ประกาศสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ที่ ม ๒/๒๕๖๖

เรื่อง มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล

.....

ด้วยสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ได้ให้ความสำคัญกับการสนับสนุนการดำเนินการของหน่วยงานของรัฐในการให้บริการประชาชนผ่านระบบดิจิทัลอย่างเต็มรูปแบบในการขับเคลื่อนประเทศในด้านต่าง ๆ ซึ่งกลไกสำคัญในการทำให้การบริการประชาชนผ่านระบบดิจิทัลทำงานได้อย่างมีประสิทธิภาพ คือ การเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลระหว่างหน่วยงานของรัฐ และการบูรณาการข้อมูลร่วมกัน โดยสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ทำหน้าที่ในการให้บริการ ส่งเสริม และสนับสนุนการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานของรัฐ ดังนั้น จึงได้จัดทำมาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูลที่ระบุ วิธีการเชื่อมโยงข้อมูลดิจิทัลระหว่างหน่วยงานของรัฐ เนื่องจากมีความจำเป็นในการให้บริการประชาชนและมีความสำคัญในการนำไปใช้ร่วมกับข้อมูลด้านอื่น เพื่อให้เกิดการแลกเปลี่ยนข้อมูลระหว่างระบบสารสนเทศได้อย่างมีความมั่นคงปลอดภัย มีความถูกต้องแม่นยำ และอยู่ภายใต้ข้อกำหนดของกฎหมายที่เกี่ยวข้อง รวมถึงเพื่อให้เป็นมาตรฐานในการทำงานร่วมกัน (Interoperability) ระหว่างหน่วยงานของรัฐ และให้การทำงานมีประสิทธิภาพมากยิ่งขึ้น

อาศัยอำนาจตามความในมาตรา ๘ (๒) มาตรา ๒๙ และมาตรา ๓๐ แห่งพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) พ.ศ. ๒๕๖๑ จึงออกประกาศ เรื่อง มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล จำนวน ๖ เรื่อง แนบท้ายประกาศฉบับนี้ เพื่อยึดถือเป็นแนวทางปฏิบัติภายในสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ประกอบด้วย

๑) มาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่อง สถาปัตยกรรมอ้างอิง เลขที่ มสพร. ๑๐-๑ : ๒๕๖๖
๒) มาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่อง ข้อกำหนดด้านการยืนยันตัวตน การควบคุมสิทธิ และบัญชีการใช้งาน เลขที่ มสพร. ๑๐-๒ : ๒๕๖๖

๓) มาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่อง ข้อกำหนดด้านโปรโตคอลระดับแอปพลิเคชัน เอนพอยน์ และการจัดการโทเคนและเซสชัน เลขที่ มสพร. ๑๐-๓ : ๒๕๖๖

๔) มาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่อง ข้อกำหนดด้านความน่าเชื่อถือและความมั่นคงปลอดภัย เลขที่ มสพร. ๑๐-๔ : ๒๕๖๖

๕) มาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่อง ข้อกำหนดด้านการตรวจสอบระบบและการลงบันทึกล็อก เลขที่ มสพร. ๑๐-๕ : ๒๕๖๖

๖) มาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่อง ข้อกำหนดด้านการกำหนดชื่อและเนมสเปซ เลขที่ มสพร. ๑๐-๖ : ๒๕๖๖

จึงประกาศให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่ ๓๑ พฤษภาคม พ.ศ. ๒๕๖๖

(นายสุพจน์ เธียรวุฒิ)
ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

dcf99e6b

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

DGA Community Standard

มสพร. 10-3 : 2566

DGA 10-3 : 2566

ว่าด้วย มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่องข้อกำหนดด้านโปรโตคอล ระดับแอปพลิเคชัน เอนพอยน์ และการจัดการโทเคนและเซสชัน

(THAILAND GOVERNMENT INFORMATION EXCHANGE STANDARD, SERIES: LINKAGE STANDARD, PART 3: STANDARD REGULATIONS FOR APPLICATION PROTOCOL, END-POINT, TOKEN AND SESSION MANAGEMENT)

เวอร์ชัน 1.0

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
สำนักนายกรัฐมนตรี

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ว่าด้วย มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่องข้อกำหนดด้านโปรโตคอล ระดับแอปพลิเคชัน เอนพอยน์ และการจัดการโทเคนและเซสชัน

มสพร. 10-3 : 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 กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ
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 เรื่องข้อกำหนดด้านโปรโตคอลระดับแอปพลิเคชัน เอนพอยน์ และการจัดการโทเคนและเซสชัน

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

มาตรฐานฉบับนี้เป็นมาตรฐานลำดับที่ 3 ในกลุ่มมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่อง ข้อกำหนดด้านโปรโตคอลระดับแอปพลิเคชัน เอนพอยน์ และการจัดการโทเคนและเซสชัน กล่าวถึงข้อกำหนดด้านโปรโตคอล (Protocol) ระดับแอปพลิเคชัน เอนพอยน์ (Endpoint) การจัดการโทเคน (Token) และเซสชัน (Session) เพื่อให้เกิดข้อตกลงร่วมกันในการกำหนดค่า เอนพอยน์ โทเคน และเซสชัน ในการทำงานได้อย่างมีประสิทธิภาพ มีความถูกต้องแม่นยำ และมีความมั่นคงปลอดภัย

สารบัญ

สารบัญรูป

สารบัญตาราง

มาตรฐานรัฐบาลดิจิทัล
ว่าด้วย มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ
ด้านการเชื่อมโยงข้อมูล เรื่อง ข้อกำหนดด้านโปรโตคอลระดับแอปพลิเคชัน เอนพอยน์ และการจัดการโทเคนและเซสชัน

1. ขอบข่าย

การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานเป็นพื้นฐานหลักที่จำเป็นต่อการพัฒนารัฐบาลดิจิทัล ในปัจจุบันประเทศไทยมีแพลตฟอร์มการแลกเปลี่ยนข้อมูลที่ให้บริการอยู่หลายแห่ง แพลตฟอร์มแต่ละแห่งมี แนวทางและพันธกิจในการดำเนินงานเป็นของตนเอง เป็นผลให้การบูรณาการข้อมูลภาครัฐจำเป็นต้อง ขับเคลื่อนด้วยการสร้างมาตรฐานหรือข้อตกลงร่วมกันในการแลกเปลี่ยนข้อมูลสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ได้เล็งเห็นความสำคัญในจุดนี้ จึงมีความจำเป็นต้องจัดทำมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ เพื่อใช้ในการ แลกเปลี่ยนข้อมูลระหว่างหน่วยงานของรัฐเพื่อให้เกิดการบูรณาการข้อมูลเกิดขึ้นอย่างเป็นรูปธรรม

เป้าประสงค์หลักของการใช้มาตรฐานฯ เป็นตัวขับเคลื่อนการบูรณาการข้อมูลภาครัฐ คือ การให้หน่วยงาน ของรัฐมีแนวทางในการพัฒนาสถาปัตยกรรมระบบสารสนเทศเพื่อใช้ในการแลกเปลี่ยนข้อมูลที่ชัดเจน มีความสอดคล้องในการเชื่อมต่อระหว่างกัน

มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ฉบับนี้ มีขอบเขตมาตรฐานที่ระดับการเชื่อมโยงข้อมูลเท่านั้น ไม่ได้ครอบคลุมถึงระดับการจัดการข้อมูลทางธุรกรรมของหน่วยงาน (Business Transaction Data) ที่เกิดขึ้นจากการเชื่อมโยงและแลกเปลี่ยนระหว่างกัน

ดังนั้นเพื่อให้บรรลุเป้าประสงค์หลักดังกล่าวเอกสารฉบับนี้จึงนำเสนอ ข้อกำหนดด้านโปรโตคอลระดับแอปพลิเคชัน เอนพอยน์ และการจัดการโทเคนและเซสชัน สำหรับประกอบเอกสารว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ เรื่องมาตรฐานสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ระดับการเชื่อมโยงข้อมูลที่เหมาะสมกับบริบทของประเทศไทยเท่านั้น

2. นิยาม

นิยามคำศัพท์ที่เกี่ยวข้องกับมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐด้านการเชื่อมโยงข้อมูล เรื่อง ข้อกำหนดด้านโปรโตคอลระดับแอปพลิเคชัน เอนพอยน์ และการจัดการโทเคนและเซสชันที่ ใช้เอกสารฉบับนี้มีดังนี้

2.1 โปรโตคอล HTTP หมายความว่า โปรโตคอลเครือข่ายพื้นฐานที่ช่วยให้สามารถถ่ายโอนเอกสารสื่อหลายมิติ (Hypermedia) บนเว็บ โดยทั่วไปคือระหว่างเบราว์เซอร์และเครื่องแม่ข่ายที่มนุษย์สามารถอ่านได้

2.2 โปรโตคอล HTTPS หมายความว่า โปรโตคอล HTTP ในรูปแบบที่เข้ารหัส ใช้ SSL หรือ TLS เพื่อเข้ารหัสการสื่อสารทั้งหมดระหว่างเครื่องลูกข่ายและเครื่องแม่ข่าย

2.3 Transport Layer Security (TLS) หมายความว่า โปรโตคอลที่แอปพลิเคชันใช้เพื่อสื่อสารอย่างปลอดภัยผ่านเครือข่าย ป้องกันการปลอมแปลงและดักฟังอีเมล การท่องเว็บ การส่งข้อความ และโปรโตคอลอื่น ๆ ทั้ง SSL และ TLS เป็นโปรโตคอลเครื่องลูกข่าย/เครื่องแม่ข่าย (Client/Server) ที่รับรองความเป็นส่วนตัวของการสื่อสารโดยใช้โปรโตคอลการเข้ารหัสเพื่อให้ความปลอดภัยผ่านเครือข่าย เมื่อเครื่องแม่ข่ายและเครื่องลูกข่ายสื่อสารโดยใช้ TLS จะทำให้มั่นใจได้ว่าไม่มีบุคคลที่สามใดสามารถดักฟังหรือยุ่งเกี่ยวกับข้อความใด ๆ ได้

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

2.5 Application Programming Interface หรือ API หมายความว่า ช่องทางการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐระหว่างผู้ให้บริการข้อมูลและผู้ใช้บริการข้อมูล

2.6 Representational State Transfer (REST API หรือ RESTful API) หมายความว่า ช่องทางการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐระหว่างระบบผู้ให้บริการข้อมูลและระบบผู้ใช้บริการข้อมูลตามมาตรฐาน TGIX

2.7 JavaScript Object Notation (JSON) หมายความว่า รูปแบบของโครงสร้างข้อมูลที่ใช้แลกเปลี่ยนผ่าน REST API

2.8 TGIX Data Format หมายความว่า รูปแบบของมาตรฐานโครงสร้างข้อมูลที่ใช้แลกเปลี่ยนผ่าน REST API ตามมาตรฐาน TGIX

2.9 ระบบผู้ให้บริการ (Provider System) หมายความว่า ระบบสารสนเทศของหน่วยงานมีการใช้บริการ API สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในแพลตฟอร์มที่ใช้มาตรฐาน TGIX

