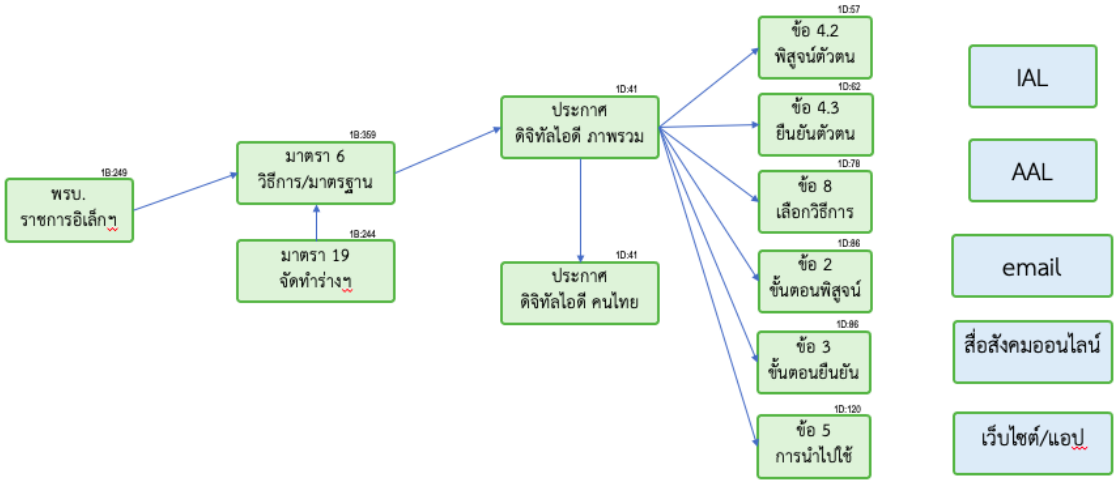
ภาคผนวก ค
ร่างพระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์

พรบ. การปฏิบัติราชการทางอิเล็กทรอนิกส์ บัญญัติขึ้นมาเพื่อส่งเสริมให้หน่วยงานของรัฐปรับเปลี่ยนรูปแบบการบริหารงานและการบริการของรัฐไปสู่ระบบดิจิทัล โดยมีมาตราสำคัญเกี่ยวกับการบูรณาการระบบดิจิทัลคือ มาตรา 6 ระบุว่าคณะรัฐมนตรีต้องกำหนดวิธีการทางอิเล็กทรอนิกส์ และมาตรฐานข้อมูลด้านเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้หน่วยงานของรัฐนำมาใช้ในการพัฒนาระบบดิจิทัลให้สอดคล้องกันและเชื่อมโยงถึงกันได้ ดังแสดงในภาพที่ ค-1



ภาพที่ ค-1 พรบ. การปฏิบัติราชการทางอิเล็กทรอนิกส์

พรบ. การปฏิบัติราชการทางอิเล็กทรอนิกส์ บัญญัติขึ้นมาเพื่อส่งเสริมให้หน่วยงานของรัฐปรับเปลี่ยนรูปแบบการบริหารงานและการบริการของรัฐไปสู่ระบบดิจิทัล โดยมีมาตราสำคัญเกี่ยวกับการบูรณาการระบบดิจิทัลคือ มาตรา 6 ระบุว่าคณะรัฐมนตรีต้องกำหนดวิธีการทางอิเล็กทรอนิกส์ และมาตรฐานข้อมูลด้านเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้หน่วยงานของรัฐนำมาใช้ในการพัฒนาระบบดิจิทัลให้สอดคล้องกันและเชื่อมโยงถึงกันได้

มาตรา 19 ระบุให้ 4 หน่วยงาน ประกอบไปด้วย สำนักงานคณะกรรมการพัฒนาระบบราชการ สำนักงานคณะกรรมการกฤษฎีกา สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ และสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ทำหน้าที่กำหนดรายละเอียดของวิธีการและมาตรฐานตามมาตรา 6 โดยให้ร่วมกันจัดทำวิธีการทางอิเล็กทรอนิกส์เพื่อเสนอต่อคณะรัฐมนตรีนำไปประกาศให้กับหน่วยงานของรัฐใช้และปฏิบัติ ที่ผ่านมาทั้ง 4 หน่วยงานได้ร่วมกันจัดทำวิธีการทางอิเล็กทรอนิกส์ที่เกี่ยวข้องมาอย่างต่อเนื่อง โดยบางเรื่องได้ดำเนินการเสร็จเรียบร้อยแล้ว และบางเรื่องยังอยู่ระหว่างการดำเนินการ

ตัวอย่างวิธีการทางอิเล็กทรอนิกส์ที่ได้จัดทำขึ้นมาเพื่อให้หน่วยงานของรัฐนำไปใช้ในการพัฒนาการบริหารงานและการจัดทำบริการสาธารณะในรูปแบบและช่องทางดิจิทัล ได้แก่ ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานและหลักเกณฑ์การจัดทำกระบวนการและการดำเนินงานทางดิจิทัลว่าด้วยเรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ สำหรับบุคคลธรรมดาที่มีสัญชาติไทย ที่มีสาระสำคัญอยู่ด้วยกัน 6 ข้อ คือ

