



มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล  
(องค์การมหาชน)

DGA Community Standard

มสพร. 10-1 : 2566

DGA 10-1 : 2566

ว่าด้วย มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ  
ด้านการเชื่อมโยงข้อมูล เรื่องสถาปัตยกรรมอ้างอิง

(THAILAND GOVERNMENT INFORMATION EXCHANGE  
STANDARD, SERIES: LINKAGE STANDARD,  
PART 1: REFERENCE ARCHITECTURE)

เวอร์ชัน 1.0

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

สำนักนายกรัฐมนตรี

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)  
ว่าด้วย มาตรฐานการเชื่อมโยงและแลกเปลี่ยน  
ข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล  
เรื่องสถาปัตยกรรมอ้างอิง

มสพร. 10-1 : 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**

ผู้ช่วยศาสตราจารย์ภูษงค์ อุทัยภาส

มหาวิทยาลัยเกษตรศาสตร์

**รองประธานกรรมการ**

นางไอรดา เหลืองวิไล

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

**กรรมการ**

นายเฉลิมชัย ก๊กเกียรติกุล

สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์  
และกิจการโทรคมนาคมแห่งชาติ

นายมารุต บุรณรัช

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

นายศุภโชค จันทระประทีน

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

นางบุญยิ่ง ชั่งสัจจา

สำนักบริหารการทะเบียน กรมการปกครอง

นายณัฐฐา พาชัยยุทธ

สำนักงานคณะกรรมการพัฒนาระบบราชการ

นายพีชโรดม ลิ้มปิยะเสีयर

สำนักงานคณะกรรมการกฤษฎีกา

นายธีรวุฒิ ธงภักดิ์

สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

นายสันติ สิทธิเลิศพิศาล

สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม

นายวีระ วีระกุล

ผู้แทนภาคดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย

นายวิทยา สุหฤทธำรง

วิศวกรรมสถานแห่งประเทศไทย

รองศาสตราจารย์เกริก ภิรมย์โสภา

ประธานคณะทำงานเทคนิคด้านมาตรฐานความมั่นคงปลอดภัย  
ภาครัฐ

รองศาสตราจารย์ธีรณี อจลากุล

ประธานคณะทำงานเทคนิคด้านมาตรฐานการบริหารจัดการ  
ข้อมูลภาครัฐ

ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูโพโรจน์

ประธานคณะทำงานเทคนิคด้านมาตรฐานการเชื่อมโยงและ  
แลกเปลี่ยนข้อมูลภาครัฐ

**กรรมการและเลขานุการ**

นางสาวอรุชฎา เกตุพรหม

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

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

**ที่ปรึกษา**

นายสุพจน์ เตียรุจดี

ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

**ประธานกรรมการ**

ผู้ช่วยศาสตราจารย์ ดร. ฐิติภูมิ หนูโพโรจน์

จุฬาลงกรณ์มหาวิทยาลัย

**รองประธานกรรมการ**

นายอาศิส อัญญาโพธิ์

ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

**กรรมการ**

นายเฉลิมชัย ก๊กเกียรติกุล

สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์  
และกิจการโทรคมนาคมแห่งชาติ

นายมารุต บุรณรัช

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

นางสาวชนิษฐ์ ผาทอง

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

นางบุญยิ่ง ชั่งสัจจา

สำนักบริหารการทะเบียน กรมการปกครอง

นายเกียรติชัย ชุ่มมงคล

นายณัฐฐา พาชัยยุทธ

สำนักงานคณะกรรมการพัฒนาระบบราชการ

นายพัชโรดม ลิ้มปิยะเสียร

สำนักงานคณะกรรมการกฤษฎีกา

นายธีรวิทย์ ธงภักดิ์

สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

นายกฤษณ์ โกวิทพัฒนา

นางสาวเกศินี ทองชูศักดิ์

นายสันติ สิทธิเลิศพิศาล

สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม

นายวีระ วีระกุล

สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย

นายวิทยา สุทธิพิตรดำรง

วิศวกรรมสถานแห่งประเทศไทย

นายคณพศ หงสาวรางกูร

สำนักงานการตรวจเงินแผ่นดิน

รองศาสตราจารย์เกริก ภิรมย์โสภา

ประธานคณะกรรมการเทคนิคด้านมาตรฐานความมั่นคงปลอดภัย  
ภาครัฐ

รองศาสตราจารย์ธีรณี อจลากุล

ประธานคณะกรรมการเทคนิคด้านมาตรฐานการบริหารจัดการ  
ข้อมูลภาครัฐ

ผู้ช่วยศาสตราจารย์มารอง ผดุงสิทธิ์

ประธานคณะกรรมการเทคนิคด้านมาตรฐานการเชื่อมโยงและ  
แลกเปลี่ยนข้อมูลภาครัฐ

## กรรมการและเลขานุการ

นางสาวอรุณชญา เกตุพรหม

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

## คณะกรรมการเทคนิคด้านมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ตามคำสั่งที่ 69/2564 ลงวันที่ 20 ตุลาคม 2564

### ที่ปรึกษา

นายสุพจน์ เตียรุจดี

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ผู้ช่วยศาสตราจารย์ภูษงค์ อุทัยภาค

มหาวิทยาลัยเกษตรศาสตร์

นางไอรดา เหลืองวิไล

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

### ประธานคณะกรรมการ

ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูโพโรจน์

จุฬาลงกรณ์มหาวิทยาลัย

### รองประธานคณะกรรมการ

ผู้ช่วยศาสตราจารย์มารอง ผดุงสิทธิ์

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี

### คณะกรรมการ

นางบุญยิ่ง ชั่งสังจา

กรมการปกครอง

นางสาวมนทิพา แข่งพิมล

กรมพัฒนาธุรกิจการค้า

นายพงศกร รियะมงคล

นายกุลเชษฐ์ ชีวะไพบูลย์

นายกำชัย จัตตานนท์

กรมศุลกากร

นางบุษยา ดวงตา

นางสาวชนิษฐา สหเมธาพัฒน์

กรมสรรพากร

นายยุทธพล จินะสี

นางสาวภัทราพรรณ วงศาโรจน์

ธนาคารแห่งประเทศไทย

นายยรรยง ดำรงค์ศิริ

นางสาวจิตสุภา วิริยะวานิช

นายกิตติพงษ์ สุขสม

นายพิสุทธิ นาคหมื่นไวย

สำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ (องค์การมหาชน)

นางศุภกิจ สกลเสาวภาคย์

กรมที่ดิน

นางดวงรัตน์ จันทระประดิษฐ์

นายอาศิส อัญญาโพธิ์  
นายมนต์ศักดิ์ โช้เจริญธรรม

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)  
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

**คณะทำงานและเลขานุการ**

นางสาวอุรชฎา เกตุพรหม

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

**ผู้ช่วยเลขานุการ**

นายเจษฎา ขจรฤทธิ์

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะกรรมการเทคนิคด้านมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ  
ตามคำสั่งที่ 85/2565 ลงวันที่ 31 ตุลาคม 2565

**ที่ปรึกษา**

นายสุพจน์ เจริญภูมิ	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูไพโรจน์	จุฬาลงกรณ์มหาวิทยาลัย
นายอาศิษ อัญญาโพธิ์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

**ประธานคณะกรรมการ**

ผู้ช่วยศาสตราจารย์มารอง ผดุงสิทธิ์	มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี
------------------------------------	---------------------------------------

**รองประธานคณะกรรมการ**

นางสาวศวลัย โชติปทุมวรรณ	มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
--------------------------	--

**คณะกรรมการ**

นางบุญยิ๊ง ชั่งสังจา	กรมการปกครอง
นางสาวมนทิพา แข่งพิมล	กรมพัฒนาธุรกิจการค้า
นายพงศกร ริยะมงคล	
นายกำชัย จัดตานนท์	กรมศุลกากร
นางบุษยา ดวงตา	
นางสาวชนิษฐา สหเมธาพัฒน์	กรมสรรพากร
นายยุทธพล จินะสี	
นางสาวภัทราพรรณ วงศาโรจน์	ธนาคารแห่งประเทศไทย
นายบรรยง ดำรงค์ศิริ	
นางสาวจิตสุภา วัระยะวานิช	
นายกิตติพงษ์ สุขสม	
นางสาวดลพร พิมพ์ชัย	สำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ (องค์การมหาชน)
นางศุภกิจ สกลเสาวภาคย์	กรมที่ดิน
นางดวงรัตน์ จันทระประดิษฐ์	

**คณะกรรมการและเลขานุการ**

นางสาวอรรชฎา เกตุพรหม	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
-----------------------	---

วิเคราะห์และจัดทำมาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัล ว่าด้วย  
มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ  
ด้านการเชื่อมโยงข้อมูล  
เรื่องสถาปัตยกรรมอ้างอิง

นายเจษฎา ขจรฤทธิ์

นายปรภากร ศิริมา

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)



## คำนำ

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

มาตรฐานฉบับนี้คือ มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่อง การสถาปัตยกรรมอ้างอิง เป็นมาตรฐานลำดับที่ 1 ในกลุ่มมาตรฐานด้านการเชื่อมโยงข้อมูล กล่าวถึงสถาปัตยกรรมอ้างอิงของการแลกเปลี่ยนข้อมูลระหว่างผู้ให้บริการข้อมูล (Data Providers) และผู้ใช้บริการข้อมูล (Data Consumers) ผ่านทางผู้ให้บริการแลกเปลี่ยนข้อมูล (Exchange Provider) เพื่อให้เกิดการอ้างอิงถึงองค์ประกอบที่เกี่ยวข้องและวิธีการทำงานร่วมกัน

## สารบัญ

1	ขอบข่าย .....	13
2	บทนิยาม.....	14
3	กฎหมายและแนวปฏิบัติที่เกี่ยวข้อง .....	16
4	ภาพรวมของมาตรฐานสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ .....	17
5	มาตรฐานสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในกลุ่ม TGIX.....	18
5.1	ภาพรวมสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในกลุ่ม TGIX.....	18
5.2	แนวทางการดำเนินการของระบบผู้ให้บริการ (Provider System).....	20
5.3	แนวทางดำเนินการของระบบผู้ใช้บริการ (Consumer System).....	22
5.4	แนวทางดำเนินการของผู้ให้บริการ TGIX Platform (TGIX Platform Provider).....	23
5.4.1	การบริการพิสูจน์และยืนยันตัวตน (Identity Provider).....	23
5.4.2	ระบบอำนวยความสะดวกการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Service Operation Center: SOC)	23
5.4.3	การบริการออกใบรับรอง (Certification Authority).....	25
5.5	ขั้นตอนการทำงานขององค์ประกอบภายในกลุ่ม TGIX.....	27
5.5.1	การเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในกลุ่ม TGIX (TGIX Intra-DX).....	27
5.5.2	การลงทะเบียน API ของผู้ให้บริการ API ที่ TGIX Platform.....	29
5.5.3	การทำข้อตกลงการให้บริการของผู้ให้บริการ API .....	29
5.5.4	การทำข้อตกลงการใช้บริการของผู้ใช้บริการ API.....	31
6	รูปแบบข้อความตามมาตรฐาน TGIX (JSON Data Format).....	32
6.1	แนวคิดในการออกแบบ .....	32
6.2	รูปแบบของข้อความ (TGIX Data Format).....	32
6.2.1	ข้อกำหนดเฮดเดอร์ของ Protocol .....	32
6.2.2	ข้อกำหนดบอดีของ Protocol.....	33
6.3	ตัวอย่างข้อความตามมาตรฐาน TGIX .....	35
6.3.1	ตัวอย่างข้อความที่กำหนด Content Type มีค่าเป็น “application/json” .....	35
6.3.2	ตัวอย่างข้อความที่กำหนด Content Type มีค่าเป็น “multipart/related” .....	35
6.4	กรณีการใช้งานที่ผู้ให้บริการสามารถเลือกดำเนินการ.....	37
6.4.1	กรณีการใช้งานเพื่อแลกเปลี่ยนข้อมูลเชิงธุรกรรม.....	37
6.4.2	กรณีการใช้งานเพื่อแลกเปลี่ยนข้อมูลที่เป็นไฟล์ .....	37

