มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

DGA Community Standard

มสพร. 10-4 : 2566

DGA 10-4 : 2566

ว่าด้วย มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่องข้อกำหนดด้านความน่าเชื่อถือและความมั่นคงปลอดภัย

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

เวอร์ชัน 1.0

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
สำนักนายกรัฐมนตรี

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ว่าด้วย มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่องข้อกำหนดด้านความน่าเชื่อถือและความมั่นคงปลอดภัย

มสพร. 10-4 : 2566

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ชั้น 17 อาคารบางกอกไทยทาวเวอร์

108 ถนนรางน้ำ แขวงถนนพญาไท เขตราชเทวี กรุงเทพฯ 10400

หมายเลขโทรศัพท์: (+66) 0 2612 6000 โทรสาร: (+66) 0 2612 6011

ประกาศโดย

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

สำนักนายกรัฐมนตรี

วันที่ 31 พฤษภาคม 2566

คณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 ตามคำสั่งที่ 66/2564 ลงวันที่ 20 ตุลาคม 2564

ประธานกรรมการ

ผู้ช่วยศาสตราจารย์ภุชงค์ อุทโยภาศ	มหาวิทยาลัยเกษตรศาสตร์

รองประธานกรรมการ

นางไอรดา เหลืองวิไล	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

กรรมการ

นายเฉลิมชัย ก๊กเกียรติกุล	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ
นายมารุต บูรณรัช	ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
นายศุภโชค จันทรประทิน	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นางบุญยิ่ง ชั่งสัจจา	สำนักบริหารการทะเบียน กรมการปกครอง
นายณัฏฐา พาชัยยุทธ	สำนักงานคณะกรรมการพัฒนาระบบราชการ
นายพัชโรดม ลิมปิษเฐียร	สำนักงานคณะกรรมการกฤษฎีกา
นายธีรวุฒิ ธงภักดิ์	สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ
นายสันติ สิทธิเลิศพิศาล	สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม
นายวีระ วีระกุล	ผู้แทนสภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย
นายวิทยา สุหฤทดำรง	วิศวกรรมสถานแห่งประเทศไทย
รองศาสตราจารย์เกริก ภิรมย์โสภา	ประธานคณะทำงานเทคนิคด้านมาตรฐานความมั่นคงปลอดภัยภาครัฐ
รองศาสตราจารย์ธีรณี อจลากุล	ประธานคณะทำงานเทคนิคด้านมาตรฐานการบริหารจัดการข้อมูลภาครัฐ
ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูไพโรจน์	ประธานคณะทำงานเทคนิคด้านมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ

กรรมการและเลขานุการ

นางสาวอุรัชฎา เกตุพรหม	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 ตามคำสั่งที่ 82/2565 ลงวันที่ 31 ตุลาคม 2565

ที่ปรึกษา

นายสุพจน์ เธียรวุฒิ	ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

ประธานกรรมการ

ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูไพโรจน์	จุฬาลงกรณ์มหาวิทยาลัย

รองประธานกรรมการ

นายอาศิส อัญญะโพธิ์	ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

กรรมการ

นายเฉลิมชัย ก๊กเกียรติกุล	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ
นายมารุต บูรณรัช	ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
นางสาวขนิษฐ์ ผาทอง	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นางบุญยิ่ง ชั่งสัจจา	สำนักบริหารการทะเบียน กรมการปกครอง
นายเกียรติชัย ชุ่มมงคล	
นายณัฏฐา พาชัยยุทธ	สำนักงานคณะกรรมการพัฒนาระบบราชการ
นายพัชโรดม ลิมปิษเฐียร	สำนักงานคณะกรรมการกฤษฎีกา
นายธีรวุฒิ ธงภักดิ์	สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ
นายกฤษณ์ โกวิทพัฒนา	
นางสาวเกศินี ทองชูศักดิ์	
นายสันติ สิทธิเลิศพิศาล	สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม
นายวีระ วีระกุล	สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย
นายวิทยา สุหฤทดำรง	วิศวกรรมสถานแห่งประเทศไทย
นายคณพศ หงสาวรางกูร	สำนักงานการตรวจเงินแผ่นดิน
รองศาสตราจารย์เกริก ภิรมย์โสภา	ประธานคณะทำงานเทคนิคด้านมาตรฐานความมั่นคงปลอดภัยภาครัฐ
รองศาสตราจารย์ธีรณี อจลากุล	ประธานคณะทำงานเทคนิคด้านมาตรฐานการบริหารจัดการข้อมูลภาครัฐ
ผู้ช่วยศาสตราจารย์มารอง ผดุงสิทธิ์	ประธานคณะทำงานเทคนิคด้านมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ

กรรมการและเลขานุการ

นางสาวอุรัชฎา เกตุพรหม สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะทำงานเทคนิคด้านมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ตามคำสั่งที่ 69/2564 ลงวันที่ 20 ตุลาคม 2564

ที่ปรึกษา

นายสุพจน์ เธียรวุฒิ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ผู้ช่วยศาสตราจารย์ภุชงค์ อุทโยภาศ มหาวิทยาลัยเกษตรศาสตร์

นางไอรดา เหลืองวิไล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ประธานคณะทำงาน

ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูไพโรจน์ จุฬาลงกรณ์มหาวิทยาลัย

รองประธานคณะทำงาน

ผู้ช่วยศาสตราจารย์มารอง ผดุงสิทธิ์ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี

คณะทำงาน

นางบุญยิ่ง ชั่งสัจจา กรมการปกครอง

นางสาวมนทิพา เข่งพิมล กรมพัฒนาธุรกิจการค้า

นายพงศกร ริยะมงคล

นายกำชัย จัตตานนท์ ผู้แทนกรมศุลกากร

นางบุษยา ดวงตา

นางสาวขนิษฐา สหเมธาพัฒน์ กรมสรรพากร

นายยุทธพล จินะสี

นางสาวภัทราพรรณ วงศาโรจน์ ธนาคารแห่งประเทศไทย

นายยรรยง ดำรงศิริ

นางสาวจิตสุภา วิระยะวานิช

นายกิตติพงษ์ สุขสม

นายพิสุทธิ นาคหมื่นไวย สำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ (องค์การมหาชน)

นางศุปกิจ สกลเสาวภาคย์ กรมที่ดิน

นางตวงรัตน์ จันทรประดิษฐ์

นายอาศิส อัญญะโพธิ์ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

นายมนต์ศักดิ์ โซ่เจริญธรรม สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะทำงานและเลขานุการ

นางสาวอุรัชฎา เกตุพรหม สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะทำงานเทคนิคด้านมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ตามคำสั่งที่ 85/2565 ลงวันที่ 31 ตุลาคม 2565

ที่ปรึกษา

นายสุพจน์ เธียรวุฒิ	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูไพโรจน์	จุฬาลงกรณ์มหาวิทยาลัย
นายอาศิส อัญญะโพธิ์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ประธานคณะทำงาน

ผู้ช่วยศาสตราจารย์มารอง ผดุงสิทธิ์	มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี

รองประธานคณะทำงาน

นางสาวยศวลัย โชติปทุมวรรณ	มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

คณะทำงาน

นางบุญยิ่ง ชั่งสัจจา	กรมการปกครอง
นางสาวมนทิพา เข่งพิมล	กรมพัฒนาธุรกิจการค้า
นายพงศกร ริยะมงคล	
นายกำชัย จัตตานนท์	กรมศุลกากร
นางบุษยา ดวงตา	
นางสาวขนิษฐา สหเมธาพัฒน์	กรมสรรพากร
นายยุทธพล จินะสี	
นางสาวภัทราพรรณ วงศาโรจน์	ธนาคารแห่งประเทศไทย
นายยรรยง ดำรงศิริ	
นางสาวจิตสุภา วิระยะวานิช	
นายกิตติพงษ์ สุขสม	
นางสาวดลพร พิมพิชัย	สำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ (องค์การมหาชน)
นางศุปกิจ สกลเสาวภาคย์	กรมที่ดิน
นางตวงรัตน์ จันทรประดิษฐ์	

คณะทำงานและเลขานุการ

นางสาวอุรัชฎา เกตุพรหม	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

วิเคราะห์และจัดทำมาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัล ว่าด้วย มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่องข้อกำหนดด้านความน่าเชื่อถือและความมั่นคงปลอดภัย

นายเจษฎา ขจรฤทธิ์ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

นายปราการ ศิริมา สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คำนำ

มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ (Thailand Government Information Exchange: TGIX) ประกอบด้วย กลุ่มมาตรฐานด้านการเชื่อมโยงข้อมูล (Linkage Standards) และกลุ่มมาตรฐานด้านความหมายข้อมูล (Semantic Standards) มาตรฐานฉบับนี้อยู่ในกลุ่มมาตรฐานด้านการเชื่อมโยงข้อมูล ที่กล่าวถึงวิธีการเพื่อให้เกิดการแลกเปลี่ยนข้อมูลระหว่างระบบสารสนเทศได้อย่างมีประสิทธิภาพ มีความถูกต้องแม่นยำ มีความมั่นคงปลอดภัย และอยู่ภายใต้ระเบียบข้อกำหนดทางกฎหมาย

มาตรฐานนี้เป็นมาตรฐานลำดับที่ 4 ในกลุ่มมาตรฐานด้านการเชื่อมโยงข้อมูล และแลกเปลี่ยนข้อมูลภาครัฐ เรื่อง ข้อกำหนดด้านความน่าเชื่อถือและความมั่นคงปลอดภัย ในส่วนแรกจะอธิบายถึงข้อกำหนดพื้นฐานด้านความน่าเชื่อถือและความมั่นคงปลอดภัย ข้อกำหนดด้านความปลอดภัยของระบบผู้ให้บริการ (Provider System) และระบบผู้ใช้บริการ (Consumer System) ในส่วนที่สองจะกล่าวถึง ข้อกำหนดด้านความความปลอดภัยขององค์ประกอบอื่น ๆ ตามมาตรฐาน TGIX และปิดท้ายด้วยข้อแนะนำด้านความปลอดภัยที่เกี่ยวข้องกับกฎหมาย