การลงทะเบียนและพิสูจน์ตัวตน (ข้อ 4.2) เป็นกระบวนการได้มาและการบันทึกข้อมูลไอเดนทิตีที่จำเป็นจากผู้สมัครใช้บริการและการตรวจสอบหลักฐานแสดงตนและตรวจสอบตัวบุคคล ที่ผู้สมัครใช้บริการอ้างความเป็นเจ้าของไอเดนทิตีในระหว่างการลงทะเบียน โดยเปรียบเทียบกับคุณลักษณะของข้อมูลที่มีอยู่เพื่อให้มั่นใจได้ว่าไอเดนทิตีนั้นมีอยู่จริง

การยืนยันตัวตน (ข้อ 4.3) เป็นกระบวนการที่ผู้ใช้บริการครอบครองและใช้ในการยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตนว่าเป็นบุคคลที่กล่าวอ้างจริง โดยอาจจะใช้ปัจจัยของการยืนยันตัวตนเพียงหนึ่งปัจจัยหรือมากกว่าหนึ่งปัจจัยก็ได้ โดยปัจจัยของการยืนยันตัวตนแบ่งออกเป็น 3 ประเภท ดังนี้ สิ่งที่ผู้ใช้บริการรู้ สิ่งที่ผู้ใช้บริการมี และสิ่งที่ผู้ใช้บริการเป็น

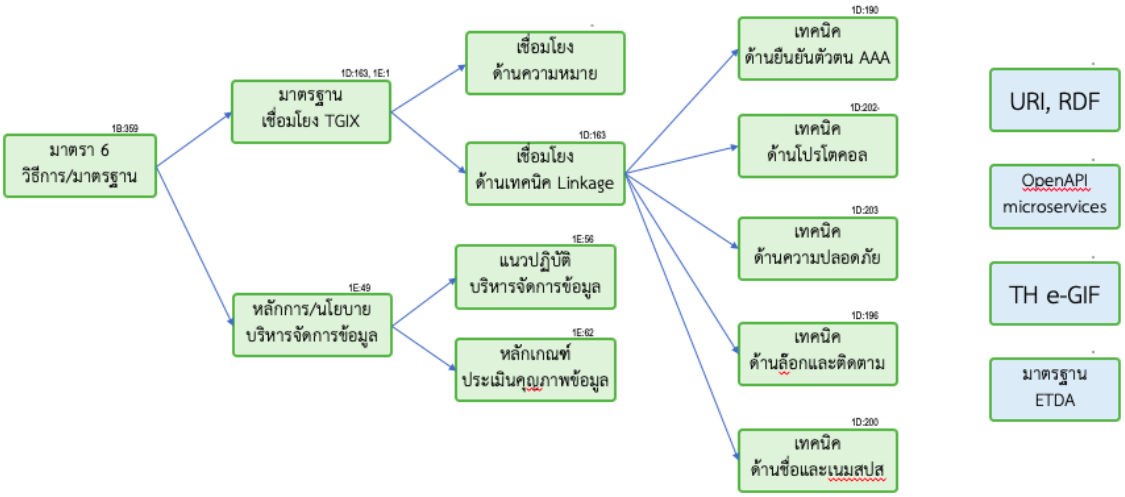
การกำหนดระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (ข้อ 8) ผู้ให้บริการภาครัฐต้องกำหนดระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน โดยนำผลของการประเมินความเสี่ยงมาประกอบกับการพิจารณาเพิ่มเติมที่เกี่ยวข้องกับการยืนยันตัวตน เพื่อให้ผู้ให้บริการภาครัฐเลือกข้อกำหนดของการยืนยันตัวตนที่เหมาะสมที่สุดสำหรับการให้บริการภาครัฐ เมื่อผู้ให้บริการภาครัฐพิจารณากลุ่มการให้บริการภาครัฐ ระดับความน่าเชื่อถือของไอเดนทิตีและรูปแบบการลงทะเบียน

และพิสูจน์ตัวตนทางดิจิทัลสำหรับบริการภาครัฐแล้ว ให้ผู้ให้บริการภาครัฐและผู้พิสูจน์และยืนยันตัวตน จัดให้มีข้อตกลงในการดำเนินการและปฏิบัติตามข้อตกลงนั้น

ข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล (ข้อ 2) การลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัลต้องทำให้มั่นใจได้ว่าผู้สมัครใช้บริการเป็นบุคคลที่กล่าวอ้างจริง โดยผ่านการแสดงต น การตรวจสอบหลักฐานแสดงตน และการตรวจสอบตัวบุคคล โดยหน่วยงานของรัฐควรพิจารณาถึงความสมดุลระหว่างความเป็นส่วนบุคคลและความต้องการที่จะใช้ข้อมูลของผู้ใช้บริการ เพื่อกำหนดเป็นคุณลักษณะขั้นต่ำที่จำเป็นในการพิสูจน์ตัวตนทางดิจิทัล เช่น เลขประจำตัวประชาชน ชื่อ ชื่อสกุล วันเดือนปีเกิด เลขหลังบัตรประจำตัวประชาชน