2.10 ระบบผู้ใช้บริการ (Consumer System) หมายความว่า ระบบสารสนเทศของหน่วยงานที่ใช้บริการ API สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในแพลตฟอร์มที่ใช้มาตรฐาน TGIX

2.11 ผู้ให้บริการ TGIX Platform (TGIX Platform Provider) หมายความว่า ระบบสารสนเทศของหน่วยงานผู้ให้บริการ TGIX Platform เพื่อสนับสนุนการเชื่อมโยงและแลกเปลี่ยนข้อมูลให้เป็นไปตามมาตรฐาน TGIX

2.12 การบริการออกใบรับรอง (Certification Authority) หมายความว่า ผู้ให้บริการที่ทำหน้าที่ออกใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) เพื่อสนับสนุนการเชื่อมโยงและแลกเปลี่ยนข้อมูลให้เป็นไปตามมาตรฐาน TGIX

2.13 ลายมือชื่อดิจิทัล (Digital Signature) หมายความว่า สิ่งที่ได้จากกระบวนการเข้ารหัสลับ (Encrypt) ของข้อความหรือข้อมูล เพื่อใช้ยืนยันความถูกต้องได้ว่า ข้อความหรือข้อมูล ที่รับ-ส่งระหว่างผู้ขอใช้บริการและผู้ให้บริการ ไม่ถูกเปลี่ยนแปลงระหว่างเกิดการเชื่อมโยงและแลกเปลี่ยนข้อมูล

2.14 โทเคน (Token) หมายความว่า ชุดตัวอักษรชุดหนึ่งที่เอามาแทน Session Id สำหรับระบุตัวตนของ client ว่าคือใคร โดยวิธีการสร้างโทเคนสามารถทำได้หลายวิธี แต่มาตรฐานที่นิยมสำหรับสร้างโทเคนนั้นจะใช้มาตรฐาน JSON Web Token

2.15 JSON Web Token (JWT) หมายความว่า มาตรฐานเปิด (RFC 7519) สำหรับการสร้างโทเคน ซึ่งเป็นชุดตัวอักษรชุดหนึ่งที่นำมาใช้ สำหรับเพิ่มความปลอดภัยในการรับส่งข้อมูลระหว่างเครื่องลูกข่าย/เครื่องแม่ข่าย (Client/Server) โดยจะต้องมีขนาดที่เหมาะสม (Compact) และเก็บข้อมูลภายในตัว (Self-contained) โดยโครงสร้างจะแบ่งออกเป็น 3 ส่วน Header เก็บอัลกอริทึมในการเข้ารหัส, Payload เก็บข้อมูลของผู้ใช้งาน Signature เป็นลายมือชื่อดิจิทัลสำหรับการตรวจสอบการแก้ไขข้อมูลในโทเคน

2.16 The open systems interconnection (OSI) หมายความว่า โมเดลที่เป็นรูปแบบแนวคิดที่สร้างขึ้นโดยองค์การระหว่างประเทศว่าด้วยมาตรฐาน เป็นองค์กรที่ออกมาตรฐานต่างๆ (International Organization for Standardization: ISO) ซึ่งช่วยให้ระบบการสื่อสารที่มีความหลากหลายสามารถสื่อสารโดยใช้โปรโตคอลมาตรฐานที่ได้จัดเตรียมสำหรับระบบคอมพิวเตอร์ต่างๆ เพื่อให้สามารถสื่อสารกันได้

2.17 Endpoint URL หมายความว่า Term ของ URL Path เป็นเหมือนภาษาพูดที่ใช้เรียก Path ของ API โดยจะเรียก URLs ทั้งหมดว่า API แต่ละ URL จะเรียกว่า Endpoint

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

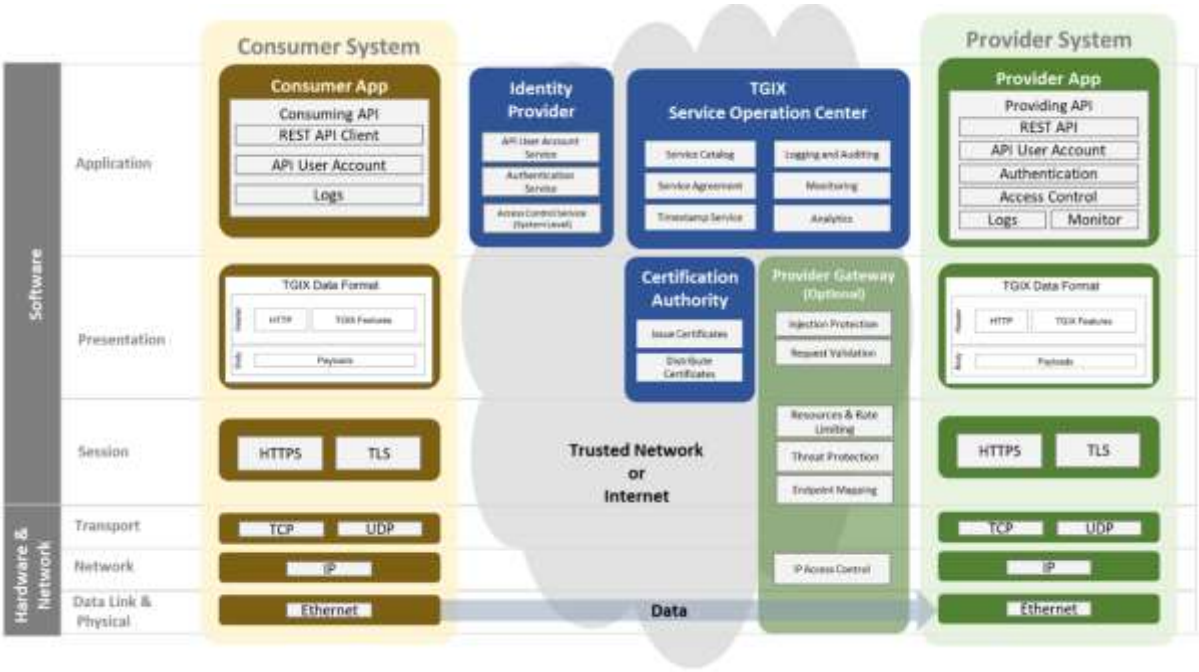
มาตรา 19 ระบุว่า ในวาระเริ่มแรก ให้สำนักงานดำเนินการให้มีศูนย์แลกเปลี่ยนข้อมูลกลางตามมาตรา 15 เป็นการชั่วคราวแต่ไม่เกินสองปี เมื่อครบกำหนดระยะเวลาดังกล่าว ให้คณะกรรมการพัฒนารัฐบาลดิจิทัลพิจารณาความจำเป็นและเหมาะสมเกี่ยวกับหน่วยงานของรัฐที่จะมาดำเนินการเกี่ยวกับศูนย์แลกเปลี่ยนข้อมูลกลาง ทั้งนี้ ในกรณีที่คณะกรรมการพัฒนารัฐบาลดิจิทัลเห็นควรให้หน่วยงานของรัฐแห่งอื่นใดทำหน้าที่แทนสำนักงาน ให้เสนอแนวทางการดำเนินการ การโอนภารกิจ งบประมาณทรัพย์สินและหนี้สินภาระผูกพัน และบุคลากรไปยังหน่วยงานของรัฐแห่งอื่นนั้นต่อคณะรัฐมนตรีเพื่อพิจารณา

4. ข้อกำหนดด้านโปรโตคอลระดับแอปพลิเคชัน เอนพอยน์และการจัดการโทเคน และเซสชัน

4.1 การทำงานของโปรโตคอล

การเชื่อมโยงและการแลกเปลี่ยนข้อมูลตามมาตรฐาน TGIX มีองค์ประกอบของสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ดังรูปที่ 1 แสดงการเชื่อมโยงข้อมูลจาก 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) โดยขั้นตอนทั้งหมดที่กล่าวมาจะทำงานอยู่บน Transmission Control Protocol (TCP)

นอกจากนี้ข้อมูลที่ใช้ในการเชื่อมโยงและแลกเปลี่ยนทั้งหมดของ REST API จะอยู่ในรูปแบบ JSON Data Format ซึ่งประกอบด้วยข้อมูลเชิงธุรกรรม (Business Data) และข้อมูลที่เกี่ยวข้องกับความปลอดภัยเพิ่มเติม เช่น ลงลายมือชื่อดิจิทัล (Digital Signature) ซึ่งในมาตรฐาน TGIX Linkage นี้กำหนดให้อยู่ในส่วนที่เป็น Header



รูปที่ 1 ภาพรวมองค์ประกอบของการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ

4.2 ข้อกำหนดด้านโปรโตคอลที่เกี่ยวข้องกับเอนพอยน์

ข้อกำหนดด้านโปรโตคอลที่เกี่ยวข้องกับเอนพอยน์ (Endpoint URL) ในการเชื่อมโยงและแลกเปลี่ยนข้อมูลตามมาตรฐาน TGIX มีดังต่อไปนี้

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

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

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

4.3 ข้อกำหนดด้านโครงสร้าง TGIX Data Format ตามมาตรฐาน TGIX

การกำหนดโครงสร้าง TGIX Data Format ตามมาตรฐาน TGIX เป็นการกำหนดรูปแบบโครงสร้างการรับส่งข้อมูลผ่าน REST API ระหว่างผู้ใช้บริการ API (Consumer System) และ ผู้ให้บริการ API (Provider System) ซึ่งมีโครงสร้างดังรูปที่ 1 โดยโครงสร้างของ TGIX Data Format สามารถแบ่งตามประเภทการแลกเปลี่ยนข้อมูลดังตารางที่ 1

ตารางที่ 1 ประเภทการแลกเปลี่ยนข้อมูล

ประเภทการแลกเปลี่ยน		**Content Type**	**รายละเอียด**
การแลกเปลี่ยนข้อมูลเชิงธุรกรรม	ข้อมูลเชิงธุรกรรมที่กำหนดลักษณะ Payload เป็นรูปแบบ JSON	กำหนด Content Type ประเภท JSON	กำหนดข้อความมีลักษณะเป็น JSON ทั้งหมด
	ข้อมูลเชิงธุรกรรมที่กำหนดลักษณะ Payload ไม่ได้เป็นรูปแบบ JSON	กำหนด Content Type ประเภท Multipart	เพื่อรองรับการการแลกเปลี่ยนข้อมูล Format อื่นๆ เช่น XML, ebXML เป็นต้น ทำให้มาตรฐาน TGIX สามารถทำงานร่วมกับ Data Format อื่นๆ ได้

ตารางที่ 2 ประเภทการแลกเปลี่ยนข้อมูล (ต่อ)

