับสนุนการดำเนินการของหน่วยงานของรัฐในการให้บริการประชาชนผ่านระบบดิจิทัล และดำเนินการในเรื่องดังต่อไปนี้

(1) กำหนดนโยบายและมาตรฐานเกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลเสนอต่อคณะกรรมการพัฒนารัฐบาลดิจิทัลให้ความเห็นชอบ

(2) ประสานและให้ความช่วยเหลือแก่หน่วยงานของรัฐในการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลระหว่างกัน รวมทั้งกำกับติดตามให้การดำเนินการดังกล่าวเป็นไปในแนวทางและมาตรฐานเดียวกันตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่คณะกรรมการพัฒนารัฐบาลดิจิทัลกำหนด

(3) จัดทำคำอธิบายชุดข้อมูลดิจิทัลของภาครัฐ และจัดเก็บบันทึกหลักฐานของการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล

(4) เรื่องอื่น ๆ ตามที่หน่วยงานมอบหมาย

4. ข้อกำหนดด้านการตรวจสอบระบบและการลงบันทึกล็อก

มาตรฐานสถาปัตยกรรมดำเนินการเชื่อมโยงและการแลกเปลี่ยนข้อมูลภาครัฐ มีส่วนประกอบหลักแยกตามบทบาทและหน้าที่ภายในกลุ่มได้แก่ ผู้ให้บริการ API (Provider System) ผู้ใช้บริการ API (Consumer System) และผู้ให้บริการ Platform (Platform Provider) ทุกส่วนประกอบหลักทำงานร่วมกันบนเครือข่ายอินเทอร์เน็ตหรือเครือข่ายเฉพาะที่หน่วยงานใช้เชื่อมโยงและแลกเปลี่ยนข้อมูล

4.1. การบันทึกล็อก (Logging)

การบันทึกล็อก (Logging) เป็นองค์ประกอบสำคัญของสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ซึ่งการบันทึกล็อก (Logging) มีวัตถุประสงค์ได้หลายอย่าง เช่น ไว้สำหรับการตรวจสอบทางกฎหมาย การตรวจสอบข้อผิดพลาดของระบบ หรือไว้ใช้สำหรับการบันทึกข้อมูลที่ใช้รับส่งระหว่างผู้ให้บริการกับผู้ใช้บริการ

4.1.1. บันทึกข้อมูลเชิงเทคนิค (Technical logs)

การบันทึกข้อมูลเชิงเทคนิค จะบันทึกข้อมูลในส่วนของ Message Header และใช้ส่งข้อมูลการเชื่อมโยงไปยัง Service Operation Center (SOC) โดยกำหนดการส่งข้อมูลการเชื่อมโยงอย่างน้อยชั่วโมงละ 1 ครั้ง รายละเอียดข้อมูลที่จำเป็นต้องเก็บในส่วนของข้อมูลเชิงเทคนิค ดังนี้

พารามิเตอร์	รายละเอียด	ผู้ให้บริการ	ผู้ใช้บริการ	SOC	Service Gateway
messageVersion	เวอร์ชั่นของ API	✓	✓	✓	✓
messageId	รหัสของข้อความ	✓	✓	✓	✓
timestamp	เวลาในการร้องขอ	✓	✓	✓	✓
clientId	รหัสของผู้ใช้บริการ	✓	✓	✓	✓
event	รายละเอียดการที่จะดำเนินการ (Action)	✓	✓	✓	✓
requestId	รหัสของการผู้ใช้บริการสำหรับตอบกลับ	✓	✓	✓	✓
messageStatus	สถานะของข้อความ	✓	✓	✓	✓
errorCode	รหัสของ Error	✓	✓		
errorMessage	ข้อความที่ต้องการแสดง Error	✓	✓		
processingTime	เวลาที่ใช้ในการร้องขอข้อมูล	✓	✓		

อ้างอิงตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 [1] จะต้องระบุวัน เวลา ข้อมูลที่สามารถระบุตัวผู้ใช้บริการได้และหมายเลขข้อมูลต้นทาง ปลายทาง เพื่อไว้ใช้ตรวจสอบได้กำหนดให้บันทึกทุกกิจกรรมการพยายามยืนยันตัวตนที่ล้มเหลว การปฏิเสธการเข้าถึง และการตรวจสอบข้อมูลนำเข้าที่ไม่ถูกต้อง

บันทึกควรอยู่ในรูปแบบที่สามารถนำเข้าระบบจัดการบันทึกล็อค (Log Management) ได้ง่าย ควรมีข้อมูลเพียงพอต่อการระบุผู้กระทำที่น่าสงสัย และเป็นไปตามหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564 [2]

4.1.2. บันทึกข้อมูลเชิงธุรกรรม (Transaction logs)

การบันทึกข้อมูลเชิงธุรกรรม จะใช้บันทึกข้อมูลในส่วนของ payload โดยกำหนดให้บันทึกแค่เนื้อหาข้อมูล ซึ่งทำให้สามารถตรวจสอบเนื้อหาข้อมูลได้ในภายหลัง ข้อความจะถูกจัดเก็บไว้ในฐานข้อมูลเป็นเวลา 90 วันหรือมากกว่านั้น จนกว่าจะลบออกโดยอัตโนมัติ ซึ่งต้องสามารถตั้งค่าของช่วงเวลาการเก็บข้อมูลผ่านไฟล์ที่ใช้กำหนดค่าเริ่มต้นต่างๆ (Configuration file)

พารามิเตอร์	รายะเอียด	ผู้ให้บริการ	ผู้ใช้บริการ	SOC	Service Gateway
messageVersion	เวอร์ชั่นของ API	✓	✓		
messageId	รหัสของข้อความ	✓	✓		
timestamp	เวลาในการร้องขอ	✓	✓		
clientId	รหัสของผู้ใช้บริการ	✓	✓		
PayloadData	เพย์โหลด	✓	✓		

4.1.3. หลักเกณฑ์การการบันทึกล็อก (Logging)