ข้อกำหนดของการยืนยันตัวตนทางดิจิทัลสำหรับบริการภาครัฐ (ข้อ 3) ให้เป็นไปตามข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทยในการยืนยันตัวตน เป็นการกำหนดระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตนที่เหมาะสมจะช่วยลดโอกาสของการยืนยันตัวตนผิดพลาด แบ่งออกเป็น 3 ระดับ คือ ระดับที่ 1 (AAL1) กำหนดให้ผู้ใช้บริการต้องยืนยันตัวตนแบบปัจจัยเดียว ระดับที่ 2 (AAL2) กำหนดให้ผู้ใช้บริการต้องยืนยันตัวตนแบบ 2 ปัจจัยที่แตกต่างกัน และระดับที่ 3 (AAL3) กำหนดให้ผู้ใช้บริการต้องยืนยันตัวตนแบบ 2 ปัจจัยขึ้นไปที่แตกต่างกัน โดยมีปัจจัยหนึ่งเป็นกุญแจที่ผ่านเกณฑ์วิธีการเข้ารหัสลับซึ่งผู้ใช้บริการต้องพิสูจน์ว่าตนครอบครองกุญแจนั้น และต้องพิสูจน์ว่าตนครอบครองปัจจัยของการยืนยันตัวตนดังกล่าวผ่านโพรโทคอลที่มีความปลอดภัยในการใช้รับส่งข้อมูลระหว่างผู้ใช้บริการและผู้พิสูจน์และยืนยันตัวตน

แนวทางการนำไปใช้ (ข้อ 5) การเลือกใช้รูปแบบ วิธีการ และระดับความน่าเชื่อถือที่เหมาะสมกับบริการภาครัฐเป็นเรื่องที่มีความสำคัญอย่างยิ่ง โดยการออกแบบและการนำไปใช้ต้องมีการพิจารณาประเด็นต่าง ๆ ดังนี้ 1) มีบริการใดบ้างที่จำเป็นต้องใช้ข้อมูลส่วนบุคคลในการให้บริการ 2) จำเป็นต้องลงทะเบียนและพิสูจน์ตัวตนหรือไม่ 3) ผู้เกี่ยวข้องมีบทบาท และหน้าที่อย่างไร 4) ช่องทางดิจิทัลที่ใช้ในการรับส่งข้อมูล เช่น อีเมล หมายเลขโทรศัพท์เคลื่อนที่ สื่อสังคมออนไลน์ เว็บไซต์ 5) ผลกระทบ ระดับความรุนแรง และความสูญเสียที่อาจเกิดขึ้นได้หากการพิสูจน์และยืนยันตัวตนผิดพลาด 6) ระดับความเสี่ยงเทียบกับระดับความน่าเชื่อถือของไอเดนทิตี



ภาพที่ ค-2 วิธีการเชื่อมโยงตาม พรบ. การปฏิบัติราชการทางอิเล็กทรอนิกส์

ร่าง พ.ร.บ. การปฏิบัติราชการทางอิเล็กทรอนิกส์ มาตรา 6 ได้ระบุไว้ว่า “เพื่อประโยชน์ในการดำเนินการตามพระราชบัญญัตินี้ให้มีประสิทธิภาพให้คณะรัฐมนตรีกำหนดวิธีการทางอิเล็กทรอนิกส์ซึ่งรวมถึงมาตรฐานข้อมูลด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่หน่วยงานของรัฐจะต้องใช้และปฏิบัติให้สอดคล้องกันและเชื่อมโยงถึงกันได้” ซึ่งได้มีการกำหนดวิธีการและมาตรฐานเชื่อมโยงไว้ด้วยกันหลายฉบับ ดังแสดงในภาพที่ 1.6-2 เป็นมาตรฐานการเชื่อมโยง และแลกเปลี่ยนข้อมูลภาครัฐ (Thailand Government Information Exchange : TGIX) ตามแผนพัฒนารัฐบาลดิจิทัลของประเทศไทยในการผลักดันให้เกิดการเชื่อมโยงข้อมูลของส่วนราชการ เข้ากับศูนย์ข้อมูลอื่น ๆ รัฐบาลจึงกำหนดให้มีการนำธรรมาภิบาลข้อมูลภาครัฐ (Data Governance : DG) มาเป็นแกนสำคัญในการประยุกต์ใช้ Big Data ภาครัฐเพื่อเพิ่มประสิทธิผลของนโยบายในการพัฒนาประเทศระยะยาว

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) หรือ สพร. ได้สร้างความร่วมมือกับหน่วยงานภาครัฐ เพื่อดำเนินการจัดทำมาตรฐานการเชื่อมโยง และแลกเปลี่ยนข้อมูลภาครัฐ (Thailand Government Information Exchange : TGIX) โดยมีจุดประสงค์เพื่อให้เกิดมาตรฐานในการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ อันนำไปสู่การบูรณาการข้อมูล และการใช้ข้อมูลเพื่อขับเคลื่อนประเทศอย่างมีประสิทธิภาพ ประกอบด้วย 1) มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ในระดับด้านความหมายข้อมูล (Semantic Standard) และ 2) มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ในระดับด้านการเชื่อมโยงข้อมูล (Linkage Standard) ซึ่งเป็นมาตรฐาน

การเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ในระดับด้านการเชื่อมโยงข้อมูล (Linkage Standard) ว่าด้วยเรื่องของสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ

องค์ประกอบของสถาปัตยกรรมของมาตรฐานการเชื่อมโยง และแลกเปลี่ยนข้อมูลภาครัฐ ประกอบด้วย การบริหารจัดการยืนยันตัวตน การควบคุมการเข้าถึง บัญชีผู้ใช้งาน โทเคน และเซสชัน นอกจากนั้นได้มีการกำหนดโปรโตคอลสำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูล ที่มีข้อกำหนดด้านโปรโตคอลระดับแอปพลิเคชัน