ประเภทการแลกเปลี่ยน		Content Type	รายละเอียด
การแลกเปลี่ยนข้อมูลที่เป็น File	ขนาดของ File ไม่เกิน 5 MB	กำหนด Content Type ประเภท Multipart	เพื่อรองรับการแลกเปลี่ยนข้อมูลแบบ File ที่มีขนาดไม่เกิน 5MB
	ขนาดของ File ที่มากกว่า 5 MB	กำหนด Content Type ประเภท Multipart โดยอาจมีคุณสมบัติ resumabled (เป็นตัวเลือก) เพื่อให้ไฟล์ต่อเนื่องกันได้กรณีเกิดการสื่อสารขัดข้อง	เพื่อรองรับการแลกเปลี่ยนข้อมูลแบบ File ที่มีขนาดเกิน 5MB และอาจมีคุณสมบัติการอัปโหลดหรือดาวน์โหลดไฟล์ต่อเนื่องได้ (ตัวเลือก) ตามมาตรฐาน Form-based File Upload in HTML: RFC-1867 [1] และ Hypertext Transfer Protocol (HTTP/1.1): Range Requests: RFC-7233 [2]

4.3.1 ส่วน TGIX Message Header

ในส่วนของ TGIX Message Header จะกำหนดไว้ในส่วนของ HTTP Header รวมถึงส่วนที่เป็น TGIX Message Signature โดยมีรายละเอียดดังตารางที่ 3

ตารางที่ 3 รายละเอียดโครงสร้างของ TGIX Message Header ส่วน HTTP Header

พารามิเตอร์	ความจำเป็น	รายละเอียด
HTTP Method	(จำเป็นต้องมี)	กำหนด HTTP Method โดยรองรับ HTTP/1.1 [3]และโดยรองรับกำหนดค่าเป็น POST, GET, DELETE, PUT, OPTIONS และ PATCH
Authorization	(จำเป็นต้องมี)	กำหนดรหัสการยืนยันตนของผู้ใช้งาน โดยกำหนดค่าเป็น Bearer เสมอ
Accept-Encoding	(จำเป็นต้องมี)	กำหนดการเข้ารหัสข้อมูล
Accept-Language	(จำเป็นต้องมี)	กำหนดภาษาในการตอบรับ
Accept	(จำเป็นต้องมี)	กำหนดประเภทของเนื้อหา
Host	(จำเป็นต้องมี)	กำหนด URL ปลายทาง
Cache-Control	(จำเป็นต้องมี)	กำหนดคำสั่งชี้แนะว่าจะต้องทำตามกลไกการเก็บแคชทั้งหมดโดยตลอดทั้งการร้องขอและการตอบรับ
Connection	(จำเป็นต้องมี)	กำหนดวิธีการเชื่อมต่อ
Content-Type	(จำเป็นต้องมี)	กำหนดชนิดของเนื้อหาที่ร้องขอ
Content-Length	(จำเป็นต้องมี)	กำหนดความยาวของข้อมูลเนื้อหา
Origin	(จำเป็นต้องมี)	กำหนด URL ต้นทาง
Tgix-Client-Id	(จำเป็นต้องมี)	กำหนดเลข unique client
Tgix-Message-Id	(จำเป็นต้องมี)	กำหนดรหัสของข้อความ
Tgix-Timestamp	(จำเป็นต้องมี)	กำหนดเวลาสร้าง message เพื่อส่งออก
Tgix-Alg	(จำเป็นต้องมี)	กำหนดอัลกอริทึมของกุญแจ เช่น RS256, RFC-7518

ตารางที่ 3 รายละเอียดโครงสร้างของ TGIX Message Header ส่วน HTTP Header

พารามิเตอร์	ความจำเป็น	รายละเอียด
Tgix- Certificate	(จำเป็นต้องมี)	กำหนด Public Key ของลายมือชื่อดิจิทัล
Tgix-Signature-Value	(จำเป็นต้องมี)	กำหนดกุญแจที่ใช้ในการลงลายมือชื่อดิจิทัล
Tgix-Request-Id	(จำเป็นต้องมี)	กำหนดรหัสของการร้องขอสำหรับตอบกลับ
X-API-KEY	(ตัวเลือก)	กำหนดรหัสของ API
Tgix-Event	(ตัวเลือก)	กำหนดรายละเอียดการที่จะดำเนินการ (Action)
Tgix-Expiration-Timestamp	(ตัวเลือก)	กำหนดเวลาที่หมดอายุของข้อความ
Tgix-Message-Version	(ตัวเลือก)	กำหนดวิธีการจัดการข้อความคนละแบบ

4.3.2 ส่วน TGIX Message Payloads

ในส่วนของ Message จะระบุให้ส่วนของ HTTP Body ซึ่งเป็น Message ที่ใช้รับส่งกันระหว่างผู้ให้บริการและผู้ใช้บริการกรณีที่เป็นรูปแบบ JSON เท่านั้น ส่วนการรับส่งข้อความที่เป็นรูปแบบอื่น ๆ จะใช้เทคนิคการกำหนดรูปแบบการรับส่งข้อมูลแบบ Multipart Content-Type เพื่อรองรับการรับส่งข้อมูลจากผู้ขอใช้บริการได้หลายรูปแบบ สามารถทำได้โดยระบุ HTTP Header Content-Type เป็นแบบ Multipart ที่ TGIX Message Headers โดยมีรายละเอียดดัง ตารางที่ 4 และอยู่ภายใต้ Header ที่เป็นรูปแบบ JSON มีรายละเอียดดัง ตารางที่ **5**

ตารางที่ 4 รายละเอียดโครงสร้างของ TGIX Message Payloads ส่วน HTTP Body

พารามิเตอร์	ความจำเป็น	รายละเอียด
messageStatus	(จำเป็นต้องมี)	กำหนดสถานะของข้อความ
messageStatus: status	(จำเป็นต้องมี)	กำหนดสถานะตามมาตรฐาน HTTP Status
messageStatus: description	(จำเป็นต้องมี)	กำหนดรายละเอียดสถานะ
messageStatus: error	(จำเป็นต้องมี)	กำหนดรายละเอียดกรณีร้องขอไม่สำเร็จ โดยผู้ให้บริการเป็นผู้กำหนดเอง
error: code	(จำเป็นต้องมี)	กำหนดรหัสของ Error
error: message	(จำเป็นต้องมี)	กำหนดข้อความที่ต้องการแสดง Error

ตารางที่ 5 รายละเอียดโครงสร้างของ TGIX Message Payloads ส่วน HTTP Header

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

4.3.3 ตัวอย่างโครงสร้าง TGIX Data Format

4.3.3.1 โครงสร้าง TGIX Data Format กรณีการแลกเปลี่ยนข้อมูลเชิงธุรกรรม

(1) การแลกเปลี่ยนข้อมูลเชิงธุรกรรม โดยกำหนดลักษณะ Payload เป็น JSON ทั้งข้อความ โดยกำหนด Content Type เป็นประเภท JSON ดังตัวอย่างรูปที่ 2

```
// ========================================================
// TGIX Message Header: HTTP Header
// ========================================================
   POST https://oneweb.tgix.com/api/v1/sendmessage HTTP/1.1
   Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxM
jM0NTY3ODkwIiwibmFtZSI6IlRHSVggREdBIiwiaWF0IjoxNTE2MjM5MDIyfQ.gs6d4E
8CIkIs8FC-IysF8p7aBbE2gapTBT0e5xwUHug
   Accept: application/json, text/plain, */*
   Accept-Encoding: gzip, deflate
   Accept-Language: en-US,en;q=0.5
   Host: localhost:8000
   Cache-Control: no-cache
   Connection: keep-alive
   Content-Type: application/json;charset=UTF-8
   Content-Length: 4515
   Origin: localhost.com
   Referer: localhost.com
   TGIX-Alg: RSA-SHA256
   TGIX-Certificate: <<public key of signer or issuer>>
   TGIX-Client-Id: 12345
   TGIX-Message-Id: 3183c52c-60a5-11ed-9b6a-0242ac120002
   TGIX-Request-Id: c350da99-7aeb-4577-a09f-5e7cc10d510c
   TGIX-Signature-Value: <<signature>>
   TGIX-Timestamp: 2023-03-14T02:08:10.239Z
// ========================================================
// TGIX Message Header: HTTP Body
// ========================================================
```

```
// ============================================================
// TGIX Message Payload
// ============================================================
{
      "PersonID": "1767400297581"
}
```

รูปที่ 2 ตัวอย่างการแลกเปลี่ยนข้อมูลเชิงธุรกรรม โดยกำหนดลักษณะ Payload เป็น JSON

(2) การแลกเปลี่ยนข้อมูลเชิงธุรกรรม โดยกำหนดลักษณะ Payload ไม่ได้เป็น JSON โดยกำหนด Content Type เป็นประเภท Multipart เพื่อรองรับ XML Message หรือการแนบ File ขนาดไม่เกิน 5 MB ดังตัวอย่างรูปที่ 3

```
// ============================================================
// TGIX Message Header: HTTP Header
// ============================================================
POST /api/v4/person/person-upload HTTP/1.1
Request Method: POST
Accept: application/json, text/plain, */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,th;q=0.8
Authorization: Bearer xxxxxxxx xxxxxx xx xxxc xxcxcxcxxc
Connection: keep-alive
Content-Length: 460
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundary7MA4YWxkTrZu0gW
Host: localhost:8000
Origin: localhost.com
Referer: localhost.com
TGIX-Alg: RSA-SHA256
TGIX-Certificate: <<public key of signer or issuer>>
TGIX-Client-Id: 12345
TGIX-Message-Id: 3183c52c-60a5-11ed-9b6a-0242ac120002
TGIX-Request-Id: c350da99-7aeb-4577-a09f-5e7cc10d510c
TGIX-Signature-Value: <<signature>>
TGIX-Timestamp: 2023-03-14T02:08:10.239Z

// ============================================================
// TGIX Message Header: HTTP Body
// ============================================================
boundary=----WebKitFormBoundary7MA4YWxkTrZu0gW
```

```
----WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name=""
Content-Type: application/json

{"cd:PersonID": "1767400297581"}

----WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name=""; filename="person-295.png"
Content-Type: image/png

(data)
----WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name=""; filename="cr_Nationality.xml"
Content-Type: text/xml

(data)
----WebKitFormBoundary7MA4YWxkTrZu0gW
```

รูปที่ 3 ตัวอย่างการแลกเปลี่ยนข้อมูลเชิงธุรกรรม โดยกำหนดลักษณะ Payload ไม่ได้เป็น JSON