บรรณานุกรม ..... 40

## สารบัญรูป

รูปที่ 1 ความหมายของ API.....	17
รูปที่ 2 แผนภาพสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐภายในกลุ่ม TGIX.....	18
รูปที่ 3 แผนภาพแสดงโครงสร้างและความสัมพันธ์ระหว่างองค์ประกอบภายในกลุ่ม TGIX.....	19
รูปที่ 4 องค์ประกอบของระบบผู้ให้บริการ (PROVIDER SYSTEM).....	20
รูปที่ 5 การเรียกใช้บริการ API.....	23
รูปที่ 6 บริการของผู้ให้บริการ TGIX PLATFORM.....	23
รูปที่ 7 โครงสร้างของข้อตกลงหรือสัญญาระหว่างผู้ให้บริการและผู้ให้บริการ .....	24
รูปที่ 8 ตัวอย่างข้อตกลงการให้บริการ .....	25
รูปที่ 9 แผนภาพแสดงการทำงานแบบลำดับปฏิสัมพันธ์ (SEQUENCE DIAGRAM) ของการแลกเปลี่ยนข้อมูลภายในกลุ่ม TGIX .....	27
รูปที่ 10 แผนภาพแสดงการทำงานแบบลำดับปฏิสัมพันธ์ (SEQUENCE DIAGRAM) ของการลงทะเบียนบริการสำหรับแลกเปลี่ยนข้อมูลภายในกลุ่ม TGIX ของผู้ให้บริการ API .....	29
รูปที่ 11 แผนภาพแสดงการทำงานแบบลำดับปฏิสัมพันธ์ (SEQUENCE DIAGRAM) ของการลงทะเบียนข้อตกลงการให้บริการสำหรับแลกเปลี่ยนข้อมูลภายในกลุ่ม TGIX ของผู้ให้บริการ API.....	30
รูปที่ 12 แผนภาพแสดงการทำงานแบบลำดับปฏิสัมพันธ์ (SEQUENCE DIAGRAM) ของการลงทะเบียนข้อตกลงการให้บริการสำหรับการแลกเปลี่ยนข้อมูลภายในกลุ่ม TGIX ของผู้ให้บริการ API.....	31
รูปที่ 13 ตัวอย่างข้อความ ที่กำหนด CONTENT TYPE ให้มีค่าเป็น “APPLICATION/JSON” .....	35
รูปที่ 14 ตัวอย่างข้อความ ที่กำหนด CONTENT TYPE ให้มีค่าเป็น “MULTIPART/RELATED” .....	36
รูปที่ 15 แสดงตัวอย่างการทำงานสำหรับการส่งไฟล์ขนาดใหญ่ .....	38
รูปที่ 16 การกำหนดค่าสำหรับ PART ที่เป็นข้อมูล BINARY .....	38

## สารบัญตาราง

ตารางที่ 1 อธิบายขั้นตอนการทำงานของ การแลกเปลี่ยนข้อมูลภายในกลุ่ม TGIX .....	28
ตารางที่ 2 อธิบายขั้นตอนการทำงานของ การลงทะเบียนและสร้างรายการบริการของผู้ให้บริการ API .....	29
ตารางที่ 3 อธิบายขั้นตอนการทำงานของ การลงทะเบียนข้อตกลงให้บริการ .....	30
ตารางที่ 4 อธิบายขั้นตอนการทำงานของ การลงทะเบียนข้อตกลงให้บริการ.....	31
ตารางที่ 5 อธิบายรายละเอียดโครงสร้างของ TGIX MESSAGE HEADERS ส่วน HTTP HEADER .....	33
ตารางที่ 6 อธิบายรายละเอียดส่วนของลายมือชื่อ (SIGNATURE).....	34

**มาตรฐานรัฐบาลดิจิทัล**  
**ว่าด้วย มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ**  
**ด้านการเชื่อมโยงข้อมูล เรื่อง สถาปัตยกรรมอ้างอิง**

**1 ขอบข่าย**

การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานเป็นพื้นฐานหลักที่จำเป็นต่อการพัฒนารัฐบาลดิจิทัล ในปัจจุบันประเทศไทยมีแพลตฟอร์มการแลกเปลี่ยนข้อมูลที่ให้บริการอยู่หลายแห่ง แพลตฟอร์มแต่ละแห่งมีแนวทางและพันธกิจในการดำเนินงานเป็นของตนเอง เป็นผลให้การบูรณาการข้อมูลภาครัฐจำเป็นต้องขับเคลื่อนด้วยการสร้างมาตรฐานหรือข้อตกลงร่วมกันในการแลกเปลี่ยนข้อมูล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ได้เล็งเห็นความสำคัญในจุดนี้ จึงมีความจำเป็นต้องจัดทำมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ เพื่อใช้ในการ แลกเปลี่ยนข้อมูลระหว่างหน่วยงานของรัฐเพื่อให้เกิดการบูรณาการข้อมูลเกิดขึ้นอย่างเป็นรูปธรรม

เป้าประสงค์หลักของการใช้มาตรฐานฯ เป็นตัวขับเคลื่อนการบูรณาการข้อมูลภาครัฐ คือ การให้หน่วยงาน ของรัฐมีแนวทางในการพัฒนาสถาปัตยกรรมระบบสารสนเทศเพื่อใช้ในการแลกเปลี่ยนข้อมูลที่ชัดเจน มีความสอดคล้องในการเชื่อมต่อระหว่างกัน

สถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ฉบับนี้ มีขอบเขตมาตรฐานที่ระดับการเชื่อมโยงข้อมูลเท่านั้น ไม่ได้ครอบคลุมถึงระดับการจัดการข้อมูลทางธุรกรรมของหน่วยงาน (Business Transaction Data) ที่เกิดขึ้นจากการเชื่อมโยงและแลกเปลี่ยนระหว่างกัน

ดังนั้นเพื่อให้บรรลุเป้าประสงค์หลักดังกล่าวเอกสารฉบับนี้ จึงนำเสนอมาตรฐานสถาปัตยกรรมสำหรับการแลกเปลี่ยนข้อมูลที่สมาชิกในกลุ่มดำเนินการตามมาตรฐาน TGIX มีรายละเอียดของส่วนประกอบต่างๆ ตลอดจนถึงขั้นตอนการทำงานของแต่ละส่วนประกอบ และแนวทางการดำเนินการตามมาตรฐานฯ ของหน่วยงานเจ้าของระบบเทคโนโลยีสารสนเทศ มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ เรื่อง มาตรฐานสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐระดับการเชื่อมโยงข้อมูลที่เหมาะสมกับบริบทของประเทศไทยเท่านั้น

## 2 บทนิยาม

นิยามคำศัพท์ที่เกี่ยวข้องกับมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่อง สถาปัตยกรรมอ้างอิงที่ใช้ในเอกสารฉบับนี้มีดังนี้

- 2.1 มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ (Thailand Government Information Exchange: TGIX) หมายความว่า มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐของประเทศไทย เรียกแบบย่อว่า “มาตรฐานฯ”
- 2.2 Application Programming Interface หรือ API หมายความว่า ช่องทางการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐระหว่างระบบผู้ให้บริการข้อมูลและระบบผู้ใช้บริการข้อมูล
- 2.3 Representational State Transfer (REST API หรือ RESTful API) หมายความว่า ช่องทางการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐระหว่างระบบผู้ให้บริการข้อมูลและระบบผู้ใช้บริการข้อมูล ตามมาตรฐาน TGIX
- 2.4 JavaScript Object Notation (JSON) หมายความว่า รูปแบบของโครงสร้างข้อมูลที่ใช้แลกเปลี่ยนผ่าน REST API
- 2.5 TGIX Data Format หมายความว่า รูปแบบของมาตรฐานโครงสร้างข้อมูลที่ใช้แลกเปลี่ยนผ่าน REST API ตามมาตรฐาน TGIX
- 2.6 ผู้ให้บริการ (Provider) หมายความว่า หน่วยงานที่เปิดให้บริการ API สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในแพลตฟอร์มที่ใช้มาตรฐาน TGIX
- 2.7 ระบบผู้ให้บริการ (Provider System) หมายความว่า ระบบสารสนเทศของหน่วยงานมีการใช้บริการ API สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในแพลตฟอร์มที่ใช้มาตรฐาน TGIX
- 2.8 ผู้ใช้บริการ (Consumer) หมายความว่า หน่วยงานที่ใช้บริการ API สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในแพลตฟอร์มที่ใช้มาตรฐาน TGIX
- 2.9 ระบบผู้ใช้บริการ (Consumer System) หมายความว่า ระบบสารสนเทศของหน่วยงานที่ใช้บริการ API สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในแพลตฟอร์มที่ใช้มาตรฐาน TGIX
- 2.10 แพลตฟอร์มมาตรฐาน TGIX-based Data Exchange Platform หมายความว่า ระบบสารสนเทศการเชื่อมโยงและแลกเปลี่ยนข้อมูลกลางที่มีมาตรฐานตาม TGIX โดยเรียกแบบย่อว่า “TGIX Platform”
- 2.11 ผู้ให้บริการ TGIX Platform (TGIX Platform Provider) หมายความว่า ระบบสารสนเทศของหน่วยงานผู้ให้บริการ TGIX Platform เพื่อสนับสนุนการเชื่อมโยงและแลกเปลี่ยนข้อมูลให้เป็นไปตามมาตรฐาน TGIX

- 2.12 การบริการพิสูจน์และยืนยันตัวตน (Identity Provider) หมายความว่า บริการของผู้ให้บริการ TGIX Platform เพื่อพิสูจน์และยืนยันตัวตนทางดิจิทัลของบุคคลหรือหน่วยงานที่ต้องการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐด้วยมาตรฐาน OAuth 2.0 หรือ Open ID Connect
- 2.13 ระบบอำนวยการกลางการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Service Operation Center: SOC) หมายความว่า บริการของผู้ให้บริการ TGIX Platform เพื่อใช้ในการจัดการและกำกับดูแลให้การเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐให้เป็นไปตามมาตรฐาน TGIX
- 2.14 การบริการออกใบรับรอง (Certification Authority) หมายความว่า ผู้ให้บริการที่ทำหน้าที่ออกใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) เพื่อสนับสนุนการเชื่อมโยงและแลกเปลี่ยนข้อมูลให้เป็นไปตามมาตรฐาน TGIX
- 2.15 API Gateway หมายความว่า เครื่องมือสำหรับจัดการ API ทำหน้าที่กรองคำขอใช้บริการ API จากระบบผู้ให้บริการแล้วประมวลผลในด้านต่างๆ เช่น จัดการกับ Rate Limit ของ API จัดการด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) ก่อนที่จะส่งคำขอต่อไปยังระบบผู้ให้บริการ
- 2.16 ข้อมูลเชิงธุรกรรม (Business Transaction Data) หมายถึงข้อมูลที่ผู้ให้บริการส่งให้แก่ผู้ให้บริการเพื่อประมวลผล แล้วตอบกลับผลการประมวลผลไปยังผู้ให้บริการ ในที่นี้หมายถึง Payload ของ TGIX Data Format