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

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

ข้อกำหนดด้านโปรโตคอลที่เกี่ยวข้องกับเอนพอยน์ ข้อกำหนดด้านโปรโตคอลที่เกี่ยวข้องกับเอนพอยน์ (Endpoint URL) ในการเชื่อมโยงและแลกเปลี่ยนข้อมูลตามมาตรฐาน TGIX กำหนดให้ผู้ใช้บริการ API (Consumer System) เรียกใช้งาน Endpoint URL ของผู้ให้บริการ (Provider System) ดังต่อไปนี้ 1) เรียกใช้งานผ่านโปรโตคอล HTTPS เท่านั้น 2) ใช้ TLS version 1.2 เป็นอย่างน้อยสำหรับการใช้งาน TLS/SSL 3) ใช้งาน Transmission Control Protocol (TCP) ผ่าน TLS/SSL เท่านั้น

ข้อกำหนดด้านโครงสร้าง TGIX JSON Data Format ตามมาตรฐาน TGIX การกำหนดโครงสร้าง TGIX JSON Data Format ตามมาตรฐาน TGIX เป็นการกำหนดรูปแบบ โครงสร้างการรับส่งข้อมูลผ่าน REST API ระหว่างผู้ใช้บริการ API (Consumer System) และผู้ให้บริการ API (Provider System) โดยโครงสร้างของ TGIX JSON Data Format สามารถแบ่งตามประเภทการแลกเปลี่ยนข้อมูล ดังนี้ 1) ส่วน TGIX Message Headers ในส่วนของ Message จะประกอบด้วย HTTP Header และ HTTP Body 2) ส่วน TGIX Message Payloads ในส่วนของ Message

ประกอบด้วย HTTP Body เป็นการกำหนดรูปแบบการรับส่งข้อมูลแบบ Multipart Content-Type เพื่อรองรับการรับส่งข้อมูลจากผู้ขอใช้บริการข้อมูลได้หลายรูปแบบ แต่อยู่ภายใต้ Header ที่เป็นเป็น JSON 3) ส่วน TGIX Message Signature ในส่วนของ Message จะประกอบด้วย HTTP Body เป็นการตรวจสอบความถูกต้องและครบถ้วนของข้อมูลที่รับส่งระหว่างผู้ใช้บริการและผู้ให้บริการ โดยการนำข้อมูล Header และ Payloads ที่ได้รับมาไปเข้ารหัสเทียบกับค่าของ sigValue ที่ถอดรหัสแล้ว ถ้าตรงกันจะถือว่าข้อมูลที่รับส่งนั้นครบถ้วนสมบูรณ์ 4) โครงสร้าง TGIX JSON Data Format กรณีการแลกเปลี่ยนข้อมูลเชิงธุรกรรมการแลกเปลี่ยนข้อมูลเชิงธุรกรรม โดยกำหนดลักษณะ Payload เป็น JSON ทั้งข้อความ โดยกำหนด Content Type เป็นประเภท JSON

ข้อกำหนดด้านความน่าเชื่อถือและความมั่นคงปลอดภัย มาตรฐานการเชื่อมโยงและการแลกเปลี่ยนข้อมูลภาครัฐระดับการเชื่อมโยงข้อมูลมีความมุ่งเน้นและให้ความสำคัญในเรื่องของความปลอดภัยและการเข้ารหัสของการแลกเปลี่ยนข้อมูลระหว่างผู้ใช้บริการ API (Consumer System) และผู้ให้บริการ API (Provider System) การกำหนดมาตรฐานในด้านความปลอดภัยและการเข้ารหัสข้อมูลที่มีการรับส่งระหว่างกันจึงเป็นสิ่งจำเป็นที่จะช่วยการลดความเสี่ยงในด้านความปลอดภัยลงได้ ในส่วนนี้จะอธิบายหลักการขั้นพื้นฐานของมาตรฐานความปลอดภัยของมาตรฐานการเชื่อมโยงและการแลกเปลี่ยนข้อมูลภาครัฐระดับการเชื่อมโยงข้อมูลที่กำหนดขึ้นเพื่อให้เป็นมาตรฐานความน่าเชื่อถือและความมั่นคงปลอดภัยการเชื่อมโยงและแลกเปลี่ยนข้อมูล โดยอ้างอิงจากหลักการในเรื่องความปลอดภัยสารสนเทศ (Information Security : InfoSec) ซึ่งประกอบไปด้วยส่วนสำคัญ 3 เรื่อง คือ Confidentiality, Integrity และ Availability หรือที่รู้จักกันคือ CIA Triad

วัตถุประสงค์ของข้อกำหนดพื้นฐานด้านความน่าเชื่อถือและความมั่นคงปลอดภัยคือการรักษาความลับของข้อมูล (Confidentiality) การรักษาความลับของข้อมูลคือการเก็บรักษาข้อมูลให้เป็นความลับและอนุญาตให้เฉพาะผู้ที่ได้รับอนุญาตเข้าถึงข้อมูลได้โดยการจำกัดสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานในระบบ (ผู้ที่มีส่วนเกี่ยวข้องในการเชื่อมโยงและการแลกเปลี่ยนข้อมูล) ด้วยการยืนยันตัวตน (Authentication) และการตรวจสอบสิทธิ์ (Authorization) ในการเข้าถึงทรัพยากร เพื่อให้มั่นใจได้ว่าจะไม่มีการเข้าถึงข้อมูลจากผู้ที่ไม่ได้รับอนุญาตมาตรฐานการเชื่อมโยงและการแลกเปลี่ยนข้อมูลภาครัฐระดับการเชื่อมโยงข้อมูล (TGIX) ใช้การส่งผ่านข้อมูลในระบบที่อาจผ่านเครือข่ายสาธารณะเช่น Internet จึงมีการกำหนดให้ใช้วิธีการส่งข้อมูลด้วยกระบวนการที่มีความปลอดภัยสูง เช่น Digital Signature และการเข้ารหัสข้อมูล (Data Encryption) ซึ่งข้อมูลจะต้องถูกส่งผ่านโปรโตคอล HTTPS บน Transport Layer Security (TLS) ที่จะช่วยป้องกันการดักฟังและป้องกันการโจรกรรมข้อมูล