4.3.3.2 โครงสร้าง TGIX Data Format กรณีการ File ขนาดเกิน 5 MB

การแลกเปลี่ยนข้อมูล File ขนาดเกิน 5 MB มีตัวอย่างดังรูปที่ 4

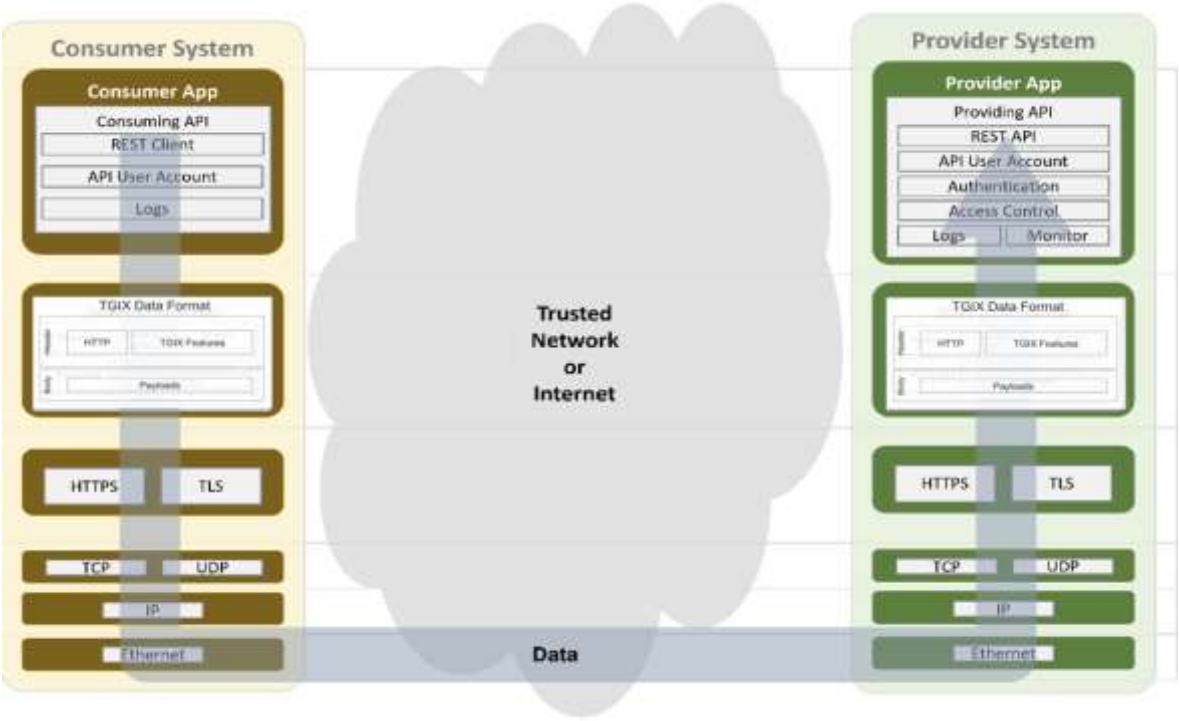
```
//Consumer System ส่ง Request ไปแจ้งว่าจะมีการ Upload File พร้อมแจ้งขนาดและจำนวน Chunk ที่จะส่ง
PATCH /document HTTP/1.1
Content-Type: multipart/byteranges; boundary=THIS_STRING_SEPARATES

//Consumer System แตก File ออกเป็น Chunk ย่อยๆ แล้วทยอย Upload ทีละ File จนสำเร็จ
--THIS STRING SEPARATES
Content-Type: text/plain
Content-Range: bytes 10-21/22

1234567890
--THIS_STRING_SEPARATES--
```

รูปที่ 4 ตัวอย่างการแลกเปลี่ยนข้อมูลเชิงธุรกรรม โดยกำหนดลักษณะ File

4.4 การบริหารจัดการ Session

4.4.1 การใช้งานเซสชัน (Session)

เซสชันตามมาตรฐาน TGIX คือกลุ่มของข้อมูลใช้สำหรับการโต้ตอบระหว่างผู้ใช้บริการ (Consumer System) และผู้ให้บริการ (Provider System) ที่เกิดขึ้นภายในช่วงเวลาที่กำหนด ดังรูปที่ 5 แสดงส่งข้อมูลระหว่างผู้ใช้บริการ (Consumer System) โดยเริ่มจากระบบของผู้ใช้บริการ สร้างชุดข้อมูลเพื่อขอใช้บริการในรูปแบบ TGIX Data Format จากนั้นส่งข้อมูลผ่าน HTTPS บน TLS โดยระบบจะทำการสร้างเซสชันการเชื่อมต่อไปยังระบบผู้ให้บริการ (Provider System) ซึ่งข้อมูลจะถูกส่งไปยังระบบผู้ให้บริการในรูปแบบ TGIX Data Format เมื่อผู้ให้ข้อมูลได้รับข้อมูลจะทำการประมวลผลและตอบกลับไปยังผู้ใช้บริการ



รูปที่ 5 การส่งข้อมูลระหว่างผู้ใช้บริการ (Consumer System) และผู้ให้บริการ (Provider System)

เซสชัน (Session) เดียวสามารถมีได้หลายกิจกรรม ซึ่งเซสชันทั้งหมดเก็บไว้ชั่วคราวในขณะที่ผู้ใช้เชื่อมต่ออยู่ ตามมาตรฐาน TGIX เมื่อผู้ใช้เข้าสู่ระบบจะมีการสร้างเซสชันสำหรับผู้ใช้ และเมื่อต้องการตรวจสอบสิทธิ์ หรือข้อมูลอื่นๆ ของผู้ใช้บริการก็สามารถใช้ข้อมูลเซสชันในการตรวจสอบ โดยผู้ให้บริการจะตรวจสอบทุกครั้งที่มีการขอใช้บริการ ซึ่งอาจมีการใช้งานร่วมกับโทเคน (Token) ส่วนรายละเอียดโทเคน จะกล่าวถึงในส่วนการบริหารจัดการโทเคนต่อไป เซสชันสามารถแบ่งออกได้เป็น 3 ส่วน คือ

(1) แอปพลิเคชันเซสชัน (Application Session)

ส่วนนี้เป็นเซสชันภายในแอปพลิเคชัน ใช้สำหรับติดตามผู้ใช้งานว่ามีการลงชื่อเข้าใช้งานหรือไม่ รวมถึงข้อมูลกิจกรรมที่เกิดขึ้นในแอปพลิเคชันว่ามีการเข้าใช้งานระบบส่วนไหนบ้าง โดยจัดเก็บข้อมูลนี้ไว้ในคุกกี้ (Cookie) หรือเก็บไว้ด้วยวิธีการอื่นๆ ที่เป็นไปตามมาตรฐานสากล

(2) เซสชันการอนุญาต (Authorization Session)

เซสชันการอนุญาต ใช้สำหรับเปลี่ยนเส้นทาง (Redirect) ไปยังบริการ (Services) ที่ผู้ใช้ขอมา โดยข้อมูลเซสชันนี้จะถูกเก็บไว้บนเซิร์ฟเวอร์ที่ทำหน้าที่กำหนดและตรวจสอบสิทธิ์ผู้ใช้

(3) เซสชันผู้ให้บริการข้อมูลประจำตัว (Identity Provider Session)

เซสชันนี้เกิดขึ้นเมื่อผู้ใช้ลงชื่อเข้าใช้งานระบบ โดยเรียกใช้บริการข้อมูลประจำตัว เช่น Identity Provider Server เมื่อมีการลงชื่อเข้าใช้ถูกต้องอยู่แล้ว ผู้ให้บริการข้อมูลประจำตัวจะสร้างเซสชันเพื่อเก็บข้อมูลประจำตัว เมื่อผู้ใช้มีการใช้งานข้อมูลประจำตัวอีกครั้งจึงไม่จำเป็นต้องลงชื่อเข้าใช้อีก

4.4.2 การกำหนดอายุของเซสชัน (Session Lifetime Limits)

มาตรฐาน TGIX แนะนำให้มีการกำหนดค่าในส่วนนี้ เพื่อเป็นการกำหนดว่าผู้ให้บริการควรจะเก็บเซสชันไว้นานเท่าไหร่ก่อนจะทำการออกจากระบบโดยอัตโนมัติ โดยผู้ให้บริการที่พัฒนาระบบตามมาตรฐาน OAuth 2.0 นั้นจะต้องมีการกำหนดค่าหมดเวลาไม่ใช้งาน (Inactivity timeout) คือกรอบเวลาหลังจากที่เซสชันของผู้ใช้จะหมดอายุหากไม่ได้โต้ตอบกับเซิร์ฟเวอร์การให้สิทธิ์ จะถูกทำให้ออกจากระบบหากเกินเวลาที่กำหนด และกรอบเวลาที่กำหนดให้ผู้ใช้งานจะต้องเข้าสู่ระบบอีกครั้ง (Require log in after)

4.4.3 การล้างเซสชัน

มาตรฐาน TGIX แนะนำให้ทำการล้างเซสชันเมื่อผู้ใช้งานออกจากระบบหรือแอปพลิเคชันนั้นๆ

4.4.3.1 การล้างเซสชันระดับแอปพลิเคชัน

เซสชันในส่วนปกติแล้วจะเกิดขึ้นเมื่อมีผู้ใช้งานเข้ามาใช้งานแอปพลิเคชันของผู้ขอใช้บริการ (Consumer) จะมีการสร้างเซสชันขึ้นมาเพื่อใช้งาน เมื่อผู้ใช้งานออกจากระบบ การล้างเซสชันในส่วนนี้จะต้องเป็นหน้าที่ของแอปพลิเคชันที่ต้องทำการล้างเซสชันทั้งหมดที่เกิดขึ้น โดยการบริหารจัดการในส่วนนี้สามารถทำได้ดังนี้

(1) การกำหนดอายุของเซสชัน (Session Expiration)

เพื่อลดระยะเวลาที่ผู้โจมตีสามารถเริ่มการโจมตีในเซสชันที่ใช้งานอยู่ และขโมยเซสชันเหล่านั้น จำเป็นต้องกำหนดอายุสำหรับทุกเซสชัน โดยกำหนดระยะเวลาที่เซสชันจะยังคงทำงานอยู่ การกำหนดอายุของเซสชันที่นานเกินความจำเป็นสำหรับเว็บแอปพลิเคชัน จะเพิ่มช่องโหว่ของการโจมตีจากเซสชันได้ โดยผู้โจมตีสามารถใช้ไอดีเซสชันที่ถูกต้องโจมตีซ้ำๆ ยิ่งการกำหนดช่วงเซสชันสั้นลงเท่าใด ผู้โจมตีก็จะมีโอกาสใช้รหัสเซสชันที่ถูกต้องน้อยลงเท่านั้น ดังนั้นการกำหนดเวลาหมดอายุของเซสชันตามมาตรฐาน TGIX แนะนำมีการกำหนดค่าให้สอดคล้องกับวัตถุประสงค์ และลักษณะการใช้งานหรือให้บริการของเว็บแอปพลิเคชัน โดย

คำนึงถึงความปลอดภัยและการใช้งาน เพื่อให้ผู้ใช้สามารถดำเนินการภายในเว็บแอปพลิเคชันให้เสร็จสิ้นได้อย่างสะดวกสบาย โดยที่เซสชันหมดอายุบ่อยครั้งจนเกินไป

เมื่อเซสชันหมดอายุ เว็บแอปพลิเคชันต้องดำเนินการเพื่อทำให้เซสชันเป็นโมฆะทั้งสองฝั่ง ทั้งฝั่งผู้ใช้งานและฝั่งผู้ให้บริการ

สำหรับกลไกการแลกเปลี่ยนเซสชันส่วนใหญ่เป็นการดำเนินการฝั่งผู้ใช้งาน เพื่อให้มั่นใจได้ว่าไอดีเซสชันใช้งานไม่ได้ ตัวอย่างเช่น หากต้องการทำให้คุกกี้ใช้งานไม่ได้ ข้อแนะนำคือ ให้ระบุค่าว่างสำหรับรหัสเซสชันและตั้งค่าแอตทริบิวต์ Expires (หรือ Max-Age) เป็นวันที่ในอดีต

(2) การทำให้เซสชันหมดอายุอัตโนมัติ (Automatic Session Expiration)