### 3 กฎหมายและแนวปฏิบัติที่เกี่ยวข้อง

#### 3.1 พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 [6]

มาตรา 13 ระบุว่าเพื่อประโยชน์ในการบริหารราชการแผ่นดินและการให้บริการประชาชน ให้หน่วยงานของรัฐจัดให้มีการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลที่มีการจัดทำและครอบครองตามที่หน่วยงานของรัฐแห่งอื่นร้องขอ ที่จะเกิดการบูรณาการร่วมกัน

มาตรา 15 ระบุว่า ให้มีศูนย์แลกเปลี่ยนข้อมูลกลางทำหน้าที่เป็นศูนย์กลางในการแลกเปลี่ยนข้อมูลดิจิทัล และทะเบียนดิจิทัลระหว่างหน่วยงานของรัฐ เพื่อสนับสนุนการดำเนินการของหน่วยงานของรัฐในการให้บริการประชาชนผ่านระบบดิจิทัล และดำเนินการในเรื่องดังต่อไปนี้

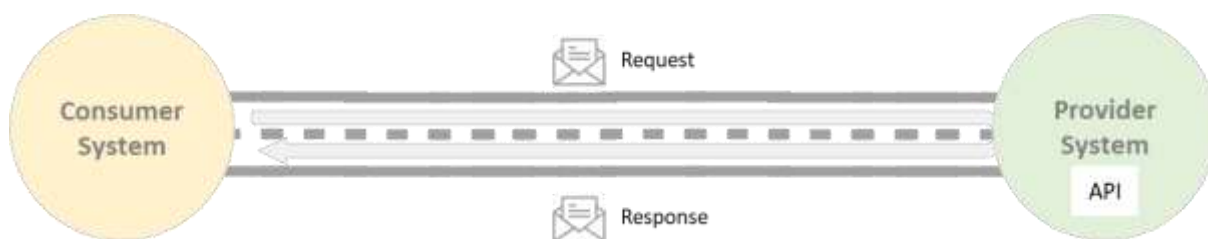
- (1) กำหนดนโยบายและมาตรฐานเกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลเสนอต่อคณะกรรมการพัฒนารัฐบาลดิจิทัลให้ความเห็นชอบ
- (2) ประสานและให้ความช่วยเหลือแก่หน่วยงานของรัฐในการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลระหว่างกัน รวมทั้งกำกับติดตามให้การดำเนินการดังกล่าวเป็นไปในแนวทางและมาตรฐานเดียวกันตามหลักเกณฑ์ 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 ภาพรวมของมาตรฐานสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ

มาตรฐานสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ (Thailand Government Information Exchange: TGIX) ฉบับนี้ มีแนวทางการจัดทำโดยคำนึงถึงความเหมาะสมกับบริบทด้านต่างๆ ของประเทศไทย กระบวนการเชื่อมโยงและแลกเปลี่ยนข้อมูล วิธีการการเชื่อมโยงและแลกเปลี่ยนข้อมูลกับระบบสารสนเทศที่เกี่ยวข้อง ความพร้อมในการดำเนินการของหน่วยงานเจ้าของระบบสารสนเทศ และความมั่นคงปลอดภัยในการเชื่อมโยงและแลกเปลี่ยนข้อมูล เป็นต้น

กระบวนการเชื่อมโยงและแลกเปลี่ยนข้อมูลดังกล่าว เป็นการการเชื่อมโยงและแลกเปลี่ยนข้อมูลผ่านทางช่องทาง Application Programming Interface หรือ API ซึ่งสร้างโดยระบบผู้ให้บริการ (Provider System) หน้าที่หลักของ API คือคอยรับคำขอ (Request) จากระบบผู้ใช้บริการ (Consumer System) เมื่อฝั่งระบบผู้ใช้บริการ API ส่งคำขอ จากนั้น API จะรับคำขอดังกล่าว นำไปประมวลผล และสรุปเป็นข้อมูลที่ตรงกับคำขอ และส่งข้อมูลเหล่านั้นกลับไปฝั่งระบบผู้ใช้บริการ API หรือเพื่อนำไปใช้งานต่อไป ดังรูปที่ 1



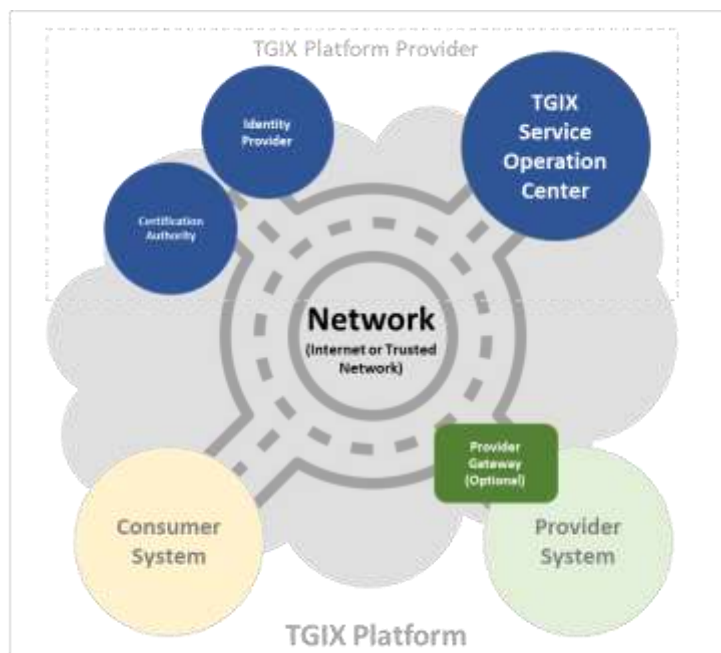
รูปที่ 1 ความหมายของ API

สถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ฉบับนี้ มีขอบเขตมาตรฐานที่ระดับการเชื่อมโยงข้อมูลเท่านั้น ไม่ได้ครอบคลุมถึงระดับการจัดการข้อมูลทางธุรกรรมของหน่วยงาน (Business Transaction Data) ที่เกิดขึ้นจากการเชื่อมโยงและแลกเปลี่ยนระหว่างกัน โดยในเล่มนี้จะมีการกล่าวถึงการเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในกลุ่ม TGIX (TGIX Intra-DX) ซึ่งเป็นมาตรฐานสถาปัตยกรรมสำหรับการแลกเปลี่ยนข้อมูลที่สมาชิกในกลุ่มดำเนินการตามมาตรฐาน TGIX มีรายละเอียดขององค์ประกอบต่างๆ ตลอดจนขั้นตอนการทำงานของแต่ละองค์ประกอบ และแนวทางการดำเนินการตามมาตรฐานฯ ของหน่วยงานเจ้าของระบบสารสนเทศ ในข้อที่ 5

## 5 มาตรฐานสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในกลุ่ม TGIX

### 5.1 ภาพรวมสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในกลุ่ม TGIX

มาตรฐานสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐภายในกลุ่ม TGIX-based Data Exchange (TGIX Intra-DX) มีองค์ประกอบหลักแยกตามบทบาทและหน้าที่ภายในกลุ่มได้แก่ ระบบผู้ให้บริการ (Provider System) ระบบผู้ใช้บริการ (Consumer System) และ ผู้ให้บริการ TGIX Platform (TGIX Platform Provider) ทุกองค์ประกอบหลักทำงานร่วมกันบนเครือข่ายอินเทอร์เน็ตหรือเครือข่ายเฉพาะที่หน่วยงานใช้เชื่อมโยงและแลกเปลี่ยนข้อมูล ดังรูปที่ 2

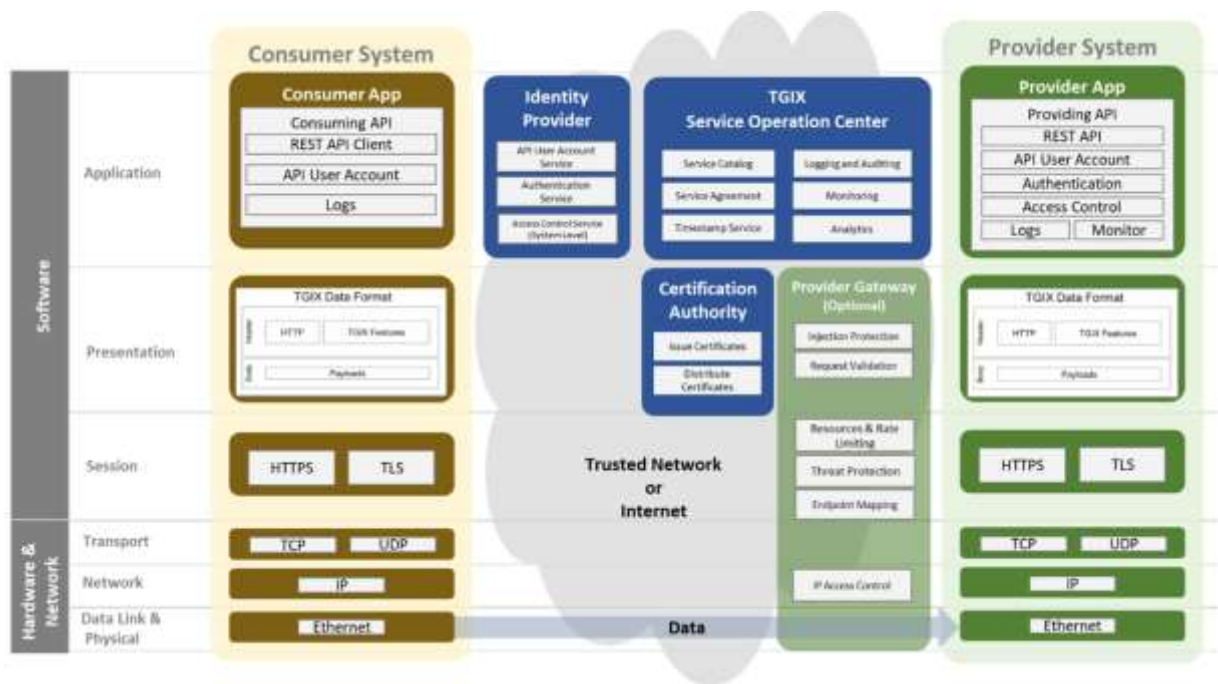


รูปที่ 2 แผนภาพสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐภายในกลุ่ม TGIX

- (1) ระบบผู้ให้บริการ (Provider System) คือระบบสารสนเทศของหน่วยงานที่เปิดให้บริการ API สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในแพลตฟอร์มที่ใช้มาตรฐาน TGIX ซึ่งประเภท API ที่กำหนดไว้เป็นมาตรฐานคือ Representational State Transfer (REST API หรือ RESTful API) [1] เป็นรูปแบบสถาปัตยกรรมซอฟต์แวร์สำหรับสร้าง Web Service API ผ่าน Hypertext Transfer Protocol (HTTP) โดยระบบผู้ให้บริการ สามารถรับคำขอและตอบกลับข้อมูลไปยังระบบผู้ใช้บริการได้ตามมาตรฐาน REST API ดังกล่าว
- (2) ระบบผู้ใช้บริการ (Consumer System) คือ ระบบสารสนเทศของหน่วยงานมีการใช้บริการ API สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในแพลตฟอร์มที่ใช้มาตรฐาน TGIX ด้วย Representational State Transfer (REST API หรือ RESTful API) โดยระบบผู้ใช้บริการ จะส่งคำขอรับบริการไปยัง Endpoint URL ที่ระบบผู้ให้บริการกำหนดไว้ และรับผลตอบกลับข้อมูลจากระบบผู้ให้บริการเพื่อนำไปประมวลผลตามความต้องการทางธุรกิจของผู้ใช้บริการ