มาตรฐานนี้ประกอบด้วยคำอธิบาย และตัวอย่างที่ใช้งาน เพื่อประยุกต์ใช้ในการเชื่อมโยงแลกเปลี่ยนข้อมูลกันระหว่างหน่วยงานได้อย่างมีประสิทธภาพ และมีความมั่นคงปลอดภัยของข้อมูล

สารบัญ

สารบัญรูป

สารบัญตาราง

มาตรฐานรัฐบาลดิจิทัล
ว่าด้วย มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ
ด้านการเชื่อมโยงข้อมูล เรื่อง ข้อกำหนดด้านความน่าเชื่อถือและความมั่นคงปลอดภัย

1. ขอบข่าย

การแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน เป็นพื้นฐานหลักที่จำเป็นต่อการพัฒนารัฐบาลดิจิทัล ในปัจจุบันประเทศไทยมีแพลตฟอร์มการแลกเปลี่ยนข้อมูลที่ให้บริการอยู่หลายแห่ง แพลตฟอร์มแต่ละแห่งมีแนวทางและพันธกิจในการดำเนินงานเป็นของตนเอง เป็นผลให้การบูรณาการข้อมูลภาครัฐ จำเป็นต้องขับเคลื่อนด้วยการสร้างมาตรฐาน หรือข้อตกลงร่วมกันในการแลกเปลี่ยนข้อมูล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ได้เล็งเห็นความสำคัญในจุดนี้ จึงมีความจำเป็นต้องจัดทำมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ เพื่อใช้ในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานของรัฐ เพื่อให้การบูรณาการข้อมูลเกิดขึ้นอย่างเป็นรูปธรรม

เป้าประสงค์หลักของการใช้มาตรฐานฯ เป็นตัวขับเคลื่อนการบูรณาการข้อมูลภาครัฐ คือ การให้หน่วยงานของรัฐ มีแนวทางในการพัฒนาสถาปัตยกรรมระบบสารสนเทศ เพื่อใช้ในการแลกเปลี่ยนข้อมูลที่ชัดเจน มีความสอดคล้องในการเชื่อมต่อระหว่างกัน

มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ฉบับนี้ มีขอบเขตมาตรฐานที่ระดับการเชื่อมโยงข้อมูลเท่านั้น ไม่ได้ครอบคลุมถึงระดับการจัดการข้อมูลทางธุรกรรมของหน่วยงาน (Business Transaction Data) ที่เกิดขึ้นจากการเชื่อมโยงและแลกเปลี่ยนระหว่างกัน

ดังนั้นเพื่อให้บรรลุเป้าประสงค์หลักดังกล่าวเอกสารฉบับนี้จึงนำเสนอ ข้อกำหนดด้านความน่าเชื่อถือและความมั่นคงปลอดภัย สำหรับประกอบเอกสาร ว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ เรื่อง มาตรฐานสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ระดับการเชื่อมโยงข้อมูลที่เหมาะสมกับบริบทของประเทศไทยเท่านั้น

2. นิยาม

นิยามคำศัพท์ที่เกี่ยวข้องกับมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่อง ข้อกำหนดด้านความน่าเชื่อถือและความมั่นคงปลอดภัยที่ใช้ในเอกสารฉบับนี้ มีดังนี้

2.1. มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ (Thailand Government Information Exchange: TGIX) หมายความว่า มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐของประเทศไทย เรียกแบบย่อว่า “มาตรฐานฯ”

2.2. โปรโตคอล HTTP หมายความว่า โปรโตคอลมาตรฐานที่ใช้ในการสื่อสาร เพื่อนำเสนอและแลกเปลี่ยนข้อมูลบนอินเทอร์เน็ต โดยเป็นการทำงานร่วมกันระหว่างเว็บเซิร์ฟเวอร์และแอปพลิเคชันเบราว์เซอร์ เพื่อให้ผู้ใช้สามารถเข้าถึงข้อมูลต่าง ๆ ที่เชื่อมโยงกันผ่านแอดเดรสหรือที่อยู่ของเว็บเซิร์ฟเวอร์ที่อ้างถึง

2.3. โปรโตคอล HTTPS หมายความว่า โปรโตคอล HTTP ที่เพิ่มคุณสมบัติการเข้ารหัสข้อมูล (encryption) เพื่อความปลอดภัยในการสื่อสารบนอินเทอร์เน็ต โดยใช้ระบบการเข้ารหัส SSL (Secure Sockets Layer) หรือ TLS (Transport Layer Security) เพื่อป้องกันการดักจับข้อมูล การปลอมแปลงข้อมูล ของผู้ที่ไม่หวังดี โดยไม่ส่งผลกระทบต่อความสะดวกสบายของผู้ใช้งาน

2.4. Transport Layer Security (TLS) หมายความว่า มาตรฐานความปลอดภัยในการสื่อสารผ่านเครือข่ายอินเตอร์เน็ต ซึ่งถือว่าเป็นเครือข่ายสาธารณะ มีวัตถุประสงค์ในการรักษาความลับและความถูกต้องของข้อมูลที่ส่งผ่านเครือข่าย โดยการใช้การเข้ารหัสข้อมูล พร้อมกันกับการยืนยันตัวตนของเซิร์ฟเวอร์ และ/หรือเครื่องผู้ใช้เพื่อความน่าเชื่อถือ TLS จึงเป็นส่วนสำคัญในการรักษาความปลอดภัย และความเป็นส่วนตัวในการสื่อสารผ่านเครือข่าย

2.5. Public Key Infrastructure (PKI) หมายความว่า ระบบสำหรับจัดการคีย์ (Key) และใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) เพื่อความปลอดภัยและความน่าเชื่อถือของข้อมูลในการสื่อสารบนเครือข่ายสาธารณะ โดยใช้วิธีการเข้ารหัสแบบอสมมาตร (Asymmetric Key Cryptography) ประกอบด้วย Certificate Authority (CA) ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) กุญแจสาธารณะ (Public Key) และกุญแจส่วนตัว (Private Key) ช่วยให้ผู้ใช้สามารถระบุตัวตน และยังเป็นการป้องกันการปฏิเสธความรับผิดชอบของผู้ใช้หรือผู้ให้บริการอีกด้วย [1]

2.6. Certification Authority (CA) หมายความว่า เป็นองค์กรซึ่งทำหน้าที่ในการให้บริการเกี่ยวกับการออกใบรับรองอิเล็กทรอนิกส์ เพื่อรับรองตัวตนที่แท้จริงของบุคคล นิติบุคคล หรือเอนทิตีใด ๆ [1]

2.7. ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) หมายความว่า ไฟล์ที่มีข้อมูลเข้ารหัสเพื่อยืนยันตัวตนของเจ้าของกุญแจสาธารณะ และเป็นส่วนหนึ่งของ Public Key Infrastructure (PKI) ใบรับรองดิจิทัลมักใช้ในการตรวจสอบตัวตนของเว็บไซต์ หรือในการลงลายมือชื่ออิเล็กทรอนิกส์ (Digital Signature) เพื่อให้มั่นใจ

ว่าการสื่อสารนั้นมาจากแหล่งที่น่าเชื่อถือ ใบรับรองนี้มีอายุการใช้งานและจะถูกออกโดย Certificate Authority (CA) ที่ได้รับการรับรอง

2.8. การเข้ารหัสแฮชฟังก์ชัน (Hash Functions) หมายความว่า ฟังก์ชันที่ใช้เปลี่ยนข้อมูลขนาดใหญ่หรือข้อมูลใด ๆ ไปเป็นข้อมูลขนาดเล็ก ที่ไม่สามารถย้อนกลับเป็นข้อมูลเดิมได้ หรือเรียกว่า "digest" เพื่อใช้ในการตรวจสอบความถูกต้องของข้อมูล หรือการลงลายมือชื่ออิเล็กทรอนิกส์ (Digital Signature) โดยมีอัลกอริทึมให้เลือกใช้ เช่น SHA-256, SHA-3 หรือ MD5

2.9. การเข้ารหัสแบบสมมาตร (Symmetric Encryption) หมายความว่า อัลกอริทึมสำหรับเข้ารหัสข้อมูลที่มีความสำคัญและต้องการปกปิดเป็นความลับ โดยมีลักษณะการเข้ารหัสแบบใช้กุญแจที่เหมือนกันทั้งในขั้นตอนเข้ารหัส และขั้นตอนถอดรหัส

2.10. การเข้ารหัสแบบอสมมาตร (Asymmetric Encryption) หมายความว่า กระบวนการเข้ารหัสและถอดรหัสข้อมูลที่ใช้คู่กุญแจที่แตกต่างกันสองอัน คือ กุญแจสาธารณะ (Public Key) และกุญแจส่วนตัว (Private Key) กรณีที่ข้อมูลที่ถูกเข้ารหัสด้วยกุญแจสาธารณะ สามารถถอดรหัสได้ด้วยกุญแจส่วนตัวเท่านั้น ส่วนข้อมูลที่ถูกเข้ารหัสด้วยกุญแจส่วนตัว สามารถถอดรหัสได้ด้วยกุญแจสาธารณะ มักใช้รับ-ส่งข้อมูลที่ต้องการความปลอดภัยสูง หรือใช้ในกระบวนการลงลายมือชื่ออิเล็กทรอนิกส์ โดยสามารถเลือกใช้อัลกอริทึม เช่น RSA, Elliptic Curve Cryptography (ECC)

2.11. ลายมือชื่ออิเล็กทรอนิกส์ (Digital Signature) หมายความว่า วิธีการยืนยันความถูกต้องและความน่าเชื่อถือของข้อมูลอิเล็กทรอนิกส์ เพื่อให้แน่ใจว่าข้อมูลไม่ถูกเปลี่ยนแปลงหรือปลอมแปลง โดยการเข้ารหัสแบบอสมมาตร และใช้กุญแจส่วนตัวของผู้ส่งเพื่อสร้างการลงนามเอกสารแบบอิเล็กทรอนิกส์ เมื่อผู้รับข้อมูลได้รับลายมือชื่ออิเล็กทรอนิกส์ สามารถใช้กุญแจสาธารณะของผู้ส่ง เพื่อตรวจสอบความถูกต้องของเอกสารที่ลงนามแบบอิเล็กทรอนิกส์นี้ได้ ช่วยให้สามารถระบุตัวตน และยังเป็นการป้องกันการปฏิเสธความรับผิดชอบของผู้ใช้หรือผู้ให้บริการอีกด้วย