เซสชันทั้งหมดควรมีการกำหนดค่าหมดเวลาเมื่อไม่มีการใช้งาน ค่าหมดเวลานี้เป็นการกำหนดระยะเวลาที่เซสชันจะยังคงอยู่และสามารถใช้งานได้ ในกรณีที่ไม่มีกิจกรรมในเซสชัน จะถูกทำให้เซสชันเป็นโมฆะเมื่อเลยช่วงเวลาที่กำหนดไว้ โดยนับตั้งแต่คำร้องขอใช้บริการครั้งล่าสุดที่ได้รับ นอกจากนี้การกำหนดค่าหมดเวลาเมื่อไม่มีการใช้งาน จะเป็นการจำกัดโอกาสที่ผู้โจมตีใช้ไอดีเซสชันในการโจมตีโดยการขโมยเซสชันได้ มาตรฐาน TGIX แนะนำให้มีการกำหนดค่าหมดเวลาของเซสชันและการหมดอายุในฝั่งผู้ให้บริการ

(3) การทำให้หมดอายุของเซสชันด้วยตนเอง (Manual Session Expiration)

เว็บแอปพลิเคชันจะต้องมีกลไกที่อนุญาตให้ผู้ใช้สามารถปิดเซสชันของตนได้ เมื่อใช้งานเว็บแอปพลิเคชันเสร็จแล้ว โดยเว็บแอปพลิเคชันต้องมีปุ่มล็อกเอาต์ ออกจากระบบที่มองเห็นและเข้าถึงได้ง่าย และสามารถเข้าถึงได้จากทุกหน้า เพื่อให้ผู้ใช้สามารถปิดเซสชันด้วยตนเอง เวลาใดก็ได้

4.4.3.2 การล้างเซสชันการอนุญาต

โดยปกติแอปพลิเคชันผู้ให้บริการกำหนดและตรวจสอบสิทธิ์ จะมีฟังก์ชันให้เรียกใช้งานอยู่แล้วเพื่อล้างเซสชัน ขึ้นอยู่กับเครื่องมือที่นำมาใช้ในการพัฒนาแอปพลิเคชัน การล้างเซสชันในส่วนนี้สามารถทำได้โดยจะต้องเรียกฟังก์ชันล้างเซสชันของแอปพลิเคชันผู้ให้บริการให้สิทธิ์

4.4.3.3 การล้างเซสชันผู้ให้บริการข้อมูลประจำตัว

ตามมาตรฐาน TGIX แนะนำให้ปฏิตามขั้นตอนการล้างเซสชันในส่วนของผู้ให้บริการ (Provider) ในการล้างเซสชันการพิสูจน์ตัวตน ก็เพียงพอสำหรับการทำงาน ประกอบกับการกำหนดอายุของเซสชัน (Session Lifetime Limits) ผู้ให้บริการพิสูจน์และยืนยันตัวตน ในกรณีที่ผู้ใช้งานไม่ได้ทำการออกจากระบบ จะถูกทำให้ออกจากระบบโดยอัตโนมัติ เมื่อถึงเวลาที่กำหนด สำหรับแอปพลิเคชันของผู้ขอใช้บริการ (Consumer) การล้างเซสชันในส่วนนี้ไม่มีความจำเป็นต้องดำเนินการใด

4.4.4 การตรวจจับการโจมตีเซสชัน (Session Attacks Detection)

โดยปกติแอปพลิเคชันจะต้องมีการออกแบบ และพัฒนาโดยคำนึงถึงความปลอดภัยของแอปพลิเคชัน ดังนั้นฟังก์ชันการทำงานด้านความปลอดภัยพื้นฐานตามมาตรฐาน TGIX แนะนำควรจะมีดังต่อไปนี้

- การเดาและการตรวจจับแบบสุ่ม ID เซสชันที่ถูกต้อง (Session ID Guessing and Brute Force Detection)

การเดาและการตรวจจับแบบสุ่ม ID เซสชันที่ถูกต้อง (Session ID Guessing and Brute Force Detection) เป็นกระบวนการตรวจจับและป้องกันการโจมตีที่พยายามเดาหรือทำการทดลองแบบสุ่มเพื่อหา I ไอดีเซสชันที่ถูกต้อง ซึ่งสามารถนำไปใช้เข้าถึงระบบของผู้ใช้งานผู้อื่นได้ วิธีการป้องกันคือ การใช้ไอดีเซสชันที่มีความยาวเพียงพอ และสุ่มออกมาจากตัวเลขที่มีความปลอดภัยสูง (Secure Random Number Generator) เพื่อลดความเป็นไปได้ในการเดาหรือทำการทดลองแบบสุ่มให้น้อยที่สุด

นอกจากนี้ควรใช้ Rate Limiting เพื่อจำกัดจำนวนครั้งในการส่งคำขอที่ผิดพลาดภายในระยะเวลาที่กำหนด ทำให้ผู้โจมตีไม่สามารถทำการทดลองเดา หรือทดลองแบบสุ่มอย่างต่อเนื่องได้

- การตรวจจับความผิดปกติของรหัสเซสชัน (Detecting Session ID Anomalies)

เป็นกระบวนการตรวจสอบความผิดปกติของรหัสเซสชันในการขอใช้บริการไปยังผู้ให้บริการ ซึ่งอาจเป็นสัญญาณของการโจมตีหรือการละเมิดความปลอดภัย การตรวจจับความผิดปกติของรหัสเซสชันอาจครอบคลุมการตรวจสอบความยาว ความสัมพันธ์ของตัวอักษร และความสุ่มของรหัสเซสชัน

การตรวจจับความผิดปกติสามารถทำได้โดยใช้วิธีการต่าง ๆ เช่น Machine การวิเคราะห์ข้อมูลทางสถิติจากไฟล์บันทึกเหตุการณ์ (logs) เพื่อตรวจสอบรูปแบบที่ผิดปกติของรหัสเซสชัน หากพบความผิดปกติระบบควรดำเนินการตามมาตรการป้องกันที่กำหนด เช่น ระงับเซสชัน แจ้งเตือนผู้ดูแลระบบ หรือขอยืนยันตัวตนของผู้ใช้งานอีกครั้ง

การตรวจจับความผิดปกติของรหัสเซสชันจะช่วยป้องกันการโจมตีที่พยายามเข้าถึงข้อมูลของผู้ใช้งานโดยไม่ได้รับอนุญาต และเสริมสร้างความปลอดภัยของในการใช้งาน

- การผูก ID เซสชันกับคุณสมบัติผู้ใช้อื่น (Binding the Session ID to Other User Properties)

เป็นวิธีการเพิ่มความปลอดภัยในการจัดการเซสชันของแอปพลิเคชันของผู้ใช้บริการ ที่เรียกไปยังผู้ให้บริการ โดยใช้คุณสมบัติเฉพาะของผู้ใช้งานเช่น IP address, User-Agent, และอื่น ๆ เพื่อให้แน่ใจว่าไอดีเซสชันที่ใช้ในแต่ละคำขอเป็นของผู้ใช้ที่ถูกต้อง

การผูกคุณสมบัติของผู้ใช้กับไอดีเซสชันทำให้ความเสี่ยงต่อการโจมตีของผู้ไม่หวังดีลดลง หากมีการพยายามนำไอดีเซสชันของผู้ใช้คนหนึ่งไปใช้กับผู้ใช้ที่ใช้มาจากคอมพิวเตอร์เครื่องอื่น คุณสมบัติที่ผูกกับไอดีเซสชันจะไม่ตรงกัน ทำให้ระบบสามารถตรวจสอบและปฏิเสธคำขอที่ไม่สอดคล้องกันได้

ทั้งนี้การผูกไอดีเซสชันกับคุณสมบัติผู้ใช้ ต้องพิจารณาระดับความเคร่งครัดในการตรวจสอบความถูกต้องเพื่อป้องกันการปฏิเสธบริการที่ไม่จำเป็น (false positives) เช่น การเปลี่ยน IP address ของผู้ใช้เนื่องจากเครือข่ายมือถือ หรือการเปลี่ยน User-Agent ในกรณีของการอัปเดตเวอร์ชันของเบราว์เซอร์

4.4.5 การป้องกันและจัดการเซสชันโดยใช้ Web Application Firewalls

การป้องกันและจัดการเซสชันโดยใช้ Web Application Firewalls (WAF) คือ การใช้เครื่องมือควบคุมการเข้าถึงและป้องกันภัยคุกคามต่อเว็บแอปพลิเคชัน WAF จะทำหน้าที่ตรวจสอบข้อมูลที่ส่งเข้า-ออกระหว่างผู้ใช้และเว็บแอปพลิเคชัน ตรวจจับและป้องกันการโจมตีเชิงเทคนิค รวมถึงการโจมตีเซสชัน เช่น Session Hijacking หรือ Brute Force Attacks นอกจากนี้ WAF ยังสามารถกำหนดกฎการทำงานเพื่อป้องกันการโจมตีที่เฉพาะเจาะจงตามความต้องการ การใช้ WAF จึงเป็นวิธีหนึ่งในการป้องกันและจัดการเซสชันอย่างมีประสิทธิภาพ ช่วยเสริมความปลอดภัยให้กับเว็บแอปพลิเคชัน

WAF สามารถใช้แอตทริบิวต์ความปลอดภัยบนคุกกี้เพื่อเพิ่มความปลอดภัยในการจัดการเซสชัน และป้องกันการโจมตีที่เกี่ยวข้องกับคุกกี้ เช่น การขโมยคุกกี้ หรือการปลอมแปลงคุกกี้ แอตทริบิวต์ที่เกี่ยวข้องประกอบด้วย "Secure", "HttpOnly" และ "SameSite"

- แอตทริบิวต์ "Secure" บังคับให้คุกกี้ส่งผ่าน HTTPS เท่านั้น ทำให้คุกกี้ไม่สามารถถูกส่งผ่าน HTTP ซึ่งไม่ปลอดภัย
- แอตทริบิวต์ "HttpOnly" ป้องกันการเข้าถึงคุกกี้โดย JavaScript ทำให้ลดความเสี่ยงจากการโจมตีแบบ Cross-site Scripting (XSS)
- แอตทริบิวต์ "SameSite" ช่วยป้องกันการโจมตีแบบ Cross-Site Request Forgery (CSRF) โดยกำหนดว่าคุกกี้สามารถส่งในคอนเท็กซ์ของเว็บไซต์ที่คล้ายกันเท่านั้น

การใช้ WAF เพื่อบังคับใช้แอตทริบิวต์ความปลอดภัยเหล่านี้ จะช่วยให้ป้องกันการโจมตีที่เกี่ยวข้องกับคุกกี้ และเพิ่มความปลอดภัยในการจัดการเซสชันของผู้ใช้

4.4.6 การจัดการเซสชันในสถาปัตยกรรม Stateless

การจัดการเซสชันในสถาปัตยกรรม Stateless เป็นวิธีการที่ออกแบบเพื่อลดการใช้สถานะของเซสชัน ในกระบวนการนี้ ข้อมูลเซสชันจะถูกเข้ารหัสและจัดเก็บอยู่ภายในโทเคน (Token) ที่ส่งผ่าน HTTP headers หรือคุกกี้ โดยที่ไม่ต้องเก็บข้อมูลเซสชันบนเซิร์ฟเวอร์