(1) ข้อมูลต้องเป็นความลับ ให้เฉพาะผู้มีสิทธิ์เข้าถึงข้อมูลได้เท่านั้น เช่น กรณีบันทึกล็อกในฐานข้อมูลจะต้องกำหนดสิทธิ์ให้ได้แค่เฉพาะอ่านเท่านั้น ไม่สามารถแก้ไขได้

(2) ข้อมูลต้องถูกต้องและสมบูรณ์ ต้องไม่มีการแก้ไขหรือเพิ่มเติมข้อมูลโดยไม่ได้รับอนุญาต

(3) ข้อมูลต้องพร้อมใช้งานตลอดเวลา เพื่อบ่งบอกประสิทธิภาพ ความน่าเชื่อถือของการทำงานและสามารถนำมาวิเคราะห์สาเหตุของปัญหาได้ทันที

4.2. การติดตาม (Monitoring)

การติดตาม (Monitoring) เป็นองค์ประกอบสำคัญของสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ เช่นเดียวกับการบันทึกล็อก โดยการติดตามด้านการปฏิบัติงานจะใช้ข้อมูลจากการบันทึกข้อมูลเชิงเทคนิค และบันทึกข้อมูลเชิงธุรกรรม มาติดตามสถิติการปฏิบัติงาน เช่น จำนวนครั้งของบริการที่ถูกเรียกใช้ ค่าเฉลี่ยของเวลาตอบสนอง แนวทางการดำเนินการการติดตาม (Monitoring) สามารถเลือกได้จากทางเลือกต่อไปนี้

(1) พัฒนาด้วยภาษาโปรแกรมของ Provider System

(2) ใช้เครื่องมือ API Gateway Monitoring เช่น Kong, 3Scale, Apigee เป็นต้น

(3) ใช้ Monitoring Solution อื่น ๆ ที่เป็นที่นิยม เช่น Prometheus Grafana, ELK Stack

4.3. สรุปการบันทึกล็อก (Logging) และการติดตาม (Monitoring)

แยกตามส่วนประกอบของมาตรฐานสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐประเภทต่าง ๆ ซึ่งรายละเอียดการบันทึกล็อก (Logging) ข้อ 4.1 และการติดตาม (Monitoring) ข้อ 4.2

บรรณานุกรม

[1] สำนักงานคณะกรรมการกฤษฎีกา. (2017, มกราคม). พระราชบัญญัติว่าด้วยการกระท าความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. ๒๕๖๐. [ออนไลน์]. เข้าถึงได้จาก: http://web.krisdika.go.th/data/law/law2/%C771/%C771-20-2560-a0001.pdf. (วันที่ค้นข้อมูล: 9 กันยายน 2021)

[2] ราชกิจจานุเบกษา. (2021, สิงหาคม). หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๖๔. [ออนไลน์]. เข้าถึงได้จาก: http://www.ratchakitcha.soc.go.th/DATA/PDF/2564/E/188/T_0009.PDF. (วันที่ค้นข้อมูล: 9 กันยายน 2021)

มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน

เรื่อง ข้อกำหนดด้านการยืนยันตัวตน การควบคุมสิทธิ์และบัญชีการใช้งาน

1. ขอบข่าย

การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานเป็นพื้นฐานหลักที่จำเป็นต่อการพัฒนารัฐบาลดิจิทัลในปัจจุบันประเทศไทยมีแพลตฟอร์มการแลกเปลี่ยนข้อมูลที่ให้บริการอยู่หลายแห่ง แพลตฟอร์มแต่ละแห่งมีแนวทางและพันธกิจในการดำเนินงานเป็นของตนเอง เป็นผลให้การบูรณาการข้อมูลจำเป็นต้องขับเคลื่อนด้วยการสร้างมาตรฐานหรือข้อตกลงร่วมกันในการแลกเปลี่ยนข้อมูล กรมอนามัยจึงมีความจำเป็นต้องจัดทำมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลเพื่อใช้ในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน เพื่อให้เกิดการบูรณาการข้อมูลเกิดขึ้นอย่างเป็นรูปธรรม

เป้าประสงค์หลักของการใช้มาตรฐานฯ เป็นตัวขับเคลื่อนการบูรณาการข้อมูลหน่วยงาน คือ การให้หน่วยงานมีแนวทางในการพัฒนาสถาปัตยกรรมระบบสารสนเทศเพื่อใช้ในการแลกเปลี่ยนข้อมูลที่ชัดเจนมีความสอดคล้องในการเชื่อมต่อระหว่างกัน

ดังนั้นเพื่อให้บรรลุเป้าประสงค์หลักดังกล่าวจึงมีเสนอข้อกำหนดด้านการยืนยันตัวตน การควบคุมสิทธิ์และบัญชีการใช้งานสำหรับทำมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน เรื่องมาตรฐานสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐระดับการเชื่อมโยงข้อมูลที่เหมาะสมกับบริบทของกรมอนามัยเท่านั้น

2. นิยาม

นิยามคำศัพท์ที่เกี่ยวข้องกับมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน เรื่อง ข้อกำหนดด้านการยืนยันตัวตน การควบคุมสิทธิ์และบัญชีการใช้งานที่ใช้ในเอกสารฉบับนี้มีดังนี้

2.1 ผู้ให้บริการ API (Provider System) หมายความว่า ระบบสารสนเทศของหน่วยงานที่เปิดให้บริการ API สำหรับให้บริการข้อมูลผ่านแพลตฟอร์มกลางการแลกเปลี่ยนข้อมูล

2.2 ผู้ใช้บริการ API (Consumer System) หมายความว่า ระบบสารสนเทศของหน่วยงานที่เรียกใช้บริการ API สำหรับใช้บริการข้อมูลผ่านแพลตฟอร์มกลางการแลกเปลี่ยนข้อมูล

2.3 การบันทึกล็อก (Logging) หมายความว่า การบันทึกข้อมูลที่ใช้ในการรับส่งระหว่างผู้ให้บริการและผู้ใช้บริการจากระบบเทคโนโลยีสารสนเทศที่ใช้งาน

2.4 ศูนย์ปฏิบัติการและให้บริการ (Service Operation Center: SOC) หมายความว่า ระบบสารสนเทศของผู้ให้บริการแพลตฟอร์มแลกเปลี่ยนข้อมูลสำหรับ เพื่อใช้ในการบริหารจัดการและกำกับดูแลการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างผู้ให้บริการและผู้ใช้บริการ