นอกจากนั้นการแลกเปลี่ยนข้อมูลผ่านมาตรฐาน TGIX ได้มีข้อกำหนดเพื่อให้มันใจว่าการแลกเปลี่ยนข้อมูลมีความปลอดภัย ประกอบด้วย 1) ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล (Transport Security) 2) ข้อกำหนดการเข้ารหัส (Encryption) 3) ข้อกำหนดด้าน Authentication Access Control และ Accounting ซึ่งกล่าวในมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูลเรื่องข้อกำหนดด้านการยืนยันตัวตนการกำหนดสิทธิ์ และบัญชีการใช้งาน 4) ข้อกำหนดด้านการบริหารจัดการ Token และ Session ซึ่งกล่าวในมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูลเรื่องข้อกำหนดของโปรโตคอลระดับแอปพลิเคชันเอนพอยน์และการจัดการโทเคนและเซสชัน

ความถูกต้องของข้อมูลคือ การตรวจสอบและทำให้มั่นใจว่าข้อมูลที่มีการแลกเปลี่ยนกันภายในมาตรฐาน TGIX มีความถูกต้องและสมบูรณ์ครบถ้วน ไม่ถูกแก้ไขหรือทำให้ได้รับความเสียหายแก่ข้อมูลที่แลกเปลี่ยนกันภายใน TGIX ซึ่งได้มีข้อกำหนดที่เกี่ยวข้อง ได้แก่ 1) ข้อกำหนดด้านความปลอดภัยของการส่งข้อมูล 2) ข้อกำหนดการจำกัดอัตราการเข้าถึงบริการและใช้ทรัพยากร (Resource and Rate Limit) (3) ข้อกำหนดการบันทึกกิจกรรมและข้อมูลจราจรคอมพิวเตอร์และการสอดส่อง 4) ข้อกำหนดการจัดการความผิดพลาด 5) ข้อกำหนดการตรวจสอบข้อมูลนำเข้า

ความพร้อมให้บริการคือ ความพร้อมใช้งานหรือให้บริการของระบบได้อย่างต่อเนื่อง เพื่อทำให้มั่นใจว่าองค์ประกอบต่าง ๆ ในมาตรฐาน TGIX มีความพร้อมให้บริการกับองค์ประกอบอื่นในมาตรฐาน TGIX ที่มีความเกี่ยวข้องกัน และเพื่อบรรเทาผลกระทบจากการไม่สามารถให้บริการได้จนนำไปสู่ผลกระทบกับผู้ใช้บริการ ซึ่งได้มีข้อกำหนดที่เกี่ยวข้องดังต่อไปนี้ 1) ข้อกำหนดเกี่ยวกับการป้องกันการโจมตี 2) ข้อกำหนดการจำกัดอัตราการเข้าถึงบริการและใช้ทรัพยากร (Resource and Rate Limit) 3) ข้อกำหนดการตรวจสอบข้อมูลนำเข้า (Input Validation) จากหลักการขั้นพื้นฐานทั้ง 3 ข้างต้น คือ การรักษาความลับ (Confidentiality) ความถูกต้องของข้อมูล (Integrity) และความพร้อมให้บริการ (Availability) โดยมาตรฐานการเชื่อมโยงและการแลกเปลี่ยนข้อมูลภาครัฐระดับการเชื่อมโยงข้อมูลจัดให้มีข้อกำหนดเพื่อเป็นกรอบแนวทางการปฏิบัติตามแนวทางการปฏิบัติที่ดี โดยจะครอบคลุมผู้ให้บริการ ผู้ใช้บริการ และองค์ประกอบอื่น ๆ ตามมาตรฐาน TGIX

ภาพรวมองค์ประกอบของการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐสามารถแบ่งข้อกำหนดเป็น 4 ส่วน คือ 1) ข้อกำหนดด้านความปลอดภัยของผู้ให้บริการ 2) ข้อกำหนดด้านความปลอดภัยของผู้ใช้บริการ 3) ข้อกำหนดด้านความปลอดภัยขององค์ประกอบอื่น ๆ ตามมาตรฐาน TGIX และ 4) ข้อกำหนดด้านความปลอดภัยที่เกี่ยวข้องกับกฎหมาย

การบันทึกข้อมูลเชิงเทคนิค (Technical logs) จะบันทึกข้อมูลในส่วนของ TGIX Message Header และใช้ส่งข้อมูลการเชื่อมโยงไปยัง TGIX Service Operation Center (SOC) โดย