ในสถาปัตยกรรม Stateless นิยมใช้ JSON Web Tokens (JWT) เป็นโทเคน เมื่อมีการยืนยันตัวตนสำเร็จ ข้อมูลผู้ใช้เฉพาะที่จำเป็นจะถูกเข้ารหัสลงในโทเคน และส่งกลับให้กับผู้ขอใช้บริการ ซึ่งจะนำโทเคนนี้ไปใช้ในการร้องขอข้อมูลต่อไป

เมื่อโทเคนถูกส่งกลับมายังเซิร์ฟเวอร์ ข้อมูลเซสชันสามารถถอดรหัสและตรวจสอบความถูกต้องของข้อมูล โดยไม่จำเป็นต้องเข้าถึงฐานข้อมูลหรือเก็บข้อมูลเซสชันในเซิร์ฟเวอร์ ทำให้สามารถประหยัดทรัพยากรของระบบ และทำให้ระบบสามารถขยายตัวได้ง่ายขึ้น

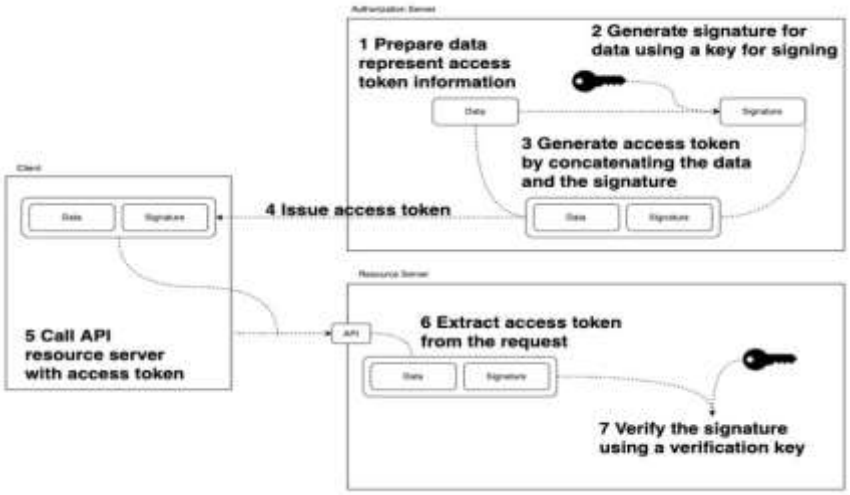
เนื่องจากสถาปัตยกรรม Stateless เป็นแนวคิดที่ระบบไม่เก็บสถานะของเซสชันระหว่างการสื่อสารของผู้ใช้บริการและผู้ให้บริการ โดยในแต่ละการขอใช้บริการจากผู้ขอใช้บริการ ถือเป็นอิสระและมีข้อมูลที่เพียงพอในการดำเนินการ ด้วยเหตุนี้เซิร์ฟเวอร์จึงไม่จำเป็นต้องเก็บข้อมูลเซสชันสำหรับผู้ใช้บริการ ทำให้ระบบมีประสิทธิภาพสูงขึ้น สถาปัตยกรรม Stateless มีข้อดีที่สำคัญดังนี้

- ความยืดหยุ่นในการขยายระบบ (Scalability) เนื่องจากไม่มีการเก็บสถานะเซสชัน จึงสามารถขยายระบบเช่น เพิ่มเซิร์ฟเวอร์ได้ง่ายขึ้น
- ลดความซับซ้อนของระบบและการจัดการทรัพยากร เนื่องจากไม่จำเป็นต้องเก็บข้อมูลเซสชันในเซิร์ฟเวอร์
- ความพร้อมในการใช้งาน (Availability) เพิ่มขึ้น เนื่องจากไม่ต้องย้ายข้อมูลเซสชันระหว่างเซิร์ฟเวอร์ในกรณีที่มีมีปัญหา

4.5 การบริหารจัดการ Token

ผู้ให้บริการจะต้องมีการกำหนดการรูปแบบการรักษาความปลอดภัยในการรับส่งข้อมูล ซึ่งมีมาตรฐานต่างๆ รองรับตัวอย่างเช่น การใช้การลงนามข้อความตาม OAuth 1.0 การตรวจสอบสิทธิ์และการอนุญาตที่ใช้ OAuth 2.0 ซึ่งตามมาตรฐาน TGIX กำหนดให้พิจารณาข้อกำหนดด้านความน่าเชื่อถือและความมั่นคงปลอดภัย โดยกำหนดให้มีการใช้การยืนยันตัวตน ด้วย Open ID Connect 1.0 (OIDC) เป็นอย่างน้อย รวมถึงโทเคน และไอดีโทเคน ซึ่งรายละเอียดของโทเคนและไอดีโทเคนได้อ้างถึงใน มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่อง ข้อกำหนดด้านการยืนยันตัวตน การกำหนดสิทธิ์ และบัญชีการใช้งาน โดยทั้งโทเคน และไอดีโทเคนได้มีการกำหนดรูปแบบการรักษาความปลอดภัยสำหรับโทเคนโดยอ้างอิงตามมาตรฐาน JSON Web Tokens (JWT): RFC-7519 [4]

การบริหารจัดการโทเคนตามรูปที่ 6 เป็นการนำเสนอรูปแบบของการสร้างและการนำไปใช้งานโทเคน โดยเริ่มจากการสร้างโทเคนซึ่งประกอบไปด้วยข้อมูล 3 ส่วนหลัก คือ ส่วนที่ระบุอัลกอริทึมของการเข้ารหัส ส่วนที่เป็นข้อมูล ส่วนที่เป็นลายเซ็นดิจิทัล จากนั้นโทเคนจะถูกส่งกลับไปยังผู้ขอใช้บริการ และผู้ขอใช้บริการจะต้องแนบโทเคนนี้ไปกับข้อมูลการร้องขอใช้งานเสมอ เมื่อระบบผู้ให้บริการได้รับการร้องขอใช้บริการจะทำการตรวจสอบความถูกต้องของผู้ร้องขอโดยดูจากโทเคน โดยการตรวจสอบก่อนว่าข้อมูลโทเคนนั้นไม่ได้ถูกเปลี่ยนแปลงแก้ไขจากนั้นจึงนำข้อมูลในโทเคนมาใช้งาน



รูปที่ 6 รูปแบบการสร้างและใช้งานโทเคนที่สร้างโดยมาตรฐาน JSON Web Token

4.5.1 มาตรฐานการสร้าง Token

สำหรับการสร้างโทเคนจะใช้มาตรฐาน JSON Web Token (JWT): RFC-7519 [4] ซึ่งมีข้อกำหนดเหมาะสำหรับการรับส่งข้อมูลเจสันออบเจ็ค เนื่องจากมีขนาดค่อนข้างเล็ก จึงส่งผ่านพารามิเตอร์ POST หรือสามารถส่งภายในส่วน Hypertext Transfer Protocol Header (HTTP Header) ได้ อีกทั้ง JWT มีข้อมูลที่จำเป็นเพียงพอที่ผู้รับ สามารถตรวจสอบความถูกต้องของโทเคนได้โดยไม่ต้องเรียกเซิร์ฟเวอร์ และเพื่อหลีกเลี่ยงการสืบค้นฐานข้อมูลมากกว่าหนึ่งครั้งสำหรับการเรียกดูข้อมูลที่เกี่ยวกับเอนติตี้ ประโยชน์ของการใช้งานมาตรฐาน JWT มีดังต่อไปนี้

(1) JWT มีขนาดที่เล็กกว่าเมื่อเทียบกับ โทเคน Security Assertion Markup Language (SAML) ซึ่งเป็นโทเคนที่เกิดจากการนำ XML มาผ่านกระบวนการแฮชและการลงลายมือชื่อดิจิทัล เนื่องจาก JavaScript Object Notation (JSON) มีความละเอียดของส่วนขยายน้อยกว่า XML ดังนั้นเมื่อมีการเข้ารหัส JWT จะมีขนาดที่เล็กกว่าโทเคน SAML สิ่งนี้ทำให้ JWT เป็นตัวเลือกที่ดีในการส่งผ่านโปรโตคอล Hypertext Transfer Protocol

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

(3) มีการใช้งานกันอย่างแพร่หลาย เนื่องจากภาษาที่ใช้ในการพัฒนาในปัจจุบันรองรับรูปแบบข้อมูลเจสันออบเจ็คอยู่แล้วจึงทำให้ใช้งานได้ง่ายกว่าเมื่อเทียบกับ XML

โครงสร้างของ โทเคนตามมาตรฐาน JWT จะประกอบไปด้วย 3 ส่วนหลักๆ และขั้นด้วย “.” โดยมีลักษณะดังนี้

```
[header].[payload].[signature]
```

ส่วนที่ 1 Header เป็นส่วนที่บอกรายละเอียดของ JWT ส่วนมากจะประกอบไปด้วย algorithm (alg), type(typ), Key ID(kid) ตัวอย่างดังรูปที่ 7

รูปที่ 7 แสดงตัวอย่าง Header ของ JWT

ส่วนที่ 2 Payload เป็นส่วนที่เก็บข้อมูลเบื้องต้นของผู้ใช้งาน และข้อมูลเพิ่มเติมที่ต้องการโดยอยู่ในรูปแบบเจสันออบเจ็ค มีรูปแบบตามตัวอย่างดังรูปที่ 8 ซึ่งประกอบไปด้วย Issuer(iss), Audience(aud), Expiration Time(exp), nonce, Access Token hash value(at_hash), Code hash value(c_hash), Issued At(iat), Time when the authentication occurred(auth_time), not before(nbf), Subject(sub), JWT ID(jti) รายละเอียดความหมายของแต่ละฟิลด์สามารถอ่านเพิ่มเติมได้ที่ ภาคผนวก ก.