2.12. ผู้ให้บริการ (Provider) หมายความว่า หน่วยงานที่เปิดให้บริการ API สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในแพลตฟอร์มที่ใช้มาตรฐาน TGIX

2.13. ระบบผู้ให้บริการ (Provider System) หมายความว่า ระบบสารสนเทศของหน่วยงานมีการใช้บริการ API สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในแพลตฟอร์มที่ใช้มาตรฐาน TGIX

2.14. ผู้ใช้บริการ (Consumer) หมายความว่า หน่วยงานที่ใช้บริการ API สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในแพลตฟอร์มที่ใช้มาตรฐาน TGIX

2.15. ระบบผู้ใช้บริการ (Consumer System) หมายความว่า ระบบสารสนเทศของหน่วยงานที่ใช้บริการ API สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในแพลตฟอร์มที่ใช้มาตรฐาน TGIX

2.16. แพลตฟอร์มมาตรฐาน TGIX-based Data Exchange Platform หมายความว่า ระบบสารสนเทศการเชื่อมโยงและแลกเปลี่ยนข้อมูลกลางที่มีมาตรฐานตาม TGIX โดยเรียกแบบย่อว่า TGIX Platform

2.17. ผู้ให้บริการ TGIX Platform (TGIX Platform Provider) หมายความว่า ระบบสารสนเทศของหน่วยงานผู้ให้บริการ TGIX Platform เพื่อสนับสนุนการเชื่อมโยงและแลกเปลี่ยนข้อมูลให้เป็นไปตามมาตรฐาน TGIX

2.18. ต้อง (Must) หมายความว่า ผู้ดำเนินการต้องทำตามข้อกำหนดในมาตรฐานฯ

2.19. ควร (Should) หมายความว่า ผู้ดำเนินการควรทำตามข้อกำหนดในมาตรฐานฯ

3. กฎหมายและแนวปฏิบัติที่เกี่ยวข้อง

3.1 พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 [6]

มาตรา 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 งบประมาณทรัพย์สินและหนี้สิน ภาระผูกพัน และบุคลากรไปยังหน่วยงานของรัฐแห่งอื่นนั้นต่อคณะรัฐมนตรีเพื่อพิจารณา

4. ข้อกำหนดด้านความน่าเชื่อถือและความมั่นคงปลอดภัย

มาตรฐานการเชื่อมโยงและการแลกเปลี่ยนข้อมูลภาครัฐ ระดับการเชื่อมโยงข้อมูลมีความมุ่งเน้นและให้ความสำคัญในเรื่องของความปลอดภัย และการเข้ารหัสของการแลกเปลี่ยนข้อมูล ระหว่างระบบผู้ใช้บริการ (Consumer System) และระบบผู้ให้บริการ (Provider System) การกำหนดมาตรฐานในด้านความปลอดภัยและการเข้ารหัสข้อมูล ที่มีการรับส่งระหว่างกันจึงเป็นสิ่งจำเป็นที่จะช่วยการลดความเสี่ยงในด้านความปลอดภัยลงได้

ในส่วนนี้ จะอธิบายหลักการขั้นพื้นฐานของมาตรฐานความปลอดภัยของมาตรฐานการเชื่อมโยงและการแลกเปลี่ยนข้อมูลภาครัฐ ระดับการเชื่อมโยงข้อมูลที่กำหนดขึ้น เพื่อให้เป็นมาตรฐานความน่าเชื่อถือและความมั่นคงปลอดภัยการเชื่อมโยงและแลกเปลี่ยนข้อมูล โดยอ้างอิงจากหลักการในเรื่องความปลอดภัยสารสนเทศ (Information Security: InfoSec) [2] ซึ่งประกอบไปด้วยส่วนสำคัญ 3 เรื่อง คือ Confidentiality, Integrity และ Availability หรือที่รู้จักกัน คือ CIA Triad [3]

4.1. จุดประสงค์ของข้อกำหนดพื้นฐานด้านความน่าเชื่อถือและความมั่นคงปลอดภัย

4.1.1. การรักษาความลับของข้อมูล (Confidentiality)

การรักษาความลับของข้อมูล คือการเก็บรักษาข้อมูลให้เป็นความลับ และอนุญาตให้เฉพาะผู้ที่ได้รับอนุญาตเข้าถึงข้อมูลได้ โดยการจำกัดสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานในระบบ (ผู้ที่มีส่วนเกี่ยวข้องในการเชื่อมโยงและการแลกเปลี่ยนข้อมูล) ด้วยการยืนยันตัวตน (Authentication) และการตรวจสอบสิทธิ์ (Authorization) ในการเข้าถึงทรัพยากร เพื่อให้มั่นใจได้ว่าจะไม่มีการเข้าถึงข้อมูลจากผู้ที่ไม่ได้รับอนุญาต

มาตรฐานการเชื่อมโยงและการแลกเปลี่ยนข้อมูลภาครัฐ ระดับการเชื่อมโยงข้อมูล (TGIX) ใช้การส่งผ่านข้อมูลในระบบที่อาจผ่านเครือข่ายสาธารณะ เช่น Internet จึงมีการกำหนดให้ใช้วิธีการส่งข้อมูลด้วยกระบวนการที่มีความปลอดภัยสูง เช่น Digital Signature และการเข้ารหัสข้อมูล (Data Encryption) ซึ่งข้อมูลจะต้องถูกส่งผ่านโปรโตคอล HTTPS บน Transport Layer Security (TLS) ที่จะช่วยป้องกันการดักจับและป้องกันการโจรกรรมข้อมูล โดยจะทำให้มั่นใจได้ว่าการแลกเปลี่ยนข้อมูลผ่านมาตรฐาน TGIX จะรักษาความลับ และความเป็นส่วนตัวของข้อมูลได้ ซึ่งได้มีข้อกำหนดที่เกี่ยวข้อง ดังต่อไปนี้

(1) ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security)
(2) ข้อกำหนดการเข้ารหัส (Encryption)
(3) ข้อกำหนดด้าน Authentication Access Control และ Accounting ซึ่งกล่าวในมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่อง ข้อกำหนดด้านการยืนยันตัวตน การกำหนดสิทธิ์ และบัญชีการใช้งาน

(4) ข้อกำหนดด้านการบริหารจัดการ Token และ Session ซึ่งกล่าวในมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่อง ข้อกำหนดของโปรโตคอลระดับแอปพลิเคชันเอนพอยน์ และการจัดการโทเคน และเซสชัน

4.1.2. ความถูกต้องของข้อมูล (Integrity)

ความถูกต้องของข้อมูล คือ การตรวจสอบ และทำให้มั่นใจว่าข้อมูลที่มีการแลกเปลี่ยนกันภายในมาตรฐาน TGIX มีความถูกต้องและสมบูรณ์ครบถ้วน ไม่ถูกแก้ไข หรือทำให้ได้รับความเสียหายแก่ข้อมูลที่แลกเปลี่ยนกันภายใน TGIX ซึ่งได้มีข้อกำหนดที่เกี่ยวข้อง ดังต่อไปนี้

(1) ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security)

(2) ข้อกำหนดการบันทึกกิจกรรมและข้อมูลจราจรคอมพิวเตอร์และการสอดส่อง (Logging & Monitoring)

(3) ข้อกำหนดการจัดการความผิดพลาด (Error handling)

4.1.3. ความพร้อมให้บริการ (Availability)

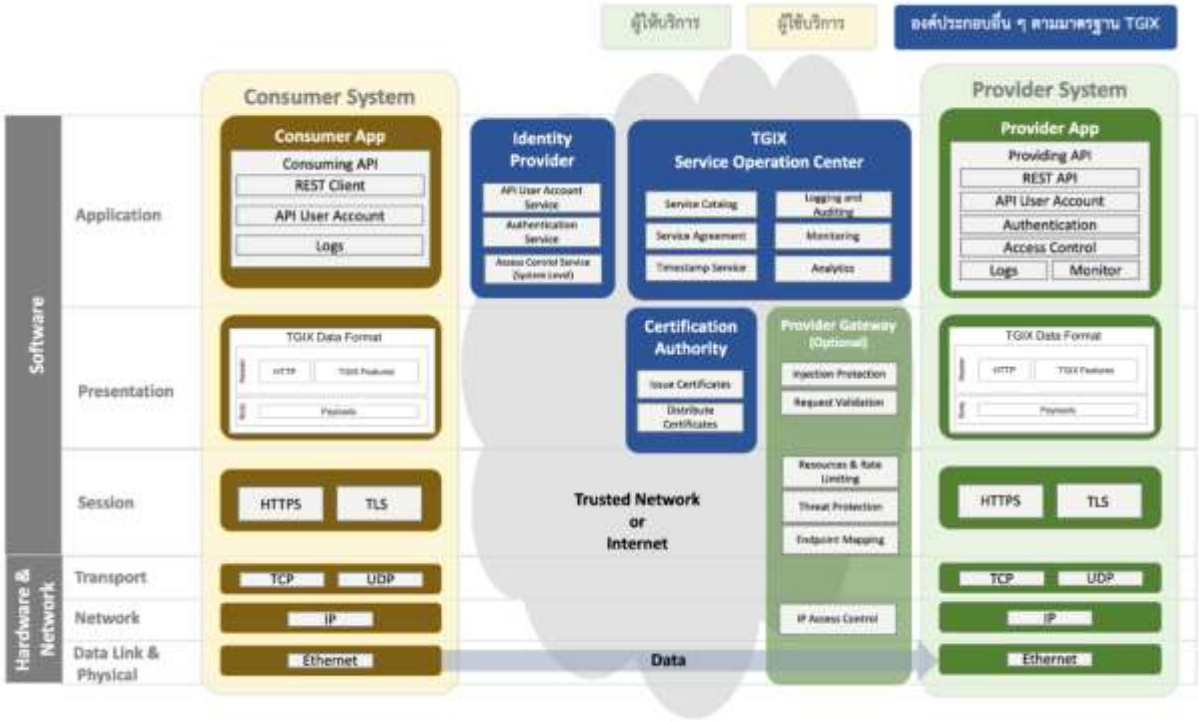
ความพร้อมให้บริการ คือความพร้อมใช้งานหรือให้บริการของระบบได้อย่างต่อเนื่อง เพื่อทำให้มั่นใจว่าองค์ประกอบต่าง ๆ ในมาตรฐาน TGIX มีความพร้อมให้บริการกับองค์ประกอบอื่น ในมาตรฐาน TGIX ที่มีความเกี่ยวข้องกัน และเพื่อบรรเทาผลกระทบจากการไม่สามารถให้บริการได้ จนนำไปสู่ผลกระทบกับผู้ใช้บริการ ซึ่งได้มีข้อกำหนดที่เกี่ยวข้อง ดังต่อไปนี้