(3) ผู้ให้บริการ TGIX Platform (TGIX Platform Provider) คือ ระบบสารสนเทศของหน่วยงานผู้ให้บริการ TGIX Platform เพื่อสนับสนุนการเชื่อมโยงและแลกเปลี่ยนข้อมูลให้เป็นไปตามมาตรฐาน TGIX โดยมีระบบอำนวยการกลางการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Service Operation Center: SOC) รวมทั้ง มีบริการพิสูจน์และยืนยันตัวตน (Identity Provider) และสนับสนุนการใช้ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) เพื่อใช้ในการยืนยันข้อความที่เป็นคำขอใช้บริการ และข้อความตอบกลับของผู้ให้บริการ

ระบบผู้ให้บริการ (Provider System), ระบบผู้ใช้บริการ (Consumer System) และ ผู้ให้บริการ TGIX Platform (TGIX Platform Provider) มีแนวทางดำเนินการดังข้อ 5.2 ข้อ 5.3 ข้อ 5.4 ตามลำดับ เพื่อการพัฒนา การบริหารจัดการและการควบคุมดูแลระบบสารสนเทศให้มีความปลอดภัย ถูกต้องเชื่อถือได้ และพร้อมใช้งานอยู่เสมอ เมื่อทุกองค์ประกอบหลักดำเนินการตามข้อ 5.2 ข้อ 5.3 ข้อ 5.4 เสร็จสิ้นแล้วจะมีองค์ประกอบย่อยดังรูปที่ 3



รูปที่ 3 แผนภาพแสดงโครงสร้างและความสัมพันธ์ระหว่างองค์ประกอบภายในกลุ่ม TGIX

## 5.2 แนวทางการดำเนินการของระบบผู้ให้บริการ (Provider System)

ระบบสารสนเทศของหน่วยงานที่ให้บริการ API มีแนวทางดำเนินการในการพัฒนา API ดังต่อไปนี้

- (1) ต้องดำเนินการพัฒนา API ประเภท Representational State Transfer (REST API หรือ RESTful API) ใช้สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในแพลตฟอร์มที่ใช้มาตรฐาน TGIX ด้วยลักษณะโครงสร้าง JavaScript Object Notation (JSON) [2] ตามรายละเอียดการออกแบบของข้อความ (TGIX Data Format) ดังตัวอย่างในบทที่ 6
- (2) ต้องดำเนินการพัฒนาองค์ประกอบอื่นๆ ของ API ตามเอกสารมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่องต่อไปนี้
  - ข้อกำหนดด้านการยืนยันตัวตน การกำหนดสิทธิ์ และบัญชีการใช้งาน
  - ข้อกำหนดด้านโปรโตคอลระดับแอปพลิเคชัน เอนพอยน์ การจัดการโทเคนและเซสชัน
  - ข้อกำหนดด้านความน่าเชื่อถือและความมั่นคงปลอดภัย
  - ข้อกำหนดด้านการตรวจสอบระบบและการลงบันทึกล็อก
  - ข้อกำหนดด้านการกำหนดชื่อและเนมสเปซ

เมื่อดำเนินการพัฒนา API แล้ว ระบบสารสนเทศของหน่วยงานที่ให้บริการ API จะมี REST API ที่ใช้ TGIX Data Format ทำงานอยู่บน HTTPS และมีองค์ประกอบอื่น ๆ ดังรูปที่ 4



รูปที่ 4 องค์ประกอบของระบบผู้ให้บริการ (Provider System)

- (3) เนื่องจากผู้ให้บริการ API ต้องเปิดให้บริการ API แก่ผู้ใช้บริการ API ที่อยู่ภายนอกหน่วยงานของตน ดังนั้นนอกจากต้องดำเนินการพัฒนา API ดังที่กล่าวไว้แล้ว หน่วยงานผู้ให้บริการ API

ต้องพิจารณาดำเนินการด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) ของระบบสารสนเทศผู้ให้บริการ API โดยเฉพาะเกี่ยวกับการป้องกันการโจมตี API แบบ Denial of Service (DoS) และ Distributed Denial of Service (DDoS) [3] จากผู้ให้บริการที่ไม่พึงประสงค์ ควรดำเนินการอย่างน้อยดังต่อไปนี้

- ควรดำเนินการป้องกันไม่ให้มีการส่ง SQL Query หรือ Command ต่างๆ ที่ไม่ต้องการผ่านส่วนต่างๆ ของ API เช่น URI Path, Query Param, Header, Form Param, Variable, XML Payload, หรือ JSON Payload เป็นต้น
- ควรดำเนินการตรวจสอบข้อมูลในคำขอ แล้วแจ้ง Response Code ที่เหมาะสมกลับไปให้ผู้ให้บริการ API ทราบ เช่น ตรวจสอบ HTTP Method ตรวจสอบ Content-Type ตรวจสอบ Resource ที่ไม่ถูกต้อง เป็นต้น
- ควรดำเนินการอนุญาตให้เฉพาะบางผู้ให้บริการ API หรือ เฉพาะ IP Address, Domain หรือ กลุ่มผู้ให้บริการเท่านั้นที่เรียกใช้ API ได้
- ควรดำเนินการป้องกันไม่ให้มีการโจมตี API จากผู้ใช้งานที่ไม่พึงประสงค์ ก่อนที่คำขอไปถึงยัง ระบบสารสนเทศที่ให้บริการ API
- ควรดำเนินการกำหนดจำนวนคำขอที่จะเรียกใช้ API โดยผู้ให้บริการ API เพื่อป้องกันการโจมตีจากผู้ให้บริการที่ไม่พึงประสงค์และลดโหลดของระบบสารสนเทศที่ให้บริการ API

นอกจากนี้ควรพิจารณาดำเนินการด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) ในเรื่องอื่นๆ เช่น OWASP API Security [4] เป็นต้น

หน่วยงานที่มีความพร้อมสูงในด้านงบประมาณและบุคลากรผู้ดูแลระบบสารสนเทศผู้ให้บริการ API ควรพิจารณาจัดหา API Gateway หรือสิ่งที่ทำหน้าที่ได้เทียบเท่า เพื่อดำเนินการเรื่องความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) ดังกล่าว

ส่วนหน่วยงานที่ติดข้อจำกัดด้านงบประมาณและบุคลากรผู้ดูแลระบบสารสนเทศผู้ให้บริการ API ควรพิจารณาดำเนินการร่วมกับหน่วยงานผู้ให้บริการ TGIX Platform ในการจัดหา API Gateway เพื่อช่วยดำเนินการเรื่องความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) ดังกล่าว

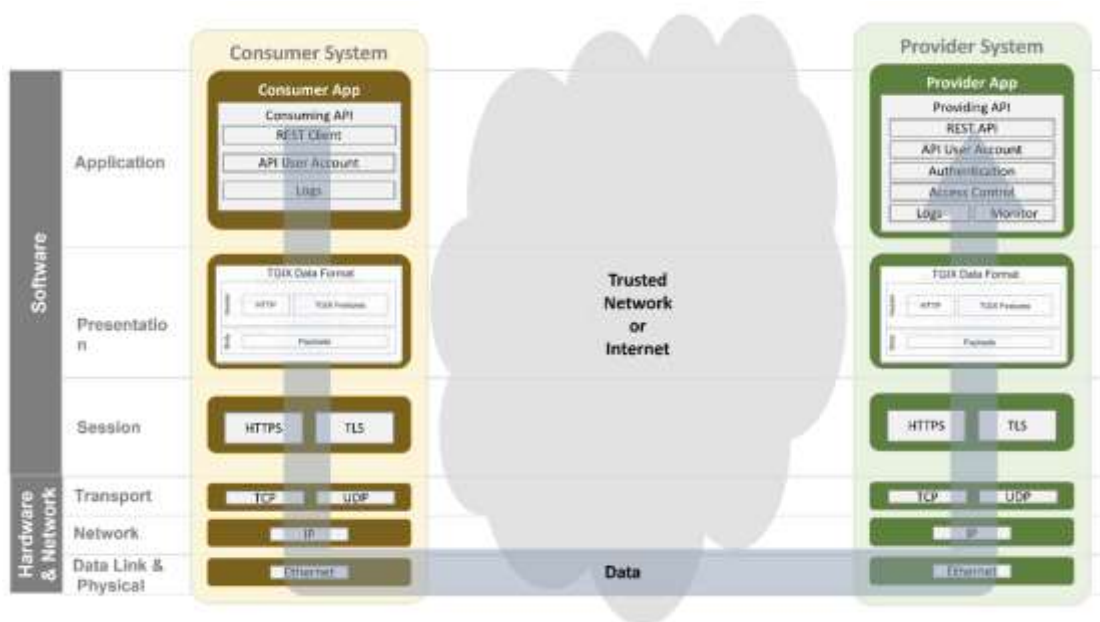
- (4) ต้องดำเนินการลงทะเบียน API พร้อมสร้างคู่มือการเรียกใช้งาน API ไว้ที่ Service Catalog ของ TGIX Service Operation Center (SOC) ซึ่งดูแลโดยผู้ให้บริการ TGIX Platform ตามขั้นตอนในหัวข้อ 5.5.3

### 5.3 แนวทางดำเนินการของระบบผู้ใช้บริการ (Consumer System)

ระบบสารสนเทศของหน่วยงานที่ใช้บริการ API มีแนวทางดำเนินการในการพัฒนา REST API Client ดังต่อไปนี้

- (1) ต้องดำเนินการทำข้อตกลงการใช้บริการ API (API Service Agreement) กับผู้ให้บริการ API ที่ TGIX Service Operation Center (SOC) ซึ่งดูแลโดยผู้ให้บริการ TGIX Platform พร้อมรับคู่มือการใช้งาน API จากผู้ให้บริการ API ตามขั้นตอนในหัวข้อ 5.5.4
- (2) ต้องดำเนินการพัฒนา REST API Client เพื่อเชื่อมกับ REST API ตามเอกสารคู่มือการใช้งาน API ที่ได้มาหลังจากทำข้อตกลงการใช้บริการ API
- (3) ต้องดำเนินการตามเอกสารมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่องต่อไปนี้
  - ข้อกำหนดด้านการยืนยันตัวตน การกำหนดสิทธิ์ และบัญชีการใช้งาน
  - ข้อกำหนดด้านโปรโตคอลระดับแอปพลิเคชัน เอนพอยน์ การจัดการโทเคนและเซสชัน
  - ข้อกำหนดด้านความน่าเชื่อถือและความมั่นคงปลอดภัย
  - ข้อกำหนดด้านการตรวจสอบระบบและการลงบันทึกล็อก
  - ข้อกำหนดด้านการกำหนดชื่อและเนมสเปซ

ผลลัพธ์ที่ได้จากการพัฒนา REST API Client เมื่อผู้ใช้บริการเรียกใช้บริการ API จะมีลักษณะการรับส่งข้อมูล ดังรูปที่ 5