รูปที่ 8 แสดงตัวอย่าง Payload ของ JWT

ส่วนที่ 3 Signature เป็นส่วนที่เกิดจากการนำเอา ส่วนของ Header และ Payload มาเข้ารหัสด้วยวิธี Base64 ของแต่ล่ะส่วน จากนั้นนำเอามาต่อกันและคั่นด้วยจุด จากนั้นนำไปเข้ารหัสด้วยวิธีการที่กำหนดอยู่ในส่วนของ Header จากนั้นจะได้ค่าเอาต์พุตให้นำไปเข้ารหัสด้วยวิธีการ Base64

4.5.2 ข้อกำหนดสำหรับพารามิเตอร์ตามมาตรฐาน JWT

ข้อกำหนดในส่วนนี้จะเป็นการอธิบายถึงรายละเอียดของแต่ละฟิลด์ที่มีการใช้งานหรือเป็นทางเลือกสำหรับการใช้งานตามมาตรฐาน TGIX ที่อ้างอิงจากมาตรฐานของ JWT โดยจะอธิบายรายละเอียด และระบุข้อกำหนดเพิ่มเติมเฉพาะส่วนของ TGIX สำหรับการใช้งานส่วนอื่นที่ไม่ได้กล่าวถึงให้ยึดตามมาตรฐาน JWT

ฟิลด์ที่จำเป็นสำหรับส่วนหัว (Required Headers) ได้แก่ Algorithm(alg) เป็นพารามิเตอร์ส่วนหัวของ JWT ที่ระบุถึงข้อมูลอัลกอริทึมในการเข้ารหัสข้อมูลที่ใช้ใน JWT ข้อกำหนดตามมาตรฐาน TGIX กำหนดให้ใช้งานอัลกอริทึม เช่น "RS256" ตามมาตรฐาน JSON Web Algorithms (JWA): RFC-7518 [5] โดยข้อมูลอัลกอริทึมทั้งหมดสามารถอ้างอิงจากได้จากมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐด้านการเชื่อมโยงข้อมูล เรื่องข้อกำหนดของความน่าเชื่อถือและความมั่นคงปลอดภัย

4.5.3 การใช้งาน JSON Web Token สำหรับมาตรฐาน TGIX

การประยุกต์ใช้มาตรฐาน JSON Web Token (JWT): RFC-7519 [4] ในมาตรฐาน TGIX นั้น นอกจากข้อกำหนดต่างๆ ที่ได้กล่าวไปข้างต้น ได้มีการกล่าวถึงขั้นตอนหรือรูปแบบการใช้งานต่างๆ ที่เหมาะสม กระบวนการต่างๆ ที่มีความจำเป็นต้องปฏิบัติตาม เพื่อเป็นแนวทางให้นักพัฒนานำไปพัฒนาระบบงานได้อย่างถูกต้องตรงตามมาตรฐานการรักษาความปลอดภัยในการรับส่งข้อมูลโดยแยกเป็นหัวข้อต่างๆ ดังนี้

4.5.3.1 การตรวจสอบโทเคน (Validate JSON Web Tokens)

การตรวจสอบโทเคนมาตรฐาน TGIX แนะนำให้ผู้ให้บริการจะต้องทำการตรวจสอบโทเคนที่ได้รับมาเสมอ โดยการตรวจสอบนั้นสามารถทำได้หลายวิธีขึ้นอยู่กับวิธีการพัฒนาและภาษาที่ใช้ในการพัฒนา มาตรฐาน TGIX เปิดกว้างให้ผู้ให้บริการสามารถเลือกเทคโนโลยีและภาษาในการพัฒนาระบบให้บริการข้อมูลได้ตามความชำนาญของผู้ให้บริการ การพัฒนาฟังก์ชันการตรวจสอบสามารถแยกออกเป็น 3 กลุ่มดังนี้

(1) ผู้ให้บริการใช้งานจากฟังกชันพื้นฐานที่มีใน Framework ที่ใช้งาน

เนื่องจากปัจจุบัน Framework ที่เป็นที่นิยมใช้งานต่างก็มีฟังก์ชันรองรับการตรวจสอบโทเคน และเป็นไปตามมาตรฐาน JSON Web Token (JWT): RFC-7519 [4] มาตรฐาน TGIX อนุญาตให้นักพัฒนาของผู้ให้บริการสามารถเลือกใช้งานได้ตามความเหมาะสม

(2) ใช้ Third-Party Libs ในการพัฒนาฟังก์ชันการตรวจสอบ

ในกรณีที่ผู้พัฒนาต้องการพัฒนาฟังก์ชันการตรวจสอบโทเคน สามารถดาวน์โหลด Libs ที่ช่วยในการตรวจสอบโทเคนได้จากเว็บ www.jwt.org ซึ่งมี Libs ที่ถูกพัฒนาในภาษาต่างๆ

มาตรฐาน TGIX แนะนำให้นักพัฒนาใช้เกณฑ์ในการเลือกใช้งานโดย ต้องขึ้นอยู่กับภาษาที่ใช้งาน และอัลกอริทึมที่เป็นไปตามข้อกำหนดของ TGIX

(3) ผู้ให้บริการทำการพัฒนาการตรวจสอบด้วยตนเอง

โทเคนที่มีการใช้งานในมาตรฐาน TGIX นั้นอ้างอิงตามมาตรฐาน JSON Web Token (JWT): RFC-7519 [4] ผู้พัฒนาระบบงานให้บริการ ต้องพัฒนาฟังก์ชันการตรวจสอบโดยทำตามมาตรฐาน JSON Web Algorithms (JWA): RFC-7518 [5] หัวข้อ 7.2 การตรวจสอบ JWT ให้ครบถ้วน

หัวข้อการตรวจสอบโทเคน นอกจากจะทำการตรวจสอบโทเคนแล้ว ตามมาตรฐาน TGIX แนะนำให้ผู้ให้บริการจะต้องทำการตรวจสอบเคลม (Claims) ซึ่งเป็นข้อมูลที่เกี่ยวข้องกับการเข้าถึง และสิทธิ์การใช้งานในระบบ โดยให้ทำการตรวจสอบโทเคนออเดียน(Token audience) และ Nonce สำหรับ Implicit Flow

การตรวจสอบโทเคนออเดียน (Token audience) ค่านี้ต้องตรงกับรหัสไคลเอ็นต์ของแอปพลิเคชันตามที่กำหนดไว้ในการตั้งค่าแอปพลิเคชัน

การตรวจสอบ nonce แนะนำให้ส่ง nonce ในคำขอโทเคน เพื่อช่วยป้องกันการโจมตีซ้ำ โดยค่า nonce ในโทเคนต้องตรงกับ nonce เดิมที่ส่งในคำขอ

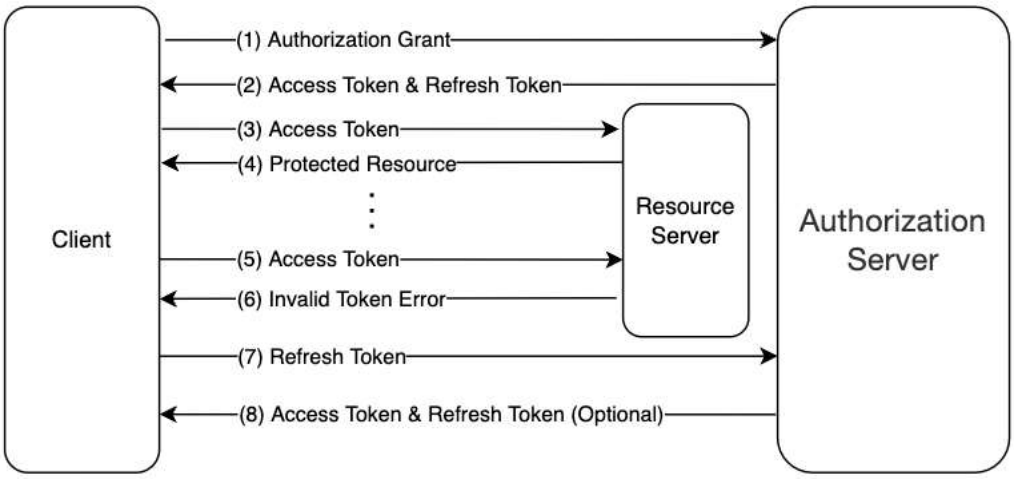
4.5.4 การถอดถอนโทเคน (Revoke Token)

เนื่องจากเมื่อมีการออกโทเคนแล้ว ทั้งโทเคนการเข้าถึง (Access Token) และโทเคน ID (ID Token) เทคนิคการเพิกถอนจะมีความแตกต่างกับของไอดีเซสชัน (Session ID) สำหรับฝั่งเซิร์ฟเวอร์อยู่ คือต้องรอให้หมดอายุตามเวลาที่กำหนด ดังนั้นเพื่อเหตุผลด้านความปลอดภัยในกรณีที่ต้องการเพิกถอนโทเคนการเข้าถึง (Access Token) และโทเคน ID (ID Token) จึงต้องมีการจำกัดเวลาที่ค่อนข้างสั้น และให้ใช้กระบวนการรีเฟรชโทเคน (Refresh Token) เป็นระยะ และทำการเพิกถอนรีเฟรชโทเคน (Refresh Token) แทน จะทำให้ผู้ใช้ขอบริการนั้น ไม่สามารถทำการต่ออายุโทเคนได้ เมื่อโทเคนการเข้าถึง (Access Token) และโทเคนไอดี (ID Token) หมดอายุ โดยมาตรฐาน TGIX แนะนำให้มีการพัฒนาฟังก์ชันการถอดถอนรีเฟรชโทเคนเพื่อใช้ในกรณีที่ต้องการยกเลิกการใช้งานโทเคนนั้น

4.5.5 การรีเฟรชโทเคน (Refresh Token)

ในกรณีที่โทเคนการเข้าถึง (Access Token) หมดอายุ จะต้องมีกระบวนการในการรีเฟรชโทเคนที่เหมาะสมเช่น ไม่ควรเรียกปลายทางเพื่อรับโทเคนการเข้าถึงใหม่ทุกครั้ง จะมีการเรียกใช้งานเมื่อโทเคนการเข้าถึง (Access Token) หมดอายุหรือใกล้หมดอายุเท่านั้นดังรูปที่ 9 ในการขอรีเฟรชโทเคน ขั้นตอนที่ 1 เมื่อ client มีการร้องขอการผู้พิสูจน์และยืนยันตัวตนผ่านแล้ว ขั้นตอนที่ 2 client จะได้รับข้อมูลโทเคนการเข้าถึง (Access Token) และรีเฟรชโทเคน (Refresh Token) กลับมา ขั้นตอนที่ 3-5 client จะสามารถใช้งานเซอร์วิสของผู้ให้บริการ(Resource Server) ได้โดยการส่งโทเคนการเข้าถึง (Access Token) ไปในส่วนหัวของ HTTP (HTTP Header) ของทุกคำร้องขอใช้บริการ ในกรณีที่ผู้ให้บริการปฏิเสธการเข้าถึงในขั้นตอนที่ 6 บริการโดยตอบกลับสถานะโทเคนการเข้าถึง (Access Token) ไม่ถูกต้อง client จะต้องทำการร้องขอไปยัง

Authorization Server ขั้นตอนที่ 7 เพื่อทำการออกโทเคนการเข้าถึง (Access Token) ใหม่เมื่อหมดอายุ ในขั้นตอนที่ 8 client จะได้รับโทเคนการเข้าถึง (Access Token) ใหม่จาก Authorization Server



รูปที่ 9 แสดงกระบวนการรีเฟรชโทเคนการเข้าถึง(Access Token) ที่หมดอายุ

การส่งคำขอ POST ไปยัง Endpoint เช่น /oauth/token โดยสามารถระบุพารามิเตอร์ต่าง ๆ ดังนี้ grant_type, refresh_token, scope, client_id, client_secret กรณีที่มีการใช้งาน Authorization code ไม่ต้องระบุ client_id กับ client_secret เพื่อเป็นการออกโทเคนการเข้าถึง ดังรูป 10

```
POST  /auth/token HTTP/1.1
Host: domain.name
grant_type=refresh_token
&refresh_token=xxxxxxxxxxx
&client_id=xxxxxxxxxx
&client_secret=xxxxxxxxxx
&scope=profile
```

รูปที่ 10 แสดงตัวอย่าง POST Message ในการขอออกโทเคนการเข้าถึง (Access Token) เมื่อหมดอายุ

