สพร. / CDV
ธันวาคม 2564

ห้ามใช้หรือยึดร่างนี้เป็นมาตรฐาน
มาตรฐานฉบับสมบูรณ์จะมีประกาศในราชกิจจานุเบกษา

ร่าง

มาตรฐานรัฐบาลดิจิทัล
Digital Government Standard

ว่าด้วย มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่อง ข้อกำหนดด้านความน่าเชื่อถือและความมั่นคงปลอดภัย

THAILAND GOVERNMENT INFORMATION EXCHANGE STANDARD SERIES: LINKAGE STANDARD PART 4 : STANDARD REGULATIONS FOR THE ASPECT TRUST AND SECURITY

สำหรับเสนอคณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์
ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ชั้น 17 อาคารบางกอกไทยทาวเวอร์ 108 ถนนรางน้ำ แขวงถนนพญาไท เขตราชเทวี กรุงเทพฯ 10400
หมายเลขโทรศัพท์: (+66) 0 2612 6000 โทรสาร: (+66) 0 2612 6011 (+66) 0 2612 6012

คณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

ประธานกรรมการ

ผู้ช่วยศาสตราจารย์ภุชงค์ อุทโยภาศ	มหาวิทยาลัยเกษตรศาสตร์

รองประธานกรรมการ

นายวิบูลย์ ภัทรพิบูล	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

กรรมการ

ผู้ช่วยศาสตราจารย์โษฑศ์รัตต ธรรมบุษดี	มหาวิทยาลัยมหิดล
ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูไพโรจน์	จุฬาลงกรณ์มหาวิทยาลัย
นายสุทธิศักดิ์ ตันตะโยธิน	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ
นายพณชิต กิตติปัญญางาม	สมาคมการค้าเพื่อส่งเสริมผู้ประกอบการเทคโนโลยีรายใหม่
นายมารุต บูรณรัช	ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
นางสาวปศิญา เชื้อดี	สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ
นายศุภโชค จันทรประทิน	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
นางสาวพลอย เจริญสม	
นางบุญยิ่ง ชั่งสัจจา	สำนักบริหารการทะเบียน กรมการปกครอง
นายณัฏฐา พาชัยยุทธ	สำนักงานคณะกรรมการพัฒนาระบบราชการ
นายพัชโรดม ลิมปิษเฐียร	สำนักงานคณะกรรมการกฤษฎีกา
นางสาวพัชรี ไชยเรืองกิตติ	
นางสาวสุภร สุขะตุงคะ	สำนักงานการตรวจเงินแผ่นดิน
นางสาวขนิษฐา ทัศนาพิทักษ์	
นายธีรวุฒิ ธงภักดิ์	สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ
นายกฤษณ์ โกวิทพัฒนา	
นายทรงพล ใหม่สาลี	สำนักงานสถิติแห่งชาติ
นางกาญจนา ภู่มาลี	

กรรมการและเลขานุการ

นางสาวอุรัชฎา เกตุพรหม	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะทำงานเทคนิคด้านมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ

ที่ปรึกษา

นายสุพจน์ เธียรวุฒิ	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ผู้ช่วยศาสตราจารย์ภุชงค์ อุทโยภาศ	มหาวิทยาลัยเกษตรศาสตร์
นายวิบูลย์ ภัทรพิบูล	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ประธานคณะทำงาน

ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูไพโรจน์	จุฬาลงกรณ์มหาวิทยาลัย

รองประธานคณะทำงาน

ผู้ช่วยศาสตราจารย์มารอง ผดุงสิทธิ์	มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี

คณะทำงาน

นายธีรวุฒิ ธงภักดิ์	กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
นายกฤษณ์ โกวิทพัฒนา	
นางสาวนฤมล พันธุ์มาดี	
นายกิติพงษ์ จันทรสกุล	กรมการค้าต่างประเทศ
นายนริศร จินตวรรณ	
ผู้แทนกรมการค้าภายใน	
นางบุญยิ่ง ชั่งสัจจา	กรมการปกครอง
นางสาวมนทิพา เข่งพิมล	กรมพัฒนาธุรกิจการค้า
นายพงศกร ริยะมงคล	
นายกุลเชษฐ์ ชีวะไพบูลย์	
นายกำชัย จัตตานนท์	ผู้แทนกรมศุลกากร
นางสาวขนิษฐา สหเมธาพัฒน์	กรมสรรพากร
ผู้แทนสำนักงบประมาณ	
นายนฤทธิ์ หรั่งทอง	สำนักงานคณะกรรมการส่งเสริมการลงทุน
นางสาวณัฐพร วัฒนสุทธิ	
นายชาวันย์ สวัสดิ์-ชูโต	สำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม
นางสาวณัฏฐา ตุณสุวรรณ	
นางสาวชมบุญ บุญคง	
นางสมศจี ศิกษมัต	ธนาคารแห่งประเทศไทย

นายอาศิส อัญญะโพธิ์ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะทำงานและเลขานุการ

นางสาวอุรัชฎา เกตุพรหม สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

นายเจษฎา ขจรฤทธิ์

วิเคราะห์และจัดทำมาตรฐานรัฐบาลดิจิทัล
มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ
ด้านการเชื่อมโยงข้อมูล
เรื่อง ข้อกำหนดด้านความน่าเชื่อถือและความมั่นคงปลอดภัย

นายเจษฎา ขจรฤทธิ์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นายปราการ ศิริมา	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นายสุเมธ สุทธิกุล	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คำนำ

ตามแผนพัฒนารัฐบาลดิจิทัลของประเทศไทยในการผลักดันให้เกิดการเชื่อมโยงข้อมูลของส่วนราชการเข้ากับศูนย์ข้อมูลอื่นๆ รัฐบาลจึงกำหนดให้มีการนำธรรมาภิบาลข้อมูลภาครัฐ (Data Governance: DG) มาเป็นแกนสำคัญในการประยุกต์ใช้ Big Data ภาครัฐเพื่อเพิ่มประสิทธิผลของนโยบายในการพัฒนาประเทศระยะยาว สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) หรือ สพร. จึงได้สร้างความร่วมมือกับหน่วยงานภาครัฐเพื่อดำเนินการจัดทำมาตรฐานการเชื่อมโยง และแลกเปลี่ยนข้อมูลภาครัฐ (Thailand Government Information Exchange: TGIX) โดยมีจุดประสงค์เพื่อให้เกิดมาตรฐานในการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ อันนำไปสู่การบูรณาการข้อมูล และการใช้ข้อมูลเพื่อขับเคลื่อนประเทศอย่างมีประสิทธิภาพ

มาตรฐานที่ทาง สพร. ดำเนินการจัดทำขึ้นประกอบด้วย 2 ส่วนที่มีความสอดคล้องกัน ได้แก่

(1) มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ในระดับด้านความหมายข้อมูล (Semantic Standard) และ

(2) มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ในระดับด้านการเชื่อมโยงข้อมูล (Linkage Standard)

มาตรฐานส่วน (2) เป็นมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ในระดับด้านการเชื่อมโยงข้อมูล (Linkage Standard) ว่าด้วยเรื่องของสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ และองค์ประกอบของสถาปัตยกรรม เช่น (1) การบริหารจัดการ Authentication และ Access Control และ บัญชีผู้ใช้งาน Accounting (2) การบริหารจัดการ Token และ Session (3) โปรโตคอล (Protocol) สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูล (4) ความมั่นคงปลอดภัย (Security) และการเข้ารหัสข้อมูล (Encryption) (5) การบันทึกล็อก (Logging) และการติดตาม (Monitoring) (6) การกำหนด namespace ของระบบ เป็นต้น

สารบัญ

สารบัญรูป

สารบัญตาราง

มาตรฐานรัฐบาลดิจิทัล

ว่าด้วย มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่อง ข้อกำหนดด้านความน่าเชื่อถือและความมั่นคงปลอดภัย

1. ขอบข่าย

การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานเป็นพื้นฐานหลักที่จำเป็นต่อการพัฒนารัฐบาลดิจิทัล ในปัจจุบันประเทศไทยมีแพลตฟอร์มการแลกเปลี่ยนข้อมูลที่ให้บริการอยู่หลายแห่ง แพลตฟอร์มแต่ละแห่งมี แนวทางและพันธกิจในการดำเนินงานเป็นของตนเอง เป็นผลให้การบูรณาการข้อมูลภาครัฐจำเป็นต้อง ขับเคลื่อนด้วยการสร้างมาตรฐานหรือข้อตกลงร่วมกันในการแลกเปลี่ยนข้อมูลสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ได้เล็งเห็นความสำคัญในจุดนี้ จึงมีความจำเป็นต้องจัดทำมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ เพื่อใช้ในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานของรัฐเพื่อให้เกิดการบูรณาการข้อมูลเกิดขึ้นอย่างเป็นรูปธรรม

เป้าประสงค์หลักของการใช้มาตรฐานฯ เป็นตัวขับเคลื่อนการบูรณาการข้อมูลภาครัฐ คือ การให้หน่วยงานของรัฐมีแนวทางในการพัฒนาสถาปัตยกรรมระบบสารสนเทศเพื่อใช้ในการแลกเปลี่ยนข้อมูลที่ชัดเจน มีความสอดคล้องในการเชื่อมต่อระหว่างกัน

ดังนั้นเพื่อให้บรรลุเป้าประสงค์หลักดังกล่าวเอกสารฉบับนี้จึงนำเสนอข้อกำหนดด้านความน่าเชื่อถือและความมั่นคงปลอดภัย สำหรับประกอบเอกสารว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ เรื่อง มาตรฐานสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐระดับการเชื่อมโยงข้อมูลที่เหมาะสมกับบริบทของประเทศไทยเท่านั้น