กำหนดการส่งข้อมูลการเชื่อมโยงอย่างน้อยชั่วโมงละ 1 ครั้ง อ้างอิงตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 จะต้องระบุ วัน เวลา ข้อมูลที่สามารถระบุตัวผู้ใช้บริการได้และหมายเลขข้อมูลต้นทาง ปลายทาง เพื่อไว้ใช้ตรวจสอบได้กำหนดให้บันทึกทุกกิจกรรมการพยายามยืนยันตัวตนที่ล้มเหลว การปฏิเสธการเข้าถึง และการตรวจสอบข้อมูลนำเข้าที่ไม่ถูกต้องบันทึกควรอยู่ในรูปแบบที่สามารถนำเข้าระบบจัดการบันทึกล็อค (Log Management) ได้ง่าย ควรมีข้อมูลเพียงพอต่อการระบุผู้กระทำที่น่าสงสัย และเป็นไปตามหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564

การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานเป็นพื้นฐานหลักที่จำเป็นต่อการพัฒนารัฐบาลดิจิทัล ในปัจจุบันประเทศไทยมีแพลตฟอร์มการแลกเปลี่ยนข้อมูลที่ให้บริการอยู่หลายแห่ง แพลตฟอร์มแต่ละแห่งมีแนวทางและพันธกิจในการดำเนินงานเป็นของตนเอง เป็นผลให้การบูรณาการข้อมูลภาครัฐจำเป็นต้องขับเคลื่อนด้วยการสร้างมาตรฐานหรือข้อตกลงร่วมกันในการแลกเปลี่ยนข้อมูลสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ได้เล็งเห็นความสำคัญในจุดนี้ จึงมีความจำเป็นต้องจัดทำมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ เพื่อใช้ในการ แลกเปลี่ยนข้อมูลระหว่างหน่วยงานของรัฐเพื่อให้เกิดการบูรณาการข้อมูลเกิดขึ้นอย่างเป็นรูปธรรม เป้าประสงค์หลักของการใช้มาตรฐานฯ เป็นตัวขับเคลื่อนการบูรณาการข้อมูลภาครัฐคือ การให้หน่วยงานของรัฐมีแนวทางในการพัฒนาสถาปัตยกรรมระบบสารสนเทศเพื่อใช้ในการแลกเปลี่ยนข้อมูลที่ชัดเจน มีความสอดคล้องในการเชื่อมต่อระหว่างกันดังนั้นเพื่อให้บรรลุเป้าประสงค์หลักดังกล่าวเอกสารฉบับนี้จึงนำเสนอข้อกำหนดด้านการกำหนดชื่อและเนมสเปซ สำหรับประกอบเอกสารว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ เรื่องมาตรฐานสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐระดับการเชื่อมโยงข้อมูลที่เหมาะสมกับบริบทของประเทศไทยเท่านั้น

การกำหนดเนมสเปซ เป็นข้อกำหนดการออกแบบและพัฒนาการให้บริการข้อมูลผ่าน API ประเภท REST ให้เป็นไปตามมาตรฐานการเชื่อมโยงและการแลกเปลี่ยนข้อมูลภาครัฐด้านการเชื่อมโยงข้อมูลสำหรับผู้ให้บริการ API (Provider System) เพื่อให้ผู้ใช้บริการ API (Consumer System) สามารถเข้าถึงเข้าถึงทรัพยากรข้อมูล (Data Resource) ที่ให้บริการได้อย่างถูกต้องและปลอดภัย การกำหนดเนมสเปซของระบบ ตามมาตรฐานการเชื่อมโยงและการแลกเปลี่ยนข้อมูลภาครัฐด้านการเชื่อมโยงข้อมูลมีแนวทางดำเนินการ ดังนี้

- การกำหนดโครงสร้างของ URI (Uniform Resource Identifier) เป็นการระบุที่อยู่ของทรัพยากรข้อมูล (Data Resource) ที่ให้บริการ โดยการกำหนดโครงสร้าง URI นั้นจะอ้างอิงตามมาตรฐานการกำหนด Uniform Resource Identifier (URI) : Generic Syntax (RFC-3986)

- การกำหนดรูปแบบ Query ผู้ให้บริการ API (Provider System) สามารถกำหนดรูปแบบ Query ซึ่งมีแนวทางในการกำหนดดังนี้
  (1) ควรใช้ _ (Underscore) ในการคั่นคำ
  (2) ควรเป็นตัวพิมพ์เล็กทั้งหมด (Lower-case)
  (3) ควรใช้ในกรณีการจัดเรียงข้อมูล (Sorting) หรือกรองข้อมูล (Filtering) เท่านั้น
  (4) ควรกำหนดเป็นภาษาอังกฤษเท่านั้น
  (5) ไม่ควรใช้ตัวอักษรที่เป็นข้อมูล Sensitive
- การกำหนดเวอร์ชันของ API ผู้ให้บริการ API (Provider System) สามารถกำหนดโดยอ้างอิงตามมาตรฐาน Semantic Versioning ซึ่งการปรับเปลี่ยนเวอร์ชันจะเปลี่ยนเมื่อมีการอัพเกรดของ API และเป็นการป้องกันการเกิดปัญหาการเรียกใช้บริการโดยไม่แจ้งการเปลี่ยนแปลงล่วงหน้า (Breaking API) โดยเวอร์ชันจะกำหนดเป็นส่วนหนึ่งใน URI