## รูปที่ 5 การเรียกใช้บริการ API

### 5.4 แนวทางดำเนินการของผู้ให้บริการ TGIX Platform (TGIX Platform Provider)

ระบบสารสนเทศของผู้ให้บริการ TGIX Platform (TGIX Platform Provider) มีแนวทางดำเนินการในการให้บริการ TGIX Platform แบ่งได้เป็น 3 บริการหลักดังรูปที่ 6



รูปที่ 6 บริการของผู้ให้บริการ TGIX Platform

#### 5.4.1 การบริการพิสูจน์และยืนยันตัวตน (Identity Provider)

ผู้ให้บริการ TGIX Platform ต้องดำเนินการให้มีบริการของแพลตฟอร์มเพื่อพิสูจน์และยืนยันตัวตนทางดิจิทัลของบุคคลหรือหน่วยงานที่ต้องการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐด้วยมาตรฐาน OAuth 2.0 หรือ Open ID Connect มีบริการย่อย 3 ด้านคือ

- (1) บริการกำหนดบัญชีรายชื่อผู้ใช้งาน (API User Account Service)
- (2) บริการยืนยันตัวตนผู้ให้บริการ API (Authentication Service)
- (3) บริการตรวจสอบสิทธิ์ของผู้ให้บริการ API เพื่ออนุญาตให้เข้าถึง API (Access Control Service (System Level))

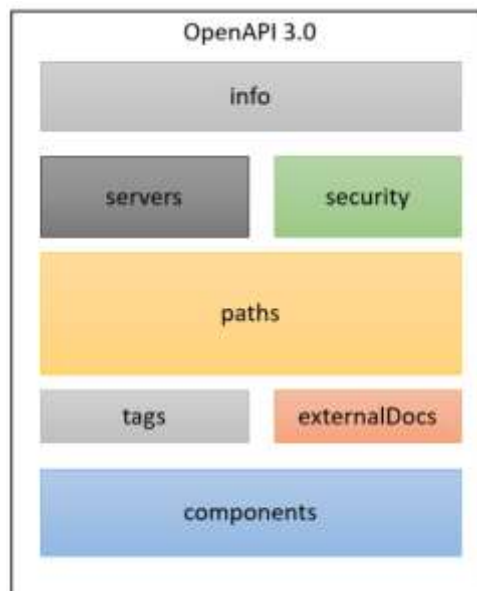
รายละเอียดขั้นตอนการดำเนินการให้บริการพิสูจน์และยืนยันตัวตน (Identity Provider) มีระบุในเอกสารมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่องข้อกำหนดด้านการยืนยันตัวตน การกำหนดสิทธิ์ และบัญชีการใช้งาน

#### 5.4.2 ระบบอำนวยการกลางการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Service Operation Center: SOC)

ผู้ให้บริการ TGIX Platform ต้องดำเนินการให้มีระบบอำนวยการกลางการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Service Operation Center: SOC) เพื่อใช้ในการจัดการและกำกับดูแลให้การเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐให้เป็นไปตามมาตรฐาน TGIX มีบริการย่อยดังต่อไปนี้



- (1) บริการรายชื่อของ API (Service Catalog) สำหรับแลกเปลี่ยนข้อมูลที่พร้อมใช้งานภายในแพลตฟอร์ม ซึ่ง API เกิดจากผู้ให้บริการมาลงทะเบียนข้อมูล API ได้แก่ชื่อ API, เวอร์ชันของ API และ Endpoint URL ไว้และอนุญาตให้สมาชิกในกลุ่ม TGIX ทำการค้นหาเพื่อเรียกดูรายชื่อของ API ได้ มาตรฐานการทำบริการรายชื่อของ API ที่แนะนำคือ OpenAPI Specification Version 3.0 [5]
- (2) บริการจัดทำข้อตกลง (Service Agreement) หรือสัญญา (Service Contract) ระหว่างผู้ให้บริการ (Provider) และผู้ใช้บริการ (Consumer) เป็นข้อมูลและเอกสารต่างๆ ที่เกี่ยวกับการใช้งาน API ที่ผู้ใช้บริการสามารถนำไปพัฒนาเป็น REST API Client ตามข้อ 5.3 ได้ ซึ่งโครงสร้างของการจัดทำข้อตกลง (Service Agreement) ซึ่งประกอบด้วยข้อมูลเพิ่มเติมจากการลงทะเบียนไว้ที่ Service Catalog ได้แก่ข้อมูลที่อยู่ของ Server ที่ให้บริการ ข้อมูลการยืนยันตัวตนและเอกสารต่างๆ ที่เกี่ยวกับการใช้งาน API ตาม OpenAPI Specification Version 3.0 [6] ดังรูปที่ 7



รูปที่ 7 โครงสร้างของข้อตกลงหรือสัญญาระหว่างผู้ให้บริการและผู้ใช้บริการ

ตัวอย่างข้อตกลงการให้บริการจาก SwaggerHub [7] ที่ใช้มาตรฐาน OpenAPI Specification Version 3.0 (OAS 3.0) แสดงในรูปที่ 8



รูปที่ 8 ตัวอย่างข้อตกลงการให้บริการ

- (3) บริการประทับรับรองเวลาอิเล็กทรอนิกส์ (Timestamp Service) โดยสามารถเชื่อมต่อกับ Time Stamping Authority (TSA) ใช้เพื่อประทับรับรองเวลาอิเล็กทรอนิกส์ ในการลงลายมือชื่อดิจิทัล (Digital Signature) รวมทั้งเพื่อสร้างความเชื่อมั่นและรับรองในเวลาในการเชื่อมโยงและแลกเปลี่ยนข้อมูล
- (4) บริการจัดเก็บ Log (Logging and Auditing) ที่เกิดจากการเชื่อมโยงและแลกเปลี่ยนข้อมูลของกลุ่ม รายละเอียดการดำเนินการตามเอกสารมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่องข้อกำหนดของการตรวจสอบระบบและการลงบันทึกล็อก
- (5) บริการตรวจสอบและวิเคราะห์ผลการตรวจสอบระบบ (Monitoring and Analytics) เป็นการนำเทคนิคของการค้นหาและวิเคราะห์จากข้อมูล Log แล้วนำผลไปแสดงผลในลักษณะแผนภูมิรูปภาพ รวมทั้งแจ้งเตือนให้กับผู้ให้บริการและผู้ใช้บริการทราบถึงปัญหาที่เกิดขึ้น รายละเอียดการดำเนินการตามเอกสารมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านการเชื่อมโยงข้อมูล เรื่องข้อกำหนดของการตรวจสอบระบบและการลงบันทึกล็อก

#### 5.4.3 การบริการออกใบรับรอง (Certification Authority)

ในการออกใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) ผู้ให้บริการ TGIX Platform สามารถที่จะดำเนินการให้มีการบริการออกใบรับรองเป็นหน่วยงาน Certification Authority เพื่อใช้ในการลงลายมือชื่ออิเล็กทรอนิกส์ยืนยันความถูกต้องของข้อความคำขอใช้บริการ และข้อความตอบกลับจากผู้ให้บริการ ทั้งนี้ขึ้นอยู่กับความพร้อมของหน่วยงาน โดยหน่วยงานสามารถเลือกดำเนินการได้ดังนี้

- (1) หน่วยงานผู้ให้บริการ TGIX Platform เลือกให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) จากหน่วยงานออกใบรับรองที่เป็นไปตามมาตรฐานสากล สำหรับใช้ในกระบวนการ

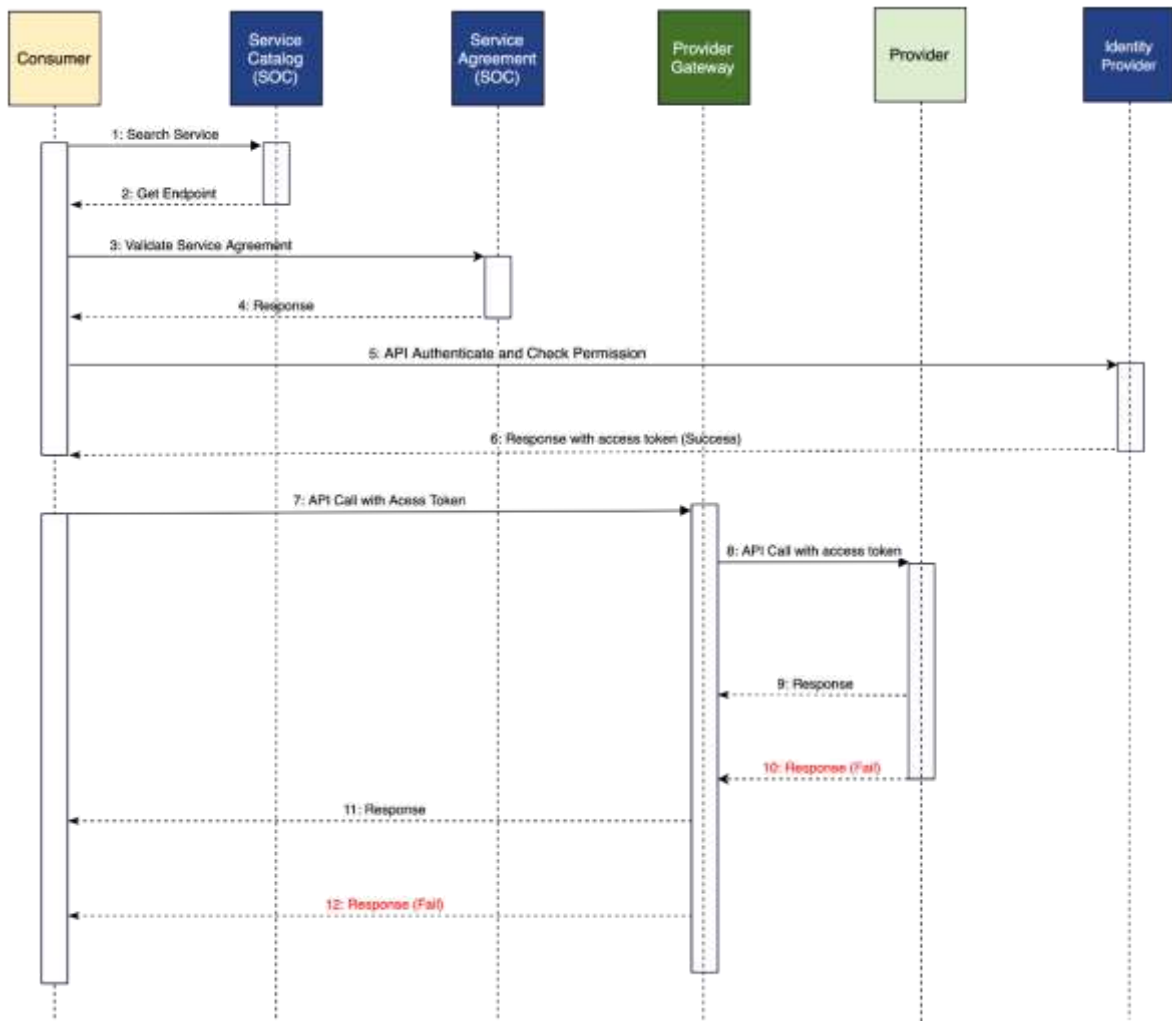
ยืนยันความถูกต้องของข้อความคำขอใช้บริการ และข้อความตอบกลับจากผู้ให้บริการ สำหรับหน่วยงานที่เข้ามาใช้บริการผ่าน TGIX Platform นี้