2.5 การติดตาม (Monitoring) หมายความว่า การนำข้อมูลเชิงเทคนิค และเชิงธุรกรรมที่บันทึกไว้มาประมวลผล เพื่อปรับปรุงและตรวจสอบ

3. กฎหมายและแนวปฏิบัติที่เกี่ยวข้อง

การเชื่อมโยงและการแลกเปลี่ยนข้อมูลภาครัฐมีการบัญญัติไว้ในกฎหมายหรือแนวปฏิบัติที่เกี่ยวข้อง ดังนี้

3.1 รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 ในมาตรา 59 ระบุว่ารัฐต้องเปิดเผยข้อมูลหรือข่าวสารสาธารณะในครอบครองของหน่วยงานของรัฐที่มิใช่ข้อมูลเกี่ยวกับความมั่นคงของรัฐหรือเป็นความลับของทางราชการตามที่กฎหมายบัญญัติ และต้องจัดให้ประชาชนเข้าถึงข้อมูลหรือข่าวสารดังกล่าวได้โดยสะดวก

3.2 พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 ในมาตรา 13 ระบุว่าเพื่อประโยชน์ในการบริหารราชการแผ่นดินและการให้บริการประชาชนให้หน่วยงานของรัฐจัดให้มีการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลที่มีการจัดทำและครอบครองตามที่หน่วยงานของรัฐแห่งอื่นร้องขอที่จะเกิดการบูรณาการร่วมกันมาตรา 15 ระบุว่าให้มีศูนย์แลกเปลี่ยนข้อมูลกลางทำหน้าที่เป็นศูนย์กลางในการแลกเปลี่ยนข้อมูลดิจิทัลและทะเบียนดิจิทัลระหว่างหน่วยงานของรัฐ เพื่อสนับสนุนการดำเนินการของหน่วยงานของรัฐในการให้บริการประชาชนผ่านระบบดิจิทัล และดำเนินการในเรื่องดังต่อไปนี้

(1) กำหนดนโยบายและมาตรฐานเกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลเสนอต่อคณะกรรมการพัฒนารัฐบาลดิจิทัลให้ความเห็นชอบ

(2) ประสานและให้ความช่วยเหลือแก่หน่วยงานของรัฐในการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลระหว่างกัน รวมทั้งกำกับติดตามให้การดำเนินการดังกล่าวเป็นไปในแนวทางและมาตรฐานเดียวกันตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่คณะกรรมการพัฒนารัฐบาลดิจิทัลกำหนด

(3) จัดทำคำอธิบายชุดข้อมูลดิจิทัลของภาครัฐ และจัดเก็บบันทึกหลักฐานของการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล

(4) เรื่องอื่น ๆ ตามที่หน่วยงานมอบหมาย

4. ข้อกำหนดด้านการยืนยันตัวตน การควบคุมสิทธิ์และบัญชีการใช้งาน

การยืนยันตัวตน (Authentication) การควบคุมสิทธิ์ (Access Control) และบัญชีการใช้งาน (Accounting) เป็นองค์ประกอบสำคัญของสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน องค์ประกอบเหล่านี้ช่วยให้ผู้ให้บริการ API (Provider System) และผู้ใช้บริการ API (Consumer System) เชื่อมโยงและแลกเปลี่ยนข้อมูลได้อย่างปลอดภัย

4.1. การยืนยันตัวตน (Authentication)

การยืนยันตัวตนเพื่อขอใช้บริการการแลกเปลี่ยนข้อมูล หมายถึง กระบวนการที่ผู้ใช้บริการ API (Consumer System) ทำการยืนยันตัวตนเพื่อขอใช้บริการ API ของผู้ให้บริการ API (Provider System) ที่เป็น REST API ซึ่งแนวทางในการยืนยันตัวตน สามารถแบ่งได้เป็น 3 วิธี คือ API Key, OAuth 2.0 และ Open ID Connect

4.2. การยืนยันตัวตนด้วย API Key

API Key ใช้เพื่อยืนยันว่าผู้ใช้บริการ API (Consumer System) ต้องการขอเข้าถึง API แบบ REST API ของผู้ให้บริการ API (Provider System) แต่ไม่ได้ต้องการการยืนยันตัวระดับตัวบุคคลที่ใช้งานในระบบของ ผู้ใช้บริการ API (Consumer System) ดังนั้น ในด้านความปลอดภัยจะเพียงพอสำหรับการเข้าถึง API ที่เป็นบริการ API ทั่วไปในหน่วยงานของผู้ให้บริการ API (Provider System) โดยข้อมูลเหล่านั้นสามารถเข้าถึงด้วย API โดยที่ไม่ต้องยืนยันตัวตนระดับบุคคล

ในด้านเทคนิคนั้น API Key เป็นค่าที่สร้างขึ้นแบบไม่ซ้ำกันโดยผู้ให้บริการ API (Provider System) แล้วส่งมอบให้ผู้ใช้บริการ API (Consumer System) เก็บไว้ใช้ในการยืนยันตัวตนระหว่างเรียกใช้งาน REST API ของผู้ให้บริการ API (Provider System)

ผู้ให้บริการ API (Provider System) และผู้ใช้บริการ API (Consumer System) มีขั้นตอนการดำเนินการดังต่อไปนี้

4.2.1 ขั้นตอนที่ 1: การสร้าง API Key (Create API Key)

ในขั้นตอนนี้ ผู้ให้บริการ API (Provider System) ต้องดำเนินการสร้าง API Key ซึ่งในแต่ละ API นั้น ผู้ให้บริการ API (Provider System) ต้องดำเนินการสร้าง API Key ให้มีค่าไม่ซ้ำกัน โดยวิธีการที่แนะนำ คือ การสุ่มด้วยวิธีการ Secure Random จากภาษาโปรแกรมที่ใช้พัฒนาระบบ เช่น โปรแกรมภาษา Java