(1) ข้อกำหนดเกี่ยวกับการป้องกันการโจมตี

(2) ข้อกำหนดการจำกัดอัตราการเข้าถึงบริการและใช้ทรัพยากร (Resource and Rate Limit)

(3) ข้อกำหนดการตรวจสอบข้อมูลนำเข้า (Input Validation)

จากหลักการขั้นพื้นฐานทั้ง 3 ข้างต้น คือ การรักษาความลับ (Confidentiality) ความถูกต้องของข้อมูล (Integrity) และความพร้อมให้บริการ (Availability) โดยมาตรฐานการเชื่อมโยงและการแลกเปลี่ยนข้อมูลภาครัฐระดับการเชื่อมโยงข้อมูล จัดให้มีข้อกำหนดเพื่อเป็นกรอบแนวทางการปฏิบัติตามแนวทางการปฏิบัติที่ดี โดยจะครอบคลุมระบบผู้ให้บริการ ระบบผู้ใช้บริการ และองค์ประกอบอื่นๆ ตามมาตรฐาน TGIX ดังรูปที่ 1



รูปที่ 1 ภาพรวมองค์ประกอบของการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ

สามารถแบ่งข้อกำหนดเป็น 4 ส่วน ดังนี้

(1) ข้อกำหนดด้านความปลอดภัยของระบบผู้ให้บริการ 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) ข้อกำหนดด้านความปลอดภัยของระบบผู้ใช้บริการ ประกอบด้วย
   ก. ข้อกำหนดด้านความมั่นคงปลอดภัยของการส่งข้อมูล (Transport Security)
   ข. ข้อกำหนดการเข้ารหัส (Encryption)
   ค. ข้อกำหนดการบันทึกกิจกรรมและข้อมูลจราจรคอมพิวเตอร์และการตรวจสอบ (Logging & Monitoring)

(3) ข้อกำหนดด้านความปลอดภัยขององค์ประกอบอื่น ๆ 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

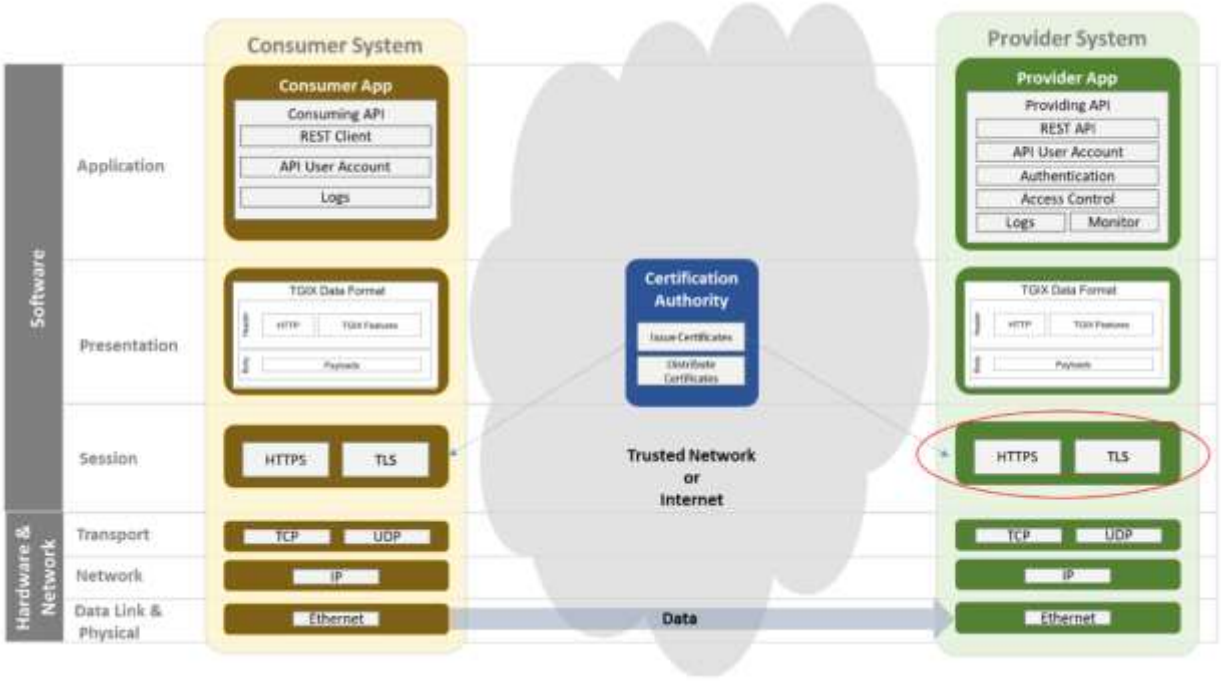
ข. ข้อกำหนดที่เกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

ค. ข้อกำหนดที่เกี่ยวกับหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของระบบผู้ให้บริการ พ.ศ. 2564

4.2. ข้อกำหนดด้านความปลอดภัยของระบบผู้ให้บริการ (Provider System)

4.2.1. ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security)

ความปลอดภัยของการส่งข้อมูล (Transport Security) ของมาตรฐาน TGIX ของระบบผู้ให้บริการจะมุ่งเน้นไปการส่งข้อความในระดับ Session ของระบบผู้ให้บริการ ในองค์ประกอบของมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลของระบบผู้ให้บริการดังรูปที่ 2



รูปที่ 2 องค์ประกอบที่เกี่ยวข้องกับความปลอดภัยของการส่งข้อมูลของระบบผู้ให้บริการการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ

เพื่อให้การรับส่งข้อมูลสำหรับบริการการแลกเปลี่ยนข้อมูล มีความปลอดภัยและเป็นไปตามข้อกำหนดพื้นฐานด้านความปลอดภัย การสื่อสารเพื่อรับส่งข้อมูลของมาตรฐาน TGIX ของระบบผู้ให้บริการจะต้องเป็นไปตามข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security) ของระบบผู้ให้บริการ [4] โดยมีรายละเอียดดังตารางที่ 1

ตารางที่ 1 ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security) ของระบบผู้ให้บริการ

ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security)	ข้อกำหนด
• การส่งข้อมูลจะต้องดำเนินการบน HTTPS โดยใช้ TLS 1.2 เป็นอย่างน้อย	√

ตารางที่ 1 ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security) ของระบบผู้ให้บริการ (ต่อ)

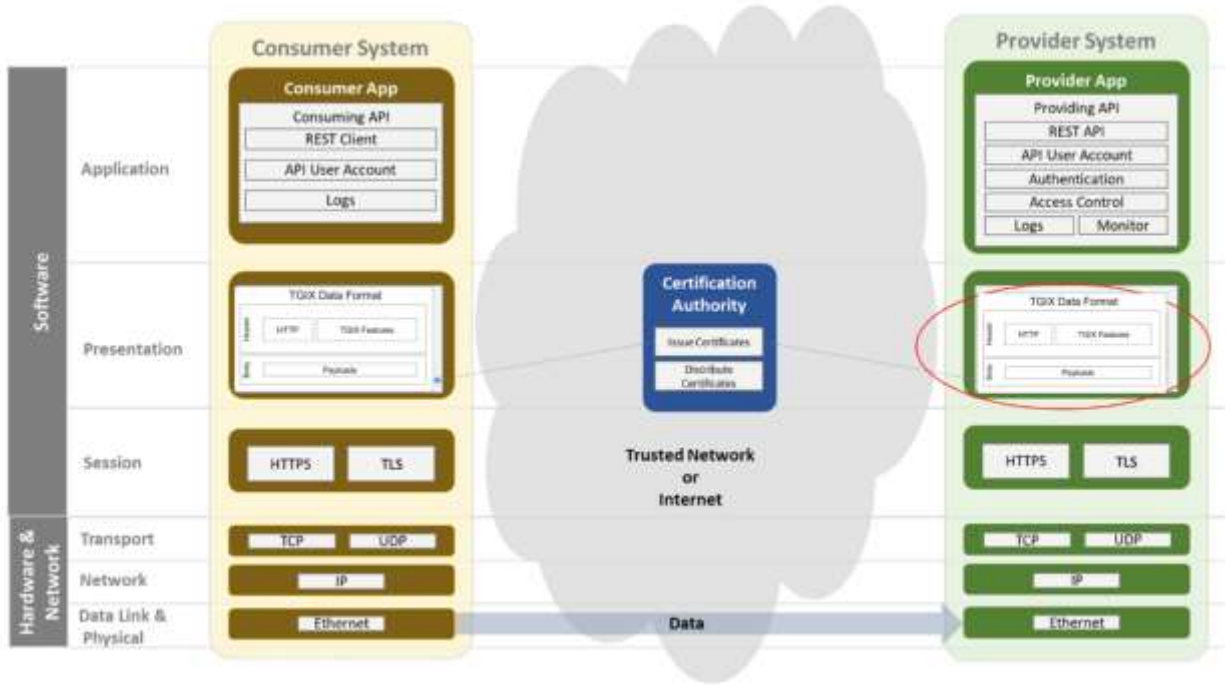
ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security)	ข้อกำหนด
● ใบรับรองอิเล็กทรอนิกส์ (Digital Certificates) ควรระบุขนาดของคู่กุญแจที่จะนำไปสร้างใบรับรองอิเล็กทรอนิกส์ อย่างน้อย 2048 bits ที่สร้างด้วย RSA หรืออัลกอรึทึมที่เทียบเท่ากัน	√
● ทุกปลายทาง (Endpoint) จะต้องใช้ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) ที่ออกโดยหน่วยงานที่ดูแลใบรับรองดิจิทัลที่ได้รับอนุญาต	○
● ห้ามทำการเปลี่ยนเส้นทาง HTTP ไปยัง HTTPS (Redirecting HTTP to HTTPS) โดยให้ปฏิเสธการเปลี่ยนเส้นทางทุกกรณี	√
● ให้ปิดการใช้งานเมธอด HTTP (HTTP Method) ที่ไม่ได้ใช้งานและส่งคืนค่า HTTP 405 ตามมาตรฐาน Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content: section-6.5.5 [5]	√
● ต้องมีการตรวจสอบ (Validate) ตามข้อกำหนดการตรวจสอบข้อมูลนำเข้า (Input Validation) ทุก ๆ การเรียกใช้งาน (Request)	√