2. นิยาม

นิยามคำศัพท์ที่เกี่ยวข้องกับมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่อง ข้อกำหนดด้านความน่าเชื่อถือและความมั่นคงปลอดภัยที่ใช้ในเอกสารฉบับนี้มีดังนี้

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

2.2. โปรโตคอล HTTPS หมายความว่า เป็นส่วนขายของโปรโตคอล 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 TGIX Platform ทำหน้าที่ออกใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) ให้แก่สมาชิกในกลุ่ม TGIX

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

2.7. การเข้ารหัสแฮชฟังก์ชัน (Hash Functions) หมายความว่า อัลกอริทึมสำหรับเข้ารหัสข้อมูลแบบทางเดียว เพื่อใช้ในกระบวนการสร้างและตรวจสอบลายมือชื่อดิจิทัล 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 ระบุว่า รัฐต้องเปิดเผยข้อมูลหรือข่าวสารสาธารณะในครอบครองของหน่วยงานของรัฐที่มิใช่ข้อมูลเกี่ยวกับความมั่นคงของรัฐหรือเป็นความลับของทางราชการตามที่กฎหมายบัญญัติ และต้องจัดให้ประชาชนเข้าถึงข้อมูลหรือข่าวสารดังกล่าวได้โดยสะดวก

3.2 พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 ในมาตรา 13 ระบุว่าเพื่อประโยชน์ในการบริหารราชการแผ่นดินและการให้บริการประชาชน ให้หน่วยงานของรัฐจัดให้มีการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลที่มีการจัดทำและครอบครองตามที่หน่วยงานของรัฐแห่งอื่นร้องขอ ที่จะเกิดการบูรณาการร่วมกัน

มาตรา 15 ระบุว่า ให้มีศูนย์แลกเปลี่ยนข้อมูลกลางทำหน้าที่เป็นศูนย์กลางในการแลกเปลี่ยนข้อมูลดิจิทัลและทะเบียนดิจิทัลระหว่างหน่วยงานของรัฐ เพื่อสนับสนุนการดำเนินการของหน่วยงานของรัฐในการให้บริการประชาชนผ่านระบบดิจิทัล และดำเนินการในเรื่องดังต่อไปนี้

(1) กำหนดนโยบายและมาตรฐานเกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลเสนอต่อคณะกรรมการพัฒนารัฐบาลดิจิทัลให้ความเห็นชอบ
(2) ประสานและให้ความช่วยเหลือแก่หน่วยงานของรัฐในการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลระหว่างกัน รวมทั้งกำกับติดตามให้การดำเนินการดังกล่าวเป็นไปในแนวทางและมาตรฐานเดียวกันตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่คณะกรรมการพัฒนารัฐบาลดิจิทัลกำหนด
(3) จัดทำคำอธิบายชุดข้อมูลดิจิทัลของภาครัฐ และจัดเก็บบันทึกหลักฐานของการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล
(4) เรื่องอื่นๆ ตามที่คณะกรรมการพัฒนารัฐบาลดิจิทัลมอบหมาย

มาตรา 19 ระบุว่า ในวาระเริ่มแรก ให้สำนักงานดำเนินการให้มีศูนย์แลกเปลี่ยนข้อมูลกลางตามมาตรา 15 เป็นการชั่วคราวแต่ไม่เกินสองปี เมื่อครบกำหนดระยะเวลาดังกล่าว ให้คณะกรรมการพัฒนารัฐบาลดิจิทัลพิจารณาความจำเป็นและเหมาะสมเกี่ยวกับหน่วยงานของรัฐที่จะมาดำเนินการเกี่ยวกับศูนย์แลกเปลี่ยนข้อมูลกลาง ทั้งนี้ ในกรณีที่คณะกรรมการพัฒนารัฐบาลดิจิทัลเห็นควรให้หน่วยงานของรัฐแห่งอื่นใดทำหน้าที่แทนสำนักงาน ให้เสนอแนวทางการดำเนินการ การโอนภารกิจ งบประมาณ ทรัพย์สินและหนี้สิน ภาระผูกพัน และบุคลากรไปยังหน่วยงานของรัฐแห่งอื่นนั้นต่อคณะรัฐมนตรีเพื่อพิจารณา

4. ข้อกำหนดด้านความน่าเชื่อถือและความมั่นคงปลอดภัย

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

ในส่วนนี้จะอธิบายหลักการขั้นพื้นฐานของมาตรฐานความปลอดภัยของมาตรฐานการเชื่อมโยงและการแลกเปลี่ยนข้อมูลภาครัฐระดับการเชื่อมโยงข้อมูลที่กำหนดขึ้นเพื่อให้เป็นมาตรฐานความน่าเชื่อถือและความมั่นคงปลอดภัยการเชื่อมโยงและแลกเปลี่ยนข้อมูล โดยอ้างอิงจากหลักการในเรื่องความปลอดภัยสารสนเทศ (Information Security: InfoSec) [1] ซึ่งประกอบไปด้วยส่วนสำคัญ 3 เรื่องคือ Confidentiality, Integrity และ Availability หรือที่รู้จักกันคือ CIA Triad [2]

4.1. จุดประสงค์ของข้อกำหนดพื้นฐานด้านความน่าเชื่อถือและความมั่นคงปลอดภัย

4.1.1. การรักษาความลับของข้อมูล (Confidentiality)

การรักษาความลับของข้อมูล คือการเก็บรักษาข้อมูลให้เป็นความลับและอนุญาตให้เฉพาะผู้ที่ได้รับอนุญาตเข้าถึงข้อมูลได้ โดยการจำกัดสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานในระบบ (ผู้ที่มีส่วนเกี่ยวข้องในการเชื่อมโยงและการแลกเปลี่ยนข้อมูล) ด้วยการยืนยันตัวตน (Authentication) และการตรวจสอบสิทธิ์ (Authorization) ในการเข้าถึงทรัพยากร เพื่อให้มั่นใจได้ว่าจะไม่มีการเข้าถึงข้อมูลจากผู้ที่ไม่ได้รับอนุญาต

มาตรฐานการเชื่อมโยงและการแลกเปลี่ยนข้อมูลภาครัฐระดับการเชื่อมโยงข้อมูล (TGIX) ใช้การส่งผ่านข้อมูลในระบบที่อาจผ่านเครือข่ายสาธารณะเช่น Internet จึงมีการกำหนดให้ใช้วิธีการส่งข้อมูลด้วยกระบวนการที่มีความปลอดภัยสูง เช่น Digital Signagture และการเข้ารหัสข้อมูล (Data Encryption) ซึ่งข้อมูลจะต้องถูกส่งผ่านโปรโตคอล HTTPS บน Transport Layer Security (TLS) ที่จะช่วยป้องกันการดักฟังและป้องกันการโจรกรรมข้อมูล โดยจะทำให้มั่นใจได้ว่าการแลกเปลี่ยนข้อมูลผ่านมาตรฐาน TGIX จะรักษาความลับ และความเป็นส่วนตัวของข้อมูลได้ ซึ่งได้มีข้อกำหนดที่เกี่ยวข้องดังต่อไปนี้

(1) ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security)

(2) ข้อกำหนดการเข้ารหัส (Encryption)

(3) ข้อกำหนดด้าน Authentication Acess Control และ Accounting ซึ่งกล่าวในมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่อง ข้อกำหนดด้านการยืนยันตัวตน การกำหนดสิทธิ์ และบัญชีการใช้งาน

(4) ข้อกำหนดด้านการบริหารจัดการ Token และ Session ซึ่งกล่าวในมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่อง ข้อกำหนดของโปรโตคอลระดับแอบพลิเคชันเอนพอยน์และการจัดการโทเคนและเซสชัน

4.1.2. ความถูกต้องของข้อมูล (Integrity)

ความถูกต้องของข้อมูล คือการตรวจสอบและทำให้มั่นใจว่าข้อมูลที่มีการแลกเปลี่ยนกันภายในมาตรฐาน TGIX มีความถูกต้องและสมบูรณ์ครบถ้วน ไม่ถูกแก้ไขหรือทำให้ได้รับความเสียหายแก่ข้อมูลที่แลกเปลี่ยนกันภายใน TGIX ซึ่งได้มีข้อกำหนดที่เกี่ยวข้องดังต่อไปนี้