หลังจากได้ค่า API Key แล้ว ผู้ให้บริการ API (Provider System) ควรเก็บรักษา API Key ไว้ในที่ปลอดภัย เช่น เก็บไว้ในฐานข้อมูลโดยท าการใส่ Prefix และ Hash ค่าของ API Key ด้วยภาษาโปรแกรมที่ใช้พัฒนาระบบ

นอกจากนี้ ผู้ให้บริการ API (Provider System) ควรระบุได้ว่ามีการส่งมอบ API Key ให้กับผู้ใช้บริการ API (Consumer System) ใดแล้วบ้าง พร้อมทั้งมีการกำหนดวันหมดอายุของ API Key สามารถกำหนดค่าตั้งต้นให้ไม่มีวันหมดอายุ แต่ควรสามารถปรับเปลี่ยนให้มีวันหมดอายุตามความเหมาะสมของ API ได้นอกจากนี้ ควรสร้าง API Key ได้ใหม่เมื่อมีการร้องขอจากผู้ใช้บริการ API (Consumer System)

4.2.2 ขั้นตอนที่ 2: การส่งมอบ API Key (Send API Key)

ในขั้นตอนนี้ ผู้ให้บริการ API (Provider System) ต้องด าเนินการส่งมอบ API Key ให้กับผู้ใช้บริการ API (Consumer System) ซึ่งการส่งมอบ API Key นั้น เกิดขึ้นหลังจากผู้ให้บริการ API (Provider System) ท าข้อตกลงเพื่อใช้บริการ API (Service Agreement) กับผู้ใช้บริการ API (Consumer System) ที่ Service Operation Center ซึ่งดูแลโดยหน่วยงานผู้บริการ Platformเรียบร้อยแล้ว โดยมีรายละเอียดตามมาตรฐานสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน ซึ่งผู้ให้บริการ API (Provider System) สามารถเลือกดำเนินการส่ง API Key ผ่านช่องทางต่าง ๆ ได้ตามความเหมาะสมและงบประมาณของหน่วยงาน เช่น

- ส่งผ่านอีเมล
- สร้าง API สำหรับส่ง API Key
- พัฒนาหน้าจอสำหรับให้ผู้ใช้บริการ API (Consumer System) มารับ API Key

4.2.3 ขั้นตอนที่ 3: การเก็บรักษา API Key (Store API Key)

ในขั้นตอนนี้ ผู้ใช้บริการ API (Consumer System) ต้องดำเนินการเก็บรักษา API Key ซึ่งหลังจากได้รับมอบ API Key แล้วนั้น ผู้ใช้บริการ API (Consumer System) ควรเก็บรักษา API Key ไว้ในที่ปลอดภัย ไม่ควรกำหนด API Key ไว้ใน Source Code ซึ่งอาจจะเกิดความผิดพลาดขณะแชร์ Source Code ให้กับบุคคลอื่นได้ ผู้ใช้บริการ API (Consumer System) ควรเก็บ API Key ไว้ใน Environment Variable หรือ File หรือที่อื่น ๆ ที่ไม่อยู่ใน Source Code หลักรวมทั้งทำการ Hash ของข้อมูล API Key ก่อนเก็บเสมอ

4.2.4 ขั้นตอนที่ 4: การยืนยันตัวตนและเรียก API ด้วย API Key (Call REST API with API Key)

ในขั้นตอนนี้ ผู้ใช้บริการ API (Consumer System) ต้องด าเนินการการยืนยันตัวตนเพื่อเรียกใช้บริการ REST API ด้วย API Key ดังรูปที ่ 2 ซึ่งเกิดขึ้นเมื่อได้รับ API Key แล้วผู้ใช้บริการ API (Consumer System) จะต้องดำเนินการส่งข้อมูล API Key เพื่อยืนยันตัวตนระหว่างเรียกใช้บริการ REST API ไปยังผู้ให้บริการ API (Provider System) โดยผู้ใช้บริการ API (Consumer System) สามารถดำเนินการตามที่ได้ตกลงไว้กับผู้ให้บริการ API (Provider System) จากวิธีต่อไปนี้

(1) ส่งข้อมูล API Key เป็นส่วนหนึ่งของ Authorization Header ขณะเรียกใช้ REST API
(2) ส่งข้อมูล API Key เป็นส่วนหนึ่งของ Basic Authentication ของ REST API
(3) ส่งข้อมูล API Key เป็นส่วนหนึ่งของ Body Data ขณะเรียกใช้ REST API
(4) ส่งข้อมูล API Key เป็นส่วนหนึ่งของ Query String ขณะเรียกใช้ REST API

4.2.5 ขั้นตอนที่ 5: การตรวจสอบความถูกต้องของ API Key (Validate API Key)

ในขั้นตอนนี้ ผู้ให้บริการ API (Provider System) ต้องดำเนินการตรวจสอบความถูกต้องของ API Key ซึ่งเกิดขึ้นเมื่อผู้ให้บริการ API (Provider System) ได้รับการขอใช้บริการ API พร้อมด้วย API Key หลังจากนั้น ผู้ให้บริการ API (Provider System) ต้องดำเนินการตรวจสอบความถูกต้องแล้วด าเนินการให้บริการ API ตามข้อมูลที่ถูกร้องขอหรือปฏิเสธการให้บริการหาก API Key ไม่ถูกต้อง ซึ่งขั้นตอนนี้ผู้ให้บริการ API สามารถดำเนินการได้ตามความเหมาะสมของภาษาโปรแกรมที่ใช้พัฒนาระบบ

4.2.6 ขั้นตอนที่ 6: การตอบกลับผลการให้บริการ API (Return Data)

ในขั้นตอนนี้ ผู้ให้บริการ API (Provider System) ต้องดำเนินการตอบกลับผลการให้บริการ API ซึ่งเกิดขึ้นเมื่อผู้ให้บริการ API (Provider System) ตรวจสอบความถูกต้องของ API Key แล้วดำเนินการให้บริการ API ตามข้อมูลที่ถูกร้องขอสำเร็จ ควรตอบกลับด้วย HTTP Code 200 ตามตัวอย่างนี้ หรือ HTTP Code อื่น ๆ ตามความเหมาะสม กรณีต้องการปฏิเสธการให้บริการ เนื่องจาก API Key ไม่ถูกต้อง ควรตอบกลับด้วย HTTP Code 401