√ จำเป็น ○ ทางเลือก

ทั้งนี้ผู้ให้บริการสามารถพิจารณาเพิ่มความเข้มข้นของความปลอดภัยโดยพิจารณาความจากเสี่ยงของธุรกรรมที่ให้บริการได้

4.2.2. ข้อกำหนดการเข้ารหัส (Encryption)

การเข้ารหัสข้อมูลของระบบผู้ให้บริการ ในกรณีที่ต้องมีการเข้ารหัสข้อมูล เช่น ข้อมูลที่มีความสำคัญที่เป็นข้อมูลเชิงธุรกรรมที่ Payload ข้อมูลลายมือชื่ออิเล็กทรอนิกส์ (Digital Signature) หรือข้อมูลโทเคน (Token) ที่อยู่ในส่วน Header เป็นต้น การเข้ารหัสข้อมูล (Encryption) ในมาตรฐาน TGIX จะมุ่งเน้นไปยังส่วน Presentation ของระบบผู้ให้บริการในองค์ประกอบของการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐของระบบผู้ให้บริการ ดังรูปที่ 3



รูปที่ 3 องค์ประกอบที่เกี่ยวข้องกับความปลอดภัยของการเข้ารหัสของระบบผู้ให้บริการการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ

เพื่อให้เป็นไปตามข้อกำหนดพื้นฐานด้านความปลอดภัย การเข้ารหัสข้อมูล (Encryption) ของมาตรฐาน TGIX ของระบบผู้ให้บริการ จะต้องเป็นไปตามข้อกำหนดการเข้ารหัส (Encryption) ของระบบผู้ให้บริการ [6] โดยมีรายละเอียดดังตารางที่ 2

ตารางที่ 2 ข้อกำหนดการเข้ารหัส (Encryption) ของระบบผู้ให้บริการ

ข้อกำหนดการเข้ารหัส (Encryption)	ข้อกำหนด
• ในกรณีที่การส่งข้อมูลที่ผู้ให้บริการพิจารณาแล้วว่ามีข้อมูลที่มีความสำคัญที่เป็นข้อมูลเชิงธุรกรรมใน Payload หรือเป็นความลับที่ต้องการการเข้ารหัสจะต้องใช้การเข้ารหัสแบบสมมาตร (Symmetric Encryption) แบบ AES (Advanced Encryption Standard) [7] โดยมีความยาวของกุญแจอย่างน้อย 128 bits (AES-128) ซึ่งสามารถเข้ารหัสเฉพาะข้อมูลนั้น ๆ ไม่จำเป็นต้องเข้ารหัสข้อมูลทั้ง Payload หมายเหตุ 1. ในกรณีที่พบปัญหาการถอดรหัส เช่น ระบบผู้ให้บริการไม่สามารถถอดรหัสข้อมูลที่ได้รับได้ ระบบผู้ให้บริการสามารถตอบกลับด้วย error message ดังตัวอย่างการตอบกลับดังรูปที่ 4	√

ตารางที่ 2 ข้อกำหนดการเข้ารหัส (Encryption) ของระบบผู้ให้บริการ (ต่อ)

ข้อกำหนดการเข้ารหัส (Encryption)	ข้อกำหนด
2. ทั้งนี้ ผู้ให้บริการสามารถพิจารณาเพิ่มความแข็งแรงของการเข้ารหัสข้อมูลโดยพิจารณาความจากเสี่ยงของธรุกรรมที่ให้บริการได้ ● สำหรับการลงลายมือชื่อเพื่อการรับประกันการยืนยันตัวตนของต้นทางและความถูกต้องของข้อมูล จะต้องใช้ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) ที่ออกโดย Certification Authority (CA) ที่ดูแลใบรับรองดิจิทัลที่ได้รับอนุญาต เช่น Thailand NRCA และอัลกอริทึมแบบใดแบบหนึ่ง ดังต่อไปนี้ ○ อัลกอริทึม DSA (Digital Siganture Algorithm) โดยมีขนาดของ Security of strength มากกว่าหรือเท่ากับ 112 bits และ Domain Parameter อย่างน้อย (L, N) = (2048, 224) ○ อัลกอริทึม ECDSA (Elliptic Curve-based Digital Signature) โดยมีขนาดของ Security of strength อย่างน้อย 112 bits และ Domain Parameter อย่างน้อย 224 bits ○ อัลกอริทึม RSA (Rivest-Shamir-Adelman algorithm) โดยมีขนาดของ Security of strength อย่างน้อย 112 bits และ Domain Parameter อย่างน้อย 2048 bits ในกรณีที่พบปัญหาการถอดรหัส เช่น ระบบผู้ให้บริการไม่สามารถถอดรหัสการตรวจสอบลายเซ็นของ JWT (JSON Web Token) ได้ ระบบผู้ให้บริการสามารถตอบกลับด้วย error message ดังตัวอย่างการตอบกลับ ในรูปที่ 5	○
● สำหรับการสร้างหรือตรวจสอบลายมือชื่อแบบดิจิทัลโดยใช้แฮชฟังก์ชัน (Hash Function) จะต้องใช้ฟังก์ชันแบบใดแบบหนึ่ง ดังต่อไปนี้ ○ 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 เช่น การสร้างกุญแจ (keys) ตัวเลขแบบใช้ครั้งเดียว (Nonces) และ ค่าสุ่มเพื่อการยืนยันตัวตน (Authentication Challenges) จะต้องใช้อัลกอริทึมแบบใดแบบหนึ่ง ดังต่อไปนี้ ○ Hash_DRBG ○ HMAC_DRBG	√

ตารางที่ 2 ข้อกำหนดการเข้ารหัส (Encryption) ของระบบผู้ให้บริการ (ต่อ)

ข้อกำหนดการเข้ารหัส (Encryption)	ข้อกำหนด
○ CTR_DRBG โดยใช้ AES-128, AES-192 และ AES-256	