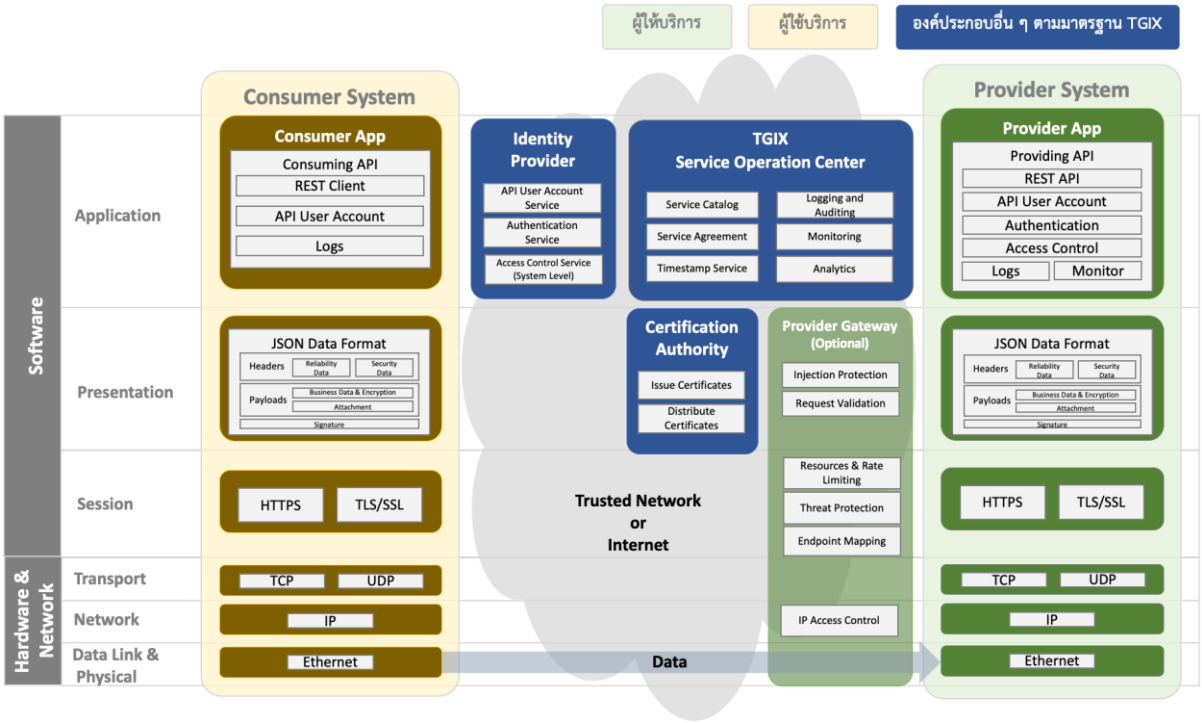
(1) ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security)
(2) ข้อกำหนดการจำกัดอัตราการเข้าถึงบริการและใช้ทรัพยากร (Resource and Rate Limit)
(3) ข้อกำหนดการบันทึกกิจกรรมและข้อมูลจราจรคอมพิวเตอร์และการสอดส่อง (Logging & Monitoring)
(4) ข้อกำหนดการจัดการความผิดพลาด (Error handling)
(5) ข้อกำหนดการตรวจสอบข้อมูลนำเข้า (Input Validation)

4.1.3. ความพร้อมให้บริการ (Availability)

ความพร้อมให้บริการ คือความพร้อมใช้งานหรือให้บริการของระบบได้อย่างต่อเนื่อง เพื่อทำให้มั่นใจว่าองค์ประกอบต่างๆ ในมาตรฐาน TGIX มีความพร้อมให้บริการกับองค์ประกอบอื่นในมาตรฐาน TGIX ที่มีความเกี่ยวข้องกัน และเพื่อบรรเทาผลกระทบจากการไม่สามารถให้บริการได้จนนำไปสู่ผลกระทบกับผู้ใช้บริการ ซึ่งได้มีข้อกำหนดที่เกี่ยวข้องดังต่อไปนี้

(1) ข้อกำหนดเกี่ยวกับการป้องกันการโจมตี
(2) ข้อกำหนดการจำกัดอัตราการเข้าถึงบริการและใช้ทรัพยากร (Resource and Rate Limit)
(3) ข้อกำหนดการตรวจสอบข้อมูลนำเข้า (Input Validation)

จากหลักการขั้นพื้นฐานทั้ง 3 ข้างต้น คือ การรักษาความลับ (Confidentiallity) ความถูกต้องของข้อมูล (Integrity) และความพร้อมให้บริการ (Availability) โดยมาตรฐานการเชื่อมโยงและการแลกเปลี่ยนข้อมูลภาครัฐระดับการเชื่อมโยงข้อมูลจัดให้มีข้อกำหนดเพื่อเป็นกรอบแนวทางการปฏิบัติตามแนวทางการปฏิบัติที่ดี โดยจะครอบคลุมผู้ให้บริการ ผู้ใช้บริการ และองค์ประกอบอื่นๆ ตามมาตรฐาน TGIX ดังรูปที่ 1



รูปที่ 1 ภาพรวมองค์ประกอบของการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ

สามารถแบ่งข้อกำหนดเป็น 4 ส่วนดังนี้

(1) ข้อกำหนดด้านความปลอดภัยของผู้ให้บริการ ประกอบด้วย

ก. ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security)

ข. ข้อกำหนดการเข้ารหัส (Encryption)

ค. ข้อกำหนดการจำกัดอัตราการเข้าถึงบริการและใช้ทรัพยากร

ง. ข้อกำหนดการบันทึกกิจกรรมและข้อมูลจราจรคอมพิวเตอร์และการตรวจสอบ (Logging & Monitoring)

จ. ข้อกำหนดการจัดการความผิดพลาด (Error handling)

ฉ. ข้อกำหนดการตรวจสอบข้อมูลนำเข้า (Input Validation)

ช. ข้อกำหนดเกี่ยวกับการป้องกันการโจมตี

(2) ข้อกำหนดด้านความปลอดภัยของผู้ใช้บริการ ประกอบด้วย

ก. ข้อกำหนดด้านความมั่นคงปลอดภัยของการส่งข้อมูล (Transport Security)

ข. ข้อกำหนดการเข้ารหัส (Encryption)

ค. ข้อกำหนดการบันทึกกิจกรรมและข้อมูลจราจรคอมพิวเตอร์และการตรวจสอบ (Logging & Monitoring)

(3) ข้อกำหนดด้านความปลอดภัยขององค์ประกอบอื่นๆ ตามมาตรฐาน TGIX ประกอบด้วย

ก. ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security)

ข. ข้อกำหนดการเข้ารหัส (Encryption)

ค. ข้อกำหนดการบันทึกกิจกรรมและข้อมูลจราจรคอมพิวเตอร์และการตรวจสอบ (Logging & Monitoring)

ง. ข้อกำหนดการจัดการความผิดพลาด (Error handling)

(4) ข้อกำหนดด้านความปลอดภัยที่เกี่ยวข้องกับกฎหมาย ประกอบด้วย

ก. ข้อกำหนดที่เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

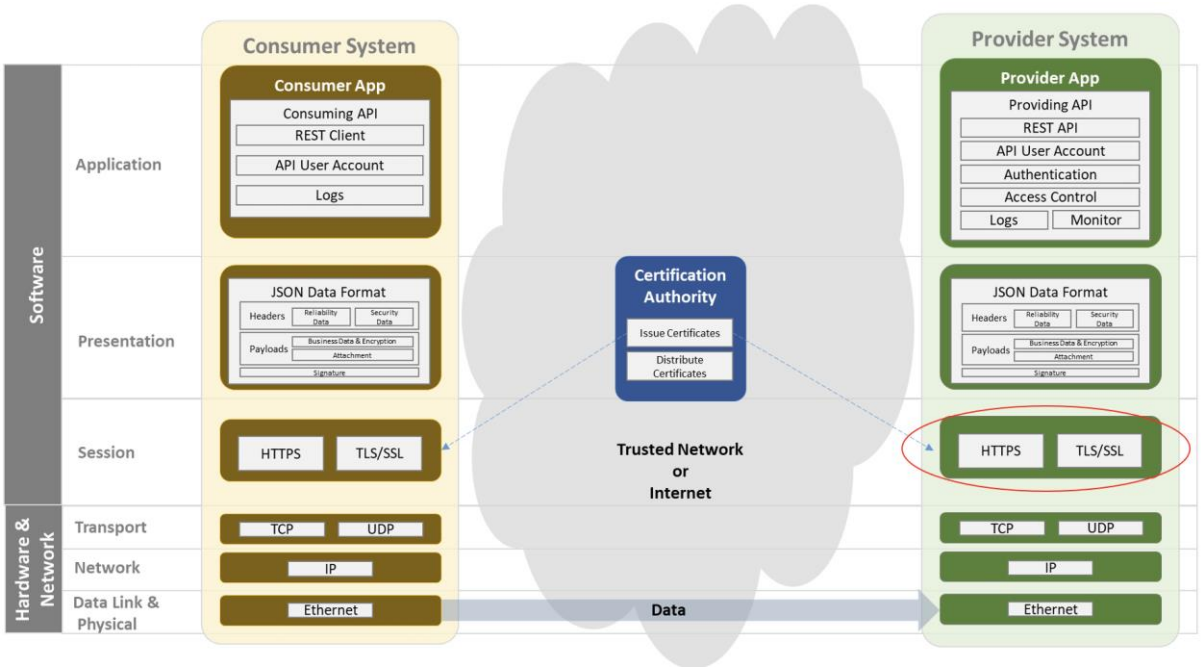
ข. ข้อกำหนดที่เกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

ค. ข้อกำหนดที่เกี่ยวกับหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564

4.2. ข้อกำหนดด้านความปลอดภัยของผู้ให้บริการ (Provider)

4.2.1. ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security)

ความปลอดภัยของการส่งข้อมูล (Transport Security) ของมาตรฐาน TGIX ของผู้ให้บริการจะมุ่งเน้นไปการส่งข้อความในระดับ Session ของผู้ให้บริการ ในองค์ประกอบของการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐของผู้ให้บริการดังรูปที่ 2



รูปที่ 2 องค์ประกอบที่เกี่ยวข้องกับความปลอดภัยของการส่งข้อมูลของผู้ให้บริการการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ

เพื่อให้การรับส่งข้อมูลสำหรับบริการการแลกเปลี่ยนข้อมูลมีความปลอดภัยและเป็นไปตามข้อกำหนดพื้นฐานด้านความปลอดภัย การสื่อสารเพื่อรับส่งข้อมูลของมาตรฐาน TGIX ของผู้ให้บริการจะต้องเป็นไปตามข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security) ของผู้ให้บริการ [3] โดยมีรายละเอียดดังตารางที่ 1

ตารางที่ 1 ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security) ของผู้ให้บริการ

ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security)	ข้อกำหนดที่แนะนำ	ข้อกำหนดที่ต้องการ
• การส่งข้อมูลจะต้องดำเนินการบน HTTPS โดยใช้ TLS 1.2 เป็นอย่างน้อย	✓	✓

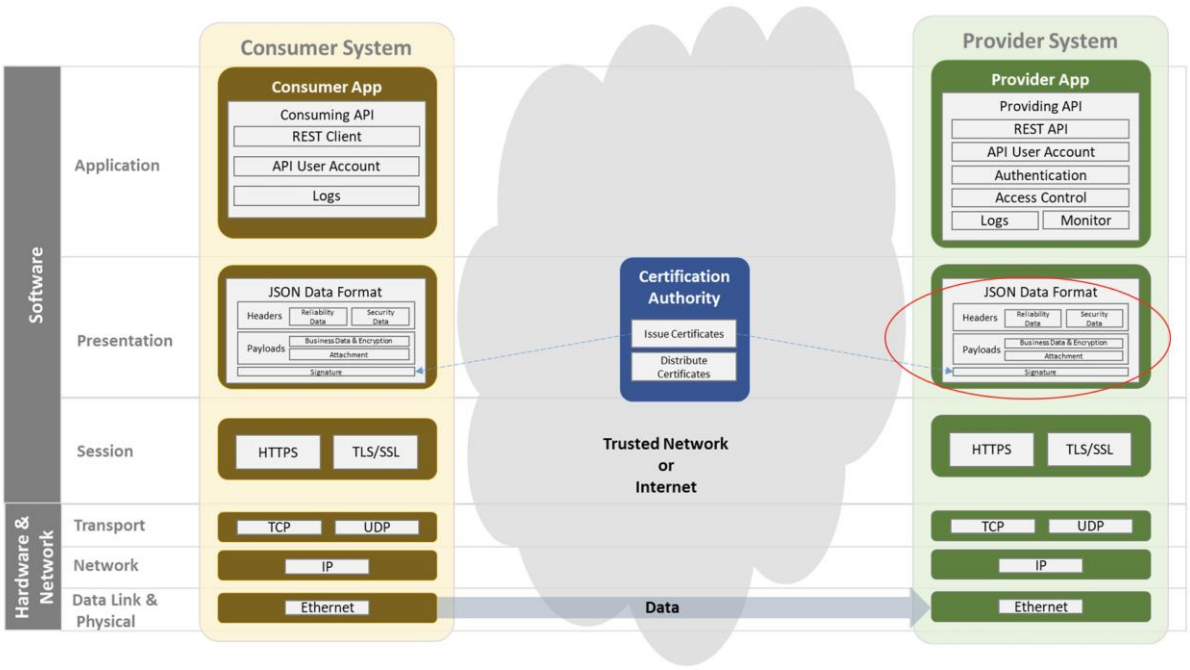
ตารางที่ 1 ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security) ของผู้ให้บริการ (ต่อ)

ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security)	ข้อกำหนดที่แนะนำ	ข้อกำหนดที่ต้องการ
● ใบรับรอง (Certificates) จะต้องมีการเข้ารหัสแฮชฟังก์ชัน (Hash Functions) แบบ SHA-2 (Secure Hash Algorithm 2) ด้วยความยาวกุญแจ (Key size) อย่างน้อย 2048 bits	✓	✓
● ทุกปลายทาง (Endpoint) จะต้องใช้ใบรับรองดิจิทัล (Digital Certificate) ที่ออกโดยหน่วยงานที่ดูแลใบรับรองดิจิทัลที่ได้รับอนุญาต	✓	○
● ห้ามทำการเปลี่ยนเส้นทาง HTTP ไปยัง HTTPS โดยให้ปฏิเสธการเปลี่ยนเส้นทางทุกกรณี	✓	✓
● ให้ปิดการใช้งานเมธอด HTTP (HTTP Method) ที่ไม่ได้ใช้งาน และส่งคืนค่า HTTP 405 ตามมาตรฐาน Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content: section-6.5.5 [4]	✓	✓
● ต้องมีการตรวจสอบ (Validate) ตามข้อกำหนดการตรวจสอบข้อมูลนำเข้า (Input Validation) ทุกๆ การเรียกใช้งาน (Request)	✓	✓

✓ จำเป็น ○ ทางเลือก

4.2.2. ข้อกำหนดการเข้ารหัส (Encryption)

การเข้ารหัสข้อมูลของผู้ให้บริการในกรณีที่ต้องมีการเข้ารหัสข้อมูล เช่น ข้อมูลที่มีความสำคัญที่เป็นข้อมูลเชิงธุรกรรมที่ Payload ข้อมูลลายเซ็นในส่วน Signature หรือข้อมูล Token ที่อยู่ในส่วน Header เป็นต้น การเข้ารหัสข้อมูล (Encyption) ของมาตรฐาน TGIX จะมุ่งเน้นไปยังส่วน Presentation ของผู้ให้บริการ ในองค์ประกอบของการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐของผู้ให้บริการดังรูปที่ 3



รูปที่ 3 องค์ประกอบที่เกี่ยวข้องกับความปลอดภัยของการเข้ารหัสของผู้ให้บริการการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ

เพื่อให้เป็นไปตามข้อกำหนดพื้นฐานด้านความปลอดภัย การเข้ารหัสข้อมูล (Encyption) ของมาตรฐาน TGIX ของผู้ให้บริการจะต้องเป็นไปตามข้อกำหนดการเข้ารหัส (Encryption) ของผู้ให้บริการ [5] โดยมีรายละเอียดดังตารางที่ 2 **Error! Reference source not found.**

ตารางที่ 2 ข้อกำหนดการเข้ารหัส (Encryption) ของผู้ให้บริการ

ข้อกำหนดการเข้ารหัส (Encryption)	ข้อกำหนดที่แนะนำ	ข้อกำหนดที่ต้องการ
• ในกรณีที่การส่งข้อมูลที่ผู้ให้บริการพิจารณาแล้วว่ามีข้อมูลที่มีความสำคัญที่เป็นข้อมูลเชิงธุรกรรมใน Payload หรือเป็นความลับที่ต้องการการเข้ารหัสจะต้องใช้การเข้ารหัสแบบสมมาตร (Symmetric Encryption) แบบ AES (Advanced Encryption Standard) [6] โดยมีความยาวของกุญแจอย่างน้อย 128 bits (AES-128) ซึ่งสามารถเข้ารหัสเฉพาะข้อมูลนั้น ๆ ไม่จำเป็นต้องเข้ารหัสข้อมูลทั้ง Payload หมายเหตุ 1. ในกรณีที่พบปัญหาการถอดรหัสเช่น ผู้ให้บริการไม่สามารถถอดรหัสข้อมูลที่ได้รับได้ ผู้ให้บริการสามารถตอบกลับด้วย error message ดังตัวอย่างการตอบกลับดังรูปที่ 4	✓	✓

ตารางที่ 2 ข้อกำหนดการเข้ารหัส (Encryption) ของผู้ให้บริการ (ต่อ)

ข้อกำหนดการเข้ารหัส (Encryption)	ข้อกำหนดที่แนะนำ	ข้อกำหนดที่ต้องการ
● 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 ในกรณีที่พบปัญหาการถอดรหัสเช่น ผู้ให้บริการไม่สามารถถอดรหัสการตรวจสอบลายเซ็นของ JWT (JSON Web Token) ได้ ผู้ให้บริการสามารถตอบกลับด้วย error message ดังตัวอย่างการตอบกลับดังตัวอย่างในรูปที่ 5	✓	○
● 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)	✓	✓
● สำหรับการสร้างตัวเลขแบบสุ่ม (Random Bit Generation) เพื่อจุดประสงค์ต่าง ๆ เช่นการสร้างกุญแจ (keys) ตัวเลขแบบใช้	✓	✓

ตารางที่ 2 ข้อกำหนดการเข้ารหัส (Encryption) ของผู้ให้บริการ (ต่อ)

ข้อกำหนดการเข้ารหัส (Encryption)	ข้อกำหนดที่แนะนำ	ข้อกำหนดที่ต้องการ
ครั้งเดียว (Nonces) และ ค่าสุ่มเพื่อการยืนยันตัวตน (Authentication Challenges) จะต้องใช้อัลกอลิธึมแบบใดแบบหนึ่งดังต่อไปนี้ ○ Hash_DRBG และ HMAC_DRBG ○ CRT_DRBG โดยใช้ AES-128, AES-192 และ AES-256		

✓ จำเป็น ○ ทางเลือก

```
"MessageStatus":{
        {
                "status":"400",
                "description":"Bad Request",
                "error": {
                        "code": "xxxx",
                        "message": "The specified data could not be decrypted"
                }
        }
}
```

รูปที่ 4 ตัวอย่าง error message ที่ตอบกลับเมื่อพบปัญหาการถอดรหัส

```
"MessageStatus":{
      {
              "status":"400",
              "description":"Bad Request",
              "error": {
                      "code": "xxxx",
                      "message": "The specified data could not be decrypted (JWT Signature)"
              }
      }
}
```

รูปที่ 5 ตัวอย่าง error message ที่ตอบกลับเมื่อพบปัญหาการถอดรหัส JWT

4.2.3. ข้อกำหนดการจำกัดอัตราการเข้าถึงบริการและใช้ทรัพยากร

การจำกัดอัตราการเข้าถึงบริการและใช้ทรัพยากรของมาตรฐาน TGIX จะมุ่งเน้นไปยังส่วน ของผู้ให้บริการ เพื่อให้เป็นไปตามข้อแนวทางการปฏิบัติที่ดีทางด้านความปลอดภัยของการให้บริการการแลกเปลี่ยนข้อมูล ผู้ให้บริการจะต้องจัดให้มีการควบคุมอัตราการเข้าถึงบริการและการใช้ทรัพยากรของระบบของผู้ให้บริการ [7] โดยทั้งผู้ให้บริการจะต้องสามารถกำหนดการจำกัดได้อย่างน้อยดังตารางที่ 3