4.3. การยืนยันตัวตนด้วยมาตรฐาน OAuth 2.0

OAuth 2.0 เป็นการรวมกระบวนการยืนยันตัวตนและจัดการสิทธิ์ให้เข้าถึงข้อมูลเข้าด้วยกัน ตามมาตรฐาน The OAuth 2.0 Authorization Framework: Bearer Token Usage: RFC-6749 [1], RFC-6750 [2] มาตรฐานOAuth 2.0 สามารถใช้ยืนยันตัวตนระดับผู้ใช้งานระบบได้ ดังนั้นจึงเหมาะสมในการเข้าถึง API ที่เป็นบริการเข้าถึงข้อมูลส่วนบุคคลหรือข้อมูลสำคัญของผู้ให้บริการ API (Provider System) รวมทั้ง API เชิงธุรกรรมประเภทที่เป็นการสร้าง ลบหรือแก้ไขข้อมูล โดยหลักการของ OAuth 2.0 จะเป็นการยืนยันตัวตนผู้ใช้งานในระบบ (End User) ของผู้ใช้บริการ API (Consumer System) กับระบบพิสูจน์และยืนยันตัวตน (Identity Provider) ที่รองรับ OAuth 2.0 เพื่อให้ได้ Access Token ซึ่งกระบวนการดังกล่าวเรียกว่าการยืนยันตัวตนและให้สิทธิ์ (Grant Type) หลังจาก ผู้ใช้บริการ API (Consumer System) ได้รับ Access Token แล้วจะนามาใช้ในการเข้าถึง API ของผู้ให้บริการ API (Provider System)

4.3.1 ขั้นตอนที่ 1 การลงทะเบียนบัญชีผู้ใช้งาน (Register User Account)

ในขั้นตอนนี้ผู้ให้บริการ API (Provider System) และผู้ใช้บริการ API (Consumer System) ดำเนินการแจ้งความประสงค์ขอลงทะเบียนบัญชีใช้งานที่ผู้พิสูจน์และยืนยันตัวตน (Identity Provider) ซึ่งดูแลโดยหน่วยงานผู้บริการ

Platform ขั้นตอนนี้จะเกิดขึ้นหลังจากที่ผู้ให้บริการ API (Provider System) และผู้ใช้บริการ API (Consumer System) ท า ข้อตกลงเพื่อใช้บริการ API (Service Agreement) ไว้ที่ Service Operation Center เรียบร้อยแล้ว

วิธีดำเนินการในขั้นตอนนี้ขึ้นอยู่กับ Identity Provider และหน่วยงานผู้บริการ Platform ตกลงกันเลือกใช้ดำเนินการเพื่อบริหารจัดการบัญชีผู้ใช้งาน

4.3.2 ขั้นตอนที่ 2: การยืนยันตัวตนเพื่อให้ได้ Access Token (Implement Grant Type)

ขั้นตอนนี้ผู้ใช้บริการ API (Consumer System) ต้องดำเนินการยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตน (Identity Provider) เพื่อให้ได้ Access Token ซึ่งในมาตรฐาน OAuth 2.0 มีประเภทการยืนยันตัวตนและให้สิทธิ์ (Grant Type) ซึ่งผู้ใช้บริการ API (Consumer System) สามารถเลือกดำเนินการได้ตามความเหมาะสมของภาษาโปรแกรมที่ใช้พัฒนาและงบประมาณที่มีโดยเลือกได้จาก 4 ประเภท ได้แก่

(1) การยืนยันตัวตนและให้สิทธิ์ (Grant Type) ประเภท Authorization Code Authorization Code เป็น Grant type ประเภทที่ผู้ใช้บริการ API (Consumer System) ยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตน (Identity Provider) โดยน า Authorization Code มาแลกเปลี่ยนเป็น Access Token

(2) การยืนยันตัวตนและให้สิทธิ์ (Grant Type) ประเภท Implicit Implicit จะมีความคล้ายกับแบบ Authorization Code แต่ต่างกันที่ผู้ใช้บริการ API (Consumer System) ไม่ต้องดำเนินการส่ง Authorization Code แล้วไปขอ Access Token อีกที แต่จะได้ Access Token กลับมาผ่านทาง Query String จากผู้พิสูจน์และยืนยันตัวตน (Identity Provider) ในคราวเดียว

(3) การยืนยันตัวตนและให้สิทธิ์ (Grant Type) ประเภท Resource Owner Passwordเป็นการยืนยันตัวตนและขอสิทธิ์โดย ผู้ใช้งานระบบของผู้ใช้บริการ API (Consumer System) จะให้ Username และ Password กับผู้ใช้บริการ API (Consumer System) โดยตรง เพื่อนำไปขอ Access Token จากผู้พิสูจน์และยืนยันตัวตน (Identity Provider)

(4) การยืนยันตัวตนและให้สิทธิ์ (Grant Type) ประเภท Client Credentials เป็นการยืนยันตัวตนและขอสิทธิ์โดยผู้ใช้บริการ API (Consumer System) จะใช้ Client ID และ Client Secret ในการส่งไปขอ Access Token ที่ผู้พิสูจน์และยืนยันตัวตน (Identity Provider) โดยจะเป็นการขอระหว่าง Server ไปยัง Server โดยตรง

เมื่อผู้ใช้บริการ API (Consumer System) ด าเนินการเสร็จเรียบร้อย ผลลัพธ์ที่ผู้ใช้บริการ API (Consumer System) ได้รับคือ Access Token ที่ได้รับการเข้ารหัสด้วย JSON Web Tokens (JWT) เพื่อใช้ส่งให้กับผู้ให้บริการ API (Provider System) ในขณะเรียกใช้บริการ REST API ของผู้ให้บริการ API (Provider System)

การดำเนินการแบบละเอียดเกี่ยวกับ JSON Web Tokens (JWT) มีรายละเอียดในเอกสารมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน เรื่องข้อกำหนดด้านโปรโตคอลระดับแอบพลิเคชันเอนพอยน์และการจัดการโทเคนและเซสชัน