√ จำเป็น ○ ทางเลือก

ทั้งนี้ผู้ให้บริการสามารถพิจารณาเพิ่มความเข้มข้นของความปลอดภัยโดยพิจารณาความจากเสี่ยงของธุรกรรมที่ให้บริการได้

```
"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

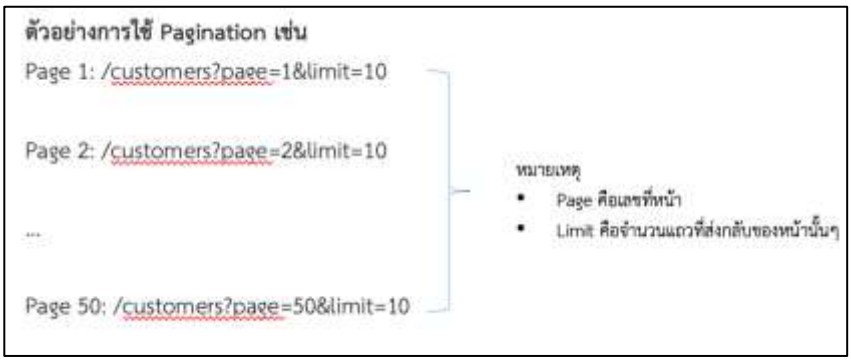
การจำกัดอัตราการเข้าถึงบริการและใช้ทรัพยากรของมาตรฐาน TGIX จะมุ่งเน้นไปยังส่วนของ ระบบผู้ให้บริการ เพื่อให้เป็นไปตามข้อแนวทางการปฏิบัติที่ดีทางด้านความปลอดภัยของการให้บริการการแลกเปลี่ยนข้อมูล ผู้ให้บริการจะต้องจัดให้มีการควบคุมอัตราการเข้าถึงบริการ และการใช้ทรัพยากรของระบบของผู้ให้บริการ [8] โดยทั้งระบบผู้ให้บริการจะต้องสามารถกำหนดการจำกัดได้อย่างน้อย ดังตารางที่ 3

ตารางที่ 3 ข้อกำหนดการจำกัดอัตราการเข้าถึงบริการและใช้ทรัพยากรของระบบผู้ให้บริการ

ข้อกำหนดการจำกัดอัตราการเข้าถึงบริการและใช้ทรัพยากร	ข้อกำหนด
● 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 ○ อื่น ๆ 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 ● อื่น ๆ ตามความเหมาะสม	√
● สามารถจำกัดจำนวนการร้องขอบริการต่อผู้ขอใช้บริการหรือบริการได้ (Number of requests per client/resource) โดยผู้ให้บริการทำการประเมินจากทรัพยากรและประสิทธิภาพที่จะให้บริการได้กับความต้องการใช้บริการของระบบผู้ใช้บริการ โดยสามารถเลือกดำเนินการได้จากตัวอย่างการ Implementation สามารถใช้เครื่องมือที่เป็นลักษณะ API Gateway ช่วยในการจำกัดเวลาการทำงานของบริการได้ (Execution timeouts) ดังตัวอย่างรูปที่ 6	○
● สามารถจำกัดจำนวนแถวข้อมูลต่อหน้าที่จะส่งกลับไปยังผู้ขอใช้บริการและตอบกลับต่อหนึ่งการร้องขอ ดังตัวอย่างรูปที่ 7 ตัวอย่างการดำเนินการทำ Pagination เพื่อจำกัดจำนวนแถวข้อมูลต่อหน้า ที่จะส่งกลับไปยังผู้ร้องขอบริการดังรูปที่7 มีจุดประสงค์เพื่อ 1. ให้การตอบกลับของ API ใช้เวลาน้อยเช่น < 2 วินาที เป็นต้น 2. ต้องการให้จำนวนข้อมูลที่ส่งกลับใน Payload มีความเหมาะสม เช่น < 500 kb	○

○ เลือกดำเนินการ √ต้องดำเนินการ

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



รูปที่ 7 ตัวอย่างการดำเนินการทำ Pagination เพื่อจำกัดจำนวนแถวข้อมูลต่อหน้าที่จะส่งกลับไปยังผู้ร้องขอบริการ

4.2.4. ข้อกำหนดการบันทึกกิจกรรมและและข้อมูลจราจรคอมพิวเตอร์และการตรวจสอบ (Logging & Monitoring)

เพื่อให้เป็นไปตามแนวทางการปฏิบัติที่ดีทางด้านความปลอดภัยของการให้บริการการแลกเปลี่ยนข้อมูล ผู้ให้บริการจะต้องจัดให้มีการบันทึกข้อมูลล็อกและการตรวจสอบ โดยระบบผู้ให้บริการจะต้องมีการปฏิบัติตามข้อกำหนด ซึ่งกล่าวในมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่อง ข้อกำหนดของการตรวจสอบระบบและการลงบันทึกล็อก

4.2.5. ข้อกำหนดการจัดการความผิดพลาด (Error Handling)

เพื่อให้เป็นไปตามข้อแนวทางการปฏิบัติที่ดีทางด้านความปลอดภัยของการให้บริการการแลกเปลี่ยนข้อมูล ในการแสดงข้อความว่าเกิดการทำงานผิดพลาดนั้น จะต้องไม่เปิดเผยข้อมูลที่มีความเสี่ยงที่อาจนำกลับมาโจมตีระบบได้ โดยระบบผู้ให้บริการจะต้องจัดให้มีการจัดการข้อผิดพลาดอย่างเหมาะสมอย่างน้อยดังตารางที่ 4

ตารางที่ 4 ข้อกำหนดการจัดการความผิดพลาด (Error Handling) ของระบบผู้ให้บริการ

ข้อกำหนดการจัดการความผิดพลาด (Error Handling)	ข้อกำหนด
● บริการจะต้องปกปิดรหัสหรือข้อความแสดงข้อผิดพลาดอื่นใดนอกเหนือจากสถานะตอบกลับหรือข้อความแสดงข้อผิดพลาดของ HTTP (HTTP status responses และ HTTP error messages) เช่น ไม่ควรแสดงข้อมูลระดับระบบ (System level) ไปในข้อผิดพลาดที่ตอบกลับ ดังตัวอย่างรูปที่ 8 [9]	√
● 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 การตรวจสอบข้อมูลที่จะนำเข้าสู่ระบบจะช่วยให้มั่นใจได้ว่าข้อมูลที่จะเข้าสู่ระบบ อยู่ในรูปแบบที่เหมาะสม ซึ่งจะช่วยป้องกันการถูกโจมตีระบบได้ โดยระบบผู้ให้บริการจะต้องจัดให้มีการตรวจสอบข้อมูลนำเข้าอย่างเหมาะสมอย่างน้อย ดังตารางที่ 5

ตารางที่ 5 ข้อกำหนดการตรวจสอบข้อมูลนำเข้า (Input Validation) ของระบบผู้ให้บริการ

ข้อกำหนดการตรวจสอบข้อมูลนำเข้า (Input Validation)	ข้อกำหนด
● การตรวจสอบข้อมูลนำเข้าฝั่งเซิร์ฟเวอร์ (server-side input Data validations) ควรจะกระทำทุกครั้งก่อนประมวลผล	√
● กำหนดการจำกัดขนาดของข้อมูลนำเข้าที่เหมาะสมและปฏิเสธข้อมูลนำเข้าที่มีขนาดเกินที่กำหนดไว้	√
● ออกแบบและพัฒนาระบบให้ตรวจสอบข้อมูลนำเข้า โดยตรวจสอบ เช่น ขนาดความยาว ช่วงของข้อมูล รูปแบบข้อมูล และประเภทข้อมูล ให้ตรงตามข้อกำหนดทางเทคนิคของบริการนั้นที่กำหนดไว้ดังตัวอย่างในรูปที่ 9	√
● ออกแบบและพัฒนาระบบให้ตรวจสอบบันทึกกิจกรรมและข้อมูลจราจรคอมพิวเตอร์ที่ไม่ผ่านการตรวจสอบข้อมูลนำเข้า (Logging input validation) เพื่อเป็นการสอดส่องความพยายามตรวจสอบข้อมูลนำเข้าที่ไม่ผ่านและมีมากผิดปกติในช่วงเวลาสั้น ๆ ซึ่งอาจจะเป็นการพยายามโจมตีระบบ	◌
● จำกัดข้อมูลนำเข้าประเภทข้อความ (String) ให้อยู่ในรูปแบบที่เหมาะสมกับประเภทข้อมูล ตามข้อกำหนดทางเทคนิคของบริการนั้น ด้วยการตรวจสอบด้วย นิพจน์ปกติ (Regular Expression) ดังตัวอย่างในรูปที่ 10	√

◌ 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 โดยระบบผู้ให้บริการจะต้องจัดให้มีการดำเนินการป้องกันการโจมตีอย่างเหมาะสมอย่างน้อย ดังตารางที่ 6

ตารางที่ 6 ข้อกำหนดเกี่ยวกับการป้องกันการโจมตีของระบบผู้ให้บริการ

ข้อกำหนดการป้องกันการโจมตีของระบบผู้ให้บริการ	ข้อกำหนด
• จัดให้มี Endpoint Mapping โดยที่ระบบผู้ให้บริการทำการเปิด Public Endpoint ของ API ให้ระบบผู้ใช้บริการใช้งาน โดยที่ระบบผู้ใช้บริการไม่ทราบ Endpoint ที่แท้จริงของ API ที่ Provider สร้างขึ้น โดยสามารถเลือกดำเนินการได้จากการใช้ API Gateway หรือสิ่งที่ทำหน้าที่ได้เทียบเท่า เข้ามาช่วยดำเนินการ	○
• 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

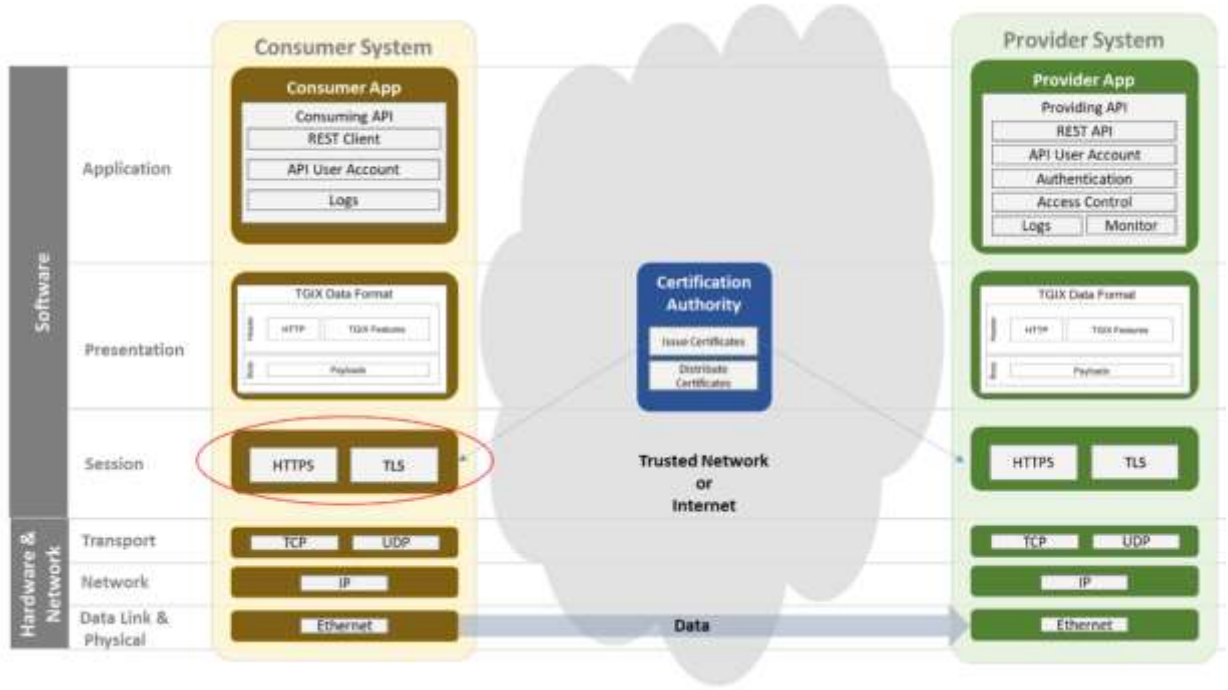
เนื่องจากข้อกำหนดที่กำหนดไว้ในมาตรฐาน TGIX เป็นข้อกำหนดขั้นพื้นฐาน ให้แต่ละหน่วยงานพิจารณาเพิ่มความเข้มข้นในการดำเนินการตามความเหมาะสมของแต่ละหน่วยงานได้ รวมทั้งในกรณีที่หน่วยงานตรวจพบความผิดปกติด้านความปลอดภัยจากการให้บริการ API สามารถพิจารณาตัดการทำงาน และลดผลกระทบสืบเนื่อง