- (2) หน่วยงานผู้ให้บริการ TGIX Platform เลือกใช้ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) ที่สร้างขึ้นด้วยตัวเอง ตามกระบวนการของหน่วยงาน (Self-Signed) เพื่อใช้ในกระบวนการยืนยันความถูกต้องของข้อความคำขอใช้บริการ และข้อความตอบกลับจากผู้ให้บริการ ตัวใบรับรองนี้เป็นทางเลือกที่มีความน่าเชื่อถือสำหรับหน่วยงานที่ใช้บริการผ่าน TGIX Platform นี้

## 5.5 ขั้นตอนการทำงานขององค์ประกอบภายในกลุ่ม TGIX

### 5.5.1 การเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในกลุ่ม TGIX (TGIX Intra-DX)

รูปที่ 9 แสดงการทำงานแบบลำดับปฏิสัมพันธ์ (Sequence Diagram) ของการแลกเปลี่ยนข้อมูลภายในกลุ่ม TGIX แสดงถึงลำดับขั้นตอนการทำงานขององค์ประกอบต่างๆ สำหรับการแลกเปลี่ยนข้อมูลกันภายในแพลตฟอร์มที่ใช้มาตรฐาน TGIX



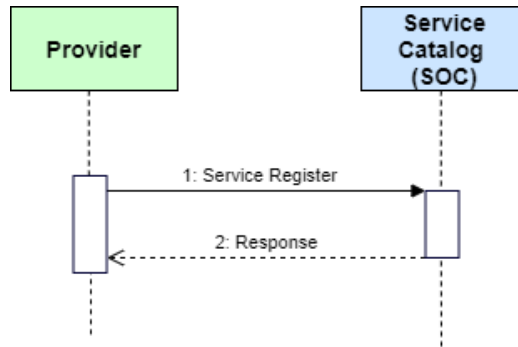
รูปที่ 9 แผนภาพแสดงการทำงานแบบลำดับปฏิสัมพันธ์ (Sequence Diagram) ของการแลกเปลี่ยนข้อมูลภายในกลุ่ม TGIX

ตารางที่ 1 อธิบายขั้นตอนการทำงานของการทำงานของการแลกเปลี่ยนข้อมูลภายในกลุ่ม TGIX

หมายเลข	จาก Object	ไปยัง Object	คำอธิบาย
1	Consumer	Service Catalog	ผู้ให้บริการ API ค้นหาบริการที่ต้องการที่ Service Catalog
2	Service Catalog	Consumer	Service Catalog ส่งข้อมูล Endpoint กลับไปยังผู้ให้บริการ API
3	Consumer	Service Agreement	ผู้ให้บริการ API ทำการตรวจสอบสิทธิ์ตามข้อตกลงการใช้บริการ (Agreement) ไปยัง Service Agreement
4	Service Agreement	Consumer	Service Agreement ส่งผลการตรวจสอบสิทธิ์ตามข้อตกลงใช้บริการ (Agreement) กลับไปยังผู้ให้บริการ API
5	Consumer	Identity Provider	ผู้ให้บริการ API ทำการยืนยันตัวตน (Authentication) และตรวจสอบสิทธิ (Authorization) ไปยัง Identity Provider
6	Identity Provider	Consumer	(กรณีการยืนยันตัวตนและสิทธิสำเร็จ) Identity Provider ตอบผลการยืนยันตัวตนพร้อมทั้งส่ง Access Token กลับไปให้ผู้ให้บริการ API
7	Consumer	Provider Gateway	ผู้ให้บริการ API เรียกใช้งานผ่าน API ไปยัง Provider Gateway พร้อมทั้งส่ง Access Token ไปด้วย
8	Provider Gateway	Provider Gateway	Provider Gateway ส่งต่อการเรียกใช้งานผ่าน API ไปยัง Provider พร้อมทั้งส่ง Access Token ไปด้วย
9	Provider Gateway	Provider Gateway	Provider ตอบกลับการเรียกใช้ API กลับไปยัง Provider Gateway
10	Provider Gateway	Provider Gateway	(กรณีการยืนยันตัวตนและสิทธิไม่สำเร็จ) Provider ตอบผลการตรวจสอบ Access Token กลับไปยัง Provider Gateway
11	Provider Gateway	Consumer	Provider Gateway ส่งต่อผลการเรียกใช้ API ไปยัง Consumer
12	Provider Gateway	Consumer	(กรณีการยืนยันตัวตนและสิทธิไม่สำเร็จ) Provider Gateway ตอบผลการตรวจสอบ Access Token กลับไปยัง Consumer

### 5.5.2 การลงทะเบียน API ของผู้ให้บริการ API ที่ TGIX Platform

รูปที่ 10 แสดงการทำงานแบบลำดับปฏิสัมพันธ์ (Sequence Diagram) ของการลงทะเบียนบริการสำหรับแลกเปลี่ยนข้อมูลภายในกลุ่ม TGIX ของผู้ให้บริการ API แสดงถึงลำดับขั้นตอนการทำงานขององค์ประกอบต่างๆ สำหรับการลงทะเบียนบริการสำหรับแลกเปลี่ยนข้อมูลภายในแพลตฟอร์มที่ใช้มาตรฐาน TGIX



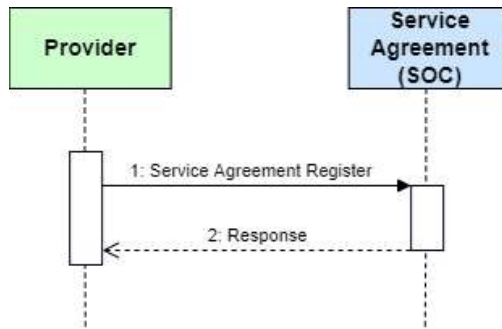
รูปที่ 10 แผนภาพแสดงการทำงานแบบลำดับปฏิสัมพันธ์ (Sequence Diagram) ของการลงทะเบียนบริการสำหรับแลกเปลี่ยนข้อมูลภายในกลุ่ม TGIX ของผู้ให้บริการ API

ตารางที่ 2 อธิบายขั้นตอนการทำงานของลงทะเบียนและสร้างรายการบริการของผู้ให้บริการ API

หมายเลข	จาก Object	ไปยัง Object	คำอธิบาย
1	Provider	Service Catalog (SOC)	ผู้ให้บริการ API ลงทะเบียนไปยัง Service Catalog (SOC)
2	Service Catalog (SOC)	Provider	Service Catalog (SOC) ตอบผลการลงทะเบียนกลับไปยังผู้ให้บริการ API

### 5.5.3 การทำข้อตกลงการให้บริการของผู้ให้บริการ API

รูปที่ 11 แสดงการทำงานแบบลำดับปฏิสัมพันธ์ (Sequence Diagram) ของการลงทะเบียนข้อตกลงการให้บริการสำหรับแลกเปลี่ยนข้อมูลภายในกลุ่ม TGIX ของผู้ให้บริการ API แสดงถึงลำดับขั้นตอนการทำงานขององค์ประกอบต่างๆ สำหรับการลงทะเบียนข้อตกลงการให้บริการของผู้ให้บริการ API ภายในแพลตฟอร์มที่ใช้มาตรฐาน TGIX



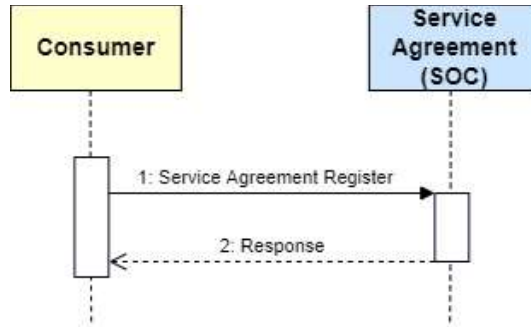
รูปที่ 11 แผนภาพแสดงการทำงานแบบลำดับปฏิสัมพันธ์ (Sequence Diagram) ของการลงทะเบียนข้อตกลงการให้บริการสำหรับแลกเปลี่ยนข้อมูลภายในกลุ่ม TGIX ของผู้ให้บริการ API

ตารางที่ 3 อธิบายขั้นตอนการทำงานของลงทะเบียนข้อตกลงให้บริการ

หมายเลข	จาก Object	ไปยัง Object	คำอธิบาย
1	Provider	Service Catalog (SOC)	ผู้ให้บริการ API ลงทะเบียนไปยัง Service Agreement (SOC)
2	Service Agreement (SOC)	Provider	Service Agreement (SOC) ตอบผลการลงทะเบียนกลับไปผู้ให้บริการ API

#### 5.5.4 การทำข้อตกลงการใช้บริการของผู้ใช้บริการ API

รูปที่ 12 แสดงการทำงานแบบลำดับปฏิสัมพันธ์ (Sequence Diagram) ของการลงทะเบียนข้อตกลงการใช้บริการสำหรับการแลกเปลี่ยนข้อมูลภายในกลุ่ม TGIX ของผู้ใช้บริการ API แสดงถึงลำดับขั้นตอนการทำงานขององค์ประกอบต่างๆ สำหรับการลงทะเบียนข้อตกลงการใช้บริการของผู้ใช้บริการ API ภายในแพลตฟอร์มที่ใช้มาตรฐาน TGIX



รูปที่ 12 แผนภาพแสดงการทำงานแบบลำดับปฏิสัมพันธ์ (Sequence Diagram) ของการลงทะเบียนข้อตกลงการใช้บริการสำหรับการแลกเปลี่ยนข้อมูลภายในกลุ่ม TGIX ของผู้ใช้บริการ API

ตารางที่ 4 อธิบายขั้นตอนการทำงานของการลงทะเบียนข้อตกลงใช้บริการ

หมายเลข	จาก Object	ไปยัง Object	คำอธิบาย
1	Consumer	Service Catalog (SOC)	ผู้ใช้บริการ API ลงทะเบียนไปยัง Service Agreement (SOC)
2	Service Agreement (SOC)	Consumer	Service Agreement (SOC) ตอบผลการลงทะเบียนกลับไปยังผู้ใช้บริการ API



## 6 รูปแบบข้อความตามมาตรฐาน TGIX (JSON Data Format)

บทนี้ให้ครอบคลุมหัวข้อการออกแบบรูปแบบข้อความ (TGIX Data Format) ในลักษณะ JSON หรือ TGIX Data Format เพื่อใช้ในเป็นข้อกำหนดของข้อความที่ใช้รับส่งตามมาตรฐาน TGIX โดยใช้มุมมองทางสถาปัตยกรรมเพื่ออธิบายโครงสร้างรูปแบบข้อความ รวมถึงวิธีการใช้งานรับส่งข้อความระหว่างผู้ให้บริการและผู้ใช้บริการ

### 6.1 แนวคิดในการออกแบบ

แนวคิดในการออกแบบรูปแบบข้อความตามมาตรฐาน TGIX คือ

- (1) รูปแบบข้อความ พัฒนาโดยอิงจาก RFC-7159 [2] “The JavaScript Object Notation (JSON) Data Interchange Format” ซึ่งเป็นฟอร์แมตสำหรับการแลกเปลี่ยนข้อมูลระหว่างคอมพิวเตอร์ เนื่องจาก JSON นั้นอยู่ในรูปข้อความธรรมดา (Plain Text) โปรแกรมคอมพิวเตอร์และมนุษย์สามารถอ่านเข้าใจได้ และได้รับความนิยมในการใช้งานในช่วงที่ได้มีการจัดทำมาตรฐาน TGIX
- (2) โครงสร้างรูปแบบข้อความจะต้องรองรับการรับส่งข้อมูลรูปแบบ XML เนื่องจากมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ เปิดกว้างให้กับผู้ให้บริการที่มีความต้องการเชื่อมโยงข้อมูลผ่านมาตรฐาน TGIX ได้ โดยมีการแก้ไขระบบที่พัฒนาอยู่เดิมให้น้อยที่สุด หรือมีการแก้ไขดัดแปลงฟังก์ชันการทำงานบางอย่างก็สามารถเชื่อมโยงข้อมูลตามมาตรฐาน TGIX ได้