4.3.3 ขั้นตอนที่ 3: การเรียกใช้REST API ด้วย Access Token (Call API with Access Token)

ขั้นตอนนี้ ผู้ใช้บริการ API (Consumer System) ต้องดำเนินการเรียกใช้บริการ REST API ของผู้ให้บริการ API (Provider System) ด้วย Access Token ซึ่งขั้นตอนนี้เกิดขึ้นหลังจากที่ผู้ใช้บริการ API (Consumer System) ได้รับ Access Token จากผู้พิสูจน์และยืนยันตัวตน (Identity Provider) แล้วผู้ใช้บริการ API (Consumer System) สามารถนำ Access Token มาประกอบเป็นส่วนหนึ่งของ HTTP Authorization Request Header เพื่อเรียกใช้บริการ REST API จากผู้ให้บริการ API (Provider System)

4.3.4 ขั้นตอนที่ 4: การตรวจสอบความถูกต้องของ Access Token (Validate Access Token)

ขั้นตอนนี้ผู้ให้บริการ API (Provider System) ต้องดำเนินการตรวจสอบความถูกต้องของ Access Token ว่าเป็น Access Token ที่ออกจากผู้พิสูจน์และยืนยันตัวตน (Identity Provider) และเป็น Access Token ที่ไม่หมดอายุ แล้วดำเนินการให้บริการ API ตามที่ถูกร้องขอเมื่อ Access Token ถูกต้อง ซึ่งการตรวจสอบ Access Token มีรายละเอียดในเอกสารมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน เรื่องข้อกำหนดด้านโปรโตคอลระดับแอบพลิเคชันเอนพอยน์และการจัดการโทเคนและเซสชัน

4.3.5 ขั้นตอนที่ 5: การตอบกลับผลการให้บริการ API (Return Data)

เมื่อผู้ให้บริการ API (Provider System) ตรวจสอบความถูกต้องของ Access Token แล้วดำเนินการให้บริการ API ตามข้อมูลที่ถูกร้องขอสำเร็จควรตอบกลับด้วย HTTP Code 200 ตามตัวอย่างนี้ หรือ HTTP Code อื่น ๆ ตามความเหมาะสม

4.4. ขั้นตอนการดำเนินการเพื่อยืนยันตัวตนด้วยมาตรฐาน Open ID Connect

Open ID Connect (OIDC) เป็นมาตรฐานการยืนยันตัวตนที่ทำงานอยู่บนมาตรฐาน OAuth 2.0 โดยมีจุดเด่น คือ การให้ระบบงานใช้ยืนยันตัวตนของผู้ใช้งานเพียงครั้งเดียวแล้วสามารถเข้าไปใช้งานระบบอื่น ๆ ได้หลายระบบ (Single Sign On) พร้อมทั้งสามารถบริหารจัดการข้อมูลผู้ใช้งานโดยใช้ผู้พิสูจน์และยืนยันตัวตน (Identity Provider) ที่รองรับมาตรฐาน Open ID Connect ในขณะที่มาตรฐาน OAuth 2.0 จะเน้นการยืนยันตัวตนเพื่อให้สิทธิ์ในการเข้าถึงทรัพยากรต่าง ๆ เช่น API เป็นต้น

ดังนั้น ผู้ให้บริการ API (Provider System) และผู้ใช้บริการ API (Consumer System) ที่ใช้มาตรฐานแล้วมีความต้องการยืนยันตัวตนผู้ใช้งานเพียงครั้งเดียวแล้วสามารถเข้าไปใช้งานระบบของหน่วยงานอื่น ๆ ในกลุ่มได้หลายระบบ (Single Sign On) สามารถเลือกยืนยันตัวตนสำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลผ่าน API ด้วยผู้พิสูจน์และยืนยันตัวตน (Identity Provider) ที่รองรับมาตรฐาน Open ID Connect ด้วยเช่นกัน ซึ่งมีขั้นตอนการดำเนินการเดียวกันกับที่ใช้ในมาตรฐาน OAuth 2.0 ตามที่กล่าวในหัวข้อก่อนหน้านี้

สิ่งที่แตกต่างกับมาตรฐาน OAuth 2.0 ที่เพิ่มขึ้นมาในมาตรฐาน Open ID Connect คือผู้ให้บริการ API (Provider System) และผู้ใช้บริการ API (Consumer System) สามารถเรียกดูข้อมูลพื้นฐานของผู้ใช้งานด้วย ID Token ซึ่งเป็น Token ที่ผ่านการเข้ารหัสด้วย JSON Web Tokens (JWT) ทั้งนี้ขึ้นอยู่กับ ผู้พิสูจน์และยืนยันตัวตน (Identity Provider ที่ใช้ดำเนินการ เช่น ID Token ที่เข้ารหัสด้วย JSON Web Token (JWT) ของ Microsoft Identity Platform [7]

การเข้ารหัสด้วย JSON Web Token (JWT) มีรายละเอียดในเอกสารมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน เรื่องข้อกำหนดด้านโปรโตคอลระดับแอบพลิเคชัน เอนพอยน์และการจัดการโทเคนและเซสชัน

4.5. การควบคุมสิทธิ์ในการเข้าถึง API (API Access Control)

การควบคุมสิทธิ์ในการเข้าถึง API มีจุดประสงค์เพื่อให้ผู้ให้บริการ API (Provider System) มั่นใจว่าเฉพาะระบบหรือบุคคลที่ได้รับอนุญาตเท่านั้นถึงจะเข้าถึง API ได้ มีข้อกำหนดดังต่อไปนี้

(1) ผู้ให้บริการ API (Provider System) ต้องตรวจสอบว่ามีเฉพาะผู้ใช้บริการ API (Consumer System) ที่ผ่านการยืนยันตัวตนเท่านั้นที่มีสิทธิ์เข้าถึง API ของผู้ให้บริการ API (Provider System) ตามรายละเอียดการยืนยันตัวตน