เมื่อเกิดปัญหาในการเรียกใช้บริการ API เช่น ตัดการเชื่อมการเรียกใช้งาน API จากภายนอก ในกรณีที่ใช้งานไม่ได้ และยังคงค้างการเชื่อมต่อ จนอาจส่งผลกระทบไปยังระบบอื่น เป็นต้น

4.3. ข้อกำหนดด้านความปลอดภัยของระบบผู้ใช้บริการ (Consumer System)

4.3.1. ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security)

ความปลอดภัยของการส่งข้อมูล (Transport Security) ของมาตรฐาน TGIX ของระบบผู้ใช้บริการ จะมุ่งเน้นไปการส่งข้อความในระดับ Session ของระบบผู้ใช้บริการ ในองค์ประกอบของการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐของระบบผู้ใช้บริการดังรูปที่ 11



รูปที่ 11 องค์ประกอบที่เกี่ยวข้องกับความปลอดภัยของการส่งข้อมูลของระบบผู้ใช้บริการการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ

เพื่อให้การรับส่งข้อมูลสำหรับบริการการแลกเปลี่ยนข้อมูล มีความปลอดภัยและเป็นไปตามข้อกำหนดพื้นฐานด้านความปลอดภัย การสื่อสารเพื่อรับส่งข้อมูลของมาตรฐาน TGIX ของระบบผู้ใช้บริการจะต้องเป็นไปตามข้อกำหนดโดยมีรายละเอียด ดังตารางที่ 7

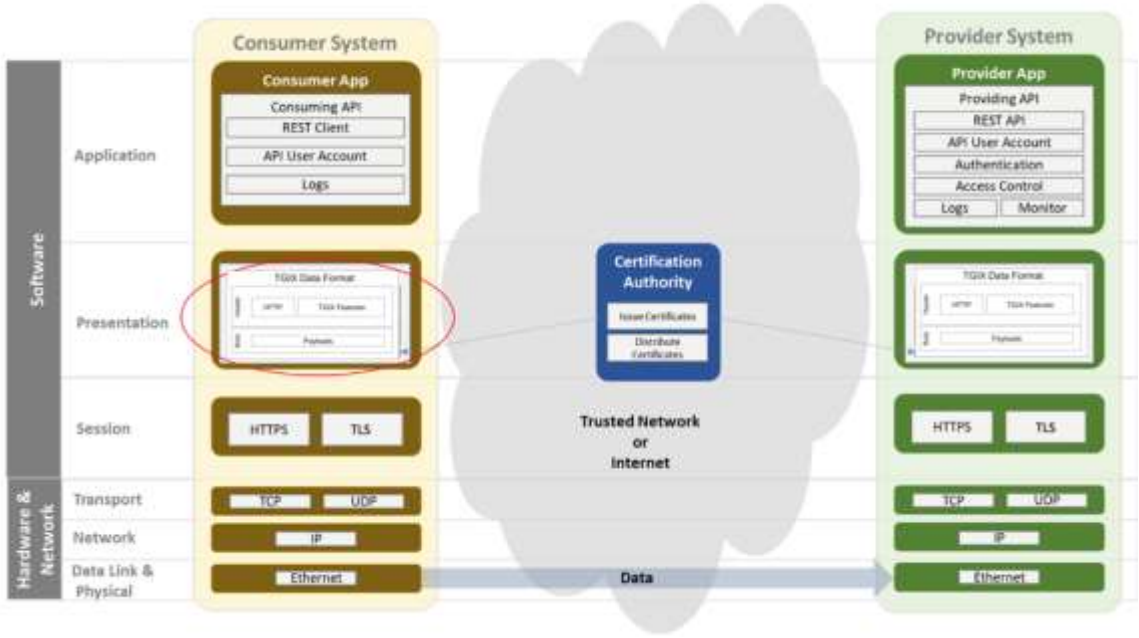
ตารางที่ 7 ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security) ของระบบผู้ใช้บริการ

ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security)	ข้อกำหนด
● การส่งข้อมูลจะต้องดำเนินการบน HTTPS โดยใช้ TLS 1.2 เป็นอย่างน้อย	√
● ใบรับรองอิเล็กทรอนิกส์ (Digital Certificates) ควรระบุขนาดของคู่กุญแจที่จะนำไปสร้างใบรับรองอิเล็กทรอนิกส์ อย่างน้อย 2048 bits ที่สร้างด้วย RSA หรืออัลกอริทึมที่เทียบเท่ากัน	√
● ทุกปลายทาง (Endpoint) จะต้องใช้ใบรับรองดิจิทัล (Digital Certificate) ที่ออกโดยหน่วยงานที่ดูแลใบรับรองดิจิทัลที่ได้รับอนุญาต	○

○ เลือกดำเนินการ √ต้องดำเนินการ

4.3.2. ข้อกำหนดการเข้ารหัส (Encryption)

การเข้ารหัสข้อมูลของระบบผู้ใช้บริการ ในกรณีที่ต้องมีการเข้ารหัสข้อมูล เช่น ข้อมูลที่มีความสำคัญที่เป็นข้อมูลเชิงธุรกรรมที่ Payload ข้อมูลลายเซ็นในส่วน Signature หรือข้อมูล Token ที่อยู่ในส่วน Header เป็นต้น การเข้ารหัสข้อมูล (Encryption) ของมาตรฐาน TGIX จะมุ่งเน้นไปยังส่วน Presentation ของระบบผู้ใช้บริการ ในองค์ประกอบของการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐของระบบผู้ใช้บริการดังรูปที่ 12



รูปที่ 12 องค์ประกอบที่เกี่ยวข้องกับความปลอดภัยของการเข้ารหัสของระบบผู้ใช้บริการการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ

เพื่อให้เป็นไปตามข้อกำหนดพื้นฐานด้านความปลอดภัย การเข้ารหัสข้อมูล (Encryption) ของมาตรฐาน TGIX ของระบบผู้ใช้บริการจะต้องเป็นไปตามข้อกำหนด โดยมีรายละเอียดดังนี้

(1) ในกรณีการส่งข้อมูลที่มีความสำคัญเป็นข้อมูลเชิงธุรกรรมใน Payload หรือ เป็นความลับที่ต้องการการเข้ารหัส ให้ดำเนินการตามข้อตกลงการใช้บริการ (Service Agreement) ที่ทำร่วมกับผู้ให้บริการ

(2) สำหรับการลายมือชื่ออิเล็กทรอนิกส์ เพื่อการรับประกันการยืนยันตัวตนของต้นทาง และความถูกต้องของข้อมูล จะต้องใช้ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) ที่ออกโดย Certification Authority (CA) ที่ดูแลใบรับรองดิจิทัลที่ได้รับอนุญาต เช่น Thailand NRCA และอัลกอลิทึมตามข้อตกลงการใช้บริการ (Service Agreement) ที่ทำร่วมกับผู้ให้บริการ

(3) สำหรับการสร้าง หรือตรวจสอบลายมือชื่อแบบดิจิทัลโดยใช้แฮชฟังก์ชัน (Hash Function) จะต้องใช้ฟังก์ชันตามข้อตกลงการใช้บริการ (Service Agreement) ที่ทำร่วมกับผู้ให้บริการ

4.3.3. ข้อกำหนดการบันทึกกิจกรรมและข้อมูลล็อกและการตรวจสอบ (Logging & Monitoring)

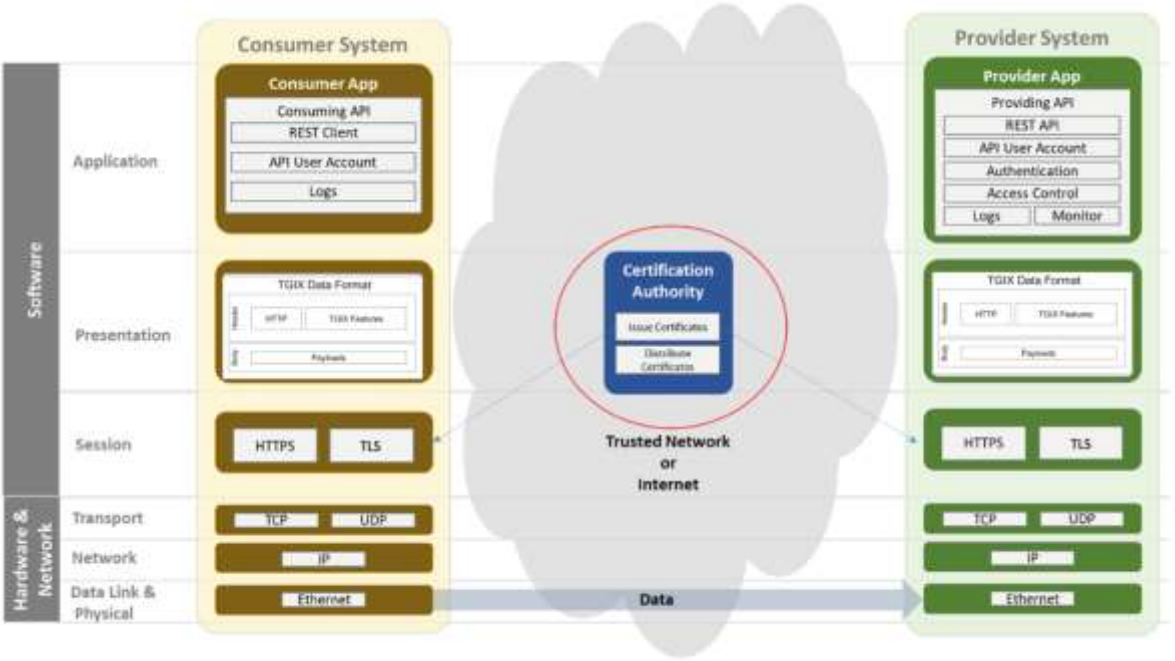
เพื่อให้เป็นไปตามแนวทางการปฏิบัติที่ดีทางด้านความปลอดภัยของการใช้บริการการแลกเปลี่ยนข้อมูล ระบบผู้ใช้บริการจะต้องจัดให้มีการบันทึกข้อมูลล็อกและการตรวจสอบ โดยระบบผู้ใช้บริการจะต้องมีการปฏิบัติตามข้อกำหนด ซึ่งกล่าวในมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่อง ข้อกำหนดของการตรวจสอบระบบและการลงบันทึกล็อก

เนื่องจากข้อกำหนดที่กำหนดไว้ในมาตรฐาน TGIX เป็นข้อกำหนดขั้นพื้นฐาน ให้แต่ละหน่วยงานพิจารณาเพิ่มความเข้มข้นในการดำเนินการตามความเหมาะสมของแต่ละหน่วยงานได้

4.4. ข้อกำหนดด้านความความปลอดภัยขององค์ประกอบอื่น ๆ ตามมาตรฐาน TGIX

4.4.1. ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security)

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



รูปที่ 13 องค์ประกอบที่เกี่ยวข้องกับความปลอดภัยของการส่งข้อมูลของ Certification Authority ในการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ

เพื่อให้การรับส่งข้อมูลสำหรับบริการการแลกเปลี่ยนข้อมูลมีความปลอดภัยและเป็นไปตามข้อกำหนดพื้นฐานด้านความปลอดภัย การสื่อสารเพื่อรับส่งข้อมูลของมาตรฐาน TGIX ของ Certification Authority จะต้องเป็นไปตามข้อกำหนด โดยมีรายละเอียดดังนี้ [4]

(1) การส่งข้อมูลจะต้องดำเนินการบน HTTPS โดยใช้ TLS 1.2 เป็นอย่างน้อย

(2) ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) ควรระบุขนาดของคู่กุญแจที่จะนำไปสร้างใบรับรองอิเล็กทรอนิกส์ อย่างน้อย 2048 bits ที่สร้างด้วย RSA หรืออัลกอริทึมที่เทียบเท่ากัน

(3) ห้ามทำการเปลี่ยนเส้นทาง HTTP ไปยัง HTTPS โดยให้ปฏิเสธการเปลี่ยนเส้นทางทุกกรณี

4.4.2. ข้อกำหนดการเข้ารหัส (Encryption)

การเข้ารหัสข้อมูลของ Certification Authority จะดำเนินการในส่วนการลงลายมือชื่ออิเล็กทรอนิกส์หรือข้อมูลโทเคน (Token) ที่อยู่ในส่วน Header เป็นต้น เพื่อให้เป็นไปตามข้อกำหนดพื้นฐานด้านความปลอดภัย การเข้ารหัสข้อมูล (Encryption) ของ Certification Authority จะต้องเป็นไปตามข้อกำหนด โดยมีรายละเอียดดังนี้ [6]

(1) สำหรับการลงลายมือชื่ออิเล็กทรอนิกส์ เพื่อการรับประกันการยืนยันตัวตนของต้นทางและความถูกต้องของข้อมูลจะต้องใช้ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) ที่ออกโดย Certification Authority (CA) ที่ดูแลใบรับรองดิจิทัลที่ได้รับอนุญาต เช่น Thailand NRCA และจะต้องใช้อัลกอริทึมแบบใดแบบหนึ่ง ดังต่อไปนี้