### 6.2 รูปแบบของข้อความ (TGIX Data Format)

ส่วนของการออกแบบโครงสร้างข้อความที่ใช้รับส่งระหว่างผู้ให้บริการและผู้ให้บริการ ตามมาตรฐาน TGIX นั้นมีการกำหนดให้ใช้ JSON เป็นข้อความสำหรับรับส่งข้อมูล พัฒนาโดยอิงจาก RFC-7159[2] “The JavaScript Object Notation (JSON) Data Interchange Format” เนื้อหาในส่วนนี้จะกล่าวถึงรายละเอียดของตัวข้อความมีดังต่อไปนี้

#### 6.2.1 ข้อกำหนดเฮดเดอร์ของ Protocol

- (1) กำหนด Content Type ให้มีค่าเป็น “application/json” สำหรับการรับส่งข้อมูลที่ทั้งผู้ให้บริการและผู้ให้บริการใช้งาน JSON
- (2) กำหนด Content Type ให้มีค่าเป็น “multipart/related” สำหรับการรับส่งข้อมูลที่ทั้งผู้ให้บริการและผู้ให้บริการใช้งาน JSON เฉพาะกรณีที่มีการแนบไฟล์ไปด้วย
- (3) กำหนด Content Type ให้มีค่าเป็น “multipart/related” สำหรับการรับส่งข้อมูลที่ผู้ให้บริการใช้งาน XML และกรณีที่มีไฟล์แนบ
- (4) กำหนด Content Type ให้มีค่าเป็น “application/json” สำหรับการรับส่งข้อมูลที่ผู้ให้บริการใช้งาน JSON แต่ผู้ให้บริการใช้งาน XML

- (5) กำหนด Content Type ให้มีค่าเป็น “multipart/related” สำหรับการรับส่งข้อมูลจากผู้ให้บริการใช้งาน JSON แต่ผู้ใช้บริการใช้งาน XML กรณีที่มีการส่งไฟล์แนบ

## 6.2.2 ข้อกำหนดบอดี้ของ Protocol

กำหนดแบ่งออกเป็น 3 ส่วนหลัก ๆ คือ

- (1) ส่วนของเฮดเดอร์ (TGIX Message Header)

เป็นส่วนจะเป็นส่วนที่ระบุถึงรายละเอียดต่างๆ ที่จำเป็นสำหรับการรับส่งข้อมูลและการเก็บ Log โดยมีรายละเอียดดังนี้

ตารางที่ 5 อธิบายรายละเอียดโครงสร้างของ TGIX Message Headers ส่วน HTTP Header

ชื่อข้อมูล	ความจำเป็น	รายละเอียด
HTTP Method	(จำเป็นต้องมี)	กำหนด HTTP Method โดยรองรับ HTTP/1.1 [3]และโดยรองรับกำหนดค่าเป็น POST, GET, DELETE, PUT, OPTIONS และ PATCH
Authorization	(จำเป็นต้องมี)	กำหนดรหัสการยืนยันตัวตนของผู้ใช้งาน โดยกำหนดค่าเป็น Bearer เสมอ
Accept-Encoding	(จำเป็นต้องมี)	กำหนดการเข้ารหัสข้อมูล
Accept-Language	(จำเป็นต้องมี)	กำหนดภาษาในการตอบรับ
Accept	(จำเป็นต้องมี)	กำหนดประเภทของเนื้อหา
Host	(จำเป็นต้องมี)	กำหนด URL ปลายทาง
Cache-Control	(จำเป็นต้องมี)	กำหนดคำสั่งชี้แนะว่าจะต้องทำตามกลไกการเก็บแคชทั้งหมด โดยตลอดทั้งการร้องขอและการตอบรับ
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
TGIX-Request-Id	(จำเป็นต้องมี)	กำหนดรหัสของการร้องขอสำหรับตอบกลับ
TGIX- Certificate	(จำเป็นต้องมี)	กำหนด Public Key ของลายมือชื่อดิจิทัล

ตารางที่ 5 อธิบายรายละเอียดโครงสร้างของ TGIX Message Headers ส่วน HTTP Header

ชื่อข้อมูล	ความจำเป็น	รายละเอียด
TGIX-Signature-Value	(จำเป็นต้องมี)	กำหนดกุญแจที่ใช้ในการลงลายมือชื่อดิจิทัล
X-API-KEY	(ตัวเลือก)	กำหนดรหัสของ API
TGIX-Event	(ตัวเลือก)	กำหนดรายละเอียดการที่จะดำเนินการ (Action)
TGIX-Expiration-Timestamp	(ตัวเลือก)	กำหนดเวลาที่หมดอายุของข้อความ
TGIX-Message-Version	(ตัวเลือก)	กำหนดวิธีการจัดการข้อความคนละแบบ

(2) ส่วนของเพโหลด (TGIX Message Payload)

ข้อความในส่วนนี้จะเป็นข้อความที่รับส่งกันระหว่างผู้ให้บริการเป็นผู้กำหนดรูปแบบตามมาตรฐาน TGIX เปิดให้เป็นไปตามรูปแบบของเซอร์วิสของผู้ให้บริการ และต้องเป็นฟอร์แมต JSON ในกรณีที่ผู้ให้บริการมีการใช้งานฟอร์แมตแบบ XML ผู้ขอใช้บริการจะต้องทำการส่งข้อความ XML นั้นภายใต้รูปแบบของ multipart/form-data หรือ multipart/related

(3) ส่วนของลายมือชื่อ (TGIX Message Signature)

มาตรฐาน TGIX กำหนดให้ต้องมีการลงลายมือชื่อดิจิทัลที่เชื่อถือได้ โดยการทำงานในส่วนนี้ของฟังก์ชันในการร้องขอใช้บริการ จะต้องมีการลงลายมือชื่อดิจิทัล (Digital Signature) กับข้อความที่รับส่งระหว่างผู้ให้บริการและผู้ใช้บริการ ทุกครั้งที่มีการร้องขอใช้บริการ โดยหลักการลงลายมือชื่อนั้นให้เป็นไปตามขั้นตอนการลงลายมือชื่อดิจิทัลที่อาศัยหลักการโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure: PKI) โดยใช้ข้อมูลส่วนของเฮดเดอร์และเพโหลดมาทำการลงลายมือชื่อดิจิทัล รายละเอียดของข้อความที่ต้องระบุในส่วนนี้คือ

ตารางที่ 6 อธิบายรายละเอียดส่วนของลายมือชื่อ (Signature)

ชื่อข้อมูล	ความจำเป็น	รายละเอียด
TGIX-Alg	(จำเป็นต้องมี)	อัลกอริทึม (Algorithm) สำหรับลงลายมือชื่อดิจิทัล ตามข้อกำหนดด้านความปลอดภัยของ TGIX
TGIX- Certificate	(จำเป็นต้องมี)	ใบรับรองที่ใช้งาน
TGIX-Message-Version	(จำเป็นต้องมี)	ข้อมูลลายมือชื่ออิเล็กทรอนิกส์

## 6.3 ตัวอย่างข้อความตามมาตรฐาน TGIX

### 6.3.1 ตัวอย่างข้อความที่กำหนด Content Type มีค่าเป็น “application/json”

ตัวอย่างข้อความ ที่กำหนด Content Type มีค่าเป็น “application/json” ใช้สำหรับการรับส่งข้อมูล ที่ทั้งผู้ให้บริการและผู้ให้บริการใช้งาน JSON และสำหรับการรับส่งข้อมูลจากผู้ให้บริการใช้งาน JSON แต่ผู้ให้บริการใช้งาน XML

```
1 //=====
2 //          Request Header
3 //=====
4 [POST, GET ,DELETE ,OPTIONS, PATCH ] https://tgixp01-sandbox.dga.or.th/api/v4/person
5 Request Method: POST
6 Accept: application/json, text/plain, */* */
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9,th;q=0.8
9 Authorization: Bearer xxxxxxxx xxxxxx xx
10 Connection: keep-alive
11 Content-Length: 49
12 Content-Type: application/json
13 Host: [Domain Name]
14 Origin: [URL : Domain Name]
15 Referer: [URL : Domain Name]
16 TGIX-Alg: RSA-SHA256
17 TGIX-Certificate: [certificate]
18 TGIX-Client-Id: 12345
19 TGIX-Message-Id: 400f0344-905e-45b9-b63e-77c3218c21ad
20 TGIX-Request-Id: c350da99-7aeb-4577-a09f-5e7cc10d510c
21 TGIX-Signature-Value: [object Object]
22 TGIX-Timestamp: 2023-03-14T02:08:10.239Z
23
24 // =====
25 //          Message Payload
26 // =====
27
28 {
29 |   | "juristicID": "0133552005772"
30 }
```

รูปที่ 13 ตัวอย่างข้อความ ที่กำหนด Content Type ให้มีค่าเป็น “application/json”

### 6.3.2 ตัวอย่างข้อความที่กำหนด Content Type มีค่าเป็น “multipart/related”

ตัวอย่างข้อความ ที่กำหนด Content Type มีค่าเป็น “multipart/related” สำหรับการรับส่งข้อมูล ที่ทั้งผู้ให้บริการและผู้ให้บริการใช้งาน JSON เฉพาะกรณีที่มีการแนบไฟล์ไปด้วย การรับส่งข้อมูลจากผู้ให้บริการ

ใช้งาน XML และกรณีที่มีไฟล์แนบ และการรับส่งข้อมูลให้ผู้ให้บริการใช้งาน JSON แต่ผู้ใช้บริการใช้งาน XML กรณีที่มีการส่งไฟล์แนบ

```
1 //=====
2 //          Request Header
3 //=====
4 POST /api/v4/person/person-upload HTTP/1.1
5 Request Method: POST
6 Accept: application/json, text/plain, */*
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9,th;q=0.8
9 Authorization: Bearer xxxxxxxx xxxxxx xx xxxc xxcxcxcxxx
10 Connection: keep-alive
11 Content-Length: 4515
12 Content-Type: multipart/form-data; boundary=----WebKitFormBoundary7MA4YWxkTrZu0gW
13 Host: [Domain Name]
14 Origin: [URL : Domain Name]
15 Referer: [URL : Domain Name]
16 TGIX-Alg: RSA-SHA256
17 TGIX-Certificate: [certificate]
18 TGIX-Client-Id: 12345
19 TGIX-Message-Id: 3183c52c-60a5-11ed-9b6a-0242ac120002
20 TGIX-Request-Id: c350da99-7aeb-4577-a09f-5e7cc10d510c
21 TGIX-Signature-Value: [signature]
22 TGIX-Timestamp: 2023-03-14T02:08:10.239Z
23 //=====
24 //          Request Header
25 //=====
26 ----WebKitFormBoundary7MA4YWxkTrZu0gW
27 Content-Disposition: form-data; name=""; filename="person_image1.png"
28 Content-Type: image/png
29
30 (data)
31 ----WebKitFormBoundary7MA4YWxkTrZu0gW
32 Content-Disposition: form-data; name=""
33 Content-Type: application/json
34
35 { "cd:PersonID": "1767400297581" }
36 ----WebKitFormBoundary7MA4YWxkTrZu0gW
37 Content-Disposition: form-data; name=""; filename="person-295.png"
38 Content-Type: image/png
39
40 (data)
41 ----WebKitFormBoundary7MA4YWxkTrZu0gW
```