(2) ผู้ให้บริการ API (Provider System) ควรออกแบบและพัฒนาการควบคุมสิทธิ์และการตรวจสอบสิทธิ์ตามบทบาทและหน้าที่ของผู้ใช้งาน API ด้วยวิธี Role-Based Access Control (RBAC) อ้างอิงจาก INCITS 359-2012[R2017] Information technology - Role Based Access Control [8] ผู้ใช้งาน API ที่กล่าวถึงนั้นสามารถเป็นระดับของผู้ใช้บริการ API (Consumer System) หรือ ระดับบุคคลผู้ใช้งาน (End User) ในระบบของผู้ใช้บริการ API (Consumer System) ทั้งนี้ขึ้นอยู่กับความต้องการทางธุรกิจ (Business Requirement) ของ API และภาษาโปรแกรมที่ใช้พัฒนา API

4.6. การบริหารจัดการบัญชีการใช้งาน (API Accounting)

บัญชีการใช้งานหมายถึงบัญชีที่ผู้ใช้บริการ API (Consumer System) ใช้สำหรับยืนยันตัวตนเพื่อใช้บริการ API ของผู้ให้บริการ API (Provider System) แบ่งประเภทบัญชีได้ตามประเภทการยืนยันตัวตนได้ 3 ประเภทบัญชี คือ

4.6.1 บัญชีใช้งานประเภท API Key ใช้สำหรับการยืนยันตัวตนด้วย API Key

เมื่อผู้ให้บริการ API (Provider System) กำหนดให้ API มีการยืนยันตัวตนด้วยบัญชีการใช้งานประเภท API Key ทั้งผู้ให้บริการ API (Provider System) และผู้ใช้บริการ API (Consumer System) ต้องดำเนินการบริหารจัดการบัญชีการใช้งานให้มีความปลอดภัย ทั้งระหว่างการจัดเก็บและการรับส่งข้อมูล API Key โดยมีแนวทางปฏิบัติดังนี้

(1) ผู้ให้บริการ API (Provider System) ต้องเก็บรักษา API Key ไว้ในที่ปลอดภัย เช่น เก็บไว้ฐานข้อมูลโดยทำการใส่ Prefix และ Hash ค่าของ API Key ดังที่กล่าวไว้ในข้อ 4.2.1

(2) ผู้ใช้บริการ API (Consumer System) ไม่ควรกำหนด API Key ไว้ใน Source Code ซึ่งอาจจะเกิดความผิดพลาดขณะแชร์ Source Code ให้กับบุคคลอื่นได้ ให้เก็บไว้ใน Environment Variable หรือ File หรือที่อื่น ๆ ที่ไม่อยู่ใน Source Code หลัก รวมทั้งทำการ Hash ของมูล API Key ก่อนเก็บเสมอ

(3) ผู้ให้บริการ API (Provider System) ควรออกแบบและพัฒนา API ให้สามารถกำหนด Access Control ของแต่ละ API Key ที่มอบให้แก่ผู้ขอใช้บริการ API ได้

(4) ผู้ให้บริการ API (Provider System) ควรออกแบบและพัฒนา API ให้สามารถกำหนดวันหมดอายุของ API Key ได้

(5) ผู้ให้บริการ API (Provider System) ควรใช้ API Key ใน API ประเภทที่เป็นการอ่านข้อมูลเท่านั้น เนื่องจาก API Key ส่วนข้อมูลประเภทที่เป็นการสร้าง ลบหรือแก้ไขข้อมูลควรใช้การยืนยันตัวตนระดับบุคคลร่วมด้วย เช่น OAuth 2.0 เป็นต้น

(6) ผู้ให้บริการ API ควรให้บริการ REST API ผ่าน HTTPS (SSL) เท่านั้น

(7) ทั้งผู้ให้บริการ API (Provider System) และผู้ใช้บริการ API (Consumer System) ควรมีการทดสอบความปลอดภัยของระบบเพื่อหาช่องโหว่ที่เกิดจากการใช้ API Key ก่อนการใช้งานจริง เช่นทดสอบตามหัวข้อ API2:2019 Broken User Authentication ของ OWASP API Security [9]

4.6.2 บัญชีใช้งาน Identity Provider ที่รองรับมาตรฐาน OAuth 2.0

เมื่อผู้ให้บริการ API (Provider System) กำหนดให้ API มีการยืนยันตัวตนด้วยบัญชีการใช้งานประเภทOAuth 2.0 ทั้งผู้ให้บริการ API (Provider System) ผู้ใช้บริการ API (Consumer System) และหน่วยงานผู้บริการ Platform เพื่อเชื่อมโยงและแลกเปลี่ยนข้อมูลจะต้องดำเนินการดังต่อไปนี้

(1) หน่วยงานผู้บริการ Platform ดำเนินการจัดเตรียมระบบพิสูจน์และยืนยันตัวตน (Identity Provider) ที่รองรับมาตรฐาน OAuth 2.0

(2) หน่วยงานผู้บริการ Platform ดำเนินการรับลงทะเบียนบัญชีผู้ใช้งานตามที่ระบุไว้ในหัวข้อ 4.3.1

(3) ผู้ให้บริการ API (Provider System) ควรให้บริการ REST API ผ่าน HTTPS (SSL) เท่านั้น

(4) Access Token ควรมีระยะเวลาการใช้งานได้จำกัด ซึ่งผู้ขอใช้บริการ API จะต้องเรียกใช้บริการ API ก่อนที่ Access Token จะหมดอายุ มีรายละเอียดในเอกสารมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน เรื่องข้อกำหนดด้านโปรโตคอลระดับแอบพลิเคชัน เอนพอยน์และการจัดการโทเคนและเซสชัน

(5) เมื่อ Access Token ใกล้หมดอายุผู้ให้บริการ API สามารถเรียก Refresh Token เพื่อขอต่ออายุ Access Token ได้มีรายละเอียดในเอกสารมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน เรื่องข้อกำหนดด้านโปรโตคอลระดับแอบพลิเคชัน เอนพอยน์และการจัดการโทเคนและเซสชัน

4.6.3 บัญชีใช้งาน Identity Provider ที่รองรับมาตรฐาน Open ID Connect

กรณีที่ผู้ให้บริการ API (Provider System) กำหนดให้ API มีการยืนยันตัวตนด้วยบัญชีการใช้งานประเภท Open ID Connect ทั้งผู้ให้บริการ API (Provider System) ผู้ใช้บริการ API (Consumer System) และหน่วยงานผู้บริการ TGIX Platform จะมีการด าเนินการเหมือนกับใช้มาตรฐาน OAuth 2.0