    ก. อัลกอริทึม DSA (Digital Signature Algorithm) โดยมีขนาดของ Security of strength มากกว่าหรือเท่ากับ 112 bits และ Domain Parameter อย่างน้อย (L, N) = (2048, 224)
    ข. อัลกอริทึม ECDSA (Elliptic Curve-based Digital Signature) โดยมีขนาดของ Security of strength อย่างน้อย 112 bits และ Domain Parameter อย่างน้อย 224 bits
    ค. อัลกอริทึม RSA (Rivest-Shamir-Adelman algorithm) โดยมีขนาดของ Security of strength อย่างน้อย 112 bits และ Domain Parameter อย่างน้อย 2048 bits
(2) สำหรับการสร้างหรือตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ โดยใช้แฮชฟังก์ชัน (Hash Function) จะต้องใช้ฟังก์ชันแบบใดแบบหนึ่ง ดังต่อไปนี้
    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) สำหรับการสร้างหรือตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ โดยใช้แฮชฟังก์ชัน (Hash Function) จะต้องใช้ฟังก์ชันตามข้อตกลงการใช้บริการ (Service Agreement) ที่ทำร่วมกับผู้ให้บริการ
(4) สำหรับการสร้างตัวเลขแบบสุ่ม (Random Bit Generation) เพื่อจุดประสงค์ต่าง ๆ เช่นการสร้างกุญแจ (keys) ตัวเลขแบบใช้ครั้งเดียว (Nonces) และ ค่าสุ่มเพื่อการยืนยันตัวตน (Authentication Challenges) จะต้องใช้อัลกอริทึมแบบใดแบบหนึ่ง ดังต่อไปนี้
    ก. Hash_DRBG
    ข. HMAC_DRBG
    ค. CTR_DRBG โดยใช้ AES-128, AES-192 และ AES-256

4.4.3. ข้อกำหนดการบันทึกกิจกรรมและข้อมูลล็อกและการตรวจสอบ (Logging & Monitoring)

เพื่อให้เป็นไปตามแนวทางการปฏิบัติที่ดีทางด้านความปลอดภัยของการให้บริการการแลกเปลี่ยนข้อมูล Certification Authority จะต้องจัดให้มีการบันทึกข้อมูลล็อกและการตรวจสอบ โดยของ Certification

Authority จะต้องมีการปฏิบัติตามข้อกำหนด ซึ่งกล่าวในมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่องข้อกำหนดของการตรวจสอบระบบและการลงบันทึกล็อก

4.4.4. ข้อกำหนดการจัดการความผิดพลาด (Error Handling)

เพื่อให้เป็นไปตามข้อแนวทางการปฏิบัติที่ดีทางด้านความปลอดภัยของการให้บริการการแลกเปลี่ยนข้อมูล เมื่อบริการที่เปิดให้บริการแสดงข้อความการทำงานผิดพลาด จะต้องไม่เปิดเผยข้อมูลที่มีความเสี่ยงที่สามารถนำมาโจมตีระบบได้ โดย ของ Certification Authority จะต้องจัดให้มีการจัดการข้อผิดพลาดอย่างเหมาะสมอย่างน้อย ดังนี้ [4]

(1) บริการจะต้องปกปิดรหัสหรือข้อความแสดงข้อผิดพลาดอื่นใดนอกเหนือจากสถานะตอบกลับหรือข้อความแสดงข้อผิดพลาดของ HTTP (HTTP status responses และ HTTP error messages) [9] 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

เนื่องจากข้อกำหนดที่กำหนดไว้ในมาตรฐาน TGIX เป็นข้อกำหนดขั้นพื้นฐาน ให้แต่ละหน่วยงานพิจารณาเพิ่มความเข้มข้นในการดำเนินการตามความเหมาะสมของแต่ละหน่วยงานได้

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 การจัดการสิทธิ์ การเข้าถึงข้อมูลส่วนบุคคล การเรียกคืนข้อมูลส่วนบุคคล การปกปิด การลบ การทำลาย หรือการกระทำอื่นใดที่กล่าวถึงข้างต้นโดยไม่คำนึงถึงลักษณะการดำเนินงานหรือวิธีการที่ใช้

กรณีที่การแลกเปลี่ยนข้อมูลเกี่ยวข้องกับการจัดเก็บหรือส่งผ่านข้อมูลส่วนบุคคลจะต้องจัดให้มีการดำเนินการดังตัวอย่างเช่น

(1) ออกแบบและพัฒนาระบบ ให้รองรับการร้องขอและจัดเก็บความยินยอมจากเจ้าของข้อมูลในกรณีมีการร้องขอข้อมูลส่วนบุคคล
(2) ออกแบบและพัฒนาระบบ ให้รองรับขอเปลี่ยนแปลงความยินยอมจากเจ้าของข้อมูลเพื่อรองรับสิทธิ์ของเจ้าของข้อมูลตามกฎหมาย
(3) ออกแบบและพัฒนาระบบ ให้รองรับการขอใช้สิทธิ์ของเจ้าของข้อมูลส่วนบุคคลตามกฎหมาย
(4) ระมัดระวังในการออกแบบและพัฒนาระบบให้มีการจัดเก็บข้อมูลเท่าที่จำเป็นเท่านั้น

เมื่อพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 [10] ถูกบังคับใช้ สมาชิกภายใน Data Exchange Platform จะต้องกำหนดผู้รับผิดชอบในการดำเนินการ บำรุงรักษาระบบ และส่วนที่เกี่ยวข้อง ให้เป็นไปตามข้อกำหนดของมาตรฐานฯ

ก.2 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 [11] เป็นกฎหมายที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ตั้งขึ้นเพื่อป้องกันและควบคุมการกระทำผิดที่จะเกิดขึ้นจากการใช้คอมพิวเตอร์ การปฏิบัติตามกฎหมายครอบคุมทั้งระบบผู้ให้บริการ ระบบผู้ใช้บริการ และองค์ประกอบอื่นตามมาตรฐาน TGIX จะต้องจัดให้มีการดำเนินการ ดังตัวอย่างเช่น

(1) การนำเข้าข้อมูลเพื่อแลกเปลี่ยนข้อมูลภายในมาตรฐาน TGIX ผู้นำเข้าข้อมูลต้องไม่นำเข้าข้อมูลอันเป็นเท็จหรือข้อมูลอื่นใดที่ขัดต่อพระราชบัญญัตินี้

(2) การให้บริการหรือเผยแพร่ข้อมูลภายในมาตรฐาน TGIX ระบบผู้ให้บริการต้องไม่ให้บริการหรือเผยแพร่ข้อมูลอันเป็นเท็จหรือข้อมูลอื่นใดที่ขัดต่อพระราชบัญญัตินี้

ก.3 หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของระบบผู้ให้บริการ พ.ศ. 2564

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

บรรณานุกรม

[1] “ETDA (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์),” 2022. [ออนไลน์]. เข้าถึงได้จาก: https://www.etda.or.th/th/Useful-Resource/Knowledge-Sharing/articles/Public-Key-Infrastructure.aspx. (วันที่ค้นข้อมูล: 8 พฤศจิกายน 2021)

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

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

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

[5] 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)

[6] 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)

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

[8] “OWASP API Security Project,” 2019. [ออนไลน์]. เข้าถึงได้จาก: https://owasp.org/www-project-api-security/.(วันที่ค้นข้อมูล: 8 พฤศจิกายน 2021)

[9] 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)

[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)