มาตรฐาน TGIX แนะนำให้รีเฟรชโทเคน ควรมีการกำหนดอายุการใช้งาน โดยจะขึ้นอยู่กับผู้ให้บริการผู้พิสูจน์และยืนยันตัวตน (Identity Provider) โดยค่าของอายุการใช้งานสามารถกำหนดได้ตั้งแต่ 30 วันจนถึง 6 เดือน

ภาคผนวก ก. รายละเอียดฟิลด์ตามมาตรฐาน JWT

ตารางที่ 6 รายละเอียดฟิลด์ตามมาตรฐาน JWT

ฟิลด์ของเฮดเดอร์		
ฟิลด์	คำอธิบายรายละเอียด	การใช้งาน
“alg”	อัลกอริทึม เป็นพารามิเตอร์ส่วนหัวของ JWT ที่ระบุถึงข้อมูลอัลกอริทึมในการเข้ารหัสข้อมูลที่ใช้ใน JWT ข้อกำหนดตามมาตรฐาน TGIX กำหนดให้ใช้งานอัลกอริทึม เช่น "RS256" ตามมาตรฐาน JSON Web Algorithms (JWA): RFC-7518 [5] โดยข้อมูลอัลกอริทึมทั้งหมดอ้างอิงจาก มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่องข้อกำหนดของความน่าเชื่อถือและความมั่นคงปลอดภัย	ฟิลด์จำเป็นสำหรับเฮดเดอร์
“*typ*”	ไทป์ (type) เป็นพารามิเตอร์ส่วนหัวของ JWT ข้อกำหนดตามมาตรฐาน ให้ระบุเป็นค่า “JWT” ตามมาตรฐาน JSON Web Token (JWT): RFC-7519 [4]	ฟิลด์ทางเลือกสำหรับเฮดเดอร์
“kid”	คีย์ไอดี (key ID) เป็นพารามิเตอร์ส่วนหัวของ JWT โดยเป็นค่าที่บ่งบอกว่าใช้กุญแจไหน ในการเข้ารหัส โทเคน JWT ตามมาตรฐาน JSON Web Signature (JWS): RFC-7515 [6] เช่น “/path/acb.key” หรือเป็น reference “77534975863792b639e15920889adaceff77”	ฟิลด์ทางเลือกสำหรับเฮดเดอร์
ฟิลด์ของเคลม (Claims)		
“iss”	ผู้ออกสิทธิ์ (Issuer) เป็นค่าที่ระบุตัวตนผู้ที่ทำการรับรองการอ้างสิทธิ์ โดยค่าข้อมูลเป็นแบบ case sensitive URL ที่แสดงถึงรูปแบบ เช่น “https://domain-name:port/path”	ฟิลด์จำเป็นสำหรับเคลม
“aud”	ผู้ชม (Audience) กลุ่มเป้าหมายที่ ID Token นี้มีไว้สำหรับ ต้องมี OAuth 2.0 client_id ของ Relying Party เป็นค่าผู้ชม นอกจากนี้ยังอาจมีตัวระบุสำหรับผู้ชมอื่นๆ ในกรณีทั่วไป ค่า aud คืออาร์เรย์ของสตริงที่คำนึงถึงขนาดตัวพิมพ์ ในกรณีพิเศษทั่วไปเมื่อมีผู้ชมหนึ่งราย ค่า aud อาจเป็นสตริงที่ละเอียดอ่อนตัวพิมพ์เล็กและตัวพิมพ์ใหญ่ เช่น “https://domain-name:port”	ฟิลด์จำเป็นสำหรับเคลม

ตารางที่ 6 รายละเอียดฟิลด์ตามมาตรฐาน JWT (ต่อ)

ฟิลด์	คำอธิบายรายละเอียด	การใช้งาน
“exp”	เวลาหมดอายุ (expiration time) ระบุเวลาหมดอายุของโทเคน "exp" กำหนดให้วันที่/เวลาปัจจุบันต้องอยู่ก่อนวันที่/เวลาหมดอายุที่ระบุไว้ในการอ้างสิทธิ์ "exp" ผู้ดำเนินการอาจกำหนดเวลาเล็กน้อย โดยปกติไม่เกินสองสามนาที เพื่อพิจารณา Leap Seconds ค่าจะต้องเป็นตัวเลขที่มีค่า NumericDate ตามมาตรฐาน JSON Web Token (JWT): RFC-7519 [4] **หมายเหตุ:** NumericDate จะมีการใช้งานโดยพารามิเตอร์ exp, iat, และข้อมูลส่วนอื่นๆ ที่เกี่ยวข้องกับเคลม โดยค่าข้อมูลนี้จะนำเสนอจำนวนตัวเลขหน่วยเป็นวินาทีเริ่มนับจากเวลาเริ่มต้นคือ วันที่ 1970-01-01T00:00:00Z UTC จนถึงปัจจุบันไม่นับรวม leap seconds เช่น “1645360320”	ฟิลด์จำเป็นสำหรับเคลม
“nonce”	นอนซ (nonce : Number used ONCE) หมายถึงตัวเลขหรือสตริงที่ไม่ซ้ำกันและถูกใช้เพียงครั้งเดียวเท่านั้น ใช้ในการเชื่อมโยงเซสชันไคลเอ็นต์กับโทเคน ID และเพื่อลดการโจมตีซ้ำ (Replay Attacks) ซึ่ง nonce จะถูกส่งจากผู้ขอใช้บริการ (ในรูปแบบโทเคน) ไปยังเซิร์ฟเวอร์เพื่อยืนยันว่าคำขอที่ส่งมานั้น ไม่ได้ถูกผู้ไม่ประสงค์ดีดักฟังและส่งคืนเข้ามาใหม่ นอกจากนี้ nonce ยังช่วยป้องกันการขโมยเซสชันและให้ความมั่นใจว่าคำขอที่ส่งมานั้นมาจากผู้ใช้ที่ถูกต้อง ตัวอย่าง nonce : “ee14908a-9248-11ec-b909-0242ac120002”	ฟิลด์ทางเลือก
“at_hash”	ค่าแฮชโทเคน (Access Token hash value) คือการเข้ารหัส base64 ของครึ่งซ้ายสุดของแฮช โดยที่อัลกอริทึมแฮชที่ใช้ คืออัลกอริทึมแฮชที่ใช้ในพารามิเตอร์ส่วนหัว alg ของส่วนหัว JOSE ของ ID Token ตัวอย่างเช่น ถ้า alg เป็น RS256 ให้แฮชค่า access_token ด้วย SHA-256 จากนั้นใช้ 128 บิตที่อยู่ทางซ้ายสุดและ base64url เข้ารหัสค่า at_hash เป็นสตริงที่คำนึงถึงขนาดตัวพิมพ์ เช่น “lOtI0BRou0Z4LPtQuE8cCw”	ฟิลด์ทางเลือก

ตารางที่ 6 รายละเอียดฟิลด์ตามมาตรฐาน JWT (ต่อ)

ฟิลด์	คำอธิบายรายละเอียด	การใช้งาน

“c_hash”	ค่าแฮชโค้ด (Code hash value) คือการเข้ารหัส base64url ของครึ่งซ้ายสุดของแฮช โดยที่อัลกอริทึมแฮชที่ใช้ คืออัลกอริทึมแฮชที่ใช้ในพารามิเตอร์ alg Header ของส่วนหัว JOSE ของ ID Token ตัวอย่างเช่น ถ้า alg เป็น HS512 ให้แฮชค่าโค้ดด้วย SHA-512 จากนั้นใช้ 256 บิตที่อยู่ทางซ้ายสุดและ base64 เข้ารหัสค่า c_hash เป็นสตริงที่คำนึงถึงขนาดตัวพิมพ์ เช่น “lOtI0BRou0Z4LPtQuE8cCw”	ฟิลด์ทางเลือก
“iat”	(Issued At) เป็นค่าที่ระบุเวลาที่ออก JWT สามารถใช้เพื่อกำหนดอายุของ JWT ค่าจะต้องเป็นตัวเลขที่มีค่า NumericDate ใช้การอ้างสิทธิ์นี้เป็นทางเลือก **หมายเหตุ:** NumericDate จะมีการใช้งานโดยพารามิเตอร์ exp, iat, และข้อมูลส่วนอื่นๆ ที่เกี่ยวข้องกับเคลม โดยค่าข้อมูลนี้จะนำเสนอจำนวนตัวเลขหน่วยเป็นวินาทีเริ่มนับจากเวลาเริ่มต้นคือ วันที่ 1970-01-01T00:00:00Z UTC จนถึงปัจจุบันไม่นับรวม leap seconds เช่น 1645360320	ฟิลด์ทางเลือก
“auth_time”	เวลาที่เกิดการตรวจสอบสิทธิ์ผู้ใช้ (Time when the authentication occurred) คือค่าจำนวนตัวเลขหน่วยเป็นวินาทีเริ่มนับจากเวลาเริ่มต้นคือ วันที่ 1970-01-01T00:00:00Z UTC จนถึงเวลาที่มีการร้องขอการตรวจสอบสิทธิ์ผู้ใช้ เช่น 1645360320	ฟิลด์ทางเลือก
“nbf”	ก่อนเวลาที่กำหนด (not before) เป็นการระบุเวลา ถ้าเหตุการณ์เกิดขึ้นก่อนเวลาที่กำหนด JWT ต้องไม่ได้รับการยอมรับสำหรับการประมวลผล การประมวลผลคำร้อง "nbf" กำหนดให้วันที่/เวลาปัจจุบันต้องอยู่หลังหรือเท่ากับวันที่/เวลาก่อนหน้าที่ระบุไว้ในการอ้างสิทธิ์ "nbf" เช่น 1645360320	ฟิลด์ทางเลือก
“sub”	หัวเรื่อง (Subject) ระบุหัวเรื่องของ JWT โดยไม่ซ้ำกัน เช่น “89d23c7e-924a-11ec-b909-0242ac120002”	ฟิลด์ทางเลือก

ตารางที่ 6 รายละเอียดฟิลด์ตามมาตรฐาน JWT (ต่อ)

ฟิลด์	คำอธิบายรายละเอียด	การใช้งาน
“jti”	เจดับเบิลยูไอดี (JWT ID) ใช้เป็นตัวเชื่อมต่อเอกลักษณ์ของ Token นั้น ๆ ในรูปของข้อมูลที่ไม่ซ้ำกัน (unique identifier) สามารถใช้เพื่อป้องกันหรือลดการโจมตีซ้ำ (Replay Attack) และรักษาความปลอดภัยในการใช้งานโทเคนนั้น ๆ นอกจากนี้ jti ยังเป็นข้อมูลที่มีประโยชน์ในการติดตามและสอบสวนโทเคนที่ถูกใช้ หรือยกเลิกการใช้งาน token ที่ควบคุมโดยระบบการอนุญาต ค่า "jti" เป็นสตริงที่คำนึงถึงขนาดตัวพิมพ์ ตามมาตรฐาน JSON Web Token (JWT): RFC-7519 [4] หัวข้อ 4.1.7	ฟิลด์ทางเลือก

บรรณานุกรม

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

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

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

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

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

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

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