ด้วยสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ได้ให้ความสำคัญกับการบริหารจัดการข้อมูล และการทำงานให้มีความสอดคล้องกัน เพื่อให้สามารถเชื่อมโยงข้อมูลเข้าด้วยกันอย่างมั่นคงปลอดภัยและ มีธรรมาภิบาล โดยดำเนินการกำหนดนโยบายหรือกฎเกณฑ์การเข้าถึงและใช้ประโยชน์จากข้อมูลที่ชัดเจนและมีระบบบริหารจัดการ รวมทั้งมีมาตรการและหลักประกันในการคุ้มครองข้อมูลที่อยู่ในความครอบครองให้มีความมั่นคงปลอดภัยและมิให้ข้อมูลส่วนบุคคลถูกละเมิด ดังนั้น จึงได้จัดทำข้อเสนอแนะสำหรับการจัดทำนโยบายและแนวปฏิบัติการบริหารจัดการข้อมูล (Recommendation for Writing Data Management Policy and Guideline) เพื่อเป็นคู่มือการใช้งานเอกสารแม่แบบนโยบายและแนวปฏิบัติการบริหารจัดการข้อมูล (Data Management Policy and Guideline Template) โดยหน่วยงานภาครัฐสามารถใช้เป็นตัวอย่างในการจัดทำนโยบายและแนวปฏิบัติการบริหารจัดการข้อมูลของหน่วยงาน ซึ่งจะเป็นกรอบและแนวทางในการบริหารจัดการข้อมูลให้มีความมั่นคงปลอดภัย มีความโปร่งใส และสามารถตรวจสอบได้ รวมทั้งเพื่อให้ข้อมูลของหน่วยงาน มีคุณภาพ เป็นที่ยอมรับและเชื่อถือของผู้ใช้งาน และสามารถนำไปบูรณาการกับหน่วยงานต่าง ๆ ได้อย่างมีประสิทธิภาพ

อาศัยอำนาจตามความในมาตรา 8 (2) มาตรา 29 และมาตรา 30 แห่งพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) พ.ศ. 2561 จึงออกประกาศเรื่องมาตรฐานของสำนักงาน พัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยข้อเสนอแนะสำหรับการจัดทำนโยบายการ

บริหารจัดการข้อมูล เลขที่ มสพร. 2-1 : 2564 และมาตรฐานว่าด้วยข้อเสนอแนะสำหรับการจัดทำแนวปฏิบัติการบริหารจัดการ ข้อมูล เลขที่ มสพร. 2-2 : 2564 แนบท้ายประกาศฉบับนี้ เพื่อยึดถือเป็นแนวทางปฏิบัติภายในของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

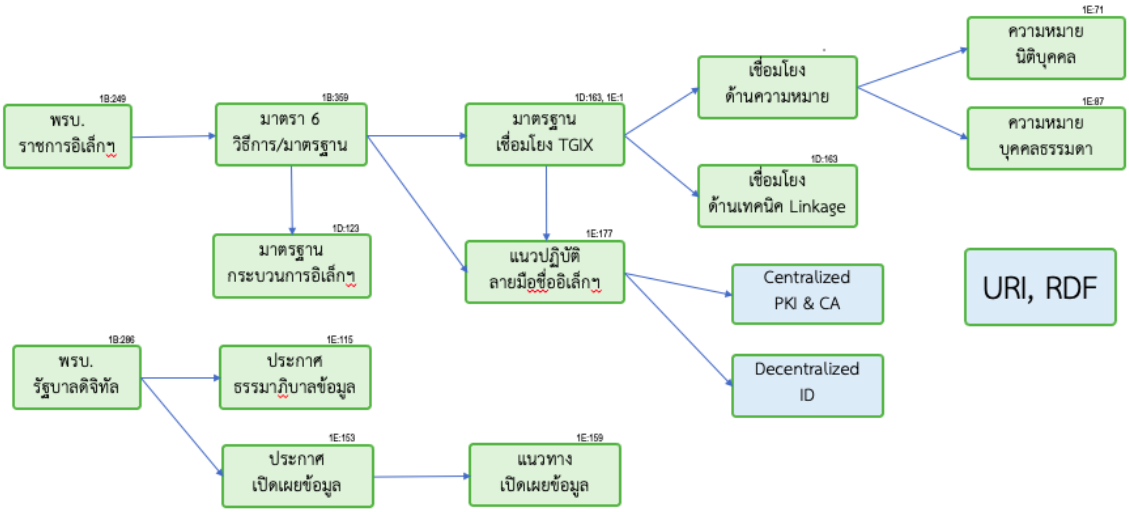
ข้อเสนอแนะสำหรับการจัดทำนโยบายการบริหารจัดการข้อมูลฉบับนี้จัดทำขึ้นเพื่อเป็นคู่มือการใช้งานเอกสารแม่แบบนโยบายการบริหารจัดการข้อมูล (Data Management Policy Template) ให้หน่วยงาน ภาครัฐใช้เป็นตัวอย่างในการจัดทำนโยบายการบริหารจัดการข้อมูลของหน่วยงาน ซึ่งจะเป็นกรอบและแนวทาง ในการบริหารจัดการข้อมูลให้มีความมั่นคงปลอดภัย มีความโปร่งใส และสามารถตรวจสอบได้ รวมทั้งเพื่อให้ ข้อมูลของหน่วยงานมีคุณภาพ เป็นที่ยอมรับและเชื่อถือของผู้ใช้งาน และสามารถนำไปบูรณาการกับหน่วยงานต่าง ๆ ได้อย่างมีประสิทธิภาพโดยข้อเสนอแนะฉบับนี้ได้จัดทำตามมาตรฐานและแนวทางแห่ง

1. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562
2. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ

และได้มีการจัดงานประชาพิจารณ์เพื่อเปิดรับฟังความคิดเห็นเป็นการทั่วไป และนำข้อมูลข้อสังเกต ข้อคิดเห็นจากผู้ทรงคุณวุฒิและจากหน่วยงานที่เกี่ยวข้อง เพื่อให้ข้อเสนอแนะเกี่ยวกับมาตรฐานฉบับนี้มีความสมบูรณ์ครบถ้วน และสามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพ

ข้อเสนอแนะสำหรับการจัดทำแนวปฏิบัติการบริหารจัดการข้อมูลจัดทำขึ้น เพื่อเป็นคู่มือการใช้งาน เอกสารแม่แบบแนวปฏิบัติการบริหารจัดการข้อมูล (Data Management Guideline Template) ซึ่งเป็นข้อเสนอแนะให้หน่วยงานภาครัฐนำ Template ไปใช้เป็นตัวอย่างในการจัดทำแนวปฏิบัติการบริหารจัดการ ข้อมูลของหน่วยงานให้สอดคล้องตามนโยบายด้านข้อมูลที่หน่วยงานจัดทำและประกาศใช้ และให้เหมาะสมกับบริบทของการทำงาน ระบบ จัดเก็บข้อมูล (Legacy System) และระบบเทคโนโลยีสารสนเทศและเครื่องมือ สำหรับการบริหารจัดการข้อมูลของหน่วยงาน รวมทั้งเป็นไปตามบทบัญญัติของกฎหมายและระเบียบที่เกี่ยวข้อง โดยข้อเสนอแนะฉบับนี้ จะแสดงคำอธิบายลักษณะของ Template คำแนะนำและเงื่อนไขในการ ใช้งาน Template ซึ่งเป็นเพียงแนวทางที่ใช้อธิบายเพื่อประกอบความเข้าใจในการจัดทำแนวปฏิบัติการ บริหารจัดการข้อมูลของหน่วยงาน ส่วนการบังคับใช้เป็นไปตามพระราชบัญญัติการบริหารงานและการ ให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 มาตรา 8 (4) และประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัลเรื่องธรรมาภิบาลข้อมูลภาครัฐ ข้อ 4 (5) อันจะนำไปสู่การบริหารจัดการข้อมูลภาครัฐอย่างเป็นระบบ รวมทั้งสนับสนุนการจัดทำบัญชีข้อมูลหน่วยงานให้ได้มาตรฐานและเป็นไปในทิศทางเดียวกัน สอดคล้องตามกรอบธรรมาภิบาลข้อมูลภาครัฐ

หลักเกณฑ์การประเมินคุณภาพข้อมูลสำหรับหน่วยงานภาครัฐทำขึ้นเพื่อเป็นกรอบและเครื่องมือการประเมินคุณภาพ ของข้อมูล เพื่อให้หน่วยงานภาครัฐใช้ในการตรวจสอบและประเมินคุณภาพข้อมูลเบื้องต้น ซึ่งจะช่วยในการบริหารจัดการคุณภาพข้อมูลอย่างมีประสิทธิภาพ และช่วยให้ได้ข้อมูลที่มีคุณภาพอันจะนำไปใช้ประโยชน์ได้อย่างเต็มที่ โดยมีกรอบการประเมินคุณภาพข้อมูลสำหรับหน่วยงานภาครัฐ หรือ DQAF ที่จัดทำขึ้น เป็นแนวทางการประเมินคุณภาพข้อมูลเบื้องต้นตามกรอบธรรมาภิบาลข้อมูลภาครัฐ โดยจัดทำเกณฑ์ตัวชี้วัดคุณลักษณะ ผลผลิตข้อมูลตามมิติคุณภาพข้อมูลตามกรอบธรรมาภิบาลข้อมูลภาครัฐที่พิจารณาเปรียบเทียบกมาตรฐานสากล เพื่อนำมาประยุกต์ใช้และกำหนดเป็นเกณฑ์ประเมินคุณภาพข้อมูลให้มีความเหมาะสมกับหน่วยงานภาครัฐ จัดทำเครื่องมือการประเมินคุณภาพข้อมูลด้วยตนเอง และข้อเสนอแนะสำหรับดำเนินการประเมินคุณภาพข้อมูล



ภาพที่ ค-3 พรบ. การปฏิบัติราชการทางอิเล็กทรอนิกส์ และ พรบ. รัฐบาลดิจิทัล

อย่างไรก็ตามบทบัญญัติของกฎหมายที่ใช้บังคับอยู่ในปัจจุบันส่วนใหญ่ยังไม่เอื้อต่อการนำวิธีการทางอิเล็กทรอนิกส์มาใช้ในการอนุญาต การให้บริการ หรือการให้สวัสดิการแก่ประชาชน ส่งผลให้ประชาชนมีภาระและต้นทุนในการติดต่อกับภาครัฐที่สูงเกินสมควร เป็นอุปสรรคต่อการเสริมสร้างความสามารถในการแข่งขันของประเทศ และไม่สอดคล้องกับเทคโนโลยีที่พัฒนาไปอย่างรวดเร็ว ดังนั้นจึงมีการจัดทำพระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ ซึ่งเป็นกฎหมายกลางว่าด้วยการปฏิบัติราชการทางอิเล็กทรอนิกส์เพื่อส่งเสริมให้การทำงาน และการให้บริการของภาครัฐสามารถใช้วิธีการทางอิเล็กทรอนิกส์เป็นหลักได้ ซึ่งได้ผ่านมติคณะรัฐมนตรีเรียบร้อยแล้ว กำลังอยู่ในระหว่างการดำเนินการประกาศใช้