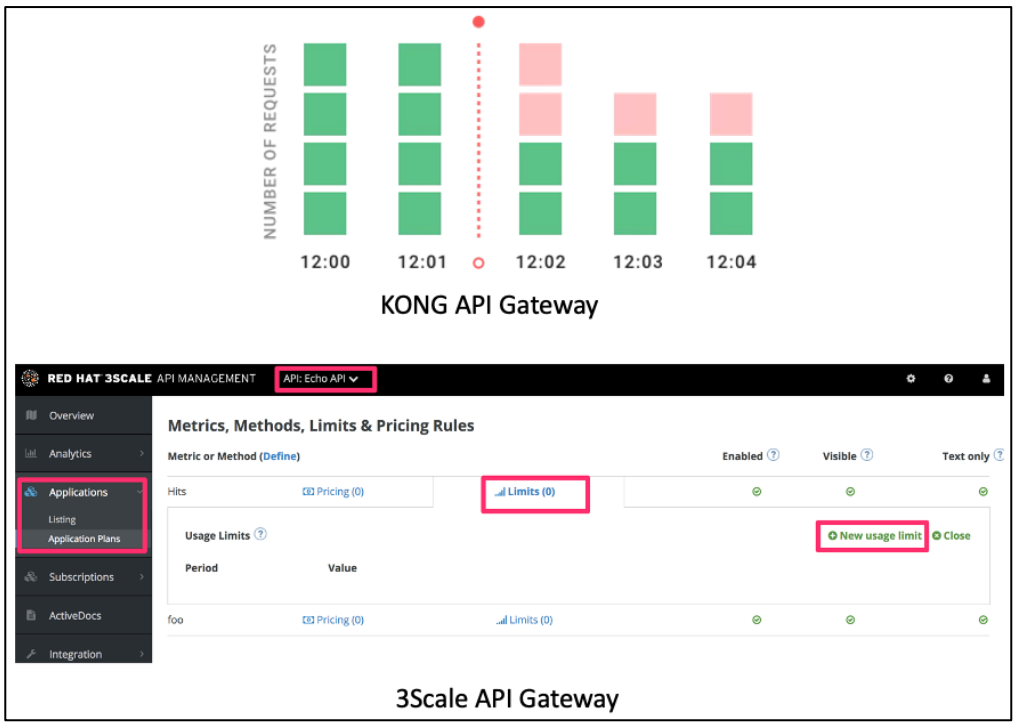
ตารางที่ 3 ข้อกำหนดการจำกัดอัตราการเข้าถึงบริการและใช้ทรัพยากรของผู้ให้บริการ

ข้อกำหนดการจำกัดอัตราการเข้าถึงบริการและใช้ทรัพยากร	ข้อกำหนดที่แนะนำ	ข้อกำหนดที่ต้องการ
● สามารถจำกัดเวลาการทำงานของบริการได้ (Execution timeouts) โดยควรกำหนดค่าตั้งต้นของขนาดสูงสุดของเวลาการทำงาน (Execution timeout) ไว้ที่ 60 วินาที หรือสามารถปรับเปลี่ยนได้ตามความเหมาะสมของการให้บริการ โดยสามารถเลือกดำเนินการได้จาก ○ การพัฒนาด้วยภาษาโปรแกรมของ Provider System ○ การระบุไว้ที่ Web Server หรือ Application Server ของ Provider System ○ การใช้ API Gateway เข้ามาช่วยดำเนินการ ○ อื่นๆ ตามความเหมาะสม	✓	✓
● สามารถจำกัดขนาดของข้อความในการร้องขอบริการได้ (Request payload size) โดยควรกำหนดค่าตั้งต้นของขนาดสูงสุดของข้อความร้องขอบริการ (Request payload size) ไว้ที่ 5 MB (Megabytes) หรือสามารถปรับเปลี่ยนได้ตามความเหมาะสมของการให้บริการ โดยสามารถเลือกดำเนินการได้จาก ○ การพัฒนาด้วยภาษาโปรแกรมของ Provider System ○ การระบุไว้ที่ Web Server หรือ Application Server ของ Provider System ○ การใช้ API Gateway เข้ามาช่วยดำเนินการ ○ อื่นๆ ตามความเหมาะสม	✓	✓

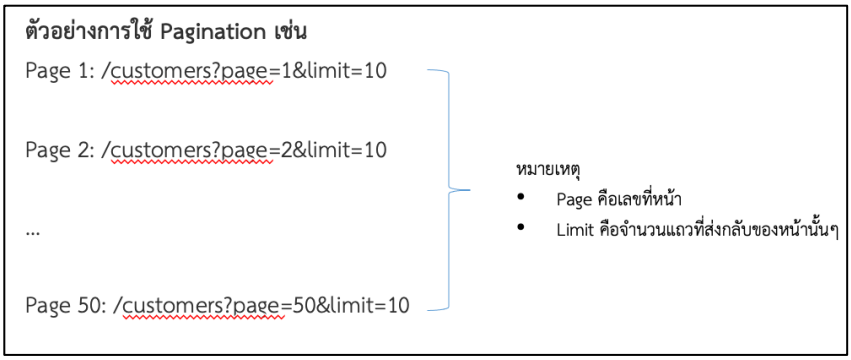
ตารางที่ 3 ข้อกำหนดการจำกัดอัตราการเข้าถึงบริการและใช้ทรัพยากรของผู้ให้บริการ (ต่อ)

ข้อกำหนดการจำกัดอัตราการเข้าถึงบริการและใช้ทรัพยากร	ข้อกำหนดที่แนะนำ	ข้อกำหนดที่ต้องการ
• สามารถจำกัดจำนวนการร้องขอบริการต่อผู้ขอใช้บริการหรือบริการได้ (Number of requests per client/resource) โดยผู้ให้บริการทำการประเมินจากทรัพยากรและประสิทธิภาพที่จะให้บริการได้กับความต้องการใช้บริการของผู้ใช้บริการโดยสามารถเลือกดำเนินการได้จากตัวอย่างการ Implementation สามารถใช้เครื่องมือที่เป็นลักษณะ API Gateway ช่วยในการสามารถจำกัดเวลาการทำงานของบริการได้ (Execution timeouts) ดังตัวอย่างรูปที่ 6**Error! Reference source not found.**	✓	○
• สามารถจำกัดจำนวนแถวข้อมูลต่อหน้าที่จะส่งกลับไปยังผู้ร้องขอบริการและตอบกลับต่อหนึ่งการร้องขอ (Number of records per page to return in a single request response) ดังตัวอย่างรูปที่ 7 ตัวอย่างการดำเนินการทำ Pagination เพื่อจำกัดจำนวนแถวข้อมูลต่อหน้าที่จะส่งกลับไปยังผู้ร้องขอบริการดัง**Error! Reference source not found.** มีจุดประสงค์เพื่อ 1. ให้การตอบกลับของ API ใช้เวลาน้อยเช่น < 2 วินาที เป็นต้น 2. ต้องการให้จำนวนข้อมูลที่ส่งกลับใน Payload มีความเหมาะสม เช่น < 500kb เป็นต้น	✓	○

○ เลือกดำเนินการ ✓ต้องดำเนินการ



รูปที่ 6 ตัวอย่างการดำเนินการ Rate Limit ด้วย API Gateway เช่น KONG, 3Scale เป็นต้น



รูปที่ 7 ตัวอย่างการดำเนินการทำ Pagination เพื่อจำกัดจำนวนแถวข้อมูลต่อหน้าที่จะส่งกลับไปยังผู้ร้องขอบริการ

4.2.4. ข้อกำหนดการบันทึกกิจกรรมและข้อมูลล็อกและการตรวจสอบ (Logging & Monitoring)

เพื่อให้เป็นไปตามแนวทางการปฏิบัติที่ดีทางด้านความปลอดภัยของการให้บริการการแลกเปลี่ยนข้อมูล ผู้ให้บริการจะต้องจัดให้มีการบันทึกข้อมูลล็อกและการตรวจสอบโดยผู้ให้บริการจะต้องมีการปฏิบัติตามข้อกำหนด ซึ่งกล่าวใน มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่องข้อกำหนดของการตรวจสอบระบบและการลงบันทึกล็อก

4.2.5. ข้อกำหนดการจัดการความผิดพลาด (Error handling)

เพื่อให้เป็นไปตามข้อแนวทางการปฏิบัติที่ดีทางด้านความปลอดภัยของการให้บริการการแลกเปลี่ยนข้อมูล เมื่อบริการที่เปิดให้บริการแสดงข้อความการทำงานผิดพลาด จะต้องไม่เปิดเผยข้อมูลที่มีความเสี่ยงที่สามารถนำมาโจมตีระบบได้ โดยผู้ให้บริการจะต้องจัดให้มีการจัดการข้อผิดพลาดอย่างเหมาะสมอย่างน้อยดังตารางที่ 4 Error! Reference source not found.