บรรณานุกรม

[1] D. Hardt. (2012, ตุลาคม). The OAuth 2.0 Authorization Framework. [ออนไลน์]. เข้าถึงได้จาก: https://datatracker.ietf.org/doc/html/rfc6749. (วันที่ค้นข้อมูล: 26 ตุลาคม 2021)

[2] M. Jones. (2012, ตุลาคม). The OAuth 2.0 Authorization Framework: Bearer Token Usage. [ออนไลน์]. เข้าถึงได้จาก: https://datatracker.ietf.org/doc/html/rfc6750. (วันที่ค้นข้อมูล: 26 ตุลาคม 2021)

[3] D. Hardt. (2012, ตุลาคม). The OAuth 2.0 Authorization Framework (RFC-6749): Section-1.3.1. [ออนไลน์]. เข้าถึงได้จาก: https://datatracker.ietf.org/doc/html/rfc6749#section-1.3.1. (วันที่ค้นข้อมูล: 26 ตุลาคม 2021)

[4] D. Hardt. (2012, ตุลาคม). The OAuth 2.0 Authorization Framework (RFC-6749): Section-1.3.2. [ออนไลน์]. เข้าถึงได้จาก: https://datatracker.ietf.org/doc/html/rfc6749#section-1.3.2. (วันที่ค้นข้อมูล: 26 ตุลาคม 2021)

[5] D. Hardt. (2012, ตุลาคม). The OAuth 2.0 Authorization Framework (RFC-6749): Section-1.3.3. [ออนไลน์]. เข้าถึงได้จาก: https://datatracker.ietf.org/doc/html/rfc6749#section-1.3.3. (วันที่ค้นข้อมูล: 26 ตุลาคม 2021)

[6] D. Hardt. (2012, ตุลาคม). The OAuth 2.0 Authorization Framework (RFC-6749): Section-1.3.4. [ออนไลน์]. เข้าถึงได้จาก: https://datatracker.ietf.org/doc/html/rfc6749#section-1.3.4. (วันที่ค้นข้อมูล: 26 ตุลาคม 2021)

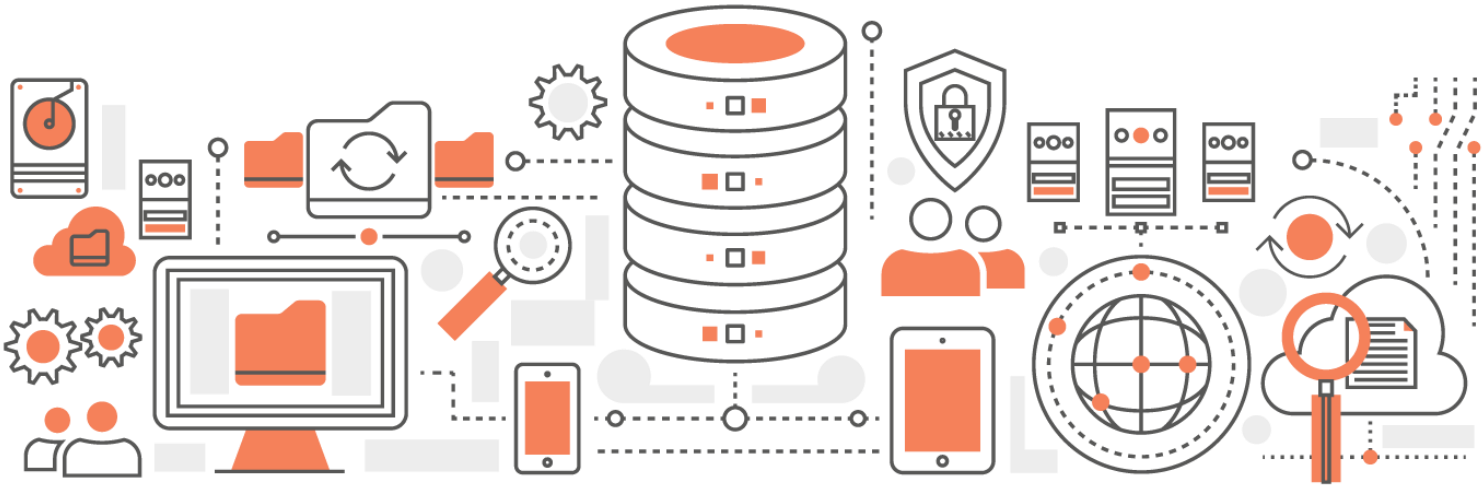
[7] Microsoft. (2021). Microsoft identity platform ID tokens. [ออนไลน์]. เข้าถึงได้จาก: https://docs.microsoft.com/en-us/azure/active-directory/develop/id-tokens. (วันที่ค้นข้อมูล: 26 ตุลาคม 2021)

[8] Information Technology Industry Council. (2017). Information technology - Role Based Access Control. [ออนไลน์]. เข้าถึงได้จาก: https://standards.incits.org/apps/group_public/project/details.php?project_id=1906. (วันที่ค้นข้อมูล: 26 ตุลาคม 2021)

[9] OWASP Foundation, Inc. (2019). OWASP API Security. [ออนไลน์]. เข้าถึงได้จาก: https://owasp.org/www-project-api-security/. (วันที่ค้นข้อมูล: 26 ตุลาคม 2021)

[10] Using API keys. (2021). [ออนไลน์]. เข้าถึงได้จาก: https://cloud.google.com/docs/authentication/api-keys. (วันที่ค้นข้อมูล: 26 ตุลาคม 2021)

[11] Hypertext Transfer Protocol (HTTP) Authentication Scheme Registry. (2021, ตุลาคม). [ออนไลน์]. เข้าถึงได้จาก: https://www.iana.org/assignments/http-authschemes/http-authschemes.xhtml#authschemes. (วันที่ค้นข้อมูล: 26 ตุลาคม 2021)



กลุ่มพัฒนาระบบข้อมูล กองแผนงาน กระทรวงสาธารณสุข