รูปที่ 14 ตัวอย่างข้อความ ที่กำหนด Content Type ให้มีค่าเป็น “multipart/related”

## 6.4 กรณีการใช้งานที่ผู้ให้บริการสามารถเลือกดำเนินการ

### 6.4.1 กรณีการใช้งานเพื่อแลกเปลี่ยนข้อมูลเชิงธุรกรรม

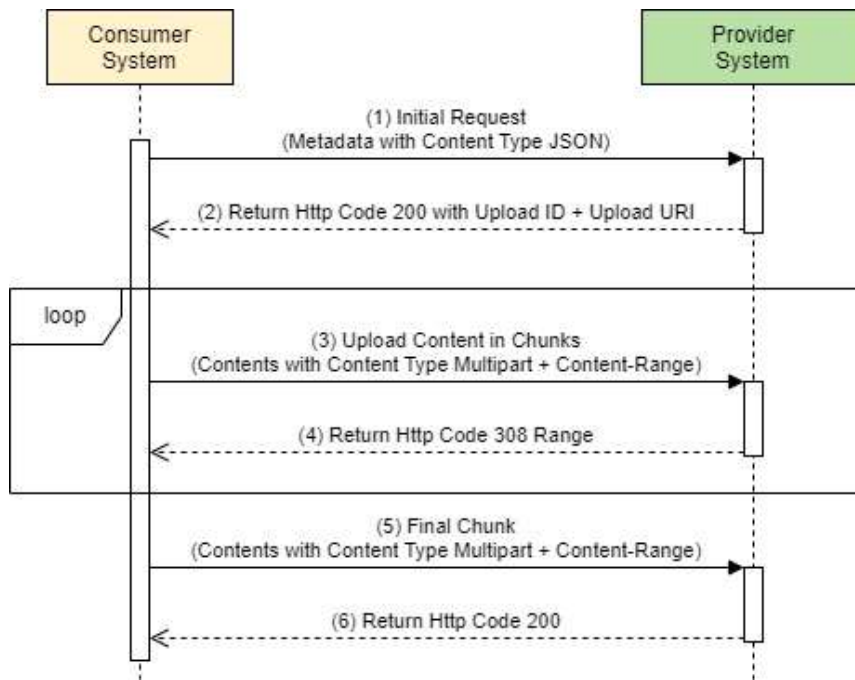
แบ่งย่อยได้เป็น 2 กรณี คือ

- (1) กรณีข้อมูลเชิงธุรกรรมมีข้อความที่รูปแบบข้อมูลมีลักษณะ JSON ทั้งข้อความ ในกรณีนี้ผู้ให้บริการสามารถดำเนินการกำหนด Content Type มีค่าเป็น “application/json” ตามตัวอย่างในหัวข้อ 6.3.1
- (2) กรณีข้อมูลเชิงธุรกรรมมีข้อความที่รูปแบบข้อมูลมีลักษณะอื่นๆ เช่น XML, ebXML เป็นต้น ทำให้มาตรฐาน TGIX ทำงานร่วมกับ Data Format อื่นๆ ได้ด้วย ในกรณีนี้ผู้ให้บริการสามารถดำเนินการกำหนด Content Type มีค่าเป็น “multipart/related” หรือ “multipart/form-data” ตามตัวอย่างในหัวข้อ 6.3.2

### 6.4.2 กรณีการใช้งานเพื่อแลกเปลี่ยนข้อมูลที่เป็นไฟล์

แบ่งย่อยได้เป็น 2 กรณี คือ

- (1) กรณีข้อมูลที่เป็นไฟล์มีขนาดไม่เกิน 5 เมกะไบต์ กรณีนี้รูปแบบข้อมูลมีลักษณะเป็น ไฟล์ขนาดไม่เกิน 5 เมกะไบต์ ซึ่งสามารถส่งร่วมกับข้อความประเภทต่างๆ เช่น JSON, XML, ebXML เป็นต้น ไปพร้อมกับไฟล์ได้ ผู้ให้บริการสามารถกำหนด Content Type มีค่าเป็น “multipart/related” หรือ “multipart/form-data” ตามตัวอย่างในหัวข้อ 6.3.2
- (2) กรณีข้อมูลที่เป็นไฟล์มีขนาดเกิน 5 เมกะไบต์ ในกรณีนี้ ผู้ให้บริการสามารถกำหนด Content Type มีค่าเป็น “multipart/related” ตามตัวอย่างในหัวข้อ 6.3.2 สิ่งที่แตกต่างกันคือการส่งไฟล์นั้น จะต้องทำการแบ่งไฟล์ออกเป็นส่วน ๆ แล้วทำการส่งส่วนต่าง ๆ ไปผ่าน multipart จนกว่าจะครบทุกส่วน โดยสามารถอาศัย “attachments.sequence” เป็นตัวกำหนดลำดับของข้อมูลที่ส่ง ตัวอย่างการทำงานดังรูปที่ 15



รูปที่ 15 แสดงตัวอย่างการทำงานสำหรับการส่งไฟล์ขนาดใหญ่

จากรูปที่ 15 ตัวอย่างการทำงานสำหรับการส่งไฟล์ขนาดใหญ่ มีแนวทางดังต่อไปนี้

- (1) ผู้ใช้บริการแจ้งว่าจะมีการส่งข้อมูลลักษณะไฟล์โดยแจ้งชื่อไฟล์พร้อมขนาดของไฟล์ไปยังผู้ให้บริการ
- (2) ผู้ให้บริการตอบกลับพร้อมแจ้งเลขที่อ้างอิงการส่งไฟล์ขนาดใหญ่ (Upload ID) และ URI สำหรับการส่งไฟล์ขนาดใหญ่กลับไปยังผู้ให้บริการ
- (3) ผู้ใช้บริการเริ่มทำการแบ่งไฟล์เป็นชิ้นย่อย ๆ โดยขนาดไม่ควรเกิน 5 เมกะไบต์ และส่งข้อมูลโดยกำหนด Content Type ให้มีค่าเป็น “multipart/related” จากนั้นใน Part ของข้อมูล Binary ให้กำหนด Content Type ให้มีค่าเป็น “multipart/byteranges; boundary=เลขที่อ้างอิงการส่งไฟล์ขนาดใหญ่” ตัวอย่างแสดงดังรูปที่ 16

```
// =====
// Request Header
// =====
HTTP/1.1 206 Partial Content
Content-Type: multipart/byteranges; boundary=เลขอ้างอิงการส่งไฟล์ขนาดใหญ่
Content-Length: <size>

--เลขอ้างอิงการส่งไฟล์ขนาดใหญ่
Content-Range: <unit> <range-start>-<range-end>/<size>
Content-Length: <range>

<<Binary Data length <range> >>
--เลขอ้างอิงการส่งไฟล์ขนาดใหญ่--
```

รูปที่ 16 การกำหนดค่าสำหรับ part ที่เป็นข้อมูล binary

- (4) แต่ครั้งที่ผู้ให้บริการได้รับไฟล์จะทำการตรวจสอบขนาดที่ได้รับจริงเทียบกับขนาดที่ผู้ใช้บริการแจ้งไว้ พร้อมทั้งส่งกลับ Http Code 308 Range
- (5) ผู้ใช้บริการดาวน์โหลดไฟล์ไปยังผู้ให้บริการผ่าน Upload URI ที่ได้ในขั้นตอนที่ 2 ถึงไฟล์สุดท้าย
- (6) ผู้ให้บริการทำการตรวจสอบถึงความครบถ้วนของไฟล์ที่ได้รับจริงเทียบกับขนาดที่ผู้ใช้บริการแจ้งไว้ หากถูกต้องครบถ้วนจะส่งกลับ Http Code 200 กลับไปให้ผู้ใช้บริการ

นอกจากมาตรฐานสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในกลุ่มหรือแพลตฟอร์ม TGIX (TGIX-Intra-DX) แล้ว ยังมีมาตรฐานสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลแบบอื่นๆ อีก เช่น มาตรฐานสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างกลุ่มหรือแพลตฟอร์ม TGIX (TGIX-Inter-DX) สำหรับแพลตฟอร์ม TGIX ด้วยกัน และมาตรฐานสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างกลุ่มหรือแพลตฟอร์ม TGIX กับแพลตฟอร์มแลกเปลี่ยนข้อมูลอื่น ๆ (TGIX Federated-DX) โดยที่มาตรฐานสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูลเหล่านี้ กำลังอยู่ในระหว่างศึกษาและพัฒนา โดยพัฒนาต่อยอดจากมาตรฐานฯที่นำเสนอในฉบับนี้



## บรรณานุกรม

- [1] Wikipedia. (2020). Representational state transfer. เข้าถึงได้จาก:  
[https://en.wikipedia.org/wiki/Representational\\_state\\_transfer](https://en.wikipedia.org/wiki/Representational_state_transfer). (วันที่ค้นข้อมูล: 30 มิถุนายน 2021)
- [2] I. E. T. F. (IETF). (2017,ธันวาคม). The JavaScript Object Notation (JSON) Data Interchange Format. เข้าถึงได้จาก <https://datatracker.ietf.org/doc/html/rfc8259>. (วันที่ค้นข้อมูล: 30 มิถุนายน 2021)
- [3] Cybersecurity and Infrastructure Security Agency. (2021) Understanding Denial-of-Service Attacks. เข้าถึงได้จาก <https://us-cert.cisa.gov/ncas/tips/ST04-015>. (วันที่ค้นข้อมูล: 30 มิถุนายน 2021)
- [4] SmartBear Software. (2020). OpenAPI Specification V.3.0.3 [swagger.io](https://swagger.io/specification/). เข้าถึงได้จาก:  
<https://swagger.io/specification/>. (วันที่ค้นข้อมูล: 30 มิถุนายน 2021)
- [5] SmartBear Software. (2018). OpenAPI-Driven API Design. เข้าถึงได้จาก  
<https://swagger.io/blog/api-design/openapi-driven-api-design/>. (วันที่ค้นข้อมูล: 30 มิถุนายน 2021)
- [6] SmartBear Software. (2021). Sample Audit Service API. เข้าถึงได้จาก  
<https://app.swaggerhub.com/apis-docs/HCLERXECP/auditservice/1.0.0#/authentication>. (วันที่ค้นข้อมูล: 30 มิถุนายน 2021)
- [7] N. Sakimura, J. Bradley, M. B. Jones, B. d. Medeiros และ C. Mortimore. (2014,พฤศจิกายน) OpenID Connect Core 1.0. เข้าถึงได้จาก [https://openid.net/specs/openid-connect-core-1\\_0.html](https://openid.net/specs/openid-connect-core-1_0.html). (วันที่ค้นข้อมูล: 30 มิถุนายน 2021)
- [8] OAuth 2.0 Authorization Framework. (2021). เข้าถึงได้จาก <https://oauth.net/2/>. (วันที่ค้นข้อมูล: 30 มิถุนายน 2021)

[9] สถาบันมาตรวิทยาแห่งชาติ. (2021). เวลามาตรฐาน. เข้าถึงได้จาก  
[http://www.nimt.or.th/main/?page\\_id=356](http://www.nimt.or.th/main/?page_id=356). (วันที่ค้นข้อมูล: 30 มิถุนายน 2021)