ตารางที่ 4 ข้อกำหนดการจัดการความผิดพลาด (Error handling) ของผู้ให้บริการ

ข้อกำหนดการจัดการความผิดพลาด (Error handling)	ข้อกำหนดที่แนะนำ	ข้อกำหนดที่ต้องการ
● บริการจะต้องปกปิดรหัสหรือข้อความแสดงข้อผิดพลาดอื่นใดนอกเหนือจากสถานะตอบกลับหรือข้อความแสดงข้อผิดพลาดของ HTTP (HTTP status responses และ HTTP error messages) เช่น ไม่ควรแสดงข้อมูลระดับระบบ (System level) ไปในข้อผิดพลาดที่ตอบกลับ ดังตัวอย่างรูปที่ 8 [8]	✓	✓
● บริการจะต้องไม่ส่งรายละเอียดข้อผิดพลาดทางเทคนิคไปยังผู้ขอใช้บริการ เช่น ไม่ควรแสดงข้อความข้อผิดพลาดของลำดับการเรียกของระบบ (Call stacks) หรือข้อความข้อผิดพลาดของคำสั่งเรียกฐานข้อมูล	✓	✓

○ เลือกดำเนินการ ✓ต้องดำเนินการ

```
"messageStatus":            // Require: only response message.
{
    "status": "",           // Require: [HTTP status: 200,401,...other code]
    "description": "",      // Require: Description or information for status
    "error": {              // Require: only provider return error
        "code": "",         // Require: Reference error code
        "message": ""       // Require: Error message
    }
}
```

รูปที่ 8 ตัวอย่างส่วนของ messageStatus ที่อยู่ใน TGIX JSON Data Format ใช้เพื่อสถานะตอบกลับหรือข้อความแสดงข้อผิดพลาดของ HTTP

4.2.6. ข้อกำหนดการตรวจสอบข้อมูลนำเข้า (Input Validation)

เพื่อให้เป็นไปตามข้อแนวทางการปฏิบัติที่ดีทางด้านความปลอดภัยของการให้บริการการแลกเปลี่ยนข้อมูล การตรวจสอบข้อมูลที่จะนำเข้าสู่ระบบจะช่วยให้มั่นใจได้ว่าข้อมุลที่จะเข้าสู่ระบบอยู่ในรูปแบบที่เหมาะสม ซึ่งจะช่วยป้องกันการถูกโจมตีระบบได้ โดยผู้ให้บริการจะต้องจัดให้มีการตรวจสอบข้อมูลนำเข้าอย่างเหมาะสมอย่างน้อยดังตารางที่ 5**Error! Reference source not found.**

ตารางที่ 5 ข้อกำหนดการตรวจสอบข้อมูลนำเข้า (Input Validation) ของผู้ให้บริการ

ข้อกำหนดการตรวจสอบข้อมูลนำเข้า (Input Validation)	ข้อกำหนดที่แนะนำ	ข้อกำหนดที่ต้องการ
● การตรวจสอบข้อมูลนำเข้าควรจะกระทำเป็นลำดับแรกสุดเท่าที่จะทำได้นับตั้งแต่ได้รับข้อมูลเข้ามาจากระบบภายนอก	✓	✓
● กำหนดการจำกัดขนาดของข้อมูลนำเข้าที่เหมาะสมและปฏิเสธข้อมูลนำเข้าที่มีขนาดเกินที่กำหนดไว้	✓	✓
● ออกแบบและพัฒนาระบบให้ตรวจสอบข้อมูลนำเข้า โดยตรวจสอบเช่น ขนาดความยาว ช่วงของข้อมูล รูปแบบข้อมูล และประเภทข้อมูล ให้ตรงตามข้อกำหนดทางเทคนิคของบริการนั้นที่กำหนดไว้ดังตัวอย่างในรูปที่ 9**Error! Reference source not found.**	✓	✓
● ออกแบบและพัฒนาระบบให้ตรวจสอบบันทึกกิจกรรมและข้อมูลจราจรคอมพิวเตอร์ที่ไม่ผ่านการตรวจสอบข้อมูลนำเข้า (Logging input validation) เพื่อเป็นการสอดส่องความพยายามตรวจสอบข้อมูลนำเข้าที่ไม่ผ่านและมีมากผิดปกติในช่วงเวลาสั้น ๆ ซึ่งอาจจะเป็นการพยายามโจมตีระบบ	○	○
● จำกัดข้อมูลนำเข้าให้อยู่ในรูปแบบที่เหมาะสมกับประเภทข้อมูลตามข้อกำหนดทางเทคนิคของบริการนั้นด้วยการตรวจสอบด้วยนิพจน์ปกติ (Regular Expression) ดังตัวอย่างในรูปที่ 10Error! Reference source not found.	✓	✓

○ เลือกดำเนินการ ✓ต้องดำเนินการ

```
"error": {
        "code": "19284",
        "message": "Input value(s) exceeded maximum length",
        "source": {
            "parameter": "last_name"
        }
}
```

รูปที่ 9 ตัวอย่างการตอบกลับเมื่อดำเนินการตรวจสอบแล้วพบข้อผิดพลาด

```
function escapeRegExp(string) {
  return string.replace(/[.*+?^${}()|[\]\\]/g, '\\$&');
}
```

รูปที่ 10 ตัวอย่างการใช้ Regular Expression ในการตรวจสอบอักขระพิเศษ

4.2.7. ข้อกำหนดเกี่ยวกับการป้องกันการโจมตี

เพื่อให้เป็นไปตามข้อแนวทางการปฏิบัติที่ดีทางด้านความปลอดภัยของการให้บริการการแลกเปลี่ยนข้อมูล การป้องกันการโจมตีจะช่วยให้มั่นใจได้ว่าระบบจะมีความพร้อมให้บริการตามข้อตกลงบริการ (Service Agreement) และป้องกันความเสียหายจากข้อมูลที่รั่วไหล โดยผู้ให้บริการจะต้องจัดให้มีการดำเนินการป้องกันการโจมตีอย่างเหมาะสมอย่างน้อยดังตารางที่ 6 **Error! Reference source not found.**

ตารางที่ 6 ข้อกำหนดเกี่ยวกับการป้องกันการโจมตีของผู้ให้บริการ

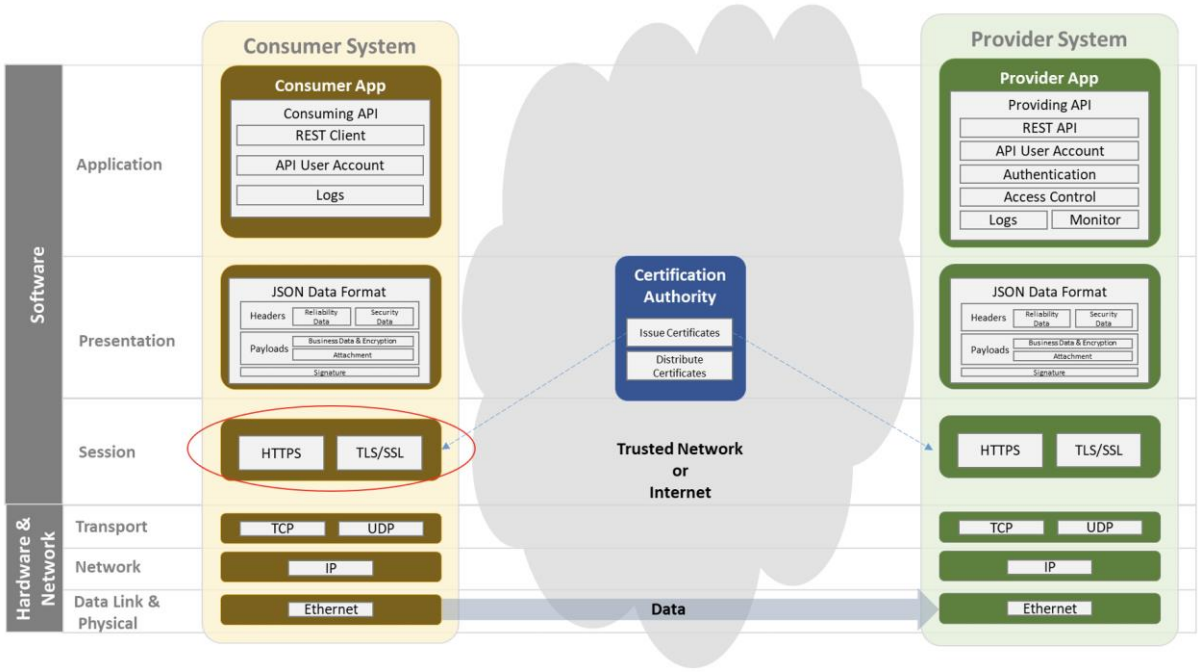
ข้อกำหนดการป้องกันการโจมตีของผู้ให้บริการ	ข้อกำหนดที่แนะนำ	ข้อกำหนดที่ต้องการ
● จัดให้มี Endpoint Mapping โดยที่ผู้ให้บริการทำการเปิด Public Endpoint ของ API ให้ผู้ใช้บริการใช้งาน โดยที่ผู้ใช้บริการไม่ทราบ Endpoint ที่แท้จริงของ API ที่ Provider สร้างขึ้น โดยสามารถเลือกดำเนินการได้จากการใช้ API Gateway หรือสิ่งที่ทำหน้าที่ได้เทียบเท่าเข้ามาช่วยดำเนินการ	✓	○
● จัดทำ IP Access Control โดยการอนุญาตให้เฉพาะระบบของผู้ใช้บริการ หรือเฉพาะ IP Address หรือ Domain ที่กำหนดเท่านั้นที่เรียกใช้ API ได้ โดยสามารถเลือกดำเนินการได้จากการใช้ API Gateway หรือสิ่งที่ทำหน้าที่ได้เทียบเท่าเข้ามาช่วยดำเนินการ	✓	○
● จัดทำ Threat Protection เพื่อการป้องกันไม่ให้มีการโจมตี API จากผู้ใช้งานที่ไม่พึงประสงค์ ก่อนที่ Request ไปถึงยังระบบของผู้ให้บริการ โดยสามารถเลือกดำเนินการได้จากการใช้ API Gateway หรือสิ่งที่ทำหน้าที่ได้เทียบเท่าเข้ามาช่วยดำเนินการ	✓	○

○ เลือกดำเนินการ ✓ต้องดำเนินการ

4.3. ข้อกำหนดด้านความปลอดภัยของผู้ใช้บริการ (Consumer)

4.3.1. ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security)

ความปลอดภัยของการส่งข้อมูล (Transport Security) ของมาตรฐาน TGIX ของผู้ใช้บริการจะมุ่งเน้นไปการส่งข้อความในระดับ Session ของผู้ใช้บริการ ในองค์ประกอบของการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐของผู้ใช้บริการดังรูปที่ 11



รูปที่ 11 องค์ประกอบที่เกี่ยวข้องกับความปลอดภัยของการส่งข้อมูลของผู้ใช้บริการการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ

เพื่อให้การรับส่งข้อมูลสำหรับบริการการแลกเปลี่ยนข้อมูลมีความปลอดภัยและเป็นไปตามข้อกำหนดพื้นฐานด้านความปลอดภัย การสื่อสารเพื่อรับส่งข้อมูลของมาตรฐาน TGIX ของผู้ใช้บริการจะต้องเป็นไปตามข้อกำหนดโดยมีรายละเอียดดังตารางที่ 7

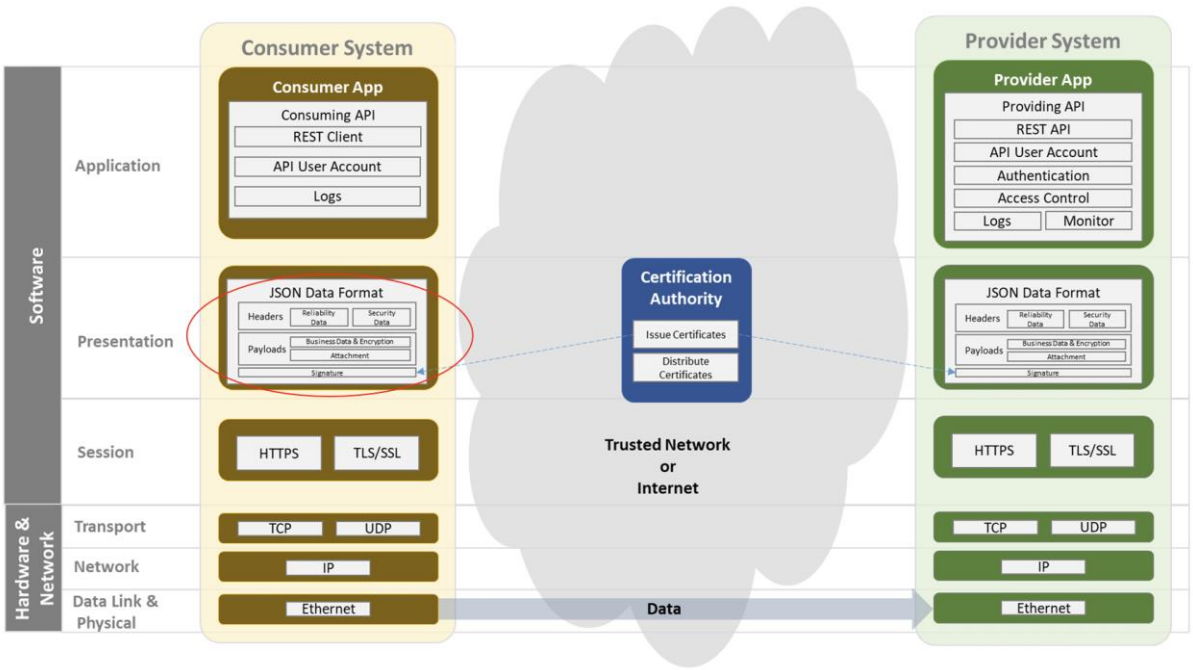
ตารางที่ 7 ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security) ของผู้ใช้บริการ

ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security)	ข้อกำหนดที่แนะนำ	ข้อกำหนดที่ต้องการ
• การส่งข้อมูลจะต้องดำเนินการบน HTTPS โดยใช้ TLS 1.2 เป็นอย่างน้อย	✓	✓
• ใบรับรอง (Certificates) จะต้องมีการเข้ารหัสแฮชฟังก์ชัน (Hash Functions) แบบ SHA-2 (Secure Hash Algorithm 2) ด้วยความยาวกุญแจ (Key size) อย่างน้อย 2048 bits	✓	✓
• ทุกปลายทาง (Endpoint) จะต้องใช้ใบรับรองดิจิทัล (Digital Certificate) ที่ออกโดยหน่วยงานที่ดูแลใบรับรองดิจิทัลที่ได้รับอนุญาต	✓	○

○ เลือกดำเนินการ ✓ต้องดำเนินการ

4.3.2. ข้อกำหนดการเข้ารหัส (Encryption)

การเข้ารหัสข้อมูลของผู้ใช้บริการในกรณีที่ต้องมีการเข้ารหัสข้อมูล เช่น ข้อมูลที่มีความสำคัญที่เป็นข้อมูลเชิงธุรกรรมที่ Payload ข้อมูลลายเซ็นในส่วน Signature หรือข้อมูล Token ที่อยู่ในส่วน Header เป็นต้น การเข้ารหัสข้อมูล (Encyption) ของมาตรฐาน TGIX จะมุ่งเน้นไปยังส่วน Presentation ของผู้ใช้บริการ ในองค์ประกอบของการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐของผู้ใช้บริการดังรูปที่ 12



รูปที่ 12 องค์ประกอบที่เกี่ยวข้องกับความปลอดภัยของการเข้ารหัสของผู้ใช้บริการการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ

เพื่อให้เป็นไปตามข้อกำหนดพื้นฐานด้านความปลอดภัย การเข้ารหัสข้อมูล (Encyption) ของมาตรฐาน TGIX ของผู้ใช้บริการจะต้องเป็นไปตามข้อกำหนดโดยมีรายละเอียดดังนี้

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

(2) สำหรับการลงลายมือชื่อดิจิทัล เพื่อการรับประกันการยืนยันตัวตนของต้นทางและความถูกต้องของข้อมูลจะต้องใช้อัลกอลิธึมตามข้อตกลงการใช้บริการ (Service Agreement) ที่ทำร่วมกับผู้ให้บริการ

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

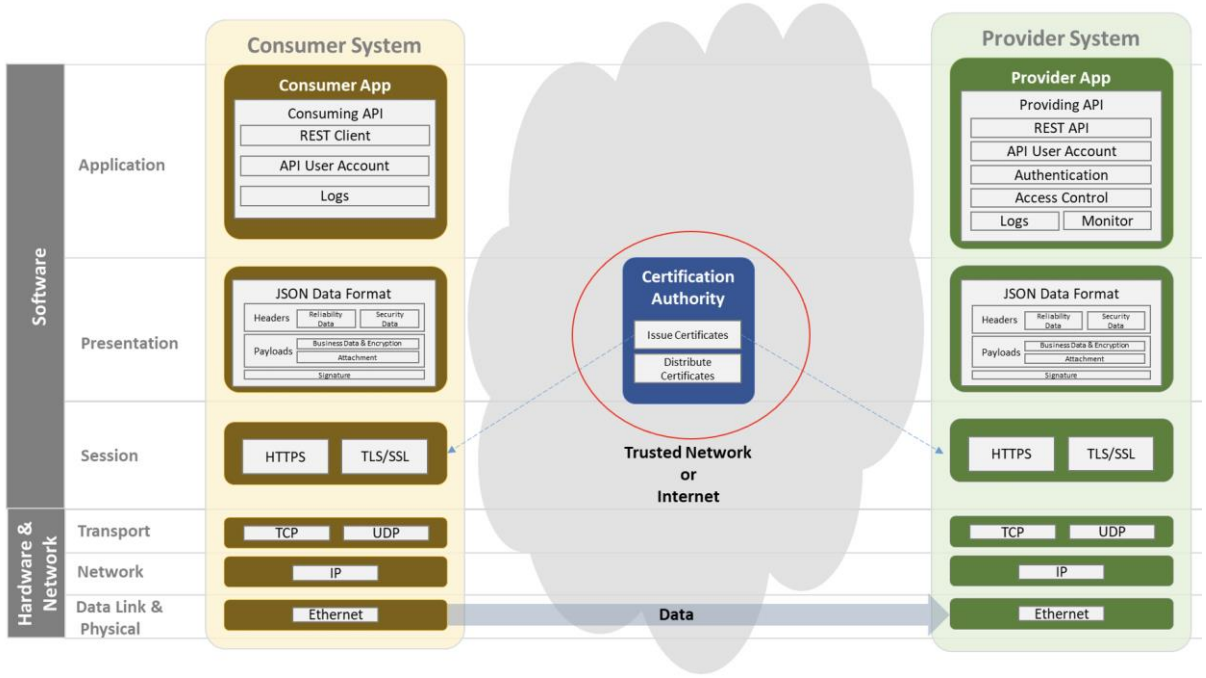
4.3.3. ข้อกำหนดการบันทึกกิจกรรมและข้อมูลล็อกและการตรวจสอบ (Logging & Monitoring)

เพื่อให้เป็นไปตามแนวทางการปฏิบัติที่ดีทางด้านความปลอดภัยของการใช้บริการการแลกเปลี่ยนข้อมูล ผู้ใช้บริการจะต้องจัดให้มีการบันทึกข้อมูลล็อกและการตรวจสอบ โดยผู้ใช้บริการจะต้องมีการปฏิบัติตามข้อกำหนดซึ่งกล่าวใน มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่อง ข้อกำหนดของการตรวจสอบระบบและการลงบันทึกล็อก

4.4. ข้อกำหนดด้านความความปลอดภัยขององค์ประกอบอื่นๆ ตามมาตรฐาน TGIX

4.4.1. ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security)

ความปลอดภัยของการส่งข้อมูล (Transport Security) ของมาตรฐาน TGIX ของ Certification Authority จะทำหน้าที่ออกใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) ในองค์ประกอบของการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐของผู้ใช้บริการดังรูปที่ 13



รูปที่ 13 องค์ประกอบที่เกี่ยวข้องกับความปลอดภัยของการส่งข้อมูลของ Certification Authority ในการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ

เพื่อให้การรับส่งข้อมูลสำหรับบริการการแลกเปลี่ยนข้อมูลมีความปลอดภัยและเป็นไปตามข้อกำหนดพื้นฐานด้านความปลอดภัย การสื่อสารเพื่อรับส่งข้อมูลของมาตรฐาน TGIX ของ Certification Authority จะต้องเป็นไปตามข้อกำหนดโดยมีรายละเอียดดังนี้ [3]

(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 ใบรับรองอิเล็กทรอนิกส์สำหรับเครื่อง 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 การลงลายมือชื่อดิจิทัล หรือข้อมูล Token ที่อยู่ในส่วน Header เป็นต้น เพื่อให้เป็นไปตามข้อกำหนดพื้นฐานด้านความปลอดภัย การเข้ารหัสข้อมูล (Encyption) ของ Certification Authority จะต้องเป็นไปตามข้อกำหนดโดยมีรายละเอียดดังนี้ [3]

(1) สำหรับการลงลายมือชื่อดิจิทัล เพื่อการรับประกันการยืนยันตัวตนของต้นทางและความถูกต้องของข้อมูลจะต้องใช้อัลกอลิธึมแบบใดแบบหนึ่งดังต่อไปนี้

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

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

   ค. อัลกอลิธึม RSA (Rivest-Shamir-Adelman algorithm) โดยมีขนาดของ Security of strength อย่างน้อย 112 bits และ Domain Parameter อย่างน้อย 2048 bits

(2) สำหรับการสร้างหรือตรวจสอบลายมือชื่อดิจิทัลโดยใช้แฮชฟังก์ชัน (Hash Function) จะต้องใช้ฟังก์ชันแบบใดแบบหนึ่งดังต่อไปนี้

   ก. SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 และ SHA-512/256)

   ข. SHA-3 (SHA3-224, SHA3-256, SHA3-384 และ SHA3-512)

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

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

   ก. Hash_DRBG และ HMAC_DRBG

   ข. CRT_DRBG โดยใช้ AES-128, AES-192 และ AES-256

4.4.3. ข้อกำหนดการบันทึกกิจกรรมและข้อมูลล็อกและการตรวจสอบ (Logging & Monitoring)

เพื่อให้เป็นไปตามแนวทางการปฏิบัติที่ดีทางด้านความปลอดภัยของการให้บริการการแลกเปลี่ยนข้อมูล Certification Authority จะต้องจัดให้มีการบันทึกข้อมูลล็อกและการตรวจสอบ โดยของ Certification Authority จะต้องมีการปฏิบัติตามข้อกำหนดซึ่งกล่าวใน มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่องข้อกำหนดของการตรวจสอบระบบและการลงบันทึกล็อก

4.4.4. ข้อกำหนดการจัดการความผิดพลาด (Error handling)

เพื่อให้เป็นไปตามข้อแนวทางการปฏิบัติที่ดีทางด้านความปลอดภัยของการให้บริการการแลกเปลี่ยนข้อมูล เมื่อบริการที่เปิดให้บริการแสดงข้อความการทำงานผิดพลาด จะต้องไม่เปิดเผยข้อมูลที่มีความเสี่ยงที่สามารถนำมาโจมตีระบบได้ โดย ของ Certification Authority จะต้องจัดให้มีการจัดการข้อผิดพลาดอย่างเหมาะสมอย่างน้อยดังนี้ [3]

(1) บริการจะต้องปกปิดรหัสหรือข้อความแสดงข้อผิดพลาดอื่นใดนอกเหนือจากสถานะตอบกลับหรือข้อความแสดงข้อผิดพลาดของ HTTP (HTTP status responses และ HTTP error messages) [8] เช่น ไม่ควรแสดงข้อมูลระดับระบบ (System level) ไปในข้อผิดพลาดที่ตอบกลับ

```
"messageStatus":            // Require: only response message.
{
    "status": "",           // Require: [HTTP status: 200,401,...other code]
    "description": "",      // Require: Description or information for status
    "error": {              // Require: only provider return error
        "code": "",         // Require: Reference error code
        "message": ""       // Require: Error message
    }
}
```

รูปที่ 14 ตัวอย่างส่วนของ messageStatus ที่อยู่ใน TGIX JSON Data Format ใช้เพื่อสถานะตอบกลับหรือข้อความแสดงข้อผิดพลาดของ HTTP

(2) บริการจะต้องไม่ส่งรายละเอียดข้อผิดพลาดทางเทคนิคไปยังผู้ขอใช้บริการ เช่น ไม่ควรแสดงข้อความข้อผิดพลาดของลำดับการเรียกของระบบ (Call stacks) หรือข้อความข้อผิดพลาดของคำสั่งเรียกฐานข้อมูล

ภาคผนวก ก. ข้อแนะนำด้านความปลอดภัยที่เกี่ยวข้องกับกฎหมาย

ก.1 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ PDPA (Personal Data Protection Act) เป็นกฎหมายที่เกี่ยวข้องกับการรักษาและปกป้องข้อมูลส่วนบุคคล ซึ่งเป็นหนึ่งในแนวทางการปฏิบัติที่ดีทางด้านความปลอดภัย ข้อมูลส่วนบุคคลและความเป็นส่วนตัวเกี่ยวข้องกับข้อมูลที่สามารถระบุตัวตนได้ไม่ว่าจะเป็นข้อมูลอะไรก็ตามที่สามารถระบุตัวบุคคลได้

การแลกเปลี่ยนข้อมูลของ TGIX จะต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 [10] ที่กำหนดไว้ว่าจะต้องมีการปฏิบัติอย่างไรกับข้อมูลส่วนบุคคล รวมถึงการเก็บรักษา การบันทึก การจัดการ การเปลี่ยนแปลง การเปิดเผย การจัดการสิทธิ์การเข้าถึงข้อมูลส่วนบุคคล การเรียกคืนข้อมูลส่วนบุคคล การปกปิด การลบ การทำลาย หรือการกระทำอื่นใดที่กล่าวถึงข้างต้นโดยไม่คำนึงถึงลักษณะการดำเนินงานหรือวิธีการที่ใช้

กรณีที่การแลกเปลี่ยนข้อมูลเกี่ยวข้องกับการจัดเก็บหรือส่งผ่านข้อมูลส่วนบุคคลจะต้องจัดให้มีการดำเนินการดังตัวอย่างเช่น

(1) ออกแบบและพัฒนาระบบให้รองรับการร้องขอและจัดเก็บความยินยอมจากเจ้าของข้อมูลในกรณีมีการร้องขอข้อมูลส่วนบุคคล
(2) ออกแบบและพัฒนาระบบให้รองรับขอเปลี่ยนแปลงความยินยอมจากเจ้าของข้อมูลเพื่อรองรับสิทธิ์ของเจ้าของข้อมูลตามกฎหมาย
(3) ระมัดระวังในการออกแบบและพัฒนาระบบให้มีการจัดเก็บข้อมูลเท่าที่จำเป็นเท่านั้น

เมื่อพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 [10] ถูกบังคับใช้ สมาชิกภายใน TGIX จะต้องผู้รับผิดชอบในการดำเนินการและบำรุงรักษาระบบและส่วนที่เกี่ยวข้องให้เป็นไปตามข้อกำหนดของกฎหมาย

ก.2 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 [11] เป็นกฎหมายที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ตั้งขึ้นเพื่อป้องกันและควบคุมการกระทำผิดที่จะเกิดขึ้นจากการใช้คอมพิวเตอร์ การปฏิบัติตามกฎหมายครอบคุมทั้งผู้ให้บริการ ผู้ใช้บริการ และองค์ประกอบอื่นตามมาตรฐาน TGIX จะต้องจัดให้มีการดำเนินการดังตัวอย่างเช่น

(1) การนำเข้าข้อมูลเพื่อแลกเปลี่ยนข้อมูลภายในมาตรฐาน TGIX ผู้นำเข้าข้อมูลต้องไม่นำเข้าข้อมูลอันเป็นเท็จหรือข้อมูลอื่นใดที่ขัดต่อพระราชบัญญัตินี้

(2) การให้บริการหรือเผยแพร่ข้อมูลภายในมาตรฐาน TGIX ผู้ให้บริการต้องไม่ให้บริการหรือเผยแพร่ข้อมูลอันเป็นเท็จหรือข้อมูลอื่นใดที่ขัดต่อพระราชบัญญัตินี้

ก.3 หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564

หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564 [12] เป็นหลักเกณฑ์ที่กำหนดแนวทางในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ตามกฎหมายในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งรายละเอียดข้อกำหนดของ TGIX ที่เกี่ยวกับการบันทึกล็อก จะกล่าวในมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่องข้อกำหนดของการตรวจสอบระบบและการลงบันทึกล็อก

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]. เข้าถึงได้จาก: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.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] สำนักงานคณะกรรมการกฤษฎีกา. (2017, มกราคม). พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (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 Bit Generators. [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: 9 กันยายน 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)